

Übersichtliche Konfiguration bei großer Leistung

Dr. Götz Güttich

Gateprotect liefert mit der xUTM-Appliance V8 ein Produkt zum Absichern mittelgroßer Unternehmensnetze. Der Hersteller hat ein besonderes Augenmerk auf die einfache Konfiguration und Administration der Lösung gelegt, so dass Administratoren ohne Schwierigkeiten dazu in der Lage sein sollten, mit dem Produkt zu arbeiten. IAIT hat sich in der Praxis angesehen, ob die Appliance diese Anforderung erfüllt.

Die Gateprotect-Appliance ist in verschiedenen virtuellen Varianten und Hardware-Versionen von Lösungen mit einer 500-MHz-CPU bis hin zu Geräten mit Dual-Xeon-Prozessoren erhältlich. Nach eigener Aussage wendet sich der Hersteller mit seinem Angebot vor allem an mittelgroße Unternehmen mit bis zu 500 Benutzern. Unsere Teststellung (die Appliance GPA-400) arbeitete mit einem Zwei-Prozessor-System und verfügte darüber hinaus über insgesamt sechs Netzwerkin-



DMZ (Demilitarisierten Zone) oder auch zum Realisieren eines separaten WLAN-Segments nutzen lassen. Administratoren nehmen die Lösung in der Regel dadurch in Betrieb, dass sie das Produkt an seiner endgültigen Arbeitsstelle im Netz platzieren (im Test setzten wir die Lösung als Internet-Router ein, also zwischen der WAN-Verbindung und unserem LAN-Switch), den Konfigurations-Client auf einer Windows-Arbeitsstation installieren und dann die Appliance mit seiner Hilfe so einrichten, dass sie die ihr zugeordneten Aufgaben übernimmt.

Client-Installation

Der Client läuft unter den aktuellen Windows-Versionen und benötigt hardwareseitig eine CPU mit einem GHz Taktfrequenz und 512 MByte RAM, lässt sich also ohne weiteres in virtuellen Maschinen betreiben. Das Setup der Lösung erfolgt – wie unter Windows üblich – über einen Wi-

zard, der den Anwendern die Sprachen Deutsch, Englisch, Französisch sowie Italienisch anbietet und im Übrigen niemanden vor irgendwelche Schwierigkeiten stellen wird.

Nach dem Durchlauf der Setup-Routine lässt sich die Software gleich aufrufen und sucht selbstständig im Netz nach der Firewall. Sollte sie sie nicht finden, haben die Administratoren im nächsten Schritt Gelegenheit, die IP-Adresse der Appliance anzugeben (die der Hersteller in Form eines Ausdrucks mitliefert) und die Verbindung auf diesem Wege aufzubauen.

Wenn die Konfigurationssoftware die Lösung zum ersten Mal kontaktiert hat, startet automatisch ein Assistent, der die Initialkonfiguration durchführen möchte. Dazu bietet er den zuständigen Mitarbeitern die beiden Optionen "Schnellstart" und "Standard". Da der Hersteller eine

IAITested

★★★★★

Excellent ! Test 11 / 2008

Fazit:
Die UTM Appliance von gateProtect konnte auf ganzer Linie überzeugen und erzielte in sämtlichen Funktionsbereichen gute Werte.

Vorteile

- + Hervorragende Übersicht
- + Einfachste Bedienung
- + VPN-Wizard und Client
- + Qualität der Hardware
- + Preis / Leistung

Nachteil

- noch keine Web-Oberfläche

gateProtect GPA 400
xUTM solution

terfaces, die sich beispielsweise für Verbindungen mit LAN und WAN, zum Einrichten einer

Konfiguration mit dem Schnellstart-Wizard empfiehlt, haben wir uns im Test dazu entschlossen, diese auch durchzuführen. Im ersten Schritt fragt der Assistent nach den freizugebenden Diensten und bietet in diesem Zusammenhang verschiedene Optionen an. Dazu gehören die Webdienste HTTP, HTTPS und DNS, FTP für Dateiübertragungen sowie die Mail-Services POP3, SMTP und IMAP4.

Darüber hinaus haben die Administratoren auch noch die Möglichkeit, über den Assistenten die Services NetBIOS, Kerberos, LDAP, DNS und RDP freizuschalten. Nach dieser Auswahl kommt die Konfiguration des Internet-Zugangs an die Reihe. Hier offeriert die UTM-Lösung ISDN-, PPPoE-, PPTPoE- und Router-Verbindungen.

