



FIREWALL

Next-Generation Firewall

- **Next-Generation Firewall**
- **Application Intelligence, Anwendungskontrolle und -visualisierung**
- **Reassembly-Free Deep Packet Inspection-Technologie**
- **Leistungsstarke Intrusion Prevention**
- **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) E8500 ist eine Firewall der nächsten Generation mit Intrusion Prevention, effektivem Schutz vor Malware sowie leistungsstarken Funktionen zur Überwachung, Kontrolle und Visualisierung von Anwendungen. Mit der patentierten SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI)-Technologie* kann die NSA E8500 über 2.800 unterschiedliche Anwendungen analysieren und kontrollieren – selbst, wenn sie mit SSL verschlüsselt sind. Die RFDPI-Engine von SonicWALL kann hunderttausende Verbindungen gleichzeitig und parallel über alle Ports ohne Einschränkungen beim Datenvolumen und mit minimalen Latenzzeiten prüfen. Dank ihrer außergewöhnlichen Kombination von ausgereifter Software und extrem leistungsstarker Hardware lässt die NSA E8500 Anwendungsverkehr kaum eine Chance, im Netzwerk unentdeckt zu bleiben.

Die NSA E8500 kann inline oder als Gateway eingesetzt werden. Wird die Appliance als Inline-Lösung im Netzwerk implementiert, können Administratoren die bestehende Infrastruktur beibehalten und Funktionen zur Analyse und Kontrolle auf der Anwendungsebene als zusätzliche Schicht für mehr Sicherheit und Transparenz hinzufügen. Die NSA E8500 eignet sich auch als umfassendes Sicherheitsgateway und bietet alle Remote Access-, Hochverfügbarkeits- und Enterprise-Funktionen, die für die Implementierung in einer anspruchsvollen Netzwerkumgebung erforderlich sind.

Funktionen und Vorteile

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

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.

*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)

Technische Daten



SonicWALL NSA E8500
01-SSC-8866

Inklusive DPI SSL-Lizenz und 1 Jahr Security Services mit IPS/GAV/Anwendungskontrolle



SonicWALL NSA E8500 High Availability
01-SSC-8867

NSA E8500	
Firewall	
Stateful-Durchsatz ¹	8,0 GBit/s
IPS-Performance ²	3,7 GBit/s
GAV-Performance ³	2,25 GBit/s
Full Deep Packet Inspection (DPI)-Performance ⁴	2,2 GBit/s
IMIX-Performance ²	2,0 GBit/s
Max. Anzahl von Verbindungen ³	1.500.000
Max. Anzahl von DPI-Verbindungen	1.250.000
Neue Verbindungen/Sekunde	80.000
Unterstützte Nodes	Unlimitiert
Schutz vor Denial of Service-Angriffen	22 Kategorien von DoS-, DDoS- und Scan-Angriffen
Unterstützte SonicPoints (max.)	128
VPN	
3DES/AES-Durchsatz ⁴	4,0 Gbit
Site-to-Site VPN-Tunnel	10.000
Enthaltene Global VPN Client-Lizenzen (max.)	2.000 (10.000)
Enthaltene SSL VPN-Lizenzen (max.)	2 (50)
Inklusive Virtual Assist-Techniker (max.)	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 (enthalten), Gateway Anti-Virus, Anti-Spyware, Application Intelligence and Control (enthalten)
Content Filtering Service (CFS) Premium Edition	HTTP URL, HTTPS IP Schlüsselwort- und Inhaltsprüfung, Blockieren von ActiveX, Java Applet und Cookies, Bandbreitenverwaltung nach Filterkategorien, Freigabe- und Sperlisten
Enforced Client Anti-Virus and 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 (enthalten)	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 und bidirektional 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.
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)	512
Routing	OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing, Multicast
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminal Services, Citrix
IPv6	kompatibel
Interne Datenbank/Single Sign-On-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 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 (mit SonicPoint APs)	802.11 a/b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TLS
Hardware	
Schnittstellen	4 Gigabit Ethernet-Schnittstellen, 4 SFP-Ports (SX, LX oder TX), 1 GbE HA-Schnittstelle, 2 USB-Ports, 1 Konsolenschnittstelle
Speicher (RAM)	2 GB
Flash-Speicher	512 MB Compact Flash
3G Wireless/Modem*	Mit USB-3G-Adapter/Modem
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	150 W
Wärmeabgabe	511,5 BTU
MTBF	12,4 Jahre
Zertifikate	Ausstehend: EAL4+, FIPS 140-2, ICSA Firewall 4.1; Aktuell: VPNC
Gehäuse	Rackfähig (1 HE)
Abmessungen	43,2 x 42,5 x 4,4 cm
Gewicht	7,9 kg
WEEE-Gewicht	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 Ixia Test-Tools. Die Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren. ³ Die tatsächliche maximale Anzahl von Verbindungen ist niedriger, wenn die vollen DPI-Services aktiviert sind. ⁴ VPN-Durchsatzmessung mittels UDP-Verkehr mit 1280 Bytes pro Paket gemäß RFC 2544. *USB-3G-Karte und Modem sind nicht enthalten. Weitere Informationen zu den unterstützten USB-Geräten: <http://www.sonicwall.com/us/products/cardsupport.html> ⁵ Der Comprehensive Anti-Spam Service unterstützt beliebig viele Benutzer, wobei die empfohlene Anzahl 250 Benutzer oder weniger beträgt.

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™

