XnetSolutions

SX-GATE

Software Update
Release Note

Version: 6.0-3.0

Inhaltsverzeichnis

Teil I Wichtige Informationen ... 6

1 Technische Unterstützung ... 6
2 Vorbereitung ... 6
3 Installation ... 6

Teil II Änderungen in dieser Software-Version ... 9

1 Neue Funktionen ... 9
- Ablaufendes CA-Zertifikat im VPN-Server ... 9
- Benutzerdefinierte CA für Client-Zertifikate im Reverse-Proxy ... 9
- Eigene Reverse-Proxy Option für Exchange Admin Center ... 9

2 Änderungen ... 9
- E-Mail Benachrichtigungen überarbeitet ... 9
- E-Mail-Abwesenheitsschaltung mit Uhrzeit ... 9
- Proxy-Einstellungen für Downloads ... 9

3 Update ... 9
- IDS/IPS-Signaturen ... 9
- URL-Filter und kostenfreie URL-Datenbank ... 9
- F-Secure Virenscanner ... 10
- Neue IPSec-Server Version ... 10

Teil III Änderungen in vorherigen Versionen ... 11

1 Version 6.0-1.0 ... 11
- Neue Funktionen ... 11
  - Kostenpflichtiges Update ... 11
  - Neue Administrationsoberfläche ... 11
  - IP-Gruppen ... 12
  - Reverse-Proxy Zertifikate je Port ... 12
  - Administrations-Server Zertifikat ... 12
  - Verteilung ankommender Mails auf IMAP-Ordner ... 12
  - SNMPv3 Server ... 12
  - Erweiterte Konfigurationsmöglichkeiten für den Einsatz als OpenVPN Client ... 13
  - Konfigurierbare Proxy-Auto-Conf Datei ... 13
  - Benutzerdefinierte DHCP-Optionen im DHCP-Server ... 13
- Änderungen ... 14
  - Überarbeitete Firewall-Konfiguration ... 14
  - Komplett überarbeitete URL-Filter Konfiguration ... 14
  - Eingabeformat für IP-Netzwerken ... 14
  - IPSec Client-Verbindungen authentifiziert mit bestimmtem Zertifikat ... 15
- Behobene Fehler ... 16

2 Version 6.0-1.1 ... 17
- Neue Funktionen ... 17
  - Schachtelung von IP-Gruppen ... 17
  - Wake-on-LAN bei RAS-Verbindungen ... 17
- Änderungen ... 18
- Behobene Fehler ... 19
  - Backup und URL-Filter Konfiguration ... 19
  - Internet Explorer Fehlermeldung "no transport" ... 19

© 2014 XnetSolutions KG

Fehlermeldung beim Eintragen eines zeitgesteuerten Updates ... 19
3 Version 6.0-1.2 ... 20
Neue Funktion ... 20
DNS IP-Gruppen ... 20
Schachtelung von Protokollen ... 20
Status-Docklet ... 20
Änderungen ... 21
Behobene Fehler ... 22
Protokollspezifische Routing von Teilnetzen ... 22
Diverse Probleme beim Zugriff auf die Administrations-Oberfläche mit Internet Explorer 10 ... 22
4 Version 6.0-1.3 ... 23
Neue Funktionen ... 23
Änderungen ... 23
Behobene Fehler ... 23
Administrations-Oberfläche ... 23
IPSec-L2TP VPN mit Android 4.1/4.2 ... 23
Neustart des Masters im Cluster ... 23
SPAM-Filter Bewertung ... 23
Log-Datei Suche nach Datumsbereich ... 23
5 Version 6.0-1.4 ... 24
Neue Funktionen ... 24
SSH TCP-Forwarding ... 24
Zugriffsberechtigungen auf Docklets ... 24
Änderungen ... 25
IPSec Server ... 25
Web-Proxy Content-Filter ... 25
Cluster-Konfiguration ... 25
Administrations-Oberfläche ... 25
F-Secure Anti-Virus ... 25
Behobene Fehler ... 26
Routing-Tabelle ... 26
Live-Log ... 26
Administrations-Oberfläche ... 26
WoL - Wakeup on LAN ... 26
6 Version 6.0-1.5 ... 27
Neue Funktionen ... 27
Avira Antivirus for Appliance Server ... 27
Änderungen ... 27
Aktualisierung der Linux-Kernels ... 27
F-Secure Anti-Virus ... 27
Behobene Fehler ... 27
URL-Filter ... 27
7 Version 6.0-1.6 ... 28
Neue Funktionen ... 28
Empfänger für Administrator-Nachricht bei E-Mail-Filterung ... 28
Änderungen ... 28
F-Secure Anti-Virus ... 28
Aktualisierung des Name-Servers ... 28
Gültigkeitsdauer neuer Zertifikate ... 28
Behobene Fehler ... 28
8 Version 6.0-1.7 ... 29
Neue Funktionen ... 29
Änderungen ... 29
FTP-Zugriff für Benutzer mit E-Mail-Konto ... 29
IPSec-VPN und L2TP-Server ... 29
Behobene Fehler ... 29
Aktualisierung des Name-Servers ... 29

© 2014 XnetSolutions KG

Gestoppter NTP-Server ... 29
Diverse Darstellungsprobleme in der Administrations-Oberfläche ... 29
9 Version 6.0-1.8 ... 30
Neue Funktionen ... 30
Zusätzliche Option bei Verifikation von Mail-Empfängern am internen Mail-Server ... 30
Änderungen ... 30
Behobene Fehler ... 30
L2TP-Durchsatz ... 30
Umleitung der Startseite im Reverse-Proxy ... 30
10 Version 6.0-2.0 ... 31
Neue Funktionen ... 31
OpenVPN Zugriff nur für ausgewählte Zertifikate ... 31
Diensteüberwachung ... 31
Remotedesktop-Gateway über Reverse-Proxy ... 31
Änderungen ... 32
glibc System-Bibliothek ... 32
Cluster-Dienst ... 32
Verbesserte SSL/TLS-Sicherheit ... 32
Komplett überarbeitetes Logging ... 32
Reverse-Proxy ... 32
Web-Proxy und URL-Filter ... 32
Web-Proxy ... 32
Web-Proxy URL-Filter ... 32
Intrusion-Prevention und -Detection (IPS/IDS) ... 33
IPSec Schlüsseltausch-Intervalle jetzt frei einstellbar ... 33
Web-Server ... 33
Behobene Fehler ... 34
Reverse-Proxy Exchange Dienste ... 34
Möglicher Denial-of-Service gegen DNS-Server ... 34
11 Version 6.0-2.1 ... 35
Neue Funktionen ... 35
Netzwerke in Proxy-Autoconf-Datei ... 35
Erweiterung des Info-Docklets ... 35
Konfigurierbarer Sitzungs-Timeout ... 35
Änderungen ... 35
Zusätzliche Konfigurationsmöglichkeiten im ADSL-Zweig des Internet-Assistenten ... 35
Behobene Fehler ... 35
Anzeige von Logdateien ... 35
Transparenter Web-Proxy mit Content-Filter ... 35
12 Version 6.0-2.2 ... 36
Neue Funktionen ... 36
Änderungen ... 36
Behobene Fehler ... 36
Systemstart bei ADSL mit aktiviertem IPSec ... 36
URL für automatisches Backup ... 36
Anzeige von Logdateien ... 36
Reverse-Proxy Zugriff auf interne Server ... 36
13 Version 6.0-2.3 ... 37
Neue Funktionen ... 37
Zusätzliche Optionen bei der Zertifikatserstellung ... 37
Konfigurierbares Update-Intervall für DNS IP-Gruppen ... 37
Passwortgeschützte Dateien im Web-Proxy Content-Filter ... 37
Änderungen ... 37
Behobenen Fehler ... 37
Web-Proxy Content-Filter ... 37
Reverse-Proxy Syntax-Prüfung ... 37
POP-/IMAP-Client Duplikatserkennung bei Sammelpostfächern ... 37

