

10/2008

IT-ADMINISTRATOR.DE

# **i**Administrator

Das Magazin für professionelle System- und Netzwerkadministration

**Im Test:  
alt-n technologies  
SecurityGateway  
Die Guten ins Töpfchen,  
die Schlechten ins Kröpfchen**

**Sonderdruck  
für EBERTLANG**

**Im Test:** alt-n technologies SecurityGateway

# Die Guten ins Töpfchen, die Schlechten ins Kröpfchen

von Sandro Lucifora



Administratoren verwenden einen erheblichen Teil ihrer Arbeitszeit auf das Aussortieren unerwünschter Nachrichten. Viren, Pishing und Spoofing stellen eine weitere Gefahr für den Mailserver dar. Um diesen aus der direkten Schusslinie zu nehmen und Spam-Nachrichten schon vorher aus dem Verkehr zu ziehen, bietet sich der Einsatz eines SMTP-Gateways wie "SecurityGateway for Exchange/SMTP Servers" aus dem Hause alt-n technologies an. Ob das Produkt auch wirklich die schlechten von den guten Nachrichten unterscheiden kann und sich als wirkungsvoller Torwächter vor dem Mailserver anschickt, stellen wir in unserem Test fest.

**E**lektronische Post wird von SMTP-Server zu SMTP-Server übertragen. Damit der Datentransfer funktioniert, muss der SMTP-Server ständig über Port 25 aus dem Internet erreichbar sein. Wenn derselbe Server zudem POP3 anbietet oder sogar den kompletten Nachrichtenspeicher beherbergt, wird die digitale Angriffsfläche immer größer. Um dennoch E-Mails direkt zu empfangen und gleichzeitig den E-Mailserver sicher in der geschützten Zone des Intranets zu belassen, bietet sich die Installation eines separaten SMTP-Gateways an. Nur das SMTP-Gateway ist dann aus dem Internet erreichbar und dient als vorgeschalteter SMTP-Server. Zusätzlich scannt dieser Dienst die eingehende Post und filtert Spam und Viren heraus.

Genau diese Funktionen bietet das "SecurityGateway" von alt-n technologies. Die Software nimmt E-Mails an, prüft sie in einem mehrstufigen Verfahren auf Berechtigung und Qualität und liefert die für legitim befundene Post an den finalen Mail-

server aus. Die Vorteile dieses Verfahrens liegen auf der Hand: Das Gateway lässt sich Hersteller-unabhängig in jedes bestehende Mail-System integrieren, ohne dass der Administrator die bestehende Mailserver-Konfiguration ändern muss.

## Installation und Konfiguration

Nach den üblichen Installationsprozeduren legten wir zunächst die Art des Verification Servers fest. Bei dieser Funktion sehen wir für das Gateway bereits einen ersten Pluspunkt, erlaubt diese

Option doch, schon im Voraus festzulegen, für welche E-Mailempfänger überhaupt Mails entgegengenommen werden. Diese Angaben können manuell direkt am Gateway-Server erfolgen. Meist sind die E-Mailempfänger aber schon anderweitig definiert. Bei größeren Umgebungen – oder schlicht um sich unnötige Arbeit zu ersparen – ist daher die Rückversicherung über das Active Directory und den Exchange Server oder einen beliebigen LDAP-Server die erste Wahl. Bei der Verwendung einer

