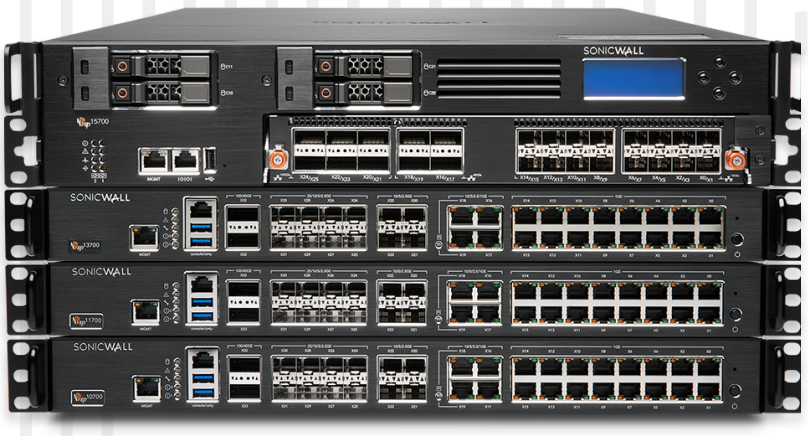
SonicWall série NS*sp* 7ème génération

La série SonicWall Network Security services platform™ (NS*sp*) propose des pare-feux de nouvelle génération ainsi qu'une densité de ports élevée et des interfaces multi-gigabits capables de traiter plusieurs millions de connexions pour les menaces zero-day et les menaces évoluées. Destinée aux grandes entreprises, à l'enseignement secondaire et supérieur, aux organismes publics et aux MSSP, elle permet d'éliminer les attaques en temps réel sans ralentir les performances. Elle est conçue pour être extrêmement fiable et pour fournir aux entreprises des services sans interruption.



AVANTAGES

SonicWall série NS*sp*

- Grande densité de ports
- Ports 100 GbE
- S'intègre au sandboxing cloud et en local
- Interface utilisateur intuitive avec gestion centralisée
- 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
- Débit de prévention des menaces >80 Mbit/s
- Alimentation redondante
- Débit d'inspection du pare-feu jusqu'à 100 Gbit/s
- Prise en charge TLS 1.3
- Prend en charge des millions de connexions TLS simultanées
- Faible coût total de possession
- Alimentée par l'équipe de recherche sur les menaces SonicWall Capture Labs

Aperçu des caractéristiques série NS*sp*
Voir toutes les caractéristiques »

100 GbE	Jusqu'à 100 Gbit/s	80 M
ports	débit du pare-feu	nb max. de connexions (NS*sp* 15700)

En savoir plus sur la série SonicWall NS*sp* 7ème génération

sonicwall.com/NS*sp*

FICHE TECHNIQUE

Pare-feux haut de gamme

Tandis que les entreprises évoluent et que le nombre d'appareils gérés et non gérés, de réseaux, de charges de travail cloud, d'applications SaaS, d'utilisateurs, de débits Internet et de connexions chiffrées augmente, tout pare-feu incapable de prendre en charge ces évolutions devient un goulot d'étranglement. Un pare-feu doit constituer un point de force et non un maillon faible.

Les nombreuses interfaces 100G/40G/25G/10G du pare-feu SonicWall NS*sp* vous permettent de traiter plusieurs millions de connexions chiffrées et non chiffrées simultanées grâce à une technologie de prévention des menaces sans précédent. Plus de 70 % des sessions étant chiffrées, il est essentiel en termes de productivité et de sécurité des informations de posséder un pare-feu capable de traiter et d'examiner ce trafic sans impacter l'expérience utilisateur.

Les règles unifiées du NS*sp* 15700 permettent aux entreprises de créer facilement et intuitivement des règles d'accès et de sécurité dans une interface unique.

