

SX-GATE

Benutzerhandbuch

1 Vorwort.....	6
1.1 Hinweise.....	6
1.2 Namensnennungen zu enthaltenen Komponenten.....	7
1.3 Warenzeichen.....	10
2 Sicherheitsmaßnahmen und Hinweise.....	11
2.1 Warnung.....	11
2.2 Zu Ihrer Sicherheit.....	12
2.3 Netzstecker.....	13
2.4 Aufstellungsort.....	14
3 Vorbereiten des neuen SX-GATES.....	15
3.1 Auspacken.....	15
3.2 Mitgeliefertes Zubehör.....	16
3.3 Herstellen der Verbindung.....	17
3.3.1 Anschluss an eine ADSL-Wählverbindung.....	17
3.3.2 Anschluss an einen externen Router / eine xDSL- Standverbindung.....	18
3.3.3 Verbinden mit dem lokalen Netzwerk (LAN).....	19
3.3.4 Anschluss an das Stromnetz.....	20
4 Inbetriebnahme.....	21
4.1 Voraussetzungen.....	21
4.2 Einschalten und Booten.....	22
4.3 Einstellen der SX-GATE IP-Adresse.....	23
4.3.1 Ändern der IP-Adresse mit Hilfe des Displays.....	23
4.3.2 Ändern der IP-Adresse mit dem Web-Browser.....	25
4.4 Überprüfen der Verbindung zum SX-GATE.....	26
5 Erste Einstellungen.....	27
5.1 Zugriff auf die Web-Administrationsoberfläche.....	27
5.2 Grundkonfiguration.....	29
6 Konfiguration der Systeme im LAN.....	30
6.1 Netzwerk Parameter.....	30
6.2 Einrichten der Web-Browser.....	31
7 Startseite.....	32
7.1 Erste Schritte.....	33
7.2 Ressourcen.....	33
7.3 Netzwerkdurchsatz.....	33
7.4 Festplatte.....	34
7.5 Updates.....	34
7.6 Dienste.....	34
7.7 SX-GATE Info.....	34
7.8 SX-GATE Status.....	34
7.9 Netzwerkkarten.....	34
7.10 Mail-Server.....	35
7.11 Live-Log.....	35

8 Mein Konto.....	37
8.1 Passwort ändern.....	37
8.2 E-Mail Einstellungen.....	38
8.3 Groupware.....	45
8.4 Kontakt.....	46
9 Statistiken.....	49
9.1 System-Last.....	49
9.2 Netzwerk.....	50
9.2.1 Verbindungen.....	50
9.2.2 Durchsatz.....	50
9.2.3 Bandbreiten.....	51
9.3 Firewall.....	52
9.3.1 Paket-Filter.....	52
9.3.2 IDS/IPS.....	52
9.4 Mail-Server.....	53
9.5 Proxies.....	54
9.5.1 Web-Proxy.....	54
9.5.2 Reverse-Proxy.....	55
9.6 Web-Server.....	56
10 Monitoring.....	57
10.1 Log-Dateien.....	57
10.2 Werkzeuge.....	62
10.3 Netzwerk.....	70
10.4 VPN.....	73
10.5 Firewall.....	77
10.6 DHCP.....	78
10.7 Mail-Server.....	79
10.8 Web-Proxy.....	84
11 Definitionen.....	86
11.1 IP-Objekte.....	86
11.2 Protokolle.....	96
11.3 Zeiträume.....	100
11.4 Domainlisten.....	101
11.5 URL-Filter Listen.....	105
12 System.....	114
12.1 Grundeinstellungen.....	114
12.2 Dienste.....	124
12.3 Benutzerverwaltung.....	133
12.3.1 Einstellungen.....	134
12.3.2 Benutzer.....	139
12.3.3 Gruppen.....	165
12.4 Zertifikatsverwaltung.....	169
12.4.1 CA Zertifikate.....	169
12.4.1.1 SX-GATE-CA.....	169

12.4.1.2 SX-GATE-CA - Zertifikate.....	173
12.4.1.3 Benutzerdefinierte CAs.....	184
12.4.2 Schlüsselbund.....	185
12.4.3 MPKI-Profile.....	200
12.5 Backup.....	203
12.6 Update.....	214
12.7 Apps.....	217
12.8 Verwaltungsserver.....	218
12.9 Lizenzen.....	226
12.10 Abschalten/Neustart.....	227
13 Assistenten.....	228
13.1 LAN Anbindung.....	228
13.2 Internet-Zugang.....	233
13.3 Proxy-Konfiguration.....	243
13.4 E-Mail Einrichtung.....	252
13.5 IPsec-VPN.....	273
13.6 Fernwartung.....	280
14 Module.....	282
14.1 Netzwerk.....	282
14.1.1 Einstellungen.....	282
14.1.2 Schnittstellen.....	288
14.1.2.1 ADSL/Mobilfunk (adsl).....	291
14.1.2.2 Ethernet (eth).....	307
14.1.2.3 VLAN 802.1Q (vlan).....	325
14.1.2.4 WLAN (wlan).....	338
14.1.2.5 L2TP.....	347
14.1.2.6 Wireguard (wg).....	349
14.1.2.7 OpenVPN Client (ovpnc).....	356
14.1.2.8 OpenVPN Server (ovpns).....	360
14.1.2.9 OpenVPN Server (ovpns) - Client-spezifische Parameter.....	365
14.1.2.10 IPsec VPN (ipsec).....	367
14.1.2.11 IPsec VPN (ipsec) - Verbindungen.....	370
14.1.2.11.1 Verbindung mit Server.....	372
14.1.2.11.2 Verbindung mit AWS.....	381
14.1.2.11.3 Verbindung mit Client.....	388
14.1.2.11.4 Verbindung mit Windows IKEv2.....	394
14.1.2.11.5 Verbindung mit XAuth Client.....	398
14.1.2.11.6 Verbindung mit L2TP Client.....	403
14.2 Firewall.....	408
14.2.1 Einstellungen.....	408
14.2.2 Regeln.....	411
14.2.3 Bridge.....	436
14.3 DHCP.....	451
14.4 DNS.....	464
14.4.1 Einstellungen.....	464
14.4.2 Zonen.....	469

14.4.2.1 Domain.....	470
14.4.2.2 IPv4-Adressbereich (Reverse lookup).....	475
14.4.2.3 IPv6-Adressbereich (Reverse lookup).....	479
14.5 Mail-Server.....	483
14.5.1 POP-/IMAP-Server.....	483
14.5.2 SMTP Einstellungen.....	485
14.5.3 SPAM/Virus/Malware.....	501
14.5.4 Archivierung.....	530
14.5.5 TLS-Verschlüsselung.....	541
14.5.6 S/MIME-Gateway.....	544
14.5.7 Domains.....	555
14.6 POP-/IMAP-Client.....	567
14.6.1 Einstellungen.....	567
14.6.2 Server.....	567
14.7 Web-Proxy.....	576
14.7.1 Einstellungen.....	576
14.7.2 URL-Filter.....	592
14.7.3 Content-Filter.....	598
14.8 Reverse-Proxy.....	609
14.8.1 Einstellungen.....	609
14.8.2 Ports.....	611
14.8.2.1	612
14.8.2.2 - Virtuelle Hosts.....	617
14.9 Weitere Proxies.....	629
14.9.1 FTP-Proxy.....	629
14.9.2 SIP-Proxy.....	632
14.9.3 POP3-/SMTP-Proxy.....	634
14.9.4 SOCKS-Proxy.....	636
14.10 HTTP-Server.....	638
14.11 FTP-Server.....	642
14.12 SNMP-Server.....	643
14.13 Logging.....	645
14.14 Virens Scanner.....	653
14.15 Zeitserver.....	657
15 L2TP-IPSec-VPN Client-Konfiguration.....	659
15.1 Microsoft Windows.....	659
15.1.1 Automatische Konfiguration.....	660
15.1.2 Manuelle Konfiguration.....	663
15.2 Mac OS X.....	678
15.3 Apple iPhone.....	686
16 Kontakt.....	689
17 Support für Ihren SX-GATE.....	690

1 Vorwort

Wir bedanken uns, dass Sie sich für das Produkt SX-GATE entschieden haben.

Bei diesem Gerät handelt es sich um einen Router, Internet-Appliance-Server, Firewall und E-Mail-Server ... und das alles in einem Gerät! Natürlich bietet Ihnen der SX-GATE je nach Ausstattungsvariante noch eine ganze Reihe weitere Features. Damit Sie ihn auch optimal für Ihre Zwecke nützen und bedienen können, haben wir versucht dieses Installationshandbuch so einfach wie möglich zu gestalten. Deshalb nehmen Sie sich bitte die Zeit, dieses Handbuch sorgfältig zu lesen, da sich einige Abschnitte auf vorgelagerte Kapitel beziehen.

Da das Produkt SX-GATE ständig weiterentwickelt wird, empfehlen wir Ihnen den Erwerb eines Wartungsvertrages, der Sie kostenfrei mit Produkt-Updates und Upgrades, also auch neuen Funktionen versorgt. Auch sollten Sie sich unbedingt bei uns registrieren lassen, damit wir Ihnen schnell und unbürokratisch im Supportfalle helfen können.

Aufgrund der ständigen Verbesserung kann es vorkommen, dass bestimmte Bereiche in diesem Handbuch noch nicht vollständig beschrieben sind. In diesem Fall, bitten wir Sie, sich auf unserer Homepage <http://www.sx-gate.de> mit etwaigen hier fehlenden Informationen zu versorgen.

Sollten doch Probleme bei der Konfiguration des Gerätes auftreten, die Sie nicht alleine lösen können, steht Ihnen selbstverständlich unter den bekannten Supportnummern technische Hilfe zur Verfügung. Alle Angaben zum Kontakt mit ihm erhalten Sie im Kapitel *Kontakt* [S.689].

1.1 Hinweise

Dieses Handbuch wurde mit größtmöglicher Sorgfalt und Genauigkeit erstellt. Trotzdem kann von der XnetSolutions KG keinerlei Gewähr sowie Haftung auf Vollständigkeit und fehlerfreien Inhalt gegeben bzw. übernommen werden.

Da dieses Gerät sicherheitskritische Funktionen bereitstellt, ist darauf zu achten, dass alle Einstellungen im Erstbetrieb überwacht und geprüft werden.

Dieses Handbuch beschreibt alle Varianten des SX-GATEs. Bitte beachten Sie, dass je nach erworbenem Modell die Funktionalität unterschiedlich ist. Fehlt bei Ihrem Gerät Funktionalität, die in diesem Handbuch beschrieben ist, so können Sie diese nachordern, sofern es die Software betrifft. Bitte wenden Sie sich in diesem Fall an Ihren Vertriebspartner (siehe Kapitel *Kontakt* [S.689]). Je nach Ausstattung der Hardware können ebenfalls einige Funktionen nicht verwendet werden. Ihr Vertriebspartner wird Ihnen auch hier Lösungsmöglichkeiten aufzeigen.

Technische Änderungen des Gerätes sind ohne vorherige Ankündigung vorbehalten.

1.2 Namensnennungen zu enthaltenen Komponenten

This product includes software developed by Christos Zoulas

This product includes software developed by Craig Metz

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>).

This product includes software developed by David Corcoran <corcoran@linuxnet.com> <http://www.linuxnet.com> (MUSCLE)

This product includes software developed by Emmanuel Dreyfus

This product includes software developed by Gunnar Ritter and his contributors

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by Inferno Nettverk A/S, Norway

This product includes software developed by Jim Paris

This product includes software developed by Lars Fenneberg

This product includes software developed by Manuel Badzong

This product includes software developed by Marko Myllynen

This product includes software developed by Pedro Roque

This product includes software developed by Reuben Hawkins

This product includes software developed by The original development of BIND 9 was underwritten by the following organizations: Sun Microsystems, Inc., Hewlett Packard, Compaq Computer Corporation, IBM, Process Software Corporation, Silicon Graphics, Inc., Network Associates, Inc., U.S. Defense Information Systems Agency, USENIX Association, Stichting NLnet - NLnet Foundation, Nominum, Inc.

This product contains software (<https://github.com/creack/pty>) developed by Keith Rarick, licensed under the MIT License.

This product contains software (<https://github.com/kr/pty>) developed by Keith Rarick, licensed under the MIT License.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes data from The Université Toulouse 1 Capitole "Blacklist UT1", maintained by Fabrice Prigent (<http://dsi.ut-capitole.fr/blacklists/>), available under the Creative Commons Attribution-ShareAlike 4.0 license. The data used in this product is available from <http://update.linogate.de/blacklists/>.

This product includes software developed at CoreOS, Inc. (<http://www.coreos.com/>).

This product includes software developed at Docker, Inc. (<https://www.docker.com>).

This product includes software developed by Adam Glass and Charle Hannum.

This product includes software developed by Berkeley Software Design Inc.

This product includes software developed by Bill Paul.

This product includes software developed by Chris Provenzano.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by David A. Holland

This product includes software developed by HD Associates, Inc

This product includes software developed by HD Associates, Inc and Jukka Antero Ukkonen.

This product includes software developed by Inferno Nettverk A/S, Norway.

This product includes software developed by John Birrell.

This product includes software developed by Kawasaki LSI.

This product includes software developed by Kungliga Tekniska Högskolan and its contributors.

This product includes software developed by Niels Provos.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Softweyr LLC, the University of California, Berkeley, and its contributors.

This product includes software developed by Trimble Navigation, Ltd.

This product includes software developed by Yen Yen Lim an North Dakota State University

This product includes software developed by the Computer System Engineering Group at Lawrence Berkeley Laboratory.

This product includes software developed by the Computer Systems Laboratory at the University of Utah.

This product includes software developed by the Kungliga Teknisk Hgskolan and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory.

This product includes software developed by the University of Michigan, Meri Network, Inc., and their contributors.

This product includes software developed for the NetBSD Project. See <http://www.NetBSD.org/> for information about NetBSD.

This product includes software developed or owned by Calder International, Inc.

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

This product includes software written by Tim Hudson (tjh@mincom.oz.au)

This product includes software developed by freebxml.org (<http://www.freebxml.org/>).

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors

1.3 Warenzeichen

Alle in diesem Dokument genannten Firmen- und Produktbezeichnungen sind eingetragene Warenzeichen des jeweiligen Inhabers. SX-GATE ist ein eingetragenes Warenzeichen der XnetSolutions KG. Die Nennung hier nicht aufgeführter Warenzeichen ist kein Hinweis auf deren freie Verfügbarkeit.

Copyright ©, XnetSolutions KG

2 Sicherheitsmaßnahmen und Hinweise

Bitte lesen Sie die nachfolgenden Abschnitte aufmerksam durch, bevor Sie den SX-GATE in Betrieb nehmen.

2.1 Warnung

Zur Verhütung von Brand und elektrischem Schlag darf dieses Gerät weder Regen noch Nässe ausgesetzt werden.

2.2 Zu Ihrer Sicherheit

Auf keinen Fall das Gehäuse öffnen oder sogar im offenen Zustand betreiben, da die Gefahr von elektrischem Schlag besteht. Zudem können schwere Geräteschäden verursacht werden. Im Inneren des Gerätes befinden sich keine Teile, die vom Nichtfachmann gewartet werden können. Bitte wenden Sie sich für Geräteerweiterungen oder Reparaturen nur an den Kundendienst.

2.3 Netzstecker

Unterlassen Sie das Anschließen des Netzsteckers mit feuchten oder gar nassen Händen. Halten Sie das Netzkabel von Heizquellen fern. Stellen Sie keine schweren Gegenstände auf das Netzkabel. Falls das Gerät Rauch, ungewöhnliche Gerüche oder Geräusche abgibt, ziehen Sie unverzüglich den Netzstecker ab und setzen Sie sich mit dem Kundendienst in Verbindung.

2.4 Aufstellungsort

Vermeiden Sie ein Aufstellen in direkter Sonneneinstrahlung, neben Heizgeräten, an Orten mit hohen Temperaturen (mehr als 35°C) oder hoher Feuchtigkeit (mehr als 90%) und sehr staubigen Orten. Stellen Sie das Gerät nicht an Plätzen auf, an denen es Vibrationen ausgesetzt sein könnte. Verwenden Sie nur eine ebene Fläche zum Aufstellen, da sonst Bauteile im Inneren beschädigt werden können. Halten Sie das Gerät auch fern von magnetischen Gegenständen bzw. Gegenständen, die Magnete enthalten, z. B. Lautsprecher-Boxen.

3 Vorbereiten des neuen SX-GATEs

3.1 Auspacken

Entnehmen Sie das Gerät vorsichtig aus der Verpackung. Bewahren Sie den Karton mit allen Verpackungsmaterialien für einen späteren Versand oder Transport auf. Sollte das Gerät starken Temperaturschwankungen ausgesetzt gewesen sein (z. B. vom kalten Fahrzeug in einen geheizten Raum), warten Sie circa 1 Stunde ab, damit es sich klimatisieren kann. Dies ist ratsam, da sich Kondensation im Gerät gebildet haben könnte, die beim Einschalten schwere Geräteschäden verursachen kann.

3.2 Mitgeliefertes Zubehör

Überprüfen Sie den Verpackungsinhalt anhand der folgenden Liste. Sollten Teile fehlen, so wenden Sie sich bitte umgehend an den technischen Kundendienst. Die entsprechende Kontaktadresse finden Sie im Kapitel *Kontakt* [S.689] in diesem Handbuch. Wir leisten selbstverständlich umgehend Ersatz.

- SX-GATE (Internet-Firewall-Gateway)
- Kaltgerätekabel (220V)

3.3 Herstellen der Verbindung

Die folgenden Verbindungsmöglichkeiten setzen voraus, dass entsprechende Anschlüsse am SX-GATE und im Installationsumfeld vorhanden sind. Die Ausstattung des Geräts kann in unterschiedlichen Ausbaustufen variieren.

3.3.1 Anschluss an eine ADSL-Wählverbindung

SX-GATE unterstützt folgende ADSL-Leitungsverfahren:

- ADSL / VDSL mit PPP-over-Ethernet (PPPoE), auch über VLAN
- ADSL mit PPP-over-ATM (PPPoA) über Modem mit PPTP-to-PPPoA-Relay

Es wird empfohlen, das DSL-Modem direkt mit einer nicht anderweitig genutzten Netzwerk-Schnittstelle des SX-GATES zu verbinden. Für die Internet-Verbindung ist eine zweite Netzwerk-Schnittstelle im System vorgesehen. Sie wird als "eth1" bezeichnet und ist u.U. auch mit "DSL" oder "WAN" beschriftet.



Der Anschluss an eine ADSL-Wählleitung muss über ein externes DSL-Modem erfolgen. Ein geeignetes Modem erhalten Sie von Ihrem Internet-Provider. Falls Ihnen ein Router mit integriertem DSL-Modem zur Verfügung gestellt wurde, wird empfohlen, den Router in den Modem-Betriebsmodus (PPPoE Passthrough) umzustellen.

3.3.2 Anschluss an einen externen Router / eine xDSL-Standverbindung

Ihr SX-GATE unterstützt die Anbindung an Ethernet-Netzwerke mit 10, 100 oder 1000 Mbit/s.

Für die Internet-Verbindung ist die zweite Netzwerk-Schnittstelle im System vorgesehen. Sie wird als "eth1" bezeichnet und ist u.U. auch mit "DSL" oder "WAN" beschriftet. Verbinden Sie diese Schnittstelle direkt mit dem externen Router. Eventuell ist dazu ein spezielles "gedrehtes" Patchkabel erforderlich. Sie können die Verbindung auch über einen dazwischengeschalteten Switch herstellen. Verwenden Sie dazu nicht den Switch, an dem das LAN angeschlossen ist, sondern ein separates Gerät.

3.3.3 Verbinden mit dem lokalen Netzwerk (LAN)

Ihr SX-GATE unterstützt die Anbindung an Ethernet-Netzwerke mit 10, 100 oder 1000 Mbit/s.

Die Verbindung des SX-GATES mit Ihrem LAN erfolgt über die erste Netzwerk-Schnittstelle des Systems. Sie wird als "eth0" bezeichnet und ist u.U auch mit "LAN" beschriftet. Verbinden Sie diese Schnittstelle mit einem freien Anschluss Ihres LAN-Switches.



Achten Sie darauf, dass Sie die Schnittstellen nicht vertauschen!
Ein Verwechseln kann dazu führen, dass Ihr SX-GATE nicht ansprechbar ist!

3.3.4 Anschluss an das Stromnetz

Verwenden Sie zum Anschluss des Gerätes an die Stromversorgung das mitgelieferte Netzkabel bzw. Netzteil. Bitte beachten Sie, dass ein Betrieb des Gerätes nur an 230 Volt Wechselstrom möglich ist.

Es wird empfohlen, das Gerät an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen. Ansonsten könnte die Konfiguration des SX-GATE oder ein Hardwarebauteil des Gerätes bei einem plötzlichen Stromausfall beschädigt werden.

4 Inbetriebnahme

4.1 Voraussetzungen

Da alle Einstellungen des SX-GATES über eine Web-Oberfläche vorgenommen werden, benötigen Sie ein Computer-System mit Web-Browser wie beispielsweise Google Chrome oder Mozilla Firefox. Sie müssen von diesem System aus via Netzwerk auf SX-GATES LAN-Schnittstelle zugreifen können. Ggf. muss dazu vorübergehend die IP-Konfiguration des Computer-Systems geändert werden.

4.2 Einschalten und Booten

Betätigen Sie den Einschalter an der Vorderseite des Gerätes. Der Bootvorgang dauert etwa zwei Minuten. Bitte warten Sie diesen Zeitraum ab, bevor Sie mit den weiteren Einstellungen fortfahren!

Einige SX-GATE-Modelle verfügen über ein eingebautes LCD-Display. Hier wird die Bereitschaft des Geräts dadurch angezeigt, dass die Boot-Meldung aus dem Display verschwindet und durch eine Status-Anzeige ersetzt wird.

4.3 Einstellen der SX-GATE IP-Adresse

SX-GATE wird werksseitig mit der IP-Adresse 192.168.0.254 und der Netzmaske 255.255.255.0 ausgeliefert. In der Regel wird es erforderlich sein, diese Werte an Ihr LAN anzupassen.



Bevor Sie eine neue Adresse konfigurieren, sollten Sie sicher stellen, dass die neue Adresse noch nicht im Netzwerk vergeben ist. Jede IP-Adresse darf nur einmal im Netzwerk vorkommen und alle System im Netzwerk müssen die gleiche Netzmaske verwenden.

Beachten Sie, dass SX-GATE nicht in der Lage ist, von einem vorhanden DHCP-Server automatisch eine IP-Adresse zu beziehen. SX-GATE ist darauf angewiesen, im LAN immer die gleiche IP-Adresse zu verwenden.

Es ist nicht möglich, IP-Adressen für das LAN frei auszuwählen. Gemäß Internet-Standard RFC-1918 sind für lokale Netzwerke Adressen vorgesehen, die mit 10, 172.16 bis 172.31 sowie 192.168 beginnen. IP-Adressen außerhalb der genannten Bereiche sind im Internet offiziell vergeben und Eigentum anderer. Es wird daher dringend empfohlen, für interne LANs nur Adressen aus diesen Bereichen zu nutzen. Wenn Sie z.B. das Netzwerk 192.168.0.0 mit der Netzmaske 255.255.255.0 verwenden, können Sie 254 IP-Adressen im Bereich 192.168.0.1 bis 192.168.0.254 in Ihrem LAN vergeben.

Um SX-GATEs LAN IP zu ändern, stehen folgende Möglichkeiten zur Verfügung:

4.3.1 Ändern der IP-Adresse mit Hilfe des Displays

Einige SX-GATE-Modelle haben eingebaute Displays für die Anzeige von Statusinformationen. Über das Display lässt sich auch SX-GATEs LAN IP-Adresse und Netzwerkmaske konfigurieren. Drücken Sie die "Enter"-Taste des Displays um die "IP-Configuration" aufzurufen. Mit Hilfe der Pfeil-Tasten "auf" und "ab" lässt sich die Zeile mit der IP-Adresse, der Netzmaske oder "Exit" auswählen. Drücken Sie dann die "Enter"-Taste auf der gewünschten Zeile.

Die IP-Adresse wird Ziffer für Ziffer geändert. Die aktuell ausgewählte Ziffer ist unterstrichen. Mit Hilfe der Pfeil-Tasten "auf" und "ab" verändern Sie den Zahlenwerte dieser Ziffer. Mit der Pfeil-Taste "rechts" wechseln Sie zur nächsten Ziffer. Drücken Sie erneut die "Enter"-Taste sobald Sie die gewünschte IP-Adresse eingestellt haben.

Die Netzmaske wird mit Hilfe der Pfeil-Tasten "auf" und "ab" schrittweise in die nächst größere bzw. kleinere Maske geändert. Drücken Sie die "Enter"-Taste, wenn Sie die Netzmaske korrekt eingestellt haben.

Mit "Exit" verlassen Sie die "IP-Configuration". Sollten Sie die IP-Adresse oder die Netzmaske geändert haben, werden Sie bei Auswahl von "Exit" gefragt, ob Sie die Änderungen übernehmen wollen ("Save?"). Mit der Pfeil-Taste "rechts" wechseln Sie zwischen "No" um die Änderungen zu verwerfen und "Yes" um sie zu speichern. Bestätigen Sie dann mit der "Enter"-Taste. Änderungen sind nach wenigen Sekunden gespeichert und konfiguriert.

4.3.2 Ändern der IP-Adresse mit dem Web-Browser

Wenn Ihr SX-GATE-Modell nicht über ein eingebautes Display verfügt, müssen Sie die IP-Adresse in der Web-Administrationsoberfläche ändern. Sie benötigen dazu ein Computer-System mit Web-Browser, das eine IP-Adresse zwischen 192.168.0.1 und 192.168.0.253 mit Netzmask 255.255.255.0 konfiguriert hat. Sollte ein System mit bereits passender Konfiguration zur Verfügung stehen, können Sie mit dem nächsten Kapitel fortfahren.

Andernfalls müssen Sie die IP-Konfiguration des Computers anpassen. Bitte entnehmen Sie Details zur IP-Konfiguration dem Betriebssystem-Handbuch Ihres Computers.

Sofern der Computer die IP-Konfiguration automatisch von einem DHCP-Server bezieht, können Sie den Computer vorübergehend direkt mit dem LAN-Anschluß des SX-GATEs verbinden. Im Auslieferungszustand fungiert SX-GATE nämlich als DHCP-Server. Um den Computer direkt mit SX-GATE verbinden zu können, ist ggf. ein gekreuztes Netzkabel erforderlich, das nicht im Lieferumfang enthalten ist. Ersatzweise können Sie einen Switch zwischenschalten, an dem jedoch kein weiteres System angeschlossen sein darf. Geben Sie dann in der IP-Konfiguration Ihres Computers die aktuelle IP-Adresse frei oder starten Sie das System neu. Anschließend sollte der Computer von SX-GATEs DHCP-Server eine passende IP-Adresse erhalten haben.

Wenn Sie die bestehende Verkabelung nicht ändern wollen oder es nicht möglich ist, eine IP-Adresse über DHCP zu beziehen, tragen Sie bitte manuell eine passende IP-Adresse (z.B. 192.168.0.1) mit Netzmaske 255.255.255.0 in der IP-Konfiguration des Computers ein.

4.4 Überprüfen der Verbindung zum SX-GATE

Das Überprüfen der Netzwerkverbindung zwischen Ihrem Computer-System und SX-GATE erfolgt mit Hilfe des "Ping"-Befehls. Beantwortet SX-GATE die Ping-Anfrage Ihres Computers, ist die IP-Verbindung in Ordnung.

Öffnen Sie ein Befehlsfenster auf Ihrem Computer und geben Sie folgenden Befehl ein:
ping 192.168.0.254

Sofern die IP-Adresse Ihres SX-GATEs bereits geändert wurde, ersetzen Sie bitte 192.168.0.254 durch die aktuelle IP.

Wenn Sie eine Fehlermeldung erhalten, überprüfen Sie bitte die Einstellungen und korrigieren Sie eventuell fehlerhafte Eingaben. Prüfen Sie ferner Kabel und Anschlüsse. Leuchten die Link-LEDs am Switch sowie an den Netzwerkkarten? Wenn eine Firewall auf Ihrem Computer installiert ist, überprüfen Sie auch, ob die Firewall das Senden und Empfangen von Ping-Befehlen zulässt.

5 Erste Einstellungen

5.1 Zugriff auf die Web-Administrationsoberfläche

Starten Sie Ihren Web-Browser, um mit der Konfiguration des SX-GATEs zu beginnen. Geben Sie dazu die Adresse "https://192.168.0.254:44344" in der Adresszeile des Browsers ein. Wurde SX-GATEs IP-Adresse zuvor geändert, ersetzen Sie bitte die voreingestellte IP 192.168.0.254 durch die neue IP-Adresse.



Der Zugriff auf die Administrationsoberfläche erfolgt verschlüsselt über das HTTPS-Protokoll (https://) auf Port 44344.

Falls Sie ohne Angabe des Ports zugreifen (https://192.168.0.254), wird die Anfrage auf Port 44344 umgeleitet.

Der Browser sollte nun eine Zertifikatswarnung anzeigen. Dies ist normal, da SX-GATE im Auslieferungszustand nicht über ein echtes Server-Zertifikat verfügt, sondern lediglich über ein auf den Namen "Internet Appliance" ausgestelltes, selbstsigniertes Zertifikat. Bestätigen Sie bitte dem Browser, dass Sie dennoch auf die Seite zugreifen wollen. Im Falle einer Umleitung auf Port 44344 müssen Sie ein zweites Mal bestätigen.

Sollten Sie keine Zertifikatswarnung erhalten, prüfen Sie bitte ob Sie die korrekte Adresse in der Adresszeile des Browsers eingegeben haben. Die Adresse muss unbedingt mit "https://" beginnen, nicht mit "http://". Stellen Sie ferner sicher, dass im Browser kein Proxy konfiguriert ist, der ggf. die Verbindung verhindern könnte.

Möglicherweise erscheint nun eine Maske, in der Sie nach dem SX-GATE Lizenzschlüssel gefragt werden. Sie erhalten den Lizenzschlüssel von Ihrem Fachhändler. Der Schlüssel besteht aus 5 Gruppen von je 5 Zeichen, getrennt durch Bindestriche. Geben Sie den Schlüssel nun ein.

Sofern noch nicht festgelegt, müssen Sie beim erstmaligen Zugriff das Kennwort für den Benutzer "admin" vergeben.



Wählen Sie bitte ein ausreichend langes und komplexes Kennwort. Es sollte aus mind. 10 Zeichen bestehen und neben Kleinbuchstaben auch Großbuchstaben, Ziffern und Sonderzeichen enthalten.

Schließlich sollte die Anmeldemaske Ihres SX-GATEs angezeigt werden.

Nachdem Sie sich angemeldet haben, erscheint auf dem Bildschirm die Startseite Ihres SX-GATEs.

5.2 Grundkonfiguration

Auf der SX-GATE-Startseite finden Sie die Checkliste "Erste Schritte". Arbeiten Sie diese Schritt für Schritt der Reihe nach ab, um die Grundkonfiguration Ihres SX-GATES vorzunehmen. Die Detailkonfiguration der einzelnen Komponenten können Sie später über das Menü auf der linken Seite bearbeiten.



Beachten Sie bitte die ausführliche Online-Hilfe, die Ihnen nähere Informationen zu den einzelnen Optionen liefert. Klicken Sie auf das Fragezeichen-Symbol oder auf den Titel der jeweiligen Option damit die zugehörige Hilfe angezeigt wird.

Sofern Sie noch die LAN IP-Adresse Ihres SX-GATES anpassen müssen, geschieht dies über den Punkt "LAN Anbindung" der Checkliste. Beachten Sie bitte, dass SX-GATE kurz nach Abschluss dieses Assistenten nicht mehr über die alte sondern nur noch über die neue IP-Adresse erreichbar ist. Sobald Sie SX-GATE unter der alten Adresse nicht mehr erreichen, sollten Sie zunächst die IP-Adresse Ihres Computers zurücksetzen, falls Sie diese zuvor für den Zugriff auf SX-GATES Standard-IP geändert hatten. Passen Sie dann die IP auch in der Adresszeile des Browsers an, um wieder auf die Administrationsoberfläche Ihres SX-GATES zugreifen zu können.

6 Konfiguration der Systeme im LAN

Damit ein Computer-System im LAN sicheren Zugang zum Internet über den SX-GATE erhält, sind verschiedene Einstellungen vorzunehmen.

6.1 Netzwerk Parameter

Damit ein Computer-System im LAN zumindest begrenzt über SX-GATE mit dem Internet kommunizieren kann, genügt es, dem System eine passende IP-Adresse und Netzmask zuzuweisen. Für vollwertigen Zugriff auf das Internet muss zudem SX-GATEs LAN-IP als Standardgateway/Router und DNS-Server eingetragen werden. Bezieht das System die Netzwerk-Konfiguration automatisch von einem DHCP-Server, sind diese Einstellungen in der Konfiguration des DHCP-Servers vorzunehmen.



In einem Windows-Netzwerk wird als DNS in der Regel die IP-Adresse des Windows-Servers und nicht des SX-GATEs eingetragen. Hinterlegen Sie SX-GATEs LAN-IP dann in der DNS-Konfiguration des Windows-Servers als Weiterleitung.

Details zur Netzwerk-Konfiguration der Systeme im LAN entnehmen Sie bitte den jeweiligen Betriebssystem-Handbüchern.

6.2 Einrichten der Web-Browser

Systeme im LAN sollten soweit als möglich SX-GATEs Proxy-, Forwarder- und Relay-Dienste zur Kommunikation mit dem Internet verwenden. Auf die Sicherung der Internet-Kommunikation von Web-Browsern ist der SX-GATE Web-Proxy spezialisiert. Damit die Browser den Proxy nutzen, muss dieser zunächst in den Browser-Einstellungen konfiguriert werden.



In der Grundeinstellung verhindert SX-GATEs Firewall die direkte Kommunikation von Systemen im LAN mit Systemen im Internet vollständig! Ohne passende Proxy-Einstellungen ist zunächst kein Internet-Zugriff möglich.

Öffnen Sie die Proxy-Einstellungen des Browsers. Diese befinden sich je nach eingesetztem Web-Browser in unterschiedlichen Konfigurations-Menüs. Suchen Sie nach Netzwerk-, Verbindungs- oder LAN-Einstellungen. Konsultieren Sie im Zweifelsfalle die Dokumentation des installierten Browsers. Tragen Sie als Proxy die LAN-IP des SX-GATEs mit Port 8080 ein.



In Browsern die auch zur Administration des SX-GATEs genutzt werden, sollte zusätzlich die LAN-IP des SX-GATE von der Proxy-Nutzung ausgeschlossen werden.

Es ist auch möglich, ein Proxy-Konfigurationsskript zu nutzen oder die automatisch Erkennung der Proxy-Konfiguration zu nutzen. Im Assistenten "Proxy-Konfiguration" erfahren Sie mehr über diese Optionen und können evtl. notwendige Einstellungen vornehmen.



In Windows-Netzwerken ist es möglich, Proxy-Einstellungen zentral mit Hilfe von Gruppenrichtlinien an die Arbeitsplätze zu verteilen.

7 Startseite

Die SX-GATE Administrations-Oberfläche kann prinzipiell ohne JavaScript und Cookies bedient werden. Der volle Funktionsumfang und Komfort steht jedoch nur bei aktiviertem JavaScript zur Verfügung. Cookies werden verwendet, um individuelle Anpassungen der Oberfläche abzuspeichern.



Alle nachfolgend beschriebenen Funktionen setzen einen modernen Browser mit aktiviertem JavaScript voraus.

Docks und Docklets

Auf der Startseite werden diverse Informations- und Status-Fenster angeboten, die im Folgenden "Docklets" bezeichnet werden. Der zentrale Fensterbereich auf der Startseite dient als "Dock" für diese Docklets. Über die Lasche am rechten Rand des zentralen Fensterbereichs lässt sich dessen Breite ändern. Bietet das Browser-Fenster ausreichend Platz, befindet sich rechts ein weiteres Dock. Dieses bleibt in allen Menüs sichtbar und empfiehlt sich für Docklets mit Informationen die man permanent im Auge behalten möchte.

Mit Ausnahme des Docklets "Erste Schritte" kann die Position aller Docklets geändert werden, indem Sie in der Titelleiste die linke Maustaste gedrückt halten und dann das Fenster verschieben. So ist es nicht nur möglich, die Position innerhalb des Docks zu ändern. Auf diese Weise lässt sich ein Docklet auch zwischen dem Dock der Startseite und dem permanent sichtbaren Dock am rechten Rand hin und her bewegen. Am oberen Rand jedes Docks befindet sich ein Bereich in dem Docklets mehrspaltig, also in voller Breite des Docks angezeigt werden. Darunter werden Docklets in Spalten mit normaler Breite eingeordnet.



Die Position der Docklets und auch die Breite der Docks werden in einem Browser-Cookie gespeichert.

Die Titelleiste der Docklets enthält diverse Symbole. Die Symbole auf der linken Seite ermöglichen es, das Docklet auf die Titelzeile zu reduzieren bzw. wieder voll darzustellen, das Docklet in einem eigenständiges Browser-Fenster zu öffnen und den Inhalt zu aktualisieren. Über die Symbole rechts lässt sich die Hilfe zum jeweiligen Docklet aufrufen und das Docklet schließen.



Um ein geschlossenes Docklet wieder sichtbar zu machen bzw. um eine Liste aller verfügbaren Docklets zu erhalten, bewegen Sie bitte die Maus auf das Schraubenschlüssel-Symbol in der rechten oberen Ecke der Administrations-Oberfläche.

Live-Log

Die laufend aktualisierte Anzeige einer Log-Datei wird ebenfalls über das Schraubenschlüssel-Symbol in der rechten oberen Ecke der Administrations-Oberfläche aktiviert. Am unteren Bildrand öffnet sich ein Fenster, dessen Höhe sich durch Ziehen an der mittig angebrachten Lasche anpassen lässt.

Online Hilfe

Die Hilfe zum aktuellen Bildschirm kann durch Klick auf das Fragezeichen geöffnet werden. Ist am rechten Bildrand das zusätzliche Dock verfügbar, öffnet sich die Hilfe darin. Der angezeigte Hilfe-Text folgt dabei automatisch der aktuell angezeigten Bildschirmmaske. Ohne das rechte Dock überlagert das Hilfe-Fenster die aktuelle Maske. Das Hilfe-Fenster lässt sich verschieben und wird automatisch geschlossen wenn auf eine andere Seite gewechselt wird.



Um die Hilfe zu einer bestimmten Seite dauerhaft anzuzeigen, klicken Sie bitte das Symbol in der Titelzeile zum Öffnen in einem separaten Browser-Fenster.

Zunächst wird immer die Hilfe zum aktuellen Reiter (Tab) angezeigt. Klicken Sie auf die farblich hinterlegten Titel, um die Texte der enthaltenen Eingabeelement oder der übergeordneten Menüpunkte anzuzeigen. Ein fehlender Pfeil vor dem Titel zeigt an, dass für diesen Punkt kein Hilfe-Text verfügbar ist.

7.1 Erste Schritte

Dieses Docklet unterstützt Sie bei der Grundkonfiguration Ihres SX-GATEs. Klicken Sie nacheinander auf die einzelnen Texte um die zugehörige Konfiguration durchzuführen. Wenn das System soweit eingerichtet ist, können Sie das Docklet mit Hilfe des "X"-Symbols in der rechten oberen Ecke schließen. Den weiteren Docklets steht so mehr Platz zur Verfügung.

7.2 Ressourcen

In diesem Docklet sehen Sie Balken für die Prozessor-Auslastung, die allgemeine System-Last sowie die Belegung von Haupt- und Swapspeicher.

7.3 Netzwerkdurchsatz

Pro Schnittstelle wird hier je ein Balken für den ein- und ausgehenden Durchsatz angezeigt. Die Prozentangabe bezieht sich dabei auf den bislang maximal

gemessenen Durchsatz seit Start des Dienstes. Schnittstellen werden erst angezeigt, sobald tatsächlich Daten geflossen sind.

7.4 Festplatte

Hier wird die Belegung der einzelnen Festplatten-Partitionen angezeigt. Bei Systemen mit RAID zeigt zudem ein rotes oder grünes Licht an, ob das RAID in Ordnung ist. Wird das RAID gerade neu aufgebaut, ist eine Fortschrittsanzeige zu sehen.

7.5 Updates

Hier sehen Sie die verfügbaren Updates.

7.6 Dienste

In dieser Übersicht werden die Dienste aufgeführt, die bei Systemstart aktiviert werden. Ein rotes Licht erscheint, wenn der Dienst aktuell gestoppt ist. Ein gelbes Licht wird bei Diensten angezeigt die aktuell laufen, bei Systemstart jedoch nicht aktiviert werden.

7.7 SX-GATE Info

Dieses Docklet fasst die wichtigsten Eckdaten zu Ihrem SX-GATE und seinen Lizenzen zusammen.

7.8 SX-GATE Status

Werden bei einem kurzen Systemcheck Unregelmäßigkeiten erkannt, finden Sie hier entsprechende Meldungen.

7.9 Netzwerkkarten

Dies ist eine Übersicht über die Einstellungen der Netzwerkkarten.

Die Werte zeigen im einzelnen:

- die Hardware-Adresse (MAC) der Netzwerkkarte
- die Geschwindigkeit, mit der die Netzwerkkarte arbeitet in MBit/s
- den ausgehandelte bzw. eingestellte Duplex Modus (Full, Half)
- ob die automatische Aushandlung (Auto-negotiation) aktiv ist
- den momentanen Linkstatus

Ein Minuszeichen oder eine weiße Ampel bedeutet, dass das System diesen Wert nicht ermitteln kann.

7.10 Mail-Server

Hier werden Summenwerte aus dem Menü "Monitoring > Mail-Server" angezeigt.

7.11 Live-Log

Neben den bereits von den Docklets bekannten Symbolen gibt es beim Live-Log weitere Steuerelemente in der Titelleiste:

- Mit dem Pause- bzw. Pfeil-Symbol kann das Live-Log angehalten bzw. fortgesetzt werden
- Über das Symbol mit dem Kreuz wird der Anzeigebereich geleert
- Das Filtersymbol öffnet und schließt den Eingabebereich für Suchfilter, die nachfolgend genauer beschrieben werden
- Drücken Sie das Diskettensymbol um den Inhalt des Live-Logs als Textdatei zu exportieren
- Schließlich haben Sie noch die Möglichkeit, das anzuzeigende Log auszuwählen

Die Filterfunktion unterscheidet nicht zwischen Groß- und Kleinschreibung und unterstützt sog. "Reguläre Ausdrücke". Nachfolgend eine kurze Erklärung der wichtigsten syntaktischen Regeln:

`+ - ? . * ^ $ () [] { } \`

Zeichen mit Sonderbedeutung. Wenn Sie nach einem dieser Zeichen suchen, müssen Sie ein "\" voranstellen. Beispielsweise finden Sie einen Punkt mit "\."

- (Minus) am Anfang des Suchbegriffs

Invertiert die Suche. Es wird nach Zeilen gesucht, die das nachfolgende Suchmuster NICHT enthalten.

. (Punkt)

Ein beliebiges Zeichen

[...]

Ein Zeichen aus der angegebenen Menge. So passt z.B. "[0-9a-f:]" auf entweder eine beliebige Ziffer, einen Buchstaben von a bis f oder den Doppelpunkt.

(...)

Gruppiert mehrere Elemente. Beispiel siehe unter "|".

? (Fragezeichen), * (Stern), + (Plus)

Hierbei handelt es sich um Multiplikatoren, die sich auf das unmittelbar davor stehende Zeichen bzw. die unmittelbar davor stehende Menge oder Gruppe beziehen. Fragezeichen bedeutet optional (null- oder einmal), Stern bedeutet

optional beliebig oft (null- bis n-mal), Plus bedeutet mindestens einmal (ein- bis n-mal).

| (Senkrechter Strich)

Oder-Verknüpfung. Um beispielsweise in der Uhrzeit 19 oder 20 Uhr zu finden, eignet sich das Muster " (19|20):"

^ (Dach), \$ (Dollar)

Diese Zeichen stehen für Beginn bzw. Ende des Textes. So sucht "^error" Zeilen mit dem Wort "error" am Spaltenbeginn.

Für jedes Suchmuster können Sie festlegen, ob dieses in allen oder nur in einer bestimmten Spalte gesucht werden soll. Drücken Sie das Plus-Symbol um weitere Eingabzeilen für Suchmuster zu erhalten. Sie können dann auch festlegen, ob diese "UND" oder "ODER" verknüpft werden sollen.

Über das Symbol am rechten Rand der Zeile mit den Spalten-Überschriften, kann die Anzeige einzelner Spalten an- und ausgeschaltet werden.

8 Mein Konto

Das Hauptmenü "Mein Konto" erlaubt es Benutzern bestimmte Einstellungen für das eigene Konto selbst vorzunehmen. Dazu gehört z.B. die Änderung des Passwortes. Im Untermenü "Kontakt" lassen sich Ansprechpartner für den Problemfall hinterlegen.

8.1 Passwort ändern

Aktuelles Passwort

Um Ihr Passwort ändern zu können, müssen Sie zunächst das derzeitige Passwort angeben.

Neues Passwort

Hier können Sie Ihr Passwort für den Zugriff auf die verschiedenen Dienste des SX-GATE ändern. Um Tippfehler weitestgehend ausschließen zu können, müssen Sie das neue Passwort zweimal eingeben.

8.2 E-Mail Einstellungen

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

8.2-A Weiterleitung.....	38
8.2-B SPAM-Filter.....	38
8.2-C SPAM Bewertung.....	40
8.2-D SPAM Adressen.....	42
8.2-E Abwesenheit.....	43
8.2-F Ordner.....	44

8.2-A Weiterleitung

E-Mail weiterleiten an

In diesem Bereich können Sie eine Weiterleitung der für Sie bestimmten E-Mails an andere interne und externe Adressen einstellen. Dazu ist im Eingabe-Feld die E-Mail-Adresse des Empfängers einzutragen. Drücken Sie dann den Schalter "Hinzufügen". Sie können beliebig viele Empfänger auf diese Weise angeben. Diese erhalten dann alle ein Exemplar von der an Ihr Postfach adressierten Mail. Um eine Weiterleitung aufzuheben, wählen Sie bitte die entsprechende Adresse in der Liste aus und drücken Sie dann den Schalter "Entfernen".

Kopie von weitergeleiteten E-Mails behalten

Werden Ihre E-Mails an andere Adressen weitergeleitet, so können Sie mit Hilfe dieses Schalters steuern, ob stets auch ein Exemplar der E-Mails in Ihr eigenes Postfach zugestellt werden soll. Ist dieser Schalter nicht aktiviert, so werden keinerlei E-Mails mehr in Ihr Postfach zugestellt sobald eine Weiterleitung aktiv ist.



Solange keine Weiterleitung eingetragen ist, hat dieser Schalter keine Funktion.

8.2-B SPAM-Filter

Wenn Sie mindestens einen der Schwellwerte aktivieren, müssen alle eingehenden E-Mails, die in Ihr Postfach zugestellt werden, einen SPAM-Mail-Filter passieren. Unter einer SPAM-Mail versteht man eine unerwünschte Werbe-Mail mit meist dubioser Herkunft.

Der SPAM-Mail-Filter des SX-GATE klassifiziert automatisch den Inhalt von E-Mails anhand typischer Phrasen oder anderer Merkmale die auf eine unerwünschte Werbe-Mail (SPAM-Mail) zutreffen. Dazu ist im SX-GATE eine Datenbank mit Kriterien enthalten, die mit einem Punktesystem bewertet werden. Das erreichte Punkteergebnis ermöglicht das Filtern von E-Mails. Alle Merkmale, die auf eine SPAM-Mail hindeuten, erhöhen den Punktestand, während für Merkmale die auf eine reguläre Mail hindeuten wieder Punkte abgezogen werden. Je höher das Bewertungsergebnis, umso wahrscheinlicher handelt es sich um eine SPAM-Mail.



E-Mails mit einer Größe von mehr als 1MB werden vom SPAM-Mail-Filter nicht klassifiziert um Ressourcen zu schonen. Dies stellt jedoch keine Beeinträchtigung dar, da SPAM-Mails typischerweise kleiner sind.

Jede untersuchte E-Mail wird vom SPAM-Mail-Filter um Kopfzeilen (Header) erweitert. Der "X-Spam-Status" zeigt den erreichten Punktwert (hits=...) sowie die Kurznamen der Merkmale, die zu diesem Punktestand geführt haben (tests=...). Dies ermöglicht es dem Empfänger, das Resultat des SPAM-Filters zu überprüfen. Die Kopfzeile "X-Spam-Level" enthält je ein "x" pro vollem erreichten Punkt (z.B. "X-Spam-Level: xxx" bei einer Punktezahl zwischen 3.00 und 3.99). Dieser Header ist bestens geeignet, um E-Mails mit Hilfe Ihres Mail-Programms automatisch zu sortieren.



Bei den meisten Mail-Programmen werden im Normalfall nur die wichtigsten Kopfzeilen angezeigt. Die weiteren Header sind aber in der Regel über einen entsprechenden Menüpunkt zugänglich.

E-Mail als SPAM markieren bei mehr als

Überschreitet der Punktwert einer E-Mail bei deren Klassifizierung diesen Schwellwert, so wird die E-Mail als SPAM-Mail markiert. Dabei wird dem Betreff der Text "***** SPAM *****" sowie die erreichten SPAM-Bewertungspunkte vorangestellt.

Markierte Mails zustellen in

Auf Wunsch können als SPAM markierte E-Mails in einen separaten SPAM-Ordner zugestellt werden. Dieser ist mit der SX-GATE-Groupware oder über den IMAP-Server (Ordner Mail/SPAM) erreichbar. Via POP3 kann der SPAM-Ordner nicht ausgelesen werden.

SPAM/HAM löschen nach

Nach der angegebenen Anzahl von Tagen werden Mails automatisch aus den Ordnern "SPAM" bzw. "HAM" gelöscht.



Diese Funktion ist unabhängig davon, ob markierte Mails automatisch im SPAM-Ordner abgelegt werden oder nicht. Der SPAM-Ordner kann also auch von Hand angelegt und befüllt werden.

E-Mail kommentarlos verwerfen bei mehr als

Beim Überschreiten des hier eingestellten Schwellwerts wird die betroffene E-Mail automatisch verworfen. Es erfolgt weder eine Benachrichtigung noch lässt sich eine so gelöschte E-Mail wiederherstellen. Die E-Mail ist unwiederbringlich verloren! Wenn Sie sichergehen wollen, dass keine gewünschte E-Mail verloren geht, sollten Sie diese Option nicht aktivieren. Nutzen Sie stattdessen den Schwellwert "E-Mail als SPAM markieren bei mehr als" zusammen mit den Möglichkeiten Ihres Mail-Programms zur automatischen Sortierung von E-Mails basierend auf den Kopfzeilen.



Um den Verlust von wichtigen E-Mails zu vermeiden, sollten Sie bei der Konfiguration dieser Einstellung sehr vorsichtig sein. Stellen Sie lieber einen zu hohen als einen zu niedrigen Wert ein. Bitte beachten Sie, dass das automatische Löschen von E-Mails durch Vorschriften oder Gesetze mit bestimmten Auflagen verbunden oder sogar verboten sein kann.

8.2-C SPAM Bewertung

Benutzerdefinierte SPAM-Regeln

Die SPAM-Prüfung kann in diesem Bereich durch eigene Regeln erweitert werden. Dazu ist zunächst festzulegen, welcher Teil der E-Mail geprüft werden soll. Wird das entsprechende Suchmuster gefunden, so wird die festgelegte Punktzahl bei der Berechnung der SPAM-Wahrscheinlichkeit verbucht.

Für folgende Bereiche kann eine SPAM-Filter-Regel definiert werden:

Betreff

Das Suchmuster wird im Betreff der E-Mail (Subject-Header) gesucht.

Absender

Hier wird der Absender (From-Header) geprüft.

Empfänger

In dieser Einstellung wird der Empfänger (To-Header) ausgewertet.

Kopfzeilen

Hiermit können beliebige Kopfzeilen (Header) ausgewertet werden.

Text

Diese Option bietet die Möglichkeit, den Nachrichten-Text einschließlich des Betreffs zu durchsuchen, also den eigentlichen Inhalt der Mail.

HTML Quelltext

Wie vor, jedoch bei E-Mails im HTML-Format inklusive der HTML-Tags.

Web-Adressen

Prüft Web-Adressen, die als Text oder als HTML-Link im Betreff oder im Text der Nachricht gefunden werden.

Regel

Diese Einstellung unterscheidet sich von den vorherigen. Sie ermöglicht es, die im SX-GATE vordefinierten Regelsätze neu zu bewerten. Entsprechend wird hier auch kein Suchmuster angegeben, sondern die interne ID der Regel. Die ID zusammen mit der ursprünglichen Bewertung ist jeweils in der Inhalts-Analyse von E-Mails enthalten, die als SPAM markiert wurden (z.B. "HTML_MESSAGE" oder "FORGED_MUA_OUTLOOK").



Bei Aktualisierung der vordefinierten Regelsätze können sich einzelne ID's ändern. Es erfolgt dabei keine Anpassung der hier angegebenen Regeln.

Bei der Angabe eines Suchmusters ("Kriterium") wird die Groß- und Kleinschreibung grundsätzlich nicht beachtet. Beginnt bzw. endet das Suchmuster mit einem Buchstaben oder einer Ziffer, muss das Suchmuster am Beginn bzw. Ende eines Wortes stehen. Das Suchmuster "all" liefert folglich bei "Hallo" keinen Treffer, bei "Das All!" hingegen schon.

Bestimmte Zeichen haben eine Sonderbedeutung:

* (Stern)

Steht für eine Folge beliebiger Zeichen. Diese kann auch komplett fehlen, also sozusagen aus 0 Zeichen bestehen. Das Suchen nach beliebigen Zeichenketten in beliebiger Länge erhöht den Ressourcen-Bedarf deutlich. Von daher trifft ein Stern maximal auf eine Kette aus 30 Zeichen zu. Das Suchmuster "a*d" findet so z.B. "ad", "a_d" und "abcd". Nutzen Sie den Stern auch, um Zeichenketten innerhalb eines Wortes zu suchen. So liefert das Suchmuster "*all*" bei "Hallo" einen Treffer.

? (Fragezeichen)

Dies steht für genau ein beliebiges Zeichen. Wird beispielsweise "a?d" angegeben, so ist "a_d" ein Treffer. Nicht gefunden wird "ad" oder "abcd".

_ (Unterstrich)

Der Unterstrich steht für eine beliebige Anzahl sogenannter "Whitespace-Character". Dies umfasst Leerzeichen, Tabulatoren und Zeilenumbrüche. Im Beispiel findet "a_d" zwar "a d", nicht jedoch "ad" oder "a_d".

Behalten Sie bitte bei der Auswahl des zugeordneten Punktwertes die eingestellten Schwellwerte im Auge. Wählen Sie für Kriterien die auf eine SPAM-Mail hindeuten einen positiven Wert. Ein negativer Wert verringert die Wahrscheinlichkeit, dass eine E-Mail als SPAM klassifiziert wird.

Englischsprachige E-Mails sind potentiell SPAM

Der größte Teil aller SPAM-Mails sind in englischer Sprache verfasst. Ist dieser Schalter aktiviert, so erhalten alle englischsprachigen E-Mails einen Aufschlag auf die SPAM-Bewertung. Die Wahrscheinlichkeit, dass die SPAM-Bewertung einer englischen E-Mail den konfigurierten SPAM-Filter-Schwellwert erreicht wird dadurch deutlich erhöht.

8.2-D SPAM Adressen

Der SPAM-Mail-Filter erreicht bei der automatischen Klassifizierung von E-Mails selbstverständlich kein 100% richtige Trefferquote. Es kann vorkommen, dass SPAM-Mails nicht erkannt oder aber "normale" E-Mails fälschlicherweise als SPAM-Mail eingestuft werden. Basierend auf der Absender-Adresse der E-Mails lässt sich mit Hilfe dieser Listen die Klassifizierung der entsprechenden E-Mails eindeutig festlegen.



Wenn kein SPAM-Filter-Schwellwert definiert ist und der SPAM-Filter als solches nicht aktiv ist, so sind die Einträge in den Listen wirkungslos.

Absenderadressen und -domains die den SPAM-Filter passieren dürfen

Um fälschlicherweise als SPAM identifizierte E-Mails zukünftig zu schützen, lässt sich hier eine Liste von einzelnen Absenderadressen hinterlegen, die den SPAM-Filter passieren dürfen. Passt der Absender einer eingehenden E-Mail zu einem Eintrag in dieser Liste, so erhält die E-Mail einen Abzug von 100 Punkten auf die automatische SPAM-Bewertung und wird so nicht von den Schwellwerten abgefangen.

Fügen Sie eine vollständige E-Mail-Adresse hinzu (z.B. benutzer@example.com), um E-Mails von dieser Adresse zukünftig nicht auszufiltern. Geben Sie alternativ lediglich den Domain-Teil der E-Mail-Adresse an (z.B. example.com), damit alle Adressen in dieser Domain den SPAM-Filter passieren dürfen.

Bekannte SPAM Absenderadressen und -domains

Wenn Sie immer wieder vom selben Absender SPAM-Mails erhalten, die durch den SPAM-Mail-Filter nicht erkannt wurden, so können Sie den Absender zu dieser Liste hinzufügen. Passt der Absender einer eingehenden E-Mail zu einem Eintrag in dieser Liste, so erhält die E-Mail einen Aufschlag von 100 Punkten auf die automatische SPAM-Bewertung und wird so vom SPAM-Filter abgefangen.

Fügen Sie eine vollständige E-Mail-Adresse hinzu (z.B. benutzer@example.com), um E-Mails von dieser Adresse zukünftig auszufiltern. Geben Sie alternativ lediglich den Domain-Teil der E-Mail-Adresse an (z.B. example.com), damit die E-Mails aller Absender aus dieser Domain vom SPAM-Filter abgefangen werden.

8.2-E Abwesenheit

Auf diesem Reiter lässt sich das Versenden automatischer Antwort-Mails sowie eine zeitlich begrenzte Mail-Weiterleitung für Ihr Postfach konfigurieren.

Die aktivierten Aktionen werden bei jeder E-Mail ausgeführt, die in Ihr Postfach zugestellt werden. Dies betrifft insbesondere auch E-Mails, die nicht Sie persönlich, sondern an einen Verteiler (Gruppe) adressiert waren dem Sie angehören.



Sofern E-Mails grundsätzlich an andere Adressen weitergeleitet werden (siehe Reiter "Weiterleitung"), sind die Einstellungen nur dann wirksam, wenn die Option "Kopie von weitergeleiteten E-Mails behalten" gewählt wurde.

Abwesenheits-Schaltung

Mit diesem Schalter werden die gewünschten Aktionen ausgewählt.

Zeitraum ab

Die gewählten Aktionen können ab sofort oder ab dem eingetragenen Datum aktiv werden. Geben Sie das Datum bitte im Format JJJJ-MM-TT HH:MM ein.

Zeitraum bis

Auf Wunsch gilt die Abwesenheits-Schaltung nur bis zu einem bestimmten Datum. Verwenden Sie bitte auch hier das Datums-Format JJJJ-MM-TT HH:MM.

E-Mails weiterleiten an

Auf Wunsch werden im gewählten Zeitraum alle Mails an eine andere Adresse weitergeleitet.

Kopie von weitergeleiteten Emails behalten

Mit Hilfe dieses Schalters legen Sie fest, ob Sie trotz Weiterleitung eine Kopie jeder Mail behalten wollen.

Abwesenheits-Nachricht

Es ist möglich, auf alle eingehenden E-Mails automatisch eine Antwort generieren zu lassen. Typische Anwendung ist der Versand von Abwesenheits-Notizen. Die Funktion kann aber z.B. auch genutzt werden, um den Eingang der E-Mail zu bestätigen.



Für E-Mails, die als SPAM markiert wurden, wird grundsätzlich keine Antwort generiert.

Der Inhalt der automatischen Antwort ist ein beliebiger Text der in diesem Eingabefeld festgelegt wird. Ist kein Text hinterlegt, so wird auch keine automatische Antwort gesendet.

8.2-F Ordner

E-Mails können automatisch anhand bestimmter Kriterien auf Unterordner Ihres Postfaches verteilt werden. Per IMAP oder Groupware kann auf diese Unterordner zugegriffen werden. Der Zugriff auf Unterordner per POP3 ist nicht möglich.

8.3 Groupware

Über diesen Menüpunkt ist es Benutzern möglich, mit Hilfe eines Web-Browsers Zugriff auf das eigene Mail-Postfach zu erhalten, vorausgesetzt die Groupware-Erweiterung ist installiert. Der Zugriff ist allen Benutzer möglich, die Mitglied der Gruppe "system-mail" sind.



Die Mitgliedschaft in der Gruppe "system-admin" ist nicht erforderlich. Allerdings ist es Benutzern mit dieser Einschränkung nicht möglich, über SX-GATEs Administrations-Oberfläche auf diesen Menüpunkt zuzugreifen. Diese Benutzer müssen die Groupware direkt über die URL
`https://NAME_ODER_IP/groupware/`
ansprechen.

Um SX-GATEs Groupware nutzen zu können, muss im Browser JavaScript aktiviert sein. Ferner müssen Cookies zugelassen werden.

Über den Zugriff auf E-Mails hinaus, bietet die SX-GATE Groupware zudem Adressbücher sowie einen Kalender mit Terminen und Aufgaben, die sich auch mit anderen Benutzern teilen lassen.

8.4 Kontakt

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

8.4-A Produktpass.....	46
8.4-B Firma.....	46
8.4-C Administrator.....	47
8.4-D Provider.....	47
8.4-E Support.....	47
8.4-F Firma	47
8.4-G Administrator	47
8.4-H Provider	47
8.4-I Support	47
8.4-J Info.....	48

8.4-A Produktpass

Hier finden Sie die wichtigsten Kenndaten zu Ihrem SX-GATE. Bitte geben Sie diese stets an, wenn Sie sich bei Fragen oder Problemen an den technischen Support wenden. Mit Hilfe des Schalters "Herunterladen" können Sie sich einen ausführlicheren Produktpass anzeigen lassen.

Ausführlichen Produktpass per Mail an ...

Hinweise zum Datenschutz

Mit Hilfe dieses Schalters können Sie den ausführlichen Produktpass per E-Mail an die angegebene Adresse senden. Die darin enthaltenen Daten werden für Vertrieb und Support des SX-GATE gespeichert und stehen ausschließlich autorisierten SX-GATE-Partnern zur Verfügung. Sie können der Nutzung dieser Daten jederzeit widersprechen und durch eine formlose E-Mail an die angegebene Adresse deren Löschung veranlassen.

8.4-B Firma

Hier können Sie Ihre Firmendaten eingeben bzw. ändern.

8.4-C Administrator

Hier können Sie Kontaktdaten zum Administrator des SX-GATE hinterlegen. Alle Benutzer mit Zugriffsberechtigung für die Administrationsoberfläche können lesend auf diese Daten zugreifen.

8.4-D Provider

Hier können Sie Kontaktdaten zu Ihrem Internet-Service-Provider hinterlegen. Alle Benutzer mit Zugriffsberechtigung für die Administrationsoberfläche können lesend auf diese Daten zugreifen.

8.4-E Support

Hier können Kontaktdaten für den technischen Support des SX-GATE hinterlegt werden. Vergessen Sie bitte bei Support-Anfragen nicht, die Daten aus dem Bereich Produktpass mit anzugeben. Alle Benutzer mit Zugriffsberechtigung für die Administrationsoberfläche können lesend auf diese Daten zugreifen.

8.4-F Firma

Hier sind Ihre Firmendaten hinterlegt.

8.4-G Administrator

Hier finden Sie die Kontaktdaten Ihres SX-GATE Administrators.

8.4-H Provider

Hier finden Sie die Kontaktdaten Ihres SX-GATE Internet-Service-Providers, an den Sie sich bei Störungen Ihrer Internetanbindung wenden können.

8.4-I Support

Hier finden Sie die Kontaktdaten des technischen Supports für SX-GATE. Vergessen Sie bitte bei Support-Anfragen nicht, die Daten aus dem Bereich Produktpass mit anzugeben.

8.4-J Info

Hier finden Sie die Kontaktdaten des Herstellers.

9 Statistiken

Im Hauptmenü "Statistiken" finden Sie diverse Statistiken zu einzelnen SX-GATE Modulen.

9.1 System-Last

Unter diesem Menüpunkt erhalten Sie verschieden graphische Statistiken, die Sie über den Systemzustand informieren. Auf der Hauptseite wird eine verkleinerte Darstellung aller Statistiken über die letzte Stunde angezeigt. Öffnen Sie den Eintrag in der Menü-Struktur der Benutzeroberfläche um Zugriff auf die vollständigen Statistiken zu erhalten. Dies umfasst jeweils eine Stunden-, Tages-, Wochen-, Monats- und Jahres-Statistik.



Die Stunden- und Tages-Statistiken werden alle 10 Minuten aktualisiert. Die anderen Statistiken täglich um Mitternacht.

Die Statistiken im Einzelnen:

Auslastung

Die wichtigste Statistik ist hier die Auslastungsstatistik. Sie gibt an, wie viele Prozesse im Durchschnitt zur Ausführung bereit stehen. Erreicht dieser Wert 100%, so ist im Durchschnitt zu jedem Zeitpunkt ein Prozess aktiv. Übersteigt dieser Wert 100%, so müssen Prozesse auf Betriebsmittel warten (Prozessor, Festplattenzugriff, ...).

Prozessor

In dieser Statistik ist die Nutzung des Prozessors aufgetragen.

Speicher

Die positiven Werte zeigen die Belegung des Hauptspeichers (RAM) an. Auf Festplatte steht darüber hinaus ein Auslagerungsbereich (swap) zur Verfügung. Dessen Nutzung wird mit negativen Werten dargestellt.

9.2 Netzwerk

In diesem Bereich sind verschiedene Statistiken zum Thema Netzwerk zusammengefasst. Diese umfassen jeweils eine Stunden-, Tages-, Wochen-, Monats- und Jahres-Statistik.



Die Stunden- und Tages-Statistiken werden alle 10 Minuten aktualisiert. Die anderen Statistiken täglich um Mitternacht.

9.2.1 Verbindungen

Die Verbindungs-Tabelle der Stateful-Inspection-Firewall wird zur Erzeugung dieser Statistik herangezogen. Einmal pro Minute werden alle zu diesem Zeitpunkt verzeichneten Verbindungen ausgelesen. Häufig auftretende, bekannte Protokolle werden mit eigener Farbe aufgetragen. Alle anderen Verbindungen werden unter "Sonstige" zusammengefasst.



Nicht ordentlich abgebaute Verbindungen werden erst nach einer längeren Zeitdauer aus der Verbindungs-Tabelle entfernt. Die Anzahl tatsächlich aktiver Verbindungen ist daher in der Regel kleiner als der angegebene Wert.

9.2.2 Durchsatz

In dieser Graphik ist die genutzte Datenrate je Schnittstelle aufgetragen. Die Datenrate der empfangenen Pakete ist als positiver Wert, die für den Versand als negativer Wert angegeben. Die Angaben verstehen sich als Kilobyte pro Zeiteinheit.

Auf einem zusätzlichen Reiter ist das insgesamt pro Monat übertragene Datenvolumen aufgeführt.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden.

9.2.3 Bandbreiten

In vielen Schnittstellen lässt sich das Bandbreitenmanagement aktivieren. Es teilt Datenverbindungen in fünf Prioritätsklassen ein. In dieser Statistik wird die prozentuale Verteilung der Bandbreite auf diese fünf Klassen angezeigt.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden.

9.3 Firewall

9.3.1 Paket-Filter

In diesem Bereich steht eine Statistik der Firewall-Ereignisse zur Verfügung. Die Statistik wird täglich um Mitternacht aktualisiert.

Neben einer Übersicht der letzten 12 Monate ist zu jedem Monat eine ausführliche Statistik verfügbar. Klicken Sie dazu auf den jeweiligen Monat in der Übersicht. Die Monats-Statistik enthält u.a. eine Übersicht über alle Tage des Monats und die Verteilung der Ereignisse nach Uhrzeit. Ferner existieren Übersichten über die beteiligten Schnittstellen, Quell- und Zieladressen (anonymisiert) sowie die angesprochenen Zielports.

In der Statistik werden folgende Begriffe aufgeführt:

Erlaubt

Die Verbindung wurde akzeptiert. Es werden ausschließlich Verbindungen gezählt, für die in der Firewall-Konfiguration die Protokollierung aktiviert ist.

Gefälscht

Ein Ping oder Traceroute wurde nicht an das eigentlich Zielsystem weitergeleitet sondern von der SX-GATE Firewall beantwortet.

Abgewiesen

Die Verbindung wurde verweigert. Der Absender wurde über eine passende Netzwerk-Kontrollnachricht darüber informiert.

Verworfen

Die Verbindung wurde verweigert. Das IP-Paket wurde verworfen ohne den Absender in irgendeiner Form darüber in Kenntnis zu setzen.

9.3.2 IDS/IPS

In diesem Menü steht eine statistische Aufbereitung der durch die Intrusion-Detection (IDS) aufgezeichneten Vorkommnisse zur Verfügung. Die Statistik wird täglich um Mitternacht aktualisiert.

Neben einer Übersicht der letzten 12 Monate ist zu jedem Monat eine ausführliche Statistik verfügbar. Klicken Sie dazu auf den jeweiligen Monat in der Übersicht. Die Monats-Statistik enthält u.a. eine Übersicht über alle Tage des Monats und die Verteilung der Ereignisse nach Uhrzeit. Weiterhin stehen Tabellen mit den am häufigsten aufgetretenen Ereignissen, den beteiligten Quell-Adressen (anonymisiert) und Diensten zur Verfügung.

9.4 Mail-Server

Sollte der Mailserver des SX-GATE aktiviert sein, so kann in diesem Bereich eine Zugriffs-Statistik abgerufen werden. Die Statistik wird täglich um Mitternacht aktualisiert.

Neben einer Übersicht der letzten 12 Monate ist zu jedem Monat eine ausführliche Statistik verfügbar. Klicken Sie dazu auf den jeweiligen Monat in der Übersicht. Die Monats-Statistik enthält u.a. eine Übersicht über alle Tage des Monats und die Verteilung der E-Mails nach Uhrzeit. Ferner wird jeweils eine Tabelle der am häufigsten gefundenen SPAM-Merkmale und Viren angezeigt. Zudem sind die häufigsten Empfängerdomains gelistet.



Die SPAM-Filter Auswertung ist nur für den benutzerunabhängigen Relay-SPAM-Filter verfügbar.

In der Statistik werden folgende Begriffe aufgeführt:

Gesendet

Jede E-Mail die erfolgreich vom Mail-Server gesendet wurde, wird in dieser Spalte gezählt.

Verworfen

Alle E-Mails die vom Virenschanner geblockt wurden, werden vom Mail-Server als verworfen deklariert und tauchen in dieser Spalte auf. Auch können vereinzelt E-Mails mit schwerwiegenden Fehlern vom Mail-System verworfen werden.

Abgelehnt

In der Spalte abgelehnt, werden alle E-Mails registriert die das Mail-System nicht abgeben konnte. Hierunter fallen unter anderem auch vom SPAM-Filter geblockte E-Mails.

Spam (abgelehnt)

Diese Spalte enthält die Anzahl aller E-Mails die als SPAM erkannt wurden. Dies beinhaltet sowohl die markierten also auch die abgelehnten Mails. Der Wert in Klammer gibt die Anzahl der abgelehnten Mails an.

Viren

Diese Werte zeigen die Anzahl der gefunden Viren.

kBytes

Das Datenvolumen aller Mail in Kilobyte ist in diesen Spalten ersichtlich.

9.5 Proxies

9.5.1 Web-Proxy

Dieser Menüpunkt bietet einen Einblick in die Nutzung des Web-Proxies Ihres SX-GATE. Die Statistik wird täglich um Mitternacht aktualisiert.



Ist der Virenskan im Web-Proxy des SX-GATE aktiviert, so kann dieser durch direkte Anfragen an den Web-Cache auf Port 8081 umgangen werden. Diese Anfragen sind nicht in der Statistik verzeichnet.

Neben einer Übersicht der letzten 12 Monate ist zu jedem Monat eine ausführliche Statistik verfügbar. Klicken Sie dazu auf den jeweiligen Monat in der Übersicht. Die Monats-Statistik enthält u.a. eine Übersicht über alle Tage des Monats und die Verteilung der Anfragen nach Uhrzeit. Ferner wird eine Tabelle der am häufigsten aufgerufenen Domains angezeigt.



Aus Gründen des Datenschutzes sind keine Übersichten je Quell-IP bzw. Benutzer verfügbar. Es ist jedoch möglich, im Menü "Monitoring > Log-Dateien" das Zugriffs-Protokoll extern zur weiteren Auswertung zu archivieren. Beachten Sie dazu jedoch die einschlägigen Bestimmungen bzgl. des Datenschutzes.

In der Statistik werden folgende Begriffe benutzt:

Anfragen

Jedes einzelne Objekt, das über den Proxy angefordert wird, zählt als eine Anfrage. Eine typische Internet-Seite besteht meist aus vielen Objekten. So ist z.B. für jede Graphik die zu einer Seite gehört eine weitere Anfrage notwendig.

Dateien

Nicht für jede Anfrage wird auch tatsächlich eine Datei empfangen. Oft wird lediglich ein Status- oder Fehler-Code zurückgeliefert. Diese Anfragen sind hier nicht berücksichtigt.

Seiten

Für diesen Wert werden nur die Anfragen gezählt, die sich üblicherweise auf den Text-Teil einer Web-Seite beziehen. Eingebettete Objekte wie insbesondere Bilder sind in diesem Wert nicht enthalten.

Besuche

Unter einem Besuch wird eine Folge von Anfragen verstanden, die von der gleichen Quell-Adresse kommen und deren zeitlicher Abstand nicht mehr als 5 Minuten beträgt.

Rechner

Dieser Wert bezieht sich auf die Anzahl unterschiedlicher Quell-Adressen.

kb

Das empfangene Datenvolumen in Kilobyte ist in diesen Spalten ersichtlich.

9.5.2 Reverse-Proxy

Ist der Reverse-Proxy des SX-GATE aktiviert, so kann hier dessen Zugriffs-Statistik abgerufen werden. Die Statistik wird täglich um Mitternacht aktualisiert.

Neben einer Übersicht der letzten 12 Monate ist zu jedem Monat eine ausführliche Statistik verfügbar. Klicken Sie dazu auf den jeweiligen Monat in der Übersicht. Die Monats-Statistik enthält u.a. eine Übersicht über alle Tage des Monats und die Verteilung der Anfragen nach Uhrzeit. Ferner wird eine Tabelle der am häufigsten aufgerufenen Dateien angezeigt. Eine Auswertung nach Ländern rundet die Statistik ab.

In der Statistik werden folgende Begriffe benutzt:

Anfragen

Jedes einzelne Objekt das angefordert wird, zählt als eine Anfrage. Eine typische Internet-Seite besteht meist aus vielen Objekten. So ist z.B. für jede Graphik die zu einer Seite gehört eine weitere Anfrage notwendig.

Dateien

Nicht für jede Anfrage wird auch tatsächlich eine Datei empfangen. Oft wird lediglich ein Status- oder Fehler-Code zurückgeliefert. Diese Anfragen sind hier nicht berücksichtigt.

Seiten

Für diesen Wert werden nur die Anfragen gezählt, die sich üblicherweise auf den Text-Teil einer Web-Seite beziehen. Eingebettete Objekte wie insbesondere Bilder sind in diesem Wert nicht enthalten.

Besuche

Unter einem Besuch wird eine Folge von Anfragen verstanden, die von der gleichen Quell-Adresse kommen und deren zeitlicher Abstand nicht mehr als 5 Minuten beträgt.

Rechner

Dieser Wert bezieht sich auf die Anzahl unterschiedlicher Quell-Adressen.

kb

Das gesendete Datenvolumen in Kilobyte ist in diesen Spalten ersichtlich.

9.6 Web-Server

Sollte der Internet Web-Server des SX-GATE aktiviert sein, so kann in diesem Bereich eine Zugriffs-Statistik abgerufen werden. Die Statistik wird täglich um Mitternacht aktualisiert.

Neben einer Übersicht der letzten 12 Monate ist zu jedem Monat eine ausführliche Statistik verfügbar. Klicken Sie dazu auf den jeweiligen Monat in der Übersicht. Die Monats-Statistik enthält u.a. eine Übersicht über alle Tage des Monats und die Verteilung der Anfragen nach Uhrzeit. Ferner wird eine Tabelle der am häufigsten aufgerufenen Dateien angezeigt. Eine Auswertung nach Ländern rundet die Statistik ab.

In der Statistik werden folgende Begriffe benutzt:

Anfragen

Jedes einzelne Objekt das angefordert wird, zählt als eine Anfrage. Eine typische Internet-Seite besteht meist aus vielen Objekten. So ist z.B. für jede Graphik die zu einer Seite gehört eine weitere Anfrage notwendig.

Dateien

Nicht für jede Anfrage wird auch tatsächlich eine Datei empfangen. Oft wird lediglich ein Status- oder Fehler-Code zurückgeliefert. Diese Anfragen sind hier nicht berücksichtigt.

Seiten

Für diesen Wert werden nur die Anfragen gezählt, die sich üblicherweise auf den Text-Teil einer Web-Seite beziehen. Eingebettete Objekte wie insbesondere Bilder sind in diesem Wert nicht enthalten.

Besuche

Unter einem Besuch wird eine Folge von Anfragen verstanden, die von der gleichen Quell-Adresse kommen und deren zeitlicher Abstand nicht mehr als 5 Minuten beträgt.

Rechner

Dieser Wert bezieht sich auf die Anzahl unterschiedlicher Quell-Adressen.

kb

Das gesendete Datenvolumen in Kilobyte ist in diesen Spalten ersichtlich.

10 Monitoring

Im Hauptmenü "Monitoring" finden Sie Überwachungsfunktionen um sich über den Status des SX-GATE oder mögliche Ursachen von Funktionsstörungen zu informieren.

10.1 Log-Dateien

Hier haben Sie die Möglichkeit, die wichtigsten Log-Dateien des SX-GATE zu durchsuchen. Diese helfen nicht zuletzt bei der Suche nach Ursachen für Fehlfunktionen. Prüfen Sie bitte die Log-Dateien bevor Sie sich an den technischen Support wenden. Bei Support-Anfragen per E-Mail ist es meist hilfreich, wenn relevante Ausschnitte der Log-Dateien beigelegt werden.

Systemintern werden gegliedert nach Funktion und Wichtigkeit mehrere Logdateien geschrieben. Die Logdateien werden täglich jeweils kurz nach 00:00 Uhr archiviert. Soweit nicht anders angegeben werden bis zu 12 archivierte Dateien im System gehalten, danach werden diese automatisch gelöscht.

Log-Datei

Wählen Sie bitte zuerst die gewünschte Log-Datei aus. Die verfügbaren Log-Dateien im einzelnen:

wichtige Meldungen

Fehler und andere wichtige Meldungen aus verschiedensten Bereichen des SX-GATE. Das Log enthält auch diverse Systemmeldungen, die während des Systemstarts erzeugt werden.

sonstige Meldungen

Diese Log-Datei enthält weitere Meldungen aus verschiedensten Bereichen.

Firewall

In diese Log-Datei protokolliert die SX-GATE Firewall.

Die Ausgabe beginnt mit dem Datum und der Uhrzeit, zu der das IP-Paket vom SX-GATE registriert wurde. Die nächste wichtige Information ist die Firewall-Stufe in der das Paket aufgezeichnet wurde.

Diese sind:

- fw-in für Pakete, die an SX-GATE adressiert sind
- fw-out für Pakete, die SX-GATE selbst erzeugt hat
- fw-fwd für Pakete die durch SX-GATE hindurch geleitet werden sollten
- fw-chk für Pakete die bei einer Plausibilitätsprüfung aufgefallen sind

Das nächste Feld gibt an, was mit dem Paket geschehen ist:

- drop: das Paket wurde verworfen
- rej: das Paket wurde verworfen, der Absender wurde informiert (ICMP-Nachricht oder TCP-Reset)
- fake: es wurde mit einem gefälschten Paket geantwortet
- acc: das Paket wurde akzeptiert. Akzeptierte Pakete werden nur geloggt, wenn Sie dies in der Konfiguration bei der jeweiligen Regel aktiviert haben.

Es folgt die Angabe des Grundes, warum das Paket protokolliert wurde. Der Grund "restricted" bedeutet, dass die aktuelle Firewall-Konfiguration eine entsprechende Verbindung nicht zulässt. Mit Hilfe einer entsprechenden Regel ließe sich diese Verbindung jedoch freigeben.

Die weiteren Felder geben u.a. an, über welche Schnittstelle das Paket empfangen wurde bzw. über welche Schnittstelle es gesendet werden sollte. Es folgen das Layer3-Protokoll des Pakets sowie die Quell- und Ziel-IP. Bei TCP und UDP werden ferner Quell-Port und Ziel-Port angegeben. Bei ICMP werden anstelle der Ports der ICMP-Typ und -Code angegeben, die Aufschluss über die Art der ICMP-Meldung geben. Für TCP-Verbindungen folgen die TCP-Flags. In der letzten Spalte ist die MAC-Adresse verzeichnet, von der das Paket empfangen wurde.

IDS/IPS

Zeigt die Meldungen des Intrusion-Detection- und -Prevention-Systems (IDS/IPS) an. Das IDS/IPS untersucht den Inhalt von IP-Paketen anhand einer Signaturdatenbank.

Neben Datum und Uhrzeit wird protokolliert, wie mit dem Paket verfahren wurde. Der Text "Drop" deutet darauf hin, dass dieses Datenpaket durch das IPS in der Firewall verworfen wurde. Der Text "wDrop" zeigt an, dass dieses Datenpaket durch die IDS aufgezeichnet wurde. Im Gegensatz zur IPS handelt es sich dabei um eine passive Komponente, die mit dem Monitor-Port eines Switches verbunden ist.

Als Referenz dient die Kombination aus Module-ID (meist 1), Regel-ID und Revisions-Nummer der Regel mit Doppelpunkten getrennt (z.B. 1:2345678:9). Sie benötigen die Regel-ID (hier "2345678"), um in der Konfiguration einzelne Regeln zu deaktivieren.

Es folgen der Informationstext der Regel sowie eine Klassifizierung, die die Art des Vorkommnisses angibt. Die Priorität zeigt an, ob es sich um ein kritisches Problem handelt (Priorität 1) oder weniger kritisch (Priorität 2, 3 oder 4). Schließlich werden das Layer-3-Protokoll, Quell- und Ziel-IP sowie die Ports angezeigt.

IPSec

Dieses Log enthält die Meldungen des SX-GATE IPSec-VPN-Servers.

OpenVPN

Dieses Log enthält die Meldungen des SX-GATE OpenVPN-Servers.

Wireguard

Dieses Log enthält die Meldungen des SX-GATE Wireguard-Servers.

Clustering

In dieser Log-Datei werden die Aktionen des Clusters protokolliert.

Mail

Dieses Log enthält die Aufzeichnung der ein- und ausgehenden Mails, Meldungen des Mail-Servers und seiner Filter-Prozesse sowie Verbindungen zum POP3- und IMAP4-Server des SX-GATE.

Web-Proxy Zugriffe

In dieser Datei werden die Zugriffe auf den Proxy des SX-GATE (Port 8080) protokolliert.

Web-Proxy Meldungen

Meldungen des SX-GATE Web-Proxies sind in diesem Log zu finden.

Reverse-Proxy Zugriffe

In dieser Datei werden die Zugriffe auf den Reverse-Proxy des SX-GATE protokolliert.

Reverse-Proxy Meldungen

Fehler und sonstige Meldungen des Reverse-Proxies werden in dieser Datei protokolliert.

Reverse-Proxy WAF

Wählen Sie diese Einstellung um Alarme der Web-Application-Firewall zu sehen. Die Alarme werden in der gleichen Logdatei wie Reverse-Proxy Meldungen aufgezeichnet, hier jedoch separat angezeigt.

SOCKS-Proxy Zugriffe

In dieser Datei werden die Zugriffe auf den SOCKS-Proxy des SX-GATE protokolliert.

WWW-Server Zugriffe

Ist der Internet Web-Server des SX-GATE aktiviert, so werden die Zugriffe in dieser Datei aufgezeichnet.

WWW-Server Meldungen

Treten beim Zugriff auf den Internet Web-Server Fehler auf, so werden diese hier festgehalten. Typische Fehler sind z.B. versuchte Zugriffe auf nicht vorhandene Dateien.

Intranet-Web-Server Meldungen

Fehler beim Zugriff auf den Web-Server für das lokale Intranet werden in diesem Log aufgezeichnet.

Debug Meldungen

Dieses log enthält Debug-Informationen generiert von verschiedensten Programmen. Im Unterschied zu anderen Log-Dateien werden nur bis zu drei archivierte Versionen dieses Logs im System gehalten.

PPP

Wählen Sie dieses Log, um Probleme beim Verbindungsaufbau von PPP-Wählverbindungen zu diagnostizieren.

Virens Scanner

In diesem Log finden Sie Meldungen von Virens Scanner und Signatur-Updates.

(APP) Web-Client

In diesem Log finden Sie Meldungen der Web-Client App.

Administrations-Oberfläche

Zugriffe auf die Administrationsoberfläche sowie Konfigurationsänderungen werden in diesem Log protokolliert.

Externe Systeme

In diesem Log finden sie Log-Meldungen die von anderen Systemen an den SX-GATE gesendet wurden.

Anzeige von maximal

Die Anzeige ist normalerweise auf 100 Zeilen beschränkt. Sie können jedoch mit Hilfe dieses Auswahlfeldes auch eine andere Schranke wählen.

Nur Zeilen mit Stichwort

Tragen Sie hier ein Suchmuster ein, damit nur die Zeilen der ausgewählten Log-Datei angezeigt werden, die dieses Muster enthalten. Suchmuster können im Stile der sog. "regular expressions" eingegeben werden.

Unter anderem haben die folgenden Zeichen eine Sonderbedeutung:

- | Oder-Verknüpfung
- (...) Gruppierung von Alternativen: "a(b|c)" steht z.B. für "ab" oder "ac"
- [...] ein Zeichen aus einer Menge von Zeichen: "[3-6X]" steht z.B. für die Ziffern 3, 4, 5, 6 oder ein X
- [^...] beliebiges Zeichen ausgenommen der angegebenen Menge von Zeichen: "[^3-6X]" steht für ein beliebiges Zeichen aber nicht 3, 4, 5, 6 oder X
- . ein beliebiges Zeichen
- ^\$()[]{}+*?\. Zeichen mit Sonderbedeutung
- \ Hebt die Sonderbedeutung des nachfolgenden Zeichens auf: "\" steht für den Punkt, "\\\$" für ein Dollar-Zeichen

So lässt sich z.B. nach den Monatsabkürzungen Jun und Jul auf folgende Weisen suchen:

- Jun|Jul
- Ju[nl]
- Ju(n|l)

Überspringe Zeilen mit Stichwort

Diese Einstellung ist komplementär zur vorhergehenden. Hier werden nur die Zeilen angezeigt, die das Suchmuster nicht enthalten.

Suchen

Mit dem Drücken dieses Schalters wird die Suche mit den zuvor angegebenen Parametern durchgeführt. Die Darstellung erfolgt in einem neuen Fenster des Web-Browsers.



Beachten Sie bitte das Disketten-Symbol in der rechten, oberen Ecke, über das Sie das angezeigte Log in eine Text-Datei exportieren können.

In der ersten Zeile des Ergebnisfensters werden Ihnen die Parameter angezeigt, die dem aktuellen Suchergebnis zugrunde liegen. Sie können diese Ergebnisse nun interaktiv weiter filtern. Rechts sehen Sie ein Histogramm über die zeitliche Verteilung der Einträge. Von den Rändern her können Sie die Größe des grauen Bereichs verändern, der den angezeigten Zeitbereich repräsentiert. Auf der linken Seite können Sie Suchmuster festlegen. Details dazu finden Sie in der Hilfe zum Live-Log.

10.2 Werkzeuge

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

10.2-A IPv4 Ping.....	62
10.2-B IPv6 Ping.....	63
10.2-C IPv4 Traceroute.....	64
10.2-D IPv6 Traceroute.....	64
10.2-E ARP-Scan.....	65
10.2-F DNS-Anfrage.....	66
10.2-G WoL.....	67
10.2-H Paketdump.....	67

10.2-A IPv4 Ping

Um Netzwerk-Verbindungen zu prüfen, ist der Befehl "ping" hilfreich. Dabei wird ein kleines IP-Paket (ICMP echo-request) an eine bestimmte Adresse geschickt. Antwortet diese mit einem Paket vom Typ "ICMP echo-reply", so kann von einer funktionierenden IP-Verbindung zu dieser Adresse ausgegangen werden.

Ping an Ziel-Adresse

Geben Sie hier die Adresse ein, an die der "ping" gesendet werden soll. Es ist möglich eine IP-Adresse oder einen DNS-Namen einzugeben. Wenn Sie einen DNS-Namen angeben, muss der Namens-Server des SX-GATE gestartet sein und die Namensauflösung funktionieren.

Quell-IP

Wenn die Pakete durch einen VPN-Tunnel laufen sollen, kann es erforderlich werden, eine bestimmte Quell-IP zu verwenden.

Paketgröße

Hier können Sie die Größe der IP-Pakete festlegen (zuzüglich 8 Byte ICMP-Header). Insbesondere bei VPN-Verbindungen kann es vorkommen, dass große Pakete (z.B. mit 1500 Byte) nicht übertragen werden können. In diesem Fall verwirft ein System auf dem Übertragungsweg fragmentierte Pakete.

Ping starten

Drücken Sie diesen Schalter, um im Abstand von einer Sekunde insgesamt 5 ping-Pakete an die eingegebene Adresse zu senden. Wenn Sie keine Antwort erhalten, kann dies u.a. folgende Ursachen haben:

- Die Gegenstelle ist ausgeschaltet oder existiert nicht
- Die Firewall der Gegenstelle verwirft ping Pakete
- Die Netzwerk-Verbindung zur Gegenstelle ist nicht verfügbar
- Die externe IP-Adresse des SX-GATE ist eine RFC1918-Adresse (192.168.*, 172.16.*-172.32.*, 10.*) und diese Adressen sind in der Firewall-Konfiguration der entsprechenden SX-GATE-Schnittstelle gesperrt.

10.2-B IPv6 Ping

Um Netzwerk-Verbindungen zu prüfen, ist der Befehl "ping" hilfreich. Dabei wird ein kleines IP-Paket (ICMP echo-request) an eine bestimmte Adresse geschickt. Antwortet diese mit einem Paket vom Typ "ICMP echo-reply", so kann von einer funktionierenden IP-Verbindung zu dieser Adresse ausgegangen werden.

Ping an Ziel-Adresse

Geben Sie hier die Adresse ein, an die der "ping" gesendet werden soll. Es ist möglich eine IP-Adresse oder einen DNS-Namen einzugeben. Wenn Sie einen DNS-Namen angeben, muss der Namens-Server des SX-GATE gestartet sein und die Namensauflösung funktionieren.

Schnittstelle / Quell-IP

Um eine Link-Local-Adresse anzusprechen ist die Angabe der Schnittstelle zwingend erforderlich. Sollen die Pakete durch einen VPN-Tunnel laufen, kann es erforderlich werden, eine bestimmte Quell-IP zu verwenden.

Paketgröße

Hier können Sie die Größe der IP-Pakete festlegen (zuzüglich 8 Byte ICMP-Header). Insbesondere bei VPN-Verbindungen kann es vorkommen, dass große Pakete (z.B. mit 1500 Byte) nicht übertragen werden können. In diesem Fall verwirft ein System auf dem Übertragungsweg fragmentierte Pakete.

Ping starten

Drücken Sie diesen Schalter, um im Abstand von einer Sekunde insgesamt 5 ping-Pakete an die eingegebene Adresse zu senden. Wenn Sie keine Antwort erhalten, kann dies u.a. folgende Ursachen haben:

- Die Gegenstelle ist ausgeschaltet oder existiert nicht
- Die Firewall der Gegenstelle verwirft ping Pakete
- Die Netzwerk-Verbindung zur Gegenstelle ist nicht verfügbar

10.2-C IPv4 Traceroute

Auch mit Traceroute lassen sich Netzwerk-Verbindungen prüfen. Im Gegensatz zum einfacheren "ping" wird hier der Weg ausgegeben, den die IP-Pakete bis zum Ziel zurücklegen.



Viele Systeme antworten nicht auf Traceroute-Pakete. Sie werden in der Anzeige mit Sternchen dargestellt.

Traceroute an Ziel-Adresse

Geben Sie hier die Adresse ein, an die der "traceroute" gesendet werden soll. Es ist möglich eine IP-Adresse oder einen DNS-Namen einzugeben. Wenn Sie einen DNS-Namen angeben, muss der Namens-Server des SX-GATE gestartet sein und die Namensauflösung funktionieren.

Quell-IP

Wenn die Pakete durch einen VPN-Tunnel laufen sollen, kann es erforderlich werden, eine bestimmte Quell-IP zu verwenden.

DNS Reverse-Lookup

Wenn aktiviert, wird versucht mittels DNS-Anfrage zu jeder IP den zugehörigen Hostnamen anzuzeigen.

Traceroute starten

Drücken Sie diesen Schalter, um den Traceroute zu starten.

10.2-D IPv6 Traceroute

Auch mit Traceroute lassen sich Netzwerk-Verbindungen prüfen. Im Gegensatz zum einfacheren "ping" wird hier der Weg ausgegeben, den die IP-Pakete bis zum Ziel zurücklegen.



Viele Systeme antworten nicht auf Traceroute-Pakete. Sie werden in der Anzeige mit Sternchen dargestellt.

Traceroute an Ziel-Adresse

Geben Sie hier die Adresse ein, an die der "traceroute" gesendet werden soll. Es ist möglich eine IP-Adresse oder einen DNS-Namen einzugeben. Wenn Sie einen DNS-Namen angeben, muss der Namens-Server des SX-GATE gestartet sein und die Namensauflösung funktionieren.

Quell-IP

Wenn die Pakete durch einen VPN-Tunnel laufen sollen, kann es erforderlich werden, eine bestimmte Quell-IP zu verwenden.

DNS Reverse-Lookup

Wenn aktiviert, wird versucht mittels DNS-Anfrage zu jeder IP den zugehörigen Hostnamen anzuzeigen.

Traceroute starten

Drücken Sie diesen Schalter, um den Traceroute zu starten.

10.2-E ARP-Scan

Der ARP-Scan nutzt das ARP-Protokoll um Systeme aufzulisten, die unmittelbar an der ausgewählten Schnittstelle angeschlossen sind, sich also im selben Netzwerksegment befinden. Ein Scan von Netzwerksegmenten jenseits von Routern ist nicht möglich.



Es werden nur Systeme mit aktiviertem IPv4-Protokoll erkannt.



Bei sehr großen Netzen kann der Scan-Vorgang mehrere Minuten (Netzmask 255.255.0.0) oder gar Stunden (Netzmaske 255.0.0.0) dauern.

Schnittstelle

Wählen Sie die Schnittstelle über die der Scan durchgeführt wird.

IP-Bereich

Ohne weitere Angabe werden alle IPv4-Adressen geprüft, die zur primären IP-Adresse und Netzmaske der gewählten Schnittstelle passen. Sie können hier jedoch auch eine einzelne IP-Adressen, eine Netzwerkadresse mit Netzmaske oder einen IP-Bereich (z.B. 192.168.0.10-192.168.0.20) angeben.

ARP-Scan starten

Drücken Sie diesen Schalter, um den ARP-Scan zu starten. Nach Abschluss des Scans können Sie das Ergebnis als Text-Datei herunterladen.

10.2-F DNS-Anfrage

In diesem Bereich können Sie die Namensauflösung testen oder gezielt Informationen aus dem DNS beziehen.

DNS-Anfrage für

Geben Sie hier ein, wonach Sie im DNS suchen wollen.

Typ

Wählen Sie hier die Art der gesuchten Information aus. Zur Auswahl stehen:

A/AAAA/PTR

IP-Adresse zu einem Rechnernamen oder Rechnername zu einer IP-Adresse

CAA

Liste der CAs, die Zertifikate für eine Domain ausstellen dürfen.

MX

Mail-Server zur angegebenen Domain

NAPTR

Komplexer Eintrag, der für Cloud- und Telekommunikationsdienste genutzt wird.

NS

Namens-Server zur angegebenen Domain

SOA

Meta-Informationen zur angegebenen Domain

TXT

Text-Informationen zur angegebenen Domain

an Name-Server

Wählen Sie hier aus, an welchen Namens-Server die Anfrage gesendet werden soll. Normalerweise erfolgt die Namensauflösung über den DNS des SX-GATE. Sofern Namens-Server Ihres Providers konfiguriert wurden, sind jedoch auch diese in der Liste aufgeführt und können so direkt kontaktiert werden. Dies ist z.B. nützlich, um deren Verfügbarkeit zu prüfen.

Von SX-GATE genutzte Provider Name-Server

Die derzeit vom SX-GATE genutzten Name-Server werden hier angezeigt. Ist die Liste leer, erfolgt die Namensauflösung mit Hilfe der Internet Root-Name-Server. Ist bei Wählverbindungen die Verwendung dynamisch zugewiesener DNS-Server aktiviert, werden hier die vom Provider zugewiesenen Server angezeigt.

DNS-Anfrage starten

Drücken Sie diesen Schalter, um die DNS-Anfrage abzusenden.

10.2-G WoL

Auf dieser Seite können Sie Wake-on-Lan-Pakete versenden um einen entsprechend konfigurierten Rechner aufzuwecken.

Mac-Adresse des aufzuweckenden Rechners

Geben Sie hier die Hardware-Adresse des Rechners an. Die Adresse muss im Format "XX:XX:XX:XX:XX:XX" angegeben werden. Jedes "X" steht dabei für eine Ziffer oder einen Buchstaben zwischen "A" und "F". Als Trennzeichen sind neben dem Doppelpunkt auch Punkte, Bindestriche und der Unterstrich zulässig.



Drücken Sie "Übernehmen" um die Mac-Adresse als Standard-Wert abzuspeichern.

10.2-H Paketdump

Um ein Netzwerk weiter zu debuggen, ist es manchmal notwendig, einzelne Pakete zu untersuchen. Mit einem Paketdump können Sie die Quell- und Ziel-Ports, IP- und MAC-Adressen und vieles mehr eines Pakets sehen. Außerdem können Sie die Richtung der Pakete beobachten und ob ein Paket überhaupt existiert.

Erster Servername, Netzwerk oder IP

Paketdumps können ziemlich schnell sehr groß werden. Hier können Sie den aufgezeichneten Datenverkehr nach IP, Netzwerk oder Hostname filtern.

Zweiter Servername, Netzwerk oder IP

Geben Sie hier eine zweite Adresse an, um ausschließlich den Datenverkehr zwischen zwei bestimmten Systemen aufzuzeichnen.

Schnittstelle

Hier können Sie die spezifische Schnittstelle auswählen, von der Sie Datenverkehr aufnehmen möchten.

Protokoll

Hier können Sie das Protokoll eingeben, das Sie aufnehmen möchten. Dadurch wird die Datei kleiner gehalten und lässt sich später auch leichter analysieren.

Portnummer (nicht mit ARP oder ICMP)

Hier können Sie die Portnummer eingeben, wenn Sie ausschließlich eine bestimmte Anwendung aufzeichnen möchten. Für die Protokolle ARP und ICMP darf diese Einstellung nicht genutzt werden.

Portnummer ausschließen (nicht mit ARP oder ICMP)

Hier können Sie die Portnummer eingeben, die im Dump ausgeschlossen werden soll. Für die Protokolle ARP und ICMP darf diese Einstellung nicht genutzt werden.

Ip-Adresse ausschließen

Hier können Sie die IP eingeben, die im Dump ausgeschlossen werden soll.

Laufzeit

Hier können Sie eingeben, für wie viele Sekunden der Paketdump laufen soll.

Paketdump starten

Drücken Sie den Schalter, um die Aufzeichnung des Datenverkehrs zu starten. Nach der angegebenen Laufzeit oder 500 Paketen, je nachdem, was zuerst erreicht wird, erscheinen Download-Schalter, mit denen Sie den resultierenden Paketdump zur weiteren Analyse herunterladen oder ansehen können.

Paketdump stoppen

Hier können Sie einen laufenden Paketdump anhalten. Dies ist besonders nützlich für Paketdumps mit unbegrenzter Laufzeit.

Pcap-Datei herunterladen

Hier können Sie den gerade erstellten Paketdump als .pcap-Datei herunterladen.

Paketdump ansehen

Hier können Sie den gerade erstellten Paketdump in Textform ansehen.

10.3 Netzwerk

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

10.3-A Routing.....	70
10.3-B Schnittstellen.....	70
10.3-C ADSL.....	70
10.3-D WLAN.....	71
10.3-E ARP.....	72

10.3-A Routing

Routing-Tabelle

Auf diesem Bildschirm wird die aktuelle Routing-Tabelle des SX-GATE angezeigt.

10.3-B Schnittstellen

Schnittstellen-Tabelle

Auf dieser Seite sehen Sie eine Übersicht über alle physikalischen Schnittstellen des SX-GATE. Je Schnittstelle laufen dabei auch Paketzähler für eingehende (RX) und ausgehende (TX) Pakete mit. Diese können insbesondere bei der Diagnose von Problemen hilfreich sein. So weist z.B. ein hoher Wert bei "carrier" auf eine fehlerhafte physikalische Verbindung hin. Das Netzkabel ist möglicherweise nicht eingesteckt oder defekt.

In der Schnittstellen-Konfiguration des SX-GATE wird für bestimmte Arten von Schnittstellen ein logischer Name definiert. Der physikalische Name dieser Schnittstellen beginnt stets mit "ppp". Zu welcher logischen Schnittstelle eine "ppp"-Schnittstelle gehört ist in der Schnittstellen-Tabelle nicht ersichtlich.

10.3-C ADSL

Sofern eine ADSL-Schnittstelle angelegt ist, lässt sich hier eine bestehende Verbindung manuell trennen bzw. die DSL-Leitung prüfen.

ADSL-Monitor

In diesem Bereich haben Sie die Möglichkeit, den Status von ADSL-Wählleitungen zu beobachten. Dazu wird die Anzeige alle 3 Sekunden automatisch aktualisiert.

Folgende Informationen werden dargestellt:

Schnittstelle

Hier wird der Name der SX-GATE ADSL-Schnittstelle ausgegeben.

Status

Hier ist der Status der Verbindung ersichtlich: "Getrennt" oder "Verbunden".

Schnittstelle

Wählen Sie hier die gewünschte Schnittstelle aus.

Jetzt auflegen

Drücken Sie diesen Schalter, damit eine eventuell bestehende Verbindung über die gewählte Schnittstelle sofort getrennt wird.

ADSL-Leitung testen

Wird dieser Schalter gedrückt, so sendet SX-GATE ein PADI-Paket über die konfigurierte Schnittstelle. Erfolgt eine Antwort in Form von PADO-Paketen, so wird der Name des DSL-Access-Concentrators Ihres Providers ausgegeben.



Diese Funktion testet die physikalische Verbindung vom SX-GATE über das DSL-Modem bis zum Access-Concentrator Ihres Providers. Der Test liefert keine Aussage darüber, ob eine erfolgreiche Netzwerk-Verbindung hergestellt werden kann.

10.3-D WLAN

Auf dieser Seite finden Sie Informationen zu den aktuell verbundenen WLAN-Clients. Die Tabellenspalten im Einzelnen:

wlan

Name der WLAN-Schnittstelle. Als Tooltip werden zusätzlich der Name des WLANs (SSID) und die Kanalnummer angezeigt.

MAC

Die MAC-Adresse des Clients.

IP

Sofern der Client seine IP-Adresse von SX-GATEs DHCP-Server bezogen hat, wird diese hier angezeigt. Hat der Client seinen Namen an den DHCP-Server übermittelt, wird dieser als Tooltip angezeigt.

Signal

Die aktuelle Signalstärke in dBm

empfangen

Die Datenmenge, die SX-GATE vom Client empfangen hat. Im Tooltip wird die Anzahl der Pakete angezeigt.

gesendet

Die Datenmenge, die SX-GATE an den Client gesendet hat. Im Tooltip wird die Anzahl der Pakete angezeigt sowie Informationen darüber, wie oft es zu Problemen beim Senden kam.

verbunden seit

Die Zeit, die seit dem letzten Verbindungsaufbau vergangen ist.



Die Datenzähler und die Verbindungsdauer werden zurückgesetzt, wenn das WLAN im SX-GATE neu gestartet wird oder sich der Client neu am WLAN anmeldet.

Weitere Details zu einem Client können Sie über das Info-Symbol in der letzten Spalte aufrufen.

10.3-E ARP

ARP-Cache

Auf dieser Seite ist der Inhalt des ARP-Caches zu sehen.

10.4 VPN

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

10.4-A IPSec.....	73
10.4-B OpenVPN.....	74
10.4-C Wireguard.....	75
10.4-D Web-Client.....	75
10.4-E SSH TCP Weiterleitung.....	76

10.4-A IPSec

IPSec-Verbindungen

In diesem Bereich werden alle zur Zeit aktiven oder gerouteten IPSec-VPN Verbindungen angezeigt. Zu jeder Verbindung werden folgende Daten angezeigt:

Name

Verbindungsname wie er bei der Konfiguration festgelegt wurde

ipsec

Name der zugehörigen ipsec-Schnittstelle



Wird nur angezeigt, wenn mehrere ipsec-Schnittstellen konfiguriert sind.

Typ

Verbindungstyp (Server, Client, L2tp, usw.)

Gegenstelle

Aktuelle IP-Adresse der Gegenstelle

ID

IPSec ID der Gegenstelle

lokales/entferntes Netz

Endpunkte des durch diese Verbindung beschriebenen Tunnels

empfangen/gesendet

Menge der über den Tunnel empfangen und gesendeten Daten

Status

Grün

Tunnel ist verbunden

Gelb

Tunnel ist im Aufbau



Beim Stoppen dieser Verbindungen kann es vorkommen, dass der Verbindungsversuch mittlerweile eine neue Statusnummer bekommen hat. In diesem Fall einfach bei der Verbindung nochmal auf Stopp drücken.

Rot

Tunnel ist nicht verbunden

Weiß

Tunnel ist nicht verbunden (Dynamisch oder Passiv)

10.4-B OpenVPN

Aktive OpenVPN-Verbindungen

In diesem Bereich werden alle zur Zeit aktiven OpenVPN-Verbindungen angezeigt. Zu jeder Verbindung werden folgende Daten angezeigt:

ovpn

Name der zugehörigen OpenVPN-Schnittstelle

Typ

Verbindungstyp (Server oder Client)

Gegenstelle

Aktuelle IP-Adresse der Gegenstelle

Zertifikat

Common Name (CN) des Gegenstellen-Zertifikats

IPv4-Addr.

Die dem Client zugewiesene IPv4-Adresse

IPv6-Addr.

Die dem Client zugewiesene IPv6-Adresse

empfangen

Anzahl der empfangenen Bytes

gesendet

Anzahl der gesendeten Bytes

verbunden seit

Zeitstempel des letzten erfolgreichen Verbindungsaufbaus

10.4-C Wireguard

Wireguard-Verbindungen

In diesem Bereich werden alle zur Zeit aktiven Wireguard-Verbindungen angezeigt. Zu jeder Verbindung werden folgende Daten angezeigt:

Schnittstelle

Name der Schnittstelle

Verbindung

Name der Verbindung. Als Tooltip wird der öffentliche Schlüssel der Gegenstelle angezeigt.

Gegenstelle

IP-Adresse und Port der Gegenstelle. Als Tooltip wird der öffentliche Schlüssel der Gegenstelle angezeigt.

erlaubte Netze

Netze, die von der Gegenstelle akzeptiert und die durch diese Verbindung zur Gegenstelle geroutet werden

Status der Verbindung seit dem letzten Start von Wireguard

grün

Durch diese Verbindung werden aktuell Daten geschickt

gelb

Der letzte Handshake liegt mehr als 3 Minuten zurück

rot

Verbindung wurde noch nicht aufgebaut

grau

Es liegen keine Statusinformationen vor

empfangen

Durch diese Verbindung empfangene Bytes

gesendet

Durch diese Verbindung gesendete Bytes

10.4-D Web-Client

Aktive Web-Client-Verbindungen

In diesem Bereich werden alle zur Zeit aktiven Web-Client Verbindungen angezeigt. Zu jeder Verbindung werden folgende Daten angezeigt:

Benutzer

Web-Client Benutzername

Protokoll

Name de Protokolls (rdp, vnc oder ssh)

Server

IP-Adresse des Server

Verbunden seit

Gibt die Verbindungszeit des Clients an

10.4-E SSH TCP Weiterleitung

SSH TCP Weiterleitungen

In diesem Bereich werden alle zur Zeit aktiven SSH TCP Weiterleitungen angezeigt. Zu jeder Verbindung werden folgende Daten angezeigt:

Benutzer

Name des Benutzer

Quelle

IP-Adresse der Quelle

Ziel

IP-Adresse des Ziels

Port

Aktueller Port des Ziels

10.5 Firewall

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

10.5-A Verbindungen.....	77
10.5-B Dynamische Firewall.....	77

10.5-A Verbindungen

Aktive Verbindungen

In diesem Tab werden die aktiven Verbindungen des SX-GATE während der letzten Sekunden angezeigt. Die Spalte "Dienst" enthält das Protokoll und den Zielport. Sofern die Anwendungserkennung aktiviert ist, werden die erkannte Anwendung und ggf. auch ein Hostname angezeigt. In der Spalte "Bytes" wird die seit Aufbau der Verbindung in die jeweilige Richtung übertragene Datenmenge angezeigt. "Dauer" ist die verstrichene Zeit seit Aufbau der Verbindung.

10.5-B Dynamische Firewall

Reputation der IP-Adressen

Die dynamische Firewall bewertet laufend das Verhalten der IP-Adressen, die über SX-GATE kommunizieren. Die aktuellen Punktestände können hier eingesehen werden. Je nach Konfiguration der Firewall werden besonders auffällige Adressen automatisch gesperrt. In diesem Fall wird zusätzlich die verbliebene Sperrdauer angezeigt.



Die Punktwerte werden mit der Zeit automatisch abgebaut. Insbesondere bei längerer Sperrdauer kann es so vorkommen, dass der Punktestand in der Zwischenzeit auf Null gesunken ist.

Eine fälschlicherweise gesperrte IP-Adresse können Sie samt der gesammelten Punkte aus der Liste entfernen. Sollte die IP wiederholt gesperrt werden, sollten Sie mit Hilfe des Firewall-Logs nach der Ursache suchen. Lässt sich die Ursache nicht beheben, können Sie die IP-Adresse im Menü "Module > Firewall > Einstellungen" auf dem Reiter (Tab) "Allgemein" dauerhaft von Sperrungen ausnehmen.

10.6 DHCP

In diesem Bereich sind die derzeit vom DHCP-Server vergebenen Adressen zu sehen.

IP Adresse

Die vom DHCP-Server zugewiesene IP Adresse

Status

Der Vergabestatus, entweder "frei" oder "aktiv" (aktuell an einen Client vergeben)

endet

Zeitpunkt, zu dem die Vergabe ausläuft. Bei freien Adressen ist an dieser Zeit zu erkennen, bis wann die IP zuletzt vergeben war. Bei aktiver Vergabe muss bis zum angegebenen Zeitpunkt erneuert werden.

MAC Adresse

Die MAC Adresse des Clients, der diese IP Adresse bezogen hat

Hostname

Einige Clients übermitteln ihren Rechnernamen an den DHCP-Server. Dieser wird hier gegebenenfalls angezeigt

10.7 Mail-Server

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

10.7-A Warteschlange.....	79
10.7-B Mail-Abholung.....	80
10.7-C MIME-Filter Quarantäne.....	80
10.7-D S/MIME Zertifikate.....	81
10.7-E Postfächer.....	82

10.7-A Warteschlange

Wartende E-Mails

E-Mails in der Sende-Warteschlange des SX-GATE Mail-Servers werden in diesem Bereich gelistet. Neben der intern vergebenen ID wird je Mail die Größe in Bytes, der Zeitpunkt zu dem die Mail in die Warteschlange aufgenommen wurde, der Absender und der Empfänger angezeigt. Bei Problemen wird ferner der aufgetretene Fehler gemeldet.

Ausgewählte E-Mails aus Warteschlange löschen

Um einzelne Mails aus der Warteschlange zu löschen, wählen Sie diese bitte zunächst mit Hilfe der Schaltfläche in der Mail-Liste aus. Drücken Sie dann diesen Schalter um die Mails zu löschen. Weder der Absender noch der Empfänger werden von der Löschung in Kenntnis gesetzt.

Alle E-Mails in Warteschlange löschen

Um alle Mails aus der Warteschlange zu löschen, drücken Sie bitte diesen Schalter. Auch hier erfolgt keinerlei Benachrichtigung der Absender und Empfänger.



Befinden sich mehr E-Mails in der Warteschlange als in obiger Liste angezeigt, so werden durch Drücken dieses Schalters auch die nicht angezeigten E-Mails gelöscht. Werden zwischen der Anzeige der obigen Liste und dem Drücken des Schalters neue E-Mails in die Warteschlange aufgenommen, so werden auch diese gelöscht.

Mailversand starten

Wenn Sie diesen Schalter drücken, versucht SX-GATE die Mails aus der Warteschlange sofort neu zuzustellen.

10.7-B Mail-Abholung***Mails jetzt beim Provider abrufen***

Drücken Sie diesen Schalter, um die protokollierte Abholung von E-Mails mit Hilfe des SX-GATE Mail-Clients zu starten. Es öffnet sich ein neues Browser-Fenster in dem sich die Kommunikation des Mail-Clients mit den konfigurierten POP3- bzw. ETRN-Servern beobachten lässt. Insbesondere lassen sich hier Fehler bei der Anmeldung am POP-Server und die Verteilung der Mails bei Sammelpostfächern beobachten.

Aktive Mail-Abholung beenden

Sollten Sie beim Versuch der protokollierten Mail-Abholung die Meldung "another foreground fetchmail is running" angezeigt bekommen, ist SX-GATE's Mail-Client bereits aktiv. Mit Hilfe dieses Schalters können Sie den laufenden Prozess beenden.



Durch das Abbrechen werden bereits abgeholte E-Mails aus einem geöffneten Postfach nicht gelöscht. Diese E-Mails werden bei der nächsten Abholung erneut zugestellt.

10.7-C MIME-Filter Quarantäne***Anhänge unter Quarantäne***

E-Mail Dateianhänge, die vom MIME-Filter des SX-GATE unter Quarantäne gestellt wurden, können hier heruntergeladen werden. Sie werden automatisch gelöscht, wenn die im Menü "Module > Mail-Server > SPAM/Virus/Malware" auf dem Reiter (Tab) "MIME-Filter" konfigurierte "Aufbewahrungszeit" überschritten ist.

Häufig werden Dateianhänge unter Quarantäne gestellt, die tatsächlich einen Virus enthalten, der aber vom Virens Scanner zum Zeitpunkt des Eintreffens der Mail noch nicht erkannt wurde. Aus diesem Grund werden die Dateianhänge im Quarantäne-Verzeichnis nach jedem Signatur-Update der installierten Virens Scanner erneut auf Viren geprüft. Wurde in einem Quarantäne-Verzeichnis ein Virus gefunden, wird dieses zukünftig nicht mehr erneut geprüft.

Zu jeder von der Quarantäne betroffenen E-Mail werden die folgenden Informationen angezeigt:

Quarantäne-Verzeichnis

Die Zeile beginnt mit dem Namen des Quarantäne-Verzeichnisses. Aus diesem Namen werden auch Datum und Uhrzeit ersichtlich, zu dem die Anhänge unter Quarantäne gestellt wurden.

E-Mail ID

Diese Spalte enthält die Id, die der Mail-Server des SX-GATE der Mail zugeordnet hat. Mit Hilfe dieser Id kann die zugehörige Mail in der Log-Datei des Mail-Servers ausfindig gemacht werden. Die Id ist verlinkt mit den vollständigen Kopfzeilen (Headern) der E-Mail.

Absender

Empfänger

Status

Solange die Dateianhänge seit dem Eintreffen der Mail noch nicht erneut von den installierten Virenscannern überprüft wurden, wird der Status als "unbekannt" angezeigt. Nach der Prüfung wechselt der Status auf "OK" oder "Virus". Wenn Sie mit dem Mauszeiger auf den Status eines Quarantäne-Verzeichnisses zeigen, wird Ihnen der Zeitpunkt des letzten Virencans bzw. der Zeitpunkt des Virenfundes angezeigt.

E-Mail Anhänge

Hier folgt die Liste der Dateianhänge mit der Möglichkeit diese Herunterzuladen. Beim Abspeichern wird grundsätzlich nicht der Original-Dateiname verwendet. Benennen Sie die Datei ggf. nach dem Speichern um, damit die Verknüpfung mit Anwendungen funktioniert.



Lassen Sie beim Herunterladen von Dateianhängen aus diesem Bereich absolute Vorsicht walten. Insbesondere bei unbekannten Absendern oder Anhängen mit seltsamen Dateinamen sollten Sie auf den Download verzichten.

Symbolspalte

Abhängig vom konfigurierte Quarantäne-Modus werden ggf. E-Mails komplett zurückgehalten. Bei diesen E-Mails wird ein grüner Pfeil angezeigt, über den Sie die E-Mail zur Zustellung freigeben können.

Klicken Sie auf das Mülltonnen-Symbol um einen Eintrag unwiderruflich aus dem Quarantäne-Bereich zu löschen.

10.7-D S/MIME Zertifikate

S/MIME-Zertifikate aus signierten E-Mails, die auf Freigabe warten

Wenn sowohl die Verifikation von Signaturen als auch die Verschlüsselung im SX-GATE S/MIME-Gateway aktiviert sind, können Zertifikate aus signiert empfangenen E-Mails gleich für die zukünftige Verschlüsselung ausgehender E-Mails genutzt werden.

Zu diesem Zweck temporär zwischengespeicherte Zertifikate können Sie hier dauerhaft zur Verschlüsselung freigeben.



Wenn innerhalb von 6 Tagen keine Freigabe erfolgt, werden die Zertifikate automatisch gelöscht.

Zu jedem Zertifikat werden folgende Informationen angezeigt:

E-Mail

Die Absender-Adresse von der das Zertifikat in Form einer Signatur empfangen wurde. Nach der Freigabe werden E-Mails an diese Adresse mit dem Zertifikat verschlüsselt. Eventuelle weitere E-Mail-Adressen, die im Zertifikat enthalten sind, werden nicht berücksichtigt.

Empfangen

Der Zeitpunkt zu dem die signierte E-Mail empfangen wurde.

Status

Gelb, wenn beim Verifizieren des Zertifikat ein Fehler auftrat. Grün bei erfolgreicher Verifikation.

Zertifikat

Der Zertifikatstext (Distinguished Name, DN).

gültig bis

Das Ablaufdatum des Zertifikats

Weitere Details zum Zertifikat erhalten Sie über das Info-Symbol. Mit dem grünen Pfeil geben Sie das Zertifikat zur Verschlüsselung ausgehender E-Mails frei. Mit dem Mülltonnen-Symbol wird ein Zertifikat aus der Liste entfernt.

Im Menü "Module > Mail-Server > S/MIME-Gateway" legen Sie auf dem Reiter (Tab) "Verifizieren" fest, ob Zertifikate automatisch oder erst nach manueller Freigabe zur Verschlüsselung genutzt werden dürfen. Die Liste der freigegebenen Zertifikate kann im selben Menü auf dem Reiter "Verschlüsseln" angezeigt und bearbeitet werden.

10.7-E Postfächer

Postfach-Liste

Sie sehen hier eine Liste der Postfächer des SX-GATE POP3-/IMAP4-Servers. Neben dem Kontonamen ist die Gesamtgröße des Postfachs angegeben.



Konten zu Benutzern die zwar angelegt wurden, auf die jedoch noch nie zugegriffen wurde, sind in dieser Übersicht möglicherweise nicht zu sehen. Das Postfach wird automatisch angelegt, sobald die erste Mail zugestellt wird.

Ein Postfach wird gelöscht, sobald der zugehörige Benutzer in der Benutzerverwaltung vollständig gelöscht wird. Wird der Benutzer lediglich aus der Gruppe "system-mail" entfernt, bleibt das Postfach erhalten und kann wieder vom Benutzer genutzt werden, sobald er wieder Mitglied der Gruppe "system-mail" ist.

10.8 Web-Proxy

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

10.8-A URL-Filter.....	84
10.8-B Content-Filter.....	84

10.8-A URL-Filter

Hier können Sie die Konfiguration des URL-Filter-Modules des Web-Proxy testen.

URL

Geben Sie hier die zu prüfende URL an.

IP

Die Quell-IP, von der die Anfrage gestellt werden soll.

Benutzer

Der Benutzer, der die Anfrage stellt.

Abfrage starten

Hiermit starten Sie die Testabfrage. Als Ausgabe erhalten Sie, ob der Zugriff erlaubt ist oder nicht und ggf. den Grund.

10.8-B Content-Filter

Content-Filter Quarantäne

Hier wird eine Liste mit den zwischengespeicherten Downloads nach Dateigröße absteigend sortiert angezeigt. Dieser Liste können Sie den Benutzernamen (falls Benutzeranmeldung am Web-Proxy aktiv ist), die IP, den Status der Virenprüfung, den Dateinamen des Downloads, dessen Größe und den Server, von dem der Download stammt, entnehmen.

Der Status der Virenprüfung kann folgende Werte annehmen, bei mehreren installierten Virensclannern auch eine Kombination:

grün

Es wurde kein bekannter Virus gefunden.

gelb

Der Status konnte nicht eindeutig festgestellt werden:

- Kein Virens Scanner installiert
- abgelaufen: Die Lizenz eines Virens Scanners ist abgelaufen.
- unbekannt: Ein Virens Scanner meldete Probleme beim Scannen der Datei.
- verschlüsselt: Die Datei ist (teilweise) verschlüsselt und konnte deshalb nicht vollständig geprüft werden.

Darüberhinaus wird darauf hingewiesen, wenn die Datei MS Office Makros (inkl. Makros mit gesetztem Autostart) enthält.

rot

In der Datei wurde ein Virus gefunden.



Es wird empfohlen, dass Dateien deren Status gelb oder rot hinterlegt ist, vor dem Ausführen oder Entpacken auf einem Arbeitsplatz-PC mit einem Virens Scanner überprüft werden.

11 Definitionen

Im Hauptmenü "Definitionen" werden verschiedene Objekte definiert, die bei der Konfiguration verwendet werden.

11.1 IP-Objekte

Benennen Sie einzelne IP-Adressen und Netze oder gruppieren Sie diese. Sie können diese Definitionen dann an verschiedensten Stellen wie z.B. in den Firewall-Regeln nutzen. Sie verbessern so die Lesbarkeit und die Übersichtlichkeit.

Für Einstellungen, die IP-Adressen erwarten, können DNS-basierte IP-Objekte die Brücke zu DNS-Daten wie Hostnamen schlagen.

Speziell für Firewall-Regeln gibt es die Möglichkeit, IP-Objekte zur Geolokation nach Ländern anzulegen.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Objekt-Typ

Legen Sie hier fest um welche Art von Objekt es sich handelt.

Gruppe

Objekte diesen Typs können eine beliebige Anzahl von Adressen aufnehmen. Auch die Schachtelung von anderen Objekten ist möglich.

Download von URL (für Firewall)

Wählen Sie diese Variante um eine Liste an IP-Adressen von einem Webserver herunterzuladen. Diese Form der Liste ist optimiert auf eine effiziente Nutzung in der Firewall. Es sind bis zu 65535 Einträge möglich.



IP-Objekte dieses Typs können nur in Firewall-Regeln genutzt werden. Eine Schachtelung in IP-Gruppen ist nicht möglich.

Download von URL (kleine Listen)

Wählen Sie diese Variante um eine Liste an IP-Adressen von einem Webserver herunterzuladen. Pro Liste sind maximal bis zu 999 Einträge möglich.



Wenn Sie dieses Objekt in der Firewall nutzen wollen, verwenden Sie bitte stattdessen den für diesen Zweck optimierten Objekt-Typ "Download von URL (für Firewall)".

DNS-Eintrag

Der Name dieser Gruppe ist ein DNS-Name. Die zugehörigen IP-Adressen werden mit Hilfe von DNS-Anfragen ermittelt und automatisch aktualisiert. Eine Aktualisierung erfolgt grundsätzlich nach Systemstart und nach Änderungen in IP-Objekten. Ferner erfolgt eine Aktualisierung wenn die erlaubte Cache-Dauer des DNS-Eintrags (TTL) abläuft, mindestens jedoch alle 3 Stunden.



DNS-Namen, die mit einer Ziffer beginnen, werden nicht akzeptiert. Gruppieren Sie diese DNS-Namen in einem Unterordner (z.B. wird "123test.example.com" nicht akzeptiert. Um diesen Host dennoch anzulegen, stellen Sie einen Unterordner als Präfix voran wie z.B. "dns/123test.example.com").



Da DNS-Informationen vergleichsweise einfach zu fälschen sind, wird der Einsatz in kritischen Bereichen (z.B. eingehende Firewall-Regeln) nicht empfohlen.

DNS-Mitschnitt

In Gruppen dieses Typs können Sie DNS-Domains und Hostnamen eintragen. Diese beinhalten stets sowohl den Namen selbst (z.B. example.com) als auch Hostnamen und Subdomains (*.example.com). Sendet ein Client eine passende DNS-Anfrage an den SX-GATE DNS-Server, werden die IP-Adressen aus der DNS-Antwort im IP-Objekt hinterlegt.



Da dieser Prozess eine gewisse Zeit benötigt, ist damit zu rechnen, dass der initale Verbindungsaufbau zu einer noch nicht freigegebenen Adresse mit Verzögerung erfolgt.



Prinzipbedingt sind IP-Objekte dieses Typs nur für ausgehende Firewall-Regeln geeignet. Der Client muss DNS-Namen zwingend entweder direkt oder indirekt über den SX-GATE DNS-Server auflösen.

Die erlaubte Cache-Dauer des DNS-Eintrags (TTL) legt fest, wann die IP-Adresse aus dem IP-Objekt wieder entfernt wird.

Azure Servicebus (WCF-Relay)

Dieser spezielle Objekt-Typ erlaubt es, die IP-Adressen zu einem WCF-Relay in der Azure-Cloud über DNS zu ermitteln. Sie müssen dazu den Namespace des WCF-Relays kennen.



Da DNS-Informationen vergleichsweise einfach zu fälschen sind, wird der Einsatz in kritischen Bereichen (z.B. eingehende Firewall-Regeln) nicht empfohlen.

Host

Ein Objekt dieses Typs repräsentiert einen einzelnen Netzwerk-Teilnehmer mit den drei Parametern MAC-Adresse, IPv4-Adresse und IPv6-Adresse. Alle drei Parameter sind dabei optional. Welche dieser drei Parameter tatsächlich berücksichtigt werden, ist abhängig vom Kontext, in dem das Objekt benutzt wird. Ist ein im jeweiligen Kontext benötigter Parameter nicht angegeben, wird das Objekt in diesem Kontext ignoriert.



Im Allgemeinen werden lediglich die IP-Adressen des Objekts verwendet. Findet zusätzlich oder ausschließlich die MAC-Adresse Anwendung, ist dies in der Dokumentation der jeweiligen Einstellung angegeben.

Die IPv6-Adresse kann auf einem Präfix basieren. Siehe dazu die Beschreibung des Typs "IPv6-Adresse".

IPv6-Präfix

Dieser Objekt-Typ steht für ein IPv6-Präfix. Er kann von einem anderen, kürzeren Präfix abhängen. Auf diese Weise lässt sich ein vom Provider erhaltenes Präfix weiter aufteilen.

Angenommen ein Präfix-Objekt enthält den vom Provider zugewiesenen Präfix "2001:db8::/48". Legen Sie nun ein weiteres Präfix-Objekt an, das sich auf den Provider-Präfix bezieht und den Eintrag "0:0:0:1::/64" enthält. Sie erhalten den Präfix "2001:db8:0:1::/64".

IPv6-Adresse

Mit Hilfe dieser Option legen Sie eine einzelne IPv6-Adresse an. Ein Objekt diesen Typs ist häufig notwendig, um die Adresse einer SX-GATE-Schnittstelle zu definieren. Soll das Objekt ein anderes, insbesondere lokales System repräsentieren, empfohlen wird den Objekt-Typ "Host" zu verwenden.

Die IPv6-Adresse kann sich auf einen Präfix beziehen. Angenommen ein Präfix-Objekt enthält den Präfix "2001:db8:0:1::/64". Mit Bezug auf dieses Präfix-Objekt und der konfigurierten Schnittstellen-ID "::1234" erhalten Sie die Adresse "2001:db8:0:1::1234".

IPv4-Netzwerk

Dieser Objekt-Typ steht für ein IPv4-Netzwerk.

IPv4-Adresse

Hiermit lässt sich eine einzelne IPv4-Adresse definieren. Soll das Objekt ein anderes, insbesondere lokales System repräsentieren, empfohlen wird den Objekt-Typ "Host" zu verwenden.

Geolokation (Ländercodes)

Wählen Sie diesen Typ um Ländercodes nach ISO 3166 einzutragen. In einer integrierten Datenbank ist zu jedem Land die Liste der diesem Land zugeordneten IP-Adressen hinterlegt.



IP-Objekte dieses Typs können nur in Firewall-Regeln genutzt werden. Eine Schachtelung in IP-Gruppen ist nicht möglich.

Bezeichner / DNS-Name

Legen Sie hier einen Namen für das Netzwerk-Objekt fest. Unter diesem Namen kann das Objekt in diversen Einstellungen referenziert werden. Wenn Sie die gruppierte Darstellung von Tabellen aktiviert haben, können Sie Objekte gruppieren, indem Sie einen Ordernamen gefolgt von einem '/' als Trennzeichen und dann den eigentlichen Objektnamen als Bezeichner verwenden (z.B. "dns/123test.example.com" oder "vpn/filiale1").

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

11.1-A Liste herunterladen.....	90
11.1-B Adressen.....	92
11.1-C IPv6-Adresse.....	93
11.1-D IPv4-Adresse.....	94
11.1-E Adressen.....	94
11.1-F Geolokation.....	95
11.1-G Verwendung.....	95

Objekt-Typ

Legen Sie hier fest um welche Art von IP-Objekt es sich handelt.

Gruppe

Objekte diesen Typs können eine beliebige Anzahl von Adressen aufnehmen. Auch die Schachtelung von anderen Objekten ist möglich.

DNS-Eintrag

Der Name dieser Gruppe ist ein DNS-Name. Die zugehörigen IP-Adressen werden mit Hilfe von DNS-Anfragen ermittelt und automatisch aktualisiert. Eine Aktualisierung erfolgt grundsätzlich nach Systemstart und nach Änderungen in IP-Objekten. Ferner erfolgt eine Aktualisierung wenn die erlaubte Cache-Dauer des DNS-Eintrags (TTL) abläuft, mindestens jedoch all 3 Stunden.



Da DNS-Informationen vergleichsweise einfach zu fälschen sind, wird der Einsatz in kritischen Bereichen (z.B. eingehende Firewall-Regeln) nicht empfohlen.

11.1-A Liste herunterladen

Lädt eine Liste mit IP-Adressen von einem Webserver. Der Download darf einzelne IPv4- und IPv6-Adressen sowie IPv4- und IPv6-Netze enthalten (z.B. 192.0.2.0/24, 192.0.2.0/255.255.255.0 oder 2001:db8::/64). IP-Objekte vom Typ "Download von URL (kleine Listen)" unterstützen zusätzlich IP-Bereiche wie z.B. "192.0.2.3-192.0.2.9".

Bei dem Download muss es sich um eine Textdatei im ASCII-Format handeln. Die Textdatei darf mit gzip oder bzip2 komprimiert sein und es dürfen mehrere Dateien in einem Zip- oder Tar-Archiv zusammengefasst werden. Der Download kann

zeitgesteuert automatisch wie auch manuell erfolgen. Einträge in der Liste können mit Leerzeichen, Tabulator oder Zeilenumbruch separiert werden.



Die Liste darf maximal 25 MB groß sein.

SSL-Zertifikat verifizieren

Aktivieren Sie diese Option, um im Falle einer HTTPS-Verbindung das Server-Zertifikat zu prüfen.

Benutzername

Sofern der Web-Server eine Benutzer-Authentifizierung via Basic-Auth benötigt, geben Sie hier bitte den Benutzernamen ein.

Passwort

Das Passwort wird nur benötigt, wenn auch ein Benutzername angegeben wurde.

Hostname/IP

Geben Sie hier bitte den Namen oder die IP-Adresse des Servers ein, von dem die Liste heruntergeladen werden soll.

Port

Sofern der Server nicht auf Port 80 (http) bzw. 443 (https) erreichbar ist, geben Sie hier bitte die Port-Nummer ein.

Dateipfad

Geben Sie hier bitte den Pfad und den Dateinamen für den gewünschten Download ein. Auch die Angabe von URL-Parametern ist möglich.

Maximale Anzahl Einträge

Bitte geben sie hier die maximale Anzahl von importierten Einträgen an.



Sollte dieser Wert überschritten werden, wird der Import abgebrochen und die alten Werte bleiben erhalten.

Zeitgesteuerter Download

Hier aktivieren Sie den regelmäßigen automatischen Download.

Startzeit

Bei einem täglichen Download legen Sie hier die Stunde fest in der der Download stattfindet. Erfolgt der Download mehrmals täglich, wird über diesen Parameter die Stunde des ersten Downloads gesteuert. Die genaue Minutenzahl wird jeweils zufällig bestimmt.

Manueller Download

Ein Download der Liste kann hier jederzeit manuell angestoßen werden. Zur Fehlerdiagnose lassen sich Debug-Meldungen zuschalten.

11.1-B Adressen**Beschreibung**

Dieser Text dient ausschließlich der Dokumentation.

Letzes Update

Datum und Uhrzeit des letzten erfolgreichen Downloads, bei dem sich der Inhalt der Liste tatsächlich geändert hat.

Adressen

Tragen Sie hier einzelne IP-Adressen oder Netzwerk-Adressen samt zugehöriger Netzmask ein (z.B. 192.168.0.0/24). Es ist auch möglich, andere Objekte einzubinden.

Domains und Hostnamen

Tragen Sie hier Domains und Hostnamen ein, zu denen die IP-Adressen gesammelt werden sollen. Dies beinhaltet stets auch alle Subdomains. Wenn Sie z.B. "example.com" eintragen, werden sowohl die IP-Adressen aus DNS-Antworten zu "example.com" als auch zu "www.example.com" gesammelt.

Typ des DNS-Eintrags

Wählen Sie hier die Art des abgefragten DNS-Eintrags aus. Üblicherweise wollen Sie zu einem Hostnamen die IPv4- (A) und IPv6-Adressen (AAAA) erfragen. In Einzelfällen sind aber ggf. auch die IP-Adressen zu bestimmten Diensten (SRV), von Mail-Servern (MX) oder von Name-Servern (NS) relevant.

Namespace

Geben Sie hier den Servicebus-Namespace ein. Sollte Ihnen der Namespace nicht bekannt sein, aktivieren Sie bitte vorübergehend "DNS-Anfragen protokollieren" im Menü "Module > DNS > Einstellungen" auf dem Reiter (Tab) "Client-Zugriff". Starten Sie anschließend die Anwendung neu. Suchen Sie dann im Log nach DNS-Anfragen der Form "NAMESPACE.servicebus.windows.net" (also z.B. "testns.servicebus.windows.net"). Ignorieren Sie dabei Einträge, bei denen der

vermeintliche NAMESPACE mit "-sb" oder "-mgmt" endet (beispielsweise "g0-prod-xy3-001-sb.servicebus.windows.net").

Abgelaufene Adressen löschen

Bei manchen DNS-Einträgen ändern sich die IP-Adressen laufend. Über einen längeren Zeitraum betrachtet, kommen dabei jedoch meist immer wieder die gleichen IP-Adressen zum Einsatz. In diesem Fall ist es sinnvoll, abgelaufene Adressen nicht sofort zu entfernen, so dass SX-GATE mit der Zeit alle IP-Adressen sammeln kann. Sie entlasten so das System, da es nicht laufend die Konfiguration aktualisieren oder gar Dienste neu starten muss.

Zuletzt erfolgreich verifiziert

Hier wird angezeigt, wann die DNS-Information zuletzt erfolgreich abgefragt werden konnte. Liegt dieser Zeitpunkt weit in der Vergangenheit, existiert vermutlich kein passender DNS Eintrag mehr.

11.1-C IPv6-Adresse

Beschreibung "..."

Dieser Text dient ausschließlich der Dokumentation.

Routing-Präfix

Sie können dieses Objekt an einen Routing-Präfix binden. Ändert sich der Routing-Präfix, wird die Adresse dieses Objekts automatisch angepasst. Ist im ausgewählten Routing-Präfix aktuell keine Adresse eingetragen, steht auch dieses Objekt für keine Adresse.

Präfix / Teilnetz

Geben Sie hier den gewünschten Präfix ein. Bezieht sich dieser Präfix auf einen Routing-Präfix, muss er üblicherweise mit Nullen beginnen. Alle im übergeordneten Präfix definierten Bits müssen auf Null gesetzt sein. Die Präfixlänge darf nicht kleiner sein als die des übergeordneten Präfixes.



Dieses Eingabefeld darf auch leer bleiben. Sofern ein Routing-Präfix ausgewählt wurde, wird einfach dessen Wert übernommen.

IP-Adresse / Schnittstellen ID

Geben Sie hier die gewünschte IPv6-Adresse ein. Bezieht sich die Adresse auf einen Routing-Präfix, muss sie üblicherweise mit Nullern beginnen. Alle durch das Präfix definierten Bits müssen auf Null gesetzt sein.

11.1-D IPv4-Adresse

Beschreibung "..."

Dieser Text dient ausschließlich der Dokumentation.

Netzwerk

Geben Sie hier eine Netzwerkadresse mit zugehöriger Netzmaske ein.

IP-Adresse

Geben Sie hier die gewünschte IPv4-Adresse ein.

11.1-E Adressen

Ein Objekt dieses Typs repräsentiert einen einzelnen Netzwerk-Teilnehmer mit den drei Parametern MAC-Adresse, IPv4-Adresse und IPv6-Adresse. Alle drei Parameter sind dabei optional. Welche dieser drei Parameter tatsächlich berücksichtigt werden, ist abhängig vom Kontext, in dem das Objekt benutzt wird. Ist ein im jeweiligen Kontext benötigter Parameter nicht angegeben, wird das Objekt in diesem Kontext ignoriert.



Im Allgemeinen werden lediglich die IP-Adressen des Objekts verwendet. Findet zusätzlich oder ausschließlich die MAC-Adresse Anwendung, ist dies in der Dokumentation der jeweiligen Einstellung angegeben.

Beschreibung "..."

Dieser Text dient ausschließlich der Dokumentation.

MAC-Adresse

Geben Sie hier die gewünschte MAC-Adresse hexadezimal im Format XX:XX:XX:XX:XX:XX ein. Die Angabe einer MAC-Adresse ist optional. Sie wird nur an wenigen Stellen tatsächlich verwendet (z.B. zur Filterung der Quell-MAC-Adresse in Firewall-Regeln).

IPv4-Adresse

Geben Sie hier optional die gewünschte IPv4-Adresse ein.

IPv6-Routing-Präfix

Sie können dieses Objekt an einen Routing-Präfix binden. Ändert sich der Routing-Präfix, wird die Adresse dieses Objekts automatisch angepasst. Ist im ausgewählten

Routing-Präfix aktuell keine Adresse eingetragen, steht auch dieses Objekt für keine IPv6-Adresse.

IPv6-Adresse / Schnittstellen ID

Geben Sie hier optional die gewünschte IPv6-Adresse ein. Bezieht sich die Adresse auf einen Routing-Präfix, muss sie üblicherweise mit Nullern beginnen. Alle durch das Präfix definierten Bits müssen auf Null gesetzt sein.

11.1-F Geolokation

IP-Objekte dieses Typs können ausschließlich in Firewall-Regeln genutzt werden.

Im SX-GATE ist eine Datenbank integriert, die alle dem jeweiligen Land zugeordneten IP-Adressen kennt. Das Land wird also nicht über DNS ermittelt.



Die Datenbank wird als Teil der SX-GATE-Updates aktualisiert. Die Aktualität der Datenbank hängt somit vom Versionsstand Ihres SX-GATES und dem Veröffentlichungsdatum dieser Version ab.



Auch wenn die Qualität der Datenbank sehr gut ist, können einzelne Fehleinträge nicht gänzlich ausgeschlossen werden.

Beschreibung "..."

Dieser Text dient ausschließlich der Dokumentation.

Ländercodes

Geben Sie hier die gewünschten Ländercodes nach ISO-3166 ein, wie Sie sie von länderspezifischen Toplevel-Domains kennen.

11.1-G Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

11.2 Protokolle

In diesem Bereich definieren Sie die Protokoll- und Portsignatur von Diensten. Dienste in Großbuchstaben sind vordefiniert und können weder bearbeitet noch gelöscht werden.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Protokoll-Kürzel

Legen Sie hier einen Namen für das Protokoll fest. In den Masken zum Anlegen oder Bearbeiten von Regeln kann das Protokoll anschließend unter diesem Namen abgerufen werden.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

11.2-A Protokollsignatur.....	97
11.2-B Anwendungserkennung.....	98
11.2-C Verwendung.....	99

Konfigurationsart

Wählen Sie hier aus, wie das Protokoll konfiguriert wird.

aus DNS SRV Einträgen

Über DNS SRV-Records kann im DNS hinterlegt werden, welche Server einen bestimmten Dienst auf welchem Port bereitstellen. Im Menü "IP-Objekte" lassen sich DNS basierte IP-Objekte definieren, die diese SRV-Records abfragen. Während das IP-Objekt dann die zugehörige IP-Liste zur Verfügung stellt, erhalten Sie über eine entsprechende Protokolldefinition Zugriff auf die Portsignatur.

11.2-A Protokollsignatur

In verschiedenen Bereichen des SX-GATE wird mit Auswahllisten von Protokollen gearbeitet. Namentlich wären hier in erster Linie die Firewall- und die SOCKS-Proxy-Konfiguration zu nennen. Hier in diesem Bereich werden die zur Auswahl stehenden Einträge konfiguriert. Zusätzlich zu einer Reihe bereits vordefinierter Protokolle lassen sich selbst nach beliebigen Einträge erstellen.

Die Bezeichnung "Protokoll" ist nicht allzu wörtlich zu nehmen. Zur Strukturierung ist es oft sinnvoll, mehrere Protokolle zusammenzufassen. So könnte man z.B. für einen bestimmten Client oder einen bestimmten Server einen eigenen Protokoll-Eintrag anlegen, in dem alle für diese Adresse erlaubten Protokolle konfiguriert werden. Ergänzend ist natürlich noch eine Regel zu erstellen, die das Protokoll mit der IP-Adresse des Clients bzw. Servers assoziiert.

Aus technischer Sicht steht hinter jedem "Protokoll" im Sinne dieses Eingabebereichs eine Liste von Signaturen bestehend aus den drei Feldern IP-Folgeprotokoll, Quell- und Ziel-Port. Portnummern sind dabei nur für die Folgeprotokolle TCP und UDP definiert.

Beschreibung

Dieser Text dient ausschließlich der Dokumentation.

IP-Objekt mit SRV-Portinformationen

Wählen Sie hier bitte das IP-Objekt aus, das die gewünschte Portsignatur bereitstellt. Es kann sich bei dem ausgewählten Objekt auch um eine IP-Gruppe handeln, die mehrere SRV-Einträge zusammenfasst.

Signatur

Die Protokollsignatur setzt sich aus folgenden Spalten zusammen:

Protokoll

Wählen Sie hier zwischen TCP und UDP. Für andere Protokolle wählen Sie bitte den untersten Schalter und geben Sie Nummer oder Name des IP-Folgeprotokolls an.

Quell-Port

Wählen Sie hier den Quell-Port aus. TCP basierende Anwendungen nutzen in der Regel einen zufälligen Quell-Port aus dem Bereich 1024-65535. Auch viele UDP basierte Anwendungen richten sich nach dieser Konvention, oft kommen jedoch auch andere Ports zum Einsatz. Wenn keine genaueren Informationen vorliegen, wählen Sie daher bitte "*" (beliebig)". Für das Protokoll ICMP kann an dieser Stelle der ICMP-Nachrichten-Typ angegeben werden.



Portnummern sind nur für UDP und TCP definiert, ICMP-Typen nur für ICMP. Für alle anderen Protokolle muss hier "*" (beliebig) ausgewählt werden.

Ziel-Port

Wählen Sie hier den Ziel-Port ein unter dem die gewünschte Anwendung erreichbar ist. Für das Protokoll ICMP kann hier der ICMP-Nachrichten-Code eingetragen werden.



Portnummern sind nur für UDP und TCP definiert, ICMP-Codes nur für ICMP. Für alle anderen Protokolle muss dieses Feld frei bleiben.

Enthaltene Protokolle

Das aktuelle Protokoll kann die Signaturen anderer Protokolle einbinden.

11.2-B Anwendungserkennung

Bei aktivierter Anwendungserkennung analysiert die Firewall die übertragenen Nutzdaten und versucht zu erkennen, um welche Anwendung es sich handelt. Indem Sie bei Protokollen die Anwendungserkennung aktivieren, können sie die Anwendungserkennung für Firewall-Regeln (ausgenommen SNAT) und im Bandbreitenmanagement nutzbar machen.



Trifft die Firewall beim Abarbeiten der Regeln auf ein Protokoll mit Anwendungserkennung, muss die Kommunikation für die weitere Analyse zunächst erlaubt werden. Erst wenn die konfigurierte Anwendung erkannt oder ausgeschlossen werden konnte, wird die Verarbeitung der Regeln fortgesetzt. Die Firewall wird damit "löchrig"!

Die Einstellungen auf dieser Seite beziehen sich ausschließlich auf die unter "Signatur" konfigurierten Protokoll-, Port-Kombinationen. Sie wirken nicht auf "Enthaltene Protokolle". Die dort konfigurierten Protokolle haben ihre eigenen Einstellungen zur Anwendungserkennung.

Wird ein Protokoll mit aktivierter Anwendungserkennung in einem Bereich verwendet, der keine Anwendungserkennung unterstützt, bleibt das Protokoll trotzdem wirksam. Es werden jedoch nur die auf dem Reiter (Tab) "Protokollsignatur" konfigurierten Einstellungen berücksichtigt.

Anwendung

Wählen Sie hier die gewünschte Anwendung aus.



Für verschlüsselte Verbindungen ist häufig das Protokoll "TLS" die richtige Wahl.

Servername (inkl. Subdomains)

Bei den Anwendungen "HTTP" und "TLS" ist es möglich, die Erkennung auf bestimmte Server einzugrenzen. Geben Sie dazu einen Server- bzw. Domainnamen ein oder wählen Sie eine Liste aus. Listen können Sie im Menü "Definitionen > Domainlisten" anlegen und verwalten.



Bei "HTTP" wird der Host-Header ausgewertet, bei "TLS" die Server-Name-Indication (SNI).

11.2-C Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

11.3 Zeiträume

Durch die Zuordnung eines hier definierten Zeitraums zu einer Firewall-Regel, können Sie deren Wirkung auf bestimmte Wochentage und Uhrzeiten einschränken.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Kurzbezeichnung

Legen Sie hier einen Namen für den Zeitraum fest. In den Masken zum Anlegen oder Bearbeiten von Firewall-Regeln kann der Zeitraum anschließend unter diesem Namen ausgewählt werden.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

11.3-A Zeitraum.....	100
11.3-B Verwendung.....	100

11.3-A Zeitraum

Beschreibung

Dieser Text dient ausschließlich der Dokumentation.

Enthaltene Zeitintervalle

Stellen Sie hier die einzelnen Zeitabschnitte zusammen aus denen sich der gesamte Zeitraum zusammensetzen soll. Um einen Zeitraum zu definieren der sich über Mitternacht erstreckt darf die Start-Uhrzeit größer sein als das Ende.

11.3-B Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

11.4 Domainlisten

In diesem Menüpunkt können Sie zentral Listen mit Server- bzw. Domainnamen anlegen. Diese Listen lassen sich dann in diversen Einstellungsoptionen, vornehmlich im Menü "Module > Web-Proxy", verwenden.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Listentyp

manuell

Bei dieser Variante wird der Listeninhalt manuell gepflegt. Der Import von Textdateien mit Servernamen bzw. Domains ist möglich.

Download von URL

Wählen Sie diese Variante um eine Liste mit Servernamen bzw. Domains von einem Webserver herunterzuladen.

Name der Liste

Legen Sie bitte hier den Namen der URL-Filter Liste fest.



Neben Kleinbuchstaben und Ziffern sind nur der Bindestrich (-) und der Unterstrich (_) zulässig. Der Name muss mit einem Kleinbuchstaben beginnen. Insbesondere die Verwendung von Umlauten sowie Leerzeichen ist nicht erlaubt.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

11.4-A Liste herunterladen.....	102
11.4-B Einträge.....	103
11.4-C Verwendung.....	104

Listentyp**manuell**

Bei dieser Variante wird der Listeninhalt manuell gepflegt. Der Import von Textdateien mit Servernamen bzw. Domains ist möglich.

Download von URL

Wählen Sie diese Variante um eine Liste mit Servernamen bzw. Domains von einem Webserver herunterzuladen.

11.4-A Liste herunterladen

Lädt eine Liste mit Servernamen bzw. Domain von einem Webserver. Der Download darf auch IP-Adressen enthalten, diese werden aber über einfachen Textvergleich und nicht über DNS-Auflösung geprüft. URLs wie z.B. <https://www.example.com> werden nicht unterstützt.

Bei dem Download muss es sich um eine Textdatei im ASCII-Format handeln. Die Textdatei darf mit gzip oder bzip2 komprimiert sein und es dürfen mehrere Dateien in einem Zip- oder Tar-Archiv zusammengefasst werden. Der Download kann zeitgesteuert automatisch wie auch manuell erfolgen. Einträge in der Liste können mit Leerzeichen, Tabulator oder Zeilenumbruch separiert werden.



Die Liste darf maximal 25 MB groß sein.

SSL-Zertifikat verifizieren

Aktivieren Sie diese Option, um im Falle einer HTTPS-Verbindung das Server-Zertifikat zu prüfen.

Benutzername

Sofern der Web-Server eine Benutzer-Authentifizierung via Basic-Auth benötigt, geben Sie hier bitte den Benutzernamen ein.

Passwort

Das Passwort wird nur benötigt, wenn auch ein Benutzername angegeben wurde.

Hostname/IP

Geben Sie hier bitte den Namen oder die IP-Adresse des Servers ein, von dem die Liste heruntergeladen werden soll.

Port

Sofern der Server nicht auf Port 80 (http) bzw. 443 (https) erreichbar ist, geben Sie hier bitte die Port-Nummer ein.

Dateipfad

Geben Sie hier bitte den Pfad und den Dateinamen für den gewünschten Download ein. Auch die Angabe von URL-Parametern ist möglich.

Maximale Anzahl Einträge

Bitte geben sie hier die maximale Anzahl von importierten Einträgen an.



Sollte dieser Wert überschritten werden, wird der Import abgebrochen und die alten Werte bleiben erhalten.

Zeitgesteuerter Download

Hier aktivieren Sie den regelmäßigen automatischen Download.

Startzeit

Bei einem täglichen Download legen Sie hier die Stunde fest in der der Download stattfindet. Erfolgt der Download mehrmals täglich, wird über diesen Parameter die Stunde des ersten Downloads gesteuert. Die genaue Minutenzahl wird jeweils zufällig bestimmt.

Manueller Download

Ein Download der Liste kann hier jederzeit manuell angestoßen werden. Zur Fehlerdiagnose lassen sich Debug-Meldungen zuschalten.

11.4-B Einträge

Beschreibung

Dieser Text dient ausschließlich der Dokumentation.

Letzes Update

Datum und Uhrzeit des letzten erfolgreichen Downloads, bei dem sich der Inhalt der Liste tatsächlich geändert hat.

Servernamen und Domains

Stellen Sie hier Ihre eigene Liste mit Domains zusammen. Dies beinhaltet auch Subdomains. Ist beispielsweise die Domain "example.com" eingetragen, so bezieht dies z.B. "www.example.com" und "ftp.example.com" mit ein.

Enthaltene Domainlisten

Hier können Sie andere Domainlisten in die aktuelle Domainliste integrieren.

11.4-C Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

11.5 URL-Filter Listen

In diesem Menüpunkt definieren Sie Listen für den URL-Filter des SX-GATE Web-Proxies um den Internet-Zugriff detailliert zu regeln. Diese Listen werden in der Web-Proxy Konfiguration einzelnen Benutzern, IP-Adressen oder Netzwerken zugeordnet.



Der URL-Filter muss über die Web-Proxy Konfiguration aktiviert werden und die jeweiligen Listen müssen in der Konfiguration auch verwendet werden. Andernfalls haben die URL-Filter Listen keine Wirkung.

Jede URL-Filter Liste beinhaltet die Möglichkeit, selbst eine Liste von Domains und Dateierweiterungen zu erstellen. Mit Hilfe einer integrierten kostenfreien URL-Datenbank bzw. einer optionalen kostenpflichtigen URL-Datenbank lässt sich der Zugriff nach inhaltlichen Kategorien reglementieren.



In den Regeln der Web-Proxy Konfiguration wird der Zugriff auf URL-Filter Listen entweder akzeptiert oder verweigert. Inhalte die erlaubt und Inhalte die blockiert werden sollen dürfen daher nicht in ein und derselben Liste enthalten sein. Legen Sie stattdessen zwei Listen an. Es ist meist hilfreich, ein Kürzel wie "_erlaubt" und "_verboten" an den Namen jeder Liste anzuhängen um den beabsichtigten Verwendungszweck zu dokumentieren.

Ein abgewiesener Zugriff wird über eine entsprechende Seite dem Benutzer angezeigt. Eine Ausnahme bilden Einträge aus der Datenbankkategorie "Werbung". Um Werbebanner auszublenden, werden Zugriffe auf ein transparentes Bild umgelenkt, sofern die URL eine gängige Dateinamenserweiterung für Bilder aufweist und detaillierte "Zugriff verweigert"-Meldungen aktiviert sind.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Listentyp**manuell**

Bei dieser Variante wird der Listeninhalt manuell gepflegt. Der Import von Textdateien mit Domains oder Dateinamenserweiterungen ist möglich. Ferner können Sie Kategorien der integrierten URL-Datenbank auswählen.

Download von URL

Wählen Sie diese Variante um eine URL-Liste von einem Webserver herunterzuladen.

Name der Liste

Legen Sie bitte hier den Namen der URL-Filter Liste fest.



Neben Kleinbuchstaben und Ziffern sind nur der Bindestrich (-) und der Unterstrich (_) zulässig. Der Name muss mit einem Kleinbuchstaben beginnen. Insbesondere die Verwendung von Umlauten sowie Leerzeichen ist nicht erlaubt.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

11.5-A Liste herunterladen.....	106
11.5-B Domains.....	108
11.5-C Dateinamen.....	109
11.5-D Datenbank-Kategorien.....	109
11.5-E Datenbank-Kategorien.....	109
11.5-F Sonstiges.....	112
11.5-G Verwendung.....	113

11.5-A Liste herunterladen

Lädt eine URL-Liste von einem Webserver. Der Download darf Servernamen, Domains und URLs (z.B. "http://example.com" oder "https://example.com/images/ad.png?a=b") enthalten. Der Download darf auch IP-Adressen enthalten, diese werden aber über einfachen Textvergleich und nicht über DNS-Auflösung geprüft.



In verschlüsselten Verbindungen (HTTPS) können URLs mit Pfad- bzw. Dateiangaben nur dann gefunden werden, wenn die Option zum Aufbrechen verschlüsselter Verbindungen aktiviert ist.

Im Server- bzw. Domainnamen und in IPs ist die Angabe des Platzhalters "*" zulässig (z.B. "srv*.example.com" oder "https://www.example.*/index.html"). Er steht für beliebige Zeichen, aber nur innerhalb der jeweiligen Teilkomponente des Namens bzw. der IP. Der Platzhalter steht nicht für mehrere Namenskomponenten (z.B. steht "www.example.*" nicht für "www.example.co.uk"). Der Platzhalter hat keine Sonderbedeutung in URL-Pfaden, Dateinamen oder Parametern.

Bei dem Download muss es sich um eine Textdatei im ASCII-Format handeln. Die Textdatei darf mit gzip oder bzip2 komprimiert sein und es dürfen mehrere Dateien in einem Zip- oder Tar-Archiv zusammengefasst werden. Der Download kann zeitgesteuert automatisch wie auch manuell erfolgen. Einträge in der Liste können mit Leerzeichen, Tabulator oder Zeilenumbruch separiert werden.



Die Liste darf maximal 25 MB groß sein.

SSL-Zertifikat verifizieren

Aktivieren Sie diese Option, um im Falle einer HTTPS-Verbindung das Server-Zertifikat zu prüfen.

Benutzername

Sofern der Web-Server eine Benutzer-Authentifizierung via Basic-Auth benötigt, geben Sie hier bitte den Benutzernamen ein.

Passwort

Das Passwort wird nur benötigt, wenn auch ein Benutzername angegeben wurde.

Hostname/IP

Geben Sie hier bitte den Namen oder die IP-Adresse des Servers ein, von dem die Liste heruntergeladen werden soll.

Port

Sofern der Server nicht auf Port 80 (http) bzw. 443 (https) erreichbar ist, geben Sie hier bitte die Port-Nummer ein.

Dateipfad

Geben Sie hier bitte den Pfad und den Dateinamen für den gewünschten Download ein. Auch die Angabe von URL-Parametern ist möglich.

Maximale Anzahl Einträge

Bitte geben sie hier die maximale Anzahl von importierten Einträgen an.



Sollte dieser Wert überschritten werden, wird der Import abgebrochen und die alten Werte bleiben erhalten.

Zeitgesteuerter Download

Hier aktivieren Sie den regelmäßigen automatischen Download.

Startzeit

Bei einem täglichen Download legen Sie hier die Stunde fest in der der Download stattfindet. Erfolgt der Download mehrmals täglich, wird über diesen Parameter die Stunde des ersten Downloads gesteuert. Die genaue Minutenzahl wird jeweils zufällig bestimmt.

Manueller Download

Ein Download der Liste kann hier jederzeit manuell angestoßen werden. Zur Fehlerdiagnose lassen sich Debug-Meldungen zuschalten.

11.5-B Domains

Benutzerdefinierte Domains (inkl. Subdomains)

Stellen Sie hier Ihre eigene Liste mit Domains oder IP-Adressen zusammen. In der Web-Proxy Konfiguration lässt sich der Zugriff auf diese URL-Filter Liste und damit auf die hier eingetragenen Domains erlauben oder verweigern. Bei Angabe einer Domain bezieht dies Subdomains mit ein. Ist beispielsweise die Domain "example.com" eingetragen, so sind auch z.B. Zugriffe auf "www.example.com" und "ftp.example.com" betroffen. Groß- und Kleinschreibung werden nicht unterschieden.



Die Adressen in dieser Liste werden exakt mit der angeforderten Adresse verglichen, ohne dabei DNS-Anfragen durchzuführen. Ist eine Domain anhand Ihres DNS-Namens gesperrt, so kann daher möglicherweise dennoch über die IP-Adresse auf den Server zugegriffen werden und umgekehrt.

11.5-C Dateinamen

Dateinamenserweiterungen

Der Zugriff auf bestimmte Dateiarten kann basierend auf der Endung des Dateinamens reglementiert werden. Geben Sie dazu hier die entsprechenden Dateinamenserweiterungen ein. Es spielt dabei keine Rolle, ob Sie eine Erweiterung als z.B. "mp3", ".mp3" oder "*.mp3" angeben. Alle drei Schreibweisen sind gleichbedeutend mit der Erweiterung "mp3". SX-GATE prüft, ob eine Anfrage mit einem Punkt, gefolgt von einer der hier angegebenen Erweiterungen endet. Groß- und Kleinschreibung spielt dabei keine Rolle.



Es erfolgt ausschließlich ein Text-Vergleich zwischen dem Dateinamen in der angefragten Adresse und den Endungen in dieser Liste. Es erfolgt keine Analyse von aus dem Internet empfangenen Daten.

11.5-D Datenbank-Kategorien

Unterhaltung

Chat, private Foren, Einkaufen, Spielen, Sport und einige mehr.

Schulprojekt Deutscher Bildungsserver

Vom "Deutschen Bildungsserver" wurde uns freundlicherweise die Online-Ressourcen-Datenbank zur Verfügung gestellt. Aus dieser wurde automatisch eine Positivliste generiert die weitgehend den Zugriff auf die Online-Ressourcen ermöglicht. Links von den Online-Ressourcen aus auf andere Server oder Serverbereiche werden jedoch im allgemeinen nicht abgedeckt.

Unbedenkliche Server

Banken und Finanzen, Blogs, Jobsuche, Nachschlagewerke, Nachrichten und Zeitschriften, Wellness und einiges mehr, die nicht in anderen Kategorien enthalten sind.

11.5-E Datenbank-Kategorien

Pornographie

Inhalte für Erwachsene (Pornografie) und Webseiten, die für Kinder ungeeignet sind.

Gewalt

Webseiten über gewalttätiges Verhalten und aggressive Waffenverkäufe.

Waffen

Webseiten über Schießstände, echte Waffen und Spielzeug-/Spielwaffen, die wie echte Waffen aussehen. Spielzeugwaffen und Wasserpistolen, die nicht wie eine echte Waffe aussehen, sind ausgeschlossen. Waffensport-Webseiten, auf denen Waffen nicht in auffälliger oder aggressiver Weise dargestellt werden, sind ausgeschlossen und gehören zur Kategorie Sport.

Warez (Cracks, Lizenzschlüssel)

Webseiten mit illegaler Software, illegalen Softwarecodes, Hackerseiten, Warez und Cracks.

Illegale Aktivitäten

Webseiten, die erklären, wie man illegale Aktivitäten durchführt.

Harte Drogen

Webseiten über harte Drogen. Bildungsseiten über Drogen und Seiten über weiche Drogen sind ausgeschlossen.

Weiche Drogen

Webseiten von Herstellern und Verkäufern weicher Drogen und Webseiten, die den Konsum weicher Drogen fördern oder diskutieren. Webseiten, die ausschließlich Produkte auf Cannabisbasis für den medizinischen Gebrauch anbieten, sowie Webseiten von Regierungen und Gesundheitseinrichtungen sind ausgeschlossen.

Alkohol

Webseiten von Alkoholherstellern und Webseiten, auf denen es hauptsächlich um den Verkauf oder Konsum von Alkohol geht. Restaurants, Bars, Supermärkte usw. sind nicht eingeschlossen. Aber einige Getränkemärkte.

Proxy-Server

Seiten, die zum Herunterladen von Inhalten anderer Seiten verwendet werden können, URL-Umschreibeseiten und VPNs. Proxies werden häufig verwendet, um einen URL-Filter zu umgehen, und sollten immer blockiert werden. Webseiten, die Wörter oder Texte, aber keine Webseiten übersetzen, sind ausgeschlossen.

DNS-over-HTTPS

Webseiten sowie IP-Adressen und Domainnamen von Diensten für DNS-Abfragen über HTTPS. DNS über HTTPS ist ein einfacher und effektiver Weg, um URL-Filterung zu umgehen, und es wird empfohlen, diese Kategorie zu verwenden.

Datensammeln von Microsoft

URLs, die von Microsoft verwendet werden, um Benutzer- und Systemdaten von Workstations, Web-Browsern und Apps zu sammeln.

Werbung

Webseiten mit Werbung, Überwachung des Nutzerverhaltens, Traffic-Tracker und Webseiten-Zähler.

Geparkte Domains

Geparkte Domains haben keinen regulären Inhalt mehr. Sie werden geparkt, um verkauft zu werden und/oder Einnahmen aus Anzeigen zu erzielen. Einige geparkte Domains werden von minderwertigen Ad-Brokern betrieben, die relativ häufig mit Betrug und Malware zu tun haben.

Peer-to-Peer

Seiten, die den Austausch von Dateien ermöglichen. Dort sind oft Filme, Musik und nicht jugendfreie Inhalte erhältlich, die oft auch das Urheberrecht verletzen.

Blogs, private Homepages/Web-Disks

Blogs, Seiten von privaten Personen und private Web-Disks.

Dynamische Adressen

Computer ohne statische IP Adresse verwenden dynamische Adressen, die von dynamischen DNS Servern verwaltet werden. Sie werden häufig verwendet um auf Computer, die Zuhause stehen, zuzugreifen und können auch als Proxy verwendet werden.

Toolbars

Webseiten für Symbolleisten von Browsern. Eine Symbolleiste ist eine Erweiterung eines Webbrowsers, die Ihre Privatsphäre verletzen oder private Dateien öffentlich machen kann.

Unterhaltung

Seiten, die der Unterhaltung dienen, wie z.B. Lifestyle, Hobby, Kunst, Museen, Mode, elektronische Karten, Zeitschriften, Horoskope, Desktop-Hintergrundbilder, Clip-Art, Fotos, Portale, Veranstaltungen, Fanseiten, Baby- und Kinderseiten, Bilderaustausch und andere Seiten für Privatpersonen, die nicht mit der Wirtschaft verbunden sind.

Bildung

Webseiten von Schulen, Universitäten, Fahrschulen und verschiedenen anderen Bildungseinrichtungen.

Restaurants und Kochrezepte

Webseiten von Restaurants und Rezeptseiten. Beachten Sie, dass Supermärkte, Imbiss- und Fastfood-Ketten in der Kategorie Einkaufen enthalten sind.

Gesundheit, Gesundheitswesen, Krankenversicherung

Webseiten von Krankenhäusern, Kliniken, Ärzten und Webseiten mit Informationen über Gesundheit.

Haus oder Wohnung kaufen oder mieten

Webseiten von Immobilienmaklern und Bauunternehmen mit Schwerpunkt auf Häusern und Wohnungen.

Chat mit KI-Bots

Webseiten, zur Kommunikation mit KI-Chatbots. Chatsbots für Bildung, Business und Kundensupport sind nicht enthalten.

Chat

Webseiten für Chat und Messaging.

Externe Web-Anwendungen

Webbasierte Texteditoren, Tabellenkalkulationen, Desktops und Groupware.

Private Foren

Webseiten mit einem Forum. Geschäftsbezogene Foren sind nicht enthalten.

Sport

Webseiten zum Thema Sport, einschließlich der Sportabschnitte von Nachrichtenseiten, Sportfans, Seiten über die aktive Ausübung einer Sportart.

Einkaufen

Webseiten mit Shops, Preisvergleichen und Auktionen, die sich an Verbraucher richten. Webseiten, die sich an Geschäftskunden richten, sind ausgeschlossen.

Reisen

Webseiten über Reisebüros, Fluggesellschaften, Tourismus-Seiten, Hotels, Ferienanlagen.

Jobsuche

Webseiten über und für Bewerbungen. Webseiten für Bewerbungen von Studenten sind nicht enthalten.

Finanzen

Webseiten von Banken, Versicherungsgesellschaften, Börsen und Börsenmaklern.

Börsen und Handelssysteme

Webseiten zum Thema Aktienmärkte und Handelssysteme sowie Webseiten zum Thema Investitionen.

Schulprojekt Deutscher Bildungsserver

Vom "Deutschen Bildungsserver" wurde uns freundlicherweise die Online-Ressourcen-Datenbank zur Verfügung gestellt. Aus dieser wurde automatisch eine Positivliste generiert die weitgehend den Zugriff auf die Online-Ressourcen ermöglicht. Links von den Online-Ressourcen aus auf andere Server oder Serverbereiche werden jedoch im allgemeinen nicht abgedeckt.

Unbedenkliche Server

In dieser Datenbank sind Adressen hinterlegt, deren Inhalte zu keiner der anderen Kategorien passen.

11.5-F Sonstiges

Beschreibung

Dieser Text dient ausschließlich der Dokumentation.

Letzes Update

Datum und Uhrzeit des letzten erfolgreichen Downloads, bei dem sich der Inhalt der Liste tatsächlich geändert hat.

URLs mit pornographischen Schlüsselwörtern

Wird dieser Schalter aktiviert, so wird nach einschlägigen Schlüsselwörtern in der angeforderten Adresse (URL) gesucht.



Auch hier wird lediglich die Adresse als solches geprüft, nicht der tatsächliche Inhalt des angesprochenen Internet-Servers.

Jugendgefährdende Inhalte in Suchergebnissen

Viele Suchmaschinen bieten einen speziellen Suchmodus an, in dem nicht jugendfreie Inhalte aus Suchergebnissen ausgeschlossen werden. Wird der Zugriff auf diese URL-Filter Liste verweigert und der Schalter ist aktiv, wird der spezielle Suchmodus in den gängigsten Suchmaschinen erzwungen.

11.5-G Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

12 System

Alle Funktionen zur laufenden administrativen Arbeit mit dem SX-GATE sind im Hauptmenü "System" zusammengefaßt. Hier finden Sie unter anderem die Benutzerverwaltung aber auch die Backup und Update Routinen.

12.1 Grundeinstellungen

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.1-A LAN Einstellungen.....	114
12.1-B Download Proxy.....	115
12.1-C Clustering.....	115
12.1-D Administrations-Server.....	119
12.1-E Verwaltungszugriff.....	121

12.1-A LAN Einstellungen

In dieser Maske werden die wichtigsten Parameter der LAN-Anbindung des SX-GATE hinterlegt. Die hier eingetragenen Daten dienen ferner als Grundeinstellung für viele weitere Einstellungen Ihres SX-GATE.

Rechnername

Legen Sie hier den Hostnamen des SX-GATE fest.

