SONICWALL

SONICWALL GLOBAL MANAGEMENT SYSTEM

Comprehensive security management, monitoring, reporting and analytics

A winning security management strategy demands deep understanding of the security environment to promote better policy coordination and decisions. Not having an enterprise-wide view of the full security construct often leaves organizations at risk to preventable cyber-attacks and compliance violations. Using numerous tools running on different platforms and reporting data in different formats make security analytics and reporting operationally inefficient. This further impairs the organization's ability to quickly recognize and respond to security risks. Organizations must establish a systematic approach to governing the network security environment to overcome these challenges.

SonicWall Global Management System (GMS) solves these challenges. GMS integrates management and monitoring, analytics, forensics and audit reporting. This forms the foundation of a security governance, compliance and risk management strategy. The feature-rich GMS platform gives distributed enterprises, service providers and other organizations a fluid, holistic approach to unifying all operational aspects of their security environment. With GMS, security teams can easily manage SonicWall firewall, wireless access point, email security and secure mobile access solutions, as well as third-party network switch solutions. This is all done via a controlled and auditable work-stream process to keep networks sharp, safe and compliant. GMS includes centralized policy management and enforcement, real-time event monitoring, granular data analytics and reporting, audit trails, and more, under a unified management platform.

Benefits:

- Establishes a unified security governance, compliance and risk management security program
- Adopts a coherent and auditable approach to security orchestration, forensics, analytics and reporting
- Reduces risk and provide a fast response to security events
- Provides an enterprise-wide view of the security ecosystem
- Automates workflows and assures security operation compliance
- Reports on HIPAA, SOX, and PCI for internal and external auditors
- Deploys fast and easy with software, virtual appliance or cloud deployment options — all at a low cost.

GOVERNS CENTRALLY

- Establish an easy path to comprehensive security management, analytic reporting and compliance to unify your network security defense program
- Automate and correlate workflows to form a fully coordinated security governance, compliance and risk management strategy

COMPLIANCE

- Helps make regulatory bodies and auditors happy with automatic PCI, HIPAA and SOX security reports
- Customize any combination of security auditable data to help you move towards specific compliance regulations

RISK MANAGEMENT

- Helps make regulatory bodies and auditors happy with automatic PCI, HIPAA and SOX security reports
- Customize any combination of security auditable data to help you move towards specific compliance regulations

GMS provides a holistic approach to security governance, compliance and risk management

GMS satisfies the enterprise's change management requirements through a workflow automation processes and procedures. The workflow feature assures the correctness and the compliance of policy changes by enforcing a rigorous process for configuring, comparing, validating, reviewing and approving policies prior to deployment. The approval groups are flexible, enabling adherence to company security policy while mitigating risk, reducing errors, improving efficiency, and ensuring high security effectiveness. With GMS's workflow automation and auditing of policy changes, enterprises gain agility and confidence in deploying the right firewall policies, at the right time, and in conformance to compliance regulations.

GMS provides a holistic approach to security governance, compliance and risk management.

1. CONFIGURE AND COMPARE

GMS configures policy **change orders** and **color-codes** diffs for clear comparisons

