XnetSolutions

SX-GATE

Software Update
Release Note

Version: 7.0-2-0

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.

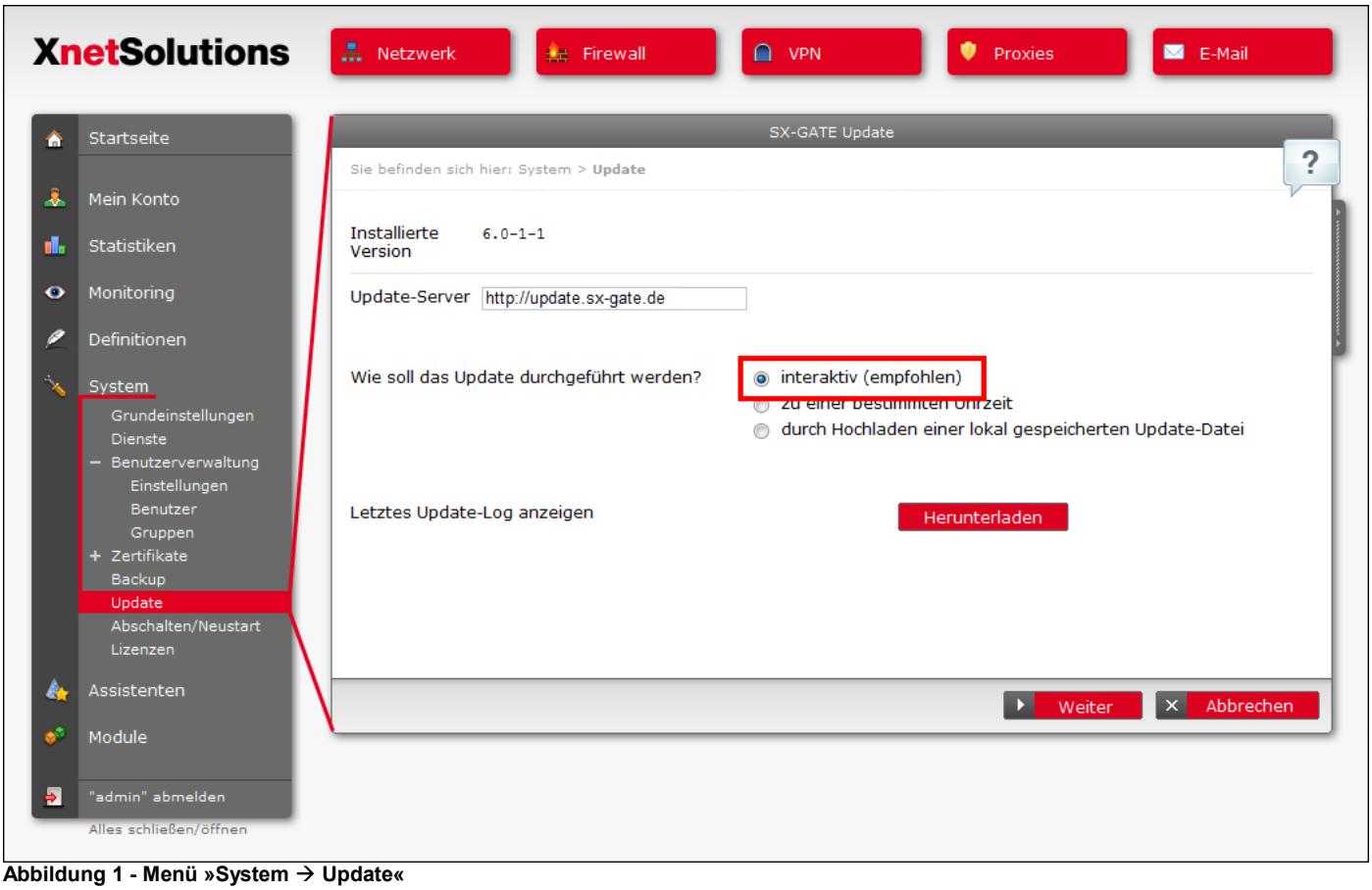

Abbildung 1 - Menü »System → Update«

- **Manuelles Software-Update**

Bevor Sie das Software-Update durchführen können ist es erforderlich, dass Sie das benötigte Software-Update Version 7.0-2-0 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.

