IAITested

Institut zur Analyse von IT-Komponenten
Rotdornstr. 2

41532 Korschenbroich

Im Test: Dell SonicWALL TZ400

Hohe Leistung für kleine Unternehmen

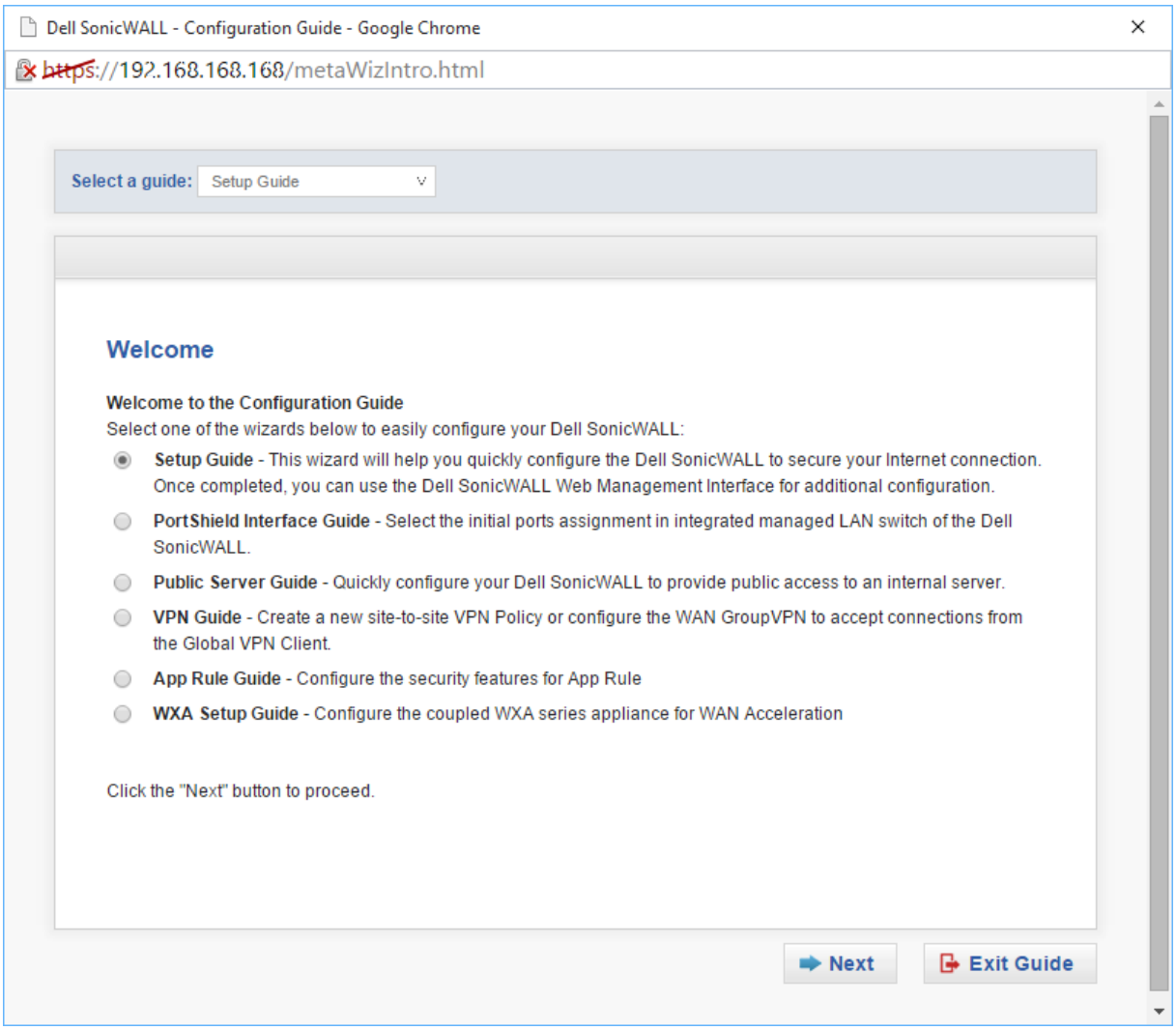
Autor: Dr. Götz Güttich

Mit der TZ400 Network Security Firewall wendet sich Dell vor allem an Home Office-User und kleine Umgebungen. Nach Angaben des Herstellers ist diese Zielgruppe mit der Lösung dazu in der Lage, alle Vorteile von Breitband-Internet-Verbindungen zu nutzen, ohne dabei beim Schutzniveau Kompromisse eingehen zu müssen. Wir haben uns im Testlabor angesehen, wie die Arbeit mit der Dell SonicWALL TZ400 abläuft und was das Produkt leistet.

Dell verfolgt mit der Dell SonicWALL TZ400 das Ziel, auch kleinere Unternehmen mit den Schutzmechanismen auszustatten, die sonst nur in großen Umgebungen Verwendung finden. Da die Lösung auch für den Einsatz in verteilten Umgebungen und entfernten Arbeitsplätzen optimiert wurde, lässt sie sich nicht nur durch das lokale Web-basierte Administrations-Tool verwalten, sondern auch mit Hilfe von SonicWALL GMS von einer zentralen Stelle aus.

Zum Leistungsumfang des Produkts gehört zunächst einmal eine High-Performance Security Engine mit Reassembly-Free Deep Packet Inspection (RFDPI). Diese überwacht den Datenverkehr auf allen Ports in beide Richtungen gleichzeitig ohne dabei Latenzen im Netz zu erzeugen. Die RFDPI normalisiert und entschlüsselt die Datenübertragungen, um Advanced Evasion-Technologien zu neutralisieren, die versuchen, Sicherheitssysteme hinters Licht zu führen und Schadcode in das Netz einzuschleusen. Mit "normalisieren" ist in diesem Zusammenhang gemeint, dass das

System bei Bedarf die Reihenfolge der IP-Pakete korrigiert. Das ist erforderlich, da die Überprüfungen in Echtzeit stattfinden und kein Proxy zum Einsatz kommt. Während der Analysen untersucht die RFDPI sämtliche OSI-Schichten von drei bis sieben. Jedes Paket wird dabei mit drei verschiedenen Signaturdatenbanken abgeglichen und zwar für Angriffe, Malware und Anwendungen. Kommt es zu einer Übereinstimmung zwischen den Signaturen in einer der Datenbanken mit dem untersuchten Paket, so führt die Appliance eine zuvor definierte Aktion aus. Handelt es sich um ankommende Malware, so unterbricht die Firewall die Verbindung, bevor irgendwelche Systeme kompromittiert werden können und loggt das Ereignis. Bei Bedarf lässt sich die Inspection Engine aber auch so konfigurieren, dass sie zum Beispiel nur eine Angriffserkennung ohne Aktion ausführt oder – im Fall der Anwendungserkennung – Bandbreitenmanagementdienste auf Layer 7 für erkannte Applikationen durchführt.



Nach dem ersten Verbindungsaufbau bietet die Appliance den Mitarbeitern eine Vielzahl von Assistenten an

