NSv 270/470/870

I firewall SonicWall della serie Network Security virtual NS*v* 270/470/870 offrono sicurezza di classe enterprise, gestione semplificata, visibilità completa, implementazione flessibile e prestazioni superiori per carichi di lavoro virtuali.

Negli ambienti virtuali vengono periodicamente scoperte vulnerabilità che comportano gravi implicazioni e problematiche a livello di sicurezza. Ma per proteggere tutti questi vettori di sicurezza bisogna essere in grado di applicare la giusta policy di sicurezza nel giusto punto di controllo di rete. Diversi problemi di sicurezza derivano infatti da policy inefficaci o configurazioni errate.

CARATTERISTICHE PRINCIPALI

Sicurezza nel cloud pubblico, privato e governativo

- Firewall di nuova generazione con prevenzione e rilevamento automatizzati delle violazioni in tempo reale
- Tecnologia Real-Time Deep Memory Inspection (RTDMI™) brevettata
- Tecnologia Reassembly-Free Deep Packet Inspection (RFDPI) brevettata
- Visibilità end-to-end completa e gestione semplificata con una policy unificata
- Controllo e intelligence delle applicazioni
- Sicurezza DNS
- Servizio di filtraggio dei contenuti (CFS 5.0) basato sulla reputazione
- Gestione firewall Wi-Fi 6
- Integrazione del controllo accessi alla rete con Aruba ClearPass
- Supporto di cloud governativi AWS e Azure negli USA
- Integrazione con Microsoft Azure Sentinel per una risposta più rapida agli incidenti
- Supporto di piattaforme cloud private (ESXi, Hyper-V, KVM, Nutanix) e pubbliche (AWS, Azure)

Protezione delle macchine virtuali

- Riservatezza dei dati
- Comunicazione sicura con prevenzione di fughe di dati
- Ispezione, monitoraggio e convalida del traffico
- Resilienza e disponibilità della rete virtuale

SCHEDA TECNICA

I firewall della serie NS*v* aiutano i team responsabili della sicurezza a ridurre questo tipo di rischi e vulnerabilità di sicurezza, che possono causare gravi interruzioni dei servizi e delle operazioni business-critical. Consentono alle aziende di controllare il traffico dinamico che passa attraverso il firewall e offrono visibilità e informazioni dettagliate sulle varie policy. Inoltre consentono di semplificare le attività di gestione, ridurre gli errori di configurazione e accelerare i tempi d'installazione, contribuendo a migliorare il livello di sicurezza complessivo.

SonicOSX e servizi di sicurezza

L'architettura SonicOSX dei firewall NS*v* 270/470/870 è basata sul sistema operativo SonicOSX 7, che offre un'interfaccia utente intuitiva e funzionalità avanzate di sicurezza, gestione e connettività.

SonicOSX 7.0 è stato costruito da zero e offre una policy unificata per la gestione integrata di varie policy di sicurezza. Consente di applicare facilmente controlli ai livelli da 3 a 7 in un'unica base di regole per ogni firewall, fornendo un sistema centralizzato per la configurazione delle policy. La nuova interfaccia web presenta visualizzazioni grafiche con informazioni sulle minacce critiche e mostra avvisi che richiedono di configurare policy di sicurezza contestuali con pochi e semplici clic.

La serie NS*v* integra inoltre 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 alla sandbox multi-engine Capture Advanced Threat Protection (ATP) basata su cloud di SonicWall per essere analizzate. Capture ATP utilizza Real-Time Deep Memory Inspection (RTDMI), una tecnologia brevettata da SonicWall, per rilevare e bloccare malware e minacce zero-day che risiedono nella memoria.

Grazie alla combinazione di Capture ATP, tecnologia RTDMI e servizi avanzati di sicurezza, i firewall della serie NS*v* bloccano il malware al gateway prima che possa raggiungere i sistemi critici.

