

UTM-Appliance für Netze aller Größen

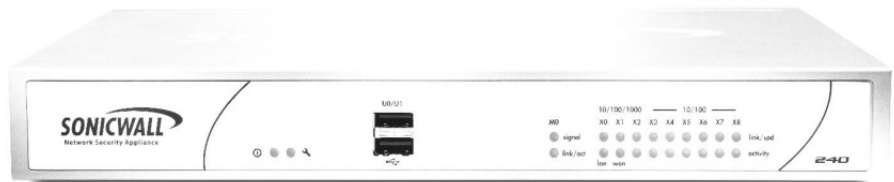
Dr. Götz Güttich

Sonicwall kombiniert in der Network-Security-Appliance-Serie (NSA) Stateful-Inspection-Firewall- und Routing-Funktionen mit diversen anderen Sicherheits-Features wie Intrusion-Prevention, Virenabwehr, Spyware-Schutz und einer Application-Firewall. Voice-over-IP-, Content-Filter-, Hochverfügbarkeits- und VPN-Funktionen gehören ebenfalls zum Leistungsumfang der Lösungen. Die UTM-Appliances der NSA-Serie sind in verschiedenen Hardware-Varianten erhältlich, die jeweils den Schutz der Netzwerke von Niederlassungen und Unternehmenszentralen sowie verteilten Netzen übernehmen. IAIT hat sich das kleinste Produkt der Serie – die NSA 240 – näher angesehen.

Die NSA 240 bringt drei GBit-Ethernet- und sechs Fast-Ethernet-Schnittstellen mit, verfügt also über einen integrierten Router. Darüber hinaus arbeitet das System mit zwei USB-Schnittstellen, einem seriellen Port, 32 MByte Flash-Speicher, 256 MByte RAM sowie zwei 500-MHz-Mips64-Octeon-CPU's und lässt sich über CLI, Web-GUI, SSH und GMS administrieren. Zudem unterstützt die Lösung bis zu 25 parallele Site-to-Site-VPN-Tunnel. Da der Hersteller einen PC-Card-Slot in die Appliance integriert hat, lassen sich zusätzlich zu klassischen Netzwerkverbindungen sowohl analoge Modem- als auch WLAN-Anbindungen ans Internet realisieren. Damit ist beispielsweise ein WAN/WAN-Failover möglich, der automatisch stattfindet, wenn der normale Internet-Zugang ausfällt.

Inbetriebnahme

Vor der Inbetriebnahme des Produkts ergibt es Sinn, zunächst einmal die Seriennummer und den Authentifizierungscode der Lösung aufzuschreiben. Die beiden Angaben finden sich auf einem



Aufkleber auf der Unterseite der Appliance und sind unbedingt erforderlich, um das Produkt online zu aktivieren. Die Registrierung erfolgt auf der Website www.mysonicwall.com und setzt das vorherige Erstellen eines Kunden-Accounts voraus. Sobald wir unsere UTM-Appliance registriert hatten (bei Bedarf ist es auch möglich, die Registrierung direkt mit der laufenden Appliance durchzuführen), schlossen wir die Lösung an und fuhren sie hoch. Danach verschoben wir einen Administrations-Client in das Subnetz 192.168.168.0 und griffen dann mit der Default-IP-Adresse 192.168.168.168 auf die Appliance zu. Bei der ersten Verbindungsaufnahme startet ein Wizard, der den Anwender durch die Initialkonfiguration führt. Dieser möchte zuerst die zu verwendende Sprache wissen (zur Zeit steht hier nur Englisch zur Auswahl) und verlangt dann ein Pass-

wort für das Administrationskonto. Dieses Vorgehen ist optimal, stellt Sonicwall doch so sicher, dass keine UTM-Lösungen mit Default-Zugangsdaten im Netz aktiv sind. Nach der Passwort-Vergabe möchte das System die Zeitzone und die PC-Card wissen, die im Betrieb zum Einsatz kommen soll. Hier stehen als Optionen Wireless-WAN und analoges Modem zur Verfügung. Anschließend muss der Administrator den zu verwendenden Netzwerkmodus angeben (statisch, DHCP, PPPoE oder PPTP). Im Test setzten wir die Appliance an einem DSL-Zugang von T-Online ein und entschieden uns an dieser Stelle deshalb für PPPoE. Daraufhin wollte der Wizard die WAN-Zugangsdaten sowie die LAN-IP-Adresse, die lokale Netzmaske und die DHCP-Konfiguration für das LAN wissen. Zum Schluss fragte der Assistent noch ab, in welcher Form die

Ports der Appliance Verwendung finden sollen. Dabei stehen mehrere Konfigurationen zur Wahl: Nur zwei Ports für LAN und WAN, ein WAN-Anschluss mit allen anderen Ports als LAN-Verbindungen, eine Konfiguration mit WAN, LAN und DMZ sowie ein Modus mit WAN, DMZ und LAN-Switch. Sobald alle Angaben gemacht wurden, zeigt das System eine Zusammenfassung an und führt die Änderungen durch. Damit steht die Lösung im Netz zur Verfügung.