Gestion et reporting simplifiés

La gestion, la surveillance et le reporting continus des activités réseau sont gérés via la solution SonicWall Network Security Manager. Elle fournit un tableau de bord intuitif permettant de gérer les opérations de pare-feu ainsi que des rapports historiques, depuis une seule et même source. La simplicité de déploiement et de configuration et la facilité de gestion permettent aux entreprises d'abaisser leur coût total de possession et de réaliser un bon retour sur investissement.

Déploiement

Pare-feu de nouvelle génération (NGFW)

- Géré via un écran unique
- La série NS*sp* s'intègre au reste de l'écosystème SonicWall.
- Visibilité totale sur votre réseau pour savoir comment les applications, les appareils et les utilisateurs appliquent les règles et éliminent les menaces et les encombrements de la bande passante.
- S'intègre au service breveté Capture ATP avec RTDMI pour le sandboxing cloud ou Capture Security Appliance pour une détection des logiciels malveillants sur site.

Inspection approfondie des paquets du trafic SSL/TLS (DPI-SSL) pour les menaces cachées.

- La série NS*sp* permet d'inspecter plusieurs millions de connexions chiffrées TLS/SSL et SSH, quels que soient le port ou le protocole.
- Les règles d'inclusion et d'exclusion permettent une personnalisation en fonction d'exigences légales et/ou de conformité spécifiques à l'entreprise.
- Prise en charge des suites de chiffrement TLS jusqu'à TLS 1.3

Segmentation et gestion de réseau

- Fonctionnement sur plusieurs réseaux segmentés, clouds ou définitions de services, avec des modèles uniques, des groupes d'appareils et des règles pour plusieurs appareils et plusieurs locataires.
- Les MSSP peuvent également prendre en charge plusieurs clients avec un canal nettoyé et des règles uniques.

Pare-feu multi-instance (uniquement sur NS*sp* 15700)

- Les versions multi-instance sont la prochaine génération des versions mutualisées.
- Chaque locataire est isolé avec des ressources de calcul dédiées pour éviter toute insuffisance éventuelle.
- Comporte des ports/locataires physiques et logiques.
- Prend en charge des règles indépendantes pour les locataires et une gestion de la configuration.
- Indépendance de version et haute disponibilité (HA) pour les locataires.

Fonctionnalité en mode filaire

- Mode Bypass pour l'introduction rapide et relativement sans interruption de matériel de pare-feu dans un réseau.
- Mode Inspect pour étendre le mode Bypass sans modifier la fonctionnalité du parcours des paquets avec zéro latence et faible risque.
- Mode Secure pour activement intercaler les processeurs multi-cœur du pare-feu dans le parcours de traitement des paquets.
- Mode Tap pour ingérer un flux de paquets en miroir via un port de commutation unique sur le pare-feu, ce qui évite toute insertion physique intermédiaire.

Protection avancée contre les menaces

- Le service SonicWall Capture Advanced Threat Protection™ (ATP) est utilisé par plus de 150 000 clients dans le monde, avec de nombreuses solutions, et permet de détecter et de bloquer plus de 1 200 nouvelles formes de logiciels malveillants chaque jour.
- La série NS*sp* s'intègre à l'appliance Capture Security pour détecter et bloquer des menaces inconnues grâce au sandboxing sur site qui utilise la technologie Real-Time Deep Memory Inspection™ (RTDMI).

Plateforme Capture Cloud

- La plateforme Capture Cloud de SonicWall 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.

Services de filtrage de contenu

- Compare les sites Web demandés à une immense base de données cloud contenant des millions d'URL, d'adresses IP et de sites évalués.
- Crée et applique les règles qui autorisent ou refusent l'accès aux sites selon l'identité d'un individu/groupe ou l'heure de la journée.
- Le service de filtrage de contenu basé sur la réputation (CFS 5.0) vous permet d'appliquer des règles d'utilisation d'Internet et de contrôler l'accès en interne à des contenus Web indésirables, non productifs voire illégaux grâce au filtrage de contenu complet. Le filtrage de contenu basé

sur la réputation fournit un score de réputation qui prévoit le risque de sécurité d'une URL.

