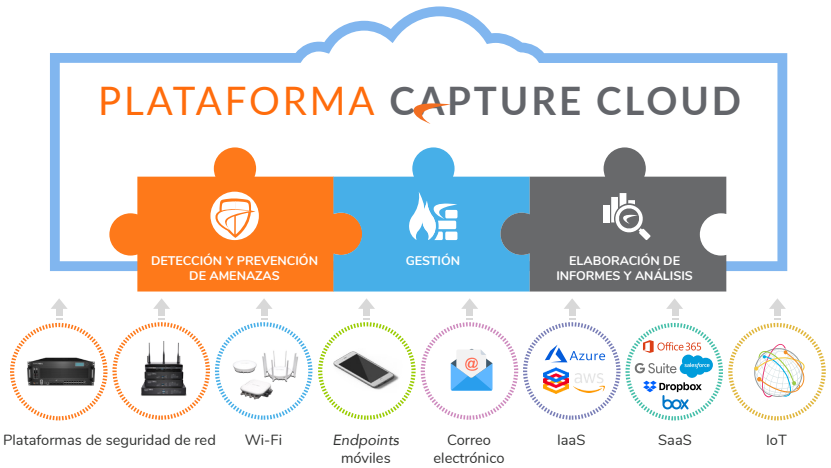
SONICWALL

Firewalls Virtuales (NSv) de SonicWall

Firewalls virtuales de última generación para entornos de nube públicos, privados o híbridos

El diseño, la implementación y el despliegue de arquitecturas de red modernas, como la virtualización y la nube, siguen siendo una estrategia innovadora para muchas organizaciones. La virtualización del centro de datos, la migración a la nube, o una combinación de ambas, ofrece importantes ventajas operativas y económicas. Sin embargo, las vulnerabilidades de los entornos virtuales están bien documentadas. Periódicamente se descubren nuevas vulnerabilidades que generan importantes implicaciones y desafíos de seguridad. A fin de garantizar que las aplicaciones y los servicios se ofrezcan de forma segura, eficiente y escalable, además de seguir combatiendo las amenazas dañinas para todas las partes del entorno virtual como las máquinas virtuales (VM), las cargas de trabajo de las aplicaciones y los datos deben figurar entre las principales prioridades.

Los Firewalls virtuales (NSv) de SonicWall ayudan a los equipos de seguridad a reducir estos tipos de riesgos y vulnerabilidades de seguridad, que pueden ocasionar graves interrupciones en sus operaciones y servicios críticos para el negocio. Los firewalls virtuales de última generación NSv integran dos tecnologías de seguridad avanzadas para proporcionar funciones innovadoras de prevención de amenazas que mantienen su red un paso por delante. La tecnología pendiente de patente Real-Time Deep Memory Inspection (RTDMI™) de SonicWall mejora nuestro galardonado servicio de *sandboxing* multimotor Capture Advanced Threat Protection (ATP). El motor RTDMI detecta y bloquea de forma proactiva las amenazas de día cero y el *malware* desconocido inspeccionando directamente la memoria. Gracias a la arquitectura en tiempo real, la tecnología SonicWall RTDMI es precisa, minimiza los falsos positivos e identifica y reduce los ataques sofisticados en los que el malware se manifiesta, actuando en menos de 100 nanosegundos. En combinación con ella, el motor patentado* de Inspección profunda de paquetes sin reensamblado (Reassembly-Free Deep Packet Inspection, RFDPI®) de paso único de SonicWall examina cada byte de cada paquete, inspeccionando el tráfico entrante y saliente en el firewall.



* Patentes estadounidenses 7.310.815; 7.600.257; 7.738.380; 7.835.361; 7.991.723

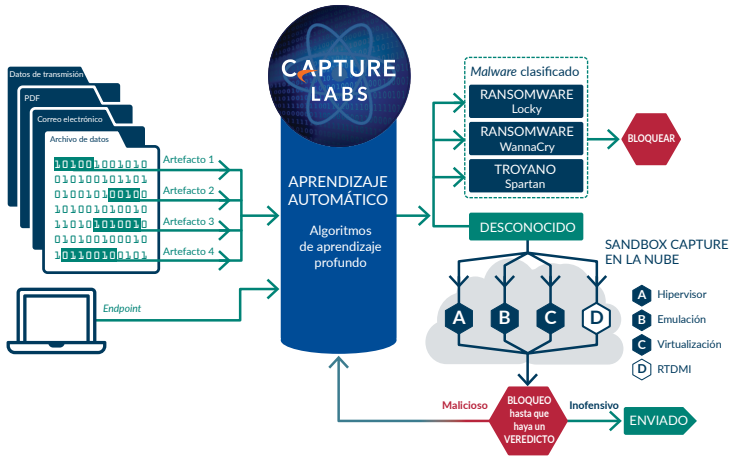
Ventajas

Seguridad en la nube pública y privada

- Firewall de última generación con detección automatizada de violaciones en tiempo real y funciones de prevención
- Tecnología de Inspección profunda de memoria en tiempo real (RTDMI) pendiente de patente
- Tecnología patentada de Inspección profunda de paquetes sin reensamblado (RFDPI)
- Visibilidad y control integral
- Inteligencia y control de aplicaciones
- Seguridad de segmentación y zonificación de seguridad
- Soporte para plataformas de nube privada (ESXi e Hyper-V) y de nube pública (AWS, Azure).
- Licencias BYOL y PAYG

Protección de máquinas virtuales

- Protección contra amenazas de día cero con Capture ATP
- Confidencialidad de los datos
- Comunicación segura con prevención de filtración de datos
- Validación, inspección y control del tráfico
- Seguridad e integridad del sistema
- Resiliencia y disponibilidad de las redes virtuales



La serie NSv ofrece la detección y prevención automatizadas de infracciones en tiempo real que las organizaciones necesitan utilizando innovadoras tecnologías de aprendizaje profundo en la plataforma Capture Cloud de SonicWall. Esta plataforma proporciona funciones de prevención de amenazas y gestión de red basadas en la nube, así como informes y análisis, para organizaciones de cualquier tamaño. Esta plataforma consolida la inteligencia de amenazas recopilada de diversas fuentes, incluido nuestro Capture ATP, así como más de 1 millón de sensores de SonicWall situados en todo el mundo. Al utilizar la plataforma Capture Cloud de SonicWall junto con prestaciones como prevención de intrusiones, *antimalware* y filtrado Web/URL, la serie NSv bloquea incluso las amenazas más sigilosas en la puerta de enlace.

