Evaluierungskriterien für Next-Generation Firewalls

Dieses Dokument beschreibt viele wichtige Features und Funktionen, die bei der Evaluierung von Next-Generation Firewalls (NGFWs) von Bedeutung sind und einen genauen Vergleich der Lösungen unterschiedlicher Anbieter erleichtern.

DELL SonicWALL

Inhaltsverzeichnis

SonicWALL

1 Was eine Next-Generation Firewall können sollte

Next-Generation Firewalls bieten alle Features einer gängigen Stateful Packet Inspection-Firewall und verfügen zusätzlich über Funktionen zur Identifizierung, Visualisierung und Kontrolle von Anwendungen unabhängig vom Port oder Protokoll. Anstatt Zugriffsregeln über bekannte Ports oder Adressen zu realisieren, können die Regeln so anwendungsbasiert pro Benutzer oder Gruppe festgelegt werden.

Das Problem herkömmlicher proxybasierter Firewalls ist, dass die Überwachung und Kontrolle nur auf den proxyfähigen Ports wie z. B. Port 80 (Internet) oder Port 25 (SMTP) erfolgen kann. Der größte Teil des böswilligen Verkehrs passiert die Firewall aber auf nicht proxyfähigen Ports oder ist per SSL verschlüsselt. Man benötigt also eine Next-Generation Firewall, die einen Rundum-Schutz gegen Bedrohungen auf beliebigen Ports bietet und dabei weder die Leistung beeinträchtigt noch die Latenz erhöht. Das lässt sich durch eine Deep Packet Inspection (DPI)-Engine mit SSL-Prüfung erreichen, die von einem integrierten Security Research Team (SRT) entwickelt wurde.

Die nachstehenden Kriterien sind Voraussetzung für jede Next-Generation Firewall, die zur Anwendungskontrolle eingesetzt wird. Unternehmen sollten sich darüber im Klaren sein, dass viele Next-Generation Firewall-Lösungen lediglich einen Teil der Funktionen bieten, die durch die Next-Generation Firewall-Technologie ermöglicht werden. Der Funktionsumfang dieser Lösungen mag für einige Unternehmen zwar nützlich sein, aber sie können nicht als vollwertige, flexible und skalierbare Next-Generation Firewalls betrachtet werden.

1. Lückenlose Stateful Packet Inspection (SPI)-Funktionalität. An erster Stelle müssen alle Funktionen und Kontrollen der vorhandenen proxybasierten SPI-Firewall abgebildet werden. Dazu gehören die Regelerstellung und -kontrolle, die Unterstützung von Site-to-Site-VPN, WAN-Failover und Lastverteilung, 3G/4G-WAN-Failover, die Unterstützung des Remote-Zugriffs über IPSec und SSL VPN, eine zentrale Verwaltung, das Reporting und Hochverfügbarkeitsfunktionen mit Clustering.

2. Intrusion Prevention. Umfassende Deep Packet Inspection bietet Schutz vor Schwachstellen in Anwendungen, Pufferüberläufen und Mischangriffen, die ein Netzwerk für Exploits anfällig machen können. Intrusion Prevention Services (IPS) bieten vor einer ganzen Reihe netzwerkbasierter Schwachstellen und Exploits Schutz, sowohl von internen als auch von externen Bedrohungen. IPS überwacht das Netzwerk auf böswilligen oder auffälligen Verkehr. Dieser wird auf der Basis vordefinierter und automatisch aktualisierter Kriterien blockiert bzw. protokolliert. Automatische Updates stellen sicher, dass neue Bedrohungen dynamisch blockiert werden.

3. Identifizierung und Kontrolle von Anwendungen. Next-Generation Firewalls erkennen Anwendungen an ihren eindeutigen Signaturen – unabhängig davon, welcher Port oder welches Protokoll verwendet wird. Die Anwendungen können in Echtzeit visualisiert werden, um eine Priorisierung der Bandbreite sicherzustellen und maximale Netzwerksicherheit und Produktivität zu gewährleisten. Administratoren können granulare Kontrollen auf Anwendungsebene einrichten, bestimmte Anwendungen priorisieren, die Bandbreite einschränken oder den Zugriff verweigern.

4. SSL-Entschlüsselung und -Prüfung. Viele Bedrohungen werden heute über sichere Kanäle verbreitet, die SSL zur Verschlüsselung nutzen. Deshalb ist es unverzichtbar, dass eine Next-Generation Firewall SSL-Verkehr entschlüsseln, untersuchen und anschließend wieder verschlüsseln kann.

