



Die SonicWALL Network Security Appliance-Serie

FIREWALL

Unified Threat Management Firewall

- **Unified Threat Management**
- **Skalierbare Multi-Core-Hardware und Reassembly-Free Deep Packet Inspection**
- **Application Intelligence, Anwendungskontrolle und -visualisierung**
- **Hochverfügbarkeitsfunktionen mit Stateful Failover und integrierter Lastverteilung**
- **Hohe Performance und niedrige TCO**
- **Erweiterte Routing Services und Netzwerkfunktionen**
- **Standardisiertes VoIP**
- **Sicherheitsdienste für verteilte WLAN-Infrastrukturen**
- **Integrierte QoS-Features**

Beim Zugriff auf interne und externe geschäftskritische Anwendungen müssen sich kleine Firmen genauso wie große Organisationen auf ihre Netzwerke verlassen können. Zwar profitieren Unternehmen von den neuesten Entwicklungen im Netzwerkbereich, doch gleichzeitig müssen sie sich gegen eine wachsende Zahl komplexer und finanziell motivierter Angriffe zur Wehr setzen, deren Ziel es ist, die Datenübertragung zu stören, die Performance herabzusetzen und die Datenintegrität zu beeinträchtigen. Veraltete Stateful Packet Inspection Firewalls bieten keinen ausreichenden Schutz vor böswilligen Angriffen, die auf der Anwendungsebene ansetzen. Punktuelle Produkte bieten zwar eine zusätzliche Sicherheitsschicht, bringen aber erhebliche Nachteile mit sich: Sie sind kostspielig, kompliziert zu verwalten, können den Missbrauch von Netzwerkressourcen nur begrenzt kontrollieren und sind nicht in der Lage, die neuesten Mischangriffe effizient auszuschalten.

Mit ihrer innovativen Multi-Core-Architektur und ihrer patentierten Reassembly-Free Deep Packet Inspection™-Technologie* (RFDPI) revolutionieren die Unified Threat Management (UTM) Firewalls der SonicWALL® Network Security Appliance (NSA)-Serie die Netzwerksicherheit und bieten umfassenden Netzwerkschutz, ohne die Performance zu beeinträchtigen. Die NSA-Serie prüft jedes einzelne Datenpaket zu 100 % auf interne oder externe Bedrohungen in Echtzeit und übertrifft damit herkömmliche Sicherheitslösungen bei Weitem.

Die NSA-Serie kombiniert die Features Intrusion Prevention, Anti-Virus, Anti-Spyware, Anti-Spam und Content Filtering mit Application Intelligence, Anwendungskontrolle und -visualisierung und bietet so umfassende UTM-Schutzfunktionen für eine Vielzahl von Angriffen. Die NSA-Appliances sind mit erweiterter Routing-, Hochverfügbarkeits- und High-Speed-IPSec- und VPN-Technologie ausgestattet. Zweigniederlassungen, Unternehmenszentralen und verteilte mittlere Firmennetzwerke profitieren auf diese Weise von mehr Sicherheit, Zuverlässigkeit, Funktionalität und Produktivität bei gleichzeitiger Reduzierung der Kosten und der Komplexität.

Mit den Modellen SonicWALL NSA 240, NSA 2400, NSA 3500 und NSA 4500 bietet die NSA-Serie skalierbare Netzwerksicherheitslösungen für Unternehmen jeder Größenordnung.

Funktionen und Vorteile

Unified Threat Management. Mithilfe der integrierten Funktionen Intrusion Prevention, Gateway Anti-Virus, Anti-Spyware, Application Intelligence und Anwendungskontrolle, Content Filtering und Anti-Spam werden Malware und Spam abgeblockt. Gleichzeitig lassen sich Anwendungen gezielt überwachen und die Weitergabe vertraulicher Informationen verhindern.

Skalierbare Multi-Core-Hardware und Reassembly-Free Deep Packet Inspection. Scant Tausende von Verbindungen und Dateien unbegrenzter Größe und neutralisiert Bedrohungen – und das in Leitungsgeschwindigkeit ohne nennenswerte zusätzliche Latenzen.

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.

