SonicWALL Analyzer

GESTION ET REPORTING

Outil d'analyse, de visualisation et de génération de rapports sur le trafic applicatif

- **Rapports graphiques exhaustifs**
- **Reporting syslog de nouvelle génération**
- **Rapports sur les événements des SRA et CDP SonicWALL**
- **Rapports universels planifiés**
- **Affichage « en un coup d'œil »**
- **Rapports de conformité**
- **Rapports multi-menaces**
- **Rapports par utilisateur**
- **Accès universel**
- **Fonctions intelligentes d'analyse des attaques**

Lorsque les employés utilisent des applications Web (messagerie Web, instantanée, Facebook®, BitTorrent...) pour des activités non professionnelles, cela entraîne des pics de consommation de la bande passante, fait chuter la productivité et compromet la sécurité du réseau. Les services informatiques ont besoin d'une solution leur permettant de sensibiliser davantage aux questions de sécurité, d'optimiser l'utilisation du réseau, de gérer intelligemment les applications et de fournir des services économiques de dépannage et d'analyse forensique. Or, la plupart des produits de reporting et d'analyse du trafic applicatif offrent une visibilité limitée et leur utilisation peut être relativement complexe.

SonicWALL® Analyzer est un outil Web convivial d'analyse du trafic et de reporting qui offre un aperçu en temps réel et historique de la santé, des performances et de la sécurité d'un réseau. Cet analyseur est compatible avec les pare-feu, les produits de sauvegarde et récupération et les solutions d'accès distant sécurisé de SonicWALL. Les entreprises de toute taille bénéficient d'une meilleure productivité de leur personnel, d'une consommation optimisée de la bande passante réseau et d'une sensibilité accrue aux questions de sécurité. SonicWALL est le seul éditeur de pare-feu à proposer une solution complète combinant l'analyse externe du trafic applicatif aux données granulaires générées par les pare-feu SonicWALL.

Fonctionnalités et avantages

Des **rapports graphiques exhaustifs** sur les menaces au niveau du pare-feu, les statistiques de consommation de la bande passante et l'analyse du trafic applicatif permettent aux entreprises de visualiser la productivité de leurs employés et les activités réseau suspectes.

La fonctionnalité de **reporting syslog de nouvelle génération** exploite les améliorations révolutionnaires de l'architecture pour simplifier la synthèse des données, permettant la génération en temps quasi réel de rapports sur les messages syslog entrants. L'accès direct aux données brutes sous-jacentes augmente encore la précision et les options de personnalisation des rapports.

La fonctionnalité de génération de **rapports sur les événements des SRA et CDP SonicWALL** puise dans les données syslog de nouvelle génération pour offrir un aperçu détaillé de la santé et du comportement de l'appliance.

Rapports universels planifiés. L'outil permet la centralisation de tous les rapports planifiés. Un rapport peut combiner les graphiques et les tableaux de plusieurs appareils. Les rapports peuvent être planifiés et envoyés en divers formats à une ou plusieurs adresses e-mail.

L'**affichage « en un coup d'œil »** personnalisable rassemble plusieurs tableaux récapitulatifs sur une même page, ce qui permet aux utilisateurs d'accéder facilement aux paramètres clés du réseau et de procéder à des analyses rapides à partir des données disponibles.

Les administrateurs peuvent générer des **rapports de conformité** de manière instantanée ou planifiée en vue de satisfaire à des exigences réglementaires spécifiques.

Les **rapports multi-menaces** permettent de collecter des informations sur les attaques contrées et d'observer instantanément l'activité des menaces détectées par les pare-feu SonicWALL à l'aide de SonicWALL Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service.

Les **rapports par utilisateur** permettent de suivre les activités d'utilisateurs individuels, au niveau local ou sur les sites distants, afin de mieux connaître la nature du trafic à travers l'ensemble du réseau, notamment l'utilisation des applications, les sites Internet consultés, l'activité de sauvegarde et les connexions VPN par utilisateur.

L'**accès universel** simplifie la consultation des données, les administrateurs pouvant analyser chaque site par simple navigateur Web.

