

- Next-Generation Firewall
- 10-GbE-Konnektivität
- Leistungsstarke Intrusion Prevention
- Application Intelligence, Control and Visualization
- Reassembly-Free Deep Packet Inspection-Technologie
- Flexible Implementierung
- Deep Packet Inspection von SSL-verschlüsseltem Verkehr (DPI SSL)
- SonicWALL Global Response Intelligent Defense (GRID)-Netzwerk
- WAN-Beschleunigung
- Remote-Zugriff für mobile Unternehmen

Mitarbeiter in Unternehmen nutzen heute eine Vielzahl von Anwendungen, die über das Firmennetzwerk oder die Cloud bereitgestellt werden. Dabei kann es sich sowohl um produktive Geschäftsanwendungen wie auch um produktivitätshemmende – und oftmals sogar gefährliche – Ablenkungen handeln. Entscheidend ist hier, dass unternehmenskritische Anwendungen bei der Bandbreitenzuteilung priorisiert werden, während Social Media-Anwendungen oder Spiele in ihrem Verbrauch eingeschränkt oder komplett gesperrt werden. Herkömmliche Stateful Packet Inspection-Firewalls scannen nur Ports und Protokolle, lassen Anwendungen aber unberücksichtigt und können somit nicht zwischen unbedenklichem und verdächtigem Datenverkehr unterscheiden.

Die Lösungen der SonicWALL® E-Class Network Security Appliance (NSA)-Serie bieten Enterprise-Performance mit eng integrierten Intrusion Prevention-Funktionen, Malware-Schutz sowie einem effektiven Tool zur Überwachung, Kontrolle und Visualisierung von Anwendungen. Mit ihrer leistungsstarken Multicore-Hardware-Plattform in Kombination mit SonicWALLs patentierter Reassembly-Free Deep Packet Inspection™-Technologie* können die E-Class NSA-Appliances Tausende unterschiedlicher Anwendungen analysieren und kontrollieren, selbst wenn die Daten SSL-verschlüsselt übertragen werden. Dank integrierter Reporting-Funktionen zur Analyse des Anwendungsverkehrs liefert die E-Class NSA-Serie aussagekräftige Daten über die Netzwerknutzung.

Mit den E-Class NSA Appliances E8510, E8500, E7500, E6500 und E5500 bietet SonicWALL eine breite Palette an skalierbaren Lösungen für anspruchsvolle Enterprise-Implementierungen in Datacentern, Campus-Netzwerken und verteilten Umgebungen. Bei Implementierung als Inline-Lösung nutzt die E-Class NSA-Serie die bestehende Infrastruktur und schafft zusätzliche Sicherheit und Transparenz im Netzwerk. Werden die Appliances als Security Gateway eingesetzt, lassen sich mit ihnen zusätzliche Enterprise-Funktionen wie Secure Remote Access und Hochverfügbarkeit bereitstellen.

Die E-Class NSA-Serie ist ein zentraler Bestandteil der Enterprise-Class-Produkte und Services in SonicWALLs Network Security-, Email Security- und Secure Remote Access-Portfolio.

Funktionen und Vorteile

Die **Next-Generation Firewall** von SonicWALL mit Reassembly-Free Deep Packet Inspection integriert Intrusion Prevention und Malware-Schutz mit erweiterter Application Intelligence und Anwendungskontrolle sowie Echtzeit-Visualisierungsfunktionen in einer Lösung.

10-GbE-Konnektivität bei der NSA E8510 erlaubt eine Implementierung in Umgebungen mit 10-GbE-Infrastruktur.

Leistungsstarke Intrusion Prevention. Schützt vor einer Vielzahl von netzwerkbasierter Bedrohungen auf der Anwendungsebene. Paket-Payloads werden auf Würmer, Trojaner, Software-Schwachstellen, Anwendungs-Exploits und sonstigen bösartigen Code überprüft.

