



- **Analyse et contrôle des applications**
- **Outils de visualisation intuitifs**
- **Filtrage RFDPI (Reassembly-Free Deep Packet Inspection) SonicWALL**
- **Puissante fonctionnalité de prévention des intrusions**
- **Déploiement flexible**
- **Sécurité dynamique**
- **Filtrage applicatif du trafic chiffré en SSL (DPI SSL)**

Les directeurs et administrateurs informatiques doivent en permanence faire face à un problème fondamental : plus ils s'efforcent d'améliorer la productivité du personnel et la qualité des services internes, plus il devient difficile d'obtenir des renseignements sur le trafic dans son ensemble. Or, ces informations sont nécessaires pour analyser avec précision les performances, déceler les menaces et agir immédiatement, afin d'assurer le bon fonctionnement des systèmes vitaux.

Les outils conventionnels ont de plus en plus de mal à collecter des renseignements sur le trafic, dans la mesure où ils identifient les protocoles par leurs ports respectifs. Les applications modernes, en revanche, basées sur le Web, utilisent de plus en plus souvent des protocoles standard comme HTTP ou HTTPS. Résultat, les pare-feu traditionnels ne « voient » plus le trafic des applications sur le réseau, ni les menaces qu'elles recèlent, ni l'utilisation excessive des ressources qu'elles entraînent. Exemple : aux yeux des pare-feu traditionnels, le trafic HTTP/HTTPS paraît anodin. Or, en fait, il peut transporter certaines applications particulièrement consommatrices de bande passante et susceptibles de compromettre la sécurité, comme les flux audio et vidéo, le trafic de messageries instantanées et des documents en divers formats. Il en va de même des sites de réseaux sociaux qui, bien qu'ils ne soient pas formellement considérés comme des applications, emploient les mêmes technologies, exposant les entreprises aux programmes malveillants et dérobant de la bande passante aux applications vitales. Pour reprendre le contrôle du trafic, les pare-feu traditionnels doivent aller bien plus loin que le simple filtrage dynamique des paquets : ils doivent analyser le trafic au niveau de la couche applicative. La seule technologie capable d'accomplir cette tâche et de superviser ces différents types d'activité réseau est le filtrage applicatif (Deep Packet Inspection).

Grâce aux services performants d'analyse et de contrôle des applications associés à la prévention et à la détection des intrusions réseau, l'appliance de sécurité réseau (NSA) E-Class E8500 de SonicWALL offre une sécurité dynamique pour le réseau global. Dotée du moteur de filtrage breveté RFDPI (Reassembly-Free Deep Packet Inspection™) de SonicWALL® et des outils sophistiqués d'Application Intelligence, la NSA E8500 est capable d'analyser et de contrôler plus de 1 100 applications individuelles, chiffrées avec SSL ou non chiffrées. Le moteur RFDPI de SonicWALL inspecte simultanément des centaines de milliers de connexions via les 65 535 ports en parallèle, sans pratiquement aucun délai ni limite dans la taille des flux. Face à cette extraordinaire association de perfectionnement logiciel et de puissance matérielle, les applications n'ont guère de chances de passer inaperçues sur le réseau.

La NSA E8500 peut être déployée comme solution intégrée ou comme passerelle au sein d'un réseau. En tant que solution intégrée, la NSA E8500 permet aux administrateurs de conserver leur infrastructure tout en ajoutant l'analyse et le contrôle des applications, et de bénéficier ainsi d'une couche supplémentaire de sécurité et de visibilité sur leur réseau. La NSA E8500 peut également faire office de passerelle de sécurité entièrement équipée, réunissant toutes les fonctionnalités d'accès distant, de haute disponibilité et haut de gamme requises dans les déploiements exigeants.

### Caractéristiques et avantages

**Analyse et contrôle des applications.** Il s'agit d'un ensemble configurable de règles granulaires pouvant être appliquées par utilisateur, application, horaire ou sous-réseau IP. Ces règles peuvent servir à restreindre le transfert de certains fichiers et documents, analyser les pièces jointes d'e-mails sur la base de critères configurables par les utilisateurs, automatiser l'allocation de bande passante par application, contrôler et inspecter les accès Web internes et externes et permettre aux utilisateurs d'ajouter des signatures personnalisées.

**Outils de visualisation intuitifs.** Ils fournissent aux administrateurs informatiques toute une série d'éléments relatifs aux applications traversant le réseau, notamment l'identité de leurs utilisateurs, ainsi que leur impact potentiel sur la sécurité.

