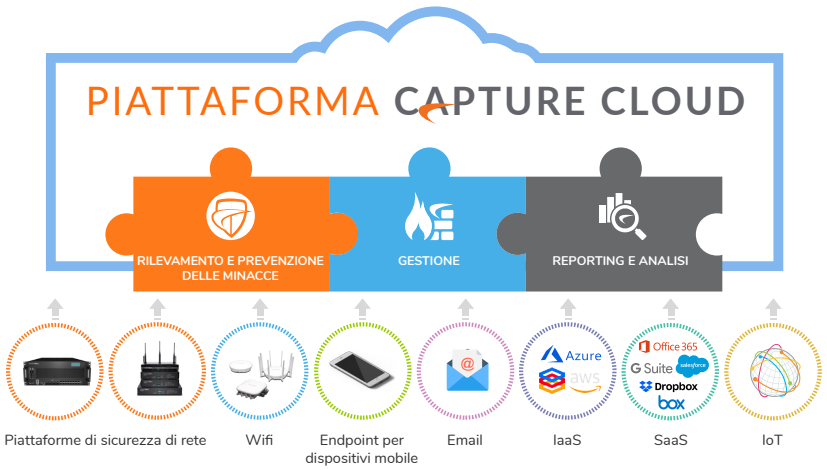
I firewall SonicWall della serie Network Security virtual (NSv)

La sicurezza di prossima generazione per ambienti cloud pubblici, privati o ibridi

La progettazione, la realizzazione e l'installazione delle moderne architetture di rete, come la virtualizzazione e il cloud, continuano ad essere una strategia in grado di cambiare i giochi per molte organizzazioni. La virtualizzazione dei data center, il passaggio al cloud, o la combinazione di queste due modalità, comportano vantaggi operativi ed economici significativi. Tuttavia, le vulnerabilità degli ambienti virtuali sono ampiamente documentate. Vengono inoltre scoperte regolarmente nuove vulnerabilità, che comportano serie implicazioni e gravi sfide da affrontare. Garantire che le applicazioni e i servizi vengano erogati in modo sicuro, efficace e modulare, senza abbassare la guardia nei confronti delle minacce ai danni di tutte le parti dell'infrastruttura virtuale, compresi macchine virtuali (VM), carichi di lavoro e dati delle applicazioni, rientra fra le priorità più importanti.

I firewall SonicWall della serie Network Security virtual (NSv) mettono i responsabili della sicurezza informatica in condizioni di ridurre i rischi e le vulnerabilità di questo tipo, che possono provocare gravi interruzioni dei servizi e delle attività aziendali essenziali.

I firewall virtuali NSv di prossima generazione integrano due tecnologie di sicurezza avanzate per la prevenzione all'avanguardia delle minacce e far sì che le reti siano sempre in anticipo rispetto ai tempi. La tecnologia di SonicWall, in attesa di brevetto, Real-Time Deep Memory Inspection (RTDMI™) migliora il nostro premiato servizio di sandboxing multi-engine Capture Advanced Threat Protection (ATP). L'engine RTDMI rileva e blocca in anticipo le minacce di massa, le minacce zero-day e i malware sconosciuti eseguendo ispezioni direttamente nella memoria. Grazie all'architettura in tempo reale, la tecnologia RTDMI è precisa, riduce al minimo i falsi positivi e identifica e attenua gli attacchi sofisticati durante i quali l'armamentario del malware resta esposto per meno di 100 nanosecondi. In abbinamento, viene utilizzato l'engine brevettato* RFDPI® (Reassembly-Free Deep Packet Inspection) a singola fase di SonicWall per esaminare i singoli byte di ogni pacchetto, ispezionando il traffico in entrata e in uscita sul firewall.



*Brevetti USA 7.310.815, 7.600.257, 7.738.380, 7.835.361, 7.991.723

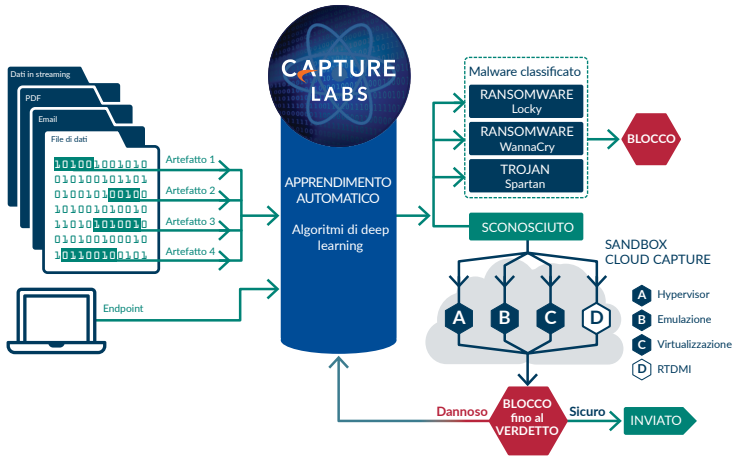
Vantaggi

Sicurezza cloud pubblica e privata

- Firewall di prossima generazione con funzioni automatiche di rilevamento e prevenzione delle violazioni in tempo reale
- Tecnologia RTDMI (Real-Time Deep Memory Inspection) in attesa di brevetto
- Tecnologia RFDPI (Reassembly-Free Deep Packet Inspection) brevettata
- Visibilità e controllo completi end-to-end
- Intelligenza e controllo delle applicazioni
- Sicurezza di segmentazione e suddivisione in zone di sicurezza
- Supporto piattaforme di cloud privato (ESXi, Hyper-V) e pubblico (AWS, Azure)
- Sistemi di licenza BYOL e PAYG

Protezione macchina virtuale

- Protezione minacce zero-day con Capture ATP
- Riservatezza dei dati
- Comunicazioni sicure con prevenzione della perdita di dati
- Validazione, ispezione e monitoraggio del traffico
- Sicurezza e integrità dei sistemi
- Resilienza e disponibilità delle reti virtuali



I firewall della serie NSv effettuano in automatico il rilevamento e la protezione automatici delle minacce in tempo reale di cui le organizzazioni hanno bisogno, utilizzando tecnologie di apprendimento profondo nella piattaforma SonicWall Capture Cloud. Questa piattaforma effettua la prevenzione delle minacce basata sul cloud e la gestione della rete e dispone inoltre di funzioni di reportistica e analisi per le organizzazioni di qualsiasi dimensione. La piattaforma consolida le informazioni sulle minacce raccolte da svariate fonti, tra cui il nostro Capture ATP, e da oltre un milione di sensori SonicWall dislocati in ogni parte del mondo. Sfruttando la piattaforma SonicWall Capture Cloud, in aggiunta a funzioni come la prevenzione delle intrusioni, l'antimalware e il filtraggio Web/URL, i firewall della serie NSv sono in grado di bloccare anche le minacce più nascoste in corrispondenza del gateway.

