



- **Potente architettura multi-core**
- **Piattaforma di sicurezza UTM**
- **Flessibilità di distribuzione**
- **Application Firewall e controllo personalizzabile**
- **Protezione dinamica**

Protezione e performance

La serie NSA (Network Security Appliance) di classe E di SonicWALL® è la prima soluzione UTM (Unified Threat Management) del settore con processore multi-core in grado di offrire l'ispezione deep packet di classe enterprise senza rallentare le prestazioni della rete. Dotate di un potente firewall con ispezione approfondita dei pacchetti, diversi livelli di protezione e una suite di caratteristiche ad elevata disponibilità, le appliance NSA E7500, E6500 e E5500 di classe E rappresentano un'ampia gamma di soluzioni scalabili per l'implementazione in reti aziendali e universitarie, ambienti distribuiti e data center.

Le appliance NSA di classe E di SonicWALL sono concepite per garantire alta scalabilità, elevate prestazioni, affidabilità di funzionamento e la massima protezione contro le minacce nella loro classe. La serie NSA protegge la rete dai più svariati attacchi ad una velocità sorprendente grazie all'architettura di elaborazione parallela a nuclei multipli, che fornisce protezione ad altissima velocità ed elevata scalabilità. Il SonicWALL Application Firewall, un set di strumenti di protezione personalizzabile che consente un controllo accurato del traffico, offre un ulteriore livello di protezione. Tutte le appliance integrano una suite di caratteristiche ad elevata disponibilità a livello hardware e di sistema per massimizzare i tempi di funzionamento e migliorare la sicurezza.

La serie NSA è parte integrante della gamma di prodotti e servizi SonicWALL di classe enterprise per la sicurezza di rete, la protezione e-mail e l'accesso remoto sicuro. Tutte le soluzioni di classe E offrono livelli di protezione avanzata, prestazioni eccezionali e grande facilità d'uso, combinate a un ottimo rapporto qualità-prezzo. La classe E di SonicWALL fornisce la protezione ad alta performance richiesta dalle reti di classe aziendale attraverso soluzioni progettate per eliminare i costi elevati e le complessità solitamente associati alla gestione di una rete sicura.

Caratteristiche e vantaggi

Potente architettura multi-core. Le appliance NSA di classe E sono basate sulla potente architettura multi-core di SonicWALL, appositamente progettata per fornire deep packet inspection ad altissima velocità e un controllo granulare intelligente e in tempo reale del traffico di rete senza rallentare la performance della rete. La potenza e la velocità di elaborazione delle appliance NSA di classe E di SonicWALL derivano dall'uso combinato di nuclei di elaborazione di sicurezza specializzati. L'uso parallelo di diversi nuclei di elaborazione aumenta drasticamente i livelli di throughput e le prestazioni d'ispezione, riducendo al contempo il carico di lavoro degli amministratori.

Piattaforma di sicurezza UTM (Unified Threat Management). La serie NSA di classe E è una piattaforma di sicurezza e connettività ad alta ridondanza specificamente concepita per una protezione ad elevata velocità contro minacce interne ed esterne alla rete, in modo da consolidare ed estendere la funzionalità di sicurezza a tutti i livelli della rete. Le appliance NSA di classe E integrano anti-virus sul gateway, anti-spyware e prevenzione delle intrusioni in tempo reale per proteggere reti e VPN da svariati attacchi dinamici tra cui worm, Trojan, virus, malware e vulnerabilità software.

Flessibilità di distribuzione. Progettate per il funzionamento ad alta ridondanza, le appliance NSA di classe E sono la soluzione ideale per applicazioni wireless e

cablate che richiedono accesso ad alta velocità ed elevata segmentazione in gruppi di lavoro. Dotate di supporto integrato per VoIP basate su standard, reti VLAN (Virtual Local Area Network), routing di classe enterprise e funzionalità QoS (Quality of Service), le appliance NSA di classe E aumentano la flessibilità di distribuzione e migliorano la produttività.

