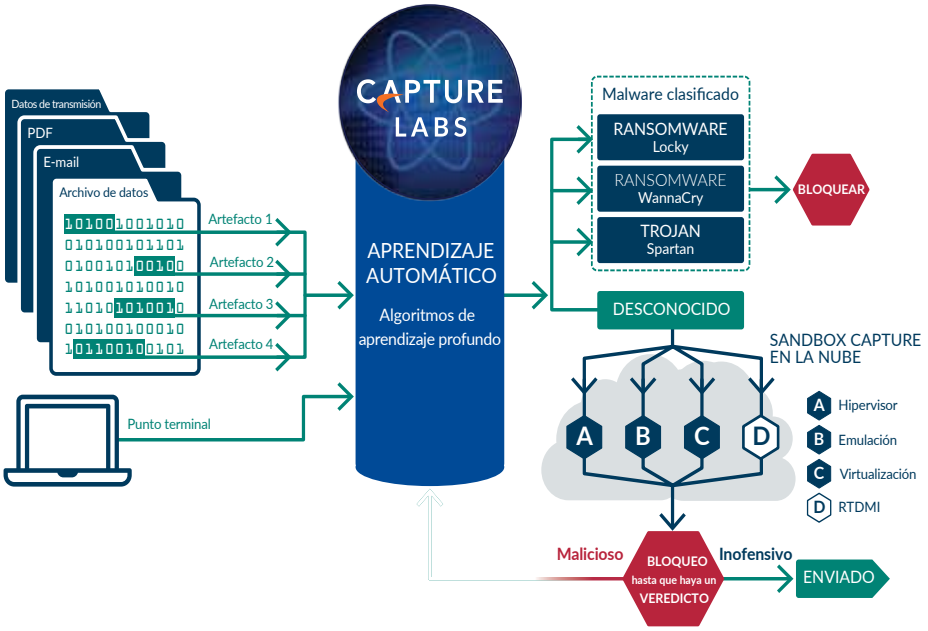
Serie SonicWall Network Security virtual (NSv)

Seguridad profunda para entornos de nube pública, privada o híbrida

El diseño, la implementación y el despliegue de arquitecturas de red modernas, como la virtualización y la nube, continúan siendo un factor de éxito importante para muchas organizaciones. La virtualización del centro de datos, la migración a la nube, o una combinación de ambas, han demostrado acarrear ventajas operacionales y económicas considerables. Sin embargo, las vulnerabilidades de los entornos virtuales están bien documentadas. Continuamente se descubren vulnerabilidades nuevas que conllevan implicaciones y retos de seguridad importantes. Para garantizar que los servicios de las aplicaciones se entreguen de forma segura, eficiente y escalable, al tiempo que se combaten las amenazas que resultan dañinas para todas las partes del framework virtual, incluidos los equipos virtuales, las cargas de trabajo de las aplicaciones y los datos deben estar entre las principales prioridades.

Los firewalls SonicWall Network Security virtual (NSv) ayudan a los equipos de seguridad a reducir este tipo de riesgos de seguridad y vulnerabilidades, que pueden causar graves interrupciones de sus operaciones y servicios críticos de negocio. Con herramientas y servicios de seguridad equipados con todas las prestaciones, como la Inspección profunda de paquetes sin reensamblado (RFDPI), controles de seguridad y servicios de redes equivalentes a los proporcionados por un firewall físico de SonicWall, NSv protege de forma efectiva todos los componentes críticos de sus entornos de nube privada/pública.

NSv puede implementarse y ponerse a disposición fácilmente en un entorno virtual multiempresa, normalmente entre redes virtuales. De este modo, puede capturar comunicaciones e intercambios de datos entre los equipos virtuales para ofrecer una prevención de brechas automatizada, mientras se establecen estrictas medidas de control del acceso a fin de garantizar la confidencialidad de los datos y la seguridad e integridad de los equipos virtuales. La completa suite de servicios de inspección de seguridad de SonicWall[1] neutraliza con éxito las amenazas de seguridad (como ataques entre equipos virtuales, ataques de canal lateral, intrusiones comunes basadas en red y vulnerabilidades de aplicaciones y protocolos). Todo el tráfico de los equipos virtuales se somete a múltiples motores de análisis de amenazas, con prevención de intrusiones, antivirus y antispyware en pasarela, antivirus en la nube, filtrado de botnets, control de aplicaciones y el sandboxing multimotor de Capture Advanced Threat Protection.



