



SonicWALL Analyzer

GESTIONE E REPORTING

Tool di reporting, visualizzazione e analisi del traffico applicativo

- Report grafici dettagliati
- Report di nuova generazione basati su syslog
- Report degli eventi di SonicWALL SRA e CDP
- Report universali pianificati
- Reporting immediato
- Reporting sulla conformità
- Report dettagliati sulle minacce
- Report basati sugli utenti
- Accesso ubiquo
- Rilevazione intelligente delle minacce

L'uso di applicazioni Web per attività non lavorative (ad es. servizi di webmail, Facebook®, messaggistica istantanea, BitTorrent) da parte dei dipendenti provoca un elevato consumo di banda, riduce la produttività e aumenta il rischio di minacce alla rete. I manager IT necessitano di una soluzione in grado di potenziare la sicurezza, ottimizzare l'uso della rete, gestire le applicazioni in modo intelligente e fornire funzioni di analisi forense e risoluzione dei problemi a un prezzo accessibile. Purtroppo la maggior parte dei prodotti di reporting e analisi del traffico delle applicazioni disponibili sul mercato offrono una visibilità limitata e sono spesso difficili da utilizzare.

SonicWALL® Analyzer è un tool di reporting e analisi del traffico, facile da utilizzare e basato sul Web, che fornisce una visione dettagliata in tempo reale (o storica) sullo stato di salute, le prestazioni e la sicurezza della rete. Analyzer supporta i firewall, i prodotti di backup e recovery e le soluzioni di accesso remoto sicuro di SonicWALL. Aziende e organizzazioni di qualsiasi dimensione possono così migliorare la produttività dei dipendenti, ottimizzare l'uso della larghezza di banda e aumentare la consapevolezza della sicurezza. SonicWALL è l'unico fornitore di firewall ad offrire una soluzione completa che combina un tool integrato di analisi del traffico delle applicazioni con i dati granulari generati dai firewall di SonicWALL.

Caratteristiche e vantaggi

I **report grafici dettagliati** su attacchi ai firewall, statistiche d'uso della larghezza di banda e analisi del traffico delle applicazioni offrono alle aziende maggiore visibilità sulla produttività dei dipendenti e su attività sospette in rete.

I **report di nuova generazione basati su syslog** utilizzano una rivoluzionaria architettura che semplifica il riepilogo dei dati, offrendo report quasi in tempo reale sui messaggi syslog in arrivo. L'accesso diretto ai dati grezzi sottostanti garantisce una migliore granularità delle analisi e maggiori possibilità di personalizzazione dei report.

I **report degli eventi di SonicWALL Secure Remote Access (SRA) e Continuous Data Protection (CDP)** utilizzano i dati dei messaggi syslog di nuova generazione per fornire una panoramica dettagliata dello stato di salute e del comportamento dell'appliance.

I **report universali pianificati** forniscono un unico modello base per tutti i report pianificati. Un report può combinare diagrammi e tabelle per più unità. I report possono essere pianificati e inviati in diversi formati ad uno o più indirizzi di posta elettronica.

Il **reporting immediato** offre diverse viste personalizzabili per visualizzare diversi report di riepilogo in un'unica pagina. Gli utenti possono accedere facilmente ai dati essenziali della rete e analizzare in breve tempo le informazioni contenute in svariati report.

Il **reporting sulla conformità** permette agli amministratori di generare report conformi alle norme vigenti. Questi report possono essere creati ad hoc o pianificati secondo normative di conformità specifiche.

I **report dettagliati sulle minacce** raccolgono informazioni sugli attacchi alla rete sventati e forniscono l'accesso immediato alle minacce rilevate dai firewall SonicWALL mediante i servizi di gateway anti-virus, anti-spyware, prevenzione delle intrusioni e controllo intelligente delle applicazioni.

I **report basati sugli utenti** permettono di monitorare le attività di singoli utenti sulla rete locale o su reti remote per avere una migliore comprensione dell'uso del traffico nell'intera rete, e in particolare riguardo ad applicazioni utilizzate, siti Web visitati, attività di backup e connessioni VPN per ogni utente.

L'**accesso ubiquo** semplifica la creazione dei report da parte degli amministratori, che possono effettuare analisi dettagliate da qualsiasi luogo mediante un normale browser Web.

