

Fiche technique du NSsp™ 15700 de SonicWall

La solution Network Security services platform™ (NSsp) 15700 de SonicWall est un pare-feu de nouvelle génération avec une densité de ports élevée et des interfaces multi-gigabit, qui peut traiter plusieurs millions de connexions contre les menaces « zero-day » et évoluées. Conçue pour les grandes entreprises, les établissements d'enseignement supérieur, les agences gouvernementales et les MSSP, elle élimine les attaques en temps réel sans perte de performance. Elle est conçue pour être hautement fiable et pour fournir un service ininterrompu aux organisations.

Pare-feu haut débit de qualité professionnelle

À mesure que les entreprises évoluent et que se multiplient les appareils gérés et non gérés, les réseaux, les charges de travail dans le cloud, les applications SaaS, les utilisateurs, les débits Internet et les connexions chiffrées, un pare-feu qui ne peut prendre en charge aucun de ces éléments devient un goulet d'étranglement dans le paysage informatique. Un pare-feu doit être un point fort, pas un point faible.

Les interfaces 100G/40G/10G multiples du NSsp 15700 de SonicWall vous

permettent de traiter simultanément plusieurs millions de connexions chiffrées ou non avec une technologie de prévention des menaces inégalée. 70 % de toutes les sessions étant chiffrées, disposer d'un pare-feu capable de traiter et d'examiner ce trafic sans perturber l'expérience de l'utilisateur final est essentiel pour favoriser la productivité et garantir la sécurité des informations.

L'interface de règles unifiée du NSsp 15700 permet aux organisations de créer de façon simple et intuitive un accès et des règles de sécurité depuis une seule interface unifiée.

Gestion et reporting simplifiés

La gestion, la surveillance et le reporting en continu des activités sont gérés depuis SonicWall Network Security Manager (en attente). Cela offre un tableau de bord intuitif pour la gestion des activités du pare-feu tout en fournissant des rapports historiques, depuis une source unique. 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.



Avantage du NSsp 15700 de SonicWall :

- Densité de ports élevée
- Ports 100 GbE
- Pare-feu multi-instances
- S'intègre sur sandboxing sur le cloud ou sur site
- Compatible SD-Branch
- Gestion unifiée sur un seul et même écran depuis le cloud ou le pare-feu
- Stockage intégré et extensible
- Alimentation redondante
- Prise en charge SonicOSX 7.0
- Prise en charge de TLS 1.3
- Prend en charge des millions de connexions TLS simultanées
- Faible coût total de possession

Déploiement

Pare-feu de nouvelle génération

- Géré depuis un seul et même écran
- NSsp 15700 intègre le reste des solutions de l'écosystème de SonicWall
- Visibilité complète sur votre réseau pour voir l'activité des applications, appareils et utilisateurs afin d'appliquer les règles et d'éliminer les menaces et goulets d'étranglement de la bande passante
- Intégration à Capture ATP avec la solution RTDMI pour le sandboxing sur le cloud ou un appareil Capture Security pour la détection des logiciels malveillants sur site

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

- NSsp 15700 assure l'inspection pour des millions de connexions TLS/SSL et SSH chiffrées et simultanées indépendamment du port ou du protocole.
- Les règles d'inclusion et d'exclusion permettent la personnalisation spécifiquement en fonction de la conformité de l'organisation ou des obligations légales.
- Prise en charge des suites de chiffrement TLS jusqu'à TLS 1.3

Segmentation et mise en réseau

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

Pare-feu multi-instances

- La multi-instance est la prochaine génération de mutualisation
- Chaque locataire est isolé avec des ressources informatiques dédiées pour éviter le manque de ressources
- Elle dispose des ports/locataires physiques et logiques
- Elle prend en charge les règles de locataire indépendant et la gestion de la configuration
- Exploitation de l'indépendance de la version et de la prise en charge haute disponibilité pour les locataires