Ventajas:

Seguridad en la nube pública y privada

- Visibilidad completa de la comunicación intrahost entre los equipos virtuales para la prevención de amenazas
- Implementación adecuada de políticas de seguridad para su aplicación en todo el entorno virtual
- Normas de habilitación de aplicaciones seguras por aplicación, usuario y dispositivo, independientemente de la ubicación de los equipos virtuales.
- Implementación de zonas y aislamientos de seguridad apropiados.

Protección de equipos virtuales

- Defensa contra las vulnerabilidades de día cero con Capture Advanced Threat Protection (ATP)
- Prevención del uso no autorizado de los sistemas virtuales
- Detención del acceso no autorizado a los recursos de datos protegidos
- Bloqueo de las acciones maliciosos e intrusivas, como la propagación de malware, la ejecución de comandos de sistema operativo, la exploración del sistema de archivos y la comunicación de comando y control
- Prevención de la interrupción del servicio de todo o parte del ecosistema virtual

Seguridad basada en la segmentación

Con el fin de lograr una efectividad óptima contra las amenazas persistentes avanzadas (APTs), para la segmentación de la seguridad de red debe aplicarse un conjunto integrado de barreras dinámicas que permita detener las amenazas avanzadas. Gracias a las prestaciones de seguridad basada en segmentos, NSv puede agrupar interfaces similares y aplicarles las mismas políticas, en lugar de tener que elaborar la misma política para cada interfaz. Al aplicar políticas de seguridad en el interior de la red virtual, puede configurarse la segmentación para organizar los recursos de la red en diferentes segmentos y permitir o restringir el tráfico entre dichos segmentos. De este modo, el acceso a los recursos internos críticos puede someterse a un control estricto.

NSv puede aplicar automáticamente restricciones de segmentación en base a criterios dinámicos, como las credenciales de identidad de los usuarios, la geolocalización de IP y el nivel de seguridad de los puntos terminales móviles. Con el fin de proporcionar una seguridad ampliada, NSv también es capaz de integrar la conmutación de red multigigabit en su política de segmentos de seguridad y en la implementación de los mismos. Aplica la política de segmentos al tráfico en los puntos de conmutación de toda la red, y gestiona globalmente la implementación de la seguridad de los segmentos desde una única consola.

Dado que los segmentos tan solo son efectivos en la medida en que lo es la seguridad que puede aplicarse entre ellos, NSv aplica un servicio de prevención de intrusiones (IPS) para escanear el tráfico tanto entrante como saliente en el segmento de la VLAN a fin de mejorar la seguridad para el tráfico de red interno. Aplica, para cada segmento, una gran variedad de servicios de seguridad en múltiples interfaces basándose en una política aplicable.

Casos de uso de implementación flexibles

Con soporte de infraestructura para implementación de alta disponibilidad, NSv cumple los requisitos de escalabilidad y disponibilidad de los Centros de datos definidos por software (SDDC). Garantiza la resiliencia del sistema, la fiabilidad del servicio y el cumplimiento normativo. Optimizado para una amplia variedad de casos de uso de implementación pública, privada e híbrida, NSv puede adaptarse a los cambios de nivel de servicio y asegurarse de que los equipos virtuales y las cargas de trabajo y los recursos de datos de sus aplicaciones estén disponibles y a salvo. Puede hacerlo todo a velocidad multi-Gbps y con baja latencia.

Las organizaciones disfrutan de todas las ventajas de seguridad de un firewall físico, más las ventajas operacionales y económicas de la virtualización. Estas incluyen escalabilidad del sistema, agilidad de las operaciones, velocidad de aprovisionamiento, gestión sencilla y reducción de los costes.

La serie NSv está disponible en múltiples variantes virtuales, cuidadosamente empaquetadas para una amplia variedad de casos de uso de implementación virtualizada y en la nube. Al proporcionar prevención de amenazas e inspección del tráfico cifrado con un rendimiento multi-gigabit, la serie NSv puede adaptarse a cargas pico y garantizar tanto la seguridad de las redes virtuales como la disponibilidad y protección de las cargas de trabajo y los recursos de datos de las aplicaciones.

