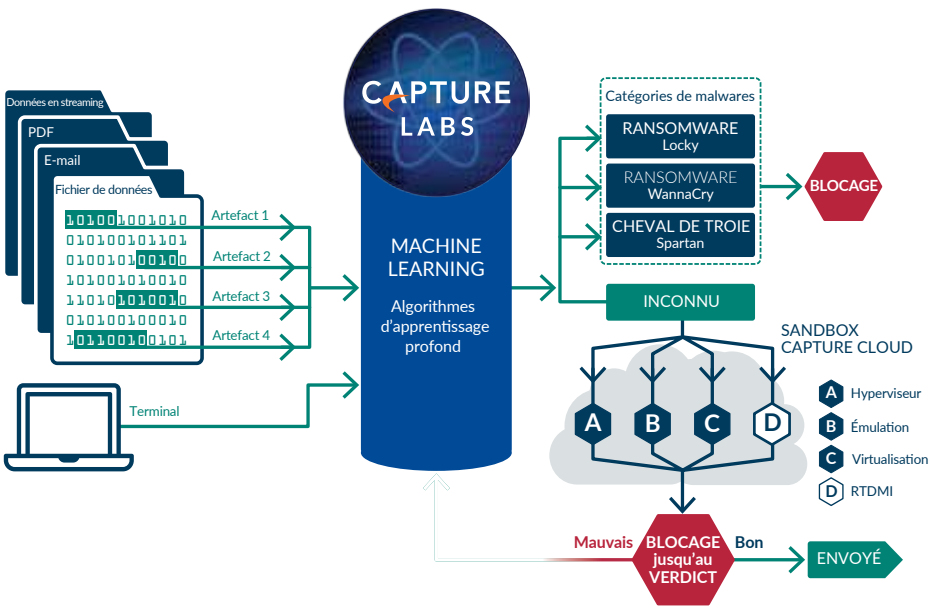
SonicWall Network Security virtual (NSv) Series

Une sécurité approfondie pour les environnements publics, privés ou Cloud hybrides

La conception, l'implémentation et le déploiement des architectures réseau modernes, comme la virtualisation et le Cloud, continuent d'être une stratégie décisive pour de nombreuses entreprises. La virtualisation du centre de données, la migration vers le Cloud, ou une combinaison des deux, ont prouvé d'importants avantages opérationnels et économiques. Les vulnérabilités dans les environnements virtuels sont toutefois bien documentées. On découvre régulièrement de nouvelles vulnérabilités qui s'accompagnent de réelles implications et de sérieux défis. Pour fournir des services d'application de manière fiable, efficace et évolutive tout en luttant contre les menaces nuisibles à toutes les parties de la structure virtuelle, notamment les machines virtuelles (VM), les charges de travail d'application et les données doivent figurer en tête de liste des priorités.

Les pare-feux SonicWall Network Security virtual (NSv) permettent aux équipes en charge de la sécurité de réduire ces types de risques et de vulnérabilités, susceptibles de sérieusement perturber les services et les opérations stratégiques de votre entreprise. Avec des outils et des services de sécurité complets, notamment technologie RFDPI (Reassembly-Free Deep Packet Inspection), contrôles de sécurité et services de mise en réseau équivalents à ce que propose un pare-feu physique SonicWall, les pare-feux NSv protègent efficacement tous les composants stratégiques de vos environnements Cloud privés/publics.

La série NSv offre un déploiement et une configuration simplifiés dans un environnement virtuel mutualisé, généralement entre réseaux virtuels. Cela permet de capturer les communications et les échanges de données entre les machines virtuelles, pour une prévention automatisée des failles, tout en établissant des mesures de contrôle d'accès strictes pour la confidentialité des données ainsi que la sécurité et l'intégrité des VM. Les menaces de sécurité (comme les attaques croisées de machines virtuelles, les attaques par canal auxiliaire, les intrusions courantes sur le réseau et les vulnérabilités des applications et des protocoles) sont parfaitement neutralisées grâce à la suite complète SonicWall de services d'inspection de sécurité[1]. L'ensemble du trafic VM est soumis à l'analyse de multiples moteurs pour détecter les menaces, notamment prévention des intrusions, antivirus de passerelle et anti-logiciels espions, antivirus Cloud, filtrage de réseaux de zombies, contrôle d'applications et sandboxing multi-moteur Capture Advanced Threat Protection.



