SX-GATE UTM-Appliance

Release Note – SX-GATE Software Version 5.2-1.5

November 2011

- **Bitte beachten Sie die Voraussetzungen bevor Sie dieses Update Installieren.**

  - Arbeitsspeicher mindestens 1024 MB (1GB)

  Sie können die aktuelle Speicherbestückung im Menüpunkt „Monitoring → System-Info" ermitteln.

  Für Fragen bzgl. der Softwareaktualisierung wenden Sie sich bitte an den technischen Support.

Neue Funktionen dieser Version

- **Bugfix: Aktualisierung des Linux-Kernels**

  Das Update behebt ein Problem in der dynamischen Firewall, das zum Einfrieren des Systems führen kann und einen Fehler in der Hardware-Erkennung großer IDE-Festplatten.

  Nach dem Update führt das System automatisch einen Neustart durch. Bitte führen Sie keinen manuellen Neustart aus.

- **Bugfix: IPSec-Server**

  Gegen den IPSec-Server ist ein Denial-of-Service Angriff bekannt geworden. Das Update behebt das Problem.

  In bestimmten Konstellationen wurden Clients und Servern mit dynamischer IP beim Verbindungsaufbau die falsche Konfiguration zugeordnet und dann aufgrund nicht zusammenpassender Parameter abgewiesen.

- **Neu: SNMPv3 Server**

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

  In dieser Versionsreihe nur auf Systemen mit Software Pflegevertrag verfügbar.

- **Neu: 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.

In dieser Versionsreihe nur auf Systemen mit Software Pflegevertrag verfügbar.

- **Update: F-Secure und Kaspersky Anti-Virus**

  Die Virenscanner von F-Secure und Kaspersky werden im Zuge des Updates aktualisiert.

- **Bugfix: DynDNS und Policy-Based-Routing bei Internet-Zugang über DHCP**

  Bei Internet-Verbindungen über DHCP (Kabelmodem) war es bisher nicht möglich, die zugewiesene IP-Adresse bei einem DynDNS-Anbieter zu aktualisieren. Ebenfalls problematisch war die Konfiguration von Routen, die an der erforderlichen Angabe eines Gateways scheiterte. Hier lässt sich nun der spezielle Wert "0.0.0.0" eintragen.

- **Neu: VLAN-ID für VDSL**

  Bisher war die VLAN-ID für VDSL-Verbindungen fest auf den Wert 7 eingestellt. Um auch Provider zu unterstützen, die mit anderen VLAN-IDs arbeiten, ist diese nun frei einstellbar.

- **Bugfix: Anlegen von VLAN-Schnittstellen**

  Seit Version 5.2-1.3 wurden neu angelegte VLAN-Schnittstellen im System nicht aktiviert.

- **Kleinere Bugfixes und Verbesserungen**

Bereits umgesetzte Änderungen

5.1-1.4

- **Bugfix: Aktualisierung des Linux-Kernels**

  Der neue Kernel 2.6.32.42 aus Version 5.2-1.3 führte auf einzelnen Systemen zu Abstürzen, deren Ursache bislang nicht geklärt werden konnte. Es wird nun wieder die ältere Version 2.6.32.28 installiert, erweitert um neue Funktionen und relevante Bugfixes aus den neueren Kerneln.

  Nach dem Update führt das System automatisch einen Neustart durch. Bitte führen Sie keinen manuellen Neustart aus.

- **Bugfix: Denial-of-Service gegen Web- und Administrations-Server**

  Mit Hilfe spezieller Anfragen war es möglich, den kompletten Speicher zu belegen.

- **Bugfix: Generierung der IDS-Statistik**

  Aufgrund eines Fehlers in Update 5.2-1.3 wurde die IDS-Statistik nicht mehr generiert.

5.1-1.3

- **Bugfix - Aktualisierung des Linux-Kernels**

  Die neue Version enthält einige kleinere Bugfixes und Neuerungen für zukünftige Erweiterungen. **Nach dem Update führt das System automatisch einen Neustart durch.** Bitte starten Sie das System nicht von Hand neu.

- **Bugfix - Neue Version des DNS-Servers**

  Gegen die alte Version war ein möglicher Denial-of-Service Angriff bekannt geworden.

