XNETSOLUTIONS
cyber. security. systems

SX-GATE

Software Update
Release Note

Version: 7.2-1-8

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.

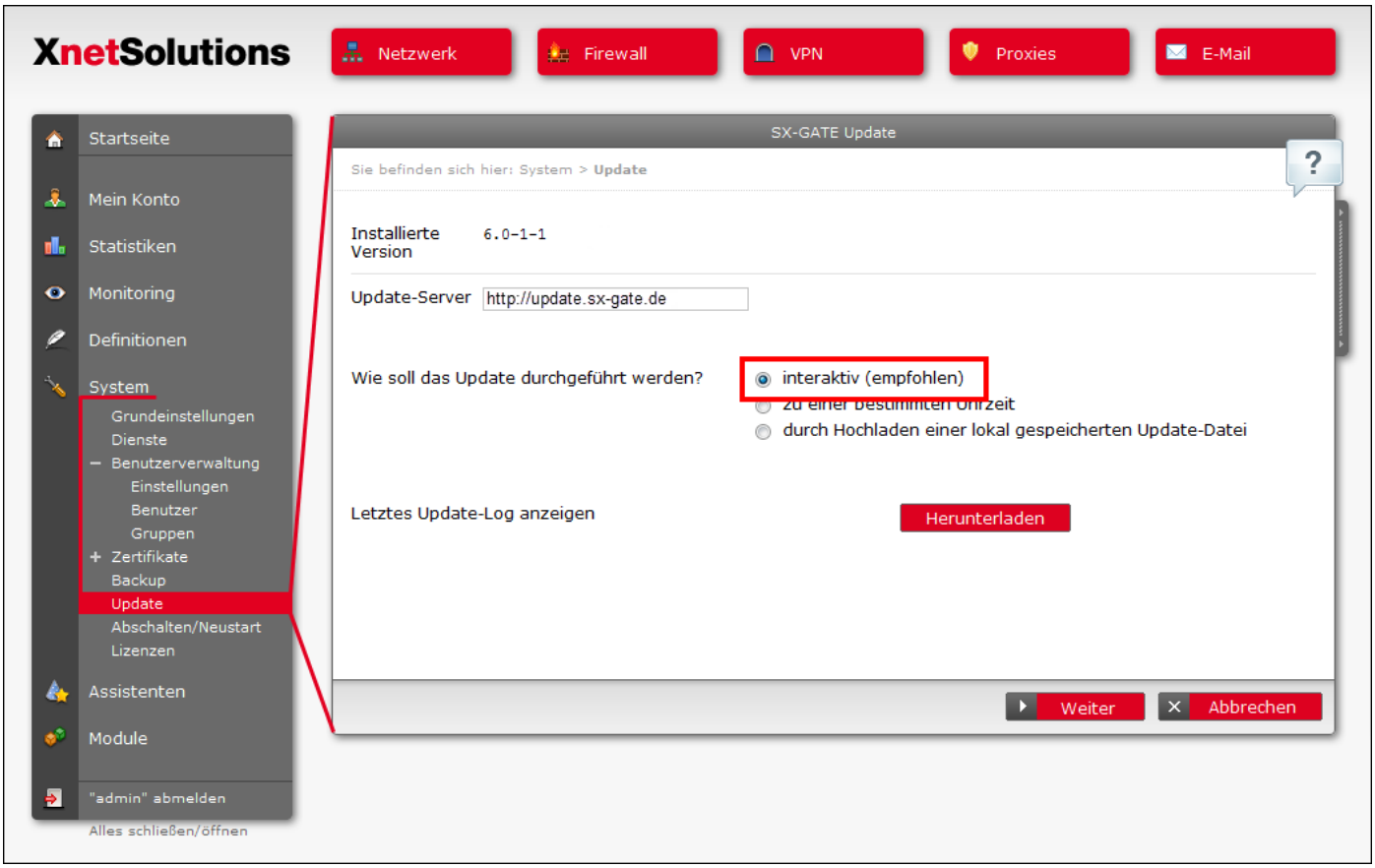

Abbildung 1 - Menü »System → Update«

- **Manuelles Software-Update**

Bevor Sie das Software-Update durchführen können ist es erforderlich, dass Sie das benötigte Software-Update Version 7.2-1-8 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.