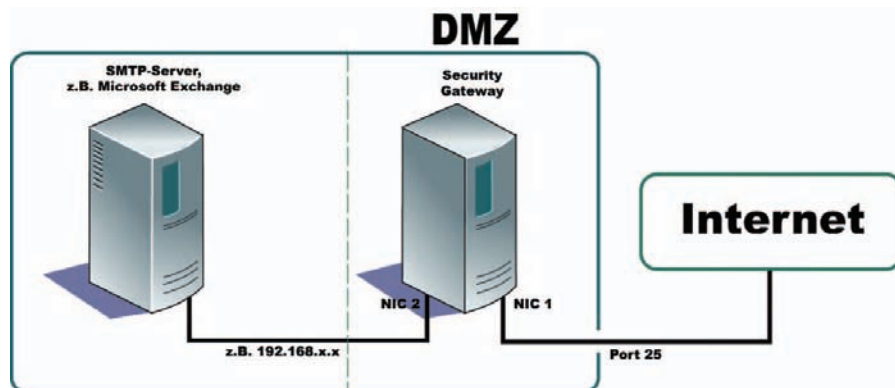
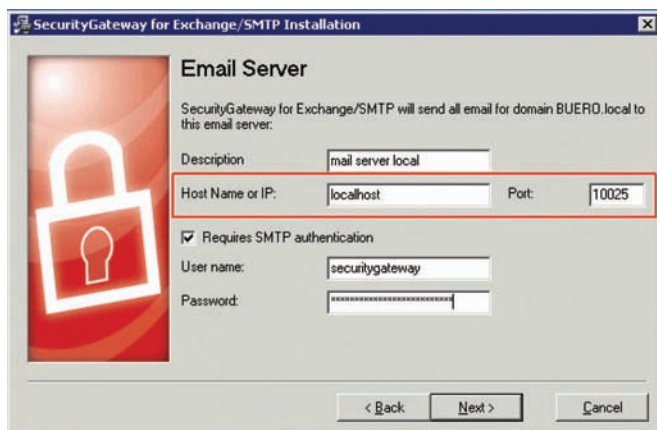


Bild 1: Schematische Darstellung der Einbindung des SecurityGateway von alt-n



**Bild 2:** Konfiguration des Gateways, wenn der Ziel-Mailserver auf derselben Hardware betrieben wird

anderen Groupware-Lösung macht die "SMTP call forward verification" die manuelle Eingabe hinfällig. Diese Funktion überprüft bei eingehenden E-Mails über das SMTP-Protokoll beim Mailserver, ob das Empfänger-Postfach existent ist.

Nachdem wir die Mail-Domain und das Prüfverfahren festgelegt hatten, definierten wir noch die IP-Adresse beziehungsweise den Host-Namen und den Mailserver, an den die E-Mails nach der Prüfung weitergeleitet werden. Hier legten wir auch den SMTP-Port fest. Diese Einstellung ist wichtig, wenn das SecurityGateway und der Mailserver auf demselben Hardware-Server laufen. In diesem Fall würden beide Dienste Port 25 auf ein- und derselben IP-Adresse überwachen, was unweigerlich zu Störungen führt. Daher mussten wir den Ziel-SMTP-Server auf einen anderen Port – beispielsweise 10025 – umstellen (siehe Bild 2). Somit nimmt das Gateway auf Port 25 die E-Mails von außen an, scannt diese und leitet sie an Port 10025 etwa des Exchange Servers weiter. Bei dieser Konstellation ist es wichtig, dass der Mailserver so konfiguriert ist, dass er E-Mails nur noch von der eigenen IP, also dem Gateway, und

Da SecurityGateway stark Festplatten-basiert arbeitet, lässt sich der E-Maildurchsatz durch schnelle Festplatten optimieren. Separate Festplatten für die Datenbank und die Logfiles steigern die Performance zusätzlich.

**Tipp 1: Schnelle Festplatten**

auch nur mit einer SMTP-Authentifizierung annimmt. Damit ist sichergestellt, dass der Mailserver auf keinen Fall als Relay-Server missbraucht werden kann. Danach findet die eigentliche Installation ihren Abschluss und die Dienste starten.

Das SecurityGateway stellt über einen eigenen, parallel zum IIS betriebenen Webserver-Dienst eine webbasierte Verwaltungs-Oberfläche zur Verfügung, die mit den gängigen Browsern zu bedienen ist. Wer die Prüfung auf erlaubte E-Mail-Empfänger über das Active Directory – spricht Exchange – einen LDAP-Server oder einen beliebigen SMTP-Server realisiert, muss für den ersten Einsatz lediglich noch die erlaubten Empfänger-Domains einrichten. Zudem sollte das Gateway wissen, mit welchem Quell-Server die Postfächer abgeglichen und an welchen Mailserver die E-Mails ausgeliefert werden. Wir haben im Test für verschiedene Domainnamen verschiedene Quellen- und Empfänger-Server konfiguriert.