Installazione

1. Cloud Edge: cloud pubblici, privati e governativi sicuri

- Protezione dei carichi di lavoro su Amazon Web Services (AWS) e Microsoft Azure
- Protezione di applicazioni e infrastrutture cloud dalle cyber minacce con funzionalità firewall avanzate di nuova generazione che integrano strumenti come VPN, IPS, CFS, AV e molto altro
- Semplice decrittazione del traffico crittografato e utilizzo del supporto TLS 1.3 per migliorare la sicurezza
- Funzioni di segmentazione e prevenzione delle minacce per garantire la conformità agli standard normativi
- Piena visibilità e controllo del traffico in diverse regioni e zone di disponibilità tramite le policy unificate
- Ottimizzazione dei costi e maggiore efficienza trasformando le spese di capitale (CAPEX) in spese operative (OPEX)
- Protezione dei sistemi cloud AWS e Azure destinati alle agenzie governative degli Stati Uniti e ai loro clienti mediante l'implementazione di firewall NS*v*
- Protezione delle risorse di calcolo virtualizzate e hypervisor per salvaguardare i carichi di lavoro su cloud privati come VMware ESXi, Microsoft Hyper-V, Nutanix e KVM
- Prevenzione delle minacce grazie alla piena visibilità sulle comunicazioni tra gli host delle macchine virtuali
- Corretta applicazione delle policy di sicurezza nell'intero ambiente virtuale
- Regole per l'abilitazione sicura delle applicazioni in base ad applicazione, utente e dispositivo, indipendentemente da dove si trova la macchina virtuale
- Implementazione di zone di sicurezza e isolamento adeguate
- Integrazione con Microsoft Azure Sentinel, una soluzione scalabile e basata sul cloud per la gestione di informazioni ed eventi di sicurezza (SIEM) e l'orchestrazione, automazione e risposta della sicurezza per la gestione delle risposte agli incidenti

2. Internet Edge

- Protezione delle risorse aziendali da attacchi al gateway Internet.
- Protezione dell'internet edge dagli attacchi più sofisticati con funzioni di sicurezza avanzate e blocco automatico delle minacce
- Funzioni di segmentazione e prevenzione delle minacce per garantire la conformità agli standard normativi
- Aumento dell'efficienza e delle prestazioni aziendali e riduzione dei costi grazie ai miglioramenti di SonicOSX
- Segmentazione dei sistemi PoS (Point of Sale) per garantire la continuità dei servizi
- Piena visibilità e controllo del traffico in diverse regioni e zone di disponibilità tramite le policy unificate

Specifiche di sistema della serie NSv

Firewall in generale	NSv 270	NSv 470	NSv 870
Sistema operativo	SonicOSX[11]		
Hypervisor supportati	VMware ESXi v5.5/v6.0/v6.5/v6.7/v7.0/v8.0, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7, Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[10]		
Cloud governativi supportati[12]	AWS e Azure (nelle regioni orientali e occidentali degli USA)		
Tipi di istanze AWS supportate	c5.large c5n.large c5d.large m5.large m5n.large	c5.xlarge c5n.xlarge c5d.xlarge m5.xlarge m5n.xlarge	c5.2xlarge c5n.2xlarge c5d.2xlarge m5.2xlarge m5n.2xlarge
Tipi di istanze Azure supportate	Standard D2 v2 Standard_B2ms Standard_D2V4 Standard_D2ds_V4 Standard_D2s_v4	Standard D3 v2 Standard_B4ms Standard_DS3_v2 Standard_D2ds_V4	Standard D4 v2 Standard_A8_v2 Standard_F8 Standard_F8s Standard_D8_v4 Standard_D8_v3 Standard_D8s_v3
Licenze	BYOL, PAYG[1]		
vCPU max. supportate	2	4	8
Numero di interfacce (ESXi/Hyper-V/KVM/Nutanix/AWS/Azure)	8/8/8/8/8/8	8/8/8/8/8/8	8/8/8/8/8/8
Numero max. di nuclei di gestione/DataPlane	1/1	1/3	1/7
Memoria min.[2]	4 GB	8 GB	10 GB
Memoria max.[3]	6 GB	10 GB	14 GB
IP/nodi supportati	Illimitato		
Storage minimo	60 GB		
Utenti SSO	500	10000	15000
Logging	Analyzer, registro locale, Syslog		
Alta disponibilità	Attiva/passiva[4]		