5. Benutzeridentifizierung. Eine Next-Generation Firewall sollte auf jeden Fall in der Lage sein, Anwendungen zu identifizieren und zu kontrollieren. Diese Funktionalität muss allerdings mit der LDAP- oder Active Directory-Infrastruktur eines Unternehmens gekoppelt sein. Es ist nicht länger erforderlich, eine Quell-IP-Adresse bis zum physischen Benutzer zu verfolgen. Next-Generation Firewalls unterstützen Single Sign-on und können eine Benutzerkennung für Zugriffskontrolle und Reporting automatisch mit einem Endpunkt verknüpfen.

Bei Next-Generation Firewalls geht es nicht nur um Anwendungskontrolle

Viele Unternehmen sehen Next-Generation Firewalls als Möglichkeit, einen sicheren Zugriff über öffentliche Verbindungen von außen zu gewährleisten. Heutzutage entstehen viele Bedrohungen aber innerhalb des Unternehmensnetzwerks und kommen von Benutzern, die auf öffentliche Websites wie Facebook und YouTube zugreifen. Mit einer Next-Generation Firewall können IT-Abteilungen den Netzwerkverkehr in beiden Richtungen authentifizieren, autorisieren und überprüfen, sodass der sichere Zugriff auf alle Ressourcen gewährleistet ist.

In diesen Bereichen sind Next-Generation Firewalls den traditionellen proxybasierten Firewalls überlegen

- Geringe Latenz
- Skalierbarkeit auf Leitungsgeschwindigkeit
- Deep Packet Inspection für alle Ports und Protokolle
- SSL-Prüfung
- Unterstützung von IPSec und SSL VPN
- Anwendungskontrolle auf Schicht 7

1 Was eine Next-Generation Firewall können sollte (Forts.)

6. Viren- und Spyware-Schutz am Gateway. Genau genommen ist es nicht nötig, dass eine Next-Generation Firewall Malware am Gateway blockiert. Dennoch ist es ideal, den gesamten Verkehr unabhängig von der Größe des Inhalts oder der Anzahl aktiver Sitzungen mit automatisierten Signaturen-Updates in beiden Richtungen zu prüfen.

7. Security Research Team. Eine Next-Generation Firewall ist nur so gut wie die verfügbaren Anwendungs-, IPS- und Anti-Malware-Signaturen. Firewall-Anbieter sollten ein integriertes Security Research Team (SRT) haben, das neue Anwendungs- und Malware-Varianten sowohl manuell als auch automatisch zusammenträgt, neue Signaturen erstellt und diese dann automatisch an die Firewalls verteilt, die den entsprechenden Service abonniert haben. Ferner sollte das SRT ein aktives Mitglied in mehreren Sicherheits-organisationen wie z. B. dem Microsoft Active Protections Program sein.

8. Weitere intelligente Firewall-Funktionen. Die Firewall sollte die Fähigkeit haben, externe Datenquellen abzufragen, um das Unternehmen besser schützen zu können. So können zum Beispiel Features wie IP-Reputation, Webfiltering usw. durch den Einsatz Cloud-basierter intelligenter Funktionen optimiert werden.

9. Hohe Performance, Verfügbarkeit und Skalierbarkeit. Bei herkömmlichen proxybasierten Firewalls führt Deep Packet Inspection zu erheblichen Performance-Einbußen. Außerdem gibt es Einschränkungen bei den Protokollen, Ports und Dateigrößen, die überprüft werden können. Eine echte Next-Generation Firewall muss Deep Packet Inspection bei nahezu Leitungs-geschwindigkeit auf allen Ports und über sämtliche Protokolle hinweg anwenden können. Darüber hinaus muss sie sich auf die heutigen 10-GbE-Netzwerke skalieren lassen. Das bedeutet nicht nur, dass die Firewall mit 10-GbE-Ports ausgestattet sein muss – sie muss auch in der Lage sein, 10-GbE-Durchsatzraten bei voll aktivierter DPI zu unterstützen.

10. Zertifizierungen und Bewertungen durch Dritte. Bewertungen und Zertifizierungen durch anerkannte und unabhängige Testorganisationen wie z. B. ICSA (Enterprise Firewall Certification) und dem IPv6-Forum sind für jede Next-Generation Firewall von entscheidender Bedeutung. Zusätzliche Zertifizierungen wie FIPS und Common Criteria sind außerdem für den Einsatz in Behörden erforderlich.

