

UTM-Appliances im Vergleichstest

Bösewichter bleiben draußen

Dr. Götz Güttich

Wenn es darum geht, Unternehmensnetze mit dem Internet zu verbinden, müssen die Administratoren umfassende Maßnahmen ergreifen, um für Datensicherheit zu sorgen. Während es früher oft genügte, einen NAT-Router – idealerweise mit einer integrierten Firewall – als Internet-Zugang zu verwenden, kommen heute noch viele andere Funktionalitäten wie Content Filter, Intrusion Protection und ähnliches hinzu, die die meisten Hersteller in einer so genannten Unified-Threat-Management-Appliance zusammenfassen.



Unified-Threat-Management-Lösungen (UTM) kommen üblicherweise in Appliance-Form und verfügen über mehrere Schnittstellen zum Anschluss von Computern im LAN und in der DMZ. Viele dieser Produkte bieten auch mehrere WAN-Ports, um Load-Balancing bei der Internet-Verbindung zu ermöglichen, beziehungsweise um einen Backup-Link zur Verfügung zu stellen, wenn der primäre Internet-Anbieter ausfällt. Abgesehen davon gehören typischerweise folgende Funktionen zum Leistungsumfang einer UTM-Lösung: Internet-Gateway, Firewall, Intrusion Protection System, VPN-Gateway, Contentfilter sowie Schutz vor Viren und

Spam. In der Regel sichern die Produkte darüber hinaus auch den Web-Verkehr ab, ermöglichen eine Benutzerauthentifizierung (beispielsweise um nur bestimmten Anwendern während zuvor festgelegter Zeiten den Zugriff auf bestimmte Webseiten zu gestatten) und bieten Quality-of-Service-Features. Zusätzlich lassen sich die genannten Lösungen meist in hochverfügbaren Konfigurationen nutzen (damit beim Internet-Zugang kein Single Point of Failure entsteht) und verfügen über umfassende Reporting-Funktionen, die den zuständigen Mitarbeitern schnell Anschluss über den Sicherheitsstatus ihrer Netze geben.



Dieser Text umfasst einen Auszug aus einem im August 2010 in den IAIT-Sonderseiten der Zeitschrift "IT-Administrator" veröffentlichten Vergleichstest von UTM-Appliances von Astaro, Gateprotect, Netgear und Sonicwall. Der Auszug konzentriert sich auf die Leistung der Gateprotect-Lösung im Test. Dr. Götz Güttich, Leiter des Testinstituts IAIT, das den Test durchgeführt hat, kam in Bezug auf die Gateprotect-Lösung zu folgendem Fazit:

"Bei der Gateprotect-Lösung sticht vor allem die gut gelöste grafische Regeldefinition ins Auge, die nicht nur dafür sorgt, dass Administratoren mit geringen Netzwerkkenntnissen dazu in die Lage versetzt werden, selbst komplexe Aufgaben auszuführen, sondern auch erfahrenen Netzwerkspezialisten viel Zeit sparen kann. Abgesehen davon verfügt das Produkt von Gateprotect über alle Funktionen, die man sich von einer UTM-Appliance wünscht. Bei unseren Sicherheitstests gab sich die Lösung ebenfalls keine Blöße, sie gilt damit als rundum empfehlenswert".

Der Test

Für diesen Test haben wir uns die GPA 400 vorgenommen. Im Mittelpunkt des Tests standen die Konfiguration und das Management der Lösung, da dies in den meisten Umgebungen die größte Rolle spielt. Was nützt schließlich ein Produkt, das einen großen Funktionsumfang vorweisen kann, wenn seine Bedienung so kompliziert ist, dass sich kein Administrator an das Konfigurationswerkzeug herantraut? Umständliche Konfigurationswerkzeuge stellen zudem eine große Zeitverschwendung dar und jeder Administrator wird lieber ein Produkt einsetzen, bei dem er für die Modifikation einer Firewallregel zwei Minuten

braucht, als eine Lösung, bei der er zunächst die Dokumentation zu Rate ziehen muss und dann den gleichen Vorgang erst nach zehn Minuten abschließen kann.