Hochverfügbarkeitsfunktionen mit Stateful Failover und integrierter Lastverteilung. Gewährleisten eine maximale Netzwerkbandbreite und einen hochverfügbaren, unterbrechungsfreien Zugriff auf geschäftskritische Ressourcen. Darüber hinaus sorgen sie dafür, dass bei einem Failover weder VPN-Tunnels noch der Netzwerkverkehr unterbrochen werden.

Hohe Performance und niedrige TCO. Die gebündelte Rechenpower mehrerer Prozessorkerne steigert die Durchsatzrate und ermöglicht eine gleichzeitige Analyse von Datenpaketen bei reduziertem Energieverbrauch.

Erweiterte Routing Services und Netzwerkfunktionen. Umfassen Netzwerktechnologien wie VLAN nach 802.1q, Multi-WAN-Failover, zonen- und objektbasierte Verwaltung, Lastverteilung und erweiterte NAT-Modi. Damit sind eine gezielte und flexible Konfiguration sowie ein umfassender Netzwerkschutz gewährleistet.

Standardisiertes VoIP. Bietet umfassenden Schutz für die gesamte VoIP-Infrastruktur, angefangen bei den Kommunikationsanlagen bis hin zu den VoIP-fähigen Geräten wie SIP-Proxies, H.323-Gatekeepern und Call-Servern.

Sicherheitsdienste für verteilte WLAN-Infrastrukturen. Die Appliance fungiert hierbei als Secure Wireless Switch und Controller, der SonicPoint Wireless Access Points automatisch erkennt und konfiguriert.

Integrierte QoS-Features. Gewährleisten dank 802.1p sowie DSCP (Differentiated Services Code Points) Class-of-Service-Kennungen eine leistungsfähige und flexible Bandbreitenverwaltung für VoIP, Multimedia und geschäftskritische Anwendungen.

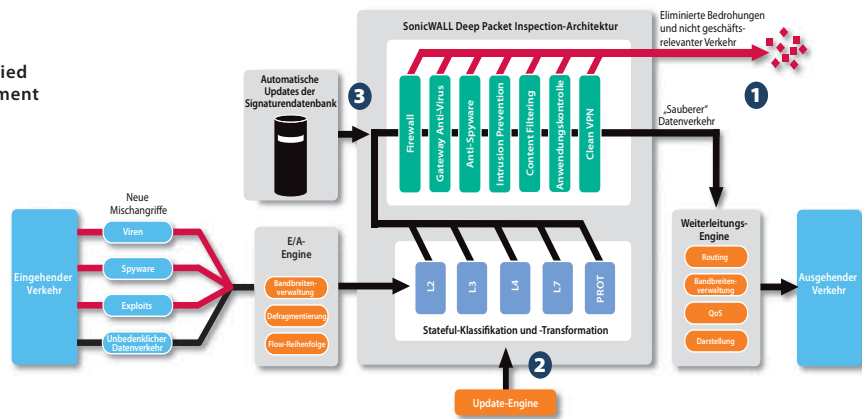
*U.S.-Patent 7,310,815 – A method and apparatus for data stream analysis and blocking (Methode und Gerät, um Datenströme zu analysieren und zu blockieren)

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™



SonicWALL Unified Threat Management in Echtzeit



Führende Sicherheitstechnologien

- 1 Die SonicWALL Deep Packet Inspection-Technologie bietet Schutz vor Gefährdungen wie Viren, Würmern, Trojanern, Spyware, Phishing-Angriffen, Internetmissbrauch und sonstigen Sicherheitsbedrohungen. Mit der Funktion Application Intelligence und Anwendungskontrolle lässt sich die Bandbreite auf der Anwendungsebene verwalten und die Weitergabe vertraulicher Informationen verhindern.
- 2 Die SonicWALL Reassembly-Free Deep Packet Inspection (RFDPI)-Technologie verwendet die Multi-Core-Architektur

von SonicWALL, um Datenpakete in Echtzeit zu prüfen, ohne dass Datenverkehr im Speicher blockiert wird. Dadurch können Sicherheitsbedrohungen unabhängig von der Dateigröße und der Anzahl gleichzeitiger Verbindungen verzögerungsfrei erkannt und eliminiert werden.