© 2014 XnetSolutions KG

Ablauf der URL-Filter Lizenz ... 37
14 Version 6.0-2.4 ... 37
Neue Funktionen ... 38
Tooltip für Protokolle, IP- und Benutzer-Gruppen ... 38
Monitoring für OpenVPN Verbindungen ... 38
Maskieren von E-Mail Absender-Adressen ... 38
Änderungen ... 39
SecureUSB-Stick Konfiguration ... 39
Aktualisierungen ... 40
Avira Antivirus ... 40
Cluster Software ... 40
Behobene Fehler ... 41
OpenSSL Crypto-Bibliothek ... 41
Web-Proxy mit Digest-Authentifizierung ... 41
Reverse-Proxy Redirects ... 41
15 Version 6.0-2.5 ... 42
Neue Funktionen ... 42
E-Mail Domain-Routing an externen E-Mail-Server ... 42
Netzwerkkarten-Docklet ... 42
Änderungen ... 43
Überarbeitete Netzwerkkarten-Erkennung ... 43
Eingabe von Top-Level-Domains (TLD) ... 43
Aktualisierungen ... 44
Behobene Fehler ... 45
Web-Proxy Content-Filter ... 45
Provider-Relay mit Submission-Port und E-Mail-Routing ... 45
OpenVPN Installationspaket mit 64-Bit Client ... 45
POP3- und SMTP-Proxy ... 45
16 Version 6.0-2-6 ... 45
Neue Funktionen ... 45
Verschlüsselung für POP3-/SMTP-Proxy ... 45
Änderungen ... 45
Aktualisierungen ... 45
Secure-Shell Server ... 45
Behobene Fehler ... 45
17 Version 6.0-2.7 ... 46
Sicherheitskritisch ... 46
OpenSSL Crypto-Bibliothek ... 46
Neue Funktionen ... 46
Änderungen ... 46
Aktualisierungen ... 46
Behobene Fehler ... 46
18 Version 6.0-2-9 ... 47
Sicherheitskritisch ... 47
Aktualisierung des Linux-Kernels ... 47
OpenSSL Crypto-Bibliothek ... 47
POP/IMAP-Client Zustellung an lokale Postfächer ... 47
Neue Funktionen ... 47
Remotedesktop Web-Access über Reverse-Proxy ... 47
Behobene Fehler ... 47
E-Mailversand: TLS Handshake failed ... 47

© 2014 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 1024 MB (1GB)**

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:

© 2014 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.

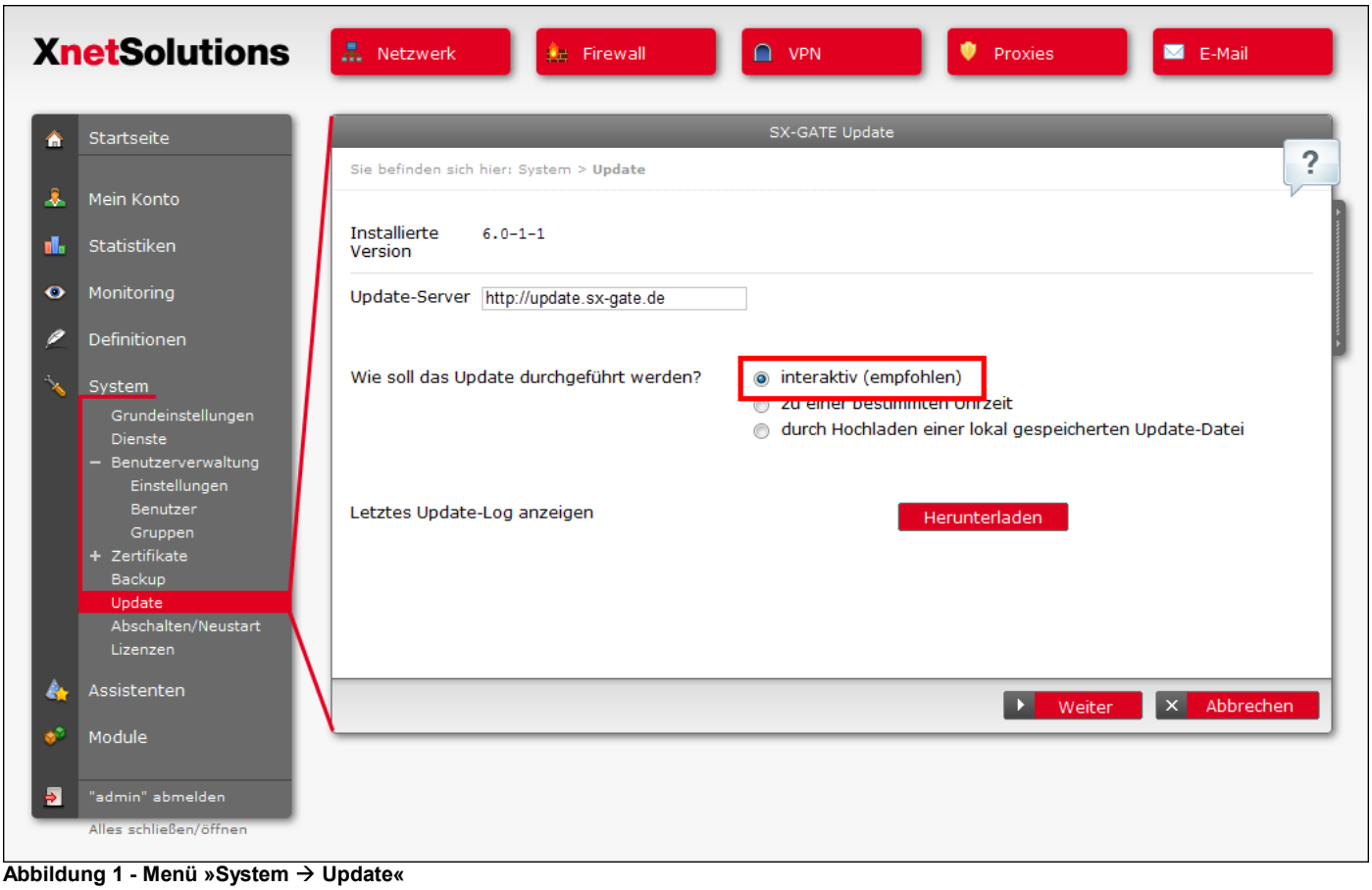

Abbildung 1 - Menü »System → Update«

- **Manuelles Software-Update**

Bevor Sie das Software-Update durchführen können ist es erforderlich, dass Sie das benötigte Software-Update Version 6.0-3.0 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.

© 2014 XnetSolutions KG

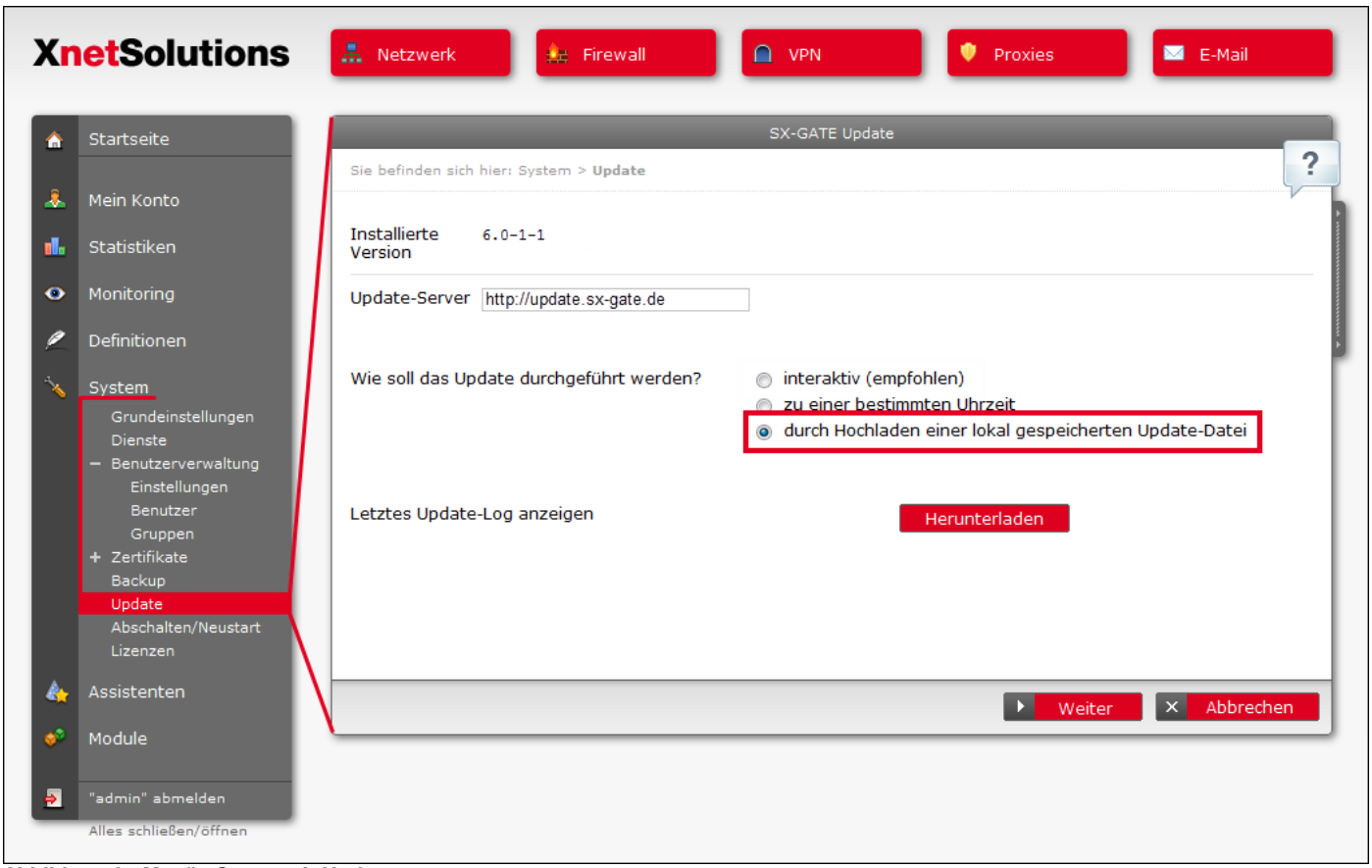

Abbildung 2 - Menü »System → Update«

Wichtig:

