Network Security Appliance Serie

Firewall der nächsten Generation

Organisationen jeder Größe sind für den Zugriff auf interne und externe geschäftskritische Anwendungen auf ihre Netzwerke angewiesen. Während Fortschritte im Netzwerkbetrieb weiterhin erhebliche Vorteile mit sich bringen, sehen Organisationen sich zunehmend mit raffinierten und finanziell motivierten Angriffen konfrontiert, die auf Unterbrechung der Kommunikation, Beeinträchtigung der Leistung und Kompromittierung von Daten abzielen. Böswillige Angriffe überwinden veraltete, auf Stateful Packet Inspection basierende Firewalls mit erweiterten Exploits auf Anwendungsebene. Einzelprodukte fügen Sicherheitsebenen hinzu, sind aber kostspielig, schwer zu verwalten, nur eingeschränkt in der Lage, Netzwerkmissbrauch zu kontrollieren, und unwirksam gegenüber den neuesten, in mehrere Richtungen zielenden Angriffen.

Mit einem einzigartigen Multi-Core-Design und der patentierten Reassembly-Free Deep Packet Inspection® (RFDPI) Technologie* bietet die Dell SonicWALL® Network Security Appliance (NSA) Serie mit Firewalls der nächsten Generation umfassenden Schutz ohne Kompromisse bei der Netzwerkleistung. Die NSA Serie mit niedriger Latenz überwindet die Beschränkungen vorhandener Sicherheitslösungen: Jedes Paket wird in seiner Gesamtheit in Echtzeit nach aktuellen internen und externen Bedrohungen durchsucht. Die NSA Serie bietet Angriffsvermeidung, Malware-Schutz, intelligente Anwendungssteuerung und Anwendungskontrolle mit Visualisierung bei bahnbrechender Leistung. Mit erweitertem Routing, Stateful-Hochverfügbarkeit und IPsec- und SSL-VPN-Technologie mit Hochgeschwindigkeit bringt die NSA Serie mehr Sicherheit, Zuverlässigkeit, Funktionalität und Produktivität in Zweigniederlassungen, zentrale Standorte und Netzwerke in dezentralen Unternehmen mittlerer Größe und minimiert gleichzeitig Kosten und Komplexität.

Die NSA Serie umfasst Dell SonicWALL NSA 220, NSA 220 Wireless-N, NSA 250M, NSA 250M Wireless-N, NSA 2400, NSA 3500 und NSA 4500 und bietet eine skalierbare Palette von Lösungen, die die Netzwerksicherheitsanforderungen jeder Organisation erfüllen.

- **Firewall der nächsten Generation**
- **Skalierbare Multi-Core-Hardware und Reassembly-Free Deep Packet Inspection**
- **Intelligente Anwendungssteuerung und Anwendungskontrolle mit Visualisierung**
- **Stateful-Hochverfügbarkeit und Lastausgleich**
- **Hohe Leistung und niedrigere Gesamtbetriebskosten**
- **Netzwerkproduktivität**
- **Erweiterte Routing-Services und Netzwerkbetrieb**
- **Standardbasiertes Voice over IP (VoIP)**
- **Dell SonicWALL Clean Wireless**
- **Integrierte Servicequalität (QoS)**
- **Integrierte Modulunterstützung**

*US- Patente 7.310.815, 7.600.257, 7.738.380, 7.835.361, 7.991.723

Eigenschaften und Vorteile

Firewall der nächsten Generation mit Eigenschaften, die Angriffsvermeidung, Gateway-Virenschutz, Spyware-Schutz und URL-Filterung mit intelligenter Anwendungssteuerung sowie Anwendungskontrolle und SSL-Entschlüsselung integrieren, um das Eindringen von Bedrohungen in das Netzwerk zu verhindern und für eine präzise Anwendungssteuerung ohne Kompromisse bei der Leistung zu sorgen.

Skalierbare Multi-Core-Hardware und Reassembly-Free Deep Packet Inspection suchen und beseitigen Bedrohungen durch Dateien beliebiger Größe mit einer Latenz von nahezu null über Tausende von Verbindungen mit Wire-Speed.

Intelligente Anwendungssteuerung und Anwendungskontrolle mit Visualisierung bieten genaue Kontrolle und Echtzeit-Visualisierung von Anwendungen, um Bandbreitenpriorisierung und maximale Netzwerksicherheit und Produktivität zu gewährleisten.

Stateful-Hochverfügbarkeit und Lastausgleich mit Eigenschaften, die die Gesamtnetzwerkbandbreite maximieren und die Verfügbarkeit des Netzwerks nahtlos aufrechterhalten. Sie bieten unterbrechungsfreien Zugriff auf geschäftskritische Ressourcen und gewährleisten, dass VPN-Tunnel und anderer Netzwerkdatenverkehr bei einem Failover nicht unterbrochen werden.