Prestazioni firewall/VPN[5,7]	NSv 270	NSv 470	NSv 870
Throughput ispezione firewall	6 Gb/s	9 Gb/s	14 Gb/s
Throughput di prevenzione minacce	1,6 Gb/s	2,9 Gb/s	8 Gb/s
Throughput IPS	4 Gb/s	6 Gb/s	8 Gb/s
Throughput DPI TLS/SSL	800 Mb/s	2 Gb/s	4 Gb/s
Throughput VPN[8]	1,4 Gb/s	3,5 Gb/s	8 Gb/s
Connessioni al secondo	13760	37270	75640
Connessioni max. (SPI)	225000	1,5 milioni	3 mln.
Connessioni max. (DPI)	125000	1,5 milioni	2 milioni
Connessioni DPI TLS/SSL	8000	20000	30000
VPN	**NSv 270**	**NSv 470**	**NSv 870**
Tunnel VPN site-to-site	75	6000	10000
Client VPN IPSec[13] (max.)	50(1000)	2000(4000)	2000(6000)
Client VPN SSL inclusi[6]	2	2	2
Client VPN SSL (max.)[6]	100	200	300
Autenticazione/crittografia	DES, 3DES, AES (128, 192, 256 bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)		
Key exchange	Gruppi Diffie-Hellman 1, 2, 5, 14v		
VPN basata su route	RIP, OSPF, BGP		
Connettività di rete	**NSv 270**	**NSv 470**	**NSv 870**
Assegnazione indirizzo IP	Statico, DHCP, server DHCP interno[9], DHCP relay[9]		
Modalità NAT	1:1, many:1, 1:many, NAT flessibile (IP sovrapposti), PAT		
Interfacce VLAN logiche e tunnel (max.)[7]	128	128	128
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, 802.1p		
Autenticazione	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, database utenti interno, servizi Terminal, Citrix		
Database utenti locale	250	2500	3200

[1]PAYG è attualmente disponibile solo su AWS.

[2]Memoria con frame Jumbo disattivato.

[3]Memoria con frame Jumbo attivato. Per i frame Jumbo è richiesta memoria aggiuntiva. I frame Jumbo non sono supportati in Azure e AWS.

[4]L'alta disponibilità è disponibile sulla piattaforma VMware ESXi e su KVM, Azure, Microsoft Hyper-V e Nutanix. NSv 270 supporta l'alta disponibilità (HA) utilizzando la dimensione di VM D3v2. L'alta disponibilità non è supportata in AWS. L'alta disponibilità in Azure richiede dimensioni del server che supportino tre o più interfacce.

[5]Le prestazioni pubblicate sono conformi alle specifiche, le prestazioni effettive possono variare a seconda dell'hardware utilizzato, delle condizioni di rete, della configurazione del firewall e dei servizi attivati. Le prestazioni e le capacità possono anche variare in base all'infrastruttura di virtualizzazione sottostante, quindi consigliamo di effettuare ulteriori prove nel proprio ambiente per assicurarsi che i requisiti di prestazioni e capacità siano soddisfatti. I parametri di prestazioni sono stati osservati utilizzando un processore Intel Xeon W (W-2195 2,3 GHz, 4,3 GHz Turbo, 24,75 M di cache) su SonicOSv 6.5.0.2 con VMware vSphere 6.5.

[6]I client SSL VPN disponibili per il programma MSSP sono 50 su NSv 270 e 75 su NSv 470. Un maggior numero di VPN SSL sarà disponibile solo dal firmware SonicOS 6.5.4.4-44v-21-723 e successivi.

[7]Le interfacce VLAN non sono supportate in Azure e AWS. Metodologie di test: prestazioni massime come da RFC 2544 (per il firewall). Rilevazione throughput di prevenzione minacce/gateway AV/anti-spyware/IPS tramite strumenti di test delle performance Keysight HTTP standard nel settore. Il test viene eseguito con più flussi attraverso varie coppie di porte. Rilevazione throughput di prevenzione delle minacce con gateway AV, anti-spyware, IPS e Application Control attivati e impostazioni predefinite del firewall. Rilevazione throughput VPN con traffico UDP mediante pacchetti da 1418 byte, crittografia AESGMAC16-256 in conformità a RFC 2544. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.