11. Stabilität, Erfahrung und Unterstützung. Bei einer langfristigen Investition spielen nicht zuletzt die Stabilität und Erfahrung des Anbieters eine wichtige Rolle. Unternehmenszahlen, finanzielle Lage und Kundenstamm sind Schlüsselfaktoren für den guten Zustand eines Anbieters. Bei größeren Projekten tragen außerdem muttersprachliche Techniker, Partner- oder Professional-Services und ein 24/7-Support zur erfolgreichen Implementierung und Bereitstellung bei.

Automatische Updates = geringere Verwaltungskosten
Next-Generation Firewalls stellen automatisierte Signaturen-Updates für Anwendungen, IPS und Malware zur Verfügung. Das bedeutet, dass Netzwerkadministratoren keine Zeit für die Recherche und das Laden von neuen Updates verschwenden müssen.

2 Evaluierungskriterien für Next-Generation Firewalls

Geprüfte NGFW-Appliance: _____

Version der NGFW-Appliance: _____

Prüfdatum: _____

3 Stateful Packet Inspection-Funktionen

Bei jeder Next-Generation Firewall, die Sie in Betracht ziehen, sollten hochflexible Zugriffsregeln und weitere Schlüsselfeatures die Basis für die Stateful Packet Inspection-Funktionen bilden.

Stateful Paket Inspection-Funktionen	Ja	Nein
3.1 Zonenbasierte Regelkontrolle Sicherheitszonen, entweder physisch oder virtuell, bieten der Firewall eine zusätzliche, flexiblere Schutzschicht. Zudem können Administratoren ähnliche Schnittstellen gruppieren und dieselben Regeln darauf anwenden, anstatt die gleichen Regeln für jede einzelne Schnittstelle separat einrichten zu müssen.		
3.2 Standardmäßig verweigerter Zugriff Die Lösung sollte den Zugriff aus dem LAN ins Internet standardmäßig verweigern und jeglichen Zugriff aus dem WAN oder DMZ auf das private LAN-Netzwerk blockieren bzw. ablehnen.		
3.3 Bandbreitenverwaltung Eine Funktion zur Verwaltung der Bandbreite sollte Administratoren die Zuweisung von garantierter, maximaler Bandbreite für Services und die Priorisierung des Datenverkehrs auf allen Firewall-Schnittstellen ermöglichen. Über Zugriffsregeln kann die Bandbreitenverwaltung selektiv auf den Netzwerkverkehr angewendet werden.		
3.4 Verbindungsbegrenzung Connection Limiting bietet eine zusätzliche Schutz- und Kontrollschicht, um Verbindungen über die Firewall mithilfe von Zugriffsregeln zu begrenzen. Diese Funktion kann gegen Denial-of-Service (DoS)-Angriffe oder andere Malware-Arten eingesetzt werden, die sich durch den Aufbau einer ungewöhnlich hohen Anzahl von Verbindungen zu beliebigen Adressen verbreiten.		
3.5 Firewall-Erkennung verhindern Die Lösung sollte mehrere Methoden anbieten, um die Erkennung der Firewall durch entsprechende Tools zu vermeiden.		
3.6 Dynamische Ports Die Lösung sollte dynamische Porttransformationen für Anwendungen unterstützen, die möglicherweise keine Standard-Ports nutzen wie FTP, Oracle SQLNET und RSTP.		
3.7 IP-Prüfsummen Die Lösung sollte über eine Option verfügen, die Prüfsummen-Checks für IP-Header und UDP-Pakete durchsetzt.		
3.8 Flood-Schutz Dank SYN/RST/FIN Flood-Schutz können Hosts hinter einer Firewall vor DoS- oder DDoS-Angriffen geschützt werden, die darauf abzielen, die verfügbaren Ressourcen des Hosts lahmzulegen.		
3.9 Multicast-Unterstützung Zur Unterstützung von Multimedia-Anwendungen und Videokonferenzen sollte die Lösung IP-Multicasting bieten, damit ein IP-Paket gleichzeitig an mehrere Hosts geschickt werden kann.		
3.10 QoS-Unterstützung Es sollte ein Quality of Service (QoS)-Mechanismus inklusive Unterstützung für DSCP und 802.1p vorhanden sein.		
3.11 SSL-Kontrolle Die Firewall sollte Einblick in den Handshake von SSL-Sitzungen gewähren und die Möglichkeit bieten, Richtlinien zu erstellen, um den Aufbau von SSL-Verbindungen zu kontrollieren.		
3.12 Flexible SPI-Regeln Die Firewall-Regeln sollten Zeitsteuerung, Aufnahme bzw. Ablehnung von Benutzern und Gruppen, Bandbreitenverwaltung, Verbindungsbegrenzung sowie Kontrolle anhand geografischer IP-Adressen und das QoS-Mapping mittels Adressobjekten unterstützen, mit denen Hosts, Netzwerke, Adressbereiche sowie FQDN- und MAC-Adressen definiert werden können.		