Les **fonctions intelligentes d'analyse des attaques** fournissent des comptes-rendus précis sur certains types d'attaques ou tentatives d'intrusion, ainsi que sur leur adresse d'origine, permettant aux administrateurs de réagir rapidement à l'arrivée de nouvelles menaces.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Spécifications

Analyzer pour la série TZ
01-SSC-3378

Analyzer pour NSA 240, NSA 2400
01-SSC-3379

Analyzer pour NSA 3500
01-SSC-3380

Analyzer pour NSA 4500
01-SSC-3381

Analyzer pour NSA E-Class et la série SuperMassive™ E10000
01-SSC-3382

Analyzer pour CDP 210
01-SSC-3383

Analyzer pour CDP 220
01-SSC-3384

Analyzer pour CDP 5040B
01-SSC-3385

Analyzer pour CDP 6080B
01-SSC-3386

Analyzer pour SRA 1200
01-SSC-3387

Analyzer pour SRA 4200
01-SSC-3388

Analyzer pour la série SRA E-Class
01-SSC-3389

SonicWALL Analyzer

Affichage pratique des statistiques de trafic, par exemple des sites Internet consultés. La fonction de zoom permet de trier les données selon des informations précises : nom du site, adresse IP, catégorie de site ou encore nombre de tentatives de connexion.

Surveillance aisée des appliances SonicWALL gérées grâce à des rapports graphiques intuitifs. Les anomalies de trafic sont facilement identifiées à partir des données d'utilisation selon un horaire particulier, l'auteur, le répondeur ou le service. Les rapports peuvent être exportés en fichier MS Excel ou PDF, ou être directement imprimés.

Des rapports granulaires sur les données du trafic permettent d'afficher les applications les plus utilisées sur le réseau. Une fois identifiées, ces applications peuvent le cas échéant être bloquées selon la catégorie, l'horaire ou l'utilisateur.

L'analyseur intègre automatiquement la gestion des menaces ; les principales menaces peuvent être facilement affichées suivant la cible, l'auteur ou le type. Inclut des rapports exhaustifs, notamment sur l'antivirus au niveau de la passerelle, l'anti-spyware et la prévention des intrusions.

Configuration requise

Système d'exploitation	Windows Server 2003 64 bits (SP2)
	Windows Server 2008 SBS 64 bits (R2)
	Windows Server 2008 Standard 64 bits (R2)
	Windows Vista Pro 64 bits (SP1)
	Windows 7 Pro 64 bits (SP1)
	Dans tous les cas, SonicWALL Analyzer fonctionne comme application 32 bits.
Matériel pour serveur Analyzer	Configuration minimale requise : Single Core 3 GHz Processeur x86, 4 Go RAM, 100 Go HDD
Java	Java SE Runtime Environment 1.6 ou version ultérieure

Navigateurs Internet
Microsoft® Internet Explorer 8.0 ou version supérieure
Mozilla Firefox 6.0 ou version supérieure
Google Chrome 13.0 et plus
pris en charge uniquement sur les plates-formes Microsoft Windows

Appliance virtuelle

Hyperviseur :	VMware ESX et ESXi
Système d'exploitation installé :	SonicLinux renforcé
Taille de l'appliance :	250 Go, 950 Go
Mémoire vive allouée :	4 Go

VMware Hardware Compatibility Guide: rendez-vous sur www.vmware.com/resources/compatibility/search.php

Appliances SonicWALL prises en charge
Appliances de sécurité réseau SonicWALL : série NSA E-Class, série NSA, série TZ et série PRO[1]
SonicWALL CDP (Continuous Data Protection)
SonicWALL CSM (Content Security Manager)
SonicWALL SRA (Secure Remote Access) E-Class et SRA pour PME[2]

Firmware SonicWALL pris en charge
Séries NSA et NSA E-Class SonicWALL : SonicOS Enhanced 5.0 ou version supérieure
Série PRO SonicWALL : SonicOS Enhanced 3.2 ou version supérieure
Série TZ SonicWALL : SonicOS Standard 3.1 ou version supérieure et SonicOS Enhanced 3.2 ou version supérieure
Série CSM SonicWALL : SonicWALL 2.0 ou version supérieure
Série SRA SonicWALL pour PME : Firmware 2.0 ou version supérieure
SonicWALL série SRA E-Class : Firmware 9.0 ou version supérieure

[1] Les anciens modèles SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2 et SonicWALL Pro/Pro-VX ne sont pas pris en charge.

[2] Uniquement les appliances SRA E-Class Aventail récentes utilisant des numéros de série de 12 caractères hexadécimaux.

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 complète de solutions de sécurité dynamique SonicWALL

SÉCURITÉ RÉSEAU | ACCÈS DISTANT SÉCURISÉ | SÉCURISATION WEB ET DE MESSAGERIE | SAUVEGARDE ET RÉCUPÉRATION | GESTION ET RÈGLES

SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™