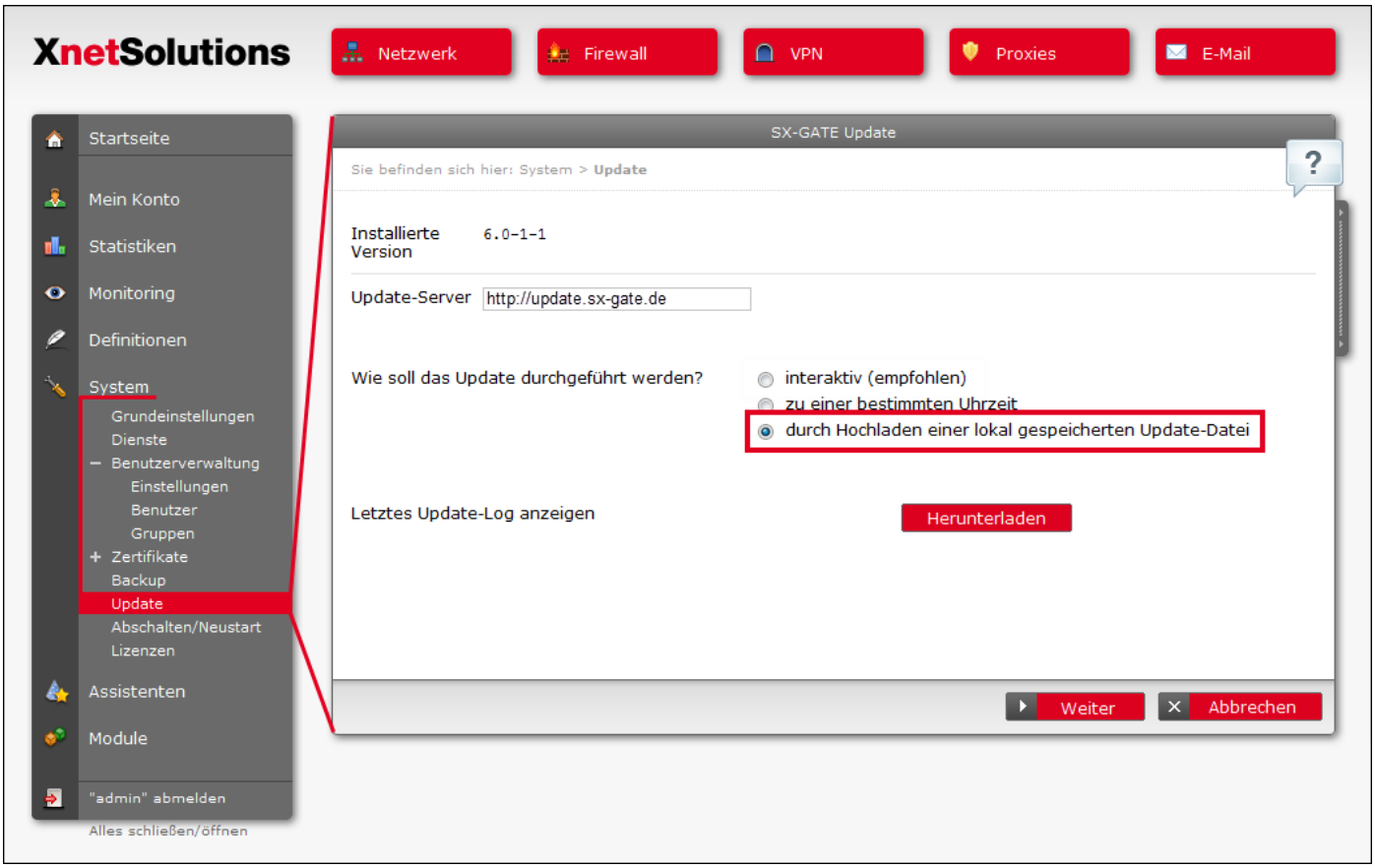

Abbildung 2 - Menü »System → Update«

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.

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.

2.1 Neu

2.1.1 Monitoring-Werkzeug ARP-Scan

Mit dem neuen Werkzeug können Sie das unmittelbar an eth-, vlan- oder wlan-Schnittstellen angeschlossene Netzwerksegment nach IPv4-Systemen durchsuchen. Angezeigt werden Ihnen neben der IP- und MAC-Adresse auch der aus der MAC-Adresse abgeleitete Hersteller des Netzwerkadapters.

2.2 Update

2.2.1 Geänderte MAC-Adressen bei WLAN-Schnittstellen

Aus technischen Gründen ändern sich die MAC-Adressen von WLAN-Schnittstellen. Die Änderung findet nach dem nächsten Reboot statt. Möglicherweise verbinden sich Clients danach erst mit Verzögerung mit dem geänderten WLAN.

2.2.2 Optimierung der Hauptspeichernutzung im URL-Filter

Es werden nur noch die Datenbank-Kategorien in den Speicher geladen, die im Regelwerk genutzt werden. Wird der kommerzielle URL-Filter verwendet und die Option zur Analyse unbekannter URLs ist aktiviert, müssen nach wie vor alle Kategorien geladen werden.