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

© 2014 XnetSolutions KG

2 Änderungen in dieser Software-Version

2.1 Neue Funktionen

2.1.1 Ablaufendes CA-Zertifikat im VPN-Server

Um bei Ablauf des CA-Zertifikats eine nahtlose Übergangsphase zu ermöglichen, wurde im IPSec- und OpenVPN-Server die Möglichkeit geschaffen, Zertifikate einer alten und neuen Version der selben CA zu akzeptieren.

2.1.2 Benutzerdefinierte CA für Client-Zertifikate im Reverse-Proxy

Bislang mussten die Client-Zertifikate grundsätzlich von der systemeigenen CA ausgestellt werden. Diese neue Möglichkeit kann auch dazu genutzt werden, bei nahendem Ablauf der systemeigenen CA für eine Übergangszeit Zertifikate der alten und der neuen CA zu akzeptieren.

2.1.3 Eigene Reverse-Proxy Option für Exchange Admin Center

Bisher wurde das Exchange Admin Center bzw. das Exchange Control Panel als Teil der OWA-Option freigegeben. Nun steht dafür ein separater Schalter zur Verfügung.

2.2 Änderungen

2.2.1 E-Mail Benachrichtigungen überarbeitet

2.2.2 E-Mail-Abwesenheitsschaltung mit Uhrzeit

Beim Zeitraum der E-Mail-Abwesenheitsschaltung kann zusätzlich zum Datum nun auch die genaue Uhrzeit angegeben werden.

2.2.3 Proxy-Einstellungen für Downloads

In einzelnen Installationen muss das System Downloads wie Virensignatur-Aktualisierungen oder Updates über einen Proxy abwickeln. Die Konfiguration dieses Proxies erfolgt nun zentral in den Grundeinstellungen.

2.3 Update

2.3.1 IDS/IPS-Signaturen

Bei Systemen mit Software-Pflegevertrag erfolgt die Aktualisierung täglich. Systeme ohne Pflegevertrag erhalten mit diesem Update neue Signaturen.

2.3.2 URL-Filter und kostenfreie URL-Datenbank

Neben der Software wird die einfache, integrierte URL-Filter Datenbank aktualisiert. Systemen mit der umfangreichen kostenpflichtigen URL-Datenbank erhalten tägliche Aktualisierungen.

© 2014 XnetSolutions KG

2.3.3 F-Secure Virenscanner

2.3.4 Neue IPSec-Server Version

Mit dem Wechsel auf die neue Version wurden einzelne unwichtige Optionen entfernt, andere hinzugefügt.

Neu hinzugekommen ist die Möglichkeit Client-Verbindungen mit XAuth und optionaler Zuweisung von IP-Adressen über ModeCfg zu konfigurieren. Damit lassen sich iOS-Geräten wie iPhone oder iPad nun auch per zertifikatsbasierter Authentifizierung anbinden. Die Konfiguration der iOS-Geräte kann bequem mit Hilfe einer Profildatei erfolgen.

Geändert hat sich mit der neuen Version das Verhalten in Bezug auf Datenkompression. Wurde bisher die Datenkompression automatisch aktiviert wenn die Gegenstelle dies wünschte, muss diese nun passend konfiguriert werden. Bei Installation des Updates wird versucht anhand der Log-Dateien festzustellen, ob bei den konfigurierten Server-Verbindungen bisher Komprimierung genutzt wurde und bei Bedarf die Option gesetzt.

© 2014 XnetSolutions KG

3 Änderungen in vorherigen Versionen

3.1 Version 6.0-1.0

3.1.1 Neue Funktionen

3.1.1.1 Kostenpflichtiges Update

Sie können das Update kostenfrei herunterladen, wenn ein Software-Updatevertrag 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 manuell 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.

3.1.1.2 Neue Administrationsoberfläche

Kernstück der Version 6.0 ist die vollständig überarbeitete Administrationsoberfläche. Neben dem frischen Design ist die konfigurierbare Startseite mit diversen Informations- und Statusfenstern die auffälligste Neuerung.

Neu ist auch das Live-Log, eine permanent aktualisierte Log-Datei Anzeige mit der Möglichkeit die Zeilen zu filtern. Bei ausreichend großem Browser-Fenster kann zudem die Hilfe permanent geöffnet bleiben und zeigt dabei immer die zur gerade aktuellen Bildschirmmaske passenden Texte an.

Für die aufwändigeren Funktionen wird ein moderner Browser mit aktiviertem JavaScript vorausgesetzt. Weitere Details zur Handhabung der neuen Funktionen finden Sie in der Hilfe zur »Startseite«. Um diese auf der neuen Administrations-Oberfläche aufzurufen, klicken Sie bitte in der Startseite auf eines der Fragezeichen-Symbole. Wählen Sie dann im Hilfe-Fenster die Zeile »Startseite» an.

Einige Hauptmenüs wurden umbenannt:

bis Version 5.2		**ab Version 6.0**
Menü »Home«	wird zu	Menü »Mein Konto«
Menü »Administration«	wird zu	Menü »System«
Menü »Konfiguration«	wird zu	Menü »Assistenten«
Menü »Expertenmodus«	wird zu	Menü »Module«

Folgende Hauptmenüpunkte sind neu:

Neu	
Monitoring	Statistiken und Netzwerkinformationen
Definitionen	Definition von Entitäten (IP-Adressgruppen, Protokolle, Zeiträume und URL-Filter Listen)

Die Statistiken aus dem Menü **»Monitoring«** sind nun unter einem **eigenen Hauptmenüpunkt** zusammengefasst.

Auch viele Untermenüs wurden umbenannt oder umstrukturiert. Die Auswahl oder das Anlegen von Entitäten erfolgt nicht mehr über den Menübaum sondern über Tabellen.

In der zusätzlichen Menüleiste am oberen Rand der Administrationsoberfläche finden Sie eine Zusammenstellung der

© 2014 XnetSolutions KG

Menüpunkte zu Kernkomponenten wie Firewall, Proxies und E-Mail. Sie erhalten so schnelleren Zugriff auf die Menüs zu einem bestimmten Thema.

Die Darstellung von Listen und Tabellen wurde komplett überarbeitet. Maximal werden zunächst nur 5 bzw. 10 Zeilen angezeigt. Gibt es mehr Einträge, erscheint am unteren rechten Rand der Liste eine zusätzliche Seitennavigation. Dort gibt es die Möglichkeit, die Liste in einer Vollbild-Darstellung mit allen Listenelementen zu öffnen. Hier ermöglicht es eine Filter-Funktion gezielt nur bestimmte Listenelemente anzuzeigen. Bei Tabellen in denen die Reihenfolge der Einträge eine Rolle spielt, lassen sich im Vollbild zudem Einträge bequem per Drag-and-Drop umsortieren.

In den Tabellen unterhalb des Menüs »Definitionen« wird sowohl die Beschreibung angezeigt und die Anzahl, wie oft das jeweilige Objekt verwendet wird. Objekte die in Verwendung sind können nicht gelöscht werden. Nach Auswahl eines Eintrags wird auf dem Reiter »Verwendung« eine Liste mit Links auf die Menüpunkte angezeigt, in denen das Objekt verwendet wird.

In den Konfigurationsmasken eines Dienstes der noch nicht gestartet wurde, wird eine entsprechende Warnmeldung eingeblendet. Zukünftig sollen derartige Warnmeldungen auch auf andere potentielle Probleme hinweisen.

3.1.1.3 IP-Gruppen

Im neuen Hauptmenü »Definitionen« lassen sich IP-Gruppen definieren. Jede Gruppe repräsentiert eine oder mehrere IP-Adressen bzw. Netzwerke. In vielen IP-Listen lassen sich alternativ zur direkten Eingabe von IP-Adressen oder Netzwerken nun auch IP-Gruppen auswählen.