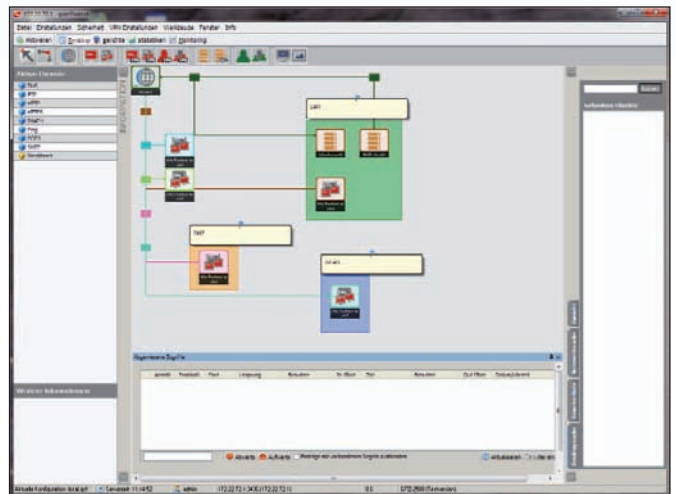
Konkret besteht der Test aus vier Teilen: Zuerst haben wir das betroffene Produkt in Betrieb genommen. Dieser Schritt besteht üblicherweise aus dem Anschluss der Appliance an das Netz und der Initialkonfiguration, die in der Regel mit Hilfe eines Wizards durchgeführt wird und die das Produkt soweit konfiguriert, dass von den Clients aus der Zugang zum Internet möglich ist. Die für diese Inbetriebnahme benötigte Arbeitszeit haben wir genauso festgehalten, wie die Zahl der zum Erreichen des genannten Ziels erforderlichen Arbeitsschritte. Als Arbeitsschritt definieren wir dabei das Klicken mit der Maus, das Ausfüllen einer Dialogbox und ähnliches.

Sobald die Appliance lief, verwendeten wir diverse Security-Werkzeuge wie beispielsweise den Portscanner Nmap, das Sicherheitstool Nessus sowie etliche andere Lösungen zum Durchführen von Penetrationstests und ähnlichen Maßnahmen, um festzustellen, wie sich das Produkt unter Last verhielt und ob sie in der Standardkonfiguration irgendwelche unnötigen Informationen über sich preisgab, die ein Angreifer für seine Zwecke nutzen könnte. Während des Tests setzten wir übrigens sowohl einen DSL-Anschluss als Internet-Zugang ein, als auch einen Fast-Ethernet WAN-Anschluss. Sämtliche Sicherheitstests fanden nicht nur an den internen, sondern auch an den externen Schnittstellen des Security-Produkts statt. Die Default-Konfiguration kam deshalb für das Security-Testing zum Einsatz, da wir bei allen Testschritten fest definierte Settings vor uns haben wollten. Bei Gateprotect waren in der Standardkonfiguration die wesentlichen Funktionen wie IPS und Gateway-Antivirus aktiv und die Firewall ließ allen Verkehr von innen nach außen zu, während gleichzeitig der Traffic in der Gegenrichtung geblockt wurde.

Im dritten Teil des Tests gingen wir das Konfigurationswerkzeug der Lösungen Schritt für Schritt durch, um uns einen Überblick über den Funktionsumfang des Produkts zu verschaffen und um die Konfiguration genau an unsere Bedürfnisse anzupassen. Nach dem Abschluss der Konfiguration kam die Lösung mehrere Tage lang zum Einsatz, um den Internetzugang für unser Testlabor sicher zu stellen. Dabei überprüften wir, wie sie sich im Alltag verhielt.