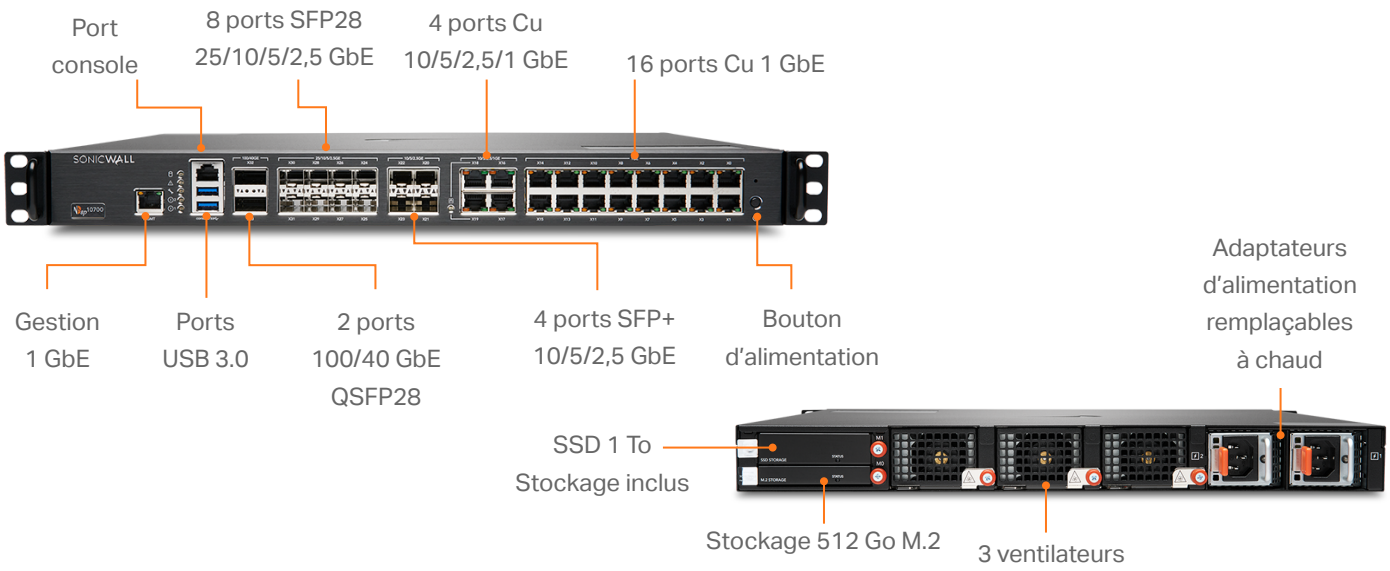
Système de prévention des intrusions (IPS)

- Fournit un moteur de filtrage applicatif configurable haute performance qui assure une protection étendue des services clés du réseau tels que Web, transfert de fichiers, services Windows et DNS.
- Conçu pour protéger contre les vulnérabilités applicatives, notamment vers, chevaux de Troie, logiciels espions et intrusions par porte dérobée.
- Le langage extensible de signatures fournit également une défense proactive contre les nouvelles vulnérabilités découvertes dans les applications et les protocoles.
- SonicWall IPS permet d'éviter le coût et le temps nécessaires à la maintenance et à la mise à jour des signatures pour les nouvelles attaques grâce à son architecture DEA (Distributed Enforcement Architecture) leader de sa catégorie.

