NSv 270/470/870

Les pare-feux SonicWall Network Security virtual NS*v* 270/470/870 assurent une sécurité haut de gamme et une gestion rationalisée, avec une visibilité totale, un déploiement flexible et des performances supérieures pour les charges de travail virtuelles.

On découvre régulièrement des vulnérabilités dans les environnements virtuels qui s'accompagnent de réelles implications et de sérieux défis. Mais la protection de tous ces vecteurs de sécurité nécessite de pouvoir appliquer la bonne règle de sécurité au point de contrôle réseau adéquat, certaines défaillances provenant de règles inefficaces ou de mauvaises configurations.

AVANTAGES

Sécurité des clouds publics, privés et gouvernementaux

- Pare-feux de nouvelle génération avec détection et prévention automatisées des failles en temps réel
- Technologie RTDMI™ (Real-Time Deep Memory Inspection) brevetée
- Technologie RFDPI (Reassembly-Free Deep Packet Inspection) brevetée
- Visibilité totale, de bout en bout, et gestion rationalisée avec Unified Policy
- Surveillance et contrôle des applications
- Sécurité DNS
- Service de filtrage de contenu basé sur la réputation (CFS 5.0)
- Gestion de pare-feu Wi-Fi 6
- Intégration du contrôle d'accès réseau avec Aruba ClearPass
- Prise en charge des clouds AWS et Azure gouvernementaux
- Intégration à Microsoft Azure Sentinel pour une réponse plus rapide aux incidents
- Prise en charge des plateformes de cloud privé (ESXi, Hyper-V, KVM, Nutanix) et public (AWS, Azure)

Protection des machines virtuelles

- Confidentialité des données
- Communication sécurisée avec prévention des fuites de données
- Validation, inspection et surveillance du trafic
- Résilience et disponibilité des réseaux virtuels

FICHE TECHNIQUE

Les pare-feux NS*v* Series 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 l'entreprise. Ils permettent aux entreprises de contrôler le trafic dynamique traversant un pare-feu et de bénéficier de la visibilité et des informations nécessaires sur des règles disparates. Ils simplifient les tâches de gestion, réduisent les erreurs de configuration et accélèrent le déploiement, améliorant ainsi la posture de sécurité globale.

SonicOSX et les services de sécurité

L'architecture de SonicOSX est au cœur des pare-feux NS*v* 270/470/870. Elle repose sur le système d'exploitation riche en fonctionnalités SonicOSX 7, doté d'une interface utilisateur intuitive et de fonctionnalités évoluées de sécurité, réseau et gestion.

SonicOSX 7.0 a été entièrement repensé et inclut notamment Unified Policy, qui permet la gestion intégrée de différentes règles de sécurité. Vous pouvez établir facilement des contrôles de couche 3 à 7 au sein d'une même base de règles sur chaque pare-feu et bénéficier ainsi d'un emplacement centralisé pour la configuration de règles. La nouvelle interface Web offre une visualisation graphique des informations essentielles sur les menaces et affiche des alertes actionnables qui vous invitent à configurer des règles de sécurité contextuelles en quelques clics.

La série NS*v* intègre en outre le SD-WAN, la prise en charge de TLS 1.3, la visualisation en temps réel, le réseau privé virtuel (VPN) haut débit et autres puissantes fonctionnalités de sécurité. Les menaces inconnues sont envoyées à la sandbox multimoteur cloud de SonicWall, Capture Advanced Threat Protection (ATP), pour y être analysées. Capture ATP exploite RTDMI (Real-Time Deep Memory Inspection), une technologie SonicWall brevetée, pour déceler et bloquer les logiciels malveillants et autres menaces zero-day qui se trouvent dans la mémoire.

Associant Capture ATP, la technologie RTDMI et des services de sécurité avancés, les pare-feux NS*v* Series stoppent les malwares à la passerelle, avant qu'ils n'atteignent vos systèmes vitaux.