Konfiguration

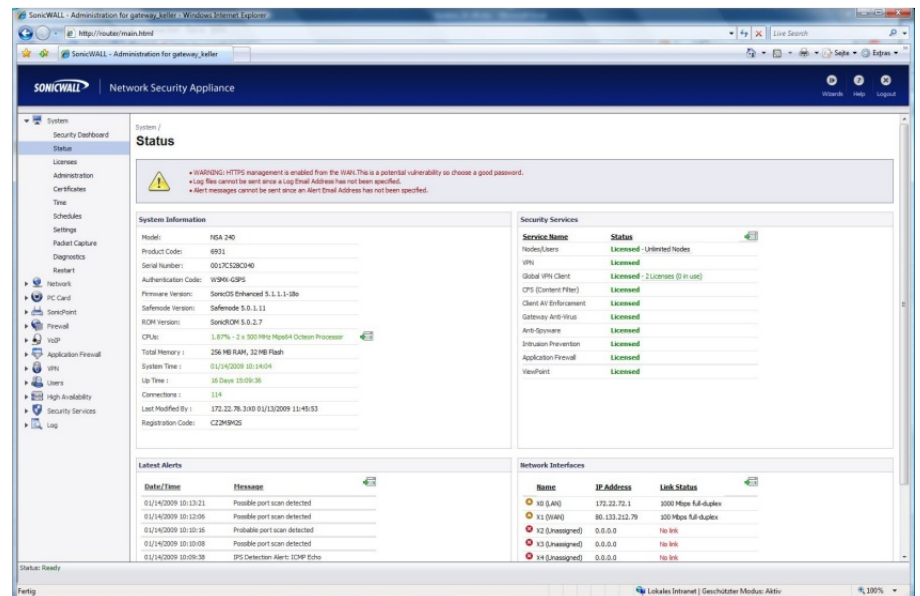
Im laufenden Betrieb kann der Administrator über die URL `http://{IP-Adresse der Appliance}` und das Zugangskonto "admin" mit dem während der Erstkonfiguration vergebenen Passwort auf die Appliance zugreifen. Nach dem Login landet er auf einer Statusseite, die ihn über Faktoren wie den Typ des Produkts, die Firmware-Version, die Seriennummer, die Hardware, die Uptime sowie vorhandene Verbindungen und Lizenzen informiert. Ansonsten wurde das Konfigurationswerkzeug Explorer-ähnlich gestaltet und verfügt über eine Menüstruktur auf der linken Seite, während sich der eigentliche Arbeitsbereich rechts befindet.

Wenden wir uns zunächst den Wizards zu, die der Hersteller in das Konfigurationstool integriert hat und die sich über einen Eintrag am oberen Fensterrand aufrufen lassen. Der erste dieser Wizards ist der Setup-Assistent, den wir bereit im vorigen Abschnitt abgearbeitet haben. Der so genannte Portshield-Interface-Wizard eignet sich im Gegensatz dazu, die Konfiguration der einzelnen Interfaces der Appliance (LAN, WAN, DMZ etc.) im laufenden

Betrieb an die gerade aktuellen Anforderungen anzupassen.

Der dritte Assistent nennt sich "Public Server" und sorgt für die Konfiguration des Port-Forwardings, um interne Dienste im Internet zur Verfügung zu stellen. Im Test gaben wir mit Hilfe des

den Key-Typ entschieden haben, so möchte der Assistent wissen, welche Diffie-Hellman-Gruppe, welche Verschlüsselung und welche Authentifizierung zum Einsatz kommen sollen. Außerdem müssen die IT-Verantwortlichen noch angeben, wie lang die Lebensdauer der Verbindung ist



Die Statusseite bietet nach dem Login einen ersten Überblick über den Zustand der Appliance

Wizards einen SSH-Server im LAN frei, dabei kam es zu keinen Schwierigkeiten. Der Assistent bietet bereits fertig konfigurierte Einträge für Web-, Mail-, FTP- und Terminal-Server, alle anderen Dienste lassen sich bei Bedarf aber auch einrichten.

Der nächste Wizard übernimmt die Konfiguration von VPN-Zugängen. Mit ihm lassen sich sowohl Site-to-Site als auch WAN-Group-Verbindungen realisieren. Gehen wir zunächst auf die WAN-Group-VPNs ein. Mit WAN-Group meint der Hersteller eingehende Connections vom Sonicwall VPN-Client. WAN-Group-VPNs arbeiten wahlweise mit dem Default-Key oder einem eigenen Preshared-Secret. Wenn sich die Anwender in Bezug auf

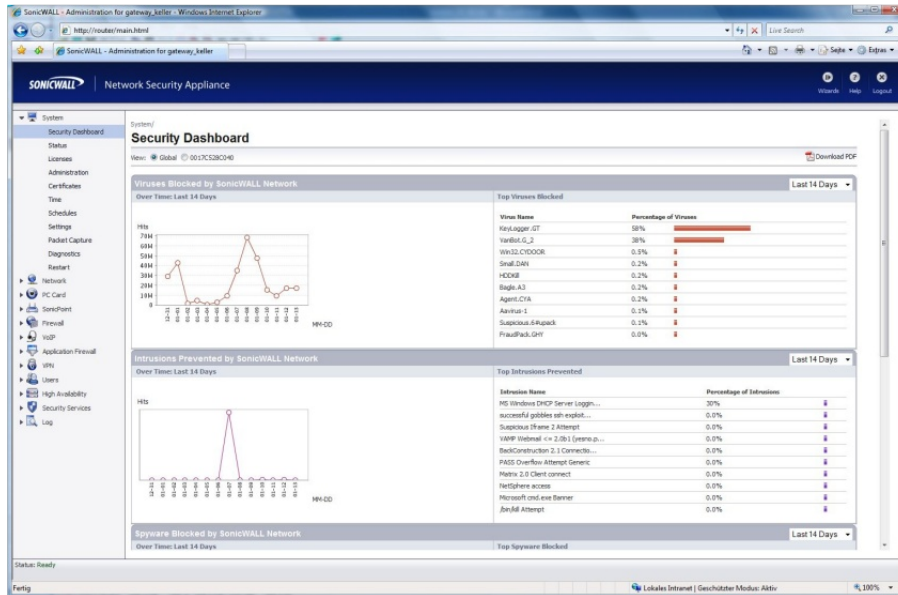
und ob das betroffene System mit einer virtuellen IP-Adresse eingebunden werden soll (dann erscheint es als interne Maschine).