4 VPN-Unterstützung

Die Unterstützung für VPNs, entweder Site-to-Site oder Client-to-Site, ist eine wichtige Komponente von Next-Generation Firewalls. Die Unterstützung von Site-to-Site-VPNs mittels IPSec ist Industriestandard, während IPSec und SSL VPN für den Client-to-Site-Zugriff genutzt werden.

4.1 Unterstützung von Site-to-Site-VPN	Ja	Nein
4.1.1 Interoperabilität mit Drittanbieter-Lösungen Ist die Lösung mit den Firewalls anderer Hersteller kompatibel, um einen heterogenen Betrieb zu ermöglichen?		
4.1.2 DHCP über VPN Dank DHCP über VPN kann die Firewall vom DHCP-Server am anderen Ende des VPN-Tunnels einen IP-Adressen-Lease beziehen. In einigen Netzwerken ist es wünschenswert, dass sich alle VPN-Netzwerke in einem logischen IP-Subnetz befinden und den Anschein erwecken, dass alle VPN-Netzwerke im Adressraum eines IP-Subnetzes sind. Das erleichtert die IP-Adressverwaltung für Netzwerke, die VPN-Tunnel benutzen.		
4.1.3 Routenbasiertes VPN Beim routenbasierten VPN werden für die VPNs statische oder dynamische Routen anstelle von festen Richtlinien konfiguriert. Das erleichtert die Konfiguration und Wartung der VPN-Richtlinien und bietet darüber hinaus die Möglichkeit, mehrere Pfade zu Redundanz- und Sicherungszwecken anzugeben.		
4.2 Unterstützung für VPN-Clients	**Ja**	**Nein**
4.2.1 IPSec-Client Es sollte ein IPSec-Client verfügbar sein, der sowohl Windows® als auch Mac OS® unterstützt und über solide Authentifizierungsmechanismen verfügt (z. B. Zwei-Faktor-Authentifizierung).		
4.2.2 SSL VPN-Client Es sollte ein SSL VPN-Client verfügbar sein, der sowohl Windows als auch Mac OS unterstützt und über eine granulare Zugriffskontrolle sowie solide Authentifizierungsmechanismen verfügt.		
4.2.3 Mobile Geräte Mobile Geräte mit Android™- bzw. iOS-Betriebssystemen sollten ebenfalls unterstützt werden.		
4.2.4 L2TP-Termination L2TP ist eine optionale VPN-Methode, die ebenfalls auf der Firewall-Plattform verfügbar sein sollte.		
4.2.5 Virtual Assist Die Virtual Assist-Technologie ermöglicht die Fehlerbehebung auf Remote-Systemen sowie die Unterstützung der Remote-Benutzer. Diese Funktion bedeutet eine deutliche Zeitersparnis für das Support-Personal und bietet zusätzliche Flexibilität bei der Handhabung von Support-Anfragen. Benutzer können Kunden den Beitritt in eine Support-„Warteschlange“ gestatten bzw. sie dazu einladen. Anschließend können sie virtuellen Support für die einzelnen Kunden durch Übernahme des Remote-Computers leisten, um technische Probleme zu diagnostizieren und zu beheben.		

5 VoIP-Unterstützung

Eine Next-Generation Firewall sollte volle Unterstützung für Voice over IP (VoIP)-Dienste bieten. Das effiziente Passieren einer Firewall ist für VoIP schwierig. Dies liegt an der Komplexität der Signale und Protokolle bei VoIP sowie an den Inkonsistenzen, die entstehen, wenn eine Firewall Quelladressen und -ports durch Network Address Translation (NAT) modifiziert.