**Mehrstufige Sicherheit**

Das Sicherheits-Menü des Gateways ist in die Oberpunkte "Spam", "Virus", "Spoofing" und "Abuse" kategorisiert. Die Anti Spam-Funktion arbeitet auf Basis des bekannten "SpamAssassin" nach heuristischen Regeln und des Bayesschen Filters. Zur Wahl steht hier, ob die Software die integrierte SpamAssassin-Engine verwendet oder auf einen Remote SpamAssassin-Daemon verbindet. Letzteres hat den Vorteil, diesen Punkt für mehrere Gateways zentral administrieren zu können. Die DNS Blacklist verwendet die Angaben von "spamhaus.org" und "spamcop.net" und ist durch weitere Listen beliebig erweiterbar. Die URI Blacklist ergänzt die Spam-Erkennung auf Basis der bekannten URIBL.

**Wirkungsvoller Spam-Schutz durch Greylisting**

Greylisting ist eine der aktuellsten Erfindungen von Spam-Filtern. Durch diese Funktion lehnt SecurityGateway die erste E-Mail von unbekanntem Absender temporär ab. Wird ein zweites Mal versucht, diese E-Mail zuzustellen (was ein regulärer und RFC-konform konfigurierter SMTP-Server macht), so wird diese E-Mail letztendlich akzeptiert. Spam-Tools versenden die E-Mails nach einer solchen Aufforderung kein zweites Mal, da sie die Rückmeldungen gar nicht empfangen. Nach der zweiten, regulären Zustellung geht das SecurityGateway von einem "guten" Mailserver aus und speichert diese Info in der lokalen Datenbank ab. Bekommt das Gateway von der gleichen Absender-Domain und über den bereits geprüften Mailserver erneut eine E-Mail, kann diese direkt durchgewunken werden.

Um das Erkennen von Viren kümmert sich die Clam AntiVirus-Engine. Mit der optionalen Erweiterung ProtectionPlus wacht im SecurityGateway die Engine von Kaspersky über virale Infekte. Das Updateintervall der Virensignaturen konnten wir stündlich oder täglich einstellen, wobei das stündliche Update erste Wahl sein sollte.

Die Systemvoraussetzungen von SecurityGateway sind abhängig vom E-Mailverkehr. Für das durchschnittliche E-Mailvolumen von 10 bis 25 Benutzern und einer exklusiven Nutzung der Hardware gibt der Hersteller folgende Mindestanforderungen für das Server-System an: Als Betriebssystem kommt nur Microsoft Windows 2000, XP, Vista oder Server 2003 in Frage. Hardwareseitig sollte die Plattform über einen Pentium 4-Prozessor (Multicore wird empfohlen) und mindestens 512 MByte Hauptspeicher (besser 2 GByte) sowie eine NTFS-Partition mit mindestens 500 MByte freiem Speicherplatz verfügen. Auf dem Client muss ein Browser wie der MSIE 6.0, Firefox 1.5, Opera 8.5, Safari 3.0 und Adobes Flash-Player in Version 8 oder neuer installiert sein.

Wir haben das Gateway auf einer virtuellen Maschine unter VMware betrieben, auf der Windows Server 2008 zum Einsatz kommt.

