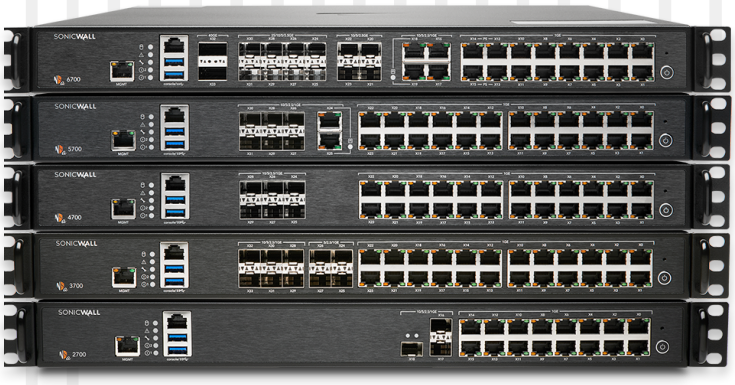
SonicWall NS*a Series*
7ème génération

Les pare-feux SonicWall Network Security Appliance (NS*a*) de septième génération offrent aux entreprises de moyenne à grande taille des performances haut de gamme au coût total de possession le plus faible de leur catégorie.

Dotés d'un éventail complet de fonctionnalités de sécurité – prévention des intrusions, VPN, contrôle applicatif, analyse des logiciels malveillants, filtrage des URL, sécurité DNS ou services Geo-IP et de botnet –, ils protègent le périmètre contre les menaces les plus évoluées sans encombrer le réseau.



NS*a Series* 7ème génération, aperçu des caractéristiques.
Voir toutes les caractéristiques »

Jusqu'à 19 Gbit/s	Jusqu'à 8 millions	40 G/25 G/10 G/ 5 G/2,5 G/1 G
Débit de prévention des menaces	Connexions	Ports

AVANTAGES

- Facteur de forme 1 U
- Prise en charge de ports 40 G/25 G/10 G/5 G/2,5 G/1 G
- Débit d'analyse multi-gigabit des menaces et malwares
- Excellentes performances TLS (sessions et débit)
- Stockage extensible
- Sécurité DNS
- Service de filtrage de contenu basé sur la réputation (CFS 5.0)
- Gestion du Wifi 6 par le pare-feu
- Intégration du contrôle d'accès réseau avec Aruba ClearPass
- Prête pour la périphérie Internet de niveau entreprise
- Tout nouveau SonicOS 7ème génération
- Fonctionnalité Secure SD-WAN
- Interface utilisateur intuitive avec gestion centralisée
- Prise en charge TLS 1.3
- Rapport prix/performances haut de gamme
- Support de l'équipe de recherche sur les menaces Capture Labs
- Grande densité de ports facilitant la mise en réseau
- Intégration de SonicWall Switch, des points d'accès SonicWave et de Capture Client
- Alimentation redondante

FICHE TECHNIQUE

De par sa grande densité de ports, dont plusieurs ports 40 GbE et 10 GbE – la solution prend en charge la redondance réseau et matériel avec la haute disponibilité et des alimentations doubles.

Les pare-feux SonicWall Network Security Appliance (NS*a*) de septième génération offrent aux entreprises de moyenne à grande taille des performances haut de gamme au coût total de possession le plus faible de leur catégorie.

Dotés d'un éventail complet de fonctionnalités de sécurité – prévention des intrusions, VPN, contrôle applicatif, analyse des logiciels malveillants, filtrage des URL, sécurité DNS ou services Geo-IP et de botnet –, ils protègent le périmètre contre les menaces les plus évoluées sans encombrer le réseau.

Les pare-feux NS*a* de 7ème génération intègrent les composants matériels les plus récents, tous conçus pour assurer un débit de prévention des intrusions multi-gigabit – même pour le trafic chiffré. De par sa grande densité de ports, dont plusieurs ports 40 GbE et 10 GbE – la solution prend en charge la redondance réseau et matériel avec la haute disponibilité et des alimentations doubles.

7ème génération : SonicOS 7 et services de sécurité

La série NS*a* de 7ème génération fonctionne sur SonicOS 7.0, un nouveau système d'exploitation entièrement pensé pour offrir une interface utilisateur moderne, des workflows intuitifs et des principes de conception orientés utilisateur. SonicOS 7 présente diverses fonctionnalités conçues pour faciliter les workflows professionnels. Il assure une configuration aisée des règles, un déploiement zéro intervention et une gestion flexible, autant d'avantages qui permettent aux entreprises d'améliorer à la fois leur sécurité et leur efficacité opérationnelle.