- **Änderung - Verzicht auf Domain-Suffix suche**

  Wenn Systemdienste einen DNS-Namen nicht auflösen konnten, wurde bislang der lokale Domain-Name angehängt und eine erneute DNS-Auflösung versucht. Bei lokalen Domains mit Wildcard-DNS-Eintrag führt dies nun vermehrt zu Problemen, seit die ersten produktiven reinen IPv6-Server im Internet erreichbar sind.

- **Update - Aktualisierung der IDS-/IPS-Signaturen**

  Systeme, die nicht im Rahmen des Pflegevertrags täglich neue Signaturen erhalten, erhalten mit diesem Update neue Signaturen für die Intrusion-Detection und -Prevention.

- **Neu - Weitere Optionen für den kostenpflichtigen URL-Filter**

  Für "Soziale Netzwerke" ist nun eine eigene Kategorie verfügbar. Die dort enthaltenen Adressen waren bisher in anderen Kategorien einsortiert. Ein neuer Schalter ermöglicht es, Adressen die nicht in der Datenbank enthalten sind an den Hersteller zu übermitteln. Die Adressen werden nach Prüfung in zukünftige Versionen der Datenbank einsortiert.

- **Neu - 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.

- **Neu - Zugewiesener DNS für L2TP-Clients**

  Da Clients häufig der zentrale Windows-Server als DNS zugewiesen werdens soll, wird diese Einstellung nun schon im Assistenten abgefragt. In der L2TP-Schnittstelle lässt sich nun zudem ein sekundärer DNS konfigurieren.

- **Bugfix - IPSec-L2TP Verbindungen von Windows XP Clients mit gleicher NAT-IP**

  Ein Windows XP IPSec-L2TP Client hinter einem NAT-Router meldet seine interne IP-Adresse beim Verbindungsaufbau nicht. In Versionsreihe 5.1 war es daher möglich, gleichzeitig VPN-Verbindungen zu mehreren Windows XP Clients mit der gleichen internen IP-Adresse aufzubauen. Dies war in Versionsreihe 5.2 nicht mehr möglich, da nun die interne IP aus anderen Werten hergeleitet wird. Um bestehende Installationen wie bisher weiter betreiben zu können, erlaubt nun ein Kompatibilitätsschalter, das alte Verhalten wieder herzustellen.

- **Bugfix - Kleinere Bugfixes im POP3-/SMTP-Proxy**

- **Update - Neue Version des OpenVPN-Servers und –Clients**

- **Update - Neue Version des DHCP-Servers und –Clients**

- **Update - Optimierte Speichernutzung bei Generierung der Firewall-Statistik**

5.1-1.2

- **Bugfix - IPSec-Verbindungen mit Apple iPhone**

  Seit der vorherigen Version 5.2-1.1 schlugen IPSec-Verbindungen mit iPhone fehl, sofern die Verbindung über einen NAT-Router lief.

- **Bugfix - Uploads über Web-Proxy**

  Datei-Uploads via Proxy zu einzelnen Web-Server sind wegen Timeout abgebrochen.

5.2-1.1

- **Bugfix - HTTPS-Verbindungen über Web-Proxy**

  In den Versionen 5.1-4.0 und 5.2-1.0 wurden bei aktiviertem Virenscan Downloads über HTTPS extrem verlangsamt.

- **Bugfix - IDS/IPS mit Kabelmodem**

  Bei Internet-Zugängen über DHCP (Kabelmodem) wurde die dynamische IP-Adresse nicht als interne IP-Adresse behandelt. Legitime ausgehende Verbindungen wurden daher unter Umständen als verdächtige eingehende Verbindung durch die Intrusion-Detection/-Prevention blockiert.

- **Bugfix - Automatische IDS-Updates**

  Bei Geräten mit dem Zeichen "=" in der Hardware-ID wurde das automatische Signatur-Update der Intrusion-Detection fälschlicherweise verweigert.

- **Bugfix - Passthrough für IPSec-Verbindungen**

  In den Versionen 5.1-4.0 und 5.2-1.0 wurden geroutete IPSec-Nat-Traversal Pakete nicht mehr maskiert (NAT), wenn die Freigabe in der Firewall-Konfiguration auf der Maske für Quelle "LAN" konfiguriert war. Die IPSec-Clients im LAN konnten in diesem Fall keine VPN-Verbindung mehr in das Internet aufbauen.