Im Test setzten wir das Produkt an einem DSL-Anschluss (im PPPoE-Modus) als Internet-Router ein und mussten dazu die zu verwendende Netzwerkverbindung und unsere Zugangsdaten eintragen. Nach einigen weiteren Fragen zur Netzwerkanbindung und den Systemeinstellungen (Timeout, Administrationspasswort, Zeitzone und ähnliches) ist die Initialkonfiguration abgeschlossen und die Appliance nimmt ihren Betrieb als Sicherheitslösung auf. Entscheiden sich die IT-Mitarbeiter anstelle der Schnellstart-Option für die Standardkonfiguration, so müssen sie sämtliche Administrationsaufgaben übrigens von Anfang an mit dem Konfigurationswerkzeug durchführen.

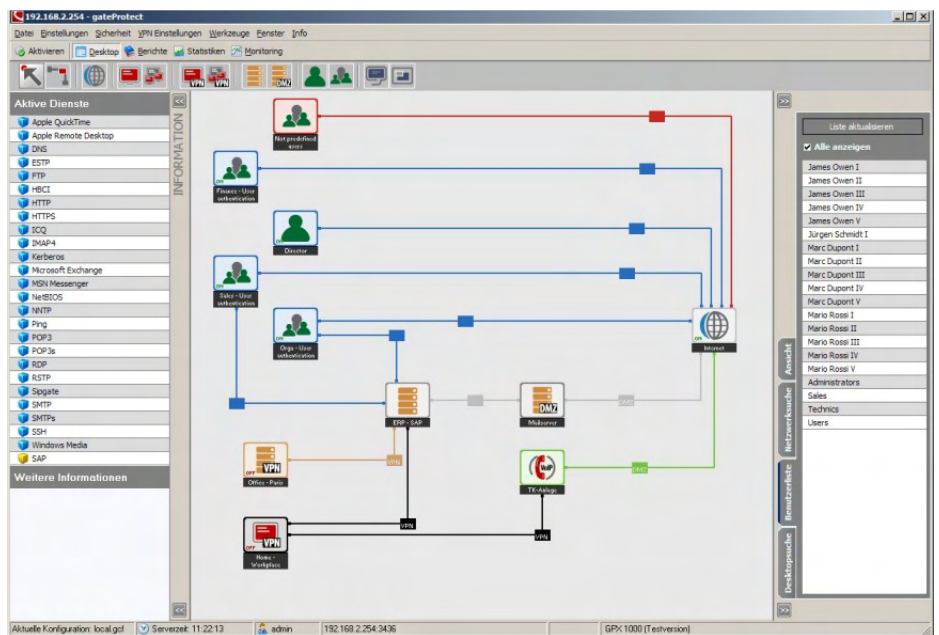
Administration

Die Konfiguration, die der Schnellstart-Wizard hinterlässt, bleibt ziemlich allgemein und erlaubt für alle Systeme im LAN

(beziehungsweise an den Nicht-WAN-Schnittstellen) das ausgehende Nutzen der vom IT-Mitarbeiter im ersten Konfigurationsschritt freigegebenen Dienste. Im nächsten Schritt ist es nun sinnvoll, diese Konfiguration mit Hilfe des Administrationswerkzeugs genau an die Anforderungen des jeweiligen Unternehmens anzupassen.

Wie bereits in der Einleitung erwähnt, stellt das Gateprotect-Administrationstool eine Besonder-

heit dar. Die Lösung arbeitet nicht – wie die Produkte der meisten anderen Hersteller – mit Listen, in denen die zu erlaubenden und zu blockierenden Dienste mit ihren Quell- und Zieladressen aufgeführt sind, sondern präsentiert ihr Regelwerk grafisch. Konkret sieht das so aus, dass die einzelnen Rechner, Benutzer, Rechnergruppen und Benutzergruppen in Form von Icons auf der Arbeitsfläche des Konfigurationswerkzeugs erscheinen und die IT-Verantwortlichen dann zwischen diesen Icons und beispielsweise der ebenfalls grafisch dargestellten Internet-Verbin-



Das Administrationswerkzeug von Gateprotect mit dem übersichtlichen Konfigurationsdesktop

dung Linien ziehen und diesen Linien dann die Rechte auf das Nutzen bestimmter Services zuweisen. Auf diese Weise lassen sich unter anderem Regeln erstellen wie "Benutzer A darf im Internet surfen und per FTP Dateien übertragen" oder "Zugriffe via SSL sind nur vom Rechner B aus möglich". Ein Klick auf die jeweilige Linie öffnet dann im Betrieb ein Fenster, über das die Administratoren die Zugriffsrechte jederzeit modifizieren können.

Wie bereits angesprochen, enthielt das Administrationstool nach der Erstkonfiguration lediglich ein Icon, das die Internet-Verbindung symbolisierte, fünf Icons die als Rechnergruppen die an die fünf internen Schnittstellen angeschlossenen LAN-Systeme repräsentierten und fünf Verbindungslinien zwischen den Rechnergruppen und dem Internet, in denen die zuvor definierten Dienste freigegeben wurden.