I firewall NSv sono di facile installazione e provisioning negli ambienti virtuali, in genere tra reti virtuali (VN) o cloud privati virtuali (VPC). Ciò consente di catturare le comunicazioni e gli scambi di dati tra macchine virtuali per la prevenzione automatica delle violazioni, istituendo al tempo stesso rigorose misure di controllo accessi per la riservatezza dei dati e l'integrità e la sicurezza delle macchine virtuali. Le minacce alla sicurezza (come gli attacchi tra macchine virtuali o su canale laterale, le intrusioni comuni provenienti dalla rete e le vulnerabilità delle applicazioni e dei protocolli) vengono neutralizzate con successo grazie alla suite completa di servizi di controllo di sicurezza di SonicWall[1]. Tutto il traffico delle macchine virtuali viene controllato attraverso engine di analisi delle minacce multiple, tra cui prevenzione delle intrusioni, antivirus e antispyware sul gateway, antivirus nel cloud, filtraggio botnet, controllo delle applicazioni e servizio di sandboxing multi-engine Capture ATP con tecnologia RTDMI.

Sicurezza tramite segmentazione

Per un'efficacia ottimale nei confronti delle minacce avanzate persistenti (APT) la segmentazione di sicurezza di rete deve utilizzare tutta una serie integrata di barriere dinamiche attivabili contro le minacce avanzate. Grazie alle funzioni di sicurezza basate sulla segmentazione, i firewall NSv possono raggruppare più interfacce dello stesso tipo ed applicarvi le stesse politiche, evitando di dover scrivere la stessa politica per ogni interfaccia. Applicando politiche di sicurezza all'interno della rete virtuale, la segmentazione può essere configurata in modo da organizzare le risorse di rete in diversi segmenti e consentire o vietare il traffico tra questi ultimi. In questo modo l'accesso alle risorse interne essenziali può essere controllato rigorosamente.

I firewall NSv applicano automaticamente le restrizioni di segmentazione sulla base di criteri dinamici, come le credenziali di identità dell'utente, la geolocalizzazione e il livello di sicurezza degli endpoint mobili. Per una maggiore sicurezza i firewall NSv sono anche in grado di integrare la funzione di switching di rete multi-gigabit nelle politiche e nell'attuazione del segmento di sicurezza. Questa funzione trasmette la politica del segmento al traffico nei punti di switching attraverso la rete e gestisce globalmente l'attuazione della sicurezza del segmento da un unico pannello di controllo.

Poiché i segmenti sono efficaci solo in ragione della sicurezza che può essere attuata tra loro, i firewall NSv utilizzano un sistema di prevenzione delle intrusioni (IPS) per la scansione del traffico in ingresso e in uscita sul segmento VLAN per migliorare la sicurezza del traffico di rete interno. Per ogni segmento questa funzione attiva tutta una serie di servizi di sicurezza su più interfacce in base alla politica attuabile.

Casistica d'impiego dell'installazione flessibile

Grazie al supporto infrastrutturale per le installazioni ad elevata disponibilità, i firewall NSv soddisfano i requisiti di modularità e disponibilità dei Software-Defined Data Center, garantendo in tal modo la resilienza del sistema, l'affidabilità del servizio e la conformità normativa. Ottimizzati per un'ampia casistica d'impiego per installazioni pubbliche, private e ibride, i firewall NSv possono adattarsi ai cambiamenti dei livelli di servizio e garantire la disponibilità e la sicurezza delle macchine virtuali, dei carichi di lavoro e dei dati delle loro applicazioni. Tutto ciò è possibile con velocità multi-Gbps e bassa latenza.

Le organizzazioni hanno a disposizione tutti i vantaggi in termini di sicurezza dei firewall fisici, oltre ai benefìci operativi ed economici della virtualizzazione, tra cui la modularità e la flessibilità operativa, la velocità di provisioning, la semplicità di gestione e la riduzione dei costi.

I firewall della serie NSv sono disponibili in diverse varianti virtuali opportunamente predisposte per un'ampia casistica di installazioni virtualizzate e nel cloud. Grazie alle funzioni di prevenzione delle minacce multi-gigabit e di ispezione del traffico crittografato, i firewall della serie NSv si adeguano agli aumenti dei livelli di capacità e garantiscono la sicurezza delle reti virtuali e dei cloud privati virtuali. Inoltre, garantiscono la disponibilità e la sicurezza dei carichi di lavoro e dei dati delle applicazioni.

Controllo centralizzato

Le installazioni dei firewall NSv possono essere gestite centralmente in loco con SonicWall Global Management System (GMS²) o con Capture Security Center², la piattaforma SonicWall aperta e modulare per la gestione della sicurezza del cloud, il monitoraggio, la reportistica e l'analisi, proposta con una formula as-a-service con un valido rapporto costi-benefìci.

Capture Security Center consente la massima visibilità, flessibilità e capacità per controllare l'intero ecosistema dei firewall SonicWall virtuali e fisici con maggiore chiarezza, precisione e velocità, il tutto da un unico pannello di controllo..

Politica unificata con SonicOSX 7.0

Il sistema operativo SonicWall SonicOSX a partire dalla versione 7.0 si contraddistingue per la funzione di politica unificata (Unified Policy) che consente la gestione integrata di diverse politiche di sicurezza nei firewall SonicWall in loco e virtuali, a partire dalla serie NSv.

CONTROLLO CENTRALIZZATO

- Stabilire un facile percorso per la gestione completa della sicurezza, il reporting analitico e la conformità per unificare i programmi di difesa per la sicurezza delle reti
- Automatizzare e correlare i flussi di lavoro per definire una strategia perfettamente coordinata di governance della sicurezza, conformità e gestione del rischio

CONFORMITÀ

- Soddisfare le esigenze degli enti normativi e di verifica per quanto riguarda i rapporti di sicurezza automatici PCI, HIPAA e SOX
- Personalizzare qualsiasi combinazione di dati di sicurezza verificabili per facilitare la conformità alle diverse normative applicabili

GESTIONE DEL RISCHIO

- Velocizzare e controllare la collaborazione, la comunicazione e la conoscenza nell'infrastruttura di sicurezza condivisa
- Adottare decisioni informate sulle politiche della sicurezza basate su informazioni sulle minacce per le quali il tempo è un fattore critico e consolidate per un maggiore livello di efficacia della sicurezza

GMS consente un approccio olistico alla governance della sicurezza, alla conformità e alla gestione dei rischi

È dotato di una nuova interfaccia web che si basa su un approccio completamente diverso basato su una concezione che mette l'utente in primo piano.

Consente la definizione di tutta una serie di politiche di sicurezza contestuali tramite avvisi azionabili e semplicità punta e clicca.