Control centralizado

Las implementaciones de NSv se gestionan de forma centralizada, tanto localmente con SonicWall GMS[3], como con SonicWall Capture Security Center[3], un software abierto y escalable de gestión, monitorización, informes y análisis de seguridad en la nube que se ofrece a modo de económica solución como servicio. Capture Security Center proporciona el máximo nivel de visibilidad, agilidad y capacidad para controlar todo el ecosistema de firewalls físicos y virtuales con mayor claridad, precisión y velocidad – todo ello desde una única consola.

Prestaciones

Plataforma SonicOS

Todos los firewalls físicos y virtuales de SonicWall, incluidos los de las series NSv, NS*a*, SuperMassive™ y TZ, se basan en la arquitectura de SonicOS. Consulte la ficha técnica de la plataforma SonicWall SonicOS para obtener una lista completa de las prestaciones y funciones.

Prevención de brechas automatizada[1]

Incluye protección completa contra las amenazas avanzadas, con funciones de prevención de malware e intrusiones de alto rendimiento y tecnología de sandboxing basada en la nube.

Seguridad las 24 horas[1]

Las nuevas actualizaciones de las amenazas se transfieren automáticamente a los firewalls con servicios de seguridad activos, donde se hacen efectivas inmediatamente sin necesidad de reiniciar el sistema ni de interrumpir el servicio.

Protección de día cero[1]

NSv protege contra los ataques de día cero con actualizaciones constantes contra los últimos métodos y técnicas de exploits, que cubren miles de exploits individuales.

API contra 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.

CONTROL CENTRALIZADO

- Establezca una ruta sencilla para la gestión completa de la seguridad, la elaboración de informes de análisis y el cumplimiento normativo a fin de unificar su programa de defensa de seguridad de red
- Automatice y correlacione los flujos de trabajo para formar una estrategia totalmente coordinada de control de la seguridad, cumplimiento normativo y gestión de riesgos

CUMPLIMIENTO NORMATIVO

- Ayuda a mantener satisfechos a los organismos reguladores y a los auditores con informes de seguridad automáticos sobre las normas PCI, HIPAA y SOX
- Personalice cualquier combinación de datos auditables de seguridad para ayudarle a avanzar hacia normas específicas

GESTIÓN DE RIESGOS

- Actúe rápidamente e impulse la colaboración, la comunicación y el conocimiento de todo el framework de seguridad compartido
- Tome decisiones informadas sobre las políticas de seguridad en base a información consolidada y crítica en el tiempo sobre las amenazas para aumentar el nivel de eficiencia de la seguridad

GMS proporciona un enfoque holístico de control de la seguridad, cumplimiento normativo y gestión de riesgos

Protección por zonas

NSv refuerza la seguridad interna al segmentar la red en múltiples zonas de seguridad con servicio de prevención de intrusiones para evitar la propagación de las amenazas de unas zonas a otras. Al crear y aplicar normas de acceso y políticas NAT al tráfico que atraviesa las diversas interfaces, puede permitir o denegar el acceso interno o externo a la red en base a diversos criterios.

Inteligencia y control de aplicaciones[1]

Con políticas específicas para las aplicaciones, NSv permite controlar el tráfico de red de forma granular a nivel de los usuarios, las direcciones de correo electrónico, las programaciones horarias y las subredes IP. Controla las aplicaciones personalizadas creando definiciones basadas en parámetros o patrones específicos únicos de una aplicación en sus comunicaciones de red. El acceso tanto interno como externo a la red se permite o deniega en base a diversos criterios.

Prevención de filtración de datos

NSv permite escanear flujos de datos en busca de palabras clave. De este modo, se restringe la transferencia de ciertos nombres de archivos, tipos de archivos, archivos adjuntos de correo electrónico, tipos de archivos adjuntos, e-mails con determinados asuntos y e-mails o archivos adjuntos con determinadas palabras clave o determinados patrones de bytes.

Gestión del ancho de banda de la capa de aplicación

Mediante Packet Monitor, NSv puede elegir entre varios ajustes de gestión de ancho de banda para reducir el uso del ancho de banda de la red por parte de una aplicación. Esto proporciona un mayor control sobre la red.

