

## Netzwerksicherheit als Plug-in: gateProtect-Appliance im Test

([http://www.zdnet.de/sicherheit\\_in\\_der\\_praxis\\_netzwerksicherheit\\_als\\_plug\\_in\\_gateprotect\\_appliance\\_im\\_test\\_story-39001543-39198451-1.htm](http://www.zdnet.de/sicherheit_in_der_praxis_netzwerksicherheit_als_plug_in_gateprotect_appliance_im_test_story-39001543-39198451-1.htm))

Mittwoch, 5. November 2008

### Netzwerksicherheit als Plug-in: gateProtect-Appliance im Test

**UTM-Security-Appliances versprechen eine absolute Sicherheit für Firmennetzwerke. ZDNet zeigt am Beispiel von gateProtect, was die Appliances leisten und wann sie durch weitere Sicherheitsmaßnahmen ergänzt werden müssen.**

Von Christoph H. Hochstätter, ZDNet

Liest man die Marketingbroschüren vieler UTM[1]-Appliance-Hersteller, so ist IT-Sicherheit ganz einfach: Man nehme eine Appliance zwischen Intra- und Internet sowie zwischen Clients und Servern ins Netz, und schon ist man vor allen Gefahren geschützt. Unified Thread Management (UTM) wehre einfach alle Gefahren ab - Viren und Spam bleiben draußen. Vertrauliche Daten hingegen können das Unternehmen nicht mehr verlassen. Das Sicherheitsunternehmen Sophos bietet diese Botschaft den mit Hochglanzbroschüren überfluteten Entscheidern sogar als Kriminalroman an.

ZDNet hat die UTM-Appliance GPX 800 von gateProtect getestet. Die GPX 800 ist eine von insgesamt sechs Hardware-Appliances, die gateProtect anbietet. Darüber hinaus gibt es von gateProtect drei Software-Appliances als VMware-Images.



Alle Appliances laufen unter Linux, wobei die beiden kleineren im "Fritzbox-Formfaktor" realisiert sind. Sie eignen sich für 10 bis 25 Benutzer. Die vier größeren Hardware-Appliances gibt es im 2U-Rackformat.

Das ZDNet-Testgerät GPX 800 ist für Netzwerkgrößen bis 500 Benutzer ausgelegt. Die Firewall soll einen Durchsatz von bis zu 3 GBit/s schaffen. VPNs sind bis zu 250 MBit/s möglich. Das Gerät besitzt eine Intel-Xeon-3040-CPU[11] mit zwei Kernen, 1,86 GHz Taktfrequenz und 2 MByte Level-2-Cache. Dazu kommen 4 GByte Hauptspeicher. Die 65-Nanometer-CPU mit 65 Watt TDP ist aus Green-IT-Gesichtspunkten nicht die optimale Wahl, jedoch wird man kaum Appliances finden, die immer auf die neueste Hardware-Technologie aufsetzen. Dafür erhält man eine Kombination aus Hard- und Software, die hinsichtlich der Stabilität intensiv getestet ist.

Die GPX 800 besitzt acht Intel-Gigabit-Ethernet-Controller mit Hardware-TCP/IP-Offloading. Somit kann man bereits mit "dummen" Ethernet-Switches ohne jegliche Layer-2- und Layer-3-Funktionalität, etwa 802.1X[12], acht virtuelle Netze aufbauen.

Mit der Firewall-Funktionalität der Appliance lässt sich der Datenverkehr nur zwischen verschiedenen Netzen einschränken, das heißt Rechnern, die an unterschiedlichen Ports der Appliance hängen. Sinnvoll ist es beispielsweise, alle Arbeitsplatzrechner an einen Port zu verbinden und alle Unternehmensserver an einen anderen. Dann lässt sich bereits auf Layer-3-Ebene festlegen, welcher Arbeitsplatzrechner mit welchem Server auf welche Weise kommunizieren darf. Will man verhindern, dass Arbeitsplatzrechner untereinander kommunizieren, so müssen im Unternehmen mindestens Layer-2-Switches installiert werden, die dafür sorgen, dass jeder Rechner nur mit der MAC-Adresse der Appliance Daten austauschen kann.

