BOUNDLESS CYBERSECURITY

2023 LINEA DI PRODOTTI

Alias

www.alias.it

SONICWALL®

Alias
www.alias.it

SONICWALL

Linee di prodotti SonicWall: in sintesi

Firewall di prossima generazione

Fascia alta: Serie NS*sp*
I firewall sono progettati per grandi imprese distribuite, data center e fornitori di servizi di sicurezza gestiti (MSSP) e si contraddistinguono per la protezione ad alta velocità, l'alta densità di porte e throughput di ispezione firewall fino a 100 Gbps.

Fascia media: Serie NS*a*
Efficacia e prestazioni di sicurezza riconosciute a livello industriale per reti di medie dimensioni, filiali e aziende distribuite.

Entry Level: Serie TZ
Prevenzione delle minacce e piattaforma SD-WAN integrate per chi lavora da casa e presso PMI e SD-Branch.

Virtuale: Serie NSv
Firewall virtuali con modelli di licenza flessibili per proteggere tutti i componenti critici delle infrastrutture cloud pubbliche e private.

Sicurezza wireless

Serie SonicWave
Sicurezza e prestazioni appositamente studiate per i dispositivi wireless di prossima generazione, gestiti nel cloud o con SonicWall Wireless Network Manager.

Serie SMA

Accesso semplice e sicuro, basato sulle politiche, alle risorse di rete e nel cloud.

Switch SonicWall

Garantisce la commutazione intelligente per la connettività sicura di prossima generazione per PMI e SD-Branch.

Serie ESA

Una soluzione di protezione multilivello contro le minacce avanzate trasmesse per posta elettronica disponibile come apparecchiatura fisica, VM o SaaS in cloud.

Capture Security appliance (CS*a*)

Verifica dei file e prevenzione dei malware effettuate internamente.

Gestione e analisi

Global Management System (GMS)
Network Security Manager
Wireless Network Manager
Controllo centralizzato, gestione dei rischi e compliance.

Capture Client

Una piattaforma client unificata con un pannello di controllo globale che mette a disposizione funzioni di protezione dell'endpoint, tra cui protezione avanzata dai malware, sandboxing, intelligence delle vulnerabilità delle applicazioni e ripristino allo stato precedente in caso di infezione.

Cloud Edge Secure Access

Una potente applicazione SaaS con semplici funzioni network-as-a-service per connettività site-to-site e cloud ibrido per AWS, Azure e Google Cloud, che abbina gli approcci alla sicurezza Zero-Trust e Least-Privilege in un'unica offerta integrata.

Cloud App Security

Una soluzione nativa per il cloud con la sicurezza di prossima generazione delle applicazioni SaaS come Office 365 e G Suite, per la protezione della posta elettronica, dei dati e delle credenziali utente contro le minacce avanzate, garantendo al tempo stesso la conformità nel cloud.

Servizi in abbonamento firewall di prossima generazione

Essential Protection Services Suite fornisce tutti i servizi di sicurezza essenziali necessari per la protezione dalle minacce note e sconosciute. La soluzione comprende Capture Advanced Threat Protection con tecnologia RTDMI, antivirus sul gateway, prevenzione delle intrusioni e controllo delle applicazioni, servizio di filtraggio dei contenuti, servizio antispam .

Advanced Protection Services Suite contiene tutti i servizi di protezione per la sicurezza avanzata della rete. Il pacchetto comprende i servizi Essential più la gestione del cloud e la reportistica basata sul cloud per 7 giorni.

Per ulteriori informazioni su sonicwall.com

Firewall sizing guide

SONICWALL	TZ APPLIANCES							NSa APPLIANCES						NSsp APPLIANCES			
	TZ 270	TZ 370	TZ 470	TZ 570	TZ 570	TZ 670	NSa 2700	NSa 3700	NSa 4700	NSa 5700	NSa 6700	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
Firmware	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOS 7	SonicOSX 7
Interfaces	1 GbE (Cu)	8	8	8	8	8	16	24	24	24	16	16	16	16	
	2.5 GbE (Cu)														
	1 GbE SFP														
	2.5 GbE SFP			2											
	2.5 GbE SFP+							4							
	5 GbE										2	2	2	2	4
	5 GbE SFP			2						2	4	4	4	4	6
	10 GbE								6	6	4	4	4		Yes
	10 GbE SFP+					2	3	6			8	8	8	8	16
	25 GbE														
	25 GbE SFP+														
	40 GbE QSFP+										2	2	2	2	4
	100 GbE QSFP28														6
Double Alimentation	No (Spare possible)	No (Spare possible)	No (Spare possible)	External as an option	External as an option	External as an option	External as an option	External as an option	External as an option	External as an option	External as an option	Yes	Yes		Yes
Add-on Storage (Stockage Logs)	Up to 256 GB optional	Up to 256 GB optional	Up to 256 GB optional	Up to 256 GB optional	32 GB expandable to 256 GB optional	32 GB expandable to 256 GB optional	64 GB expandable to 256 GB optional	128 GB expandable to 256 GB optional	128 GB expandable to 256 GB optional	128 GB expandable to 256 GB optional	256 GB expandable to 256 GB optional	1 TB SSD 512GB M2	1 TB SSD 512GB M2	1 TB SSD 512GB M2	2x 480 Go
Rackable	Optional rack kit	Optional rack kit	Optional rack kit	Optional rack kit	Optional rack kit	Optional rack kit	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Users	Recommended simultaneous users	<25	<50	<80	<150	<200	<250	<400	<600	<800	<1200	<4000	<6000	<8000	Performance distributed according to the number of instances (multi Tenants)
Performance	Firewall	2,0 Gbps	3,0 Gbps	3,5 Gbps	4,0 Gbps	5,0 Gbps	5,2 Gbps	5,5 Gbps	18,0 Gbps	28,0 Gbps	36,0 Gbps	42,0 Gbps	47 Gbps	60 Gbps	
	IPS	1,0 Gbps	1,5 Gbps	2,0 Gbps	2,5 Gbps	3,0 Gbps	3,4 Gbps	3,8 Gbps	10,0 Gbps	17,0 Gbps	20,0 Gbps	28,0 Gbps	37,0 Gbps	48 Gbps	
	Inspection Anti-Malware	750 Mbps	1,0 Gbps	1,5 Gbps	2,0 Gbps	2,5 Gbps	2,9 Gbps	3,5 Gbps	9,5 Gbps	15,0 Gbps	18,5 Gbps	27,0 Gbps	35,0 Gbps		
	SSL Inspection and Decryption (DPI SSL)	300 Mbps	500 Mbps	600 Mbps	750 Mbps	800 Mbps	800 Mbps	850 Mbps	5,0 Gbps	7,0 Gbps	9,0 Gbps	10,0 Gbps	11,5 Gbps	16,5 Gbps	
Connections TCP/IP	SSL Inspection and Decryption (DPI SSL)	25.000	30.000	35.000	50.000	75.000	125.000	150.000	350.000	350.000	750.000	1.500.000	1.750.000	1.500.000	
VPN	VPN IPSec site to site	50	100	150	200	250	2.000	3.000	4.000	6.000	6.000	6.000	12.000	12.000	
	Clients VPN IPSec	5(200)	5(200)	5(200)	10(500)	10(500)	50(1000)	50(1000)	50(3000)	2000(4000)	2000(6000)	2000(6000)	2000(6000)	2000(6000)	
	Clients VPN SSL	1(50)	2(100)	2(150)	2(200)	2(250)	2(500)	2(500)	2(1000)	2(1500)	2(1500)	2(3000)	2(3000)	2(3000)	

Estimated table. All SonicWall firewalls are NOT limited by concurrent licenses/users (excluding IPSec or SSL VPN clients).

Il existe d'autres facteurs à prendre en compte lors du dimensionnement d'un firewall en complément du nombre d'utilisateurs et du débit de la bande passante.

Alias www.alias.it SONICWALL®

Serie SonicWall TZ (Gen 7)

Piattaforma SD-Branch integrata per PMI e filiali di nuova generazione

La nuova serie TZ di SonicWall offre i primi firewall di nuova generazione (NGFW) in formato desktop con interfacce Ethernet da 10 o 5 Gigabit. La serie comprende una vasta gamma di prodotti adatti per diversi casi d'uso.

Progettati per PMI e imprese distribuite con sedi SD-Branch, i firewall della serie TZ di 7ª generazione (Gen 7) si distinguono per la comprovata efficacia della sicurezza e l'ottimo rapporto qualità-prezzo. Questi firewall NGFW rispondono alle attuali tendenze in tema di crittografia web, dispositivi connessi e mobilità ad alta velocità, fornendo una soluzione che soddisfa l'esigenza di rilevamento automatico e prevenzione delle violazioni in tempo reale.

CARATTERISTICHE PRINCIPALI

- Interfacce 10/5/2,5/1 GBE in formato desktop
- Compatibilità SD-Branch
- Funzione Secure SD-WAN
- Onboarding con la app SonicExpress
- Implementazione zero-touch
- Gestione da un unico pannello di controllo tramite cloud o firewall
- Integrazione con switch SonicWall, access point SonicWave e Capture Client
- Memoria integrata ed espandibile
- Alimentazione ridondante
- Alta densità di porte
- Failover cellulare
- SonicOS 7.0
- Supporto per TLS 1.3
- Prestazioni innovative
- Elevato numero di connessioni
- Prestazioni DPI veloci
- Basso costo totale di proprietà

La serie TZ (Gen 7) in breve. Specifiche complete »

Throughput di prevenzione minacce (max.)	Connessioni (max.)	Porte
2,5 Gb/s	1,5 milioni	8x1GbE, 2x2,5/5/10GbE

Trovate la soluzione SonicWall giusta per la vostra azienda:

sonicwall.com/TZ

> "Il TZ570 è facile da implementare, utilizzare e gestire, offre una configurazione guidata e menu chiari. Utilizzo volentieri i prodotti SonicWall e apprezzo molto il fatto che SonicWall abbia ampliato il supporto tecnico."
>
> – Gaurav Pandey, Head IT, Delhivery
>
> **Leggi il caso di studio »**

I firewall della serie TZ Gen 7 offrono un'elevata scalabilità e un alto numero di porte (fino a 10). La memoria integrata ed espandibile fino a 256 GB consente diverse funzioni tra cui registrazione di log, creazione di report, memorizzazione in cache, backup del firmware e molto altro. Un secondo alimentatore opzionale, disponibile per alcuni modelli, garantisce una maggiore ridondanza in caso di guasti.

L'installazione dei firewall TZ Gen 7 è ulteriormente semplificata dalla modalità Zero-Touch, che consente di installare contemporaneamente i firewall in più sedi con un intervento minimo del personale IT. I nuovi dispositivi, basati su hardware di nuova generazione e dotati di funzionalità firewall, switch e wireless, consentono di gestire da un unico pannello di controllo gli switch SonicWall e gli access point SonicWave. La stretta integrazione con Capture Client garantisce inoltre una protezione ottimale degli endpoint.

SonicOS e servizi di sicurezza

L'architettura SonicOS è l'elemento centrale dei firewall TZ di nuova generazione. I firewall TZ di 7ª generazione sono basati sul sistema operativo SonicOS 7.0, dotato di una nuova e moderna interfaccia utente e di numerose funzionalità avanzate di sicurezza, gestione e connettività. La serie TZ Gen 7 integra funzionalità SD-WAN, supporto TLS 1.3, visualizzazione in tempo reale, rete privata virtuale (VPN) ad alta velocità e altre potenti funzioni di sicurezza.

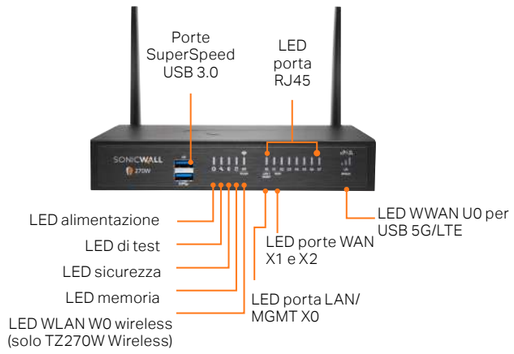
Le minacce sconosciute vengono inviate per l'analisi alla sandbox multiengine Capture Advanced Threat Protection (ATP) basata su cloud di SonicWall. Capture ATP è basato sulla nostra tecnologia Real-Time Deep Memory Inspection (RTDMI™) brevettata. Il motore RTDMI di Capture ATP rileva e blocca il malware e le minacce zero-day mediante l'analisi diretta in memoria.

L'azione combinata di Capture ATP con tecnologia RTDMI e di servizi di sicurezza come Reassembly-Free Deep Packet Inspection (RFDPI), protezione antivirus e antispyware, sistema di prevenzione delle intrusioni, controllo e gestione delle applicazioni, servizi di filtraggio dei contenuti e ispezione DPI-SSL, consente ai firewall della serie TZ di bloccare malware, ransomware e altre minacce avanzate a livello del gateway. Per ulteriori informazioni consultare il foglio dati di SonicOS e Security Services.

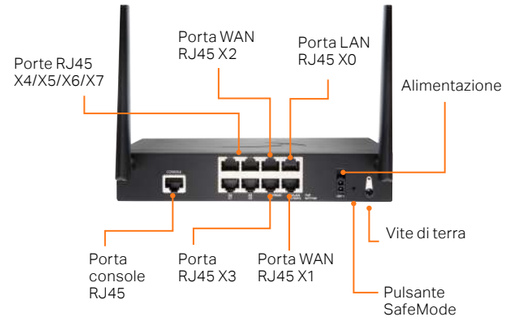
Serie SonicWall TZ270

I firewall della serie TZ270, progettati per ambienti domestici e filiali snelle, si distinguono per la comprovata efficacia della sicurezza e l'ottimo rapporto qualità-prezzo.

Pannello anteriore TZ270W



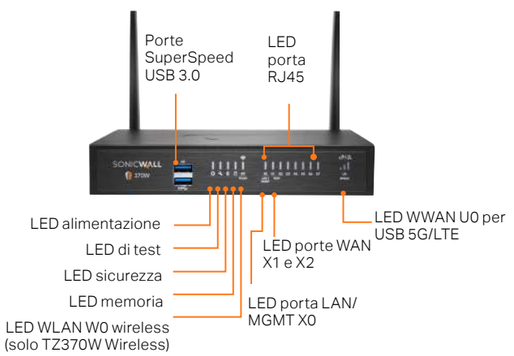
Pannello posteriore TZ270W



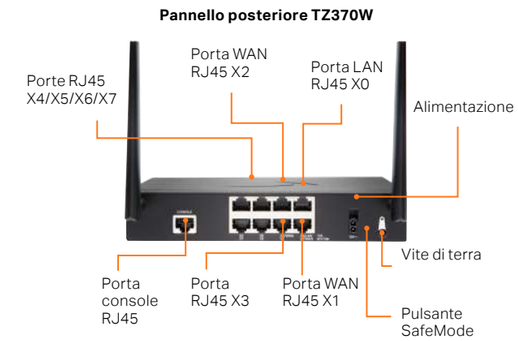
Serie SonicWall TZ370

I firewall della serie TZ370, progettati per piccole aziende e filiali snelle, si distinguono per la comprovata efficacia della sicurezza e l'ottimo rapporto qualità-prezzo.

Pannello anteriore TZ370W



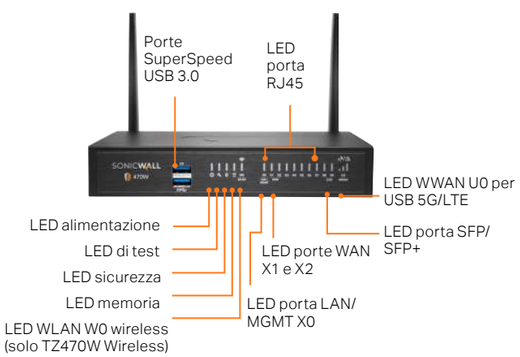
Pannello posteriore TZ370W



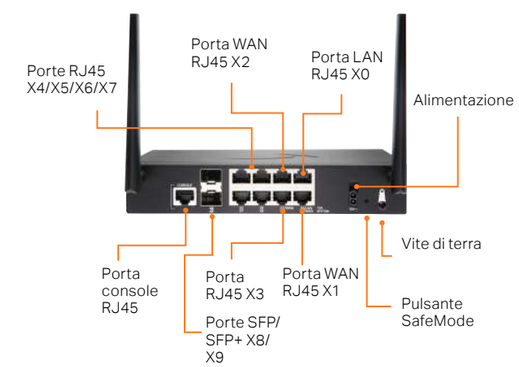
Serie SonicWall TZ470

I firewall della serie TZ470, progettati per piccole imprese e aziende distribuite con sedi SD-Branch, si distinguono per la comprovata efficacia della sicurezza e l'ottimo rapporto qualità-prezzo.

Pannello anteriore TZ470W



Pannello posteriore TZ470W



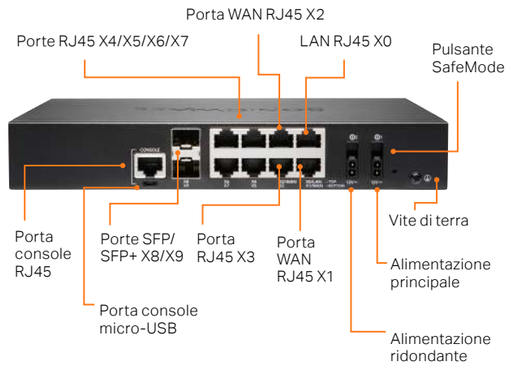
Alias www.alias.it SONICWALL®

Serie SonicWall TZ570

I firewall della serie TZ570, progettati per PMI e aziende distribuite con sedi SD-Branch, si distinguono per la comprovata efficacia della sicurezza e l'ottimo rapporto qualità-prezzo.

Pannello anteriore TZ570W

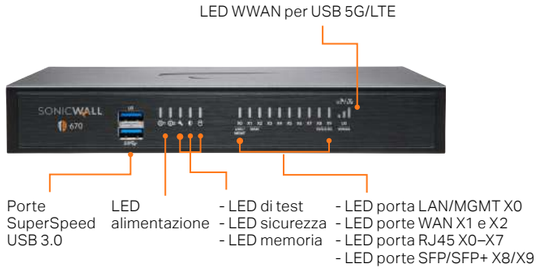
Pannello posteriore TZ570W



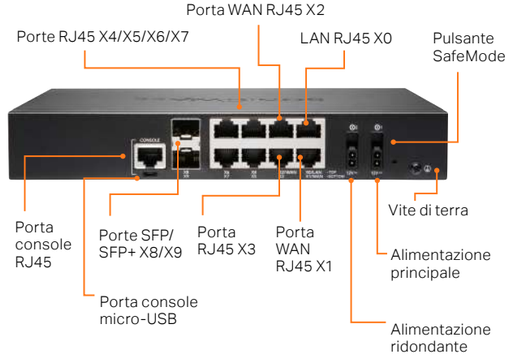
Serie SonicWall TZ670

I firewall della serie TZ670, progettati per imprese di medie dimensioni e aziende distribuite con sedi SD-Branch, si distinguono per la comprovata efficacia della sicurezza e l'ottimo rapporto qualità-prezzo.

