

- **Firewall di nuova generazione**
- **Connettività a 10 GbE**
- **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)**
- **Accelerazione WAN**

Oggi le applicazioni aziendali risiedono sia sulla rete che nel cloud e possono includere soluzioni aziendali produttive come pure applicazioni controproducenti e spesso pericolose. 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 addirittura completamente bloccate. I tradizionali firewall con ispezione Stateful Packet scansionano solo le porte e i protocolli — ma non le applicazioni — e quindi non sono in grado di distinguere le applicazioni "buone" da quelle "cattive".

Le soluzioni della serie E-Class NSA (Network Security Appliance) di SonicWALL® forniscono prestazioni di classe enterprise quali prevenzione delle intrusioni, protezione anti-malware e funzioni di visualizzazione e controllo intelligente delle applicazioni. Grazie alla combinazione della brevettata tecnologia Reassembly-Free Deep Packet Inspection™ (RFDPI)* di SonicWALL con una potente piattaforma hardware multi-core, la serie E-Class NSA è in grado di analizzare e monitorare migliaia di applicazioni, anche quelle crittografate con SSL. Le soluzioni della serie E-Class NSA possono essere implementate come firewall di nuova generazione o come firewall UTM (Unified Threat Management).

La serie E-Class NSA, composta dalle appliance SonicWALL E-Class NSA E8510, E8500, E7500, E6500 e E5500, offre un'ampia gamma di soluzioni scalabili per qualsiasi esigenza di implementazione in data center, reti aziendali e universitarie e ambienti distribuiti. Se utilizzate come soluzioni in linea, le appliance della serie E-Class NSA sfruttano l'infrastruttura esistente aggiungendo un ulteriore livello di sicurezza e di visibilità della rete. Se implementate come gateway di sicurezza, offrono funzioni aggiuntive come accesso remoto sicuro, alta disponibilità e altre caratteristiche di classe enterprise.

La serie E-Class NSA è parte integrante della gamma di prodotti e servizi SonicWALL di classe enterprise per la sicurezza di rete, la protezione della posta elettronica e l'accesso remoto sicuro.

Caratteristiche e vantaggi

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

Grazie alla **connettività a 10 GbE**, l'NSA E8510 può essere implementato in ambienti con un'infrastruttura a 10 GbE.

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 migliaia di 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.

L'**accelerazione WAN** riduce la latenza e aumenta le velocità di trasferimento tra siti remoti, favorendo una maggiore efficienza della rete.

* Brevetti USA 7,310,815; 7,600,257; 7,738,380; 7,835,361

Tecnologia di analisi e controllo intelligente delle applicazioni

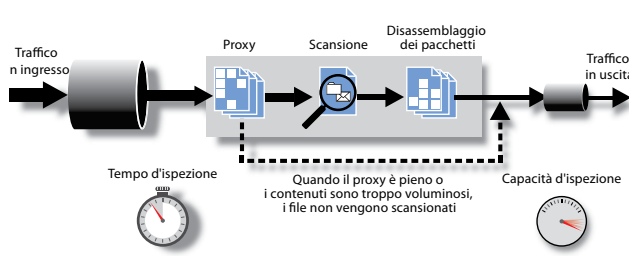
SonicWALL Application Intelligence and Control offre funzioni di controllo granulare e visualizzazione in tempo reale delle applicazioni che consentono di gestire la larghezza di banda secondo criteri di priorità, garantendo il massimo livello di protezione di rete e produttività. Questa funzionalità, integrata nei firewall SonicWALL di nuova generazione, utilizza la tecnologia Reassembly-Free Deep Packet Inspection per identificare e controllare le applicazioni in uso, indipendentemente dalla porta e dal protocollo. Con un database di signature delle minacce in continua espansione, attualmente in grado di rilevare oltre 3.500 applicazioni e milioni di minacce malware, consente di mantenere un controllo granulare delle applicazioni, limitare o assegnare priorità alla banda disponibile e rifiutare l'accesso a determinati siti Web. Il SonicWALL App Flow Monitor fornisce grafici in tempo reale relativi ad applicazioni in uso, banda in ingresso e in uscita, connessioni attive a siti Web e attività degli utenti, con possibilità di inviare dati in modo continuo agli analizzatori NetFlow/IPFIX.