NSv es fácil de implementar y suministrar en un entorno virtual, normalmente entre redes virtuales (VN) o nubes privadas virtuales (VPC). Esto le permite capturar las comunicaciones y los intercambios de datos entre máquinas virtuales para la prevención automatizada de violaciones, al tiempo que establece estrictas medidas de control de acceso para mantener la confidencialidad de los datos y la seguridad y la integridad de la VM. Las amenazas de seguridad (como los ataques entre máquinas virtuales o de canal lateral, las intrusiones comunes basadas en la red y las vulnerabilidades de aplicaciones y protocolos) se neutralizan con éxito gracias al paquete integral de servicios de inspección de seguridad de SonicWall[1]. Todo el tráfico de la VM se somete a múltiples motores de análisis de amenazas, como prevención de intrusiones, antivirus para puertas de enlace y antispyware, antivirus para la nube, filtrado de *botnets*, control de aplicaciones y *sandboxing* multimotor Capture ATP con tecnología RTDMI.

Seguridad de segmentación

Para lograr la máxima eficacia frente a las amenazas persistentes avanzadas, la segmentación de seguridad de la red debe aplicar un conjunto integrado de barreras dinámicas y ejecutables a las amenazas avanzadas. Con las funciones de seguridad basada en segmentos, NSv puede agrupar interfaces similares y aplicarles las mismas políticas, en vez de tener que programar la misma política para cada interfaz. Al aplicar políticas de seguridad en el interior de la VN, la segmentación se puede configurar para organizar los recursos de la red en diferentes segmentos y permitir o restringir el tráfico entre esos segmentos. De esta manera, se puede realizar un estricto control del acceso a los recursos internos críticos.

NSv aplica automáticamente restricciones de segmentación basadas en criterios dinámicos, como las credenciales de identidad del usuario, la localización geo-IP y el nivel de seguridad de los *endpoints* móviles. Para lograr una mayor seguridad, NSv también puede integrar conmutación de red multigigabit en su política de segmentos de seguridad y su aplicación. Esto dirige la política de segmentos al tráfico en los puntos de conmutación de toda la red y gestiona a nivel global la aplicación de la seguridad en el segmento desde un único panel.

Dado que los segmentos solo son tan efectivos como lo sea la seguridad que se puede aplicar entre ellos, NSv aplica un sistema de prevención de intrusiones (IPS) para analizar el tráfico entrante y saliente en el segmento VLAN a fin de mejorar la seguridad para el tráfico de red interno. Para cada segmento, aplica una gama completa de servicios de seguridad en múltiples interfaces basados en la política aplicable.

Casos de uso de implementación flexible

Con soporte de infraestructura para la implementación de alta disponibilidad, NSv cumple los requisitos de escalabilidad y disponibilidad de los centros de datos definidos por software. Garantiza la resiliencia del sistema, la fiabilidad del servicio y el cumplimiento normativo. Optimizado para una amplia gama de casos de uso de implementación pública, privada e híbrida, NSv puede adaptarse a los cambios de nivel de servicio y garantiza que las VM y sus cargas de trabajo de aplicaciones y activos de datos estén disponibles y seguros. Todo esto puede hacerlo a una velocidad de multiGbps con baja latencia.

Las organizaciones obtienen todas las ventajas de seguridad de un firewall físico, con los beneficios operativos y económicos de la virtualización. Esto incluye escalabilidad del sistema, agilidad de las operaciones, velocidad de aprovisionamiento, gestión sencilla y reducción de costes.

La serie NSv está disponible en múltiples versiones virtuales cuidadosamente ofertadas para una amplia gama de casos de uso de implementación virtualizada y en la nube. Al ofrecer funciones de prevención de amenazas multigigabit e inspección del tráfico cifrado, la serie NSv se adapta a los aumentos de nivel de capacidad y garantiza la seguridad de la VN y la VPC. La serie también garantiza la disponibilidad y la seguridad de las cargas de trabajo de las aplicaciones y los activos de datos.

Control central

Las implementaciones de NSv se pueden gestionar a nivel central bien en las instalaciones con Global Management System (GMS²) de SonicWall o con Capture Security Center², la plataforma abierta y escalable de gestión de la seguridad, monitorización, informes y análisis en la nube de SonicWall que se suministra a modo de oferta como servicio por un precio económico.

Capture Security Center proporciona lo último en visibilidad, agilidad y capacidad para controlar todo el ecosistema de firewalls virtuales y físicos de SonicWall con mayor claridad, precisión y velocidad, todo desde un único panel.

Motor de políticas unificadas con SonicOS 7

El Motor de políticas unificadas de SonicWall ofrece gestión integrada de varias políticas de seguridad en los firewalls virtuales y físicos de SonicWall, a partir de la serie NSv.

CONTROL CENTRAL

- Establezca una vía fácil para la gestión integral de la seguridad, informes analíticos y cumplimiento normativo con el objetivo de unificar su programa de defensa de seguridad de red
- Automatice y correlacione los flujos de trabajo para crear una estrategia de administración de la seguridad, cumplimiento normativo y gestión de riesgos plenamente coordinada.

CUMPLIMIENTO

- Cree informes de seguridad automáticos de PCI, HIPAA y SOX conforme a los requisitos exigidos por los organismos reguladores y los auditores
- Personalice cualquier combinación de datos de seguridad auditables para ayudarle a cumplir normativas específicas

GESTIÓN DE RIESGOS

- Actúe rápidamente e impulse la colaboración, la comunicación y el conocimiento en todo el marco de seguridad compartido
- Adopte decisiones informadas sobre políticas de seguridad basadas en información unificada sobre amenazas en las que el tiempo es crucial para lograr un nivel más alto de eficiencia de seguridad

GMS ofrece un enfoque integral del control de la seguridad, el cumplimiento y la gestión de riesgos

El motor cuenta con una nueva interfaz web que soporta un enfoque totalmente diferente: se hace énfasis en el diseño pensando primero en el usuario.

Esto se traduce en una configuración intuitiva de las políticas de seguridad contextuales a través de alertas configurables y con la sencillez de tan solo hacer clic.

Visualmente, también es más atractiva que la interfaz clásica. En una vista de panel único de firewall, la interfaz presenta al usuario información sobre la efectividad de las diferentes reglas de seguridad.