Das schließt die Konfiguration ab und die VPN-Verbindung steht nun zur Einwahl bereit. Beim Einrichten von Site-to-Site-VPNs geben die zuständigen Mitarbeiter zunächst einen Namen und den zu verwendenden Preshared Key an, definieren dann die Remote-Peer-IP-Adresse, teilen dem System die zu verbindenden Netzwerkadressen mit und legen dann VPN-spezifische Details wie Diffie-Hellmann-Gruppe, Verschlüsselung und so weiter fest. Sobald die genannten Angaben gemacht wurden, schließt der Wizard die Konfiguration ab.

Im Test richteten wir mit Hilfe des Sonicwall-VPN-Clients eine WAN-Group-Verbindung zu einem Client-System unter Windows XP Professional mit Service Pack 3 ein. Der genannte Client lässt sich über eine Windows-

ziehungsweise Benutzernamen und Passwort, holt sich dann die Konfigurationsdaten vom Gateway und richtet die Verbindung ein. Der Aufbau eines Tunnels ist folglich extrem einfach. Sollte der automatische Download der

der Filterung, so überwacht das System auch Attachments und Sendungen bestimmter Größe. Beim Web-Zugriff bietet die Appliance zusätzlich die Möglichkeit, nach URLs und bestimmten Browsern zu suchen. Auf diese Weise lässt sich etwa das Surfen mit dem Internet-Explorer unterbinden. Sobald die Verantwortlichen die jeweils zu überwachenden Inhalte festgelegt haben, definieren sie die von der UTM-Lösung durchzusetzende Aktion (Block, Bypass oder Log) und vergeben einen Policy-Namen. Damit ist die Regelerstellung abgeschlossen. Generell können wir sagen, dass die von Sonicwall bereit gestellten Assistenten eine große Hilfe beim schnellen Einrichten der wichtigsten Gateway-Funktionen darstellen.



Mit dem Security-Dashboard erhalten die Anwender umfassende Informationen zu den gerade im Netz aktiven Bedrohungen

übliche Setup-Routine einspielen, verlangt während der Installation das Ausschalten der auf dem Zielsystem vorhandenen Desktop-Firewalls und Disk-Protecti-on-Lösungen und benötigt zur Kommunikation die UDP-Ports 67 und 68. Wenn das Setup abgeschlossen ist, können die Anwender die Software starten. Beim ersten Mal kommt sie mit einem Connection-Wizard hoch, der zunächst fragt, ob der Aufbau eines VPNs zu einem entfernten oder einem lokalen Gateway (letzteres ergibt beispielsweise zum Absichern von WLAN-Anbindungen Sinn) gewünscht ist. Beim lokalen VPN fragt er lediglich noch, ob er für die Verbindung ein Icon auf dem Desktop erzeugen soll, beim Remote-VPN möchte er zusätzlich noch wissen, wie die IP-Adresse der Gegenstelle lautet. Ja nach Konfiguration fragt das System beim Verbindungsaufbau noch nach dem Preshared-Key be-

Konfigurationsparameter vom Gateway aus irgendwelchen Gründen nicht möglich sein, so haben die Administratoren immer noch die Option, die Konfigurationsinformationen über das Web-Interface der Appliance manuell zu exportieren und auf dem Client einzuspielen. Im Test ergaben sich dabei keine Schwierigkeiten.

Doch nun zurück zu den Wizards. Der letzte Assistent, den Sonicwall anbietet, der "Application Firewall Wizard", sorgt für die einfache Definition der Application Level Policies. Mit seiner Hilfe legen die Administratoren Regeln zum Überwachen des SMTP-, POP3-, FTP- und Web-Zugriffsverkehrs fest. Dabei sind sie unter anderem dazu in der Lage, Up- und Downloads zu filtern und darüber hinaus bei FTP-Verbindungen Dateinamen und -endungen im Auge zu behalten. Stehen E-Mails im Mittelpunkt

Funktionen der Appliance

Gehen wir nun noch etwas genauer auf den gesamten Funktionsumfang der Appliance ein. Die Wizards sind ja lediglich dazu da, den Administratoren die Arbeit zu erleichtern und erstrecken sich bei Leibe nicht auf alle Funktionsbereiche der Lösung. Deswegen müssen die zuständigen Mitarbeiter im laufenden Betrieb oft auch Konfigurationsänderungen über die einzelnen Menüpunkte des Administrationswerkzeugs vornehmen. Dieses wurde recht übersichtlich gestaltet und sollte eigentlich keinen IT-Fachmann vor unüberwindliche Hindernisse stellen. Im Rahmen der Systemkonfiguration stellt Sonicwall den Anwendern zunächst einmal das so genannte Security Dashboard zur Verfügung. Dieses präsentiert Real-Time-Protection-Daten von Sonicwall-Appliances auf der ganzen Welt. Damit ermöglicht es den IT-Verantwortlichen, sich jederzeit ein umfassendes Bild über

die gerade im Netz aktiven Bedrohungen durch Viren, Intrusion-Versuche, Spyware und ähnliches zu machen. Die jeweils gleichen Daten lassen sich an der selben Stelle auch für das lokale System ausgeben, so dass jederzeit ein schneller Überblick über die Bedrohungen für das eigene Netz realisierbar ist. Uns erschien das Dashboard als gute Idee, erlangen die zuständigen Mitarbeiter auf diese Weise doch umfassende Informationen über die im Auge zu behaltende Malware.

Über die Lizenzverwaltung lassen sich Dienste wie VPN, Antivirus und ähnliches lizensieren, Ablaufdaten für aktive Lizenzen einsehen und die Lizenzen auf der Appliance mit denen im Online-Konto unter www.mysonicwall.com synchronisieren. Die "Administration" übernimmt im Gegensatz dazu das Festlegen des Administratorpassworts und der Richtlinien für das Passwort in Bezug auf Gültigkeitsdauer und Komplexität. Dazu kommen noch die Definition der Ports für HTTP-, HTTPS- und SSH-Zugänge, das Angeben von Lockout-Zeiten nach einer gewissen Zahl fehlgeschlagener Login-Versuche und das Setzen der SNMP-Settings. Der Appliance fehlt folglich keines der grundlegenden Features zur Zugriffssicherheit.