Les pare-feux série NS*a* de 7ème génération prennent en charge des fonctionnalités réseau évoluées, telles que le SD-WAN, le routage dynamique, la haute disponibilité des couches 4 à 7 ainsi que le VPN haut débit. Outre les fonctionnalités de pare-feu et de commutateur, ils proposent une seule et même interface permettant de gérer à la fois les commutateurs et les points d'accès.

Conçue pour déjouer les cyberattaques d'aujourd'hui et de demain, la série NS*a* de 7ème génération donne accès aux services de sécurité avancés des pare-feux SonicWall, afin de protéger votre infrastructure IT dans son intégralité. Des solutions et services tels que Cloud Application Security, le service de sandboxing dans le cloud Capture ATP (Advanced Threat Protection), les technologies brevetées Real-Time Deep Memory Inspection (RTDMI™) et Reassembly-Free Deep Packet Inspection (RFDPI) – pour l'ensemble du trafic, y compris TLS 1.3 – assurent une protection complète au niveau de la passerelle contre les menaces les plus furtives et les plus dangereuses, notamment les menaces zero-day et chiffrées.

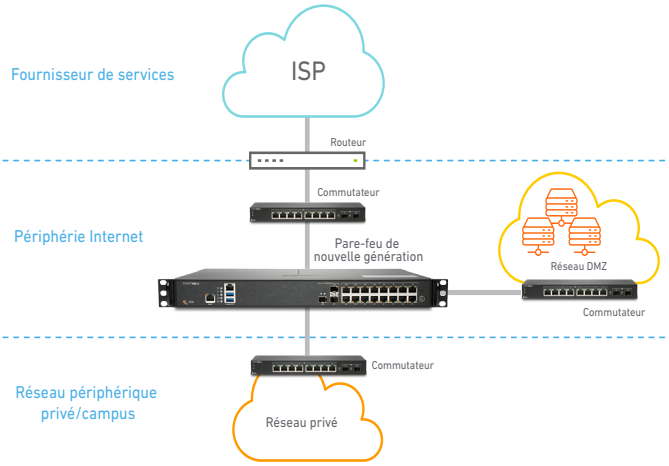
Déploiements

La série NS*a* de 7ème génération présente principalement deux options de déploiement pour les entreprises moyennes et distribuées :

Déploiement à la périphérie d'Internet

Dans cette option de déploiement standard, le pare-feu NS*a* de 7ème génération protège les réseaux privés contre le trafic malveillant provenant d'Internet, et vous permet de :

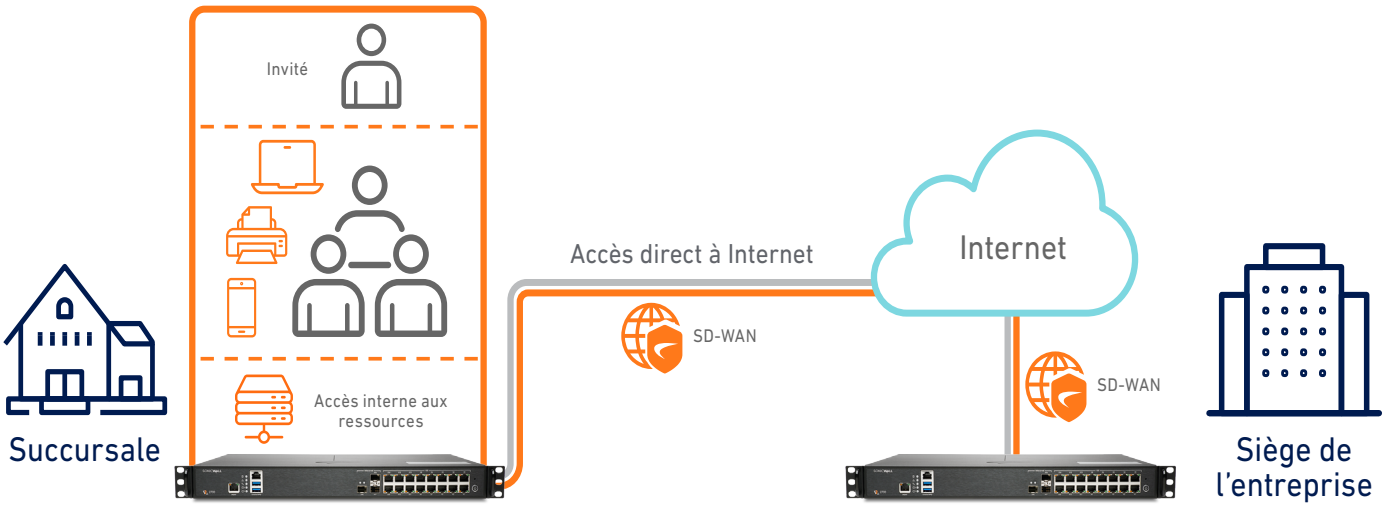
- Déployer une solution de pare-feu éprouvée, offrant les meilleures performances et la plus grande densité de ports de sa catégorie (y compris la connectivité 40 GbE et 10 GbE)
- Gagner en visibilité et inspecter le trafic chiffré, y compris TLS 1.3, afin de bloquer les menaces évasives provenant d'Internet – sans compromettre les performances
- Protéger votre entreprise grâce à une sécurité intégrée, englobant l'analyse des logiciels malveillants, la sécurité des applications cloud, le filtrage des URL et les services de réputation
- Economiser de la place et de l'argent avec une solution de pare-feu intégrée alliant des fonctionnalités de sécurité et de réseau de pointe
- Simplifier les processus et maximiser l'efficacité grâce à un système de gestion centralisée via une interface utilisateur intuitive sur un seul écran



