XNETSOLUTIONS
cyber. security. systems

SX-GATE

Software Update
Release Note

Version: 7.1-4-1

Inhaltsverzeichnis

Teil I Wichtige Informationen ... 7

1 Technische Unterstützung ... 7
2 Vorbereitung ... 7
3 Installation ... 7

Teil II Änderungen in dieser Software-Version ... 10

1 Bugfix ... 11
F-Secure Virenscanner-App ... 11
URL-Filter Datenbank-Kategorie "Spyware" ... 11
2 Änderung ... 12
Domainlisten und IP-Listen ... 12

Teil III Änderungen in vorherigen Versionen ... 13

1 Version 7.1-4-0 ... 13
Neu ... 13
Globale Sperrliste für Firewall ... 13
Installationspakete für Verwaltungsserver ... 13
Transparentes Proxying in DMZ-Schnittstellen ... 13
IP-Objekt für Azure Servicebus WCF-Relay ... 13
Update ... 14
Diverse Software-Komponenten ... 14
Kleinere Bugfixes und Verbesserungen ... 14
Sicherheitskritisch ... 15
Zugriff auf Groupware ... 15
Bugfix ... 16
Groupware Filter-Regeln für Postfächer mit Sonderzeichen ... 16
Änderung ... 17
Laufzeitumgebung für Apps ... 17
F-Secure Virenscanner als App ... 17
IP-Objekte und Domainlisten ... 17
2 Version 7.1-3-8 ... 18
Sicherheitskritisch ... 18
Sicherheitslücken in diversen Komponenten ... 18
3 Version 7.1-3-7 ... 19
Neu ... 19
IPsec-Fallback für Verbindungen zu AWS ... 19
Update ... 19
Avira Antivirus ... 19
Änderung ... 19
Verbesserte Import-Funktion ... 19
Bugfix ... 19
Denial-of-Service über OpenSSL Crypto-Bibliothek ... 19
Syntax-Fehler in exportierter OpenVPN-Konfiguration ... 19
Sicherheitskritisch ... 19
Cache poisoning im DNS-Forwarder ... 19
4 Version 7.1-3-6 ... 20
Neu ... 20

© 2022 XnetSolutions KG

Wake-on-LAN bei Verbindungsaufbau von OpenVPN-Clients ... 20
Update ... **21**
Konfiguration des Kaspersky Antivirus Signatur-Updates ... 21
Kleinere Bugfixes und Verbesserungen ... 21
5 Version 7.1-3-5 ... **22**
Sicherheitskritisch ... **22**
Überlauf in NSS Kryptographie-Bibliothek ... 22
Bugfix ... **23**
Transparenter HTTPS-Proxy über Content-Filter ... 23
Update ... **24**
Aktualisierung des Avira Virenscanners ... 24
Kleinere Bugfixes und Verbesserungen ... 24
6 Version 7.1-3-4 ... **25**
Update ... **25**
Aktualisierung des Linux-Kernels ... 25
Aktualisierung diverser Software-Komponenten ... 25
Bugfix ... **26**
Löschen aller Mails aus der Warteschlange ... 26
Neu ... **27**
Alternativer ADSL-PPPoE-Treiber ... 27
7 Version 7.1-3-3 ... **28**
Update ... **28**
Aktualisierung des Linux-Kernels ... 28
Neu ... **29**
Neue Installationspakete für IPsec-L2TP unter Windows ... 29
SSH-Server Schlüssel ... 29
Verwaltungszugriff ... 29
Erlaubte IPs im SNMP-Server ... 29
Statische Kennwörter im Web-Client ... 29
Bugfix ... **30**
Unvollständige ping-Antwortpakete ... 30
Graphische Firewall-Statistik ... 30
Probleme bei DNS-Auflösung ... 30
8 Version 7.1-3-2 ... **31**
Bugfix ... **31**
Tägliche Aufgaben ... 31
9 Version 7.1-3-1 ... **32**
Sicherheitskritisch ... **32**
WLAN Sicherheitslücke FragAttacks ... 32
Bugfix ... **32**
Zertifikatsabruf über ACME ... 32
VPN-Installationspakete für Windows ... 32
Mailversand aus Groupware-App in Version 4.x ... 32
SPAM-Filter-Regeln mit beliebigen Zeichen ... 32
Neu ... **32**
Verifikation von Mail-Server-Zertifikaten über DANE ... 32
Anfertigen von Netzwerk-Dumps ... 32
10 Version 7.1-3-0 ... **33**
Neu ... **33**
Bandbreitenbegrenzung im Web-Proxy ... 33
Ausnahmeliste für transparentes Proxying ... 33
Änderung ... **34**
Verbesserte Kommunikationssicherheit im Cluster ... 34
Verbessertes Bandbreitenmanagement ... 34
Update ... **35**
Aktualisierung diverser Software-Komponenten ... 35
11 Version 7.1-2-2 ... **36**
Neu ... **36**

© 2022 XnetSolutions KG

Konfigurationsoptionen für Webclient 1.2.0 ... 36
Umleitung statt Fehlermeldung für unbekannte Pfade im Reverse-Proxy ... 36
Tabellen in der Administrationsoberfläche ... 36
Archivierungsmöglichkeit für IDS/IPS-Logs ... 36
Bugfix ... **37**
Fehlfunktion des DHCP-Relays in bestimmten Netzwerkkonstellationen ... 37
12 Version 7.1-2-1 ... **38**
Bugfix ... **38**
Fehlende Berechtigungen seit 7.1-2.0 ... 38
Konfigurationsänderungen im SPAM-Filter ... 38
Setzen der Systemzeit ... 38
13 Version 7.1-2-0 ... **39**
Update ... **39**
Kaspersky Antivirus ... 39
Diverse Software-Komponenten ... 39
OpenVPN 2.4 ... 39
Neu ... **40**
Aktualisierung der SSL/TLS-Parameter ... 40
Web-Proxy Funktionalität ... 40
Zwei-Faktor-Authentifzierung für OpenVPN ... 40
OpenVPN-Parameter "tls-crypt" ... 40
Vordefinierte IP-Listen ... 40
Eigene SNMP-MIB ... 41
Mikrofonunterstützung für RDP Web-Client ... 41
Filterung von E-Mail-Anhängen im TNEF-Format (winmail.dat) ... 41
Konfigurierbare Links auf E-Mail Quarantäne ... 41
Zertifikatsverwaltung ... 41
Dynamischer DNS via NAT-Router ... 41
Änderung ... **42**
Konfiguration des IPsec-Servers ... 42
Benutzerdefinierte SPAM-Filter Regeln ... 42
Konfiguration des DNS-Servers ... 42
Konfiguration des DHCP-Servers ... 42
Bugfix ... **43**
Login-Fehler bei URLs mit Zugangsdaten (z.B. ftp://login:password@ftp.example.com) über Web-Proxy Content-Filter ... 43
Probleme mit einzelnen Webseiten bei aktivierter Tunnel-Erkennung im URL-Filter des Web-Proxies ... 43
14 Version 7.1-1-7 ... **44**
Update ... **44**
Neue IDS/IPS Version ... 44
15 Version 7.1-1-6 ... **45**
Update ... **45**
Aktualisierung des Linux-Kernels ... 45
Bugfix ... **45**
Schriftglättung im Web-Client ... 45
Anzeige des Außenstellen-Menüs ... 45
Neu ... **45**
Passwort durchreichen im Web-Client ... 45
Erweiterungen des Web-Clients ... 45
Erweiterungen des Außenstellen-Menüs ... 45
Anderung ... **46**
URL-Filter im Web-Proxy Content-Filter ... 46
Mehr Server-Prozesse für Groupware ... 46
16 Version 7.1-1-5 ... **47**
Sicherheitskritisch ... **47**
PPP-Protokoll ... 47
Deaktivierung des SMB1-Protokolls ... 47
Bugfix ... **47**

© 2022 XnetSolutions KG

Unterbrechungsfreie CA-Migration ... 47
Neu ... **47**
Schachtelung von CA-Bündeln ... 47
Neues Startseiten-Docklet mit Informationen zum E-Mail-Server ... 47
17 Version 7.1-1-4 ... **48**
Neu ... **48**
Markierung des Betreffs von Quarantäne-Mails ... 48
Protokoll-Definition aus DNS SRV-Records ... 48
Änderung ... **48**
Domain-Signaturen im S/MIME-Gateway ... 48
Bugfix ... **48**
Avira Antivirus ... 48
Vereinzelte Durchsatzprobleme durch Intrusion-Prevention ... 48
18 Version 7.1-1-3 ... **49**
Neu ... **49**
IMAP Gruppen-Ordner ... 49
Fernverwaltung für VPN-Außenstellen mit SATELLITE ... 49
Verbindungen von IPS ausnehmen ... 49
Bugfix ... **49**
Zustellung von Quarantäne-Mails an lokale Postfächer ... 49
Endlosschleife bei Anzeige IPsec-Log ... 49
19 Version 7.1-1-2 ... **50**
Änderung ... **50**
Lizenzierung der S/MIME-Gateway Erweiterung ... 50
Backup bei Erneuerung eines Schlüssels im Schlüsselbund ... 50
Löschen abgelaufener Adressen in DNS IP-Objekten ... 50
Neu ... **50**
Neue Funktionen im S/MIME-Gateway ... 50
DHCP-Relay-Server ... 50
Update ... **51**
Let's Encrypt-Zertifikate ... 51
Bugfix ... **51**
Endlosschleife bei Anzeige IPsec-Log ... 51
20 Version 7.1-1-1 ... **52**
Sicherheitskritisch ... **52**
Aktualisierung POP3-/IMAP4-Server ... 52
Neu ... **52**
Neue Kategorien beim kommerziellen URL-Filter ... 52
21 Version 7.1-1-0 ... **53**
Neu ... **53**
Optionale Erweiterungen durch installierbare "Apps" ... 53
Web-Client für RDP, VNC und SSH ... 53
Bisheriger Webmailer wird durch neue Groupware ersetzt ... 53
S/MIME-E-Mail-Verschlüsselungs-Gateway ... 54
Makro-Erkennung im Dateianhangs-Filter für E-Mails ... 54
E-Mail-Synchronisation im Cluster ... 54
Zwei-Faktor-Authentifizierung für den Zugriff auf die Administrations-Oberfläche ... 54
Erweiterte Funktionalität der DNS IP-Objekte ... 54
Hintergrundbild und dunkles Farbschema ... 55
Startseiten Docklet "Updates" ... 55
Menüpunkt "CA-Zertifikate" ... 55
Änderung ... **56**
Geänderter Port 44344 für die Administrations-Oberfläche ... 56
Speicherformat der Postfächer und E-Mailbackup ... 56
Überarbeitetes Lizenz-Menü ... 56
Nicht mehr unterstützte Funktionen ... 57
Bugfix ... **58**

© 2022 XnetSolutions KG

Fehlerhaftes Routing bei IPsec-Tunneln mit SNAT ... 58
Funktionen aus Version 7.0 die in Version 7.1 für alle Systeme verfügbar sind ... 59
Neu ... 59
Bridging ... 59
Bündelung von Netzwerkkarten ... 59
URL-Filter Meldung beim Aufbrechen von SSL-Verbindungen ... 59
Benutzerspezifische Meldung nach Anmeldung an Administrations-Oberfläche ... 59
Lesezugriff auf Administrationsoberfläche ... 59
URL-Filter Benutzergruppen aus Active-Directory ... 59
Zertifikate von Let's Encrypt ... 59
Avira Makro-Erkennung im Web-Proxy ... 60
Monitoring für SSH-TCP-Forwarding ... 60
Protokollierung auf Syslog-Server ... 60

© 2022 XnetSolutions KG

1 Wichtige Informationen

Die in dieser Release Note enthaltenen Informationen beruhen auf sorgfältiger Recherche. Dennoch läßt es sich nicht ausschließen, dass eine Information im Einzelfall unzutreffend ist. Wir bitten daher um Ihr Verständnis, wenn wir keine Gewähr für die Richtigkeit der Informationen übernehmen und jede Haftung ausschließen. Sollten Sie feststellen, dass eine Information unzutreffend ist, bitten wir um Ihre Rückmeldung.