Application Intelligence, Control and Visualization. Bietet eine granulare Überwachung und Echtzeit-Visualisierung von Anwendungen, um eine Priorisierung der Bandbreite zu ermöglichen und maximale Netzwerksicherheit und Produktivität zu gewährleisten.

Reassembly-Free Deep Packet Inspection-Technologie. Erkennt Tausende von Anwendungen sowie Millionen von Malware-Bedrohungen und sorgt so für einen automatischen und nahtlosen Netzwerkschutz. Daneben werden Hunderttausende gleichzeitiger Verbindungen über sämtliche Ports hinweg geprüft – ohne Einschränkungen beim Datenvolumen und mit minimalen Latenzzeiten.

Flexible Implementierung durch Bereitstellung als konventionelles Gateway oder als Inline-Lösung. Mit einer Inline-Implementierung können Administratoren die

bestehende Infrastruktur beibehalten und Application Intelligence and Control-Funktionen als zusätzliche Schicht für mehr Sicherheit und Transparenz hinzufügen.

Deep Packet Inspection von SSL-verschlüsseltem Verkehr (DPI SSL). Transparente Entschlüsselung und Prüfung von ein- und ausgehendem HTTPS-Verkehr durch die SonicWALL RFDPI. Der Verkehr wird anschließend wieder verschlüsselt und an die ursprüngliche Zieladresse geschickt, falls keine Bedrohungen oder Sicherheitsschwachstellen entdeckt wurden.

SonicWALL Global Response Intelligent Defense (GRID)-Netzwerk. Threat Protection, Intrusion Detection und Prevention sowie Services zur Anwendungskontrolle werden rund um die Uhr aktualisiert, um größtmögliche Sicherheit zu gewährleisten. Die komplette Suite an Sicherheitservices bietet Schutz vor über einer Million unterschiedlicher Malware-Angriffe.

WAN-Beschleunigung. Verkürzt die Latenzzeiten und sorgt für einen schnelleren Datentransfer zwischen verschiedenen Standorten und somit für eine größere Netzwerkeffizienz.

Remote-Zugriff für mobile Unternehmen. Sichere Konnektivität für den Zugriff auf Unternehmensressourcen von Windows-, Windows Mobile-, Linux-, Apple Macintosh- und iOS- sowie Google Android-Geräten.

* U.S.-Patente 7,310,815; 7,600,257; 7,738,380; 7,835,361

Application Intelligence und Anwendungskontrolle

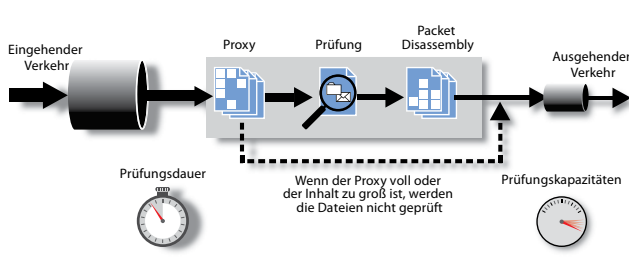
Die Funktion SonicWALL Application Intelligence and Control bietet eine granulare Überwachung und Echtzeit-Visualisierung von Anwendungen, um eine Priorisierung der Bandbreite zu ermöglichen und maximale Netzwerksicherheit und Produktivität zu gewährleisten. Als integraler Bestandteil der Next-Generation Firewalls von SonicWALL arbeitet sie mit der Reassembly-Free Deep Packet Inspection-Technologie und ermöglicht die Erkennung und Kontrolle aktuell genutzter Anwendungen – unabhängig vom Port oder Protokoll. Dank einer ständig erweiterten Signaturreferenzdatenbank, die derzeit über 3.700 Anwendungen und Millionen von Malware-Bedrohungen erkennt, kann der Administrator Anwendungen ganz gezielt kontrollieren, Bandbreite vorrangig zuweisen oder begrenzen und den Zugriff auf Websites sperren. Der SonicWALL App Flow Monitor liefert Echtzeit-Grafiken zu Anwendungen, zur Bandbreiten-belegung in ein- und ausgehender Richtung, zu aktiven Website-Verbindungen sowie zur allgemeinen Benutzeraktivität und kann dabei fortlaufend Daten an NetFlow/IPFIX-Analyser senden.