Déploiements

1. Périphérie cloud : des clouds publics, privés et gouvernementaux sécurisés

- Sécurisez les charges de travail sur Amazon Web Services (AWS) et Microsoft Azure
- Protégez les applications et infrastructures cloud contre les cybermenaces grâce aux fonctionnalités avancées des pare-feux de nouvelle génération – VPN, IPS, CFS, AV, etc.
- Déchiffrez aisément le trafic chiffré et améliorez votre sécurité grâce à TLS 1.3
- Garantissez la conformité avec les normes réglementaires grâce aux fonctionnalités de prévention des menaces et de segmentation
- Bénéficiez d'une visibilité et d'un contrôle parfaits du trafic entre différentes régions et zones de disponibilité grâce à Unified Policy
- Profitez de l'avantage financier et de l'efficacité du passage du modèle CapEx au modèle OpEx
- Sécurisez les clouds AWS et Azure destinés aux agences gouvernementales et à leurs clients en déployant des pare-feux NS*v*
- Sécurisez les ressources informatiques virtualisées et les hyperviseurs pour protéger les charges de travail des clouds privés sur VMware ESXi, Microsoft Hyper-V, Nutanix et KVM
- Prévenez les menaces grâce à une visibilité totale sur les communications intra-hôte entre machines virtuelles
- Garantissez l'application correcte des règles de sécurité dans l'environnement virtuel
- Établissez des règles fiables d'activation par application, utilisateur et appareil, quel que soit l'emplacement de la machine virtuelle
- Mettez en place des zones de sécurité et d'isolement adéquates
- Bénéficiez de l'intégration à Microsoft Azure Sentinel, une solution de gestion des informations et des événements de sécurité (SIEM) et d'orchestration, d'automatisation et de réponse aux incidents de sécurité (SOAR) évolutive, cloud native qui accélère la réponse aux incidents

2. Périphérie Internet

- Protégez les ressources de l'entreprise contre les attaques au niveau de la passerelle Internet.
- Sécurisez la périphérie Internet face aux attaques les plus évoluées grâce à des fonctionnalités de sécurité de pointe et bloquez automatiquement les menaces
- Garantissez la conformité avec les normes réglementaires grâce aux fonctionnalités de prévention des menaces et de segmentation
- Gagnez en efficacité et en performances tout en réduisant les coûts grâce aux améliorations offertes par SonicOSX
- Segmentez les systèmes TPV (points de vente) stratégiques pour garantir la continuité des activités
- Bénéficiez d'une visibilité et d'un contrôle parfaits du trafic entre différentes régions et zones de disponibilité grâce à Unified Policy

Spécifications système NS*v* Series

Pare-feu – Général	NS*v* 270	NS*v* 470	NS*v* 870
Système d'exploitation	SonicOSX[11]		
Hyperviseurs pris en charge	VMware ESXi v5.5/v6.0/v6.5/v6.7/v7.0/v8.0, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7, Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[10]		
Clouds gouvernementaux pris en charge[12]	AWS et Azure (dans les régions Est et Ouest des États-Unis)		
Types d'instances AWS pris en charge	c5.large c5n.large c5d.large m5.large m5n.large	c5.xlarge c5n.xlarge c5d.xlarge m5.xlarge m5n.xlarge	c5.2xlarge c5n.2xlarge c5d.2xlarge m5.2xlarge m5n.2xlarge
Types d'instances Azure pris en charge	Standard D2 v2 Standard_B2ms Standard_D2V4 Standard_D2ds_V4 Standard_D2s_v4	Standard D3 v2 Standard_B4ms Standard_DS3_v2 Standard_D2ds_V4	Standard D4 v2 Standard_A8_v2 Standard_F8 Standard_F8s Standard_D8_v4 Standard_D8_v3 Standard_D8s_v3
Licences	BYOL, PAYG[1]		
Nb max. de vCPU pris en charge	2	4	8
Nombre d'interfaces (ESXi/Hyper-V/KVM/Nutanix/AWS/Azure)	8/8/8/8/8/8	8/8/8/8/8/8	8/8/8/8/8/8
Nb. cœurs max. gestion/DataPlane	1/1	1/3	1/7
Mémoire min.[2]	4 Go	8 Go	10 Go
Mémoire max.[3]	6 Go	10 Go	14 Go
IP/nœuds pris en charge	Illimitée		
Stockage minimum	60 Go		
Utilisateurs de l'authentification unique (SSO)	500	10 000	15 000
Journalisation	Analyzer, Local Log, Syslog		
Haute disponibilité	Active/passive[4]		