Avantages :

Sécurité Cloud privé et public

- Visibilité complète sur la communication intra-hôte entre machines virtuelles pour la prévention des menaces
- Définition appropriée de règles de sécurité et application de ces règles dans l'environnement virtuel
- Règles fiables d'activation par application, utilisateur et appareil, quel que soit l'emplacement de la machine virtuelle
- Mise en place de zones de sécurité adéquates et d'isolements

Protection des machines virtuelles

- Protection contre les vulnérabilités zero-day avec Capture Advanced Threat Protection (ATP)
- Éviter la prise de contrôle non autorisée des systèmes virtuels
- Blocage de l'accès non autorisé aux données protégées
- Blocage des actions malveillantes et intrusives, comme la diffusion de logiciels malveillants, l'exécution de commandes de système d'exploitation, l'exploration du système de fichiers et la communication C&C
- Éviter les interruptions de service d'une partie ou de l'ensemble de l'écosystème virtuel

La sécurité par la segmentation

Afin d'assurer une efficacité optimale face aux menaces persistantes avancées (APT), la segmentation de la sécurité réseau doit installer toute une série de barrières intégrées, dynamiques et automatiques. Avec des fonctionnalités basées sur des segments, les pare-feux NSv permettent de regrouper des interfaces similaires et de leur appliquer les mêmes règles au lieu d'avoir à écrire les mêmes règles pour chaque interface. En appliquant des règles de sécurité à l'intérieur du réseau virtuel, la segmentation permet d'organiser les ressources selon différents segments et d'autoriser ou restreindre le trafic entre ces segments. L'accès aux ressources stratégiques internes peut ainsi être rigoureusement contrôlé.

La série NSv permet aussi d'appliquer automatiquement des restrictions de segmentation en fonction de critères dynamiques, comme par exemple les informations d'identité des utilisateurs, la localisation GeoIP ou encore le statut de sécurité des terminaux mobiles. Pour encore plus de sécurité, les pare-feux NSv intègrent également la commutation réseau à une vitesse multi-gigabits aux règles de sécurité des segments. Ils appliquent les règles de segments au trafic au niveau des points de commutation du réseau et gèrent de manière globale l'application de ces règles depuis un seul et même écran.

Les segments n'étant efficaces que si les mesures de sécurité qui leur sont appliquées le sont également, les pare-feux NSv appliquent un service de prévention des intrusions (IPS) pour analyser le trafic entrant et sortant sur le segment VLAN, afin de renforcer la sécurité du trafic réseau interne. Pour chaque segment, un ensemble complet de services de sécurité est mis en œuvre sur plusieurs interfaces par le biais de règles rigoureuses.

Cas d'utilisation de déploiement flexible

Grâce à une infrastructure autorisant la haute disponibilité (HA), la série NSv répond aux exigences d'évolutivité et de disponibilité définies par le SDDC (Software Defined Data Centers). Elle garantit la résilience des systèmes, la fiabilité des services et la conformité aux règlementations. Optimisée pour un vaste éventail de cas d'utilisation de déploiement publics, privés et hybrides, la série NSv peut s'adapter aux différents niveaux de service et garantir la disponibilité et la sécurité des machines virtuelles, de leurs charges utiles d'application et des données. Elle peut réaliser tout ceci à une vitesse de plusieurs Gbits/s et à faible latence.

Les entreprises bénéficient de tous les avantages de sécurité d'un pare-feu physique avec les avantages opérationnels et économiques de la virtualisation. Cela inclut l'évolutivité des systèmes, l'agilité opérationnelle, la vitesse de configuration, la simplicité de la gestion et la réduction de coûts.

