XnetSolutions

SX-GATE

Software Update
Release Note

Version: 7.0-1-0

Inhaltsverzeichnis

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:

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.

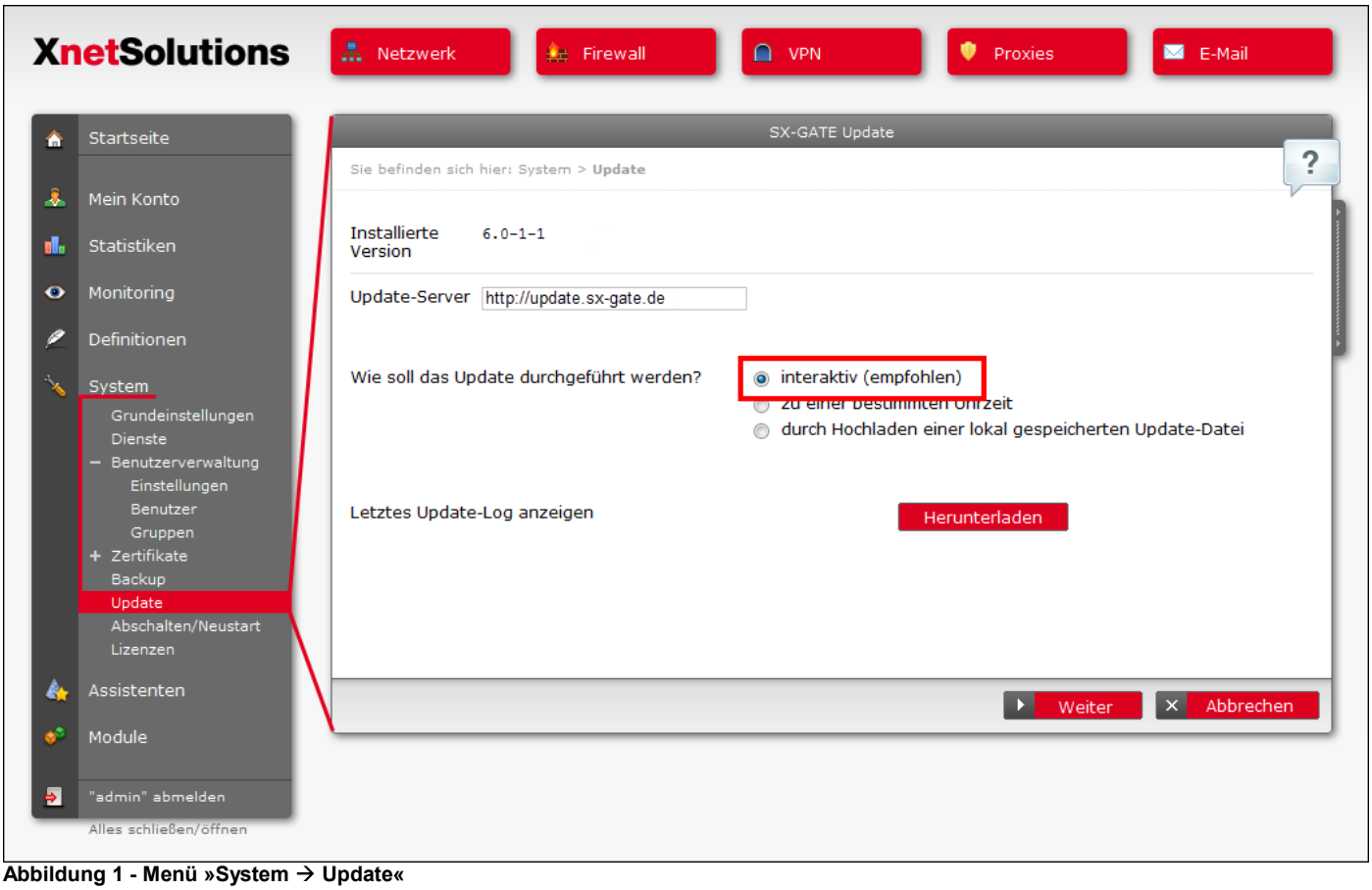

Abbildung 1 - Menü »System → Update«

- **Manuelles Software-Update**

Bevor Sie das Software-Update durchführen können ist es erforderlich, dass Sie das benötigte Software-Update Version 7.0-1-0 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.