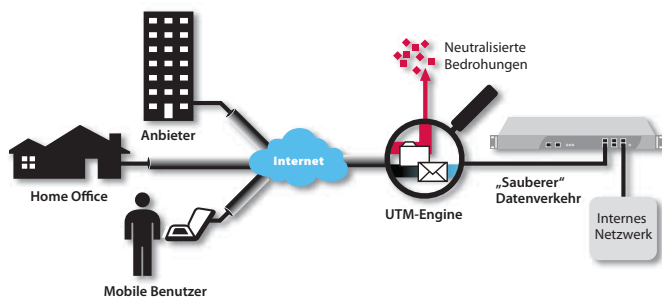
- 3 Dank automatisierter und regelmäßiger Sicherheitsupdates bietet die SonicWALL NSA-Serie einen dynamischen Schutz gegen neue und wechselnde Sicherheitsbedrohungen, ohne dass der Administrator eingreifen muss.

Application Intelligence und Anwendungs-kontrolle

Die Funktion SonicWALL Application Intelligence und Anwendungskontrolle bietet eine granulare Überwachung und Echtzeit-Visualisierung von Anwendungen, um eine Priorisierung der Bandbreite sicherzustellen 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 anhand einfacher vordefinierter Kategorien (wie Social Media oder Spiele) – unabhängig vom Port oder Protokoll. Der SonicWALL



Application Flow Monitor liefert Echtzeit-Grafiken zu Anwendungen, zur Bandbreitenbelegung in ein- und ausgehender Richtung, zu aktiven Website-Verbindungen sowie zur allgemeinen Benutzeraktivität.



SonicWALL Clean VPN
Mithilfe der innovativen SonicWALL Clean VPN™-Technologie schaltet die Network Security Appliance-Serie Sicherheitsschwachstellen und böswilligen Code aus. Verbindungen von mobilen Benutzern und Datenverkehr von Niederlassungen werden ohne Zutun des Benutzers auf Malware gescannt, bevor sie das Unternehmensnetzwerk erreichen.



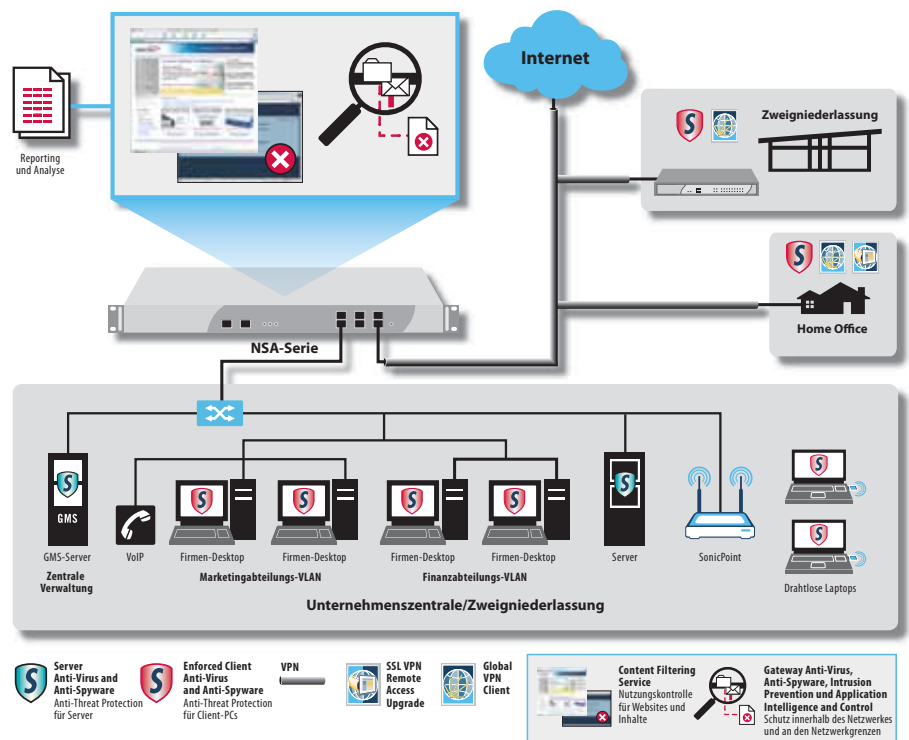
Zentralisierte Regelverwaltung

Die Network Security Appliance-Serie lässt sich mit dem SonicWALL Global Management System (GMS®) verwalten. Das ausgezeichnete Programm bietet flexible, leistungsstarke und intuitive Tools zur zentralen Verwaltung der Konfiguration, zeigt Überwachungsdaten in Echtzeit an und erstellt Regel- bzw. Compliance-Berichte.