Les pare-feux de la série NSv sont disponibles dans de multiples variantes virtuelles, soigneusement conçues pour un vaste éventail de cas d'utilisation de déploiement virtualisé et Cloud. Grâce à leurs performances en termes de prévention des menaces à une vitesse multi-gigabits et d'inspection du trafic chiffré, les pare-feux de la série NSv peuvent s'adapter aux augmentations de capacité et garantir la disponibilité et la sécurité des réseaux virtuels, des charges utiles d'application et des données.

Une gouvernance centrale

Les déploiements NSv sont gérés de manière centrale via SonicWall GMS[3] sur site et SonicWall Capture Security Center[3], un logiciel ouvert et évolutif de gestion de la sécurité Cloud, de surveillance, de création de rapports et d'analyse, fourni en tant que solution SaaS (Software-as-a-Service). Capture Security Center offre une visibilité, une agilité et une capacité optimales permettant de contrôler l'ensemble de l'écosystème des pare-feux virtuels et physiques SonicWall, avec davantage de clarté, de précision et de rapidité, le tout depuis un seul et même écran.

Fonctionnalités

Plateforme SonicOS

L'architecture SonicOS est au cœur de tous les pare-feux physiques et virtuels SonicWall, notamment NSv et NS*a* Series, SuperMassive™ Series et TZ Series. Reportez-vous à la fiche technique de la plateforme SonicWall SonicOS pour la liste complète des fonctionnalités.

Prévention automatisée des failles[1]

Cette fonctionnalité inclut une protection avancée complète contre les menaces, notamment prévention hautes performances des intrusions et des logiciels malveillants et sandboxing Cloud.

Sécurité en continu[1]

Les nouvelles mises à jour sont automatiquement appliquées aux pare-feux sur le terrain dotés de services de sécurité actifs et prennent effet immédiatement, sans redémarrage ni interruption.

Protection de type « zero-day »[1]

Les pare-feux NSv protègent le réseau contre les attaques de type « zero-day » avec des mises à jour constantes répondant aux dernières méthodes et techniques d'attaque et couvrant des milliers de failles.

GOUVERNANCE CENTRALE

- Faciliter la mise en place d'une solution complète de gestion de la sécurité, d'analyse, de création de rapports et de mise en conformité afin d'unifier votre programme de protection de la sécurité réseau
- Automatiser et mettre en corrélation les workflows pour coordonner parfaitement la stratégie de gouvernance de la sécurité, de mise en conformité et de gestion des risques

CONFORMITÉ

- Satisfaire aux exigences des instances de règlementation et des auditeurs via des rapports automatiques de sécurité PCI, HIPAA et SOX
- Personnaliser toute combinaison de données de sécurité vérifiables pour faciliter la mise en conformité avec des exigences spécifiques

GESTION DES RISQUES

- Évoluer rapidement et favoriser la collaboration, la communication et les connaissances sur toute la structure de sécurité partagée
- Prendre des décisions avisées en matière de règles de sécurité, sur la base d'informations sur les menaces consolidées et prioritaires, pour un niveau supérieur de sécurité et d'efficacité

La plateforme GMS fournit une approche globale en matière de gouvernance de la sécurité, de mise en conformité et de gestion des risques.

API de menaces

La série NSv permet de recevoir tout type de flux de renseignements propriétaires, d'OEM ou de fournisseurs tiers et de les exploiter pour combattre les menaces évoluées : zero-day, initié malveillant, identifiants compromis, ransomwares et menaces persistantes avancées.

Protection par zone

La série NSv renforce la sécurité interne en segmentant le réseau en plusieurs zones de sécurité avec service de prévention des intrusions, ce qui empêche les menaces de se propager entre ces zones. La création et l'application de règles d'accès et de règles NAT au trafic traversant les différentes interfaces permettent d'autoriser ou de refuser l'accès réseau interne ou externe en fonction de différents critères.

Surveillance et contrôle des applications[1]

Avec des règles spécifiques aux applications, les pare-feux NSv permettent un contrôle granulaire du trafic réseau au niveau utilisateurs, adresses e-mail, horaires et sous-réseaux IP. Ils contrôlent les applications personnalisées en créant des signatures basées sur leurs paramètres ou schémas spécifiques dans leurs communications réseau. L'accès réseau interne ou externe est autorisé ou refusé en fonction de différents critères.