Wir wollten die Regeln nun genauer festlegen und Systeme definieren, die im Internet surfen durften, Rechner einrichten, die lediglich per SSH auf externe

Server zugreifen konnten und Einträge anlegen, die sich ausschließlich Firmware-Updates aus dem Internet holen konnten. Dazu mussten wir der Firewall zunächst die Rechner und Benutzer im Netz bekannt machen.

Dafür gibt es zwei Wege: Zum einen die manuelle Vorgehensweise, hier zogen wir ein Rechner- oder Benutzer- beziehungsweise Gruppenicon aus der Icon-Leiste auf den Arbeitsbereich und ga-

ten mit allen Informationen (also IP-Adresse, Benutzername etc.) per Drag-and-Drop in den Arbeitsbereich zu ziehen und dort mit Verbindungsrechten zu versehen.

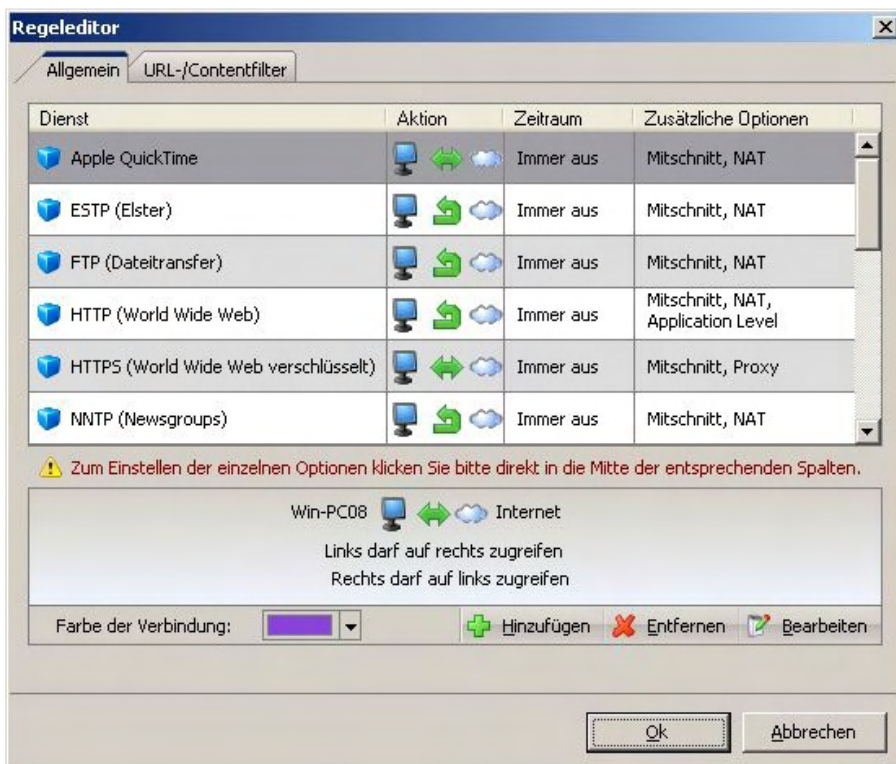
Im Test ergaben sich beim Import der Active-Directory-Daten keine Probleme und die Suchfunktion fand alle im Netz aktiven Bestandteile. Die genannte Funktion spart den Administratoren folglich – vor allem in größeren Netzwerken – viel Zeit und

geben beziehungsweise zu blockieren. Alle wichtigen Services, wie HTTP, HTTPS, FTP, SMTP, POP oder auch Elster hat der Hersteller bereits vordefiniert, es ist aber auch möglich, eigene Einträge anzulegen.

Letzteres funktioniert über das zu verwendende Protokoll (AH, ESP, GRE, ICMP, TCP, UDP) und – falls erforderlich – den Port. Im Test hinterließ das Konfigurationswerkzeug einen hervorragenden Eindruck, wir hatten die Systeme unseres Netzwerks schnell erfasst und konnten innerhalb kürzester Zeit auf ein komplexes, aber voll funktionsfähiges Regelwerk zugreifen. Die Rechner- und Benutzergruppen helfen in der Praxis sehr dabei, den Überblick zu behalten. Mit ihrer Unterstützung sind auch Administratoren größerer Netze relativ einfach dazu in der Lage, für klare Verhältnisse zu sorgen.

Sie müssen dazu nicht für jeden Rechner ein eigenes Icon anlegen, sondern können ganze Netze, Rechnergruppen oder an bestimmte Interfaces angeschlossene Systeme zusammenfassen und so zum Beispiel jeweils einheitliche Regeln für unterschiedliche Abteilungen wie etwa die Buchhaltung oder die Entwicklung festlegen. Um die Übersicht noch weiter zu verbessern, bietet das System auch noch die Option an, bestimmte Bereiche – die etwa die Icons der Server der Datenbank umfassen – farblich zu hinterlegen und so hervorzuheben oder auch Notizen auf dem Administrationsdesktop anzubringen.