Flexible, individuell anpassbare Implementierungsoptionen – die NSA-Serie im Überblick

Alle SonicWALL Network Security Appliance-Lösungen bieten Unified Threat Management Protection. Dank ihrer bahnbrechenden Multi-Core-Architektur und Reassembly-Free Deep Packet Inspection-Technologie bietet die NSA-Serie internen und externen Netzwerkschutz, ohne die Performance zu beeinträchtigen. Jede Appliance der NSA-Serie verfügt über High-Speed-Intrusion Prevention, Funktionen zur Prüfung von Dateien und Dateiinhalten, eine leistungsstarke Application Intelligence und Anwendungskontrolle sowie zahlreiche erweiterte flexible Netzwerk- und Konfigurationsfeatures. Die NSA-Serie bietet eine komfortable und erschwingliche Plattform, die sich in den unterschiedlichsten Netzwerkumgebungen von Unternehmen, Zweigniederlassungen und verteilten Organisationen leicht implementieren und verwalten lässt.

- Die **SonicWALL NSA 4500** ist für Unternehmenszentralen sowie für größere verteilte Netzwerkumgebungen ausgelegt, die eine hohe Durchsatzkapazität und Performance benötigen.
- Die **SonicWALL NSA 3500** ist für die Netzwerkumgebungen von Unternehmen und Zweigniederlassungen sowie für verteilte Unternehmen geeignet, die eine erhebliche Durchsatz-Kapazität und Performance benötigen.
- Die **SonicWALL NSA 2400** ist ideal für kleine bis mittlere Unternehmen und Zweigniederlassungen geeignet, die ihre Durchsatz-Kapazität und Performance optimieren möchten.
- Die **SonicWALL NSA 240** eignet sich optimal für kleine bis mittlere Unternehmen und Niederlassungen.



Sicherheitsservices und Upgrades



Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control Service.

Bietet umfassenden Echtzeit-Netzwerkschutz vor komplexen Angriffen über die Anwendungsebene und contentbasierten Angriffen (z. B. Viren, Spyware, Würmer, Trojaner sowie Software-Schwachstellen wie Pufferüberläufe). Die Funktion Application Intelligence

und Anwendungskontrolle umfasst eine Reihe konfigurierbarer Tools, mit denen sich die Anwendungsebene gezielt überwachen lässt und die Weitergabe vertraulicher Informationen verhindert werden kann. Darüber hinaus ist eine Visualisierung des Netzwerkverkehrs möglich.



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.



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 Reporting. Das komfortable webbasierte Reporting-tool liefert detaillierte Informationen zum Thema Performance und Sicherheit. 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.



Virtual Assist ist ein Remote-Support-Tool für IT-Techniker, mit dem sie Zugriff auf einen PC oder auf ein Laptop erhalten können, um Remote-Support zu leisten. Mit der Erlaubnis des Benutzers können Techniker so innerhalb kürzester Zeit über einen Webbrowser auf den Computer zugreifen und Probleme remote identifizieren und beheben, ohne dass ein vorinstallierter „Fat Client“ erforderlich ist.



Dynamic Support Services. Sind je nach Bedarf entweder während der üblichen Geschäftszeiten oder rund um die Uhr (24/7) verfügbar. Die Dynamic Support Services umfassen erstklassigen technischen Support, wichtige Firmware-Updates und -Upgrades, Zugriff auf elektronische Support-Tools und Vorbaustaustausch von Hardware, damit Unternehmen ihre Investitionen in SonicWALL-Technologie bestmöglich nutzen können.