Performances pare-feu/VPN[5,7]	NSv 270	NSv 470	NSv 870
Débit de filtrage pare-feu	6 Gbit/s	9 Gbit/s	14 Gbit/s
Débit de prévention des menaces	1,6 Gbit/s	2,9 Gbit/s	8 Gbit/s
Débit IPS	4 Gbit/s	6 Gbit/s	8 Gbit/s
Débit DPI TLS/SSL	800 Mbit/s	2 Gbit/s	4 Gbit/s
Débit VPN[8]	1,4 Gbit/s	3,5 Gbit/s	8 Gbit/s
Connexions par seconde	13 760	37 270	75 640
Nb max. de connexions (SPI)	225 000	1,5 M	3 M
Nb max. de connexions (DPI)	125 000	1,5 M	2 Mio
Connexions DPI TLS/SSL	8 000	20 000	30 000
VPN	**NSv 270**	**NSv 470**	**NSv 870**
Tunnels VPN site à site	75	6 000	10 000
Clients VPN IPSec[13] (maximum)	50 (1 000)	2 000 (4 000)	2 000 (6 000)
Clients VPN SSL inclus[6]	2	2	2
Nb max. de clients VPN SSL[6]	100	200	300
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	**NSv 270**	**NSv 470**	**NSv 870**
Attribution d'adresses IP	Statique, DHCP, serveur DHCP interne[9], relais DHCP[9]		
Modes NAT	1:1, plusieurs:1, 1:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT		
Interfaces VLAN et de tunnel logiques (maximum)[7]	128	128	128
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage à base de règles		
Qualité de service	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		
Base de données utilisateurs locale	250	2 500	3 200

[1]PAYG est actuellement disponible uniquement sur AWS.
[2]Mémoire avec trame Jumbo désactivée.
[3]Mémoire avec trame Jumbo activée. Mémoire supplémentaire requise pour les trames Jumbo. Les trames Jumbo ne sont pas prises en charge sur Azure et AWS.
[4]La haute disponibilité est disponible sur plateforme VMware ESXi, KVM, Azure, Microsoft Hyper-V et Nutanix. NSv 270 prend en charge la haute disponibilité avec une machine virtuelle de taille D3v2. La haute disponibilité n'est pas prise en charge sur AWS. La haute disponibilité sur Azure requiert une taille de serveur supportant trois interfaces ou plus.
[5]Les valeurs de performances publiées correspondent aux spécifications. Les performances réelles peuvent varier en fonction du matériel sous-jacent, des conditions réseau, de la configuration du pare-feu et des services activés. Les performances et la capacité peuvent également varier selon l'infrastructure de virtualisation sous-jacente. Nous recommandons des tests supplémentaires dans votre environnement afin de garantir le respect de vos exigences.