Machen die zuständigen Mitarbeiter während der Konfiguration einen Fehler und definieren



Die Konfiguration der Verbindungen umfasst die freigegebenen und geblockten Dienste, den Zeitraum, die Content-Filter-Konfiguration und ähnliches

ben dann die Details wie IP-Adresse, Benutzername oder Netzwerkadresse an. Zum anderen stellt die Appliance auch Funktionen zum Suchen von Rechnern im Netz und zum Importieren der Benutzerdaten eines Active-Directory-Servers zur Verfügung und präsentiert die darüber gefundenen Systeme und Konten in einer Liste bekannter Objekte auf der rechten Seite des Arbeitsfensters. Von dort waren wir nach dem Such- beziehungsweise Importvorgang dazu in der Lage, die jeweiligen Komponenten

manuell einzugeben. Das macht zudem eine fehleranfällige manuelle Dateneingabe fast überall überflüssig.

Nachdem die einzelnen Objekte erst mal im Arbeitsbereich zur Verfügung standen, gingen wir daran, die jeweiligen Verbindungsregeln festzulegen. Dazu selektierten wir in der Icon-Leiste des Konfigurationswerkzeugs die Quelle und Ziel an und hatten dann die Option, für die Verbindung bestimmte Dienste, Dienstgruppen und Richtungen freizu-

zum Beispiel widersprüchliche Regeln, so weist das Konfigurationswerkzeug sie unverzüglich auf diese Sachlage hin und verhindert so Schlimmeres – eine sehr nützliche Funktion.

Darüber hinaus bietet das Administrationswerkzeug auch noch eine ganze Reihe weiterer nützlicher Features. So umfasst das Werkzeug auf der linken Fensterseite eine Liste mit allen Diensten, die in der Konfiguration freigegeben wurden. Selektiert der Anwender eine Verbindung oder eines der Icons, so hebt das System die darauf aktiven Services in der Liste farblich hervor. Es ist sogar möglich, andersherum vorzugehen und auf einen Dienst in der Liste zu klicken. Daraufhin präsentiert das Konfigurationswerkzeug alle Verbindungen, auf denen der jeweilige Service zugelassen wurde.

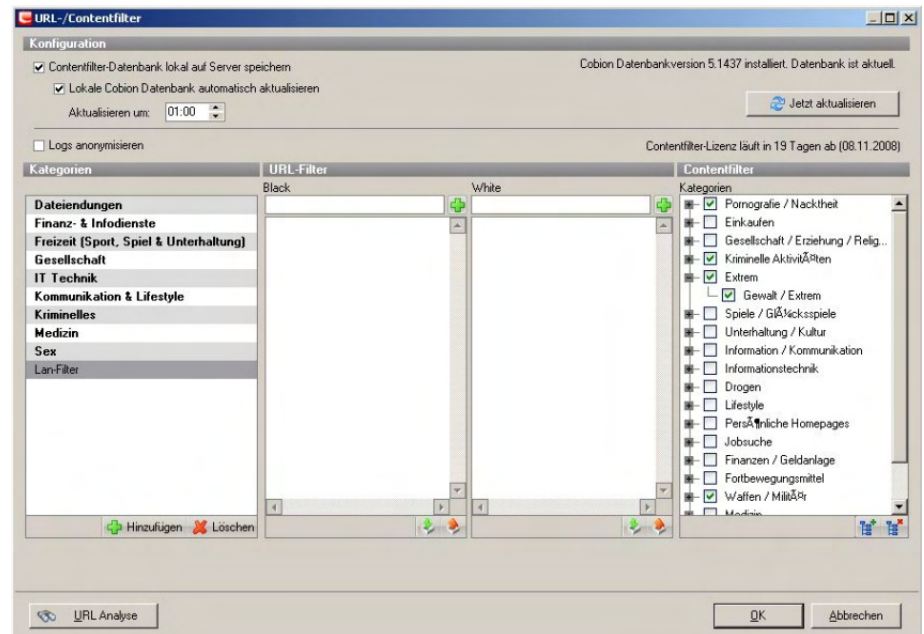
Auf diese Weise erhalten die Verantwortlichen jederzeit eine schnelle Übersicht über die Zugriffsmöglichkeiten der einzelnen Systeme. Diese pragmatische und eingängige Herangehensweise sorgt nicht nur dafür, dass erfahrene Sicherheitsspezialisten ohne weiteres dazu in der Lage sind, umfassende Regelwerke mit der Gateprotect-Lösung zu erstellen, sondern hilft auch Administratoren, die nicht jeden Tag mit der Konfiguration von Firewalls beschäftigt sind, beim schnellen Anpassen ihrer Settings. Der Konfigurationsdesktop bringt also auch für die Zielgruppe der IT-Mitarbeiter ohne spezielle Sicherheitskenntnisse Vorteile.