2.2.3 Domain sls.microsoft.com zur Domainliste WINDOWS hinzugefügt

Domain sls.microsoft.com zur Domainliste WINDOWS hinzugefügt

2.3 Bugfix

2.3.1 Transparenter Web-Proxy

Seit Version 7.1-5.1 bzw. 7.2-1.1 kam es bei transparentem Proxying zu Verbindungsproblemen mit Servern, die im DNS laufend ihre IP-Adresse ändern.

2.3.2 IP-Objekt-Typ "DNS-Mitschnitt"

DNS-Antworten mit mehrere IPs der selben Adressfamilie wurden ignoriert.

2.3.3 S/MIME-Gateway: Übernahme von Zertifikaten aus signierten Mails zur Verschlüsselung

Einzelne Organisationen nutzen unterschiedliche S/MIME-Zertifikate zum Signieren und zur Verschlüsselung. Das S/MIME-Gateway hat aus der Signatur eingehender Mails bislang stets das zum Signieren benutzte Zertifikat für die spätere Verschlüsselung von ausgehenden Mails übernommen, auch wenn dieses gar nicht für die Verschlüsselung vorgesehen war. Mit diesem Zertifikat verschlüsselte Mails konnten dann in der Regel vom Empfänger nicht gelesen werden. Der Verwendungszweck wird jetzt überprüft und das korrekte Zertifikat für die Verschlüsselung ausgewählt.

2.3.4 Einstellungen zum Backup auf Cluster-Systemen

Die Einstellungen zum automatischen Erstellen von Backups wurden auf dem Cluster-Master bisher mit den Einstellungen des Backup-Knotens überschrieben.

2.3.5 Konfiguration des Mail-Servers wird nicht aktualisiert

Seit Version 7.2-1.5 wurde die Mail-Server Konfiguration nicht mehr aktualisiert, sofern ein von der Absender-Domain abhängiges Provider-Relay konfiguriert ist.

2.3.6 Kleinere Bugfixes und Verbesserungen

3 Änderungen in vorherigen Versionen

3.1 Version 7.2.1-7

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.

3.1.1 Neu

3.1.1.1 Backup privater Schlüssel

Sofern das Systembackup als passwortverschlüsselte Datei erstellt wird, enthält es ab sofort auch private Schlüssel aus dem Schlüsselbund. Der private CA-Schlüssel ist nach wie vor nicht Bestandteil des Backups.

Falls Sie das Systembackup auf das verschlüsselte Format umstellen wollen, sollten Sie bedenken, dass das Backup nutzlos ist, wenn das Passwort zur Entschlüsselung nicht mehr bekannt ist.

Im Backup-Menü wurde ferner die Möglichkeit geschaffen, manuell ein passwortverschlüsseltes Backup der privaten Schlüssel zu erstellen.

3.1.1.2 Verschlüsselte Übertragung von Backups und Logdateien

Das bisher zu diesem Zweck genutzte Secure-Copy-Protokoll (SCP) gilt als veraltet. Ab sofort steht alternativ das SFTP-Protokoll zur Verfügung, das ebenfalls auf Secure-Shell basiert.
Sowohl für SCP als auch für SFTP kann nun neben dem RSA- auch der ED25519-Schlüssel des Systems zur Authentizierung genutzt werden.

3.1.1.3 Neuer IP-Objekt-Typ "DNS-Mitschnitt"

Gelegentlich geben Softwareanbieter leider nur ganze Domains anstatt einzelner Servernamen an, die für das funktionieren der Software in der Firewall freigeschaltet werden sollen (z.B. *.example.com). Wenn die Software auch über den Web-Proxy kommunizieren kann, ist eine solche Freigabe kein Problem. Aber es wurde schwierig, wenn der Zugriff tatsächlich in der Firewall freigegeben werden musste. Der neue IP-Objekt-Typ versucht es zu lösen, in dem er IP-Adressen sammelt, die er in DNS-Antworten zur jeweiligen Domain findet. Der neue IP-Objekt-Typ ist ausschließlich in Firewall-Regeln nutzbar und üblicherweise nur als Ziel bei Weiterleitungs-Regeln in das Internet sinnvoll. Voraussetzung ist, das der Client DNS-Anfragen direkt oder indirekt über den DNS-Server der Firewall auflöst. Eine kurze Verzögerung bis zur Freigabe einer Verbindung in der Firewall ist systembedingt.

3.1.2 Update

3.1.2.1 Diverse Systemkomponenten

Aktualisiert werden der Linux-Kernel, Avira Antivirus, Web-Proxy, Web-Server und SSH-Server, sowie diverse System-Bibliotheken und Werkzeuge.