**Systemvoraussetzungen**



Bild 3: Die umfangreiche Web-Oberfläche ermöglicht individuelle Sicherheitseinstellungen

### Keine Chance für Spoofer

Als Spoofing wird der Täuschungsversuch von Mailservern bezeichnet, die ihre wirkliche Identität, zum Beispiel in Form von gefälschten IP-Adressen, zu verschleiern versuchen. SecurityGateway hat einige wirkungsvolle Waffen, um die Identität des Absender-Servers vorweg zu prüfen. Neben der ersten Stufe, dem Reverse Lookup, kommen die DKIM-Prüfung und das Sender Policy Framework (SPF) zusammen mit der Prüfung der Sender ID einer jeden E-Mail zum Tragen. Die zusätzliche Callback-Prüfung ist eine weitere Hürde für Spam-Mails. Oft werden Spam-Mails ohne die Angabe im "from" des E-Mail Header versendet. Kann dadurch der Absender nicht verifiziert werden, lehnt das Gateway die E-Mail ab.

Den Schutz davor, als Relay-Server (also als Spam-Server) missbraucht zu werden, regeln wir im Gateway durch das Festlegen der zugelassenen Absender-Adressen. Die zusätzliche Einrichtung der SMTP-Authentifizierung ist ein weiterer Schutz vor Missbrauch.

Weitere, individuelle Filter lassen sich anhand von Regeln für Mail-Inhalte und

Anhänge erstellen. So konnten wir zum Beispiel im Test festlegen, dass ausführbaren Dateien grundsätzlich geblockt werden und Audiofiles automatisch in die Quarantäne wandern. Diese Einstellungen werden wahlweise global für alle Domains oder für einzelne Domains vorgenommen. Individuelle und manuell konfigurierte Black- und Whitelists auf Basis einzelner E-Mailadressen, Domains und IPs runden die mächtige Sicherheitskonfiguration ab.

### Prüfung ausgehender Mails verfeinert Erkennungsrate

Neben dem eingehenden wird auch der ausgehende Datenverkehr überwacht. Voraussetzung dafür war, dass wir unserem Mailserver mitteilen, dass wir E-Mails nicht mehr direkt oder über einen externen SMTP-Server, sondern nur noch über das SecurityGateway verschicken wollten.

Das Gateway kann den ausgehenden E-Mailverkehr analysieren und dazulernen. Die klassischen Beispiele sind die Verwendung der Begriffe „Sex“ und „Viagra“ im Mailbody. Diese führen beim Empfang regulär dazu, dass eine E-Mail

Wer seinen internen Mailserver nicht als MX-Record für seine Internet-Domain eingetragen hat oder über eine dynamische IP verfügt, kann mit einem POP3-Connector externe Postfächer abrufen und über das SMT-Protokoll an das SecurityGateway verteilen. Neben kostenpflichtigen Tools ist das kostenlose Programm "PullMail" ideal für diese Aufgabe. Das Werkzeug wird wahrscheinlich nicht mehr weiter entwickelt, ist aber unter [1] noch im Internet erhältlich.

### Tipp 2: Pullmail bei dynamischen IPs

als Spam klassifiziert und isoliert wird. Doch kann die Benutzung dieser Begriffe etwa für Unternehmen aus der Pharmazie oder dem Erotik-Gewerbe alltäglich und normal sein. Erkennt das Gateway, dass E-Mails mit solchen Schlüsselwörtern versendet werden, werden die Kriterien für den E-Mail Empfang automatisch angepasst. Das gilt auch für E-Mailabsender, deren Domain oder Mailserver – aus welchen Gründen auch immer – auf einer Blacklist stehen. Regelmäßig würde das Gateway dann den Empfang der E-Mail verweigern. Erkennt die Software anhand des ausgehenden E-Mailverkehrs, dass an eine Domain auf der Blacklist E-Mails versendet werden, finden umgekehrt auch Nachrichten des Absenders ihr Ziel.

