



SonicWALL ViewPoint

MONITORING AND REPORTING

Comprehensive Network Reporting Solution

- Comprehensive set of graphical reports
- "At-a-Glance" reporting
- Compliance reporting
- Multi-threat reporting
- User-based reporting
- Automated report scheduling
- Ubiquitous access
- New attack intelligence
- Multiple concurrent sessions

Understanding network events, activity and usage such as security threats, employee Internet utilization and bandwidth consumption is essential for organizations of all sizes. To optimize security, manage growth and plan for future needs, IT administrators require a tool that provides an intelligent, comprehensive view of events and activities throughout the network.

SonicWALL® ViewPoint™ is an easy-to-use Web-based reporting tool that fully complements and extends SonicWALL's security products and services. Comprehensive reporting capabilities provide administrators instant insight into the health of their network including both performance and security. Using both a customizable dashboard and a variety of historical reports, SonicWALL ViewPoint helps organizations of all sizes track network utilization, monitor security activity and view Web usage.

SonicWALL ViewPoint software is easy to install and maintain, allowing multiple users to log in simultaneously and generate reports specific to their areas of responsibilities. Traffic over wired and wireless LAN, WAN or VPN networks are illustrated based on information and events received from SonicWALL appliances. Furthermore, SonicWALL ViewPoint provides customizable and scheduled reports in a variety of exportable formats that aid organizations in preparing for regulatory compliance audits.

Features and Benefits

Comprehensive set of graphical reports

includes firewall attacks, bandwidth usage, Web site visits, user activity, which provides visibility into suspicious activity and employee productivity.

"At-a-Glance" reporting provides a customizable view that illustrates multiple summary reports on a single page, helps users navigate to vital network metrics and allows them to quickly analyze data across a variety of reports.

Compliance reporting gives administrators the capability to generate and view reports that fulfill compliance requirements. Delivered both on an ad-hoc and scheduled basis, these reports can be saved as templates for future use and customized for specific corporate regulatory mandates.

Multi-threat reporting provides the ability to collect information on thwarted attacks and gives instant access to threat activity on SonicWALL's Network Security appliances using the Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service.

User-based reporting tracks users' activities locally or on remote network sites, resulting in a greater understanding of usage behavior across the entire network.

Automated report scheduling provides support for e-mailing and archiving daily/weekly/monthly reports through a variety of exportable formats, allowing users to share data with the management team or archive for future reference.

Ubiquitous access simplifies reporting access by allowing administrators to view all reporting functions from any location using only a standard Web browser.

New attack intelligence offers more granular reporting on the type of attack or intrusion, as well as the source of the attack, enabling administrators to react faster to incoming threats.

Multiple concurrent sessions allows multiple users to log in and generate reports simultaneously on the system, yielding greater flexibility without compromising performance.



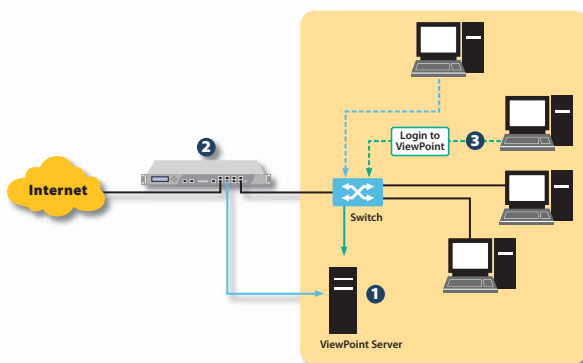
Sonicwall Approved Partner

Tel North: 0151 2031400 Tel South: 0118 9071600
Email: Info@castleforce.com Web: www.castleforce.com



Specifications

SonicWALL ViewPoint Architecture

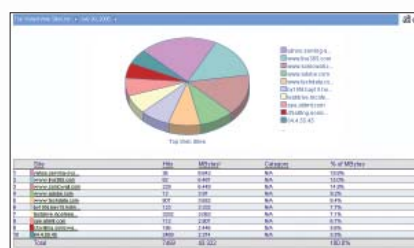


- 1 SonicWALL ViewPoint software is installed on a local network computer behind the SonicWALL Network Security appliance.
- 2 The administrator configures the main SonicWALL Network Security appliance to send syslog data to the SonicWALL ViewPoint server.
- 3 Multiple users can log into SonicWALL ViewPoint simultaneously to run and view firewall summary reports such as "At-a-Glance," Top Users of Bandwidth, Summary Bandwidth and Attack Summary.

Sample ViewPoint Reports



"At-a-Glance"
Customized views illustrate multiple summary reports.



Web Usage
Administrators can view all aspects of Web usage behavior throughout the network. Find out how much time employees spend surfing Web sites, discover exactly what Web sites were accessed at what time and reveal hidden usage patterns.



Attack Summary
Collect information on thwarted attacks using SonicWALL subscription services.



Services and Protocols
Users can view the types and kinds of traffic that are transmitted throughout their network. Find out what kinds of traffic could be eliminated for maximum network performance.

Minimum System Requirements

Operating System

Windows Server 2000 (SP4), Windows Server 2003 32 bit and 64 bit (SP2), Windows Server 2008 SBS 64 bit, Windows Server 2008 Standard 32 bit and 64 bit (SP1), Windows XP Professional 32 bit (SP3), Windows Vista 32 and 64 bit (SP1).

In all instances SonicWALL ViewPoint is running as a 32 bit application.

Hardware for ViewPoint Server

x86 Environment: Minimum 3 GHz processor single-CPU Intel processor, 2 GB RAM and 100 GB disk space

Java

Java Plug-in version 1.5 or later

Supported SonicWALL Appliances

SonicWALL Network Security appliances: E-Class NSA Series, NSA Series TZ Series, PRO Series, SonicWALL CSM appliances, SonicWALL SSL VPN appliances

Supported Internet Browsers

Microsoft® Internet Explorer 6.0 or higher, Mozilla Firefox 2.0 or higher

Supported SonicWALL Firmware

SonicWALL Network Security appliances:
E-Class NSA Series, NSA Series: SonicOS Enhanced 5.0 or higher
PRO Series: SonicOS Enhanced 3.2 or higher
TZ Series: SonicOS Standard 3.1 or higher, and SonicOS Enhanced 3.2 or higher
SonicWALL CSM appliances: SonicWALL 2.0 or higher
SonicWALL SSL VPN appliances: SonicWALL SSL VPN SMB Firmware 2.0 or higher, SonicWALL Aventail E-Class SSL VPN Firmware 9.0 or higher



SonicWALL ViewPoint

01-SSC-2902 ViewPoint for TZ Series and SSL-VPN 200
01-SSC-2901

SonicWALL ViewPoint for NSA Series, PRO Series, SSL-VPN 2000 and 4000
01-SSC-2902

SonicWALL ViewPoint for E-Class NSA Series
01-SSC-2905

Note: ViewPoint comes standard on PRO 4060, 4100, 5060, and CSM 2100, 2200 and 3200 appliances.



Sonicwall Approved Partner

Tel North: 0151 2031400 Tel South: 0118 9071600
Email: info@castleforce.com Web: www.castleforce.com