Pannello anteriore TZ670W



Pannello posteriore TZ670W



Specifiche tecniche della serie SonicWall TZ (Gen 7)

Firewall in generale	SERIE TZ270	SERIE TZ370	SERIE TZ470	SERIE TZ570	SERIE TZ670
Sistema operativo			SonicOS 7.0		
Interfacce	8x1GbE, 2 USB 3.0, 1 Console	8x1GbE, 2 USB 3.0, 1 Console	8x1GbE, 2x2,5G SFP+, 2 USB 3.0, 1 Console	8x1GbE, 2x5G SFP+, 2 USB 3.0, 1 Console	8x1GbE, 2x10G SFP+, 2 USB 3.0, 1 Console
Supporto wireless	2x2 802.11ac Wave 2 (TZ270W)	2x2 802.11ac Wave 2 (TZ370W)	2x2 802.11ac Wave 2 (TZ470W)	2x2 802.11ac Wave 2 (TZ570W)	N/D
Supporto PoE (Power over Ethernet)	N/D	N/D	N/D	5 PoE o 3 PoE+ (TZ570P	N/D
Slot di espansione memoria (in basso)			Opzionale fino a 256 GB		Opzionale fino a 256 GB, 32 GB inclusi
Gestione			Network Security Manager, CLI, SSH, Web UI, GMS, API REST		
Alimentazione ridondante	N/D	N/D	N/D	Sì	Sì
Utenti Single Sign-On (SSO)	1.000	1.000	2.500	2.500	2.500
Interfacce VLAN	64	128	128	256	256
Access point supportati (max.)	16	16	32	32	32

Firewall/prestazioni VPN	SERIE TZ270	SERIE TZ370	SERIE TZ470	SERIE TZ570	SERIE TZ670
Throughput di ispezione firewall[1]	2 Gb/s	3 Gb/s	3,5 Gb/s	4 Gb/s	5 Gb/s
Throughput di prevenzione delle minacce[2]	750 Mb/s	1 Gb/s	1,5 Gb/s	2 Gb/s	2,5 Gb/s
Throughput di ispezione applicazioni[2]	1 Gb/s	1,5 Gb/s	2 Gb/s	2,5 Gb/s	3 Gb/s
Throughput IPS[2]	1 Gb/s	1,5 Gb/s	2 Gb/s	2,5 Gb/s	3 Gb/s
Throughput di ispezione anti-malware[2]	750 Mb/s	1 Gb/s	1,5 Gb/s	2 Gb/s	2,5 Gb/s
Throughput con decrittazione e ispezione TLS/SSL (SSL DPI)[2]	300 Mb/s	500 Mb/s	600 Mb/s	750 Mb/s	800 Mb/s
Throughput VPN IPSec[3]	750 Mb/s	1,38 Gb/s	1,5 Gb/s	1,8 Gb/s	2,1 Gb/s
Connessioni al secondo	6.000	9.000	12.000	16.000	25.000
Connessioni SPI (max.)	750.000	900.000	1.000.000	1.250.000	1.500.000
Connessioni DPI (max.)	150.000	200.000	250.000	400.000	500.000
Connessioni DPI SSL (max.)	25.000	30.000	35.000	50.000	75.000

VPN	SERIE TZ270	SERIE TZ370	SERIE TZ470	SERIE TZ570	SERIE TZ670
Tunnel VPN site-to-site	50	100	150	200	250
Client VPN IPSec (max.)	5 (200)	5 (200)	5 (200)	10 (500)	10 (500)
Licenze VPN SSL (max.)	1 (50)	2 (100)	2 (150)	2 (200)	2 (250)
Autenticazione/crittografia	DES, 3DES, AES (128, 192, 256 bit)/MD5, SHA-1, crittografia Suite B				
Key exchange	Gruppi Diffie-Hellman 1, 2, 5, 14v				
VPN basata su routing	RIP, OSPF, BGP				
Certificati supportati	Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA per VPN da SonicWall a SonicWall, SCEP				
Caratteristiche VPN	Dead Peer Detection, DHCP su VPN, attraversamento NAT con IPSec, gateway della VPN ridondante, VPN basata su routing				
Piattaforme client della VPN globale supportate	Microsoft® Windows 10				
NetExtender	Microsoft® Windows 10, Linux				
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome OS, Windows 10				

Servizi di sicurezza	SERIE TZ270	SERIE TZ370	SERIE TZ470	SERIE TZ570	SERIE TZ670
Servizi Deep Packet Inspection	Antispyware e antivirus per gateway, prevenzione delle intrusioni, SSL DPI				
Content Filtering Service (CFS)	Scansione HTTP URL, HTTPS IP, parole chiave e contenuti, filtraggio basato su tipi di file come ActiveX, Java, cookie per la privacy, elenchi di siti consentiti/vietati				
Servizio antispam completo	Sì				
Visualizzazione delle applicazioni	Sì				
Controllo delle applicazioni	Sì				
Capture Advanced Threat Protection	Sì				

Connettività di rete	SERIE TZ270	SERIE TZ370	SERIE TZ470	SERIE TZ570	SERIE TZ670
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				
Protocolli di routing	BGP, OSPF, RIPv1/v2, route statici, routing basato su policy				
Qualità del servizio (QoS)	Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1e (WMM)				
Autenticazione	LDAP (domini multipli), XAUTH/RADIUS, SSO, Novell, database utenti interno, servizi Terminal, Citrix, Common Access Card (CAC)				

Alias www.alias.it SONICWALL®

Riepilogo delle funzioni di SonicOS 7.0

Firewall

- Ispezione Stateful Packet
- Ispezione Reassembly-Free Deep Packet
- Protezione da attacchi DDoS (UDP/ICMP/SYN flood)
- Supporto IPv4/IPv6
- Autenticazione biometrica per l'accesso remoto
- Proxy DNS
- Supporto API completo
- Integrazione switch SonicWall
- Scalabilità SD-WAN
- Procedura guidata di usabilità SD-WAN[1]
- Containerizzazione SonicCoreX e SonicOS[1]
- Scalabilità connessioni (SPI, DPI, DPI SSL)

Pannello di controllo ottimizzato[1]

- Visualizzazione migliorata dei dispositivi
- Riepilogo traffico e utenti principali
- Informazioni sulle minacce
- Centro notifiche

Decrittazione e ispezione TLS/SSL/SSH

- TLS 1.3 con sicurezza migliorata[1]
- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi di host
- Controllo SSL
- Migliorie per DPI-SSL con CFS
- Controlli DPI SSL granulari in base a zone o regole

Capture Advanced Threat Protection[2]

- Real-Time Deep Memory Inspection
- Analisi multi-engine basata sul cloud
- Sandbox virtuale
- Analisi a livello hypervisor
- Emulazione di sistema completa
- Ispezione di un'ampia varietà di file
- Invio automatizzato e manuale
- Informazioni sulle minacce con aggiornamenti in tempo reale
- Blocco fino al verdetto
- Capture Client

Prevenzione delle intrusioni[2]

- Scansione basata sulle firme
- Aggiornamenti automatici delle firme
- Ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Implementazione GeoIP
- Filtraggio botnet con elenco dinamico
- Corrispondenza con espressioni regolari

Anti-malware[2]

- Scansione anti-malware basata sui flussi
- Antivirus per gateway
- Antispyware per gateway
- Ispezione bidirezionale
- Nessun limite alle dimensioni dei file
- Database dei malware nel cloud

Identificazione delle applicazioni[2]

- Controllo delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme per applicazioni personalizzate
- Prevenzione di perdite di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Ampio database di firme delle applicazioni

Visualizzazione e analisi del traffico

- Attività degli utenti
- Utilizzo di applicazioni/larghezza di banda/minacce
- Analisi basate su cloud

Filtraggio dei contenuti Web HTTP/HTTPS[2]

- Filtraggio degli URL
- Proxy avoidance
- Blocco in base a parole chiave
- Filtraggio basato su policy (esclusione/inclusione)
- Inserimento intestazione HTTP
- Categorie di classificazione CFS per la gestione della larghezza di banda
- Modello di policy unificato con controllo delle applicazioni
- Content Filtering Client

VPN

- Secure SD-WAN
- Provisioning automatico delle VPN
- VPN IPSec per connettività site-to-site
- Accesso remoto tramite VPN SSL e client IPSec
- Gateway VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN basata su routing (OSPF, RIP, BGP)

Connettività di rete

- PortShield
- Rilevamento percorsi MTU
- Registrazione avanzata
- VLAN trunking
- Mirroring delle porte (NSa 2650 e successivi)
- QoS livello 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall
- Routing basato su policy (ToS/metrico ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Alta disponibilità A/P con sincronizzazione dello stato
- Bilanciamento del carico in ingresso/in uscita
- Alta disponibilità - Attiva/Standby con sincronizzazione dello stato
- Modalità Bridge (L2), Wire/Wire virtuale, Tap, NAT
- Routing asimmetrico
- Supporto CAC (Common Access Card)

VoIP

- Controllo QoS granulare
- Gestione della larghezza di banda
- DPI per il traffico VoIP
- Supporto gatekeeper H.323 e proxy SIP

Gestione, monitoraggio e supporto

- Supporto Capture Security Appliance (CSa)
- Capture Threat Assessment (CTA) v2.0
  - Progettazione o template di nuova concezione
  - Confronti con la media di settore e globale
- Nuova UI/UX, layout intuitivo delle funzioni[1]
  - Pannello di controllo
  - Informazioni sui dispositivi, applicazioni, minacce
  - Visualizzazione della topologia
  - Definizione e gestione semplificate delle policy
- Statistiche d'uso per policy e oggetti[1]
  - Utilizzato / non utilizzato
  - Attivo / non attivo
- Ricerca globale di dati statici
- Supporto di memorizzazione[1]
- Gestione memoria interna ed esterna[1]
- Supporto scheda USB WWAN (5G/ LTE/4G/3G)
- Supporto Network Security Manager (NSM)
- GUI Web
- Interfaccia a riga di comando (CLI)
- Registrazione e provisioning zero-touch
- Reportistica semplificata CSC[1]
- Supporto app mobile SonicExpress
- SNMPv2/v3
- Gestione e reportistica centralizzate con SonicWall Global Management System (GMS)[2]
- Logging
- Esportazione verso Netflow/IPFix
- Backup della configurazione basato su cloud
- Piattaforma Security Analytics di BlueCoat
- Visualizzazione della larghezza di banda e delle applicazioni
- Gestione IPv4 e IPv6
- Schermata di gestione CD
- Gestione degli switch Dell serie N e X, compresi gli switch a cascata

Debugging e diagnostica

- Monitoraggio ottimizzato dei pacchetti
- Terminale SSH su interfaccia utente

Wireless

- Gestione access point SonicWave nel cloud
- WIDS/WIPS
- Prevenzione di access point non autorizzati
- Fast roaming (802.11k/r/v)
- Connettività di rete 802.11s mesh
- Selezione automatica dei canali
- Analisi dello spettro RF
- Vista planimetrica
- Visualizzazione della topologia
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy
- MiFi extender
- Migliorie e potenziamenti RF
- Quota ciclica ospite

Wireless integrato (solo TZ270/370/470/570W)

- Wireless 802.11ac Wave 2
- Dual-band (2,4 GHz e 5 GHz)
- Standard wireless 802.11 a/b/g/n/ac
- Rilevamento e prevenzione di intrusioni wireless
- Servizi wireless guest
- Messaggistica hotspot leggera
- Segmentazione degli access point virtuali
- Captive portal
- ACL cloud

[1] Nuova funzione, disponibile su SonicOS 7.0
[2] Richiede un abbonamento aggiuntivo

Maggiori informazioni sulla serie SonicWall TZ Gen 7:

www.sonicwall.com/TZ

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative che si adattano perfettamente alla nuova "normalità iperdistribuita", in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibile economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Datasheet-TZSeries-Gen7-A4-JK-6016

Serie SonicWall NS*a* Gen 7

La serie di firewall SonicWall Network Security Appliance (NS*a*) di 7ª generazione (Gen 7) offre a medie e grandi aziende prestazioni leader del settore con il costo totale di proprietà più basso della categoria.

Grazie a funzionalità di sicurezza complete come prevenzione delle intrusioni, VPN, controllo delle applicazioni, analisi del malware, filtraggio degli URL, sicurezza DNS e servizi Geo-IP e Bot-net, protegge il perimetro di rete da minacce avanzate senza creare colli di bottiglia.

CARATTERISTICHE PRINCIPALI

- Fattore di forma 1 RU
- Supporto per porte da 40G/25G/10G/5G/2,5G/1G
- Analisi minacce e malware a velocità multi-gigabit
- Prestazioni TLS superiori (sessioni e throughput)
- Memoria espandibile
- Predisposizione per Internet edge aziendale
- Nuovo SonicOS di 7ª generazione
- Funzionalità SD-WAN sicura
- Pannello di gestione intuitivo
- Supporto per TLS 1.3
- Eccellente rapporto prezzo/prestazioni
- Prestazioni DPI veloci
- Basso TCO
- Alta densità di porte per una semplice connettività di rete
- Integrazione con SonicWall Switch, SonicWave Access Point e Capture Client
- Alimentazione ridondante

La serie NS*a* Gen 7 in breve. Specifiche complete »

Fino a 19 Gb/s	Fino a 8 milioni	40G/25G/10G/5G/2,5G/1G
Throughput di prevenzione delle minacce	Connessioni	Porte

Trovate la soluzione SonicWall giusta per la vostra azienda:

sonicwall.com/products

La soluzione offre un'elevata densità di porte, tra cui diverse porte 40 GbE e 10 GbE, e supporta la ridondanza di rete e hardware con elevata disponibilità e doppia alimentazione.

La serie di firewall SonicWall Network Security Appliance (NS*a*) di 7ª generazione (Gen 7) offre a medie e grandi aziende prestazioni leader del settore con il costo totale di proprietà più basso della categoria.

Grazie a funzionalità di sicurezza complete come prevenzione delle intrusioni, VPN, controllo delle applicazioni, analisi del malware, filtraggio degli URL, sicurezza DNS e servizi Geo-IP e Bot-net, protegge il perimetro di rete da minacce avanzate senza creare colli di bottiglia.

La serie NS*a* Gen 7 è stata riprogettata con i componenti hardware più recenti, sviluppati per garantire una prevenzione delle minacce a velocità multi-gigabit, anche per il traffico crittografato. La soluzione offre un'elevata densità di porte, tra cui diverse porte 40 GbE e 10 GbE, e supporta la ridondanza di rete e hardware con elevata disponibilità e doppia alimentazione.

SonicOS 7.0 e servizi di sicurezza di 7ª generazione

La serie NS*a* Gen 7 utilizza SonicOS 7.0, un nuovo sistema operativo appositamente realizzato per fornire una moderna interfaccia utente, flussi di lavoro intuitivi e un approccio che mette l'utente in primo piano. SonicOS 7.0 offre diverse funzionalità concepite per facilitare i flussi di lavoro aziendali. Offre un semplice sistema di configurazione delle policy, installazione zero-touch e gestione flessibile per consentire alle aziende di migliorare la sicurezza e l'efficienza operativa.

La serie NS*a* di 7ª generazione supporta funzionalità di rete avanzate quali SD-WAN, routing dinamico, alta disponibilità ai livelli 4-7 e funzioni VPN ad alta velocità. Oltre a integrare funzionalità firewall e switch, l'appliance offre un unico pannello di controllo per gestire sia gli switch che i punti di accesso.

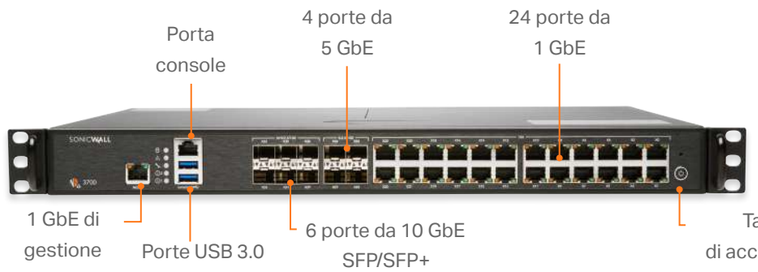
Creata per mitigare gli attacchi informatici avanzati attuali e futuri, la serie NS*a* Gen 7 offre l'accesso ai servizi di sicurezza firewall avanzati di SonicWall, che permettono di proteggere l'intera infrastruttura IT. Soluzioni e servizi come Cloud Application Security, sandbox Capture Advanced Threat Protection (ATP) basata sul cloud, ispezione Real-Time Deep Memory Inspection (RTDMI™) e Reassembly-Free Deep Packet Inspection (RFDPI) per ogni tipo di traffico, TLS 1.3 incluso, offrono la protezione completa dei gateway contro malware nascosti e pericolosi, comprese le minacce zero-day e crittografate.

Alias www.alias.it SONICWALL®

Serie SonicWall NS*a* Gen 7

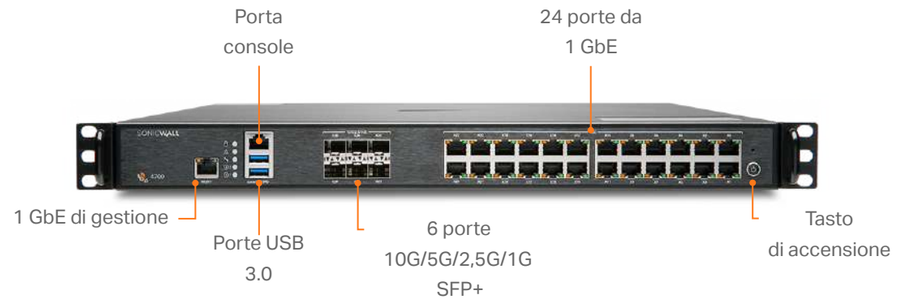
NS*a* 2700

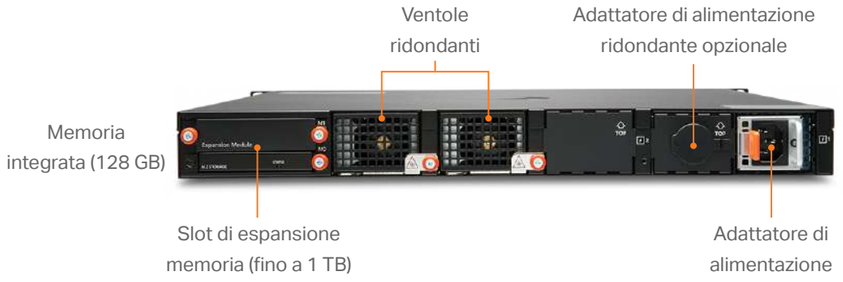
NS*a* 3700



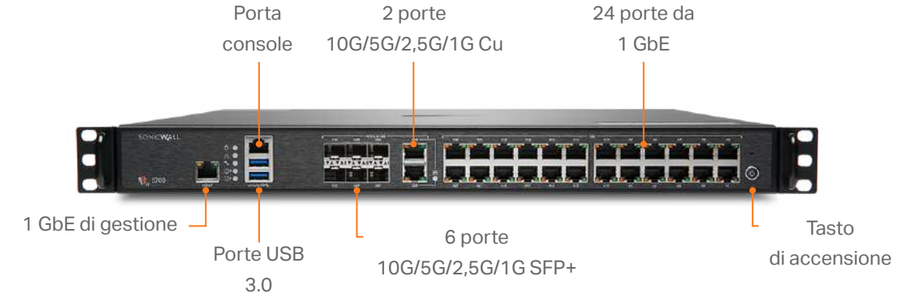
Serie SonicWall NS*a* Gen 7 (continua)

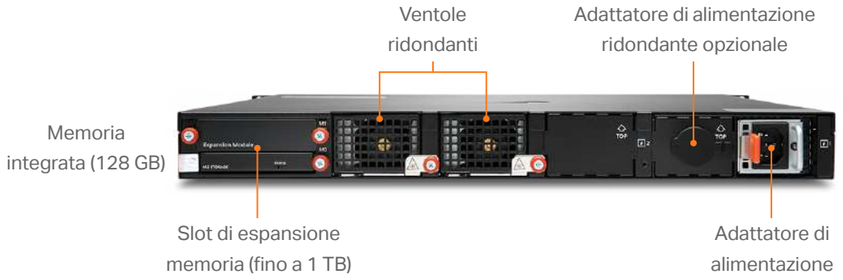
NS*a* 4700





NS*a* 5700

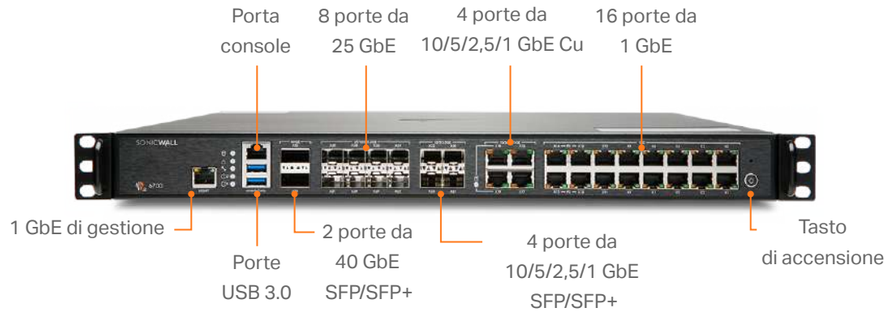


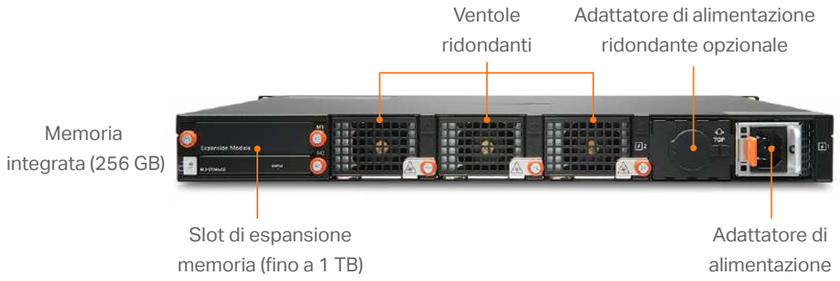


Alias www.alias.it SONICWALL®

Serie SonicWall NS*a* Gen 7 (continua)