Global VPN Client-Upgrade verwenden einen Software-Client, der auf Windows-Rechnern installiert ist. Sie bieten Remote-Benutzern einen sicheren Zugriff auf E-Mail, Dateien, Anwendungen sowie auf Intranets und steigern so die Produktivität der Mitarbeiter. Upgrade-Lizenzen sind für eine Vielzahl von User Packs verfügbar, so dass die Lösung flexibel mit dem Unternehmen wachsen kann.



SSL VPN Remote Access-Upgrade bieten PCs, Macs und Linux-Systemen einen clientlosen Remote-Zugriff auf Netzwerkebene. Die SonicWALL UTM Appliances mit integrierter SSL VPN-Technologie ermöglichen einen nahtlosen und sicheren Remote Access auf E-Mail, Dateien, Intranets und Anwendungen von zahlreichen Client-Plattformen. Der Zugriff erfolgt über NetExtender, einen Lightweight-Client, der automatisch ohne Zutun des Benutzers auf dem Rechner installiert und konfiguriert wird.



SonicWALL Comprehensive Anti-Spam Service (CASS) bietet kleinen bis mittelgroßen Unternehmen umfassenden Spam- und Virenschutz und lässt sich in kürzester Zeit auf bestehenden SonicWALL-Firewalls implementieren. Neben einer rascheren Bereitstellung vereinfacht CASS auch die Administration und reduziert durch die Konsolidierung mehrerer Lösungen den Gesamtaufwand. Der Anti-Spam Service lässt sich innerhalb von nur zehn Minuten konfigurieren und mit einem Mausklick aktivieren.

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.

Technische Daten



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 2400
TotalSecure* (1 Jahr)
01-SSC-8760



SonicWALL Adapter
PC-Karte-Expresscard
(für NSA 240)
01-SSC-2887

Weitere Informationen über die Netzwerksicherheitslösungen von SonicWALL erhalten Sie auf unserer Website unter www.sonicwall.com/de.