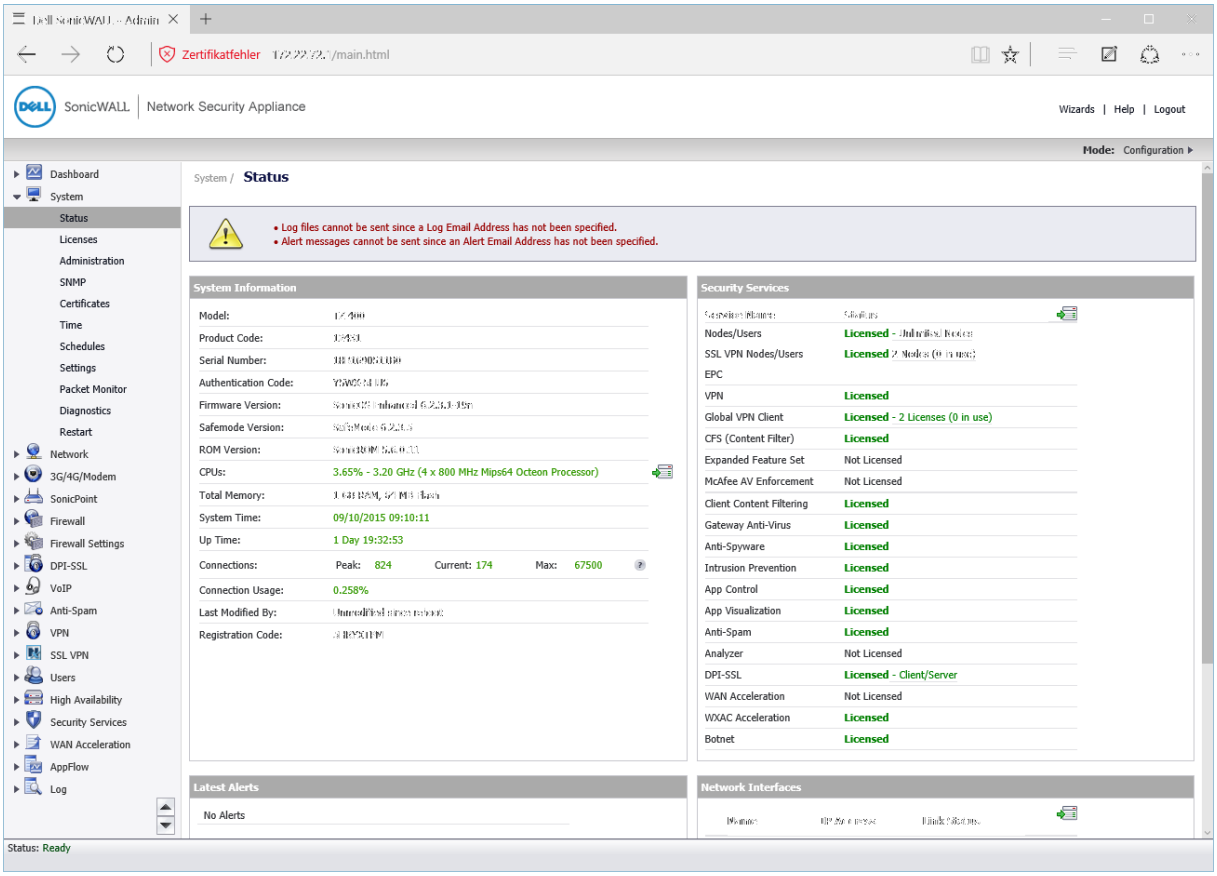
Eine Intrusion Prevention-Funktion (IPS) schützt vor Angriffen auf Applikationsebene und IPSec- sowie SSL-VPNs sorgen für sichere Zugriffe auf die Unternehmensressourcen von außen. Zusätzlich bietet die Appliance auch noch Antivirus- und Anti-Spyware-Features auf Gateway-Ebene zum Blocken von Trojanern, Viren, Keyloggern und ähnlichem. Ein Content/URL-Filter steht ebenfalls

zur Verfügung und viele Wizards helfen den Administratoren bei der Konfiguration und Verwaltung der Appliance.

Darüber hinaus stellt Dell diverse Remote Access-Clients für VPN-Zugriffe auf das System zur Verfügung. Diese arbeiten mit Android-, iOS-, Linux-, MacOS- und Windows-Systemen zusammen.

Die Appliance

Hardware-seitig verfügt die Appliance über eine Vierkern-CPU mit 800 MHz Taktfrequenz (Mips64 Octeon), ein GByte RAM und sieben GBit-Ethernet-Anschlüsse für Kupferkabel. Damit erreicht das Produkt einen Firewall Inspection-Durchsatz von 1300 MBit pro Sekunde. Der Application Inspection-Durchsatz liegt bei 900 MBit pro Sekunde, genau wie der IPS-Durchsatz. Bei Anti-Malware-Inspektionen erreicht die Lösung immer noch einen Throughput von 300 MBit pro Sekunde und bei SSL-Entschlüsselungen und Analysen kommt das Produkt auf 100 MBit pro Sekunde. Der IPSec-Durchsatz beträgt 900 MBit pro Sekunde und die Appliance bietet Unterstützung für 500 Single-Sign-On-Benutzer und 50 VLAN-Interfaces. Support für 3G- beziehungsweise 4G-Komponenten wurde ebenfalls in das Produkt integriert, so dass sich ein alternativer Internet-Zugang einrichten lässt, der zum Einsatz kommen kann, wenn die normale Verbindung ausfällt. Mit den Appliances TZ300 sowie TZ500 und TZ600 bietet Dell bei Bedarf noch weitere Network Security Firewalls für kleinere und größere Umgebungen an, so dass sich die Produkte durchaus in verschiedenen Szenarien einsetzen lassen. In diesem Fall findet zwar eine andere Hardware Verwendung, der Funktionsumfang ist aber bei allen TZ-Modellen gleich. Das vereinfacht die Verwaltung verteilter Installationen, da überall dasselbe Management-Werkzeug zum Einsatz kommt.



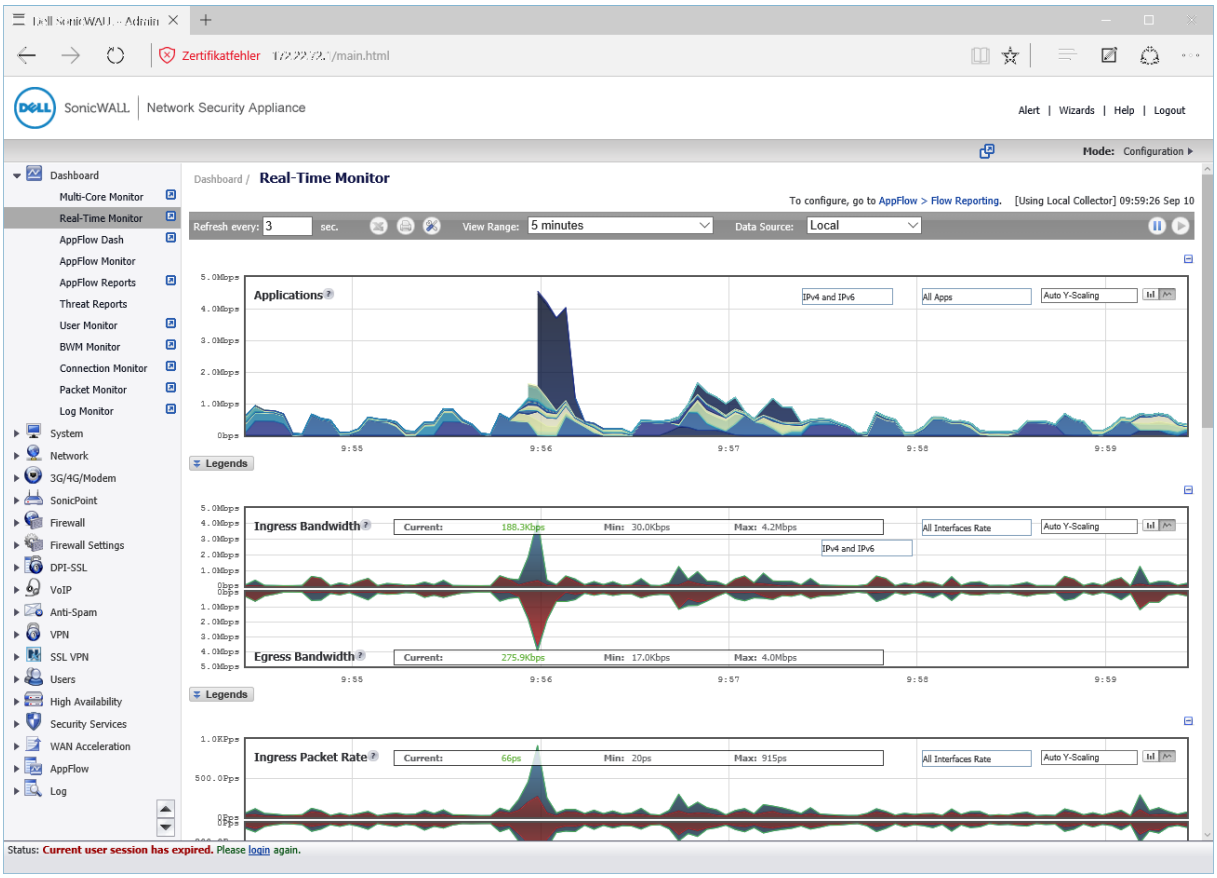
Die Statusübersicht erscheint nach dem Login beim laufenden System

Updates

Um sicher zu stellen, dass die Firewalls stets über die aktuellen Gegenmaßnahmen gegen aktuelle Bedrohungen verfügen, beschäftigt Dell In-House das so genannte SonicWALL Threat Research Team. Dieses Team verwendet mehr als eine Million Sensoren auf der ganzen Welt zum Sammeln von Malware-Samples und von Informationen über die neuesten Bedrohungen. Diese Daten werden ständig in die Intrusion Prevention-, Anti-Malware- und Application Detection-Systeme integriert. Kunden, die eine Dell SonicWALL Firewall einsetzen, erhalten – wenn sie über ein gültiges Abonnement verfügen – rund um die Uhr aktualisierte Daten zum Schutz vor Bedrohungen. Diese Updates sind sofort aktiv, ohne Neustarts der Appliances oder andere Unterbrechungen. Zusätzlich greifen die Firewalls auch noch über das Internet auf den "Dell SonicWALL CloudAV"-Dienst zu, der die Signaturen auf der Appliance nochmals um mehr als 17 Millionen weiterer Erkennungsmuster ergänzt.