5.1 VoIP-Features	Ja	Nein
5.1.1 SIP und H.323 Für VoIP-Funktionalität müssen SIP und H.323 voll unterstützt werden.		
5.1.2 Legitimität des Datenverkehrs Jedes VoIP-Signal- und -Medienpaket, das die Firewall passiert, sollte mit Stateful Inspection geprüft werden, um sicherzustellen, dass es sich um legitimen Datenverkehr handelt.		
5.1.3 Schutz auf Anwendungsschicht für VoIP-Protokolle Ein vollständiger Schutz vor Exploits auf der Anwendungsschicht sollte über VoIP-spezifische Signaturen zur Verfügung gestellt werden. Diese verhindern, dass böswilliger Datenverkehr zu geschützten VoIP-Telefonen und -Servern vordringen kann.		
5.1.4 Schutz vor DoS und DDoS-Angriffen Schutz vor DoS- und DDoS-Angriffen wie SYN Flood, Ping of Death und LAND (IP), die darauf abzielen, das Netzwerk oder einen Dienst lahmzulegen.		
5.1.5 Stateful Monitoring Stellt sicher, dass an sich gültige Pakete auch für den aktuellen Zustand der jeweiligen VoIP-Verbindung geeignet sind.		
5.1.6 Unterstützung von Geräten mit Verschlüsselung Das Gerät sollte Verschlüsselung einsetzen können, um den Medienaustausch in einem VoIP-Gespräch zu schützen oder VoIP-Geräte abzusichern, die keine verschlüsselte Übertragung unterstützen.		
5.1.7 Schutz auf der Anwendungsschicht Die Deep Packet Inspection-Engine sollte Angriffe aus VoIP-Exploits auf der Anwendungsschicht erkennen und verhindern.		
5.1.8 Anrufverfolgung und Qualitätsüberwachung Der Administrator sollte eine Tabelle mit dem Anrufstatus der aktiven VoIP-Verbindungen anzeigen können.		
5.1.9 Kontrolle von unerlaubten oder Spam-Anrufen Stellt sicher, dass eingehende Anrufe durch den H.323 Gatekeeper oder SIP-Proxy genehmigt und authentifiziert sind und dass das Gerät unerlaubte und unerwünschte Anrufe blockieren kann.		

6 Sicherheit

Eine Next-Generation Firewall sollte diverse integrierte Security- und Deep Packet Inspection-Funktionen zur Verfügung stellen. Die beste Lösung kann ein Netzwerk vor modernen Angriffsvektoren und Exploits schützen.

6.1 Deep Packet Inspection	Ja	Nein
6.1.1 SIP und H.323 Für VoIP-Funktionalität müssen SIP und H.323 voll unterstützt werden.		
6.1.2 Datenstrombasierte Paketverarbeitung Die Lösung sollte auf einer datenstrombasierten bzw. Reassembly-Free-Architektur aufbauen, die zur Prüfung keinen Umweg über einen Proxy erfordert.		
6.1.3 Keine Beschränkungen bei der Dateigröße Die Deep Packet Inspection-Engine sollte in der Lage sein, jede Datei unabhängig von Größe und Protokoll ohne Pufferung der Pakete zu prüfen. Daher sollte sie keine Einschränkungen bei der Dateigröße haben.		
6.1.4 Intrusion Prevention Bidirektionaler IPS-Schutz bei wichtigen Netzwerkdiensten wie Internet, E-Mail, Dateitransfer, Windows-Diensten und DNS.		
6.1.5 Virenschutz am Gateway Echtzeit-Virenprüfung des gesamten Firewall-Verkehrs in beiden Richtungen. Dabei sollten auch mehrere Anwendungsprotokolle sowie allgemeine TCP-Ströme und komprimierte Daten unterstützt werden.		
6.1.6 Spyware-Schutz am Gateway Die Lösung sollte Schutz vor aufdringlicher Spyware bieten. Dazu sollten Installation und Zustellung von Spyware an der Firewall unterbunden und die Weitergabe von gesammelten Informationen durch bereits installierte Spyware nach außen verhindert werden.		
6.1.7 Content Filtering/URL Filtering Setzt Richtlinien zum Blockieren von anstößigen, unerwünschten oder unproduktiven Webinhalten anhand vordefinierter Kategorien bzw. individueller Definitionen durch.		
6.1.8 SSL-Prüfung Entschlüsselung und Prüfung des gesamten SSL-Verkehrs in sowohl ein- als auch ausgehender Richtung.		
6.1.9 SSO-Integration Die Lösung unterstützt die Überwachung von Windows-Domänen-Anmeldungen, um Informationen zur Benutzerkennung für Reporting- und Analysezwecke festzuhalten. Hier sollte enthalten sein: • Unterstützung für Windows-, Mac- und Linux-Systeme • Agent-basierter SSO • SSO mit browserbasierter NTLM-Authentifizierung • Browserbasierte manuelle Authentifizierung		