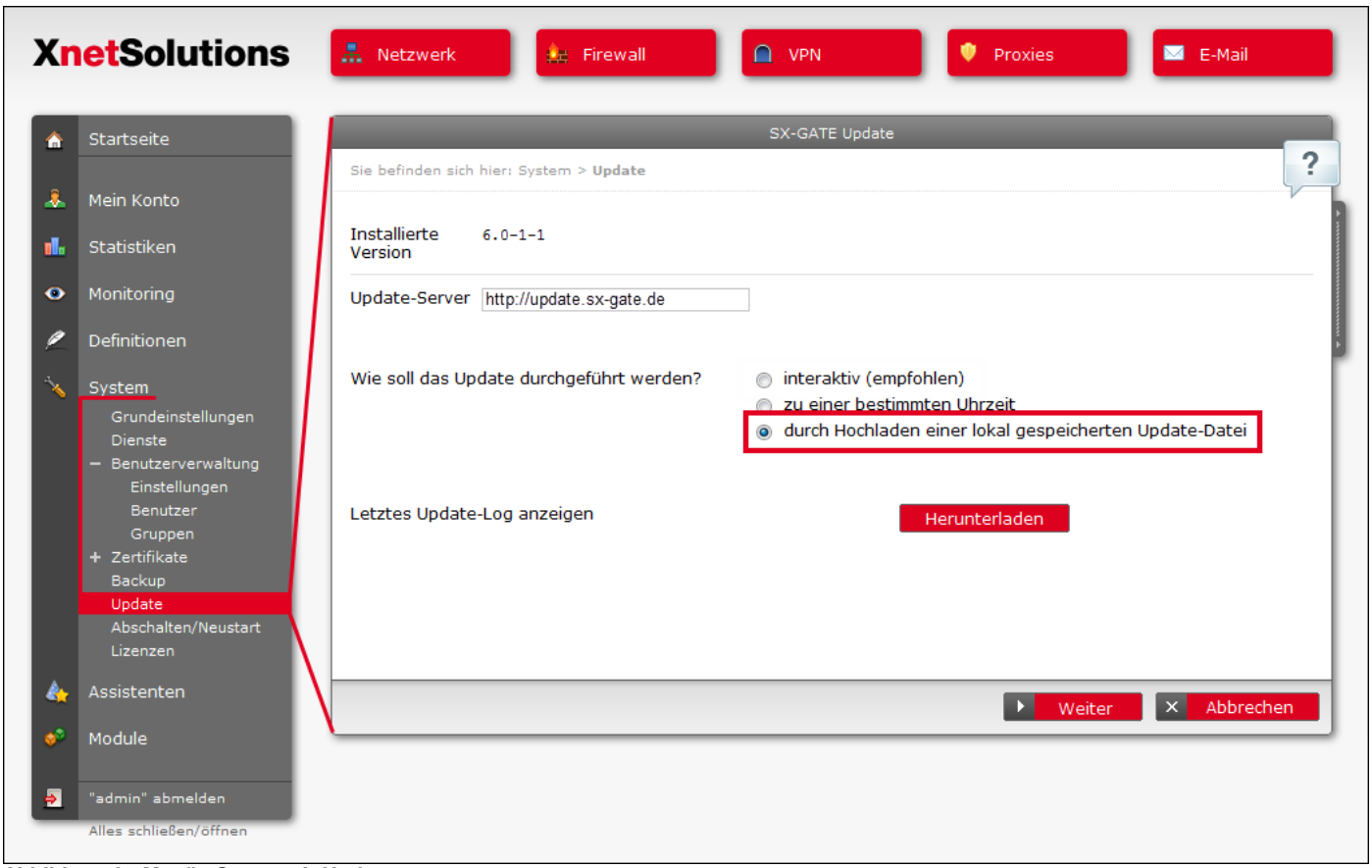

Abbildung 2 - Menü »System → Update«

Wichtig:

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

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.