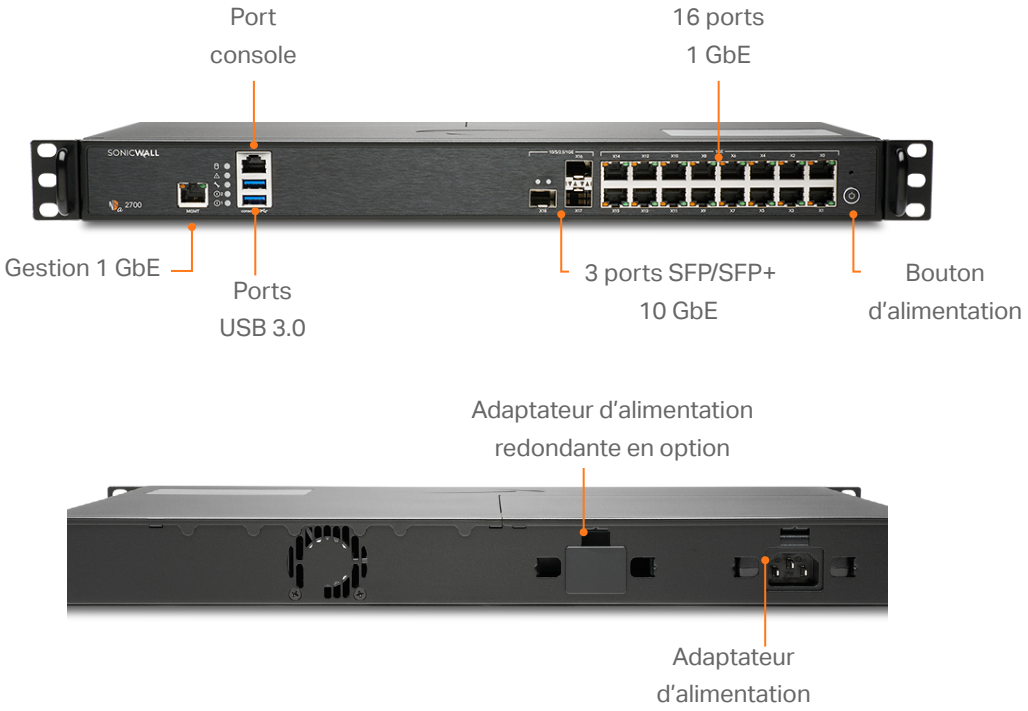
Entreprises moyennes et distribuées

La série SonicWall NS*a* de 7ème génération prend en charge le SD-WAN et peut être gérée de manière centralisée, ce qui en fait une solution idéale pour les entreprises moyennes et distribuées. Ce déploiement permet aux organisations de :

