



SonicWALL Application Intelligence and Control

PARE-FEU

Contrôle granulaire des applications, intelligence et visualisation en temps réel

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.

Analysant chaque octet de chaque paquet sur l'ensemble du trafic réseau, SonicWALL® assure un service complet d'intelligence et de contrôle au niveau applicatif, quels que soient le port ou le protocole, permettant de déterminer exactement quelles applications sont utilisées et par qui. Les pare-feu nouvelle génération de SonicWALL exploitent une bibliothèque de signatures de menaces enrichie en continu, capable actuellement de reconnaître plus de 3 000 applications et de détecter des millions d'éléments malveillants afin de protéger le réseau de manière automatique et transparente. La solution détecte et élimine les programmes malveillants, les intrusions, les fuites de données et les violations de règles avant que ceux-ci ne fassent des dégâts sur le réseau d'une entreprise ou auprès de ses utilisateurs.

SonicWALL Application Intelligence and Control offre des capacités de gestion et un niveau de convivialité inédits permettant aux administrateurs réseau de conserver un contrôle granulaire sur les applications et les utilisateurs. Ils peuvent aisément créer des règles de gestion de la bande passante sur la base de catégories logiques prédéfinies (par ex. médias sociaux ou jeux), d'applications individuelles ou même d'utilisateurs ou de groupes. A la création de nouvelles applications, de nouvelles signatures sont envoyées aux pare-feu et les règles concernées sont automatiquement mises à jour, sans que les TI n'aient à perdre un temps précieux à actualiser les règles et objets d'applications. Les administrateurs doivent également pouvoir visualiser le trafic applicatif afin de contrôler convenablement l'utilisation du réseau et d'adapter les règles en fonction d'observations importantes. L'Application Flow Monitor de SonicWALL fournit des graphiques en temps réel de l'activité relative aux applications, permettant aux administrateurs de modifier les règles en vue d'augmenter la productivité du réseau.

Le service d'Application Intelligence and Control est disponible avec SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention sous forme d'abonnements de un, deux ou trois ans, ou au sein de la SonicWALL Comprehensive Gateway Security Suite pour les pare-feu TZ 210, NSA et NSA E-Class.

Caractéristiques et avantages

Intelligence applicative. Ce service s'appuie sur le filtrage RFDPI (Reassembly-Free Deep Packet Inspection™) de SonicWALL pour analyser chaque paquet et identifier les applications utilisées ainsi que leurs utilisateurs. SonicWALL entretient une bibliothèque de signatures destinée à protéger les réseaux de manière automatique et transparente.

Contrôle applicatif. Ce service permet de configurer des règles flexibles visant à limiter ou bloquer des applications, fichiers, URL et pièces jointes d'e-mails en fonction, entre autres, du type d'application, de l'utilisateur du réseau, d'horaires ou encore de signatures personnalisées.

Visualisation applicative. Ce service fournit des graphiques en temps réel des applications, de la bande passante consommée en entrée et en sortie, des utilisateurs, des sites Internet actuellement consultés, etc. De plus, il permet d'exporter ces mêmes données vers un analyseur NetFlow/IPFIX à des fins de surveillance hors ligne, de dépannage et de diagnostic des activités réseau.

Prévention des fuites de données. Elle bloque et contrôle la transmission de données sensibles par FTP, en

pièce jointe de services Webmail (Hotmail® ou Gmail®, par ex.), ou via les serveurs de messagerie SMTP et POP3 de l'entreprise.

Gestion de la bande passante au niveau applicatif. Cette fonctionnalité garantit la qualité de service (QoS) en réservant le débit à des applications vitales ou à des groupes à certaines heures de la journée.

Mises à jour et notifications automatisées. Elles garantissent la protection du réseau contre les menaces les plus récentes, ce qui simplifie l'administration.