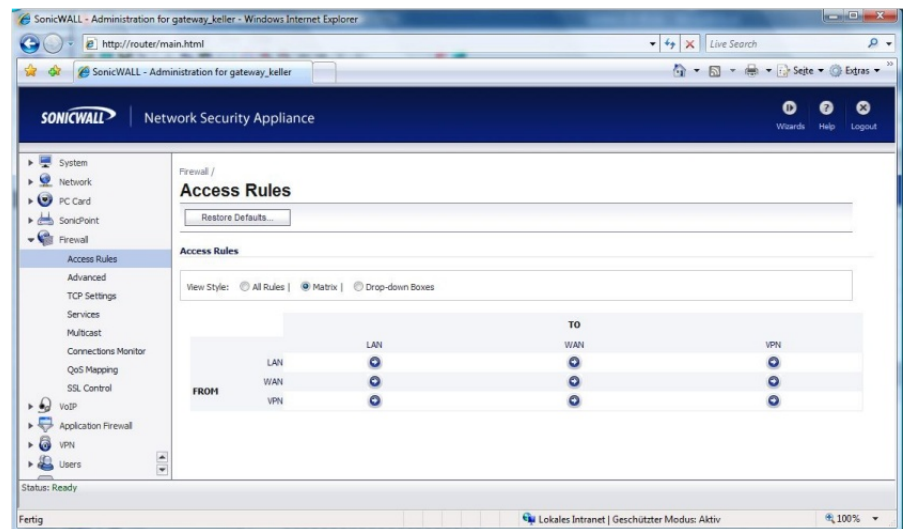
Die nächsten Funktionen sind schnell erklärt. Die Zertifikatsverwaltung hilft beim Erstellen von Signing Requests sowie beim Einsehen und Importieren von Zertifikaten. "Time" dient zum Angeben der Zeitzone und der NTP-Settings. Unter "Schedules" legen die Administratoren Zeiträume an, die beim Erstellen von Regeln zum Einsatz kommen, wie beispielsweise "Arbeitsstunden" oder "Wochenende". Damit

lässt sich die Gültigkeit der Regeln auf bestimmte Zeiträume beschränken, so dass die Anwender beispielsweise während ihrer Arbeitszeit auf andere Websites Zugriff erhalten, als in ihrer Freizeit.

Mit Hilfe des "Settings"-Dialogs lassen sich Diagnosereports erzeugen, die Einstellungen sichern und die Firmware der Appliance aktualisieren. Im Test führten wir ein Firmware-Update von Version 5.1.1.1-150 auf 5.1.1.1-180 durch. Dazu mussten wir die Firmware aus dem Download-Bereich unseres Kontos unter www.mysonicwall.com herunterladen und auf unserem Adminis-

übertragungen im Netz zu verschaffen. Die dabei gesammelten Informationen lassen sich auch auf einem FTP-Server ablegen, und zwar im Test-, HTML- oder Libcap-Format. Bei Bedarf stellt das Web-Interface sämtliche Pakete auch im Detail oder als HEX-Dump dar. Da ein Sniffer auf dem Gateway oft nützlich ist, fiel diese Funktionalität im Test recht positiv auf.

Die Diagnosefunktionen bieten den Administratoren die Option, Tech-Support-Reports zu VPN-Keys, dem ARP-Cache, den DHCP-Bindings oder IKE Informationen zu erzeugen. Darüber hi-



Übersichtlich: Die Matrix-förmige Definition der Firewall-Regeln

trationsrechner speichern. Anschließend genügte es, die entsprechende Datei mit Hilfe des Administrationswerkzeugs auf das Sonicwall-System hochzuladen, das sie daraufhin ohne weiteres Zutun einspielte.

Unter "Packet Capture" stellt Sonicwall noch einen Sniffer zur Verfügung, der den zuständigen Mitarbeitern dabei hilft, ihren Verkehr im Auge zu behalten. Er ist dazu in der Lage, die von bestimmten Interfaces, IP-Adressen, Quellen und Zielen kommenden Pakete aufzuzeichnen und so Klarheit über die Daten-

aus stehen den IT-Mitarbeitern hier Werkzeuge wie Ping und Traceroute zur Verfügung und sie haben die Möglichkeit, den Webserver der Appliance, die CPUs und viele andere Parameter der Lösung zu überwachen. Restarts des Produkts stellen über den Diagnosedialog ebenfalls kein Problem dar.

Über die Netzwerkkonfiguration richten die Administratoren nicht nur die Interfaces ein und sehen Verkehrsstatistiken an, sondern konfigurieren auch den WAN-Failover, das Load-Balancing und die Zonen für die vorhande-

nen Schnittstellen (zum Beispiel Trusted und Untrusted für LAN und WAN). Auf Zonenbasis lassen sich dann Dienste wie Content Filter, Spyware-Schutz oder IPS aktivieren oder abschalten. Mit Hilfe der DNS-Settings legen die zuständigen Mitarbeiter fest, ob das System mit fest eingestellten DNS-Servern arbeitet oder die DNS-Server des Internet-Providers nutzt.

"Adress Objects" übernimmt im Gegensatz dazu das Definieren der Objekte, die dann bei der Regeldefinition zum Einsatz kommen. Dazu gehören unter anderem Subnetze, IP-Adressen, Access Points, White-Lists, Black-Lists und Hosts. Mit diesen Objekten lassen sich dann Regeln erstellen, die etwa einem Host den Zugriff auf bestimmte Subnetze erlauben.