Reassembly-Free Deep Packet Inspection Engine

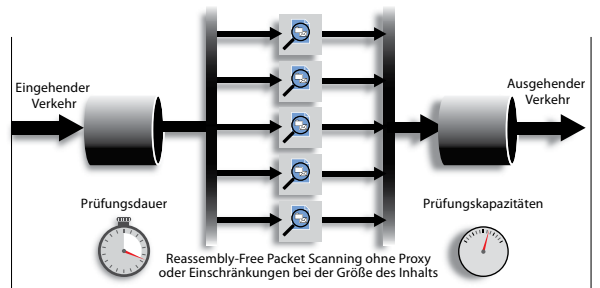
Als skalierbare Inspection Engine für Anwendungen kann die SonicWALL Reassembly-Free Deep Packet Inspection Engine unbegrenzt große Dateien und Inhalte in Echtzeit analysieren, ohne dass dafür die Datenpakete oder der Content wieder zusammengesetzt werden müssen. Diese Methode wurde speziell für Echtzeit-Anwendungen und latenzkritischen Datenverkehr konzipiert und erlaubt auch ohne Proxyverbindungen eine umfassende Kontrolle des Netzwerkverkehrs. Auf diese Weise lässt sich High-Speed-Netzwerkverkehr nicht nur effizienter, sondern auch zuverlässiger prüfen.

Packet Assembly-basiertes Verfahren



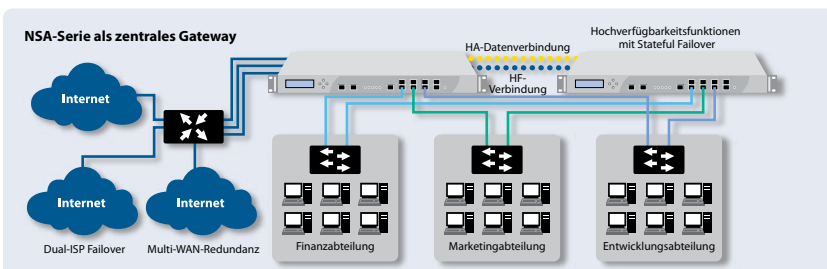
Architekturen anderer Anbieter

Packet Reassembly-freies Verfahren



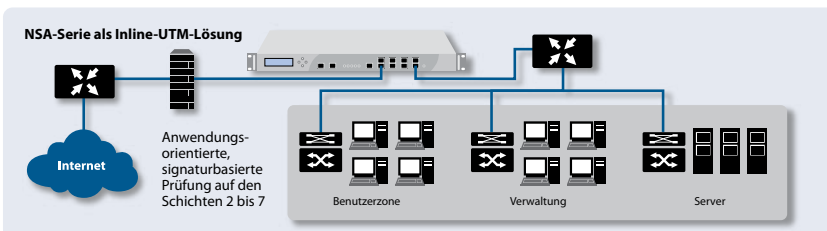
SonicWALL-Architektur

Flexible und individuelle Implementierungsoptionen



Zentrales Gateway

Als zentrales Gateway implementiert bietet die E-Class NSA-Serie eine skalierbare Hochgeschwindigkeitsplattform mit VLANs und Sicherheitszonen für Netzwerksicherheit und -segmentierung. Außerdem verfügt die E-Class NSA-Serie über Redundanzfunktionen wie z. B. WAN-Lastverteilung, ISP Failover und Active/Active DPI.



