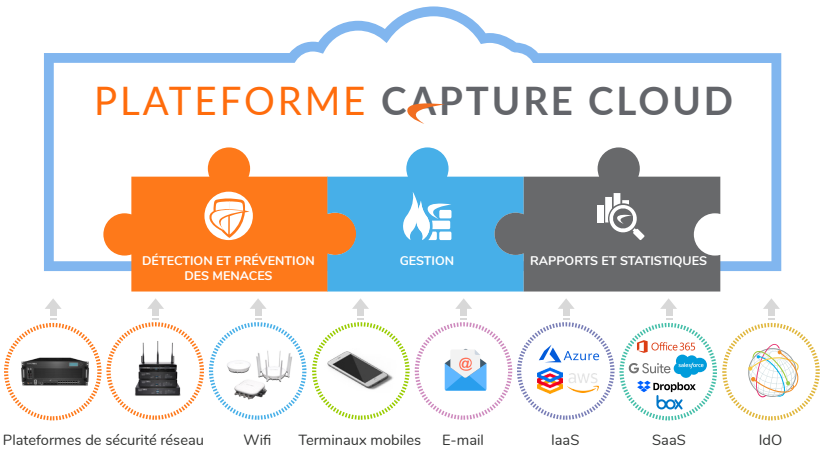
Pare-feu de la série Network Security virtual (NSv) de SonicWall

Sécurité de nouvelle génération pour les environnements cloud publics, privés ou hybrides

La conception, la mise en œuvre et le déploiement d'architectures réseau modernes, telles que la virtualisation et le cloud, restent une stratégie innovante pour de nombreuses organisations. La virtualisation du centre de données, la migration vers le cloud, ou une combinaison des deux, offrent des avantages opérationnels et économiques considérables. Les vulnérabilités au sein des environnements virtuels sont toutefois bien documentées. De nouvelles vulnérabilités entraînant de graves implications et défis en matière de sécurité sont régulièrement découvertes. Pour garantir une livraison sûre, efficace et évolutive des applications et services tout en continuant à lutter contre les menaces dangereuses à tous les niveaux du cadre virtuel, y compris les machines virtuelles (MV), les charges de travail applicatives et les données doivent être des priorités absolues.

Le pare-feu de la série Network Security virtual (NSv) de SonicWall aide les équipes de sécurité à réduire ces risques de sécurité et vulnérabilités, qui pourraient gravement perturber les services et opérations critiques de votre entreprise. Les pare-feu virtuels de nouvelle génération NSv intègrent deux technologies de sécurité avancées pour fournir une prévention de pointe des menaces, permettant à votre réseau de garder une longueur d'avance. La technologie Real-Time Deep Memory Inspection (RTDMI™) en instance de brevet de SonicWall améliore notre service sandbox Capture Advanced Threat Protection (ATP) multi-moteur primé. Le moteur RTDMI détecte et bloque proactivement les logiciels malveillants de masse, les attaques zero-day et autres logiciels malveillants inconnus en inspectant directement dans la mémoire. Grâce à son architecture en temps réel, la technologie SonicWall RTDMI est précise, minimise les faux positifs et identifie et atténue les attaques sophistiquées au cours desquelles les armes sont exposées pendant moins de 100 nanosecondes. En parallèle, le moteur RFDPI® (Reassembly-Free Deep Packet Inspection) single-pass breveté* de SonicWall examine chaque octet de chaque paquet, inspectant simultanément le trafic entrant et sortant sur le pare-feu.



Avantages

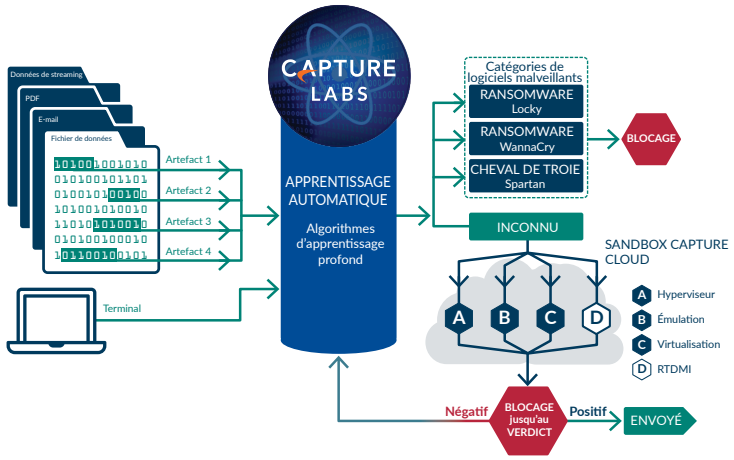
Sécurité des clouds publics et privés

- Pare-feu de nouvelle génération avec capacités automatisées de détection et de prévention des intrusions en temps réel
- Technologie RTDMI (Real-Time Deep Memory Inspection) en instance de brevet
- Technologie RFDPI (Reassembly-Free Deep Packet Inspection) brevetée
- Visibilité et contrôle complets de bout en bout
- Surveillance et contrôle des applications
- Sécurité par segmentation et zones de sécurité
- Prise en charge des plateformes de cloud privé (ESXi, Hyper-V) et de cloud public (AWS, Azure)
- Licences BYOL et PAYG

Protection des machines virtuelles

- Protection contre les menaces zero-day avec Capture ATP
- Confidentialité des données
- Communications sécurisées avec prévention des fuites de données
- Validation, contrôle et surveillance du trafic
- Sécurité et intégrité du système
- Résilience et disponibilité des réseaux virtuels

** Brevets américains 7 310 815 ; 7 600 257 ; 7 738 380 ; 7 835 361 ; 7 991 723*



Le pare-feu de la série NSv fournit la détection et la prévention en temps réel automatisées des intrusions dont les organisations ont besoin, grâce à des technologies d'apprentissage profond innovantes sur la plateforme Capture Cloud de SonicWall. Cette plateforme assure la prévention des menaces et la gestion du réseau dans le cloud, à quoi s'ajoutent des fonctionnalités de reporting et d'analyse pour les entreprises de toute taille. Cette plateforme consolide les renseignements sur les menaces à partir de plusieurs sources, dont notre service Capture ATP, ainsi que plus de 1 million de capteurs SonicWall répartis dans le monde entier. Tirant parti de la plateforme Capture Cloud SonicWall en plus de fonctionnalités (prévention des intrusions, anti-logiciels malveillants et filtrage des URL/Web notamment), le pare-feu de la série NSv bloque même les menaces les plus furtives à la passerelle.