**Filtrage RFDPI (Reassembly-Free Deep Packet Inspection) SonicWALL.** Il permet de contrôler plus de 1 100 applications individuelles sur le réseau et d'inspecter simultanément des centaines de milliers de connexions via les 65 535 ports, sans pratiquement aucun délai ni limite dans la taille des flux.

**Puissante fonctionnalité de prévention des intrusions.** Elle protège contre un vaste éventail de menaces au niveau de la couche applicative. Pour cela, elle recherche directement dans le contenu des paquets de données les éventuels vers, chevaux de Troie,

vulnérabilités logicielles, applications poste à poste, messageries instantanées, intrusions par porte dérobée et autres programmes malveillants.

**Déploiement flexible.** Soit comme passerelle classique, soit comme solution intégrée pour permettre aux administrateurs de conserver leur infrastructure tout en ajoutant l'analyse et le contrôle des applications, et de bénéficier ainsi d'une couche supplémentaire de sécurité et de visibilité sur leur réseau.

**Sécurité dynamique.** Les services de protection contre les menaces, de détection et prévention des intrusions et d'analyse des applications sont mis à jour en continu, 24 heures/24, 7 jours/7, pour une sécurité maximum. La suite complète de services de prévention des intrusions protège contre plus d'un million d'attaques malware individuelles.

**Filtrage applicatif du trafic chiffré en SSL (DPI SSL).** Le trafic HTTPS entrant et sortant est déchiffré et analysé en toute transparence par le moteur RFDPI SonicWALL, avant d'être rechiffré et envoyé à sa destination d'origine en l'absence de menace ou de vulnérabilité.

## Spécifications



SonicWALL NSA E8500

Remarque : les indications de performances et les capacités sont susceptibles d'être modifiées jusqu'à la mise sur le marché du produit.

