

Netzwerkrouter mit UMTS-Failover

Dr. Götz Güttich

Eigentlich stellt der Sonicwall TZ 190 viel mehr als nur einen Netzwerkrouter mit UMTS-Failover dar. Das Produkt verfügt nämlich auch über einen eingebauten, verwaltbaren Switch mit acht Ports, Firewall-Funktionalitäten und diverse andere Sicherheitsfunktionen, die teilweise – wie beispielsweise der Viren- und der Spyware-Schutz – optional sind. Wir haben im Testlabor des IAIT sämtliche Funktionen der Lösung unter die Lupe genommen.

Die Sicherheitsappliance "TZ 190" von Sonicwall lässt sich verhältnismäßig einfach in Betrieb nehmen. Es genügt, eine PCMCIA-basierte UMTS-Karte in das Gerät einzustecken, das Gerät über einen seiner Switch-Ports mit dem LAN zu verbinden und die WAN-Schnittstelle an ein DSL-Modem oder einen vergleichbaren Kommunikationsport anzuschließen. Daraufhin lässt sich das Produkt hochfahren. Der Hersteller empfiehlt allerdings, zuerst die verwendete UMTS-Karte in einem Notebook soweit vorzukonfigurieren, dass sie dazu in der Lage ist, eine Verbindung zum Internet aufzubauen, da es keine Möglichkeit gibt, an der Konfiguration dieser Karte etwas zu ändern, solange sie sich in der Appliance befindet.

Erstkonfiguration

Da die Lösung werksseitig mit der Default-IP-Adresse 192.168.168.168 ausgeliefert wird, müssen die Administratoren zuerst dafür sorgen, dass ihre Konfigurationsworkstation mit dem Produkt kommunizieren kann. Das lässt sich entweder über eine Route oder über das Verschieben des entsprechenden Clients in das angesprochene Subnetz erreichen. Danach können sich die Verantwortlichen über einen



Browser mit der Appliance verbinden. Sobald dies geschehen ist, startet ein Setup-Wizard. Um diesen anzuzeigen, sollte der Browser des Konfigurationsclients allerdings Popups zulassen. Der Wizard fragt nun zunächst nach einem Passwort, um den Zugriff auf die Appliance abzusichern. Dieses Vorgehen gilt als vorbildlich, da es von Anfang an verhindert, dass irgendwelche Router mit Standardpasswörtern im Netz zum Einsatz kommen. Danach geht es an die Konfiguration der Zeitzone und der WAN-Anschlüsse. Dabei ist es möglich, den Internet-Zugang entweder über den regulären WAN-Port zu realisieren oder über das "Wireless WAN" (WWAN), in unserem Test war das der UMTS-Zugang. Als dritte Option können sich die Verantwortlichen dafür entscheiden, das WWAN als Ersatzzugang zu nutzen, wenn der kabelgebundene WAN-Port ausfällt (Failover). Diese Funktion ist mit Sicherheit für sämtliche Netzwerke mit Hochverfügbarkeitsansprüchen an die Internetverbindung

von sehr großem Nutzen. Danach kommt die Konfiguration des WWAN-Zugangs an die Reihe, hier genügt es, das Land, in dem das Produkt betrieben werden soll auszuwählen. Die wesentlichsten Provider der betroffenen Region wurden bereits vordefiniert und stehen dann zur Selektion zur Verfügung (für Deutschland sind das T-Mobile, Vodafone, E-Plus, O2 und Quam). Sollte sich der gewünschte Provider nicht in der Liste finden, lässt sich der Zugang selbstverständlich auch manuell einrichten. Sobald die zur WWAN-Konfiguration erforderlichen Angaben vorgenommen wurden, fragt der Wizard noch nach einer LAN-IP-Adresse, zeigt eine Zusammenfassung der angegebenen Parameter an und führt dann die gewünschten Änderungen durch. Danach ist die Erstkonfiguration abgeschlossen und die Lösung gibt noch eine Meldung aus, dass sich die zuständigen IT-Mitarbeiter unter der neuen IP-Adresse wieder mit dem Produkt verbinden können.

Verwaltung im laufenden Betrieb

Nach dem Abschluss des Setup-Wizards sollten sich die Administratoren zunächst beim Konfigurationsinterface der Appliance einloggen und dort unter "Network/Interfaces" die Zugangsdaten für den kabelgebundenen Internet-Anschluss angeben. Hierbei unterstützt der TZ 190 neben PPPoE auch eine statische WAN-IP-Adresse, Adresszuweisungen via DHCP sowie L2TP und PPTP. Nach dem Abschluss der Konfiguration der Internet-Zugangsdaten ist das Gerät betriebsbereit und ermöglicht in der Standardeinstellung Internet-Zugriffe, bei denen aller ausgehende Verkehr erlaubt und alle eingehenden Verbindungen untersagt sind.