Hohe Leistung und niedrigere Gesamtbetriebskosten werden erzielt durch die gleichzeitige Nutzung der Verarbeitungsleistung mehrerer Kerne, um den Datendurchsatz erheblich zu steigern und Fähigkeiten für die parallele Prüfung bereitzustellen und gleichzeitig den Stromverbrauch zu senken.

Netzwerkproduktivität wird erhöht, da IT nicht autorisierte, nicht produktive und nicht mit der Tätigkeit zusammenhängende Anwendungen und Websites wie Facebook® oder YouTube® identifizieren und drosseln oder blockieren kann. Darüber hinaus kann der WAN-Datenverkehr bei der Integration mit Dell SonicWALL WAN Acceleration Appliance (WXA) Lösungen optimiert werden.

Erweiterte Routing-Services und Netzwerkbetrieb mit Eigenschaften, die 802.1q-VLANs, Multi-WAN-Failover, zonen- und objektbasierte Verwaltung, Lastausgleich, erweiterte NAT-Modi und mehr umfassen. Sie bieten punktgenaue Flexibilität bei der Konfiguration und umfassenden Schutz nach Ermessen des Administrators.

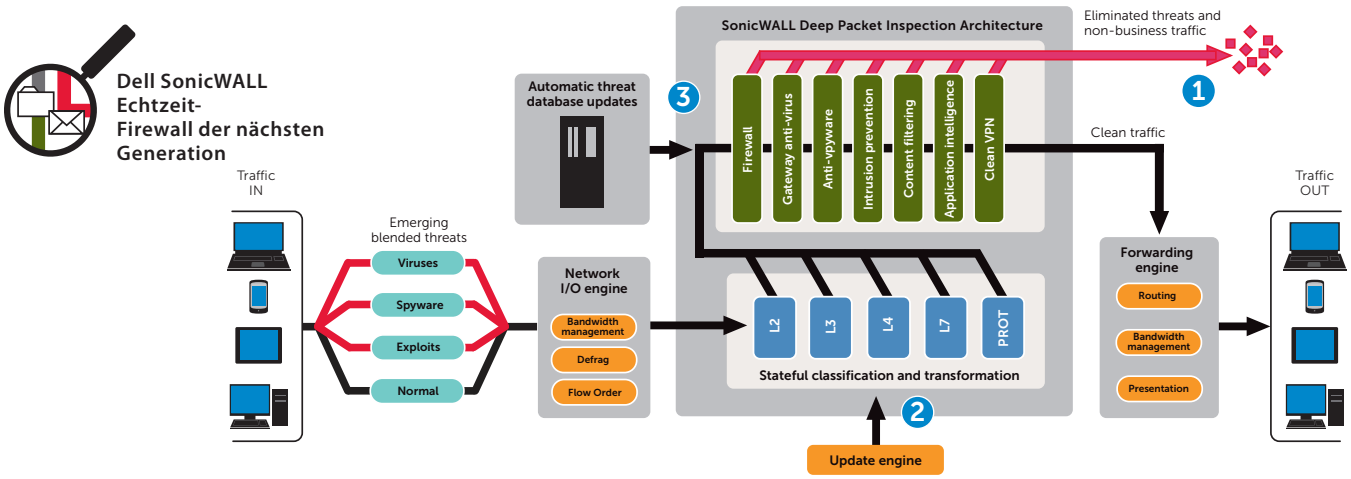
Standardbasiertes Voice over IP (VoIP) mit Fähigkeiten, die höchste Sicherheit für jedes Element der VoIP-Infrastruktur bieten, von Kommunikationssystemen bis zu VoIP-fähigen Geräten, zu denen SIP-Proxys, H.323-Gatekeeper und Call Server gehören.

Dell SonicWALL Clean Wireless, optional integriert in Dual-Band Wireless-Modelle oder über Dell SonicWALL SonicPoint Wireless-Zugriffspunkte, bietet leistungsstarkes und sicheres 802.11a/b/g/n 3x3 MIMO Wireless und ermöglicht die Suche nach unbefugten Wireless-Zugriffspunkten gemäß PCI DSS.

Integrierte Servicequalität (QoS) mit Eigenschaften, die den Branchenstandard 802.1p und DSCP CoS-Kennzeichner (Differentiated Services Code Points Class of Service) nutzen, um leistungsstarkes und flexibles Bandbreitenmanagement bereitzustellen, das für VoIP, Multimedia-Inhalte und geschäftskritische Anwendungen von entscheidender Bedeutung ist.

