

Im Test: gateProtect GPO-125

Sicherheit per Drag-and-Drop

von Sandro Lucifora

Das größte Sicherheitsrisiko heutiger Firewall-Systeme besteht darin, dass zur effektiven Abwehr von Angriffen immer komplexere Sicherheitsfunktionen integriert sein müssen. Das führt zwangsläufig dazu, dass die Konfiguration der Schutzsysteme kompliziert und unübersichtlich wird. Daraus folgt meist eine fehlerhafte Konfiguration, die aus dem Sicherheitssystem oft ein offenes Scheunentor macht. gateProtect will mit dem eigens entwickelten eGUI – dem "ergonomic graphic user interface" – die Bedienbarkeit wieder in den Mittelpunkt stellen. Ob das gelungen ist, haben wir in einem Test für Sie herausgefunden.

Mit der Firewall GPO-125 haben wir eine Appliance als Einstiegslösung im Test. Sie ist für Unternehmen mit bis zu 25 Mitarbeitern ausgelegt. Zu den Features gehören Application Level Firewall, VPN SSL über Zertifikate, Anti-Spam mit Real Time Detection, Antivirus, Intrusion Detection, URL- und Content Filtering.

Internet-Verbindung einrichten

Der "rote Kasten" wird nach dem Anschluss im Netzwerk als Gateway definiert und regelt so den zukünftigen Datenverkehr ins und aus dem Internet. Die Internetverbindung baut das System wahlweise über PPPoE beziehungsweise PPTPoE und ein angeschlossenes DSL-Modem auf oder es nutzt einen separaten, eigenständigen Router. Als dritte Option bietet der Internet-Wizard auch die ISDN-Wählverbindung an, die jedoch in der GPO-Appliance fehlschlägt, da diese Funktion eine eingebaute ISDN-Karte voraussetzt. Das ist der Hinweis, dass die gateProtect-Lösung nicht nur auf einer fertigen Appliance arbeitet, sondern auch als Software-Lösung auf einem eigenen Server installiert werden kann.

Bedient beziehungsweise eingerichtet wird die Appliance ausschließlich durch den Administrations-Client oder das Command Center, das einen sinnvollen Einsatz findet, wenn mehrere gateProtect-Firewalls im Überblick und/oder zusammenhängend ad-

ministriert werden. Nach der Installation richteten wir mit dem Installations-Wizard eine PPPoE-Verbindung über ein angeschlossenes DSL-Modem ein. Im Test wählten wir zudem zeitweise auch einen Router für den Internetzugang. Dabei fiel uns auf, dass der Router unbedingt an einem separaten der vier Netzwerk-Ports der Appliance angeschlossen oder in einem anderen IP-Bereich betrieben werden muss. Zudem darf im Router keine Firewall-Funktion aktiviert sein und jeglicher Datenverkehr muss weitergeleitet werden. Ansonsten finden die in der Appliance definierten Regeln teilweise keine Anwendung, da diese gegebenenfalls schon vorab durch den Router gestört werden.

Failover: Wenn eine Leitung weg ist

Klar von Vorteil ist die Möglichkeit, mehrere Internetverbindungen konfigurieren und als Backup-Leitung festlegen zu können. In der Praxis zeigte sich diese Funktion jedoch nur unter bestimmten Voraussetzungen als optimal – was jedoch nichts mit der Appliance selbst zu tun hatte. Im Test richteten wir über eine zweite DSL-Leitung

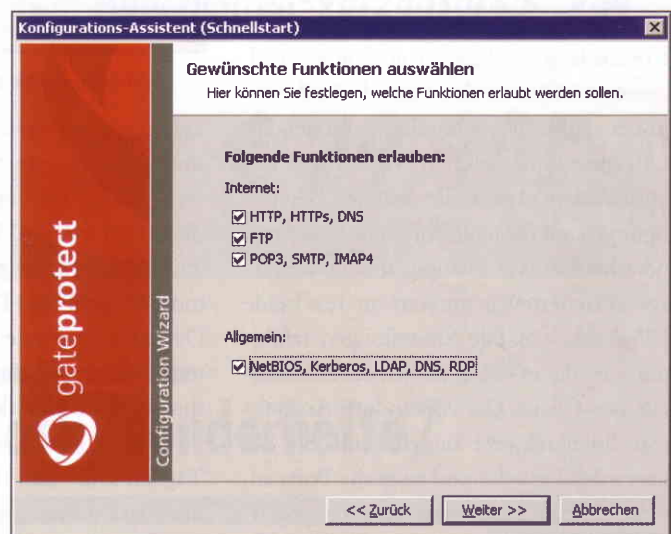


Bild 1: Die wichtigsten Dienste werden schon bei der Einrichtung der Internet-Verbindung vordefiniert