An dieser Stelle ist es sinnvoll, zunächst auf die Konfigurationsoptionen einzugehen, um so den Leistungsumfang der Appliance deutlich zu machen. Nach dem Login findet sich der Administrator in einem übersichtlich gestalteten Konfigurationswerkzeug wieder, das auf der linken Seite eine Menüzeile enthält, die zu den einzelnen Funktionen verzweigt. Selektiert er den ersten Punkt "System", so erhält er zunächst eine Statusseite, die Systemmeldungen sowie -informationen (wie Firmware-Version, Speicher oder Uptime) enthält und Aufschluss darüber gibt, welche der optionalen Sicherheitsdienste aktiv sind. Darüber hinaus zeigt sie die letzten Alert-Meldungen und den Status der einzelnen Netzwerkinterfaces an. Die Systemmeldungen enthalten manchmal recht interessante Informationen, denn sie machen die zuständigen Mitarbeiter beispielsweise aufmerksam, wenn eine Konfiguration des Routers

The screenshot displays the SonicWall Administration web interface. The main content area is titled "System > Status". It features several panels:

- System Messages:** A warning message: "WARNING: A rule exists allowing HTTP/HTTPS management from the WAN. This is a potential vulnerability. Choose a good password." and a note: "Log messages cannot be sent because you have not specified an outbound SMTP server address."
- System Information:** Details for the TZ190 Enhanced device, including Model, Serial Number, Authentication Code, Firmware Version, ROM Version, CPU usage, Total Memory, System Time, Up Time, Current Connections, Last Modified By, and Registration Code.
- Security Services:** A table showing the status of various services: Nodes/Users (Licensed, Unlimited Nodes), VPN (Licensed), Global VPN Client (Licensed, 2 Licenses (0 in use)), CFS (Content Filter) (Licensed), Client AV Enforcement (Licensed), Gateway Anti-Virus (Licensed), Anti-Spyware (Licensed), Intrusion Prevention (Licensed), E-Mail Filter (Licensed), and ViewPoint (Licensed).
- Latest Alerts:** A table of recent alerts with columns for Date/Time and Message. Alerts include WLB Resource availability, WAN auto-dial failure, WLB Resource failure, SonicWALL activation, and WAN Dial-up failure.
- Network Interfaces:** A table showing the status of LAN (LAN), WAN (WAN), OPT (Unassigned), and WWAN (WAN) interfaces, including their IP addresses and link statuses.

The status bar at the bottom indicates "Status: The configuration has been updated." and "Fertig".

Die Übersichtsseite des TZ-190-Konfigurationswerkzeugs

über den WAN-Port möglich ist, da dies ein potentielleres Sicherheitsrisiko darstellen kann.

Unter "Lizenzen" geben die Administratoren die vorhandenen Lizenzen an. Gleichzeitig ermöglicht dieser Unterpunkt auch den Zukauf der bereits erwähnten optionalen Dienste wie Anti-Virus, Mail-Filtering, Anti-Spyware und anderes. Unter "Administration" legen die Mitarbeiter der IT-Abteilung im Gegensatz dazu den Device-namen fest und setzen das Passwort, die Länge des Idle-Timeouts sowie die Zugriffsmöglichkeiten auf die Appliance. Neben dem Web-Interface verfügt die Lösung unter anderem über einen SSH-Server und unterstützt die Kommunikation via SNMP.

Die nächsten Funktionen in diesem Bereich sind schnell erklärt, denn sie befassen sich mit der Verwaltung der Zertifikate (einschließlich des Erstellens eines Signing-Requests), der Konfiguration der Zeiteinstellungen

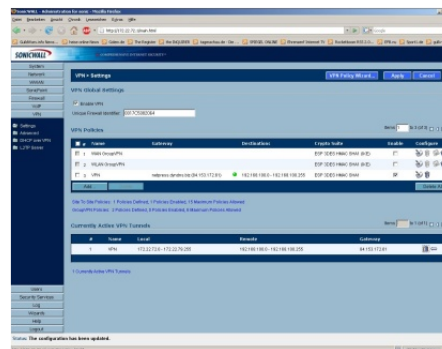
(mit Zeitzone und NTP-Server) und der Definition der Zeiträume für den Scheduler. Mit deren Hilfe unterscheidet die Appliance beispielsweise zwischen Arbeits- und Freizeit und setzt auf Wunsch für die jeweiligen Zeiträume spezielle Policies in Kraft. Unter "Settings" lassen sich die Konfigurationseinstellungen im- und exportieren, gleichzeitig ist es hier auch möglich, Firmware-Updates durchzuführen. Dazu müssen die Verantwortlichen die Firmware zunächst von ihrem lokalen Rechner auf die Appliance hochladen. Daraufhin bietet diese die verfügbaren Firmware-Versionen in einer Liste an und ermöglicht einen Neustart entweder mit der alten oder der neuen Firmware. Dabei sind die zuständigen Mitarbeiter gleichzeitig dazu in der Lage, die Appliance auf Default- oder auf vorher abgespeicherte Backup-Settings zurückzusetzen. Im Test führten wir Firmware-Upgrades von Version 3.6.0.0 auf Version 3.6.0.1 und später auf Version 3.6.0.2-28e durch und behielten während dieser