Fonctionnalité du mode filaire

- Mode contournement pour l'introduction rapide et peu perturbatrice du matériel du pare-feu sur un réseau
- Mode inspection pour prolonger le mode contournement sans altérer de façon fonctionnelle le cheminement des paquets à faible risque et à latence zéro
- Mode sécurisé pour interposer activement les processeurs multicœurs du pare-feu sur le cheminement de traitement du paquet
- Mode Tap pour ingérer un flux de paquets en miroir depuis un seul port de commutateur sur le pare-feu, éliminant le besoin d'une insertion physique par un intermédiaire

Protection avancée contre les menaces

- SonicWall Capture Advanced Threat Protection™ (ATP) est utilisé par plus de 150 000 clients partout dans le monde parmi un ensemble de solutions, et il aide à découvrir et à arrêter plus de 1 200 nouvelles formes de logiciels malveillants chaque jour ouvrable.
- Pour les clients particulièrement sensibles à la conformité et à la performance, la solution NSsp 15700 intègre Capture Security appliance (CSa), un appareil local basé sur la technologie d'analyse de fichier basée sur la mémoire, 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

- Comparaison des sites Web demandés par rapport à une base de données géante sur le cloud qui contient des millions d'URL, d'adresses IP et de sites Web classés
- Création et application de règles qui autorisent ou bloquent l'accès aux sites en fonction de l'identité de l'individu ou du groupe, ou en fonction de l'heure, pour plus de 50 catégories prédéfinies

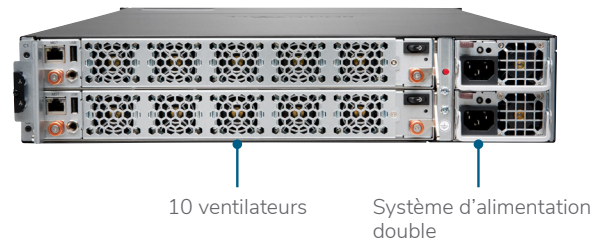
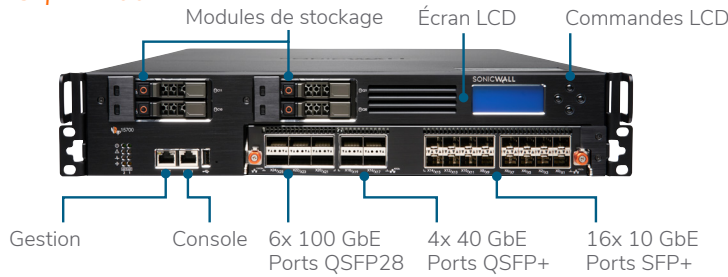
Système de prévention des intrusions (IPS)

- Moteur d'inspection approfondie des paquets configurable et haute performance pour la protection élargie des services clés du réseau, notamment le Web, le courrier électronique, le transfert de fichiers, les services Windows et le DNS
- Protection contre les vulnérabilités d'applications et contre les vers, les chevaux de Troie et les failles de P2P, des logiciels espions et des portes dérobées
- Le langage de signature extensible offre une défense proactive contre les vulnérabilités des applications et des protocoles récemment découvertes
- L'IPS de SonicWall permet de se décharger du fardeau long et coûteux que représentent l'entretien et la mise à jour des signatures pour les nouvelles attaques grâce à l'architecture de mise en œuvre distribuée (DEA) de SonicWall, leader du secteur

IdO et contrôle des applications

- Le NSsp 15700 répertorie des milliers d'applications sur App Control et surveille leur trafic à la recherche de comportements anormaux depuis la solution Application Firewall intégrée
- Segment géré depuis les appareils non gérés avec une gestion unique et des profils d'accès