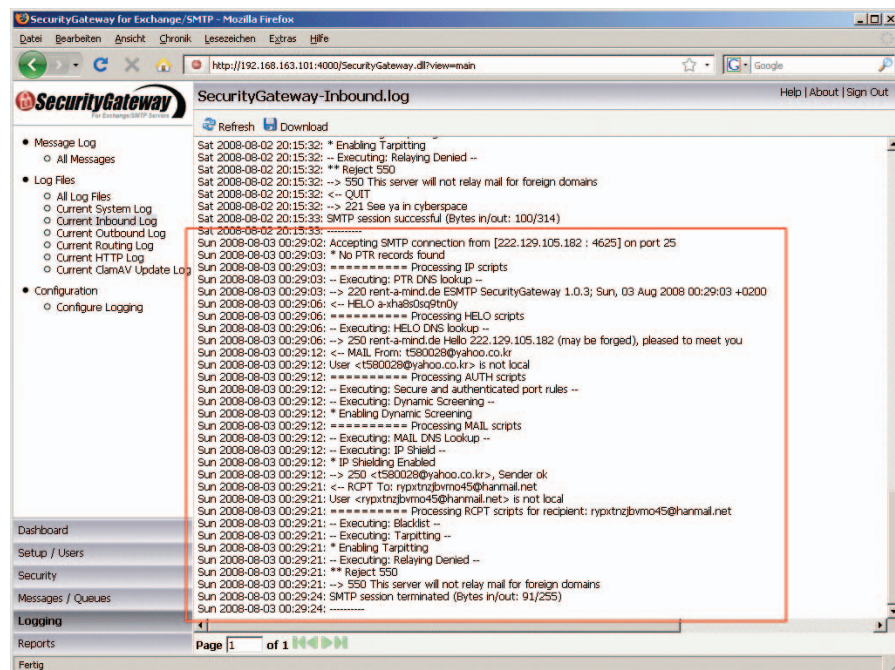


Bild 4: Ausschnitt aus einer Logdatei, die einen erfolglosen externen Versuch dokumentiert, das SecurityGateway zum Spam-Versand zu missbrauchen

**Produkt**

SMTP-Gateway zum Filtern von Spam und der Abwehr von Viren.

**Hersteller**

alt-n technologies  
www.altn.de

**Preis**

Die Lizenz für zehn User kostet 474 Euro im ersten und 100 Euro ab dem zweiten Jahr. Das optionale Virenschutz-Modul ProtectionPlus schlägt für die gleiche Nutzeranzahl mit 143 Euro im ersten und 100 Euro ab dem zweiten Jahr zu Buche. Weitere Lizenzstufen sind 25, 50 und 100 User.

**Technische Daten**

www.it-administrator.de/downloads/datenblaetter

**So urteilt IT-Administrator (max. 10 Punkte)**



**Dieses Produkt eignet sich**

**optimal** zur Absicherung bestehender E-Mail-Systeme auf Exchange-Basis unter Verwendung von Active Directory.

**teilweise** zur Absicherung kleinerer E-Mail-Systeme auch ohne Active Directory unter Verwendung eines LDAP-Servers oder SMTP-Zustellprüfung.

**nicht** für den lokalen Betrieb auf einer Workstation.

**alt-n technologies SecurityGateway**

**Hervorragende Erkennungsraten**

Im Test haben wir uns eines Webservice bedient und unsere Versuchs-Domain mit zufälligen Spam- und Viren-Mails beschießen lassen. Weiterhin haben wir eine zum Test konnektierte Internet-Domain auf die Blacklist von spamhaus.org gesetzt. So vorbereitet, konnten wir über mehrere Wochen reale und manipulierte Mails empfangen und die Effektivität der Plattform testen. An unsere Testdomain ist keine ungewollte E-Mail durchgekommen,