Vorgänge sämtliche Konfigurationseinstellungen bei. Dabei traten keinerlei Probleme auf. Das System wartet sogar mit dem erneuten Login nach dem Reboot solange, bis die Appliance den Startvorgang abgeschlossen hat. Auf diese Weise kommt es zu keinen Timeout-Meldungen im Browser und der ganze Vorgang hinterlässt einen sehr runden Eindruck.

Funktionen zum Aktivieren des so genannten FIPS-Mode, der eine Compliance zu den Sicherheitsbestimmungen nach FIPS 140-2 garantiert, zum Neustart der Lösung und zur Diagnose schließen den Leistungsumfang des System-Menüs ab. Zu den Diagnosewerkzeugen gehören ein Monitor für aktive Verbindungen, ein DNS-Lookup-Tool, eine Anzeige der CPU-Last sowie eine Find-Path-Funktion, die angibt, ob sich das Suchziel im LAN befindet und welche MAC-Adresse es hat. Darüber hinaus steht noch ein Paket-Trace-Werkzeug zur Verfügung. Dieses bietet unter anderem diverse Filterfunktionen, die sich auf die Aufzeichnung und die Anzeige der Pakete anwenden lassen und die es folglich ermöglichen, beispielsweise nur den Verkehr zwischen bestimmten Hosts mitzuschneiden. Sämtliche Paketdetails sind darstell- (auch als HEX-Ansicht) und archivierbar. Funktionen zum Pingen, ein Prozess Monitor, ein Real Time Blacklist Lookup, ein Traceroute-Befehl, eine Reverse Name Resolution und eine Anzeige der Webserver-Auslastung tragen das ihrige dazu bei, dass der Administrator beim Umgang mit der Appliance über nichts im Unklaren gelassen wird. Treten irgendwelche Schwierigkeiten auf, so

können die User an gleicher Stelle Reports für den technischen Support von Sonicwall erstellen, die Auskünfte über VPN-Keys, den ARP-Cache, die DHCP-Bindings und den IKE-Status geben.

Der zweite Hauptpunkt "Network" übernimmt – wie bereits angesprochen – die Konfiguration der Interfaces, also LAN, WAN, WWAN (einschließlich Failover) und OPT. OPT wurde



Unter den VPN-Settings findet sich auch eine Aufzählung der gerade aktiven VPN-Tunnel

vom Hersteller dazu vorgesehen, eine DMZ einzurichten, WLAN-Komponenten einzubinden und vergleichbare Subnetze mit speziellen Sicherheitsanforderungen zu realisieren. An gleicher Stelle lässt sich auch die WWAN-Verbindung jederzeit abbrechen oder wiederherstellen. Darüber hinaus haben die Administratoren hier Gelegenheit, das so genannte Port Shield Interface einzurichten. Damit lassen sich die acht LAN-Switch-Ports in unterschiedliche Sicherheitszonen aufteilen, die voneinander jeweils durch eine Packet-Inspection-Firewall getrennt sind. Außerdem zeigt das System noch Verkehrsstatistiken mit den über die einzelnen Interfaces gelaufenen Paketen an.

Abgesehen von diesen ganzen Funktionen dient der Netzwerk-Konfigurationspunkt noch zum

Konfigurieren der Verbindungen über die einzelnen Switch-Ports (mit Parametern wie Vollduplex, Halbduplex und Auto-Negotiation), zum Einrichten des Load-Balancings zwischen einen vorhandenen WAN-Interfaces, zum Einstellen der Monitoring-Funktionen für die WAN-Verbindungen und zum Einrichten der Zones. Mit Hilfe dieser Funktion lassen sich bestimmte Schnittstellen bestimmten Zonen zuordnen, die die Administratoren dann wiederum mit Sicherheitstypen wie Trusted, Untrusted, Public, Encrypted und Wireless verknüpfen. Ein "Interface Trust"-Feature sorgt auf Wunsch dafür, dass in Zonen mit mehreren Interfaces alle Rechner aus allen angeschlossenen Netzen miteinander kommunizieren können. Darüber hinaus lassen sich auf Zonenbasis auch Sicherheitsfunktionen wie Content Filtering, Client-Anti-Virus, Gateway-Anti-Virus, Anti-Spyware oder auch Intrusion Protection aktivieren.