Dal punto di vista estetico, è molto più accattivante rispetto all'interfaccia classica. L'interfaccia, tramite la visualizzazione centralizzata del firewall, presenta all'utente le informazioni sull'efficacia delle diverse regole di sicurezza,

consentendo ad esso di modificare in modo uniforme le regole predefinite per le funzioni antivirus, antispyware, filtraggio dei contenuti, prevenzioni delle intrusioni, filtraggio della geolocalizzazione IP ed ispezione approfondita dei pacchetti del traffico crittografato del gateway.

Grazie alla funzione di politica unificata, SonicWall rende possibile una modalità operativa più razionale, che riduce gli errori di configurazione e i tempi d'installazione, a tutto vantaggio della sicurezza generale.

Formule di licenza flessibili.

I firewall NSv supportano le formule di licenza Bring Your Own License (BYOL) e Pay As You Go (PAYG). Le licenze BYOL per i firewall NSv possono essere acquistate direttamente presso SonicWall, i partner e i rivenditori. Le licenze PAYG si acquistano direttamente su AWS Marketplace. Si tratta di licenze basate sull'uso, con pagamento a tariffa oraria o annuale.

Funzioni

Piattaforma SonicOS
L'architettura SonicOS è al centro di tutti i firewall SonicWall fisici e virtuali, compresi quelli delle serie NSv e NSa, SuperMassive e TZ. Per l'elenco completo delle funzioni e delle caratteristiche consultare il datasheet della piattaforma SonicWall SonicOS.

Prevenzione automatica delle violazioni[1]
NSv garantisce la protezione avanzata completa contro le minacce, compresi un'efficace prevenzione delle intrusioni e del malware e il sandboxing basato su cloud con la tecnologia RDTMI di SonicWall.

Sicurezza 24 ore su 24[1]
NSv garantisce la protezione contro il movimento laterale, oltre a quella del traffico in ingresso e in uscita. Gli aggiornamenti sulle minacce vengono inviati automaticamente ai firewall con servizi di sicurezza attivi e sono immediatamente efficaci senza riavvii o interruzioni.

Protezione zero-day[1]
I firewall NSv proteggono la rete dagli attacchi zero-day, questa opzione assicura aggiornamenti costanti a fronte delle tecniche e dei metodi di exploit più recenti, coprendo migliaia di singoli exploit.

API per la gestione delle minacce
I firewall NSv ricevono e sfruttano tutti i feed di intelligence proprietari dei produttori di dispositivi originali e di terzi per contrastare minacce avanzate come zero-day, utenti malintenzionati, credenziali compromesse, ransomware e minacce persistenti avanzate.

Protezione per zone
NSv potenzia la sicurezza interna consentendo la segmentazione della rete in più zone di sicurezza, con un servizio di prevenzione dalle intrusioni che impedisce alle minacce di propagarsi tra le diverse zone. Definendo e applicando regole di accesso e politiche NAT al traffico che passa attraverso le diverse interfacce, è in grado di consentire o negare l'accesso alla rete interna o a quella esterna sulla base di diversi criteri.

Intelligenza e controllo delle applicazioni[1]
NSv effettua il controllo granulare del traffico di rete a livello di utente, di indirizzo di posta elettronica, di pianificazione e di maschera di sottorete IP, con politiche specifiche per le singole applicazioni. Controlla le applicazioni personalizzate, definendo segnature basate su parametri specifici o pattern esclusivi delle singole applicazioni. L'accesso alla rete interna o a quella esterna è consentito o negato sulla base di diversi criteri.

Prevenzione della perdita di dati
NSv consente di effettuare la scansione dei flussi di dati per parole chiave, limitando in tal modo il trasferimento di determinati nomi di file, tipi di file, allegati di posta elettronica, tipi di allegati, messaggi di posta elettronica con determinati oggetti e messaggi o allegati di posta elettronica con determinate parole chiave o determinati pattern di byte.

Gestione della larghezza di banda per i livelli delle applicazioni
NSv può scegliere tra diverse impostazioni di gestione della larghezza di banda per ridurre l'uso della stessa da parte delle applicazioni che utilizzano packet monitor. Ciò consente un ulteriore controllo della rete.

[1] *È necessario l'abbonamento a SonicWall Advanced Gateway Security Services (AGSS).*
[2] *Per SonicWall Global Management System e Capture Security Center sono necessari una licenza e un abbonamento appositi.*

Comunicazioni sicure
NSv garantisce che lo scambio di dati tra gruppi di macchine virtuali avvenga in condizioni di sicurezza, che prevedano isolamento, riservatezza, integrità e controllo del flusso di informazioni tra le reti ricorrendo alla segmentazione.

Controllo degli accessi
NSv verifica che solo le macchine virtuali che soddisfino determinate serie di condizioni siano in grado di accedere ai dati appartenenti a un'altra macchina virtuale, tramite VLAN.

Autenticazione degli utenti
NSv definisce politiche che controllino o limitino l'accesso alle macchine virtuali e al carico di lavoro da parte di utenti non autorizzati.

Riservatezza dei dati
NSv impedisce la sottrazione di informazioni e l'accesso illegittimo a dati e servizi protetti.

Resilienza e disponibilità delle reti virtuali
NSv impedisce l'interruzione e il degrado delle comunicazioni e dei servizi applicativi.

Sicurezza e integrità dei sistemi
NSv impedisce la sottrazione non autorizzata di sistemi e servizi della macchina virtuale.

Meccanismi di validazione, ispezione e monitoraggio del traffico
NSv rileva le irregolarità e i comportamenti dannosi per bloccare gli attacchi mirati ai carichi di lavoro delle macchine virtuali.

Opzioni di installazione
NSv può essere installato su una vasta gamma di piattaforme virtualizzate e cloud per diverse casistiche di sicurezza degli ambienti cloud pubblici e privati.

Modelli di licenza flessibili
SonicWall propone modelli di licenza permanenti o temporanei. Le licenze permanenti riguardano tipicamente i casi in cui le licenze per i firewall e i servizi di sicurezza devono essere acquistate separatamente e hanno di conseguenza scadenze diverse. Le licenze temporanee vengono utilizzate esclusivamente quando le licenze per i firewall e i servizi di sicurezza vengono acquistate assieme e scadono nello stesso momento.

Per l'installazione nei cloud pubblici sono disponibili licenze permanenti e temporanee secondo la formula Bring Your Own License (BYOL).

Sono disponibili modelli di licenza SonicWall temporanei o in abbonamento semplici e flessibili, sotto forma di pacchetti di software e servizi di sicurezza per i firewall relativi a un singolo SKU. Queste formule vengono offerte per i cloud privati (ESXi e Hyper-V) e quelli pubblici (AWS, Azure). La prossima scadenza del servizio viene comunicata in anticipo.