2. VALIDATE

GMS performs an integrity **validation of the policy's** logic

3. REVIEW & APPROVE

GMS emails reviewers and logs a **(dis)approval audit trail** of the policy

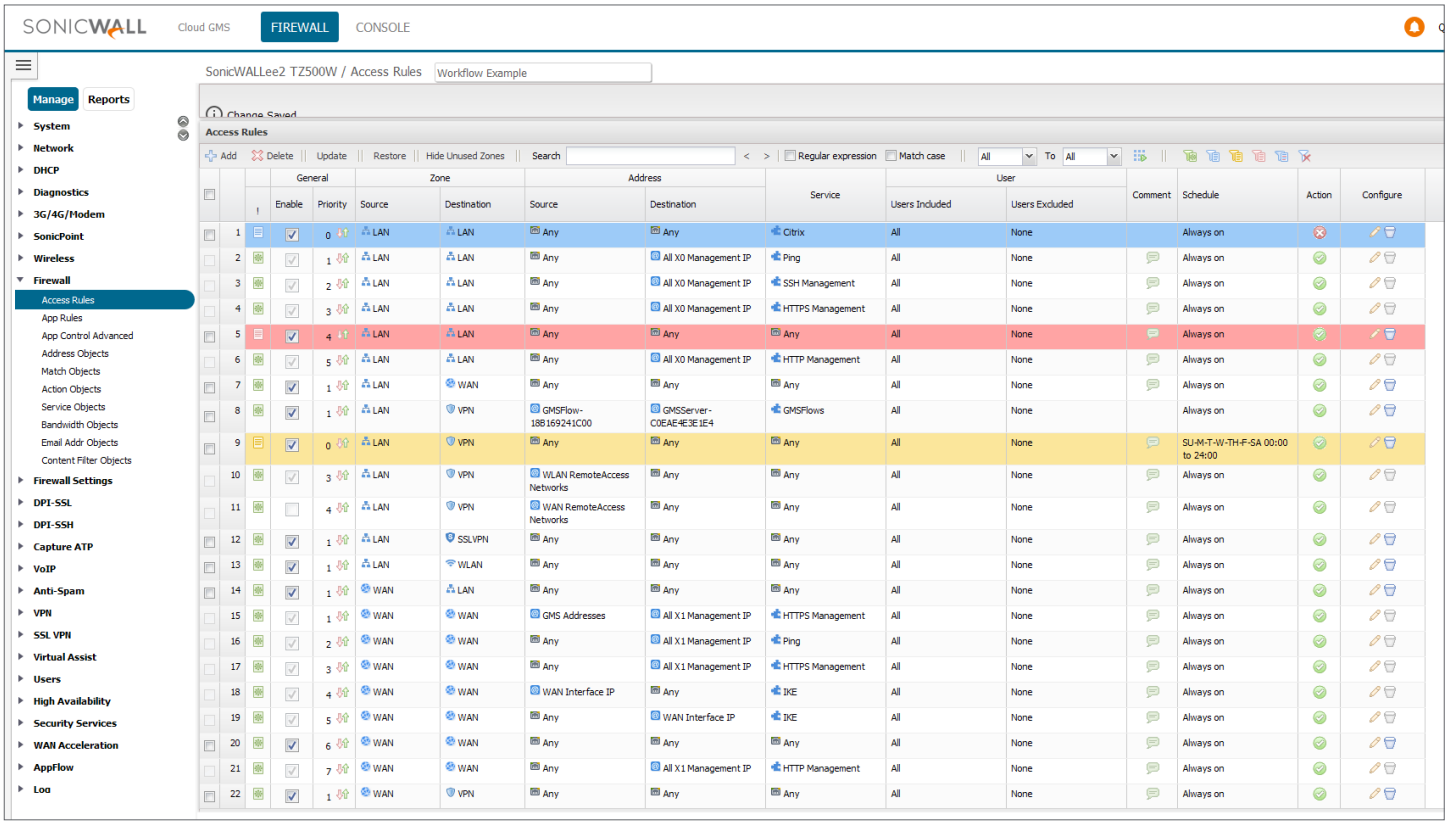
4. DEPLOY

GMS deploys the policy changes immediately or **on a schedule**

5. AUDIT

The change logs enable accurate policy **auditing** and precise **compliance** data