Application Firewall e controllo personalizzabile.

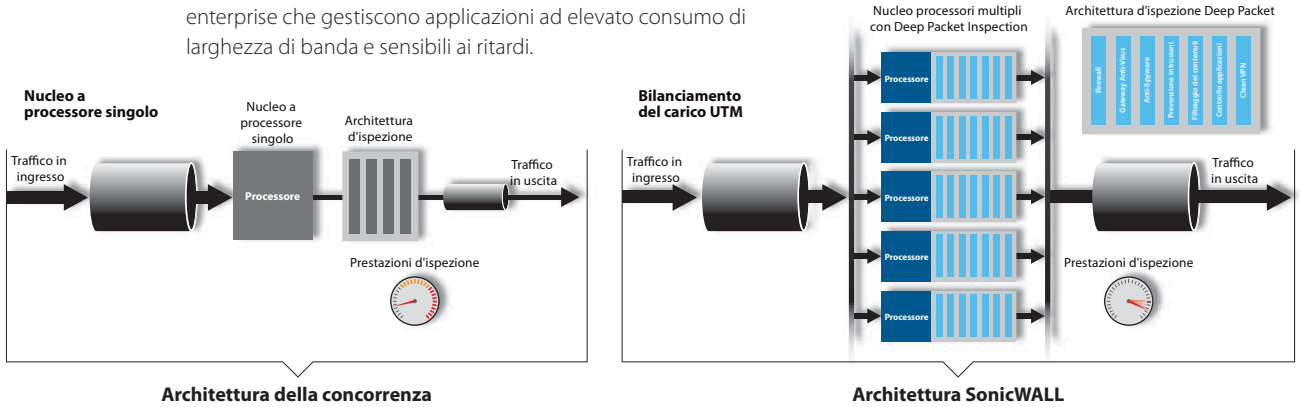
Application Firewall è una serie configurabile di policy granulari specifiche per applicazione e personalizzabili in base ad utente, applicazione, procedure pianificate o livelli di sottorete IP. Con queste policy è possibile limitare il trasferimento di file e documenti specifici, scansionare gli allegati e-mail secondo criteri configurabili dall'utente, controllare automaticamente la larghezza di banda, monitorare gli accessi Internet interni ed esterni e supportare signature personalizzate.

Protezione dinamica. I servizi di prevenzione dinamica delle minacce, filtraggio dei contenuti e controllo degli applicativi vengono costantemente aggiornati – 24 ore al giorno, 7 giorni su 7 – per ottimizzare la sicurezza e ridurre i costi di gestione. Grazie all'imposizione automatizzata delle nuove signature di protezione non è più necessario aggiornare manualmente le policy di sicurezza e gestire server o workstation tramite patch dedicate, a tutto vantaggio della produttività IT.

Architettura delle appliance NSA di classe E

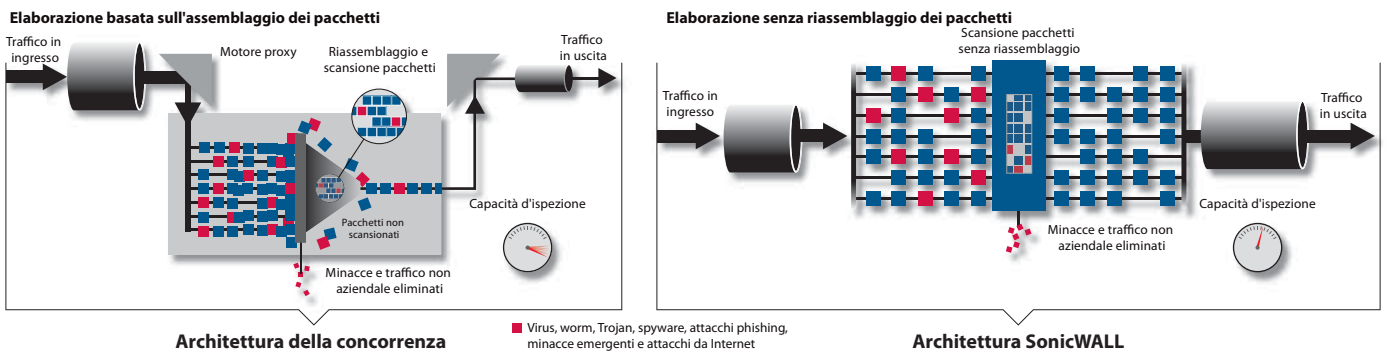
Protezione contro le minacce completa, integrata e migliore della categoria
Bilanciamento del carico UTM (Unified Threat Management)

