



Die SonicWALL Network Security Appliance-Serie

FIREWALL

Next-Generation Firewall

- **Next-Generation Firewall**
- **Skalierbare Multi-Core-Hardware und Reassembly-Free Deep Packet Inspection**
- **Application Intelligence, Control and Visualization**
- **Hochverfügbarkeitsfunktionen mit Stateful Failover und Lastverteilung**
- **Hohe Performance und niedrige TCO**
- **Netzwerkproduktivität**
- **Erweiterte Routing Services und Netzwerkfunktionen**
- **Standardisiertes VoIP**
- **SonicWALL Clean Wireless**
- **Integrierte QoS-Features**
- **Unterstützung für integrierte Module**

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® (RFDP) Technologie* bieten die Next-Generation Firewalls der SonicWALL® Network Security Appliance (NSA)-Serie umfassenden Netzwerkschutz, ohne die Performance zu beeinträchtigen. Die latenzarme 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 Intrusion Prevention mit Malware-Schutz sowie Application Intelligence Control and Visualization-Funktionen und liefert so eine herausragende Performance. 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 220, NSA 220 Wireless-N, NSA 250M, NSA 250M Wireless-N, NSA 2400, NSA 3500 und NSA 4500 bietet die NSA-Serie skalierbare Netzwerksicherheitslösungen für Unternehmen jeder Größenordnung.

Funktionen und Vorteile

Next-Generation Firewall. Die integrierten Funktionen Intrusion Prevention, Gateway Anti-Virus, Anti-Spyware, URL-Filtering, Application Intelligence and Control und SSL-Entschlüsselung verhindern, dass Bedrohungen in das Netzwerk gelangen und bieten eine gezielte Anwendungskontrolle, ohne die Performance zu beeinträchtigen.

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

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.

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.

Netzwerkproduktivität. IT-Verantwortliche können unerlaubte, nicht arbeitsrelevante Anwendungen und Websites wie Facebook® oder YouTube® identifizieren und die Bandbreite entsprechend drosseln oder sperren, wodurch das Netzwerk produktiver genutzt wird. In

Kombination mit den SonicWALL WAN Acceleration Appliance (WXA)-Lösungen lässt sich außerdem der WAN-Verkehr optimieren.

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.

SonicWALL Clean Wireless. Kann optional in Dual-Band Wireless-Modellen oder mit SonicWALL SonicPoint Wireless Access Points integriert werden und ermöglicht eine leistungsstarke und sichere 802.11a/b/g/n-3x3 MIMO-Wireless-Kommunikation. Mit den Clean Wireless-Lösungen lassen sich außerdem unberechtigte Wireless Access Points gemäß PCI DSS identifizieren.

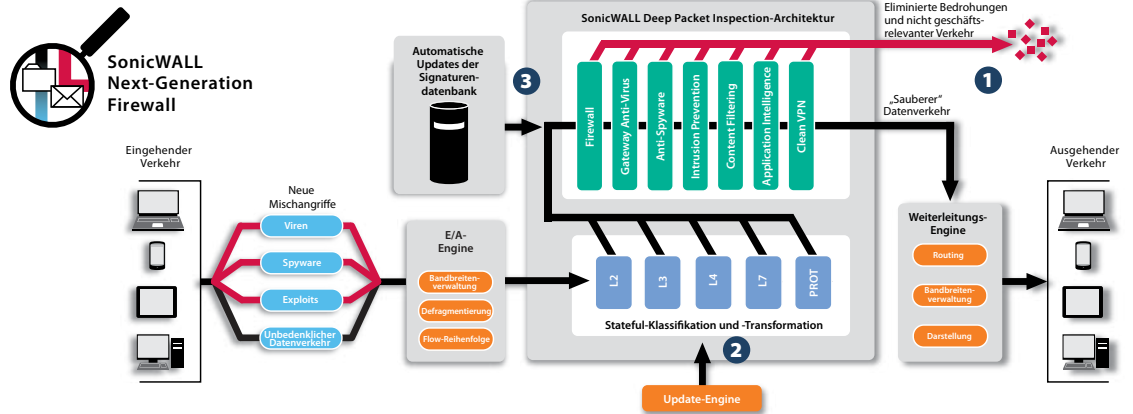
Integrierte QoS-Features. Gewährleisten dank 802.1p sowie DSCP (Differentiated Services Code Points) Class-of-Service-Kennungen eine leistungsfähige und flexible Bandbreitenverwaltung für VoIP, Multimedia und geschäftskritische Anwendungen.