Integrierte Modulunterstützung auf NSA 250M und NSA 250M Wireless-N Appliances verringert Anschaffungs- und Wartungskosten durch Gerätekonsolidierung und erhöht die Flexibilität bei der Bereitstellung.

Dynamische Sicherheitsarchitektur und Verwaltung



Erstklassiger Schutz vor Bedrohungen

1 Dell SonicWALL Deep Packet Inspection schützt vor Netzwerkrisiken wie Viren, Würmern, Trojanern, Spyware, Phishing-Angriffen, aufkommenden Bedrohungen und Internet-Missbrauch. Application Intelligence and Control sorgt in hohem Umfang für zusätzliche Steuerelemente zur Verhinderung von Datenlecks und Verwaltung der Bandbreite auf der Anwendungsebene.

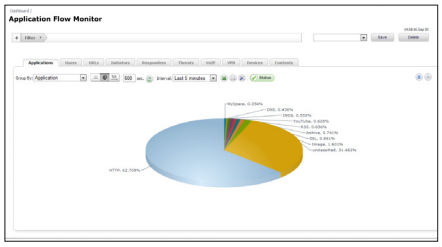
2 Die Technologie Dell SonicWALL Reassembly-Free Deep Packet Inspection (RFDPI) nutzt die Multi-Core-Architektur von Dell SonicWALL, um Pakete in Echtzeit zu durchsuchen, ohne den Datenverkehr im Arbeitsspeicher zum Erliegen zu bringen.

Durch diese Funktionalität ist es möglich, Bedrohungen in Dateien jeder Größe und über eine unbegrenzte Zahl paralleler Verbindungen ohne Unterbrechung zu identifizieren und zu beseitigen.

3 Die Dell SonicWALL NSA Serie bietet dynamischen Netzwerkschutz durch fortlaufende, automatisierte Sicherheitsupdates und schützt so vor aufkommenden und sich entwickelnden Bedrohungen, ohne dass Eingriffe durch Administratoren erforderlich sind.

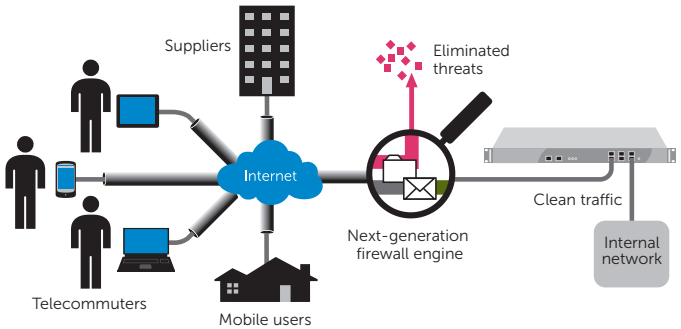
Application Intelligence and Control

Dell SonicWALL Application Intelligence and Control bietet genaue Kontrolle und Echtzeit-Visualisierung von Anwendungen, um Bandbreitenpriorisierung und maximale Netzwerksicherheit und Produktivität zu gewährleisten. Diese Funktion, die in Dell SonicWALL Firewalls der nächsten Generation integriert ist, verwendet Dell SonicWALL RFDPI-Technologie zur Identifizierung und Kontrolle verwendeter Anwendungen mit benutzerdefinierten vordefinierten Anwendungskategorien, beispielsweise soziale Medien oder Spiele – unabhängig von Port oder Protokoll. Dell SonicWALL Application Traffic Analytics bietet Echtzeit- und gründliche historische Analysen von Daten, die über die Firewall übertragen werden, einschließlich Anwendungsaktivitäten nach Benutzer.



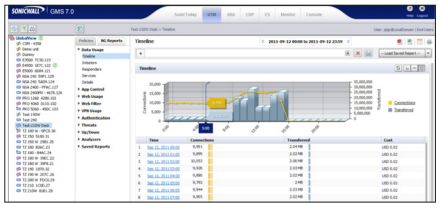
Dell SonicWALL Clean VPN

Dell SonicWALL Clean VPN™ sichert die Integrität des VPN-Zugriffs für Remote-Geräte, einschließlich derjenigen, die iOS oder Android ausführen. Dazu wird eine Vertrauensstellung für Remote-Benutzer und diese Endpunktgeräte hergestellt, und es werden Anti-Malware-Sicherheitsservices, Angriffsvermeidung sowie intelligente Anwendungssteuerung und Anwendungskontrolle angewendet, um den Transport von bösartigen Bedrohungen zu verhindern.