Domain

Geben Sie hier die Domain für SX-GATE ein. Sofern Ihre Firma bereits über eine Internet-Domain verfügt, empfiehlt es sich, diese zu verwenden. Besitzen Sie noch keine Internet-Domain, so geben Sie bitte eine Domain an, die es so garantiert nicht im Internet gibt (z.B. "firma.intern"). Andernfalls kann es zu Konflikten kommen.



Die Domain von der hier die Rede ist hat nichts mit einer eventuell vorhandenen Windows-NT Domäne zu tun.

IP-Adresse

Tragen Sie hier die IP-Adresse für die primäre Ethernet-Schnittstelle des SX-GATE ein (eth0). Üblicherweise ist diese Schnittstelle mit dem internen LAN verbunden.

Netzmaske

In diesem Feld muss die zur internen IP-Adresse passende Netzmaske hinterlegt werden.

Sprache

Wählen Sie hier die Standard-Sprache aus, in der die Oberfläche dargestellt werden soll.



Damit die Oberfläche in geänderter Sprache dargestellt wird, müssen Sie die Oberfläche über die Startseite neu aufrufen. Eventuell muss zuvor der Cache Ihres Web-Browsers geleert werden.

12.1-B Download Proxy

Hier können Sie einen eventuell erforderlichen Proxy für vom SX-GATE durchgeführte Downloads konfigurieren. Dies betrifft z.B. SX-GATE, Virenschanner-Signaturen, IDS und URL-Filter Updates.

12.1-C Clustering

Diese Funktion bietet Ihnen die Möglichkeit, zwei SX-GATE zu einem Failover-Cluster zu verbinden. Dabei wird keine zusätzliche Schnittstelle benötigt, da die Synchronisation über die LAN-Schnittstelle stattfinden kann. Die LAN-Schnittstellen der zwei SX-GATEs sollten dabei direkt über einen Switch miteinander verbunden sein.



Zur Abklärung technischer Randbedingungen empfehlen wir, sich vor Einsatz dieses Features mit dem technischen Support in Verbindung zu setzen.

Die Konfiguration des Clusters wird, bis auf die Schnittstellen, grundsätzlich am Backup-Knoten vorgenommen und über "Konfiguration des Masters aktualisieren" auf den Master-Knoten übertragen. Bevor Sie die Konfiguration übertragen können, muss der öffentliche SSH-ed25519 oder SSH-RSA Schlüssel des Backup-Knoten auf dem Master-Knoten eingespielt werden.

Die Überwachung des Clusters übernimmt der Dienst Cluster-Knoten, der unter "System > Dienste" aktiviert werden muss.

Damit der Cluster nach "außen" als ein Server erscheint, müssen Sie ihm auf den entsprechenden Schnittstellen eine gemeinsame virtuelle IP-Adresse (VIP) vergeben. Diese konfigurieren Sie unter "Module > Netzwerk > Schnittstellen". Wählen Sie die entsprechende Schnittstelle aus und vergeben unter "zusätzliche IPv4-Adressen (Aliase) bzw. Cluster-IP-Adressen" die entsprechende Adresse. Voraussetzung dafür ist, dass die Schnittstelle auf dem Master-Knoten ebenfalls existiert.

Mitglied in Failover-Cluster

Wählen Sie hier die Rolle dieses SX-GATEs im Failover-Cluster.

IP des Masters

In diesem Feld geben Sie die IP-Adresse der Schnittstelle auf dem Master an, die zur Synchronisation zwischen Master und Backup benutzt werden soll. Im Normalfall wird hierzu die LAN-Schnittstelle benutzt.

IP des Backups

In diesem Feld geben Sie die IP-Adresse der Schnittstelle auf dem Backup an, die zur Synchronisation zwischen Master und Backup benutzt werden soll. Die IP-Adressen von Master und Backup müssen aus dem gleichen IP-Adressbereich stammen.

Eigenen Öffentlichen SSH Schlüssel exportieren

Hier können Sie den öffentlichen SSH Schlüssel herunterladen. Sie müssen diesen auf dem Master-Knoten importieren, damit der Backup-Knoten die Konfiguration des Masters aktualisieren kann.

SSH Schlüssel verwalten

Hier kann man die Einträge des öffentlichen SSH-Schlüssels des Masters auf dem Backup verwalten. Falls das Backup nicht in der Lage ist, mit dem Master zu kommunizieren, der Master ersetzt wurde oder ein neuer Master hinzugefügt wurde, klicken Sie bitte hier.

SSH Schlüssel verwalten

Damit das Backup in der Lage ist, Konfiguration und Mail an den Master zu synchronisieren, verbindet sich der Backup-Knoten über SSH mit dem Master. Um sicherzustellen, dass das Backup mit dem richtigen Knoten kommuniziert, wird der öffentliche SSH-Schlüssel des Masters auf dem Backup importiert. Dieser Assistent ermöglicht es, die derzeit zur IP des Masters hinterlegten Schlüssel einzusehen und mit den von der IP des Masters aktuell genutzten Schlüsseln zu vergleichen. Wenn mindestens einer der hinterlegten Schlüssel mit den aktuellen Schlüsseln des Masters übereinstimmt, dann ist bereits alles in Ordnung und dieser Dialog kann verlassen werden. Wenn nicht, dann kann man hier Schlüssel löschen, hinzufügen und ersetzen. Beim Hinzufügen von Schlüsseln, sollten Sie prüfen, ob die hier angezeigten Schlüssel

mit den auf der Administrations-Oberfläche des Masters angezeigten Schlüsseln übereinstimmen.

Hinterlegte öffentliche SSH-Schlüssel des Masters

Dies sind die derzeit auf dem Backup hinterlegten öffentlichen SSH-Schlüssel des Masters. Sofern nachfolgend die aktuellen öffentlichen SSH-Schlüssel des Master-Knotens angezeigt werden, sollte mindestens einer davon identisch sein.

Aktuell von der IP des Masters abgerufene öffentliche SSH-Schlüssel

Dies sind die öffentlichen SSH-Schlüssel, die soeben vom Master-Knoten abgerufen wurden. Wenn weiter oben auch die lokal hinterlegten Public-Key-Einträge angezeigt wurden und mindestens einer davon identisch ist, sind keine weiteren Schritte erforderlich. Andernfalls sollten Sie diese Schlüssel mit den in der Administrations-Oberfläche des Masters angezeigten Schlüsseln vergleichen. Sind sie identisch und werden Sie nicht bereits weiter oben angezeigt, dann sollten sie hinzugefügt oder als Ersatz für alle bereits vorhandenen Schlüssel verwendet werden.

Bitte wählen Sie

Unverändert lassen

Für den Fall, dass alles schon korrekt ist, können Sie hier klicken.

Hinterlegte Einträge mit den aktuell vom Master abgerufenen Schlüsseln ersetzen

Um die hinterlegten Schlüssel zu löschen und stattdessen die soeben vom Master abgerufenen Schlüssel einzutragen, klicken Sie bitte hier. Dies ist üblicherweise notwendig, wenn der Master-Knoten ersetzt worden ist. Es ist wichtig, dass die neuen Schlüssel mit den in der Administrations-Oberfläche des Masters angezeigten übereinstimmen.

Vom Master abgerufene Schlüssel hinzufügen

Im Falle eines neuen Master-Knotens, neuer Master-Schlüssel, einer Schlüsselrotation oder ähnlichem kann diese Option verwendet werden, um neue öffentliche SSH-Schlüssel vom Master zu importieren. Es ist wichtig, dass die neuen Schlüssel mit den in der Administrations-Oberfläche des Masters angezeigten übereinstimmen.

Hinterlegte Einträge löschen

Falls der Cluster abgebaut wurde, die hinterlegten Schlüssel des Masters falsch sind, oder diese aus einem anderen Grund gelöscht werden sollen, klicken Sie bitte hier.

Temporärer Zugriff auf alle Einstellungen

Bis Sie sich abmelden erhalten Sie Zugriff auf alle Einstellungen. Etwaige Änderungen an sonst nicht verfügbaren Einstellungen werden bei der nächsten Synchronisation mit dem Backup-Knoten überschrieben.

Öffentlichen SSH Schlüssel des Backups importieren

Hier importieren Sie den öffentlichen SSH Schlüssel des Backup-Knotens.

Automatisch synchronisieren

Konfigurationsänderungen auf dem Backup-System müssen auf das Master-System übertragen werden. Sie können dies jederzeit mit der Befehlsschaltfläche "Konfiguration des Masters aktualisieren" von Hand auslösen. Damit dies nicht vergessen wird, können Sie aber auch die automatische Synchronisation aktivieren.



Insbesondere wenn Benutzer Zugriff auf die Einstellungen im Menü "Mein Konto" haben, empfiehlt es sich, die automatische Synchronisation zumindest für Benutzer-Einstellungen zu aktivieren. Da der Administrator ja nicht weiß, wann Benutzer ihre Einstellungen ändern, ist nur so eine zeitnahe Synchronisation möglich.

Verzögerung nach letzter Änderung

Steht dieser Parameter auf "0", wird jede Änderung sofort an das Master-System übertragen. Andernfalls wird die Übertragung erst angestoßen, wenn die letzte Änderung entsprechend lang zurück liegt. Mehrere aufeinanderfolgende Konfigurationsänderungen werden so in einer Aktualisierung zusammengefasst. Auf dem Master-System reduziert sich so die Häufigkeit von Neustarts betroffener Dienste.

Konfiguration des Masters aktualisieren

Mit dieser Option übertragen Sie die aktuelle Konfiguration auf den Master-Knoten. Neben der Benutzer- und System-Konfiguration werden auch private Schlüssel und Zertifikate kopiert. Auf dem Master-Knoten bereits vorhandenes Schlüsselmaterial wird dabei überschrieben. Die Zertifikate der einzelnen Dienste werden allerdings nur dann berücksichtigt, wenn es sich nicht um selbstsignierte Zertifikate handelt. Folgende Komponenten sind betroffen:

- SX-GATE CA (der private Schlüssel wird nicht übertragen!)
- SX-GATE VPN-Server (IPSec und OpenVPN)
- verbindungspezifische Schlüssel aus OpenVPN Client-Schnittstellen
- SX-GATE Mail-Server (SMTP, IMAP und POP3)
- SX-GATE Reverse-Proxy

Nicht übermittelt werden folgende Schlüssel und Zertifikate, da diese entweder individuell für jeden Knoten sind oder deren Nutzung auf dem Master-Knoten nicht sinnvoll ist:

- privater Schlüssel der SX-GATE CA
- SSL-Proxy CA zum Aufbrechen von SSL-Verbindungen
- SX-GATE Administrations-Server

Eigene öffentliche SSH-Schlüssel

Hier werden die eigenen öffentlichen SSH-Schlüssel angezeigt. Diese werden vom Backup-Knoten benötigt, um die Identität dieses Hosts zu verifizieren.

12.1-D Administrations-Server

Auf dieser Seite konfigurieren Sie den Administrations-Webserver.

Einmalpasswörter bei direktem Zugriff

Zusätzlich zu Benutzername und Kennwort kann für den Zugriff auf die Administrations-Oberfläche ein Einmalpasswort abgefragt werden. In dieser Einstellung legen Sie fest, ob Einmalkennwörter bei direktem Zugriff auf Port 44344 (bzw. unverschlüsselt auf Port 8000) aktiviert sein sollen.



Der direkte Zugriff erfolgt typischerweise aus lokalen Netzwerken. Sofern Internetzugriff auf die Administrations-Oberfläche gewünscht ist, sollte die Verbindung über den Reverse-Proxy erfolgen.

Die Änderung dieser Einstellung wirkt sich unmittelbar auf die bestehende Sitzung aus, kann also ohne erfolgreiche Authentifizierung mit Einmalkennwort nicht wieder rückgängig gemacht werden.



Aktivieren Sie Einmalpasswörter schrittweise. Sorgen Sie zunächst dafür, dass ein zweiter Benutzer Zugriff auf dieses Menü hat. Aktivieren Sie nur bei einem dieser Benutzer das Einmalkennwort und wählen Sie dann die Option "optional".



Erfolgt der Zugriff über die Konsole (127.0.0.1) wird grundsätzlich kein Einmalkennwort verlangt.

optional

In dieser Einstellung müssen sich nur die Benutzer mit Einmalpasswort anmelden, für die in der Benutzerverwaltung Einmalkennwörter aktiviert wurden. Alle anderen Benutzer können sich ohne Einmalpasswort anmelden.

erforderlich

In dieser Einstellung müssen sich alle Benutzer mit Einmalpasswort anmelden. Benutzer, für die in der Benutzerverwaltung Einmalkennwörter nicht aktiviert wurden, können sich auf diesem Weg nicht anmelden.

Einmalpasswörter bei Zugriff über Reverse-Proxy

Zusätzlich zu Benutzername und Kennwort kann für den Zugriff auf die Administrations-Oberfläche ein Einmalpasswort abgefragt werden. In dieser Einstellung legen Sie fest, ob Einmalkennwörter bei Zugriff über Reverse-Proxy erforderlich sind. Der Zugriff über Reverse-Proxy wird typischerweise genutzt, falls der Zugriff auf die Administrations-Oberfläche aus dem Internet notwendig ist.

optional

In dieser Einstellung müssen sich nur die Benutzer mit Einmalpasswort anmelden, für die in der Benutzerverwaltung Einmalkennwörter aktiviert wurden. Alle anderen Benutzer können sich ohne Einmalpasswort anmelden.

erforderlich

In dieser Einstellung müssen sich alle Benutzer mit Einmalpasswort anmelden. Benutzer, für die in der Benutzerverwaltung Einmalkennwörter nicht aktiviert wurden, können sich auf diesem Weg nicht anmelden.

Temporärer Zugriff auf versteckte Menüs

Bis Sie sich abmelden erhalten Sie Zugriff auf ansonsten versteckte Menüs.

HTTPS-Schlüssel/Zertifikat auswählen

Dieses Zertifikat wird für den direkten verschlüsselten Zugriff auf die Administrationsoberfläche verwendet. Beim Zugriff über Reverse-Proxy spielt dieses Zertifikat keine Rolle.



Nutzen Sie den Reverse-Proxy, um aus dem Internet auf den Administrations-Servers zuzugreifen. Der Reverse-Proxy ermöglicht es, nur Teilbereiche (z.B. Mail-Quarantäne) freizugeben. Um den Internet-Zugriff auf die Administrationsoberfläche abzusichern, kann der Reverse-Proxy zudem Authentifizierung über Client-Zertifikate verlangen.

Wählen Sie hier einen der Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.

12.1-E Verwaltungszugriff

Über die nachfolgenden Einstellungen geben Sie den Zugriff frei, falls SX-GATE von einem zentralen System aus verwaltet werden soll.

Verbindungsart

Wählen Sie bitte aus, wie die Verbindung zwischen dem SX-GATE und dem zentralen Verwaltungsserver aufgebaut werden soll.



Wenn Sie diese Einstellung ändern, werden eventuell bestehende ausgehende Tunnel beendet.

eingehend

Wählen Sie diese Variante, wenn der Verwaltungsserver die Verwaltungsverbindung direkt zu Ihrem SX-GATE aufbaut. Die Verbindung erfolgt mittel Secure-Shell (SSH) zum Server auf Port 22.

Diese Variante bietet sich an, wenn bereits eine VPN-Verbindung zwischen Verwaltungsserver und SX-GATE besteht. Der Verwaltungsserver sollte die interne IP des SX-GATES für den Zugriff verwenden.

Wenn keine VPN-Verbindung besteht, der SX-GATE SSH-Server aber aus dem Internet direkt angesprochen werden kann und der Verwaltungsserver über eine statische IP verfügt, ist diese Verbindungsvariante ebenfalls möglich. In der Firewall der Internet-Schnittstelle ist der Zugriff für den Managementserver mit Protokoll "SSH" auf den SX-GATE freizugeben.



Geben Sie in der Firewall keinesfalls den Zugriff für beliebige Quell-Adressen frei. Nur der Verwaltungsserver darf Zugriff erhalten.

Cluster-Systeme können diese Verbindungsvariante nur dann nutzen, wenn beide Systeme vom Verwaltungsserver aus unter einer individuellen Adresse erreichbar sind.

ausgehend

Diese Variante ist etwas umfangreicher zu konfigurieren, funktioniert aber in praktisch allen Situationen. Dabei baut der verwaltete SX-GATE zuerst einen SSH-Tunnel zum Verwaltungsserver auf. Diese Verbindung nutzt den Port 2222 (SSH TCP-Forwarder). Der Verwaltungsserver kann sich dann über den

Tunnel zu Ihrem SX-GATE verbinden. Es müssen dazu keine Firewall-Regeln konfiguriert werden.

Verwaltungsserver

Im Fall von "Verbindungsart ausgehend" legen Sie hier die Adresse des Verwaltungsservers fest, zu der sich SX-GATE verbinden soll.

Verbindungs-ID

Im Fall von "Verbindungsart ausgehend" geben Sie hier die Verbindungs-ID ein, die Ihnen vom Betreiber des Verwaltungsservers mitgeteilt wird.

Privater Schlüssel für die Anmeldung auf Verwaltungsserver

Bei einer ausgehenden Verbindung nutzt SX-GATE diesen Schlüssel, um sich beim Verwaltungsserver anzumelden.



Private Schlüssel werden im Menü "System > Zertifikatsverwaltung > Schlüsselbund" verwaltet.

Zugehöriger öffentlicher Schlüssel

Den zugehörigen öffentlichen Schlüssel müssen Sie dem Betreiber des Verwaltungsservers mitteilen, damit dieser den Zugang für Ihren SX-GATE freigeben kann.

Öffentlicher ed25519-Schlüssel, der dem Besitzer des zugehörigen privaten Schlüssels Zugriff auf Ihren SX-GATE erlaubt

Sie erhalten diesen Schlüssel vom Administrator des Verwaltungsservers. Der Verwaltungsserver erhält dadurch Zugriff auf Ihren SX-GATE über den ssh-Dienst.

Fehlerprotokoll anzeigen

Hier können Sie sich die Fehlermeldungen anzeigen lassen, falls die Verbindung mit dem Verwaltungsserver fehlschlägt.

Öffentlichen Schlüssel des SSH-TCP-Forwarders am Verwaltungsserver aktualisieren.

Sollte auf dem Verwaltungsserver ein Tausch des SSH-Schlüssels für den TCP-Forwarder notwendig geworden sein, können Sie hier den gespeicherten öffentlichen Schlüssel aktualisieren.

Installationspaket für den Verwaltungszugriff einspielen

Um die Fernverwaltung dieses Systems bequem einrichten zu können, kann Ihnen ein Installationspaket zur Verfügung gestellt werden. Sie müssen dazu nur die erhaltene Datei hochladen und das zugehörige Kennwort eingeben.

Installationspaket hochladen***Zu installierende Datei (*.rin)***

Wählen Sie hier bitte das Installationspaket aus. Darin sind ein privater ed25519-Schlüssel für die Anmeldung am Verwaltungsserver und eine Konfigurationsdatei enthalten. Die Datei ist mit einem Passwort verschlüsselt.

Please select the installation file. It contains a private ed25519 key for logging on to the management server and a configuration file. The file is encrypted with a password.

12.2 Dienste

In diesem Menü werden die verschiedenen Dienste angezeigt, die SX-GATE bereitstellt. Die Dienste lassen sich in diesem Menü starten, stoppen oder neu starten. Der Status des Dienstes wird über das grüne oder rote Ampel-Symbol angezeigt.



Über "starten", "neu starten" bzw. "stoppen" wird zugleich festgelegt, ob der Dienst beim nächsten Neustart des Systems aktiviert werden soll oder nicht.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.2-A Netzwerk-Dienste.....	124
12.2-B Server-Dienste.....	126
12.2-C Weitere Server.....	128
12.2-D System-Dienste.....	130

12.2-A Netzwerk-Dienste

In dieser Maske ist der Status der verschiedensten Netzwerk-Dienste zu sehen.



Auf dem Backup-Knoten eines Clusters wird bei pausierten Diensten der Status "gelb" angezeigt. Ein Dienst wird pausiert, wenn er nur auf dem aktiven Knoten laufen darf.

Ethernet

Dieser Dienst repräsentiert die Netzwerkschnittstellen des SX-GATE. Da diese eine zentrale Bedeutung haben, ist hier nur ein Neustart möglich. Das Beenden dieses Dienstes ist nicht vorgesehen, da ansonsten auch kein Zugriff mehr auf die Administrations-Oberfläche möglich wäre.

WLAN

Dieser Dienst ermöglicht Clients per Wireless-LAN anzubinden.

IPv6 Router Advertisement

Dieser Dienst ist erforderlich, um SX-GATE als IPv6-Router nutzen zu können.

ADSL (PPP over Ethernet)

ADSL-Wählverbindungen werden über diesen Dienst gesteuert. Ein Neustart dieses Dienstes trennt alle aktiven ADSL-Wählverbindungen.



Sind alle ADSL-Schnittstellen so eingestellt, dass die Wählverbindungen permanent online gehalten werden sollen, so wird dieser Dienst solange als gestoppt angezeigt, bis mindestens eine Verbindung erfolgreich erstellt ist.

Wireguard VPN

Um Wireguard-VPNs (Virtual Private Networks) zu nutzen, muss dieser Dienst gestartet werden. Ein Neustart dieses Dienstes beendet alle zur Zeit aktiven Wireguard-Verbindungen.



Der Dienst kann nicht gestartet werden, solange nicht zumindest eine wg-Schnittstelle konfiguriert wurde.

IPSec VPN

Um IPSec-VPNs (Virtual Private Networks) zu nutzen, muss dieser Dienst gestartet werden. Ein Neustart dieses Dienstes beendet alle zur Zeit aktiven IPSec-Verbindungen. Die Gegenstellen werden darüber jedoch benachrichtigt, so dass nach dem Neustart sofort automatisch eine neue Verbindung ausgehandelt werden kann.



Der Dienst kann nicht gestartet werden, solange nicht zumindest eine ipsec-Schnittstelle mit einer zugehörigen Verbindung konfiguriert wurde.

L2TP-Server

Starten Sie diesen Dienst, wenn IPSec-L2TP-Verbindungen genutzt werden sollen. Ein Neustart dieses Dienstes trennt alle aktiven L2TP-Verbindungen.

OpenVPN

Um OpenVPN basierende VPNs (Virtual Private Networks) zu nutzen, muss dieser Dienst gestartet werden. Ein Neustart dieses Dienstes beendet alle zur Zeit aktiven Verbindungen.



Der Dienst kann nicht gestartet werden, solange nicht zumindest eine ovnc- oder ovns-Schnittstelle konfiguriert wurde.

Firewall

Die Firewall des SX-GATE ist immer aktiv. Dieser Dienst kann daher nicht beendet werden. Ein Neustart ist jedoch möglich.

Intrusion Detection

Das Intrusion-Detection-System (IDS) überwacht den Inhalt von Datenpaketen basierend auf einer Signatur-Datenbank. Verdächtigen Pakete werden protokolliert. Das IDS lässt sich je Schnittstelle in der Firewall-Konfiguration aktivieren.

DHCPv4-Server

Der DHCP-Dienst kann dazu genutzt werden, entsprechend konfigurierten Systemen im LAN automatisch die IP-Konfiguration zuzuweisen.

DHCPv4-Relay

Der DHCP-Relay-Dienst nimmt DHCP-Anfragen entgegen und leitet sie an einen DHCP-Server in einem anderen Netzwerk weiter.

DHCPv6-Server

Der DHCP-Dienst kann dazu genutzt werden, entsprechend konfigurierten Systemen im LAN automatisch die IP-Konfiguration zuzuweisen.

12.2-B Server-Dienste

In dieser Maske ist der Status der verschiedensten Server-Dienste zu sehen.

DNS-Server

Dieser Dienst ist erforderlich zur DNS Namens-Auflösung. Clients in internen Netzwerken sollten DNS-Anfragen über diesen Dienst in das Internet weiterleiten lassen. Neben der Nutzung als DNS-Forwarder ist es auch möglich, diesen Dienst zur Verwaltung von Internet-Domains einzusetzen.



Alle Komponenten des SX-GATE, die DNS-Informationen benötigen, wenden sich an diesen Server-Dienst. Im normalen Betrieb muss dieser Dienst daher unbedingt aktiv sein.

Mail-Server

Ein SMTP-Mail-Server wird durch diesen Server-Dienst zur Verfügung gestellt. Interne Clients oder auch interne Mail-Server sollten E-Mails in das Internet über den SMTP-Mail-Server des SX-GATE versenden. Auch für eingehende E-Mails ist nach Möglichkeit dieser Dienst zu nutzen. Der direkte Empfang von Mails mit SMTP ist möglich. Zusammen mit dem Mail-Client wird dieser Dienst auch zur Zustellung von E-Mails genutzt, die der SX-GATE Mail-Client von POP-Servern abrufen. Eingehende E-Mails können in Postfächer des SX-GATE zugestellt oder aber an einen internen Mail-Server weitergeleitet werden.



Für den Versand von System-Nachrichten, die von SX-GATE generiert wurden, wird dieser Dienst nicht benötigt.

POP-/IMAP-Server

Dieser Dienst ermöglicht den Zugriff auf Postfächer, die auf SX-GATE gespeichert sind.



Der Zugriff auf Postfächer ist auch mittels Web-Browser über die SX-GATE Groupware möglich.

Web-Proxy

Die Browser-Kommunikation mit dem Internet sollte über den Web-Proxy des SX-GATE abgewickelt werden. Der Browser ist entsprechend zu konfigurieren.

Reverse-Proxy

Der Reverse-Proxy erlaubt den Zugriff auf Web-Server im LAN und kann zur Last-Verteilung der Zugriffe auf Web-Server in einer DMZ genutzt werden.

SIP-Proxy

Dieser Dienst stellt einen Outbound-Proxy für das Voice-over-IP-Protokoll SIP zur Verfügung.

POP3-/SMTP-Proxy

Über diesen transparenten Proxy können sich Benutzer mit POP3- und SMTP-Servern im Internet verbinden. Der Proxy läuft auf Port 8110.

SOCKS-Proxy

SOCKS ist ein generischer Proxy der seine Dienste auf Port 1080 anbietet.

SSH TCP-Forwarder

Secure-Shell-Clients können authentifizierte und verschlüsselte Kanäle zum TCP-Forwarder öffnen. Durch diese Kanäle lassen sich TCP-Verbindungen zu (meist internen) Servern leiten. Der SSH TCP-Forwarder wird über Port 2222 angesprochen.

HTTP-Server

Ist dieser Server-Dienst gestartet, so stellt SX-GATE einen einfachen Web-Server zur Verfügung. Dieser kann dazu genutzt werden, Dokumente für die internen Netzwerke zur Verfügung zu stellen. Entsprechende Konfiguration vorausgesetzt, ist auch ein weiterer Bereich verfügbar, auf den auch vom Internet aus zugegriffen werden kann.

Windows-Freigaben

Aktivieren Sie diesen Dienst, um den SX-GATE Web-Server bequem via Windows Netzwerk-Freigaben zu pflegen.

NTP-Zeitserver

Der NTP-Zeitserver ermöglicht es anderen Systemen, deren Systemzeit mit der des SX-GATE zu synchronisieren.



Erfolgt die Zeitsynchronisation mit Hilfe der Protokolle time, daytime oder über die Windows-Freigaben, muss dieser Dienst nicht aktiviert werden.

Obwohl dieser Dienst nicht erforderlich ist, um SX-GATEs eigene Systemzeit mit NTP-Servern im Internet zu synchronisieren, sorgt er für eine kontinuierliche Angleichung der Systemzeit wenn er aktiv ist.

SNMP-Server

Der SNMP-Server erlaubt die Überwachung des SX-GATE mit Hilfe des Simple Network Management Protocols. Der Dienst kann im Menü "Module > SNMP-Server" eingerichtet werden.

12.2-C Weitere Server

Die Dienste, die hier angegeben sind, werden oft nur selten kontaktiert. Um System-Ressourcen zu sparen werden diese nur bei Bedarf aufgerufen. Eine Art Meta-Server wacht dazu über die zu diesen Diensten gehörenden Ports und aktiviert den angesprochenen Dienst bei Bedarf automatisch. Legen Sie in dieser Maske fest, welche Dienste zur Verfügung stehen sollen.

Dienste

Dieser Dienst ist verantwortlich für die Verfügbarkeit aller nachfolgenden Server-Anwendungen.



Ist dieser Dienst gestoppt, so steht keiner der folgenden Server mehr zur Verfügung.

FTP-Proxy

Auf TCP-Port 2121 steht ein FTP-Proxy zur Verfügung. Verwenden Sie diesen, wenn mit FTP-Clients auf FTP-Server im Internet zugegriffen werden soll. Die Konfiguration dieses Dienstes erfolgt im Menü "Module > Weitere Proxies > FTP-Proxy".



Dieser Dienst ist nur für "echte" FTP-Clients nutzbar. Der Zugriff auf FTP-Server mit Hilfe eines Web-Browser kann über den Web-Proxy auf TCP-Port 8080 erfolgen.

FTP-Server

Mit FTP können Dateien von und zu SX-GATE übertragen werden. Dies ist jedoch nur bestimmten Benutzern möglich. Nähere Informationen finden Sie unter "Module > FTP-Server".

TFTP-Server

TFTP ist ein sehr einfaches Protokoll um Dateien auszutauschen. Es kennt weder Verschlüsselung noch Authentifizierung. Jeder, der Zugriff auf den TFTP-Port des SX-GATES hat, kann dort Dateien hoch- und herunterladen!



Stellen Sie daher unbedingt sicher, dass nur die Systeme Zugriff auf den TFTP-Port 69 (UDP) erhalten, für die dies notwendig ist. Konfigurieren Sie entsprechende Sperrregeln in der Firewall.

Die Verwaltung von Dateien auf dem TFTP-Server erfolgt mit Hilfe des vordefinierten Benutzers "ftpadmin", den Sie im Menü "Module > FTP-Server" aktivieren können. Nachdem Sie sich per FTP als "ftpadmin" auf dem SX-GATE angemeldet haben, gehen Sie bitte auf die oberste Verzeichnisebene und wechseln Sie von dort in das Verzeichnis "_tftp". Hier können Sie Dateien für den Download bereitstellen und hier finden Sie auch per TFTP hochgeladene Dateien.

Dateien, die per TFTP auf den SX-GATE hochgeladen wurden, können zwar überschrieben, aber nicht per TFTP heruntergeladen werden. Der "ftpadmin" muss bei

einer hochgeladenen Datei zuerst Leserechte für alle erteilen, damit diese auch per TFTP heruntergeladen werden kann.

Time

Über TCP-Port 37 kann die aktuelle Systemzeit des SX-GATE in binärer Form abgerufen werden. Aktivieren Sie diesen Dienst falls Client-Systeme eine Zeitsynchronisation mit dem time-Protokoll gemäß RFC 868 durchführen.

Daytime

Die Systemzeit ist auch auf TCP-Port 13 verfügbar, Hier jedoch in "lesbarer" Form.

12.2-D System-Dienste

In dieser Maske ist der Status einiger System-Dienste zu sehen.

System-Logging

Die meisten Komponenten des SX-GATE nutzen diesen Dienst, um die verschiedensten Informationen, Status- oder Fehlermeldungen zu protokollieren.



Es ist nicht empfehlenswert, diesen Dienst dauerhaft zu deaktivieren. Ursachen für Fehler aber auch sicherheitsrelevante Vorfälle werden in diesem Falle nicht mehr protokolliert und können daher nicht nachvollzogen werden.

Server-Dienst für geplante Aufgaben

Dieser Dienst ist für die zeitgesteuerte Ausführung verschiedenster Funktionen erforderlich (cron). Dazu gehört z.B. die Generierung von Statistiken, die Archivierung von Log-Dateien, das zeitgesteuerte Abholen von E-Mails und auch die Aktualisierung der Virenschanner-Signaturen.



Auch dieser Dienst sollte nicht über einen längeren Zeitraum deaktiviert werden. Verschiedene wichtige Funktionen stehen in diesem Falle nicht mehr zur Verfügung.

Diensteüberwachung

Dieser System Dienst dient zur Überwachung der folgenden Dienste:

- DNS-Server
- Mail-Server
- Web-Proxy
- Reverse-Proxy
- SIP-Proxy
- POP3-/SMTP-Proxy

Beendet sich ein Dienst aus unbekanntem Grund, wird er automatisch vom System neu gestartet.



Es wird lediglich geprüft, ob ein Dienst noch in der Prozessliste aufgeführt ist. Ein Dienst der noch läuft aber seiner Aufgabe nicht mehr nachkommt, wird nicht erkannt.

Fällt ein Dienst mehrfach in einem bestimmten Zeitraum aus, wird der Dienst nicht mehr neu gestartet. Auf einem Cluster Master-Knoten führt dies zu einem Failover bis der Dienst entweder deaktiviert wird oder wieder läuft.

Cluster-Knoten

Dieser Dienst wird für das Clustering (Menü "System > Grundeinstellungen", Tab "Clustering") benötigt.

Mitgliedschaft in Windows Domäne

Mit Hilfe dieses Dienstes kann SX-GATE einer Windows Domäne beitreten. Der Dienst wird derzeit ausschließlich für die NTLM-Authentifizierung des Web-Proxies benötigt.



Um Mitglied einer Windows Domäne werden zu können, muss zunächst ein Computer Konto für SX-GATE angelegt werden. Nutzen Sie dazu am besten den Assistenten "Proxy-Konfiguration".

Apcupsd USV-Client

Wird SX-GATE über ein USV von APC mit Strom versorgt und diese USV mit der Software apcupsd überwacht, kann SX-GATE deren Status abfragen und sich im Bedarfsfall rechtzeitig automatisch abschalten.

Secure-Shell Server (SSH)

Dieser Dienst erlaubt den verschlüsselten Netzwerkzugriff auf die Betriebssystemebene Ihres SX-GATEs. Der Dienst wird in erster Linie vom technischen Support für die Fernwartung genutzt. Sollte der Dienst nicht laufen, wird er durch den Ferwartungs-Assistenten bei Bedarf gestartet. In bestimmten Situationen kann der Dienst jedoch auch für den lokalen Administrator hilfreich sein.



Auf dem Master-Knoten eines SX-GATE Clusters wird der Dienst für die Synchronisation der Konfiguration benötigt.

SX-GATE Konfigurations-Dienst

Die Administrations-Oberfläche des SX-GATE wird von diesem Dienst bereitgestellt. Es ist daher nicht möglich diesen Dienst zu beenden.



Wenn Sie diesen Dienst neu starten erhalten Sie nach dem Abschicken des Befehls in der Regel eine Fehlermeldung. Durch den Neustart kann die Antwort nicht mehr übermittelt werden.

12.3 Benutzerverwaltung

Die Benutzerverwaltung des SX-GATE dient in erster Linie dazu, Benutzer mit Berechtigungen für einzelne Dienste des SX-GATE auszustatten. Dazu dienen die folgenden vier vordefinierten Systemgruppen, die nicht gelöscht werden können: "system-mail", "system-proxy", "system-ras" und "system-admin". Benutzer die diesen Gruppen zugeordnet sind, verfügen über ein persönliches Konto mit Passwort, das den Zugriff auf den zu dieser Systemgruppe gehörigen Dienst ermöglicht.

Die Bedeutung der vordefinierten System-Gruppen im Einzelnen:

system-mail

Die Gruppe "system-mail" enthält alle Benutzer, die über ein Postfach auf dem SX-GATE verfügen. Auf dieses Konto kann z.B. mit POP3, IMAP4 oder der SX-GATE-Groupware zugegriffen werden.



Wird ein Benutzer aus der Gruppe system-mail entfernt, bleibt sein Postfach erhalten und kann weiter genutzt werden, wenn der Benutzer zu einem späteren Zeitpunkt wieder zu dieser Gruppe hinzugefügt wird. Das Postfach wird hingegen gelöscht, wenn der Benutzer vollständig aus der Benutzerverwaltung entfernt wird.

Da jede Gruppe zugleich als Mail-Verteiler fungiert und jeder lokale Benutzer mit Mail-Berechtigung Mitglied der Gruppe "system-mail" sein muss, erreicht eine E-Mail an "system-mail" automatisch alle lokalen Benutzer.



Um diesen Mail-Verteiler unter einem gebräuchlicheren Namen verfügbar zu machen (z.B. "alle") legen Sie bitte eine entsprechende Gruppe an und fügen Sie auf dem Reiter (Tab) "Mail-Einstellungen" unter "Externe Mail-Adressen" den Eintrag "system-mail" hinzu.

system-proxy

Ein Benutzer muss Mitglied dieser Gruppe sein, um Zugriff auf SX-GATE Proxy-Dienste zu erhalten, die Authentifizierung erfordern.

system-admin

Mitgliedern dieser Gruppe ist der Zugriff auf die Administrations-Oberfläche des SX-GATE möglich. Grundsätzlich haben alle Mitglieder Zugriff auf das Menü "Mein Konto". Der Zugriff auf weitere Menüpunkte kann durch den Administrator ermöglicht werden.

system-ras

Bei manchen IPSec-Verbindungen verlangt SX-GATE eine Authentifizierung durch den Benutzer. Diese wird nur von Mitgliedern dieser Gruppe akzeptiert.

12.3.1 Einstellungen

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.3.1-A Active-Directory Anbindung.....	134
12.3.1-B Benutzer- und Gruppenimport.....	136
12.3.1-C Passwortsynchronisation.....	139

12.3.1-A Active-Directory Anbindung

SX-GATE lässt sich mit einem Microsoft Active-Directory verbinden. Diese Funktion kann zum einmaligen Import oder regelmäßigen Abgleich der enthaltenen Benutzer und Gruppen genutzt werden. Leitet der SX-GATE Mail-Server eingehende Mails an einen internen Exchange-Server weiter, kann SX-GATE zudem im Active-Directory die Existenz von Mail-Adressen überprüfen.



SX-GATE greift ausschließlich lesend auf das Active-Directory zu.

Active-Directory Server

Hier legen Sie die IP-Adresse des Active-Directory Servers fest, auf dem die Benutzerdaten gespeichert sind. Dies ist in der Regel die Adresse Ihres Domänen-Controllers.

LDAP-Suchpfad

Geben Sie hier den LDAP-Pfad an, an den sich SX-GATE im Active-Directory binden soll. Alle relevanten Benutzer und Gruppen müssen hierarchisch unterhalb dieses Pfades befinden.

Im einfachsten Fall geben Sie hier lediglich den Namen des Active-Directories an (z.B. ad.example.com). Es kann jedoch auch ein exakter Distinguished Name (DN) angegeben werden wie z.B. "CN=users,DC=ad,DC=example,DC=com" oder "OU=internet-benutzer,DC=ad,DC=example,DC=com".

Benutzername für Suche im Active-Directory

Ist die anonyme Suche im Active-Directory erlaubt, kann dieses Feld leer bleiben. Geben Sie andernfalls den Anmeldenamen eines Benutzers ein, der die

notwendigen Berechtigungen hat (Bind DN). Befinden sich der Benutzer im Active-Directory Container "users", genügt hier die Eingabe des Benutzernamens (z.B. "suchbenutzer"). Andernfalls muss der vollständige DN angegeben werden (z.B. "CN=suchbenutzer,OU=edv,DC=ad,DC=example,DC=com").



Im Microsoft SBS lautet der Standardpfad für Benutzer beispielsweise "cn=suchbenutzer,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=example,DC=com" und muss daher als DN angegeben werden.

Passwort

Ist eine Anmeldung am Active Directory erforderlich, so geben Sie hier bitte das entsprechende Kennwort ein.

SSL Verschlüsselung

Durch Aktivieren dieser Option wird die Kommunikation zwischen SX-GATE und dem Active Directory verschlüsselt.

LDAP-Anbindung prüfen

Sobald zumindest die Adresse des Servers angegeben wurde, können Sie mit Hilfe dieses Schalters die LDAP-Verbindung testen.



Sollten Sie Einstellungen auf dieser Seite verändert haben, so drücken Sie bitte zunächst "Übernehmen".

12.3.1-B Benutzer- und Gruppenimport

Benutzer und Gruppen können aus dem Active-Directory importiert werden. Im Active-Directory ist der Import folgendermaßen vorzubereiten:

- Legen Sie eine Verteiler-Gruppe an (z.B. "internet-benutzer") der nachfolgend alle für SX-GATE relevanten Objekte zugeordnet werden.
- Ordnen Sie dieser Gruppe all die Gruppen zu, die in die SX-GATE Gruppenverwaltung übernommen werden sollen.



Es werden nur unmittelbar zugeordnete Gruppen berücksichtigt. Untergruppen einer zugeordneten Gruppe werden nicht in die Gruppenverwaltung des SX-GATE übernommen.

Üblicherweise werden Sie im Active-Directory auch die Pendants zu den für Sie relevanten System-Gruppen des SX-GATE anlegen und zuordnen.

- Beim Import der so festgelegten Gruppen werden jeder dieser Gruppen all die Benutzer zugeordnet, die im Active-Directory direktes oder indirektes Mitglied der Gruppe sind.



Indirekte Mitglieder werden mittels einer hierarchischen Suche in der Gruppenstruktur unterhalb der gerade bearbeiteten Gruppe ermittelt.

- Aus der Menge aller Benutzer die auf diese Weise ermittelt wurden ergibt sich automatisch, welche Benutzer in der Benutzerverwaltung des SX-GATE angelegt sein müssen.

Was geschieht nun mit Gruppen und Benutzern die auf SX-GATE angelegt sind, für die jedoch im Active-Directory keine Entsprechung zu finden ist? Grundsätzlich macht es dabei keinen Unterschied, ob der betroffene Benutzer bzw. die Gruppe manuell im SX-GATE angelegt wurde oder ob es sich um ein aus dem Active-Directory importiertes Objekt handelt, das nicht länger den zuvor geschilderten Kriterien für den Import entspricht.



Durch den Import wird in der SX-GATE Benutzer- und Gruppenverwaltung kein Objekt vollständig gelöscht um den Verlust von Daten oder Einstellungen zu vermeiden.

- Die Benutzerzuordnung einer SX-GATE System-Gruppe bleibt unverändert, wenn die Gruppe nicht oder nicht mehr mit dem Active-Directory abgeglichen werden soll.
- Einer normalen Gruppe werden alle ihre Mitglieder entzogen. Eine Gruppe kann damit z.B. nach wie vor noch als Mailverteiler für externe Adressen fungieren. Löschen Sie nicht mehr benötigte Gruppen bitte manuell.
- Daraus ergibt sich, dass ein Benutzer nur noch Mitglied von System-Gruppen ist, die nicht im Active-Directory verwaltet werden. Die Mitgliedschaft in allen anderen Gruppen wird beendet. Die vollständige Löschung eines Benutzers muss manuell erfolgen.

Eine Gruppe wird unter ihrem regulären Windows-Namen (Common Name) in den SX-GATE übernommen. Der "Benutzeranmeldename Windows NT 3.5x/4.0" (SAMAccountName) wird hingegen für den Import der Benutzer verwendet. Großbuchstaben werden dabei sowohl bei Benutzern als auch bei Gruppen in Kleinbuchstaben gewandelt.



Benutzer und Gruppen die nicht den Namenskonventionen des SX-GATE entsprechen werden nicht importiert. Der Name eines Benutzers bzw. einer Gruppe muss mit einem Buchstaben beginnen und darf neben Buchstaben aus dem Bereich a-z nur Ziffern, Punkte, Binde- oder Unterstriche enthalten.

Neben der Benutzer- und Gruppenstruktur können auch die Kennwörter der Benutzer an das Active-Directory angeglichen werden. Dazu ist jedoch die Installation einer Bibliothek (DLL) auf dem Windows-Domänen-Controller erforderlich. Nähere Informationen dazu finden Sie auf dem Reiter (Tab) "Passwortsynchronisation".



Ein neu importierter Benutzer bleibt so lange gesperrt, bis der Administrator auf dem SX-GATE ein Kennwort für diesen Benutzer festlegt. Dies gilt nicht wenn die Passwort-DLL im Domänen-Controller installiert ist und für den Benutzer bereits ein Kennwort hinterlegt hat.

Active-Directory SX-GATE-Gruppe

Legen Sie hier die Active-Directory Gruppe fest unter der alle für SX-GATE relevanten Objekte zu finden sind. Befinden sich alle relevanten Benutzer und Gruppen im Active-Directory Container "users", genügt hier die

Eingabe des Gruppennamens (z.B. "internet-benutzer"). Andernfalls muss der vollständige Distinguished Name (DN) angegeben werden (z.B. "CN=internet-benutzer,OU=edv,DC=ad,DC=example,DC=com").



Im Microsoft SBS lautet der Standardpfad für Gruppen beispielsweise "cn=internet-benutzer,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=example,DC=com" und muss daher als DN angegeben werden.

Ordnen Sie dieser Gruppe im Active-Directory bitte ausschließlich Gruppen zu. Diese werden später als SX-GATE Gruppe importiert. Die unterhalb dieser Gruppenebene gefunden Benutzerobjekte werden schließlich als SX-GATE Benutzer importiert. Dabei dürfen die Benutzer auch in Untergruppen enthalten sein, wobei diese Untergruppen nicht als Gruppe importiert werden.



Benutzer-Objekte, die im Active-Directory der hier angegebenen Gruppe als direkte Mitglieder zugeordnet wurden, spielen beim Import keine Rolle.

Zeitintervall für automatischen Import

Über diesen Parameter wird der automatische Import deaktiviert oder der zeitliche Abstand zwischen zwei Aktualisierungen eingestellt.

Import-Protokoll senden

Wählen Sie hier aus unter welchen Umständen ein Protokoll des Imports gesendet werden soll. Dieses wird per E-Mail an den Administrator zugestellt.

Import testen

Mit diesem Schalter wird geprüft, ob im Active-Directory die erwartete Benutzer- und Gruppenstruktur vorgefunden wird.



Sollten Sie Einstellungen auf dieser Seite verändert haben, so drücken Sie bitte zunächst "Übernehmen".

Jetzt importieren

Der Import der Benutzer und Gruppen kann über diesen Schalter gestartet werden. Sofern im Domänen-Controllers die SX-GATE-Passwort-DLL installiert ist, werden auch die Kennwörter aktualisiert. Ein Protokoll des Vorgangs wird in einem neuen Browser-Fenster angezeigt.



Sollten Sie Einstellungen auf dieser Seite verändert haben, so drücken Sie bitte zunächst "Übernehmen".

12.3.1-C Passwortsynchronisation

Microsoft's Active-Directory erlaubt den Zugriff auf die gespeicherten Kennwörter seiner Benutzer nicht. Um dennoch die Kennwörter des SX-GATE mit dem Active-Directory abgleichen zu können, steht hier eine Bibliothek (DLL) zur Verfügung, die auf dem Windows-Domänen-Controller installiert werden muss. Die Bibliothek klinkt sich in den Prozess der Kennwort-Änderung ein. Immer wenn ein Benutzer sein Windows-Passwort ändert, wird das neue Kennwort dieser Bibliothek mitgeteilt. Diese berechnet daraus den Einweg-Hash wie er vom SX-GATE für die Authentifizierung benötigt wird und speichert diesen Wert im Active-Directory ab. Beim Import wird das so gespeicherte Kennwort automatisch in die Benutzerverwaltung des SX-GATE übernommen.



Ein Einweg-Hash lässt keine unmittelbaren Rückschlüsse auf das ursprüngliche Passwort zu.

Um die DLL zu installieren laden Sie bitte das Setup herunter und starten es. Starten Sie den Domänen-Controller neu um die Bibliothek zu aktivieren.

12.3.2 Benutzer

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Anmeldename

Legen Sie bitte hier den Anmeldennamen (Login) des Benutzers fest.



Neben Kleinbuchstaben und Ziffern sind im Anmeldenamen nur der Bindestrich (-), der Punkt (.) und der Unterstrich (_) zulässig. Der Login muss mit einem Kleinbuchstaben beginnen. Insbesondere die Verwendung von Umlauten sowie Leerzeichen im Anmeldenamen ist nicht erlaubt.

Vorname

Hier können Sie den Vornamen des Benutzers eingeben. Eine Eintragung ist nicht notwendig.

Nachname

Optional kann hier der Nachname des Benutzers angegeben werden.

Passwort

Vergeben Sie hier das Passwort für den neuen Benutzer.



Zunächst ist es einem neuen Benutzer nicht möglich, auf irgendeinen SX-GATE-Dienst zuzugreifen, der ein Passwort erfordert. Fügen Sie den Benutzer zu System-Gruppen hinzu, um diesen mit entsprechenden Berechtigungen auszustatten.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.3.2-A Gruppen.....	141
12.3.2-B Passwort.....	142
12.3.2-C Mail-Administration.....	144
12.3.2-D Mail-Weiterleitung.....	145
12.3.2-E SPAM-Filter.....	146
12.3.2-F SPAM Bewertung.....	148
12.3.2-G SPAM Adressen.....	150
12.3.2-H Abwesenheit.....	150
12.3.2-I Mail-Ordner.....	152
12.3.2-J SOCKS-Proxy.....	152
12.3.2-K RDP Web-Client.....	153
12.3.2-L VNC Web-Client.....	157
12.3.2-M SSH Web-Client.....	159
12.3.2-N SSH TCP Weiterleitung.....	160
12.3.2-O RAS Einstellungen.....	161
12.3.2-P Docklets.....	163
12.3.2-Q Menü Statistiken	163
12.3.2-R Menü Monitoring	164
12.3.2-S Menü Definitionen	164
12.3.2-T Menü System	164
12.3.2-U Menü Assistenten	164
12.3.2-V Menü Module	165
12.3.2-W Anmeldeoptionen.....	165
12.3.2-X Benutzerdaten.....	165

12.3.2-A Gruppen

In dieser Eingabemaske sehen Sie die dem Benutzer zugeordneten bzw. die noch verfügbaren Gruppen. Um einen Benutzer gleichzeitig in mehrere Gruppen aufzunehmen bzw. aus mehreren Gruppen zu entfernen, können Sie in der jeweiligen Liste mehrere Einträge auswählen. Halten Sie dazu während der Auswahl die STRG-Taste gedrückt.



Bei einer Neuanlage eines Benutzers ist dieser zunächst keiner Gruppe zugeordnet. Insbesondere sind also auch noch keinerlei Konten für den Benutzer angelegt, da er dazu in entsprechende System-Gruppen aufgenommen werden muss.

Die Bedeutung der System-Gruppen im Einzelnen:

system-admin

Mitglieder dieser Gruppe haben Zugriff auf die Administrations-Oberfläche des SX-GATE. Wird der entsprechende Benutzer nicht mit zusätzlichen Rechten ausgestattet, so beschränkt sich die Sichtbarkeit der Oberfläche jedoch auf das Menü "Mein Konto".

system-mail

Der Benutzer verfügt über ein Postfach auf SX-GATE. Mit Login und Passwort kann der Benutzer über POP3, IMAP4 oder Groupware auf dieses Postfach zugreifen.

Optional kann dem Benutzer die Berechtigung erteilt werden, sich mit seinen Zugangsdaten für die Benutzung des SX-GATE Mail-Relay-Servers anzumelden. Dies ist dann erforderlich, wenn der SX-GATE Mail-Server so konfiguriert ist, dass Mail-Versand in das Internet nur nach erfolgreicher Benutzeranmeldung mit SMTP-Auth erlaubt ist.

system-proxy

Manche der Proxies des SX-GATE können so eingestellt werden, dass Zugriffe nur nach erfolgreicher Benutzeranmeldung möglich sind. Durch Zuordnung zu dieser Gruppe erhält ein Benutzer die entsprechende Berechtigung.

system-ras

Mitglieder dieser Gruppe können sich bei IPsec-XAuth- und IPsec-L2TP-Verbindungen am SX-GATE authentifizieren.



Der Benutzer "admin" ist stets Mitglied der Gruppen "system-mail" und "system-admin". Daher werden diese beiden Gruppen beim Benutzer "admin" nicht angezeigt.

12.3.2-B Passwort

SX-GATE unterscheidet zwischen zwei Arten von Passwörtern. Das Benutzer-Passwort wird jedem Benutzer bereits beim Anlegen zugeteilt. Dieses Passwort kann vom Benutzer selbst jederzeit unter "Mein Konto > Passwort ändern" geändert werden. Voraussetzung dafür ist, dass der Benutzer Mitglied der Gruppe "system-admin" ist und daher Zugriff auf die Benutzeroberfläche des SX-GATE hat.

Je System-Gruppe kann der Administrator jedoch auch ein festes Kennwort vergeben. Dieses Kennwort kann nur in dieser Maske geändert werden, was Administratoren vorbehalten ist.

Benutzer-Passwort zurücksetzen

Mit dieser Funktion können Sie das Benutzer-Passwort ändern. Von der Änderung des Kennwortes sind alle Zugänge des Benutzers betroffen für die kein festes Passwort konfiguriert wurde.

Einmal-Passwörter

Aktivieren Sie Einmal-Passwörter für diesen Benutzer indem Sie einen Schlüssel setzen. Löschen Sie den Schlüssel um Einmal-Passwörter zu deaktivieren.



Es kommen zeitbasierte Einmal-Passwörter (TOTP) mit 6 Stellen, 30 Sekunden Gültigkeitsdauer, berechnet mit SHA1 zum Einsatz.

Festes Passwort für system-admin

Hier können Sie für den gewählten Benutzer ein festes Kennwort für den Zugriff auf die Administrations-Oberfläche des SX-GATE setzen oder wieder deaktivieren.

Festes Passwort für system-mail

Mit Hilfe dieser Funktion können Sie für den gewählten Benutzer ein festes Kennwort für den Zugriff auf E-Mail Funktionen setzen oder wieder deaktivieren. Betroffen sind der Zugriff auf den POP3-, IMAP4- und Groupware-Server des SX-GATE sowie die SMTP-Auth Anmeldung am Mail-Relay-Server des SX-GATE.



Nutzen Sie diese Funktion, wenn die Benutzer das Kennwort für den Zugriff auf Ihr Mail-Konto nicht selbst verwalten. Dies ist z.B. der Fall wenn die Mails durch einen zentralen Mail-Server abgerufen werden.

Festes Passwort für system-proxy

Hier können Sie für den gewählten Benutzer ein festes Kennwort für den Zugriff auf Proxies setzen oder wieder deaktivieren.

Festes Passwort für system-ras

Hier können Sie für den gewählten Benutzer ein festes Kennwort für den RAS-Zugriff setzen oder wieder deaktivieren.

12.3.2-C Mail-Administration

Weitere Mail-Verteilkennungen (Aliase)

Die E-Mail-Adresse eines Benutzers ergibt sich automatisch aus dessen Anmeldenamen (Login). Um einem Benutzer weitere E-Mail-Adressen zuzuordnen, können Sie hier die entsprechenden Verteilkennungen (local part) eintragen. Darunter ist der Teil der E-Mail-Adresse vor dem "@" zu verstehen. Damit also z.B. der Benutzer mit dem Login "mustermann" nicht nur unter der Adresse "mustermann@example.com" sondern auch als "hans.mustermann@example.com" erreichbar ist, müsste "hans.mustermann" in die Liste aufgenommen werden.



Ist bei mehreren Benutzern der selbe Alias eingetragen, so erhalten alle Benutzer ein Exemplar der entsprechend adressierten E-Mails. Wird als Alias der Name einer SX-GATE Gruppe hinzugefügt, so erhält der Benutzer entsprechend ein Exemplar der an die Gruppe adressierten Mails. Theoretisch lassen sich mit Hilfe von Aliasen auch Mail-Verteiler erzeugen. Aus Gründen der Übersichtlichkeit sollten Sie jedoch Aliase nur für Adressen verwenden, die fest mit dem Benutzer verknüpft sind. Definieren Sie entsprechende Gruppen, um Verteiler oder Funktionen wie z.B. "vertrieb" und "hausmeister" abzubilden.

S/MIME-Schlüssel

Sofern Sie SX-GATE als E-Mail-Verschlüsselungs-Gateway verwenden, können Sie hier die S/MIME-Schlüssel des jeweiligen lokalen Benutzers auswählen. Die Schlüssel werden im Menü System > Zertifikatsverwaltung > Schlüsselbund" administriert.



Beachten Sie bitte den Hinweis zur Erneuerung ablaufender Zertifikate weiter unten.

Wählen Sie diese Konfiguration, wenn die Mail-Programme der Benutzer direkt mit dem SX-GATE Mail-Server kommunizieren und sich am SX-GATE anmelden können.



Wenn der Versand über einen internen Mail-Server erfolgt, werden die Zertifikate üblicherweise benutzerunabhängig im Menü "Module > Mail-Server > S/MIME-Gateway" konfiguriert.

Ausgehende E-Mails werden signiert, sofern der Absender (From- oder Sender-Header) zur E-Mail-Adresse im Zertifikat passt und die E-Mail nicht bereits signiert oder

verschlüsselt ist. Um die hier referenzierten Zertifikate nutzen zu können, muss sich der Versender zusätzlich authentifizieren (SMTP Auth).

Verschlüsselt empfangene E-Mails werden automatisch entschlüsselt, wenn SX-GATE über einen passenden Schlüssel verfügt und die Empfänger-Adresse zur E-Mail-Adresse im Zertifikat passt. Beim Entschlüsseln wird keinerlei Bezug zum Benutzerkonto hergestellt. Streng genommen spielt es daher keine Rolle, in welchem Konto der Schlüssel hinterlegt ist. Lediglich die Empfänger-Adressen laut SMTP-Protokoll sind entscheidend.



Wenn Sie einen Schlüssel aus der Liste entfernen, kann SX-GATE damit verschlüsselte E-Mails nicht mehr entschlüsseln. Diese E-Mails werden dann in verschlüsselter Form zugestellt. Sollte der Schlüssel bereits vollständig vernichtet worden sein, ist eine Entschlüsselung auch nachträglich nicht mehr möglich.

In der Übergangszeit nach der Erneuerung eines Zertifikats werden üblicherweise noch über einen längeren Zeitraum E-Mails empfangen, die mit dem alten Zertifikat verschlüsselt wurden. Dies kann selbst dann noch vorkommen, wenn das alte Zertifikat bereits abgelaufen ist. SX-GATE unterstützt Sie in dieser Übergangsphase wie folgt: Wenn Sie im Menü "System > Zertifikatsverwaltung > Schlüsselbund" ein Schlüsselpaar erneuern, wird das vorherige gesichert. Das S/MIME-Gateway nutzt dann automatisch das alte Schlüsselpaar weiterhin zum Entschlüsseln eingehender Mails, während das aktuelle Schlüsselpaar sowohl zum Entschlüsseln als auch zum Signieren genutzt wird. Steht also ein Zertifikat zur Erneuerung an, dann erneuern Sie es bitte im bestehenden Eintrag unter "Schlüsselbund". Fügen Sie keinen neuen Eintrag hinzu. Auch die S/MIME-Gateway-Konfiguration muss nicht angepasst werden.



Es wird immer nur das zuletzt genutzte Schlüsselpaar gesichert, nicht etwa mehrere Generationen.

12.3.2-D Mail-Weiterleitung

Die Einstellungen in diesem Bereich können auch vom Benutzer selbst über das Menü "Mein Konto > E-Mail Einstellungen" geändert werden. Um Zugriff auf dieses Menü zu haben muss der Benutzer Mitglied der Gruppe "system-admin" sein.

E-Mail weiterleiten an

In diesem Bereich können E-Mails des ausgewählten Benutzers an andere interne und externe Adressen weitergeleitet werden. Es können beliebig viele Empfänger auf diese Weise angegeben werden. Diese erhalten dann alle ein Exemplar der Mails für den ausgewählten Benutzer.

Benutzer behält Kopie weitergeleiteter E-Mails

Werden die E-Mails des Benutzers an andere Adressen weitergeleitet, so können Sie mit Hilfe dieses Schalters steuern, ob stets auch ein Exemplar der E-Mails in das Postfach des Benutzers zugestellt werden soll. Ist dieser Schalter nicht aktiviert, so werden keinerlei E-Mails mehr in das Postfach zugestellt sobald eine Weiterleitung aktiv ist.



Solange keine Weiterleitung eingetragen ist, hat dieser Schalter keine Funktion.

12.3.2-E SPAM-Filter

Die Einstellungen in diesem Bereich können auch vom Benutzer selbst über das Menü "Mein Konto > E-Mail Einstellungen" geändert werden. Um Zugriff auf dieses Menü zu haben muss der Benutzer Mitglied der Gruppe "system-admin" sein.

Wenn mindestens einer der Schwellwerte aktiviert ist, müssen alle eingehenden E-Mails, die in das Postfach des ausgewählten Benutzers zugestellt werden, einen SPAM-Mail-Filter passieren. Unter einer SPAM-Mail versteht man eine unerwünschte Werbe-Mail mit meist dubioser Herkunft.

Der SPAM-Mail-Filter des SX-GATE klassifiziert automatisch den Inhalt von E-Mails anhand typischer Phrasen oder anderer Merkmale die auf eine unerwünschte Werbe-Mail (SPAM-Mail) zutreffen. Dazu ist im SX-GATE eine Datenbank mit Kriterien enthalten, die mit einem Punktesystem bewertet werden. Das erreichte Punkteergebnis ermöglicht das Filtern von E-Mails. Alle Merkmale, die auf eine SPAM-Mail hindeuten, erhöhen den Punktestand, während für Merkmale die auf eine reguläre Mail hindeuten wieder Punkte abgezogen werden. Je höher das Bewertungsergebnis, umso wahrscheinlicher handelt es sich um eine SPAM-Mail.



E-Mails mit einer Größe von mehr als 1MB werden vom SPAM-Mail-Filter nicht klassifiziert um Ressourcen zu schonen. Dies stellt jedoch keine Beeinträchtigung dar, da SPAM-Mails typischerweise kleiner sind.

Jede untersuchte E-Mail wird vom SPAM-Mail-Filter um Kopfzeilen (Header) erweitert. Der "X-Spam-Status" zeigt den erreichten Punktwert (hits=...) sowie die Kurznamen der Merkmale, die zu diesem Punktestand geführt haben (tests=...). Dies ermöglicht es dem Empfänger, das Resultat des SPAM-Filters zu überprüfen. Die Kopfzeile "X-Spam-Level" enthält je ein "x" pro vollem erreichten Punkt (z.B. "X-Spam-Level: xxx" bei einer Punktezahl zwischen 3.00 und 3.99). Dieser Header ist bestens geeignet, um E-Mails mit Hilfe Ihres Mail-Programms automatisch zu sortieren.



Bei den meisten Mail-Programmen werden im Normalfall nur die wichtigsten Kopfzeilen angezeigt. Die weiteren Header sind aber in der Regel über einen entsprechenden Menüpunkt zugänglich.

E-Mail als SPAM markieren bei mehr als

Überschreitet der Punktwert einer E-Mail bei deren Klassifizierung diesen Schwellwert, so wird die E-Mail als SPAM-Mail markiert. Dabei wird dem Betreff der Text "***** SPAM *****" sowie die erreichten SPAM-Bewertungspunkte vorangestellt.

Markierte Mails zustellen in

Auf Wunsch können als SPAM markierte E-Mails in einen separaten SPAM-Ordner zugestellt werden. Dieser ist mit SX-GATEs Groupware oder über den IMAP-Server (Ordner Mail/SPAM) erreichbar. Via POP3 kann der SPAM-Ordner nicht ausgelesen werden.

SPAM/HAM löschen nach

Nach der angegebenen Anzahl von Tagen werden Mails automatisch aus den Ordnern "SPAM" bzw. "HAM" gelöscht.



Diese Funktion ist unabhängig davon, ob markierte Mails automatisch im SPAM-Ordner abgelegt werden oder nicht. Der SPAM-Ordner kann also auch von Hand angelegt und befüllt werden.

E-Mail kommentarlos verwerfen bei mehr als

Beim Überschreiten des hier eingestellten Schwellwerts wird die betroffene E-Mail automatisch verworfen. Es erfolgt weder eine Benachrichtigung noch lässt sich eine so gelöschte E-Mail wiederherstellen. Die E-Mail ist unwiederbringlich verloren! Wenn Sie sichergehen wollen, dass keine gewünschte E-Mail verloren geht, sollten Sie diese Option nicht aktivieren. Nutzen Sie stattdessen den Schwellwert "E-Mail als SPAM markieren bei mehr als" zusammen mit den Möglichkeiten Ihres Mail-Programms zur automatischen Sortierung von E-Mails basierend auf den Kopfzeilen.



Um den Verlust von wichtigen E-Mails zu vermeiden, sollten Sie bei der Konfiguration dieser Einstellung sehr vorsichtig sein. Stellen Sie lieber einen zu hohen als einen zu niedrigen Wert ein. Bitte beachten Sie, dass das automatische Löschen von E-Mails durch Vorschriften oder Gesetze mit bestimmten Auflagen verbunden oder sogar verboten sein kann.

12.3.2-F SPAM Bewertung

Die Einstellungen in diesem Bereich können auch vom Benutzer selbst über das Menü "Mein Konto > E-Mail Einstellungen" geändert werden. Um Zugriff auf dieses Menü zu haben muss der Benutzer Mitglied der Gruppe "system-admin" sein.

Benutzerdefinierte SPAM-Regeln

Die SPAM-Prüfung kann in diesem Bereich durch eigene Regeln erweitert werden. Dazu ist zunächst festzulegen, welcher Teil der E-Mail geprüft werden soll. Wird das entsprechende Suchmuster gefunden, so wird die festgelegte Punktzahl bei der Berechnung der SPAM-Wahrscheinlichkeit verbucht.

Für folgende Bereiche kann eine SPAM-Filter-Regel definiert werden:

Betreff

Das Suchmuster wird im Betreff der E-Mail (Subject-Header) gesucht.

Absender

Hier wird der Absender (From-Header) geprüft.

Empfänger

In dieser Einstellung wird der Empfänger (To-Header) ausgewertet.

Kopfzeilen

Hiermit können beliebige Kopfzeilen (Header) ausgewertet werden.

Text

Diese Option bietet die Möglichkeit, den Nachrichten-Text einschließlich des Betreffs zu durchsuchen, also den eigentlichen Inhalt der Mail.

HTML Quelltext

Wie vor, jedoch bei E-Mails im HTML-Format inklusive der HTML-Tags.

Web-Adressen

Prüft Web-Adressen, die als Text oder als HTML-Link im Betreff oder im Text der Nachricht gefunden werden.

Regel

Diese Einstellung unterscheidet sich von den vorherigen. Sie ermöglicht es, die im SX-GATE vordefinierten Regelsätze neu zu bewerten. Entsprechend wird hier auch kein Suchmuster angegeben, sondern die interne ID der Regel. Die ID

zusammen mit der ursprünglichen Bewertung ist jeweils in der Inhalts-Analyse von E-Mails enthalten, die als SPAM markiert wurden (z.B. "HTML_MESSAGE" oder "FORGED_MUA_OUTLOOK").



Bei Aktualisierung der vordefinierten Regelsätze können sich einzelne ID's ändern. Es erfolgt dabei keine Anpassung der hier angegebenen Regeln.

Bei der Angabe eines Suchmusters ("Kriterium") wird die Groß- und Kleinschreibung grundsätzlich nicht beachtet. Beginnt bzw. endet das Suchmuster mit einem Buchstaben oder einer Ziffer, muss das Suchmuster am Beginn bzw. Ende eines Wortes stehen. Das Suchmuster "all" liefert folglich bei "Hallo" keinen Treffer, bei "Das All!" hingegen schon.

Bestimmte Zeichen haben eine Sonderbedeutung:

* (Stern)

Steht für eine Folge beliebiger Zeichen. Diese kann auch komplett fehlen, also sozusagen aus 0 Zeichen bestehen. Das Suchen nach beliebigen Zeichenketten in beliebiger Länge erhöht den Ressourcen-Bedarf deutlich. Von daher trifft ein Stern maximal auf eine Kette aus 30 Zeichen zu. Das Suchmuster "a*d" findet so z.B. "ad", "a_d" und "abcd". Nutzen Sie den Stern auch, um Zeichenketten innerhalb eines Wortes zu suchen. So liefert das Suchmuster "*all*" bei "Hallo" einen Treffer.

? (Fragezeichen)

Dies steht für genau ein beliebiges Zeichen. Wird beispielsweise "a?d" angegeben, so ist "a_d" ein Treffer. Nicht gefunden wird "ad" oder "abcd".

_ (Unterstrich)

Der Unterstrich steht für eine beliebige Anzahl sogenannter "Whitespace-Character". Dies umfasst Leerzeichen, Tabulatoren und Zeilenumbrüche. Im Beispiel findet "a_d" zwar "a d", nicht jedoch "ad" oder "a_d".

Behalten Sie bitte bei der Auswahl des zugeordneten Punktwertes die eingestellten Schwellwerte im Auge. Wählen Sie für Kriterien die auf eine SPAM-Mail hindeuten einen positiven Wert. Ein negativer Wert verringert die Wahrscheinlichkeit, dass eine E-Mail als SPAM klassifiziert wird.

Englischsprachige E-Mails sind potentiell SPAM

Der größte Teil aller SPAM-Mails sind in englischer Sprache verfasst. Ist dieser Schalter aktiviert, so erhalten alle englischsprachigen E-Mails einen Aufschlag auf die SPAM-Bewertung. Die Wahrscheinlichkeit, dass die SPAM-Bewertung einer englischen E-Mail den konfigurierten SPAM-Filter-Schwellwert erreicht wird dadurch deutlich erhöht.

12.3.2-G SPAM Adressen

SPAM-Filter umgehen für folgende Absenderadressen und -domains

Um fälschlicherweise als SPAM identifizierte E-Mails zukünftig zu schützen, lässt sich hier eine Liste von einzelnen Absenderadressen hinterlegen, die den SPAM-Filter passieren dürfen. Passt der Absender einer eingehenden E-Mail zu einem Eintrag in dieser Liste, so erhält die E-Mail einen Abzug von 100 Punkten auf die automatische SPAM-Bewertung und wird so nicht von den Schwellwerten abgefangen.



Im Menü "Module > Mail-Server > SPAM/Virus/Malware" lässt sich eine benutzerübergreifende Positiv-Liste definieren.

Fügen Sie eine vollständige E-Mail-Adresse hinzu (z.B. benutzer@example.com), um E-Mails von dieser Adresse zukünftig nicht auszufiltern. Geben Sie alternativ lediglich den Domain-Teil der E-Mail-Adresse an (z.B. example.com), damit alle Adressen in dieser Domain den SPAM-Filter passieren dürfen.

Bekannte SPAM Absenderadressen und -domains

Empfängt ein Benutzer immer wieder vom selben Absender SPAM-Mails, die durch den SPAM-Mail-Filter nicht erkannt wurden, so können Sie den Absender zu dieser Liste hinzufügen. Passt der Absender einer eingehenden E-Mail zu einem Eintrag in dieser Liste, so erhält die E-Mail einen Aufschlag von 100 Punkten auf die automatische SPAM-Bewertung und wird so vom SPAM-Filter abgefangen.



Im Menü "Module > Mail-Server > SMTP Einstellungen" lässt sich benutzerübergreifende der Empfang von bestimmten Mails sperren.

Fügen Sie eine vollständige E-Mail-Adresse hinzu (z.B. benutzer@example.com), um E-Mails von dieser Adresse zukünftig auszufiltern. Geben Sie alternativ lediglich den Domain-Teil der E-Mail-Adresse an (z.B. example.com), damit die E-Mails aller Absender aus dieser Domain vom SPAM-Filter abgefangen werden.

12.3.2-H Abwesenheit

Auf diesem Reiter lässt sich das Versenden automatischer Antwort-Mails sowie eine zeitlich begrenzte Mail-Weiterleitung für das Postfach des Benutzers konfigurieren.

Die aktivierten Aktionen werden bei jeder E-Mail ausgeführt, die in das Postfach des Benutzers zugestellt wird. Dies betrifft insbesondere auch E-Mails, die nicht an den

Benutzer persönlich, sondern an einen Verteiler (Gruppe) adressiert waren dem der Benutzer angehört.



Sofern E-Mails grundsätzlich an andere Adressen weitergeleitet werden (siehe Reiter "Mail-Weiterleitung"), sind die Einstellungen nur dann wirksam, wenn die Option "Benutzer behält Kopie weitergeleiteter E-Mails" gewählt wurde.

Die Einstellungen in diesem Bereich können auch vom Benutzer selbst über das Menü "Mein Konto > E-Mail Einstellungen" geändert werden. Um Zugriff auf dieses Menü zu haben, muss der Benutzer Mitglied der Gruppe "system-admin" sein.

Abwesenheits-Schaltung

Mit diesem Schalter werden die gewünschten Aktionen ausgewählt.

Zeitraum ab

Die gewählten Aktionen können ab sofort oder ab dem eingetragenen Datum aktiv werden. Geben Sie das Datum bitte im Format JJJJ-MM-TT HH:MM ein.

Zeitraum bis

Auf Wunsch gilt die Abwesenheits-Schaltung nur bis zu einem bestimmten Datum. Verwenden Sie bitte auch hier das Datums-Format JJJJ-MM-TT HH:MM.

E-Mails weiterleiten an

Auf Wunsch werden im gewählten Zeitraum alle Mails an eine andere Adresse weitergeleitet.

Kopie von weitergeleiteten Emails behalten

Mit Hilfe dieses Schalters legen Sie fest, ob dem Benutzer trotz Weiterleitung eine Kopie jeder Mail zugestellt wird.

Abwesenheits-Nachricht

Es ist möglich, auf alle eingehenden E-Mails automatisch eine Antwort generieren zu lassen. Typische Anwendung ist der Versand von Abwesenheits-Notizen. Die Funktion kann aber z.B. auch genutzt werden, um den Eingang der E-Mail zu bestätigen.



Die Absenderadresse der Antwort-Mail lässt sich mit Hilfe der Option "Primäre Mail-Adresse des Benutzers" auf dem Reiter (Tab) "Benutzerdaten" festlegen.



Für E-Mails, die als SPAM markiert wurden, wird grundsätzlich keine Antwort generiert.

Der Inhalt der automatischen Antwort ist ein beliebiger Text der in diesem Eingabefeld festgelegt wird. Ist kein Text hinterlegt, so wird auch keine automatische Antwort gesendet.

12.3.2-I Mail-Ordner

E-Mails können automatisch anhand bestimmter Kriterien auf Unterordner des Benutzer-Postfaches verteilt werden. Per IMAP oder Groupware kann auf diese Unterordner zugegriffen werden. Der Zugriff auf Unterordner per POP3 ist nicht möglich.

12.3.2-J SOCKS-Proxy

SOCKS bietet einen generischen Proxy-Dienst für Anwendungen, die sich nicht mit Hilfe von anderen Proxies oder von NAT-Firewall-Regeln mit dem Internet verbinden können. Unterstützt werden die Protokolle SOCKS4 und SOCKS5. Mit Hilfe von SOCKS-Wrapper-Anwendungen können nahezu alle netzwerkfähigen Programme den SOCKS-Proxy nutzen. Manche Anwendungen beinhalten sogar schon von sich aus einen SOCKS-Client.



Für Protokolle wie HTTP, HTTPS, FTP usw. für die SX-GATE einen speziellen Proxy-Dienst zur Verfügung stellt, sollte SOCKS nicht verwendet werden. Spezielle Proxy-Dienste können die jeweiligen Anforderungen besser abbilden als ein generischer Proxy-Dienst.



Daten, die über den SOCKS-Proxy übertragen werden unterliegen keinerlei Virenschutz. Ebenso werden übertragene Protokolle nicht hinsichtlich ihrer Korrektheit überprüft.

In der Grundeinstellung sind keinerlei Verbindungen über SOCKS-Proxy erlaubt. Verbindungen müssen explizit freigegeben werden. Auch im Menü "Module > Weitere Proxies > SOCKS-Proxy" können SOCKS-Regeln eingetragen werden. Diese gelten für alle SOCKS-fähigen Anwendungen und können ohne weiteres genutzt werden. Die in dieser Maske konfigurierten Regeln sind benutzerspezifisch. Eine Anmeldung mit Benutzername und Kennwort ist erforderlich.



Mit Hilfe der benutzerspezifischen SOCKS-Regeln lassen sich konzeptuell "benutzerbezogene Firewall-Regeln" realisieren.

Benutzerspezifische Regeln

Die hier konfigurierten Regeln beschreiben, welche Verbindungen der aktuell gewählte Benutzer nach Authentifizierung aufbauen darf.

Wählen Sie zunächst das gewünschte Protokoll aus. Optional können Sie durch Angabe einer einzelnen IP-Adresse bzw. eines Netzwerks mit zugehöriger Netzmaske die Freigabe auf bestimmte Clients oder Server beschränken.



Protokoll-Definitionen werden im Menü "Definitionen > Protokolle" vorgenommen.



Protokoll-Signaturen die sich weder auf UDP noch auf TCP beziehen werden ignoriert.

12.3.2-K RDP Web-Client

Der auf HTML5 basierende RDP Web-Client ermöglicht den Zugriff auf Windows Rechner über jeden HTML5 fähigen Browser. Auf dem Client wird dafür weder eine spezielle Software noch ein Plugin benötigt.



Die Verbindung zum Web-Client erfolgt über SX-GATEs Reverse-Proxy, der entsprechend konfiguriert sein muss. Der Zugriff erfolgt über den URL-Pfad "/webclient" (z.B. <https://SX-GATE/webclient>).



Änderungen an der Konfiguration werden erst wirksam, wenn sich der Benutzer neu am Web-Client anmeldet. Das Öffnen einer neuen RDP-Sitzung ist nicht ausreichend.

Damit diese Einstellungen angezeigt werden, muss die Web-Client App installiert und der Benutzer Mitglied der Gruppe "system-ras" sein.

Farbtiefe

Hier geben Sie die genutzte Farbtiefe in Bits Per Pixel an. Eine geringere Farbtiefe reduziert die übertragene Datenmenge.

Resize Methode

Die Methode, die zur Aktualisierung des RDP-Servers verwendet werden soll, wenn sich die Breite oder Höhe der Client-Anzeige ändert. Wenn sie auf Keine gesetzt ist, wird keine Aktion ausgeführt, wenn sich die Größe der Client-Anzeige ändert.

Verwendet den mit RDP 8.1 hinzugefügten "Display Update" Kanal, um dem Server zu signalisieren, wenn sich die Anzeigegröße des Clients geändert hat.

Wenn Reconnect gesetzt ist wird die RDP-Sitzung automatisch getrennt, wenn sich die Größe des Client-Displays geändert hat, und die Verbindung wird mit der neuen Größe wieder hergestellt.

Zwischenablage

Mit diesem Schalter können Sie das Verhalten der Zwischenablage im Web-Client festlegen.



Diese Option erfordert mind. Version 1.2.0-1 des Web-Clients.

Dateiübertragung

Ist die "Dateiübertragung" aktiv, wird ein Verzeichnis des SX-GATEs in der RDP-Sitzung zur Verfügung gestellt, über das ein Datenaustausch zwischen RDP-Server und Browser in beide Richtungen möglich ist. Auf dem Server wird das Verzeichnis als Netzwerkordner eingebunden. Auf Seiten des Browsers erhalten Sie Zugriff auf den SX-GATE-Ordner indem Sie die Menüleiste des Web-Clients einblenden.



Die Menüleiste des Web-Clients wird mit der Tastenkombination "Strg-Alt-Umschalttaste" geöffnet und geschlossen.



Die Optionen "Nur Download " und "Nur Upload" erfordern mind. Version 1.2.0-1 des Web-Clients.

Drucken

Wenn Sie "Drucken" aktivieren, wird in der RDP-Sitzung ein virtueller Drucker zur Verfügung gestellt, mit dessen Hilfe sich Dokumente vom Server an den Client

übermitteln lassen. Ein direkter Ausdruck ist im Web-Browser leider nicht möglich, weshalb der Browser die Ausdrücke als Download im PDF-Format zur Verfügung stellt. Lassen Sie sich das Dokument anzeigen um es auszudrucken oder speichern Sie es für einen späteren Ausdruck zwischen.

Mikrofon

Sofern der Browser Zugriff auf ein Mikrofon hat, öffnet dieser Schalter einen Kanal für Audio-Eingabegeräte.



Diese Option erfordert mind. Version 1.1.0-2 des Web-Clients.

Clientname

Den hier angegebenen Namen stellt der RDP-Server in der Umgebungsvariable CLIENTNAME zur Verfügung.

RDP Verbindungen

Legen Sie hier die RDP-Verbindungen fest, die der Benutzer aufbauen darf. Folgende Parameter lassen sich konfigurieren:

Aktiv

Mit Hilfe dieses Schalters lässt sich eine Verbindung vorübergehend deaktivieren. Bereits bestehende Verbindungen werden nicht getrennt.

Servername, IP oder Host-Objekt (WoL)

Hier legen Sie den Zielcomputer fest. Achten Sie bitte bei Angabe eines DNS-Namens darauf, dass SX-GATE diesen Namen auch auflösen kann. Für interne DNS-Namen ist dazu ggf. in der DNS-Konfiguration eine Weiterleitungs-Zone einzurichten.



Um den Zielcomputer per Wake-on-LAN anschalten zu können, wählen Sie bitte ein IP-Objekt vom Typ "Host" aus, in dem die MAC-Adresse und die IPv4-Adresse konfiguriert sein müssen. Legen Sie benötigte Objekte im Menü "Definitionen > IP-Objekte" an.

Port

Der Port ist in der Regel 3389.

Domäne (optional)

Auf Wunsch können Sie hier die Windows-Domäne eintragen, damit diese im Anmeldebildschirm des RDP-Servers vorausgewählt wird.

Benutzername (optional)

Auf Wunsch können Sie hier den Windows-Benutzernamen eintragen, damit dieser im Anmeldebildschirm des RDP-Servers automatisch hinterlegt wird.

Passwort

Das Kennwort zur Anmeldung am RDP-Server muss üblicherweise vom Benutzer eingegeben werden. Sollten die Kennwörter auf dem SX-GATE und dem RDP-Server identisch sein, können Sie die Option "durchreichen" wählen. Das Kennwort, mit dem sich der Benutzer am SX-GATE-Web-Client angemeldet hat, wird dann an den RDP-Server weitergegeben.

Sicherheit

Der erforderliche Sicherheitsmodus für die Verbindung zwischen SX-GATE und RDP-Server ist abhängig von der Konfiguration des Servers.

Vom Server vorgegeben

Es wird die beste Sicherheitsstufe gewählt, die der Server vorgibt.

Standard Verschlüsselung

In diesem Modus werden nur die übertragenen Daten verschlüsselt.

TLS Verschlüsselung

In dieser Variante ist die komplette Verbindung TLS verschlüsselt.

NLA + TLS Verschlüsselung

Wählen Sie diesen Modus, wenn der Server Network-Level-Authentication (NLA) erfordert. Benutzername und Passwort werden dabei schon vor Verbindungsaufbau abgefragt. Die RDP-Sitzung beginnt erst nach erfolgreicher Authentifizierung. Die Verbindung ist ebenso TLS verschlüsselt.

Tastatur Layout

Sollten Tasten vertauscht sein, wählen Sie hier bitte das auf dem Windows-System konfigurierte Tastaturlayout aus. Probleme gibt es üblicherweise nur beim Zugriff auf Windows Client-Systeme. Auf Server-Systemen stehen in der Regel mehrere Tastaturlayouts zur Verfügung und passen sich an den Client an.

Schriftglättung

Aktivieren Sie diese Option um Text mit glatten Kanten darzustellen. Text über RDP wird standardmäßig mit Ecken und Kanten gerendert, da dies die Anzahl der vom Text verwendeten Farben reduziert und damit die für die Verbindung benötigte Bandbreite verringert.

Terminal-Server Konsole

Diese Option ist nur beim Zugriff auf Terminalserver und nur für Administratoren relevant. Anstatt eine normale Terminalserver-Sitzung zu öffnen, ermöglicht sie es, den Terminalserver zu administrieren.

Kommentar bzw. Anzeigename

Der Kommentar wird in der Oberfläche des Web-Clients angezeigt und soll die Auswahl der Verbindung erleichtern. Ist kein Kommentar angegeben, werden Server-Adresse und -Port sowie ggf. der Benutzername angezeigt.

12.3.2-L VNC Web-Client

Der auf HTML5 basierende VNC Web-Client ermöglicht den Zugriff auf VNC Server über jeden HTML5 fähigen Browser. Auf dem Client wird dafür weder eine spezielle Software noch ein Plugin benötigt.



Die Verbindung zum Web-Client erfolgt über SX-GATEs Reverse-Proxy, der entsprechend konfiguriert sein muss. Der Zugriff erfolgt über den URL-Pfad "/webclient" (z.B. <https://SX-GATE/webclient>).



Änderungen an der Konfiguration werden erst wirksam, wenn sich der Benutzer neu am Web-Client anmeldet. Das Öffnen einer neuen VNC-Sitzung ist nicht ausreichend.

Damit diese Einstellungen angezeigt werden, muss die Web-Client App installiert und der Benutzer Mitglied der Gruppe "system-ras" sein.

Farbtiefe

Hier geben Sie die genutzte Farbtiefe in Bits Per Pixel an. Eine geringere Farbtiefe reduziert die übertragene Datenmenge.

Zwischenablage

Mit diesem Schalter können Sie das Verhalten der Zwischenablage im Web-Client festlegen.



Diese Option erfordert mind. Version 1.2.0-1 des Web-Clients.

VNC Verbindungen

Legen Sie hier die VNC-Verbindungen fest, die der Benutzer aufbauen darf. Folgende Parameter lassen sich konfigurieren:

Aktiv

Mit Hilfe dieses Schalters lässt sich eine Verbindung vorübergehend deaktivieren. Bereits bestehende Verbindungen werden nicht getrennt.

Servername, IP oder Host-Objekt (WoL)

Hier legen Sie den Zielcomputer fest. Achten Sie bitte bei Angabe eines DNS-Namens darauf, dass SX-GATE diesen Namen auch auflösen kann. Für interne DNS-Namen ist dazu ggf. in der DNS-Konfiguration eine Weiterleitungs-Zone einzurichten.



Um den Zielcomputer per Wake-on-LAN anschalten zu können, wählen Sie bitte ein IP-Objekt vom Typ "Host" aus, in dem die MAC-Adresse und die IPv4-Adresse konfiguriert sein müssen. Legen Sie benötigte Objekte im Menü "Definitionen > IP-Objekte" an.

Port

Der Port ist in der Regel 5900.

Passwort

Wählen Sie die Option "abfragen", falls der VNC-Server passwortgeschützt ist. Das Kennwort muss dann vom Benutzer eingegeben werden, sobald er die Verbindung zum VNC-Server aufbauen will. Sollten die Kennwörter auf dem SX-GATE und dem VNC-Server identisch sein, können Sie die Option "durchreichen" wählen. Das Kennwort, mit dem sich der Benutzer am SX-GATE-Web-Client angemeldet hat, wird dann an den VNC-Server weitergegeben.

Mauszeiger Fix

Setzen Sie diese Option, wenn kein Mauszeiger zu sehen ist. Normalerweise wird der Mauszeiger vom Client verwaltet. Wenn der VNC-Server dies aber nicht unterstützt, muss der Maus-Zeiger vom Server gezeichnet werden. Die Reaktionen der Maus erscheinen dann mitunter träge.

Rot-Blau Fix

Aktivieren Sie diese Option, wenn die Farben rot und blau vertauscht sind. Manche VLC-Server senden die Bild-Daten falsch.

Nur Lesen

Wenn gesetzt, wird an der Verbindung keine Eingabe akzeptiert. Benutzer sehen nur den Desktop und was andere Benutzer machen, die den gleichen Desktop verwenden.

Kommentar bzw. Anzeigename

Der Kommentar wird in der Oberfläche des Web-Clients angezeigt und soll die Auswahl der Verbindung erleichtern. Ist kein Kommentar angegeben, werden Server-Adresse und -Port angezeigt.

12.3.2-M SSH Web-Client

Der auf HTML5 basierende SSH Web-Client ermöglicht den Zugriff auf SSH Server über jeden HTML5 fähigen Browser. Auf dem Client wird dafür weder eine spezielle Software noch ein Plugin benötigt.



Die Verbindung zum Web-Client erfolgt über SX-GATEs Reverse-Proxy, der entsprechend konfiguriert sein muss. Der Zugriff erfolgt über den URL-Pfad "/webclient" (z.B. <https://SX-GATE/webclient>).



Änderungen an der Konfiguration werden erst wirksam, wenn sich der Benutzer neu am Web-Client anmeldet. Das Öffnen einer neuen SSH-Sitzung ist nicht ausreichend.

Damit diese Einstellungen angezeigt werden, muss die Web-Client App installiert und der Benutzer Mitglied der Gruppe "system-ras" sein.

Farbschema

Hier geben Sie das gewünschte Farbschema der SSH Konsole an.

Schriftart

Wählen Sie hier die gewünschte Schriftart der SSH Konsole aus.

Schriftgröße

Bestimmen Sie hier welche Schriftgröße in der SSH Konsole genutzt werden soll.

SSH Verbindungen

Legen Sie hier die SSH-Verbindungen fest, die der Benutzer aufbauen darf. Folgende Parameter lassen sich konfigurieren:

Aktiv

Mit Hilfe dieses Schalters lässt sich eine Verbindung vorübergehend deaktivieren. Bereits bestehende Verbindungen werden nicht getrennt.

Servername, IP oder Host-Objekt (WoL)

Hier legen Sie den Zielcomputer fest. Achten Sie bitte bei Angabe eines DNS-Namens darauf, dass SX-GATE diesen Namen auch auflösen kann. Für interne DNS-Namen ist dazu ggf. in der DNS-Konfiguration eine Weiterleitungs-Zone einzurichten.



Um den Zielcomputer per Wake-on-LAN anschalten zu können, wählen Sie bitte ein IP-Objekt vom Typ "Host" aus, in dem die MAC-Adresse und die IPv4-Adresse konfiguriert sein müssen. Legen Sie benötigte Objekte im Menü "Definitionen > IP-Objekte" an.

Port

Der Port ist in der Regel 22.

Benutzername (optional)

Hier kann der Benutzername vorgegeben werden, der zur Anmeldung am SSH-Server verwendet werden muss. Wird kein Benutzername vorgegeben, wird er beim Verbindungsaufbau abgefragt.

Passwort

Das Kennwort zur Anmeldung am SSH-Server muss üblicherweise vom Benutzer eingegeben werden. Sollten die Kennwörter auf dem SX-GATE und dem SSH-Server identisch sein, können Sie die Option "durchreichen" wählen. Das Kennwort, mit dem sich der Benutzer am SX-GATE-Web-Client angemeldet hat, wird dann an den SSH-Server weitergegeben.

Kommentar bzw. Anzeigename

Der Kommentar wird in der Oberfläche des Web-Clients angezeigt und soll die Auswahl der Verbindung erleichtern. Ist kein Kommentar angegeben, werden Server-Adresse und -Port sowie ggf. der Benutzername angezeigt.

12.3.2-N SSH TCP Weiterleitung

Secure-Shell-Clients können authentifizierte und verschlüsselte Kanäle öffnen, durch die sich TCP-Verbindungen zu (meist internen) Servern leiten lassen. Eine SSH Weiterleitung ist technisch zwischen einfachem DNAT und VPN anzusiedeln. Anders als bei DNAT ist die Verbindung durch Authentifizierung und Verschlüsselung

abgesichert. Verglichen mit einem VPN hat der SSH-Tunnel jedoch einige Nachteile wie die fehlende Transparenz für die Client-Anwendung, es stehen ausschließlich unidirektionale TCP-Verbindungen zur Verfügung und unbedarfte Benutzer können leichter Opfer von Man-in-the-Middle Attacken werden. Eine SSH-Weiterleitung lässt sich dafür leichter konfigurieren.

Der zugehörige SX-GATE SSH-Server ist auf Port 2222 erreichbar. Um den Zugriff aus dem Internet zu erlauben muss gegebenenfalls eine passende Firewall-Regel eingetragen werden. Nutzen Sie dazu das vordefinierte Protokoll "SSH-FWD".



Mit Hilfe von Firewall DNAT-Regeln ist es möglich, den Dienst auf einem anderen Port erscheinen zu lassen. So könnte z.B. der HTTPS-Port 443 auf 2222 umgeleitet werden, damit SSH-Clients leichter Firewalls und Proxies überwinden können.

Öffentlicher SSH-Schlüssel (ed25519 oder RSA)

Geben Sie hier den öffentlichen SSH-Schlüssel des Clients ein. Der Schlüssel beginnt mit "ssh-rsa" oder "ssh-ed25519", gefolgt von einem Leerzeichen und mindestens 68 Buchstaben, Ziffern, Schrägstrichen, Plus- und Gleichheits-Zeichen in einer langen Zeile. Leerzeichen oder Zeilenumbrüche innerhalb dieser Zeichenfolge sind nicht erlaubt. Optional darf am Ende ein Leerzeichen und ein Kommentar angehängt sein. Stark verkürztes Beispiel eines Schlüssels: "ssh-rsa AA3x/5+eW48oPvX= Kommentar".

Erlaubte Verbindungen

Der SSH-Client darf sich ausschließlich zu den hier angegebenen Adressen und Ports verbinden.



Aus technischen Gründen werden derzeit Protokoll-Signaturen ignoriert, bei denen als Ziel-Port ein Nummernbereich angegeben ist. Dieses Verhalten kann sich in zukünftigen SX-GATE Versionen ändern.

12.3.2-O RAS Einstellungen

Diese Einstellungen sind nur für Mitglied der Gruppe "system-ras" verfügbar. Sie beziehen sich auf Fernzugriffe via IPsec-VPN.

WoL bei Einwahl an Mac-Adresse

Wenn Sie hier die Hardware-Adresse der Netzwerk-Karte eines Rechners eintragen, wird dieser bei Einwahl des Benutzers mittels Wake-on-LAN geweckt. Die

Einwahl muss dazu entweder per IPsec-L2TP oder per OpenVPN mit aktivierter Benutzeranmeldung erfolgen.

Die Adresse muss im Format "XX:XX:XX:XX:XX:XX" angegeben werden. Jedes "X" steht dabei für eine Ziffer oder einen Buchstaben zwischen "A" und "F". Als Trennzeichen sind neben dem Doppelpunkt auch Punkte, Bindestriche und der Unterstrich zulässig.

Zugewiesene IP

Bei allen RAS-Diensten, die eine Authentifizierung am SX-GATE erfordern, wird dem Client eine IP-Adresse zugewiesen. Dabei stehen zwei verschiedene Möglichkeiten zur Wahl. Es kann entweder eine schnittstellenbezogene, benutzerunabhängige IP-Adresse zugewiesen werden oder eine persönliche IP je Benutzer.



Wenn Sie dem RAS-Einwähler eine frei IP-Adresse aus dem LAN zuweisen, konfiguriert SX-GATE einen Proxy-ARP-Eintrag für diese Adresse. Die Systeme im LAN benötigen in diesem Fall keine speziellen Routing-Einträge für die Kommunikation mit dem RAS-Client.



Grundsätzlich gilt: IP-Adressen müssen immer eindeutig vergeben werden. Deshalb darf es keinerlei Überschneidungen zwischen schnittstellenbezogenen, benutzerspezifischen und anderweitig verwendeten IP-Adressen geben. Treten Überschneidungen auf, so ist die Verfügbarkeit der einzelnen Systeme nicht gewährleistet.

Benutzerbezogene RAS-IP-Adressen werden von folgenden RAS-Diensten verwendet:

- L2TP/IPSec-VPN (l2tp0)
- IPSec-VPN mit XAUTH

IP-Adresse der RAS-Schnittstelle

In dieser Einstellung wird dem Benutzer die in der jeweiligen RAS-Schnittstelle konfigurierte IP-Adresse zugewiesen.

persönliche IP

Wählen Sie diese Option damit dem Benutzer bei jeder RAS-Einwahl stets eine persönliche IP-Adresse zugewiesen wird. Durch diese Zuordnung wird es möglich, in der Firewall-Konfiguration des SX-GATE für diesen RAS-Benutzer eigene Firewall-Regeln zu definieren.

Nachfolgend kann für jeden SX-GATE RAS-Dienst separat festgelegt werden, ob sich der Benutzer mit diesem verbinden darf und welche persönliche

IP zugewiesen wird. Üblicherweise wird für jeden RAS-Dienst die selbe IP verwendet, es können aber natürlich auch unterschiedliche Adressen konfiguriert werden. Die in den jeweiligen RAS-Schnittstellen eingestellten IP-Adressen haben für Einwahlen dieses Benutzers keine Bedeutung mehr.

L2TP/IPSec-VPN

Legen Sie hier fest, ob sich der aktuelle Benutzer mit SX-GATE's L2TP-Server verbinden darf und welche IP-Adresse zugewiesen wird.



Die maximale Anzahl gleichzeitiger L2TP-Verbindungen ergibt sich aus der Anzahl IP-Adressen die unter "Module > Netzwerk > l2tp0" konfiguriert sind. Die Konfiguration benutzerspezifischer IPs hat darauf keinen Einfluss. Selbst bei Konfigurationen in denen ausschließlich benutzerspezifische IP-Adressen verwendet werden sollen, ist es notwendig, in der L2TP-Schnittstelle ausreichend viele IP-Adressen zu vergeben.

XAuth/IPSec-VPN

Legen Sie hier fest, ob sich der aktuelle Benutzer mit SX-GATE's XAuth/IPSec-Server verbinden darf und welche IP-Adresse zugewiesen wird.

12.3.2-P Docklets

Durch Aktivierung der entsprechenden Schalter können Sie dem aktuell gewählten Benutzer Zugriff auf die Info- und Status-Fenster gewähren, die u.a. auf der Startseite angezeigt werden.



Diese Einstellungen sind nur bei Mitgliedern der Gruppe "system-admin" verfügbar.

12.3.2-Q Menü Statistiken

Durch Aktivierung der entsprechenden Schalter können Sie dem aktuell gewählten Benutzer Zugriff auf die entsprechenden Menüpunkte aus dem Hauptmenü "Statistiken" geben.



Diese Einstellungen sind nur bei Mitgliedern der Gruppe "system-admin" verfügbar.

12.3.2-R Menü Monitoring

Durch Aktivierung der entsprechenden Schalter können Sie dem aktuell gewählten Benutzer Zugriff auf die entsprechenden Menüpunkte aus dem Hauptmenü "Monitoring" geben.



Diese Einstellungen sind nur bei Mitgliedern der Gruppe "system-admin" verfügbar.

12.3.2-S Menü Definitionen

Durch Aktivierung der entsprechenden Schalter können Sie dem aktuell gewählten Benutzer Zugriff auf die entsprechenden Menüpunkte aus dem Hauptmenü "Definitionen" geben.



Diese Einstellungen sind nur bei Mitgliedern der Gruppe "system-admin" verfügbar.

12.3.2-T Menü System

Durch Aktivierung der entsprechenden Schalter können Sie dem aktuell gewählten Benutzer Zugriff auf die entsprechenden Menüpunkte aus dem Hauptmenü "System" geben.



Diese Einstellungen sind nur bei Mitgliedern der Gruppe "system-admin" verfügbar.

12.3.2-U Menü Assistenten

Durch Aktivierung der entsprechenden Schalter können Sie dem aktuell gewählten Benutzer Zugriff auf die entsprechenden Menüpunkte aus dem Hauptmenü "Assistenten" geben.



Diese Einstellungen sind nur bei Mitgliedern der Gruppe "system-admin" verfügbar.

12.3.2-V Menü Module

Durch Aktivierung der entsprechenden Schalter können Sie dem aktuell gewählten Benutzer Zugriff auf die entsprechenden Menüpunkte aus dem Hauptmenü "Module" geben.



Diese Einstellungen sind nur bei Mitgliedern der Gruppe "system-admin" verfügbar.

12.3.2-W Anmeldeoptionen

Meldung nach dem Anmelden

Die hier angegebene Meldung wird nach dem Anmelden dieses Benutzers solange angezeigt, bis sie vom Benutzer geschlossen wird.

12.3.2-X Benutzerdaten

Die Felder auf dieser Seite haben in erster Linie informativen Charakter. Bei Benutzern mit lokalem E-Mail-Postfach (Mitglieder der Gruppe "system-mail") stehen die Daten in der SX-GATE-Groupware als Adressbuch zur Verfügung.

Primäre Mail-Adresse des Benutzers

Legt die hauptsächlich vom Benutzer verwendete Mail-Adresse fest. Die Adresse wird als Absender verwendet, wenn SX-GATE stellvertretend für den Benutzer eine E-Mail versendet (Autoantwort-Funktion).

12.3.3 Gruppen

Mit jeder Gruppe ist automatisch ein gleichnamiger Mail-Verteiler verknüpft. Somit ist es möglich, z.B. eine Gruppe "info" zu erstellen. Alle Benutzer, die sich in dieser Gruppe befinden, erhalten ein Exemplar der E-Mails, die an diese Gruppe adressiert sind. Voraussetzung dafür ist natürlich, dass der entsprechende Benutzer auch über ein lokales Mail-Konto verfügt, also Mitglied der Gruppe "system-mail" ist. Zusätzlich lassen sich zu jeder Gruppe weitere externe Mail-Empfänger angeben.

In Verbindung mit der URL-Filter-Option des Web-Proxies lässt sich die Anwendung einzelner URL-Filter Listen auf bestimmte Gruppen einschränken. Dies ermöglicht individuelle Einstellungen für einzelne Benutzergruppen.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Gruppenname

Legen Sie bitte hier den Namen der Gruppe fest.



Neben Kleinbuchstaben und Ziffern sind im Gruppennamen nur der Bindestrich (-), der Punkt (.) und der Unterstrich (_) zulässig. Der Gruppenname muss mit einem Kleinbuchstaben beginnen. Insbesondere die Verwendung von Umlauten sowie Leerzeichen im Gruppennamen ist nicht erlaubt.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.3.3-A Benutzer.....	166
12.3.3-B Mail-Einstellungen.....	167
12.3.3-C Verwendung.....	168

12.3.3-A Benutzer

Zugehörige Benutzer

In diesem Eingabebereich sehen Sie alle Benutzer, die der Gruppe bereits zugeordnet wurden sowie alle noch nicht zugeordneten Benutzer. Um mehrere Benutzer gleichzeitig in eine Gruppe aufzunehmen bzw. aus einer Gruppe zu entfernen, können Sie in der jeweiligen Liste mehrere Einträge gleichzeitig auswählen. Halten Sie dazu während der Auswahl die STRG-Taste gedrückt.



Der Benutzer "admin" wird in den System-Gruppen "system-mail" und "system-admin" nicht angezeigt, da dieser Benutzer stets Mitglied dieser Gruppen ist.

12.3.3-B Mail-Einstellungen

Mails weiterleiten wenn authentifiziert (SMTP-Auth)

Der Mail-Server des SX-GATEs kann so eingestellt werden, dass für die Weiterleitung von E-Mails in das Internet Benutzeranmeldung erforderlich ist. Mit Hilfe dieses Schalters legen Sie fest, welche Benutzer berechtigt sind, nach Authentifizierung Mails in das Internet zu senden. Berechtigt sind alle Benutzer, die Mitglied mindestens einer Gruppe sind, bei der dieser Schalter aktiviert ist.



Nur Mitglieder der Gruppe "system-mail" verfügen über ein Konto, mit dem eine Anmeldung überhaupt erst möglich ist.

In der Grundeinstellung ist im Mail-Server die Authentifizierung deaktiviert. Der Mail-Versand von internen IP-Adressen in das Internet ist bereits ohne Benutzeranmeldung möglich, während der Mail-Versand von externen Adressen in das Internet grundsätzlich verboten ist. Im Menü "Module > Mail-Server > SMTP Einstellungen" können Sie die Authentifizierung auf dem Reiter (Tab) "Relay Kontrolle" über zwei Optionen zuschalten. Aktivieren Sie die Option "SMTP-Auth erforderlich für lokale Benutzer", wenn nicht jeder interne Benutzer E-Mails in das Internet senden darf sondern nur noch authentifizierte und berechtigte Benutzer. Aktivieren Sie "SMTP-Auth immer anbieten", um externen Adressen die Anmeldung zu erlauben, so dass z.B. Außendienstmitarbeiter SX-GATE als Mail-Relay-Server nutzen können.

Mailgruppen-Funktion

Anhand der Information, welche lokalen Benutzer Mitglied einer Gruppe sind (siehe Reiter (Tab) "Benutzer"), kann SX-GATE automatisch eine entsprechende Mailgruppe erstellen. Enthalten sind dabei aber nur die Benutzer, die zugleich Mitglied der Gruppe "system-mail" sind, also über ein lokales Mail-Konto verfügen.



Wird ein der Gruppe zugeordneter Benutzer gelöscht, aus der Gruppe "system-mail" entfernt oder in "system-mail" aufgenommen, so wird dies automatisch in der Mailgruppe berücksichtigt.

Die E-Mail-Adresse der Gruppe ergibt sich aus dem Gruppennamen. Lautet die lokale Domain "example.com", ist die Gruppe "gruppe" unter "gruppe@example.com" erreichbar.

Wählen Sie hier aus, welche Art von Mailgruppen-Funktion Sie nutzen wollen.

keine

Mit dieser Gruppe ist keine E-Mail-Adresse verknüpft.

Verteiler

Wird eine Mail an die Gruppe zugestellt, erhält jedes Gruppenmitglied und jede externe E-Mail-Adresse eine Kopie der Mail.

IMAP-Ordner

Mit der Gruppe ist ein gemeinsamer IMAP-Ordner verknüpft, auf den alle Gruppenmitglieder Zugriff haben. Eine Mail an die Gruppe wird in diesen Ordner zugestellt. Sofern Einträge unter "Externe Mail-Adressen" vorhanden sind, erhält jede Adresse eine Kopie der Mail.

Externe Mail-Adressen

Dieser Eingabebereich dient dazu, externe E-Mail-Adressen oder andere Gruppen in einen Verteiler aufzunehmen.



Verweisen die hier eingegebenen Adressen auf lokale Benutzer oder Gruppen, so werden diese Einträge nicht automatisch entfernt, wenn der entsprechende Benutzer oder die Gruppe gelöscht werden.

12.3.3-C Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

12.4 Zertifikatsverwaltung

12.4.1 CA Zertifikate

In diesem Menü verwalten Sie die CA-Zertifikate, die SX-GATE kennt. Sie finden hier zum einen SX-GATEs eigene CA, die es Ihnen ermöglicht selbst Zertifikate auszustellen. Zur Verifikation von Zertifikaten lassen sich aber auch CA-Zertifikate hinterlegen.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Name

Geben Sie hier einen Namen für die CA bzw. das CA-Bündel ein. Dieser Name dient ausschließlich zur Identifikation und kann daher frei vergeben werden.

12.4.1.1 SX-GATE-CA

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.4.1.1-A CA Zertifikat.....	169
12.4.1.1-B CA Sperrliste.....	171
12.4.1.1-C SSL-Proxy CA.....	172

Für die Arbeit mit Zertifikaten innerhalb geschlossener Benutzergruppen ist es in der Regel nicht nötig, Zertifikate bei Zertifizierungsstellen zu kaufen. Nutzen Sie SX-GATE um kostenlos selbst Zertifikate auszustellen.

12.4.1.1-A CA Zertifikat

In diesem Bereich wird das Stammzertifikat des SX-GATE verwaltet. Andere häufig genutzte Bezeichnungen dafür sind "Root-Zertifikat" oder "CA-Zertifikat".



In der Grundeinstellung ist auf SX-GATE kein CA-Zertifikat installiert. Es muss in dieser Maske zuerst erstellt werden.

Mit dem Stammzertifikat werden alle von SX-GATE ausgestellten Zertifikate unterschrieben. Es spielt die zentrale Rolle für das Vertrauensverhältnis bei zertifikatsbasierender Authentifizierung. Aus diesem Grunde ist das Stammzertifikat stets durch ein Passwort geschützt, das bei allen Operationen anzugeben ist.



Das Stammzertifikat ist aus Sicherheitsgründen nicht Bestandteil des SX-GATE-Backups. Nutzen Sie die Export-Funktion auf dieser Maske um ein Backup zu erstellen.

Öffentlichen Schlüssel exportieren

Hier können Sie den öffentlichen Schlüssel des CA-Zertifikats herunterladen. Alle Anwendungen die Zertifikate zur Authentifizierung nutzen benötigen diesen.



SX-GATE liefert den öffentlichen Schlüssel seiner CA zusammen mit jedem ausgestellten Zertifikat aus. Sollte ein Client also ein von SX-GATE ausgestelltes Zertifikat erhalten, so ist es in der Regel nicht notwendig, dieses separat weiterzugeben.

CA Zertifikat erstellen oder importieren

Mit Hilfe dieser Funktion können Sie erstmalig ein Stammzertifikat erstellen oder das Backup eines solchen Zertifikats einspielen.



Ein von SX-GATE selbst ausgestelltes Stammzertifikat ist 20 Jahre gültig. Grundsätzlich ist es nicht sinnvoll, dieses Zertifikat lange bevor es abläuft zu erneuern - es sei denn die Vertraulichkeit ist nicht länger gewährleistet.

CA Zertifikat erstellen

Mit Hilfe dieser Funktion können Sie erstmalig ein Stammzertifikat erstellen.



Ein von SX-GATE selbst ausgestelltes Stammzertifikat ist 20 Jahre gültig. Grundsätzlich ist es nicht sinnvoll, dieses Zertifikat lange bevor es abläuft zu erneuern - es sei denn die Vertraulichkeit ist nicht länger gewährleistet.

CA Schlüsselpaar sichern

Das Schlüsselpaar des Stammzertifikats kann zu Sicherungszwecken im PKCS#12-Format exportiert werden. Bitte beachten Sie, dass dieser Export also auch den privaten Schlüssel enthält, der unbedingt geheim bleiben muss.

Privaten CA-Schlüssel löschen

Um die Sicherheit der SX-GATE CA zu erhöhen, lässt sich der private Schlüssel des Stammzertifikats löschen. Nutzen Sie diese Möglichkeit, wenn Sie in nächster Zeit keine neuen Zertifikate ausstellen müssen.



Bevor Sie den privaten Schlüssel löschen, müssen Sie selbstverständlich mit Hilfe der Export-Funktion ein Backup erstellen. Bewahren Sie dieses auf einem sicheren Medium an einem sicheren Ort auf. Installieren Sie den privaten Schlüssel mit Hilfe der Import-Funktion sobald Sie die CA wieder benötigen.

12.4.1.1-B CA Sperrliste

Nutzt eine Anwendung zur Authentifizierung die Vertrauensstellung zur Stammzertifizierungsstelle, so stellt sich das Problem, wie bestimmte Zertifikate von dieser Vertrauensstellung ausgenommen werden können. Dies wird z.B. dann relevant, wenn ein Mitarbeiter die Firma verlässt oder ein Notebook gestohlen wird. Eine CA kann dazu mit Hilfe von Sperrlisten (Certificate revocation list, CRL) Zertifikate vorzeitig für ungültig erklären.



Die Sperrliste muss auf allen Systemen installiert werden, zu denen potentiell eine unberechtigte Verbindung mit Hilfe des widerrufenen Zertifikats aufgebaut werden könnte.

CRL-Verteilungsstelle festlegen

Beim Erstellen von Zertifikaten, kann im Zertifikat eine URL hinterlegt werden, unter der stets die aktuellste Version der CRL heruntergeladen werden kann. Ein System, dass das Zertifikat überprüfen will, kann so jederzeit auf die aktuelle CRL zurückgreifen.



Nach dem Ausstellen einer neuen CRL muss diese stets manuell auf den angegebenen Server übertragen werden.

Zertifikats-Sperrliste exportieren

In diesem Bereich kann die CRL im PEM-Format exportiert werden.

Neue Zertifikats-Sperrliste erstellen

Jedes Mal nachdem Sie ein Zertifikat vorzeitig widerrufen haben, müssen Sie mit Hilfe dieser Funktion eine neue Sperrliste generieren.



Die Sperrliste muss von der CA mit Hilfe des Stammzertifikats signiert werden.



Vergessen Sie nicht, die neue Sperrliste auf den relevanten Systemen zu installieren. Um die Sperrliste im VPN-Server des SX-GATE zu aktualisieren nutzen Sie bitte die entsprechende Funktion am Ende des Assistenten oder unter "Module > Netzwerk > Einstellungen".

Lokale CA-Sperrliste im VPN-Server hinterlegen

Arbeitet der SX-GATE VPN-Server mit Zertifikaten der eigenen SX-GATE CA, haben Sie hier die Möglichkeit, die derzeitige Zertifikats-Sperrliste (CRL) in den lokalen VPN-Server zu übertragen. Sinn einer Zertifikats-Sperrliste ist es, bestimmte Zertifikate bereits vor deren Ablaufdatum als ungültig zu erklären. Dies ist z.B. notwendig, wenn ein Mitarbeiter die Firma verlässt und diesem zeitnah der VPN-Zugang verwehrt werden muss.

12.4.1.1-C SSL-Proxy CA

Die SSL-Interceptor-Funktion des Web-Proxies ermöglicht es, verschlüsselte Verbindungen aufzubrechen, um darin z.B. nach Viren zu scannen. Dabei wird dem Client anstelle des original Web-Server-Zertifikats ein lokal vom Proxy erstelltes Zertifikat mit identischen Daten präsentiert. Um die Proxy-Zertifikate auszustellen, ist eine eigene Stammzertifizierungsstelle (CA) erforderlich, die sich hier festlegen lässt.



Das Stammzertifikat ist aus Sicherheitsgründen nicht Bestandteil des SX-GATE-Backups. Nutzen Sie die Export-Funktion auf dieser Maske um ein Backup zu erstellen.

Öffentlichen Schlüssel exportieren

Hier können Sie den öffentlichen Schlüssel der Proxy-CA herunterladen. Das Zertifikat sollte in allen Browser-Clients installiert werden.

Proxy Schlüsselpaar sichern

Das Schlüsselpaar des Proxy-Zertifikats kann zu Sicherungszwecken im PKCS#12-Format exportiert werden. Bitte beachten Sie, dass dieser Export also auch den privaten Schlüssel enthält, der unbedingt geheim bleiben muss.

Proxy-Zertifikat erstellen oder importieren

Mit Hilfe dieser Funktion können Sie ein neues Proxy-Stammzertifikat erstellen oder das Backup eines solchen Zertifikats einspielen.



Ein von SX-GATE selbst ausgestelltes Stammzertifikat ist 20 Jahre gültig. Grundsätzlich ist es nicht sinnvoll, dieses Zertifikat lange bevor es abläuft zu erneuern - es sei denn die Vertraulichkeit ist nicht länger gewährleistet.

12.4.1.2 SX-GATE-CA - Zertifikate

In diesem Bereich können Sie Zertifikate erstellen, die mit dem Stammzertifikat der SX-GATE-Zertifizierungsstelle (CA) signiert werden. Die CA des SX-GATE stellt eine kostenlose Alternative zum Kauf von Zertifikaten kommerzieller Zertifizierungsstellen dar. Zur zertifikatsbasierten Authentifizierung innerhalb geschlossener Benutzergruppen ist die SX-GATE-CA vollständig ausreichend.

In erster Linie dient die CA des SX-GATES zur Erstellung von Zertifikaten für VPN. Auch der VPN-Server des SX-GATES benötigt ein eigenes Zertifikat. Wählen Sie den vordefinierten Eintrag "VPN" um das Zertifikat für SX-GATES VPN-Server auszustellen.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann

der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Zertifikatsname

Geben Sie hier einen Namen für das Zertifikat ein. Dieser Name dient ausschließlich zur Identifikation des Zertifikats und kann daher frei vergeben werden.

Zertifikat exportieren

Hier haben Sie die Möglichkeit, das Zertifikat herunterzuladen. Das Zertifikat ist der von der CA signierte öffentliche Schlüssel. Das Dateiformat ist PEM.



Der private Schlüssel ist nicht in der SX-GATE-CA hinterlegt.

Vorzeitig für ungültig erklärt am

Zu diesem Zeitpunkt wurde das Zertifikat für die Aufnahme in die Zertifikats-Sperrliste der SX-GATE-CA vorgemerkt.



Alleine durch die Eingabe des Datums wird das Zertifikat noch nicht ungültig. Mit Hilfe der entsprechenden CA-Funktion muss zunächst eine neue Sperrliste (certificate revocation list, CRL) erstellt und diese dann in den relevanten Anwendungen installiert werden.

Zertifikat widerrufen

Bei der Authentifizierung mit Hilfe von Zertifikaten wird je nach Anwendung häufig nur geprüft, ob zu der Stammzertifizierungsstelle (CA), die das Zertifikat ausgestellt hat ein Vertrauensverhältnis besteht. Ist dies gegeben und das Zertifikat ist noch nicht abgelaufen, so wird die Authentifizierung erfolgreich abgeschlossen. Es kann jedoch notwendig werden, ein Zertifikat zu widerrufen bevor es regulär abläuft. Dies ist z.B. denkbar, wenn ein Mitarbeiter die Firma verlässt oder ein Notebook mit einem entsprechenden Zertifikat gestohlen wird.



Zum Erstellen einer vollständigen CRL dürfen Zertifikate vor dem regulären Ablaufdatum nicht gelöscht werden.

Widerruf zurücknehmen

Ein bereits widerrufenes Zertifikat kann wieder aktiviert werden. Neben der Entsperrung als solches muss selbstverständlich eine neue CRL generiert und verteilt werden.

Zertifikat neu erstellen

Mit Hilfe dieser Funktion erstellen bzw. erneuern Sie das Zertifikat. Das neue Zertifikat hat eine Gültigkeitsdauer von einem Jahr und wird von der SX-GATE-CA signiert.



Sie sollten ein hier bereits ausgestelltes Zertifikat erst unmittelbar vor dessen Ablauf erneuern. Andernfalls ist es nicht mehr möglich, das vorherige Zertifikat in die Zertifikats-Sperrliste aufzunehmen.

Zertifikat erstellen

In dieser Maske geben Sie die Zertifikatsdaten für das Zertifikat ein.

CN

Sofern Sie dieses Zertifikat für einen Server-Dienst ausstellen, sollten Sie hier den DNS-Namen oder die IP-Adresse eingeben, mit deren Hilfe das System aus dem Internet adressiert wird. Auch ein Wildcard-Zertifikat (z.B. *.example.com) ist möglich. Ist das Zertifikat für einen Benutzer, so können Sie z.B. dessen Namen oder E-Mail Adresse eintragen.

Alternative Bezeichner

Bei der Überprüfung, ob das Server-Zertifikat auch tatsächlich zum angesprochenen Server gehört, werten viele Clients bevorzugt dieses Feld aus. Sie können hier alle Namen oder auch IP-Adressen eintragen, unter denen der Server angesprochen wird. Auch Wildcard-Zertifikate (z.B. *.example.com) sind möglich. Für ein Benutzer-Zertifikat kann die E-Mail-Adresse hinterlegt werden.

Passworteingabe

Zu dem neuen Zertifikat gehört auch der private Schlüssel, der unbedingt geheim zu halten ist. Um dies auch während der Übermittlung an den Nutzer des Zertifikates zu gewährleisten, wird der Zugriff auf die PKCS#12-Datei durch ein Kennwort geschützt. Geben Sie dieses Kennwort über einen sicheren Kanal getrennt von der PKCS#12-Datei an den Nutzer weiter.

Zertifikats-Anfrage

Die Zertifikats-Anfrage wird mit dem Aufruf dieser Seite erstellt und kann im nächsten Schritt mit Hilfe des CA-Zertifikats signiert werden.

Verwendungszweck: Server Authentifizierung

Setzen Sie diesen Verwendungszweck (Extended Key Usage) für ein Server-Zertifikat (z.B. Web- oder VPN-Server).



Abhängig vom Client und dessen Konfiguration kann es passieren, dass der Client die Verbindung verweigert, wenn dieses Attribut im Server-Zertifikat fehlt.

Verwendungszweck: Client Authentifizierung

Setzen Sie diesen Verwendungszweck (Extended Key Usage) für ein Client-Zertifikat (z.B. Web-Browser oder VPN-Client). So kann unter Umständen verhindert werden, dass sich der Client gegenüber anderen Clients missbräuchlich als Server ausgibt.

Verwendungszweck: E-Mail-Schutz (S/MIME)

Setzen Sie diesen Verwendungszweck (Extended Key Usage) für ein Benutzer-Zertifikat, das zum Signieren und für die Ende-zu-Ende-Verschlüsselung von E-Mails mit S/MIME genutzt werden soll.

Zertifikat signieren

Mit dem Aufruf dieser Seite wird das Zertifikat signiert.

Installations-Paket erstellen**Windows IPSec-L2TP Parameter*****SX-GATE Internet-IP oder -Servername***

Geben Sie hier bitte den DNS-Namen oder die IP-Adresse an, unter der SX-GATE vom Client aus erreichbar ist.

Direkten Internetzugriff erlauben

Wenn diese Option deaktiviert ist, besteht für den Client kein direkter Internetzugriff mehr, sobald die VPN-Verbindung hergestellt ist. Das Standardgateway des Clients wird auf den VPN-Tunnel umgesetzt. Der Zugang zum Internet erfolgt nun über das VPN und somit über Firewall und Proxies des SX-GATE. Wird die VPN-Verbindung wieder getrennt, wird auch das Standardgateway zurückgesetzt und der Client geht wie gehabt direkt in das Internet.

Ist die Option aktiviert, bleibt der direkte Internetzugang für den Client bestehen. Nur die relevanten IP-Adressen werden über das VPN geroutet.

Direkten Internetzugriff erlauben

- Nein

Lesen Sie bitte weiter bei [Windows IPSec-L2TP Paket](#) (S. 177)

VPN-Server hinter NAT-Router

Wenn diese Option gesetzt ist, wird der benötigte Windows Registry Key beim Anlegen der Verbindung automatisch gesetzt.

Verbindungsspezifischer DNS-Suffix

Optional kann dem Windows-Client ein verbindungsspezifischer DNS-Suffix zugewiesen werden. Auf diese Weise kann z.B. der Client Rechner im LAN anhand des Rechnernamens (ohne Eingabe der Domain) auflösen.

Windows IPSec-L2TP Routen

Zusätzliche Routen (nur Powershell)

Hier können Sie zusätzliche lokale Netzwerke angeben, die über die VPN-Verbindung geroutet werden sollen. Um eine Route zu einem einzelnen Rechner zu setzen, geben Sie bitte dessen IP-Adresse ein.



Die Routen werden nur mit dem Powershell Installationspaket gesetzt. Bei dem veralteten CMAK Installationspaket werden die Routen nicht berücksichtigt.

Windows IPSec-L2TP Paket

Installationspaket für Windows IPSec-L2TP (Powershell)

Über diese Schaltfläche lässt sich ein unter Windows selbstextrahierendes ZIP-Archiv herunterladen. Neben der PKCS#12-Datei mit den Zertifikaten und dem privaten Schlüssel enthält das Archiv ein Powershell Script zum Import von Zertifikaten, um automatisiert eine IPSec-L2TP-Verbindung unter Windows zu konfigurieren.

Nach Doppelklick unter Windows entpackt sich das Archiv und startet automatisch den Installations Dialog.



Die Verbindungen werden mit den sicheren Algorithmen AES256-SHA256-DH20 als IKEv1 IKE-Proposals (Phase 1) und AES256-SHA256 als IKEv1 ESP-Proposals (Phase 2) angelegt.

Installationspaket für Windows IPSec-L2TP (CMAK veraltet)

Über diese Schaltfläche lässt sich ein unter Windows selbstextrahierendes ZIP-Archiv herunterladen. Neben der PKCS#12-Datei mit den Zertifikaten und dem privaten Schlüssel enthält das Archiv ein Tool zum Import von Zertifikaten und Steuerdateien für Microsofts "Verbindungsmanager-Verwaltungskit", VMVK (Englisch: "Connection Manager Administration Kit", CMAK) um automatisiert eine IPSec-L2TP-Verbindung unter Windows zu konfigurieren.

Nach Doppelklick unter Windows entpackt sich das Archiv und versucht zunächst Schlüssel und Zertifikate zu installieren. Dazu wird in einem DOS-Fenster das Passwort abgefragt, mit dem die PKCS#12-Datei geschützt ist. Nach Bestätigung wird dann die Verbindung eingerichtet.



Verbindungen die über CMAK angelegt werden nutzen für die Datenintegrität den veralteten Windows Standard SHA-1 (IKEv1 IKE-Proposals (Phase 1) AES256-SHA1-DH20 und IKEv1 ESP-Proposals (Phase 2) AES128-SHA1).

Windows IPSec-IKEv2 Parameter

SX-GATE Internet-IP oder -Servername

Geben Sie hier bitte den DNS-Namen oder die IP-Adresse an, unter der SX-GATE vom Client aus erreichbar ist.

Direkten Internetzugriff erlauben

Wenn diese Option deaktiviert ist, besteht für den Client kein direkter Internetzugriff mehr, sobald die VPN-Verbindung hergestellt ist. Das Standardgateway des Clients wird auf den VPN-Tunnel umgesetzt. Der Zugang zum Internet erfolgt nun über das VPN und somit über Firewall und Proxies des SX-GATE. Wird die VPN-Verbindung wieder getrennt, wird auch das Standardgateway zurückgesetzt und der Client geht wie gehabt direkt in das Internet.

Ist die Option aktiviert, bleibt der direkte Internetzugang für den Client bestehen. Nur die relevanten IP-Adressen werden über das VPN geroutet.

Direkten Internetzugriff erlauben

- Nein

Lesen Sie bitte weiter bei [Windows IPSec-IKEv2 Paket](#) (S. 179)

Verbindungsspezifischer DNS-Suffix

Optional kann dem Windows-Client ein verbindungsspezifischer DNS-Suffix zugewiesen werden. Auf diese Weise kann z.B. der Client Rechner im LAN anhand des Rechnernamens (ohne Eingabe der Domain) auflösen.

Windows IPSec-IKEv2 Routen

Zusätzliche Routen (nur Powershell)

Hier können Sie zusätzliche lokale Netzwerke angeben, die über die VPN-Verbindung geroutet werden sollen. Um eine Route zu einem einzelnen Rechner zu setzen, geben Sie bitte dessen IP-Adresse ein.



Die Routen werden nur mit dem Powershell Installationspaket gesetzt. Bei dem veralteten CMAK Installationspaket werden die Routen nicht berücksichtigt.

Windows IPSec-IKEv2 Paket

Installationspaket für Windows IPSec-IKEv2 (Powershell)

Über diese Schaltfläche lässt sich ein unter Windows selbstextrahierendes ZIP-Archiv herunterladen. Neben der PKCS#12-Datei mit den Zertifikaten und dem privaten Schlüssel enthält das Archiv ein Powershell Script zum Import von Zertifikaten, um automatisiert eine IPSec-L2TP-Verbindung unter Windows zu konfigurieren.

Nach Doppelklick unter Windows entpackt sich das Archiv und startet automatisch den Installations Dialog.



Die Verbindungen werden mit den sicheren Algorithmen AES256-SHA256-DH20 als IKEv1 IKE-Proposals (Phase 1) und AES256-SHA256 als IKEv1 ESP-Proposals (Phase 2) angelegt.

OpenVPN Parameter

SX-GATE Internet-IP oder -Servername

Geben Sie hier bitte den DNS-Namen oder die IP-Adresse an, unter der SX-GATE vom Client aus erreichbar ist.

OpenVPN-Server-Schnittstelle

Wählen Sie hier bitte die OpenVPN-Server-Schnittstelle aus, mit der sich der Client verbinden soll. In der Client-Konfiguration werden das dazu passenden Protokoll, die Port-Nummer und die Verschlüsselungseinstellungen eingetragen.

OpenVPN Paket

Privater-Schlüssel kennwortgeschützt in .ovpn-Datei eingebettet

Hier können Sie eine OpenVPN-Konfigurationsdatei für den Client herunterladen. Der private Schlüssel mit dem zugehörigen Zertifikat und das CA-Zertifikat sind in die Datei

eingebettet. Der private Schlüssel ist mit dem zuvor von Ihnen festgelegten Kennwort geschützt.

Privater-Schlüssel ungeschützt in .ovpn-Datei eingebettet

Wie vor, jedoch mit unverschlüsseltem privaten Schlüssel. Zum Aufbau der VPN-Verbindung ist somit kein Passwort erforderlich. Wir empfehlen daher, serverseitig die Benutzerauthentifizierung zu aktivieren.



Unbefugter Zugriff auf die Konfigurationsdatei muss sowohl auf dem Transportweg zum Client als auch auf dem Client selbst mit geeigneten Maßnahmen verhindert werden.

Privater-Schlüssel in kennwortgeschützter PKCS#12-Datei

Zur Vereinfachung der OpenVPN-Konfiguration unter Windows ist das hier angebotene selbstextrahierende ZIP-Archiv gedacht. Es enthält den privaten Schlüssel mit dem zugehörigen Zertifikat und das CA-Zertifikat in einer PKCS#12-Datei. Ferner liegt eine OpenVPN-Konfigurationsdatei mit passenden Einstellungen bei. Nach Doppelklick werden diese Dateien in das systemweite OpenVPN-Konfigurations-Verzeichnis unter Windows entpackt.

Bei jedem Verbindungsaufbau muss auf dem Client das Kennwort eingegeben werden, um den privaten Schlüssel aus der PKCS#12-Datei auslesen zu können.

Import des privaten Schlüssels in Windows-Zertifikatsspeicher des Benutzers

Zur Vereinfachung der OpenVPN-Konfiguration unter Windows ist das hier angebotene selbstextrahierende ZIP-Archiv gedacht. Es enthält den privaten Schlüssel mit dem zugehörigen Zertifikat und das CA-Zertifikat in einer PKCS#12-Datei. Ferner liegt eine OpenVPN-Konfigurationsdatei mit passenden Einstellungen bei. Nach Doppelklick und Abfrage des Import-Passworts wird der private Schlüssel und das Zertifikat im Windows-Zertifikatsspeicher des Benutzers installiert. Die .ovpn-Datei wird in das systemweite OpenVPN-Konfigurations-Verzeichnis entpackt.

Der Client kann die VPN-Verbindung ohne Eingabe eines Kennworts starten. Wir empfehlen daher, serverseitig die Benutzerauthentifizierung zu aktivieren.

Privater-Schlüssel kennwortgeschützt in .ovpn-Datei eingebettet

Ab OpenVPN-Version 2.6 ist im Windows-Client "OpenVPN GUI" Start-Before-Logon (SBL) verfügbar. Wenn es fertig eingerichtet ist, erscheint auf dem Windows-Anmeldebildschirm ein zusätzliches Symbol. Klickt man darauf, kann man schon vor der Anmeldung an Windows die VPN-Verbindung aufbauen. Danach ist es möglich, sich über das VPN direkt an einer Windows-Domäne anzumelden.



In den Einstellungen von "OpenVPN GUI" muss der "Pre-Logon Authentication Provider" (PLAP) aktiviert werden.

Das hier angebotene selbstextrahierende ZIP-Archiv enthält eine OpenVPN-Konfigurationsdatei, in die der verschlüsselte private Schlüssel eingebettet ist. Unter Windows wird diese Datei im systemweiten OpenVPN-Konfigurations-Verzeichnis "config-auto" abgelegt. Ferner wird dort eine Datei mit einem zufälligen Passwort für die interne Kommunikation von OpenVPN erzeugt.

Bei jedem Verbindungsaufbau muss auf dem Client das Kennwort eingegeben werden, um den privaten Schlüssel lesen zu können.

Import des privaten Schlüssels in Windows-Zertifikatsspeicher des Computers

Ab OpenVPN-Version 2.6 ist im Windows-Client "OpenVPN GUI" Start-Before-Logon (SBL) verfügbar. Wenn es fertig eingerichtet ist, erscheint auf dem Windows-Anmeldebildschirm ein zusätzliches Symbol. Klickt man darauf, kann man schon vor der Anmeldung an Windows die VPN-Verbindung aufbauen. Danach ist es möglich, sich über das VPN direkt an einer Windows-Domäne anzumelden.



In den Einstellungen von "OpenVPN GUI" muss der "Pre-Logon Authentication Provider" (PLAP) aktiviert werden.

Das hier angebotene selbstextrahierende ZIP-Archiv enthält den privaten Schlüssel mit dem zugehörigen Zertifikat und das CA-Zertifikat in einer PKCS#12-Datei. Ferner liegt eine OpenVPN-Konfigurationsdatei mit passenden Einstellungen bei. Unter Windows muss das Archiv als Administrator installiert werden. Nach Abfrage des Import-Passworts wird der private Schlüssel und das Zertifikat im Windows-Zertifikatsspeicher des Computers installiert. Die .ovpn-Datei wird in das systemweite OpenVPN-Konfigurations-Verzeichnis "config-auto" abgelegt. Ferner wird dort eine Datei mit einem zufälligen Passwort für die interne Kommunikation von OpenVPN erzeugt.

Der Client kann die VPN-Verbindung ohne Eingabe eines Kennworts starten. Wir empfehlen daher, serverseitig die Benutzerauthentifizierung zu aktivieren.

iOS IPsec Parameter

Hier können Sie einige wenige Parameter des Profils festlegen. Das Profil legt zudem fest, dass bei bestehender VPN-Verbindung die Proxy-Konfiguration über Proxy-Auto-Konfigurationsdatei der SX-GATE erfolgen soll.

SX-GATE Internet-IP oder -Servername

Geben Sie hier bitte den DNS-Namen oder die IP-Adresse an, unter der SX-GATE vom Client aus erreichbar ist.

XAUTH Login des Benutzers

Geben Sie hier den Benutzernamen an, mit dem sich der Benutzer am SX-GATE anmelden muss. Wenn Sie das Feld leer lassen, wird der Name beim Verbindungsaufbau abgefragt.

iOS IPsec Profil***iOS Profil für IPsec VPN***

Über diese Schaltfläche lässt sich ein iOS Profil für die IPsec VPN-Verbindung herunterladen. Neben den Konfigurationseinstellungen enthält das Profil Zertifikate und einen privaten Schlüssel im PKCS#12-Format.

Während der Installation des Profils wird das Passwort abgefragt, mit dem die PKCS#12-Datei geschützt ist.

Parameter für SX-GATE Außenstelle***Internet-IP oder -Servername des zentralen SX-GATES***

Geben Sie hier bitte den DNS-Namen oder die IP-Adresse an, unter der der lokale SX-GATE von der Außenstelle aus erreichbar ist.

IPsec Server-Verbindung

Wählen Sie hier bitte die IPsec Verbindung aus, mit der sich die Außenstelle verbinden soll. Dies ist erforderlich, um der Außenstelle die passenden Einstellungen zu übermitteln.

Konfigurationspaket für SX-GATE Außenstelle***Installationspaket für SX-GATE Außenstelle***

Zur Vereinfachung der Konfiguration einer VPN-Verbindungen mit einem anderen SX-GATE ist das hier angebotene Tar-Archiv gedacht. Es enthält den privaten Schlüssel mit dem zugehörigen Zertifikat und das CA-Zertifikat in einer PKCS#12-Datei. Ferner liegt eine Konfigurationsdatei mit passenden Einstellungen bei. Importieren Sie diese Datei auf dem anderen SX-GATE.

iOS Exchange Parameter***SX-GATE Internet-IP oder -Servername***

Geben Sie hier bitte den DNS-Namen oder die IP-Adresse an, unter der SX-GATE vom Client aus erreichbar ist.

Windows Login des Benutzers

Geben Sie hier den Windows-Benutzernamen inkl. der Windows-Domäne im Format "login@domäne" an. Wenn Sie das Feld leer lassen, wird die Adresse bei der Installation des Profils abgefragt.

Exchange E-Mail Adresse des Benutzers

Geben Sie hier die E-Mail Adresse des Exchange-Benutzers an. Wenn Sie das Feld leer lassen, wird die Adresse bei der Installation des Profils abgefragt.

iOS Exchange Profil***iOS Profil für Zugriff auf Exchange***

Über diese Schaltfläche lässt sich ein iOS Profil für den Zugriff auf Exchange herunterladen. Neben den Konfigurationseinstellungen enthält das Profil Zertifikate und einen privaten Schlüssel im PKCS#12-Format, mit denen sich das iOS am SX-GATE Reverse-Proxy anmelden muss.

Während der Installation des Profils wird sowohl das Passwort abgefragt mit dem die PKCS#12-Datei geschützt ist, als auch das Kennwort für die Benutzeranmeldung am Exchange-Server.

Unter "Schlüsselbund" installieren

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Name des Schlüssels

Geben Sie hier einen Namen für den Schlüssel ein. Dieser Name dient ausschließlich zur Identifikation des Schlüssels und kann daher frei vergeben werden.

Lokales VPN-Server Zertifikat erstellen

Mit Hilfe dieser Funktion erstellen bzw. erneuern Sie das Zertifikat für SX-GATEs eigenen VPN-Server. Das neue Zertifikat ist bis zu sechs Jahre gültig und wird von der SX-GATE-CA signiert.

Neues VPN-Server Zertifikat ausstellen

In dieser Maske geben Sie die Zertifikatsdaten für das Zertifikat ein.

CN

Sofern SX-GATE im Internet über eine feste IP-Adresse oder einen bestimmten DNS-Namen verfügt, sollten Sie diesen hier angeben. Wählen Sie sonst einen anderen möglichst eindeutigen Bezeichner für Ihren SX-GATE.

Alternative Bezeichner

Bei der Überprüfung, ob das Server-Zertifikat auch tatsächlich zum angesprochenen Server gehört, werten viele Clients bevorzugt dieses Feld aus. Sie können hier alle Namen oder auch IP-Adressen eintragen, unter denen der IPsec-Server aus dem Internet angesprochen wird.



Die Angabe ist zwingend erforderlich, wenn MacOS VPN-Clients angebunden werden sollen. MacOS-Clients erwarten, dass im alternativen Bezeichner des Server-Zertifikats die im MacOS-Client konfigurierte Server-Adresse enthalten ist.

Zertifizierungsanfrage

Die Zertifizierungsanfrage wird mit dem Aufruf dieser Seite erstellt und kann im nächsten Schritt mit Hilfe des CA-Zertifikats signiert werden.

Verwendungszweck: Server Authentifizierung

Die Aktivierung dieses Schalters wird empfohlen. In der Grundkonfiguration prüft der Windows-IPsec-Client, ob das VPN-Server-Zertifikat diesen Wert als "Extended Key Usage" enthält.



Abhängig vom Client und dessen Konfiguration kann es passieren, dass der Client die Verbindung verweigert, wenn dieses Attribut im Server-Zertifikat fehlt.

Zertifikat signieren

Mit dem Aufruf dieser Seite wird das Zertifikat signiert. Beenden Sie den Vorgang mit "Fertigstellen" um den neuen VPN-Server Schlüssel zu installieren.

12.4.1.3 Benutzerdefinierte CAs

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.4.1.3-A Zertifikate.....	185
12.4.1.3-B Verwendung.....	185

Hier können Sie bei Bedarf externe oder lokale CA-Zertifikate hochladen, wenn einzelne SX-GATE-Dienste diese zur Verifikation von Zertifikaten benötigen. Wählen Sie diese anschließend in der Konfiguration des jeweiligen Dienstes aus.

12.4.1.3-A Zertifikate

CA-Zertifikat bzw. -Bündel exportieren

Hier haben Sie die Möglichkeit, das Zertifikat bzw. das Zertifikats-Bündel herunterzuladen. Das Dateiformat ist PEM.



Zertifikate auf die unter "Enthaltene CA-Zertifikate bzw. -Bündel" verwiesen wird, sind nicht Bestandteil des Exports.

CA-Zertifikat oder CA-Bündel importieren

Hier können Sie CA-Zertifikate im PEM-Format hochladen. Im PEM-Format liegt das Zertifikat in base64-kodierter Form und damit als einfache Text-Datei vor. Das Zertifikat ist mit den Begrenzungszeilen "-----BEGIN CERTIFICATE-----" und "-----END CERTIFICATE-----" umgeben. Text außerhalb dieser Begrenzer wird ignoriert. Durch einfaches Aneinanderhängen können Sie mehrere CA-Zertifikate in einer Datei zusammenfassen und als "CA-Bündel" hochladen.



Sie sollten hier ausschließlich Stammzertifikate (Root-CAs) hochladen. Ob es sich tatsächlich um Stamm- bzw. CA-Zertifikate handelt, wird von der Administrationsoberfläche nicht geprüft.

Enthaltene CA-Zertifikate bzw. -Bündel

Nutzen Sie diesen Eingabebereich, um mehrere CA-Zertifikate oder -Bündel zu kombinieren.

12.4.1.3-B Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

12.4.2 Schlüsselbund

In diesem Menü werden alle Schlüsselpaare verwaltet, die von den verschiedenen Server-Diensten dieses SX-GATES genutzt werden. Ein Schlüsselpaar besteht dabei grundsätzlich aus einem privaten Schlüssel und dem zugehörigen öffentlichen

Schlüssel. Der öffentliche Schlüssel liegt dabei in Form eines Zertifikats vor, ist also von einer Zertifizierungsstelle (CA) unterschrieben worden.



Private Schlüssel sind aus Sicherheitsgründen nicht Bestandteil des SX-GATE-Backups. Nutzen Sie die Export-Funktion beim jeweiligen Schlüsselpaar um ein Backup zu erstellen.

Sie können hier sowohl Schlüsselpaare mit Zertifikaten von öffentlichen Zertifizierungsstellen also auch Schlüsselpaare mit einem Zertifikat der SX-GATE-CA hinterlegen. Als einfache Platzhalter dienen Schlüsselpaare mit selbstsigniertem Zertifikat. Dazu gehört auch das vordefinierte Schlüsselpaar "DUMMY", das im Auslieferungszustand als Standardzertifikat in allen Server-Diensten konfiguriert ist. Das Schlüsselpaar "DUMMY" dient auch als Fallback, wenn ein Schlüsselpaar unvollständig ist, also der private Schlüssel fehlt. Bitte beachten Sie, dass von selbstsignierten Zertifikaten keine Backups angefertigt werden können.

Um ein Schlüsselpaar für einen bestimmten SX-GATE-Server auszuwählen, wechseln Sie bitte in das Menü des jeweiligen Server-Dienstes.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Name des Schlüssels

Geben Sie hier einen Namen für den Schlüssel ein. Dieser Name dient ausschließlich zur Identifikation des Schlüssels und kann daher frei vergeben werden.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.4.2.1-A Aktuelles Schlüsselpaar.....	187
12.4.2.1-B Vorheriges Schlüsselpaar.....	195
12.4.2.1-C Verwendung.....	195

Beantragungsmethode

Wählen Sie aus, wie Sie das neue Zertifikat beantragen wollen.

manuell

In dieser Variante müssen Sie die Zertifizierungsanfrage (Certificate Signing Request, CSR) manuell als Datei oder per Kopieren-und-Einfügen an die CA übermitteln. Sobald die CA das Zertifikat ausgestellt hat, müssen Sie dieses als Datei oder per Kopieren-und-Einfügen in den SX-GATE importieren.

ACME (z.B. Let's Encrypt)

Wählen Sie diese Variante um Zertifikate automatisch über das ACME-Protokoll auszustellen und zu erneuern. Unterstützt wird derzeit nur die HTTP-Autorisierung. Die SX-GATE Firewall muss dazu eingehende HTTP-Verbindungen an einen HTTP-Port seines Reverse-Proxies weiterleiten, der wiederum für die ACME HTTP-Autorisierung konfiguriert sein muss.

Managed PKI

Diese Variante ist nur sinnvoll, wenn sehr viele Zertifikate benötigt werden (z.B. bei Nutzung des SX-GATE S/MIME-Gateways). Auch hier werden Zertifikate automatisch ausgestellt und erneuert.



Aktuell unterstützt SX-GATE nur die CA SwissSign. Gerne ergänzen wir hier weitere CAs. Wir benötigen dazu eine Schnittstellenbeschreibung und einen Testzugang.

12.4.2.1-A Aktuelles Schlüsselpaar

Auf diesem Reiter (Tab) wird das derzeit aktive Schlüsselpaar verwaltet. Wenn Sie das aktuelle Schlüsselpaar ersetzen (z.B. durch Ausstellen eines neuen Schlüsselpaares oder Einspielen des Backups eines Schlüsselpaares), wird das alte Schlüsselpaar automatisch gesichert. Ein eventuell bereits zuvor gesichertes Schlüsselpaar wird dabei überschrieben. Es wird also nur eine Generation vorheriger Schlüsselpaare gesichert. Sobald ein gesichertes Schlüsselpaar zur Verfügung steht, wird der Reiter "Vorheriges Schlüsselpaar" angezeigt.



Das vorherige Schlüsselpaar wird ggf. vom SX-GATE S/MIME-Gateway zur Entschlüsselung genutzt.



Private Schlüssel sind aus Sicherheitsgründen nicht Bestandteil des SX-GATE-Backups. Insbesondere bei gekauften Zertifikaten sollten Sie daher ein Backup des Schlüsselpaares erstellen.

MPKI-Profil

Die Profile werden im Menü "System > Zertifikatsverwaltung > MPKI-Profile" erstellt und beinhalten die Zugangsdaten zur Kommunikation mit der CA, das gewünschte Zertifikatsprodukt und weitere Parameter.

Manuelle Verlängerung

Das Zertifikat wird automatisch verlängert, sofern im Profil die automatische Verlängerung aktiviert ist. Sie können hier die automatische Verlängerung für dieses individuelle Zertifikat deaktivieren.

Ausgestelltes Zertifikat importieren

Dieser Assistent wird angezeigt, sobald Sie eine Zertifikatsanfrage an eine externe CA erstellt haben. Sobald Sie das Zertifikat von der CA zurück erhalten haben, können Sie es hier importieren.

Zertifikats-Datei auswählen

Hier wird das Zertifikat importiert, dass Sie auf die Zertifikats-Anfrage hin von der Zertifizierungsstelle erhalten haben. Sowohl das PEM- als auch das DER-Format werden unterstützt.

Zertifikat prüfen

Prüfen Sie hier noch einmal das Zertifikat bevor es installiert wird.

Lesen Sie bitte weiter bei [Zertifikat installieren](#)

CA-Zertifikat auswählen

Das Zertifikat muss ergänzt werden um die Zertifikate eventueller Zwischen-Zertifizierungsstellen (Intermediate CAs) bis zum Wurzel-Zertifikat (Root CA). Alle Zertifikate müssen im PEM- oder im DER-Format vorliegen. Sie erhalten die Zertifikate von Ihrer Zertifizierungsstelle.

CA-Zertifikat prüfen

Das hochgeladene Zertifikat wird an die Zertifizierungs-Kette angehängt.

Lesen Sie bitte weiter bei [CA-Zertifikat auswählen](#)

Zertifikat installieren

Der Import-Vorgang ist abgeschlossen. Das Zertifikat kann jetzt installiert werden.

Zertifikats-Anfrage löschen

Hiermit können Sie die Zertifikats-Anfrage verwerfen.



Beachten Sie bitte, dass der private Schlüssel dadurch unwiderbringlich vernichtet wird.

Zertifikat exportieren

Hier haben Sie die Möglichkeit, das Zertifikat herunterzuladen. Das Zertifikat ist der von der CA signierte öffentliche Schlüssel. Das Dateiformat ist PEM.



Dies ist keine Backup-Funktion, da der private Schlüssel nicht enthalten ist.

ACME-Server

Falls Zertifikate automatisiert über das ACME-Protokoll abgerufen werden, wird hier der Name des ACME-Servers angezeigt.

Zertifikatsabruf über ACME konfigurieren

ACME Einstellungen

Legen Sie hier fest, von welcher CA und mit welchen Daten das Zertifikat bezogen werden soll.

ACME-Server

Tragen Sie hier den Server ein, von dem Sie die Zertifikate automatisiert beziehen wollen. Sofern die CA eine Testumgebung zur Verfügung stellt, empfehlen wir Ihnen, das erstmalige Ausstellen eines Zertifikats für einen Servernamen zunächst in der Testumgebung durchzuführen. Die Anzahl der erlaubten Vorgänge ist in der Produktivumgebung oft begrenzt, so dass Sie bei Problemen eventuell kurzzeitig gesperrt werden.

E-Mail Kontaktadresse für CA

Manche CAs fragen nach der E-Mail-Adresse eines Administrators wenn man sich dort registriert.

CN

Stellen Sie das Zertifikat auf den DNS-Namen aus, über den aus dem Internet auf den Dienst zugegriffen wird.



Zertifikate für IP-Adressen sind von den uns bekannten CAs nicht über das ACME-Protokoll verfügbar.

Alternative Bezeichner

Bei der Überprüfung, ob das Server-Zertifikat auch tatsächlich zum angesprochenen Server gehört, werten die meisten Clients bevorzugt dieses Feld aus. Sie können hier alle Namen eintragen, unter denen der Server angesprochen wird.



Wildcard-Zertifikate und IP-Adressen in Zertifikaten sind von den uns bekannten CAs nicht über das ACME-Protokoll verfügbar.

Schlüsselstärke

Alte Systeme wie z.B. Windows XP vor SP3 unterstützen ggf. nur Schlüssel mit max. 2048 Bit.

Zertifikat über ACME abrufen / erneuern

Mit dieser Funktion rufen Sie ein Zertifikat mit den zuvor festgelegten Parametern über das ACME-Protokoll ab.

Registrierung prüfen

Zunächst registriert sich SX-GATE beim ACME-Server. Üblicherweise müssen Sie dabei auch die Vertragsbedingungen der CA zur Kenntnis nehmen und akzeptieren.

Zertifikat neu ausstellen

Starten Sie hier den Abruf eines neuen Zertifikats.



Um ein Zertifikat der lokalen SX-GATE-CA zu erhalten, stellen Sie dieses bitte im Menü "System > Zertifikatsverwaltung > CA Zertifikate" aus. Folgen Sie dazu dem Link "Zertifikate" in der "SX-GATE-CA"-Zeile. Am Ende dieses Prozesses wird Ihnen angeboten, das neue Schlüsselpaar im "Schlüsselbund" zu installieren.

Aktion auswählen

Bitte wählen Sie die gewünschte Aktion

Das Zertifikat kann auf verschiedene Arten ausgestellt werden:

Zertifikats-Anfrage an externe CA erstellen

Um sich ein Zertifikat von einer öffentlichen Zertifizierungsstelle (CA) ausstellen zu lassen, müssen Sie eine Zertifikats-Anfrage (Certificate Signing Request, CSR) einreichen. Dazu generiert SX-GATE zunächst ein RSA-Schlüsselpaar und fragt die Daten für die Zertifikats-Anfrage ab. Anschließend können Sie die Zertifikats-Anfrage als Datei herunterladen oder als Text herauskopieren und an die CA weiterleiten. Ein Import-Assistent ist nun verfügbar, über den Sie das Zertifikat einspielen können, sobald Sie es von der CA erhalten.

Von SX-GATE-CA signiertes Zertifikat erstellen

Von der SX-GATE-CA ausgestellte Zertifikate eignen sich für die Verwendung in einem geschlossenen Nutzerkreis wie z.B. VPN für die eigenen Mitarbeiter.

Selbstsigniertes Zertifikat erstellen

Ein selbstsigniertes Zertifikat ist in der Regel höchstens für Testbetrieb sinnvoll. Das Zertifikat erhält eine Gültigkeitsdauer von einem Jahr.



Dieses Zertifikat wird nicht von der SX-GATE CA signiert.

Bitte wählen Sie die gewünschte Aktion

- Zertifikats-Anfrage an externe CA erstellen
Lesen Sie bitte weiter bei [Zertifikats-Anfrage erstellen](#) (S. 191)
- Von SX-GATE-CA signiertes Zertifikat erstellen
Lesen Sie bitte weiter bei [Von SX-GATE-CA signiertes Zertifikat erstellen](#) (S. 191)
- Selbstsigniertes Zertifikat erstellen
Lesen Sie bitte weiter bei [Zertifikatsdaten](#) (S. 192)

Von SX-GATE-CA signiertes Zertifikat erstellen

Zertifikate der lokalen SX-GATE-CA erhalten Sie über das Menü "CA Zertifikate". Folgen Sie dort dem Link "Zertifikate" in der "SX-GATE-CA"-Zeile. Wählen Sie am Ende des Zertifikats-Ausstellungsprozesses bitte 'Unter "Schlüsselbund" installieren'.

Zertifikats-Anfrage an externe CA erstellen

Zertifikats-Anfrage erstellen

In diesem Bereich geben Sie die Zertifikatsdaten für das neue Zertifikat ein.

CN

Stellen Sie das Zertifikat auf die Adresse aus, über die üblicherweise aus dem Internet auf den Dienst zugegriffen wird. Dies ist in der Regel der Internet DNS-

Name des SX-GATEs. Auch die Erstellung eines Wildcard-Zertifikats ist möglich (z.B. *.example.com), dies ist jedoch in der Regel mit deutlich höheren Kosten verbunden.

Alternative Bezeichner

Bei der Überprüfung, ob das Server-Zertifikat auch tatsächlich zum angesprochenen Server gehört, werten viele Clients bevorzugt dieses Feld aus. Sie können hier alle Namen oder auch IP-Adressen eintragen, unter denen der Server angesprochen wird. Auch Wildcard-Zertifikate (z.B. *.example.com) sind möglich.



Nicht jede CA übernimmt diese Daten aus der Zertifikats-Anfrage. Multidomain- und Wildcard-Zertifikate sind häufig deutlich teurer. Bitte klären Sie dies ab, bevor Sie das Zertifikat beantragen.

Zertifikats-Anfrage

Die Zertifikats-Anfrage wird mit dem Aufruf dieser Seite erstellt.

Selbstsigniertes Zertifikat erstellen

Zertifikatsdaten

Ein selbstsigniertes Zertifikat ist in der Regel höchstens für Testbetrieb sinnvoll.

Zertifikat erstellen

Das selbstsignierte Zertifikat wurde erstellt.

Zertifikat aktualisieren (Re-Issue)

Diese Funktion wird nur sehr selten benötigt. Es wird dabei kein neues Schlüsselpaar generiert sondern das alte weiterverwendet. Die Zertifizierungsstelle stellt Ihnen lediglich ein neu signiertes Zertifikat zur Verfügung.



Falls das alte Zertifikat demnächst abläuft, empfehlen wir ein neues Schlüsselpaar zu generieren. Stellen Sie dazu über den Assistenten "Zertifikat neu ausstellen" eine neue Zertifikats-Anfrage.

Zertifikats-Datei auswählen

Hier wird das neue Zertifikat importiert, dass Sie von der Zertifizierungsstelle erhalten haben. Sowohl das PEM- als auch das DER-Format werden unterstützt.

Zertifikat prüfen

Prüfen Sie hier noch einmal das Zertifikat bevor es installiert wird.

Lesen Sie bitte weiter bei [Zertifikat installieren](#)

CA-Zertifikat auswählen

Das Zertifikat muss ergänzt werden um die Zertifikate eventueller Zwischen-Zertifizierungsstellen (Intermediate CAs) bis zum Wurzel-Zertifikat (Root CA). Alle Zertifikate müssen im PEM- oder im DER-Format vorliegen. Sie erhalten die Zertifikate von Ihrer Zertifizierungsstelle.

CA-Zertifikat prüfen

Das hochgeladene Zertifikat wird an die Zertifizierungs-Kette angehängt.

Lesen Sie bitte weiter bei [CA-Zertifikat auswählen](#)

Zertifikat installieren

Der Import-Vorgang ist abgeschlossen. Das Zertifikat kann jetzt installiert werden.

Zertifikatsabruf per MPKI konfigurieren

Zertifikats-Anfrage erstellen

In diesem Bereich geben Sie die Zertifikatsdaten für das neue Zertifikat ein. Voreinstellungen können im Profil hinterlegt werden.

CN

Stellen Sie das Zertifikat auf die Adresse aus, über die üblicherweise aus dem Internet auf den Dienst zugegriffen wird. Dies ist in der Regel der Internet DNS-Name des SX-GATES. Auch die Erstellung eines Wildcard-Zertifikats ist möglich (z.B. *.example.com), dies ist jedoch in der Regel mit deutlich höheren Kosten verbunden. Bei S/MIME-Zertifikaten wird die E-Mail-Adresse oder der Name des Besitzers eingetragen.

Alternative Bezeichner

Bei der Überprüfung, ob das Server-Zertifikat auch tatsächlich zum angesprochenen Server gehört, werten viele Clients bevorzugt dieses Feld aus. Sie können hier alle Namen eintragen, unter denen der Server angesprochen wird. Auch Wildcard-Zertifikate (z.B. *.example.com) sind möglich.



Nicht jede CA übernimmt diese Daten aus der Zertifikats-Anfrage. Multidomain- und Wildcard-Zertifikate sind häufig deutlich teurer. Bitte klären Sie dies ab, bevor Sie das Zertifikat beantragen.

Zertifikat widerrufen**Grund**

Geben Sie hier bitte den Grund des Widerrufs an.

Grund

Wählen Sie bitte den Grund des Widerrufs aus.

Backup des Schlüsselpaars importieren

Ein im PKCS#12-Format vorliegendes Schlüsselpaar kann hier importiert werden.

Datei auswählen

Wählen Sie hier die PKCS#12-Datei mit dem Schlüsselpaar aus und geben Sie das Kennwort ein, mit dem die Datei geschützt ist.

Zertifikat prüfen

Prüfen Sie hier noch einmal das Zertifikat, bevor es installiert wird.

Lesen Sie bitte weiter bei [Zertifikat installieren](#)

CA-Zertifikat auswählen

Das Zertifikat muss ergänzt werden um die Zertifikate eventueller Zwischen-Zertifizierungsstellen (Intermediate CAs) bis zum Wurzel-Zertifikat (Root CA). Alle Zertifikate müssen im PEM- oder im DER-Format vorliegen. Sie erhalten die Zertifikate von Ihrer Zertifizierungsstelle.

CA-Zertifikat prüfen

Das hochgeladene Zertifikat wird an die Zertifizierungs-Kette angehängt.

Lesen Sie bitte weiter bei [CA-Zertifikat auswählen](#)

Zertifikat installieren

Der Import-Vorgang ist abgeschlossen. Das Zertifikat kann jetzt installiert werden.

Backup des Schlüsselpaars erstellen

Das Schlüsselpaar kann zu Sicherungszwecken im PKCS#12-Format exportiert werden. Bitte beachten Sie, dass dieser Export also auch den privaten Schlüssel enthält, der unbedingt geheim bleiben muss.



Ohne dieses Backup kann ein gekauftes Zertifikat nicht wiederhergestellt werden.

12.4.2.1-B Vorheriges Schlüsselpaar

Nach der Aktualisierung eines Schlüsselpaars wird auf diesem Reiter (Tab) das zuvor genutzte Schlüsselpaar angezeigt. Das Backup soll in erster Linie vor versehentlichem Verlust schützen.



Das SX-GATE S/MIME-Gateway nutzt das alte Schlüsselpaar ggf. aktiv zur Entschlüsselung von eingehenden E-Mails, die noch mit dem alten Zertifikat verschlüsselt wurden.



Es wird nur eine Generation alter Schlüssel auf dem Gerät gesichert. Das vorherige Schlüsselpaar ist kein Bestandteil des SX-GATE-Backups.

Backup des vorherigen Schlüsselpaars erstellen

Das Schlüsselpaar kann zu Sicherungszwecken im PKCS#12-Format exportiert werden. Bitte beachten Sie, dass dieser Export also auch den privaten Schlüssel enthält, der unbedingt geheim bleiben muss.



Ohne dieses Backup kann ein gekauftes Zertifikat nicht wiederhergestellt werden.

Vorheriges und aktuelles Schlüsselpaar tauschen

Um das vorherige Schlüsselpaar zu reaktivieren, können Sie es mit dem aktuellen Schlüsselpaar tauschen.

12.4.2.1-C Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.4.2.2-A Ed25519-Schlüssel.....	196
12.4.2.2-B Vorheriges Schlüsselpaar.....	196
12.4.2.2-C Verwendung.....	197

12.4.2.2-A Ed25519-Schlüssel

Öffentlichen Schlüssel herunterladen

Hier haben Sie die Möglichkeit, den öffentlichen Schlüssel herunterzuladen.



Dies ist keine Backup-Funktion, da der private Schlüssel nicht enthalten ist.

Backup des privaten Schlüssels importieren

Ein Ed25519-Schlüssel im Format OpenSSH kann hier importiert werden.

Schlüssel installieren

Der Import-Vorgang ist abgeschlossen. Der Schlüssel kann jetzt installiert werden.

Backup des privaten Schlüssels erstellen

Der private Schlüssel kann zu Sicherungszwecken im OpenSSH-Format exportiert werden. Bitte beachten Sie, dass der private Schlüssel unbedingt geheim bleiben muss.

12.4.2.2-B Vorheriges Schlüsselpaar

Nach der Aktualisierung eines Schlüsselpaars wird auf diesem Reiter (Tab) das zuvor genutzte Schlüsselpaar angezeigt. Das Backup soll in erster Linie vor versehentlichem Verlust schützen.

Backup des privaten Schlüssels erstellen

Der private Schlüssel kann zu Sicherungszwecken im OpenSSH-Format exportiert werden. Bitte beachten Sie, dass der private Schlüssel unbedingt geheim bleiben muss.

Vorheriges und aktuelles Schlüsselpaar tauschen

Um das vorherige Schlüsselpaar zu reaktivieren, können Sie es mit dem aktuellen Schlüsselpaar tauschen.

12.4.2.2-C Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.4.2.3-A X25519-Schlüssel.....	197
12.4.2.3-B Vorheriges Schlüsselpaar.....	198
12.4.2.3-C Verwendung.....	198

12.4.2.3-A X25519-Schlüssel

Backup des privaten Schlüssels importieren

Ein zuvor aus einem SX-GATE exportierter X25519-Schlüssel kann hier importiert werden. Es handelt sich um ein spezielles, verschlüsseltes Backup-Format.



Unverschlüsselte private X25519-Schlüssel, wie sie der Wireguard-Befehl "genkey" erzeugt, können nicht importiert werden.

Schlüssel installieren

Der Import-Vorgang ist abgeschlossen. Der Schlüssel kann jetzt installiert werden.

Backup des privaten Schlüssels erstellen

Der private Schlüssel kann zu Sicherungszwecken exportiert werden. Zum Schutz wird der Schlüssel mit einem Kennwort AES-256 verschlüsselt. Bitte beachten Sie, dass der private Schlüssel unbedingt geheim bleiben muss.

12.4.2.3-B Vorheriges Schlüsselpaar

Nach der Aktualisierung eines Schlüsselpaars wird auf diesem Reiter (Tab) das zuvor genutzte Schlüsselpaar angezeigt. Das Backup soll in erster Linie vor versehentlichem Verlust schützen.

Backup des privaten Schlüssels erstellen

Der private Schlüssel kann zu Sicherungszwecken im OpenSSH-Format exportiert werden. Bitte beachten Sie, dass der private Schlüssel unbedingt geheim bleiben muss.

Vorheriges und aktuelles Schlüsselpaar tauschen

Um das vorherige Schlüsselpaar zu reaktivieren, können Sie es mit dem aktuellen Schlüsselpaar tauschen.

12.4.2.3-C Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.4.2.4-A RSA-Schlüssel.....	198
12.4.2.4-B Vorheriges Schlüsselpaar.....	200
12.4.2.4-C Verwendung.....	200

12.4.2.4-A RSA-Schlüssel

Öffentlicher Schlüssel (DKIM-Format)

Für DKIM muss der öffentliche Schlüssel im DNS der zu signierenden Domain hinterlegt werden. Der Name des DNS-Eintrags setzt sich zusammen aus dem Selektor und dem Text "_domainkey". Beim Selektor handelt es sich um einen beliebigen Bezeichner Ihrer Wahl, der den DKIM-Schlüssel identifizieren soll. Der erforderliche Typ des DNS-Eintrags ist "TXT". Als Wert geben Sie den hier angezeigten Text ein.



Abhängig von der Verwaltungsoberfläche Ihres DNS-Servers kann es notwendig sein, diesen sehr langen Eintrag in mehrere Teile mit jeweils maximal 255 Zeichen aufzubrechen (z.B. dkim._domainkey TXT "Teil1" "Teil2" ... "TeilX").

Wenn Sie z.B. als Selektor den Text "dkim" verwenden wollen und die Domain "example.com" signiert werden soll, würde der zugehörige DNS-Eintrag "dkim._domainkey.example.com." heißen.

Der Schlüssel sollte regelmäßig erneuert werden. Ersetzen Sie dazu bitte nicht das bestehende Schlüsselpaar über "Neuen Schlüssel generieren". Legen Sie stattdessen einen neuen Eintrag unter "Schlüsselbund" an und hinterlegen Sie den neuen öffentlichen Schlüssel unter einem anderen Selektor im DNS.



Wenn Sie den DKIM-Schlüssel jährlich ändern, könnten Sie z.B. die Jahreszahl in den Selektor aufnehmen.

Nachdem Sie den öffentlichen Schlüssel im DNS verfügbar gemacht haben, können Sie DKIM für die entsprechende Domain im Menü "Module > Mail-Server > Domains" aktivieren.

Öffentlichen Schlüssel herunterladen (SSH-Format)

Hier haben Sie die Möglichkeit, den öffentlichen Schlüssel herunterzuladen.



Dies ist keine Backup-Funktion, da der private Schlüssel nicht enthalten ist.

Backup des privaten Schlüssels importieren

Ein RSA-Schlüssel im Format OpenSSH, PEM oder PKCS#8 kann hier importiert werden.

Schlüssel installieren

Der Import-Vorgang ist abgeschlossen. Der Schlüssel kann jetzt installiert werden.

Backup des privaten Schlüssels erstellen

Der private Schlüssel kann zu Sicherungszwecken im OpenSSH-Format exportiert werden. Bitte beachten Sie, dass der private Schlüssel unbedingt geheim bleiben muss.

12.4.2.4-B Vorheriges Schlüsselpaar

Nach der Aktualisierung eines Schlüsselpaars wird auf diesem Reiter (Tab) das zuvor genutzte Schlüsselpaar angezeigt. Das Backup soll in erster Linie vor versehentlichem Verlust schützen.

Backup des privaten Schlüssels erstellen

Der private Schlüssel kann zu Sicherungszwecken im OpenSSH-Format exportiert werden. Bitte beachten Sie, dass der private Schlüssel unbedingt geheim bleiben muss.

Vorheriges und aktuelles Schlüsselpaar tauschen

Um das vorherige Schlüsselpaar zu reaktivieren, können Sie es mit dem aktuellen Schlüsselpaar tauschen.

12.4.2.4-C Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

12.4.3 MPKI-Profile

Viele CAs bieten als "Managed PKI" (MPKI) eine Schnittstelle an, über die automatisiert Zertifikate gekauft werden können. Sinnvoll ist dies, wenn sehr viele Zertifikate benötigt werden, wie z.B. bei Nutzung des SX-GATE S/MIME-Gateways.



Sofern Ihre Wunsch-CA vom SX-GATE noch nicht unterstützt wird, benötigen wir eine Schnittstellenbeschreibung und einen Testzugang um die CA verfügbar zu machen.

In diesem Menü legen Sie Profile an, in denen die Einstellungen zusammengefasst sind, um Zertifikate eines bestimmten Typs von einer bestimmten CA abzurufen.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann

der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Profilname

Das Profil repräsentiert die Einstellungen, um ein bestimmtes Zertifikatsprodukt bei einer bestimmten CA einzukaufen. Wenn Sie sich dazu entscheiden, im "Schlüsselbund" ein Zertifikat über eine MPKI-Schnittstelle abzurufen, müssen Sie dort das gewünschte Profil anhand des Profilnamens auswählen. Sie können den Profilnamen frei wählen.

A profile represents the settings to buy a specific certificate product from a specific CA. If you decide to use an MPKI interface to get a certificate for the "Schlüsselbund", you must select a profile by its name there. You can choose the profilename freely.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.4.3-A CA Einstellungen.....	201
12.4.3-B Standardwerte.....	202
12.4.3-C Verwendung.....	202

12.4.3-A CA Einstellungen

Auf diesem Reiter (Tab) legen Sie die CA fest und wählen das gewünschte Zertifikats-Produkt aus.

API Auswahl

Sofern Sie Zugang zur Testumgebung haben, empfehlen wir dringend, zunächst den Zertifikatsabruf über die Testumgebung einzurichten, da hier in der Regel keine Kosten entstehen. Wechseln Sie auf die Produktivumgebung, sobald alles reibungslos funktioniert.

Aktuell unterstützen wir nur SwissSign. Gerne ergänzen wir hier weitere CAs. Wir benötigen dazu eine Schnittstellenbeschreibung und einen Testzugang.

Login

Tragen Sie hier die Zugangsdaten ein, die Sie von der CA erhalten haben, um sich an der MPKI anzumelden.

Automatisch erneuern

Aktivieren Sie diese Option, um Zertifikate kurz vor Ablauf automatisch zu verlängern.



In den Einstellungen der einzelnen Zertifikate können Sie die automatisch Verlängerung individuell deaktivieren.



Durch die automatische Verlängerung entstehen in der Regel Kosten!

Verlängerung

Legen Sie hier fest, wieviele Tage vor Ablauf ein Zertifikat erneuert werden soll, sofern die automatische Verlängerung aktiviert ist.

Ausgewähltes Produkt

Hier wird Ihnen das ausgewählte Zertifikatsprodukt angezeigt.

Produkt auswählen

Wählen Sie hier das Zertifikatsprodukt aus, das über dieses Profil bestellt werden soll.



Sollten Sie unterschiedliche Zertifikatsprodukte benötigen, müssen Sie für jedes ein eigenes Profil anlegen.

12.4.3-B Standardwerte

Auf diesem Reiter (Tab) legen Sie Standardwerte für die Felder und Eigenschaften der Zertifikate fest, die mit diesem Profil verknüpft sind. Sie können diese Werte in den individuellen Einstellungen des jeweiligen Zertifikats überschreiben.

12.4.3-C Verwendung

Diese Liste zeigt an, in welchen Einstellungen die Definition derzeit verwendet wird.

12.5 Backup

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.5-A Aktionen.....	203
12.5-B Systembackup.....	205
12.5-C Userbackup.....	208
12.5-D Mailbackup.....	210
12.5-E CA-Schlüssel.....	212
12.5-F Schlüsselbund-Backup.....	213

12.5-A Aktionen

Backup einspielen

Generell ist es vor dem Zurückschreiben eines Backups empfehlenswert, zuvor eine Sicherung der momentanen Einstellungen durchzuführen, da die aktiven Einstellungen mit denen aus dem Backup überschrieben werden.



