



# SonicWALL ViewPoint

GESTIONE BASATA SU POLICY

Soluzione di reporting completa

- Report grafici dettagliati
- Reporting immediato
- Reporting sulla conformità
- Reporting dettagliato sulle minacce
- Report basati sugli utenti
- Implementazione come software e appliance virtuale
- Pianificazione automatizzata dei report
- Accesso ubiquo
- Rilevazione intelligente delle minacce
- Reporting per Application Control e SSL VPN

Una comprensione dettagliata degli eventi e delle attività svolte in rete, tra cui l'utilizzo di Internet e delle applicazioni da parte dei dipendenti e il consumo della larghezza di banda, è d'importanza fondamentale per le aziende di ogni dimensione. Lo strumento ideale per ottimizzare la sicurezza, gestire la crescita e pianificare le esigenze future deve quindi fornire una visione intelligente e onni-comprendiva di ogni attività della rete.

SonicWALL® ViewPoint™ è un tool di reporting facile da utilizzare e basato sul Web che si integra alla perfezione con i prodotti e i servizi di sicurezza SonicWALL, ampliandone le funzionalità. Le sue avanzate funzioni di reporting offrono agli amministratori una visione istantanea sullo stato di salute della rete aziendale, come ad esempio sulle performance e sulla sicurezza. SonicWALL ViewPoint permette ad aziende di qualsiasi dimensione di monitorare l'utilizzo della rete, del Web e delle applicazioni nonché delle attività di sicurezza attraverso un dashboard personalizzabile e diversi report storici.

SonicWALL ViewPoint può essere implementato come applicazione software su server Windows® di terzi o come appliance virtuale SonicWALL in un ambiente VMware®. Sulla base delle informazioni e degli eventi ricevuti dalle appliance SonicWALL viene visualizzato il traffico sulle reti LAN wireless o cablate, WAN o VPN. I report generati da SonicWALL ViewPoint, oltre ad essere personalizzabili e pianificabili secondo le diverse esigenze, possono essere esportati in diversi formati per garantire alle aziende la piena conformità alle normative vigenti.

## Caratteristiche e vantaggi

Il **report grafici dettagliati** sulle attività riguardanti la rete, inclusi attacchi ai firewall, utilizzo della larghezza di banda, visite ai siti Web, utilizzo delle applicazioni e comportamento in rete degli utenti, forniscono un maggiore controllo su eventuali attività sospette e sulla produttività dei dipendenti.

Il **reporting immediato** consente di visualizzare in una sola schermata diversi report di riepilogo, aiutando gli utenti a interpretare i dati vitali della rete e ad analizzare velocemente le informazioni contenute in svariati report.

Il **reporting sulla conformità** permette agli amministratori di generare e visualizzare report conformi alle norme vigenti. Questi report possono essere creati sul momento o pianificati, in base alle normative di conformità aziendali specifiche.

Il **reporting dettagliato sulle minacce** consente di raccogliere informazioni sugli attacchi alla rete sventati e fornisce un accesso immediato alle appliance di sicurezza SonicWALL per mezzo del Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service.

Grazie al **reporting basato sugli utenti** è possibile monitorare le attività degli utenti sulla rete locale o su reti remote per meglio comprendere le dinamiche di utilizzo dell'intera rete.

Implementazione flessibile come **software** (installabile nell'infrastruttura esistente) o come **appliance virtuale** (sfruttando le risorse di calcolo condivise per ottimizzare l'utilizzo, semplificare la migrazione e ridurre i costi di capitale).

La **pianificazione automatizzata dei report** supporta funzionalità e-mail e l'archiviazione di report giornalieri/settimanali/mensili – esportabili in diversi formati – per la condivisione dei dati tra utenti e management e l'archiviazione dei report per un uso futuro.

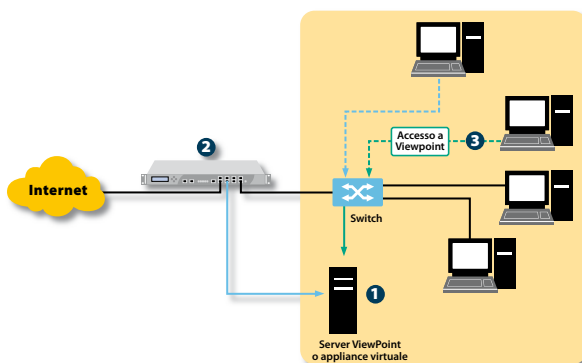
L'**accesso ubiquo** semplifica l'accesso ai report da parte degli amministratori, che possono utilizzare tutte le funzioni di reporting da qualsiasi luogo tramite un normale browser Web.

La **rilevazione intelligente delle minacce** fornisce un reporting granulare per ogni minaccia o tentativo d'intrusione, completo di informazioni sulla fonte dell'attacco, e consente di reagire con la massima prontezza ad ogni minaccia.