3.1.3 Bugfix

3.1.3.1 Web-Proxy Content-Filter

Insbesondere bei langsamer Internetanbindung (z.B. über VPN) kam es trotz des Bugfixes aus Version 7.2-1.6 immer noch zu Problemen beim transparenten HTTPS-Proxying mit auf Chromium basierenden Browsern wie Chrome oder Edge.
Das Update behebt ferner sporadische Verbindungsprobleme bei aktivierter SSL-Prüfung von CONNECT-Verbindungen.

3.1.3.2 Kleinere Bugfixes und Verbesserungen

3.2 Version 7.2-1-6

3.2.1 Neu

3.2.1.1 Automatische Zertifikatsverwaltung

Kunden mit Bedarf an vielen Kauf-Zertifikaten (z.B. bei Nutzung des S/MIME-Gateways) können Zertifikate nun über die Managed-PKI-Schnittstelle (MPKI) einer CA automatisiert beantragen und verlängern. Die Funktion ist noch als experimentell anzusehen und unterstützt aktuell nur die CA SwissSign. Gerne fügen wir weitere CAs hinzu. Dazu benötigen wir die Schnittstellenbeschreibung und einen Testzugang.

3.2.1.2 Neue Kategorien im kommerziellen URL-Filter

Hinzugefügt wurden die Kategorien Alkohol, weiche Drogen, geparkte Domains und KI-Chats.

3.2.2 Update

3.2.2.1 Avira Antivirus

3.2.3 Sicherheitskritisch

3.2.3.1 Sicherheitslücken in diversen Komponenten

Das Update behebt weniger kritische Sicherheitslücken im Linux-Kernel, IPsec-Server, Web-Proxy, DNS, Java und in System-Bibliotheken.

3.2.4 Bugfix

3.2.4.1 Transparentes HTTPS-Proxying mit Chromium-Browsern

Mit dem Update auf Chromium 124 ist es auf Chromium basierenden Browsern wie Chrome oder Edge nicht mehr möglich gewesen, mittels transprentem HTTPS-Proxying auf Internet-Seiten zuzugreifen

3.2.4.2 Beschädigte Header im S/MIME-Gateway

In Version 7.2-1.5 wurde beim Ändern langer Betreff-Zeilen und des Content-Types ein Steuerzeichen eingefügt, das manchen Systemen dazu geführt hat, dass der Betreff abgeschnitten oder die verschlüsselte Mail nicht gelesen werden konnte.

3.2.4.3 Kleinere Bugfixes und Verbesserungen

3.3 Version 7.2-1-5

3.3.1 Neu

3.3.1.1 DMARC-Verifikation von eingehenden Mails

Neben SPF können per SMTP aus dem Internet empfangene Mails nun auch über DMARC verifiziert werden. DMARC kombiniert SPF mit DKIM. Die Prüfung ist erfolgreich, wenn entweder SPF oder DKIM erfolgreich geprüft werden konnten und zusätzlich der im Mailprogramm angezeigte Absender (From-Header) zur SPF- bzw. DKIM-Domain passt. Wie bei SPF entscheidet der Inhaber einer Domain, ob Empfänger von Mails aus seiner Domain überhaupt eine DMARC-Verifikation durchführen können und was im Fehlerfall zu tun ist: die Mail abweisen, als potentiellen SPAM behandeln oder einfach passieren lassen.

3.3.1.2 Optionen zur Abholung und zum Versand von Mails

Zur Unterstützung von Arztpraxen, die die Schutzfunktionen des Mail-Servers gegen Schadsoftware auch für die Kommunikation mit KIM (Kommunikation im Medizinwesen) nutzen wollen, wurden diverse Konfigurationsoptionen ergänzt. Damit sollte eine Verbindung mit allen Varianten und Konfigurationen von KIM-Clientmodulen möglich sein. Im POP-Client lässt sich nun ein Client-Zertifikat hinterlegen und der Server-Port (hier: Port des KIM-Clientmodul) frei konfigurieren. Für den Versand von Mails ist ebenfalls der Server-Port (KIM-Clientmodul) frei konfigurierbar. Zudem wird nun auch für ausgehende Verbindungen SMTPS unterstützt und beim Routing einer externen Domain (hier: kim.telematik) lassen sich Zugangsdaten hinterlegen.

3.3.1.3 Automatisches Mailbackup je Benutzer

Das Backup der lokalen Postfächer konnte bisher nur als eine große Datei erstellt werden. Um bei der Erstellung des Backups weniger Speicherplatz zu benötigen, ist jetzt auch eine Datei pro Benutzerkonto möglich.