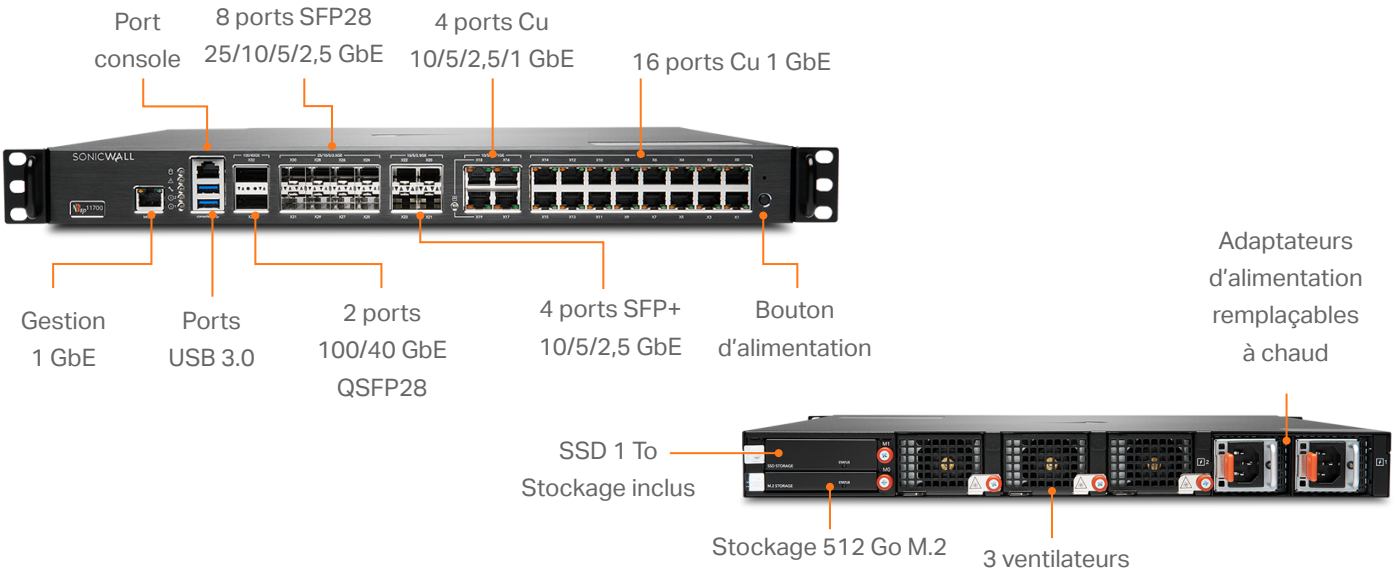
IoT et contrôle d'applications

- La série NS*sp* répertorie des milliers d'applications grâce au contrôle applicatif et surveille dans leur trafic les comportements anormaux.