Le soluzioni a singolo processore dotate di tecnologie di protezione multiple sono fortemente limitate dalla presenza di un unico processore centralizzato. Il bilanciamento del carico UTM di SonicWALL integra l'ispezione deep packet ad alta velocità e un motore di classificazione del traffico con più nuclei di sicurezza per ispezionare applicativi, file e traffico basato sui contenuti in tempo reale senza impatti significativi sulla performance o la scalabilità del sistema. Ciò rende possibile la scansione e il controllo delle minacce nelle reti di classe enterprise che gestiscono applicazioni ad elevato consumo di larghezza di banda e sensibili ai ritardi.

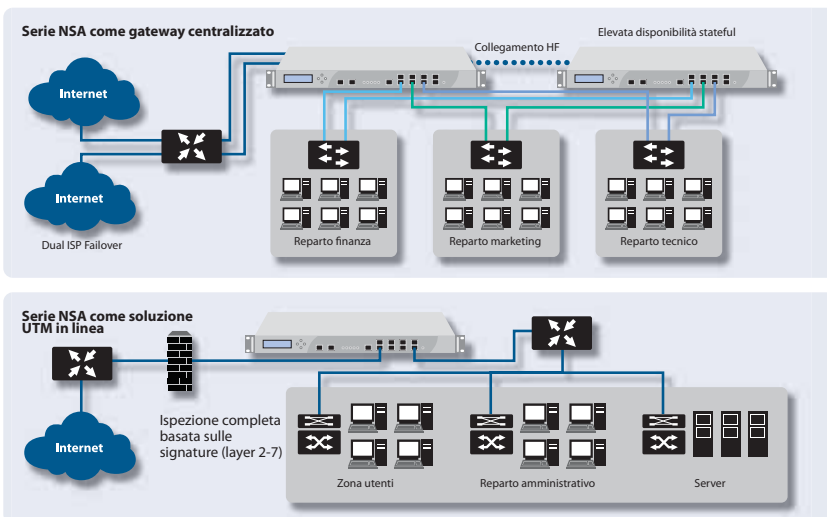


Motore di gestione unificata delle minacce

Il motore NSA UTM di classe E di SonicWALL è il primo motore d'ispezione scalabile, a livello applicazione, in grado di analizzare file e contenuti di qualsiasi dimensione in tempo reale 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 e ispezione complete senza alcuna connessione proxy. Il traffico di rete ad alta velocità viene così ispezionato con maggiore efficienza e affidabilità, migliorando sensibilmente l'esperienza degli utenti finali.



Opzioni d'implementazione flessibili e personalizzabili



Gateway centralizzato

Le appliance della serie 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 alta disponibilità stateful.