Filtrage applicatif pour le trafic SSL. Il étend la protection au trafic chiffré en SSL, ce qui améliore le respect des règles de conformité, le filtrage de contenu et la prévention des fuites de données, et permet de supprimer une voie d'accès supplémentaire pour les programmes malveillants. Le trafic est tout d'abord déchiffré, puis inspecté, avant d'être rechiffré en toute transparence pour l'utilisateur. Le filtrage peut être configuré pour les connexions entrantes et sortantes.*

* 01-SSC-8680 Licence de mise à niveau DPI SSL pour les NSA 3500 et supérieures.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

- Intelligence applicative
- Contrôle applicatif
- Visualisation applicative
- Prévention des fuites de données
- Gestion de la bande passante au niveau applicatif
- Mises à jour et notifications automatisées
- Filtrage applicatif pour le trafic SSL

Intelligence, contrôle et visualisation au niveau applicatif

Identifier

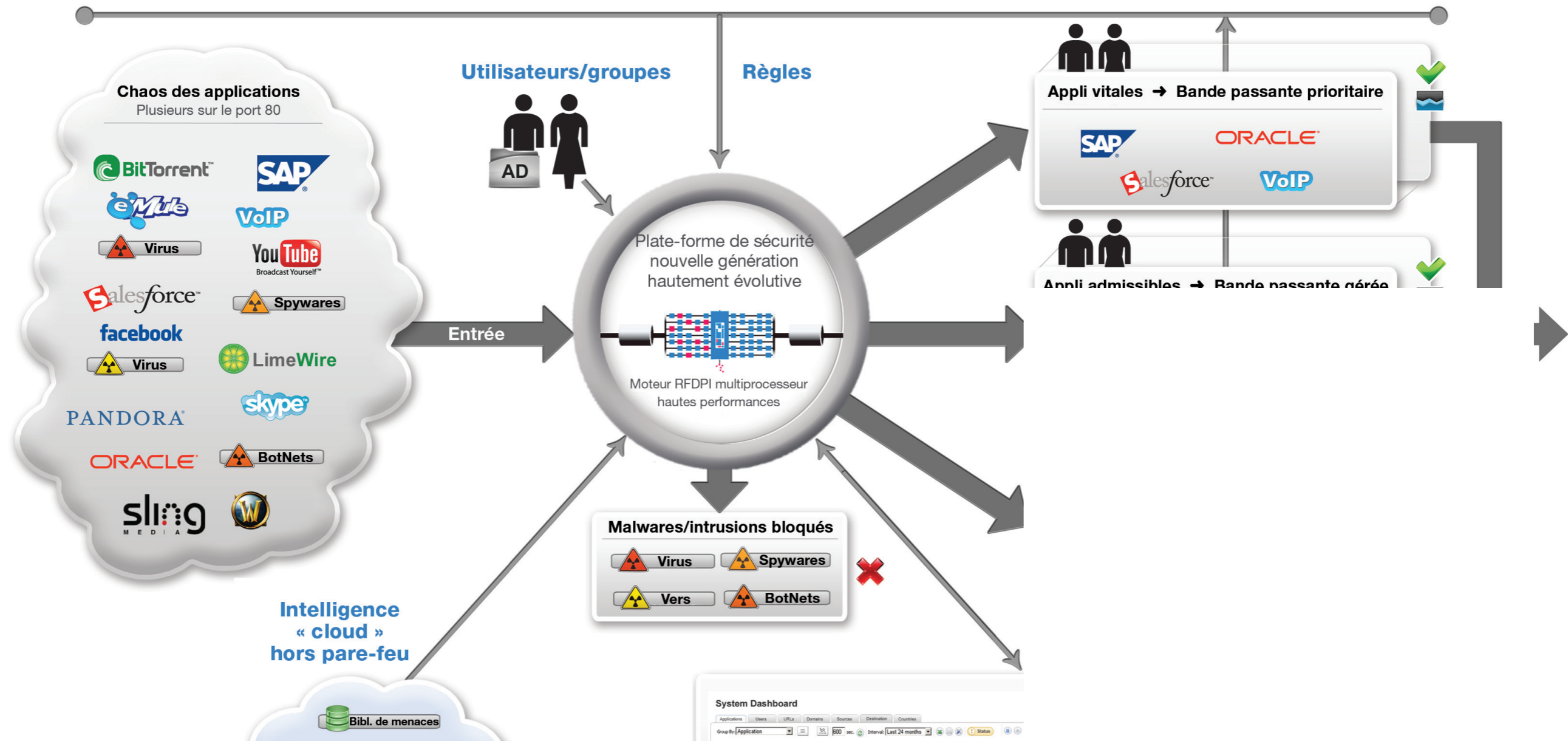
- Par application
 - Pas par port ni protocole
- Par utilisateur/groupe
 - Pas par adresse IP
- Par inspection du contenu
 - Pas par nom de fichier

Catégoriser

- Par application
- Par catégorie d'applications
- Par destination
- Par contenu
- Par utilisateur/groupe

