SonicWALL E-CLASS Network Security Appliance

SICUREZZA DI RETE

SonicWALL NSA E8500 – Protezione e controllo a livello delle applicazioni

- **Protezione e controllo a livello delle applicazioni**
- **Strumenti di visualizzazione intuitivi**
- **Ispezione approfondita dei pacchetti reassembly-free di SonicWALL**
- **Potente prevenzione delle intrusioni**
- **Implementazione flessibile**
- **Sicurezza dinamica**
- **Ispezione Deep Packet del traffico crittografato con SSL (DPI SSL)**

Un problema fondamentale per i CIO e gli amministratori IT è che, nonostante i continui sforzi per aumentare la produttività della forza lavoro e migliorare la qualità dei servizi interni, continua a mancargli visibilità sul traffico totale che attraversa le loro reti. Le informazioni sul traffico di rete sono necessarie per creare analisi accurate delle prestazioni, scoprire le minacce ed essere in grado di reagire immediatamente, garantendo un funzionamento ininterrotto dei sistemi mission-critical.

Gli strumenti convenzionali, che identificano i protocolli in base alle rispettive porte, hanno sempre più difficoltà a proteggere e controllare il traffico in quanto le nuove applicazioni sono maggiormente basate sul Web e utilizzano sempre più spesso protocolli standard quali HTTP e HTTPS. Di conseguenza i firewall tradizionali non riescono più a rilevare il traffico applicativo che attraversa la rete, le eventuali minacce veicolate da queste applicazioni e un loro utilizzo inefficiente della rete. Ad esempio il traffico HTTP/HTTPS, che risulta innocuo a un firewall tradizionale, può trasportare applicazioni ad alto consumo di banda e potenzialmente pericolose per la sicurezza, quali streaming video/audio, traffico chat e documenti di vario formato. Lo stesso vale per i siti di social networking che, pur non essendo formalmente classificati come vere e proprie applicazioni, utilizzano le stesse tecnologie e quindi espongono le aziende al malware e sottraggono larghezza di banda alle applicazioni mission-critical. Per riprendere il controllo su questo traffico, i firewall tradizionali devono evolversi oltre la semplice ispezione di tipo stateful ed essere in grado di analizzare il traffico a livello applicativo. L'unica tecnologia capace di monitorare tutte queste nuove attività in rete è l'ispezione approfondita dei pacchetti (Deep Packet Inspection).

L'appliance E-Class NSA (Network Security Appliance) E8500 di SonicWALL offre sicurezza dinamica per la rete globale grazie alle potenti funzionalità di controllo intelligente delle applicazioni e di prevenzione e rilevamento delle intrusioni in rete. Mediante il brevettato motore SonicWALL® Reassembly-Free Deep Packet Inspection™ (RFDPI) e sofisticate capacità di Application intelligence, l'NSA E8500 è in grado di analizzare e controllare più di 1.100 applicazioni singole, sia crittografate con SSL che non crittografate. Questa eccezionale combinazione di sofisticazione software e potenza hardware impedisce al traffico delle applicazioni di nascondersi nella rete. Il brevettato motore RFDPI™ di SonicWALL consente infatti di ispezionare centinaia di migliaia di connessioni simultaneamente su 65.535 porte, con una latenza pari quasi a zero e una dimensione illimitata degli stream.

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

Protezione e controllo a livello delle applicazioni mediante un set configurabile di policy granulari, applicabili in base all'utente, all'applicazione, all'orario o al subnet IP. Queste policy possono essere utilizzate per limitare il trasferimento di determinati file e documenti, effettuare la scansione di allegati e-mail in base a criteri configurabili dall'utente, automatizzare l'allocazione della larghezza di banda per le applicazioni, controllare e ispezionare l'accesso Web sia interno che esterno e consentire agli utenti di aggiungere signature personalizzate.

Gli **strumenti di visualizzazione intuitivi** offrono agli amministratori IT un'ampia gamma di data point sulle applicazioni che attraversano la rete, compreso chi le sta utilizzando e l'impatto potenziale sulla sicurezza.

L'**ispezione approfondita dei pacchetti reassembly-free di SonicWALL** è in grado di controllare oltre 1.100 singole applicazioni sulla rete e ispezionare centinaia di migliaia di connessioni simultaneamente su 65.535 porte, con una latenza pari quasi a zero e una dimensione illimitata degli stream.

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, applicativi peer-to-peer (P2P) e di messaggistica istantanea, backdoor exploit e altro codice maligno.

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.

La **sicurezza dinamica** 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 1.000.000 di attacchi malware.

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.

SONICWALL®

PROTEZIONE ALLA VELOCITÀ DEL BUSINESS

Specifiche tecniche

SonicWALL NSA E8500

Nota: i dati prestazionali e le capacità del prodotto sono soggetti a modifiche prima della messa in commercio del prodotto.

Certificazioni

Common Criteria EAL4+ CERTIFIED

ICSA labs CERTIFIED FIREWALL - CORPORATE

	NSA E8500
Firewall	
Throughput Stateful[1]	8,0 Gbps
Prestazioni IPS[2]	3,5 Gbps
Prestazioni GAV[2]	2,3 Gbps
Prestazioni UTM[2]	2,0 Gbps
Prestazioni IMIX[2]	2,0 Gbps
Connessioni (max.)[3]	3.000.000
Connessioni DPI (max.)	1.500.000
Nuove connessioni/sec.	60.000
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	Sì (OSPF, RIP)
Supporto certificati	Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA per VPN da SonicWALL a SonicWALL, SCEP
Gateway ridondante	Sì
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	Prevenzione intrusioni (incluso), gateway anti-virus, anti-spyware e Application Intelligence (incluso)
Content Filtering Service (CFS), edizione Premium	Scansione HTTP URL, HTTPS IP, parole chiave e contenuti, blocco controlli ActiveX, applet Java e cookie
Client anti-virus e anti-spyware imposti sul gateway	HTTP/S, SMTP, POP3, IMAP e FTP, Enforced McAfee™ Client, blocco degli allegati e-mail
Comprehensive Anti-Spam Service	Sì
Application Intelligence (incluso)	Implementazione a livello di applicazioni e monitoraggio della larghezza di banda, regolazione di traffico web, e-mail, allegati e-mail e trasferimenti di file, scansione e blocco di documenti e file in base a parole/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
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
Alta disponibilità	Attiva/passiva con State Sync, UTM attiva/attiva con State Sync
Bilanciamento del carico	Sì (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	1 console, 4 Gigabit Ethernet, 4 SFP (SX, LX o TX), 1 Gigabit Ethernet ad alta disponibilità, 2 USB
Memoria (RAM)	2 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	EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1
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 UTM/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 UTM.

[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

Linea di protezione completa 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

SONICWALL®
PROTEZIONE ALLA VELOCITÀ DEL BUSINESS