Les mesures de performances ont été relevées avec processeur Intel Xeon (Platinum 8268 @2,9 GHz, 3,9 GHz Turbo, 37,5 Mo de cache) exécutant SonicOS 7.0.1 avec VMware vSphere 7.0.
[6]Clients VPN SSL disponibles pour le programme MSSP : 50 sur NSv 270 et 75 sur NSv 470. Nombre de VPN SSL supérieur disponible uniquement à partir du firmware SonicOS 6.5.4.4-44v-21-723 et plus récent.
[7]Les interfaces VLAN ne sont pas prises en charge sur Azure et AWS.
Méthodes de test : performances maximales basées sur RFC 2544 (pour pare-feu). Débit de prévention des menaces/antivirus de passerelle/anti-logiciels espions/IPS mesuré en utilisant les tests de performance HTTP Keysight conformes aux standards actuels. Tests réalisés avec plusieurs flux sur plusieurs paires de ports. Débit de prévention des menaces mesuré en ayant activé l'antivirus de passerelle, l'anti-logiciels espions, l'IPS et le contrôle des applications avec paramètres de pare-feu par défaut. Débit VPN mesuré sur le trafic UDP avec chiffrement AESGMAC16-256 de paquets de 1 418 octets selon RFC 2544. Toutes les caractéristiques, fonctionnalités et disponibilités peuvent faire l'objet de modifications.
[8]Tous les paramètres de performances sont testés sur un Dell R740 avec SR-IOV et Turbo Boost.
[9]Pris en charge sur les plateformes de cloud privé, pas de cloud public.
[10]Nutanix AHV est pris en charge sur SonicWall NSv 270/470/870 exécutant le firmware SonicOSX 7.0.0 ou supérieur.
[11]Les utilisateurs de SonicOSX 7.0.1 et supérieur pourront sélectionner et alterner entre les modes Classic/Global et Policy.
[12]Cloud gouvernemental disponible uniquement via BYOL.
[13]Clients GVC disponibles pour le programme MSSP : 25 sur NSv 270 et 50 sur NSv 470.

Récapitulatif des fonctionnalités de SonicOSX 7.0

Pare-feu

- Inspection stateful des paquets
- Reassembly-Free Deep Packet Inspection
- Protection contre les attaques DDoS (UDP/ICMP/SYN flood)
- Prise en charge IPv4/IPv6
- Authentification biométrique pour l'accès distant
- Proxy DNS
- API REST
- Intégration de SonicWall Switch[1]
- Intégration points d'accès SonicWall Wi-Fi 6
- Service de filtrage de contenu basé sur la réputation (CFS 5.0)
- Filtrage des DNS
- SD-WAN
  - Évolutivité SD-WAN
  - Assistant d'utilisation SD-WAN
- API
  - Prise en charge complète d'API
- Mutualisation[3]
  - Prise en charge de la mutualisation
  - Vue des locataires avec prise en charge firmware par locataire
- Alternance entre modes Classic/Global et Policy[4]

Unified Policy

- Unified Policy associe les règles de la couche 3 à la couche 7 :
  - Source/Destination IP/Port/Service
  - Contrôle des applications
  - Botnet/Geo-IP CFS/Web
  - Diagramme de règles
  - Application des services de sécurité single pass - IPS/GAV/AS/Capture ATP
  - Objets basés sur les profils pour sécurité des terminaux/gestion de la bande passante/qualité de service/filtrage de contenus/prévention des intrusions
- Profils d'action pour les règles de sécurité/DoS
- Gestion des règles :
  - Clonage
  - Analyse des règles Shadow
  - Modification cellule
  - Exportation des règles
  - Modification groupe
- Gestion des vues
  - Règles utilisées/non utilisées
  - Règles actives/non actives
  - Regroupement par section/personnalisé
  - Grille/mise en page personnalisables

Déchiffrement et inspection TLS/SSL/SSH

- TLS1.3
- Prise en charge de TLS 1.3 avec sécurité renforcée
- Inspection approfondie des paquets pour TLS/SSL/SSH
- Inclusion/exclusion d'objets, de groupes ou de noms d'hôtes
- Contrôle SSL
- Contrôles DPI-SSL granulaires par zone ou règle

Capture advanced threat protection[2]

- Real-Time Deep Memory Inspection
- Analyse multimoteur cloud
- Sandboxing virtualisé
- Analyse au niveau de l'hyperviseur
- Émulation complète du système
- Examen de nombreux types de fichiers
- Soumission automatique et manuelle
- Mises à jour en temps réel des renseignements sur les menaces
- Blocage jusqu'au verdict
- Capture Client