Zusätzlich zu den genannten Funktionen gehören noch diverse weitere Konfigurationsdialoge zu den Netzwerkeinstellungen, wie etwa zum Routing (mit Advanced Routing), zu den NAT-Policies, zum DHCP-Server, zum ARP-Cache, zu DynDNS, zu einem eventuell vorhandenen Web-Proxy und zum IP-Helper. Der letztgenannte übernimmt das Weiterleiten von DHCP-Anfragen, die bei der Sonicwall-Lösung eingehen, an einen zentralen DHCP-Server. Im Test hinterließ die Netzwerkkonfiguration einen übersichtlichen Eindruck.

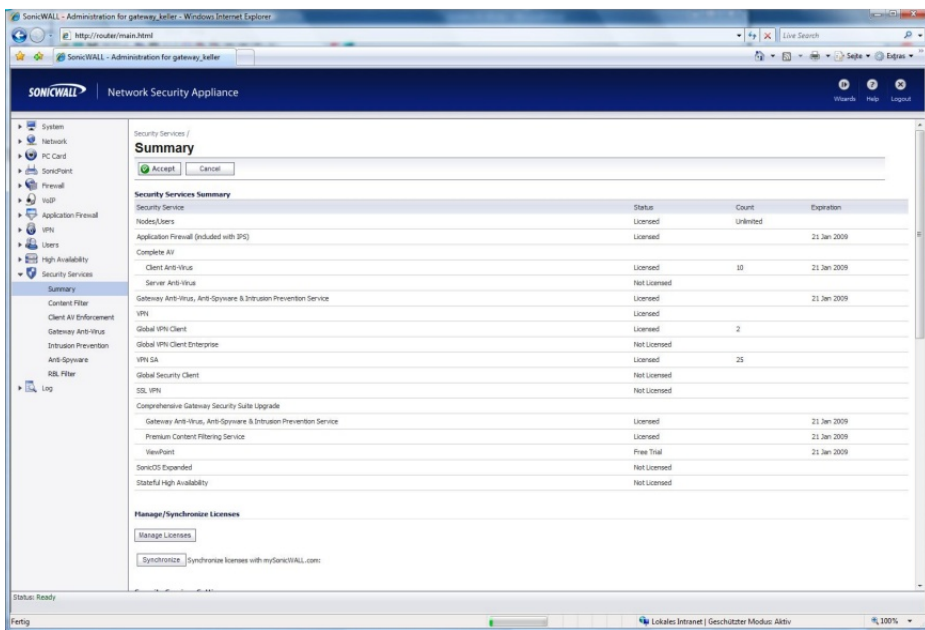
Im Konfigurationsmenü für die PC-Card sehen die Verantwortlichen nicht nur den Status dieser Komponente ein, sondern nehmen auch Einstellungen zum Wireless WAN (WWAN), beziehungsweise zum analogen Modem vor, während die Sonicpoint-Settings den Administratoren da-

bei helfen, die Zusammenarbeit der NSA-Appliance mit Sonicwall Access Points zu konfigurieren. Dazu gehören auch Erkennungsfunktionen für Rogue Access Points, Netstumbler- sowie Wellenreiteraktivitäten und ähnliches.

Im Rahmen der Firewall-Konfiguration nehmen die Verantwortlichen die Definition der Regeln für den Verkehr zwischen den einzelnen Netzen vor. Die Sonicwall-Lösung präsentiert diese Regeln nicht nur auf die traditionelle Art in Listenform, sondern auch als Matrix, die klar zeigt, welche Regel für welche Verkehrsrichtung gilt (LAN nach

domize IP" und "Drop Source Routed IP Pakets" zu aktivieren, während die "TCP Settings" zum Einsatz kommen, um eine TCP-Compliance mit den RFCs 793 und 1122 zu erzwingen, beziehungsweise TCP-Verbindungs-Timeouts zu setzen. An gleicher Stelle stehen auch TCP-Verkehrsstatistiken zur Verfügung.

Die Definition der Dienste läuft über den Services-Dialog ab. Hier legen die IT-Mitarbeiter die Dienste fest, die sie über die Regeln freigeben oder blockieren möchten. Dabei hat der Hersteller die meisten Services bereits vordefiniert, es ist aber auch möglich, eigene anzulegen. Das



Mit Hilfe der Übersichtsseite der Sicherheitsdienste verwalten die Administratoren unter anderem ihre Lizenzen

WAN, WAN nach DMZ und so weiter). Die Regeln selbst bestehen aus der Quell- und der Zielzone, dem Dienst, den zulässigen Benutzern und dem Zeitplan, für den die Regel Gültigkeit besitzt. Bei Bedarf lassen sich die Regeln auch mit QoS-Einstellungen kombinieren.

Die Advanced-Settings zur Firewall ermöglichen es den Administratoren, Funktionen wie "Ran-

geht über den Namen, das Protokoll (TCP, UDP, GRE, L2TP etc.) und – bei Bedarf – die Port-Range. Um die Übersichtlichkeit zu verbessern, lassen sich die Dienste auch in Dienstgruppen zusammenfassen.