3.3.2 Bugfix

3.3.2.1 Verbindungsabbrüche bei Windows-IKEv2 IPsec-Verbindungen

Beim Re-Keying, das typischerweise nach einer Stunde stattfindet, kam es zu Verbindungsabbrüchen.

3.3.2.2 Download von URL-Filter-Listen im UTF-8-Format

Listen im UTF-8-Format wurden bisher nicht importiert.

3.3.2.3 Kleinere Bugfixes und Verbesserungen

3.4 Version 7.2-1-4

3.4.1 Neu

3.4.1.1 DKIM-Signaturen für E-Mails

Ausgehende Mails können jetzt mit DKIM signiert werden. Legen Sie dazu im Schlüsselbund einen neuen Eintrag vom Typ "RSA-Schlüssel (SSH, DKIM)" an und generieren Sie das Schlüsselpaar. Publizieren Sie dann den öffentlichen Schlüssel im DNS der zu signierenden Domain. Sobald Sie in der Domain-Konfiguration des Mail-Servers den DKIM-Schlüssel festlegen einer Domain festlegen, werden die ausgehenden Mails signiert. Haben Sie im DNS der Domain auch SPF konfiguriert? Dann können Sie nun auch einen DMARC-Eintrag im DNS hinterlegen.

3.4.1.2 Assistent für die Anbindung von Wireguard-Clients

Bisher gab es einen gemeinsamen Assistenten für die Anbindung von Routern und Clients. Aufgrund häufiger Fehlkonfiguration haben wir einen speziell auf die Anbindung von Clients abgestimmten Assistenten ergänzt.

3.4.2 Sicherheitskritisch

3.4.2.1 Sicherheitslücken in diversen Komponenten

Das Update behebt weniger kritische Sicherheitslücken im Linux-Kernel, dem SSH-Server und in System-Bibliotheken.

3.4.3 Update

3.4.3.1 Cluster-Dienst

3.4.4 Bugfix

3.4.4.1 Kleinere Bugfixes und Verbesserungen

3.5 Version 7.2-1-3

3.5.1 Neu

3.5.1.1 OpenVPN Benutzeranmeldung mit Passwort

Bisher wurden ausschließlich Einmal-Passwörter zur Benutzeranmeldung am OpenVPN-Server unterstützt. Ab sofort ist es auch möglich, sich nur mit dem Benutzerpasswort oder mit Benutzerpasswort und Einmal-Passwort anzumelden.

3.5.1.2 Individuelle Zugangsdaten für Mailversand über Provider-Relay

Je Absender-Adresse (Envelope-From) lassen sich jetzt individuelle SMTP-Zugangsdaten für den Versand ausgehender Mails konfigurieren.

3.5.1.3 Unterstützung für indirekte Netze im DHCP-Server

Der DHCP-Server für IPv4 kann nun auch für Netzwerke eingesetzt werden, die über ein DHCP-Relay kommunizieren müssen.

3.5.2 Änderung

3.5.2.1 Netzwerk 239.255.255.0/24 auf Bridge-Schnittstellen

Für Multicast-Pakete zu IPs aus dem Netz 239.255.255.0/24 muss keine Route mehr konfiguriert werden.

3.5.3 Update

3.5.3.1 Neue OpenVPN-Version

OpenVPN wird mit diesem Update aktualisiert. Bitte beachten Sie, dass in der neuen Version die Netzmaske für das Transfernetz ausreichend groß gewählt werden muss. Die Netzmasken 255.255.255.252 und 255.255.255.248 sind nicht mehr zulässig. Die Voreinstellung 255.255.255.0 ist mehr als ausreichend.

3.5.3.2 Diverse Systemkomponenten

Aktualisiert werden u.a. der Web-Server und das Archivierungswerkzeug tar. Dadurch behobene Sicherheitslücken befinden sich in nicht genutzten Teilkomponenten.

3.5.4 Bugfix

3.5.4.1 Diverse Bugfixes für IPsec ab Version 7.2

Bei IPsec-Verbindungen über eine ADSL-Schnittstelle fehlte in bestimmten Konfigurationen nach dem Neuaufbau der ADSL-Verbindung eine Route. Die IPsec-Verbindung war in diesem Fall zwar aufgebaut, es konnten jedoch keine Daten übertragen werden.
Transparentes Proxying in ipsec-Schnittstellen funktionierte nur, wenn es mit Hilfe von DNAT-Regeln konfiguriert wurde. Die Häkchen für transparentes Proxying zeigten keine Wirkung.
IKEv2-Verbindungen zu Gegenstellen hinter einem NAT-Router wurden durch die Dead-Peer-Detection nicht neu gestartet, wenn sich die IP-Adresse des NAT-Routers ändert

3.5.4.2 Absturz des Web-Proxies

Das Update behebt einen Fehler, über den ein bösartiger Web-Server den Proxy zum Absturz bringen könnte.