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 supplementari 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 NSA di classe E 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

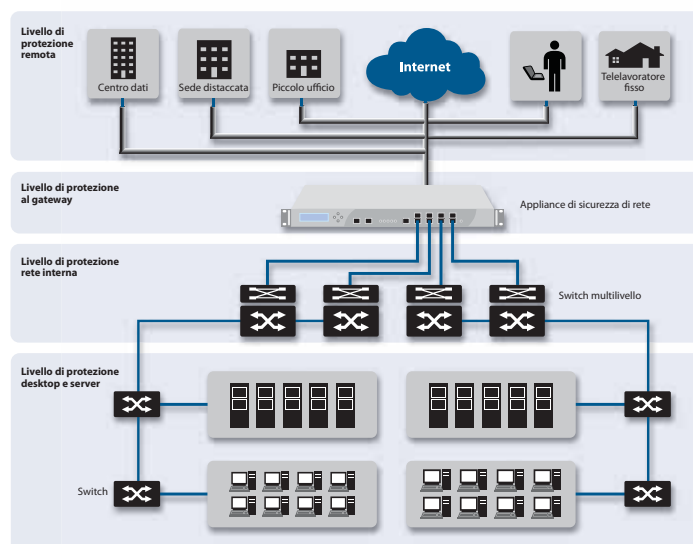
Facilmente integrabili in ambienti di rete esistenti, le appliance NSA di classe E offrono una protezione centralizzata – a livello gateway – per applicativi, file e traffico basato sui contenuti in entrata e in uscita e il monitoraggio della larghezza di banda e delle applicazioni senza compromettere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

Protezione interna

Le soluzioni della serie NSA di classe E 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 NSA di classe E 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 NSA di classe E 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 NSA di classe E 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 NSA (Network Security Appliance) di classe E supportano una serie in continua crescita di servizi dinamici in abbonamento e software progettati per l'integrazione immediata in qualsiasi topologia di rete.



La soluzione 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).



Enforced Client and Server 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.



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 55 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 24x7 per la classe E di SonicWALL
Creato specificamente per i clienti che utilizzano appliance della classe E, il supporto 24x7 per la classe E fornisce funzionalità e qualità dei servizi di classe enterprise. Il supporto 24x7 di classe E 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.

Specifiche tecniche

Codici della serie NSA di classe E



SonicWALL NSA E7500

01-SSC-7000



SonicWALL NSA E6500

01-SSC-7004



SonicWALL NSA E5500

01-SSC-7008

SonicWALL NSA E7500 - Servizi di sicurezza

SonicWALL Content Filtering Service, edizione Premium Business per NSA E7500 (1 anno)
01-SSC-7329

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

SonicWALL Comprehensive Gateway Security Suite per NSA E7500 (1 anno)
01-SSC-6120

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

SonicWALL NSA E6500 - Servizi di sicurezza

SonicWALL Content Filtering Service, edizione Premium Business per NSA E6500 (1 anno)
01-SSC-7330

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

SonicWALL Comprehensive Gateway Security Suite per NSA E6500 (1 anno)
01-SSC-6121

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

SonicWALL NSA E5500 - Servizi di sicurezza

SonicWALL Content Filtering Service, edizione Premium Business per NSA E5500 (1 anno)
01-SSC-7331

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

SonicWALL Comprehensive Gateway Security Suite per NSA E5500 (1 anno)
01-SSC-6122

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.