6 Sicherheit (Fortsetzung)

6.2 Zusätzliche Sicherheitsservices	Ja	Nein
6.2.1 Verhinderung von DNS Rebinding-Attacken Die Lösung sollte DNS Rebinding-Attacken verhindern, die eine Domäne auf den DNS-Server des Angreifers registrieren und so die Same-Origin-Policy des Browsers aushebeln.		
6.2.2 Schutz vor MAC-IP-Spoofing Es sollte ein Schutz vor MAC-IP-Spoofing vorhanden sein, um Spoofing-Angriffe auf den OSI-Schichten 2 und 3 zu verhindern. Dazu sollten sowohl Funktionen für die Zugangskontrolle als auch für die Eliminierung von Spoofing-Angriffen verfügbar sein.		
6.2.3 Integrierter Client-Virenschutz Die Firewall sollte in der Lage sein, jeden Endpunkt kontinuierlich zu überwachen, um die Version der Virensignaturen-Datei zu überprüfen und den Download/die Installation von neuen Virensignaturen-Dateien bei Bedarf automatisch anzustoßen. Zusätzlich kann der Zugriff eines Benutzers auf das Internet blockiert werden, bis der Endpunkt den Virenschutzrichtlinien des Unternehmens entspricht.		
6.2.4 Real-Time Blacklists RBL Filtering ist eine wichtige Voraussetzung, um effizienten Spamschutz auf einer Next-Generation Firewall zu gewährleisten.		
6.2.5 Geo-IP-Filter Es sollten Filterfunktionen verfügbar sein, damit Verbindungen von und zu bestimmten geografischen Standorten kontrolliert werden können.		
6.2.6 Botnet-Filter Mit Botnet-Filtern können Verbindungen von oder zu Botnet-Command-and-Control-Servern blockiert werden.		
6.2.7 DLP Data Leak Prevention sollte vorhanden sein, um alle ausgehenden Pakete auf vertrauliche Passagen, Lesezeichen oder Muster mithilfe eines Regular Expression Processors zu prüfen.		
6.3 Security Research Team	**Ja**	**Nein**
6.3.1 Unternehmenseigenes Research-Team Anbieter von Next-Generation Firewalls sollten über ein Security Research Team verfügen, das aus eigenen Mitarbeitern besteht und firmeneigenes Know-how nutzt.		
6.3.2 Automatisierte Sandbox-Umgebung Das Security Research Team sollte eine automatisierte Sandbox-Umgebung sowie entsprechende Prozesse einsetzen, um neue Malware-Signaturen innerhalb von Minuten sammeln, analysieren und erstellen zu können.		
6.3.3 Dynamische Updates Signaturen-Updates sollten automatisch und ohne ein Eingriff des Administrators an die Next-Generation Firewall übertragen werden.		
6.3.4 Cloud-basierte Signaturen Die Lösung sollte ein Cloud-basiertes Sicherheitspaket umfassen, damit eine unbegrenzte Anzahl von Signaturen zur Verfügung steht, die von der Firewall in Echtzeit überprüft werden können.		
6.3.5 Echtzeit-Statistiken Die Firewall sollte Echtzeit-Statistiken mit einem Überblick zu aktiven Bedrohungen, Viren, Eindringversuchen und Spyware entsprechend den Vorgaben des Security Research Teams bieten.		
6.3.6 Übermittlung verdächtiger Dateien Es sollte eine einfache Methode geben, um verdächtige Dateien oder Netzwerk-Traces an das Security Research Team zu übermitteln und so die Erstellung von Signaturen zu ermöglichen.		

7 Volle Unterstützung für Anwendungsintelligenz

Next-Generation Firewalls sollten die vollständige Kontrolle über Anwendungen in den Bereichen Application Intelligence, Control & Visualization ermöglichen.

