



The SonicWALL Global Management System

GLOBAL MANAGEMENT SYSTEM

Centralized Internet Security Monitoring and Management Solution

Features and Benefits

- **Comprehensive security management**
- **Managed VPN services**
- **Real-time, active network monitoring**
- **Remote VPN client connection management**
- **Centralized graphical reporting**
- **Detailed graphical deployment maps**
- **Streamlined license management**
- **Multi-tier policy hierarchy architecture**
- **Distributed security management**
- **Customizable viewing**
- **SNMP support**

SonicWALL® Global Management System enables small organizations, distributed enterprises and service providers to monitor and manage anywhere from a few to thousands of SonicWALL Internet security appliances, all from a central location. SonicWALL GMS is a cost-effective global management solution that reduces staffing requirements, speeds up deployment, and lowers the cost of managing security services.

Extending SonicWALL's renowned easy-to-use management interface, SonicWALL GMS provides a highly scalable, sophisticated security management system for geographically distributed networks. SonicWALL GMS gives administrators the integrated tools to manage all security policies and services throughout a large-scale, multiple policy enterprise or service provider environment. Administrators can configure SonicWALL firewall settings as well as SonicWALL upgrade and subscription services, such as VPN, intrusion prevention, anti-virus and content filtering via a Web-based interface. Security policies can be centrally pushed to SonicWALL Internet security appliances on an individual, group or global basis over encrypted VPN tunnels to ensure maximum security.

Features and Benefits

Configuration and management tools for **comprehensive security management** allow administrators to globally define, distribute, enforce and deploy a full range of VPN and security policies for thousands of SonicWALL appliances.

Managed VPN services allows administrators to globally define, distribute, enforce, deploy and monitor VPN policies for SonicWALL VPN gateways that use both standard and enhanced firmware.

Active-network monitoring lowers maintenance costs, reduces network and system downtime and improves customer service by providing real-time active monitoring of both networks and systems. **Net monitor** includes device up/down status, latency monitoring, application monitoring, VPN monitoring and statistics, uptime calculations, and security events for GMS management activities.

Network administrators can **manage remote VPN client connections** by defining user policies for remote Global VPN Client users.

Centralized graphical reporting of firewall and network activities provides insight into usage trends and security events of the SonicWALL appliances.

Visualization viewer provides detailed, graphical maps of the GMS security management deployment, speeding up and simplifying the exploration and understanding of large GMS deployments.

Streamlined license management simplifies storing, applying, tracking and updating security license information for all managed SonicWALL appliances.

Multi-tier policy hierarchy architecture allows administrators to create a hierarchy that groups SonicWALL appliances with similar security profiles, providing the flexibility to manage security policies on an individual, group, regional or global level.

Segments and distributes management responsibilities among a group of individuals and assign different privileges for **distributed security management**.

Customizable viewing capabilities enable network administrators to visualize the managed SonicWALL appliances at any logical view, including a hierarchical view using pre-defined or customized attributes.

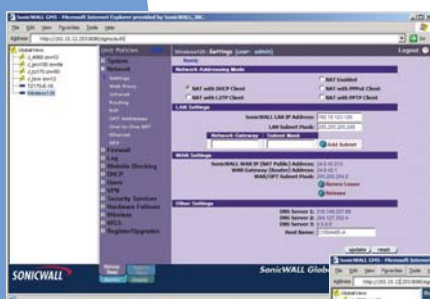
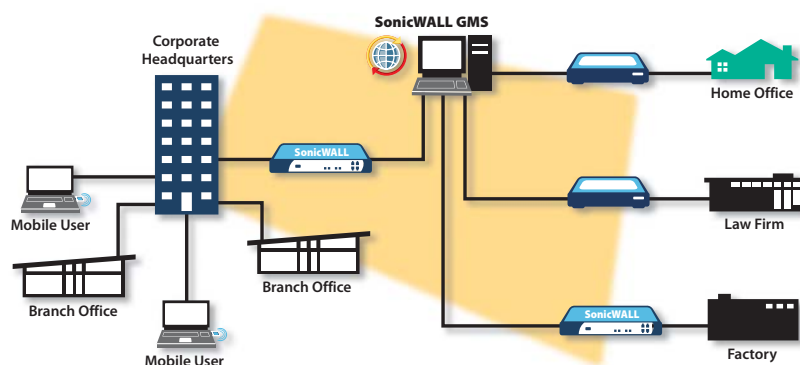
SNMP support provides a powerful, real-time alert mechanism that greatly enhances the ability to pinpoint and respond to critical network events.



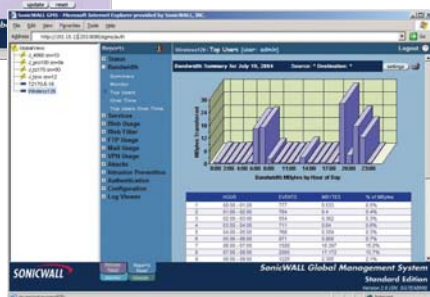
Specifications

SonicWALL Global Management System

Providing a comprehensive security management solution for service providers.



SonicWALL GMS allows administrators to easily create security policies for the SonicWALL Internet security appliances and enforce them at the global, group or unit level.



SonicWALL GMS allows administrators to generate a wide range of informative and historical reports to provide insight into usage trends, such as which Web sites have been accessed by whom, and security events of the managed SonicWALL Internet security appliances.

SonicWALL Minimum System Requirements

GMS. Windows 2000 Server (SP4), Windows 2000 Professional (SP4), Windows XP Professional (SP1) or Windows 2003 Server. 1GB RAM, 300MB disk space, 1.2GHz processor.

GMS. Solaris 8. 650 MHz UltraSPARC III processor, 1 GB memory, two 40 GB IDE drives.

Database. Oracle 9.2.0.1 Standard and Enterprise Editions on Windows XP Professional (SP1), Windows 2000 Server (SP4) or Solaris 8; Microsoft SQL Server 2000 SP3 on Windows 2003 Server (SP3), 80 GB disk space.

Java Database Connectivity (JDBC) driver. Type 3 or 4, JDBC 2.0 compliant. JDBC driver is installed with SonicWALL GMS.

SonicWALL Internet security appliances. Minimum firmware version 6.3.1.2, SonicOS Wireless 1.0, SonicOS Standard 2.0 or SonicOS Enhanced 2.0 required.

GMS Gateway. Minimum firmware version 6.3.1.2, SonicOS Standard 2.0 or SonicOS Enhanced 2.0 required and SonicWALL VPN-based Internet security appliance.

Part Numbers. Contact your SonicWALL sales representative.

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com



*When used with SonicWALL Long Range Dual Band Wireless Card

©2004 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice. F108.SW0215.A4.v1