

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. IAIT hat sich vier dieser Lösungen, nämlich die Produkte von Astaro, Gateprotect, Netgear und Sonicwall, genau angesehen.

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 Aufschluss über den Sicherheitsstatus ihrer Netze geben.

Der Test

Für diesen Test haben wir uns Appliances für mittelgroße Unternehmensnetze mit um die 300 Arbeitsplätzen vorgenommen. Der Grund dafür liegt darin, dass diese Produkte üblicherweise in den Hauptniederlassungen mittelständischer Unternehmen zum Einsatz kommen und damit den Grundstein für die Sicherheitsarchitektur dieser Organisationen darstellen. Im Mittelpunkt des Tests standen die Konfiguration und das Management der Lösungen, 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 Initalkonfiguration, 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 die Lösung 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 der Security-Produkte statt. Die Default-Konfiguration kam deshalb für das Security-Testing zum Einsatz, da wir bei allen Produkten vergleichbare Settings vor uns haben wollten. Üblicherweise 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 der Produkte zu verschaffen und um die Konfiguration genau an unsere Bedürfnisse anzupassen. In diesem Zusammenhang überprüften wir auch die Usability der Produkte und beantworteten beispielsweise Fragen wie „Wie groß ist die Zahl der Schritte, die zum Aktivieren eines URL-Filters nötig sind?“ und „Wie viele Schritte benötigt der Administrator zum Ändern einer Firewallregel?“. Nach dem Abschluss der Konfiguration kam die jeweilige Appliance 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 Appliances auch wirklich so viel Verkehr verkraften, 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 bösartig und hat nicht das Ziel, die Appliance zum Absturz oder zum Stehen zu bringen, sondern simu-

liert eben nur den von vielen Anwendern erzeugten Verkehr. In der letzten Testphase führten wir mit den Lösungen nicht nur allgemeine Durchsatztests auf Basis der Protokolle TCP und UDP durch sondern analysierten auch das Verhalten der Produkte 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 den Durchsatz beim Übertragen größerer Files analysieren wollten, um den Protokoll-Overhead 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. Innerhalb des Tests lassen sie sich aber durchaus für Vergleiche heranziehen.

Netgear Prosecure Unified Threat Management UTM25

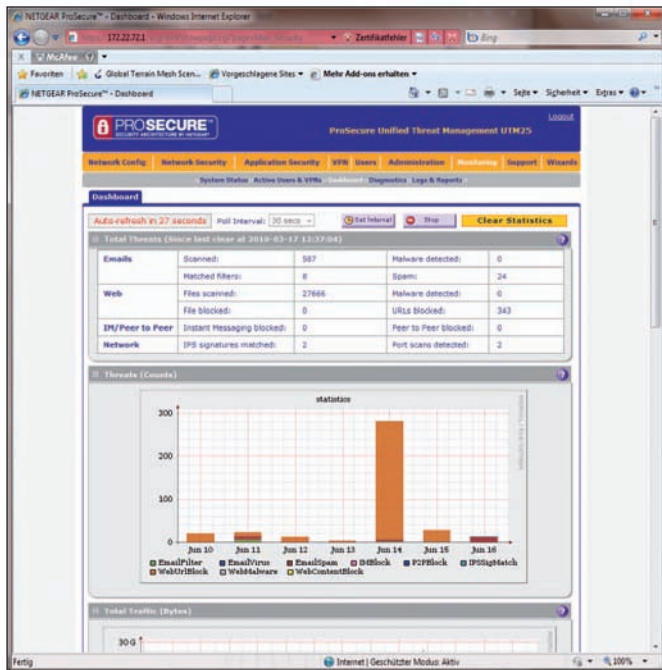
Die erste Appliance im Test, die Prosecure Unified Threat Management UTM25, stellt gleich die erste (und einzige) Ausnahme dar. Sie eignet sich nämlich nicht für Unternehmensumgebungen mit 300 Arbeitsplätzen, sondern unterstützt lediglich bis zu 30 Client-Systeme. Der

Grund dafür liegt darin, dass Netgear zur Zeit noch an einem leistungsfähigeren System arbeitet, das den gleichen Funktionsumfang wie die UTM25 haben wird, größere Umgebungen unterstützen soll und wohl im zweiten Halbjahr 2010 auf den Markt kommt. Da bei uns der Funktionsumfang im Mittelpunkt des Tests stand, waren wir in diesem Fall der Meinung, dass es legitim ist, die genannte Ausnahme zu machen. Die UTM25 kommt mit vier LAN- und zwei WAN-Anschlüssen und unterstützt bis zu 25 VPN-Tunnel.

Inbetriebnahme

Netgear liefert sein Produkt mit einem gedruckten Schnellstart-Guide und einer CD mit dem VPN-Client und der Dokumentation. Die Schnellstartanleitung reichte für uns zur Inbetriebnahme des Produkts vollkommen aus, so dass wir nicht auf die Handbücher in elektronischer Form zurückgreifen mussten. Nach dem Hochfahren der Hardware genügt es, wenn sich der Administrator mit der Default-Adresse <https://192.168.1.1> verbindet und sich mit den Standardanmeldedaten "admin" und "password" bei der Appliance anmeldet. Daraufhin landet er im Konfigurationswerkzeug und kann den Setup-Wizard aufrufen, der die Initialkonfiguration durchführt. Dieser fragt zunächst nach der LAN-Konfiguration mit IP-Adresse, DNS-Servern und Proxy und möchte dann die WAN-Konfiguration für den Internetzugang wissen. Es ist auch möglich, das Gerät als DHCP-Server einzusetzen, der den Clients im LAN automatisch IP-Adressen zuweist. Was die WAN-Verbindungen angeht, unterstützt das Produkt neben einer Arbeitsweise als DHCP-Client auch feste IP-Adressen, PPTP sowie PPPoE für DSL-Anschlüsse. Im nächsten Schritt folgen die Defi-





Das Dashboard der Netgear-Appliance liefert den Administratoren einen schnellen Überblick über den aktuellen Sicherheitsstatus

dition der Zeitzone und die NTP-Konfiguration, bevor es an die Angabe der zu überwachenden Ports geht. Hier bietet die Lösung die Ports 25(SMTP), 110 (POP3), 143 (IMAP), 80 (HTTP), 443 (HTTPS), 21 (FTP) sowie Settings für Instant Messaging und Bittorrent an. Sobald diese Angaben gemacht wurden, geht es daran, der Appliance mitzuteilen, was sie mit infizierter Mail machen soll. Hier stehen die Optionen “Blockieren”, “Löschen” und “Loggen” zur Verfügung.