Richten Sie Ihre Rückmeldung bitte an die folgende E-Mail Adresse: support@xnetsolutions.de

1.1 Technische Unterstützung

Um technische Unterstützung bei der Durchführung des Software-Updates zu erhalten, können Sie unseren technischen Support via Telefon oder E-Mail erreichen. Wenn Sie den technischen Support kontaktieren, halten Sie bitte folgende Informationen bereit:

- momentan installierte SX-GATE Software-Version
- Geräte-ID
- SX-GATE Support-IP-Adresse

Diese Informationen können Sie über die Startseite auslesen.

So erreichen Sie den technischen Support:

Rufnummer:	+49 (0) 7032-95596-21
E-Mail:	support@xnetsolutions.de

1.2 Vorbereitung

Das Update der Systemsoftware erfolgt mit einer Update-Datei, um alle notwendigen Komponenten und Subsysteme intelligent zu aktualisieren. Die aktuelle Update-Datei enthält dabei alle vorherigen Updates seit dem letzten Update auf eine Hauptversion. Die Updates sind immer in der Reihenfolge der Versionsnummerierung zu installieren.

Hinweis:

Die Folge eines unterbrochenen Update-Vorgangs könnte sein, dass Ihr SX-GATE nicht mehrt bootet. Schalten Sie das SX-GATE deshalb nicht aus oder führen einen manuellen Neustart durch, während das Update durchgeführt wird. Sollte ein Neustart notwendig sein, wird dies durch das Update automatisch durchgeführt.

1.3 Installation

Bitte beachten Sie, dass Ihr SX-GATE die erforderlichen Voraussetzungen erfüllen muss, bevor Sie dieses Software-Update Installieren.

- **Arbeitsspeicher mindestens 2048 MB (2 GB) - optimal mindestens 4096 MB (4 GB)**

Sie können die aktuelle Speicherbestückung in der Konfigurationsoberfläche **auf der Startseite** einsehen. Für alle Fragen bzgl. des Software-Updates wenden Sie sich bitte an den technischen Support.

Gehen Sie folgendermaßen vor, um ein Software-Update durchzuführen:

© 2022 XnetSolutions KG

Hinweis:

Erstellen Sie bitte vor dem durchführen des Software-Updates ein System-Backup, ein Benutzer-Backup und ein E-Mail-Backup.

Für das Durchführen eines Software-Updates haben Sie die folgenden Möglichkeiten:

- **Automatisches Software-Update über die SX-GATE Konfigurationsoberfläche**

Führen Sie über das Menü **»System → Update«** ein interaktives Software-Update durch. Wählen Sie dazu die Option **»interaktiv (empfohlen)«** und folgen Sie den Anweisungen auf dem Bildschirm. Wählen Sie im folgenden die Schaltfläche **»Weiter«**, um das Update automatisch zu installieren. Über das Fortschreiten des Software-Updates und einen bei Bedarf erforderlichen Reboot des SX-GATE werden Sie im interaktiven Update-Log informiert.

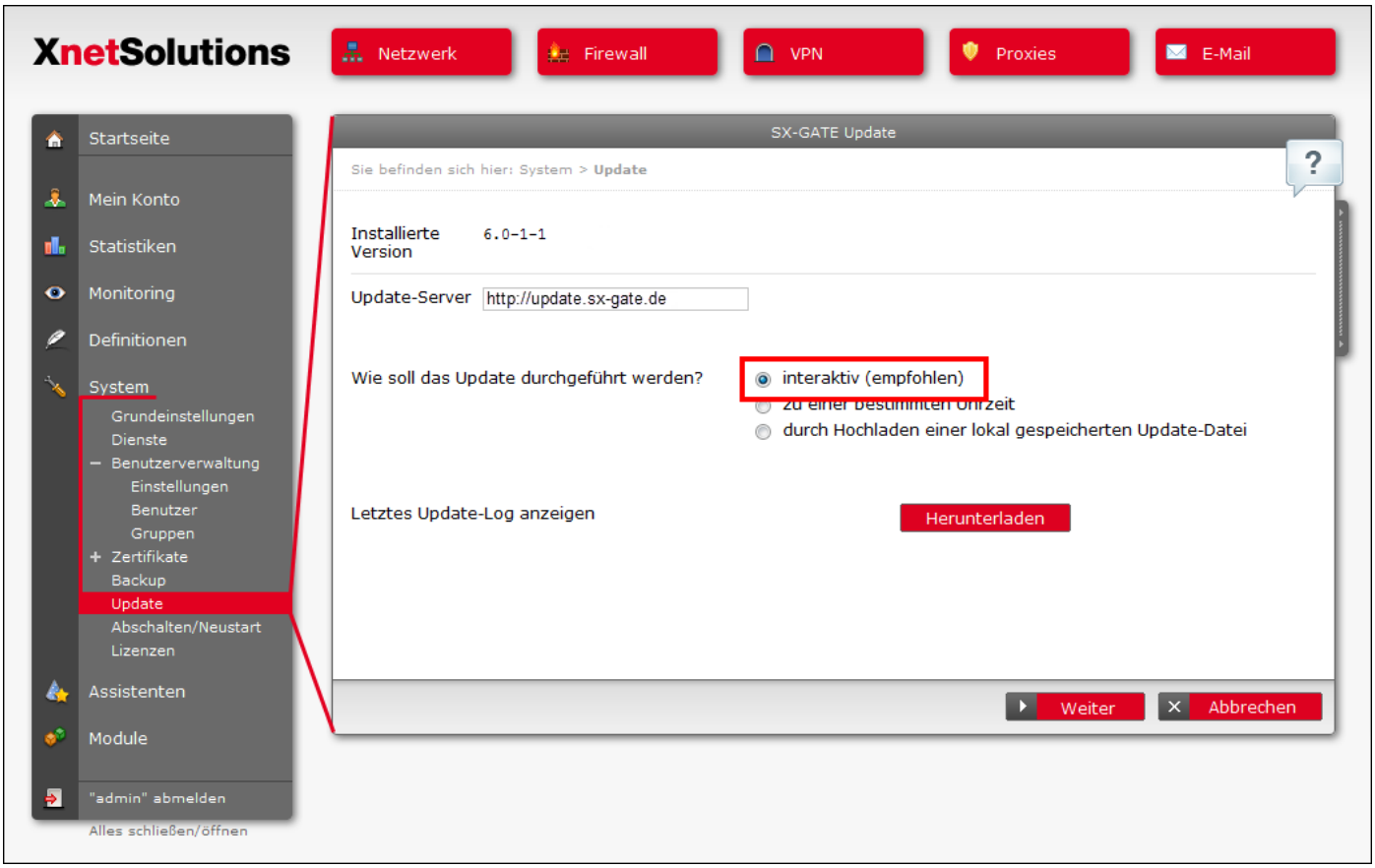

Abbildung 1 - Menü »System → Update«

- **Manuelles Software-Update**

Bevor Sie das Software-Update durchführen können ist es erforderlich, dass Sie das benötigte Software-Update Version 7.1-4-1 von der SX-GATE Update-Webseite herunterladen.

Die Update-Webseite erreichen Sie unter http://www.xnetsolutions.de → Menü **»Support -> Software Updates«**.

Führen Sie über das Menü **»System → Update«** ein manuelles Software- Update durch. Wählen Sie dazu die Option »durch Hochladen einer lokal gespeicherten Update-Datei« und folgenden Sie den Anweisungen auf dem Bildschirm.

© 2022 XnetSolutions KG

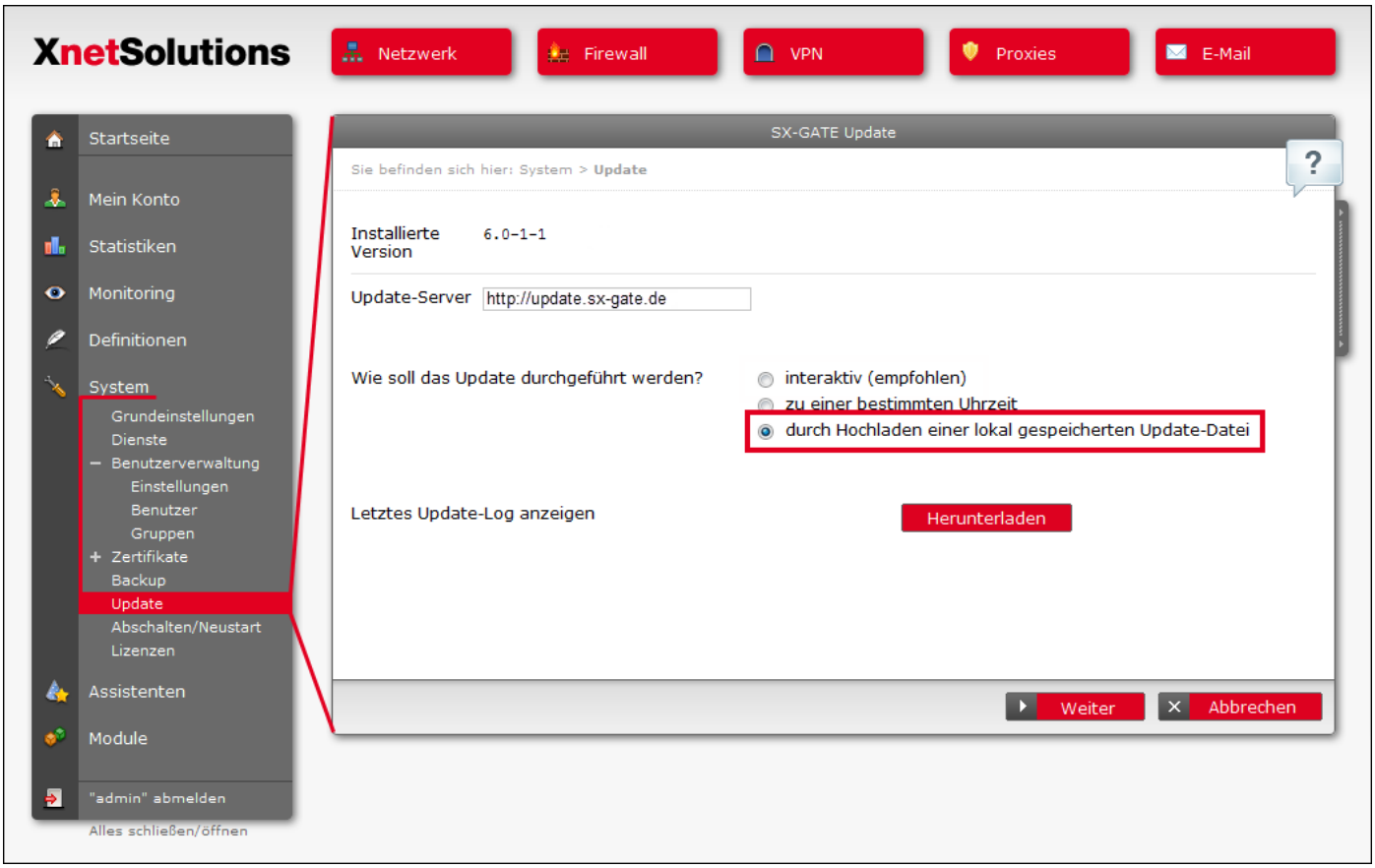

Abbildung 2 - Menü »System → Update«

Wichtig:

Der Update-Vorgang kann, je nach Größe des Updates und Leistungsfähigkeit des SX-GATE, einige Zeit in Anspruch nehmen.

© 2022 XnetSolutions KG

2 Änderungen in dieser Software-Version

Neustart erforderlich

Nach dem Update führt das System automatisch einen oder mehrere Neustarts durch. Bitte führen Sie keinen manuellen Reboot durch! Das System kann dadurch funktionsunfähig werden.