Die ehemalige Liste der lokalen IP-Subnetze aus dem Menü »Administration -> Grundeinstellungen«, die standardmäßig von vielen Diensten genutzt wird, wurde zur vordefinierten IP-Gruppe »INTRANET«.

3.1.1.4 Reverse-Proxy Zertifikate je Port

Im Reverse-Proxy kann nun für jeden HTTPS-Port ein eigenes Server-Zertifikat hinterlegt werden. Damit ist es ggf. nicht mehr erforderlich, ein Wildcard- oder Multi-Domain-Zertifikat zu erwerben. Die Masken zum Erstellen, Importieren und Exportieren der Zertifikate finden sie nun in der Port-Konfiguration des Reverse-Proxies.

3.1.1.5 Administrations-Server Zertifikat

Das HTTPS-Zertifikat für die Administrations-Oberfläche kann nun ebenfalls bei einer externen CA beantragt werden. Sofern aus dem Internet auf die Administrations-Oberfläche zugegriffen werden soll, empfehlen wir jedoch die Verwendung des Reverse-Proxies. Dieser kann den Zugriff auf Teilbereiche (wie z.B. Webmail) einschränken oder über Client-Zertifikate eine stärkere Authentifizierung verlangen. Die Masken zum Erstellen, Importieren und Exportieren der Zertifikate finden sie nun im Menü »System -> Grundeinstellungen«.

3.1.1.6 Verteilung ankommender Mails auf IMAP-Ordner

Bei Benutzer-Postfächern ist es nun möglich, basierend auf Informationen aus den Kopfzeilen ankommender E-Mails gleich in IMAP-Ordner einzusortieren.

3.1.1.7 SNMPv3 Server

Diverse Status-Informationen lassen sich nun per SNMP abfragen. Die Konfiguration erfolgt im Menü »Monitoring -> Netzwerk«.

Hinweis:

Diese Funktion konnten bereits in der Software Version 5.2 auf Systemen mit Software-Pflegevertrag genutzt werden. In Software Version 6.0 ist diese Funktionen auf allen Systemen verfügbar.

© 2014 XnetSolutions KG

3.1.1.8 Erweiterte Konfigurationsmöglichkeiten für den Einsatz als OpenVPN Client

In OpenVPN Client-Schnittstellen lässt sich nun verbindungsspezifisches Schlüsselmaterial hinterlegen. Bisher wurden stets die Zertifikate und der Schlüssel verwendet, die auch für OpenVPN Server- und IPSec-Verbindungen genutzt werden.

Beim Import von verbindungsspezifischem Schlüsselmaterial werden neben dem PKCS#12-Format auch Installationspakete für Windows-Clients und OpenVPN-Konfigurationsdateien mit eingebetteten Schlüsseln unterstützt. Die Einstellungen der OpenVPN Client-Schnittstelle lassen sich dabei gleich an die im Installationspaket bzw. der Konfigurationsdatei gefundenen Werte anpassen, was die Konfiguration von OpenVPN Client-Verbindungen deutlich erleichtert.

Um die Kompatibilität mit OpenVPN-Servern Dritter zu erhöhen, wurden Eingabefelder für die OpenVPN-Parameter »tls-auth«, »keydir« und »comp-lzo« hinzugefügt.

Hinweis:

Diese Funktion konnten bereits in der Software Version 5.2 auf Systemen mit Software-Pflegevertrag genutzt werden. In Software Version 6.0 ist diese Funktionen auf allen Systemen verfügbar.

3.1.1.9 Konfigurierbare Proxy-Auto-Conf Datei

Die bislang fest vorgegebene PAC-Datei lässt sich nun um beliebige Domains bzw. Adressen erweitern, auf die Browser direkt bzw. über Proxy zugreifen sollen.

Hinweis:

Diese Funktion konnten bereits in der Software Version 5.2 auf Systemen mit Software-Pflegevertrag genutzt werden. In Software Version 6.0 ist diese Funktionen auf allen Systemen verfügbar.

3.1.1.10 Benutzerdefinierte DHCP-Optionen im DHCP-Server

Hinweis:

Diese Funktion konnten bereits in der Software Version 5.2 auf Systemen mit Software-Pflegevertrag genutzt werden. In Software Version 6.0 ist diese Funktionen auf allen Systemen verfügbar.

© 2014 XnetSolutions KG

3.1.2 Änderungen

3.1.2.1 Überarbeitete Firewall-Konfiguration

Der erste Konfigurations-Reiter fasst die Firewall-Grundkonfiguration der jeweiligen Schnittstelle kurz zusammen:

Besteht für ein- bzw. ausgehende Verbindungen standardmäßig Vollzugriff?
Wie sieht es bei Weiterleitungen aus?

Je Quell-Zone ist angegeben ob Regeln erforderlich sind oder Vollzugriff besteht und ob NAT angewandt wird.

Für Weiterleitungs-Regeln standen bisher fünf Tabellen zur Verfügung - je eine für die vier Quell-Zonen sowie eine für zonenunabhängige Weiterleitungen. Zukünftig gibt es nur noch eine Tabelle. Die Quell-Zone kann darin je Regel festgelegt werden.

Die neue tabellarische Darstellung des Regelwerks, zusammen mit der Möglichkeit, IP-Gruppen zu definieren, erhöht die Übersichtlichkeit. Nutzen Sie bei umfangreichen Regelwerken die Vollbild-Darstellung.
Protokolle und Zeiträume werden wie die IP-Gruppen im neuen Hauptmenü »Definitionen« festgelegt.

3.1.2.2 Komplett überarbeitete URL-Filter Konfiguration

Die ehemaligen Proxylisten sind nun im Menü »Definitionen -> URL-Filter Listen« zu finden.

Im Gegensatz zu früher wird auch nicht mehr innerhalb der Liste festgelegt, was gesperrt und was freigegeben wird. Jede Liste besteht nur noch aus einer einzigen benutzerdefinierten Domain-Liste, einer Liste von Dateinamenserweiterungen sowie allen verfügbaren URL-Datenbank Kategorien und weiteren Optionen.

Statt in der Benutzerverwaltung wird nun im neuen Menü »Module -> Web-Proxy -> URL-Filter« festgelegt, wie mit Anfragen zu verfahren ist. Eine Tabelle mit Regeln wird sequentiell bis zum ersten Treffer durchlaufen. Vorbedingungen entscheiden, ob die Regel überhaupt geprüft wird. Hier gibt es die bekannten Möglichkeiten, bestimmte Regeln nur während oder außerhalb der Arbeitszeiten zu aktivieren und Regeln an Benutzergruppen zu binden.

Neu ist die Möglichkeit, Regeln für einzelne Client IP-Adressen, Netzwerke oder IP-Gruppen zu definieren. So ist nun auch bei Installationen ohne Proxy-Authentifizierung eine differenzierte Konfiguration möglich. Bei jeder Regel wird schließlich festgelegt, ob der Zugriff erlaubt oder verweigert wird, wenn die angefragte Adresse in der verknüpften URL-Filter Liste enthalten ist.

Die Konfiguration von bestehenden Systemen wird automatisch migriert. Dabei kann es vorkommen, dass eine alte Proxyliste in mehrere neue URL-Filter Listen aufgeteilt wird. Wir empfehlen, die Konfiguration nach dem Update zu prüfen und ggf. zu vereinfachen.

Die URL-Filter Konfiguration ist vom Benutzer- in das System-Backup gewechselt. Auf Cluster-Systemen werden Änderungen in der URL-Filter Konfiguration auf dem Backup-Knoten solange nicht auf dem Master übernommen, bis auch der Backup-Knoten auf die neue URL-Filter Konfiguration aktualisiert wurde.

3.1.2.3 Eingabeformat für IP-Netzwerken

Anstelle zweier separater Eingabefelder für Netzwerk-Adresse und zugehöriger Netzmaske (z.B. »192.0.2.0« und »255.255.255.0«) erfolgt die Eingabe nun in einem Eingabefeld, mit Schrägstrich getrennt.

Die Netzmaske wird in Form des kürzen Suffixes angegeben (im Beispiel »192.0.2.0/24«). Bei aktiviertem JavaScript kann die Netzmaske auch in herkömmlicher Form eingegeben werden (also »192.0.2.0/255.255.255.0«). Die Eingabe wird dann automatisch konvertiert.