NS*a* 6700





SERVIZI OFFERTI DAI PARTNER

Serve aiuto per pianificare, ottimizzare o installare una soluzione SonicWall? I SonicWall Advanced Services Partners hanno seguito corsi di formazione per fornire servizi professionali di livello mondiale. Per maggiori informazioni:

www.sonicwall.com/PES

Alias www.alias.it

SONICWALL®

Specifiche di sistema della serie NS*a* Gen 7

Firewall	NS*a* 2700	NS*a* 3700	NS*a* 4700	NS*a* 5700	NS*a* 6700
Sistema operativo			SonicOS 7		
Interfacce	16x1GbE, 3x10G SFP+, 2 USB 3.0, 1 console, 1 porta di gestione	24x1GbE, 6x10G SFP+, 4x5G SFP+, 2 USB 3.0, 1 console, 1 porta di gestione	6 x 10G/5G/2,5G/1G (SFP+); 24 x 1GbE Cu 2 USB 3.0, 1 console, 1 porta di gestione	6 x 10G/5G/2,5G/ 1G (SFP+); 2x 10G/5G/2,5G/ 1G (Cu); 24 x 1GbE Cu 2 USB 3.0, 1 console, 1 porta di gestione	2x40G; 8x25G, 4 x10G/5G/2,5/ 1G SFP+, 4 x 10G/5G/2,5G/ 1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 console, 1 porta di gestione
Archiviazione	64 GB M.2	128 GB M.2	128 GB	128 GB	256 GB M.2
Espansione	Slot di espansione memoria (fino a 256 GB)	Slot di espansione memoria (fino a 256 GB)	Slot di espansione memoria (fino a 1 TB)	Slot di espansione memoria (fino a 1 TB)	Slot di espansione memoria (fino a 1 TB)
Interfacce VLAN	256	256	512	512	512
Punti di accesso supportati (max.)	32	32	512	512	512
Firewall/prestazioni VPN					
Throughput di ispezione firewall[1]	5,2 Gb/s	5,5 Gb/s	18 Gb/s	28 Gb/s	36 Gb/s
Throughput di prevenzione delle minacce[2]	3,0 Gb/s	3,5 Gb/s	9,5 Gb/s	15 Gb/s	19 Gb/s
Throughput di ispezione applicazioni[2]	3,6 Gb/s	4,2 Gb/s	11 Gb/s	18 Gb/s	20 Gb/s
Throughput IPS[2]	3,4 Gb/s	3,8 Gb/s	10 Gb/s	17 Gb/s	20 Gb/s
Throughput di ispezione anti-malware[2]	2,9 Gb/s	3,5 Gb/s	9,5 Gb/s	16 Gb/s	18,5 Gb/s
Throughput con decrittazione e ispezione TLS/SSL (SSL DPI)[2]	800 Mb/s	850 Mb/s	5 Gb/s	7 Gb/s	9 Gb/s
Throughput VPN IPSec[3]	2,10 Gb/s	2,2 Gb/s	11 Gb/s	15 Gb/s	19 Gb/s
Connessioni al secondo	21.500	22.500	115.000	228.000	228.000
Connessioni max. (SPI)	1.500.000	2.000.000	4.000.000	5.000.000	8.000.000
Connessioni max DPI-SSL	125.000	150.000	350.000	350.000	750.000
Connessioni max. (DPI)	500.000	750.000	2.000.000	3.500.000	6.000.000
VPN					
Tunnel VPN site-to-site	2.000	3.000	4.000	6.000	6.000
Client VPN IPSec (max)	50 (1.000)	50 (1.000)	500 (3000)	2000 (4000)	2000 (6000)
Licenze VPN SSL (max)	2 (500)	2 (500)	2 (1.000)	2 (1.500)	2 (1.500)
Crittografia/autenticazione	DES, 3DES, AES (128, 192, 256 bit)/MD5, SHA-1, crittografia Suite B				
Key exchange	Gruppi Diffie-Hellman 1, 2, 5, 14v				
VPN basata su routing	RIP, OSPF, BGP				
Certificati supportati	Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA per VPN da SonicWall a SonicWall, SCEP				
Caratteristiche VPN	Dead Peer Detection, DHCP su VPN, attraversamento NAT con IPSec, gateway della VPN ridondante, VPN basata su routing				
Piattaforme del client della VPN globale supportate	Windows 10		Microsoft® Windows Vista a 32/64 bit, Windows 7 a 32/64 bit, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Windows 10		
NetExtender	Windows 10 e Linux		Microsoft Windows Vista a 32/64 bit, Windows 7, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Mac OS X 10.4 e versioni successive, Linux FC3 e versioni successive/Ubuntu 7 e versioni successive/OpenSUSE		
Mobile Connect	Apple iOS, Mac OS X, Android, Kindle Fire, Chrome OS, Windows 10		Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (incorporato)		
Servizi di sicurezza					
Servizi Deep Packet Inspection	Antispyware e antivirus per gateway, prevenzione delle intrusioni, SSL DPI				

Alias www.alias.it

SONICWALL®

NSv 270/470/870

The SonicWall Network Security virtual NSv 270/470/870 firewalls, deliver enterprise-class security, streamlined management, complete visibility, flexible deployment, while delivering superior performance for virtual workloads.

Vulnerabilities within virtual environments are discovered regularly that yield serious security implications and challenges. But protecting all these security vectors requires the ability to also consistently apply the right security policy to the right network control point, as some security failures can be attributed to ineffective policies or misconfigurations.

HIGHLIGHTS

Public and private cloud security

- Next-gen firewall with automated real-time breach detection and prevention capabilities
- Patent-pending Real-Time Deep Memory Inspection (RTDMI) technology
- Patented Reassembly-Free Deep Packet Inspection (RFDPI) technology
- Complete end-to-end visibility and streamlined management with Unified Policy
- Application intelligence and control
- Segmentation security and security zoning
- Support across private cloud (ESXi, Hyper-V, KVM, Nutanix) and public cloud (AWS, Azure) platforms

Virtual machine protection

- Data confidentiality
- Secure communication with data leakage prevention
- Traffic validation, inspection and monitoring
- Virtual network resilience and availability
- SonicOSX 7.0

Find the right SonicWall solution for your enterprise:

sonicwall.com/NSv

NSv firewall series help security teams reduce these types of security risks and vulnerabilities, which can cause serious disruption to business-critical services and operations. It enables enterprises to control dynamic traffic passing through a firewall and provides visibility and insight into disparate policies. It help simplify management tasks, reduce configuration errors and speed up deployment time, all of which contribute to a better overall security posture.

SonicOSX and Security Services

The SonicOSX architecture is at the core of NSv 240/470/870 firewalls. It is powered by the feature rich SonicOSX 7.0 operating system with new modern looking UX/UI, advanced security, networking and management capabilities.

Built from the ground up, SonicOSX 7.0 features Unified Policy that offers integrated management of various security policies. Easily provision layer 3 to layer 7 controls in a single rule base on every firewall, providing a centralized location for configuring policies. The new web interface presents meaningful visualizations of threat information, and displays actionable alerts prompting you to configure contextual security policies with point-and-click simplicity.

NSv further integrates SD-WAN, TLS 1.3 support, real-time visualization, high-speed virtual private networking (VPN) and other robust security features. Unknown threats are sent to SonicWall's cloud-based Capture Advanced Threat Protection (ATP) multiengine sandbox for analysis. Enhancing Capture ATP is our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. As one of Capture ATP's engine, RTDMI detects and blocks malware and zero-day threats by inspecting directly in memory.

By leveraging Capture ATP with RTDMI technology, in addition to security advanced services, NSv series firewalls stop malware, ransomware and other advanced threats at the gateway.

Deployments

1. Cloud Edge and Data Center Secure Public Clouds

- Secure workloads on Amazon Web Services (AWS) and Microsoft Azure
- Protect cloud applications and cloud infrastructures from cyber threats with advanced next-generation firewall features that incorporates VPN, IPS, CFS, AV and much more
- Decrypt encrypted traffic easily and utilize TLS 1.3 support for improved security
- Ensure compliance with regulatory standards by implementing threat prevention and segmentation capabilities
- Appropriately scale and right-size your infrastructure
- Gain complete visibility and control of traffic across multiple regions and availability zones with Unified Policy
- Attain cost benefit and efficiency by shifting from CAPEX to OPEX
- Secure Private Clouds
- Secure virtualized compute resources and hypervisors to protect private cloud workloads on VMware ESXi, Microsoft Hyper-V, Nutanix and KVM
- Prevent threats with complete visibility into intra-host communication between virtual machines
- Ensure appropriate application of security policies throughout the virtual environment
- Deliver safe application enablement rules by application, user and device, regardless of VM location
- Implement proper security zoning and isolations
- Gain complete visibility and streamlined provisioning of traffic across multiple locations and availability zones with Unified Policy
- Decrypt encrypted traffic easily and utilize TLS 1.3 support for improved security

2. Internet Edge

- Protect corporate resources from attacks at the Internet gateway.
- Secure Internet edge from the most advanced attacks with advanced security features and automatically block threats
- Ensure compliance with regulatory standards by implementing threat prevention and segmentation capabilities
- Improve business efficiency, performance and reduce costs by leveraging SonicOSX enhancements
- Segment critical PoS (Point of Sale) systems, to ensure business continuity
- Gain complete visibility and control of traffic across multiple regions and availability zones with Unified Policy

Alias www.alias.it SONICWALL®

NS*v* Series System Specifications

Firewall General	NS*v* 270	NS*v* 470	NS*v* 870
Operating system	SonicOSX[12]		
Supported Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7, Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[11]		
Supported Public Cloud Platforms (Instance Type)[1]	AWS (c5.large), Azure (Std D2 v2)	AWS (c5.xlarge), Azure (Std D3 v2)	AWS (c5.2xlarge), Azure (Std D4 v2)
Licensing	BYOL, PAYG[2]		
Max Supported vCPUs	2	4	8
Interface Count (ESXi/Hyper-V/KVM/Nutanix/AWS/Azure)	8/8/8/8/2/2	8/8/8/8/4/4	8/8/8/8/8/8
Max Mgmt/DataPlane Cores	1/1	1/3	1/7
Min Memory[3]	6 GB	8 GB	10 GB
Max Memory[4]	6 GB	10 GB	14 GB
Supported IP/Nodes	Unlimited		
Minimum Storage	60 GB		
SSO users	500	10,000	15,000
Logging	Analyzer, Local Log, Syslog		
High availability	Active/Passive[5]		
Firewall/VPN Performance[6,8]	**NS*v* 270**	**NS*v* 470**	**NS*v* 870**
Firewall Inspection Throughput	6 Gbps	9 Gbps	14 Gbps
Threat Prevention Throughput	1.6 Gbps	2.9 Gbps	8 Gbps
IPS Throughput	4 Gbps	6 Gbps	8 Gbps
TLS/SSL DPI Throughput	800 Mbps	2 Gbps	4 Gbps
VPN Throughput[9]	1.4 Gbps	3.5 Gbps	8 Gbps
Connections per second	13,760	37,270	75,640
Maximum connections (SPI)	225,000	1.5M	3M
Maximum connections (DPI)	125,000	1.5M	2M
TLS/SSL DPI Connections	8,000	20,000	30,000
VPN	**NS*v* 270**	**NS*v* 470**	**NS*v* 870**
Site-to-Site VPN Tunnels	75	6000	10,000
IPSec VPN clients (Maximum)	50(1000)	2000(4000)	2000(6000)
SSL VPN Clients Included[7]	2	2	2
SSL VPN Clients Maximum[7]	100	200	300
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)		
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v		
Route-based VPN	RIP, OSPF, BGP		
Networking	**NS*v* 270**	**NS*v* 470**	**NS*v* 870**
IP address assignment	Static, DHCP, internal DHCP server[10], DHCP relay[10]		
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT		
Max VLAN[8]	128	128	128
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing		
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p		
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix		

[1]Pending availability.
[2]PAYG is currently available only on AWS.
[3]Memory with Jumbo frame disabled.
[4]Memory with Jumbo frame enabled. Additional memory is required for Jumbo frames. Jumbo frames are not supported on Azure and AWS.
[5]High availability is available on VMware ESXi platform, KVM, Azure, Microsoft Hyper-V and Nutanix. HA is not supported on AWS.
[6]Published performance numbers are up to the specification and the actual performance may vary depending on underlying hardware, network conditions; firewall configuration and activated services. Performance and capacities may also vary based on underlying virtualization infrastructure, and we recommend additional testing within your environment to ensure your performance and capacity requirements are met. Performance metrics were observed using Intel Xeon W Processor (W-2195 2.3GHz, 4.3GHz Turbo, 24.75M Cache) running SonicOSv 6.5.0.2 with VMware vSphere 6.5.
[7]Increased SSL VPN number will be available only from SonicOS 6.5.4.4-44v-21-723 firmware and onwards.
[8]VLAN interfaces are not supported on Azure and AWS. Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Threat Prevention/GatewayAV/ Anti-Spyware/IPS throughput measured using industry standard Keysight HTTP performance test tools. Testing done with multiple flows through multiple port pairs. Threat Prevention throughput measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled with default firewall settings. VPN throughput measured with UDP traffic using 1418 byte packet size AESGMAC16-256 Encryption adhering to RFC 2544. All specifications, features and availability are subject to change.
[9]All performance parameters are tested using Dell R740 with SR-IOV and Turbo boost.
[10]Supported on Private Cloud and not on Public Cloud Platforms.
[11]Nutanix AHV is supported on SonicWall NSv 270/470/870 running SonicOSX 7.0.0 firmware and onwards.
[12]SonicOSX 7.0.1 onwards user will be able to select and switch between Classic/Global and Policy mode.

Alias www.alias.it

SONICWALL®

Serie SonicWall NS*sp* Gen 7

La serie SonicWall Network Security services platform™ (NS*sp*) offre firewall di nuova generazione con elevata densità di porte e interfacce a velocità multi-gigabit, in grado di gestire milioni di connessioni alla ricerca di minacce zero-day e avanzate. Progettati per grandi aziende, istituti di istruzione superiore, enti pubblici e MSSP, eliminano gli attacchi in tempo reale senza rallentare le prestazioni. I firewall sono progettati per garantire un'elevata affidabilità, fornendo servizi ininterrotti alle aziende.

NS*sp* in breve Specifiche complete »

100 GbE	Fino a 100 Gbps	80 mln.
Porte	Throughput ispezione firewall	Connessioni max. (NS*sp* 15700)

CARATTERISTICHE PRINCIPALI

Serie SonicWall NS*sp*

- Alta densità di porte
- Porte da 100 GbE
- Integrazione con sandbox on-premise e in cloud
- Gestione da un unico pannello
- Throughput di prevenzione minacce oltre 80 Gb/s
- Alimentazione ridondante
- Throughput di ispezione firewall fino a 100 Gb/s
- Supporto per TLS 1.3
- Supporto di milioni di connessioni TLS simultanee
- Basso costo totale di proprietà

Maggiori informazioni sulla serie SonicWall NS*sp* Gen 7:

sonicwall.com/NS*sp*

Alias www.alias.it

SONICWALL®

Firewall di classe enterprise

Man mano che le aziende evolvono, aumentano anche i dispositivi gestiti e non gestiti, le reti, i carichi di lavoro nel cloud, le applicazioni SaaS, gli utenti, la velocità di Internet e le connessioni crittografate. Un firewall che non è in grado di supportare tutte queste utenze diventa un collo di bottiglia. Un firewall deve essere un punto di forza, non un punto debole.

Le interfacce multiple a 100G/40G/25G/10G del firewall SonicWall NS*sp* consentono di gestire milioni di connessioni simultanee, crittografate e non crittografate, con una tecnologia di prevenzione delle minacce senza precedenti. Considerando che il 70% delle sessioni sono crittografate, per garantire la produttività e la sicurezza delle informazioni è fondamentale disporre di un firewall in grado di elaborare ed esaminare questo traffico senza compromettere l'esperienza d'uso.

Le policy unificate di NS*sp* permettono alle aziende di creare policy di accesso e sicurezza da un'unica interfaccia in modo semplice e intuitivo.

Gestione e reportistica semplificate

La gestione, il monitoraggio e il reporting continuo delle attività di rete sono gestiti tramite il Network Security Manager di SonicWall, che offre un pannello di controllo intuitivo per gestire le operazioni dei firewall e fornire report storici, il tutto da un'unica fonte. Le procedure semplificate di installazione e configurazione e la facilità di gestione consentono alle aziende di ridurre il costo totale di proprietà e ottenere un elevato ritorno sull'investimento.

Implementazione

Next-Generation Firewall (NGFW)

- Gestione da un unico pannello di controllo
- NS*sp* si integra con il resto dell'ecosistema di soluzioni SonicWall
- Piena visibilità sulla rete per monitorare il comportamento di applicazioni, dispositivi e utenti, in modo da applicare policy ed eliminare le minacce e i colli di bottiglia della larghezza di banda
- Integrazione con Capture ATP con RTDMI per le sandbox basate su cloud o con Capture Security Appliance per il rilevamento di malware on-premise

Ispezione Deep Packet del traffico SSL/TLS (DPI-SSL) per rilevare minacce nascoste

- I firewall NS*sp* consentono di ispezionare milioni di connessioni TLS/SSL ed SSH crittografate simultanee, indipendentemente dalla porta o dal protocollo
- Le regole di inclusione ed esclusione consentono di personalizzare i controlli in base a requisiti di conformità specifici dell'azienda e/o legali
- Supporto di suite di cifratura fino a TLS 1.3

Segmentazione e connettività di rete

- Funzionamento su diverse reti segmentate, ambienti cloud o servizi definiti con modelli, policy e gruppi di dispositivi univoci per diversi dispositivi e tenant
- Gli MSSP possono anche supportare più clienti con un servizio clean pipe e policy univoche

Firewall multi-istanza (solo per NS*sp* 15700)

- La multi-istanza è la nuova generazione della multi-tenancy
- Ogni tenant è isolato con risorse di calcolo dedicate per evitare l'esaurimento delle risorse
- Dispone di porte e tenant fisici e logici
- Supporta la gestione di policy e configurazioni indipendenti per i tenant
- Sfrutta l'indipendenza dalle versioni e il supporto ad alta disponibilità (HA) per i tenant

Funzioni in modalità Wire

- Modalità Bypass per integrare i firewall hardware in una rete rapidamente e quasi senza interruzioni
- Modalità Inspect per estendere la modalità Bypass senza modificare la funzionalità del percorso dei pacchetti a basso rischio e zero latenza
- Modalità Secure per interporre attivamente i processori multi-core del firewall nel percorso di elaborazione dei pacchetti
- Modalità Tap per acquisire un flusso di pacchetti in mirroring attraverso un'unica porta switch sul firewall, eliminando la necessità di un inserimento fisico intermedio

Protezione contro le minacce avanzate

- SonicWall Capture Advanced Threat Protection™ (ATP), utilizzato da oltre 150.000 clienti nel mondo in diverse soluzioni, permette di scoprire e bloccare più di 1.200 nuove forme di malware ogni giorno lavorativo
- NS*sp* si integra con Capture Security appliance per rilevare e bloccare minacce sconosciute tramite una sandbox on-premise che usa la tecnologia Real-Time Deep Memory Inspection™ (RTDMI).