eine Failover-Funktion ein. Im simulierten Ausfall der Hauptleitung hat die Appliance in wenigen Sekunden das Routing auf die Backup-Leitung umgestellt – eine einwandfreie Leistung der Firewall. Doch technisch betrachtet laufen beide DSL-Zugänge über dieselbe Hausleitung – auch, wenn es sich dabei um unterschiedliche DSL-Anbieter handelte. Fällt also eine Leitung aus, weil es Probleme in der Hauszuführung gibt (zum Beispiel am Telekom-Knotenpunkt), sind beide DSL-Zugänge offline. Was in diesem Fall durch die Backup-Funktion aufgefangen wird, sind zum Beispiel Ausfälle bei der Zugangsauthentifizierung eines DSL-Anbieters. Zudem zeigt ein Failover seine Wirkung, wenn die zwei-



te Backupleitung auf einem anderen Weg ins Haus kommt wie die Hauptleitung – zum Beispiel über einen anderen Verteilerpunkt oder via Fernseekabel.

Berechtigungen

Über die eGUI der gateProtect-Appliance galt es nun, die erste Konfiguration für die Internet-Nutzung vorzunehmen. Der Assistent richtete zu Anfang die wichtigsten Dienste zur Nutzung ein. Wir haben so recht schnell die Dienste HTTP/S, DNS, FTP und die Mailfunktionen POP3 und SMTP freigeschaltet. Damit konnte sofort jeder im Netzwerk das Internet mit den wichtigsten Funktionen nutzen.

Grundsätzlich ist erst einmal jeglicher Datenverkehr, sowohl ein- als auch ausgehend, gesperrt. Daher ist eine individuelle Nachjustierung der Regeln schnell notwendig. Um diese vorzunehmen, mussten wir uns entscheiden, ob sich die weiteren Berechtigungen auf die angeschlossene Hardware oder hardwareunabhängig auf den Benutzer beziehen. Wir nutzten im Test beide Möglichkeiten. Die Einstellungen erfolgten über das eGUI-Interface des Administrations-Client. Das vorhandene Analyse-tool für blockierte Zugriffe hilft bei der ersten Fehlersuche und zeigt die Ports an, über die von intern oder extern zugegriffen werden soll, die Firewall dies jedoch verhindert hat. Wir haben Ihnen dazu in unserem Link-Bereich [1] eine Übersicht der bekannten Ports von Programmen und Trojaner in einer Liste zusammengestellt.

Regeln für die Hardware

Im Test haben wir die Regeln für den angeschlossenen Exchange-Server so erweitert, dass von außen der Zugriff auf Outlook Web Access möglich ist. Durch die eGUI konnten wir das Vorhaben sehr einfach umsetzen. Mittels Drag-and-Drop haben wir ein neues Objekt auf die Arbeitsfläche gezogen und diesem den Namen des Servers, den Objekt-Typ Server, die Netzwerkkarte und die IP-Adresse des Servers zugeteilt. Im nächsten Schritt stellten wir mit dem Verbindungswerkzeug einen Anschluss zum Internet her,