Fehleingaben wie z.B. »192.0.2.1/24« (die ».1« wird durch die Netzmaske ausgeblendet) werden bei aktiviertem JavaScript nicht mehr akzeptiert. Sofern beim Update auf diese Version derartige Fehleingaben erkannt werden, wird die Netzmaske entfernt, der Eintrag also zu »192.0.2.1«. Im Update-Log sowie per Mail an den Administrator wird auf die Konvertierung hingewiesen.

© 2014 XnetSolutions KG

3.1.2.4 IPSec Client-Verbindungen authentifiziert mit bestimmtem Zertifikat

Normalerweise werden IPSec Clients authentifiziert indem überprüft wird, ob deren Zertifikate von der vertrauenswürdigen CA ausgestellt wurden. Für diese Installationen hat sich nichts geändert. Die Änderung betrifft Systeme, bei denen Clients über individuelle Zertifikate (in der Regel von externen CAs) authentifiziert werden. War es bisher möglich, in einer IPSec-L2tp- oder IPSec-Client-Verbindung beliebig viele Zertifikate zu hinterlegen, muss nun für jeden Client eine eigene Verbindung angelegt werden.

© 2014 XnetSolutions KG

3.1.3 Behobene Fehler

keine

© 2014 XnetSolutions KG

3.2 Version 6.0-1.1

3.2.1 Neue Funktionen

3.2.1.1 Schachtelung von IP-Gruppen

Einer IP-Gruppe können nun auch andere IP-Gruppen hinzugefügt werden.

3.2.1.2 Wake-on-LAN bei RAS-Verbindungen

Bei Verbindungsaufbau über IPSec-L2TP VPN, ISDN- oder Modem-Einwahl kann benutzerabhängig ein Rechner per Wake-on-LAN geweckt werden.

© 2014 XnetSolutions KG

3.2.2 Änderungen

keine

© 2014 XnetSolutions KG

3.2.3 Behobene Fehler

3.2.3.1 Backup und URL-Filter Konfiguration

Beim Einspielen eines Backups von Version 5.x auf einem System mit Version 6.0-1.0 ging die URL-Filter Konfiguration verloren. Systeme, die nach dem 25. Oktober 2012 auf Version 6.0-1.0 aktualisiert wurden, sind nicht betroffen.

3.2.3.2 Internet Explorer Fehlermeldung "no transport"

Diese Fehlermeldung wird unter Version 6.0-1.0 in der Administrationsoberfläche angezeigt, wenn sich der Seiteninhalt automatisch aktualisieren sollte. Systeme, die nach dem 25. Oktober 2012 auf Version 6.0-1.0 aktualisiert wurden, sind nicht betroffen.

Auch beim Einspielen des Updates wird der Seiteninhalt regelmäßig aktualisiert. Tritt der Fehler auf, kann der Fortschritt des Updates nicht beobachtet werden. Das Update läuft dennoch problemlos weiter.

3.2.3.3 Fehlermeldung beim Eintragen eines zeitgesteuerten Updates

In Version 6.0-1.0 wird beim Einplanen eines Update zu einer bestimmten Uhrzeit ein Fehler gemeldet. Das Update findet dennoch zur gewünschten Zeit statt.

© 2014 XnetSolutions KG

3.3 Version 6.0-1.2

3.3.1 Neue Funktion

3.3.1.1 DNS IP-Gruppen

Eine IP-Gruppe kann nun auch einen DNS-Eintrag repräsentieren. Der Name der IP-Gruppe wird in diesem Fall täglich im DNS aufgelöst und die erhaltenen IP-Adressen in der IP-Gruppe eingetragen.

3.3.1.2 Schachtelung von Protokollen

Einem Protokoll können nun auch andere Protokolle hinzugefügt werden.

3.3.1.3 Status-Docklet

Der kurze Systemcheck, der in Version vor 6.0 im Menü »Home -> System-Status« durchgeführt wurde, ist nun wieder verfügbar. Das neue Status-Docklet führt den Test alle 10 Minuten durch.
Falls das Docklet nicht automatisch erscheint, können Sie es über das Werkzeug-Symbol in der rechten oberen Ecke der Administrations-Oberfläche aktivieren.

© 2014 XnetSolutions KG

3.3.2 Änderungen

keine

© 2014 XnetSolutions KG

3.3.3 Behobene Fehler

3.3.3.1 Protokollspezifische Routing von Teilnetzen

In den bisherigen 6.0 Versionen funktionierten protokollspezifische Routen nicht, wenn als Quelle oder Ziel ein Teilnetz angegeben war. Routen ohne Protokollangabe sowie Routen für einzelne oder beliebige IP-Adressen waren nicht betroffen.

3.3.3.2 Diverse Probleme beim Zugriff auf die Administrations-Oberfläche mit Internet Explorer 10

© 2014 XnetSolutions KG

3.4 Version 6.0-1.3

3.4.1 Neue Funktionen

keine

3.4.2 Änderungen

keine

3.4.3 Behobene Fehler

3.4.3.1 Administrations-Oberfläche

Das Öffnen von Docklets in einem separaten Browser-Fenster funktionierte bislang nicht. In 6.0-1.2 verschwand außerdem das Menü, wenn in der Vollbild-Ansicht einer Tabelle Schaltflächen angeklickt wurden.

3.4.3.2 IPSec-L2TP VPN mit Android 4.1/4.2

Bei manchen Geräten gab es Probleme mit dem Verbindungsaufbau.

3.4.3.3 Neustart des Masters im Cluster

Abhängig von der Netzwerkkonfiguration wurde bei einzelnen Installationen der Netzwerkkarten-Status nach einem Neustart des Master-Knotens nicht korrekt erkannt. Der Master blieb daraufhin im Fehler-Status.

3.4.3.4 SPAM-Filter Bewertung

Verbindungen von Mail-Servern aus erst vor kurzem vergebenen IP-Netzen wurden fälschlicherweise noch wegen Nutzung unzulässiger IP-Bereiche bewertet.

3.4.3.5 Log-Datei Suche nach Datumsbereich

In den erweiterten Optionen der Log-Datei Suche funktionierte seit 5.2-3.0 die Suche in einem Datumsbereich nicht mehr.

© 2014 XnetSolutions KG

3.5 Version 6.0-1.4

3.5.1 Neue Funktionen

3.5.1.1 SSH TCP-Forwarding

Mit SSH TCP-Forwarding steht eine einfachere Variante des gesicherten Fernzugriffs für Clients zur Verfügung. In dieser Variante kann auf bequeme Weise mit einem speziell gesicherten USB-Stick eine gesicherte RDP-Verbindung zur Verfügung gestellt werden.

3.5.1.2 Zugriffsberechtigungen auf Docklets

Der Zugriff auf die Info- und Statusfenster der Startseite muss jetzt in der Benutzerverwaltung individuell freigegeben werden.

© 2014 XnetSolutions KG

3.5.2 Änderungen

3.5.2.1 IPSec Server

Die neue Version beseitigt Inkompatibilitäten mit MacOS 10.8 und iOS 6.0 bis 6.0.2 und implementiert eine Methode um Probleme mit Routern zu umgehen, die fragmentierte Pakete nicht verarbeiten können.

3.5.2.2 Web-Proxy Content-Filter

Statusmeldungen während des Virenscanns werden nur noch ausgegeben, wenn als Client ein normaler Web-Browser identifiziert wird. Probleme mit Update-Programmen, die mit Statusmeldungen nicht umgehen können, sollen so vermieden werden. Ein Eintrag als "vertrauenswürdiger Server" ist dann nicht mehr notwendig.

3.5.2.3 Cluster-Konfiguration

Um Einrichtung und Pflege eines Clusters zu erleichtern, werden nun auch Zertifikate und private Schlüssel vom Backup an den Master übertragen. Sollten auf den beiden Cluster-Knoten individuell verschiedene Schlüssel installiert sein, werden diese bei der nächsten Synchronisation überschrieben!

Dies beinhaltet:

- das Zertifikat der CA
- Privater Schlüssel und Zertifikat des VPN-Servers
- Privater Schlüssel und Zertifikat des E-Mail-Servers
- Privater Schlüssel und Zertifikat des Reverse-Proxy

Bei den genannten Server-Diensten sind selbstsignierte Zertifikate jedoch ausgenommen.

Grundsätzlich nicht kopiert werden:

- der private Schlüssel der CA
- Privater Schlüssel und Zertifikat der SSL-Proxy CA
- Privater Schlüssel und Zertifikat des Administrations-Servers

Das Menü des Master-Knotens ist normalerweise stark eingeschränkt. Für temporäre Änderungen lässt sich jetzt für die Dauer der aktuellen Sitzung Vollzugriff freischalten. Das Update beseitigt zusätzlich ein Problem beim Installieren des Backup-Schlüssels im Master. Bei Neugeräten werden längere Schlüssel verwendet, die beim Hochladen nicht akzeptiert wurden.