Sono disponibili tre formule di licenze temporanee - IPS/App Control Subscription, TotalSecure Subscription e TotalSecure Advanced Subscription - della durata di un anno. A seconda dei livelli di offerta, il software NSv viene fornito sotto forma di pacchetto con Intrusion Prevention System (IPS), controllo delle applicazioni, assistenza, Capture Security Center (CSC), Comprehensive Gateway Security Suite (CGSS) o Advanced Gateway Security Suite (AGSS).

Specifiche di sistema della serie NSv

CARATTERISTICHE GENERALI DEI FIREWALL	NSv 10	NSv 25	NSv 50	NSv 100
Sistema operativo	SonicOS[1]			
Hypervisor supportati	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2012 / 2016, KVM Ubuntu 16.04 / CentOS 7			
Piattaforme cloud pubbliche supportate (tipo di istanza)	AWS (c5.large), Azure (Std D2 v2)			
Licenze	BYOL, PAYG[2]			
Numero massimo di vCPU supportato	2	2	2	2
Conteggio interfacce (ESXi/Hyper-V/KVM)	8/8/8	8/8/8	8/8/8	8/8/8
Numero massimo di core Management Plane/ Data Plane	1/1	1/1	1/1	1/1
Dimensione minima memoria[3]	4 GB	4 GB	4 GB	4 GB
Dimensione massima memoria[4]	6 GB	6 GB	6 GB	6 GB
IP/Nodi supportati	10	25	50	100
Memoria fisica massima	60 GB			
Utenti SSO	25	50	100	100
Accesso	Analyzer, Local Log, Syslog			
Elevata disponibilità	Attiva/passiva			
PRESTAZIONI FIREWALL/VPN	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Velocità di ispezione del firewall	2 Gbps	2,5 Gbps	3 Gbps	3,5 Gbps
Piena velocità DPI (GAV/GAS/IPS)	450 Mbps	550 Mbps	650 Mbps	750 Mbps
Velocità di ispezione delle applicazioni	1 Gbps	1,25 Gbps	1,5 Gbps	1,75 Gbps
Velocità IPS	1 Gbps	1,25 Gbps	1,5 Gbps	1,75 Gbps
Velocità di ispezione anti-malware	450 Mbps	550 Mbps	650 Mbps	750 Mbps
Velocità IMIX	750 Mbps	850 Mbps	950 Mbps	1100 Mbps
Velocità DPI TLS/SSL	650 Mbps	750 Mbps	850 Mbps	950 Mbps
Velocità IPS	500 Mbps	550 Mbps	600 Mbps	650 Mbps
Connessioni al secondo	1.800	5.000	8.000	10.000
Numero massimo di connessioni (SPI)	2.500	6.250	12.500	25.000
Numero massimo di connessioni (DPI)	2.500	6.250	12.500	25.000
Connessioni DPI TLS/SSL	500	1.000	2.000	4.000
VPN	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Tunnel VPN da sede a sede	10	10	25	50
Client VPN IPSec	10 (10)	10 (10)	10 (25)	10 (25)
Client VPN SSL inclusi[7]	2	2	2	2
Client VPN SSL massimo[7]	50	50	50	50
Crittografia/autenticazione	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Scambio chiavi	Gruppi Diffie-Hellman 1, 2, 5, 14v			
VPN basato su routing	RIP, OSPF, BGP			
CONNETTIVITÀ DI RETE	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Assegnazione indirizzo IP	Statici, DHCP, server DHCP interno, relay DHCP			
Modalità NAT	1:1, many:1, 1:many, NAT flessibile (IP sovrapposti), PAT			
VLAN max	25	25	50	50
Protocolli di routing	BGP, OSPF, RIPv1/v2, static route, routing basato sulle politiche			
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 interno utente, Terminal Services, Citrix			
VoIP	SIP			
Standard	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			
Gruppi SD-WAN max	12	12	18	32
Membri SD-WAN max per prodotto	24	24	36	64

Specifiche di sistema della serie NSv (cont.)

CARATTERISTICHE GENERALI DEI FIREWALL	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Sistema operativo	SonicOS[1]				
Hypervisor supportati	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7				
Piattaforme cloud pubbliche supportate (tipo di istanza)	AWS (c5.large), Azure (Std D2 v2)	N/D	AWS (c5.xlarge), Azure (Std D3 v2)	AWS (c5.2xlarge), Azure (Std D4 v2)	AWS (c5.4xlarge), Azure (Std D5 v2)
Licenze	BYOL, PAYG[2]				
Numero massimo di vCPU supportato	2	3	4	8	16
Conteggio interfacce (ESXi/Hyper-V/KVM/ AWS/Azure)	8/8/8/2/2	8/8/8/-/-	8/8/8/4/4	8/8/8/8/8	8/8/8/8/8
Numero massimo di core Management Plane/Data Plane	1/1	1/2	1/3	1/7	1/15
Dimensione minima memoria[3]	6 GB	6 GB	8 GB	10 GB	12 GB
Dimensione massima memoria[4]	6 GB	8 GB	10 GB	14 GB	18 GB
IP/Nodi supportati	Illimitati	Illimitati	Illimitati	Illimitati	Illimitati
Memoria fisica massima	60 GB				
Utenti SSO	500	5.000	10.000	15.000	20.000
Accesso	Analyzer, Local Log, Syslog				
Elevata disponibilità	Attiva/passiva[5]				
PRESTAZIONI FIREWALL/VPN	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Velocità diispezione del firewall	4,1 Gbps	5,9 Gbps	7,8 Gbps	13,9 Gbps	17,2 GBPS
Piena velocità DPI (GAV/GAS/IPS)	900 Mbps	1,6 Gbps	2,2 Gbps	4,0 Gbps	6,4 Gbps
Velocità di ispezione delle applicazioni	2,3 Gbps	3,4 Gbps	4,1 Gbps	5,5 Gbps	6,4 Gbps
Velocità IPS	2,3 Gbps	3,4 Gbps	4,1 Gbps	5,5 Gbps	6,7 GBPS
Velocità di ispezione anti-malware	900 Mbps	1,6 Gbps	2,2 Gbps	4,0 Gbps	6,6 Gbps
Velocità IMIX	1,5 Gbps	2,3 Gbps	2,8 Gbps	4,2 Gbps	5,3 Gbps
Velocità DPI TLS/SSL	1,1 Gbps	1,2 Gbps	1,8 Gbps	3,4 Gbps	5,1 GBPS
Velocità IPS	750 Mbps	1,4 Gbps	1,9 Gbps	4,2 Gbps	8,4 Gbps
Connessioni al secondo	13.760	24.360	37.270	75.640	125.000
Numero massimo di connessioni (SPI)	225.000	1M	1,5M	3M	4M
Numero massimo di connessioni (DPI)	125.000	500.000	1,5M	2M	2,5M
Connessioni DPI TLS/SSL	8.000	12.000	20.000	30.000	50.000
VPN	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Tunnel VPN da sede a sede	75	100	6000	10.000	25.000
Client VPN IPSec (max)	50 (1000)	50 (1000)	2000 (4000)	2000 (6000)	2000 (10.000)
Client VPN SSL inclusi[7]	2	2	2	2	2
Client VPN SSL massimo[7]	100	150	200	300	400
Crittografia/autenticazione	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)				
Scambio chiavi	Gruppi Diffie-Hellman 1, 2, 5, 14v				
VPN basato su routing	RIP, OSPF, BGP				
CONNETTIVITÀ DI RETE	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Assegnazione indirizzo IP	Statici, DHCP, server DHCP interno, relay DHCP				
Modalità NAT	1:1, many:1, 1:many, NAT flessibile (IP sovrapposti), PAT				
VLAN max[8]	128	128	128	128	128
Protocolli di routing	BGP, OSPF, RIPv1/v2, static route, routing basato sulle politiche				
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 interno utente, Terminal Services, Citrix				
VoIP	SIP				
Standard	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				
Gruppi SD-WAN max	38	38	70	102	102
Membri SD-WAN max per prodotto	76	76	140	204	204