Esto permite al usuario modificar las reglas predefinidas para antivirus de puerta de enlace, antispyware, filtrado de contenido, prevención de intrusiones, filtrado de geo-IP e inspección profunda de paquetes del tráfico cifrado sin contratiempos.

Con el Motor de políticas unificadas, SonicWall ofrece una experiencia más optimizada que reduce los errores de configuración y el tiempo de implementación para lograr una mejor posición general de seguridad.

Licencias flexibles

NSv admite licencias Bring Your Own License (BYOL) y Pay As You Go (PAYG). La licencia BYOL para NSv se puede adquirir directamente a través de SonicWall, un *partner* o un distribuidor. Mientras que la licencia PAYG se adquiere directamente en AWS Marketplace. Este tipo de licencia es una licencia basada en el uso en la que el pago se realiza según el uso por hora o año.

Prestaciones

Plataforma SonicOS
La arquitectura SonicOS constituye el núcleo de todos los firewalls físicos y virtuales de SonicWall, incluidas las series NSv y NSa, la serie SuperMassive y la serie TZ. Consulte la ficha técnica de la Plataforma SonicOS de SonicWall para conocer la lista completa de prestaciones y funciones.

Prevención automatizada de violaciones[1]
NSv ofrece protección avanzada completa contra amenazas, incluida la prevención de intrusiones y *malware* de alto rendimiento, y *sandboxing* basado en la nube gracias a la tecnología RTDMI de SonicWall.

Seguridad las 24 horas del día[1]
NSv garantiza la protección de movimientos laterales, además de la protección del tráfico entrante y saliente. Las nuevas actualizaciones de amenazas se transfieren automáticamente a los firewalls con servicios de seguridad activos, donde se hacen efectivas inmediatamente sin necesidad de reiniciar el sistema ni interrumpir el servicio.

Protección de día cero[1]
NSv protege la red ante los ataques de día cero con actualizaciones constantes contra los últimos métodos y técnicas de *exploits*, que cubren miles de *exploits* individuales.

API de amenazas
NSv recibe y utiliza cualquier información de inteligencia propietaria, de fabricantes de equipos originales o de terceros para combatir las amenazas avanzadas como los ataques de día cero, usuarios internos maliciosos, credenciales comprometidas, *ransomware* y amenazas persistentes avanzadas.

Protección por zonas
NSv refuerza la seguridad interna al permitir la segmentación de la red en múltiples zonas de seguridad con servicio de prevención de intrusiones que impide la propagación de las amenazas de unas zonas a otras. Gracias a la creación y aplicación de reglas de acceso y políticas NAT al tráfico que pasa por las distintas interfaces, puede permitir o denegar el acceso a la red interna o externa en función de diferentes criterios.

Inteligencia y control de aplicaciones[1]
NSv ofrece un control pormenorizado del tráfico de la red a nivel de usuario, dirección de correo electrónico, programa y subred IP con políticas específicas para las aplicaciones. Controla las aplicaciones personalizadas creando definiciones basadas en parámetros específicos o patrones exclusivos de una aplicación. El acceso a la red interna o externa se permite o deniega atendiendo a diferentes criterios.

Prevención de filtración de datos
NSv permite buscar palabras clave en los flujos de datos. Esto limita la transferencia de determinados nombres de archivo, tipos de archivo, adjuntos de correo electrónico, tipos de adjuntos, correos electrónicos con determinados asuntos y correos electrónicos con determinadas palabras clave o patrones de byte.

Gestión del ancho de banda de la capa de aplicaciones
NSv puede seleccionar entre varias configuraciones de gestión de ancho de banda para reducir el uso de ancho de banda de una aplicación utilizando el monitor de paquetes. Esto ofrece un mayor control de la red.

[1] *Requiere suscripción a SonicWall Advanced Gateway Security Services (AGSS).*
[2] *SonicWall Global Management System y Capture Security Center requieren licencias o suscripciones separadas.*

Comunicación segura
NSv garantiza que el intercambio de datos entre grupos de máquinas virtuales se realiza de forma segura, incluido el aislamiento, la confidencialidad, la integridad y el control del flujo de información dentro de estas redes mediante el uso de segmentación.

Control de acceso
NSv verifica que solo las VM que cumplan un determinado conjunto de condiciones puedan acceder a datos que pertenezcan a otra VM mediante el uso de VLAN.

Autenticación de usuarios
NSv crea políticas para controlar o restringir el acceso a la VM y la carga de trabajo por parte de usuarios no autorizados.

Confidencialidad de los datos
NSv bloquea el robo de información y el acceso ilegítimo a datos y servicios protegidos.

Resiliencia y disponibilidad de las redes virtuales
NSv evita la interrupción o degradación de los servicios y las comunicaciones de las aplicaciones.

Seguridad e integridad del sistema
NSv detiene la apropiación no autorizada de los sistemas y servicios de las VM.

Mecanismos de validación, inspección y control del tráfico
NSv detecta irregularidades y comportamientos maliciosos para detener los ataques dirigidos contra las cargas de trabajo de las VM.

Opciones de implementación
NSv se puede implementar en una amplia variedad de plataformas virtualizadas y en la nube para diversos casos de uso de seguridad de nube pública o privada.

Modelos de licencias flexibles
SonicWall ofrece modelos de licencias perpetuas y no perpetuas. La licencia perpetua es un modelo operativo tradicional en el que las licencias del firewall y del servicio de seguridad se deben adquirir por separado. Por lo tanto, estas licencias vencen por separado. La licencia no perpetua es una oferta única en la que las licencias del firewall y del servicio de seguridad se agrupan y vencen al mismo tiempo. Para las implementaciones de nubes públicas, las licencias perpetuas y no perpetuas están disponibles como licencia Bring Your Own License (BYOL).

El modelo de licencia no perpetua o por suscripción de SonicWall ofrece flexibilidad y sencillez, ya que el software del firewall y los servicios de seguridad se agrupan bajo un único SKU. Este modelo está disponible para las ofertas tanto de nube privada (ESXi e Hyper-V) como de nube pública (AWS, Azure). Antes de que expire el servicio, se envían notificaciones de vencimiento del servicio.

El modelo de licencia no perpetua está disponible en tres versiones: Suscripción IPS/App Control, Suscripción TotalSecure y Suscripción TotalSecure Advanced, durante un periodo de un año. En función de los niveles de oferta, el software NSv se agrupa junto con Intrusion Prevention System (IPS), control de aplicaciones, soporte, Capture Security Center (CSC), Comprehensive Gateway Security Suite (CGSS) o Advanced Gateway Security Suite (AGSS).