Le pare-feu NSv offre un déploiement et une configuration simplifiés dans un environnement virtuel, généralement entre réseaux virtuels ou clouds privés virtuels. Cela lui permet de capturer les communications et les échanges de données entre les machines virtuelles en vue de la prévention automatisée des intrusions, tout en établissant des mesures de contrôle d'accès strictes pour la confidentialité des données et la sécurité et l'intégrité des machines virtuelles. Les menaces de sécurité (telles que les attaques inter-machines virtuelles ou par canal auxiliaire, les intrusions communes basées sur le réseau et les vulnérabilités des applications et des protocoles) sont neutralisées grâce à la suite complète de services d'inspection de sécurité de SonicWall[1]. Tout le trafic des machines virtuelles est soumis à de multiples moteurs d'analyse des menaces, notamment la prévention des intrusions, les logiciels antivirus et anti-espions de passerelle, les logiciels antivirus de cloud, le filtrage de réseaux de zombies, le contrôle des applications et le service sandbox multimoteur Capture ATP avec la technologie RTDMI.

Segmentation de la sécurité

Pour assurer une efficacité optimale contre les menaces persistantes avancées, la segmentation de la sécurité réseau doit appliquer un ensemble intégré de barrières dynamiques et applicables aux menaces avancées. Grâce aux capacités de sécurité basées sur les segments, le pare-feu NSv peut regrouper des interfaces similaires et leur appliquer les mêmes politiques plutôt que de devoir écrire la même politique pour chaque interface. En appliquant des politiques de sécurité à l'intérieur du réseau virtuel, la segmentation peut être configurée pour organiser les ressources réseau en différents segments et autoriser ou restreindre le trafic entre ces segments. De cette manière, l'accès aux ressources critiques internes peut être strictement contrôlé.

Le pare-feu NSv applique automatiquement des restrictions de segmentation sur base de critères dynamiques, tels que les informations d'identification de l'utilisateur, la localisation géo-IP et le niveau de sécurité des terminaux mobiles. Pour une sécurité étendue, le pare-feu NSv est également capable d'intégrer la commutation réseau multi-gigabit dans sa politique de segmentation de sécurité et son application. Il dirige la politique de segmentation vers le trafic aux points de commutation sur l'ensemble du réseau et permet de gérer globalement l'application de la sécurité des segments à partir d'un écran unique.

Puisque l'efficacité des segments dépend de la sécurité applicable entre eux, le pare-feu NSv applique un système de prévention des intrusions (IPS) pour analyser le trafic entrant et sortant sur le segment VLAN afin d'améliorer la sécurité du trafic réseau interne. Pour chaque segment, il met en œuvre un ensemble complet de services de sécurité sur des interfaces multiples en fonction d'une politique applicable.

Déploiement flexible – Cas d'utilisation

Grâce à une infrastructure autorisant la haute disponibilité, le pare-feu NSv répond aux exigences d'évolutivité et de disponibilité définies par les centres de données définis par logiciel. Il garantit la résilience du système, la fiabilité du service et la conformité réglementaire. Optimisé pour un large éventail de cas d'utilisation de déploiements publics, privés et hybrides, le pare-feu NSv peut s'adapter aux changements de niveau de service et garantir la disponibilité et la sécurité des machines virtuelles, des charges de travail applicatives et des actifs de données. Et il peut réaliser tout cela à une vitesse multi-Gbit/s avec une faible latence.

Les organisations tirent parti de tous les avantages de sécurité d'un pare-feu physique, avec les avantages opérationnels et économiques de la virtualisation. Ceux-ci comprennent l'évolutivité du système, l'agilité opérationnelle, la rapidité de mise à disposition, une gestion simplifiée et une réduction des coûts.

Le pare-feu de la série NSv est disponible en plusieurs versions virtuelles soigneusement conditionnées pour un large éventail de cas d'utilisation de déploiement cloud et virtualisé. Grâce à la prévention des menaces multi-gigabit et à l'inspection du trafic chiffré de haute performance, le pare-feu de la série NSv s'adapte aux augmentations de niveau de capacité et assure la sécurité des réseaux virtuels et clouds privés virtuels. La série garantit également la disponibilité et la sécurité des charges de travail applicatives et des actifs de données.

Gouvernance centrale

Les déploiements NSv peuvent être gérés de manière centralisée, soit sur site avec Global Management System (GMS²) de SonicWall, soit avec Capture Security Center², la plateforme ouverte et évolutive de SonicWall pour la gestion, la surveillance, le reporting et l'analyse de la sécurité du cloud, proposée en tant que service économique.

Capture Security Center fournit la meilleure solution possible en termes de visibilité, d'agilité et de capacité à gérer l'ensemble de l'écosystème des pare-feu virtuels et physiques SonicWall avec plus de clarté, de précision et de rapidité, de manière optimale depuis un seul et même écran.

Moteur de règles unifié avec SonicOS 7

Le moteur de règles unifié Unified Policy Engine de SonicWall offre une gestion intégrée de diverses politiques de sécurité sur les pare-feu SonicWall virtuels et sur site, à commencer par la série NSv.

GOUVERNANCE CENTRALE

- Dotez-vous d'un cheminement facile vers une gestion complète de la sécurité, un reporting analytique et la conformité pour unifier votre programme de défense de la sécurité du réseau
- Automatisez et corrélez les flux de travail pour aboutir à une gouvernance de la sécurité, une stratégie de conformité et de gestion des risques entièrement coordonnées

CONFORMITÉ

- Élaborez des rapports de sécurité PCI, HIPAA et SOX automatiques pour satisfaire les attentes des organismes de réglementation et des auditeurs
- Personnalisez toute combinaison de données de sécurité auditables pour vous faciliter la transition vers des réglementations de conformité spécifiques

GESTION DES RISQUES

- Réagissez rapidement et incitez à la collaboration, à la communication et au partage de connaissances dans un cadre de sécurité commun
- Prenez des décisions éclairées en matière de politique de sécurité sur la base d'informations disponibles en temps utile et consolidées sur les menaces afin d'améliorer l'efficacité de la sécurité

GMS propose une approche globale de la gouvernance de la sécurité, de la conformité et de la gestion des risques

Le moteur est doté d'une nouvelle interface Web qui prend en charge une approche radicalement différente, et où l'accent est mis sur la conception centrée sur l'utilisateur.