In der Rubrik zur Web Security legen die IT-Verantwortlichen anschließend fest, ob das Produkt HTTP-, HTTPS- und FTP-Verkehr überwacht. Im nächsten Schritt geht es an die Angabe der zu blockierenden Web-Kategorien. Hier bietet die Lösung eine Vielzahl unterschiedlicher Einstellungsmöglichkeiten an, dazu gehören unter anderem “Commerce”, “Drugs and Violence”, “Leisure and News” sowie “Technology”. An dieser Stelle fällt auf, dass es sich um ein US-amerikanisches Produkt handelt, beispielsweise existiert eine Kategorie “Politics and Religion”, die diese beiden doch etwas unterschiedlichen Themenbereiche

zusammenfasst. Der Contentfilter lässt sich auch mit einem Scheduler kombinieren, so dass die Sperrungen der Webseiten bei Bedarf nur zu bestimmten Tageszeiten aktiv sind. Auf diese Weise kann ein Unternehmen beispielsweise während der Mittagspause oder nach Feierabend den Zugriff auf Freizeitangebote freigeben und während der Arbeitszeit sperren, eine sehr sinnvolle Lösung. Zum Abschluss des Wizards geben die Adminis-

tratoren noch an, an welche Adresse das System E-Mail-Benachrichtigungen verschicken soll (dabei unterstützt die Appliance auch SMTP-Server, die eine Authentifizierung verlangen) und auf welche Weise die Appliance automatische Updates durchführt. Das schließt die Initialkonfiguration ab und der Internetzugang funktioniert. Im Test hielten wir uns bei der Arbeit mit dem Wizard soweit wie möglich an die vom Hersteller vorgegebenen Default-Einstellungen und benötigten zur Inbetriebnahme des Systems 18 Arbeitsschritte. Der ganze Vorgang war nach einer Viertelstunde abgeschlossen. Generell kann man zur Inbetriebnahme sagen, dass sie schnell und einfach von der Hand geht und keinen Administratoren vor irgendwelche Schwierigkeiten stellen wird. Negativ fiel uns allerdings auf, dass der Setup-Wizard die IT-Mitarbeiter nicht zwingt, das Administratorpasswort zu ändern. Diesen Schritt, der unserer Meinung nach ebenfalls zur Initialkonfiguration gehört, mussten wir im Test während des Betriebs manuell nachholen. Folglich ist es möglich, die Lösung mit einem Standardpasswort im Netz arbeiten zu lassen, was eine potentielle Sicherheitslücke dar-

stellt. Der Hersteller vertritt – im Gegensatz zu uns – die Meinung, da es sich bei der UTM25 um ein Produkt für den professionellen Einsatz und um kein Consumerprodukt handle, sei der Zwang zum Ändern des Passworts nicht erforderlich, da die Administratoren schon wissen würden, was sie tun.

Der Sicherheitstest

Beim Portscan des internen Interfaces fanden wir heraus, dass die Ports 23 (Telnet) sowie 80 (HTTP) und 443 (HTTPS, die beiden letzten für das Konfigurationswerkzeug) offen waren. Nessus stellte darüber hinaus nichts ungewöhnliches fest. 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

Wenn sich ein Administrator im laufenden Betrieb beim Konfigurationswerkzeug anmeldet, so landet er in einer Systemübersicht, die Aufschluss über die Hardwareauslastung und ähnliches gibt. Gehen wir an dieser Stelle aber genauer auf den Funktionsumfang und den Aufbau des Managementwerkzeugs ein. Das Tool arbeitet – wie praktisch alle Lösungen dieser Art – mit einer Menüstruktur. Der erste Punkt in diesem Menü befasst sich mit der Netzwerkkonfiguration. Hier können die zuständigen Mitarbeiter die beiden WAN-Interfaces der Appliance mit Auto-Rollover und Load-Balancing konfigurieren, die DynDNS-Konfiguration vornehmen und einen Traffic-Meter einrichten, der bei Bedarf beim Erreichen eines Schwellenwerts sämtlichen Verkehr unterbindet (auf bereits erwähnte oder selbstverständliche Optionen wie das Zuweisen von IP-Adressen gehen wir in diesem Testbericht aus Platzgründen nicht weiter ein). Die LAN-Einstellungen umfassen Funktionen zum Einrichten von

VLANs, die mit den vier LAN-Interfaces der Appliance (von denen eines allerdings normalerweise für die DMZ vorgesehen ist) arbeiten.

Der nächste Menüpunkt nennt sich "Network Security" und stellt das Herzstück der Appliance dar. Hier konfigurieren die Administratoren die Firewall mit Regeln, die sie dem System – wie bei solchen Lösungen üblich – in Form von Listen mitteilen. Diese Regeln setzen sich im Wesentlichen aus dem Dienst (also FTP, SMTP, etc.), der Aktion (Blocken, Durchlassen, etc.), den LAN-Benutzern (einzelne Adresse, Adressbereich, Gruppe), den WAN-Benutzern, dem QoS-Profil und dem Bandbreitenprofil zusammen. Auf diese Weise haben die zuständigen Mitarbeiter beispielsweise die Option, HTTPS-Verkehr aus dem Internet zu einem bestimmten Server im LAN zuzulassen. Abgesehen davon bietet die Firewall auch noch Funktionen zum Blockieren von TCP- und UDP-Floods und zum VPN-Passthrough.

Die Konfiguration des IPS läuft einfach nach Pattern für bestimmte Angriffsmuster. Diese können die Administratoren je nach Beschaffenheit ihrer Infrastruktur aktivieren oder deaktivieren. Wenn beispielsweise kein Oracle-Server im Unternehmen existiert, muss das IPS auch keine Angriffe auf Oracle-Systeme im Auge behalten, und es gibt keinen Grund, die dazugehörigen Ressourcen nicht für andere Aufgaben freizumachen. Das IPS ist auch dazu in der Lage, die Firewall so umzukonfigurieren, dass sie erkannte Angreiferadressen für einen bestimmten Zeitraum (standardmäßig sind das fünf Minuten) automatisch sperrt.

In der Konfiguration der Firewallobjekte lassen sich Dienste definieren (mit Port und Typ, also TCP, UDP oder ICMP), QoS- und Bandbreitenprofile anlegen und Zeitpläne für die Gültigkeitsdauer der Regeln einrichten. Der Adressfilter dient im Gegensatz dazu zum Ausfiltern bestimmter MAC-Adressen.

Unter „Application Security“ finden die zuständigen Mitarbeiter die Einstellungen zum Überwachen diverser E-Mail-, Web-, Instant-Messaging- und Peer-to-Peer-Services. Dazu kommen Funktionen zum Einrichten der Mailfilter und der Antivirusfunktion von Sophos (mit dem Einfügen von Warnungen in die Betreffzeile beziehungsweise dem Löschen infizierter Attachments). Die Mailfilter können Mails nach Dateitypen und Schlüsselwörtern ausfiltern.