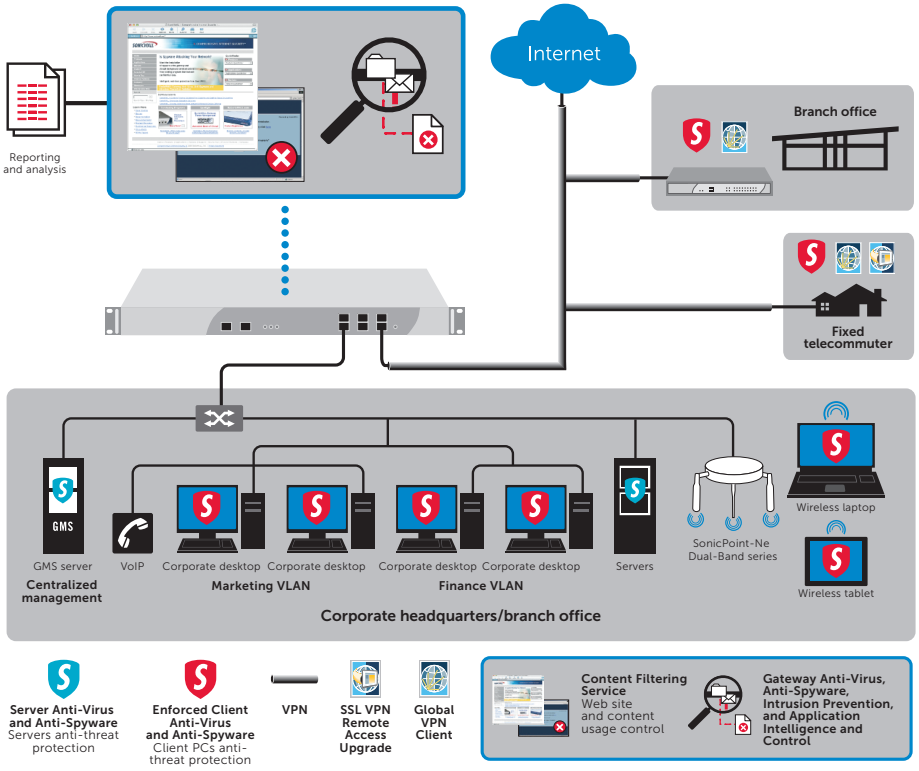
SonicWALL

Zentralisierte Richtlinienverwaltung
Die Network Security Appliance Serie kann mit dem SonicWALL Global Management System verwaltet werden. Es bietet flexible, leistungsstarke und intuitive Tools für die Verwaltung von Konfigurationen, die Anzeige von Überwachungsmetriken in Echtzeit und die Integration von Richtlinien und Compliance-Berichten und die Analyse von Anwendungsdatenverkehr – all das von einem zentralen Standort.



Flexible, anpassbare Bereitstellungsoptionen – NSA Serie auf einen Blick

Jede SonicWALL Network Security Appliance Lösung bietet Schutz durch Firewalls der nächsten Generation und nutzt ein bahnbrechendes Multi-Core-Hardwaredesign und Reassembly-Free Deep Packet Inspection für internen und externen Netzwerkschutz ohne Kompromisse bei der Netzwerkleistung. Jedes Produkt der NSA Serie kombiniert Hochgeschwindigkeits-Angriffsvermeidung, Datei- und Inhaltsprüfung und leistungsstarke Anwendungssteuerung sowie Anwendungskontrolle mit einer Vielzahl von Funktionen für erweiterten Netzwerkbetrieb und flexible Konfiguration. Die NSA Serie bietet eine zugängliche und erschwingliche Plattform, die in einer Vielzahl von Unternehmens-, Niederlassungs- und verteilten Netzwerkumgebungen einfach bereitzustellen und zu verwalten ist.



- Die SonicWALL NSA 4500 ist ideal für große verteilte Umgebungen und Unternehmensumgebungen mit einem zentralen Standort, die hohe Datendurchsatzkapazität und Leistung erfordern.
- Die SonicWALL NSA 3500 ist ideal für verteilte, Niederlassungs- und Unternehmensumgebungen, die beträchtliche Datendurchsatzkapazität und Leistung benötigen.
- Die SonicWALL NSA 2400 ist ideal für Niederlassungsumgebungen und Umgebungen in kleinen und mittelständischen Unternehmen, die sich um Datendurchsatzkapazität und Leistung sorgen.
- Die SonicWALL NSA 220, NSA 220 Wireless-N, NSA 250M und NSA 250M Wireless-N sind ideal für Niederlassungsstandorte in verteilten Unternehmensumgebungen, Umgebungen in kleinen und mittelständischen Unternehmen und Einzelhandelsumgebungen

Sicherheitsservices und Upgrades

Die Dell Services Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Application Intelligence and Control sorgen für intelligenten Echtzeit-Netzwerksicherheitsschutz vor raffinierten Angriffen auf Anwendungsebene und inhaltsbasierten Angriffen wie Viren, Spyware, Würmern und Trojanern sowie Schutz vor Schwachstellen in der Software, beispielsweise Pufferüberlauf. Application Intelligence and Control bietet eine Suite mit konfigurierbaren Tools zur Verhinderung von Datenlecks, präzise Steuerelemente auf Anwendungsebene sowie Tools für die Visualisierung des Netzwerkdatenverkehrs.