Especificaciones del sistema de la serie NSv

FIREWALL GENERAL	NSv 10	NSv 25	NSv 50	NSv 100
Sistema operativo	SonicOS[1]			
Hipervisores compatibles	VMware ESXi v5.5/v6.0/v6.5/v6.7, Microsoft Hyper-V Win 2012/2016, KVM Ubuntu 16.04/CentOS 7			
Plataformas de nubes públicas compatibles (tipo de instancia)	AWS (c5.large), Azure (Std D2 v2)			
Concesión de licencias	BYOL, PAYG[2]			
Número máximo de vCPU soportados	2	2	2	2
Número de interfaces (ESXi/Hyper-V/KVM)	8/8/8	8/8/8	8/8/8	8/8/8
Número máximo de núcleos de gestión/ DataPlane	1/1	1/1	1/1	1/1
Memoria mínima[3]	4 GB	4 GB	4 GB	4 GB
Memoria máxima[4]	6 GB	6 GB	6 GB	6 GB
IP/Nodos soportados	10	25	50	100
Almacenamiento mínimo	60 GB			
Usuarios de SSO	25	50	100	100
Protocolización	Analizador, Registro local, Registro del sistema			
Alta disponibilidad	Activo/Pasivo			
RENDIMIENTO DE FIREWALL/VPN[6]	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Rendimiento de inspección	2 Gbps	2,5 Gbps	3 Gbps	3,5 Gbps
Rendimiento de DPI completo (GAV/GAS/IPS)	450 Mbps	550 Mbps	650 Mbps	750 Mbps
Rendimiento de inspección de aplicaciones	1 Gbps	1,25 Gbps	1,5 Gbps	1,75 Gbps
Rendimiento de IPS	1 Gbps	1,25 Gbps	1,5 Gbps	1,75 Gbps
Rendimiento de inspección *antimalware*	450 Mbps	550 Mbps	650 Mbps	750 Mbps
Rendimiento de IMIX	750 Mbps	850 Mbps	950 Mbps	1100 Mbps
Rendimiento de TLS/SSL DPI	650 Mbps	750 Mbps	850 Mbps	950 Mbps
Rendimiento de VPN	500 Mbps	550 Mbps	600 Mbps	650 Mbps
Conexiones por segundo	1.800	5.000	8.000	10.000
Conexiones máximas (SPI)	2.500	6.250	12.500	25.000
Número máximo de conexiones (DPI)	2.500	6.250	12.500	25.000
Conexiones TLS/SSL DPI	500	1.000	2.000	4.000
VPN	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Túneles VPN entre emplazamientos	10	10	25	50
Clientes VPN IPSec	10 (10)	10 (10)	10 (25)	10 (25)
Clientes SSL VPN incluidos[7]	2	2	2	2
Clientes SSL VPN (máx.)[7]	50	50	50	50
Cifrado/autenticación	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, Suite B, Common Access Card (CAC)			
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14v			
VPN basada en enrutamiento	RIP, OSPF, BGP			
REDES	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Asignación de direcciones IP	Estática, DHCP, servidor DHCP interno, relé DHCP			
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT			
VLAN máx.	25	25	50	50
Protocolos de enrutamiento	BGP4, OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas			
QoS	Prioridad de ancho de banda, ancho de banda máximo, ancho de banda garantizado, marcado DSCP, 802.1p			
Autenticación	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de datos de usuarios interna, Terminal Services, Citrix			
VoIP	SIP			
Estándares	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			
Número máximo de grupos SD-WAN	12	12	18	32
Número máximo de miembros SD-WAN por producto	24	24	36	64

Especificaciones del sistema de la serie NSv, continuación

FIREWALL GENERAL	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Sistema operativo	SonicOS[1]				
Hipervisores compatibles	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7				
Plataformas de nubes públicas compatibles (tipo de instancia)	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)
Concesión de licencias	BYOL, PAYG[2]				
Número máximo de vCPU soportados	2	3	4	8	16
Número de interfaces (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
Número máximo de núcleos de gestión/ DataPlane	1/1	1/2	1/3	1/7	1/15
Memoria mínima[3]	6 GB	6 GB	8 GB	10 GB	12 GB
Memoria máxima[4]	6 GB	8 GB	10 GB	14 GB	18 GB
IP/Nodos soportados	Ilimitados	Ilimitados	Ilimitados	Ilimitados	Ilimitados
Almacenamiento mínimo	60 GB				
Usuarios de SSO	500	5.000	10.000	15.000	20.000
Protocolización	Analizador, Registro local, Registro del sistema				
Alta disponibilidad	Activa/Pasiva[5]				
RENDIMIENTO DE FIREWALL/VPN[6]	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Rendimiento de inspección	4,1 Gbps	5,9 Gbps	7,8 Gbps	13,9 Gbps	17,2 GBPS
Rendimiento de DPI completo (GAV/GAS/IPS)	900 Mbps	1,6 Gbps	2,2 Gbps	4,0 Gbps	6,4 Gbps
Rendimiento de inspección de aplicaciones	2,3 Gbps	3,4 Gbps	4,1 Gbps	5,5 Gbps	6,4 Gbps
Rendimiento de IPS	2,3 Gbps	3,4 Gbps	4,1 Gbps	5,5 Gbps	6,7 GBPS
Rendimiento de inspección *antimalware*	900 Mbps	1,6 Gbps	2,2 Gbps	4,0 Gbps	6,6 Gbps
Rendimiento de IMIX	1,5 Gbps	2,3 Gbps	2,8 Gbps	4,2 Gbps	5,3 Gbps
Rendimiento de TLS/SSL DPI	1,1 Gbps	1,2 Gbps	1,8 Gbps	3,4 Gbps	5,1 GBPS
Rendimiento de VPN	750 Mbps	1,4 Gbps	1,9 Gbps	4,2 Gbps	8,4 Gbps
Conexiones por segundo	13.760	24.360	37.270	75.640	125.000
Conexiones máximas (SPI)	225.000	1M	1.5M	3M	4M
Número máximo de conexiones (DPI)	125.000	500.000	1.5M	2M	2.5M
Conexiones TLS/SSL DPI	8.000	12.000	20.000	30.000	50.000
VPN	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Túneles VPN entre emplazamientos	75	100	6000	10.000	25.000
Clientes VPN IPSec (máximo)	50 (1000)	50 (1000)	2000 (4000)	2000 (6000)	2000 (10.000)
Clientes SSL VPN incluidos[7]	2	2	2	2	2
Clientes SSL VPN (máx.)[7]	100	150	200	300	400
Cifrado/autenticación	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, Suite B, Common Access Card (CAC)				
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14v				
VPN basada en enrutamiento	RIP, OSPF, BGP				
REDES	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Asignación de direcciones IP	Estática, DHCP, servidor DHCP interno, relé DHCP				
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT				
VLAN máx.[8]	128	128	128	128	128
Protocolos de enrutamiento	BGP4, OSPF, RIPv1/v2, rutas estáticas, enrutamiento basado en políticas				
QoS	Prioridad de ancho de banda, ancho de banda máximo, ancho de banda garantizado, marcado DSCP, 802.1p				
Autenticación	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de datos de usuarios interna, Terminal Services, Citrix				
VoIP	SIP				
Estándares	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				
Número máximo de grupos SD-WAN	38	38	70	102	102
Número máximo de miembros SD-WAN por producto	76	76	140	204	204