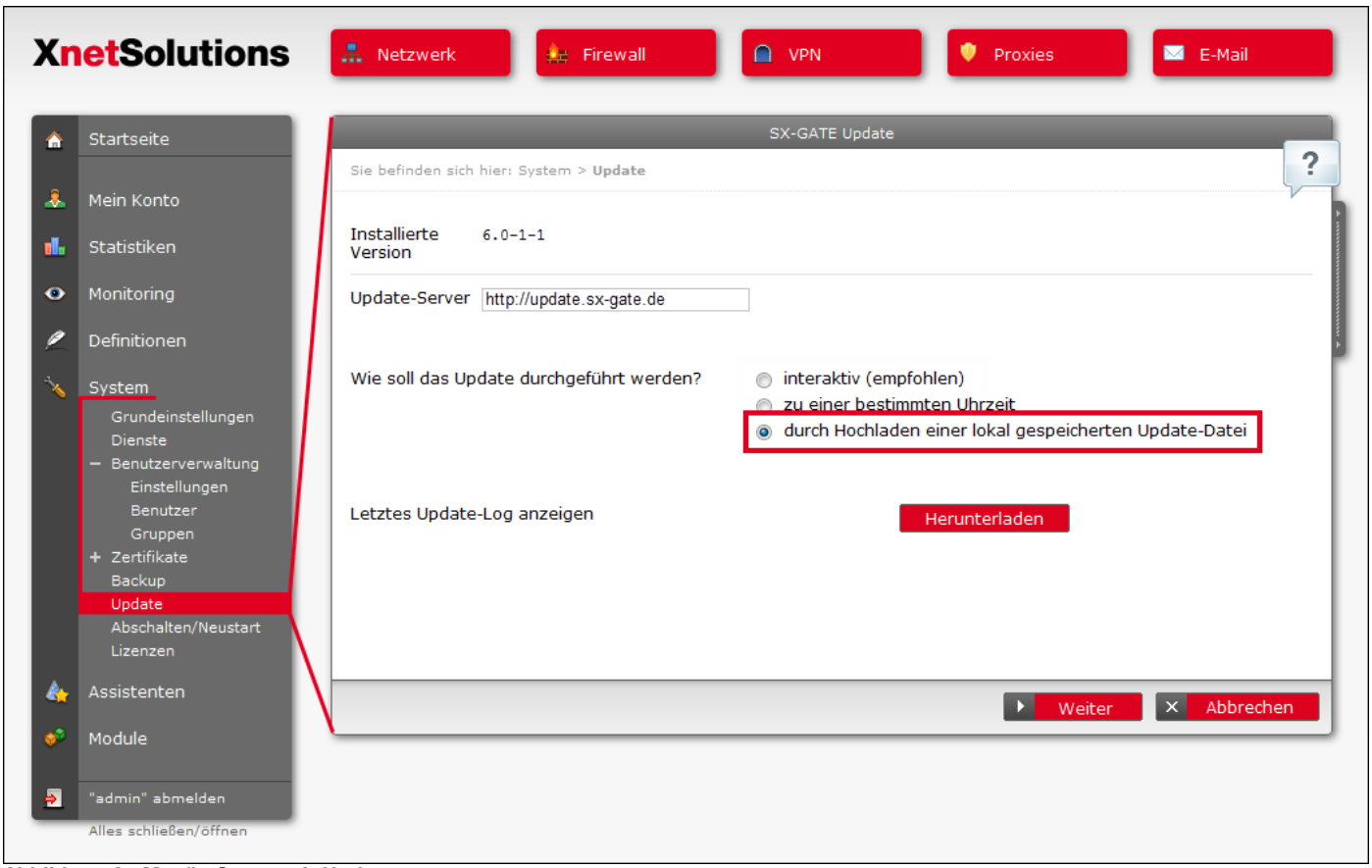

Abbildung 2 - Menü »System → Update«

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.