Comunicación segura

NSv garantiza la seguridad del intercambio de datos entre grupos de equipos virtuales, incluyendo el aislamiento, la confidencialidad, la integridad y el control del flujo de información dentro de estas redes mediante el uso de la segmentación.

Control de acceso

NSv se encarga de que solo aquellos equipos virtuales que cumplan un determinado conjunto de condiciones puedan acceder a datos que pertenezcan a otro equipo virtual utilizando VLANs.

Autenticación de usuarios

NSv crea políticas para controlar o restringir el acceso a equipos virtuales y cargas de trabajo por parte de usuarios no autorizados.

Confidencialidad de los datos

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

Resiliencia y disponibilidad de la red virtual

NSv previene la interrupción o degradación de los servicios y las comunicaciones de las aplicaciones.

Seguridad e integridad del sistema

NSv detiene el uso no autorizado de los sistemas y servicios de los equipos virtuales.

Mecanismos de validación, inspección y monitorización del tráfico

NSv detecta irregularidades y comportamientos maliciosos y detiene los ataques contra las cargas de trabajo de los equipos virtuales.

Opciones de implementación[2]

NSv puede implementarse en una amplia variedad de plataformas virtualizadas y de nube para varios casos de uso de seguridad en la nube privada/pública.

[1] Requiere suscripción a SonicWall Advanced Gateway Security Services (AGSS).
[2] La próxima versión incluirá soporte de imágenes de equipos virtuales (VMI) para MS Hyper-V, Amazon y MS Azure.
[3] SonicWall Global Management System y Capture Security Center requieren licencias o suscripciones separadas.

Especificaciones del sistema de la serie NSv

Firewall general	NSv 10	NSv 25	NSv 50	NSv 100
Sistema operativo	SonicOS			
Hipervisores soportados	VMware ESXi v5.5 / v6.0 / v6.5			
N° máx. de vCPUs soportados	2	2	2	2
Cantidad máx. núcleos gestión/ DataPlane	1/1	1/1	1/1	1/1
Memoria mín.	4 GB	4 GB	4 GB	4 GB
IP/nodos soportados	10	25	50	100
Almacenamiento mínimo	60 GB			
Usuarios con SSO	25	50	100	100
Protocolización	Analyzer, Local Log, Syslog			
Alta disponibilidad	Activa/pasiva			
Rendimiento de firewall/VPN				
Rendimiento de inspección del firewall	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 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 IMIX	750 Mbps	850 Mbps	950 Mbps	1100 Mbps
Rendimiento TLS/SSL DPI	650 Mbps	750 Mbps	850 Mbps	950 Mbps
Rendimiento VPN	500 Mbps	550 Mbps	600 Mbps	650 Mbps
Conexiones por segundo	1.800	5.000	8.000	12.000
Conexiones máximas (SPI)	10.000	50.000	125.000	150.000
Conexiones máximas (DPI)	10.000	50.000	100.000	125.000
Conexiones TLS/SSL DPI	500	1.000	2.000	4.000
VPN				
Túneles VPN entre emplazamientos	10	10	25	50
Clientes VPN IPSec	10	10	25	25
Clientes SSL VPN NetExtender (máximos)	2(10)	2(25)	2(25)	2(25)
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			
Interconexión				
Asignación de direcciones IP	Estática, DHCP, servidor DHCP interno, relé DHCP			
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT			
Interfaces VLAN	25	25	50	50
Protocolos de enrutamiento	BGP, 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 Sevices, Citrix			
VoIP	H323-v1-5 completo, SIP			
Estándares	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			

Especificaciones del sistema de la serie NSv (cont.)