Die Appliance bedient man üblicherweise mit einer Windows-Client-Applikation. Ein Einloggen auf Shell-Ebene ist in der Regel nicht erforderlich, aber dennoch möglich. gateProtect empfiehlt, dass nur Administratoren und Partner, die die Platin-Zertifizierung von gateProtect besitzen, auf der Shell-Ebene arbeiten.

#### Arbeiten mit dem Administrationsclient

Nach dem ersten Einloggen in den Administrationsclient stellt man üblicherweise zunächst die Internetverbindung her. Das kann auf drei Arten geschehen: Per PPPoE, von gateProtect als DSL-Verbindung bezeichnet, mit Standard-IP-Routing, oder über ISDN.



Dabei vermisst man die Möglichkeit der Zuweisung einer IP-Adresse über DHCP. Diese Variante verwenden alle deutschen Kabel-Internet-Anbieter sowie viele Telekommunikationsunternehmen, die Glasfaser bis zum Kunden anbieten. In diesem Fall kommt man um einen zusätzlichen Router nicht herum.

Die Verwaltung der Internetzugänge ist komfortabel. Es lassen sich mehrere Zugänge konfigurieren. Ein Zugang kann als Backup-Zugang definiert werden. So lässt sich beispielsweise bei Ausfall der DSL-Leitung kurzfristig ISDN nutzen.

## Netzwerksicherheit als Plug-in: gateProtect-Appliance im Test

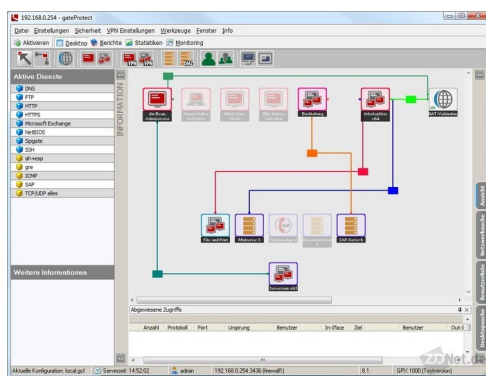
([http://www.zdnet.de/sicherheit\\_in\\_der\\_praxis\\_netzwerksicherheit\\_als\\_plug\\_in\\_gateprotect\\_appliance\\_im\\_test\\_story-39001543-39198451-1.htm](http://www.zdnet.de/sicherheit_in_der_praxis_netzwerksicherheit_als_plug_in_gateprotect_appliance_im_test_story-39001543-39198451-1.htm))

Eine Backup-Anbindung über UMTS ist nur über einen externen Router möglich. Viele Unternehmen bevorzugen UMTS-Zugänge als Backup, da gegenüber ISDN eine höhere Geschwindigkeit zu erzielen ist. Andere Hersteller, beispielsweise Lancom, bieten Geräte mit integriertem UMTS-Modul an.

Ebenso integriert ist eine Funktion für dynamisches DNS. Auch wenn die Hauptverbindung eine feste IP-Adresse besitzt, erhält man spätestens bei Nutzung einer Backupverbindung eine andere IP-Adresse. Mit dynamischem DNS kann man erreichen, dass erlaubte Verbindungen von außen, beispielsweise VPN oder E-Mail, jederzeit aufgebaut werden können.

Dynamisches DNS lässt sich allerdings nur über Provider wie DynDNS.org nach RFC2845 realisieren. DDNS nach RFC2136 mit BIND oder dem Microsoft-DNS-Server wird nicht unterstützt, was vor allem Großunternehmen vermissen werden.

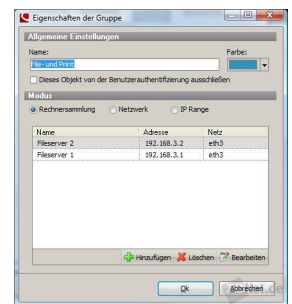
In einem ZDNet-TestszENARIO wird eine kleine Firma dargestellt. Alle Mitarbeiter dürfen auf zwei Fileserver und den Mailserver zugreifen. Zudem sollen alle Mitarbeiter gängige Internetdienste nutzen können. Die Mitarbeiter aus der Buchhaltung erhalten zudem Zugang zum SAP-Server. Der Administrator muss Zugriff auf alle Server haben, insbesondere auf den Datenbankserver und die Telefonanlage, die alle anderen nur indirekt benutzen. Außerdem bekommt der Administrator uneingeschränkten Internet-Zugang.