NSsp 15700



Caractéristiques du NSsp 15700 de SonicWall

GÉNÉRALITÉS DES PARE-FEU		NSsp 15700
Système d'exploitation	SonicOSX 7	
Interfaces	6 x 100 GbE QSFP28, 4 x 40 GbE QSFP+, 16 x 10 GbE SFP+	
Stockage intégré	2 x 480 GB SSD	
Gestion	CLI, SSH, IU Web, API REST	
Utilisateurs SSO	100 000	
Journalisation	Analyzer, Local Log, Syslog, IPFIX, NetFlow	
PERFORMANCES PARE-FEU/VPN		NSsp 15700
Débit d'inspection du pare-feu	105 Gbit/s	
Débit prévention des menaces	82 Gbit/s	
Débit d'inspection des applications	86 Gbit/s	
Débit IPS	76,5 Gbit/s	
Débit IMIX	28,5 Gbit/s	
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)	21 Gbit/s	
Débit VPN	32 Gbit/s	
Connexions par seconde	800k	
Nombre maximum de connexions (SPI)	80M	
Nombre maximum de connexions (DPI)	50M	
Connexions maximales (DPI-SSL)	3M	
VPN		NSsp 15700
Tunnels VPN site à site	25 000	
Clients VPN IPSec (maximum)	2 000 (10 000)	
Clients VPN SSL NetExtender (maximum)	2 (3 000)	
Chiffrement/authentification	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	
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 Vista 32/64 bits, Windows 7 32/64 bits, Windows 8.0 32/64 bits, Windows 8.1 32/64 bits, Windows 10	
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		NSsp 15700
Pare-feu multi-instances	Nombre maximum de locataires pour le matériel : 12	
Attribution d'adresses IP	Statique, (DHCP, PPPoE, L2TP et client PPTP), serveur DHCP interne, relais DHCP	
Modes NAT	1 à 1, plusieurs à 1, 1 à plusieurs, NAT flexible (IP superposées), PAT, mode transparent	
Interfaces VLAN	512	
Mode filaire	Oui	
Protocoles de routage	BGP, OSPF, RIPv1/v2, routes statiques, routage à base de règles	

Caractéristiques du NSsp 15700 de SonicWall

Qualité de service	Priorité de la bande passante, bande passante maximale, bande passante garantie, marquage DSCP, 802.1p
Authentification	LDAP, XAUTH/RADIUS, SSO, Novell, base de données utilisateurs interne, Terminal Services, Citrix
VoIP	H.323/v1-5 complet, SIP
Normes	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3
Certifications (en cours)	Pare-feu ICSA, antivirus ICSA, FIPS 140-2, NDPP Common Criteria (pare-feu et IPS), APL UC, USGv6, CsFC
Haute disponibilité	Active/passive avec synchro. d'état, DPI actif/actif avec synchro. d'état, clustering actif/actif
MATÉRIEL	NSsp 15700
Alimentation électrique	Double, redondant, 1 200 W
Ventilateurs	10
Puissance d'entrée	100 à 240 V CA, 50-60 Hz
Consommation électrique maximale (W)	1065
Format	2U rackable
Dimensions	68,6 x 43,8 x 8,8 po
Poids	26 kg
Poids DEEE	30,1 kg
Poids avec emballage	37,3 kg
Dimension du colis	28 x 63 x 86 po
Réglementations majeures	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, notification UL DGN pour le Mexique, DEEE, REACH, ANATEL, BSMI
Environnement (en fonctionnement/stockage)	0 à 40 °C (32 à 105 °F)/-40 à 70 °C (-40 à 158 °F)
Taux d'humidité	10 à 95 % sans condensation

Récapitulatif des fonctionnalités de SonicOSX

Pare-feu

- Inspection d'état 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 Switch SonicWall

Politique de sécurité unifiée

- La politique de sécurité combine les règles de la couche 4 à la couche 7 :
 - Source/IP de destination IP/Port/Service
 - Contrôle des applications
 - Filtrage CFS/Web
 - Application des services de sécurité en un seul passage
 - IPS/GAV/AS/Capture ATP
- Gestion des règles :
 - Clonage
 - Analyse de la règle de l'ombre
 - Modification dans la cellule
 - Modification groupée
- Affichages de gestion
 - Règles utilisées/non utilisées
 - Règles actives/inactives
 - 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
- Politiques de déchiffrement pour SSL/TLS et SSH

