SonicWALL ViewPoint

Comprehensive network reporting solution

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**
- **“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**

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).
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 illustrate 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.

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.

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

Minimum System Requirements

Operating System
Windows Server 2003, 32 bit and 64 bit (SP2), Windows Server 2008 (R2), Windows XP Professional 32 bit (SP3), Windows Vista 32 and 64 bit (SP1), Windows 7 32 bit and 64 bit.

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, T2 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 Avnetail 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

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

© 2011 SonicWALL, Inc. All rights reserved. SonicWALL® is a registered trademark of SonicWALL, Inc. and all other SonicWALL product and service names and slogans are trademarks or registered trademarks of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective owners. 04/11 SW 1215