Die Handhabung von Mailbackups unterscheidet sich. Bitte beachten Sie dazu die folgenden Hinweise.

Eine Mailbackup-Datei enthält sowohl alle E-Mail-Ordner als auch die Daten aus den Heimat-Verzeichnissen der Benutzer. Sofern die SX-GATE-Groupware genutzt wird, sind ferner die Daten aus der Groupware wie Adressbücher, Kalender, Mail-Filter und sonstige Einstellungen im Backup enthalten.

Das Mailbackup kann sehr groß werden. Bei der Übertragung des Backups im Ganzen kann es zu langen Wartezeiten kommen, ggf. wird die Datei auch aufgrund ihrer Größe vom Administrations-Server abgelehnt. Insbesondere wenn nur einzelne Konten restauriert werden sollen, empfiehlt es sich daher, das Mailbackup mit einem Entpacker für ZIP-Dateien zu öffnen.



Es können nur unveränderte .rbu-Dateien an den SX-GATE übermittelt werden. Manche Entpacker erlauben es, den Inhalt von Archiven zu verändern und dann das Archiv in veränderter Form abzuspeichern. Das Backup wird dadurch möglicherweise beschädigt und vom SX-GATE nicht mehr akzeptiert.

Das Mailbackup enthält je Benutzer eine eigene .rbu-Datei. Verwenden Sie diese, um das Mailbackup eines einzelnen Benutzers zurückzusichern. Selbst diese Backup-Datei kann jedoch nochmals geöffnet werden. Sie enthält je eine Backup-Datei für das Heimat-Verzeichnis mit den E-Mails ("folders-<Benutzername>.rbu") und ggf. eine für die Groupware-Daten ("sogo-<Benutzername>.rbu") des jeweiligen Benutzers. Auch diese können unabhängig voneinander installiert werden.



Extrahieren und installieren Sie nur die Datei mit Heimat-Verzeichnis und E-Mails bzw. den Groupware-Daten eines Benutzers, wenn der jeweils andere Bereich nicht überschrieben werden darf.

Beim Zurücksichern eines Mailbackups werden die Daten eines Benutzers nur dann restauriert, wenn die folgenden Bedingungen erfüllt sind:

- Der Benutzer existiert auf SX-GATE
- Der Benutzer ist Mitglied der Gruppe "system-mail"

Beim Restaurieren von E-Mails, Groupware-Adressbüchern und Groupware-Kalendern werden die Daten aus dem Backup mit dem aktuellen Bestand zusammengeführt. Bereits gelöschte Elemente werden also wiederhergestellt, neue Einträge bleiben erhalten. In einen anderen Ordner (auch Papierkorb!) verschobene Elemente werden nicht wiederhergestellt, da sie ja noch vorhanden sind.



Es ist trotzdem nicht auszuschließen, dass beim Zusammenführen Duplikate entstehen.



In der Groupware werden Mail-Filter, Abonnements und sonstige Einstellungen mit den Daten aus dem Backup überschrieben.



Beim Einspielen eines Mailbackups aus Versionsreihe 7.0 oder älter wird der E-Mail-Bestand komplett aus dem Backup übernommen. Neue E-Mails gehen verloren!

Konfiguration zurücksetzen

In diesem Bereich haben Sie die Möglichkeit, die Grundkonfiguration des SX-GATE wiederherzustellen.

Art auswählen

Welcher Zustand soll wiederhergestellt werden

Wählen Sie hier bitte aus, welche Bereiche des SX-GATE zurückgesetzt werden sollen.



Wenn Sie den Reset durchführen wird die IP-Adresse des SX-GATE wieder auf den Default-Wert 192.168.0.254 gesetzt.

Standard Systemkonfiguration

Das Zurücksetzen auf diesen Zustand entspricht dem Einspielen des Systembackups eines neuen SX-GATE. Es sind ausschließlich die System-Einstellungen betroffen. Andere Bereiche wie z.B. Benutzer und deren E-Mails, Logdateien und Statistiken bleiben erhalten.

Auslieferungszustand

Im Gegensatz zur vorhergehenden Option wird bei Auswahl dieser Einstellung das System in den Auslieferungszustand zurückgesetzt. Neben den Systemeinstellungen werden dabei insbesondere auch Benutzer, E-Mails, Logdateien und Statistiken gelöscht. Als Kennwort des Administrators wird das Standard-Passwort eingestellt.

Konfigurationseinstellungen anzeigen

Drücken Sie diesen Schalter, um die aktuellen System- und Benutzereinstellungen des SX-GATE anzuzeigen. Es öffnet sich ein neues Browser-Fenster in dem alle Einstellungen für Sie dokumentiert sind. Bitte beachten Sie, das es sich hierbei nicht um ein Backup handelt, sondern lediglich um eine rohe Darstellung der Systemeinstellungen.

12.5-B Systembackup

Diese Abschnitt dient zum Sichern der Systemeinstellungen (Systembackup). Die Einstellungen der Benutzerverwaltung sind in diesem Backup nicht enthalten.



CA-Schlüssel des SX-GATEs sind aus Sicherheitsgründen nicht im Backup enthalten. Sofern das Backup nicht verschlüsselt wird, sind auch keine privaten Schlüssel aus dem Schlüsselbund enthalten. Backups dieser Schlüssel erstellen Sie auf den Reitern (Tabs) "CA-Schlüssel" und "Schlüsselbund-Backup".



Halten Sie die Sicherungsdateien stets unter Verschluss, da sie in falschen Händen auch gelesen werden können!

Systembackup jetzt erstellen

Zum manuellen Erstellen eines Systembackups verwenden Sie bitte diesen Schalter.

Automatisches Systembackup über

Wählen Sie hier das Protokoll für das Backup. Mit Ausnahme von Secure-Copy und SFTP erfolgt die Übertragung des Backups auf das Zielsystem unverschlüsselt. Auf dem Zielsystem wird die Backup-Datei nur dann verschlüsselt abgelegt, wenn Sie ein verschlüsseltes Backup konfiguriert haben. Im Falle eines unverschlüsselten Backups sorgen Sie bitte für einen angemessenen Schutz der Datei.



Die Authentifizierung bei Secure-Copy und SFTP erfolgt über SX-GATEs SSH ED25519-, bzw. RSA-Schlüssel. Bitte konfigurieren Sie den SSH-, bzw. SFTP Server entsprechend.

Passwort für Backupverschlüsselung

Prinzipiell ist ein verschlüsseltes Backup einem unverschlüsselten vorzuziehen.



Bedenken Sie jedoch, dass das Backup nutzlos ist, wenn das Kennwort zum Entschlüsseln nicht mehr bekannt ist!



Ein verschlüsseltes Systembackup enthält auch die privaten Schlüssel aus dem Schlüsselbund, nicht jedoch die SX-GATE CA-Schlüssel.

Benutzername

Geben Sie hier den Benutzernamen an, mit dem sich SX-GATE am Backup-Server anmelden soll.



Beim Backup auf eine Windows-Netzwerkfreigabe müssen Sie hier in der Regel auch den Windows-Domännennamen angeben. Verwenden Sie dabei die Schreibweise "Domäne/Benutzername". Verwenden Sie nicht den unter Windows üblichen Backslash ("\").

Pfad und Dateiname

Geben Sie hier das Verzeichnis und den Dateinamen an, unter dem das Backup gespeichert werden soll. Die Angabe eines Verzeichnisses ist optional. Wird ein Verzeichnis angegeben, so muss dieses jedoch bereits existieren.

In den Dateinamen lassen sich Variablen einbauen. Auf diese Weise werden zuvor erstellte Backups nicht sofort wieder überschrieben. Es stehen u.a. folgende Variablen zur Verfügung:

- %Y: Jahr 4-stellig (z.B. 2001)
- %y: Jahr 2-stellig (z.B. 01)
- %m: Monat (von 01 bis 12)
- %d: Tag (von 01 bis 31)
- %H: Stunde (von 00 bis 23)
- %M: Minute (von 00 bis 59)
- %S: Sekunde (von 00 bis 59)
- %U: Woche des Jahres (Werte von 00 bis 53)
- %w: Tag der Woche (0 für Sonntag bis 6 für Samstag)
- %j: Tag im Jahr (von 001 bis 366)

Wenn als Ziel des Backups z.B.

"backup/%m.%d.rbu"

angegeben wird, enthält der Dateiname stets den aktuellen Monat und Tag. Eine Backup-Datei würde somit erst im folgenden Jahr wieder überschrieben werden.

Erstellt

Um das Backup nicht zu vergessen, nutzen Sie am Besten das automatische Backup. Stellen Sie hier die Häufigkeit sowie die Uhrzeit ein, zu der das Backup durchgeführt werden soll.



Ein monatliches Backup wird jeweils am ersten jedes Monats durchgeführt, ein wöchentliches immer Montags.



Prüfen Sie in regelmäßigen Abständen, ob das Backup noch funktioniert.

Automatisches Systembackup testen

Versucht die aktuelle Systemkonfiguration an den konfigurierten Speicherort zu übertragen.

12.5-C Userbackup

Diese Abschnitt dient zum Sichern der Einstellungen aus dem Menü "System > Benutzerverwaltung".



Halten Sie die Sicherungsdateien stets unter Verschluss, da sie in falschen Händen auch gelesen werden können!

Userbackup jetzt erstellen

Zum manuellen Erstellen eines Userbackups verwenden Sie bitte diesen Schalter.

Automatisches Userbackup über

Wählen Sie hier das Protokoll für das Backup. Mit Ausnahme von Secure-Copy und SFTP erfolgt die Übertragung des Backups auf das Zielsystem unverschlüsselt. Auf dem Zielsystem wird die Backup-Datei nur dann verschlüsselt abgelegt, wenn Sie ein verschlüsseltes Backup konfiguriert haben. Im Falle eines unverschlüsselten Backups sorgen Sie bitte für einen angemessenen Schutz der Datei.



Die Authentifizierung bei Secure-Copy und SFTP erfolgt über SX-GATEs SSH ED25519-, bzw. RSA-Schlüssel. Bitte konfigurieren Sie den SSH-, bzw. SFTP Server entsprechend.

Benutzername

Geben Sie hier den Benutzernamen an, mit dem sich SX-GATE am Backup-Server anmelden soll.



Beim Backup auf eine Windows-Netzwerkfreigabe müssen Sie hier in der Regel auch den Windows-Domänennamen angeben. Verwenden Sie dabei die Schreibweise "Domäne/Benutzername". Verwenden Sie nicht den unter Windows üblichen Backslash ("\").

Pfad und Dateiname

Geben Sie hier das Verzeichnis und den Dateinamen an, unter dem das Backup gespeichert werden soll. Die Angabe eines Verzeichnisses ist optional. Wird ein Verzeichnis angegeben, so muss dieses jedoch bereits existieren.

In den Dateinamen lassen sich Variablen einbauen. Auf diese Weise werden zuvor erstellte Backups nicht sofort wieder überschrieben. Es stehen u.a. folgende Variablen zur Verfügung:

- %Y: Jahr 4-stellig (z.B. 2001)
- %y: Jahr 2-stellig (z.B. 01)
- %m: Monat (von 01 bis 12)
- %d: Tag (von 01 bis 31)
- %H: Stunde (von 00 bis 23)
- %M: Minute (von 00 bis 59)
- %S: Sekunde (von 00 bis 59)
- %U: Woche des Jahres (Werte von 00 bis 53)
- %w: Tag der Woche (0 für Sonntag bis 6 für Samstag)
- %j: Tag im Jahr (von 001 bis 366)

Wenn als Ziel des Backups z.B.

"backup/%m.%d.rbu"

angegeben wird, enthält der Dateiname stets den aktuellen Monat und Tag. Eine Backup-Datei würde somit erst im folgenden Jahr wieder überschrieben werden.

Erstellt

Um das Backup nicht zu vergessen, nutzen Sie am Besten das automatische Backup. Stellen Sie hier die Häufigkeit sowie die Uhrzeit ein, zu der das Backup durchgeführt werden soll.



Ein monatliches Backup wird jeweils am ersten jedes Monats durchgeführt, ein wöchentliches immer Montags.



Prüfen Sie in regelmäßigen Abständen, ob das Backup noch funktioniert.

Automatisches Userbackup testen

Versucht die aktuelle Benutzerkonfiguration an den konfigurierten Speicherort zu übertragen.

12.5-D Mailbackup

Diese Abschnitt dient zum Sichern des Posteingangs, der Heimat-Verzeichnisse und der Groupware-Daten aller Benutzer (Mailbackup). In den Heimat-Verzeichnissen werden Mail-Ordner von IMAP und Groupware gespeichert. die Groupware-Daten beinhalten Einstellungen, Adressbücher, Kalenderdaten und Filtereinstellungen.



Halten Sie die Sicherungsdateien stets unter Verschluss, da sie in falschen Händen auch gelesen werden können!

Mailbackup jetzt erstellen

Zum manuellen Erstellen eines Mailbackups verwenden Sie bitte diesen Schalter.



Es wird immer ein vollständiges Backup mit allen Mail-Benutzern erstellt, unabhängig von der Einstellung "Pro Mail-Benutzer eine Backupdatei erstellen?".

Automatisches Mailbackup über

Wählen Sie hier das Protokoll für das Backup. Mit Ausnahme von Secure-Copy und SFTP erfolgt die Übertragung des Backups auf das Zielsystem unverschlüsselt. Auf dem Zielsystem wird die Backup-Datei nur dann verschlüsselt abgelegt, wenn Sie ein verschlüsseltes Backup konfiguriert haben. Im Falle eines unverschlüsselten Backups sorgen Sie bitte für einen angemessenen Schutz der Datei.



Die Authentifizierung bei Secure-Copy und SFTP erfolgt über SX-GATEs SSH ED25519-, bzw. RSA-Schlüssel. Bitte konfigurieren Sie den SSH-, bzw. SFTP Server entsprechend.



Es wird dringend davon abgeraten, das Mailbackup via E-Mail zuzustellen. Dies gilt insbesondere dann, wenn es an einen lokalen Benutzer zugestellt wird. Verbleibt die E-Mail mit dem Backup im Posteingang, so kann sich die Größe der Mailbackup-Datei schnell aufschaukeln.

Benutzername

Geben Sie hier den Benutzernamen an, mit dem sich SX-GATE am Backup-Server anmelden soll.



Beim Backup auf eine Windows-Netzwerkfreigabe müssen Sie hier in der Regel auch den Windows-Domänennamen angeben. Verwenden Sie dabei die Schreibweise "Domäne/Benutzername". Verwenden Sie nicht den unter Windows üblichen Backslash ("\").

Pfad und Dateiname

Geben Sie hier das Verzeichnis und den Dateinamen an, unter dem das Backup gespeichert werden soll. Die Angabe eines Verzeichnisses ist optional. Wird ein Verzeichnis angegeben, so muss dieses jedoch bereits existieren.

In den Dateinamen lassen sich Variablen einbauen. Auf diese Weise werden zuvor erstellte Backups nicht sofort wieder überschrieben. Es stehen u.a. folgende Variablen zur Verfügung:

- %Y: Jahr 4-stellig (z.B. 2001)
- %y: Jahr 2-stellig (z.B. 01)
- %m: Monat (von 01 bis 12)
- %d: Tag (von 01 bis 31)
- %H: Stunde (von 00 bis 23)
- %M: Minute (von 00 bis 59)
- %S: Sekunde (von 00 bis 59)
- %U: Woche des Jahres (Werte von 00 bis 53)
- %w: Tag der Woche (0 für Sonntag bis 6 für Samstag)
- %j: Tag im Jahr (von 001 bis 366)

Wenn als Ziel des Backups z.B.

"backup/%m.%d.rbu"

angegeben wird, enthält der Dateiname stets den aktuellen Monat und Tag. Eine Backup-Datei würde somit erst im folgenden Jahr wieder überschrieben werden.

Erstellt

Um das Backup nicht zu vergessen, nutzen Sie am Besten das automatische Backup. Stellen Sie hier die Häufigkeit sowie die Uhrzeit ein, zu der das Backup durchgeführt werden soll.



Ein monatliches Backup wird jeweils am ersten jedes Monats durchgeführt, ein wöchentliches immer Montags.



Prüfen Sie in regelmäßigen Abständen, ob das Backup noch funktioniert.

Pro Mail-Benutzer eine Backupdatei erstellen?

Wenn diese Option aktiviert ist, dann wird im konfigurierten Ziel pro Mail-Benutzer eine eigene Backupdatei erstellt. Dem konfigurierten Dateiname wird hierbei der Anmeldename des Benutzers und ein Unterstrich vorangestellt.

Automatisches Mailbackup testen

Versucht den aktuellen E-Mailbestand an den konfigurierten Speicherort zu übertragen.

12.5-E CA-Schlüssel

Private Schlüssel sind aus Sicherheitsgründen nicht Bestandteil der regulären Backups. Insbesondere die CA-Schlüssel sind jedoch von essentieller Bedeutung für die Funktionalität. Da CA-Zertifikate viele Jahre gültig sind und normalerweise während der Gültigkeitsdauer nicht verändert werden, genügt ein einmaliges Backup. Die Backup-Datei wird durch ein Kennwort geschützt.



Hinterlegen Sie das Backup an sicheren Orten und bedenken Sie bitte, dass die CA viele Jahre gültig ist. Die Speichermedien müssen daher für Langzeitarchivierung geeignet sein. Stellen Sie sicher, dass das für den Import der Backup-Datei benötigte Kennwort nicht in Vergessenheit geraten kann.

Der Import von hier gesicherten CA-Schlüsseln erfolgt im Menü "System > Zertifikatsverwaltung > CA Zertifikate" unter "SX-GATE-CA".

CA Schlüsselpaar sichern

Das Schlüsselpaar des Stammzertifikats kann zu Sicherungszwecken im PKCS#12-Format exportiert werden. Bitte beachten Sie, dass dieser Export also auch den privaten Schlüssel enthält, der unbedingt geheim bleiben muss.

Proxy Schlüsselpaar sichern

Das Schlüsselpaar des Proxy-Zertifikats kann zu Sicherungszwecken im PKCS#12-Format exportiert werden. Bitte beachten Sie, dass dieser Export also auch den privaten Schlüssel enthält, der unbedingt geheim bleiben muss.

12.5-F Schlüsselbund-Backup

Dieser Abschnitt dient zum Sichern der privaten Schlüssel aus dem Menü "System > Zertifikatsverwaltung > Schlüsselbund".



Halten Sie die Sicherungsdateien stets unter Verschluss!

12.6 Update

Das Einspielen eines Updates dauert in der Regel einige Minuten und löst ggf. selbständig einen Neustart des Systems aus. Bitte beachten Sie die Hinweise in den README-Dateien zum jeweiligen Update. Die Versionsinformation sollte nach einem Update einen neuen Wert anzeigen. Sollte dies nicht der Fall sein, so wenden Sie sich bitte an den technischen Support. Ist ein automatisches Update bereits eingeplant, erscheint hier eine entsprechende Meldung. Hier ist es dann auch möglich, das automatische Update zu löschen.

SX-GATE Update

In diesem Bereich können Sie Ihren SX-GATE auf den neusten Stand bringen.



Prüfen Sie bitte unbedingt in regelmäßigen Abständen, ob neue Updates zur Verfügung stehen. Werden sicherheitsrelevante Updates nicht installiert, so kann dies die Sicherheit Ihrer Netzwerke beeinträchtigen.

Installierte Version

In diesem Bereich wird der aktuell installierte Versionsstand Ihres SX-GATE angezeigt.

Update-Server

Um den Update-Vorgang so einfach wie möglich zu gestalten, kann SX-GATE selbständig prüfen, welche Updates installiert werden müssen. Geben Sie hier die URL an, über die SX-GATE-Updates bezogen werden können.

Wie soll das Update durchgeführt werden?

Wählen Sie hier aus, wie SX-GATE das Update vornehmen soll.

interaktiv (empfohlen)

Wählen Sie diesen Option, um zunächst eine Übersicht der verfügbaren Updates zu erhalten. Nach Bestätigung wird das nächste erforderliche Update installiert. Wiederholen Sie diesen Vorgang solange, bis keine neuen Updates mehr verfügbar sind.

zu einer bestimmten Uhrzeit

Auch hier wird zunächst eine Liste der verfügbaren Updates angezeigt. Hier legen Sie jedoch eine Uhrzeit fest, zu der der SX-GATE beginnen soll, Updates selbständig zu installieren. Es wird in jedem Fall das nächste anstehende Update eingespielt. Anschließend werden automatisch alle nachfolgenden regulären Updates installiert. Vor Beta-Versionen und kostenpflichtigen Updates endet die

Aktualisierung. Auch wenn eine Wahl zwischen mehrere alternativen Updates getroffen werden muss, endet die Installation.

durch Hochladen einer lokal gespeicherten Update-Datei

Falls die Update-Datei in Form einer *.rup-Datei bereits lokal bei Ihnen vorliegt, können Sie diese Datei auch manuell hochladen.

Wie soll das Update durchgeführt werden?

- interaktiv (empfohlen)
Lesen Sie bitte weiter bei **Verfügbare Updates** (S. 215)
- zu einer bestimmten Uhrzeit
Lesen Sie bitte weiter bei **Update planen** (S. 215)
- durch Hochladen einer lokal gespeicherten Update-Datei
Lesen Sie bitte weiter bei **Datei auswählen** (S. 216)

Letztes Update-Log anzeigen

Mit Hilfe dieses Schalters können Sie Meldungen einsehen, die beim letzten Update erzeugt wurden. Bei Problemen während des Update-Vorgangs geben diese Meldungen ggf. Aufschluss über deren Ursache.



Das Log wird automatisch gelöscht, wenn 10 Tage nicht mehr darauf zugegriffen wurde.

Update planen

Wählen Sie hier den gewünschten Tag und stellen die Uhrzeit ein zu der das Update durchgeführt werden soll. SX-GATE lädt und installiert zu diesem Zeitpunkt nacheinander alle verfügbaren Updates.



Sollten Sie einen in der Vergangenheit liegenden Zeitpunkt festgelegt haben, so erfolgt das Update sofort nachdem alle erforderlichen Angaben getätigt wurden.

Verfügbare Updates

Die hier angezeigten Updates sind aktuell für Ihren SX-GATE verfügbar.



Bitte beachten Sie die Hinweise aus der "README"-Datei.

Update bestätigen

Mit "Fertigstellen" ist die Auswahl des Updates abgeschlossen.

Datei auswählen

Wählen Sie bitte eine gültige SX-GATE Updatedatei aus.

12.7 Apps

Installierte Apps

Die derzeit installierten Apps werden hier mitsamt Versionsnummer und Status angezeigt. Apps können hier zudem gestartet, neu gestartet oder gestoppt werden. Eine gestartete App wird beim Neustart der Laufzeitumgebung automatisch gestartet. Eine gestoppte App bleibt nach einem Neustart gestoppt.



Apps werden in getrennten Umgebungen ausgeführt (Container-Virtualisierung). Die dazu benötigte Laufzeitumgebung starten Sie im Menü "System > Dienste" auf dem Reiter (Tab) "System-Dienste".

Online nach Updates und weiteren Apps suchen

Für diese Funktion ist eine Internet-Verbindung erforderlich, da SX-GATE sich mit dem Update-Server verbinden muss. Es wird dann eine Liste aller verfügbarer Apps angezeigt, über die Sie Aktualisierungen anstoßen bzw. weitere Apps installieren können.



Apps müssen unabhängig von den SX-GATE-Updates aktualisiert werden. Vergessen Sie daher nicht, auch regelmäßig nach App-Updates zu suchen.

12.8 Verwaltungsserver

In diesem Menü können SX-GATE und SX-GATE Satellite erfasst werden. Sie können dann zentral Updates an die Geräte verteilen und sehen den aktuellen Status.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

12.8-A Einstellungen.....	218
12.8-B SX-GATE.....	219
12.8-C SX-GATE Satellite.....	221

12.8-A Einstellungen

Privater Schlüssel des SSH TCP-Forwarders (Port 2222)

Um Probleme mit NAT-Routern aus dem Weg zu gehen und um keine Firewall-Regeln auf den zu verwaltenden Systemen konfigurieren zu müssen, werden gerne SSH-Tunnel genutzt. Dabei öffnet der zu verwaltende SX-GATE eine Verbindung zum SSH TCP-Forwarder des Verwaltungsservers. Den vom TCP-Forwarder genutzten SSH-Schlüssel legen Sie hier fest. Wir empfehlen, für diesen Zweck im Menü "System > Zertifikatsverwaltung > Schlüsselbund" einen eigenen ed25519-Schlüssel zu generieren.



Verwenden Sie auf einem Managementserver-Cluster nicht den vordefinierten Schlüssel "SSH_ED25519", da dieser nicht synchronisiert wird.

Privater Anmeldeschlüssel des Verwaltungsservers

Dieser Schlüssel wird für die Anmeldung an den zu verwaltenden SX-GATES verwendet. Wir empfehlen, für diesen Zweck im Menü "System > Zertifikatsverwaltung > Schlüsselbund" einen eigenen ed25519-Schlüssel zu generieren.



Verwenden Sie auf einem Managementserver-Cluster nicht den vordefinierten Schlüssel "SSH_ED25519", da dieser nicht synchronisiert wird.

Zugehöriger öffentlicher Schlüssel

Dieser öffentliche Schlüssel muss auf den zu verwaltenden SX-GATEs konfiguriert werden, damit sich der Verwaltungsserver dort anmelden kann.

12.8-B SX-GATE

Um einen anderen SX-GATE verwalten zu können, müssen Sie diesen entsprechend konfigurieren. Sie finden die Einstellungen ab Version 7.1-3.3 im Menü "System > Grundeinstellungen" auf dem Reiter (Tab) "Verwaltungszugriff".



Die Informationen werden alle 5 Minuten aktualisiert. Bei einem neu hinzugefügten System kann es entsprechend bis zu 5 Minuten dauern, bis erstmalig Informationen zur Verfügung stehen.

Verwaltbare SX-GATEs

Folgende Daten müssen Sie konfigurieren, um ein System zu verwalten:

Name bzw. Gruppe/Name

Diese Feld steht zu Ihrer freien Verfügung. Das Zeichen '/' dient als Trennzeichen für eine Gruppierung von Einträgen, was nützlich ist, wenn Sie sehr viele Systeme verwalten (z.B. "VIP-Kunden/Berlin - nachts aktualisieren").

Aktiv

Sie können den regelmäßigen Abruf von Informationen hier deaktivieren, z.B. wenn ein System vorübergehend nicht verfügbar ist. Im Falle eines SSH-Tunnels kann sich das System aber nach wie vor erfolgreich verbinden.

Adresse / Verbindungs-ID

Je nach Richtung der Verwaltungsverbindung tragen Sie bitte hier ein:

Verbindung vom Verwaltungsserver zum verwalteten SX-GATE

IP-Adresse oder DNS-Name des SX-GATEs

SSH-Tunnel vom verwalteten SX-GATE zum Verwaltungsserver

Eine individuelle Verbindungs-ID zwischen 10000 und 20000. Die ID entspricht dem TCP-Port, der auf dem Verwaltungsserver geöffnet wird. Über diesen Port kann dann der Verwaltungsserver auf den verwalteten SX-GATE zugreifen.

Öffentlicher Schlüssel des verwalteten Servers

Ein Eintrag ist hier nur bei SSH-Tunnels erforderlich (Verbindungsaufbau vom verwalteten SX-GATE zum Verwaltungsserver). Der benötigte öffentliche Schlüssel wird auf dem zu verwaltenden SX-GATE angezeigt.

Folgende Informationen werden zu den Systemen angezeigt:

Version

Die zuletzt ermittelte Version des verwalteten SX-GATE.

Apps

Die Anzahl der installierten Apps.

Status

Der Status zeigt derzeit nur an, wann die Daten zum letzten Mal erhoben werden konnten:

grün

Die Daten wurden innerhalb der letzten 10 Minuten erhoben und sind damit aktuell

rot

Die Daten wurden zuletzt vor mehr als 10 Minuten erhoben und sind damit nicht mehr aktuell

grau

Es konnten bisher noch keine Daten erhoben werden

Folgende Aktionen werden angeboten:

Details

Die Übersicht der erhaltenen Daten. Hier werden die zuletzt erhaltenen Daten ausgewertet, auch wenn diese nicht mehr aktuell sind

Administrieren

Es wird eine Verbindung zur Administrationsoberfläche des verwalteten SX-GATEs aufgebaut. Dazu wird ein Tunnel zwischen der Benutzeroberfläche und einem zufälligen Port größer als 20000 auf der LAN IP des Verwaltungsservers aufgebaut. Fünf Minuten nach der letzten Aktivität wird der Tunnel automatisch wieder abgebaut. Immer wenn Sie auf diesen Link klicken, wird ein neuer Tunnel aufgebaut



Jeder, der Zugriff auf die LAN-IP des Verwaltungsservers hat, kann sich über den Tunnel mit der Administrationsoberfläche des verwalteten SX-GATEs verbinden. Schränken Sie den Zugriff bei Bedarf über Firewall-Regeln ein.

Fernwartung öffnen

Auf dem verwalteten SX-GATE wird eine Fernwartungsverbindung geöffnet

Neue Verbindung mit Installationspaket

Mit diesem Assistenten können Sie eine neue Verbindung einrichten und bekommen am Ende die Möglichkeit, ein Installationspaket herunterzuladen. Auf dem zu verwaltenden SX-GATE eingespielt, ist dieser dann im Handumdrehen konfiguriert.



Unterstützt ausschließlich getunnelte Verbindungen, die vom verwalteten SX-GATE aus aufgebaut werden.

Supporttunnel /-schlüssel entfernen

Geräte auswählen

Statusübersicht:

Folgende Zustände sind möglich:

vorgemerkt

Der SX-GATE ist auf der Warteliste.

Anfrage gesendet

Die Anfrage für das Entfernen der Supporttunnel /-schlüssel wurde an SX-GATE gesendet.

abgeschlossen

Die Anfrage ist auf SX-GATE erfolgreich abgeschlossen.

fehlgeschlagen

Die Anfrage konnte auf SX-GATE nicht erfolgreich abgeschlossen werden.

Status unbekannt

Der Status der Abfrage ist unbekannt.

Aussenstellen mit geöffneten Supporttunnel oder freigegebenen Authorisierungsschlüssel

In der Tabelle sind alle SX-GATE gelistet, zu denen ein Supporttunnel offen ist oder ein Authorisierungsschlüssel freigegeben ist. Der Wert -1 bedeutet, daß die Anzahl der öffentlichen Schlüssel nicht ermittelt werden konnte.

12.8-C SX-GATE Satellite

Verwaltbare Außenstellen

Passende Außenstellen müssen hier manuell erfasst werden. Um sich mit einem SX-GATE Satellite verbinden zu können, muss dieser per SSH erreichbar sein und das SSH-Zertifikat des SX-GATES installiert haben. Das Zertifikat wird zusammen mit den VPN-Installationspaketen installiert.



Wird die SX-GATE Hardware getauscht, erhält dieser auch einen neuen SSH-Schlüssel. SX-GATE Satellite die das VPN-Installationspaket vor dem Hardwaretausch erhalten haben, sind dann nicht mehr erreichbar. Backup-Funktionen für den SSH-Schlüssel bzw. die Möglichkeit ein SSH-Zertifikat auf dem SX-GATE Satellite zu hinterlegen ohne dafür ein neues VPN-Installationspaket ausstellen zu müssen, werden zeitnah nachgereicht.

Folgende Informationen werden zu den Außenstellen erfasst bzw. angezeigt:

IPsec-Verbindung

Name der IPsec-Verbindung aus dem Menü "Module > Netzwerk > Schnittstellen".

Management-IP

Die IP-Adresse des SX-GATE Satellites, zu der sich SX-GATE per SSH verbinden soll. Üblicherweise wird hier die interne IP-Adresse des SX-GATE Satellites angegeben, die dann über VPN angesprochen wird. Sie können aber auch die externe IP eintragen, wofür allerdings auf dem SX-GATE Satellite eine entsprechende Firewall-Regel konfiguriert werden muss.

Zertifikat

Das Zertifikat der IPsec-Verbindung aus dem Menü "System > Zertifikatsverwaltung > CA Zertifikate". Diese Angabe ist optional und für eine zukünftige Erweiterung vorgesehen.

Ablaufdatum

Das Zertifikat auf dem SX-GATE Satellite ist gültig zum dem angegebenen Zeitpunkt.

Version

Die ermittelte Version

WLAN

Die Verfügbarkeit der WLAN-Schnittstelle auf dem SX-GATE Satellite.

Status

Der Status wird über eine Ampel signalisiert. Es gibt vier möglichen Ergebnisse:

grün

Die letzte Aktualisierung war erfolgreich und es wurden keine Fehler oder Warnungen festgestellt.

gelb

Es liegt mindestens ein Fehler oder eine Warnung vor.

rot

Die letzte Aktualisierung ist fehlgeschlagen.

weiß

Es liegen keine Informationen vor oder die Gegenstelle ist unbekannt. Zusätzliche Details werden Ihnen in Form eines Tooltips angezeigt, wenn Sie mit der Maus auf die Ampel zeigen.

Update einspielen

Über diesen Assistenten können Sie mehrere Außenstellen zentral aktualisieren.



Stellen Sie sicher, dass während des Updates niemand in der Außenstelle das Gerät ausschaltet. Es kann dadurch irreparabel beschädigt werden!



Derzeit kann ein Update nur auf SX-GATE Satellite mit mind. Version 3.1.1 eingespielt werden.

Datei auswählen

Falls ein Update im Hintergrund läuft, wird die Übersicht über den letzten Stand des gesamten Update-Prozesses geladen. Die Anzeige wird auf dieser Seite nicht automatisch aktualisiert.

Andernfalls können Sie eine Firmware auswählen und hochladen.

Geräte auswählen

Nach der erfolgreichen Prüfung der Firmware werden hier die Details zur Firmware und die passenden Aussenstellen angezeigt.



Stellen Sie sicher, dass während des Updates niemand in der Außenstelle das Gerät ausschaltet. Es kann dadurch irreparabel beschädigt werden!

Details der Firmware:

Folgende Informationen werden zur Firmware angezeigt:

Version

Architektur

Es werden 32- und 64-bit Versionen unterstützt.



64-Bit Firmware kann grundsätzlich nur auf SX-GATE Satellite mit mind. Version 3.2.0 eingespielt werden. Weitere Voraussetzung ist, dass die Hardware 64-bit unterstützt.

Geignet für Version

Abhängig von der SX-GATE Satellite-Version benötigen Sie ein bestimmtes Image:

< 3.1.1

Legacy-Firmware

>= 3.1.1

Standard-Firmware

Verfügbare und für das Update geeignete Geräte:

Wählen Sie aus der Liste die Außenstellen aus, die aktualisiert werden sollen.



In der Tabelle werden nur die Außenstellen gelistet, welche mit der gewünschten Firmware bespielt werden können.

Die Außenstellen werden sequenziell bespielt. Sollte ein Updatevorgang fehlschlagen, so wird der gesamte Vorgang abgebrochen. Der Updatevorgang einer Außenstelle ist in drei Abschnitte unterteilt:

Firmware hochladen

Die Firmware wird auf die Außenstelle kopiert. Anschließend wird geprüft, ob die Kopie korrekt übertragen wurde.



Bitte beachten Sie, dass die Dauer des Vorgang abhängig von der verfügbaren Bandbreite ist.

Den Installationsvorgang starten

Der Installationsvorgang wird auf der Außenstelle gestartet und dauert je nach Hardware und installieren Version zwischen 3 und 10 Minuten. In dieser Zeit ist die Außenstelle nicht erreichbar.



Stellen Sie sicher, dass in dieser Zeit niemand in der Außenstelle das Gerät ausschaltet. Es kann dadurch irreparabel beschädigt werden!

Warten auf die Ergebnisse der Installation.

Die Installation gilt als fehlgeschlagen, wenn die Außenstelle nach 10 Minuten nicht erreichbar ist oder die neue Firmware nicht installiert wurde.

12.9 Lizenzen

Lizenz-Nummer (Support-IP)

Hierbei handelt es sich um die Software-Lizenz-Nummer Ihres Systems.

Hardware-ID

SX-GATE Lizenz-Schlüssel sind speziell für das jeweilige Gerät ausgestellt. Diese ID identifiziert Ihre SX-GATE Hardware.

Maximale Benutzeranzahl

Wird die maximal zulässige Anzahl Benutzer erreicht, so können keine neuen Benutzer mehr angelegt werden. Erwerben Sie falls erforderlich bitte zusätzlich Benutzer.

Lizenzschlüssel aktivieren

Hier spielen Sie die unterschiedlichen SX-GATE Lizenzen ein.

SX-GATE Lizenzschlüssel

Lizenzschlüssel eingeben

Bitte geben Sie den Lizenzschlüssel ein

Hier finden Sie den Lizenzschlüssel des SX-GATE. Dieser Schlüssel steuert u.a. die erlaubte Benutzerzahl und die verfügbaren Optionen. Wenn Sie z.B. nach dem Kauf zusätzlicher Benutzer einen neuen Lizenzschlüssel erhalten, können Sie diesen hier hinterlegen.



Ein SX-GATE Lizenzschlüssel besteht grundsätzlich aus 29 Zeichen. Bitte achten Sie bei der Eingabe darauf, ähnliche Zeichen nicht zu verwechseln (z.B. O und 0). Sollten Sie den neuen Schlüssel auf elektronischem Wege erhalten haben, so nutzen Sie nach Möglichkeit die Funktionen "Kopieren" und "Einfügen" der jeweiligen Anwendungen.

12.10 Abschalten/Neustart

Bitte wählen Sie:

Sollte ein Neustart des SX-GATE notwendig sein, oder das Gerät abgeschaltet werden müssen, so wählen Sie bitte einen dieser Punkte.

SX-GATE neu starten

Diese Option führt einen Neustart des Systems aus. Wählen Sie die Option und bestätigen Sie mit "Fertigstellen". In diesem Fall kann es bis zu 5 Minuten dauern, bis der SX-GATE wieder einsatzbereit ist.

SX-GATE herunterfahren und ausschalten

Ist diese Option ausgewählt, so wird das System heruntergefahren und ausgeschaltet. Nach Betätigung des Schalters "Fertigstellen" können dabei bis zu 2 Minuten vergehen.

13 Assistenten

Die Grundkonfiguration des SX-GATE sollten Sie über die Assistenten des Hauptmenüs "Assistenten" vornehmen. Schritt für Schritt wird hier die Konfiguration von Teilbereichen wie Netzwerkanbindung oder Mail-System durchgeführt.

13.1 LAN Anbindung

IP-Adresse des SX-GATE

Der SX-GATE benötigt im internen LAN eine eindeutige, feste IP-Adresse! Vergeben Sie keine Adresse, die in Ihrem LAN (Local Area Network) bereits von einem anderen Gerät verwendet wird. Fragen Sie bei Zweifeln den Betreuer Ihres Netzwerkes.

Beachten Sie bitte, dass Sie den IP-Adressbereich für Ihr LAN nicht ganz beliebig vergeben dürfen. Gemäß Internetstandard RFC-1918 sind für lokale Netzwerke alle Adressen vorgesehen, die mit 10, mit 172.16 bis 172.31 oder mit 192.168 beginnen. Alle IP-Adresse außerhalb dieser privaten Subnetze sind entweder reserviert oder im Internet offiziell vergeben und das Eigentum von Firmen. Es empfiehlt sich daher dringend, für das interne LAN nur diese privaten Subnetze zu verwenden. Im Falle des Netzwerks "192.168.0.0" mit der Netzmaske "255.255.255.0" können Sie z.B. 254 IP-Adressen im Bereich 192.168.0.1 bis 192.168.0.254 an Computer in Ihrem LAN vergeben.

In der IP-Konfiguration aller Server und Arbeitsstationen in Ihrem LAN, die direkten Zugang zum Internet benötigen, tragen Sie bitte die IP-Adresse des SX-GATE als Gateway und Name-Server (DNS) ein. Sind in der IP-Konfiguration des Computers bereits andere Gateways und Name-Server eingetragen, so sollten Sie diese entfernen. Der Zugriff auf das Internet mittels Web-Browser sowie die E-Mail-Kommunikation erfolgt in der Regel mit Hilfe des Web-Proxies und der Mail-Funktionen des SX-GATE. Diese sind auch ohne Eintragung von DNS und Gateway nutzbar. Ist der DNS des SX-GATE im jeweiligen Computer nicht konfiguriert, so beachten Sie bitte, dass Sie dann bei allen Einstellungen nie den Namen des SX-GATE angeben dürfen. Sie müssen stets dessen IP-Adresse angeben.

Am einfachsten ist es, wenn ein DHCP-Server eingesetzt wird. Die Adressen für Gateway (Router) und Name-Server (DNS) werden im DHCP-Server hinterlegt. Die Arbeitsstationen im LAN können dann so konfiguriert werden, dass diese die IP-Konfiguration automatisch vom DHCP-Server beziehen. Falls SX-GATE selbst als DHCP-Server fungieren soll, können Sie die entsprechenden Einstellungen in den Folgemasken vornehmen.

LAN IP-Adresse des SX-GATE

Tragen Sie hier die IP-Adresse ein, unter der der SX-GATE in Ihrem internen Netzwerk erreichbar sein soll. Die IP muss zu den Adressen passen, die auf den anderen Geräten in Ihrem LAN eingestellt ist.

LAN Netzmaske

Tragen Sie in diesem Feld die Netzmaske passend zu Ihrem Netzwerk ein. Auf allen Computern in diesem Netzwerk muss die gleiche Netzmaske konfiguriert sein.

Name des SX-GATE

Legen Sie hier den Namen des SX-GATE fest. Dieser besteht aus dem Servernamen selbst und der zugehörigen Domain. Insbesondere die hier angegebene Domain dient als Voreinstellung für viele Konfigurationsoptionen des SX-GATE.

Geben Sie als Namen z.B. "gateway" und als Domain z.B. "example.com" ein, so wird der SX-GATE mit dem Internet-Browser im internen LAN unter der Adresse

"https://gateway.example.com"

erreichbar sein - entsprechende DNS-Konfiguration der Arbeitsstationen vorausgesetzt.

Name des SX-GATE

Geben Sie hier den Hostnamen für SX-GATE an. Dieser darf nur aus den Buchstaben "a" bis "z", Ziffern und Bindestrichen bestehen.

Domain

Geben Sie hier die Domain für SX-GATE ein. Sofern Ihre Firma bereits über eine Internet-Domain verfügt, empfiehlt es sich, diese zu verwenden. Besitzen Sie noch keine Internet-Domain, so geben Sie bitte eine Domain an, die es so garantiert nicht im Internet gibt (z.B. "firma.intern"). Andernfalls kann es zu Konflikten kommen.



Die Domain von der hier die Rede ist hat nichts mit einer eventuell vorhandenen Windows-NT Domäne zu tun.

Intranet IP-Adressen**Lokale IP-Netzwerke**

Damit SX-GATE unterscheiden kann, ob ein Zugriff aus dem Internet oder dem internen LAN erfolgt, werden hier die Netzwerke eingetragen, die dem LAN zuzurechnen sind. Manche Dienste, wie z.B. der Mail-Server des SX-GATE, bieten spezielle Funktionen nur den hier angegebenen lokalen Netzwerken an. Andere Dienste, wie der Web-

Proxy, verweigern IP-Adressen außerhalb der hier angegebenen Adressbereiche völlig ihre Dienste.

Diese Einstellung hat keinerlei Einfluss auf Firewall-Regeln.

SX-GATE DHCP-Server

DHCP-Server aktivieren

Mit Hilfe des DHCP-Dienstes des SX-GATE lässt sich sowohl die Vergabe der IP-Adressen als auch die IP-Konfiguration der Arbeitsstationen im LAN zentral verwalten und automatisieren. SX-GATE kann diese Aufgabe in Ihrem LAN übernehmen, wenn noch kein anderer Server diese wahrnimmt.

Sollte sich in Ihrem LAN bereits ein DHCP-Server befinden, kann der DHCP-Server des SX-GATE auch als sekundärer DHCP-Server konfiguriert werden. Auf diese Weise wird der DHCP-Dienst auch bei einem Ausfall des primären Servers aufrecht erhalten.

DHCP-Server aktivieren

- ja
Lesen Sie bitte weiter bei [Backup DHCP-Server](#) (S. 230)
- nein
Lesen Sie bitte weiter bei [Konfiguration übernehmen](#) (S. 232)
- als Relay
Lesen Sie bitte weiter bei [Konfiguration übernehmen](#) (S. 232)

Backup DHCP-Server

SX-GATE als sekundären DHCP-Server verwenden

Aktivieren Sie diese Option, wenn Sie SX-GATE als sekundären DHCP-Server verwenden wollen.



Sollten Sie den DHCP-Server unnötigerweise als sekundären DHCP-Server konfiguriert haben, äußert sich dies in einer verlängerten Startdauer der Arbeitsstationen. Sind mehrere primäre DHCP-Server aktiv, weist der jeweils schneller antwortende Server die IP-Konfiguration zu. Je nach Verhalten der beteiligten Server kann es unter Umständen aber auch zu Störungen kommen.

Im Unterschied zum primären DHCP-Dienst antwortet SX-GATE als sekundärer DHCP-Server nicht auf die erste Anfrage eines Gerätes nach eine IP-Adresse. SX-GATE antwortet erst dann, wenn einige Sekunden vergangen sind und das Gerät

immer noch nach einer IP-Adresse verlangt. In diesem Falle geht der SX-GATE davon aus, dass der eigentliche DHCP-Server nicht verfügbar ist und weist der Arbeitsstation eine IP-Adresse zu.



Bitte beachten Sie, dass sich die dynamisch zugewiesenen IP-Adressbereiche des primären und des sekundären DHCP-Servers nicht überschneiden dürfen, da der primäre Server nichts von der Existenz des sekundären weiß. Folglich kann es bei Überschneidungen zu Konflikten kommen.

Zuzuweisende IP-Adressen

Per DHCP zu vergebende Adressbereiche

Geben Sie hier Adressbereiche ein, die per DHCP dynamisch an Geräte zugewiesen werden können. Die Adressen aus diesen Bereichen dürfen nicht statisch an Geräte vergeben sein.



Die Adressbereiche müssen dem gleichen IP-Netzwerk angehören wie die IP-Adresse des SX-GATE, die Sie zu Beginn dieses Assistenten festgelegt haben.



Die Adressbereiche passen automatisch zur SX-GATE-IP, wenn Sie diese auf spezielle Art und Weise angeben. Setzen Sie dazu den Netzwerkteil der Adresse auf "0". Ist beispielsweise das Subnetz zur SX-GATE-IP "192.168.0.0/24", so steht der Bereich "0.0.0.100-0.0.0.199" tatsächlich für "192.168.0.100-192.168.0.199".

Sie sollten all den Geräten, die Dienste in Ihrem lokalen Netzwerk zur Verfügung stellen (z.B. Server, Netzwerkdrucker, Router und Switches) feste Adressen zuteilen. So sind diese Dienste immer unter der selben Adresse erreichbar. Der Einsatz des DHCP-Dienstes empfiehlt sich hauptsächlich für die Konfiguration von Arbeitsstationen und mobilen Computern. Hier kommt es häufiger vor, dass Geräte hinzukommen, ausgetauscht oder entfernt werden.

Dimensionieren Sie den Bereich der dynamisch zuweisbaren Adressen entsprechend der Anzahl von Geräten in Ihrem Netzwerk ausreichend groß! Ein zu klein gewählter Bereich führt dazu, dass nicht alle Geräte mit einer IP-Adresse versorgt werden können und somit keine IP-Verbindung in Ihr Netzwerk erhalten.

Konfiguration übernehmen

Die Konfiguration des SX-GATE wurde bis jetzt noch nicht verändert. Drücken Sie auf "Fertigstellen" um Änderungen in das System zu übernehmen oder "Abbrechen" um keine Änderungen vorzunehmen.



Sollten Sie die IP-Adresse des SX-GATE geändert haben, so ist SX-GATE nach dem "Fertigstellen" nicht mehr unter der alten Adresse ansprechbar. Nach einigen Sekunden können Sie SX-GATE unter dessen neuer Adresse erreichen. Sollte die neue IP-Adresse sich in einem anderen IP-Netzwerk befinden, so kann es erforderlich sein, zunächst Ihre Arbeitsstation umzukonfigurieren.

13.2 Internet-Zugang

Art der Internet-Anbindung

Auf welche Weise erfolgt der Internet-Zugang

Es gibt verschiedene Arten der Internetanbindung. Dieser Konfigurations-Assistent unterstützt Sie, wenn Sie auf eine der folgenden Arten an das Internet angebunden sind:

DSL-Wählleitung mit PPP-over-Ethernet/PPPoE (via DSL-Modem oder Router im Modem-Betrieb)

Hierbei handelt es sich um eine DSL-Verbindung, die mit Hilfe eines DSL-Modems hergestellt wird. SX-GATE kommuniziert mit dem Modem über das Protokoll PPP-over-Ethernet und steuert darüber auch den Auf- und Abbau der Verbindung.

Über Router (statische Internet-IP des SX-GATEs eingeben)

SX-GATE befindet sich hinter einem Router, der seinerseits mit einer beliebigen Technik an das Internet angebunden ist.

Wird der SX-GATE nachträglich zwischen Router und LAN eingebaut, dann ist darauf zu achten, dass zwischen Router und SX-GATE ein anderes IP-Netzwerk als im LAN verwendet wird. Der Router muss dazu in der Regel umkonfiguriert werden. Verwenden Sie alternativ den Bridge-Modus.



Konfigurieren Sie für die Verbindung zum Router niemals IP-Adressen aus dem selben IP-Netzwerk, das bereits für das LAN in Verwendung ist.

Internet-IP über DHCP (Kabel-Modem oder Router)

In dieser Variante wird dem SX-GATE die Internet-IP per DHCP zugewiesen. Dies ist bei Kabelanschlüssen üblich. SX-GATE ist in diesem Fall mit einem Kabel-Modem verbunden.

Möglich ist auch, dass ein vorgelagerter Router dem SX-GATE eine IP-Adresse per DHCP zuweist. Wir empfehlen in diesem Fall jedoch manuell eine feste IP-Adresse zu vergeben.

SX-GATE als Bridge zwischen Router and LAN (transparente Firewall; nur für einfache Netzwerke empfohlen)

Verbindet Router und LAN über eine Bridge.



Wählen Sie diese Option nur für einfache Netzwerke, die ohne Routing auskommen (kein VPN, keine internen Router, keine weiteren Schnittstellen, die nicht ebenfalls Teil der Bridge sind). Andernfalls kann die Firewall-Konfiguration schnell komplex und damit fehleranfällig werden.

SX-GATE als Server in LAN oder DMZ (Netzwerkanschluss nur über eth0)

Wenn SX-GATE nicht als Router und Internet-Gateway sondern als Server fungiert (z.B. Proxy-, Mail- oder VPN-Server), sollte diese Einstellung die richtige Wahl sein. SX-GATE muss in diesem Fall über die LAN-Schnittstelle eth0 mit dem Internet-Router verbunden sein.

Auf welche Weise erfolgt der Internet-Zugang

- <Bitte auswählen>
 - Lesen Sie bitte weiter bei [Art der Internet-Anbindung](#) (S. 233)
- DSL-Wählleitung mit PPP-over-Ethernet/PPPoE (via DSL-Modem oder Router im Modem-Betrieb)
 - Lesen Sie bitte weiter bei [ADSL-Parameter](#) (S. 234)
- Über Router (statische Internet-IP des SX-GATES eingeben)
 - Lesen Sie bitte weiter bei [Internet IP-Adressen](#) (S. 235)
- Internet-IP über DHCP (Kabel-Modem oder Router)
 - Lesen Sie bitte weiter bei [IP-Vergabe über DHCP](#) (S. 236)
- SX-GATE als Bridge zwischen Router and LAN (transparente Firewall; nur für einfache Netzwerke empfohlen)
 - Lesen Sie bitte weiter bei [IP-Konfiguration der Bridge](#) (S. 236)
- SX-GATE als Server in LAN oder DMZ (Netzwerkanschluss nur über eth0)
 - Lesen Sie bitte weiter bei [IP-Konfiguration](#) (S. 237)

ADSL-Parameter

Geben Sie hier bitte die Zugangsdaten (Benutzername/Login und Passwort) für die Einwahl bei Ihrem Provider ein. Sollten Sie von Ihrem Provider mehrere verschiedene Kennungen erhalten haben (z.B. auch für E-Mail / POP3 und für die Pflege Ihres Web-Servers), so verwenden Sie bitte die DSL-Einwahl-Kennung. Wichtig ist ferner die korrekte VLAN-Konfiguration, die abhängig vom Provider und dem eingesetzten Modem ist.

VLAN-ID

Tragen Sie hier eine VLAN-ID ein, wenn es sich um einen DSL-Zugang handelt, der über VLAN angesprochen wird. Die Kommunikation mit dem DSL-Modem erfolgt dann über entsprechend markierte VLAN-Pakete. Die zu verwendende VLAN-ID erfragen Sie bitte bei Ihrem Provider.



DSL-Zugänge der Deutschen Telekom nutzen in der Regel VLAN-ID 7, DSL-Zugänge von Vodafone VLAN-ID 132.

Lokale IP-Adresse

Sie haben die Möglichkeit, eine von der Gegenstelle zugewiesene dynamische IP-Adresse zu akzeptieren oder eine bestimmte IP-Adresse festzulegen.

*Lesen Sie bitte weiter bei **Zugewiesenen DNS-Server verwenden***

Internet IP-Adressen

Die Kommunikation mit dem externen Router erfolgt über die zweite Netzwerkkarte des SX-GATE (eth1). Diese darf noch nicht anderweitig in Verwendung sein.

Der externe Router und SX-GATE können direkt miteinander verbunden werden. Alternativ verbinden Sie die beiden Geräte über einen eigenen Switch. An diesem Switch dürfen ausschließlich Geräte angeschlossen sein, deren IP-Adresse ebenfalls zu dem Transfernetz zwischen Router und SX-GATE gehören.



Bitte beachten Sie, dass die hier eingetragenen IP-Adressen nicht aus dem Adress-Bereich stammen dürfen, der bereits für Ihr LAN konfiguriert wurde. Wird also z.B. in Ihrem LAN das Subnetz 192.168.0.0 mit einer Netzmaske von 255.255.255.0 verwendet, so dürfen die hier eingetragenen Adressen nicht ebenfalls mit 192.168.0 beginnen.



Alle Geräte die an dem Transfernetz zwischen SX-GATE und Router angeschlossen sind, werden nicht durch die SX-GATE Firewall gegenüber dem Internet geschützt. Platzieren Sie diese Geräte stattdessen in einer Demilitarisierten Zone (DMZ), die sich ebenfalls mit Hilfe des SX-GATE einrichten lässt.

Internet IP-Adresse des SX-GATE

Tragen Sie hier die externe IP-Adresse des SX-GATE ein. Sofern Sie von Ihrem Provider einen ganzen Bereich von externen IP-Adressen erhalten haben, wählen Sie bitte eine davon. Bitte beachten Sie, dass in einem IP-Netzwerk stets die erste und letzte IP-Adresse reserviert sind. Die erste IP-Adresse (Netzwerk-Adresse) endet stets mit einer geraden Zahl, während die letzte IP (Broadcast-Adresse) immer ungerade endet. Prüfen Sie daher bei den Angaben des Providers, ob der Ihnen zugeteilte Adressbereich diese reservierten Adressen beinhaltet oder nicht. Sie dürfen dem SX-

GATE selbstverständlich nicht die IP-Adresse zuweisen, die dem Router zugeteilt wurde.



Die IP-Adresse des SX-GATE auf der externen Schnittstelle darf nicht Bestandteil des selben IP-Kreises sein, der für Ihr LAN vorgesehen ist. Auf keinen Fall darf diese Adresse identisch mit der LAN IP-Adresse des SX-GATE sein.

IP-Adresse des Internet-Routers (Gateway)

Tragen Sie hier die (interne) IP-Adresse des Routers ein. In den Angaben Ihres Providers wird diese eventuell auch als "Gateway" bezeichnet.

Netzmaske des Transfernetzes

Tragen Sie hier die zugehörige Netzmaske ein. Lautet die Netzmaske die Sie von Ihrem Provider erhalten haben 255.255.255.252, so gibt es keine Möglichkeit weitere Geräte an das Transfernetz anzuschließen. Bei anderen Netzmasken ist es prinzipiell möglich, weitere Geräte in dem Transfernetz anzuschließen (z.B. Web-Server, Mail-Server, ...). Auf diese Server kann dann jedoch in der Regel ungeschützt direkt aus dem Internet zugegriffen werden. Wir empfehlen stattdessen den Aufbau einer sogenannten Demilitarisierten Zone (DMZ) die sich mit Hilfe des SX-GATE einrichten lässt.

Lesen Sie bitte weiter bei [DNS-Server des Providers](#)

IP-Vergabe über DHCP

In diesem Modus erfolgt die IP-Konfiguration automatisch.

Lesen Sie bitte weiter bei [Zugewiesenen DNS-Server verwenden](#)

IP-Konfiguration der Bridge

IP-Adresse des vorgeschalteten Routers

Tragen Sie hier die (interne) IP-Adresse des Routers ein. In den Angaben Ihres Providers wird diese eventuell auch als "Gateway" bezeichnet.

Lesen Sie bitte weiter bei [DNS-Server des Providers](#)

IP-Konfiguration

IP-Adresse des Internet-Routers

Tragen Sie hier die (interne) IP-Adresse des Routers ein. In den Angaben Ihres Providers wird diese eventuell auch als "Gateway" bezeichnet.

Lesen Sie bitte weiter bei [DNS-Server des Providers](#)

Zugewiesenen DNS-Server verwenden

Zugewiesene DNS-Server verwenden

Aktivieren Sie diese Option, um die vom Provider automatisch zugewiesenen DNS-Server zur Namensauflösung zu verwenden.

Zugewiesene DNS-Server verwenden

- ☐ ja (empfohlen)
Lesen Sie bitte weiter bei [Übergeordneten Proxy-Server verwenden](#) (S. 238)
- ☐ nein
Lesen Sie bitte weiter bei [DNS-Server des Providers](#) (S. 237)

DNS-Server des Providers

DNS-Anfragen an folgende übergeordnete DNS-Server weiterleiten

Tragen Sie hier die IP-Adressen der Name-Server (DNS) Ihres Providers ein. DNS wird benötigt, um den Namen eines Web-Servers oder die Domain einer Mail-Adresse der IP-Adresse des zugehörigen Web- oder Mail-Servers zuzuordnen. Sie erfahren die hier einzutragenden Adressen bei Ihrem Provider. Sind mehrere Server angegeben, werden diese in der Reihenfolge ihrer Antwortgeschwindigkeit befragt.



Bitte verwenden Sie nur DNS-Server die auch wirklich von Ihrem Internetzugangspunkt aus genutzt werden dürfen. Falls keiner der konfigurierten DNS-Server erreichbar ist, sind die meisten Internet-Dienste nicht verwendbar.

Falls Ihnen keine DNS-Server bekannt sind, können Sie auch die direkte Namensauflösung über die sogenannten "Root-Nameserver" des Internet verwenden. Tragen Sie dazu einfach keinen DNS-Server ein. In diesem Falle ist jedoch unter Umständen mit einer deutlich verlängerten Antwortzeit zu rechnen.

Übergeordneten Proxy-Server verwenden

Internetverbindung über Proxy-Dienst des Providers

Wenn gewünscht bzw. verfügbar, kann der Web-Proxy des SX-GATE einen vorgelagerten Proxy-Server verwenden. Andernfalls verbindet sich der Web-Proxy des SX-GATE immer direkt mit der angesprochenen Adresse.



Die Verwendung des Proxies kann auch aufgrund einer Vorschrift zwingend erforderlich sein.

Internetverbindung über Proxy-Dienst des Providers

- ja
Lesen Sie bitte weiter bei [Übergeordneter Proxy-Server](#) (S. 238)
- nein
Lesen Sie bitte weiter bei [SMTP Relay-Server verwenden](#) (S. 239)

Übergeordneter Proxy-Server

Name oder IP-Adresse des Proxy-Servers

Erfragen Sie den Namen oder die IP-Adresse des Proxy-Servers beim Betreiber.

Port-Nummer

Die Angabe der Portnummer ist zwingend erforderlich. Auch diese erfahren Sie beim Betreiber. Üblicherweise wird hier 80, 3128 oder 8080 verwendet.

Verbindungen ausschließlich über diesen Proxy erstellen

Falls sich SX-GATE hinter einer entsprechend reglementierten Firewall befindet, kann es nötig werden, alle Anfragen über den Proxy-Server abzuwickeln. Aktivieren Sie in diesem Falle bitte die Option.

Andernfalls geht SX-GATE davon aus, dass es sich um einen caching Proxy handelt, der ausschließlich zur Geschwindigkeitssteigerung dient. In diesem Falle optimiert der SX-GATE Web-Proxy die Weiterleitung von Anfragen. Nur die Anfragen, die möglicherweise im Cache des Proxies liegen könnten, werden auch an diesen weitergeleitet. Für Anfragen, die ohnehin nicht in einem Cache gespeichert werden dürfen, wird stattdessen eine direkte Verbindung zum Ziel-Web-Server hergestellt. Nicht im Cache ablegbar sind z.B. Anfragen für Dateien die nur nach Benutzeranmeldung heruntergeladen werden dürfen oder verschlüsselte (https) Verbindungen.

SMTP Relay-Server verwenden

Ausgehende E-Mails über Mail-Relay des Providers versenden

Ausgehende Mails können entweder direkt an den E-Mail-Server des Empfängers oder zunächst an den Mail-Relay-Server Ihres Providers versendet werden. Aufgabe eines Mail-Relay-Servers ist es, E-Mails von Mail-Clients oder Mail-Servern anzunehmen und an den Mail-Server des Empfängers oder einen weiteren Relay-Server weiterzuleiten.

Bei einer Internet-Anbindung mit dynamischer IP muss ein Relay-Server genutzt werden. Bei fester IP ist auch direkter Versand möglich, allerdings muss für die IP-Adresse ein passender Reverse-Lookup-Eintrag im DNS konfiguriert sein.

Ausgehende E-Mails über Mail-Relay des Providers versenden

- ja
Lesen Sie bitte weiter bei [SMTP Relay-Server](#) (S. 239)
- über Microsoft 365 mit OAUTH2
Lesen Sie bitte weiter bei [Microsoft 365 OAUTH2](#) (S. 240)
- nein
Lesen Sie bitte weiter bei [NTP Zeitserver aktivieren](#) (S. 242)

SMTP Relay-Server

Nach Möglichkeit sollten Sie als SMTP-Relay-Server den Server verwenden, den Ihr Internetzugangsprovider anbietet. In diesem Falle ist in der Regel keine Benutzeranmeldung erforderlich. Lassen Sie die Felder für die Zugangsdaten leer.

Name oder IP-Adresse des Relay-Servers

Tragen Sie bitte hier den Namen oder die IP-Adresse des Mail-Relay-Servers Ihres Providers ein. Der gesamte Mailverkehr in das Internet wird dann über den hier eingetragenen Server Ihres Providers abgewickelt. Dieser kümmert sich dann um die Zustellung an den Mail-Server des Empfängers. Treten bei der Zustellung vom Relay-Server an den Empfänger Fehler auf, so wird der Relay-Server versuchen die Mail erneut zuzustellen bzw. den Absender über die Unzustellbarkeit in Kenntnis setzen.

SMTP-Auth Benutzername

Sind der Betreiber des SMTP-Relay-Servers und der Provider der Ihren Internetzugang bereitstellt nicht identisch, so müssen Sie sich am SMTP-Relay-Server in der Regel anmelden. Der Provider verhindert so den Missbrauch seines Relay-Servers durch SPAM-Mail Versender. Das standardisierte Verfahren zur Anmeldung heißt SMTP-Auth.

Fragen Sie im Zweifelsfall bei Ihrem Provider nach, ob Sie sich bei seinem Relay-Server anmelden müssen, ob der Relay-Server SMTP-Auth unterstützt und mit

welchen Zugangsdaten Sie sich anmelden können. Lassen Sie dieses Feld leer, wenn Sie sich nicht mit SMTP-Auth anmelden müssen.



Gemäß dem SMTP-Auth Standard handelt es sich um eine sogenannte "Hop-to-Hop" Authentifizierung. Dies bedeutet, dass sich nur der unmittelbare Kommunikationspartner (in diesem Falle der SX-GATE Mail-Server) am Relay anmeldet. Aus diesem Grund erfolgt die SMTP-Auth Anmeldung immer mit den gleichen Zugangsdaten. Es ist nicht möglich, dass sich SX-GATE abhängig vom jeweiligen Absender mit verschiedenen Zugangsdaten anmeldet.

SMTP-Auth Passwort

Geben Sie hier das SMTP-Auth Passwort ein.

Lesen Sie bitte weiter bei [NTP Zeitserver aktivieren](#)

Microsoft 365 OAUTH2

Für den Versand von Mails über ein "Microsoft 365"-Konto mit dem OAuth2-Verfahren nutzt SX-GATE den "Client-Credentials Flow". In "Entra ID" (ehemals Azure Active Directory) wird dazu für den SX-GATE Mail-Server eine Anwendung mit zugehörigem Anwendungskennwort angelegt. Die Anwendung erhält die Berechtigung für den SMTP-Versand. SX-GATE nutzt ausschließlich ein Benutzerkonto für den Mail-Versand. Diesem Konto muss die Sendeberechtigung für alle Absenderadressen erteilt werden. Nun kann der SX-GATE mit seiner Anwendungs-ID und dem Anwendungskennwort einen kurzlebigen Zugriffstoken abrufen und mit diesem die Mails über das angegebene Benutzerkonto versenden.

Die Schritte im Einzelnen:

Anwendung anlegen

Melden Sie sich bei Microsoft Azure mit einem Administratorenkonto an (<https://portal.azure.com>).

Wählen Sie "Microsoft Entra ID", dann "Verwalten > App-Registrierungen".

Klicken Sie auf "Neue Registrierung" und vergeben Sie einen beliebigen Namen. Lassen Sie die weiteren Einstellungen unverändert und legen Sie die Anwendung mit "Registrieren" an.

Jetzt links im Menü "Zertifikate & Geheimnisse" anklicken. Unter "Geheime Clientschlüssel" generieren Sie mit "Neuer geheimer Clientschlüssel" ein Anwendungskennwort, das Sie mit "Hinzufügen" abspeichern.

Kopieren Sie nun sofort das Kennwort in der Spalte "Wert" durch Klick auf das Kopiersymbol hinter dem Kennwort. Zu einem späteren Zeitpunkt ist dies nicht mehr möglich. Übertragen Sie das Kennwort in die OAuth2-Konfiguration des SX-GATE Mail-Servers bzw. speichern Sie es an einem sicheren Ort zwischen, um es später im SX-GATE zu konfigurieren.

Klicken Sie nun im Menü links auf "Verwalten > API-Berechtigungen", dann "Berechtigung hinzufügen". Wählen Sie "Von meiner Organisation verwendete APIs" und geben Sie im Suchfeld "Office" ein. Wählen Sie "Office 365 Exchange Online" aus. Klicken Sie auf "Anwendungsberechtigungen". Öffnen Sie die Rubrik "SMTP" und selektieren Sie die "SMTP.SendAsApp"-Berechtigung. Schließen Sie das Fenster mit "Berechtigungen hinzufügen". Klicken Sie abschließend auf "Administratorzustimmung für DOMAINNAME erteilen".

Klicken Sie im linken Menü auf "Übersicht" und übertragen Sie die "Anwendungs-ID (Client)" und die "Verzeichnis-ID (Mandant)" in die OAuth2-Konfiguration des SX-GATE Mail-Servers bzw. speichern Sie die Werte zwischen, um sie später im SX-GATE zu konfigurieren.

Verlassen Sie nun die Anwendungs-Registrierung, indem Sie oben links auf "Home" klicken.

Öffnen Sie erneut "Microsoft Entra ID" und wählen Sie diesmal "Verwalten > Unternehmensanwendungen". Kopieren Sie sich für später die "Objekt-ID" der zuvor angelegten Anwendung. Hier wird auch nochmal die "Anwendungs-ID" angezeigt. Sie benötigen beide Werte gleich für die Exchange-Konfiguration.

Zugriffsrechte im Exchange erteilen

SX-GATE nutzt für den Mailversand lediglich ein Benutzerkonto. Entscheiden Sie sich für ein Konto und prüfen Sie dann im "Microsoft 365 admin center" (<https://admin.microsoft.com>), ob für dieses Konto "Authentifiziertes SMTP" erlaubt ist. Wählen Sie dazu unter "Benutzer > Aktive Benutzer" das Konto aus. Nach Klick auf "E-Mail" werden Ihnen unter "E-Mail Apps" die Berechtigungen angezeigt.

Gehen Sie nun alle anderen Benutzer und Gruppen durch und erteilen Sie "Senden als"-Berechtigung für das zum Versand genutzte Konto.

Zugangsdaten im SX-GATE hinterlegen

Sofern noch nicht geschehen, tragen Sie die zuvor kopierten Werte in die OAuth2-Konfiguration des SX-GATE Mail-Clients ein.

Tragen Sie das für den Versand zu verwendende Benutzerkonto bei "SMTP-Auth Benutzername" ein. Die Angabe des zugehörigen Benutzerpassworts ist nicht erforderlich, da sich SX-GATE mit seinem Anwendungskennwort anmelden kann.

Name oder IP-Adresse des Relay-Servers

Für Microsoft 365 ist dies typischerweise `smtp.office365.com`.

Mandant (Tenant)

Tragen Sie hier den Namen oder die ID Ihres "Entra ID"-Mandanten ein.

OAuth2 Anwendungs-ID

Geben Sie hier die Anwendungs-ID (Client-ID) ein, die Sie in "Entra ID" für den SX-GATE Mail-Server registriert haben.

Geheimer OAuth2-Clientschlüssel

Geben Sie hier das Anwendungskennwort ein, das Sie im Azure Active-Directory für den SX-GATE Mail-Server generiert haben.



Das Anwendungskennwort ist im Azure AD mit einer begrenzten Gültigkeitsdauer versehen. Bitte denken Sie stets daran, rechtzeitig ein neues Anwendungskennwort im Azure AD festzulegen und in den SX-GATE zu übertragen.

NTP Zeitserver aktivieren

Systemzeit mit Zeitserver abgleichen und lokal zur Verfügung stellen

Mit dieser Einstellung können Sie den NTP-Zeitserver auf Ihrem SX-GATE aktivieren. Der Dienst erfüllt zwei Aufgaben. Einerseits synchronisiert er die Systemzeit mit öffentlich verfügbaren Zeitservern im Internet. Andererseits können andere Systeme dann SX-GATE als ihren Zeitserver nutzen.

Systemzeit mit Zeitserver abgleichen und lokal zur Verfügung stellen

- ja
Lesen Sie bitte weiter bei **NTP Zeitserver** (S. 242)
- nein
Lesen Sie bitte weiter bei **Konfiguration übernehmen** (S. 242)

NTP Zeitserver

Namen oder IP-Adressen der Zeitserver

Konfigurieren Sie hier die Zeitserver, mit denen SX-GATE die Systemzeit abgleichen soll.

Konfiguration übernehmen

Die Konfiguration des SX-GATE wurde bis jetzt noch nicht verändert. Drücken Sie auf "Fertigstellen" um Änderungen in das System zu übernehmen oder "Abbrechen" um keine Änderungen vorzunehmen.

13.3 Proxy-Konfiguration

Browser Konfiguration

Wie werden die Browser konfiguriert?

Die Browser können entweder manuell konfiguriert werden oder die Proxy-Einstellungen automatisch mittels Web-Proxy Auto-Discovery (WPAD) beziehen. Ist am Arbeitsplatz-Rechner DHCP aktiv, so kann WPAD über DHCP zum Einsatz kommen. Nur wenige Browser unterstützen dieses Verfahren. WPAD über DNS hat mit diesen Einschränkungen nicht zu kämpfen. Dazu wird jedoch der Intranet-HTTP-Server des SX-GATE benötigt.

manuell oder zentral

Wählen Sie diese Einstellung, um die Browser-Konfiguration komplett manuell vorzunehmen, wenn Sie im Browser eine zentrale Konfigurationsdatei (Proxy-Autoconf URL) einstellen wollen oder wenn Sie eine Active-Directory Gruppenrichtlinie nutzen möchten.

automatisch (WPAD)

In dieser Einstellung lässt sich die WPAD-Unterstützung im SX-GATE einrichten. Browser können dann die Proxy-Konfiguration automatisch vornehmen, sofern diese Möglichkeit im Browser aktiviert ist. Eine manuelle Konfiguration der Browser (siehe vorherige Option) ist unabhängig davon nach wie vor möglich.

Wie werden die Browser konfiguriert?

- manuell oder zentral
Lesen Sie bitte weiter bei [Manuelle oder zentrale Browser-Konfiguration](#) (S. 243)
- automatisch (WPAD)
Lesen Sie bitte weiter bei [Web-Proxy Auto-Discovery \(WPAD\)](#) (S. 244)

Manuelle oder zentrale Browser-Konfiguration

Manuelle Browser-Konfiguration

Öffnen Sie die Eingabemaske für Proxy-Einstellungen im Browser und konfigurieren Sie SX-GATE's IP-Adresse zusammen mit Port "8080" als Proxy-Server. Verwenden Sie diese Einstellungen für alle Protokolle außer "SOCKS". Zumindest auf dem Administrator-PC empfiehlt es sich, Zugriffe auf die SX-GATE Administrations-Oberfläche unter Umgehung des Proxies direkt durchzuführen. Fügen Sie daher die IP-Adresse des SX-GATE in die Liste der direkt zu kontaktierenden Server ein.

Zentrale Browser-Konfiguration

In den Proxy-Einstellungen der Browser bzw. in den Active Directory Gruppenrichtlinien kann die Adresse einer Proxy-Autoconf-Datei hinterlegt werden. Der SX-GATE Administrations-Webserver bietet eine passende Datei an. Um diese zu nutzen, tragen Sie bitte die Adresse "http://<SX-GATES LAN-IP>:8000/proxy.pac" ein.

Lesen Sie bitte weiter bei [Web-Proxy Zugriff](#)

Web-Proxy Auto-Discovery (WPAD)

Die meisten Web-Browser können die Proxy-Konfiguration automatisch beziehen. Dazu lädt der Browser eine Konfigurationsdatei von einem Web-Server herunter. Die Adresse dieser Datei wird mit Hilfe der Web-Proxy Auto-Discovery (WPAD) ermittelt. Dieses Verfahren sieht u.a. vor, die Adresse via DHCP bekannt zu geben. Bislang wird dies aber nur vom Microsoft Internet Explorer unterstützt sofern auf dem Client DHCP aktiv ist. Alternativ kommt ein DNS basiertes Verfahren zum Einsatz. Dieses wird auch von anderen Browsern unterstützt und funktioniert auch dann, wenn DHCP nicht verwendet wird.



In den Browsern muss die automatische Suche nach Proxy-Einstellungen aktiviert sein.

WPAD über DHCP verwenden

Die DHCP-Methode wird bislang nur vom Microsoft Internet-Explorer unterstützt. Der Arbeitsplatz-Rechner muss zudem den SX-GATE DHCP-Server nutzen.



Wird nicht SX-GATES DHCP-Server sondern ein anderer DHCP-Server genutzt, so muss die WPAD-URL auf diesem hinterlegt werden. Tragen Sie die URL "http://<SX-GATES LAN-IP>:8000/proxy.pac" ein, um SX-GATES vordefinierte Proxy-Autoconf-Datei zu verwenden.

WPAD über DNS verwenden

Das alternative DNS basierte Verfahren aktivieren Sie hier. Der Browser versucht dabei die Datei "wpad.dat" vom Web-Server mit der Adresse "wpad.<LOKALE DOMAIN>" herunterzuladen.

Geben Sie hier die Netzwerk-Domain ein, die in Ihren Arbeitsstationen eingestellt ist. SX-GATE richtet dann passende DNS-Einträge in seinem Name-Server ein und aktiviert im Intranet-Web-Server eine Umleitung der Datei "wpad.dat" auf die Adresse "http://<SX-GATES LAN-IP>:8000/proxy.pac"

. Dabei handelt es sich um eine vordefinierte Konfigurationsdatei, die Browser anweist, den SX-GATE Web-Proxy zu nutzen.



Sollten sich die Arbeitsstationen in verschiedenen Subdomains befinden (z.B. "vertrieb.example.com" und "management.example.com"), so können Sie die gemeinsame Hauptdomain eintragen ("example.com").

Web-Proxy Zugriff

Der Web-Proxy des SX-GATE ist für den gesicherten Browser-Zugriff auf das Internet zuständig. Neben HTTP und HTTPS wird auch der Browser-Zugriff auf FTP-Adressen unterstützt. Für reine FTP-Clients kann der Web-Proxy nicht verwendet werden. Aktivieren Sie dazu den FTP-Proxy. Im Laufe dieses Assistenten wird Ihnen die entsprechende Option angeboten.

Zugriff für Browser mit konfiguriertem Web-Proxy

Bevorzugt sollte der Proxy in den Browsern konfiguriert werden. Nur so ist eine Benutzeranmeldung am Proxy möglich. Ferner kann auch auf unübliche HTTP Ports ohne weiteres zugegriffen werden.

Proxy-Authentifizierung

Wählen Sie hier bitte aus, ob und wie sich Benutzer am Proxy anmelden müssen.

ohne Benutzeranmeldung

In dieser Einstellung kann der Proxy ohne vorherige Anmeldung genutzt werden. Die Möglichkeit benutzerbezogene Einstellungen vorzunehmen geht hier jedoch verloren.

manuelle Benutzeranmeldung

Wählen Sie diese Einstellung um Benutzern erst nach Eingabe von Benutzername und Kennwort Zugriff auf das Internet zu gewähren. Legen Sie die gewünschten Benutzer in der Benutzerverwaltung an und ordnen Sie diese der Gruppe "system-proxy" zu.

automatische Benutzeranmeldung (NTLM)

Dabei wird der Benutzer automatisch mit seiner derzeitigen Windows-Domänenanmeldung authentifiziert. Eine manuelle Eingabe von Benutzername und Kennwort ist nicht erforderlich, es sei denn, der Browser unterstützt diese Art der Anmeldung nicht. In diesem Fall müssen die Zugangsdaten eines berechtigten Windows-Benutzers eingegeben werden.



Bei NTLM-Authentifizierung ist nicht die SX-GATE-Gruppe "system-proxy" ausschlaggebend dafür, ob eine Benutzer berechtigt ist den Web-Proxy zu nutzen oder nicht. Von daher ist es auch nicht notwendig, für diesen Zweck Benutzerkonten im SX-GATE anzulegen.

Proxy-Authentifizierung

- ohne Benutzeranmeldung
Lesen Sie bitte weiter bei [Web-Proxy Filter](#) (S. 248)
- manuelle Benutzeranmeldung
Lesen Sie bitte weiter bei [Web-Proxy Filter](#) (S. 248)
- Benutzeranmeldung an LDAP-Server
Lesen Sie bitte weiter bei [Web-Proxy Filter](#) (S. 248)
- Benutzeranmeldung an Windows (veraltet)
Lesen Sie bitte weiter bei [Web-Proxy Filter](#) (S. 248)

Zugriff für Browser ohne Proxy-Konfiguration (Transparenter Proxy)

Nicht immer ist es erwünscht oder möglich, Proxyeinstellungen in den Browsern vorzunehmen. Mit den folgenden Optionen werden Web-Proxy und Firewall des SX-GATEs so umkonfiguriert, dass HTTP- bzw. HTTPS-Zugriffe auf die Standard-Ports 80 und 443 automatisch an den Web-Proxy umgeleitet werden. Der Assistent passt dabei grundsätzlich nur die Firewall-Konfiguration der Ethernet-Schnittstelle "eth0" an. Ein Parallelbetrieb von Browsern mit und ohne konfiguriertem Proxy ist möglich.



Bei transparenten Zugriffen findet grundsätzlich keine Benutzeranmeldung am Proxy statt.



Für Browser ohne Proxy-Konfiguration sind einige Besonderheiten zu beachten. Damit der transparente Zugriff funktioniert, muss SX-GATE in der Netzwerk-Konfiguration der Arbeitsstation als Gateway eingetragen sein. Zudem wird DNS benötigt. Für FTP-Zugriffe ist im weiteren Verlauf des Assistenten der transparente FTP-Proxy zu aktivieren. Internet-Zugriffe mit HTTP und HTTPS zu anderen Ports als 80 bzw. 443 sind nicht ohne weiteres möglich. Dazu muss die Firewall-Konfiguration angepasst werden.

Windows Einstellungen

IP-Adresse des ActiveDirectory-Servers

Um SX-GATE an ein ActiveDirectory anzubinden, geben Sie hier bitte die IP-Adresse des Servers ein. Falls Sie die Anbindung im NT4-Kompatibilitätsmodus betreiben möchten, geben Sie bitte stattdessen den NetBIOS-Namen Ihrer Windows-Domäne ein.



Der NetBIOS-Domänen-Name wird u.a. in der "Netzwerkumgebung" angezeigt - ggf. unter der Bezeichnung "Arbeitsgruppe". Ein NetBIOS-Domänen-Name enthält in der Regel keinen Punkt (z.B. "EXAMPLE"). Im Gegensatz dazu entspricht der Active-Directory Domain-Name einer Internet-Domain und enthält daher zumindest einen Punkt (z.B. "example.com").

Erlaubte Benutzer

Wählen Sie hier aus, welche Benutzer Zugriff auf den Proxy erhalten sollen.

Domänen-Konto erstellen

Um zukünftig die Anmeldung an die Windows-Domäne delegieren zu können, muss für SX-GATE ein Computer-Konto in der Domäne erstellt werden. Geben Sie dazu bitte die Zugangsdaten eines Administratoren-Kontos ein.



Dies ist ein einmaliger Vorgang. Die Zugangsdaten werden daher nicht gespeichert.

Administrator Login

Geben Sie hier bitte den Kontonamen eines Windows Administrators ein. Falls Sie bereits ein Computer-Konto für SX-GATE erstellt haben, brauchen Sie keine Zugangsdaten anzugeben. Lassen Sie das Feld einfach leer. Das System prüft dann auf der nächsten Maske, ob das Computer-Konto noch gültig ist.

Web-Proxy Filter

URL-Filter

SX-GATE enthält eine nach Kategorien aufgeteilte Datenbank von Internet-Adressen, auf die der Zugriff beschränkt werden kann. Darüber hinaus besteht die Möglichkeit, selbst Adress-Listen anzulegen oder den Zugriff auf bestimmte Datei-Typen anhand des Namens zu verbieten. Der Filter wird mit Hilfe dieses Schalters aktiviert.



Im Menü "Definitionen > URL-Filter Listen" werden die Listen zusammengestellt. Unter "Module > Web-Proxy > URL-Filter" werden die Listen für einzelne IP-Adressen oder Benutzergruppen aktiviert.

Content-Filter

Aktivieren Sie diesen Filter wenn Dateien, die über den Web-Proxy des SX-GATE heruntergeladen werden, geprüft werden sollen.



In der Grundeinstellung ist lediglich die Virenprüfung aktiviert. Aus Performance-Gründen sind dabei bestimmte Inhalts-Typen ausgenommen.



Für die Virenprüfung muss auf SX-GATE ein funktionsfähiger Virens Scanner installiert sein. Die Lizenzen für den Virens Scanner sind nicht im SX-GATE enthalten und müssen separat erworben werden.

FTP-Proxy

Soll der FTP-Proxy aktiviert sein?

Für den FTP-Zugriff auf das Internet stellt SX-GATE einen eigenen Proxy zur Verfügung.

ja

In dieser Einstellung kann der FTP-Proxy ausschließlich von reinen FTP-Clients, nicht jedoch durch Web-Browser genutzt werden.



Der nicht-transparente FTP-Zugriff für Web-Browser erfolgt über den Web-Proxy auf Port 8080.

Konfigurieren Sie im FTP-Client SX-GATE als Proxy auf Port 2121. Die Bezeichnung für den einzustellenden Proxy-Typ variiert. Üblich sind "USER ohne Login", "USER with no login" und "USER user@host:port". Kann im FTP-Client kein Proxy eingestellt werden, so muss unabhängig vom eigentlichen Ziel stets eine FTP-Verbindung zu Port 2121 des SX-GATE aufgebaut werden (z.B. "ftp 192.168.0.254 2121"). Geben Sie hier den Benutzernamen auf dem Ziel-Server gefolgt von einem "@"-Zeichen und der Adresse des Ziel-Servers ein (z.B. "benutzer@ftp.example.com").



Um den Proxy zu nutzen muss dieser im FTP-Client als Proxy konfiguriert sein bzw. die Verbindung manuell über Port 2121 des SX-GATE aufgebaut werden.

ja, als transparenter Proxy

Die Firewall-Konfiguration der Ethernet-Schnittstelle "eth0" wird bei Auswahl dieser Option so umkonfiguriert, dass Verbindung zu Port 21 automatisch an den FTP-Proxy umgelenkt werden. Der FTP-Proxy kann auf diese Weise sowohl von FTP-Clients als auch von Web-Browsern genutzt werden ohne den Proxy in deren Konfiguration einzutragen.



Damit der transparente Zugriff funktioniert, muss SX-GATE in der Netzwerk-Konfiguration der Arbeitsstation als Gateway eingetragen sein. Häufig wird zudem DNS benötigt.

Soll der FTP-Proxy aktiviert sein?

- nein

Lesen Sie bitte weiter bei [Konfiguration übernehmen](#) (S. 251)

FTP-Proxy Filter

FTP-Proxy Virenskan

Um Dateien die über den FTP-Proxy heruntergeladen werden auf Viren zu prüfen, muss dieser Schalter aktiviert werden.



Diese Option ist wirkungslos wenn auf SX-GATE kein funktionsfähiger Virens Scanner installiert ist. Die Lizenzen für den Virens Scanner sind nicht im SX-GATE enthalten und müssen separat erworben werden.

FTP-Zieladressen

FTP-Proxy erlaubt Zugriff auf

Wählen Sie, zu welchen Konten auf welchem FTP-Server Verbindungen aufgebaut werden dürfen.

bestimmte FTP-Server und Konten

Wählen Sie diese Einstellung um in der Folgemaske den Zugriff auf einzelne Adressen zu beschränken.

beliebige FTP-Server und Konten

Diese Option gestattet den Zugriff auf beliebige FTP-Server. Sowohl der Zugriff ohne Anmeldung (anonymous FTP) also auch mit Anmeldung als bestimmter Benutzer ist möglich.

FTP-Proxy erlaubt Zugriff auf

- beliebige FTP-Server und Konten

Lesen Sie bitte weiter bei **Konfiguration übernehmen** (S. 251)

FTP-Proxy Ziel-Adressen

Vom FTP-Proxy akzeptierte Ziel-Adressen

Legen Sie hier fest, auf welche Konten welchen FTP-Servers zugegriffen werden darf. Ist die Liste leer, so verweigert der FTP-Proxy alle Zugriffe.

Konto

Geben Sie hier das Konto des FTP-Servers an auf das zugegriffen werden soll. Für Zugriff ohne Anmeldung (anonymous FTP) wählen Sie bitte "ftp (anonymous)" aus. Um ausschließlich die Anmeldung als bestimmter Benutzer zu akzeptieren, ist stattdessen der Login in der Option darüber einzugeben. Lassen Sie das Eingabefeld leer um den Zugriff auf beliebige Konten des FTP-Servers zu erlauben.

Ziel-Server

Der Name bzw. die IP-Adresse des Ziel-FTP-Servers ist hier anzugeben. Wird keine Adresse angegeben, so akzeptiert der Proxy Zugriffe auf beliebige FTP-Server.

Nachfolgend einige typische Beispielregeln, die Sie je nach Bedarf kombinieren können.

Zugriff auf beliebige FTP-Server mit anonymous FTP

Wählen Sie "ftp (anonymous)" aus und drücken Sie "Hinzufügen". Es wird die Regel "ftp@*" in die Liste aufgenommen.



Der Zugriff auf frei verfügbare Daten ist mit Hilfe dieser Regel möglich, während der Zugang zu geschützten Bereichen wie z.B. die Pflege privater Homepages nicht möglich ist.

Zugriff auf alle Konten eines bestimmten FTP-Servers

Geben Sie den Servernamen (z.B. ftp.example.com) als "Ziel-Server" ein, wählen Sie die obere Option bei "Konto", lassen Sie das zugehörige Eingabefeld jedoch frei. "Hinzufügen" erzeugt die Regel "*@ftp.example.com".

Zugriff auf ein bestimmtes Konto eines bestimmten FTP-Servers

Tragen Sie Konto und Servername in die entsprechenden Felder ein und drücken Sie "Hinzufügen". Die erstellte Regel lautet dann z.B. "webmaster@www.example.com".

Konfiguration übernehmen

Die Konfiguration des SX-GATE wurde bis jetzt noch nicht verändert. Drücken Sie auf "Fertigstellen" um Änderungen in das System zu übernehmen oder "Abbrechen" um keine Änderungen vorzunehmen.

13.4 E-Mail Einrichtung

Konfiguration der E-Mail Dienste

Welchen Bereich wollen Sie konfigurieren?

Um das komplette Mail-System des SX-GATE zu konfigurieren, sollten Sie mit der ersten Option "Lokale und interne Domains" beginnen. Am Ende dieses Bereiches wird Ihnen angeboten, zunächst auch die weiteren Bereiche abzuarbeiten, so dass schließlich alle notwendigen Einstellungen abgefragt wurden. Dies ist insbesondere bei der Erstinstallation wichtig. Sie können aber selbstverständlich jederzeit auch die Konfiguration von Teilbereichen anpassen. Wählen Sie dazu die gewünschte Option.



Die Einstellung, über welchen Mail-Relay-Server des Providers ausgehende E-Mails gesendet werden sollen, ist abhängig von Ihrem Internet-Zugang. Daher wird diese Einstellung im Assistenten "Assistenten > Internet-Zugang" vorgenommen

Wählen Sie "Lokale und interne Domains" um festzulegen, welche E-Mail Domains lokal verwaltet werden. SX-GATE kann selbst die Postfächer für diese Domains führen oder die E-Mails für diese Domains an einen anderen Mail-Server in Ihrem LAN weiterleiten.

Sicherheitsmechanismen und Filter wie der Mail-Virens scanner werden in "Mail-Filter" aktiviert.

Die erforderlichen Einstellungen für den Empfang von E-Mails können Sie im Bereich "Mail-Empfang" vornehmen. Sofern SX-GATE E-Mails von POP-Servern im Internet abholen muss, können Sie die jeweiligen Postfächer angeben. Werden die E-Mails von einem ETRN-Server abgerufen oder direkt per SMTP zugestellt, kann die notwendige Firewall-Konfiguration vorgenommen werden.



Mit dem Fertigstellen dieses Konfigurations-Assistenten wird das Mail-System des SX-GATE aktiv. Stellen Sie daher zuvor sicher, dass die Benutzer-Postfächer verfügbar sind. Alternativ können Sie diese Option überspringen und "Mail-Empfang" später konfigurieren.

Zeitabhängigen Parameter für den Versand und die Abholung von E-Mails werden schließlich unter "Versand- und Abholzeiten" eingestellt. Diese lassen sich für die Art Ihrer Internet-Anbindung optimieren.

Welchen Bereich wollen Sie konfigurieren?

- Lokale und interne Domains
Lesen Sie bitte weiter bei [Domains](#) (S. 253)
- Mail-Filter
Lesen Sie bitte weiter bei [SPAM-Filter aktivieren](#) (S. 258)
- Mail-Empfang
Lesen Sie bitte weiter bei [Mail-Empfang](#) (S. 264)
- Versand- und Abholzeiten
Lesen Sie bitte weiter bei [Sendewarteschlange](#) (S. 271)

Domains

SX-GATE kann mehrere lokale und/oder interne Domains verwalten.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

E-Mail Domain

Geben Sie hier eine E-Mail-Domain ein. Mails an diese Domain werden dann entweder in ein lokales Postfach auf SX-GATE zugestellt oder an einen internen Mailserver weitergeleitet.

Domain-Typ

E-Mails zustellen an

Wählen Sie "an SX-GATE Postfach" wenn SX-GATE selbst als E-Mail-Server fungieren soll. E-Mails an die Domains, die Sie nachfolgenden spezifizieren können, werden dabei in Postfächer auf dem SX-GATE zugestellt. Auf diese können die Benutzer dann mit Hilfe der SX-GATE-Groupware zugreifen oder die Mails mit einem Mail-Client über das POP3- oder IMAP4-Protokoll abrufen.



Um ein Benutzer-Postfach auf dem SX-GATE einzurichten, müssen Sie in der Benutzerverwaltung (System > Benutzerverwaltung > Benutzer) die entsprechenden Benutzer anlegen und diese der Gruppe "system-mail" zuordnen.

Sofern Sie bereits einen Mail-Server in Ihrem LAN betreiben und diesen auch weiterhin nutzen wollen, kann SX-GATE alle E-Mails, die an bestimmte Domains adressiert sind, an diesen internen Mail-Server weiterleiten. Für die E-Mail-Kommunikation mit dem Internet können so die Sicherheitsmechanismen des SX-GATE Mail-Servers genutzt werden, ohne auf das bestehende Mail-System verzichten zu müssen. Um dieses Szenario zu konfigurieren wählen Sie bitte "an internen Mail-Server".

E-Mails zustellen an

- an SX-GATE Postfach
Lesen Sie bitte weiter bei **Benutzer** (S. 254)
- an internen Mail-Server
Lesen Sie bitte weiter bei **Empfänger verifizieren** (S. 254)

Benutzer

Benutzer mit Mail-Berechtigung

Hier legen Sie fest, welche Benutzer Mitglied in der SX-GATE Gruppe "system-mail" sind. Für Mitglieder ist auf dem SX-GATE ein Mail-Konto bestehend aus einem Postfach und der zugehörigen E-Mail-Adresse eingerichtet. Die Benutzer können auf ihre Mails mit POP3, IMAP4 oder der SX-GATE-Groupware zugreifen.



Um neue Benutzer anzulegen wechseln Sie bitte nach Beendigung dieses Assistenten in die Benutzerverwaltung. Legen Sie dort die benötigten Benutzer an und nehmen Sie diese in die Gruppe "system-mail" auf.

Empfänger verifizieren

Empfänger-Adressen vorab verifizieren

Aktivieren Sie diese Option, damit SX-GATE beim Empfang jeder Mail zunächst überprüft, ob der interne Mail-Server eine E-Mail mit den angegebenen Empfänger-Adressen überhaupt akzeptieren würde. Die Überprüfung findet schon statt, bevor der eigentliche Inhalt der Mail an SX-GATE übermittelt wird. Mails an unbekannte Empfänger werden so gar nicht erst angenommen.



Diese Option wirkt auf alle Empfänger-Domains, die SX-GATE an einen internen Mail-Server weiterleitet.



Die Adressverifikation wird auch dann aktiv, wenn SX-GATE E-Mails von einem POP- oder IMAP-Server abholt. Verweigert der interne Mail-Server die Annahme, wird die Mail in der Regel kommentarlos verworfen.

mit SMTP

Dies ist das einfachste Verfahren, das mit fast allen Mail-Servern funktioniert. Für jede eingehende E-Mail öffnet SX-GATE eine SMTP-Verbindung zum internen Mail-Server. Die vom Sender übermittelten Absender- und Empfänger-Adressen der E-Mail werden an den internen Mail-Server durchgereicht. Anhand der Rückmeldungen des internen Servers wird nun dem Sender signalisiert, ob dieser mit der Übertragung der Mail fortfahren darf oder ob die Annahme der Mail z.B. aufgrund ungültiger Adressdaten verweigert wird.



Mit diesem Verfahren können Sie sogar etwaige Optionen Ihres internen Mail-Servers zur Sperrung bestimmter Absender-Adressen nutzen.



Stellen Sie sicher, dass der interne Mail-Server nicht existierenden Empfänger-Adresse unmittelbar zurückweist. Nachfolgend ist beschrieben, wie Sie dies in Microsoft Exchange aktivieren können.

Bei Microsoft Exchange Servern muss zunächst der Empfängerfilter aktiviert werden. Installieren Sie dazu die Antispam-Agents indem Sie das Skript "Install-AntispamAgents" in den Unterordnern des Exchange Programm-Ordners suchen und starten. Aktivieren Sie dann den Empfängerfilter in der Exchange Management-Shell mit dem Befehl

```
"Set-RecipientFilterConfig -Enabled $true -RecipientValidation-Enabled $true"
```

. Seit Exchange 2013 muss ferner ein zusätzlicher HubTransport-Connector vom Exchange-Server bereitgestellt werden (Typ: Internet). Der Connector muss anonymen Zugriff erlauben. Wir empfehlen ferner, dass ausschließlich die SX-GATE-IP Zugriff auf diesen Connector erhält. Bei aktivierter Windows-Firewall muss üblicherweise der Zugriff auf den neuen Connector-Port mit einer zusätzlichen Regel freigegeben werden. Tragen Sie die Port-Nummer des Connectors schließlich im SX-GATE auf der nachfolgenden Bildschirmmaske ein.

mit LDAP (Active-Directory)

Die gewünschten Empfänger-Adressen werden bei diesem Verfahren im Active-Directory gesucht (Attribut "proxyAddresses"). Die notwendigen Parameter für die LDAP-Suche werden auf der Folgemaske abgefragt.

Empfänger-Adressen vorab verifizieren

- deaktiviert
Lesen Sie bitte weiter bei [Interner Mail-Server](#) (S. 257)
- mit SMTP
Lesen Sie bitte weiter bei [Empfänger mit SMTP-Callout verifizieren](#) (S. 256)
- mit LDAP (Active-Directory)
Lesen Sie bitte weiter bei [Empfänger mit LDAP verifizieren](#) (S. 256)

Empfänger mit SMTP-Callout verifizieren

SMTP-Port für Verifikation

Die Verifikation der Adressen kann über einen vom Mailversand abweichenden Port erfolgen.

Lesen Sie bitte weiter bei [Interner Mail-Server](#)

Empfänger mit LDAP verifizieren

Active-Directory Server

Hier legen Sie die IP-Adresse des Active-Directory Servers fest, auf dem die Benutzerdaten gespeichert sind. Dies ist in der Regel die Adresse Ihres Domänen-Controllers.

LDAP-Suchpfad

Geben Sie hier den LDAP-Pfad an, an den sich SX-GATE im Active-Directory binden soll. Alle relevanten Benutzer und Gruppen müssen hierarchisch unterhalb dieses Pfades befinden.

Im einfachsten Fall geben Sie hier lediglich den Namen des Active-Directories an (z.B. ad.example.com). Es kann jedoch auch ein exakter Distinguished Name (DN) angegeben werden wie z.B. "CN=users,DC=ad,DC=example,DC=com" oder "OU=internet-benutzer,DC=ad,DC=example,DC=com".

Benutzername für Suche im Active-Directory

Ist die anonyme Suche im Active-Directory erlaubt, kann dieses Feld leer bleiben. Geben Sie andernfalls den Anmeldenamen eines Benutzers ein, der die notwendigen Berechtigungen hat (Bind DN). Befinden sich der Benutzer im Active-

Directory Container "users", genügt hier die Eingabe des Benutzernamens (z.B. "suchbenutzer"). Andernfalls muss der vollständige DN angegeben werden (z.B. "CN=suchbenutzer,OU=edv,DC=ad,DC=example,DC=com").



Im Microsoft SBS lautet der Standardpfad für Benutzer beispielsweise "cn=suchbenutzer,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=example,DC=com" und muss daher als DN angegeben werden.

Passwort

Ist eine Anmeldung am Active Directory erforderlich, so geben Sie hier bitte das entsprechende Kennwort ein.

SSL Verschlüsselung

Durch Aktivieren dieser Option wird die Kommunikation zwischen SX-GATE und dem Active Directory verschlüsselt. Der Active Directory Server nimmt SSL-Verbindungen nur an, wenn im Windows Zertifikatsspeicher ein entsprechendes Zertifikat hinterlegt wurde.

Lesen Sie bitte weiter bei [Interner Mail-Server](#)

Interner Mail-Server

Mails weiterleiten an Mail-Server

Tragen Sie bitte die Adresse des internen Mail-Servers ein. Alle Mails, die an einen Empfänger aus der aktuell gewählten Domain gerichtet sind, werden nicht in das Internet weitergeleitet, sondern umgehend an den internen Mail-Server mit SMTP zugestellt. Richten Sie dazu bitte entsprechende Mail-Verteiler und Benutzer-Konten auf Ihrem internen Mail-Server ein.



Um Mail-Schleifen zu vermeiden, muss der interne Mail-Server die Domain als lokale Domain behandeln. Er darf seinerseits nicht versuchen, diese E-Mails zurück in das Internet zu schicken.

SPAM-Filter aktivieren

SPAM-Filter Konfiguration

Unter einer SPAM-Mail versteht man eine unerwünschte Werbe-Mail mit meist dubioser Herkunft. SX-GATES SPAM-Filter identifiziert diese Mails und macht sie entweder deutlich erkennbar oder verweigert die Annahme bzw. verwirft die Mail.



Die Auswahl einer der Optionen beeinflusst lediglich, welche Bildschirmmasken nachfolgend angezeigt werden. Einen unmittelbaren Einfluss auf die Konfiguration des SX-GATE gibt es nicht.

SPAM-Filter Konfiguration

- gemeinsamen SPAM-Filter konfigurieren
Lesen Sie bitte weiter bei [Gemeinsamer SPAM-Filter](#) (S. 258)
- individueller SPAM-Filter je SX-GATE Benutzer-Postfach
Lesen Sie bitte weiter bei [Individueller SPAM-Filter](#) (S. 258)
- SPAM-Filter-Konfiguration überspringen
Lesen Sie bitte weiter bei [Virens Scanner aktivieren](#) (S. 262)

Individueller SPAM-Filter

Der individuelle SPAM-Filter je SX-GATE Benutzer-Postfach muss in der Benutzer-Verwaltung für jedes Konto separat konfiguriert werden.

Lesen Sie bitte weiter bei [SPAM-Filter Einstellungen](#)

Gemeinsamer SPAM-Filter

Um den SPAM-Mail-Filter zu aktivieren, müssen Sie mindestens einen der Schwellwerte festlegen. Damit aktivieren Sie den SPAM-Mail-Filter im Relay-Modus. In diesem Modus untersucht der SPAM-Filter jede eingehende E-Mail während sie den SX-GATE Mail-Server passiert. Dabei ist es nicht möglich, unterschiedliche Schwellwerte in Abhängigkeit des Benutzers zu definieren, da die Mail-Adressen ja nicht vom SX-GATE sondern vom internen Mail-Server verwaltet werden.

Der SPAM-Mail-Filter des SX-GATE klassifiziert automatisch den Inhalt von E-Mails anhand typischer Phrasen oder anderer Merkmale die auf eine unerwünschte Werbe-Mail (SPAM-Mail) zutreffen. Dazu ist im SX-GATE eine Datenbank mit Kriterien enthalten, die mit einem Punktesystem bewertet werden. Das erreichte Punkteergebnis ermöglicht das Filtern von E-Mails. Alle Merkmale, die auf eine SPAM-Mail hindeuten, erhöhen den Punktestand, während für Merkmale die auf eine reguläre

Mail hindeuten wieder Punkte abgezogen werden. Je höher das Bewertungsergebnis, umso wahrscheinlicher handelt es sich um eine SPAM-Mail.



E-Mails mit einer Größe von mehr als 1MB werden vom SPAM-Mail-Filter nicht klassifiziert um Ressourcen zu schonen. Dies stellt jedoch keine Beeinträchtigung dar, da SPAM-Mails typischerweise deutlich kleiner sind.

Jede untersuchte E-Mail wird vom SPAM-Mail-Filter um Kopfzeilen (Header) erweitert. Der "X-Spam-Status" zeigt den erreichten Punktwert (hits=...) sowie die Kurznamen der Merkmale, die zu diesem Punktestand geführt haben (tests=...). Dies ermöglicht es dem Empfänger, das Resultat des SPAM-Filters zu überprüfen. Die Kopfzeile "X-Spam-Level" enthält je ein "x" pro vollem erreichten Punkt (z.B. "X-Spam-Level: xxx" bei einer Punktezahl zwischen 3.00 und 3.99). Dieser Header ist bestens geeignet, um E-Mails im Mail-Programm des Benutzers automatisch zu sortieren.



Bei den meisten Mail-Programmen werden im Normalfall nur die wichtigsten Kopfzeilen angezeigt. Die weiteren Header sind aber in der Regel über einen entsprechenden Menüpunkt zugänglich.

E-Mail als SPAM markieren bei mehr als

Überschreitet der Punktwert einer E-Mail bei deren Klassifizierung diesen Schwellwert, so wird die E-Mail als SPAM-Mail markiert. Dabei wird dem Betreff der Text "***** SPAM *****" vorangestellt. Zudem enthält die E-Mail dann eine kurze Beschreibung, wie sich dieser Punktwert zusammensetzt. Die Original-Mail ist als Anhang zugeordnet.

Durch die Verschiebung der ursprünglichen Mail in den Anhang soll verhindert werden, dass das bloße Anklicken der E-Mail bereits unerwünschte Aktionen auslöst. In Abhängigkeit vom verwendeten Mail-Programm genügt eventuell bereits das Auswählen einer E-Mail, um durch die Vorschaufunktion z.B. Bilder zu einer mit HTML formatierten Mail aus dem Internet nachzuladen. Der Versender der SPAM-Mail erhält so unbemerkt Rückmeldung darüber, dass die SPAM-Mail geöffnet wurde. Als Folge davon wird die E-Mail-Adresse als lohnendes Ziel für weitere SPAM-Mails registriert, was sich auf Dauer zu einer wahren Flut von SPAM-Mails entwickeln kann.

Annahme verweigern bei mehr als

Beim Überschreiten des hier eingestellten Schwellwerts verweigert SX-GATE's Mail-Server die Annahme der betroffenen E-Mail. Es ist in diesem Fall Aufgabe des zustellenden Systems entsprechend zu reagieren und z.B. den Absender oder einen Administrator darüber zu informieren. Wenn Sie sichergehen wollen, dass keine gewünschte E-Mail verloren geht, sollten Sie diese Option nicht aktivieren. Nutzen Sie stattdessen den Schwellwert "E-Mail als SPAM markieren bei mehr als" zusammen

mit den Möglichkeiten der Mail-Client-Programme zur automatischen Sortierung von E-Mails basierend auf den Kopfzeilen.



E-Mails die durch den SX-GATE Mail-Client von POP-Servern abgeholt wurden verwirft der Mail-Client kommentarlos wenn SX-GATE's Mail-Server die Annahme aufgrund des SPAM-Filters verweigert. Es erfolgt weder eine Benachrichtigung noch lässt sich eine so gelöschte E-Mail wiederherstellen. Die E-Mail ist unwiederbringlich verloren!



Um den Verlust von wichtigen E-Mails zu vermeiden, sollten Sie bei der Konfiguration dieser Einstellung sehr vorsichtig sein. Stellen Sie lieber einen zu hohen als einen zu niedrigen Wert ein. Bitte beachten Sie, dass das automatische Löschen von E-Mails durch Vorschriften oder Gesetze mit bestimmten Auflagen verbunden oder sogar verboten sein kann.

SPAM-Filter Einstellungen

Neben der integrierten Regel-Datenbank kann der SX-GATE SPAM-Filter auch mit verschiedenen Echtzeit-Listen im Internet Kontakt aufnehmen. Auf diese Weise kann die Qualität der SPAM-Erkennung drastisch gesteigert werden.



Die in dieser Maske eingestellten Parameter gelten sowohl für den globalen Relay-SPAM-Filter als auch für die persönlichen SPAM-Filter der lokalen Benutzer. Letztere müssen in der SX-GATE Benutzerverwaltung individuell aktiviert werden.



Aktivieren Sie diese Optionen nicht, wenn Sie über eine teure Wählleitung an das Internet angebunden sind. Je nach Konfiguration wird selbst für interne E-Mails eine Verbindung in das Internet aufgebaut. Dies kann zu sehr hohen Online-Zeiten mit entsprechenden Kosten führen.

Ebenfalls äußerst sinnvoll ist die Aktivierung des Bayes-Filters. Der SPAM-Filter passt sich damit permanent und automatisch an sein Umfeld an, indem er das typische Vokabular gewollter E-Mails erlernt und sich zugleich an die Themen aktueller SPAM-Wellen anpasst.

DNS basierende Listen

Im Internet stehen schwarze Listen (RBL: Realtime Black Lists) zur Verfügung, in denen die Mail-Server verzeichnet sind, von denen häufig SPAM-Mails versendet werden. Eine andere Form schwarzer Listen enthält die Adressen von Web-Servern, die oft mit Hilfe von SPAM-Mails beworben werden (URIBL: URI Black Lists). Das Ziel von Verweisen (Links) im Text von E-Mails wird gegen URL Black Lists geprüft. Darüber hinaus gibt es auch weiße Listen, in denen unauffällige Mail-Server verzeichnet sind.

Bei der Analyse einer Mail kann eine Reihe dieser Listen befragt werden. Jeder einzelne Treffer wird dabei jedoch nur mit einem relativ geringen Punktwert berücksichtigt. Nur wenn mehrere der Listen potentiellen SPAM melden, ist deren Einfluss signifikant. Je nachdem wie die Einträge in den Listen gewonnen wurden, unterscheidet sich deren Verlässlichkeit. Wählen Sie aus den folgenden Optionen die gewünschte Stufe aus.

wenige

Wählen Sie diese Einstellung, wenn nur ausreichend sichere SPAM-Quellen in die Bewertung einfließen sollen. Insbesondere automatisch erzeugte Listen werden hier nicht berücksichtigt. Die URI Black Lists sind aktiviert.

mittel

Zusätzlich zu sicheren SPAM-Quellen beinhaltet diese Stufe auch solche Adressen, die mit Hilfe automatischer SPAM-Fallen gewonnen wurden.

viele

Ist diese Option ausgewählt, so fließen zusätzlich bekannte dynamische IP-Adressen sowie koreanische und chinesische Relay-Server in die Bewertung ein.

Razor2 verteiltes Spamfilter Netzwerk aktivieren

Bei dieser Option wird eine unscharfe Prüfsumme über Teile der E-Mail gebildet und mittels eines eigenen Protokolls (TCP-Port 2703) an Razor2-Server im Internet übermittelt. Diese stellen eine Datenbank mit Prüfsummen bekannter SPAM-Mails zur Verfügung. Im Falle einer Übereinstimmung erhält die SPAM-Bewertung der E-Mail einen Aufschlag. Die Höhe dieses Aufschlags richtet sich nach der Vertrauenswürdigkeit der Instanzen, die dem Razor-System die SPAM-Mail gemeldet haben.

Bayes-Filter aktivieren

Wenn aktiviert, lernt der SPAM-Mail-Filter während des Bearbeitens eingehender E-Mails eigenständig Eigenschaften hinzu, die auf ungewollte Mails (SPAM) bzw. auf gewollte Mails (HAM) hindeuten. Dabei werden E-Mails mit mehr als 10 bzw. mit 0 oder weniger Bewertungspunkten berücksichtigt.



Der Bayes-Filter wird erst dann in die Bewertung einbezogen, wenn mind. 200 SPAM-Mails und mind. 200 HAM-Mails eingelernt wurden.

Virens Scanner aktivieren

Mail-Virens Scanner aktivieren

Aktivieren Sie diese Option, um alle E-Mails, die den Mail-Server des SX-GATE passieren, auf Viren überprüft werden sollen. Sowohl eingehende als auch ausgehende E-Mails werden geprüft.



Diese Funktion kann erst genutzt werden, wenn ein Virens Scanner auf dem SX-GATE installiert ist. Die Lizenzen für den Virens Scanner sind nicht im SX-GATE enthalten und müssen separat erworben werden.

Wenn in einer E-Mail ein Virus gefunden wird, so wird diese in einen Quarantäne-Bereich verschoben. Der Administrator wird davon per Mail in Kenntnis gesetzt. Bei bestimmten Virengattungen wie z.B. Makro-Viren aber auch dem EICAR-Virens Scanner-Testfile wird zudem der Absender der E-Mail benachrichtigt. Dem Administrator ist es möglich, auf den Quarantäne-Bereich zuzugreifen. 10 Tage nach dem letzten Lesezugriff auf eine E-Mail im Quarantäne-Bereich wird diese automatisch gelöscht.

Attachment-Filter aktivieren

Filterung von Dateianhängen

Dateianhänge können vom SX-GATE basierend auf der Endung des Dateinamens gefiltert werden. Wir empfehlen die Nutzung dieser Komponente insbesondere zur Verbesserung des Virenschutzes. Dies gilt selbst dann, wenn Sie bereits Virens Scanner einsetzen. In der Regel kann ein Virens Scanner einen Virus nur dann identifizieren, wenn er dessen Signatur bereits kennt. Durch die Filterung von Dateianhängen können Dateien ausgefiltert werden, die vom Virens Scanner nicht erkannt wurden, deren Dateianhänge jedoch für Viren typische Endungen haben. Auch lässt sich diese Komponente zur Durchsetzung von Bestimmungen nutzen, die den Versand bestimmter Dateiformate unterbinden sollen.

ein- und ausgehende E-Mails

Während bei eingehenden E-Mails meist ein Quarantäne-Verfahren zum Einsatz kommt, werden ausgehende E-Mails mit unerwünschten Anhängen grundsätzlich zurückgewiesen.

Filterung von Dateianhängen

- <nicht aktiviert>
Lesen Sie bitte weiter bei [Konfiguration übernehmen](#) (S. 263)
- nur eingehende E-Mails
Lesen Sie bitte weiter bei [Gefährliche Anhänge](#) (S. 263)
- ein- und ausgehende E-Mails
Lesen Sie bitte weiter bei [Gefährliche Anhänge](#) (S. 263)

Gefährliche Anhänge

Dateianhänge mit folgenden Dateierweiterungen oder MIME-Typen ausfiltern

Wenn der Dateiname eines E-Mail Anhangs mit einer der hier angegebenen Erweiterungen endet oder der "Content-Type"-Header eines Dateianhangs einem hier eingetragenen MIME-Typ entspricht, wird der Anhang vom Filter beanstandet. Die E-Mail als solches wird entweder zurückgewiesen, komplett zurückgehalten oder die beanstandeten Anhänge werden durch eine Warnmeldung ersetzt und die so modifizierte E-Mail dann an die Empfänger ausgeliefert.

Der Administrator oder ein Benutzer, dem vom Administrator die Zugriffsberechtigung für den Menüpunkt "Monitoring > Mail-Server" erteilt wurde, kann auf Dateianhänge im Quarantäne-Bereich zugreifen bzw. die Zustellung von zurückgehaltenen E-Mails veranlassen. Sie werden automatisch gelöscht, wenn die im Menü "Module > Mail-Server > SPAM/Virus/Malware" auf dem Reiter (Tab) "MIME-Filter" konfigurierte "Aufbewahrungszeit" überschritten ist.

Sie können Dateierweiterungen im Format ext, .ext oder *.ext angeben. Alle drei Formate sind gleichbedeutend. Die Groß-/Kleinschreibung spielt keine Rolle.

Alternativ können Sie auch MIME-Typen wie z.B. "application/zip" angeben. Ein Stern dient als Platzhalter (z.B. "application/*").

Konfiguration übernehmen

Die Konfiguration des SX-GATE wurde bis jetzt noch nicht verändert. Drücken Sie auf "Fertigstellen" um Änderungen in das System zu übernehmen oder "Abbrechen" um keine Änderungen vorzunehmen.

Mail-Empfang

Wie empfängt SX-GATE eingehende E-Mails aus dem Internet

Bei allen Arten der Internetanbindung kann es erforderlich sein, E-Mails von einem POP-Server im Internet abzurufen. Wenn SX-GATE über eine Wählleitung mit fester IP-Adresse an das Internet angebunden ist, kommt unter Umständen das ETRN-Protokoll zum Einsatz. Bei Standleitungen mit fester IP-Adresse ist SX-GATE jederzeit aus dem Internet adressierbar. In diesen Fällen könnten E-Mails direkt mit SMTP zugestellt werden. Wenn Sie sich nicht sicher sind, auf welchem Wege Sie eingehende E-Mails empfangen, so fragen Sie bitte bei Ihrem Provider nach.

Wie empfängt SX-GATE eingehende E-Mails aus dem Internet

- Durch Abruf vom POP- oder ETRN-Server eines Providers
Lesen Sie bitte weiter bei **Server** (S. 265)
- E-Mails werden direkt per SMTP zugestellt
Lesen Sie bitte weiter bei **Firewall-Zugriff für SMTP** (S. 264)

Firewall-Zugriff für SMTP

SMTP-Zugriff auf SX-GATE aus Schnittstelle ...

Für den Empfang von eingehenden E-Mails via SMTP ist es in der Regel erforderlich, den entsprechenden Zugriff im Firewall freizuschalten. Sofern der SMTP-Zugriff ohnehin freigegeben ist, wird eine entsprechende Meldung angezeigt. Andernfalls können Sie eine passende Regel definieren. Ist dabei in der Liste keine Regel konfiguriert, so ist der SMTP-Zugriff gesperrt.



Mit diesem Assistenten werden lediglich die Firewall-Einstellungen der aktuellen Internet-Schnittstelle geprüft. Je nach Firewall-Einstellung der anderen Schnittstellen kann es erforderlich sein, auch dort den SMTP-Port freizugeben.

Sie können hier Firewall-Regeln definieren, die den SMTP-Port für bestimmte oder für alle Internet-IP-Adressen freigeben.

Ist im DNS als Mail-Exchanger für Ihre Domain die Internet-Adresse des SX-GATE eingetragen, so werden E-Mails direkt vom Mail-Server des Absenders an SX-GATE geschickt. Wählen Sie daher bitte als "Internet-Quell-IP" den Wert "*" (beliebig) und fügen Sie die Firewall-Regel hinzu. Der SMTP-Zugriff ist so beliebigen Quell-Adressen gestattet. Wenn Sie sich nicht sicher sind, was im DNS eingestellt ist, so können Sie dies über eine entsprechende DNS-Anfrage prüfen. Fragen Sie im Zweifelsfall Ihren Provider.

Werden E-Mails ausschließlich mit Hilfe des ETRN-Protokolls abgerufen, so kommen die SMTP-Verbindungen stets von der Adresse des ETRN-Servers. Auch wenn eingehende E-Mails grundsätzlich zunächst an den Mail-Server des Providers gesendet werden und dieser die Mails mit SMTP an SX-GATE weiterleitet, ist die Quell-Adresse der SMTP-Verbindungen immer die selbe - nämlich die des Provider Mail-Servers. Beim Hinzufügen der Firewall-Regel sollten Sie daher als "Internet-Quell-IP" die entsprechende IP-Adresse angeben und die zugehörige Option auswählen. So ist gewährleistet, dass SMTP-Verbindungen nur von Servern aus aufgebaut werden können, von denen es notwendig ist.

Konfiguration übernehmen

Die Konfiguration des SX-GATE wurde bis jetzt noch nicht verändert. Drücken Sie auf "Fertigstellen" um Änderungen in das System zu übernehmen oder "Abbrechen" um keine Änderungen vorzunehmen.

Server

SX-GATE kann E-Mails von mehreren POP3-, IMAP4- oder ETRN-Servern abrufen.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

E-Mail abholen von POP/ETRN-Server

Geben Sie hier den Namen oder die IP-Adresse des neuen POP- oder ETRN-Servers an. Sie können diese Daten bei Ihrem Provider erfragen.

Servertyp

Protokoll für den Zugriff auf diesen Server

Legen Sie hier bitte das Protokoll für den Zugriff auf diesen Server fest. Sie erfahren die notwendige Einstellung bei Ihrem Provider.

Häufig kommt das POP3-Protokoll zum Einsatz. Dabei liegen die E-Mails in einzelnen Konten beim Provider, auf die mit Benutzername und zugehörigem Kennwort zugegriffen wird. Sie können die E-Mail aus so einem Konto lokal an einen bestimmten

Benutzer oder eine bestimmte Gruppe zustellen (single-drop) oder aber den Inhalt eines solchen Kontos anhand der Adresse des Empfängers verteilen lassen (multi-drop).

Das APOP-Verfahren entspricht POP3, lediglich die Anmeldung erfolgt auf andere Weise.

IMAP kann alternativ zu POP3 genutzt werden, wenn es bei POP3 Probleme mit zu kurzen Timeouts gibt.

Um Mails von "Microsoft 365"-Postfächern per POP3 oder IMAP abzuholen, ist eine spezielle Authentifizierung erforderlich. Wählen Sie in diesem Fall den jeweiligen OAUTH2-Eintrag.

ETRN ist ein Befehl des ESMTP-Protokolls. ETRN kommt unter Umständen zum Einsatz, wenn SX-GATE über eine Wählleitung mit fester IP-Adresse an das Internet angebunden ist. Dabei versucht der Mail-Server des Providers eingehende E-Mails direkt mit SMTP an SX-GATE zuzustellen. Ist dieser jedoch gerade nicht erreichbar, weil z.B. die Wählleitung nicht online ist, werden alle eingehenden E-Mails auf dem Mail-Server des Providers in einer Warteschlange zwischengespeichert. Geht die Wählleitung online, so kann SX-GATE dies dem Mail-Server des Providers mit Hilfe des ETRN-Befehls anzeigen. Der Befehl veranlasst, dass nun erneut versucht wird, die wartenden E-Mails zuzustellen.

Protokoll für den Zugriff auf diesen Server

- POP3
Lesen Sie bitte weiter bei [Einzelkonten](#) (S. 269)
- Microsoft 365 POP3 (OAUTH2)
Lesen Sie bitte weiter bei [OAuth2](#) (S. 266)
- APOP
Lesen Sie bitte weiter bei [Einzelkonten](#) (S. 269)
- IMAP
Lesen Sie bitte weiter bei [Einzelkonten](#) (S. 269)
- Microsoft 365 IMAP (OAUTH2)
Lesen Sie bitte weiter bei [OAuth2](#) (S. 266)
- ETRN (ESMTP)
Lesen Sie bitte weiter bei [ETRN-Domains](#) (S. 271)

OAuth2

Um Mails von einem "Microsoft 365"-Konto abholen zu können, ist eine Authentifizierung mit dem OAuth2-Verfahren notwendig. Der SX-GATE nutzt dabei den "Client-Credentials Flow". Vergleichbar mit einem Benutzerkonto wird dazu in "Entra ID" (ehemals Azure Active-Directory) für den SX-GATE Mail-Client eine Anwendung mit zugehörigem Anwendungskennwort angelegt. Die Anwendung erhält die Berechtigung für den POP3- bzw. IMAP4-Zugriff. Abschließend muss der Anwendung mit Hilfe der Exchange-Verwaltungsshell Zugriff auf die gewünschten

Postfächer gewährt werden. Nun kann der SX-GATE mit seiner Anwendungs-ID und dem Anwendungskennwort einen kurzlebigen Zugriffstoken abrufen und mit diesem die Mails aus allen entsprechend konfigurierten Postfächern abrufen.

Die Schritte im Einzelnen:

Anwendung anlegen

Melden Sie sich bei Microsoft Azure mit einem Administratorenkonto an (<https://portal.azure.com>).

Wählen Sie "Microsoft Entra ID", dann "Verwalten > App-Registrierungen".

Klicken Sie auf "Neue Registrierung" und vergeben Sie einen beliebigen Namen. Lassen Sie die weiteren Einstellungen unverändert und legen Sie die Anwendung mit "Registrieren" an.

Jetzt links im Menü "Zertifikate & Geheimnisse" anklicken. Unter "Geheime Clientschlüssel" generieren Sie mit "Neuer geheimer Clientschlüssel" ein Anwendungskennwort, das Sie mit "Hinzufügen" abspeichern.

Kopieren Sie nun sofort das Kennwort in der Spalte "Wert" durch Klick auf das Kopiersymbol hinter dem Kennwort. Zu einem späteren Zeitpunkt ist dies nicht mehr möglich. Übertragen Sie das Kennwort in die OAuth2-Konfiguration des SX-GATE Mail-Clients bzw. speichern Sie es an einem sicheren Ort zwischen, um es später im SX-GATE zu konfigurieren.

Klicken Sie nun im Menü links auf "Verwalten > API-Berechtigungen", dann "Berechtigung hinzufügen". Wählen Sie "Von meiner Organisation verwendete APIs" und geben Sie im Suchfeld "Office" ein. Wählen Sie "Office 365 Exchange Online" aus. Klicken Sie auf "Anwendungsberechtigungen". Öffnen Sie die Rubriken "IMAP" und/oder "POP" und selektieren Sie die jeweilige "AccessAsApp"-Berechtigung. Schließen Sie das Fenster mit "Berechtigungen hinzufügen". Klicken Sie abschließend auf "Administratorzustimmung für DOMAINNAME erteilen".

Klicken Sie im linken Menü auf "Übersicht" und übertragen Sie die "Anwendungs-ID (Client)" und die "Verzeichnis-ID (Mandant)" in die OAuth2-Konfiguration des SX-GATE Mail-Clients bzw. speichern Sie die Werte zwischen, um sie später im SX-GATE zu konfigurieren.

Verlassen Sie nun die Anwendungs-Registrierung, indem Sie oben links auf "Home" klicken.

Öffnen Sie erneut "Microsoft Entra ID" und wählen Sie diesmal "Verwalten > Unternehmensanwendungen". Kopieren Sie sich für später die "Objekt-ID" der zuvor angelegten Anwendung. Hier wird auch nochmal die "Anwendungs-ID" angezeigt. Sie benötigen beide Werte gleich für die Exchange-Konfiguration.

Zugriffsrechte im Exchange erteilen

Prüfen Sie zunächst im "Microsoft 365 admin center" (<https://admin.microsoft.com>), ob für die gewünschten Benutzer der POP3- bzw. IMAP4-Zugriff erlaubt ist. Wählen Sie dazu unter "Benutzer > Aktive Benutzer" den jeweiligen Benutzer aus. Nach Klick auf "E-Mail" werden Ihnen unter "E-Mail Apps" die Berechtigungen angezeigt.

Verbinden Sie sich nun mit der Exchange Management-Shell. Öffnen Sie dazu die Powershell und installieren Sie falls notwendig das Modul zum ExchangeOnline-

Management ("Install-Module ExchangeOnlineManagement"). Ggf. muss das Modul noch importiert werden ("Import-Module ExchangeOnlineManagement").

Die Verbindung wird aufgebaut mit "Connect-ExchangeOnline -UserPrincipalName ADMINBENUTZER". Um die Verbindung über einen Proxy herzustellen, können Sie diesen zuvor mit z.B. "\$proxyoptions = New-PSSessionOption -ProxyAccessType ieconfig" in einer Variablen speichern. Ergänzen Sie dann den Connect-Befehl mit der Option "-PSSessionOption \$proxyoptions".

Registrieren Sie einmalig die Anwendung mit "New-ServicePrincipal -AppId ANWENDUNGS_ID -ServiceId OBJEKT_ID", wobei Sie ANWENDUNGS_ID und OBJEKT_ID mit den zuvor kopierten Werten ersetzen.

Ist die Anwendung bereits registriert, können Sie die Objekt-ID, hier "ServiceId" genannt, jederzeit mit "Get-ServicePrincipal" wieder abrufen.

Bei jedem Benutzerpostfach, das der SX-GATE abrufen soll, muss nun der Zugriff für diese ID freigeschaltet werden: "Add-MailboxPermission -Identity BENUTZER -User OBJEKT_ID -AccessRights FullAccess". Als BENUTZER geben Sie dessen E-Mail-Adresse an.

Zugangsdaten im SX-GATE hinterlegen

Sofern noch nicht geschehen, tragen Sie die zuvor kopierten Werte in die OAuth2-Konfiguration des SX-GATE Mail-Clients ein.

Bei der Konfiguration der einzelnen Benutzerpostfächer wird kein Passwort abgefragt, da sich SX-GATE mit seinem Anwendungskennwort bei allen Benutzerpostfächern anmelden kann.

Mandant (Tenant)

Tragen Sie hier den Namen oder die ID Ihres "Entra ID"-Mandanten ein.

OAuth2 Anwendungs-ID

Geben Sie hier die Anwendungs-ID (Client-ID) ein, die Sie in "Entra ID" für den SX-GATE Mail-Client registriert haben.

Geheimer OAuth2-Clientschlüssel

Geben Sie hier das Anwendungskennwort ein, das Sie im Azure Active-Directory für den SX-GATE Mail-Client generiert haben.



Das Anwendungskennwort ist im Azure AD mit einer begrenzten Gültigkeitsdauer versehen. Bitte denken Sie stets daran, rechtzeitig ein neues Anwendungskennwort im Azure AD festzulegen und in den SX-GATE zu übertragen.

Einzelkonten

Gespiegelte Postfächer (single-drop)

Mit Hilfe der Schaltflächen "Hinzufügen" und "Entfernen" können Sie dem POP-Server neue Postfächer hinzufügen bzw. eingetragene Postfächer löschen.



In dieser Liste werden lediglich Einzelkonten angezeigt. Die Bearbeitung von Sammelkonten erfolgt in den nachfolgenden Eingabemasken.

Um auf ein POP-Konto beim Provider zugreifen zu können, benötigen Sie den Kontonamen (Login) und das zugehörigen Passwort. Erfragen Sie diese Daten bei Ihrem Provider.

Bei jedem Konto ist zusätzlich der lokale Empfänger inklusive Domain anzugeben. Alle E-Mails aus dem POP-Postfach beim Provider werden mit SMTP an diese Adresse zugestellt. Daher auch der Name Einzelkonto (single-drop). Dabei muss die Zieladresse jedoch nicht zwangsläufig die Adresse eines einzelnen Benutzers sein. Es kann sich selbstverständlich auch um einen Mail-Verteiler (Gruppe) handeln.

Sammelpostfach konfigurieren

Sammelpostfach konfigurieren

Der Nachteil von Einzelkonten (single-drop) ist der doppelte Verwaltungsaufwand. Die Konten müssen sowohl beim Provider als auch lokal angelegt werden. Abhilfe kann hier ein Sammelkonto (multi-drop) schaffen.

Die meisten Provider unterstützen es, POP3-Sammelkonten einzurichten. In ein solches Konto fließen alle Mails, die an eine (oder sogar mehrere) Domains gerichtet sind, unabhängig vom Empfänger. Möglich sind auch Mischlösungen, wobei die E-Mails für bestimmte Benutzer in Einzelkonten abgelegt werden, während die E-Mails für alle anderen Empfänger in ein Sammelkonto laufen.

Es kann sinnvoll sein, ein Sammelkonto beim Provider bei der Abholung wie ein Einzelkonto zu behandeln. Alle Mails aus dem Sammelkonto werden dann lokal an ein bestimmtes Konto oder einen bestimmten Verteiler zugestellt. Typischerweise existieren in diesem Falle auf dem Mail-Server des Providers für jeden Mitarbeiter ein Einzelkonto und für alle unbekannte Adressen ein Sammelkonto, dessen Inhalt lokal an einen bestimmten Benutzer oder Verteiler (wie z.B. info) ausgeliefert wird.

Verarbeitet SX-GATE hingegen den Inhalt eines POP3-Postfaches als Sammelkonto, so wird beim Abholen versucht, aus dem Inhalt jeder Mail den ursprünglichen Empfänger zu rekonstruieren. Ist dies möglich, so wird die Mail lokal an diesen

Empfänger zugestellt. Um ein neues Mail-Konto oder einen neuen Verteiler anzulegen ist auf Seiten des Providers kein Eingriff notwendig - die Kontenverwaltung wird ausschließlich lokal vorgenommen.



Nicht immer lässt sich der eigentliche Empfänger bei einer Mail aus einem Sammelkonto rekonstruieren! Problematisch sind all die E-Mails, bei denen die Empfängerinformation ausschließlich im Umschlag der Mail (envelope) und nicht in der eigentlichen E-Mail übermittelt wird. Dies ist insbesondere der Fall bei:

- E-Mails die als blinde Kopie (Bcc) verschickt wurden.
- E-Mails die an mehrere Empfänger versendet wurden, wobei die Empfänger nicht einzeln sondern über einen Verteiler angegeben wurden (insbesondere bei Mailing-Listen).
- Bestimmte Provider-Mail-Server, die die benötigte Information nicht in den Mails hinterlegen.

Lässt sich der Empfänger einer Mail aus einem Sammelkonto nicht rekonstruieren, so wird diese Mail stets an den Administrator zugestellt.

Sollten sich in diesem Zusammenhang Probleme ergeben, so sollte man eine Mischlösung aus Einzel- und Sammelkonten wählen. Neu eingerichtet Adressen können dabei mit Hilfe des Sammelkontos sofort in Betrieb genommen werden. Ergeben sich wiederholte Fehlzustellungen, so wird das Konto beim Provider als Einzelkonto angelegt.

Sammelpostfach konfigurieren

- ja
Lesen Sie bitte weiter bei **Sammelkonten** (S. 270)
- nein
Lesen Sie bitte weiter bei **Konfiguration übernehmen** (S. 265)

Sammelkonten

Sammelpostfächer (multi-drop)

Mit Hilfe der Schaltflächen "Hinzufügen" und "Entfernen" können Sie dem POP-Server neue Postfächer hinzufügen bzw. eingetragene Postfächer löschen. In dieser Liste werden lediglich Sammelkonten angezeigt.

Um auf ein POP-Konto beim Provider zugreifen zu können, benötigen Sie den Kontonamen (Login) und das zugehörigen Passwort. Erfragen Sie diese Daten bei Ihrem Provider.

Bei jedem Konto ist zusätzlich die lokale Domain anzugeben. Beim Abholen von E-Mails aus den hier angegebenen Konten wird versucht, aus dem Inhalt der E-Mail den ursprünglichen Empfänger zu ermitteln. Die E-Mail wird dann an diesen Empfänger zugestellt. War der Empfänger nicht zu ermitteln, so wird die E-Mail an den Administrator zugestellt.

Es ist zwar möglich, von einem POP-Server mehrere Konten als Sammelkonto abzuholen, im Normalfall ist dies jedoch nicht sinnvoll, da nur ein einziges Konto tatsächlich ein Sammelkonto ist.

Sammelkonto-Domains

Zur Ermittlung des Empfängers nach folgenden Domains suchen

Um den Empfänger einer E-Mail rekonstruieren zu können, muss SX-GATE wissen, nach welchen Adressen gesucht werden soll. In bestimmten Kopfzeilen (Header) der E-Mail wird nach E-Mail-Adressen gesucht, die mit den hier angegebenen Domains enden. Wird ein passender Eintrag gefunden, so ersetzt SX-GATE den Domain-Teil der E-Mail-Adresse durch die beim Postfach angegebene Ziel-Domain und stellt die Mail zu. Wird hingegen keine passende Adresse ermittelt, so erhält der Administrator die E-Mail.



Wird nirgends hinterlegt nach welcher Domain zu suchen ist, gehen alle E-Mails aus dem Sammelkonto an den Administrator.

Lesen Sie bitte weiter bei [Konfiguration übernehmen](#)

ETRN-Domains

ETRN aufrufen für folgende Domains

Geben Sie hier die Domains an, die mit Hilfe des ETRN-Befehls vom Mail-Server des Providers abgerufen werden sollen. Der Mail-Server des Providers wird dann versuchen, wartende E-Mails für diese Domains per SMTP zuzustellen.

Lesen Sie bitte weiter bei [Firewall-Zugriff für SMTP](#)

Sendewarteschlange

Erneuter Sendeversuch von Mails in der Warteschlange

Ist der Mail-Server an den der SX-GATE eine E-Mail zustellen soll vorübergehend nicht erreichbar oder tritt während des Sendevorgangs ein Fehler auf, so wird die E-Mail in den Wartezustand versetzt. Wählen Sie hier bitte aus, nach welcher Zeitspanne erneut versucht werden soll, die Mail zuzustellen.



Bei schmalbandigen Internet-Anbindungen sollten Sie hier kein zu kurzes Intervall einstellen, um die Bandbreite nicht durch die wiederholte Übertragung immer wieder fehlschlagender E-Mails zu belegen. Ein langes Intervall empfiehlt sich auch, wenn die Kosten für die Internet-Anbindung nach angefallener Datenmenge berechnet werden.

Abholzeiten

Zeitplan für Mail-Abruf von POP/ETRN-Servern

Konfigurieren Sie hier zu welchen Zeiten E-Mails von POP- oder ETRN-Servern abgerufen werden sollen. Sofern Sie die Mail-Abholung bereits mit dem Aufbau der Wählverbindung gekoppelt haben, brauchen Sie hier nicht unbedingt zusätzliche Zeiten definieren.



Ist kein POP- oder ETRN-Server konfiguriert bzw. sind dort keine Konten oder Domains eingetragen, so erfolgt zu den angegebenen Zeiten auch keine Aktion.

13.5 IPsec-VPN

IPsec-VPN konfigurieren

Welche Aufgabe wollen Sie konfigurieren?

Anbindung von L2TP-IPsec-Clients

Mit Hilfe dieses Assistenten können Sie SX-GATEs VPN-Server für Verbindungen mit L2TP-IPsec-Clients vorbereiten. Die Konfiguration dazu wird in den Schnittstellen "l2tp0" und "ipsec0" vorgenommen. Die zugehörige Verbindung erhält den Namen "L2TP".

Anbindung an zentralen SX-GATE

Falls es sich bei diesem Gerät um einen SX-GATE in einer Außenstelle handelt, können Sie hier das vom zentralen SX-GATE ausgestellte IPsec-Installationspaket einspielen. Die Konfiguration erfolgt in Schnittstelle "ipsec0".

Welche Aufgabe wollen Sie konfigurieren?

- Anbindung von L2TP-IPsec-Clients
Lesen Sie bitte weiter bei [L2TP-IPsec-VPN konfigurieren](#) (S. 273)
- Anbindung an zentralen SX-GATE
Lesen Sie bitte weiter bei [Datei auswählen](#) (S. 278)

L2TP-IPsec-VPN konfigurieren

Allgemeine Informationen zu L2TP-IPsec

Das Protokoll L2TP (Layer Two Tunneling Protocol) dient der Anbindung eines entfernten Arbeitsplatzes an ein bestimmtes Netzwerk - typischerweise dem LAN. Obwohl sich der L2TP-Client physikalisch nicht im LAN befindet, wird ihm eine frei IP-Adresse aus dem LAN zugewiesen. Im Netzwerk wird dann den anderen Geräten im LAN vorgetäuscht, der L2TP-Client sei direkt an das LAN angeschlossen. Die Konfiguration der Geräte im LAN muss so nicht geändert werden (Routing).

SX-GATE stellt einen L2TP-Server zur Verfügung, der die eingehenden L2TP-Verbindungen mit Benutzername und Kennwort authentifiziert. Neben der Authentifizierung sorgt der L2TP-Server für die Zuweisung der IP-Adresse an den L2TP-Client und für die transparente Einbindung des L2TP-Clients in das LAN. In der laufenden Verbindung extrahiert der L2TP-Server die Nutzdaten aus dem L2TP-Kanal bzw. bettet Datenpakete aus dem LAN in L2TP-Pakete ein.

Um die Vertraulichkeit der Daten zu gewährleisten, wird die L2TP-Verbindung durch einen IPsec-VPN-Tunnel geschützt. Dieser VPN-Tunnel besteht zwischen SX-GATE und dem L2TP-IPsec-Client. Neben der Möglichkeit zur stärkeren Authentifizierung

durch Zertifikate, verschlüsselt das VPN jedes L2TP-Paket und stellt während der Datenübertragung die Authentizität der Pakete sicher.

Kommuniziert ein L2TP-Clients mit einem Gerät im LAN, so werden die Nutzdaten als auf der Strecke zwischen dem L2TP-Client und SX-GATE zunächst in L2TP- und dann in IPsec-Pakete eingepackt. Router die sich zwischen dem L2TP-Client und SX-GATE befinden "sehen" lediglich das IPsec-VPN.

Hinweise zu diesem Assistenten

VPN-Verbindungen bieten eine Vielzahl unterschiedlicher Konfigurationsmöglichkeiten, die nicht alle durch diesen Assistenten abgedeckt werden können. Der Assistent richtet daher eine typische L2TP-IPsec-Verbindung ein. In Einzelfällen kann es vorkommen, dass darüber hinaus in anderen Menüpunkten der SX-GATE-Konfigurationsoberfläche Anpassungen erforderlich werden.



Beachten Sie unbedingt die Hinweise auf den einzelnen Bildschirmmasken. Sie finden dort unter Umständen wichtige Informationen zu Konfigurations-Schritten die außerhalb dieses Assistenten vorgenommen werden müssen.

Dieser Assistent richtet grundsätzlich die VPN-Verbindung "L2TP" in der Schnittstelle "ipsec0" ein. Falls erforderlich werden diese neu angelegt. Wird die Schnittstelle "ipsec0" neu angelegt, so nutzt diese die aktuelle Internet-Schnittstelle (Default-Route) als Basis.

Zur Authentifizierung bevorzugt der Assistent Zertifikate von einer vertrauenswürdigen Zertifizierungsstelle (CA). Falls zuvor noch keine Festlegung erfolgte, wird die in SX-GATE eingebaute CA verwendet. Bei Bedarf wird die SX-GATE-CA und der Schlüssel für SX-GATES VPN-Server zuvor initialisiert.

Lesen Sie bitte weiter bei [Neues VPN-Server Zertifikat ausstellen](#)

Lesen Sie bitte weiter bei [Vertrauenswürdige VPN CA](#)

Lesen Sie bitte weiter bei [L2TP IP-Adressen](#)

Neues VPN-Server Zertifikat ausstellen

In dieser Maske geben Sie die Zertifikatsdaten für das Zertifikat ein.

CN

Sofern SX-GATE im Internet über eine feste IP-Adresse oder einen bestimmten DNS-Namen verfügt, sollten Sie diesen hier angeben. Wählen Sie sonst einen anderen möglichst eindeutigen Bezeichner für Ihren SX-GATE.

Alternative Bezeichner

Bei der Überprüfung, ob das Server-Zertifikat auch tatsächlich zum angesprochenen Server gehört, werten viele Clients bevorzugt dieses Feld aus. Sie können hier alle Namen oder auch IP-Adressen eintragen, unter denen der IPsec-Server aus dem Internet angesprochen wird.



Die Angabe ist zwingend erforderlich, wenn MacOS VPN-Clients angebunden werden sollen. MacOS-Clients erwarten, dass im alternativen Bezeichner des Server-Zertifikats die im MacOS-Client konfigurierte Server-Adresse enthalten ist.

Zertifizierungsanfrage

Die Zertifizierungsanfrage wird mit dem Aufruf dieser Seite erstellt und kann im nächsten Schritt mit Hilfe des CA-Zertifikats signiert werden.

Verwendungszweck: Server Authentifizierung

Die Aktivierung dieses Schalters wird empfohlen. In der Grundkonfiguration prüft der Windows-IPsec-Client, ob das VPN-Server-Zertifikat diesen Wert als "Extended Key Usage" enthält.



Abhängig vom Client und dessen Konfiguration kann es passieren, dass der Client die Verbindung verweigert, wenn dieses Attribut im Server-Zertifikat fehlt.

Zertifikat signieren

Mit dem Aufruf dieser Seite wird das Zertifikat signiert. Beenden Sie den Vorgang mit "Fertigstellen" um den neuen VPN-Server Schlüssel zu installieren.

Vertrauenswürdige VPN CA

Zur Authentifizierung einer IPsec-VPN-Verbindung prüft SX-GATE, ob das von der Gegenstelle übermittelte Zertifikat von der als vertrauenswürdig eingestuften Zertifizierungsstelle (CA) ausgestellt wurde. Die aktuell als vertrauenswürdig eingestufte CA ist nicht identisch mit SX-GATEs eigener CA. Sofern Sie eine externe CA zur Erstellung von Zertifikaten nutzen ist dies selbstverständlich in Ordnung. Andernfalls haben Sie hier die Möglichkeit, die SX-GATE-CA als neue vertraute CA festzulegen.



Wenn Sie die vertrauenswürdige CA ändern funktionieren möglicherweise andere VPN-Verbindungen nicht mehr.

Grundsätzlich ist es zwar denkbar, mehr als eine CA als vertrauenswürdige einzustufen, aus Gründen der Übersichtlichkeit bietet SX-GATE jedoch nur die Möglichkeit eine CA zu hinterlegen. Sofern die Zertifikate Ihrer Kommunikationspartner von verschiedenen Zertifizierungsstellen ausgestellt werden, müssen Sie sich für eine davon entscheiden. Für alle anderen Verbindungen müssen Sie auf den Authentifizierungsmodus mit direkter Angabe des öffentlichen Schlüssels der Gegenstelle zurückgreifen. Die entsprechende Konfiguration kann jedoch nicht in diesem Assistenten vorgenommen werden. Wechseln Sie dazu in das Menü "Module. Auch das Festlegen einer externen CA als vertrauenswürdige kann nur dort vorgenommen werden.



Die Authentifizierung über vertrauenswürdige CA funktioniert nur, wenn auch das Zertifikat des SX-GATE VPN-Servers von dieser CA ausgestellt wurde.

Lesen Sie bitte weiter bei [L2TP IP-Adressen](#)

L2TP IP-Adressen

An L2TP-Clients zuzuweisende IP-Adressen

Geben Sie hier die IP-Adressen an, die den L2TP-Clients zugewiesen werden sollen. Die Adressen dürfen nicht bereits anderweitig in Benutzung sein. Verwenden Sie nach Möglichkeit IP-Adressen aus dem Netzwerk, mit dem sich der L2TP-Client verbinden will. Dieses Netzwerk muss direkt an SX-GATE angeschlossen sein.



Die Anzahl der hier eingetragenen IP-Adressen bestimmt die maximale Anzahl gleichzeitiger L2TP-Verbindungen.

Sie können einzelne IPs oder ganze Blöcke von Adressen hinzufügen. Die Angabe eines Adress-Blocks erfolgt mit Hilfe einer Netzwerk-Adresse und der dazu passenden Netzmaske. Angenommen im LAN wird das Netzwerk 192.168.0.0/24 verwendet: Mit dem Eintrag 192.168.0.160/27 fügen Sie einen Block von insgesamt 32 Adressen aus dem Bereich 192.168.0.160 bis 192.168.0.191 hinzu.



Die Adress-Blöcke dürfen keine Netzwerk- oder Broadcast-Adressen der lokalen Ethernet-Netzwerke enthalten. Ausgenommen sind Netzwerk- und Broadcast-Adresse eines Class-C-Netzes (*.0 bzw. *.255). Diese werden automatisch aus dem Adress-Block ausgenommen.



Die Eingabe einer falschen Netzmaske kann fatale Folgen haben. So würde im obigen Beispiel der Eintrag 192.168.0.160/255.255.255.0 (Netzmaske 255.255.255.0 anstelle von 255.255.255.224) alle 254 Adressen aus dem Bereich 192.168.0.1 bis 192.168.0.254 freischalten, also der selbe Bereich der auch im LAN verwendet wird.

DNS

Als DNS-Server zuweisen

Mit dieser Einstellung können Sie festlegen, welchen Namens-Server der Client verwenden soll.

Benutzer

Benutzer mit RAS-Zugang

Der L2TP-Server authentifiziert die jeweiligen Benutzer mit Benutzernamen und Passwort. Dies ist ausschließlich Mitgliedern der SX-GATE-Gruppe "system-ras" möglich. In dieser Übersicht sehen Sie, welche Benutzer aktuell über die entsprechende Berechtigung verfügen und welche nicht. Um mehrere Benutzer gleichzeitig in die Gruppe aufzunehmen bzw. aus der Gruppe zu entfernen, können Sie in der jeweiligen Liste mehrere Einträge gleichzeitig auswählen. Halten Sie dazu während der Auswahl die STRG-Taste gedrückt.



Um neue Benutzer anzulegen wechseln Sie bitte nach Beendigung dieses Assistenten in die Benutzerverwaltung. Legen Sie dort die benötigten Benutzer an und nehmen Sie diese in die Gruppe "system-ras" auf.

Konfiguration übernehmen

Die Konfiguration des SX-GATE wurde bis jetzt noch nicht verändert. Drücken Sie auf "Fertigstellen" um Änderungen in das System zu übernehmen oder "Abbrechen" um keine Änderungen vorzunehmen.

Datei auswählen

Wählen Sie hier bitte das Installationspaket aus. Neben einer Datei mit den Konfigurationsparametern enthält das Paket auch eine passwortgeschützte PKCS#12-Datei mit einem RSA-Schlüsselpaar. Um die PKCS#12-Datei öffnen zu können, müssen Sie das zugehörige Kennwort eingeben.

Zertifikat prüfen

Prüfen Sie hier noch einmal das Zertifikat, bevor es installiert wird.

Lesen Sie bitte weiter bei [VPN-Server Zertifikat importiert](#)

CA-Zertifikat auswählen

Das Zertifikat muss ergänzt werden um die Zertifikate eventueller Zwischen-Zertifizierungsstellen (Intermediate CAs) bis zum Wurzel-Zertifikat (Root CA). Alle Zertifikate müssen im PEM- oder im DER-Format vorliegen. Sie erhalten die Zertifikate von Ihrer Zertifizierungsstelle.

CA-Zertifikat prüfen

Das hochgeladene Zertifikat wird an die Zertifizierungs-Kette angehängt.

Lesen Sie bitte weiter bei [CA-Zertifikat auswählen](#)

VPN-Server Zertifikat importiert

Das Schlüsselpaar wurde importiert.

CA Zertifikat prüfen

Die vom SX-GATE VPN-Server als vertrauenswürdig eingestufte CA sollte im Normalfall identisch sein mit der CA, die das Zertifikat des VPN-Servers ausgestellt hat. Sofern das CA-Zertifikat Bestandteil der hochgeladenen PKCS#12-Datei ist, kann die vertrauenswürdige CA gleich mit importiert werden.



Wenn Sie die vertrauenswürdige CA ändern, lassen sich Verbindungen, die über die alte CA authentifiziert werden müssen, nicht mehr herstellen.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden.

VPN-Verbindung prüfen

Speziell für die Konfiguration eines SX-GATEs in einer Außenstelle bietet sich das Hochladen eines Installationspakets an. Mit dem Bestätigen dieser Maske wird eine passende IPsec-Verbindung über die Schnittstelle ipsec0 angelegt. Die im Installationspaket enthaltene Internet-Adresse der Gegenstelle dient als Verbindungsname. Falls erforderlich, wird die Schnittstelle ipsec0 angelegt, der IPsec-Dienst gestartet und weitere notwendige Einstellungen vorgenommen.



Sofern bereits eine IPsec-Verbindung mit dem selben Namen existiert, wird diese überschrieben.

13.6 Fernwartung

Zugriffsmethode auswählen

Wie kann der technische Support auf SX-GATE zugreifen?

Dem technischen Support kann auf folgende Weise der Zugriff ermöglicht werden:

Über das Internet (ausgehend)

Auch bei dieser Variante wird es dem technischen Support ermöglicht, mit Secure Shell über das Internet auf Ihren SX-GATE zuzugreifen. Hier erstellt jedoch Ihr SX-GATE eine ausgehende Verbindung über die sich der technische Support rückwärts zu Ihrem Gerät verbinden kann (Reverse-Tunnel). Dies ist nur solange möglich, wie die ausgehende Verbindung besteht. Nützlich ist diese Variante insbesondere, wenn aufgrund eines vorgelagerten NAT-Routers oder einer Firewall keine eingehenden Verbindungen möglich sind.

Über das Internet (eingehend)

Wählen Sie diese Option um eine Firewall-Regel zu definieren, die es dem technischen Support erlaubt über das Internet mit Secure-Shell auf SX-GATE zuzugreifen. Über den Assistenten können Sie eine bereits konfigurierte Regel auch deaktivieren oder wieder löschen.

Wie kann der technische Support auf SX-GATE zugreifen?

- Über das Internet (ausgehend)
Lesen Sie bitte weiter bei **Verbindung aufbauen** (S. 281)
- Über das Internet (eingehend)
Lesen Sie bitte weiter bei **Firewall-Zugriff für Secure-Shell** (S. 280)

Firewall-Zugriff für Secure-Shell

SSH-Zugriff auf SX-GATE aus Schnittstelle ...

Der technische Support nutzt Secure-Shell-Verbindungen für den Zugriff auf SX-GATE. Der zugehörige TCP-Port 22 (ssh) ist dazu freizugeben. Besteht ohnehin Vollzugriff auf SX-GATE, so wird dies über eine entsprechende Meldung angezeigt. Andernfalls können Sie hier passende Regeln definieren oder auch entfernen. Ist in der Liste keine Regel eingetragen, so ist der SSH-Zugriff gesperrt.



Sofern sich eine oder mehrere übergeordnete Firewalls vor dem SX-GATE befinden, müssen auch diese eingehende Secure-Shell-Verbindungen zulassen.

Die für den Zugriff erforderlichen Einstellungen bezüglich IP-Adresse und Port-Bereich erfragen Sie bitte beim technischen Support.

Konfiguration übernehmen

Die Konfiguration des SX-GATE wurde bis jetzt noch nicht verändert. Drücken Sie auf "Fertigstellen" um Änderungen in das System zu übernehmen oder "Abbrechen" um keine Änderungen vorzunehmen.

Verbindung aufbauen

Bitte wählen Sie

Vom technischen Support erfahren Sie, mit welchem Server sich Ihr SX-GATE verbinden muss. Ist die Verbindung erstellt, kann sich der technische Support rückwärts über diese Verbindung am SX-GATE einloggen. Wenn Sie die Verbindung trennen, werden alle bestehenden Support-Verbindungen abgebrochen. Der technische Support kann dann auch keine neue Verbindung mehr herstellen.

14 Module

Das Hauptmenü "Module" dient der Detailkonfiguration der einzelnen Module des SX-GATE. In diesem Bereich werden fundierte Fachkenntnisse vorausgesetzt. Die modulübergreifende Grundkonfiguration sollte soweit als möglich mit Hilfe der Assistenten aus dem Hauptmenü "Assistenten" vorgenommen werden.

14.1 Netzwerk

14.1.1 Einstellungen

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.1-A Allgemein.....	282
14.1.1-B IPSec Parameter.....	284
14.1.1-C VPN Zertifikat.....	285
14.1.1-D Vertrauenswürdige VPN CA.....	286

14.1.1-A Allgemein

IPv6

Diese Einstellung aktiviert oder deaktiviert die IPv6-Unterstützung des SX-GATES.

Router-Modus

Wählen Sie diese Option, wenn sich SX-GATE im Netzwerk als IPv6-Router zu erkennen geben soll.

Host-Modus

Diese Einstellung ist sinnvoll, wenn SX-GATE beispielsweise als reiner Proxy oder Mail-Relay-Server in einer DMZ befindet.

Standard Gateway über Schnittstelle

Geben Sie hier die Schnittstelle an, über die die Anbindung an das Internet erfolgt. Alle IP-Pakete mit Zieladressen, für die keine andere Routing-Information vorhanden ist, werden über die hier ausgewählte Schnittstelle versendet.



Sie können diese Einstellung auch verwenden, um schnell zwischen zwei Internet-Anbindungen zu wechseln (z.B. Standleitung über eth1, ADSL-Wählleitung über adsl0). Bitte beachten Sie jedoch, dass beim Wechsel der Anbindung ggf. auch andere Werte wie verwendete Namens-Server, Proxy des Providers oder Mail-Relay des Providers an den entsprechenden Stellen zu ändern sind.

Cluster mit geteiltem Internet-Zugang

Aktivieren Sie diesen Schalter, wenn Master und Backup den Internet-Zugang nur wechselseitig nutzen können, also z.B. nur eine ADSL-Leitung oder - bei Anbindung über einen vorgeschalteten Router - nur eine Internet-IP zur Verfügung steht. Das Backup-System geht dann über den Master ins Internet, solange es im Backup-Status ist. Bei einem Failover wird die Internet-Verbindung vom Backup-Knoten übernommen.



Der Master-Knoten muss in diesem Fall dem Backup uneingeschränkten Zugriff auf das Internet erlauben. Fügen Sie dazu auf dem Backup-Knoten in der Firewall-Konfiguration der Internet-Schnittstelle eine entsprechende Weiterleitungs-Regel hinzu. Wählen Sie als Protokoll "*". Als Quell-IP tragen Sie bitte die Backup-IP gemäß Cluster-Konfiguration ein. Synchronisieren Sie schließlich die Regel auf den Master-Knoten.

Fallback bei Störung

Ist diese Option aktiviert, so wechselt das System automatisch auf die eingestellte Schnittstelle, wenn die Internet-Verbindung gestört ist. Bei ADSL-Verbindungen wird dazu geprüft, ob eine aktive PPP-Verbindung besteht. Bei anderen Schnittstellenarten wird per "ping" geprüft, ob eine zu definierende Liste an Adressen erreichbar ist. Je nach Art des Problems kann es einige Minuten dauern, bis der Wechsel durchgeführt wird.

Während des Fallbacks wird im Hintergrund geprüft, ob die Störung beseitigt ist. Bei Erfolg wird nach wenigen Minuten auf die ursprüngliche Schnittstelle zurück geschaltet.



Durch Neustart des ADSL- bzw. des Netzwerk-Dienstes erfolgt sofort ein Wechsel zurück auf die ursprüngliche Internet-Verbindung.

Bei Fallback auf eine ADSL-Schnittstelle, muss der zugehörige Dienst gestartet und die Schnittstelle funktionsbereit konfiguriert sein.

Die Einstellungen für DNS, Mail-Relay und Proxy-Server des Providers werden durch das Fallback nicht verändert. Insbesondere wenn die ADSL- und die Fallback-Verbindung über verschiedene Provider erstellt werden, ist daher darauf zu achten, dass diese Dienste über beide Internetzugänge genutzt werden können.

Fallback Mailbenachrichtigung

Benachrichtigungen über einen Fallback werden an diese E-Mail-Adresse verschickt.

Verbindungstest mit ping an

Per ping an die hier angegebenen Adressen wird geprüft, ob die Internet-Verbindung besteht. Es können auch IP-Objekte ausgewählt werden, aus denen jedoch nur IP-Adressen genutzt werden. Eventuell enthaltene Netzwerke werden ignoriert.



Verwenden Sie bitte keine auf DNS basierenden IP-Objekte mit sich häufig ändernden IP-Adressen. Jede Adressänderung führt zu einem Neustart der Netzwerkverbindungen.

14.1.1-B IPsec Parameter

MTU für ipsec-Schnittstellen

Wenn IP Pakete durch den IPsec-Header erweitert werden, wird häufig die maximale Paketgröße überschritten, die für den Verbindungsweg zum entfernten IPsec-Server gilt. Die Pakete müssen daher fragmentiert werden. Dies kann mit bestimmten Internet-Routern zu Problemen führen, insbesondere wenn diese so konfiguriert sind, dass fragmentierte Pakete einfach verworfen werden.

Bemerkbar macht sich dies z.B. dadurch, dass Datenpakete mit einem Volumen von mehr als 1500 Byte nicht übertragen werden, während die Kommunikation mit Paketen von weniger als z.B. 1200 Byte problemlos funktioniert. Auch der Verbindungsaufbau als solches kann betroffen sein. Typischerweise kommt keine IPsec-Verbindung zustande, im IPsec-Log häufen sich jedoch Meldungen über doppelt übertragene Pakete.

Verkleinern Sie im Problemfall die MTU (Maximum Transmit Unit). Mit Hilfe dieses Parameters können Sie die maximale Größe der Datenpakete festlegen, die anschließend verschlüsselt werden. Wählen Sie einen Wert der klein genug ist, so dass die verschlüsselten Pakete auf dem Übertragungsweg nicht mehr fragmentiert werden müssen. Je kleiner die MTU gewählt wird, desto geringer wird jedoch der mögliche Durchsatz.

Mehrdeutige IDs

Ist diese Option nicht aktiviert, trennt ein neuer Verbindungsaufbau eine bereits bestehende Verbindung mit der selben ID. Dies ist insbesondere bei Clients

mit Wählverbindung und dynamischer IP-Adresse wichtig, damit längst getrennte Verbindungen nicht unnötig Ressourcen belegen oder gar die Einwahl neuer Clients verhindern. Sie sollten diesen Schalter daher nur aktivieren, wenn es tatsächlich verschiedene Gegenstellen gibt, die sich mit der gleichen ID verbinden müssen.

14.1.1-C VPN Zertifikat

Für die Authentifizierung von VPN-Verbindungen über X.509-Zertifikate benötigt der VPN-Server des SX-GATE ein eigenes Schlüsselpaar mit Zertifikat.



Das Schlüsselpaar wird sowohl für IPsec also auch für OpenVPN basierende VPNs verwendet.

Um einen neuen SX-GATE für IPsec-Client-Verbindungen vorzubereiten oder um den VPN-Server eines Außenstellen-SX-GATES mittels Installationspaket vorzubereiten, wechseln Sie bitte in das Menü "Assistenten > IPsec-VPN".

Zertifikate werden ansonsten im Menü "System > Zertifikatsverwaltung" administriert. Im Untermenü "CA Zertifikate" können Sie die "SX-GATE-CA" initialisieren und dann unter "Zertifikate" selbst Zertifikate ausstellen. Im Untermenü "Schlüsselbund" lassen sich Schlüsselpaare importieren, die Sie von einer anderen Zertifizierungsstelle erhalten haben.

Wenn Sie den VPN-Server des SX-GATE nicht nutzen oder VPN-Verbindungen ausschließlich über preshared keys authentifizieren, ist dieser Bereich belanglos.

Schlüssel/Zertifikat auswählen

Wählen Sie hier einen der Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.

Öffentlichen Schlüssel exportieren

Falls die VPN-Gegenstelle zur Authentifizierung den öffentlichen Schlüssel des SX-GATE-VPN-Servers benötigt, kann dieser hier im PEM-Format exportiert werden.



Bitte versichern Sie sich, ob die Gegenstelle wirklich den öffentlichen Schlüssel des VPN-Servers benötigt. Möglicherweise wird stattdessen der öffentliche Schlüssel der CA benötigt, die das SX-GATE-Zertifikat ausgestellt hat.

14.1.1-D Vertrauenswürdige VPN CA

Bei zertifikatsbasierter Authentifizierung wird im Normalfall geprüft, ob das vom Gegenüber präsentierte Zertifikat von einer vertrauenswürdigen Stammzertifizierungsstelle (Root-CA) ausgestellt wurde. Welche CA die SX-GATE VPN-Server als vertrauenswertig ansehen, lässt sich hier festlegen. Sie können entweder die lokale CA des SX-GATE einstellen oder den öffentlichen Schlüssel einer CA importieren.

Grundsätzlich ist es zwar denkbar, mehr als eine CA als vertrauenswertig einzustufen, aus Gründen der Übersichtlichkeit bietet SX-GATE jedoch nur die Möglichkeit eine CA zu hinterlegen. Sofern die Zertifikate Ihrer Kommunikationspartner von verschiedenen Zertifizierungsstellen ausgestellt wurden, müssen Sie sich für eine entscheiden.



In der IPsec-Konfiguration besteht die Möglichkeit, den öffentlichen Schlüssel der Gegenstelle zu importieren. Damit kann eine Verbindung auch dann authentifiziert werden, wenn das Zertifikat von einer anderen CA stammt. Bei OpenVPN basierten Verbindungen besteht die Möglichkeit individuelle Zertifikate anderer CAs zu nutzen, wenn SX-GATE die Client-Rolle übernimmt.

Wenn Sie den VPN-Server des SX-GATE nicht nutzen oder VPN-Verbindungen ausschließlich über preshared keys oder mit Angabe eines bestimmten öffentlichen Schlüssels authentifizieren, ist dieser Bereich belanglos.

Das zweite CA-Zertifikat löschen

Sind nach einem Wechsel der CA alle Systeme auf die neue CA umgestellt, können Sie das alte CA-Zertifikat hier löschen.

Neue vertrauenswürdige CA festlegen

Legen Sie hier fest, welche CA vom VPN-Server des SX-GATE als vertrauenswertig eingestuft werden soll. Sie können den öffentlichen Schlüssel der lokalen SX-GATE-CA kopieren, den öffentlichen Schlüssel einer CA im PEM-Format importieren oder diesen aus einer PKCS#12-Datei extrahieren.

Lokales VPN-Server Zertifikat erstellen

Mit Hilfe dieser Funktion erstellen bzw. erneuern Sie das Zertifikat für SX-GATES eigenen VPN-Server. Das neue Zertifikat ist bis zu sechs Jahre gültig und wird von der SX-GATE-CA signiert.

Neues VPN-Server Zertifikat ausstellen

In dieser Maske geben Sie die Zertifikatsdaten für das Zertifikat ein.

CN

Sofern SX-GATE im Internet über eine feste IP-Adresse oder einen bestimmten DNS-Namen verfügt, sollten Sie diesen hier angeben. Wählen Sie sonst einen anderen möglichst eindeutigen Bezeichner für Ihren SX-GATE.

Alternative Bezeichner

Bei der Überprüfung, ob das Server-Zertifikat auch tatsächlich zum angesprochenen Server gehört, werten viele Clients bevorzugt dieses Feld aus. Sie können hier alle Namen oder auch IP-Adressen eintragen, unter denen der IPsec-Server aus dem Internet angesprochen wird.



Die Angabe ist zwingend erforderlich, wenn MacOS VPN-Clients angebunden werden sollen. MacOS-Clients erwarten, dass im alternativen Bezeichner des Server-Zertifikats die im MacOS-Client konfigurierte Server-Adresse enthalten ist.

Zertifizierungsanfrage

Die Zertifizierungsanfrage wird mit dem Aufruf dieser Seite erstellt und kann im nächsten Schritt mit Hilfe des CA-Zertifikats signiert werden.

Verwendungszweck: Server Authentifizierung

Die Aktivierung dieses Schalters wird empfohlen. In der Grundkonfiguration prüft der Windows-IPsec-Client, ob das VPN-Server-Zertifikat diesen Wert als "Extended Key Usage" enthält.



Abhängig vom Client und dessen Konfiguration kann es passieren, dass der Client die Verbindung verweigert, wenn dieses Attribut im Server-Zertifikat fehlt.

Zertifikat signieren

Mit dem Aufruf dieser Seite wird das Zertifikat signiert. Beenden Sie den Vorgang mit "Fertigstellen" um den neuen VPN-Server Schlüssel zu installieren.

Vertrauenswürdige CA-Zertifikat löschen

Diese Funktion ermöglicht es Ihnen, die vertrauenswürdige CA des VPN-Servers zu löschen. Danach werden keine VPN-Verbindungen mehr akzeptiert, die sich mit X.509-Zertifikaten anmelden wollen, die von dieser CA unterschrieben wurden. Ausgenommen sind davon die Verbindungen, für die der öffentliche Schlüssel der Gegenstelle zur Authentifizierung im SX-GATE hinterlegt ist.

Zertifikats-Sperrliste der CA importieren

Hier haben Sie die Möglichkeit, eine Zertifikats-Sperrliste (CRL) zur vertrauenswürdigen CA zu hinterlegen bzw. zu aktualisieren. Sinn einer Zertifikats-Sperrliste ist es, bestimmte Zertifikate bereits vor deren Ablaufdatum als ungültig zu erklären. Dies ist z.B. notwendig, wenn ein Mitarbeiter die Firma verlässt und diesem zeitnah der VPN-Zugang verwehrt werden muss. Sie können die CRL von der lokalen SX-GATE CA kopieren oder eine CRL-Datei im PEM-Format importieren.



Die CRL ist nur dann wirksam, wenn sie von der vertrauenswürdigen CA ausgestellt wurde.

Lokale CA-Sperrliste im VPN-Server hinterlegen

Arbeitet der SX-GATE VPN-Server mit Zertifikaten der eigenen SX-GATE CA, haben Sie hier die Möglichkeit, die derzeitige Zertifikats-Sperrliste (CRL) in den lokalen VPN-Server zu übertragen. Sinn einer Zertifikats-Sperrliste ist es, bestimmte Zertifikate bereits vor deren Ablaufdatum als ungültig zu erklären. Dies ist z.B. notwendig, wenn ein Mitarbeiter die Firma verlässt und diesem zeitnah der VPN-Zugang verwehrt werden muss.

Zertifikats-Sperrliste der CA löschen

Diese Funktion ermöglicht es Ihnen, die Zertifikat-Sperrliste zu löschen. Darin widerrufen Zertifikate sind danach wieder gültig.

14.1.2 Schnittstellen

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Schnittstellentyp

Um eine neue Schnittstelle anzulegen, wählen Sie hier bitte den Schnittstellentyp aus den Sie anlegen wollen.

ADSL/Mobilfunk (adsl)

Für eine ADSL-Schnittstelle wird eine der Netzwerkkarte des Systems genutzt. Welche Netzwerkkarte Sie verwenden wollen, können Sie nach dem Anlegen der Schnittstelle in den zugehörigen Einstellungen festlegen. Für Mobilfunk wird hingegen ein USB-Stick benötigt, den Sie über den SX-GATE-Fachhandel beziehen können.

Ethernet (eth)

Die Netzwerkkarten des SX-GATE sind fortlaufend nummeriert beginnend von 0. Die Schnittstelle eth2 gehört damit zur dritten Netzwerkkarte.

VLAN 802.1Q (vlan)

VLAN Schnittstellen sind logische Schnittstellen, die Ethernet Frames nach dem IEEE 802.1Q Standard markieren. Eine VLAN Schnittstelle muss einer zugrundeliegenden Netzwerk-Schnittstelle zugewiesen werden. Die Schnittstellennummer der angelegten VLAN Schnittstelle entspricht der VLAN-ID. Es sind Werte im Bereich 1 bis 4094 zulässig.



Ein über eine VLAN-Schnittstelle geroutetes Paket wird automatisch mit dem zugehörigen VLAN-Tag versehen. Empfangen werden ausschließlich Pakete mit entsprechendem VLAN-Tag.



Ist die zugrundeliegende Netzwerk-Schnittstelle als normale Netzwerk-Schnittstelle angelegt, werden darüber Pakete ohne VLAN-Tag gesendet bzw. empfangen. Falls dies nicht erwünscht ist, sollten Sie die Schnittstelle löschen oder den VLAN-Switch entsprechend konfigurieren.