[1]*Actualmente admite SonicOS 6.5.4.*
[2]*PAYG solo está disponible actualmente en AWS.*
[3]*Memoria con Jumbo frame deshabilitado.*
[4]*Memoria con Jumbo frame habilitado. Se requiere memoria adicional para los Jumbo frames. Los Jumbo frames no se admiten en Azure y AWS.*
[5]*Alta disponibilidad disponible en la plataforma VMware ESXi y Microsoft Hyper-V. La alta disponibilidad no se admite en Azure y AWS.*
[6]*Las cifras de rendimiento publicadas son conformes a las especificaciones. El rendimiento real puede variar dependiendo del hardware subyacente, las condiciones de la red, la configuración del firewall y los servicios activados. El rendimiento y las capacidades también pueden variar en función de la infraestructura de virtualización subyacente, por lo que recomendamos realizar pruebas adicionales en su entorno para asegurarse de que se cumplen sus requisitos de rendimiento y capacidad. Los parámetros de rendimiento se observaron utilizando un procesador Intel Xeon W (W-2195 2,3 GHz, 4,3 GHz Turbo, 24,75 M Cache) ejecutando SonicOSv 6.5.0.2 con VMware vSphere 6.5.*
[7]*Un número mayor de SSL VPN estará disponible únicamente a partir de la versión de firmware SonicOS 6.5.4.4-44v-21-723 y superiores.*
[8]*Las interfaces VLAN no se admiten en Azure y AWS.*
Métodos de prueba: Rendimiento máximo basado en RFC 2544 (para firewall). Rendimiento DPI completo/Gateway AV/Anti-Spyware/IPS medido mediante la prueba de rendimiento HTTP estándar Spirent WebAvalanche y las herramientas de prueba Ixia.
Para las pruebas se han utilizado múltiples flujos a través de múltiples pares de puertos. Medición del rendimiento de VPN basada en el tráfico UDP con paquetes de 1418 bytes de conformidad con RFC 2544. Las especificaciones y prestaciones están sujetas a modificaciones.

Prestaciones

MOTOR RFDPI	
Función	**Descripción**
Inspección profunda de paquetes sin reensamblado (RFDPI)	Este motor de inspección de alto rendimiento patentado y propietario realiza análisis bidireccionales del tráfico basados en flujos sin almacenamiento en búfer ni proxys a fin de descubrir posibles intentos de intrusión o ataques de *malware* y de identificar el tráfico de aplicaciones independientemente del puerto.
Inspección bidireccional	Escanea el tráfico entrante y saliente de forma simultánea en busca de amenazas con el fin de evitar que la red se utilice para la distribución de *malware* o se convierta en una plataforma de lanzamiento de ataques en el caso de que se introduzca un equipo infectado.
Inspección basada en flujos	La tecnología de inspección sin proxy ni búfer proporciona un rendimiento DPI de latencia ultrabaja para millones de flujos de red simultáneos sin limitaciones de tamaño de archivos ni flujos, y puede aplicarse a protocolos comunes y a flujos de TCP sin procesar.
Altamente paralelo y escalable	El diseño único del motor RFDPI, en combinación con la arquitectura multinúcleo, proporciona un rendimiento DPI elevado y tasas de establecimiento de sesiones nuevas extremadamente altas para hacer frente a los picos de tráfico de las redes más exigentes.
Inspección de paso único	La arquitectura DPI de paso único escanea el tráfico simultáneamente para la detección de *malware* y de intrusiones y para la identificación de aplicaciones, reduciendo drásticamente la latencia de la DPI y garantizando la correlación de toda la información sobre las amenazas en una única arquitectura.

FIREWALL Y REDES	
Función	**Descripción**
API REST	Permiten al firewall recibir y utilizar cualquier información de inteligencia propietaria, de fabricantes de equipos originales o de terceros para combatir las amenazas avanzadas como los ataques de día cero, usuarios internos maliciosos, credenciales comprometidas, *ransomware* y amenazas persistentes avanzadas.
Inspección dinámica de paquetes	Todo el tráfico de la red se inspecciona, se analiza y se somete a las políticas de acceso del firewall.
Alta disponibilidad[1]	La serie NSv soporta alta disponibilidad Activa/Pasiva (A/P) con sincronización de estado.
Protección contra ataques DDoS/DOS	La protección contra inundaciones SYN proporciona una defensa contra los ataques de DoS mediante el uso de tecnologías de listas negras de nivel 3 (SYN proxy) y nivel 2 (SYN). Asimismo, ofrece protección contra ataques DoS/DDoS mediante funciones de protección contra inundaciones UDP/ICMP y de limitación de la tasa de conexión.
Soporte IPv6	La versión 6 del protocolo de Internet (IPv6) se encuentra en las primeras fases para sustituir a IPv4. Con SonicOS, el hardware será compatible con las implementaciones de filtrado y de modo Wire.
Opciones de implementación flexibles	La serie NSv puede implementarse en el modo tradicional NAT, en el modo puente de capa 2, en el modo Wire y en el modo de TAP de red.
Equilibrio de carga WAN	Equilibra la carga de múltiples interfaces WAN mediante Round Robin o Spillover o utilizando métodos basados en porcentajes.
Calidad de Servicio (QoS) avanzada	Garantiza las comunicaciones críticas con etiquetado 802.1p y DSCP y reasignación del tráfico VoIP en la red.
Soporte de proxy SIP	Bloquea las llamadas *spam*: todas las llamadas entrantes han de ser autorizadas y autenticadas por el proxy SIP.
Autenticación biométrica	Soporta la autenticación de dispositivos móviles, como el reconocimiento de huellas dactilares, que no pueden ser fácilmente duplicadas ni compartidas, con el fin de autenticar la identidad del usuario de forma segura para que pueda acceder a la red.
Autenticación abierta e inicio de sesión social	Permite a los usuarios invitados utilizar sus credenciales de servicios de redes sociales, como Facebook, Twitter o Google+, para iniciar sesión y acceder a Internet y a otros servicios para usuarios invitados mediante una conexión inalámbrica de un host, una LAN o zonas DMZ, utilizando una autenticación de paso a través.