Enforced Client Anti-Virus and Anti-Spyware garantiert gemeinsam mit Dell SonicWALL Firewalls und wahlweise McAfee® oder Kaspersky® Technologie, dass auf allen Endpunkten die neuesten Versionen der Software für Viren- und Spyware-Schutz installiert und aktiv sind.

Content Filtering Service erzwingt Schutz- und Produktivitätsrichtlinien mit einer innovativen Bewertungsarchitektur, bei der eine dynamische Datenbank eingesetzt wird, um bis zu 56 Kategorien mit unzulässigen Webinhalten zu blockieren.

Analyzer ist ein flexibles, benutzerfreundliches webbasiertes Tool zur Analyse von Anwendungsdatenverkehr und Erstellung von Berichten. Es bietet aussagekräftige Einblicke, in Echtzeit und historisch, in den Zustand, die Leistung und die Sicherheit des Netzwerks.

Virtual Assist ist ein Remote-Support-Tool, mit dem ein Techniker die Steuerung eines PCs oder Notebooks übernehmen kann, um technische Remote-Unterstützung zu leisten. Mit der entsprechenden Berechtigung kann der Techniker sofort über einen Webbrowser auf einen Computer zugreifen. So kann ein Problem auf einfache Weise remote diagnostiziert und behoben werden, ohne dass ein vorinstallierter "Fat Client" notwendig ist.

Dynamic Support-Services sind je nach Kundenanforderung während der wöchentlichen Arbeitszeiten (8x5) oder rund um die Uhr (24x7) verfügbar. Zu den Merkmalen gehören erstklassiger technischer Support, wichtige Firmware-Updates und -Upgrades, Zugriff auf umfangreiche elektronische Tools und rechtzeitiger Austausch von Hardware, damit Organisationen ihre Dell SonicWALL Investition optimal nutzen können.

Global VPN-Client-Upgrades nutzen einen Softwareclient, der auf Windows-Computern installiert ist, und erhöhen die Produktivität von Mitarbeitern durch sicheren Zugriff auf E-Mail, Dateien, Intranets und Anwendungen für Remote-Benutzer.

SSL-VPN-Remote-Zugriff-Upgrades bieten ohne Client Remote-Zugriff auf Netzwerkebene für PCs, Macs und Linux Systeme. Mit integrierter SSL-VPN-Technologie ermöglichen Dell SonicWALL Firewall-Appliances nahtlosen und sicheren Remote-Zugriff auf E-Mail, Dateien, Intranets und Anwendungen von einer Vielzahl von Clientplattformen über NetExtender, einem Lightweight-Client, der auf den Rechner des Benutzers übertragen wird.

Dell SonicWALL® Mobile Connect™, eine einzelne, vereinheitlichte Client-App für Apple® iOS und Google® Android™, bietet Benutzern von Smartphones und Tablet-PCs überragenden Netzwerkzugriff auf Unternehmensressourcen und akademische Ressourcen über verschlüsselte SSL-VPN-Verbindungen.

Comprehensive Anti-Spam Service (CASS) bietet kleinen und mittelständischen Unternehmen umfassenden Schutz vor Spam und Viren bei sofortiger Bereitstellung über vorhandene Dell SonicWALL Firewalls. CASS beschleunigt die Bereitstellung, vereinfacht die Verwaltung und verringert den Overhead durch Konsolidierung von Lösungen, mit einem Mausklick aufrufbare Anti-Spam-Services und eine erweiterte Konfiguration in nur zehn Minuten.

Deep Packet Inspection für SSL-verschlüsselten Datenverkehr (DPI-SSL) entschlüsselt sowohl eingehenden als auch ausgehenden HTTPS-Datenverkehr und durchsucht ihn mit Dell SonicWALL RFDPI auf Bedrohungen. Der Datenverkehr wird anschließend wieder verschlüsselt und an sein ursprüngliches Ziel gesendet, wenn keine Bedrohungen oder Schwachstellen entdeckt wurden.