Motore Reassembly-Free Deep Packet Inspection

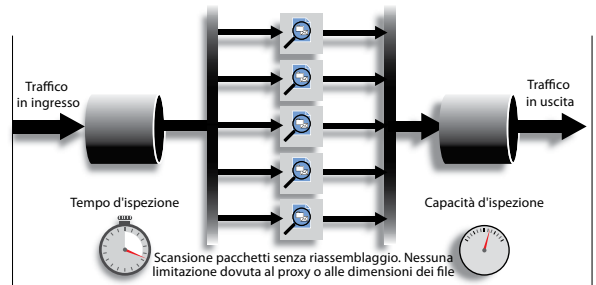
Il Reassembly-Free Deep Packet Inspection di SonicWALL è un motore d'ispezione a livello applicativo scalabile, in grado di analizzare in tempo reale file e contenuti di qualsiasi dimensione senza la necessità di riassemblare i pacchetti o il contenuto delle applicazioni. Questo innovativo strumento d'ispezione, sviluppato specificamente per applicazioni in tempo reale e traffico sensibile ai ritardi, offre funzioni di controllo senza alcuna connessione proxy. Il traffico di rete ad alta velocità viene così ispezionato con maggiore efficienza e affidabilità, migliorando l'esperienza degli utenti finali.

Elaborazione basata sull'assemblaggio dei pacchetti



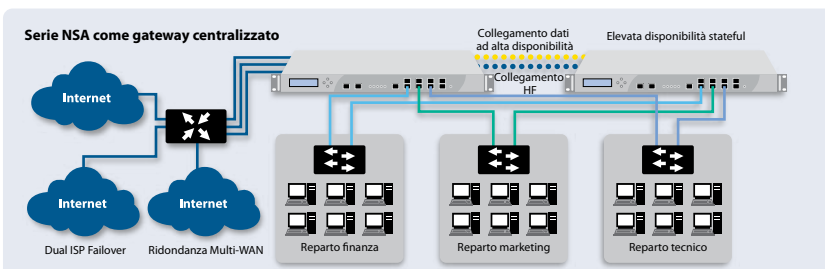
Architettura della concorrenza

Elaborazione senza riassetto dei pacchetti



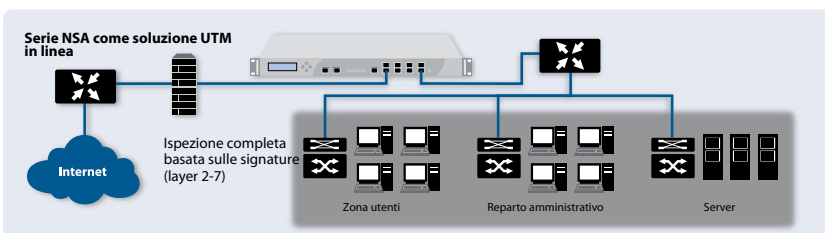
Architettura SonicWALL

Opzioni d'implementazione flessibili e personalizzabili



Gateway centralizzato

Le appliance della serie E-Class NSA, implementate a livello gateway presso la sede centrale di un'azienda, forniscono una piattaforma scalabile ad alta velocità per un'efficace segmentazione e protezione della rete tramite VLAN e zone di sicurezza. Le funzionalità di ridondanza includono bilanciamento del carico WAN, ISP failover e DPI attiva/attiva.



Modalità Bridge (Layer 2)

La modalità bridge di livello 2 garantisce il rilevamento e la prevenzione di intrusioni in linea, aggiungendo un livello di protezione a zone supplementare per segmenti di rete e reparti aziendali e semplificando al contempo la protezione multilivello. Gli amministratori IT possono così limitare l'accesso a dati sensibili presenti in unità aziendali o server database specifici.

Protezione multilivello

Protezione di postazioni remote

Le appliance della serie E-Class NSA integrano VPN (Virtual Private Network) ad altissime prestazioni e facilmente scalabili in migliaia di end point e uffici remoti. L'innovativa tecnologia Clean VPN™ di SonicWALL blocca eventuali vulnerabilità e codici maligni "filtrando" in tempo reale il traffico prima che entri nella rete aziendale, senza alcuna necessità d'intervento da parte dell'utente.