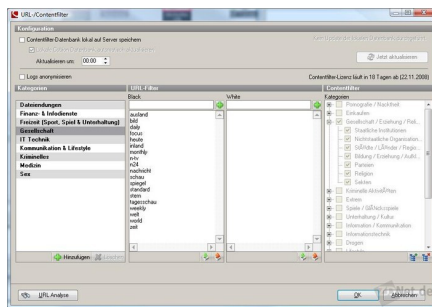
Ein solches Szenario ist hier gezeigt. Das Netzwerk aller Arbeitsplatzrechner hängt dabei an der Netzwerkkarte eth4 der Appliance. Alle Server hängen an eth3. Die Verbindungen zeigen, welche Server und Dienste von den Clients erreicht werden können.

Bereits in einem solchen kleinen Demo-Szenario kann es im Administrationsclient leicht unübersichtlich werden. Sinnvoll ist es daher, Rechner mit gleichen Rechten möglichst in Gruppen zusammenzufassen.

Im Bild sieht man, dass die beiden Fileserver des Unternehmens in eine Gruppe „File und Print“ gestellt wurden. Das gleiche passiert mit den Rechnern der Buchhaltungsmitarbeiter. Sie kommen in die Gruppe „Buchhaltung“.

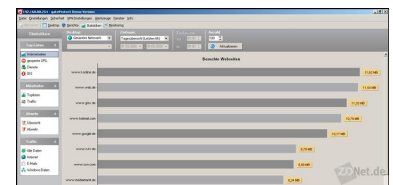


## Ausbalancieren von Freiheit und Sicherheit beim Internet-Zugang



Beim Internet-Zugriff lässt sich genau festlegen, welche Dienste einzelne Anwender nutzen dürfen. Bei den Diensten FTP, HTTP und HTTPS lässt sich darüber hinaus eine Proxy-Nutzung erzwingen. Das kann auf klassische Weise geschehen, so dass die Benutzer die UTM-Appliance als Proxy in ihrem Browser konfigurieren müssen, oder aber transparent als sogenannter „Hidden Proxy“.

Verwendet man einen Proxy, so kann der URL- und Content-Filter genutzt werden. Dabei lässt sich Benutzern der Zugang zu bestimmten Websites sperren. Ebenso ist eine Sperre nach Inhalten möglich. Dabei blockt die Firewall Webseiten, die bestimmte Schlüsselwörter enthalten, siehe Bild.



Sehr umfangreich sind die Logging- und Statistikfunktionen. Je nach Konfiguration lassen sich alle besuchten Websites nach Benutzer auswerten. Inwieweit solche Funktionen aktiviert werden, sollte man stets mit dem Betriebsrat klären.

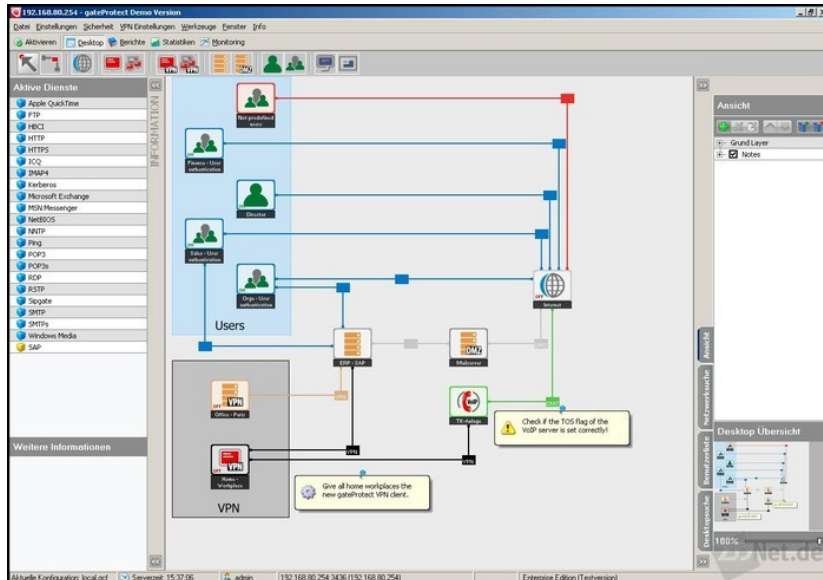
Nicht ganz ungefährlich ist die Verwendung der Proxy-Funktion bei HTTPS. HTTPS ist wie jede SSL/TLS-Verschlüsselung eine End-to-End-Verschlüsselung. Die Appliance muss als Man-in-the-Middle agieren. Das heißt, dass einerseits alle HTTPS-Verbindungen auf der Firewall entschlüsselt werden. Andererseits kann der Nutzer das Zertifikat des HTTPS-Servers nicht mehr überprüfen. Befindet sich im Internet ein weiterer Man-in-the-Middle, der ein gefälschtes Zertifikat unterschreibt, kann das nicht mehr festgestellt werden.