Piattaforma Capture Cloud

- La piattaforma Capture Cloud di SonicWall offre la prevenzione delle minacce basata sul cloud e la gestione della rete, oltre a funzionalità di reporting e analisi, per organizzazioni di qualsiasi dimensione.

Servizi di filtraggio dei contenuti

- Verifica dei siti web richiesti a fronte di un imponente database nel cloud che contiene milioni di URL, indirizzi IP e siti web classificati.
- Creazione e applicazione di policy che autorizzano o negano l'accesso ai siti in base all'identità individuale o di gruppo, o all'ora del giorno, per oltre 50 categorie predefinite

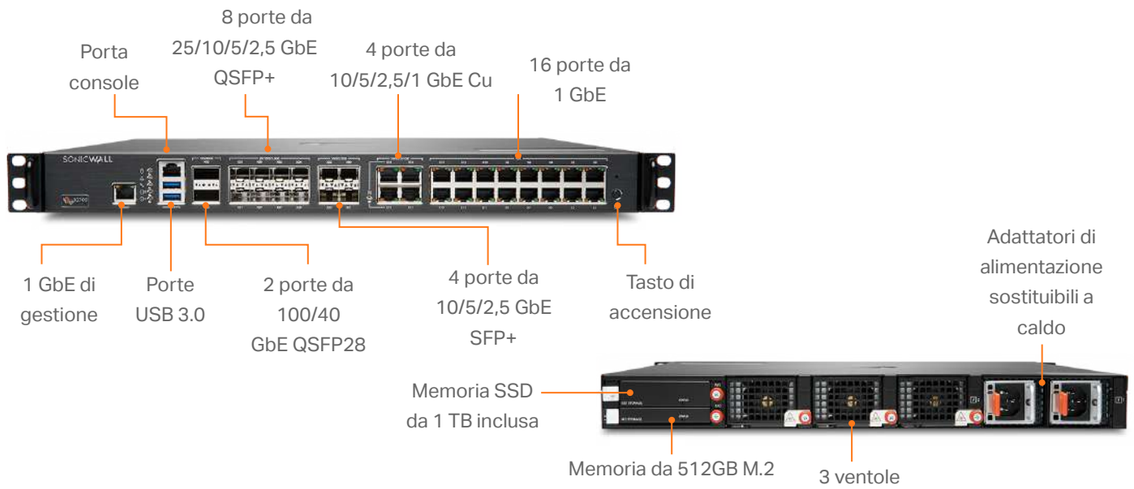
Sistema di prevenzione delle intrusioni (IPS)

- Offre un motore di ispezione approfondita dei pacchetti configurabile e ad alte prestazioni per la protezione estesa dei principali servizi di rete, come navigazione Web, posta elettronica, trasferimento di file, servizi Windows e DNS
- Progettato per fornire protezione dalle vulnerabilità delle applicazioni e da worm, trojan, exploit peer-to-peer, spyware e backdoor exploit
- Il linguaggio estensibile delle firme consente una difesa proattiva nei confronti delle vulnerabilità scoperte di recente in applicazioni e protocolli.
- SonicWall IPS elimina i lunghi e costosi interventi di manutenzione e aggiornamento delle firme per i nuovi attacchi grazie all'architettura leader del settore Distributed Enforcement Architecture (DEA) di SonicWall

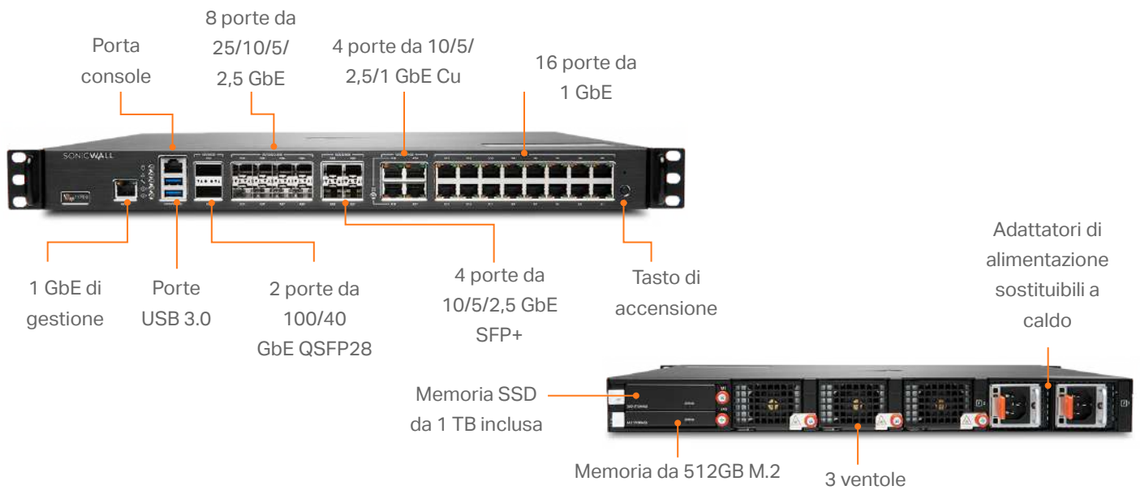
IoT e controllo delle applicazioni

- NS*sp* cataloga migliaia di applicazioni tramite il controllo delle applicazioni e monitora il loro traffico per rilevare comportamenti anomali

NS*sp* 10700

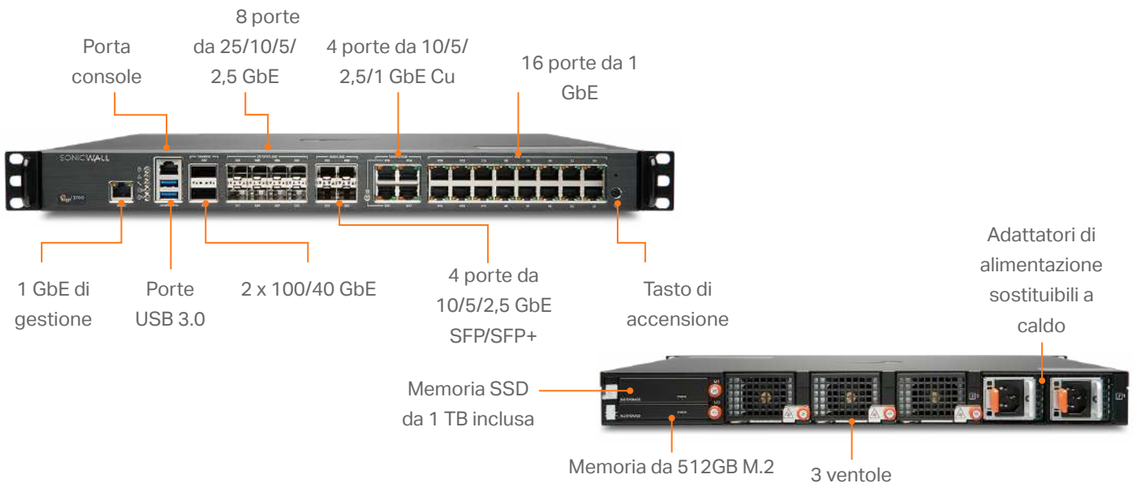


NS*sp* 11700

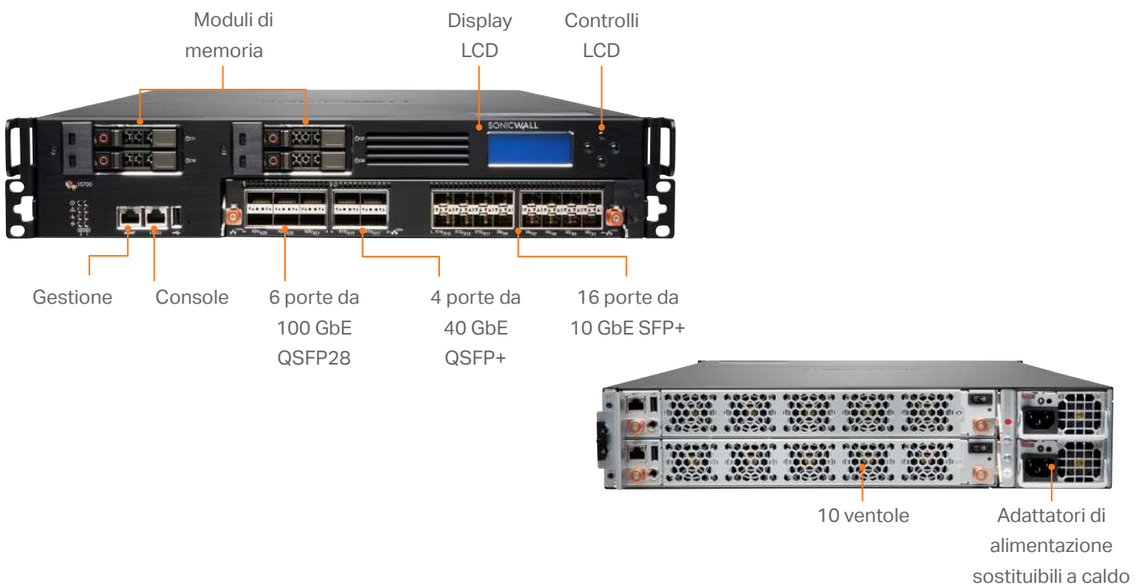


Alias www.alias.it SONICWALL®

NS*sp* 13700



NS*sp* 15700



Specifiche tecniche della serie SonicWall NS*sp*

Firewall in generale	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Sistema operativo	SonicOS 7.0.1	SonicOS 7.0.1	SonicOS 7.0.1	SonicOSX 7.0
Interfacce	2x100G; 8x25G, 4x10G/5G/2,5G/1G (SFP+), 4 x 10G/5G/2,5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 console, 1 porta di gestione	2x100G; 8x25G, 4x10G/5G/2,5G/1G (SFP+), 4 x 10G/5G/2,5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 console, 1 porta di gestione	2x100/40 GbE QSFP28, 8x25/10/5/2,5 GbE SFP28, 4x10/5/2,5 GbE SFP+, 4x10/5/2,5/1 GbE Cu, 16x1 GbE 2 USB 3.0, 1 console, 1 porta gestione	6 x 100 GbE QSFP28, 4 x 40 GbE QSFP+, 16 x 10 GbE SFP+
Memoria integrata	1,5 TB	1,5 TB	1,5 TB	2 SSD da 480 GB
Gestione	CLI, SSH, Web UI, API REST			
Utenti SSO	100.000			
Logging	Analyzer, registro locale, Syslog, IPFIX, NetFlow			

Firewall/prestazioni VPN	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Throughput di ispezione firewall[1]	42	47	60 Gb/s	105 Gb/s
Throughput di prevenzione delle minacce[2]	27	35	45,5 Gb/s	82 Gb/s
Throughput di ispezione applicazioni[2]	30	44	57 Gb/s	86 Gb/s
Throughput IPS[2]	28	37	48 Gb/s	76,5 Gb/s
Throughput con decrittazione e ispezione TLS/SSL (SSL DPI)[2]	10	11,5	16,5 Gb/s	21 Gb/s
Throughput VPN[3]	22,5	26,7	29 Gb/s	32 Gb/s
Connessioni al secondo	280.000	280.000	280.000	800.000
Connessioni max. (SPI)	15.000.000	20.000.000	25.000.000	80.000.000
Connessioni max. (DPI)	12.000.000	17.000.000	22.000.000	50.000.000
Connessioni max. (DPI SSL)	1.500.000	1.750.000	2.000.000	3.000.000

VPN	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Tunnel VPN site-to-site	6.000	12.000	12.000	25.000
Client VPN IPSec (max)	2000 (6000)	2000 (6000)	2.000 (6.000)	2.000 (10.000)
Licenze VPN SSL (max)	2 (3000)			
Autenticazione/crittografia	DES, 3DES, AES (128, 192, 256 bit)/MD5, SHA (1.256.384.512), crittografia Suite B		DES, 3DES, AES (128, 192, 256 bit)/MD5, SHA-1, crittografia Suite B	
Key exchange	Gruppi Diffie-Hellman 1, 2, 5, 14v			
VPN basata su routing	RIP, OSPF, BGP			
Caratteristiche VPN	Dead Peer Detection, DHCP su VPN, attraversamento NAT con IPSec, gateway VPN ridondante, VPN basata su routing			
Piattaforme client della VPN globale supportate	Microsoft® Windows Vista a 32/64 bit, Windows 7 a 32/64 bit, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Windows 10			
NetExtender	Microsoft Windows Vista a 32/64 bit, Windows 7, Windows 8.0 a 32/64 bit, Windows 8.1 a 32/64 bit, Mac OS X 10.4 e versioni successive, Linux FC3 e versioni successive/Ubuntu 7 e versioni successive/ OpenSUSE			
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (incorporato)			

Connettività di rete	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Firewall multi-istanza	N/D	N/D	N/D	Tenant massimi per hardware: 12
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay			
Modalità NAT	1:1, many:1, 1:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente			
Interfacce VLAN	1024			

Alias www.alias.it
SONICWALL®

SonicWave 600 Series Wireless Access Points

Superior Performance in Wireless Solutions

SonicWall's 600 Series Wireless Access Points (APs) use 802.11ax — the most advanced technology available — for superior performance in complex, multi-device environments. Cloud-managed using SonicWall's Wireless Network Manager (WNM), these APs offer a number of additional features that provide an enhanced experience, all while delivering the best-in-class security that you expect from SonicWall.

HIGHLIGHTS

Performance

- 802.11ax
- Increased throughput
- Reduced latency
- Better power management

User experience

- Longer battery life
- Neighboring network avoidance
- Target Wake Time (TWT)

Best-in-class wireless security

- WIDS for threat detection
- WIPS for active threat remediation
- Rogue AP and device detection

Intuitive cloud management and monitoring tool

- Integrated Switch management
- Alerts and rich analytics
- Automatic firmware updates
- Integrates with Wireless Network Manager and WiFi Planner
- RF spectrum analysis

Zero-Touch Deployment

- Fast and easy deployment
- Auto-detection and auto-provisioning
- Compatible with SonicExpress mobile app

Performance

SonicWall's SonicWave 600 Series Access Points utilize 802.11ax technology, improving performance in complex environments. The use of 1024 QAM allows more data to pass through, and 802.11ax provides enhancements in MU-MIMO, with both uplink and downlink capabilities.

Additionally, 802.11ax works in both the 2.4 GHz and 5 GHz bands. Testing has shown that 802.11ax can reduce latency by 75% and enable up to a 4X improvement in overall throughput, with nominal data rate improvement of up to 37% compared to 802.11ac Wave 2.

Enhanced user experience

SonicWave APs enhance the user experience in a number of ways. Not only are processor speeds faster, but beamforming allows for a more direct connection that is faster and more reliable than without beamforming. Improved power control methods help to avoid interference with nearby networks, making for a better experience. And Target Wake Time management helps preserve battery life in mobile devices.

Best-in-class wireless security

Most SonicWave access points include a separate radio dedicated to security, which performs rogue AP detection, passive scanning and packet capturing.

The SonicWave solution also integrates additional security-related features, including wireless intrusion detection and prevention, virtual AP segmentation, wireless guest services, RF monitoring and wireless packet capture. SonicWave APs also feature zero-wait DFS, which identifies and avoids interference with radar systems while eliminating the wait associated with being booted from one DFS channel and finding another to connect with.

Intuitive cloud management and monitoring tool

SonicWave APs are easy to set up and deploy. They integrate with SonicWall Wireless Network Manager, which is a highly intuitive, scalable and centralized Wi-Fi network management system capable of delivering rich wireless and switching analytics, as well as simplified, single-pane-of-glass onboarding via the cloud. The APs also integrate with WiFi Planner, a site survey tool that enables you to optimally design and deploy a wireless network, resulting in a reduced total cost of ownership. And with RF spectrum analysis, you can detect and identify the source of RF interference and monitor the health of a wireless system.

Zero-Touch Deployment

Zero-Touch makes it easy to register your unit and onboard SonicWave APs with the help of the SonicWall SonicExpress mobile app. The APs are automatically detected and provisioned with Zero-Touch Deployment. Available on iOS and Android, the SonicExpress mobile app lets network administrators monitor and manage networks from anywhere.

Alias www.alias.it SONICWALL®

Alias www.alias.it SONICWALL®

SonicWave 600 Series Specifications

HARDWARE SPECIFICATIONS	SONICWAVE 621	SONICWAVE 641	SONICWAVE 681
Location	Indoor	Indoor	Indoor
Maximum power consumption (W)	21	23	34
Status indicators	Seven (7) LED (Power, security, BLE, LAN, 5G, 2.4G, WWAN)		
Antennas	4 internal	8 internal	12 internal
Wired network ports	(1) 100/1000/2.5 GbE auto-sensing RJ-45 for Ethernet and Power over Ethernet (PoE) (model 621/641); (1) 100/1000/5.0 GbE auto-sensing RJ-45 for Ethernet and Power over Ethernet (PoE) (model 681); (1) Micro-USB console; (1) USB 3.0		
5G/4G/LTE USB modem support	Yes	Yes	Yes
Accessories included	Ceiling Mounting Kit	Ceiling Mounting Kit	Ceiling Mounting Kit
Virtual access points/SSID group	Up to 8 per access point		
Chassis	UL 1024 plenum rated		
Ethernet interface	1 x 2.5GbE	1 x 2.5GbE	1 x 5GbE
USB 3.0	1	1	1
Console (micro USB-type)	1	1	1
Kensington lock hold	Yes	Yes	Yes
PoE power requirement	802.3at	802.3at	802.3bt type 3
12V DC Jack	Yes	Yes	Yes
Unit dimensions (cm)	17.4 x 17.4 x 3	20 x 20 x 3.7	21.3 x 21.3 x 3.9
Shipping dimensions (cm)	23 x 22.9 x 7.4	23 x 22.9 x 7.4	26.5 x 24 x 9.5
Unit weight (kg)	0.68	0.85	1.10
WEEE weight (kg)	0.79	1.2	1.49
Shipping weight (kg)	1.27	1.2	1.49

STANDARDS AND COMPLIANCE	SONICWAVE 621	SONICWAVE 641	SONICWAVE 681
IEEE standards	802.11ax, 802.11ac, 802.11n, 802.11g, 802.11b, 802.11a, 802.11e, 802.11i, 802.11r, 802.11k, 802.11v, 802.11w		
Compliance	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11e, IEEE 802.11i, IEEE 802.3at, IEEE 802.3bz, WPA3, WPA2, AES, IEEE 802.11r, IEEE 802.11k, IEEE 802.11v, IEEE 802.11w		
Regulatory	FCC/ICES Class B, CE, RCM/ACMA, VCCI Class B, TELEC, BSMI, NCC, MSIP, ANATEL, Customs Union, RoHS (Europe/China), WEEE		
Safety approvals	UL E211396, UL 62368-1, UL 60950-1 cUL CAN/CSA C22.2 No. 62368-1-14, CAN/CSA C22.2 No. 62368-1-14, EN 60950-1 Or EN 62368-1, IEC 60950-1, IEC 62368-1, Europe: EN 60950-1, EN 62368-1, Taiwan: CNS 1336-1		
Radio approvals	USA: FCC Part 15C, 15E, Canada: ISED RSS-247, Europe: (RED) EN 300 328, EN 301 893, Aus/NZ: AS/NZs 4268, Taiwan: NCC LP002, Additional country approvals for Japan, Korea, China, India, Brazil		
EMI approvals	USA: FCC P15B, Canada: ICES-003, Europe: EN 301 489-1, -17, EN 55032, EN 55024, Aus/NZ: CISPR 32, Japan: VCCI, Taiwan: CNS 13438		
Exposure approvals	USA: FCC Part 2, Canada: RSS-102, Europe: EN 50385, Aus/Nz: ASNZS 2772		
MIMO	MU-MIMO 2x2 (2 streams) 621 MU-MIMO 4x4 (4 streams) 641 MU-MIMO 8x8 (8 streams) 681		
Max/Recommended connected clients per radio	256/150		
Safety	UL, cUL, TUV/GS, CB, CE, BSMI, Mexico CoC, Customs Union		
USB WAN failover and load balancing	Yes	Yes	Yes