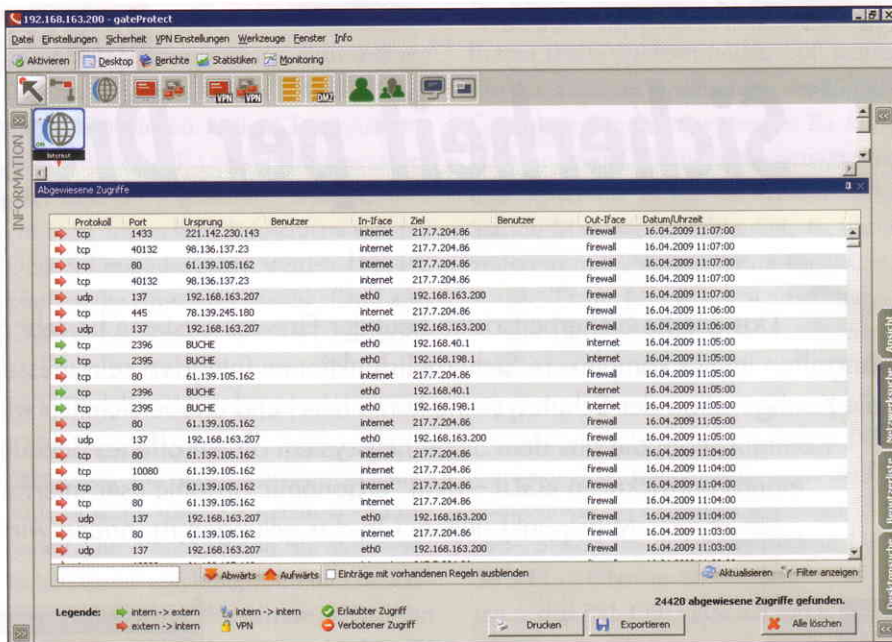


Bild 2: Die Übersicht der abgewiesenen Zugriffe gibt Aufschluss über Ports, die eventuell konfiguriert werden müssen

indem wir nur das Objekt für das Internet und den neu erstellten Server anklickten – es öffnete sich der Regeleditor, in dem die Regel für HTTPS eingerichtet wird. Zusätzlich benötigten wir für den Remote-Zugriff via HTTPS den Port 4125. Da es für diesen keinen fertig eingerichteten Dienst gab, legten wir diese Regel mit wenigen Mausklicks neu an.

Täglich sollte sich die Uhr dieses Servers über das Internet abgleichen, daher erlaubten wir auch den NTP-Dienst für den Server. Da die Abfrage nur vom Server in das Internet und nicht umgekehrt erfolgen darf, legten wir hierbei auch die umgekehrte Datenfluss-Richtung fest: Bei den zuvor angelegten Regeln musste vom Internet über die jeweiligen Ports auf den Server zugegriffen werden. Der NTP-Dienst darf nur vom Server ins Internet verbinden. Diese Richtungen werden anhand von grünen Pfeilen im Regeleditor dargestellt. Nach der Aktivierung der Regeln haben wir die Firewall für diese Funktion fertig konfiguriert. Angenommen, im Netzwerk sollen sich nun acht von 25 Computern über den NTP-Dienst Zeit-synchronisieren. In diesem Fall muss dieser Dienst nicht für jeden Computer, also für acht separate Objekte, aktiviert werden. Vielmehr lässt sich hierfür per Drag-and-Drop eine Com-

puter-Gruppe einrichten. Dieser werden dann die einzelnen Rechner per IP-Adresse zugeordnet und die entsprechende Regel zentral definiert.

Regeln für die Benutzer

Ein geteilter Arbeitsplatz ist nicht mehr ganz neu: Das bedeutet, dass ein Computer zum Beispiel durch zwei oder mehr Teilzeitkräf-

Performance

- Firewalldurchsatz: 200 MBit/s
- VPN (AES 192) Durchsatz: 50 MBit/s
- E-Mails pro Tag: 5.000
- Gleichzeitige Verbindungen: 250.000

Firewall

Layer Funktion, Single Sign On (xUA), Paketfilter, IDS, NAT, DHCP-Server, DMZ, Bridging, Internet-Failover, Webblocking, Mailfilter.

Besondere Features

High-End-Firewall-Funktion, Extended User Authentication, VPN Gateway (SSL mit X.509 Zertifikaten und IPSec), Proxies (HTTP, FTP, POP3,SMTP, SIP), Application Level (Deep Packet Inspection), Hochverfügbarkeit, VLAN.

Optional

Spam-Filter auf Commtouch-Basis, Virus Filter von Kaspersky sowie Web-Filter von IBM.