Cela permet une configuration intuitive des politiques de sécurité contextuelles par le biais d'alertes exploitables, avec une simplicité « pointer et cliquer ».

Cette nouvelle interface est également visuellement plus attrayante que l'interface classique. Avec l'affichage du pare-feu sur un seul écran, l'interface présente à l'utilisateur des informations sur l'efficacité des différentes règles de sécurité.

L'utilisateur est en mesure de modifier en toute simplicité les règles prédéfinies pour les logiciels antivirus et antispyware, le filtrage du contenu, la prévention des intrusions, le filtrage géo-IP et l'inspection approfondie des paquets du trafic chiffré.

Grâce au moteur Unified Policy Engine, SonicWall offre une expérience simplifiée qui permet de réduire les erreurs de configuration et le temps de déploiement pour une meilleure stratégie globale en matière de sécurité.

Licences flexibles

NSv prend en charge les licences Bring Your Own License (BYOL) et Pay As You Go (PAYG). La licence BYOL pour NSv peut être achetée directement auprès de SonicWall, d'un partenaire ou d'un revendeur. Quant à la licence PAYG, elle est achetée directement auprès d'AWS Marketplace. Ce type de licence est une licence basée sur l'utilisation, pour laquelle le paiement est effectué à l'utilisation, et établi sur une base horaire ou annuelle.

Fonctionnalités

Plateforme SonicOS
L'architecture SonicOS est au cœur de chaque pare-feu SonicWall physique et virtuel, notamment les séries NSv et NSa, la série SuperMassive et la série TZ. Consultez la fiche technique de la plateforme SonicWall SonicOS pour obtenir la liste complète des fonctionnalités et des capacités.

Prévention automatisée des intrusions[1]
La série NSv offre une protection avancée complète contre les menaces, y compris une prévention haute performance des intrusions et des logiciels malveillants, et un sandboxing basé sur le cloud avec la technologie RTDMI de SonicWall.

Mises à jour de sécurité en continu[1]
La série NSv offre une protection des mouvements latéraux ainsi que du trafic entrant et sortant. Les nouvelles mises à jour sont automatiquement appliquées aux pare-feu dotés de services de sécurité actifs et prennent effet immédiatement, sans redémarrage ni interruption.

Protection de type « zero-day »[1]
La série NSv offre une protection 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.

Menace API
La série NSv reçoit tout type de flux de renseignements propriétaires, d'OEM ou de fournisseurs tiers et les exploite 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 permettant de segmenter le réseau en plusieurs zones de sécurité avec prévention des intrusions, empêchant les menaces de se propager entre ces zones. En créant et en appliquant des règles d'accès et des politiques NAT au trafic qui circule entre les différentes interfaces, le pare-feu peut autoriser ou refuser l'accès au réseau interne ou externe en fonction de différents critères.

Surveillance et contrôle des applications[1]
La série NSv offre un contrôle granulaire sur le trafic réseau au niveau des utilisateurs, des adresses électroniques, des calendriers et des sous-réseaux IP grâce à des politiques spécifiques aux applications. Elle contrôle les applications personnalisées en créant des signatures basées sur des paramètres spécifiques ou des schémas particuliers à une application. L'accès au réseau interne ou externe est autorisé ou refusé en fonction de différents critères.

Prévention des fuites de données
La série NSv permet d'analyser les flux de données afin d'identifier des mots-clés. Cela limite le transfert de certains noms de fichiers, types de fichiers, pièces jointes, types de pièces jointes, e-mails avec certains objets, et e-mails ou pièces jointes avec certains mots-clés ou schémas d'octets.

Gestion de la bande passante de la couche applicative
La série NSv peut sélectionner différents paramètres de gestion de la bande passante réseau afin de réduire l'utilisation de la bande passante du réseau par une application grâce à un moniteur de paquets, ce qui offre un contrôle supplémentaire sur le réseau.

Communications sécurisées
La série NSv permet de s'assurer que l'échange de données entre les groupes de machines virtuelles est effectué en toute sécurité, y compris l'isolement, la confidentialité, l'intégrité et le contrôle des flux d'informations au sein de ces réseaux via l'utilisation de la segmentation.

[1] *Requiert un abonnement aux SonicWall Advanced Gateway Security Services (AGSS).*
[2] *SonicWall Global Management System et Capture Security Center requièrent une licence ou un abonnement séparé.*

Contrôle des accès
La série NSv fait en sorte que seules les MV qui répondent à un ensemble de conditions donné puissent accéder à des données appartenant à une autre MV en utilisant des VLAN.

Authentification des utilisateurs
La série NSv crée des politiques pour contrôler ou restreindre l'accès aux MV et à la charge de travail par des utilisateurs non autorisés.

Confidentialité des données
La série NSv empêche le vol d'informations et l'accès illégitime aux données et services protégés.

Résilience et disponibilité des réseaux virtuels
La série NSv empêche la perturbation ou la dégradation des services applicatifs et des communications.

Sécurité et intégrité du système
La série NSv bloque la prise de contrôle non autorisée des systèmes et services des MV.

Mécanismes de validation, de contrôle et de surveillance du trafic
La série NSv repère les irrégularités et les comportements malveillants afin de bloquer les attaques ciblant les charges de travail des MV.

Options de déploiement
La série NSv peut être déployée sur une grande variété de plateformes virtualisées et cloud pour divers cas d'utilisation de sécurité cloud privé ou public.

Modèles de licences flexibles
SonicWall propose des modèles de licences perpétuelles et non perpétuelles. Le modèle de licences perpétuelles est un modèle opérationnel traditionnel selon lequel les licences de pare-feu et des services de sécurité doivent être achetées séparément. Par conséquent, ces licences expirent séparément. Le modèle de licences non perpétuelles est un modèle unique selon lequel les licences de pare-feu et des services de sécurité sont regroupées et expirent en même temps. Pour les déploiements sur cloud public, des licences perpétuelles et non perpétuelles sont disponibles selon le modèle « Bring Your Own License » (BYOL).

Le modèle de licences non perpétuelles ou par abonnement de SonicWall offre la souplesse et la simplicité, car une seule référence regroupe le logiciel de pare-feu et les services de sécurité. Ce modèle est disponible à la fois pour les offres de cloud privé (ESXi et Hyper-V) et de cloud public (AWS, Azure). Des notifications d'expiration des services sont envoyées avant l'expiration des services.