Kostenpflichtiges Update

Sie können das Update kostenfrei herunterladen, wenn ein Software-Pflegevertrag besteht oder das Gerät erst vor kurzem gekauft wurde. Der Download ist für die entsprechenden Geräte bereits freigeschaltet. Systeme, auf die diese Voraussetzungen nicht zutreffen, werden nach dem käuflichen Erwerb des Updates freigeschaltet.

Die Zugangsdaten zum Download des Updates werden beim Interaktiven Update vom System selbständig übermittelt. Sollten Sie das Update von Hand herunterladen, so geben Sie bitte als Benutzername die Support-IP (z.B. 172.18.253.15) und als Kennwort die Geräte-ID (z.B. 473I-QN34-O@:5) des Systems ein.

Wichtiger Hinweis:

Beachten Sie bitte unbedingt die Informationen zum geänderten Port der Administrations-Oberfläche sowie zum Speicherformat der Postfächer auf dem System.

Wichtiger Hinweis:

Aufgrund zahlreicher Aktualisierungen dauert der Update-Vorgang deutlich länger als üblich (nach dem Download mind. 10-15 Minuten). Bitte haben Sie Geduld.

© 2022 XnetSolutions KG

2.1 Bugfix

2.1.1 F-Secure Virenscanner-App

Auf einzelnen Geräten kam es nach einem Neustart zu Problemen mit dem Mail-Virenscan.
Der Web-Proxy Content-Filter zeigte bei passwortgeschützten oder verschlüsselten Dateien die falsche Meldung an (Virenscanner nicht installiert).

2.1.2 URL-Filter Datenbank-Kategorie "Spyware"

In der kostenfreien URL-Filter-Datenbank wurde in Version 7.1-4.0 eine neue Datenquelle für die Kategorie "Spyware" integriert. Diese fasst den Begriff Spyware jedoch sehr weit, was zu Problemen bei einzelnen Webseiten führte. Wir haben die aus dieser Datenquelle übernommenen Einträge nun deutlich reduziert.

© 2022 XnetSolutions KG

2.2 Änderung

2.2.1 Domainlisten und IP-Listen

Folgende Ergänzungen wurden in den Domainlisten vorgenommen:

- OFFICE: cdn.office.net
- WINDOWS: Update-Server für Exchange Antimalware
- ANTIVIRUS: Update-Server für Sophos-Virenscanner

In den IP-Objekten wurden die neuen IP-Listen GOOGLE_CLOUD und MICROSOFT_AZURE eingeführt. Die IP-Liste AMAZON wurde zu AMAZON_AWS umbenannt.

© 2022 XnetSolutions KG

3 Änderungen in vorherigen Versionen

3.1 Version 7.1-4-0

3.1.1 Neu

3.1.1.1 Globale Sperrliste für Firewall

In den globalen Einstellungen der Firewall lässt sich jetzt eine schnittstellenunabhängige Sperrliste für IP-Adressen konfigurieren. Zu IP-Adressen in dieser Liste dürfen weder ein- noch ausgehende Verbindungen aufgebaut werden. Die Verwendung von beliebigen IP-Objekten, inklusive Geolokation, ist möglich.

3.1.1.2 Installationspakete für Verwaltungsserver

Dank der neuen Installationspakete lassen sich jetzt weitere Systeme im Handumdrehen an den Verwaltungsserver anbinden. Das Installationspaket wird vom Administrator des Verwaltungsservers erstellt und ist mit einem Kennwort geschützt. Auf dem Zielsystem muss nur noch das Installationspaket hochgeladen und das zugehörige Kennwort eingegeben werden.
Um das Installationspaket nutzen zu können, muss auch auf den zu verwaltenden Systemen mindestens Version 7.1-4.0 installiert sein. Es wird ausschließlich der Tunnel-Modus unterstützt, bei dem das verwaltete System die Verbindung zum Verwaltungsserver initiiert.

3.1.1.3 Transparentes Proxying in DMZ-Schnittstellen

Die Schalter zur einfachen Konfiguration von transparentem Proxying sind nun auch in DMZ-Schnittstellen verfügbar. Bisher standen die Schalter nur in LAN- und RAS-Schnttstellen zur Verfügung. In DMZ-Schnittstellen musste das transparente Proxying mit Hilfe von Firewall-Regeln eingerichtet werden.
Bereits in Version 7.1-3.7 wurden die Einstellmöglichkeiten bei den Schaltern für transparentes Web-Proxying erweitert. Ist in der Konfiguration des Web-Proxies erlaubt, den Content-Filter zu umgehen, lässt sich jetzt wählen ob der transparente Zugriff mit oder ohne Content-Filter erfolgen soll. Bisher konnte der Zugriff ohne Content-Filter nur mit Hilfe von Firewall-Regeln eingerichtet werden.
Hilfreich ist der transparente Zugriff ohne Content-Filter, wenn der Content-Filter verschlüsselte (HTTPS-)Verbindungen aufbricht, an manchen Schnittstellen aber Geräte angeschlossen sind, auf denen das Proxy-CA-Zertifikat nicht installiert werden kann (z.B. Mitarbeiter-WLAN mit privaten Endgeräten). Sollen diese Geräte dennoch den Proxy nutzen, würden Sie bei diesen Schnittstellen das transparente HTTPS-Proxying ohne Content-Filter einstellen. Vergessen Sie jedoch nicht, ggf. den Zugriff des Proxies auf vertrauenswürdige Netze wie das LAN einzuschränken.

3.1.1.4 IP-Objekt für Azure Servicebus WCF-Relay

Nach Angabe des Servicebus-Namespaces ermittelt dieses IP-Objekt über DNS die IP-Adressen der zugehörigen Relay-Server.

© 2022 XnetSolutions KG

3.1.2 Update

3.1.2.1 Diverse Software-Komponenten

Mit dem Update werden der Linux-Kernel, der Avira-Virenscanner, diverse System-Bibliotheken und Anwendungen aktualisiert. Auch die vordefinierten Listen der vertrauenswürdigen CAs und die kostenlose URL-Filter-Datenbank werden aktualisiert. Systeme ohne tägliche Aktualisierung der IDS-Regeln (Systeme ohne Pflegevertrag) erhalten mit diesem Update neue IDS-Regeln.

3.1.2.2 Kleinere Bugfixes und Verbesserungen

© 2022 XnetSolutions KG

3.1.3 Sicherheitskritisch

3.1.3.1 Zugriff auf Groupware

Auf Systemen mit installierter Groupware hat der Reverse-Proxy seit Version 7.1-3.4 Zugriff stets an die Groupware weitergeleitet, selbst wenn in der Konfiguration des Reverse-Proxies die Groupware-Option nicht aktiviert war.

© 2022 XnetSolutions KG

3.1.4 Bugfix

3.1.4.1 Groupware Filter-Regeln für Postfächer mit Sonderzeichen

Groupware Filter-Regeln, die E-Mails automatisch in Postfächer mit Sonderzeichen im Namen sortieren sollten, haben stattdessen in einen neuen Ordner mit kodiertem Sonderzeichen sortiert.
Bestehende Filter-Regeln werden durch das Update nicht verändert. Sie können die Regeln nun aber bearbeiten und auf den korrekten Ordnernamen mit Sonderzeichen umstellen.

© 2022 XnetSolutions KG

3.1.5 Änderung

3.1.5.1 Laufzeitumgebung für Apps

Mit dem Update wechseln wir die Laufzeitumgebung für Apps von "Docker" auf das leichtgewichtigere "Podman". Letzterer kommt insbesondere ohne einen eigenen Dienst aus.
Systeme, auf denen Apps installiert sind, müssen diese zuvor auf die aktuellste Version bringen. Das Update bricht sonst mit einer Fehlermeldung ab. Anschließend werden die Apps automatisch in Podman importiert, sofern es der verfügbare Speicherplatz zulässt. Reicht der Speicherplatz nicht aus, wird das Update mit einer passenden Handlungsempfehlung abgebrochen.

3.1.5.2 F-Secure Virenscanner als App

Die neue Version des F-Secure Scanners wird als App installiert. Dieses Update aktualisiert den alten Scanner noch nicht automatisch auf die neue App. Ein automatisches Upgrade wird erst in einer späteren Version stattfinden. Installieren Sie bitte nach dem Update (und nach dem Neustart) die F-Secure App im Menü "System > Apps", um die alte durch die neue Version zu ersetzen.
Mit der neuen Version bietet nun auch F-Secure eine Cloud-Option zur Unterstützung des Scan-Prozesses an. Diese Option ist standardmäßig aktiviert, kann aber in der Administrationsoberfläche deaktiviert werden. Mit der Cloud-Option sollen neue Schädlinge schneller erkannt werden, noch bevor neue Signaturdateien den Weg bis zum lokalen Scanner gefunden haben. Ferner werden Links in E-Mails geprüft. Verweisen diese auf einen Webserver, der von F-Secure eine schlechte Reputation erhalten hat, wird die Mail wie eine Virusmail behandelt (auch wenn in der Mail strenggenommen kein Virus enthalten ist).

3.1.5.3 IP-Objekte und Domainlisten

Nachdem die Microsoft Cloud Deutschland Ende 2021 geschlossen wurde, entfallen das IP-Objekt und die Domainliste MICROSOFT_365_DE. Verwenden Sie stattdessen bitte MICROSOFT_365. Weiterhin sind die IP-LISTS AMAZON_VIDEO, BITTORRENT, HOTSPOT_SHIELD, MINING, PS_VUE, WECHAT, WHATSAPP und WHATSAPP_FILES nicht mehr verfügbar.
Soweit sie nicht verwendet werden, werden diese Listen durch das Update gelöscht. Listen, die noch in Verwendung sind, werden geleert und mit einem entsprechenden Kommentar versehen. Ferner wird eine entsprechende E-Mail an den "admin" gesendet.
Die IP-LIST MS_ONE_DRIVE wurde in SHAREPOINT umbenannt. TEAMS kann als Synonym für SKYPE verwendet werden. Neu sind die IP-LISTS EXCHANGE und INSTAGRAM.
Unter GEO wurden vordefinierte Geolokations-Objekte für Deutschland (DE), deutschsprachige Länder (DACH) und die Europäische Union (EU) angelegt.

© 2022 XnetSolutions KG

3.2 Version 7.1-3-8

3.2.1 Sicherheitskritisch

3.2.1.1 Sicherheitslücken in diversen Komponenten

Das Update behebt weniger kritische Sicherheitslücken im Linux-Kernel, beim Komprimieren mit der zlib-Bibliothek, in der XML-Parser-Bibliothek expat und im Avira Virenscanner.

© 2022 XnetSolutions KG

3.3 Version 7.1-3-7

3.3.1 Neu

3.3.1.1 IPsec-Fallback für Verbindungen zu AWS

Ein Virtual-Private-Gateway (VPG) in der AWS-Cloud kann zur Erhöhung der Verfügbarkeit unter zwei IP-Adressen angesprochen werden. Ein neuer IPsec-Verbindungstyp ermöglicht es nun, beide VPG-IPs zu konfigurieren und bei Störung der Verbindung zu einer der IPs automatisch die Verbindung zur anderen IP aufzubauen.

3.3.2 Update

3.3.2.1 Avira Antivirus

3.3.3 Änderung

3.3.3.1 Verbesserte Import-Funktion

Beim Import von Daten in eine zweispaltige Tabelle, bei der die zweite Spalte lediglich für Kommentare vorgesehen ist, müssen die zu importierenden Daten nun nicht mehr im zweispaltigen Format (mit Tabulator) vorliegen. Es lassen sich auch einfache Listen mit einem Wert pro Zeile importieren. So lassen sich jetzt beispielsweise von extern bezogene IP-Listen einfach in ein IP-Objekt importieren.

3.3.4 Bugfix

3.3.4.1 Denial-of-Service über OpenSSL Crypto-Bibliothek

Das Update beseitigt einen Fehler in der OpenSSL System-Bibliothek, der in Anwendungen zu einer Endlos-Schleife führen konnte.