Der Test

Im Test integrierten wir die TZ400 als Internet-Gateway in unser Netzwerk und führten die Erstkonfiguration mit dem dafür gedachten Assistenten durch. Anschließend nahmen wir uns das Management-Interface der Lösung vor und untersuchten den kompletten Leistungsumfang des Produkts. Dabei passten wir auch gleich die vom Setup-Wizard vorgenommene Konfiguration im Detail an die Anforderungen in unserem Netz an.

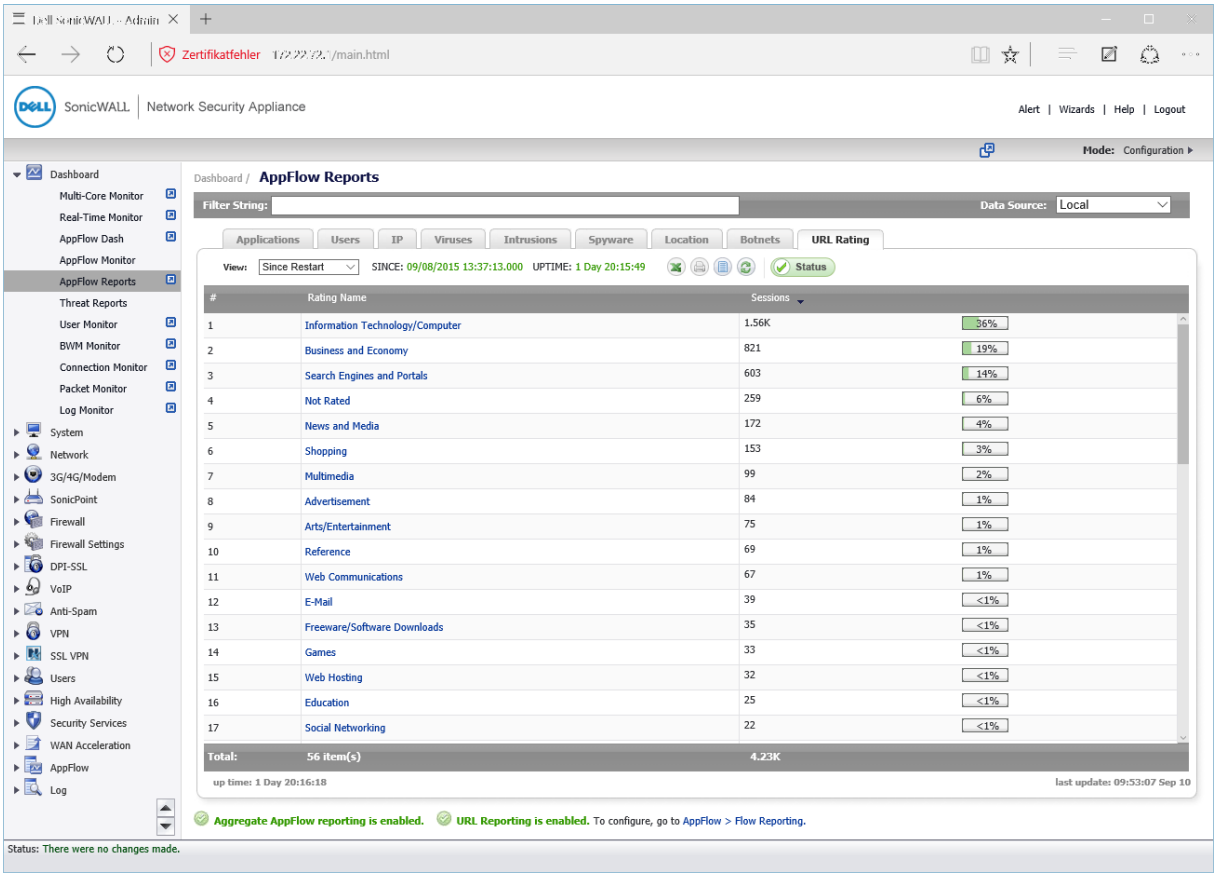


Der Real Time-Monitor gibt Aufschluss über die von der Appliance übertragenen Datenströme

Nachdem alles zu unserer Zufriedenheit lief, verwendeten wir diverse Sicherheitswerkzeuge wie den Portscanner nmap, die Vulnerability-Scanner Nessus und NexPose sowie das Security-Tool Metasploit, um potentielle Bedrohungen beziehungsweise Lücken im System aufzudecken. Darüber hinaus setzten wir auch diverse Angriffswerkzeuge, wie zum Beispiel DoS-Werkzeuge ein, um festzustellen, ob wir die Appliance in die Knie zwingen konnten.

Installation

Nach dem Anschluss des Geräts an unsere Internet-Verbindung und unseren LAN-Switch verschoben wir zunächst einen Client-Rechner in das Subnetz 192.168.168.0, damit wir auf das Web-Interface des Dell-Produkts zugreifen konnten, das standardmäßig über die URL HTTPS://192.168.168.168 erreichbar ist. Dort konnten wir uns dann mit den Default-Credentials "admin" und "password" einloggen. Daraufhin hatten wir Gelegenheit, den eben erwähnten Konfigurationsassistenten zu starten, der den Administratoren dabei hilft, das Produkt in Betrieb zu nehmen. Dieser fragt im ersten Schritt nach einem neuen Passwort für den Administrator-Account. Das ergibt sehr viel Sinn, da auf diese Weise vermieden wird, dass irgendwelche Sicherheitsappliances von Dell SonicWALL mit Standardpasswörtern im Netz online gehen.



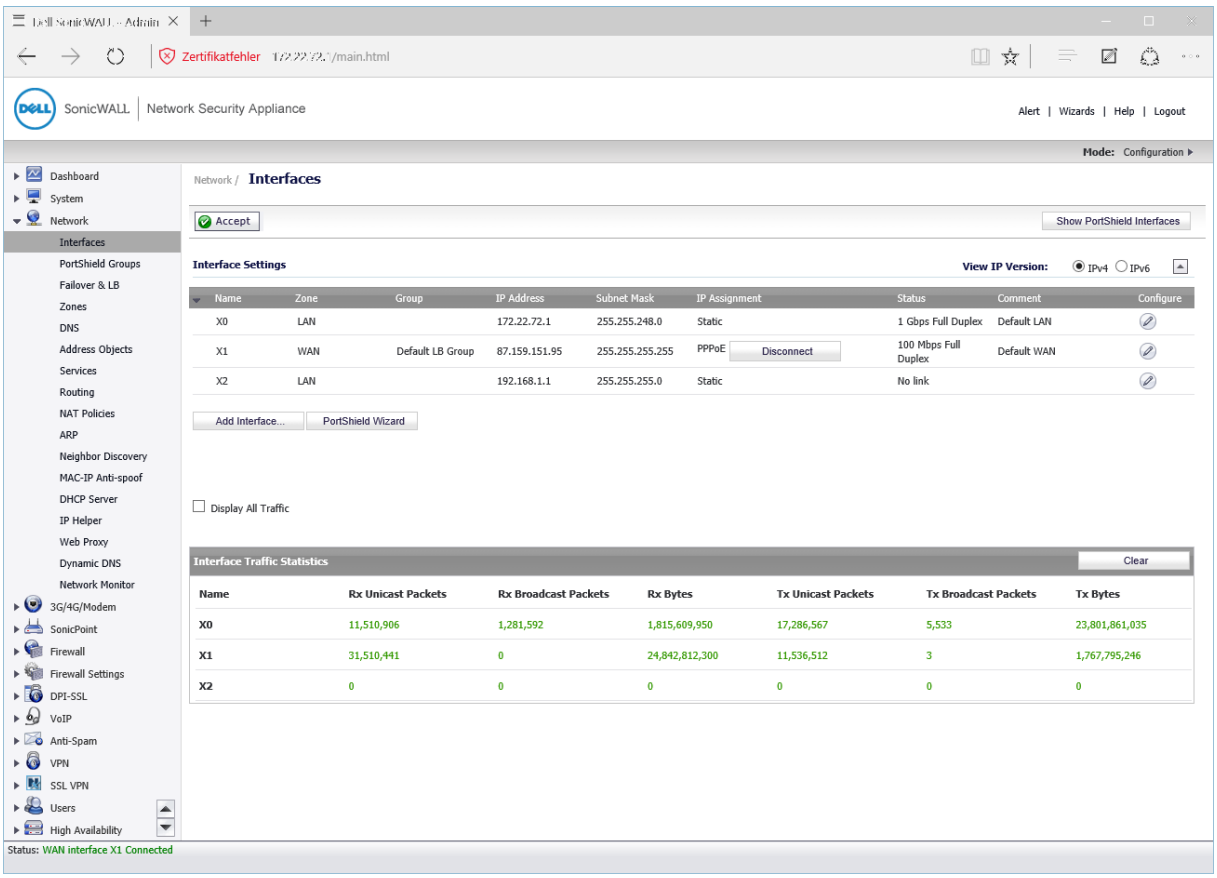
Über die App Flow-Reports finden die zuständigen Mitarbeiter heraus, welche Web-Rubriken am meisten genutzt wurden

Bei den nächsten Schritten geht es an die Konfiguration der Zeitzone und – falls vorhanden – des im USB-Slot befindlichen 3G- oder 4G-Modems. Danach kommt die

Konfiguration des Internet-Zugangs an die Reihe. Bei uns wurde dieser über einen DSL-Anschluss der Telekom realisiert. Die TZ400 erkannte von selbst, dass im Internet ein PPPoE-Server vorhanden war und bot uns den entsprechenden Konfigurationsdialog an. Neben PPPoE unterstützt das Produkt übrigens auch Internet-Verbindungen über statische und dynamische IP-Adressen und PPTP-Connections.