Daten

Firewall	NSA 220/W	NSA 250M/W	NSA 2400	NSA 3500	NSA4500
SonicOS Version	SonicOS 5.8.1.1		SonicOS Enhanced 5.6 (oder höher)		
Stateful-Durchsatz[1]	600 Mbit/s	750 Mbit/s	775 Mbit/s	1,5 Gbit/s	2,75 Gbit/s
GAV-Leistung[2]	115 Mbit/s	140 Mbit/s	160 Mbit/s	350 Mbit/s	690 Mbit/s
IPS-Leistung[2]	195 Mbit/s	250 Mbit/s	275 Mbit/s	750 Mbit/s	1,4 Gbit/s
Volle DPI-Leistung[2]	110 Mbit/s	130 Mbit/s	150 Mbit/s	240 Mbit/s	600 Mbit/s
IMIX-Leistung[2]	180 Mbit/s	210 Mbit/s	235 Mbit/s	580 Mbit/s	700 Mbit/s
Max. Anz. Verbindungen[3]	85.000	110.000	225.000	325.000	500.000
Max. Anz. DPI-Verbindungen	32.000	64.000	125.000	175.000	250.000
Neue Verbindungen/s	2200	3000	4000	7000	10.000
Unterstützte Knoten	Unbeschränkt				
Schutz vor Denial of Service-Angriffen	22 Klassen mit DoS-, DDoS- und Scan-Angriffen				
Unterstützte SonicPoints (maximal)	16	24	32	48	64
VPN					
3DES/AES-Durchsatz[5]	150 Mbit/s	200 Mbit/s	300 Mbit/s	625 Mbit/s	1,0 Gbit/s
VPN-Tunnel von Standort zu Standort	25	50	75	800	1500
Mitgelieferte Global VPN-Clientlizenzen (maximal)	2 (25)	2 (25)	10 (250)	50 (1000)	500 (3000)
Mitgelieferte SSL-VPN-Lizenzen (maximal)	2 (15)	2 (15)	2 (25)	2 (30)	2 (30)
Secure Virtual Assist mitgeliefert (maximal)	1 30-Tage-Testversion (5)	1 30-Tage-Testversion (5)	1 (5)	2 (10)	2 (10)
Verschlüsselung/Authentifizierung/DH-Gruppe	DES, 3DES, AES (128, 192, 256-Bit), MD5, SHA-1/DH-Gruppen 1, 2, 5, 14				
Schlüsselaustausch	IKE-Schlüsselaustausch, IKEv2, manueller Schlüssel, PKI (X.509), L2TP over IPsec				
Routenbasiertes VPN	Ja (OSPF, RIP)				
Zertifikatsunterstützung	VeriSign, Thawte, Cybertrust, RSA Keon, Entrust und Microsoft CA für Dell SonicWALL-zu-Dell SonicWALL-VPNs, SCEP				
Dead Peer Detection	Ja				
DHCP über VPN	Ja				
IPsec-NAT-Traversal	Ja				
Redundantes VPN-Gateway	Ja				
Unterstützte Global VPN-Clientplattformen	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32/64-Bit, Windows 7 32/64-Bit				
Unterstützte SSL-VPN-Plattformen	Microsoft® Windows 2000/XP/Vista 32/64-Bit/Windows 7, Mac 10.4+, Linux FC 3+/Ubuntu 7+/OpenSUSE				
Unterstützte Mobile Connect Plattformen	iOS 4.2 und höher, Android™ 4.0 und höher				
Sicherheitsservices					
Deep Packet Inspection Service	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Application Intelligence and Control				
Content Filtering Service	(CFS) HTTP URL,HTTPS IP, Schlüsselwort- und Inhaltssuche, ActiveX, Java Applet und Cookie-Blockierung Bandbreitenmanagement nach Filterkategorien, weiße/schwarze Listen				
Von Gateway erzwungener Client-Viren- und -Spyware-Schutz	McAfee® oder Kaspersky®				
Umfassender Anti-Spam-Service[1]	Unterstützt				
Application Intelligence and Control	Bandbreitenmanagement und -kontrolle für Anwendungen, Priorisierung oder Blockierung von Anwendungen nach Signaturen, Kontrolle von Dateiübertragungen, Suche nach Schlüsselwörtern oder Phrasen				
DPI SSL[6]	Bietet die Möglichkeit, HTTPS-Datenverkehr transparent zu entschlüsseln, diesen Datenverkehr mit der Dell SonicWALL Technologie Deep Packet Inspection (GAV/AS/IPS/Application Intelligence/CFS) nach Bedrohungen zu durchsuchen und dann den Datenverkehr wieder zu verschlüsseln und an sein Ziel zu senden, wenn keine Bedrohungen oder Schwachstellen gefunden wurden. Diese Funktion kann für Clients und Server eingesetzt werden.				
Netzwerkbetrieb					
IP-Adressenzuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay				
NAT-Modi	1-zu-1, 1-zu-viele, viele-zu-1, viele-zu-viele, Flexible NAT (überlappende IPs), PAT, transparenter Modus				
VLAN-Schnittstellen (802.1q)	25	35	25	50	200
Routing	OSPF, RIPv1/v2, statische Routen, richtlinienbasiertes Routing, Multicast				
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p				
IPv6	Ja				