Als letzten Testschritt führten wir mit Hilfe des Lastgenerationswerkzeugs Ixchariot von Ixia (in der Version 7.10 mit Service Pack 1) noch diverse Messungen durch, um sicherzustellen, dass die Appliance auch wirklich so viel Verkehr verkraftete, wie von den Herstellern angegeben. Ixchariot stellt eine Lösung dar, die IT-Spezialisten in die Lage versetzt, den in einem Unternehmen typischen Webverkehr künstlich zu erzeugen und so große Netzlast unter realistischen Bedingungen zu generieren. Im Gegensatz zu den zuvor genannten Security-Tools ist diese Last nicht bössartig und hat nicht das Ziel, die Appliance zum Absturz oder zum Stehen zu bringen, sondern simuliert eben nur den von vielen Anwendern erzeugten Verkehr.

In der letzten Testphase führten wir mit der Lösung nicht nur allgemeine Durchsatztests auf Basis der Protokolle TCP und UDP durch, sondern analysierten auch das Verhalten des Produkts unter Last mit Protokollen wie FTP, NNTP und HTTP (wir verwendeten für unsere HTTP-Messungen ein Skript, das eine GIF-Datei übertrug, da wir vor allem



Mit dem Konfigurationsdesktop für die Firewall-Funktionalität verfügt Gateprotect über ein echtes Alleinstellungsmerkmal

den Durchsatz beim Übertragen größerer Files analysieren wollten, um den Protokolloverhead zu minimieren). In diesem Zusammenhang ist es wichtig darauf hinzuweisen, dass der Performance-Test aus zwei Teilen bestand. Die UTM-Hersteller liefern bei ihren Produkten üblicherweise Informationen über den Datendurchsatz mit, zum Beispiel 650 MBit/s für den VPN- oder den IPS-Durchsatz. Im Testlabor versuchten wir zum einen, diese Angaben zu verifizieren, zum anderen führten wir aber auch eigene Messungen mit Konfigurationen durch, die sich nicht nur auf einzelne Komponenten wie die Firewall oder das IPS bezogen, sondern auf die Funktionalität der Lösung als Ganzes mit allen aktiven Security-Features. Wir halten diesen Ansatz für realistischer, müssen allerdings zugestehen, dass die Ergebnisse dieser Messungen stark von unserer Standardkonfiguration und unserem Testumfeld abhängen und somit keine Allgemeingültigkeit besitzen.

Gateprotect GPA 400

Die Appliance von Gateprotect arbeitet mit sechs Ethernet-Ports zum Anschluss diverser Netzwerke. Das Produkt verwendet kein Webinterface, sondern eine Windows-basierte Konfigurationssoftware. Der Grund dafür liegt in der Konfiguration der Fire-

wallregeln, die mittels grafischer Elemente durchgeführt wird, dazu später mehr. Zum Einrichten der Appliance ist es also erforderlich, das Gerät im Netz in Betrieb zu nehmen (standardmäßig kommt es mit der IP-Adresse 192.168.0.254 auf dem ersten Interface), einen Windows-Client ins gleiche Subnetz zu verschieben, darauf die Konfigurationssoftware zu installieren (das läuft – wie bei Windows üblich – mit Hilfe eines Setup-Wizards ab) und diese abschließend zu starten. Daraufhin findet die Software die Appliance (sie sucht automatisch auf der Adresse 254 im aktuellen Subnetz) und der Administrator kann sich mit den Default-Accountdaten “admin”/”admin” einloggen.

Nach dem ersten Login fragt ihn der Konfigurationsclient zunächst, ob ein Schnellstart-Wizard abgearbeitet werden soll, oder ob der zuständige Mitarbeiter alles manuell über die Konfigurationsoberfläche einrichten möchte. Wir entschieden uns dazu, zunächst den Wizard laufen zu lassen und die Konfiguration dann manuell an unsere Wünsche anzupassen.