Damit sind die Parameter, die die Administratoren bei der Konfiguration der TZ 190 modifizieren können, aber noch lange nicht abgeschlossen. Es folgen noch die Einstellungen für die DNS-Server, das Routing, die ARP-Einträge, der Konfigurationsdialog für den DHCP-Server und die IP-Helper-Funktion, die das Weiterleiten von DHCP-Anfragen an einen zentralen DHCP-Server übernimmt. Der Einsatz der letztgenannten Funktion ergibt vor allem in Umgebungen mit VLANs Sinn, in denen nicht an jedem Interface ein DHCP-Server hängt. Dazu kommen noch ein Web-Proxy, ein Konfigurationsdialog für NAT-Policies, in dem die Verant-

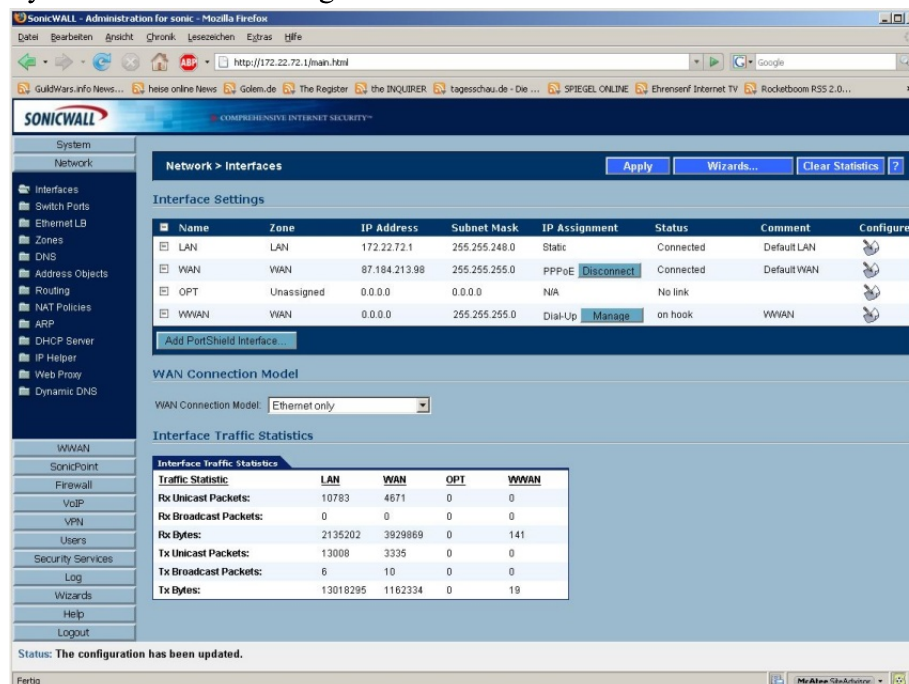
wortlichen den Verkehrsfluss von innen nach außen und zwischen den einzelnen Interfaces steuern können (dieser Punkt macht auch ein Portforwarding möglich), die DynDNS-Konfiguration und ein Bereich zum Festlegen von "Address Objects". Die letztgenannten Objekte können beispielsweise LAN- oder WAN-Subnetze sein, es kann sich dabei aber auch um WAN-Management-IP-Adressen, WLAN-Interfaces, Gateways sowie User-White- oder User-Black-Lists handeln. Sämtliche hier definierten Geräte und Parameter lassen sich auch in Gruppen zusammenfassen und die Objekte und Objektgruppen kommen dann bei der Definition der Firewall-Regeln zum Einsatz (dazu später mehr).

Unter "WWAN" zeigt die Appliance zunächst die Aktivität und Signalstärke der drahtlosen WAN-Schnittstelle an. Außerdem haben die zuständigen Mitarbeiter an dieser Stelle Gelegenheit, zu definieren, wenn das System eine Verbindung aufbau-

en soll – zum Beispiel bei ausgehenden NTP-Paketen. Das sogenannte Interface Monitoring überprüft durch ständige Kontaktaufnahmen zu "responder.global.sonicwall.com", ob die Appliance online arbeitet und eine Konfiguration des User- und Management-Logins schließt den Leistungsumfang dieses Unterpunkts ab. Dabei lässt sich unter anderem festlegen, dass das Produkt Login-Versuche via HTTP automatisch auf das sicherere HTTPS umleitet. Ansonsten sind in diesem Bereich noch der Punkt zur Konfiguration der Verbindungsprofile mit Service-Provider, Einwahlnummer und einer Option zum Limitieren der zu übertragenen Daten sowie die Statistik zur Datennutzung von Interesse. Weiter geht es unter "SonicPoint" mit einem Dialog zum Einbinden der SonicPoint genannten WLAN-Access-Points in die Konfiguration der Appliance. An dieser Stelle findet sich auch ein Intrusion Detection System zum Aufspüren von Rogue Access Points.