Die Antispamfunktion arbeitet mit White- und Blacklists sowie den Realtime-Blacklists von Spamhaus und Spamcop, bei Bedarf lassen sich aber auch eigene Listen hinzufügen. Darüber hinaus steht für SMTP und POP3 ein System für Distributed Spam Analysis zur Verfügung, das einen heuristischen Scan durchführt.

Bei den HTTP/HTTPS-Einstellungen aktivieren die Administratoren Malware-Scans und den Content Filter mit den bereits erwähnten Kategorien. Letzterer kann auch Erweiterungen ausfiltern, Datenübertragungen nach Keywords blockieren und Inhalte wie Active-X beziehungsweise Javascript unterdrücken. Der URL-Filter verwendet wieder Black- und White-Listen, die auch Wildcards unterstützen. Auf Wunsch ist die Appliance zusätzlich dazu in der Lage, HTTPS-Verkehr mit Hilfe eines Proxies zu überwachen. Abgesehen davon existiert noch eine Liste mit "Trusted Hosts", deren HTTPS-Datenübertragungen nicht überwacht werden. Für den FTP-Verkehr lassen sich ähnliche Filter implementieren, im Test ergaben sich dabei keine Probleme.

An VPNs unterstützt die Appliance IP-Sec-VPNs (mit den dafür erforderlichen Settings für IKE, Algorithmen, PSK, SA Lifetime, Radius-Authentifizierung und so weiter) und SSL-VPNs. Zum Konfigurieren der VPNs stehen auch zwei Wizards zur Verfügung, die uns im Test vor keinerlei Schwierigkeiten stellten.

Die Benutzerverwaltung der Appliance arbeitet mit einer lokalen Benutzerliste, hierbei unterstützt die Lösung Administrationskonten, IPsec-VPN-User, SSL-VPN-Benutzer und Guests. Alle Benutzer lassen sich auch zu Gruppen hinzufügen. Darüber hinaus arbeitet das System zur Authentifizierung mit Diensten wie Radius, NT-Authentifizierung, Active Directory und LDAP zusammen.

Ansonsten ist noch der Menüpunkt „Administration“ von Interesse. Hier lassen sich das Remote Management via WAN-Port mit HTTPS aktivieren, die SNMP-Konfiguration vornehmen, die Einstellungen sichern und wieder herstellen, die Systemupdates konfigurieren (für die Pattern, die Engine und die Firmware, standardmäßig liegt das Update-Intervall bei einer Stunde) und die Zeitzone festlegen.

Die Monitoring-Funktionen umfassen zunächst die bereits erwähnte Systemstatus-Seite mit CPU-Last, Diskauslastung, aktiven Diensten, Firmware- und Patternversionen und so weiter. Im Test kam bei uns die Firmware 1.0.23-0 zum Einsatz. Außerdem gibt es noch Listen für aktive Benutzer und VPN-Verbindungen und ein Dashboard. Mit Hilfe dieser ganzen Informationen können die zuständigen Mitarbeiter sich schnell ein Bild über den Status ihrer Netzwerkanbindung machen.

An Diagnosefunktionen stellt das Produkt Ping, DNS-Lookups und ähnliches bereit. Zusätzlich bietet die Appliance auch noch eine große Zahl an Log-Dateien, beispielsweise zu "Sicheren Loginversuchen", "Neustarts", dem "WAN Status" und so weiter. Die Logs lassen sich bei Bedarf auch per Mail an den Administrator schicken. Insgesamt hat Netgear zudem 13 Reports vordefiniert.

Der 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 folgenden Ergebnissen: Nach Angaben des Herstellers bietet die Appliance einen Antivirus-Durchsatz von 15 MBit/s. Bei der Firewall liegt der gleiche Wert bei 127 MBit/s und bei VPN-Verbindungen bei 70 MBit/s. Diese Herstellerangaben erfüllte die Lösung im Großen und Ganzen gut. 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 10,237 MBit/s. HTTP-GIF-Übertragungen gingen mit 8,323 MBit/s über die Bühne, bei FTP lag der Wert bei 11,612 beim Hoch- und 13,353 beim Herunterladen. DNS-Lookups arbeitete die Appliance mit 0,937 MBit/s ab, bei NNTP lag der Durchsatzwert bei 3,711 MBit/s. Bei diesen Werten muss man im Hinterkopf behalten, dass es sich um die in Bezug auf die Performance schwächste Hardware im Testumfeld handelt, deswegen sind die Werte nicht eins zu eins mit denen der anderen Produkte im Test vergleichbar.

Zusammenfassung

Die Netgear-Prosecure-Unified-Threat-Management-UTM25-Appliance war im Test schnell eingerichtet. Ihr Funktionsumfang umfasst alles, was sich ein Administrator von einer UTM-Appliance erwartet. Das Konfigurationswerkzeug ist übersichtlich und lässt sich von IT-Mitarbeitern mit Netzwerkkenntnissen – auch wegen der guten Online-Hilfe – problemlos und intuitiv bedienen. Die Arbeit mit der Lösung ging folglich flott von der Hand und es kam nie zu Schwierigkeiten. Das Produkt konnte aber nicht nur bei Konfiguration und Administration überzeugen, sondern gab sich auch im Sicherheitstest keine Blöße und erfüllte während des Performance-Testings voll die Erwartungen. Zum Schluss noch kurz

ein paar Angaben zur Usability: Der Administrator benötigt vier Arbeitsschritte, um eine Firewall-Regel zu ändern und fünf Arbeitsschritte, um eine URL-Filterkategorie zu aktivieren.

Astaro Security Gateway 220

Die Astaro-Appliance kommt mit acht Ports und unterstützt laut Angaben des Herstellers 75 bis 300 Benutzer. Zur Inbetriebnahme der Lösung genügt es, das Produkt mit dem Netzwerk zu verbinden und hochzufahren. Anschließend können die Administratoren über die URL <https://192.168.0.1:4444> auf den Setup-Wizard des Systems zugreifen. Dieser präsentiert zunächst einen Willkommensbildschirm und fragt dann nach Hostnamen, Unternehmensnamen sowie der Stadt und dem Land, in dem die Appliance zum Einsatz kommt. Darüber hinaus müssen die IT-Mitarbeiter an dieser Stelle das Administratorpasswort ändern, eine sehr sinnvolle Maßnahme, da diese verhindert, dass irgendwelche Produkte mir Standardpasswörtern im Netz aktiv sind. Wurden die genannten Schritte abgearbeitet, erscheint der Login-Screen. Nach dem Einloggen startet automatisch ein Assistent, der die Initialkonfiguration durchführt. Er ermöglicht das Einspielen alter Konfigurationsdaten aus einer Datei, das Hochladen eines Lizenz-Files, die Konfiguration des LAN (mit DHCP-Server), das Einrichten des WAN-Anschlusses (statisch, DHCP, PPPoE oder PPPoA) und das Freigeben externer Dienste. Im Rahmen des Setups bietet das System für letzteres die Services HTTP, HTTPS, FTP, Citrix, Apple Remote Desktop, RDP, SSH, Telnet, SMTP, POP3, IMAP, SIP, H.323 und Instant

Messaging. Beim Instant Messaging unterstützt Astaro unter anderem AOL, Google Talk, ICQ, IRC und Yahoo. Es besteht also schon beim ersten Setup die Option, die Firewall relativ genau an die jeweiligen Bedürfnisse anzupassen.