La **rilevazione intelligente delle minacce** fornisce report granulari su determinati tipi di attacco o tentativi d'intrusione, completi di informazioni sull'indirizzo di origine dell'attacco, per poter reagire rapidamente ad ogni minaccia.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Specifiche tecniche



- Analyzer per la serie TZ
01-SSC-3378
- Analyzer per NSA 240, NSA 2400
01-SSC-3379
- Analyzer for NSA 3500
01-SSC-3380
- Analyzer per NSA 4500
01-SSC-3381
- Analyzer per le serie E-Class NSA
e SuperMassive™ E10000
01-SSC-3382
- Analyzer per CDP 210
01-SSC-3383
- Analyzer per CDP 220
01-SSC-3384
- Analyzer per CDP 5040B
01-SSC-3385
- Analyzer per CDP 6080B
01-SSC-3386
- Analyzer per SRA 1200
01-SSC-3387
- Analyzer per SRA 4200
01-SSC-3388
- Analyzer per la serie E-Class SRA
01-SSC-3389

SonicWALL Analyzer



Visualizzazione semplificata di statistiche sul traffico, come ad es. i siti Web più visitati. Analisi dettagliata dei report per ordinare i dati in base a criteri specifici come nome, indirizzo IP, categoria di sito Web e numero di tentativi di connessione.



I report grafici intuitivi semplificano ulteriormente il monitoraggio delle appliance SonicWALL gestite. Eventuali anomalie del traffico sono facilmente rilevabili esaminando i dati di utilizzo in base a periodo di tempo, origine, destinazione o servizio. I report possono essere esportati in MS Excel o PDF o direttamente verso una stampante.



Le funzionalità di reporting granulare integrate permettono di visualizzare informazioni sull'uso del traffico di rete da parte delle principali applicazioni. Facile identificazione delle applicazioni rilevate o bloccate più frequentemente in base a categoria, origine o periodo di tempo.



La gestione delle minacce, integrata di serie in Analyzer, consente di visualizzare le minacce più frequenti in base a obiettivo, origine o tipologia. Tutti gli strumenti di reporting completo sulle minacce, come gateway anti-virus, prevenzione delle intrusioni e anti-spyware, sono inclusi nella soluzione.

Requisiti di sistema

Sistema operativo

Windows Server 2003 64 bit (SP2)
Windows Server 2008 SBS 64 bit (R2)
Windows Server 2008 Standard 64 bit (R2)
Windows Vista Pro 64 bit (SP1)
Windows 7 Pro 64 bit (SP1)
In tutti i casi descritti SonicWALL Analyzer funziona come applicazione a 32 bit.

Hardware per Analyzer Server

Requisiti minimi: Single Core 3 GHz
Processore x86, 4 GB di RAM, 100 GB di HDD

Java

Java SE Runtime Environment 1.6 o successivo

Browser

Microsoft® Internet Explorer 8.0 o successivo
Mozilla Firefox 6.0 o successivo
Google Chrome 13.0 e successivo
Supportato solo su piattaforme Microsoft Windows

Appliance virtuale

Hypervisor: VMware ESX e ESXi
Sistema operativo installato: SonicLinux hardened
Dimensioni appliance: 250 GB, 950 GB
RAM allocata: 4 GB
Guida alla compatibilità hardware per VMware: visitare www.vmware.com/resources/compatibility/search.php

Appliance SonicWALL supportate

SonicWALL Network Security Appliance (NSA): serie E-Class NSA, serie NSA, serie TZ e serie PRO¹
SonicWALL Continuous Data Protection
SonicWALL Content Security Manager (CSM)
SonicWALL Secure Remote Access (SRA); versione E-Class e PMI

Firmware SonicWALL supportato

Serie SonicWALL E-Class NSA e NSA: SonicOS Enhanced 5.0 o superiore
Serie SonicWALL PRO: SonicOS Enhanced 3.2 o superiore
Serie SonicWALL TZ: SonicOS Standard 3.1 o superiore e Enhanced 3.2 o superiore
Serie SonicWALL CSM: SonicWALL 2.0 o superiore
Serie SonicWALL SRA per le PMI: firmware 2.0 o superiore
Serie SonicWALL E-Class SRA: firmware 9.0 o superiore

¹ I vecchi modelli SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2 e SonicWALL Pro-VX non sono supportati.

² Solo nuove appliance Aventura E-Class SRA con numeri di serie a 12 cifre esadecimali.



SonicWALL Italy
T + 39.010.7407851
Italy@sonicwall.com
Contatti Supporto SonicWALL
www.sonicwall.com/emea/4724.html

Linea di soluzioni di sicurezza dinamica SonicWALL



**SICUREZZA
DI RETE**



**ACCESSO
REMOTO SICURO**



**SICUREZZA
WEB / E-MAIL**



**BACKUP E
RECOVERY**



**GESTIONE
BASATA SU POLICY**



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™