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

Firewall	NSA 240	NSA 2400	NSA 3500	NSA 4500
SonicOS-Version	SonicOS Enhanced 5.6 (oder höher)			
Stateful-Durchsatz ¹	600 MBit/s	775 MBit/s	1,5 GBit/s	2,75 GBit/s
GAV-Performance ²	115 MBit/s	160 MBit/s	350 MBit/s	690 MBit/s
IPS-Performance ²	195 MBit/s	275 MBit/s	750 MBit/s	1,4 MBit/s
UTM-Performance ²	110 MBit/s	150 MBit/s	240 MBit/s	600 MBit/s
IMIX-Performance ²	195 MBit/s	235 MBit/s	580 MBit/s	700 MBit/s
Max. Anzahl von Verbindungen ³	85.000/110.000 ⁴	225.000	325.000	500.000
Max. Anzahl von DPI-Verbindungen	32.000/50.000 ⁴	125.000	175.000	250.000
Neue Verbindungen/Sek.	2.000	4.000	7.000	10.000
Unterstützte Nodes	Unlimitiert			
Schutz vor Denial of Service (DoS)	22 Kategorien von DoS, DDoS und Scan-Angriffen			
Unterstützte SonicPoints (max.)	16	32	32	64
VPN	NSA 240	NSA 2400	NSA 3500	NSA 4500
3DES/AES-Durchsatz ⁵	150 MBit/s	300 MBit/s	625 MBit/s	1,0 GBit/s
Site-to-Site-VPN-Tunnel	25/50 ⁴	75	800	1.500
Enthaltene Global VPN Client-Lizenzen (max.)	2 (25)	10 (250)	50 (1.000)	500 (3.000)
Enthaltene SSL VPN-Lizenzen (max.)	2 (15)	2 (25)	2 (30)	2 (30)
Inklusive Virtual Assist (max.)	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, 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			
Dead Peer Detection	Ja			
DHCP über VPN	Ja			
IPSec NAT-Traversal	Ja			
Redundantes VPN-Gateway	Ja			
Unterstützte Global VPN Client-Plattformen	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32 Bit/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			
Sicherheitsservices	NSA 240	NSA 2400	NSA 3500	NSA 4500
Deep Packet Inspection Service	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control			
Content Filtering Service (CFS) Premium Edition	Prüfung nach HTTP URL, HTTPS IP, Schlüsselwörtern und Content, Blockieren von ActiveX, Java Applets und Cookies Bandbreitenverwaltung nach Filterkategorien, Freigabe- und Sperlisten			
Enforced Client Anti-Virus und Anti-Spyware	HTTPS, SMTP, POP3, IMAP und FTP, Blockieren von E-Mail-Anhängen mittels Enforced McAfee™-Clients			
Comprehensive Anti-Spam Service ⁶	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 ⁷	Bietet die Möglichkeit, HTTPS-Verkehr transparent zu entschlüsseln, den Datenverkehr mit dem Deep Packet Inspection-Technologie 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	NSA 240	NSA 2400	NSA 3500	NSA 4500
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)	10/25 ⁸	25	50	200
Routing	OSPF, RIPv1/v2, statische Routen, regelbasiertes 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			
Interne Datenbank/Single Sign-On-Benutzer	100/100 Benutzer	250/250 Benutzer	300/500 Benutzer	1.000/1.000 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			
System	NSA 240	NSA 2400	NSA 3500	NSA 4500
Zonenspezifische Sicherheitsfunktionen	Ja			
Zeitsteuerung	Einmalig, regelmäßig			
Objekt-/gruppenbasiertes Management	Ja			
DDNS	Ja			
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 (optional) ⁹	Active/Passive mit State Sync (optional)	Active/Passive mit State Sync	Active/Passive mit State Sync
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, WPA2, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS			
Hardware	NSA 240	NSA 2400	NSA 3500	NSA 4500
Schnittstellen	3 GE-Gigabit-, 6 10/100- und 2 USB-Ports, PC-Karten-Steckplatz (optional 3G/Analogmodem), 1 Konsolenschnittstelle	(6) 10/100/1000 Kupfer-Gigabit-Ports, 1 Konsolenschnittstelle, 2 USB-Ports		
Speicher (RAM)	256 MB	512 MB	512 MB	512 MB
Flash-Speicher	32 MB Compact Flash	512 MB Compact Flash		
3G Wireless/Modem*	Mit 3G-USB-Adapter/Modem			
Stromversorgung	Externe 36 W-Stromversorgung		Single-180 W ATX-Stromversorgung	
Lüfter	Kein Lüfter		2 Lüfter	
Netzspannung	10-240 V, 50-60 Hz		100-240 VAC, 60-50 Hz	
Maximale Leistungsaufnahme	15 W	42 W	64 W	66 W
Wärmeabgabe	51,1 BTU	144 BTU	219 BTU	225 BTU
Zertifikate	EAL4+, VPNC, ICSA Firewall 4.1		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1	
Ausstehende Zertifikate	FIPS 140-2		-	
Gehäuse und Abmessungen	18,1 x 3,8 x 26,7 cm	Rackfähig (1 HE) 43,2 x 26 x 4,4 cm		Rackfähig (1 HE) 43,2 x 33,7 x 4,4 cm
Gewicht	1,16 kg	3,65 kg		5,14 kg
WEEE-Gewicht	1,43 kg	3,65 kg		5,14 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	0-40° C	5-40° C		
MTBF	9,5 Jahre	16,0 Jahre	14,3 Jahre	14,1 Jahre
Luftfeuchtigkeit	0-95 % nicht kondensierend	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 UTM-/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. ³ Die tatsächliche maximale Anzahl von Verbindungen ist bei aktivierten UTM-Services niedriger. ⁴ Nur mit Stateful HA- und Expansion-Upgrade für die NSA 240. ⁵ VPN-Durchsatzmessung mittels UDP-Verkehr mit 1280 Bytes pro Paket gemäß RFC 2544. ⁶ Unterstützung auf der NSA 3500 und höher. ⁷ Nicht für die NSA 2400 verfügbar. ⁸ USB-3-G-Karte und Modem sind nicht enthalten. Weitere Informationen zu den unterstützten USB-Geräten: <http://www.sonicwall.com/us/products/cardsupport.html> ⁹ Der Comprehensive Anti-Spam Service unterstützt beliebig viele Benutzer, wobei die empfohlene Anzahl 250 Benutzer oder weniger beträgt.

Zertifikate



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

SonicWALL-Lösungen für dynamische Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™