2.1 Neustart erforderlich

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

2.2 Sicherheitskritisch

2.2.1 Aktualisierung des Linux-Kernels

Im Linux-Kernel wurden zwei Sicherheitslücken beseitigt, die es lokalen Benutzern erlauben, erweiterte Zugriffsrechte zu erlangen.

2.3 Neue Funktionen

2.3.1 Erweiterte Möglichkeiten bei der Filterung von E-Mail Dateianhängen

Bisher wurden beanstandete Anhänge aus der E-Mail entfernt und durch eine Warnung ersetzt. Die so veränderte Mail wurde an die Empfänger ausgeliefert, die entfernten Anhänge in einem Quarantäneverzeichnis abgelegt. Ab sofort steht ein zweites, alternatives Verfahren zur Verfügung. Hierbei wird die komplette E-Mail zurückgehalten. Die Empfänger erhalten lediglich eine Benachrichtigungsmail aus der u.a. Absender, Betreff und die beanstandeten Anhänge hervorgehen. In der Administrationsoberfläche kann die unter Quarantäne gestellte E-Mail mit einem einfachen Klick zur Zustellung freigegeben werden.

Um den Administrator zu entlasten, kann dieser den Empfängern erlauben, unter bestimmten Voraussetzungen selbst auf den Quarantänebereich zuzugreifen. Abhängig vom gewählten Quarantäne-Verfahren erhalten die Empfänger entweder Links zum Herunterladen der entfernten Anhänge oder einen Link über den die zurückgehaltene E-Mail zur Zustellung freigegeben wird.

Grundsätzlich müssen folgende Voraussetzungen erfüllt sein, damit der Benutzer Zugriff auf die Quarantäne erhält:

- Es wurde in der E-Mail noch kein Virus entdeckt
- Die E-Mail enthält keine "gefährlichen Dateianhänge". Für E-Mails mit "gefährlichen Dateianhängen" wird dem Empfänger kein Link zugesandt. Ggf. müssen Sie häufig beanstandete aber dennoch benötigte Dateianhänge in der Konfiguration von der Liste der "gefährlichen" auf die Liste der "verbotenen" Anhänge umtragen.
- Der Administrator hat den Zugriff erlaubt und die dabei festgelegten Vorbedingungen sind erfüllt

Folgende Vorbedingungen kann der Administrator festlegen:

- Die E-Mail wurde in der Zwischenzeit mit aktualisierten Virenscanner-Signaturen erneut gescannt
- Zusätzlich hat die E-Mail eine konfigurierbare Zeitdauer in der Quarantäne verbracht

2.3.2 Import und Export von Konfigurationstabellen

In der Administrationsoberfläche lässt sich der Inhalt vieler Tabellen nun exportieren und importieren. Auf diese Weise lassen sich z.B. Konfigurationen zwischen Geräten austauschen oder innerhalb des Geräts beispielsweise von einer Schnittstelle auf die andere übertragen. Auch der Import externer Daten wie z.B. Adresslisten ist möglich, sofern die Daten im passenden Format vorliegen.

2.3.3 Konfigurierbare Proxy-IP in Proxy-Autokonfigurations-Datei auf Cluster-Systemen

2.3.4 Externe Archivierung des Reverse-Proxy Logs nun in Oberfläche konfigurierbar

2.4 Änderung

2.4.1 Filterung von E-Mail Dateianhängen bei ausgehenden E-Mails

Sofern der Dateianhangs-Filter auch bei ausgehenden E-Mails aktiviert ist, werden ausgehende E-Mails mit beanstandeten Anhängen ab sofort zurückgewiesen und nicht mehr unter Quarantäne gestellt.

2.5 Update

2.5.1 Externe Archivierung des Reverse-Proxy Logs nun in Oberfläche konfigurierbar

2.5.2 URL-Filter Datenbank

2.5.3 Aktualisierung diverser Software-Komponenten

2.6 Bugfix

2.6.1 Aktualisierung der Virenscanner von Avira, F-Secure und Kaspersky

Das Update behebt gelegentliche Abstürze des F-Secure Scanners.