Die restlichen Funktionen der Firewall-Konfiguration befassen sich mit der Multicast-Konfiguration, dem QoS-Mapping und der SSL-Steuerung. Letztere arbeitet

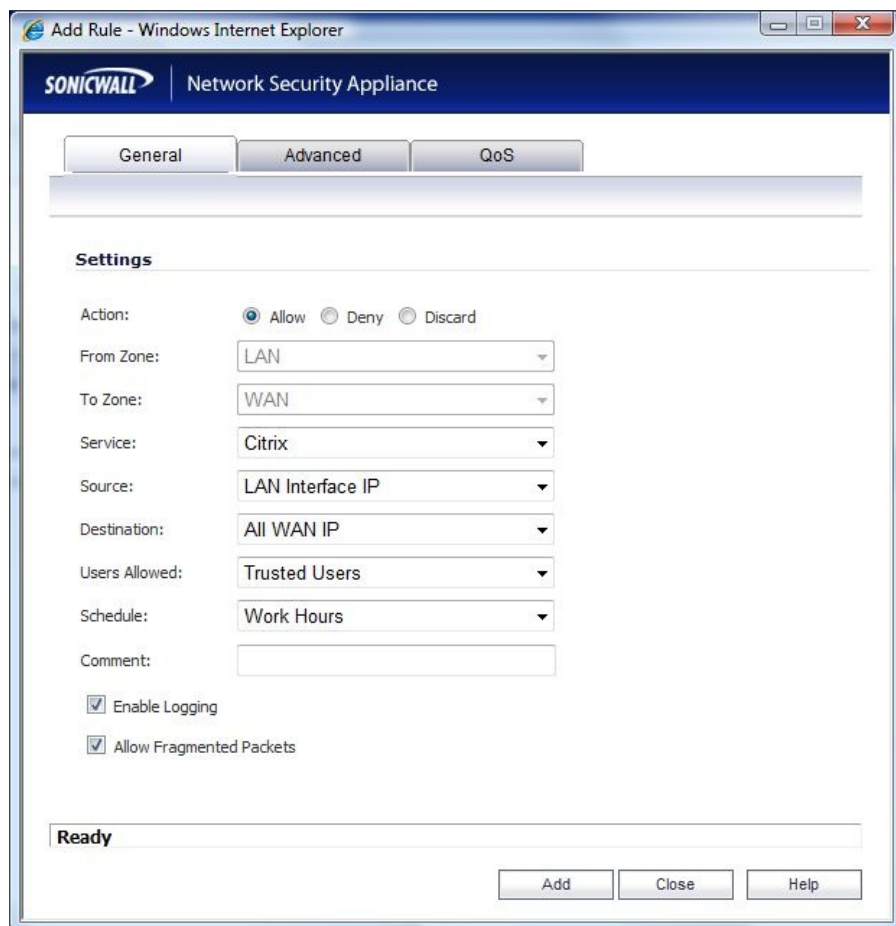
mit Black- und Whitelists und erkennt beziehungsweise blockiert schwache Verschlüsselungsalgorithmen und Zertifikate, die von Certificate Authorities stammen, die als "untrusted" gelten. Damit liefert die Sonicwall-Appliance sehr nützliche und leistungsstarke Werkzeuge zum Absichern von SSL-Verbindungen. Ein Ver-

Die Application-Firewall-Sektion bietet den Verantwortlichen die Option, Regeln zu definieren, die über den Leistungsumfang des dazugehörigen Wizards hinausgehen. Zur Arbeit mit diesen Policies lassen sich auch so genannte Anwendungsobjekte erstellen, die festlegen, wann das System aktiv wird. Für die Applicati-

ches zur Verfügung. Es gibt sogar die Option, eigene Aktionen zu definieren (wie "Disable E-Mail-Attachment – Add Text", "HTTP Redirect" oder auch "FTP Notification Reply"). Bei Bedarf arbeitet die Application-Firewall auch mit "E-Mail User Objects" zusammen. Dabei handelt es sich um Listen mit E-Mail-Nutzern. Der Leistungsumfang des Gateways in diesem Bereich kann folglich durchaus überzeugen und das Produkt verhielt sich im Test erwartungsgemäß.

Im Rahmen der VPN-Konfiguration legen die IT-Verantwortlichen VPN-Policies fest. Neben den bereits erwähnten manuellen Schlüsseln und Preshard Keys mit IKE unterstützt das System auch den Einsatz von Zertifikaten. Es wäre gut, wenn Sonicwall diese in einem der nächsten Firmware-Releases auch in die Konfiguration mit dem Assistenten integrieren würde. Dazu kommen dann noch die sonst üblichen VPN-Einstellungen wie Proposals, Netzwerke, Keepalive-Time, NetBIOS-Broadcast und so weiter. Mit Hilfe des Advanced-Dialogs aktivieren die Mitarbeiter Funktionen wie "IKE Dead Peer Detection", NAT Traversal" oder auch "OCSP Checking". An gleicher Stelle lassen sich zudem Einstellungen zu "DHCP over VPN" vornehmen (mit einer Liste der aktiven Leases) und ein L2TP-Server aktivieren, beziehungsweise eine Liste der aktiven L2TP-Sitzungen anzeigen. Der genannte Server übernimmt bei Bedarf unter anderem die sichere Kommunikation mit externen Windows-Clients.

Die Benutzerverwaltung der Appliance arbeitet mit LDAP, Radius und lokalem Login. Eine Status-



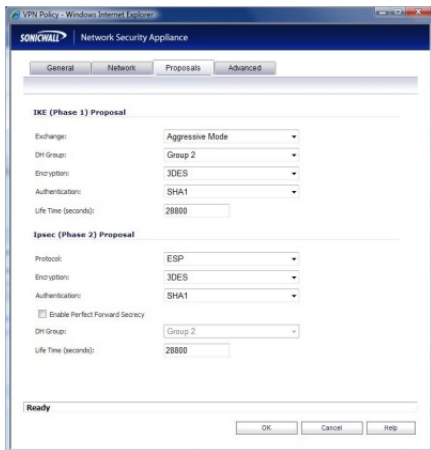
Die Regeldefinition der NSA-240-Appliance wird keinen IT-Mitarbeiter vor unlösbare Aufgaben stellen

bindungsmonitor, dessen Ausgabe sich nach Quelle, Ziel und Protokoll filtern lässt, schließt den Leistungsumfang der Firewall-Rubrik ab.