3.5.2.4 Administrations-Oberfläche

Bei noch nicht übernommenen Änderungen wird der Benutzer gewarnt. Ferner wurde das Sitzungs-Timeout auf 15 Minuten verlängert.

3.5.2.5 F-Secure Anti-Virus

Aktualisierung des F-Secure Virenscanners.

© 2014 XnetSolutions KG

3.5.3 Behobene Fehler

3.5.3.1 Routing-Tabelle

Bei Routing-Einträgen für einzelne Protokolle wurde im Menü "Monitoring" der falsche Protokoll-Name angezeigt.

3.5.3.2 Live-Log

Ein Teil der Log-Dateien wurde im Live-Log nicht angezeigt, wenn der Hostname einen Bindestrich enthält.

3.5.3.3 Administrations-Oberfläche

Administrations-Oberfläche gestoppt nach Änderung des Zertifikats oder Neustart des Dienstes.

3.5.3.4 WoL - Wakeup on LAN

WoL bei Benutzereinwahl funktionierte nicht.

© 2014 XnetSolutions KG

3.6 Version 6.0-1.5

3.6.1 Neue Funktionen

3.6.1.1 Avira Antivirus for Appliance Server

SX-GATE unterstützt ab dem 01. April 2013, neben den bereits vorhandenen Virenscannern von F-Secure und Kaspersky, Avira Antivirus for Appliance Server. Die entsprechenden Lizenzen ab April 2013 bestellbar.

3.6.2 Änderungen

3.6.2.1 Aktualisierung der Linux-Kernels

Nach dem Update führt das System automatisch einen Neustart durch. Bitte starten Sie das System nicht von Hand neu.

3.6.2.2 F-Secure Anti-Virus

Aktualisierung des F-Secure-Virenscanners.

3.6.3 Behobene Fehler

3.6.3.1 URL-Filter

URL-Filter-Regeln für einzelne Client-Adressen funktionierten nicht, wenn die IP-Adresse ohne Netzmaske "/32" angegeben war.

Seit Softwareversion 6.0-1-0 wurde zudem der Grund für die Sperrung nicht mehr angezeigt, wenn detaillierte »Zugriff verweigert«-Meldungen eingestellt sind. Ebenfalls seit Softwareversion 6.0-1-0 funktionierte bei Neugeräten der Download der kommerziellen URL-Filter-Datenbank nicht. Geräte bei denen die Zugangsdaten vor dem Update auf Softwareversion 6.0-1-0 eingetragen wurden, waren nicht betroffen.

© 2014 XnetSolutions KG

3.7 Version 6.0-1.6

3.7.1 Neue Funktionen

3.7.1.1 Empfänger für Administrator-Nachricht bei E-Mail-Filterung

E-Mail-Benachrichtigungen bei Virenfund in E-Mails und bei gefilterten E-Mail-Anhängen können nun an eine benutzerdefinierte Adresse gesendet werden.

3.7.2 Änderungen

3.7.2.1 F-Secure Anti-Virus

Das Update behebt sporadisch auftretende falsch gesetzte Zugriffsrechte nach Signatur-Updates.

3.7.2.2 Aktualisierung des Name-Servers

Die neue Version behebt eine mögliche Denial-of-Service Schwachstelle.

3.7.2.3 Gültigkeitsdauer neuer Zertifikate

Neue CA-Zertifikate sind ab sofort 20 Jahre gültig, von der CA ausgestellte Zertifikate bis zu 6 Jahre.

3.7.3 Behobene Fehler

keine

© 2014 XnetSolutions KG

3.8 Version 6.0-1.7

3.8.1 Neue Funktionen

keine

3.8.2 Änderungen

3.8.2.1 FTP-Zugriff für Benutzer mit E-Mail-Konto

Seit Version 5.2-3.0 war es Mitgliedern der Gruppe »system-mail« möglich, sich am FTP-Server anzumelden, wenn alle der nachfolgenden Randbedingungen erfüllt waren:
Der FTP-Server ist aktiv, die Firewall-Konfiguration erlaubt den Zugriff und in der FTP-Server Konfiguration ist der »Zugriff für admin« für die IP-Adresse des Clients freigegeben.

3.8.2.2 IPSec-VPN und L2TP-Server

Update des IPSec-VPN und L2TP-Server

3.8.3 Behobene Fehler

3.8.3.1 Aktualisierung des Name-Servers

Die neue Version behebt eine mögliche Denial-of-Service Schwachstelle.

3.8.3.2 Gestoppter NTP-Server

Auf Systemen mit DHCP-Schnittstellen (Kabelmodem) oder IDS-Paketmonitor-Schnittstellen konnte vorkommen, dass sich der NTP-Server nicht starten lässt.

3.8.3.3 Diverse Darstellungsprobleme in der Administrations-Oberfläche

Diverse Darstellungsprobleme in der Administrations-Oberfläche behoben

© 2014 XnetSolutions KG

3.9 Version 6.0-1.8

3.9.1 Neue Funktionen

3.9.1.1 Zusätzliche Option bei Verifikation von Mail-Empfängern am internen Mail-Server

In der neuen Einstellungen werden Mails ohne Verifikation angenommen und in der lokalen Warteschlange vorgehalten, wenn der interne Mail-Server vorübergehend nicht verfügbar ist.

In dieser Versionsreihe nur auf Systemen mit Software Pflegevertrag verfügbar.

3.9.2 Änderungen

keine

3.9.3 Behobene Fehler

3.9.3.1 L2TP-Durchsatz

Mit dem in der vorherigen Version 6.0-1.7 aktualisierte L2TP-Server war der Durchsatz deutlich eingeschränkt.

3.9.3.2 Umleitung der Startseite im Reverse-Proxy

Unterschiedliche Umleitungsziele je nach Hostname funktionierten bislang nicht. Ferner stand die Option in Version 6.0 fälschlicherweise nur Pflegevertragskunden zur Verfügung.

© 2014 XnetSolutions KG

3.10 Version 6.0-2.0

3.10.1 Neue Funktionen

3.10.1.1 OpenVPN Zugriff nur für ausgewählte Zertifikate

Bisher konnte konnte sich jeder OpenVPN-Client mit einem Zertifikat der konfigurierten VPN-CA eine Verbindung zu allen OpenVPN-Server Schnittstellen aufbauen. Eine neue Option ermöglicht es nun, dies je OpenVPN-Server Schnittstelle auf einzelne Zertifikate einzuschränken.

3.10.1.2 Diensteüberwachung

Dabei werden die wichtigsten Dienste überwacht und bei Ausfall automatisch neu gestartet. Bei wiederholtem Ausfall wird auf Cluster-Systemen ein Failover ausgelöst.

3.10.1.3 Remotedesktop-Gateway über Reverse-Proxy

Eine neue Option erlaubt den Zugriff auf Remotedesktop-Gateway-Server.

© 2014 XnetSolutions KG

3.10.2 Änderungen

3.10.2.1 glibc System-Bibliothek

Das Update beseitigt eine Schwachstelle in der glibc-Bibliothek, die von nahezu allen Anwendungen genutzt wird. Nach dem Update führt das System automatisch einen Neustart durch. Bitte starten Sie das System nicht von Hand neu.

3.10.2.2 Cluster-Dienst

Die neue Version des Cluster-Dienstes ist für den neuen Failover bei Ausfall eines Dienstes erforderlich.

Nach dem Update eines Master-Knotens bleibt der Dienst gestoppt, da neue und alte Version der Cluster-Software nicht kompatibel zueinander sind. Bitte aktualisieren Sie zeitnah den Backup-Knoten. Starten Sie dann im Menü »System > Dienste« den Dienst »Cluster-Knoten«.

Sollte eine zeitnahe Aktualisierung des Backup-Knotens nicht möglich sein, können Sie den Dienst »Cluster-Knoten« auch auf dem Backup-System stoppen und auf dem Master reaktivieren.

3.10.2.3 Verbesserte SSL/TLS-Sicherheit

Durch ein Update diverser System-Bibliotheken und Dienste wird die Sicherheit von SSL/TLS-Verbindungen erhöht. Insbesondere wird TLS 1.2 nachgerüstet.

3.10.2.4 Komplett überarbeitetes Logging

Neue Such-Masken ermöglichen ein bequemes Filtern und herunterladen.

Auch die Aufteilung der Meldungen auf die verschiedenen Log-Dateien wurde verbessert. Alle wichtigen Komponenten verfügen nun über eine eigene Log-Datei. Insbesondere Firewall- und IPSec-Meldungen werden nun in eigene Logs geschrieben. Sofern Logs extern archiviert werden, müssen Sie die Konfiguration ggf. darauf anpassen.