Layer 2 Bridge-Modus

Der Layer 2 Bridge-Modus verfügt über ein Inline Intrusion Detection System und eine zusätzliche zonenbasierte Sicherheitsschicht für Netzwerksegmente oder Geschäftsbereiche und verringert so die Komplexität der Multi-Layer-Sicherheitslösung. Außerdem können Administratoren auf diese Weise den Zugriff auf sensible Daten nach bestimmten Geschäftsbereichen oder Datenbank-Servern einschränken.

Mehrschichtiger Schutz

Effizienter Schutz für Remote-Standorte

Die E-Class NSA-Serie bietet Ultra-High-Performance VPNs, die sich problemlos für tausende von Endpunkten und Zweigstellen skalieren lassen. Die innovative SonicWALL Clean VPN™-Technologie säubert den Datenverkehr in Echtzeit und ohne Benutzer-Eingriff, bevor dieser das Unternehmensnetzwerk erreicht. Auf diese Weise werden Sicherheitsschwachstellen und bösartiger Code neutralisiert.

Gateway-Schutz

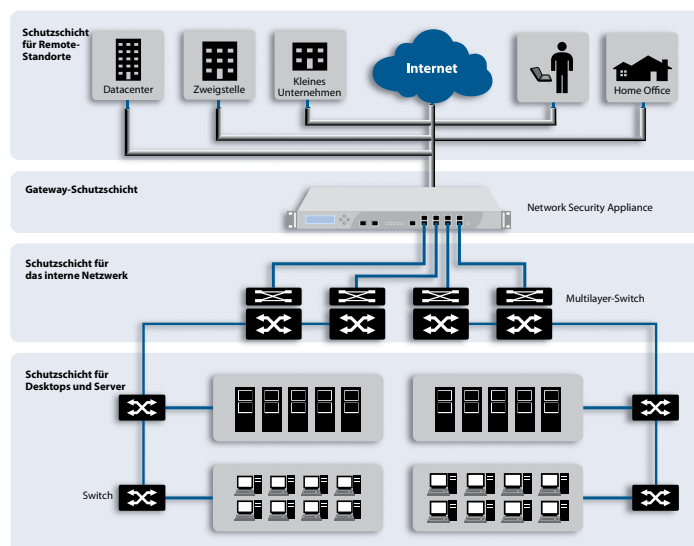
Die E-Class NSAs lassen sich leicht in bestehende Umgebungen integrieren und bieten einen zentralisierten Gateway-Schutz für alle eingehenden und ausgehenden Anwendungen und Dateien sowie für den contentbasierten Datenverkehr. Gleichzeitig überwachen die E-Class NSAs Anwendungen und Bandbreite, ohne die Performance oder Skalierbarkeit zu beeinträchtigen.

Interner Schutz

Mit einer Vielzahl unterschiedlicher Konfigurationsoptionen ausgestattet, prüft die E-Class NSA-Serie auch den Datenverkehr über LAN-Schnittstellen und VLANs und dehnt so den Netzwerkschutz auf das interne Netzwerk aus. Die speziell für LAN-Netzwerkbedrohungen konzipierte E-Class NSA-Serie überwacht und reagiert auf Malware, DoS-Angriffe, Bedrohungen durch Sicherheitslücken, Regelverletzungen, vertrauliche Dokumente und den Missbrauch von Netzwerkressourcen innerhalb des internen Netzwerks.

Desktop- und Server-Schutz

Dank ihres Anti-Virus- und Anti-Spyware-Clients mit heuristischer Analyse bietet die E-Class NSA-Serie neben den Netzwerk- und Gateway-basierten Sicherheitsfunktionen außerdem einen zusätzlichen Endpunkt-Schutz für Arbeitsstationen und Server. Diese automatisierte Client-Lösung kontrolliert den Netzwerkzugriff, indem sie nur Endpunkten mit den neuesten Signaturen oder Engine-Updates den Zugang zum Internet erlaubt. Ist die Enforcement-Funktion der Appliance aktiviert, wird jeder Endpunkt angewiesen, den Enforced Anti-Virus and Anti-Spyware Client herunterzuladen, ohne dass ein Administrator eingreifen muss. Auf diese Weise wird die



Implementierung von Endpunkt-Sicherheitsfunktionen automatisiert.