ENVIRONMENTAL	SONICWAVE 621	SONICWAVE 641	SONICWAVE 681
Temperature range	32 to 104°F, 0 to 40°C		
Humidity	10 - 95%, non-condensing		

RADIO SPECIFICATIONS	SONICWAVE 621	SONICWAVE 641	SONICWAVE 681
Radio 1: 2.4GHz	11ax 2x2	11ax 4x4	11ax 4x4
Radio 2: 5GHz	11ax 2x2	11ax 4x4	11ax 8x8
Radio 3: Scanning radio (dual-band selectable)	11ac 1x1	11ac 1x1	11ac 1x1
Radio 4: 2.4GHz BLE/BT 5.0	Yes	Yes	Yes
Antenna Type	Internal	Internal	Internal
Frequency bands	802.11a: 5.180-5.825 GHz, 802.11b/g: 2.412-2.472 GHz, 802.11n: 2.412-2.472 GHz, 5.180-5.825 GHz, 802.11ac: 2.412-2.472 GHz, 5.180-5.825 GHz		
Operating channels	802.11a: US and Canada 12, Europe 11, Japan 4, Singapore 4, Taiwan 4, 802.11b/g: US and Canada 1-11, Europe 1-13, Japan 1-14 (14-802.11b only), 802.11n (2.4 GHz): US and Canada 1-11, Europe 1-13, Japan 1-13 802.11n (5 GHz): US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64 802.11ac: US and Canada 36-48/149-165, Europe 36-48, Japan 36-48, Spain 36-48/52-64		
Transmit output power	Regulatory and Country Code compliant		
Transmit power control	Supported		
Data rates supported	802.11a: 6,9,12,18,24,36,48,54 Mbps per channel, 802.11b: 1,2,5.5,11 Mbps per channel, 802.11g: 6,9,12,18,24,36,48,54 Mbps per channel, 802.11n: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per channel, 802.11ac: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7, 1040, 1170, 1300, 1560, 1733.4 Mbps per channel, 802.11ax: update to 1147.5 Mbps (Radio 1) and 4.804 Gbps (Radio 2)		
Modulation technology spectrum	802.11a: Orthogonal Frequency Division Multiplexing (OFDM), 802.11b: Direct Sequence Spread Spectrum (DSSS), 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS), 802.11n: Orthogonal Frequency Division Multiplexing (OFDM), 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM), 802.11ax: Orthogonal Frequency-Division Multiple Access (OFDMA)		

SECURITY	SONICWAVE 621	SONICWAVE 641	SONICWAVE 681
Data Encryption	WPA3, WPA2, IPSec, 802.11i, AES, SSL VPN**		
SSL-VPN Client*	NetExtender, Connect Tunnel		
Advanced Security Services	Capture ATP, CFS, Geo-IP, Botnet, Anti-virus (Cloud)		

AUTHENTICATION	SONICWAVE 621	SONICWAVE 641	SONICWAVE 681
Authentication	RADIUS, Active Directory, single sign-on (SSO), local user		
Captive Portal	Click-through, external server, social account (Facebook, Google, Twitter and LinkedIn) sign-on		
Captive Portal Sign On	Local users, RADIUS, LDAP, OTP, AD		

REPORTING	SONICWAVE 621	SONICWAVE 641	SONICWAVE 681
Alerts	Critical alert notification via SMS		

*SonicWave acts as an SSL-VPN client
**When used with SonicWall Secure Mobile Access Series appliance

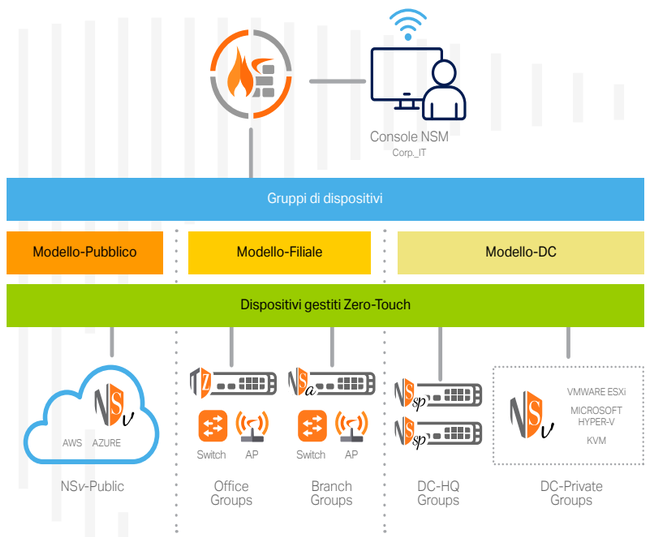
Alias www.alias.it SONICWALL®

Alias www.alias.it SONICWALL®

Network Security Manager

Sistema unificato e scalabile di gestione firewall per qualsiasi ambiente

Che si tratti di proteggere una piccola attività, un'impresa distribuita, più attività o una rete chiusa, la sicurezza di rete può trovarsi sopraffatta da disordini operativi, rischi occulti ed esigenze normative. Storicamente, le prassi di gestione efficiente dei firewall si basano principalmente su sistemi affidabili e misure di controllo operativo. Tuttavia, errori frequenti, configurazioni errate e forse anche violazioni di tali controlli continuano ad essere sfide costanti per i Security Operation Center (SOC) ben gestiti.



CARATTERISTICHE PRINCIPALI

Business

- Riduzione dei costi di gestione della sicurezza
- Conoscenza del panorama delle minacce e della situazione di sicurezza
- Riduzione delle spese di capitale con SaaS

Operatività

- Eliminazione dei silos di gestione dei firewall
- Facile integrazione di qualsiasi numero di firewall in remoto
- Visibilità in tutte le operazioni di sicurezza
- Definizione di configurazione e policy coerenti tra tutti i dispositivi gestiti
- Facilitazione di una rapida implementazione di reti SD-WAN

Sicurezza

- Audit, commit e messa in pratica di policy di sicurezza coerenti in tutti gli ambienti
- Definizione di configurazioni SD-WAN coerenti in tutti i siti
- Caccia e reazione alle problematiche ai rischi con velocità
- Monitoraggio e tracciamento dei risultati degli interventi di policy con maggiore chiarezza
- Prevenzione dell'accesso non autorizzato, comprese le minacce interne

Gestione centralizzata.
Sicurezza migliorata.

www.sonicwall.com/nsm

Alias
www.alias.it

SONICWALL®

SonicWall Network Security Manager (NSM), un sistema centralizzato di gestione firewall multi-tenant, consente di gestire centralmente tutte le operazioni dei firewall, senza errori, applicando workflow verificabili. Reporting e analytics[1,2] offrono visibilità da un unico punto di gestione e consentono di monitorare e scoprire le minacce unificando e correlando i log su tutti i firewall. NSM contribuisce inoltre a mantenere la conformità in quanto fornisce audit trail completi su ogni modifica della configurazione e reporting granulare. La soluzione è scalabile per organizzazioni di qualsiasi dimensione che gestiscono reti con migliaia di dispositivi firewall distribuiti in più sedi. NSM fa tutto con meno fatica e in meno tempo.

Mantenere il controllo: coordinamento delle operazioni dei firewall da un'unica posizione

NSM offre tutto il necessario per ottenere un sistema unificato di gestione dei firewall. Offre visibilità a livello di tenant, controllo dei dispositivi in base ai gruppi e scalabilità illimitata per gestire e fornire centralmente le operazioni di sicurezza di rete SonicWall, che includono l'implementazione e la gestione di tutti i dispositivi firewall, tutti i gruppi di dispositivi e tutti i tenant, la sincronizzazione e l'applicazione di policy di sicurezza coerenti negli ambienti con controlli locali flessibili e il monitoraggio di ogni aspetto da un dashboard dinamico con report e analytics dettagliati. Inoltre, NSM consente di gestire tutto da un'unica console user-friendly a cui è possibile accedere da qualsiasi postazione utilizzando qualsiasi dispositivo abilitato tramite browser.

Gestione multi-tenant

A mano a mano che l'ambiente firewall cresce, sorge la necessità di un sistema di gestione dei firewall che sia scalabile insieme all'ambiente. NSM offre una gestione multi-tenant completa e l'isolamento indipendente del controllo delle policy tra tutti i tenant gestiti. Questa separazione racchiude tutte le caratteristiche e le funzioni di gestione di NSM che determinano il funzionamento del firewall per ciascun tenant. È possibile configurare ogni tenant in modo che disponga del proprio set di utenti, gruppi e ruoli per guidare la gestione dei gruppi di dispositivi, l'orchestrazione delle policy e tutte le altre attività amministrative entro i limiti dell'account tenant assegnato.

Gestione di gruppi di dispositivi

Device Group offre un metodo efficace per creare e gestire dispositivi firewall sotto forma di gruppi o raggruppamenti gerarchici e per provvedere al commit ed all'implementazione di modelli di configurazione su gruppi di firewall, che consentono di sincronizzare e applicare policy, oggetti e requisiti di impostazione sui vari gruppi di firewall selezionati in modo coerente e affidabile. Tutte le modifiche alle policy approvate nel modello vengono applicate automaticamente a tutti i gruppi di dispositivi collegati a quel modello. Il raggruppamento di dispositivi può essere stabilito in modo granulare in base a qualsiasi caratteristica, come tipo di rete, posizione, unità aziendale, struttura organizzativa o una combinazione di tali attributi, per facilitare gestione, identificazione e associazione.

Gestione dei modelli, commit e implementazione

I workflow semplificati di NSM consentono di progettare, convalidare, verificare, approvare e confermare facilmente e rapidamente i modelli di configurazione per la gestione di uno o di migliaia di dispositivi firewall in molte posizioni geografiche. I modelli con varie policy firewall, impostazioni e oggetti correlati sono stabiliti indipendentemente dal dispositivo e vengono utilizzati da NSM per eseguire il push centralizzato e automatico su dispositivi o gruppi di dispositivi che richiedono configurazioni simili.

I modelli combinati con le Template Variable consentono di implementare e rifornire centralmente migliaia di firewall remoti, nonché di stabilire una configurazione coerente preservando valori univoci e specifici per ciascun dispositivo, come IP di interfaccia, configurazione DNS, nome host del firewall ecc. Le aziende distribuite possono facilmente integrare e proteggere nuove filiali e siti remoti utilizzando un unico modello e rendendo superflue le configurazioni manuali e separate per ciascun dispositivo in ciascuna posizione.

Alias
www.alias.it

SONICWALL®

Orchestrazione e monitoraggio SD-WAN

NSM semplifica l'implementazione di reti SD-WAN a livello dell'intera azienda tramite un workflow intuitivo e autoguidato. Inoltre stabilisce e applica centralmente il traffico basato sulle applicazioni e altre configurazioni di gestione del traffico tra migliaia di siti, come filiali e negozi al dettaglio. In aggiunta, NSM consente di monitorare lo stato e le prestazioni dell'intero ambiente SD-WAN al fine di garantire configurazioni coerenti, ottenere prestazioni ottimali delle applicazioni e consentire ai team dell'infrastruttura di rete di individuare e risolvere rapidamente i problemi.

Orchestrazione e monitoraggio VPN

NSM semplifica le configurazioni e le policy VPN con un processo di installazione passo-passo basato su procedure guidate, consentendo quindi agli amministratori di sistema di stabilire la connettività e le comunicazioni tra un sito e l'altro in modo rapido e senza errori utilizzando un workflow autoguidato e ripetibile. Inoltre, il monitoraggio VPN aiuta a mantenere il polso della situazione delle VPN utilizzate, offrendo una visibilità completa su attività, stato e prestazioni dell'intero ambiente VPN. Gli amministratori di rete possono sfruttare queste informazioni per monitorare lo stato della connessione, i dati trasferiti e la larghezza di banda consumata sui tunnel VPN interessati. Gli avvisi consentono agli amministratori di mantenere l'integrità delle connessioni VPN in modo proattivo, garantendo quindi una connettività continua tra i siti.

Maggiore efficacia: lavorare in modo più intelligente con interventi di sicurezza più veloci e meno impegnativi

NSM è uno strumento di gestione della produttività che consente di lavorare in modo più intelligente e attuare interventi di sicurezza più veloci e meno impegnativi. La sua struttura si basa su processi aziendali, sul principio della semplificazione e, in alcuni casi, sull'automazione dei workflow per migliorare il coordinamento della sicurezza. Inoltre aiuta a ridurre la complessità, il tempo e i sovraccarichi nell'esecuzione delle operazioni quotidiane di sicurezza e delle attività amministrative.

Implementazione completamente automatizzata con grande facilità

In NSM è integrato il servizio di implementazione completamente automatizzata Zero-Touch Deployment che consente di implementare e rendere operativi firewall, switch e access point SonicWall in sedi remote e filiali con grande facilità. L'intero processo richiede un intervento minimo da parte dell'utente ed è completamente automatizzato. I dispositivi abilitati «zero-touch» vengono spediti direttamente ai siti di installazione. Una volta registrati e collegati alla rete, tutti i dispositivi connessi sono immediatamente operativi, con sicurezza e connettività perfettamente funzionanti. I modelli predisposti per i dispositivi vengono inviati automaticamente a tutti i dispositivi connessi una volta che vengono stabiliti i collegamenti di comunicazione con NSM. Tutto questo elimina i tempi, i costi e la complessità dei tradizionali processi di integrazione (onboarding) in loco.

Gestione delle modifiche senza errori

NSM consente l'accesso immediato a potenti workflow automatizzati conformi ai requisiti di gestione e audit delle modifiche alle policy firewall dei SOC. Inoltre permette modifiche alle policy senza errori attraverso l'applicazione di una serie di procedure rigorose che comprendono il confronto, la convalida e l'autorizzazione delle configurazioni prima dell'implementazione. I gruppi di approvazione sono flessibili per essere conformi alle procedure di audit interne di vari team funzionali. NSM consente di migliorare l'efficienza operativa, ridurre i rischi ed eliminare configurazioni errate con il processo di workflow con approvazione obbligatoria.

Automazione della gestione con API RESTful

Le API RESTful di NSM consentono agli operatori di sicurezza più esperti di utilizzare un approccio standard alla gestione delle funzionalità specifiche di NSM in modo programmatico senza un'interfaccia di gestione Web. Questo facilita l'interoperabilità tra NSM e le console di gestione di terze parti per aumentare l'efficienza del team di sicurezza interno. I servizi API possono automatizzare le operazioni del firewall per qualsiasi dispositivo gestito e comprendono tipiche attività quotidiane come la gestione di gruppi di dispositivi e tenant, configurazioni di audit, esecuzione di controlli di integrità del sistema e altro ancora.

Maggiore consapevolezza: indagini sui rischi nascosti con monitoraggio, reporting e analytics attivi[1,2]

La dashboard interattiva di NSM offre monitoraggio e reporting in tempo reale nonché dati di analisi. Queste informazioni aiutano a risolvere i problemi, indagare sui rischi e adottare interventi di policy di sicurezza intelligenti per un approccio di sicurezza più adattivo.

Osserva tutto, ovunque sia

NSM, in combinazione con gli Analytics,[1,2] offre fino a 7 giorni di visibilità continua a 360° sull'intero ecosistema di sicurezza SonicWall a livello di tenant, gruppo o dispositivo e fornisce analisi statiche, quasi in tempo reale, di tutto il traffico di rete e delle comunicazioni di dati che attraversano l'ecosistema firewall. Tutti i dati del log vengono automaticamente registrati, aggregati, contestualizzati e presentati in maniera significativa, utilizzabile e facilmente fruibile. È quindi possibile eseguire operazioni di rilevamento, interpretazione, assegnare priorità e adottare interventi difensivi e correttivi adeguati in base alle informazioni corroborate dai dati e con consapevolezza della situazione. I report programmati consentono di personalizzare i report con qualsiasi combinazione di dati sul traffico e offrono fino a 365 giorni di log registrati a livello di dispositivo per analisi cronologiche, rilevamento di anomalie, individuazione delle falle di sicurezza e altro ancora. Tutto questo aiuta nel monitoraggio, nella misurazione e nell'esecuzione di efficaci operazioni di rete e sicurezza.

Comprensione del rischio

Con l'aggiunta di funzionalità di drill-down e pivoting è possibile indagare più a fondo e mettere in correlazione i dati per esaminare e scoprire minacce e problemi nascosti con maggiore precisione e sicurezza. Utilizzando una combinazione di report storici, analytics basate su utenti e applicazioni, e con visibilità sugli endpoint, è possibile analizzare in modo approfondito vari modelli e tendenze correlati al traffico in ingresso/uscita, l'uso delle applicazioni, l'accesso di utenti e dispositivi, azioni sulle minacce e altro ancora. Il tutto permette di acquisire consapevolezza della situazione e preziose informazioni e nozioni non soltanto per scoprire i rischi per la sicurezza, ma anche per orchestrare i rimedi durante il monitoraggio e il tracciamento dei risultati per promuovere e guidare l'applicazione coerente della sicurezza in tutto l'ambiente.

Ottimizzazione della produttività della forza lavoro

User Analytics[1,2] offre una visione ampia e trasparente delle applicazioni Web e delle attività di utilizzo di Internet della forza lavoro. Le funzionalità di drill-down consentono agli analisti di orientare e analizzare facilmente e rapidamente i punti di interesse dei dati a livello di utente e di stabilire misure controllate da policy comprovate per utenti e applicazioni rischiose mentre si sviluppano nel processo di rilevamento. Inoltre, i Productivity Report[1,2] forniscono informazioni sull'utilizzo di Internet e sul comportamento dei dipendenti in un periodo specificato. Lo strumento genera istantanee d'impatto e report dettagliati che classificano le attività Web degli utenti per gruppi di produttività, come gruppi produttivi, non produttivi, accettabili, non accettabili o definiti dall'utente, aiutando le organizzazioni a comprendere e controllare meglio l'utilizzo di Internet.

Implementazione flessibile

I clienti possono implementare NSM in vari modi per soddisfare al meglio i propri requisiti operativi, normativi e di budget.

Per ottenere un'esperienza senza manutenzione, NSM è disponibile come offerta SaaS con hosting di SonicWall e accessibile tramite Internet. Con NSM SaaS è possibile ottenere una scalabilità su richiesta riducendo i costi operativi. Non vi è alcuna necessità di implementare hardware o software, programmare la manutenzione, personalizzare il software, eseguire configurazioni o aggiornamenti, tenere conto di tempi di inattività, ammortamento e costi di ritiro. Tutte queste spese vengono eliminate e sostituite da un abbonamento annuale dal costo basso e prevedibile.

Per avere totale controllo e conformità del sistema, è possibile implementare NSM nel cloud pubblico di Microsoft Azure o come appliance virtuale in un cloud privato su VMWare, Microsoft Hyper-V o KVM, che offrono tutti i vantaggi operativi ed economici della virtualizzazione, tra cui scalabilità e agilità del sistema, velocità di provisioning del sistema, semplicità di gestione e riduzione dei costi.

Funzionalità di sicurezza

Le organizzazioni statali, pubbliche, sanitarie, farmaceutiche e di altro tipo spesso implementano reti chiuse per mantenere la privacy e l'isolamento delle loro applicazioni mission-critical e dei sistemi informatici più sensibili, come i sistemi per documentazione riservata, SCADA e strutture di ricerca. NSM supporta gli ambienti di rete chiusi e offre agli amministratori un metodo offline per eseguire le operazioni di onboarding, la gestione delle licenze, delle patch e degli aggiornamenti del sistema NSM e dei firewall sotto la sua gestione senza dover contattare il SonicWall License Manager e MySonicWall.

