



FIREWALL

Firewall di nuova generazione

- **Firewall di nuova generazione**
- **Potente prevenzione delle intrusioni**
- **Controllo intelligente e visualizzazione delle applicazioni**
- **Tecnologia Reassembly-Free Deep Packet Inspection**
- **Implementazione flessibile**
- **Ispezione Deep Packet del traffico crittografato con SSL (DPI SSL)**
- **Rete SonicWALL GRID (Global Response Intelligent Defense)**

Per gli amministratori IT può essere una vera e propria sfida garantire l'uso efficace di soluzioni aziendali mission-critical e, al tempo stesso, contrastare l'utilizzo di applicazioni inutili e spesso pericolose da parte dei dipendenti. Le applicazioni d'importanza strategica richiedono la massima priorità nell'utilizzo della banda disponibile, mentre quelle di social media e gaming devono essere limitate nell'accesso alla banda o completamente bloccate. I firewall con ispezione Stateful Packet utilizzati in molte aziende controllano le porte e i protocolli, ma non sono in grado di risolvere questo problema in quanto non riescono a identificare le applicazioni. In poche parole, i firewall con ispezione Stateful Packet non sono in grado di distinguere il traffico "buono" da quello "cattivo".

L'appliance E-Class NSA (Network Security Appliance) E8500 di SonicWALL® fornisce un firewall di nuova generazione che include prevenzione delle intrusioni, protezione anti-malware e potenti funzioni di visualizzazione e controllo intelligente delle applicazioni. Mediante la brevettata tecnologia SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI)*, l'NSA E8500 è in grado di analizzare e controllare più di 2.800 applicazioni, anche se crittografate con SSL. Questa eccezionale combinazione di sofisticazione software e potenza hardware impedisce al traffico delle applicazioni di nascondersi nella rete. Il motore RFDPI di SonicWALL consente infatti di ispezionare centinaia di migliaia di connessioni simultaneamente su tutte le porte, con una latenza pari quasi a zero e una dimensione illimitata dei file.

L'NSA E8500 può essere implementato sia in linea che come gateway in una rete. Quando utilizzato come soluzione in linea, l'NSA E8500 consente agli amministratori di mantenere l'infrastruttura esistente aggiungendo al contempo la protezione e il controllo a livello delle applicazioni come ulteriore livello di sicurezza e di visibilità della propria rete. L'NSA E8500 può anche essere installato come gateway di sicurezza tradizionale, offrendo tutte le funzionalità di accesso remoto, elevata disponibilità e servizi di classe aziendale richiesti nelle implementazioni più complesse.

Caratteristiche e vantaggi

Il **firewall di nuova generazione** di SonicWALL con tecnologia Reassembly-Free Deep Packet Inspection™ (RFDPI) include prevenzione delle intrusioni, protezione anti-malware e controllo intelligente delle applicazioni, ora ampliato con la visualizzazione in tempo reale.

La **potente prevenzione delle intrusioni** protegge da una vasta gamma di attacchi a livello di applicazione basati sulla rete mediante la scansione dei payload dei pacchetti alla ricerca di worm, Trojan, vulnerabilità del software, exploit di applicazioni e altro codice maligno.

Il **controllo intelligente con visualizzazione delle applicazioni** offre funzioni di controllo granulare e visualizzazione in tempo reale delle applicazioni per gestire la larghezza di banda secondo criteri di priorità, garantendo il massimo livello di protezione di rete e produttività.

La **tecnologia Reassembly-Free Deep Packet Inspection** protegge la rete in modo automatico e trasparente monitorando oltre 2.800 applicazioni, rilevando milioni di malware e ispezionando centinaia di migliaia di connessioni simultaneamente su tutte le porte, con una latenza pari quasi a zero e una dimensione illimitata dei file.

L'**implementazione flessibile** come gateway tradizionale o come soluzione in linea consente agli amministratori di mantenere l'infrastruttura esistente, aggiungendo la protezione e il controllo a livello delle applicazioni come ulteriore livello di sicurezza e di visibilità della propria rete.