Le modèle de licences non perpétuelles est disponible en trois versions sur une période d'un an : abonnement IPS/App Control, abonnement TotalSecure et abonnement TotalSecure Advanced. En fonction des niveaux d'offre, le logiciel NSv est groupé dans une combinaison de solutions comprenant le système de prévention des intrusions (IPS), le contrôle des applications, l'assistance, Capture Security Center (CSC), Comprehensive Gateway Security Suite (CGSS) ou Advanced Gateway Security Suite (AGSS).

Spécifications système des pare-feu de la série NSv

GÉNÉRALITÉS DES PARE-FEU	NSv 10	NSv 25	NSv 50	NSv 100
Système d'exploitation	SonicOS[1]			
Hyperviseurs pris en charge	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2012 / 2016, KVM Ubuntu 16.04 / CentOS 7			
Plateformes de cloud public prises en charge (type d'instance)	AWS (c5.large), Azure (Std D2 v2)			
Licences	BYOL, PAYG[2]			
Nombre maximum de CPU virtuels pris en charge	2	2	2	2
Nombre d'interfaces (ESXi/Hyper-V/KVM)	8/8/8	8/8/8	8/8/8	8/8/8
Nombre maximum de cœurs de gestion/de plan de données	1/1	1/1	1/1	1/1
Mémoire minimum[3]	4 Go	4 Go	4 Go	4 Go
Mémoire maximum[4]	6 Go	6 Go	6 Go	6 Go
Adresses 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	Mode actif/passif			
PERFORMANCES PARE-FEU/VPN[6]	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Débit d'inspection des pare-feu	2 Gbit/s	2,5 Gbit/s	3 Gbit/s	3,5 Gbit/s
Débit DPI total (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
Connexions maximales (SPI)	2 500	6 250	12 500	25 000
Nombre maximum de connexions (DPI)	2 500	6 250	12 500	25 000
Connexions DPI TLS/SSL	500	1 000	2 000	4 000
VPN	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Tunnels VPN site à site	10	10	25	50
Clients VPN IPSec	10(10)	10(10)	10(25)	10(25)
Clients VPN SSL inclus[7]	2	2	2	2
Clients VPN SSL (maximum)[7]	50	50	50	50
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B, carte CAC (Common Access Card)			
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v			
VPN basé sur le routage	RIP, OSPF, BGP			
GESTION DE RÉSEAU	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Attribution d'adresses IP	Statique, DHCP, serveur DHCP interne, relais DHCP			
Modes NAT	1 à 1, plusieurs à 1, 1 à plusieurs, NAT flexible (adresses IP superposées), PAT			
Nombre maximum de VLAN	25	25	50	50
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage à base de règles			
Qualité de service	Priorité de la bande passante, bande passante maximale, bande passante garantie, marquage DSCP, 802.1p			
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix			
VoIP	SIP			
Normes	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			
Nombre maximum de groupes SD/WAN	12	12	18	32
Nombre maximum de membres SD-WAN par produit	24	24	36	64

SONICWALL®

Spécifications système des pare-feu de la série NSv (suite)

GÉNÉRALITÉS DES PARE-FEU	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Système d'exploitation	SonicOS[1]				
Hyperviseurs pris en charge	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7				
Plateformes de cloud public prises en charge (type d'instance)	AWS (c5.large), Azure (Std D2 v2)	S.O.	AWS (c5.xlarge), Azure (Std D3 v2)	AWS (c5.2xlarge), Azure (Std D4 v2)	AWS (c5.4xlarge), Azure (Std D5 v2)
Licences	BYOL, PAYG[2]				
Nombre maximum de CPU virtuels pris en charge	2	3	4	8	16
Nombre d'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
Nombre maximum de cœurs de gestion/de plan de données	1/1	1/2	1/3	1/7	1/15
Mémoire minimum[3]	6 Go	6 Go	8 Go	10 Go	12 Go
Mémoire maximum[4]	6 Go	8 Go	10 Go	14 Go	18 Go
Adresses 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[5]				
PERFORMANCES PARE-FEU/VPN[6]	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Débit d'inspection des pare-feu	4,1 Gbit/s	5,9 Gbit/s	7,8 Gbit/s	13,9 Gbit/s	17,2 GBIT/S
Débit DPI total (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/s	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	37 270	75 640	125 000
Connexions maximales (SPI)	225 000	1 million	1,5 million	3 millions	4 MILLIONS
Nombre maximum de connexions (DPI)	125 000	500 000	1,5 million	2 millions	2,5 millions
Connexions DPI TLS/SSL	8 000	12 000	20 000	30 000	50 000
VPN	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Tunnels VPN site à site	75	100	6 000	10 000	25 000
Clients VPN IPSec (maximum)	50 (1 000)	50 (1 000)	2 000 (4 000)	2 000 (6 000)	2 000 (10 000)
Clients VPN SSL inclus[7]	2	2	2	2	2
Clients VPN SSL (maximum)[7]	100	150	200	300	400
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B, carte CAC (Common Access Card)				
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v				
VPN basé sur le routage	RIP, OSPF, BGP				
GESTION DE RÉSEAU	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Attribution d'adresses IP	Statique, DHCP, serveur DHCP interne, relais DHCP				
Modes NAT	1 à 1, plusieurs à 1, 1 à plusieurs, NAT flexible (adresses IP superposées), PAT				
Nombre maximum de VLAN[8]	128	128	128	128	128
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage à base de règles				
Qualité de service	Priorité de la bande passante, bande passante maximale, bande passante garantie, marquage DSCP, 802.1p				
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix				
VoIP	SIP				
Normes	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				
Nombre maximum de groupes SD/WAN	38	38	70	102	102
Nombre maximum de membres SD-WAN par produit	76	76	140	204	204