Firewall general	NSa 200	NSa 300	NSa 400	NSa 800	NSa 1600
Sistema operativo	SonicOS				
Hipervisores soportados	VMware ESXi v5.5 / v6.0 / v6.5				
N° máx. de vCPUs soportados	2	3	4	8	16
Cantidad máx. núcleos gestión/ DataPlane	1/1	1/2	1/3	1/7	1/15
Memoria mín.	6 GB	8 GB	8 GB	10 GB	12 GB
IP/nodos soportados	Ilimitados	Ilimitados	Ilimitados	Ilimitados	Ilimitados
Almacenamiento mínimo	60 GB				
Usuarios con SSO	500	5.000	10.000	15.000	20.000
Protocolización	Analyzer, Local Log, Syslog				
Alta disponibilidad	Activa/pasiva				
Rendimiento de firewall/VPN					
Rendimiento de inspección del firewall	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 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 IMIX	1,5 Gbps	2,3 Gbps	2,8 Gbpsv	4,2 Gbps	5,3 Gbps
Rendimiento TLS/SSL DPI	1,1 Gbps	1,2 Gbps	1,8 Gbps	3,4 Gbps	5,1 Gbps
Rendimiento VPN	750 Mbps	1,4 Gbps	1,9 Gbps	4,2 Gbps	8,4 Gbps
Conexiones por segundo	13.760	24.360	32.270	75.640	125.000
Conexiones máximas (SPI)	225.000	1M	1,5 millones	3 millones	4 millones
Conexiones máximas (DPI)	125.000	500.000	1,5 millones	2 millones	2,5 millones
Conexiones TLS/SSL DPI	8.000	12.000	20.000	30.000	50.000
VPN					
Túneles VPN entre emplazamientos	75	100	6000	10.000	25.000
Clientes VPN IPSec (máx.)	50(1.000)	50(1.000)	2000(4.000)	2000(6.000)	2000(10.000)
Clientes SSL VPN NetExtender (máx.)	2(100)	2(100)	2(100)	2(100)	2(100)
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				
Interconexión					
Asignación de direcciones IP	Estática, DHCP, servidor DHCP interno, relé DHCP				
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT				
Interfaces VLAN	50	256	500	512	512
Protocolos de enrutamiento	BGP, 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 Sevices, Citrix				
VoIP	H323-v1-5 completo, SIP				
Estándares	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				

[1] *Las cifras de rendimiento publicadas representan los valores máximos. El rendimiento real puede variar en función del hardware subyacente, las condiciones de la red, la configuración del firewall y los servicios activados. El rendimiento y las capacidades pueden variar asimismo en base a la infraestructura de virtualización, y recomendamos realizar pruebas adicionales en su entorno para asegurarse de que se cumplan los requisitos de rendimiento y capacidad. Los parámetros de rendimiento se han obtenido utilizando un procesador Intel Xeon W (W-2195 2,3GHz, 4,3GHz Turbo, 24,75MB Cache) con SonicOSv 6.5.0.2 y VMware vSphere 6.5.*

Métodos de prueba:
Rendimiento máximo basado en RFC 2544 (para firewalls).
Rendimiento DPI pleno/Gateway AV/Anti-Spyware/IPS medido mediante la prueba de rendimiento HTTP estándar Spirent WebAvalanche y 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. Todas las especificaciones y prestaciones están sujetas a modificación.