Il **reporting per Application Control e SSL VPN** permette una migliore gestione dell'efficienza e della produttività della rete. Gli amministratori possono generare report per l'Application Control relativi ad applicazioni, utenti o policy specifiche e report SSL VPN basati su utenti specifici, larghezza di banda consumata, accessi alle risorse e dati di autenticazione. Gli utenti possono eseguire analisi dettagliate dei report. Implementazione flessibile come software (installabile nell'infrastruttura esistente) o come appliance virtuale (sfruttando le risorse di calcolo condivise per ottimizzare l'utilizzo, semplificare la migrazione e ridurre i costi di capitale).

# Specifiche tecniche

## Architettura SonicWALL ViewPoint



- 1 Il software SonicWALL ViewPoint viene installato sulla rete locale dove si trova l'appliance di sicurezza SonicWALL.
- 2 L'amministratore deve configurare l'appliance di sicurezza SonicWALL principale per l'invio dei dati syslog al server ViewPoint o all'appliance virtuale.
- 3 Mediante un comune browser, l'amministratore può accedere a SonicWALL ViewPoint da PC differenti per generare e visualizzare report di riepilogo dei firewall (ad es. riepilogo immediato, utenti che impegnano maggiormente la banda, riepilogo della larghezza di banda utilizzata o riepilogo degli attacchi).

## Esempi di report di ViewPoint



### Report immediato

Le schermate personalizzate contengono diversi report di riepilogo.



### Utilizzo del Web e delle applicazioni

Grazie alla possibilità di esaminare in che modo gli utenti della rete utilizzano il Web, gli amministratori possono capire quanto tempo viene trascorso dai dipendenti a navigare in Internet, quali pagine Web vengono visitate e quali applicazioni vengono utilizzate in un qualsiasi momento, ottenendo indicazioni preziose su modelli di utilizzo non conosciuti.



### Riepilogo degli attacchi

Fornisce informazioni sugli attacchi sventati tramite i servizi in abbonamento di SonicWALL.



### Servizi, protocolli e applicazioni

Gli utenti possono vedere le tipologie di traffico trasmesse attraverso la rete aziendale e quindi decidere quale traffico può essere eliminato per incrementare le performance della rete.

## Requisiti minimi di sistema

### Sistema operativo

Windows Server 2003 a 32 e 64 bit (SP2), Windows Server 2008 SBS a 64 bit (R2), Windows Server 2008 Standard a 32 bit (SP2) e 64 bit (R2), Windows XP Professional a 32 bit (SP3), Windows Vista a 32 e 64 bit (SP1), Windows 7 a 32 e 64 bit.

In tutti i casi descritti SonicWALL ViewPoint funziona come applicazione a 32 bit.

### Hardware per ViewPoint Server

Ambiente x86: (minimo) processore Intel a CPU singola da 3 GHz, 2 GB di RAM e 100 GB di spazio su disco

### Java

Plug-in Java, versione 1.6 o successiva

### Appliance SonicWALL supportate

Appliance di sicurezza SonicWALL: serie E-Class NSA, serie NSA, serie TZ, serie PRO, appliance SonicWALL CSM, appliance SonicWALL SSL VPN

### Browser supportati

Microsoft® Internet Explorer 6.0 o successivo, Mozilla Firefox 2.0 o successivo  
Supportato solo sulle piattaforme Microsoft Windows

Per ulteriori informazioni sui tool di reporting e gestione delle policy SonicWALL, tra cui ViewPoint, visitate il nostro sito all'indirizzo <http://www.sonicwall.com/products/mgmt.html>

### Firmware SonicWALL supportato

Appliance di sicurezza SonicWALL:

Serie E-Class NSA, serie NSA: SonicOS Enhanced 5.0 o successivo

Serie PRO: SonicOS Enhanced 3.2 o successivo

Serie TZ: SonicOS Standard 3.1 o successivo e SonicOS Enhanced 3.2 o successivo

Appliance SonicWALL CSM: SonicWALL 2.0 o successivo

Appliance SonicWALL SSL VPN: SonicWALL SSL VPN per le PMI, firmware 2.0 o successivo, e SonicWALL Aventura E-Class SSL VPN, firmware 9.0 o successivo

### Appliance virtuale

Hypervisor: VMware ESX e ESXi

Sistema operativo installato: SonicLinux hardened

Dimensioni appliance: 250 GB - 950 GB

Memoria allocata: 3 GB

Guida alla compatibilità hardware per VMware:

<http://www.vmware.com/resources/compatibility/search.php>

## Linea di protezione completa SonicWALL



SICUREZZA  
DI RETE



ACCESSO  
REMOTO SICURO



SICUREZZA  
WEB / E-MAIL



BACKUP E  
RECOVERY



GESTIONE  
BASATA SU POLICY

# SONICWALL

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

SonicWALL Italy  
T + 39.010.7407851  
Italy@sonicwall.com

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