3.10.2.5 Reverse-Proxy

Die neue Version ist auf weitestgehende Nutzung von Perfect-Forward-Secrecy bei verschlüsselten Verbindungen getrimmt.

3.10.2.6 Web-Proxy und URL-Filter

Die neue Version unterstützt nun durchgängig HTTP/1.1. Transparente Web-Proxy-Zugriffe erfolgen nun über den dedizierten Port 8082.

3.10.2.7 Web-Proxy

Die neue Version unterstützt nun durchgängig HTTP/1.1. Transparente Web-Proxy-Zugriffe erfolgen nun über den dedizierten Port 8082.

3.10.2.8 Web-Proxy URL-Filter

Sowohl die URL-Filter Software als auch die integrierte URL-Filter Datenbank wird aktualisiert.

© 2014 XnetSolutions KG

3.10.2.9 Intrusion-Prevention und -Detection (IPS/IDS)

Neben der Software werden auch die Signaturen auf allen Systemen aktualisiert.

3.10.2.10 IPSec Schlüsseltausch-Intervalle jetzt frei einstellbar

3.10.2.11 Web-Server

© 2014 XnetSolutions KG

3.10.3 Behobene Fehler

3.10.3.1 Reverse-Proxy Exchange Dienste

Die URL-Prüfung für OutlookAnywhere Zugriff wurde an Microsoft Exchange 2013 angepasst. Die Verbindungs-Timeouts für ActiveSync und OutlookAnywhere wurden erhöht.

3.10.3.2 Möglicher Denial-of-Service gegen DNS-Server

© 2014 XnetSolutions KG

3.11 Version 6.0-2.1

3.11.1 Neue Funktionen

3.11.1.1 Netzwerke in Proxy-Autoconf-Datei

In der Proxy-Autoconf-Datei lassen sich nun auch IP-Netzwerke eintragen, auf die ohne Proxy zugegriffen werden soll. Auch IP-Gruppen werden unterstützt.

3.11.1.2 Erweiterung des Info-Docklets

Es werden nun zusätzlich Informationen zu den IDS-/IPS-Signaturen und, sofern lizensiert, zur kommerziell gepflegte URL-Filter Datenbank angezeigt. Falls Fallback für die Internet-Schnittstelle aktiviert ist, werden ferner die Namen der Fallback-Schnittstelle sowie der aktuell aktiven Internet-Schnittstelle angezeigt.

3.11.1.3 Konfigurierbarer Sitzungs-Timeout

Auf vielfachen Wunsch lässt sich der Sitzungs-Timeout jetzt auf dem Anmelde-Bildschirm einstellen.

3.11.2 Änderungen

3.11.2.1 Zusätzliche Konfigurationsmöglichkeiten im ADSL-Zweig des Internet-Assistenten

3.11.3 Behobene Fehler

3.11.3.1 Anzeige von Logdateien

Mit dem Update werden einzelne Darstellungsfehler beseitigt sowie die Anzeigegeschwindigkeit erhöht.

3.11.3.2 Transparenter Web-Proxy mit Content-Filter

In Version 6.0-2.0 funktionierte der transparente Web-Proxy in Kombination mit dem Content-Filter nicht mehr.

© 2014 XnetSolutions KG

3.12 Version 6.0-2.2

3.12.1 Neue Funktionen

keine

3.12.2 Änderungen

keine

3.12.3 Behobene Fehler

3.12.3.1 Systemstart bei ADSL mit aktiviertem IPSec

Systeme die vor dem 23.11.2013 auf 6.0-2.0 aktualisiert wurden, konnten beim Systemstart hängen bleiben, wenn die Internetanbindung über ADSL erfolgt und der IPSec-Dienst aktiviert ist.

3.12.3.2 URL für automatisches Backup

Auf Systemen die vor dem 23.11.2013 auf Version 6.0-2.0 aktualisiert wurden, sind die URLs für das automatisch Backup z.T. falsch konvertiert worden. Betroffen sind URLs die mehr als eine Datumsvariable enthalten sowie FTP-URLs ohne Zugangsdaten (anonymes FTP). Die Fehler werden mit diesem Update behoben. Kontrollieren Sie trotzdem sicherheitshalber ob die Backups ordnungsgemäß erstellt werden.

3.12.3.3 Anzeige von Logdateien

Der Zugriff auf die Log-Datei Suche war über Reverse-Proxy und bei deaktiverten Cookies nicht möglich. Mit dem Update werden ferner einzelne Darstellungsfehler beseitigt sowie die Anzeigegeschwindigkeit erhöht.

3.12.3.4 Reverse-Proxy Zugriff auf interne Server

In Version 6.0-2.0 und auf Systemen die vor dem 20.11.2013 auf Version 6.0-2.1 aktualisiert wurden, verbindet sich der Reverse-Proxy nicht mit Backend-Servern, die die unsichere clientseitige SSL-renegotiation unterstützten.

© 2014 XnetSolutions KG

3.13 Version 6.0-2.3

3.13.1 Neue Funktionen

3.13.1.1 Zusätzliche Optionen bei der Zertifikatserstellung

Die Bitlänge und der Signaturalgorithmus lässt sich nun auswählen. Ferner können Zertifikate nun mehrere alternative Bezeichner (Subject Alternative Names) erhalten.

3.13.1.2 Konfigurierbares Update-Intervall für DNS IP-Gruppen

Bisher wurden die IP-Adressen von DNS IP-Gruppen täglich aktualisiert. Nun ist dies auch stündlich oder sogar minütlich möglich, was auch die Nutzung mit dynamischen DNS-Adressen erlaubt.

3.13.1.3 Passwortgeschützte Dateien im Web-Proxy Content-Filter

Eine neue Option erlaubt es, passwortgeschützte Dateien ungeprüft auszuliefern anstatt diese Dateien im Quarantäne-Bereich abzulegen.

3.13.2 Änderungen

keine

3.13.3 Behobenen Fehler

3.13.3.1 Web-Proxy Content-Filter

Seit Version 6.0-2.0 gab es Probleme mit Web-Anwendungen, die den HTTP Expect-Mechanismus nutzen. Bei der Nutzung als transparenter Proxy wurden Zugriffe verweigert, wenn der Client einen externen DNS nutzte oder wenn der Client aufgrund von Caching über abweichende DNS-Informationen verfügte.

3.13.3.2 Reverse-Proxy Syntax-Prüfung

Die neue Version des Reverse-Proxies aus 6.0-2.0 nutzt eine geänderte Syntax-Prüfung, die bei einigen Anwendungen zu Problemen führte. Mit dem Update wird das alte Verhalten wiederhergestellt.

3.13.3.3 POP-/IMAP-Client Duplikatserkennung bei Sammelpostfächern

Abhängig von Provider und Konfiguration funktionierte die neue Duplikatserkennung des POP-/IMAP-Clients aus 5.2-3.2 und 6.0-2.0 nicht immer ohne zusätzlichen Konfigurationsaufwand. Mit dem Update wird das alte Verhalten wiederhergestellt.

3.13.3.4 Ablauf der URL-Filter Lizenz

Bislang erfolgte keine Benachrichtigung, wenn die Aktualisierung der kommerziellen URL-Filter Datenbank aufgrund abgelaufener Lizenz verweigert wurde.

3.14 Version 6.0-2.4

© 2014 XnetSolutions KG

3.14.1 Neue Funktionen

3.14.1.1 Tooltip für Protokolle, IP- und Benutzer-Gruppen

In der Administrationsoberfläche lässt sich nun überall wo eines dieser Objekte verwendet wird anzeigen, wofür dieses Objekt steht.

3.14.1.2 Monitoring für OpenVPN Verbindungen

3.14.1.3 Maskieren von E-Mail Absender-Adressen

© 2014 XnetSolutions KG

3.14.2 Änderungen

3.14.2.1 SecureUSB-Stick Konfiguration

Die Installation des Terminal-Server-Clients auf dem USB-Stick ist nicht mehr zwingend erforderlich. Wird der Terminal-Server-Client auf dem Stick nicht gefunden, wird auf den Client des Computers zurückgegriffen, an dem der Stick gerade angeschlossen ist.

Ferner kann die »/public«-Option beim Aufruf des Terminal-Server-Clients nun abgewählt werden. Dadurch werden bestimmte Einstellungen für die nächste Benutzung im System zwischengespeichert. Die Option sollte nur dann abgewählt werden, wenn der Stick ausschließlich auf einem privaten Computer zum Einsatz kommt.