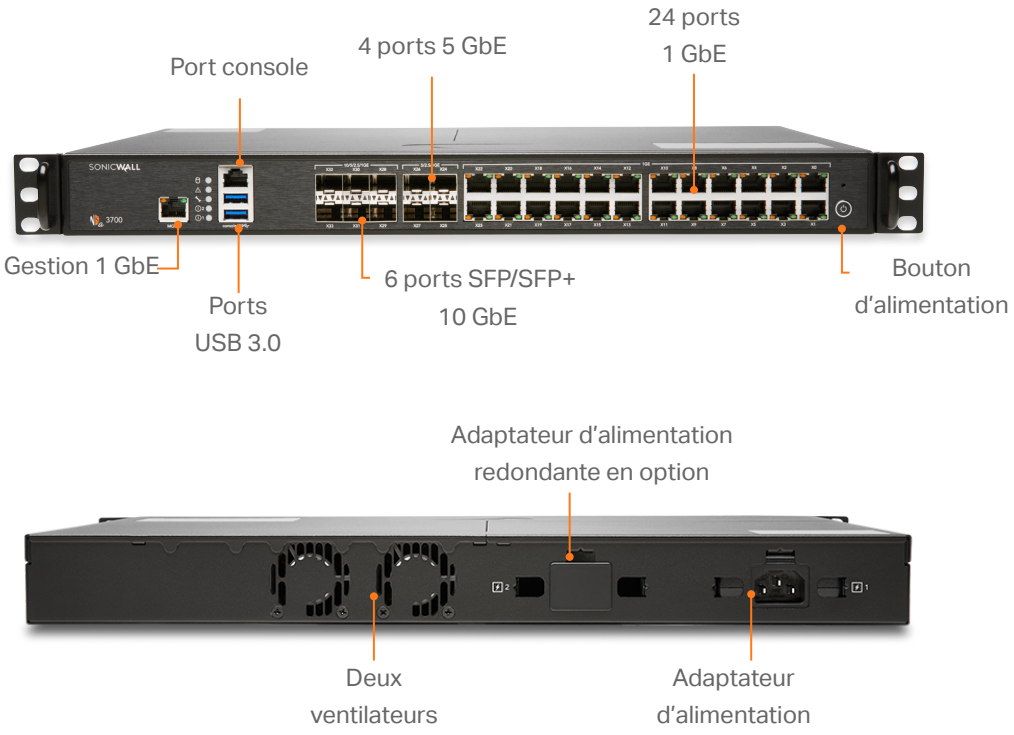
- S'armer durablement face à un paysage de menaces en constante mutation en investissant dans un pare-feu garant de performances d'analyse multi-gigabits
- Fournir un accès direct et sécurisé aux différentes succursales au lieu d'avoir à repasser par le siège de l'entreprise
- Permettre aux succursales distribuées d'accéder en toute sécurité aux ressources internes, que ce soit au siège ou dans un cloud public, et d'améliorer ainsi sensiblement la latence au niveau des applications
- Bloquer automatiquement les menaces utilisant des protocoles chiffrés, comme TLS 1.3, et sécuriser ainsi le réseau face aux attaques les plus évoluées
- Simplifier les processus et maximiser l'efficacité grâce à un système de gestion centralisée via une interface utilisateur intuitive sur un seul écran
- Profiter de la grande densité de ports incluant la connectivité 40 GbE et 10 GbE, conçue pour prendre en charge les entreprises distribuées et les réseaux WAN