Im nächsten Schritt wendet sich der Wizard der Konfiguration des IPS zu. Hier haben die zuständigen Mitarbeiter die Option, Abwehrmaßnahmen gegen Angriffe auf Windows, Linux, Web-Server, Mail-Server und Datenbankserver zu aktivieren. Funktionen zum Blocken von Instant-Messaging- und Peer-to-Peer-Verkehr, zum Durchsuchen des Verkehrs nach Viren und Spyware, zum Einrichten des Content Filters und zum Konfigurieren der Sicherungsfunktionen für den Mail-Verkehr runden den Leistungsumfang des Assistenten ab. Im Test benötigten wir für die Inbetriebnahme des Systems knapp 20 Minuten und es waren 36 Arbeitsschritte nötig, was bei der umfassenden Konfiguration nicht zu viel ist. An Content-Filter-Kategorien bietet Astaro übrigens "Community/Education/Religion", "Criminal Activities", "Drugs", "Extremistic Sites", "Finance/Investing", "Games/Gambles", "Nudity" und ähnliches an.

Beim Einrichten der Appliance traten im Test keine Probleme auf und die Setup-Routinen wurden so gestaltet, dass im Betrieb wohl kein Administrator irgendwelche Schwierigkeiten bekommen wird.

Sicherheitstest

Im nächsten Schritt unterzogen wir die Appliance der bereits aus dem Test des Netgear-Geräts bekannten Security-Ana-





Auch bei Astaro erfahren die zuständigen Mitarbeiter sofort, was im Netz los ist

lyse. Dabei ergaben sich keine nennenswerten Probleme, es ist lediglich erwähnenswert, dass die Appliance in der Standardkonfiguration auf einen externen Ping antwortet und dass das System defaultmäßig den Download von Dateitypen wie EXE, MSI und ähnlichem unterbindet. Ohne eine Anpassung der Regeln kann also im internen Netz niemand eine Installationsdatei aus dem Internet herunterladen, die Defaulteinstellungen sind also durchaus restriktiv. Nmap fand während eines Scans des internen Ports heraus, dass die Appliance mit Linux-2.6 lief und dass die Ports für DNS, POP3, das Konfigurationswerkzeug und den Proxy geöffnet waren. Das war durchaus alles so wie gewollt.

Funktionsumfang

Wenn sich der Administrator im täglichen Betrieb bei der Appliance anmeldet, so landet er zunächst in einer Dashboard-Übersicht, die ihm Informationen über den Typ, die Uptime, die Firmware-Version (im Test war das die 7.504), die Auslastung und die aktuellen Bedrohungen präsentiert. Die jeweiligen Konfigurationsoptionen stehen dann – wie bei sol-

chen Lösungen üblich – über eine Menüstruktur auf der linken Seite zur Verfügung. Im Test fiel uns auf, dass der Funktionsumfang der Appliance relativ groß ist und dass sich dementsprechend viele Einträge im Konfigurationsmenü befinden, so dass wir hier aus Platzgründen bei weitem nicht auf alles eingehen können, was das System bietet. Trotzdem konnte der Hersteller die einzelnen Einträge thematisch

so ordnen, dass auch ein Administrator, der nicht regelmäßig mit der Lösung arbeitet, dazu in die Lage versetzt wird, in den meisten Fällen schnell die Punkte zu finden, die er gerade benötigt, und zwar ohne großes Studium der Dokumentation.

Im Bereich “Verwaltung” finden sich nicht nur Systemeinstellungen wie Hostname, Zeitzone und die Passwortkonfiguration, sondern auch Settings zum Web-Interface selbst, mit dem Idle-TIMEOUT und der Zugriffssteuerung. An gleicher Stelle lässt sich das System auch so konfigurieren, dass es das Konfigurationstool nach drei fehlgeschlagenen Login-Versuchen für einen definierten Zeitraum sperrt (standardmäßig sind das zehn Minuten).

Das Update der Antivirus-Pattern (Astaro setzt auf der Appliance übrigens Avira und Clam-AV ein) erfolgt mit einem Default-Intervall von 15 Minuten und die gesamte Konfiguration lässt sich jederzeit – bei Bedarf auch automatisch – in eine Datei sichern. Es ist sogar möglich, die Konfigurationsbackups per Mail versenden zu lassen.

Ebenfalls von Interesse ist das Benutzerportal, über das die Anwender auf die Appliance zugreifen können, beispielsweise um Mails einzusehen, die das System unter Quarantäne gestellt hat. Dieses unterstützt 16 verschiedene Sprachen von Arabisch bis Türkisch und ermöglicht es den Usern zudem, Whitelists mit Mail-Adressen zu erstellen, die das UTM-Produkt auf keinen Fall ausfiltern darf.

Was die Benachrichtigungen angeht, so versendet die Lösung nicht nur Alerts bei Intrusion-Prevention-Alarmen, sondern auch bei Systemereignissen wie Restarts, Wechseln der Masterrolle im Cluster, fehlgeschlagenen Speicherversuchen von Logdateien und ähnlichem. Es steht auch eine Selbstüberwachung zur Verfügung, die den Syslog-Server, den DHCP-Daemon oder auch den SSH-Server neu startet, wenn eine dieser Komponenten sich aufgehängt hat. Die Appliance unterstützt zudem SNMP.

Bei der Benutzerverwaltung ist erwähnenswert, dass die Möglichkeit besteht, Userkonten automatisch zu erstellen. Den Benutzern stehen dann im Betrieb verschiedene Funktionen zu, wie ein HTTP-Proxy, das bereits erwähnte Benutzerportal, ein SMTP-Proxy oder auch das SSL-VPN. Die Lösung arbeitet zudem mit dem Active Directory, dem E-Directory, LDAP, Radius und Tacacs+ zusammen.

Ähnlich wie die meisten anderen UTM-Lösungen setzt die Astaro-Appliance Netzwerkobjekte ein, die interne und externe Adressen und Dienste wie RDP oder auch Instant Messaging definieren. Die Dienste lassen sich nach Quelle, Ziel und Protokoll anlegen, dabei kennt das System TCP, UDP, ICMP, IP, ESP und AH. Es ist auch möglich, die Services in Gruppen zusammenzufassen. So genannte Zeitereignisse sorgen dafür, dass einzelne Regeln nur zu bestimmten Zeiträumen aktiv sind.