Technische Daten



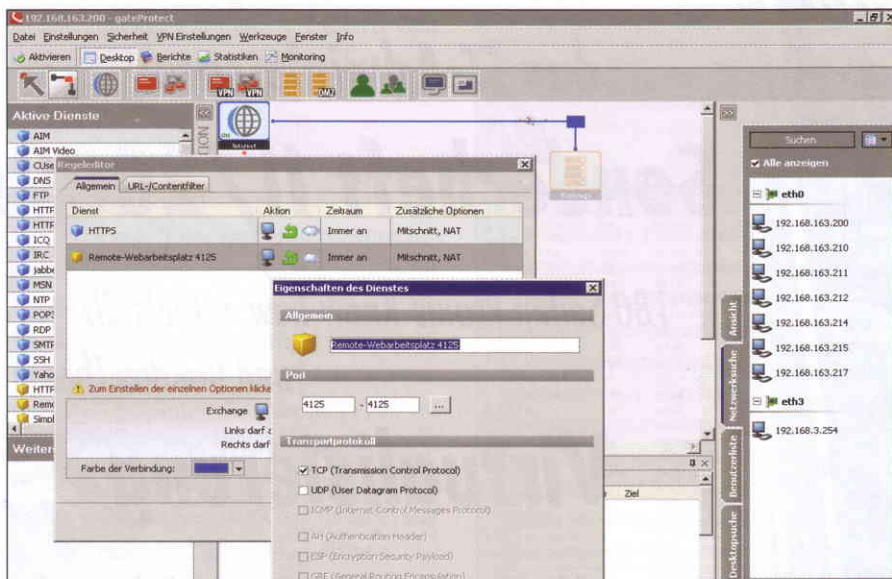


Bild 3: Vordefinierte Regeln lassen sich über den Regeleditor eintragen und auch eigene Regeln hinzufügen

te mit unterschiedlichen Aufgaben gemeinsam genutzt wird. In diesem Fall ist es nicht immer erwünscht, für einen Computer, sondern vielmehr für einen einzelnen Benutzer verschiedene Regeln festzulegen. Wie bei den IP-basierten Regeln werden in der eGUI auch Anwender und Anwendergruppen als Objekte behandelt. Der Vorteil dabei ist, dass die Regeln dadurch Hardware-unabhängig funktionieren. In unserem Testscenario arbeiteten zum Beispiel mehrere Entwickler an verschiedenen Rechnern – einige sind freie Mitarbeiter und benutzen zeitversetzt den selben Computer. Nicht alle dieser Mitarbeiter durften per FTP Daten auf den Produktiv-Server hochladen. Um das zu realisieren, griffen wir auf die Benutzerauthentifizierung für Regeln zurück. Dazu aktivierten wir zunächst die Benutzerliste aus dem AD des Netzwerkes.

Im Anschluss legten wir auf der Arbeitsfläche des Administrations-Clients – nach demselben Prinzip wie zuvor Computer und Computer-Gruppen – Benutzer beziehungsweise Benutzergruppen an. Statt einer IP-Adresse ordneten wir die Benutzernamen aus dem AD als Mitglied des neuen Objektes zu. Im nächsten Schritt verbanden wir das Internet-Objekt mit der Benutzergruppe und trugen über den Regeleditor die Berechtigung zum FTP-Zugriff ein. Damit der Firewall bekannt ist, an

welchem Computer sich der Benutzer befindet, muss sich dieser per Web-Browser an der Appliance anmelden. Solange die Browsersitzung geöffnet ist, erhält der Computer mit der ermittelten IP-Adresse die Regeln des angemeldeten Benutzers; in unserem Test war der FTP-Upload an jedem Computer, aber abhängig von den Benutzern möglich. Mit dieser Funktion können auch tiefgehende Sicherheiten gesteuert werden. Wie in unserem Szenario der Teilleistungszeitkräfte lässt sich so auch ein HBCI-Zugriff, um Online-Kontoaktivitäten vorzunehmen, ausschließlich auf Benutzerebene ermöglichen.

Gefilterter Datenstrom

Die Sicherung des Netzwerkes auf Port-Ebene bildet die Basis für den Schutz der eigenen Daten vor Angreifern. Doch verstecken sich auch in den übertragenen Daten selbst weitere Sicherheitsrisiken. So können zum Beispiel Trojaner und Viren über die freigegebenen Protokolle eingeschleust werden. Auch Schadcode von Internetseiten findet durch die offene Tür Einlass in das Netzwerk. Um auch diese Risiken auszuschließen, hat die GPO-125 drei weitere, effektive Schutzmechanismen:

- Der Webfilter ist eine Kombination aus URL- und Content-Filter. HTTP-Suchanfragen werden automatisch mit

erlaubten Kategorien von Webseiten und Inhalten abgeglichen und bei Notwendigkeit geblockt. Die Filtergruppen können dabei individuell aus 60 hinterlegten Filter-Kategorien zusammengestellt werden.