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminal Services, Citrix				
Benutzer interne Datenbank/einmaliges Anmelden	100/100 Benutzer	150/150 Benutzer	250/250 Benutzer	300/500 Benutzer	1000/1000 Benutzer
VoIP	Voll H.323v1-5-kompatibel, SIP, Gatekeeper-Unterstützung, Management der ausgehenden Bandbreite, VoIP über WLAN, Deep Inspection Security, vollständige Interoperabilität mit den meisten VoIP-Gateway- und Kommunikationsgeräten				
System					
Zonensicherheit	Ja				
Zeitpläne	Einmal, periodisch				
Objekt-/gruppenbasierte Verwaltung	Ja				
DDNS	Ja				
Verwaltung und Überwachung	Web-GUI (HTTP, HTTPS), Befehlszeile (SSH, Konsole), SNMP v2: globale Verwaltung mit Dell SonicWALL GMS				
Protokollierung und Berichterstellung	Analyzer, lokales Protokoll, Syslog, Solera Networks, NetFlow v5/v9, IPFIX mit Erweiterungen, Echtzeit-Visualisierung				
Hochverfügbarkeit	Optional aktiv/passiv mit State Sync				
Lastausgleich	Ja (abgehend mit prozentbasierter, Round-Robin- und Spillover-Lastverteilung; eingehend mit RoundRobin- oder zufälliger Verteilung, Sticky IP, blockweiser Neuzuordnung und symmetrischer Neuzuordnung)				
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Wireless-Standards	802.11 a/b/g/n, WPA2, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS				
Unterstützung von WAN-Beschleunigung[8]	Ja				
Integriertes Wireless-LAN					
Standards	802.11a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS		–	–	–
VAPs (Virtual Access Points)5– Diversity-Antennen (5 dBi)	Extern dreifach, abnehmbar		–	–	–
Sendeleistung – 802.11a/ 802.11b/802.11g	15,5 dBm max./18 dBm max./ 17 dBM bei 6 Mbit/s, 13 dBM bei 54 Mbit/s		–	–	–
Sendeleistung – 802.11n (2,4 GHz)/ 802.11n (5,0 GHz)	19 dBm MCS 0, 11 dBm MCS 15/17 dBm MCS 0, 12 dBm MCS 15		–	–	–
Empfangsempfindlichkeit – 802.11a/802.11b/802.11g	-95 dBm MCS 0, -81 dBm MCS 15/-90 dBm bei 11 Mbit/s / -91 dBm bei 6Mbit/s, -74 dBm bei 54 Mbit/s		–	–	–
Empfangsempfindlichkeit – 802.11n (2,4 GHz)/802.11n (5,0 GHz)	-89 dBm MCS 0, -70 dBm MCS 15/ -95 dBm MCS 0, -76 dBm MCS 15		–	–	–
Hardware					
Schnittstellen	(7) 10/100/1000 Kupfer-Gigabit-Ports, 2 USB, 1 Konsolenschnittstelle	(5) 10/100/1000 Kupfer-Gigabit-Ports, 2 USB, 1 Konsolenschnittstelle Modulsteckplatz	(6) 10/100/1000 Kupfer-Gigabit-Ports, 1 Konsolenschnittstelle, 2 USB		
Modul	Nein	Ja	Nein	Nein	Nein
Arbeitsspeicher (RAM)	512 MB				
Flash-Speicher	32 MB Compact Flash		512 MB Compact Flash		
3G Wireless/Modem[7]*	Mit 3G/4G-USB-Adapter oder Modem		–	Mit 3G/4G-USB-Adapter oder Modem	
Netzteil	36 W extern		Ein 180-W-ATX-Netzteil		
Lüfter	Kein Lüfter/1 interner Lüfter	2 interne Lüfter	2 Lüfter		
Eingangsspannung	10-240 V, 50-60 Hz				
Max. Stromverbrauch	11 W/15 W	12 W/16 W	42 W	64 W	66 W
Gesamtwärmeabgabe	37 BTU/50 BTU	41 BTU/55 BTU	144 BTU	219 BTU	225 BTU
Zertifizierungen	VPNC, ICSA Firewall 4.1		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1, IPv6 Phase 2		
Ausstehende Zertifizierungen	EAL4+, FIPS 140-2 Level 2, IPv6 Phase 1, IPv6 Phase 2		–		
Formfaktor und Abmessungen	1U Rack-Montagefähigkeit/ 18,10 x 3,81 x 26,67 cm 7,125 x 1,5 x 10,5 Zoll/		1U Rack-Montagefähigkeit/ 43,18 x 26 x 4,44 cm 17 x 10,25 x 1,75 Zoll/		1U Rack-Montagefähigkeit/ 43,18 x 33,65 x 4,44 cm 17 x 13,25 x 1,75 Zoll
Gewicht	0,88 kg/1,95 lb/ 0,97 kg/2,15 lb/	1,38 kg/3,05 lb/ 1,43 kg/3,15 lb/	3,65 kg/8,05 lb/		5,14 kg/11,30 lb/
WEEE-Gewicht	V 1,38 kg/3,05 lb/ 1,56 kg/3,45 lb/	2,0 kg/4,4 lb/ 2,11 kg/4,65 lb	3,65 kg/8,05 lb/		5,14 kg/11,30 lb/
Wichtige Standards	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE				
Umgebung	0-40 °C/40-105 °F		5-40 °C/40-105 °F		
MTBF	28 Jahre/15 Jahre	23 Jahre/14 Jahre	14,3 Jahre	14,1 Jahre	14,1 Jahre
Feuchtigkeit	5-95 % nicht kondensierend		10-90 % nicht kondensierend		