L'**ispezione Deep Packet del traffico crittografato con SSL (DPI SSL)** decifra e scansiona in modo trasparente il traffico HTTPS in entrata e in uscita utilizzando il motore RFDPI di SonicWALL. Se non vengono rilevate minacce o vulnerabilità, il traffico esaminato viene poi ricodificato e inviato alla destinazione prevista.

La **rete SonicWALL GRID (Global Response Intelligent Defense)** aggiorna costantemente - 24 ore al giorno, 7 giorni la settimana - i servizi di protezione dalle minacce, prevenzione e rilevamento delle intrusioni e controllo degli applicativi per ottimizzare la sicurezza. La suite completa di servizi di prevenzione delle minacce offre protezione contro più di un milione di attacchi malware.

*Brevetto USA 7310815 - A method and apparatus for data stream analysis and blocking (Metodo e dispositivo per l'analisi e il bloccaggio di flussi di dati).

Specifiche tecniche



SonicWALL NSA E8500
01-SSC-8866

Include una licenza DPI SSL e 1 anno di servizi di sicurezza, inclusi IPS/GAV/Application Control



SonicWALL NSA E8500 ad alta disponibilità
01-SSC-8867

NSA E8500	
Firewall	
Throughput Stateful ¹	8,0 Gbps
Prestazioni IPS ²	3,7 Gbps
Prestazioni GAV ²	2,25 Gbps
Prestazioni Deep Packet Inspection (DPI) completo ²	2,2 Gbps
Prestazioni IMIX ²	2,0 Gbps
Connessioni (max.) ³	1.500.000
Connessioni DPI (max.)	1.250.000
Nuove connessioni/sec.	80.000
Nodi supportati	illimitati
Prevenzione attacchi Denial of Service	22 classi di attacchi DoS, DDoS e scanning
SonicPoint supportati (max.)	128
VPN	
Throughput 3DES/AES ⁴	4,0 Gbps
Tunnel VPN site-to-site	10.000
Licenze Global VPN Client in bundle (max.)	2.000 (10.000)
Licenze SSL VPN in bundle (max.)	2 (50)
Tecnici Virtual Assist in bundle (max.)	1 (25)
Crittografia/autenticazione/gruppi DH	DES, 3DES, AES (a 128, 192, 256 bit)/MD5, SHA-1/Gruppi DH 1, 2, 5, 14
Scambio delle chiavi	IKE, IKEv2, connessione manuale, PKI (X.509), L2TP over IPSec
VPN route-based	Si (OSPF, RIP)
Supporto certificati	Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA per VPN da SonicWALL a SonicWALL, SCEP
Gateway ridondante	Si
Piattaforme Global VPN Client supportate	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32 bit/64 bit, Windows 7
Piattaforme SSL VPN supportate	Microsoft® Windows 2000 / XP / Vista 32/64 bit / Windows 7, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE
Servizi di sicurezza	
Servizio d'ispezione Deep Packet	Intrusion Prevention (incluso), Gateway Anti-Virus, Anti-Spyware, Application Intelligence and Control (incluso)
Content Filtering Service (CFS), edizione Premium	Scansione HTTP URL, HTTPS IP, parole chiave e contenuti, blocco controlli ActiveX, applet Java e cookie, gestione della banda per le categorie di filtraggio, liste di autorizzazione/blocco
Enforced Client Anti-Virus and Anti-Spyware	HTTPS, SMTP, POP3, IMAP e FTP, blocco degli allegati e-mail mediante client McAfee™ imposto
Comprehensive Anti-Spam Service ⁵	Supportato
Application Intelligence and Control (incluso)	Gestione e controllo della larghezza di banda delle applicazioni, prioritizzazione o blocco delle applicazioni in base alle signature, controllo dei trasferimenti di file, scansione in base a parole o frasi chiave
DPI SSL	Possibilità di decifrare il traffico HTTPS in ingresso e in uscita in modo trasparente, scansionarlo alla ricerca di minacce con la Deep Packet Inspection (GAV/AS/IPS/Application Intelligence/CFS) di SonicWALL e infine di ricodificarlo e inviarlo a destinazione se non vengono rilevate minacce o vulnerabilità.
Networking	
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay
Modalità NAT	1:1, 1:many, many:1, many:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente
Interfacce VLAN (802.1q)	512
Routing	OSPF, RIPv1/v2, route statici, routing basato su policy, Multicast
QoS (Quality of Service)	Priorità larghezza di banda, larghezza di banda massima / garantita, DSCP marking, 802.1p
Autenticazione	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, database utenti interno, servizi Terminal Server, Citrix
IPv6	compatibile
Database interno/Single Sign-on utenti	2.500/7.000 utenti
VoIP	H.323 v. 1-5, SIP, supporto gatekeeper, gestione larghezza di banda in uscita, VoIP over WLAN, protezione Deep Inspection, interoperabilità completa con la maggior parte dei gateway VoIP e dispositivi di comunicazione
Aggregazione del link	Si
Ridondanza delle porte	Si
Sistema	
Gestione e monitoraggio	Web GUI (HTTP, HTTPS), linea di comando (SSH, Console), SNMP v2: Gestione globale con SonicWALL GMS
Logging e reporting	ViewPoint, registro locale, Syslog, reti Solera, NetFlow v5/v9, IPFIX con estensioni, visualizzazione in tempo reale
Alta disponibilità	Attiva/passiva con State Sync, DPI attiva/attiva con State Sync
Bilanciamento del carico	Si (in uscita con modalità percentuale, round robin e spill-over, in entrata con round robin, distribuzione casuale, sticky IP, rimappatura blocchi e simmetrica)
Standard	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3
Standard wireless (con i punti di accesso SonicPoint)	802.11 a/b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TTLS
Hardware	
Interfacce	4 Gigabit Ethernet, 4 SFP (SX, LX o TX), 1 Gigabit Ethernet ad alta disponibilità, 2 USB, 1 console
Memoria (RAM)	4 GB
Memoria Flash	512 MB Compact Flash
3G Wireless/modem*	Con adattatore 3G USB/modem
Alimentazione	Alimentatore doppio (250 W ATX), hot swap
Ventole	Due ventilatori hot swap
Display	Display LCD anteriore
Tensione d'esercizio	100-240 V AC, 60-50 Hz
Potenza max. assorbita	150 W
Calore sviluppato	511,5 BTU
MTBF	12,4 anni
Certificazioni	In attesa: EAL4+, FIPS 140-2, ICSA Firewall 4.1. Attualmente: VPNC
Fattore di forma	1U rack-mountable
Misure	43,2 x 42,5 x 4,4 cm
Peso	7,9 kg
Peso sec. WEEE	7,9 kg
Principali normative di conformità	FCC Class A, CES Class A, CE, C-Tick, VCCI, MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE
Condizioni ambientali	da 5 a 40 °C
Umidità	10-90%, non condensante