3.3.4.2 Syntax-Fehler in exportierter OpenVPN-Konfiguration

Bei aktivierten Einmalpasswörtern für OpenVPN-Verbindungen enthielten das für die Clients exportierte Installationspaket bzw. die exportierten OpenVPN-Konfigurationsdateien einen Syntax-Fehler.

3.3.5 Sicherheitskritisch

3.3.5.1 Cache poisoning im DNS-Forwarder

Das Problem betrifft ausschließlich Konfigurationen, bei denen Provider-Nameserver konfiguriert sind, zugleich aber auch die Namensauflösung über die Internet-Root-Nameserver erlaubt ist. Bei einer Namensauflösung über die Root-Server wurden potentiell manipulierte Nameserver-Informationen aus dem Cache verwendet, die über die Provider-Nameserver bezogen wurden.

© 2022 XnetSolutions KG

3.4 Version 7.1-3-6

3.4.1 Neu

3.4.1.1 Wake-on-LAN bei Verbindungsaufbau von OpenVPN-Clients

Bisher wurde das automatische Anschalten eines PCs per Wake-on-LAN nur im Web-Client und beim Verbindungsaufbau von IPsec-L2TP-Clients unterstützt. Ab sofort ist dies auch bei OpenVPN-Clients möglich. Voraussetzung ist, dass in der Konfiguration der OpenVPN-Server-Schnittstelle die Benutzerauthentifzierung mit Einmalpasswörtern aktiviert ist. Wie für IPsec-L2TP-Clients muss die MAC-Adresse des zu weckenden PCs in den RAS-Einstellungen der Benutzerverwaltung beim jeweiligen Benutzer hinterlegt werden.

© 2022 XnetSolutions KG

3.4.2 Update

3.4.2.1 Konfiguration des Kaspersky Antivirus Signatur-Updates

Die Konfiguration für das Signatur-Update des Kaspersky-Scanners muss bis 31.01.2022 angepasst werden. Ohne die Anpassung wird das Signatur-Update nach diesem Datum fehlschlagen.

3.4.2.2 Kleinere Bugfixes und Verbesserungen

© 2022 XnetSolutions KG

3.5 Version 7.1-3-5

3.5.1 Sicherheitskritisch

3.5.1.1 Überlauf in NSS Kryptographie-Bibliothek

Die Bibliothek wird von IPsec, OpenVPN, der Intrusion-Prevention und der Administrations-Oberfläche genutzt. Die Sicherheitslücke erlaubt einem nicht authentifizierten Angreifer potentiell die Ausführung von Code.

© 2022 XnetSolutions KG

3.5.2 Bugfix

3.5.2.1 Transparenter HTTPS-Proxy über Content-Filter

Bei deaktivierter SSL-Prüfung wurde bei transparenten HTTPS-Verbindungen fälschlicherweise die IP und nicht der Servername als Ziel der Verbindung genutzt. Sofern die Proxy-Konfiguration HTTPS-Zugriffe auf IP-Adressen verbietet, wurden die Verbindungen abgewiesen. Andernfalls kam es bei aufgebrochenen HTTPS-Verbindungen zu Problemen mit einzelnen Servern, die beim SSL-Verbindungsaufbau auf die Angabe des Servernamens angewiesen sind.

© 2022 XnetSolutions KG

3.5.3 Update

3.5.3.1 Aktualisierung des Avira Virenscanners

3.5.3.2 Kleinere Bugfixes und Verbesserungen

© 2022 XnetSolutions KG

3.6 Version 7.1-3-4

3.6.1 Update

3.6.1.1 Aktualisierung des Linux-Kernels

3.6.1.2 Aktualisierung diverser Software-Komponenten

© 2022 XnetSolutions KG

3.6.2 Bugfix

3.6.2.1 Löschen aller Mails aus der Warteschlange

Beim Löschen aller Mails aus der Mail-Server Warteschlange wurden fälschlicherweise auch alle Mails aus dem Quarantäne-Bereich gelöscht.

© 2022 XnetSolutions KG

3.6.3 Neu

3.6.3.1 Alternativer ADSL-PPPoE-Treiber

Für ADSL-Verbindungen mit PPP-over-Ethernet kann jetzt ein alternativer Treiber ausgewählt werden, der Bandbreiten jenseits von 200 MBit/s unterstützt.

© 2022 XnetSolutions KG

3.7 Version 7.1-3-3

3.7.1 Update

3.7.1.1 Aktualisierung des Linux-Kernels

© 2022 XnetSolutions KG

3.7.2 Neu

3.7.2.1 Neue Installationspakete für IPsec-L2TP unter Windows

Die bisher genutzten Installationspakete basierten auf Microsofts CMAK-Profilen, bei denen nach wie vor SHA1 zum Einsatz kommt. Wir haben uns daher entschieden, nun eine eigene, auf Powershell basierende Lösung anzubieten. Neben der Nutzung von SHA2 bietet die neue Lösung folgende Vorteile:

- Konfiguration zusätzlicher Routen bei Split-Tunneling
- Gleichzeitige Installation mehrerer Verbindung zu unterschiedlichen Zielsystemen möglich

Anders als bei CMAK lassen sich die Einstellungen der VPN-Verbindung auf dem Windows-Client nachträglich anpassen.

Die bisherigen, CMAK-basierten Profile, werden parallel nach wie vor angeboten, es wird jedoch empfohlen, nach und nach auf die neue Alternative umzustellen.
Bei beiden Varianten des Installationspakets lässt sich nun der Windows Registry-Schlüssel über das Installationspaket setzen, der benötigt wird, wenn sich der VPN-Server hinter einem NAT-Router befindet.

3.7.2.2 SSH-Server Schlüssel

Die vom Secure-Shell-Server genutzten RSA- und ed25519-Schlüssel sind nun im Schlüsselbund hinterlegt. So kann nun ein Backup des Schlüssels erstellt oder zurückgesichert werden bzw. jederzeit ein neuer Schlüssel genriert werden

3.7.2.3 Verwaltungszugriff

In dieser Versionsreihe nur auf Systemen mit Software-Pflegevertrag verfügbar.

Dem Fachhändler oder, bei einem Verbund mehrerer Systeme, einem zentralen System kann Zugriff für Verwaltungsaufgaben gewährt werden. In der ersten Ausbaustufe ist neben dem Abruf einiger grundlegenden Informationen der Aufbau von Fernwartungsverbindungen, das Starten von Updates und der Zugriff auf die Administrations-Oberfläche möglich.
Das zugehörige Menü auf dem zentralen System wurde von "Außenstellen" in "Verwaltungsserver" umbenannt.

3.7.2.4 Erlaubte IPs im SNMP-Server

Welche IP-Adressen Zugriff auf den SNMP-Server erhalten, lässt sich jetzt über die Administrations-Oberfläche einstellen.

3.7.2.5 Statische Kennwörter im Web-Client

Das Kennwort des Zielsystems lässt sich jetzt in der Konfiguration einer Web-Client-Verbindung eintragen, so dass sich der Benutzer nur am Web-Client selbst anmelden muss. Generell emfehlen wir dieses Vorgehen nicht, es kann aber nützlich sein, um beispielsweise externen Dienstleistern vorrübergehend priviligierten Zugriff auf ein internes System zu ermöglichen, ohne das Passwort dieses Systems ändern oder weitergeben zu müssen.

© 2022 XnetSolutions KG

3.7.3 Bugfix

3.7.3.1 Unvollständige ping-Antwortpakete

Das in Version 7.1-3.0 aktualisierte Werkzeug ping ignorierte unvollständige Antwortpakete. Systeme, die das pingbasierte Leitungsfallback konfiguriert haben und die neben den Google-Nameservern keine oder nur eine weitere Adresse per ping auf Verfügbarkeit prüfen, wechselten daraufhin in den Fallback-Modus, da die Google-Nameserver große ping-Pakete nur unvollständig beantworten.

3.7.3.2 Graphische Firewall-Statistik

Seit Version 7.1-3.0 wurde die Statistik nicht mehr aktualisiert.

3.7.3.3 Probleme bei DNS-Auflösung

Auf Systemen, die zur Namensauflösung die DNS-Root-Nameserver nutzen, kam es insbesondere nach einem Neustart des Systems bei der Auflösung bestimmter Adressen zu Fehlern.

© 2022 XnetSolutions KG

3.8 Version 7.1-3-2

3.8.1 Bugfix

3.8.1.1 Tägliche Aufgaben

Seit Version 7.1-3-0 wurden die täglichen Aufgaben, wie das Erstellen der Statistiken oder das Rotieren der Logfiles, usw., nicht mehr ausgeführt.

© 2022 XnetSolutions KG

3.9 Version 7.1-3-1

3.9.1 Sicherheitskritisch

3.9.1.1 WLAN Sicherheitslücke FragAttacks

Auf Geräten mit WLAN-Unterstützung sichert das Update den WLAN-Protokollstack gegen FragAttacks.

3.9.2 Bugfix

3.9.2.1 Zertifikatsabruf über ACME

Der Abruf von Zertifikaten über das ACME-Protokoll (Let's Encrypt) schlug in 7.1-3.0 fehl. Die neue Version der Komponente, die zur Kommunikation mit dem ACME-Server genutzt wird, konnte dessen Zertifikat nicht verifizieren.

3.9.2.2 VPN-Installationspakete für Windows

Mit Version 7.1-3.0 erstellte IPsec-L2TP- und OpenVPN-Installationspakete (*.exe) ließen sich nicht installieren.

3.9.2.3 Mailversand aus Groupware-App in Version 4.x

In Version 7.1-3.0 schlug der Versand von Mails aus der Groupware-App heraus fehl, wenn diese in Version 4.x installiert war.

3.9.2.4 SPAM-Filter-Regeln mit beliebigen Zeichen

Benutzerdefinierte SPAM-Filter-Regeln unterstützten bisher nur Suchmuster mit ASCII-Zeichen. Jetzt sind beliebige Zeichen möglich.

3.9.3 Neu

3.9.3.1 Verifikation von Mail-Server-Zertifikaten über DANE

Wenn ein Mail-Server eine E-Mail an einen anderen Mail-Server weiterleitet, ist es nicht praktikabel, das Zertifikat des Ziel-Servers grundsätzlich zu verifizieren. Viele Mail-Server sind nämlich nicht mit gültigen Zertifikaten ausgestattet. DANE ermöglicht es dem Betreiber eines Mail-Servers, im DNS die Information zu hinterlegen, dass und wie das Zertifikat seines Mail-Server verifiziert werden kann. Die Unterstützung von DANE in der Variante DANE-EE kann nun im Mail-Server aktiviert werden.

3.9.3.2 Anfertigen von Netzwerk-Dumps

Im Menü "Monitoring > Netzwerk > Werkzeuge" gibt es jetzt die Möglichkeit, einen Paketdump zu erstellen. Der Dump lässt sich als pcap-Datei herunterladen oder als Text anzeigen.

© 2022 XnetSolutions KG

3.10 Version 7.1-3-0

3.10.1 Neu

3.10.1.1 Bandbreitenbegrenzung im Web-Proxy

In dieser Versionsreihe nur auf Systemen mit Software-Pflegevertrag verfügbar.

Die Bandbreite lässt sich anhand der Client-IPs und/oder des angesprochenen Servernamens begrenzen. Bei lokaler Benutzeranmeldung ist auch eine Begrenzung je Benutzergruppe möglich.

3.10.1.2 Ausnahmeliste für transparentes Proxying

In der Firewall-Konfiguration von LAN- und RAS-Schnittstellen gibt es nun eine Ausnahmeliste für Ziel-Adressen, zu denen kein transparentes Proxying durchgeführt werden soll.

© 2022 XnetSolutions KG

3.10.2 Änderung

3.10.2.1 Verbesserte Kommunikationssicherheit im Cluster

Wenn sich der Backup-Knoten mit dem Master verbindet, wird nun auch der Schlüssel des Masters geprüft.