Die Konfiguration der Einstellungen zur Telefonie über das Internet läuft über das VoIP-Menü (Voice over IP) ab. Dabei unterstützt das System die Protokolle H.323 und SIP. Zusätzlich zu den Konfigurationsoptionen bietet es an dieser Stelle auch eine Übersicht über den Status der Anrufe.

on Objects gibt es verschiedene Objekt-Typen (wie Active-X, Class ID, E-Mail From, FTP-Command oder HTTP-Referrer) und Match-Types (Exact Match, Partial Match, Prefix Match, Suffix Match). Dazu kommen dann die zu filternden Inhalte oder die zulässigen Mailgrößen. Auf diese Weise haben die Administratoren sehr viele Möglichkeiten, genau an ihre Anforderungen angepasste Filter zu erzeugen. An Aktionen stellt die Appliance Block, Reset, Drop, Bypass und ähnli-

übersicht zeigt die verbundenen User mit der bis zum automatischen Logout verbleibenden Inaktivitätszeit. Bei den Einstellungen legen die zuständigen Mitarbeiter unter anderem URLs fest, die keine Benutzerauthentifizierung benötigen und aktivieren einen "Single Sign On" mit dem Sonicwall SSO-Agenten. Im Test stellte uns das Benutzermanage-



Beim Festlegen der VPN-Parameter bietet das Konfigurationsinterface die üblichen Kandidaten an

ment, mit dem sich übrigens auch Gruppen und Gastkonten administrieren lassen, vor keine Probleme.

Das nächste Menü befasst sich mit der Hochverfügbarkeit, da sich zwei der Sonicwall-Appliances auf Wunsch parallel betreiben lassen, um einen Single-Point-of-Failure beim Internetzugang auszuschließen. Interessanter ist aber die Definition der "Security Services", denn sie übernimmt sämtliche Einstellungen zum Content Filter sowie zu den Anti-Viren-, Anti-Spyware und sonstigen Funktionen. Eine Übersichtsseite bietet in diesem Zusammenhang Aufschluss darüber, welche Dienste mit welchen Lizenzen aktiviert wurden und zu welchem Termin letztere ablaufen. An gleicher Stelle verwalten die Administratoren die Lizenzen, stellen das "Security

Service Setting" ein (hier gibt es die Optionen "Maximum Security" und "Performance Optimized") und nehmen diverse allgemeine Einstellungen zu den Security Services vor.

Im Detail geht es dann zunächst an die Einstellungen des Content Filters. Im Betrieb stehen den Anwendern Filter von Sonicwall und Websense zur Verfügung. Die dazugehörige Funktion blockiert bei Bedarf neben URL-Listen zu bestimmten Themen wie "Gaming", "Sex" und ähnlichem auch Active-X-, Java- und Cookie-Übertragungen. Das Content Filtering lässt sich jederzeit für Trusted Sites deaktivieren.

Mit dem "Client Antivirus Enforcement" unterstützt die Appliance die IT-Abteilung beim Warten der Antivirus-Software auf den Clients (hierfür kommt eine von Sonicwall speziell angepasste Variante des McAfee-Virenschanners zum Einsatz). Wenn diese Funktion aktiv ist, überwacht das System die Version der Antiviren-Pattern auf dem Client-Rechnern und stößt eine Aktualisierung an, wenn diese veraltet sind. Außerdem blockiert sie den Internet-Zugang der betroffenen Anwender, wenn ihre Anti-Viren-Lösung sich nicht auf dem aktuellen Stand befindet. Damit sorgt das Produkt dafür, dass Anwender, die beispielsweise aus Performance-Gründen ungefragt die Antivirus-Lösung ihres Notebooks entfernt haben, nicht mehr ins Netz kommen können. Das nächste Menü übernimmt die Konfiguration der Antivirus-Software auf dem Gateway selbst. Hier sehen die Administratoren eine Liste der Signaturen ein, geben die zu überwachenden Protokolle an (wie HTTP, FTP, IMAP, SMTP, POP3, CIFS/NetBIOS

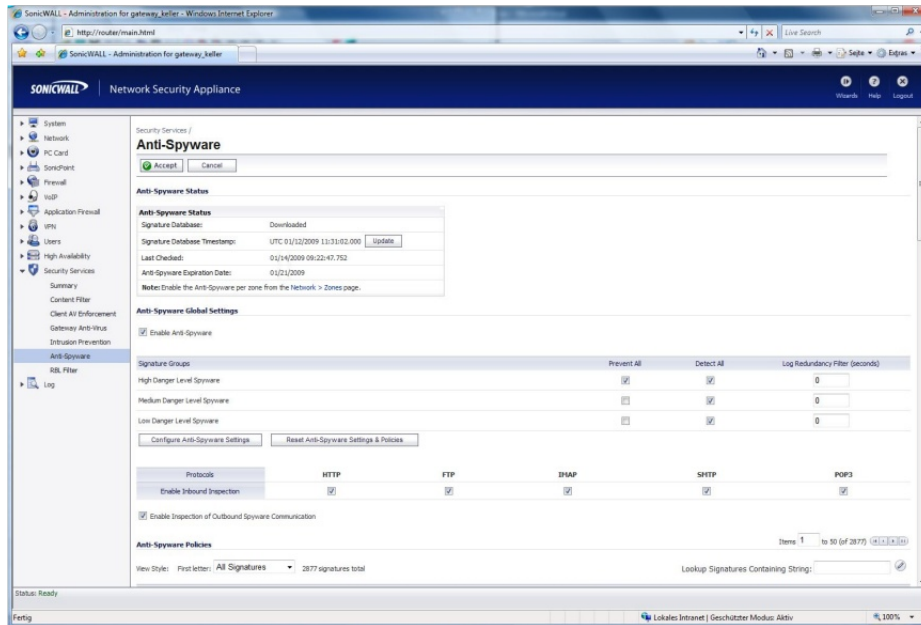
und TCP Stream) und legen zusätzliche Einstellungen fest, zum Beispiel zum Einschränken der Übertragungen passwortgeschützter Zip-Dateien und ähnlichem. Außerdem informieren sich die zuständigen Mitarbeiter an dieser Stelle über die Version der Antivirensignatur und können sie bei Bedarf gleich manuell aktualisieren. Zum Schutz vor Viren setzt Sonicwall übrigens eine selbst entwickelte Stream-basierte Engine ein, die über 50 Protokolle überwachen kann.