Prévention des fuites de données

Avec la série NSv, il est possible d'analyser des flux de données pour rechercher des mots clés. Cela restreint le transfert de fichiers selon le nom ou le type, de pièces jointes, également selon le type, d'e-mails portant sur un sujet particulier, ainsi que d'e-mails ou de pièces jointes contenant certains mots-clés ou séquences d'octets spécifiques.

Gestion de la bande passante pour la couche applicative

Grâce à la surveillance des paquets, les pare-feux NSv offrent la possibilité de choisir parmi plusieurs paramètres de gestion de la bande passante réseau afin d'en réduire l'utilisation par une application. Cela permet de mieux contrôler le réseau.

Communication sécurisée

La série NSv garantit que l'échange de données entre les groupes de machines virtuelles s'effectue de manière sécurisée, y compris isolement, confidentialité, intégrité et contrôle du flux d'informations au sein de ces réseaux via la segmentation.

Contrôle d'accès

Avec la série NSv, seules les machines virtuelles respectant un ensemble donné de conditions sont en mesure d'accéder aux données qui appartiennent à une autre machine via l'utilisation de VLAN.

Authentification des utilisateurs

Les pare-feux NSv permettent de créer des règles afin de contrôler ou de restreindre l'accès aux machines virtuelles et aux charges utiles par les utilisateurs non autorisés.

Confidentialité des données

Les pare-feux NSv bloquent le vol d'informations et l'accès non autorisé aux données et services protégés

Résilience et disponibilité des réseaux virtuels

Les pare-feux NSv permettent d'éviter toute perturbation ou dégradation des services applicatifs et des communications.

Sécurité et intégrité des systèmes

Les pare-feux NSv bloquent la prise de contrôle non autorisée des systèmes et services des machines virtuelles.

Mécanismes de validation, d'inspection et de surveillance du trafic

Les pare-feux NSv détectent les anomalies et les comportements malveillants et bloquent les attaques visant les charges utiles de machines virtuelles.

Options de déploiement[2]

Les pare-feux NSv peuvent être déployés sur de nombreuses plateformes virtualisées et Cloud pour différents cas d'utilisation de sécurité Cloud privé/public.

[1] Nécessite un abonnement SonicWall Advanced Gateway Security Services (AGSS).
[2] La prise en charge VMI (Virtual Machine Image) pour MS Hyper-V, Amazon et MS Azure sera assurée dans une prochaine version.
[3] SonicWall Global Management System et Capture Security Center nécessitent une licence et un abonnement distincts.