Der gesamte Installationsprozess wird bei dieser Softwareversion ca. 30 Minuten in Anspruch nehmen.

2.1 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 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.

2.2 Neue Funktionen

2.2.1 IPv6-Unterstützung

Mit dem Update erhält das System weitgehende Unterstützung für IPv6. IPv6 ist zunächst deaktiviert und muss unter "Module > Netzwerk > Einstellungen" aktiviert werden. Danach lässt es sich je nach Bedarf in den einzelnen Schnittstellen zuschalten.

Sollten Ihnen bei den IPv6-Netzwerkfunktion Möglichkeiten fehlen, bitten wir um Rückmeldung. Eine Unterstützung von IPv6-in-IPv4-Tunneln (IPv6 über reine IPv4-Anbindungen) ist derzeit nicht geplant.

Bei den Server-Diensten ist für den SIP-Proxy keine IPv6-Unterstützung geplant. Aktuelle fehlt noch die IPv6-Unterstützung für folgende Komponenten: POP3-/SMTP-Proxy, FTP-Proxy und dynamischer DNS. Bei folgenden Komponenten gibt es noch Einschränkungen: IPsec-L2TP-Verbindungen können zwar über IPv6 mit dem Server kommunizieren, als Nutzdaten kann jedoch nur IPv4 übertragen werden (IPv4-in-IPv6). IPsec-Xauth-Verbindungen können für IPv6 nur ohne ModeCfg genutzt werden. Im Web-Proxy URL-Filter ist es noch nicht möglich, Regeln für bestimmte IPv6-Client-IPs zu konfigurieren.

2.2.2 IP-Gruppen / IP-Objekte

Der Menüpunkt "IP-Gruppen" wurde in "IP-Objekte" umbenannt. Neben den bekannten Typen "Gruppe" und "DNS-Eintrag" lassen sich nun auch IP-Objekte folgenden Typs anlegen:

- **Geolokation**

  Der Typ "Geolokation" kann nur in Firewall-Regeln genutzt werden. Hier können Sie Länderkennungen wie "DE", "AT" oder "CH" eintragen, um Verbindungen basierend auf dem Herkunfts- oder Zielland freizugeben. Die Zuordnung von IP-Adressen auf Länder erfolgt dabei mit Hilfe einer im System hinterlegten Datenbank.

- **IPv6-Präfix und IPv6-Adresse**

  Die Objekt-Typen "IPv6-Präfix" und "IPv6-Adresse" sind vor allem dann nützlich, wenn dynamisch vom Provider zugewiesene IPv6-Präfixe an interne Netze weiterverteilt werden müssen. In beiden Objekt-Arten kann eine Teil-Adresse und ein Bezug auf ein weiteres IP-Objekt vom Typ "IPv6-Präfix" konfiguriert werden, die zusammengerechnet die tatsächliche Adresse ergeben.

- **IPv4-Adresse**

  Der ebenfalls neue Objekt-Typ "IPv4-Adresse" hat keine tiefergehende Bedeutung. Er kann in komplexen Konfigurationen zur besseren Strukturierung und Lesbarkeit beitragen.

2.2.3 Erweiterte Möglichkeiten bei der Firewall-Konfiguration

Firewall-Regeln können nun mit einem Ablaufzeitpunkt versehen werden, ab dem keine neuen Verbindungen mehr von dieser Regel akzeptiert werden. Gedacht ist dies vor allem für temporäre Regeln. Bisher wurde von Administratoren oft vergessen, diese wieder zu löschen.

Ab sofort ist es auch möglich, Firewall-Regeln zu konfiguieren, die Verbindungen verbieten. Der Verbindungswunsch kann entweder ohne Rückmeldung verworfen oder mit einer ICMP-Antwort abgelehnt werden.

Bislang wurde SNAT als Teil von Weiterleitungs-Regeln konfiguriert. Ab sofort steht dafür eine eigene Konfigurationstabelle zur Verfügung.

2.2.4 Mehrere Zeiträume für URL-Filter-Regeln

Bisher konnte für den URL-Filter nur ein Zeitraum "Arbeitszeiten" definiert werden. Nun sind beliebig viele Zeiträume möglich, die individuell in den URL-Filter-Regeln verwendet werden können. Die Zeiträume werden im Menü "Definitionen > Zeiträume" festgelegt.