Unterstützung für integrierte Module bei den NSA 250M- und NSA 250M Wireless-N-Appliances sorgt für reduzierte Anschaffungs- und Wartungskosten dank einer Konsolidierung der Geräte und ermöglicht mehr Flexibilität bei der Implementierung.

*U.S.-Patente 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™



Führende Sicherheitstechnologien

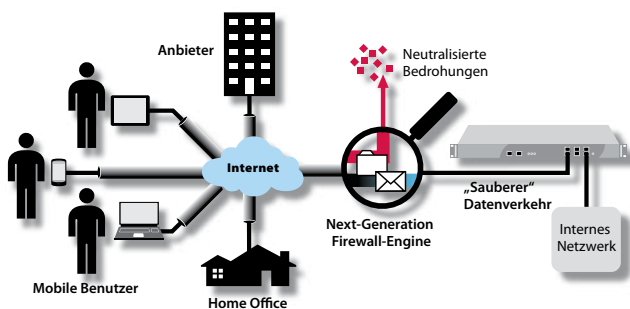
- 1 Die SonicWALL Deep Packet Inspection-Technologie bietet Schutz vor Gefährdungen wie Viren, Würmern, Trojanern, Spyware, Phishing-Angriffen, Internetmissbrauch und sonstigen Sicherheitsbedrohungen. Mit der Funktion Application Intelligence and Control lässt sich die Bandbreite auf der Anwendungsebene 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 and Control

Die Funktion SonicWALL Application Intelligence and Control 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 RFDPI-Technologie und ermöglicht die Erkennung und Kontrolle aktuell genutzter Anwendungen anhand einfacher vordefinierter Kategorien (wie Social Media oder Spiele) – unabhängig vom Port oder Protokoll. SonicWALLs Lösungen zur Analyse des Anwendungsverkehrs liefern einen detaillierten Einblick in aktuelle und historische von der Firewall übermittelte Daten einschließlich Anwendungsaktivitäten nach Benutzer.



SonicWALL Clean VPN

SonicWALL Clean VPN™ stellt die Vertrauenswürdigkeit von Remote-Benutzern und von Endpunkt-Geräten sicher und verwendet Sicherheitservices zum Schutz vor Malware, sowie Intrusion Prevention- und Application Intelligence and Control-Funktionen, die verhindern, dass böswillige Bedrohungen in das Unternehmensnetzwerk gelangen. Dies gewährleistet die Integrität des VPN-Zugriffs von Remote-Geräten (einschließlich Geräte mit iOS).