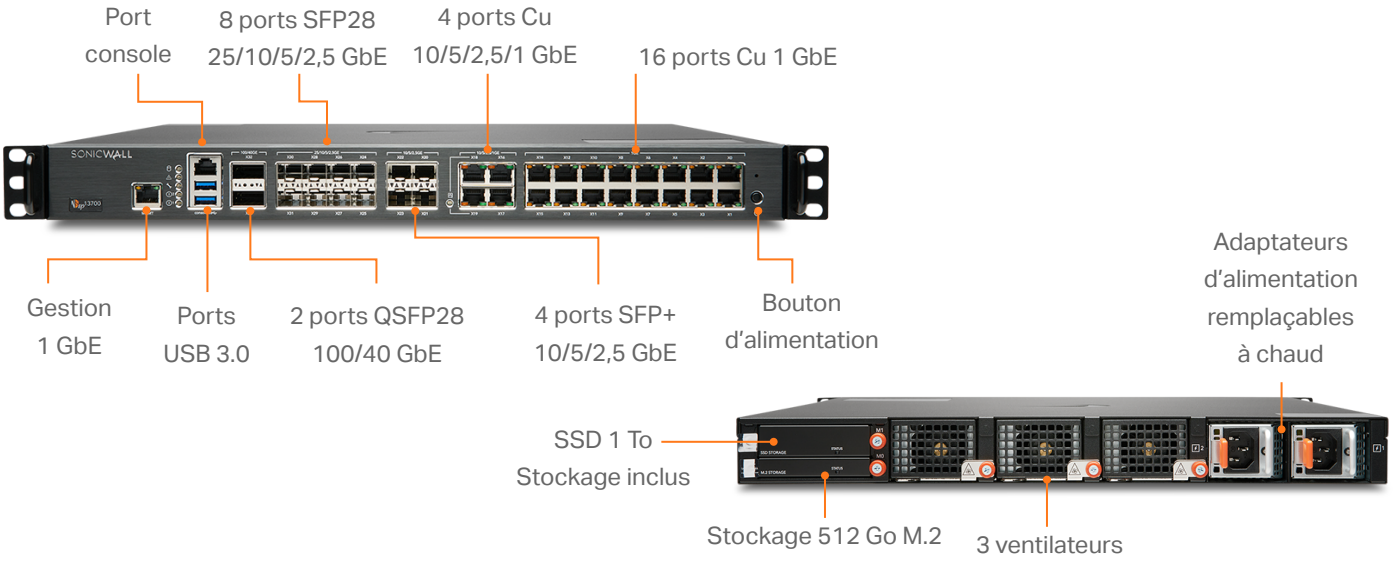
NS*sp* 10700



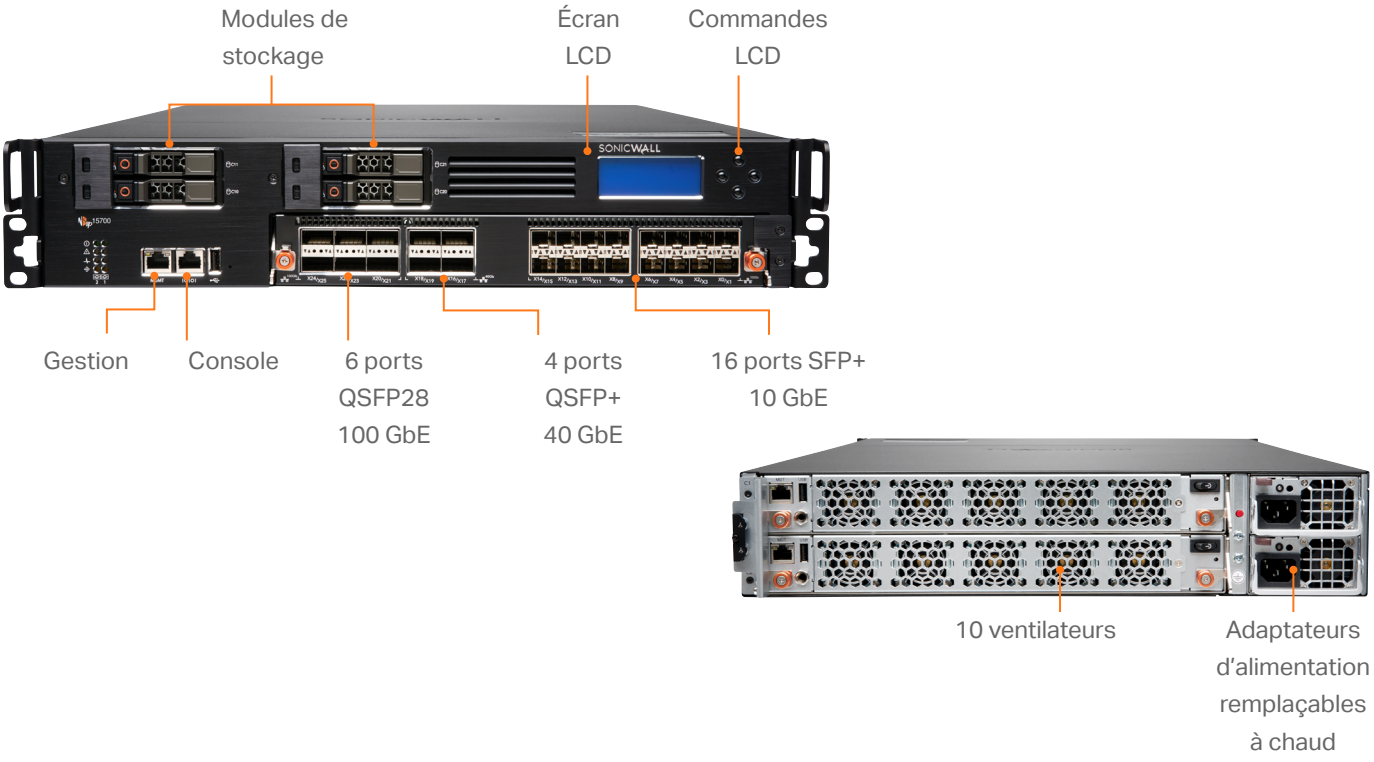
NS*sp* 11700



NS*sp* 13700



NS*sp* 15700



Caractéristiques SonicWall série NS*sp*

Pare-feu – Général	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Système d'exploitation	SonicOS 7.0.1	SonicOS 7.0.1	SonicOS 7.0.1	SonicOSX 7.0.1
Interfaces	2 QSFP28 100/40 Gbe ; 8 SFP28 25/10/5/2,5 GbE ; 4 (SFP+) 10 G/5 G/2,5 G/1 G ; 4 (Cu) 10 G/5 G/2,5 G/1 G ; 16 (Cu) 1 GbE ; 2 USB 3.0, 1 console, 1 port de gestion	2 QSFP28 100/40 GbE ; 8 SFP28 25/10/5/2,5 GbE ; 4 (SFP+) 10 G/5 G/2,5 G/1 G ; 4 (Cu) 10 G/5 G/2,5 G/1 G ; 16 (Cu) 1 GbE ; 2 USB 3.0, 1 console, 1 port de gestion	2 QSFP28 100/40 GbE ; 8 SFP28 25/10/5/2,5 GbE ; 4 SFP+ 10/5/2,5 GbE ; 4 Cu 10/5/2,5/1 GbE ; 16 1 GbE ; 2 USB 3.0, 1 console, 1 port de gestion	6 QSFP28 100 GbE ; 4 QSFP+ 40 GbE ; 16 SFP+ 10 GbE ; 3 USB 3.0, 1 console, 1 port de gestion
Stockage total	1,5 To	1,5 To	1,5 To	2 x 480 Go SSD
Gestion	CLI, SSH, Web UI, API REST			