WLAN (wlan)

Um eine eingebaute WLAN-Karte zu nutzen, legen Sie bitte die WLAN-Schnittstellen mit der Nummer 0 an. Es ist möglich, bis zu sieben weitere SSIDs auf der selben WLAN-Karte und dem selben Kanal zur Verfügung zu stellen. Legen Sie dazu bitte WLAN-Schnittstellen mit Nummern größer als 0 an.

Wireguard (wg)

Für jede Schnittstelle diesen Typs wird eine eigene Wireguard-Instanz mit jeweils eigenen Einstellungen erzeugt. Da eine Wireguard-Instanz eine beliebige Zahl von Gegenstellen bedienen kann, genügt häufig eine Schnittstelle. Mehrere Schnittstellen sind nützlich, um Gegenstellen zu Gruppieren (z.B. Clients und VPN-Server) und wenn unterschiedliche Firewall-Einstellungen erforderlich

sind (z.B. eigene Mitarbeiter bzw. Außenstellen und externe Mitarbeiter bzw. Fremdfirmen).

OpenVPN Client (ovpnc)

Sie benötigen eine Schnittstelle diesen Typs, wenn sich SX-GATE mit einem OpenVPN-Server verbinden soll. Für jede Verbindung zu einem OpenVPN-Server ist eine eigene Schnittstelle anzulegen.

OpenVPN Server (ovpns)

Für jede Schnittstelle diesen Typs wird eine eigene OpenVPN-Server-Instanz mit jeweils eigenen Einstellungen erzeugt. Da eine Server-Instanz eine beliebige Zahl von Clients bedienen kann, genügt es in der Regel, eine einzige Server-Instanz zu erzeugen. Mehrere Schnittstellen sind nützlich, um Gegenstellen zu Gruppieren (z.B. Clients und VPN-Server) und wenn unterschiedliche Firewall-Einstellungen erforderlich sind (z.B. eigene Mitarbeiter bzw. Außenstellen und externe Mitarbeiter bzw. Fremdfirmen).

IPSec VPN (ipsec)

Schnittstellen dieses Typs sind logische Schnittstellen. Eine ipsec-Schnittstelle wird auf eine andere Schnittstelle aufgesetzt, um dieser VPN-Funktionalität zu verleihen. Vergeben Sie für die Schnittstelle eine beliebige einstellige Nummer. Ausschließlich ipsec0 unterstützt dabei Basis-Schnittstellen mit dynamischer IP-Adresse, wobei die Internet-Anbindung (Defaultroute) über eben diese Basis-Schnittstelle erfolgen muss.

Schnittstellen-Nummer

Geben Sie hier die Schnittstellen-Nummer ein. Beachten Sie dabei bitte die oben beschriebenen Besonderheiten zu den einzelnen Schnittstellen-Typen.

Firewall-Vertrauensstufe

Legen Sie hier die Grundeinstellung der Firewall für diese Schnittstelle fest.

14.1.2.1 ADSL/Mobilfunk (adsl)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.1-A ADSL/PPPoE.....	292
14.1.2.1-B ADSL/PPTP.....	294
14.1.2.1-C Mobilfunk.....	295
14.1.2.1-D IP-Adressen.....	297
14.1.2.1-E Routing.....	298
14.1.2.1-F Bandbreitenmanagement / QoS.....	298
14.1.2.1-G Priorisierung.....	301
14.1.2.1-H Dynamischer DNS.....	303
14.1.2.1-I Limits.....	304
14.1.2.1-J Ethernet.....	306

Verbindungstyp

Stellen Sie hier bitte den erforderlichen ADSL-Typ ein.

ADSL/PPPoE

Zum Anschluss an eine DSL-Leitungen über die mit PPP-over-Ethernet (PPPoE) kommuniziert wird, muss SX-GATE mit einem DSL-Router im Bridge-Modus oder einem DSL-Modem verbunden werden.

ADSL/PPTP

Um SX-GATE an einem PPP-over-ATM (PPPoA) Anschluss zu betreiben, ist ein DSL-Modem mit integriertem PPtP-to-PPPoA Relay erforderlich. SX-GATE kommuniziert mit diesem Modem über das PPtP-Protokoll.

Mobilfunk

Wählen Sie diese Einstellung um SX-GATE per LTE/UMTS/GPRS an das Internet anzubinden. Dazu ist ein zertifizierter USB-Stick mit gültiger SIM-Karte an SX-GATE anzuschließen.

IPv4 Modus

Bei aktiviertem IPv6 wählen Sie hier die Art der IPv4-Anbindung aus.

Dual-Stack

Wählen Sie diese Zugangsart, wenn der Provider sowohl eine IPv4- als auch eine IPv6-Adresse zuweist. Bei der IPv4-Adresse kann es sich dabei durchaus auch

um eine interne IP nach RFC-1918 handeln, die dann beim Provider nochmal übersetzt wird (Carrier-Grade NAT).

Dual-Stack Lite (DS-Lite)

Bei einem DS-Lite Zugang stellt der Provider eine reine IPv6-Verbindung zur Verfügung. IPv4-Pakete werden in Form eines Tunnels über die IPv6-Verbindung zu einem speziellen Gateway des Providers geleitet. Erst dort erhält das IPv4-Paket seine endgültige Absender-Adresse (Carrier-Grade NAT) und wird in das IPv4-Internet weitergeleitet.

IPv6 Modus

manuelle IP

In dieser Einstellung muss die IPv6-Konfiguration manuell erfolgen. Router-Advertisements werden ignoriert.

automatische IP (SLAAC/DHCPv6)

Wählen Sie diese Einstellung, wenn SX-GATE seine IPv6-Konfiguration automatisch anhand der empfangenen Router-Advertisements vornehmen soll.

14.1.2.1-A ADSL/PPPoE

Beschreibung

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Login

Geben Sie hier die Benutzerkennung ein, mit der sich der SX-GATE bei der Gegenstelle anmelden soll.

Passwort

Geben Sie hier das Passwort für die Anmeldung bei der Gegenstelle ein.

Verwendete Netzwerkkarte

Wählen Sie hier den Namen der Netzwerkkarte aus, die mit dem ADSL-Modem verbunden ist. Wir empfehlen eine eigene Netzwerkkarte für die ADSL-Verbindung zu nutzen, d.h. eine Netzwerkkarte die im Menübaum nicht bereits unter "Netzwerk" gelistet ist.

VDSL über VLAN

Tragen Sie hier eine VLAN-ID ein, wenn es sich um einen VDSL-Zugang handelt, der über VLAN angesprochen wird. Die Kommunikation mit dem DSL-Modem erfolgt dann über entsprechend markierte VLAN-Pakete. Die zu verwendende VLAN-ID erfragen Sie bitte bei Ihrem Provider.



VDSL-Zugänge der Deutschen Telekom nutzen in der Regel VLAN-ID 7, VDSL-Zugänge von Vodafone VLAN-ID 132.

Neuen Treiber verwenden

Der neue Treiber unterstützt höhere Geschwindigkeiten. Aktivieren Sie diese Option bei Anbindungen über 200 Mbit/s.

Verbindung trennen bei Inaktivität

Wählen Sie hier, wie für den Auf- und Abbau der DSL-Wählverbindung verfahren werden soll.

Die Wählverbindung kann automatisch aufgebaut werden, sobald Daten in das Internet übertragen werden sollen. Die Verbindung wird in diesem Falle wieder getrennt, wenn während der konfigurierten Zeitspanne keine Daten mehr über die Leitung übertragen wurden.

Alternativ kann die Internet-Verbindung permanent gehalten werden. Eine getrennte Verbindung wird sofort wieder aufgebaut.



Häufig trennt der Internet-Zugangs-Provider von sich aus die Leitung, wenn über einen bestimmten Zeitraum hinweg keine Daten übertragen werden. Möglicherweise wird die Verbindung auch getrennt, wenn die Verbindungsdauer einen bestimmten Wert überschreitet (z.B. nach 24 Stunden).



Aktivieren Sie die permanente Verbindung nur, wenn die Internet-Verbindung von Ihrem Provider nicht zeitbasierend abgerechnet wird.

Verbindung trennen um

Manche Provider trennen eine ADSL-Verbindung wenn diese 24 Stunden ununterbrochen online ist. Findet diese Trennung regelmäßig während der üblichen Arbeitszeit statt, kann dies störend sein. Konfigurieren Sie hier eine Uhrzeit zu der grundsätzlich eine bestehende Verbindung vom SX-GATE getrennt werden soll. Auf diese Weise lässt sich die Zwangstrennung z.B. in die Nachtstunden verlegen.

Lassen Sie das Eingabefeld leer wenn kein Verbindungsabbau erwünscht ist.

14.1.2.1-B ADSL/PPTP

Beschreibung

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Login

Geben Sie hier die Benutzerkennung ein, mit der sich der SX-GATE bei der Gegenstelle anmelden soll.

Passwort

Geben Sie hier das Passwort für die Anmeldung bei der Gegenstelle ein.

Modem IP

Für PPPoA-Verbindungen muss hier die IP-Adresse des Modems angegeben werden. SX-GATE stellt eine PPtP-Verbindung zu dieser Adresse her.



Die Standard-IP vieler Modems lautet 10.0.0.138.



Zusätzlich zur adsl-Schnittstelle muss eine eth-Schnittstelle mit passender IP-Adresse eingerichtet sein, über die das Modem angesprochen wird.

Verbindung trennen bei Inaktivität

Wählen Sie hier, wie für den Auf- und Abbau der DSL-Wählverbindung verfahren werden soll.

Die Wählverbindung kann automatisch aufgebaut werden, sobald Daten in das Internet übertragen werden sollen. Die Verbindung wird in diesem Falle wieder getrennt, wenn während der konfigurierten Zeitspanne keine Daten mehr über die Leitung übertragen wurden.

Alternativ kann die Internet-Verbindung permanent gehalten werden. Eine getrennte Verbindung wird sofort wieder aufgebaut.



Häufig trennt der Internet-Zugangs-Provider von sich aus die Leitung, wenn über einen bestimmten Zeitraum hinweg keine Daten übertragen werden. Möglicherweise wird die Verbindung auch getrennt, wenn die Verbindungsdauer einen bestimmten Wert überschreitet (z.B. nach 24 Stunden).



Aktivieren Sie die permanente Verbindung nur, wenn die Internet-Verbindung von Ihrem Provider nicht zeitbasierend abgerechnet wird.

Verbindung trennen um

Manche Provider trennen eine ADSL-Verbindung wenn diese 24 Stunden ununterbrochen online ist. Findet diese Trennung regelmäßig während der üblichen Arbeitszeit statt, kann dies störend sein. Konfigurieren Sie hier eine Uhrzeit zu der grundsätzlich eine bestehende Verbindung vom SX-GATE getrennt werden soll. Auf diese Weise lässt sich die Zwangstrennung z.B. in die Nachtstunden verlegen.

Lassen Sie das Eingabefeld leer wenn kein Verbindungsabbau erwünscht ist.

14.1.2.1-C Mobilfunk

Beschreibung

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Bevorzugter Modus

In manchen Situationen können bessere Durchsatzraten erzielt werden, wenn man zum Beispiel UMTS anstatt LTE bevorzugt. Mit dieser Einstellung kann der angegebene Modus erzwungen werden.

Login

Geben Sie hier die Benutzerkennung ein, mit der sich der SX-GATE bei der Gegenstelle anmelden soll.



Bei Mobilfunk-Verbindungen ist, abhängig vom Provider, die Angabe von Zugangsdaten nicht immer notwendig.

Passwort

Geben Sie hier das Passwort für die Anmeldung bei der Gegenstelle ein.

APN

Geben Sie hier den Zugangspunkt (Access Point Name) an. Diesen finden Sie normalerweise in den Unterlagen von Ihrem Provider.

PIN

Hier geben Sie die PIN-Nummer ein, mit der Ihre SIM-Karte geschützt ist. Sollten Sie keine PIN vergeben haben, lassen Sie das Feld bitte leer.

Einwahl-Nummer

Geben Sie hier die für Ihren Provider benötigte Einwahl-Nummer an. Diese ist üblicherweise *99#, kann aber auch z.B. *99***1# lauten.

Verbindung trennen bei Inaktivität

Wählen Sie hier, wie für den Auf- und Abbau der DSL-Wählverbindung verfahren werden soll.

Die Wählverbindung kann automatisch aufgebaut werden, sobald Daten in das Internet übertragen werden sollen. Die Verbindung wird in diesem Falle wieder getrennt, wenn während der konfigurierten Zeitspanne keine Daten mehr über die Leitung übertragen wurden.

Alternativ kann die Internet-Verbindung permanent gehalten werden. Eine getrennte Verbindung wird sofort wieder aufgebaut.



Häufig trennt der Internet-Zugangs-Provider von sich aus die Leitung, wenn über einen bestimmten Zeitraum hinweg keine Daten übertragen werden. Möglicherweise wird die Verbindung auch getrennt, wenn die Verbindungsdauer einen bestimmten Wert überschreitet (z.B. nach 24 Stunden).



Aktivieren Sie die permanente Verbindung nur, wenn die Internet-Verbindung von Ihrem Provider nicht zeitbasierend abgerechnet wird.

Verbindung trennen um

Manche Provider trennen eine ADSL-Verbindung wenn diese 24 Stunden ununterbrochen online ist. Findet diese Trennung regelmäßig während der üblichen Arbeitszeit statt, kann dies störend sein. Konfigurieren Sie hier eine Uhrzeit zu der grundsätzlich eine bestehende Verbindung vom SX-GATE getrennt werden soll. Auf diese Weise lässt sich die Zwangstrennung z.B. in die Nachtstunden verlegen.

Lassen Sie das Eingabefeld leer wenn kein Verbindungsabbau erwünscht ist.

14.1.2.1-D IP-Adressen

IPv4-Adresse

Sie haben die Möglichkeit, eine von der Gegenstelle zugewiesene dynamische IP-Adresse zu akzeptieren oder eine bestimmte IP-Adresse festzulegen.

DS-Lite Address-Family-Transition-Router (AFTR)

Bei Internetzugängen über Dual-Stack Lite werden IPv4-Pakete über IPv6 getunnelt. Der Tunnel terminiert auf Seiten des Providers an einem speziellen Router. Sofern dessen Adresse nicht über DHCP automatisch bezogen werden kann, müssen Sie die Adresse hier angeben.

IPv6-Adresse

Geben Sie hier die IPv6-Adresse für die Schnittstelle ein.

Präfixlänge

Bei der IPv6-Präfixlänge handelt es sich um das Pendant zur IPv4-Netzmaske. Die typische Präfixlänge ist 64, eventuell haben Sie von Ihrem Provider jedoch auch einen größeren Wert erhalten.

IPv6-Privacy-Extension (RFC3041)

Eine dynamisch per SLAAC ermittelte IPv6-Adresse basiert auf der Hardware-Adresse der zugehörigen Netzwerkkarte und kann daher global eindeutig verfolgt werden. Wenn Sie diese Option aktivieren, ermittelt SX-GATE zusätzlich eine zufällige temporäre Adresse, die bevorzugt verwendet wird.

IPv6-Präfixdelegation anfordern

Aktivieren Sie diesen Schalter um sich vom Provider einen Block IPv6-Netzwerke per DHCP zuweisen zu lassen. Diese Netze können dann vom SX-GATE an lokale Netze weiterverteilt werden.

Für den vom Provider zugewiesenen Adressblock wird im Menü "Definitionen > IP-Objekte" automatisch ein Eintrag erstellt (für die Schnittstelle "adsl0" lautet dieser "ipv6_prefix_adsl0"). Legen Sie dort Einträge vom Typ "IPv6-Präfix" oder "IPv6-Adresse" an, die sich auf den zugewiesenen Präfix beziehen und ihn weiter unterteilen. Die so definierten Objekte können Sie dann in zahlreichen Konfigurations-Optionen verwenden.

zusätzliche IPv6-Adressen (Aliase)

Nutzen Sie diesen Bereich, um weitere IPv6-Adressen an diese Netzwerkkarte zu binden.

14.1.2.1-E Routing

Erweitertes Routing

Auf diesem Reiter können statische Routen konfiguriert werden. Neben herkömmlichen Routen, bei denen lediglich die Ziel-Adresse bei der Routing-Entscheidung berücksichtigt wird, können auch erweiterte Routen erstellt werden. Dabei lassen sich die Quell-Adresse sowie Protokoll- und Port-Nummern auswerten (Policy-based Routing).

Statische Routen müssen für Netzwerke spezifiziert werden, die sich hinter der Gegenstelle befinden. Für die Gegenstelle selbst ist kein Eintrag erforderlich. Das Zielnetzwerk wird über die Netzwerkadresse und die zugehörige Netzmaske spezifiziert, womit das Netzwerk automatisch auch der SX-GATE Firewall bekannt gemacht wird.

Regeln für spezielle Protokolle oder Quell-Adressen bieten sich an, wenn mehrere Internet-Anbindungen zur Verfügung stehen. So ließe sich z.B. das Surfen im Internet über eine ADSL-Verbindung leiten, während die übrige Kommunikation wie Mail oder VPN über eine SDSL-Leitung läuft.

Die Priorität der einzelnen Routen ergibt sich nicht aus der Reihenfolge in der sie eingetragen werden. Entscheidend ist vielmehr, wie spezifisch die Routen sind. Schnittstellenübergreifend haben Routen, bei denen Protokoll, Quelle und Ziel angegeben sind, die höchste Priorität. Regeln mit Ziel haben Vorrang vor Regeln mit Protokoll, diese wiederum vor Regeln mit Angabe einer Quelle. Innerhalb von Quelle und Ziel erfolgt die Sortierung nach absteigender Netzmaske. Die Reihenfolge bei Überschneidungen im Protokoll ist nicht definiert.

14.1.2.1-F Bandbreitenmanagement / QoS

Für das Bandbreiten-Management müssen Sie die Bandbreite der Anbindung festlegen. Die eingehende und ausgehende Bandbreite kann dabei unterschiedlich sein (ADSL). Solange Sie keine Bandbreite festlegen, ist das Bandbreitenmanagement auf dieser Schnittstelle deaktiviert. Wenn Sie lediglich die ein- oder die ausgehende Bandbreite eintragen, ist das Bandbreitenmanagement auch nur in dieser Richtung aktiv.



Die Angabe einer falschen Bandbreite kann zu Problemen führen. Dies gilt insbesondere, wenn die eingestellte Bandbreite höher ist als die tatsächlich verfügbare. Fragen Sie im Zweifel Ihren Provider.

Bandbreite ausgehend (Uplink)

Geben Sie hier die ausgehende Bandbreite (Uplink) an. Bei asymmetrischen Anbindungen ist dies in der Regel der kleinere Wert. Es werden dann alle über diese Schnittstelle ausgehenden Datenpakete vom Bandbreitenmanagement verarbeitet. Die Verbindungsrichtung (eingehende oder ausgehende Verbindung) spielt dabei keine Rolle.

Bandbreite eingehend (Downlink)

Geben Sie hier die eingehende Bandbreite (Downlink) an. Bei asymmetrischen Anbindungen ist dies in der Regel der größere Wert. Es werden dann alle über diese Schnittstelle eingehenden Datenpakete vom Bandbreitenmanagement verarbeitet. Die Verbindungsrichtung (eingehende oder ausgehende Verbindung) spielt dabei keine Rolle. Lassen Sie das Feld leer, wenn Sie kein eingehendes Bandbreitenmanagement wünschen.

Eingehendes Bandbreitenmanagement ist eigentlich ein Widerspruch in sich. Das Umsortieren von auf die Übertragung wartend Datenpaketen nach Priorität müsste eigentlich auf der anderen Seite der (Internet-)Verbindung vorgenommen werden, denn nur dort ist dies zuverlässig möglich. Beim eingehenden Bandbreitenmanagement sind die Pakete ja bereits übertragen worden. Internet-Anbindungen mit providerseitigem Quality-of-Service/Bandbreitenmanagement sind jedoch oft sehr teuer, so dass eingehendes Bandbreitenmanagement trotz seiner Einschränkungen gewünscht wird.



Eingehendes Bandbreitenmanagement reduziert die verfügbare Bandbreite um bis zu 20%. Es funktioniert nur, solange das eingehende Datenvolumen zu einem ausreichend hohen Anteil über TCP-Verbindungen abgewickelt werden.

Quality-of-Service (QoS) für Voice-over-IP (VoIP)

Bei VoIP spielt die Latenzzeit, also die Zeitspanne die ein Sprachdatenpaket vom Absender zum Empfänger benötigt, eine große Rolle. Das Bandbreitenmanagement des SX-GATE optimiert den Versand von VoIP-Paketen daher mit Hilfe eines speziellen Quality-of-Service Moduls.



Um als VoIP-Paket erkannt zu werden, muss ein IP-Paket gemäß Diffserv-Code-Point Expedited-Forwarding (DSCP EF) markiert sein.

Die Bandbreite eines einzelnen Gesprächs ist abhängig vom jeweils verwendeten Codec. Der Codec bestimmt dabei, wie stark das Gespräch komprimiert wird. Je stärker der Codec das Gespräch komprimiert, desto weniger Bandbreite wird benötigt. Im

Gegenzug sinkt jedoch die Qualität des Gesprächs mit der Zunahme der Kompression. Die folgende Tabelle gibt die Nettobandbreite typischer Codecs an. Bei Codecs die mit verschiedenen Bandbreiten genutzt werden, ist jeweils die maximale Bandbreite angegeben.

Codec	max. Bandbreite (bit/s)
G.711	64000
G.722	64000
G.722.1	32000
G.723.1	6400
G.726	40000
G.728	16000
G.729	8000
GSM	13000
iLBC	15200

Max. Anzahl gleichzeitiger Gespräche

Geben Sie die maximal erwartete Anzahl gleichzeitiger unverschlüsselter Gespräche an, die über diese Schnittstelle abgewickelt werden. Die Anzahl der Gespräche dient als Grundlage für die Berechnung der insgesamt für VoIP zu reservierenden Bandbreite. Der Wert "0" deaktiviert die Priorisierung.



Die Insgesamt zur Verfügung stehende Bandbreite der Anbindung darf nicht überschritten werden.

Bitrate des verwendeten Codecs

Geben Sie die Nettobandbreite des verwendeten Codecs an. Bei Verwendung unterschiedlicher Codecs orientieren Sie sich bitte am Codec mit dem größten Bandbreitenbedarf.



Zur Berechnung der insgesamt benötigten Bandbreite wird vom System automatisch der IP-Overhead eingerechnet. Dieser ist umso größer, je kleiner die Bitrate des Codecs ist.

Max. Anzahl Gespräche über IPSec

Geben Sie die maximal erwartete Anzahl gleichzeitiger Gespräche über IPSec-VPN an, die über diese Schnittstelle abgewickelt werden. Die Anzahl der Gespräche dient als Grundlage für die Berechnung der insgesamt für VoIP zu reservierenden Bandbreite. Der Wert "0" deaktiviert die Priorisierung.



Wenn aktiviert, werden VoIP-Datenpakete gegenüber anderem VPN-Datenverkehr bevorzugt. Selbiges gilt nach der Verschlüsselung für die entstandenen VPN-Pakete.



Die Insgesamt zur Verfügung stehende Bandbreite der Anbindung darf nicht überschritten werden.

Bitrate des Codecs im IPSec

Geben Sie die Nettobandbreite des verwendeten Codecs an. Bei Verwendung unterschiedlicher Codecs orientieren Sie sich bitte am Codec mit dem größten Bandbreitenbedarf.



Zur Berechnung der insgesamt benötigten Bandbreite wird vom System automatisch der IP- und der IPSec-Overhead eingerechnet. Dieser ist umso größer, je kleiner die Bitrate des Codecs ist.

14.1.2.1-G Priorisierung

Mit Hilfe dieser Funktion können Datenpakete auf verschiedene Prioritätsklassen aufgeteilt werden. Jeder Klasse ist eine anteilige Mindestbandbreite zugeordnet. Nicht benötigte Bandbreite einer höherpriorien Klasse steht den nachfolgenden Klassen zur Verfügung.

Aus technischer Sicht wird durch die Regeln das ToS- bzw. DSCP-Feld von IP-Paketen überschrieben. Setzt eine lokale Anwendung bereits das ToS/DSCP-Feld passend, ist keine Regel für ausgehende Pakete notwendig. Bei eingehenden Paketen wird das ToS/DSCP-Feld häufig auf dem Weg durch das Internet verändert, so dass für das eingehende Bandbreitenmanagement üblicherweise Regeln erforderlich sind.



Manche Provider stellen Datenpakete mit gesetztem ToS/DSCP-Feld in Rechnung. Bitte prüfen Sie Ihre Vertragsbedingungen.

Die Mindestbandbreiten werden wie folgt verteilt: Die für VoIP benötigte Bandbreite gemäß Konfiguration wird reserviert und von der insgesamt verfügbaren Bandbreite abgezogen. Von der verbliebenen Bandbreite entfallen 10% auf leere TCP ACK-Pakete, 50% auf hochprioritäre Datenpakete und je 20% auf Pakete mit normaler oder niedriger Priorität.



Für das eingehende Bandbreitenmanagement werden nicht-TCP Pakete grundsätzlich wie hochprioritäre Datenpakete behandelt.

Priorisierung von Verbindungen

Fügen Sie dieser Liste die Signaturen der Datenpakete hinzu, die eine höhere oder niedriger Priorität erhalten sollen. Treffen mehrere Regeln auf ein Datenpaket zu, so wird die Priorität des ersten passenden Eintrags angewendet.

Die einzelnen Eingabefelder haben dabei folgende Bedeutungen:

Protokoll

Legt die IP-Protokoll und Port-Signatur fest. Bei eingehendem Bandbreitenmanagement werden ausschließlich TCP-Protokolle berücksichtigt.



Protokoll-Definitionen werden im Menü "Definitionen > Protokolle" vorgenommen.

Lokale IP/Netzwerk

Auf dieser Seite steht die aus Sicht der gewählten Schnittstelle lokale Adresse. Bei einem ausgehenden Datenpaket entspricht dies der Quell-IP (vor SNAT), bei einem eingehenden Datenpaket der Ziel-IP (vor DNAT).



Wenn Sie die Priorisierung bei DNAT- oder SNAT-Verbindungen auf bestimmte lokale IPs beschränken wollen, sind üblicherweise zwei Regeln erforderlich um beide Verbindungsrichtungen abzudecken: Für eingehende Datenpakete muss eine SX-GATE IP angegeben werden, für ausgehende Datenpakete die interne IP (des LAN-Clients bzw. des per DNAT angesprochenen Servers).

Richtung

Wählen Sie hier bitte aus, in welcher Richtung die Portsignatur des gewählten Protokolls interpretiert wird. Erläutert am Beispiel HTTP bedeutet der Richtungspfeil "-->", der HTTP-Port 80 befindet sich auf der externen Seite. Das ausgehende Bandbreitenmanagement verarbeitet folglich Pakete zu Port 80, das eingehende von Port 80. Wird der entgegengesetzt orientierte Pfeil "<--" gewählt, werden eingehende HTTP-Verbindungen verarbeitet. Pakete zu Port 80 durchlaufen das eingehende Bandbreitenmanagement, Pakete von Port 80 das ausgehende. Der Doppelpfeil "↔" steht für beide Interpretationsrichtungen.

Externe IP/Netzwerk

Auf dieser Seite steht die aus Sicht der gewählten Schnittstelle externe Adresse. Bei einem ausgehenden Datenpaket entspricht dies der Ziel-IP, bei einem eingehenden Datenpaket der Quell-IP.

Priorität

Wählen Sie hier die gewünschte Priorisierung aus.

14.1.2.1-H Dynamischer DNS

Dynamischer DNS ermöglicht es, ein Gerät, das eigentlich mit einer dynamischen IP-Adresse an das Internet angebunden ist, unter dessen jeweils aktueller Adresse aufzufinden. Mit Hilfe dieses Dienstes kann also vom Internet aus auf SX-GATE zugegriffen werden, obwohl dieser nur über eine dynamische IP-Adresse verfügt. Die Adressierung im dynamischen DNS erfolgt mit Hilfe eines üblichen DNS-Rechnernamens (Fully-Qualified-Domain-Name, FQDN). Es gibt eine Reihe von Anbietern, die dynamischen DNS sowohl als kostenlose als auch als kostenpflichtige Dienstleistung zur Verfügung stellen.



Nach einem IP-Wechsel vergehen einige Sekunden bis Minuten, bis der DNS-Name auch tatsächlich auf die neue IP-Adresse verweist.

Sofern SX-GATE selbst die dynamische IP erhält (ADSL-Schnittstelle mit dynamischer IP oder Ethernet-Schnittstelle mit IP-Vergabe über DHCP), konfigurieren Sie dynamischen DNS bitte in der jeweiligen Schnittstelle im Menü "Module > Netzwerk > Schnittstellen". SX-GATE aktualisiert seine IP-Adresse im dynamischen DNS dann einmalig bei jedem Verbindungsaufbau bzw. IP-Wechsel.

Für den Fall, dass sich SX-GATE hinter einem NAT-Router befindet und dieser die dynamische IP erhält, muss der NAT-Router eingehende Verbindungen an SX-GATE weiterreichen können (DNAT, Portforwarding, Exposed Host). Optimalerweise konfigurieren Sie dynamischen DNS im NAT-Router, da nur dieser die aktuelle dynamische IP kennt. Ist dies nicht möglich, konfigurieren Sie dynamischen DNS bitte hilfsweise im SX-GATE Menü "Module > DNS > Einstellungen". SX-GATE versucht

dann in regelmäßigen Abständen die dynamische IP des NAT-Routers mit Hilfe eines Internet-Dienstes zu ermitteln.

Protokoll

Für die Aktualisierung der Einträge im dynamischen DNS gibt es leider keinen einheitlichen Standard. SX-GATE unterstützt jedoch eine ganze Reihe von Protokollen für diese Aktualisierung. Bitte klären Sie zunächst mit dem Anbieter des dynamischen DNS-Dienstes, welches Protokoll verwendet wird und ob dieses vom SX-GATE unterstützt wird.

Update-Server des Anbieters

Tragen Sie hier bitte den Namen des Servers ein, der die Nachrichten zur Aktualisierung der dynamischen IP-Adresse entgegen nimmt. Dieser Server ist nicht immer identisch mit dem Webserver des Anbieters.

Update-URL

Tragen Sie hier bitte die Update-URL (auch "Direct URL" genannt) zur Aktualisierung der dynamischen IP-Adresse ein. Die URL kann die Platzhalter <host>, <ipaddr>, <username> und <password> enthalten, die durch den dynamischen DNS-Namen, die IP-Adresse, den Benutzernamen und das Passwort ersetzt werden. Beispiel: `http://dynupdate.exampledyndns.com/nic/update?hostname=<domain>&myip=<ipaddr>`

Dynamischer DNS-Name des SX-GATES

Über ein Benutzerkonto bei dem jeweiligen Anbieter lassen sich in der Regel mehrere DNS-Namen verwalten. Daher ist hier der vollständige Name (inkl. Domain) anzugeben, unter dem SX-GATE im dynamischen DNS erreichbar ist.

Benutzername

Keine Aktualisierung des Eintrags im dynamischen DNS ohne entsprechende Anmeldung. Geben Sie hier den Benutzernamen (login) für das Konto an.

Passwort

Geben Sie hier schließlich das entsprechende Kennwort für die Aktualisierung an.

Jetzt aktualisieren

Hiermit können Sie die eingegebenen Verbindungsdaten testen.

14.1.2.1-l Limits

Bei einer Internet-Anbindung über eine ADSL-Wählleitung besteht die Möglichkeit, bestimmte Obergrenzen für die Verbindungsdauer und -anzahl zu definieren. Die Einstellung gilt jeweils für die Schnittstelle, die im SX-GATE als Standard-Gateway konfiguriert wurde.



Erfolgt die Gebührenabrechnung Ihres Internet-Zugangs in Abhängigkeit von Verbindungsdauer oder -häufigkeit, so empfiehlt es sich in Ihrem eigenen Interesse entsprechende Grenzen einzustellen. Nur so können Sie sich vor hohen Gebühren zu schützen, die z.B. durch das Fehlverhalten einer Anwendung verursacht werden.

Für jedes der nachfolgenden Kriterien lassen sich zwei Grenzwerte definieren. Bei Erreichen des ersten Limits wird eine Warn-E-Mail an den Administrator gesendet. Wird das zweite Limit überschritten, so wird ebenfalls eine E-Mail gesendet. Zudem wird die Schnittstelle deaktiviert.



Eine deaktivierte Schnittstelle wird wieder aktiviert, sobald der zugehörige Dienst neu gestartet wird.

Damit ein Grenzwert nicht überprüft wird, ist das jeweilige Eingabefeld leer zu lassen.

Für jedes der Kriterien werden auch die bislang aufgelaufenen Werte angezeigt.



Erst mit dem vollständigen Aufbau einer IP-Verbindung beginnen die Zähler zu laufen. Wird also eine ADSL-Verbindung erstellt, die Anmeldung beim Provider schlägt jedoch fehl, so wird diese Verbindung nicht berücksichtigt.

Warnmeldung nach Verbindungsdauer

Mit diesen Grenzwerten wird die Gesamtdauer der aktuellen Verbindung überwacht.

Warnmeldung bei Summe Verbindungsdauer

Mit diesen Grenzwerten wird die Gesamtdauer aller Verbindungen überwacht. Über den Schalter "Summe Verbindungsdauer und Anzahl zurücksetzen" wird konfiguriert, wie oft die Gesamtdauer zurückgesetzt werden soll.

Warnmeldung bei Anzahl Verbindungen

Mit diesen Grenzwerten wird die Anzahl aller Verbindungen überwacht. Über den Schalter "Summe Verbindungsdauer und Anzahl zurücksetzen" wird konfiguriert, wie oft deren Summe zurückgesetzt werden soll.

Summe Verbindungsdauer und Anzahl zurücksetzen

Die Summen werden in dem hier eingestellten Intervall zurückgesetzt.



Eine gestoppte Schnittstelle wird durch das Zurücksetzen der Summe nicht neu gestartet.

Jetzt zurücksetzen

Mit Hilfe dieses Schalters können die Summenwerte jederzeit zurückgesetzt werden.



Eine gestoppte Schnittstelle wird auch mit dem Ausführen dieser Funktion nicht wieder aktiviert. Starten Sie den entsprechenden Dienst unter "System > Dienste" neu.

14.1.2.1-J Ethernet

Bei Problemen mit der automatischen Erkennung der erforderlichen Netzwerkkarten-Parameter können Sie hier auf die manuelle Konfiguration umschalten.



Nicht alle Netzwerkkarten unterstützen die manuelle Konfiguration.

Geschwindigkeit

Legen Sie hier die von der Netzwerkkarte zu verwendenden Geschwindigkeit fest.

Duplex

Wählen Sie hier bitte den gewünschten Duplex-Modus.

14.1.2.2 Ethernet (eth)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.2-A Einstellungen.....	309
14.1.2.2-B IP-Adressen.....	312
14.1.2.2-C IPv6 Router-Advertisement.....	314
14.1.2.2-D Routing.....	316
14.1.2.2-E Bandbreitenmanagement / QoS.....	317
14.1.2.2-F Priorisierung.....	320
14.1.2.2-G Dynamischer DNS.....	321
14.1.2.2-H Paket Monitor.....	323
14.1.2.2-I Server Adressen.....	323
14.1.2.2-J Optionale Regeln.....	323

Schnittstellen-Modus

Legen Sie hier fest, wie die Netzwerkkarte genutzt werden soll.

eigenständiges Netzwerk

In diesem Modus erhält die Netzwerkkarte eine eigene IP-Konfiguration.

weiterer Port für Bündelung

Wählen Sie diese Einstellung, wenn Sie die Netzwerkkarte einem Bündel hinzufügen wollen.



Um ein neues Bündel zu erstellen, wählen Sie bitte die Option "eigenständiges Netzwerk" und aktivieren Sie dort die Bündelung.

weiterer Bridge-Port

Mit dieser Option können Sie die Netzwerkkarte zu einer bereits konfigurierten Bridge hinzufügen.



Um eine neue Bridge zu erstellen, wählen Sie bitte die Option "eigenständiges Netzwerk" und aktivieren Sie dort die Bridge.

IDS Paketmonitor

Wählen Sie diesen speziellen Modus um die Netzwerkkarte durch das Intrusion-Detection-System (IDS) überwachen zu lassen. Die Netzwerkkarte muss dazu mit dem Monitor-Port eines Switches verbunden werden.



Das IDS wird in diesem Fall als passive Komponente gestartet, die auffällige Pakete lediglich protokolliert. Im aktiven Modus läuft das IDS im Rahmen der Firewall auf den Internet-Schnittstellen.

IPv4-Modus

Wählen Sie hier die Art der IPv4-Anbindung aus.



SX-GATEs primäre Netzwerk-Schnittstelle (eth0) muss stets eine statische Adresse erhalten, weswegen diese Einstellung für eth0 nicht zur Verfügung steht.

automatische IP (DHCP)

Beispielsweise bei der Internet-Anbindung über Kabel-Modem wird die IP-Adresse oft mit Hilfe des DHCP-Protokolls dynamisch zugewiesen. Wählen Sie in diesem Falle die entsprechende Option.

Dual-Stack Lite (DS-Lite)

Diese Option ist nur verfügbar, wenn IPv6 aktiviert ist und die Schnittstelle nicht als Bridge konfiguriert ist. Bei einem DS-Lite Zugang stellt der Provider eine reine IPv6-Verbindung zur Verfügung. IPv4-Pakete werden in Form eines Tunnels über die IPv6-Verbindung zu einem speziellen Gateway des Providers geleitet. Erst dort erhält das IPv4-Paket seine endgültige Absender-Adresse (Carrier-Grade NAT) und wird in das IPv4-Internet weitergeleitet.

IPv6-Modus

Wählen Sie hier die Art der IPv6-Anbindung aus.

manuelle IP

In dieser Einstellung muss die IPv6-Konfiguration manuell erfolgen. Router-Advertisements werden ignoriert.

automatische IP (SLAAC/DHCPv6)

Wählen Sie diese Einstellung, wenn SX-GATE seine IPv6-Konfiguration automatisch anhand der empfangenen Router-Advertisements vornehmen soll.

14.1.2.2-A Einstellungen

Beschreibung

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Bündelung von Netzwerkkarten

Mehrere Netzwerkkarten können gebündelt werden, um Ausfallsicherheit oder höheren Durchsatz zu erzielen.



Wenn Sie diese Einstellung aktivieren, besteht das "Bündel" zunächst nur aus einer Netzwerkkarte. Um weitere Netzwerkkarten hinzuzufügen, legen Sie diese bitte als eth-Schnittstellen an bzw. wählen Sie bereits angelegte eth-Schnittstellen aus. Ändern Sie dann die Einstellung "Schnittstellen-Modus" auf "weiterer Port für Bündelung" und ordnen Sie dort die Schnittstelle dem Bündel zu.

aktiv/passiv

In diesem Modus ist jeweils nur eine der zugeordneten Netzwerkkarten aktiv. Verliert diese den Link, wird automatisch auf eine andere Karte gewechselt.

Verbinden Sie die zugeordneten Netzwerkkarten mit verschiedenen Switches, um für Ausfallsicherheit zu sorgen. In den Switches ist keine spezielle Konfiguration oder Funktionalität erforderlich.

Dynamic Link Aggregation IEEE 802.3ad/802.1AX

Dieser Modus erhöht den Durchsatz. Er bietet nur begrenzte Ausfallsicherheit, da alle Netzwerkkarten mit dem gleichen Switch verbunden werden müssen. Erst mit einem sog. virtuellen Switch, der aus mehreren physischen Switches besteht, erhält man auch Ausfallsicherheit.



Die Verteilung der ausgehenden Pakete basiert auf den beteiligten MAC-Adressen. Der Modus ist daher nicht geeignet, wenn bevorzugt mit der selben Gegenstelle (z.B. einem Router oder Gateway) kommuniziert wird.

Verbinden Sie die zugeordneten Netzwerkkarten mit einem Switch, der Link Aggregation unterstützt. Die Ports des Switches müssen entsprechend eingestellt sein. Alle zugeordneten Netzwerkkarten müssen sich mit der gleichen Geschwindigkeit verbinden und im Full-Duplex-Modus sein.

Loadbalancing nach MAC

Diese Einstellung entspricht weitestgehend der vorherigen Variante. Die Einschränkung, dass alle Netzwerkkarten mit der selben Geschwindigkeit arbeiten müssen, besteht hier jedoch nicht. Beachten Sie bitte, dass im Switch die beteiligten Ports gruppiert werden müssen. Die Hersteller nutzen dazu verschiedene Bezeichnungen (z.B. EtherChannel oder Trunking).

Loadbalancing pro Paket

Ausgehende Pakete werden reihum über die verfügbaren Schnittstellen versendet. Damit ist dieser Modus der einzige, bei dem schon eine einzige Verbindung über mehrere Netzwerkkarten verteilt wird und so von der Bündelung profitieren kann.

Nutzen Sie diese Variante, wenn bevorzugt mit einer bestimmten Gegenstelle (z.B. Router oder Gateway) kommuniziert wird und die Anbindung entweder direkt (ohne Switch) oder über parallele, unabhängige Switches erfolgt. Die Gegenstelle muss dies unterstützen und entsprechend konfiguriert sein. Sie erhalten höheren Durchsatz und Ausfallsicherheit.

Sie können diese Variante auch nutzen, wenn Sie die beteiligten Netzwerkkarten mit einer Portgruppe (EtherChannel, Trunk) eines Switches verbinden. Sie müssen dann aber damit rechnen, dass Pakete häufig in geänderter Reihenfolge beim Ziel ankommen, was speziell bei TCP zu Wiederholungen bei der Übertragung führen wird. Ausfallsicherheit ist in diesem Fall aufgrund der Anbindung an einen einzigen Switch nur begrenzt gegeben.

Zuordnen zu Schnittstellen-Bündel

Wählen Sie hier das Schnittstellen-Bündel aus, zu dem Sie die Schnittstelle hinzufügen wollen.

Bridge

Ähnlich wie ein Switch, verbindet eine Bridge mehrere Netzwerk-Segmente zu einem großen Netzwerk. Im SX-GATE besteht dabei die Möglichkeit, den Datenaustausch mit Hilfe von Firewall-Regeln zu filtern. So ist es z.B. auch möglich, SX-GATE als transparente Firewall zwischen dem LAN und einem Internet-Router zu betreiben.



Es ist nicht möglich, auf einer Bridge-Schnittstelle DS-Lite zu konfigurieren.

Beachten Sie bitte, dass bei Verbindungen, die von außerhalb der Bridge in die Bridge hinein geroutet werden, zum Zeitpunkt der Filterung in der Firewall noch nicht bekannt ist, über welchen Bridge-Port die Verbindung anschließend gesendet wird. Entsprechend sind in der Firewall Weiterleitungs-Regeln, Regeln für ausgehende Verbindungen (Quelle ist ein SX-GATE-Dienst) und SNAT-Regeln stets für die Bridge

als ganzes und damit portunabhängig zu konfigurieren. Auch eine eigene Ziel-Zone muss für die Bridge als ganzes eingestellt werden.

Im Gegensatz dazu werden Regeln für Verbindungen innerhalb der Bridge, also Verbindungen die von einem Bridge-Port an einen anderen Bridge-Port weitergeleitet werden, je Bridge-Port konfiguriert. Das selbe gilt für DNAT-Regeln und Regeln für eingehende Verbindungen (Ziel ist ein SX-GATE-Dienst). Die Firewall-Zone lässt sich für jeden Bridge-Port individuell festlegen. Als Quell-Zone steht diese auch außerhalb der Bridge zur Verfügung, wenn eine Verbindung aus der Bridge heraus in eine Schnittstelle außerhalb der Bridge geroutet wird.

Spanning-Tree-Protokoll

Wenn Sie mehrere Switches und Bridges so miteinander verbunden haben, dass es alternative Kommunikationswege zwischen den Geräten gibt, müssen Sie das Spanning-Tree-Protokoll (STP) auf allen beteiligten Switches und Bridges aktivieren. Über das Protokoll stellen die Gerät sicher, dass die Netzwerk-Topologie zyklensfrei bleibt, reagieren aber auch auf Ausfälle.

Bekannte Ziele routen

Wenn dieser Schalter aktiviert wird, werden bestimmte Pakete nicht durch die Bridge sondern über das Routing des SX-GATES weitergeleitet. Das betrifft Pakete an Ziel-Adressen, die im SX-GATE auf anderen Schnittstellen oder in VPNs konfiguriert sind bzw. zu denen eine statische Route konfiguriert wurde.



Diese Einstellung ist nur dann sinnvoll, wenn sich der SX-GATE als transparente Firewall zwischen Client-Systemen und einem Router befindet, der in den Client-Systemen als Standard-Gateway konfiguriert ist.



Firewall-Regeln für diese Verbindungen müssen im Untermenü "Regeln" und nicht im Untermenü "Bridge" konfiguriert werden.

Zuordnen zu Bridge

Wählen Sie hier die Bridge aus, mit der Sie die Netzwerkkarte verbinden wollen.

Netzwerkkarten-Parameter

Bei Problemen mit der automatischen Erkennung der erforderlichen Netzwerkkarten-Parameter können Sie hier auf die manuelle Konfiguration umschalten.



Nicht alle Netzwerkkarten unterstützen die manuelle Konfiguration.

Geschwindigkeit

Legen Sie hier die von der Netzwerkkarte zu verwendenden Geschwindigkeit fest.

Duplex

Wählen Sie hier bitte den gewünschten Duplex-Modus.

14.1.2.2-B IP-Adressen

IPv4-Adresse

Geben Sie hier die IPv4-Adresse ein, die SX-GATE auf dieser Schnittstelle erhalten soll. Bei der Schnittstelle eth0 lässt sich dieser Wert nur mit Hilfe des Menüpunktes "System > Grundeinstellungen" verändern.



Die hier angegebene IP-Adresse darf nicht zu einem IP-Adress-Bereich gehören, der bereits auf einer anderen Schnittstelle konfiguriert ist.

IPv4-Netzmaske

Geben Sie hier die Netzmaske ein, die zu der angegebenen IP-Adresse gehört.

IPv4-Standard-Gateway

Vereinfacht ausgedrückt versteht man unter einem Standard Gateway einen Router, über den das Internet erreicht werden kann. Ist ein solcher Router an dieser Schnittstelle angeschlossen, so tragen Sie bitte hier dessen IP-Adresse ein. Im Menü "Module > Netzwerk > Einstellungen" wird ausgewählt, über welche Schnittstelle tatsächlich der Internet-Zugang erfolgt. Wird dort diese Schnittstelle ausgewählt, so installiert SX-GATE eine Default-Route über das hier eingetragene Gateway.

zusätzliche IPv4-Adressen (Aliase) bzw. Cluster-IP-Adressen

Nutzen Sie diesen Bereich, um weitere IP-Adressen an diese Netzwerkkarte zu binden. Es kann sich hierbei um Adressen aus dem gleichen Netzwerk handeln, aus dem auch die primäre IP-Adresse stammt. Nutzen Sie dies, um z.B. mehrere Internet-Adressen auf die Internet-Schnittstelle zu binden und anschließend mit Hilfe von Firewall-Regeln die Zugriffe auf verschiedene interne Adressen weiterzuleiten. Möglich ist aber auch die Vergabe von Adressen aus anderen Netzwerken, wenn im selben physikalischen Ethernet-Segment mehrere IP-Netzwerke konfiguriert sind.

DS-Lite Address-Family-Transition-Router (AFTR)

Bei Internetzugängen über Dual-Stack Lite werden IPv4-Pakete über IPv6 getunnelt. Der Tunnel terminiert auf Seiten des Providers an einem speziellen Router. Sofern dessen Adresse nicht über DHCP automatisch bezogen werden kann, müssen Sie die Adresse hier angeben.

IPv6-Adresse

Geben Sie hier die IPv6-Adresse für die Schnittstelle ein. Falls diese Adresse auf einem dynamisch zugewiesenen Präfix basieren soll, legen Sie bitte im Menü "Definitionen > IP-Objekte" einen Eintrag vom Typ "IPv6-Adresse" an, der auf den entsprechenden Präfix verweist.

IPv6-Präfixlänge

Bei der IPv6-Präfixlänge handelt es sich um das Pendant zur IPv4-Netzmaske. Die typische Präfixlänge ist 64.



Bei Präfixlängen größer als 64 funktionieren bestimmte IPv6-Verfahren wie z.B. SLAAC nicht mehr. Verwenden Sie größere Präfixe nur, wenn Ihnen die Auswirkungen bekannt sind.

IPv6-Standard-Gateway

Falls an der aktuellen Schnittstelle ein Router angeschlossen ist, über den das Internet erreicht werden kann, können Sie hier dessen IP-Adresse angeben.



Es kann sowohl eine globale Adresse als auch eine Link-Local-Adresse (fe80:...) angegeben werden.

IPv6-Privacy-Extension (RFC3041)

Eine dynamisch per SLAAC ermittelte IPv6-Adresse basiert auf der Hardware-Adresse der zugehörigen Netzwerkkarte und kann daher global eindeutig verfolgt werden. Wenn Sie diese Option aktivieren, ermittelt SX-GATE zusätzlich eine zufällige temporäre Adresse, die bevorzugt verwendet wird.

IPv6-Präfixdelegation anfordern

Aktivieren Sie diesen Schalter um sich vom Provider einen Block IPv6-Netzwerke per DHCP zuweisen zu lassen. Diese Netze können dann vom SX-GATE an lokale Netze weiterverteilt werden.

Für den vom Provider zugewiesenen Adressblock wird im Menü "Definitionen > IP-Objekte" automatisch ein Eintrag erstellt (für die Schnittstelle "eth1" lautet dieser

"ipv6_prefix_eth1"). Legen Sie dort Einträge vom Typ "IPv6-Präfix" oder "IPv6-Adresse" an, die sich auf den zugewiesenen Präfix beziehen und ihn weiter unterteilen. Die so definierten Objekte können Sie dann in zahlreichen Konfigurations-Optionen verwenden.

zusätzliche IPv6-Adressen (Aliase) bzw. Cluster-IP-Adressen

Nutzen Sie diesen Bereich, um weitere IPv6-Adressen an diese Netzwerkkarte zu binden. Es kann sich hierbei um Adressen aus dem gleichen Netzwerk handeln, aus dem auch die primäre IP-Adresse stammt oder auch andere IP-Adressen (z.B. ULA-Adressen).

14.1.2.2-C IPv6 Router-Advertisement

Router-Advertisement (RA) dient der automatischen IPv6-Konfiguration von Endgeräten. Router mit Internetanbindung geben den Endgeräten auf diese Weise ihre IP-Adresse bekannt. Auch die Präfixlänge des lokalen Netzwerks wird über RA bekanntgegeben.



Selbst wenn DHCPv6 für die Adressvergabe zum Einsatz kommt, ist RA unverzichtbar. Weder die Router-Adresse noch die Präfixlänge können über DHCPv6 zugewiesen werden.

Router-Advertisement

per Unicast an einzelne Clients

Wenn Sie IPv6 nicht im ganzen Netzwerk ausrollen wollen, können Sie mit Hilfe dieser Einstellung Router-Advertisements gezielt an eine Liste manuell konfigurierter Clients schicken.

aktiviert

Wählen Sie diese Einstellung um per Multicast alle Endgeräte über die Verfügbarkeit von IPv6 zu informieren.

Router Priorität

Über diesen Schalter kann beeinflusst werden, für welchen Router sich ein Endgerät entscheidet, wenn mehrere Router zur Auswahl stehen.



Manche Endgeräte werten diese Option nicht aus oder müssen erst entsprechend konfiguriert werden.

Router Advertisements senden an

Sofern Sie sich dazu entschieden haben, Router-Advertisements nur per Unicast an einzelne Clients zu senden, müssen Sie die Link-Local Adressen der Clients hier angeben. Link-Local Adressen beginnen stets mit "fe80:".

Präfixe für zustandslose Adressvergabe (SLAAC)

Sofern sich die Endgeräte selbständig eine IPv6-Adresse konfigurieren sollen, geben Sie hier bitte die gewünschten Präfixe an.

Der Präfix kann auf einem vom Provider dynamisch zugewiesenen Präfix basieren. Beim Hinzufügen eines neuen Eintrags werden Ihnen die im Menü "Definitionen > IP-Objekte" angelegten Präfixe zur Auswahl angeboten. Sie können im besagten Menü auch selbst Einträge vom Typ "IPv6-Präfix" anlegen, um z.B. den vom Provider erhaltenen Präfix weiter zu unterteilen.

DHCPv6

Mithilfe dieses Schalters teilen Sie den Endgeräte mit, inwiefern ein DHCPv6-Server im Netzwerk verfügbar ist.

keine IP-Vergabe, nur Zusatzinformationen (O-Flag)

In dieser Einstellung können Endgeräte lediglich Informationen wie z.B. die Adresse des DNS-Servers via DHCP beziehen.

ja (M-Flag und O-Flag)

Soll den Endgeräten eine IPv6-Adresse per DHCPv6 zugewiesen werden, müssen Sie diese Einstellung wählen.

DNS 1 (RDNSS)

Name-Server Adressen können über die RA-Erweiterung RDNSS zugewiesen werden. Da diese Option jedoch von vielen Geräten nicht unterstützt wird, sollten Sie die DNS-Adressen zumindest parallel auch über DHCPv6 verteilen.

DNS-Suffix (DNSSL)

Auch ein DNS-Suffix für die Namensauflösung von Host-Namen ohne Domain-Angabe kann über RA verteilt werden. Auch diese Erweiterung wird jedoch von vielen Endgeräten noch nicht unterstützt.

Veröffentlichte Routen

Über Router-Advertisements können gezielt Routen zu einzelnen IPv6-Präfixen verteilt werden.



Manche Endgeräte werten diese Option nicht aus oder müssen erst entsprechend konfiguriert werden.

14.1.2.2-D Routing

Erweitertes Routing

Auf diesem Reiter können statische Routen konfiguriert werden. Neben herkömmlichen Routen, bei denen lediglich die Ziel-Adresse bei der Routing-Entscheidung berücksichtigt wird, können auch erweiterte Routen erstellt werden. Dabei lassen sich die Quell-Adresse sowie Protokoll- und Port-Nummern auswerten (Policy-based Routing).

Statische Routen müssen für Netzwerke spezifiziert werden, die nicht direkt an der Netzwerk-Karte anliegen, sondern die sich hinter einem Router befinden. Das Zielnetzwerk wird über die Netzwerkadresse und die zugehörige Netzmaske spezifiziert, womit das Netzwerk automatisch auch der SX-GATE Firewall bekannt gemacht wird. Als Gateway ist die IP-Adresse des Routers anzugeben.



Die IP-Adresse des Gateways muss stets dem selben IP-Netzwerk angehören, dem auch SX-GATE angehört. Netzwerkadresse und Netzmaske des Zielnetzes müssen hingegen ein anderes IP-Netzwerk adressieren.



Geben Sie als Gateway-Adresse bitte 0.0.0.0 an, falls dessen IP-Adresse dynamisch von einem DHCP-Server bezogen wird.

Regeln für spezielle Protokolle oder Quell-Adressen bieten sich an, wenn mehrere Internet-Anbindungen zur Verfügung stehen. So ließe sich z.B. das Surfen im Internet über eine ADSL-Verbindung leiten, während die übrige Kommunikation wie Mail oder VPN über eine SDSL-Leitung läuft.

Die Priorität der einzelnen Routen ergibt sich nicht aus der Reihenfolge in der sie eingetragen werden. Entscheidend ist vielmehr, wie spezifisch die Routen sind. Schnittstellenübergreifend haben Routen, bei denen Protokoll, Quelle und Ziel angegeben sind, die höchste Priorität. Regeln mit Ziel haben Vorrang vor Regeln mit Protokoll, diese wiederum vor Regeln mit Angabe einer Quelle. Innerhalb von Quelle und Ziel erfolgt die Sortierung nach absteigender Netzmaske. Die Reihenfolge bei Überschneidungen im Protokoll ist nicht definiert.

14.1.2.2-E Bandbreitenmanagement / QoS

Für das Bandbreiten-Management müssen Sie die Bandbreite der Anbindung festlegen. Die eingehende und ausgehende Bandbreite kann dabei unterschiedlich sein (ADSL). Solange Sie keine Bandbreite festlegen, ist das Bandbreitenmanagement auf dieser Schnittstelle deaktiviert. Wenn Sie lediglich die ein- oder die ausgehende Bandbreite eintragen, ist das Bandbreitenmanagement auch nur in dieser Richtung aktiv.



Die Angabe einer falschen Bandbreite kann zu Problemen führen. Dies gilt insbesondere, wenn die eingestellte Bandbreite höher ist als die tatsächlich verfügbare. Fragen Sie im Zweifel Ihren Provider.

Bandbreite ausgehend (Uplink)

Geben Sie hier die ausgehende Bandbreite (Uplink) an. Bei asymmetrischen Anbindungen ist dies in der Regel der kleinere Wert. Es werden dann alle über diese Schnittstelle ausgehenden Datenpakete vom Bandbreitenmanagement verarbeitet. Die Verbindungsrichtung (eingehende oder ausgehende Verbindung) spielt dabei keine Rolle.

Bandbreite eingehend (Downlink)

Geben Sie hier die eingehende Bandbreite (Downlink) an. Bei asymmetrischen Anbindungen ist dies in der Regel der größere Wert. Es werden dann alle über diese Schnittstelle eingehenden Datenpakete vom Bandbreitenmanagement verarbeitet. Die Verbindungsrichtung (eingehende oder ausgehende Verbindung) spielt dabei keine Rolle. Lassen Sie das Feld leer, wenn Sie kein eingehendes Bandbreitenmanagement wünschen.

Eingehendes Bandbreitenmanagement ist eigentlich ein Widerspruch in sich. Das Umsortieren von auf die Übertragung wartenden Datenpaketen nach Priorität müsste eigentlich auf der anderen Seite der (Internet-)Verbindung vorgenommen werden, denn nur dort ist dies zuverlässig möglich. Beim eingehenden Bandbreitenmanagement sind die Pakete ja bereits übertragen worden. Internet-Anbindungen mit providerseitigem Quality-of-Service/Bandbreitenmanagement sind jedoch oft sehr teuer, so dass eingehendes Bandbreitenmanagement trotz seiner Einschränkungen gewünscht wird.



Eingehendes Bandbreitenmanagement reduziert die verfügbare Bandbreite um bis zu 20%. Es funktioniert nur, solange das eingehende Datenvolumen zu einem ausreichend hohen Anteil über TCP-Verbindungen abgewickelt werden.

Quality-of-Service (QoS) für Voice-over-IP (VoIP)

Bei VoIP spielt die Latenzzeit, also die Zeitspanne die ein Sprachdatenpaket vom Absender zum Empfänger benötigt, eine große Rolle. Das Bandbreitenmanagement des SX-GATE optimiert den Versand von VoIP-Paketen daher mit Hilfe eines speziellen Quality-of-Service Moduls.



Um als VoIP-Paket erkannt zu werden, muss ein IP-Paket gemäß Diffserv-Code-Point Expedited-Forwarding (DSCP EF) markiert sein.

Die Bandbreite eines einzelnen Gesprächs ist abhängig vom jeweils verwendeten Codec. Der Codec bestimmt dabei, wie stark das Gespräch komprimiert wird. Je stärker der Codec das Gespräch komprimiert, desto weniger Bandbreite wird benötigt. Im Gegenzug sinkt jedoch die Qualität des Gesprächs mit der Zunahme der Kompression. Die folgende Tabelle gibt die Nettobandbreite typischer Codecs an. Bei Codecs die mit verschiedenen Bandbreiten genutzt werden, ist jeweils die maximale Bandbreite angegeben.

Codec	max. Bandbreite (bit/s)
G.711	64000
G.722	64000
G.722.1	32000
G.723.1	6400
G.726	40000
G.728	16000
G.729	8000
GSM	13000
iLBC	15200

Max. Anzahl gleichzeitiger Gespräche

Geben Sie die maximal erwartete Anzahl gleichzeitiger unverschlüsselter Gespräche an, die über diese Schnittstelle abgewickelt werden. Die Anzahl der Gespräche dient als Grundlage für die Berechnung der insgesamt für VoIP zu reservierenden Bandbreite. Der Wert "0" deaktiviert die Priorisierung.



Die Insgesamt zur Verfügung stehende Bandbreite der Anbindung darf nicht überschritten werden.

Bitrate des verwendeten Codecs

Geben Sie die Nettobandbreite des verwendeten Codecs an. Bei Verwendung unterschiedlicher Codecs orientieren Sie sich bitte am Codec mit dem größten Bandbreitenbedarf.



Zur Berechnung der insgesamt benötigten Bandbreite wird vom System automatisch der IP-Overhead eingerechnet. Dieser ist umso größer, je kleiner die Bitrate des Codecs ist.

Max. Anzahl Gespräche über IPSec

Geben Sie die maximal erwartete Anzahl gleichzeitiger Gespräche über IPSec-VPN an, die über diese Schnittstelle abgewickelt werden. Die Anzahl der Gespräche dient als Grundlage für die Berechnung der insgesamt für VoIP zu reservierenden Bandbreite. Der Wert "0" deaktiviert die Priorisierung.



Wenn aktiviert, werden VoIP-Datenpakete gegenüber anderem VPN-Datenverkehr bevorzugt. Selbiges gilt nach der Verschlüsselung für die entstandenen VPN-Pakete.



Die Insgesamt zur Verfügung stehende Bandbreite der Anbindung darf nicht überschritten werden.

Bitrate des Codecs im IPSec

Geben Sie die Nettobandbreite des verwendeten Codecs an. Bei Verwendung unterschiedlicher Codecs orientieren Sie sich bitte am Codec mit dem größten Bandbreitenbedarf.



Zur Berechnung der insgesamt benötigten Bandbreite wird vom System automatisch der IP- und der IPSec-Overhead eingerechnet. Dieser ist umso größer, je kleiner die Bitrate des Codecs ist.

14.1.2.2-F Priorisierung

Mit Hilfe dieser Funktion können Datenpakete auf verschiedene Prioritätsklassen aufgeteilt werden. Jeder Klasse ist eine anteilige Mindestbandbreite zugeordnet. Nicht benötigte Bandbreite einer höherpriorien Klasse steht den nachfolgenden Klassen zur Verfügung.

Aus technischer Sicht wird durch die Regeln das ToS- bzw. DSCP-Feld von IP-Paketen überschrieben. Setzt eine lokale Anwendung bereits das ToS/DSCP-Feld passend, ist keine Regel für ausgehende Pakete notwendig. Bei eingehenden Paketen wird das ToS/DSCP-Feld häufig auf dem Weg durch das Internet verändert, so dass für das eingehende Bandbreitenmanagement üblicherweise Regeln erforderlich sind.



Manche Provider stellen Datenpakete mit gesetztem ToS/DSCP-Feld in Rechnung. Bitte prüfen Sie Ihre Vertragsbedingungen.

Die Mindestbandbreiten werden wie folgt verteilt: Die für VoIP benötigte Bandbreite gemäß Konfiguration wird reserviert und von der insgesamt verfügbaren Bandbreite abgezogen. Von der verbliebenen Bandbreite entfallen 10% auf leere TCP ACK-Pakete, 50% auf hochpriorie Datenpakete und je 20% auf Pakete mit normaler oder niedriger Priorität.



Für das eingehende Bandbreitenmanagement werden nicht-TCP Pakete grundsätzlich wie hochpriorie Datenpakete behandelt.

Priorisierung von Verbindungen

Fügen Sie dieser Liste die Signaturen der Datenpakete hinzu, die eine höhere oder niedriger Priorität erhalten sollen. Treffen mehrere Regeln auf ein Datenpaket zu, so wird die Priorität des ersten passenden Eintrags angewendet.

Die einzelnen Eingabefelder haben dabei folgende Bedeutungen:

Protokoll

Legt die IP-Protokoll und Port-Signatur fest. Bei eingehendem Bandbreitenmanagement werden ausschließlich TCP-Protokolle berücksichtigt.



Protokoll-Definitionen werden im Menü "Definitionen > Protokolle" vorgenommen.

Lokale IP/Netzwerk

Auf dieser Seite steht die aus Sicht der gewählten Schnittstelle lokale Adresse. Bei einem ausgehenden Datenpaket entspricht dies der Quell-IP (vor SNAT), bei einem eingehenden Datenpaket der Ziel-IP (vor DNAT).



Wenn Sie die Priorisierung bei DNAT- oder SNAT-Verbindungen auf bestimmte lokale IPs beschränken wollen, sind üblicherweise zwei Regeln erforderlich um beide Verbindungsrichtungen abzudecken: Für eingehende Datenpakete muss eine SX-GATE IP angegeben werden, für ausgehende Datenpakete die interne IP (des LAN-Clients bzw. des per DNAT angesprochenen Servers).

Richtung

Wählen Sie hier bitte aus, in welcher Richtung die Portsignatur des gewählten Protokolls interpretiert wird. Erläutert am Beispiel HTTP bedeutet der Richtungspfeil "-->", der HTTP-Port 80 befindet sich auf der externen Seite. Das ausgehende Bandbreitenmanagement verarbeitet folglich Pakete zu Port 80, das eingehende von Port 80. Wird der entgegengesetzt orientierte Pfeil "<--" gewählt, werden eingehende HTTP-Verbindungen verarbeitet. Pakete zu Port 80 durchlaufen das eingehende Bandbreitenmanagement, Pakete von Port 80 das ausgehende. Der Doppelpfeil "<=>" steht für beide Interpretationsrichtungen.

Externe IP/Netzwerk

Auf dieser Seite steht die aus Sicht der gewählten Schnittstelle externe Adresse. Bei einem ausgehenden Datenpaket entspricht dies der Ziel-IP, bei einem eingehenden Datenpaket der Quell-IP.

Priorität

Wählen Sie hier die gewünschte Priorisierung aus.

14.1.2.2-G Dynamischer DNS

Dynamischer DNS ermöglicht es, ein Gerät, das eigentlich mit einer dynamischen IP-Adresse an das Internet angebunden ist, unter dessen jeweils aktueller Adresse aufzufinden. Mit Hilfe dieses Dienstes kann also vom Internet aus auf SX-GATE zugegriffen werden, obwohl dieser nur über eine dynamische IP-Adresse verfügt.

Die Adressierung im dynamischen DNS erfolgt mit Hilfe eines üblichen DNS-Rechnernamens (Fully-Qualified-Domain-Name, FQDN). Es gibt eine Reihe von Anbietern, die dynamischen DNS sowohl als kostenlose als auch als kostenpflichtige Dienstleistung zur Verfügung stellen.



Nach einem IP-Wechsel vergehen einige Sekunden bis Minuten, bis der DNS-Name auch tatsächlich auf die neue IP-Adresse verweist.

Sofern SX-GATE selbst die dynamische IP erhält (ADSL-Schnittstelle mit dynamischer IP oder Ethernet-Schnittstelle mit IP-Vergabe über DHCP), konfigurieren Sie dynamischen DNS bitte in der jeweiligen Schnittstelle im Menü "Module > Netzwerk > Schnittstellen". SX-GATE aktualisiert seine IP-Adresse im dynamischen DNS dann einmalig bei jedem Verbindungsaufbau bzw. IP-Wechsel.

Für den Fall, dass sich SX-GATE hinter einem NAT-Router befindet und dieser die dynamische IP erhält, muss der NAT-Router eingehende Verbindungen an SX-GATE weiterreichen können (DNAT, Portforwarding, Exposed Host). Optimalerweise konfigurieren Sie dynamischen DNS im NAT-Router, da nur dieser die aktuelle dynamische IP kennt. Ist dies nicht möglich, konfigurieren Sie dynamischen DNS bitte hilfsweise im SX-GATE Menü "Module > DNS > Einstellungen". SX-GATE versucht dann in regelmäßigen Abständen die dynamische IP des NAT-Routers mit Hilfe eines Internet-Dienstes zu ermitteln.

Protokoll

Für die Aktualisierung der Einträge im dynamischen DNS gibt es leider keinen einheitlichen Standard. SX-GATE unterstützt jedoch eine ganze Reihe von Protokollen für diese Aktualisierung. Bitte klären Sie zunächst mit dem Anbieter des dynamischen DNS-Dienstes, welches Protokoll verwendet wird und ob dieses vom SX-GATE unterstützt wird.

Update-Server des Anbieters

Tragen Sie hier bitte den Namen des Servers ein, der die Nachrichten zur Aktualisierung der dynamischen IP-Adresse entgegen nimmt. Dieser Server ist nicht immer identisch mit dem Webserver des Anbieters.

Update-URL

Tragen Sie hier bitte die Update-URL (auch "Direct URL" genannt) zur Aktualisierung der dynamischen IP-Adresse ein. Die URL kann die Platzhalter <host>, <ipaddr>, <username> und <password> enthalten, die durch den dynamischen DNS-Namen, die IP-Adresse, den Benutzernamen und das Passwort ersetzt werden. Beispiel: `http://dynupdate.exampledyndns.com/nic/update?hostname=<domain>&myip=<ipaddr>`

Dynamischer DNS-Name des SX-GATES

Über ein Benutzerkonto bei dem jeweiligen Anbieter lassen sich in der Regel mehrere DNS-Namen verwalten. Daher ist hier der vollständige Name (inkl. Domain) anzugeben, unter dem SX-GATE im dynamischen DNS erreichbar ist.

Benutzername

Keine Aktualisierung des Eintrags im dynamischen DNS ohne entsprechende Anmeldung. Geben Sie hier den Benutzernamen (login) für das Konto an.

Passwort

Geben Sie hier schließlich das entsprechende Kennwort für die Aktualisierung an.

Jetzt aktualisieren

ref link="#main_modules#sm_devices#tr_dyndns_checkdd"/>

14.1.2.2-H Paket Monitor***Lokale Netze***

Für IDS-Regeln die zwischen internen und externen Netzwerken unterscheiden, wird hier festgelegt, welche Adressen zu internen Systemen gehören.

14.1.2.2-I Server Adressen

Manche IDS-Regeln sind auf spezielle Server-Dienste ausgerichtet. Geben Sie hier die IP-Adressen an, auf denen entsprechende Server-Dienste zur Verfügung gestellt werden. Sind keine Adressen angegeben, wird davon ausgegangen, dass der Dienst auf allen internen Adressen zur Verfügung steht, was sich nachteilig auf die Leistung des Systems auswirkt.

14.1.2.2-J Optionale Regeln

Einige wichtigen Regelsätze sind grundsätzlich aktiv. Die zusätzlichen Regelsätze auf diesem Reiter lassen sich bei Bedarf zuschalten.

Angriffe gegen Web-Server

Aktiviert Regeln, die speziell auf Angriffe gegen Web- und FTP-Server ausgerichtet sind.

Angriffe gegen Mail-Server

Aktiviert Regeln, die speziell auf Angriffe gegen SMTP-, IMAP4- und POP3-Server ausgerichtet sind.

Angriffe gegen Internet-Server

Aktiviert Regeln die speziell auf Angriffe gegen sonstige Internet-Dienste wie z.B. DNS oder SIP (VoIP) ausgerichtet sind.

Angriffe gegen LAN-Server

Aktiviert Regeln zu Angriffen gegen Dienste die eher in LANs anzutreffen sind. Dazu gehören u.a. Windows-Dienste, Unix-RPC und SQL-Server.



Die meisten Regeln sprechen nur an, wenn der Zugriff von außerhalb erfolgt.

Erweiterte Browser Überwachung

Dieser Regelsatz überwacht Browser auf Angriffe und veraltete Software-Komponenten.

Betriebsfremde Tätigkeiten

Ergänzt Regeln zur Protokollierung von Aktivitäten, die in der Regel nichts mit normalen Geschäftstätigkeiten in einer Firma zu tun haben. Dies beinhaltet insbesondere Online-Spiele, Chat oder die Nutzung von Peer-to-Peer Software.

Verbindungen mit dem Tor-Netzwerk

Dieser Schalter aktiviert eine Liste von IP-Adressen, die dem Tor-Netzwerk zur Anonymisierung von Zugriffen zugerechnet werden.

14.1.2.3 VLAN 802.1Q (vlan)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.3-A Einstellungen.....	326
14.1.2.3-B IP-Adressen.....	327
14.1.2.3-C IPv6 Router-Advertisement.....	329
14.1.2.3-D Routing.....	331
14.1.2.3-E Bandbreitenmanagement / QoS.....	332
14.1.2.3-F Priorisierung.....	335
14.1.2.3-G Dynamischer DNS.....	337

Schnittstellen-Modus

Legen Sie hier fest, wie die VLAN-Schnittstelle genutzt werden soll.

eigenständiges VLAN

In diesem Modus erhält die VLAN-Schnittstelle eine eigene IP-Konfiguration.

weiterer Bridge-Port

Mit dieser Option können Sie die VLAN-Schnittstelle zu einer bereits konfigurierten Bridge hinzufügen.



Um eine neue Bridge zu erstellen, wählen Sie bitte die Option "eigenständiges VLAN" und aktivieren Sie dort die Bridge.

IPv4-Modus

Wählen Sie hier die Art der IPv4-Anbindung aus.

automatische IP (DHCP)

Beispielsweise bei der Internet-Anbindung über Kabel-Modem wird die IP-Adresse oft mit Hilfe des DHCP-Protokolls dynamisch zugewiesen. Wählen Sie in diesem Falle die entsprechende Option.

Dual-Stack Lite (DS-Lite)

Diese Option ist nur verfügbar, wenn IPv6 aktiviert ist und die Schnittstelle nicht als Bridge konfiguriert ist. Bei einem DS-Lite Zugang stellt der Provider eine reine IPv6-Verbindung zur Verfügung. IPv4-Pakete werden in Form eines Tunnels über

die IPv6-Verbindung zu einem speziellen Gateway des Providers geleitet. Erst dort erhält das IPv4-Paket seine endgültige Absender-Adresse (Carrier-Grade NAT) und wird in das IPv4-Internet weitergeleitet.

IPv6-Modus

Wählen Sie hier die Art der IPv6-Anbindung aus.

manuelle IP

In dieser Einstellung muss die IPv6-Konfiguration manuell erfolgen. Router-Advertisements werden ignoriert.

automatische IP (SLAAC/DHCPv6)

Wählen Sie diese Einstellung, wenn SX-GATE seine IPv6-Konfiguration automatisch anhand der empfangenen Router-Advertisements vornehmen soll.

14.1.2.3-A Einstellungen

Beschreibung

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Verwendete Netzwerkkarte

Wählen Sie hier den Namen der Netzwerkkarte aus, auf die die VLAN Schnittstelle gebunden werden soll.

Bridge

Ähnlich wie ein Switch, verbindet eine Bridge mehrere Netzwerk-Segmente zu einem großen Netzwerk. Im SX-GATE besteht dabei die Möglichkeit, den Datenaustausch mit Hilfe von Firewall-Regeln zu filtern. So ist es z.B. auch möglich, SX-GATE als transparente Firewall zwischen dem LAN und einem Internet-Router zu betreiben.

Beachten Sie bitte, dass bei Verbindungen, die von außerhalb der Bridge in die Bridge hinein geroutet werden, zum Zeitpunkt der Filterung in der Firewall noch nicht bekannt ist, über welchen Bridge-Port die Verbindung anschließend gesendet wird. Entsprechend sind in der Firewall Weiterleitungs-Regeln, Regeln für ausgehende Verbindungen (Quelle ist ein SX-GATE-Dienst) und SNAT-Regeln stets für die Bridge als ganzes und damit portunabhängig zu konfigurieren. Auch eine eigene Ziel-Zone muss für die Bridge als ganzes eingestellt werden.

Im Gegensatz dazu werden Regeln für Verbindungen innerhalb der Bridge, also Verbindungen die von einem Bridge-Port an einen anderen Bridge-Port weitergeleitet werden, je Bridge-Port konfiguriert. Das selbe gilt für DNAT-Regeln und Regeln für eingehende Verbindungen (Ziel ist ein SX-GATE-Dienst). Die Firewall-Zone lässt sich für jeden Bridge-Port individuell festlegen. Als Quell-Zone steht diese auch außerhalb der Bridge zur Verfügung, wenn eine Verbindung aus der Bridge heraus in eine Schnittstelle außerhalb der Bridge geroutet wird.

Spanning-Tree-Protokoll

Wenn Sie mehrere Switches und Bridges so miteinander verbunden haben, dass es alternative Kommunikationswege zwischen den Geräten gibt, müssen Sie das Spanning-Tree-Protokoll (STP) auf allen beteiligten Switches und Bridges aktivieren. Über das Protokoll stellen die Gerät sicher, dass die Netzwerk-Topologie zyklenfrei bleibt, reagieren aber auch auf Ausfälle.

Bekannte Ziele routen

Wenn dieser Schalter aktiviert wird, werden bestimmte Pakete nicht durch die Bridge sondern über das Routing des SX-GATES weitergeleitet. Das betrifft Pakete an Ziel-Adressen, die im SX-GATE auf anderen Schnittstellen oder in VPNs konfiguriert sind bzw. zu denen eine statische Route konfiguriert wurde.



Diese Einstellung ist nur dann sinnvoll, wenn sich der SX-GATE als transparente Firewall zwischen Client-Systemen und einem Router befindet, der in den Client-Systemen als Standard-Gateway konfiguriert ist.



Firewall-Regeln für diese Verbindungen müssen im Untermenü "Regeln" und nicht im Untermenü "Bridge" konfiguriert werden.

Zuordnen zu Bridge

Wählen Sie hier die Bridge aus, mit der Sie die VLAN-Schnittstelle verbinden wollen.

14.1.2.3-B IP-Adressen

IPv4-Adresse

Geben Sie hier die IPv4-Adresse ein, die SX-GATE auf dieser Schnittstelle erhalten soll.



Die hier angegebene IP-Adresse darf nicht zu einem IP-Adress-Bereich gehören, der bereits auf einer anderen Schnittstelle konfiguriert ist.

IPv4-Netzmaske

Geben Sie hier die Netzmaske ein, die zu der angegebenen IP-Adresse gehört.

IPv4-Standard-Gateway

Vereinfacht ausgedrückt versteht man unter einem Standard Gateway einen Router, über den das Internet erreicht werden kann. Ist ein solcher Router an dieser Schnittstelle angeschlossen, so tragen Sie bitte hier dessen IP-Adresse ein. Im Menü "Module > Netzwerk > Einstellungen" wird ausgewählt, über welche Schnittstelle tatsächlich der Internet-Zugang erfolgt. Wird dort diese Schnittstelle ausgewählt, so installiert SX-GATE eine Default-Route über das hier eingetragene Gateway.

zusätzliche IPv4-Adressen (Aliase) bzw. Cluster-IP-Adressen

Nutzen Sie diesen Bereich, um weitere IP-Adressen an diese Netzwerkkarte zu binden. Es kann sich hierbei um Adressen aus dem gleichen Netzwerk handeln, aus dem auch die primäre IP-Adresse stammt. Nutzen Sie dies, um z.B. mehrere Internet-Adressen auf die Internet-Schnittstelle zu binden und anschließend mit Hilfe von Firewall-Regeln die Zugriffe auf verschiedene interne Adressen weiterzuleiten. Möglich ist aber auch die Vergabe von Adressen aus anderen Netzwerken, wenn im selben physikalischen Ethernet-Segment mehrere IP-Netzwerke konfiguriert sind.

DS-Lite Address-Family-Transition-Router (AFTR)

Bei Internetzugängen über Dual-Stack Lite werden IPv4-Pakete über IPv6 getunnelt. Der Tunnel terminiert auf Seiten des Providers an einem speziellen Router. Sofern dessen Adresse nicht über DHCP automatisch bezogen werden kann, müssen Sie die Adresse hier angeben.

IPv6-Adresse

Geben Sie hier die IPv6-Adresse für die Schnittstelle ein. Falls diese Adresse auf einem dynamisch zugewiesenen Präfix basieren soll, legen Sie bitte im Menü "Definitionen > IP-Objekte" einen Eintrag vom Typ "IPv6-Adresse" an, der auf den entsprechenden Präfix verweist.

IPv6-Präfixlänge

Bei der IPv6-Präfixlänge handelt es sich um das Pendant zur IPv4-Netzmaske. Die typische Präfixlänge ist 64.



Bei Präfixlängen größer als 64 funktionieren bestimmte IPv6-Verfahren wie z.B. SLAAC nicht mehr. Verwenden Sie größere Präfixe nur, wenn Ihnen die Auswirkungen bekannt sind.

IPv6-Standard-Gateway

Falls an der aktuellen Schnittstelle ein Router angeschlossen ist, über den das Internet erreicht werden kann, können Sie hier dessen IP-Adresse angeben.



Es kann sowohl eine globale Adresse als auch eine Link-Local-Adresse (fe80:...) angegeben werden.

IPv6-Privacy-Extension (RFC3041)

Eine dynamisch per SLAAC ermittelte IPv6-Adresse basiert auf der Hardware-Adresse der zugehörigen Netzwerkkarte und kann daher global eindeutig verfolgt werden. Wenn Sie diese Option aktivieren, ermittelt SX-GATE zusätzlich eine zufällige temporäre Adresse, die bevorzugt verwendet wird.

IPv6-Präfixdelegation anfordern

Aktivieren Sie diesen Schalter um sich vom Provider einen Block IPv6-Netzwerke per DHCP zuweisen zu lassen. Diese Netze können dann vom SX-GATE an lokale Netze weiterverteilt werden.

Für den vom Provider zugewiesenen Adressblock wird im Menü "Definitionen > IP-Objekte" automatisch ein Eintrag erstellt (für die Schnittstelle "eth1" lautet dieser "ipv6_prefix_eth1"). Legen Sie dort Einträge vom Typ "IPv6-Präfix" oder "IPv6-Adresse" an, die sich auf den zugewiesenen Präfix beziehen und ihn weiter unterteilen. Die so definierten Objekte können Sie dann in zahlreichen Konfigurations-Optionen verwenden.

zusätzliche IPv6-Adressen (Aliase) bzw. Cluster-IP-Adressen

Nutzen Sie diesen Bereich, um weitere IPv6-Adressen an diese Netzwerkkarte zu binden. Es kann sich hierbei um Adressen aus dem gleichen Netzwerk handeln, aus dem auch die primäre IP-Adresse stammt oder auch andere IP-Adressen (z.B. ULA-Adressen).

14.1.2.3-C IPv6 Router-Advertisement

Router-Advertisement (RA) dient der automatischen IPv6-Konfiguration von Endgeräten. Router mit Internetanbindung geben den Endgeräten auf diese Weise ihre IP-Adresse bekannt. Auch die Präfixlänge des lokalen Netzwerks wird über RA bekanntgegeben.



Selbst wenn DHCPv6 für die Adressvergabe zum Einsatz kommt, ist RA unverzichtbar. Weder die Router-Adresse noch die Präfixlänge können über DHCPv6 zugewiesen werden.

Router-Advertisement

per Unicast an einzelne Clients

Wenn Sie IPv6 nicht im ganzen Netzwerk ausrollen wollen, können Sie mit Hilfe dieser Einstellung Router-Advertisements gezielt an eine Liste manuell konfigurierter Clients schicken.

aktiviert

Wählen Sie diese Einstellung um per Multicast alle Endgeräte über die Verfügbarkeit von IPv6 zu informieren.

Router Priorität

Über diesen Schalter kann beeinflusst werden, für welchen Router sich ein Endgerät entscheidet, wenn mehrere Router zur Auswahl stehen.



Manche Endgeräte werten diese Option nicht aus oder müssen erst entsprechend konfiguriert werden.

Router Advertisements senden an

Sofern Sie sich dazu entschieden haben, Router-Advertisements nur per Unicast an einzelne Clients zu senden, müssen Sie die Link-Local Adressen der Clients hier angeben. Link-Local Adressen beginnen stets mit "fe80:".

Präfixe für zustandslose Adressvergabe (SLAAC)

Sofern sich die Endgeräte selbständig eine IPv6-Adresse konfigurieren sollen, geben Sie hier bitte die gewünschten Präfixe an.

Der Präfix kann auf einem vom Provider dynamisch zugewiesenen Präfix basieren. Beim Hinzufügen eines neuen Eintrags werden Ihnen die im Menü "Definitionen > IP-Objekte" angelegten Präfixe zur Auswahl angeboten. Sie können im besagten Menü auch selbst Einträge vom Typ "IPv6-Präfix" anlegen, um z.B. den vom Provider erhaltenen Präfix weiter zu unterteilen.

DHCPv6

Mithilfe dieses Schalters teilen Sie den Endgeräte mit, inwiefern ein DHCPv6-Server im Netzwerk verfügbar ist.

keine IP-Vergabe, nur Zusatzinformationen (O-Flag)

In dieser Einstellung können Endgeräte lediglich Informationen wie z.B. die Adresse des DNS-Servers via DHCP beziehen.

ja (M-Flag und O-Flag)

Soll den Endgeräten eine IPv6-Adresse per DHCPv6 zugewiesen werden, müssen Sie diese Einstellung wählen.

DNS 1 (RDNSS)

Name-Server Adressen können über die RA-Erweiterung RDNSS zugewiesen werden. Da diese Option jedoch von vielen Geräten nicht unterstützt wird, sollten Sie die DNS-Adressen zumindest parallel auch über DHCPv6 verteilen.

DNS-Suffix (DNSSL)

Auch ein DNS-Suffix für die Namensauflösung von Host-Namen ohne Domain-Angabe kann über RA verteilt werden. Auch diese Erweiterung wird jedoch von vielen Endgeräten noch nicht unterstützt.

Veröffentlichte Routen

Über Router-Advertisements können gezielt Routen zu einzelnen IPv6-Präfixen verteilt werden.



Manche Endgeräte werten diese Option nicht aus oder müssen erst entsprechend konfiguriert werden.

14.1.2.3-D Routing

Erweitertes Routing

Auf diesem Reiter können statische Routen konfiguriert werden. Neben herkömmlichen Routen, bei denen lediglich die Ziel-Adresse bei der Routing-Entscheidung berücksichtigt wird, können auch erweiterte Routen erstellt werden. Dabei lassen sich die Quell-Adresse sowie Protokoll- und Port-Nummern auswerten (Policy-based Routing).

Statische Routen müssen für Netzwerke spezifiziert werden, die nicht direkt an der Netzwerk-Karte anliegen, sondern die sich hinter einem Router befinden. Das Zielnetzwerk wird über die Netzwerkadresse und die zugehörige Netzmaske spezifiziert, womit das Netzwerk automatisch auch der SX-GATE Firewall bekannt gemacht wird. Als Gateway ist die IP-Adresse des Routers anzugeben.



Die IP-Adresse des Gateways muss stets dem selben IP-Netzwerk angehören, dem auch SX-GATE angehört. Netzwerkadresse und Netzmaske des Zielnetzes müssen hingegen ein anderes IP-Netzwerk adressieren.

Regeln für spezielle Protokolle oder Quell-Adressen bieten sich an, wenn mehrere Internet-Anbindungen zur Verfügung stehen. So ließe sich z.B. das Surfen im Internet über eine ADSL-Verbindung leiten, während die übrige Kommunikation wie Mail oder VPN über eine SDSL-Leitung läuft.

Die Priorität der einzelnen Routen ergibt sich nicht aus der Reihenfolge in der sie eingetragen werden. Entscheidend ist vielmehr, wie spezifisch die Routen sind. Schnittstellenübergreifend haben Routen, bei denen Protokoll, Quelle und Ziel angegeben sind, die höchste Priorität. Regeln mit Ziel haben Vorrang vor Regeln mit Protokoll, diese wiederum vor Regeln mit Angabe einer Quelle. Innerhalb von Quelle und Ziel erfolgt die Sortierung nach absteigender Netzmaske. Die Reihenfolge bei Überschneidungen im Protokoll ist nicht definiert.

14.1.2.3-E Bandbreitenmanagement / QoS

Für das Bandbreiten-Management müssen Sie die Bandbreite der Anbindung festlegen. Die eingehende und ausgehende Bandbreite kann dabei unterschiedlich sein (ADSL). Solange Sie keine Bandbreite festlegen, ist das Bandbreitenmanagement auf dieser Schnittstelle deaktiviert. Wenn Sie lediglich die ein- oder die ausgehende Bandbreite eintragen, ist das Bandbreitenmanagement auch nur in dieser Richtung aktiv.



Die Angabe einer falschen Bandbreite kann zu Problemen führen. Dies gilt insbesondere, wenn die eingestellte Bandbreite höher ist als die tatsächlich verfügbare. Fragen Sie im Zweifel Ihren Provider.

Bandbreite ausgehend (Uplink)

Geben Sie hier die ausgehende Bandbreite (Uplink) an. Bei asymmetrischen Anbindungen ist dies in der Regel der kleinere Wert. Es werden dann alle über diese Schnittstelle ausgehenden Datenpakete vom Bandbreitenmanagement verarbeitet. Die Verbindungsrichtung (eingehende oder ausgehende Verbindung) spielt dabei keine Rolle.

Bandbreite eingehend (Downlink)

Geben Sie hier die eingehende Bandbreite (Downlink) an. Bei asymmetrischen Anbindungen ist dies in der Regel der größere Wert. Es werden dann alle über diese Schnittstelle eingehenden Datenpakete vom Bandbreitenmanagement verarbeitet. Die Verbindungsrichtung (eingehende oder ausgehende Verbindung) spielt dabei keine Rolle. Lassen Sie das Feld leer, wenn Sie kein eingehendes Bandbreitenmanagement wünschen.

Eingehendes Bandbreitenmanagement ist eigentlich ein Widerspruch in sich. Das Umsortieren von auf die Übertragung wartend Datenpaketen nach Priorität müsste

eigentlich auf der anderen Seite der (Internet-)Verbindung vorgenommen werden, denn nur dort ist dies zuverlässig möglich. Beim eingehenden Bandbreitenmanagement sind die Pakete ja bereits übertragen worden. Internet-Anbindungen mit providerseitigem Quality-of-Service/Bandbreitenmanagement sind jedoch oft sehr teuer, so dass eingehendes Bandbreitenmanagement trotz seiner Einschränkungen gewünscht wird.



Eingehendes Bandbreitenmanagement reduziert die verfügbare Bandbreite um bis zu 20%. Es funktioniert nur, solange das eingehende Datenvolumen zu einem ausreichend hohen Anteil über TCP-Verbindungen abgewickelt werden.

Quality-of-Service (QoS) für Voice-over-IP (VoIP)

Bei VoIP spielt die Latenzzeit, also die Zeitspanne die ein Sprachdatenpaket vom Absender zum Empfänger benötigt, eine große Rolle. Das Bandbreitenmanagement des SX-GATE optimiert den Versand von VoIP-Paketen daher mit Hilfe eines speziellen Quality-of-Service Moduls.



Um als VoIP-Paket erkannt zu werden, muss ein IP-Paket gemäß Diffserv-Code-Point Expedited-Forwarding (DSCP EF) markiert sein.

Die Bandbreite eines einzelnen Gesprächs ist abhängig vom jeweils verwendeten Codec. Der Codec bestimmt dabei, wie stark das Gespräch komprimiert wird. Je stärker der Codec das Gespräch komprimiert, desto weniger Bandbreite wird benötigt. Im Gegenzug sinkt jedoch die Qualität des Gesprächs mit der Zunahme der Kompression. Die folgende Tabelle gibt die Nettobandbreite typischer Codecs an. Bei Codecs die mit verschiedenen Bandbreiten genutzt werden, ist jeweils die maximale Bandbreite angegeben.

Codec	max. Bandbreite (bit/s)
G.711	64000
G.722	64000
G.722.1	32000
G.723.1	6400
G.726	40000
G.728	16000

Codec	max. Bandbreite (bit/s)
G.729	8000
GSM	13000
iLBC	15200

Max. Anzahl gleichzeitiger Gespräche

Geben Sie die maximal erwartete Anzahl gleichzeitiger unverschlüsselter Gespräche an, die über diese Schnittstelle abgewickelt werden. Die Anzahl der Gespräche dient als Grundlage für die Berechnung der insgesamt für VoIP zu reservierenden Bandbreite. Der Wert "0" deaktiviert die Priorisierung.



Die Insgesamt zur Verfügung stehende Bandbreite der Anbindung darf nicht überschritten werden.

Bitrate des verwendeten Codecs

Geben Sie die Nettobandbreite des verwendeten Codecs an. Bei Verwendung unterschiedlicher Codecs orientieren Sie sich bitte am Codec mit dem größten Bandbreitenbedarf.



Zur Berechnung der insgesamt benötigten Bandbreite wird vom System automatisch der IP-Overhead eingerechnet. Dieser ist umso größer, je kleiner die Bitrate des Codecs ist.

Max. Anzahl Gespräche über IPSec

Geben Sie die maximal erwartete Anzahl gleichzeitiger Gespräche über IPSec-VPN an, die über diese Schnittstelle abgewickelt werden. Die Anzahl der Gespräche dient als Grundlage für die Berechnung der insgesamt für VoIP zu reservierenden Bandbreite. Der Wert "0" deaktiviert die Priorisierung.



Wenn aktiviert, werden VoIP-Datenpakete gegenüber anderem VPN-Datenverkehr bevorzugt. Selbiges gilt nach der Verschlüsselung für die entstandenen VPN-Pakete.



Die Insgesamt zur Verfügung stehende Bandbreite der Anbindung darf nicht überschritten werden.

Bitrate des Codecs im IPSec

Geben Sie die Nettobandbreite des verwendeten Codecs an. Bei Verwendung unterschiedlicher Codecs orientieren Sie sich bitte am Codec mit dem größten Bandbreitenbedarf.



Zur Berechnung der insgesamt benötigten Bandbreite wird vom System automatisch der IP- und der IPSec-Overhead eingerechnet. Dieser ist umso größer, je kleiner die Bitrate des Codecs ist.

14.1.2.3-F Priorisierung

Mit Hilfe dieser Funktion können Datenpakete auf verschiedene Prioritätsklassen aufgeteilt werden. Jeder Klasse ist eine anteilige Mindestbandbreite zugeordnet. Nicht benötigte Bandbreite einer höherpriorien Klasse steht den nachfolgenden Klassen zur Verfügung.

Aus technischer Sicht wird durch die Regeln das ToS- bzw. DSCP-Feld von IP-Paketen überschrieben. Setzt eine lokale Anwendung bereits das ToS/DSCP-Feld passend, ist keine Regel für ausgehende Pakete notwendig. Bei eingehenden Paketen wird das ToS/DSCP-Feld häufig auf dem Weg durch das Internet verändert, so dass für das eingehende Bandbreitenmanagement üblicherweise Regeln erforderlich sind.



Manche Provider stellen Datenpakete mit gesetztem ToS/DSCP-Feld in Rechnung. Bitte prüfen Sie Ihre Vertragsbedingungen.

Die Mindestbandbreiten werden wie folgt verteilt: Die für VoIP benötigte Bandbreite gemäß Konfiguration wird reserviert und von der insgesamt verfügbaren Bandbreite abgezogen. Von der verbliebenen Bandbreite entfallen 10% auf leere TCP ACK-Pakete, 50% auf hochpriorie Datenpakete und je 20% auf Pakete mit normaler oder niedriger Priorität.



Für das eingehende Bandbreitenmanagement werden nicht-TCP Pakete grundsätzlich wie hochpriorie Datenpakete behandelt.

Priorisierung von Verbindungen

Fügen Sie dieser Liste die Signaturen der Datenpakete hinzu, die eine höhere oder niedriger Priorität erhalten sollen. Treffen mehrere Regeln auf ein Datenpaket zu, so wird die Priorität des ersten passenden Eintrags angewendet.

Die einzelnen Eingabefelder haben dabei folgende Bedeutungen:

Protokoll

Legt die IP-Protokoll und Port-Signatur fest. Bei eingehendem Bandbreitenmanagement werden ausschließlich TCP-Protokolle berücksichtigt.



Protokoll-Definitionen werden im Menü "Definitionen > Protokolle" vorgenommen.

Lokale IP/Netzwerk

Auf dieser Seite steht die aus Sicht der gewählten Schnittstelle lokale Adresse. Bei einem ausgehenden Datenpaket entspricht dies der Quell-IP (vor SNAT), bei einem eingehenden Datenpaket der Ziel-IP (vor DNAT).



Wenn Sie die Priorisierung bei DNAT- oder SNAT-Verbindungen auf bestimmte lokale IPs beschränken wollen, sind üblicherweise zwei Regeln erforderlich um beide Verbindungsrichtungen abzudecken: Für eingehende Datenpakete muss eine SX-GATE IP angegeben werden, für ausgehende Datenpakete die interne IP (des LAN-Clients bzw. des per DNAT angesprochenen Servers).

Richtung

Wählen Sie hier bitte aus, in welcher Richtung die Portsignatur des gewählten Protokolls interpretiert wird. Erläutert am Beispiel HTTP bedeutet der Richtungspfeil "-->", der HTTP-Port 80 befindet sich auf der externen Seite. Das ausgehende Bandbreitenmanagement verarbeitet folglich Pakete zu Port 80, das eingehende von Port 80. Wird der entgegengesetzt orientierte Pfeil "<--" gewählt, werden eingehende HTTP-Verbindungen verarbeitet. Pakete zu Port 80 durchlaufen das eingehende Bandbreitenmanagement, Pakete von Port 80 das ausgehende. Der Doppelpfeil "↔" steht für beide Interpretationsrichtungen.

Externe IP/Netzwerk

Auf dieser Seite steht die aus Sicht der gewählten Schnittstelle externe Adresse. Bei einem ausgehenden Datenpaket entspricht dies der Ziel-IP, bei einem eingehenden Datenpaket der Quell-IP.

Priorität

Wählen Sie hier die gewünschte Priorisierung aus.

14.1.2.3-G Dynamischer DNS

Dynamischer DNS ermöglicht es, ein Gerät, das eigentlich mit einer dynamischen IP-Adresse an das Internet angebunden ist, unter dessen jeweils aktueller Adresse aufzufinden. Mit Hilfe dieses Dienstes kann also vom Internet aus auf SX-GATE zugegriffen werden, obwohl dieser nur über eine dynamische IP-Adresse verfügt. Die Adressierung im dynamischen DNS erfolgt mit Hilfe eines üblichen DNS-Rechnernamens (Fully-Qualified-Domain-Name, FQDN). Es gibt eine Reihe von Anbietern, die dynamischen DNS sowohl als kostenlose als auch als kostenpflichtige Dienstleistung zur Verfügung stellen.



Nach einem IP-Wechsel vergehen einige Sekunden bis Minuten, bis der DNS-Name auch tatsächlich auf die neue IP-Adresse verweist.

Sofern SX-GATE selbst die dynamische IP erhält (ADSL-Schnittstelle mit dynamischer IP oder Ethernet-Schnittstelle mit IP-Vergabe über DHCP), konfigurieren Sie dynamischen DNS bitte in der jeweiligen Schnittstelle im Menü "Module > Netzwerk > Schnittstellen". SX-GATE aktualisiert seine IP-Adresse im dynamischen DNS dann einmalig bei jedem Verbindungsaufbau bzw. IP-Wechsel.

Für den Fall, dass sich SX-GATE hinter einem NAT-Router befindet und dieser die dynamische IP erhält, muss der NAT-Router eingehende Verbindungen an SX-GATE weiterreichen können (DNAT, Portforwarding, Exposed Host). Optimalerweise konfigurieren Sie dynamischen DNS im NAT-Router, da nur dieser die aktuelle dynamische IP kennt. Ist dies nicht möglich, konfigurieren Sie dynamischen DNS bitte hilfsweise im SX-GATE Menü "Module > DNS > Einstellungen". SX-GATE versucht dann in regelmäßigen Abständen die dynamische IP des NAT-Routers mit Hilfe eines Internet-Dienstes zu ermitteln.

Protokoll

Für die Aktualisierung der Einträge im dynamischen DNS gibt es leider keinen einheitlichen Standard. SX-GATE unterstützt jedoch eine ganze Reihe von Protokollen für diese Aktualisierung. Bitte klären Sie zunächst mit dem Anbieter des dynamischen DNS-Dienstes, welches Protokoll verwendet wird und ob dieses vom SX-GATE unterstützt wird.

Update-Server des Anbieters

Tragen Sie hier bitte den Namen des Servers ein, der die Nachrichten zur Aktualisierung der dynamischen IP-Adresse entgegen nimmt. Dieser Server ist nicht immer identisch mit dem Webserver des Anbieters.

Update-URL

Tragen Sie hier bitte die Update-URL (auch "Direct URL" genannt) zur Aktualisierung der dynamischen IP-Adresse ein. Die URL kann die Platzhalter <host>, <ipaddr>, <username> und <password> enthalten, die durch den dynamischen DNS-Namen, die IP-Adresse, den Benutzernamen und das Passwort ersetzt werden. Beispiel: `http://dynupdate.examplerdyndns.com/nic/update?hostname=<domain>&myip=<ipaddr>`

Dynamischer DNS-Name des SX-GATES

Über ein Benutzerkonto bei dem jeweiligen Anbieter lassen sich in der Regel mehrere DNS-Namen verwalten. Daher ist hier der vollständige Name (inkl. Domain) anzugeben, unter dem SX-GATE im dynamischen DNS erreichbar ist.

Benutzername

Keine Aktualisierung des Eintrags im dynamischen DNS ohne entsprechende Anmeldung. Geben Sie hier den Benutzernamen (login) für das Konto an.

Passwort

Geben Sie hier schließlich das entsprechende Kennwort für die Aktualisierung an.

Jetzt aktualisieren

`ref link="#main_modules#sm_devices#tr_dyndns_checkdd"/>`

14.1.2.4 WLAN (wlan)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.4-A Einstellungen.....	339
14.1.2.4-B IP-Adressen.....	342
14.1.2.4-C IPv6 Router-Advertisement.....	343
14.1.2.4-D Authentifizierung.....	345
14.1.2.4-E MAC-Filter.....	347

Schnittstellen-Modus

Legen Sie hier fest, wie die WLAN-Schnittstelle genutzt werden soll.

eigenständiges WLAN

In diesem Modus erhält die WLAN-Schnittstelle eine eigene IP-Konfiguration.

weiterer Bridge-Port

Mit dieser Option können Sie die WLAN-Schnittstelle zu einer bereits konfigurierten Bridge hinzufügen.



Um eine neue Bridge zu erstellen, wählen Sie bitte die Option "eigenständiges WLAN" und aktivieren Sie dort die Bridge.

IPv6-Modus

Wählen Sie hier die Art der IPv6-Anbindung aus.

manuelle IP

In dieser Einstellung muss die IPv6-Konfiguration manuell erfolgen. Router-Advertisements werden ignoriert.

14.1.2.4-A Einstellungen

Beschreibung

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Ländercode

Hier sehen Sie die aktuelle Ländereinstellung des WLAN-Adapters. Diese legt die verfügbaren Kanäle und die Sendeleistung fest.



Der Betrieb einer WLAN-Karte mit falscher Ländereinstellung kann dazu führen, dass die WLAN-Karte mit Einstellungen arbeitet, die in Ihrem Land verboten sind. Wenden Sie sich bitte an Ihren SX-GATE-Fachhändler falls die Einstellung nicht korrekt ist.

SSID

Geben Sie hier bitte den Namen des WLANs an.

SSID verstecken

Wenn Sie diese Option aktivieren, ist der Name des WLANs nicht sichtbar. Clients müssen den Namen kennen um sich verbinden zu können.



Mit entsprechenden Werkzeugen kann ein Angreifer das versteckte WLAN dennoch einfach aufspüren.

Client Isolierung deaktivieren

Die Client Isolierung ist ein Sicherheitsmechanismus der verhindert, dass WLAN Clients im selben Netz direkt miteinander kommunizieren können. Dies ist besonders für Gastnetze oder Netze in denen die Benutzer ihre eigenen Geräte mitbringen wichtig.

Wenn Sie diese Option setzen, können die WLAN Clients ungeschützt aufeinander zugreifen.

Frequenzband

Wählen Sie hier bitte das gewünschte Frequenzband aus.

Kanal (2,4 GHz)

Der Kanal kann automatisch ausgewählt werden. Alternativ können Sie hier einen festen Kanal einstellen.



Welche Kanäle verfügbar sind ist abhängig von der Ländereinstellung.

Kanal (5 GHz)

Für eine feste Auswahl stehen nur wenige Kanäle zur Verfügung, da es bei den meisten Kanälen im 5 GHz-Band zu Überschneidungen mit Radarstationen kommen kann. Wir empfehlen daher die automatische Auswahl des Kanals in Verbindung mit Radarerkennung und dynamischer Frequenzwahl (DFS). Erst dann steht ein breites Spektrum an Kanälen zur Verfügung.



Welche Kanäle verfügbar sind ist abhängig von der Ländereinstellung.

Radarererkennung / DFS

Aktivieren Sie die Radarererkennung und Dynamic Frequency Selection (DFS) nach IEEE 802.11h um im 5 GHz Band auch die Kanäle 52-64 und 100-140 nutzen zu können.



Die tatsächlich genutzten Kanäle sind abhängig von der Ländereinstellung.

IEEE 802.11n

Mit dieser Einstellung aktivieren Sie den IEEE 802.11n Modus, der den Durchsatz durch Nutzung mehrerer paralleler Datenströme über mehrere Antennen vergrößern kann.

20 MHz Kanäle

In dieser Einstellung wird die Standard-Kanalbreite von 20 MHz genutzt.

40 MHz Kanäle

Um den Durchsatz nochmals zu erhöhen, können Sie die Bandbreite der Kanäle auf 40 MHz erweitern.



Beim Betrieb im 2,4 GHz-Band werden dann jedoch rund die Hälfte aller verfügbaren Frequenzen genutzt, was den überlappungsfreien Betrieb mit anderen WLANs im Umkreis erschwert.

Bridge

Ähnlich wie ein Switch, verbindet eine Bridge mehrere Netzwerk-Segmente zu einem großen Netzwerk. Im SX-GATE besteht dabei die Möglichkeit, den Datenaustausch mit Hilfe von Firewall-Regeln zu filtern. So ist es z.B. auch möglich, SX-GATE als transparente Firewall zwischen dem LAN und einem Internet-Router zu betreiben.

Beachten Sie bitte, dass bei Verbindungen, die von außerhalb der Bridge in die Bridge hinein geroutet werden, zum Zeitpunkt der Filterung in der Firewall noch nicht bekannt ist, über welchen Bridge-Port die Verbindung anschließend gesendet wird. Entsprechend sind in der Firewall Weiterleitungs-Regeln, Regeln für ausgehende Verbindungen (Quelle ist ein SX-GATE-Dienst) und SNAT-Regeln stets für die Bridge als ganzes und damit portunabhängig zu konfigurieren. Auch eine eigene Ziel-Zone muss für die Bridge als ganzes eingestellt werden.

Im Gegensatz dazu werden Regeln für Verbindungen innerhalb der Bridge, also Verbindungen die von einem Bridge-Port an einen anderen Bridge-Port weitergeleitet werden, je Bridge-Port konfiguriert. Das selbe gilt für DNAT-Regeln und Regeln für

eingehende Verbindungen (Ziel ist ein SX-GATE-Dienst). Die Firewall-Zone lässt sich für jeden Bridge-Port individuell festlegen. Als Quell-Zone steht diese auch außerhalb der Bridge zur Verfügung, wenn eine Verbindung aus der Bridge heraus in eine Schnittstelle außerhalb der Bridge geroutet wird.

Spanning-Tree-Protokoll

Wenn Sie mehrere Switches und Bridges so miteinander verbunden haben, dass es alternative Kommunikationswege zwischen den Geräten gibt, müssen Sie das Spanning-Tree-Protokoll (STP) auf allen beteiligten Switches und Bridges aktivieren. Über das Protokoll stellen die Gerät sicher, dass die Netzwerk-Topologie zyklenfrei bleibt, reagieren aber auch auf Ausfälle.

Bekannte Ziele routen

Wenn dieser Schalter aktiviert wird, werden bestimmte Pakete nicht durch die Bridge sondern über das Routing des SX-GATES weitergeleitet. Das betrifft Pakete an Ziel-Adressen, die im SX-GATE auf anderen Schnittstellen oder in VPNs konfiguriert sind bzw. zu denen eine statische Route konfiguriert wurde.



Diese Einstellung ist nur dann sinnvoll, wenn sich der SX-GATE als transparente Firewall zwischen Client-Systemen und einem Router befindet, der in den Client-Systemen als Standard-Gateway konfiguriert ist.



Firewall-Regeln für diese Verbindungen müssen im Untermenü "Regeln" und nicht im Untermenü "Bridge" konfiguriert werden.

Zuordnen zu Bridge

Wählen Sie hier die Bridge aus, mit der Sie die WLAN-Schnittstelle verbinden wollen.

14.1.2.4-B IP-Adressen

IPv4-Adresse

Geben Sie hier die IPv4-Adresse ein, die SX-GATE auf dieser Schnittstelle erhalten soll.



Die hier angegebene IP-Adresse darf nicht zu einem IP-Adress-Bereich gehören, der bereits auf einer anderen Schnittstelle konfiguriert ist.

IPv4-Netzmaske

Geben Sie hier die Netzmaske ein, die zu der angegebenen IP-Adresse gehört.

zusätzliche IPv4-Adressen (Aliase) bzw. Cluster-IP-Adressen

Nutzen Sie diesen Bereich, um weitere IP-Adressen an diese WLAN-Schnittstelle zu binden. Es kann sich hierbei um Adressen aus dem gleichen Netzwerk handeln, aus dem auch die primäre IP-Adresse stammt. Möglich ist aber auch die Vergabe von Adressen aus anderen Netzwerken, wenn im selben WLAN mehrere IP-Netzwerke konfiguriert sind.

IPv6-Adresse

Geben Sie hier die IPv6-Adresse für die Schnittstelle ein. Falls diese Adresse auf einem dynamisch zugewiesenen Präfix basieren soll, legen Sie bitte im Menü "Definitionen > IP-Objekte" einen Eintrag vom Typ "IPv6-Adresse" an, der auf den entsprechenden Präfix verweist.

IPv6-Präfixlänge

Bei der IPv6-Präfixlänge handelt es sich um das Pendant zur IPv4-Netzmaske. Die typische Präfixlänge ist 64.



Bei Präfixlängen größer als 64 funktionieren bestimmte IPv6-Verfahren wie z.B. SLAAC nicht mehr. Verwenden Sie größere Präfixe nur, wenn Ihnen die Auswirkungen bekannt sind.

zusätzliche IPv6-Adressen (Aliase) bzw. Cluster-IP-Adressen

Nutzen Sie diesen Bereich, um weitere IPv6-Adressen an diese WLAN-Karte zu binden. Es kann sich hierbei um Adressen aus dem gleichen Netzwerk handeln, aus dem auch die primäre IP-Adresse stammt oder auch andere IP-Adressen (z.B. ULA-Adressen).

14.1.2.4-C IPv6 Router-Advertisement

Router-Advertisement (RA) dient der automatischen IPv6-Konfiguration von Endgeräten. Router mit Internetanbindung geben den Endgeräten auf diese Weise ihre IP-Adresse bekannt. Auch die Präfixlänge des lokalen Netzwerks wird über RA bekanntgegeben.



Selbst wenn DHCPv6 für die Adressvergabe zum Einsatz kommt, ist RA unverzichtbar. Weder die Router-Adresse noch die Präfixlänge können über DHCPv6 zugewiesen werden.

Router-Advertisement

per Unicast an einzelne Clients

Wenn Sie IPv6 nicht im ganzen Netzwerk ausrollen wollen, können Sie mit Hilfe dieser Einstellung Router-Advertisements gezielt an eine Liste manuell konfigurierter Clients schicken.

aktiviert

Wählen Sie diese Einstellung um per Multicast alle Endgeräte über die Verfügbarkeit von IPv6 zu informieren.

Router Priorität

Über diesen Schalter kann beeinflusst werden, für welchen Router sich ein Endgerät entscheidet, wenn mehrere Router zur Auswahl stehen.



Manche Endgeräte werten diese Option nicht aus oder müssen erst entsprechend konfiguriert werden.

Router Advertisements senden an

Sofern Sie sich dazu entschieden haben, Router-Advertisements nur per Unicast an einzelne Clients zu senden, müssen Sie die Link-Local Adressen der Clients hier angeben. Link-Local Adressen beginnen stets mit "fe80:".

Präfixe für zustandslose Adressvergabe (SLAAC)

Sofern sich die Endgeräte selbständig eine IPv6-Adresse konfigurieren sollen, geben Sie hier bitte die gewünschten Präfixe an.

Der Präfix kann auf einem vom Provider dynamisch zugewiesenen Präfix basieren. Beim Hinzufügen eines neuen Eintrags werden Ihnen die im Menü "Definitionen > IP-Objekte" angelegten Präfixe zur Auswahl angeboten. Sie können im besagten Menü auch selbst Einträge vom Typ "IPv6-Präfix" anlegen, um z.B. den vom Provider erhaltenen Präfix weiter zu unterteilen.

DHCPv6

Mithilfe dieses Schalters teilen Sie den Endgeräten mit, inwiefern ein DHCPv6-Server im Netzwerk verfügbar ist.

keine IP-Vergabe, nur Zusatzinformationen (O-Flag)

In dieser Einstellung können Endgeräte lediglich Informationen wie z.B. die Adresse des DNS-Servers via DHCP beziehen.

ja (M-Flag und O-Flag)

Soll den Endgeräten eine IPv6-Adresse per DHCPv6 zugewiesen werden, müssen Sie diese Einstellung wählen.

DNS 1 (RDNSS)

Name-Server Adressen können über die RA-Erweiterung RDNSS zugewiesen werden. Da diese Option jedoch von vielen Geräten nicht unterstützt wird, sollten Sie die DNS-Adressen zumindest parallel auch über DHCPv6 verteilen.

DNS-Suffix (DNSSL)

Auch ein DNS-Suffix für die Namensauflösung von Host-Namen ohne Domain-Angabe kann über RA verteilt werden. Auch diese Erweiterung wird jedoch von vielen Endgeräten noch nicht unterstützt.

Veröffentlichte Routen

Über Router-Advertisements können gezielt Routen zu einzelnen IPv6-Präfixen verteilt werden.



Manche Endgeräte werten diese Option nicht aus oder müssen erst entsprechend konfiguriert werden.

14.1.2.4-D Authentifizierung

Authentifizierung und Verschlüsselung

Wählen Sie hier die Authentifizierungsmethode und Verschlüsselung. Für die paarweise Verschlüsselung wird bei allen Methoden AES (CCMP) verwendet.



WPA3 wird nur von neuerer Hardware unterstützt und benötigt auch aktuelle Software Versionen (iOS 13/iPadOS 13, Android 10 oder Windows 10 ab Version 1903).

Management Frame Protection (MFP)

Die Management Frame Protection (MFP) dient dazu Verwaltungs-Frames, die unverschlüsselt übertragen werden müssen, zu schützen. Steht diese Option auf "Erforderlich", können sich nur noch Clients verbinden, die Management Frame

Protection (MFP) unterstützen. In der Einstellung "Optional" können sich auch nicht MFP fähige Clients verbinden, allerdings ohne den zusätzlichen Schutz.



Für WPA3-SAE ist die "Management Frame Protection (MFP)" Voraussetzung und kann daher nicht deaktiviert werden. Es empfiehlt sich hier die Option "Erforderlich" zu wählen.

WPA Passphrase

Vergeben Sie hier bitte das WLAN-Passwort. Es muss aus mindestens 8 Zeichen bestehen. Wir empfehlen eine komplexe Passphrase mit mindestens 32 Zeichen anstelle eines normalen Passworts. Es sollten möglichst unterschiedliche Zeichen enthalten sein (Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen) und am besten nicht aus normalen Wörtern bestehen, die in einem Wörterbuch zu finden sind.

Authentifizierungsserver Adresse

Bitte tragen Sie hier den Authentifizierungsserver ein.

Authentifizierungsserver Port

Dies ist der Port über den der Authentifizierungsserver erreichbar ist.

Authentifizierungsserver Passphrase

Geben Sie hier den geheimen Schlüssel ein, mit dem sich SX-GATE am Authentifizierungsserver anmelden soll.

Kontoführung

Mit diesem Schalter aktivieren Sie die Kontoführung.

Kontoführungsserver Adresse

Bitte tragen Sie hier den Kontoführungsserver ein.

Kontoführungsserver Port

Dies ist der Port über den der Kontoführungsserver erreichbar ist.

Kontoführungsserver Passphrase

Geben Sie hier den geheimen Schlüssel ein, mit dem sich SX-GATE am Kontoführungsserver anmelden soll.

NAS ID

Die NAS ID wird in der Kommunikation mit dem Authentifizierungs-/Kontoführungsserver genutzt und dient zur Identifizierung. Da jede SSID eine eigene NAS ID hat,

sollte sie möglichst eindeutig sein. Zum Beispiel eine Kombination aus SSID und FQDN.

14.1.2.4-E MAC-Filter

Bei aktiviertem MAC-Filter können sich nur noch Clients verbinden, deren MAC-Adresse hier hinterlegt wurde.



Der MAC-Filter bietet nur begrenzten Zugangsschutz, da versierte Anwender oder Angreifer die MAC-Adresse ihres Clients leicht fälschen können.

MAC-Filter

Mit diesem Schalter aktivieren Sie den MAC-Filter.

Erlaubte MAC-Adressen

Tragen Sie hier die MAC-Adressen der Clients ein, denen Sie Zugang erlauben möchten. Sie können auch auf Objekte vom Typ "Host" verweisen, die im Menü "Definitionen > IP-Objekte" angelegt wurden. Es werden nur Objekte berücksichtigt, in denen tatsächlich eine MAC-Adresse hinterlegt wurde. Eventuell im Objekt hinterlegte IP-Adressen werden ignoriert.

14.1.2.5 L2TP

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.5-A IP-Adressen.....	347
14.1.2.5-B DNS.....	348

14.1.2.5-A IP-Adressen

Diese Schnittstelle ist für die Verwendung in Kombination mit dem IPSEC VPN-Server des SX-GATE gedacht. Es ist jedoch auch möglich ohne einen VPN-Kanal zu nutzen mit dem L2TP-Server des SX-GATE Kontakt aufzunehmen.

Beschreibung

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Lokale IP-Adresse

Legen Sie hier die IP-Adresse fest, die SX-GATE auf dieser Schnittstelle verwendet. Es bietet sich an, die LAN-IP-Adresse zu nutzen.

Zuzuweisende IP-Adressen

Geben Sie hier die IP-Adressen an, die den Gegenstellen zugewiesen werden sollen. Handelt es sich dabei um IP-Adressen aus einem der direkt an SX-GATE angeschlossenen Netzwerke, so wird zusätzlich ein Proxy-ARP Eintrag erzeugt, der das transparente Einbinden der Gegenstelle in das Netzwerk ermöglicht.



Die Anzahl der hier eingetragenen IP-Adressen bestimmt die maximale Anzahl gleichzeitiger L2TP-Verbindungen.

Um einen ganzen Block von Adressen einzutragen, müssen Sie eine Netzwerk-Adresse mit dazu passender Netzmaske eingeben. Angenommen im LAN wird das Netzwerk 192.168.0.0/24 verwendet: Mit dem Eintrag 192.168.0.160/27 fügen Sie einen Block von insgesamt 32 Adressen aus dem Bereich 192.168.0.160 bis 192.168.0.191 hinzu.



Die Adress-Blöcke dürfen keine Netzwerk- oder Broadcast-Adressen der lokalen Ethernet-Netzwerke enthalten. Ausgenommen sind Netzwerk- und Broadcast-Adresse eines Class-C-Netzes (*.0 bzw. *.255). Diese werden automatisch aus dem Adress-Block ausgenommen.

14.1.2.5-B DNS

Als DNS-Server zuweisen

Mit dieser Einstellung können Sie festlegen, welchen Namens-Server der Client verwenden soll.

Sekundärer DNS

Bei Bedarf kann hier ein weiterer Name-Server hinterlegt werden.

WINS 1

Hier können Sie den primären WINS-Server festlegen. WINS wird von Windows benötigt, um Rechner netzwerkübergreifend zu finden.

WINS 2

Hier kann ein zweiter WINS-Server eingetragen werden.

14.1.2.6 Wireguard (wg)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.6-A Allgemein.....	349
14.1.2.6-B Verbindungen.....	351

14.1.2.6-A Allgemein**Beschreibung**

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Privater Schlüssel

Wählen Sie einen der X25519-Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.

Verbindung importieren

Importieren Sie eine Wireguard-Konfigurationsdatei oder ein SX-GATE-Installationspaket für Wireguard (*.rin).



Diese Option wird nur angeboten, solange noch kein private Schlüssel ausgewählt wurde.

Öffentlicher Schlüssel

Hier wird der zugehörige öffentliche Schlüssel angezeigt. Um ein VPN aufbauen zu können, muss dieser der Gegenstelle mitgeteilt werden.

Lokaler Port

Tragen Sie hier den Port ein, unter dem der Wireguard-Server erreichbar ist.



In der Firewall-Konfiguration müssen Sie eine Protokoll-Definition für diesen UDP-Port anlegen und in der Firewall-Konfiguration den Internet-Zugriff auf SX-GATE für dieses Protokoll erlauben.



Falls Sie mehrere Wireguard-Schnittstellen anlegen, müssen sich diese im Protokoll unterscheiden. Sie dürfen ferner keine Port-Nummer nutzen, die andere UDP-Dienste des SX-GATES nutzen.

Virtuelle IPv4-Adresse

Die hier konfigurierte IPv4-Adresse wird als Quell-IP gesetzt, wenn auf der Wireguard-Schnittstelle NAT für ausgehende Verbindungen konfiguriert ist und wenn SX-GATE selbst Verbindungen über das VPN initiiert.



Sie können hier sowohl die IP-Adresse einer anderen SX-GATE-Schnittstelle eintragen als auch die IP-Adresse eines bisher nicht genutzten Netzes.

Virtuelle IPv6-Adresse

Konfigurieren Sie hier eine IPv6-Adresse, wenn SX-GATE selbst IPv6-Verbindungen über das VPN initiiert.

Keepalive-Intervall

Ist hier ein Wert konfiguriert, sendet SX-GATE regelmäßig ein leeres Paket über das VPN. Das kann erforderlich sein, wenn sich vor dem SX-GATE ein NAT-Router befinden, der andernfalls bei längeren Pausen die Verbindung für eingehende Pakete schließt.



Die gesendeten Pakete werden von der Gegenstelle nicht beantwortet.

14.1.2.6-B Verbindungen

Gegenstellen

Um ein neues VPN über diese Wireguard-Schnittstelle einzurichten, legen Sie hier einen neuen Eintrag an. Folgende Werte sind zu konfigurieren:

Name bzw. Gruppe/Name

Dient zu Ihrer Information. Nutzen Sie das Trennzeichen '/' zur Gruppierung wenn Sie sehr viele Verbindungen konfigurieren müssen.

Adresse der Gegenstelle und Port

Wenn konfiguriert, versucht SX-GATE die Verbindung aktiv zu initiieren (Wireguard-Parameter "Endpoint").

Client-IP bzw. entfernte Netze

Tragen Sie hier die IP oder das Netz ein, mit dem verschlüsselt kommuniziert werden soll. Pakete zu diesen Adressen werden dann vom SX-GATE in das VPN geroutet. Aus dem VPN werden nur Pakete mit passender IP akzeptiert (Wireguard-Parameter "AllowedIPs").



Um mehrere Netze zu konfigurieren, legen Sie bitte im Menü "Definitionen > IP-Objekte" eine IP-Gruppe an und wählen Sie diese anschließend hier aus.

Preshared Key

Das VPN kann zusätzlich über einen symmetrischen Schlüssel gesichert werden. Beide Kommunikationspartner nutzen hier den gleichen Wert. Anders als der öffentliche Schlüssel muss dieser Schlüssel auf einem vertraulichen Kanal ausgetauscht werden.

Öffentlicher Schlüssel

Geben Sie hier den öffentlichen Schlüssel der Gegenstelle ein.

Neue Verbindung zu Client anlegen mit Konfigurationsexport für Client

Mit diesem Assistenten legen Sie eine neue Verbindung zu einem Client wie z.B. einem Smartphone oder PC an und können zugleich eine passende Konfiguration für diesen Client exportieren. Für mobile Endgeräte kann die Konfiguration als QR-Code angezeigt werden. Alternativ wird eine Wireguard-Konfigurationsdatei (*.conf) angeboten.



Für jeden Client muss eine eigene Verbindung konfiguriert werden.

Einstellungen für den lokalen SX-GATE

Die Einstellungen auf dieser Seite werden in die Liste der Wireguard-Verbindungen des lokalen SX-GATES eingetragen. Einzelne Einstellungen werden zudem auch Teil der exportierten Konfiguration für die Gegenstelle.

Verbindungsname bzw. Gruppe/Name

Client-IP für Kommunikation via Wireguard

Tragen Sie hier die IP ein, die der Client innerhalb der verschlüsselten Wireguard-Verbindung nutzen soll (auf dem Client: Wireguard-Parameter "Address"). Pakete zu dieser Adresse werden vom SX-GATE in das VPN geroutet. Aus dem VPN werden nur Pakete mit dieser IP akzeptiert (auf dem SX-GATE: Wireguard-Parameter "AllowedIPs").



Konfigurieren Sie bitte für jeden Client eine individuelle, anderweitig ungenutzten IP-Adresse. Die Adresse darf nicht zu einem anderen lokalen Netzwerk wie z.B. dem LAN gehören.

Preshared Key

Öffentlicher Schlüssel der Gegenstelle

Einstellungen für die Gegenstelle

Auf dieser Seite nehmen Sie Einstellungen für die Gegenstelle vor. Sie werden Teil der exportierten Konfiguration.

Internet-Adresse Ihres lokalen SX-GATES

Die Gegenstelle wird sich später mit der hier konfigurierten Adresse verbinden (Wireguard-Parameter "Endpoint" in der Konfigurationsdatei der Gegenstelle).

Lokale Netze

Tragen Sie hier die lokalen IPs und Netze ein, die die Gegenstelle über das VPN erreichen soll. Pakete zu diesen Ziel-Adressen werden von der Gegenstelle in das VPN geroutet. Aus dem VPN wird die Gegenstelle nur Pakete mit entsprechender Quell-IP akzeptiert (Wireguard-Parameter "AllowedIPs" in der Konfigurationsdatei der Gegenstelle).



Die Gegenstelle kann diese Einstellung nach belieben abändern und so versuchen auch andere Netzwerke anzusprechen. Wenn Sie der Gegenstelle nicht vertrauen, sollten Sie über Firewall-Regeln sicherstellen, dass die Gegenstelle nur die gewünschten Systeme ansprechen kann.

Preshared Key

Der PSK wird im lokalen SX-GATE hinterlegt und an die Gegenstelle übermittelt.

Öffentlicher Schlüssel Ihres lokalen SX-GATES

Der öffentliche Schlüssel Ihres lokalen SX-GATES wird der Gegenstelle übermittelt.

IP-Adresse des Clients

Diese Adresse setzt der Client auf seiner Wireguard-Schnittstelle und verwendet diese innerhalb der verschlüsselten Wireguard-Verbindung (Wireguard-Parameter "Address" in der Konfigurationsdatei der Gegenstelle).

Zuzuweisende DNS-IP

Mit dieser Einstellung können Sie versuchen, der Gegenstelle einen DNS-Server zuzuweisen (Wireguard-Parameter "DNS" in der Konfiguration der Gegenstelle).

Verbindungsspezifischer DNS-Suffix

Optional kann auf dem Client ein verbindungsspezifischer DNS-Suffix gesetzt werden (Domainname im Wireguard-Parameter "DNS" der Konfiguration der Gegenstelle).

Keepalive-Intervall

Mit dieser Einstellung können Sie versuchen, die Keepalive-Funktion auf der Gegenstelle zu aktivieren. Die Gegenstelle sendet dann regelmäßig ein leeres Paket über das VPN, das jedoch nicht beantwortet wird. Das kann erforderlich sein, wenn sich vor der Gegenstelle ein NAT-Router befinden, der andernfalls bei längeren Pausen die Verbindung für eingehende Pakete schließt (Wireguard-Parameter "PersistentKeepalive" in der Konfigurationsdatei der Gegenstelle).

Neue Verbindung zu Router anlegen mit Konfigurationsexport für Gegenstelle

Mit diesem Assistenten legen Sie eine neue Verbindung an und können zugleich eine passende Konfiguration für die Gegenstelle exportieren. Handelt es sich bei der Gegenstelle ebenfalls um einen SX-GATE, empfiehlt sich der Export als verschlüsseltes Installationspaket (*.rin). Für mobile Endgeräte kann die Konfiguration als QR-Code angezeigt werden. Schließlich kann auch eine Wireguard-Konfigurationsdatei (*.conf) exportiert werden.

Einstellungen für den lokalen SX-GATE

Die Einstellungen auf dieser Seite werden in die Liste der Wireguard-Verbindungen des lokalen SX-GATES eingetragen. Einzelne Einstellungen werden zudem auch Teil der exportierten Konfiguration für die Gegenstelle.

Verbindungsname bzw. Gruppe/Name

Dient zu Ihrer Information. Nutzen Sie das Trennzeichen '/' zur Gruppierung wenn Sie sehr viele Verbindungen konfigurieren müssen.

Adresse der Gegenstelle

Wenn Sie hier die IP-Adresse oder den Hostnamen der Gegenstelle konfigurieren und nachfolgend auch einen Port konfigurieren, versucht SX-GATE die Verbindung aktiv zu initiieren (Wireguard-Parameter "Endpoint").

zugehöriger Port (bei fester IP)

Wird ignoriert, wenn die Option "dynamisch" bei "Adresse der Gegenstelle" aktiviert ist (wird in der lokalen Wireguard-Konfiguration bei "Endpoint" verwendet, in der Konfigurationsdatei der Gegenstelle als "ListenPort" eingetragen).

Entfernte Netze

Tragen Sie hier das Netz ein, mit dem verschlüsselt kommuniziert werden soll. Pakete zu diesen Adressen werden dann von diesem SX-GATE in das VPN geroutet. Aus dem VPN werden nur Pakete mit passender IP akzeptiert (Wireguard-Parameter "AllowedIPs").



Um mehrere Netze zu konfigurieren, legen Sie bitte im Menü "Definitionen > IP-Objekte" eine IP-Gruppe an und wählen Sie diese anschließend hier aus.

Preshared Key

Das VPN kann zusätzlich über einen symmetrischen Schlüssel gesichert werden. Beide Kommunikationspartner nutzen hier den gleichen Wert. Anders als der öffentliche Schlüssel muss dieser Schlüssel auf einem vertraulichen Kanal ausgetauscht werden.

Öffentlicher Schlüssel der Gegenstelle

Die neue Verbindung wird im lokalen SX-GATE mit dem öffentlichen Schlüssel der Gegenstelle verknüpft. Der dazugehörige private Schlüssel wurde neu generiert und ist Teil der exportierten Konfiguration.

Einstellungen für die Gegenstelle

Auf dieser Seite nehmen Sie Einstellungen für die Gegenstelle vor. Sie werden Teil der exportierten Konfiguration.

Kommentar

Dieser Wert ist nur im Installationspaket für SX-GATE enthalten.

Internet-Adresse Ihres lokalen SX-GATES

Die Gegenstelle wird sich später mit der hier konfigurierten Adresse verbinden (Wireguard-Parameter "Endpoint" in der Konfigurationsdatei der Gegenstelle).

Lokale Netze

Tragen Sie hier die lokalen IPs und Netze ein, die die Gegenstelle über das VPN erreichen soll. Pakete zu diesen Ziel-Adressen werden von der Gegenstelle in das VPN geroutet. Aus dem VPN wird die Gegenstelle nur Pakete mit entsprechender Quell-IP akzeptiert (Wireguard-Parameter "AllowedIPs" in der Konfigurationsdatei der Gegenstelle).



Die Gegenstelle kann diese Einstellung nach belieben abändern und so versuchen auch andere Netzwerke anzusprechen. Wenn Sie der Gegenstelle nicht vertrauen, sollten Sie über Firewall-Regeln sicherstellen, dass die Gegenstelle nur die gewünschten Systeme ansprechen kann.

Preshared Key

Der PSK wird im lokalen SX-GATE hinterlegt und an die Gegenstelle übermittelt.

Öffentlicher Schlüssel Ihres lokalen SX-GATES

Der öffentliche Schlüssel Ihres lokalen SX-GATES wird der Gegenstelle übermittelt.

Zuzuweisende IPv4-Adresse

Mit dieser Einstellung können Sie versuchen, der Gegenstelle eine IP-Adresse zuzuweisen (Wireguard-Parameter "Address" in der Konfigurationsdatei der Gegenstelle).

Zuzuweisende IPv6-Adresse

Mit dieser Einstellung können Sie versuchen, der Gegenstelle eine IPv6-Adresse zuzuweisen (Wireguard-Parameter "Address" in der Konfigurationsdatei der Gegenstelle).

Zuzuweisende DNS-IP

Mit dieser Einstellung können Sie versuchen, der Gegenstelle einen DNS-Server zuzuweisen (Wireguard-Parameter "DNS" in der Konfigurations der Gegenstelle).

Verbindungsspezifischer DNS-Suffix

Optional kann auf dem Client ein verbindungsspezifischer DNS-Suffix gesetzt werden (Domainname im Wireguard-Parameter "DNS" der Konfigurations der Gegenstelle).

Keepalive-Intervall

Mit dieser Einstellung können Sie versuchen, die Keepalive-Funktion auf der Gegenstelle zu aktivieren. Die Gegenstelle sendet dann regelmäßig ein leeres Paket über das VPN, das jedoch nicht beantwortet wird. Das kann erforderlich sein, wenn sich vor der Gegenstelle ein NAT-Router befinden, der andernfalls bei längeren Pausen die Verbindung für eingehende Pakete schließt (Wireguard-Parameter "PersistentKeepalive" in der Konfigurationsdatei der Gegenstelle).

14.1.2.7 OpenVPN Client (ovpnc)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.7-A OpenVPN Server.....	356
14.1.2.7-B Authentifizierung.....	358
14.1.2.7-C Verschlüsselung.....	359

14.1.2.7-A OpenVPN Server**Beschreibung**

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Server

Geben Sie hier Namen oder IP-Adresse des OpenVPN-Servers ein.

OpenVPN-Protokoll

OpenVPN kann die Nutzdaten entweder in UDP- oder in TCP-Pakete verpacken. Bitte stellen Sie hier das Protokoll ein, das der Server verwendet.

Port

Tragen Sie hier den Port ein, unter dem der OpenVPN-Server erreichbar ist.

Zusätzliche Prüfung des Server-Zertifikats

Zum Schutz vor Man-in-the-Middle-Attacken sollten die Daten des Server-Zertifikats einer zusätzlichen Überprüfung unterzogen werden.

Zertifikats-Typ "Server"

In dieser Einstellung wird die Verbindung nur dann aufgebaut, wenn das Server-Zertifikat ein nsCertType-Attribut mit dem Wert "server" enthält.



Zertifikate die mit SX-GATEs CA ausgestellt werden, enthalten dieses Attribut nicht. Wählen Sie daher diese Option nicht, wenn der Server ein solches Zertifikat nutzt.

Zertifikats-Verwendungszweck "Server"

In dieser Einstellung wird die Verbindung nur dann aufgebaut, wenn das Server-Zertifikat ein keyUsage-Attribut mit dem Wert "digitalSignature" sowie entweder "keyEncipherment" oder "keyAgreement" enthält. Zusätzlich muss ein extendedKeyUsage-Attribut mit dem Wert "TLS Web Server Authentication" enthalten sein.

Zertifikats-ID

Geben Sie hier die Zertifikats-Daten (subject) des Server-Zertifikats ein. Eine Verbindung ist nur dann möglich, wenn das Server-Zertifikat genau diese Daten enthält. Alternativ ist auch nur die Angabe des Common Names (CN) möglich.

Komprimierung

Wenn der Server die Option "compress" oder "comp-lzo" nutzt, muss diese auch auf dem Client aktiviert werden.

Installationspaket oder Konfigurationsdatei importieren

Nutzen Sie diesen Assistenten um einen privaten Schlüssel mit zugehörigem Zertifikat und CA-Zertifikat zu importieren. Es lassen sich sowohl PKCS#12-Dateien (*.p12, *.pfx), SX-GATE OpenVPN-Installationspakete für Windows (*.exe) also auch OpenVPN-Konfigurationsdateien mit eingebetteten Schlüsseln (*.ovpn) importieren. Bei den beiden letzteren werden die OpenVPN-Konfigurationsparameter gleich mit abgeglichen.



Der importierte Schlüssel und die Zertifikate sind nicht Bestandteil des SX-GATE Backups. Bitte bewahren Sie die für den Import genutzte Datei als Backup auf. Da diese einen privaten Schlüssel enthält, ist für entsprechenden Schutz zu sorgen.

Datei auswählen

Wählen Sie hier bitte das Installationspaket oder die PKCS#12-Datei aus. Im Installationspaket ist neben einer Datei mit Konfigurationsparametern ebenfalls eine PKCS#12-Datei enthalten. Dabei handelt es sich um eine passwortgeschützte Datei mit einem RSA-Schlüsselpaar. Um die PKCS#12-Datei öffnen zu können, müssen Sie das zugehörige Kennwort eingeben.

Zertifikat prüfen

Prüfen Sie hier noch einmal das Zertifikat, bevor es installiert wird.

Lesen Sie bitte weiter bei [OpenVPN-Client Zertifikat importiert](#)

CA-Zertifikat auswählen

Das Zertifikat muss ergänzt werden um die Zertifikate eventueller Zwischen-Zertifizierungsstellen (Intermediate CAs) bis zum Wurzel-Zertifikat (Root CA). Alle Zertifikate müssen im PEM- oder im DER-Format vorliegen. Sie erhalten die Zertifikate von Ihrer Zertifizierungsstelle.

CA-Zertifikat prüfen

Das hochgeladene Zertifikat wird an die Zertifizierungs-Kette angehängt.

Lesen Sie bitte weiter bei [CA-Zertifikat auswählen](#)

OpenVPN-Client Zertifikat importiert

Das Schlüsselpaar wurde importiert.

14.1.2.7-B Authentifizierung

Zertifikat

SX-GATE authentifiziert OpenVPN-Verbindungen grundsätzlich über Zertifikate. Normalerweise werden dabei die Zertifikate verwendet, die unter "Module > Netzwerk" auf den Reitern "VPN Zertifikat" und "Vertrauenswürdige VPN CA" hinterlegt sind. Alternativ können Sie auch individuelles Schlüsselmateriale für diese OpenVPN-Verbindung auswählen. Wählen Sie dazu einen der Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.

14.1.2.7-C Verschlüsselung

Verschlüsselungsverfahren

Wählen Sie hier das auf dem Server konfigurierte Verschlüsselungsverfahren aus. Dadurch wird festgelegt, wie die zu übertragenden Daten geschützt werden. Diese Einstellung entspricht den OpenVPN-Konfigurationsparametern "cipher" sowie ggf. "keysize".



Zusätzlich akzeptiert SX-GATE die Zuweisung von Verschlüsselungsverfahren durch den Server. Akzeptiert wird AES-GCM mit 128, 192 oder 256 Bit (Konfigurationsparameter "ncp-ciphers").

Hashverfahren

Wählen Sie hier das auf dem Server konfigurierte Hashverfahren zur Authentifizierung der einzelnen Datenpakete aus (HMAC). Dies entspricht dem OpenVPN-Konfigurations-Parameter "auth".



Bei AES-GCM-Verschlüsselung wird dieser Parameter für die Nutzdatenübertragung nicht benötigt. Für die Sicherung des Steuerkanals wird der Parameter ausschließlich bei "tls-auth" benötigt.

Sicherung des Steuerkanals

Wählen Sie die passende Option, wenn der Server dies erfordert.

TLS-Auth/TLS-Crypt Schlüssel

Tragen Sie hier den Schlüssel für tls-auth bzw. tls-crypt ein. Der Schlüssel besteht aus mehreren Zeilen. Es müssen sowohl die Startzeile "-----BEGIN OpenVPN Static key V1-----" als auch die Endzeile "-----END OpenVPN Static key V1-----" enthalten sein.

14.1.2.8 OpenVPN Server (ovpns)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.8-A VPN-Tunnel.....	360
14.1.2.8-B Authentifizierung.....	362
14.1.2.8-C Verschlüsselung.....	363
14.1.2.8-D DHCP-Optionen.....	364

14.1.2.8-A VPN-Tunnel

Beschreibung

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

OpenVPN-Protokoll

OpenVPN kann die Nutzdaten entweder in UDP- oder in TCP-Pakete verpacken. UDP gilt zwar als das performantere Protokoll, bei Verwendung von TCP gibt es jedoch seltener Probleme, z.B. mit Firewalls oder Fragmentierung. Unter Umständen lässt sich mit TCP sogar eine Verbindung über einen Web-Proxy aufbauen.



Wenn Sie eine zweite OpenVPN-Server-Schnittstelle anlegen, in der das andere Protokoll eingestellt ist, kann der Client das Protokoll frei wählen.

Port

Tragen Sie hier den Port ein, unter dem der OpenVPN-Server erreichbar ist.



Sollten Sie sich gegen den Standard-Port 1194 entscheiden, müssen Sie in der Firewall-Konfiguration eine entsprechende Protokoll-Definition anlegen.



Falls Sie mehrere OpenVPN-Server-Schnittstellen anlegen, müssen sich diese entweder im Protokoll oder im Port unterscheiden.

IPv4 Transfernetz

Über diesen Parameter legen Sie den Adress-Bereich fest, aus dem den Clients IPv4-Adressen zugewiesen werden. Das konfigurierte Netzwerk darf noch nicht anderweitig in Gebrauch sein. Wir empfehlen die Verwendung eines Teilnetzes aus den gemäß RFC-1918 für privaten Gebrauch reservierten Netzen (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).



Sollten Sie mehrere OpenVPN-Server-Schnittstellen angelegt haben, dürfen diese nicht die selben Adressbereiche verwenden.

Die Anzahl der Adressen legt zugleich fest, wie viele Clients sich gleichzeitig verbinden können. Dabei gilt die Formel: $\text{Anzahl Adressen} / 4 - 2 = \text{Anzahl Verbindungen}$. Bei der Netzmaske 255.255.255.0 entspricht dies $256 / 4 - 2 = 62$ Verbindungen.

IPv6 Transfernetz

Über diesen Parameter legen Sie den Adress-Bereich fest, aus dem den Clients IPv6-Adressen zugewiesen werden. Das konfigurierte Netzwerk darf noch nicht anderweitig in Gebrauch sein. Die Vergabe eines vollen /64-Adressblocks wird empfohlen, ist jedoch nicht zwingend erforderlich.



Sollten Sie mehrere OpenVPN-Server-Schnittstellen angelegt haben, dürfen diese nicht die selben Adressbereiche verwenden.

Zugriff nur für freigegebene Zertifikate

Sobald diese Option aktiviert ist, dürfen sich nur noch Clients verbinden, deren Zertifikat unter "Client-spezifische Parameter" freigegeben ist.

Veröffentlichte lokale Netzwerke

In der Regel bezieht ein OpenVPN-Client die VPN-Netzwerk-Konfiguration automatisch. Über diesen Parameter werden ihm die relevanten lokalen Netzwerke mitgeteilt.



Der Client ist nicht an diese Weisung gebunden und kann nach belieben andere Netze über das VPN routen.

14.1.2.8-B Authentifizierung

Benutzeranmeldung

Sobald diese Option aktiviert ist, müssen sich alle Clients mit ihrem SX-GATE-Benutzernamen anmelden. Wir empfehlen, ein Verfahren mit zeitbasiertem Einmal-Passwort (TOTP) zu nutzen. Einmal-Passwörter werden in der Benutzerverwaltung je Benutzer aktiviert.



Anmelden können sich ausschließlich Benutzer, die Mitglied der Gruppe "system-ras" sind.

Benutzerpasswort

Als Passwort muss das für den Benutzer in der SX-GATE-Benutzerverwaltung hinterlegte Kennwort eingegeben werden. Wird die Option nachträglich aktiviert, muss in der Konfiguration des Clients die Option "auth-user-pass" gesetzt werden.

Einmal-Passwort

Als Passwort muss ein Einmal-Passwort (6-stelliger Zahlencode) eingegeben werden, nicht das Benutzerpasswort. Um bei einem OpenVPN-Client nachträglich die Anmeldung zu aktivieren, müssen folgende Zeilen in dessen Konfigurationsdatei ergänzt werden: "auth-user-pass", "auth-nocache" und "reneg-sec 0".

Benutzerpasswort + Einmal-Passwort

In dieser Einstellung wird neben dem Benutzerpasswort auch ein Einmal-Passwort abgefragt. Wird diese Option zu einem späteren Zeitpunkt ausgewählt, müssen in Clients die folgenden Option konfiguriert werden: "auth-user-pass", "auth-nocache", "static-challenge PIN 1" und "reneg-sec 0".

Sicherung des Steuerungskanals

Sobald diese Option aktiviert und ein zugehöriger Schlüssel generiert ist, wird der Steuerungskanal zusätzlich verschlüsselt und die übermittelten Nachrichten authentifiziert. Dies schützt vor Denial-of-Service Angriffen, verschlüsselt den TLS-Handshake inklusive der dabei übermittelten Zertifikate und macht den Datenverkehr schwerer als OpenVPN identifizierbar.



Auf allen Clients muss der selbe Schlüssel konfiguriert sein.

14.1.2.8-C Verschlüsselung

Verschlüsselungsverfahren

Wählen Sie hier das Verschlüsselungsverfahren aus, mit dem die zu übertragenden Daten geschützt werden. Diese Einstellung entspricht den OpenVPN-Konfigurationsparametern "cipher" und "ncp-cipher".

Zusätzlich akzeptiertes, altes Verschlüsselungsverfahren

Wählen Sie hier das Verschlüsselungsverfahren aus, das von OpenVPN-Clients mit Version 2.3 oder älter bzw. von OpenVPN-Clients mit alter Konfiguration genutzt wird. Der gewählte Algorithmus wird an den OpenVPN-Konfigurationsparameter "ncp-cipher" angehängt.



Algorithmen mit CBC sollten nicht mehr genutzt werden. Bitte stellen Sie dies in der Konfiguration des Clients auf AES-GCM um (z.B. "cipher AES-256-GCM").

Zugehöriges Hashverfahren

Wählen Sie hier das Hashverfahren aus, das zur Authentifizierung der einzelnen Datenpakete genutzt werden soll (HMAC). Dies entspricht dem OpenVPN-Konfigurations-Parameter "auth".



Für AES-GCM wird dieser Parameter nicht benötigt.

TLS-Protokoll

Wählen Sie hier die TLS-Verschlüsselungsstärke aus.



Im Rahmen der Produktpflege werden die mit der jeweiligen Auswahl verbundenen Parameter von Zeit zu Zeit angepasst.

veraltet

Um Kompatibilität mit älteren Clients zu gewährleisten, werden in dieser Einstellung AES-Algorithmen mit dem nicht mehr empfohlenen Cipher-Block-Chaining CBC und dem veralteten Hash-Algorithmus SHA1 aktiviert. Die minimale TLS-Version ist 1.0.

kompatibel

Wählen Sie diese Einstellung für weitreichende Kompatibilität mit älteren Client-Systemen. Der veraltete Hash-Algorithmus SHA1 ist dabei aktiviert. Die minimale TLS-Version ist 1.2.

aktuell

In dieser Einstellung werden nur noch halbwegs aktuelle Client-Systeme unterstützt. Es wird mindestens TLS 1.2 vorausgesetzt. Wählen Sie diese Option für hohe Sicherheit.

maximal

Erfordert TLS 1.3.

14.1.2.8-D DHCP-Optionen

Als DNS-Server zuweisen

Mit dieser Einstellung können Sie festlegen, welchen Namens-Server der Client verwenden soll.

Sekundärer DNS

Bei Bedarf kann hier ein weiterer Name-Server hinterlegt werden.

DNS ausschließlich über OpenVPN

Windows-Clients schicken DNS-Anfragen trotz VPN-Verbindung unter Umständen an DNS-Server, die in anderen Windows-Netzwerkadaptern konfiguriert sind. Aktivieren Sie diese Option, damit OpenVPN unter Windows diese DNS-Anfragen blockiert und Windows somit ausschließlich die per OpenVPN zugewiesenen DNS-Server nutzt.



Nicht-Windows-Systeme ignorieren diese Einstellung.

WINS 1

Hier können Sie den primären WINS-Server festlegen. WINS wird von Windows benötigt, um Rechner netzwerkübergreifend zu finden.

WINS 2

Hier kann ein zweiter WINS-Server eingetragen werden.

DNS-Suffix

Hier können Sie einstellen, welcher Domain-Suffix dem Client für die Verbindung zugewiesen wird.

14.1.2.9 OpenVPN Server (ovpns) - Client-spezifische Parameter

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Zertifikatsbezeichner des Clients

Einträge sind in diesem Bereich nur dann notwendig, wenn über OpenVPN eine Netzwerk-Netzwerk-Koppelung vorgenommen werden soll. In diesem Fall muss OpenVPN Routen zu den Netzwerken konfigurieren, die sich hinter der Gegenstelle befinden.

Die Zuordnung der Netze zu den einzelnen Clients erfolgt anhand des Zertifikats mit dem sich der Client ausweist. Das Feld "Common Name" (CN) ist dabei ausschlaggebend. Tragen Sie dessen Wert hier ein.

Zugewiesenes IPv4-Transfernetz

In der Konfiguration der Server-Schnittstelle wurde ein Adress-Bereich festgelegt, aus dem jedem Client dynamisch ein Transfer-Netzwerk zugewiesen wird. Soll einem Client ein festes IPv4-Transfer-Netzwerk und damit eine feste IPv4-Adresse zugeordnet werden, können Sie dies hier einstellen.



Mit der von Ihnen angegebenen IP-Adresse legen Sie fest, welches Transfer-Netz dem Client zugeordnet wird. Der Client erhält grundsätzlich die dritte IP-Adresse aus dem Transfer-Netzwerk. Um die Client-Adresse zu berechnen, gehen Sie bitte folgendermaßen vor: Ist die letzte Zahl der IP-Adresse nicht durch vier teilbar, so ersetzen Sie diese bitte durch die nächst kleinere durch vier teilbare Zahl. Addieren Sie zwei und Sie erhalten die dem Client zugewiesene IP-Adresse.



Das Transfer-Netz darf nicht anderweitig in Verwendung sein. Insbesondere darf es nicht Teil des Adress-Bereichs sein, aus dem die dynamisch zugewiesenen Transfer-Netze stammen.

Zugewiesene IPv6-IP

In der Konfiguration der Server-Schnittstelle wurde ein Adress-Bereich festgelegt, aus dem jedem Client dynamisch ein Transfer-Netzwerk zugewiesen wird. Soll einem Client eine feste IPv6-Adresse zugeordnet werden, können Sie dies hier einstellen. Als Transfer-Netzwerk wird das zur konfigurierten IP-Adresse passende /64-Netzwerk konfiguriert.



Die IPv6-Adresse darf nicht anderweitig in Verwendung sein. Insbesondere darf sie nicht Teil des Adress-Bereichs sein, aus dem die dynamisch zugewiesenen Transfer-Netze stammen. Die festen IPv6-Adressen mehrerer Clients der selben OpenVPN-Schnittstelle dürfen zum selben Netzwerk gehören.

Entfernte Netzwerke

Geben Sie hier die Netzwerke an, die zum Client geroutet werden sollen.

14.1.2.10 IPSec VPN (ipsec)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.10-A Gemeinsame Einstellungen.....	367
14.1.2.10-B Dynamische Gegenstellen.....	367
14.1.2.10-C Priorisierung.....	369

14.1.2.10-A Gemeinsame Einstellungen

Beschreibung

Dieses Feld steht für Dokumentationszwecke zu Ihrer freien Verfügung.

Basisschnittstelle

Hier ist die Schnittstelle eingestellt, mit der die ipsec-Schnittstelle verknüpft ist. Damit wird der Basis-Schnittstelle VPN-Funktionalität verliehen. Über eine ipsec-Schnittstelle können beliebig viele VPN-Verbindungen aufgebaut werden.



Jede Basisschnittstelle kann jeweils nur von einer IPSec-Schnittstelle verwendet werden.

Internet / dynamische IP

Diese Option ist nur bei Schnittstelle ipsec0 verfügbar. Sofern die Basisschnittstelle über eine dynamische IP-Adresse an das Internet angebunden ist, muss diese Einstellung gewählt werden.

14.1.2.10-B Dynamische Gegenstellen

Gemeinsame Passphrase (Preshared-Key)

Wenn Verbindungen zu Gegenstellen mit dynamischer IP-Adresse genutzt werden, muss für alle Verbindungen die über eine gemeinsame Passphrase authentifiziert werden die selbe Passphrase verwendet werden. Eine eindeutige Authentifizierung der Gegenstelle ist somit nicht möglich. Eine spätere Änderung der Passphrase erfordert damit z.B. die Änderung bei allen Kommunikationspartnern mit denen kommuniziert wird. Es empfiehlt sich daher die Authentifizierung über Zertifikate.

Um für die erwartete Sicherheit der VPN-Verbindung zu sorgen, sollte die Passphrase im Gegensatz zu einem üblichen Passwort möglichst lang sein, unterschiedliche Zeichen enthalten (Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen) und am besten nicht aus normalen Wörtern bestehen die in einem Wörterbuch zu finden sind. Sind diese Bedingungen erfüllt, wird abhängig von den verwendeten Verschlüsselungs- und Hash-Algorithmen folgende Mindestlänge für den Preshared-Key empfohlen:

Verschlüsselung	Hash	Anzahl Zeichen
3DES	MD5 / SHA1	14
AES-128	SHA2-256	22
AES-256	SHA2-512	43

IKEv1 IKE-Proposals (Phase 1)

Mit dieser Einstellung wird die Kombination aus Verschlüsselungsalgorithmus, Hashverfahren und Diffie-Hellman-Gruppe festgelegt, mit deren Hilfe die Kommunikation zwischen den IKE-Servern gesichert wird.



Sind keinerlei Proposals vorgegeben, werden alle Proposals akzeptiert, mit denen der SX-GATE umgehen kann.

Die hier eingetragenen Proposals werden für Verbindungen zu Gegenstelle mit dynamischer IP-Adresse verwendet. Dies beinhaltet grundsätzlich alle Client-Verbindungen. Eine individuelle Zuweisung ist für diese Kommunikationspartner nicht möglich, da zu Beginn der Phase 1 im Mainmode noch keine Informationen über die Identität der Gegenstelle zur Verfügung stehen.

IKEv2 IKE-Proposals (Phase 1)

Mit dieser Einstellung wird die Kombination aus Verschlüsselungsalgorithmus, Hashverfahren und Diffie-Hellman-Gruppe festgelegt, mit deren Hilfe die Kommunikation zwischen den IKE-Servern gesichert wird.



Sind keine Proposals vorgegeben, werden alle möglichen Kombinationen aus AES, SHA2 die SX-GATE unterstützt und mindestens Diffie-Hellman Gruppe 14 akzeptiert. Da es sich bei AES-GCM um einen AEAD Algorithmus handelt, der die Verschlüsselung und Authentifizierung in einem Schritt macht, legt die ausgewählte Hash-Funktion hier ausschließlich die pseudozufällige Funktion (PRF) fest.

Die hier eingetragenen Proposals werden für Verbindungen zu Gegenstelle mit dynamischer IP-Adresse verwendet. Dies beinhaltet grundsätzlich alle Client-Verbindungen. Eine individuelle Zuweisung ist für diese Kommunikationspartner nicht möglich, da zu Beginn der Phase 1 im Mainmode noch keine Informationen über die Identität der Gegenstelle zur Verfügung stehen.

14.1.2.10-C Priorisierung

Mit Hilfe dieser Funktion können Datenpakete auf verschiedene Prioritätsklassen aufgeteilt werden. Jeder Klasse ist eine anteilige Mindestbandbreite zugeordnet. Nicht benötigte Bandbreite einer höherpriorioren Klasse steht den nachfolgenden Klassen zur Verfügung.

Aus technischer Sicht wird durch die Regeln das ToS- bzw. DSCP-Feld von IP-Paketen überschrieben. Setzt eine lokale Anwendung bereits das ToS/DSCP-Feld passend, ist keine Regel für ausgehende Pakete notwendig. Bei eingehenden Paketen wird das ToS/DSCP-Feld häufig auf dem Weg durch das Internet verändert, so dass für das eingehende Bandbreitenmanagement üblicherweise Regeln erforderlich sind.



Manche Provider stellen Datenpakete mit gesetztem ToS/DSCP-Feld in Rechnung. Bitte prüfen Sie Ihre Vertragsbedingungen.

Die Mindestbandbreiten werden wie folgt verteilt: Die für VoIP benötigte Bandbreite gemäß Konfiguration wird reserviert und von der insgesamt verfügbaren Bandbreite abgezogen. Von der verbliebenen Bandbreite entfallen 10% auf leere TCP ACK-Pakete, 50% auf hochprioriäre Datenpakete und je 20% auf Pakete mit normaler oder niedriger Priorität.



Für das eingehende Bandbreitenmanagement werden nicht-TCP Pakete grundsätzlich wie hochprioriäre Datenpakete behandelt.

Priorisierung von Verbindungen

Fügen Sie dieser Liste die Signaturen der Datenpakete hinzu, die eine höhere oder niedriger Priorität erhalten sollen. Treffen mehrere Regeln auf ein Datenpaket zu, so wird die Priorität des ersten passenden Eintrags angewendet.

Die einzelnen Eingabefelder haben dabei folgende Bedeutungen:

Protokoll

Legt die IP-Protokoll und Port-Signatur fest. Bei eingehendem Bandbreitenmanagement werden ausschließlich TCP-Protokolle berücksichtigt.



Protokoll-Definitionen werden im Menü "Definitionen > Protokolle" vorgenommen.

Lokale IP/Netzwerk

Auf dieser Seite steht die aus Sicht der gewählten Schnittstelle lokale Adresse. Bei einem ausgehenden Datenpaket entspricht dies der Quell-IP (vor SNAT), bei einem eingehenden Datenpaket der Ziel-IP (vor DNAT).



Wenn Sie die Priorisierung bei DNAT- oder SNAT-Verbindungen auf bestimmte lokale IPs beschränken wollen, sind üblicherweise zwei Regeln erforderlich um beide Verbindungsrichtungen abzudecken: Für eingehende Datenpakete muss eine SX-GATE IP angegeben werden, für ausgehende Datenpakete die interne IP (des LAN-Clients bzw. des per DNAT angesprochenen Servers).

Richtung

Wählen Sie hier bitte aus, in welcher Richtung die Portsignatur des gewählten Protokolls interpretiert wird. Erläutert am Beispiel HTTP bedeutet der Richtungspfeil "-->", der HTTP-Port 80 befindet sich auf der externen Seite. Das ausgehende Bandbreitenmanagement verarbeitet folglich Pakete zu Port 80, das eingehende von Port 80. Wird der entgegengesetzt orientierte Pfeil "<--" gewählt, werden eingehende HTTP-Verbindungen verarbeitet. Pakete zu Port 80 durchlaufen das eingehende Bandbreitenmanagement, Pakete von Port 80 das ausgehende. Der Doppelpfeil "↔" steht für beide Interpretationsrichtungen.

Externe IP/Netzwerk

Auf dieser Seite steht die aus Sicht der gewählten Schnittstelle externe Adresse. Bei einem ausgehenden Datenpaket entspricht dies der Ziel-IP, bei einem eingehenden Datenpaket der Quell-IP.

Priorität

Wählen Sie hier die gewünschte Priorisierung aus.

14.1.2.11 IPSec VPN (ipsec) - Verbindungen

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann

der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Verbindung mit

Wählen Sie hier den Typ der Gegenstelle aus zu der Sie eine Verbindung einrichten wollen.

Server

Ein Server kann entweder eine dynamische oder eine statische IP-Adresse haben. Typischerweise ist das eigentliche Ziel der VPN-Verbindung ein Netzwerk, das hinter diesem Server liegt. Bei dem Server handelt es sich in diesem Falle um ein VPN-Gateway. Für jeden Server ist eine eigene Verbindung einzurichten.

AWS

Optimierte Konfiguration für Verbindungen zu AWS.

Client

Bei einer Client-Verbindung wird von einer dynamischen IP-Adresse ausgegangen. Sie können jedoch auch eine Client-Verbindung definieren, wenn die IP-Adresse tatsächlich statisch ist. Bei diesem Verbindungstyp ist es nicht möglich, einen VPN-Tunnel zu Netzwerken zu erstellen, die sich hinter dem Client befinden. Mit Hilfe einer einzigen Client-Verbindung können alle gleich konfigurierten Clients bedient werden.

Windows IKEv2

Bei diesem Verbindungstyp handelt es sich um eine spezielle Verbindung für Windows Clients mit IKEv2 und Computerzertifikat. Haben Sie eine Windows IKEv2 Verbindung angelegt, können Sie am Ende der Client-Zertifikatsaustellung ein Installationspaket für Windows runterladen.

XAuth Client

Eine XAuth Client-Verbindung entspricht weitestgehend einer Client-Verbindung. Zusätzlich wird jedoch noch eine Benutzerauthentifizierung über die IPSec-Erweiterung "XAuth" angefordert. Abhängig vom Benutzer kann dem Client eine individuelle IP-Adresse zugewiesen werden.

L2TP Client

Dieser Verbindungs-Typ entspricht ebenfalls weitgehend der Client-Verbindung. Der VPN-Tunnel wird hier jedoch ausschließlich für das L2TP-Protokoll zwischen dem Client und dem SX-GATE eingerichtet. Die VPN-Pakete werden entschlüsselt und der darin enthaltene L2TP-Datenstrom an den L2TP-Server des SX-GATE weitergeleitet. Dieser authentifiziert den Benutzer und weist dem Client auf Wunsch eine individuelle IP-Adresse zu. Die Konfiguration des L2TP-Servers erfolgt in der L2TP-Schnittstelle des SX-GATES.

Verbindungsname

Geben Sie hier einen Namen für die VPN-Verbindung an. Dieser Name dient ausschließlich zur Identifikation der Verbindung und kann daher frei vergeben werden.

14.1.2.11.1 Verbindung mit Server

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.11.1-A VPN-Tunnel.....	372
14.1.2.11.1-B Authentifizierung.....	374
14.1.2.11.1-C Verschlüsselung.....	377
14.1.2.11.1-D Optionen.....	379
14.1.2.11.1-E Verbindung.....	380
14.1.2.11.1-F Befehle.....	380

Gegenstelle mit

Legen Sie mit Hilfe dieses Schalters fest, ob die Gegenstelle eine feste oder eine dynamisch IP-Adresse hat. Beim Wechsel auf die Einstellung "fester IP / dyn. DNS" wird als IP-Adresse zunächst "0.0.0.0" angezeigt. Ändern Sie diesen Wert bitte in die korrekte Adresse.

14.1.2.11.1-A VPN-Tunnel**Adresse des VPN-Servers**

Diese Einstellung ist nur dann verfügbar, wenn Sie eine Gegenstelle mit fester IP-Adresse spezifizieren. Geben Sie hier die IP-Adresse der Gegenstelle an. Es ist auch möglich hier einen DNS-Namen anzugeben. Nutzen Sie diese Möglichkeit, wenn die Gegenstelle eine dynamisch IP-Adresse hat, aber mit Hilfe von dynamischem DNS stets unter einem bestimmten Namen erreichbar ist.



Der DNS-Name wird nur einmalig beim Start des VPN-Servers zu einer IP-Adresse aufgelöst. Verfügt die VPN-Basischnittstelle über eine dynamische IP-Adresse, so erfolgt auch nach jedem Verbindungsaufbau der Internet-Wählverbindung ein Neustart des VPN-Servers und damit eine DNS-Auflösung.



Mit Hilfe von dynamischem DNS ist es prinzipiell möglich, eine VPN-Verbindung zwischen zwei VPN-Server zu erstellen, wobei beide eine dynamisch IP-Adresse haben. Aufgrund der Latenzzeit der Aktualisierungen im dynamischen DNS kann es jedoch vorkommen, dass die Kommunikationspartner nicht mehr zusammenfinden. In diesem Falle ist ein VPN-Neustart von einem der Partner erforderlich.

Entfernte Netzwerke

Geben Sie hier die Netzwerke an, mit denen Sie eine VPN-Verbindung erstellen wollen. Um die Verbindung zu einem einzelnen Rechner zu erstellen, geben Sie bitte dessen IP-Adresse ein. Wenn keine entfernten Netzwerke angegeben sind, werden ausschließlich VPN-Verbindungen zum entfernten Server selbst aufgebaut.

Lokale Netzwerke

Geben Sie hier die lokalen Netzwerke an, mit denen Sie eine VPN-Verbindung erstellen wollen. Um die Verbindung zu einem einzelnen Rechner zu erstellen, geben Sie bitte dessen IP-Adresse ein. Wenn keine lokalen Netzwerke angegeben sind, werden ausschließlich VPN-Verbindungen zum SX-GATE selbst aufgebaut.

Tunnel SX-GATE <-> entfernter Server

Wenn Sie lokale oder entfernte Netzwerke angegeben haben, besteht zunächst keine VPN-Verbindung zwischen SX-GATE selbst mit seiner externen IP-Adresse und der Gegenstelle selbst mit deren externer IP-Adresse. Aktivieren Sie diesen Schalter, um diese Verbindung hinzuzufügen.

Tunnel SX-GATE <-> entfernte Netzwerke

Wenn Sie sowohl lokale als auch entfernte Netzwerke angegeben haben, bestehen zunächst ausschließlich Verbindungen zwischen diesen Netzen. Aktivieren Sie diesen Schalter um zusätzlich eine Verbindung zwischen der externen IP-Adresse von SX-GATE selbst und den entfernten Netzen zu erstellen.

Tunnel lokale Netzwerke <-> entfernter Server

Wenn Sie sowohl lokale als auch entfernte Netzwerke angegeben haben, bestehen zunächst ausschließlich Verbindungen zwischen diesen Netzen. Aktivieren Sie diesen Schalter um zusätzlich eine Verbindung zwischen der externen IP-Adresse von der Gegenstelle selbst und den lokalen Netzen zu erstellen.

14.1.2.11.1-B Authentifizierung

Authentifizierungsmethode

Wählen Sie hier bitte aus, wie sich die Kommunikationspartner gegenseitig authentifizieren sollen. Zur Verfügung stehen die Authentifizierung mit X.509-Zertifikaten und die Authentifizierung über eine gemeinsame Passphrase (preshared key).

Die Authentifizierung über Zertifikate ist aufgrund des Public-Key-Verfahrens zwar umfangreicher zu konfigurieren, jedoch konzeptionell sicherer. Dabei verfügt jeder Kommunikationspartner über einen privaten Schlüssel der unbedingt geheim zu halten ist sowie einen zugehörigen öffentlichen Schlüssel der nicht besonders geschützt werden muss.

Im Gegensatz dazu entspricht die Authentifizierung über gemeinsame Passphrase einem Kennwort, das beide Kommunikationspartner kennen müssen und das natürlich geheim zu halten ist. Die Bezeichnung Passphrase legt nahe, dass diese länger sein sollte als bei Passwörtern üblich.

bestimmtes Zertifikat

Bei dieser Option muss der öffentliche Schlüssel des VPN-Servers der Gegenstelle in den SX-GATE importiert werden. Nachteil dieses Verfahrens: Wechselt die Gegenstelle ihr Zertifikat, weil das alte z.B. abgelaufen ist, müssen Sie hier zunächst den öffentlichen Schlüssel des neuen Zertifikats importieren, bevor die VPN-Verbindung wieder erfolgreich hergestellt werden kann. Insbesondere bei vielen Gegenstellen wächst der Verwaltungsaufwand schnell.



Beachten Sie bitte, dass Zertifikate nur eine begrenzte Zeit gültig sind (z.B. 1 Jahr).

Zertifikat anhand CA

Dies ist das allgemein übliche und von uns empfohlene Verfahren der zertifikatsbasierenden Authentifizierung. Die Gegenstelle wird akzeptiert, wenn sie sich mit einem Zertifikat ausweist, das von der im SX-GATE als vertrauenswürdig eingestufte Zertifizierungsstelle (CA) ausgestellt wurde. Diese CA wird unter "Module > Netzwerk > Einstellungen" konfiguriert.



Das Zertifikat des SX-GATE VPN-Servers muss ebenfalls von der vertrauenswürdigen CA ausgestellt worden sein. Die Authentifizierung schlägt andernfalls fehl.

Läuft das Zertifikat der Gegenstelle ab, kann es dort jederzeit erneuert werden, ohne dass lokal eine Änderung vorgenommen werden muss. Einzige Voraussetzung bleibt, dass das neue Zertifikat ebenfalls von der vertrauten CA ausgestellt wird.



Mit dem Ablauf des vertrauten CA-Zertifikats hingegen verlieren alle Zertifikate ihre Gültigkeit. Ein CA-Zertifikat ist in der Regel aber deutlich länger gültig (z.B. 10 Jahre).

Passphrase (PSK)

Mit dieser Einstellung entscheiden Sie sich für die Authentifizierung über eine gemeinsame Passphrase. Um die Sicherheit der VPN-Verbindung zu erhöhen, sollte diese möglichst lang sein, unterschiedliche Zeichen enthalten (Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen) und am besten nicht aus normalen Wörtern bestehen die in einem Wörterbuch zu finden sind.



Für alle Gegenstellen mit dynamischer IP muss die selbe gemeinsame Passphrase verwendet werden. Daher ist diese direkt in der ipsec-Schnittstelle und nicht in der Verbindung einzugeben.

Lokale ID

Bei Authentifizierung über Passphrase (Preshared Key) identifizieren sich die Kommunikationspartner in der Regel über ihre externe IP-Adresse. Die Angabe einer abweichenden IP-Adresse, die Identifizierung über Hostnamen oder E-Mail Adressen ist alternativ möglich.

Hier wird die ID eingegeben mit der sich SX-GATE bei der Gegenstelle ausweist.

ID der Gegenstelle (bei PSK)

Bei einer Gegenstelle mit fester IP wird als ID die konfigurierte IP erwartet. Verwendet die Gegenstelle eine andere IP (z.B. weil sie sich hinter einem NAT-Router befindet), einen Hostnamen (FQDN) oder eine E-Mail Adresse (USER@FQDN) als ID, muss dies hier angepasst werden.

Bei einer Gegenstelle mit dynamischer IP ist es sinnvoll, in der Gegenstelle eine feste ID einzustellen und diese hier zu hinterlegen. Sind mehrere Kommunikationspartner in Besitz des selben Preshared Keys, kann so erschwert werden, dass sich die falsche Partei mit dieser Server-Verbindung verbindet.