- Die Scan-Engine für Antivirus basiert auf der Technologie von Kaspersky. Das Gateway scannt dabei HTTP, FTP, POP3 und SMTP auf unerwünschten Code. Dateien werden auf der Firewall auf Viren gescannt und erst dann an den anfragenden Benutzer weitergegeben. Mit der konfigurierbaren Antivirus-Datei-Größe legen wir fest, bis zu welcher Größe eine Datei auf Viren gescannt wird. Hierzu haben wir das Limit auf bis zu 30 MByte angehoben. Trotz dessen, dass die gesamte Datei im Speicher der Appliance gescannt wird, konnten wir keine spürbaren Performance-Einbußen feststellen. Lediglich der FTP-Upload wies wenige Sekunden Verzögerung auf. Im Bedarfsfall muss der Administrator für das eigene Unternehmen hier den idealen Wert durch Ausprobieren herausfinden.
- Der Spam-Filter der UTM-Firewall scannt den E-Mailverkehr auf bekannte Spam-Signaturen und löscht oder markiert die erkannten E-Mails. Das Besondere hierbei ist, dass das eigentliche Filtern extern erfolgt und somit keine Ressourcenauslastung erfolgt. Durch die

Der Vorteil der PPTP-VPN-Verbindung ist unter anderem, dass diese mit den Windows-Bordmitteln erstellt und genutzt werden kann. Als Nachteil kann sich schnell zeigen, dass das Gateway auf den VPN-Tunnel umgestellt wird. Daher erfolgt bei aktiver PPTP-VPN-Verbindung der Internetzugriff über den VPN-Tunnel und das verbundene Netzwerk. Im Gegenzug ist sowohl an der Appliance als auch dem Arbeitsplatz die Einrichtung der IPSec-Verbindung wesentlich aufwändiger. Zudem wird ein eigener VPN-Client benötigt. Dadurch erfolgt jedoch nur das Routing an interne Adressen in das verbundene Netzwerk; Zugriffe auf das Internet laufen unverändert über die bestehende Internetverbindung. Nachteil bei diesem VPN-Typ ist, dass er den Tunnel nur mit einem Subnetz verbinden kann. So können Sie über die GPO-125 nicht auf mehrere Netzwerke hinter der Firewall zugreifen.

Tipps: PPTP-VPN vs. IPSec-VPN





eingesetzte Real Time Detection-Technik erkennt die Appliance Spam, Virus und Phishing-Attacken anhand von charakteristischen Mustern schon bei der erstmaligen Ausbreitung. Dadurch sollen laut Hersteller mehr als 97 Prozent der Spam-Versender rechtzeitig und vor der Verbreitung erkannt und abgefangen werden. Im Test stellten wir vielfach fest, dass die Appliance Spam-Mails erkannt hat, die durch andere Spam-Filter wie Spam-Assassin und kostenpflichtige Produkte unbehelligt durchgelassen wurden.

Vorteilhaft bei diesen Viren- und Spam-Scannern: Es ist unerheblich, über welches System und von welchem Provider die E-Mails ins Haus kommen – ob sie via POP3 abgefragt oder über SMTP zugestellt werden. Jeder Datenfluss über die Protokolle findet die passende Prüfung.

Virtual Private Network

Oft ist der Zugriff mit dem Notebook oder dem Heimarbeitsrechner auf die internen Daten gewünscht. Die Lösung dafür ist das VPN. Diese Funktion liefert die Appliance serienmäßig mit. Dabei konnten wir uns im Test zwischen der einfachen PPTP-Lösung, einer IPSec-Verbindung oder dem VPN-SSL-Zugriff entscheiden. Für den Einsatz von PPTP mussten wir lediglich den User aktivieren und haben über die Windows-Netzwerkeinstellung die VPN-Verbindung aufgebaut. Der Aufwand für die Einrichtung von IPSec war dagegen deutlich höher. Da wir IPSec über ein Zertifikat und nicht mit PSK einsetzen, mussten wir zunächst mit dem Zertifikatsmanager ein Host-, dann die jeweiligen Client-Zertifikate erstellen. Danach wurde die IPSec-Verbindung eingerichtet. Clientseitig haben wir den gateProtect-IPSec-Client verwendet. Dieser benötigt noch das IPSec-Zertifikat, das aus