[1] *Attualmente supporta SonicOS 6.5.4.*
[2] *PAYG è attualmente disponibile solo su AWS.*
[3] *Memoria con Jumbo frame disabilitato.*
[4] *Memoria con Jumbo frame disabilitato. Ulteriore memoria necessaria per Jumbo frame. Jumbo frame non supportati su Azure e AWS.*
[5] *Elevata disponibilità disponibile su piattaforma VMware ESXi e Microsoft Hyper-V, plus HA non supportata su Azure e AWS.*
[6] *I dati pubblicati relativi alle prestazioni sono riferiti alle specifiche. Le prestazioni effettive possono essere diverse a seconda delle condizioni dell'hardware e della rete sottostanti, della configurazione del firewall e dei servizi attivati. Inoltre, le prestazioni e le caratteristiche possono essere diverse a seconda dell'infrastruttura di virtualizzazione sottostante e si consiglia di verificare il prodotto nell'ambiente specifico per garantire il rispetto delle prestazioni e delle caratteristiche richieste. Le prestazioni sono state verificate con processore Intel Xeon W (W-2195 2.3GHz, 4.3GHz Turbo, 24.75M Cache) e sistema operativo SonicOSv 6.5.0.2 con VMware vSphere 6.5.*
[7] *Un maggior numero di VPN SSL possibile solo a partire dal firmware SonicOS 6.5.4.4-44v-21-723.*
[8] *Interfacce VLAN non supportate su Azure e AWS.*
Metodologie di test: Prestazioni massime come da RFC 2544 (per il firewall). Rilevazione completa della velocità DPI/Gateway AV/Anti-Spyware/IPS effettuata con il test di performance Spirent WebAvalanche HTTP standard nell'industria e gli strumenti di test Ixia.
Il test viene eseguito con più flussi attraverso varie coppie di porte. Velocità VPN misurata considerando il traffico UDP con pacchetti di 1418 byte in base al valore RFC 2544. Tutte le specifiche e le caratteristiche sono soggette a modifiche.

Funzioni

ENGINE RFDPI

Funzione	Descrizione
Reassembly-Free Deep Packet Inspection (RFDPI)	Si tratta di un engine di ispezione proprietario, brevettato e di prestazioni elevate, che esegue analisi bidirezionali del traffico basate sui flussi senza proxy o buffering allo scopo di individuare tentativi di intrusione, rilevare malware e identificare il traffico delle applicazioni in qualsiasi porta.
Ispezione bidirezionale	Con la scansione contemporanea del traffico in ingresso e in uscita per il rilevamento delle minacce, questa opzione impedisce l'utilizzo della rete come vettore di malware e come piattaforma per sferrare attacchi qualora venga introdotto un computer infetto.
Ispezione basata sui flussi	La tecnologia di ispezione priva di proxy e buffering genera una latenza estremamente bassa per le attività di ispezione DPI su milioni di flussi di rete simultanei, senza limiti per la dimensione dei flussi e dei file. Inoltre può essere applicata sia a protocolli comuni, sia a flussi TCP primari.
Architettura altamente parallela e scalabile	L'esclusivo engine RFDPI basato su architettura multi-core consente un'elevata velocità di DPI e la creazione di nuove sessioni in tempi estremamente brevi, agevolando la gestione dei picchi di traffico in reti complesse.
Ispezione single-pass	Un'architettura DPI a passaggio singolo consente di rilevare contemporaneamente malware e intrusioni e identificare le applicazioni, riducendo notevolmente la latenza dell'ispezione DPI e correlando tutte le informazioni sulle minacce in un'unica architettura.

FIREWALL E CONNETTIVITÀ DI RETE

Funzione	Descrizione
API REST	Consentono al firewall di ricevere e sfruttare tutti i feed di intelligence proprietari dei produttori di dispositivi originali e di terzi per contrastare minacce avanzate come zero-day, utenti malintenzionati, credenziali compromesse, ransomware e minacce persistenti avanzate.
Ispezione Stateful Packet	Tutto il traffico della rete viene ispezionato, esaminato e reso conforme alle politiche di accesso del firewall.
Elevata disponibilità[1]	La serie NSv supporta la sincronizzazione di stato attiva/passiva (A/P).
Protezione da attacchi DDoS/DoS	La protezione da flood SYN offre una difesa contro gli attacchi DoS mediante tecnologie di blacklisting al layer 3 (SYN proxy) e al layer 2 (SYN). Inoltre, protegge da DoS/DDoS attraverso la protezione da flood UDP/ICMP e la limitazione della velocità di connessione.
Supporto IPv6	Il protocollo IPv6 (Internet Protocol versione 6) è in procinto di sostituire il protocollo IPv4. Con SonicOS, l'hardware supporta il filtraggio e le implementazioni in modalità Wire.
Opzioni di implementazione flessibili	La serie NSv può essere installata con le modalità tradizionali NAT, bridge Layer 2, Wire e Network Tap.
Bilanciamento del carico WAN	Bilancia il carico su più interfacce WAN con metodi basati sulle modalità round robin, percentuale o spill-over.
Qualità del servizio (QoS) avanzata	Garantisce l'integrità delle comunicazioni strategiche tramite tagging 802.1p e DSCP e rimappatura del traffico VoIP sulla rete.
Supporto proxy SIP	Blocca le chiamate di spam richiedendo che tutte le chiamate in entrata siano autorizzate e autenticate dal proxy SIP.
Autenticazione biometrica	Supporto dell'autenticazione per dispositivi mobili come il riconoscimento delle impronte digitali, che non può essere facilmente condivisa o duplicata, per autenticare in modo sicuro l'identità degli utenti che accedono alla rete.
Autenticazione aperta e social login	Consente agli utenti ospiti di utilizzare le loro credenziali da servizi di social network come Facebook, Twitter o Google+ per accedere a Internet e ad altri servizi come ospiti attraverso la rete wireless, la LAN o le zone DMZ di un host tramite autenticazione pass-through.