Passphrase (Preshared Key)

Geben Sie hier den Preshared Key ein, wenn die Authentifizierung über gemeinsame Passphrase ausgewählt wurde. Um für die erwartete Sicherheit der VPN-Verbindung zu sorgen, sollte die Passphrase im Gegensatz zu einem üblichen Passwort möglichst lang sein, unterschiedliche Zeichen enthalten (Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen) und am besten nicht aus normalen Wörtern bestehen die in einem Wörterbuch zu finden sind. Sind diese Bedingungen erfüllt, wird abhängig von den verwendeten Verschlüsselungs- und Hash-Algorithmen folgende Mindestlänge für den Preshared-Key empfohlen:

Verschlüsselung	Hash	Anzahl Zeichen
3DES	MD5 / SHA1	14
AES-128	SHA2-256	22
AES-256	SHA2-512	43



Sofern die Gegenstelle als dynamische IP konfiguriert wurde, kann keine individuelle Passphrase eingestellt werden. Für alle Preshared-Key-Verbindungen der Schnittstelle bei denen dynamische IP-Adressen involviert sind, gilt die selbe Passphrase. Diese lässt sich eine Menüebene höher auf dem Reiter (Tab) "Dynamische Gegenstellen" einstellen.

ID der Gegenstelle (bei CA basierter Authentifizierung)

Bei IPSec-Server-Verbindungen mit Authentifizierung über vertraute Stammzertifizierungsstelle (CA) ist es sinnvoll, die ID hier anzugeben, mit der sich die Gegenstelle meldet. So kann verhindert werden, dass sich der Besitzer eines beliebigen Zertifikats der vertrauenswürdigen CA als der Server ausgibt. Bei Gegenstellen mit fester IP ist die Angabe der ID verpflichtend. Sollte Ihnen die ID nicht bekannt sein, finden Sie diese z.B. bei einem Verbindungsversuch im Log. Als ID werden die Zertifikatsdaten (Distinguished Name, DN) erwartet. Die Verwendung einer IP-Adresse oder eines DNS-Namens als ID ist hier nicht möglich.



Dieser Wert muss angepasst werden, wenn die Gegenstelle die ID ändert, z.B. weil sie ein neues Zertifikat erhält und der DN des neuen Zertifikats sich von dem des alten Zertifikats unterscheidet.

Öffentlichen Schlüssel importieren

Legen Sie hier den öffentlichen Schlüssel der Gegenstelle fest. Wurde das Zertifikat der Gegenstelle von der lokalen SX-GATE-CA ausgestellt, so kann er von dort kopiert werden. Alternativ muss dieser aus einer Datei im PEM-Format importiert werden.



Hier muss der öffentliche Schlüssel des VPN-Servers der Gegenstelle importiert werden - nicht der öffentliche Schlüssel der ausstellenden Zertifizierungsstelle (CA).

14.1.2.11.1-C Verschlüsselung

Schlüsselaustauschprotokoll

Hier wählen Sie die Art des Protokolls mit dem der Schlüsselaustausch durchgeführt wird.

IKEv1

Es werden in beide Richtungen nur IKEv1 Verbindungen akzeptiert.

IKEv2

Es werden in beide Richtungen nur IKEv2 Verbindungen akzeptiert.

Schlüsseltausch IKE-Server (Phase 1) alle

Wählen Sie hier die Zeitspanne aus, nach der die Schlüssel der an dieser VPN-Verbindung beteiligten Internet-Key-Exchange-Server neu vereinbart wird.

IKEv1 IKE-Proposals (Phase 1)

Mit dieser Einstellung wird die Kombination aus Verschlüsselungsalgorithmus, Hashverfahren und Diffie-Hellman-Gruppe festgelegt, mit deren Hilfe die Kommunikation zwischen den IKE-Servern gesichert wird.



Sind keine Proposals vorgegeben, werden alle möglichen Kombinationen akzeptiert, die SX-GATE unterstützt. Wird eine IKEv1 Verbindung von SX-GATE initiiert, wird AES-256, AES-128 und 3DES in Verbindung mit SHA2-256, SHA2-512 und SHA1 sowie den Diffie-Hellman Gruppen 14 und 5 vorgeschlagen.

IKEv2 IKE-Proposals (Phase 1)

Mit dieser Einstellung wird die Kombination aus Verschlüsselungsalgorithmus, Hashverfahren und Diffie-Hellman-Gruppe festgelegt, mit deren Hilfe die Kommunikation zwischen den IKE-Servern gesichert wird.



Sind keine Proposals vorgegeben, werden alle möglichen Kombinationen aus AES, SHA2 die SX-GATE unterstützt und mindestens Diffie-Hellman Gruppe 14 akzeptiert. Bei ausgehenden Verbindungen erhalten AES_GCM256 und AES_GCM128 den Vorzug, gefolgt von AES-256 und AES-128, in Kombination mit SHA2-512, SHA2-256 und den Diffie-Hellman Gruppen 14, 15, 16, 18, 19, 20, 21 und 31. Da es sich bei AES-GCM um einen AEAD Algorithmus handelt, der die Verschlüsselung und Authentifizierung in einem Schritt macht, legt die ausgewählte Hash-Funktion hier ausschließlich die pseudozufällige Funktion (PRF) fest.

Schlüsseltausch VPN-Verbindung (Phase 2) alle

Wählen Sie hier die Zeitspanne aus, nach der der Schlüssel für die VPN-Datenpakete neu vereinbart wird.

IKEv1 ESP-Proposals (Phase 2)

Mit den Proposals der Phase 2 wird festgelegt, welcher Verschlüsselungsalgorithmus und welches Hashverfahren für die sichere Übermittlung der Daten zulässig sind.



Sind keinerlei Proposals vorgegeben, werden alle Proposals akzeptiert, mit denen SX-GATE umgehen kann. In der Rolle des Initiators werden bei IKEv1 alle Kombinationen aus AES-128 und 3DES mit SHA1 vorgeschlagen.

IKEv2 ESP-Proposals (Phase 2)

Mit den Proposals der Phase 2 wird festgelegt, welcher Verschlüsselungsalgorithmus und welches Hashverfahren für die sichere Übermittlung der Daten zulässig sind. Da AES_GCM ein AEAD-Algorithmus ist, ist kein separates Hashverfahren erforderlich.



Sind keinerlei Proposals vorgegeben, werden alle sicheren Proposals akzeptiert, mit denen SX-GATE umgehen kann.

Perfect-Forward-Secrecy

Perfect forward secrecy (PFS) für Phase 2 erhöht die Sicherheit einer VPN-Verbindung. Kommt ein Angreifer in Besitz der gemeinsamen Passphrase bzw. des privaten Schlüssel der VPN-Verbindung, so ist es ihm bei aktivierter PFS dennoch nicht möglich, eine zuvor aufgezeichnete VPN-Kommunikation zu entschlüsseln. Sie sollten PFS nur dann deaktivieren, wenn es aus Gründen der Interoperabilität mit anderen IPSEC-Implementierungen erforderlich ist.

Bei eingehenden Verbindungen akzeptiert SX-GATE ausschließlich in der Einstellung "deaktiviert" Verbindungen ohne PFS. In allen anderen Einstellungen werden beliebige Diffie-Hellman Gruppen akzeptiert. Initiiert hingegen SX-GATE die Verbindung, wird in der Einstellung "erforderlich" stets die selbe DH-Gruppe wie in Phase 1 verwendet. Für IKEv1 können Sie auch eine bestimmte DH-Gruppe vorgeben, sobald in "IKEv1 ESP-Proposals (Phase 2)" Vorgaben gemacht wurden.

SHA2-256 96bit Draft Version

Bei SHA2-256 wird der ESP Hash normalerweise bei 128 Bits abgeschnitten. Manche IPsec Anwendungen (Linux vor 2.6.33, oder manche Cisco Router) verwenden die Draft Version welche nach 96 Bits abschneidet.

Diese Option aktiviert die 96bits Draft Version, um mit diesen Gegenstellen kompatibel zu sein.

Eine andere Möglichkeit wäre, SHA2-384 oder SHA2-512 zu nutzen.

14.1.2.11.1-D Optionen

Dead-Peer-Detection

Bei aktivierter Dead-Peer-Detection (DPD) wird alle 30 Sekunden geprüft, ob die Gegenstelle noch erreichbar ist. Die Prüfung findet statt, wenn keine Nutzdaten mehr übertragen werden. Antwortet die Gegenstelle nicht mehr, wird die Verbindung nach 120 Sekunden abgebrochen. Falls die Gegenstelle über eine feste IP-Adresse verfügt, wird versucht, eine neue Verbindung herzustellen.



Um diese Funktion nutzen zu können, muss die Gegenstelle ebenfalls DPD gemäß RFC3706 unterstützen.

IPComp Komprimierung

Falls aktiviert, werden die Daten vor der Verschlüsselung komprimiert.



Bei einer eingehenden Verbindung muss die Gegenstelle die selbe Einstellung verwenden, andernfalls wird die Verbindung abgewiesen.

14.1.2.11.1-E Verbindung

Verbindungsaufbau

Legen Sie hier fest, wie der Aufbau der VPN-Verbindung erfolgen soll.

aktiv

Der VPN-Server des SX-GATE versucht aktiv Kontakt mit der Gegenstelle aufzunehmen. Selbstverständlich wird auch auf eingehende Verbindungsanfragen von Seiten der Gegenstelle reagiert. Hat die Gegenstelle eine dynamische IP-Adresse, so steht diese Option nicht zur Verfügung.

passiv

Bei dieser Einstellung wartet SX-GATE bis die Gegenstelle Kontakt aufnimmt.

deaktiviert

Mit dieser Einstellung wird die zugehörige VPN-Verbindung deaktiviert.

Gateway für Routing

Um korrekte Einträge in der Routing-Tabelle vornehmen zu können, müssen Sie hier einstellen, über welches Gateway die Gegenstelle erreichbar ist oder ob sich diese im gleichen Netzwerk-Segment wie SX-GATE befindet.

14.1.2.11.1-F Befehle

Aktion

Sie haben hier die Möglichkeit, den Verbindungszustand von Hand zu ändern.



Mit dem nächsten Neustart des IPSec-Dienstes (z.B. nach Änderung der Konfiguration) wird wieder der auf dem Reiter (Tab) "Verbindung" konfigurierte Verbindungszustand hergestellt.

Verbindung neu aufbauen

Sofern die Verbindung aktiv ist, wird diese zunächst getrennt. Anschließend wird die Verbindung neu aufgebaut. Ein Protokoll des Verbindungsaufbaus wird angezeigt.

Auf eingehende Verbindungen warten

Eine bestehende Verbindung wird getrennt. SX-GATE wartet bis die Gegenstelle die Verbindung neu aufbaut.

Verbindung deaktivieren

Eine bestehende Verbindung wird getrennt. Ein Verbindungsaufbau ist bis auf weiteres nicht möglich.

14.1.2.11.2 Verbindung mit AWS

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.11.2-A VPN-Tunnel.....	381
14.1.2.11.2-B Authentifizierung.....	382
14.1.2.11.2-C Verschlüsselung.....	384
14.1.2.11.2-D Optionen.....	386
14.1.2.11.2-E Verbindung.....	387
14.1.2.11.2-F Befehle.....	387

14.1.2.11.2-A VPN-Tunnel

Um ein VPN zwischen SX-GATE und AWS zu konfigurieren, sind AWS-seitig folgende Parameter zu konfigurieren:

- Statisches Routing
- Das lokale IPv4 Netzwerk aus Sicht von AWS muss der Einstellung "AWS Netzwerk" auf dem SX-GATE entsprechen
- Das entfernte IPv4 Netzwerk aus Sicht von AWS muss der Einstellung "Lokales Netzwerk" auf dem SX-GATE entsprechen

AWS Virtual-Private-Gateway (VPG) IP 1

Geben Sie hier die erste IP-Adresse des Virtual-Private-Gateways (VPGs) ein.

AWS Virtual-Private-Gateway (VPG) IP 2

Geben Sie hier die zweite IP-Adresse des Virtual-Private-Gateways (VPGs) ein.

AWS Netzwerk

Geben Sie hier das Netzwerk ein, das für die Virtual-Private-Cloud (VPC) vergeben wurde, zu der Sie sich verbinden wollen.

Lokales Netzwerk

Geben Sie hier das lokale Netzwerke ein, das das VPN nutzen darf.

Um mehreren Netzen den Zugriff zu ermöglichen, müssen Sie diese mit Hilfe einer geeignet gewählten Netzmaske in einem Netzwerk zusammenfassen (z.B. "192.168.0.0/16" für alle beliebigen 192.168er Netze). Im Extremfall können Sie hier auch "0.0.0.0/0" eingeben.

Alternativ können Sie auch mit SNAT arbeiten. Konfigurieren Sie dazu hier ein beliebiges Netzwerk. Es kann sich um ein real genutztes lokales Netzwerk handeln, Sie können aber auch ein bislang ungenutztes Netzwerk eintragen. In den Firewall-Regeln der ipsec-Schnittstelle konfigurieren Sie dann SNAT-Regeln, die die gewünschten lokalen Netze auf das hier konfigurierte Netzwerk abbilden.

14.1.2.11.2-B Authentifizierung**Authentifizierungsmethode**

Wählen Sie hier bitte aus, wie sich die Kommunikationspartner gegenseitig authentifizieren sollen. Zur Verfügung stehen die Authentifizierung mit X.509-Zertifikaten und die Authentifizierung über eine gemeinsame Passphrase (preshared key).

Die Authentifizierung über Zertifikate ist aufgrund des Public-Key-Verfahrens zwar umfangreicher zu konfigurieren, jedoch konzeptionell sicherer. Dabei verfügt jeder Kommunikationspartner über einen privaten Schlüssel der unbedingt geheim zu halten ist sowie einen zugehörigen öffentlichen Schlüssel der nicht besonders geschützt werden muss.

Im Gegensatz dazu entspricht die Authentifizierung über gemeinsame Passphrase einem Kennwort, das beide Kommunikationspartner kennen müssen und das natürlich geheim zu halten ist. Die Bezeichnung Passphrase legt nahe, dass diese länger sein sollte als bei Passwörtern üblich.

bestimmtes Zertifikat

Bei dieser Option muss der öffentliche Schlüssel des VPN-Servers der Gegenstelle in den SX-GATE importiert werden. Nachteil dieses Verfahrens: Wechselt die Gegenstelle ihr Zertifikat, weil das alte z.B. abgelaufen ist, müssen Sie hier zunächst den öffentlichen Schlüssel des neuen Zertifikats

importieren, bevor die VPN-Verbindung wieder erfolgreich hergestellt werden kann. Insbesondere bei vielen Gegenstellen wächst der Verwaltungsaufwand schnell.



Beachten Sie bitte, dass Zertifikate nur eine begrenzte Zeit gültig sind (z.B. 1 Jahr).

Zertifikat anhand CA

Dies ist das allgemein übliche und von uns empfohlene Verfahren der zertifikatsbasierenden Authentifizierung. Die Gegenstelle wird akzeptiert, wenn sie sich mit einem Zertifikat ausweist, das von der im SX-GATE als vertrauenswürdig eingestufte Zertifizierungsstelle (CA) ausgestellt wurde. Diese CA wird unter "Module > Netzwerk > Einstellungen" konfiguriert.



Das Zertifikat des SX-GATE VPN-Servers muss ebenfalls von der vertrauenswürdigen CA ausgestellt worden sein. Die Authentifizierung schlägt andernfalls fehl.

Läuft das Zertifikat der Gegenstelle ab, kann es dort jederzeit erneuert werden, ohne dass lokal eine Änderung vorgenommen werden muss. Einzige Voraussetzung bleibt, dass das neue Zertifikat ebenfalls von der vertrauten CA ausgestellt wird.



Mit dem Ablauf des vertrauten CA-Zertifikats hingegen verlieren alle Zertifikate ihre Gültigkeit. Ein CA-Zertifikat ist in der Regel aber deutlich länger gültig (z.B. 10 Jahre).

Passphrase (PSK)

Mit dieser Einstellung entscheiden Sie sich für die Authentifizierung über eine gemeinsame Passphrase. Um die Sicherheit der VPN-Verbindung zu erhöhen, sollte diese möglichst lang sein, unterschiedliche Zeichen enthalten (Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen) und am besten nicht aus normalen Wörtern bestehen die in einem Wörterbuch zu finden sind.



Für alle Gegenstellen mit dynamischer IP muss die selbe gemeinsame Passphrase verwendet werden. Daher ist diese direkt in der ipsec-Schnittstelle und nicht in der Verbindung einzugeben.

Lokale ID

Bei Authentifizierung über Passphrase (Preshared Key) identifizieren sich die Kommunikationspartner in der Regel über ihre externe IP-Adresse. Die Angabe einer abweichenden IP-Adresse, die Identifizierung über Hostnamen oder E-Mail Adressen ist alternativ möglich.

Hier wird die ID eingegeben mit der sich SX-GATE bei der Gegenstelle ausweist.

Preshared-Key für Virtual-Private-Gateway (VPG) IP 1

Geben Sie hier den Preshared-Key für die Verbindung mit der ersten Virtual-Private-Gateway IP ein.

Preshared-Key für Virtual-Private-Gateway (VPG) IP 2

Geben Sie hier den Preshared-Key für die Verbindung mit der zweiten Virtual-Private-Gateway IP ein.

ID (Zertifikats-DN) von Virtual-Private-Gateway (VPG) IP 1

Geben Sie hier die von der ersten Virtual-Private-Gateway IP genutzten ID ein.

ID (Zertifikats-DN) von Virtual-Private-Gateway (VPG) IP 2

Geben Sie hier die von der zweiten Virtual-Private-Gateway IP genutzten ID ein.

Öffentlichen Schlüssel importieren

Legen Sie hier den öffentlichen Schlüssel der Gegenstelle fest. Wurde das Zertifikat der Gegenstelle von der lokalen SX-GATE-CA ausgestellt, so kann er von dort kopiert werden. Alternativ muss dieser aus einer Datei im PEM-Format importiert werden.



Hier muss der öffentliche Schlüssel des VPN-Servers der Gegenstelle importiert werden - nicht der öffentliche Schlüssel der ausstellenden Zertifizierungsstelle (CA).

14.1.2.11.2-C Verschlüsselung

Schlüsselaustauschprotokoll

Hier wählen Sie die Art des Protokolls mit dem der Schlüsselaustausch durchgeführt wird.

IKEv1

Es werden in beide Richtungen nur IKEv1 Verbindungen akzeptiert.

IKEv2

Es werden in beide Richtungen nur IKEv2 Verbindungen akzeptiert.

Schlüsseltausch IKE-Server (Phase 1) alle

Wählen Sie hier die Zeitspanne aus, nach der die Schlüssel der an dieser VPN-Verbindung beteiligten Internet-Key-Exchange-Server neu vereinbart wird.

IKEv1 IKE-Proposals (Phase 1)

Mit dieser Einstellung wird die Kombination aus Verschlüsselungsalgorithmus, Hashverfahren und Diffie-Hellman-Gruppe festgelegt, mit deren Hilfe die Kommunikation zwischen den IKE-Servern gesichert wird.



Sind keine Proposals vorgegeben, werden alle möglichen Kombinationen akzeptiert, die SX-GATE unterstützt. Wird eine IKEv1 Verbindung von SX-GATE initiiert, wird AES-256, AES-128 und 3DES in Verbindung mit SHA2-256, SHA2-512 und SHA1 sowie den Diffie-Hellman Gruppen 14 und 5 vorgeschlagen.

IKEv2 IKE-Proposals (Phase 1)

Mit dieser Einstellung wird die Kombination aus Verschlüsselungsalgorithmus, Hashverfahren und Diffie-Hellman-Gruppe festgelegt, mit deren Hilfe die Kommunikation zwischen den IKE-Servern gesichert wird.



Sind keine Proposals vorgegeben, werden alle möglichen Kombinationen aus AES, SHA2 die SX-GATE unterstützt und mindestens Diffie-Hellman Gruppe 14 akzeptiert. Bei ausgehenden Verbindungen erhalten AES_GCM256 und AES_GCM128 den Vorzug, gefolgt von AES-256 und AES-128, in Kombination mit SHA2-512, SHA2-256 und den Diffie-Hellman Gruppen 14, 15, 16, 18, 19, 20, 21 und 31. Da es sich bei AES-GCM um einen AEAD Algorithmus handelt, der die Verschlüsselung und Authentifizierung in einem Schritt macht, legt die ausgewählte Hash-Funktion hier ausschließlich die pseudozufällige Funktion (PRF) fest.

Schlüsseltausch VPN-Verbindung (Phase 2) alle

Wählen Sie hier die Zeitspanne aus, nach der der Schlüssel für die VPN-Datenpakete neu vereinbart wird.

IKEv1 ESP-Proposals (Phase 2)

Mit den Proposals der Phase 2 wird festgelegt, welcher Verschlüsselungsalgorithmus und welches Hashverfahren für die sichere Übermittlung der Daten zulässig sind.



Sind keinerlei Proposals vorgegeben, werden alle Proposals akzeptiert, mit denen SX-GATE umgehen kann. In der Rolle des Initiators werden bei IKEv1 alle Kombinationen aus AES-128 und 3DES mit SHA1 vorgeschlagen.

IKEv2 ESP-Proposals (Phase 2)

Mit den Proposals der Phase 2 wird festgelegt, welcher Verschlüsselungsalgorithmus und welches Hashverfahren für die sichere Übermittlung der Daten zulässig sind. Da AES_GCM ein AEAD-Algorithmus ist, ist kein separates Hashverfahren erforderlich.



Sind keinerlei Proposals vorgegeben, werden alle sicheren Proposals akzeptiert, mit denen SX-GATE umgehen kann.

Perfect-Forward-Secrecy

Perfect forward secrecy (PFS) für Phase 2 erhöht die Sicherheit einer VPN-Verbindung. Kommt ein Angreifer in Besitz der gemeinsamen Passphrase bzw. des privaten Schlüssel der VPN-Verbindung, so ist es ihm bei aktivierter PFS dennoch nicht möglich, eine zuvor aufgezeichnete VPN-Kommunikation zu entschlüsseln. Sie sollten PFS nur dann deaktivieren, wenn es aus Gründen der Interoperabilität mit anderen IPSEC-Implementierungen erforderlich ist.

Bei eingehenden Verbindungen akzeptiert SX-GATE ausschließlich in der Einstellung "deaktiviert" Verbindungen ohne PFS. In allen anderen Einstellungen werden beliebige Diffie-Hellman Gruppen akzeptiert. Initiiert hingegen SX-GATE die Verbindung, wird in der Einstellung "erforderlich" stets die selbe DH-Gruppe wie in Phase 1 verwendet. Für IKEv1 können Sie auch eine bestimmte DH-Gruppe vorgeben, sobald in "IKEv1 ESP-Proposals (Phase 2)" Vorgaben gemacht wurden.

14.1.2.11.2-D Optionen

Dead-Peer-Detection

Bei aktivierter Dead-Peer-Detection (DPD) wird regelmäßig geprüft, ob die Gegenstelle noch erreichbar ist. Die Prüfung findet statt, wenn keine Nutzdaten mehr übertragen werden. Antwortet die Gegenstelle nicht mehr, wird die Verbindung abgebaut und versucht, eine Verbindung zur anderen Virtual-Private-Gateway IP aufzubauen.

DPD-Intervall

Zeitabstand, in dem die Verfügbarkeit der Verbindung getestet wird.

DPD-Timeout

Antwortet die Gegenstelle nicht, wird nach der hier konfigurierten Zeitdauer auf die andere VPG-IP gewechselt. Der Wert sollte mindestens dreimal so groß sein wie "DPD-Intervall".

IPComp Komprimierung

Falls aktiviert, werden die Daten vor der Verschlüsselung komprimiert.



Bei einer eingehenden Verbindung muss die Gegenstelle die selbe Einstellung verwenden, andernfalls wird die Verbindung abgewiesen.

14.1.2.11.2-E Verbindung

Verbindungsaufbau

Legen Sie hier fest, wie der Aufbau der VPN-Verbindung erfolgen soll.

aktiv

Der VPN-Server des SX-GATE versucht sich aktiv mit AWS zu verbinden.

passiv

Bei dieser Einstellung wartet SX-GATE bis AWS Kontakt aufnimmt.

deaktiviert

Mit dieser Einstellung wird die zugehörige VPN-Verbindung deaktiviert.

Gateway für Routing

Um korrekte Einträge in der Routing-Tabelle vornehmen zu können, müssen Sie hier einstellen, über welches Gateway die Gegenstelle erreichbar ist oder ob sich diese im gleichen Netzwerk-Segment wie SX-GATE befindet.

14.1.2.11.2-F Befehle

Aktion

Sie haben hier die Möglichkeit, den Verbindungszustand von Hand zu ändern.



Mit dem nächsten Neustart des IPSec-Dienstes (z.B. nach Änderung der Konfiguration) wird wieder der auf dem Reiter (Tab) "Verbindung" konfigurierte Verbindungszustand hergestellt.

Verbindung neu aufbauen

Sofern die Verbindung aktiv ist, wird diese zunächst getrennt. Anschließend wird die Verbindung neu aufgebaut. Ein Protokoll des Verbindungsaufbaus wird angezeigt.

Auf eingehende Verbindungen warten

Eine bestehende Verbindung wird getrennt. SX-GATE wartet bis die Gegenstelle die Verbindung neu aufbaut.

Verbindung deaktivieren

Eine bestehende Verbindung wird getrennt. Ein Verbindungsaufbau ist bis auf weiteres nicht möglich.

14.1.2.11.3 Verbindung mit Client

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.11.3-A VPN-Tunnel.....	388
14.1.2.11.3-B Authentifizierung.....	389
14.1.2.11.3-C Verschlüsselung.....	392
14.1.2.11.3-D Optionen.....	393
14.1.2.11.3-E Verbindung.....	393
14.1.2.11.3-F Befehle.....	393

14.1.2.11.3-A VPN-Tunnel

Lokale Netzwerke

Geben Sie hier die lokalen Netzwerke an, zu denen der Client eine VPN-Verbindung erstellen will. Um die Verbindung zu einem einzelnen Rechner zu erstellen, geben Sie bitte dessen IP-Adresse ein. Wenn keine lokalen Netzwerke angegeben sind, werden ausschließlich VPN-Verbindungen zum SX-GATE selbst aufgebaut.

Tunnel SX-GATE <-> Client

Wenn Sie lokale Netzwerke angegeben haben, besteht zunächst keine VPN-Verbindung zwischen SX-GATE selbst mit seiner externen IP-Adresse und der Gegenstelle. Aktivieren Sie diesen Schalter, um diese Verbindung hinzuzufügen.

Virtuelle IP

Die IKEv1-IPSec-Erweiterung "Mode Config" bzw. der IKEv2 "Addresspool" erlaubt es, dem Client eine IP-Adresse für die IPSec-Kommunikation zuzuweisen. Ohne virtuelle IP-Adresse wird der Client seine eigene (externe) IP für die Kommunikation verwenden.



Bei IKEv2 Clients hinter einem NAT-Router ist ein Addresspool zwingend erforderlich.

Geben Sie hier einen Adressbereich an, aus dem der Client sich seine IP-Adresse bezieht. Die Anzahl der IP-Adressen legt fest, wie viele Clients maximal zur selben Zeit verbunden sein können.

Als DNS-Server zuweisen

Mit dieser Einstellung können Sie festlegen, welchen Namens-Server der Client verwenden soll.

14.1.2.11.3-B Authentifizierung

Authentifizierungsmethode

Wählen Sie hier bitte aus, wie sich die Kommunikationspartner gegenseitig authentifizieren sollen. Zur Verfügung stehen die Authentifizierung mit X.509-Zertifikaten und die Authentifizierung über eine gemeinsame Passphrase (preshared key).

Die Authentifizierung über Zertifikate ist aufgrund des Public-Key-Verfahrens zwar umfangreicher zu konfigurieren, jedoch konzeptionell sicherer. Dabei verfügt jeder Kommunikationspartner über einen privaten Schlüssel der unbedingt geheim zu halten ist sowie einen zugehörigen öffentlichen Schlüssel der nicht besonders geschützt werden muss.

Im Gegensatz dazu entspricht die Authentifizierung über gemeinsame Passphrase einem Kennwort, das beide Kommunikationspartner kennen müssen und das natürlich geheim zu halten ist. Für Client-Verbindungen ist diese Variante eher ungeeignet, da alle Verbindungen mit dynamischen IP-Adressen mit dem selben Preshared Key authentifiziert werden müssen.

bestimmte X.509-Zertifikate

Bei dieser Option muss der öffentliche Schlüssel des VPN-Clients in den SX-GATE importiert werden. Nachteil dieses Verfahrens: Wechselt der Client sein Zertifikat, weil das alte z.B. abgelaufen ist, müssen Sie hier zunächst den öffentlichen Schlüssel des neuen Zertifikats importieren, bevor die VPN-Verbindung wieder erfolgreich hergestellt werden kann. Insbesondere bei vielen Gegenstellen wächst der Verwaltungsaufwand schnell.



Beachten Sie bitte, dass Zertifikate nur eine begrenzte Zeit gültig sind (z.B. 1 Jahr).

Sollten Sie sich dennoch für dieses Verfahren entscheiden, müssen Sie nacheinander für jeden Client eine identische Verbindung anlegen und darin das Zertifikat des Clients importieren.

alle Zertifikate von vertrauter CA

Dies ist das allgemein übliche und von uns empfohlene Verfahren der zertifikatsbasierenden Authentifizierung. Der Client wird akzeptiert, wenn er sich mit einem Zertifikat ausweist, das von der im SX-GATE als vertrauenswürdig eingestufte Zertifizierungsstelle (CA) ausgestellt wurde. Diese CA wird unter "Module > Netzwerk > Einstellungen" konfiguriert.



Das Zertifikat des SX-GATE VPN-Servers muss ebenfalls von der vertrauenswürdigen CA ausgestellt worden sein. Die Authentifizierung schlägt andernfalls fehl.

Läuft das Zertifikat des Clients ab, kann es dort jederzeit erneuert werden, ohne dass lokal eine Änderung vorgenommen werden muss. Einzige Voraussetzung bleibt, dass das neue Zertifikat ebenfalls von der vertrauten CA ausgestellt wird.



Mit dem Ablauf des vertrauten CA-Zertifikats hingegen verlieren alle Zertifikate ihre Gültigkeit. Ein CA-Zertifikat ist in der Regel aber deutlich länger gültig (z.B. 10 Jahre).

Passphrase (PSK)

Mit dieser Einstellung entscheiden Sie sich für die Authentifizierung über eine gemeinsame Passphrase.



Alle Verbindungen mit dynamischer IP müssen die selbe gemeinsame Passphrase verwenden. Daher ist diese direkt in der ipsec-Schnittstelle und nicht in der Verbindung einzugeben.

ID der Gegenstelle (bei PSK)

Bei Authentifizierung über Passphrase (Preshared Key) identifizieren sich die Kommunikationspartner über eine IP-Adresse, einen Hostnamen (FQDN) oder auch eine E-Mail Adresse (USER@FQDN). Wenn Sie diese Verbindung auf einen Client mit bestimmter ID beschränken wollen, können Sie diese ID hier festlegen. Falls Ihnen diese ID nicht bekannt ist, finden Sie diese z.B. bei einem Verbindungsversuch im Log.



Bei einem Client mit dynamischer IP, der als ID seine IP-Adresse übermittelt, muss die Möglichkeit bestehen die ID auf einen festen Wert einzustellen. Andernfalls ist er über die ID nicht identifizierbar.

ID der Gegenstelle (bei CA basierter Authentifizierung)

Um diese Verbindung auf einen bestimmten Client zu beschränken, können Sie hier die ID eingeben, mit der sich die Gegenstelle meldet. Falls Ihnen diese ID nicht bekannt ist, finden Sie diese z.B. bei einem Verbindungsversuch im Log. Als ID werden die Zertifikatsdaten (Distinguished Name, DN) erwartet. Die Verwendung einer IP-Adresse oder eines DNS-Namens als ID ist hier nicht möglich.



Dieser Wert muss angepasst werden, wenn die Gegenstelle die ID ändert, z.B. weil sie ein neues Zertifikat erhält und der DN des neuen Zertifikats sich von dem des alten Zertifikats unterscheidet.

Öffentlichen Schlüssel importieren

Legen Sie hier den öffentlichen Schlüssel des Clients fest. Wurde das Zertifikat von der lokalen SX-GATE-CA ausgestellt, so kann es von dort kopiert werden. Alternativ muss es aus einer Datei im PEM-Format importiert werden.



Hier muss der öffentliche Schlüssel des Clients selbst importiert werden - nicht der öffentliche Schlüssel der ausstellenden Zertifizierungsstelle (CA).

14.1.2.11.3-C Verschlüsselung

Schlüsselaustauschprotokoll

Hier wählen Sie die Art des Protokolls mit dem der Schlüsselaustausch durchgeführt wird.

IKEv1

Es werden nur IKEv1 Verbindungen akzeptiert.

IKEv2

Es werden nur IKEv2 Verbindungen akzeptiert.

IKEv1 ESP-Proposals (Phase 2)

Mit den Proposals der Phase 2 wird festgelegt, welcher Verschlüsselungsalgorithmus und welches Hashverfahren für die sichere Übermittlung der Daten zulässig sind.



Sind keinerlei Proposals vorgegeben, werden alle Proposals akzeptiert, mit denen SX-GATE umgehen kann.

IKEv2 ESP-Proposals (Phase 2)

Mit den Proposals der Phase 2 wird festgelegt, welcher Verschlüsselungsalgorithmus und welches Hashverfahren für die sichere Übermittlung der Daten zulässig sind. Da AES_GCM ein AEAD-Algorithmus ist, ist kein separates Hashverfahren erforderlich.



Sind keinerlei Proposals vorgegeben, werden alle sicheren Proposals akzeptiert, mit denen SX-GATE umgehen kann.

Perfect Forward-Secrecy

Perfect forward secrecy (PFS) für Phase 2 erhöht die Sicherheit einer VPN-Verbindung. Kommt ein Angreifer in Besitz der gemeinsamen Passphrase bzw. des privaten Schlüssel der VPN-Verbindung, so ist es ihm bei aktivierter PFS dennoch nicht möglich, eine zuvor aufgezeichnete VPN-Kommunikation zu entschlüsseln. Sie sollten PFS nur dann auf "deaktiviert" stellen, wenn es aus Gründen der Interoperabilität mit anderen IPSEC-Implementierungen erforderlich ist.

14.1.2.11.3-D Optionen

Dead-Peer-Detection

Bei aktivierter Dead-Peer-Detection (DPD) wird alle 30 Sekunden geprüft, ob die Gegenstelle noch erreichbar ist. Die Prüfung findet statt, wenn keine Nutzdaten mehr übertragen werden. Antwortet die Gegenstelle nicht mehr, wird die Verbindung nach 120 Sekunden abgebrochen. Falls die Gegenstelle über eine feste IP-Adresse verfügt, wird versucht, eine neue Verbindung herzustellen.



Um diese Funktion nutzen zu können, muss die Gegenstelle ebenfalls DPD gemäß RFC3706 unterstützen.

14.1.2.11.3-E Verbindung

Verbindungsaufbau

Hier können Sie die VPN-Verbindung aktivieren bzw. deaktivieren.

passiv

Bei dieser Einstellung wartet SX-GATE bis die Gegenstelle Kontakt aufnimmt.

deaktiviert

Mit dieser Einstellung wird die zugehörige VPN-Verbindung deaktiviert.

Gateway für Routing

Um korrekte Einträge in der Routing-Tabelle vornehmen zu können, müssen Sie hier einstellen, über welches Gateway die Gegenstelle erreichbar ist oder ob sich diese im gleichen Netzwerk-Segment wie SX-GATE befindet.

14.1.2.11.3-F Befehle

Aktion

Sie haben hier die Möglichkeit, den Verbindungszustand von Hand zu ändern.



Mit dem nächsten Neustart des IPSec-Dienstes (z.B. nach Änderung der Konfiguration) wird wieder der auf dem Reiter (Tab) "Verbindung" konfigurierte Verbindungszustand hergestellt.

Auf eingehende Verbindungen warten

Alle bestehenden Verbindungen werden getrennt. SX-GATE wartet bis die Gegenstellen die Verbindung neu aufbaut.

Verbindungen deaktivieren

Alle bestehenden Verbindungen werden getrennt. Ein Verbindungsaufbau ist bis auf weiteres nicht möglich.

14.1.2.11.4 Verbindung mit Windows IKEv2

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.11.4-A VPN-Tunnel.....	394
14.1.2.11.4-B Optionen.....	396
14.1.2.11.4-C Verbindung.....	397
14.1.2.11.4-D Befehle.....	397

14.1.2.11.4-A VPN-Tunnel

Diese Verbindung nutzt die unter "Dynamische Gegenstellen" eingestellten IKEv2 IKE-Proposals (Phase 1). Stellen Sie daher sicher, dass entweder keine Proposals vorgegeben sind oder tragen Sie die für diese Verbindung empfohlenen Proposals "AES-256-SHA2_256-MODP2048 (DH14)" ein.

In Phase 2 werden alle gängigen, sicheren IKEv2 ESP-Proposals akzeptiert.

Windows nutzt standardmässig die unsichere Diffie-Hellman Group 2 (MODP1024). Nutzen Sie daher entweder unser Installationspaket für Verbindung mit Windows IKEv2 oder sorgen Sie dafür, dass unter Windows die richtigen Proposals eingestellt sind.

Dies können Sie z.Bsp. mit folgendem Powershell Befehl erreichen:

```
Set-VpnConnectionIPsecConfiguration -ConnectionName "Verbindungsname" -
CipherTransformConstants AES256 -AuthenticationTransformConstants SHA256128
-EncryptionMethod AES256 -IntegrityCheckMethod SHA256 -PfsGroup PFS2048 -
DHGroup Group14
```

Authentifizierungsmethode

Wählen Sie hier bitte aus, wie sich die Kommunikationspartner gegenseitig authentifizieren sollen.

alle Zertifikate von vertrauter CA

Dies ist das allgemein übliche und von uns empfohlene Verfahren der zertifikatsbasierenden Authentifizierung. Der Client wird akzeptiert, wenn er sich mit einem Zertifikat ausweist, das von der im SX-GATE als vertrauenswürdig eingestufte Zertifizierungsstelle (CA) ausgestellt wurde. Diese CA wird unter "Module > Netzwerk > Einstellungen" konfiguriert.



Das Zertifikat des SX-GATE VPN-Servers muss ebenfalls von der vertrauenswürdigen CA ausgestellt worden sein. Die Authentifizierung schlägt andernfalls fehl.

Läuft das Zertifikat des Clients ab, kann es dort jederzeit erneuert werden, ohne dass lokal eine Änderung vorgenommen werden muss. Einzige Voraussetzung bleibt, dass das neue Zertifikat ebenfalls von der vertrauten CA ausgestellt wird.



Mit dem Ablauf des vertrauten CA-Zertifikats hingegen verlieren alle Zertifikate ihre Gültigkeit. Ein CA-Zertifikat ist in der Regel aber deutlich länger gültig (z.B. 10 Jahre).

bestimmte X.509-Zertifikate

Bei dieser Option muss der öffentliche Schlüssel des VPN-Clients in den SX-GATE importiert werden. Nachteil dieses Verfahrens: Wechselt der Client sein Zertifikat, weil das alte z.B. abgelaufen ist, müssen Sie hier zunächst den öffentlichen Schlüssel des neuen Zertifikats importieren, bevor die VPN-Verbindung wieder erfolgreich hergestellt werden kann. Insbesondere bei vielen Gegenstellen wächst der Verwaltungsaufwand schnell.



Beachten Sie bitte, dass Zertifikate nur eine begrenzte Zeit gültig sind (z.B. 1 Jahr).

Sollten Sie sich dennoch für dieses Verfahren entscheiden, müssen Sie nacheinander für jeden Client eine identische Verbindung anlegen und darin das Zertifikat des Clients importieren.

Globaler Adressbereich

Ist der globale Adressbereich deaktiviert, werden nur Clients zugelassen, die unter "Adressbereiche definierter Gegenstellen" angegeben sind. Wollen Sie Clients mit beliebiger ID zulassen, müssen Sie einen entsprechenden Adressbereich definieren. Die Größe des Adressbereichs bestimmt die maximale Anzahl gleichzeitiger Verbindungen.

Zuzuweisende IP-Adressen

Geben Sie hier einen Adressbereich an, aus dem der Client sich seine IP-Adresse bezieht.

Die Anzahl der IP-Adressen legt fest, wie viele Clients maximal zur selben Zeit verbunden sein können.

Adressbereiche definierter Gegenstellen

In dieser Tabelle können Sie mit Hilfe der Relative Distinguished Names (RDN) eines Zertifikates Windows Clients bestimmte IP-Adressen zuordnen. Dadurch lassen sich z.Bsp. verschiedenen Gruppen unterschiedliche Adressbereiche zuordnen, die wiederum in der Firewall getrennt behandelt werden können.

Die angegebenen Adressbereiche dürfen sich dabei nicht überschneiden. Es ist aber möglich mehreren Clients den gleichen Adressbereich zuzuordnen, in dem man bei Zuzuweisende IP-Adressen identische Werte eingibt. Die Größe des Adressbereichs begrenzt hier die maximale Anzahl der Clients, die sich gleichzeitig verbinden können.

Öffentlichen Schlüssel importieren

Legen Sie hier den öffentlichen Schlüssel des Clients fest. Wurde das Zertifikat von der lokalen SX-GATE-CA ausgestellt, so kann es von dort kopiert werden. Alternativ muss es aus einer Datei im PEM-Format importiert werden.



Hier muss der öffentliche Schlüssel des Clients selbst importiert werden - nicht der öffentliche Schlüssel der ausstellenden Zertifizierungsstelle (CA).

14.1.2.11.4-B Optionen

Dead-Peer-Detection

Bei aktivierter Dead-Peer-Detection (DPD) wird alle 30 Sekunden geprüft, ob die Gegenstelle noch erreichbar ist. Die Prüfung findet statt, wenn keine Nutzdaten mehr übertragen werden. Antwortet die Gegenstelle nicht mehr, wird die Verbindung nach 120 Sekunden abgebrochen. Falls die Gegenstelle über eine feste IP-Adresse verfügt, wird versucht, eine neue Verbindung herzustellen.



Um diese Funktion nutzen zu können, muss die Gegenstelle ebenfalls DPD gemäß RFC3706 unterstützen.

Als DNS-Server zuweisen

Mit dieser Einstellung können Sie festlegen, welchen Namens-Server der Client verwenden soll.

14.1.2.11.4-C Verbindung

Verbindungsaufbau

Hier können Sie die VPN-Verbindung aktivieren bzw. deaktivieren.

passiv

Bei dieser Einstellung wartet SX-GATE bis die Gegenstelle Kontakt aufnimmt.

deaktiviert

Mit dieser Einstellung wird die zugehörige VPN-Verbindung deaktiviert.

Gateway für Routing

Um korrekte Einträge in der Routing-Tabelle vornehmen zu können, müssen Sie hier einstellen, über welches Gateway die Gegenstelle erreichbar ist oder ob sich diese im gleichen Netzwerk-Segment wie SX-GATE befindet.

14.1.2.11.4-D Befehle

Aktion

Sie haben hier die Möglichkeit, den Verbindungszustand von Hand zu ändern.



Mit dem nächsten Neustart des IPSec-Dienstes (z.B. nach Änderung der Konfiguration) wird wieder der auf dem Reiter (Tab) "Verbindung" konfigurierte Verbindungszustand hergestellt.

Auf eingehende Verbindungen warten

Alle bestehenden Verbindungen werden getrennt. SX-GATE wartet bis die Gegenstellen die Verbindung neu aufbaut.

Verbindungen deaktivieren

Alle bestehenden Verbindungen werden getrennt. Ein Verbindungsaufbau ist bis auf weiteres nicht möglich.

14.1.2.11.5 Verbindung mit XAuth Client

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.11.5-A VPN-Tunnel.....	398
14.1.2.11.5-B Authentifizierung.....	399
14.1.2.11.5-C Verschlüsselung.....	401
14.1.2.11.5-D Optionen.....	402
14.1.2.11.5-E Verbindung.....	402
14.1.2.11.5-F Befehle.....	402

14.1.2.11.5-A VPN-Tunnel

Virtuelle IP (Mode Config)

Die IPSec-Erweiterung "Mode Config" erlaubt es, dem Client eine IP-Adresse für die IPSec-Kommunikation zuzuweisen. Ohne Mode Config wird der Client seine eigene (externe) IP für die Kommunikation verwenden.

Um Mode Config zu aktivieren müssen Sie einen Block von IP-Adressen hinterlegen, der den Clients zugewiesen wird. Die Anzahl der IP-Adressen legt fest, wie viele Clients maximal zur selben Zeit verbunden sein können. Ergänzend ist es möglich, in der Benutzerverwaltung benutzerspezifische Adressen für XAuth-Verbindungen zu hinterlegen. Ein Benutzer für den eine individuelle Adresse festgelegt wurde beansprucht keine der hier konfigurierten IP-Adressen, so dass sich die Anzahl gleichzeitig möglicher Verbindungen entsprechend erhöht. Soll ausschließlich mit benutzerspezifischen Adressen gearbeitet werden, wählen Sie bitte die Option "ausschließlich individuelle Benutzer IPs".



Die zu vergebenden Adress-Bereiche für XAuth dürfen sich überschneiden.

Als DNS-Server zuweisen

Mit dieser Einstellung können Sie festlegen, welchen Namens-Server der Client verwenden soll.

14.1.2.11.5-B Authentifizierung

Authentifizierungsmethode

Wählen Sie hier bitte aus, wie sich die Kommunikationspartner gegenseitig authentifizieren sollen. Zur Verfügung stehen die Authentifizierung mit X.509-Zertifikaten und die Authentifizierung über eine gemeinsame Passphrase (preshared key).

Die Authentifizierung über Zertifikate ist aufgrund des Public-Key-Verfahrens zwar umfangreicher zu konfigurieren, jedoch konzeptionell sicherer. Dabei verfügt jeder Kommunikationspartner über einen privaten Schlüssel der unbedingt geheim zu halten ist sowie einen zugehörigen öffentlichen Schlüssel der nicht besonders geschützt werden muss.

Im Gegensatz dazu entspricht die Authentifizierung über gemeinsame Passphrase einem Kennwort, das beide Kommunikationspartner kennen müssen und das natürlich geheim zu halten ist. Für Client-Verbindungen ist diese Variante eher ungeeignet, da alle Verbindungen mit dynamischen IP-Adressen mit dem selben Preshared Key authentifiziert werden müssen.

bestimmte X.509-Zertifikate

Bei dieser Option muss der öffentliche Schlüssel des VPN-Clients in den SX-GATE importiert werden. Nachteil dieses Verfahrens: Wechselt der Client sein Zertifikat, weil das alte z.B. abgelaufen ist, müssen Sie hier zunächst den öffentlichen Schlüssel des neuen Zertifikats importieren, bevor die VPN-Verbindung wieder erfolgreich hergestellt werden kann. Insbesondere bei vielen Gegenstellen wächst der Verwaltungsaufwand schnell.



Beachten Sie bitte, dass Zertifikate nur eine begrenzte Zeit gültig sind (z.B. 1 Jahr).

Sollten Sie sich dennoch für dieses Verfahren entscheiden, müssen Sie für nacheinander für jeden Client eine identische Verbindung anlegen und darin das Zertifikat des Clients importieren.

alle Zertifikate von vertrauter CA

Dies ist das allgemein übliche und von uns empfohlene Verfahren der zertifikatsbasierenden Authentifizierung. Der Client wird akzeptiert, wenn er sich mit einem Zertifikat ausweist, das von der im SX-GATE als vertrauenswürdig eingestufte Zertifizierungsstelle (CA) ausgestellt wurde. Diese CA wird unter "Module > Netzwerk > Einstellungen" konfiguriert.



Das Zertifikat des SX-GATE VPN-Servers muss ebenfalls von der vertrauenswürdigen CA ausgestellt worden sein. Die Authentifizierung schlägt andernfalls fehl.

Läuft das Zertifikat des Clients ab, kann es dort jederzeit erneuert werden, ohne dass lokal eine Änderung vorgenommen werden muss. Einzige Voraussetzung bleibt, dass das neue Zertifikat ebenfalls von der vertrauten CA ausgestellt wird.



Mit dem Ablauf des vertrauten CA-Zertifikats hingegen verlieren alle Zertifikate ihre Gültigkeit. Ein CA-Zertifikat ist in der Regel aber deutlich länger gültig (z.B. 10 Jahre).

Passphrase (PSK)

Mit dieser Einstellung entscheiden Sie sich für die Authentifizierung über eine gemeinsame Passphrase.



Alle Verbindungen mit dynamischer IP müssen die selbe gemeinsame Passphrase verwenden. Daher ist diese direkt in der ipsec-Schnittstelle und nicht in der Verbindung einzugeben.

ID der Gegenstelle (bei PSK)

Bei Authentifizierung über Passphrase (Preshared Key) identifizieren sich die Kommunikationspartner über eine IP-Adresse, einen Hostnamen (FQDN) oder auch eine E-Mail Adresse (USER@FQDN). Wenn Sie diese Verbindung auf einen Client mit bestimmter ID beschränken wollen, können Sie diese ID hier festlegen. Falls Ihnen diese ID nicht bekannt ist, finden Sie diese z.B. bei einem Verbindungsversuch im Log.



Bei einem Client mit dynamischer IP, der als ID seine IP-Adresse übermittelt, muss die Möglichkeit bestehen die ID auf einen festen Wert einzustellen. Andernfalls ist er über die ID nicht identifizierbar.

ID der Gegenstelle (bei CA basierter Authentifizierung)

Um diese Verbindung auf einen bestimmten Client zu beschränken, können Sie hier die ID eingeben, mit der sich die Gegenstelle meldet. Falls Ihnen diese ID nicht bekannt ist, finden Sie diese z.B. bei einem Verbindungsversuch im Log. Als ID werden die Zertifikatsdaten (Distinguished Name, DN) erwartet. Die Verwendung einer IP-Adresse oder eines DNS-Namens als ID ist hier nicht möglich.



Dieser Wert muss angepasst werden, wenn die Gegenstelle die ID ändert, z.B. weil sie ein neues Zertifikat erhält und der DN des neuen Zertifikats sich von dem des alten Zertifikats unterscheidet.

Öffentlichen Schlüssel importieren

Legen Sie hier den öffentlichen Schlüssel des Clients fest. Wurde das Zertifikat von der lokalen SX-GATE-CA ausgestellt, so kann es von dort kopiert werden. Alternativ muss es aus einer Datei im PEM-Format importiert werden.



Hier muss der öffentliche Schlüssel des Clients selbst importiert werden - nicht der öffentliche Schlüssel der ausstellenden Zertifizierungsstelle (CA).

14.1.2.11.5-C Verschlüsselung

Hier gelten grundsätzlich die für Gegenstellen mit dynamischer IP konfigurierten IKE-Proposals.

IKEv1 ESP-Proposals (Phase 2)

Mit den Proposals der Phase 2 wird festgelegt, welcher Verschlüsselungsalgorithmus und welches Hashverfahren für die sichere Übermittlung der Daten zulässig sind.



Sind keinerlei Proposals vorgegeben, werden alle Proposals akzeptiert, mit denen SX-GATE umgehen kann.

Perfect Forward-Secrecy

Perfect forward secrecy (PFS) für Phase 2 erhöht die Sicherheit einer VPN-Verbindung. Kommt ein Angreifer in Besitz der gemeinsamen Passphrase bzw. des privaten Schlüssels der VPN-Verbindung, so ist es ihm bei aktivierter PFS dennoch nicht möglich, eine zuvor aufgezeichnete VPN-Kommunikation zu entschlüsseln. Sie sollten PFS nur dann auf "deaktiviert" stellen, wenn es aus Gründen der Interoperabilität mit anderen IPSEC-Implementierungen erforderlich ist.

SHA2-256 96bit Draft Version

Bei SHA2-256 wird der ESP Hash normalerweise bei 128 Bits abgeschnitten. Manche IPsec Anwendungen (Linux vor 2.6.33, oder manche Cisco Router) verwenden die Draft Version welche nach 96 Bits abschneidet.

Diese Option aktiviert die 96bits Draft Version, um mit diesen Gegenstellen kompatibel zu sein.

Eine andere Möglichkeit wäre, SHA2-384 oder SHA2-512 zu nutzen.

14.1.2.11.5-D Optionen

Dead-Peer-Detection

Bei aktivierter Dead-Peer-Detection (DPD) wird alle 30 Sekunden geprüft, ob die Gegenstelle noch erreichbar ist. Die Prüfung findet statt, wenn keine Nutzdaten mehr übertragen werden. Antwortet die Gegenstelle nicht mehr, wird die Verbindung nach 120 Sekunden abgebrochen. Falls die Gegenstelle über eine feste IP-Adresse verfügt, wird versucht, eine neue Verbindung herzustellen.



Um diese Funktion nutzen zu können, muss die Gegenstelle ebenfalls DPD gemäß RFC3706 unterstützen.

14.1.2.11.5-E Verbindung

Verbindungsaufbau

Hier können Sie die VPN-Verbindung aktivieren bzw. deaktivieren.

passiv

Bei dieser Einstellung wartet SX-GATE bis die Gegenstelle Kontakt aufnimmt.

deaktiviert

Mit dieser Einstellung wird die zugehörige VPN-Verbindung deaktiviert.

Gateway für Routing

Um korrekte Einträge in der Routing-Tabelle vornehmen zu können, müssen Sie hier einstellen, über welches Gateway die Gegenstelle erreichbar ist oder ob sich diese im gleichen Netzwerk-Segment wie SX-GATE befindet.

14.1.2.11.5-F Befehle

Aktion

Sie haben hier die Möglichkeit, den Verbindungszustand von Hand zu ändern.



Mit dem nächsten Neustart des IPSec-Dienstes (z.B. nach Änderung der Konfiguration) wird wieder der auf dem Reiter (Tab) "Verbindung" konfigurierte Verbindungszustand hergestellt.

Auf eingehende Verbindungen warten

Alle bestehenden Verbindungen werden getrennt. SX-GATE wartet bis die Gegenstellen die Verbindung neu aufbaut.

Verbindungen deaktivieren

Alle bestehenden Verbindungen werden getrennt. Ein Verbindungsaufbau ist bis auf weiteres nicht möglich.

14.1.2.11.6 Verbindung mit L2TP Client

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.1.2.11.6-A Authentifizierung.....	403
14.1.2.11.6-B Verschlüsselung.....	406
14.1.2.11.6-C Optionen.....	406
14.1.2.11.6-D Verbindung.....	407
14.1.2.11.6-E Befehle.....	407

14.1.2.11.6-A Authentifizierung

Authentifizierungsmethode

Wählen Sie hier bitte aus, wie sich die Kommunikationspartner gegenseitig authentifizieren sollen. Zur Verfügung stehen die Authentifizierung mit X.509-Zertifikaten und die Authentifizierung über eine gemeinsame Passphrase (preshared key).

Die Authentifizierung über Zertifikate ist aufgrund des Public-Key-Verfahrens zwar umfangreicher zu konfigurieren, jedoch konzeptionell sicherer. Dabei verfügt jeder Kommunikationspartner über einen privaten Schlüssel der unbedingt geheim zu halten ist sowie einen zugehörigen öffentlichen Schlüssel der nicht besonders geschützt werden muss.

Im Gegensatz dazu entspricht die Authentifizierung über gemeinsame Passphrase einem Kennwort, das beide Kommunikationspartner kennen müssen und das natürlich geheim zu halten ist. Für Client-Verbindungen ist diese Variante eher ungeeignet, da alle Verbindungen mit dynamischen IP-Adressen mit dem selben Preshared Key authentifiziert werden müssen.

bestimmte X.509-Zertifikate

Bei dieser Option muss der öffentliche Schlüssel des VPN-Clients in den SX-GATE importiert werden. Nachteil dieses Verfahrens: Wechselt der Client sein Zertifikat, weil das alte z.B. abgelaufen ist, müssen Sie hier zunächst den öffentlichen Schlüssel des neuen Zertifikats importieren, bevor die VPN-Verbindung wieder erfolgreich hergestellt werden kann. Insbesondere bei vielen Gegenstellen wächst der Verwaltungsaufwand schnell.



Beachten Sie bitte, dass Zertifikate nur eine begrenzte Zeit gültig sind (z.B. 1 Jahr).

Sollten Sie sich dennoch für dieses Verfahren entscheiden, müssen Sie für nacheinander für jeden Client eine identische Verbindung anlegen und darin das Zertifikat des Clients importieren.

alle Zertifikate von vertrauter CA

Dies ist das allgemein übliche und von uns empfohlene Verfahren der zertifikatsbasierenden Authentifizierung. Der Client wird akzeptiert, wenn er sich mit einem Zertifikat ausweist, das von der im SX-GATE als vertrauenswürdig eingestufte Zertifizierungsstelle (CA) ausgestellt wurde. Diese CA wird unter "Module > Netzwerk > Einstellungen" konfiguriert.



Das Zertifikat des SX-GATE VPN-Servers muss ebenfalls von der vertrauenswürdigen CA ausgestellt worden sein. Die Authentifizierung schlägt andernfalls fehl.

Läuft das Zertifikat des Clients ab, kann es dort jederzeit erneuert werden, ohne dass lokal eine Änderung vorgenommen werden muss. Einzige Voraussetzung bleibt, dass das neue Zertifikat ebenfalls von der vertrauten CA ausgestellt wird.



Mit dem Ablauf des vertrauten CA-Zertifikats hingegen verlieren alle Zertifikate ihre Gültigkeit. Ein CA-Zertifikat ist in der Regel aber deutlich länger gültig (z.B. 10 Jahre).

Passphrase (PSK)

Mit dieser Einstellung entscheiden Sie sich für die Authentifizierung über eine gemeinsame Passphrase.



Alle Verbindungen mit dynamischer IP müssen die selbe gemeinsame Passphrase verwenden. Daher ist diese direkt in der ipsec-Schnittstelle und nicht in der Verbindung einzugeben.

ID der Gegenstelle (bei PSK)

Bei Authentifizierung über Passphrase (Preshared Key) identifizieren sich die Kommunikationspartner über eine IP-Adresse, einen Hostnamen (FQDN) oder auch eine E-Mail Adresse (USER@FQDN). Wenn Sie diese Verbindung auf einen Client mit bestimmter ID beschränken wollen, können Sie diese ID hier festlegen. Falls Ihnen diese ID nicht bekannt ist, finden Sie diese z.B. bei einem Verbindungsversuch im Log.



Bei einem Client mit dynamischer IP, der als ID seine IP-Adresse übermittelt, muss die Möglichkeit bestehen die ID auf einen festen Wert einzustellen. Andernfalls ist er über die ID nicht identifizierbar.

ID der Gegenstelle (bei CA basierter Authentifizierung)

Um diese Verbindung auf einen bestimmten Client zu beschränken, können Sie hier die ID eingeben, mit der sich die Gegenstelle meldet. Falls Ihnen diese ID nicht bekannt ist, finden Sie diese z.B. bei einem Verbindungsversuch im Log. Als ID werden die Zertifikatsdaten (Distinguished Name, DN) erwartet. Die Verwendung einer IP-Adresse oder eines DNS-Namens als ID ist hier nicht möglich.



Dieser Wert muss angepasst werden, wenn die Gegenstelle die ID ändert, z.B. weil sie ein neues Zertifikat erhält und der DN des neuen Zertifikats sich von dem des alten Zertifikats unterscheidet.

Öffentlichen Schlüssel importieren

Legen Sie hier den öffentlichen Schlüssel des Clients fest. Wurde das Zertifikat von der lokalen SX-GATE-CA ausgestellt, so kann es von dort kopiert werden. Alternativ muss es aus einer Datei im PEM-Format importiert werden.



Hier muss der öffentliche Schlüssel des Clients selbst importiert werden - nicht der öffentliche Schlüssel der ausstellenden Zertifizierungsstelle (CA).

14.1.2.11.6-B Verschlüsselung

Hier gelten grundsätzlich die für Gegenstellen mit dynamischer IP konfigurierten IKE-Proposals.

IKEv1 ESP-Proposals (Phase 2)

Mit den Proposals der Phase 2 wird festgelegt, welcher Verschlüsselungsalgorithmus und welches Hashverfahren für die sichere Übermittlung der Daten zulässig sind.



Sind keinerlei Proposals vorgegeben, werden alle Proposals akzeptiert, mit denen SX-GATE umgehen kann.

Perfect Forward-Secrecy

Perfect forward secrecy (PFS) für Phase 2 erhöht die Sicherheit einer VPN-Verbindung. Kommt ein Angreifer in Besitz der gemeinsamen Passphrase bzw. des privaten Schlüssel der VPN-Verbindung, so ist es ihm bei aktivierter PFS dennoch nicht möglich, eine zuvor aufgezeichnete VPN-Kommunikation zu entschlüsseln. Sie sollten PFS nur dann auf "deaktiviert" stellen, wenn es aus Gründen der Interoperabilität mit anderen IPSEC-Implementierungen erforderlich ist.

14.1.2.11.6-C Optionen

Dead Peer Detection

Bei aktivierter Dead-Peer-Detection (DPD) wird alle 30 Sekunden geprüft, ob die Gegenstelle noch erreichbar ist. Die Prüfung findet statt, wenn keine Nutzdaten mehr übertragen werden. Antwortet die Gegenstelle nicht mehr, wird die Verbindung nach 120 Sekunden abgebrochen. Falls die Gegenstelle über eine feste IP-Adresse verfügt, wird versucht, eine neue Verbindung herzustellen.



Um diese Funktion nutzen zu können, muss die Gegenstelle ebenfalls DPD gemäß RFC3706 unterstützen.

14.1.2.11.6-D Verbindung

Verbindungsaufbau

Hier können Sie die VPN-Verbindung aktivieren bzw. deaktivieren.

passiv

Bei dieser Einstellung wartet SX-GATE bis die Gegenstelle Kontakt aufnimmt.

deaktiviert

Mit dieser Einstellung wird die zugehörige VPN-Verbindung deaktiviert.

Gateway für Routing

Um korrekte Einträge in der Routing-Tabelle vornehmen zu können, müssen Sie hier einstellen, über welches Gateway die Gegenstelle erreichbar ist oder ob sich diese im gleichen Netzwerk-Segment wie SX-GATE befindet.

14.1.2.11.6-E Befehle

Aktion

Sie haben hier die Möglichkeit, den Verbindungszustand von Hand zu ändern.



Mit dem nächsten Neustart des IPSec-Dienstes (z.B. nach Änderung der Konfiguration) wird wieder der auf dem Reiter (Tab) "Verbindung" konfigurierte Verbindungszustand hergestellt.

Auf eingehende Verbindungen warten

Alle bestehenden Verbindungen werden getrennt. SX-GATE wartet bis die Gegenstellen die Verbindung neu aufbaut.

Verbindungen deaktivieren

Alle bestehenden Verbindungen werden getrennt. Ein Verbindungsaufbau ist bis auf weiteres nicht möglich.

14.2 Firewall

14.2.1 Einstellungen

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.2.1-A Allgemein.....	408
14.2.1-B ALGs.....	409
14.2.1-C Intrusion Detection.....	410
14.2.1-D Intrusion Detection Update.....	411

14.2.1-A Allgemein

Anwendungserkennung

Mit diesem Schalter aktivieren Sie die Anwendungserkennung in der Firewall. Die Firewall analysiert dabei die übertragenen Nutzdaten und versucht zu erkennen, um welche Anwendung es sich handelt.

Nach der Aktivierung werden erkannte Protokolle und ggf. zugehörige Hostnamen im Menü "Monitoring > Firewall" unter "Verbindungen" angezeigt.

Im Menü "Definitionen > Protokolle" können Sie eigene Protokolle anlegen und darin die Anwendungserkennung aktivieren. Regeln in der Firewall (ausgenommen SNAT) und im Bandbreitenmanagement, die so ein Protokoll verwenden, greifen erst dann, wenn auch das Anwendungsprotokoll erkannt wurde.



Trifft die Firewall beim Abarbeiten der Regeln auf ein Protokoll mit Anwendungserkennung, muss die Kommunikation für die weitere Analyse zunächst erlaubt werden. Erst wenn die konfigurierte Anwendung erkannt oder ausgeschlossen werden konnte, wird die Verarbeitung der Regeln fortgesetzt. Die Firewall wird damit "löchrig"!

IPv4-Routing

Mit Hilfe dieses Schalters können Sie das IPv4-Routing aktivieren. Ist das IPv4-Routing deaktiviert, so sind unabhängig von den konfigurierten Firewall-Regeln ausschließlich Verbindungen zu oder vom SX-GATE möglich. Verbindungen durch den

SX-GATE hindurch sind vollständig unterbunden. Es erfolgt in diesem Fall auch keine Protokollierung dieser Pakete durch die Firewall.

Asymmetrisches Routing im LAN

Dieser Schalter deaktiviert die Stateful-Inspection für Pakete die innerhalb der selben Schnittstelle weitergeleitet werden. Berücksichtigung finden ausschließlich Ethernet- und VLAN-Schnittstellen, die in der Firewall als "Zone/Klassifizierung (Vertrauen) LAN (hoch)" eingestuft sind.

Freigegebene IP-Adressen

IP-Adressen auf dieser Liste sind ausgenommen von

- Sperrung auffälliger IP-Adressen durch dynamische Firewall
- Sperrung nach wiederholt fehlgeschlagener Benutzeranmeldung
- Portscan-Überwachung
- der nachfolgenden Sperrliste

Gesperrte IP-Adressen

Verbindungen von und zu IP-Adressen auf dieser Liste werden verworfen.

14.2.1-B ALGs

Application-Level-Gateways

Manche Protokolle nutzen mehrere unterschiedliche Verbindungen. Oft wird über einen Kontrollkanal dynamisch ausgehandelt, über welche Ports anschließend Daten übertragen werden sollen. Für einzelne Protokolle bietet die SX-GATE-Firewall Module an, die den Kontrollkanal überwachen und die benötigten Verbindungen vorübergehend automatisch freigeben. Nutzen Sie diese Module wann immer möglich, da Sie andernfalls eventuell ganze Blöcke von Ports dauerhaft freigeben müssen - oft sogar für eingehende Verbindungen aus dem Internet.

Auf der anderen Seite können es die Firewall-Module einem Angreifer ermöglichen, durch manipulierte Pakete unerwünschte Verbindungen zu öffnen. Sie sollten die Module daher nur gezielt für die Verbindungen aktivieren, für die sie auch wirklich benötigt werden. Aktivieren Sie beispielsweise bei Internet-Telefonie das SIP-Modul nur für Verbindungen von Ihrer Telefonanlage zum SIP-Gateway Ihres Telefonie-Anbieters.

Änderungen in diesem Bereich wirken sich erst auf neue Verbindungen aus. Bei TCP-Verbindungen genügt es in der Regel, die Anwendung auf dem Client neu zu starten.



UDP-Verbindungen werden u.U. über Stunden in der Firewall als Verbindung geführt. Wir empfehlen bei Änderungen daher einen Reboot.

14.2.1-C Intrusion Detection

Das Intrusion-Detection-System (IDS) des SX-GATE analysiert IP-Pakete um potentielle Sicherheitsprobleme aufzuspüren. Untersucht werden dabei sowohl die Kopfdaten von IP-Paketen als auch die tatsächlichen Nutzdaten. Basis der Analyse ist eine Signatur-Datenbank.

Das IDS ist grundsätzlich in der Internet-Schnittstelle aktiviert. Es arbeitet dort mit einer Teilmenge der verfügbaren Signaturen und soll hier in erster Linie bereits befallene lokale Systeme ausfindig machen. Diese sollen daran gehindert werden, Daten in das Internet zu übermitteln und sich als Schädling weiter zu verbreiten. Als schädlich erkannte Datenpakete werden verworfen.



Als Internet-Schnittstelle zählt die Schnittstelle auf die das Standard-Gateway verweist sowie alle Schnittstellen mit Routen in das Zielnetzwerk "***".

Zusätzlich kann das IDS über eine dedizierte Netzwerkkarte mit dem Monitor-Port eines Switches verbunden werden. In dieser Konfiguration steht die vollständige Regelbasis zur Verfügung. Allerdings läuft das IDS hier nur im passiven Modus, d.h. auffällige Datenpakete werden zwar protokolliert aber nicht verworfen.

Deaktivierte Regeln

Hier können Sie einzelne Regeln deaktivieren, falls diese wiederholt zu Fehlalarmen führen. Geben Sie dazu hier die Regelnummer ein. Im Log wird diese in der Form [1:REGELNUMMER:Zahl] protokolliert. Steht im Log also z.B. [1:2010123:0], geben Sie hier bitte 2010123 ein.



Die Regeln werden sowohl in der aktiven IDS (Internet-Schnittstelle) als auch in der passiven IDS (Monitor-Port) deaktiviert.

Freigegebene Verbindungen

Möchten Sie einzelne Verbindungen oder auch ganze Protokolle von der Intrusion Detection ausnehmen, können Sie hier entsprechende Regeln konfigurieren.



Bitte beachten Sie, das vom SX-GATE ausgehend initiierte Verbindungen (Proxy, Mailserver, usw.) über eine zusätzlich konfigurierte Internet-Schnittstelle nicht direkt anhand der Quell-IP festgemacht werden können. Im Normalfall kann für diese Verbindungen aber die Quell-IP der Default Schnittstelle genommen werden.

Lokale Netze

Für IDS-Regeln die zwischen internen und externen Netzwerken unterscheiden, wird hier festgelegt, welche Adressen zu internen Systemen gehören.



Statische IP-Adressen der Internet-Schnittstellen werden stets automatisch ergänzt.

IPS Zusatzregeln für Angriffe gegen Web-Server

Aktiviert Regeln, die speziell auf Angriffe gegen Web- und FTP-Server ausgerichtet sind.

IPS Zusatzregeln für Angriffe gegen Mail-Server

Aktiviert Regeln, die speziell auf Angriffe gegen SMTP-, IMAP4- und POP3-Server ausgerichtet sind.

14.2.1-D Intrusion Detection Update

Bei Geräten mit Software-Pflegevertrag werden die Signaturen mehrmals wöchentlich aktualisiert.

Update-Server

Die Adresse des Update-Servers kann im Menü "System > Update" geändert werden. Auch die Angabe eines Proxies ist dort möglich.

IDS-Signaturen automatisch aktualisieren

Wenn das Update aktiviert ist, prüft SX-GATE täglich zwischen 18:00 und 21:00 Uhr, ob neue Signaturen verfügbar sind.

14.2.2 Regeln

Die SX-GATE Firewall wird pro Schnittstelle konfiguriert. Entsprechend der Vertrauenswürdigkeit der angeschlossenen Netzwerke wird jede Schnittstelle

zusätzlich einer von vier Zonen zugeordnet. Daraus ergibt sich die Basiskonfiguration der Firewall. Diese Basiskonfiguration kann dann durch die Definition weiterer Regeln verfeinert werden.



Durch unbedachte Änderungen in diesem Bereich kann die Sicherheit des SX-GATE und aller durch SX-GATE geschützten Netzwerke beeinträchtigt werden.

Grundsätzlich müssen Regeln in der Firewall-Konfiguration nur für den Verbindungsaufbau definiert werden. Die Stateful-Inspection sorgt dafür, dass insbesondere Antwort-Pakete automatisch akzeptiert werden.

Entscheidend ist, dass Firewall-Regeln in der richtigen Schnittstelle konfiguriert werden. Nachfolgend ist die Schnittstelle, über die eine Verbindung SX-GATE erreicht als "Eingangs-Schnittstelle" bezeichnet. Die Schnittstelle über die eine Verbindung SX-GATE in Richtung Ziel verlässt, wird als "Ausgangs-Schnittstelle" bezeichnet. Es gibt folgende Arten von Verbindungen:

DNAT (in)

DNAT oder Portforwarding ändert das Ziel einer Verbindung und wird in der Eingangs-Schnittstelle auf dem Reiter (Tab) "DNAT > *" konfiguriert. DNAT kann sowohl auf eingehende als auch auf geroutete Verbindungen angewandt werden. Durch DNAT kann sich die Verbindungsart auch ändern. Aus einer eingehenden kann eine weitergeleitete Verbindung werden oder umgekehrt. Über die DNAT-Regel hinaus sind keine weiteren Firewall-Regeln notwendig um eine Verbindung aufbauen zu können.

Eingehende Verbindungen (in)

Dies umfasst alle Verbindungen, deren Ziel SX-GATE selbst ist. Wählen Sie in der Administrations-Oberfläche die Eingangs-Schnittstelle aus. Die Regeln werden auf dem Reiter (Tab) " ... > SX-GATE" konfiguriert.

Weitergeleitete Verbindungen, Routing (fwd)

Alle Verbindungen die SX-GATE passieren, gehören zu dieser Gruppe. SX-GATE ist also weder Quelle noch Ziel der Verbindung. Die Verbindung wird von SX-GATE geroutet. Weiterleitungsregeln werden auf dem Reiter (Tab) "*" > SX-GATE > ... " eingetragen.



Firewall-Regeln für weitergeleitete Verbindungen werden in der Ausgangs-Schnittstelle konfiguriert. Wählen Sie in der Administrations-Oberfläche also bitte die Schnittstelle, über die die Verbindung SX-GATE verlässt.

Ausgehende Verbindungen (out)

Damit sind Verbindungen gemeint, die SX-GATE selbst initiiert. Wählen Sie in der Administrations-Oberfläche die Ausgangs-Schnittstelle. Dort sind die Regeln auf dem Reiter (Tab) "SX-GATE > ..." zu konfigurieren.

Weitergeleitete und ausgehende Verbindungen passieren zusätzlich noch die SNAT-Regeln, die auf dem Reiter (Tab) "*" > SNAT" konfiguriert werden. Dabei wird die ursprüngliche Absender-IP ggf. durch eine andere IP-Adresse ersetzt. In der Grundkonfiguration wird bei IPv4-Verbindungen, die aus den Zonen LAN und RAS in die Zone Internet weitergeleitet werden, automatisch die primäre SX-GATE-IP der Ausgangs-Schnittstelle als Absender-IP gesetzt (Auto-SNAT), da davon ausgegangen wird, dass in den internen Netzen IPv4-Adressen genutzt werden, die nicht im Internet geroutet werden.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.2.2-A Allgemein.....	416
14.2.2-B DNAT > *	417
14.2.2-C Transp. Proxy.....	420
14.2.2-D ... > SX-GATE.....	423
14.2.2-E * > SX-GATE >	426
14.2.2-F * > SX-GATE >	428
14.2.2-G SX-GATE >	431
14.2.2-H * > SNAT.....	433
14.2.2-I Optionen.....	436

Zone/Klassifizierung (Vertrauen)


Legen Sie über diesen Schalter die Basis-Konfiguration der Firewall für die ausgewählte Schnittstelle fest. In der nachfolgenden Matrix lässt sich das Standard-Verhalten der Firewall für entsprechende Kombinationen von Vertrauensstellungen ablesen. Die Quelle bezieht sich dabei auf die Klassifikation der Eingangs-Schnittstelle, das Ziel entsprechend auf die Klassifikation der Ausgangs-Schnittstelle. Die Zeile bzw.

Spalte die als "SX-GATE" betitelt ist beschreibt das Verhalten für Verbindungen von bzw. zu SX-GATE.

Quelle	Ziel				
	Internet (keines)	DMZ (gering)	RAS (mittel)	LAN (hoch)	SX-GATE
Internet (keines)					
DMZ (gering)					
RAS (mittel)	Auto-SNAT				
LAN (hoch)	Auto-SNAT				
SX-GATE					

	Zugriff gesperrt. Freigabe über Regeln
	Zugriff gesperrt. Freigabe über Regeln oder durch Änderung der Grundkonfiguration
	Zugriff erlaubt. Sperrung durch Änderung der Grundkonfiguration

Bei der Auswahlliste der Klassifizierungen ist jeweils der typische Anwendungsfall angegeben. Dieser dient lediglich als Orientierungshilfe. Im Einzelfall kann es durchaus sinnvoll sein, von diesen Vorschlägen abzuweichen. Bedenken Sie bei Änderungen jedoch stets die Auswirkungen. Dies gilt insbesondere bei extremen Abweichungen von den Vorschlägen, wie z.B. der Auswahl von "LAN (hoch)" in der Internet-Schnittstelle.



Wird die Klassifizierung der Schnittstelle geändert, über die die Administration des SX-GATE erfolgt, so ist darauf zu achten, dass mit den neuen Einstellungen nach wie vor der HTTPS-Zugriff auf SX-GATE möglich bleibt. Andernfalls ist kein Zugriff mehr auf die Administrations-Oberfläche möglich. Eine Änderung der Konfiguration kann dann nur noch über Konsole vorgenommen werden.

Internet (keines)

Typischerweise wird diese Einstellung für die Internet-Schnittstelle verwendet. In der Grundeinstellung ist insbesondere der Zugriff aus dem Internet auf SX-GATE gesperrt. Selbiges gilt auch für den direkten Zugriff vom LAN auf das Internet. Die gezielte Freigabe von Verbindungen vom Internet auf SX-GATE ist im Bereich " ... > SX-GATE" möglich. Direkte Verbindungen vom LAN in das

Internet können auf dem Reiter (Tab) "*" > SX-GATE > ... " erlaubt werden, soweit möglich sollten jedoch stattdessen die Komponenten Proxy, Mail-Server, Mail-Client und DNS-Forwarder des SX-GATE genutzt werden. Diese erhöhen die Sicherheit der Browser-, E-Mail- und DNS-Kommunikation von Systemen im LAN mit dem Internet deutlich.

Für erlaubte IPv4-Verbindungen aus dem LAN- oder RAS-Bereich, ist in dieser Einstellung implizit Network-Address-Translation (NAT) aktiviert, sofern in den Regeln auf dem Reiter (Tab) "*" > SNAT" nichts anderes festgelegt wurde. Die Quell-Adresse von ausgehenden IP-Paketen wird dabei automatisch durch die externe IP-Adresse des SX-GATE ersetzt. Ausgenommen sind Internet-Anbindungen mit DS-Lite und Verbindungen die innerhalb einer Bridge weitergeleitet werden.

DMZ (gering)

Werden Internet-Server in einem separaten Netzwerk-Segment betrieben, spricht man von einer Demilitarisierten Zone (DMZ). Dies ist der typische Anwendungsfall dieser Einstellung. Dabei besteht insbesondere Vollzugriff vom LAN auf alle Server in der DMZ. Der Zugriff vom Internet auf die DMZ muss hingegen im Bereich "*" > SX-GATE > ... " explizit freigegeben werden.



Ist Vollzugriff vom LAN auf die DMZ nicht erwünscht, so ändern Sie bitte die Voreinstellung auf dem Reiter "Allgemein".

RAS (mittel)

Diese Einstellung ist zunächst weitestgehend identisch zur Einstellung "LAN (hoch)". Es besteht jedoch die Möglichkeit, Verbindungen aus Schnittstellen mit dieser Einstellung zu allen Zielen einzuschränken. In der Einstellung "LAN (hoch)" ist dies nur in Richtung Internet möglich.

LAN (hoch)

Mit dieser Einstellung sind die geringsten Auflagen verbunden. Aus diesen Netzen heraus ist in der Grundeinstellung lediglich der direkte Zugriff auf das Internet nicht gestattet. Der Zugriff aus dem LAN in alle anderen Schnittstellen-Typen ist nicht beschränkt. Wenn diese Konfiguration zu offen ist, wechseln Sie bitte auf die Option "RAS (mittel)".

Zone/Klassifizierung (Vertrauen) der Bridge als Ziel-Schnittstelle

Normalerweise erfolgt die Firewall-Konfiguration einer Bridge individuell je Port im Menü "Bridge". Für Verbindungen, die von außerhalb in eine Bridge hinein geroutet werden, ist jedoch ausnahmsweise keine Firewall-Konfiguration je Bridge-Port möglich, da zu dem Zeitpunkt, zu dem die Firewall eine solche Verbindung überprüft, der Ziel-Port der Bridge noch nicht ermittelt wurde. Auch Verbindungen die SX-GATE in die

Bridge initiiert und die SNAT-Konfiguration erfolgt nicht per Port sondern für die Bridge als ganzes.

Durch Auswahl der Firewall-Zone legen Sie für die zuvor genannten Verbindungsarten das Standard-Verhalten der Firewall fest. Ihre Auswahl hat keine Auswirkung auf Verbindungen innerhalb der Bridge oder Verbindungen, die ihren Ursprung in der Bridge haben. Die hier festgelegte Klassifizierung kann sich von der der Bridge-Ports unterscheiden. Die nachfolgende Matrix zeigt das Standard-Verhalten der Firewall für entsprechende Kombinationen von Vertrauensstellungen. Die Quelle bezieht sich dabei auf die Klassifikation der Eingangs-Schnittstelle, das Ziel auf die Klassifikation der Bridge. Die Zeile, die mit "SX-GATE" betitelt ist, beschreibt das Verhalten für Verbindungen die SX-GATE initiiert.

Quelle	Ziel			
	Internet (keines)	DMZ (gering)	RAS (mittel)	LAN (hoch)
Internet (keines)				
DMZ (gering)				
RAS (mittel)	Auto-SNAT			
LAN (hoch)	Auto-SNAT			
SX-GATE				

	Zugriff gesperrt. Freigabe über Regeln
	Zugriff gesperrt. Freigabe über Regeln oder durch Änderung der Grundkonfiguration
	Zugriff erlaubt. Sperrung durch Änderung der Grundkonfiguration

14.2.2-A Allgemein

Beschreibung "..."

Dieser Text dient ausschließlich der Dokumentation.

Netflow/IPFIX

Aktivieren Sie diesen Schalter, um Verbindungen mit Netflow/IPFIX zu exportieren, deren Quelle oder Ziel diese Schnittstelle ist.



Im Falle einer Bridge wird der Datenverkehr aller Ports exportiert.

Grundkonfiguration

In der Matrix lässt sich das Standardverhalten der Firewall für die aktuelle Schnittstelle ablesen und z.T. auch konfigurieren. Die angegebenen Voreinstellungen hängen ab von der Zone, der die Schnittstelle zugeordnet ist. Diese Zuordnung erfolgt über die Option "Zone/Klassifizierung (Vertrauen)".

Grundkonfiguration bei Routing in die Bridge

In der Matrix lässt sich das Standardverhalten der Firewall für die aktuelle Schnittstelle ablesen und z.T. auch konfigurieren. Die angegebenen Voreinstellungen hängen ab von der Zone, der die Schnittstelle zugeordnet ist. Diese Zuordnung erfolgt über die Option "Zone/Klassifizierung (Vertrauen) der Bridge als Ziel-Schnittstelle".

14.2.2-B DNAT > *

Auf diesem Reiter (Tab) definieren Sie Portforwarding-Regeln (DNAT). Dabei wird die Ziel-Adresse von Verbindungen verändert. Auf diese Weise ist es z.B. möglich, direkt aus dem Internet eine Verbindung zu einem Rechner mit einer internen IP-Adresse herzustellen. DNAT-Regeln müssen in der Schnittstelle konfiguriert werden, über die SX-GATE die Verbindung empfängt.



Sofern das Ziel einer IPv4-Verbindung nach der DNAT-Verarbeitung nicht SX-GATE selbst ist, muss "IPv4-Routing" unter "Module > Firewall > Einstellungen" angeschaltet sein.



Eine DNAT-Verbindung kann nur dann funktionieren, wenn das neue Verbindungs-Ziel die Antwort-Pakete via SX-GATE an den Client zurücksendet. Nur dann hat SX-GATE die Möglichkeit, die Antwort-Pakete so anzupassen, dass diese vom Client zugeordnet werden können. Verfügt das Verbindungs-Ziel über keine passende Rück-Route, konfigurieren Sie bitte zusätzlich eine entsprechende SNAT-Regel.

DNAT (Portweiterleitung): Quelle ..., Ziel beliebig

Um einen neuen Eintrag hinzuzufügen, drücken Sie bitte auf die Schaltfläche "Neuer Eintrag" in der unteren linken Ecke der Tabelle. Sie können einen bestehenden Eintrag als Vorlage verwenden: Drücken Sie dazu auf das zugehörige "Kopieren"-Symbol, das

Sie in der letzten Spalte finden. Ein Ändern von Einträgen ist über das Stiftsymbol "Bearbeiten" möglich. Einzelne Einträge löschen Sie über die Mülltonne "Entfernen" in der jeweiligen Zeile. Mit der Mülltonne "Markierte Einträge löschen" im Kopf der Tabelle löschen Sie alle Zeilen, die Sie zuvor über die Kästchen am rechten Rand jeder Zeile ausgewählt haben. Das Kästchen in der Titlezeile wählt alle Zeilen aus. Mit Hilfe der Pfeilsymbole "Auf" und "Ab" kann die jeweilige Zeile um eine Position nach oben bzw. unten verschoben werden. Halten Sie die Maustaste auf dem "Drag'n'Drop" Symbol rechts neben den Pfeilen gedrückt, um eine Zeile per Drag&Drop auf eine andere Position zu schieben. Ein Klick auf die Spaltentitel ändert die Sortierung. Beachten Sie bitte auch die Symbole für den Export und Import von Einträgen am unteren Rand der Tabelle.



Tabellen mit vielen Zeilen werden nicht vollständig angezeigt. Am unteren rechten Rand der Tabelle werden stattdessen Schaltflächen zur Seitenschaltung eingeblendet. Alternativ ist eine gruppierte Anzeige wählbar. Über eine weitere Schaltfläche kann die komplette Tabelle im Vollbildmodus geöffnet werden. Diese Darstellung empfiehlt sich insbesondere dann, wenn Sie einen Eintrag per Drag&Drop über viele Zeilen verschieben wollen.



Die Regeln werden der Reihe nach geprüft. Die erste zutreffende Regel wird angewandt. Spezifischere Regeln müssen daher über den allgemeineren stehen. Eine Regel, die nur für eine spezielle IP-Adresse gilt, sollte also über einer Regel stehen, die für das selbe Protokoll aber beliebige IP-Adressen gilt.

Die Bedeutung der Felder im Einzelnen:

Aktiv

Mit Hilfe dieses Schalters lassen sich Regeln jederzeit aktivieren und deaktivieren. Um eine temporäre Firewall-Regel zu konfigurieren, wählen Sie das Datum und die Uhrzeit aus, bis zu deren Erreichen die Regel aktiv bleiben soll.

Log

Dieser Schalter aktiviert die Protokollierung der jeweiligen Regel. Bei TCP-Verbindungen wird nur der Verbindungsaufbau im Log vermerkt. Bei anderen IP-Protokollen wird jedes Paket protokolliert.



Um die Log-Dateien nicht zu groß werden zu lassen sollte die Protokollierung nur zu Diagnose-Zwecken und für selten genutzte Zugänge verwendet werden.

Protokoll

Wählen Sie hier das gewünschte Protokoll aus. Jedes Protokoll steht für eine Liste aus IP-Protokoll- und Port-Signaturen. Im Menü "Definitionen > Protokolle" können Sie diese einsehen und bei Bedarf auch mit eigenen Definitionen erweitern.

Die Applikationserkennung funktioniert hier nur eingeschränkt, da DNAT-Regeln das tatsächliche Ziel einer Verbindung schon mit dem ersten Paket festlegen müssen. Bei TCP-Verbindung wurden zu diesem Zeitpunkt noch keinerlei Nutzdaten übertragen, die eine Erkennung der Anwendung erlauben würden. Bei anderen IP-Protokollen wie z.B. UDP kann zumindest bei manchen Anwendungen bereits das erste Datenpaket zu einer Erkennung führen. Ist die Anwendung noch unbekannt, greift die DNAT-Regel bereits, wenn lediglich das IP-Protokoll und die Portsignatur des Pakets passen. Stellt sich später im Laufe der Verbindung heraus, dass es sich nicht um die gewünschte Anwendung handelt, wird die Verbindung unterbrochen.

Quelle (...)

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Quell-Adressen. Um einem einzelnen Client den Zugriff zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Sie können sich bei der Quelle der Regel auch auf MAC-Adressen beziehen. Verweisen Sie dazu auf Objekte vom Typ "Host", die Sie zuvor im Menü "Definitionen > IP-Objekte" anlegen müssen. Ist in einem solchen Objekt nur die MAC-Adresse angegeben, wird die Quelle ausschließlich anhand der MAC-Adresse gefiltert, und zwar sowohl für IPv4 als auch für IPv6. Ist zusätzlich eine IP-Adresse angegeben, greift die Regel nur, wenn bei einem IP-Paket sowohl die MAC- als auch die IP-Adresse passen. Ist im Objekt zwar eine IPv4-Adresse spezifiziert aber keine IPv6-Adresse, greift die Regel nur bei IPv4-Paketen. Ist eine IPv6-Adresse spezifiziert aber keine IPv4-Adresse, gilt die Regel entsprechend nur für IPv6.



Sie können mehrere Objekte vom Typ "Host" in einer Gruppe zusammenfassen, um mehrere MAC-Adressen und MAC-/IP-Kombinationen mit einer Regel zu erfassen.

Zugriff

Wählen Sie aus, ob der Zugriff erlaubt oder verboten sein soll. Bei einem verbotenen Verbindungsversuche verwirft SX-GATE das IP-Paket.

Ziel

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Ziel-Adressen. Um den Zugriff auf einen einzelnen Server zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Ziel-Netzwerk freigegeben werden, muss

die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.



Wenn SX-GATE die IP-Adresse dynamisch bezieht, darf hier kein Wert vorgegeben werden.

zu IP

Hier wird festgelegt, an welche Adresse das Paket weitergeleitet wird. Es kann sich dabei sowohl um eine IP-Adresse des SX-GATE (ausgenommen 127.0.0.1) als auch um die Adresse eines anderen Systems handeln. Bei "verwerfen" muss zwar eine Adresse angegeben werden, diese wird aber nicht verwendet.

Durch Eingabe einer Netzwerk-Adresse samt zugehöriger Netzmaske, lässt sich eine statische 1:1-Abbildung zwischen den Adressen zweier Netzwerke konfigurieren. Der Eintrag "10.0.0.0/24" ersetzt beispielsweise die ersten drei Komponenten jeder Ziel-IP mit "10.0.0.". Aus der Ziel-IP "192.168.1.254" wird so also "10.0.0.254".



Es ist in diesem Fall nicht möglich, auch den Ziel-Port umzuschreiben. Das Feld "Port" muss frei bleiben.

Port

Lassen Sie dieses Feld frei um den Ziel-Port des ursprünglichen Pakets beizubehalten. Andernfalls geben Sie bitte hier den neuen Ziel-Port an.

Zeitraum

Eine Regel kann auf Wunsch nur zu bestimmten Uhrzeiten an bestimmten Wochentagen gelten. Die Zeiträume werden im Menü "Definitionen > Zeiträume" festgelegt und könne hier zugewiesen werden.

DoS

Optional kann zusätzlich die Überwachung auf Denial-of-Service Angriffe durch die dynamische Firewall zugeschaltet werden. Für TCP-Verbindungen bezieht sich die Angabe auf die maximale Anzahl Verbindungen pro Quell-IP. Für alle anderen Protokolle wird die Anzahl Pakete pro Quell-IP begrenzt.

Kommentar

Dieses Feld können Sie zur Dokumentation nutzen. Bei aktiviertem Logging werden bis zu 14 Zeichen aus diesem Feld mitprotokolliert.

14.2.2-C Transp. Proxy

Einige SX-GATE Dienste können als transparenter Proxy fungieren. Ohne den Client umkonfigurieren zu müssen, können so die Vorteile dieses Dienstes genutzt werden.

Die Schalter auf dieser Seite aktivieren die notwendigen Firewall-Regeln um bestimmte Verbindungen an den zugehörigen SX-GATE-Proxy umzuleiten.



Stellen Sie sicher, dass der jeweilige Proxy-Dienst auch aktiviert ist.

Die Regeln gelten unabhängig von Quell- und Ziel-Adressen für alle Clients die an der gewählten Schnittstelle angeschlossen sind. Um den transparenten Zugriff nur für bestimmte Adressen zu nutzen, können alternativ selbst entsprechende Regeln auf dem Reiter (Tab) "DNAT > *" konfiguriert werden.

Anhand der Umleitung auf SX-GATEs Web-Proxy soll exemplarisch erläutert werden, welche Firewall-Regeln mit der Aktivierung der entsprechenden Option verknüpft sind. Im Beispiel sei die IP-Adresse des SX-GATE 192.168.0.254. Verbindungen zu Port 80 (HTTP) beliebiger Server müssen also an SX-GATEs Web-Proxy auf Port 8082 umgeleitet werden. Dies bewerkstelligt die DNAT-Regel "HTTP:*->*>192.168.0.254(8082)".

Kein transparenter Proxy für Verbindungen zu

Verbindungen zu bestimmten Zielen können vom transparenten Proxying ausgenommen werden (z.B. interne Netze).



Verbindungen zu IP-Adressen des SX-GATEs sind stets automatisch vom transparenten Proxying ausgenommen.

Port 80 (HTTP) auf Web-Proxy

Dieser Schalter aktiviert transparenten Zugriff auf SX-GATEs Web-Proxy. Zugriffe auf Port 80 beliebiger Ziel-Adressen werden dazu an den Web-Proxy umgelenkt. Eine Proxy-Authentifizierung findet bei transparenten Zugriffen grundsätzlich nicht statt.



Diese Option ist nicht verfügbar, wenn in der Konfiguration des Web-Proxies der transparente Proxy-Modus deaktiviert ist.

ohne Content-Filter

Bei Auswahl dieser Einstellung werden die Verbindungen an den Web-Proxy auf Port 8083 umgeleitet. Der Content-Filter wird dadurch umgangen. Sie können diese Option für ein Netzwerk mit geringerem Schutzbedarf wählen, wenn der Content-Filter wiederholt unerwartete Probleme verursacht. Stellen Sie dann jedoch sicher, dass die Firewall den Zugriff auf Netze mit höherem Schutzbedarf sowohl direkt als auch über Proxy verhindert.



Diese Option ist nicht verfügbar, wenn der Content-Filter deaktiviert ist oder das Umgehen des Content-Filters deaktiviert ist.

aktiviert

In dieser Einstellung werden die Verbindungen an den lokalen Port 8082 umgeleitet. Sowohl der URL- als auch der Content-Filter des Web-Proxies werden genutzt, sofern diese aktiviert sind.

Port 443 (HTTPS) auf Web-Proxy

Dieser Schalter aktiviert transparenten HTTPS Zugriff auf SX-GATEs Web-Proxy. Zugriffe auf Port 443 beliebiger Ziel-Adressen werden dazu an den Web-Proxy umgelenkt. Eine Proxy-Authentifizierung findet bei transparenten Zugriffen grundsätzlich nicht statt.



Diese Option ist nicht verfügbar, wenn in der Konfiguration des Web-Proxies der transparente Proxy-Modus deaktiviert ist.

ohne Content-Filter

Bei Auswahl dieser Einstellung werden die Verbindungen an den Web-Proxy auf Port 8446 umgeleitet. Der Content-Filter wird dadurch umgangen. Dies ist hilfreich, wenn im Content-Filter das Aufbrechen von SSL-Verbindungen aktiviert ist, auf den Endgeräten aber keine Proxy-CA installiert werden kann, wie es z.B. bei einem Mitarbeiter-WLAN mit privaten Endgeräten (BYOD) der Fall ist.



Diese Option ist nicht verfügbar, wenn der Content-Filter deaktiviert ist oder das Umgehen des Content-Filters deaktiviert ist.

aktiviert

In dieser Einstellung werden die Verbindungen an den lokalen Port 8445 umgeleitet. Sowohl der URL- als auch der Content-Filter des Web-Proxies werden genutzt, sofern diese aktiviert sind.

Port 21 (FTP) auf FTP-Proxy

Analog zur vorhergehenden Option werden über diesen Schalter Verbindungen zu Port 21 an den SX-GATE FTP-Proxy umgeleitet (Port 2121).

Port 5060 (Voice-over-IP SIP) auf SIP-Proxy

Dieser Schalter wirkt sich auf Pakete des Voice-over-IP Protokolls SIP aus. Pakete zu TCP- und UDP-Port 5060 mit beliebiger Ziel-Adresse werden an die Adresse des SX-GATE und damit an den SIP-Proxy gesendet.

Port 110 (POP3) auf POP3-/SMTP-Proxy

Verbindungen zu TCP-Port 110 einer Internet IP-Adresse werden mit Hilfe dieser Option über SX-GATEs POP3-Proxy (Port 8110) umgeleitet.

Port 25 (SMTP) auf

Direkte SMTP-Verbindungen in das Internet lassen sich mit Hilfe dieser Option abfangen und an einen Server-Dienst auf dem SX-GATE umleiten. Die Ziel-IP von Verbindungen zu Port 25 wird dabei durch die IP-Adresse des SX-GATE ersetzt.

Mail-Relay-Server

Bei Auswahl dieser Einstellung werden die Verbindungen an den SX-GATE Mail-Relay-Server umgeleitet. Dieser übernimmt die weitere Verarbeitung vollständig, so als hätte der Absender keine Verbindung in das Internet versucht sondern die Mail unmittelbar an SX-GATEs Mail-Relay-Server übergeben.

SMTP-Proxy

Hier wird die Mail an SX-GATEs POP3-/SMTP-Proxy (Port 8110) übergeben, der seinerseits Verbindung mit dem ursprünglich adressierten Mail-Server aufnimmt. Sofern die entsprechende Option aktiviert ist, prüft SX-GATEs SMTP-Proxy die Mail dabei auf Viren. Die eigentliche Verarbeitung der Mail erfolgt jedoch durch den vom Absender vorgegebenen Mail-Server.

Port 53 (DNS) auf DNS-Forwarder

DNS-Pakete lassen sich durch diesen Schalter an den Namens-Server des SX-GATE umlenken. Dies betrifft sowohl TCP- als auch UDP-Pakete zu Port 53.

14.2.2-D ... > SX-GATE

Auf diesem Reiter (Tab) geht es um Verbindungen zu SX-GATE. Ziel ist einer der Server-Dienste, die SX-GATE anbietet.

Eingehende Verbindungen: Quelle ..., Ziel SX-GATE

Um einen neuen Eintrag hinzuzufügen, drücken Sie bitte auf die Schaltfläche "Neuer Eintrag" in der unteren linken Ecke der Tabelle. Sie können einen bestehenden Eintrag als Vorlage verwenden: Drücken Sie dazu auf das zugehörige "Kopieren"-Symbol, das Sie in der letzten Spalte finden. Ein Ändern von Einträgen ist über das Stiftsymbol "Bearbeiten" möglich. Einzelne Einträge löschen Sie über die Mülltonne "Entfernen" in der jeweiligen Zeile. Mit der Mülltonne "Markierte Einträge löschen" im Kopf der Tabelle

löschen Sie alle Zeilen, die Sie zuvor über die Kästchen am rechten Rand jeder Zeile ausgewählt haben. Das Kästchen in der Titlezeile wählt alle Zeilen aus. Mit Hilfe der Pfeilsymbole "Auf" und "Ab" kann die jeweilige Zeile um eine Position nach oben bzw. unten verschoben werden. Halten Sie die Maustaste auf dem "Drag'n'Drop" Symbol rechts neben den Pfeilen gedrückt, um eine Zeile per Drag&Drop auf eine andere Position zu schieben. Ein Klick auf die Spaltentitel ändert die Sortierung. Beachten Sie bitte auch die Symbole für den Export und Import von Einträgen am unteren Rand der Tabelle.



Tabellen mit vielen Zeilen werden nicht vollständig angezeigt. Am unteren rechten Rand der Tabelle werden stattdessen Schaltflächen zur Seitenschaltung eingeblendet. Alternativ ist eine gruppierte Anzeige wählbar. Über eine weitere Schaltfläche kann die komplette Tabelle im Vollbildmodus geöffnet werden. Diese Darstellung empfiehlt sich insbesondere dann, wenn Sie einen Eintrag per Drag&Drop über viele Zeilen verschieben wollen.



Die Regeln werden der Reihe nach geprüft. Die erste zutreffende Regel wird angewandt. Spezifischere Regeln müssen daher über den allgemeineren stehen. Eine Regel, die nur für eine spezielle IP-Adresse gilt, sollte also über einer Regel stehen, die für das selbe Protokoll aber beliebige IP-Adressen gilt.

Die Bedeutung der Felder im Einzelnen:

Aktiv

Mit Hilfe dieses Schalters lassen sich Regeln jederzeit aktivieren und deaktivieren. Um eine temporäre Firewall-Regel zu konfigurieren, wählen Sie das Datum und die Uhrzeit aus, bis zu deren Erreichen die Regel aktiv bleiben soll.

Log

Dieser Schalter aktiviert die Protokollierung der jeweiligen Regel. Bei TCP-Verbindungen wird nur der Verbindungsaufbau im Log vermerkt. Bei anderen IP-Protokollen wird jedes Paket protokolliert.



Um die Log-Dateien nicht zu groß werden zu lassen sollte die Protokollierung nur zu Diagnose-Zwecken und für selten genutzte Zugänge verwendet werden.

Protokoll

Wählen Sie hier das gewünschte Protokoll aus. Jedes Protokoll steht für eine Liste aus IP-Protokoll- und Port-Signaturen. Im Menü "Definitionen > Protokolle"

können Sie diese einsehen und bei Bedarf auch mit eigenen Definitionen erweitern.

Quelle (...)

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Quell-Adressen. Um einem einzelnen Client den Zugriff zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Sie können sich bei der Quelle der Regel auch auf MAC-Adressen beziehen. Verweisen Sie dazu auf Objekte vom Typ "Host", die Sie zuvor im Menü "Definitionen > IP-Objekte" anlegen müssen. Ist in einem solchen Objekt nur die MAC-Adresse angegeben, wird die Quelle ausschließlich anhand der MAC-Adresse gefiltert, und zwar sowohl für IPv4 als auch für IPv6. Ist zusätzlich eine IP-Adresse angegeben, greift die Regel nur, wenn bei einem IP-Paket sowohl die MAC- als auch die IP-Adresse passen. Ist im Objekt zwar eine IPv4-Adresse spezifiziert aber keine IPv6-Adresse, greift die Regel nur bei IPv4-Paketen. Ist eine IPv6-Adresse spezifiziert aber keine IPv4-Adresse, gilt die Regel entsprechend nur für IPv6.



Sie können mehrere Objekte vom Typ "Host" in einer Gruppe zusammenfassen, um mehrere MAC-Adressen und MAC-/IP-Kombinationen mit einer Regel zu erfassen.

Zugriff

Wählen Sie aus, ob der Zugriff erlaubt oder verboten sein soll. Bei einem verbotenen Verbindungsversuche kann SX-GATE das IP-Paket wahlweise einfach verwerfen oder aber mit einem ICMP-Antwortpaket "administratively prohibited" zurückweisen. Letzteres informiert den Absender über die Sperrung.

Zeitraum

Eine Regel kann auf Wunsch nur zu bestimmten Uhrzeiten an bestimmten Wochentagen gelten. Die Zeiträume werden im Menü "Definitionen > Zeiträume" festgelegt und könne hier zugewiesen werden.

DoS

Optional kann zusätzlich die Überwachung auf Denial-of-Service Angriffe durch die dynamische Firewall zugeschaltet werden. Für TCP-Verbindungen bezieht sich die Angabe auf die maximale Anzahl Verbindungen pro Quell-IP. Für alle anderen Protokolle wird die Anzahl Pakete pro Quell-IP begrenzt.

Kommentar

Dieses Feld können Sie zur Dokumentation nutzen. Bei aktiviertem Logging werden bis zu 14 Zeichen aus diesem Feld mitprotokolliert.

14.2.2-E * > SX-GATE > ...

Auf diesem Reiter (Tab) geht es um Verbindungen, die SX-GATE weiterleitet. SX-GATE fungiert dabei als Router. Dabei sind stets zwei Schnittstellen beteiligt: Die Eingangs-Schnittstelle, über die die Verbindung SX-GATE erreicht, und die Ausgangs-Schnittstelle, über die die Verbindung SX-GATE wieder verlässt. SX-GATE selbst ist dabei weder Quelle noch Ziel der Verbindung.



Weiterleitungs-Regeln werden im SX-GATE stets in der Ausgangs-Schnittstelle konfiguriert.

Weiterleitungen: Quelle beliebig, Ziel ...

Um einen neuen Eintrag hinzuzufügen, drücken Sie bitte auf die Schaltfläche "Neuer Eintrag" in der unteren linken Ecke der Tabelle. Sie können einen bestehenden Eintrag als Vorlage verwenden: Drücken Sie dazu auf das zugehörige "Kopieren"-Symbol, das Sie in der letzten Spalte finden. Ein Ändern von Einträgen ist über das Stiftsymbol "Bearbeiten" möglich. Einzelne Einträge löschen Sie über die Mülltonne "Entfernen" in der jeweiligen Zeile. Mit der Mülltonne "Markierte Einträge löschen" im Kopf der Tabelle löschen Sie alle Zeilen, die Sie zuvor über die Kästchen am rechten Rand jeder Zeile ausgewählt haben. Das Kästchen in der Titlezeile wählt alle Zeilen aus. Mit Hilfe der Pfeilsymbole "Auf" und "Ab" kann die jeweilige Zeile um eine Position nach oben bzw. unten verschoben werden. Halten Sie die Maustaste auf dem "Drag'n'Drop" Symbol rechts neben den Pfeilen gedrückt, um eine Zeile per Drag&Drop auf eine andere Position zu schieben. Ein Klick auf die Spaltentitel ändert die Sortierung. Beachten Sie bitte auch die Symbole für den Export und Import von Einträgen am unteren Rand der Tabelle.



Tabellen mit vielen Zeilen werden nicht vollständig angezeigt. Am unteren rechten Rand der Tabelle werden stattdessen Schaltflächen zur Seitenschaltung eingeblendet. Alternativ ist eine gruppierte Anzeige wählbar. Über eine weitere Schaltfläche kann die komplette Tabelle im Vollbildmodus geöffnet werden. Diese Darstellung empfiehlt sich insbesondere dann, wenn Sie einen Eintrag per Drag&Drop über viele Zeilen verschieben wollen.



Die Regeln werden der Reihe nach geprüft. Die erste zutreffende Regel wird angewandt. Spezifischere Regeln müssen daher über den allgemeineren stehen. Eine Regel, die nur für eine spezielle IP-Adresse gilt, sollte also über einer Regel stehen, die für das selbe Protokoll aber beliebige IP-Adressen gilt.

Die Bedeutung der Felder im Einzelnen:

Aktiv

Mit Hilfe dieses Schalters lassen sich Regeln jederzeit aktivieren und deaktivieren. Um eine temporäre Firewall-Regel zu konfigurieren, wählen Sie das Datum und die Uhrzeit aus, bis zu deren Erreichen die Regel aktiv bleiben soll.

Log

Dieser Schalter aktiviert die Protokollierung der jeweiligen Regel. Bei TCP-Verbindungen wird nur der Verbindungsaufbau im Log vermerkt. Bei anderen IP-Protokollen wird jedes Paket protokolliert.



Um die Log-Dateien nicht zu groß werden zu lassen sollte die Protokollierung nur zu Diagnose-Zwecken und für selten genutzte Zugänge verwendet werden.

Protokoll

Wählen Sie hier das gewünschte Protokoll aus. Jedes Protokoll steht für eine Liste aus IP-Protokoll- und Port-Signaturen. Im Menü "Definitionen > Protokolle" können Sie diese einsehen und bei Bedarf auch mit eigenen Definitionen erweitern.

Quell-Zone

Verwenden Sie diese Einstellung, wenn die Regel ausschließlich für Verbindungen aus einer bestimmten Zone gelten soll.

Quell-IP/Netzwerk

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Quell-Adressen. Um einem einzelnen Client den Zugriff zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Sie können sich bei der Quelle der Regel auch auf MAC-Adressen beziehen. Verweisen Sie dazu auf Objekte vom Typ "Host", die Sie zuvor im Menü "Definitionen > IP-Objekte" anlegen müssen. Ist in einem solchen Objekt nur die MAC-Adresse angegeben, wird die Quelle ausschließlich anhand der MAC-Adresse gefiltert, und zwar sowohl für IPv4 als auch für IPv6. Ist zusätzlich eine IP-Adresse angegeben, greift die Regel nur, wenn bei einem IP-Paket sowohl die MAC- als auch die IP-Adresse passen. Ist im Objekt zwar eine IPv4-

Adresse spezifiziert aber keine IPv6-Adresse, greift die Regel nur bei IPv4-Paketen. Ist eine IPv6-Adresse spezifiziert aber keine IPv4-Adresse, gilt die Regel entsprechend nur für IPv6.



Sie können mehrere Objekte vom Typ "Host" in einer Gruppe zusammenfassen, um mehrere MAC-Adressen und MAC-/IP-Kombinationen mit einer Regel zu erfassen.

Zugriff

Wählen Sie aus, ob der Zugriff erlaubt oder verboten sein soll. Bei einem verbotenen Verbindungsversuche kann SX-GATE das IP-Paket wahlweise einfach verwerfen oder aber mit einem ICMP-Antwortpaket "administratively prohibited" zurückweisen. Letzteres informiert den Absender über die Sperrung.

Ziel (...)

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Ziel-Adressen. Um den Zugriff auf einen einzelnen Server zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Ziel-Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Zeitraum

Eine Regel kann auf Wunsch nur zu bestimmten Uhrzeiten an bestimmten Wochentagen gelten. Die Zeiträume werden im Menü "Definitionen > Zeiträume" festgelegt und könne hier zugewiesen werden.

DoS

Optional kann zusätzlich die Überwachung auf Denial-of-Service Angriffe durch die dynamische Firewall zugeschaltet werden. Für TCP-Verbindungen bezieht sich die Angabe auf die maximale Anzahl Verbindungen pro Quell-IP. Für alle anderen Protokolle wird die Anzahl Pakete pro Quell-IP begrenzt.

Kommentar

Dieses Feld können Sie zur Dokumentation nutzen. Bei aktiviertem Logging werden bis zu 14 Zeichen aus diesem Feld mitprotokolliert.

14.2.2-F * > SX-GATE > ...

Dieser Reiter (Tab) ist ausschließlich in Bridge-Schnittstellen verfügbar. Es geht dabei um Verbindungen, die von außerhalb der Bridge in die Bridge geroutet werden. Zum Zeitpunkt der Bearbeitung durch die Bridge ist leider noch nicht bekannt, an welchen Bridge-Port die Verbindung weitergeleitet wird. Daher lassen sich die Regeln nicht je Bridge-Port sondern nur für die Bridge als ganzes konfigurieren.

Weiterleitungen: Quelle: beliebige Schnittstelle außerhalb der Bridge, Ziel: Bridge ...

Um einen neuen Eintrag hinzuzufügen, drücken Sie bitte auf die Schaltfläche "Neuer Eintrag" in der unteren linken Ecke der Tabelle. Sie können einen bestehenden Eintrag als Vorlage verwenden: Drücken Sie dazu auf das zugehörige "Kopieren"-Symbol, das Sie in der letzten Spalte finden. Ein Ändern von Einträgen ist über das Stiftsymbol "Bearbeiten" möglich. Einzelne Einträge löschen Sie über die Mülltonne "Entfernen" in der jeweiligen Zeile. Mit der Mülltonne "Markierte Einträge löschen" im Kopf der Tabelle löschen Sie alle Zeilen, die Sie zuvor über die Kästchen am rechten Rand jeder Zeile ausgewählt haben. Das Kästchen in der Titlezeile wählt alle Zeilen aus. Mit Hilfe der Pfeilsymbole "Auf" und "Ab" kann die jeweilige Zeile um eine Position nach oben bzw. unten verschoben werden. Halten Sie die Maustaste auf dem "Drag'n'Drop" Symbol rechts neben den Pfeilen gedrückt, um eine Zeile per Drag&Drop auf eine andere Position zu schieben. Ein Klick auf die Spaltentitel ändert die Sortierung. Beachten Sie bitte auch die Symbole für den Export und Import von Einträgen am unteren Rand der Tabelle.



Tabellen mit vielen Zeilen werden nicht vollständig angezeigt. Am unteren rechten Rand der Tabelle werden stattdessen Schaltflächen zur Seitenschaltung eingeblendet. Alternativ ist eine gruppierte Anzeige wählbar. Über eine weitere Schaltfläche kann die komplette Tabelle im Vollbildmodus geöffnet werden. Diese Darstellung empfiehlt sich insbesondere dann, wenn Sie einen Eintrag per Drag&Drop über viele Zeilen verschieben wollen.



Die Regeln werden der Reihe nach geprüft. Die erste zutreffende Regel wird angewandt. Spezifischere Regeln müssen daher über den allgemeineren stehen. Eine Regel, die nur für eine spezielle IP-Adresse gilt, sollte also über einer Regel stehen, die für das selbe Protokoll aber beliebige IP-Adressen gilt.

Die Bedeutung der Felder im Einzelnen:

Aktiv

Mit Hilfe dieses Schalters lassen sich Regeln jederzeit aktivieren und deaktivieren. Um eine temporäre Firewall-Regel zu konfigurieren, wählen Sie das Datum und die Uhrzeit aus, bis zu deren Erreichen die Regel aktiv bleiben soll.

Log

Dieser Schalter aktiviert die Protokollierung der jeweiligen Regel. Bei TCP-Verbindungen wird nur der Verbindungsaufbau im Log vermerkt. Bei anderen IP-Protokollen wird jedes Paket protokolliert.



Um die Log-Dateien nicht zu groß werden zu lassen sollte die Protokollierung nur zu Diagnose-Zwecken und für selten genutzte Zugänge verwendet werden.

Protokoll

Wählen Sie hier das gewünschte Protokoll aus. Jedes Protokoll steht für eine Liste aus IP-Protokoll- und Port-Signaturen. Im Menü "Definitionen > Protokolle" können Sie diese einsehen und bei Bedarf auch mit eigenen Definitionen erweitern.

Quell-Zone

Verwenden Sie diese Einstellung, wenn die Regel ausschließlich für Verbindungen aus einer bestimmten Zone gelten soll.

Quell-IP/Netzwerk

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Quell-Adressen. Um einem einzelnen Client den Zugriff zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Sie können sich bei der Quelle der Regel auch auf MAC-Adressen beziehen. Verweisen Sie dazu auf Objekte vom Typ "Host", die Sie zuvor im Menü "Definitionen > IP-Objekte" anlegen müssen. Ist in einem solchen Objekt nur die MAC-Adresse angegeben, wird die Quelle ausschließlich anhand der MAC-Adresse gefiltert, und zwar sowohl für IPv4 als auch für IPv6. Ist zusätzlich eine IP-Adresse angegeben, greift die Regel nur, wenn bei einem IP-Paket sowohl die MAC- als auch die IP-Adresse passen. Ist im Objekt zwar eine IPv4-Adresse spezifiziert aber keine IPv6-Adresse, greift die Regel nur bei IPv4-Paketen. Ist eine IPv6-Adresse spezifiziert aber keine IPv4-Adresse, gilt die Regel entsprechend nur für IPv6.



Sie können mehrere Objekte vom Typ "Host" in einer Gruppe zusammenfassen, um mehrere MAC-Adressen und MAC-/IP-Kombinationen mit einer Regel zu erfassen.

Zugriff

Wählen Sie aus, ob der Zugriff erlaubt oder verboten sein soll. Bei einem verbotenen Verbindungsversuche kann SX-GATE das IP-Paket wahlweise einfach verwerfen oder aber mit einem ICMP-Antwortpaket "administratively prohibited" zurückweisen. Letzteres informiert den Absender über die Sperrung.

Ziel (...)

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Ziel-Adressen. Um den Zugriff auf einen einzelnen Server zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Ziel-Netzwerk freigegeben werden, muss

die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Zeitraum

Eine Regel kann auf Wunsch nur zu bestimmten Uhrzeiten an bestimmten Wochentagen gelten. Die Zeiträume werden im Menü "Definitionen > Zeiträume" festgelegt und könne hier zugewiesen werden.

DoS

Optional kann zusätzlich die Überwachung auf Denial-of-Service Angriffe durch die dynamische Firewall zugeschaltet werden. Für TCP-Verbindungen bezieht sich die Angabe auf die maximale Anzahl Verbindungen pro Quell-IP. Für alle anderen Protokolle wird die Anzahl Pakete pro Quell-IP begrenzt.

Kommentar

Dieses Feld können Sie zur Dokumentation nutzen. Bei aktiviertem Logging werden bis zu 14 Zeichen aus diesem Feld mitprotokolliert.

14.2.2-G SX-GATE > ...

Auf diesem Reiter (Tab) geht es um Verbindungen die SX-GATE initiiert.



Neben System-Funktionen wie der Übermittlung von Backups gehören dazu insbesondere auch Verbindungen die von den Proxy-Servern des SX-GATE aufgebaut werden.

Eine Beschränkung in diesem Bereich kann z.B. dann sinnvoll sein, wenn SX-GATE zwei Netzwerke trennt, die aufeinander keinen Zugriff erhalten dürfen. Direkte Verbindungen können über entsprechende Konfiguration der Weiterleitungsregeln unterbunden werden. Falls jedoch Zugriff auf die Proxies des SX-GATE besteht, könnte mit deren Hilfe ein indirekter Zugriff auf das andere Netzwerk erfolgen. Ausgehende Verbindungen über Proxy können daher mit Hilfe dieses Bereichs unterbunden werden.

Ausgehende Verbindungen: Quelle SX-GATE, Ziel ...

Um einen neuen Eintrag hinzuzufügen, drücken Sie bitte auf die Schaltfläche "Neuer Eintrag" in der unteren linken Ecke der Tabelle. Sie können einen bestehenden Eintrag als Vorlage verwenden: Drücken Sie dazu auf das zugehörige "Kopieren"-Symbol, das Sie in der letzten Spalte finden. Ein Ändern von Einträgen ist über das Stiftsymbol "Bearbeiten" möglich. Einzelne Einträge löschen Sie über die Mülltonne "Entfernen" in der jeweiligen Zeile. Mit der Mülltonne "Markierte Einträge löschen" im Kopf der Tabelle löschen Sie alle Zeilen, die Sie zuvor über die Kästchen am rechten Rand jeder Zeile ausgewählt haben. Das Kästchen in der Titlezeile wählt alle Zeilen aus. Mit Hilfe der Pfeilsymbole "Auf" und "Ab" kann die jeweilige Zeile um eine Position nach oben bzw. unten verschoben werden. Halten Sie die Maustaste auf dem "Drag'n'Drop" Symbol

rechts neben den Pfeilen gedrückt, um eine Zeile per Drag&Drop auf eine andere Position zu schieben. Ein Klick auf die Spaltentitel ändert die Sortierung. Beachten Sie bitte auch die Symbole für den Export und Import von Einträgen am unteren Rand der Tabelle.



Tabellen mit vielen Zeilen werden nicht vollständig angezeigt. Am unteren rechten Rand der Tabelle werden stattdessen Schaltflächen zur Seitenschaltung eingeblendet. Alternativ ist eine gruppierte Anzeige wählbar. Über eine weitere Schaltfläche kann die komplette Tabelle im Vollbildmodus geöffnet werden. Diese Darstellung empfiehlt sich insbesondere dann, wenn Sie einen Eintrag per Drag&Drop über viele Zeilen verschieben wollen.



Die Regeln werden der Reihe nach geprüft. Die erste zutreffende Regel wird angewandt. Spezifischere Regeln müssen daher über den allgemeineren stehen. Eine Regel, die nur für eine spezielle IP-Adresse gilt, sollte also über einer Regel stehen, die für das selbe Protokoll aber beliebige IP-Adressen gilt.

Die Bedeutung der Felder im Einzelnen:

Aktiv

Mit Hilfe dieses Schalters lassen sich Regeln jederzeit aktivieren und deaktivieren. Um eine temporäre Firewall-Regel zu konfigurieren, wählen Sie das Datum und die Uhrzeit aus, bis zu deren Erreichen die Regel aktiv bleiben soll.

Log

Dieser Schalter aktiviert die Protokollierung der jeweiligen Regel. Bei TCP-Verbindungen wird nur der Verbindungsaufbau im Log vermerkt. Bei anderen IP-Protokollen wird jedes Paket protokolliert.



Um die Log-Dateien nicht zu groß werden zu lassen sollte die Protokollierung nur zu Diagnose-Zwecken und für selten genutzte Zugänge verwendet werden.

Protokoll

Wählen Sie hier das gewünschte Protokoll aus. Jedes Protokoll steht für eine Liste aus IP-Protokoll- und Port-Signaturen. Im Menü "Definitionen > Protokolle" können Sie diese einsehen und bei Bedarf auch mit eigenen Definitionen erweitern.

Zugriff

Wählen Sie aus, ob der Zugriff erlaubt oder verboten sein soll. Bei einem verbotenen Verbindungsversuche kann SX-GATE das IP-Paket wahlweise

einfach verwerfen oder aber mit einem ICMP-Antwortpaket "administratively prohibited" zurückweisen. Letzteres informiert den Absender über die Sperrung.

Ziel (...)

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Ziel-Adressen. Um den Zugriff auf einen einzelnen Server zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Ziel-Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

DoS

Optional kann zusätzlich die Überwachung auf Denial-of-Service Angriffe durch die dynamische Firewall zugeschaltet werden. Für TCP-Verbindungen bezieht sich die Angabe auf die maximale Anzahl Verbindungen pro Quell-IP. Für alle anderen Protokolle wird die Anzahl Pakete pro Quell-IP begrenzt.

Kommentar

Dieses Feld können Sie zur Dokumentation nutzen. Bei aktiviertem Logging werden bis zu 14 Zeichen aus diesem Feld mitprotokolliert.

14.2.2-H * > SNAT

Auf diesem Reiter (Tab) definieren Sie Regeln für die Network-Adress-Translation (NAT, SNAT). Dabei wird die Quell-Adresse von Verbindungen verändert. Dies ist notwendig, wenn Pakete mit internen Absender-IPs in das Internet versendet werden sollen. Stehen SX-GATE mehrere Internet-IPs zur Verfügung, kann SNAT aber auch dazu genutzt werden, für einzelne Dienste eine bestimmte Absender-IP zu nutzen.



In den meisten Fällen muss hier keine Regel konfiguriert werden. Das Standard-Verhalten ist "automatisches SNAT", d.h. nur in Schnittstellen der Zone "Internet" wird überhaupt SNAT angewandt und zwar auf IPv4-Verbindungen aus der LAN- oder RAS-Zone. Davon ausgenommen sind Internet-Anbindungen mit DS-Lite.

SNAT: Quelle beliebig, Ziel ...

Um einen neuen Eintrag hinzuzufügen, drücken Sie bitte auf die Schaltfläche "Neuer Eintrag" in der unteren linken Ecke der Tabelle. Sie können einen bestehenden Eintrag als Vorlage verwenden: Drücken Sie dazu auf das zugehörige "Kopieren"-Symbol, das Sie in der letzten Spalte finden. Ein Ändern von Einträgen ist über das Stiftsymbol "Bearbeiten" möglich. Einzelne Einträge löschen Sie über die Mülltonne "Entfernen" in der jeweiligen Zeile. Mit der Mülltonne "Markierte Einträge löschen" im Kopf der Tabelle löschen Sie alle Zeilen, die Sie zuvor über die Kästchen am rechten Rand jeder Zeile ausgewählt haben. Das Kästchen in der Titlezeile wählt alle Zeilen aus. Mit Hilfe der

Pfeilsymbole "Auf" und "Ab" kann die jeweilige Zeile um eine Position nach oben bzw. unten verschoben werden. Halten Sie die Maustaste auf dem "Drag'n'Drop" Symbol rechts neben den Pfeilen gedrückt, um eine Zeile per Drag&Drop auf eine andere Position zu schieben. Ein Klick auf die Spaltentitel ändert die Sortierung. Beachten Sie bitte auch die Symbole für den Export und Import von Einträgen am unteren Rand der Tabelle.



Tabellen mit vielen Zeilen werden nicht vollständig angezeigt. Am unteren rechten Rand der Tabelle werden stattdessen Schaltflächen zur Seitenschaltung eingeblendet. Alternativ ist eine gruppierte Anzeige wählbar. Über eine weitere Schaltfläche kann die komplette Tabelle im Vollbildmodus geöffnet werden. Diese Darstellung empfiehlt sich insbesondere dann, wenn Sie einen Eintrag per Drag&Drop über viele Zeilen verschieben wollen.



Die Regeln werden der Reihe nach geprüft. Die erste zutreffende Regel wird angewandt. Spezifischere Regeln müssen daher über den allgemeineren stehen. Eine Regel, die nur für eine spezielle IP-Adresse gilt, sollte also über einer Regel stehen, die für das selbe Protokoll aber beliebige IP-Adressen gilt.

Die Bedeutung der Felder im Einzelnen:

Aktiv

Mit Hilfe dieses Schalters lassen sich Regeln jederzeit aktivieren und deaktivieren.

Log

Dieser Schalter aktiviert die Protokollierung der jeweiligen Regel. Bei TCP-Verbindungen wird nur der Verbindungsaufbau im Log vermerkt. Bei anderen IP-Protokollen wird jedes Paket protokolliert.



Um die Log-Dateien nicht zu groß werden zu lassen sollte die Protokollierung nur zu Diagnose-Zwecken und für selten genutzte Zugänge verwendet werden.

Protokoll

Wählen Sie hier das gewünschte Protokoll aus. Jedes Protokoll steht für eine Liste aus IP-Protokoll- und Port-Signaturen. Im Menü "Definitionen > Protokolle" können Sie diese einsehen und bei Bedarf auch mit eigenen Definitionen erweitern.

Einstellungen zur Anwendungserkennung werden ignoriert.

Quell-Zone

Verwenden Sie diese Einstellung, wenn die Regel ausschließlich für Verbindungen aus einer bestimmten Zone oder für Verbindungen die von SX-GATE selbst ausgehen gelten soll.

Quell-IP/Netzwerk

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Quell-Adressen. Um einem einzelnen Client den Zugriff zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Eine Filterung der Quelle nach MAC-Adresse ist bei SNAT-Regeln leider nicht möglich. In Objekten angegebene MAC-Adressen werden ignoriert.

NAT

Mit diesem Schalter steuern Sie die Network-Address-Translation (NAT, SNAT) für diese Regel. Dabei ersetzt SX-GATE die ursprüngliche Quell-IP-Adresse durch seine eigene.

Bei automatischem NAT findet dies ausschließlich bei IPv4-Verbindungen aus dem LAN- oder RAS-Bereich in das Internet Anwendung. Ausgenommen sind Internet-Anbindungen mit DS-lite.

Je Regel kann auch eine spezielle IP-Adresse angegeben werden, die bei aktiviertem SNAT eingesetzt wird. Hat SX-GATE mehrere Internet-IP-Adressen, so lässt sich auf diese Weise eine feste Zuordnung zwischen einer internen und einer externen IP-Adresse herstellen. Wenn keine Adresse eingetragen wird, verwendet SX-GATE automatisch die primäre IP-Adresse der jeweiligen Schnittstelle.



Wenn SX-GATE die IP-Adresse dynamisch bezieht, darf hier kein Wert vorgegeben werden.

Durch Eingabe einer Netzwerk-Adresse samt zugehöriger Netzmaske, lässt sich sogar eine statische 1:1-Abbildung zwischen den Adressen zweier Netzwerke konfigurieren. Der Eintrag "10.0.0.0/24" ersetzt beispielsweise die ersten drei Komponenten jeder Quell-IP mit "10.0.0". Aus der Quell-IP "192.168.1.254" wird so also "10.0.0.254".

Ziel (...)

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Ziel-Adressen. Um den Zugriff auf einen einzelnen Server zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Ziel-Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Kommentar

Dieses Feld können Sie zur Dokumentation nutzen. Bei aktiviertem Logging werden bis zu 14 Zeichen aus diesem Feld mitprotokolliert.

14.2.2-I Optionen

Automatische Sperrung auffälliger IPs (dynamische Firewall)

Zugriffe auf gesperrte Ports, Überschreiten der in den Firewall-Regeln vorgegebenen maximalen Verbindungsrate, Portscans aber auch Pings oder Traceroutes werden pro IP laufend registriert. Wird dabei für eine IP ein Schwellwert überschritten, kann diese IP für einen bestimmten Zeitraum automatisch gesperrt werden.

Private IP-Adressen (RFC-1918 und RFC-4193) sperren

Bei aktiviertem Schalter werden alle Pakete die über diese Schnittstelle laufen auf IP-Adressen aus den Netzwerken 192.168.0.0/255.255.0.0, 172.16.0.0/255.240.0.0 und 10.0.0.0/255.0.0.0 sowie fc00::/7 überprüft. Alle eingehenden und ausgehenden Pakete mit entsprechender Quell- oder Ziel-Adresse werden verworfen.

Traceroute und ICMP-Ping beantwortet Firewall

Eingehende ICMP echo-request-Pakete werden unabhängig von der eigentlichen Ziel-Adresse von der Firewall beantwortet. Eingehende Pakete mit niedrigen TTL-Werten deuten auf einen Traceroute hin. Diese werden ebenfalls unabhängig von der eigentlichen Ziel-Adresse vom SX-GATE beantwortet. Für den Absender des traceroutes sieht es so aus, als ob er im SX-GATE das Ziel-System erreicht hat.



Wird SX-GATE vor einem Netzwerk mit Internet-Adressen betrieben (z.B. vor einer DMZ), so kann deren Struktur und die tatsächlich aktiven Rechner weitgehend verborgen werden.

14.2.3 Bridge

Sofern es Schnittstellen gibt, die als Bridge konfiguriert sind, kann in diesem Menü die Firewall für die einzelnen Ports der Bridges konfiguriert werden. Dazu gehören insbesondere DNAT-Regeln, der Zugriff aus der Bridge auf SX-GATE-Dienste sowie Firewall-Regeln für Verbindungen die innerhalb der Bridge von einem Bridge-Port an einen anderen weitergeleitet werden. Für jeden Bridge-Port muss zudem die gewünschte Firewall-Zone ausgewählt werden, um die Grundkonfiguration der Firewall festzulegen.



Für Verbindungen, die von anderen Schnittstellen (oder Bridges) in eine Bridge geroutet werden, ist keine portspezifische Konfiguration der Firewall möglich. Selbiges gilt für Verbindungen, die ein SX-GATE-Dienst initiiert und die SNAT-Konfiguration. Konfigurieren Sie diese Einstellungen bitte im Menü "Regeln".



Durch unbedachte Änderungen in diesem Bereich kann die Sicherheit des SX-GATE und aller durch SX-GATE geschützten Netzwerke beeinträchtigt werden.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.2.3-A Allgemein.....	438
14.2.3-B DNAT > *	438
14.2.3-C Transp. Proxy.....	442
14.2.3-D ... > SX-GATE.....	445
14.2.3-E * > Bridge >	447
14.2.3-F Optionen.....	450

Zone/Klassifizierung (Vertrauen) des Bridge-Ports

Legen Sie über diesen Schalter die Basis-Konfiguration der Firewall für den ausgewählte Bridge-Port fest. Die Einstellung gilt für Verbindungen innerhalb der Bridge, für Verbindungen zu SX-GATE-Diensten und für Verbindungen die aus der Bridge heraus in eine andere Schnittstelle (oder Bridge) geroutet werden.

In der nachfolgenden Matrix lässt sich das Standard-Verhalten der Firewall für entsprechende Kombinationen von Vertrauensstellungen ablesen. Die Quelle bezieht sich dabei auf die Klassifikation des Eingangs-Ports, das Ziel entsprechend auf die

Klassifikation des Ausgangs-Ports (bei Verbindungen innerhalb der Bridge) bzw. der Ausgangs-Schnittstelle (bei Verbindungen die aus der Bridge heraus in eine andere Schnittstelle oder Bridge geroutet werden). Die Spalte "SX-GATE" beschreibt das Verhalten für Verbindungen zu SX-GATE. Innerhalb der Bridge wird kein SNAT durchgeführt. Der Vermerk "Auto-SNAT" bezieht sich rein auf Verbindungen die aus der Bridge heraus geroutet werden.

Quelle	Ziel				
	Internet (keines)	DMZ (gering)	RAS (mittel)	LAN (hoch)	SX-GATE
Internet (keines)					
DMZ (gering)					
RAS (mittel)	Auto-SNAT				
LAN (hoch)	Auto-SNAT				

	Zugriff gesperrt. Freigabe über Regeln
	Zugriff gesperrt. Freigabe über Regeln oder durch Änderung der Grundkonfiguration
	Zugriff erlaubt. Sperrung durch Änderung der Grundkonfiguration

14.2.3-A Allgemein

Beschreibung "..."

Dieser Text dient ausschließlich der Dokumentation.

Grundkonfiguration

In der Matrix lässt sich das Standardverhalten der Firewall für die aktuelle Schnittstelle ablesen und z.T. auch konfigurieren. Die angegebenen Voreinstellungen hängen ab von der Zone, der die Schnittstelle zugeordnet ist. Diese Zuordnung erfolgt über die Option "Zone/Klassifizierung (Vertrauen) des Bridge-Ports".

14.2.3-B DNAT > *

Auf diesem Reiter (Tab) definieren Sie Portforwarding-Regeln (DNAT). Dabei wird die Ziel-Adresse von Verbindungen verändert. Auf diese Weise ist es z.B. möglich, direkt aus dem Internet eine Verbindung zu einem Rechner mit einer internen IP-Adresse

herzustellen. DNAT-Regeln müssen in der Schnittstelle konfiguriert werden, über die SX-GATE die Verbindung empfängt.



Sofern das Ziel einer IPv4-Verbindung nach der DNAT-Verarbeitung nicht SX-GATE selbst ist, muss "IPv4-Routing" unter "Module > Firewall > Einstellungen" angeschaltet sein.



Eine DNAT-Verbindung kann nur dann funktionieren, wenn das neue Verbindungs-Ziel die Antwort-Pakete via SX-GATE an den Client zurücksendet. Nur dann hat SX-GATE die Möglichkeit, die Antwort-Pakete so anzupassen, dass diese vom Client zugeordnet werden können. Verfügt das Verbindungs-Ziel über keine passende Rück-Route, konfigurieren Sie bitte zusätzlich eine entsprechende SNAT-Regel.

DNAT (Portweiterleitung): Quelle ..., Ziel beliebig

Um einen neuen Eintrag hinzuzufügen, drücken Sie bitte auf die Schaltfläche "Neuer Eintrag" in der unteren linken Ecke der Tabelle. Sie können einen bestehenden Eintrag als Vorlage verwenden: Drücken Sie dazu auf das zugehörige "Kopieren"-Symbol, das Sie in der letzten Spalte finden. Ein Ändern von Einträgen ist über das Stiftsymbol "Bearbeiten" möglich. Einzelne Einträge löschen Sie über die Mülltonne "Entfernen" in der jeweiligen Zeile. Mit der Mülltonne "Markierte Einträge löschen" im Kopf der Tabelle löschen Sie alle Zeilen, die Sie zuvor über die Kästchen am rechten Rand jeder Zeile ausgewählt haben. Das Kästchen in der Titlezeile wählt alle Zeilen aus. Mit Hilfe der Pfeilsymbole "Auf" und "Ab" kann die jeweilige Zeile um eine Position nach oben bzw. unten verschoben werden. Halten Sie die Maustaste auf dem "Drag'n'Drop" Symbol rechts neben den Pfeilen gedrückt, um eine Zeile per Drag&Drop auf eine andere Position zu schieben. Ein Klick auf die Spaltentitel ändert die Sortierung. Beachten Sie bitte auch die Symbole für den Export und Import von Einträgen am unteren Rand der Tabelle.



Tabellen mit vielen Zeilen werden nicht vollständig angezeigt. Am unteren rechten Rand der Tabelle werden stattdessen Schaltflächen zur Seitenschaltung eingeblendet. Alternativ ist eine gruppierte Anzeige wählbar. Über eine weitere Schaltfläche kann die komplette Tabelle im Vollbildmodus geöffnet werden. Diese Darstellung empfiehlt sich insbesondere dann, wenn Sie einen Eintrag per Drag&Drop über viele Zeilen verschieben wollen.



Die Regeln werden der Reihe nach geprüft. Die erste zutreffende Regel wird angewandt. Spezifischere Regeln müssen daher über den allgemeineren stehen. Eine Regel, die nur für eine spezielle IP-Adresse gilt, sollte also über einer Regel stehen, die für das selbe Protokoll aber beliebige IP-Adressen gilt.

Die Bedeutung der Felder im Einzelnen:

Aktiv

Mit Hilfe dieses Schalters lassen sich Regeln jederzeit aktivieren und deaktivieren. Um eine temporäre Firewall-Regel zu konfigurieren, wählen Sie das Datum und die Uhrzeit aus, bis zu deren Erreichen die Regel aktiv bleiben soll.

Log

Dieser Schalter aktiviert die Protokollierung der jeweiligen Regel. Bei TCP-Verbindungen wird nur der Verbindungsaufbau im Log vermerkt. Bei anderen IP-Protokollen wird jedes Paket protokolliert.



Um die Log-Dateien nicht zu groß werden zu lassen sollte die Protokollierung nur zu Diagnose-Zwecken und für selten genutzte Zugänge verwendet werden.

Protokoll

Wählen Sie hier das gewünschte Protokoll aus. Jedes Protokoll steht für eine Liste aus IP-Protokoll- und Port-Signaturen. Im Menü "Definitionen > Protokolle" können Sie diese einsehen und bei Bedarf auch mit eigenen Definitionen erweitern.

Die Applikationserkennung funktioniert hier nur eingeschränkt, da DNAT-Regeln das tatsächliche Ziel einer Verbindung schon mit dem ersten Paket festlegen müssen. Bei TCP-Verbindung wurden zu diesem Zeitpunkt noch keinerlei Nutzdaten übertragen, die eine Erkennung der Anwendung erlauben würden. Bei anderen IP-Protokollen wie z.B. UDP kann zumindest bei manchen Anwendungen bereits das erste Datenpaket zu einer Erkennung führen. Ist die Anwendung noch unbekannt, greift die DNAT-Regel bereits, wenn lediglich das IP-Protokoll und die Portsignatur des Pakets passen. Stellt sich später im Laufe der Verbindung heraus, dass es sich nicht um die gewünschte Anwendung handelt, wird die Verbindung unterbrochen.

Quelle (...)

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Quell-Adressen. Um einem einzelnen Client den Zugriff zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Sie können sich bei der Quelle der Regel auch auf MAC-Adressen beziehen. Verweisen Sie dazu auf Objekte vom Typ "Host", die Sie zuvor im Menü "Definitionen > IP-Objekte" anlegen müssen. Ist in einem solchen Objekt nur die MAC-Adresse angegeben, wird die Quelle ausschließlich anhand der MAC-Adresse gefiltert, und zwar sowohl für IPv4 als auch für IPv6. Ist zusätzlich eine IP-Adresse angegeben, greift die Regel nur, wenn bei einem IP-Paket sowohl die MAC- als auch die IP-Adresse passen. Ist im Objekt zwar eine IPv4-Adresse spezifiziert aber keine IPv6-Adresse, greift die Regel nur bei IPv4-Paketen. Ist eine IPv6-Adresse spezifiziert aber keine IPv4-Adresse, gilt die Regel entsprechend nur für IPv6.



Sie können mehrere Objekte vom Typ "Host" in einer Gruppe zusammenfassen, um mehrere MAC-Adressen und MAC-/IP-Kombinationen mit einer Regel zu erfassen.

Zugriff

Wählen Sie aus, ob der Zugriff erlaubt oder verboten sein soll. Bei einem verbotenen Verbindungsversuche verwirft SX-GATE das IP-Paket.

Ziel

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Ziel-Adressen. Um den Zugriff auf einen einzelnen Server zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Ziel-Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.



Wenn SX-GATE die IP-Adresse dynamisch bezieht, darf hier kein Wert vorgegeben werden.

zu IP

Hier wird festgelegt, an welche Adresse das Paket weitergeleitet wird. Es kann sich dabei sowohl um eine IP-Adresse des SX-GATE (ausgenommen 127.0.0.1) als auch um die Adresse eines anderen Systems handeln. Bei "verwerfen" muss zwar eine Adresse angegeben werden, diese wird aber nicht verwendet.

Durch Eingabe einer Netzwerk-Adresse samt zugehöriger Netzmaske, lässt sich eine statische 1:1-Abbildung zwischen den Adressen zweier Netzwerke konfigurieren. Der Eintrag "10.0.0.0/24" ersetzt beispielsweise die ersten drei Komponenten jeder Ziel-IP mit "10.0.0.". Aus der Ziel-IP "192.168.1.254" wird so also "10.0.0.254".



Es ist in diesem Fall nicht möglich, auch den Ziel-Port umzuschreiben. Das Feld "Port" muss frei bleiben.

Port

Lassen Sie dieses Feld frei um den Ziel-Port des ursprünglichen Pakets beizubehalten. Andernfalls geben Sie bitte hier den neuen Ziel-Port an.

Zeitraum

Eine Regel kann auf Wunsch nur zu bestimmten Uhrzeiten an bestimmten Wochentagen gelten. Die Zeiträume werden im Menü "Definitionen > Zeiträume" festgelegt und können hier zugewiesen werden.

DoS

Optional kann zusätzlich die Überwachung auf Denial-of-Service Angriffe durch die dynamische Firewall zugeschaltet werden. Für TCP-Verbindungen bezieht sich die Angabe auf die maximale Anzahl Verbindungen pro Quell-IP. Für alle anderen Protokolle wird die Anzahl Pakete pro Quell-IP begrenzt.

Kommentar

Dieses Feld können Sie zur Dokumentation nutzen. Bei aktiviertem Logging werden bis zu 14 Zeichen aus diesem Feld mitprotokolliert.

14.2.3-C Transp. Proxy

Einige SX-GATE Dienste können als transparenter Proxy fungieren. Ohne den Client umkonfigurieren zu müssen, können so die Vorteile dieses Dienstes genutzt werden. Die Schalter auf dieser Seite aktivieren die notwendigen Firewall-Regeln um bestimmte Verbindungen an den zugehörigen SX-GATE-Proxy umzuleiten.



Stellen Sie sicher, dass der jeweilige Proxy-Dienst auch aktiviert ist.

Die Regeln gelten unabhängig von Quell- und Ziel-Adressen für alle Clients die an der gewählten Schnittstelle angeschlossen sind. Um den transparenten Zugriff nur für bestimmte Adressen zu nutzen, können alternativ selbst entsprechende Regeln auf dem Reiter (Tab) "DNAT > *" konfiguriert werden.

Anhand der Umleitung auf SX-GATEs Web-Proxy soll exemplarisch erläutert werden, welche Firewall-Regeln mit der Aktivierung der entsprechenden Option verknüpft sind. Im Beispiel sei die IP-Adresse des SX-GATE 192.168.0.254. Verbindungen zu Port 80 (HTTP) beliebiger Server müssen also an SX-GATEs Web-Proxy auf Port 8082 umgeleitet werden. Dies bewerkstelligt die DNAT-Regel "HTTP:*->*>192.168.0.254(8082)".

Kein transparenter Proxy für Verbindungen zu

Verbindungen zu bestimmten Zielen können vom transparenten Proxying ausgenommen werden (z.B. interne Netze).



Verbindungen zu IP-Adressen des SX-GATEs sind stets automatisch vom transparenten Proxying ausgenommen.

Port 80 (HTTP) auf Web-Proxy

Dieser Schalter aktiviert transparenten Zugriff auf SX-GATEs Web-Proxy. Zugriffe auf Port 80 beliebiger Ziel-Adressen werden dazu an den Web-Proxy umgelenkt. Eine Proxy-Authentifizierung findet bei transparenten Zugriffen grundsätzlich nicht statt.



Diese Option ist nicht verfügbar, wenn in der Konfiguration des Web-Proxies der transparente Proxy-Modus deaktiviert ist.

ohne Content-Filter

Bei Auswahl dieser Einstellung werden die Verbindungen an den Web-Proxy auf Port 8083 umgeleitet. Der Content-Filter wird dadurch umgangen. Sie können diese Option für ein Netzwerk mit geringerem Schutzbedarf wählen, wenn der Content-Filter wiederholt unerwartete Probleme verursacht. Stellen Sie dann jedoch sicher, dass die Firewall den Zugriff auf Netze mit höherem Schutzbedarf sowohl direkt als auch über Proxy verhindert.



Diese Option ist nicht verfügbar, wenn der Content-Filter deaktiviert ist oder das Umgehen des Content-Filters deaktiviert ist.

aktiviert

In dieser Einstellung werden die Verbindungen an den lokalen Port 8082 umgeleitet. Sowohl der URL- als auch der Content-Filter des Web-Proxies werden genutzt, sofern diese aktiviert sind.

Port 443 (HTTPS) auf Web-Proxy

Dieser Schalter aktiviert transparenten HTTPS Zugriff auf SX-GATEs Web-Proxy. Zugriffe auf Port 443 beliebiger Ziel-Adressen werden dazu an den Web-Proxy umgelenkt. Eine Proxy-Authentifizierung findet bei transparenten Zugriffen grundsätzlich nicht statt.



Diese Option ist nicht verfügbar, wenn in der Konfiguration des Web-Proxies der transparente Proxy-Modus deaktiviert ist.

ohne Content-Filter

Bei Auswahl dieser Einstellung werden die Verbindungen an den Web-Proxy auf Port 8446 umgeleitet. Der Content-Filter wird dadurch umgangen. Dies ist hilfreich, wenn im Content-Filter das Aufbrechen von SSL-Verbindungen aktiviert ist, auf den Endgeräten aber keine Proxy-CA installiert werden kann, wie es z.B. bei einem Mitarbeiter-WLAN mit privaten Endgeräten (BYOD) der Fall ist.



Diese Option ist nicht verfügbar, wenn der Content-Filter deaktiviert ist oder das Umgehen des Content-Filters deaktiviert ist.

aktiviert

In dieser Einstellung werden die Verbindungen an den lokalen Port 8445 umgeleitet. Sowohl der URL- als auch der Content-Filter des Web-Proxies werden genutzt, sofern diese aktiviert sind.

Port 21 (FTP) auf FTP-Proxy

Analog zur vorhergehenden Option werden über diesen Schalter Verbindungen zu Port 21 an den SX-GATE FTP-Proxy umgeleitet (Port 2121).

Port 5060 (Voice-over-IP SIP) auf SIP-Proxy

Dieser Schalter wirkt sich auf Pakete des Voice-over-IP Protokolls SIP aus. Pakete zu TCP- und UDP-Port 5060 mit beliebiger Ziel-Adresse werden an die Adresse des SX-GATE und damit an den SIP-Proxy gesendet.

Port 110 (POP3) auf POP3-/SMTP-Proxy

Verbindungen zu TCP-Port 110 einer Internet IP-Adresse werden mit Hilfe dieser Option über SX-GATEs POP3-Proxy (Port 8110) umgeleitet.

Port 25 (SMTP) auf

Direkte SMTP-Verbindungen in das Internet lassen sich mit Hilfe dieser Option abfangen und an einen Server-Dienst auf dem SX-GATE umleiten. Die Ziel-IP von Verbindungen zu Port 25 wird dabei durch die IP-Adresse des SX-GATE ersetzt.

Mail-Relay-Server

Bei Auswahl dieser Einstellung werden die Verbindungen an den SX-GATE Mail-Relay-Server umgeleitet. Dieser übernimmt die weitere Verarbeitung vollständig, so als hätte der Absender keine Verbindung in das Internet versucht sondern die Mail unmittelbar an SX-GATEs Mail-Relay-Server übergeben.

SMTP-Proxy

Hier wird die Mail an SX-GATEs POP3-/SMTP-Proxy (Port 8110) übergeben, der seinerseits Verbindung mit dem ursprünglich adressierten Mail-Server aufnimmt.

Sofern die entsprechende Option aktiviert ist, prüft SX-GATEs SMTP-Proxy die Mail dabei auf Viren. Die eigentliche Verarbeitung der Mail erfolgt jedoch durch den vom Absender vorgegebenen Mail-Server.

Port 53 (DNS) auf DNS-Forwarder

DNS-Pakete lassen sich durch diesen Schalter an den Namens-Server des SX-GATE umlenken. Dies betrifft sowohl TCP- als auch UDP-Pakete zu Port 53.

14.2.3-D ... > SX-GATE

Auf diesem Reiter (Tab) geht es um Verbindungen zu SX-GATE. Ziel ist einer der Server-Dienste, die SX-GATE anbietet.

Eingehende Verbindungen: Quelle ..., Ziel SX-GATE

Um einen neuen Eintrag hinzuzufügen, drücken Sie bitte auf die Schaltfläche "Neuer Eintrag" in der unteren linken Ecke der Tabelle. Sie können einen bestehenden Eintrag als Vorlage verwenden: Drücken Sie dazu auf das zugehörige "Kopieren"-Symbol, das Sie in der letzten Spalte finden. Ein Ändern von Einträgen ist über das Stiftsymbol "Bearbeiten" möglich. Einzelne Einträge löschen Sie über die Mülltonne "Entfernen" in der jeweiligen Zeile. Mit der Mülltonne "Markierte Einträge löschen" im Kopf der Tabelle löschen Sie alle Zeilen, die Sie zuvor über die Kästchen am rechten Rand jeder Zeile ausgewählt haben. Das Kästchen in der Titlezeile wählt alle Zeilen aus. Mit Hilfe der Pfeilsymbole "Auf" und "Ab" kann die jeweilige Zeile um eine Position nach oben bzw. unten verschoben werden. Halten Sie die Maustaste auf dem "Drag'n'Drop" Symbol rechts neben den Pfeilen gedrückt, um eine Zeile per Drag&Drop auf eine andere Position zu schieben. Ein Klick auf die Spaltentitel ändert die Sortierung. Beachten Sie bitte auch die Symbole für den Export und Import von Einträgen am unteren Rand der Tabelle.



Tabellen mit vielen Zeilen werden nicht vollständig angezeigt. Am unteren rechten Rand der Tabelle werden stattdessen Schaltflächen zur Seitenschaltung eingeblendet. Alternativ ist eine gruppierte Anzeige wählbar. Über eine weitere Schaltfläche kann die komplette Tabelle im Vollbildmodus geöffnet werden. Diese Darstellung empfiehlt sich insbesondere dann, wenn Sie einen Eintrag per Drag&Drop über viele Zeilen verschieben wollen.



Die Regeln werden der Reihe nach geprüft. Die erste zutreffende Regel wird angewandt. Spezifischere Regeln müssen daher über den allgemeineren stehen. Eine Regel, die nur für eine spezielle IP-Adresse gilt, sollte also über einer Regel stehen, die für das selbe Protokoll aber beliebige IP-Adressen gilt.

Die Bedeutung der Felder im Einzelnen:

Aktiv

Mit Hilfe dieses Schalters lassen sich Regeln jederzeit aktivieren und deaktivieren. Um eine temporäre Firewall-Regel zu konfigurieren, wählen Sie das Datum und die Uhrzeit aus, bis zu deren Erreichen die Regel aktiv bleiben soll.

Log

Dieser Schalter aktiviert die Protokollierung der jeweiligen Regel. Bei TCP-Verbindungen wird nur der Verbindungsaufbau im Log vermerkt. Bei anderen IP-Protokollen wird jedes Paket protokolliert.



Um die Log-Dateien nicht zu groß werden zu lassen sollte die Protokollierung nur zu Diagnose-Zwecken und für selten genutzte Zugänge verwendet werden.

Protokoll

Wählen Sie hier das gewünschte Protokoll aus. Jedes Protokoll steht für eine Liste aus IP-Protokoll- und Port-Signaturen. Im Menü "Definitionen > Protokolle" können Sie diese einsehen und bei Bedarf auch mit eigenen Definitionen erweitern.

Quelle (...)

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Quell-Adressen. Um einem einzelnen Client den Zugriff zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Sie können sich bei der Quelle der Regel auch auf MAC-Adressen beziehen. Verweisen Sie dazu auf Objekte vom Typ "Host", die Sie zuvor im Menü "Definitionen > IP-Objekte" anlegen müssen. Ist in einem solchen Objekt nur die MAC-Adresse angegeben, wird die Quelle ausschließlich anhand der MAC-Adresse gefiltert, und zwar sowohl für IPv4 als auch für IPv6. Ist zusätzlich eine IP-Adresse angegeben, greift die Regel nur, wenn bei einem IP-Paket sowohl die MAC- als auch die IP-Adresse passen. Ist im Objekt zwar eine IPv4-Adresse spezifiziert aber keine IPv6-Adresse, greift die Regel nur bei IPv4-Paketen. Ist eine IPv6-Adresse spezifiziert aber keine IPv4-Adresse, gilt die Regel entsprechend nur für IPv6.



Sie können mehrere Objekte vom Typ "Host" in einer Gruppe zusammenfassen, um mehrere MAC-Adressen und MAC-/IP-Kombinationen mit einer Regel zu erfassen.

Zugriff

Wählen Sie aus, ob der Zugriff erlaubt oder verboten sein soll. Bei einem verbotenen Verbindungsversuche kann SX-GATE das IP-Paket wahlweise einfach verwerfen oder aber mit einem ICMP-Antwortpaket "administratively prohibited" zurückweisen. Letzteres informiert den Absender über die Sperrung.

Zeitraum

Eine Regel kann auf Wunsch nur zu bestimmten Uhrzeiten an bestimmten Wochentagen gelten. Die Zeiträume werden im Menü "Definitionen > Zeiträume" festgelegt und könne hier zugewiesen werden.

DoS

Optional kann zusätzlich die Überwachung auf Denial-of-Service Angriffe durch die dynamische Firewall zugeschaltet werden. Für TCP-Verbindungen bezieht sich die Angabe auf die maximale Anzahl Verbindungen pro Quell-IP. Für alle anderen Protokolle wird die Anzahl Pakete pro Quell-IP begrenzt.

Kommentar

Dieses Feld können Sie zur Dokumentation nutzen. Bei aktiviertem Logging werden bis zu 14 Zeichen aus diesem Feld mitprotokolliert.

14.2.3-E * > Bridge > ...

Auf diesem Reiter (Tab) geht es um Verbindungen, die SX-GATE von einem Bridge-Port an einen anderen weiterleitet. SX-GATE selbst ist dabei weder Quelle noch Ziel der Verbindung.



Weiterleitungs-Regeln werden im SX-GATE stets im Ausgangs-Port konfiguriert.

Bridging: Quelle: beliebiger Bridge-Port, Ziel: Bridge-Port ...

Um einen neuen Eintrag hinzuzufügen, drücken Sie bitte auf die Schaltfläche "Neuer Eintrag" in der unteren linken Ecke der Tabelle. Sie können einen bestehenden Eintrag als Vorlage verwenden: Drücken Sie dazu auf das zugehörige "Kopieren"-Symbol, das Sie in der letzten Spalte finden. Ein Ändern von Einträgen ist über das Stiftsymbol "Bearbeiten" möglich. Einzelne Einträge löschen Sie über die Mülltonne "Entfernen" in der jeweiligen Zeile. Mit der Mülltonne "Markierte Einträge löschen" im Kopf der Tabelle löschen Sie alle Zeilen, die Sie zuvor über die Kästchen am rechten Rand jeder Zeile ausgewählt haben. Das Kästchen in der Titlezeile wählt alle Zeilen aus. Mit Hilfe der Pfeilsymbole "Auf" und "Ab" kann die jeweilige Zeile um eine Position nach oben bzw.

unten verschoben werden. Halten Sie die Maustaste auf dem "Drag'n'Drop" Symbol rechts neben den Pfeilen gedrückt, um eine Zeile per Drag&Drop auf eine andere Position zu schieben. Ein Klick auf die Spaltentitel ändert die Sortierung. Beachten Sie bitte auch die Symbole für den Export und Import von Einträgen am unteren Rand der Tabelle.



Tabellen mit vielen Zeilen werden nicht vollständig angezeigt. Am unteren rechten Rand der Tabelle werden stattdessen Schaltflächen zur Seitenschaltung eingeblendet. Alternativ ist eine gruppierte Anzeige wählbar. Über eine weitere Schaltfläche kann die komplette Tabelle im Vollbildmodus geöffnet werden. Diese Darstellung empfiehlt sich insbesondere dann, wenn Sie einen Eintrag per Drag&Drop über viele Zeilen verschieben wollen.



Die Regeln werden der Reihe nach geprüft. Die erste zutreffende Regel wird angewandt. Spezifischere Regeln müssen daher über den allgemeineren stehen. Eine Regel, die nur für eine spezielle IP-Adresse gilt, sollte also über einer Regel stehen, die für das selbe Protokoll aber beliebige IP-Adressen gilt.

Die Bedeutung der Felder im Einzelnen:

Aktiv

Mit Hilfe dieses Schalters lassen sich Regeln jederzeit aktivieren und deaktivieren. Um eine temporäre Firewall-Regel zu konfigurieren, wählen Sie das Datum und die Uhrzeit aus, bis zu deren Erreichen die Regel aktiv bleiben soll.

Log

Dieser Schalter aktiviert die Protokollierung der jeweiligen Regel. Bei TCP-Verbindungen wird nur der Verbindungsaufbau im Log vermerkt. Bei anderen IP-Protokollen wird jedes Paket protokolliert.



Um die Log-Dateien nicht zu groß werden zu lassen sollte die Protokollierung nur zu Diagnose-Zwecken und für selten genutzte Zugänge verwendet werden.

Protokoll

Wählen Sie hier das gewünschte Protokoll aus. Jedes Protokoll steht für eine Liste aus IP-Protokoll- und Port-Signaturen. Im Menü "Definitionen > Protokolle" können Sie diese einsehen und bei Bedarf auch mit eigenen Definitionen erweitern.

Quell-Zone

Verwenden Sie diese Einstellung, wenn die Regel ausschließlich für Verbindungen aus einer bestimmten Zone gelten soll.

Quell-IP/Netzwerk

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Quell-Adressen. Um einem einzelnen Client den Zugriff zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Sie können sich bei der Quelle der Regel auch auf MAC-Adressen beziehen. Verweisen Sie dazu auf Objekte vom Typ "Host", die Sie zuvor im Menü "Definitionen > IP-Objekte" anlegen müssen. Ist in einem solchen Objekt nur die MAC-Adresse angegeben, wird die Quelle ausschließlich anhand der MAC-Adresse gefiltert, und zwar sowohl für IPv4 als auch für IPv6. Ist zusätzlich eine IP-Adresse angegeben, greift die Regel nur, wenn bei einem IP-Paket sowohl die MAC- als auch die IP-Adresse passen. Ist im Objekt zwar eine IPv4-Adresse spezifiziert aber keine IPv6-Adresse, greift die Regel nur bei IPv4-Paketen. Ist eine IPv6-Adresse spezifiziert aber keine IPv4-Adresse, gilt die Regel entsprechend nur für IPv6.



Sie können mehrere Objekte vom Typ "Host" in einer Gruppe zusammenfassen, um mehrere MAC-Adressen und MAC-/IP-Kombinationen mit einer Regel zu erfassen.

Zugriff

Wählen Sie aus, ob der Zugriff erlaubt oder verboten sein soll. Bei einem verbotenen Verbindungsversuche kann SX-GATE das IP-Paket wahlweise einfach verwerfen oder aber mit einem ICMP-Antwortpaket "administratively prohibited" zurückweisen. Letzteres informiert den Absender über die Sperrung.

Ziel (...)

Ohne Eintrag in diesen Feldern gilt die Regel für beliebige Ziel-Adressen. Um den Zugriff auf einen einzelnen Server zu gestatten, geben Sie bitte dessen IP-Adresse ein. Soll hingegen ein ganzes Ziel-Netzwerk freigegeben werden, muss die Netzwerk-Adresse zusammen mit einer passenden Netzmaske eingegeben werden (z.B. 192.168.0.0/24). Soll eine Regel für mehrere einzelne Adressen oder Netzwerke gelten, legen Sie bitte dafür eine Gruppe im Menü "Definitionen > IP-Objekte" an bzw. wählen Sie eine bereits definierte Gruppe aus.

Zeitraum

Eine Regel kann auf Wunsch nur zu bestimmten Uhrzeiten an bestimmten Wochentagen gelten. Die Zeiträume werden im Menü "Definitionen > Zeiträume" festgelegt und könne hier zugewiesen werden.

DoS

Optional kann zusätzlich die Überwachung auf Denial-of-Service Angriffe durch die dynamische Firewall zugeschaltet werden. Für TCP-Verbindungen bezieht sich die Angabe auf die maximale Anzahl Verbindungen pro Quell-IP. Für alle anderen Protokolle wird die Anzahl Pakete pro Quell-IP begrenzt.

Kommentar

Dieses Feld können Sie zur Dokumentation nutzen. Bei aktiviertem Logging werden bis zu 14 Zeichen aus diesem Feld mitprotokolliert.

14.2.3-F Optionen

Automatische Sperrung auffälliger IPs (dynamische Firewall)

Zugriffe auf gesperrte Ports, Überschreiten der in den Firewall-Regeln vorgegebenen maximalen Verbindungsrate, Portscans aber auch Pings oder Traceroutes werden pro IP laufend registriert. Wird dabei für eine IP ein Schwellwert überschritten, kann diese IP für einen bestimmten Zeitraum automatisch gesperrt werden.

Private IP-Adressen (RFC-1918 und RFC-4193) sperren

Bei aktiviertem Schalter werden alle Pakete die über diese Schnittstelle laufen auf IP-Adressen aus den Netzwerken 192.168.0.0/255.255.0.0, 172.16.0.0/255.240.0.0 und 10.0.0.0/255.0.0.0 sowie fc00::/7 überprüft. Alle eingehenden und ausgehenden Pakete mit entsprechender Quell- oder Ziel-Adresse werden verworfen.

Traceroute und ICMP-Ping beantwortet Firewall

Eingehende ICMP echo-request-Pakete werden unabhängig von der eigentlichen Ziel-Adresse von der Firewall beantwortet. Eingehende Pakete mit niedrigen TTL-Werten deuten auf einen Traceroute hin. Diese werden ebenfalls unabhängig von der eigentlichen Ziel-Adresse vom SX-GATE beantwortet. Für den Absender des traceroutes sieht es so aus, als ob er im SX-GATE das Ziel-System erreicht hat.



Wird SX-GATE vor einem Netzwerk mit Internet-Adressen betrieben (z.B. vor einer DMZ), so kann deren Struktur und die tatsächlich aktiven Rechner weitgehend verborgen werden.

14.3 DHCP

Für Ethernet-, VLAN- und WLAN-Schnittstellen kann im SX-GATE der DHCP-Server konfiguriert werden. Für das unmittelbar am SX-GATE angeschlossene Netz können sowohl IPv4- als auch IPv6-Adressen verteilt werden. Klicken Sie dazu auf den jeweiligen Schnittstellennamen. Für IPv4 lassen sich zudem Adressen für Netze vergeben, die über ein DHCP-Relay mit dem SX-GATE kommunizieren. Die Einrichtung erfolgt durch Klick auf "Indirekte Subnetze" neben dem zugehörigen Schnittstellennamen. Alternativ kann SX-GATE für IPv4 auch als DHCP-Relay konfiguriert werden. Klicken Sie dazu wiederum auf den Schnittstellennamen.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden.

14.3.1

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.3.1-A Dynamische IPv4-Adressen.....	452
14.3.1-B Feste IPv4-Adressen.....	453
14.3.1-C Netzwerk-Parameter.....	454
14.3.1-D Windows-Parameter.....	454
14.3.1-E Weitere Parameter.....	455
14.3.1-F Eigene Optionen.....	455
14.3.1-G DHCPv4-Relay.....	456
14.3.1-H Dynamische IPv6-Adressen.....	456
14.3.1-I Feste IPv6-Adressen.....	457
14.3.1-J DHCPv6 Netzwerk-Parameter.....	458

DHCPv4

Wählen Sie hier den DHCPv4-Modus aus.

Server

In diesem Modus vergibt SX-GATE die IP-Adresse.

Relay

In diesem Modus nimmt SX-GATE DHCP-Anfragen entgegen, leitet Sie dann aber an einen DHCP-Server in einem anderen Netzwerk weiter.

14.3.1-A Dynamische IPv4-Adressen

Per DHCP zu vergebende Adressbereiche

Hier können Sie Adressbereiche definieren, die SX-GATE per DHCP dynamisch an anfragende Geräte vergeben soll. Bitte stellen Sie sicher, dass von den hier eingetragenen Adressen keine bereits einem Gerät im Netzwerk fest zugeordnet ist. Andernfalls kann es zu Konflikten mit doppelten IP-Adressen kommen.



Adressen können auch relativ zum primären Adressbereich der Schnittstelle angegeben werden, indem der Netzwerkteil der Adresse auf "0" gesetzt wird. Ist das primäre Subnetz z.B. 192.168.0.0/24, so steht der Bereich "0.0.0.100-0.0.0.199" tatsächlich für "192.168.0.100-192.168.0.199".



Alle hier angegebenen Adressbereiche müssen zum primären IP-Adressbereich der jeweiligen Schnittstelle passen.

Gültigkeits-Dauer vergebener Adressen

Mit Hilfe der Gültigkeits-Dauer können Sie bestimmen, wie lange eine zugewiesene Adresse für ein Gerät reserviert bleiben soll. Setzen Sie diese Adresse auf einen niedrigen Wert, wenn häufig Geräte nur kurz in das LAN eingebunden werden.

SX-GATE ist Backup DHCP-Server (secondary)

Aktivieren Sie diese Option, wenn Sie SX-GATE als sekundären DHCP-Server verwenden wollen.



Sollten Sie den DHCP-Server unnötigerweise als sekundären DHCP-Server konfiguriert haben, äußert sich dies in einer verlängerten Startdauer der Arbeitsstationen. Sind mehrere primäre DHCP-Server aktiv, weist der jeweils schneller antwortende Server die IP-Konfiguration zu. Je nach Verhalten der beteiligten Server kann es unter Umständen aber auch zu Störungen kommen.

Im Unterschied zum primären DHCP-Dienst antwortet SX-GATE als sekundärer DHCP-Server nicht auf die erste Anfrage eines Gerätes nach eine IP-Adresse. SX-GATE antwortet erst dann, wenn einige Sekunden vergangen sind und das Gerät immer noch nach einer IP-Adresse verlangt. In diesem Falle geht der SX-GATE davon aus, dass der eigentliche DHCP-Server nicht verfügbar ist und weist der Arbeitsstation eine IP-Adresse zu.



Bitte beachten Sie, dass sich die dynamisch zugewiesenen IP-Adressbereiche des primären und des sekundären DHCP-Servers nicht überschneiden dürfen, da der primäre Server nichts von der Existenz des sekundären weiß. Folglich kann es bei Überschneidungen zu Konflikten kommen.

14.3.1-B Feste IPv4-Adressen

Fest zugewiesene IPv4-Adressen

Mit Hilfe dieses Eingabebereiches können Sie bewerkstelligen, dass bestimmten Geräten per DHCP immer die selbe IPv4-Adresse zugewiesen wird. Das Gerät wird dabei an der Hardware-Adresse von dessen Netzwerkkarte (MAC-Adresse) identifiziert. Um einem Gerät eine feste Adresse zuzuweisen, geben Sie bitte in den entsprechenden Feldern die gewünschte IP-Adresse, einen Namen, sowie die das Gerät identifizierende MAC-Adresse ein. Die IP-Adresse kann dabei relativ zum primären Adressbereich der Schnittstelle angegeben werden, indem der Netzwerkteil der Adresse auf "0" gesetzt wird. Ist das primäre Subnetz z.B. 192.168.0.0/24, so steht die Adresse "0.0.0.200" tatsächlich für "192.168.0.200". Der Name dient lediglich zu Ihrer Information und kann frei vergeben werden. Die MAC-Adresse ist in hexadezimaler Schreibweise anzugeben, wobei die einzelnen Bytes durch Doppelpunkte voneinander zu trennen sind (z.B. 0a:43:94:fc:83:0e).



Wird die Netzwerkkarte eines hier definierten Gerätes getauscht, so ändert sich dessen MAC-Adresse. Um der neuen Netzwerkkarte wieder die richtige Adresse zuzuordnen, ist der Eintrag hier entsprechend anzupassen.



Fest vergebene IP-Adressen dürfen nicht im Bereich der dynamisch zu vergebenden IP-Adressen enthalten sein, müssen aber zum primären IP-Adressbereich der jeweiligen Schnittstelle passen.

14.3.1-C Netzwerk-Parameter

Die meisten Einstellungen in diesem Bereich beziehen sich in der Regel immer auf Ihren SX-GATE. Deswegen sind in der Grundeinstellung hierfür stets die entsprechenden Werte voreingestellt. Diese Vorgaben können im Bedarfsfall jedoch beliebig geändert werden.

Domain-Name

Diese Einstellung legt fest, welcher Domain-Name den Clients per DHCP zugewiesen wird.

Gateway (Router)

Das Standard-Gateway für DHCP-Clients wird mit Hilfe dieser Einstellung festgelegt.

DNS 1

Der SX-GATE DHCP-Server weist diese IP-Adresse als primären Namens-Server zu.

DNS 2

Hier haben Sie optional die Möglichkeit, einen zweiten Namens-Server einzutragen. Dieser wird von den Clients dann befragt, wenn der primäre DNS nicht verfügbar ist bzw. nur mit Verzögerung antwortet. Tragen Sie hier z. B. den DNS Ihres Providers ein oder ein Namens-Server innerhalb Ihres LANs.

14.3.1-D Windows-Parameter

Die Einstellungen in diesem Bereich sind speziell für Microsoft-Windows-Netzwerke vorgesehen. Die Angabe von Werte ist optional.

Web-Proxy Auto-Discovery URL

Die meisten Web-Browser können die Proxy-Konfiguration automatisch beziehen. Dazu lädt der Browser eine Konfigurationsdatei von einem Web-Server herunter. Die Adresse dieser Datei wird mit Hilfe der Web-Proxy Auto-Discovery (WPAD) ermittelt. Dieses Verfahren sieht u.a. vor, die Adresse via DHCP bekannt zu geben. Bislang wird dies aber nur vom Microsoft Internet Explorer unterstützt sofern auf dem Client DHCP aktiv ist. Alternativ können Sie im Menü "Module > HTTP-Server" ein DNS basiertes Verfahren aktivieren. Dieses wird auch von anderen Browsern unterstützt und funktioniert auch dann, wenn DHCP nicht verwendet wird.