Weitere Security-Funktionen

Die restlichen Befehle und Funktionen der UTM-Appliance sind über eine Menüleiste verfügbar. Hier speichern die Verantwortli-

chen ihre Konfigurationen und nehmen diverse Einstellungen vor. Dazu gehören die Server-Settings, die Hostname, Domäne, Routing, die NTP-Konfiguration, die Zeitzone und ähnliches umfas-

ren fest, ob das System als Proxy arbeiten soll und – wenn ja – wie. Insgesamt bietet die Lösung drei verschiedene Proxies für HTTP, HTTPS und VoIP (SIP) an. Der HTTP-Proxy kann so-



Die Content-Filter-Konfiguration läuft – wie bei solchen Tools üblich – nach Kategorien ab. Dazu kommen Filterlisten.

sen. Dazu kommen noch externe Konfigurationszugriffe auf die Firewall und eine Funktion zum Abschalten der Ping-Antworten.

Die Netzwerkkonfiguration dient nicht nur zum Konfigurieren der einzelnen Netzwerkkarten, sondern übernimmt auch die Arbeit mit VLAN-Interfaces, Bridges und SSL-VPN-Zugängen. Die Internet-Verbindung beherrscht übrigens nicht nur Zugänge via Router, DSL und ISDN sondern unterstützt auch das Einrichten und Aktualisieren von DynDNS-Konten, so dass auch die Anwender von DSL-Zugängen mit dynamischen IP-Adressen dazu in der Lage sind, von extern aus auf ihre Dienste zuzugreifen. Das ist insbesondere in Zusammenhang mit den VPN-Funktionen von Bedeutung, davon später mehr.

Ebenfalls von Interesse sollten die Proxy-Einstellungen sein, denn hier legen die Administrato-

ren wohl als transparenter als auch als intransparenter Proxy über Port 10080 zum Einsatz kommen und im intransparenten Modus lässt er sich mit Authentifizierungsfunktionen (Benutzerauthentifizierung, Radius-Authentifizierung etc.) kombinieren.

Eine Traffic-Shaping-Funktion, die das Festlegen von QoS-Schwellwerten für die einzelnen Dienste der jeweiligen Netzkomponenten ermöglicht, gehört genauso zum Leistungsumfang der Software wie das Hochverfügbarkeits-Feature, mit dem IT-Mitarbeiter dazu in der Lage sind, ihren Internet-Zugang so zu konfigurieren, dass er auch beim Ausfall einer Appliance noch funktioniert.

Dazu kommen noch Angaben zu den auf den einzelnen Interfaces laufenden DHCP-Servern, der zu verwendenden Sprache (Deutsch, Englisch, Französisch, Ita-

lienisch) und den Benachrichtigungen. Letzte sind möglich als E-Mail-Alerts, Syslog-Meldungen und SNMP-Traps und decken alle relevanten Themenbereiche ab. Im Test ergaben sich bei der Konfiguration und dem Einsatz der Benachrichtigungen keine Schwierigkeiten.

Die Benutzerverwaltung übernimmt die Aufgabe, unterschiedliche Benutzerkonten zu erzeugen,

Die Benutzerauthentifizierung dient zum Konfigurieren der Benutzeranmeldungen. Wie bereits erwähnt, unterstützt sie nicht nur eine lokale Benutzerdatenbank auf der Appliance, sondern auch den Zugriff auf Active-Directory-Daten. Auf Wunsch lässt sich sogar ein Single-Sign-On-System mit Kerberos realisieren.

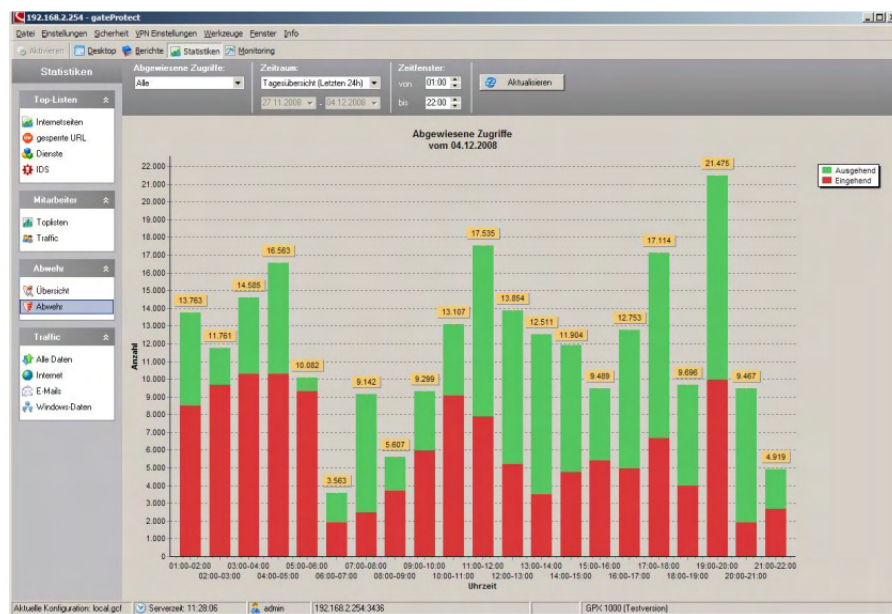
Das Sicherheitsmenü übernimmt die Konfiguration des Content-Fil-