## Certifications



NSA E8500	
<b>Pare-feu</b>	
Débit dynamique <sup>1</sup>	8,0 Gbit/s
Performances IPS <sup>2</sup>	3,5 Gbit/s
Performances GAV <sup>3</sup>	2,3 Gbit/s
Performances UTM <sup>3</sup>	2,0 Gbit/s
Performances IMIX <sup>3</sup>	2,0 Gbit/s
Connexions (max.) <sup>3</sup>	3 000 000
Connexions DPI (max.)	1 500 000
Nouvelles connexions/s	60 000
Nb de nœuds pris en charge	Illimité
Prévention des attaques par déni de service	22 classes d'attaques DoS, DDos et scans
SonicPoint pris en charge (max.)	128
<b>VPN</b>	
Débit 3DES/AES <sup>4</sup>	4,0 Gbit/s
Tunnels VPN site à site	10 000
Licences Global VPN Client incluses (max.)	2 000 (10 000)
Licences VPN SSL incluses (max.)	2 (50)
Techniciens Virtual Assist inclus (max.)	1 (25)
Chiffrement/authentification/groupes DH	DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1/groupes DH 1, 2, 5, 14
Echange de clés	IKE, IKEv2, clé manuelle, PKI (X.509), L2TP sur IPSec
VPN à base de routes	Oui (OSPF, RIP)
Certificats pris en charge	Verisign, Thawte, Cybertrust, RSA Keon, Entrust et Microsoft CA pour VPN SonicWALL à SonicWALL, SCEP
Passerelle VPN redondante	Oui
Plates-formes Global VPN Client prises en charge	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32/64 bits, Windows 7
Plates-formes VPN SSL prises en charge	Microsoft® Windows 2000 / XP / Vista 32/64 bits / Windows 7, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE
<b>Services de sécurité</b>	
Services de filtrage applicatif	Intrusion Prevention Service (inclus), Gateway Anti-Virus, Anti-Spyware and Application Intelligence (inclus)
Content Filtering Service (CFS) Premium Edition	Analyse d'URL HTTP, d'IP HTTPS, de mots-clés et de contenus, blocage ActiveX, d'applets Java et de cookies
Gateway-enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP et FTP, clients McAfee™ activés, blocage de pièces jointes
Comprehensive Anti-Spam Service	Oui
Application Intelligence (inclus)	Exécution au niveau des applications et contrôle de la bande passante, régulation du trafic Web, des e-mails, des pièces jointes et des transferts de fichiers, analyse et restriction de l'accès de documents et fichiers sur la base de mots et expressions clés
DPI SSL	Possibilité de déchiffrer de manière transparente le trafic HTTPS dans les deux directions, de scanner ce trafic à la recherche de menaces grâce à la technologie de filtrage applicatif (DPI) SonicWALL (GAV/AS/IPS/Application Intelligence/CFS), puis de rechiffrer le trafic et de l'envoyer à sa destination dans la mesure où aucune menace ou vulnérabilité n'a été détectée
<b>Mise en réseau</b>	
Attribution d'adresses IP	Statique, (client DHCP, PPPoE, L2TP et PPTP), serveur DHCP interne, relais DHCP
Modes NAT	1:1, 1:plusieurs, plusieurs:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT, mode transparent
Interfaces VLAN (802.1q)	512
Routeage	OSPF, RIPv1/v2, routes statiques, routage à base de règles, multidiffusion
QoS	Priorité, bande passante maximum, garantie, marquage DSCP, 802.1p
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix
IPv6	Compatible
Base de données interne/utilisateurs SSO	2 500/7 000 utilisateurs
VoIP	H.323v1-5 intégral, SIP, gatekeeper support, gestion de la bande passante sortante: VoIP sur le WLAN, sécurité par filtrage applicatif, interopérabilité totale avec la plupart des dispositifs de passerelles et de communication VoIP
<b>Système</b>	
Gestion et surveillance	Interface utilisateur Web (HTTP, HTTPS), ligne de commande (SSH, console) SNMP v2 : gestion globale avec SonicWALL GMS
Journalisation et rapports	ViewPoint®, Local Log, Syslog, Solera Networks
Haute disponibilité	Active/passive avec synchro. d'état, UTM active/active avec synchro. d'état
Équilibrage de charge	Oui, (sortant, cyclique, suivant le pourcentage du trafic et par débordement) (entrant, cyclique, répartition aléatoire, sticky IP, remappage de blocs et symétrique)
Normes	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3
Normes sans fil (avec les points d'accès SonicPoint)	802.11 a/b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TTLS
<b>Matériel</b>	
Interfaces	1 interface console, 4 Gigabit Ethernet, 4 SFP (SX, LX ou TX), 1 interface Gbe HA, 2 USB
Mémoire (RAM)	2 Go
Mémoire flash	Compact Flash 512 Mo
Sans-fil 3G/modem*	Avec adaptateur USB 3G/modem
Alimentation	2 ATX 250 W, remplaçables à chaud
Ventilateurs	Ventilateurs doubles, remplaçables à chaud
Affichage	Ecran LCD
Alimentation d'entrée	100-240 VCA, 60-50 Hz
Consommation max.	150 W
Dissipation thermique totale	511,5 BTU
MTBF	12,4 ans
Certifications	EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1
Facteur de forme	1U rackable
Dimensions	43,2 x 42,5 x 4,4 cm/17 x 16,8 x 1,8 in
Poids	7,9 kg/17,30 lbs
Poids DEEE	7,9 kg/17,30 lbs
Conformité aux normes suivantes	FCC classe A, CE5 classe A, CE, G-Tick, VCCI, MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, DEEE
Environnement	5-40 °C, 40-105 °F
Humidité	10-90 % non condensée

<sup>1</sup> Méthodes de test : performances maximales basées sur RFC 2544 (pour pare-feu). Les performances réelles peuvent varier suivant les conditions de réseau et les services activés.

<sup>2</sup> Débit UTM/Gateway AV/Anti-Spyware/IPS basé sur le test de performances HTTP standard Spirent WebAvalanche et les outils de test Ixia. Tests effectués avec différents flux, via plusieurs paires de ports.

<sup>3</sup> Le nombre maximal effectif de connexions est inférieur quand les services UTM sont activés.

<sup>4</sup> Débit VPN basé sur le trafic UDP par paquets de 1280 octets selon RFC 2544.

\* Carte USB 3G et modem non fournis. Pour savoir quels appareils USB sont pris en charge, consultez <http://www.sonicwall.com/us/products/cardsupport.html>

## La gamme SonicWALL de protection complète



SÉCURITÉ RÉSEAU



ACCÈS DISTANT SÉCURISÉ



SÉCURISATION WEB ET DE MESSAGERIE



SAUVEGARDE ET RÉCUPÉRATION



GESTION ET RÉGLÉS

## SonicWALL France

T +33 1 49 33 73 19 France@sonicwall.com

## SonicWALL BeNeLux

T +32 (0) 15 280 985 Benelux@sonicwall.com

## Contacts du support SonicWALL

[www.sonicwall.com/emea/4724.html](http://www.sonicwall.com/emea/4724.html)

PROTECTION AT THE SPEED OF BUSINESS™