GESTIÓN E INFORMES	
Función	**Descripción**
Gestión basada en la nube y local	Funciones de configuración y gestión de los dispositivos SonicWall disponibles en la nube a través del SonicWall Capture Security Center y localmente utilizando el Sistema de gestión global (GMS) de SonicWall.
Potente gestión de dispositivos individuales	Ofrece una interfaz intuitiva basada en Web que puede configurarse de forma rápida y sencilla, una interfaz de línea de comandos completa y soporte para SNMPv2/3.
Informes IPFIX/Netflow de flujos de aplicaciones	Exporta análisis del tráfico de aplicaciones y datos de uso mediante protocolos IPFIX o NetFlow para supervisar y elaborar informes en tiempo real y de datos antiguos con herramientas como SonicWall Scrutinizer u otras compatibles con IPFIX y NetFlow con extensiones.

REDES PRIVADAS VIRTUALES (VPN)	
Función	**Descripción**
VPN con aprovisionamiento automático	Simplifica y reduce al máximo la complejidad de las implementaciones de firewalls distribuidas automatizando el aprovisionamiento inicial de la pasarela VPN de extremo a extremo entre los firewalls de SonicWall, mientras que los sistemas de seguridad y conectividad funcionan de forma instantánea y automática.
VPN IPSec para conectividad entre emplazamientos	La VPN IPSec de alto rendimiento permite a la serie NSv actuar como un concentrador VPN para miles de emplazamientos grandes, oficinas remotas u oficinas domésticas.
Acceso remoto mediante SSL VPN o cliente IPSec	Permite utilizar la tecnología SSL VPN sin clientes o un cliente IPSec de fácil gestión para el acceso sencillo a correos electrónicos, archivos, ordenadores, sitios Intranet y aplicaciones desde una variedad de plataformas.

[1]*La alta disponibilidad no se admite actualmente en AWS y Azure*

Pasarela VPN redundante	Al utilizarse múltiples WANs, pueden configurarse una VPN primaria y otra secundaria para permitir la reconexión y la recuperación automáticas de todas las sesiones VPN.
VPN basada en enrutamiento	El enrutamiento dinámico a través de enlaces VPN garantiza un servicio sin interrupciones en caso de fallo temporal del túnel VPN, ya que el tráfico entre los *endpoints* puede redireccionarse fácilmente a través de rutas alternativas.

RECONOCIMIENTO DE CONTENIDO/CONTEXTUAL	
Función	**Descripción**
Seguimiento de la actividad de los usuarios	La identificación de usuario y la actividad están disponibles a través de la integración fluida de las funciones SSO con AD/LDAP/Citrix1/Terminal Services1 en combinación con una amplia información obtenida a través de DPI.
GeoIP – Identificación del tráfico en base al país	Identifica y controla el tráfico de red dirigido a, o procedente de, países determinados para ofrecer protección contra ataques de amenazas de origen conocido o sospechoso, o para investigar el tráfico sospechoso originado en la red. Permite crear listas personalizadas de países y *botnets* para anular etiquetas de país o *botnet* erróneas asociadas con una dirección IP. Elimina el filtrado de direcciones IP no deseado debido a errores de clasificación.
Filtrado DPI de expresiones regulares	Previene la filtración de datos gracias a que identifica y controla el contenido que atraviesa la red mediante la coincidencia de expresiones regulares. Permite crear listas personalizadas de países y *botnets* para anular etiquetas de país o *botnet* erróneas asociadas con una dirección IP.

Servicios de suscripción de prevención de violaciones de seguridad

CAPTURE ADVANCED THREAT PROTECTION	
Función	**Descripción**
Sandbox multimotor	La plataforma de *sandbox* multimotor, que incluye *sandboxing* virtualizado, emulación de sistema completo y tecnología de análisis de nivel de hipervisor, ejecuta el código sospechoso y analiza su comportamiento, proporcionando una visibilidad completa de la actividad maliciosa.
Inspección de memoria profunda en tiempo real (RTDMI)	Esta tecnología basada en la nube, pendiente de patente, detecta y bloquea el *malware* que no presenta ningún comportamiento malicioso y oculta su armamento mediante cifrado. Al obligar al *malware* a revelar su armamento a la memoria, el motor RTDMI detecta y bloquea de forma proactiva las amenazas de mercado masivo, de día cero y el malware desconocido.
Bloqueo hasta que haya un veredicto	A fin de evitar el acceso a la red de archivos potencialmente peligrosos, los archivos enviados a la nube para su análisis pueden retenerse en la pasarela hasta que se emita un veredicto.
Análisis de gran variedad de tipos y tamaños de archivos	Soporta análisis de una amplia variedad de tipos de archivos, ya sea de forma individual o en grupo, como los programas ejecutables (PE), DLL, PDF, documentos MS Office, archivos, JAR y APK, así como múltiples sistemas operativos, como Windows, Android, Mac OS X y entornos multinavegador.
Rápida implementación dedefiniciones	Cuando se detecta un archivo malicioso, inmediatamente se pone una definición a disposición de los firewalls con suscripción a SonicWall Capture ATP y se envía a las bases de datos de definiciones de Gateway Anti-Virus e IPS ya las bases de datos de reputación de URL, IP y dominios en el transcurso de 48 horas.
Capture Client	Capture Client es una plataforma de cliente unificada que proporciona múltiples prestaciones de protección de *endpoints*, como protección de *malware* avanzada y soporte para la visibilidad del tráfico cifrado. Utiliza tecnologías de protección multicapa, funciones completas de informes y prestaciones de refuerzo de protección de *endpoints*.