- **Bugfix - Graphische Statistik zum Bandbreiten-Management**

  Seit Version 5.2-0.1 bzw. 5.2-1.0 wurden die Statistiken nicht mehr fortgeschrieben.

5.2-1.0

- **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.

- **Update - Aktualisierung der Linux-Kernels**

  Ab sofort sind auch mehr wie 3 GB Hauptspeicher nutzbar.

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

- **Neu - Überarbeitetes Intrusion-Detection-/ Intrusion-Prevention-System (IDS/IPS)**

  Die neue Version des IDS/IPS ist als aktive Komponente innerhalb der Firewall angesiedelt. Kritische Datenpakete werden automatisch blockiert.

  Zusätzlich lässt sich das IDS als passive Komponente an den Monitor-Port eines Switches anbinden. Dafür ist eine dedizierte Netzwerkkarte erforderlich. Hier lassen sich je nach Einsatzzweck weitere Regelsätze aktivieren. Auffällige IP-Pakete werden protokolliert.

  Die protokollierten Ereignisse zu beiden Einsatzzwecken werden in Form einer graphischen Statistik aufbereitet.

  Systeme mit Software-Pflegevertrag erhalten mehrmals pro Woche aktuelle Signaturen für die Intrusion-Detection und -Prevention. Mit der Installation dieses Updates wird die Aktualisierung automatisch aktiviert, sofern ein Lizenzschlüssel mit Pflegevertrag-Option erkannt wird.

- **Neu - Zahlreiche Erweiterungen im Reverse-Proxy**

  Für den Zugriff auf Exchange-Server unterstützt der Reverse-Proxy neben Outlook-Web-Access und Active-Sync nun auch Outlook-Anywhere. Alle drei Möglichkeiten lassen sich separat aktivieren.

  Es lassen sich nun beliebig viele virtuelle Hosts anlegen. Jedem Servernamen lassen sich so unabhängig voneinander eigene Hintergrundserver zuordnen. Vordefiniert ist der Standard-Host "*".

  Neben der Möglichkeit unterschiedliche Hintergrundserver über virtuelle Hosts auszuwählen, können Anfragen auch nach URL-Pfad verschiedenen Hintergrundservern zugeordnet werden. Authentifizierung und Lastverteilung lassen sich nach Bedarf je Pfad zuschalten.

  Die Verbindung zwischen Reverse-Proxy und Hintergrundserver kann jetzt auch mit HTTPS verschlüsselt werden.

- **Neu - Erweiterungen im Web-Proxy URL-Filter**

  Alternativ zur integrierten, kostenfreien URL-Datenbank kann nun auch eine deutlich umfangreichere, allerdings kostenpflichtige Datenbank genutzt werden. Jährliche Lizenzen, für Bildungseinrichtungen zum ermäßigten Preis, sind über den Fachhandel erhältlich. Die kostenpflichtige Datenbank empiehlt sich insbesondere für Schulen, die üblicherweise höhere Ansprüche an eine URL-Datenbank stellen.

Aber auch die kostenfreie URL-Datenbank wurde nochmals erweitert. Es stehen dort nun Datenbanken mit "unbedenklichen" Internet-Adressen zur Verfügung. Nutzen Sie diese Datenbanken wenn als Standardverhalten eingestellt ist, dass der Zugriff auf alle nicht explizit freigegebenen Adressen verweigert werden soll.

Unabhängig von der genutzten URL-Datenbank lässt sich beim Zugriff auf die gängigsten Suchmaschinen der Jugendschutzfilter erzwingen. Zudem bietet der URL-Filter eine neue Option zur Erkennung von Proxy-Tunneln in verschlüsselten Verbindungen in Ergänzung zu den bereits bestehenden Möglichkeiten im Content-Filter des Web-Proxies.

- **Neu - Web-Proxy Digest-Authentifizierung**

  Die Digest-Authentifizierung bietet die gesicherte Übertragung des Kennworts vom Browser zum Web-Proxy zu Lasten der Speicherung von Passwort-Äquivalenten im Benutzer-Backup. Die neue Methode steht nur bei lokaler Authentifzierung zur Verfügung. Vor deren Aktivierung müssen alle Benutzer die Kennwörter ändern, damit ein entsprechendes Passwort-Äquivalent erzeugt werden kann. Selbiges gilt, falls Benutzerkennwörter automatisiert aus dem ActiveDirectory importiert werden. Hier muss zuvor eine neue Version der Passwort-DLL im Windows-Server installiert werden.