7.1 Anwendungsintelligenz, -visualisierung und -kontrolle	Ja	Nein
7.1.1 SIP und H.323 Für VoIP-Funktionalität müssen SIP und H.323 voll unterstützt werden.		
7.1.2 Echtzeit-Überwachung Echtzeit-Überwachung von Paketraten, Paketgrößen, Verbindungsgeschwindigkeiten, ein- und ausgehender Bandbreite sowie Anwendungen, die die Next-Generation Firewall passieren.		
7.1.3 Datenanalyse Integrierte Datenanalysefunktionen, die ein einfaches Reporting zu Anwendungsdaten oder die Filterung nach bestimmten Benutzern oder Anwendungen ermöglichen.		
7.1.4 Datenexport Einfache Methode zum Exportieren von Daten zur schnellen Berichterstellung im CSV-Format.		
7.1.5 Detaillierte Reports Ein detaillierter Kurzbericht aller gesammelten Daten sollte über die Verwaltungskonsole bzw. einen externen Berichtsmechanismus leicht zugänglich sein.		
7.1.6 Tabellen/Tortendiagramme Zur einfachen visuellen Analyse sollten die gesammelten Daten in Form von linearen Tabellen, Tortendiagrammen oder Grafiken bereitgestellt werden.		
7.1.7 Leichte Erstellung von Anwendungsregeln Es sollte jederzeit möglich sein, eine Regel für eine bestimmte Anwendung zu erstellen, um diese zu blockieren oder in der Bandbreite zu beschränken.		
7.1.8 Anwendungskontrolle Über die reine Identifizierung und Kontrolle von Anwendungen hinaus sollte auch die Kontrolle von speziellen Funktionen innerhalb einer Anwendung möglich sein (z. B. Zulassen von Yahoo IM, aber keine Dateitransfers über IM).		

8 Sonstige wichtige Features

Eine ideale Lösung sollte über eine Reihe weiterer Features verfügen, die für eine Top-Konfiguration erforderlich sind.

8.1 Wichtige Features	Ja	Nein
8.1.1 IPv6 Unterstützung für IPv6, zertifiziert durch das IPv6-Forum.		
8.1.2 Multi-WAN Die Fähigkeit, zwei oder mehrere WAN-Verbindungen ohne zusätzliche Kosten oder Lizenzen zu unterstützen.		
8.1.3 WAN-Failover Automatisiertes Failover zum Sichern der WAN-Schnittstellen bei Ausfall des primären WAN.		
8.1.4 Lastverteilung im WAN Ebenfalls zu den wichtigen Funktionen zählt die WAN-übergreifende Unterstützung der Lastverteilung beim ausgehenden Datenverkehr.		
8.1.5 Dynamisches DNS Unterstützung von dynamischem DNS bei WAN-Verbindungen.		
8.1.6 Hochverfügbarkeit Unterstützung für Active/Passive, Active/Active sowie geclusterte Hochverfügbarkeitskonfigurationen mit Stateful-Synchronisierung. Darüber hinaus ermöglichen führende Next-Generation Firewalls Active/Active UTM, wenn die Verbindungen von einem primären Knoten gehandhabt und die Prozessorkerne beider Knoten gleichzeitig für die Deep Packet Inspection eingesetzt werden.		
8.1.7 3G/4G-Modem-Failover Fällt das primäre WAN aus, wird das integrierte 3G/4G-Modem aktiv, um den nahtlosen Übergang zu einem Mobilfunkanbieter zu ermöglichen.		
8.1.8 Integrierte WAN-Beschleunigung Es werden Lösungen zur integrierten WAN-Beschleunigung angeboten, die im 1-Arm-Modus auf der Next-Generation Firewall bereitgestellt werden. Es sind Sicherheitsservices für die Full Deep Packet Inspection des gesamten beschleunigten Verkehrs vorhanden, der die Firewall passiert.		
8.1.9 10-GbE-Unterstützung Die Unterstützung von 10-GbE ist unverzichtbar, um zentralen und künftigen Anforderungen von Netzwerken gerecht zu werden. Die bloße Existenz von 10-GbE-Ports allein reicht nicht aus, da Next-Generation Firewalls in der Lage sein müssen, einen 10-GbE-Durchsatz bei gleichzeitig aktivierten Sicherheitsservices zu unterstützen.		
8.1.10 Zentrale Verwaltungskonsole Für verteilte Umgebungen muss eine zentrale Verwaltungskonsole zur Überwachung, Verwaltung, Protokollierung und Berichterstellung zur Verfügung stehen.		

9 Einfache Konfiguration und Verwaltung

Gute Next-Generation Firewalls verfügen über eine intuitive Konfigurationsoberfläche. Außerdem stellen sie dem Administrator im laufenden Betrieb schnell und effektiv die nötigen Informationen bereit.