Die Intrusion-Prevention-Konfiguration informiert die IT-Verantwortlichen zunächst über ihren Status und das Datum des letzten Updates. Gleichzeitig bietet auch sie eine Option zum sofortigen Aktualisieren ihrer Datenbank an. Darüber hinaus legen die Administratoren fest, ob das System Angriffe hoher, mittlerer oder niedriger Priorität erkennen und verhindern soll. Eine editierbare Liste der IPS-Policies mit Benutzern, IP-Bereichen, Zeiträumen und vergleichbarem schließt die Konfiguration der Intrusion Prevention ab. Das dabei verwendete System kommt ebenfalls von Sonicwall. Die letzten beiden Punkte der Security Services befassen sich mit den gleichfalls von Sonicwall implementierten Anti-Spyware-Funktionen und den RBL-Filtern. Auch bei den Anti-Spyware-Settings gibt es wieder die Möglichkeit, den letzten Updatezeitpunkt einzusehen und die Datenbank manuell auf den letzten Stand zu bringen. Außerdem geben die Verantwortlichen noch an, ob die Appliance Spyware mit hohem, mittlerem oder niedrigem Gefahrenniveau erkennen und abblocken soll. An Protokollen überwacht das System HTTP, FTP, IMAP, SMTP und POP3 eingehend. Eine Unter-

suchung ausgehenden Verkehrs lässt sich auf Wunsch ebenfalls aktivieren. Auch hier gehört wieder eine editierbare Liste mit Signaturen zum Leistungsumfang des Konfigurationstools. Diese Liste enthält unter anderem Zeiträume und ausgenommene Benutzer. Der RBL-Filter übernimmt das Real Time Blocking

"Automation"-Feature übernimmt das automatische Mailen von Log- und Alert-Meldungen, bei Bedarf auch mit einem Mail-Server, der SMTP-Authentifizierung verlangt. Die Seite zur "Name Resolution" legt fest, welche Dienste in welcher Reihenfolge zum Auflösen der Rechnernamen in den Log-Files zum Einsatz

Anschließend nahmen wir das Produkt mit diversen Sicherheits- und "Hacker"-Tools unter die Lupe, um zu sehen, ob es freiwillig irgendwelche Informationen preisgibt, die ein Hacker zum Angriff nutzen könnte und ob es sich durch Denial-of-Service-Angriffe aus der Ruhe bringen ließ. Dabei stellten wir fest, dass Portscanner wie nmap auch mit aktiver OS-Erkennung keine relevanten Daten über das System gewinnen konnten, während Nessus nur auf der internen Schnittstelle anhand der vom HTTP-Server gewonnenen Daten dazu in der Lage war, die Lösung als Sonicwall-Appliance zu erkennen. Unsere Hackertools hatten weder auf der internen, noch auf der externen Schnittstelle nennenswerte Auswirkungen. Zu guter Letzt definierten wir noch diverse Regeln für die Application Firewall und versuchten, etliche Viren durch die Appliance zu schicken. Dabei kam es zu keinen Überraschungen, alle Viren wurden erkannt und die Regeln arbeiteten wie erwartet.



Die Anti-Spyware-Funktion überprüft auf Wunsch auch den ausgehenden Verkehr

nach Listen von Spamhaus und dnsbl.sorbs.net. Bei Bedarf fügen die Administratoren dem System auch eigene RBL-Server hinzu. Mit dieser Dienste-Vielfalt konnte die Appliance in Bezug auf die vorhandenen Funktionen voll überzeugen. Ein Konfigurationsdialog zum Logging schließt den Funktionsumfang des Web-Interfaces ab. Hier zeigen die Administratoren das Log als Liste an, löschen es, mailen es weiter und filtern die Einträge nach Quelle, Ziel und vergleichbarem. Außerdem legen sie den Logging- sowie den Alert-Level fest und beschränken die Anzeige auf bestimmte Kategorien wie "Attacks", "DDNS Activities", "Multicast", "PPPoE" oder auch "VoIP". In der Syslog-Konfiguration lässt sich noch ein externer Syslog-Host definieren und das

kommen und die Reports-Sektion ermöglicht das Erstellen von Berichten, beispielsweise zur Bandbreitennutzung nach IP-Adressen oder nach Diensten.

Der Test

Im Test richteten wir die NSA 240 als unseren Internet Gateway ein, aktivierten alle Security Funktionen und stellten das Betriebsniveau auf "maximale Sicherheit". Anschließend betrieben wir das Gerät mehrere Wochen lang als Web-Zugangslösung, um festzustellen, wie es sich bei der alltäglichen Nutzung verhielt. Dabei kam es zu keinen Schwierigkeiten, es war nur ab und an erforderlich, den Content Filter umzukonfigurieren, da er manche Webseite blockierte, die wir zur Arbeit benötigten. Das ist aber nichts ungewöhnliches.

Fazit

Unter dem Strich hinterließ die Sonicwall-Lösung einen guten Eindruck. Das Konfigurationsinterface ist übersichtlich und hilft den Administratoren trotz des großen Funktionsumfangs dabei, den Überblick zu behalten. Auch die Hilfefunktion, die sehr ausführlich und umfangreich gestaltet wurde, konnte im Test überzeugen. Was die Performance im laufenden Betrieb angeht, so ergaben sich keine negativen Überraschungen. Das Produkt gilt dank seiner Multi-Prozessor-Technik sogar als besonders leistungsstarke UTM in ihrem Segment. Damit können wir die NSA 240 als absolut empfehlenswert einstufen.