so wie erwartet. Ebenfalls von Interesse: der Anti-Spam- und Mail-Filter. Beim Mail-Filter setzt das System auf Black- und Whitelists, während die Anti-Spam-Funktion (die ebenfalls eine eigene Lizenz benötigt und von Commtouch stammt) darüber hinaus auch noch die Möglichkeit bietet, Mails, die dem System als "verdächtig", "bekannt" oder "bestätigt" erscheinen, mit einer Spam-Kennung im Betreff zu versehen. Mit Hilfe dieser Kennung lassen sie sich später auf den Clients bei Bedarf automatisch in einen Spam-Ordner verschieben.

Bei einer echten UTM-Appliance darf natürlich auch die optionale Antivirus-Funktion nicht fehlen. Gateprotect setzt an dieser Stelle auf Kaspersky und der dazugehörige Konfigurationsdialog zeigt nicht nur Informationen über das letzte Update an, sondern versetzt die zuständigen Mitarbeiter außerdem dazu in die Lage, den Scanner für die Protokolle HTTP, FTP, SMTP und POP zu aktivieren und festzulegen, wie die Antivirus-Funktion mit bestimmten Dateien, wie etwa Archivdateien, umgehen soll.

Im Test ergaben sich beim Umgang mit der Antivirus-Engine keine Probleme, das System verkräftete auch Archivbomben wie "42.zip". Eine positive Besonderheit soll an dieser Stelle nicht verschwiegen werden: Die Appliance scannt auf Wunsch auch HTTPS-Verkehr.

Zu guter Letzt gehört auch noch ein Intrusion Detection System (IDS) auf Snort-Basis mit zum Leistungsumfang der Lösung. Die Administratoren haben hier Gelegenheit, die gewünschte Sicherheitsstufe festzulegen, Regel-



Die Statistikfunktion bietet Aufschluss über die von der UTM-Appliance vorgenommenen Maßnahmen

die auf Wunsch verschiedene Zugriffsrechte auf die einzelnen Funktionen des Konfigurationswerkzeugs erhalten.

Auf diese Weise ist es beispielsweise möglich, einzelnen Usern die Arbeit mit der Benutzerverwaltung, den Reporting-Einstellungen und den Proxy-Settings zu erlauben, während andere mit dem Konfigurationsdesktop Regeln verändern dürfen. Damit hat jedes Unternehmen die Chance, die Administration der Sicherheits-Appliance auf mehrere unterschiedliche Schultern zu verteilen (also Arbeitsteilung zu praktizieren), ohne einzelnen Benutzern mehr Rechte einräumen zu müssen als nötig.

Er basiert auf der Technik von Cobion und ermöglicht sowohl das Blockieren bestimmter Kategorien wie beispielsweise "Medizin", "Sex" oder "Gesellschaft", als auch den Einsatz von Black- und White-Listen, zum Beispiel zum Blocken von Inhalten wie "mp3" oder "wma".

Wenn die Unternehmenspolicies den Schutz der Privatsphäre der User verlangen, haben die Verantwortlichen die Option, eine Anonymisierungsfunktion für die Content-Filter-Logs zuzuschalten. Der Content-Filter wird getrennt lizenziert und die Administratoren aktivieren ihn im Betrieb auf Verbindungsebene. Im Test verhielt sich das Feature

gruppen wie "DDoS" und "Backdoor" zu aktivieren, anzugeben, welche Rechner zum internen Netz gehören, die Erkennungsmuster zu aktualisieren und die Leistung des IDS einzuschränken, um System-Performance für andere Dinge frei zu bekommen. In diesem Zusammenhang ergibt es beispielsweise Sinn, Angriffe auf bestimmte Ports nur für festgelegte Adressen zu registrieren oder auch die Portscanüberwachung auszuschalten.