© 2014 XnetSolutions KG

3.14.3 Aktualisierungen

3.14.3.1 Avira Antivirus

3.14.3.2 Cluster Software

© 2014 XnetSolutions KG

3.14.4 Behobene Fehler

3.14.4.1 OpenSSL Crypto-Bibliothek

Die neue Version beseitigt potentielle Denial-of-Service Angriffsmöglichkeiten.

3.14.4.2 Web-Proxy mit Digest-Authentifizierung

Bei aktivierter Digest-Authentifizierung konnte es seit 6.0-2.0 zu Abstürzen des Web-Proxies kommen.

3.14.4.3 Reverse-Proxy Redirects

Abhängig vom Web-Server oder der Web-Applikation auf dem Hintegrund-Server konnte es seit Version 6.0-2.0 vorkommen, dass HTTP-Redirects die direkt auf den Hintergrund-Server verweisen nicht umgeschrieben wurden.

© 2014 XnetSolutions KG

3.15 Version 6.0-2.5

3.15.1 Neue Funktionen

3.15.1.1 E-Mail Domain-Routing an externen E-Mail-Server

Ein ausgehendes E-Mail-Routing steht ausschließlich internen Clients oder authentifizierten Benutzern zur Verfügung. Auf Wunsch kann dieses E-Mail-Routing auch für Subdomains gelten. Praktisches Anwendungsbeispiel ist der Versand über ein De-Mail-Gateway.

3.15.1.2 Netzwerkkarten-Docklet

Auf der Startseite steht ein neues Status-Fenster zur Verfügung, in dem der "Link"-Status aller Ethernet-Ports angezeigt wird.

© 2014 XnetSolutions KG

3.15.2 Änderungen

3.15.2.1 Überarbeitete Netzwerkkarten-Erkennung

Beim Erweitern des Systems mit zusätzlichen Netzwerkkarten waren teilweise Eingriffe auf Systemebene notwendig, um wieder alle benötigten Treiber in der richtigen Reihenfolge zu laden.

3.15.2.2 Eingabe von Top-Level-Domains (TLD)

In einigen Eingabefeldern können nun auch ganze TLDs eingetragen werden, so z.B. in den URL-Filter Listen.

© 2014 XnetSolutions KG

3.15.3 Aktualisierungen

keine

© 2014 XnetSolutions KG

3.15.4 Behobene Fehler

3.15.4.1 Web-Proxy Content-Filter

TLS 1.1/1.2 wurde bei aktivierter SSL-Versionsprüfung fälschlicherweise abgewiesen. Die SSL-/TLS-Sicherheit bei aktivierter Option "SSL aufbrechen" wurde verbessert. So ist der Content-Filter nun auf weitestgehende Nutzung von Perfect-Forward-Secrecy und TLS 1.2 optimiert. Das Update beseitigt vereinzelte defekte Links bei der Nutzung als transparenter Proxy. Ferner konnten Web-Anwendungen hängen bleiben, wenn diese den HTTP-Expect Mechanismus nutzen, der Server dies jedoch ignoriert.

3.15.4.2 Provider-Relay mit Submission-Port und E-Mail-Routing

Bei manchen Provider E-Mail-Servern müssen E-Mails auf dem E-Mail-Submission-Port 587 oder einem anderen providerspezifischen Port eingeliefert werden. Ist zugleich für bestimmte Empfänger-Adressen ein E-Mail-Routing zu einem anderen E-Mail-Server konfiguriert, wurde dieser Server ebenfalls auf dem Submission Port angesprochen.

3.15.4.3 OpenVPN Installationspaket mit 64-Bit Client

Wenn der 64-Bit OpenVPN Windows-Client installiert ist, wurde das Installationsverzeichnis für die OpenVPN-Konfigurationsdatei nicht gefunden.

3.15.4.4 POP3- und SMTP-Proxy

Das Update behebt Abstürze des POP3-/SMTP-Proxies.

3.16 Version 6.0-2-6

3.16.1 Neue Funktionen

3.16.1.1 Verschlüsselung für POP3-/SMTP-Proxy

Der transparente POP3- und SMTP-Proxy kommt zum Einsatz, um internen Anwendern direkten Zugriff auf beliebige POP3- und SMTP-Server zu erlauben. Bislang erfolgte die Kommunikation über diesen Proxy durchgängig unverschlüsselt. Ab sofort wird internetseitig automatisch Verschlüsselung aktiviert, wenn der Server dies unterstützt.

3.16.2 Änderungen

keine

3.16.3 Aktualisierungen

3.16.3.1 Secure-Shell Server

Dieser Dienst wird für SSH TCP-Weiterleitungen und die Fernwartung verwendet. Die neue Version führt den neuen Schlüsseltausch-Algorithmus Curve25519 ein. Nicht mehr zeitgemäße Krypto-Verfahren wurden deaktiviert.

3.16.4 Behobene Fehler

keine

© 2014 XnetSolutions KG

3.17 Version 6.0-2.7

3.17.1 Sicherheitskritisch

3.17.1.1 OpenSSL Crypto-Bibliothek

Die OpenSSL Crypto-Bibliothek wird von diversen Systemkomponenten genutzt um verschlüsselte Verbindungen herzustellen oder entgegenzunehmen. Ein kritischer Fehler ermöglicht es, über die verschlüsselte Verbindung Zugriff auf einen größeren Speicherbereich zu erhalten, der sensitive Daten wie den privaten Schlüssel des Servers aber auch Dokumente und Kennwörter enthalten kann. Betroffen sind alle Versionen ab 6.0-2.0.

3.17.2 Neue Funktionen

keine

3.17.3 Änderungen

keine

3.17.4 Aktualisierungen

keine

3.17.5 Behobene Fehler

keine

© 2014 XnetSolutions KG

3.18 Version 6.0-2-9

3.18.1 Sicherheitskritisch

3.18.1.1 Aktualisierung des Linux-Kernels

Das Update behebt zwei Sicherheitslücken, die von einem lokal auf dem System angemeldeten Angreifer ausgenutzt werden können, um privilegierte Befehle auszuführen oder das System zum Absturz zu bringen. Ferner werden Treiber für Netzwerkkarten, VMware und Hyper-V aktualisiert.

Nach dem Update führt das System automatisch einen Neustart durch. Bitte starten Sie das System nicht von Hand neu.

3.18.1.2 OpenSSL Crypto-Bibliothek

Die OpenSSL Crypto-Bibliothek wird von diversen Systemkomponenten genutzt um verschlüsselte Verbindungen herzustellen oder entgegenzunehmen.

Ein Angreifer, der eine Man-in-the-Middle Attacke gegen einen Client und einen Server durchführen kann, die gleichermaßen betroffene OpenSSL-Versionen nutzen, konnte den generierten Schlüssel schwächen und so die Verbindung entschlüsseln oder modifizieren.

Die neue Version beseitigt ferner einen möglichen Absturz, wenn das System eine verschlüsselte Verbindung zu einem bösartigen Server aufbaut.

3.18.1.3 POP/IMAP-Client Zustellung an lokale Postfächer

War der lokale E-Mail-Server gestoppt oder nahm dieser aufgrund hoher Systemlast keine E-Mails an, wurden E-Mails nach der Abholung vom POP-/IMAP-Server des Providers teils am lokalen E-Mail-Server vorbei und damit ungeprüft in lokale Postfächer zugestellt. Betroffen sind Systeme die auf Version 5.2-3.2/5.2-3.3 aktualisiert wurden sowie Systeme ab 6.0-2.0.

Systeme, die E-Mails per SMTP erhalten oder an einen internen E-Mail-Server weiterleiten, waren nicht betroffen.

3.18.2 Neue Funktionen

3.18.2.1 Remotedesktop Web-Access über Reverse-Proxy

Ergänzend für den Zugriff auf ein Remotedesktop-Gateway steht im Reverse-Proxy nun auch ein Schalter für Remotedesktop Web-Access zur Verfügung.

In dieser Versionsreihe nur auf Systemen mit Software Pflegevertrag verfügbar.

3.18.3 Behobene Fehler

3.18.3.1 E-Mailversand: TLS Handshake failed

Seit Version 6.0-2.7 gibt es Probleme beim verschlüsselten Mail-Versand an Mail-Server, die Cisco IronPort einsetzen. Inwieweit das Problem nur mit bestimmten Versionen dieses Produkts auftritt, ist uns nicht bekannt. Systeme, die ausgehende Mails über den Relay-Server ihres Providers versenden, sind in der Regel nicht betroffen.

Ursache ist eine neue TLS-Erweiterung, die die Kompatibilität mit älteren SSL-Implementierungen verbessern soll. Als Workaround haben wir diese Erweiterung entfernt, bis das Problem gelöst ist.

© 2014 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

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