Analyzer

Application traffic analytics, visualization and reporting tool

When employees use web applications (e.g., web mail, Facebook®, instant messaging, BitTorrent), for non-work-related activity, bandwidth utilization spikes, productivity plummets and threats to the network begin to emerge. IT needs a solution to strengthen security awareness, optimize network utilization, intelligently manage applications, and cost effectively provide troubleshooting and forensics analysis. However, most third-party application traffic analytics and reporting products offer limited visibility and can be complex to use.

Dell® SonicWALL® Analyzer is an easy-to-use web-based traffic analytics and reporting tool that provides real-time and historical insight into the health, performance and security of the network. Analyzer supports Dell SonicWALL firewalls, backup and recovery products, and secure remote access solutions. Organizations of all sizes benefit from enhanced employee productivity, optimized network bandwidth utilization and increased security awareness. Dell SonicWALL is the only firewall vendor that provides a complete solution by combining off-box application traffic analytics with granular data generated by Dell SonicWALL firewalls.

- **Comprehensive graphical reports**
- **Next-gen syslog reporting**
- **Dell SonicWALL SRA and CDP event reporting**
- **Universal scheduled reports**
- **At-a-glance reporting**
- **Compliance reporting**
- **Multi-threat reporting**
- **User-based reporting**
- **Ubiquitous access**
- **New attack intelligence**

Features and benefits

Comprehensive graphical reports on firewall threats, bandwidth usage statistics, and application traffic analysis, provides organizations visibility into employee productivity and suspicious network activity.

Next-gen syslog reporting uses revolutionary architecture enhancements to streamline data summarization, allowing for near real-time reporting of incoming syslog messages. Direct access to the underlying raw data further facilitates extensive granular capabilities and highly customizable reporting.

Dell SonicWALL Secure Remote Access (SRA) and Continuous Data Protection (CDP) event reporting leverages next-generation syslog data to provide powerful insight into the appliance's health and behavior.

Universal scheduled reports provide a single entry point for all scheduled reports. One report can combine charts and tables for multiple units. Reports can be scheduled and sent out in various formats to one or more email addresses.

At-a-glance reporting offers customizable views to illustrate multiple summary reports on a single page. Users can easily navigate through vital network metrics to analyze data quickly across a variety of reports.

Compliance reporting enables administrators to generate reports that fulfill compliance requirements on an ad-hoc and scheduled basis for specific regulatory mandates.

Multi-threat reporting collects information on thwarted attacks providing instant access to threat activities detected by Dell SonicWALL firewalls using the Dell SonicWALL Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service.

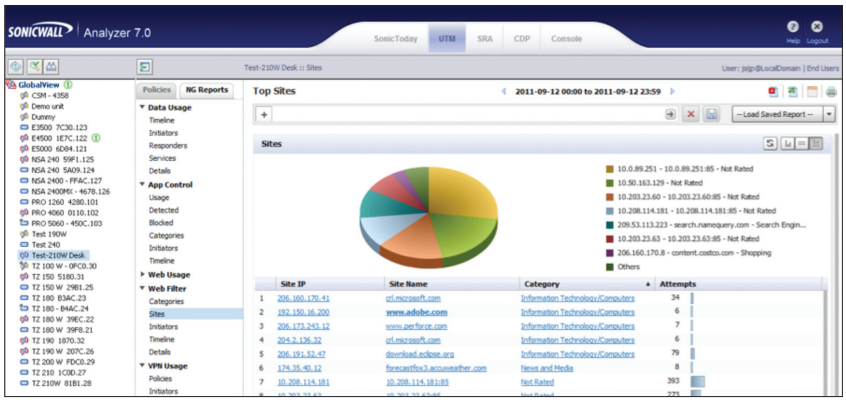
User-based reporting tracks individual user activities locally or on remote network sites to provide even greater insight into traffic usage across the entire network and, more specifically, application usage, web sites visited, backup activity and VPN connections per user.

Ubiquitous access simplifies reporting to provide administrators with analysis of any location using only a standard web browser.

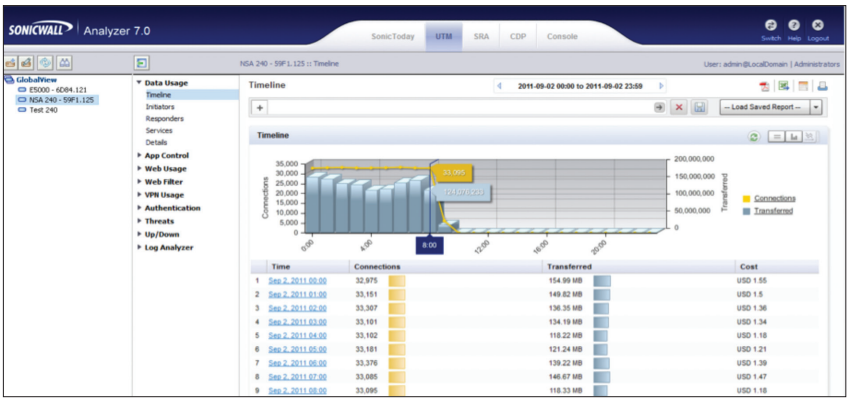
New attack intelligence offers granular reporting on specific types of attacks or intrusion attempts and the source address of the attack to enable administrators to react quickly to incoming threats.