3.10.2.2 Verbessertes Bandbreitenmanagement

Bei Internetanbindungen mit hoher Bandbreite erzielen die Prioritätsklassen "niedrig" und "normal" nun einen höheren und gleichmäßigeren Durchsatz.

© 2022 XnetSolutions KG

3.10.3 Update

3.10.3.1 Aktualisierung diverser Software-Komponenten

© 2022 XnetSolutions KG

3.11 Version 7.1-2-2

3.11.1 Neu

3.11.1.1 Konfigurationsoptionen für Webclient 1.2.0

Die Zwischenablage für RDP- und VNC-Verbindungen kann nun deaktiviert oder auf eine Richtung beschränkt werden. Bei RDP-Verbindungen kann der Dateitransfer nun ebenfalls auf eine Richtung beschränkt werden. Ferner können die zusätzlichen Tastaturlayouts für RDP-Verbindungen konfiguriert werden.

3.11.1.2 Umleitung statt Fehlermeldung für unbekannte Pfade im Reverse-Proxy

Zugriffe auf URL-Pfade für die kein Hintergrund-Server konfiguriert wurde, sind bisher mit einer Fehlermeldung abgewiesen worden. Alternativ kann nun eine Umleitung auf eine beliebige URL mit oder ohne Beibehaltung des URL-Pfads konfiguriert werden. Als spezieller Anwendungsfall lassen sich in einem unverschlüsselten HTTP-Port alle Anfragen auf die entsprechende verschlüsselte HTTPS-Seite umleiten.

3.11.1.3 Tabellen in der Administrationsoberfläche

Bisher konnte über das Einstellungs-Menü in der rechten, oberen Ecke festgelegt werden, ob sortierbare Tabellen mit mehr als 20 Einträgen mit einer Seitenschaltung oder in einer gruppierten Ansicht dargestellt werden sollen. Dies lässt sich nun individuell je Tabelle einstellen. Die Voreinstellung für Tabellen zur Auswahl von Unterobjekten ist die gruppierte Ansicht. Für Wertetabellen ist die Seitenschaltung voreingestellt.

3.11.1.4 Archivierungsmöglichkeit für IDS/IPS-Logs

© 2022 XnetSolutions KG

3.11.2 Bugfix

3.11.2.1 Fehlfunktion des DHCP-Relays in bestimmten Netzwerkkonstellationen

© 2022 XnetSolutions KG

3.12 Version 7.1-2-1

3.12.1 Bugfix

3.12.1.1 Fehlende Berechtigungen seit 7.1-2.0

Nach der Aktualisierung der SELinux-Berechtigungen in 7.1-2.0 schlugen einzelne Operationen aufgrund fehlender Zugriffsrechte fehl. Betroffen waren das Ausschalten des Geräts über den Schalter am Gehäuse, die Archivierung von Logdateien auf Windows-Netzwerkfreigaben, die neue OpenVPN-Funktion Anmeldung mit Einmal-Passwörtern und das Generieren eines neuen OpenVPN-Schlüssels für tls-crypt.

3.12.1.2 Konfigurationsänderungen im SPAM-Filter

Änderungen an der SPAM-Filter-Konfiguration wurden in 7.1-2.0 erst nach manuellem Neustart wirksam.

3.12.1.3 Setzen der Systemzeit

Das Einstellen der Systemzeit über Administrationsoberfläche sowie zeitgesteuert täglich bzw. wöchentlich funktionierte in Version 7.1-2.0 nicht mehr. Die kontinuierliche Zeitsynchronisation mittels NTP-Dienst war nicht betroffen.

© 2022 XnetSolutions KG

3.13 Version 7.1-2-0

3.13.1 Update

3.13.1.1 Kaspersky Antivirus

Für diese Version sind andere Signaturen erforderlich. Mit 337 MB ist das Update des Scanners daher ungewöhnlich umfangreich. Deshalb haben wir den neuen Scanner nicht wie sonst üblich in das Update integriert, sondern laden diesen bei Bedarf nach.

Systeme, auf denen eine ältere Version des Kaspersky-Scanners installiert ist, laden zu Beginn der Update-Prozedur zunächst das 337 MB große Kaspersky-Update von unserer Webseite herunter.

Sie haben alternativ die Möglichkeit, selbst die neue Version des Kaspersky-Scanners von unserer Webseite herunterzuladen und vor dem Update manuell einzuspielen.

3.13.1.2 Diverse Software-Komponenten

Mit dem Update werden der Linux-Kernel, die Virenscanner-Engines, diverse System-Bibliotheken und Anwendungen aktualisiert. Auch die vordefinierten Listen der vertrauenswürdigen CAs, die URL-Filter-Datenbank und das SPAM-Filter-Regelwerk werden aktualisiert. Systeme ohne tägliche Aktualisierung der IDS-Regeln (Systeme ohne Pflegevertrag) erhalten mit diesem Update neue IDS-Regeln.

3.13.1.3 OpenVPN 2.4

Die neue Version bietet vor allem verbesserte kryptographische Sicherheit. Das bevorzugte Verschlüsselungsverfahren ist jetzt AES-GCM. Clients, auf denen ebenfalls OpenVPN 2.4 installiert ist, profitieren automatisch von der verbesserten Sicherheit, da der Server in der Regel das auf dem Client konfigurierte Verschlüsselungsverfahren überstimmen kann.

Beim Ausstellen eines neuen Client-Zertifikats lässt sich neben dem Installations-Paket für Windows-Clients nun auch eine ovpn-Konfigurationsdatei herunterladen. Der private Schlüssel ist dabei wahlweise mit oder ohne Kennwortschutz hinterlegt.

Der Import einer OpenVPN-Konfiguration in einer OpenVPN-Client-Schnittstelle unterstützt nun zusätzlich die Parameter "compress" und "tls-crypt".

© 2022 XnetSolutions KG

3.13.2 Neu

3.13.2.1 Aktualisierung der SSL/TLS-Parameter

Für verschlüsselte Verbindungen steht nun in fast allen Komponenten TLS-1.3 zur Verfügung. In vielen Komponenten lässt sich dabei das TLS-Niveau konfigurieren. Als Voreinstellung für Komponenten, die üblicherweise nur von einem geschlossenen Benutzerkreis angesprochen werden, ist "aktuell" gesetzt. Der Client muss dazu mindestens TLS-1.2 unterstützen. Algorithmen mit Cipher-Block-Chaining und SHA1 sind deaktiviert. Für ausgehende Verbindungen und für Komponenten, die potentiell auch von beliebigen Internet-Nutzern angesprochen werden, ist "kompatibel" voreingestellt. Dies erlaubt TLS-1.0 und SHA1. Weitere möglche Einstellungen sind "veraltet" (Cipher-Block-Chaining) und "maximal" (ausschließlich TLS-1.3).

3.13.2.2 Web-Proxy Funktionalität

Bisher hatten sich Proxy-Authentifzierung und transparentes Proxying gegenseitig ausgeschlossen. Nun lässt sich beides gleichzeitig nutzen. Prinzipbedingt findet bei transparenten Verbindungen keine Authentifizierung statt. Ferner ist transparentes Proxying für HTTPS nun auch ohne aktivierten Content-Filter möglich.

Der Content-Filter Port für transparentes HTTPS-Proxying wechselt von 8084 zu 8445. Bitte passen Sie etwaige manuell konfigurierte DNAT-Regeln an. Der Port 8445 darf nicht anderweitig belegt sein.

Clients können den Web-Proxy nun auch verschlüsselt ansprechen. In den meisten Browsern ist dies jedoch nicht direkt konfigurierbar. Die Proxy-Konfiguration muss dazu in der Regel über WPAD bzw. PAC-Datei erfolgen.
Die Liste der vertrauenswürdigen CA-Zertifikate, die beim Aufbrechen von SSL-Verbindungen im Content-Filter genutzt wird, lässt sich jetzt konfigurieren.

3.13.2.3 Zwei-Faktor-Authentifzierung für OpenVPN

In dieser Versionsreihe nur auf Systemen mit Software-Pflegevertrag verfügbar.

Je OpenVPN-Server-Schnittstelle kann jetzt die Benutzerauthentifzierung mit zeitbasierten Einmal-Passwörtern (TOTP) aktiviert werden. Eine Anmeldung an dieser Schnittstelle ist dann nur noch für Mitglieder der Benutzergruppe "system-ras" möglich, für die Einmal-Passwörter aktiviert sind.

3.13.2.4 OpenVPN-Parameter "tls-crypt"

In dieser Versionsreihe nur auf Systemen mit Software-Pflegevertrag verfügbar.

Je OpenVPN-Server-Schnittstelle kann der Kontrollkanal der Verbindungen mit einem zusätzlichen symmetrischen Schlüssel abgesichert werden. OpenVPN-Datenströme sind damit nur noch schwer als solche zu identifizieren. Unter anderem wird auch der TLS-Handshake beim Verbindungsaufbau verschlüsselt, bei dem mit TLS-Version 1.2 oder älter Zertifikate im Klartext übertragen werden.

3.13.2.5 Vordefinierte IP-Listen

Als IP-Objekt stehen unter dem Präfix "IP-LISTS/" nun Listen mit den IP-Adressen diverser Dienste oder Firmen zur Verfügung. Die Listen werden über die normalen Updates aktualisiert. Manuelle Änderungen sind zwar möglich, werden beim nächsten Update jedoch überschrieben. Die Daten in den Listen basieren auf öffentlich verfügbaren Informationen. Insbesondere für die Richtigkeit und Vollständigkeit wird keine Gewähr übernommen.

© 2022 XnetSolutions KG

3.13.2.6 Eigene SNMP-MIB

Zur SNMP-basierten Überwachung des Systems steht nun zusätzlich zu den Standard-MIBs eine eigen MIB mit z.B. Versionsinformationen, Lizenzen und Dienste-Status zur Verfügung.

3.13.2.7 Mikrofonunterstützung für RDP Web-Client

Für RDP Web-Clients lässt sich nun je Benutzer auch der Audio-Input-Kanal (Mikrofonunterstützung) aktivieren. Mind. Version 1.1.0-2 der Web-Client-App ist dazu erforderlich.

3.13.2.8 Filterung von E-Mail-Anhängen im TNEF-Format (winmail.dat)

Optional lässt sich nun auch der Inhalt von winmail.dat-Anhängen auf unerwünschte Dateien untersuchen. Falls der Dateianhangs-Filter so eingestellt ist, dass unerwünschte Anhänge aus der Mail entfernt und in den Quarantäne-Bereich verschoben werden sollen, wird im Fall eines windmail.dat-Anhangs grundsätzlich die komplette Mail in Quarantäne gestellt.

3.13.2.9 Konfigurierbare Links auf E-Mail Quarantäne

Der Servername, der in Links auf E-Mails und Anhänge in Quarantäne genutzt wird, lässt sich nun anpassen.

3.13.2.10 Zertifikatsverwaltung

Im Schlüsselbund ist es nun möglich, Zertifikate zu aktualisieren ohne das zugrundeliegende RSA-Schlüsselpaar zu erneuern (re-issue). Diese Funktion wird eher selten benötigt, z.B. wenn eine CA nach einem Sicherheitsvorfall Zertifikate neu signiert. Ferner lässt sich eine nicht mehr benötigte Zertifikatsanfrage nun löschen.

3.13.2.11 Dynamischer DNS via NAT-Router

Bisher ließ sich dynamischer DNS nur auf Schnittstellen konfigurieren, die selbst eine dynamische IP zugewiesen bekommen. Im Menü "DNS" lässt sich dynamischer DNS jetzt auch für Fälle konfigurieren, in denen ein vorgelagerter NAT-Router die dynamische IP erhält. Die im DNS zu hinterlegende externe IP wird in diesem Fall regelmäßig von einem konfigurierbaren externen Dienst abgefragt.