Contrôler

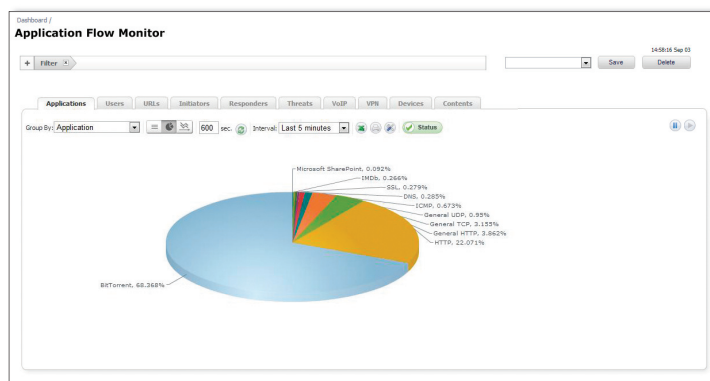
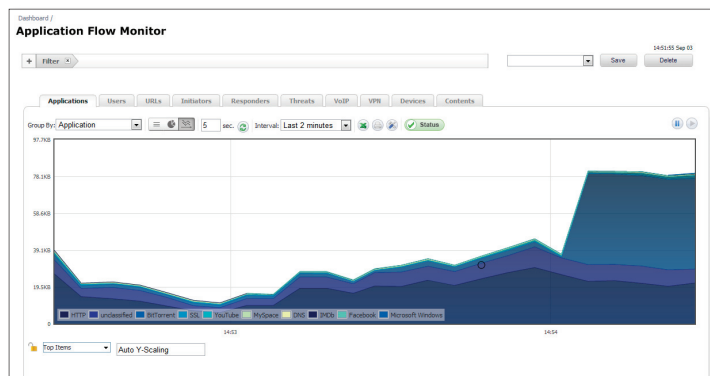
- Hiérarchiser les applications par règle
- Gérer les applications par règle
- Bloquer les applications par règle
- Détecter et bloquer les programmes malveillants
- Détecter et prévenir les tentatives d'intrusion



Spécifications

Visualisation applicative

Des graphiques en temps réel des applications, de la bande passante en entrée et en sortie, des sites Internet visités et de l'activité de tous les utilisateurs permettent aux administrateurs de modifier les règles en fonction des besoins du réseau.



Liste des caractéristiques

Fonctionnalités d'Application Intelligence

- Analyse et identification de l'ensemble du trafic indépendamment des ports ou protocoles pour un contrôle total
- Prévention des fuites de données avec surveillance des contenus définis par l'utilisateur
- Gestion de la bande passante au niveau applicatif fournie par une riche bibliothèque de signatures actualisée en permanence et la création de règles efficaces
- Actions prédéfinies et personnalisées : journalisation, journalisation et blocage, messages utilisateurs personnalisés, contournement DPI et gestion de la bande passante
- Filtrage applicatif du trafic passant par les protocoles chiffrés en SSL

Bibliothèque de signatures

- Bibliothèque à mise à jour dynamique contenant des milliers de signatures d'applications et de contenus

Journalisation et rapports

- Journaux et alertes en temps réel
- Rapports granulaires via SonicWALL ViewPoint et GMS
- Netflow/IPFIX avec journalisation d'extensions pour une analyse et une visualisation supplémentaires, prêtes à l'emploi, du trafic

Evolutivité

- Capacité d'analyse d'un grand nombre de téléchargements simultanés de fichiers de taille illimitée

Pour plus d'informations sur la gamme SonicWALL de services de sécurité à valeur ajoutée, dont Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Application Intelligence and Control, Comprehensive Anti-Spam Service, Enforced Client Anti-Virus and Anti-Spyware et Content Filtering Service, rendez-vous sur <http://www.sonicwall.com>.



Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service

NSA E7500 (1 an)

01-SSC-6130

NSA E6500 (1 an)

01-SSC-6131

NSA E5500 (1 an)

01-SSC-6132

NSA 5000 (1 an)

01-SSC-6159

NSA 4500 (1 an)

01-SSC-6133

NSA 3500 (1 an)

01-SSC-6134

NSA 2400 (1 an)

01-SSC-6135

Série NSA 240 (1 an)

01-SSC-6162

Série TZ 210 (1 an)

01-SSC-6165

Des services d'abonnement pluri-annuels sont également disponibles.

Pour connaître les références de la gamme complète d'appliances de sécurité réseau SonicWALL, rendez-vous sur www.sonicwall.com.

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

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

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™