Das Netzwerkmenü bietet eine Übersicht über die am häufigsten aufgetretenen

Dienste, die Top Talker und die Concurrent Connections. Hier lassen sich auch die Schnittstellen konfigurieren, das Bridging einrichten und statische sowie dynamische Routen definieren. An gleicher Stelle finden sich zudem die QoS-Konfiguration, das Multicast-Routing und das Uplink-Monitoring, beispielsweise für IPSec-Tunnel.

Über den Eintrag "Netzwerkdienste" nehmen die Administratoren die DNS-, DHCP- und NTP-Konfiguration vor, während das Menü "Network Security" das Herzstück der Appliance darstellt. Hier erfolgen die Konfiguration des Paketfilters mit den Firewall-Regeln, die NAT-Konfiguration mit DNAT und SNAT sowie die Administration des IPS mit der Erkennung der Angriffe auf Betriebssysteme, Server, Clients, Protokollanomalien, Malware, Instant Messaging und Multimedia-Daten. Anti-DoS- und Anti-Flooding- sowie Anti-Portscan-Funktionen schließen die Konfiguration der Netzwerkdienste ab. An dieser Stelle ist es noch erwähnenswert, dass die Astaro-Lösung in jedem Hauptmenü, in dem dieses Vorgehen Sinn ergibt, eine Übersicht mit den gerade aktuellen Informationen liefert. In dem Bereich Netzwerksicherheit finden sich darin unter anderem die Quellrechner der am meisten verworfenen Datenübertragungen, die häufigsten Angreifer und so weiter in einer grafischen Übersicht.

Unter "Web Security" stehen in der eben erwähnten Übersicht die häufigsten Domänen nach Verkehr, die häufigsten Benutzer nach Verweildauer und ähnliches. Zusätzlich veranlassen die zuständigen Mitarbeiter an dieser Stelle, dass die Appliance Datenübertragungen aus dem Internet nach Viren durchsucht (bei Bedarf ist es auch möglich, HTTPS-Verkehr zu scannen), bestimmte Dateitypen ausfiltert, URL-Filter einsetzt (mit den bereits angesprochenen Kategorien) und den FTP- sowie Mail-Verkehr (mit Antispam-Funktion) im Auge behält. Für die Filter lassen sich jederzeit Ausnahmen definie-

ren und das System bietet umfassende Funktionen zum Verschlüsseln von E-Mails. Es ist auch möglich, den Benutzern automatisch Quarantäneberichte zuzustellen, die sie darüber informieren, welche ihrer Mails in der Quarantäne gelandet sind.

Abgesehen von den bereits genannten Funktionen sichert die Appliance auch VoIP-Verkehr ab, untersucht Instant-Messaging- und Peer-to-Peer-Datenübertragungen (Edonkey, Gnutella, Mute, etc.) und bietet Support für IPSec- und SSL-VPNs. Eine Zertifikatsverwaltung gehört ebenfalls zum Leistungsumfang des Produkts.

Zusätzlich von Interesse sind die Protokoll- und Berichtsfunktionen: Die Lösung protokolliert nicht nur lokal, sondern kann ihre Informationen auch an einen externen Syslog-Host weiterschicken und über SSH, FTP, CIFS oder Mail-Übertragungen so genannte ausgelagerte Protokollarchive pflegen. Es ist ebenfalls kein Problem, die Protokolle über das Konfigurationstool einzusehen. Berichte stehen für das Accounting, die Authentifizierung, die E-Mail-Sicherheit, das IPS, den Paketfilter, die Web-Sicherheit, die Hardware, die Netzwerknutzung und ähnliches zur Verfügung. Insgesamt hat Astaro 22 Reports vordefiniert. Supportwerkzeuge wie Ping und Traceroute, eine Prozessliste und so weiter schließen den Leistungsumfang der Lösung ab.

Lasttest

Da die Astaro-Appliance für deutlich größere Netze als das System von Netgear ausgelegt wurde, erhielten wir bei unseren Lasttests auch viel höhere Durchsatzwerte. Konkret ergaben sich bei unseren Tests mit aktivierten Sicherheitsfunktionen folgende Ergebnisse: Der TCP-Durchsatz lag durchschnittlich bei 96,957 MBit pro Sekunde. HTTP-GIF-Übertragungen erreichten einen maximalen Durchsatz von 24,253 MBit/s, bei FTP lag der Wert bei 66,767 beim Hoch- und 72,836 beim He-

runterladen. DNS-Lookups arbeitete die Appliance mit 3,700 MBit/s ab, bei NNTP lag der entsprechende Wert bei 12,269. Diese Ergebnisse sind mit den nun folgenden vergleichbar, da sich alle weiteren Appliances an Einsatzgebiete mit ähnlichen Anforderungen wenden. An allgemeinen Durchsatzwerten gibt der Hersteller an, dass die Appliance 1,8 GBit/s beim Firewall-Durchsatz, 260 MBit/s bei VPNs und im UTM-Betrieb 65 MBit/s erreicht. Auch hier hielt das Produkt die Angaben des Herstellers in Bezug auf den Datendurchsatz im Wesentlichen ein.

Zusammenfassung

Im Test konnte das Produkt von Astaro voll überzeugen. Die Lösung war schnell und einfach in Betrieb genommen und das manuelle Anpassen der Konfiguration an die lokalen Bedürfnisse unseres LANs ging ebenfalls flott und problemlos von der Hand. Das liegt nicht zuletzt an dem klar gegliederten Konfigurationsinterface, mit dem die meisten Administratoren sofort arbeiten können, ohne erst auf das Handbuch zurückzugreifen – und das trotz des großen Funktionsumfangs. Bei den Sicherheitstests ergaben sich keine Schwierigkeiten und bei den Lasttests konnte das System sämtliche in es gesetzten Erwartungen voll erfüllen. Was die Usability angeht, so benötigt ein Administrator drei Arbeitsschritte um eine Firewallregel zu ändern und zum Aktivieren eines URL-Filters fallen ebenfalls drei Arbeitsschritte an.

Sonicwall Network Security Appliance 3500

Das Produkt von Sonicwall umfasst sechs GBit-Ethernet- sowie zwei USB-Ports und einen seriellen Anschluss. Es eignet sich für Umgebungen mit 300 bis 500 Arbeitsplätzen und unterstützt bis zu 800 VPN-Tunnel. Auch hier läuft die Inbetriebnahme des Systems über einen Setup-Wizard ab. Nach dem Aufruf der URL <http://192.168.168.168> präsentiert



die Appliance zunächst einen Willkommensbildschirm, fragt dann nach dem zukünftig zu verwendenden Administrator-Passwort sowie der Zeitzone und möchte im nächsten Schritt wissen, wie der in das Geräte integrierte USB-Slot zu nutzen ist. Hierbei stehen die Modi "Modem", "3G" und "None" zur Verfügung, der USB-Slot dient also dazu, eine Backup-Internet-Verbindung über ein alternatives Medium herzustellen, wenn der primäre Internet-Anschluss versagt. Bei der WAN-Konfiguration unterstützt das Produkt eine statische IP-Adresse sowie DHCP, PPPoE und PPTP. Zum Abschluss der Initialkonfiguration möchte der Wizard noch die neue LAN-IP-Adresse und -Netzmaske wissen, damit schließt die Setup-Routine und das System ist fast betriebsbereit. Insgesamt nahm bei uns das initiale Setup 15 Arbeitsschritte und 20 Minuten in Anspruch.