Zentralisierte Regelverwaltung

Das SonicWALL Global Management System (GMS®) bietet Organisationen, Service-Anbietern und Unternehmen mit verteilten Netzwerken eine flexible, leistungsstarke und intuitive Lösung für die Erstellung von Berichten und zur zentralen Verwaltung von E-Class NSA Next-Generation Firewalls.



Abo-Services

Jede E-Class-Network Security Appliance unterstützt eine wachsende Anzahl von dynamischen Abo-Services und Softwarelösungen, die sich nahtlos in jedes Netzwerk integrieren lassen.



Der **Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service** bietet umfassenden Echtzeit-Netzwerkschutz gegen komplexe Angriffe über die Anwendungsebene und contentbasierte Angriffe (z. B. Viren, Spyware, Würmer, Trojaner sowie Software-Schwachstellen wie Pufferüberläufe).



Application Intelligence and Control bietet eine Echtzeit-Visualisierung des Netzwerkverkehrs, individuell anpassbare Regeln und eine gezielte Überwachung von Anwendungen und Benutzern.



Content Filtering Service setzt eine innovative Rating-Architektur ein, die maximalen Schutz vor anstößigen Webinhalten und privatem Surfen bietet. Mithilfe einer dynamischen Datenbank werden über 56 Kategorien von unerwünschtem Web-Content blockiert.



Analyzer ist ein benutzerfreundliches webbasiertes Analyse- und Reporting-Tool zur Überwachung des Anwendungsverkehrs, das aktuelle und historische Daten zum Zustand sowie zur Performance und Sicherheit des Netzwerkes liefert.



SonicWALL E-Class 24/7-Support

Der speziell für E-Class-Kunden konzipierte E-Class 24/7-Support bietet Support-Funktionen und Servicequalität der Enterprise-Klasse. Der E-Class 24/7-Support umfasst telefonischen und webbasierten technischen Support rund um die Uhr, an 365 Tagen im Jahr, sowie direkten Kontakt mit einem Team hervorragend ausgebildeter und erfahrener Support-Ingenieure. Hinzu kommen Software- und Firmware-Updates bzw. -Upgrades, Vorabaustausch von Hardware, Zugriff auf elektronische Support-Tools, moderierte Diskussionsgruppen und vieles mehr.

Deep Packet Inspection von SSL-verschlüsseltem Verkehr (DPI SSL). Transparente Entschlüsselung und Prüfung von ein- und ausgehendem HTTPS-Verkehr durch die SonicWALL RFDPI. Der Verkehr wird anschließend wieder verschlüsselt und an die ursprüngliche Zieladresse geschickt, falls keine Bedrohungen oder Sicherheitsschwachstellen entdeckt wurden.



Enforced Client Anti-Virus and Anti-Spyware bietet Laptops, Desktop-PCs und Servern umfassenden Viren- und Spyware-Schutz mittels eines einzigen integrierten Clients. Anti-Virus- und Anti-Spyware-Regeln sowie Definitionen und Software-Updates werden automatisch im gesamten Netzwerk angewendet.



Die **SonicWALL Mobile Connect™** Unified Client App für iOS bietet Apple® iPad®, iPhone®- und iPod touch®-Benutzern vollen Zugriff auf Netzwerkebene, um Ressourcen in Unternehmen und Bildungseinrichtungen über verschlüsselte SSL VPN-Verbindungen einzusehen.