PREVENCIÓN DE AMENAZAS CIFRADAS	
Función	**Descripción**
Descifrado e inspección TLS/SSL	Descifra e inspecciona el tráfico cifrado mediante TLS/SSL sobre la marcha, sin necesidad de proxys, en busca de *malware*, intrusiones y filtraciones de datos, y aplica políticas de control de aplicaciones, URL y contenido para ofrecer protección contra las amenazas ocultas en el tráfico cifrado mediante SSL. Incluido con las suscripciones de seguridad para todos los modelos de la serie NSv.
Inspección SSH	La inspección profunda de paquetes de SSH (DPI-SSH) descifra e inspecciona los datos que atraviesan los túneles SSH para prevenir ataques que utilicen SSH.

PREVENCIÓN DE INTRUSIONES	
Función	**Descripción**
Protección basada en contramedidas	El sistema de prevención de intrusiones (IPS) estrechamente integrado utiliza definiciones y otras contramedidas para escanear los datos útiles de los paquetes en busca de vulnerabilidades y *exploits*, cubriendo de este modo un amplio abanico de ataques y vulnerabilidades.
Actualizaciones automáticas de las definiciones	El equipo de investigación de amenazas de SonicWall investiga e implementa contramedidas IPS, actualizando continuamente una larga lista que cubre más de 50 categorías de ataques. Las nuevas actualizaciones se hacen efectivas en el acto, sin que sea necesario reiniciar los sistemas ni interrumpir su servicio.
Protección IPS entre zonas	Refuerza la seguridad interna al segmentar la red en múltiples zonas de seguridad con prevención de intrusiones para evitar la propagación de las amenazas de unas zonas a otras.
Detección y bloqueo de actividades de comando y control (CnC) procedente de ataques botnets	Identifica y bloquea el tráfico de comando y control originado en *bots* de la red local y dirigido a IP y dominios identificados como propagadores de *malware* o conocidos como puntos de CnC.
Abuso/anomalía de protocolo	Identifica y bloquea ataques que abusan de los protocolos para intentar eludir el IPS.

Protección de día cero	Protege la red ante los ataques de día cero con actualizaciones constantes contra los últimos métodos y técnicas de *exploits*, que cubren miles de *exploits* individuales.
Tecnología antievasión	La amplia normalización de flujos, la descodificación y otras técnicas impiden que las amenazas puedan penetrar la red sin ser detectadas utilizando técnicas de evasión en las capas 2-7.

PREVENCIÓN DE AMENAZAS

Función	Descripción
Antimalware en pasarela	El motor RFDPI analiza todo el tráfico entrante, saliente y dentro de una misma zona en busca de virus, troyanos, registradores de pulsaciones de teclas y otros tipos de *malware* en archivos de una longitud y un tamaño ilimitados en todos los puertos y flujos de TCP.
Protección *antimalware* de Capture Cloud	Los servidores de la nube de SonicWall disponen de una base de datos de decenas de millones de definiciones de amenazas que se actualiza continuamente y se utiliza para aumentar las capacidades de la base de datos de definiciones integrada, lo que proporciona a la tecnología RFDPI una amplia cobertura de amenazas.
Actualizaciones de seguridad las 24 horas	Las nuevas actualizaciones de amenazas se transfieren automáticamente a los firewalls con servicios de seguridad activos, donde se hacen efectivas inmediatamente sin necesidad de reiniciar el sistema ni interrumpir el servicio.
Inspección TCP bidireccional (sinprocesar)	El motor RFDPI puede analizar flujos de TCP sin procesar en cualquier puerto y en ambas direcciones, con lo que se previenen los ataques que intentan infiltrarse por sistemas de seguridad desactualizados que se centran en proteger solo algunos puertos más conocidos.
Amplio soporte de protocolos	Identifica protocolos comunes, como HTTP/S, FTP, SMTP, SMBv1/v2 y otros tipos, que no envían datos en TCP sin procesar, y descodifica cargas útiles para la inspección de *malware*, incluso si no se ejecutan en puertos estándares y bien conocidos.

INTELIGENCIA Y CONTROL DE APLICACIONES

Función	Descripción
Control de aplicaciones	Controle aplicaciones, o funciones de aplicaciones individuales, identificadas por el motor RFDPI mediante su cotejo con una base de datos en continuo crecimiento de miles de definiciones de aplicaciones, con el objetivo de aumentar la seguridad y la productividad de la red.
Identificación personalizada de aplicaciones	Controle las aplicaciones personalizadas creando definiciones basadas en parámetros específicos o patrones exclusivos de una aplicación en sus comunicaciones de red para conseguir un mayor control de la red.
Gestión del ancho de banda de las aplicaciones	Asigne y regule de forma detallada el ancho de banda disponible para aplicaciones o categorías de aplicaciones críticas, a la vez que limita el tráfico de aplicaciones no esenciales.
Control granular	Controle aplicaciones (o componentes específicos de una aplicación) basándose en programaciones, grupos de usuarios, listas de exclusión y una gama de acciones con una completa identificación de usuario mediante SSO a través de la integración de LDAP/AD/Terminal Services/Citrix.

FILTRADO DE CONTENIDO

Función	Descripción
Filtrado de contenido dentro y fuera	Aplique políticas de usos aceptables y bloquee el acceso a sitios Web HTTP/HTTPS que contengan información o imágenes inaceptables o improductivas con Content Filtering Service y Content Filtering Client.
Cliente de filtrado de contenido reforzado	Amplíe el refuerzo de políticas para bloquear contenido de Internet para dispositivos Windows, Mac OS, Android y Chrome situados fuera del perímetro del firewall.
Controles granulares	Bloquee contenido utilizando las categorías predefinidas o cualquier combinación de categorías. El filtrado puede programarse por hora del día, por ejemplo, durante el horario laboral o escolar, y aplicarse a usuarios individuales o grupos.
Almacenamiento en caché Web	Las clasificaciones de URL se almacenan en caché en el firewall de SonicWall, con lo que se reduce el tiempo de respuesta para el posterior acceso a sitios que se visitan con frecuencia a solo una fracción de segundo.