© 2022 XnetSolutions KG

3.13.3 Änderung

3.13.3.1 Konfiguration des IPsec-Servers

Die Konfigurationsoptionen "IKEv1 bevorzugen" und "IKEv2 bevorzugen" stehen nicht mehr zur Verfügung. Verbindungen können nur noch entweder für IKEv1 oder IKEv2 konfiguriert werden. Die Konfiguration wird entsprechend konvertiert, wenn eine der beiden entfallenen Optionen konfiguriert war.

In der Konfiguration der Verschlüsselungsparameter stehen für Phase 1 zusätzliche DH-Gruppen, bei IKEv2 zudem AES-GCM zur Verfügung.

Für L2TP-IPsec-Verbindunge war es möglich, Kennwörter im Klartext zu speichern, um eine Authentifzierung über Challenge-Response-Verfahren wie CHAP zu ermöglichen. Diese Möglichkeit wurde deaktiviert, kann aber im Bedarfsfalls durch den technischen Support wieder aktiviert werden. Sofern kein Bedarf mehr für diese Funktion besteht, wird die Funktionalität in einer kommenden Version vollständig entfernt.

3.13.3.2 Benutzerdefinierte SPAM-Filter Regeln

Um Fehlkonfigurationen zu vermeiden, wurde die Bedeutung der Suchmuster leicht verändert. Suchmuster, die mit einem Buchstaben oder einer Ziffer beginnen bzw. enden, treffen ab sofort nur noch zu, wenn der Suchbegriff am Anfang bzw. Ende eines Wortes steht. Bestehende Suchmuster werden automatisch konvertiert, so dass diese nach wie vor auch innerhalb eines Wortes Übereinstimmungen finden ("muster" wird zu "*muster*" konvertiert).

3.13.3.3 Konfiguration des DNS-Servers

Bei DNS-Regeln und bei benutzerdefinierten Einträgen in Domain- und Reverse-Lookup-Zonen ist nun ein Export und Import möglich. Bei den benutzerdefinierten Einträgen lässt sich zudem ein individueller TTL-Wert konfigurieren. Die Konfiguration von CAA-Records ist jetzt möglich. In Weiterleitungs-Zonen können IP-Objekte genutzt werden.

3.13.3.4 Konfiguration des DHCP-Servers

Der DHCP-Server kann nun auch ohne Angabe eine IP-Bereichs je Schnittstelle aktiviert werden. Dies ermöglicht den Betrieb mit ausschließlich statisch zugewiesenen IP-Adressen.

© 2022 XnetSolutions KG

3.13.4 Bugfix

3.13.4.1 Login-Fehler bei URLs mit Zugangsdaten (z.B. ftp://login:password@ftp.example.com) über Web-Proxy Content-Filter

Die Zugangsdaten wurden fälschlicherweise in Kleinbuchstaben konvertiert.

3.13.4.2 Probleme mit einzelnen Webseiten bei aktivierter Tunnel-Erkennung im URL-Filter des Web-Proxies

© 2022 XnetSolutions KG

3.14 Version 7.1-1-7

3.14.1 Update

3.14.1.1 Neue IDS/IPS Version

Die neue Version bietet zusätzliche und leistungsfähigere Signaturen. Aktualisieren Sie bitte zeitnah, da die Signaturen für ältere Versionen nur noch teilweise aktualisiert werden können.

© 2022 XnetSolutions KG

3.15 Version 7.1-1-6

3.15.1 Update

3.15.1.1 Aktualisierung des Linux-Kernels

3.15.2 Bugfix

3.15.2.1 Schriftglättung im Web-Client

Der Schalter für die Schriftglättung bei RDP-Verbindungen war bislang wirkungslos.

3.15.2.2 Anzeige des Außenstellen-Menüs

Mit steigender Anzahl Einträge kam es zu Anzeigefehlern oder Timeouts.

3.15.3 Neu

3.15.3.1 Passwort durchreichen im Web-Client

Werden für die Anmeldung am Web-Client und am Zielsystem die gleichen Kennwörter genutzt, kann die Verbindung nun so konfiguriert werden, dass das Kennwort durchgereicht wird und nicht ein zweites Mal eingegeben werden muss.

3.15.3.2 Erweiterungen des Web-Clients

Die Administrationsoberfläche unterstützt folgenden Neuerungen, für die jedoch mindestens Version 1.1.0 des Web-Clients installiert sein muss.

- Anschalten des Zielsystems per Wake-on-LAN.
  Legen Sie dazu zunächst IP-Objekte vom Typ "Host" an, in denen die MAC-Adresse und die IPv4-Adresse der Zielsysteme konfiguriert werden. Wählen Sie diese Objekte anschließend in der Benutzerverwaltung als Zielsystem in den entsprechenden Web-Client-Verbindungen aus.
- Anzeige der aktiven Verbindungen im Menü "Monitoring > Netzwerk > Status".
- Option zur dynamischen Änderung der Bildschirmauflösung bei RDP. Das Zielsystem muss dazu RDP in Version 8.1 unterstützen (ab Windows 8, Windows Server 2012).
- Zusätzliche Tastatur-Layouts für RDP, darunter Deutsch (Schweiz), Englisch (Großbritannien) und Türkisch.

Version 1.0.0 des Web-Clients ignoriert diese Einstellungen.

3.15.3.3 Erweiterungen des Außenstellen-Menüs

In der Übersicht wird zusätzlich das Ablaufdatum des Zertifikats sowie die Verfügbarkeit von WLAN-Hardware angezeigt. Über ein Link-Symbol kann direkt die Administrations-Oberfläche der Außenstelle geöffnet werden. Weitere Details werden nicht mehr über Tooltip sondern mit Klick auf das Info-Icon angezeigt.

© 2022 XnetSolutions KG

3.15.4 Anderung

3.15.4.1 URL-Filter im Web-Proxy Content-Filter

Bei aktiviertem Content-Filter erfolgt eine zusätzliche Prüfung auf gesperrte Dateinamen, wenn zusammen mit der Datei ein von der URL abweichender Dateiname übermittelt wird.

3.15.4.2 Mehr Server-Prozesse für Groupware

Die maximale Anzahl gleichzeitiger Verbindungen wird basierend auf der Anzahl E-Mail-Konten berechnet. Um Engpässe zu vermeiden, stehen nun mehr Prozesse zur Verfügung.

© 2022 XnetSolutions KG

3.16 Version 7.1-1-5

3.16.1 Sicherheitskritisch

3.16.1.1 PPP-Protokoll

Das Update behebt einen Puffer-Überlauf im PPP-Dienst der für ADSL- und für L2TP-Verbindungen genutzt wird. Die Sicherheitslücke ist kritisch, da sie bereits vor einer Authentifzierung ausgenutzt werden kann.

3.16.1.2 Deaktivierung des SMB1-Protokolls

Das automatisch Backup und die Archivierung von Logdateien auf eine Windows-Freigabe erfolgte bislang aufgrund eines Konfigurationsfehlers mit dem veralteten und unsicheren SMB1-Protokoll oder älter. Mit dem Update wird mindestens die SMB-Protokollversion 2.1.0 vorausgesetzt (mind. Windows 2008R2 bzw. Windows 7).

Bei der NTLM-Authentifzierung und den Netzwerk-Freigaben standen zwar alle aktuellen SMB-Protokollversionen zur Verfügung, SMB1 war aber ebenfalls noch möglich. Ein Angreifer konnte daher einen Protokoll-Downgrade auf das SMB1-Protokoll erzwingen. Auch hier wird nun mindestens SMB 2.1.0 vorausgesetzt.

3.16.2 Bugfix

3.16.2.1 Unterbrechungsfreie CA-Migration

In Version 7.1-1.4 war die unterbrechungsfreie VPN-Migration zu einem neuen eigenen CA-Zertifikat nicht möglich.

3.16.3 Neu

3.16.3.1 Schachtelung von CA-Bündeln

Insbesondere um die Erweiterung des Standard-CA-Bündels durch eigene CAs zu erleichtern, ist es nun möglich, CA-Bündel hierarchisch zu verknüpfen.

3.16.3.2 Neues Startseiten-Docklet mit Informationen zum E-Mail-Server

© 2022 XnetSolutions KG

3.17 Version 7.1-1-4

3.17.1 Neu

3.17.1.1 Markierung des Betreffs von Quarantäne-Mails

E-Mails mit potentiell gefährlichen Dateianhängen werden vom Dateianhangs-Filter entweder unter Quarantäne gestellt oder ohne die beanstandeten Anhänge zugestellt. Auf Wunsch kann der Betreff betroffener E-Mails nun mit einem beliebigen Text markiert werden.

3.17.1.2 Protokoll-Definition aus DNS SRV-Records

In den Definitionen können IP-Objekte angelegt werden, die DNS SRV-Records abfragen. Ein Bestandteil von SRV-Records ist die Information, auf welchem UDP- oder TCP-Port ein Dienst angeboten wird. Es besteht jetzt die Möglichkeit, von einer Protokoll-Definition aus auf ein IP-Objekt zu verweisen, um die Portinformationen als Protokoll nutzbar zu machen.

3.17.2 Änderung

3.17.2.1 Domain-Signaturen im S/MIME-Gateway

Bei eingehenden E-Mails mit Domain-Signaturen wird ab sofort im Betreff der Zusatz "[SIGNIERT VON <*@domain>]" angezeigt.
E-Mail-Clients sollten eine Domain-Signatur aufgrund des nicht zur Absender-Adresse passenden Zertifikats als fehlerhaft anzeigen. Neben der Option, korrekte Signaturen grundsätzlich zu entfernen, haben wir daher die Option ergänzt, nur Domain-Signaturen zu entfernen.

3.17.3 Bugfix

3.17.3.1 Avira Antivirus

Aufgrund einer falsch konfigurierten Update-Prozedur konnte sich der Scanner nach dem Signatur-Update vom 14.01.2020 gegen 16:00 Uhr nicht mehr mit den Servern für Online-Abfragen verbinden.

3.17.3.2 Vereinzelte Durchsatzprobleme durch Intrusion-Prevention

© 2022 XnetSolutions KG

3.18 Version 7.1-1-3

3.18.1 Neu

3.18.1.1 IMAP Gruppen-Ordner

In dieser Versionsreihe nur auf Systemen mit Software Pflegevertrag verfügbar.

Bisher wurden Benutzergruppen vom E-Mail-Server grundsätzlich als E-Mail-Verteiler genutzt. Jedes Gruppenmitglied erhielt dabei eine Kopie der an die Gruppe addressierten E-Mails. Jetzt lässt sich in der Gruppenverwaltung je Gruppe auswählen, ob diese für den E-Mail-Server keine Bedeutung haben soll, als E-Mail-Verteiler fungiert oder ob ein gemeinsamer IMAP-Ordner für die Gruppenmitglieder zur Verfügung gestellt werden soll.

3.18.1.2 Fernverwaltung für VPN-Außenstellen mit SATELLITE

Diese Funktion ist noch nicht vollständig umgesetzt und daher noch als experimentell zu betrachten. Für Feedback wären wir dankbar.

Im neuen Menüpunkt "System > Außenstellen" können Sie Ihre SATELLITEs erfassen. Sofern der Zugriff auf die Systeme möglich ist, wird ein Status u.a. mit der Versionsnummer angezeigt. Ferner wird die Möglichkeit angeboten, Updates an die Außenstellen zu verteilen. Dazu muss aktuell mind. SATELLITE-Version 3.1.1 installiert sein.

Beachten Sie bitte, dass aktuell nur von dem System aus auf die Außenstelle zugegriffen werden kann, das das VPN-Installationspaket für die Außenstelle ausgestellt hat. Eine Möglichkeit, den Zugriff nachträglich zu authorisieren wird später nachgereicht.

3.18.1.3 Verbindungen von IPS ausnehmen

Basierend auf Protokoll, Quell- und Ziel-Adresse lassen sich nun Verbindungen von der Verarbeitung durch das Intrusion-Prevention-System ausnehmen.

3.18.2 Bugfix

3.18.2.1 Zustellung von Quarantäne-Mails an lokale Postfächer

Die Zustellung von E-Mails in der Quarantäne an lokale Postfächer funktionierte nicht. Die Zustellung an interne E-Mail-Server sowie der Zugriff auf Dateianhänge in der Quarantäne waren davon nicht betroffen.