2.2.5 Reverse-Proxy Exchange-Backend für MAPI-over-HTTP

Aktuelle Exchange- und Outlook-Versionen kommunizieren ggf. nicht mehr über RPC- sondern mit MAPI-over-HTTP. In der Reverse-Proxy-Konfiguration wurde ein entsprechender Schalter hinzugefügt.

2.2.6 Umbenennen von Einträgen

Tabellen in der Administrations-Oberfläche, in denen die Einträge der ersten Spalte als Link ausgeführt sind, verweisen auf komplexe Elemente. Dazu gehören z.B. Benutzer und die Definitionen von Protokollen oder IP-Objekten. Diese Einträge können nun weitestgehend umbenannt werden. Klicken Sie dazu auf das Stift-Symbol am rechten Rand der jeweiligen Tabellenzeile.

Wichtiger Hinweis:
Bis einschließlich Version 6.0-4.8 entsprach das Stift-Symbol dem Link in der ersten Spalte und ermöglichte das Bearbeiten der Einstellungen des jeweiligen Elements.

2.2.7 Anzeige von Tabellen

Die max. Anzahl von Zeilen in Tabellen wurde verdoppelt.

Beim Überschreiten der max. Zeilenzahl wurden die Einträge bisher auf mehrere Seiten aufgeteilt. Als Alternative zur Seitenschaltung lassen sich Tabellen, in denen die Reihenfolge der Einträge keine Rolle spielt, jetzt auch gruppiert anzeigen. Die Gruppierung bezieht sich dabei immer auf die Spalte, nach der aktuell sortiert wird. Abhängig vom Datentyp der Spalte wird z.B. nach Anfangsbuchstabe, Ordner-Name oder identischen Einträgen gruppiert. Die Gruppierung lässt sich über das Werkzeugsymbol in der rechten, oberen Ecke aktivieren.

2.2.8 Zusatzinformationen zu IP-Adressen

Bei der Anzeige von Log-Dateien und im Netzwerk-Monitoring sind IP-Adressen vielfach als Link ausgeführt. Auf Klick werden das Herkunftsland sowie der über Reverse-Lookup ermittelte DNS-Name angezeigt.

2.2.9 Zusatzinformationen in Log und Monitoring

Im Maillog ist zu jeder E-Mail eine ganze Reihe von Einträgen zu finden, die oft nicht unmittelbar hintereinander stehen. Neben der ID jeder Mail befindet sich nun ein Link, über den alle zu dieser Mail gehörenden Zeilen in einem separaten Fenster angezeigt werden.

In der Log-Anzeige der Intrusion-Detection (IDS) lässt sich über einen Link der zugehörige Paket-Dump abrufen.

Im IPsec-Log können über einen Link ebenfalls zusammengehörige Zeilen abgerufen werden.

Durch Klick auf das Info-Symbol im IPsec-Reiter des Netzwerk-Monitorings werden Detailinformationen zur jeweiligen IPsec-Verbindung angezeigt.

2.2.10 LDAP-Zugang testen

Für den Active-Directory Benutzerimport und die Mail-Adressverifikation via LDAP stehen nun Testfunktionen zur Verfügung.

2.2.11 Geschwindigkeit und Duplex-Betrieb der Netzwerkkarten konfigurierbar

2.2.12 Reverse-Proxy Option für Strict-Transport-Security

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

In den HTTPS-Ports des Reverse-Proxies lässt sich nun HTTP Strict-Transport-Security aktivieren. Diese Option weist den Browser an, für eine bestimmte Zeitdauer ausschließlich per HTTPS auf den Server zuzugreifen und dem Benutzer keine Möglichkeit zu geben, Zertifikatsfehler zu ignorieren. Damit sollen Man-in-the-Middle Attacken erschwert werden.

2.2.13 Remotedesktop-Gateway über Reverse-Proxy

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

Neue Optionen erlauben den Zugriff auf Remotedesktop-Gateway-Server und mit Remotedesktop Web-Access.