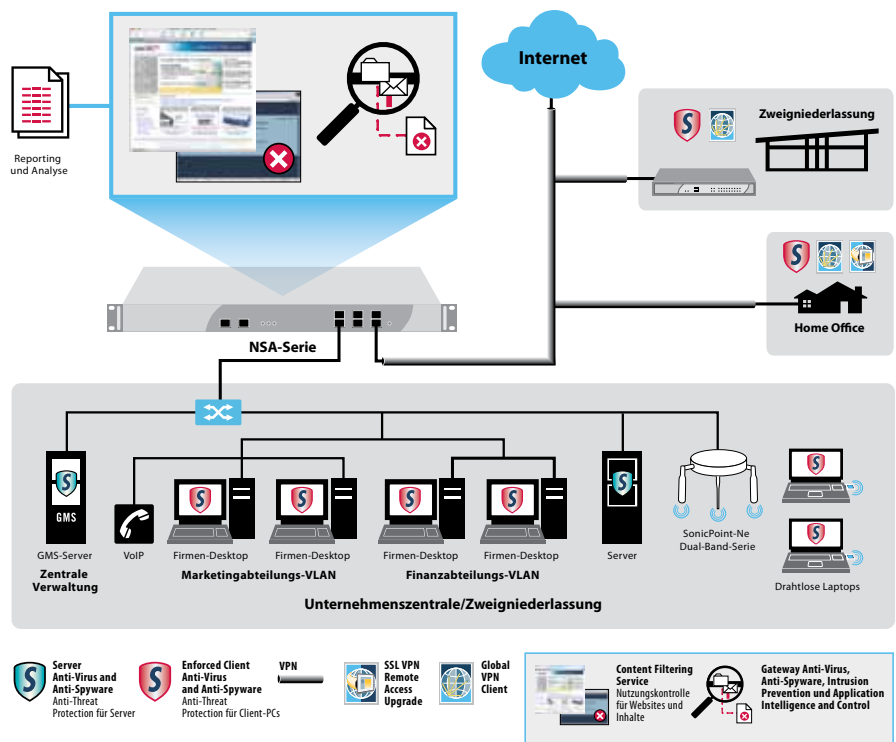
Zentralisierte Regelverwaltung

Die Network Security Appliance-Serie kann mit dem SonicWALL Global Management System verwaltet werden. Mithilfe flexibler, leistungsstarker und intuitiver Tools lassen sich damit von einer zentralen Stelle aus Konfigurationen verwalten, Überwachungsdaten in Echtzeit anzeigen, Regel- bzw. Compliance-Berichte erstellen und der Anwendungsverkehr analysieren.

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 and Control 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 größere verteilte Netzwerkumgebungen sowie für Unternehmenszentralen ausgelegt, die eine hohe Durchsatz-Kapazität und Performance benötigen.
- Die SonicWALL **NSA 3500** ist für verteilte Unternehmen sowie für die Zweigniederlassungen und Netzwerkumgebungen von Unternehmen geeignet, die eine erhebliche Durchsatz-Kapazität und Performance benötigen.
- Die SonicWALL **NSA 2400** ist ideal für Zweigniederlassungen und kleine bis mittlere Unternehmen geeignet, die ihre Durchsatz-Kapazität und Performance optimieren möchten.
- Die SonicWALL **NSA 220, NSA 220 Wireless-N, NSA 250M und NSA 250M Wireless-N** eignen sich optimal für Zweigniederlassungen in verteilten Netzwerkumgebungen sowie für kleine bis mittlere Unternehmen und für Einzelhandelsgeschäfte.



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 and Control 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.

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.

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

Vorabtausch von Hardware, damit Unternehmen ihre Investitionen in SonicWALL-Technologie bestmöglich nutzen können.

Global VPN Client-Upgrades 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.

SSL VPN Remote Access-Upgrades bieten PCs, Macs und Linux-Systemen einen clientlosen Remote-Zugriff auf Netzwerkebene. Die SonicWALL Firewall 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 auf dem Rechner des Benutzers installiert wird.