dem Administrations-Client exportiert und auf dem Arbeitsplatz aktiviert wird. Für jeden VPN-Tunnel beziehungsweise jede Verbindung mussten wir dann das VPN-Objekt auf der Arbeitsfläche des Administrationsclients platzieren und mit dem internen Netzwerk verbinden. Das Objekt war damit der VPN-Endpunkt der Verbindung. Durch den bekannten Regeleditor legten wir auch hier wieder fest, welche Aktivitäten durch das VPN in das interne Netzwerk erlaubt waren.

Wissen, was passiert

Die Statistiken geben dem Administrator schnell Aufschluss darüber, welche Seiten am meisten frequentiert sind. Die Übersicht der Dienste lässt erkennen, welcher Dienst wie stark genutzt wurde. Aufschlussreich ist auch die Übersicht des Traffics nach Arbeitsplätzen. Die Übersicht der Abwehr zeigte in unserem Test zum Beispiel, dass innerhalb von nur vier Tagen 529.816 eingehende Zugriffe abgewiesen sowie 67 Viren über HTTP(S), vier über POP3 und 885 Spam-Nachrichten erkannt wurden – eine stolze Statistik. Das Balkendiagramm der abgewiesenen Zugriffe zeigte für einen Tag den Spitzenwert von 149.896 Hits.

Fazit

Die Appliance GPO-125 ist für Unternehmen mit bis zu 25 Mitarbeitern ausgelegt und als Stand-Alone-Gerät konzipiert. Bei etwa 300 Benutzern wird das Arbeiten über die Firewall sehr zäh. Trotz der gut gelungenen und intuitiv zu bedienenden eGUI von gateProtect ist die Konfiguration einer Firewall immer noch nichts für den einfachen Anwender. Das Handwerk selber ausführen zu können, befreit nicht von der Notwendigkeit zu wissen, was gemacht werden muss. Die Erfahrung zeigt, dass Anwender mangels Wissen eine Firewall oft komplett aufmachen. Der erfahrene Administrator jedoch kann durch die eGUI eine ganze Menge Zeit und Arbeit sparen. Die Drag-and-Drop-Funktion, die einfache Regelkonfiguration und die Benutzerauthentifizierung lassen in kurzer Zeit sonst mühevoll erstellte Si-

cherheitseinstellungen entstehen. Die erfolgreich eingesetzten Viren-, Content- und Spam-Filter als auch die VPN-Lösungen runden die Funktionalitäten ab. Die Appliance bietet allerdings wie die kleinere Variante GPO-75 keinen HTTPS-Proxy. Mit der gateProtect GPO-125 hatten wir nichtsdestotrotz ein Gerät im Test, das in seiner Bedienung und Funktionsweise als auch in der Preisgestaltung ein rundes Bild liefert – und das besitzt durchaus Seltenheitswert. (dr)

Produkt

Sicherheits-Appliance mit Firewall, Webproxy, VPN, Antivirus und Spam-Filter.

Hersteller

gateProtect
www.gateprotect.de

Preis

Appliance GPO-125:
ab 846 Euro
Sicherheits-Paket (Virus-, Web- und Spam-Filter):
1 Jahr: 295 Euro
3 Jahre: 797 Euro (entspricht 266 Euro/Jahr)

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Sicherheit/Zuverlässigkeit:	10
Regeldefinition:	9
Viren-/Spam-Erkennung:	9
Laufender Administrationsaufwand:	10
VPN-Zugriff:	9

Dieses Produkt eignet sich

optimal für kleinere und mittlere Unternehmen mit bis zu 25 Anwendern.

teilweise für Netzwerke mit 50 und mehr Usern.

nicht für den Schutz mit großem Datenverkehr-Aufkommen.

gateProtect GPO-125 V8.5

Portliste

www.it-administrator.de/downloads/
datenblaetter/1009-gateprotect-Portliste.pdf

Links