Prévention des intrusions[2]

- Analyse basée sur des signatures
- Intégration du contrôle d'accès réseau avec Aruba ClearPass
- Mise à jour automatique des signatures
- Moteur d'inspection bidirectionnelle
- Fonctionnalité de règles IPS granulaires
- Localisation GeoIP
- Filtrage de réseaux de zombies avec liste dynamique
- Détection des expressions régulières

Protection contre les logiciels malveillants[2]

- Analyse des logiciels malveillants basée sur les flux
- Antivirus de passerelle
- Anti-logiciels espions de passerelle
- Inspection bidirectionnelle
- Pas de limitation de la taille des fichiers
- Base de données cloud de logiciels malveillants

Identification des applications[2]

- Contrôle des applications
- Gestion de la bande passante applicative
- Création de signatures d'applications personnalisées
- Prévention des fuites de données
- Création de rapports sur les applications via NetFlow/IPFIX
- Base de données complète des signatures d'applications

Visualisation et analyse du trafic

- Activité des utilisateurs
- Utilisation par les applications/bande passante/menaces
- Analyse dans le cloud

Filtrage du contenu Web HTTP/HTTPS[2]

- Filtrage des URL
- Évitement de proxy
- Blocage par mots-clés
- Service de filtrage de contenu basé sur la réputation (CFS 5.0)
- Filtrage des DNS
- Filtrage à base de règles (exclusion/inclusion)
- Insertion d'en-tête HTTP
- Catégories d'évaluation CFS pour la gestion de la bande passante
- Modèle unifié de règles avec contrôle des applications
- Content Filtering Client

VPN

- SD-WAN sécurisé
- Configuration automatique du VPN
- VPN IPSec pour la connectivité site à site
- Accès client à distance IPSec et VPN SSL
- Passerelle VPN redondante
- Mobile Connect pour iOS, Mac OS X, Windows, Chrome, Android et Kindle Fire
- VPN basé sur le routage (RIP/OSPF/BGP)

Tableau de bord amélioré

- Vue améliorée de l'appareil
- Résumé des pics de trafic et utilisateurs
- Renseignements sur les menaces
- Centre de notification
- Surveillance améliorée des paquets
- Terminal SSH sur l'interface
- Nouveau design/modèle
- Comparaison à la moyenne du secteur et mondiale

Gestion de réseau

- PortShield[1]
- Trames Jumbo
- Découverte MTU de chemin
- Journalisation améliorée
- Jonction VLAN
- Mise en miroir des ports (NS*a* 2650 et plus récentes)

- Qualité de service de couche 2
- Sécurité des ports
- Routage dynamique (RIP/OSPF/BGP)
- Contrôleur sans fil SonicPoint[1]
- Routage à base de règles (ToS/ métrique et ECMP)
- NAT
- Serveur DHCP
- Gestion de la bande passante
- Agrégation de liens[1] (statique et dynamique)
- Redondance de ports[1]
- Haute disponibilité A/P avec synchro. d'état
- Clustering A/A[1]
- Équilibrage de la charge entrante/sortante
- Mode NAT, mode TAP, mode filaire/filaire virtuel, mode pont de couche 2[1]
- Basculement WAN 3G/4G[1]
- Routage asymétrique
- Prise en charge Common Access Card (CAC)
- Conteneurisation SonicCoreX et SonicOS

Politique de déchiffrement

- Unified Policy pour le trafic SSL/TLS

Politique DoS

- Unified Policy pour la prévention des attaques DoS/DDoS

VoIP

- Contrôle QoS granulaire
- Gestion de la bande passante
- DPI du trafic VoIP
- Prise en charge des proxys SIP et des contrôleurs d'accès H.323