[8]Tutti i parametri di prestazioni vengono testati utilizzando Dell R740 con SR-IOV e Turbo Boost.

[9]Supportato su piattaforme di cloud privato e non di cloud pubblico.

[10]Nutanix AHV è supportato su SonicWall NSv 270/470/870 con firmware SonicOSX 7.0.0 e successivi.

[11]Gli utenti di SonicOSX 7.0.1 e successivi potranno scegliere e commutare tra le modalità Classic/Global e Policy.

[12]Cloud governativo disponibile solo per client BYOL.

[13]I client GVC disponibili per il programma MSSP sono 25 su NSv 270 e 50 su NSv 470.

SONICWALL

Riepilogo delle funzioni di SonicOSX 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
- API REST
- Integrazione switch SonicWall[1]
- Integrazione AP SonicWall Wi-Fi 6
- Servizio di filtraggio dei contenuti (CFS 5.0) basato sulla reputazione
- Filtraggio degli DNS
- SD-WAN
  - Scalabilità SD-WAN
  - Procedura guidata di usabilità SD-WAN
- API
  - Supporto API completo
- Multi-tenancy[3]
  - Supporto multi-tenant
  - Visualizzazione tenant con supporto firmware per ogni tenant
- Commutazione tra le modalità Classic/Global e Policy[4]

Policy unificate

- La policy unificata abbina le regole dei livelli da 3 a 7:
  - IP/porta/servizio di origine/destinazione
  - Application Control
  - CFS/Web Botnet/Geo-IP
  - Diagramma regole
  - Applicazione servizi di sicurezza Single Pass - IPS/GAV/AS/Capture ATP
  - Oggetti basati su profili per la sicurezza degli endpoint/BWM/QoS/CFS/prevenzione intrusioni
- Profili di azione per regole di sicurezza/DoS
- Gestione delle regole:
  - Clonazione
  - Analisi di regole nascoste
  - Modifica nelle celle
  - Esportazione delle regole
  - Modifica di gruppi
- Gestione delle viste
  - Regole utilizzate/non utilizzate
  - Regole attive/inattive
  - Raggruppamento di sezioni/personalizzato
  - Griglia/layout personalizzabili

Decrittazione e ispezione TLS/SSL/SSH

- TLS1.3
- Supporto di TLS 1.3 con sicurezza migliorata
- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi di host
- Controllo SSL
- 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
- Integrazione del controllo accessi alla rete con Aruba ClearPass
- Aggiornamenti automatici delle firme
- Motore di ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Identificazione tramite GeoIP
- Filtraggio Botnet con elenco dinamico
- Corrispondenza con espressioni regolari

Anti-malware[2]

- Scansione antimalware 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 rapporti sulle applicazioni tramite NetFlow/IPFIX
- Ampio database di firme delle applicazioni

Visualizzazione e analisi del traffico

- Attività degli utenti
- Utilizzo 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
- Servizio di filtraggio dei contenuti (CFS 5.0) basato sulla reputazione
- Filtraggio degli DNS
- 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 una connettività Site-to-Site
- Accesso remoto tramite VPN SSL e client IPSec
- Gateway per la rete VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN basato su routing (RIP/OSPF/BGP)

Pannello di controllo ottimizzato

- Visualizzazione migliore dei dispositivi
- Riepilogo traffico e utenti principali
- Informazioni sulle minacce
- Centro notifiche
- Monitoraggio ottimizzato dei pacchetti
- Terminale SSH su interfaccia utente
- Progettazione/template di nuova concezione
- Confronti con la media di settore e globale

Connettività di rete

- PortShield[1]
- Frame Jumbo
- Indagine del percorso MTU
- Registrazione avanzata
- VLAN trunking
- Mirroring delle porte (NS*a* 2650 e successivi)
- QoS livello 2
- Sicurezza delle porte

SONICWALL

- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall[1]
- Routing basato su policy (ToS/metrico ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link[1] (statica e dinamica)
- Ridondanza delle porte[1]
- Alta disponibilità A/P con sincronizzazione dello stato
- Clustering A/A[1]
- Bilanciamento del carico in ingresso/in uscita
- Bridge L2,[1] modalità Wire/Virtual Wire, modalità Tap, modalità NAT
- Failover WAN 3G/4G[1]
- Routing asimmetrico
- Supporto CAC (Common Access Card)
- Containerizzazione SonicCoreX e SonicOS