3.5.4.3 Kleinere Bugfixes und Verbesserungen

3.6 Version 7.2-1-2

3.6.1 Neu

3.6.1.1 Nutzung des Windows Zertifikatsspeichers mit OpenVPN

Neue Varianten der Windows-Installationspakete für OpenVPN können das Schlüsselpaar im Zertifikatsspeicher von Windows ablegen. Für normale Verbindungen wird der Zertifikatsspeicher des Benutzers verwendet. Bei Paketen für PLAP/SBL (Start-before-Login) muss der Schlüssel im Zertifikatsspeicher des Computers abgelegt werden.

3.6.1.2 Automatischer Download von URL-Listen

Bisher konnten URL-Filter-Listen nur manuell gepflegt oder manuell importiert werden. Jetzt lassen sich auch URL-Filter-Listen anlegen, die regelmäßig URL-Listen von einem Web-Server herunterladen. Die Listen dürfen dabei ganze Domains, URLs, IP-Adressen und Suchmuster wie z.B. "example.*" enthalten.

3.6.2 Bugfix

3.6.2.1 IPsec-L2TP und IPsec mit IPComp Komprimierung

Bei IPsec-L2TP-Verbindungen kam es bei manchen Installationen zu sporadischen Routing-Fehlern. Bei IPsec mit aktivierter Komprimierungsoption wurden einzelne Pakete fälschlicherweise von der Firewall verworfen.

3.6.2.2 Kleinere Bugfixes und Verbesserungen

3.7 Version 7.2-1-1

3.7.1 Sicherheitskritisch

3.7.1.1 Sicherheitslücken im Web-Proxy

Im Web-Proxy wurden diverse Sicherheitslücken behoben. Besonders kritisch ist die Möglichkeit für einen Angreifer eigenen Code zur Ausführung bringen, sofern Benutzeranmeldung mit Digest-Authentifizierung aktiviert ist. Über eine weitere kritische Lücke war es möglich, Anfragen oder Antworten mittels widersprüchlicher Angaben durch den Proxy zu schmuggeln.

3.7.2 Neu

3.7.2.1 Wireguard DNS-Suffix

Beim Erstellen von Wireguard-Konfigurationen für Gegenstellen lässt sich jetzt ein DNS-Suffix angeben.

3.7.3 Bugfix

3.7.3.1 IPsec Verbindungen zu Clients

In Version 7.2-1.0 wurden Verbindungen vom Typ "Windows IKEv2" wegen eines Fehlers in der Konfiguration nicht geladen. Gleiches galt für Verbindungen vom Typ "Client", wenn IKEv2 als Protokoll ausgewählt und keine virtuelle IP konfiguriert war.

Beim Erstellen von Installationspaketen für Windows IPsec-L2TP (Powershell) wurden fälschlicherweise Installationspakete für Windows IKEv2 ausgeliefert.

3.7.3.2 Kleinere Bugfixes und Verbesserungen

3.8 Version 7.2-1-0

3.8.1 Update

3.8.1.1 IPSec

Der IPsec-Dienst wird aktualisiert und nutzt ab sofort eine in den Linux-Kernel integrierte Schnittstelle anstelle eines eigenen Moduls.

Mit der alten IPsec-Version war es bedingt möglich, dass sich mehrere IPsec-L2TP-Clients gleichzeitig über den selben (!) NAT-Router mit dem selben VPN-Server verbinden. Dies ist in der neuen Version im Allgmeinen nicht mehr möglich. Sollten Sie auf dieses Szenario angewiesen sein, empfehlen wir den Wechsel auf IKEv2-Verbindungen oder auf OpenVPN. Das Update wird abgebrochen, sollten zu Beginn des Vorgangs mehrere IPsec-L2TP-Clients über den selben NAT-Router verbunden sein.

Ein neuer IPsec-Verbindungtyp "Windows IKEv2" soll die Migration auf IKEv2-Verbindungen erleichtern. Mittelfristig steht zu erwarten, dass die Betriebssysteme die Unterstützung von IPsec-L2TP einstellen. Leider steht bei IKEv2 jedoch noch keine kombinierte Authentifizierung aus Computerzertifikat und Benutzerlogin zur Verfügung. Für Mehrfaktor-Authentifzierung empfehlen wir den Wechsel auf OpenVPN.

Die IKEv2-Interoperabilität mit anderen Produkten wurde verbessert.