Im ersten Schritt bietet der Assistent an, die Dienste HTTP, HTTPS, DNS, FTP, POP3, SMTP, IMAP4, NetBIOS, Kerberos, LDAP und RDP im Netz zu erlauben. Danach geht es an die Konfiguration des WAN-Zugangs, hier unterstützt das Produkt ISDN, klassisches Routing, PPPoE und PPTPoE. Sobald die entsprechenden Angaben gemacht wurden, möchte der Wizard noch wissen, ob der DNS-Server manuell festgelegt wird, oder ob die Server des Providers zum Einsatz kommen sollen. Anschließend können die Administratoren noch zwei externe Server angeben, die die UTM-Appliance regelmäßig kontaktiert, um zu prüfen, ob eine Internet-Verbindung besteht. Zum Schluss fragt der Assistent nach der Konfiguration von NTP und Zeitzone, führt ein Update der Antivirus-Lösung von Kaspersky durch und möchte ein Passwort für den SSH-Zugriff auf die Konsole der Appliance wissen. Damit ist das Initialsetup abgeschlossen und die Internetverbindung steht. Bei uns war es

anschließend nur noch erforderlich, die Konfiguration des LAN-Interface manuell anzupassen. Im Test benötigten wir zum Einrichten der Appliance knapp 20 Minuten und 15 Arbeitsschritte.

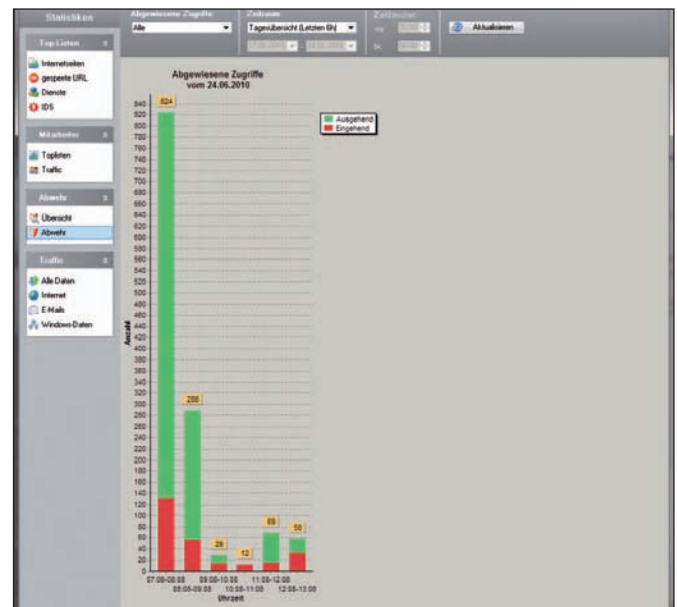
Sicherheitstest

Beim Sicherheitstest fanden Nessus und nmap heraus, dass auf dem internen Interface die Ports für SSH und DNS offen waren, das war aber auch so gewollt. Ansonsten ergaben sich weder intern noch extern irgendwelche Überraschungen oder Unregelmäßigkeiten und die Appliance arbeitete auch während DoS-Angriffen problemlos weiter. Diesen Teil des Tests hat das Produkt also mit Bravour bestanden.

Funktionsumfang

Nach dem Einloggen bei der Appliance findet sich der IT-Verantwortliche im Arbeitsbereich für die grafische Regelerstellung wieder. Hier ist es möglich, Netzwerkelemente wie Server, Netzwerke, Clients, DMZ-Anschlüsse, VPN-Verbindungen, Benutzer und ähnliches als Icons darzustellen, zwischen diesen Icons Linien zu ziehen und dann diesen Linien bestimmte Berechtigungen zuzuweisen. Die Firewallkonfiguration erfolgt also nicht wie bei den anderen Produkten nach Regellisten oder Matrizen, sondern mit Hilfe grafischer Darstellungen des Netzwerks. Dieser Ansatz wirkt sehr übersichtlich und eingängig. Um beispielsweise eine SSH-Verbindung ins Internet zu erlauben, reicht es, ein LAN-Subnetzicon mit der dazugehörigen Netzwerkadresse zu definieren, ein Icon für die Internet-Verbindung

