



PARE-FEU

Pare-feu nouvelle génération

- **Pare-feu nouvelle génération**
- **Puissante fonctionnalité de prévention des intrusions**
- **Application Intelligence, Control and Visualization**
- **Technologie de filtrage RFDPI (Reassembly-Free Deep Packet Inspection)**
- **Déploiement flexible**
- **Filtrage applicatif du trafic chiffré en SSL (DPI SSL)**
- **Réseau GRID (Global Response Intelligent Defense) SonicWALL**

La tâche des administrateurs informatiques relève parfois d'un véritable défi : ils doivent fournir à l'entreprise des solutions efficaces, indispensables à son activité, tout en gérant l'utilisation improductive, et souvent dangereuse, d'applications par les employés. En termes de bande passante, la priorité doit être accordée aux applications vitales, tandis que les médias sociaux et autres jeux en ligne doivent pouvoir être limités, voire totalement bloqués. Les pare-feu à filtrage dynamique de paquets utilisés par nombre d'entreprises fonctionnent sur la base des informations de port et de protocole. Par conséquent, ils ne sont pas en mesure d'identifier les applications et ne peuvent donc pas résoudre le problème. En résumé, les pare-feu à filtrage dynamique de paquets ne savent pas distinguer le bon du mauvais.

L'appliance de sécurité réseau (NSA) E-Class E8500 de SonicWALL® est un pare-feu nouvelle génération intégrant étroitement la prévention des intrusions, la protection anti-malware et le puissant service d'Application Intelligence, Control and Visualization. Dotée de la technologie de filtrage brevetée RFDPI (Reassembly-Free Deep Packet Inspection™)* de SonicWALL, la NSA E8500 est capable d'analyser et de contrôler plus de 2 800 applications, même chiffrées en SSL. Le moteur RFDPI de SonicWALL inspecte simultanément des centaines de milliers de connexions via tous les ports, sans pratiquement aucun délai ni limite dans la taille des fichiers. 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 le service d'Application Intelligence and Control, 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

Pare-feu nouvelle génération SonicWALL avec filtrage RFDPI (Reassembly-Free Deep Packet Inspection™). Il intègre étroitement les services de prévention des intrusions, de protection anti-malware et d'Application Intelligence and Control optimisés, avec visualisation en temps réel.

Puissante fonctionnalité de prévention des intrusions. Elle protège contre un vaste éventail de menaces au niveau de la couche applicative en recherchant directement dans le contenu des paquets de données les éventuels vers, chevaux de Troie, vulnérabilités logicielles, exploits et autres programmes malveillants.

Application Intelligence, Control and Visualization. Ce service assure un contrôle granulaire et une visualisation en temps réel des applications, permettant de garantir la hiérarchisation de la bande passante, ainsi qu'une sécurité réseau et une productivité maximales.

Technologie de filtrage RFDPI (Reassembly-Free Deep Packet Inspection). Elle permet de contrôler plus de 2 800 applications et détecte des millions d'éléments malveillants, afin de protéger le réseau de manière automatique et transparente, tout en inspectant simultanément des centaines de milliers de connexions à travers tous les ports, sans limites dans la taille des flux ni pratiquement aucun délai.

Déploiement flexible. Soit comme passerelle classique, soit comme solution intégrée pour permettre aux administrateurs de conserver leur infrastructure tout en ajoutant le service d'Application Intelligence and Control, et de bénéficier ainsi d'une couche supplémentaire de sécurité et de visibilité sur leur réseau.

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.

Réseau GRID (Global Response Intelligent Defense) SonicWALL. Il assure la mise à jour en continu des services de protection, de détection, de prévention des intrusions et de contrôle applicatif, 24 h/24, 7 j/7, pour une sécurité maximum. La suite complète de services de prévention des intrusions protège contre plus d'un million d'attaques de programmes malveillants.

* Brevet U.S. n° 7310815 – A method and apparatus for data stream analysis and blocking (méthode et appareil d'analyse et de blocage du flux de données).

Spécifications



SonicWALL NSA E8500
01-SSC-8866

Inclut une licence DPI SSL et 1 an de services de sécurité avec IPS/GAV/Application Control



SonicWALL NSA E8500 High Availability
01-SSC-8867

NSA E8500	
Pare-feu	
Débit dynamique ¹	8,0 Gbit/s
Performances IPS ²	3,7 Gbit/s
Performances GAV ²	2,25 Gbit/s
Performances Full DPI (filtrage applicatif) ²	2,2 Gbit/s
Performances IMIX ²	2,0 Gbit/s
Connexions (max.) ³	1 500 000
Connexions DPI (max.)	1 250 000
Nouvelles connexions/s	80 000
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
VPN	
Débit 3DES/AES ⁴	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 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
Services de sécurité	
Deep Packet Inspection Service	Intrusion Prevention (inclus), Gateway Anti-Virus, Anti-Spyware, Application Intelligence and Control (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, gestion de la bande passante sur les catégories de filtrage, listes d'autorisation/interdiction
Enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP et FTP, blocage automatique de pièces jointes par le client McAfee™
Comprehensive Anti-Spam Service ⁵	Pris en charge
Application Intelligence and Control (inclus)	Gestion et contrôle de la bande passante applicative, applications priorisées ou bloquées en fonction de signatures, contrôle des transferts de fichiers, analyse 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 rechiffre le trafic et de l'envoyer à sa destination dans la mesure où aucune menace ou vulnérabilité n'a été détectée
Mise en réseau	
Attribution d'adresses IP	Statique, (client DHCP, PPPoE, L2TP et PPTP), serveur DHCP interne, relais DHCP
Modes NAT	1:1, 1:plusieurs, plusieurs:1, plusieurs:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT, mode transparent
Interfaces VLAN (802.1q)	512
Routing	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
Agrégation de liens	Oui
Redondance de ports	Oui
Système	
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, NetFlow v5/v9, IPFIX avec extensions, visualisation en temps réel
Haute disponibilité	Active/passive avec synchro. d'état, DPI actif/actif 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-TLS
Matériel	
Interfaces	4 Gigabit Ethernet, 4 SFP (SX, LX ou TX), 1 GbE HA, 2 USB, 1 interface console
Mémoire (RAM)	4 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	En instance : EAL4+, FIPS 140-2, ICSA Firewall 4.1 ; actuelles : VPNC
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, CES classe A, CE, C-Tick, VCCI, MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, DEEE
Environnement	5-40 °C, 40-105 °F
Humidité	10-90 % non condensée

¹Méthodes 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. ²Débit Full DPI/ 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.

³Le nombre maximal réel de connexions est inférieur quand les services DPI sont pleinement activés. ⁴Débit 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> ⁵Comprehensive Anti-Spam Service prend en charge un nombre illimité d'utilisateurs, mais est recommandé pour 250 utilisateurs ou moins.

La gamme SonicWALL de solutions de sécurité dynamique



SÉCURITÉ
RÉSEAU



ACCÈS DISTANT
SÉCURISÉ



SÉCURISATION WEB
ET DE MESSAGERIE



SAUVEGARDE ET
RÉCUPÉRATION



GESTION
ET RÈGLES

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

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