Sobald das eben genannte Setup abgeschlossen wurde, ist es vor der endgültigen Inbetriebnahme der Appliance noch erforderlich, das Produkt online auf der Site www.mysonicwall.com zu registrieren und die Lizenzen mit dem eben genannten Portal zu synchronisieren. Dieser Vorgang dauerte bei uns nochmal sechs Minuten, danach konnten wir mit der Appliance arbeiten.

Sicherheitstest

Nachdem wir alle für unseren Test gewünschten Funktionen der Sonicwall-Appliance aktiviert hatten, führten wir zunächst unseren Sicherheitstest durch. Dabei stellten wir fest, dass das Produkt intern die Ports 80 und 443 offen hat – diese dienen der Konfiguration über das Web-Interface – und dass extern alle Ports geschlossen waren. Immerhin schlug nmap bei der Betriebssystemerkennung

SonicOS vor, was allerdings keine Sicherheitslücke darstellt. Nessus fand keine Schwachstellen und während

DoS-Angriffen arbeitete das Produkt weiter. Lediglich bei Angriffen auf den LAN-Port von innen ließ sich der Datenverkehr über das Sonicwall-Gerät mit einem Tool, das sehr viele Datenpakete erzeugte, deutlich verlangsamen. In der Vergangenheit hatten wir bei einem Test eines vergleichbaren Sonicwall-Produkts ein ähnliches Problem (siehe http://iait.eu/oneclick_uploads/2009/03/iait_test_sonicwall_tz_190.pdf), damals erklärte der Hersteller, dass es sich um keine Sicherheitslücke handle, da das LAN-Interface eine kontrollierte Umgebung darstelle (Seite sieben des Dokuments). Wir teilen diese Meinung nicht ganz, weil das interne Netz heute keineswegs mehr als sichere Zone gelten kann und da andere Lösungen dieses Problem nicht haben, aber unter dem Strich stimmt es schon, dass Angriffe wohl nur selten auf diesem Weg kommen.

Funktionsumfang

Nach dem Login im laufenden Betrieb findet sich der Administrator in einem sehr übersichtlichen Konfigurationsinterface wieder, das neben der Menüstruktur auf der linken Seite am oberen Bildschirmrand Konfigurationswizards für das Setup (diesen Wizard haben wir im vorherigen Schritt bereits abgearbeitet), das Verfügbarmachen eines öffentlichen Serverdienstes via Portforwarding, die VPN-Konfiguration und das Einrichten der Application Firewall bereitstellt. Im Test ergaben sich bei der Arbeit mit den Assistenten keine Probleme.

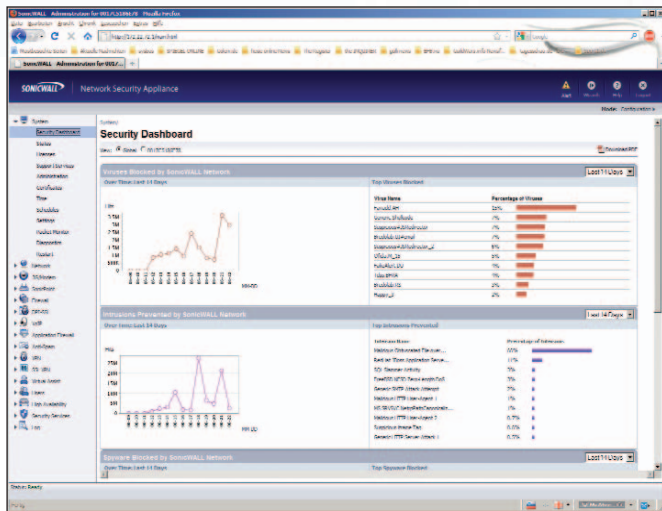
Direkt nach dem Einloggen zeigt das Managementtool eine Statusseite an, die Informationen wie Speicherauslastung, CPU-Last, Firmwareversion (im Test kam die Firmware 5.6.0.3-40o zum Einsatz), Lizenzen, die letzten Alarmmel-

dungen und ähnliches bereit hält. Diese Ansicht bietet einen schnellen Überblick über das System.

Interessanter ist das Dashboard, über das sich die zuständigen Mitarbeiter über den Security-Status im Allgemeinen informieren können. Dieses liefert unter anderem Übersichten über die von Sonicwall weltweit geblockten Viren, die verhinderten Intrusions, die geblockte Spyware und die unterbundenen Peer-to-Peer- und Web-TV-Übertragungen. Alle angebotenen Statistiken lassen sich nicht nur für die Sonicwall-Aktionen weltweit anzeigen, sondern auch für das lokale Gerät. Damit erhalten die zuständigen Mitarbeiter einen schnellen Überblick darüber, welche Bedrohungen lokal und im Internet gerade am meisten verbreitet sind. Zusätzlich besteht auch die Möglichkeit, die grafische Übersicht als PDF-Datei herunterzuladen.

Der nächste Punkt der Systemkonfiguration befasst sich mit den Lizenzen. Hier steht eine Übersicht mit der jeweiligen Gültigkeitsdauer zur Verfügung. Abgesehen davon können die Administratoren an gleicher Stelle auch Lizenzkeys eingeben, wenn keine Lizenzsynchronisation mit dem Online-Portal durchgeführt werden soll. Weitere Optionen befassen sich mit der Zertifikatsverwaltung, den Supportverträgen (mit Ablaufdatum) und der Administration (mit Hostname, mehreren Administratorkonten, Porteinstellungen, SNMP sowie der Passwortkonfiguration mit Lebensdauer und Komplexität). Die Konfiguration von NTP beziehungsweise Zeitzone und die Definition von Zeiträumen für die Gültigkeit von Regeln schließen die Systemkonfiguration ab.

Die Netzwerkkonfiguration befasst sich mit den Interfaces, den Failover-Settings und dem Einrichten von Zonen. Die Zonen stellen das Herzstück der Konfiguration dar. Vordefiniert wurden Zonen für LAN, WAN, DMZ, VPN, SSL VPN, Multicast und WLAN. Es



Das Security-Dashboard von Sonicwall liefert Daten von vielen Sonicwall-Produkten im Internet

lassen sich jederzeit eigene Zonen definieren. Allen Zonen wird ein "Security Type" zugewiesen (Trusted, Untrusted, Public, Encrypted oder Wireless). Außerdem arbeiten die Sicherheitsdienste Content Filter, IPS, Antivirus, Anti-Spyware und ähnliches auf Zonenbasis. Sie werden also nicht global in den jeweiligen Konfigurationsmenüs aktiviert, sondern innerhalb der betroffenen Zonen der Netzwerkkonfiguration. Wenn man sich erst einmal an diesen Ansatz gewöhnt hat, erscheint er als sehr sinnvoll und übersichtlich.