Utilisateurs de l'authentification unique (SSO)	100 000			
Points d'accès pris en charge (max.)	512	512	512	512
Journalisation	Analytics, Local Log, Syslog, IPFIX, NetFlow			

Performances pare-feu/VPN	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Débit d'inspection du pare-feu[1]	42 Gbit/s	47 Gbit/s	60 Gbit/s	105 Gbit/s
Débit de prévention des menaces[2]	28 Gbit/s	37 Gbit/s	45,5 Gbit/s	82 Gbit/s
Débit d'inspection des applications[2]	30 Gbit/s	44 Gbit/s	57 Gbit/s	86 Gbit/s
Débit IPS[2]	28 Gbit/s	37 Gbit/s	48 Gbit/s	76,5 Gbit/s
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)[2]	10 Gbit/s	11,5 Gbit/s	16,5 Gbit/s	21 Gbit/s
Débit VPN[3]	22,5 Gbit/s	26,7 Gbit/s	29 Gbit/s	32 Gbit/s
Connexions par seconde	280 000	280 000	280 000	800 000
Nb max. de connexions (SPI)	15 000 000	20 000 000	25 000 000	40 000 000
Nb max. de connexions (DPI)	12 000 000	17 000 000	22 000 000	40 000 000
Connexions maximales (DPI-SSL)	1 500 000	1 750 000	2 000 000	4 000 000