Spécifications système NSv Series

Pare-feu – Général	NSv 10	NSv 25	NSv 50	NSv 100
Système d'exploitation	SonicOS			
Hyperviseurs pris en charge	VMware ESXi v5.5 / v6.0 / v6.5			
vCPU prises en charge max.	2	2	2	2
Nb. cœurs max. gestion/DataPlane	1/1	1/1	1/1	1/1
Mémoire min.	4 Go	4 Go	4 Go	4 Go
IP/nœuds pris en charge	10	25	50	100
Stockage minimum	60 Go			
Utilisateurs de l'authentification unique (SSO)	25	50	100	100
Journalisation	Analyzer, Local Log, Syslog			
Haute disponibilité	Active/passive			
Performances pare-feu/VPN				
Débit d'inspection du pare-feu	2 Gbit/s	2,5 Gbit/s	3 Gbit/s	3,5 Gbit/s
Débit DPI complet (GAV/GAS/IPS)	450 Mbit/s	550 Mbit/s	650 Mbit/s	750 Mbit/s
Débit d'inspection des applications	1 Gbit/s	1,25 Gbit/s	1,5 Gbit/s	1,75 Gbit/s
Débit IPS	1 Gbit/s	1,25 Gbit/s	1,5 Gbit/s	1,75 Gbit/s
Débit d'inspection des logiciels malveillants	450 Mbit/s	550 Mbit/s	650 Mbit/s	750 Mbit/s
Débit IMIX	750 Mbit/s	850 Mbit/s	950 Mbit/s	1 100 Mbit/s
Débit DPI TLS/SSL	650 Mbit/s	750 Mbit/s	850 Mbit/s	950 Mbit/s
Débit VPN	500 Mbit/s	550 Mbit/s	600 Mbit/s	650 Mbit/s
Connexions par seconde	1 800	5 000	8 000	10 000
Nb. de connexions max. (SPI)	10 000	50 000	125 000	150 000
Nb. de connexions max. (DPI)	10 000	50 000	100 000	125 000
Connexions DPI TLS/SSL	500	1 000	2 000	4 000
VPN				
Tunnels VPN site à site	10	10	25	50
Clients VPN IPSec	10	10	25	25
Clients VPN SSL NetExtender (max.)	2 (10)	2 (25)	2 (25)	2 (25)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v			
VPN basé sur le routage	RIP, OSPF, BGP			
Gestion de réseau				
Attribution d'adresses IP	Statique, DHCP, serveur DHCP interne, relais DHCP			
Modes NAT	1:1, plusieurs:1, 1:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT			
Interfaces VLAN	25	25	50	50
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage basé sur des règles			
QoS	Priorité, bande passante max., garantie, marquage DSCP, 802.1p			
Authentification	XAUTH/RADIUS, Active Directory, authentification unique (SSO), LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix			
VoIP	H323-v1-5 complet, SIP			
Normes	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			

Caractéristiques des pare-feux NSv Series (suite)

Pare-feu – Général	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Système d'exploitation	SonicOS				
Hyperviseurs pris en charge	VMware ESXi v5.5 / v6.0 / v6.5				
vCPU prises en charge max.	2	3	4	8	16
Nb. cœurs max. gestion/DataPlane	1/1	1/2	1/3	1/7	1/15
Mémoire min.	6 Go	8 Go	8 Go	10 Go	12 Go
IP/nœuds pris en charge	Illimité	Illimité	Illimité	Illimité	Illimité
Stockage minimum	60 Go				
Utilisateurs de l'authentification unique (SSO)	500	5 000	10 000	15 000	20 000
Journalisation	Analyzer, Local Log, Syslog				
Haute disponibilité	Active/passive				
Performances pare-feu/VPN					
Débit d'inspection du pare-feu	4,1 Gbit/s	5,9 Gbit/s	7,8 Gbit/s	13,9 Gbit/s	17,2 Gbit/s
Débit DPI complet (GAV/GAS/IPS)	900 Mbit/s	1,6 Gbit/s	2,2 Gbit/s	4,0 Gbit/s	6,4 Gbit/s
Débit d'inspection des applications	2,3 Gbit/s	3,4 Gbit/s	4,1 Gbit/s	5,5 Gbit/s	6,4 Gbit/s
Débit IPS	2,3 Gbit/s	3,4 Gbit/s	4,1 Gbit/s	5,5 Gbit/s	6,7 Gbit/s
Débit d'inspection des logiciels malveillants	900 Mbit/s	1,6 Gbit/s	2,2 Gbit/s	4,0 Gbit/s	6,6 Gbit/s
Débit IMIX	1,5 Gbit/s	2,3 Gbit/s	2,8 Gbit/sv	4,2 Gbit/s	5,3 Gbit/s
Débit DPI TLS/SSL	1,1 Gbit/s	1,2 Gbit/s	1,8 Gbit/s	3,4 Gbit/s	5,1 Gbit/s
Débit VPN	750 Mbit/s	1,4 Gbit/s	1,9 Gbit/s	4,2 Gbit/s	8,4 Gbit/s
Connexions par seconde	13 760	24 360	32 270	75 640	125 000
Nb max. de connexions (SPI)	225 000	1 Mio	1,5 Mio	3 Mio	4 Mio
Nb max. de connexions (DPI)	125 000	500 000	1,5 Mio	2 Mio	2,5 Mio
Connexions TLS/DPI	8 000	12 000	20 000	30 000	50 000
VPN					
Tunnels VPN site à site	75	100	6000	10 000	25 000
Clients VPN IPSec (max.)	50 (1 000)	50 (1 000)	2000 (4 000)	2000 (6 000)	2000 (10 000)
Clients VPN SSL NetExtender (max.)	2 (100)	2 (100)	2 (100)	2 (100)	2 (100)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B, Common Access Card (CAC)				
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v				
VPN basé sur le routage	RIP, OSPF, BGP				
Gestion de réseau					
Attribution d'adresses IP	Statique, DHCP, serveur DHCP interne, relais DHCP				
Modes NAT	1:1, plusieurs:1, 1:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT				
Interfaces VLAN	50	256	500	512	512
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage basé sur des règles				
QoS	Priorité, bande passante max., garantie, marquage DSCP, 802.1p				
Authentification	XAUTH/RADIUS, Active Directory, authentification unique (SSO), LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix				
VoIP	H323-v1-5 complet, SIP				
Normes	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				