VPN-Konfiguration

An VPNs (Virtual Private Networks) unterstützt das Produkt PPTP-, IPSec- und SSL-VPNs. Im Test setzten wir den Gateprotect-VPN-Client ein, um von einem externen Notebook unter Windows XP Service Pack 2 aus eine Verbindung in unser Testlabor aufzubauen. Dabei hielten wir uns an die Empfehlungen des Herstellers und verwendeten zum Verbindungsaufbau den dafür vorgesehenen Wizard im Verwaltungstool der Appliance.

Dieser fragt die für eine IPSec-Verbindung üblichen Parameter wie Zertifikate, Verschlüsselungsalgorithmen und ähnliches ab, richtet dann die Verbindung auf Serverseite ein und ermöglicht den IT-Verantwortlichen zu guter Letzt den Download einer Konfigurationsdatei, die die Verbindungsdaten für den Client enthält. Auf Client-Seite reicht es in diesem Zusammenhang, die VPN-Software zu installieren und auf die genannte Konfigurationsdatei zu klicken, danach öffnet sich der Tunnel. Das Vorgehen ist also – zumindest was homogene Gateprotect-Umgebungen angeht – ziemlich narrensicher und wird zweifellos keinen Administratoren in Verwirrung stürzen.

Da der Hersteller zwar VPN-Verbindungen mit Preshared Keys unterstützt, aber die Arbeit mit zertifikatsbasierten VPNs empfiehlt, richteten wir im Test eine Verbindung mit Zertifikaten ein. Dabei kam es zu keinen Problemen, es fiel allerdings auf, wie vorbildlich (auch für SSL-VPNs) der Hersteller das Zertifikatsmanagement realisiert hat.

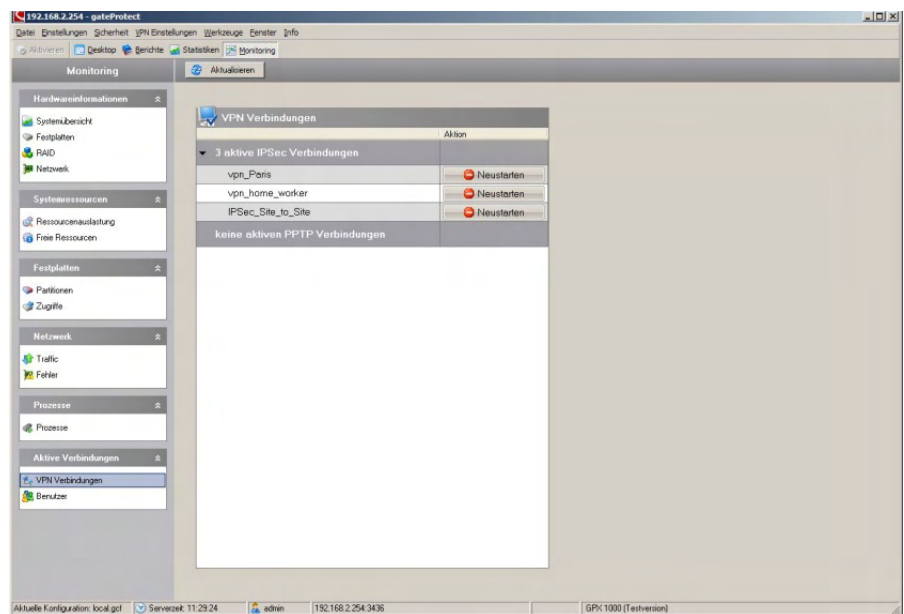
Das System weist den Anwender genau darauf hin, welche Zertifikate gebraucht werden, unterstützt ihn bei deren Erstellung und hilft auch beim Verwalten der CAs und beim Erstellen von

tiefgehende Security-Kenntnisse auf die Sprünge hilft.

Die übrigen Funktionen

Diagnosewerkzeuge wie Ping und Traceroute runden den Leistungsumfang des Administrationswerkzeugs ab. Unterhalb der Menüzeile findet sich eine Icon-Leiste, mit der die Administratoren zwischen mehreren unterschiedlichen Fensteransichten umschalten können.

An Fenstern bietet das Tool neben dem genannten Konfigurationsdesktop, auf dem die Benutzer die Rechner und ihre Ver-



Die Monitoring-Sektion informiert die Administratoren über den Systemstatus und die aktiven Verbindungen

Requests. Aufgrund dieser Funktionalitäten sollte selbst ein unerfahrener Anwender innerhalb kürzester Zeit ein funktionierendes VPN auf Basis von Zertifikaten zu Stande bringen.

Zusammenfassend lässt sich sagen, dass Gateprotect die VPN-Konfiguration sehr gut gelöst hat. Auch hier gilt also, dass das Konfigurationswerkzeug nicht nur den Sicherheitsspezialisten die tägliche Arbeit erleichtert, sondern auch Administratoren ohne

bindungen konfigurieren, auch noch Seiten mit Berichten, Statistiken und einer Systemübersicht.