Stellen Sie hier die URL ein, unter der die Konfigurationsdatei heruntergeladen werden kann. Der SX-GATE Konfigurations-Server stellt selbst eine passende Konfigurationsdatei zur Verfügung. Nutzen Sie diese wenn die Browser den SX-GATE Web-Proxy verwenden sollen. Alternativ können Sie aber auch die Adresse einer eigenen Konfigurationsdatei hinterlegen.

WINS 1

Hier können Sie den primären WINS-Server festlegen. WINS wird von Windows benötigt, um Rechner netzwerkübergreifend zu finden.

WINS 2

Hier kann ein zweiter WINS-Server eingetragen werden.

NetBIOS-Knotentyp

Hier lässt sich der NetBIOS-Knotentyp zuweisen. Über diese Einstellung wird die Nutzung von WINS bzw. Broadcast-Paketen durch Windows-Clients geregelt.

14.3.1-E Weitere Parameter**NTP-Server 1**

Tragen Sie hier die IP-Adresse eines NTP-Zeitserver ein, von dem die Clients die Systemzeit beziehen können.

NTP-Server 2

Hier haben Sie optional die Möglichkeit, einen zweiten NTP-Server einzutragen.

BOOTP Server-IP

Geben Sie hier die IP-Adresse des Servers an, von dem das Boot-Image geladen werden soll.

BOOTP-Datei

Geben Sie hier den Dateinamen des Boot-Images an.

14.3.1-F Eigene Optionen**Benutzerdefinierte DHCP-Optionen**

Für spezielle Anwendungsfälle können hier eigene Optionen definiert werden. Dabei stehen jedoch nur elementare Datentypen zur Verfügung.



Um eine Liste von IP-Adressen oder Zahlen zu erhalten, geben Sie diese bitte mit Komma getrennt an.

14.3.1-G DHCPv4-Relay

Adressen der DHCP-Server

Geben Sie hier die IP-Adressen der DHCP-Server an, an die SX-GATE DHCP-Anfragen weiterleiten soll.



Stellen Sie bitte sicher, dass auf den DHCP-Servern eine Route konfiguriert ist, die Pakete für das Client-Netzwerk zum SX-GATE schickt.

Der Relay-Server nutzt das Feld "Link-Selection" der DHCP-Option 82 (Agent-Information-Option) um dem DHCP server mitzuteilen, aus welchem IP-Kreis er die Adresse für den DHCP-Client auswählen soll. Das Feld Relay-Agent-IP (giaddr) enthält die IP der Schnittstelle, über die das Relay mit dem DHCP-Server kommuniziert.



Es kann notwendig sein, den IP-Bereich dieser SX-GATE-Schnittstelle im DHCP-Server zusätzlich zum IP-Bereich für die DHCP-Clients zu definieren, damit der DHCP-Server dies unterstützt.

14.3.1-H Dynamische IPv6-Adressen

Per DHCP zu vergebender Adressbereich

Hier können Sie den Adressbereich definieren, den SX-GATE per DHCP dynamisch an anfragende Geräte vergeben soll. Bitte stellen Sie sicher, dass von den hier eingetragenen Adressen keine bereits einem Gerät im Netzwerk fest zugeordnet ist. Andernfalls kann es zu Konflikten mit doppelten IP-Adressen kommen.



Der hier angegebene Adressbereich muss zum primären IP-Adressbereich der jeweiligen Schnittstelle passen.

Der Präfix kann auf einem vom Provider dynamisch zugewiesenen Präfix basieren. Beim Hinzufügen eines neuen Eintrags werden Ihnen die im Menü "Definitionen > IP-Objekte" angelegten Präfixe zur Auswahl angeboten. Sie können im besagten Menü auch selbst Einträge vom Typ "IPv6-Präfix" anlegen, um z.B. den vom Provider erhaltenen Präfix weiter zu unterteilen.

Gültigkeits-Dauer vergebener Adressen

Mit Hilfe der Gültigkeits-Dauer können Sie bestimmen, wie lange eine zugewiesene Adresse für ein Gerät reserviert bleiben soll. Setzen Sie diese Adresse auf einen niedrigen Wert, wenn häufig Geräte nur kurz in das LAN eingebunden werden.

14.3.1-I Feste IPv6-Adressen

Fest zugewiesene IPv6-Adressen

Mit Hilfe dieses Eingabebereiches können Sie bewerkstelligen, dass bestimmten Geräten per DHCP immer die selbe IPv6-Adresse zugewiesen wird. Das Gerät wird dabei an der Hardware-Adresse von dessen Netzwerkkarte (MAC-Adresse) identifiziert. Um einem Gerät eine feste Adresse zuzuweisen, geben Sie bitte in den entsprechenden Feldern die gewünschte IP-Adresse, einen Namen, sowie die das Gerät identifizierende MAC-Adresse ein. Der Name dient lediglich zu Ihrer Information und kann frei vergeben werden. Die MAC-Adresse ist in hexadezimaler Schreibweise anzugeben, wobei die einzelnen Bytes durch Doppelpunkte voneinander zu trennen sind (z.B. 0a:43:94:fc:83:0e).



Wird die Netzwerkkarte eines hier definierten Gerätes getauscht, so ändert sich dessen MAC-Adresse. Um der neuen Netzwerkkarte wieder die richtige Adresse zuzuordnen, ist der Eintrag hier entsprechend anzupassen.

Falls es sich bei dem Gerät um einen Router handelt, können Sie diesem neben einer IPv6-Adresse auch einen IPv6-Präfix zuweisen, den der Router seinerseits an nachgelagerte Geräte verteilt. Eine entsprechende Route für den Präfix wird vom SX-GATE automatisch konfiguriert.



Der verwendete Präfix darf sich nicht mit anderen lokalen Netzen überschneiden. Insbesondere darf die dem Router zugewiesene IPv6-Adresse nicht Teil des Präfixes sein.

Sowohl die zugewiesenen IPv6-Adressen als auch die zugewiesenen Präfixe können auf einem vom Provider dynamisch zugewiesenen Präfix basieren. Beim Hinzufügen eines neuen Eintrags werden Ihnen die im Menü "Definitionen > IP-Objekte" angelegten IPv6-Adressen bzw. Präfixe zur Auswahl angeboten. Legen im besagten Menü bitte bei Bedarf Einträge vom Typ "IPv6-Adresse" bzw. "IPv6-Präfix" an, mit denen Sie den vom Provider erhaltenen Präfix entsprechend unterteilen.

14.3.1-J DHCPv6 Netzwerk-Parameter

Die meisten Einstellungen in diesem Bereich beziehen sich in der Regel immer auf Ihren SX-GATE. Deswegen sind in der Grundeinstellung hierfür stets die entsprechenden Werte voreingestellt. Diese Vorgaben können im Bedarfsfall jedoch beliebig geändert werden.

DNS 1

Der SX-GATE DHCP-Server weist diese IP-Adresse als primären Namens-Server zu.

DNS 2

Hier haben Sie optional die Möglichkeit, einen zweiten Namens-Server einzutragen. Dieser wird von den Clients dann befragt, wenn der primäre DNS nicht verfügbar ist bzw. nur mit Verzögerung antwortet. Tragen Sie hier z. B. den DNS Ihres Providers ein oder ein Namens-Server innerhalb Ihres LANs.

14.3.2 - Indirekte Subnetze

Netze, die über einen Router mit SX-GATE verbunden sind, können vom SX-GATE DHCP-Server mit IPv4-Konfigurationen versorgt werden. Dazu muss auf dem Router ein DHCP-Relay laufen, das DHCP-Anfragen an den SX-GATE weiterleitet. Legen Sie dann hier diese indirekt verbundenen Netze an, um zugehörige DHCP-Konfigurationen zu erstellen.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.3.2-A Dynamische IPv4-Adressen	459
14.3.2-B Feste IPv4-Adressen	460
14.3.2-C Netzwerk-Parameter	461
14.3.2-D Windows-Parameter	461
14.3.2-E Weitere Parameter	462
14.3.2-F Eigene Optionen	463

14.3.2-A Dynamische IPv4-Adressen

Kommentar

Dieses Feld steht zu Dokumentationszwecken zu Ihrer freien Verfügung.

Per DHCP zu vergebende Adressbereiche

Hier können Sie Adressbereiche definieren, die SX-GATE per DHCP dynamisch an anfragende Geräte vergeben soll. Bitte stellen Sie sicher, dass von den hier eingetragenen Adressen keine bereits einem Gerät im Netzwerk fest zugeordnet ist. Andernfalls kann es zu Konflikten mit doppelten IP-Adressen kommen.



Adressen können auch relativ zum Subnetz angegeben werden, indem der Netzwerkteil der Adresse auf "0" gesetzt wird. Ist das Subnetz z.B. 192.168.0.0/24, so steht der Bereich "0.0.0.100-0.0.0.199" tatsächlich für "192.168.0.100-192.168.0.199".



Alle hier angegebenen Adressbereiche müssen zum Subnetz passen.

Gültigkeits-Dauer vergebener Adressen

Mit Hilfe der Gültigkeits-Dauer können Sie bestimmen, wie lange eine zugewiesene Adresse für ein Gerät reserviert bleiben soll. Setzen Sie diese Adresse auf einen niedrigen Wert, wenn häufig Geräte nur kurz in das LAN eingebunden werden.

SX-GATE ist Backup DHCP-Server (secondary)

Aktivieren Sie diese Option, wenn Sie SX-GATE als sekundären DHCP-Server verwenden wollen.



Sollten Sie den DHCP-Server unnötigerweise als sekundären DHCP-Server konfiguriert haben, äußert sich dies in einer verlängerten Startdauer der Arbeitsstationen. Sind mehrere primäre DHCP-Server aktiv, weist der jeweils schneller antwortende Server die IP-Konfiguration zu. Je nach Verhalten der beteiligten Server kann es unter Umständen aber auch zu Störungen kommen.

Im Unterschied zum primären DHCP-Dienst antwortet SX-GATE als sekundärer DHCP-Server nicht auf die erste Anfrage eines Gerätes nach eine IP-Adresse. SX-GATE antwortet erst dann, wenn einige Sekunden vergangen sind und das Gerät immer noch nach einer IP-Adresse verlangt. In diesem Falle geht der SX-GATE davon aus, dass der eigentliche DHCP-Server nicht verfügbar ist und weist der Arbeitsstation eine IP-Adresse zu.



Bitte beachten Sie, dass sich die dynamisch zugewiesenen IP-Adressbereiche des primären und des sekundären DHCP-Servers nicht überschneiden dürfen, da der primäre Server nichts von der Existenz des sekundären weiß. Folglich kann es bei Überschneidungen zu Konflikten kommen.

14.3.2-B Feste IPv4-Adressen

Fest zugewiesene IPv4-Adressen

Mit Hilfe dieses Eingabebereiches können Sie bewerkstelligen, dass bestimmten Geräten per DHCP immer die selbe IPv4-Adresse zugewiesen wird. Das Gerät wird dabei an der Hardware-Adresse von dessen Netzwerkkarte (MAC-Adresse) identifiziert. Um einem Gerät eine feste Adresse zuzuweisen, geben Sie bitte in den entsprechenden Feldern die gewünschte IP-Adresse, einen Namen, sowie die das Gerät identifizierende MAC-Adresse ein. Die IP-Adresse kann dabei relativ zum primären Adressbereich der Schnittstelle angegeben werden, indem der Netzwerkteil der Adresse auf "0" gesetzt wird. Ist das primäre Subnetz z.B. 192.168.0.0/24, so steht die Adresse "0.0.0.200" tatsächlich für "192.168.0.200". Der Name dient lediglich zu Ihrer Information und kann frei vergeben werden. Die MAC-Adresse ist in hexadezimaler Schreibweise anzugeben, wobei die einzelnen Bytes durch Doppelpunkte voneinander zu trennen sind (z.B. 0a:43:94:fc:83:0e).



Wird die Netzwerkkarte eines hier definierten Gerätes getauscht, so ändert sich dessen MAC-Adresse. Um der neuen Netzwerkkarte wieder die richtige Adresse zuzuordnen, ist der Eintrag hier entsprechend anzupassen.



Fest vergebene IP-Adressen dürfen nicht im Bereich der dynamisch zu vergebenden IP-Adressen enthalten sein, müssen aber zum primären IP-Adressbereich der jeweiligen Schnittstelle passen.

14.3.2-C Netzwerk-Parameter

Die meisten Einstellungen in diesem Bereich beziehen sich in der Regel immer auf Ihren SX-GATE. Deswegen sind in der Grundeinstellung hierfür stets die entsprechenden Werte voreingestellt. Diese Vorgaben können im Bedarfsfall jedoch beliebig geändert werden.

Domain-Name

Diese Einstellung legt fest, welcher Domain-Name den Clients per DHCP zugewiesen wird.

Gateway (Router)

Das Standard-Gateway für DHCP-Clients wird mit Hilfe dieser Einstellung festgelegt.

DNS 1

Der SX-GATE DHCP-Server weist diese IP-Adresse als primären Namens-Server zu.

DNS 2

Hier haben Sie optional die Möglichkeit, einen zweiten Namens-Server einzutragen. Dieser wird von den Clients dann befragt, wenn der primäre DNS nicht verfügbar ist bzw. nur mit Verzögerung antwortet. Tragen Sie hier z. B. den DNS Ihres Providers ein oder ein Namens-Server innerhalb Ihres LANs.

14.3.2-D Windows-Parameter

Die Einstellungen in diesem Bereich sind speziell für Microsoft-Windows-Netzwerke vorgesehen. Die Angabe von Werte ist optional.

Web-Proxy Auto-Discovery URL

Die meisten Web-Browser können die Proxy-Konfiguration automatisch beziehen. Dazu lädt der Browser eine Konfigurationsdatei von einem Web-Server herunter. Die Adresse dieser Datei wird mit Hilfe der Web-Proxy Auto-Discovery (WPAD) ermittelt. Dieses Verfahren sieht u.a. vor, die Adresse via DHCP bekannt zu geben. Bislang wird dies aber nur vom Microsoft Internet Explorer unterstützt sofern auf dem Client DHCP aktiv ist. Alternativ können Sie im Menü "Module > HTTP-Server" ein DNS basiertes Verfahren aktivieren. Dieses wird auch von anderen Browsern unterstützt und funktioniert auch dann, wenn DHCP nicht verwendet wird.

Stellen Sie hier die URL ein, unter der die Konfigurationsdatei heruntergeladen werden kann. Der SX-GATE Konfigurations-Server stellt selbst eine passende Konfigurationsdatei zur Verfügung. Nutzen Sie diese wenn die Browser den SX-GATE Web-Proxy verwenden sollen. Alternativ können Sie aber auch die Adresse einer eigenen Konfigurationsdatei hinterlegen.

WINS 1

Hier können Sie den primären WINS-Server festlegen. WINS wird von Windows benötigt, um Rechner netzwerkübergreifend zu finden.

WINS 2

Hier kann ein zweiter WINS-Server eingetragen werden.

NetBIOS-Knotentyp

Hier lässt sich der NetBIOS-Knotentyp zuweisen. Über diese Einstellung wird die Nutzung von WINS bzw. Broadcast-Paketen durch Windows-Clients geregelt.

14.3.2-E Weitere Parameter**NTP-Server 1**

Tragen Sie hier die IP-Adresse eines NTP-Zeitserver ein, von dem die Clients die Systemzeit beziehen können.

NTP-Server 2

Hier haben Sie optional die Möglichkeit, einen zweiten NTP-Server einzutragen.

BOOTP Server-IP

Geben Sie hier die IP-Adresse des Servers an, von dem das Boot-Image geladen werden soll.

BOOTP-Datei

Geben Sie hier den Dateinamen des Boot-Images an.

14.3.2-F Eigene Optionen

Benutzerdefinierte DHCP-Optionen

Für spezielle Anwendungsfälle können hier eigene Optionen definiert werden. Dabei stehen jedoch nur elementare Datentypen zur Verfügung.



Um eine Liste von IP-Adressen oder Zahlen zu erhalten, geben Sie diese bitte mit Komma getrennt an.

14.4 DNS

14.4.1 Einstellungen

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.4.1-A Provider-DNS.....	464
14.4.1-B Client-Zugriff.....	465
14.4.1-C DNS-Regeln.....	466
14.4.1-D Dynamischer DNS.....	467

14.4.1-A Provider-DNS

Namensauflösung über folgende Nameserver

DNS-Anfragen für Adressen, für die SX-GATE nicht selbst zuständig ist, werden an Namens-Server im Internet weitergeleitet. Dazu sollte der SX-GATE die DNS-Anfrage zunächst an die DNS-Server Ihres Providers weitergeben, die Sie hier spezifizieren können. Sind mehrere Server angegeben, werden diese in der Reihenfolge ihrer Antwortgeschwindigkeit befragt.



Sind keine Nameserver hinterlegt, erfolgt die Namensauflösung stets mit Hilfe der sogenannten Root-Nameserver des Internets. Die Namensauflösung nimmt in diesem Falle jedoch meist deutlich mehr Zeit in Anspruch.

Ausschließlich diese Namens-Server befragen

Mit Hilfe dieses Schalters steuern Sie, ob SX-GATE zusätzlich zu den angegebenen Namens-Servern des Providers auch die Internet Root-Nameserver befragt werden dürfen. Bei fehlender oder verzögerter Antwort des zunächst befragten Provider DNS kann eine entsprechende Anfrage an die Root-Name-Server gestellt werden. Sollte sich SX-GATE hinter einer Firewall befinden, so ist dieses Verhalten im allgemeinen nicht erwünscht. Aktivieren Sie in diesem Falle diese Option. Sind keine Namens-Server des Providers spezifiziert, so hat dieser Schalter keine Wirkung.

DNS wenn möglich automatisch beziehen

Wenn diese Option aktiviert ist und SX-GATE über eine ADSL-Wählverbindung an das Internet angeschlossen ist oder die IP-Konfiguration per DHCP erhält, werden

die Name-Server des Providers automatisch bezogen. Es wird ausschließlich die Schnittstelle berücksichtigt, über die die Default-Route führt.



Dynamisch bezogene DNS Adressen haben Vorrang vor manuell konfigurierten. Letztere werden nur dann verwendet, wenn keine DNS-Information bezogen werden konnte.

14.4.1-B Client-Zugriff

Lokale IP-Adressen

Diese Einstellung beeinflusst sowohl die DNS-Forwarder-Funktion des SX-GATE (DNS-Proxy) als auch die Namens-Server-Funktionalität. Nur lokale IP-Adressen können SX-GATE als DNS-Proxy nutzen. Die Weiterleitung von DNS-Anfragen in das Internet (recursion) ist entsprechend eingeschränkt. Die Abfrage von lokalen DNS-Zonen die nicht als "Öffentliche Zone" konfiguriert sind, ist ebenfalls nur den hier eingestellten lokalen Adressen möglich.

DNSSec Validierung

Aktivieren Sie diesen Schalter, damit der SX-GATE DNS-Forwarder alle erhaltenen Antworten mittels DNSSec überprüft.



Bei aktivierter Validierung erhöhen sich der Bedarf an Speicher, CPU und Netzwerkbandbreite.

Antworten mit privaten IPs sperren

Aktivieren Sie diesen Schalter, um DNS-Rebinding Angriffe zu verhindern. Die Weiterleitung von DNS-Antworten mit IPs aus den privaten IP-Bereichen 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, fe80::/10 und fc00::/7 wird dann blockiert.

DNS-Anfragen protokollieren

Dieser Schalter aktiviert die Aufzeichnung jeder Anfrage an den DNS-Server des SX-GATE. Dies kann insbesondere bei der Internetanbindung über Wählleitung nützlich sein, um fehlerhaft konfigurierte Rechner im LAN aufzuspüren, die mit DNS-Anfragen wiederholt Verbindungsaufbauten in das Internet auslösen.



Bei aktivierter Protokollierung kann es durch das oft hohe Aufkommen an DNS-Anfragen zu Leistungseinbußen kommen. Zudem kann die Größe der Logdateien und damit auch der davon belegte Festplattenplatz stark ansteigen. Die dauerhafte Aktivierung dieser Funktion wird daher nicht empfohlen.

14.4.1-C DNS-Regeln

DNS-Antworten überschreiben und sperren

Hier können DNS-Antworten überschrieben oder auch ganz gesperrt werden. Welche Werte für einen neuen Eintrag anzugeben sind, hängt vom gewählten Typ des Eintrags ab.

A/AAAA/CNAME

Abhängig vom Wert der als "Ziel" angegeben wurde, wird der Namen auf eine IPv4-Adresse, IPv6-Adresse oder einen anderen DNS-Namen abgebildet. Wenn Sie "Ziel" leer lassen, wird der angefragte Name als nicht existent gemeldet.

Um einen Reverse-Lookup zu überschreiben (PTR), tragen Sie die IP-Adresse unter "DNS-Name" in der Schreibweise mit ".in-addr.arpa" bzw. ".ip6.arpa" ein. Bei "Ziel" wird der zugehörige Hostname oder auch nichts eingetragen.

MX

Gibt den Mail-Server für eine Domain an. Geben Sie in das erste Feld eine Mail-Domain (den Teil hinter dem @) ein. Im zweiten Feld muss der Hostname eines Mail-Servers hinterlegt werden. Der MX-Zahlenwert gibt die Priorität an. Der MX-Eintrag mit der niedrigsten Priorität wird als erstes kontaktiert. Im Fehlerfall wird dann versucht, die Mail an die Server mit höheren Prioritätswerten zuzustellen. Sind für die selbe Domain mehrere MX-Einträge mit gleicher Priorität hinterlegt, so wird bei der Auflösung der DNS-Anfrage zufällig eine der Adressen ausgewählt. Ist unter dieser Adresse kein Mail-Server erreichbar, wird mit der nächsten Adresse fortgefahren.

NS

Gibt den Namens-Server für eine Domain an. Geben Sie in das erste Feld eine Domain ein. Im zweiten Feld muss der Hostname eines Namens-Servers hinterlegt werden. Sind für eine Domain mehrere NS-Einträge hinterlegt, wählt der Client zufällig einen davon aus. Ist dieser Namens-Server nicht erreichbar, wird mit der nächsten Adresse fortgefahren.

SRV

Spezifiziert den Server für einen bestimmten Dienst. Der Eintrag muss mit "_Dienstname._Protokoll" beginnen (z.B. "_sip._udp"). Als Wert geben Sie bitte den zugehörigen UDP- bzw. TCP-Port, ein Leerzeichen und dann den Servernamen an (z.B. "5060 www.example.com").

TXT

Erlaubt die Angabe eines beliebigen Textes.

14.4.1-D Dynamischer DNS

Dynamischer DNS ermöglicht es, ein Gerät, das eigentlich mit einer dynamischen IP-Adresse an das Internet angebunden ist, unter dessen jeweils aktueller Adresse aufzufinden. Mit Hilfe dieses Dienstes kann also vom Internet aus auf SX-GATE zugegriffen werden, obwohl dieser nur über eine dynamische IP-Adresse verfügt. Die Adressierung im dynamischen DNS erfolgt mit Hilfe eines üblichen DNS-Rechnernamens (Fully-Qualified-Domain-Name, FQDN). Es gibt eine Reihe von Anbietern, die dynamischen DNS sowohl als kostenlose als auch als kostenpflichtige Dienstleistung zur Verfügung stellen.



Nach einem IP-Wechsel vergehen einige Sekunden bis Minuten, bis der DNS-Name auch tatsächlich auf die neue IP-Adresse verweist.

Sofern SX-GATE selbst die dynamische IP erhält (ADSL-Schnittstelle mit dynamischer IP oder Ethernet-Schnittstelle mit IP-Vergabe über DHCP), konfigurieren Sie dynamischen DNS bitte in der jeweiligen Schnittstelle im Menü "Module > Netzwerk > Schnittstellen". SX-GATE aktualisiert seine IP-Adresse im dynamischen DNS dann einmalig bei jedem Verbindungsaufbau bzw. IP-Wechsel.

Für den Fall, dass sich SX-GATE hinter einem NAT-Router befindet und dieser die dynamische IP erhält, muss der NAT-Router eingehende Verbindungen an SX-GATE weiterreichen können (DNAT, Portforwarding, Exposed Host). Optimalerweise konfigurieren Sie dynamischen DNS im NAT-Router, da nur dieser die aktuelle dynamische IP kennt. Ist dies nicht möglich, konfigurieren Sie dynamischen DNS bitte hilfsweise im SX-GATE Menü "Module > DNS > Einstellungen". SX-GATE versucht dann in regelmäßigen Abständen die dynamische IP des NAT-Routers mit Hilfe eines Internet-Dienstes zu ermitteln.

Protokoll

Für die Aktualisierung der Einträge im dynamischen DNS gibt es leider keinen einheitlichen Standard. SX-GATE unterstützt jedoch eine ganze Reihe von Protokollen für diese Aktualisierung. Bitte klären Sie zunächst mit dem Anbieter des dynamischen DNS-Dienstes, welches Protokoll verwendet wird und ob dieses vom SX-GATE unterstützt wird.

Update-Server des Anbieters

Tragen Sie hier bitte den Namen des Servers ein, der die Nachrichten zur Aktualisierung der dynamischen IP-Adresse entgegen nimmt. Dieser Server ist nicht immer identisch mit dem Webserver des Anbieters.

Update-URL

Tragen Sie hier bitte die Update-URL (auch "Direct URL" genannt) zur Aktualisierung der dynamischen IP-Adresse ein. Die URL kann die Platzhalter <host>, <ipaddr>, <username> und <password> enthalten, die durch den dynamischen DNS-Namen, die IP-Adresse, den Benutzernamen und das Passwort ersetzt werden. Beispiel: `http://dynupdate.exampledynDNS.com/nic/update?hostname=<domain>&myip=<ipaddr>`

Dynamischer DNS-Name des SX-GATES

Über ein Benutzerkonto bei dem jeweiligen Anbieter lassen sich in der Regel mehrere DNS-Namen verwalten. Daher ist hier der vollständige Name (inkl. Domain) anzugeben, unter dem SX-GATE im dynamischen DNS erreichbar ist.

Benutzername

Keine Aktualisierung des Eintrags im dynamischen DNS ohne entsprechende Anmeldung. Geben Sie hier den Benutzernamen (login) für das Konto an.

Passwort

Geben Sie hier schließlich das entsprechende Kennwort für die Aktualisierung an.

URL zur Ermittlung der Internet-IP

Tragen Sie hier die URL eines Internetdienstes ein, über den SX-GATE die externe IP ermitteln kann (z.B. `checkip.dyndns.org`). Die so ermittelte Adresse hinterlegt SX-GATE dann im dynamischen DNS.

Intervall zur Prüfung auf IP-Änderung

Legen Sie hier das Zeitintervall fest, in dem SX-GATE prüft, ob sich die externen IP geändert hat.



Eine möglichst häufige Prüfung ist natürlich wünschenswert. Möglicherweise limitiert jedoch der Internetdienst zur Ermittlung der externen IP die Häufigkeit der Zugriffe.



Auf Cluster-Systemen aktualisiert jeweils ausschließlich der aktuelle Master-Knoten den dynamischen DNS.

Jetzt aktualisieren

Hiermit können Sie die eingegebenen Verbindungsdaten testen.

14.4.2 Zonen

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Zonen Typ

Legen Sie hier eine neue DNS-Zone an, für die SX-GATE zuständig (authoritative) sein soll. DNS-Anfragen an eine solche Zone werden nicht an Namens-Server im Internet weitergeleitet sondern vom DNS des SX-GATE beantwortet.

IPv4-Adressbereich (Reverse lookup)

Eine Reverse-Lookup-Zone kann üblicherweise nur für die Netzwerke der Klassen A, B und C eingerichtet werden (Netzmasken 255.0.0.0, 255.255.0.0 und 255.255.255.0). Geben Sie dazu ausschließlich die signifikanten Teile der IP-Adresse an. Einige Beispiele:

Klasse A: 10.0.0.0/255.0.0.0 (10.in-addr.arpa.)

Eingabe: 10

Klasse B: 10.5.0.0/255.255.0.0 (5.10.in-addr.arpa.)

Eingabe: 10.5

Klasse C: 10.5.0.0/255.255.255.0 (0.5.10.in-addr.arpa.)

Eingabe: 10.5.0



Wurde von Ihrem Provider eine sogenannte "Classless in-addr.arpa Delegation" gemäß RFC 2317 vorgenommen, so sind hier eventuell von diesem Schema abweichende Einträge notwendig. Bedenken Sie jedoch, dass sich der hier angegebene Name vom tatsächlichen Zonen-Namen dahingehend unterscheidet, dass die Reihenfolge der durch Punkte getrennten Einzelteile invertiert wird.

IPv6-Adressbereich (Reverse lookup)

Geben Sie hier bitte nur die relevanten Stellen des IPv6-Präfixes an, für den Sie Adressen definieren möchten. Sofern der Präfix nicht mit einem Doppelpunkt oder

einer vier-stelligen Hexadezimalzahl endet, müssen ggf. führende Nullen ergänzt werden (z.B. statt "2001:db8" entweder "2001:0db8" oder "2001:db8:").

Netzwerk: fd00::/8 (d.f.ip6.arpa.)

Eingabe: "fd"

Netzwerk: fd00::/12 (0.d.f.ip6.arpa.)

Eingabe: "fd0"

Netzwerk: 2001:db8::/32 (8.b.d.0.1.0.0.2.ip6.arpa.)

Eingabe: "2001:db8:" oder "2001:0db8". Die Eingabe "2001:db8" steht hingegen für 2001:db80/28 und wäre somit falsch.

Netzwerk: 2001:db8::/64 (0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.)

Eingabe: "2001:db8:0:0:" oder "2001:db8:0:0000". Falsch wären z.B. "2001:db8:0:" (steht für 2001:db8::/112) oder "2001:db8:0:0" (steht für 2001:db8::/52).

14.4.2.1 Domain

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.4.2.1-A Einträge.....	471
14.4.2.1-B SOA.....	473
14.4.2.1-C NS.....	473
14.4.2.1-D MX.....	474
14.4.2.1-E Zugriffsberechtigungen.....	474
14.4.2.1-F Weiterleitung.....	475

Typ

Wählen Sie hier bitte aus, in welcher Funktion SX-GATE die DNS-Zone verwaltet.

Master

Die Einträge in der DNS-Zone müssen in dieser Einstellung auf SX-GATE vorgenommen werden. SX-GATE ist für deren Inhalt verantwortlich.

Slave

In dieser Einstellung spiegelt SX-GATE den Inhalt einer DNS-Zone, die auf einem anderen Namens-Server verwaltet wird. Der Inhalt selbst kann auf SX-GATE nicht verändert werden. Um den Zonen-Transfer durchführen zu können, muss die Adresse des Master-Servers im Reiter (Tab) "Zugriffsberechtigungen" eingetragen werden.

Weiterleitung

Anders als bei den vorigen Optionen, tritt SX-GATE hier nicht als Verwalter für die Zone auf sondern leitet Anfragen an einen anderen Name-Server weiter.

14.4.2.1-A Einträge

Benutzerdefinierte Einträge

Hier können entsprechende Einträge in der Zone vorgenommen werden. Für NS- und MX-Einträge zur Zone selbst nutzen Sie bitte die entsprechenden eigenen Reiter (Tabs).



Beachten Sie bitte stets die absolute bzw. relative Schreibweise eines DNS-Eintrags. Endet ein Eintrag mit einem Punkt, so handelt es sich um einen absoluten Eintrag (z.B. "www.example.com."). Bei einem relativen Eintrag fehlt dieser Punkt. Die aktuelle Zone wird dann automatisch an den Eintrag angehängt. Lautet die Zone "example.com", so wird damit aus dem Eintrag "www" automatisch "www.example.com.". Wird fälschlicherweise "www.example.com" angegeben - also ohne schließenden Punkt - so ist dieser Eintrag gleichbedeutend mit "www.example.com.example.com.".

Welche Werte für einen neuen Eintrag anzugeben sind, hängt vom gewählten Typ des Eintrags ab.

A

Bildet einen Namen auf eine IP-Adresse ab. Geben Sie in das erste Feld einen relativen oder absoluten Namen ein, in das zweite eine IP-Adresse. Sind für einen Namen mehrere A-Einträge hinterlegt, so wählt der Client bei der DNS-Anfrage zufällig einen Eintrag aus. Ist der angesprochene Dienst auf dieser IP-Adresse nicht erreichbar, wird mit der nächsten Adresse fortgefahren.

AAAA

Wie "A" jedoch für IPv6 Adressen.

CAA

Legt fest, welche CAs berechtigt sind, für den entsprechenden Host- oder Domainnamen Zertifikate auszustellen. CAA-Records werden ausschließlich von CAs beim Ausstellen eines Zertifikats abgefragt und sollen das misbräuchliche Ausstellen von Zertifikaten erschweren. Geben Sie im ersten Feld den Host- oder Domainnamen ein, im zweiten die CA-Domain. Fragen Sie bei Ihrer CA nach, welchen Wert sie im CAA-Record erwartet. Tragen Sie anstelle der CA-Domain einen Strichpunkt ein, um das Ausstellen von Zertifikaten für einen Host oder eine Domain zu verbieten. Um mehrere CAs zuzulassen, können Sie mehrere CAA-Einträge je Host oder Domain hinterlegen.

Wird im zweiten Feld nur der CA-Name bzw. ein Strichpunkt angegeben, wird ein Eintrag vom Typ "issue" erzeugt, also die Ausstellung eines normalen Zertifikats beeinflusst. Dies ist gleichbedeutend mit der Schreibweise "issue ca.example.com" bzw. "issue ;". Um die Ausstellung von Wildcard-Zertifikaten zu beeinflussen, geben Sie "issuewild" gefolgt von einem Leerzeichen und entweder die CA-Domain oder einen Strichpunkt ein (z.B. "issuewild ca.example.com" oder "issuewild ;"). Mit "iodef" gefolgt von einem Leerzeichen und einer URL können Sie sich Verstöße gegen die Policy melden lassen (z.B. "iodef mailto:hostmaster@example.com").

CNAME

Verknüpft einen Namen mit einem anderen Namen. Geben Sie in beide Felder einen relativen oder absoluten Namen ein.

MX

Gibt den Mail-Server für eine Domain an. Geben Sie in das erste Feld eine Mail-Domain (den Teil hinter dem @) in absoluter oder relativer Schreibweise ein. Im zweiten Feld muss der Hostname eines Mail-Server in absoluter oder relativer Schreibweise hinterlegt werden. Der MX-Zahlenwert gibt die Priorität an. Der MX-Eintrag mit der niedrigsten Priorität wird als erstes kontaktiert. Im Fehlerfall wird dann versucht, die Mail an die Server mit höheren Prioritätswerten zuzustellen. Sind für die selbe Domain mehrere MX-Einträge mit gleicher Priorität hinterlegt, so wird bei der Auflösung der DNS-Anfrage zufällig eine der Adressen ausgewählt. Ist unter dieser Adresse kein Mail-Server erreichbar, wird mit der nächsten Adresse fortgefahren.

NS

Gibt den Namens-Server für eine Domain an. Geben Sie in das erste Feld eine Domain in absoluter oder relativer Schreibweise ein. Im zweiten Feld muss der Hostname eines Namens-Servers in absoluter oder relativer Schreibweise hinterlegt werden. Sind für eine Domain mehrere NS-Einträge hinterlegt, wählt der Client zufällig einen davon aus. Ist dieser Namens-Server nicht erreichbar, wird mit der nächsten Adresse fortgefahren.

SRV

Spezifiziert den Server für einen bestimmten Dienst. Der Eintrag muss mit "_Dienstname._Protokoll" beginnen (z.B. "_sip._udp"). Als Wert geben Sie bitte den zugehörigen UDP- bzw. TCP-Port, ein Leerzeichen und dann den Servernamen an (z.B. "5060 www.example.com.).

TXT

Erlaubt die Angabe eines beliebigen Textes.

Über die "TTL" können Sie festlegen, wie lange der Eintrag maximal in Caches zwischengespeichert werden darf. Ist kein Wert angegeben, gilt der Standardwert, der auf dem Reiter (Tab) "SOA" konfiguriert wird.

14.4.2.1-B SOA

Zu jeder Zone muss ein Start-Of-Authority Eintrag hinterlegt werden. Dieser enthält Verwaltungsinformationen, von denen einige hier konfiguriert werden können.

Start-of-Authority Servername

Mit Hilfe diesen Wertes konfigurieren Sie den Namen des primären DNS für die ausgewählte Zone. Üblicherweise wird eine DNS-Zone auf sekundäre Server gespiegelt. Der hier konfigurierte Wert bleibt dabei unverändert, so dass ersichtlich wird, welcher der Namens-Server primär für die Einträge verantwortlich ist.

Start-of-Authority E-Mail

Hier wird die E-Mail-Adresse des administrativen Ansprechpartners für die gewählte Zone festgelegt.

Aufsteigende Versionsnummer (serial)

Jede DNS-Zone verfügt über eine fortlaufende Versionsnummer. Sekundäre DNS-Server entscheiden anhand dieser Nummer, ob die Einträge aktualisiert wurden und damit ein Zonentransfer notwendig ist. Die Versionsnummer wird vom SX-GATE automatisch nach jeder Änderung erhöht. Mit Hilfe des Eingabefeldes ist es jedoch möglich, den Wert selbst vorzugeben.



Steht die Versionsnummer auf einem kleineren Wert als bei den Kopien auf den sekundären Servern, kann dies zu Inkonsistenzen führen. Prüfen Sie die Versionsnummer insbesondere nach dem Einspielen eines Backups.

Standard TTL

Legen Sie hier fest, wie lange Einträge dieser Zone in Caches zwischengespeichert werden dürfen.

14.4.2.1-C NS

Geben Sie hier alle für die gewählte Zone zuständigen primären und sekundären Namens-Server an. Damit werden entsprechende NS-Einträge in der Zone generiert. Die Namen der DNS-Server können dabei entweder relativ zur aktuellen Zone (z.B. "ns") oder absolut angegeben werden. Bei der absoluten Adressierung ist der Namen mit einem Punkt abzuschließen (z.B. "ns.example.com.").

14.4.2.1-D MX

Hier konfigurieren Sie die Mail-Server (Mail-Exchanger) für die zur gewählten Zone gehörende E-Mail-Domain. Damit werden entsprechende MX-Einträge in der Zone generiert. Die Namen der Mail-Server können dabei entweder relativ zur aktuellen Zone (z.B. mail) oder absolut angegeben werden. Bei der absoluten Adressierung ist der Namen mit einem Punkt abzuschließen (z.B. mail.example.com.).

Der Zahlenwert gibt die Priorität an. Der MX-Eintrag mit der niedrigsten Priorität wird als erstes kontaktiert. Im Fehlerfall wird dann versucht, die Mail an die Server mit höheren Prioritätswerten zuzustellen.

14.4.2.1-E Zugriffsberechtigungen

Master

Diese Einstellung ist nur verfügbar, wenn SX-GATE als sekundärer Server (slave) für diese Zone konfiguriert ist. Geben Sie hier an, von welchem Namens-Server die Zonendatei gespiegelt werden soll.

Öffentliche Zone

DNS-Anfragen an diese Zone werden stets beantwortet, wenn die Anfrage von einer internen Adresse kommt. Um welche Adressen es sich dabei handelt ist unter "Module > DNS > Einstellungen" auf dem Tab "Client-Zugriff" definiert. Sollen die Informationen aus dieser Zone beliebigen IP-Adressen zur Verfügung stehen, so muss die Zone mit Hilfe dieses Schalters als "öffentlich" markiert werden.



Um DNS-Anfragen aus dem Internet an den Namens-Server des SX-GATE zu ermöglichen, sind in der Firewall-Konfiguration in der Regel eingehende Verbindungen zu Port 53 für die Protokolle UDP und TCP freizugeben.

Zonentransfers erlauben von folgenden IP-Adressen aus

Soll diese Zone auf sekundären Namens-Servern gespiegelt werden, so müssen Sie hier deren IP-Adressen hinterlegen. Ein Zonentransfer wird nur den hier angegebenen Adressen gestattet.

14.4.2.1-F Weiterleitung

Anfragen weiterleiten an Name-Server

Geben Sie hier die Name-Server an, an die Anfragen für die aktuelle Zone weitergeleitet werden sollen. Der übliche Weg der Namensauflösung über den DNS des Providers oder die Internet-Root-Server lässt sich auf diese Weise für einzelne Domains außer Kraft setzen.



Anfragen an diese Zone werden nur beantwortet, wenn der Client berechtigt ist, rekursive DNS-Anfragen zu stellen. Konfiguriert wird dies unter "Module > DNS > Einstellungen" auf dem Reiter (Tab) "Client-Zugriff".

Neben der Eingabe von IP-Adressen können Sie auch auf DNS IP-Objekte verweisen.

14.4.2.2 IPv4-Adressbereich (Reverse lookup)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.4.2.2-A Einträge.....	476
14.4.2.2-B SOA.....	477
14.4.2.2-C NS.....	478
14.4.2.2-D Zugriffberechtigungen.....	478
14.4.2.2-E Weiterleitung.....	479

Typ

Wählen Sie hier bitte aus, in welcher Funktion SX-GATE die DNS-Zone verwaltet.

Master

Die Einträge in der DNS-Zone müssen in dieser Einstellung auf SX-GATE vorgenommen werden. SX-GATE ist für deren Inhalt verantwortlich.

Slave

In dieser Einstellung spiegelt SX-GATE den Inhalt einer DNS-Zone, die auf einem anderen Namens-Server verwaltet wird. Der Inhalt selbst kann auf SX-GATE nicht verändert werden. Um den Zonen-Transfer durchführen zu können, muss die

Adresse des Master-Servers im Reiter (Tab) "Zugriffberechtigungen" eingetragen werden.

Weiterleitung

Anders als bei den vorigen Optionen, tritt SX-GATE hier nicht als Verwalter für die Zone auf sondern leitet Anfragen an einen anderen Name-Server weiter.

14.4.2.2-A Einträge

Benutzer Einträge

Hier können entsprechende Einträge in der Zone vorgenommen werden. Für NS-Einträge zur Zone selbst nutzen Sie bitte den entsprechenden eigenen Reiter (Tab).

Welche Werte für einen neuen Eintrag anzugeben sind, hängt vom gewählten Typ des Eintrags ab.

PTR

Bildet eine IP-Adresse auf einen Namen ab.

Geben Sie in das erste Feld die Zahlen ein, die relativ zum Zonennamen auf eine vollständige Adresse fehlen. Bei mehreren Zahlen müssen diese dabei in umgekehrter Reihenfolge spezifiziert werden. Um z.B. in der Zone "172.16" die Adresse "172.16.5.10" zu definieren, ist hier "10.5" einzugeben. Durch die relative Adressierung (kein Punkt hinter "10.5") wird der Eintrag automatisch zu einem vollständigen PTR-Eintrag ergänzt - in diesem Falle "10.5.16.172.in-addr.arpa.". Im zweiten Feld ist der entsprechende Hostname zu dieser Adresse anzugeben.

NS

Gibt den Namens-Server für eine Reverse-Lookup-Zone an.

Geben Sie im ersten Feld den IP-Bereich relativ zur aktuellen Zone an, für den Sie den Namens-Server festlegen wollen. Bei mehreren Zahlen müssen diese dabei in umgekehrter Reihenfolge spezifiziert werden. Um z.B. in der Zone "10" einen Namensserver für "10.16.5" zu definieren, geben Sie "5.16" ein. Tatsächlich wollen Sie ja "5.16.10.in-addr.arpa." definieren. Durch die relative Adressierung (kein Punkt hinter "5.16") wird der Eintrag automatisch um die aktuelle Zone zu "5.16.10.in-addr.arpa." ergänzt.

Im zweiten Feld muss der Hostname eines Namens-Servers hinterlegt werden. Sind für eine Domain mehrere NS-Einträge hinterlegt, wählt der Client zufällig einen davon aus. Ist dieser Namens-Server nicht erreichbar, wird mit der nächsten Adresse fortgefahren.

Über die "TTL" können Sie festlegen, wie lange der Eintrag maximal in Caches zwischengespeichert werden darf. Ist kein Wert angegeben, gilt der Standardwert, der auf dem Reiter (Tab) "SOA" konfiguriert wird.

Fehlende PTR-Einträge automatisch ergänzen

Alle Adressen, die nicht mit Hilfe von PTR-Einträgen manuell auf Namen abgebildet wurden, lassen sich mit Hilfe dieses Schalters automatisch zuweisen.



Diese Funktion steht für Zonen die ein Klasse A-Netzwerk beschreiben nicht zur Verfügung.

mit Hostname

Mit Hilfe dieser Einstellung wird der automatisch generierte Rechnername festgelegt. Dem hier angegebenen Wert wird bei einem Klasse C Netzwerk jeweils die letzte Stelle der IP-Adresse angehängt. Bei einem Klasse B Netzwerk wird darüber hinaus ein Bindestrich und die vorletzte Stelle der IP-Adresse hinzugefügt.

und Domain

Schließlich wird mit Hilfe dieses Eingabebereichs die Domain festgelegt, die an die automatisch generierten Hostnamen angehängt wird.

14.4.2.2-B SOA

Zu jeder Zone muss ein Start-Of-Authority Eintrag hinterlegt werden. Dieser enthält Verwaltungsinformationen, von denen einige hier konfiguriert werden können.

Start-of-Authority Servername

Mit Hilfe diesen Wertes konfigurieren Sie den Namen des primären DNS für die ausgewählte Zone. Üblicherweise wird eine DNS-Zone auf sekundäre Server gespiegelt. Der hier konfigurierte Wert bleibt dabei unverändert, so dass ersichtlich wird, welcher der Namens-Server primär für die Einträge verantwortlich ist.

Start-of-Authority E-Mail

Hier wird die E-Mail-Adresse des administrativen Ansprechpartners für die gewählte Zone festgelegt.

Aufsteigende Versionsnummer (serial)

Jede DNS-Zone verfügt über eine fortlaufende Versionsnummer. Sekundäre DNS-Server entscheiden anhand dieser Nummer, ob die Einträge aktualisiert wurden und damit ein Zonentransfer notwendig ist. Die Versionsnummer wird vom SX-GATE automatisch nach jeder Änderung erhöht. Mit Hilfe des Eingabefeldes ist es jedoch möglich, den Wert selbst vorzugeben.



Steht die Versionsnummer auf einem kleineren Wert als bei den Kopien auf den sekundären Servern, kann dies zu Inkonsistenzen führen. Prüfen Sie die Versionsnummer insbesondere nach dem Einspielen eines Backups.

Standard TTL

Legen Sie hier fest, wie lange Einträge dieser Zone in Caches zwischengespeichert werden dürfen.

14.4.2.2-C NS

Geben Sie hier alle für die gewählte Zone zuständigen primären und sekundären Namens-Server an. Damit werden entsprechende NS-Einträge in der Zone generiert. Verwenden Sie die absolute Adressierung mit schließendem Punkt (z.B. "ns.example.com.").

14.4.2.2-D Zugriffsberechtigungen**Master**

Diese Einstellung ist nur verfügbar, wenn SX-GATE als sekundärer Server (slave) für diese Zone konfiguriert ist. Geben Sie hier an, von welchem Namens-Server die Zonendatei gespiegelt werden soll.

Öffentliche Zone

DNS-Anfragen an diese Zone werden stets beantwortet, wenn die Anfrage von einer internen Adresse kommt. Um welche Adressen es sich dabei handelt ist unter "Module > DNS > Einstellungen" auf dem Tab "Client-Zugriff" definiert. Sollen die Informationen aus dieser Zone beliebigen IP-Adressen zur Verfügung stehen, so muss die Zone mit Hilfe dieses Schalters als "öffentlich" markiert werden.



Um DNS-Anfragen aus dem Internet an den Namens-Server des SX-GATE zu ermöglichen, sind in der Firewall-Konfiguration in der Regel eingehende Verbindungen zu Port 53 für die Protokolle UDP und TCP freizugeben.

Zonentransfers erlauben von folgenden IP-Adressen aus

Soll diese Zone auf sekundären Namens-Servern gespiegelt werden, so müssen Sie hier deren IP-Adressen hinterlegen. Ein Zonentransfer wird nur den hier angegebenen Adressen gestattet.

14.4.2.2-E Weiterleitung

Anfragen weiterleiten an Name-Server

Geben Sie hier die Name-Server an, an die Anfragen für die aktuelle Zone weitergeleitet werden sollen. Der übliche Weg der Namensauflösung über den DNS des Providers oder die Internet-Root-Server lässt sich auf diese Weise für einzelne Adressbereiche außer Kraft setzen.



Anfragen an diese Zone werden nur beantwortet, wenn der Client berechtigt ist, rekursive DNS-Anfragen zu stellen. Konfiguriert wird dies unter "Module > DNS > Einstellungen" auf dem Reiter (Tab) "Client-Zugriff".

Neben der Eingabe von IP-Adressen können Sie auch auf DNS IP-Objekte verweisen.

14.4.2.3 IPv6-Adressbereich (Reverse lookup)

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.4.2.3-A Einträge.....	480
14.4.2.3-B SOA.....	481
14.4.2.3-C NS.....	481
14.4.2.3-D Zugriffberechtigungen.....	482
14.4.2.3-E Weiterleitung.....	482

Typ

Wählen Sie hier bitte aus, in welcher Funktion SX-GATE die DNS-Zone verwaltet.

Master

Die Einträge in der DNS-Zone müssen in dieser Einstellung auf SX-GATE vorgenommen werden. SX-GATE ist für deren Inhalt verantwortlich.

Slave

In dieser Einstellung spiegelt SX-GATE den Inhalt einer DNS-Zone, die auf einem anderen Namens-Server verwaltet wird. Der Inhalt selbst kann auf SX-GATE nicht verändert werden. Um den Zonen-Transfer durchführen zu können, muss die

Adresse des Master-Servers im Reiter (Tab) "Zugriffsberechtigungen" eingetragen werden.

Weiterleitung

Anders als bei den vorigen Optionen, tritt SX-GATE hier nicht als Verwalter für die Zone auf sondern leitet Anfragen an einen anderen Name-Server weiter.

14.4.2.3-A Einträge

Benutzer Einträge

Hier können entsprechende Einträge in der Zone vorgenommen werden. Für NS-Einträge zur Zone selbst nutzen Sie bitte den entsprechenden eigenen Reiter (Tab).

Welche Werte für einen neuen Eintrag anzugeben sind, hängt vom gewählten Typ des Eintrags ab.

PTR

Bildet eine IP-Adresse auf einen Namen ab.

Geben Sie in das erste Feld die Zahlen ein, die relativ zum Zonennamen auf eine vollständige Adresse fehlen. Dabei können Sie zwischen der normalen Schreibweise für IPv6-Adressen wählen oder aber den originalen Syntax des PTR-Records benutzen (umgekehrte Reihenfolge der Ziffern mit Punkten getrennt). Um beispielsweise in der Zone 2001:db8:0:0: die Adresse 2001:db8::1 zu definieren, wären folgende Angaben möglich: ":1", "0:0:0:1" oder "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0".

Im zweiten Feld ist der entsprechende Hostname zu dieser Adresse anzugeben.

NS

Gibt den Namens-Server für eine Reverse-Lookup-Zone an.

Geben Sie im ersten Feld den IP-Bereich relativ zur aktuellen Zone an, für den Sie den Namens-Server festlegen wollen. Bei mehreren Zahlen müssen diese dabei in umgekehrter Reihenfolge und mit Punkten getrennt spezifiziert werden. Um z.B. in der Zone 2001:db8:0: einen Namensserver für 2001:db8:0:1::/64 zu delegieren, geben Sie "1.0.0.0" ein. Tatsächlich wollen Sie ja "1.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa." definieren. Durch die relative Adressierung (kein Punkt hinter "1.0.0.0") wird der Eintrag automatisch um die aktuelle Zone (0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.) ergänzt.

Im zweiten Feld muss der Hostname eines Namens-Servers hinterlegt werden. Sind für eine Domain mehrere NS-Einträge hinterlegt, wählt der Client zufällig einen davon aus. Ist dieser Namens-Server nicht erreichbar, wird mit der nächsten Adresse fortgefahren.

Über die "TTL" können Sie festlegen, wie lange der Eintrag maximal in Caches zwischengespeichert werden darf. Ist kein Wert angegeben, gilt der Standardwert, der auf dem Reiter (Tab) "SOA" konfiguriert wird.

14.4.2.3-B SOA

Zu jeder Zone muss ein Start-Of-Authority Eintrag hinterlegt werden. Dieser enthält Verwaltungsinformationen, von denen einige hier konfiguriert werden können.

Start-of-Authority Servername

Mit Hilfe diesen Wertes konfigurieren Sie den Namen des primären DNS für die ausgewählte Zone. Üblicherweise wird eine DNS-Zone auf sekundäre Server gespiegelt. Der hier konfigurierte Wert bleibt dabei unverändert, so dass ersichtlich wird, welcher der Namens-Server primär für die Einträge verantwortlich ist.

Start-of-Authority E-Mail

Hier wird die E-Mail-Adresse des administrativen Ansprechpartners für die gewählte Zone festgelegt.

Aufsteigende Versionsnummer (serial)

Jede DNS-Zone verfügt über eine fortlaufende Versionsnummer. Sekundäre DNS-Server entscheiden anhand dieser Nummer, ob die Einträge aktualisiert wurden und damit ein Zonentransfer notwendig ist. Die Versionsnummer wird vom SX-GATE automatisch nach jeder Änderung erhöht. Mit Hilfe des Eingabefeldes ist es jedoch möglich, den Wert selbst vorzugeben.



Steht die Versionsnummer auf einem kleineren Wert als bei den Kopien auf den sekundären Servern, kann dies zu Inkonsistenzen führen. Prüfen Sie die Versionsnummer insbesondere nach dem Einspielen eines Backups.

Standard TTL

Legen Sie hier fest, wie lange Einträge dieser Zone in Caches zwischengespeichert werden dürfen.

14.4.2.3-C NS

Geben Sie hier alle für die gewählte Zone zuständigen primären und sekundären Namens-Server an. Damit werden entsprechende NS-Einträge in der Zone generiert. Verwenden Sie die absolute Adressierung mit schließendem Punkt (z.B. "ns.example.com.").

14.4.2.3-D Zugriffsberechtigungen

Master

Diese Einstellung ist nur verfügbar, wenn SX-GATE als sekundärer Server (slave) für diese Zone konfiguriert ist. Geben Sie hier an, von welchem Namens-Server die Zonendatei gespiegelt werden soll.

Öffentliche Zone

DNS-Anfragen an diese Zone werden stets beantwortet, wenn die Anfrage von einer internen Adresse kommt. Um welche Adressen es sich dabei handelt ist unter "Module > DNS > Einstellungen" auf dem Tab "Client-Zugriff" definiert. Sollen die Informationen aus dieser Zone beliebigen IP-Adressen zur Verfügung stehen, so muss die Zone mit Hilfe dieses Schalters als "öffentlich" markiert werden.



Um DNS-Anfragen aus dem Internet an den Namens-Server des SX-GATE zu ermöglichen, sind in der Firewall-Konfiguration in der Regel eingehende Verbindungen zu Port 53 für die Protokolle UDP und TCP freizugeben.

Zonentransfers erlauben von folgenden IP-Adressen aus

Soll diese Zone auf sekundären Namens-Servern gespiegelt werden, so müssen Sie hier deren IP-Adressen hinterlegen. Ein Zonentransfer wird nur den hier angegebenen Adressen gestattet.

14.4.2.3-E Weiterleitung

Anfragen weiterleiten an Name-Server

Geben Sie hier die Name-Server an, an die Anfragen für die aktuelle Zone weitergeleitet werden sollen. Der übliche Weg der Namensauflösung über den DNS des Providers oder die Internet-Root-Server lässt sich auf diese Weise für einzelne Adressbereiche außer Kraft setzen.



Anfragen an diese Zone werden nur beantwortet, wenn der Client berechtigt ist, rekursive DNS-Anfragen zu stellen. Konfiguriert wird dies unter "Module > DNS > Einstellungen" auf dem Reiter (Tab) "Client-Zugriff".

Neben der Eingabe von IP-Adressen können Sie auch auf DNS IP-Objekte verweisen.

14.5 Mail-Server

14.5.1 POP-/IMAP-Server

SX-GATE stellt für jeden Benutzer, der Mitglied der Gruppe "system-mail" ist, ein Postfach bereit. Damit E-Mails in ein E-Mail-Konto zugestellt werden, muss mindestens eine Mail-Domain mit "Zustellung an SX-GATE Postfach" konfiguriert sein.

Dieser Dienst ermöglicht den Zugriff auf SX-GATE E-Mail-Konten mit Hilfe der Protokolle POP3 und IMAP4. Während mit POP3 lediglich der Zugriff auf den Posteingang möglich ist, erlaubt IMAP4 eine serverseitige Mail-Verwaltung mit Ordnerstrukturen.



Der Zugriff auf Postfächer ist auch mittels Web-Browser über die SX-GATE-Groupware möglich, sofern diese installiert ist.

POP3 (Port 110)

Der Zugriff auf den Posteingang ist hier zunächst unverschlüsselt. Sofern der Mail-Client die entsprechenden Protokollerweiterungen unterstützt, kann jedoch eine verschlüsselte Verbindung ausgehandelt werden.

POP3 verschlüsselt (Port 995)

Mit Hilfe dieses Dienstes erfolgt der Zugriff auf den Posteingang von Anfang an verschlüsselt.

IMAP4 (Port 143)

Die Verbindung zu diesem Server-Dienst ist zunächst unverschlüsselt. Sofern der Mail-Client die entsprechenden Protokollerweiterungen unterstützt, kann jedoch eine verschlüsselte Verbindung ausgehandelt werden.

IMAP4 verschlüsselt (Port 993)

Hier erfolgt der Zugriff von Anfang an verschlüsselt.

Verschlüsselung erzwingen

Aktivieren Sie diese Option um bei Verbindungen zu den zunächst unverschlüsselten Ports 110 und 143 den Wechsel auf eine verschlüsselte Verbindung zu erzwingen. Clients, die nicht auf eine verschlüsselte Verbindung wechseln wollen oder können, werden abgewiesen.

TLS-Protokoll

Wählen Sie hier die Verschlüsselungsstärke aus.



Im Rahmen der Produktpflege werden die mit der jeweiligen Auswahl verbundenen Parameter von Zeit zu Zeit angepasst.

veraltet

Um Kompatibilität mit älteren Clients zu gewährleisten, werden in dieser Einstellung AES-Algorithmen mit dem nicht mehr empfohlenen Cipher-Block-Chaining CBC und dem veraltete Hash-Algorithmus SHA1 aktiviert. Die minimale TLS-Version ist 1.0.

kompatibel

Wählen Sie diese Einstellung für weitreichende Kompatibilität mit älteren Client-Systemen. Der veraltete Hash-Algorithmus SHA1 ist dabei aktiviert. Die minimale TLS-Version ist 1.2.

aktuell

In dieser Einstellung werden nur noch halbwegs aktuelle Client-Systeme unterstützt. Es wird mindestens TLS 1.2 vorausgesetzt. Wählen Sie diese Option für hohe Sicherheit.

maximal

Erfordert TLS 1.3. Bevor Sie sich für diese Einstellung entscheiden, sollten Sie prüfen, ob alle Clients TLS 1.3 unterstützen.

Postfächer täglich erneut auf Viren scannen

Lokale E-Mail-Postfächer können regelmäßig auf Viren geprüft werden. Dadurch können Viren gefunden werden, die mit den Antivirus-Signaturen beim Eintreffen der Mail nicht erkannt wurden.



Damit diese Funktion wirksam ist, muss ein funktionsfähiger Virens Scanner auf SX-GATE installiert sein. Die Lizenzen für den Virens Scanner sind nicht im SX-GATE enthalten und müssen separat erworben werden. Nähere Informationen zu unterstützten oder bereits installierten Virens Scannern finden Sie im Menü "Module > Virens Scanner". Dort ist auch die Installation von Virens Scannern vorzunehmen.

14.5.2 SMTP Einstellungen

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.5.2-A Provider-Relay.....	485
14.5.2-B Versand-Parameter.....	489
14.5.2-C PGP / SMIME.....	491
14.5.2-D Relay Kontrolle.....	492
14.5.2-E Empfangs-Filter.....	494
14.5.2-F Limits.....	498
14.5.2-G Archivierung / Milter.....	499

14.5.2-A Provider-Relay

SMTP-Relay-Server des Providers

Mit Hilfe dieser Einstellung legen Sie fest, wie ausgehende E-Mails versendet werden sollen. SX-GATE kann Mails direkt an den Mail-Server des Empfängers weiterleiten. Welcher Mail-Server dies ist, wird über DNS ermittelt. Geben Sie hier einen Relay-Server (Smarthost) ein, so werden ausgehende Mails grundsätzlich an diesen weitergeleitet. Der Relay-Server ist dann für den weiteren Versand zum Empfänger verantwortlich.



Diese Einstellung hat keinerlei Auswirkung auf E-Mails an Empfänger-Domains, die SX-GATE an lokale Postfächer oder spezifische (interne) Mail-Server ausliefert.

Die Nutzung eines Relay-Servers empfiehlt sich insbesondere bei der Internet-Anbindung über Wählleitungen. Ist der Ziel-Server schlecht erreichbar, ist so der Relay-Server für wiederholte Zustellversuche zuständig. Die Wählleitung wird dadurch nicht unnötig belastet. Bei Wählleitungen mit dynamischer IP-Adresse kann hinzukommen, dass manche Mail-Server E-Mails von diesen Adressen nicht annehmen.

Relay-Server Port

Sofern der Relay-Server keine Verbindungen auf dem Standard-Port 25 entgegennimmt, können Sie hier die abweichende Portnummer eintragen (üblicherweise 465 oder 587).

Protokoll

Eine Auswahl ist hier nur erforderlich, wenn der Relay-Server per SMTPS angesprochen werden muss und dabei nicht den Standard-Port 465 nutzt.

Authentifizierungsmethode

Die Übermittlung der SMTP-Auth Zugangsdaten kann mit Hilfe verschiedener Verfahren erfolgen. Mit Hilfe dieses Schalters kann ein bestimmtes erzwungen werden. Darf SX-GATE das Verfahren selbst bestimmen, so werden die MD5 basierenden Algorithmen bevorzugt, da hier das Kennwort nicht im Klartext übermittelt wird.



Nicht jeder Relay-Server unterstützt alle Methoden. Wird ein Verfahren zwingend vorgeschrieben, das der Server nicht anbietet, so erfolgt keine Authentifizierung. Möglicherweise verweigert der Relay-Server dann die Annahme der E-Mail.

Microsoft 365 OAUTH2

Für den Versand von Mails über ein "Microsoft 365"-Konto mit dem OAuth2-Verfahren nutzt SX-GATE den "Client-Credentials Flow". In "Entra ID" (ehemals Azure Active-Directory) wird dazu für den SX-GATE Mail-Server eine Anwendung mit zugehörigem Anwendungskennwort angelegt. Die Anwendung erhält die Berechtigung für den SMTP-Versand. SX-GATE nutzt ausschließlich ein Benutzerkonto für den Mail-Versand. Diesem Konto muss die Sendeberechtigung für alle Absenderadressen erteilt werden. Nun kann der SX-GATE mit seiner Anwendungs-ID und dem Anwendungskennwort einen kurzlebigen Zugriffstoken abrufen und mit diesem die Mails über das angegebene Benutzerkonto versenden.

Die Schritte im Einzelnen:

Anwendung anlegen

Melden Sie sich bei Microsoft Azure mit einem Administratorenkonto an (<https://portal.azure.com>).

Wählen Sie "Microsoft Entra ID", dann "Verwalten > App-Registrierungen". Klicken Sie auf "Neue Registrierung" und vergeben Sie einen beliebigen Namen. Lassen Sie die weiteren Einstellungen unverändert und legen Sie die Anwendung mit "Registrieren" an.

Jetzt links im Menü "Zertifikate & Geheimnisse" anklicken. Unter "Geheime Clientschlüssel" generieren Sie mit "Neuer geheimer Clientschlüssel" ein Anwendungskennwort, das Sie mit "Hinzufügen" abspeichern.

Kopieren Sie nun sofort das Kennwort in der Spalte "Wert" durch Klick auf das Kopiersymbol hinter dem Kennwort. Zu einem späteren Zeitpunkt ist dies nicht mehr möglich. Übertragen Sie das Kennwort in die OAuth2-Konfiguration des SX-GATE Mail-Servers bzw. speichern Sie es an einem sicheren Ort zwischen, um es später im SX-GATE zu konfigurieren.

Klicken Sie nun im Menü links auf "Verwalten > API-Berechtigungen", dann "Berechtigung hinzufügen". Wählen Sie "Von meiner Organisation verwendete APIs" und geben Sie im Suchfeld "Office" ein. Wählen Sie "Office 365 Exchange Online" aus. Klicken Sie auf "Anwendungsberechtigungen". Öffnen Sie die Rubrik "SMTP" und selektieren Sie die "SMTP.SendAsApp"-Berechtigung. Schließen Sie das Fenster mit "Berechtigungen hinzufügen". Klicken Sie abschließend auf "Administratorzustimmung für DOMAINNAME erteilen".

Klicken Sie im linken Menü auf "Übersicht" und übertragen Sie die "Anwendungs-ID (Client)" und die "Verzeichnis-ID (Mandant)" in die OAuth2-Konfiguration des SX-GATE Mail-Servers bzw. speichern Sie die Werte zwischen, um sie später im SX-GATE zu konfigurieren.

Verlassen Sie nun die Anwendungs-Registrierung, indem Sie oben links auf "Home" klicken.

Öffnen Sie erneut "Microsoft Entra ID" und wählen Sie diesmal "Verwalten > Unternehmensanwendungen". Kopieren Sie sich für später die "Objekt-ID" der zuvor angelegten Anwendung. Hier wird auch nochmal die "Anwendungs-ID" angezeigt. Sie benötigen beide Werte gleich für die Exchange-Konfiguration.

Zugriffsrechte im Exchange erteilen

SX-GATE nutzt für den Mailversand lediglich ein Benutzerkonto. Entscheiden Sie sich für ein Konto und prüfen Sie dann im "Microsoft 365 admin center" (<https://admin.microsoft.com>), ob für dieses Konto "Authentifiziertes SMTP" erlaubt ist. Wählen Sie dazu unter "Benutzer > Aktive Benutzer" das Konto aus. Nach Klick auf "E-Mail" werden Ihnen unter "E-Mail Apps" die Berechtigungen angezeigt.

Gehen Sie nun alle anderen Benutzer und Gruppen durch und erteilen Sie "Senden als"-Berechtigung für das zum Versand genutzte Konto.

Zugangsdaten im SX-GATE hinterlegen

Sofern noch nicht geschehen, tragen Sie die zuvor kopierten Werte in die OAuth2-Konfiguration des SX-GATE Mail-Clients ein.

Tragen Sie das für den Versand zu verwendende Benutzerkonto bei "SMTP-Auth Benutzername" ein. Die Angabe des zugehörigen Benutzerpassworts ist nicht erforderlich, da sich SX-GATE mit seinem Anwendungskennwort anmelden kann.

SMTP-Auth Benutzername

Sollte für die Nutzung des Relay-Servers Ihres Providers eine Benutzeranmeldung mit SMTP AUTH erforderlich sein, so tragen Sie hier bitte den Benutzernamen ein. Ist dieses Felder leer, wird auch keine Benutzeranmeldung vorgenommen.



Die Benutzeranmeldung am Relay-Server Ihres Providers bezieht sich auf ausgehende Mails und hat nichts mit der Benutzeranmeldung zu tun, die Sie für die Abholung von Mails vom POP3-Server Ihres Providers benötigen. Sollten Sie wirklich eine Benutzeranmeldung für ausgehende Mails benötigen, so können diese Zugangsdaten aber durchaus mit denen des POP3-Servers identisch sein.



SMTP-Auth ist gemäß Standard eine "Hop-to-Hop"-Authentifizierung. Dies bedeutet, dass die Anmeldung nur die beiden unmittelbar miteinander kommunizierenden Systeme betrifft. In diesem Falle muss sich also der SX-GATE Mail-Server gegenüber dem Relay-Server authentifizieren und nicht in etwa z.B. der Benutzer, der die Mail geschrieben hat. SX-GATE meldet sich daher normalerweise nur mit einem bestimmten Login an. Eine unterschiedliche Anmeldung in Abhängigkeit vom Absender der E-Mail ist zwar möglich, aber eventuell mit Einschränkungen verbunden (siehe "Authentifizierung abhängig von Absender-Adresse" weiter unten).

In der Regel verlangt ein Relay-Server nur dann nach einer Benutzeranmeldung, wenn der Internetzugang über einen anderen Provider erfolgt.



Es empfiehlt sich stets den Mail-Relay-Server des Providers zu verwenden, über den auch der Internet-Zugang erfolgt. So ist normalerweise keine Benutzeranmeldung erforderlich. Zudem ist die Übermittlung der E-Mails an den Relay-Server nicht von Engpässen im Internet betroffen und erfolgt daher im Allgemeinen mit höherer Bandbreite.

Mandant (Tenant)

Tragen Sie hier den Namen oder die ID Ihres "Entra ID"-Mandanten ein.

OAuth2 Anwendungs-ID

Geben Sie hier die Anwendungs-ID (Client-ID) ein, die Sie in "Entra ID" für den SX-GATE Mail-Server registriert haben.

Geheimer OAuth2-Clientschlüssel

Geben Sie hier das Anwendungskennwort ein, das Sie im Azure Active-Directory für den SX-GATE Mail-Server generiert haben.



Das Anwendungskennwort ist im Azure AD mit einer begrenzten Gültigkeitsdauer versehen. Bitte denken Sie stets daran, rechtzeitig ein neues Anwendungskennwort im Azure AD festzulegen und in den SX-GATE zu übertragen.

Authentifizierung mit Zertifikat

Alternativ oder zusätzlich zur Passwort-Authentifizierung kann sich SX-GATE auch mit einem Client-Zertifikat gegenüber anderen Mail-Servern ausweisen, sofern die Verbindung verschlüsselt ist.

Wählen Sie hier einen der Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.

Authentifizierung abhängig von Absender-Adresse

Sofern der Provider verlangt, dass beim Mailversand die zur Absender-Adresse passenden Zugangsdaten verwendet werden müssen, können Sie hier je Absender-Adresse den zugehörigen Benutzernamen und das Passwort hinterlegen. Als Absender gilt der sog. "Envelope-From", also der Absender wie er auch im Maillog des SX-GATEs angezeigt wird.



In bestimmten Situationen (z.B. unzustellbare Mail) oder von bestimmten Funktionen (z.B. Abwesenheitsbenachrichtigung) werden Mails mit leerem Absender verschickt (der sog. SMTP null reverse-path). Möglicherweise nimmt der Provider solche Mails nicht an, so dass diese verworfen werden oder eine Benachrichtigung an den lokalen Administrator auslösen. Stellen in so einem Fall um auf direkten Mailversand oder wechseln Sie zu einem Provider, der ein vollwertiges SMTP-Relay zur Verfügung stellt.

14.5.2-B Versand-Parameter

Versand ausgehender E-Mails

Ausgehende E-Mails können sofort weitergeleitet oder aber gesammelt und zu einem späteren Zeitpunkt gebündelt versendet werden. In diesem Falle werden die Mails in eine Warteschlange eingereiht und erst dann versendet, wenn diese das nächste Mal abgearbeitet wird. Dies ist insbesondere bei der Anbindung an das Internet über eine Wählleitung interessant um Verbindungskosten zu sparen.

Warteschlange abarbeiten alle

Mit Hilfe dieser und der folgenden Einstellung steuern Sie, wann E-Mails, die sich in der Sende-Warteschlange des SX-GATE Mail-Servers befinden, ausgeliefert werden sollen. Eine E-Mail wartet in der Sende-Warteschlange wenn der vorhergehende Versuch die Mail zuzustellen fehlgeschlagen ist oder wenn ausgehende Mails grundsätzlich zunächst in die Warteschlange eingereiht werden.



Mindestens eine der beiden Optionen muss aktiviert und funktionsfähig sein. Ansonsten bleiben E-Mails für immer in der Warteschlange liegen.

Die Sende-Warteschlange wird vom Mail-Server im hier angegebenen Zeitabstand abgearbeitet. Dieser Wert gibt somit die minimale Zeitdauer an, die eine E-Mail bis zum nächsten Zustellversuch in der Warteschlange verbringt.

Warteschlange bei Internet-Einwahl abarbeiten

Aktivieren Sie diese Option, wenn SX-GATE mit einer direkt angeschlossenen ADSL-Wählleitung an das Internet angebunden ist. Bei jedem Verbindungsaufbau dieser Wählleitung wird versucht, die E-Mails aus der Sende-Warteschlange zu übermitteln.



Ist SX-GATE nicht über eine entsprechende PPP Wählverbindung direkt am Internet angeschlossen, so ist diese Einstellung wirkungslos.

Warnmeldung an Absender, wenn die Mail nicht ausgeliefert wurde nach

Wenn bei der Abarbeitung der Sende-Warteschlange eine E-Mail nicht zugestellt werden kann, diese sich aber bereits mindestens die hier angegebene Zeitspanne in der Warteschlange befindet, so wird der Absender darüber informiert. Pro E-Mail erfolgt nur einmal eine solche Benachrichtigung.



Eine Benachrichtigung erfolgt grundsätzlich nur beim Abarbeiten der Sende-Warteschlange. Die tatsächliche Zeitdauer bis zur Benachrichtigung kann daher länger sein als die hier eingestellte Zeit. Stimmen Sie diesen Parameter mit dem Zeitintervall ab, in dem die Warteschlange abgearbeitet wird.

Mail als unzustellbar zurück wenn nicht ausgeliefert nach

Diese Option ist ähnlich der vorhergehenden. Hier wird eine wartende Mail jedoch als unzustellbar an den Absender zurück geschickt, wenn diese nach Überschreiten dieser

Zeitspanne noch immer nicht zugestellt werden kann. Eine Überprüfung der Zeitspanne findet auch hier nur beim Abarbeiten der Warteschlange statt.



Auch hier kann die tatsächliche Dauer bis zur Unzustellbarkeitsmeldung vom eingestellten Wert abweichen. Beachten Sie bitte die Hinweise zur vorigen Option.

HELO/EHLO-Name

Stellen Sie hier ein, welchen Namen SX-GATE beim Versand von E-Mails im HELO/EHLO-Befehl verwenden soll. Neben der Möglichkeit einen festen Namen einzustellen, kann SX-GATE diesen auch dynamisch ermitteln. Dies geschieht mit Hilfe eines DNS Reverse-Lookups zur Quell-IP der ausgehenden Verbindung.



Bei Verbindungen über die eth0-Schnittstelle wird bei dynamisch ermitteltem Namen stets SX-GATEs Hostname gemäß System > Grundeinstellungen verwendet.

Absender für SX-GATE E-Mails

SX-GATE generiert selbst E-Mails wie z.B. Status- oder Warnmeldungen. Mit Hilfe dieses Eingabebereichs stellen Sie die dabei von SX-GATE verwendeten Absender ein. Sie können eine vollständige E-Mail-Adresse eintragen oder nur eine Domain. Wenn Sie eine Domain eintragen, bleibt der Teil vor dem @-Zeichen unverändert (meist "root").

14.5.2-C PGP / SMIME

Der PGP/SMIME-Filter verhindert, dass versehentlich unverschlüsselte Mails an Adressaten versendet werden, mit denen nur verschlüsselt kommuniziert werden soll. Akzeptiert werden Mails die der Mail-Client mit PGP (GPG) oder S/MIME zumindest teilverschlüsselt hat. Andernfalls wird die Annahme verweigert. Ausgenommen von der Überprüfung sind E-Mails mit leerem Absender, wie sie häufig bei z.B. Unzustellbarkeits-Benachrichtigungen, Empfangsbestätigungen oder Abwesenheits-Nachrichten vorkommen.



Es werden ausschließlich ausgehende Mails überprüft.

PGP / SMIME Filter

Dieser Schalter aktiviert oder deaktiviert den Filter.

Unverschlüsselte Mails an folgende Mail-Adressen und -Domains unterbinden

Geben Sie hier die Empfänger an, die ausschließlich verschlüsselte E-Mails erhalten sollen. Neben einzelnen Mail-Adresse können auch ganze Mail-Domains angegeben werden (z.B. "benutzer@example.com" oder "example.com").

14.5.2-D Relay Kontrolle

Es ist stets sicherzustellen, dass nur interne IP-Adressen ohne weiteres Mails in das Internet versenden dürfen. Andernfalls ist damit zu rechnen, dass der Mail-Server in kürzester Zeit als sogenannter "offener Relay-Server" für den Versand von SPAM-Mails missbraucht wird.



Grundsätzlich ist es unabhängig von der Quell-IP-Adresse immer möglich, E-Mails an Empfänger innerhalb der lokalen Empfänger-Domains zu senden. Dies umfasst gleichermaßen Domains die in ein SX-GATE Postfach zugestellt werden und Domains die an einen speziellen (internen) Mail-Server weitergeleitet werden. Auch Authentifizierung ist in diesem Falle nie erforderlich.

Lokale IP-Adressen

In diesem Bereich lässt sich festlegen, welche IP-Adressen als "lokal" angesehen werden. Sofern nicht durch andere Optionen eingeschränkt, dürfen ausschließlich die hier angegebenen IP-Adressen E-Mails ohne weiteres in das Internet zu versenden.



Sie sollten hier niemals den Zugriff für beliebige Adressen freigeben.



Die SX-GATE Groupware verfügt, sofern sie installiert ist, über eine eigene IP-Adresse, die automatisch immer als "lokal" betrachtet wird, auch wenn Sie nicht in dieser Liste aufgeführt ist.

Mit Hilfe dieser Einstellung ist es auch möglich, nur bestimmten Systemen im LAN den Mail-Versand in das Internet zu erlauben, während alle anderen nur interne Mails versenden dürfen. Das entscheidende Kriterium ist dabei die IP-Adresse von der der SX-GATE die E-Mail empfängt. Über die nachfolgenden Optionen lässt sich der E-Mail-Versand in das Internet auch benutzerbezogen einschränken.

SMTP-Auth erforderlich für lokale Benutzer

Ist dieser Schalter aktiviert, so leitet SX-GATE E-Mails von internen Adressen nicht in das Internet weiter, wenn keine Authentifizierung erfolgte. Als interne Adressen gelten dabei die oben unter "Lokale IP-Adressen" angegebenen Adressen.



Der Schalter aktiviert zugleich SMTP-Authentifizierung in der SX-GATE Groupware, sofern diese aktiviert ist.

Nutzen Sie diese Einstellung, um den Mail-Versand in das Internet nur bestimmten lokalen Benutzern zu erlauben. Die SMTP-Auth Berechtigung kann Benutzergruppen unter "System > Benutzerverwaltung > Gruppen" erteilt werden.

SMTP-Auth immer anbieten

Wenn diese Option aktiviert ist, wird sowohl internen als auch externen Clients die Möglichkeit angeboten, sich zu authentifizieren. Externen IP-Adressen ist es normalerweise nicht gestattet, über SX-GATE E-Mails in das Internet zu versenden. Mit Hilfe dieses Schalters kann dies bestimmten Benutzern nach Authentifizierung erlaubt werden. Welche Benutzer dazu berechtigt sind wird, wie bei der vorherigen Option beschrieben, über die Benutzergruppen festgelegt. Interne Adressen müssen sich ggf. authentifizieren wenn ausgehende Mails durch das Modul "S/MIME-Gateway" signiert werden sollen.

Client-Systeme sollten E-Mails über die Submission-Ports 465 oder 587 an den Mail-Server übermitteln. Dann ist es ausreichend, wenn Authentifizierung ausschließlich an den Submission-Ports möglich ist. Sind diese Ports aus dem Internet gar nicht erreichbar, erhöht das zudem die Sicherheit, da Zugangsdaten nicht durch Probieren ermittelt werden können.

nur auf Submission-Ports

Aktivieren Sie diese Option, wenn Authentifizierung nur über die Submission-Ports 465 und 587 möglich sein soll.

auch auf Port 25

Aktivieren Sie diese Option, wenn Authentifizierung auch über Port 25 möglich sein soll.

Nur verschlüsselte Benutzeranmeldung zulassen

Aktivieren Sie diese Option, wenn SMTP-Auth Passwörter nie im Klartext übertragen werden sollen. Die SMTP-Auth Methoden PLAIN und LOGIN sind somit nur noch über SMTP-Verbindungen möglich, die mit Hilfe von TLS verschlüsselt werden.



Betroffen ist SMTP-Auth sowohl für ausgehende Verbindungen (Anmeldung beim Relay-Server des Providers) als auch bei eingehenden Verbindungen (Mail-Relay in das Internet nur für authentifizierte Clients).

Submission-Port 465 (SMTPS)

Aktiviert den Submission-Port 465. Verbindungen zu diesem Port sind von Anfang an verschlüsselt.

Submission-Port 587

Aktiviert den Submission-Port 587. Verbindungen zu diesem Port sind zunächst unverschlüsselt. Sofern es die Konfiguration des SX-GATEs zulässt, kann auf Anforderung des Clients auf verschlüsselte Kommunikation gewechselt werden (STARTTLS).

14.5.2-E Empfangs-Filter

Lesebestätigung unterdrücken

Öffnet ein Benutzer eine E-Mail mit gewünschter Lesebestätigung (Message Disposition Notification - MDN), wird er üblicherweise von seinem Mail-Programm gefragt, ob tatsächlich eine Lesebestätigung geschickt werden soll. Stimmt er zu, erhält der Absender per E-Mail die Bestätigung, dass seine Mail geöffnet wurde. In den meisten Mail-Programmen ist es möglich die Konfiguration zu ändern, so dass Lesebestätigungen ohne Nachfrage entweder nie oder immer geschickt werden.

Wenn Sie diese Option aktivieren, filtert SX-GATE bei eingehenden E-Mails die Header heraus, mit denen eine Lesebestätigung angefordert wird. Der Versand von Lesebestätigungen lässt sich so unabhängig von den Einstellungen der Mail-Programme unterbinden.



Der Versand von Zustellbestätigungen (Delivery Status Notification - DSN) wird nicht unterdrückt.

Von extern empfangene Mails markieren

Die im Mail-Programm angezeigten Absender-Adressen (From- und Sender-Header) lassen sich problemlos fälschen. Gutgläubige Mitarbeiter könnten z.B. auf eine E-Mail mit der Absenderadresse eines Vorgesetzten hereinfallen. Mit dieser Option lässt sich der Betreff von Mails markieren, wenn diese von extern empfangen wurden. Nicht als extern zählen authentifizierte Verbindungen und Verbindungen von Adressen die unter

"Lokale IP-Adressen" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" eingetragen wurden.

bei gefälschtem Absender aus lokaler Domain

In dieser Einstellung wird der Betreff nur dann markiert, wenn in der Absenderadresse eine der lokalen Domains genutzt wird. Dem Betreff wird dabei der Text "*****FAKE***** [Sender]" vorangestellt.



Sendet ein lokaler Absender eine E-Mail an eine Mailingliste, ist zu erwarten, dass die von der Mailingliste zurück gesendete E-Mail fälschlicherweise markiert wird.



Aktivieren Sie diese Option nur dann, wenn E-Mails mit lokalen Absenderdomains ausschließlich über lokale Systeme (SX-GATE bzw. interner Mailserver) in das Internet gesendet werden.

Interne Adressen vorab verifizieren

Aktivieren Sie diese Option, damit SX-GATE beim Empfang jeder Mail zunächst überprüft, ob der interne Mail-Server eine E-Mail mit den angegebenen Empfänger-Adressen überhaupt akzeptieren würde. Die Überprüfung findet schon statt, bevor der eigentliche Inhalt der Mail an SX-GATE übermittelt wird. Mails an unbekannte Empfänger werden so gar nicht erst angenommen.



Diese Option wirkt auf alle Empfänger-Domains, die SX-GATE an einen internen Mail-Server weiterleitet.



Die Adressverifikation wird auch dann aktiv, wenn SX-GATE E-Mails von einem POP- oder IMAP-Server abholt. Verweigert der interne Mail-Server die Annahme, wird die Mail in der Regel kommentarlos verworfen.

mit SMTP

Dies ist das einfachste Verfahren, das mit fast allen Mail-Servern funktioniert. Für jede eingehende E-Mail öffnet SX-GATE eine SMTP-Verbindung zum internen Mail-Server. Die vom Sender übermittelten Absender- und Empfänger-Adressen der E-Mail werden an den internen Mail-Server durchgereicht. Anhand der Rückmeldungen des internen Servers wird nun dem Sender signalisiert, ob dieser mit der Übertragung der Mail fortfahren darf oder ob die Annahme der Mail z.B. aufgrund ungültiger Adressdaten verweigert wird.



Mit diesem Verfahren können Sie sogar etwaige Optionen Ihres internen Mail-Servers zur Sperrung bestimmter Absender-Adressen nutzen.



Stellen Sie sicher, dass der interne Mail-Server nicht existierenden Empfänger-Adresse unmittelbar zurückweist. Nachfolgend ist beschrieben, wie Sie dies in Microsoft Exchange aktivieren können.

Bei Microsoft Exchange Servern muss zunächst der Empfängerfilter aktiviert werden. Installieren Sie dazu die Antispam-Agents indem Sie das Skript "Install-AntispamAgents" in den Unterordnern des Exchange Programm-Ordners suchen und starten. Aktivieren Sie dann den Empfängerfilter in der Exchange Management-Shell mit dem Befehl

`"Set-RecipientFilterConfig -Enabled $true -RecipientValidation-Enabled $true"`

. Seit Exchange 2013 muss ferner ein zusätzlicher HubTransport-Connector vom Exchange-Server bereitgestellt werden (Typ: Internet). Der Connector muss anonymen Zugriff erlauben. Wir empfehlen ferner, dass ausschließlich die SX-GATE-IP Zugriff auf diesen Connector erhält. Bei aktivierter Windows-Firewall muss üblicherweise der Zugriff auf den neuen Connector-Port mit einer zusätzlichen Regel freigegeben werden. Tragen Sie die Port-Nummer des Connectors schließlich im SX-GATE unter "SMTP-Port für Verifikation" ein.

mit LDAP (Active-Directory)

Die gewünschten Empfänger-Adressen werden bei diesem Verfahren im Active-Directory gesucht (Attribut "proxyAddresses"). Die notwendigen Parameter für die LDAP-Suche konfigurieren Sie bitte im Menü "System > Benutzerverwaltung > Einstellungen".

Mail annehmen wenn Verifikation nicht möglich

Ist diese Option ausgeschaltet und eine Verifikation ist nicht möglich, weil der dazu benötigte Server nicht erreichbar ist, wird ein temporärer SMTP-Fehler gesendet. Meldet der interne Mail-Server bei Verifikation mit SMTP einen temporären Fehler (z.B. unzureichender Speicherplatz), wird dieser unverändert weitergegeben. Die Mail verbleibt somit in beiden Fällen auf dem zustellenden System. Dieses wird in der Regel später weitere Zustellversuche unternehmen. SX-GATE akzeptiert die Mail erst, wenn diese erfolgreich gegenüber dem internen Mail-Server verifiziert werden konnte.

Wenn Sie diese Option aktivieren, nimmt SX-GATE hingegen in beiden Situationen die Mail ohne Verifikation an. Die Mail verbleibt in SX-GATEs Warteschlange, falls der interne Mail-Server nicht erreichbar ist oder temporäre Fehler meldet. SX-GATE schickt die Mail als unzustellbar an den Absender zurück, falls der interne Mail-Server die Mail ablehnt (z.B. wegen unbekannter Empfänger-Adresse) oder die auf dem Reiter

(Tab) "Versand-Parameter" konfigurierte maximale Haltedauer in der Warteschlange abgelaufen ist (Einstellung "Mail als unzustellbar zurück wenn nicht ausgeliefert nach").

SMTP-Port für Verifikation

Die Verifikation der Adressen kann über einen vom Mailversand abweichenden Port erfolgen.

LDAP-Anbindung testen

Mit diesem Schalter wird geprüft, ob im Active-Directory E-Mail-Adressen gefunden werden.

E-Mail an unbekannte lokale Empfänger

Soll eine Mail an eine lokale Domain zugestellt werden und der Adressat existiert auf dem SX-GATE weder als Konto noch als Verteiler (Gruppe), so kann SX-GATE die Annahme der Mail verweigern. Das System, das die E-Mail an SX-GATE übermitteln wollte muss dann den Absender darüber in Kenntnis setzen. Alternativ können E-Mails für unbekannte Empfänger an ein bestimmtes Benutzer-Konto bzw. an einen bestimmten Verteiler ausgeliefert werden. Die Eingabe einer kompletten E-Mail-Adresse (mit "@" und Domain) ist dabei nicht erlaubt. Geben Sie nur den Namen des gewünschten Benutzers (Login) bzw. der Gruppe an.



Die Annahme von E-Mails die mit Hilfe des SX-GATE Mail-Clients von POP-Servern abgeholt wurden, kann nicht verweigert werden. Wird dennoch diese Option ausgewählt, so werden die betroffenen E-Mails an den Administrator zugestellt.

Mails von folgenden Mail-Adressen, Mail-Domains oder IP-Adressen abweisen

Die Annahme von E-Mails von bestimmten Adressen lässt sich mit Hilfe dieses Bereichs verhindern. Folgende Eingaben sind hier möglich:

Eine vollständige E-Mail-Adresse (z.B. spam@example.com)

E-Mails von diesem Absender werden abgelehnt. Entscheidend ist dabei der sog. "Envelope-From", nicht der From-Header der üblicherweise von Mail-Client-Programmen als Absender angezeigt wird.

Ein Domainname (z.B. example.com)

Hier wird die Annahme von E-Mails mit beliebigem Absendern aus der entsprechenden Domain und deren Subdomains verweigert. Im Beispiel würden sowohl spam@example.com als auch info@www.example.com abgewiesen werden.

Neben der Überprüfung der E-Mail-Adresse wird zudem mittels DNS der Hostname zu der IP-Adresse ermittelt, von der die SMTP-Verbindung kommt. Gehört dieser Hostname zu der gesperrten Domain, so wird die E-Mail ebenfalls nicht angenommen. Nehmen wir an, die Verbindung käme von der Adresse

169.254.254.20 und laut DNS wäre der Hostname zu dieser IP 254-20.ppp-pool.example.com, so würde auch hier die Sperre greifen.

Eine IP-Adresse

E-Mails die über SMTP-Verbindungen von gesperrten IP-Adresse zugestellt werden, weist SX-GATE ab.



Im Maillog des SX-GATE wird für jede E-Mail sowohl der "Envelope-From" als auch die Quell-IP aufgezeichnet. Suchen Sie nach der Zeile, die die Quell-Informationen zu der E-Mail enthält ("from="). Bei "from=" ist die "Envelope-From"-Adresse angegeben. Die Quell-Adresse der SMTP-Verbindung finden Sie bei "relay=".



Bei E-Mails die mit Hilfe des SX-GATE Mail-Clients von einem POP-Server abgeholt wurden, ist die Quell-IP-Adresse der Verbindung stets SX-GATE selbst (127.0.0.1, localhost). Bei diesen Mails ist folglich nur die Überprüfung der E-Mail-Adresse des Absenders sinnvoll.

14.5.2-F Limits

In diesem Bereich werden diverse Obergrenzen eingestellt, die SX-GATE und nachgelagerte Systeme vor Überlastung schützen sollen. Betroffen sind alle SMTP-Verbindungen, die zu SX-GATE aufgebaut werden. Es spielt dabei keine Rolle, ob die Verbindung von einem Mail-Client-Programm oder einem anderen Mail-Server kommt. Die Beschränkungen greifen im Normalfall allesamt bereits vor der Übermittlung des eigentlichen Inhalts der E-Mail.

Maximal Anzahl gleichzeitiger Verbindungen

Dieser Parameter limitiert die Gesamtzahl der geöffneten Verbindungen zum SX-GATE Mail-Server. Eingerechnet werden also sowohl Verbindungen aus dem internen LAN als auch von extern aus dem Internet. Die Einstellung soll das System vor Überlastung schützen.

Maximal Anzahl gleichzeitiger Verbindungen pro IP

Mit dieser Einstellung limitieren Sie die Anzahl paralleler Verbindungen je IP. Es soll so verhindert werden, dass einzelne Server den SX-GATE Mail-Server überlasten können.

Im Gegensatz zur vorherigen Option, sind ausschließlich Verbindungen von externen Adressen betroffen. Von daher wirkt sich dieser Wert nur dann aus, wenn SX-GATE E-Mails direkt aus dem Internet empfängt und nicht z.B. von POP-Servern abholt.



Als externe Adressen zählen alle IPs, die nicht unter "Lokale IP-Adressen" auf dem Reiter (Tab) "Relay Kontrolle" eingetragen sind.

Maximal Anzahl Verbindungen pro IP und Minute

Ähnlich der vorherigen Einstellung wird auch hier die Anzahl der Verbindungen je IP begrenzt, jedoch deren Anzahl pro Minute. Auch hier sind nur Verbindungen von Extern betroffen.

Maximal Anzahl Empfänger pro Nachricht

Hier legen Sie fest, wie viele Empfänger maximal pro Zustellversuch in einer Nachricht akzeptiert werden. Beim Überschreiten dieser Grenze werden weitere Empfänger-Adressen mit einem "vorübergehenden Fehler" abgelehnt. Für diese Adressen muss ein erneuter Zustellversuch unternommen werden.

Maximal zulässige Größe einer E-Mail

Der Sinn einer E-Mail ist nicht die Übertragung von Datenmengen im Bereich von vielen Megabyte. Das SMTP-Protokoll ist dafür nicht ausgelegt. Viele Mail-Server im Internet akzeptieren Mails daher auch nur bis zu einer bestimmten Größe oder brechen die Übertragung nach einer bestimmten Zeit ab. Es empfiehlt sich deshalb, auch im SMTP-Server des SX-GATE eine entsprechende Größenbeschränkung einzustellen.

Maximal zulässige Größe der E-Mail-Header

Sollten E-Mails aufgrund übergroßer Header abgewiesen werden, können Sie hier die zulässige Größe anpassen.

14.5.2-G Archivierung / Milter

Die Milter-Schnittstelle erlaubt die Anbindung eines externen, milterfähigen Mail-Filter-Produkts über das Netzwerk. Insbesondere zur Anbindung einer Archivierungslösung ist die Milter-Schnittstelle optimal geeignet.

Steht keine externe Archivierungsmöglichkeit mit Milter-Schnittstelle zur Verfügung, kann jede E-Mail automatisch in Kopie an einen zusätzlichen Empfänger weitergeleitet werden. Ob sich hinter dem zusätzlichen Empfänger ein Postfach des SX-GATE, eine Adresse auf einem internen Mail-Server oder auch eine Adresse im Internet handelt spielt dabei keine Rolle. Die Konfiguration dieser Funktion kann für ein- und ausgehende E-Mails getrennt vorgenommen werden.



Sollte es sich bei dem zusätzlichen Empfänger um ein SX-GATE Postfach handeln, so ist dieses regelmäßig zu leeren. Der POP3/IMAP4-Server des SX-GATE ist nicht als Langzeit-Archiv konzipiert.



Beachten Sie bei Aktivierung unbedingt die einschlägigen Rechtsvorschriften. Die Aktivierung dieser Funktion kann durch Vorschriften oder Gesetze mit bestimmten Auflagen verbunden oder sogar verboten sein.

Archivierungs-Adresse für ausgehende E-Mails

Geben Sie hier die E-Mail-Adresse ein, an die jede ausgehende E-Mail in Kopie gesendet werden soll.



Als ausgehende E-Mail zählt jede E-Mail die SX-GATE von einer internen IP-Adresse erhält. Welche Adressen als intern gelten ist auf dem Reiter (Tab) "Relay Kontrolle" festgelegt. Auch authentifiziert angelieferte E-Mails zählen als intern.

Archivierungs-Adresse für eingehende E-Mails

Geben Sie hier die E-Mail-Adresse ein an die jede eingehende E-Mail in Kopie gesendet werden soll. Sie können die selbe Adresse verwenden wie für ausgehende E-Mails.



Diese Funktion wird erst nach dem Virensan-Modul ausgeführt. Virenverseuchte E-Mails werden daher nicht in das Archiv einbezogen. Vor der Weiterleitung an den Archiv-Benutzer wird die E-Mail ggf. noch durch Dateianhangs- und Relay-SPAM-Filter modifiziert. Verwirft letzterer die Mail, wird diese ebenfalls nicht in das Archiv einbezogen.

Externer Milter

Dieser Schalter erlaubt es, einen externen Milter in den SX-GATE Mail-Server einzubinden. Wählen Sie bitte aus, zu welchem Zeitpunkt bei der E-Mail-Verarbeitung der externe Milter kontaktiert werden soll.

Adresse des Milters

Geben Sie hier den Hostnamen oder die IP des externen Milters ein.

Port der Milter-Applikation

Der TCP-Port an dem der Milter Verbindungen entgegennimmt muss hier eingetragen werden.

14.5.3 SPAM/Virus/Malware

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.5.3-A Plausibilitätstests.....	501
14.5.3-B Greylisting.....	505
14.5.3-C SPF/DMARC-Filter.....	510
14.5.3-D Virens Scanner.....	512
14.5.3-E MIME-Filter.....	513
14.5.3-F MIME-Filter Regeln.....	517
14.5.3-G MIME-Filter Optionen.....	519
14.5.3-H Relay SPAM-Filter.....	522
14.5.3-I SPAM Bewertung.....	524
14.5.3-J SPAM Module.....	526
14.5.3-K SPAM Einstellungen.....	529

14.5.3-A Plausibilitätstests

Die Kriterien, die in diesem Bereich eingestellt werden, sollen die nachgelagerten Malware- und SPAM-Filter entlasten, indem ein Teil der unerwünschten Post bereits im Vorfeld aussortiert wird. Untersucht werden alle SMTP-Verbindungen die zu SX-GATE aufgebaut werden. Es spielt dabei keine Rolle, ob die Verbindung von einem Mail-Client-Programm oder einem anderen Mail-Server kommt. Eine E-Mail, die die hier vorgegebenen Richtlinien verletzt, wird bereits vor der Übermittlung der eigentlichen Nutzdaten abgewiesen.

Schutz vor automatisierten Mail-Programmen

SPAM- und Virenmails werden häufig über recht einfache Routinen verbreitet, die in kürzester Zeit so viele Mails wie möglich generieren sollen. Dies macht sich diese Schutzfunktion zu Nutze: Normalerweise beantwortet ein Mail-Server eine neue Verbindung sofort mit einer Begrüßungsmeldung. Auf diese wartet der Zusteller und sendet dann seinerseits eine Begrüßung. Sobald diese Option aktiviert ist, sendet

SX-GATE die Begrüßung erst nach einer minimalen Verzögerung. Wartet der Client nicht darauf sondern schickt schon zuvor seine Befehle ab, wird die Verbindung als unerwünscht abgelehnt.



Die Funktion wirkt sich ausschließlich auf Verbindungen von externen IP-Adressen aus. Als externe Adressen zählen alle IPs, die nicht unter "Lokale IP-Adressen" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" eingetragen sind. SX-GATE muss E-Mails daher direkt per SMTP aus dem Internet empfangen. Auf E-Mails die von einem POP-Server abgeholt werden, hat diese Einstellung keinen Einfluss.



Durch diese Funktion kann auch der Empfang erwünschter E-Mails beeinträchtigt werden.

Prüfe HELO/EHLO

Mit dieser Option lässt sich erzwingen, dass sich das sendende System mit einem plausiblen Rechnernamen meldet. Der Rechnername muss mindestens einen Punkt enthalten und darf nicht identisch zum Rechnernamen des SX-GATE sein. Trifft dies nicht zu, wird die E-Mail abgewiesen.



Authentifizierte Verbindungen und Verbindungen von Adressen die unter "Lokale IP-Adressen" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" eingetragen wurden, sind von dieser Überprüfung ausgenommen. Auch auf E-Mails die von einem POP-Server abgeholt werden, hat diese Einstellung keinen Einfluss.

Prüfe Reverse-DNS

Aktivieren Sie diese Option um die DNS-Information zur Quell-IP eingehender Verbindungen zu untersuchen. Bei vielen zum SPAM-Versand missbrauchten Heim-PCs schlägt diese Überprüfung fehl.



Diese Überprüfung wird weder bei authentifizierten noch bei lokalen Verbindungen durchgeführt. Auch bei E-Mails die von einem POP3-Server abgeholt werden ist diese Option wirkungslos.

auf Existenz

In dieser Einstellung wird die Annahme von Mails verweigert, wenn kein Reverse-DNS Eintrag für die sendende IP existiert.

mit Rückauflösung

Auch hier muss ein Eintrag im Reverse-DNS existieren. Zu dem über Reverse-DNS erhaltenen Rechnernamen wird dann jedoch mit Hilfe einer weiteren DNS-Anfrage wieder die IP-Adresse ermittelt. Stimmt diese IP-Adresse nicht mit der ursprünglichen IP überein, wird die Mail nicht angenommen (Forward-confirmed Reverse DNS).



Diese Einstellung stellt hohe Anforderungen an die DNS-Konfiguration eines Mail-Servers. Es ist damit zu rechnen, dass in Einzelfällen der Empfang erwünschter E-Mails beeinträchtigt wird.

Prüfe Absenderdomain

Mit dieser Option aktivieren Sie die Überprüfung des Domain-Teils der Absender-Adresse jeder eingehenden E-Mail.



Von dieser Überprüfung können auch gewünschte E-Mails betroffen sein, die fälschlicherweise einen ungültigen Absender benutzen. Dies kommt beispielsweise bei automatisch generierten E-Mails von falsch eingestellten Online-Registrierungen oder Bestell-Systemen vor.

auf Existenz

Mails werden nicht angenommen, wenn die Absenderdomain im DNS nicht existiert.

auf gültigen Mailserver

In dieser Einstellung wird zusätzlich die IP-Adresse des Mail-Servers für diese Domain ermittelt. Handelt es sich um eine ungültige IP, wird die Verbindung abgewiesen. Bei Verbindungen von internen IP-Adressen wird der Test nicht durchgeführt.

Meldet DNS bei der Namensauflösung der Absender-Domain einen permanenten Fehler (z.B. Domain existiert nicht), so verweigert der SX-GATE Mail-Server die Annahme der E-Mail mit einer Fehlermeldung. Es ist Aufgabe des Zustellers (E-Mail-Client eines Benutzers oder anderer Mail-Server) geeignet zu reagieren.



Wurde die E-Mail mit Hilfe des SX-GATE Mail-Clients von einem POP-Server abgerufen, so wird die Mail kommentarlos verworfen. Aufgrund der ungültigen Domain wäre eine Unzustellbarkeitsbenachrichtigung an den Absender zwecklos. Die Zustellung an den lokalen Administrator würde dem eigentlichen Zweck, der Abweisung von SPAM-Mails, widersprechen.

DNS kann jedoch auch ein vorübergehendes Problem bei der Namensauflösung melden (z.B. DNS-Server nicht erreichbar). Die Reaktion des Mail-Servers hängt dann davon ab, ob der SX-GATE Mail-Client in der Konfiguration aktiviert ist. Ist dies nicht der Fall, verweigert der SX-GATE Mail-Server die Annahme der Mail mit einem temporären Fehler. Es ist dann dem Zusteller überlassen, ob und wie oft dieser die Zustellung zu einem späteren Zeitpunkt wiederholt bevor der Absender über das Problem unterrichtet wird. Ist das DNS-Problem bei einem späteren Zustellversuch behoben, so wird die E-Mail akzeptiert. Ist der SX-GATE Mail-Client hingegen aktiviert, so werden E-Mails grundsätzlich bei temporärem DNS-Fehler akzeptiert. Dadurch wird vermieden, dass der SX-GATE Mail-Client immer wieder die selbe E-Mail vom Provider abrufen sollte das angeblich temporäre DNS-Problem in Wahrheit dauerhaft sein.

Mails mit eigener Domain als Absender abweisen

Viele unerwünschte Mails verwenden in der Absender-Adresse die Domain des Empfängers. Mit dieser Option werden eingehende E-Mails abgewiesen, wenn in der Absender-Adresse eine der lokalen Domains angegeben ist. Authentifizierte Verbindungen und Verbindungen von Adressen die unter "Lokale IP-Adressen" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" eingetragen wurden, sind von dieser Überprüfung ausgenommen. Auch auf E-Mails, die von einem POP-Server abgeholt werden, hat diese Einstellung keinen Einfluss.



Geprüft wird hier der sog. "Envelope-From" und nicht der von Mailprogrammen angezeigte Absender (From-Header). Eine Prüfung des From-Headers erlaubt die Option "Von extern empfangene Mails markieren" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Empfangs-Filter".



Aktivieren Sie diese Option nur dann, wenn E-Mails mit lokalen Absenderdomains ausschließlich über lokale Systeme (SX-GATE bzw. interner Mailserver) in das Internet gesendet werden.

14.5.3-B Greylisting

Das Konzept der Grauen Liste (Greylisting) soll bereits die Übermittlung vieler Viren- und SPAM-Mails verhindern. Virens Scanner und SPAM-Filter werden entlastet. Greylisting darf jedoch auf gar keinen Fall als Ersatz für Virens Scanner und SPAM-Filter gesehen werden. Die Graue Liste macht es sich zu Nutze, dass bei diesen unerwünschten E-Mails häufig nur ein Zustellversuch unternommen wird. Schlägt dieser fehl, erfolgt kein weiterer Versuch mehr und die E-Mail ist abgewehrt.



Die Aktivierung der Grauen Liste ist nur dann sinnvoll, wenn eingehende E-Mails direkt per SMTP an SX-GATE zugestellt werden. Die Graue Liste ist insbesondere wirkungslos bei E-Mails die von POP-Servern abgeholt werden.

Ist die Graue Liste aktiviert, so lässt sich SX-GATE bei einer eingehenden E-Mail die Adressen von Absender und Empfänger übermitteln. Danach wird die Verbindung mit dem Hinweis auf einen temporären Fehler abgebrochen, ohne dass der eigentliche Inhalt der E-Mail übermittelt wurde. Da der Zustellversuch in der Regel ja nicht vom Mailprogramm des Absender direkt sondern durch dessen Postausgangs-Server vorgenommen wird, erlangt der Absender zunächst keine Kenntnis über die Verzögerung. Aufgrund des temporären Fehlers wird der Mail-Server vielmehr zu einem späteren Zeitpunkt einen erneuten Zustellversuch unternehmen. Dies ist der entscheidende Unterschied zum Verhalten vieler SPAM-Mail Versender und den Verbreitungsroutinen der meisten Viren-Programme.

Konfiguriert wird das Verhalten der Grauen Liste über drei Parameter. Zunächst wird festgelegt, wie viel Zeit nach dem ersten Zustellversuch mindestens vergehen muss. Ein weiterer Parameter legt fest, innerhalb welcher Frist dann eine erneute Zustellung erfolgen muss. Innerhalb dieser Zeitspanne werden E-Mails sofort angenommen die von der registrierten Quell-IP kommen und den bekannten Absender und Empfänger aufweisen. Erfolgt keine erneute Zustellung wird die Freigabe gelöscht. Andernfalls verlängert jede E-Mail die Gültigkeit einer Freigabe auf einen einstellbaren Wert.

Auf die beschriebene Weise entsteht rasch eine Datenbank von "bekannten Kommunikationsbeziehungen". E-Mails die sich einer bereits bekannten Kombination aus Quell-IP, Absender und Empfänger zuordnen lassen, werden sofort akzeptiert. Beim Empfang von E-Mails mit einer unbekannten oder lange nicht genutzten Kombination kommt es hingegen zu einer Verzögerung.



Wann ein Mail-Server einen erneuten Zustellversuch unternimmt ist in dessen Konfiguration festgelegt. SX-GATE hat darauf keinen Einfluss. In den meisten Fällen wird die Zustellung nach weniger als einer Stunde erneut versucht. Längere Intervalle kommen aber vor. Es lässt sich auch nicht gänzlich ausschließen, dass manche Mail-Server keine weiteren Zustellversuche unternehmen. Üblicherweise wird dann jedoch der Absender über das Problem unterrichtet. Eine Positivliste mit wichtigen Mail-Servern die sich derart verhalten ist integriert.

Um unerwünschte Verzögerungen zu vermeiden, kann die Graue Liste in der Konfiguration für bestimmte Absender oder Empfänger außer Kraft gesetzt werden. Grundsätzlich hat die Graue Liste keinen Einfluss bei

- Verbindungen von lokalen IP-Adressen (vgl. Option "Lokale IP-Adressen" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle")
- Verbindungen von IP-Adressen die in der integrierten Liste von Servern enthalten sind, die keine weiteren Zustellversuche unternehmen
- E-Mails die von POP-Servern abgeholt wurden
- authentifizierten Verbindungen (SMTP Auth)

Arbeitsweise

Mit diesem Schalter aktivieren Sie die Graue Liste. Wie in der obigen Beschreibung der Wirkungsweise erwähnt, ist dies nur dann sinnvoll, wenn eingehende E-Mails direkt per SMTP empfangen werden. Für mindestens eine lokale Domain muss folglich im Internet DNS der Mail-Exchanger-Eintrag (MX) auf die externe IP-Adresse des SX-GATE verweisen.



Eventuelle Backup-MX-Einträge müssen aus dem DNS entfernt werden. Ausgenommen sind Backup-Server, die nur dann E-Mails annehmen, wenn SX-GATE tatsächlich unerreichbar ist sowie Backup-Server die selbst mit Greylisting arbeiten. Stimmen Sie in diesem Fall das zeitliche Verhalten der Grauen Listen aufeinander ab.



Nicht geeignet sind Konstellationen in denen SX-GATE eingehende E-Mails zwar per SMTP empfängt, dies aber grundsätzlich von einem vorgelagerten Mail-Relay-Server. Eine Umstellung auf direkten Empfang sollte in diesem Fall jedoch einfach möglich sein.

DNS-Blacklist prüfen

Dies ist die schwächste Einstellung für das Greylisting und kann in der Regel problemlos auf jedem Mail-Server aktiviert werden, der die Grundvoraussetzungen für den Betrieb der Grauen Liste erfüllt. Beim Verbindungsaufbau prüft SX-GATE, ob die Quell-IP der Verbindung in einer der einschlägigen Echtzeit-Datenbanken als bekannter SPAM-Versender oder als dynamische IP-Adresse verzeichnet ist. Nur wenn dies der Fall ist, wird für diese E-Mail das Greylisting angewandt.

Exchange2k-/Sammelkonto-Modus

Diese Einstellung ist ausschließlich für zwei spezielle Szenarien gedacht. Bei jeder ausgehenden Mail wird dabei der Absender automatisch als Empfänger freigegeben. Jede weitere ausgehende Mail erneuert die Freigabe, die andernfalls nach der unter "Verfallsdauer nach letzter Nutzung" konfigurierten Zeitspanne automatisch gelöscht wird. Die Anlernphase für diese Konfiguration ist sehr kurz, da jeder lokale Benutzer lediglich eine Mail versenden muss.



Wichtige lokale E-Mail-Adressen, die selten oder nie als Absender-Adresse von ausgehenden Mails genutzt werden, sollten manuell unter "Freigegebene Empfänger" eingetragen werden.



Wählen Sie diese Einstellung nur, wenn eines der nachfolgend beschriebenen Szenarien zutrifft. Die Graue Liste ist andernfalls mehr oder weniger wirkungslos.

Nutzen Sie diese Option, wenn SX-GATE einen nachgelagerten Microsoft Exchange Server in Version 2000 oder älter beliefert. Diese Versionen sind nicht in der Lage, eine E-Mail an eine unbekannte lokale Adresse vorab abzulehnen. Vielmehr wird die Mail angenommen und, falls der Empfänger nicht existiert, eine Unzustellbarkeits-Mitteilung an den Absender zurückgeschickt. Die Anzahl der zu verarbeitenden Mails wird dadurch nahezu verdoppelt, was eine erhöhte Belastung der gesamten Infrastruktur nach sich zieht. Schlimmer noch: Insbesondere bei SPAM-Mails wird der Unzustellbarkeits-Bericht häufig an eine gefälschte oder nicht existierende Adresse gesendet, was zu weiteren Unannehmlichkeiten führt. Der spezielle Greylisting-Modus des SX-GATE kann hier helfen, die Anzahl der Unzustellbarkeits-Meldungen zu verringern, da Mails an unbekannte Adressen das Greylisting durchlaufen müssen.



Exchange 2003 und neuer kann so eingestellt werden, dass E-Mails an unbekannte Adressen unmittelbar abgewiesen werden. Dies wiederum kann SX-GATE abprüfen. Beachten Sie dazu bitte die Einstellung "Interne Adressen vorab verifizieren" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Empfangs-Filter".

Der zweite Anwendungsfall sind sog. "Catch-All" E-Mail-Domains. Dabei geht es um E-Mail-Domains in denen es keine unbekannten Empfänger gibt. Jede E-Mail deren Empfänger-Adresse keinem Benutzer zugeordnet werden kann, wird in ein Sammelpostfach (Zentraleingang) zugestellt. Ein Großteil dieser Mails wird auf SPAM-Mails entfallen, die an mehr oder weniger zufällige Empfänger-Adressen gesendet wurden. Die beste Lösung wäre ein vollständiger Verzicht auf das Sammelpostfach. Leitet SX-GATE alle Mails an einen internen Mail-Server weiter, so aktivieren Sie im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Empfangs-Filter" die Option "Interne Adressen vorab verifizieren" und deaktivieren Sie das Sammelkonto in der Konfiguration des internen Mail-Servers. Falls SX-GATE selbst das Sammelkonto führt, kann dieses an gleicher Stelle mit Hilfe der Option "E-Mail an unbekannte lokale Empfänger" deaktiviert werden. Ist es nicht möglich auf das Sammelkonto zu verzichten, kann diese spezielle Greylisting-Option dabei helfen, SX-GATE zu entlasten und den SPAM-Anteil im Sammelkonto zu verringern.

Mailpartner freigeben

Generell muss in dieser Einstellung jede eingehende E-Mail das Greylisting durchlaufen. Zusätzlich wird aber bei jeder ausgehenden E-Mail die Kombination aus Absender und Empfänger ermittelt und in umgekehrter Reihenfolge für eingehende E-Mails freigeben. Dadurch wird gewährleistet, dass Antwort-Mails und der weitere Nachrichtenaustausch zwischen den selben Kommunikationspartnern ohne Verzögerung abläuft. Die Freigabe ist dabei unabhängig von der IP-Adresse des Absenders. Jede weitere ausgehende E-Mail mit der selben Adresskombination erneuert die Freigabe. Eine nicht mehr genutzte Freigabe verfällt nach der unter "Verfallsdauer nach letzter Nutzung" eingestellten Zeitspanne.



Verzögerungen bei der Kommunikation werden in dieser Einstellung nur dann vermieden, wenn der E-Mail-Austausch von einem lokalen Benutzer initiiert wird. Wichtige Empfänger- oder Absender-Adressen bei denen eine Verzögerung nicht akzeptabel ist, sollten daher unbedingt manuell unter "Freigegebene Empfänger" bzw. "Freigegebene Empfänger" eingetragen werden. Erklären Sie zudem den Anwendern die vor allem in der Anfangsphase zu erwartenden Verzögerungen.

immer aktiv

Hiermit wird die "reine" Form der Grauen Liste aktiviert. Jede eingehende Mail wird dabei zunächst verzögert, sofern die Kombination aus IP-Adresse, Absender und Empfänger noch nicht bekannt ist.



Um Akzeptanzproblemen seitens der Anwender zu begegnen, raten wir dringend dazu, diesen die zu erwartenden Verzögerungen zu erklären und schon vor Aktivierung der Grauen Liste wichtige Absender und Empfänger unter "Freigegebene Empfänger" bzw. "Freigegebene Empfänger" einzutragen.

Zustellung akzeptieren nach frühestens

Wird eine neue Kombination aus Quell-IP, Absender und Empfänger in der Grauen Liste erkannt, so gibt dieser Parameter an, nach wie viel Minuten Verbindungen mit dieser Kombination freigegeben werden. Eine erneute Zustellung hat also frühestens nach Ablauf dieser Zeitspanne Aussicht auf Erfolg.



Erfolgt ein erneuter Zustellversuch vor der Freigabe, wird auch dieser mit einem temporären Fehler abgebrochen. Die verbleibende Dauer bis zur Freigabe verlängert sich dadurch jedoch nicht.

Verfallsdauer ungenutzter Freigaben

Dieser Parameter legt fest, innerhalb welcher Zeitspanne nach Freigabe ein erneuter Zustellversuch erfolgen muss. Andernfalls wird die Freigabe wieder gelöscht. Ein niedriger Wert verkleinert einerseits die interne Datenbank und verringert die Gefahr, dass Verbindungsversuche fälschlicherweise als erneuter Zustellversuch gewertet werden. Andererseits kann dadurch aber auch die Zustellung gewünschter Mails scheitern.



Relay-Server die erneute Zustellversuche erst nach längerem Zeit-Intervall unternehmen, können E-Mails nicht mehr an SX-GATE zustellen, wenn dieser Parameter auf einen zu kleinen Wert gestellt wird.

Verfallsdauer nach letzter Nutzung

Erfolgt ein erneuter Zustellversuch, so wird die entsprechende Kombination aus Quell-IP, Absender und Empfänger als Freigegeben abgespeichert. Diese Freigabe gilt für die hier konfigurierte Zeitspanne und wird durch jede neue E-Mail automatisch entsprechend verlängert.

Freigegebene Absender

In dieser Liste lassen sich IP-Adressen bzw. DNS-Namen von Mail-Servern eintragen. Die Graue Liste lässt E-Mails grundsätzlich passieren, wenn die Quelle der Verbindung hier freigegeben ist. Es ist ferner möglich, die E-Mail Adressen einzelner Absender oder ganzer Domains zu hinterlegen. Um beispielsweise alle Absender der Domain "example.com" freizugeben tragen Sie bitte "*"@example.com" ein.



Bedenken Sie bitte, dass sich die Absender-Adresse einer E-Mail nahezu beliebig fälschen lässt. Es wird ausschließlich die im SMTP-Protokoll übermittelte Absender-Adresse geprüft (Envelope-From).

Freigegebene Empfänger

Um zeitliche Verzögerungen bei bestimmten Empfänger-Adressen auszuschließen, können diese hier eingegeben werden. Um die Graue-Liste für eine komplette Domain zu deaktivieren, kann auch hier ein Stern als Platzhalter verwendet werden (z.B. "*"@example.com").

14.5.3-C SPF/DMARC-Filter

SPF steht für "Sender-Policy-Framework". Der Inhaber einer Domain kann dabei im DNS hinterlegen, dass nur bestimmte Server berechtigt sind, E-Mails für diese Domain zu verschicken. Das bedeutet, dass der gesamte Mailverkehr von dieser Domain über die angegebenen Server gesendet werden muss. Der Empfänger kann den SPF-Eintrag im DNS abrufen und E-Mails abweisen, die nicht der Vorgabe entsprechen. Dabei wird zum einen der sog. HELO-Name geprüft, also der Rechnername mit dem sich das sendende System beim Empfängersystem vorstellt. Ferner wird der sog. Envelope-Sender, also die SMTP-Absenderadresse, geprüft. Diese ist maßgeblich für den Mailversand und nicht unbedingt identisch mit der Absenderadresse, die im

Mail-Programm angezeigt wird. SPF kann einen Beitrag zur Abwehr von SPAM und Schadsoftware leisten, indem es E-Mails mit gefälschtem Absender abweist.



Wenn Sie sich dafür entscheiden, einen restriktiven SPF-Eintrag für die eigene Domain anzulegen, wird der Filter auch Mails abfangen, die die eigene Domain als Absender missbrauchen. Sofern SX-GATE ausgehende Mails direkt versendet, sollten Sie jedoch im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Versand-Parameter" prüfen, ob ein gültiger HELO-Name verwendet wird. Eine Alternative zum SPF-Eintrag für die eigene Domain ist die Option "Mails mit eigener Domain als Absender abweisen" auf dem Reiter (Tab) "Plausibilitätstests".



Probleme kann es insbesondere mit von Dritten weitergeleiteten E-Mails einer SPF geschützten Domain geben. Beachten Sie bitte unbedingt auch die Hinweise zur Option "Freigegebene IP-Adressen".

DMARC steht für "Domain-based Message Authentication, Reporting and Conformance" und soll das letztgenannte Problem entschärfen. Es kombiniert dazu SPF und DKIM (DomainKeys Identified Mail). Ein Domaininhaber, der seine Domain mit DMARC absichern will, muss ausgehende Mails mit DKIM signieren, im DNS den öffentlichen DKIM-Schlüssel hinterlegen und ebenfalls im DNS sowohl eine SPF- als auch eine DMARC-Richtlinie konfigurieren. Das Mailsystem des Empfängers prüft bei einer eingehenden Mail sowohl SPF als auch DKIM. Die DMARC-Prüfung gilt als erfolgreich, wenn entweder SPF oder DKIM erfolgreich geprüft werden konnten, wobei zusätzlich die Domain aus der Absender-Adresse laut "From"-Header einem Vergleich standhalten muss: Im Falle von SPF wird sie mit der Domain aus der SMTP-Absender-Adresse (Envelope-From) verglichen, bei DKIM mit der Domain aus der DKIM-Signatur. Die Domains müssen gleich sein, wobei die meisten DMARC-Richtlinie auch Unterdomains zulassen.

Der SPF/DMARC-Filter prüft ausschließlich eingehende E-Mails. Nicht geprüft werden somit E-Mails, die von IP-Adressen empfangen werden, die im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" unter "Lokale IP-Adressen" konfiguriert sind. Authentifiziert angelieferte E-Mails werden ebenfalls nicht geprüft.



Die Aktivierung der SPF/DMARC-Prüfung ist nur dann sinnvoll, wenn eingehende E-Mails direkt per SMTP an SX-GATE zugestellt werden. Der Filter ist insbesondere wirkungslos bei E-Mails die von POP-Servern abgeholt werden.

SPF/DMARC prüfen

Über diesen Schalter können Sie die Prüfung aktivieren.

nur SPF

In dieser Einstellung wird ausschließlich SPF geprüft und zwar schon bevor die eigentliche Mail übertragen wird.

DMARC oder SPF

Aktiviert die DMARC-Prüfung. Sofern zu einer Domain nur eine SPF- aber keine DMARC-Richtlinie veröffentlicht wurde, findet eine SPF-Prüfung statt.

Freigegebene IP-Adressen

Vom SPF/DMARC-Filter nicht geprüft werden eingehende E-Mails von IP-Adressen die als "Lokale IP-Adressen" auf dem Reiter (Tab) "Relay Kontrolle" des Menüs "Module > Mail-Server > SMTP Einstellungen" konfiguriert wurden. Oft müssen jedoch noch weitere Adressen freigegeben werden:

Backup-MX

Ist für die eigene Domain ein Backup-MX konfiguriert, muss SX-GATE eingehende Mails von diesem Backup-MX grundsätzlich ohne Prüfung annehmen, da der Backup-MX im Sinne von SPF ja kein autorisierter Versender von E-Mails der Absender-Domain ist.



Wird ein Backup-MX genutzt, muss dieses ebenfalls eine SPF/DMARC-Filterung durchführen. Andernfalls kann SX-GATEs SPF/DMARC-Filter über den Backup-MX umgangen werden und ist somit wirkungslos. Verzichten Sie ggf. auf den Backup-MX .

Eigene externe Systeme

Ist für die eigene Domain ein restriktiver SPF-Eintrag konfiguriert, müssen häufig eigene externe Systeme freigegeben werden. Dies ist der Fall wenn das System z.B. seinen Status oder auch kritische Zustände per Mail meldet und dabei die eigene, von SPF geschützte Domain als Absender nutzt.

14.5.3-D Virens Scanner

Virens can aktivieren

Ist dieser Schalter aktiviert, so werden alle ein- und ausgehenden E-Mails die den Mail-Server des SX-GATE passieren auf Viren geprüft. Ausgenommen davon sind Mails, die auf der Systemebene von SX-GATE generiert wurden wie z.B. Statusmeldungen und Backups. E-Mails, die SX-GATE-Erweiterungen wie insbesondere die Groupware versenden, werden gescannt.



Damit diese Funktion wirksam ist, muss ein funktionsfähiger Virens Scanner auf SX-GATE installiert sein. Die Lizenzen für den Virens Scanner sind nicht im SX-GATE enthalten und müssen separat erworben werden. Nähere Informationen zu unterstützten oder bereits installierten Virens Scannern finden Sie im Menü "Module > Virens Scanner". Dort ist auch die Installation von Virens Scannern vorzunehmen.

Wird ein Virus gefunden, so wird die Mail temporär im Quarantäneverzeichnis "virusmails" gespeichert. Auf dieses kann nur der Benutzer "admin" über die Konsole, Secure-Shell oder FTP zugreifen. Handelt es sich bei dem gefundenen Virus um einen Makro-Virus oder das EICAR-Virens Scanner Testmuster, wird der Absender der E-Mail benachrichtigt.

E-Mail Nachricht bei Virenfund

Auf Wunsch wird ein Administrator per E-Mail über jeden Virenfund unterrichtet. Die Benachrichtigung enthält weitere Details zu der verseuchten E-Mail.

14.5.3-E MIME-Filter

Die in diesem Bereich angebotenen Funktionen erlauben es, E-Mails im MIME-Format zu filtern. MIME ist das übliche Format, wenn es darum geht E-Mails im HTML-Format oder mit Dateianhängen zu versenden.



Das automatische Verändern von E-Mails kann durch Vorschriften oder Gesetze mit bestimmten Auflagen verbunden oder sogar verboten sein.

Manche der Optionen unterscheiden zwischen eingehenden und ausgehenden E-Mails. Um als ausgehende E-Mail zu gelten, muss die IP-Adresse von der SX-GATE die E-Mail empfängt unter "Lokale IP-Adressen" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" hinterlegt sein. Authentifiziert angelieferte E-Mails gelten ebenfalls als lokal.



Auf SX-GATE System-Mails wird keine der Filter-Optionen angewandt.

Dateianhangs-Filter

Aktivieren Sie diese Option um in E-Mails nach unerwünschten Dateianhängen zu suchen. Ausgehende E-Mails mit unerwünschten Anhängen werden zurückgewiesen.

Bei eingehenden E-Mails ist dies ebenfalls möglich, meist kommt hier jedoch ein Quarantäne-Verfahren zum Einsatz. Die beanstandeten Anhänge werden dabei temporär in einem Quarantänebereich gespeichert, auf den Sie über das Menü "Monitoring > Mail-Server" zugreifen können. Die Anhänge werden nach jedem Signatur-Update der installierten Virens Scanner erneut auf Viren geprüft. Einträge in der Quarantäne werden automatisch und ohne weitere Benachrichtigung gelöscht, wenn die weiter unten konfigurierte "Aufbewahrungszeit" überschritten ist.

Wir empfehlen die Aktivierung dieses Filters als Ergänzung zum Virens Scanner. Ein Virens Scanner erkennt nur entweder bereits bekannte Viren oder Viren die aufgrund bestimmter Vorgehensmuster identifiziert werden können. Die Filterung bestimmter Dateianhänge kann daher die Sicherheit erhöhen.

nur eingehende E-Mails

Aktivieren Sie diese Option, wenn nur in eingehenden E-Mails nach Dateianhängen mit unerwünschten Dateinamens-Endungen gesucht werden soll.

ein- und ausgehende E-Mails

Bei Auswahl dieser Einstellung wird jede E-Mail, die den SX-GATE Mail-Server passiert, gefiltert. Während das Verhalten des Filters für eingehende E-Mails konfigurierbar ist, werden ausgehende E-Mails mit unerwünschten Anhängen grundsätzlich zurückgewiesen.

ZIP-/RAR-Archive untersuchen

Ist dieser Schalter aktiviert, so wird auch in angehängten ZIP- und RAR-Archiven nach Dateien mit unerwünschten Endungen gesucht. Enthält das Archiv mindestens eine gesperrte Datei oder nicht ausschließlich erlaubte Dateien, so gilt das gesamte Archiv als unerwünscht.



Andere Archiv-Formate als ZIP und RAR werden durch diese Funktion nicht unterstützt. Die Suche ist nicht rekursiv. Archive innerhalb von Archiven werden also nicht untersucht.

TNEF-Datei (winmail.dat) untersuchen

Ist dieser Schalter aktiviert, so wird auch in TNEF-Datei (winmail.dat) nach Dateien mit unerwünschten Endungen gesucht. Enthält die Datei mindestens eine gesperrte Datei oder nicht ausschließlich erlaubte Dateien, so gilt die gesamte TNEF-Datei als unerwünscht.



Andere Datei-Formate als TNEF werden durch diese Funktion nicht unterstützt. Die Suche ist nicht rekursiv. TNEF-Dateien innerhalb von TNEF-Dateien werden also nicht untersucht.



Falls die "Quarantäne-Modus für eingehende E-Mails" auf "Anhang entfernen" steht wird trotzdem die E-mail komplett zurückgehalten.

Quarantäne-Modus für eingehende E-Mails

Legen Sie hier fest, wie mit E-Mails verfahren werden soll, die unerwünschte Dateianhänge enthalten.

Sofern eines der Quarantäne-Verfahren gewählt wird, kann ein Administrator die beanstandeten Anhänge im Menü "Monitoring > Mail-Server" inspizieren und jederzeit an die Empfänger weiterleiten. Über die Option "Benutzerzugriff auf Quarantäne" kann den Empfängern zusätzlich die Möglichkeit eingeräumt werden, über einen Link auf die Quarantäne zuzugreifen, sofern bestimmte Voraussetzungen erfüllt sind.

Anhang entfernen

In dieser Einstellung werden alle beanstandeten Anhänge in der E-Mail durch einen entsprechenden Hinweistext ersetzt. Die modifizierte E-Mail wird dann an die Empfänger ausgeliefert.

Der Vorteil dieser Variante ist, dass die Empfänger sofort soviel von der ursprünglichen E-Mail wie möglich erhalten. Für den Administrator wird diese Option hingegen aufwändiger, falls er regelmäßig Anhänge aus der Quarantäne holen und an die Empfänger weiterleiten muss. Die Anhänge müssen nämlich einzeln heruntergeladen und manuell an die Benutzer weitergeleitet werden.

E-Mail zurückhalten

Hier wird die komplette E-Mail zurückgehalten. Die Empfänger erhalten eine Benachrichtigungs-E-Mail.



Bei aktivierter Funktion "Quarantäne-Modus für eingehende E-Mails" gilt: Ist eine E-Mail an mehrere Empfänger gerichtet, wird über den Link die Zustellung an alle Empfänger ausgelöst.

Der Vorteil dieser Einstellung ist, dass die Signatur von signierten E-Mails nicht zerstört wird. Hinzu kommt, dass für den Administrator die Zustellung einer unter Quarantäne gestellten E-Mail in dieser Variante nur ein Klick ist.

E-Mail abweisen; keine Quarantäne

Wählen Sie diese Einstellung, um die Annahme von E-Mails mit unerwünschten Anhängen komplett zu verweigern. Weder die Empfänger noch der Administrator werden in diesem Fall benachrichtigt. Es obliegt dem zustellenden System, den Absender über die Unzustellbarkeit zu informieren.



Wir raten dringend von dieser Option ab, falls SX-GATE E-Mails per POP oder IMAP vom Mail-Server eines Providers abholt. Wird in diesem Szenario die Annahme einer Mail verweigert, sendet SX-GATE einen Unzustellbarkeitsbericht an den Absender zurück. Ist die Absender-Adresse gefälscht, betrifft dies unbeteiligte Dritte.

Markierung für den Betreff betroffener Mails

Der Betreff einer E-Mail, die zurückgehalten wurde bzw. aus der Anhänge entfernt wurden, kann auf Wunsch ein beliebiger Text vorangestellt werden (z.B. "*** VORSICHT ***" oder "[GEFILTERT]").

Benutzerzugriff auf Quarantäne

Um den Administrator zu entlasten, kann der Benutzer unter bestimmten Umständen selbständig auf die Quarantäne zugreifen. Abhängig von der Einstellung unter "Quarantäne-Modus für eingehende E-Mails" erhält er entweder einen Link um sich unter Quarantäne gestellte Anhänge herunterzuladen oder er kann über einen Link die Zustellung der unter Quarantäne gestellten E-Mail veranlassen. Beim Aufruf des Links erhält der Benutzer eine Fehlermeldung, falls in der Mail zwischenzeitlich ein Virus gefunden wurde oder die hier konfigurierten Voraussetzungen noch nicht erfüllt sind.



Die Empfänger erhalten keinen Link auf Anhänge bzw. E-Mails mit Anhängen aus der Liste "Gefährliche Dateianhänge" sowie bei Office-Dokumenten mit Makros, wenn "Office-Dokumente sind gefährlich" aktiviert ist.

nein

In dieser Einstellung erhalten die Empfänger keinen Zugriff auf die Quarantäne.

sofort

Unabhängig davon, ob der Quarantäne-Bereich in der Zwischenzeit mit aktualisierten Virens Scanner-Signaturen gescannt wurde oder nicht, kann der Empfänger jederzeit darauf zugreifen.

nach dem nächsten Virens Scanner Signatur-Update

Erst wenn der Quarantäne-Bereich mit aktualisierten Virens Scanner-Signaturen überprüft wurde, kann ein Empfänger darauf zugreifen. Der Administrator kann jederzeit über die Administrations-Oberfläche auf die Quarantäne zugreifen.



Neue Signaturen werden von den Herstellern der Virens Scanner in unregelmäßigen Zeitabständen veröffentlicht. Entscheidend ist nicht, wann SX-GATE das nächste Mal nach neuen Signaturen sucht, sondern ob tatsächlich auch neue Signaturen verfügbar sind.

nach frühestens

Zusätzlich zu einem erneuten Scan mit aktualisierten Virens Scanner-Signaturen, müssen E-Mails eine gewisse Zeit im Quarantäne-Bereich verbringen, bevor ein Empfänger Zugriff erhält. Sind mehrere Stunden eingestellt, wird die Quarantäne unter Umständen mit mehrmals aktualisierten Signaturen gescannt.

Hostname im Link

Bei aktivierter Option "Benutzerzugriff auf Quarantäne" werden HTTPS-Links per Mail verschickt, über die der Benutzer Dateien bzw. E-Mails aus der Quarantäne abrufen kann. Sie können hier den im Link verwendeten Servernamen bzw. IP-Adresse festlegen. Unter dieser Adresse muss vom Client aus der SX-GATE Reverse-Proxy erreichbar und für den Zugriff auf die Quarantäne konfiguriert sein.

E-Mail Nachricht bei Quarantäne

Auf Wunsch kann ein Administrator per Mail über jede E-Mail informiert werden, die ganz oder in Teilen unter Quarantäne gestellt wird.

Aufbewahrungszeit

Anzahl an Tagen, die Dateianhänge bzw. E-Mails im Quarantäne-Verzeichnis aufbewahrt werden sollen, bevor diese gegen Mitternacht gelöscht werden.

14.5.3-F MIME-Filter Regeln

Auf diesem Reiter (Tab) wird festgelegt, ob bzw. welche Anhänge beanstandet werden sollen. Die Prüfung erfolgt dabei in der Reihenfolge, in der die Eingabelemente angeordnet sind.

Office-Dokumente sind gefährlich

Aktivieren Sie diese Funktion, um Office-Dokumente auf Makros zu untersuchen und ggf. als gefährlich einzustufen. Die Überprüfung findet unabhängig vom Dateinamen statt. Auch Archive werden, soweit möglich, rekursiv entpackt und durchsucht. Die Liste "Vertrauenswürdige Absender" wird dabei nicht berücksichtigt.



Ein Zugriff auf Anhänge die aufgrund dieser Einstellung unter Quarantäne gestellt wurden, ist nur dem Administrator möglich.

Gefährliche Dateianhänge

Anhänge mit den hier angegebenen Dateinamenserweiterungen oder MIME-Typen werden auf jeden Fall beanstandet, selbst wenn in nachfolgenden Einstellungen Ausnahmen wie insbesondere unter "Vertrauenswürdige Absender" konfiguriert wurden. Geben Sie hier potentiell gefährliche Dateinamenserweiterungen ein.



Ein Zugriff auf Anhänge die aufgrund dieser Einstellung unter Quarantäne gestellt wurden, ist nur dem Administrator möglich.

Als Dateinamenserweiterung können Sie z.B. ".exe", ".exe" oder "*.exe" angeben. Alle drei Schreibweisen sind gleichbedeutend mit der Erweiterung ".exe". SX-GATE prüft, ob der Dateiname eines Anhangs mit einem Punkt, gefolgt von einer der hier angegebenen Erweiterungen endet. Groß- und Kleinschreibung spielt dabei keine Rolle.

Alternativ können Sie auch MIME-Typen wie z.B. "application/zip" angeben. Ein Stern dient als Platzhalter (z.B. "application/*"). Die konfigurierten MIME-Typen werden mit dem beim Dateianhang angegebenen "Content-Type" verglichen.

Vertrauenswürdige Absender

Eine Filterung gemäß der Optionen "Gefährliche Dateianhänge" und "Office-Dokumente sind gefährlich" findet in jedem Fall statt. Ansonsten dürfen die hier angegebenen Absender beliebige Dateianhänge senden. Die in den nachfolgenden Einstellungen getroffenen Einschränkungen gelten für diese Absender nicht.

Fügen Sie eine vollständige E-Mail-Adresse hinzu (z.B. benutzer@example.com), um beliebige Anhänge von dieser einen Adresse zu erlauben. Geben Sie alternativ lediglich den Domain-Teil der E-Mail-Adresse an (z.B. example.com), damit alle Adressen in dieser Domain beliebige Anhänge senden dürfen.

Office-Dokumente sind unerwünscht

Aktivieren Sie diese Funktion, um Office-Dokumente auf Makros zu untersuchen und ggf. zu beanstanden. Die Überprüfung findet unabhängig vom Dateinamen statt. Auch Archive werden, soweit möglich, rekursiv entpackt und durchsucht.

Erlaubte Dateianhänge

Diese Einstellung ist nur verfügbar, wenn "Alle übrigen Dateianhänge sind: unerwünscht" konfiguriert ist. Ausschließlich Dateianhänge mit den hier angegebenen

Endungen oder MIME-Typen dürfen passieren. Alle anderen Anhänge werden beanstandet.

Als Dateinamenserweiterung können Sie z.B. ".pdf", ".pdf" oder "*.pdf" angeben. Alle drei Schreibweisen sind gleichbedeutend mit der Erweiterung ".pdf". SX-GATE prüft, ob der Dateiname eines Anhangs mit einem Punkt, gefolgt von einer der hier angegebenen Erweiterungen endet. Groß- und Kleinschreibung spielt dabei keine Rolle.

Alternativ können Sie auch MIME-Typen wie z.B. "image/png" angeben. Ein Stern dient als Platzhalter (z.B. "image/*"). Die konfigurierten MIME-Typen werden mit dem beim Dateianhang angegebenen "Content-Type" verglichen.

Unerwünschte Dateianhänge

Diese Einstellung ist nur verfügbar, wenn "Alle übrigen Dateianhänge sind: erlaubt" konfiguriert ist. Alle Dateianhänge mit den hier angegebenen Endungen und MIME-Typen werden beanstandet. Alle anderen Anhänge werden durchgeleitet.

Als Dateinamenserweiterung können Sie z.B. ".zip", ".zip" oder "*.zip" angeben. Alle drei Schreibweisen sind gleichbedeutend mit der Erweiterung ".zip". SX-GATE prüft, ob der Dateiname eines Anhangs mit einem Punkt, gefolgt von einer der hier angegebenen Erweiterungen endet. Groß- und Kleinschreibung spielt dabei keine Rolle.

Alternativ können Sie auch MIME-Typen wie z.B. "application/zip" angeben. Ein Stern dient als Platzhalter (z.B. "application/*"). Die konfigurierten MIME-Typen werden mit dem beim Dateianhang angegebenen "Content-Type" verglichen.

Alle übrigen Dateianhänge sind

Legen Sie hier die Grundeinstellung des Filters fest.

14.5.3-G MIME-Filter Optionen

Die in diesem Bereich werden weitere MIME-Filter Einstellungen angeboten, die auch unabhängig vom Dateianhangs-Filter genutzt werden können.



Das automatische Verändern von E-Mails kann durch Vorschriften oder Gesetze mit bestimmten Auflagen verbunden oder sogar verboten sein.

Manche der Optionen unterscheiden zwischen eingehenden und ausgehenden E-Mails. Um als ausgehende E-Mail zu gelten, muss die IP-Adresse von der der SX-GATE die E-Mail empfängt unter "Lokale IP-Adressen" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" hinterlegt sein. Authentifiziert angelieferte E-Mails gelten stets als lokal.



Auf SX-GATE System-Mails wird keine der Filter-Optionen angewandt.

Signierte E-Mails nicht bearbeiten

Die Signatur einer E-Mail wird ungültig, wenn der Inhalt verändert wird. Aktivieren Sie diesen Schalter, um mit PGP oder S/MIME signierte Mails ungeprüft passieren zu lassen. Die Einstellung wirkt sich auf folgende Optionen aus:

Bei eingehenden E-Mails

"Dateianhangs-Filter" auf dem Reiter (Tab) "MIME-Filter", sofern bei der Option "Quarantäne-Modus für eingehende E-Mails" die Einstellung "Anhang entfernen" gewählt wurde.

Optionen "HTML-Nachrichten bereinigen" und "Redundante HTML-Teile entfernen" auf dieser Seite

"Von extern empfangene Mails markieren" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Empfangs-Filter".

Bei ausgehenden E-Mails

"Text-Zusatz" in der Domain-Konfiguration unter "Module > Mail-Server > Domains"



Bedenken Sie bitte, dass diese Option einem Angreifer eine einfache Möglichkeit bietet, die genannten Filter zu umgehen.

HTML-Nachrichten bereinigen

E-Mail Nachrichten im HTML-Format bieten verschiedene Möglichkeiten des Missbrauchs. Das Spektrum reicht vom Ausnutzen von Sicherheitslücken des Mailprogrammes über Web-Bugs die typischerweise SPAM-Mail-Versendern das Öffnen der SPAM-Mail melden bis zu Phishing-Mails mit deren Hilfe versucht wird an Zugangsdaten gutgläubiger Anwender zu kommen.

Diese Gefahren können mit Hilfe dieser Funktion weitgehend entschärft werden. Bedenkliche HTML-Elemente werden dazu aufgespürt und umbenannt. Die so abgeänderten Elemente sind dem Anzeigeprogramm unbekannt und können so keinen Schaden mehr anrichten. Kennern von HTML erschließt sich dennoch aus dem Quelltext der HTML-Datei das ursprüngliche Original. Bei ungewollt geänderten Dateien ist eine Rekonstruktion einfach möglich. Dazu ist jedes Vorkommen des Textes "DEFANGED_" im Dokument zu löschen.



Dieser Filter wird ausschließlich auf eingehende E-Mails angewandt.



Diese Option filtert auch Dateianhänge im HTML-Format. Verpacken Sie HTML-Dateien in Archiven um ungewollte Änderungen zu vermeiden.

aktiviert

Aktivieren Sie diese Option um HTML in E-Mails zu entschärfen. HTML-Tags die der Einbindung aktiver Komponenten dienen wie auch Formular-Elemente werden dann unschädlich gemacht. Selbiges gilt für Skript-Sprachen, unbekannte HTML-Elemente. Verweise auf externe Ressourcen die unbemerkt Aktionen auslösen, werden ebenfalls gefiltert. Das Ziel von Verweisen wird entfernt, wenn es auf aktive Komponenten verweist.

radikal

Wählen Sie diese Einstellung, um über die Maßnahmen der Option "aktiviert" hinaus grundsätzlich alle Referenzen und Ziele von Verweisen unbenutzbar zu machen.

Redundante HTML-Teile entfernen

Einige Mailprogramme können so eingestellt werden, dass die eigentliche Nachricht zweimal in der Mail enthalten ist: Einmal als reiner Text und einmal im HTML-Format. Die beiden Formate sind als alternativer Inhalt gekennzeichnet (multipart/alternative). Gemäß der Fähigkeit und Einstellung des Mailprogrammes beim Empfänger wird einer der beiden Teile beim Öffnen der E-Mail angezeigt.

Ist dieser Schalter aktiviert, so wird bei alternativen Inhalten der HTML-Teil entfernt.



Es werden nur eingehende E-Mails gefiltert. Auf E-Mails die ausschließlich im HTML-Format geschrieben sind hat diese Option keine Auswirkung.



Der entfernte HTML-Teil wird nicht im Quarantäne-Verzeichnis abgelegt, ist also unwiederbringlich verloren. Es erfolgt auch keine Benachrichtigung des Administrators.

Nutzen Sie diese Option um Bandbreite zu sparen wenn z.B. mit mobilen Endgeräten auf die Mail zugegriffen werden soll. Zudem wird der Schutz lokaler Benutzer vor unerwünschten Nebeneffekten von HTML-Mails verbessert ohne den Verlust von Information befürchten zu müssen. Bei regulären E-Mails ist grundsätzlich davon auszugehen, dass der Textinhalt in beiden Formaten identisch ist. Dies trifft insbesondere bei SPAM-Mails aber auch bei manchen Werbe-Mails nicht immer zu.



Im Text-Teil fehlen gegenüber HTML insbesondere jegliche Formatierungen wie z.B. Farben und Schriftgrößen. Ferner sind Verweise (Links) nicht anklickbar. Manche Mailprogramm verfügen jedoch über eine entsprechende Erkennungsfunktion. Weiterhin fehlen externe Ressourcen, die mit Hilfe entsprechender Verweise beim Öffnen der Mail aus dem Internet nachgeladen werden. Dies wird jedoch in der Regel nur in unseriösen E-Mails genutzt (Web-Bugs).



Bei E-Mails die durch diese Funktion verändert wurden kann sich die Erkennungsrate des SPAM-Filters verschlechtern.

14.5.3-H Relay SPAM-Filter

Unter einer SPAM-Mail versteht man eine unerwünschte Werbe-Mail mit meist dubioser Herkunft. Der SPAM-Mail-Filter versucht diese E-Mails zu erkennen und diese je nach gewählter Konfiguration zu kennzeichnen oder die Annahme zu verweigern.

Der SPAM-Mail-Filter des SX-GATE klassifiziert automatisch den Inhalt von E-Mails anhand typischer Phrasen oder anderer Merkmale die auf eine unerwünschte Werbe-Mail (SPAM-Mail) zutreffen. Dazu ist im SX-GATE eine Datenbank mit Kriterien enthalten, die mit einem Punktesystem bewertet werden. Das erreichte Punkteergebnis ermöglicht das Filtern von E-Mails. Alle Merkmale, die auf eine SPAM-Mail hindeuten, erhöhen den Punktestand, während für Merkmale die auf eine reguläre Mail hindeuten wieder Punkte abgezogen werden. Je höher das Bewertungsergebnis, umso wahrscheinlicher handelt es sich um eine SPAM-Mail.



E-Mails mit einer Größe von mehr als 1MB werden vom SPAM-Mail-Filter nicht klassifiziert um Ressourcen zu schonen. Dies stellt jedoch keine Beeinträchtigung dar, da SPAM-Mails typischerweise deutlich kleiner sind.

Jede untersuchte E-Mail wird vom SPAM-Mail-Filter um Kopfzeilen (Header) erweitert. Der "X-Spam-Status" zeigt den erreichten Punktwert (hits=...) sowie die Kurznamen der Merkmale, die zu diesem Punktestand geführt haben (tests=...). Dies ermöglicht es dem Empfänger, das Resultat des SPAM-Filters zu überprüfen. Die Kopfzeile "X-Spam-Level" enthält je ein "x" pro vollem erreichten Punkt (z.B. "X-Spam-Level: xxx" bei einer Punktezahl zwischen 3.00 und 3.99). Dieser Header ist bestens geeignet, um E-Mails im Mail-Programm des Benutzers automatisch zu sortieren.



Bei den meisten Mail-Programmen werden im Normalfall nur die wichtigsten Kopfzeilen angezeigt. Die weiteren Header sind aber in der Regel über einen entsprechenden Menüpunkt zugänglich.

Im SX-GATE kann der SPAM-Filter an zwei verschiedenen Stellen aktiviert werden: In der Benutzerverwaltung individuell je Postfach oder hier auf dem Reiter (Tab) "Relay SPAM-Filter" pauschal für alle Empfänger.



Die Einstellungen auf allen anderen Reitern zum Thema SPAM hier im Menü "Mail-Server" gelten für beide SPAM-Filter Varianten.

Leitet SX-GATE E-Mails an einen anderen (internen) Mail-Server weiter, so muss der SPAM-Filter hier im Relay-Modus aktiviert werden. Verwaltet hingegen SX-GATE die Postfächer Ihrer Domains stehen beide Alternativen zur Auswahl.



Mit Aktivierung des Relay-SPAM-Filters wird der benutzerbezogene SPAM-Filter deaktiviert.

Um den SPAM-Mail-Filter im Relay-Modus zu aktivieren, müssen Sie mindestens einen der Schwellwerte festlegen. Im Relay-Modus untersucht der SPAM-Filter jede eingehende E-Mail während sie den SX-GATE Mail-Server passiert. Dabei ist es nicht möglich, unterschiedliche Schwellwerte in Abhängigkeit des Benutzers zu definieren.



Die Unterscheidung, ob es sich um eine eingehende oder ausgehende E-Mail handelt erfolgt anhand der Quell-IP-Adresse der SMTP-Verbindung. Im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" legt der Parameter "Lokale IP-Adressen" fest, welche IP-Adressen zu internen Absendern gehören. Der Relay-SPAM-Filter ignoriert deren E-Mails. Das selbe gilt für authentifiziert eingelieferte Mails.

E-Mail als SPAM markieren bei mehr als

Überschreitet der Punktwert einer E-Mail bei deren Klassifizierung diesen Schwellwert, so wird die E-Mail als SPAM-Mail markiert. Dabei wird dem Betreff der Text "***** SPAM *****" sowie die erreichten SPAM-Bewertungspunkte vorangestellt.

Markierte E-Mails zustellen an

Anstatt als SPAM markierte E-Mails an die eigentlichen Empfänger zuzustellen, ist es mit Hilfe dieser Einstellung auch möglich, potentielle SPAM-Mails an eine bestimmte Adresse umzuleiten. Die Kopfzeile (Header) "X-Spam-Orig-To:" einer umgeleiteten E-Mail enthält in diesem Falle die Adressen der ursprünglichen Empfänger.



Das automatische Umleiten von E-Mails kann durch Gesetze oder Vorschriften mit bestimmten Auflagen verbunden oder sogar ganz verboten sein.

Annahme verweigern bei mehr als

Beim Überschreiten des hier eingestellten Schwellwerts verweigert SX-GATE's Mail-Server die Annahme der betroffenen E-Mail. Es ist in diesem Fall Aufgabe des zustellenden Systems entsprechend zu reagieren und z.B. den Absender oder einen Administrator darüber zu informieren. Wenn Sie sichergehen wollen, dass keine gewünschte E-Mail verloren geht, sollten Sie diese Option nicht aktivieren. Nutzen Sie stattdessen den Schwellwert "E-Mail als SPAM markieren bei mehr als" zusammen mit den Möglichkeiten der Mail-Client-Programme zur automatischen Sortierung von E-Mails basierend auf den Kopfzeilen.



E-Mails die durch den SX-GATE Mail-Client von POP-Servern abgeholt wurden verwirft der Mail-Client kommentarlos wenn SX-GATE's Mail-Server die Annahme aufgrund des SPAM-Filters verweigert. Es erfolgt weder eine Benachrichtigung noch lässt sich eine so gelöschte E-Mail wiederherstellen. Die E-Mail ist unwiederbringlich verloren!



Um den Verlust von wichtigen E-Mails zu vermeiden, sollten Sie bei der Konfiguration dieser Einstellung sehr vorsichtig sein. Stellen Sie lieber einen zu hohen als einen zu niedrigen Wert ein. Bitte beachten Sie, dass das automatische Löschen von E-Mails durch Vorschriften oder Gesetze mit bestimmten Auflagen verbunden oder sogar verboten sein kann.

14.5.3-I SPAM Bewertung

Die Einstellungen in diesem Bereich wirken sich nicht nur auf den Relay-SPAM-Filter aus, sondern auch auf den benutzerbezogenen SPAM-Filter, der in der Benutzerverwaltung konfiguriert wird.

Benutzerdefinierte SPAM-Regeln

Die SPAM-Prüfung kann in diesem Bereich durch eigene Regeln erweitert werden. Dazu ist zunächst festzulegen, welcher Teil der E-Mail geprüft werden soll. Wird das entsprechende Suchmuster gefunden, so wird die festgelegte Punktzahl bei der Berechnung der SPAM-Wahrscheinlichkeit verbucht.

Für folgende Bereiche kann eine SPAM-Filter-Regel definiert werden:

Betreff

Das Suchmuster wird im Betreff der E-Mail (Subject-Header) gesucht.

Absender

Hier wird der Absender (From-Header) geprüft.

Empfänger

In dieser Einstellung wird der Empfänger (To-Header) ausgewertet.

Kopfzeilen

Hiermit können beliebige Kopfzeilen (Header) ausgewertet werden.

Text

Diese Option bietet die Möglichkeit, den Nachrichten-Text einschließlich des Betreffs zu durchsuchen, also den eigentlichen Inhalt der Mail.

HTML Quelltext

Wie vor, jedoch bei E-Mails im HTML-Format inklusive der HTML-Tags.

Web-Adressen

Prüft Web-Adressen, die als Text oder als HTML-Link im Betreff oder im Text der Nachricht gefunden werden.

Regel

Diese Einstellung unterscheidet sich von den vorherigen. Sie ermöglicht es, die im SX-GATE vordefinierten Regelsätze neu zu bewerten. Entsprechend wird hier auch kein Suchmuster angegeben, sondern die interne ID der Regel. Die ID zusammen mit der ursprünglichen Bewertung ist jeweils in der Inhalts-Analyse von E-Mails enthalten, die als SPAM markiert wurden (z.B. "HTML_MESSAGE" oder "FORGED_MUA_OUTLOOK").



Bei Aktualisierung der vordefinierten Regelsätze können sich einzelne ID's ändern. Es erfolgt dabei keine Anpassung der hier angegebenen Regeln.

Bei der Angabe eines Suchmusters ("Kriterium") wird die Groß- und Kleinschreibung grundsätzlich nicht beachtet. Beginnt bzw. endet das Suchmuster mit einem Buchstaben oder einer Ziffer, muss das Suchmuster am Beginn bzw. Ende eines Wortes stehen. Das Suchmuster "all" liefert folglich bei "Hallo" keinen Treffer, bei "Das All!" hingegen schon.

Bestimmte Zeichen haben eine Sonderbedeutung:

*** (Stern)**

Steht für eine Folge beliebiger Zeichen. Diese kann auch komplett fehlen, also sozusagen aus 0 Zeichen bestehen. Das Suchen nach beliebigen Zeichenketten in beliebiger Länge erhöht den Ressourcen-Bedarf deutlich. Von daher trifft ein Stern maximal auf eine Kette aus 30 Zeichen zu. Das Suchmuster "a*d" findet so z.B. "ad", "a_d" und "abcd". Nutzen Sie den Stern auch, um Zeichenketten innerhalb eines Wortes zu suchen. So liefert das Suchmuster "*all*" bei "Hallo" einen Treffer.

? (Fragezeichen)

Dies steht für genau ein beliebiges Zeichen. Wird beispielsweise "a?d" angegeben, so ist "a_d" ein Treffer. Nicht gefunden wird "ad" oder "abcd".

_ (Unterstrich)

Der Unterstrich steht für eine beliebige Anzahl sogenannter "Whitespace-Character". Dies umfasst Leerzeichen, Tabulatoren und Zeilenumbrüche. Im Beispiel findet "a_d" zwar "a d", nicht jedoch "ad" oder "a_d".

Behalten Sie bitte bei der Auswahl des zugeordneten Punktwertes die eingestellten Schwellwerte im Auge. Wählen Sie für Kriterien die auf eine SPAM-Mail hindeuten einen positiven Wert. Ein negativer Wert verringert die Wahrscheinlichkeit, dass eine E-Mail als SPAM klassifiziert wird.

SPAM-Filter umgehen für folgende Absenderadressen und -domains

Der SPAM-Mail-Filter erreicht bei der automatischen Klassifizierung von E-Mails selbstverständlich kein 100% richtige Trefferquote. Um fälschlicherweise als SPAM identifizierte E-Mails zukünftig zu schützen, lässt sich hier eine Liste von einzelnen Absenderadressen hinterlegen, die den SPAM-Filter passieren dürfen. Passt der Absender einer eingehenden E-Mail zu einem Eintrag in dieser Liste, so erhält die E-Mail einen Abzug von 100 Punkten auf die automatische SPAM-Bewertung und wird so nicht von den Schwellwerten abgefangen.

Fügen Sie eine vollständige E-Mail-Adresse hinzu (z.B. benutzer@example.com), um E-Mails von dieser Adresse zukünftig nicht auszufiltern. Geben Sie alternativ lediglich den Domain-Teil der E-Mail-Adresse an (z.B. example.com), damit alle Adressen in dieser Domain den SPAM-Filter passieren dürfen.

14.5.3-J SPAM Module

Die Einstellungen in diesem Bereich wirken sich nicht nur auf den Relay-SPAM-Filter aus, sondern auch auf den benutzerbezogenen SPAM-Filter, der in der Benutzerverwaltung konfiguriert wird.

DNS basierende Listen

Im Internet stehen schwarze Listen (RBL: Realtime Black Lists) zur Verfügung, in denen die Mail-Server verzeichnet sind, von denen häufig SPAM-Mails versendet werden. Eine andere Form schwarzer Listen enthält die Adressen von Web-Servern, die oft

mit Hilfe von SPAM-Mails beworben werden (URIBL: URI Black Lists). Das Ziel von Verweisen (Links) im Text von E-Mails wird gegen URL Black Lists geprüft. Darüber hinaus gibt es auch weiße Listen, in denen unauffällige Mail-Server verzeichnet sind.

Bei der Analyse einer Mail kann eine Reihe dieser Listen befragt werden. Jeder einzelne Treffer wird dabei jedoch nur mit einem relativ geringen Punktwert berücksichtigt. Nur wenn mehrere der Listen potentiellen SPAM melden, ist deren Einfluss signifikant. Je nachdem wie die Einträge in den Listen gewonnen wurden, unterscheidet sich deren Verlässlichkeit. Wählen Sie aus den folgenden Optionen die gewünschte Stufe aus.

wenige

Wählen Sie diese Einstellung, wenn nur ausreichend sichere SPAM-Quellen in die Bewertung einfließen sollen. Insbesondere automatisch erzeugte Listen werden hier nicht berücksichtigt. Die URI Black Lists sind aktiviert.

mittel

Zusätzlich zu sicheren SPAM-Quellen beinhaltet diese Stufe auch solche Adressen, die mit Hilfe automatischer SPAM-Fallen gewonnen wurden.

viele

Ist diese Option ausgewählt, so fließen zusätzlich bekannte dynamische IP-Adressen in die Bewertung ein.

Razor2 verteiltes Spamfilter Netzwerk

Bei dieser Option wird eine unscharfe Prüfsumme über Teile der E-Mail gebildet und mittels eines eigenen Protokolls (TCP-Port 2703) an Razor2-Server im Internet übermittelt. Diese stellen eine Datenbank mit Prüfsummen bekannter SPAM-Mails zur Verfügung. Im Falle einer Übereinstimmung erhält die SPAM-Bewertung der E-Mail einen Aufschlag. Die Höhe dieses Aufschlags richtet sich nach der Vertrauenswürdigkeit der Instanzen, die dem Razor-System die SPAM-Mail gemeldet haben.



Aktivieren Sie diese Option nicht, wenn Sie über eine teure Wählleitung an das Internet angebunden sind. Für jede E-Mail wird die Razor2-Prüfsumme in das Internet gesendet, selbst für interne E-Mails. Dies kann zu sehr hohen Online-Zeiten mit entsprechenden Kosten führen.

Bayes-Filter aktivieren

Wenn aktiviert, lernt der SPAM-Mail-Filter während des Bearbeitens eingehender E-Mails eigenständig Eigenschaften hinzu, die auf ungewollte Mails (SPAM) bzw. auf

gewollte Mails (HAM) hindeuten. Dabei werden E-Mails mit mehr als 10 bzw. mit 0 oder weniger Bewertungspunkten berücksichtigt.



Der Bayes-Filter wird erst dann in die Bewertung einbezogen, wenn mind. 200 SPAM-Mails und mind. 200 HAM-Mails eingelernt wurden.

Zudem können nicht erkannte SPAM-Mails sowie fälschlicherweise als SPAM markierte E-Mails gezielt eingelernt werden. Voraussetzung dafür ist ein Benutzerkonto auf SX-GATE mit Mail-Berechtigung (Gruppe system-mail). Der Zugriff auf dieses Konto muss mit IMAP oder mit Hilfe der SX-GATE Groupware erfolgen.



Es empfiehlt sich, in der Benutzerkonfiguration die Option zu aktivieren, alle als SPAM markierten Mails im Ordner "SPAM" abzulegen. Der Ordner wird bei Bedarf automatisch angelegt.

Beim Zugriff über IMAP müssen spezielle Mail-Ordner angelegt werden. In den Ordner "SPAM" verschieben Sie bitte nicht erkannte SPAM-Mails. Eine Kopie von fälschlicherweise als SPAM markierten E-Mails kann im Ordner "HAM" abgelegt werden.

Täglich kurz nach Mitternacht wird eine Übersicht des Inhalts dieser Ordner per Mail an den zugehörigen Benutzer gesendet. Zu diesem Zeitpunkt erfolgt bei aktiviertem Bayes-Filter auch das Einlernen. In der Benutzerverwaltung wird je Benutzer konfiguriert, nach wieviel Tagen E-Mails aus diesen Ordnern automatisch gelöscht werden.

Texterkennung für Bilder

Manche SPAM-Mails versenden ihre Botschaften in Bildern. Damit soll verhindert werden, dass die Mail mit herkömmlicher Textanalyse als SPAM-Mail entlarvt wird. Mit der Texterkennung (OCR) wird versucht, Text in Bildern zu identifizieren. Werden typische SPAM-Mail Worte in einer E-Mail gefunden, so wird deren SPAM-Bewertung um einen feste Grundwert und einen Aufschlag je verdächtigem Wort erhöht.



Um das System zu entlasten, wird die Texterkennung nicht durchgeführt, wenn eine Mail bereits über andere Verfahren eine ausreichend hohe SPAM-Bewertung erreicht hat.

Englischsprachige E-Mails sind potentiell SPAM

Der größte Teil aller SPAM-Mails sind in englischer Sprache verfasst. Ist dieser Schalter aktiviert, so erhalten alle englischsprachigen E-Mails einen Aufschlag auf die SPAM-Bewertung. Die Wahrscheinlichkeit, dass die SPAM-Bewertung einer

englischen E-Mail den konfigurierten SPAM-Filter-Schwellwert erreicht wird dadurch deutlich erhöht.



Nutzen Sie "Benutzerdefinierte SPAM-Regeln" um die Bewertung dieser Einstellung zu ändern. In der Benutzerverwaltung ist dies sogar für einzelne lokale Konten möglich. Die ID der Regel lautet "UNWANTED_LANGUAGE_BODY".



Da diese Einstellung für alle Benutzer gilt, sollte diese doch recht drastische Maßnahme mit allen Betroffenen abgesprochen werden.

Mails mit Fernost-Zeichensatz sind potentiell SPAM

E-Mails für deren Darstellung Zeichensätze aus Japan, Korea, Thailand und China erforderlich sind, erhalten bei Aktivierung dieses Schalters einen deutlichen Aufschlag auf die SPAM-Bewertung.

Mails mit Kyrillischem Zeichensatz sind potentiell SPAM

E-Mails in kyrillischer Schrift, erhalten bei Aktivierung dieses Schalters einen deutlichen Aufschlag auf die SPAM-Bewertung.

14.5.3-K SPAM Einstellungen

Die Einstellungen in diesem Bereich wirken sich nicht nur auf den Relay-SPAM-Filter aus, sondern auch auf den benutzerbezogenen SPAM-Filter, der in der Benutzerverwaltung konfiguriert wird.

Originalinhalt erkannter SPAM-Mails

Mit diesem Parameter können Sie beeinflussen, in welcher Form der Inhalt einer als SPAM markierte E-Mail weitergeleitet wird. In jedem Fall wird dem Betreff der E-Mail der Text "*****SPAM*****" und die erzielten Bewertungs-Punkte vorangestellt.

als Anhang zuordnen

In dieser Einstellung enthält die E-Mail eine Vorschau auf den Original-Inhalt sowie eine Aufschlüsselung der Bewertungs-Punkte. Der Original-Inhalt der SPAM-Mail ist als Anhang zugeordnet.

Durch die Verschiebung der ursprünglichen Mail in den Anhang soll verhindert werden, dass das bloße Anklicken der E-Mail bereits unerwünschte Aktionen auslöst. In Abhängigkeit vom verwendeten Mail-Programm genügt eventuell bereits das Auswählen einer E-Mail, um durch die Vorschaufunktion z.B. Bilder zu

einer mit HTML formatierten Mail aus dem Internet nachzuladen. Der Versender der SPAM-Mail erhält so unbemerkt Rückmeldung darüber, dass die SPAM-Mail geöffnet wurde. Als Folge davon wird die E-Mail-Adresse als lohnendes Ziel für weitere SPAM-Mails registriert, was sich auf Dauer zu einer wahren Flut von SPAM-Mails entwickeln kann.

unverändert weiterleiten

Hier wird der Inhalt im Original weitergeleitet. Details über die Zusammensetzung der Bewertungs-Punkte sind in den Kopfzeilen (Header) der Mail zu finden.

Immer ausführlichen Report anfügen

Ist diese Option aktiviert, wird auch E-Mails die nicht als SPAM klassifiziert wurden eine ausführliche Aufschlüsselung der erhaltenen SPAM-Bewertungs-Punkte hinzugefügt. Zu finden ist diese Auswertung als Kopfzeile (Header) "X-Spam-Report".

E-Mail-Adresse des SPAM-Administrators

Geben Sie hier die Adresse des SPAM-Filter-Administrators an. Diese wird dem Benutzer in E-Mails angezeigt, die als SPAM markiert wurden.

14.5.4 Archivierung

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.5.4-A Allgemein.....	531
14.5.4-B Benutzer.....	532
14.5.4-C Mail-Zuführung.....	534
14.5.4-D Speichermedien.....	536
14.5.4-E Zeitstempel.....	537
14.5.4-F Backup.....	538
14.5.4-G Werkzeuge.....	539

Die Mail-Archivierung kann im Menü "System > Apps" nachinstalliert werden. Es handelt sich um eine kostenpflichtige Erweiterung.

Die Archivierung speichert Mails in verschlüsselter Form auf einer Netzwerkfreigabe und stellt eine Suchmaske zur Verfügung, über die per Web-Browser E-Mails im Archiv gesucht, aufgerufen und heruntergeladen werden können.

14.5.4-A Allgemein

Vier-Augen-Login für Auditoren

Wenn aktiviert, muss bei jeder Anmeldung der speziellen Benutzer "auditor" oder "revisor" zur Bestätigung zusätzlich das Kennwort des Benutzers "admin" eingegeben werden.

Löschfunktion für Auditoren

In bestimmten Situationen kann es notwendig sein, E-Mails vorzeitig aus dem Archiv zu löschen.

deaktiviert

Manuelles Löschen ist deaktiviert. Mails werden ausschließlich nach Ablauf der Archivierungsfrist gelöscht.

nach Zustimmung

In dieser Einstellung muss der Löschwunsch durch den speziellen Benutzer "dataofficer" bestätigt oder abgelehnt werden.

aktiviert

Wählen Sie diese Einstellung, wenn Auditoren E-Mails ohne weiteres löschen dürfen.

Ablage in Unterordner

Mit Hilfe dieser Option ist eine benutzerübergreifende Strukturierung des Mailbestands möglich. In der Administrations-Oberfläche der Archivierungs-App kann der "admin" Ordner anlegen und per Regelwerk neu ankommende Mails automatisiert auf Ordner verteilen. Zudem kann der "admin" einzelnen Benutzern die Berechtigung geben, manuell Mails in bestimmte Ordner zu verschieben. Während der "auditor" dieses Recht grundsätzlich für alle Ordner hat, kann der "revisor" wahlweise entweder unbeschränkt mit allen Ordnern arbeiten oder darf ausschließlich auf Mails in ausgewählten Ordnern zugreifen. So ließe sich z.B. der Zugriff eines Steuerprüfers auf Ordner mit steuerlich relevanten Mails begrenzen.

Standard-Archivierungsdauer

Neu ankommende Mails werden nach der hier konfigurierten Anzahl von Tagen automatisch gelöscht. In der Administrations-Oberfläche der Archivierungs-App kann der "admin" Regeln konfigurieren, um Mails von der Archivierung auszunehmen oder mit abweichender Archivierungsdauer zu speichern, so dass z.B. Bewerbungen gar nicht erst archiviert oder schon nach wenigen Wochen gelöscht werden.



Eine Änderung dieses Wertes wirkt sich nicht auf bereits archivierte Mails aus.

Kopfzeile mit zusätzlicher Empfänger-Adresse

Insbesondere wenn Mail von einem POP- oder IMAP-Server abgeholt werden, steht die eigentliche Empfänger-Adresse aus der SMTP-Kommunikation (Envelope-Recipient) oft nicht mehr zur Verfügung. Mit etwas Glück wurde die Adresse jedoch in einem Header wie z.B. "X-Envelope-To:" hinterlegt. Konfigurieren Sie hier bei Bedarf bitte den Namen des Headers.



Eine Änderung dieses Wertes wirkt sich nicht auf bereits archivierte Mails aus.

Kopfzeile, die SPAM-Mails kennzeichnet

Beginnt eine Kopfzeile einer zu archivierenden Mail mit dem hier konfigurierten Wert, wird die Mail im Archiv als SPAM-Mail markiert.



Eine Änderung dieses Wertes wirkt sich nicht auf bereits archivierte Mails aus.