Nachdem wir unsere PPPoE-Zugangsdaten eingetragen hatten fragte uns der Assistent, ob die Appliance auf WAN-Seite auf HTTPS-Anfragen und Pings antworten sollte. Ersteres ist sinnvoll, wenn das Web-Interface über das Internet von außen erreichbar sein muss, letzteres dient zu Diagnosezwecken.

Nach dem Abschluss der WAN-Konfiguration kommen die LAN-Einstellungen mit lokaler IP-Adresse und Netzmaske an die Reihe. Anschließend will der Wizard wissen, wie die sieben Netzwerk-Ports der Appliance Verwendung finden sollen. Dabei haben die Administratoren die Wahl zwischen WAN/LAN-Zuweisungen, WAN/LAN/OPS-Konfigurationen, WAN/LAN/High Availability-Ports oder einer Konfiguration mit WAN und zwei unterschiedlichen LAN-Anschlüssen. Wir entschieden uns im Test für die letztgenannte Option, da wir an einem getrennten Port noch einen separaten WLAN Access-Point für ein Gäste-WLAN anschließen wollen, der ohne Zugriff auf unsere LAN-Infrastruktur arbeitete. Als wir alle Einstellungen vorgenommen hatten, zeigte der Assistent eine Zusammenfassung an und führte die entsprechenden Änderungen durch. Zum Schluss wies er uns noch darauf hin, dass sich die LAN IP-Adresse geändert hatte und gab an, über welche URL wir die Appliance im laufenden Betrieb erreichen konnten.

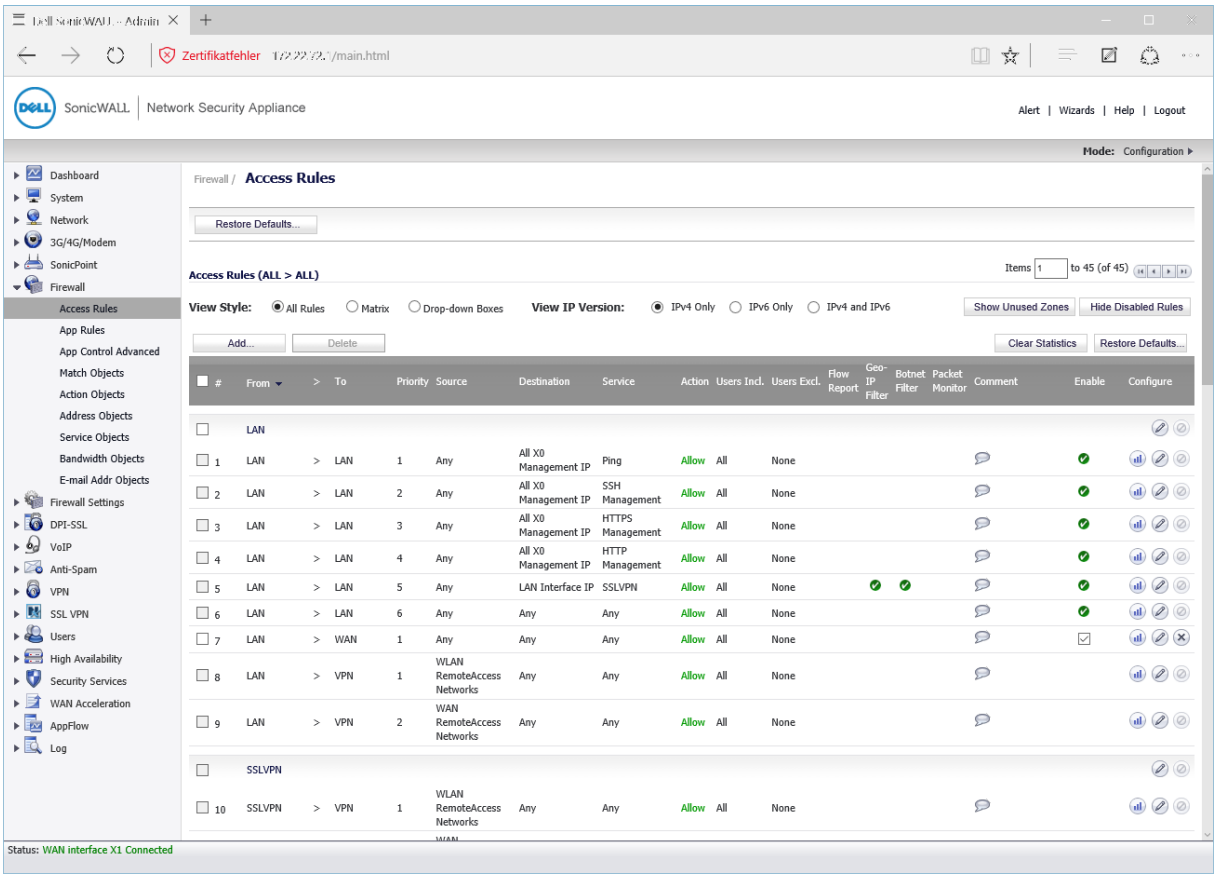


Die Übersicht über die Netzwerkinterfaces

Das Konfigurationswerkzeug

Als wir uns anschließend erneut mit der Appliance verbanden, verlangte das System, dass wir die Lösung in unserem Mysonicwall-Konto, das wird bereits zuvor für einen anderen Test angelegt hatten, registrierten. Danach war das System einsatzbereit und wir konnten uns dem Leistungsumfang der Management-Umgebung zuwenden.

Die Seite, auf der die Administratoren nach dem Login üblicherweise landen, nennt sich Systemstatus. Sie umfasst diverse Informationen zur Appliance selbst, wie Angaben zum Modell, zur Firmware, zu ROM und RAM, zur Systemzeit, zum Prozessor, zu den Verbindungen und ähnlichem. Außerdem zeigt sie – falls vorhanden – eine Liste mit den aktuellen Alarmmeldungen an, informiert die zuständigen Mitarbeiter über den Status der Interfaces und bietet Details zu den lizensierten Diensten wie Gateway-Antivirus, IPS, Anti-Spam und so weiter.