Um ein Szenario wie oben zu realisieren, müssen alle Client-Rechner feste IP-Adressen haben, oder man muss alle Rechner mit besonderen Rechten, etwa den des Administrators und die der Buchhaltung, an einen eigenen Port der Firewall anschließen. Lässt sich beides nicht einfach bewerkstelligen, beispielsweise aus verkabelungstechnischen Gründen, kann man Benutzerauthentifizierung verwenden. Dabei werden die Zugriffsrechte nicht pro Rechner, sondern pro Benutzer vergeben. Das erfordert jedoch, dass auf jedem Rechner der Authentifizierungsclient installiert ist. Alternativ steht ein Webclient zur Verfügung. Dabei darf das Browserfenster nicht geschlossen werden.

## Netzwerksicherheit als Plug-in: gateProtect-Appliance im Test

([http://www.zdnet.de/sicherheit\\_in\\_der\\_praxis\\_netzwerksicherheit\\_als\\_plug\\_in\\_gateprotect\\_appliance\\_im\\_test\\_story-39001543-39198451-1.htm](http://www.zdnet.de/sicherheit_in_der_praxis_netzwerksicherheit_als_plug_in_gateprotect_appliance_im_test_story-39001543-39198451-1.htm))

Bei Verwendung der Benutzerauthentifizierung muss sich jeder Anwender vor dem Zugriff auf Netzwerkressourcen zusätzlich anmelden. Ein Beispiel für eine Topologie mit benutzerbasierter Authentifizierung zeigt dieser Screen.



### Eingehende Verbindungen restriktiv handhaben

Einkommende Verbindungen aus dem Internet sind standardmäßig geblockt. Das gilt auch für das ICMP-Protokoll, das unter anderem für Ping verwendet wird. Einkommende Verbindungen, beispielsweise für einen Mailserver, muss man einzeln erlauben. Dazu wird ein DMZ-Objekt definiert. Im Fall eines Mailservers leitet man TCP-Port 25 aus dem Internet an den Mail-Server weiter.

Grundsätzlich werden alle ankommenden und ausgehenden Pakete auf Viren gescannt. Dazu verwendet gateProtect die Engine und die sich selbst aktualisierende Datenbank von Kaspersky. Das ersetzt wie bei allen Appliances nicht den Virenschutz auf Client- und Server-Maschinen. Immer wenn eine End-To-End-Verschlüsselung verwendet wird, kann die Appliance keinen Scan durchführen.

E-Mail wird zusätzlich nach Spam durchsucht. Technisch verwendet die Appliance dafür einen SMTP-Proxy, der den Datenverkehr auf TCP-Port 25 automatisch abfängt. Die Spamdatenbank wird ebenfalls automatisch aktualisiert und basiert auf Daten, die von großen E-Mail-Providern stammen. Geht dort eine große Anzahl gleichlautender E-Mails ein, so besteht Spamverdacht. Diese Methode ist recht zuverlässig, allerdings auch ein wenig anfällig gegen False Positives, da Opt-In-Newsletter manchmal als Spam erkannt werden. Whitelists helfen, dieses Problem zu reduzieren.

Neben der Konfiguration auf Portebene ist die Appliance in der Lage, die Protokolle HTTP, FTP, POP3, SMTP und DNS auf der Layer-7-Ebene zu erkennen. Das erlaubt beispielsweise, dass sich Nutzer mit Webservern verbinden können, die nicht auf dem Standard-Port 80 laufen. Ebenso sieht man so, ob Malware versucht, den Standard-Port 80 für andere Protokolle als HTTP zu verwenden. Schadprogramme, etwa Botnets, die ihre Befehle per HTTP-Tunnel empfangen, werden auf diese Weise allerdings nicht identifiziert.