Información de pedido de la serie NSv

Producto	SKU
SonicWall NSv 10 Virtual Appliance Total Secure Advanced Edition (1 año)	01-SSC-5875
SonicWall NSv 25 Virtual Appliance Total Secure Advanced Edition (1 año)	01-SSC-5923
SonicWall NSv 50 Virtual Appliance Total Secure Advanced Edition (1 año)	01-SSC-5926
SonicWall NSv 100 Virtual Appliance Total Secure Advanced Edition (1 año)	01-SSC-5929
SonicWall Nsv 200 Virtual Appliance Total Secure Advanced Edition (1 año)	01-SSC-5950
SonicWall NSv 300 Virtual Appliance Total Secure Advanced Edition (1 año)	01-SSC-5964
SonicWall NSv 400 Virtual Appliance Total Secure Advanced Edition (1 año)	01-SSC-6084
SonicWall NSv 800 Virtual Appliance Total Secure Advanced Edition (1 año)	01-SSC-6101
SonicWall NSv 1600 Virtual Appliance Total Secure Advanced Edition (1 año)	01-SSC-6109
Suscripciones de soporte y seguridad para NSv 10	**SKU**
Paquete Advanced Gateway Security Suite para NSv 10 Virtual Appliance (1 año)	01-SSC-5008
Soporte 24x7 para NSv 10 Virtual Appliance (1 año)	01-SSC-4830
Suscripciones de soporte y seguridad para NSv 25	**SKU**
Paquete Advanced Gateway Security Suite para NSv 25 Virtual Appliance (1 año)	01-SSC-5165
Soporte 24x7 para NSv 25 Virtual Appliance (1 año)	01-SSC-5161
Suscripciones de soporte y seguridad para NSv 50	**SKU**
Paquete Advanced Gateway Security Suite para NSv 50 Virtual Appliance (1 año)	01-SSC-5194
Soporte 24x7 para NSv 50 Virtual Appliance (1 año)	01-SSC-5189
Suscripciones de soporte y seguridad para NSv 100	**SKU**
Paquete Advanced Gateway Security Suite para NSv 100 Virtual Appliance (1 año)	01-SSC-5219
Soporte 24x7 para NSv 100 Virtual Appliance (1 año)	01-SSC-5216
Suscripciones de soporte y seguridad para NSv 200	**SKU**
Paquete Advanced Gateway Security Suite para NSv 200 Virtual Appliance (1 año)	01-SSC-5306
Capture Advanced Threat Protection para NSv 200 Virtual Appliance (1 año)	01-SSC-5309
Content Filtering Service Premium Business Edition para NSv 200 Virtual Appliance (1 año)	01-SSC-5335
Gateway Anti-Malware, Intrusion Prevention And Application Control para NSv 200 Virtual Appliance (1 año)	01-SSC-5364
Soporte 24x7 para NSv 200 Virtual Appliance (1 año)	01-SSC-5303
Suscripciones de soporte y seguridad para NSv 300	**SKU**
Paquete Advanced Gateway Security Suite para NSv 300 Virtual Appliance (1 año)	01-SSC-5584
Capture Advanced Threat Protection para NSv 300 Virtual Appliance (1 año)	01-SSC-5587
Content Filtering Service Premium Business Edition para NSv 300 Virtual Appliance (1 año)	01-SSC-5649
Gateway Anti-Malware, Intrusion Prevention And Application Control para NSv 300 Virtual Appliance (1 año)	01-SSC-5671
Soporte 24x7 para NSv 300 Virtual Appliance (1 año)	01-SSC-5581
Suscripciones de soporte y seguridad para NSv 400	**SKU**
Paquete Advanced Gateway Security Suite para NSv 400 Virtual Appliance (1 año)	01-SSC-5681
Capture Advanced Threat Protection para NSv 400 Virtual Appliance (1 año)	01-SSC-5684
Content Filtering Service Premium Business Edition para NSv 400 Virtual Appliance (1 año)	01-SSC-5690
Gateway Anti-Malware, Intrusion Prevention And Application Control para NSv 400 Virtual Appliance (1 año)	01-SSC-5693
Soporte 24x7 para NSv 400 Virtual Appliance (1 año)	01-SSC-5678
Suscripciones de soporte y seguridad para NSv 800	**SKU**
Paquete Advanced Gateway Security Suite para NSv 800 Virtual Appliance (1 año)	01-SSC-5737
Capture Advanced Threat Protection para NSv 800 Virtual Appliance (1 año)	01-SSC-5748
Content Filtering Service Premium Business Edition para NSv 800 Virtual Appliance (1 año)	01-SSC-5774
Gateway Anti-Malware, Intrusion Prevention And Application Control para NSv 800 Virtual Appliance (1 año)	01-SSC-5777
Soporte 24x7 para NSv 800 Virtual Appliance (1 año)	01-SSC-5709
Suscripciones de soporte y seguridad para NSv 1600	**SKU**
Paquete Advanced Gateway Security Suite para NSv 1600 Virtual Appliance (1 año)	01-SSC-5787
Capture Advanced Threat Protection para NSv 1600 Virtual Appliance (1 año)	01-SSC-5789
Content Filtering Service Premium Business Edition para NSv 1600 Virtual Appliance (1 año)	01-SSC-5801
Gateway Anti-Malware, Intrusion Prevention And Application Control para NSv 1600 Virtual Appliance (1 año)	01-SSC-5803
Soporte 24x7 para NSv 1600 Virtual Appliance (1 año)	01-SSC-5785

Acerca de nosotros

SonicWall lleva más de 25 años combatiendo la industria del crimen cibernético, defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 negocios en más de 150 países, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Para más información, consulte nuestra página Web.
www.sonicwall.com

Datasheet-NSvVirtualFirewalls-US-VG-MKTG2648

SONICWALL®