Die DNS-Konfiguration gehört genauso zur Netzwerkverwaltung wie das Einrichten von Adressobjekten wie Subnetzen, IP-Adressen sowie User-Black- und User-White-Lists. Die genannten Objekte finden dann bei der Regeldefinition Verwendung. Das gleiche gilt für die Services. Hier hat der Hersteller die wichtigsten vordefiniert, es lassen sich aber auch eigene definieren und zwar nach Name, Protokoll (ICMP, IGMP, TCP, UDP, GRE, ESP, AH, EIGRP, OSPF, PIMSM und L2TP), Port Range, etc. Die zuständigen Mitarbeiter können die Services zudem in Gruppen zusammenfassen, um die Übersichtlichkeit zu erhöhen.

Die nächsten Punkte des Netzwerkmens befassen sich mit der Konfiguration des

Routings, der NAT-Policies, des DHCP-Servers, des Web-Proxies und der DynDNS-Konten. Ein Dialog zum Einrichten statischer ARP-Einträge beziehungsweise zum Aktivieren einer MAC-IP-Anti-Spoof-Funktion, ein Netzwerkmonitor und ähnliches schließen die Netzwerkkonfiguration ab.

Weitere Konfigurationsmenüs übernehmen

das Einrichten alternativer Netzwerkverbindungen über die USB-Schnittstelle mittels Modem oder 3G-Device und die Sonicpoint-Konfiguration, die das Anbinden der gleichnamigen WLAN-Access-Points von Sonicwall durchführt. Für unseren Test interessanter ist da der Menüpunkt Firewall mit den Zugriffregeln, die sich als Liste, Matrix oder Drop-Down-Box konfigurieren lassen. Die Regeln arbeiten mit Quelle, Ziel, Dienst, erlaubten Benutzern, Schedule, QoS-Settings etc. Dazu kommen noch diverse andere Firewall-Funktionen wie "Drop Source Routed IP Packets", "Syn Flood Protection" oder auch "Enable Header Checksum Enforcement". Ein MAC-Blacklisting und ein Verbindungsmonitor stehen ebenfalls zur Verfügung.

Weitere Punkte, die von Interesse sind, umfassen die VoIP-Konfiguration, das Einrichten des Anti-Spam-Features (mit Funktionen wie "Tag", "Reject", "Delete", "in Junk Box" und ähnlichem), des RBL-Filters (der nur zum Einsatz kommt, wenn die Anti-Spam-Funktion inaktiv ist) und der VPN-Verbindungen. Die Lösung unterstützt, wie die anderen Produkte im Test auch, IPSec- und SSL-VPNs mit den dafür notwendigen Optionen wie IKE Dead Peer Detection, Aggressive Mode, NAT-Traversal, DHCP over VPN, etc.

Was die Benutzerverwaltung angeht, so arbeitet die Appliance neben einer lokalen Datenbank noch mit LDAP und Radius zusammen. Außerdem stellt sie bei Bedarf Guest Accounts zur Verfügung.

Von besonderem Interesse ist abschließend das Konfigurationsmenü für die Sicherheitsdienste. Hier verwalten die zuständigen Mitarbeiter den Content Filter, das IPS, Anti-Virus- und Anti-Spyware-Funktionen sowie den RBL-Filter. Der entsprechende Menüpunkt umfasst zunächst eine tabellarische Übersicht mit Lizenzinformationen, dem Betriebsmodus (Maximum Security oder Performance Optimized) und ähnlichem. Unter "Content Filter" wählen die Administratoren aus, ob sie die Filtertechnologie von Sonicwall oder von Websense nutzen möchten, außerdem lassen sich die zu verwendenden Kategorien festlegen ("Violence/Hate/Racism", "Nudism", "Weapons" etc., insgesamt gibt es 64 Kategorien). Bei Bedarf erzeugen die zuständigen Mitarbeiter auch benutzerdefinierte Listen, sorgen dafür, dass das System Komponenten wie Java, Active-X und ähnliches ausfiltert und definieren Trusted Domains. Im Test fiel uns auf, dass der Content Filter von Sonicwall manchmal Seiten der Boulevardpresse sperrt, und zwar mit der Begründung "Intimate Apparel/Schwimmsuite". Diese Sperrung findet nicht immer statt, sondern meist nur dann, wenn die Seiten auch gerade entsprechende Bilder enthalten. Auf Nachfrage teilte uns Sonicwall hierzu mit, dass die Content-Filter von einem Team in Russland gepflegt und immer wieder aktualisiert werden. Falsche Kategorisierungen lassen sich dem Hersteller darüber hinaus über einen Link auf der Sperrseite melden. Im Test klassifizierte das Tool die Website unseres Allergologen als "Pornography" und sperrte sie dementsprechend, als wir das gemeldet hatten, dauerte es keine 24 Stunden, bis der Zugriff frei war. Der Content Filter hinterließ folglich einen sehr guten Eindruck: Fehlklassifizierungen kommen immer wieder vor, aber nur selten können die Benutzer zeitnah etwas dagegen unternehmen.

Beim Antivirus bietet Sonicwall nicht nur eine Gateway-Antivirus-Lösung (ein eigenes Sonicwall-Produkt, dass dazu in der Lage ist, den Datenstream direkt zu scannen) sondern auch ein Client-Antivirus-Enforcement. Bei letzterem erhalten nur Clients Zugriff auf das Internet, die über eine aktive Antivirus-Software (von McAfee) verfügen. Das Lizenzmanagement läuft in diesem Fall über die Appliance.

Beim Gateway-Antivirus wählen die zuständigen Mitarbeiter die zu überwachenden Protokolle (HTTP, FTP, IMAP, SMTP, POP3, CIFS/NetBIOS und TCP Stream) und nehmen Einstellungen dazu vor, die zum Beispiel festlegen, ob das System auch ZIP-Dateien durchsucht. Das Standardintervall für Patternupdates liegt bei einer Stunde.

Für das IPS lassen sich wieder bestimmte Signaturgruppen auswählen oder deaktivieren, es ist auch möglich, eine IPS-Exclusion-List anzulegen. Die Anti-Spyware-Funktion stuft die verseuchten Mails nach ihrer Gefährlichkeit ein und bei den RBL-Filtern haben die IT-Verantwortlichen jederzeit die Option, eigene Listen einzufügen.