Protezione al gateway

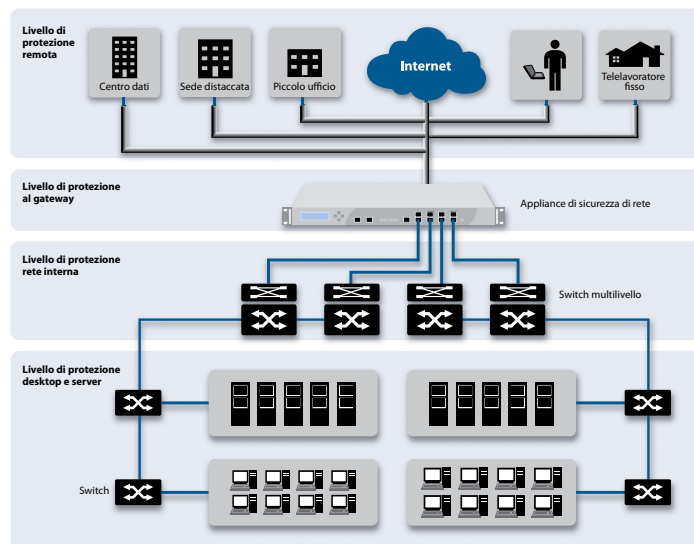
Facilmente integrabili in ambienti di rete esistenti, le appliance E-Class NSA offrono una protezione centralizzata – a livello gateway – per applicativi, file e traffico basato sui contenuti in entrata e in uscita e il monitoraggio della larghezza di banda e delle applicazioni senza compromettere le prestazioni o la scalabilità del sistema.

Protezione interna

Le soluzioni della serie E-Class NSA ad alta configurabilità estendono la protezione alla rete interna ispezionando il traffico in transito attraverso le interfacce LAN e le reti VLAN. Create appositamente per contrastare le minacce alle reti LAN, le appliance della serie E-Class NSA controllano e bloccano codice dannoso a livello interno, attacchi Denial of Service, exploit e vulnerabilità software, documenti riservati, violazioni delle policy e un utilizzo improprio della rete.

Protezione a livello desktop e server

Oltre alla protezione a livello di rete e di gateway, la serie E-Class NSA fornisce protezione aggiuntiva per server e workstation presso gli end point mediante un client anti-virus e anti-spyware con euristica avanzata. Questa soluzione di client imposto controlla gli accessi alla rete, limitando l'accesso Internet agli end point che non dispongono dei più recenti aggiornamenti o signature per il motore d'ispezione. Una volta attivata l'opzione sull'appliance, ogni end point viene "forzato" a scaricare il client anti-virus e anti-spyware senza alcun intervento da parte dell'amministratore, automatizzando così la distribuzione della sicurezza presso gli end point.



Gestione centralizzata delle policy

Il SonicWALL Global Management System (GMS®) fornisce una serie di strumenti potenti, flessibili e intuitivi per gestire centralmente le configurazioni E-Class NSA nelle imprese distribuite, elaborare i dati di monitoraggio centralizzato in tempo reale e integrare le policy e i report sulla conformità.



Servizi in abbonamento

Tutte le appliance di sicurezza di rete E-Class NSA (Network Security Appliance) supportano una serie in continua crescita di servizi dinamici in abbonamento e software progettati per l'integrazione immediata in qualsiasi topologia di rete.



Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service offre una protezione intelligente e in tempo reale della rete contro attacchi sofisticati a livello applicazione e basati su contenuti tra cui virus, spyware, worm, Trojan e vulnerabilità software (buffer overflow).



Il **controllo intelligente delle applicazioni** fornisce la visualizzazione in tempo reale del traffico di rete, policy personalizzabili ed il controllo ad alta granularità di applicazioni e utenti.



Content Filtering Service consente di potenziare le policy di protezione e produttività grazie all'innovativa architettura di valutazione integrata che, attraverso un database dinamico, è in grado di bloccare e impedire l'accesso ad oltre 56 categorie di contenuti ritenuti non idonei.



ViewPoint è un tool di reporting facile da utilizzare e basato sul Web che offre una panoramica immediata sulle prestazioni e la sicurezza della rete. ViewPoint permette ad aziende di qualsiasi dimensione di monitorare l'utilizzo di Internet, garantire la conformità del sistema alle normative e sorvegliare lo stato di sicurezza della rete per mezzo di report

storici creati attraverso dashboard e sommari dettagliati.



Supporto E-Class 24x7 di SonicWALL

Creato specificamente per i clienti che utilizzano appliance della serie E-Class, il supporto E-Class 24x7 fornisce funzionalità e qualità dei servizi di classe enterprise. Il supporto E-Class 24x7 include l'accesso telefonico e via Web (24 ore al giorno, 365 giorni l'anno) a un team di consulenti tecnici altamente specializzati, aggiornamenti software e firmware, sostituzione anticipata dell'hardware in caso di guasto, accesso a tool di supporto elettronici e gruppi di discussione con moderatore e molto altro ancora.



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.