3.18.2.2 Endlosschleife bei Anzeige IPsec-Log

In den meisten Zeilen des IPsec-Logs gibt es einen Link, der ein extra Fenster mit allen zur selben Verbindung gehörenden Zeilen öffnet. Durch dieses Fenster wurde eine Endlosschleife ausgelöst, die zu dauerhaft hoher Systemauslastung führte.

© 2022 XnetSolutions KG

3.19 Version 7.1-1-2

3.19.1 Änderung

3.19.1.1 Lizenzierung der S/MIME-Gateway Erweiterung

Auf vielfachen Wunsch hin wurde die Lizenzierung des S/MIME-Gateways umgestellt. Die Lizenzierung erfolgt nicht mehr anhand der Anzahl Systembenutzer sondern anhand der Anzahl S/MIME-Schlüssel. S/MIME-Schlüssel, die als E-Mail-Domain-Zertifikat genutzt werden, müssen nicht lizenziert werden.

3.19.1.2 Backup bei Erneuerung eines Schlüssels im Schlüsselbund

Wird im Schlüsselbund ein Schlüssel geändert, bleibt der vorherige Schlüssel nun als Backup auf dem System erhalten.

In Verbindung mit dem S/MIME-Gateway wird der Backup-Schlüssel genutzt, um beim Wechsel des S/MIME-Schlüssels eingehende E-Mails entschlüsseln zu können, die noch mit dem alten Schlüssel verschlüsselt wurden.

3.19.1.3 Löschen abgelaufener Adressen in DNS IP-Objekten

Die Standardeinstellung zum Löschen abgelaufener Einträge in DNS IP-Objekten wurde von "sofort" auf "nach 6 Stunden" geändert. So werden laufende Neustarts von Diensten vermieden, wenn sich DNS-Einträge bereits nach wenigen Minuten oder gar Sekunden ändern. Alle auf "sofort" konfigurierten DNS IP-Objekte werden durch das Update automatisch umgestellt.

3.19.2 Neu

3.19.2.1 Neue Funktionen im S/MIME-Gateway

Das S/MIME-Gateway unterstützt nun auch das nicht standardisierte Konzept der E-Mail-Domain-Zertifikate. Diese Funktion kann auf fast allen Systemen kostenfrei genutzt werden (Ausnahme: Lizenzen ohne E-Mail-Option wie z.B. Enterprise-VPN oder Enterprise-Proxy). Bei E-Mail-Domain-Zertifikaten wird für die S/MIME-Kommunikation mit definierten Partnern ein einziges S/MIME-Zertifikat für die gesamte E-Mail-Domain anstatt eines Zertifikats je E-Mail-Adresse genutzt. Dabei können sogar Zertifikate einer internen CA zum Einsatz kommen. Das Verfahren setzt jedoch voraus, dass die Gegenstelle eine entsprechend konfigurierbare E-Mail-Verschlüsselung nutzt.

Das Anlegen von Benutzern entfällt ab sofort, wenn das S/MIME-Gateway in Kombination mit einem internen E-Mail-Server betrieben wird. Für interne E-Mail-Server die vertrauenswürdige Absender-Adressen garantieren, wird jetzt eine eigene Liste mit zugehörigen S/MIME-Schlüsseln gepflegt.

In der Benutzerverwaltung lassen sich jetzt mehrere S/MIME-Schlüssel je Benutzer hinterlegen. Zum Signieren ausgehender E-Mails wird automatisch der zur Absender-E-Mail-Adresse passende Schlüssel gewählt.

In vorherigen Version konnten mehrere Schlüssel je Benutzer hinterlegt werden, um eingehende E-Mails zu entschlüsseln, die mit alten Zertifikaten verschlüsselt wurden. Diese Funktionalität ist ab sofort in den Schlüsselbund integriert.

3.19.2.2 DHCP-Relay-Server

In Ethernet- und VLAN-Schnittstellen kann das SX-GATE nun auch als DHCP-Relay-Server fungieren. Anfragen von Clients werden dabei an einen DHCP-Server in einem anderen Netzwerk weitergeleitet.

© 2022 XnetSolutions KG

3.19.3 Update

3.19.3.1 Let's Encrypt-Zertifikate

Der Client zum Abruf von Let's Encrypt-Zertifikaten nutzt ab jetzt das Protokoll ACMEv2.

3.19.4 Bugfix

3.19.4.1 Endlosschleife bei Anzeige IPsec-Log

In den meisten Zeilen des IPsec-Logs gibt es einen Link, der ein zusätzliches Fenster mit allen zur selben Verbindung gehörenden Log-Einträgen öffnet. Durch dieses Fenster wurde eine Endlosschleife ausgelöst, die zu dauerhaft hoher Systemauslastung führte.

© 2022 XnetSolutions KG

3.20 Version 7.1-1-1

3.20.1 Sicherheitskritisch

3.20.1.1 Aktualisierung POP3-/IMAP4-Server

Das Update behebt ein kritisches Sicherheitsproblem. Einem Angreifer war es damit ohne Authentifizierung möglich, geschützte Informationen auszulesen oder sogar eigenen Programmcode auszuführen.

3.20.2 Neu

3.20.2.1 Neue Kategorien beim kommerziellen URL-Filter

Beim kommerziellen URL-Filter wurden neue Kategorien hinzugefügt: Waffen, DNS-over-HTTPS, Filme und Serien mit fragwürdigem Rechtsstatus, Bildung, Restaurants und Kochrezepte, Gesundheit, Gesundheitswesen, Krankenversicherung, Haus oder Wohnung kaufen oder mieten und Börsen und Handelssysteme.

© 2022 XnetSolutions KG

3.21 Version 7.1-1-0

3.21.1 Neu

3.21.1.1 Optionale Erweiterungen durch installierbare "Apps"

Im neuen Menüpunkt "System > Apps" können optionale Erweiterungen in Form von "Apps" installiert werden. Beachten Sie bitte, das installierte "Apps" unabhängig von System-Updates aktualisiert werden müssen. Prüfen Sie daher bitte das "Apps"-Menü regelmäßig in Bezug auf verfügbare Updates, sobald Sie "Apps" installiert haben.

3.21.1.2 Web-Client für RDP, VNC und SSH

Diese neue Komponente wird als "App" über das Menü "System > Apps" installiert. Sie ermöglicht den Zugriff auf Remote-Desktops (RDP), VNC-Server sowie Secure-Shell-Server mit Hilfe eines Web-Browsers (HTML5). Ein spezieller Client ist nicht erforderlich. Der Zugriff erfolgt ausschließlich über Reverse-Proxy und lässt sich daher auf Wunsch mit Client-Zertifikaten zusätzlich absichern. Auf Wunsch kann die Anmeldung über Zwei-Faktor-Authentifizierung mit zeitbasierten Einmal-Passwörtern (TOTP) erfolgen. Entsprechende TOTP Smartphone-Apps sind kostenfrei verfügbar (z. B. Google Authenticator). Alternativ bieten wir TOTP Hardware-Token an.

Hinweis:

Für diese optionale Erweiterung muss eine Lizenz erworben werden.

3.21.1.3 Bisheriger Webmailer wird durch neue Groupware ersetzt

Der in die Jahre gekommene Webmailer wird mit dem Update durch eine deutlich umfangreichere Groupware ersetzt, die ebenfalls als "App" installiert wird. Die auf der Groupware greift auf E-Mails ausschließlich via IMAP zu. Ein Zugriff auf E-Mails ist somit jederzeit auch ohne Groupware möglich. Adressen, Termine, Aufgaben, Mail-Filter und Einstellungen speichert die Groupware in einer Datenbank. Sowohl die Groupware als auch die Datenbank werden als "App" installiert.

Anders als der bisherige Webmailer ist die Groupware nicht vorinstalliert. Sie können sie jederzeit kostenlos über das Menü "System > Apps" nachinstallieren bzw. aktualisieren. Installieren Sie zuerst die App "Datenbank", danach die App "Groupware".

Gegenüber dem alten Webmailer bietet die Groupware folgende Vorteile:

- moderne, auf Smartphones ausgerichtete Web-Oberfläche
- Freigeben und Abonnieren von Kalendern und Adressbüchern mit individueller Rechtevergabe
- Planung und Austausch von Terminen via E-Mail über iCalendar
- Frei/Belegt-Anzeige
- Aufgabenlisten (TODOs)
- Markierung von E-Mails, Terminen und Aufgaben
- Delegation von Konten ("Senden als")

Für die native Anbindung von Smartphone-Apps, Outlook und anderen E-Mailclients bieten wir eine Erweiterung mit den Protokollen "Exchange-ActiveSync", "CalDAV" und "CardDAV" an.

Hinweis:

Für diese optionale Erweiterung muss eine Lizenz erworben werden. Der Zugriff auf die Groupware via Webbrowser bleibt kostenfrei.

© 2022 XnetSolutions KG

3.21.1.4 S/MIME-E-Mail-Verschlüsselungs-Gateway

Mit dieser neuen Komponente können Sie S/MIME-Signaturen und S/MIME-Verschlüsselung für die externe Kommunikation einsetzen, ohne S/MIME auf den lokalen E-Mail-Clients einrichten und pflegen zu müssen.

Hinweis:

Für diese optionale Erweiterung muss eine Lizenz erworben werden.

Eingehende E-Mails lassen sich mit dieser Lösung automatisch entschlüsseln und zwar vor sicherheitsrelevanten Prüfungen wie Virenscan oder Dateianhangs-Filter. Ferner werden die Signaturen eingehender E-Mails geprüft. Die in den Signaturen enthaltenen Zertifikate können auf Wunsch automatisch für den verschlüsselten Versand freigegeben werden. Alle zukünftigen E-Mails an diese Kommunikationspartner werden dann ohne weiteres Zutun automatisch verschlüsselt. Eine manuelle Freigabe sowie der manuelle Import von Zertifikaten für die automatische Verschlüsselung ausgehender E-Mails ist ebenfalls möglich. Jede ausgehende E-Mail kann zudem automatisch signiert werden.

Wichtig:

Für das Signieren ausgehender E-Mails und das Entschlüsseln eingehender E-Mails wird je E-Mail-Adresse ein S/MIME-Zertifikat benötigt, das in der Benutzerverwaltung hinterlegt werden muss. Je Zertifikat ist dabei ein eigener Benutzer erforderlich.

3.21.1.5 Makro-Erkennung im Dateianhangs-Filter für E-Mails

Der Dateianhangs-Filter kann jetzt gezielt Dateianhänge unter Quarantäne stellen, wenn diese ein Office-Dokument mit Makro enthalten. Es lässt sich dabei zwischen Autoexec-Makros und beliebigen Makros unterscheiden. Sofern der Dateianhangs-Filter aktiviert ist, wird diese neue Funktion mit dem Update automatisch aktiviert.

Nach wie vor ist es sinnvoll, Office-Dokumente anhand des Dateinamens unter Quarantäne zu stellen, wenn schon anhand der Dateiendung erkennbar ist, dass ein Makro enthalten ist (docm, dotm, pptm, potm, xlsm, xltm). Wer jedoch auch die "klassischen" Office-Dateiendungen filtert (doc, ppt, xls), kann diese ggf. jetzt freigeben und mit Hilfe der neuen Optionen nur dann unter Quarantäne stellen, wenn tatsächlich ein Makro enthalten ist.

3.21.1.6 E-Mail-Synchronisation im Cluster

Auf Cluster-Systemen mit lokalen E-Mail-Domains werden die Inhalte der Postfächer ab sofort zwischen den beiden Cluster-Knoten synchronisiert.