Der Status von IPsec-Verbindungen lässt sich nun auch in Form eines Docklets auf der Startseite verfolgen.

3.8.2 Neu

3.8.2.1 OpenVPN-Installationspaket für Windows mit SBL/PLAP

Eine zusätzliche Variante des OpenVPN-Installationspakets für Windows sorgt dafür, dass unter Windows Start-Before-Login (SBL) mittels Pre-Logon-Authentication-Provider (PLAP) genutzt werden kann. Auf dem Anmeldebildschirm von Windows erscheint ein zusätzliches Icon, über das sich der VPN-Tunnel schon vor der Benutzeranmeldung aufbauen lässt. Über den VPN-Tunnel kann dann eine Windows-Benutzeranmeldung direkt an der Windows-Domäne erfolgen.

Unter Windows muss dazu OpenVPN-GUI ab Version 2.6 installiert sein. Die Absicherung des VPN-Tunnels mit Einmalpasswörtern ist möglich.

3.8.2.2 Wireguard-VPN

Mit Wireguard hält eine weitere VPN-Variante zur Anbindung von Clients und VPN-Routern Einzug. Die Authentifizierung erfolgt dabei ausschließlich über ein Public-Key-Verfahren. Eine zusätzliche Benutzerauthentifzierung oder Einmal-Passwörter sind in Wireguard nicht verfügbar.

Wir empfehlen, IPsec-Verbindungen mit Fritz!Boxen auf Wireguard umzustellen, da diese IPsec nach wie vor nur mit Preshared-Key authentifizieren können. Seitens der Fritz!Box steigt dadurch zudem der Durchsatz.

3.8.2.3 Anwendungserkennung in der Firewall

In der Firewall lässt sich jetzt eine Anwendungserkennung zuschalten. Sie analysiert die über eine Netzwerkverbindung übertragenen Daten und versucht daraus auf die zugehörige Anwendung zu schließen.

Nutzen lässt sich die Anwendungserkennung im Bandbreitenmanagement und in Firewall-Regeln (ausgenommen SNAT-Regeln). Den Einsatz in Firewall-Regeln empfehlen wir nur eingeschränkt, da eine Regel mit aktivierter Anwendungserkennung für die Analyse zunächst alle potentiell in Frage kommende Verbindungen passieren lassen muss. Die Firewall wird dadurch "löchrig", was ein gerne verschwiegener Nachteil der bei Next-Generation-Firewalls

beworbenen Anwendungserkennung ist. Für HTTP und HTTPS ist bei eingehenden Verbindungen der Reverse-Proxy, bei ausgehenden Verbindungen der Web-Proxy zu bevorzugen.

Um die Anwendungserkennung zu nutzen, müssen Sie diese zunächst in den Firewall-Einstellungen aktivieren. Die erkannten Anwendungen werden dann im Firewall-Monitoring bei den Verbindungen angezeigt. Für die Nutzung im Bandbreitenmanagement und in Firewall-Regeln lässt sich im Definitionen-Menü bei den einzelnen Protokollen die zugehörige Anwendung festlegen. Bei vordefinierten Protokollen ist die Anwendungserkennung deaktiviert.

3.8.2.4 Export von Definitionen

Objekte aus den Menüs unterhalb von "Definitionen" lassen sich jetzt exportieren und auf anderen Systemen über das Backup-Menü einspielen. Das Zielsystem darf dabei jedoch keine ältere Softwareversion haben als das Quellsystem.

3.8.2.5 Virenscan von Postfächern

Wenn das System als Mail-Server mit Postfächern genutzt wird, können diese ab sofort täglich auf Viren geprüft werden. Mails mit Viren, die zum Zeitpunkt des Eintreffens der Mail noch nicht vom Virenscanner erkannt wurden, werden dann im Nachhinein aussortiert. Eine E-Mail-Benachrichtigung wird in diesem Fall an den jeweiligen Benutzer und an den "admin" gesendet.

Um das System nicht zu stark zu belasten, ist der Virenscan auf neuere Mails beschränkt. Das Alter in Tagen, bis zu dem die Mails regelmäßig überprüft werden, muss konfiguriert werden.

3.8.2.6 S/MIME-Gateway: automatisches Löschen abgelaufener Zertifikate

Das S/MIME-Gateway sammelt auf Wunsch selbständig Zertifikate von Kommunikationspartnern, um Mails an diese Kommunikationspartner zukünftig automatisch zu verschlüsseln. Abgelaufene Zertifikate von Kommunikationspartnern können jetzt nach einer konfigurierbaren Zeitdauer automatisch gelöscht werden.