- **Neu - Aktualisierter IPSec-Server**

  Die neue Version beseitigt Probleme Windows 7 Clients, bei denen es nach ein bis zwei Stunden zu Verbindungsabbrüchen kam.

  Bei der Erstellung von IPSec-L2TP-Installationspaketen für Windows-Clients lässt sich nun freigeben, dass der Client die eigene Internetverbindung auch dann nutzen kann, wenn der VPN-Kanal aufgebaut wurde. Bisher wurde das Standardgateway des Clients zwingend auf die VPN-Verbindung umgeschaltet.

  IPSec-Installationspakete können jetzt auch für Geräte in Außenstellen erzeugt werden um auf einfache Weise eine VPN-Verbindung zwischen den Standorten zu konfigurieren.

- **Änderung - Verbesserte Zertifikats-Dialoge**

  Die verschiedenen Dialoge für den Umgang mit Zertifikaten wurden teilweise überarbeitet. Über Verkettung der einzelnen Dialoge werden typische Folgen von Arbeitsschritten abgebildet, so dass zukünftig notwendige Schritte nicht mehr so leicht vergessen werden können.

- **Änderung - Wegfall der Autostart-Option**

  Ob ein Dienst nach einem Neustart des Systems automatisch wieder gestartet wird oder nicht, wird durch explizites Starten bzw. Stoppen des Dienstes festgelegt. Bisher wurde dies über einen eigenen Schalter festgelegt.

- **Neu - Graphische Statistik der Firewall-Meldungen**

- **Neu - Externe Archivierung der Administrations-Logs**

- **Folgende Features konnten bereits in den 5.1er Versionen auf Systemen mit Software-Pflegevertrag genutzt werden. In Version 5.2 sind diese Funktionen nun auf allen Systemen verfügbar.**

- **Neu - Neue Mail-Server Optionen zur SPAM-Abwehr**

  Bei der SMTP-Kommunikation muss sich das zustellende System mit seinem Rechnernamen anmelden. Ist diese Angabe unvollständig oder offensichtlich gefälscht, wird die Verbindung abgelehnt.

  Ein weiterer Test prüft, ob für das zustellende System ein Reverse-Eintrag im DNS zu finden ist. In erweiterter Form muss zudem ein dazu passender Forward-Eintrag existieren.

  Die bisherige Prüfung nach gültigen Absenderdomains wurde erweitert. Wenn gewünscht muss die Domain nicht nur existieren, es muss auch ein Mail-Server mit gültiger IP-Adresse angegeben sein.

- **Neu - PGP-/ S/MIME-Filter**

  Der Filter hilft bei der Umsetzung interner Richtlinien, nach denen an bestimmte Empfänger ausschließlich verschlüsselte Mails gesendet werden dürfen. Ausgehende Mails, die versehentlich nicht mit PGP, GPG oder S/MIME verschlüsselt wurden, werden vom Filter zurückgewiesen.

- **Neu - E-Mail Lesebestätigung unterdrücken**

  Eine neue Option im Mail-Server ermöglicht es, bei eingehenden E-Mails zentral die Anforderungen von Lesebestätigungen (Message Disposition Notifications, MDNs) zu unterdrücken.

- **Neu - Web-Proxy Content-Type Filter**

  Im Web-Proxy lassen sich nun Zugriffe anhand des Typs sperren (z.B. "video/*").

- **Neu - Internetzugang über UMTS**

  Mit Hilfe eines zertifizierten UMTS-USB-Sticks lassen sich Internetverbindungen über UMTS/GPRS herstellen. Die UMTS-Verbindung kann als regulärer Internetzugang genutzt werden, bietet sich aber auch als Fallback für eine ADSL-Leitung an.

- **Neu - Netwerkverbindungs-Monitoring**

  Eine neue Monitoring-Funktion zeigt alle Netzwerk-Verbindungen die in den letzten Sekunden aktiv waren mit der insgesamt seit bestehen der Verbindung übertragenen Datenmenge.

- **Neu - Anzeige der vom DHCP-Server vergebenen Adressen**

Hinweis

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 bitte 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 Rückmeldung.

SX-GATE UTM-Appliance

Richten Sie diese bitte an: support@xnetsolutions.de

Erstellt am: 02.10.2011