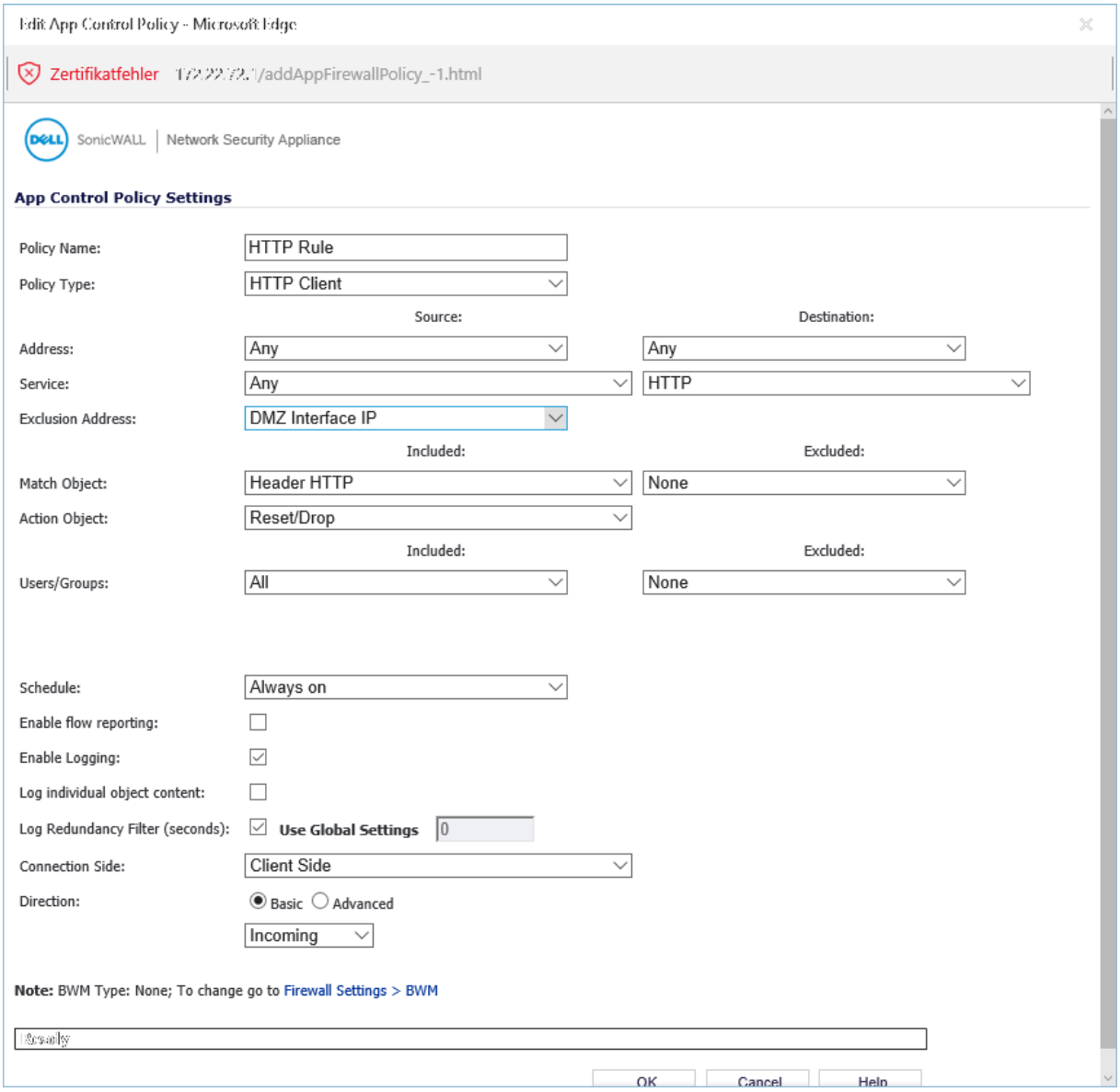


Die Zugriffsregeln der Firewall

Die Administratoren sind über eine Menüstruktur auf der linken Bildschirmseite dazu in der Lage, innerhalb des Konfigurationswerkzeugs zu navigieren. Wechseln sie auf den obersten Eintrag in dieser Menüstruktur, so landen sie im "Dashboard". Dieses enthält diverse Überwachungsfunktionen. Der "Multi Core Monitor" behält die CPU im Auge, während der "Real Time Monitor" den Datenfluss visualisiert. Der "App Flow Dash" bietet im Gegensatz dazu Informationen zu den Top-Anwendungen (DNS, HTTPS, etc.), den Top-Usern, den TOP-Viren und den Top-Intrusions.

Über den "App Flow Monitor" sind die Verantwortlichen dazu in der Lage, genau zu analysieren, welche Protokolle und URLs die Anwender genutzt haben, von welchen IP-Adressen die Anfragen und Antworten kamen und welche Treats dabei auftraten. Der App Flow Monitor umfasst auch Informationen zu VoIP- und VPN-Verbindungen. Alle Daten lassen sich sowohl als Torten- als auch als Liniendiagramm oder auch als Liste visualisieren. Die Benutzer können sämtliche Angaben jederzeit entsprechend ihrer Wünsche filtern. Administratoren haben mit diesem Tool folglich ein sehr mächtiges Werkzeug zur Analyse ihres Datenverkehrs in der Hand.

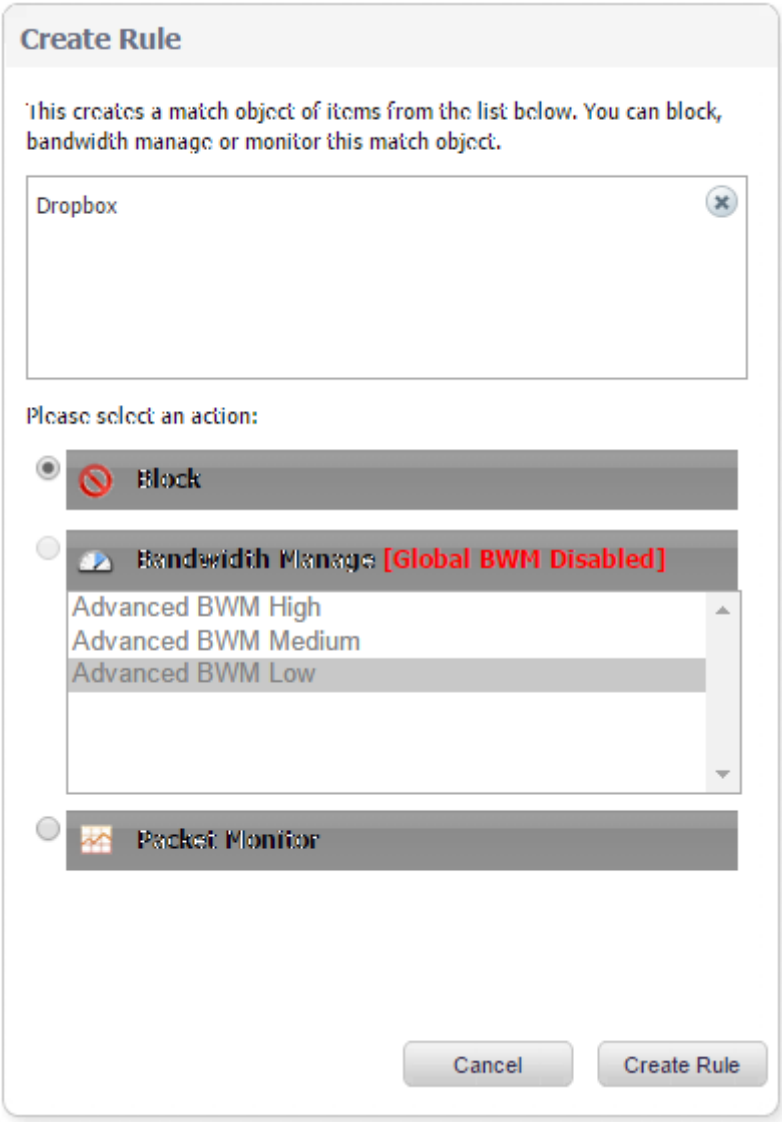
Die "App Flow Reports" liefern Informationen zu Anwendungs-Sessions, Benutzern, IP-Adressen, Viren, Intrusions, Spyware, Botnetzen und Locations. Zu diesen Informationen gehören – je nach Themenbereich – Sessions, übertragene Bytes und vieles mehr. Bei den Locations zeigt das Tool an, welche Web-Adressen in welchen Ländern am meisten besucht worden sind und eine URL-Rating Funktion gibt zudem Aufschluss darüber, auf welche Rubriken (Technologien, E-Mail, New and Media, etc.) die Zugriffe erfolgten.



Eine App Control-Policy mit Typ, Adresse, Dienst, Match Object, Action Object und Benutzern

Bei den "Threat Reports", die global und lokal verfügbar sind, informieren sich die IT-Verantwortlichen über die blockierten Viren, die verhinderten Intrusions sowie unterbundene Spyware- und Multimedia-Übertragungen. Ein "User Monitor" zeigt zudem die eingeloggten Anwender und der "BWM Monitor" präsentiert Details zum Bandbreitenmanagement. Im "Connection Monitor" sehen die zuständigen Mitarbeiter bei Bedarf die aktiven Verbindungen in Listenform ein und der "Packet Monitor" stellt einen Sniffer dar, mit dem sich sämtliche Datenübertragungen mitschneiden und analysieren lassen. Der "Log Monitor", der das Anzeigen und Filtern der Log-Einträge erlaubt, schließt den Leistungsumfang des Dashboards ab.

Unter "System" erfolgt die Verwaltung der Dell-Appliance. Zunächst einmal findet sich hier die eben bereits genannte "Statusübersicht", an gleicher Stelle lassen sich aber auch die Lizenzen verwalten, das Administrator-Passwort ändern, SSH-Zugriffe erlauben, die SNMP-Konfiguration vornehmen, Zertifikate einspielen und die Zeiteinstellungen festlegen. Darüber hinaus definieren die zuständigen Mitarbeiter hier auch Zeitpläne, die beispielsweise Arbeitszeiten von Freizeiten oder dem Wochenende unterscheiden, so dass zu verschiedenen Zeiten unterschiedliche Zugriffsregeln in Kraft treten können. Der Im- und Export der Konfigurationseinstellungen ist ebenfalls unter System möglich, das gleiche gilt für Firmware-Updates und das Aktivieren der FIPS- (Federal Information Processiong Standard) und NDPP-Modi (Network Device Protection Profile). Ein Diagnosemenü mit Werkzeugen wie Ping, Traceroute und vielem mehr rundet den Funktionsumfang der Systemkonfiguration ab.