3.8.2.7 S/MIME-Gateway: Ausnahmeliste für das automatische Signieren

Es kann vorkommen, dass bestimmte Empfänger keine signierten Mails annehmen. Zu diesem Zweck lassen sich jetzt einzelne Empfängeraddressen oder ganze Empfängerdomains in eine Liste eintragen. Mails zu diesen Empfängern werden nicht automatisch signiert.

3.8.2.8 Verschlüsselung von Backups

Optional können die vom System erzeugten Backups nun verschlüsselt werden. Aber Vorsicht: Sollte das Kennwort zu den Backups verloren gehen, ist das Backup nutzlos!

3.8.2.9 Portnummer für Backups mit Secure-Copy

Backups mit SSH/SCP können jetzt an beliebige Ports übermittelt werden.

3.8.2.10 Syslog- und TFTP-Server

Zur Unterstützung von aktiven Netzwerkkomponenten, die ausschließlich über flüchtigen Speicher verfügen, sind jetzt Syslog- und TFTP-Server verfügbar.

3.8.3 Änderung

3.8.3.1 Protokollmodule in der Firewall (ALGs)

Manche Protokolle bestehen aus mehreren voneinander abhängigen Verbindungen. Für häufig benutzte gibt es in der Firewall Module, die sich um das Zuordnen und Freischalten abhängiger Verbindungen kümmern. Manchmal werden diese Module auch Application-Level-Gateways (ALGs) genannt.

Aus Sicherheitsgründen wird empfohlen, diese Module nicht grundsätzlich zu aktivieren. Besser ist es, nur die tatsächlich benötigten Module anzuschalten und - sofern möglich - die Nutzung auf einzelne Clients oder Server zu beschränken.

Das Update prüft, ob die Module für FTP, SIP, H.323, PPTP und IRC benötigt werden. Das ist der Fall, wenn entweder eine aktive Verbindung mit dem jeweiligen Modul oder eine Firewall-Regel mit den entsprechenden Ports gefunden wird. Bei FTP und SIP wird zusätzlich geprüft, ob die entsprechenden Proxy-Dienste aktiviert sind. Das entsprechende Modul wird dann für die Kommunikation mit beliebigen IP-Addressen aktiviert. In den Firewall-Einstellungen lässt sich die Konfiguration dann weiter anpassen.

Bei Neugeräten sind in der Grundkonfiguration zukünftig alle Module deaktiviert.

3.8.3.2 TLS-Parameter der Administrationsoberfläche

Die Administrationsoberfläche kann ab sofort nicht mehr mit veralteten Browsern aufgerufen werden. Die Unterstützung von TLS1.0, TLS1.1, 3DES und SHA1 wurde deaktiviert.

3.8.3.3 Überarbeitung des Menüs "Monitoring"

Bei den Untermenüs "Log-Dateien > Einstellungen" und "Netzwerk > SNMP" handelte es sich um Konfigurationsmenüs. Konsequenterweise wurden die Menüs daher in das Hauptmenü "Module" verschoben. Die neuen Untermenüs haben dort die Titel "SNMP-Server" und "Logging".

Die zweite Menüebene des Menüs "Monitoring > Netzwerk" wurde vollständig aufgelöst. Die neuen Menüpunkte "Werkzeuge", "Netzwerk", "VPN", "Firewall" und "DHCP" finden Sie nun direkt unter "Monitoring".

Der Bereich "Monitoring" in den thematisch gegliederten Menüs am oberen Rand der Administrationsoberfläche wurde entsprechend angepasst und um direkte Links auf zugehörige Log-Dateien erweitert. Im VPN-Menü wurde Wireguard ergänzt.

3.8.3.4 Optimierungen im Layout der Administrationsoberfläche

3.8.3.5 Sonderzeichen in Passwörtern

Beim Setzen oder Ändern von Passwörtern über die Administrationsoberfläche werden enthaltene Sonderzeichen wie z. B. Umlaute zukünftig in UTF-8-Kodierung weiterverarbeitet. Alle aktuellen Browser und die Mehrheit sonstiger Clients arbeitet ebenfalls mit UTF-8. Einzelne Clients und Protokolle können aber nach wie vor nicht damit umgehen, so dass die Nutzung solcher Sonderzeichen nicht empfohlen wird.

3.8.3.6 Zeitsynchronisation

Die Zeitsynchronisation findet nun ausschließlich über NTP statt. Die Routinen wurden überarbeitet, um insbesondere beim Neustart des Systems sicherzustellen, dass die Systemzeit korrekt ist.

3.8.3.7 Der telnet-Dienst wurde entfernt

3.8.4 Bugfix

3.8.4.1 Kleinere Bugfixes und Verbesserungen

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