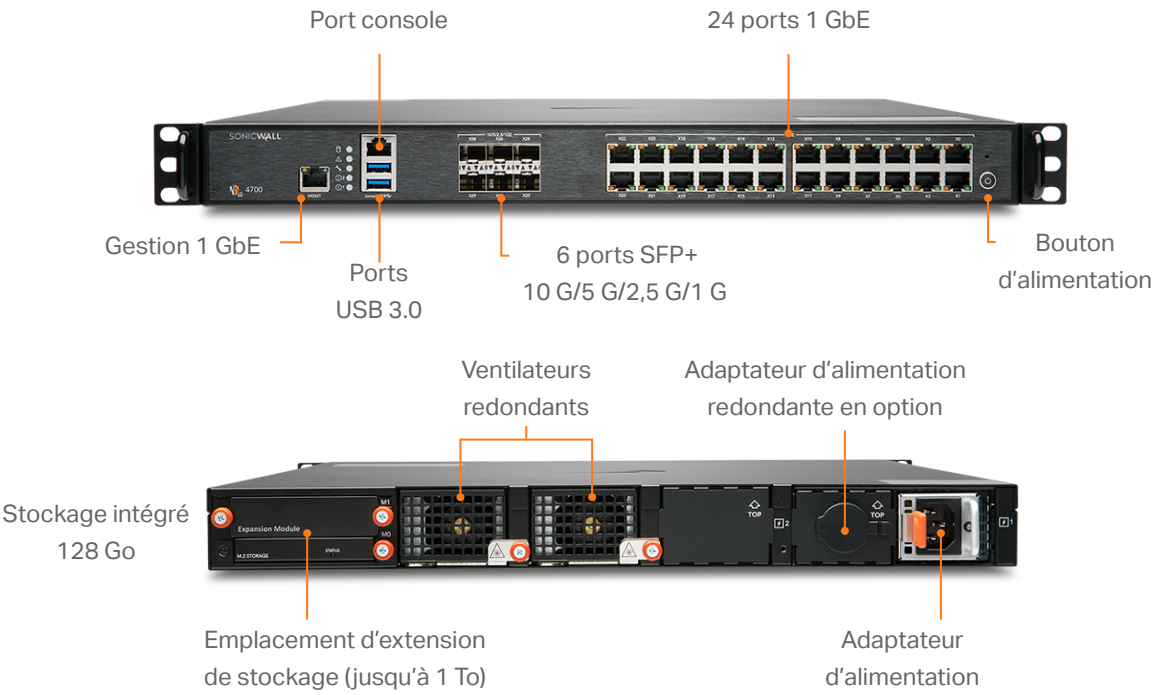
NS*a* 2700



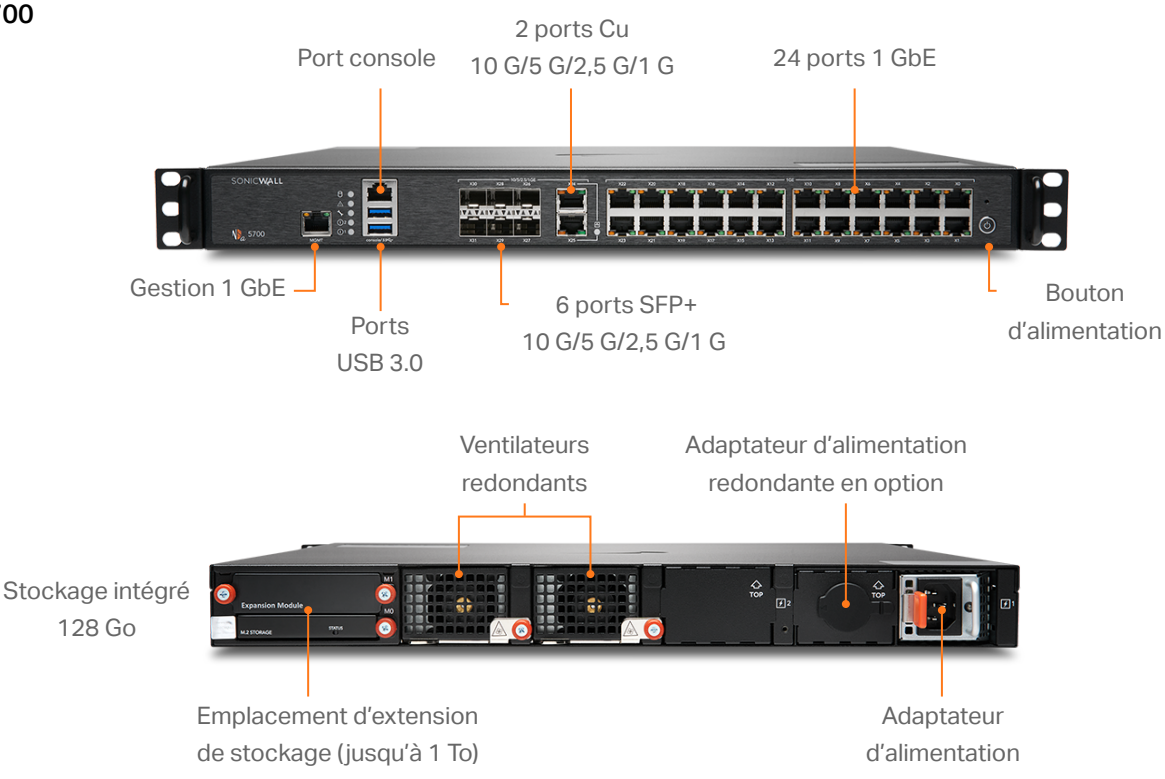
NS*a* 3700



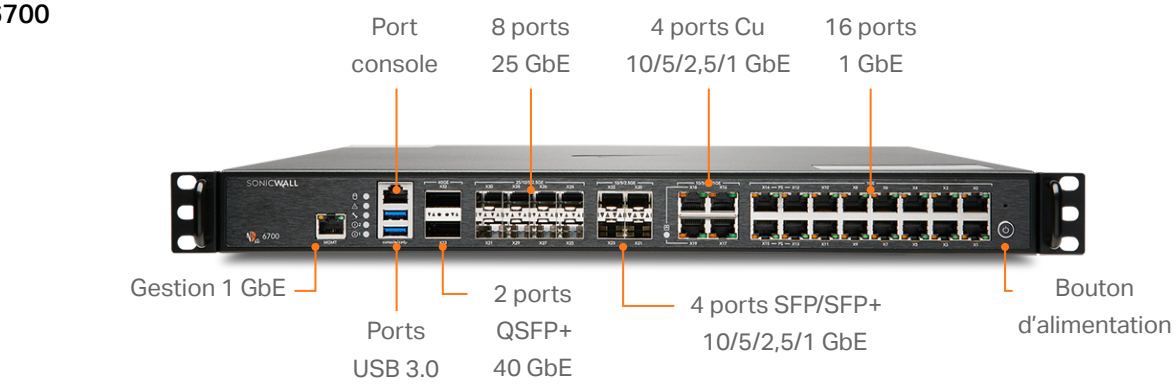
NS*a* 4700

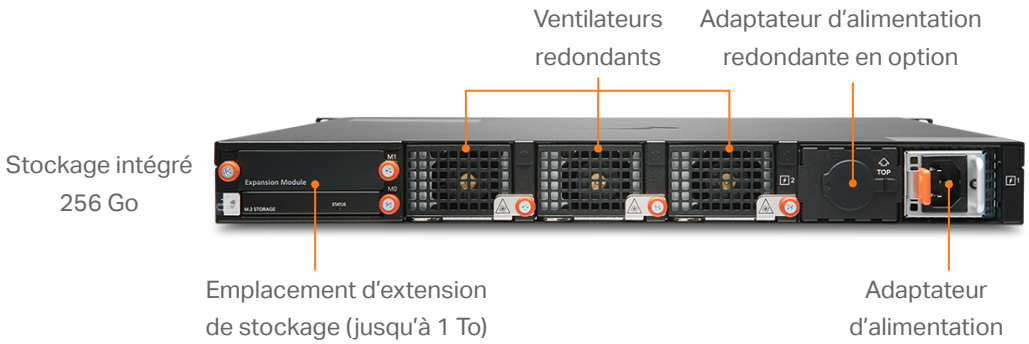


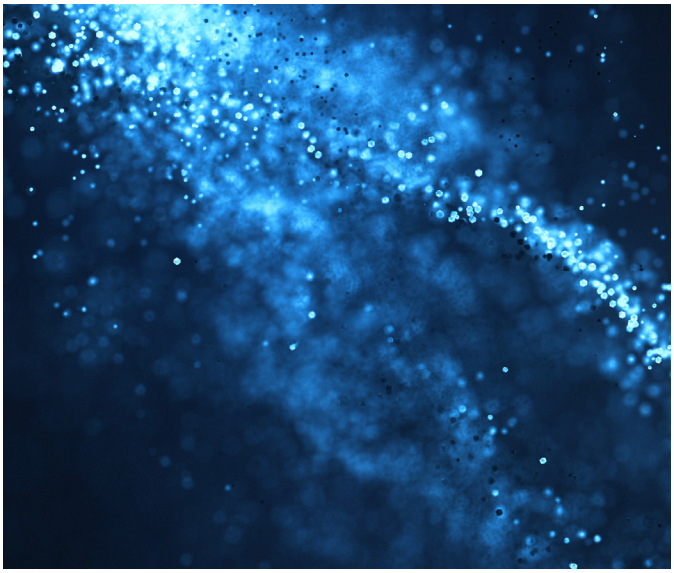
NS*a* 5700



NS*a* 6700







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

Série NS*a* 7ème génération, spécifications système

Pare-feu	NS*a* 2700	NS*a* 3700	NS*a* 4700	NS*a* 5700	NS*a* 6700
Système d'exploitation			SonicOS 7		
Interfaces	16 x 1 GbE, 3 x SFP+ 10 G, 2 USB 3.0, 1 console, 1 port de gestion	24 x 1 GbE, 6 x SFP+ 10 G, 4 x SFP+ 5 G, 2 USB 3.0, 1 console, 1 port de gestion	6 x 10 G/5 G/2,5 G/1 G (SFP+) ; 24 x Cu 1 GbE 2 USB 3.0, 1 console, 1 port de gestion	6 x 10 G/5 G/ 2,5 G (SFP+) ; 2 x 10 G/5 G/ 2,5 G/1 G (Cu) ; 24 x 1 GbE (Cu) 2 USB 3.0, 1 console, 1 port de gestion	2 x 40 G ; 8 x 25 G, 4 x 10 G/5 G/2,5 G/ 1 G SFP+, 4 x 10 G/5 G/2,5 G/1 G (Cu) ; 16 x 1 GbE (Cu) 2 USB 3.0, 1 console, 1 port de gestion
Stockage	64 Go M.2	128 Go M.2	128 Go	128 Go	256 Go M.2
Extension	Emplacement d'extension de stockage (jusqu'à 256 Go)	Emplacement d'extension de stockage (jusqu'à 256 Go)	Emplacement d'extension de stockage (jusqu'à 1 To)	Emplacement d'extension de stockage (jusqu'à 1 To)	Emplacement d'extension de stockage (jusqu'à 1 To)
Interfaces VLAN et de tunnel logiques (maximum)	256	256	512	512	512
Utilisateurs de l'authentification unique (SSO)	40000	40000	50000	50000	70000
Points d'accès pris en charge (max.)	512	512	512	512	512
Performances pare-feu/VPN					
Débit d'inspection du pare-feu[1]	5,2 Gbit/s	5,5 Gbit/s	18 Gbit/s	28 Gbit/s	36 Gbit/s
Débit de prévention des menaces[2]	3,0 Gbit/s	3,5 Gbit/s	9,5 Gbit/s	15 Gbit/s	19 Gbit/s
Débit d'inspection des applications[2]	3,6 Gbit/s	4,2 Gbit/s	11 Gbit/s	18 Gbit/s	20 Gbit/s
Débit IPS[2]	3,4 Gbit/s	3,8 Gbit/s	10 Gbit/s	17 Gbit/s	20 Gbit/s