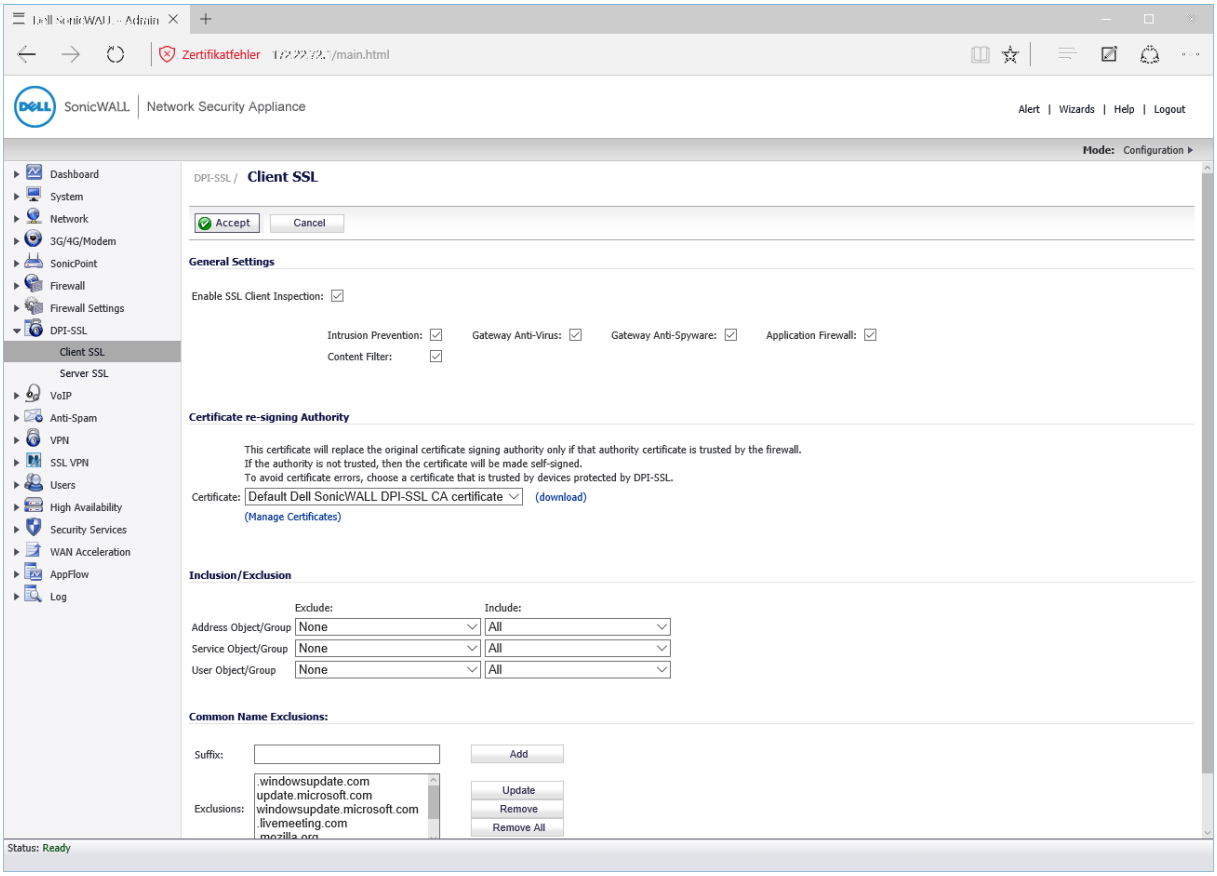


Die Erzeugung einer App Control-Rule direkt aus dem App Flow-Monitor

Bei den Netzwerkeinstellungen nehmen die Administratoren sämtliche Settings für die Netzwerkinterfaces vor. Sie sind beispielsweise dazu in der Lage, einzelne Ports bestimmten Netzen zuzuweisen, Failover und Load Balancing zu konfigurieren und Zonen wie DMZ, LAN, WAN, VPN oder auch WLAN zu verwalten. An gleicher Stelle legen die IT-Verantwortlichen auch die Adressobjekte an. Bei diesen Objekten handelt es sich um Einträge, die bestimmte Komponenten wie Gateways, Netzwerke oder auch Hosts definieren. Sie stellen die Grundlage für die Regeldefinition zur Verfügung. Es gibt auch Objektgruppen wie "All Interface IPs", "Firewalled Subnets" und ähnliches, um die Konfiguration zu vereinfachen und übersichtlicher zu gestalten.

Unter "Services" finden sich im Gegensatz dazu die im Netz eingesetzten Protokolle wie FTP, HTTP und ähnliches. Diese lassen sich auch bearbeiten, anlegen beziehungsweise löschen und auch hier gibt es die Option, Protokolle in Gruppen zusammenzufassen. Dell SonicWALL hat bei den Objekten und Diensten praktisch alles vordefiniert, was für die Regelerstellung erforderlich ist. Meist werden die Administratoren im laufenden Betrieb wohl nur noch einzelne Hosts zusätzlich anlegen müssen. Im Test stellte dieser Vorgang übrigens kein Problem dar.

Die Definition der NAT-Regeln erfolgt ebenfalls im Netzwerkbereich. An gleicher Stelle nehmen die IT-Mitarbeiter auch Einstellungen zum Routing vor, konfigurieren den DHCP-Server und den Web-Proxy, legen die Dyndns-Einstellungen fest und vieles mehr. Es ist sogar möglich, Einträge für ARP, das Network Discovery-Protokoll und ähnliches hinzuzufügen.



Die Konfigurationsseite für die DPI-SLL

Die nächsten Hauptpunkte befassen sich mit der Einrichtung von am USB-Port angeschlossenen 3G- oder 4G-Modems und der WLAN-Konfiguration über Dell SonicWALL Sonicpoint WLAN-Komponenten. Interessanter ist der Bereich "Firewall", denn hier legen die Verantwortlichen die Firewall-Regeln fest und arbeiten mit den Application Rules. Was die Zugriffsregeln angeht, so lassen diese sich über die Aktion (Zulassen, Blocken, etc.), die Quelle des Datenstroms, das Ziel, das Protokoll und die beteiligten Benutzer definieren. Es ist auch möglich, ihnen Funktionen wie "Flow Report", "Geo IP Filter" (dazu später mehr) und "Packet Monitor" hinzuzufügen. Im Test ergaben sich dabei keine Schwierigkeiten und das System verhielt sich wie erwartet.

Die Anwendungsregeln

Die Anwendungsregeln dienen zum Überwachen der Datenströme bestimmter Applikationen wie SMTP, POP3, HTTP und FTP. Ihre Definition erfolgt über Quelle, Ziel und "Match Object". Das Match Object bestimmt, wann eine Regel aktiv wird. Es kann sich dabei um Dateinamen, Cookies, URLs, FTP-Befehle und ähnliches handeln.

Findet die Appliance eine Entsprechung zu einem Match Object im Datenstrom, so führt sie die in der Regel definierte Aktion (Drop, Monitor, etc.) aus.

Für unseren Test definierten wir eine Regel, die den "cd"-Befehl bei FTP-Verbindungen untersagte. Nach der Implementierung dieser Policy gab das System nach der Eingabe von "cd" im FTP-Client aus, dass der Host die Verbindung unterbrochen habe. Die Regel funktionierte also einwandfrei und untersagte den Anwendern das Wechseln der Verzeichnisse auf FTP-Servern. Da sich die Applikation-Rules sehr genau an die Anforderungen der jeweiligen Umgebung anpassen lassen, haben die Administratoren mit ihnen ein sehr mächtiges Mittel zum Steuern der Datenströme und das Benutzerverhaltens in der Hand.

App Rules lassen sich auch "On the fly" direkt aus dem App Flow-Monitor heraus erzeugen. Dazu genügt es, eine Anwendung, wie zum Beispiel "DoubleClick" aus der Liste zu selektieren und anschließend auf "Create Rule" zu gehen. Danach öffnet sich ein Fenster, das dem Administrator die Wahl gibt, die jeweilige Anwendung zu blockieren, ihre Bandbreite zu verwalten oder ihre Datenübertragungen zu überwachen. Im Test klappte das ohne Probleme und die Funktion ist im Arbeitsalltag sicher sehr praktisch. Es gibt auch einen Wizard, der beim Anlegen der Regeln für SMTP-, POP3-, FTP- und Web-Zugriffe hilft. Mit ihnen ist es unter anderem möglich, FTP-Übertragungen auf bestimmte Dateiinhalte, Dateinamen und Erweiterungen zu untersuchen. Bei Web-Übertragungen lässt sich unter anderem die Nutzung bestimmter Web-Browser herausfinden. In der Praxis gestaltet sich die Arbeit mit dem dazugehörigen Wizard sehr einfach.