Enforced Client Anti-Virus and Anti-Spyware fornisce una protezione completa contro virus e spyware tramite un semplice client, integrabile nei computer sia fissi che portatili, forzando la distribuzione automatizzata di policy anti-virus e anti-spyware, nuove definizioni e aggiornamenti software nell'intera rete.

Codici della serie E-Class NSA



SonicWALL NSA E8510
01-SSC-9770



SonicWALL NSA E8500
01-SSC-8866



SonicWALL NSA E8500 HA (High Availability)
01-SSC-8867



SonicWALL NSA E7500
01-SSC-7000

SonicWALL NSA E7500 TotalSecure* (1 anno)
01-SSC-7027



SonicWALL NSA E6500
01-SSC-7004

SonicWALL NSA E6500 TotalSecure* (1 anno)
01-SSC-7028



SonicWALL NSA E5500
01-SSC-7008

SonicWALL NSA E5500 TotalSecure* (1 anno)
01-SSC-7029

SonicWALL NSA E7500 - Servizi di sicurezza

SonicWALL GAV / IPS / Application Intelligence per NSA E7500 (1 anno)
01-SSC-6130

SonicWALL Comprehensive Gateway Security Suite per NSA E7500 (1 anno)
01-SSC-9220

Supporto 24x7 classe E di SonicWALL per NSA E7500 (1 anno)
01-SSC-7254

SonicWALL NSA E6500 - Servizi di sicurezza

SonicWALL GAV / IPS / Application Intelligence per NSA E6500 (1 anno)
01-SSC-6131

SonicWALL Comprehensive Gateway Security Suite per NSA E6500 (1 anno)
01-SSC-9221

Supporto 24x7 classe E di SonicWALL per NSA E6500 (1 anno)
01-SSC-7257

SonicWALL NSA E5500 - Servizi di sicurezza

SonicWALL GAV / IPS / Application Intelligence per NSA E5500 (1 anno)
01-SSC-6132

SonicWALL Comprehensive Gateway Security Suite per NSA E5500 (1 anno)
01-SSC-9222

Supporto 24x7 classe E di SonicWALL per NSA E5500 (1 anno)
01-SSC-7260

Sono disponibili anche abbonamenti pluriennali. Per maggiori dettagli visitare il sito www.sonicwall.com.

*Include abbonamento di 1 anno a Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention, Application Intelligence Service, Content Filtering Service, supporto E-Class 24x7 e ViewPoint Reporting.