Débit d'inspection des logiciels malveillants[2]	2,9 Gbit/s	3,5 Gbit/s	9,5 Gbit/s	16 Gbit/s	18,5 Gbit/s
Débit d'inspection et de déchiffrement SSL/TLS (DPI-SSL)[2]	800 Mbit/s	850 Mbit/s	5 Gbit/s	7 Gbit/s	9 Gbit/s
Débit VPN IPSec[3]	2,10 Gbit/s	2,2 Gbit/s	11 Gbit/s	15 Gbit/s	19 Gbit/s
Connexions par seconde	21000	22000	115000	228000	228000
Nb max. de connexions (SPI)	1500000	2000000	4000000	5000000	8000000
Nb max. de connexions DPI-SSL	125000	150000	350000	350000	750000
Nb max. de connexions (DPI)	500000	750000	2000000	3500000	6000000
VPN					
Tunnels VPN site à site	2000	3000	4000	6000	6000
Clients VPN IPSec (max.)	50 (1000)	50 (1000)	500 (3000)	2000 (4000)	2000 (6000)
Licences VPN SSL (max.)	2 (500)	2 (500)	2 (1000)	2 (1500)	2 (1500)
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				
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, NAT Traversal IPSec, passerelle VPN redondante, VPN basé sur le routage				
Plateformes Global VPN Client prises en charge	Windows 10		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	Windows 10 et Linux		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, Android, Kindle Fire, Chrome OS, Windows 10		Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (intégré)		
Services de sécurité					
Services d'inspection approfondie des paquets	Antivirus de passerelle, anti-logiciels espions, prévention des intrusions, DPI-SSL				
Content Filtering Service (CFS)	Analyse des URL HTTP, des IP HTTPS, du contenu et des mots-clés, filtrage complet basé sur le type de fichiers comme ActiveX, Java, cookies de confidentialité, listes blanches/noires				

Série NS*a* 7ème génération, spécifications système

Pare-feu	NS*a* 2700	NS*a* 3700	NS*a* 4700	NS*a* 5700	NS*a* 6700
Service anti-spam complet			Prise en charge		
Visualisation des applications			Oui		
Contrôle des applications			Oui		
Capture Advanced Threat Protection			Oui		
Gestion de réseau					