2.2.14 Erweiterte Funktionen beim Aufbrechen von SSL-Verbindungen im Web-Proxy

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

Ist das Aufbrechen von SSL-Verbindungen aktiviert, können jetzt HTTPS-Verbindungen zu Port 443 auch transparent an den Proxy umgeleitet werden. Im Proxy darf jedoch keine Authentifizierung konfiguriert sein.

Das Verhalten bei abgelaufenen Zertifikaten und bei Zertifikaten die auf einen abweichenden Server-Namen ausgestellt wurden lässt sich nun konfigurieren. Wurde die Entscheidung, ob dieser Verbindung zu trauen ist, bisher dem Anwender überlassen, kann die Verbindung nun auch grundsätzlich abgewiesen werden.

Wie der Proxy auf fehlgeschlagene OCSP-Anfragen reagieren soll, lässt sich ebenfalls einstellen.

Sofern der URL-Filter aktiviert ist greifen bei aufgebrochenen SSL-Verbindungen nun auch pfadbasierte Sperren wie z.B. gesperrte Dateinamenserweiterungen oder der Jugendschutzfilter bei Suchmaschinen.

2.2.15 Passwortgeschützte Dateien im Web-Proxy Content-Filter

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

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

2.2.16 Abfrage des Web-Proxy URL-Filters

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

Im "Monitoring"-Menü lässt sich über eine Abfragemaske das Verhalten des URL-Filters testen.

2.2.17 Sender-Policy-Framework (SPF) Filter

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

Für Systeme, die eingehende E-Mails direkt per MX-Eintrag im DNS erhalten, steht ein neuer Filter zur Verfügung. Über einen DNS-Eintrag kann der Inhaber einer Domain festlegen, dass E-Mails mit entsprechender Absender-Adresse ausschließlich über bestimmte Systeme gesendet werden dürfen. Mit dem SPF-Filter werden diese Einträge ausgewertet und E-Mails abgewiesen, die nicht dieser Vorgabe entsprechen. SPF richtet sich also gegen E-Mails mit gefälschten Absender-Adressen und leistet damit indirekt auch einen Beitrag zur Abwehr bestimmer SPAM- und Schädlings-Mails.

SPF kann Probleme mit weitergeleiteten Mails verursachen. Ferner müssen häufig einzelne Adressen manuell von der Filterung ausgenommen werden (z.B. Backup-MX). Beachten Sie bitte unbedingt die Informationen in der Online-Hilfe.

2.2.18 Erweiterte Möglichkeiten im E-Mail Anhangsfilter

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

Unter dem Eindruck der aktuellen Virenwelle haben uns viele Anregungen zur Erweiterung des Dateianhangsfilters erreicht. Folgende Änderungen habe wir in dieser Version umgesetzt:

Die altbekannte Liste der zu sperrenden Dateinamenserweiterungen heißt nun "Gefährliche Datei-Anhänge". Entsprechende Dateien werden grundsätzlich aus der E-Mail entfernt und in das Quarantäne-Verzeichnis gestellt. Die von uns empfohlene Vorbelegung dieser Liste finden Sie in der Online-Hilfe.

Es folgt eine neue Liste mit "vertrauenswürdigen Absendern". Sie können einzelne E-Mail Addressen oder auch ganze Domains eingeben. Diese dürfen beliebige Anhänge senden, mit Ausnahme der "Gefährlichen Datei-Anhänge".

Abhängig von der nun ebenfalls konfigurierbaren Standardeinstellung des Filters - alle übrigen Anhänge entweder weiterleiten oder ausfiltern - wird eine weitere Liste mit Dateinamenserweiterungen angeboten. Werden alle übrigen Anhänge unter Quarantäne gestellt, ist dies eine Liste mit für alle freigegebenen Dateinamenserweiterungen. Tragen Sie also hier eher unbedenkliche Dateien wie z.B. Bilder oder PDF ein. Sind hingegen alle übrigen Dateianhänge erlaubt, steht Ihnen eine weitere Liste mit zu filternden Dateierweiterungen zur Verfügung. Im Unterschied zu den "Gefährlichen Datei-Anhängen" dürfen entsprechende Anhänge passieren, wenn sie von "vertrauenswürdigen Absendern" kommen. Hier könnte man in Anbetracht der aktuellen Situation beispielsweise normale Office-Dokumente wie doc, docx, xls, usw. eintragen.