ANTIVIRUS Y *ANTISPYWARE* REFORZADOS

Función	Descripción
Protección en varios niveles	Utilice las funciones del firewall, como la primera capa de defensa en el perímetro, junto con la protección de *endpoints*, a fin de bloquear los virus que penetran en la red por medio de portátiles, unidades de memoria flash y otros sistemas no protegidos.
Opción de aplicación automatizada	Asegúrese de que todos los equipos que accedan a la red tengan instalado y activo el software antivirus y/o certificado DPI-SSL apropiado. De este modo, eliminará los costes asociados habitualmente a la gestión de soluciones antivirus para equipos de escritorio.
Opción de instalación e implementación automatizadas	La implementación y la instalación máquina a máquina de clientes antivirus y *antispyware* se realiza de forma automática en toda la red, con lo que se minimiza la sobrecarga administrativa.
Antivirus de próxima generación	Capture Client utiliza un motor de inteligencia artificial estático para determinar las amenazas antes de que puedan ejecutarse y regresar a un estado previo a la infección.
Protección *antispyware*	La potente función de protección *antispyware* analiza y bloquea la instalación de un completo conjunto de programas de *spyware* en equipos de escritorio y portátiles antes de que éstos transmitan datos confidenciales, lo que contribuye a aumentar la seguridad y el rendimiento de los equipos de escritorio.

Visión de conjunto de las prestaciones de SonicOS

Control global sobre

- Control centralizado de la visibilidad de IPv6
- Inhabilitación global del procesamiento del tráfico de IPv6
- Inhabilitación de políticas VPN por defecto, pantallas de configuración y reglas autogeneradas

Seguridad de usuario e inicio de sesión

- Bloqueo de usuario basado en los intentos de inicio de sesión por rango de dirección IP
- Bloqueo de usuario desde CLI
- Cambio de contraseña forzado en el primer inicio de sesión
- Soporte de autenticación de dos factores (TOTP)
- Soporte de portal sin necesidad de intervención para políticas de usuarios invitados
- Soporte IPv6 para servicio de invitados
- Soporte de contabilidad TACACS+
- Control de cuota para todos los usuarios
- Autenticación dinámica HTTP de botnets

Red y sistema

- Soporte SD-WAN
- Soporte de seguridad de DNS / sumidero de DNS
- FQDN sobre TCP DNS
- Objetos de dirección FQDN para NAT
- Relé DHCPv6
- Modo de direccionamiento IPv6 para la puerta de enlace de la capa de aplicación VoIP H.323
- Soporte básico de plano de control (CP) múltiple
- Redireccionamiento HTTP/HTTPS con descarga de plano de datos
- Descarga de IP auxiliar al plano de datos
- Copia de seguridad de firmware en almacenamiento local
- Cifrado de alta disponibilidad
- Soporte de carga de firmware de alta disponibilidad
- Optimización del enrutamiento basado en políticas de rutas estáticas y dinámicas
- Mejoras en el rendimiento/desempeño
- Función de vigilancia para supervisar la condición del firewall
- Mayor escalabilidad para enrutamiento avanzado a través de interfaces de túnel VPN numeradas
- Actualización de las librerías H.323 basada en el compilador OSS Noklava v10.5.0 ASN.1
- Actualización de prioridades del hilo de tareas
- SSLVPN y marcadores en el plano de datos

Servicios de seguridad

- Control pormenorizado del bloqueo hasta que haya un veredicto de Capture ATP
- Visualización de nombre de archivo descriptivo para los protocolos distintos a HTTP de Capture ATP
- Bloqueo CFS de vídeos individuales de YouTube
- Soporta filtrado de contenido HTTPS y DPI-SSL
- Antivirus de última generación (SentinelOne) y aplicación de DPI-SSL
- Mejora de rendimiento de la protección WAN DDOS

Políticas / objetos

- Mejoras de las reglas de acceso
- Enrutamiento basado en aplicaciones
- Objetos con direcciones dinámicas
- Exclusión de política CFS
- Objetos de filtrado de contenido HTTPS basado en política
- Soporte de grupos de listas URI en objetos de filtrado de contenido
- Inserción de encabezado personalizado CFS para las peticiones HTTP
- UUID para reglas y objetos
- UUID para políticas CFS
- Anulación de MAC de origen para las políticas NAT

DPI-SSL / DPI-SSH

- Lista blanca dinámica basada en la nube de DPI-SSL
- Bloqueo DPI-SSH de la habilitación del puerto SSH
- Bloqueo DPI-SSH de la habilitación X11
- Protección del puerto de descifrado SSL en Packet Mirror / Packet Capture
- Control pormenorizado DPI-SSL por zona
- Control DPI-SSL basado en reglas de acceso
- Bloqueo de cliente DPI-SSL o permiso de certificados CA caducados
- Ampliación de solicitud de estado del certificado TLS
- Soporte para CRL local
- Verificación mejorada del certificado DPI-SSL
- Soporte para cifrado relacionado con ECDSA
- Soporte de versión de OpenSSL LTS para certificación federal

Inicio de sesión, supervisión y generación de informes

- Capacidad para comprobar que la DPI se ha realizado en un paquete específico
- Nombre de archivo e inicio de sesión URI para el control de aplicaciones
- Registros de inicio de sesión a disposición del administrador
- Auditoría de configuración
- Inicio de sesión para mapeo NAT para conexiones TCP
- Soporte FTP para la automatización de registros
- Soporte de análisis e informes de Capture Security Center (CSC) para NSv
- Inicio de sesión en Capture ATP del emisor/receptor de correo electrónico
- Mejoras en el cliente Capture Threat Assessment (SWARM v3)
- Función para restablecer los datos estadísticos de SFR (SWARM)
- Posibilidad de seleccionar el idioma del informe de SonicFlow

API

- SonicOS API fase 1
- Soporte de autenticación de SonicOS API
- SonicOS API fase 2
- LHM RESTful API

IU de gestión web de SonicOS

- Búsqueda global de SonicOS
- Mejoras de uso para páginas de contenido
- Almacenamiento de preferencias de IU del lado del cliente por usuario
- Asignación de nombre descriptivo a las pantallas de gestión de SonicOS
- Nuevo diseño de la inferfaz web de SonicOS

Información de pedido de la serie NSv

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

**Consulte con su distribuidor local de SonicWall para obtener una lista completa de los SKU*

Acerca de SonicWall

SonicWall ofrece ciberseguridad sin límites para la era hiperdistribuida y una realidad laboral en la que todo el mundo usa tecnología móvil, a distancia y poco segura. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y posibilitar una economía revolucionaria, SonicWall cierra la brecha comercial en materia de ciberseguridad para empresas, gobiernos y pymes de todo el mundo. Para obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
(Estados Unidos)
Encontrará más información en nuestro sitio web.
www.sonicwall.com

Datasheet-NSvVirtualFirewalls-US-VG-2088