Interessanter ist die nun folgende Firewall-Konfiguration, denn sie wurde vom Hersteller sehr gut gelöst. Unter "Access Rules" findet der Administrator eine Tabelle, die übersichtlich in Matrixform anzeigt, welche Regeln für welche Verkehrsrichtungen zwischen LAN, VPN und WAN zulässig sind. Wer einen traditionelleren Ansatz zur Firewall-Konfiguration bevorzugt, hat auch die Möglichkeit, die Regeln nach Zonen sortiert oder in einer Liste anzuzeigen. Die Regeldefinition selbst erfolgt nach Aktion (Allow, Deny, Discard), der Zone, dem Dienst (hier hat Sonicwall bereits alle wesentlichen Services vordefiniert), Quelle, Ziel (jeweils nach den bereits erwähnten definierten Netzwerkobjekten), zugelassenen Benutzern und den Zeiträumen, zu denen die Regel gültig sein soll. Darüber hinaus stehen Optionen zum Logging, zum Festlegen der Quality of Service und zum Zulassen fragmentierter Pakete zur Verfügung. Unter "Advanced" lassen sich unter anderem noch weitere Features wie "Stealth Mode" oder "Decrement IP TTL for forwarded Traffic" modifizieren, Checksummen für TCP/IP-Header und UDP-Pakete erzwingen beziehungsweise dynamische Ports für Oracle, Windows Messenger und RTSP-Transformationen festlegen.

Die "TCP-Settings" umfassen im Gegensatz dazu umfassende Verkehrsstatistiken mit Verbindungen, Paketen, Syn-Floods etc. sowie die eigentlichen "TCP-Settings", mit denen sich zum Beispiel die Einhaltung der durch die RFCs 793 und 1122 gestellten Anforderungen erzwingen lässt. Außerdem bietet



In der Interface-Übersicht der Netzwerkkonfiguration lassen sich die einzelnen Verbindungen konfigurieren

das Produkt Syn-Flood-Protection auf Layer 2 und 3 sowie die Option, einen Syn-Proxy zu nutzen, falls ein Angriff erwartet wird. Punkte zum Definieren zusätzlicher Services nach Name, Protokoll (TCP/IP, UDP, GRE, ESP, L2TP etc.) und Ports sowie eine Multicast-Konfiguration mit Multicast Policies und Multicast Snooping (Data Forwarding) schließen – gemeinsam mit einem Verbindungsmonitor – den Konfigurationsbereich für die Firewall ab.

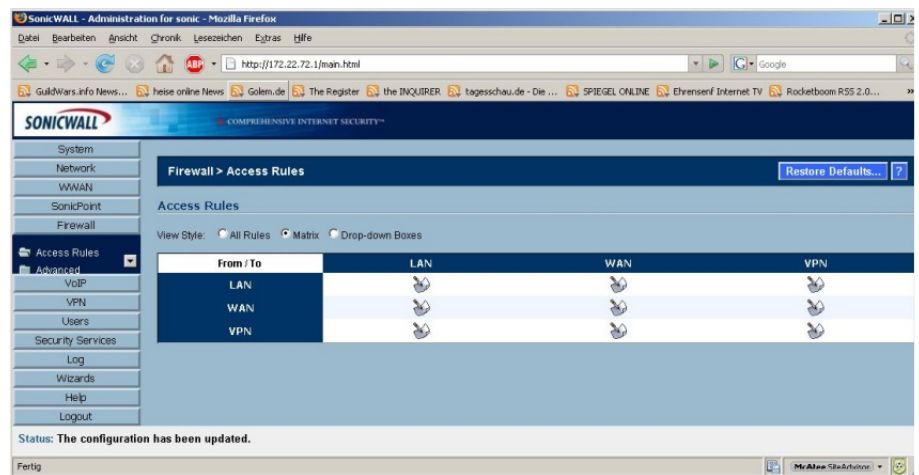
Die nächsten Hauptpunkte umfassen die VoIP-Konfiguration (mit Einstellungen zu SIP und H.323), die VPN-Einstellungen und die Benutzerverwaltung. Bei der Einrichtung von VPN-Tunneln ergibt es Sinn, zunächst mit dem dafür vorgesehenen Wizard die Grundeinstellungen vorzunehmen und dann im VPN-Konfigurationsdialog nachzuarbeiten. Hier lassen sich Unique Identifier vergeben, VPN-Policies wie IKE mit Preshared Key oder VPN-Tunnel mit zertifikatsgebundener Authentifizierung einrichten, NetBIOS-Broadcasts definieren und Einstellungen zur Kommunikation mit einem VPN-Client festlegen (Sonicwall bietet seinen Kunden zum Einbinden einzelner Arbeitsplätze selbst eine entsprechende Software an). Zudem zeigt das Konfigurationswerkzeug an dieser Stelle die aktiven VPN-Tunnel an und bietet eine Dead-Peer-Detection sowie eine Funktion zum Übertragen von DHCP-Informationen via VPN. Die Benutzerverwaltung ermöglicht im Gegensatz dazu zum einen die Anzeige der Benutzeraktivitäten, zum anderen das Anlegen von Benutzerkonten und Gruppen beziehungsweise die Konfiguration der