GESTIONE E REPORTISTICA

Funzione	Descrizione
Gestione basata sul cloud e in sede	La configurazione e la gestione delle apparecchiature SonicWall sono disponibili via cloud attraverso il SonicWall Capture Security Center e in sede tramite il SonicWall Global Management System (GMS).
Gestione avanzata con un unico dispositivo	Configurazione comoda e veloce tramite l'interfaccia web intuitiva, oltre a un'interfaccia CLI completa e al supporto per SNMPv2/3.
Report sul flusso delle applicazioni con IPFIX/ NetFlow	Le statistiche di traffico e i dati sull'uso delle applicazioni possono essere esportati tramite i protocolli IPFIX o NetFlow per il monitoraggio e la creazione di report in tempo reale e storici con strumenti come SonicWall Scrutinizer o altri che supportano IPFIX e NetFlow con estensioni.

RETE PRIVATA VIRTUALE (VPN)

Funzione	Descrizione
Provisioning automatico delle VPN	Semplifica l'installazione dei firewall in ambienti distribuiti complessi automatizzando il provisioning iniziale del gateway VPN da sito a sito tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività.
VPN IPSec per la connettività Site-to-Site	La rete VPN IPSec di prestazioni elevate consente di utilizzare la serie NSv come concentratore di VPN per migliaia di altri siti di grandi dimensioni, filiali e per chi lavora da casa.
Accesso remoto tramite VPN SSL o client IPSec	Sfruttando la tecnologia VPN SSL senza client o un client IPSec semplice da gestire, è possibile accedere in tutta semplicità a messaggi di posta elettronica, file, computer, siti intranet e applicazioni da un'ampia serie di piattaforme.

[1] *L'elevata disponibilità non è attualmente supportata su AWS e Azure*

SONICWALL®

Gateway per la rete VPN ridondante	Se si utilizzano più WAN, è possibile configurare una VPN principale e una secondaria per consentire failover e failback automatizzati e trasparenti per tutte le sessioni VPN.
VPN basato su routing	La possibilità di eseguire il routing dinamico tramite collegamenti VPN garantisce un'operatività continua anche in caso di guasto temporaneo al tunnel VPN, perché il traffico viene instradato senza interruzioni tra gli endpoint attraverso route alternative.

SENSIBILITÀ AL CONTESTO/AL CONTENUTO	
Funzione	**Descrizione**
Tracciamento delle attività degli utenti	Per consentire il tracciamento delle attività e l'identificazione degli utenti le tecnologie AD/LDAP/Citrix1/ Terminal Services1 SSO integrate si combinano con le informazioni esaustive ricavate dall'ispezione DPI.
GeoIP per l'identificazione del traffico da determinati paesi	Con questa opzione è possibile identificare e controllare il traffico di rete in ingresso o in uscita da determinati paesi. Lo scopo è proteggere dagli attacchi provenienti da origini note o sospette di attività pericolose o analizzare il traffico sospetto che ha origine nella rete. Possibilità di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associati a un indirizzo IP. Elimina il filtraggio non voluto degli indirizzi IP dovuto ad errata classificazione.
Filtro DPI con espressioni regolari	Questa opzione identifica e controlla i contenuti che attraversano la rete mediante la corrispondenza delle espressioni regolari per impedire perdite di dati. Consente di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associati a un indirizzo IP.

Servizi in abbonamento per la prevenzione delle violazioni

CAPTURE ADVANCED THREAT PROTECTION	
Funzione	**Descrizione**
Sandboxing multi-engine	La piattaforma sandbox multi-engine, che comprende l'emulazione completa del sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato, ne analizza il comportamento e fornisce visibilità completa sulle attività dannose.
Real-Time Deep Memory Inspection (RTDMI)	Questa tecnologia basata su cloud, in attesa di brevetto, rileva e blocca i malware che non evidenziano comportamenti dannosi e nascondono il loro armamentario tramite crittografia. Forzando il malware a scoprire il suo armamentario nella memoria, l'engine RTDMI rileva e blocca in anticipo le minacce generalizzate, quelle zero-day ed i malware sconosciuti.
Blocco fino al verdetto	Per impedire l'ingresso di file potenzialmente dannosi nella rete, i file inviati al cloud per l'analisi possono essere trattenuti al gateway finché non viene determinata la loro natura.
Analisi di un'ampia gamma di tipi e dimensioni di file	Supporta l'analisi di un'ampia gamma di tipi di file, sia individualmente, sia come gruppo, compresi programmi eseguibili (PE), DLL, PDF, documenti MS Office, archivi, JAR e APK, oltre a svariati sistemi operativi, tra cui Windows, Android, Mac OS X e ambienti multi-browser.
Rapida distribuzione delle firme	Quando un file è identificato come dannoso, viene immediatamente distribuita una firma ai firewall con abbonamento a SonicWall Capture ATP, ai database delle firme per Gateway Anti-Virus e IPS, nonché ai database di URL, IP e reputazione dei domini nel giro di 48 ore.
Capture Client	Capture Client è una piattaforma client unificata che presenta numerose funzioni di protezione dell'endpoint, tra cui quella avanzata contro i malware e supporto per la visibilità del traffico crittografato. La piattaforma sfrutta tecnologie di protezione su più livelli, reporting completo e applicazione della protezione degli endpoint.

PREVENZIONE DELLE MINACCE CRITTOGRAFATE	
Funzione	**Descrizione**
Decrittazione e ispezione TLS/SSL	Esegue la decrittazione e l'ispezione del traffico crittografato TLS/SSL in tempo reale, senza proxy, di malware, intrusioni e fughe di dati, e applica politiche di controllo di applicazioni, URL e contenuti per proteggere la rete dalle minacce nascoste nel traffico crittografato. Opzione compresa negli abbonamenti di sicurezza per tutti i modelli della serie NSv.
Ispezione SSH	La Deep Packet Inspection di SSH (DPI-SSH) esegue la decrittazione e l'ispezione dei dati che attraversano il tunnel SSH per prevenire gli attacchi che sfruttano SSH.