Archiv versendet Mails über Mail-Server

Benutzer können sich aus dem Archiv heraus archivierte Mails zusenden lassen. Der Versand erfolgt über den hier konfigurierten Mail-Server.

SMTP-Auth Benutzername

Falls für den Versand über den Mail-Server eine Benutzeranmeldung erforderlich ist, können Sie hier die benötigten Daten eingeben. Andernfalls kann das Eingabefeld leer bleiben.

14.5.4-B Benutzer

Benutzerverwaltung

Legen Sie hier bitte fest, wie die Verwaltung von Benutzern und Gruppen in der Mail-Archivierung erfolgen soll.



Bei nachträglicher Umstellung zwischen "SX-GATE Benutzerverwaltung" und einer der anderen Option - egal in welcher Richtung - gehen alle benutzer- und gruppenbezogenen Einstellungen sowie Notizen und Kategorisierungen im Archiv verloren!

Benutzerverwaltung der App

In diesen Einstellungen werden Benutzer und Gruppen vom "admin" über die Administrations-Oberfläche der Archivierungs-App gepflegt. Diese Variante bietet maximale Flexibilität zum Preis einer redundanten Benutzerverwaltung.

SX-GATE Benutzerverwaltung

Wählen Sie diese Option, wenn SX-GATE zugleich Ihr Mail-Server ist, also die E-Mail-Postfächer und somit auch die Benutzer auf dem SX-GATE bereits angelegt sind. Die Benutzer und Gruppen sind dann automatisch auch in der Archivierungs-App verfügbar.



Beim nachträglichen Umstellen auf oder von dieser Variante gehen alle benutzer- und gruppenbezogenen Einstellungen sowie Notizen und Kategorisierungen im Archiv verloren!

Microsoft Exchange (Active-Directory)

Fungiert ein lokaler Exchange-Server als Mail-Server, empfiehlt sich diese Einstellung.



Konfigurieren Sie die LDAP-Anbindung an das Active-Directory im Menü "System > Benutzerverwaltung > Einstellungen".

Passwort für "auditor" zurücksetzen

Der Login "auditor" ist der spezielle Zugang, für den für die Inhalte des Archivs verantwortlichen Mitarbeiter mit unbeschränktem Zugriff auf alle E-Mails.

Passwort für "revisor" zurücksetzen

Der "revisor" ist als Zugang für einen externen Prüfer gedacht. In den Einstellungen der Administrations-Oberfläche der App kann der "admin" festlegen, ob der Benutzer uneingeschränkter Zugriff auf alle E-Mails erhält oder nur Mails einer bestimmten Domain oder in bestimmten Ordnern sehen darf.

Passwort für "dataofficer" zurücksetzen

Dieser Benutzer wird nur dann benötigt, wenn die Löschfunktion nach Zustimmung aktiviert ist. In diesem Fall muss der "dataofficer" zustimmen, wenn "auditor" oder "revisor" die Löschung einer Mail beantragen.

14.5.4-C Mail-Zuführung

Archivierung durch SX-GATE Mail-Server

Wir empfehlen, nach Möglichkeit dies Art der Archivierung zu nutzen. In dieser Einstellung werden die Mails archiviert, während sie vom SX-GATE Mail-Server verarbeitet werden.



Um Mails zu archivieren, die nicht über den SX-GATE Mail-Server geschickt werden, sind zusätzliche oder alternative Methoden vorzusehen. Das betrifft insbesondere interne Mails, wenn gehostete oder interne Mail-Server zum Einsatz kommen.

In dieser Variante werden die Mails in einem dem Exchange Journal ähnlichen Format gespeichert. Vorteil dieses Verfahrens ist, dass auch die sog. Envelope-Empfänger berücksichtigt werden, wie sie z.B. bei E-Mails in Blindkopie (Bcc) vorkommen.

Beim Einsatz des SX-GATE S/MIME-Gateways werden eingehende Mails vor der Archivierung entschlüsselt. Ausgehende Mails werden vor dem Verschlüsseln archiviert.

Ansonsten werden die Mails inhaltlich unmittelbar nach der Virenprüfung extrahiert und im Original archiviert. Insbesondere sind Änderungen, die durch den SX-GATE MIME- oder SPAM-Filter vorgenommen werden, nicht in der archivierten Mail enthalten. Gleichwohl können Mails im Archiv als SPAM gekennzeichnet werden, die der Relay-SPAM-Filter als SPAM markiert. Mails, die der MIME-Filter im Quarantäne-Verzeichnis zurückhält, werden erst nach Freigabe archiviert. Vom MIME- oder SPAM-Filter abgewiesene Mails werden nicht archiviert.



Der benutzerspezifische SPAM-Filter wird erst nach der Archivierung aufgerufen. Die Mail wird also archiviert, auch wenn der SPAM-Filter sie anschließend verwirft. Auch eine Kennzeichnung als SPAM findet im Archiv nicht statt. Aktivieren Sie anstelle des benutzerspezifischen SPAM-Filters daher bitte den Relay-SPAM-Filter Ihres SX-GATES.

Archivierung über Mail an Domain

Mails an die hier konfigurierte Domain werden vom SX-GATE Mail-Server an das Archiv zugestellt. Was vor dem @-Zeichen steht, spielt dabei keine Rolle. Verwenden Sie einen beliebigen Wert. Nutzen Sie diese Funktion z.B. in Kombination mit der Journal-Funktion von Microsoft Exchange Servern.

Archivierung über DNAT-Regel in Firewall

Während bei den zuvor genannten Methoden die Mail über den SX-GATE Mail-Server an das Archiv übermittelt wurden, können Sie mit Hilfe der passenden Firewall-Regel auch direkt mit dem SMTP-Server des Archivs kommunizieren. Legen Sie bitte manuell eine DNAT-Regel an, die die Verbindung an die hier angegebene Adresse weiterleitet.



Es wird dringend davon abgeraten, den SMTP-Server des Archivs für beliebige Internet-Adressen erreichbar zu machen!

Zur Archivierung erforderliche Kopfzeile

Wenn Sie hier den Namen und den Wert eines Mail-Headers eintragen, werden per SMTP zugestellte E-Mails nur dann archiviert, wenn sie eine Kopfzeile enthalten, die genau mit diesem Wert beginnt. Dies dient als zusätzlicher Schutz, wenn der SMTP-Dienst des Archivs auch aus wenig vertrauenswürdigen Netzen adressiert werden kann.



Achten Sie sowohl beim Namen als auch beim Wert des Mail-Headers auf die Groß- und Kleinschreibung.



E-Mails ohne diesen Header werden vom Archiv verworfen und nicht archiviert.

Bei E-Mails aus Microsoft 365 können Sie z.B. anhand der Default-Domain filtern: "X-OriginatorOrg: ...".

Schlüssel/Zertifikat für STARTTLS auswählen

Bei der Archivierung über DNAT-Regel kann die Verbindung mit STARTTLS verschlüsselt werden. Wählen Sie dazu einen der Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.

14.5.4-D Speichermedien

Zum Archiv gehören die verschlüsselten E-Mails, eine Datenbank mit den Meta-Daten und der Suchindex. Legen Sie hier fest, auf welchen Medien die verschlüsselten E-Mails und das Backup der Datenbank gespeichert werden.



Wir empfehlen die Speicherung auf einem separaten Speichergerät (z.B. NAS).



Stellen Sie sicher, dass regelmäßig ein Backup der auf den Speichermedien gesicherten Daten angefertigt wird.

Speichermedien

Konfigurieren Sie hier die Speichermedien. Geht der Speicherplatz aus, können Sie weitere Medien hinzufügen. Ist ein Medium vorübergehend nicht verfügbar, können Sie es deaktivieren.



Löschen Sie niemals ein Medium aus der Liste, wenn darauf E-Mails archiviert wurden oder wenn es ein Medium mit höherer ID gibt, auf dem E-Mails archiviert wurden.



Kontaktieren Sie den technischen Support, wenn Sie den Mailbestand mehrerer Medien auf einem Medium zusammenführen wollen.

Das spezielle Speichermedium "lokal (nur zu Testzwecken)" ist für Tests gedacht. Die Daten werden dabei im Gerät gespeichert, wobei der verfügbare Speicherplatz eher begrenzt ist.



Wenn die Archivierungs-App gelöscht wird, gehen alle auf diesem Medium gespeicherten Mails und Datenbank-Backups verloren.

Schreibe auf Speicher

Sofern mehrere Speichermedien definiert sind, wählen Sie hier das Medium aus, auf dem neue Mails archiviert werden sollen und auf dem auch das Datenbank-Backup gespeichert wird.

14.5.4-E Zeitstempel

Gesetzliche Vorgaben zur Archivierung beinhalten in der Regel auch die Pflicht nachzuweisen, dass die archivierten Dokumente nicht verändert wurden. Im SX-GATE wird dazu ein Zeitstempel-Dienst genutzt.

Grundsätzlich wird zu jeder archivierten Mail eine Prüfsumme in der Datenbank gespeichert, mit deren Hilfe die Integrität der jeweiligen Mail verifiziert werden kann. Um nun aber zusätzlich den Beweis führen zu können, dass auch die Datenbank nicht manipuliert wurde, wird ein externes Testat in Form des Zeitstempel-Dienstes benötigt. Dabei wird aus den Prüfsummen mehrerer Mails eine weitere Prüfsumme gebildet, die dann vom Zeitstempel-Dienst signiert wird.



Häufig ist die Nutzung spezieller akkreditierter Zeitstempel-Dienste vorgeschrieben.

Zeitintervall für Zeitstempel

Zeitstempel für neu archivierte Mails werden im hier konfigurierten Zeitintervall abgerufen. Zusätzlich wird alle 15 Minuten ein neuer Zeitstempel für jeweils 10000 Mails angefordert, wenn mehr als 10000 Mails auf einen Zeitstempel warten.

URL des Zeitstempel-Dienstes

Geben Sie hier bitte die URL des aktuell genutzten Zeitstempel-Dienstes an (z.B. "http://tsa.example.com/" oder "https://ca.example.com/tsa/").

Benutzername

Sofern für die Nutzung des Zeitstempeldienstes eine Anmeldung mit Benutzername und Passwort erforderlich ist, geben Sie hier bitte die Zugangsdaten an. Lassen Sie die Eingabefelder leer, wenn keine Anmeldung erforderlich ist.

CA-Zertifikate aller bisher genutzten Zeitstempel-Dienste

Die Zeitstempel werden mit Hilfe der hier eingetragenen CA-Zertifikate verifiziert. Bei der Anzeige von E-Mails im Archiv, die noch keinen Zeitstempel erhalten haben, wird ein Fehler bei der Verifikation gemeldet. Ist die Liste leer, werden Zeitstempel nicht überprüft.



CAs verwenden in der Regel eigene Stammzertifikate für den Zeitstempeldienst, die nicht in den "üblichen" Zertifikats-Bündeln enthalten sind. Importieren Sie das benötigte Stammzertifikat daher bitte zunächst im Menü "System > Zertifikatsverwaltung > CA Zertifikate".

Zeitstempel-Konfiguration testen

Der Test ruft einen Zeitstempel von der konfigurierten URL ab und versucht das Ergebnis mit Hilfe der konfigurierten CAs zu verifizieren.

14.5.4-F Backup

Um das Archiv wieder herstellen zu können, müssen folgende Komponenten gesichert werden:

Archiv-Schlüssel

Backup kann auf dieser Seite erstellt werden

Datenbank mit den Meta-Daten

Aktivieren Sie das regelmäßige automatische Backup auf dieser Seite. Das Backup wird auf dem gerade aktiven Speichermedium abgelegt.

Speichermedien mit den verschlüsselten E-Mails und dem Datenbank-Backup

Nutzen Sie externe Werkzeuge um die Daten zu sichern. Um verteilte oder intern gespeicherte Daten einem externen Werkzeug zugänglich zu machen, kann SX-GATE eine Spiegelkopie aller Speichermedien auf einer Netzwerkfreigabe ablegen



Der Suchindex wird nicht gesichert und muss im Falle eines Datenverlustes neu aufgebaut werden.

Backup des Archivschlüssels erstellen

Hier haben Sie die Möglichkeit, ein Backup des Archiv-Schlüssels zu erstellen. Sollte dieser Schlüssel einmal verloren gehen, kann das Archiv nicht mehr gelesen werden. Gerät der Schlüssel oder dessen Backup in falsche Hände, können damit die verschlüsselt gespeicherten Mails und das Datenbank-Backup ausgelesen werden.



Der Archiv-Schlüssel ist weder Bestandteil der regulären SX-GATE-Backups, noch ist er im Datenbank-Backup oder einem anderen Backup enthalten.

Automatisches Backup der Datenbank

Auf dem aktiven Medium wird im Verzeichnis "database" für jedes vollständige Backup ein Unterverzeichnis erstellt. Darin werden das vollständige Backup sowie zugehörige inkrementelle Backups abgelegt.



Das Unterverzeichnis eines vollständigen Backups wird automatisch vom aktiven Medium gelöscht, wenn es älter als sieben Tage ist und mindestens zwei neuere Unterverzeichnisse mit vollständigen Backups existieren.

Inklusive Spiegelung des Archivs und des Datenbank-Backups auf Windows-Freigabe

Aktivieren Sie diese Option, um die verschlüsselten Mails aller Speichermedien samt Datenbank-Backups auf eine Netzwerkfreigabe zu spiegeln. Die Spiegelung wird im Rahmen des automatischen Datenbank-Backups durchgeführt. Sie können die Spiegelung aber auch manuell auslösen.



Nutzen Sie ein externes Werkzeug um den Spiegel regelmäßig zu sichern.

Jetzt ein Backup der Datenbank erstellen

Erstellt ein inkrementelles Backup der Datenbank. Ist kein vollständiges Backup auf dem aktiven Medium vorhanden, wird stattdessen ein vollständiges Backup erstellt.

Jetzt ein Backup des Archivs und des Datenbank-Backups erstellen

Spiegelt den Mailbestand und die Datenbank-Backups aller Speichermedien auf die konfigurierte Netzwerkfreigabe.

14.5.4-G Werkzeuge

Index aktualisieren

Der Suchindex wird automatisch alle 30 Minuten aktualisiert. Aktualisieren Sie den Index, um vor kurzem eingetroffene Mails sofort im Archiv zu finden.

Index neu erstellen

Mit dieser Funktion wird der Suchindex neu aufgebaut. Dazu müssen alle gespeicherten Mails eingelesen werden.

E-Mails von einem POP3-/IMAP4-Server importieren

Nutzen Sie diese Funktion um einmalig E-Mails von einem POP- oder IMAP-Server zu importieren.

E-Mails von einem Speichermedium importieren

Nutzen Sie diese Funktion um einmalig E-Mails von einem der Speichermedien zu importieren. Die Mails müssen auf dem Medium im Verzeichnis "import" abgelegt werden und im eml-Format vorliegen.

E-Mails auf ein Speichermedium exportieren

Überschaubare Mengen von E-Mails können über die Suchmaske des Archivs heruntergeladen werden. Nutzen Sie den Export auf ein Speichermedium, um größere Mengen oder auch alle Mails zu exportieren. Die Mails werden auf dem Medium im Verzeichnis "export" als eml-Dateien abgelegt. Als Dateiname dient eine für jede Mail eindeutige ID. Sie können daher den Export bei Bedarf mehrfach mit unterschiedlichen Suchabfragen durchführen, so dass sich die Ergebnisse im Export-Verzeichnis überlagern.

Auswahl***Ablegen auf Speichermedium***

Die Mails werden auf dem gewählten Speichermedium im Verzeichnis "export" abgelegt.

Suchkriterium

Lassen Sie das Feld leer, um alle Mails zu exportieren. Soll der Export eingeschränkt werden, gehen Sie bitte wie folgt vor:

- Melden Sie sich in der Suchmaske des Archivs als "auditor" oder "revisor" an
- Stellen Sie dort die gewünschte Suche zusammen
- Unterhalb der Ergebnisliste wird der Link "sphinx" angezeigt. Kopieren Sie die Suchbedingung die angezeigt wird, wenn Sie den Link anklicken
- Fügen Sie die Suchbedingung hier ein

Autorisierung durch Benutzer

Um den Export freizugeben, muss zusätzlich das Kennwort des hier ausgewählten Benutzers eingegeben werden.

Auswahl prüfen***Anzahl ausgewählter Mails***

Zeigt an, wieviele Mails im nächsten Schritt exportiert werden.

14.5.5 TLS-Verschlüsselung

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.5.5-A Allgemein.....	541
14.5.5-B Mail-Server Zertifikat.....	543
14.5.5-C Vertrauenswürdige CAs.....	544

Der SX-GATE unterstützt die verschlüsselte Übermittlung von Mail mit Hilfe des STARTTLS-Befehls. Dabei wird jedoch nur die SMTP-Verbindung zwischen dem SX-GATE Mail-Server und dem unmittelbaren Kommunikationspartner verschlüsselt.



Es handelt sich hier weder um eine durchgängige Verschlüsselung vom Absender bis zum Empfänger der Mail, noch ermöglicht es diese Option die Authentizität der Mail festzustellen.

14.5.5-A Allgemein

TLS-Verschlüsselung

Sie können TLS-Verschlüsselung für bestimmte Verbindungen erzwingen, um die verschlüsselte Übermittlung von E-Mails zu gewährleisten. Ist es dem Mail-Server des SX-GATE freigestellt, wann immer es möglich ist verschlüsselte Verbindungen zu benutzen, kann es in Einzelfällen nötig sein, die Verschlüsselung bei bestimmten Kommunikationspartnern zu unterbinden. Beides lässt sich in diesem Bereich konfigurieren.

erzwingen bei Mail an Empfänger-Domain

Diese Einstellung empfiehlt sich, wenn der Mail-Versand zu der Empfänger-Domain nicht unbedingt an einen bestimmten Ziel-Server gebunden ist (z.B. weil ein Backup-Mail-Server existiert). Unterstützt der angesprochene Mail-Server keinen verschlüsselten Mail-Versand, wird die Mail zurückgehalten. Zu einem späteren Zeitpunkt wird dann erneut versucht, die Mail zuzustellen.

erzwingen bei Kommunikation mit Server/Client

Geben Sie die IP-Adresse oder den DNS-Namen (nicht die Mail-Domain) eines Mail-Servers oder Mail-Clients ein. Anders als bei der vorherigen Option wird die verschlüsselte Kommunikation hier auch bei eingehenden Mails erzwungen. Unverschlüsselt wird eine eingehende Mail nicht akzeptiert. Kann

eine ausgehende Mail nicht verschlüsselt übermittelt werden, so wird diese von SX-GATE als unzustellbar an den Absender zurückgeschickt.

verhindern bei Kommunikation mit Server/Client

Geben Sie auch hier die IP-Adresse oder den DNS-Namen (nicht die Mail-Domain) eines Mail-Servers oder Mail-Clients ein. Bei eingehenden Verbindungen wird diesem die Verschlüsselungsoption nicht angeboten. Wird dem SX-GATE bei ausgehenden Verbindungen Verschlüsselung angeboten, so wird dies ignoriert.

Server-Identität verifizieren

Sofern Verschlüsselung erforderlich ist, wird mit dieser Option bei ausgehenden Mails zusätzlich verlangt, dass der Server sich mit einem Zertifikat der CA meldet, die auf dem Reiter (Tab) "Vertrauenswürdige CAs" eingetragen wurde. Das Zertifikat muss ferner auf den korrekten Server-Namen ausgestellt sein.



In Kombination mit "erzwingen bei Kommunikation mit Server/Client" wird bei deaktivierter Verifikation zusätzlich "DANE" für Verbindungen zum konfigurierten Server ausgeschaltet. In Kombination mit "verhindern bei Kommunikation mit Server/Client" hat diese Option keine Bedeutung.

TLS-Verschlüsselung immer versuchen und anbieten (STARTTLS)

Ist dieser Schalter aktiviert, so versucht SX-GATE von sich aus ausgehende Mails verschlüsselt zu versenden, wenn die Gegenstelle dies unterstützt. SX-GATE bietet zudem Verschlüsselung bei allen eingehenden Verbindungen an. In diesem Falle entscheidet die Gegenstelle, ob sie von dieser Option Gebrauch macht.

TLS-Protokoll

Wählen Sie hier die Verschlüsselungsstärke aus. Die Einstellung wirkt sich sowohl auf den Versand als auch auf den Empfang von E-Mails aus.



Im Rahmen der Produktpflege werden die mit der jeweiligen Auswahl verbundenen Parameter von Zeit zu Zeit angepasst.

veraltet

Um Kompatibilität mit älteren Systemen zu gewährleisten, werden in dieser Einstellung AES-Algorithmen mit dem nicht mehr empfohlenen Cipher-Block-Chaining CBC aktiviert. Die minimale TLS-Version ist 1.0.

kompatibel

Wählen Sie diese Einstellung für weitreichende Kompatibilität mit älteren Systemen. Die minimale TLS-Version ist 1.0.

aktuell

In dieser Einstellung werden nur noch halbwegs aktuelle Systeme unterstützt. Es wird mindestens TLS 1.2 vorausgesetzt. Wählen Sie diese Option für erhöhte Sicherheit. Bei direkter Kommunikation mit beliebigen Mailservern im Internet ist jedoch damit zu rechnen, dass mit einzelnen Systemen kein Empfang oder Versand möglich ist.

maximal

Erfordert TLS 1.3. Diese Einstellung eignet sich nicht für die direkte Kommunikation mit beliebigen Mail-Systemen im Internet (direkter Versand oder Empfang per DNS MX-Record). Bevor Sie sich für diese Einstellung entscheiden, sollten Sie prüfen, ob alle Systeme, mit denen potentiell kommuniziert wird, tatsächlich TLS 1.3 unterstützen.

Server-Zertifikate mit DANE/TLSA verifizieren

Anders als bei HTTPS, ist es bei der TLS-verschlüsselten Kommunikation zwischen Mail-Server nicht üblich, das Zertifikat des Ziel-Servers zu prüfen. Mail-Server sind nämlich häufig nicht mit gültigen Zertifikaten ausgestattet. Über DANE (DNS-based Authentication of Named Entities) kann der Betreiber eines Mail-Server im DNS die Information hinterlegen, dass und wie das Zertifikat seines Mail-Servers geprüft werden kann. Die Verbindung ist dann gegen Man-in-the-Middle-Attacken geschützt.



DANE basiert auf DNSSEC. Im SX-GATE DNS-Server muss daher die DNSSEC-Validierung aktiviert sein (Menü "Module > DNS > Einstellungen", auf dem Reiter "Client-Zugriff").

Sollten die Verbindung zu einem bestimmten Mail-Server aufgrund einer Fehlkonfiguration scheitern, können Sie DANE für diesen Server durch einen Eintrag in der obigen Tabelle "TLS-Verschlüsselung" deaktivieren. Fügen Sie dazu einen Eintrag mit "Verschlüsselung erzwingen bei Kommunikation mit Server/Client" aber ohne "Server-Identität verifizieren" hinzu.

14.5.5-B Mail-Server Zertifikat

SX-GATEs Mail-Server weist sich mit diesem Zertifikat gegenüber Clients und anderen Mail-Servern aus, die E-Mails verschlüsselt an SX-GATE übermitteln können (SMTP STARTTLS). Ferner nutzt es der POP3- und IMAP4-Server des SX-GATEs um verschlüsselten Zugriff zu ermöglichen.

Schlüssel/Zertifikat auswählen

Wählen Sie hier einen der Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.

14.5.5-C Vertrauenswürdige CAs

Wenn SX-GATE eine E-Mail über eine TLS-verschlüsselte Verbindung versendet, wird das Zertifikat des Ziel-Servers geprüft. Hinterlegen Sie hier die CA-Zertifikate, die SX-GATE dabei als vertrauenswürdig einstufen soll.



In der Grundkonfiguration stellt SX-GATE die Mail auch dann zu, wenn das Zertifikat des Ziel-Servers nicht erfolgreich geprüft werden konnte. Um das Verhalten für bestimmte Empfänger zu ändern, tragen Sie diese bitte auf dem Reiter (Tab) "Allgemein" in die Tabelle "TLS-Verschlüsselung" ein und aktivieren Sie dabei die Option "Server-Identität verifizieren".

14.5.6 S/MIME-Gateway

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.5.6-A Allgemein.....	545
14.5.6-B Entschlüsseln.....	547
14.5.6-C Verifizieren.....	548
14.5.6-D Signieren.....	550
14.5.6-E Verschlüsseln.....	552

Das S/MIME-Gateway ermöglicht den automatisierten Einsatz von S/MIME nach außen hin samt zentralem Schlüsselmanagement. Eingehende E-Mails lassen sich automatisch Entschlüsseln sowie deren Signatur prüfen. Der Status dieser Operationen wird im Betreff der Mail angezeigt. Als Teil der Signatur empfangene Zertifikate können für den verschlüsselten Versand genutzt werden. Ausgehende Mails werden soweit möglich automatisch signiert und verschlüsselt.



Bevor Sie diese Komponente einsetzen, sollten Sie sich der Implikationen bewusst sein. An sich soll S/MIME sicherstellen, dass der Absender tatsächlich der angegebene ist und es verspricht Verschlüsselung und Schutz vor Veränderung von Ende-zu-Ende. All dies ist beim Einsatz eines S/MIME-Gateways nur noch eingeschränkt gewährleistet, da die Kommunikation zwischen Gateway und internem Absender bzw. internem Empfänger nicht durch S/MIME abgesichert und daher auf verschiedenste Weise angreifbar ist.

Kritisch zu betrachten sind insbesondere folgende Punkte:

- Für den Gegenüber ist der fehlende Ende-zu-Ende-Charakter von S/MIME in keinsten Weise ersichtlich.
- Ursprünglich verschlüsselte Mails werden im Normalfall unverschlüsselt im Postfach abgelegt.
- Bevor eine Mail signiert wird, sollte der Absender authentifiziert werden. Insbesondere beim Einsatz eines internen Mail-Servers ist dies jedoch oft nicht direkt möglich, so dass letztlich darauf vertraut werden muss, dass der angegebene Absender korrekt ist.
- Selbst wenn im internen Netzwerk zur Kommunikation stets TLS-Verschlüsselung genutzt wird, sind Man-in-the-Middle-Angriffe möglich, da Zertifikatsfehler gerne ignoriert werden.
- Um Entschlüsseln und Signieren zu können, benötigt das S/MIME-Gateway die privaten Schlüssel der lokalen Benutzer.

14.5.6-A Allgemein

Hier legen Sie fest, welche Funktionen das S/MIME-Gateway übernehmen soll. Das Verifizieren und Verschlüsseln kann einfach aktiviert werden. Hierzu sind keine Voraussetzungen wie z.B. private Schlüssel erforderlich. Um hingegen Signieren und Entschlüsseln zu können, müssen Sie zunächst S/MIME-Schlüssel im Menü "System > Zertifikatsverwaltung > Schlüsselbund" hochladen. Wo Sie anschließend Verweise auf diese Schlüssel eintragen müssen, ist abhängig von der Einsatzumgebung:

Sie wollen Domain-Zertifikate für die Kommunikation mit bestimmten Empfängern nutzen

Domain-Zertifikate werden im Menü "Module > Mail-Server > Domains" je Domain konfiguriert.

Der Versand von Mails erfolgt direkt über SX-GATE

Verknüpfen Sie die S/MIME-Schlüssel in der Benutzerverwaltung mit Benutzerkonten. Aktivieren Sie ferner die Benutzeranmeldung im SMTP-Server (Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle").

Der Versand von Mails erfolgt über einen internen Mail-Server

Hinterlegen Sie die S/MIME-Schlüssel auf dem Reiter (Tab) "Signieren" und tragen Sie die Adresse des internen Mail-Servers bei "Absender-Adresse vertrauen wenn empfangen von" ein. Falls die Signaturfunktion deaktiviert sein sollte, werden die Schlüssel stattdessen auf dem Reiter "Entschlüsseln" hinterlegt.

Mails entschlüsseln

Aktivieren Sie diese Option um Mails automatisch zu entschlüsseln, sofern SX-GATE über einen passenden Schlüssel verfügt und die Empfänger-Adresse im S/MIME-Zertifikat enthalten ist.

Signatur eingehender Mails verifizieren

Wenn diese Option aktiviert ist, verifiziert SX-GATE die Signaturen eingehender E-Mails. Dies beinhaltet neben der Prüfung der Signatur als solches auch die Prüfung des verwendeten Zertifikats. Es muss gültig sein, von einer vertrauenswürdigen CA stammen, für das Signieren von E-Mails qualifiziert sein und die E-Mail-Adresse des Absenders beinhalten.



Die Verifikation wird nur bei E-Mails durchgeführt, die entweder von einem POP-Server abgeholt oder von einer externen IP-Adresse ohne Authentifizierung empfangen wurden. Als externe Adressen zählen alle IPs, die nicht unter "Lokale IP-Adressen" im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" eingetragen sind.

Ausgehende Mails signieren

Ausgehende Mails werden signiert, wenn diese Option aktiviert ist und eine Reihe von Voraussetzungen erfüllt sind. Grundsätzlich nicht signiert werden E-Mails an lokale Empfänger, also E-Mails die in ein SX-GATE-Postfach zugestellt oder an einen internen Mail-Server weitergeleitet werden. Bereits verschlüsselte oder signierte E-Mails werden ebenfalls nicht signiert. SX-GATE kann eine E-Mail nur dann signieren, wenn ein zur Absender-Adresse passender Schlüssel verfügbar ist. Jeder Schlüssel ist dabei mit einem Benutzerkonto verknüpft und um ihn nutzen zu können, muss sich der Absender normalerweise authentifizieren. Falls dies nicht möglich ist, kann hilfsweise der in der E-Mail angegebenen Absender-Adresse vertraut werden. SX-GATE sollte ausschließlich den Daten von Mails vertrauen, die von Server-Systemen empfangen wurden, die ihrerseits den Absender authentifizieren und die Absender-Adresse nur akzeptieren, wenn diese zum authentifizierten Nutzer passt. Server-Systeme denen Sie insoweit vertrauen, können in Form einer IP-Liste konfiguriert werden.



Diese Option sollten Sie nur zusammen mit der Option "Mails entschlüsseln" einsetzen, denn sobald Sie signierte E-Mails versenden, müssen Sie damit rechnen, verschlüsselte Mails zurück zu erhalten.

Mails verschlüsseln

SX-GATE verschlüsselt E-Mails automatisch, sofern diese Option aktiviert ist und zur Empfänger-Adresse ein S/MIME-Zertifikat vorliegt. Grundsätzlich nicht verschlüsselt werden bereits verschlüsselte E-Mails und Mails an lokale Empfänger, also E-Mails die in ein SX-GATE-Postfach zugestellt oder an einen internen Mail-Server weitergeleitet werden.

14.5.6-B Entschlüsseln

Auf diesem Reiter (Tab) legen Sie Details zur Entschlüsselung fest. Welche Voraussetzungen erfüllt sein müssen, damit SX-GATE eine Mail entschlüsselt, können Sie in der Dokumentation des Reiters "Allgemein" nachlesen.

Markierung für den Betreff verschlüsselter Mails

Legen Sie hier fest, wie SX-GATE den Betreff von E-Mails markieren soll, die entschlüsselt wurden. Das gewählte Symbol bzw. der konfigurierte Text wird zuvor grundsätzlich aus dem Betreff aller Mails ausgefiltert. Damit wird zum einen verhindert, dass der Status gefälscht wird. Anwender können auf eine markierte Mail aber auch einfach antworten, ohne selbst die Markierung aus dem Betreff entfernen zu müssen.

UTF-8 Symbol ##

Die Darstellung des Symbols ist abhängig vom Mail-Client des Empfängers. Das Symbol wird unter Umständen auch gar nicht angezeigt!

Entschlüsselte Mails als "vertraulich" markieren

Wenn aktiviert, setzt SX-GATE bei entschlüsselten Mails die Kopfzeile "Sensitivity: company-confidential", wodurch in manchen Mail-Clients die Mail als "vertraulich" markiert wird. Die Kopfzeile wird zuvor bei E-Mails entfernt, die von extern empfangen wurden, damit der Status nicht gefälscht werden kann. Von intern empfangene Mails behalten den Header. Enthält eine E-Mail bereits einen Sensitivity-Header mit anderem Wert (z.B. "personal" oder "private"), wird der Header weder gelöscht noch verändert und die Mail somit nicht als "vertraulich" markiert.

S/MIME-Schlüssel

Zusätzlich zu eventuellen in der Benutzerverwaltung hinterlegten S/MIME-Schlüsseln werden alle hier eingetragenen Schlüssel dazu genutzt, verschlüsselt empfangene E-Mails automatisch zu entschlüsseln. Die Empfänger-Adresse muss dabei zur E-Mail-Adresse im Zertifikat passen.



Wenn Sie einen Schlüssel aus der Liste entfernen, kann SX-GATE damit verschlüsselte E-Mails nicht mehr entschlüsseln. Diese E-Mails werden dann in verschlüsselter Form zugestellt. Sollte der Schlüssel bereits vollständig vernichtet worden sein, ist eine Entschlüsselung auch nachträglich nicht mehr möglich.

In der Übergangszeit nach der Erneuerung eines Schlüssels werden üblicherweise noch über einen längeren Zeitraum E-Mails empfangen, die mit dem alten Zertifikat verschlüsselt wurden. Dies kann selbst dann noch vorkommen, wenn das alte Zertifikat bereits abgelaufen ist. Wenn Sie im Menü "System > Zertifikatsverwaltung > Schlüsselbund" ein Schlüsselpaar erneuern, wird das vorherige gesichert. Das S/MIME-Gateway nutzt dann automatisch weiterhin das alte Schlüsselpaar zum Entschlüsseln eingehender Mails.



Es wird immer nur das zuletzt genutzte Schlüsselpaar gesichert, nicht etwa mehrere Generationen.

14.5.6-C Verifizieren

Auf diesem Reiter (Tab) legen Sie Details zur Verifikation von Signaturen fest. Wie und unter welchen Voraussetzungen SX-GATE eine signierte Mail verifiziert, können Sie in der Dokumentation des Reiters "Allgemein" nachlesen.

Korrekte Signaturen entfernen

Auf Wunsch wird die Signatur von erfolgreich verifizierten E-Mails entfernt. Schlägt die Verifikation in irgendeinem Punkt fehl, bleibt die Signatur stets erhalten.

nur Domain-Signaturen

Falls es Kommunikationspartner mit Domain-Zertifikat gibt, die dieses auch zum Signieren einsetzen, sollten deren Signaturen entfernt werden. Andernfalls wird sich das Mailprogramm des Empfängers über die nicht zur Signatur passende Absenderadresse beschweren.

Binär signierte Mails konvertieren

Eine Mail kann auf zweierlei Arten signiert werden: Mit der Signatur als separatem Mailanhang (smime.p7s) oder als binäres Format in Form einer sogenannten opaken Signatur. Es gibt Mailclients, die opak signierte Mails nicht unterstützen. Diese zeigen dann eine leere Mail an, die lediglich einen Anhang (smime.p7m) enthält. Sollten solche Mailclients bei Ihnen im Einsatz sein, kann SX-GATE opak signierte Mails automatisch in das Format mit angehängter Signatur umwandeln.

Empfangene Zertifikate zur Verschlüsselung nutzen

Die als Teil von Signaturen empfangenen Zertifikate können vom SX-GATE verwendet werden, um dem Gegenüber zukünftig verschlüsselte Mails zu senden. Berücksichtigt werden Zertifikate nur, wenn der Verifikations-Prozess fehlerfrei durchlaufen wurde oder es höchstens Unstimmigkeiten mit dem Zertifikat als solches gibt (abgelaufen, unbekannte CA, falscher Verwendungszweck). Die Liste der aktuell freigegebenen Zertifikate können Sie auf dem Reiter (Tab) "Verschlüsseln" einsehen und bearbeiten.

nach manueller Freigabe

Die empfangenen Zertifikate werden lediglich temporär zwischengespeichert. Sie können sich die Zertifikate im Menü "Monitoring > Mail-Server" auf dem Reiter (Tab) "S/MIME Zertifikate" anzeigen lassen und auf Wunsch für die Verschlüsselung freigeben.

automatisch wenn fehlerfrei verifiziert

Wenn der Verifikations-Prozess ohne Fehler abgeschlossen werden kann, wird das für die Signatur verwendete Zertifikat automatisch freigegeben. Bei Zertifikatsfehlern ist eine manuelle Freigabe erforderlich.

automatisch

Auch fehlerhafte Zertifikate werden automatisch zur Verschlüsselung freigegeben.

Markierung für den Betreff signierter Mails bei "im Auftrag" und Domainsignatur

Üblicherweise ist der Absender einer Mail im From-Header angegeben. Bei einer im Auftrag gesendeten Mail steht der tatsächliche Absender hingegen im Sender-Header. Leider zeigen manche Mail-Clients den Sender-Header nicht an. So kann der Eindruck erweckt werden, der Absender im From-Header hätte die Mail signiert. Um dies zu verhindern, fügt SX-GATE die E-Mail-Adresse des Signaturgebers in den Betreff ein, wenn die E-Mail-Adresse des Sender-Headers nicht auch im From-Header zu finden ist.



Da Sender-Header in der Praxis nur selten verwendet werden, werden Sie diese Markierung fast nie zu Gesicht bekommen.

Bei Domainsignaturen kann lediglich die Absenderdomain und nicht die vollständige Absenderadresse als korrekt angenommen werden. Daher wird bei Domainsignatur z.B. mit "**@example.com" markiert.

Markierungen für den Betreff signierter Mails

Legen Sie hier fest, wie SX-GATE den Betreff von signierten E-Mails markieren soll, deren Signatur überprüft wurde. Die gewählten Symbole bzw. der konfigurierte Text wird zuvor grundsätzlich aus dem Betreff aller Mails ausgefiltert. Damit wird zum einen

verhindert, dass der Status gefälscht wird. Anwender können auf eine markierte Mail aber auch einfach antworten, ohne selbst die Markierung aus dem Betreff entfernen zu müssen.

UTF-8 Symbole

Die Darstellung der Symbole ist abhängig vom Mail-Client des Empfängers. Die Symbole werden unter Umständen auch gar nicht angezeigt!

CA-Zertifikate

Welche CA-Zertifikate bei der Verifikation von Signaturen als vertrauenswürdig gelten sollen, lässt sich hier einstellen. Weiterhin können Sie festlegen, ob anhand von Certificate-Revocation-Lists (CRLs) geprüft werden soll, ob Zertifikate widerrufen wurden. Dabei kann entweder nur das Zertifikat des Kommunikationspartners (Endzertifikat) oder die komplette Zertifikatskette geprüft werden.

Von manchen Kommunikationspartnern erhalten Sie unter Umständen signierte Mails, die nicht mit einem Kaufzertifikat sondern mit Zertifikaten einer eigenen und somit nicht vertrauenswürdigen CA unterschrieben wurden. SX-GATE wird diese Mails entsprechend mit der Markierung für "Zertifikat nicht vertrauenswürdig" versehen. Wenn Sie regelmäßig mit diesem Kommunikationspartner Kontakt haben, können Sie dessen CA im S/MIME-Gateway hinterlegen, so dass die Signaturen fortan erfolgreich geprüft werden können. Um Missbrauch zu verhindern, wird die CA dabei mit einzelnen E-Mail-Adressen oder E-Mail-Domains verknüpft. Nur für diese Absender wird die spezielle CA genutzt.

Nachdem Sie sich das CA-Zertifikat haben zukommen lassen, müssen Sie es im Menü "System > Zertifikatsverwaltung > CA Zertifikate" importieren. Fügen Sie anschließend hier einen neuen Eintrag hinzu, wobei Sie die CA mit dem Absender verknüpfen.

14.5.6-D Signieren

Auf diesem Reiter (Tab) legen Sie Details zum Signieren von E-Mails fest. Welche Voraussetzungen erfüllt sein müssen, damit SX-GATE eine Mail signiert, können Sie in der Dokumentation des Reiters "Allgemein" nachlesen.

Absender-Adresse vertrauen wenn empfangen von

Um Missbrauch zu verhindern, empfehlen wir zum Signieren Benutzerauthentifizierung und mit Benutzerkonten verknüpfte S/MIME-Schlüssel zu nutzen. Wird zusätzlich zum SX-GATE ein interner Mail-Servers genutzt, ist eine direkte Anmeldung des Clients am SX-GATE jedoch häufig nicht möglich. Tragen Sie die IP-Adresse des internen Mail-Servers in die Liste ein, sofern SX-GATE darauf vertrauen kann, dass die Absender-Adressen (From- oder Sender-Header) korrekt sind, die in E-Mails von diesem Server übermittelt werden. Konfigurieren Sie dann unter "Ohne Authentifizierung nutzbare S/MIME-Schlüssel" die gewünschten Zertifikate.



Nutzen Sie diese Option nur wenn unbedingt notwendig. Geben Sie keine größeren Netzwerke wie z.B. "INTRANET" frei. Stellen Sie sicher, dass alle hier freigegebenen Systeme korrekte Absender-Adressen garantieren können.



Die SX-GATE Groupware, sofern sie installiert ist, garantiert korrekte Absender-Adressen und wird daher automatisch als vertrauenswürdig betrachtet.

Ohne Authentifizierung nutzbare S/MIME-Schlüssel

Hier konfigurierte Schlüssel dürfen zum Signieren ausgehender E-Mails verwendet werden ohne dass sich der Absender authentifiziert. Die Schlüssel werden im Menü System > Zertifikatsverwaltung > Schlüsselbund" administriert.



Beachten Sie bitte den Hinweis zur Erneuerung ablaufender Zertifikate weiter unten.

Voraussetzung ist, dass SX-GATE die Mail von einer unter "Absender-Adresse vertrauen wenn empfangen von" konfigurierten Adresse empfängt. Anhand der E-Mail-Adresse des Absenders (From- oder Sender-Header) wird dann nach dem zugehörigen Schlüssel gesucht.



Wählen sie diese Variante, wenn die Benutzer ausgehende Mails zunächst an einen internen Mail-Server übermitteln, der die Mails dann an SX-GATE weiterleitet. Sollten die Benutzer ausgehende Mails direkt an SX-GATE übergeben, empfehlen wir stattdessen die Zertifikate in der Benutzerverwaltung mit den zugehörigen Benutzerkonten zu verknüpfen und authentifizierten Mailversand zu nutzen.

Zusätzlich zu eventuellen in der Benutzerverwaltung hinterlegten S/MIME-Schlüsseln werden alle hier hinterlegten Schlüssel auch dazu genutzt, verschlüsselt empfangene E-Mails automatisch zu entschlüsseln. Die Empfänger-Adresse muss dabei zur E-Mail-Adresse im Zertifikat passt.



Wenn Sie einen Schlüssel aus der Liste entfernen, kann SX-GATE damit verschlüsselte E-Mails nicht mehr entschlüsseln. Diese E-Mails werden dann in verschlüsselter Form zugestellt. Sollte der Schlüssel bereits vollständig vernichtet worden sein, ist eine Entschlüsselung auch nachträglich nicht mehr möglich.

In der Übergangszeit nach der Erneuerung eines Schlüssels werden üblicherweise noch über einen längeren Zeitraum E-Mails empfangen, die mit dem alten Zertifikat verschlüsselt wurden. Dies kann selbst dann noch vorkommen, wenn das alte Zertifikat bereits abgelaufen ist. SX-GATE unterstützt Sie in dieser Übergangsphase wie folgt: Wenn Sie im Menü "System > Zertifikatsverwaltung > Schlüsselbund" ein Schlüsselpaar erneuern, wird das vorherige gesichert. Das S/MIME-Gateway nutzt dann automatisch das alte Schlüsselpaar weiterhin zum Entschlüsseln eingehender Mails, während das aktuelle Schlüsselpaar sowohl zum Entschlüsseln als auch zum Signieren genutzt wird. Steht also ein Zertifikat zur Erneuerung an, dann erneuern Sie es bitte im bestehenden Eintrag unter "Schlüsselbund". Fügen Sie keinen neuen Eintrag hinzu. Auch die S/MIME-Gateway-Konfiguration muss nicht angepasst werden.



Es wird immer nur das zuletzt genutzte Schlüsselpaar gesichert, nicht etwa mehrere Generationen.

Nicht signieren zu Empfängeradresse/-domain

Mails an Domains oder Adressen in dieser Liste werden nicht signiert.

Befehlswort im Betreff für "nicht signieren"

Beginnt der Betreff einer E-Mail mit dem hier konfigurierten Befehlswort (inklusive der eckigen Klammern), wird SX-GATE die Mail nicht signieren. Das Befehlswort wird aus dem Betreff entfernt.



Der Betreff kann mit mehreren Befehlswörtern beginnen (z.B. "[NOCRYPT][NOSIGN] ..."). Befehlswörter werden nur bei authentifiziert übermittelten Mails und bei Mails von lokalen IP-Adressen berücksichtigt und gelöscht.

14.5.6-E Verschlüsseln

Auf diesem Reiter (Tab) legen Sie Details zum Verschlüsseln von E-Mails fest. Welche Voraussetzungen erfüllt sein müssen, damit SX-GATE eine Mail verschlüsselt, können Sie in der Dokumentation des Reiters "Allgemein" nachlesen.

Befehlswort im Betreff für "nicht verschlüsseln"

Beginnt der Betreff einer E-Mail mit dem hier konfigurierten Befehlswort (inklusive der eckigen Klammern), wird SX-GATE die Mail nicht verschlüsseln. Das Befehlswort wird aus dem Betreff entfernt.



Der Betreff kann mit mehreren Befehlswörtern beginnen (z.B. "[NOSIGN][NOCRYPT] ..."). Befehlswörter werden nur bei authentifiziert übermittelten Mails und bei Mails von lokalen IP-Adressen berücksichtigt und gelöscht.

Befehlswort im Betreff für "zwingend verschlüsseln"

Beginnt der Betreff einer E-Mail mit dem hier konfigurierten Befehlswort (inklusive der eckigen Klammern), muss SX-GATE die Mail verschlüsseln. Das Befehlswort wird aus dem Betreff entfernt. Steht kein passender Schlüssel für alle externen Empfänger zur Verfügung, findet keine Zustellung statt und die Mail geht als unzustellbar an den Absender zurück.



Der Betreff kann mit mehreren Befehlswörtern beginnen (z.B. "[NOSIGN][CRYPT] ..."). Befehlswörter werden nur bei authentifiziert übermittelten Mails und bei Mails von lokalen IP-Adressen berücksichtigt und gelöscht.



Eine zwingende Verschlüsselung an lokale Empfänger (SX-GATE-Postfach oder interner Mail-Server) findet nicht statt.

Als "vertraulich" markierte Mails zwingend verschlüsseln

Manche Mail-Clients können eine E-Mail als "vertraulich" markieren. Dazu wird in der Mail die Kopfzeile "Sensitivity: company-confidential" gesetzt. Ist dieser Header gesetzt, kann SX-GATE dies als Anweisung verstehen, die Mail unbedingt verschlüsselt zu versenden. Der Header selbst wird gelöscht. Steht kein passender Schlüssel für alle externen Empfänger zur Verfügung, findet keine Zustellung statt und die Mail geht als unzustellbar an den Absender zurück.



Der Header wird nur bei authentifiziert übermittelten Mails und bei Mails von lokalen IP-Adressen berücksichtigt und gelöscht.



Eine zwingende Verschlüsselung an lokale Empfänger (SX-GATE-Postfach oder interner Mail-Server) findet nicht statt.

Abgelaufene Partner-Zertifikate löschen nach

Auf Wunsch prüft das System täglich, ob Empfänger-Zertifikate abgelaufen sind und löscht diese. Der Empfänger erhält ab dann unverschlüsselte Mails. Häufig ist es daher besser, ein abgelaufenes Zertifikat noch eine Weile weiterzuverwenden.

Geben Sie die Anzahl Monate an, nach denen ein abgelaufenes Zertifikat gelöscht wird. Mit "0" werden abgelaufene Zertifikate sofort gelöscht. Lassen Sie das Feld leer, wenn abgelaufene Zertifikate nicht automatisch gelöscht werden sollen.

S/MIME-Partner bearbeiten

Für den verschlüsselten Versand muss zur E-Mail-Adresse des Empfängers das passende S/MIME-Zertifikat hinterlegt werden. Sie können entsprechende Einträge hier von Hand vornehmen. Auf dem Reiter (Tab) "Verifizieren" lässt sich aber auch ein mehr oder weniger automatischer Prozess konfigurieren, bei dem SX-GATE die benötigten Daten selbständig aus signierten E-Mails extrahiert.

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Empfänger E-Mail-Adresse

Geben Sie hier die Email-Adresse eines externen Empfängers ein. Für den verschlüsselten Versand von E-Mails an diese Adresse können Sie anschließend das zugehörige Zertifikat hochladen.



Falls der Empfänger ein Domain-Zertifikat einsetzt, können Sie anstelle einer individuellen E-Mail-Adresse auch einen Domainnamen eingeben.

S/MIME-Zertifikat

Status

Falls beim verschlüsselten Versand Problem mit einem bestimmten Empfänger auftreten, können Sie dessen Zertifikat hier deaktivieren.

Herkunft

Zeigt an, ob das Zertifikat manuell hochgeladen oder aus einer signierten Mail extrahiert wurde.

14.5.7 Domains

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

E-Mail Domain

Geben Sie hier eine Empfänger-Domain an. Mails an diese Domain werden dann entweder in ein lokales Postfach auf SX-GATE zugestellt oder an einen speziellen (internen) Mailserver weitergeleitet.

Zustellung

Für jede Empfänger-Domain lässt sich individuell festlegen, wohin ankommende E-Mails zugestellt werden:

an SX-GATE Postfach

Mails an eine Domain dieses Typs werden in ein Benutzer-Konto bzw. über einen Mail-Verteiler des SX-GATE zugestellt.

an internen Mail-Server

Wählen Sie diese Einstellung, um eingehende E-Mails an einen bestimmten Mail-Server nach intern weiterzuleiten. Ein typisches Beispiel wäre ein Mail-Server im LAN wie z.B. Microsoft Exchange, der die Benutzerpostfächer verwaltet.

an externen Mail-Server

Diese Einstellung ermöglicht es, ausgehende E-Mails über einen bestimmten Mail-Server zu versenden. Erlaubt ist dies nur authentifizierten Benutzern sowie

lokalen Adressen, wie im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" konfiguriert.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.5.7-A Lokale Domain.....	556
14.5.7-B Mail-Server.....	557
14.5.7-C Virtuelle Empfänger.....	558
14.5.7-D Mailrouting.....	559
14.5.7-E Absender Adressen.....	560
14.5.7-F Provider-Relay.....	561
14.5.7-G Text-Zusatz.....	562
14.5.7-H DKIM.....	562
14.5.7-I S/MIME.....	564

Zustellung

an SX-GATE Postfach

Mails an eine Domain dieses Typs werden in ein Benutzer-Konto bzw. über einen Mail-Verteiler des SX-GATE zugestellt.

an internen Mail-Server

Wählen Sie diese Einstellung, um eingehende E-Mails an einen bestimmten Mail-Server nach intern weiterzuleiten. Ein typisches Beispiel wäre ein Mail-Server im LAN wie z.B. Microsoft Exchange, der die Benutzerpostfächer verwaltet.

an externen Mail-Server

Diese Einstellung ermöglicht es, ausgehende E-Mails über einen bestimmten Mail-Server zu versenden. Erlaubt ist dies nur authentifizierten Benutzern sowie lokalen Adressen, wie im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" konfiguriert.

14.5.7-A Lokale Domain

Art der Domain

Folgende Arten stehen zur Wahl:

einfache Domain

Bei einer einfachen Domain werden ankommende E-Mails direkt an Benutzerkonten oder -gruppen zugestellt, so wie dies in der SX-GATE Benutzerverwaltung festgelegt ist.

erweiterte Domain

Die erweiterte Domain ermöglicht es, die Empfänger-Adresse vor der Zustellung zu verändern. Damit wird es z.B. möglich, E-Mails an info@example.com und info@example.net an verschiedene Empfänger zuzustellen.

Alias-Domain

Wählen Sie die Alias-Domain, wenn Sie zwei lokale Domains in der selben Art und Weise verarbeiten wollen. Sollen beispielsweise E-Mails an die Domains example.net genau wie Mails an example.com verteilt werden, müsste example.com als erweiterte Domain mit Verteilregeln angelegt werden. Dann wird die Domain example.net angelegt und zum Alias für example.com erklärt.

Domain verarbeiten wie

Geben Sie hier die Empfänger-Domain an, die Anstelle der ursprünglichen Empfänger-Domain eingesetzt werden soll.

14.5.7-B Mail-Server

E-Mails weiterleiten an

Tragen Sie hier den Mail-Server ein, an den alle E-Mails für die aktuell ausgewählte Domain weitergeleitet werden sollen.

Backup-Server

Sollte für den oben konfigurierten Server ein Ersatz-System existieren, können Sie dieses hier eintragen. SX-GATE übergibt Mails an dieses Zweit-System, wenn der primäre Server nicht erreichbar ist. Falls kein Ersatz-Server existiert, lassen Sie das Feld bitte leer.

Inklusive Subdomains

Aktivieren Sie diesen Schalter, wenn auch alle Subdomains an den angegebenen Server weitergeleitet werden sollen.

Server Port

Sofern der Server keine Verbindungen auf dem Standard-Port 25 entgegennimmt, können Sie hier die abweichende Portnummer eintragen (üblicherweise 465 oder 587).

Protokoll

Eine Auswahl ist hier nur erforderlich, wenn der Server per SMTPS angesprochen werden muss und dabei nicht den Standard-Port 465 nutzt.

SMTP-Auth Benutzername

Sollte für die Nutzung des Servers eine Benutzeranmeldung mit SMTP AUTH erforderlich sein, so können Sie die den Benutzernamen und das Passwort in die entsprechenden Felder eintragen. Sind diese Felder leer, wird auch keine Benutzeranmeldung vorgenommen.



SMTP-Auth ist gemäß Standard eine "Hop-to-Hop"-Authentifizierung. Dies bedeutet, dass die Anmeldung nur die beiden unmittelbar miteinander kommunizierenden Systeme betrifft. In diesem Falle muss sich also der SX-GATE Mail-Server gegenüber dem Relay-Server authentifizieren und nicht in etwa z.B. der Benutzer, der die Mail geschrieben hat. SX-GATE kann folglich nur einen bestimmten Login für SMTP-Auth nutzen. Eine unterschiedliche Anmeldung in Abhängigkeit vom Absender der E-Mail kann im Menü "SMTP Einstellungen" konfiguriert werden.

14.5.7-C Virtuelle Empfänger

Umsetzung Empfänger-Adressen

Die Zustellung von E-Mails an lokale Konten erfolgt normalerweise anhand des lokalen Teils der E-Mail-Adresse, d.h. dem Teil vor dem "@"-Zeichen. Sollte der lokale Teil der Empfänger-Adresse nicht mit dem tatsächlich gewollten Empfänger übereinstimmen, können Sie hier die Empfänger-Adresse umschreiben. Diese Konfiguration kann je Domain unterschiedlich vorgenommen werden. Damit wird es insbesondere möglich, E-Mail-Adressen in unterschiedlichen Domains aber mit dem selben lokalen Teil an verschiedene Empfänger auszuliefern. Während also z.B. "info@example.com" regulär an das Konto "info" zugestellt wird, könnte "info@example.net" an ein Konto "info_net" umgeleitet werden.



Einstellungen die unabhängig von der Empfänger-Domain sind, sollten Sie in der Benutzerverwaltung vornehmen. Dies ist beispielsweise der Fall, wenn ein Benutzer in allen lokalen Domains nicht nur unter "Nachname" sondern auch unter "Vorname.Nachname" erreichbar sein soll. Das selbe gilt für die Weiterleitung der E-Mails eines Kontos an eine andere Adresse.

Tragen Sie in dieser Liste die ursprüngliche Empfänger-Adresse und deren neues Ziel ein. Alternativ kann auch die Annahme der Mail verweigert werden. Als Ziel kann eine beliebige interne oder externe E-Mail-Adresse angegeben werden. Wird bei einer internen Adresse eine vollständige E-Mail-Adresse mit Domain angegeben, so finden evtl. weitere Adressumsetzungen statt. Prüfen Sie dazu diese Maske in der entsprechenden Domain. Wird die Adresse des internen Empfängers hingegen ohne

Domain eingetragen, also beispielsweise direkt der Name einer SX-GATE-Gruppe oder eines SX-GATE-Postfaches, so wird unmittelbar ausgeliefert. Das eingestellte Verhalten einer Gruppe bzw. eines Postfaches bleibt dabei selbstverständlich erhalten. Dazu gehört z.B. die Verteilung einer E-Mail an alle Mitglieder einer Gruppe wie auch die Berücksichtigung eventueller Weiterleitungen in der Konfiguration eines Benutzer-Postfaches.



Prüfen Sie die Konfiguration genau, so dass keine Mail-Schleifen entstehen. Eine E-Mail-Adresse darf also weder direkt noch indirekt wieder an sich selbst weitergeleitet werden.

Zustellung aller übrigen Adressen *@...

Wird eine Adresse in keinem der Eingabebereiche dieser Maske gefunden, so erfolgt die Zustellung unabhängig von der adressierten Domain an SX-GATEs Benutzer und Gruppen. Auf dem Reiter (Tab) "Lokale Domain" ist zudem festgelegt, wie mit unbekannten Adressen zu verfahren ist. Wird dieses Verhalten nicht gewünscht, so kann hier das Standardverhalten je Domain festgelegt werden. Dieses wird für alle E-Mails wirksam, deren Empfänger nicht in der Liste "Umsetzung Empfänger-Adressen" eingetragen sind.

Die Annahme entsprechender E-Mails kann durch SX-GATE verweigert werden. Alternativ kann die Zustellung an eine beliebige interne oder externe E-Mail-Adresse erfolgen. Auch hier gelten die selben Regeln wie für den vorhergehenden Eingabebereich: Wird eine interne E-Mail-Adresse komplett mit Domain eingetragen, erfolgt zunächst eine weitere Verteilung gemäß der auf dieser Bildschirmmaske festgelegten Regeln. Wird der Empfänger ohne Domain angegeben, also z.B. der Name einer SX-GATE-Gruppe oder eines SX-GATE-Postfaches, wird direkt an dieses zugestellt. Das Verhalten der Gruppe oder des Postfaches an sich bezüglich der weiteren E-Mail-Verteilung wird auch hier berücksichtigt. Schließlich besteht noch die Möglichkeit, das spezielle Ziel "*@DOMAIN" anzugeben, also z.B. "*@example.com". In diesem Fall wird von der ursprünglichen Empfänger-Adresse lediglich die Domain ausgetauscht. Der Teil der Adresse vor dem "@"-Zeichen bleibt unverändert. Nutzen Sie diese Möglichkeit, wenn die bereits definierte Adressumsetzung einer Domain von einer weiteren Domain mitverwendet werden kann.



Auch in diesem Bereich sind Mail-Schleifen unbedingt zu vermeiden. Eine E-Mail-Adresse darf weder direkt noch indirekt an sich selbst weitergeleitet werden.

14.5.7-D Mailrouting

Der Versand von E-Mails erfolgt im Normalfall über das Mail-Relay Ihres Providers bzw. direkt an den Mail-Server des Empfängers der über DNS ermittelt wird. Mit Hilfe

von Mailrouting-Einträgen können Sie abweichend davon für einzelne Adressen einen bestimmten Ziel-Server festlegen.

Routing einzelner Empfänger-Adressen

Dieser Bereich ermöglicht es Ihnen, die E-Mails für bestimmte Benutzer an einen abweichenden Mail-Server weiterzuleiten. Falls notwendig, kann dabei auch die Empfänger-Adresse der E-Mail geändert werden. Tragen Sie dazu zwei Regeln zur ursprünglichen Empfänger-Adresse ein: eine mit dem Ziel-Server, eine mit der neuen Empfänger-Adresse.



Einträge in diesem Bereich haben Vorrang vor Einträgen, die auf anderen Reitern dieser Maske für die selbe Empfängeradresse konfiguriert wurden.



Um eine Mail-Schleife zu verhindern, muss unbedingt gewährleistet sein, dass der angegebene Mail-Server eine auf diese Weise erhaltene E-Mail nicht direkt oder indirekt wieder an SX-GATE weiterleitet.

In der Praxis ist hier ein Eintrag nur dann erforderlich, wenn mehrere Mail-Server die Postfächer zu einer lokalen Domain verwalten. In einem typischen Szenario holt SX-GATE die E-Mails der lokalen Domain vom POP3-Server des Providers. Ein einzelner Benutzer hat jedoch keinen Zugriff auf SX-GATE und muss seine E-Mails selbst beim POP-Server des Providers abholen. Versucht nun ein lokaler Benutzer eine E-Mail an diesen externen Benutzer zu senden, stellt SX-GATE diese normalerweise lokal zu. Ein Eintrag in diesem Bereich erlaubt es nun gezielt, die eigentlich lokale E-Mail in das Internet weiterzuleiten.

14.5.7-E Absender Adressen

Umsetzung Absender-Adressen

Hier haben Sie die Möglichkeit, bestimmte Absender-Adressen bei Mails zu verändern. Tragen Sie in die Liste die zu suchende Adresse ein und durch welche sie ersetzt werden soll.



Sollte für die neue Absender-Adresse wiederum eine Adress-Umsetzung konfiguriert sein, wird diese nicht berücksichtigt. Eine Verkettung findet also nicht statt.

Absender-Adresse aller übrigen Adressen *@...

Alle Absender-Adressen für die oben keine bestimmte Umsetzung konfiguriert wurde, können pauschal auf eine bestimmte Mail-Adresse geändert werden. Sollten Sie unabhängig vom tatsächlichen Absender nur die Domain ändern wollen, geben Sie bitte `"*@DOMAIN"` ein, also z.B. `"*@example.com"`. Der Teil vor dem "@"-Zeichen wird dann unverändert übernommen.



Sollte für die neue Absender-Adresse oder in der neuen Domain wiederum eine Umsetzung der Absender-Adresse konfiguriert sein, wird diese nicht berücksichtigt.

14.5.7-F Provider-Relay***Provider-Relay für Absenderdomain "..."***

In Ausnahmefällen kann es erforderlich sein, ausgehende E-Mails je nach Absenderdomain über unterschiedliche Provider zu versenden.



Bestimmte Mails, wie z.B. Empfangsbestätigungen oder Unzustellbarkeitsberichte, werden ohne Absenderadresse gesendet. Diese werden daher nicht über das hier konfigurierte Relay gesendet werden, selbst wenn sie sich auf eine Mail zu dieser Domain beziehen.

Relay-Server Port

Sofern der Relay-Server keine Verbindungen auf dem Standard-Port 25 entgegennimmt, können Sie hier die abweichende Portnummer eintragen (üblicherweise 465 oder 587).

Protokoll

Eine Auswahl ist hier nur erforderlich, wenn der Relay-Server per SMTPS angesprochen werden muss und dabei nicht den Standard-Port 465 nutzt.

SMTP-Auth Benutzername

Sollte für die Nutzung des Relay-Servers eine Benutzeranmeldung mit SMTP AUTH erforderlich sein, so können Sie die den Benutzernamen und das Passwort in die entsprechenden Felder eintragen. Sind diese Felder leer, wird auch keine Benutzeranmeldung vorgenommen.



SMTP-Auth ist gemäß Standard eine "Hop-to-Hop"-Authentifizierung. Dies bedeutet, dass die Anmeldung nur die beiden unmittelbar miteinander kommunizierenden Systeme betrifft. In diesem Falle muss sich also der SX-GATE Mail-Server gegenüber dem Relay-Server authentifizieren und nicht in etwa z.B. der Benutzer, der die Mail geschrieben hat. SX-GATE kann folglich nur einen bestimmten Login für SMTP-Auth nutzen. Eine unterschiedliche Anmeldung in Abhängigkeit vom Absender der E-Mail kann im Menü "SMTP Einstellungen" konfiguriert werden.

14.5.7-G Text-Zusatz

Der hier eingetragene Textbaustein wird an jede ausgehende E-Mail angehängt, die den SX-GATE Mail-Server passiert. Die Unterscheidung zwischen ein- und ausgehenden E-Mails wird im Menü "Module > Mail-Server > SMTP Einstellungen" auf dem Reiter (Tab) "Relay Kontrolle" durch die Werte in "Lokale IP-Adressen" vorgenommen. Authentifiziert angelieferte E-Mails zählen stets zu den ausgehenden E-Mails.

Zeilenumbrüche werden in die Ausgabe übernommen. Wird der Textbaustein an eine HTML-Mail angehängt, so wird stattdessen ein HTML-Zeilenumbruch (
) eingefügt. Der gesamte Textbaustein ist bei HTML-Mails in -Tags eingeschlossen. Zur Formatierung lassen sich beliebige HTML-Tags verwenden. Wird der Textbaustein einer normalen Text-Mail hinzugefügt, werden alle eingegebenen HTML-Formatierungen (Passagen zwischen den Zeichen "<" und ">") entfernt.



Vermeiden Sie im Text die Zeichen "<" und ">". Textbereiche könnten sonst fälschlicherweise entfernt werden.

14.5.7-H DKIM

DKIM steht für "DomainKeys Identified Mail" und wird auf ausgehende Mails angewandt. Es wird eine Prüfsumme über ausgewählte Kopfzeilen wie z.B. Absender, Empfänger und Betreff sowie über den Inhalt der Mail gebildet. Die Prüfsumme wird signiert und als Kopfzeile in die Mail eingefügt. Der öffentliche Schlüssel des für die Signatur verwendeten Schlüsselpaars muss im DNS veröffentlicht werden. Empfänger der Mail können mit Hilfe des öffentlichen Schlüssels überprüfen, dass die signierten Teile der Mail unterwegs nicht verändert wurden. Auch kann der Empfänger davon ausgehen, dass die Mail tatsächlich von jemandem aus der Domain verschickt wurde, die in der Absender-Adresse steht.



DKIM erfordert einen Eintrag im DNS der jeweiligen Domain.

DKIM-Schlüssel

Um das Signieren von Mails für die Domain zu konfigurieren, wählen Sie bitte einen RSA-Schlüssel aus, den Sie im Menü "System > Schlüsselbund" anlegen und verwalten können. Beachten Sie, dass es sich um einen Schlüssel vom Typ "RSA-Schlüssel (SSH, DKIM)" handeln muss.



Manche Systeme im Internet unterstützen noch keine RSA-Schlüssel mit einer Schlüssellänge von mehr als 2048 Bit.

Der Schlüssel sollte regelmäßig (z.B. jährlich) getauscht werden. Wir empfehlen dazu, für den neuen RSA-Schlüssel einen neuen Eintrag im "Schlüsselbund" anzulegen anstatt im bestehenden Eintrag ein neues Schlüsselpaar zu erzeugen.



Beachten Sie bitte die Hinweise zum Schlüsseltausch in der Dokumentation zu "Name des DNS-Eintrags".

Name des DNS-Eintrags

Für DKIM ist ein passender DNS-Eintrag in der jeweiligen Domain erforderlich. Er setzt sich zusammen aus dem Selektor und dem Text "_domainkey". Beim Selektor handelt es sich um einen beliebigen Bezeichner, den Sie hier eintragen können und der den genutzten DKIM-Schlüssel identifizieren soll.



Wenn Sie den DKIM-Schlüssel jährlich ändern, könnten Sie z.B. die Jahreszahl in den Selektor aufnehmen.

Der Selektor ist auch in der DKIM-Kopfzeile enthalten, die jeder signierten Mail hinzugefügt wird. Das validierende System rekonstruiert aus dem Selektor und der Domain den DNS-Namen, unter dem der öffentliche Schlüssel abgerufen werden kann.

Gehen Sie wie folgt vor, um den DKIM-Schlüssel einer Domain zu erneuern:

- Legen Sie im Menü "System > Schlüsselbund" einen neuen Eintrag vom Typ "RSA-Schlüssel (SSH, DKIM)" an. Es ist ratsam, den neuen Eintrag so zu benennen, dass daraus hervorgeht, dass es sich um einen DKIM-Schlüssel handelt und wie der zugehörige Selektor heißen wird. Erzeugen Sie das Schlüsselpaar.
- Fügen Sie im DNS einen neuen DKIM-Eintrag hinzu, wobei Sie einen neuen Selektor und natürlich den öffentlichen Schlüssel des soeben generierten neuen Schlüsselpaars hinterlegen.
- Warten Sie, bis der neue DKIM-Eintrag auf allen für Ihre Domain zuständigen DNS-Servern verfügbar ist.
- Wählen Sie dann unter "DKIM-Schlüssel" das neue Schlüsselpaar aus und ändern Sie gleichzeitig den Selektor unter "Name des DNS-Eintrags".

Daten des DNS-Eintrags

Der TXT-Eintrag im DNS der Domain muss den hier angezeigten Wert haben.



Abhängig von der Verwaltungsoberfläche Ihres DNS-Servers kann es notwendig sein, diesen sehr langen Eintrag in mehrere Teile mit jeweils maximal 255 Zeichen aufzubrechen (z.B. dkim._domainkey TXT "Teil1" "Teil2" ... "TeilX").

14.5.7-I S/MIME

Das SX-GATE S/MIME-Gateway unterstützt sogenannte Domain-Zertifikate. Während normalerweise für jede Absender-Adresse ein individueller S/MIME-Schlüssel beantragt werden müsste, werden mit einem Domain-Zertifikat alle ausgehenden Mails einer oder auch mehrerer lokaler Domains mit einem einzigen Schlüssel signiert und natürlich werden verschlüsselt eingehende Mails mit dem selben Schlüssel entschlüsselt. Was sich zunächst verlockend anhört, hat jedoch einen entscheidenden Nachteil: Der Mail-Client des Empfängers einer signierten Mail sollte eine deutliche Warnung anzeigen, wenn die E-Mail-Adresse des Absenders nicht in dem für die Signatur genutzten Zertifikat enthalten ist.



Domain-Zertifikate sind kein anerkannter Standard. Sie eignen sich nur für die Kommunikation mit Gegenstellen, die darüber informiert wurden, dass ein Domain-Zertifikat zum Einsatz kommt und die die dort eingesetzte Mail-Software entsprechend konfigurieren konnten. Üblicherweise ist dies nur der Fall, wenn die Gegenstelle ebenfalls ein Mail-Verschlüsselungs-Gateway nutzt.

Da es sich ohnehin nicht um ein standardisiertes Verfahren handelt, kann ggf. ein selbst erstelltes Zertifikat zum Einsatz kommen (z.B. von der SX-GATE-CA ausgestellt). Sie können aber natürlich auch ein gekauftes S/MIME-Zertifikat nutzen. Falls Sie die E-Mail-Adresse im Zertifikat frei wählen können, empfehlen wir, einen administrativen Kontakt einzutragen.



Technisch gesehen ist ein Domain-Zertifikat ein ganz normales S/MIME-Zertifikat wie jedes andere auch, das lediglich etwas zweckentfremdet eingesetzt wird. Falls Sie das Zertifikat bei einer CA beantragen, müssen Sie also nicht etwa ein besonderes Zertifikat erwerben. So ist es z.B. nicht erforderlich, ein von manchen CAs angebotenes Abteilungs-Zertifikat zu kaufen, das meist teurer ist als ein auf eine natürliche Person ausgestelltes Zertifikat.

S/MIME-Domain-Schlüssel

Sofern Sie SX-GATE als E-Mail Verschlüsselungs-Gateway verwenden, können Sie hier den S/MIME-Schlüssel auswählen, der als Domain-Zertifikat für das Signieren ausgehender und das Entschlüsseln eingehender Mails genutzt werden soll. Die Schlüssel werden im Menü System > Zertifikatsverwaltung > Schlüsselbund" administriert.



Das Domain-Zertifikat einer Gegenstelle zum Verifizieren eingehender und Verschlüsseln ausgehender Mails hinterlegen Sie im Menü "Module > Mail-Server > S/MIME-Gateway" auf dem Reiter (Tab) "Verschlüsseln". Legen Sie dazu unter "S/MIME-Partner bearbeiten" einen Eintrag für die Domain der Gegenstelle an (z.B. "example.com").

Ausgehende E-Mails mit entsprechender Absender-Domain (From- oder Sender-Header) werden mit dem Domain-Zertifikat signiert, wenn der Empfänger unter "Signiere Mails an folgende Empfänger-Adressen und -Domains" gelistet ist, kein individueller S/MIME-Schlüssel für den Absender verfügbar ist und die E-Mail nicht bereits signiert oder verschlüsselt ist.



Beachten Sie bitte, dass sich Absender-Adressen oft leicht fälschen lassen. Dies wird insbesondere dann relevant, wenn die Mails mehrerer Domains mit unterschiedlichem Zweck oder Eigentümern über SX-GATE versendet werden.

Verschlüsselt empfangene E-Mails werden automatisch entschlüsselt, wenn SX-GATE über einen passenden Schlüssel verfügt und die Domain der Empfänger-Adresse zum Domain-Zertifikat passt.



Wenn Sie den Schlüssel entfernen, kann SX-GATE damit verschlüsselte E-Mails nicht mehr entschlüsseln. Diese E-Mails werden dann in verschlüsselter Form zugestellt. Sollte der Schlüssel bereits vollständig vernichtet worden sein, ist eine Entschlüsselung auch nachträglich nicht mehr möglich.

In der Übergangszeit nach der Erneuerung eines Zertifikats werden üblicherweise noch über einen längeren Zeitraum E-Mails empfangen, die mit dem alten Zertifikat verschlüsselt wurden. Dies kann selbst dann noch vorkommen, wenn das alte Zertifikat bereits abgelaufen ist. Wenn Sie im Menü "System > Zertifikatsverwaltung > Schlüsselbund" ein Schlüsselpaar erneuern, wird das vorherige gesichert. Das S/MIME-Gateway nutzt dann automatisch weiterhin das alte Schlüsselpaar zum Entschlüsseln eingehender Mails.



Es wird immer nur das zuletzt genutzte Schlüsselpaar gesichert, nicht etwa mehrere Generationen.

Signiere Mails an folgende Empfänger-Adressen und -Domains

Tragen Sie hier individuelle E-Mail-Adressen oder ganze Domains der Empfänger ein, an die mit dem Domain-Zertifikat signierte E-Mails geschickt werden dürfen.



Wenn die Liste leer ist, wird mit dem Domain-Zertifikat ausschließlich entschlüsselt, nicht jedoch signiert.

14.6 POP-/IMAP-Client

14.6.1 Einstellungen

Hier wird eingestellt, wann E-Mails von einem POP- oder ETRN-Server abgerufen werden. Sind weder POP- noch ETRN-Server konfiguriert, so sind diese Einstellungen ohne Belang. Das selbe gilt für POP-Server, für die keine Postfächer angegeben wurden bzw. für ETRN-Server ohne abzurufende Domains.

Abholzeiten

In diesem Bereich wird die zeitgesteuerte Mail-Abholung konfiguriert.

Mails abholen bei jedem PPP-Verbindungsaufbau

Wenn SX-GATE mit einer PPP-Wählleitung an das Internet angebunden ist, kann die Mail-Abholung automatisch bei jedem Aufbau einer neuen Wählverbindung gestartet werden.



Mit Hilfe dieser Option lassen sich ggf. Gebühren sparen. Sollte jedoch die Wählverbindung quasi permanent online sein, so ist diese Einstellung wenig sinnvoll. Das selbe gilt bei extrem seltenem Verbindungsaufbau.

Unbekannte Empfänger aus Sammelpostfächern zustellen an

E-Mails aus einem Sammelkonto die sich keinem lokalen Empfänger zuordnen lassen, werden an die hier angegebene Adresse zugestellt.

14.6.2 Server

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.6.2-A OAuth2.....	569
14.6.2-B Postfächer.....	571
14.6.2-C Multi-drop-Parameter.....	571
14.6.2-D Multi-drop-Domains.....	572
14.6.2-E Server Einstellungen.....	573
14.6.2-F ETRN.....	575

Protokoll

Legen Sie hier bitte das Protokoll für den Zugriff auf diesen Server fest. Sie erfahren die notwendige Einstellung bei Ihrem Provider.

POP3

Dies ist das gebräuchlichste Protokoll. Dabei liegen die E-Mails in einzelnen Konten beim Provider, auf die mit Benutzername und zugehörigem Kennwort zugegriffen wird. Sie können die E-Mail aus so einem Konto lokal an einen bestimmten Benutzer oder eine bestimmte Gruppe zustellen (single-drop) oder aber den Inhalt eines solchen Kontos anhand der Adresse des Empfängers verteilen lassen (multi-drop).

Microsoft 365 POP3 (OAUTH2)

Nutzen Sie diese Einstellung zur Abholung von "Microsoft 365"-Postfächern mit POP3.

APOP

Das APOP-Verfahren entspricht POP3, lediglich die Anmeldung erfolgt auf andere Weise.

IMAP

Bei manchen POP-Server ist ein sehr kurzer Timeout für Verbindungen konfiguriert. Sollte es deshalb zu Problemen kommen, hilft evtl. die Umstellung auf das IMAP-Protokoll.

Microsoft 365 IMAP (OAUTH2)

Nutzen Sie diese Einstellung zur Abholung von "Microsoft 365"-Postfächern mit IMAP.

ETRN (ESMTP)

ETRN ist ein Befehl des ESMTP-Protokolls. ETRN kommt unter Umständen zum Einsatz, wenn SX-GATE über eine Wahlleitung mit fester IP-Adresse an das Internet angebunden ist. Dabei versucht der Mail-Server des Providers

eingehende E-Mails direkt mit SMTP an SX-GATE zuzustellen. Ist dieser jedoch gerade nicht erreichbar, weil z.B. die Wählleitung nicht online ist, werden alle eingehenden E-Mails auf dem Mail-Server des Providers in einer Warteschlange zwischengespeichert. Geht die Wählleitung online, so kann SX-GATE dies dem Mail-Server des Providers mit Hilfe des ETRN-Befehls anzeigen. Der Befehl veranlasst, dass nun erneut versucht wird, die wartenden E-Mails zuzustellen.

14.6.2-A OAuth2

Um Mails von einem "Microsoft 365"-Konto abholen zu können, ist eine Authentifizierung mit dem OAuth2-Verfahren notwendig. Der SX-GATE nutzt dabei den "Client-Credentials Flow". Vergleichbar mit einem Benutzerkonto wird dazu in "Entra ID" (ehemals Azure Active-Directory) für den SX-GATE Mail-Client eine Anwendung mit zugehörigem Anwendungskennwort angelegt. Die Anwendung erhält die Berechtigung für den POP3- bzw. IMAP4-Zugriff. Abschließend muss der Anwendung mit Hilfe der Exchange-Verwaltungsshell Zugriff auf die gewünschten Postfächer gewährt werden. Nun kann der SX-GATE mit seiner Anwendungs-ID und dem Anwendungskennwort einen kurzlebigen Zugriffstoken abrufen und mit diesem die Mails aus allen entsprechend konfigurierten Postfächern abrufen.

Die Schritte im Einzelnen:

Anwendung anlegen

Melden Sie sich bei Microsoft Azure mit einem Administratorenkonto an (<https://portal.azure.com>).

Wählen Sie "Microsoft Entra ID", dann "Verwalten > App-Registrierungen".

Klicken Sie auf "Neue Registrierung" und vergeben Sie einen beliebigen Namen. Lassen Sie die weiteren Einstellungen unverändert und legen Sie die Anwendung mit "Registrieren" an.

Jetzt links im Menü "Zertifikate & Geheimnisse" anklicken. Unter "Geheime Clientschlüssel" generieren Sie mit "Neuer geheimer Clientschlüssel" ein Anwendungskennwort, das Sie mit "Hinzufügen" abspeichern.

Kopieren Sie nun sofort das Kennwort in der Spalte "Wert" durch Klick auf das Kopiersymbol hinter dem Kennwort. Zu einem späteren Zeitpunkt ist dies nicht mehr möglich. Übertragen Sie das Kennwort in die OAuth2-Konfiguration des SX-GATE Mail-Clients bzw. speichern Sie es an einem sicheren Ort zwischen, um es später im SX-GATE zu konfigurieren.

Klicken Sie nun im Menü links auf "Verwalten > API-Berechtigungen", dann "Berechtigung hinzufügen". Wählen Sie "Von meiner Organisation verwendete APIs" und geben Sie im Suchfeld "Office" ein. Wählen Sie "Office 365 Exchange Online" aus. Klicken Sie auf "Anwendungsberechtigungen". Öffnen Sie die Rubriken "IMAP" und/oder "POP" und selektieren Sie die jeweilige "AccessAsApp"-Berechtigung. Schließen Sie das Fenster mit "Berechtigungen hinzufügen". Klicken Sie abschließend auf "Administratorzustimmung für DOMAINNAME erteilen".

Klicken Sie im linken Menü auf "Übersicht" und übertragen Sie die "Anwendungs-ID (Client)" und die "Verzeichnis-ID (Mandant)" in die OAuth2-Konfiguration des

SX-GATE Mail-Clients bzw. speichern Sie die Werte zwischen, um sie später im SX-GATE zu konfigurieren.

Verlassen Sie nun die Anwendungs-Registrierung, indem Sie oben links auf "Home" klicken.

Öffnen Sie erneut "Microsoft Entra ID" und wählen Sie diesmal "Verwalten > Unternehmensanwendungen". Kopieren Sie sich für später die "Objekt-ID" der zuvor angelegten Anwendung. Hier wird auch nochmal die "Anwendungs-ID" angezeigt. Sie benötigen beide Werte gleich für die Exchange-Konfiguration.

Zugriffsrechte im Exchange erteilen

Prüfen Sie zunächst im "Microsoft 365 admin center" (<https://admin.microsoft.com>), ob für die gewünschten Benutzer der POP3- bzw. IMAP4-Zugriff erlaubt ist. Wählen Sie dazu unter "Benutzer > Aktive Benutzer" den jeweiligen Benutzer aus. Nach Klick auf "E-Mail" werden Ihnen unter "E-Mail Apps" die Berechtigungen angezeigt.

Verbinden Sie sich nun mit der Exchange Management-Shell. Öffnen Sie dazu die Powershell und installieren Sie falls notwendig das Modul zum ExchangeOnline-Management ("Install-Module ExchangeOnlineManagement"). Ggf. muss das Modul noch importiert werden ("Import-Module ExchangeOnlineManagement").

Die Verbindung wird aufgebaut mit "Connect-ExchangeOnline -UserPrincipalName ADMINBENUTZER". Um die Verbindung über einen Proxy herzustellen, können Sie diesen zuvor mit z.B. "\$proxyoptions = New-PSSessionOption -ProxyAccessType ieconfig" in einer Variablen speichern. Ergänzen Sie dann den Connect-Befehl mit der Option "-PSSessionOption \$proxyoptions".

Registrieren Sie einmalig die Anwendung mit "New-ServicePrincipal -AppId ANWENDUNGS_ID -ServiceId OBJEKT_ID", wobei Sie ANWENDUNGS_ID und OBJEKT_ID mit den zuvor kopierten Werten ersetzen.

Ist die Anwendung bereits registriert, können Sie die Objekt-ID, hier "ServiceId" genannt, jederzeit mit "Get-ServicePrincipal" wieder abrufen.

Bei jedem Benutzerpostfach, das der SX-GATE abrufen soll, muss nun der Zugriff für diese ID freigeschaltet werden: "Add-MailboxPermission -Identity BENUTZER -User OBJEKT_ID -AccessRights FullAccess". Als BENUTZER geben Sie dessen E-Mail-Adresse an.

Zugangsdaten im SX-GATE hinterlegen

Sofern noch nicht geschehen, tragen Sie die zuvor kopierten Werte in die OAuth2-Konfiguration des SX-GATE Mail-Clients ein.

Bei der Konfiguration der einzelnen Benutzerpostfächer wird kein Passwort abgefragt, da sich SX-GATE mit seinem Anwendungskennwort bei allen Benutzerpostfächern anmelden kann.

Mandant (Tenant)

Tragen Sie hier den Namen oder die ID Ihres "Entra ID"-Mandanten ein.

OAuth2 Anwendungs-ID

Geben Sie hier die Anwendungs-ID (Client-ID) ein, die Sie in "Entra ID" für den SX-GATE Mail-Client registriert haben.

Geheimer OAuth2-Clientschlüssel

Geben Sie hier das Anwendungskennwort ein, das Sie im Azure Active-Directory für den SX-GATE Mail-Client generiert haben.



Das Anwendungskennwort ist im Azure AD mit einer begrenzten Gültigkeitsdauer versehen. Bitte denken Sie stets daran, rechtzeitig ein neues Anwendungskennwort im Azure AD festzulegen und in den SX-GATE zu übertragen.

14.6.2-B Postfächer

Postfächer

In diesem Eingabebereich definieren Sie, welche Konten vom POP-Server des Providers abzurufen sind und wie diese lokal zugestellt werden sollen.

Um ein neues Konto zu definieren, geben Sie zunächst die Zugangsdaten ein, die Sie von Ihrem Provider erhalten haben. Geben Sie danach die gewünschte Adresse des Empfängers an. Um ein Sammelpostfach (multi-drop) zu definieren, lassen Sie den Benutzernamen des Empfängers leer oder tragen Sie das Zeichen "*" ein. Wenn Sie beim Empfänger keine Domain angeben, so wird "localhost" angenommen. Standardmäßig erfolgt die weitere Zustellung mit Hilfe des SX-GATE Mail-Servers. Alternativ können Sie einen abweichenden Mail-Server angeben, an den die abgerufenen E-Mails direkt weitergegeben werden.



Werden E-Mails nicht über den Mail-Server des SX-GATE sondern direkt an einen anderen Mail-Server weitergeleitet, so werden damit alle Funktionen und Sicherheitsmechanismen des SX-GATE Mail-Servers umgangen. Dazu gehören insbesondere Virenskan, Attachment-Filter und SPAM-Filter.

14.6.2-C Multi-drop-Parameter

Die Einstellungen auf dieser Seite sind ausschließlich für Sammelkonten (multi-drop) relevant.

Ausgewerteter Mail-Header

Um den ursprünglichen Empfänger einer E-Mail aus einem Sammelpostfach zu ermitteln, werden die Kopfzeilen der E-Mail (Header) nach E-Mail-Adressen mit der richtigen Domain abgesucht. Hier können Sie wählen, welche Header zu durchsuchen sind. Die Grundeinstellung "Received:" ist dabei zwar am unzuverlässigsten, dafür aber fast immer verfügbar. Prüfen Sie, ob einer der anderen hier angebotenen Header ein besseres Resultat liefert.



In der Einstellung "Received:" werden ferner die folgenden Header in der angegebenen Reihenfolge geprüft: "Resent-To:", "Resent-Cc:", "Resent-Bcc:", "To:", "Cc:", "Bcc:" und "Apparently-To:". Der erste Header mit passender E-Mail-Adresse wird verwendet.

Anzahl zu überspringender Header

Normalerweise wird stets das erste Vorkommen eines Headers geprüft. Sind grundsätzlich mehrere Header vom gleichen Typ in den E-Mails enthalten, wobei der erste Header nicht den gewünschten Wert enthält, so können Sie hier festlegen, wie viele dieser Header zu überspringen sind.

Präfix vor Empfängernamen

Abhängig vom POP-Server des Providers kann es vorkommen, dass in den Mail-Headern zwar die Mail-Adresse des Empfängers verzeichnet ist, jedoch stets ein bestimmter Text vorangestellt wurde. Geben Sie diesen hier ein, um SX-GATE zu veranlassen, den Präfix automatisch zu entfernen. So wird die Mail dann an den richtigen Empfänger zugestellt.

14.6.2-D Multi-drop-Domains

Die Einstellungen auf dieser Seite sind ausschließlich für Sammelkonten (multi-drop) relevant.

Um den ursprünglichen Empfänger einer E-Mail aus einem Sammelpostfach zu ermitteln, werden die Kopfzeilen der E-Mail (Header) nach E-Mail-Adressen mit der richtigen Domain abgesucht. Hier stellen Sie ein nach welchen Domains zu suchen ist und wie mit diesen weiter zu verfahren ist.



Bei der Suche nach E-Mail Adressen mit passender Domain, werden auch alle Subdomains der hier gelisteten Domains als Treffer akzeptiert.



Wenn Sie keine Domain eingeben, werden alle E-Mails aus Sammelkonten an den Administrator zugestellt.

Nach folgenden Domains suchen und durch die beim Postfach angegebene Domain ersetzen

Wird in den untersuchten Kopfzeilen eine Adresse mit einer der hier angegebenen Domains gefunden, so wird von der E-Mail-Adresse lediglich der Name des Empfängers übernommen. Als Domain wird die Domain verwendet, die beim Anlegen des Sammelkontos als Empfänger-Domain eingestellt wurde.

Am Einfachsten lässt sich dies anhand eines Beispiels erklären. Gehen wir davon aus, in dieser Liste sei die Domain "example.org" eingetragen. In einer E-Mail wird die Adresse "test@www.example.org" gefunden. Da eingetragene Domains stets auch auf Subdomains passen, handelt es sich tatsächlich um einen Treffer. Als ursprünglicher Empfänger wurde also "test" ermittelt. Bei der Spezifikation des Sammelkontos ist als Empfänger "*@example.com" angegeben. Daher wird die E-Mail nun an die Adresse "test@example.com" ausgeliefert.

Nach folgenden Domains suchen und diese unverändert weitergeben

Wird in den untersuchten Kopfzeilen eine Adresse mit einer der hier angegebenen Domain gefunden, so wird die komplette Adresse unverändert als Empfänger übernommen.

Gehen wir im Beispiel von den selben Einstellungen wie im vorigen Beispiel aus. Diesmal ist die Domain "example.org" jedoch in dieser Liste eingetragen. Wie zuvor ist auch hier die E-Mail-Adresse "test@www.example.org" trotz der Subdomain ein Treffer. Die Mail wird nun jedoch an "test@www.example.org" gesendet.

14.6.2-E Server Einstellungen

Port

Die Port, zu dem sich SX-GATE verbindet, ist abhängig vom gewählten Protokoll und der Option "Verschlüsselten Port verwenden (SSL)". Bei POP3 wird der Port 110 bzw. der verschlüsselte Port 995 kontaktiert. Bei IMAP sind es die Ports 143 bzw. 993. Sie können hier jedoch auch einen abweichenden Port konfigurieren.

Verbindung verschlüsseln, Serverzertifikat verifizieren

Mit dieser Einstellung wird eine verschlüsselte Verbindung forciert. Die Verbindung schlägt fehl, wenn der Server keine Verschlüsselung unterstützt oder das Server-Zertifikat nicht erfolgreich überprüft werden kann.

Verschlüsselten Port verwenden (SSL)

Wenn der Provider den SSL-verschlüsselten Zugriff auf seinen Mail-Server via TCP-Port 995 (POP3) bzw. 993 (IMAP4) anbietet, kann dies nach Aktivierung dieses Schalters genutzt werden.



Auch wenn diese Option nicht aktiviert ist, wird auf eine verschlüsselte Verbindung gewechselt, sofern der Server mitteilt, dass er auch verschlüsselte Kommunikation unterstützt. Die gesamte Kommunikation erfolgt über Port 110 (POP3) bzw. 143 (IMAP4).

Authentifizierung mit Zertifikat

Zusätzlich zur Passwort-Authentifizierung kann sich SX-GATE auch mit einem Client-Zertifikat gegenüber dem Mail-Server ausweisen, sofern die Verbindung verschlüsselt ist. Ein individuelles Zertifikat je Postfach ist bislang nicht möglich.

Wählen Sie hier einen der Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.

Nachrichten auf Server belassen

Wenn diese Option aktiviert ist, werden Mails nach dem Herunterladen nicht gelöscht.



Diese Option ist in erster Linie für kurzzeitiges Debugging gedacht. Diese Einstellung darf nur dann über einen längeren Zeitraum aktiv bleiben, wenn die Postfächer auf anderem Wege regelmäßig bereinigt werden.

Nur neue Nachrichten abrufen

Mit dieser Einstellung werden nur neue Nachrichten abgerufen. Bereits abgeholte Nachrichten werden ignoriert und verbleiben auf dem POP-Server.

Max. Anzahl Nachrichten pro Verbindung

Dieser Parameter legt fest, wie viele Nachrichten maximal über eine Verbindung abgeholt werden. Wenn sich mehr E-Mails im Postfach des POP-Servers befinden, holt SX-GATE diese erst beim den nächsten Abholzyklen ab.



Erst mit dem ordnungsgemäßen Ende der Verbindung werden die abgerufenen Mails auf dem Server gelöscht. Bricht die Verbindung vorzeitig ab, so werden alle Mails erneut heruntergeladen und zugestellt. Der Parameter sollte daher nur in Ausnahmefällen verändert werden (Grundeinstellung: 50).



Wird ein zu hoher Wert für diesen Parameter eingestellt, kann dies im ungünstigsten Fall zu einer Überlastung des Systems führen!

14.6.2-F ETRN

ETRN aufrufen für Domain

Geben Sie hier alle Domains an, die mit Hilfe von ETRN Kommandos vom ausgewählten Server abgerufen werden sollen.

14.7 Web-Proxy

Dieser Proxy-Dienst ist für den Browser-Zugriff auf das Internet gedacht. Unterstützt werden die Protokolle HTTP, HTTPS und FTP (nur Download). Anfragen werden auf Port 8080 entgegengenommen. Konfigurieren Sie Ihre Web-Browser bitte entsprechend wenn der Proxy nicht transparent betrieben wird.

14.7.1 Einstellungen

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.7.1-A Client-Zugriff.....	577
14.7.1-B SX-GATE-Anmeldung.....	579
14.7.1-C NTLM-Anmeldung.....	579
14.7.1-D Windows-Anmeldung.....	581
14.7.1-E LDAP-Anmeldung.....	581
14.7.1-F Anmeldeoptionen.....	583
14.7.1-G PAC-Datei.....	584
14.7.1-H Ziel-Ports.....	585
14.7.1-I ICAP.....	586
14.7.1-J Bandbreitenbegrenzung.....	587
14.7.1-K Provider-Proxy.....	588
14.7.1-L Proxy Auswahl.....	589
14.7.1-M Cache-Parameter.....	590
14.7.1-N Erweitert.....	592

Benutzeranmeldung

Mit Hilfe dieser Optionen ist es möglich, den Zugriff via Proxy auf das Internet nur nach Benutzeranmeldung zu erlauben. Der Proxy muss dazu im Browser konfiguriert sein.



Bei transparentem Proxying (Umleitung der Verbindung in der Firewall statt Konfiguration des Browsers) erfolgt grundsätzlich keine Authentifizierung.

Es stehen verschiedene Möglichkeiten der Authentifizierung zur Auswahl:

keine

Der Zugriff auf das Internet via Proxy ist ohne Anmeldung möglich. Es ist in diesem Falle nicht notwendig, Benutzerkonten für den Proxy-Zugriff (Gruppe "system-proxy") anzulegen.

an SX-GATE

Bei Auswahl dieser Option ist der Zugriff in das Internet möglich, wenn sich der Benutzer mit Kennwort authentifiziert hat. Die Konten und Passwörter sind dazu in der SX-GATE Benutzerverwaltung einzurichten (Gruppe "system-proxy").

an Windows-Domäne (NTLM)

Hier wird der Benutzer automatisch mit seiner derzeitigen Windows-Domänenanmeldung authentifiziert. Die manuelle Eingabe von Benutzername und Kennwort entfällt in der Regel.

an LDAP-Server

Ist diese Option gewählt, so ist der Zugriff auf das Internet möglich, wenn der Benutzer sich gegenüber einem LDAP-Server authentifizieren kann. Das Anlegen von Benutzern auf SX-GATE ist nicht zwingend erforderlich, wenn Sie von dieser Authentifizierungs-Methode Gebrauch machen wollen.

an Windows (veraltet)

Ist diese Option gewählt, so ist der Zugriff auf das Internet möglich, wenn der Benutzer mit seinem Windows-Benutzernamen und seinem Windows-Kennwort Zugriff auf eine bestimmte Datei hat. Diese Datei wird auf dem Primären-Domain-Controller (PDC) Ihrer Windows-Domain hinterlegt. Mit Hilfe der Dateizugriffsrechte des PDC steuern Sie den Zugriff auf diese Datei. Das Anlegen von Benutzern auf SX-GATE ist nicht zwingend erforderlich, wenn Sie von dieser Authentifizierungs-Methode Gebrauch machen wollen.

14.7.1-A Client-Zugriff

Proxy-Zugriff für folgende Quell-IP-Adressen

Nutzen Sie diese Einstellung um nur bestimmten IP-Adressen Zugriff auf den Proxy-Server zu geben.

Nutzung als transparenter Proxy erlauben

Der SX-GATE Web-Proxy kann auch transparent betrieben werden. HTTP-Zugriffe auf Port 80 eines Web-Server im Internet können dann mit Hilfe einer entsprechenden Firewall-Regel an den Web-Proxy umgeleitet werden ohne die Client-Konfiguration anzupassen. Wird diese Option aktiviert, so wählen Sie bitte anschließend unter "Module > Firewall > Regeln" die Schnittstelle aus, über die der Client die Verbindung aufnimmt. In der Regel ist dies SX-GATE's LAN-Schnittstelle "eth0". Aktivieren Sie dort die Umleitung von Verbindungen zu Port 80 auf dem Reiter (Tab) "Transp. Proxy".



Bei transparenten Zugriffen wird grundsätzlich keine Benutzeranmeldung am Proxy verlangt.

Schlüssel/Zertifikat für TLS-Port

Die Kommunikation zwischen Client und Proxy kann verschlüsselt erfolgen. Wählen Sie dazu einen der Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.



Die Browser müssen das ausgewählte Zertifikat als vertrauenswürdig akzeptieren.

Der Proxy-Port für verschlüsselte Verbindungen ist 8443. In den Proxy-Einstellungen der Browser wird üblicherweise keine Option angeboten, um verschlüsselte Verbindungen zu aktivieren. Die Browser müssen stattdessen über automatische Proxy-Konfiguration (PAC-Datei, WPAD) konfiguriert werden.



Die vom SX-GATE bereitgestellte PAC-Datei wird automatisch angepasst, sobald der TLS-Port aktiviert wird.

TLS-Protokoll

Wählen Sie hier die Verschlüsselungsstärke für die verschlüsselte Kommunikation mit dem Proxy aus.



Im Rahmen der Produktpflege werden die mit der jeweiligen Auswahl verbundenen Parameter von Zeit zu Zeit angepasst.

veraltet

Um Kompatibilität mit älteren Clients zu gewährleisten, werden in dieser Einstellung AES-Algorithmen mit dem nicht mehr empfohlenen Cipher-Block-Chaining CBC und dem veraltete Hash-Algorithmus SHA1 aktiviert. Die minimale TLS-Version ist 1.0.

kompatibel

Wählen Sie diese Einstellung für weitreichende Kompatibilität mit älteren Client-Systemen. Der veraltete Hash-Algorithmus SHA1 ist dabei aktiviert. Die minimale TLS-Version ist 1.2.

aktuell

In dieser Einstellung werden nur noch halbwegs aktuelle Client-Systeme unterstützt. Es wird mindestens TLS 1.2 vorausgesetzt. Wählen Sie diese Option für hohe Sicherheit. Unter Windows sind Internet-Explorer 11, Edge oder ein alternativer Browser wie Chrome oder Firefox erforderlich.

maximal

Erfordert TLS 1.3.

14.7.1-B SX-GATE-Anmeldung

Die Einstellungen in diesem Bereich sind nur dann wirksam, wenn Benutzerauthentifizierung im Proxy aktiviert ist und als Modus die Option "an SX-GATE" gewählt wurde.

Authentifizierungsmethoden

Legen Sie hier fest, über welche Authentifizierungsmethoden sich Clients anmelden können.

Basic

Dies ist die einfachste Authentifizierungsmethode.



In diesem Modus wird das Kennwort vom Browser zum Proxy praktisch im Klartext übertragen. Mit entsprechenden Netzwerk-Analyse Programmen lässt es sich abhören.

Digest

Wählen Sie diese Einstellung wenn das Kennwort grundsätzlich gesichert übertragen werden soll.

Digest + Basic

In dieser Einstellung bleibt die Kompatibilität mit Clients gewahrt, die Digest-Authentifizierung nicht unterstützen. Clients die beide Authentifizierungsmethoden kennen, bevorzugen automatisch Digest.

14.7.1-C NTLM-Anmeldung

Diese Einstellung ist nur bei der Authentifizierungsoption "an Windows-Domäne (NTLM)" verfügbar.

Das Anlegen von Konten auf dem SX-GATE in der Gruppe "system-proxy" ist für die reine Anmeldung nicht erforderlich. Sollten Sie jedoch den URL-Filter verwenden,

so kann es notwendig werden, manche oder alle Benutzer auch auf dem SX-GATE anzulegen. Nur so ist es möglich, für einzelne Gruppen und damit für bestimmte Benutzer abweichende Zugriffsrechte festzulegen.

Erlaubte Benutzer

Wählen Sie hier aus, welche Benutzer Zugriff auf den Proxy erhalten sollen.

Domänen-Konto erstellen

Um zukünftig die Anmeldung an die Windows-Domäne delegieren zu können, muss zunächst für SX-GATE ein Computer-Konto in der Domäne erstellt werden. Mit Hilfe dieses Assistenten können Sie die Windows-Domäne konfigurieren und das Konto anlegen.

Windows-Domäne

Um in der Windows-Domäne ein Computer-Konto erstellen zu können, sind Administratoren-Rechte erforderlich. Bitte geben Sie die Zugangsdaten eines Windows Administrators ein.



Dies ist ein einmaliger Vorgang. Die Zugangsdaten werden nicht gespeichert.

IP-Adresse des ActiveDirectory-Servers

Um SX-GATE an ein ActiveDirectory anzubinden, geben Sie hier bitte die IP-Adresse des Servers ein. Falls Sie die Anbindung im NT4-Kompatibilitätsmodus betreiben möchten, geben Sie bitte stattdessen den NetBIOS-Namen Ihrer Windows-Domäne ein.



Der NetBIOS-Domänen-Name wird u.a. in der "Netzwerkumgebung" angezeigt - ggf. unter der Bezeichnung "Arbeitsgruppe". Ein NetBIOS-Domänen-Name enthält in der Regel keinen Punkt (z.B. "EXAMPLE"). Im Gegensatz dazu entspricht der Active-Directory Domain-Name einer Internet-Domain und enthält daher zumindest einen Punkt (z.B. "example.com").

Administrator Login

Geben Sie hier bitte den Kontonamen eines Windows Administrators ein.

14.7.1-D Windows-Anmeldung

Diese Einstellung ist nur bei der Authentifizierungsoption "an Windows (veraltet)" verfügbar.

Das Anlegen von Konten auf dem SX-GATE in der Gruppe "system-proxy" ist für die reine Anmeldung nicht erforderlich. Sollten Sie jedoch den URL-Filter verwenden, so kann es notwendig werden, manche oder alle Benutzer auch auf dem SX-GATE anzulegen. Nur so ist es möglich, für einzelne Gruppen und damit für bestimmte Benutzer abweichende Zugriffsrechte festzulegen.

Windows-Domain

Tragen Sie hier Ihre Windows-Domain ein. Erstellen Sie ferner auf der NETLOGON-Freigabe Ihres Primary-Domain-Controllers (PDC) eine Datei mit Namen "proxyauth". Diese Datei muss ausschließlich das Wort "allow" enthalten. Vergeben Sie nun Leseberechtigung auf diese Datei für all die Benutzer, die Zugriff auf das Internet erhalten sollen.

14.7.1-E LDAP-Anmeldung

Dieser Eingabebereich steht nur dann zur Verfügung, wenn die Authentifizierungsmethode "an LDAP-Server" ausgewählt wurde.

Das Anlegen von Konten auf dem SX-GATE in der Gruppe "system-proxy" ist für die reine Anmeldung nicht erforderlich. Sollten Sie jedoch den URL-Filter verwenden, so kann es notwendig werden, manche oder alle Benutzer auch auf dem SX-GATE anzulegen. Nur so ist es möglich, für einzelne Gruppen und damit für bestimmte Benutzer abweichende Zugriffsrechte festzulegen.

LDAP-Server

Tragen Sie bitte in dieses Feld die IP-Adresse oder den DNS-Namen des LDAP-Servers ein.

Verschlüsselte LDAP-Verbindung

Aktivieren Sie sicheres LDAP für verschlüsselte Kommunikation zwischen Web-Proxy und LDAP-Server.



Die Kommunikation zwischen Browser und Web-Proxy ist nicht verschlüsselt. Das Kennwort des Benutzers wird hier quasi im Klartext übertragen.

Servertyp

Wählen Sie hier nun den Typ des LDAP-Servers. Die verschiedenen Typen unterscheiden sich dahingehend, wie ein Benutzer im LDAP-Verzeichnis gefunden werden kann.

anderer (UID)

In dieser Einstellung wird nach Objekten gesucht, die den Anmeldenamen als Attribut "UID" führen. Diese Konvention wird von den meisten LDAP-Servern verwendet.

MS ActiveDirectory (SAM)

Bei der Auswahl dieser Einstellung wird das Benutzerobjekt anhand des Attributs "SAMAccountName" im ActiveDirectory gesucht. In der Benutzerverwaltung wird dieses Attribut als "BenutzeranmeldeName Windows NT 3.5x/4.0" geführt. Bitte beachten Sie, dass die Suche im ActiveDirectory mit dem Leserecht verknüpft ist. Ist der lesende Zugriff auf ein Benutzerobjekt nicht erlaubt, so ist eine Anmeldung als dieser Benutzer nicht möglich.

MS ActiveDirectory (CN)

Wählen Sie diesen Typ, wenn das Benutzer-Objekt anhand des Attributs "CN" identifiziert wird. Im Microsoft ActiveDirectory entspricht das Attribut "CN" dem nachträglich nicht mehr änderbaren Namen für das Benutzerobjekt. Die Verwendung dieses Attributes als Benutzerkennung kann problematisch werden, da hier oft Sonderzeichen und Leerzeichen enthalten sind.

LDAP-Suchpfad

Für die Verwendung der LDAP-Authentifizierung ist ferner die Angabe des Suchpfades erforderlich. Geben Sie hier den für Ihren LDAP-Server benötigten Pfad ein. In diesem Container müssen die Benutzerobjekte abgelegt sein. Beispiele hierzu:

- CN=users,DC=ad,DC=example,DC=com
- OU=SBSUsers,OU=Users,OU=MyBusiness,DC=example,DC=com

Hierarchische Suche

Aktivieren Sie die hierarchische Suche, wenn Benutzerobjekte nicht nur unmittelbar im zuvor angegebenen Suchpfad gefunden werden sollen sondern auch hierarchisch tiefer liegende Objekte einbezogen werden müssen. Die Suche im LDAP-Server kann bestimmte Berechtigungen erfordern.

Erlaubte Benutzer

Die Menge der erlaubten Benutzer kann zusätzlich über das "memberOf"-Attribut von LDAP-Benutzer-Objekten eingeschränkt werden. Im Microsoft Active Directory entspricht dies der Mitgliedschaft eines Benutzers in einer Gruppe. Geben Sie den vollständigen DN der Gruppe an (z.B. "CN=internetbenutzer,CN=users,DC=ad,DC=example,DC=com"). Wenn Sie dieses Eingabefeld

leer lassen, können sich alle im LDAP-Suchpfad gefundenen Benutzer am Proxy anmelden.

Benutzername für Suche im LDAP

Die hierarchische Suche bzw. die Suche des Benutzerobjekts anhand des Attributs "SAMAccountName" erfordert die Berechtigung, den LDAP-Suchpfad anonym durchsuchen zu dürfen (im ActiveDirectory bedeutet dies Leseberechtigung für "Jeder"). Ist dies nicht gegeben oder gewünscht, so kann sich SX-GATE am LDAP-Server anmelden. Geben Sie dazu hier den Benutzernamen für das LDAP-Konto ein.



Bitte beachten Sie, dass Sie als LDAP-Konto den kompletten distinguished Name (DN) des Kontos eingeben müssen (z.B. "CN=proxyuser,CN=users,DC=ad,DC=example,DC=com").

14.7.1-F Anmeldeoptionen

Diese Maske ist nicht verfügbar, wenn die Proxy-Authentifizierung deaktiviert ist.

Zugriff ohne Benutzeranmeldung auf folgende Domains

Geben Sie hier Domain-Namen oder IP-Adressen ein, wenn für den Zugriff auf diese Adressen keine Authentifizierung erforderlich sein soll. Die Angabe von Domains schließt dabei Subdomains mit ein. So ermöglicht z.B. die Angabe von "example.com" auch den Zugriff auf "www.example.com" und "ftp.example.com" ohne Benutzeranmeldung.



Zugriffe auf den Hostnamen von SX-GATE sowie die SX-GATE eth0-IP sind immer ohne Proxy-Anmeldung möglich.

Viele Internet-Seiten binden Elemente von anderen Internet-Domains ein. Um die Authentifizierung auf einer bestimmten Internet-Seite komplett zu deaktivieren, müssen alle von dieser Seite referenzierten Domains hier eingetragen werden.

Zugriff ohne Benutzeranmeldung für folgende Clients

Verbindungen von Adressen dieser Liste dürfen den Proxy ohne Benutzeranmeldung verwenden.

Mehrfachanmeldung eines Benutzers verhindern

Dieser Schalter bindet ein Benutzeranmeldung für 10 Minuten an die IP-Adresse von der aus der letzte Zugriff stattgefunden hat. Erfolgt innerhalb dieser Zeitspanne ein Zugriff von einer anderen IP-Adresse aus, besteht die Möglichkeit, dass der Benutzer seine Anmeldedaten weitergegeben hat. Der Zugriff wird daher gesperrt.

14.7.1-G PAC-Datei

In den Proxy-Einstellungen der Browser bzw. in den Active Directory Gruppenrichtlinien kann die Adresse einer Proxy-Autoconf-Datei (PAC-Datei) hinterlegt werden. Der SX-GATE Administrations-Webserver bietet eine passende Datei an. Um diese zu nutzen, tragen Sie bitte die Adresse "http://<SX-GATEs LAN-IP>:8000/proxy.pac" ein.

Die vom SX-GATE angebotene PAC-Datei instruiert den Browser, alle Verbindungen über den SX-GATE Web-Proxy zu leiten. Ausgenommen sind Verbindungen zum Rechner auf dem der Browser läuft (IP 127.0.0.1 bzw. primäre IP dieses Rechners), Verbindungen zum SX-GATE (LAN-IP bzw. vollständiger Hostname gemäß "System > Grundeinstellungen") sowie Verbindungen zu einem Hostnamen ohne Domainangabe. Weitere Ausnahmen können über die folgenden Eingabefelder definiert werden.

Verbindung zu Ziel-Domain

Je Domain lässt sich hier festlegen, ob der Browser eine direkte Verbindung aufbauen oder den SX-GATE-Proxy nutzen soll. Dabei ist die Reihenfolge der Einträge entscheidend. Es ist auch möglich, einzelne IP-Adressen einzugeben. Da keine DNS-Auflösung stattfindet, wirkt sich dies jedoch nur dann aus, wenn im Browser explizit eine dieser IP-Adressen als Verbindungsziel eingegeben wurde.

Netzwerke mit direkter Verbindung

Tragen Sie hier IP-Netzwerke ein, zu denen der Browser direkte Verbindungen herstellen soll. Der Proxy wird für diese Verbindungen nicht genutzt. Meist wird im Browser keine IP-Adresse sondern ein Rechnernamen als Verbindungsziel angegeben. Der Browser muss daher mit Hilfe einer DNS-Anfrage zu jedem Rechnernamen die zugehörige IP-Adresse nachschlagen.



Werden ausschließlich einzelne Server über IP-Adresse angesprochen, empfehlen wir deren IP-Adresse unter "Verbindung zu Ziel-Domain" einzutragen. Der Browser muss keine DNS-Anfragen stellen, solange hier kein Netzwerk eingetragen ist.

Proxy-Adresse im Cluster-Betrieb

Wählen Sie hier bitte aus, welche Proxy-Adresse im Cluster-Betrieb in den PAC-Dateien eingetragen werden soll, die Master und Backup verteilen.

Individuelle IP des jeweiligen Knotens

Der Client verbindet sich zum Proxy des Cluster-Knotens, von dem er die PAC-Datei bezogen hat.

Gemeinsame Cluster-IP

Der Client verbindet sich zum Proxy des aktiven Cluster-Knotens. Bei einem Failover wechselt die IP auf den jeweils anderen Cluster-Knoten. Die Verbindung des Clients zum Proxy bricht daher ab und muss vom Client neu aufgebaut werden.

Master-IP mit Fallback auf Backup-IP

Der Client verbindet sich bevorzugt zum Proxy auf dem Master-Knoten. Im Falle eines Cluster-Failovers läuft die Verbindung weiter über den Master, sofern die Verbindung noch funktioniert. Ist der Master nicht erreichbar, verbindet sich der Client zum Backup-Knoten.

Backup-IP mit Fallback auf Master-IP

Wie vor, hier wird jedoch der Backup bevorzugt, so dass dieser aktiver genutzt wird.

Benutzerdefinierter Eintrag

Tragen Sie hier einen DNS-Namen ein, der auf die individuellen IPs beider Cluster-Knoten verweist um über DNS-Round-Robin ein Loadbalancing zu erreichen. Auch hier bricht die Proxy-Verbindung bei einem Cluster-Failover nicht ab. Ist der Proxy auf der aktuell ausgewählten IP nicht mehr erreichbar, wechselt der Client zum Proxy auf der anderen IP.

14.7.1-H Ziel-Ports

Erlaubte Ziel-Ports für unverschlüsselte Verbindung

Hier schränken Sie ein, auf welche Server-Ports via Proxy zugegriffen werden darf. Von Bedeutung sind hier insbesondere der Port 80 (HTTP) und 21 (FTP). Auf welche Server-Ports der verschlüsselte Zugriff erlaubt sein soll, wird nicht mit dieser Einstellung festgelegt.

Erlaubte CONNECT Ziele

Mit CONNECT bietet der Proxy seinen Clients die Möglichkeit, nahezu beliebige Protokolle über den Proxy zu tunneln. Mit CONNECT werden z.B. auch verschlüsselte Verbindungen (HTTPS) abgewickelt.



In der Regel ist es ausreichend, hier den Port 443 (HTTPS) freizugeben. Geben Sie hier keine unnötigen Ziel-Ports frei um Missbrauch vorzubeugen.



Die Inhalte von Verbindungen, die mit Hilfe des CONNECT-Befehls aufgebaut wurden, können vom Content-Filter nur dann untersucht werden, wenn dort das Aufbrechen verschlüsselter Verbindungen aktiviert ist.

CONNECT zu IP-Adressen verbieten

Manche Software-Produkte, darunter viele Peer-to-Peer Clients, missbrauchen die CONNECT-Methode um unbehelligt mit dem Internet kommunizieren zu können. Häufig wird dabei jedoch eine Verbindung zu einer IP-Adresse und nicht zu einem Hostnamen angefordert. Aktivieren Sie diesen Schalter um CONNECTs zu IP-Adressen abzuweisen.



Über den Eingabebereich "Erlaubte CONNECT Ziele" kann der Zugriff auf einzelne IP-Adressen gezielt freigegeben werden.



Sofern Sie auf die SX-GATE Administrations-Oberfläche über den Web-Proxy per IP zugreifen, wird nach der Aktivierung dieses Schalters der Zugriff auf die Administrations-Oberfläche nicht länger möglich sein.

14.7.1-I ICAP

Der SX-GATE Web-Proxy kann externe Filter einbinden, die über eine ICAP-Schnittstelle verfügen.

ICAP-Server für Anfrage-Filter (REQMOD)

Wenn die Anfragen die der Web-Proxy von Browsern erhält durch einen ICAP-Server überprüft werden sollen, geben Sie hier bitte dessen Namen ein.

Aufrufpfad des Anfrage-Filters

Insbesondere wenn der ICAP-Server verschiedene Dienste anbietet, kann es notwendig sein hier einen entsprechenden Zugriffspfad festzulegen. Auch die Angabe von Parametern ist möglich.

ICAP-Server für Antwort-Filter (RESPMOD)

Sollen die Daten die der Web-Proxy von Servern im Internet erhält durch einen ICAP-Server überprüft werden, so geben Sie bitte hier dessen Namen oder IP-Adresse an.

Aufrufpfad des Antwort-Filters

Insbesondere wenn der ICAP-Server verschiedene Dienste anbietet, kann es notwendig sein hier einen entsprechenden Zugriffspfad festzulegen. Auch die Angabe von Parametern ist möglich.

14.7.1-J Bandbreitenbegrenzung

Bandbreitenbegrenzung

Um die Internet-Anbindung nicht zu überlasten, kann die Bandbreite für bestimmte Anfragen limitiert werden. Eine neue Anfrage wird dabei der Reihe nach mit den hier konfigurierten Regeln verglichen und dem Bandbreitenkontingent der ersten passenden Regel zugerechnet.



Liefert keine der Regeln einen Treffer, wird die Bandbreite nicht begrenzt.

Eine Regel setzt sich aus folgenden Parametern zusammen:

Quell-IP/Netzwerk

Um die Regel auf Zugriffe von bestimmten Adressen zu beschränken, wählen Sie bitte ein IP-Objekt aus oder tragen Sie eine IP bzw. eine Netzwerk-Adresse mit zugehöriger Netzmaske ein. Lassen Sie das Feld leer, wenn die Regel für beliebige Quell-Adressen gelten soll. In der Tabelle wird dann ein "*" angezeigt.

Gruppe

Bei aktivierter Proxy-Authentifizierung können Sie durch Auswahl einer Gruppe die Gültigkeit der Regel auf bestimmte Benutzer begrenzen. Benutzer und Gruppen werden im Menü "System > Benutzerverwaltung" konfiguriert. Bei Auswahl von "*" gilt die Regel unabhängig vom Benutzer für jede Anfrage, auch für nicht authentifizierte Anfragen.



Active-Directory-Gruppen stehen hier leider noch nicht zur Verfügung.

Zieldomain

Tragen Sie hier eine Zieldomain ein, um die Regel auf Zugriffe zu dieser Domain (inkl. Subdomains) zu begrenzen. Bei Auswahl von "*" gilt die Regel unabhängig vom Ziel der Anfrage.

Bandbreitenlimit

Legen Sie hier das Bandbreitenkontingent in kbit/s fest, das für die zu dieser Regel passenden Anfragen gilt. Gleichzeitige Verbindungen müssen sich dieses Kontingent teilen.



Ein leeres Eingabefeld bzw. der spezielle Wert "0" stehen für unbegrenzte Bandbreite.

Maximale Größe für Uploads

Diese Einstellung beschränkt die Größe von POST- und PUT-Requests, mit deren Hilfe Dateien oder Formularparameter übermittelt werden.



Die Einschränkung greift nur bei unverschlüsselten Verbindungen.

Maximale Größe für Downloads

Diese Option beschränkt die Größe von Objekten, die über den Proxy heruntergeladen werden dürfen. Im allgemeinen teilt der angesprochene Server die Größe der zu übermittelnden Daten bereits im Voraus mit, so dass eine Fehlermeldung unmittelbar bei der Anfrage generiert werden kann. Ist die Größe der angeforderten Daten jedoch im Vorfeld nicht bekannt, so wird der laufende Download beim Erreichen der Schranke kommentarlos abgebrochen.



Die Einschränkung greift nur bei unverschlüsselten Verbindungen.

14.7.1-K Provider-Proxy

Bietet Ihnen Ihr Provider einen Proxy-Server zur Verwendung an, so können Sie den Web-Proxy des SX-GATE so konfigurieren, dass er sich über den Proxy des Providers in das Internet verbindet. Sofern der Provider einen caching Proxy anbietet, kann dieser den Internetzugang beschleunigen. Die Verwendung des Proxies kann aber auch aufgrund einer Sicherheitsvorschrift zwingend erforderlich sein.

Proxy-Server des Providers

Geben Sie den Namen oder die IP-Adresse des Proxy-Servers in diesem Feld ein. Lassen Sie dieses Feld leer, wenn Sie keinen Provider-Proxy nutzen wollen.

Port

Hier müssen Sie den Port angeben, über den der Provider-Proxy angesprochen wird. Übliche Werte sind 80, 3128 oder 8080.

Ausschließlich verwenden

Falls Ihr Provider eine entsprechend reglementierte Firewall betreibt, kann es nötig werden, alle Anfragen über dessen Proxy-Server abzuwickeln. Aktivieren Sie in diesem Falle bitte diese Option. Andernfalls geht SX-GATE davon aus, dass es sich um einen reinen caching Proxy handelt, der ausschließlich zur Geschwindigkeitssteigerung dient.

In diesem Falle optimiert der SX-GATE Web-Proxy die Weiterleitung von Anfragen. Nur die Anfragen, die möglicherweise im Cache des Provider-Proxys liegen könnten, werden auch an diesen weitergeleitet. Für Anfragen, die ohnehin nicht in einem Cache gespeichert werden dürfen, wird stattdessen eine direkte Verbindung zum Ziel-Web-Server hergestellt. Nicht im Cache ablegbar sind z.B. Anfragen für Dateien die nur nach Benutzeranmeldung heruntergeladen werden dürfen oder verschlüsselte (https) Verbindungen.

Am Provider-Proxy anmelden als Benutzer

Falls erforderlich kann sich der Web-Proxy des SX-GATE auch beim Proxy des Providers authentifizieren. Geben Sie den zugehörigen Benutzernamen und das Kennwort in die entsprechenden Felder ein. Ist keine Anmeldung am Proxy des Providers notwendig, so bleiben diese Felder leer.

14.7.1-L Proxy Auswahl***Proxies für spezielle Ziel-Adressen***

Falls einzelne Domains oder IP-Adressen ausschließlich über bestimmte Proxies zu erreichen sind, können Sie diese hier konfigurieren. Die Angabe einer Ziel-Domain schließt grundsätzlich alle Subdomains mit ein.

Provider-Proxy umgehen für Zugriff auf

Dieser Bereich kann dazu verwendet werden, auf bestimmte Adressen (z.B. aus dem Intranet) stets direkt zuzugreifen. Ein vorgeschalteter Proxy oder Firewall der unter "Proxy-Server des Providers" konfiguriert ist, wird bei Zugriffen auf die hier angegebene Adressen nicht verwendet. Die Angabe von Domains schließt dabei Subdomains mit ein. So ermöglicht z.B. die Angabe von "example.com" auch den direkten Zugriff auf "www.example.com" und "ftp.example.com".



Auf den vollständigen Namen von SX-GATE selbst erfolgt immer direkter Zugriff.

14.7.1-M Cache-Parameter

Zunächst ein paar allgemeine Hinweis zur Zwischenspeicherung von Seiten im Cache des Proxies.

Nicht gespeichert werden u.a. Objekte

- auf die verschlüsselt zugegriffen wird (HTTPS)
- für die der Web-Server eine Benutzeranmeldung verlangt
- für die der Web-Server die Zwischenspeicherung explizit verbietet
- deren Größe einen bestimmten konfigurierbaren Wert überschreiten
- von konfigurierbaren Adressen, für die das Caching deaktiviert wurde

Bereits gespeicherte Seiten werden vom Web-Server neu bezogen, wenn z.B.

- der Browser eine entsprechende Anfrage abschickt (Aktualisieren)
- ein vom Web-Server festgelegtes Verfallsdatum überschritten wurde

Befindet sich ein Objekt ohne definiertes Verfallsdatum schon längere Zeit im Cache, beginnt der Proxy des SX-GATE damit, beim Web-Server nachzufragen, ob sich das Objekt seither verändert hat. Falls ja wird das Objekt neu übertragen. Der Zeitpunkt ab dem der SX-GATE diese Aktualisierungsanfragen sendet ist linear davon abhängig, wie lange die letzte Veränderung der Datei auf dem Web-Server her ist. Als obere Grenze gilt hier jedoch 7 Tage bei FTP und 3 Tage bei HTTP.

Ist die Kapazitätsgrenze des Caches erreicht, so werden verfallene Objekte und die Objekte auf die am längsten nicht mehr Zugriffen wurde gelöscht.

Werden beim Zugriff auf einen Web-Server veraltete Dokumente angezeigt, so nutzen Sie bitte die "Aktualisieren"-Funktion Ihres Browsers.



Zu einer vollständigen Aktualisierung der Anzeige muss im Browser oft eine Tastenkombination gedrückt werden (Internet-Explorer: Strg-F5). Werden dennoch veraltete Seiten angezeigt, so löschen Sie bitte den Cache des Browsers.

Hauptspeicher-Cache

Geben Sie hier an, wie viel Speicherplatz der Proxy-Cache im Hauptspeicher für die Zwischenspeicherung von Seiten nutzen darf. Die Auslieferung von Objekten aus dem Hauptspeicher-Cache erfolgt besonders schnell.

Festplatten-Cache

Hier legen Sie fest wie viel Speicherplatz der Proxy-Cache auf der Festplatte belegen darf. Der Wert "0" deaktiviert den Festplatten-Cache. Physikalisch werden die Seiten im Verzeichnis "/var/spool/squid/" auf der Festplatte abgelegt.



Bevor Sie diesen Wert erhöhen, sollten Sie den freien Speicherplatz in der entsprechenden Festplattenpartition prüfen.

Maximale Objektgröße im Cache

Um eine schnelle Überfüllung des Caches zu vermeiden, werden Dateien die eine bestimmte Größe überschreiten nicht zwischengespeichert. Legen Sie hier diese Größe fest.



Um ein großes Objekt in den Cache einlagern zu können, müssen zuvor oft extrem viele kleine Objekte entfernt werden. Ist dieser Parameter zu hoch eingestellt, kann es in diesen Situationen zu massiven Performance-Einbrüchen kommen.

Dateien von folgenden Adressen nicht im Cache speichern

Damit SX-GATE bestimmte Objekte nie im Cache ablegt, können Sie die entsprechenden Adressen hier hinterlegen. Die Angabe von Domains schließt dabei Subdomains mit ein. So verhindert z.B. die Angabe von "example.com" auch das Einlagern in den Cache für Objekte von "www.example.com" und "ftp.example.com".



Durch das Hinzufügen einer neuen Adresse werden bereits im Cache befindliche Objekte von dieser Adresse nicht entfernt.



Auch Browser verfügen meist über einen Cache für die Zwischenspeicherung von Objekten. Dieser Eingabebereich beeinflusst nicht, ob oder wie lange ein Browser Dateien im Cache vorhält.

Cache löschen

Mit Hilfe dieser Funktion wird sowohl der Hauptspeicher- als auch der Festplatten-Cache des SX-GATE Web-Proxies gelöscht. Der Proxy wird dazu kurzzeitig gestoppt

und mit geleertem Cache wieder gestartet. Erst danach wird begonnen, den ursprünglichen Inhalt des Caches im Hintergrund zu löschen.



Je nach Größe des Caches kann das Löschen im Hintergrund viele Minuten dauern. In dieser Zeit sollte kein Update oder Neustart des SX-GATE durchgeführt werden.

14.7.1-N Erweitert

Mail-Adresse des Administrators

Die hier eingestellte E-Mail-Adresse des Administrators wird angezeigt, wenn der Web-Proxy Anwendern gegenüber eine Fehlermeldung ausgibt.

Name des Web-Proxies

Die hier eingestellte Rechnername wird angezeigt, wenn der Web-Proxy Anwendern gegenüber eine Fehlermeldung ausgibt.

Mailadresse zur Anmeldung für anonymous FTP

Wird anonym auf FTP-Server zugegriffen (anonymous FTP), so verlangt der FTP-Server als Passwort nach einer beliebigen E-Mail-Adresse. Die Adresse, die der SX-GATE Web-Proxy beim Zugriff auf einen solchen Server angibt, wird hier festgelegt.

14.7.2 URL-Filter

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.7.2-A Regeln.....	593
14.7.2-B Optionen.....	595
14.7.2-C Datenbank.....	596

Der URL-Filter überprüft jede Anfrage eines Browsers anhand der angeforderten Adresse (URL). Die Überprüfung der Antwort eines Webserver im Internet wird vom URL-Filter nicht durchgeführt. Dies ist Aufgabe der Web-Proxy Komponente Content-Filter.

URL-Filter aktivieren

Mit Hilfe dieses Schalters wird der URL-Filter aktiviert. Dieser ermöglicht es, den Zugriff auf bestimmte Internet-Adressen zu verbieten.

14.7.2-A Regeln

Benutzergruppen

Wählen Sie, aus welcher Quelle die in den Regeln verwendeten Benutzergruppen bezogen werden.



Wenn die Authentifizierung im Proxy deaktiviert ist oder keine Benutzergruppen im Regelwerk verwendet werden, ist diese Einstellung ohne Belang.

aus SX-GATE Benutzerverwaltung

Benutzergruppen werden im SX-GATE-Menü "System > Benutzerverwaltung" konfiguriert.

aus Windows Domäne

Diese Einstellung erfordert, dass für SX-GATE ein Computer-Konto in der Windows-Domäne verfügbar ist. Das Konto lässt sich anlegen, wenn Sie im Menü "Module > Web-Proxy > Einstellungen" die "Benutzeranmeldung" auf "an Windows-Domäne (NTLM)" stellen.



In der Windows-Domäne müssen die gewünschten Gruppen als Sicherheitsgruppen angelegt werden. Es werden ausschließlich Benutzer gefunden, die direkte Mitglieder der Gruppen sind. Es ist also nicht möglich, Gruppen zu schachteln.



Werden in der Windows-Domäne Benutzer ergänzt oder entfernt, dauert es bis zu 15 Minuten, bis die Änderungen auf dem SX-GATE wirksam werden.

URL-Filter Regeln

Bei aktiviertem URL-Filter wird jede Anfrage eines Clients auf Zulässigkeit überprüft. Dazu wird das hier konfigurierte Regelwerk sequentiell durchlaufen. Erfüllt eine Anfrage alle Vorbedingungen einer Regel bezüglich Uhrzeit, Quell-IP und Benutzer, wird die

angeforderte Internet-Adresse in der referenzierten URL-Filter Liste gesucht. Bei einem Treffer wird der Zugriff entsprechend der Regel akzeptiert oder mit einer Sperrmeldung beantwortet. Nachfolgende Regeln werden dann nicht mehr abgearbeitet. Liefert die URL-Filter Liste hingegen keinen Treffer, wird mit der Überprüfung der nächste Regel fortgesetzt.



Liefert keine der Regeln einen Treffer, wird der Zugriff erlaubt.

Eine Regel setzt sich aus folgenden Parametern zusammen:

Aktiv

Hiermit schalten Sie Regeln ein oder aus.

Zeitraum

Die Gültigkeit kann zeitlich begrenzt werden. Legen Sie dazu im Menü "Definitionen > Zeiträume" entsprechende Zeiträume fest. Eine Regel kann entweder innerhalb oder außerhalb eines ausgewählten Zeitraums gültig sein.

Quell-IP/Netzwerk

Um die Regel auf Zugriffe von bestimmten Adressen zu beschränken, wählen Sie bitte ein IP-Objekt aus oder tragen Sie eine IP bzw. eine Netzwerk-Adresse mit zugehöriger Netzmaske ein. Lassen Sie das Feld leer, wenn die Regel für beliebige Quell-Adressen gelten soll. In der Tabelle wird dann ein "*" angezeigt.

Gruppe

Bei aktivierter Proxy-Authentifizierung können Sie durch Auswahl einer Gruppe die Gültigkeit der Regel auf bestimmte Benutzer begrenzen. Benutzer und Gruppen werden im Menü "System > Benutzerverwaltung" konfiguriert. Bei Auswahl von "*" gilt die Regel unabhängig vom Benutzer für jede Anfrage, auch für nicht authentifizierte Anfragen.

Zugriff

Hier legen Sie fest, ob beim Zutreffen der Regel die Anfrage akzeptiert oder blockiert werden soll.

Filter-Liste

Die angefragte URL wird in der angegebenen URL-Filter Liste gesucht. URL-Filter Listen werden im Menü "Definitionen > URL-Filter Listen" konfiguriert. Achten Sie beim Anlegen von URL-Filter Listen auf aussagekräftige Namen, dann wird das Regelwerk verständlicher. Wählen Sie den Eintrag "*", wenn die Regel für beliebige URLs gelten soll.



Soll der Zugriff ausschließlich auf freigegebene URLs erlaubt sein, sind mindestens zwei Regeln erforderlich. Die erste Regel erlaubt den Zugriff auf die URL-Filter Liste mit den freigegebenen Adressen. Die zweite Regel verbietet den Zugriff auf alle URLs (Filter-Liste "*").

14.7.2-B Optionen

Proxy-Tunnel Erkennung

Mit dieser Option aktivieren Sie das Überprüfen auf getunnelte Proxy-Verbindungen (https), die die lokalen Sicherheitsrichtlinien zu umgehen versuchen.



Diese Option ist nur bei Anfragen aktiv, bei denen die Kategorie "Proxy-Server" blockiert wird.

IP Adressen rückwärts auflösen

Wenn diese Option aktiviert ist, dann wird für eine IP Adresse rückwärts nach dem DNS-Namen gesucht. Damit wird verhindert, dass gesperrte URLs aufgerufen werden können, indem die IP Adresse des Servers in der Adresszeile des Browsers verwendet wird.

Meldung "Zugriff verweigert"

Mit Ausnahme von Sperren durch die Datenbank-Kategorie "Werbung" wird an den Browser für alle verbotenen Zugriffe ein Fehler gesendet. Bei verschlüsselten Verbindungen handelt es sich lediglich um einen Fehlercode. Dem Anwender wird dann eine browserabhängige Meldung angezeigt. Bei unverschlüsselten Verbindungen oder wenn das Aufbrechen verschlüsselter Verbindungen aktiviert ist, kann der Proxy eine Fehlermeldungen an den Anwender senden. Es stehen dabei verschiedene Varianten zur Auswahl.

Einfach

In dieser Einstellung erscheint eine kurze Fehlermeldung die lediglich auf die Zugriffsbeschränkung aufmerksam macht.

Detailliert

Wählen Sie diese Option um nähere Details anzeigen zu lassen. Dazu gehört z.B. die Information ob der Zugriff aufgrund einer gesperrten Dateinamenserweiterung verweigert wurde oder in welcher Datenbank-Kategorie eine gesperrte Domain enthalten ist.



Bei extrem vielen verbotenen Zugriffen in kurzer Zeit kann das System durch diese Einstellung unter Umständen stark belastet werden.

Detailliert mit Protokollierung

Erweitert die vorhergehende Option um die Protokollierung gesperrter Zugriffe.

Eigene URL:

Es ist auch möglich, eine selbst erstellte Fehlermeldung festzulegen. Geben Sie dazu hier eine vollständige Web-Server URL an (z.B. <http://www.example.com/verboten.html>) die bei einer verbotenen Anfrage angezeigt werden soll.



Im Web-Browser wird die hier angegebene URL im Context des verbotenen Ziel-Servers angezeigt. Referenziert die Fehlermeldung Objekte wie z.B. Bilder oder sind Links enthalten, so müssen diese daher als vollständige URL (inklusive <http://> und Servername bzw. IP) angegeben werden.

14.7.2-C Datenbank

Zu verwendende Datenbank:

Sie haben die Wahl zwischen zwei Datenbanken:

frei verfügbare

Bei der kostenfreien URL-Datenbank handelt es sich um eine Zusammenstellung diverser, im Internet frei verfügbarer Adress-Listen, die lediglich einen Bruchteil der tatsächlich existierenden Seiten zu den einzelnen Kategorien enthält. Auch mit falsch zugeordneten Einträgen ist zu rechnen.



Die kostenfreie URL-Datenbank genügt höheren Ansprüchen, wie sie z.B. von Bildungseinrichtungen gefordert werden, in der Regel nicht.

kommerzielle

Um diese kommerzielle Datenbank nutzen zu können, müssen Sie eine kostenpflichtige Lizenz erwerben. Bitte wenden Sie sich an Ihren SX-GATE Fachhändler.

Täglich aktualisieren um

Die Datenbank kann täglich aktualisiert werden. Geben Sie hierfür die Uhrzeit an, zu der Sie die Aktualisierung wünschen. Lassen Sie das Eingabefeld leer um keine automatischen Aktualisierungen vorzunehmen.



Um die kommerzielle Datenbank nutzen zu können benötigen Sie Login und Passwort!

Nichtkategorisierte URLs hochladen

Durch das Aktivieren dieser Option werden URLs, die dem URL-Filter unbekannt sind, an den Hersteller übermittelt um die Qualität der Datenbank zu verbessern. Die Daten werden vor dem Verschicken anonymisiert, d.h. es werden keine IP Adressen, Benutzernamen oder Passwörter übermittelt.

Zusätzlich werden noch Daten zur statistischen Auswertung übertragen:

- Informationen zu Hardware und Betriebssystem (z.B. i686, Anzahl der CPUs, Linux 2.6.32.28)
- Hostname (z.B. router)
- Anzahl unterschiedlicher IPs, die Anfragen stellten
- Anzahl der Anfragen
- Anzahl der HTTPS-Anfragen
- Anzahl der erkannten Tunnel
- Anzahl der gesperrten Anfragen
- Anzahl, wie oft nicht jugendfreie Inhalte in Suchergebnissen ausgeblendet wurden



Diese Funktion kann nur verwendet werden, wenn Sie keinen übergeordneten Proxy verwenden!

Datenbank jetzt aktualisieren

Drücken Sie diesen Schalter um sofort eine Aktualisierung der Datenbank durchzuführen.

14.7.3 Content-Filter

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.7.3-A Allgemein.....	598
14.7.3-B Virusscan.....	600
14.7.3-C Tag-Filter.....	602
14.7.3-D Tag-Filter Whitelist.....	603
14.7.3-E Content-Typ-Filter.....	604
14.7.3-F SSL-Filter.....	604

Content-Filter

Hier aktivieren Sie den Content-Filter, der neben der Virensan-, Tag-Filter- und SSL-Filter-Funktionalität bietet.



Die Virensan-Funktion kann erst dann genutzt werden, wenn auch ein funktionsfähiger Virensan im SX-GATE installiert ist. Die Lizenzen für den Virensan sind nicht im SX-GATE enthalten und müssen separat erworben werden. Nähere Informationen zu unterstützten oder bereits installierten Virensan finden Sie im Menü "Module > Virensan". Dort ist auch die Installation von Virensan vorzunehmen.

14.7.3-A Allgemein

Content-Typ verifizieren

Antworten vom Webserver enthalten in der Regel den Dateityp im HTTP-Header. Fehlkonfigurierte oder bösartige Webserver liefern hier allgemeine bzw. unzutreffende Content-Typen.

Mit dieser Einstellung versucht der SX-GATE den korrekten Dateityp anhand spezifischer Inhalte am Dateianfang zu ermitteln.



Das Aktivieren dieser Einstellung kann die Anzahl der auf Viren zu untersuchenden Dateien und somit die allgemeine Systemlast stark erhöhen!

Kann über Port 8081/8444 umgangen werden

Ist die Content-Filter-Option aktiviert, so laufen auf SX-GATE zwei hintereinandergeschaltete Proxy-Server. Der Content-Filter-Proxy nimmt Anfragen auf TCP-Port 8080 bzw. 8443 entgegen und leitet sie an den Proxy-Cache auf Port 8081 weiter. Normalerweise werden direkte Verbindungen zu Port 8081 nicht akzeptiert. Aktivieren Sie diesen Schalter um dieses Verhalten zu ändern. Konfigurieren Sie dann im Client den Proxy-Port 8081 bzw. 8444 um den Content-Filter (Virenskan, Tagfilter, ...) grundsätzlich zu umgehen. Um auch bei transparentem Proxying den Content-Filter umgehen zu können, werden zudem die Ports 8083 (HTTP) und 8446 (HTTPS) aktiviert.



Aktivieren Sie diese Option nur um die Kompatibilität mit älteren SX-GATE Versionen wiederherzustellen. Für Anwendungen die nicht mit dem Virenskan-Proxy des SX-GATE zusammenarbeiten, sollten Sie stattdessen Einträge im Bereich "Vertrauenswürdige Server (inkl. Subdomains)" vornehmen.

Vertrauenswürdige Server (inkl. Subdomains)

Der Content-Filter kann die Funktionalität einzelner Webseiten beeinträchtigen. In dieser Tabelle haben Sie die Möglichkeit, für bestimmte Server den Content-Filter zu deaktivieren bzw. durch das Setzen einzelner Haken selektiv nur bestimmte Teilkomponenten zu nutzen. Die Einträge gelten stets auch für Subdomains. Dabei hat ein Eintrag für eine spezifischere Domain (z.B. www.example.com) Vorrang vor einem allgemeineren Eintrag (z.B. example.com).



Wenn die Virenprüfung oder die Option "Content-Typ verifizieren" aktiviert sind, entfernt der Content-Filter aus Anfragen den Wunsch, nur Teile einer Datei herunterzuladen. Es werden immer die kompletten Dateien heruntergeladen und dies dem Client auch angezeigt. Insbesondere manche Software-Aktualisierungs-Programme gehen jedoch fest davon aus, dass sie nur den angeforderten Bereich der Datei erhalten, so dass es zu Problemen kommen kann. Deaktivieren Sie in diesem Fall bitte die genannten Komponenten für den entsprechenden Server.



Wenn die Komponenten "Tag-Filter" oder "Content-Typ verifizieren" aktiviert sind, werden Anfragen so modifiziert, dass keine automatische Komprimierung von Inhalten zugelassen wird.

Virusscan

Die Status-Meldungen des Virensan-Moduls können mit bestimmten Clients zu Problemen führen. Betroffen sind insbesondere Programme, die automatisch Downloads durchführen (z.B. zur Aktualisierung von Software-Komponenten). Sie können für bestimmte Server die Fortschrittsanzeige abschalten oder den Virensan komplett deaktivieren.

Tag-Filter

Ist der Tag-Filter aktiv, so können unter Umständen bestimmte Web-Seiten unbenutzbar werden. Deaktivieren Sie den Filter für betroffene Server indem Sie diesen der Liste hinzufügen ohne den entsprechenden Haken zu setzen.

Content-Typ

Ist der Schalter abgewählt, deaktivieren Sie sowohl die Option "Content-Typ verifizieren" als auch den "Content-Typ-Filter" für die jeweilige Domain.

SSL brechen

Insbesondere zum Schutz der Vertraulichkeit kann es gewünscht sein, SSL-Verbindungen zu bestimmten Servern nicht aufzubrechen.

SSL prüfen

Schlägt eine der konfigurierten SSL-Prüfungen bei einem bestimmten Server fehl, können Sie hier eine Ausnahme für den Server definieren.

14.7.3-B Virusscan

Folgende Content-Typen nicht auf Viren scannen

Hinterlegen Sie hier eine Liste von Content-Typen, die nicht auf Viren geprüft werden sollen. Die Angabe erfolgt im Format "Haupttyp/Untertyp", wobei als Haupt- oder Untertyp auch ein Stern (*) für einen beliebigen Typen angegeben werden kann (z.B. "image/*" für beliebige Bildformate). Wird bei einer angeforderten Web-Seite ein Content-Type übermittelt, der sich nicht in dieser Liste befindet, so wird die heruntergeladene Datei vor der Auslieferung vom Virensanalyzer geprüft.



Soll nur der Tag-Filter benutzt und der Virensan komplett deaktiviert werden, so fügen Sie bitte den Content-Typ "*/*" hinzu.



Alle Content-Typen zu scannen ist zwar möglich, kann jedoch zu massiven Problemen aufgrund der hohen Systembelastung führen. Begrenzen Sie in diesem Falle unbedingt den Parameter "Maximale Anzahl gleichzeitiger Virenskan-Prozesse". Ferner wird dringend davon abgeraten, endlose Datenströme zu scannen. Diese können insbesondere bei Audio- und Video-Datentypen vorkommen ("audio/*" und "video/*").

Diese Komponente scannt ausschließlich Dateien, die über den Virenskan-Proxy des SX-GATE heruntergeladen wurden. Der Virenskan-Proxy muss aktiviert sein. Verschlüsselte Verbindungen werden nicht überprüft, es sei denn, die Option zum Aufbrechen verschlüsselter Verbindungen ist aktiviert.



Benutzer des Microsoft Internet-Explorer ab Version 5 können mit rechter Maustaste über einem FTP-Link die Funktion "Kopieren nach Ordner..." ausführen. Diese Funktion aktiviert einen direkten FTP-Download unter Umgehung des Web-Proxies. Sollte im Firewall der direkte FTP-Zugriff freigegeben sein werden auf diese Weise angeforderte Downloads nicht auf Viren gescannt! Ist der direkte FTP-Zugriff im Firewall nicht erlaubt, so scheitert der Download über diese Funktion.

Passwortgeschützte Dateien ungeprüft ausliefern

Mit dieser Einstellungen können Sie konfigurieren wie passwortgeschützte Dateien behandelt werden sollen. Standardmäßig werden diese blockiert und vorübergehend im Quarantäneverzeichnis vorgehalten. Ist die Option aktiv, dann werden diese Dateien ohne Virenprüfung ausgeliefert.

Sonderbehandlung ab einer Dateigröße von

Dateien die größer als 2GB sind, können von den Virenskannern nicht verarbeitet werden. Auf Wunsch lässt sich hier aber auch ein niedrigeres Limit einstellen. Dateien die dieses Limit überschreiten, werden gesondert behandelt. Beachten Sie dazu den nachfolgenden Parameter.

Größere Downloads werden

Hier legen Sie fest, wie mit größeren Dateien verfahren wird.



Dateien von Servern die unter "Vertrauenswürdige Server (inkl. Subdomains)" aufgeführt sind werden in jedem Fall akzeptiert.

Maximale Anzahl gleichzeitiger Virensan-Prozesse

Hiermit können Sie die maximal Anzahl gleichzeitig vom Virensan-Proxy gestarteter Virensanner beschränken. So lassen sich Überlast-Situationen vermeiden, die Aufgrund sehr vieler paralleler Scan-Vorgänge entstehen.



Ein typischer Anwendungsfall ist das Scannen von Grafiken und Bildern (Dateitypen "image/*"). Da beim Aufruf einer Internet-Seite häufig sehr viele Grafiken gleichzeitig geladen und gescannt werden müssen, kann dies bei fehlender Begrenzung zur Überlastung des Systems führen.

14.7.3-C Tag-Filter

Folgende Content-Typen auf Tags prüfen

Um potentiell gefährliche Tags aus HTML-Seiten zu entfernen, kann in der folgenden Liste angegeben werden, in welchen Dokumenten nach Tags gesucht werden soll. Geben Sie den entsprechenden Content-Typ im Format "Haupttyp/Untertyp" ein, wobei als Haupt- oder Untertyp auch ein Stern (*) für einen beliebigen Typen angegeben werden kann (z.B. "*/html"). Wird eine Datei mit einem der hier angegebenen Content-Typen empfangen, so wird dieses vom Tag-Filter bearbeitet.

Diese Komponente prüft ausschließlich Dateien, die über den Virensan-Proxy des SX-GATE heruntergeladen wurden. Der Virensan-Proxy muss aktiviert sein. Verschlüsselte Verbindungen werden nicht überprüft, es sei denn, die Option zum Aufbrechen verschlüsselter Verbindungen ist aktiviert.

Script-Sprachen ausblenden

Aktivieren Sie diesen Schalter, um den Tag "<script>" sowie Skript-Handler wie "onLoad" oder "onClick" unkenntlich zu machen. Damit wird die Ausführung von Skript-Sprachen wie JavaScript oder VBScript teilweise unterbunden.



Nach Aktivierung dieses Schalters ist mit Problemen bei der Bedienung vieler Internet-Präsenzen zu rechnen.

APPLET-Tags ausblenden

Aktivieren Sie diesen Schalter, um den Tag "<applet>" unkenntlich zu machen. Dieser Tag wird zum Aufruf von Java-Applets genutzt.

EMBED-Tags ausblenden

Aktivieren Sie diesen Schalter, um den Tag "<embed>" unkenntlich zu machen. Dieser Tag wird u.a. zum Einbinden von Plugins genutzt.

OBJECT-Tags ausblenden

Aktivieren Sie diesen Schalter, um den Tag "<object>" unkenntlich zu machen. Dieser Tag wird u.a. zum Aufruf von Java-Applets, ActiveX-Controls und Plugins genutzt.

14.7.3-D Tag-Filter Whitelist**Erlaubte Anwendungen**

Über "Vertrauenswürdige Server (inkl. Subdomains)" auf dem Reiter (Tab) "Allgemein" kann die Filterung für einzelne Server außer Kraft gesetzt werden. Die Liste "Erlaubte Anwendungen" ermöglicht es im Gegensatz dazu, bestimmte Anwendungen von der Filterung auszunehmen. Die Identifikation der Anwendung ist abhängig vom jeweiligen HTML-Tag. Um den korrekten Eintrag für die Freigabe einer Anwendung zu finden, müssen Sie im HTML-Quellcode der Seite den zugehörigen Aufruf finden.



Beachten Sie bitte, dass der Tag-Filter bei einem gefilterten Tag den ersten Buchstaben durch ein Ausrufezeichen ersetzt. Um gefilterte object-, embed- oder applet-Tags zu finden, suchen Sie also bitte nach "!bject", "!mbed" oder "!pplet".

Folgende Werte können in die Liste aufgenommen werden:

Class-IDs

Kommt ausschließlich in object-Tags im Attribut "classid" vor und setzt sich aus dem Text "clsid:" und einer strukturierten Zahlen-/ Buchstabenkombination zusammen. Adobe Flash wird z.B. mit folgendem Code eingebunden:

```
<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000">
```

. Fügen Sie für dieses Beispiel "clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" der Liste hinzu.



Sollte es neben dem classid- auch noch ein type-Attribut geben, ist zusätzlich der dort angegebene Content-Typ freizugeben (siehe unten).

Content-Typen

Wird bei object- und embed-Tags verwendet. Sie finden den einzutragenden Wert jeweils im type-Attribut. Beispiele hierfür wären

```
<object type="application/x-shockwave-flash">
```

bzw.

`<embed type="application/x-shockwave-flash">`

. Tragen Sie zur Freigabe in beiden Fällen "application/x-shockwave-flash" in die Liste ein.



Ist beim object-Tag zusätzlich eine classid angegeben, muss diese ebenfalls freigegeben werden (siehe oben). Fehlt der "type" bei einem embed-Tag, so ist leider keine gezielte Freigabe möglich.

Java-Klassen

Findet Anwendung sowohl bei object- als auch bei applet-Tags. Bei object-Tags ist wiederum das classid-Attribut ausschlaggebend. Um

`<object classid="java:test.class">`

freizugeben, fügen Sie bitte "java:test.class" in die Liste ein. Bei applet-Tags tragen Sie hingegen ein "java:" gefolgt vom Wert des code-Attributs ein. Im Beispiel

`<applet code="test.class">`

wäre also "java:test.class" einzutragen.

14.7.3-E Content-Typ-Filter

Folgende Content-Typen sperren

Hinterlegen Sie hier eine Liste von Content-Typen, die vom Proxy gefiltert werden sollen. Die Angabe erfolgt im Format "Haupttyp/Untertyp", wobei als Haupt- oder Untertyp auch ein Stern (*) für einen beliebigen Typen angegeben werden kann (z.B. "video/*" für beliebige Filmformate).

Diese Komponente prüft ausschließlich Dateien, die über den Virensan-Proxy des SX-GATE heruntergeladen wurden. Der Virensan-Proxy muss aktiviert sein. Verschlüsselte Verbindungen werden nicht überprüft, es sei denn, die Option zum Aufbrechen verschlüsselter Verbindungen ist aktiviert.

14.7.3-F SSL-Filter

SSL-Prüfung bei CONNECT-Verbindungen

Für verschlüsselte Kommunikation fordert der Browser über die CONNECT-Methode eine Verbindung zum Ziel-Server an. Die Nutzdaten dieser Verbindung werden nicht weiter gefiltert, da ja von verschlüsselter Kommunikation auszugehen ist. Manche Anwendungen nutzen jedoch dieses Schlupfloch, um die Firewall zu umgehen. Bei aktivierter SSL-Prüfung wird dies unterbunden, sofern nicht tatsächlich verschlüsselt kommuniziert wird.



Wenn "SSL aufbrechen" aktiviert ist, findet diese Option nur noch Anwendung, wenn über "Vertrauenswürdige Server (inkl. Subdomains)" das Aufbrechen der Verbindung für eine Domain deaktiviert wurde, die SSL-Prüfungen aber aktiv sind. Bei aufgebrochenen Verbindungen werden grundsätzlich nur SSL-verschlüsselte Verbindungen zugelassen. Zudem muss innerhalb der verschlüsselten Verbindung das HTTP-Protokoll verwendet werden.

SSL aufbrechen

Normalerweise ist es nicht möglich, den Inhalt von verschlüsselten Verbindungen zu untersuchen. SX-GATEs Virensan-Proxy ist jedoch in der Lage, die Verbindung aufzusplitten. Es besteht dann eine verschlüsselte Verbindung zwischen Browser und Proxy sowie eine weitere verschlüsselte Verbindung zwischen Proxy und Web-Server im Internet. Der Proxy weist sich dabei gegenüber dem Browser mit einem dem Web-Server-Zertifikat nachempfundenen aber selbst erstellten Zertifikat aus. Signiert werden diese Zertifikate von einem speziellen Stammzertifikat, das im Menü "System > Zertifikatsverwaltung > CA Zertifikate" unter "SX-GATE-CA" auf dem Reiter (Tab) "SSL-Proxy CA" festgelegt wird. Dort lässt sich auch der öffentliche Schlüssel herunterladen, der in allen Client-Browsern hinterlegt werden sollte. Andernfalls muss der Benutzer das Zertifikat für jeden Server bestätigen auf den verschlüsselt zugegriffen werden soll.



Verbindungen zu Servern die auf dem Reiter (Tab) "Allgemein" unter "Vertrauenswürdige Server (inkl. Subdomains)" eingetragen wurden, werden nicht aufgebrochen.

TLS-Protokoll (intern)

Legen Sie hier die Verschlüsselungsstärke für die Kommunikation der Browser mit dem Proxy fest. Sofern der Web-Proxy auch verschlüsselt angesprochen werden kann, wird diese Einstellung im Menü "Module > Web-Proxy > Einstellungen" konfiguriert.



Im Rahmen der Produktpflege werden die mit der jeweiligen Auswahl verbundenen Parameter von Zeit zu Zeit angepasst.

veraltet

Um Kompatibilität mit veralteten Clients zu gewährleisten, werden in dieser Einstellung AES-Algorithmen mit dem nicht mehr empfohlenen Cipher-Block-Chaining CBC und dem veralteten Hash-Algorithmus SHA1 aktiviert. Die minimale TLS-Version ist 1.0.

kompatibel

Wählen Sie diese Einstellung für weitreichende Kompatibilität mit älteren Client-Systemen. Der veraltete Hash-Algorithmus SHA1 ist dabei aktiviert. Die minimale TLS-Version ist 1.2.

aktuell

In dieser Einstellung werden nur noch halbwegs aktuelle Client-Systeme unterstützt. Es wird mindestens TLS 1.2 vorausgesetzt. Wählen Sie diese Option für hohe Sicherheit. Unter Windows sind Internet-Explorer 11, Edge oder ein alternativer Browser wie Chrome oder Firefox erforderlich.

maximal

Erfordert TLS 1.3.

TLS-Protokoll (extern)

Legen Sie hier die Verschlüsselungsstärke für die Kommunikation des Proxies mit den Web-Servern fest.



Im Rahmen der Produktpflege werden die mit der jeweiligen Auswahl verbundenen Parameter von Zeit zu Zeit angepasst.

veraltet

Um Kompatibilität mit veralteten Servern zu gewährleisten, werden in dieser Einstellung AES-Algorithmen mit dem nicht mehr empfohlenen Cipher-Block-Chaining CBC und dem veralteten Hash-Algorithmus SHA1 aktiviert. Die minimale TLS-Version ist 1.0.

kompatibel

Wählen Sie diese Einstellung für weitreichende Kompatibilität mit älteren Servern. Der veraltete Hash-Algorithmus SHA1 ist dabei aktiviert. Die minimale TLS-Version ist 1.2.

aktuell

In dieser Einstellung werden nur noch halbwegs aktuelle Client-Systeme unterstützt. Es wird mindestens TLS 1.2 vorausgesetzt. Wählen Sie diese Option für hohe Sicherheit. Unter Windows sind Internet-Explorer 11, Edge oder ein alternativer Browser wie Chrome oder Firefox erforderlich.

Vertrauenswürdige CAs

Web-Server-Zertifikaten müssen von einer der hier hinterlegten CAs ausgestellt worden sein, um erfolgreich verifiziert werden zu können.

Unbekannte CA blockieren

Legen Sie hier fest, wie sich der Proxy verhalten soll, wenn sich ein Web-Server mit einem Zertifikat ausweist, dessen Herkunft nicht verifiziert werden kann. Dazu gehören sowohl selbstsignierte Zertifikate als auch Zertifikate die von einer CA ausgestellt wurden, die SX-GATE nicht bekannt sind. Wenn deaktiviert, stellt der Proxy für den Server ein selbstsigniertes Zertifikat aus. Entsprechend wird der Browser eine Warnmeldung anzeigen und dem Anwender die Entscheidung überlassen, ob die Verbindung aufgebaut werden soll. Aktivieren Sie diese Option wenn SX-GATE die Verbindung abweisen soll ohne dem Anwender eine Wahl zu lassen.

Abgelaufene Zertifikate blockieren

Wenn diese Option aktiviert ist, dann wird die Verbindung vom Proxy verweigert, sofern ein Server-Zertifikat außerhalb seines Gültigkeitszeitraums liegt. Andernfalls erhält der Benutzer in seinem Web-Browser eine entsprechende Warnung und kann das Zertifikat bei Bedarf akzeptieren.

Nicht übereinstimmende Servernamen blockieren

Wenn diese Option aktiviert ist, dann werden Zugriffe auf Server nur dann erlaubt, wenn deren Name im verwendeten Zertifikat aufgelistet ist. Andernfalls erhält der Benutzer in seinem Web-Browser eine entsprechende Warnung und kann das Zertifikat bei Bedarf akzeptieren.

Gültigkeit von Zertifikaten über OCSP überprüfen

nein

Es wird keine Überprüfung der Zertifikate über OCSP vorgenommen.

ja, bei Abfragefehler erlauben

Gültigkeitsprüfung der Zertifikate mit OCSP wird vorgenommen. Nur zurückgezogene Zertifikate führen zum Abbruch der Verbindung.

ja, bei Abfragefehler blockieren

Gültigkeitsprüfung der Zertifikate mit OCSP wird vorgenommen. Zusätzlich zu zurückgezogenen Zertifikaten führen auch Abfragefehler, wie z.B. Verbindungsfehler zum OCSP-Responder, zum Abbruch der Verbindung.

Detaillierte Fehlermeldung bei Sperrung durch URL-Filter

Mit dieser Option legen Sie fest, wie der Proxy bei aufgebrochenen Verbindungen vorgehen soll, wenn eine Domain im URL-Filter vollständig gesperrt ist.



Wird vom URL-Filter nicht die gesamte Domain sondern lediglich einzelne Dateien oder Unterverzeichnisse gesperrt, wird immer eine detaillierte Fehlermeldung angezeigt.

Ist die Option ausgeschaltet, wird bereits der SSL-Verbindungsaufbau vom Proxy abgewiesen. Es findet keine Verbindung in das Internet statt. Allerdings ist es so nicht möglich, im Browser eine passende Fehlermeldung anzuzeigen. Der Browser wird eine allgemeine Fehlermeldung ausgeben, dass der Proxy die Verbindung abgelehnt hat.

Wenn Sie die Option einschalten, wird hingegen ein vollständiger SSL-Verbindungsaufbau mit dem Zielsever durchgeführt. Jede einzelne Anfrage wird dann aber vom Proxy mit der in der URL-Filter-Konfiguration festgelegten Fehlermeldung abgewiesen. Der Zielsever im Internet registriert also einen SSL-Verbindungsaufbau, erhält über diese Verbindung aber keine Anfragen.

14.8 Reverse-Proxy

Der Reverse-Proxy dient dem Zugriff aus dem Internet auf lokale Web-Server. Während für den Zugriff auf Web-Server im LAN der Schutzgedanke im Vordergrund steht, kann der Reverse-Proxy auch als Lastverteiler für Web-Server in einer DMZ fungieren. Die Verbindung zum Reverse-Proxy kann sowohl mit HTTP als auch mit HTTPS erfolgen. Auch die Hintergrund-Server lassen sich mit HTTP oder HTTPS ansprechen.

14.8.1 Einstellungen

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.8.1-A Filter.....	609
14.8.1-B WAF.....	610
14.8.1-C WAF-Regeln.....	611

14.8.1-A Filter

Wenn in einer Webanwendung eine Sicherheitslücke entdeckt wird, aber noch kein Update dafür verfügbar ist, kann es hilfreich sein, bestimmte Zugriffe zu sperren. Die auf dieser Seite konfigurierten Sperren gelten gleichermaßen für alle Zugriffe, die über den Reverse-Proxy laufen.

Gesperrte URLs

Die hier konfigurierten Suchmuster beziehen sich auf den URL-Pfad inkl. URL-Parameter (also alles nach dem Servernamen). Groß- und Kleinschreibung wird nicht unterschieden. Beginnt oder endet das Suchmuster mit einem Buchstaben oder einer Ziffer, muss das Suchmuster am Beginn bzw. Ende eines Wortes oder einer URL-Komponente (Pfad, Dateiname, Parametername, ...) stehen. Das Suchmuster "all" liefert folglich bei "/hallo/" keinen Treffer, bei "/all/" oder "/liste?q=all" hingegen schon. Das Sonderzeichen "*" steht für eine beliebige Anzahl beliebiger Zeichen. So liefert "*all*" auch bei "/hallo/" einen Treffer. Das "+" steht für ein Plus- oder Leerzeichen.



%-codierte Zeichen in der URL werden vor der Suche umgewandelt.

Gesperrte Header

Anfragen, die einen hier gesperrten Header enthalten, werden abgefangen. Wenn Sie einen Header-Namen angeben, wird das Muster im Wert des angegebenen Headers gesucht.



Ist kein Header angegeben ("*"), erfolgt die Suche in allen Headern inklusive den Header-Namen.

Groß- und Kleinschreibung wird nicht unterschieden. Beginnt oder endet das Suchmuster mit einem Buchstaben oder einer Ziffer, muss das Suchmuster am Beginn bzw. Ende eines Wortes stehen. Das Sonderzeichen "*" steht für eine beliebige Anzahl beliebiger Zeichen. Das "+" steht für ein Plus- oder Leerzeichen.

14.8.1-B WAF

Die Web-Application-Firewall (WAF) prüft die Anfragen der Clients auf Einhaltung von Standards, ungewöhnliche Eigenschaften und bekannte Angriffe. Auffällige Zugriffe werden abgewiesen.



Die Signaturen werden im Zuge der SX-GATE-Updates aktualisiert.

Web-Application-Firewall

Aktivieren Sie hier die WAF. Grundsätzlich ist danach mit Fehlalarmen zu rechnen. Behalten Sie daher bitte das zugehörige Log "Reverse-Proxy WAF" im Auge und konfigurieren Sie Ausnahmen für problematische Regeln. Beim erweiterten Regelwerk ist mit mehr Fehlalarmen zu rechnen.

Ausnahmen für Regeln

Tragen Sie hier die IDs der Regeln ein, die Sie deaktivieren wollen. Sie finden Alarme der WAF zusammen mit der zugehörigen Regel-ID im Log "Reverse-Proxy WAF".

Wenn Sie als "Bereich" den Eintrag "*" (vollständig) auswählen, wird die Regel vollständig deaktiviert. Bei manchen Alarmen ist es jedoch auch möglich, die Regel gezielter zu deaktivieren. Wählen Sie dazu den entsprechenden Eintrags aus der Liste, um die Regel nur bei der Überprüfung von Parametern (ARGS), Cookies oder Headern deaktivieren. Unter "Name" lässt sich dies weiter auf den Parameter, Cookie oder Header mit einem ganz bestimmten Namen einschränken.



Wenn als "Bereich" "*" (vollständig) ausgewählt ist, hat "Name" keine Funktion.

14.8.1-C WAF-Regeln

Abhängig von den Technologien, die auf Ihrem Webserver zum Einsatz kommen, können Sie hier zusätzliche Regeln aktivieren.

Für einige wenige Anwendungen können Sie hier auch Ausnahmen aktivieren, die problematische Regeln für bestimmte URLs deaktivieren.

14.8.2 Ports

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Reverse-Proxy Port

Tragen Sie hier den Port ein, auf dem Anfragen entgegengenommen werden sollen.



Der hier festgelegte Port muss in der Regel noch in der Firewall-Konfiguration des SX-GATE freigegeben werden.



Für unverschlüsselte Zugriffe möchten Sie möglicherweise den HTTP Standard-Port 80 nutzen. Dieser ist möglicherweise aber bereits belegt. Prüfen Sie dazu bitte unter "System > Dienste" auf dem Reiter (Tab) "Server-Dienste" ob der Dienst "HTTP-Server" aktiviert ist. Falls ja, kann Port 80 vom Reverse-Proxy nicht genutzt werden. Verwenden Sie in diesem Falle einen anderen freien Port (z.B. 8888). Wenn die Zugriffe trotzdem zu Port 80 erfolgen sollen, können Sie in der Firewall-Konfiguration der gewünschten Schnittstellen DNAT-Regeln konfigurieren, die Zugriffe auf Port 80 an den Reverse-Proxy-Port umleiten.

Verbindung

Wählen Sie hier aus, welche Art von Verbindung an diesem Port erwartet wird.

verschlüsselt (https://)

Durch diese Einstellung müssen die Clients eine SSL/TLS verschlüsselte Verbindung zum SX-GATE aufbauen.

authentifiziert (https://)

In dieser Einstellung müssen sich die Clients mit einem Zertifikat der SX-GATE CA ausweisen.

unverschlüsselt (http://)

Die Kommunikation zwischen den Clients und dem SX-GATE erfolgt unverschlüsselt.

14.8.2.1

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.8.2.1-A Allgemein.....	613
14.8.2.1-B Zertifikat.....	615
14.8.2.1-C Vertrauenswürdige CA.....	616

Verbindung

Wählen Sie hier aus, welche Art von Verbindung an diesem Port erwartet wird.

authentifiziert (https://)

In dieser Einstellung müssen sich die Clients mit einem Zertifikat der SX-GATE CA ausweisen.

14.8.2.1-A Allgemein

Der Reverse-Proxy kann auf zwei Arten eingesetzt werden. Als Vermittler der Anfragen an interne Web-Server weiterleitet und als Load-Balancer der Anfragen an eine Server-Farm verteilt.

Die Einstellungen in diesem Bereich legen fest, wie der Reverse-Proxy aus dem Internet erreichbar ist und welchen Einschränkungen alle Anfragen unterliegen. Zur Konfiguration der Hintergrund-Server, an die die Anfragen dann weitergeleitet werden, öffnen Sie bitte den Menü-Baum indem Sie auf das Plus-Symbol klicken. Sie haben dort die Möglichkeit, je angesprochenem Hostnamen einen Satz Hintergrund-Server zu konfigurieren (virtuelles Hosting). Zugriffe auf Hostnamen für die kein eigener Eintrag angelegt wurde, werden abgewiesen bzw. gemäß der Einstellungen des speziellen Eintrags "*" verarbeitet.

Informationstext für Anmeldefenster

Auf Wunsch gewährt der Reverse-Proxy den Zugriff auf einzelne Backend-Server erst nach erfolgreicher Authentifizierung. Akzeptiert werden ausschließlich Anmeldungen von Mitgliedern der SX-GATE-Gruppe "system-proxy". Web-Browser fragen die Zugangsdaten üblicherweise in einem kleinen Fenster ab, in dem u.a. der hier eingestellte Text angezeigt wird. Dem Anwender kann auf diese Weise mitgeteilt werden, wofür er sich anmelden soll.



Verwenden Sie einen möglichst unverfänglichen Text um nicht die Neugierde potentieller Angreifer auf sich zu lenken.

Syntax-Prüfung der Anfragen

Zur Erhöhung der Sicherheit kann mit Hilfe dieser Option die formale Gültigkeit der angeforderten URLs geprüft werden. Sind ungültige Zeichen in der URL enthalten oder entspricht die Reihenfolge der Angaben nicht dem Standard, so wird der Zugriff verweigert.

tolerant

In dieser Variante wird eine ganze Reihe von nicht standardkonformen Zeichen in einer URL akzeptiert. Verwenden Sie diese Einstellung wenn die restriktiveren Optionen nicht zum Erfolg führen. Wird der Zugriff auf den Hintergrund-Server dennoch verweigert, muss diese Option deaktiviert werden.

Microsoft optimiert

Diese Option ist für den Zugriff auf Microsofts Outlook-Web-App (OWA) optimiert. Diverse Abweichungen vom Standard werden in dieser Einstellung akzeptiert. Vereinzelte Probleme in speziellen Fällen können jedoch nicht gänzlich ausgeschlossen werden.

streng

In dieser Einstellung orientiert sich die Überprüfung weitgehend am Standard gemäß RFC2396.

Erweiterte HTTP-Befehle zulassen

In der Grundeinstellung werden ausschließlich Zugriffe mit den HTTP-Methoden "GET", "POST" und "HEAD" vom Reverse-Proxy akzeptiert. Aktivieren Sie diesen Schalter um zusätzlich "PUT" und alle WebDAV-Zugriffsmethoden freizugeben.



Für den Zugriff auf Microsofts Outlook-Web-App (OWA), mit Outlook Anywhere oder auf ein Remotedesktop-Gateway muss diese Option aktiviert sein.

Maximale Größe für Uploads

Diese Einstellung beschränkt die Größe von Anfragen. Formularparameter oder Dateien wie sie beispielsweise mit "POST" und "PUT" übertragen werden, dürfen diese Gesamtgröße nicht überschreiten. Bleibt das Feld leer, so erfolgt keine Begrenzung.

TLS-Protokoll

Wählen Sie hier die Verschlüsselungsstärke aus. Für allgemein zugängliche und unkritische Inhalte können Sie einen niedrigen Wert wählen, so das maximale Browserkompatibilität erreicht wird. Wählen Sie einen hohen Wert, wenn Sie Dienste einem geschlossenen Benutzerkreis zur Verfügung stellen.