Zusammenarbeit mit Authentifizierungsservern (Radius, LDAP, etc.). Die lokalen Konten lassen sich nicht nur mit einem Login-Namen und einem Passwort versehen, sondern auch mit einem Kommentar, bestimmten Gruppenzugehörigkeiten und dem Recht, VPN-Zugriffe durchzuführen. Dazu kommen noch so genannte Gastkonten mit beschränkter Lebensdauer, die sich auf Wunsch auch automatisch anlegen lassen. Diese dienen dazu, externen Nutzern auf unkomplizierte Weise einen temporären Netzwerkzugang zu ermöglichen. Die letzten beiden Konfigurationspunkte des Hauptmenüs befassen sich mit Sicherheitsdiensten und Logs. Zu den Sicherheitsdiensten, die – wie bereits gesagt – zum größten Teil getrennt zu lizenzieren sind, gehören ein Content Filter mit Filterlisten, Keyword-Blocking und der Fähigkeit, aktive Inhalte wie Java, ActiveX und ähnliches auszufiltern. Surft ein Anwender eine zu blockierende Seite an, so gibt das System eine frei definierbare

Ebenfalls von Interesse ist die Gateway Antivirus-Funktion. Diese überwacht wahlweise den TCP-Stream oder HTTP-, FTP-, IMAP-, SMTP- beziehungsweise POP3-Verkehr. Auf Wunsch lässt sich zudem die Übertragung passwortgeschützter ZIP-Dateien, mit Makros versehener Office-Files und gepackter ausführbarer Dateien unterbinden.

Das integrierte Intrusion Prevention System erkennt wahlweise Angriffe mit hoher, mittlerer und niedriger Priorität. Darüber hinaus steht auch eine Exclusion-Liste zur Verfügung.

Zu den weiteren Sicherheitsfunktionen gehören ein Feature zum Durchsetzen von Antiviren-Policies auf den Clients (mit Updates) und eine Anti-Spyware-Lösung, die genau wie das Gateway-Anti-Virus-Tool HTTP-, FTP-, IMAP-, SMTP- und POP3-Verkehr überwacht und sich so konfigurieren lässt, dass sie Spyware mit hohem, mittlerem oder niedrigem Gefahrenpotential auf-



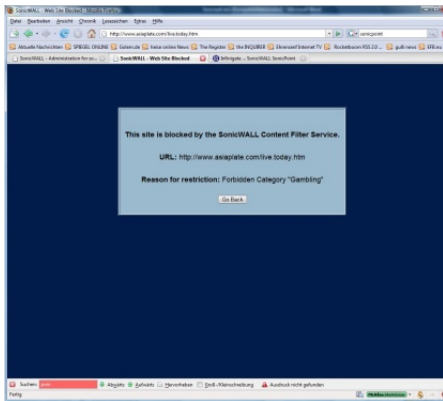
Übersichtlich: Die Firewall-Konfiguration in Matrixform

Meldung aus, etwa "Diese Seite wurde vom Content-Filter-System geblockt". Abgesehen davon ist der genannte Filter dazu in der Lage, die maximale Webnutzung einzugrenzen.

spürt. Auch hier gehört eine Exclusion-Liste zum Leistungsumfang.

Last but not least erhöhen noch zwei weitere Filter das Si-

cherheitsniveau: Der E-Mail-Filter ist dazu in der Lage, eingehende Attachments zu deaktivieren beziehungsweise zu



Der Content-Filter in Betrieb

löschen und der RBL-Filter aktiviert das Blocken von Datenübertragungen mit Hilfe von Real-Time-Block-Lists. Diese Listen lassen sich auf Wunsch von den Administratoren einbinden, bereits vordefiniert wurden die Dienste sbl-xbl.spamhaus.org und dnsbl.sorbs.net.