Attribution d'adresses IP	Statique (client DHCP, PPPoE, L2TP et PPTP), serveur DHCP interne, relais DHCP				
Modes NAT	1 à 1, 1 à plusieurs, plusieurs à 1, plusieurs à plusieurs, NAT flexible (adresses IP superposées), PAT, mode transparent				
Protocoles de routage	BGP4, 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)				
Base de données utilisateurs locale	1000	1000	2500	2500	3200
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				
Compatible FIPS 140-2	Oui	Oui	En instance	En instance	En instance
Certifications	Pare-feu d'entreprise ICSA, antivirus ICSA, IPv6/USGv6				
Certifications (en cours)	NDPP Common Criteria pare-feu avec VPN et IPS				
Carte CAC (Common Access Card)	Prise en charge				
Haute disponibilité	Active/passive avec synchronisation d'état				
Matériel					
Format	1U rackable				
Ventilateurs	1	2	2 (amovibles)	2 (amovibles)	3 (amovibles)
Bloc d'alimentation	60 W	90 W	350 W	350 W	350 W
Consommation électrique maximale (W)	21,5	36,3	108,1	128,1	139,2
Alimentation redondante	100-240 VCA, 50-60 Hz				
Dissipation thermique totale	73,32 BTU	123,78 BTU	368,62 BTU	436,82 BTU	474,67 BTU
Dimensions	43 x 32,5 x 4,5 cm 16,9 x 12,8 x 1,8 in	43 x 32,5 x 4,5 cm 16,9 x 12,8 x 1,8 in	43 x 46,5 x 4,5 cm 16,9 x 18,1 x 1,8 in	43 x 46,5 x 4,5 cm 16,9 x 18,1 x 1,8 in	43 x 46,5 x 4,5 cm 16,9 x 18,1 x 1,8 in
Poids	4,0 kg/8,8 lb	4,6 kg/10,2 lb	7,8 kg	7,8 kg	8,1 kg
Poids DEEE	4,2 kg/9,3 lb	4,8 kg/10,6 lb	9,6 kg	9,6 kg	9,9 kg
Poids avec emballage	6,4 kg/14,1 lb	7 kg/15,4 lb	13,5 kg	13,5 kg	13,8 kg
Environnement (en fonctionnement/stockage)	0-40 °C (32-105 °F)/-40 à 70 °C (-40 à 158 °F)				
Taux d'humidité	5 à 95 % sans condensation	5 à 95 % sans condensation	0-90%, non condensée	0-90%, non condensée	0-90%, non condensée
Réglementation					
Numéros de modèles réglementaires	1RK51-109	1RK52-110	1RK53-115	1RK53-116	1RK54-118
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				