VPN	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Tunnels VPN site à site	6 000	12 000	12 000	25 000
Clients VPN IPSec (max.)	2 000 (6 000)	2 000 (6 000)	2 000 (6 000)	2 000 (10 000)
Licences VPN SSL (max.)	100 (3 000)	100 (3 000)	100 (3 000)	256 (3 000)
Chiffrement/authentification	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA (1,256,384,512), Suite B Cryptography		DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1, Suite B Cryptography	
Échange de clés	Groupes Diffie Hellman 1, 2, 5, 14v			
VPN basé sur le routage	RIP, OSPF, BGP			
Certificats pris en charge	Verisign, Thawte, Cybertrust, RSA Keon, Entrust et Microsoft CA pour VPN SonicWall à SonicWall, SCEP			
Fonctionnalités VPN	Dead Peer Detection, DHCP sur VPN, traversée du NAT IPSec, passerelle VPN redondante, VPN basé sur le routage			
Plateformes Global VPN Client prises en charge	Microsoft® Windows 11, Windows 10 (64 et 32 bits)			
NetExtender	Microsoft Windows Vista 32/64 bits, Windows 7, Windows 8.0 32/64 bits, Windows 8.1 32/64 bits, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE			
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (intégré)			

Gestion de réseau	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Pare-feu multi-instance	N/D	N/D	N/D	Nb. max. de clients par équipement : 12
Attribution d'adresses IP	Statique (client DHCP, PPPoE, L2TP et PPTP), serveur DHCP interne, relais DHCP			
Modes NAT	1:1, plusieurs:1, 1:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT, mode transparent			
Interfaces VLAN et de tunnel logiques (maximum)	1 024			

Caractéristiques SonicWall série NS*sp*

Gestion de réseau	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Mode filaire	–	–	–	Oui
Protocoles de routage	BGP4, OSPF, RIPv1/v2, routes statiques, routage basé sur des règles	BGP4, OSPF, RIPv1/v2, routes statiques, routage basé sur des règles	BGP4, OSPF, RIPv1/v2, routes statiques, routage basé sur des règles	BGP, OSPF, RIPv1/v2, routes statiques, routage basé sur des règles
Qualité de service	Priorité de la bande passante, bande passante maximale, bande passante garantie, marquage DSCP, 802.1e (WMM)			
Authentification	LDAP (domaines multiples), XAUTH/RADIUS, TACACS+, SSO, comptabilité Radius NTLM, base de données utilisateurs interne, 2FA, Terminal Services, Citrix, Common Access Card (CAC)		LDAP (domaines multiples), XAUTH/RADIUS, SSO, Novell, base de données utilisateurs interne, Terminal Services, Citrix, Common Access Card (CAC)	
Base de données utilisateurs locale	4 000	4 000	4 000	5 000
VoIP	H323-v1-5 complet, SIP			
Normes	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Conforme FIPS 140-2	En instance	En instance	En instance	Oui
Certifications	Pare-feu d'entreprise ICSA, antivirus ICSA, IPv6/USGv6			
Certifications (en cours)	NDPP Common Criteria, pare-feu avec VPN et IPS			
Haute disponibilité	Active/passive avec synchronisation d'état			

Matérielle	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Bloc d'alimentation	2 x350 W	2 x350 W	2 x350 W	Double, redondante, 1200 W
Ventilateurs	3 (amovibles)	3 (amovibles)	3 (amovibles)	10
Alimentation redondante	100-240 VCA, 50-60 Hz			
Consommation électrique maximale (W)	155,3	155,3	181,2	834,4
Dissipation thermique totale	529,57 BTU	529,57 BTU	617,89 BTU	2 845,3 BTU
Format	1U rackable	1U rackable	1U rackable	2U rackable
Dimensions	43 x 46 x 4,5 cm 16,9 x 18,1 x 1,8 in	43 x 46 x 4,5 cm 16,9 x 18,1 x 1,8 in	43 x 46 x 4,5 cm 16,9 x 18,1 x 1,8 in	68,6 x 43,8 x 8,8 (cm)
Poids	9,1 kg	9,1 kg	9,1 kg	26 kg
Poids DEEE	11 kg	11 kg	11 kg	30,1 kg
Poids avec emballage	14,9 kg	14,9 kg	14,9 kg	37,3 kg
Environnement (en fonctionnement/stockage)	0 à 40 °C (32 à 105 °F)/-40 à 70 °C (-40 à 158 °F)			
Taux d'humidité	0-90%, non condensée	0-90%, non condensée	0-90%, non condensée	10 à 95 % sans condensation