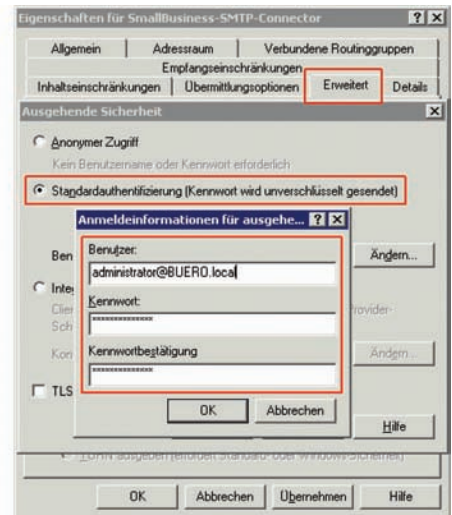
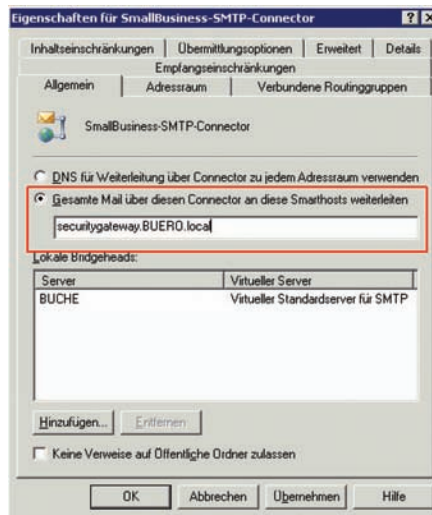


Bild 5: Exemplarische Einstellungen bei einem SmallBusiness-SMTP-Connector, um das SecurityGateway auch bei ausgehenden Mails zu nutzen


ohne vorher in Isolationshaft zu geraten. Erst, als wir an diese Domain über das Gateway auch gezielt E-Mails versendet haben, erkannte SecurityGateway, dass der Empfang vereinzelter Nachrichten anscheinend gewünscht ist.

Wie schon angesprochen, erweitert das gegen Aufpreis erhältliche ProtectionPlus die Sicherheitsmerkmale von SecurityGateway um eine AntiViren-Engine von Kaspersky. Zwar hat die im Test geprüfte integrierte ClamAV-Engine keine Viren durchgelassen, es ist jedoch zu vermuten, dass diese sich bei sehr neuen Viren im direkten Vergleich schwerer tun könnte. Denn in Sachen Aktualität von Virensignaturen ist die Kaspersky-Engine bisher so gut wie unschlagbar.

**Fazit**

Der Einsatz eines SMTP-Gateways ist grundsätzlich sinnvoll, um ein bestehendes E-Mail-System um leistungsstarke Spam- und Virenfilter zu ergänzen als auch den eigenen Mailserver aus der DMZ des Netzwerks zu holen. Das SecurityGateway hat im mehrwöchigen Test funktional keine Schwächen gezeigt und Spams, Viren und Phishing-Mails zielsicher blockiert. Die Lernfunktion zeigte nach ein paar hundert versendeten E-Mails erste Wirkung. Die vielfältigen Einstellungen können allerdings auch nach hinten losgehen: Wer das Kor-

sett seines Gateways zu eng schnürt, blockiert möglicherweise erwünschte E-Mails. Daher ist es vor allem in den ersten Wochen und Monaten notwendig, dass die Regeln und Logdateien ständig analysiert und angepasst werden. Entgegen der Regel für eine Firewall, zunächst nichts zuzulassen und nach und nach die Ports zu öffnen, sollten Sie bei SecurityGateway erst einmal auf die Basiseinstellungen zurückgreifen, um diese dann nach einem mehrwöchigen Lernprozess und dem Auswertem der Logdateien Schritt für Schritt zu verfeinern.

Wer die kleinste Lizenzierung für zehn User wählt, wird seine E-Mails vermutlich eher über POP3 beim Internet-Provider abholen. Über einen Workaround und einen zusätzlichen POP3-Connector (siehe Tipp 2) lässt sich das auch weiterhin realisieren. Wünschenswert wäre allerdings, dass diese Funktion bereits im Gateway integriert ist. Ansonsten ist SecurityGateway schnell einsetzbar, lässt sich bei Bedarf sehr differenziert und individuell konfigurieren und zeigt sich äußerst zuverlässig. Bei 50 Euro pro User im ersten Jahr und 10 Euro in den Folgejahren sollte sich die Anschaffung sehr schnell amortisiert haben. (ln) 

[1] Pullmail  
www.msxfaq.net/tools/pullmail.htm

Links