Artikelnr. für die E-Class NSA-Serie



SonicWALL NSA E8510 01-SSC-9770



SonicWALL NSA E8500 01-SSC-8866



SonicWALL NSA E7500 01-SSC-7000

SonicWALL NSA E7500 TotalSecure* (1 Jahr) 01-SSC-7027



SonicWALL NSA E6500 01-SSC-7004

SonicWALL NSA E6500 TotalSecure* (1 Jahr) 01-SSC-7028



SonicWALL NSA E5500 01-SSC-7008

SonicWALL NSA E5500 TotalSecure* (1 Jahr) 01-SSC-7029

SonicWALL NSA E8500 Security Services

SonicWALL GAV / IPS / Application Intelligence für NSA E8500 (1 Jahr) 01-SSC-8940

SonicWALL Comprehensive Gateway Security Suite für NSA E8500 (1 Jahr) 01-SSC-8950

SonicWALL E-Class Support 24/7 für NSA E8500 (1 Jahr) 01-SSC-8946

SonicWALL NSA E7500 Security Services

SonicWALL GAV / IPS / Application Intelligence für NSA E7500 (1 Jahr) 01-SSC-6130

SonicWALL Comprehensive Gateway Security Suite für NSA E7500 (1 Jahr) 01-SSC-9220

SonicWALL E-Class Support 24/7 für NSA E7500 (1 Jahr) 01-SSC-7254

SonicWALL NSA E6500 Security Services

SonicWALL GAV / IPS / Application Intelligence für NSA E6500 (1 Jahr) 01-SSC-6131

SonicWALL Comprehensive Gateway Security Suite für NSA E6500 (1 Jahr) 01-SSC-9221

SonicWALL E-Class Support 24/7 für NSA E6500 (1 Jahr) 01-SSC-7257

SonicWALL NSA E5500 Security Services

SonicWALL GAV / IPS / Application Intelligence für NSA E5500 (1 Jahr) 01-SSC-6132

SonicWALL Comprehensive Gateway Security Suite für NSA E5500 (1 Jahr) 01-SSC-9222

SonicWALL E-Class Support 24/7 für NSA E5500 (1 Jahr) 01-SSC-7260

Lizenzen auch für mehrere Jahre erhältlich. Weitere Informationen unter www.sonicwall.com/de

*Mit einem Jahr Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence Service, Content Filtering Service und E-Class 24/7-Support