PREVENZIONE DELLE INTRUSIONI	
Funzione	**Descrizione**
Protezione basata su contromisure	Il sistema di prevenzione delle intrusioni (IPS) integrato utilizza le firme e altre contromisure per eseguire la scansione dei payload dei pacchetti in cerca di exploit e vulnerabilità, coprendo un'ampia serie di vulnerabilità e attacchi.
Aggiornamenti automatici delle firme	Il team del SonicWall Threat Research ricerca continuamente nuovi aggiornamenti e li installa in numerose contromisure IPS, che interessano oltre 50 categorie di attacchi. Gli aggiornamenti sono subito attivi senza la necessità di riavvii o interruzioni del servizio.
Protezione IPS interna alle zone	La segmentazione della rete in varie zone di sicurezza, protette dalle intrusioni, consente di potenziare la sicurezza interna poiché impedisce alle minacce di propagarsi oltre i confini di una zona.
Rilevamento e blocco di comando e controllo Botnet (CnC)	Questa opzione consente di individuare e bloccare il traffico di comando e controllo proveniente dai bot nella rete locale e diretto ai domini e agli indirizzi IP che sono stati identificati come fonte di propagazione di malware o punti CnC noti.
Anomalia/abuso di protocolli	Individua e blocca gli attacchi che sfruttano i protocolli noti per tentare di eludere il controllo IPS.

Protezione zero-day	Per proteggere la rete dagli attacchi zero-day, questa opzione assicura aggiornamenti costanti a fronte delle tecniche e dei metodi di exploit più recenti, coprendo migliaia di singoli exploit.
Tecnologia antievasione	La normalizzazione estesa dei flussi, la decodifica e altre tecniche assicurano che le minacce basate su tecniche di evasione ai livelli 2-7 non possano entrare in rete senza essere rilevate.

PREVENZIONE DELLE MINACCE

Funzione	Descrizione
Antimalware a livello gateway	L'engine RFDPI sottopone a scansione tutto il traffico in ingresso, in uscita e interno alle zone in cerca di virus, trojan, keylogger e altri malware, interessando file di dimensioni e lunghezza illimitati in tutte le porte e in tutti i flussi TCP.
Protezione Capture Cloud contro il malware	Un database residente sui server cloud SonicWall, costantemente aggiornato con decine di milioni di firme delle minacce, viene consultato per ottimizzare le capacità del database di firme integrato nel dispositivo, garantendo così un'ampia copertura delle minacce da parte dell'engine RFDPI.
Aggiornamenti di sicurezza costanti	I nuovi aggiornamenti sulle minacce vengono inviati automaticamente ai firewall sul campo con servizi di sicurezza attivi e sono subito attivi senza riavvii o interruzioni.
Ispezione bidirezionale dei TCP primari	L'engine RFDPI è in grado di scansionare flussi TCP primari in entrambe le direzioni su qualsiasi porta, bloccando gli attacchi che tentano di passare attraverso sistemi di sicurezza obsoleti, concepiti per proteggere solo poche porte note.
Ampio supporto di protocolli	Oltre a identificare i protocolli più comuni come HTTP/S, FTP, SMTP, SMBv1/v2 e altri, che non inviano dati nel TCP primario, questa opzione consente di decodificare i payload in cerca di malware, anche se non sono eseguiti in porte standard note.

INTELLIGENZA E CONTROLLO DELLE APPLICAZIONI

Funzione	Descrizione
Controllo delle applicazioni	Per potenziare la sicurezza e la produttività della rete vengono controllate le applicazioni, o le singole funzioni delle stesse, identificate dall'engine RFDPI utilizzando un database in continua espansione, contenente migliaia di firme di applicazioni.
Identificazione di applicazioni personalizzate	Controlla le applicazioni personalizzate generando firme basate su parametri specifici o su modelli di comunicazione in rete univoci per ogni applicazione, in modo da garantire un maggiore controllo sulla rete.
Gestione della larghezza di banda delle applicazioni	Il traffico delle applicazioni superflue viene bloccato, mentre la larghezza di banda disponibile viene regolamentata e allocata in modo granulare per le applicazioni o le categorie di applicazioni più importanti.
Controllo granulare	Consente di controllare le applicazioni o i componenti specifici di un'applicazione in base a pianificazioni, gruppi di utenti, elenchi di esclusione e una serie di attività con identificazione SSO degli utenti completa, mediante l'integrazione di LDAP/AD/Terminal Services/Citrix.

FILTRAGGIO DEI CONTENUTI

Funzione	Descrizione
Filtraggio dei contenuti interno/esterno	Mette in atto le politiche di utilizzo accettabili e blocca l'accesso a siti web HTTP/HTTPS contenenti informazioni o immagini discutibili o non produttive con Content Filtering Service e Content Filtering Client.
Enforced Content Filtering Client	Estende l'applicazione delle politiche per bloccare i contenuti Internet per dispositivi Windows, Mac OS, Android e Chrome situati all'esterno del perimetro del firewall.
Controlli granulari	L'uso di categorie predefinite o di una combinazione qualsiasi di categorie consente di bloccare determinati contenuti. Il filtraggio può essere pianificato in base all'ora del giorno, ad esempio durante l'orario scolastico o lavorativo, e applicato a gruppi o singoli utenti.
Cache Web	Le classificazioni degli URL sono memorizzate nella cache locale del firewall SonicWall, in modo che il tempo di risposta per l'accesso successivo ai siti web visitati con maggior frequenza sia inferiore a un secondo.

ANTIVIRUS E ANTISPYWARE APPLICATI

Funzione	Descrizione
Protezione su più livelli	Utilizza le funzioni del firewall come primo livello di difesa perimetrale, insieme alla protezione degli endpoint, per bloccare i virus che entrano nella rete tramite laptop, chiavette USB e altri sistemi non protetti.
Opzione di applicazione automatizzata	Assicura che ogni computer che accede alla rete abbia installato e attivato il software antivirus appropriato e/o il certificato DPI-SSL, eliminando i costi comunemente associati alla gestione dell'antivirus desktop.
Distribuzione e installazione automatizzate	La distribuzione e l'installazione macchina per macchina dei client antivirus e antispyware sono automatizzate sull'intera rete, il che riduce al minimo l'impegno amministrativo.
Antivirus di nuova generazione	Capture Client utilizza un engine statico di intelligenza artificiale (AI) per determinare le minacce prima che possano essere eseguite e per ripristinare uno stato precedente non infetto.
Protezione antispyware	La potente protezione contro gli spyware garantisce il massimo livello di prestazioni e sicurezza analizzando e bloccando i programmi spyware più diffusi e pericolosi, prima che questi possano carpire dati sensibili da computer fissi o portatili.