Per una maggiore sicurezza, NSM applica diverse misure di controllo dell'accesso agli account per impedire l'accesso non autorizzato all'interfaccia di gestione di NSM. Inoltre concede controlli amministrativi specifici in base ai ruoli dell'utente e attiva il blocco degli account in base a un numero specificato di tentativi di accesso non riusciti. L'accesso utente è consentito, inoltre, solo quando si accede da un elenco specificato di indirizzi IP di origine autorizzati ed è protetto dall'autenticazione a due fattori (2FA)[3].

Alias www.alias.it SONICWALL®

Riepilogo delle funzionalità

Gestione

- Gestione a livello di tenant e gruppo di dispositivi
- Modelli di configurazione
- Raggruppamento di dispositivi
- Conversione da configurazione del dispositivo a modello
- Procedura guidata di commit e implementazione
- Audit della configurazione
- Config – Diff
- Gestione e pianificazione offline
- Gestione delle policy di sicurezza dei firewall
- Gestione delle policy di sicurezza VPN
- Gestione di SD-WAN
- Gestione dei servizi di sicurezza
- Alta disponibilità
- Backup della configurazione
- API RESTful
- Aggiornamento del firmware multi-dispositivo
- Amministrazione basata sui ruoli
- Gestione di access point e switch
- Intelligent Platform Monitoring (IPM)[3]
- Gestione dei certificati multi-dispositivo

Monitoraggio[1,2]

- Integrità e stato dei dispositivi
- Stato della licenza e del supporto
- Riepilogo rete/minacce
- Centro avvisi e notifiche
- Log eventi
- Visualizzazione della topologia

Analytics[1,2]

- Attività basate sull'utente
- Utilizzo delle applicazioni
- Visibilità su più prodotti con Capture Client
- Visualizzazione dinamica in tempo reale
- Funzionalità di drill-down e pivoting

Reporting[1,2]

- Report PDF programmati - Livello tenant/gruppo/dispositivo
- Report personalizzabili
- Sistema di logging centralizzato
- Rapporto su minacce multiple
- Report basato sugli utenti
- Report sull'utilizzo dell'applicazione
- Report su larghezza di banda e servizi
- Creazione di report sulla larghezza di banda per utente

Sicurezza

- Supporto per rete chiusa
- Blocco degli account
- Controllo dell'accesso agli account
- Supporto 2FA[3]
- Supporto TFA dell'app di autenticazione

Licenze e pacchetti

Gestione			
Funzionalità	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Tenant	Sì	Sì	Sì
Inventario dispositivi	Sì	Sì	Sì
Policy di push a livello di gruppo	Sì	Sì	Sì
Gruppo di dispositivi	Sì	Sì	Sì
Modelli	Sì	Sì	Sì
Commit e implementazione (automazione del workflow)	Sì	Sì	Sì
Audit della configurazione	Sì	Sì	Sì
Config Diff	Sì	Sì	Sì
Automazione dei flussi di lavoro	Sì	Sì	Sì
API	Sì	Sì	Sì
Implementazione zero-touch	Sì	Sì	Sì
Orchestrazione e monitoraggio SD-WAN	Sì	Sì	Sì
Orchestrazione e monitoraggio VPN	Sì	Sì	Sì
Pianificazione attività	Sì	Sì	Sì
Backup/ripristino	Sì	Sì	Sì
Aggiornamenti del firmware	Sì	Sì	Sì
Gestione di access point e switch	Sì	Sì	Sì

Licenze e pacchetti, continua

Reporting			
Funzionalità	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Dashboard a livello di gruppo/tenant	Sì	No	No
Capture ATP (livello dispositivo)	Sì	Sì	No
Capture Threat Assessment (livello dispositivo)	Sì	Sì	No
Report sulla produttività[5]	No	Sì	No
Report VPN	No	Sì	No
Visibilità e reporting a livello di gruppo	Sì	No	No
Programmazione report (flusso, CTA e gestione)	Sì (tranne report di flusso)	Sì	No
Giorni di reporting dei dati	7 giorni	365 giorni	No

Analisi			
Funzionalità	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Analytics basati sull'utente – Livello dispositivo	No	Sì	No
Analytics delle applicazioni – Livello dispositivo	No	Sì	No
Analytics delle minacce – Livello dispositivo	No	Sì	No
Drill-down e pivot – Livello dispositivo	No	Sì	No

Alias www.alias.it SONICWALL®

Alias www.alias.it SONICWALL®

SonicWall Capture Client

Blocca le violazioni a una velocità senza precedenti e in modo autonomo

La crescente minaccia posta dal ransomware e da altri attacchi basati su malware ha dimostrato che l'efficacia di una soluzione di protezione dei client non è misurabile solo in termini di compliance degli endpoint. La tecnologia antivirus tradizionale utilizza un approccio basato su firme ormai superato, che non è riuscito a tenere il passo con il malware e le tecniche di elusione emergenti.

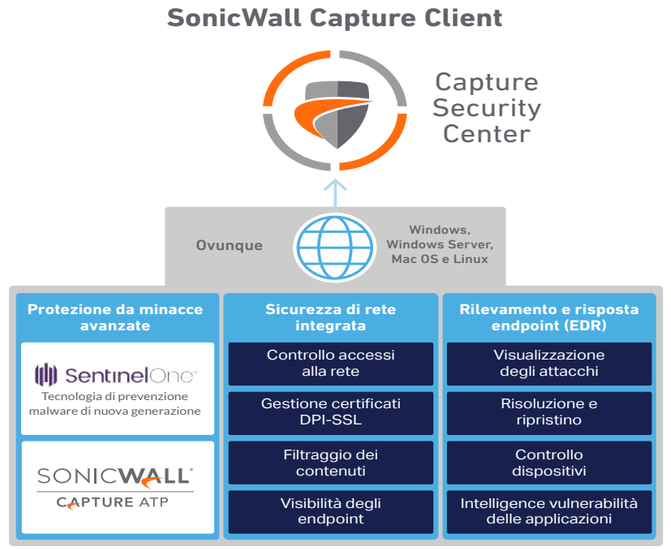
Inoltre, con la diffusione di fenomeni come il telelavoro, la mobilità e il BYOD, è più che mai indispensabile garantire una protezione costante, il controllo delle vulnerabilità delle applicazioni, l'implementazione di policy web e altro ancora per gli endpoint, ovunque essi siano. SonicWall Capture Client è una soluzione unificata che offre molteplici funzionalità di protezione e di rilevamento e risposta (EDR) per gli endpoint.

CARATTERISTICHE PRINCIPALI

- Rilevamento efficace e immediato delle minacce senza interferenze
- Gestione centralizzata e via cloud con funzionalità multi-tenant per rafforzare la sicurezza di rete e degli endpoint
- Soluzione semplice e intuitiva che consente a team di sicurezza e responsabili IT di bloccare le moderne minacce informatiche

Sicurezza degli endpoint su misura per le aziende

Leggi il documento: sonicwall.com



Capture Client applica la protezione dalle minacce avanzate basata sul comportamento, con tecnologia NGAV di SentinelOne.

L'integrazione con Capture ATP garantisce una maggiore efficacia in termini di sicurezza, tempi di risposta più rapidi e un TCO più basso.

Caratteristiche e vantaggi

Monitoraggio continuo del comportamento

- Profilo completo delle attività relative a file, applicazioni, processi e alla rete
- Protezione da malware basati su file o di tipo fileless
- Visione a 360 gradi degli attacchi con informazioni di intelligence concrete

Threat hunting con visibilità approfondita

- La funzionalità Deep Visibility consente di cercare minacce in base a indicatori di comportamento e indicatori di compromissione (IOC) sui dispositivi Windows, MacOS e Linux gestiti
- Ricerca e risposta automatizzate alle minacce con regole e avvisi personalizzati

Integrazione con Capture Advanced Threat Protection (ATP)

- I file sospetti sui dispositivi Windows vengono automaticamente sottoposti all'analisi sandbox avanzata
- Rilevamento delle minacce prima dell'esecuzione, come ad es. i malware ad attivazione ritardata
- Confronto con i verdetti sui file del database di Capture ATP, senza dover caricare i file nel cloud

Capacità di ripristino esclusive

- Supporto di policy per rimuovere completamente le minacce
- Ripristino autonomo di uno stato noto degli endpoint prima che vengano avviate attività dannose

Tecniche multilivello basate su metodi euristici

- Intelligence nel cloud, analisi statica avanzata e protezione comportamentale dinamica
- Protezione e risoluzione di malware noti e sconosciuti prima, durante o dopo un attacco

Intelligence delle vulnerabilità delle applicazioni

- Catalogazione di ogni applicazione installata e ogni rischio associato
- Analisi delle vulnerabilità note con dettagli sulle vulnerabilità ed esposizioni comuni (CVE) e sui livelli di gravità segnalati
- Questi dati sono utilizzabili per assegnare priorità alle patch e ridurre la superficie di attacco

Controllo in rete degli endpoint

- Aggiunta di controlli simili a quelli di un firewall sugli endpoint
- Base di regole di quarantena aggiuntiva per gestire i dispositivi infetti

Remote Shell[1]

- Elimina la necessità di avere un contatto fisico con i dispositivi per risolvere eventuali problemi, modificare le configurazioni locali ed eseguire indagini forensi

Nessuna necessità di scansioni o aggiornamenti periodici

- Massimo livello di protezione in ogni momento, senza limitare la produttività degli utenti
- Scansione completa all'installazione e monitoraggio continuo in seguito per rilevare attività sospette

Integrazione opzionale con i firewall SonicWall

- Possibilità di eseguire l'ispezione approfondita dei pacchetti di traffico crittografato (DPI-SSL) sugli endpoint
- Semplice installazione di certificati affidabili su ogni endpoint
- Gli utenti non protetti vengono indirizzati a una pagina di download di Capture Client prima di accedere a Internet da dietro un firewall

Filtraggio dei contenuti

- Blocca gli indirizzi IP e i domini di siti dannosi
- Aumenta la produttività degli utenti riducendo la larghezza di banda o limitando l'accesso a contenuti web non idonei o improduttivi

Controllo dei dispositivi

- Blocco dei dispositivi potenzialmente infetti per impedirne la connessione agli endpoint
- Utilizzo di policy di autorizzazione granulari

Alias www.alias.it SONICWALL®

Funzionalità di Capture Client

Funzionalità	Advanced	Premier
Gestione cloud, reportistica e analisi (CSC)	✓	✓
Integrazioni della sicurezza di rete		
Visibilità e implementazione degli endpoint	✓	✓
Distribuzione dei certificati DPI-SSL	✓	✓
Filtraggio dei contenuti	✓	✓
Protezione avanzata degli endpoint		
Antimalware di nuova generazione	✓	✓
Sandbox Capture Advanced Threat Protection	✓	✓
ActiveEDR (rilevamento e risposta degli endpoint)		
Visualizzazione degli attacchi	✓	✓
Risoluzione e ripristino	✓	✓
Controllo dei dispositivi	✓	✓
Intelligence e vulnerabilità delle applicazioni	✓	✓
Rilevamento di punti di accesso non autorizzati		✓
Controllo in rete degli endpoint		✓
ActiveEDR, ricerca e intelligence delle minacce		
Threat hunting con visibilità approfondita		✓
Remote Shell[1]		✓
Catalogo delle esclusioni		✓

[1] Remote shell sarà disponibile su richiesta in un nuovo account (con 2FA abilitato) direttamente sulla console S1.

Capture Client - Requisiti di sistema | SonicWall

Best practice per le attività globali di sicurezza degli endpoint per MSSP e aziende distribuite

Leggi il documento: www.sonicwall.com

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Datasheet-CaptureClient-A4-JK-6217

Alias www.alias.it

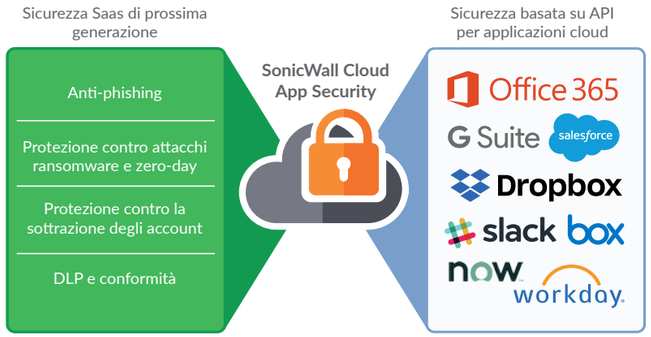
SONICWALL®

Alias www.alias.it

SONICWALL®

SonicWall Cloud App Security

SonicWall Cloud App Security offre la sicurezza di prossima generazione delle applicazioni SaaS come Office 365 e G Suite, proteggendo email, dati e credenziali utente dalle minacce avanzate e garantendo al tempo stesso la conformità nel cloud. Se si sta passando al cloud, SonicWall offre la migliore sicurezza in assoluto basata su API con un basso TCO, minimi costi d'installazione e un'esperienza utente senza soluzioni di continuità.



Visibilità: Identificazione di tutti i servizi cloud (sanzionati e non) utilizzati dai dipendenti dell'organizzazione, compresa la visibilità del traffico est-ovest (da cloud a cloud), dal momento che gli utenti possono autenticarsi su applicazioni non sanzionate utilizzando software sanzionati, come Office 365.

Sicurezza della posta elettronica di prossima generazione: Dal momento che la posta elettronica sta diventando l'applicazione SaaS più diffusa, proteggere questo importante vettore è fondamentale per la sicurezza SaaS. La soluzione prevede il trasferimento degli allegati nella sandbox, la protezione avanzata degli URL e la protezione BEC (Business Email Compromise).

Protezione avanzata contro le minacce: Prevenzione della propagazione dei malware tramite app come OneDrive, Box e Dropbox con scansione in tempo reale delle minacce conosciute e sandboxing Capture ATP per le minacce zero-day e sconosciute.

Sicurezza dei dati: Attuazione di politiche di sicurezza data-centriche, che consentono controlli d'accesso granulari, impedendo il caricamento di file sensibili o riservati. La soluzione comprende strumenti politici basati sui ruoli, classificazione dei dati e tecnologie per la prevenzione delle perdite di dati per il monitoraggio dell'attività degli utenti e il blocco o la limitazione degli accessi.

Conformità: La soluzione raccoglie un audit trail completo per ogni azione, compresi gli eventi in tempo reale e quelli storici e mette a disposizione semplici modelli DLP per l'effettuazione dei controlli delle politiche e la conformità normativa in tempo reale.

Vantaggi:

Sicurezza della posta elettronica di prossima generazione

- Blocco dei ransomware, degli attacchi zero-day e delle email di phishing mirato prima che raggiungano la casella di posta in arrivo dell'utente
- Il trasferimento degli allegati nella sandbox e la protezione avanzata degli URL assicurano una protezione avanzata contro le minacce
- Scansione del traffico email in ingresso, in uscita e interno in Office 365 e G Suite
- Blocco degli attacchi di impersonazione tramite apprendimento automatico e intelligenza artificiale (AI)
- Richiamo di email nocive dalle caselle della posta in arrivo degli utenti dopo l'invio

Sicurezza SaaS di prossima generazione (CASB)

- Visibilità e controllo a livello granulare sulle applicazioni informatiche sanzionate e nascoste
- Copertura completa sul traffico user-to-cloud e cloud-to-cloud
- Prevenzione dell'upload di dati sensibili e della condivisione non autorizzati dei file
- Definizione di politiche coerenti in materia di sicurezza dei dati sulle applicazioni sanzionate
- Protezione contro la sottrazione degli account (ATO), minacce interne, credenziali compromesse
- Blocco della propagazione di ransomware e malware zero-day nel cloud
- Attuazione di politiche normative sulla conformità tramite semplici modelli DLP
- Identificazione delle violazioni e delle lacune di sicurezza tramite l'analisi degli eventi storici e in tempo reale

La sicurezza diventa semplice e accessibile

- Esperienza utente completa con accesso da qualsiasi dispositivo e da qualunque postazione
- Eliminazione di punti deboli, problematiche di latenza e necessità di riorientare il traffico tramite proxy
- Automazione dell'individuazione delle applicazioni nel cloud in abbinamento a SonicWall NGFW
- Riduzione del costo totale di proprietà (TCO) grazie alla rapidità d'installazione e alla facilità d'uso

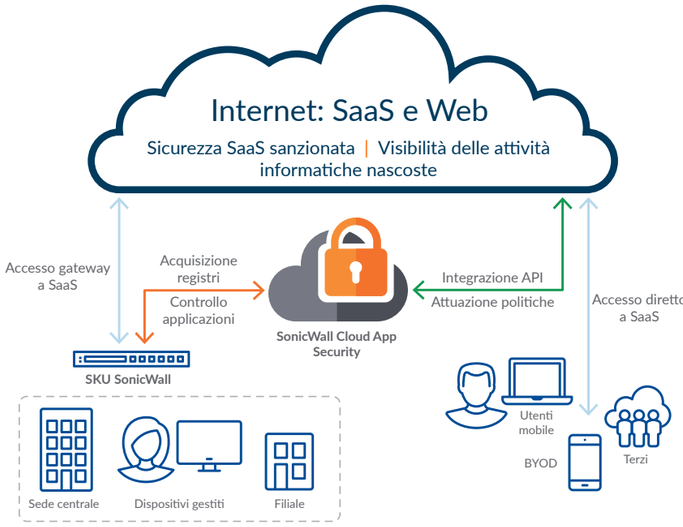
Panoramica della soluzione

Descrizione della soluzione SonicWall

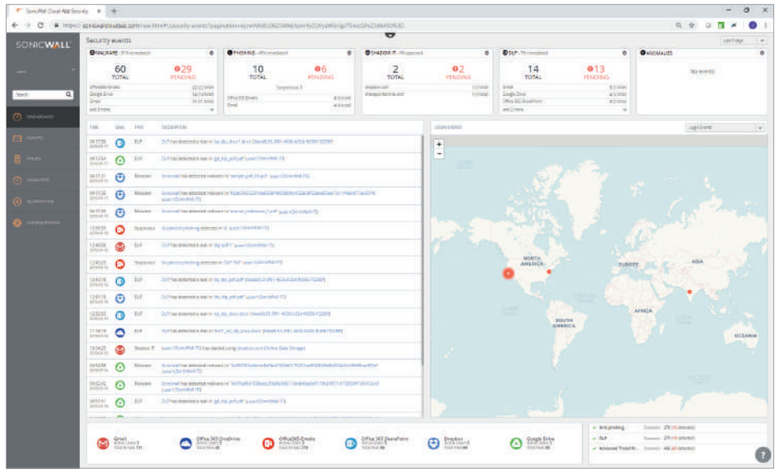
La soluzione SonicWall Cloud App Security consente la scansione fuori banda del traffico alle applicazioni SaaS sanzionate e non tramite API e analisi dei registri del traffico.

La soluzione si integra perfettamente con le applicazioni SaaS sanzionate utilizzando API native, mettendo a disposizione funzionalità CASB: visibilità, protezione avanzata delle minacce, prevenzione di perdite di dati (DLP) e conformità. Utilizzata in abbinamento a un firewall di prossima generazione (NGFW) SonicWall, Cloud App Security consente la visibilità e il controllo della visibilità delle attività informatiche nascoste per l'uso del cloud in rete.

La soluzione consente ai responsabili informatici di installare le applicazioni SaaS senza compromettere la sicurezza e la conformità. Gli amministratori possono definire da un'unica console le politiche coerenti per tutte le applicazioni SaaS installate a livello dell'organizzazione. È possibile utilizzare i modelli di report DLP e di conformità predefiniti per chiudere rapidamente le falle di sicurezza e definire politiche personalizzate per soddisfare le esigenze aziendali e normative. Sia che si debbano gestire pochi utenti o centinaia di migliaia di dipendenti in ogni parte del mondo, la soluzione può essere modulata in funzione delle proprie esigenze, senza bisogno d'installare e gestire alcun hardware.



Sicurezza SaaS basata su API con funzioni CASB



Il pannello di controllo in tempo reale consente agli amministratori di monitorare l'uso delle applicazioni a rischio, tracciare l'attività degli utenti, il volume delle transazioni e la sede in cui le applicazioni vengono utilizzate. La soluzione garantisce l'adozione sicura delle applicazioni SaaS senza ricadute sulla produttività del personale.