¹ Metodologie di test: prestazioni massime come da RFC 2544 (per il firewall). Le prestazioni effettive possono variare in base alle condizioni della rete e ai servizi attivati. ² Rilevazione throughput per DPI completo/Gateway AV/Anti-Spyware/IPS tramite il test di performance Spirent WebAvalanche HTTP standard nell'industria e gli strumenti di test Ixia. Test eseguiti con flussi multipli attraverso coppie di porte multiple. ³ Il numero massimo effettivo di connessioni diminuisce quando sono attivati i servizi DPI completi. ⁴ Rilevazione throughput VPN tramite traffico UDP con pacchetti da 1280 byte, in conformità a RFC 2544. *Scheda USB 3G e modem non inclusi. Per i dispositivi USB supportati vedi <http://www.sonicwall.com/us/products/cardsupport.html> ⁵ Il Comprehensive Anti-Spam Service supporta un numero illimitato di utenti ma è consigliato per un massimo di 250 utenti.

Linea di soluzioni di sicurezza dinamica SonicWALL



SICUREZZA
DI RETE



ACCESSO
REMOTO SICURO



SICUREZZA
WEB / E-MAIL



BACKUP E
RECOVERY



GESTIONE
BASATA SU POLICY

SonicWALL Italy
T + 39.010.7407851
Italy@sonicwall.com

Contatti Supporto SonicWALL

www.sonicwall.com/emea/4724.html **DYNAMIC SECURITY FOR THE GLOBAL NETWORK™**

SONICWALL®