Die Konfiguration der drei Scanner wurde bezüglich der max. Anzahl gleichzeitiger Scanprozesse und der Prozesspriorität aneinander angeglichen.

2.6.2 Speicherleck im IPsec-Server

Auf Systemen, die aufgrund einer Fehlkonfiguration laufend erfolglos neue Verbindungen aufbauen, wuchs der Speicherbedarf des IPsec-Dienstes kontinuierlich.

2.6.3 Anzeigefehler im LCD-Display

Bei Geräten mit LCD-Display kam es seit dem Update auf Version 7.0 zu unterschiedlich stark ausgeprägten Anzeigefehlern und Problemen bei der Bedienung des Displays.

3 Änderungen in vorherigen Versionen

3.1 Version 7.0-1-2

3.1.1 Sicherheitskritisch

3.1.1.1 Aktualisierung des Linux-Kernels_2

Im Linux-Kernel wurde eine Sicherheitslücke beseitigt, die es lokalen Benutzern erlaubt, Dateien zu überschreiben, für die sie eigentlich nur Leserechte besitzen.

3.1.2 Neue Funktionen

3.1.2.1 Freigabe von gesperrten IPs in der dynamischen Firewall

Fälschlicherweise gesperrte IPs lassen sich im Monitoring der dynamischen Firewall nun direkt freigeben.

3.1.2.2 Sperrung von DNS-Antworten mit privaten IP-Adressen

Aktivieren Sie diese neue Option in der DNS-Konfiguration, um sich besser vor DNS-Rebind-Angriffen zu schützen.

3.1.2.3 Testmöglichkeit für Backup und Logdatei-Archivierung

Ob die konfigurierten Zugangsdaten für die automatische Erstelleung von Backups und für die Archivierung von Logdateien korrekt sind, kann nun mit Hilfe einer Testfunktion geprüft werden.

3.1.2.4 "Pause"-Schalter für Live-Log

3.2 Version 7.0-1-1

3.2.1 Neue Funktionen

3.2.1.1 Eingehende E-Mails mit Absenderadresse aus der eigenen Domain

Unerwünschte E-Mails nutzen häufig die Empfängerdomain in der Absenderadresse. Für diese Art von E-Mails gibt es nun zwei neue Optionen, die Sie jedoch nur dann aktivieren dürfen, wenn E-Mails mit der eigenen Domain ausschließlich über lokale Systeme in das Internet versendet werden.

Steht die lokale Domain im sog. Envelope-From, kann die Mail komplett abgewiesen werden. Bisher war dies nur mit aktiviertem SPF-Filter in Kombination mit einem restriktiven SPF-Eintrag für die eigene Domain möglich.

Die zweite Option greift, wenn die lokale Domain im From-Header steht. Der Inhalt des From-Headers wird dem Empfänger im Mailprogramm als Absender angezeigt. Einem gutgläubigen Mitarbeiter könnte über einen gefälschten From-Header vorgetäuscht werden, es handle sich z.B. um die E-Mail seines Vorgesetzten. Bei aktivierter Option wird dem Betreff der Text "*****FAKE***** [Sender]" vorangestellt.

3.2.1.2 Optionale IPS Regeln

Es lassen sich nun zusätzliche Intrusion-Prevention Regelsätze aktivieren, falls sie lokale Mail- oder Web-Server mit direktem Zugriff aus dem Internet betreiben.

3.2.2 Bugfix

3.2.2.1 Asymmetrisches Routing im LAN

In Version 7.0-1.0 funktionierte das asymmetrische Routing im LAN nicht.

3.2.2.2 IPsec-L2TP-Einwahl im Cluster

In Version 7.0-1.0 funktionierte die L2TP-Einwahl auf Clustersystemen nicht.

3.2.2.3 Last-Problem mit Web-Proxy

Das Update behebt ein Last-Problem im Web-Proxy Content-Filter.

3.2.2.4 Syntax-Fehler in Proxy-Autoconf-Datei

In Version 7.0-1.0 war die PAC-Datei fehlerhaft, sofern keine Netzwerke mit direkter Verbindung konfiguriert waren.

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