Policy di decrittazione

- Policy unificate per il traffico SSL/TLS

Policy DoS

- Policy unificate per la prevenzione di attacchi DoS/DDoS

VoIP

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

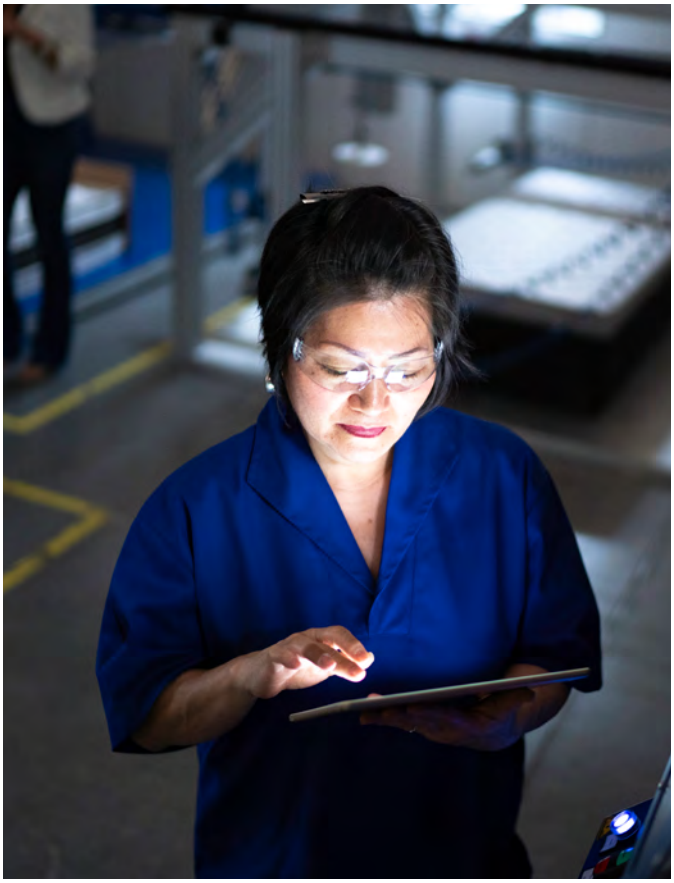
Gestione e monitoraggio

- GUI Web
- CLI (Command Line Interface)
- Registrazione e provisioning zero-touch
- Supporto app mobile SonicExpress
- SNMPv2/v3
- Gestione e reportistica centralizzate con Network Security Manager (NSM)[2]
- Logging
- Esportazione per Netflow/IPFix
- Backup della configurazione basato su cloud
- Visualizzazione della larghezza di banda e delle applicazioni
- Gestione IPv4 e IPv6
- Creazione immediata di rapporti (Scrutinizer)
- Display di gestione LCD[1]
- Gestione di switch N-Series e X-Series di Dell, inclusi gli switch a cascata[1]
- Reportistica per Network Security Manager

Wireless[1]

- Gestione firewall e AP 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
- Visualizzazione in pianta
- Visualizzazione della topologia
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy
- MiFi extender
- Quota ciclica ospite
- Portale ospite LHM

[1] Non supportato sui firewall della serie NS*v*
[2] Richiede un abbonamento aggiuntivo
[3] Disponibile solo sui firewall NSsp
[4] Disponibile su SonicOSX 7.0.1 e successivi



SERVIZI OFFERTI DAI PARTNER

Serve aiuto per pianificare, ottimizzare o installare una soluzione SonicWall? I SonicWall Advanced Services Partner sono qualificati per fornire servizi professionali di altissimo livello. Per maggiori informazioni:

www.sonicwall.com/PES

Maggiori informazioni sulle serie SonicWall NS*v* 270/470/870

www.sonicwall.com/NS*v*

SonicWall

SonicWall fornisce soluzioni di cybersecurity stabili, scalabili e trasparenti 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-NSv-270-470-870-JK-9963