Capture Advanced Threat Protection²

- 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 contre les intrusions²

- Analyse basée sur des signatures
- Mise à jour automatique des signatures
- Inspection bidirectionnelle
- Fonctionnalité de règles IPS granulaires
- Localisation GeolIP
- Filtrage de réseaux de zombies avec liste dynamique
- Détection des expressions régulières

Anti-logiciels malveillants²

- 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 applications²

- 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/HTTPS²

- Filtrage des URL
- Évitement de proxy
- Blocage par mots-clés
- 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

- Architecture multi-instances
- PortShield
- Trames Jumbo
- Découverte de cheminement MTU
- Journalisation améliorée
- Jonction VLAN
- 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 liens¹ (statique et dynamique)
- Redondance de ports¹
- Haute disponibilité A/P avec synchro. d'état
- Clustering A/A¹
- Équilibrage de la charge entrante/ sortante
- Haute disponibilité – active/passive 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
- Inscription et configuration sans intervention
- Prise en charge de l'application mobile SonicExpress
- SNMPv2/v3
- Gestion et reporting centralisés avec SonicWall Global Management System (GMS)²
- Journalisation
- Exportation NetFlow/IPFix
- Sauvegarde cloud de la configuration
- Plateforme d'analyse de sécurité BlueCoat
- Visualisation de la bande passante et des applications
- Gestion IPv4 et IPv6

¹ Pas pris en charge sur les pare-feux de la série NSv

² Requiert un abonnement supplémentaire.

Produit	Référence
SONICWALL NSSP 15700	02-SSC-2722
OFFRE ESSENTIELLE DE LA SUITE SÉCURITÉ DE PASSERELLE POUR NSSP 15700, 1 AN	02-SSC-4739
OFFRE ESSENTIELLE DE LA SUITE SÉCURITÉ DE PASSERELLE POUR NSSP 15700, 3 ANS	02-SSC-4740
OFFRE ESSENTIELLE DE LA SUITE SÉCURITÉ DE PASSERELLE POUR NSSP 15700, 5 ANS	02-SSC-4741
ASSISTANCE 24 H/24, 7 J/7 POUR NSSP 15700, 1 AN	02-SSC-4733
ASSISTANCE 24 H/24, 7 J/7 POUR NSSP 15700, 3 ANS	02-SSC-4734
ASSISTANCE 24 H/24, 7 J/7 POUR NSSP 15700, 5 ANS	02-SSC-4735

Offres	Référence
SONICWALL NSSP 15700 TOTALSECURE, ÉDITION ESSENTIELLE, 1 AN	02-SSC-4764
SONICWALL NSSP 15700 TOTALSECURE, ÉDITION ESSENTIELLE, 3 ANS	02-SSC-4766
SONICWALL NSSP 15700 TOTALSECURE, ÉDITION ESSENTIELLE, 5 ANS	02-SSC-4765

Accessoires	Référence
10 GB-SR SFP+ MODULE DE FIBRE À COURTE PORTÉE MULTI-MODE, SANS CÂBLE	01-SSC-9785
10 GB-LR SFP+ MODULE DE FIBRE À LONGUE PORTÉE MODE UNIQUE, SANS CÂBLE	01-SSC-9786
10 GB SFP+ CUIVRE AVEC 1 M DE CÂBLE TWINAX	01-SSC-9787
10 GB SFP+ CUIVRE AVEC 3 M DE CÂBLE TWINAX	01-SSC-9788
10 GB-SX SFP, MODULE DE FIBRE À COURTE PORTÉE MULTI-MODE, SANS CÂBLE	01-SSC-9789
10 GB-LX SFP, MODULE DE FIBRE À LONGUE PORTÉE MODE UNIQUE, SANS CÂBLE	01-SSC-9790
1GB-RJ45 SFP, MODULE CUIVRE, SANS CÂBLE	01-SSC-9791
SONICWALL SFP+ 10GBASE-T, TRANSMETTEUR CUIVRE, MODULE RJ45	02-SSC-1874

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites 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 en savoir plus, rendez-vous sur www.sonicwall.com.