Abschließend noch kurz zum Logging und den Reports: Die Sonicwall-Lösung arbeitet bei den Logs mit Kategorien, wie "Firewall Event" oder "High Availability". Diesen weisen die Administratoren dann im Betrieb Alerts und Log-Ziele wie das normale Log oder das Syslog zu. Das System verwendet bei Bedarf auch externe Syslog-Server. Die Logs und Alerts lassen sich zudem jederzeit automatisch per Mail verschicken. Abgesehen davon stellt die Sicherheitslösung noch drei Reports zur Verfügung, und zwar zu Web Site Hits sowie zur Bandbreitennutzung nach IP-Adressen beziehungsweise nach Diensten.

Lasttest

Die Ergebnisse unseres Performance-Tests sahen folgendermaßen aus: Der TCP-

Durchsatz lag durchschnittlich bei 66,446 MBit/s. HTTP-GIF-Übertragungen erreichten einen maximalen Durchsatz von 24,235 MBit/s, bei FTP lag der Wert bei 50,075 beim Hoch- und 66,767 beim Herunterladen. DNS-Lookups arbeitete die Appliance mit 3,895 MBit/s ab und bei NNTP lag der entsprechende Wert bei 15,961 MBit/s. Die allgemeinen Leistungsangaben des Herstellers, die die Lösung generell einhielt, lauten folgendermaßen: Der Firewalldurchsatz liegt bei 1,5 GBit/s, der UTM-Durchsatz bei 240 MBit/s, der Antivirusdurchsatz bei 350 MBit/s, der IPS-Durchsatz bei 750 MBit/s und der VPN-Durchsatz bei 625 MBit/s.

Fazit

Die Appliance von Sonicwall lässt sich problemlos konfigurieren und administrieren. Auch das Setup wurde einfach und gerade heraus gestaltet. Die leichte Anfälligkeit gegen DoS-Angriffe auf den LAN-Port sollte niemand zu hoch bewerten. Abgesehen davon müssen wir das sehr übersichtliche, gut aufgeräumte und intuitiv gestaltete Web-Interface des Produkts hervorheben, dass die Arbeit mit der Lösung sehr einfach macht. Zum Schluss kurz zur Usability: Das Ändern einer Firewall-Regel nimmt drei Schritte in Anspruch, das Aktivieren eines URL-Filters fünf.

Gateprotect GPA 400

Die Appliance von Gateprotect arbeitet mit sechs Ethernet-Ports zum Anschluss diverser Netzwerke. Das Produkt verwendet – anders als die anderen hier vorgestellten Systeme – kein Webinterface, sondern eine Windows-basierte Konfigurationssoftware. Der Grund dafür liegt in der Konfiguration der Firewallregeln, 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

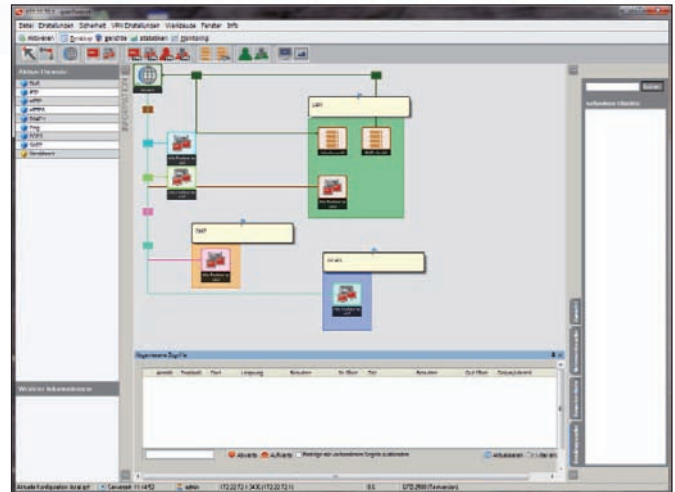
Beim Sicherheitstest ergaben sich keine Überraschungen. Die Appliance arbeitete wie erwartet und ließ sich nicht aus dem Tritt bringen. Nessus und nmap fanden lediglich heraus, dass auf dem internen Interface die Ports für SSH und DNS offen waren, das war aber auch so gewollt.

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 zugänglich. 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 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



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

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 gefundene 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 genannte Vertrauensliste dient zur Definition vertrauenswürdiger Hosts, deren HTTP- oder FTP-Verkehr nicht untersucht wird.

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 Analysewerkzeuge wie Ping in die Hand.

Lasttest

Die Ergebnisse des Performance-Tests sahen diesmal folgendermaßen aus: Der TCP-Durchsatz lag durchschnittlich 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. Im allgemeinen Teil gab der Hersteller an, dass die Appliance einen Firewalldurchsatz von 1,4 GBit/s schaffen würde, während der VPN-Durchsatz bei 190 MBit/s liegt. Auch hier hielt das Produkt die Angaben des Herstellers in Bezug auf den Datendurchsatz ein.

Fazit

Bei der Gateprotect-Lösung fällt 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 – in diesem Zusammenhang sei nochmals das gelungene Reporting hervorgehoben. Auch bei den Si-

cherheitstests gab sich die Appliance keine Blöße. Deswegen ist sie rundum empfehlenswert. Zur Usability: Die zuständigen IT-Mitarbeiter brauchen jeweils fünf Arbeitsschritte zum Ändern einer Firewall-Regel und zum Aktivieren eines Content-Filters.

Zusammenfassung

Was die Leistung, die Sicherheit und die UTM-Grundfunktionen angeht, existieren zwischen den hier getesteten Produkten keine nennenswerten Unterschiede. Dafür hat jedes Produkt seine spezifischen Besonderheiten. Gateprotect glänzt beispielsweise mit einer gut durchdachten grafischen Firewall-Konfiguration, zwingt die IT-Mitarbeiter aber auf der anderen Seite, die Konfiguration über eine Windows-Software durchzuführen und nicht über einen Browser. Astaro bringt wohl den größten Leistungsumfang im Test mit während Sonicwall positiv mit der Gateway-Antivirus-Funktion, die den Datenstream direkt untersuchen kann, und dem Client-Antivirus-Feature hervorsticht. Netgear bietet schließlich eine übersichtliche und schnell konfigurierbare Lösung, die wohl die meisten üblichen Anforderungen an die IT-Sicherheit abdeckt. Hier müssen die Interessenten allerdings noch ein paar Wochen warten, bis es die Lösung in einer etwas größeren Version für Netze mit um die 300 Arbeitsplätzen gibt. Es gilt also, im Vorfeld genau zu klären, welche Funktionen in welchen Unternehmensbereichen besonders wichtig sind, und dann seine Auswahl entsprechend zu treffen.

Impressum

Herausgeber:
Institut zur Analyse
von IT-Komponenten (IAIT)
Dr. Götz Güttich
Tel.: 02182/5783974
Fax: 02182/5783975
Web: www.guettich.de
Blog: www.iait.eu