



FIREWALL

Next-Generation Firewall

- **Next-Generation Firewall**
- **Leistungsstarke Intrusion Prevention**
- **Application Intelligence, Anwendungskontrolle und -visualisierung**
- **Reassembly-Free Deep Packet Inspection-Technologie**
- **Flexible Implementierung**
- **Deep Packet Inspection von SSL-verschlüsseltem Verkehr (DPI SSL)**
- **SonicWALL Global Response Intelligent Defense (GRID)-Netzwerk**

IT-Administratoren stehen heute vor einer echten Herausforderung: Sie müssen die Verfügbarkeit und Effizienz unternehmenskritischer Lösungen gewährleisten und gleichzeitig die Nutzung unproduktiver und oftmals gefährlicher Anwendungen kontrollieren. Das geht nur, wenn die Bandbreite für unternehmenskritische Anwendungen priorisiert und Social Media-Anwendungen oder Spiele in ihrem Verbrauch eingeschränkt oder komplett gesperrt werden. Stateful Packet Inspection-Firewalls, wie sie noch in vielen Unternehmen eingesetzt werden, bieten hier keine Lösung: Da sie lediglich Ports und Protokolle prüfen, sind sie nicht in der Lage, Anwendungen zu identifizieren, geschweige denn, zwischen unbedenklichem und verdächtigem Datenverkehr zu unterscheiden.

Die SonicWALL® E-Class Network Security Appliance (NSA)-Serie nutzt neben einer Multi-Core-Architektur die patentierte Reassembly-Free Deep Packet Inspection™ (RFDPI)-Technologie* von SonicWALL und bietet robusten Firewallschutz der nächsten Generation sowie erweiterte Anwendungskontrolle für komplexe Netzwerke. Die E-Class NSA-Appliances E7500, E6500 und E5500 verbinden Application Intelligence, Anwendungskontrolle und -visualisierung mit mehrstufigen Sicherheitsmechanismen, einer erweiterten Bandbreitenverwaltung und zahlreichen Hochverfügbarkeitsfunktionen. Damit bieten sie ein umfassendes Spektrum an skalierbaren Lösungen für die verschiedensten Infrastrukturen wie etwa Rechenzentren, Campus-Netzwerke oder verteilte Umgebungen.

Die E-Class NSA-Serie ist ein wichtiger Bestandteil von SonicWALLs Enterprise-Class-Portfolio an Network Security-, E-Mail Security- und Secure Remote Access-Produkten und -Services. Alle E-Class-Lösungen bieten größtmögliche Sicherheit und höchste Performance, kombiniert mit intelligenten Funktionen, optimaler Benutzerfreundlichkeit und einem unschlagbaren Preis-Leistungs-Verhältnis. Die SonicWALL E-Class bietet Unternehmen mit Enterprise-Class-Netzwerken High-Performance Protection in einer Lösung, die einen sicheren Netzwerkbetrieb ermöglicht und dabei Kosten und Komplexität senkt.

Funktionen und Vorteile

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

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, Anwendungskontrolle und -visualisierung 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 mehr als 2.800 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- und Anwendungskontrollfunktionen 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 Sicherheitsservices bietet Schutz vor über einer Million unterschiedlicher Malware-Angriffe.

Application Intelligence und Anwendungskontrolle

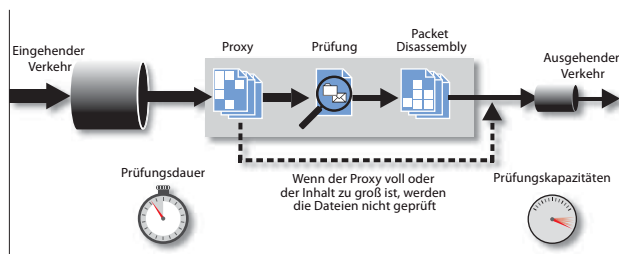
Die Funktion SonicWALL Application Intelligence und Anwendungskontrolle bietet eine granulare Überwachung und Echtzeit-Visualisierung von Anwendungen, um eine Priorisierung der Bandbreite zu ermöglichen und maximale Netzwerksicherheit und Produktivität zu gewährleisten. Als integraler Bestandteil der 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 2.800 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 Application Flow Monitor liefert Echtzeit-Grafiken zu Anwendungen, zur Bandbreitenbelegung 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

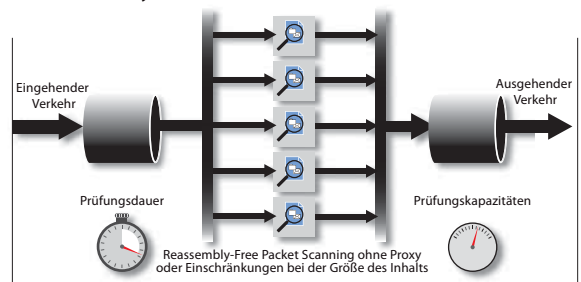
Als skalierbare Inspection Engine für Anwendungen kann die SonicWALL Reassembly-Free Deep Packet Inspection Engine unbegrenzt große Dateien und Inhalte in Echtzeit analysieren, ohne dass dafür die Datenpakete oder der Content wieder zusammengesetzt werden müssen. Diese Methode wurde speziell für Echtzeit-Anwendungen 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