[1]*Prend actuellement en charge SonicOS 6.5.4.*
[2]*PAYG est actuellement uniquement disponible sur AWS.*
[3]*Mémoire avec trames Jumbo désactivées.*
[4]*Mémoire avec trames Jumbo activées. Mémoire additionnelle requise pour les trames Jumbo. Trames Jumbo non prises en charge sur Azure ou AWS.*
[5]*La haute disponibilité est disponible sur la plateforme VMware ESXi et Microsoft Hyper-V mais pas sur Azure et AWS.*
[6]*Les chiffres de performance publiés sont conformes aux spécifications. 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 en fonction de l'infrastructure de virtualisation sous-jacente. Nous recommandons également de procéder à des tests supplémentaires dans votre environnement pour vérifier que vos exigences en matière de performances et de capacités sont satisfaites. Les indicateurs de performance ont été observés en utilisant le processeur Intel Xeon W (W-2195 2,3 GHz, 4,3 GHz Turbo, cache 24,75 M) exécutant SonicOS v 6.5.0.2 avec VMware vSphere 6.5.*
[7]*L'augmentation du nombre de VPN SSL ne sera disponible qu'avec le firmware SonicOS 6.5.4.4-44v-21-723 et les versions ultérieures.*
[8]*Les interfaces VLAN ne sont pas prises en charge sur Azure ou AWS.*
Méthodes de test : performances maximales basées sur RFC 2544 (pour pare-feu). Débit DPI/antivirus de passerelle/anti-logiciels espions/IPS 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 des fonctionnalités.

Fonctionnalités

MOTEUR RFDPI

Fonctionnalité	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	Ce moteur d'inspection hautes performances, propriétaire et breveté effectue des analyses bidirectionnelles des flux de trafic, sans proxy ni mise en mémoire tampon, pour détecter les tentatives d'intrusion, les logiciels malveillants et le trafic des applications indépendamment du port.
Inspection bidirectionnelle	Le trafic entrant et sortant est analysé simultanément pour garantir que le réseau n'est pas utilisé pour distribuer des logiciels malveillants ou lancer des attaques en cas d'intrusion d'une machine infectée.
Inspection basée sur les flux	Cette technologie d'inspection sans proxy et sans mise en mémoire tampon offre des performances à ultra faible latence pour l'inspection DPI de millions de flux réseau simultanés, sans limite de taille des flux et des fichiers. Elle peut en outre être appliquée à des protocoles courants, ainsi qu'aux flux TCP bruts.
Hautement parallèle et extensible	La conception unique du moteur RFDPI fonctionne de concert avec l'architecture multicœurs pour fournir un haut débit DPI et des taux d'établissement de nouvelles sessions extrêmement élevés afin de gérer les pics de trafic sur les réseaux exigeants.
Inspection en un seul passage	L'architecture DPI en un seul passage analyse simultanément le trafic pour identifier les logiciels malveillants, les intrusions et les applications, ce qui réduit considérablement la latence DPI et garantit que toutes les informations sur les menaces sont corrélées au sein d'une architecture unique.

PARE-FEU ET GESTION DE RÉSEAU

Fonctionnalité	Description
API REST	Permet au pare-feu 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.
Inspection d'état des paquets	Tout le trafic réseau est inspecté, analysé et mis en conformité avec les règles d'accès du pare-feu.
Haute disponibilité[1]	La série NSv prend en charge le mode Actif/Passif (A/P) avec synchronisation de l'état.
Protection contre les attaques DDoS/DoS	La protection contre les inondations SYN permet de contrer les attaques DoS à l'aide des technologies de liste noire SYN de couche 2 et de proxy SYN de couche 3. Par ailleurs, elle offre la possibilité de se prémunir contre les attaques DoS/DDoS via la protection contre les inondations UDP/ICMP et la limitation du débit de connexion.
Support 24 h/24, 7 j/7	Le protocole IPv6 (Internet Protocol version 6) commence à remplacer le protocole IPv4. Avec le système d'exploitation SonicOS, le matériel prendra en charge les implémentations en mode filaire et filtrage.
Options de déploiement flexibles	La série NSv peut être déployée en mode NAT traditionnel, pont de couche 2, filaire et TAP réseau.
Équilibrage de charge WAN	Équilibre la charge de plusieurs interfaces WAN à l'aide des méthodes Round Robin, Spillover ou Percentage.
Qualité de service avancée (QoS)	Protège les communications critiques avec le marquage 802.1p et DSCP, ainsi que le remappage du trafic VoIP sur le réseau.
Prise en charge de proxy SIP	Bloque les appels indésirables en exigeant que tous les appels entrants soient autorisés et authentifiés par un proxy SIP.
Authentification biométrique	Prend en charge les modes d'authentification d'appareils mobiles, comme la reconnaissance d'empreinte digitale, difficiles à dupliquer ou à partager, en vue de déterminer en toute sécurité l'identité de l'utilisateur pour l'accès au réseau.
Authentification ouverte et social login	Permet aux utilisateurs invités d'utiliser leurs identifiants sur les services de réseaux sociaux comme Facebook, Twitter ou Google+ pour se connecter et accéder à Internet et à d'autres services invités par le biais de zones sans fil, LAN ou DMZ d'un hôte en utilisant l'authentification directe.

GESTION ET CRÉATION DE RAPPORTS

Fonctionnalité	Description
Gestion dans le cloud et sur site	La configuration et la gestion des appliances SonicWall peuvent se faire dans le cloud via le SonicWall Capture Security Center ou sur site avec SonicWall Global Management System (GMS).
Gestion puissante avec un seul appareil	L'interface Web intuitive offre une interface de ligne de commande complète, prend en charge le protocole SNMPv2/3 et permet une configuration rapide et pratique.
Rapports sur les flux applicatifs IPFIX/NetFlow	Exporte des analyses du trafic applicatif et des données d'utilisation via les protocoles IPFIX ou NetFlow pour offrir une surveillance et des rapports historiques et en temps réel avec des outils comme SonicWall Scrutinizer ou d'autres outils prenant en charge IPFIX et NetFlow via des extensions.

RÉSEAU PRIVÉ VIRTUEL (VPN)

Fonctionnalité	Description
Configuration automatique du VPN	Simplifie sensiblement le déploiement de pare-feu distribués en automatisant la configuration initiale de la passerelle VPN site à site entre les pare-feu SonicWall. Sécurité et connectivité se mettent en place instantanément et automatiquement.
VPN IPSec pour la connectivité site à site	Le VPN IPSec hautes performances permet à la série NSv de servir de concentrateur VPN pour des milliers d'autres bureaux à domicile, succursales ou sites de grande taille.
Accès client à distance IPSec ou VPN SSL	Utilise la technologie VPN SSL sans client ou un client IPSec facile à gérer pour accéder simplement à la messagerie électronique, aux fichiers, ordinateurs, pages intranet et applications depuis un vaste éventail de plateformes.