Da Angreifer von außen vielfach selbstentwickelte Layer-7-Protokolle verwenden, sollte die Protokollerkennung nur dazu verwendet werden, Nutzern die Verbindung zu erlauben, falls ein Protokoll sicher erkannt wurde. Unbekannte Protokolle auf Nicht-Standard-Ports sollte man grundsätzlich verbieten, wenn man auf Nummer sicher gehen möchte.

Schwierig zu entscheiden sind Dinge wie der SSH-Port 22. Da die Firewall den SSH-Handshake nicht sicher erkennt, kann eine eingeschleuste Malware darüber ausspionierte Daten „nach Hause“ schicken. Sperrt man hingegen den Port, so können Benutzer kein SSH verwenden. Das gilt dann automatisch auch für den Filetransfer mit SCP oder SFTP.

Zu den ausgereiften Funktionen gehört die VPN-Verbindung zwischen Standorten, die mit UTM-Appliances von gateProtect ausgerüstet sind. Ebenso ist eine VPN-Einwahl von mobilen Mitarbeitern mittels des mitgelieferten VPN-Clients möglich.

## Netzwerksicherheit als Plug-in: gateProtect-Appliance im Test

([http://www.zdnet.de/sicherheit\\_in\\_der\\_praxis\\_netzwerksicherheit\\_als\\_plug\\_in\\_gateprotect\\_appliance\\_im\\_test\\_story-39001543-39198451-1.htm](http://www.zdnet.de/sicherheit_in_der_praxis_netzwerksicherheit_als_plug_in_gateprotect_appliance_im_test_story-39001543-39198451-1.htm))

gateProtect unterstützt die Protokolle IPSec und VPNs mittels SSL/TLS. PPTP ist ebenfalls möglich, hauptsächlich um Windows-Clients den Zugang ohne zusätzliche Software zu ermöglichen.

Ebenso kann man VPNs zwischen Standorten herstellen, die nicht über gateProtect-Appliances angebunden sind. Für die VPNs der Hersteller Cisco und Funkwerk ist beim gateProtect-Support Know-how vorhanden. Bei anderen Herstellern muss man unter Umständen ein wenig Zeit in die Konfiguration investieren.

### Fazit

Die UTM-Appliances von gateProtect bieten eine sehr gute und sehr sichere Lösung für das, was mit einer Firewall erreicht werden kann. Das gilt gleichermaßen für die Regelungen beim Zugriff auf Unternehmensserver bereits auf Layer-3-Ebene und für die Sicherung des Internet-Traffics.

Die grafische Administrationssoftware ist sehr ausgereift und bietet viele Möglichkeiten. Ein Zugang zur Appliance mittels SSH ist nicht erforderlich, wenngleich möglich, um beispielsweise weitere Sicherungssysteme, die für Linux verfügbar sind, zu integrieren.

Unerfahrene Administratoren kommen allerdings trotz des grafischen Clients nicht besonders weit. Ohne weitreichende Kenntnisse des TCP/IP-Protokolls und das Wissen, welche Ports für welche Dienste zuständig sind, wird man es weder schaffen, Benutzern Zugang zu den Diensten zu verschaffen, die sie benötigen, noch das Unternehmensnetzwerk gegen Gefahren abzusichern.

Auch muss man bedenken, dass eine Firewall nicht vor allen Gefahren schützen kann. Gegen beabsichtigten oder unbeabsichtigten Datendiebstahl schützt die Firewall nicht. Das gleiche gilt für alle Verbindungen, die End-to-End verschlüsselt sind. Hier greift kein Viren- und Spamschutz. Eine Ausnahme bildet der transparente HTTPS-Proxy, der allerdings andere sicherheitstechnische Nachteile hat, beispielsweise, dass Anwender die Authentizität von Server-Zertifikaten nicht mehr überprüfen können.

Neben den Firewallaufgaben ist die VPN-Funktionalität hervorzuheben. Sowohl Site-to-Site- als auch Site-to-End-VPNs für die Einwahl von mobilen Benutzern lassen sich mit den gateProtect-Appliances komfortabel und sicher einrichten.