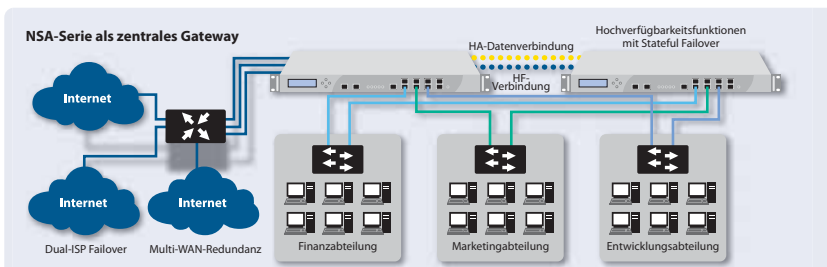
Architekturen anderer Anbieter

Packet Reassembly-freies Verfahren



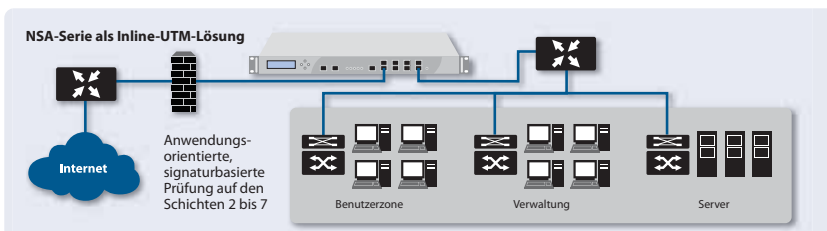
SonicWALL-Architektur

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 Sicherheitschwachstellen und bösartiger Code neutralisiert.

Gateway-Schutz

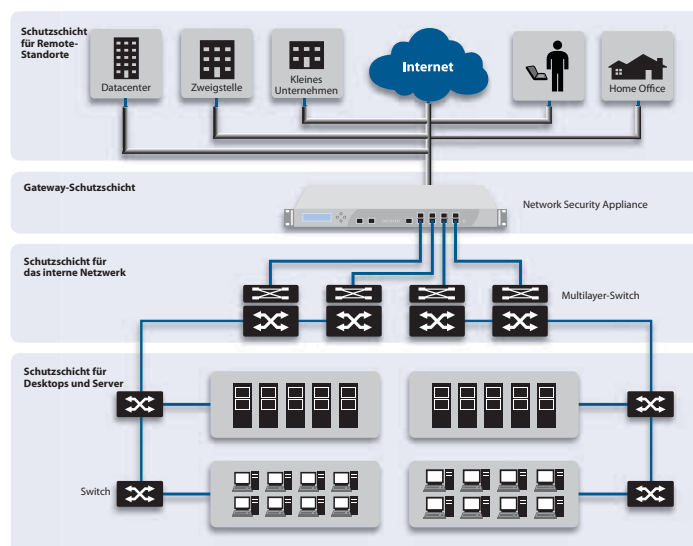
Die E-Class NSAs lassen sich leicht in bestehende Umgebungen integrieren und bieten einen zentralisierten Gateway-Schutz für alle eingehenden und ausgehenden Anwendungen und Dateien sowie für den contentbasierten Datenverkehr. Gleichzeitig überwachen die E-Class NSAs Anwendungen und Bandbreite, ohne 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 Netzwerkkressourcen 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 flexible, leistungsstarke und intuitive Tools, um die E-Class NSA-Serie in verteilten Unternehmensnetzwerken zentral zu verwalten und zu konfigurieren. Darüber hinaus lassen sich mit GMS Überwachungsdaten in Echtzeit anzeigen und Regel- bzw. Compliance-Berichte erstellen.



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 Intrusion Prevention and Application Intelligence and Control Service

von SonicWALL bietet umfassenden Echtzeit-Netzwerkschutz gegen komplexe Angriffe über die Anwendungsebene und contentbasierte Angriffe (z. B. Viren, Spyware, Würmer, Trojaner sowie Software-Schwachstellen wie Pufferüberläufe). Die Funktion Application Intelligence und Anwendungskontrolle ermöglicht eine Echtzeit-Visualisierung des Netzwerkverkehrs mit individuell anpassbaren Regeln und der Möglichkeit, Anwendungen und Benutzer im Netzwerk gezielt zu überwachen.



Enforced Client and Server 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.



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.