[1]*La haute disponibilité n'est actuellement pas prise en charge sur Azure et AWS.*

SONICWALL®

Passerelle VPN redondante	Si plusieurs WAN sont utilisés, un VPN principal et un VPN secondaire peuvent être configurés pour permettre un basculement automatique fluide et la restauration de toutes les sessions VPN.
VPN basé sur le routage	La possibilité d'effectuer un routage dynamique sur des liens VPN garantit une disponibilité continue en cas de panne temporaire d'un tunnel VPN via la redirection fluide du trafic entre les points de terminaison sur des routes alternatives.

INDICATEUR DE CONTEXTE/CONTENU	
Fonctionnalité	**Description**
Suivi de l'activité des utilisateurs	Fournit les données d'identification et d'activité des utilisateurs grâce à l'intégration transparente des services SSO AD/LDAP/Citrix1/Terminal Services1 associée aux nombreuses informations obtenues par l'inspection approfondie des paquets.
Identification du trafic par pays GeoIP	Identifie et contrôle le trafic réseau en direction ou provenant de pays spécifiques pour contrer les attaques liées à une activité d'origine suspecte ou connue ou pour faire des recherches sur le trafic suspect provenant du réseau. Possibilité de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP. Supprime le filtrage indésirable des adresses IP dû à une classification erronée.
Filtrage DPI des expressions régulières	Empêche les fuites de données en identifiant et en contrôlant les contenus qui transitent sur le réseau via l'identification des expressions régulières. Permet de créer des listes personnalisées de pays et de réseaux de zombies pour contourner un étiquetage incorrect associé à une adresse IP.

Services d'abonnement de prévention des intrusions

CAPTURE ADVANCED THREAT PROTECTION	
Fonctionnalité	**Description**
Service de sandbox multimoteur	La plateforme sandbox multimoteur, qui inclut le sandboxing virtualisé, l'émulation complète du système et une technologie d'analyse au niveau de l'hyperviseur, exécute le code suspect et analyse son comportement, offrant ainsi une visibilité complète sur l'activité malveillante.
Inspection approfondie de la mémoire en temps réel (RTDMI)	Cette technologie basée dans le cloud, en attente de brevet, détecte et bloque les logiciels malveillants qui ne manifestent aucun comportement malveillant et dissimulent leur armement au moyen d'un cryptage personnalisé. En forçant les logiciels malveillants à révéler leur armement dans la mémoire, le moteur RTDMI détecte et bloque de façon proactive les menaces « Zero Day » et les logiciels malveillants inconnus mais de grande diffusion.
Blocage jusqu'au verdict	Pour empêcher les fichiers potentiellement malveillants de pénétrer sur le réseau, les fichiers envoyés dans le cloud pour y être analysés peuvent être retenus à la passerelle jusqu'à ce qu'un verdict soit rendu.
Analyse de nombreux types de fichiers de toute taille	Ce service assure l'analyse d'un vaste éventail de fichiers, individuellement ou en groupe, notamment les programmes exécutables (PE), DLL, PDF, documents MS Office, archives, JAR et APK, ainsi que de divers systèmes d'exploitation comme Windows, Android ou Mac OS X et des environnements multi-navigateurs.
Déploiement rapide des signatures	Lorsqu'un fichier est identifié comme étant malveillant, une signature est immédiatement mise à la disposition des pare-feu ayant un abonnement à SonicWall Capture ATP, avant d'être envoyée sous 48 heures aux bases de données de signatures Gateway Anti-Virus et IPS ainsi qu'aux bases de données d'URL, d'IP et de réputation de domaine.
Capture Client	Capture Client est une plateforme client unifiée fournissant diverses fonctionnalités de protection des terminaux, dont une protection anti-logiciels malveillants avancée et la visibilité sur le trafic chiffré. Elle repose sur des technologies de protection multicouche, un reporting complet et l'exécution automatique de la protection des terminaux.

PROTECTION CONTRE LES MENACES CHIFFRÉES	
Fonctionnalité	**Description**
Déchiffrement et inspection TLS/SSL	Déchiffre et inspecte le trafic chiffré TLS/SSL à la volée, sans proxy, pour détecter les logiciels malveillants, les intrusions et les fuites de données, et applique les règles de contrôle du contenu, des URL et des applications afin de contrer les menaces dissimulées dans le trafic chiffré. Inclus avec les abonnements de sécurité pour tous les modèles de la série NSv.
Inspection SSH	L'inspection approfondie des paquets SSH (DPI-SSH) déchiffre et inspecte les données traversant les tunnels SSH en vue de prévenir les attaques qui exploitent ce protocole.

PRÉVENTION DES INTRUSIONS	
Fonctionnalité	**Description**
Protection basée sur des contre-mesures	Le système de prévention des intrusions (Intrusion Prevention System, IPS) étroitement intégré s'appuie sur les signatures et autres contre-mesures pour détecter les vulnérabilités et les attaques, dont il couvre une large palette, au sein de la charge utile.
Mise à jour automatique des signatures	L'équipe de recherche des menaces SonicWall recherche et déploie en continu des mises à jour pour une longue liste de contre-mesures IPS couvrant plus de 50 catégories d'attaque. Les nouvelles mises à jour prennent effet immédiatement, sans redémarrage ni interruption de service.
Protection IPS intrazone	Renforce la sécurité interne en segmentant le réseau en plusieurs zones de sécurité avec prévention des intrusions, empêchant les menaces de se propager entre ces zones.
Détection et blocage de la commande et du contrôle (Command and Control, CnC) des réseaux de zombies	Identifie et bloque le trafic CnC provenant de robots sur le réseau local vers des IP et des domaines identifiés comme propageant des logiciels malveillants ou comme des points CnC connus.
Abus/anomalies de protocoles	Identifie et bloque les attaques exploitant les protocoles dans le but de contourner le système IPS.

Protection de type « zero-day »	Protège 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.
Technologie anti-évasion	La normalisation intensive des flux, le décodage et d'autres techniques empêchent les menaces d'entrer sur le réseau sans se faire détecter via des techniques d'évasion sur les couches 2 à 7.