[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 de SonicOS 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
- Prise en charge complète d'API
- Intégration de SonicWall Switch
- Intégration points d'accès SonicWall Wi-Fi 6
- Évolutivité SD-WAN
- Assistant d'utilisation SD-WAN[1]
- Évolutivité des connexions (SPI, DPI, DPI-SSL)
- Tableau de bord amélioré[1]
- Vue améliorée de l'appareil
- Résumé des pics de trafic et utilisateurs
- Renseignements sur les menaces
- Centre de notification

Déchiffrement et inspection TLS/SSL/SSH

- TLS 1.3 avec sécurité renforcée[1]
- Inspection approfondie des paquets pour TLS/SSL/SSH
- Inclusion/exclusion d'objets, de groupes ou de noms d'hôtes
- Contrôle SSL
- Améliorations pour DPI-SSL avec CFS
- Contrôles DPI-SSL granulaires par zone ou règle
- Capture Advanced Threat Protection[2]
- Real-Time Deep Memory Inspection
- Analyse multimoteur cloud[2]
- 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[2]
- Blocage jusqu'au verdict
- Capture Client[2]

Prévention des intrusions[2]

- 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[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
- Logiciels malveillants cloud

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 (OSPF, RIP, BGP)

Gestion de réseau

- PortShield
- Trames Jumbo
- Découverte MTU de chemin
- Journalisation améliorée
- Jonction VLAN
- Mise en miroir des ports (SonicWall Switch)
- Qualité de service de couche 2
- Sécurité des ports
- Routage dynamique (RIP/OSPF/BGP)
- Contrôleur sans fil SonicWall
- Routage à base de règles (ToS/ métrique et ECMP)
- NAT
- Serveur DHCP
- Gestion de la bande passante
- Haute disponibilité active/passive avec synchronisation d'état
- Équilibrage de la charge entrante/sortante
- Haute disponibilité – active/standby avec synchronisation d'état
- Mode NAT, mode TAP, mode filaire virtuel/filaire, mode pont de couche 2
- Routage asymétrique
- Prise en charge Common Access Card (CAC)

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, surveillance et support

- Prise en charge de Capture Security Appliance (CS*a*)
- Capture Threat Assessment (CTA) v2.0
- Nouveau design ou modèle
- Comparaison à la moyenne du secteur et mondiale
- Nouvelle UI/UX, présentation intuitive des fonctionnalités[1]
- Tableau de bord
- Informations sur l'appareil, application, menaces

Récapitulatif des fonctionnalités de SonicOS 7.0 (suite)

Gestion, surveillance et support (suite)

- Vue topologique
- Création et gestion simplifiée de règles
- Statistiques d'utilisation de règles/objets[1]
- Utilisé/non utilisé
- Actif/inactif
- Recherche globale de données statiques
- Prise en charge du stockage[1]
- Gestion du stockage interne et externe[1]
- Cartes USB WWAN prises en charge (5G/LTE/4G/3G)
- Prise en charge de Network Security Manager (NSM)
- Interface utilisateur Web
- Interface de ligne de commande
- Enregistrement et configuration zéro intervention
- Reporting simple CSC[1]
- Prise en charge de l'appli. mobile SonicExpress
- SNMPv2/v3
- Création de rapports et gestion centralisées avec SonicWall Global Management System (GMS)[2]
- API de rapports et analyses
- 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
- Ecran de gestion CD
- Gestion des commutateurs Dell série N et série X, notamment en cascade

Débogage et diagnostics

- Surveillance améliorée des paquets
- Terminal SSH sur l'interface

Connectivité sans fil

- Gestion cloud et 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
- Améliorations RF
- Quota cyclique invités

[1] Nouvelle fonctionnalité, disponible sur SonicOS 7.0
[2] Requiert un abonnement supplémentaire

En savoir plus sur la série SonicWall NSa 7ème génération

www.sonicwall.com/products/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, 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