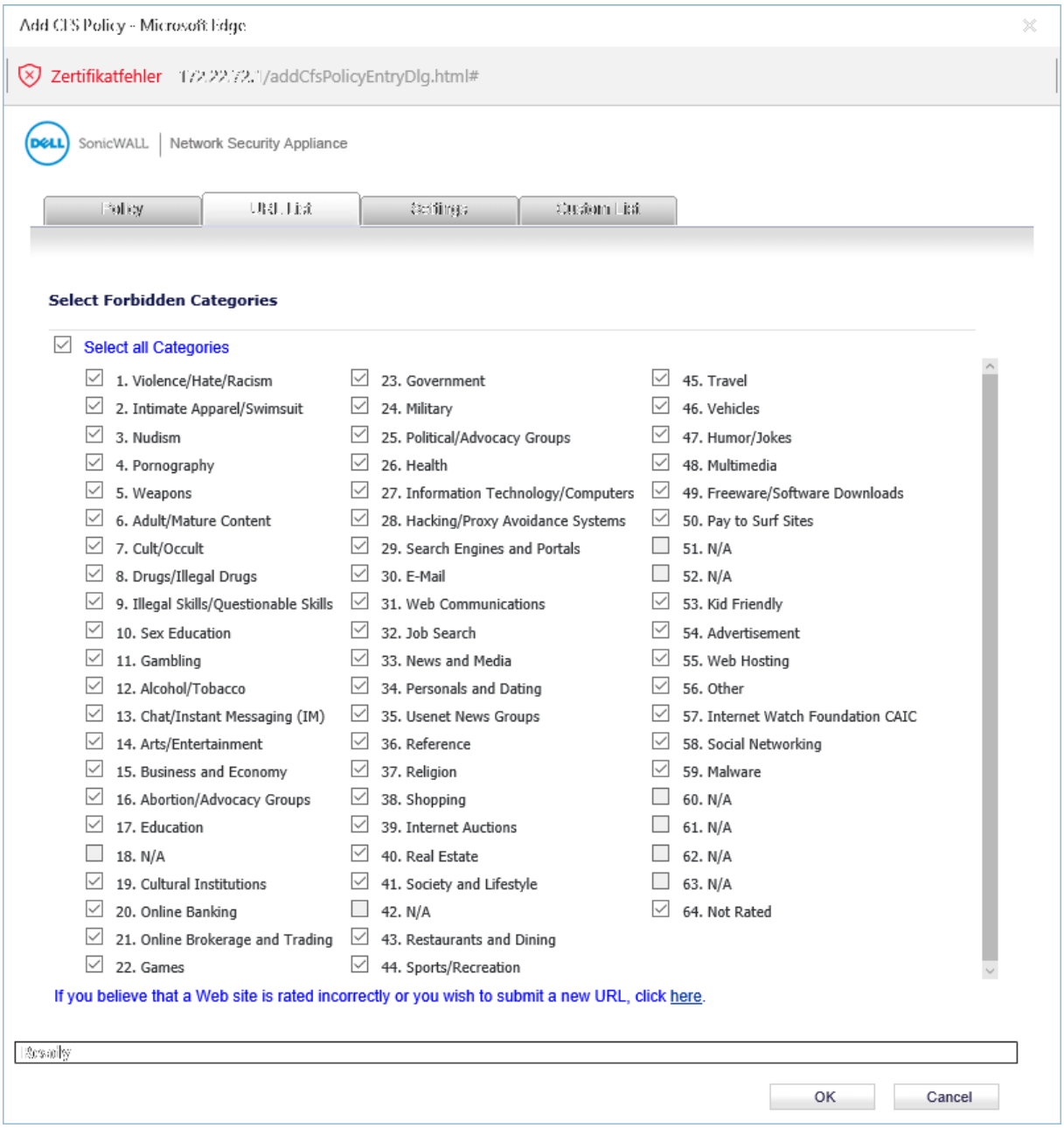
Ebenfalls unter Firewall aktivieren die Administratoren bei Bedarf die "Appliation Control Advanced". Dabei handelt es sich um einen Konfigurations-Dialog, über den sie direkt globale App Control Policies für einzelne Anwendungen und auch Anwendungskategorien konfigurieren können. Hier führen die Verantwortlichen falls nötig auch ein Update der dazugehörigen Signaturdatenbank durch und sehen eine Liste der definierten Anwendungen ein. Punkte zum Anlegen von Match Objects, Action Objects (Block, Drop, Monitor, etc.), Adressobjekten wie Netzwerken oder Hosts, Service Objects (also Protokollen), Bandwidth Objects und E-Mail-Adressobjekten schließen die Firewall-Konfiguration ab. Die E-Mail Objects kommen zusammen mit Mail-Filter-Regeln zum Einsatz und definieren die dabei verwendeten E-Mail-Adressen.

Im Menüpunkt "Firewall Settings" nehmen die Administratoren schließlich Einstellungen zum Bandbreitenmanagement, zur Flood-Protection, zum Multicast, zum QoS-Mapping und zum Überwachen von SSL-Verbindungen vor. Außerdem lassen sich hier der Stealth Mode aktivieren, Firewall-Regeln auf den internen LAN-Verkehr auf dem gleiche Interface anwenden und vieles mehr.

Deep Packet Inspection für SSL-Verbindungen

Die Deep Packet Inspection für SSL (DPI-SSL) – eine der wichtigsten Funktionen der TZ400 – entschlüsselt den SSL-Verkehr transparent, untersucht ihn auf Bedrohungen und verschlüsselt ihn anschließend vor der Weiterleitung an den Zielhost wieder. Im Betrieb kann die Appliance sowohl ein- als auch ausgehenden SSL-Verkehr untersuchen. Die DPI lässt sich zusammen mit den Diensten Antivirus, Anti-Spyware, IPS, Content Filter und Application Firewall nutzen und es ist auch möglich, Ausnahmen zu definieren, die sicherstellen, dass die Übertragungen von bestimmten

Adressen oder Benutzern beziehungsweise von bestimmten Diensten nicht analysiert werden. Im Test traten bei der Arbeit mit der DPI-SSL-Funktion keine Überraschungen auf und sie arbeitete sofort nach ihrer Aktivierung wie erwartet. Wir konnten das daran sehen, dass unsere Browser im LAN bei aktiver DPI-SSL Zertifikatsfehler meldeten. Das lag daran, dass wir das Standardzertifikat der Appliance verwendeten, das nicht als sicher galt. Die Appliance ersetzt ja das Zertifikat der besuchten Webseite nach der lokalen Entschlüsselung durch ihr eigenes, so dass die Browser glaubten, sie hätten es mit einem nicht sicheren Zertifikat zu tun. Abhilfe schafft hier entweder die Installation eines sicheren Zertifikats auf der Appliance oder der Import des unsicheren Zertifikats in den betroffenen Browser.



Die Kategorien des SSL-Filters

Die nächsten Einträge des Konfigurationswerkzeugs befassen sich mit der VoIP-Konfiguration mit SIP und H323 und den Einstellungen der Anti-Spam-Funktion. Letztere arbeitet entweder mit einem RBL-Filter oder mit einer vollwertigen Anti-Spam-

Lösung, die separat lizensiert werden muss. Diese Lösung setzt die Installation der so genannten Dell Junkstore App auf einem Server im Netz voraus. Sobald diese Software aktiv ist, kann sie zum Einsatz kommen, um potentielle Spam-Nachrichten aufzunehmen. Es gibt auch die Option, Mails direkt zu löschen, letzteres ergibt beispielsweise bei Nachrichten Sinn, die virenverseucht ankommen. Benutzerdefinierte Zugriffslisten gehören genauso zum Leistungsumfang der Anti-Spam-Lösung wie umfassende Statistiken, die die Verantwortlichen über die aufgetretenen Bedrohungen informieren.

Unter "VPN" finden sich alle Einstellungen zum Einrichten von IPSec-VPNs, während "SSL-VPN" den einfachen Zugriff auf Unternehmensressourcen via Browser ermöglicht. Das SSL-VPN lässt sich dabei einfach durch das Klicken auf einen Zonennamen (LAN, WAN, DMZ, etc.) aktivieren und steht dann im entsprechenden Netz zur Verfügung. Damit die Anwender damit arbeiten können, müssen die Administratoren allerdings noch unter "Virtual Office" die zu nutzenden Dienste freigeben. Hierfür stehen neben den Terminal Services auch SSH, Telnet und VNC zur Verfügung. Über die SSL-VPN-Konfiguration steht außerdem auch der Windows NetExtender-Client zum Download bereit, über den die Anwender von Windows-Systemen direkt ohne Browser auf die SSL-VPN-Dienste zugreifen können.

Die Benutzerverwaltung unterstützt sowohl lokale Benutzerkonten als auch Authentifizierungen über LDAP und Radius. Bei Bedarf lassen sich auch Gästekonten einrichten und SSO-Szenarien (Single Sign On) realisieren. Da die Benutzer – wie bereits angesprochen – auch Teil der Regeln sein können, ist es beispielsweise möglich, Policies zu definieren, die es nur bestimmten Usern nach einer Authentifizierung erlauben, bestimmte Dienste (wie etwa Facebook) zu nutzen.