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

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

Firewall	NSA 220/W	NSA 250M/W	NSA 2400	NSA 3500	NSA 4500
SonicOS-Version	SonicOS 5.8.1.1				
Staatful-Durchsatz ¹	600 Mbit/s	750 Mbit/s	775 Mbit/s	1,5 Gbit/s	2,75 Gbit/s
GAU-Performance ²	115 Mbit/s	140 Mbit/s	160 Mbit/s	350 Mbit/s	690 Mbit/s
IPS-Performance ³	195 Mbit/s	250 Mbit/s	275 Mbit/s	750 Mbit/s	1,4 Gbit/s
Full DPI-Performance ⁴	110 Mbit/s	130 Mbit/s	150 Mbit/s	240 Mbit/s	600 Mbit/s
IMIX-Performance ⁵	180 Mbit/s	210 Mbit/s	235 Mbit/s	580 Mbit/s	700 Mbit/s
Max. Anzahl von Verbindungen ⁶	85.000	110.000	225.000	325.000	500.000
Max. Anzahl von DPI-Verbindungen	32.000	64.000	125.000	175.000	250.000
Neue Verbindungen/Sek.	2.200	3.000	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	24	32	48	64
VPN					
3DES/AES-Durchsatz ⁷	150 Mbit/s	200 Mbit/s	300 Mbit/s	625 Mbit/s	1,0 Gbit/s
Site-to-Site-VPN-Tunnel	25	50	75	800	1.500
Enthaltene Global VPN Client-Lizenzen (max.)	2 (25)	2 (25)	10 (250)	50 (1.000)	500 (3.000)
Enthaltene SSL VPN-Lizenzen (max.)	2 (15)	2 (15)	2 (25)	2 (30)	2 (30)
Inklusive Virtual Assist (max.)	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	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 Over VPN	Ja				
IPSec NAT-Traversal	Ja				
Redundantes VPN-Gateway	Ja				
Unterstützte Global VPN Client-Plattformen	Microsoft* Windows 2000, Windows XP, Microsoft* Vista 32/64-bit, Windows 7 32/64-bit				
Unterstützte SSL-Plattformen	Microsoft* Windows 2000 / XP / Vista 32/64 Bit / Windows 7, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE				
Unterstützte Mobile Connect-Plattform	iOS 4.2 und höher				
Sicherheitsservices					
Deep Packet Inspection Service	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Application Intelligence and Control				
Content Filtering Service	Prüfung nach HTTP URL, HTTPS IP, Schlüsselwörtern und Content, Blockieren von ActiveX, Java Applets und Cookies				
Premium Edition (CES)	Bandbreitenverwaltung nach Filterkategorien, Freigabe- und Sperrlisten				
Gateway-enforced Client Anti-Virus und Anti-Spyware	SonicWALL Enforced Client Anti-Virus und Anti-Spyware – McAfee				
Comprehensive Anti-Spam Service ⁸	Unterstützt				
Application Intelligence and Control	Verwaltung der Bandbreite von Anwendungen und Anwendungskontrolle, Priorisierung oder Sperren von Anwendungen nach Signaturen, Kontrolle von Dateitransfers, Scannen nach Schlüsselwörtern und -phrasen				
DPI SSL ⁹	Bietet die Möglichkeit, HTTPS-Verkehr transparent zu entschlüsseln, den Datenverkehr mit dem Deep Packet Inspection-Technologie von SonicWALL (GAV/AS/IPS/Application Intelligence/CES) 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-Clients), interner DHCP-Server, DHCP-Relay				
NAT-Modi	1:1, 1:many, many:1, many:many, flexible NAT (überlappende IPs), PAT, transparenter Modus				
VLAN Interfaces (802.1q)	25	35	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	150/150 Benutzer	250/250 Benutzer	300/500 Benutzer	1.000/1.000 Benutzer
VoIP	Voll H.323v1-S-kompatibel, SIP, Gatekeeper-Unterstützung, Verwaltung der ausgehenden Bandbreite, VoIP über WLAN, Deep Inspection Service, vollständige Interoperabilität mit den meisten VoIP-Gateway- und Kommunikationsgeräten				
System					
Zonenspezifische Sicherheitsfunktionen	Ja				
Zeitsteuerung	Einmalig, regelmäßig				