Im Rahmen der Produktpflege werden die mit der jeweiligen Auswahl verbundenen Parameter von Zeit zu Zeit angepasst.

veraltet

In dieser Einstellung wird das veraltete Hash-Verfahren SHA1 aktiviert. Die minimale TLS-Version ist 1.0.

kompatibel

Wählen Sie diese Einstellung für weitreichende Kompatibilität mit älteren Client-Systemen. Der veraltete Hash-Algorithmus SHA1 ist dabei aktiviert. Die minimale TLS-Version ist 1.2.

aktuell

In dieser Einstellung werden nur noch halbwegs aktuelle Client-Systeme unterstützt. Es wird mindestens TLS 1.2 vorausgesetzt. Wählen Sie diese Option für hohe Sicherheit. Unter Windows sind Internet-Explorer 11, Edge oder ein alternativer Browser wie Chrome oder Firefox erforderlich.

maximal

Erfordert TLS 1.3. Diese Option ist derzeit nur für geschlossene Benutzerkreise sinnvoll. Bevor Sie sich für diese Einstellung entscheiden, sollten Sie prüfen, ob alle Clients TLS 1.3 unterstützen.

Browser anweisen für alle Domains stets eine sichere Verbindung zu verwenden

Mit dieser Einstellung aktivieren Sie HTTP Strict-Transport-Security. Dabei wird der Browser angewiesen, Zugriffe auf diesen Servernamen ab sofort ausschließlich verschlüsselt vorzunehmen. Zudem wird es dem Browser dem Anwender nicht erlauben, ungültige Zertifikate zu akzeptieren. Diese Maßnahmen greifen nach dem ersten Besuch des Browsers und sollen Man-in-the-Middle Attacken erschweren. Nicht alle Browser unterstützen jedoch diese Funktion.



Die browserseitigen Einschränkungen gelten für jeden virtuellen Hostnamen unter dem der Browser diesen Reverse-Proxy-Port anspricht. Aktivieren Sie diese Option nicht, wenn unter einem der Hostnamen auch Web-Server betrieben werden, auf die unverschlüsselt zugegriffen werden muss.

Der Browser setzt die genannten Einschränkungen für die hier konfigurierte Anzahl an Tagen in Kraft. Mit dem speziellen Wert "0" wird der Browser angewiesen, die Einschränkungen aufzuheben, was allerdings einen erneuten fehlerfreien Zugriff durch den Browser voraussetzt. Lassen Sie das Feld leer, wenn der Reverse-Proxy keine Strict-Transport-Security Option setzen soll.



Für den produktiven Einsatz sollten Sie einen Wert in der Größenordnung mehrere Monate konfigurieren. Hohe Werte verbessern die Sicherheit für die Clients, erfordern aber auch mehr Weitblick vom Administrator.

14.8.2.1-B Zertifikat

Dieses Zertifikat wird für den verschlüsselten Zugriff auf den Reverse-Proxy des SX-GATE verwendet.

Schlüssel/Zertifikat auswählen

Wählen Sie hier einen der Schlüssel aus, die im Menü "System > Zertifikatsverwaltung > Schlüsselbund" administriert werden.

14.8.2.1-C Vertrauenswürdige CA

Legen Sie hier die Zertifizierungsstelle (CA) fest, mit der die Clients authentifiziert werden.

Vertrauenswürdige CA

Wählen Sie hier die gewünschte CA aus.

Vertrauenswürdige CA importieren**CA-Zertifikat auswählen**

Das Zertifikat muss ergänzt werden um die Zertifikate eventueller Zwischen-Zertifizierungsstellen (Intermediate CAs) bis zum Wurzel-Zertifikat (Root CA). Alle Zertifikate müssen im PEM-Format vorliegen. Sie erhalten die Zertifikate von Ihrer Zertifizierungsstelle.

CA-Zertifikat ergänzt

Das hochgeladene Zertifikat wird an die Zertifizierungs-Kette angehängt.

Lesen Sie bitte weiter bei [CA-Zertifikat auswählen](#)

Lesen Sie bitte weiter bei [CA-Zertifikat installieren](#)

CA-Zertifikat installieren

Der Import-Vorgang ist abgeschlossen. Das neue Zertifikat kann jetzt installiert werden.

Zertifikats-Sperrliste der CA importieren

Hier haben Sie die Möglichkeit, eine Zertifikats-Sperrliste (CRL) zur vertrauenswürdigen CA zu hinterlegen bzw. zu aktualisieren. Sinn einer Zertifikats-Sperrliste ist es, bestimmte Zertifikate bereits vor deren Ablaufdatum als ungültig zu erklären. Dies ist z.B. notwendig, wenn ein Mitarbeiter die Firma verlässt und diesem Zugang verwehrt werden muss. Die CRL muss im PEM-Format importieren werden.



Die CRL ist nur dann wirksam, wenn sie von der vertrauenswürdigen CA ausgestellt wurde.

Zertifikats-Sperrliste der CA löschen

Diese Funktion ermöglicht es Ihnen, die Zertifikat-Sperrliste zu löschen. Darin widerrufen Zertifikate sind danach wieder gültig.

14.8.2.2 - Virtuelle Hosts

In einer tabellarischen Übersicht werden die verfügbaren Objekte angezeigt. Bei mehrspaltigen Tabellen kann die Sortierung durch Klick auf den Titel der Spalte geändert werden. Sind mehr als 20 Einträge in der Tabelle, erscheint am rechten unteren Tabellenrand eine Navigationsleiste. Sie können zwischen einer gruppierten Anzeige und einer Seitenschaltung zum Vor- und Zurückblättern wählen. Die Tabelle kann auch im Vollbild-Modus angezeigt werden, wobei dann alle Einträge sichtbar sind. Durch Klick auf den Titel eines Eintrags in der linken Spalte wechseln Sie in die Detail-Ansicht. Sofern in der rechten Spalte Stift oder Mülltonne angezeigt werden, kann der Eintrag umbenannt oder gelöscht werden. Neue Objekte werden über die Lasche "Neuer Eintrag" am linken unteren Tabellenrand angelegt.

Servername (Virtueller Host)

Aus den Anfragen die ein Web-Browser schickt geht üblicherweise hervor, welcher Servername im Web-Browser eingegeben wurde (Host-Header). Geben Sie hier einen DNS-Namen oder eine IP ein unter der der SX-GATE Reverse-Proxy aus dem Internet zu erreichen ist. Nur Anfragen mit dem passenden Host-Header werden an die nachfolgend konfigurierten Hintergrund-Server weitergeleitet.



Der Host-Header lässt sich leicht fälschen. Nutzen Sie virtuelle Hosts daher niemals, um Zugriffe aus unterschiedlichen Sicherheitszonen (z.B. LAN und Internet) auf verschiedene Hintergrundserver aufzuteilen. Konfigurieren Sie stattdessen für jede Sicherheitszone einen eigenen Reverse-Proxy-Port und verteilen Sie Zugriffe aus den unterschiedlichen Sicherheitszonen mit Hilfe von DNAT-Regeln in der Firewall-Konfiguration auf den zugehörigen Ports.

Um einen Hintergrund-Server für Anfragen ohne oder mit beliebigem anderen Host-Header zu definieren, lassen Sie das Feld bitte leer. Es wird dann ein Eintrag mit dem Namen "*" erstellt.



Ist kein virtueller Host "*" definiert oder ist darin kein Hintergrundserver aktiviert, werden Zugriffe ohne passenden Host-Header mit einer Fehlermeldung abgewiesen. Unberechtigte Zugriffe lassen sich so erschweren.

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.8.2.2-A Microsoft IIS-Dienste.....	618
14.8.2.2-B SX-GATE Dienste.....	621
14.8.2.2-C Hintergrund-Server.....	623
14.8.2.2-D Verbindungsparameter.....	626
14.8.2.2-E Lastverteilung.....	627

14.8.2.2-A Microsoft IIS-Dienste

Der Reverse-Proxy bietet optimierte Einstellungen für den Zugriff auf ausgewählte Dienste eines Microsoft IIS-Servers. Dabei wird sichergestellt, dass nur die explizit freigegebenen Bereiche des IIS aus dem Internet angesprochen werden können.

Remotedesktop-Gateway

Tragen Sie hier die IP-Adresse des Microsoft Internet-Information-Servers (IIS) ein, der als Remotedesktop-Gateway fungiert. Der Reverse-Proxy verbindet sich mit dem IIS über HTTPS. Im IIS muss der RPC-Proxy-Dienst im Verzeichnis "/rpc" konfiguriert sein. Lassen Sie das Eingabefeld frei, wenn kein Remotedesktop-Gateway veröffentlicht werden soll.



Nach unserem Kenntnisstand wird eine Authentifizierung am Reverse-Proxy mittels Client-Zertifikat vom Microsoft Terminalserver-Client nicht unterstützt.

Zugriff auf RD Web Access

Aktivieren Sie diesen Schalter, wenn auf Remotedesktop Web Access (RDWEB) zugegriffen werden soll. Folgende Pfade werden freigegeben: "/rdweb", "/remoteDesktopGateway" und "/KdcProxy".



Um mit einem Web-Browser auf RDWEB zuzugreifen, hängen Sie an die Adresse bitte den passenden Einstiegspfad an (z.B. <https://www.example.com/rdweb>).



Diese Option greift nur, wenn auch ein Remotedesktop-Gateway angegeben wurde.

Exchange-Dienste: internes Verbindungs-Protokoll

Um den Zugriff auf Exchange-Dienste zu aktivieren, wählen Sie bitte zunächst das Protokoll für die Verbindung von SX-GATE zu Exchange/IIS aus. Sofern Sie sich für unverschlüsselte Kommunikation entscheiden, müssen Sie dies ggf. in den einzelnen Exchange-Diensten gesondert freigeben (SSL-Offloading, SSL-Verschiebung).



Beachten Sie bitte die technischen Vorgaben von Microsoft. Der IIS als Backend-Server muss intern auf den Standard-Ports 443 (verschlüsselt) bzw. 80 (unverschlüsselt) erreichbar sein. Von extern muss der Reverse-Proxy des SX-GATE auf Port 443 (verschlüsselt) angesprochen werden.

IIS mit Exchange-Diensten

Tragen Sie hier die IP-Adresse des Microsoft Internet-Information-Servers (IIS) ein, der die Exchange Dienste zur Verfügung stellt.

Zugriff auf OWA

Aktivieren Sie diesen Schalter, wenn auf Outlook-Web-App (OWA) zugegriffen werden soll. Folgende Pfade werden freigegeben: "/owa", "/exchange", "/exchweb", "/public" und "/oab".



Um mit einem Web-Browser auf OWA zuzugreifen, hängen Sie an die Adresse bitte den passenden Einstiegspfad an (z.B. <https://www.example.com/owa>).

Zugriff auf Exchange Admin Center / Control Panel

Aktivieren Sie diesen Schalter, wenn auf das Exchange Admin Center (EAC), bzw. bei älteren Exchange Versionen das Exchange Control Panel (ECP) zugegriffen werden soll. Es wird der Pfad "/ecp" freigegeben.



Um mit einem Web-Browser auf EAC bzw. ECP zuzugreifen, hängen Sie an die Adresse bitte den passenden Einstiegspfad an (z.B. <https://www.example.com/ecp>).

Zugriff mit Exchange-Active-Sync (EAS)

Insbesondere mobile Geräte nutzen das ActiveSync-Protokoll um sich mit Exchange zu verbinden. Die Option gibt den IIS-Pfad "/Microsoft-Server-ActiveSync" frei.

Zugriff mit RPC/Outlook-Anywhere

Ist diese Option aktiviert, kann Outlook über einen HTTPS-Tunnel mit Exchange kommunizieren. Im IIS muss dazu der RPC-Proxy-Dienst im Verzeichnis "/rpc" konfiguriert sein. In neueren Exchange- und Outlook-Versionen wird diese Technik von MAPI-über-HTTP abgelöst.



Bevor Sie den Zugriff mit Outlook testen, sollten Sie sicherstellen, dass es beim Aufbau der HTTPS-Verbindung keine Probleme gibt. Greifen Sie dazu am besten mit dem Web-Browser des Outlook-PCs auf den Reverse-Proxy zu. Das Zertifikat darf nicht abgelaufen sein, muss auf den korrekten Servernamen ausgestellt sein und die Zertifizierungsstelle die das Zertifikat ausgegeben hat muss dem Outlook PC bekannt sein.



Nach unserem Kenntnisstand wird eine Authentifizierung am Reverse-Proxy mittels Client-Zertifikat von Outlook nicht unterstützt.

Zugriff mit MAPI-über-HTTP

Outlook-Clients ab 2010 SP2, 2013 SP1 und 2016 können sich mit MAPI-über-HTTP zu einem Exchange-Server mit mindestens Version 2013 SP1 oder 2016 verbinden. Das zugehörige virtuelle Verzeichnis im IIS lautet "/mapi".

Zugriff auf die Exchange Web-Services

Dies ist die modernste Schnittstelle für den Zugriff auf Exchange. Sie wird beispielsweise von Outlook 2011 für Mac genutzt. Freigegeben werden diverse Dateien im Pfad "/ews/".

Client-Konfiguration über Autodiscover

Mit dieser Option geben Sie den Zugriff auf die Autodiscover-Funktion des Exchange-Servers frei (diverse Dateien im Verzeichnis "/autodiscover/"). Dies erlaubt externen Outlook-Benutzern und ActiveSync-Clients eine einfache Konfiguration des Dienstes.

Für die Domain "example.com" sucht der Client den Autodiscover-Server zunächst unter "example.com", dann unter "autodiscover.example.com". Schließlich prüft der Client, ob im DNS ein Eintrag vom Typ "SRV" für die Domain

"_autodiscover._tcp.example.com" vorhanden ist. Der Eintrag muss auf Port 443 und den DNS-Namen des SX-GATEs verweisen (z.B. "owa.example.com"). Der Vorteil des SRV-Eintrags ist, dass im Server-Zertifikat kein zusätzlicher Hostname enthalten sein muss. Ein günstiges Zertifikat ist daher in der Regel ausreichend.

14.8.2.2-B SX-GATE Dienste

Der Reverse-Proxy wird benötigt, um auf SX-GATE-Erweiterungen (Apps) zuzugreifen. Es ist außerdem möglich, auf den SX-GATE Administrations-Server zuzugreifen. Im Unterschied zum direkten Zugriff, kann im Reverse-Proxy der Zugriff auf einen Teilbereich eingeschränkt werden. So lässt sich der Zugriff auf die Mail-Quarantäne erlauben, während die SX-GATE Administration gesperrt bleibt.

SX-GATE-Groupware

Ist dieser Schalter aktiviert, so werden alle Anfragen, deren URL mit "/groupware", "/SOGGo" oder "/SOGGo.woa" beginnt, an die SX-GATE-Groupware weitergeleitet. Um Gründen der Rückwärtskompatibilität werden ferner die Pfade "/webmail" und "/cgi-bin/openwebmail" umgeleitet. Die Groupware-Erweiterung (App) muss dazu installiert sein.



Um mit einem Web-Browser auf die Groupware zuzugreifen, hängen Sie an die Adresse bitte "/groupware" an (z.B. <https://www.example.com/groupware>).

SX-GATE Active-Sync

Mobile Clients und Outlook können über Exchange-Active-Sync (EAS) an die SX-GATE Groupware angebunden werden. Die Option gibt den Pfad "/Microsoft-Server-ActiveSync" frei. Sollte EAS bereits auf dem Reiter (Tab) "Microsoft IIS-Dienste" aktiviert sein, hat die Weiterleitung an Exchange Vorrang.

SX-GATE CalDAV

Mit dieser Option wird der Zugriff auf den CalDAV-Bereich der SX-GATE Groupware freigegeben. Jede Software, die einen CalDAV-Client enthält, kann so auf Termine aus den Groupware-Kalendern zugreifen. Die Option aktiviert die Pfade "/SOGGo/dav/*/Calendar", "/SOGGo/dav/public/*/Calendar" und "/.well-known/caldav".

SX-GATE CardDAV

Mit dieser Option wird der Zugriff auf den CardDAV-Bereich der SX-GATE Groupware freigegeben. Jede Software, die einen CardDAV-Client enthält, kann so auf Kontakte aus den Groupware-Adressbüchern zugreifen. Die Option aktiviert die Pfade "/SOGGo/dav/*/Contacts", "/SOGGo/dav/public/*/Contacts" und "/.well-known/carddav".

SX-GATE RDP/VNC/SSH Web-Client

Der clientlose Zugriff auf RDP-, VNC- und SSH-Server mittels Web-Client wird über diese Option freigeschaltet. Dazu muss die entsprechende SX-GATE-Erweiterung (App) installiert sein. Die Option leitet den URL-Pfad "/webclient" weiter.



Um mit einem Web-Browser auf den Web-Client zuzugreifen, hängen Sie an die Adresse bitte "/webclient" an (z.B. <https://www.example.com/webclient>).

SX-GATE E-Mail-Quarantäne

Mit diesem Schalter wird der Benutzerzugriff auf das E-Mail Quarantäne-Verzeichnis freigegeben. Dazu werden Anfragen für die URL "/cgi-bin/unquarantine.cgi" an den SX-GATE Administrations-Server weitergeleitet.



Diese Option wird nur dann benötigt, wenn im Menü "Module > Mail-Server > SPAM/Virus/Malware" auf dem Reiter (Tab) "MIME-Filter" die Option "Benutzerzugriff auf Quarantäne" aktiviert ist.

SX-GATE-Administration

Dieser Schalter erlaubt den Zugriff auf die Administrations-Oberfläche des SX-GATE via Reverse-Proxy.



Um mit einem Web-Browser auf die Administrations-Oberfläche zuzugreifen, hängen Sie an die Adresse bitte "/riabconf/de" an (z.B. <https://www.example.com/riabconf/de>).

An den Administrations-Server werden Anfragen umgeleitet, deren URL mit "/riabconf", "/js", "/styles" oder "/flags" beginnt. Betroffen sind ferner Anfragen nach bestimmten Dateien in Unterverzeichnissen, deren Name lediglich aus einem einzelnen Buchstaben oder einer Ziffer besteht.

ACME HTTP-Authorisierung

Sie benötigen diese Option, wenn SX-GATE Zertifikate von einer CA via ACME (Automatic Certificate Management Environment) bezieht (z.B. von Let's Encrypt). Es wird der Pfad "/.well-known/acme-challenge/" freigegeben.

14.8.2.2-C Hintergrund-Server

Benutzerdefinierte Hintergrund-Server

Tragen Sie hier die Server ein, an die der Reverse-Proxy Anfragen weiterleiten soll. Dabei können je URL-Pfad unterschiedliche Einstellungen gemacht werden. Groß- und Kleinschreibung spielen keine Rolle. Die Reihenfolge der Einträge ist aber entscheidend. Falls es zu einem Pfad mehrere Einträge gibt, fungiert der Reverse-Proxy als Lastverteiler.

Es ist nicht möglich, den URL-Pfad aus Anfragen durch den Reverse-Proxy modifizieren zu lassen (z.B. "/PfadA" an Hintergrund-Server A ohne Pfad, "/PfadB" an Hintergrund-Server B ohne Pfad). Der URL-Pfad wird immer unverändert weitergegeben. Sollen auf verschiedenen Hintergrund-Servern identische Pfade angesprochen werden, müssen Sie im Reverse-Proxy entweder unterschiedliche virtuelle Hosts konfigurieren oder verschiedene externe IPs mit unterschiedlichen Reverse-Proxy Ports verwenden.

Akt.

Mit Hilfe dieses Schalters lässt sich der Eintrag deaktivieren.

Auth.

Wenn aktiviert, ist der Zugriff auf den Hintergrund-Server erst nach Anmeldung möglich. Akzeptiert werden ausschließlich Anmeldungen von Mitgliedern der SX-GATE-Gruppe "system-proxy". Nutzen Sie diese Option, wenn nur einem eingeschränkten Benutzerkreis der Zugriff auf den Hintergrund-Server möglich sein soll. Nicht autorisierten Personen bleibt so verborgen, welche Server-Software im Hintergrund läuft und welche Anwendung zur Verfügung gestellt wird. Der Reverse-Proxy des SX-GATE verlangt vom Web-Browser eine sogenannte "Basic-Authentifizierung". Dabei fragt der Web-Browser die Zugangsdaten üblicherweise mit Hilfe eines kleinen Anmeldefensters ab.



Bei Basic-Authentifizierung werden Benutzername und Kennwort quasi im Klartext übertragen. Es sollten daher ausschließlich verschlüsselte Verbindungen (HTTPS) zum Reverse-Proxy genutzt werden.

Bitte prüfen Sie, inwieweit die Hintergrund-Server für den Zugriff ebenfalls Authentifizierung verlangen. Werden die Zugangsdaten mit Hilfe eines in die Web-Seite eingebetteten Formulars abgefragt, ist dies kein Problem. Der Benutzer muss sich dann zunächst am Reverse-Proxy, anschließend am Hintergrund-Server anmelden.



Fordert ein Hintergrund-Server ebenfalls Basic-Authentifizierung an, so darf die Authentifizierung im Reverse-Proxy nicht aktiviert werden.

URL-Pfad

Nur Anfragen mit passenden Pfad werden an den zugehörigen Hintergrund-Server weitergeleitet. Die Angabe ist als Präfix zu verstehen, d.h. danach sind beliebige Zeichen zulässig. Innerhalb der Pfadangabe dient das Symbol "*" als Platzhalter für beliebige Zeichen (inkl. dem Pfad-Trennzeichen). So passt z.B. der URL-Pfad "/bilder/a.gif?id=1" auf das Suchmuster "/*.gif". Der spezielle Pfad "/" definiert den Hintergrund-Server für beliebige Pfade und sollte daher immer als letzter Eintrag in der Liste stehen.



Falls es keinen "/" Eintrag gibt, werden Browser mit einer Fehlermeldung abgewiesen wenn diese nicht auf einen der angegebenen Pfade zugreifen.

Protokoll

Die Kommunikation zwischen SX-GATE und dem Hintergrund-Server kann sowohl verschlüsselt als auch unverschlüsselt erfolgen.

Server

Geben Sie hier bitte die IP-Adresse oder den DNS-Namen des Hintergrund-Servers an.

Port

Fehlt die Angabe, wird der Hintergrund-Server auf den Standard-Ports (80 bei HTTP, 443 bei HTTPS) angesprochen.

Faktor

Sofern die Lastverteilung aktiviert ist (mehrere Einträge mit identischem URL-Pfad), können über diesen Wert Unterschiede in der Leistungsfähigkeit der Hintergrund-Server ausgeglichen werden.

Kommentar

Dieses Feld steht zu Ihrer freien Verfügung.

Startseite umleiten auf URL

Wenn gewünscht, kann der Reverse-Proxy Zugriffe auf die Startseite (Pfad "/") mit einem HTTP-Redirect auf die hier angegebene Adresse beantworten. Auf diese Weise können Browser auf den Pfad eines bestimmten Hintergrund-Servers umgeleitet werden, ohne dass der Pfad dem Benutzer bekannt ist bzw. ohne dass dieser im Browser eingetippt werden muss. Geben Sie z.B. "https://owa.example.com/owa" ein, um Zugriffe auf "https://owa.example.com" an das Backend für Outlook-Web-App umzuleiten. Die Startseite kann auch auf die SX-GATE-Administrationsoberfläche umgeleitet werden. In dieser speziellen Einstellung werden zusätzlich auch Pfade die mit "/riabconf" beginnen umgeleitet.



Die Einstellung ist wirkungslos, wenn ein benutzerdefinierter Hintergrund-Server für den Pfad "/" konfiguriert ist.

Alle anderen Pfade

Legen Sie fest, wie mit URL-Pfaden verfahren werden soll, für die noch kein Hintergrund-Server konfiguriert wurde.



Die Einstellung ist wirkungslos, wenn ein benutzerdefinierter Hintergrund-Server für den Pfad "/" konfiguriert ist.

von http:// auf https:// umleiten (inkl. Pfad)

Mit dieser Einstellung können Sie unverschlüsselte auf verschlüsselte Verbindungen umleiten. URL-Pfade und Parameter bleiben dabei erhalten. So wird z.B. der Zugriff auf `http://www.example.com/pfad/datei.html` auf `https://www.example.com/pfad/datei.html` umgeleitet.

umleiten auf URL

Leiten Sie die Anfrage an eine beliebige URL um. Die URL muss mit `http://` oder `https://` beginnen. Durch Angabe eines URL-Pfades steuern Sie, ob Pfad und Parameter aus der Browser-Anfrage übernommen werden sollen oder nicht.



Enthält die hier konfigurierte URL keine Pfadangabe, werden Pfad und Parameter aus der Browser-Anfrage übernommen. Mit Pfadangabe (es genügt bereits ein "/"), werden die Browser stets an die konfigurierte Adresse umgeleitet.

Im Beispiel fragt der Browser die URL `"https://example.com/test.html?lang=de"` an.

Konfigurierte URL: `"https://www.example.com"` (ohne Pfad)

Browser wird umgeleitet nach `"https://www.example.com/test.html?lang=de"`

Konfigurierte URL: `"https://www.example.com/"` (Pfad ist "/")

Browser wird umgeleitet nach `"https://www.example.com/"`

Konfigurierte URL: `"https://www.example.com/willkommen/"` (Pfad ist `"/willkommen/"`)

Browser wird umgeleitet nach `"https://www.example.com/willkommen/"`

14.8.2.2-D Verbindungsparameter

Der Reverse-Proxy wird benötigt, um auf SX-GATE-Erweiterungen (Apps) zuzugreifen. Es ist außerdem möglich, auf den SX-GATE Administrations-Server zuzugreifen. Im Unterschied zum direkten Zugriff, kann im Reverse-Proxy der Zugriff auf einen Teilbereich eingeschränkt werden. So lässt sich der Zugriff auf die Mail-Quarantäne erlauben, während die SX-GATE Administration gesperrt bleibt.

TLS-Protokoll für HTTPS-Verbindungen

Wählen Sie hier die Verschlüsselungsstärke für HTTPS-Verbindungen vom SX-GATE zu den Hintergrund-Servern aus.



Im Rahmen der Produktpflege werden die mit der jeweiligen Auswahl verbundenen Parameter von Zeit zu Zeit angepasst.

veraltet

In dieser Einstellung wird das veraltete Hash-Verfahren SHA1 aktiviert. Die minimale TLS-Version ist 1.0.

kompatibel

Wählen Sie diese Einstellung für weitreichende Kompatibilität mit älteren Server-Systemen. Der veraltete Hash-Algorithmus SHA1 ist dabei aktiviert. Die minimale TLS-Version ist 1.2.

aktuell

In dieser Einstellung werden nur noch halbwegs aktuelle Server-Systeme unterstützt. Es wird mindestens TLS 1.2 vorausgesetzt. Wählen Sie diese Option für hohe Sicherheit.

maximal

Erfordert TLS 1.3.

HTTP(S)-Eigenschaften

Mit dieser Einstellung legen Sie fest, welche HTTP-Version für die Verbindung zum Hintergrund-Server genutzt wird und ob mehrere Anfragen über eine Verbindung geschickt werden dürfen.



Die Einstellung betrifft ausschließlich Verbindungen, die auf dem Reiter (Tab) "Hintergrund-Server" konfiguriert werden.

HTTP/1.0, eine Anfrage pro Verbindung

Dies ist die empfohlene Variante. Durch das Schließen der Verbindung nach jeder Anfrage werden die Auswirkungen von Speicherlöchern und Software-Fehlern begrenzt.

HTTP/1.1, mehrere Anfragen pro Verbindung

Der Reverse-Proxy hält Verbindungen zum Hintergrund-Server offen und sendet mehrere Anfragen über die gleiche Verbindung. Das erhöht den Durchsatz und reduziert die Last auf stark frequentierten Systemen. Greifen gerade mehrere Clients über den Reverse-Proxy auf den selben Hintergrund-Server zu, werden ggf. Anfragen unterschiedlicher Clients über die selbe Verbindung gesendet.

Integrierte Windows-Authentifizierung

Dieser Modus entspricht dem zuvor beschriebenen, jeder Verbindung eines Clients zum Reverse-Proxy wird jedoch exklusiv eine Verbindung vom Reverse-Proxy zum Hintergrund-Server zugeordnet. Dies ist erforderlich, wenn der Hintergrund-Server vom Client eine NTLM- oder Kerberos-Authentifizierung verlangt, da dabei nicht wie üblich einzelne Anfragen sondern die komplette Verbindung als ganzes authentifiziert wird.



Für Verbindungen, die auf dem Reiter (Tab) "Microsoft IIS-Dienste" konfiguriert werden, wird stets dieser Modus verwendet, unabhängig von der hier gewählten Einstellung.

14.8.2.2-E Lastverteilung

Sind auf dem Reiter (Tab) "Hintergrund-Server" mehrere Hintergrund-Server für den selben URL-Pfad konfiguriert, fungiert SX-GATE als Lastverteiler.

Aufgabe eines Lastverteilers ist es, die Anfragen auf eine Reihe von Hintergrund-Servern zu verteilen, die die identischen Inhalte bzw. Anwendungen zur Verfügung stellen. SX-GATEs Reverse-Proxy verteilt die Anfragen zufällig unter Berücksichtigung eines Gewichtungsfaktors, den Sie bei der Konfiguration des Hintergrund-Servers festlegen können. Die optionale Sitzungs-Erkennung erlaubt es, dass aufeinanderfolgende Anfragen des selben Clients immer an den selben Hintergrund-Server geleitet werden. Reagiert ein Hintergrund-Server nicht mehr, so erhält dieser vorübergehend keine neuen Anfragen mehr. Der Reverse-Proxy prüft dann im Abstand von 10 Sekunden ob der Server wieder verfügbar ist.

Sitzungs-Erkennung

Manche Anwendungen erfordern es, dass aufeinanderfolgende Anfragen des selben Clients immer vom selben Hintergrund-Server verarbeitet werden müssen. Der Hintergrund-Server führt dabei in der Regel selbst eine Sitzungs-Erkennung durch. Im

Optimalfall kann der Reverse-Proxy das selbe Kriterium zur Erkennung einer Sitzung anwenden wie der Hintergrund-Server.

<keine>

In dieser Einstellung werden Anfragen grundsätzlich zufällig auf die Hintergrund-Server verteilt. Diese Einstellung ist optimal für den Zugriff auf statische Informationsangebote.

IP-Adresse

Dies ist die einfachste Form der Sitzungserkennung. Aufeinanderfolgende Anfragen von der selben Quell-IP werden immer an den selben Hintergrund-Server weitergeleitet. Diese Methode kann problematisch werden wenn sich die Clients hinter einem Proxy-Cache befinden. Nutzen Sie diese Methode daher nur, wenn die Sitzungs-Erkennung nicht zu 100% zuverlässig sein muss oder wenn keine der folgenden Optionen in Frage kommt.

Basic Authentifizierung

Muss sich der Client mit Hilfe der sogenannten "Basic-Authentifizierung" anmelden, so kommt diese Option in Frage. Die Zugangsdaten werden dabei vom Browser in einem kleinen Anmeldefenster abgefragt. Aufeinanderfolgende Anfragen mit identischen Anmeldedaten erhält stets der selbe Hintergrund-Server. Es spielt dabei keine Rolle ob der Hintergrund-Server die Anmeldung verlangt oder SX-GATE's Reverse-Proxy.

URL-Parameter

Wird die Sitzungs-Kennung grundsätzlich als Wert eines bestimmten URL-Parameters übergeben, so wählen Sie bitte diese Option. Geben Sie dabei den Namen des entsprechenden Parameters an. Der Parameter-Teil einer URL beginnt mit einem Fragezeichen. Einzelnen Parameter werden durch "&"-Zeichen voneinander getrennt und haben die Form "Name=Wert". Aufeinanderfolgende Anfragen die den selben Wert für den angegebenen Parameter enthalten werden stets an den selben Hintergrund-Server geleitet.

Cookie

Erkennen die Hintergrund-Server eine Sitzung anhand eines Cookies, so wählen Sie bitte diese Option und geben Sie den Namen des Cookies an. Alle aufeinanderfolgenden Anfragen, die einen entsprechenden Cookie mit dem selben Wert enthalten, werden so vom selben Hintergrund-Server bearbeitet.

14.9 Weitere Proxies

In diesem Menü werden die folgenden Proxy-Dienste konfiguriert:

FTP-Proxy

FTP-Clients können diesen Proxy zur Kommunikation mit dem Internet verwenden. Es sind sowohl Up- als auch Downloads möglich. Verbindungen erfolgen über Port 2121 sofern nicht der transparente Zugriff aktiviert ist.

SIP-Proxy

Mit Hilfe des SIP-Proxies können sich SIP-Clients (z.B. VoIP-Telefone) über den SX-GATE ins Internet verbinden. Dabei kann der Proxy entweder als reiner Proxy oder als einfacher VoIP-Registrar eingesetzt werden. Durch den Dienst kann die NAT-Barriere des Gateways überwunden werden und Clients sind sowohl Lokal als auch aus dem Internet erreichbar.

POP3-/SMTP-Proxy

Dieser Proxy ermöglicht es Mail-Clients im LAN in Kontakt mit beliebigen POP3- und SMTP-Server im Internet zu treten. Die Nutzung ist ausschließlich transparent möglich.

SOCKS-Proxy

Bei einem SOCKS-Proxy handelt es sich um einen generischen Proxy, der seine Dienste auf Port 1080 anbietet. Anwendung, die nicht von selbst Unterstützung für SOCKS bieten, lassen sich meist mit Hilfe von SOCKS-Client-Software proxy-fähig machen.

14.9.1 FTP-Proxy

Der FTP-Proxy ermöglicht FTP-Clients den indirekten Zugriff auf FTP-Server. Im Vergleich zu einer Freigabe direkter FTP-Verbindungen in der Firewall bietet der Zugriff über Proxy diverse Vorteile. Es besteht keine direkte IP-Verbindung zwischen FTP-Client und FTP-Server. Restriktive Einstellungen bezüglich der erlaubten Ziel-Adressen verhindern Missbrauch. Die Sicherheitsüberprüfung der übertragenen Befehle sowie der optionale Virensan von Downloads erhöhen die Sicherheit zusätzlich.



In der Grundeinstellung ist jeglicher Zugriff über den FTP-Proxy verboten. Der Zugriff auf einzelne oder auch beliebige Server muss zunächst explizit freigegeben werden.

Mit Hilfe einer entsprechenden Regel in der Firewall-Konfiguration kann der FTP-Proxy auch transparent betrieben werden. Transparent bedeutet, dass der Client gar nicht merkt, dass die Anfragen über einen Proxy geleitet werden. Zudem ist keine Änderung an der Client-Konfiguration erforderlich. Wählen Sie unter "Module > Firewall > Regeln" die Schnittstelle aus, über die der Client die Verbindung aufnimmt. In der

Regel ist dies SX-GATE's LAN-Schnittstelle "eth0". Aktivieren Sie dort die Umleitung von Verbindungen zu Port 21 auf dem Reiter (Tab) "Transp. Proxy".

Auch ohne transparenten Zugriff kann jeder FTP-Client den Proxy nutzen. Bietet der FTP-Client die Konfiguration eines Proxies an, so tragen Sie SX-GATE als Proxy-Server mit Port 2121 ein. Die Bezeichnung des Proxy-Typs variiert von FTP-Client zu FTP-Client. Häufig wird dieser als "USER ohne Login", "USER with no login", "USER user@host:port" oder ähnlich bezeichnet. Selbst wenn der FTP-Client keine Proxy-Konfiguration anbietet, kann der SX-GATE-Proxy problemlos genutzt werden. Um in diesem Fall eine Verbindung mit einem FTP-Server aufzunehmen, dürfen Sie sich nicht mehr wie gewohnt direkt mit diesem verbinden. Geben Sie stattdessen als FTP-Server grundsätzlich SX-GATE an, egal wohin Sie sich verbinden wollen. Vergessen Sie nicht den abweichenden Port 2121. Bei einem FTP-Client der direkt über Befehlszeile aufgerufen wird (z.B. MS-DOS Eingabeaufforderung) wird die Portnummer in der Regel einfach als weiterer Parameter angegeben (z.B. "ftp 192.168.0.254 2121"). Anstelle des gewohnten Benutzernamens geben Sie nun den Benutzernamen gefolgt von einem "@"-Zeichen und der Adresse des Ziel-Servers an (z.B. "benutzer@ftp.example.com"). Falls erforderlich, kann ein abweichender Port auf dem Ziel-Server mit Doppelpunkt angehängt werden (z.B. "benutzer@ftp.example.com:21000"). Die Anmeldung erfolgt mit dem normalen Kennwort. Eine Benutzerauthentifizierung durch SX-GATE's FTP-Proxy findet nicht statt.



Im nicht-transparenten Modus kann der FTP-Proxy nur von "echten" FTP-Clients, nicht aber von Web-Browsern genutzt werden. Der FTP-Download via Web-Browser kann über SX-GATE's Web-Proxy auf Port 8080 erfolgen.

Zugriff auf folgende FTP-Server erlauben

In diesem Bereich legen Sie fest, auf welche Konten welchen FTP-Servers via Proxy zugegriffen werden darf. Ist die Liste leer, so verweigert der FTP-Proxy alle Zugriffe.

Konto

Geben Sie hier das Konto des FTP-Servers an auf das zugegriffen werden soll. Für anonymen Zugriff (anonymous FTP) geben Sie bitte "ftp" an. Lassen Sie das Eingabefeld leer um den Zugriff auf beliebige Konten des FTP-Servers zu erlauben.

Ziel-Server

Der Name bzw. die IP-Adresse des Ziel-FTP-Servers ist hier anzugeben. Wird keine Adresse angegeben, so akzeptiert der Proxy Zugriffe auf beliebige FTP-Server.

Port

Optional kann ein abweichender Port des FTP-Servers angegeben werden. Wird kein Port angegeben, so wird vom FTP-Standard-Port 21 ausgegangen.

Nachfolgend einige typische Beispielregeln, die Sie je nach Bedarf kombinieren können. Die Angabe des Server-Ports kann dabei grundsätzlich entfallen.

Zugriff auf beliebige FTP-Server

Lassen Sie dazu alle Felder frei und drücken Sie auf "Hinzufügen". Es erscheint die Regel "*@*:21".



Eine Kombination mit weiteren Regeln ist nur dann sinnvoll, wenn diese den Zugriff auf einen anderen Port betreffen.

Zugriff auf beliebige FTP-Server mit anonymous FTP

Geben Sie "ftp" als "Konto" ein und lassen Sie alle anderen Felder frei. Mit "Hinzufügen" wird die Regel "ftp@*:21" in die Liste aufgenommen.



Der Zugriff auf frei verfügbare Daten ist mit Hilfe dieser Regel möglich, während der Zugang zu geschützten Bereichen wie z.B. die Pflege privater Homepages nicht möglich ist.

Zugriff auf alle Konten eines bestimmten FTP-Servers

Geben Sie den Servernamen (z.B. ftp.example.com) als "Ziel-Server" ein, lassen Sie "Konto" jedoch frei. "Hinzufügen" erzeugt die Regel "*@ftp.example.com:21".

Zugriff auf ein bestimmtes Konto eines bestimmten FTP-Servers

Tragen Sie Konto und Servername in die entsprechenden Felder ein und drücken Sie "Hinzufügen". Die erstellte Regel lautet dann z.B. "webmaster@www.example.com:21".

Virenscan für Downloads

Ist dieser Schalter aktiviert, so werden alle Downloads die über den FTP-Proxy heruntergeladen werden auf Viren überprüft.



Uploads werden nicht gescannt.



Damit diese Funktion wirksam ist, muss ein funktionsfähiger Virens Scanner auf SX-GATE installiert sein. Die Lizenzen für den Virens Scanner sind nicht im SX-GATE enthalten und müssen separat erworben werden. Nähere Informationen zu unterstützten oder bereits installierten Virenscannern finden Sie im Menü "Module > Virens Scanner". Dort ist auch die Installation von Virenscannern vorzunehmen.

Sonderzeichen zulassen

Der Proxy filtert nicht druckbare Zeichen und Sonderzeichen wie z.B. Umlaute in Befehlen aus. Sofern Sie Zugriff auf Dateien mit Sonderzeichen benötigen, müssen Sie diesen Schalter aktivieren.

14.9.2 SIP-Proxy

Der Einsatz von Network-Adress-Translation (NAT) bei der direkten Kommunikation von Clients im LAN mit dem Internet ist für den uneingeschränkten Einsatz von Voice-over-IP ein Hindernis. Aus diesem Grund bietet SX-GATE für IP-Telefone die das SIP-Protokoll unterstützen einen SIP-Proxy mit integriertem RTP-Proxy an. Sowohl die Signalisierung als auch das eigentliche Gespräch können so über den Proxy geführt werden.



Lediglich IP-Telefone die an der SX-GATE-Schnittstelle eth0 angeschlossen sind können sich mit dem SIP-Proxy verbinden. Es wird ausschließlich die Kommunikation mit UDP unterstützt.

Der SIP-Proxy kann auf zweierlei Art verwendet werden.

Outbound-Proxy mit externem Registrar

Bei dieser Variante melden sich die IP-Telefone bei einem externen Registrar im Internet an. Zusatzdienste des VoIP-Providers wie z.B. Anrufbeantworter oder Gateways in das leitungsgebundene Telefonnetz stehen weitestgehend zur Verfügung. Der Proxy des SX-GATE dient hier in erster Linie dazu, eingehende Rufe an das richtige interne IP-Telefon durchzustellen.



Ein Anruf an ein anderes lokales IP-Telefon wird nicht über den externen Registrar geführt.



Ist SX-GATE mit einer dynamischen IP an das Internet angebunden, dann muss in den IP-Telefonen ein sehr kurzes Anmeldeintervall eingestellt werden. Der Registrar erfährt erst bei der nächsten Anmeldung des IP-Telefons vom Wechsel der Internet-IP. Die maximale Zeitdauer für die ein lokales IP-Telefon nicht erreichbar ist entspricht daher dem konfigurierten Anmeldeintervall.

Um dieses Szenario zu konfigurieren, geben Sie bitte die interne IP-Adresse des SX-GATE im IP-Telefon als Outbound-Proxy an. Die Zugangsdaten sowie den Namen des Registrar-Servers erfahren Sie von Ihrem VoIP-Provider.

Lokaler Registrar

Der SIP-Proxy des SX-GATE kann auch als einfacher Registrar genutzt werden. Damit eingehende Rufe SX-GATE erreichen, muss ein entsprechender Eintrag im DNS auf die externe IP-Adresse des SX-GATE verweisen.



Bei dynamischer IP des SX-GATE muss auf dynamisches DNS zurückgegriffen werden. Das Anmeldeintervall des IP-Telefons spielt hier keine Rolle. Nach einem Wechsel der IP-Adresse sind die Teilnehmer für die Dauer der Aktualisierung des DNS-Eintrags nicht erreichbar.

Die IP-Telefone müssen in diesem Falle folgendermaßen konfiguriert werden: Geben Sie den verwendeten DNS-Namen als Registrar-Server ein. Der Benutzername ist beliebig, muss aber eindeutig sein. Eingehende Rufe erreichen den Teilnehmer unter diesem Namen. Als Outbound-Proxy ist schließlich auch in diesem Szenario die interne IP-Adresse des SX-GATE einzutragen.



Eine Authentifizierung der Benutzer findet nicht statt. Die Nutzung des SIP-Proxies kann jedoch auf bestimmte IP-Adressen eingeschränkt werden.

In der Firewall-Konfiguration der Internet-Schnittstelle ist der Zugriff auf SX-GATE für den UDP-Port 5060 freizugeben.



Wird ein externer Registrar verwendet, so ist es unter Umständen ausreichend, lediglich Pakete von einzelnen IPs des VoIP-Providers zu akzeptieren.

Registrierungen von folgenden IP-Adressen akzeptieren

Der SIP-Proxy des SX-GATE erlaubt es ausschließlich den hier angegebenen Adressen sich zu registrieren. Dabei spielt es keine Rolle ob SX-GATE selbst als Registrar fungiert oder ob ein externer Registrar genutzt wird.



Die hier angegebenen Adressen müssen allesamt an der SX-GATE-Schnittstelle eth0 angeschlossen sein.

Zu löschende SIP-Header

Werden SIP-Nachrichten so groß, dass das zugehörige Netzwerkpaket fragmentiert werden muss, führen häufig zu Problemen. Mit etwas Glück lässt sich die Fragmentierung vermeiden, indem unnötige Header entfernt werden.

14.9.3 POP3-/SMTP-Proxy

Über den POP3-/SMTP-Proxy ist es Benutzern möglich, E-Mails von beliebigen POP3-Servern im Internet zu holen bzw. über beliebige SMTP-Server zu versenden, ohne auf SX-GATEs Virenschutz und SPAM-Filter verzichten zu müssen.



Der Proxy ist primär dafür gedacht, einzelne (private) Mailkonten zu bedienen. Der reguläre (geschäftliche) Mail-Verkehr sollte über SX-GATEs Mail-Client und -Server abgewickelt werden, die über deutlich mehr Leistungsmerkmale verfügen.

Der POP3-/SMTP-Proxy kann ausschließlich transparent verwendet werden. Aktivieren Sie dazu in der Firewall-Konfiguration die entsprechenden Schalter oder geben Sie manuell DNAT-Regeln ein, die POP3- bzw. SMTP-Verbindungen an Port 8110 umleiten.

Sollte Ihr Provider den Pop-Server nicht auf Port 110 sondern ausschließlich auf Port 995 (POP3S) anbieten, gehen Sie bitte wie folgt vor:

- Richten Sie Ihren Mail-Client so ein, dass er eine unverschlüsselte Verbindung zu Port 995 aufbaut.
- Konfigurieren Sie in der Firewall-Konfiguration der SX-GATE LAN-Schnittstelle eine DNAT-Regel, die das Protokoll POP3S auf Port 8110 des SX-GATEs umleitet.

Maximale Anzahl gleichzeitiger Verbindungen

Dieser Parameter legt fest, wie viele Verbindungen gleichzeitig über den Proxy laufen dürfen.



Wenn die Virensan-Option aktiviert ist, legt dieser Parameter zugleich fest, wie viele Scanner-Instanzen der Proxy potentiell gleichzeitig aktiviert. Je nach installiertem Virensan besteht das Risiko einer System-Überlastung. Der Wert sollte daher nicht zu hoch eingestellt werden.

Zertifikate prüfen

Während die Kommunikation zwischen Client und Proxy grundsätzlich unverschlüsselt ist, erfolgt die internetseitige Kommunikation zwischen Proxy und POP- bzw. SMTP-Server verschlüsselt, sofern dies der Server unterstützt. Ist dieser Schalter aktiviert, wird zudem geprüft, ob das Server-Zertifikat gültig ist und von einer vertrauenswürdigen CA ausgestellt wurde.



Ob der Servername im Zertifikat mit dem im Client angegebenen Zertifikat übereinstimmt kann nicht geprüft werden, da dem Proxy diese Information nicht vorliegt.

Virensan

Ist dieser Schalter aktiviert, so werden E-Mails auf Viren geprüft, die über den Proxy per POP3 heruntergeladen bzw. per SMTP versendete werden. Das Verhalten im Falle eines Virenfundes unterscheidet sich je nach Protokoll. Bei POP3 wird anstelle der infizierten E-Mail eine Nachricht ausgeliefert, die über den Virenfund informiert. Bei SMTP wird die Verbindung mit einer Fehlermeldung beendet.



Damit diese Funktion wirksam ist, muss ein funktionsfähiger Virensan auf SX-GATE installiert sein. Die Lizenzen für den Virensan sind nicht im SX-GATE enthalten und müssen separat erworben werden. Nähere Informationen zu unterstützten oder bereits installierten Virensanern finden Sie im Menü "Module > Virensan". Dort ist auch die Installation von Virensanern vorzunehmen.



Ist kein Virensan installiert, die Virensan-Lizenz abgelaufen oder wenn ein unerwarteter Fehler beim Scannen auftritt, wird der POP3/SMTP-Proxy beendet.

Nachricht an admin bei Virenfund

Grundsätzlich wird jeder Virenfund protokolliert. Für POP3-Verbindungen kann sich der Administrator zusätzlich per E-Mail über jeden Virenfund unterrichten lassen.

E-Mail als SPAM markieren bei mehr als

Diese Einstellung wirkt sich nur auf POP3-Verbindungen aus. Überschreitet der Punktwert einer E-Mail bei deren Klassifizierung diesen Schwellwert, so wird die E-Mail als SPAM-Mail markiert. Dabei wird dem Betreff der Text "***** SPAM *****" vorangestellt.



Das Verhalten des SPAM-Filters an sich wird unter "Module > Mail-Server > SPAM/Virus/Malware " konfiguriert.

14.9.4 SOCKS-Proxy

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.9.4-A Verbindungen.....	636
14.9.4-B Client-Zugriff.....	637

14.9.4-A Verbindungen

SOCKS bietet einen generischen Proxy-Dienst für Anwendungen, die sich nicht mit Hilfe von anderen Proxies oder von NAT-Firewall-Regeln mit dem Internet verbinden können. Unterstützt werden die Protokolle SOCKS4 und SOCKS5. Mit Hilfe von SOCKS-Wrapper-Anwendungen können nahezu alle netzwerkfähigen Programme den SOCKS-Proxy nutzen. Manche Anwendungen beinhalten sogar schon von sich aus einen SOCKS-Client.



Für Protokolle wie HTTP, HTTPS, FTP usw. für die SX-GATE einen speziellen Proxy-Dienst zur Verfügung stellt, sollte SOCKS nicht verwendet werden. Spezielle Proxy-Dienste können die jeweiligen Anforderungen besser abbilden als ein generischer Proxy-Dienst.



Daten, die über den SOCKS-Proxy übertragen werden unterliegen keinerlei Virenschutz. Ebenso werden übertragene Protokolle nicht hinsichtlich ihrer Korrektheit überprüft.

In der Grundeinstellung sind keinerlei Verbindungen über SOCKS-Proxy erlaubt. Verbindungen müssen explizit freigegeben werden. Regeln die in dieser Maske eingetragen werden gelten für alle SOCKS-fähigen Anwendungen gleichermaßen. Es ist jedoch auch möglich in der Benutzerverwaltung SOCKS-Verbindungen für jeden Benutzer einzeln zu konfigurieren. Diese Regeln stehen dem jeweiligen Benutzer erst nach erfolgreicher Authentifizierung zur Verfügung.

Globale Regeln

Die hier konfigurierten Regeln beschreiben, welche Verbindungen über den SOCKS-Proxy aufgebaut werden dürfen.

Wählen Sie zunächst das gewünschte Protokoll aus. Optional können Sie durch Angabe einer einzelnen IP-Adresse bzw. eines Netzwerks mit zugehöriger Netzmaske die Freigabe auf bestimmte Clients oder Server beschränken.



Protokoll-Definitionen werden im Menü "Definitionen > Protokolle" vorgenommen.



Protokoll-Signaturen die sich weder auf UDP noch auf TCP beziehen werden ignoriert.

14.9.4-B Client-Zugriff

Proxy-Zugriff für folgende Quell-IP-Adressen

Der SOCKS-Proxy des SX-GATE akzeptiert ausschließlich Verbindungen von Clients mit den hier angegebenen Adressen.

14.10 HTTP-Server

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.10-A Intranet.....	638
14.10-B WWW.....	639
14.10-C Webseiten-Pflege.....	640
14.10-D Erweitert.....	641

14.10-A Intranet

SX-GATE bietet Ihnen die Möglichkeit, Dokumente im Intranet mit Hilfe eines Web-Servers zu publizieren. Der Intranet-Web-Server kann ausschließlich von Adressen angesprochen werden, die unter "Definitionen > IP-Objekte" in "INTRANET" hinterlegt sind. Auch über den Web-Proxy des SX-GATE ist ein Zugriff möglich. Die Verwaltung der in diesem Bereich abgelegten Seiten ist sowohl über die Windows-Netzwerkumgebung als auch über FTP möglich. Nutzen Sie zur Anmeldung jeweils den vordefinierten Benutzer "intranet".



In der Grundkonfiguration ist dieser Dienst nicht aktiv. Starten Sie den Web-Server unter "System > Dienste".

Servername des Intranet-Servers

Hier legen Sie den Namen des Intranet-Servers fest. Gegebenenfalls müssen Sie noch für einen passenden DNS-Eintrag zu diesem Namen sorgen. Der Intranet-Server wird entweder über den hier konfigurierten Namen oder über die LAN-IP-Adresse angesprochen.

Web-Proxy Auto-Discovery Domain

Die meisten Web-Browser können die Proxy-Konfiguration automatisch beziehen. Dazu lädt der Browser eine Konfigurationsdatei von einem Web-Server herunter. Die Adresse dieser Datei wird mit Hilfe der Web-Proxy Auto-Discovery (WPAD) ermittelt. Dieses Verfahren sieht zum einen vor, die Adresse per DHCP bekannt zu geben. Konfiguriert wird dies im Menü "Module > DHCP" auf dem Reiter (Tab) "Windows-Parameter". Das alternative DNS basierte Verfahren aktivieren Sie hier. Der Browser versucht dabei die Datei "wpad.dat" vom Web-Server mit der Adresse "wpad.<LOKALE DOMAIN>" herunterzuladen.

Geben Sie hier die Netzwerk-Domain ein, die in Ihren Arbeitsstationen eingestellt ist. SX-GATE richtet dann passende DNS-Einträge in seinem Name-Server ein und aktiviert im Intranet-Web-Server eine Umleitung der Datei "wpad.dat" auf die Adresse "http://<SX-GATEs LAN-IP>:8000/proxy.pac"

. Dabei handelt es sich um eine vordefinierte Konfigurationsdatei, die Browser anweist, den SX-GATE Web-Proxy zu nutzen.



Sollten sich die Arbeitsstationen in verschiedenen Subdomains befinden (z.B. "vertrieb.example.com" und "management.example.com"), so können Sie die gemeinsame Hauptdomain eintragen ("example.com").

Passwort des Benutzers "intranet" ändern

Hier können Sie das Passwort für den vordefinierten Benutzer "intranet" festlegen oder dieses Konto deaktivieren. Der Benutzer "intranet" dient der Pflege des Intranet-Web-Server Verzeichnisses.



Dieser Benutzer ist in der Benutzerverwaltung des SX-GATE nicht aufgeführt.

14.10-B WWW

SX-GATE bietet Ihnen die Möglichkeit, einen einfachen Internet-Web-Server zu betreiben. Die Verwaltung der in diesem Bereich abgelegten Seiten ist sowohl über die Windows-Netzwerkumgebung als auch über FTP möglich. Nutzen Sie zur Anmeldung jeweils den vordefinierten Benutzer "www".

WWW-Server aktivieren

Mit Hilfe dieses Schalters aktivieren Sie den Internet-Web-Server. Ist dieser Schalter nicht aktiviert, so steht lediglich der Intranet-Bereich für die lokalen Netzwerke zur Verfügung.



Um den Zugriff aus dem Internet auf den Web-Server zu ermöglichen, muss in der Regel der HTTP-Port 80 in der Firewall-Konfiguration freigegeben werden. Zudem ist der Web-Server in der Grundkonfiguration nicht aktiv. Starten Sie diesen unter "System > Dienste".

Servername des WWW-Servers

Hier legen Sie den Namen des Web-Servers fest (z.B. www.example.com). Gegebenenfalls müssen Sie noch für einen passenden DNS-Eintrag zu diesem Namen sorgen. Dieser wird in der Regel durch Ihren Provider vorgenommen.

Passwort des Benutzers "www" ändern

Hier können Sie das Passwort für den vordefinierten Benutzer "www" festlegen oder dieses Konto deaktivieren. Der Benutzer "www" dient der Pflege des WWW-Server Verzeichnisses.



Dieser Benutzer ist in der Benutzerverwaltung des SX-GATE nicht aufgeführt.

14.10-C Webseiten-Pflege

Die Windows-Freigaben des SX-GATE können verwendet werden um die Web-Server des SX-GATE bequem über die Windows-Netzwerkumgebung zu verwalten.



Im Auslieferungszustand ist der entsprechende Server-Dienst deaktiviert. Starten Sie diesen unter "System > Dienste".

Zugriff über Windows-Freigabe

Der Zugriff auf die Windows-Freigaben ist ausschließlich von Adressen möglich, die unter "Definitionen > IP-Objekte" in "INTRANET" hinterlegt sind.

Windows Arbeitsgruppe oder Domäne

Bitte tragen Sie hier den Namen Ihrer Windows-Arbeitsgruppe oder -Domäne ein.



Verwechseln Sie bitte die Windows-Domäne nicht mit Ihrer Internet-Domain.

Intranet-Server Freigabe aktiv

Mit Hilfe dieses Schalters aktivieren Sie die Freigabe "intranet". Über diese können Sie die statischen Dokumente auf dem Intranet-Server des SX-GATE pflegen.



Um sich mit dieser Freigabe verbinden zu können, müssen Sie sich als Benutzer "intranet" anmelden. Das zugehörige Passwort wird im Menü "Module > HTTP-Server" festgelegt.

Intranet-CGI Freigabe aktiv

Mit Hilfe dieses Schalters aktivieren Sie die Freigabe "intracgi". Über diese können Sie CGI-Skripts auf dem Intranet-Server des SX-GATE pflegen.



Um sich mit dieser Freigabe verbinden zu können, müssen Sie sich als Benutzer "intranet" anmelden. Das zugehörige Passwort wird im Menü "Module > HTTP-Server" festgelegt.

WWW-Server Freigabe aktiv

Mit Hilfe dieses Schalters aktivieren Sie die Freigabe "www". Über diese können Sie die statischen Dokumente auf dem Web-Server des SX-GATE pflegen.



Um sich mit dieser Freigabe verbinden zu können, müssen Sie sich als Benutzer "www" anmelden. Das zugehörige Passwort wird im Menü "Module > HTTP-Server" festgelegt.

WWW-CGI Freigabe aktiv

Mit Hilfe dieses Schalters aktivieren Sie die Freigabe "wwwcgi". Über diese können Sie CGI-Skripts auf dem Web-Server des SX-GATE pflegen.



Um sich mit dieser Freigabe verbinden zu können, müssen Sie sich als Benutzer "www" anmelden. Das zugehörige Passwort wird im Menü "Module > HTTP-Server" festgelegt.

14.10-D Erweitert

E-Mail Adresse des Administrators

Übermittelt der Web-Server eine Fehlermeldung an den Browser, so wird dem Anwender diese Adresse als Kontaktadresse für den Web-Server angezeigt.

14.11 FTP-Server

Hier können Sie konfigurieren, welche Benutzerklasse wie Zugriff auf den FTP-Server des SX-GATE hat. Die Beschränkung "nur aus lokalen IP-Subnetzen" bezieht sich dabei auf Quell-IP-Adressen, die in "Definitionen > IP-Objekte" unter "INTRANET" hinterlegt sind.

Zugriff für admin

Dieser Schalter legt die Zugriffsberechtigung für den Benutzer "admin" fest.

Zugriff für ftpadmin/intranet/www

Hier können Sie konfigurieren, ob der Zugriff für die vorgegebenen Benutzer "ftpadmin", "www" und "intranet" zugelassen ist. Der Benutzer "ftpadmin" dient der Pflege der FTP-Verzeichnisse für anonymen Zugriff (anonymous FTP) und der Pflege des TFTP-Server-Verzeichnisses. Die Benutzer "www" und "intranet" sind vorgesehen, um die entsprechenden Bereiche des SX-GATE Web-Servers zu pflegen. Die Verzeichnisse dieser Benutzer sind dabei speziell abgesichert, so dass der FTP-Client diese nicht verlassen kann.

Zugriff ohne Anmeldung (anonymous)

Der SX-GATE bietet Ihnen die Möglichkeit, mit Hilfe des eingebauten anonymous FTP-Servers Dateien bereitzustellen. Die Verwaltung dieser Dateien erfolgt über FTP mit Hilfe des vordefinierten Benutzers "ftpadmin". FTP-Clients, die als anonymer Benutzer mit dem FTP-Server verbunden sind, können das Basis-Verzeichnis dieses Dienstes nicht verlassen.

Upload in Verzeichnis "incoming" für anonymous

Wenn es möglich sein soll, bei anonymer Anmeldung Dateien auf dem SX-GATE zu speichern, aktivieren Sie bitte den entsprechenden Schalter. Die Dateien müssen auf dem FTP-Server im Verzeichnis "incoming" abgelegt werden. Vom Benutzer "ftpadmin" kann in diesem Verzeichnis eine Verzeichnishierarchie angelegt werden. Das Herunterladen von Dateien aus dem Verzeichnis "incoming" ist anonymen Benutzern nicht möglich.

Passwort des Benutzers "ftpadmin" ändern

Hier können Sie das Passwort für den vordefinierten Benutzer "ftpadmin" festlegen oder dieses Konto deaktivieren. Der Benutzer "ftpadmin" dient der Pflege des FTP-Server-Verzeichnisses für anonymous FTP und der Pflege des TFTP-Server-Verzeichnisses.



Dieser Benutzer ist in der Benutzerverwaltung des SX-GATEs nicht aufgeführt.

14.12 SNMP-Server

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.12-A Allgemein.....	643
14.12-B SX-GATE-OIDs.....	644

14.12-A Allgemein

Diverse Informationen zum Status des SX-GATE lassen sich über SNMP abfragen. Starten Sie dazu bitte den Dienst im Menü "System > Dienste".



Es wird ausschließlich SNMPv3 unterstützt. Authentifizierung und Verschlüsselung sind verpflichtend.

Zugriff für folgende IP-Adressen

Nur die hier freigegebenen IP-Adressen dürfen Informationen vom SNMP-Server abrufen.

Benutzername

Geben Sie hier den Benutzernamen und das Kennwort an, mit dem sich Clients am SNMP-Server anmelden müssen. Das Kennwort muss mindestens 8 Zeichen lang sein.

Authorisationsprotokoll

Wählen Sie hier das Verfahren zur gesicherten Übermittlung des Kennworts.



Die Protokolle MD5 und SHA1 sollten nicht mehr verwendet werden. SHA-224 wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht empfohlen. Sie werden aus Kompatibilitätsgründen angeboten. Verwenden Sie bitte SHA-256,SHA-384 oder SHA-512.

Privacy Passphrase

Die SNMP-Kommunikation wird mit Hilfe dieser Passphrase verschlüsselt. Verwenden Sie bitte einen möglichst langen Text, bestehend aus Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen. Die Mindestlänge beträgt 8 Zeichen.

Privacy Protocol

Wählen Sie bitte den Verschlüsselungsalgorithmus aus.



Das DES Protokoll sollte nicht mehr verwendet werden. Er wird aus Kompatibilitätsgründen angeboten. Verwenden Sie bitte stattdessen AES-256, AES-192 oder AES-128.

Kontakt-Information

Dieser Wert dient ausschließlich der Information.

Standort-Information

Dieser Wert dient ausschließlich der Information.

14.12-B SX-GATE-OIDs

SX-GATE verfügt über produktspezifische OIDs. Diese können Sie hier aktivieren.

Die Werte der einzelnen, individuellen OIDs werden unabhängig von ihrem Abruf regelmäßig aktualisiert. Das Intervall ist an die Basis-OID gekoppelt und liegt zwischen einer Minute (z.B. Status eines Dienstes) und 12 Stunden (z.B. SX-GATE-Version). Weitere Informationen finden Sie in der Beschreibung der SX-GATE-MIB.



Es kann bis zu 15 Sekunden dauern, bis die vollständigen Werte nach dem erstmaligen Abruf einer OID nach dem Neustart des Dienstes zur Verfügung stehen.

SX-GATE-oids aktivieren

SX-GATE-oids aktivieren

14.13 Logging

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.13-A Archivierung.....	645
14.13-B Externer Syslog-Server.....	647
14.13-C SX-GATE Syslog-Server.....	648
14.13-D Netflow/IPFIX.....	648
14.13-E Anomalieerkennung.....	649

14.13-A Archivierung

Neben der Archivierung auf dem System selbst lassen sich bestimmte Log-Dateien automatisch extern auf einen SMB-, FTP-, SFTP- oder Secure-Shell-Server gzip-komprimiert archivieren. Auch ein Versenden per E-Mail ist möglich, dies ist aufgrund der eventuellen Größe der Log-Dateien jedoch nicht zu empfehlen. Die externe Archivierung erfolgt wie auch die interne in der Regel kurz nach 00:00 Uhr.



Bitte beachten Sie die gesetzlichen Rahmenbedingungen. Die Archivierung von Log-Dateien könnte insbesondere aus Gründen des Datenschutzes nicht zulässig sein.

In den folgenden Feldern können Sie je Log-Datei bestimmen, ob und wie diese archiviert werden soll. Lassen Sie das Feld leer, wenn keine Archivierung gewünscht ist. Andernfalls geben Sie bitte das Ziel der Archivierung in URL-Schreibweise an.

Archivierung via SMB (Windows-Freigabe):

Um das Log auf einem SMB-Server abzulegen, verwenden Sie bitte das Format "smb://LOGIN:PASSWORT@ADRESSE/SHARE/PFAD/DATEINAME".

Lautet die URL beispielsweise

"smb://admin:geheim@127.0.0.1/logs/pfad/messages.log",

so meldet sich SX-GATE am SMB-Server 127.0.0.1 als Benutzer "admin" mit dem Kennwort "geheim" an. Das Backup wird auf der Freigabe "logs" im Verzeichnis "pfad" als Datei "messages.log" abgespeichert. Die Angabe der Freigabe ist zwingend, das Verzeichnis ist optional. Wird ein Verzeichnis angegeben, so muss dieses jedoch bereits existieren.

Archivierung via FTP:

Um das Log auf einem FTP-Server abzulegen, verwenden Sie bitte das Format "ftp://LOGIN:PASSWORT@ADRESSE/PFAD/DATEINAME".

Lautet die URL beispielsweise

"ftp://admin:geheim@127.0.0.1/logs/messages.log",

so meldet sich SX-GATE am FTP-Server 127.0.0.1 als Benutzer "admin" mit dem Kennwort "geheim" an. Das Backup wird im Verzeichnis "logs" als Datei "messages.log" abgespeichert. Die Angabe eines Verzeichnisses ist optional. Wird ein Verzeichnis angegeben, so muss dieses jedoch bereits existieren.

Sollte die Archivierung nur über einen vorgeschalteten FTP-Proxy möglich sein, so fügen Sie bitte ein Leerzeichen und eine FTP-Proxy-Spezifikation an. Diese ist im Format

"ftpproxy://ADRESSE:PORT"

anzugeben. Sofern der Proxy Authentifizierung erfordert, verwenden Sie bitte das Format

"ftpproxy://LOGIN:PASSWORT@ADRESSE:PORT".

Archivierung via SFTP

Das Log lässt sich auch verschlüsselt an einen SFTP-Server übermitteln. Geben Sie das Ziel im Format

"sftp://LOGIN@ADRESSE/PFAD/DATEINAME"

an (z.B. sftp://admin@127.0.0.1/logs/messages.log). Die Authentifizierung erfolgt dabei nicht über ein Passwort sondern mit Hilfe des ED25519- oder RSA-Schlüssels von SX-GATE. Der SFTP-Server ist entsprechend zu konfigurieren. Das angegebene Verzeichnis muss auf dem Zielsystem existieren.

Archivierung via Secure-Copy (Secure-Shell)

Wie SFTP überträgt auch Secure-Copy das Log verschlüsselt. Geben Sie das Ziel im Format

"scp://LOGIN@ADRESSE/PFAD/DATEINAME"

an (z.B. scp://admin@127.0.0.1/logs/messages.log). Die Authentifizierung erfolgt dabei nicht über ein Passwort sondern mit Hilfe des ED25519- oder RSA-Schlüssels von SX-GATE. Der Secure-Shell-Server ist entsprechend zu konfigurieren. Auch hier ist die Angabe von Unterverzeichnissen optional. Angegebene Verzeichnisse müssen bereits existieren.

Archivierung via E-Mail:

Aufgrund der Größe der Log-Dateien wird dringend von diesem Verfahren abgeraten. Sollten Sie diese Methode dennoch nutzen wollen, so geben Sie die URL bitte im Format "mailto:ADRESSE" an.

Sowohl bei der Archivierung über FTP also auch über SMB und Secure-Copy lassen sich in den Dateinamen Variablen einbauen. Auf diese Weise werden zuvor archivierte Log-Dateien nicht sofort wieder überschrieben.

Es stehen u.a. folgende Variablen zur Verfügung:

- %Y: Jahr 4-stellig (z.B. 2001)
- %y: Jahr 2-stellig (z.B. 01)
- %m: Monat (von 01 bis 12)
- %d: Tag (von 01 bis 31)
- %H: Stunde (von 00 bis 23)
- %M: Minute (von 00 bis 59)
- %S: Sekunde (von 00 bis 59)
- %U: Woche des Jahres (Werte von 00 bis 53)
- %w: Tag der Woche (0 für Sonntag bis 6 für Samstag)
- %j: Tag im Jahr (von 001 bis 366)

Wenn als Ziel der Archivierung z.B.

"scp://admin@127.0.0.1/logs/messages-%m-%d.log"

angegeben wird, enthält der Dateiname stets den aktuellen Monat und Tag als Zahl. Eine Log-Datei würde somit erst im folgenden Jahr wieder überschrieben werden.

Alle alten Log-Dateien löschen

Dieser Befehl löscht alle alten Log-Dateien im System. Sollte aufgrund ungewöhnlich großer Log-Dateien der Speicherplatz knapp werden, kann so wieder Platz geschaffen werden. Je nach Rotations-Zyklus der jeweiligen Log-Datei werden alle Einträge des Vortages, der Vorwoche bis einschließlich Samstag bzw. des Vormonats gelöscht. Die aktuellen Log-Dateien bleiben unverändert erhalten.



Das Löschen der Log-Dateien sollte nur im Notfall ausgeführt werden. Wachsen die Log-Dateien sehr schnell an, ist die Ursache oft eine Fehlkonfiguration. Versuchen Sie diese ausfindig zu machen und abzustellen.



Die gelöschten Log-Dateien gehen unwiederbringlich verloren.

Archivierung testen

Mit diesem Befehl wird versucht, die aktuellen Log-Dateien an die konfigurierten Ziel-URLs zu übertragen.

14.13-B Externer Syslog-Server

Wenn Sie einen externen Syslog-Server im Einsatz haben, dann können Sie hier das Weiterleiten an diesen Server konfigurieren.



Es werden nur Log-Meldungen weitergeleitet, die über die Syslog-API generiert werden. Deshalb werden Meldungen in folgende Logdateien nicht übertragen:

- IDS/IPS
- Web-Proxy Zugriffe
- Web-Proxy Meldungen
- Reverse-Proxy Zugriffe
- Reverse-Proxy Meldungen
- WWW-Server Zugriffe
- WWW-Server Meldungen
- Intranet-Web-Server Meldungen
- Administrations-Oberfläche

14.13-C SX-GATE Syslog-Server

SX-GATE kann als Syslog-Server für andere Systeme fungieren.



Der Zugriff auf den Syslog-Dienst ist weder authentifiziert noch verschlüsselt. Nutzen Sie Firewall-Regeln, um den Zugriff auf diesen Port auf das absolut notwendige einzuschränken.

Port

Legen Sie hier fest, auf welchem Port der Syslog-Server angesprochen werden soll. Der Standard-Port ist 514.

14.13-D Netflow/IPFIX

Informationen zu Netzwerkverbindungen können an einen Netflow v5, v9 oder IPFIX-Server zur weiteren Analyse übermittelt werden.

Modus

Wählen Sie aus, welche Verbindungen übermittelt werden sollen.

ausgewählte Schnittstellen

Aktivieren Sie den Export in den Einstellungen der jeweiligen Schnittstelle im Menü "Module > Firewall > Regeln".

alle Schnittstellen

Die Verbindungen aller Schnittstellen werden exportiert. Ausgenommen ist geräteinterne Kommunikation.



Die erzeugte Datenmenge kann sehr hoch werden.

Kollektor

Geben Sie das System an, an das SX-GATE die Daten übermitteln soll. Der Kollektor sollte sich in einem lokalen Netzwerk befinden.



Die Daten werden weder authentifiziert noch verschlüsselt übermittelt.

14.13-E Anomalieerkennung

Die Anomalieerkennung sucht nach auffällig hohen Werten bei der Anzahl Zeilen in bestimmten Logdateien und beim Durchsatz der Internet-Schnittstelle. Ergibt die stündliche statistische Auswertung, dass eine Anomalie vorliegt, wird der "admin" per E-Mail benachrichtigt. Weitere Informationen zur Diagnose der gefundenen Anomalie finden Sie beim zugehörigen Schalter auf diesem Reiter (Tab).



Wenn Sie eine E-Mail-Benachrichtigung erhalten haben, bedeutet dies nicht, dass tatsächlich ein Fehler oder Problem vorliegt. Sie sollten die Mail trotzdem zum Anlass nehmen, das System zu überprüfen.

In der Regel werden Sie dem Problem durch Analyse von Log-Dateien im Menü "Monitoring > Log-Dateien" nachgehen. Wählen Sie die passende Log-Datei aus, erhöhen Sie die Anzahl angezeigter Zeilen deutlich und grenzen Sie den Zeitraum auf z.B. eine Stunde vor bis eine Stunde nach dem Auftreten der Anomalie ein. Falls nötig, können Sie das Log mit bestimmten Stichworten vorfiltern. Senden Sie dann den Suchauftrag ab. Beachten Sie bei der Anzeige der Ergebnisse das Histogramm links oben. Durch Ziehen der seitlichen Ränder, können Sie die Anzeige auf den Zeitbereich mit den häufigsten Einträgen einschränken.

Log "IDS/IPS"

Dieser Sensor zählt die "Priorität 1" Alarme des IDS/IPS-Systems. Zeilen, die entweder "Attempt" oder "ET_SCAN" enthalten, werden ignoriert.

Analysieren Sie die Log-Datei "IDS/IPS". Einen Überblick über die längere zeitliche Entwicklung erhalten Sie unter "Statistiken > Firewall > IDS/IPS".



Die Statistik wird täglich nach Mitternacht aktualisiert.

Log "Firewall"

Dieser Sensor zählt im Firewall-Log die Zeilen mit "drop" oder "rej", also abgefangene Pakete.

Analysieren Sie die Log-Datei "Firewall". Einen Überblick über die längere zeitliche Entwicklung erhalten Sie unter "Statistiken > Firewall > Paket-Filter".



Die Statistik wird täglich nach Mitternacht aktualisiert.

Log "Web-Proxy Zugriffe" (nur 400er Fehlercodes)

Dieser Sensor zählt Web-Proxy Zugriffe mit 400er Statuscodes. Diese Statuscodes werden gesendet, wenn der Client einen ungültigen Zugriff macht, z.B. wenn das Ziel der Anfrage nicht existiert oder bei aktivierter Benutzeranmeldung um vom Client Zugangsdaten anzufordern.

Analysieren Sie die Log-Datei "Web-Proxy Zugriffe". Filtern Sie die Suchergebnisse nach Statuscodes im 400er-Bereich. Einen Überblick über die längere zeitliche Entwicklung erhalten Sie unter "Statistiken > Proxies > Web-Proxy".



Die Statistik wird täglich nach Mitternacht aktualisiert.

Log "Web-Proxy Zugriffe"

Dieser Sensor zählt alle Web-Proxy Zugriffe.

Analysieren Sie die Log-Datei "Web-Proxy Zugriffe". Einen Überblick über die längere zeitliche Entwicklung erhalten Sie unter "Statistiken > Proxies > Web-Proxy".



Die Statistik wird täglich nach Mitternacht aktualisiert.

Log "Reverse-Proxy Zugriffe" (nur 500er Fehlercodes)

Dieser Sensor zählt Reverse-Proxy Zugriffe mit 500er Statuscodes. Diese Statuscodes werden gesendet, wenn ein serverseitiger Fehler vorliegt, z.B. kein passender Hintergrundserver definiert ist oder der Hintergrundserver nicht erreichbar ist.

Analysieren Sie die Log-Datei "Reverse-Proxy Zugriffe". Filtern Sie die Suchergebnisse nach Statuscodes im 500er-Bereich. Einen Überblick über die längere zeitliche Entwicklung erhalten Sie unter "Statistiken > Proxies > Reverse-Proxy".



Die Statistik wird täglich nach Mitternacht aktualisiert.

Log "Reverse-Proxy Zugriffe"

Dieser Sensor zählt alle Reverse-Proxy Zugriffe.

Analysieren Sie die Log-Datei "Reverse-Proxy Zugriffe". Einen Überblick über die längere zeitliche Entwicklung erhalten Sie unter "Statistiken > Proxies > Reverse-Proxy".



Die Statistik wird täglich nach Mitternacht aktualisiert.

Internetnutzung (eingehend)

Dieser Sensor überwacht die eingehend übertragene Datenmenge auf der Internet-Schnittstelle. Auslöser für einen Alarm kann ein lokales System sein, das sich viele Daten aus dem Internet holt oder ein externes System, das viele Daten schickt.

Sofern die Internet-Schnittstelle auch aktuell noch stark ausgelastet ist, können Sie sich die derzeit aktiven Verbindungen im Menü "Monitoring > Firewall" anzeigen lassen. Klicken Sie auf die entsprechenden Spaltentitel der Tabelle, um diese nach der übertragenen Datenmenge zu sortieren. Um zu prüfen, ob ein internes System der Verursacher ist, sortieren Sie nach der übertragenen Datenmenge vom Ziel zur Quelle. Um zu prüfen, ob ein externes System verantwortlich ist, sortieren Sie nach der Datenmenge von der Quelle zum Ziel.

Im Nachhinein ist es ansonsten leider schwierig nachzuvollziehen, was der Auslöser war. Eine graphische Darstellung der Bandbreitennutzung und der Anzahl Verbindungen erhalten Sie unter "Statistiken > Netzwerk". Weitere Anhaltspunkte liefern ggf. die täglich nach Mitternacht aktualisierten Menüs "Statistiken > Proxies" und "Statistiken > Web-Server". Wenn eine permanente Analysemöglichkeit gewünscht ist, kann auf dem Reiter (Tab) "Netflow/IPFIX" ein kontinuierlicher Export der

umfangreichen Firewall-Verbindungsdaten an ein darauf spezialisiertes System eingerichtet werden.

Internetnutzung (ausgehend)

Dieser Sensor überwacht die ausgehend übertragene Datenmenge auf der Internet-Schnittstelle. Auslöser für einen Alarm kann ein lokales System sein, das viele Daten in das Internet sendet oder ein externes System, das viele Daten holt.

Sofern die Internet-Schnittstelle auch aktuell noch stark ausgelastet ist, können Sie sich die derzeit aktiven Verbindungen im Menü "Monitoring > Firewall" anzeigen lassen. Klicken Sie auf die entsprechenden Spaltentitel der Tabelle, um diese nach der übertragenen Datenmenge zu sortieren. Um zu prüfen, ob ein internes System der Verursacher ist, sortieren Sie nach der übertragenen Datenmenge von der Quelle zum Ziel. Um zu prüfen, ob ein externes System verantwortlich ist, sortieren Sie nach der Datenmenge vom Ziel zur Quelle.

Im Nachhinein ist es ansonsten leider schwierig nachzuvollziehen, was der Auslöser war. Eine graphische Darstellung der Bandbreitennutzung und der Anzahl Verbindungen erhalten Sie unter "Statistiken > Netzwerk". Weitere Anhaltspunkte liefern ggf. die täglich nach Mitternacht aktualisierten Menüs "Statistiken > Proxies" und "Statistiken > Web-Server". Wenn eine permanente Analysemöglichkeit gewünscht ist, kann auf dem Reiter (Tab) "Netflow/IPFIX" ein kontinuierlicher Export der umfangreichen Firewall-Verbindungsdaten an ein darauf spezialisiertes System eingerichtet werden.

14.14 Virens Scanner

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.14-A Signatur-Update.....	653
14.14-B Avira.....	653
14.14-C WithSecure (F-Secure).....	654
14.14-D Kaspersky.....	655
14.14-E Installation / Update / Deinstallation.....	655

14.14-A Signatur-Update

Virensignaturen automatisch aktualisieren

Aktivieren Sie diesen Schalter, wenn die Virensignaturen für die installierten Virens Scanner regelmäßig aktualisiert werden sollen.

Benachrichtigung über Signatur-Update

Auf Wunsch wird der Administrator per E-Mail über jedes versuchte Update in Kenntnis gesetzt. Ist diese Option nicht aktiviert, wird nur im wiederholten Fehlerfall eine Nachricht gesendet, d.h. bei einem einzelnen fehlgeschlagenen Updateversuch erfolgt noch keine Benachrichtigung.



Grundsätzlich ist es empfehlenswert, sich auch über scheinbar erfolgreiche Updates unterrichten zu lassen. Nicht jeder Fehlerzustand kann vom System automatisch als solcher identifiziert werden.

14.14-B Avira

Der Avira Virens Scanner für SX-GATE muss exklusiv über den SX-GATE Fachhandel bezogen werden. Die verfügbaren Lizenzen gelten ausschließlich für die Installation des Scanners auf SX-GATE und sind abhängig von der Anzahl Benutzer. Die Gültigkeit ist zeitlich begrenzt. Die Lizenz muss also regelmäßig erneuert werden. Dies geschieht mit Hilfe eines speziellen Lizenzschlüssels, den Sie beim Erwerb bzw. bei der Verlängerung einer Lizenz in Form einer Datei erhalten. Diese muss in diesem Menü im Bereich "Installation / Update / Deinstallation" installiert werden. Über den Ablauf der Lizenz informiert SX-GATE den Administrator rechtzeitig per E-Mail.



Eventuelle Software-Updates des Avira Virens scanners werden als Bestandteil der regulären SX-GATE Updates vorgenommen.

Online-Unterstützung des Scanners?

Wenn die Online-Unterstützung aktiviert ist, dann kontaktiert der Scanner den Onlinedienst des Scanner-Herstellers um die Erkennungsrate zu verbessern.

Installierte Version

In diesem Bereich werden nähere Informationen zum installierten Avira Scanner angezeigt. Durch den Aufruf dieser Seite erfolgt zudem eine Funktionsprüfung. Bei Erfolg wird der Status "OK" gemeldet.

Signaturen jetzt aktualisieren

Drücken Sie diesen Schalter um sofort eine Aktualisierung der Avira Virensignaturen durchzuführen.

14.14-C WithSecure (F-Secure)

Der WithSecure Virens scanner für SX-GATE muss exklusiv über den SX-GATE Fachhandel bezogen werden. Die verfügbaren Lizenzen gelten ausschließlich für die Installation des Scanners auf SX-GATE und sind abhängig von der Anzahl Benutzer. Die Gültigkeit ist zeitlich begrenzt. Die Lizenz muss also regelmäßig erneuert werden. Dies geschieht mit Hilfe eines speziellen Lizenzschlüssels, den Sie beim Erwerb bzw. bei der Verlängerung einer Lizenz in Form einer Datei erhalten. Diese muss in diesem Menü im Bereich "Installation / Update / Deinstallation" installiert werden. Über den Ablauf der Lizenz informiert SX-GATE den Administrator rechtzeitig per E-Mail.



Installation und Aktualisierungen der WithSecure Antivirus App nehmen Sie bitte auf "System > Apps" vor.

Online-Unterstützung des Scanners?

Wenn die Online-Unterstützung aktiviert ist, dann kontaktiert der Scanner den Onlinedienst des Scanner-Herstellers um die Erkennungsrate zu verbessern.

Installierte Version

In diesem Bereich werden nähere Informationen zum installierten WithSecure Scanner angezeigt. Durch den Aufruf dieser Seite erfolgt zudem eine Funktionsprüfung. Bei Erfolg wird der Status "OK" gemeldet.

Signaturen jetzt aktualisieren

Drücken Sie diesen Schalter um sofort eine Aktualisierung der WithSecure Virensignaturen durchzuführen.

14.14-D Kaspersky

Der Kaspersky Virenschanner für SX-GATE muss exklusiv über den SX-GATE Fachhandel bezogen werden. Die verfügbaren Lizenzen gelten ausschließlich für die Installation des Scanners auf SX-GATE und sind abhängig von der Anzahl Benutzer. Die Gültigkeit ist zeitlich begrenzt. Die Lizenz muss also regelmäßig erneuert werden. Dies geschieht mit Hilfe eines speziellen Lizenzschlüssels, den Sie beim Erwerb bzw. bei der Verlängerung einer Lizenz in Form einer Datei erhalten. Diese muss in diesem Menü im Bereich "Installation / Update / Deinstallation" installiert werden. Über den Ablauf der Lizenz informiert SX-GATE den Administrator rechtzeitig per E-Mail.



Eventuelle Software-Updates des Kaspersky Virenschanners werden als Bestandteil der regulären SX-GATE Updates vorgenommen.

Online-Unterstützung des Scanners?

Wenn die Online-Unterstützung aktiviert ist, dann kontaktiert der Scanner den Onlinedienst des Scanner-Herstellers um die Erkennungsrate zu verbessern.

Installierte Version

In diesem Bereich werden nähere Informationen zum installierten Kaspersky Scanner angezeigt. Durch den Aufruf dieser Seite erfolgt zudem eine Funktionsprüfung. Bei Erfolg wird der Status "OK" gemeldet.

Signaturen jetzt aktualisieren

Drücken Sie diesen Schalter um sofort eine Aktualisierung der Kaspersky Virensignaturen durchzuführen.

14.14-E Installation / Update / Deinstallation

Lizenzen für Virenschutzprogramme sind nicht im Lieferumfang enthalten und müssen daher separat erworben werden. Nähere Informationen finden Sie in der Dokumentation zur Bildschirmmaske des Scanners.

Virenschanner-Engine, -Signaturen oder -Lizenzschlüssel hochladen

In diesem Bereich können Sie Virenschanner-Programme installieren oder aktualisieren. Auch lassen sich hier Signatur-Pakete manuell hochladen.

Avira

Der Avira Scanner kann nur mit Hilfe eines speziell für SX-GATE angepassten Archivs (*.rin) installiert werden. Zusätzlich ist hier auch die Lizenzschlüssel-Datei des Avira zu installieren. Diese Datei hat die Endung "*.key". Um eine abgelaufene Avira-Lizenz zu erneuern, genügt es die Lizenzschlüssel-Datei in diesem Bereich an SX-GATE zu übermitteln. Die Aktualisierung der Avira Scanner-Software erfolgt über die regulären SX-GATE Updates. Ein Update kann auch hier durch Hochladen eines entsprechenden Archivs vorgenommen werden.

F-Secure

Hier kann auch die Lizenzschlüssel-Datei des F-Secure Virenschanners installiert werden. Diese Datei hat die Endung "*.key". Um eine abgelaufene F-Secure-Lizenz zu erneuern, genügt es die Lizenzschlüssel-Datei in diesem Bereich an SX-GATE zu übermitteln.

Kaspersky

Auch der Kaspersky Scanner kann nur mit Hilfe eines speziell für SX-GATE angepassten Archivs (*.rin) installiert werden. Zusätzlich ist hier auch die Lizenzschlüssel-Datei des Kaspersky zu installieren. Diese Datei hat die Endung "*.key". Um eine abgelaufene Kaspersky-Lizenz zu erneuern, genügt es die Lizenzschlüssel-Datei in diesem Bereich an SX-GATE zu übermitteln. Die Aktualisierung der Kaspersky Scanner-Software erfolgt über die regulären SX-GATE Updates. Ein Update kann zwar auch hier durch Hochladen eines entsprechenden Archivs vorgenommen werden, allerdings könnte dies zu Problemen mit dem Lizenzschlüssel führen.

Virenschanner deinstallieren

In diesem Bereich können Sie einen auf SX-GATE installierten Virenschanner deinstallieren.

14.15 Zeitserver

Die Einstellungen in diesem Menü sind in der Benutzeroberfläche thematisch gegliedert. Wechseln Sie zwischen den verschiedenen Bereichen indem Sie auf die Reiter (Tabs) im oberen Bildbereich klicken.

14.15-A Zeitsynchronisation.....	657
14.15-B SX-GATE Zeit.....	658

14.15-A Zeitsynchronisation

Der SX-GATE holt sich auf Wunsch die genaue Uhrzeit über öffentliche Zeitserver im Internet. SX-GATE bietet seinerseits die Zeit aber auch anderen Systemen in Ihrem lokalen Netzwerk an. Die Zeit kann über die TCP-Ports 13 (daytime) und 37 (time), über UDP-Port 123 (NTP) sowie über die Windows-Freigaben des SX-GATE abgerufen werden.



Um die Zeit des SX-GATE über das NTP-Protokoll abfragen zu können, muss der SX-GATE-Dienst "NTP-Zeitserver" aktiviert sein.



Um die Systemzeit älterer Windows-Clients (vor Windows 2000) zu aktualisieren, ist der SX-GATE-Dienst "Windows-Freigaben" zu aktivieren. Mit dem DOS-Befehl
 "NET TIME /SET \\SX-GATE-IP-Adresse /YES"
 holt sich der Windows-Rechner dann die Systemzeit. Tragen Sie diesen Befehl im Login-Skript des Domain-Controllers oder der Autoexec-Batch-Datei eines Arbeitsplatz-Rechners ein um diesen Vorgang zu automatisieren. Der NTP-Serverdienst ist dazu nicht erforderlich.

Synchronisations-Intervall

Wählen Sie die Häufigkeit der Synchronisation der SX-GATE-Systemzeit mit den angegebenen Zeitservern. SX-GATE aktualisiert die Zeit entweder täglich oder jeden Sonntag zwischen 4:00 Uhr und 4:59 Uhr. Sofern der SX-GATE-Dienst "NTP-Zeitserver" läuft, führt dieser zusätzlich eine fortlaufende Synchronisation durch.

Öffentliche Zeitserver

SX-GATE ruft die Systemzeit von den hier angegebenen Zeitservern ab. Es empfiehlt sich die Nutzung der Server-Pools aus der Domain ntp.org (z.B. de.pool.ntp.org). Unter einem Hostnamen aus dieser Domain ist jeweils eine Reihe von öffentlichen NTP-Servern registriert. Bei der DNS-Namensauflösung wird dabei jeweils zufällig einer ausgewählt. Ist mindestens eine Adresse aus der Domain pool.ntp.org angegeben, so kontaktiert SX-GATE insgesamt stets mindestens drei Pool-Server.

Zeitserver testen

Mit Hilfe dieser Funktion können Sie überprüfen, ob die angegebenen Zeitserver erreichbar sind.



Die aktuelle Systemzeit des SX-GATE wird durch den Aufruf dieser Funktion nicht geändert. Wechseln Sie auf den Reiter (Tab) "SX-GATE Zeit" um die Zeit einzustellen.

14.15-B SX-GATE Zeit

Systemzeit jetzt synchronisieren

Drücken Sie diesen Schalter, um die Systemzeit des SX-GATE sofort mit den angegebenen Zeitservern zu synchronisieren. Bitte beachten Sie, dass dafür eine Verbindung in das Internet notwendig ist.

SX-GATE Zeitzone

Hier wird die aktuelle Zeitzone-Einstellung des SX-GATE angezeigt.

Zeitzone ändern

Mit Hilfe dieses Schalters können Sie die Zeitzone-Einstellung des SX-GATE anpassen.

15 L2TP-IPSec-VPN Client-Konfiguration

15.1 Microsoft Windows

Diese Anleitung beschreibt, wie mit Hilfe der in Windows integrierten IPSec-Implementierung ein L2TP-IPSec-VPN zu SX-GATE konfiguriert werden muss. Dabei orientiert sich die Beschreibung an Windows 7.



Je nach verwendeter Windows-Version können sich die hier abgebildeten Bildschirmmasken von denen unterscheiden, die Ihnen im Verlauf der Installation begegnen werden.

Voraussetzungen für den Windows-Client:

- Manuelle Konfiguration: Windows 2000 oder neuer
- Automatische Konfiguration: Windows XP SP2 oder neuer, zertifikatsbasierte Authentifizierung.
- Falls NAT-Traversal benötigt wird: Auf Systemen mit Windows XP (bis einschliesslich SP1) oder Windows 2000 muss zunächst der Microsoft-Patch Q818043 eingespielt werden
- Die Authentifizierung über eine gemeinsame Passphrase (preshared key) wird von Windows 2000 sowie der automatischen Konfiguration nicht unterstützt

SX-GATES VPN-Server sollte bereits fertig konfiguriert sein. Es empfiehlt sich dringend, dazu den Assistenten "IPsec-VPN" aus dem Menü "Assistenten" zu verwenden. Falls zur Authentifizierung X.509-Zertifikate zum Einsatz kommen sollen, so sollten Sie die benötigten Schlüssel und Zertifikate bereits erstellt haben.



Auf der letzten Bildschirmmaske des Assistenten "IPsec-VPN" finden Sie einen Hinweis, wie in Ihrem Falle bei der Erstellung eines Zertifikats vorzugehen ist. Bitte durchlaufen Sie den Assistenten erneut, falls Sie diesen Hinweis übersehen haben.

Hintergrundinformationen zu L2TP-IPSec

Eine L2TP IPSec Verbindung bezieht zwei verschiedene SX-GATE-Dienste ein:

IPSec-VPN

Die IPSec-Verbindung stellt einen sicheren Tunnel für das L2TP-Protokoll zur Verfügung.

Nur L2TP-Pakete (UDP-Port 1701) werden in diesem Tunnel transportiert.

Der IPSec-Tunnel wird entweder mit Hilfe einer gemeinsamen Passphrase (preshared key) oder durch X.509-Zertifikate authentifiziert.

L2TP-Server

Vergleichbar mit einer Wählverbindung nutzt L2TP das PPP-Protokoll.

PPP wird u.a. für die Benutzeranmeldung, die Zuweisung der IP-Adresse und die Verbindung zwischen Client und lokalem Netz als solches genutzt.

Benutzer authentifizieren sich mit Hilfe von PAP



Obwohl hier das Kennwort im Klartext übermittelt wird ist dies sicher. Bedenken Sie, dass die gesamte L2TP-Kommunikation durch den IPSec-Tunnel abgesichert wird.

Es gibt zwei verschiedene Möglichkeiten wie Sie eine L2TP-IPSec-VPN Verbindung konfigurieren können.

Automatische Konfiguration

Sie benutzen das Installationspaket, das Ihnen nach dem Erstellen eines Zertifikats vom SX-GATE zum Herunterladen angeboten wird. Dieses erledigt den Zertifikatsimport und die Verbindungskonfiguration auf dem Windows-Client für Sie.

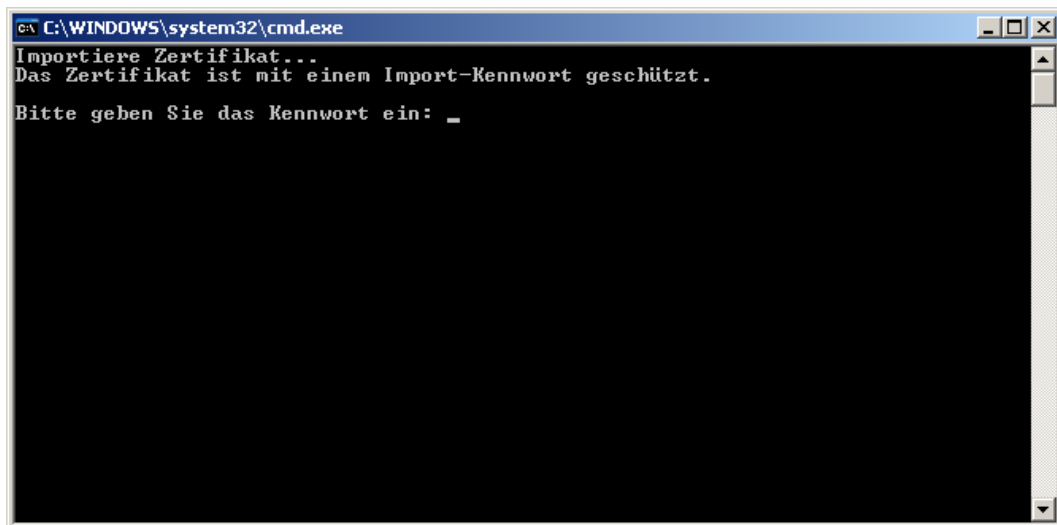
Manuelle Konfiguration

Die manuelle Konfiguration erfordert es, sämtliche Verbindungseinstellungen selbst durchzuführen. Werden zur Authentifizierung Zertifikate verwendet, ist zudem für deren korrekten Import zu sorgen.

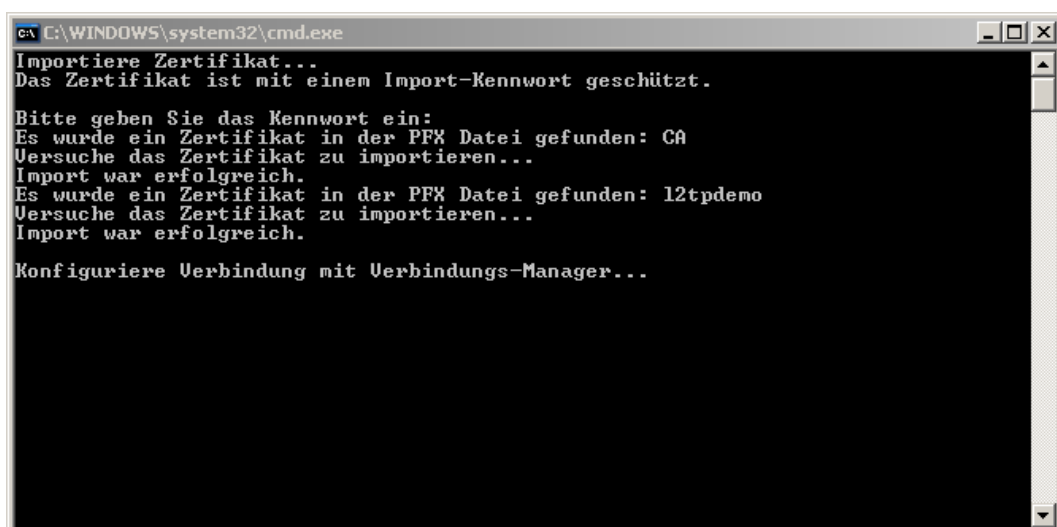
15.1.1 Automatische Konfiguration

Wie im Kapitel "System > Zertifikatsverwaltung > CA Zertifikate > Zertifikate" unter "Installations-Paket erstellen" beschrieben, wird Ihnen beim Erstellen eines neuen Zertifikats ein Installationspaket für Windows zum Herunterladen angeboten. Übertragen Sie diese Datei auf den Client, mit dem Sie eine L2TP-Verbindung zum SX-GATE aufbauen möchten.

Nach dem Start des Programms öffnet sich ein Fenster, in dem Sie aufgefordert werden das Import-Kennwort einzugeben.

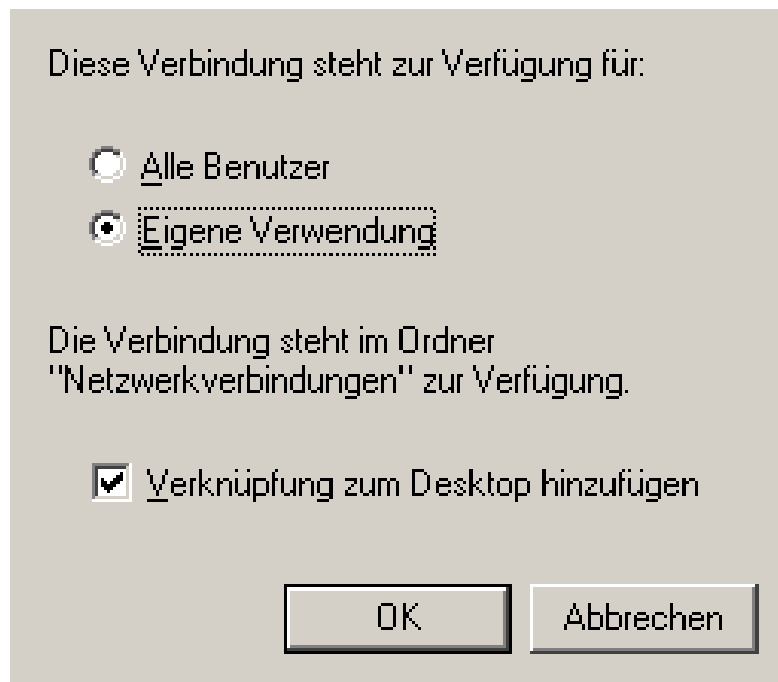


Mit diesem Kennwort können die Zertifikate ausgelesen und somit importiert werden.



Sollte beim Zertifikatsimport ein Fehler auftreten, weil z.B. eine zu alte Windows-Version verwendet wird, werden die für den manuellen Import nötigen Dateien in das Heimatverzeichnis des aktuellen Benutzers kopiert.

Als nächstes wird das "Verbindungsmanager-Verwaltungs-kit" gestartet um die VPN-Verbindung zu konfigurieren. Hier müssen Sie lediglich angeben, ob die Verbindung jedem, oder nur dem aktuell angemeldeten Benutzer zur Verfügung steht.



Diese Verbindung steht zur Verfügung für:

☐ Alle Benutzer

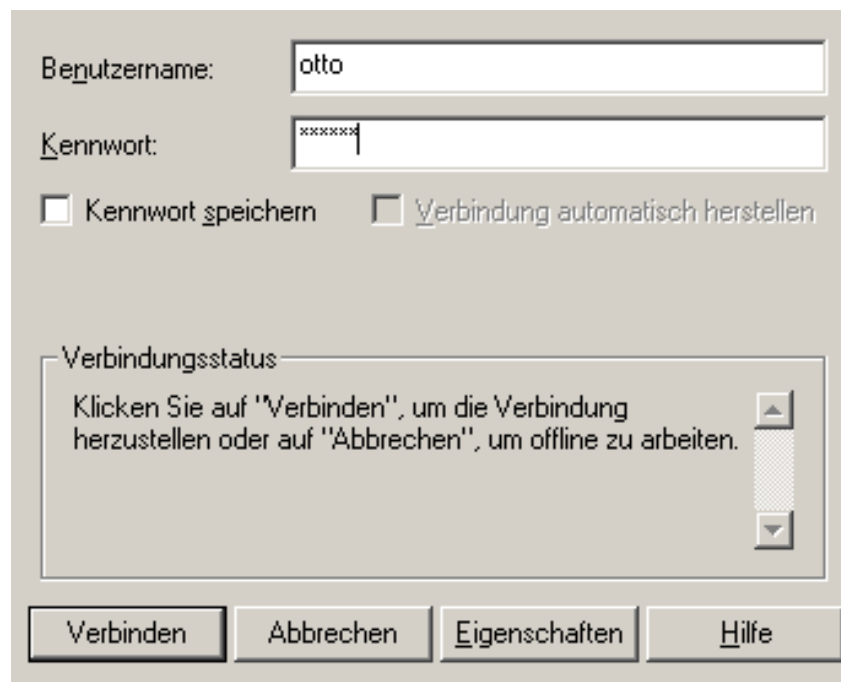
☒ Eigene Verwendung

Die Verbindung steht im Ordner "Netzwerkverbindungen" zur Verfügung.

☒ Verknüpfung zum Desktop hinzufügen

OK Abbrechen

Nach der erfolgreichen Konfiguration wird der Verbindungsmanager gestartet. Um nun die Verbindung zum SX-GATE aufzubauen, müssen Sie noch den Benutzernamen und das zugehörige Kennwort eines Mitglieds der SX-GATE-Gruppe "system-ras" eingeben.



Benutzername: otto

Kennwort: xxxxxx

☐ Kennwort speichern ☐ Verbindung automatisch herstellen

Verbindungsstatus

Klicken Sie auf "Verbinden", um die Verbindung herzustellen oder auf "Abbrechen", um offline zu arbeiten.

Verbinden Abbrechen Eigenschaften Hilfe

Klicken Sie "Verbinden" um die L2TP-Verbindung mit dem SX-GATE herzustellen.

15.1.2 Manuelle Konfiguration

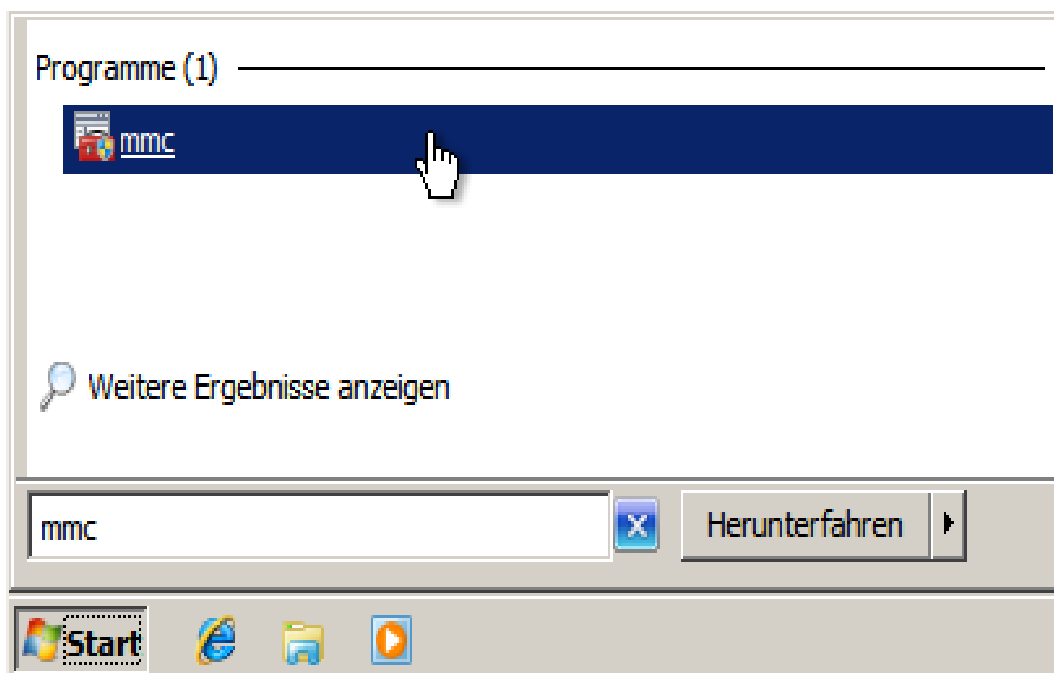
IPSec-Authentifizierungsmethode wählen

Sofern Sie zur Authentifizierung der IPSec-Verbindung keine Zertifikate verwenden wollen, können Sie die Beschreibung des Zertifikats-Imports überspringen.

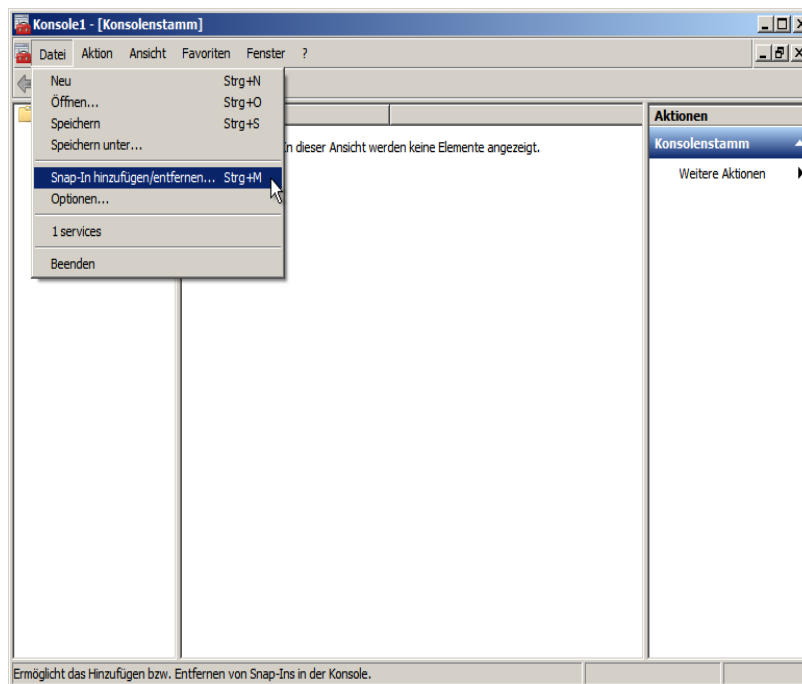
- X.509 Zertifikat
Lesen Sie bitte weiter bei [Management-Konsole einrichten](#) (S. 663)
- gemeinsame Passphrase (preshared key)
Lesen Sie bitte weiter bei [Verbindungskonfiguration](#) (S. 670)

Management-Konsole einrichten

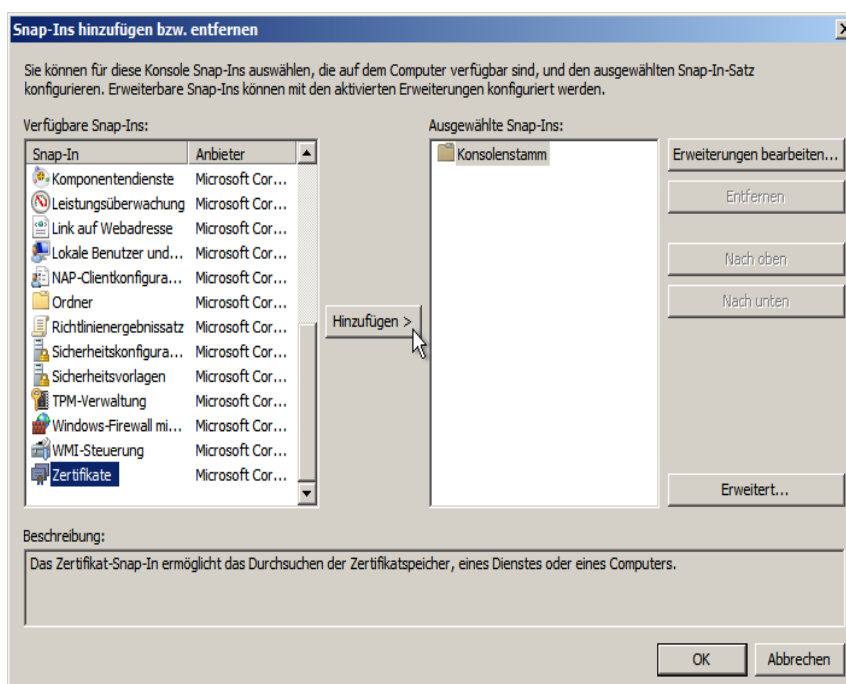
Für die Verwaltung der Zertifikate wird die Management-Konsole benötigt. Zum Starten geben Sie im Windows Startmenü in der Eingabezeile das Kommando "mmc" ein und bestätigen dies mit der Eingabetaste.



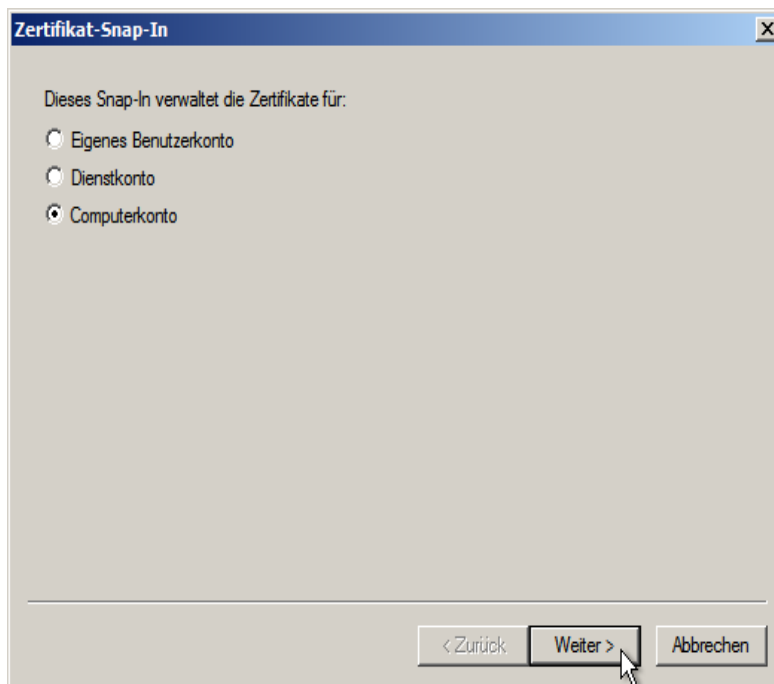
Öffnen Sie das Menü "Datei" und wählen Sie "Snap-In hinzufügen/entfernen"



Wählen Sie aus der Liste der verfügbaren Snap-Ins "Zertifikate" aus und drücken Sie "Hinzufügen".



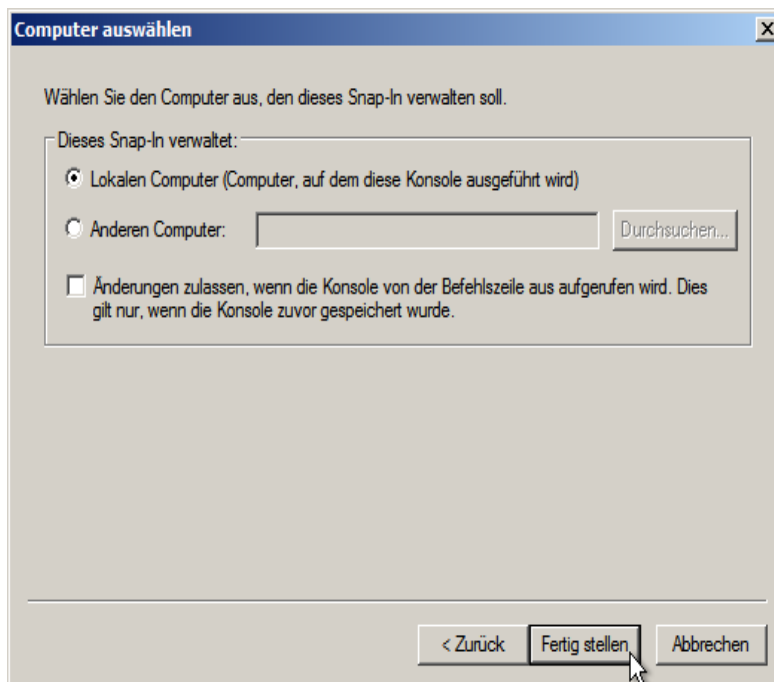
In der nun folgenden Maske ist unbedingt der Typ "Computerkonto" auszuwählen.



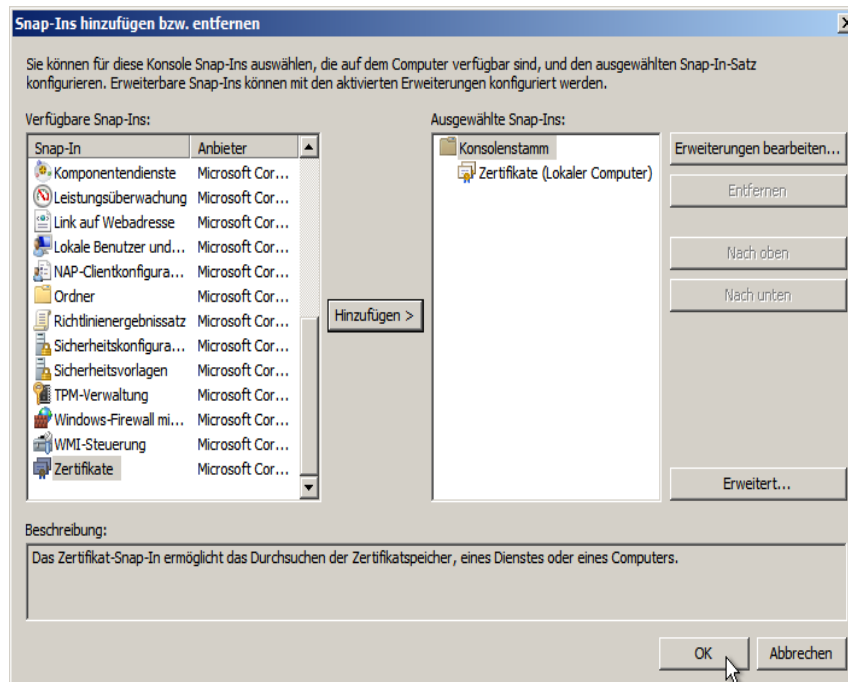
Fahren Sie fort mit "Weiter".

Das Snap-In verwaltet den "Lokalen Computer".

Mit "Fertigstellen" wird das Hinzufügen des Snap-Ins abgeschlossen.



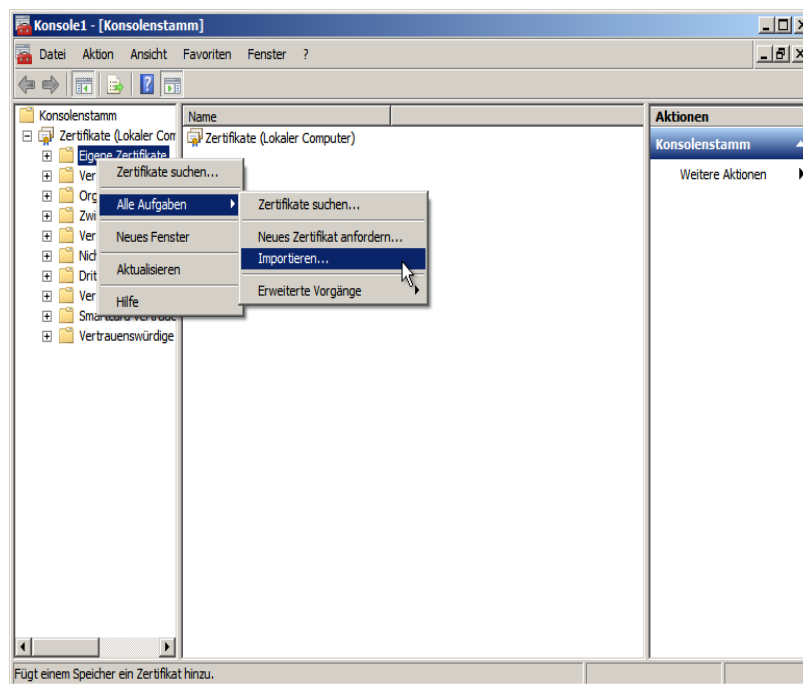
Nachdem Sie "OK" gedrückt haben ist das System für den Import des VPN-Schlüssels vorbereitet.



Zertifikat importieren

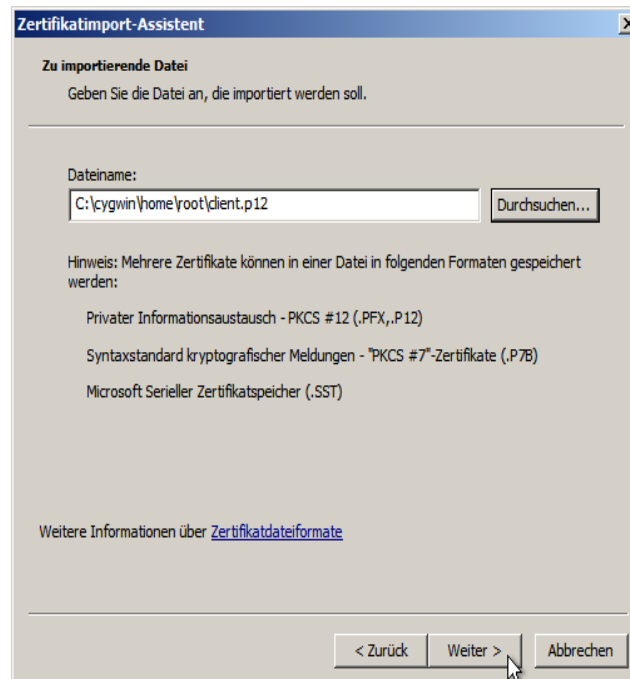
Öffnen Sie in der Baumstruktur den "Konsolenstamm" und den darin enthaltenen Eintrag "Zertifikate (Lokaler Computer)".

Klicken Sie mit der rechten Maustaste auf den Eintrag "Eigene Zertifikate" und wählen Sie aus dem Kontext-Menü "Alle Aufgaben > Importieren".



Verlassen Sie den Willkommen-Bildschirm mit "Weiter".

Wählen Sie die PKCS#12-Datei (*.p12) aus, die die benötigten Zertifikate und den privaten Schlüssel enthält. Eventuell müssen Sie dazu den Dateityp auf "Privater Informationsaustausch (*.pfx;*.p12)" stellen, um die Datei auswählen zu können.

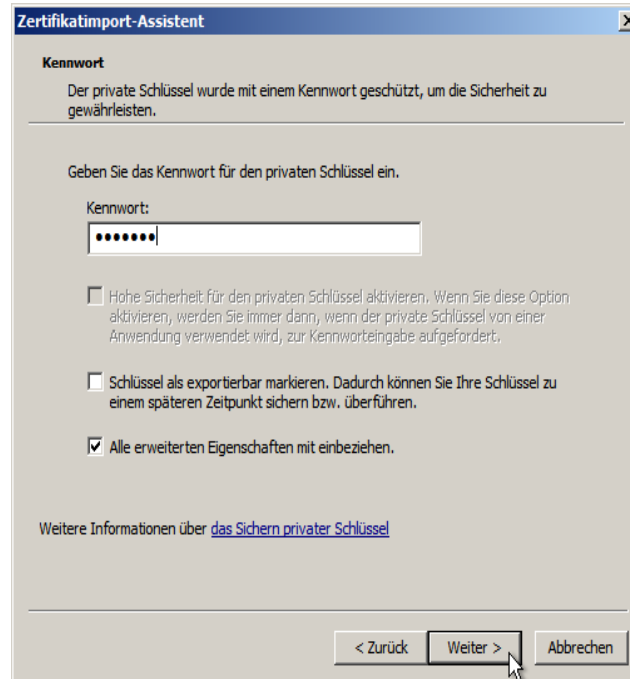


Fahren Sie fort mit "Weiter".

Sie werden nun nach dem Kennwort für die PKCS#12-Datei gefragt.

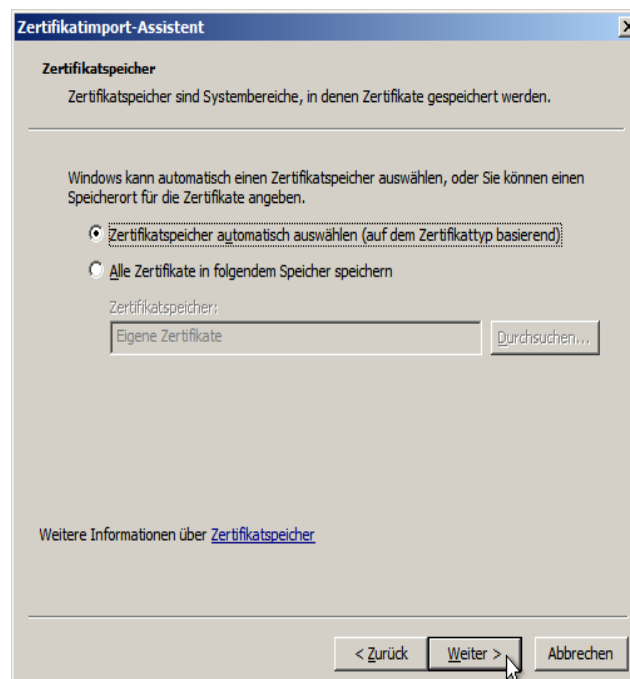


Dieses Kennwort wurde beim Erstellen des Zertifikats festgelegt und schützt die PKCS#12-Datei vor unberechtigtem Lesezugriff. Verwechseln Sie dieses Kennwort nicht mit dem CA-Passwort, das zum Signieren eines jeden neuen Zertifikat eingegeben werden muss.



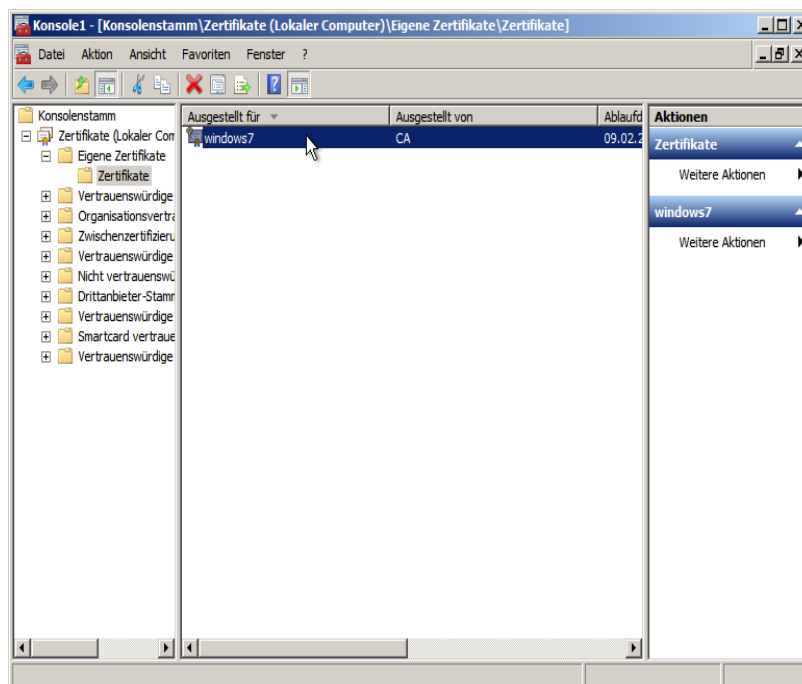
Drücken Sie "Weiter"

In der nun folgenden Bildschirmmaske ist unbedingt der Eintrag "Zertifikatsspeicher automatisch auswählen (auf dem Zertifikattyp basierend)" auszuwählen.

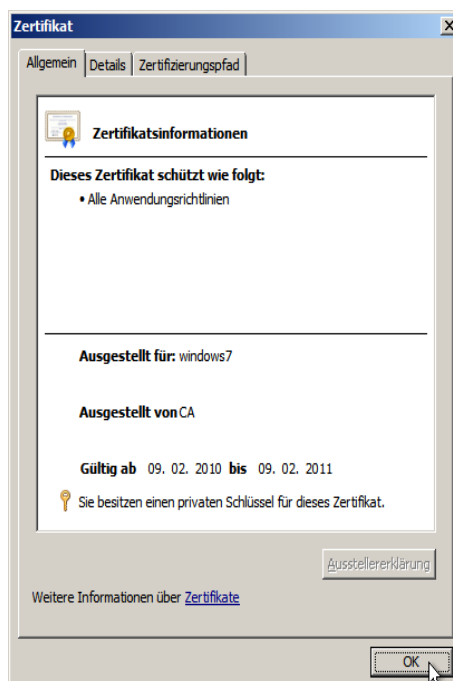


Schliessen Sie den Import-Vorgang mit "Weiter" und "Fertigstellen" ab.

Wenn Sie aus dem Menü "Vorgang" den Eintrag "Aktualisieren" anwählen, sollte das soeben importierte Zertifikat im Ordner "Zertifikate" unterhalb von "Eigene Zertifikate" erscheinen.



Öffnen und prüfen Sie das Zertifikat mit einem Doppelklick.



Wenn das Zertifikats-Symbol am oberen Rand des Dialog-Fensters wie im abgebildeten Screenshot erscheint, ist der Zertifikatsimport abgeschlossen.

Ist das Symbol jedoch durchgestrichen, so ist das Zertifikat ungültig. Die VPN-Verbindung wird damit nicht funktionieren. Die häufigsten Gründe hierfür sind:

Gültigkeitszeitraum abgelaufen

Vergleichen Sie bitte den Gültigkeitszeitraum des Zertifikats mit der aktuellen Systemzeit

Stammzertifikat fehlt

Prüfen Sie ob im Ordner "Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate" das Zertifikat der Stammzertifizierungsstelle (CA) enthalten ist. Falls nein muss dieses separat importiert werden. Fragen Sie Ihre CA nach deren Zertifikat



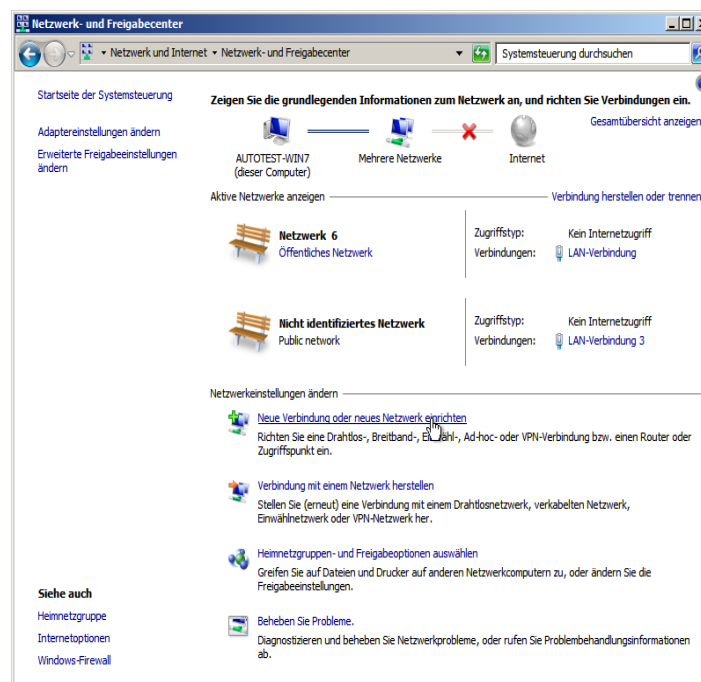
Sofern Sie die SX-GATE-CA zur Ausstellung von Zertifikaten nutzen wird das CA-Zertifikat automatisch importiert, da es grundsätzlich in der PKCS#12-Datei enthalten ist

Stammzertifikat ist ungültig

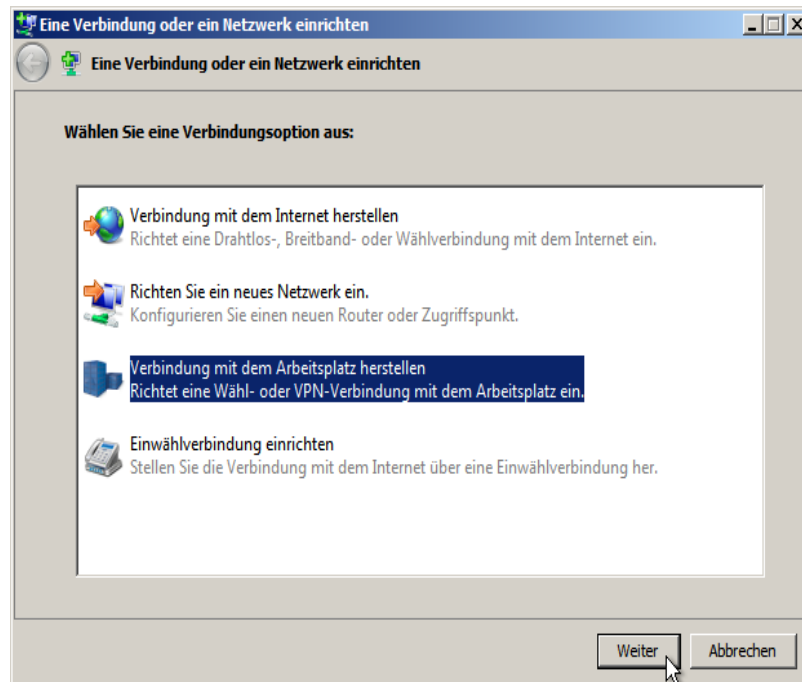
Öffnen Sie das entsprechende Stammzertifikat mit einem Doppelklick und prüfen Sie auch hier den Gültigkeitszeitraum

Verbindungskonfiguration

Starten Sie das "Netzwerk- und Freigabecenter" und wählen dort "Neue Verbindung oder neues Netzwerk einrichten".



Verlassen Sie den Willkommens-Bildschirm mit "Weiter".
Wählen Sie die Option "Verbindung mit dem Arbeitsplatz herstellen".

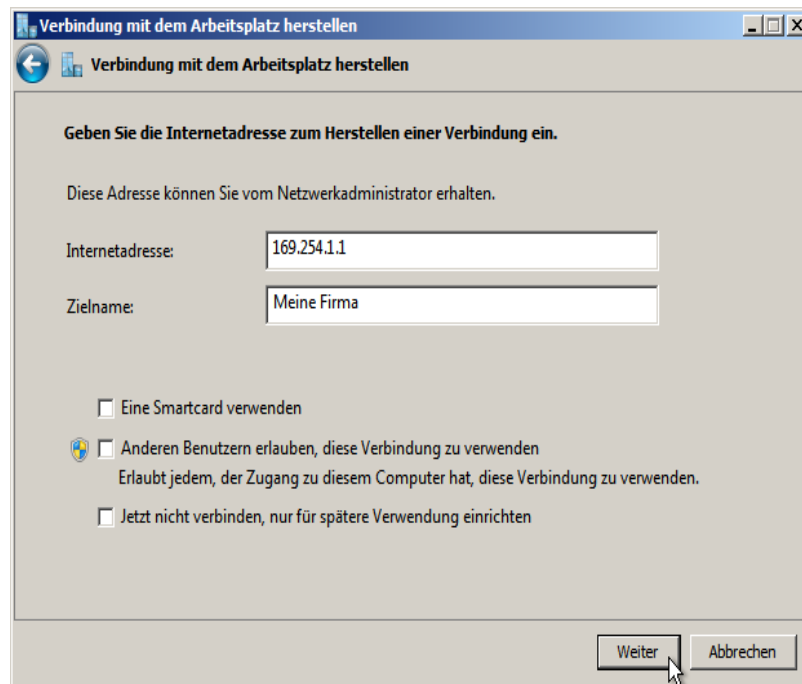


Mit "Weiter" gelangen Sie zur Auswahl des Verbindungs-Typs.

Wählen Sie "Die Internetverbindung (VPN) verwenden".



Geben Sie SX-GATEs externe (Internet) IP-Adresse als Adresse des VPN-Servers an, und vergeben Sie eine aussagekräftige Bezeichnung für die Verbindung (z.B. den Firmennamen).



Mit "Weiter" und "Fertigstellen" schließen Sie die Grundkonfiguration der Verbindung ab. Es empfiehlt sich, auf der Fertigstellen-Seite eine Verknüpfung zu der Verbindung auf dem Desktop erstellen zu lassen.

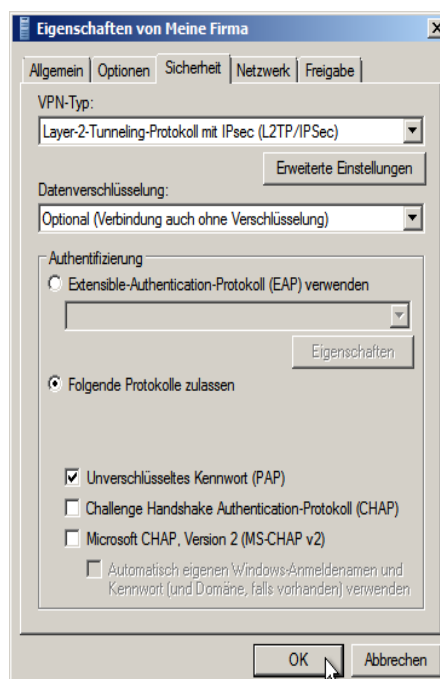
Verbindungseigenschaften

Starten Sie nun die soeben angelegte Verbindung. Der "Verbindung herstellen"-Dialog öffnet sich.



Bevor Sie die Verbindung herstellen können, müssen Sie noch mit "Eigenschaften" die Verbindungsparameter bearbeiten.

Wechseln Sie auf den Reiter (Tab) "Sicherheit" und wählen den VPN-Typ "Layer-2-Tunneling-Protokoll mit IPsec (L2TP/IPSec)".



Bei "Datenverschlüsselung" ist "Optional" auszuwählen, und im Bereich Authentifizierung "Unverschlüsseltes Kennwort (PAP)".



Obwohl bei manchen Windows-Versionen beim Übernehmen dieser Einstellungen mit "OK" eine Sicherheits-Warnung erscheint, ist die Benutzung dieser Parameter sicher. Das PAP-Protokoll kommt erst zum Einsatz, wenn der IPSec-Tunnel bereits erstellt ist. Die IPSec-Verschlüsselung schützt daher das Kennwort.

Wie erfolgt die Authentifizierung?

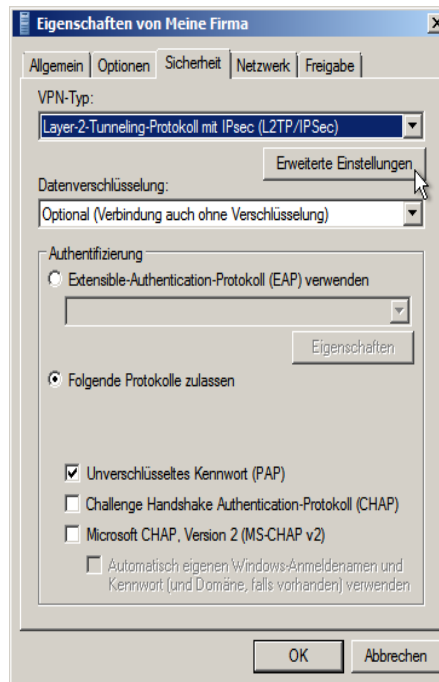
Bei einigen Windows-Versionen kann die Authentifizierung über eine gemeinsame Passphrase (preshared key) erfolgen. Wurde dieses Authentifizierungsverfahren auf dem SX-GATE konfiguriert, so muss dies auch auf dem Windows-System eingestellt werden.

Wie erfolgt die Authentifizierung?

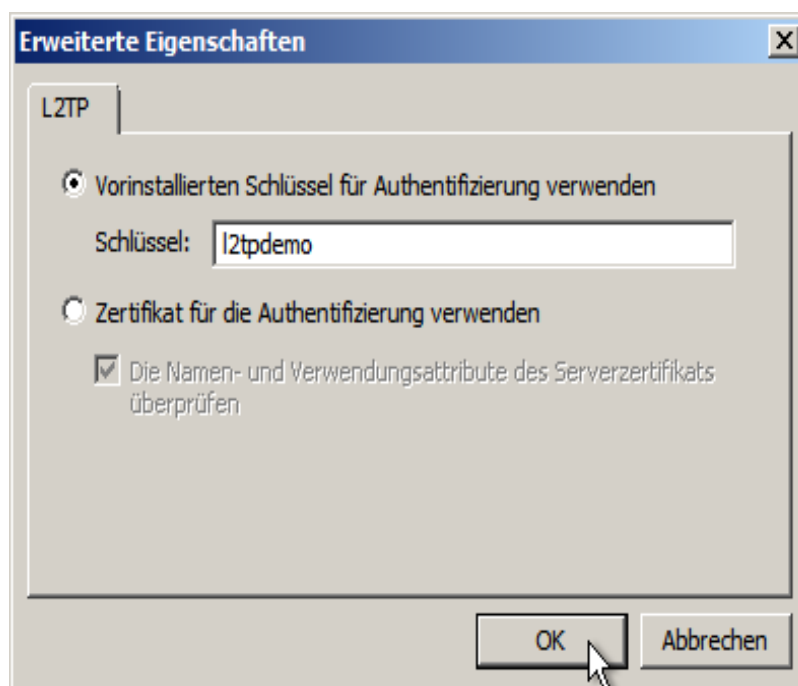
- X.509 Zertifikat
Lesen Sie bitte weiter bei [Verbindung herstellen](#) (S. 676)
- gemeinsame Passphrase (preshared key)
Lesen Sie bitte weiter bei [Gemeinsame Passphrase](#) (S. 675)

Gemeinsame Passphrase

Sofern zur Authentifizierung der IPSec-Verbindung eine gemeinsame Passphrase (preshared key) verwendet wird, müssen Sie im Reiter "Sicherheit" noch "Erweiterte Einstellungen" vornehmen.



Aktivieren Sie "Vorinstallierten Schlüssel für Authentifizierung verwenden" und geben Sie den Schlüssel an, den Sie auch im SX-GATE konfiguriert haben.



Verbindung herstellen

Schließen Sie das Dialog-Fenster mit "OK".

Geben Sie den Benutzernamen und das Kennwort eines Mitglieds der SX-GATE-Gruppe "system-ras" ein.



Klicken Sie "Verbinden" um die L2TP-Verbindung mit SX-GATE herzustellen. Prüfen Sie z.B. mit "ping" ob das entfernte Netzwerk erreichbar ist.



Sofern Sie über eine Wählverbindung mit dem Internet verbunden sind, sollten Sie sicherstellen, dass diese vor dem Aufbau der L2TP-Verbindung verfügbar ist.

Problemdiagnose

Probleme können beim Verbindungsaufbau sowohl im IPSec- als auch im L2TP-Bereich auftreten. Prüfen Sie bitte die entsprechenden Log-Dateien, inwieweit diese aussagekräftige Fehlermeldungen enthalten.

Probleme beim IPSec-Verbindungsaufbau lassen sich auf SX-GATE mit Hilfe der Log-Datei "IPSec" aus dem Menü "Monitoring" -> Log-Dateien" nachvollziehen.

Treten beim L2TP-Verbindungsaufbau Probleme auf, so finden Sie nähere Informationen in SX-GATEs Log-Datei "PPP".

Sollten die Meldungen in den genannten Quellen keine eindeutigen Rückschlüsse auf die Ursache des Problems zulassen, so senden Sie bitte die Log-Ausschnitte zu einem Verbindungsversuch an den technischen Support.

15.2 Mac OS X

Voraussetzungen

Voraussetzungen für den Mac OS X Client:

- Mac OS X 10.5 (Leopard) oder neuer
- Bei Verwendung von X.509 Zertifikaten muss der "alternative Bezeichner" des Zertifikates mit der IP-Adresse oder dem DynDNS-Namen des Servers übereinstimmen!

SX-GATEs VPN-Server sollte bereits fertig konfiguriert sein. Es empfiehlt sich dringend, dazu den Assistenten "IPsec-VPN" aus dem Menü "Assistenten" zu verwenden. Falls zur Authentifizierung X.509-Zertifikate zum Einsatz kommen sollen, so sollten Sie die benötigten Schlüssel und Zertifikate bereits erstellt haben.



Auf der letzten Bildschirmmaske des Assistenten "IPsec-VPN" finden Sie einen Hinweis, wie in Ihrem Falle bei der Erstellung eines Zertifikats vorzugehen ist. Bitte durchlaufen Sie den Assistenten erneut, falls Sie diesen Hinweis übersehen haben.

IPSec-Authentifizierungsmethode wählen

Sofern Sie zur Authentifizierung der IPSec-Verbindung keine Zertifikate verwenden wollen, können Sie die Beschreibung des Zertifikats-Imports überspringen.

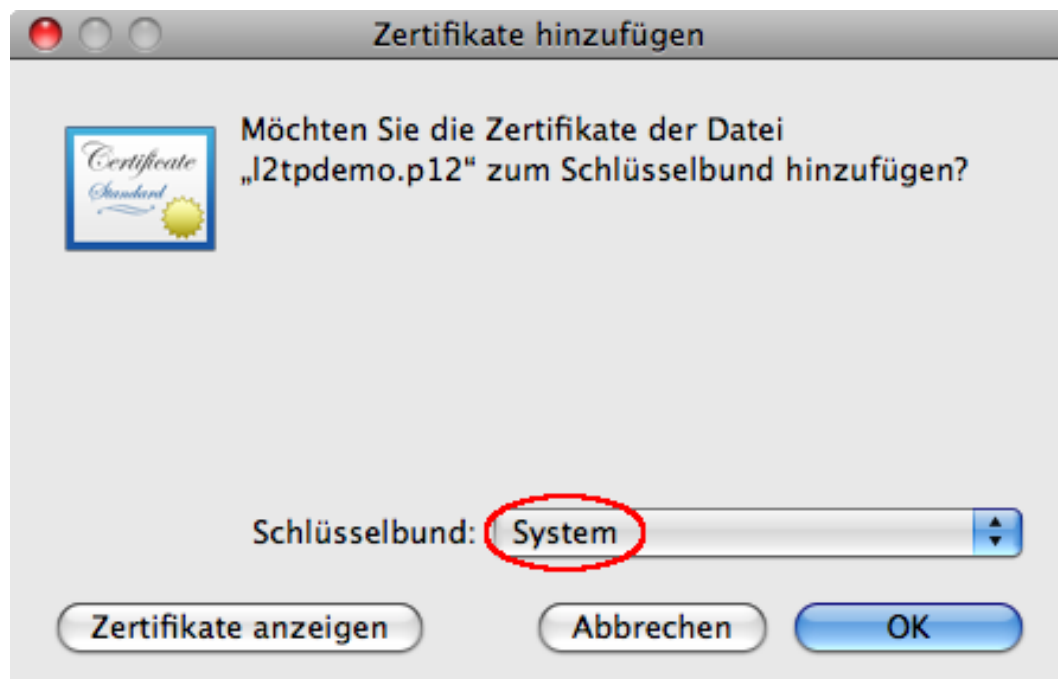


Bitte beachten Sie, dass die gezeigten Screenshots von der Mac OS X Version 10.5 (Leopard) gemacht wurden. Je nach verwendeter Mac OS X Version können sich die hier abgebildeten Bildschirmmasken von denen unterscheiden, die Ihnen begegnen werden.

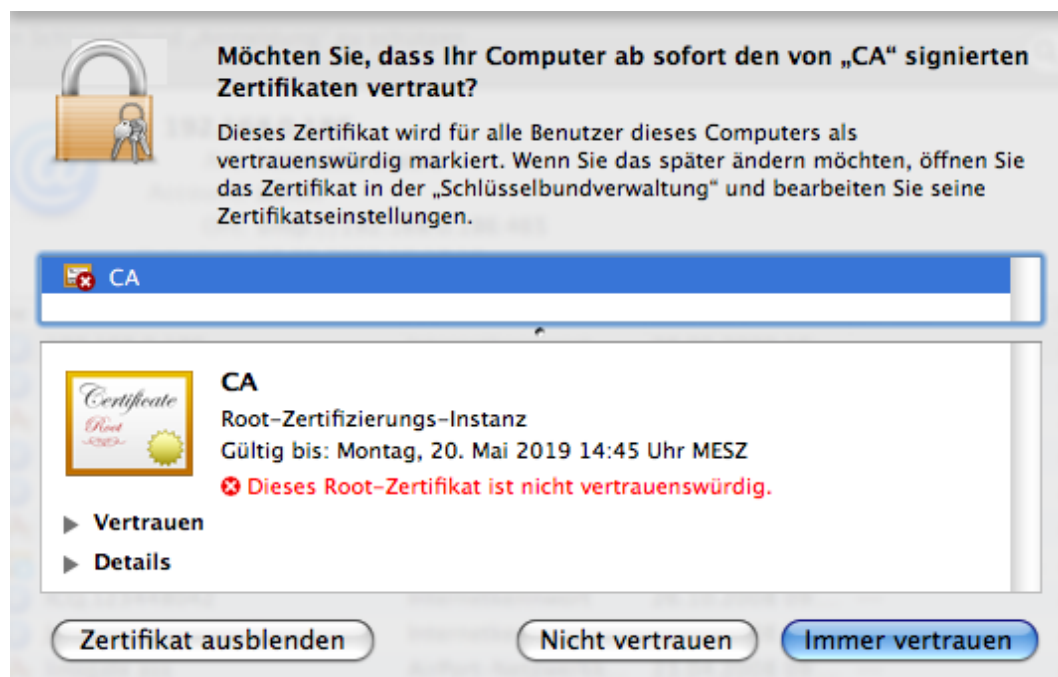
- X.509 Zertifikat
Lesen Sie bitte weiter bei [Zertifikat importieren](#) (S. 679)
- gemeinsame Passphrase (preshared key)
Lesen Sie bitte weiter bei [Verbindung konfigurieren](#) (S. 681)

Zertifikat importieren

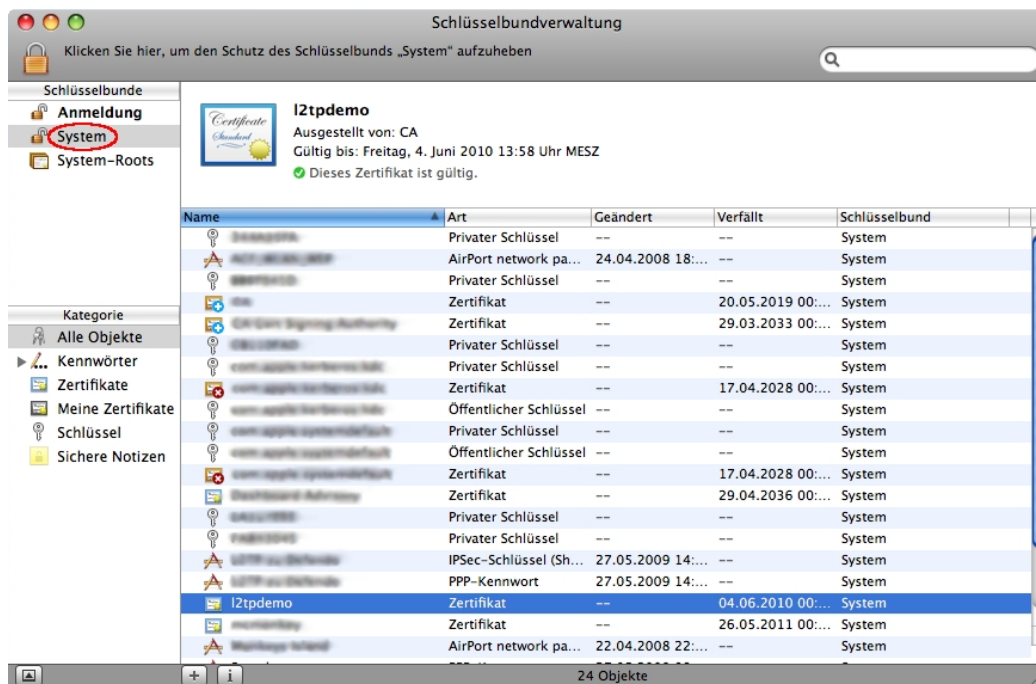
Durch Doppelklicken der Zertifikatsdatei (hier "l2tpdemo.p12") wird automatisch das Programm "Schlüsselbundverwaltung" geöffnet. Sie werden nach dem Schlüsselbund gefragt, zu dem das Zertifikat hinzugefügt werden soll. Wählen Sie hier bitte "System" aus und geben falls gefordert die entsprechenden Kennwörter ein.



Anschließend werden Sie gefragt ob Sie den Zertifikaten, die von der angezeigten CA unterschrieben wurden, vertrauen möchten. Wählen Sie "Immer vertrauen".



Im Hauptfenster der "Schlüsselbundverwaltung" sehen Sie nun das von Ihnen hinzugefügte Zertifikat.

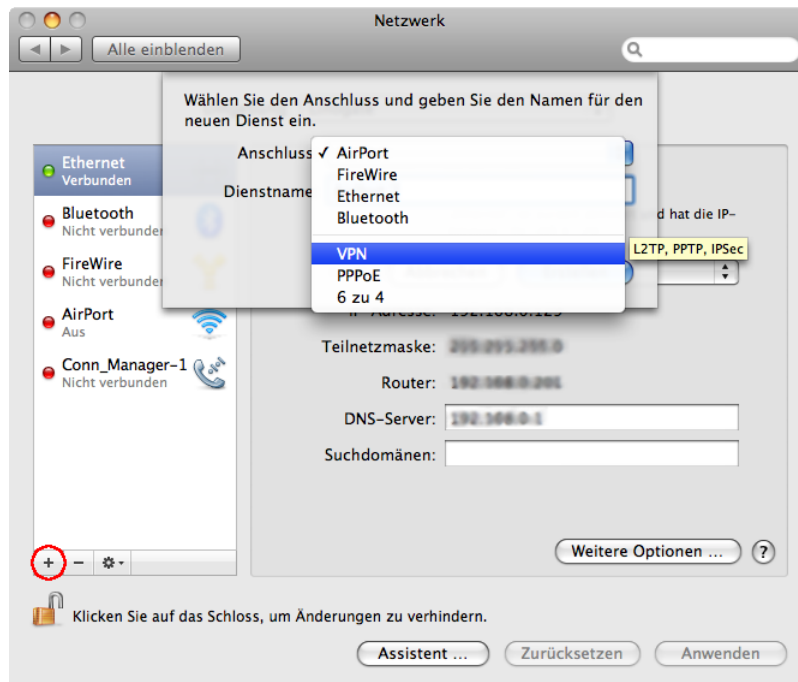


Bitte beachten Sie dass Sie das Zertifikat dem Schlüsselbund "System" hinzugefügt haben. Die Anwendung zeigt Ihnen aber normalerweise den Schlüsselbund "Anmeldung". Sie müssen daher ggf. den Schlüsselbund wechseln.

Wenn Ihnen das Zertifikat als gültig angezeigt wird, können Sie mit der Konfiguration der Verbindung fortfahren.

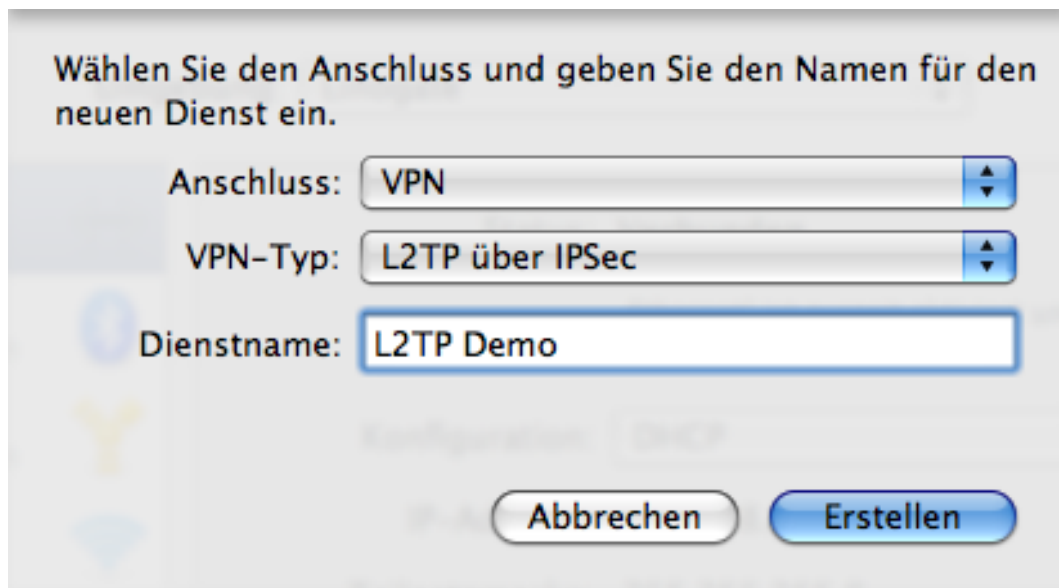
Verbindung konfigurieren

Die Verbindungskonfiguration wird in den "Systemeinstellungen" im "Netzwerk"-Dialog durchgeführt. Fügen Sie dazu in der gewünschten Netzwerkumgebung eine VPN-Schnittstelle durch Drücken des "+"-Symbols hinzu.

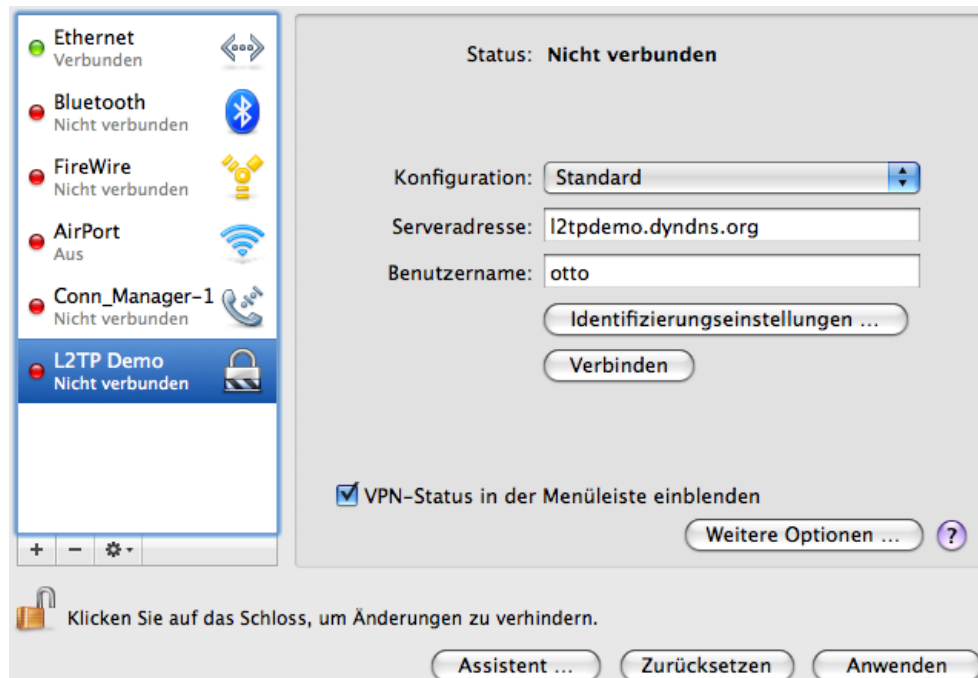


Sie können Änderungen in diesem Dialog nur durchführen, wenn das "Schloss"-Symbol geöffnet dargestellt wird. Ist dies nicht der Fall bekommen Sie den Hinweis: "Klicken Sie auf das Schloss, um Änderungen vorzunehmen" angezeigt.

Stellen Sie sicher, dass beim VPN-Typ "L2TP über IPSec" ausgewählt ist und vergeben Sie einen Dienstenamen.



Wenn Sie die Schnittstelle erstellt haben müssen Sie noch die "Serveradresse" in Form des DNS-Namen oder einer IP-Adresse, sowie den Benutzernamen eines Benutzers der SX-GATE-Gruppe "system-ras" angeben.



Die Serveradresse muss mit dem "alternativen Bezeichner" des Zertifikates übereinstimmen, das Sie auf dem SX-GATE erstellt haben.

Klicken Sie anschließend auf "Identifizierungseinstellungen".

Identifizierungseinstellungen

In den Identifizierungseinstellungen geben Sie sowohl an wie sich der Benutzer, als auch der Computer bei der Gegenstelle authentifizieren.

Die Benutzer-Identifizierung am SX-GATE erfolgt mittels Kennwort. Geben Sie im zugehörigen Feld dahinter das Passwort des Benutzers ein, den Sie im Netzwerkdialog angegeben haben.

Bei Rechner-Identifizierung hängt die weitere Vorgehensweise davon ab, wie Sie sich am SX-GATE authentifizieren:

- Lesen Sie bitte weiter bei [Authentifizierung mit Pre-Shared-Key](#) (S. 683)
- Lesen Sie bitte weiter bei [Authentifizierung mit Zertifikaten](#) (S. 684)

Authentifizierung mit Pre-Shared-Key

Wenn Sie sich mittels Pre-Shared-Key am SX-GATE authentifizieren möchten, wählen Sie in den Identifizierungseinstellungen der VPN-Verbindung, unter "Rechner-Identifizierung" den Punkt "Schlüssel ("Shared Secret")" aus, und geben im Feld dahinter das Passwort ein.

The screenshot shows a dialog box titled 'Identifizierungseinstellungen'. It is divided into two main sections: 'Benutzer-Identifizierung' and 'Rechner-Identifizierung'. In the 'Benutzer-Identifizierung' section, the 'Kennwort' option is selected with a radio button, and there is a password input field. Other options like 'RSA-SecurID', 'Zertifikat', 'Kerberos', and 'CryptoCard' are listed but not selected. In the 'Rechner-Identifizierung' section, the 'Schlüssel („Shared Secret“)' option is selected with a radio button, and there is a password input field. The 'Zertifikat' option is also present with a 'Wählen ...' button. At the bottom of the dialog, there is a 'Gruppenname:' label followed by an empty text field, with '(Optional)' written below it. Two buttons, 'Abbrechen' and 'OK', are located at the bottom right of the dialog.

Durch drücken des "OK"-Knopfes gelangen Sie zurück in den Netzwerkdialog. Hier müssen Sie die durchgeführten Einstellungen durch Drücken des "Anwenden"-Knopfes

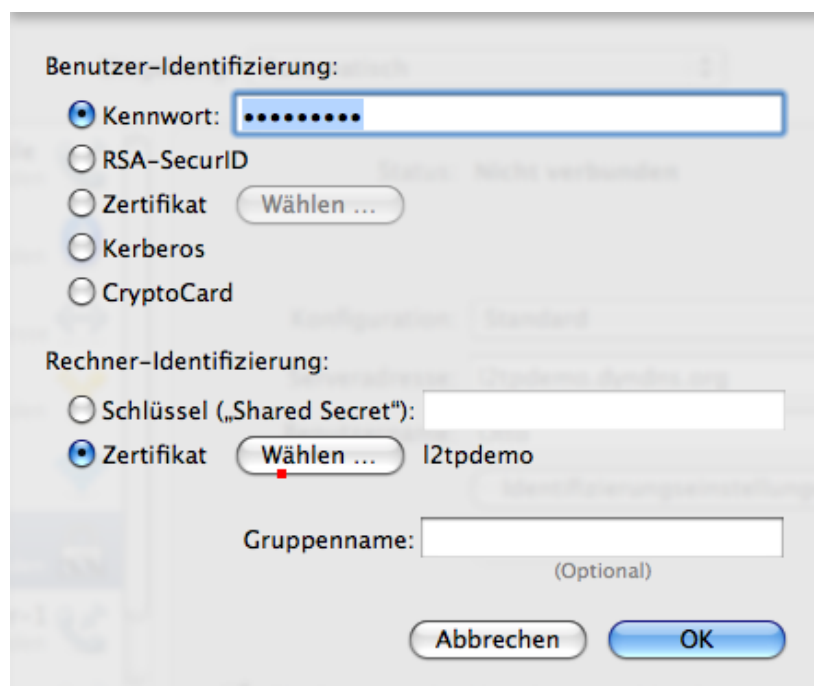
übernehmen. Anschließend können Sie den Verbindungsaufbau durch Drücken auf "Verbinden" starten.

Authentifizierung mit Zertifikaten

Wenn Sie sich mittels Zertifikat am SX-GATE authentifizieren möchten, wählen Sie in den Identifizierungseinstellungen der VPN-Verbindung, unter "Rechner-Identifizierung" den Punkt "Zertifikat" und wählen das entsprechende Zertifikat aus.



Unter Mac OS X Version 10.5 (Leopard) reagiert der Knopf nur an einer bestimmten Stelle, welche unterhalb der Schrift im Bereich zwischen dem Buchstaben "W" und "ä" liegt. Im unten abgebildeten Screenshot wird diese Stelle durch den roten Punkt markiert. In der aktuellen Version 10.6 (Snow Leopard) wurde dieser Fehler behoben.



Der Name des ausgewählten Zertifikats erscheint nun rechts neben dem "Wählen"-Knopf. Gehen Sie nun zurück ins Hauptmenü ("OK") und wählen hier "Anwenden" um die Einstellungen zu übernehmen. Mit dem "Verbinden"-Knopf können Sie nun den Verbindungsaufbau starten.

Troubleshooting

Bei der Authentifizierung mittels Zertifikat kann es passieren, dass das angegebene Zertifikat in den Identifizierungseinstellungen nicht übernommen wird. Dies erkennen

Sie daran, dass beim erneuten Öffnen des Dialoges der Name des Zertifikates nicht mehr neben dem "Wählen"-Knopf erscheint. Das Verhalten war in Mac OS X Version 10.5 wiederholt feststellbar wenn die Netzwerkumgebung "Standart" aktiv war.

Abhilfe konnte wie folgt geschafft werden: Sie wählen bei der Rechner-Identifizierung zuerst "Schlüssel" aus, und tragen einen X-Beliebigen Wert (z.B. "test") in das Feld dahinter ein. Was hier genau eingetragen wird ist irrelevant, da der Schlüssel beim Verbindungsaufbau nicht verwendet wird. Gehen Sie auf "OK" und im Hauptdialog auf "Anwenden". Erneut in den Identifizierungseinstellungen überprüfen Sie, dass die Rechner-Identifizierung immer noch auf Schlüssel steht, und im Feld dahinter (dargestellt durch Punkte) der Dummy-Wert eingetragen ist. Wechseln Sie nun die Rechner-Identifizierungsmethode von Schlüssel auf Zertifikat und geben das entsprechende Zertifikat an. Nachdem Sie nun mit "OK" und "Anwenden" die Änderungen speichern, sollte das gewählte Zertifikat weiterhin eingestellt bleiben.

15.3 Apple iPhone

Alternative XAUTH

Für die VPN-Anbindung eines iOS-Geräts empfehlen wir ein IPsec-VPN mit XAUTH. Bei XAUTH unterstützt iOS Zertifikate uneingeschränkt und die Verbindung lässt sich auf dem iOS-Gerät einfach per Profil (.mobileconfig-Dateien) einrichten.

Um eine XAUTH-Verbindung auf dem SX-GATE zu konfigurieren, sollte der VPN-Server bereits fertig konfiguriert sein. Nutzen Sie dazu den Assistenten "IPsec-VPN" aus dem Menü "Assistenten". Legen Sie dann im Menü "Module > Netzwerk" zur gewünschten ipsec-Schnittstelle eine neue Verbindung vom Typ "XAuth Client" an. Legen Sie unter "Virtuelle IP (Mode Config)" einen Adress-Pool an und setzen Sie die Authentifizierungsmethode auf "alle Zertifikate von vertrauter CA".

Wie im Kapitel "System > Zertifikatsverwaltung > CA Zertifikate > Zertifikate" unter "Installations-Paket erstellen" beschrieben, wird Ihnen beim Erstellen eines neuen Zertifikats ein Profil für iOS zum Herunterladen angeboten. Übertragen Sie diese Datei auf den Client, mit dem Sie die XAUTH-Verbindung zum SX-GATE aufbauen möchten.

Voraussetzungen

Falls Sie sich gegen eine IPsec-XAUTH-Verbindung entschieden haben, wird nachfolgend beschrieben, wie Sie eine IPsec-L2TP-Verbindung für ein iOS-Gerät einrichten.

SX-GATEs VPN-Server sollte bereits fertig konfiguriert sein. Es empfiehlt sich dringend, dazu den Assistenten "IPsec-VPN" aus dem Menü "Assistenten" zu verwenden.



Der Assistent konfiguriert den VPN-Server für zertifikatsbasierte Authentifizierung, welche vom iPhone nur in Verbindung mit gekauften Zertifikaten bestimmter CAs funktioniert. Zur Authentifizierung wird daher häufig eine Passphrase (Preshared-Key) verwendet.

Wenn Sie bisher noch keinerlei zertifikatsbasierte Verbindungen verwenden, müssen Sie im SX-GATE lediglich die Authentifizierungsmethode auf "Passphrase (PSK)" stellen. Haben Sie dagegen bereits zertifikatsbasierte Verbindungen in Betrieb, müssen Sie manuell eine zweite identische Verbindung anlegen, bei der Sie dann die Authentifizierungsmethode auf "Passphrase (PSK)" stellen. Sie finden die Verbindungen im Menü "Module > Netzwerk" unterhalb der gewünschten ipsec-Schnittstelle (meist ipsec0).

Um die gemeinsame Passphrase (PSK) einzutragen, öffnen Sie bitte das Menü "Module > Netzwerk" und klicken Sie auf die gewünschte ipsec-Schnittstelle.

Konfiguration

Öffnen Sie das Programm "Einstellungen" und wählen dort im Menü "Allgemein ==> Netzwerk ==> VPN". Hier können Sie durch Drücken auf "VPN hinzufügen" eine neue Verbindung konfigurieren.



VPN-Zugang bearbeiten

Stellen Sie zunächst sicher dass Sie als VPN-Typ "L2TP" ausgewählt haben und geben Sie eine Bezeichnung für die Verbindung an (z.B. SX-GATE-VPN). Als Server muss entweder eine IP-Adresse oder der (Dyn)DNS-Namen des SX-GATE eingegeben werden.

Bei "Account" ist der Benutzername gefragt, mit dem Sie sich auf dem SX-GATE anmelden wollen. Bitte beachten Sie, dass dieser Benutzer auf dem SX-GATE bereits existieren, und der SX-GATE-Gruppe "system-ras" angehören muss. Optional können Sie noch das Kennwort angeben, mit dem sich der Benutzer am entfernten System anmeldet. Möchten Sie stattdessen bei jedem Verbindungsaufbau nach dem Kennwort gefragt werden, lassen Sie dieses Feld einfach leer.

Zu guter Letzt müssen Sie noch im Feld Shared-Secret den gemeinsamen Pre-Shared-Key angeben.

Haben Sie diese Einstellungen durchgeführt, übernehmen Sie diese durch Drücken auf "Sichern" und gelangen somit automatisch zurück ins Hauptmenü.



Die neu konfigurierte Verbindung wird nun mit der angegebenen Beschreibung im VPN-Menü aufgelistet. Durch antippen der Verbindung wird der Verbindungsaufbau initiiert. Wenn der Tunnel erfolgreich aufgebaut wurde, wird dies durch ein kleines VPN-Symbol in der oberen Menüleiste angezeigt.

16 Kontakt

Wir stehen Ihnen über folgende Kanäle zur Verfügung:

Support-Rufnummer: 07032-95596-21 (Mo-Do 9-12 Uhr, 13-17 Uhr, Fr 9-12 Uhr, 13-16 Uhr)

Support-E-Mail: support@xnetsolutions.de

Postanschrift:

XnetSolutions KG
Benzstraße 32
D-71083 Herrenberg
Germany

Internet: <http://www.xnetsolutions.de>

17 Support für Ihren SX-GATE

Eine Unterstützung bei kniffligen Problemstellungen kann durch Ihre dedizierte Freigabe auch Online via Internet erfolgen. So kann Ihnen unsere Support-Mitarbeiter erklären, was zu tun ist, oder spezifische Probleme mit dem SX-GATE Betriebssystem selbst erledigen.

Dieser Service steht Ihnen montags bis donnerstags in der Zeit von 9 bis 12 Uhr und von 13 bis 17 Uhr und freitags von 9 bis 12 Uhr und von 13 bis 16 Uhr zur Verfügung.

Support-Rufnummer SX-GATE: 07032-95596-21

E-Mail Support SX-GATE: support@xnetsolutions.de

Weiteren Support sowie eine umfangreiche Knowledge-Base und FAQs finden Sie im Internet unter <http://www.xnetsolutions.de> .

Updates erhalten Sie unter <http://update.sx-gate.de> .

Für eine Anfrage halten Sie bitte folgende Informationen bereit (siehe Mein Konto -> Kontakt -> Produktpass):

Fernwartungs-IP-Adresse

Version und Updatelevel