Specifiche tecniche

	NSA E5500	NSA E6500	NSA E7500	NSA 8500	NSA 8510
Firewall					
Versione SonicOS	SonicOS Enhanced 5.6 (o superiore)				SonicOS Enhanced 5.8.1 (o superiore)
Throughput stateful¹	3,9 Gbps	5 Gbps	5,6 Gbps	8,0 Gbps	
Prestazioni GAV²	1,0 Gbps	1,69 Gbps	1,84 Gbps	2,25 Gbps	
Prestazioni IPS²	2,0 Gbps	2,3 Gbps	2,58 Gbps	3,7 Gbps	
Prestazioni Deep Packet Inspection (DPI) completo²	850 Mbps	1,59 Gbps	1,7 Gbps	2,2 Gbps	
Prestazioni IMIX²	1,1 Gbps	1,4 Gbps	1,6 Gbps	2,0 Gbps	
Connessioni (max.)³	750.000	1.000.000	1.500.000	1.500.000	
Connessioni DPI completo (max.)	500.000	600.000	1.000.000	1.250.000	
Nuove connessioni/Sec	30.000	60.000	64.000	85.000	
Nodi supportati	Illimitati				
Prevenzione attacchi Denial of Service	22 classi di attacchi DoS, DDoS e scanning				
SonicPoint supportati (max.)	96				128
VPN					
Throughput 3DES/AES⁴	1,7 Gbps	2,7 Gbps	3,0 Gbps	4,0 Gbps	
Tunnel VPN site-to-site	4.000	6.000	10.000		
Licenze Global VPN Client in bundle (max.)	2.000 (4.000)	2.000 (6.000)		2.000 (10.000)	
Licenze SSL VPN in bundle (max.)	2 (50)	2 (50)	2 (50)		
Virtual Assist in bundle (max.)	1 (25)	1 (25)	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 VPN ridondante	Sì				
Global VPN Client, piattaforme supportate	Microsoft® Windows 2000, Windows XP, Microsoft® Vista a 32 bit/64 bit, Windows 7				
Piattaforme SSL VPN supportate	Microsoft® Windows 2000 / XP / Vista 32/64 bit / Windows 7 32/64 bit, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE				
Servizi di sicurezza					
Servizio d'ispezione Deep Packet	Prevenzione intrusioni, gateway anti-virus, anti-spyware e Application Intelligence				
Content Filtering Service (CFS) Premium Edition	Scansione HTTP URL, HTTPS IP, parole chiave e contenuti, blocco controlli ActiveX, applet Java e cookie, gestione della banda per le categorie di valutazione, liste di autorizzazione/blocco personalizzabili				
Enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP e FTP, blocco degli allegati e-mail mediante client McAfee™ imposto				
Comprehensive Anti-Spam Service⁵	Supportato				
Application Intelligence and Control	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	Offre la possibilità di decifrare il traffico HTTPS in modo trasparente, scansionarlo alla ricerca di minacce con la tecnologia 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. Questa caratteristica funziona sia per i client che per i server.				
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)	400	500	512		
Routing	OSPF, RIPv1/v2, route statici, routing basato su policy, Multicast				
QoS	Priorità larghezza di banda, larghezza di banda massima / garanzia, DSCP marking, 802.1p				
Autenticazione	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, database utenti interno, servizi Terminal Server, Citrix				
IPv6	Sì				
Database interno/Single Sign-on utenti	1.500/2.500 utenti	2.500/4.000 utenti	2.500/7.000 utenti		
VoIP	Supporto completo H.323 v. 1-5, SIP e gatekeeper, gestione larghezza di banda in uscita, VoIP over WLAN, protezione Deep Inspection, interoperabilità completa con i gateway VoIP e i dispositivi di comunicazione più comuni				
Aggregazione dei link	Sì				
Ridondanza delle porte	Sì				
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 (HA)	Attiva/passiva con State Sync, DPI attiva/attiva				
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	802.11 a/b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TTLS				
Supporto accelerazione WAN	Sì				
Hardware					
Interfacce	(8) 10/100/1000 porte Gigabit in rame, 1 GbE ad alta disponibilità, 1 interfaccia console, 2 USB		(4) SFP (SX, LX o TX), (4) 10/100/1000 GbE, 1 GbE ad alta disponibilità, 2 USB, 4 interfaccia console	(2) SFP+ 10GbE, (4) 10/100/1000 GbE, 1 GbE ad alta disp. 2 USB, 1 interfaccia console	
Memoria (RAM)	1 GB	1 GB	2 GB	4 GB	
Memoria Flash	512 MB Compact Flash				
3G Wireless/modem*	Con un adattatore 3G o modem analogico supportato				
Alimentazione elettrica	Alimentatore singolo (250 W ATX)		Alimentatore doppio (250 W ATX), hot swap		
Ventilatori	Due ventilatori hot swap				
Display	Display LCD anteriore				
Tensione d'esercizio	100-240 V AC, 60-50 Hz				
Potenza max. assorbita	81 W	90 W	150 W		
Calore sviluppato	276 BTU	307 BTU	511,5 BTU		
MTBF	11,9	11,9	12,4		
Certificazioni	EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1, IPv6 Phase 2		ICSA Firewall 4.1		—
Certificazioni (in attesa)	—		EAL4+, FIPS 140-2 Level 2, VPNC, IPv6 Phase 1 e 2		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1 e 2
Fattore di forma	1U rack-mount				
Misure	43,2 x 42,5 x 4,4 cm				
Peso	6,80 kg	6,85 kg	7,9 kg		
Peso WEEE	6,80 kg	6,85 kg	7,9 kg		
Principali normative di conformità	FCC Class A, CES Class A, CE, G-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE				
Condizioni ambientali	da 5 a 40 °C				
Umidità	10-90% non condensante				

¹Metodologia 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. ²Rilevazione throughput per DPI completo/Gateway AV/Anti-Spyware/IPS tramite il test di performance Spirent WebAviArchie HTTP standard nell'industria e gli strumenti di test Ixia. Test eseguiti con flussi multipli attraverso coppie di porte multiple. ³Il numero massimo effettivo di connessioni diminuisce quando sono attivati i servizi UTM. ⁴Rilevazione throughput VPN tramite traffico UDP con pacchetti da 1280 byte, in conformità a RFC 2544. ⁵Scheda USB 3G e modem non inclusi. Per i dispositivi USB supportati vedi <http://www.sonicwall.com/us/products/cardsupport.html> ⁶Comprehensive Anti-Spam Service supporta un numero illimitato di utenti ma è consigliato per un massimo di 250 utenti. ⁷Con appliance della serie SonicWALL WXA

Certificazioni



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™