9.1 Einfache Konfiguration	Ja	Nein
9.1.1 Setupassistent Dank einem webbasierten Setupassistenten, der den Administrator Schritt für Schritt durch die übliche Konfiguration führt, lässt sich das Setup schnell und leicht durchführen.		
9.1.2 Objektbasierte Architektur Es lassen sich administrative Objekte erstellen und gruppieren, um den Verwaltungsaufwand zu reduzieren und redundante Arbeiten zu vermeiden.		
9.1.3 Safemode-Konfiguration Die Next-Generation Firewall kann in einen sicheren Modus versetzt werden, um schnell zu einer bekannten Konfiguration zurückzukehren.		
9.2 Einfache Verwaltung	**Ja**	**Nein**
9.2.1 Webbasierte Verwaltung Administrative Aufgaben werden über eine Webschnittstelle ausgeführt, sodass keine zusätzliche Hardware oder weitere Software-Clients und Agents erforderlich sind.		
9.2.2 Einfache Upgrades Die Verwaltungskonsole bietet einfache Upgrades und ermöglicht zuverlässige Rollbacks zu früheren Konfigurationen.		
9.2.3 Dienstprogramm für Import/Export Die Lösung bietet ein Import-/Export-Dienstprogramm, um Konfigurationsangaben auf mehreren Next-Generation Appliances zu synchronisieren.		
9.3 Einfache Überwachung/Protokollierung	**Ja**	**Nein**
9.3.1 Log Viewer Die Lösung sollte einen Log Viewer unterstützen, der eine einfache Anzeige und Filterung der Protokolldateien erlaubt.		
9.3.2 Export von Protokolldateien Der Export von gefilterten bzw. kompletten Protokolldateien sollte mit einem Mausklick über Syslog möglich sein.		
9.3.3 Enterprise MIB Es sollte eine produktspezifische MIB vorhanden sein, um den Austausch mit Management-Tools anderer Anbieter zu ermöglichen.		
9.3.4 Grafische Anzeige Die Lösung sollte die Anzeige der Systemkennzahlen in der Hauptverwaltungskonsole unterstützen, damit Schlüsseldaten leichter und schneller angezeigt und analysiert werden können.		
9.3.5 Berichte zu Datenströmen Die Lösung sollte die beiden Standards NetFlow und IPFIX unterstützen, damit Datenstrom- und Deep Packet Inspection-Berichte an externe Partner weitergeleitet werden können.		

10 WLAN-Features

Im Idealfall sollte die Lösung Unterstützung für WLAN-Umgebungen bieten und den WLAN-Benutzern dabei sämtliche Sicherheitsservices zur Verfügung stellen.

10.1 WLAN-Unterstützung	Ja	Nein
10.1.1 Integriertes WLAN Für den Einsatz in kleinen Unternehmen: Integrierte WLAN-Unterstützung für die neueste Generation von Wireless-Protokollen.		
10.1.2 Verteiltes WLAN Die Next-Generation Firewall agiert als Wireless Controller für Konfigurationen mit Wireless Access Points.		
10.1.3 Mehrere SSIDs Die Firewall sollte mehrere isolierte SSIDs für den internen und externen Drahtlosverkehr zur Verfügung stellen.		
10.1.4 Gastzugriff Die Firewall sollte eine individuelle Authentifizierung von Gastbenutzern über interne und/oder externe Repositorys ermöglichen.		
10.1.5 Sicherheit in drahtlosen Netzwerken Deep Packet Inspection und Anwendungskontrolle für den gesamten Wireless-Verkehr, Wireless IDS und MAC-Enforcement.		
10.1.6 Fairnet Die Firewall sollte sicherstellen, dass alle Wireless-Benutzer gleich viel Bandbreite erhalten (Lastverteilung für Wireless Clients).		

11 Stabilität und Erfahrung des Unternehmens

Idealerweise sollte die Lösung von einem etablierten Technologieanbieter stammen, der einen ausgezeichneten Kundensupport bietet und gute Analystenbewertungen vorweisen kann.

Stabilität und Erfahrung des Unternehmens	Ja	Nein
11.1 Referenzkunden Kundenreferenzen und Fallstudien des Unternehmens sind leicht zugänglich.		
11.2 Patente Das Unternehmen verfügt über ein überzeugendes Patentportfolio, das die Schlüsseltechnologien seiner Next-Generation Firewall schützt.		
11.3 Gute Analystenbewertungen Das Unternehmen lässt seine Vision und deren Umsetzung laufend durch anerkannte Analysten validieren.		
11.4 Branchenzertifizierungen Das Unternehmen besitzt Branchenzertifizierungen von renommierten Instituten (z. B. ICSA) für seine Next-Generation Firewall-Technologie.		
11.5 Weltweiter Support Das Unternehmen bietet optional weltweiten Support durch qualifizierte Techniker rund um die Uhr.		

DELL SonicWALL