Sicurezza completa per Office 365 e G Suite

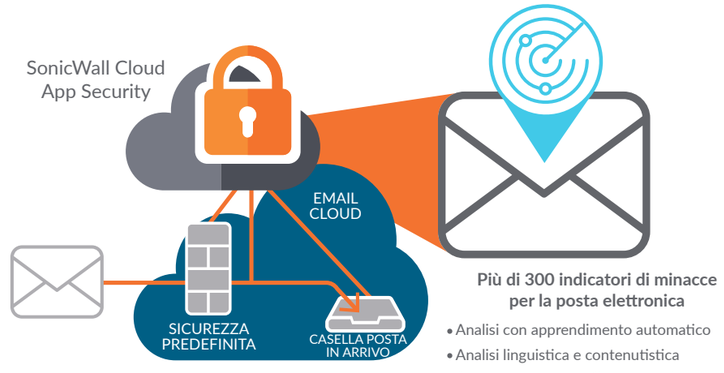
Sicurezza di prossima generazione per la posta elettronica nel cloud

SonicWall Cloud App Security comprende la funzione di sicurezza della posta elettronica di prossima generazione progettata per le piattaforme di posta elettronica in cloud. Normalmente, quando le organizzazioni spostano la posta elettronica nel cloud, fanno esclusivamente affidamento sulla sicurezza offerta dal fornitore del servizio o la integrano con un proxy MTA tradizionale. I gateway di posta elettronica esterni, tuttavia, potrebbero non essere sufficienti per rilevare e bloccare le minacce di oggi.

Oltre ai tradizionali livelli di sicurezza della posta elettronica dei controlli SPF, DKIM e DMARC, ed al filtraggio degli URL tramite le principali fonti di dati per le blacklist degli URL, l'esclusiva architettura di Cloud App Security offre una protezione che le soluzioni con gateway esterni non sono in grado di dare, ovvero:

- Aggiunge un livello di protezione contro le minacce avanzate: Cloud App Security blocca i messaggi di phishing che Office 365 e G Suite non sono riusciti ad intercettare. La soluzione utilizza l'apprendimento automatico, l'intelligenza artificiale e l'analisi dei big data per offrire potenti funzioni anti-phishing, sandboxing degli allegati, protezione avanzata degli URL e protezione contro l'impersonazione.
- Monitora le email in arrivo, in uscita e interne: l'integrazione del SaaS in Cloud App Security consente di scansionare e mettere in quarantena tutte le email prima che arrivino nella casella di posta in arrivo dell'utente, sia che provengano dall'esterno dell'organizzazione, sia da un account interno compromesso.
- Scansiona i messaggi storici per individuare eventuali minacce: alla prima connessione Cloud App Security scansiona i messaggi storici (anche quelli degli account chiusi) per individuare potenziali violazioni o account compromessi.
- Richiamo messaggi a livello globale: i messaggi dannosi possono essere modificati o richiamati in qualsiasi momento indipendentemente dal fatto che siano dannosi, contengano informazioni riservate o siano stati trasmessi perché accidentalmente un dipendente ha selezionato "rispondi a tutti".

Poiché la protezione della posta elettronica di Cloud App Security viene applicata a monte della casella di posta in arrivo ma a valle dei filtri inattivi Microsoft o Google (come pure degli eventuali gateway MTA installati), i suoi algoritmi di apprendimento automatico sono tarati espressamente per individuare le minacce che non sono state ancora intercettate. Inoltre, Cloud App Security è in grado di integrare i risultati delle scansioni native nei suoi algoritmi di rilevamento.



La protezione virtuale in linea blocca i messaggi dannosi prima che raggiungano la casella di posta in arrivo degli utenti

Alias www.alias.it SONICWALL®

Caratteristiche

FUNZIONALITÀ		VANTAGGIO
Visibilità	Cloud Application Discovery	Individua automaticamente le applicazioni nel cloud utilizzando i file di registro dei firewall SonicWall per individuare le attività nascoste in rete
	Visibilità dell'uso del cloud	Visualizzazione grafica in tempo reale delle applicazioni in uso, del volume di traffico, dell'attività degli utenti e delle sedi
	Valutazione dei rischi delle applicazioni	Assunzione di decisioni informate di blocco/sblocco delle applicazioni sulla base della valutazione del rischio
	Monitoraggio eventi	Monitoraggio delle singole azioni, compresi gli eventi in tempo reale e quelli storici, effettuato nell'ambiente SaaS aziendale
Sicurezza della posta elettronica di prossima generazione	Anti-phishing	Blocco degli attacchi di phishing progettati per aggirare la sicurezza predefinita di Office 365 o G Suite
	Anti-spoofing	Protezione del marchio aziendale e degli utenti dalle frodi mediante posta elettronica e dagli attacchi di impersonazione
	Sandboxing degli allegati	Blocca gli allegati nocivi ai messaggi di posta elettronica per impedire che arrivino nella casella di posta in arrivo degli utenti
	Protezione avanzata degli URL	Garantisce la protezione degli utenti dagli URL nocivi integrati
Protezione avanzata contro le minacce	Protezione contro i malware zero-day	Impedisce la memorizzazione e la propagazione dei malware tramite applicazioni come Box, Dropbox, OneDrive e G Drive
	Protezione contro la sottrazione degli account	Protegge le credenziali SaaS individuando il comportamento anomalo degli utenti, le violazioni dei permessi e la variazione delle configurazioni
Sicurezza dei dati	Classificazione dei dati	Identifica i dati sensibili o riservati ed applica le politiche a livello di SaaS per controllare come possono essere condivise le informazioni
	Controllo accessi incentrato sui dati	Gestisce i permessi dei file sulla base del tipo di dati che contengono
	Individuazione delle anomalie tramite flussi di lavoro	Garantisce che la messa in sicurezza dei dati non abbia ricadute sull'attività mediante esecuzione in tempo reale
Conformità	Modelli di conformità	Riduce il carico di lavoro amministrativo utilizzando semplici modelli di conformità per soddisfare i requisiti per SOX, PCI, HIPAA e GDPR
	Audit trail	Accede ai dati degli eventi storici per le verifiche di conformità retrospettiva e reportistica in tempo reale
	Attuazione delle politiche	Attua la conformità in tempo reale con ogni SaaS per controllare i permessi di accesso, spostare file, bloccare e modificare messaggi di posta elettronica e comunicare con utenti ed amministratori

Alias www.alias.it

SONICWALL®

Alias www.alias.it

SONICWALL®

SONICWALL SECURE MOBILE ACCESS (SMA)

Accesso sicuro dovunque e in qualsiasi momento a risorse aziendali in ambienti multi-cloud basato sull'identità, l'ubicazione e l'affidabilità di utenti e dispositivi.

SonicWall SMA costituisce un gateway di accesso sicuro unificato che consente alle organizzazioni di accedere - in qualsiasi luogo e in qualsiasi momento e su qualsiasi dispositivo - a risorse aziendali mission critical. L'engine delle politiche di controllo granulare degli accessi di SMA, l'autorizzazione dei dispositivi in base al contesto, la VPN a livello di applicazione e l'autenticazione avanzata con Single Sign-On consentono alle aziende di adottare il BYOD e la mobilità in un ambiente multi-cloud.

Mobilità e BYOD
Per le organizzazioni che desiderano adottare il BYOD, lavorare in modo flessibile o consentire l'accesso a terzi, SMA diventa il punto di attuazione centrale per tutti questi aspetti. SMA offre la migliore sicurezza nel settore per ridurre al minimo le minacce in superficie, rendendo più sicure le organizzazioni grazie al supporto dei più recenti algoritmi di crittografia e cifrari. SMA di SonicWall consente agli amministratori di fornire un accesso mobile sicuro e privilegi basati sulle identità in modo che gli utenti finali ottengano un accesso semplice e veloce alle applicazioni, ai dati e alle risorse aziendali di cui hanno bisogno. Allo stesso tempo, le aziende possono definire criteri di BYOD sicuro per proteggere le proprie reti e i dati aziendali da accessi non autorizzati e dal malware.

Il passaggio al cloud
Per le aziende che si apprestano a compiere la migrazione verso il cloud, SMA offre un'infrastruttura Single Sign-On (SSO) che utilizza un singolo portale web per autenticare gli utenti in un ambiente informatico ibrido. L'esperienza di accesso è coerente e trasparente, indipendentemente dal fatto che la risorsa aziendale si trovi in sede, nel web o in un cloud in hosting. SMA inoltre si integra con le principali tecnologie di autenticazione multifattoriale attualmente disponibili in campo industriale per garantire una maggiore sicurezza.

Fornitori di servizi gestiti
SMA propone una soluzione chiavi in mano per offrire un elevato grado di continuità e modularità aziendale sia alle organizzazioni con proprie infrastrutture, sia ai provider di servizi gestiti. SMA è in grado di supportare fino a 20.000 connessioni simultanee su una singola apparecchiatura, con una modularità verticale fino a centinaia di migliaia di utenti tramite un clustering intelligente.
I data center possono ridurre i costi con il clustering attivo/attivo e con un bilanciatore di carico dinamico integrato, che consente di riallocare il traffico globale verso il data center più ottimizzato in tempo reale e in base alle esigenze dell'utente. Gli strumenti SMA mettono le aziende specializzate in condizione di fornire servizi con tempi di indisponibilità zero, consentendo loro di soddisfare i requisiti più esigenti dei Service Level Agreement (SLA).

SMA fornisce ai reparti informatici la migliore esperienza e l'accesso più sicuro possibile a seconda dello scenario d'uso. Disponibile come apparecchiatura fisica hardened o potente apparecchiatura virtuale, SMA si inserisce senza soluzione di continuità nelle infrastrutture interne e/o nel cloud esistenti. Le organizzazioni possono scegliere tra una gamma di soluzioni per l'accesso sicuro basato sul web completamente clientless per terzi o dipendenti tramite dispositivi personali, oppure un più tradizionale accesso completo a tunnel VPN basato su client per i dirigenti da qualsiasi tipo di dispositivo. SonicWall SMA ha una soluzione sia per le organizzazioni che devono fornire un accesso sicuro e affidabile a cinque utenti da un'unica postazione, sia per le imprese che necessitano di modularità fino a migliaia di utenti in reti distribuite globalmente.

SonicWall SMA consente alle organizzazioni di adottare mobilità e BYOD senza timori, e di passare più facilmente al cloud. SMA consente più autonomia ai lavoratori, mettendo a loro disposizione modalità di accesso valide per tutti.

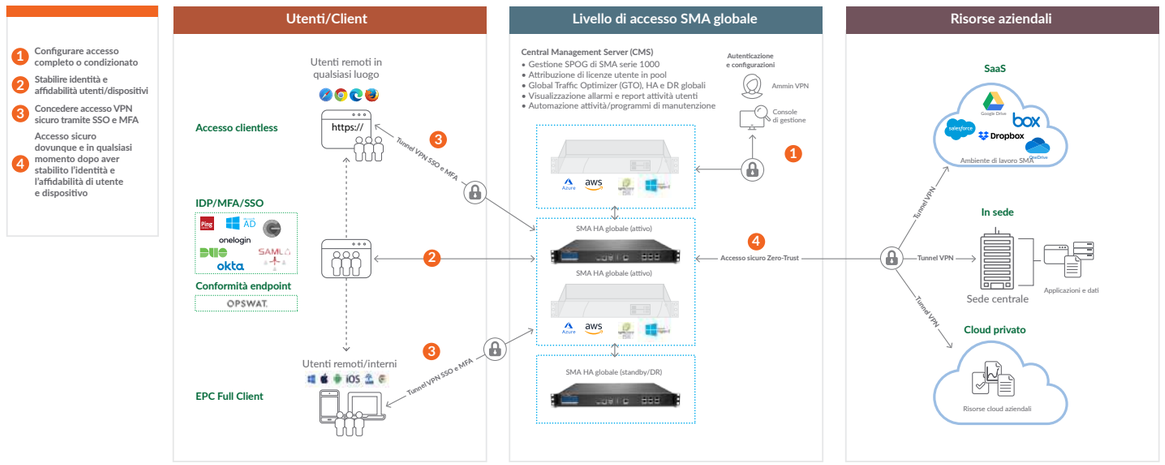
Vantaggi:

- Accesso sicuro unificato a tutte le risorse di rete e nel cloud "in qualsiasi momento, per qualsiasi dispositivo e per qualsiasi applicazione"
- Controllare chi accede a quali risorse definendo politiche granulari tramite il robusto engine di controllo degli accessi
- Aumentare la produttività consentendo il Single Sign-On federato a qualsiasi applicazione SaaS o locale con un singolo URL
- Ridurre il costo totale della proprietà e la complessità della gestione degli accessi consolidando le componenti delle infrastrutture in un ambiente informatico ibrido
- Sapere quali dispositivi cercano di collegarsi e concedere l'accesso sulla base delle politiche e dello stato di salute degli endpoint
- Impedire le violazioni da parte del malware scansionando tutti i file caricati in rete tramite la sandbox Capture ATP
- Proteggersi contro gli attacchi basati sul web e garantire la conformità PCI con l'add-on Web Application Firewall
- Bloccare gli attacchi DDoS e zombie tramite il rilevamento Geo IP e la protezione Botnet
- Disporre della funzionalità sicura con agente nativo tramite accesso clientless HTML5 basato su web browser senza l'impegno di dover installare e mantenere agenti sui dispositivi endpoint
- Ottenere informazioni approfondite fruibili per prendere le decisioni giuste con il monitoraggio in tempo reale e la reportistica completa
- Installare sotto forma di apparecchiature fisiche o virtuali in cloud privati su ESXi o Hyper-V, o in ambienti cloud pubblici AWS o Microsoft Azure
- Abilitare l'emissione dinamica delle licenze di accesso basate sulla domanda in tempo reale, con indirizzamento automatico dell'endpoint alla connessione più performante e dalla latenza più bassa
- Riduzione dei costi iniziali grazie al bilanciamento del carico integrato senza hardware o servizi aggiuntivi, senza alcun impatto per l'utente sul failover dell'apparecchiatura
- Assicurazione contro le interruzioni di servizio o i picchi stagionali grazie all'immediata modularità della capacità

Installazione SMA

Un gateway dalla sicurezza potenziata per l'accesso sicuro, sempre e ovunque, da qualsiasi dispositivo

I gateway SMA mettono a disposizione un accesso remoto sicuro end-to-end completo alle risorse aziendali che si trovano in sede, nel cloud e in datacenter ibridi. Si tratta di apparecchiature che utilizzano controlli di accesso basati sulle politiche e sull'identità, autenticazione contestuale dei dispositivi e VPN a livello di applicazioni per consentire l'accesso a dati, risorse e applicazioni dopo aver stabilito l'identità e l'affidabilità dell'utente, dell'ubicazione e del dispositivo. Vengono installate in modo flessibile sotto forma di apparecchiature Linux hardened o di apparecchiature virtuali in cloud privati su ESXi o Hyper-V, o in ambienti cloud pubblici AWS o Microsoft Azure.



Installazione SMA nel cloud / in sede

Installazione flessibile con apparecchiature fisiche e virtuali

SonicWall SMA può essere installato come apparecchiatura hardened ad alte prestazioni o come apparecchiatura virtuale, sfruttando le risorse di calcolo condivise per ottimizzare l'utilizzo, facilitare la migrazione e ridurre i costi di investimento. I dispositivi hardware sono basati su un'architettura multi-core ad elevate prestazioni che offre accelerazione SSL, throughput VPN e potenti proxy per garantire un accesso sicuro e affidabile. Per le organizzazioni regolamentate e per quelle federali, SMA è disponibile anche con certificazione FIPS 140-2 Level 2. Le apparecchiature virtuali SMA offrono le stesse caratteristiche avanzate di accesso sicuro delle principali piattaforme virtuali o del cloud, come Microsoft Hyper-V, VMware ESX e AWS.

Licenze d'uso utilizzabili da diverse apparecchiature

Le organizzazioni che dispongono di apparecchiature distribuite su scala globale possono beneficiare dell'oscillazione della domanda di licenze d'uso legata ai fusi orari. Indipendentemente dal fatto che un'organizzazione utilizzi licenze VPN complete o licenze ActiveSync di base, la gestione centralizzata di SMA riassegna le licenze alle apparecchiature gestite nelle aree geografiche in cui si sono avuti picchi di domanda dalle applicazioni di altre zone geografiche, nelle quali l'uso è diminuito per via dell'assenza dal lavoro degli utenti nelle ore notturne.

Visibilità di rete con profilatura dei dispositivi sulla base delle situazioni contingenti

Il sistema di autenticazione di fascia alta, che tiene conto delle situazioni contingenti, consente l'accesso solo ai dispositivi affidabili e agli utenti autorizzati. Anche i portatili e i PC vengono analizzati per rilevare la presenza o l'assenza di software di sicurezza, certificati client e ID dei dispositivi. Prima di consentire l'accesso i dispositivi mobili vengono analizzati per verificare le informazioni di sicurezza essenziali come jailbreak o stato della root, ID del dispositivo, stato dei certificati e versione del sistema operativo. Ai dispositivi che non soddisfano i requisiti della politica non viene concesso l'accesso alla rete e l'utente viene avvisato della mancata conformità.

Esperienza coerente da un unico portale web

Gli utenti non devono ricordarsi tutti gli URL delle singole applicazioni o conservare segnalibri dettagliati. SMA dispone di un portale di accesso centralizzato che fornisce agli utenti un URL per accedere a tutte le applicazioni fondamentali da un browser web standard. Quando l'utente ha effettuato l'accesso da un browser, nella finestra del browser viene visualizzato un portale web personalizzabile destinato agli utenti, con un unico punto di controllo per accedere a qualsiasi applicazione SaaS o locale. Il portale visualizza solamente i collegamenti e i segnalibri personalizzati relativi a un gruppo, a un utente o a un dispositivo endpoint specifico. Il portale è una piattaforma agnostica e supporta tutte le principali piattaforme, compresi i dispositivi Windows, Mac OS, Linux, iOS e Android, oltre a supportare numerosi browser per tutti questi dispositivi.

Single Sign-On federato alle applicazioni SaaS e a quelle locali

Eliminare l'esigenza di password multiple e porre fine alle cattive prassi di sicurezza come il riutilizzo delle password. SMA consente un SSO federato alle applicazioni SaaS ospitate nel cloud e a quelle fuori sede. SMA si integra con diversi server di autenticazione, autorizzazione e contabilità e tecnologie leader nel campo dell'autenticazione multifattoriale per una maggiore sicurezza. Il Single Sign-On sicuro viene fornito solo ai dispositivi endpoint autorizzati dopo che SMA verifica l'integrità e la conformità degli endpoint. L'engine della politica di accesso garantisce che gli utenti possano visualizzare solo le applicazioni autorizzate e concedere l'accesso previa autenticazione andata a buon fine. La soluzione supporta un SSO federato anche quando si utilizzano client VPN, mettendo a disposizione dei clienti un'esperienza di autenticazione senza soluzione di continuità sia che utilizzino un accesso sicuro basato su client o clientless.

Prevenire le violazioni e le minacce avanzate

SonicWall SMA aggiunge un livello di sicurezza d'accesso per migliorare la sicurezza e ridurre la superficie di accesso per le minacce.

- SMA si integra con la sandbox multi-engine basata su cloud SonicWall Capture ATP per effettuare la scansione di tutti i file caricati dagli utenti con endpoint non gestiti o da quelli fuori dalla rete aziendale. Ciò garantisce che gli utenti abbiano lo stesso livello di protezione dalle minacce avanzate, come ransomware o il malware zero-day, quando sono in viaggio come se fossero in ufficio[1].
- Il servizio SonicWall Web Application Firewall mette a disposizione delle aziende una soluzione affidabile e integrata per rendere sicure le applicazioni interne basate sul web. Ciò consente ai clienti di garantire la riservatezza dei dati e che i servizi web interni non vengano compromessi in presenza di accessi da parte di utenti malintenzionati o fraudolenti.
- Il rilevamento di Geo-IP e Botnet protegge le organizzazioni dagli attacchi DDoS e zombie e dagli endpoint compromessi che funzionano come botnet.