Wichtiger Hinweis:
Sie können mehrere Dateinamenserweiterungen auf einmal hinzufügen, wenn Sie diese mit Leerzeichen getrennt eingeben (z.B. "doc docx xls").

2.2.19 Verifikation der Empfängeradressen am internen Mail-Server

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

Der für die Verifikation mit SMTP genutzte Port des internen Mail-Servers ist nun konfigurierbar. Alternativ ist die Verifikation nun auch mittels LDAP-Abfrage eines Active-Directories möglich. Nutzen Sie eine dieser beiden Möglichkeiten, falls als interner Mail-Server Exchange 2013 zum Einsatz kommt.

Eine weitere neue Option ermöglicht es, Mails ohne Verifikation anzunehmen, falls der interne Mail-Server vorübergehend nicht verfügbar ist. Die Mails werden dann in der lokalen Warteschlange zwischengespeichert.

2.2.20 Maskieren von E-Mail Absender-Adressen

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

2.2.21 Individuelles Mail-Relay je Absender-Domain

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

In Einzelfällen kann es notwendig sein, ausgehende Mails je nach Absender-Domain über unterschiedliche Relay-Server zu versenden.

2.2.22 Maildomain Routing an externen Mail-Server

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

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

2.2.23 OpenVPN Zugriff nur für ausgewählte Zertifikate

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

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.

2.2.24 Vereinfachtes Überschreiben von DNS-Einträgen

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

In bestimmten Situationen kann es notwendig werden, Informationen aus dem Internet-DNS für lokale Clients mit anderen Informationen zu überschreiben. Solche Einträge können nun direkt konfiguriert werden, ohne eine entsprechende Domain-Zone anlegen zu müssen. Dabei können auch Aliase (CNAME) genutzt werden.

2.2.25 DNSSec Validierung

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

Im DNS-Forwarder kann die Validierung aller erhaltenen DNS-Antworten mittels DNSSec aktiviert werden.

2.2.26 Konfigurierbares Update-Intervall für DNS IP-Gruppen

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

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.

2.2.27 Diensteüberwachung

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

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

2.2.28 Erweiterung der Netzwerk-Werkzeuge

Diese Funktion konnte bereits in den 6.0er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 7.0 ist diese Funktion auf allen Systemen verfügbar.

Das Werkzeug "Traceroute" wurde ergänzt. Bei "Ping" besteht nun die Möglichkeit, die Paketgröße festzulegen. Ferner erlaubt es die Auswahl der Schnittstelle, VPN-Tunnel mit unterschiedlichen Quell-IPs zu testen.

2.3 Änderung

2.3.1 Cluster-Dienst

Der Cluster-Dienst wird aktualisiert um eine verbesserte IPv6-Unterstützung zu erhalten. Zudem wird die Kommunikation zwischen den Cluster-Knoten von Multicast auf Unicast und von einem variablen auf einen festen Port umgestellt.

Wichtiger Hinweis:
Nach dem Update des Master-Knotens findet keine Synchronisation der Firewall-Verbindungstabelle mehr statt, bis auch der Backup-Knoten aktualisiert ist. In diesem Zustand ist damit zu rechnen, dass im Falle eines Failovers nahezu alle offenen Verbindungen abbrechen.

Auf Clustern mit geteiltem Internet-Zugang wird die Internet-Schnittstelle im Backup-Status deaktiviert.

2.3.2 ISDN-Unterstützung

Die Unterstützung für ISDN stellen wir mit Version 7.0 ein. Das Update wird daher abgebrochen, wenn eine ISDN-Karte im System gefunden wird und der zugehörige Treiber konfiguriert ist. Setzen Sie sich bitte mit dem technischen Support in Verbindung, falls Sie ISDN noch dringend benötigen. Wird ISDN nicht mehr benötigt, erfahren Sie über den technischen Support, wie Sie die Treiberkonfiguration löschen können. Alternativ können Sie auch die ISDN-Karte ausbauen.