anzulegen (standardmäßig erzeugt die Software bereits bei der Grundkonfiguration Icons für das Internet und die Netze an allen Ethernet-Ports der Appliance), dann mit dem dafür vorgesehen Tool eine Verbindungslinie zwischen den beiden Icons zu zeichnen und danach auf diese Linien doppelzuklicken. Daraufhin öffnet sich ein Fenster, in dem die Administratoren das SSH-Protokoll und die Richtung des freizugehenden Datenverkehrs auswählen können. Das Anlegen der Icons läuft einfach durch das Ziehen einer entsprechenden Vorlage (für Clients, Server und so weiter) aus der Iconleiste ab, nach einem Doppelklick lassen sich dem Icon dann Informationen wie die IP-Adresse und ähnliches hinzufügen. Selektiert der zuständige Mitarbeiter eine Verbindungslinie mit der Maus, so erscheint in einem Bereich links im Konfigurationsfenster eine Liste mit den auf der jeweiligen Verbindung freigegebenen Diensten. Links unten finden sich darüber hinaus Details zum gerade aktiven Objekt, wie etwa die dazugehörige IP-Adresse. Die Objekte lassen sich jederzeit zu Gruppen zusammenfassen, mit Notizen versehen oder mit unterschiedlichen Farben unterlegen, um Regionen wie das LAN oder die DMZ hervorzuheben. Das Konfigurationsinterface bleibt also



Die Statistikfunktionen der Gateprotect-Appliance liefern den zuständigen Mitarbeitern einen schnellen Überblick über den Sicherheitsstatus ihrer Netzwerke

auch bei komplexen Szenarien übersichtlich und der grafische, leicht verständliche Konfigurationsansatz hilft nicht nur unerfahrenen Administratoren bei der Arbeit, sondern kann auch Profis viel Zeit sparen. Eine Suchfunktion zum schnellen Auffinden bestimmter Objekte rundet den Leistungsumfang der Firewallkonfiguration ab. Im Betrieb ist es außerdem jederzeit möglich, eigene Dienste und ähnliches zur Konfiguration hinzuzufügen.

Die Berichte und Statistiken stehen über weitere Arbeitsfenster zur Verfügung. Die Lösung bietet den Administratoren darin diverse Berichte, die sich mit Themen wie dem IDS, dem System und ähnlichem befassen.

Die Statistiken lassen sich nach Benutzern, Desktops, dem gesamten Netz und vergleichbaren Faktoren erstellen und liefern Top-Listen zu den Datenübertragungen, bestimmten Diensten, Internetseiten, gesperrten URLs und so weiter. Es stehen auch Übersichten über abgewiesene Zugriffe, gefundene Viren und Vergleichbares zur Verfügung.

Über das Monitoringfenster haben die zuständigen Mitarbeiter Zugriff auf eine Systemübersicht, die Festplattenauslastung, den Netzwerkstatus, Informationen über die Partitionsauslastung, den Netzwerkverkehr, die Festplattenzugriffe, die laufenden Prozesse mit der von ihnen erzeugten Last und ähnliches. Insgesamt stellt das System von Gateprotect 15 vordefinierte Reports bereit.

Alle bis jetzt noch nicht genannten Funktionen – also sämtliche Features mit globaler und nicht userbezogener Wirkung – werden über Befehle konfiguriert, die sich über die Menüleiste aufrufen lassen. In diesem Zusammenhang sind zunächst die Spracheinstellungen (das System unterstützt neben Deutsch auch Englisch, Französisch, Spanisch und Italienisch) und die Zeiteinstellungen zu erwähnen. Dazu kommen noch die Konfiguration der Interfaces, Bridges, VLANs und SSL-VPN-

Schnittstellen sowie das Routing mit statischen Einträgen, RIP und OSPF.

Die Benutzerverwaltung steht ebenfalls über die Menüleiste zur Verfügung. Den Benutzerkonten lassen sich hier Rechte auf den Administrationsclient oder den Statistikclient zuweisen. Es ist sogar möglich, ihnen den Zugriff auf einzelne Module der Software zu gestatten, wie etwa den Konfigurationsdesktop, die DHCP-Einstellungen und so weiter.