PRÉVENTION DES MENACES

Fonctionnalité	Description
Anti-logiciels malveillants de passerelle	Le moteur RFDPI analyse tout le trafic entrant, sortant et intrazone pour détecter les virus, chevaux de Troie, enregistreurs de frappes et autres logiciels malveillants dans les fichiers, quelles que soient leur taille et leur longueur, sur tous les ports et les flux TCP.
Protection anti-logiciels malveillants Capture Cloud	Les serveurs cloud SonicWall hébergent une base de données contenant des dizaines de millions de signatures de menaces, mise à jour en continu. Cette dernière est utilisée pour augmenter les capacités de la base de données de signatures locale, offrant au moteur RFDPI une couverture étendue des menaces.
Mises à jour de sécurité en continu	Les nouvelles mises à jour sont automatiquement appliquées aux pare-feu sur le terrain dotés de services de sécurité actifs et prennent effet immédiatement, sans redémarrage ni interruption.
Inspection TCP brute bidirectionnelle	Le moteur RFDPI est capable d'analyser les flux TCP bruts sur tous les ports de manière bidirectionnelle, empêchant ainsi les attaques visant à contourner les systèmes de sécurité obsolètes qui sécurisent uniquement quelques ports connus.
Prise en charge étendue des protocoles	Identifie les protocoles courants (HTTP/S, FTP, SMTP, SMBv1/v2, etc.) qui n'envoient pas de données sous forme de flux TCP bruts, et décode les charges utiles, qu'elles soient ou non exécutées sur des ports standard connus, pour identifier les logiciels malveillants.

SURVEILLANCE ET CONTRÔLE DES APPLICATIONS

Fonctionnalité	Description
Contrôle des applications	Compare les applications, ou les fonctionnalités des applications, identifiées par le moteur RFDPI à une base de données en constante expansion de plusieurs milliers de signatures pour renforcer la sécurité et la productivité réseau.
Identification des applications personnalisées	Contrôle les applications personnalisées en créant des signatures basées sur leurs paramètres ou schémas spécifiques dans leurs communications réseau afin de mieux contrôler le réseau.
Gestion de la bande passante applicative	Alloue et régule la bande passante disponible de manière granulaire selon l'importance ou la catégorie des applications tout en limitant le trafic vers les applications non essentielles.
Contrôle granulaire	Contrôle les applications, ou des composants spécifiques d'une application, en fonction de calendriers, de groupes d'utilisateurs, de listes d'exclusion et de plusieurs actions en effectuant une identification SSO complète des utilisateurs via l'intégration LDAP/AD/Terminal Services/Citrix.

FILTRAGE DU CONTENU

Fonctionnalité	Description
Filtrage du contenu interne/externe	Applique des règles d'utilisation acceptables et bloque l'accès aux sites Web HTTP/HTTPS contenant des informations ou des images répréhensibles ou non productives via Content Filtering Service et Content Filtering Client.
Client de filtrage de contenu renforcé	Étend l'application des règles pour bloquer les contenus Internet des appareils Windows, Mac OS, Android et Chrome situés hors du périmètre du pare-feu.
Contrôles granulaires	Bloque les contenus à l'aide de catégories prédéfinies ou d'associations de catégories. Le filtrage peut être planifié à certains moments de la journée, pendant les heures de bureau ou d'école par exemple, et appliqué à des groupes ou utilisateurs spécifiques.
Mise en cache Web	Les évaluations d'URL sont mises en cache localement sur le pare-feu SonicWall pour accélérer l'accès ultérieur aux sites les plus fréquentés.

ANTIVIRUS ET ANTI-LOGICIELS ESPIONS APPLIQUÉS

Fonctionnalité	Description
Protection multicouche	Utilise les fonctionnalités du pare-feu comme première couche de défense au niveau du périmètre et les associe à la protection des terminaux pour bloquer les virus qui entrent sur le réseau par le biais des ordinateurs portables, des clés USB ou d'autres systèmes non protégés.
Option d'application automatisée	S'assure que chaque ordinateur qui accède au réseau utilise le bon logiciel antivirus et/ou un certificat DPI-SSL installé et actif, éliminant ainsi les coûts couramment liés à la gestion des antivirus installés sur les ordinateurs de bureau.
Option de déploiement et d'installation automatisés	Le déploiement et l'installation, ordinateur par ordinateur, des clients antivirus et anti-logiciels espions sont automatiques sur le réseau, ce qui limite la charge d'administration.
Antivirus de nouvelle génération	Capture Client utilise un moteur statique d'intelligence artificielle (IA) pour identifier des menaces avant qu'elles ne puissent s'exécuter et pour revenir à un état précédant l'infection.
Protection contre les logiciels espions	Une protection puissante contre les logiciels espions analyse et bloque l'installation d'un large éventail de logiciels espions sur les ordinateurs portables et de bureau avant qu'ils ne transmettent des données confidentielles, renforçant ainsi les performances et la sécurité des postes de travail.

Récapitulatif des fonctionnalités de SonicOS

Contrôle global sur

- Contrôle centralisé de la visibilité IPv6
- Désactivation globale du traitement du trafic IPv6
- Désactivation des politiques VPN par défaut, des écrans de configuration et des règles générées automatiquement

Sécurité des connexions et des utilisateurs

- Blocage des utilisateurs basé sur les tentatives de connexion par plage d'adresses IP
- Blocage des utilisateurs depuis CLI
- Forcer le changement de mot de passe lors de la première connexion
- Prise en charge de l'authentification à deux facteurs (TOTP)
- Prise en charge d'un portail de politiques d'utilisateurs invités sans intervention
- Prise en charge IPv6 pour les services invités
- Prise en charge de la comptabilité TACACS+
- Contrôle des quotas pour tous les utilisateurs
- Authentification HTTP dynamique des réseaux de zombies

Mise en réseau et système

- Prise en charge SD-WAN
- Prise en charge de la sécurité DNS / des entonnoirs DNS
- FQDN sur TCP/DNS
- Objets d'adresses FQDN pour NAT
- Relais DHCPv6
- Mode d'adressage IPv6 pour la passerelle des couches applicatives VoIP H.323
- Prise en charge de cœurs de plan de commande multiples
- Redirection HTTP/HTTPS avec délestage des plans de données
- Délestage de l'assistant IP sur le plan de données
- Sauvegarde du firmware dans le stockage local
- Chiffrement haute disponibilité
- Prise en charge du chargement de firmware haute disponibilité
- Optimisation du routage statique et dynamique basée sur les politiques
- Améliorations des performances/ du débit
- Fonctionnalité de surveillance de l'état de santé du pare-feu
- Évolutivité améliorée pour le routage avancé via des interfaces de tunnel VPN numérotées
- Mise à jour des bibliothèques H.323 sur base du compilateur OSS Noklava v10.5.0 ASN.1
- Mise à jour des priorités des threads de tâches
- SSLVPN et signet sur le plan de données