ViewPoint von SonicWALL ist ein komfortables webbasiertes Reportingtool, das detaillierte Informationen über die Performance und Sicherheit liefert. Historische Reports auf der Grundlage von Übersichten und detaillierten Zusammenfassungen unterstützen große und kleine Organisationen bei der Kontrolle der Internetnutzung, bei der Einhaltung gesetzlicher Vorschriften sowie bei der Überwachung der Netzwerksicherheit.



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 Sicherheitschwachstellen entdeckt wurden.

Artikelnummern für die E-Class NSA-Serie



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 E7500 Security Services

SonicWALL Content Filtering Service Premium Business Edition für NSA E7500 (1 Jahr)
01-SSC-7329

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 Content Filtering Service Premium Business Edition für NSA E6500 (1 Jahr)
01-SSC-7330

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 Content Filtering Service Premium Business Edition für NSA E5500 (1 Jahr)
01-SSC-7331

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, E-Class Support 24/7 und ViewPoint Reporting.

Technische Daten

	NSA E5500	NSA E6500	NSA E7500
Firewall			
SonicOS-Version			
SonicOS Enhanced 5.6 (oder höher)			
Stateful-Durchsatz¹	3,9 GBit/s	5 GBit/s	5,6 GBit/s
GAV-Performance²	1,0 GBit/s	1,69 GBit/s	1,84 GBit/s
IPS-Performance²	2,0 GBit/s	2,3 GBit/s	2,58 GBit/s
Full Deep Packet Inspection (DPI)-Performance²	850 MBit/s	1,59 GBit/s	1,7 GBit/s
IMIX-Performance²	1,1 GBit/s	1,4 GBit/s	1,6 GBit/s
Max. Anzahl von Verbindungen³	750.000	1.000.000	1.500.000
Max. Anzahl Full DPI-Verbindungen	500.000	600.000	1.000.000
Neue Verbindungen/Sekunde	15.000	20.000	25.000
Unterstützte Nodes	Unlimitiert		
Schutz vor Denial of Service-Angriffen	22 Kategorien von DoS-, DDoS- und Scan-Angriffen		
Unterstützte SonicPoints (max.)	96	128	128
VPN			
3DES/AES-Durchsatz⁴	1,7 GBit/s	2,7 GBit/s	3 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)	1 (25)
Verschlüsselung/Authentifizierung/DH-Gruppen	DES, 3DES, AES (128, 192, 256 Bit)/MD5, 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, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE		
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	Blockieren von E-Mail-Anhängen mittels Enforced McAfee™-Clients		
Comprehensive Anti-Spam Service⁵	Unterstützt		
Application Intelligence und Anwendungskontrolle	Verwaltung der Bandbreite von 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 den 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-Benutzer	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	ViewPoint, lokale Logdatei, Syslog, Solera Networks, NetFlow v5/v9, IPFIX mit Erweiterungen, Echtzeit-Visualisierung		
Hochverfügbarkeit	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-TTLS		
Hardware			
Schnittstellen	(8) 10/100/1000 Kupfer-Gigabit-Ports, 1 GbE HA-Schnittstelle, 1 Konsolenschnittstelle, 2 USB-Schnittstellen	(8) 10/100/1000 Kupfer-Gigabit-Ports, 1 GbE HA-Schnittstelle, 1 Konsolenschnittstelle, 2 USB-Schnittstellen	1 Konsolenschnittstelle, 4 Gigabit-Ethernet-Schnittstellen, 4 SFP-Ports (Sx, Lx oder Tx), 1 GbE HA-Schnittstelle, 2 USB-Schnittstellen
Speicher (RAM)	1 GB	1 GB	2 GB
Flash-Speicher	512 MB Compact Flash	512 MB Compact Flash	512 MB Compact Flash
3G Wireless/Modem⁶	Mit USB-3G-Adapter/Modem		
Stromversorgung	Single-250 W ATX-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		
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		

¹ Testmethoden: Maximalleistung auf Basis von RFC 2544 (für Firewall). Die tatsächliche Leistung kann je nach Netzwerkbedingungen bzw. aktivierten Diensten variieren. ² Messung des Full DPI-/Gateway AV-/Anti-Spyware-/IPS-Durchsatzes mittels Industriestandard-HTTP Performance-Test WebAvalanche von Spirent und kia Test-Tools. Die Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren. ³ Die tatsächliche maximale Anzahl von Verbindungen ist bei aktivierten UTM-Services niedriger. ⁴ VPN-Durchsatzmessung mittels UDP-Verkehr mit 1280 Bytes pro Paket gemäß RFC 2544. ⁵ USB-3G-Karte und Modem sind nicht enthalten. Weitere Informationen zu den unterstützten USB-Geräten: <http://www.sonicwall.com/us/products/cardsupport.html> ⁶ Der Comprehensive Anti-Spam Service unterstützt beliebig viele Benutzer, wobei die empfohlene Anzahl 250 Benutzer oder weniger beträgt.

Zertifikate



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™