[1] *Les chiffres de performance publiés correspondent à la spécification et les performances réelles peuvent varier en fonction du matériel sous-jacent, des conditions du réseau, de la configuration du pare-feu et des services activés. Les performances et les capacités peuvent également varier selon la virtualisation sous-jacente ; nous recommandons des tests supplémentaires dans votre environnement pour garantir le respect de vos exigences en termes de performances et de capacités. Les indicateurs de performance ont été observés avec le processeur Intel Xeon W (W-2195 2,3 GHz, 4,3GHz Turbo, 24,75 MB cache) et SonicOSv 6.5.0.2 avec VMware vSphere 6.5.*

Méthodes de test :
Performances maximales basées sur RFC 2544 (pour pare-feu).
Débit DPI/antivirus de passerelle/anti-logiciels espions/IPS complet mesuré en utilisant les tests de performance HTTP Spirent WebAvalanche et les outils de test Ixia conformes aux standards actuels.
Tests réalisés avec plusieurs flux sur plusieurs paires de ports.
Débit VPN mesuré à l'aide du trafic UDP avec une taille de paquet de 1 418 octets et conformément à la norme RFC 2544. Sous réserve de modification des spécifications et caractéristiques.

Informations de commande des pare-feux NSv Series

Produit	Référence
Appliance virtuelle SonicWall NSv 10 Total Secure Advanced Edition (1 an)	01-SSC-5875
Appliance virtuelle SonicWall NSv 25 Total Secure Advanced Edition (1 an)	01-SSC-5923
Appliance virtuelle SonicWall NSv 50 Total Secure Advanced Edition (1 an)	01-SSC-5926
Appliance virtuelle SonicWall NSv 100 Total Secure Advanced Edition (1 an)	01-SSC-5929
Appliance virtuelle SonicWall Nsv 200 Total Secure Advanced Edition (1 an)	01-SSC-5950
Appliance virtuelle SonicWall NSv 300 Total Secure Advanced Edition (1 an)	01-SSC-5964
Appliance virtuelle SonicWall NSv 400 Total Secure Advanced Edition (1 an)	01-SSC-6084
Appliance virtuelle SonicWall NSv 800 Total Secure Advanced Edition (1 an)	01-SSC-6101
Appliance virtuelle SonicWall NSv 1600 Total Secure Advanced Edition (1 an)	01-SSC-6109
Abonnements de support et de sécurité pare-feu NSv 10	**Référence**
Offre Advanced Gateway Security Suite pour appliance virtuelle NSv 10 (1 an)	01-SSC-5008
Support 24x7 pour appliance virtuelle NSv 10 (1 an)	01-SSC-4830
Abonnements de support et de sécurité pare-feu NSv 25	**Référence**
Offre Advanced Gateway Security Suite pour appliance virtuelle NSv 25 (1 an)	01-SSC-5165
Support 24x7 pour appliance virtuelle NSv 25 (1 an)	01-SSC-5161
Abonnements de support et de sécurité pare-feu NSv 50	**Référence**
Offre Advanced Gateway Security Suite pour appliance virtuelle NSv 50 (1 an)	01-SSC-5194
Support 24x7 pour appliance virtuelle NSv 50 (1 an)	01-SSC-5189
Abonnements de support et de sécurité pare-feu NSv 100	**Référence**
Offre Advanced Gateway Security Suite pour appliance virtuelle NSv 100 (1 an)	01-SSC-5219
Support 24x7 pour appliance virtuelle NSv 100 (1 an)	01-SSC-5216