Riepilogo delle funzioni di SonicOS

Controllo globale

- Controllo centralizzato della visibilità IPv6
- Disattivazione a livello globale dell'elaborazione del traffico IPv6
- Disattivazione delle politiche VPN predefinite, delle schermate di configurazione e delle regole autogenerate

Sicurezza accessi e utenti

- Blocco utente basato sui tentativi di accesso da parte di un intervallo di indirizzi IP
- Blocco utente dalla CLI
- Forzatura variazione password al primo accesso
- Supporto autenticazione a due fattori (TOTP)
- Supporto portale zero-touch politiche utente ospite
- Supporto IPv6 servizio ospite
- Supporto contabilità TACACS+
- Controllo quota per tutti gli utenti
- Autenticazione HTTP botnet dinamico

Reti e sistema

- Supporto SD-WAN
- Supporto sicurezza SicurDNS / supporto sinkhole DNS
- FQDN su DNS TCP
- Oggetti indirizzo FQDN per NAT
- Relay DHCPv6
- Modalità indirizzo IPv6 per VoIP application layer gateway H.323
- Supporto core Multiple control plane (CP)
- Reindirizzamento HTTP/HTTPS con data plane offload
- Offload dell'IP helper sul data plane
- Backup del firmware su memoria locale
- Crittografia ad elevata disponibilità
- Supporto upload firmware ad elevata disponibilità
- Ottimizzazione del routing dei percorsi statici e dinamici basata sulle politiche
- Miglioramenti delle prestazioni e della velocità
- Funzione watchdog per il monitoraggio dello stato del firewall
- Modularità migliorata per routing avanzato su interfacce tunnel VPN numerate
- Aggiornamento librerie H.323 basato su compilatore ASN.1 OSS Noklava v10.5.0
- Aggiornamenti prioritari task thread
- SSLVPN e bookmark su Data Plane

Servizi di sicurezza

- Blocco Capture ATP fino al controllo granulare dei verdetti
- Visualizzazione semplificata dei nomi file di Capture ATP per protocolli non-HTTP
- Blocco CFS di singoli video YouTube
- Supporto filtraggio cumulativo contenuti HTTPS e DPI-SSL
- Attivazione DPI-SSL e anti-virus (SentinelOne) di prossima generazione
- Miglioramento delle prestazioni della protezione Wan DDOS

Politiche e oggetti

- Miglioramenti delle regole d'accesso
- Routing basato sulle applicazioni
- Oggetti indirizzi dinamici
- Esclusione politiche CFS
- Oggetti filtraggio contenuti HTTPS basato sulle politiche
- Supporto gruppi elenchi URI negli oggetti di filtraggio contenuti
- Inserimento header CFS personalizzati per richieste HTTP
- UUID per regole e oggetti
- UUID per politiche CFS
- Forzatura MAC source per politiche NAT

DPI-SSL e DPI-SSH

- Cloud dinamico DPI-SSL basato su white list
- Bloccaggio DPI-SSH del forwarding delle porte SSH
- Bloccaggio DPI-SSH del forwarding X11
- Preservazione porte decrittazione SSL in packet mirror / packet capture
- Controllo granulare DPI-SSL basato sulle zone
- Regole d'accesso basate su controllo DPI-SSL
- Blocco o autorizzazione certificati CA scaduti per client DPI-SSL
- Estensione richiesta stato certificati TLS
- Supporto per CRL locale
- Verifica avanzata certificati DPI-SSL
- Supporto per cifrari relativi a ECDSA
- Supporto release LTS OpenSSL per certificazioni federali

Registrazione, monitoraggio e reportistica

- Possibilità di verificare che la DPI è stata eseguita su un pacchetto specifico
- Registrazione nome file e URI per controllo applicazioni
- Registrazioni di accesso visualizzate per l'amministratore
- Verifiche di configurazione
- Registrazione mappatura NAT per connessioni TCP
- Supporto FTP per automazione log
- Supporto reportistica e analisi Capture Security Center (CSC) per NSv
- Registrazione Capture ATP di mittente/destinatario email
- Miglioramenti client di verifica Capture threat (SWARM v3)
- Funzione di ripristino dei dati statistici SFR (SWARM)
- Opzione di scelta del linguaggio di output per report SonicFlow

API

- API SonicOS fase 1
- Supporto autenticazione API SonicOS
- API SonicOS fase 2
- API LHM RESTful

Interfaccia utente per la gestione di SonicOS da web

- Ricerca globale SonicOS
- Miglioramenti utilizzabilità per pagine di contenuti
- Memorizzazione preferenze interfaccia utente lato client utente
- Pin friendly name per schermate di gestione SonicOS da web
- Refactoring del layout dell'interfaccia web di SonicOS

Informazioni per l'ordinazione della serie NSv

PRODOTTO	ESXI SKU	HYPER-V SKU	AZURE SKU	AWS SKU	KVM SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition (1-year)	01-SSC-5875	02-SSC-1387	02-SSC-3426	02-SSC-3452	02-SSC-3494
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition (1-year)	01-SSC-5923	02-SSC-1395	02-SSC-3454	02-SSC-3464	02-SSC-3497
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition (1-year)	01-SSC-5926	02-SSC-1399	02-SSC-3470	02-SSC-3474	02-SSC-3504
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition (1 anno)	01-SSC-5929	02-SSC-1405	02-SSC-3480	02-SSC-3489	02-SSC-3513
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition (1 anno)	01-SSC-5950	02-SSC-1412	02-SSC-0868	02-SSC-0906	02-SSC-3519
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition (1-year)	01-SSC-5964	02-SSC-1420	—	—	02-SSC-3526
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition (1-year)	01-SSC-6084	02-SSC-1427	02-SSC-0888	02-SSC-0912	02-SSC-3531
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition (1-year)	01-SSC-6101	02-SSC-1429	02-SSC-0889	02-SSC-0914	02-SSC-3533
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition (1-year)	01-SSC-6109	02-SSC-1436	02-SSC-0895	02-SSC-0921	02-SSC-3540
PRODOTTO	ESXI SKU	HYPER-V SKU	AZURE SKU	AWS SKU	KVM SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition (3-year)	01-SSC-5873	02-SSC-1386	02-SSC-3427	02-SSC-3453	02-SSC-3491
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition (3-year)	01-SSC-5890	02-SSC-1397	02-SSC-3457	02-SSC-3465	02-SSC-3498
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition (3-year)	01-SSC-5924	02-SSC-1398	02-SSC-3471	02-SSC-3472	02-SSC-3505
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition (3-year)	01-SSC-5928	02-SSC-1404	02-SSC-3478	02-SSC-3486	02-SSC-3514
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition (3-year)	01-SSC-5951	02-SSC-1411	02-SSC-0866	02-SSC-0903	02-SSC-3515
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition (3-year)	01-SSC-5965	02-SSC-1419	—	—	02-SSC-3523
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition (3-year)	01-SSC-6089	02-SSC-1426	02-SSC-0887	02-SSC-0911	02-SSC-3527
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition (3-year)	01-SSC-6102	02-SSC-1428	02-SSC-0891	02-SSC-0913	02-SSC-3538
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition (3-year)	01-SSC-6108	02-SSC-1435	02-SSC-0897	02-SSC-0920	02-SSC-3542

**Per l'elenco completo degli SKU rivolgersi al rivenditore locale SonicWall di fiducia*

SonicWall

SonicWall fornisce soluzioni di cibersicurezza illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune di cibersicurezza per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare il sito www.sonicwall.com.

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

Datasheet-2473-NSvVirtualFirewalls-US-COG-2473