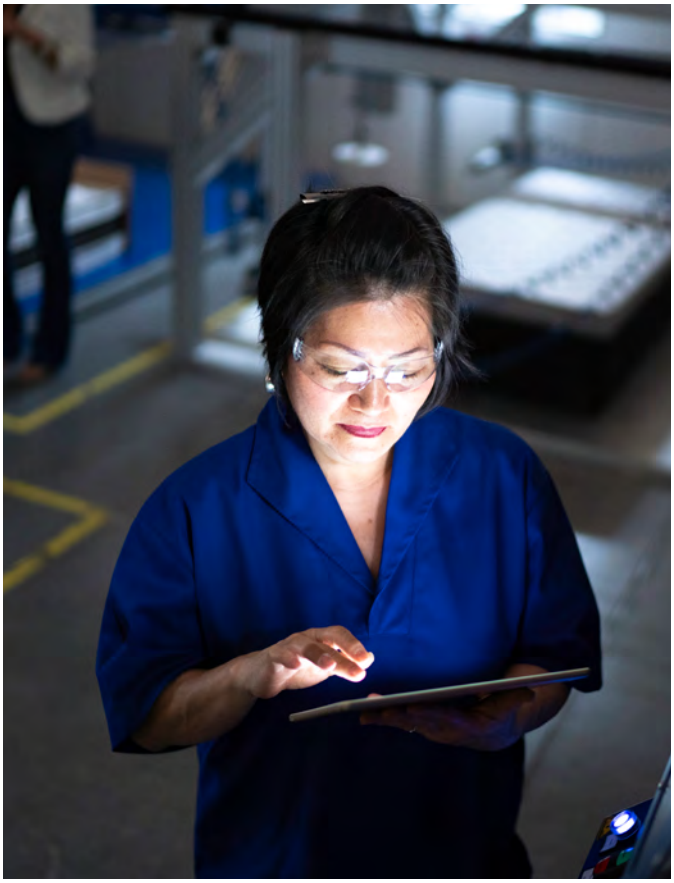
Gestion et surveillance

- Interface utilisateur Web
- Interface de ligne de commande
- Enregistrement et configuration zéro intervention
- Prise en charge de l'appli. mobile SonicExpress
- SNMPv2/v3
- Création de rapports et gestion centralisées avec Network Security Manager (NSM)[2]
- Journalisation
- Exportation NetFlow/IPFix
- Sauvegarde cloud de la configuration
- Visualiseur de bande passante et d'applications
- Gestion IPv4 et IPv6
- Création de rapports hors pare-feu (Scrutinizer)
- Écran de gestion LCD[1]
- Gestion des commutateurs Dell série N et série X, notamment en cascade[1]
- Reporting Network Security Manager

Sans-fil[1]

- Gestion cloud et sur pare-feu des points d'accès SonicWave
- WIDS/WIPS
- Prévention des points d'accès sauvages
- Itinérance rapide (802.11k/r/v)
- Réseau maillé 802.11s
- Sélection de canal automatique
- Analyse du spectre des radiofréquences
- Vue plan de sol
- Vue topologique
- Orientation de bande
- Formation de faisceaux
- Équité du temps d'utilisation du réseau
- Bluetooth à basse consommation
- Extendeur MiFi
- Quota cyclique invités
- Portail invités LHM

[1] Non pris en charge sur les pare-feux NS*v* Series
[2] Requiert un abonnement supplémentaire
[3] Disponible uniquement sur les pare-feux NSsp
[4] Disponible sur SonicOSX 7.0.1 et plus récent



PARTNER ENABLED SERVICES

Vous avez besoin d'aide pour planifier, déployer ou optimiser votre solution SonicWall ? Les partenaires SonicWall Advanced Services sont spécialement formés pour vous fournir des services professionnels de premier ordre. En savoir plus sur

www.sonicwall.com/PES

En savoir pllus sur la série SonicWall NSv 270/470/870

www.sonicwall.com/NSv

À propos de SonicWall

SonicWall offre une solution de cybersécurité stable, évolutive et transparente 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 de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, rendez-vous sur www.sonicwall.com.

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