Die nächsten Punkte befassen sich mit der Konfiguration der Hochverfügbarkeitsfunktion und der Sicherheitsdienste. Bei letzteren handelt es sich um den Content Filter, das IPS-System, das Client Antivirus-Enforcement, die Anti-Spyware und ähnliches. Über den Content-Filter lassen sich ActiveX- beziehungsweise Java-Verbindungen und Cookies blockieren sowie URLs nach bestimmten Kategorien unterbinden (zum Beispiel Medien, Malware, Military und Social Networking). Neben dem Content Filter-Service unterstützt das System auch Websense Enterprise.

Das Client AV-Enforcement sorgt dafür, dass nur Clients mit aktiver und aktueller Antivirus-Software ins Netz dürfen, während der Gateway Antivirus den Verkehr über die Protokolle HTTP, FTP, IMAP, SNMP, POP3 und CIFS unter die Lupe nimmt. Bei Bedarf ist er auch dazu in der Lage, TCP-Streams zu analysieren.

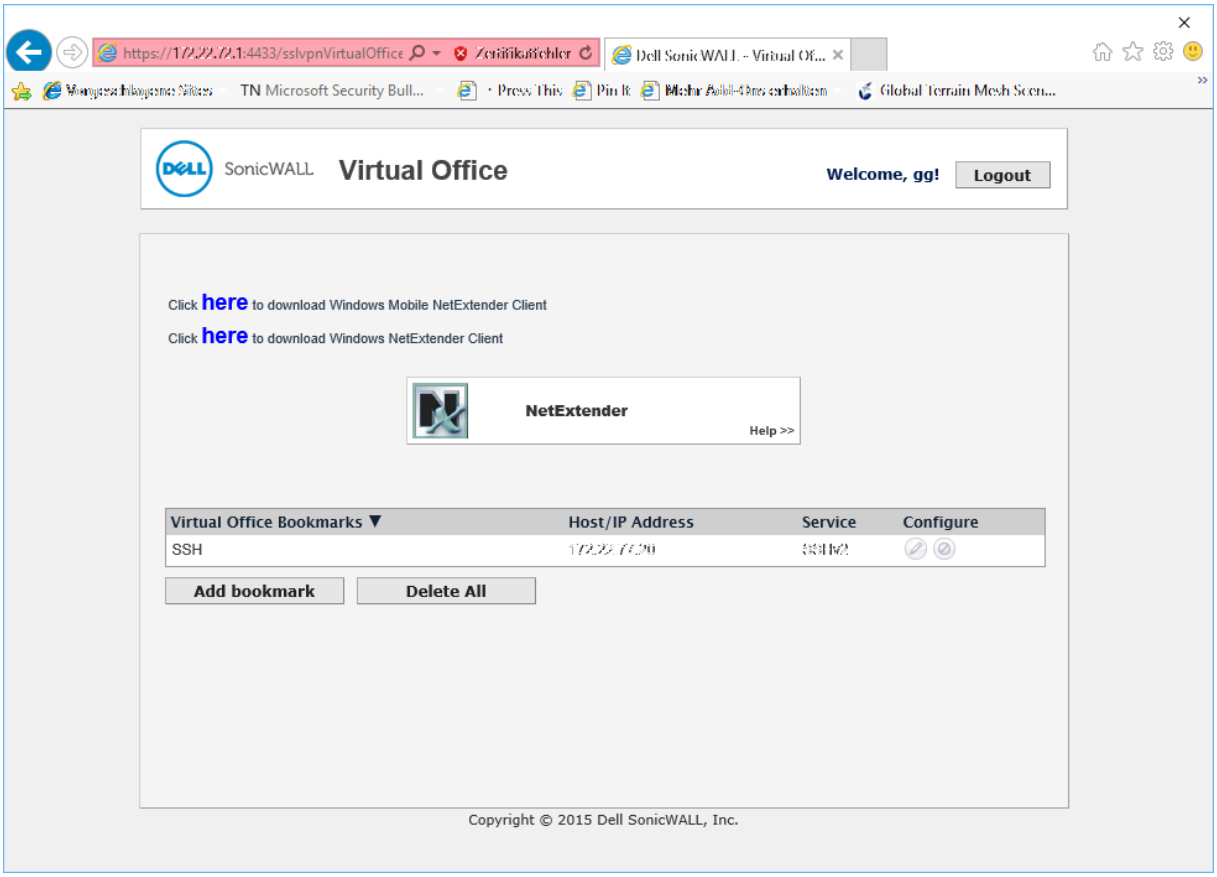
Das IPS unterscheidet zwischen Angriffen hoher, mittlerer und niedriger Priorität und behandelt diese unterschiedlich. Die Liste der entsprechenden Policies lässt sich jederzeit bearbeiten. Die Anti-Spyware-Funktion untersucht Übertragungen über die Protokolle HTTP, FTP, IMAP, SMTP und POP3. Auch dabei kommen Regeln zum Einsatz, die die zuständigen Mitarbeiter jederzeit modifizieren können. Der "Botnet Filter" blockt und loggt Botnet-Verbindungen, der "Geo IP-Filter" blockiert Connections zu bestimmten Ländern und bei der RBL-Filter-Konfiguration haben die Administratoren schließlich Gelegenheit, zusätzlich zu den Listen von spamhaus.org und sorbs.net auch eigene Einträge hinzuzufügen und White- sowie Blacklists anzulegen.

Die letzten Punkte des Konfigurationswerkzeugs befassen sich mit der WAN-Beschleunigung, dem App Flow-Reporting mit Real Time-Datensammlung und dem Logging. Die App Flow-Funktion unterstützt Netflow 5, Netflow 9 und IPFIX (auch mit Extensions und Extensions V2). Über das Logging haben die Administratoren die Option, die Farbe für bestimmte Log-Typen festzulegen, einen Syslog-Server anzulegen, Mail-Alerts zu definieren, Logs zu bestimmten Zeiten an zuständige Mitarbeiter zu mailen und Reports zu erzeugen, beispielsweise für Web Site Hits, Bandbreitennutzungen nach IP-Adressen oder auch Bandbreitennutzungen nach Diensten.

Die Lösung im Betrieb

Wie angesprochen nahmen wir die WAN- und LAN-Ports der Lösung während des Tests mit diversen Security-Tools unter die Lupe. nmap stellte dabei richtig fest, dass im LAN die Ports 22, 80 und 443 offen waren. 22 hatten wir für SSH-Zugriffe freigegeben und über Port 80 leitet die Appliance eingehende Browseranfragen direkt auf das SSL-basierte Web-Interface um. Die Informationen, die nmap sammeln konnte, reichten nicht aus, um anzugeben, welches Betriebssystem auf der Appliance aktiv war. Auf den externen Ports konnte nmap überhaupt nichts finden, was auch unserer Konfiguration entsprach.

Der Scan mit Nessus brachte keine Vulnerabilities zu Tage, Metasploit konnte immerhin am internen Interface herausfinden, dass es sich bei der TZ400 um ein Sonicwall-Gerät handelte und NexPose gab an, dass es sich wahrscheinlich um eine Lösung von Sonicwall handelte. Bei den Angriffen mit den DoS-Tools stellten wir fest, dass Attacken auf das WAN-Interface – das wir zu diesem Zeitpunkt mit einer statischen IP-Adresse konfiguriert hatten – nichts brachten, während Angriffe auf das LAN-Interface mit manchen dieser Werkzeuge dafür sorgten, dass die Datenübertragungen stehen blieben. Nach dem Ende der Angriffe lief dann alles wieder normal weiter. Das ist zwar nicht schön, kann aber nicht wirklich als Sicherheitslücke gelten, da es sich ja beim LAN-Interface um die sichere Schnittstelle handelt, auf die im Betrieb keine Angriffe erfolgen sollten.



Nach dem Login beim SSL-VPN

Zusammenfassend bleibt also das Fazit, dass die Appliance keine überflüssigen oder potentiell gefährlichen Informationen im Netz bereitstellt und auch keine leicht herausfindbaren Sicherheitslücken mitbringt. Darüber hinaus lassen sie Angriffe auf das externe Interface kalt.

Fazit

Im Test konnte uns die SonicWALL TZ400 von Dell überzeugen. Das Produkt verfügt über einen sehr großen Leistungsumfang, lässt sich aber trotzdem schnell und einfach in Betrieb nehmen und später auch leicht verwalten. Die Tools zum Überwachen des Netzwerkverkehrs überzeugen ebenso wie die Reports und Alarme. Besonders positiv müssen wir aber die sehr leistungsfähigen Regeln zur Anwendungskontrolle und die einfach zu konfigurierende Deep-Paket-Inspection für SSL-Übertragungen hervorheben, die bei uns im Test ohne weiteren Verwaltungsaufwand sofort ihre Arbeit aufnahm. Administratoren, die kleinere oder verteilte Umgebungen absichern müssen, sollten sich die SonicWALL TZ-Serie von Dell auf jeden Fall einmal anschauen.