Kommen wir jetzt noch einmal kurz auf den Konfigurationsdesktop zurück. Dieser unterscheidet nicht nur nach Systemen und Gruppen, sondern ermöglicht es den IT-Verantwortlichen auch, für Desktops, Server und Notebooks unterschiedliche System-Icons zu verwenden. Damit wird die grafische Darstellung übersichtlicher, was die zugrun-

deliegenden Konfigurationsparameter (IP-Adresse etc.) angeht, sind die Einträge identisch. Auf die gleiche Art und Weise wie die Rechner legen die Administratoren auf Wunsch auch VPN-Sys-

Die restlichen Funktionen sind schnell erklärt. Unter Berichte finden sich ein Gesamtbericht, eine Liste mit aktuellen Ereignissen (Timeouts und so weiter) sowie ein IDS-Report. Die Statistiken

griffsrechte einzeln zu regeln, ist eingängig, schnell verständlich und sorgt im Betrieb für ein sehr übersichtliches Interface, und zwar gleichermaßen für Sicherheitsspezialisten und Administratoren ohne Zusatzausbildung im Security-Umfeld.



Der VPN-Client versah im Test klaglos seinen Dienst

teme, VPN-Gruppen, VoIP-Komponenten, Drucker und DMZ-Hosts an. Bei den VPN-Systemen fragt die Appliance nach der einzusetzenden VPN-Verbindung, während bei den DMZ-Hosts ein Wizard startet, der unter anderem den Namen, das betroffene Interface, die IP-Adresse und den Typ (Mail-Server, Web-Server, FTP-Server) wissen möchte. Alternativ können die Benutzer die freizugebenden Dienste auch selbst definieren.

Was die Verbindungen selbst betrifft, so lassen sich auch hier mehrere Dienste zusammenfassen und der Gültigkeitszeitraum der Regeln einschränken. Damit ist es beispielsweise möglich, dafür zu sorgen, dass bestimmte Benutzer in den Pausen und nach Dienstschluss mehr Zugriffsrechte erhalten, als während der Arbeitszeit.

Abgesehen davon legen die Administratoren im Rahmen der Regelkonfiguration auch noch fest, ob das System die Zugriffe für statistische Zwecke mitschneidet, den Proxy für die Verbindung nutzt oder einen Application Level Gateway einsetzt. An gleicher Stelle erfolgt auch die Konfiguration des Port-Forwardings.

lassen sich für bestimmte Systeme, Benutzer und Zeiträume ausgeben und umfassen besuchte Internetseiten, gesperrte URLs, Dienste (also genutzte Protokolle), das IDS, das Verkehrsaufkommen, Mitarbeiter, den E-Mail-Verkehr und übertragene Windows-Daten.

Es ist übrigens möglich, Daten wie beispielsweise URLs direkt aus den statistischen Übersichten in den Content-Filter zu übernehmen. Das Monitoring bietet den Anwendern schließlich Hardwareinformationen wie den Festplattenplatz, Daten der CPUs, die Uptime und ähnliches. Dazu kommen Übersichten über die Systemressourcen, die Partitionen, den Netzwerkverkehr, die Prozesse und die aktiven VPN- sowie Benutzerverbindungen.

Fazit

Im Test hinterließ die xUTM-Appliance V8 einen ausgesprochen guten Eindruck. Die Lösung war – nicht zuletzt dank vieler Wizards – schnell in Betrieb genommen und was die einfache Konfiguration angeht, so macht der Hersteller keine leeren Versprechungen. Der Ansatz, die Systeme und Benutzer als Icons zu symbolisieren und für jede Verbindung die Zu-

Auch sonst gab sich die Lösung im Test keine Blöße. Wir setzten die Appliance im Betrieb diversen Angriffen von DoS-Tools, Security-Test-Suites und Malware-Programmen aus. Dabei kam es zu keinen Instabilitäten oder Verzögerungen. Auch bei Portscans zeigte das Produkt nicht mehr als unbedingt nötig. Alle im Test eingesetzten Viren wurden gefunden und der Content-Filter verhielt sich entsprechend der Anforderung.



Wizards wie dieser helfen bei der täglichen Arbeit mit dem Produkt

rungen. Damit konnte das Produkt von Gateprotect auf der ganzen Linie überzeugen und erzielte in allen Funktionsbereichen gute Werte. Deswegen sollten nicht nur Sicherheitsexperten einen Blick auf die Lösung werfen, sondern auch Administratoren, die eine einfach zu bedienende Firewall suchen.

Dr. Götz Güttich leitet das Institut zur Analyse von IT-Komponenten (IAIT) in Korschenbroich.

Sein Testblog findet sich unter www.iait.eu.