	NSA E5500	NSA E6500	NSA E7500
Firewall			
Versione SonicOS	SonicOS Enhanced 5.0 (o superiore)		
Throughput stateful¹	2 Gbps	3 Gbps	5,5 Gbps
Prestazioni GAV²	750 Mbps	900 Mbps	1,8 Gbps
Prestazioni IPS²	550 Mbps	850 Mbps	1,2 Gbps
Prestazioni UTM (throughput)	400 Mbps	750 Mbps	1 Gbps
Connessioni (max.)	700.000	750.000	1.000.000
Nuove connessioni/Sec	10.000	19.000	25.000
Nodi supportati	Illimitati		
Prevenzione attacchi Denial of Service	22 classi di attacchi DoS, DDoS e scanning		
VPN			
Throughput 3DES/AES¹	1,5 Gbps	2,5 Gbps	4 Gbps
Tunnel VPN site-to-site	4.000	6.000	10.000
Licenze Global VPN Client in bundle per l'accesso remoto	2.000	2.000	2.000
Crittografia / autenticazione	DES, 3DES, AES (a 128, 192, 256 bit)/MD5, SHA-1		
Scambio delle chiavi	IKE, IKEv2, connessione manuale, PKI (X.509)		
L2TP/IPSec	Sì		
Supporto certificati	Verisign, Thawte, Baltimore, RSA Keon, Entrust e Microsoft CA per VPN SonicWALL-to-SonicWALL		
Gateway VPN ridondante	Sì		
Global VPN Client, piattaforme supportate	Microsoft® Windows 2000, Windows XP, Microsoft® Vista a 32 bit		
Servizi di sicurezza con Deep Packet Inspection			
Deep Packet Inspection con servizio signature	Ampio database di signature. Controllo di applicazioni peer-to-peer e di instant messaging, aggiornamento signature tramite l'architettura di applicazione distribuita		
Content Filtering Service (CFS), edizione Premium	Scansione URL HTTP, IP HTTPs, parole chiave e contenuti, blocco controlli ActiveX, applet Java e cookie		
Client Anti-Virus and Anti-Spyware imposto sul gateway	HTTP/S, SMTP, POP3, IMAP e FTP, Enforced McAfee™ Client, blocco degli allegati e-mail		
Application Firewall	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		
Networking			
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay		
Modalità NAT	One-to-one, one-to-many, many-to-one, many-to-many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente		
Interfacce VLAN (802.1q)	256	256	512
Routing	OSPF, RIPv1/v2, route statici, routing basato su policy, Multicast		
QoS	Priorità larghezza di banda, larghezza di banda massima / garantita, DSCP marking, 802.1p		
Autenticazione	XAUTH/RADIUS, Active Directory, SSO, LDAP, database utenti interno		
Database utenti	1.500 utenti	2.500 utenti	2.500 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		
Sistema			
Gestione e monitoraggio	Web GUI (HTTP, HTTPS), linea di comando (SSH, Console), SNMP v2: Gestione globale con SonicWALL GMS		
Logging e reporting	ViewPoint®, Local Log, Syslog		
Alta disponibilità (HA)	Attiva/passiva 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		
Standard wireless	802.11 a/b/g, WEP, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS		
Hardware			
Interfacce	(8) 10/100/1000 porte Gigabit in rame, interfaccia 1 Gigabit Ethernet HA, 1 interfaccia console, 2 USB (uso futuro)	(8) 10/100/1000 porte Gigabit in rame, interfaccia 1 Gigabit Ethernet HA, 1 interfaccia console, 2 USB (uso futuro)	1 interfaccia console, 4 Gigabit Ethernet, 4 SFP (SX, LX o TX), interfaccia 1 Gigabit Ethernet HA, 2 USB (uso futuro)
Memoria (RAM)	1 GB	1 GB	2 GB
Memoria Flash	512 MB Compact Flash	512 MB Compact Flash	16 MB, 512 MB Compact Flash
Alimentazione elettrica	Alimentatore singolo (250 W ATX)	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
Certificazioni (in attesa)	ICSA IPsec VPN 1.0d, ICSA Firewall 4.1, FIPS 140-2 Level 2, EAL-4+		
Fattore di forma	1U rack-mount		
Misure	43,1 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, C-Tick, VCCI, MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE		
Condizioni ambientali	da 5 a 40 °C		
Umidità	10-90% non condensante		

¹Rilevazione throughput per firewall e VPN tramite traffico UDP in conformità a RFC 2544.

²Rilevazione throughput per Gateway AV/Anti-Spyware/IPS tramite il test di performance Spirent WebAvalanche HTTP standard nell'industria.

Italia / Supporto

Numero verde: 800.909.106

Telefono: +31 (0) 411.617.814

E-mail: sales_support-europe@sonicwall.com

Italia / Uffici

Telefono: +39.010.7407851

E-mail: italy@sonicwall.com



PROTEZIONE ALLA VELOCITÀ DEL BUSINESS™