3.21.1.7 Zwei-Faktor-Authentifizierung für den Zugriff auf die Administrations-Oberfläche

Um den Zugriff auf die Administrations-Oberfläche besser abzusichern, kann nun ein zusätzliches Einmal-Passwort abgefragt werden. Die Funktion lässt sich für direkte Zugriffe und Zugriffe über Reverse-Proxy unabhängig konfigurieren. Werden Einmal-Passwörter als verpflichtend konfiguriert, können sich Benutzer ohne Einmal-Kennwort nicht anmelden. Bei "optional" wird das Einmal-Passwort nur bei Konten mit aktiviertem Einmal-Kennwort verlangt.

3.21.1.8 Erweiterte Funktionalität der DNS IP-Objekte

Neben Hostnamen können nun auch Service-, Mail-Exchanger- und Name-Server-Einträge (SRV, MX, NS) im DNS als Basis für IP-Objekte dienen.

Die Aktualisierung von DNS-basierten IP-Objekten erfolgt zudem nicht mehr in festen Intervallen sondern basierend auf der individuellen Cache-Dauer (TTL) der Einträge.

Bei DNS-basierten Loadbalancern ändern sich die einem Servernamen zugeordneten IP-Adressen unter Umständen im Sekundentakt. Über einen längeren Zeitraum betrachtet, werden jedoch immer wieder die selben Adressen genutzt. Eine neue Option erlaubt es, alte Adressen noch eine Weile vorzuhalten, was die Anzahl der Konfigurationsänderungen deutlich verringert.

© 2022 XnetSolutions KG

3.21.1.9 Hintergrundbild und dunkles Farbschema

Das neue dunkle Farbschema ist jetzt der Standard. Es lässt sich über das Werkzeug-Menü in der rechten oberen Ecke deaktivieren.

3.21.1.10 Startseiten Docklet "Updates"

Das neue Docklet prüft die Verfügbarkeit von neuen System- oder App-Updates.

3.21.1.11 Menüpunkt "CA-Zertifikate"

Im neuen Menüpunkt "System > Zertifikatsverwaltung > CA-Zertifikate" lassen sich CA-Zertifikate hinterlegen, die als vertrauenswürdig gelten sollen. Hier können Sie auch die von uns gepflegten CA-Bündel einsehen. Die beiden bisherigen Menüpunkte der eigenen CA wurden in das neue Menü verschoben.

© 2022 XnetSolutions KG

3.21.2 Änderung

3.21.2.1 Geänderter Port 44344 für die Administrations-Oberfläche

Der Browser-Zugriff auf die zuvor beschriebenen "Apps" erfolgt ausschließlich über Reverse-Proxy, der daher ab sofort eine zentralere Rolle spielt. Wir haben daher beschlossen, zukünftig den Reverse-Proxy auf Port 443 zu aktivieren. Zuvor war Port 443 durch die Administrations-Oberfläche belegt, die Sie nun auf Port 44344 erreichen.

Um Ihnen die Umstellung zu erleichtern, leitet der Reverse-Proxy Zugriffe für die Administrations-Oberfläche mittels Redirect auf die LAN-IP, Port 44344 um. Durch den Redirect greift der Browser anschließend direkt auf die Administrations-Oberfläche zu und nicht über den Reverse-Proxy. So soll die versehentliche Freigabe des Internet-Zugriffs auf die Administrations-Oberfläche vermieden werden, wenn der Internet-Zugriff auf Port 443 geöffnet wird.

Wichtig:

Falls Sie von außerhalb des LANs zugreifen, wird dieser Redirect nicht funktionieren. Nutzen Sie für den externen Zugriff auf die Administrations-Oberfläche den Reverse-Proxy oder stellen Sie sicher, dass der Zugriff auf Port 44344 möglich ist.

3.21.2.2 Speicherformat der Postfächer und E-Mailbackup

Postfächer auf dem System werden zukünftig in einem anderen Format gespeichert. Beim Update und beim Einspielen eines Backups im alten Format werden die Daten entsprechend konvertiert.

Hinweis:

Wir empfehlen, vor dem Update den E-Mail-Server zu stoppen und ein aktuelles E-Mailbackup zu erstellen. Erstellen Sie nach dem Update erneut ein Backup, jetzt im neuen Format, bevor Sie den E-Mail-Server wieder starten.

Wichtig:

Abhängig von der Anzahl der E-Mails kann die Konvertierung der Postfächer mehrere Minuten - bei E-Mailbeständen im Bereich von zehntausenden von E-Mails auch Stunden - in Anspruch nehmen. Das Ausschalten oder ein Neustart des Systems in dieser Phase kann zum Verlust von Daten führen.

Wird ein Backup mit Daten im neuen Format eingespielt, werden zukünftig die E-Mails aus dem Backup mit dem aktuellen E-Mailbestand zusammengeführt, d.h. gelöschte E-Mails werden aus dem Backup wiederhergestellt, neue E-Mails und Änderungen bleiben erhalten. Falls Sie die Groupware nutzen, gilt selbiges für Adressen, Termine und Aufgaben. Die benutzerspezifischen Einstellungen der Groupware sowie die E-Mail-Filter werden aus dem Backup übernommen.

Wichtig:

Beim Einspielen eines E-Mailbackups im alten Format findet keine Zusammenführung statt. Die Daten aus dem Backup werden eingespielt, eventuelle neue E-Mails gehen verloren.

Bisher wurden die Daten aus dem Backup nur für die Konten restauriert, für die kein Posteingangs-Ordner existiert. Dieser Mechanismus existiert nicht mehr. Um gezielt die Daten bestimmter Konten wiederherzustellen, müssen Sie das E-Mailbackup mit einem ZIP-Entpacker öffnen. Das E-Mailbackup enthält je Konto eine eigene Backup-Datei. Extrahieren Sie die Backups der gewünschten Konten und spielen Sie diese nacheinander ein.

3.21.2.3 Überarbeitetes Lizenz-Menü

Ab sofort lassen sich hier alle Arten von Lizenzschlüsseln anzeigen und ändern (Basissystem, Virenscanner, URL-Filter, Apps).

© 2022 XnetSolutions KG

3.21.2.4 Nicht mehr unterstützte Funktionen

- McAfee Virenscanner
- LDAP-Server für LDAP-Adressbuch
- IMAP/Webmail-Zugriff des admin-Benutzers auf Dateianhangs- und Virenquarantäne
- Löschen und Bearbeiten von Postfächern

© 2022 XnetSolutions KG

3.21.3 Bugfix

3.21.3.1 Fehlerhaftes Routing bei IPsec-Tunneln mit SNAT

In seltenen Fällen ist es notwendig, die lokale Absender-Adresse per SNAT zu verändern, bevor eine Verbindung über einen IPsec-Tunnel geleitet wird. Manuell konfigurierte Routen erhielten in diesen Konstellationen Vorrang, so dass die eigentlich für IPsec bestimmten Verbindungen möglicherweise falsch geroutet wurden.

© 2022 XnetSolutions KG

3.21.4 Funktionen aus Version 7.0 die in Version 7.1 für alle Systeme verfügbar sind

3.21.4.1 Neu

3.21.4.1.1 Bridging

Ethernet-, VLAN- und WLAN-Schnittstellen können in einer Bridge zusammengeschaltet werden. Für Verbindungen innerhalb der Bridge und für Verbindungen aus der Bridge heraus erfolgt dabei die Firewall-Konfiguration individuell je Port. Somit ist auch der Betrieb als transparente Firewall zwischen zwei Netzwerk-Segmenten möglich (z.B. zwischen LAN und Router). Für Verbindungen in eine Bridge hinein ist die Firewall-Konfiguration lediglich je Bridge, nicht aber je Port möglich.

3.21.4.1.2 Bündelung von Netzw erkkarten

Netzwerkkarten lassen sich nun Bündeln um eine redundante Verbindung mit Switches herzustellen oder den Durchsatz zu erhöhen.

3.21.4.1.3 URL-Filter Meldung beim Aufbrechen von SSL-Verbindungen

Beim Aufbrechen von SSL-Verbindungen im Web-Proxy wurde eine neue Option hinzugefügt, die die Darstellung von Sperr-Meldungen des URL-Filters betrifft. Ist eine Domain komplett gesperrt, hat der Proxy bisher schon den Verbindungsaufbau abgewiesen. Im Browser wurde daher nur eine allgemeine Fehlermeldung angezeigt, wonach der Proxy die Verbindung verweigert. Mit der neuen Option kann alternativ dazu der Verbindungsaufbau zunächst erlaubt werden, so dass dann die konkrete Sperr-Meldung des URL-Filters im Browser angezeigt wird.

3.21.4.1.4 Benutzerspezifische Meldung nach Anmeldung an Administrations-Oberfläche

In der Benutzerverwaltung kann bei Benutzern mit Zugriff auf die Administrations-Oberfläche (Gruppe "system-admin") eine Meldung hinterlegt werden, die jedesmal angezeigt wird, nachdem sich der Benutzer angemeldet hat.

3.21.4.1.5 Lesezugriff auf Administrationsoberfläche

Der "admin" kann jetzt Benutzern der Gruppe "system-admin" Leseberechtigung auf die wichtigsten Konfigurationsmenüs erteilen. So lässt sich beispielsweise ein Auditor-Zugang realisieren. Bisher konnte der "admin" anderen Benutzern nur den Vollzugriff auf einzelne Menüs erlauben.

3.21.4.1.6 URL-Filter Benutzergruppen aus Active-Directory

Der URL-Filter kann Benutzergruppen nun direkt aus dem Active-Directory auslesen. Voraussetzung ist ein Computer-Konto in der Windows-Domäne, wie es auch für die NTLM-Authentifizierung des Proxies erforderlich ist.

3.21.4.1.7 Zertifikate von Let's Encrypt

Ab sofort können Zertifikate automatisiert über das ACME-Protokoll aktualisiert werden, was die Nutzung von kostenlosen Let's Encrypt-Zertifikaten ermöglicht. Eine entsprechende Alternative steht im Menü "Schlüsselbund" beim Ausstellen neuer Zertifikate zur Verfügung. Die Authentifizierung erfolgt dabei über das Verfahren "http-01". Sie müssen dazu den Reverse-Proxy auf Port 80 aus dem Internet erreichbar machen, virtuelle Hosts für die gewünschten Domains anlegen und darin jeweils das vordefinierte Backend "ACME HTTP-Authorisierung" aktivieren.

© 2022 XnetSolutions KG

3.21.4.1.8 Avira Makro-Erkennung im Web-Proxy

In Kombination mit dem Avira Virenscanner lassen sich im Web-Proxy Content-Filter Office-Dokumente blockieren, wenn diese Makros oder Autostart-Makros enthalten.

3.21.4.1.9 Monitoring für SSH-TCP-Forwarding

Auf einem neuen Reiter im Menü "Monitoring > Netzwerk > Status" werden jetzt Verbindungen mit dem SSH-TCP-Forwarder angezeigt.

3.21.4.1.10 Protokollierung auf Syslog-Server

Der Inhalt der meisten Log-Dateien kann jetzt in Kopie auf einen Syslog-Server gesendet werden.

© 2022 XnetSolutions KG

Testmöglichkeit

Überzeugen Sie sich zwei Wochen lang von unseren Produkten und Leistungen – ganz ohne Verpflichtung und völlig kostenfrei.

Kompetente Beratung

Oft ist die gewünschte Lösung einfacher und effizienter zu realisieren als erwartet.
Sprechen Sie mit uns über Ihre Anforderungen.
Gemeinsam finden wir den richtigen Weg.

Erreichbarkeit

Ihren persönlichen Ansprechpartner erreichen Sie ohne Umwege über seine direkte Durchwahl.

Vorabaustausch

Im Falle einer Störung senden wir Ihnen umgehend vorab ein vorinstalliertes und voll funktionstüchtiges Gerät zu.

Hotline

Bei allen technischen Fragen können Sie sich auf ein erfahrenes Support-Team verlassen.

XNETSOLUTIONS
cyber. security. systems

Benzstraße 32, 71083
Herrenberg/Germany
Telefon +49 (0) 7032 955 96-0
Telefax +49 (0) 7032 955 96-25
info@xnetsolutions.de
w w w .xnetsolutions.de