Abonnements de support et de sécurité pare-feu NSv 200	**Référence**
Offre Advanced Gateway Security Suite pour appliance virtuelle NSv 200 (1 an)	01-SSC-5306
Capture Advanced Threat Protection pour appliance virtuelle NSv 200 (1 an)	01-SSC-5309
Content Filtering Service Premium Business Edition pour appliance virtuelle NSv 200 (1 an)	01-SSC-5335
Anti-logiciels malveillants de passerelle, prévention des intrusions et contrôle des applications pour appliance virtuelle NSv 200 (1 an)	01-SSC-5364
Support 24x7 pour appliance virtuelle NSv 200 (1 an)	01-SSC-5303
Abonnements de support et de sécurité pare-feu NSv 300	**Référence**
Offre Advanced Gateway Security Suite pour appliance virtuelle NSv 300 (1 an)	01-SSC-5584
Capture Advanced Threat Protection pour appliance virtuelle NSv 300 (1 an)	01-SSC-5587
Content Filtering Service Premium Business Edition pour appliance virtuelle NSv 300 (1 an)	01-SSC-5649
Anti-logiciels malveillants de passerelle, prévention des intrusions et contrôle des applications pour appliance virtuelle NSv 300 (1 an)	01-SSC-5671
Support 24x7 pour appliance virtuelle NSv 300 (1 an)	01-SSC-5581
Abonnements de support et de sécurité pare-feu NSv 400	**Référence**
Offre Advanced Gateway Security Suite pour appliance virtuelle NSv 400 (1 an)	01-SSC-5681
Capture Advanced Threat Protection pour appliance virtuelle NSv 400 (1 an)	01-SSC-5684
Content Filtering Service Premium Business Edition pour appliance virtuelle NSv 400 (1 an)	01-SSC-5690
Anti-logiciels malveillants de passerelle, prévention des intrusions et contrôle des applications pour appliance virtuelle NSv 400 (1 an)	01-SSC-5693
Support 24x7 pour appliance virtuelle NSv 400 (1 an)	01-SSC-5678
Abonnements de support et de sécurité pare-feu NSv 800	**Référence**
Offre Advanced Gateway Security Suite pour appliance virtuelle NSv 800 (1 an)	01-SSC-5737
Capture Advanced Threat Protection pour appliance virtuelle NSv 800 (1 an)	01-SSC-5748
Content Filtering Service Premium Business Edition pour appliance virtuelle NSv 800 (1 an)	01-SSC-5774
Anti-logiciels malveillants de passerelle, prévention des intrusions et contrôle des applications pour appliance virtuelle NSv 800 (1 an)	01-SSC-5777
Support 24x7 pour appliance virtuelle NSv 800 (1 an)	01-SSC-5709
Abonnements de support et de sécurité pare-feu NSv 1600	**Référence**
Offre Advanced Gateway Security Suite pour appliance virtuelle NSv 1600 (1 an)	01-SSC-5787
Capture Advanced Threat Protection pour appliance virtuelle NSv 1600 (1 an)	01-SSC-5789
Content Filtering Service Premium Business Edition pour appliance virtuelle NSv 1600 (1 an)	01-SSC-5801
Anti-logiciels malveillants de passerelle, prévention des intrusions et contrôle des applications pour appliance virtuelle NSv 1600 (1 an)	01-SSC-5803
Support 24x7 pour appliance virtuelle NSv 1600 (1 an)	01-SSC-5785

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

Datasheet-NSvVirtualFirewalls-US-VG-MKTG2648

SONICWALL®