Unter “Internet” besteht unter anderem die Möglichkeit, Internetzugänge (bei Bedarf auch mit Backupleitung) zu definieren, externe Systeme anzupingen und DynDNS-Konten zu verwalten. Außerdem lassen sich über die Menüleiste Einstellungen zu Traffic Shaping und QoS vornehmen, der Proxy konfigurieren (transparent, intransparent, mit Cache-Größe, beim SSL-Proxy auch mit Zertifikaten) und die Hochverfügbarkeitssettings festlegen. Dazu kommen noch Settings zum DHCP-Server, zum Reporting (für das automatische Versenden von Reports per E-Mail) und die Benutzerliste, die nicht nur lokale Benutzer unterstützt, sondern auch Active-Directory- beziehungsweise LDAP-Authentifizierung und Single-Sign-On mit Kerberos. An gleicher Stelle finden sich darüber hinaus Konfigurationen für die automatischen Systemupdates, die standardmäßig täglich ablaufen.

Unter “Sicherheit” bietet die Konfigurationssoftware alle Optionen zum Verwalten des Contentfilters, des Mailfilters und der Antivirus-Funktion. Der Contentfilter arbeitet mit Dateiendungen und Kategorien wie “Finanz- und Infodienste”, “Freizeit”, “Gesellschaft” und so weiter. Der Mailfilter verwendet Black- und Whitelists und bietet eine Antispam-Funktion, die gefundenen Spam auf Wunsch kennzeichnen kann. Die Antivirusfunktion untersucht die Protokolle HTTP, FTP, POP3 und SMTP und lässt sich unter anderem auch für gepackte Dateien aktivieren. Eine so ge-

nannte Vertrauensliste dient zur Definition vertrauenswürdiger Hosts, deren HTTP- oder FTP-Verkehr nicht untersucht wird. Die minimale Intervall-Zeit für die Updates der Antivirus-Pattern liegt bei einer Stunde. Settings zu Zertifikaten, dem IPS mit Regelgruppen und ähnliches runden den Leistungsumfang dieses Bereichs ab.

Die restlichen Menüpunkte befassen sich mit den IPSec- und SSL-VPNs mit den dafür üblichen Einstellungen (zum Einrichten der VPNs stehen auch Wizards und Importfunktionen zur Verfügung) und liefern den Administratoren diverse Werkzeuge in die Hand. Zu letzteren gehören unter anderem Ping, Traceroute und DNS-Lookups.

Lasttest

Für den Test führten wir mit Ixchariot diverse Skripts aus, die generellen TCP-Verkehr erzeugten und Licht auf die Leistung der Appliance bei der Arbeit mit den Protokollen HTTP, HTTPS, FTP, DNS und NNTP warfen. Dabei kamen wir zu dem Ergebnis, dass die Lösung die Herstellerangaben in Bezug auf den Datendurchsatz im Großen und Ganzen einhielt. Laut Gateprotect schafft das Produkt einen Firewalldurchsatz von 1,4 GBit/s, während der VPN-Durchsatz bei 190 MBit/s liegt. Im nächsten Schritt des Performancetests verwendeten wir die bereits angesprochene allgemeine UTM-Konfiguration, um einen Einblick in die Leistung des Systems während der praktischen Arbeit an einem Ethernet-WAN-Anschluss zu erlangen. In diesem Szenario lag der durchschnittliche TCP-Durchsatz bei 88,594 MBit/s. HTTP-GIF-Übertragungen erreichten einen maximalen Durchsatz von 26,076 MBit/s, bei FTP lag der Wert bei 68,303 MBit/s beim Hoch- und 74,392 MBit/s beim Herunterladen. DNS-Lookups arbeitete die Appliance mit 3,693 MBit/s ab, bei NNTP lag der entsprechende Wert bei 15,814 MBit/s. Mit dem Lasttest war unsere Analyse abgeschlossen und wir kamen zu dem auf Seite 1 publizierten Fazit.