Services de sécurité

- Blocage par Capture ATP jusqu'au verdict du contrôle granulaire
- Affichage des noms de fichiers compatible avec Capture ATP pour les protocoles non-HTTP
- Blocage CFS de vidéos YouTube individuelles
- Prise en charge simultanée du filtrage de contenu HTTPS et DPI-SSL
- Antivirus de nouvelle génération (SentinelOne) et application DPI-SSL
- Amélioration des performances de protection DDOS des WAN

Politiques / objets

- Améliorations des règles d'accès
- Routage basé sur les applications
- Objets d'adresses dynamiques
- Exclusion des politiques CFS
- Objets de filtrage de contenu HTTPS basé sur des politiques
- Prise en charge de groupes de listes URI dans les objets de filtrage de contenu
- Insertion d'en-tête CFS personnalisé pour les demandes HTTP
- UUID pour les règles et les objets
- UUID pour les politiques CFS
- Contournement MAC source pour les politiques NAT

DPI-SSL / DPI-SSH

- Liste blanche DPI-SSL dynamique basée sur le cloud
- Blocage DPI-SSH du transfert de port SSH
- Blocage DPI-SSH du transfert X11
- Préservation du port de déchiffrement SSL dans les miroirs/captures de paquets
- Contrôle DPI-SSL granulaire par zone
- Règles d'accès basées sur le contrôle DPI-SSL
- Blocage des clients DPI-SSL ou autorisation des certificats d'autorités de certification expirés
- Extension des demandes de statuts des certificats TLS
- Prise en charge CRL locale
- Vérification améliorée des certificats DPI-SSL
- Prise en charge des codes de chiffrement ECDSA
- Prise en charge de la version OpenSSL LTS pour la certification fédérale

Consignation, surveillance et reporting

- Possibilité de vérifier que la DPI a été effectuée sur un paquet spécifique
- Consignation des noms de fichiers et URI pour le contrôle des applications
- Enregistrements de connexion affichés pour l'administrateur
- Audit de la configuration
- Consignation du mappage NAT pour les connexions TCP
- Prise en charge FTP pour l'automatisation de la consignation
- Prise en charge des rapports et analyses Capture Security Center (CSC) pour NSv
- Consignation Capture ATP pour les expéditeurs/destinataires d'e-mails
- Améliorations du client Capture Threat Assessment (SWARM v3)
- Fonction de réinitialisation des données statistiques SFR (SWARM)
- Option de sélection de la langue du rapport SonicFlow

API

- SonicOS API phase 1
- Prise en charge de l'authentification SonicOS API
- SonicOS API phase 2
- LHM RESTful API

Interface de gestion Web SonicOS

- Recherche globale SonicOS
- Améliorations de la convivialité des pages de contenu
- Stockage des préférences d'interface côté client par utilisateur
- Épinglage d'un nom convivial sur les écrans de gestion Web SonicOS
- Refonte de la disposition de l'interface Web SonicOS

Informations de commande des pare-feu de la série NSv

PRODUIT	RÉFÉRENCE ESXI	RÉFÉRENCE HYPER-V	RÉFÉRENCE AZURE	RÉFÉRENCE AWS	RÉFÉRENCE KVM
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition (1 an)	01-SSC-5875	02-SSC-1387	02-SSC-3426	02-SSC-3452	02-SSC-3494
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition (1 an)	01-SSC-5923	02-SSC-1395	02-SSC-3454	02-SSC-3464	02-SSC-3497
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition (1 an)	01-SSC-5926	02-SSC-1399	02-SSC-3470	02-SSC-3474	02-SSC-3504
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition (1 an)	01-SSC-5929	02-SSC-1405	02-SSC-3480	02-SSC-3489	02-SSC-3513
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition (1 an)	01-SSC-5950	02-SSC-1412	02-SSC-0868	02-SSC-0906	02-SSC-3519
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition (1 an)	01-SSC-5964	02-SSC-1420	—	—	02-SSC-3526
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition (1 an)	01-SSC-6084	02-SSC-1427	02-SSC-0888	02-SSC-0912	02-SSC-3531
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition (1 an)	01-SSC-6101	02-SSC-1429	02-SSC-0889	02-SSC-0914	02-SSC-3533
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition (1 an)	01-SSC-6109	02-SSC-1436	02-SSC-0895	02-SSC-0921	02-SSC-3540

PRODUIT	RÉFÉRENCE ESXI	RÉFÉRENCE HYPER-V	RÉFÉRENCE AZURE	RÉFÉRENCE AWS	RÉFÉRENCE KVM
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition (3 ans)	01-SSC-5873	02-SSC-1386	02-SSC-3427	02-SSC-3453	02-SSC-3491
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition (3 ans)	01-SSC-5890	02-SSC-1397	02-SSC-3457	02-SSC-3465	02-SSC-3498
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition (3 ans)	01-SSC-5924	02-SSC-1398	02-SSC-3471	02-SSC-3472	02-SSC-3505
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition (3 ans)	01-SSC-5928	02-SSC-1404	02-SSC-3478	02-SSC-3486	02-SSC-3514
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition (3 ans)	01-SSC-5951	02-SSC-1411	02-SSC-0866	02-SSC-0903	02-SSC-3515
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition (3 ans)	01-SSC-5965	02-SSC-1419	—	—	02-SSC-3523
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition (3 ans)	01-SSC-6089	02-SSC-1426	02-SSC-0887	02-SSC-0911	02-SSC-3527
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition (3 ans)	01-SSC-6102	02-SSC-1428	02-SSC-0891	02-SSC-0913	02-SSC-3538
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition (3 ans)	01-SSC-6108	02-SSC-1435	02-SSC-0897	02-SSC-0920	02-SSC-3542

**Veuillez contacter votre revendeur SonicWall pour obtenir la liste complète des références*

À propos de SonicWall

SonicWall offre une Boundless Cybersecurity pour l'ère de l'hyper-distribution dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant une percée économique par de véritables économies. SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour en savoir plus, rendez-vous sur www.sonicwall.com.

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

Datasheet-NSvVirtualFirewalls-US-VG-2088