Object-based/Group-based Management	Ja				
DDNS	Ja				
Verwaltung und Überwachung	Web-Oberfläche (HTTP, HTTPS), Command Line (SSH, Konsole) SNMP v2; zentrale Verwaltung mit SonicWALL GMS				
Logging and Reporting	Analyzer, lokale Logdatei, Syslog, Solera Networks, NetFlow v5/v9, IPFIX mit Erweiterungen, Echtzeit-Visualisierung				
Hochverfügbarkeit	Active/Passive mit State Sync (optional)				
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-TLS				
Unterstützung für WAN-Beschleunigung ⁹	Ja				
Integriertes Wireless LAN					
Standards	802.11a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, PSK, 802.1x, EAP-PEAP, EAP-TLS)				
Virtual Access Points (VAPs) – Antennen (Diversity mit 5 dB)	Extern, drei, abnehmbar				
Sendeleistung – 802.11a/802.11b/802.11g	Max. 15,5 dBm/max. 18 dBm/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				
Empfangsleistung des Senders – 802.11a/802.11b/802.11g	-95 dBm MCS 0, -81 dBm MCS 15/-90 dBm bei 11 Mbit/s, -91 dBm bei 6 Mbit/s, -74 dBm bei 54 Mbit/s				
Empfangsleistung des Senders – 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-Ports, 1 Konsolenanschluss	(5) 10/100/1000 Kupfer-Gigabit-Ports, 2 USB-Ports, 1 Konsolenanschluss Modul-Slot		(6) 10/100/1000 Kupfer-Gigabit-Ports, 1 Konsolenanschluss, 2 USB-Ports	
Modul	Nein	Ja	Nein	Nein	Nein
Speicher (RAM)	512 MB				
Flash-Speicher	32 MB Compact Flash				
3G Wireless/Modem**	Mit 3G/4G-USB-Adapter/Modem		Mit 3G/4G-USB-Adapter/Modem		
Stromversorgung	Externe 36 W-Stromversorgung		Single-180 W ATX-Stromversorgung		
Fans	Kein Lüfter/1 interner Lüfter	2 interne Lüfter	10-240 V, 50-60 Hz		2 Lüfter
Netzspannung					
Maximale Leistungsaufnahme	11 W/15 W	12 W/16 W	42 W	64 W	66 W
Wärmeabgabe	37 BTU/50 BTU	41 BTU/55 BTU	144 BTU	219 BTU	225 BTU
Zertifikate	VPNC, ICSA Firewall 4.1		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1, IPv6 Phase 2		
Ausstehende Zertifikate	EAL4+, FIPS 140-2 Level 2, IPv6 Phase 1, IPv6 Phase 2		—		
Gehäuse und Abmessungen	Rackfähig (1 HE)/ 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	0,88 kg/ 0,97 kg	1,38 kg/ 1,43 kg	3,65 kg	5,14 kg	
WEEE-Gewicht	1,38 kg/ 1,56 kg	2,0 kg/ 2,11 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, TÜVGS, CB, NOM, RoHS, WEEE				
Umgebungstemperatur	0-40° C			5-40° C	
MTBF	28 Jahre/15 Jahre	23 Jahre/14 Jahre	14,3 Jahre	14,1 Jahre	14,1 Jahre

¹ Testmethoden: Maximale Leistung 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 Ixia Test-Tools. Die Tests erfolgen mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren. ³ Die tatsächliche maximale Anzahl von Verbindungen ist bei aktivierten Next Generation Firewall-Services niedriger. ⁴ VPN-Durchsatzmessung mittels UDP-Verkehr mit 1280 Bytes pro Paket gemäß RFC 2544. ⁵ Unterstützung auf der NSA 3500 und höher. ⁶ Nicht für die NSA 2400 verfügbar. ⁷ USB-3G-Karte und Modem sind nicht enthalten. Weitere Informationen zu den unterstützten USB-Geräten: <http://www.sonicwall.com/us/products/cardsupport.html>. ⁸ Der Comprehensive Anti-Spam Service unterstützt beliebig viele Benutzer, wobei die empfohlene Anzahl 250 Benutzer oder weniger beträgt. ⁹ Mit SonicWALL WXA-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 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 and Control Service, Content Filtering Service und Dynamic Support 24/7



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