Zertifikate



Technische Daten

	NSA E5500	NSA E6500	NSA E7500	NSA 8500	NSA 8510
Firewall					
SonicOS-Version	SonicOS Enhanced 5.6 (oder höher)				SonicOS Enhanced 5.8.0.6 (oder höher)
Stateful-Durchsatz ¹	3,9 GBit/s	5 GBit/s	5,6 GBit/s		8,0 GBit/s
GAV-Performance ²	1,0 GBit/s	1,69 GBit/s	1,84 GBit/s		2,25 GBit/s
IPS-Performance ²	2,0 GBit/s	2,3 GBit/s	2,58 GBit/s		3,7 GBit/s
Full Deep Packet Inspection (DPI)-Performance ²	850 MBit/s	1,59 GBit/s	1,7 GBit/s		2,2 GBit/s
IMIX-Performance ²	1,1 GBit/s	1,4 GBit/s	1,6 GBit/s		2,0 GBit/s
Max. Anzahl von Verbindungen ²	750.000	1.000.000	1.500.000		1.500.000
Max. Anzahl Full DPI-Verbindungen	500.000	600.000	1.000.000		1.250.000
Neue Verbindungen/Sekunde	30.000	60.000	64.000		85.000
Unterstützte Nodes	Unlimitiert				
Schutz vor Denial of Service-Angriffen	22 Kategorien von DoS-, DDoS- und Scan-Angriffen				
Unterstützte SonicPoints (max.)	96			128	
VPN					
3DES/AES-Durchsatz ⁴	1,7 GBit/s	2,7 GBit/s	3,0 GBit/s		4,0 GBit/s
Site-to-Site VPN-Tunnel	4.000	6.000		10.000	
Enthaltene Global VPN Client-Lizenzen (max.)	2.000 (4.000)	2.000 (6.000)		2.000 (10.000)	
Enthaltene SSL VPN-Lizenzen (max.)	2 (50)	2 (50)		2 (50)	
Inklusive Virtual Assist (max.)	1 (25)			1 (25)	
Verschlüsselung/Authentifizierung/DH-Gruppen	DES, 3DES, AES (128, 192, 256 Bit)/MDS, SHA-1/DH-Gruppen 1, 2, 5, 14				
Schlüsselaustausch	IKE, IKEv2, manueller Schlüssel, PKI (X.509), L2TP über IPsec				
Route-basiertes VPN	Ja (OSPF, RIP)				
Unterstützte Zertifikate	Verisign, Thawte, Cybertrust, RSA Keon, Entrust, und Microsoft CA für SonicWALL-to-SonicWALL VPNs, SCEP				
Redundantes VPN-Gateway	Ja				
Unterstützte Global VPN Client-Plattformen	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32 Bit/64 Bit, Windows 7				
Unterstützte SSL VPN-Plattformen	Microsoft® Windows 2000 / XP / Vista 32/64 Bit / Windows 7 32/64 Bit, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE				
Unterstützte Mobile Connect-Plattform	iOS 4.2 und höher				
Sicherheitsservices					
Deep Packet Inspection Service	Intrusion Prevention, Gateway Anti-Virus, Anti-Spyware und Application Intelligence				
Content Filtering Service (CFS) Premium Edition	Prüfung nach HTTP URL, HTTPS IP, Schlüsselwörtern und Content, Blockieren von ActiveX, Java Applets und Cookies, Bandbreitenverwaltung nach Ratingkategorien, individuelle Freigabe- und Sperlisten				
Enforced Client Anti-Virus und Anti-Spyware	HTTP/S, SMTP, POP3, IMAP und FTP, Blockieren von E-Mail-Anhängen mittels Enforced McAfee™-Clients				
Comprehensive Anti-Spam Service ⁵	Unterstützt				
Application Intelligence and Control	Anwendungen und Anwendungskontrolle, Priorisierung oder Sperren von Anwendungen nach Signaturen, Kontrolle von Dateitransfers, Scannen nach Schlüsselwörtern und -phrasen				
DPI-SSL	Bietet die Möglichkeit, HTTPS-Verkehr transparent zu entschlüsseln, den Datenverkehr mit dem Deep Packet Inspection-Technologien von SonicWALL (GAV/AS/IPS/Application Intelligence/CFS) auf Bedrohungen zu prüfen und anschließend den Verkehr wieder verschlüsselt an die Zieladresse zu senden, wenn keine Bedrohungen oder Sicherheitsgefahren gefunden wurden. Dieses Feature funktioniert für Clients und für Server.				
Networking					
IP-Adresszuweisung	Statisch (DHCP, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay				
NAT-Modi	1:1, 1:many, many:1, many:many, flexible NAT (überlappende IPs), PAT, transparenter Modus				
VLAN-Ports (802.1q)	400	500		512	
Routing	OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing, Multicast				
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p				