Die bereits erwähnte Logging-Funktion kommt mit einer Filterfunktion, die es ermöglicht, nur bestimmte Kategorien wie Alarme beziehungsweise Systemfehler oder nur bestimmte Datenübertragungen – die beispielsweise von genau festgelegten IP-Adressen stammen – anzuzeigen. Die Log-Dateien lassen sich auch exportieren und per Mail verschicken. Dazu kommen noch die allgemeinen Syslog-Einstellungen und eine Funktion, die die Logs zu bestimmten Zeit an definierte E-Mail-Adressen sendet. Letztere unterstützt bei der Authentifizierung leider nur POP vor SMTP und keine "echte" SMTP-Authentifizierung, weswegen sie mit einigen Mail-Servern nicht zusammenarbeitet. Von den gesammelten Daten lassen sich auch Reports erstellen, zum Bei-

spiel über die Nutzung der Dienste und die Website-Hits.

Für das Setup der Appliance mit WAN-Zugriff, die VPN-Konfiguration und das Bereitstellen eines internen Dienstes nach außen via Port-Forwarding stellt Sonicwall zusätzlich zu den bereits genannten Konfigurationsoptionen noch spezielle Wizards zur Verfügung. Das gleiche gilt für die Port-Shield-Interfaces, also für die Konfiguration des integrierten verwaltbaren LAN-Switches.

Im Test

Nachdem wir die Lösung so konfiguriert hatten, dass sie den Schutz unseres Netzwerks übernehmen konnte, gingen wir zum Produktivbetrieb über. Dabei fiel zunächst auf, dass die integrierte Hilfefunktion zwar gut und nützlich ist, leider aber noch nicht für alle Funktionen zur Verfügung steht. Es bleibt zu hoffen, dass der Hersteller die noch fehlenden Teile bald ergänzt.

Eine der interessantesten Funktionen des TZ 190 ist sicher der WWAN-Failover. Deswegen haben wir diesem im Test ein besonders großes Augenmerk gewidmet. Der Failover selbst funktionierte ohne Schwierigkeiten. Nachdem wir zu diesem positiven Ergebnis gekommen waren, machten wir uns daran, zu prüfen, wie gut sich ein UMTS-Zugang für die Arbeit eines ganzen LANs eignet. Dazu luden wir von einer Workstation aus von einem nahegelegenen FTP-Server eine große Datei herunter, führten auf anderen Rechnern parallel dazu mehrere Windows- und Debian-Linux-Online-Updates durch, setzten ein System ein, um eine Remote-Desktop-Verbindung zu einem externen Host

aufzubauen und verwendeten einige andere Arbeitsstationen, um "normal" im Web zu surfen und E-Mail-Verkehr zu bearbeiten. Dabei ergab sich, dass die UMTS-Geschwindigkeit durchaus ausreicht, ein vernünftiges Arbeiten auch ganzer Workgroups zu ermöglichen. Die Datenübertragungen liefen zwar langsamer als gewohnt, blieben aber trotzdem auf einem Niveau, bei dem die Arbeitsgeschwindigkeit nicht störte. In manchen Fällen wird der Benutzer gar nicht merken, dass es einen WAN-Failover gab, sondern nur vermuten, dass er eine langsame Serververbindung erwischt hat. Etwas anders sieht es bei der Remote-Desktop-Verbindung aus, da die auftretenden Latenzen die Arbeit auf dem entfernten Host doch etwas zäh ablaufen ließ.

Hier gilt nur, dass der Zugriff zwar möglich ist, dass es aber in der Praxis Sinn ergibt, wenn möglich solche Remote-Arbeiten zu verschieben, bis der "normale" Internet-Zugang wieder funktioniert. Da ein LAN in relativ kurzer Zeit einen sehr hohen Datendurchsatz erzeugen kann, empfiehlt es sich übrigens für eine Backup-Verbindung auf WWAN-Basis unbedingt, eine UMTS-Flatrate oder einen Vertrag mit Zeitbeschränkung zu wählen, da ein Volumentarif unter Umständen sehr schnell sehr hohe Kosten verursacht.

VPN-Verbindung

Im nächsten Schritt bauten wir eine Preshared-Key-basierte VPN-Verbindung zu einem Sonicwall Pro 2040 Enhanced auf, also eine LAN-LAN-Kopplung mit Hilfe von IPSec. Hierzu verwendeten wir zunächst den Wizard und passten dann die neu

erstellte Konfiguration manuell an unsere Gegebenheiten an. Der Wizard möchte im ersten Schritt wissen, ob das VPN Site-To-Site laufen soll oder ob es an die Anbindung einer WAN-Group geht. Danach müssen die zuständigen Mitarbeiter noch angeben, wie das VPN heißt, wie der Preshared Key lautet und welche Adresse die Gegenstelle hat (dabei unterstützt das System auch DynDNS-Adressen).