[1] Testmethoden: Maximalleistung auf Basis von RFC 2544 (für Firewall). Die tatsächliche Leistung kann je nach Netzwerkbedingungen und aktivierten Services variieren. [2] Volle DPI-Leistung/ Gateway-Viren-/Spyware-Schutz/IPS-Durchsatz gemessen mit Spirent WebAvalanche HTTP-Leistungstest nach Branchenstandard und Ixia Testtools. Getestet wurde mit mehreren Datenströmen über mehrere Portpaare. [3] Die tatsächliche maximale Verbindungsanzahl ist niedriger, wenn Services für Firewalls der nächsten Generation aktiviert sind. [5] VPN-Durchsatz gemessen mit UDP-Datenverkehr mit einer Paketgröße von 1280 Byte gemäß RFC 2544. [6] Unterstützt auf der NSA 3500 und höher. [7] Nicht verfügbar auf NSA 2400. *USB-3G-Karte und Modem nicht enthalten. Informationen zu unterstützten USB-Geräten finden Sie unter http://www.Dell SonicWALL.com/us/products/cardsupport.html. [1] Der Comprehensive Anti-Spam Service unterstützt eine unbeschränkte Anzahl von Benutzern, wird aber für 250 Benutzer oder weniger empfohlen. [8] Mit Dell SonicWALL WXA Series Appliance.

Network Security Appliance 4500
01-SSC-7012

NSA 4500 TotalSecure* (1 Jahr)
01-SC-7032

Network Security Appliance 3500
01-SSC-7016

NSA 3500 TotalSecure* (1 Jahr)
01-SC-7033

Network Security Appliance 2400
01-SSC-7020

NSA 2400 TotalSecure* (1 Jahr)
01-SC-7035

Network Security Appliance 250M
01-SSC-9755

Network Security Appliance 250M Wireless-N
01-SSC-9758 (international)

Network Security Appliance 250M TotalSecure*
01-SSC-9747

Network Security Appliance 250M Wireless-N TotalSecure*
01-SSC-9749 (international)

Network Security Appliance 220
01-SSC-9750

Network Security Appliance 220 Wireless-N
01-SSC-9753 (international)

Network Security Appliance 220 TotalSecure*
01-SSC-9744

Network Security Appliance 220 Wireless-N TotalSecure*
01-SSC-9746 (international)

Weitere Informationen zu Dell SonicWALL Netzwerksicherheitslösungen finden Sie unter **www.sonicwall.com**.

*Enthält für ein Jahr Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Application Intelligence and Control, Content Filtering Service und Dynamic Support Services rund um die Uhr.

Security Monitoring Services von Dell SecureWorks sind für diese Appliance-Serie erhältlich. Weitere Informationen erhalten Sie unter **www.dell.com/secureworks**.

Zertifizierungen

Common Criteria EAL4+ CERTIFIED

FIPS 140-2 VALIDATED

ICSA labs CERTIFIED FIREWALL - CORPORATE

DELL SonicWALL