Réglementation	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Numéros de modèles réglementaires	1RK54-118	1RK54-119	1RK54-118	2RK05-0FE
Conformité aux normes suivantes	FCC classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI classe A, MSIP/KCC classe A, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH, ANATEL, BSMI	FCC classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI classe A, MSIP/KCC classe A, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH, ANATEL, BSMI	FCC classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI classe A, MSIP/KCC classe A, UL, cUL, TÜV/GS, CB, Mexico CoC par UL, DEEE, REACH, ANATEL, BSMI	FCC classe A, ICES classe A, CE (EMC classe A, LVD, RoHS), C-Tick, VCCI classe A, MSIP/KCC classe A, UL, cUL, TÜV/GS, CB, UL Mexico notification DGN, DEEE, REACH, ANATEL, BSMI

[1] Méthodes de test : performances maximales basées sur RFC 2544 (pour pare-feu). Les performances réelles peuvent varier en fonction des conditions réseau et des services activés.

[2] Débit de prévention des menaces/antivirus de passerelle/anti-logiciels espions/IPS mesuré en utilisant les outils de test 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-spyware, l'IPS et le contrôle des applications.

[3] 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.

Récapitulatif des fonctionnalités SonicOSX et SonicOS

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
- Intégration points d'accès SonicWall Wi-Fi 6

Règles de sécurité unifiées

- Les règles unifiées combinent les règles de la couche 3 à la couche 7 :
  - Source/Destination IP/Port/Service
  - Contrôle des applications
  - CFS/Filtrage Web
  - Application des services « single pass » de sécurité
  - IPS/GAV/AS/Capture ATP
- Gestion des règles :
  - Clonage
  - Analyse des règles Shadow
  - Modification cellule
  - Modification groupe
- Gestion des vues
  - Règles utilisées/non utilisées
  - Règles actives/non actives
  - Sections

Déchiffrement et inspection TLS/SSL/SSH

- TLS 1.3
- 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
- Règles de déchiffrement SSL/TLS et SSH

Capture Advanced Threat Protection[1]

- 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
- Intégration Capture Client

Prévention des intrusions[1]

- Analyse basée sur des signatures
- Intégration du contrôle d'accès réseau avec Aruba ClearPass
- Mise à jour automatique des signatures
- 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[1]

- 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[1]

- 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[1]

- 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
- Content Filtering Client

VPN

- 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 (OSPF, RIP, BGP)

Gestion de réseau

- Pare-feu multi-instance (uniquement sur NS*sp* 15700)
- PortShield
- Trames Jumbo
- Découverte du chemin MTU
- Journalisation améliorée
- VLAN Trunking
- Mise en miroir des ports
- Qualité de service de couche 2
- Sécurité des ports
- Routage dynamique (RIP/OSPF/BGP)
- Routage à base de règles (ToS/métrique et ECMP)
- NAT
- Serveur DHCP
- Gestion de la bande passante
- Agrégation de liens (statique et dynamique)
- Redondance de ports
- Haute disponibilité active/passive avec synchronisation d'état
- Équilibrage de la charge entrante/sortante
- Haute disponibilité – active/standby avec synchronisation d'état
- Mode filaire virtuel/filaire, mode TAP, mode NAT
- Routage asymétrique

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
- API Rest
- Prise en charge de l'appli. mobile SonicExpress
- SNMPv2/v3
- Gestion et reporting centralisés avec SonicWall Network Security Manager (NSM)[1]
- Journalisation
- Exportation NetFlow/IPFix
- Sauvegarde cloud de la configuration
- Visualisation de la bande passante et des applications
- Gestion IPv4 et IPv6

[1] Requiert un abonnement supplémentaire

Trouvez le pare-feu SonicWall qui vous convient

www.sonicwall.com/firewalls

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, consultez notre site à l'adresse : www.sonicwall.com.

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

Datasheet-NSsp-A4-JK-9962