2.3.3 FTP-Server

Der FTP-Server wird durch eine andere Software ersetzt. Mit der neuen Software ist es leider nicht mehr möglich, den anonymen Zugriff auf bestimmte Netze zu beschränken.

Wichtiger Hinweis:
Sofern der anonyme Zugriff nur für lokale IP-Subnetze erlaubt war, wird dieser mit dem Update gesperrt.

2.3.4 Firewall-Report

Der per E-Mail versendete Wählleitungs- und Firewall-Report wird nicht mehr angeboten.

2.3.5 Neue dynamische Firewall

Die dynamische Firewall beobachtet die Kommunikation und kann bei auffälligem Verhalten die zugehörige Quell-IP automatisch sperren. Bei der Neuimplementierung dieses Moduls wurde vor allem auf eine einfache Konfigurierbarkeit und die Vermeidung von Fehlalarmen Wert gelegt. Ein Dienst muss für die dynamische Firewall nun nicht mehr gestartet werden. Analysiert wird der komplette Datenverkehr über alle Schnittstellen. Die Reputation der einzelnen IP-Adressen kann im Monitoring-Menü ausgelesen werden. Bislang gibt es lediglich zwei Konfigurationsoptionen: In der Firewall-Konfiguration der Schnittstellen lässt sich die automatische Sperrung auffälliger IPs aktivieren, was in erster Linie in den Internet-Schnittstellen empfohlen wird, sofern eingehende Verbindungen erlaubt sind. Zudem kann in den globalen Einstellungen der Firewall eine Liste von IPs hinterlegt werden, die nie gesperrt werden, sollte es zu Fehlerkennungen kommen.

2.3.6 Vertrauenswürdige Server im Web-Proxy Content-Filter

Ein Eintrag in die Liste der vertrauenswürdigen Server hat bisher alle Komponenten des Content-Filters für diesen Server deaktiviert. Ab sofort lassen sich auch nur Teilkomponenten deaktivieren.

2.3.7 Web-Proxy Cache

Das Standardverhalten für das Caching im Web-Proxy wurde verändert. Der Festplatten-Cache ist nun deaktiviert (zuvor 200MB). Dafür werden nun 128MB Hauptspeicher für das Caching verwendet (zuvor 8MB). Steht ein Parameter noch auf dem alten Vorgabewert, wird dieser durch das Update automatisch umgestellt. Ist ein benutzerdefinierter Wert eingestellt, bleibt dieser erhalten.

2.3.8 Anzeige der Log-Dateien

In einigen Log-Dateien werden bestimmte Zeilen nun farblich hinterlegt, um das Log übersichtlicher und inhaltlich leichter zugänglich zu machen.

2.4 Update

2.4.1 Migration auf 64-Bit Basissystem

Das Basissystem wird aktualisiert und weitgehend auf 64 Bit umgestellt. Dazu ist ein dreimaliger Neustart des Systems erforderlich, die vom Update selbständig durchgeführt werden. Nach dem Beginn der eigentlichen Update-Prozedur ist das System und damit auch das Internet für mehrere Minuten nicht erreichbar. Auf älterer und entsprechend langsamer Hardware kann dieser Zustand u.U. 10-15 Minuten andauern. Bitte haben Sie Geduld und starten Sie das System keinesfalls selbst neu, da das System bei Unterbrechung des Updatevorgangs unbenutzbar werden kann!

Wichtiger Hinweis:
Aufgrund des gestiegenen Speicherbedarfs empfehlen wir das Update nur für Systeme mit mindestens 2 GB Hauptspeicher. Für einen weiterhin performanten Betrieb empfehlen wir 4 GB Hauptspeicher.

Wichtiger Hinweis:
Stellen Sie vor dem Einspielen des Updates sicher, dass Sie über ein aktuelles Backup des Systems verfügen.

2.5 Bugfix

2.5.1 Firewall-Regeln in ipsec-Schnittstellen

Aus technischen Gründen war es bisher nicht möglich, Weiterleitungsregeln für ipsec-Schnittstellen auf bestimmte Quell-Zonen einzuschränken. Dieses Problem konnte nun beseitigt werden.

3 Änderungen in vorherigen Versionen

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