SonicWALL ViewPoint

POLICY AND MANAGEMENT

Comprehensive network reporting solution

- **Comprehensive set of graphical reports**
- **"At-a-Glance" reporting**
- **Compliance reporting**
- **Multi-threat reporting**
- **User-based reporting**
- **Software and virtual appliance options**
- **Automated report scheduling**
- **Ubiquitous access**
- **New attack intelligence**
- **Reporting for Application Control and SSL VPN**

Understanding network events, activity and usage such as security threats, employee application usage and 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 and application usage.

SonicWALL ViewPoint can be deployed as a software application on a third party Windows® server or as a SonicWALL Virtual Appliance in a VMware® environment. 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 include firewall attacks, bandwidth usage, Web site visits, application usage, 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 enables administrators to generate and view reports that fulfill compliance requirements on an ad-hoc and scheduled basis for specific corporate regulatory mandates.

Multi-threat reporting can 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.

Flexible deployment options include **software** (leveraging existing infrastructure) or a **virtual appliance** (leveraging shared computing resources to optimize utilization, ease of migration and reduce capital costs).

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.

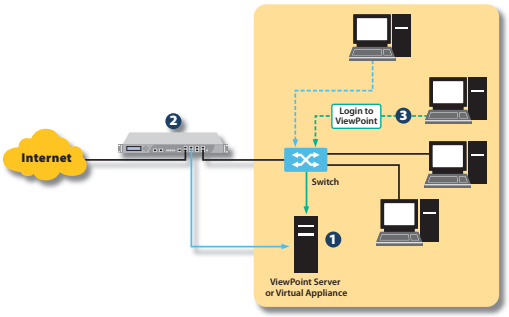
New attack intelligence offers more granular reporting on the type of attack or intrusion, as well as the source of the attack, enabling administrators to react faster to incoming threats.

Reporting for Application Control and SSL VPN enables better management of network efficiency and productivity. Administrators may generate Application Control reports such as top application, users and policies, and SSL VPN reports based on top users, bandwidth consumed, resources accessed and authentication metrics. Users can drill down in reports. Flexible deployment options include software (leveraging existing infrastructure) or a virtual appliance (leveraging shared computing resources to optimize utilization, ease of migration and reduce capital costs).

SONICWALL®

Specifications

SonicWALL ViewPoint Architecture

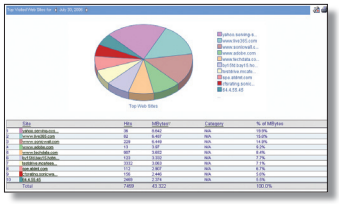


1. SonicWALL ViewPoint software is installed on a local network computer behind the SonicWALL Network Security appliance.
2. The administrator configures the main SonicWALL Network Security appliance to send syslog data to the SonicWALL ViewPoint server or virtual appliance.
3. Using a Web browser, the administrator can log into SonicWALL ViewPoint from different PCs 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 illlustrate multiple summary reports.

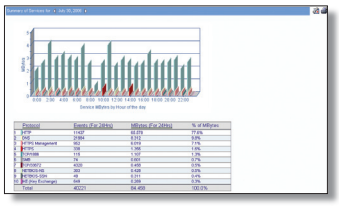


Web and Application Usage

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, what applications are used at what time, and reveal hidden usage patterns.

Attack Summary

Collect information on thwarted attacks using SonicWALL subscription services.



Services, Protocols and Applications

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 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), Windows 7 32 bit and 64 bit.

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 1.6 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 only on Microsoft Windows platforms

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

Virtual Appliance

Hypervisor: VMware ESX and ESXi

Operation System Installed: Hardened SonicLinux

Appliance Size: 250 GB - 950 GB

Allocated Memory: 3 GB

VMware Hardware Compatibility Guide: http://www.vmware.com/resources/compatibility/search.php

For more information on SonicWALL Policy and Management tools including ViewPoint, please visit our Web site at **http://www.sonicwall.com/us/Centralized_Management_and_Reporting.html**

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

SonicWALL's line-up of comprehensive protection

NETWORK SECURITY | SECURE REMOTE ACCESS | WEB AND E-MAIL SECURITY | BACKUP AND RECOVERY | POLICY AND MANAGEMENT

SonicWALL, Inc.
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com