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminal Services, Citrix				
IPv6	Ja				
Interne Datenbank/Single Sign-On-Ben.	1.500/2.500 Benutzer	2.500/4.000 Benutzer		2.500/7.000 Benutzer	
VoIP	Voll H.323v1-5-kompatibel, SIP, Gatekeeper-Unterstützung, Verwaltung der ausgehenden Bandbreite, VoIP über WLAN, Deep Inspection Security, vollständige Interoperabilität mit den meisten VoIP Gateway- und Kommunikationsgeräten				
Link Aggregation	Ja				
Port-Redundanz	Ja				
System					
Verwaltung und Überwachung	Web-Oberfläche (HTTP, HTTPS), Command Line (SSH, Konsole) SNMP v2; zentrale Verwaltung mit SonicWALL GMS				
Logging und Reporting	Analyzer, Scrutinizer, GMS, lokale Logdatei, Syslog, Solera Networks, NetFlow v5/v9, IPFIX mit Erweiterungen, Echtzeit-Visualisierung				
Hochoverfügbarkeit	Active/Passive mit State Sync, Active/Active DPI				
Lastverteilung	Ja (abgehend mit prozentbasierter, Round-Robin- und Spillover-Lastverteilung; ankommend mit Round-Robin, zufälliger Verteilung, Sticky IP, blockweiser Neuordnung und symmetrischer Neuordnung)				
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, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TLS				
Unterstützung für WAN-Beschleunigung	Ja				
Hardware					
Schnittstellen	8 10/100/1000-Kupfer-Gigabit-Ports, 1 GbE HA-Schnittstelle, 1 Konsolenschnittstelle, 2 USB-Schnittstellen		4 SFP-Ports (SX, LX oder TX), 10/100/1000-GbE-Schnittstellen, 1 GbE HA-Schnittstelle, 2 USB-Schnittstellen, 1 Konsolenschnittstelle		2 SFP- und 10-GbE-Ports, 1000 GbE, 1 GbE HA Interface, 2 USB, 1 Konsolenschnittstelle
Speicher (RAM)	1 GB	1 GB	2 GB		4 GB
Flash-Speicher	512 MB Compact Flash				
3G Wireless/Modem*	Mit unterstütztem 3G-Adapter oder Analogmodem				
Stromversorgung	Single-250 W ATX-Stromversorgung		Dual-250 W ATX, hot-swappable		
Lüfter	Dual-Lüfter, hot-swappable				
Display	Front-LCD-Display				
Netzspannung	100-240 VAC, 60-50 Hz				
Maximale Leistungsaufnahme	81 W	90 W		150 W	
Wärmeabgabe	276 BTU	307 BTU		511,5 BTU	
MTBF	11,9	11,9		12,4	
Zertifikate	EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1, IPv6 Phase 2		ICSA Firewall 4.1		—
Ausstehende Zertifikate	—		EAL4+, FIPS 140-2 Level 2, VPNC, VPNC, IPv6 Phase 1 und 2		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1 und 2
Gehäuse	Rackfähig (1 HE)				
Abmessungen	43,2 x 42,5 x 4,4 cm				
Gewicht	6,80 kg	6,85 kg		7,9 kg	
WEEE-Gewicht	6,80 kg	6,85 kg		7,9 kg	
Erfüllt folgende Standards/Normen	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE				
Umgebungstemperatur	5-40° C				
Luftfeuchtigkeit	10-90 % nicht kondensierend				

¹Testmethoden: Maximalleistung auf Basis von RFC 2544 (für Firewall). Die tatsächliche Leistung kann je nach Netzwerkbedingungen bzw. aktivierten Diensten variieren. ²Messung des Full DPI-/Gateway AV-/Anti-Spyware-/IPS-Durchsatzes mittels Industriestandard-HTTP Performance-Test WebAvalanche von Spirent und Ixia Test-Tools. Die Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren. ³Die tatsächliche maximale Anzahl von Verbindungen ist bei aktivierten UTM-Services niedriger. ⁴VPN-Durchsatzmessung mittels UDP-Verkehr mit 1280 Bytes pro Paket gemäß RFC 2544. ⁵USB-3G-Karte und Modem sind nicht enthalten. Weitere Informationen zu den unterstützten USB-Geräten: <http://www.sonicwall.com/us/products/cardsupport.html> ^{Der}

SonicWALL-Lösungen für dynamische Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT

SonicWALL Deutschland

Tel: +49 89 4545 946 www.sonicwall.de

SonicWALL Schweiz

Tel: +41 44 810 31 35 www.sonicwall.ch

SonicWALL Österreich

Tel: +41 44 810 31 35 www.sonicwall.at



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™