Accesso clientless sicuro basato sul browser senza soluzione di continuità

La natura "clientless" di SonicWall SMA significa che gli amministratori non devono installare manualmente componenti fat client sui computer da utilizzare per l'accesso remoto. In questo modo si elimina qualsiasi dipendenza da Java e l'impegno per il reparto informatico, aumentando di conseguenza in modo notevole la possibilità di accesso remoto. Ciò significa che, in assenza di requisiti di pre-installazione o di pre-configurazione, i telelavoratori autorizzati possono operare da qualsiasi computer, in qualsiasi parte del mondo, ed accedere in modo sicuro alle risorse aziendali. Nella sua forma più pura, l'accesso sicuro è basato rigorosamente sul browser tramite HTML5, il che offre agli utenti un'esperienza senza soluzione di continuità e unificata.

Offrire un'esperienza "Always On"

Per consentire agli utenti un'esperienza senza soluzione di continuità, SMA mette a disposizione una Always On VPN per i dispositivi Windows gestiti. Gli amministratori possono configurare le impostazioni in modo che venga stabilita automaticamente una connessione VPN ogniqualvolta un client endpoint autorizzato rileva la presenza di una rete pubblica o non affidabile. Ogni accesso al dispositivo Windows mette a disposizione dell'utente una connessione sicura con le risorse aziendali. Gli utenti non devono effettuare l'accesso sui loro client VPN né gestire ulteriori password. Ciò consente un'esperienza senza soluzione di continuità per gli utenti mobili per accedere alle risorse critiche esattamente come se si trovassero in ufficio e consente agli amministratori dei sistemi informatici di mantenere il controllo sui dispositivi gestiti, migliorando la sicurezza dell'organizzazione.

Gestione intuitiva e reportistica completa

SonicWall offre una piattaforma di gestione intuitiva basata sul web, Central Management Server (CMS), per semplificare la gestione delle apparecchiature e fornire ampie funzionalità di reportistica. L'interfaccia utente grafica di facile uso agevola la gestione di apparecchiature e politiche singole o multiple. Ogni pagina mostra come sono configurati i parametri di tutte le macchine in gestione. La gestione unificata delle politiche consente di creare e monitorare le politiche e le configurazioni di accesso. Un'unica politica può controllare l'accesso da parte di utenti, dispositivi e applicazioni, a dati, server e reti. I responsabili informatici possono automatizzare le attività di routine e quelle pianificate, liberando i team addetti alla sicurezza dai compiti ripetitivi affinché si concentrino su attività di sicurezza strategiche, come la risposta agli eventi imprevisti. Essi, inoltre, acquisiscono utili indicazioni sulle tendenze d'accesso degli utenti e sullo stato di salute dell'intero sistema attraverso una reportistica di facile uso e la funzione di log centralizzata.

Consentire la disponibilità dei servizi 24x7

Le organizzazioni hanno l'esigenza di mantenere i servizi forniti attivi e funzionanti con un elevato grado di affidabilità per consentire l'accesso sicuro alle applicazioni critiche in qualsiasi momento. Le apparecchiature SMA supportano la modalità tradizionale attivo/passivo ad alta disponibilità (HA) per organizzazioni che dispongono di un unico data center, o la modalità attivo/attivo HA globale o il clustering attivo/standby per i data center locali o distribuiti. Entrambi i modelli HA consentono agli utenti un'esperienza uniforme con failover a impatto zero e persistenza di sessione.

Implementazione del client VPN in base alle vostre esigenze

È possibile scegliere tra un'ampia gamma di client VPN per fornire un accesso remoto sicuro e vincolante a vari endpoint, compresi portatili, smartphone e tablet.

Client VPN	SO supportato	Modello SMA supportato	Caratteristica principale
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	Tutti i modelli	Fornisce l'autenticazione biometrica, tramite VPN app e implementazione del controllo degli endpoint
Connect Tunnel (Thin Client)	Windows, Mac OS e Linux	6200, 6210, 7200, 7210, 8200v, 9000	Fornisce un'esperienza completa "come in ufficio" con un solido controllo degli endpoint
NetExtender (Thin Client)	Windows e Linux	210, 410, 500v	Implementa politiche di accesso granulari ed estende l'accesso alla rete tramite client nativi

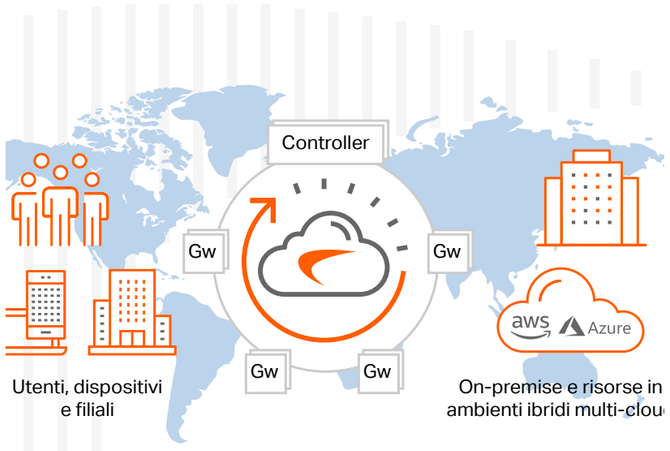
Alias www.alias.it SONICWALL®

Cloud Edge Secure Access

Fornisce l'accesso alla rete zero-trust su scala globale in pochi minuti

SonicWall Cloud Edge Secure Access offre un semplice servizio NaaS (Network-as-a-Service) per la connettività site-to-site e in cloud ibrido per AWS, Azure, Google Cloud e molti altri. Grazie alle tecnologie di sicurezza Zero-Trust e Least-Privilege e alla microsegmentazione software-defined, gli utenti e i dispositivi possono accedere unicamente alle risorse necessarie.

Le aziende possono così offrire la flessibilità del telelavoro, mantenere la flessibilità operativa e, allo stesso tempo, proteggere le risorse ad alto valore aggiunto dalle costose violazioni della sicurezza.



Le funzioni in breve. Riepilogo completo delle funzioni »

10-1.000+	5-15 min.	30+ PoP
Possibili utenti	Tempo d'installazione	In Europa, USA, Medio Oriente e Asia

CARATTERISTICHE PRINCIPALI

- Accesso Zero-Trust con policy di microsegmentazione software-defined per prevenire la diffusione di violazioni.
- Autenticazione Single Sign-On e a più fattori mediante i servizi LDAP, Okta, Google e Azure Identity Provider.
- Network Traffic Control (NTC) consente la protezione a livello di firewall definendo chi (e da dove) può accedere a reti e servizi specifici.
- Device Posture Check (DPC) concede l'accesso alla rete solo ai dispositivi autenticati e conformi.
- App client disponibili per i sistemi operativi macOS, Win10, Android e iOS.
- Accesso Remote Desktop senza client tramite RDP, VNC, SSH e HTTP/HTTPS per l'accesso via web con qualsiasi dispositivo pubblico.
- Migliore esperienza d'uso con i moderni e veloci tunnel WireGuard.
- La VPN sempre attiva emula un'esperienza come in ufficio e mantiene un livello di sicurezza elevato negli hotspot pubblici.
- Semplice interfaccia di configurazione delle policy con drag-and-drop per risparmiare tempo e pannello di controllo per semplificare i controlli di conformità.
- Il monitoraggio della rete offre una panoramica completa del modello di traffico e del livello di sicurezza di utenti, gruppi e server.

L'accesso in modalità Zero Trust limita l'esposizione alle aree sensibili della rete e salvaguardia le risorse aziendali

www.sonicwall.com/cloud-edge

Alias www.alias.it

SONICWALL®

Le soluzioni VPN tradizionali non sono state create per il cloud e presentano alcuni problemi essenziali: la fiducia implicita, che consente alle minacce di muoversi lateralmente all'interno della rete, i tempi d'installazione relativamente lunghi e una maggiore latenza nel cloud a causa del ripetuto reinstradamento del traffico (hair-spinning), che incide sulla qualità dell'esperienza degli utenti.

Gartner prevede che entro il 2023 il 60% delle imprese eliminerà gradualmente la maggior parte delle reti private virtuali (VPN) ad accesso remoto per passare a soluzioni di accesso alla rete zero-trust (ZTNA).

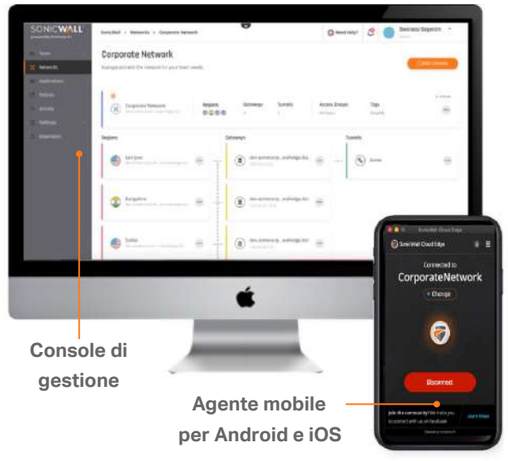
Infrastruttura progettata per una rapida scalabilità e l'implementazione globale

SonicWall Cloud Edge Secure Access è basato sull'avanzata architettura Software-Defined Perimeter (SDP) nativa del cloud, che consente una rapida implementazione e l'onboarding self-service.

- **Installazione più rapida** – In meno di 15 minuti un responsabile IT può registrarsi, creare un gateway e configurare policy granulari basate sul contesto della rete e degli utenti.
- **Onboarding veloce degli utenti** – Un utente finale può scegliere di connettersi tramite il proprio dispositivo o un'applicazione desktop client, oppure di evitare l'installazione del client se utilizza un computer pubblico, a condizione che sia disponibile un browser. Con il modello d'installazione self-service, l'onboarding può essere completato in 5 minuti.

L'architettura SDP è intrinsecamente sicura perché separa il controller di autenticazione degli utenti e dei dispositivi dai gateway, che fungono da garanti dell'affidabilità. Grazie alla distribuzione dei gateway vicino alle sedi degli utenti finali, Cloud Edge Secure Access può essere rapidamente ampliato per mantenere prestazioni elevate e consentire un'esperienza ottimale nel cloud.

La separazione delle funzioni consente inoltre a Cloud Edge Secure Access di bloccare cyber minacce comuni come attacchi DDos, SYN flood e Slowloris.



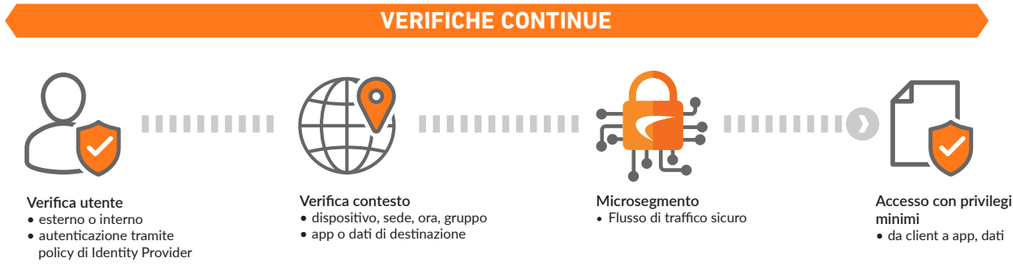
Sicurezza a livello di micro-perimetro definita dal software che segue gli utenti

Oggi i dipendenti desiderano la flessibilità di lavorare da qualsiasi luogo, mentre le aziende vogliono sfruttare le efficienze operative e i risparmi sui costi offerti dal cloud. In questa nuova realtà invertita, dove il lavoro si svolge all'esterno delle postazioni centralizzate e della protezione fisica del firewall, è necessario integrare l'attuale modello di servizi on-premise con un agile modello di sicurezza che "segue" l'utente.

Con SonicWall Cloud Edge Secure Access il perimetro è definito dal software, vale a dire che ogni segmento di micro perimetro racchiude un particolare tipo di flusso di traffico definito dalle policy di accesso. Il segmento inizia dall'utente e si estende a reti, servizi o asset specifici in qualsiasi ambiente cloud, garantendo un approccio molto più versatile.

Alias www.alias.it

SONICWALL®



Accesso Zero-Trust alla rete

Non fidarsi di nulla e verificare tutto

Le policy Zero-Trust consentono agli utenti esterni in possesso dei requisiti adeguati di accedere in sicurezza a una serie di risorse di rete con il supporto di:

- **Autenticazione federata SSO e multifattoriale** – Questa combinazione offre agli utenti un unico portale per autenticarsi in un ambiente IT ibrido, creando un'esperienza coerente e senza soluzione di continuità.
- **Integrazione con i principali fornitori di gestione delle identità basati su cloud** – Le aziende possono estendere la durata operativa delle risorse interne esistenti o passare ai moderni servizi di gestione delle identità basati su cloud, forniti da società come Azure AD, Google Authenticator e Okta.
- **Accesso basato sul contesto con Device Posture Check (PDC)** – Autorizza l'accesso alla rete solo ai dispositivi conformi e autorizzati che superano le verifiche di integrità del sistema operativo e di assenza di malware, garantendo che nessun malware possa entrare nell'infrastruttura.
- **Microsegmentazione software-defined** – Network Traffic Control (NTC) segmenta con precisione tutto il traffico in entrata per impedire che malware o utenti non autorizzati compromettano le risorse della rete e i dati sensibili.
- **Controllo degli accessi basato sul minimo privilegio** – Le aziende possono controllare le interazioni degli utenti con le risorse in base ad attributi rilevanti, tra cui l'identità dell'utente e di gruppo e la sensibilità dei dati.

Lavorare in sicurezza ovunque

Da postazioni attendibili agli hotspot pubblici

- **Protezione Wi-Fi automatica** – Cloud Edge Secure Access per Windows e Mac OS monitora in modo proattivo l'ambiente e attiva automaticamente una connessione di accesso sicura negli hotspot pubblici. Questo livello di protezione aggiuntivo blocca le intercettazioni Wi-Fi, che sono sempre più comuni e possono comportare furti di dati e violazioni della conformità.
- **Kill switch** – Quando una connessione di accesso protetta viene interrotta, questo strumento sospende immediatamente la connessione Internet del dispositivo per impedire potenziali violazioni e furti di dati.
- **Reti Wi-Fi affidabili** – Quando un SSID viene specificato come "attendibile", la funzione di protezione Wi-Fi automatica non si attiva.
- **VPN/applicazioni sempre attive** – Questa pratica funzione ricollega automaticamente un utente all'applicazione o a una serie di applicazioni senza richiedere di nuovo il login o l'autenticazione.

Interconnettività site-to-site o Network-as-a-Service (NaaS)

Grazie ai servizi di connettività site-to-site e Network-as-a-Service (NaaS) di Cloud Edge Secure Access, gli amministratori IT possono collegare velocemente filiali dislocate in luoghi geograficamente distanti. Il NaaS permette di connettere in modo rapido e sicuro chioschi mobili, negozi e punti vendita alle risorse nel cloud senza ricorrere a costose soluzioni MPLS.

- **Servizi di interconnessione site-to-site o site-to-cloud** – La soluzione consente di connettersi facilmente agli ambienti cloud più diffusi, come AWS, Azure e Google Cloud, o di creare una connessione di comunicazione sicura tra reti dislocate in sedi diverse.
- **Implementazione multi-regionale** – Gli amministratori possono installare gateway Cloud Edge dedicati in diverse sedi per offrire velocità e prestazioni ottimali alle filiali e ai dipendenti internazionali.
- **Backbone globale ad alte prestazioni** – Il servizio SonicWall Cloud Edge è disponibile in tutto il mondo. L'infrastruttura garantisce una latenza minima grazie ai gateway distribuiti vicino alle sedi dei clienti e al bilanciamento del carico tra i server.
- **Tunnel sicuro WireGuard all'avanguardia** – Un responsabile IT può utilizzare qualsiasi router o firewall della filiale con IPsec per collegarsi al gateway Cloud Edge più vicino. SonicWall consiglia il tunnel WireGuard, che offre prestazioni molto più veloci e può essere eseguito su un server Linux della filiale per collegarsi al gateway più vicino.

Supporto multi-tenancy nativo con portale dedicato ad ogni cliente e servizi di abbonamento a livelli per aiutare gli MSSP ad aumentare la redditività.

Riepilogo delle funzionalità

Scalabilità e prestazioni

- Da decine a migliaia di utenti
- 1 Gb/s per ogni gateway cliente
- Scalabilità orizzontale in cloud con più gateway

Funzionalità della piattaforma cloud

- Stato del servizio cloud: https://www.sonicwall.com/support
- Gestione cloud inclusa
- Infrastruttura gestita da SonicWall
- Servizi gestiti da MSSP e clienti
- Gateway cloud e indirizzi IP dedicati per ogni cliente
- Bilanciamento del carico su gateway ridondanti incluso
- Scelta della connettività IPsec e WireGuard tra due siti
- Scelta del server DNS interno o predefinito

Funzionalità di sicurezza Zero-Trust

- Accesso clientless tramite HTTP, HTTPS, RDP, VNC, SSH
- App client disponibile per piattaforme Windows, Mac, iOS e Android
- Verifiche dei dispositivi e del contesto (con DPC, accesso basato sul tempo, monitoraggio continuo di utenti e dispositivi)
- Applicazione di policy di minimo privilegio per l'accesso (con politiche di controllo degli accessi)
- Microsegmentazione software-defined (con NTC)
- Segmentazione basata su policy e applicabile per gruppo, rete, utente, applicazione, servizi, dispositivo
- Controllo e monitoraggio del flusso di traffico di rete in micro-segmenti tra utenti, gruppi e servizi in base a regole personalizzabili
- Policy di controllo granulare degli accessi basate su utente, applicazione, Geo IP, geolocalizzazione (paese), tipo di browser, sistema operativo, data e ora

Sicurezza negli hotspot pubblici

- Lo split tunneling consente l'interruzione locale del traffico delle subnet
- Kill Switch impedisce una potenziale violazione interrompendo la connessione Internet del dispositivo per prevenire esfiltrazioni di dati
- La protezione Wi-Fi automatica protegge automaticamente i dispositivi dei dipendenti quando si collegano a Wi-Fi pubblici non protetti
- Il filtraggio DNS blocca l'accesso a determinati siti web, categorie di siti e indirizzi IP

Autenticazione

- Supporto Single Sign-On per fornitori come Okta, G Suite, Azure AD e Active Directory LDAP
- Autenticazione a due fattori integrata tramite SMS o DUO Security e integrazione con Google Authenticator 2FA
- Verifica di sicurezza e conformità dei dispositivi prima dell'accesso alla rete con Device Posture Check

Interoperabilità tra firewall e router aziendali

- SonicWall, Check Point, Fortinet, Palo Alto Networks, WatchGuard, Sophos, Xyxel, UniFi, pfSense, Cisco e Untangle

Monitoraggio, registrazione e supporto

- Soluzione cloud completamente gestita con supporto 24x7 incluso
- Controlli di attività e report per monitorare login, installazioni gateway, connessioni di dispositivi e app
- Integrazione SIEM per acquisire, conservare e distribuire informazioni ed eventi di sicurezza in tempo reale a tutte le applicazioni SIEM
- Elenco automatico dei dispositivi che si collegano alla rete e log corrispondenti.
- Integrazione con Splunk per la percentuale di clic

Conformità

- ISO 27001 e 27002, SOC-2 tipo 2

Alias www.alias.it SONICWALL®

DISTRIBUTORI AUTORIZZATI:

Alias

www.alias.it

Alias
www.alias.it

SONICWALL®

Contattaci SonicWall:

Fabrizio Corradini - Country Manager Italy - fcorradini@sonicwall.com
Valerio Branca - Channel Account Manager North Italy - vbranca@SonicWall.com
Mafalda Barbuto - Inside Channel Account Manager - mbarbuto@sonicwall.com
Margherita Iasiuolo - Distribution Accounts Manager South EMEA - miasiuolo@SonicWall.com
Federico Diamantini - Solutions Engineer - fdiamantini@SonicWall.com
Paolo Melchiori - Senior Solutions Engineer - pmelchiori@SonicWall.com
Jessica Ferrerons - Marketing Manager South EMEA & Benelux - jferrerons@sonicwall.com

SONICWALL®