Anschließend definieren die Benutzer noch die Adressbereiche des eigenen und des entfernten Netzwerks und geben die Proposals für die Verbindungsaufnahme an, wie beispielsweise die Diffie Hellman Group sowie die Verschlüsselungs- und Authentifizierungs-Algorithmen. Zum Schluss zeigt der Wizard noch eine Zusammenfassung an und trägt die Konfigurationsänderungen dann ein. Nun passten wir den neuen Eintrag noch manuell im Konfigurationsinterface an die Gegebenheiten des Testlabs an, im Wesentlichen dadurch, dass wir den Modus "IKE using Preshared Keys" auf "Manual Key" umstellten und die Proposals neu vergaben, danach stand die VPN-Verbindung.

Der Test des Gateway-Antivirus-Schutzes brachte ebenfalls keine negativen Überraschungen mit sich. Das System erkannte zuverlässig Testviren – wie beispielsweise Eicar – und filterte die gefährlichen Inhalte aus.

Firewall-Test

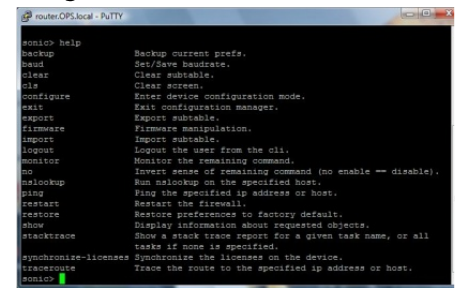
Zum Schluss nahmen wir die in die Appliance integrierte Firewall genauer unter die Lupe. Bei einem Scan mit dem Portscanner Nmap ergaben sich keine Überraschungen – die Lö-

sung behielt sowohl auf dem internen als auch auf dem externen Interface alle relevanten Informationen für sich. Danach setzten wir das Produkt mit Hilfe einiger Hackertools, die wir von einschlägigen Internet-Seiten heruntergeladen hatten, diversen Angriffsszenarien aus. Dabei ergab sich, dass der der TZ 190 einen Großteil der Attacken schadlos übersteht. Nur bei manchen DoS-Angriffen ist eine deutliche Verlangsamung des über die Appliance gerouteten Verkehrs spürbar. Bei einer DoS-Attacke mit einem bestimmten Angriffswerkzeug auf den internen Port lässt sich sogar der gesamte Verkehr zum Stillstand bringen. Das Produkt stürzt dabei allerdings nicht ab und nimmt nach Ende des Angriffs den normalen Betrieb wieder auf. Der Hersteller sagte dazu im Wesentlichen folgendes:

"Bei dem angegebenen Verhalten handelt es sich nicht um ein DoS-Problem. Es handelt sich auch nicht um eine Schwäche des IPS, sondern um irregulären Netzwerkverkehr, der das LAN durchläuft, unseren Validation Code aufruft und so eine hohe CPU-Last erzeugt. Der Grund dafür, dass die Last so hoch geht, ergibt sich daraus, dass der "Angriff" mit Fast-Ethernet-Geschwindigkeit über das LAN-Interface erfolgt. Eine gleichartige Attacke über den WAN-Anschluss – also das Interface das in der Praxis solchen Angriffen mit der größten Wahrscheinlichkeit ausgesetzt ist – würde keine vergleichbaren Auswirkungen haben.

Wer die Behauptung aufstellt, dass es sich dabei um eine Verwundbarkeit handelt, muss sowohl die Parameter und Konditionen des Angriffs, als auch

den Effekt verstehen und sich über alle damit zusammenhängenden Faktoren im Klaren



Die Appliance lässt sich auch via SSH und Kommandozeile bedienen

sein. Der Effekt ist lediglich eine hohe CPU-Last, während das Gerät einem ungültigen (gespoofen) LAN-Verkehr in Fast-Ethernet-Geschwindigkeit beziehungsweise ungültigen TCP-Flags ausgesetzt ist. Die Zahl der Spoofing-Arten, die sich einsetzen lassen, um ungültigen Fast-Ethernet zu erzeugen, der sämtliche Ressourcen konsumiert (CPU oder Netzwerkbandbreite) ist grenzenlos. Das LAN ist eine kontrollierte Umgebung uns sollte auch als solche behandelt werden."

Fazit

Die TZ 190 von Sonicwall stellt eine Sicherheits-Appliance mit einem beeindruckenden Leistungsumfang dar. Nicht nur die integrierten Sicherheitsdienste überzeugen, sondern auch die verhältnismäßig einfache Konfiguration und Administration. Ein besonderes Plus der dem Gerät zur Zeit zu einem gewissen Alleinstellungsmerkmal verhilft, ergibt sich allerdings aus der WWAN-Failover-Funktion. Deren Einsatz ist in sehr vielen Umgebungen sinnvoll, sorgt sie doch für eine hochverfügbare Internetanbindung, ohne dass die Anwender dazu einen zweiten drahtgebundenen Netzzugang bereit halten müssen.