Dell SonicWALL Analyzer

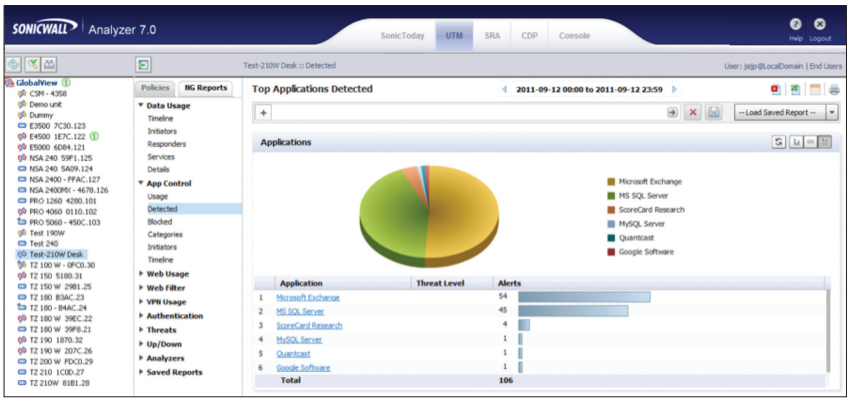
Easily view traffic usage statistics such as top websites visited. Drill down reporting allows for sorting of data according to granular details, such the site name, IP address, website category and number of connections attempted.



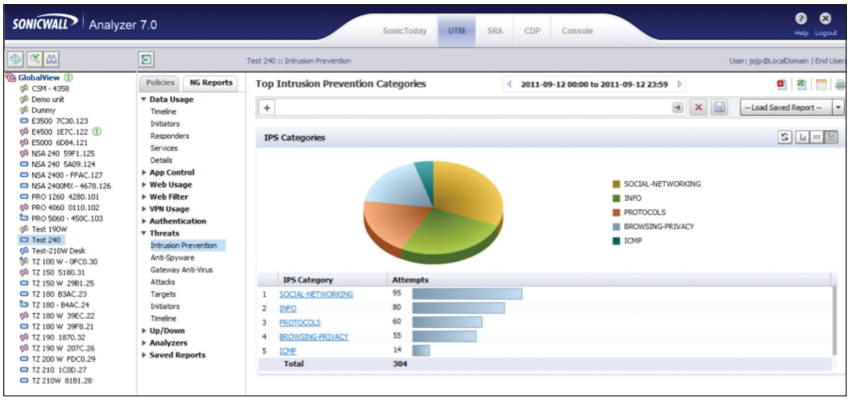
Monitoring managed Dell SonicWALL appliances is a breeze with intuitive graphical reports. Easily identify traffic anomalies based on usage data for a specific timeline, initiator, responder or service. Export reports to MS Excel, PDF or directly to a printer.



Built-in granular reporting allows for traffic usage data to be displayed according to top applications on the network. Easily identify the top applications detected or blocked according to category, timeline or initiator.



Threat management comes standard with Analyzer; easily view the top threats to the network by target, initiator, or threat type. Comprehensive threat reporting, such as Gateway Anti-Virus, Intrusion Prevention, and Anti-Spyware, are all included.



DELL SonicWALL

System requirements

Operating system

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 all instances Dell SonicWALL Analyzer is running as a 32 bit application.

Hardware for Analyzer Server

Minimum Requirements: Single Core 3GHz x86 Processor, 4 GB RAM, 100 GB HDD

Java

Java SE Runtime Environment 1.6 or later

Internet browsers

Microsoft® Internet Explorer 8.0 or higher

Mozilla Firefox 6.0 or higher

Google Chrome 13.0 and above

Supported only on Microsoft Windows platforms

Virtual appliance

Hypervisor: VMware ESX and ESXi

Operation System Installed: Hardened SonicLinux

Appliance Size: 250 GB, 950 GB

Allocated RAM: 4 GB

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

Supported Dell SonicWALL appliances

Dell SonicWALL Network Security Appliances (NSA): E-Class NSA Series, NSA Series, TZ Series, and PRO Series[1]

Dell SonicWALL Continuous Data Protection Series

Dell SonicWALL Content Security Manager (CSM) Series

Dell SonicWALL E-Class and SMB Secure Remote Access (SRA) Series[2]

Supported Dell SonicWALL firmware

Dell SonicWALL E-Class NSA and NSA Series: SonicOS Enhanced 5.0 or higher

Dell SonicWALL PRO Series: SonicOS Enhanced 3.2 or higher

Dell SonicWALL TZ Series: SonicOS Standard 3.1 or higher, and Enhanced 3.2 or higher

Dell SonicWALL CSM Series: Dell SonicWALL 2.0 or higher

Dell SonicWALL SRA for SMB Series: Firmware 2.0 or higher

Dell SonicWALL E-Class SRA Series: Firmware 9.0 or higher

[1] Legacy Dell SonicWALL XPRS/XPRS2, Dell SonicWALL SOHO2, Dell SonicWALL Tele2, and Dell SonicWALL Pro/Pro-VX models are not supported.

[2] Only newer Dell SonicWALL Aventail E-Class SRA appliances using 12 character hexidecimal serial numbers.

Dell SonicWALL Analyzer

Analyzer for TZ Series
01-SSC-3378

Analyzer for NSA 240, NSA 2400
01-SSC-3379

Analyzer for NSA 3500
01-SSC-3380

Analyzer for NSA 4500
01-SSC-3381

Analyzer for E-Class NSA and SuperMassive™ E10000 Series
01-SSC-3382

Analyzer for CDP 210
01-SSC-3383

Analyzer for CDP 220
01-SSC-3384

Analyzer for CDP 5040B
01-SSC-3385

Analyzer for CDP 6080B
01-SSC-3386

Analyzer for SRA 1200
01-SSC-3387

Analyzer for SRA 4200
01-SSC-3388

Analyzer for E-Class SRA Series
01-SSC-3389

DELL SonicWALL