GMS Workflow Automation: Five steps to error-free policy management



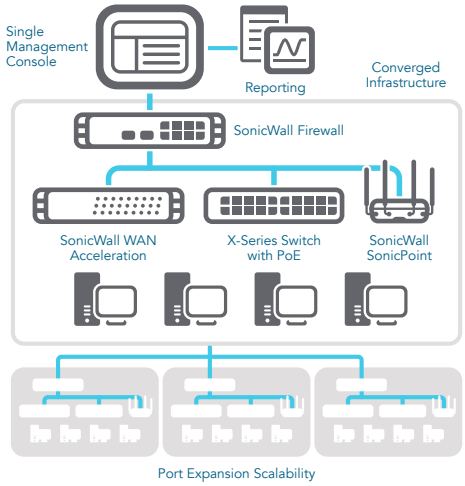
Security management and monitoring features	
Feature	Description
Centralized security and network management	Helps administrators deploy, manage and monitor a distributed network security environment.
Federate policy configuration	Easily sets policies for thousands of SonicWall firewalls, wireless access points, email security, secure remote access devices and switches from a central location.
Change Order Management and Work Flow	Assures the correctness and compliance of policy changes by enforcing a process for configuring, comparing, validating, reviewing and approving policies prior to deployment. The approval groups are user-configurable for adherence to company security policy. All policy changes are logged in an auditable form that ensures the firewall complies with regulatory requirements. All granular details of any changes made are historically preserved to help with compliance, audit trailing, and troubleshooting.
Sophisticated VPN deployment and configuration	Simplifies the enablement of VPN connectivity, and consolidates thousands of security policies.
Offline management	Enables scheduling of configurations and firmware updates on managed appliances to minimize service disruptions.
Streamlined license management	Simplifies appliance management via a unified console, as well as the management of security and support license subscriptions.
Universal dashboard	Features customizable widgets, geographic maps and user-centric reporting.
Active-device monitoring and alerting	Provides real-time alerts with integrated monitoring capabilities, and facilitates troubleshooting efforts, thus allowing administrators to take preventative action and deliver immediate remediation.
SNMP support	Provides powerful, real-time traps for all Transmission Control Protocol/Internet Protocol (TCP/IP) and SNMP-enabled devices and applications, greatly enhancing troubleshooting efforts to pinpoint and respond to critical network events.
Application Visualization and Intelligence	Shows historic and real-time reports of what applications are being used, and by which users. Reports are completely customizable using intuitive filtering and drill-down capabilities.
Rich integration options	Provides application programming interface (API) for web services, command line interface (CLI) support for the majority of functions, and SNMP trap support for both service providers and enterprises.
Dell Networking X-Series switch management	Dell X-Series switches can now be managed easily within TZ, NSA and SuperMassive series firewalls to offer single-pane-of-glass management of the entire network security infrastructure.
Security reporting and analytics	
Feature	Description
Botnet Report	Includes four report types: Attempts, Targets, Initiators, and Timeline containing attack vector context such as Botnet ID, IP Addresses, Countries, Hosts, Ports, Interfaces, Initiator/Target, Source/Destination, and User.
Geo IP Report	Contains information on blocked traffic that is based on the traffic's country of origin or destination. Includes four report types: Attempts, Targets, Initiators, and Timeline containing attack vector context such as Botnet ID, IP Addresses, Countries, Hosts, Ports, Interfaces, Initiator/Target, Source/Destination, and User
MAC Address Report	Shows the Media Access Control (MAC) address on the report page. Includes device-specific information (Initiator MAC and Responder MAC) in five report types: • Data Usage > Initiators • Data Usage > Responders • Data Usage > Details • User Activity > Details • Web Activity > Initiators

Security reporting and analytics con't	
Feature	Description
Capture ATP Report	Shows detail threat behavior information to respond to a threat or infection.
HIPPA, PCI and SOX reports	Includes pre-defined PCI, HIPAA and SOX report templates to satisfy security compliance audits.
Rogue Wireless Access Point Reporting	Shows all wireless devices in use as well as rogue behavior from ad-hoc or peer-to-peer networking between hosts and accidental associations for users connecting to neighboring rogue networks.
Flow analytics and reports	Provides a flow reporting agent for application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring. Offers administrators an effective and efficient interface to visually monitor their network in real-time, providing the ability to identify applications and websites with high bandwidth demands, view application usage per user and anticipate attacks and threats encountered by the network. • A Real-Time Viewer with drag and drop customization • A Real-Time Report screen with one-click filtering • A Top Flows Dashboard with one-click View By buttons • A Flow Reports screen with five additional flow attribute tabs • A Flow Analytics screen with powerful correlation and pivoting features • A Session Viewer for deep drill-downs of individual sessions and packets.
Intelligent reporting and activity visualization	Provides comprehensive management and graphical reports for SonicWall firewalls, email security and secure mobile access devices. Enables greater insight into usage trends and security events while delivering a cohesive branding for service providers.
Centralized logging	Offers a central location for consolidating security events and logs for thousands of appliances, providing a single point to conduct network forensics.
Real-time and historic next-generation syslog reporting	Through a revolutionary enhancement in architecture, streamlines the time-consuming summarization process, allowing for near real-time reporting on incoming syslog messages. Also provides the ability to drill down into data and customize reports extensively.
Universal scheduled reports	Schedules reports that are automatically created and mailed out across multiple appliances of various types to authorized recipients.
Application traffic analytics	Provides organizations with powerful insight into application traffic, bandwidth utilization and security threats, while providing powerful troubleshooting and forensics capabilities.

Scalable distributed architecture

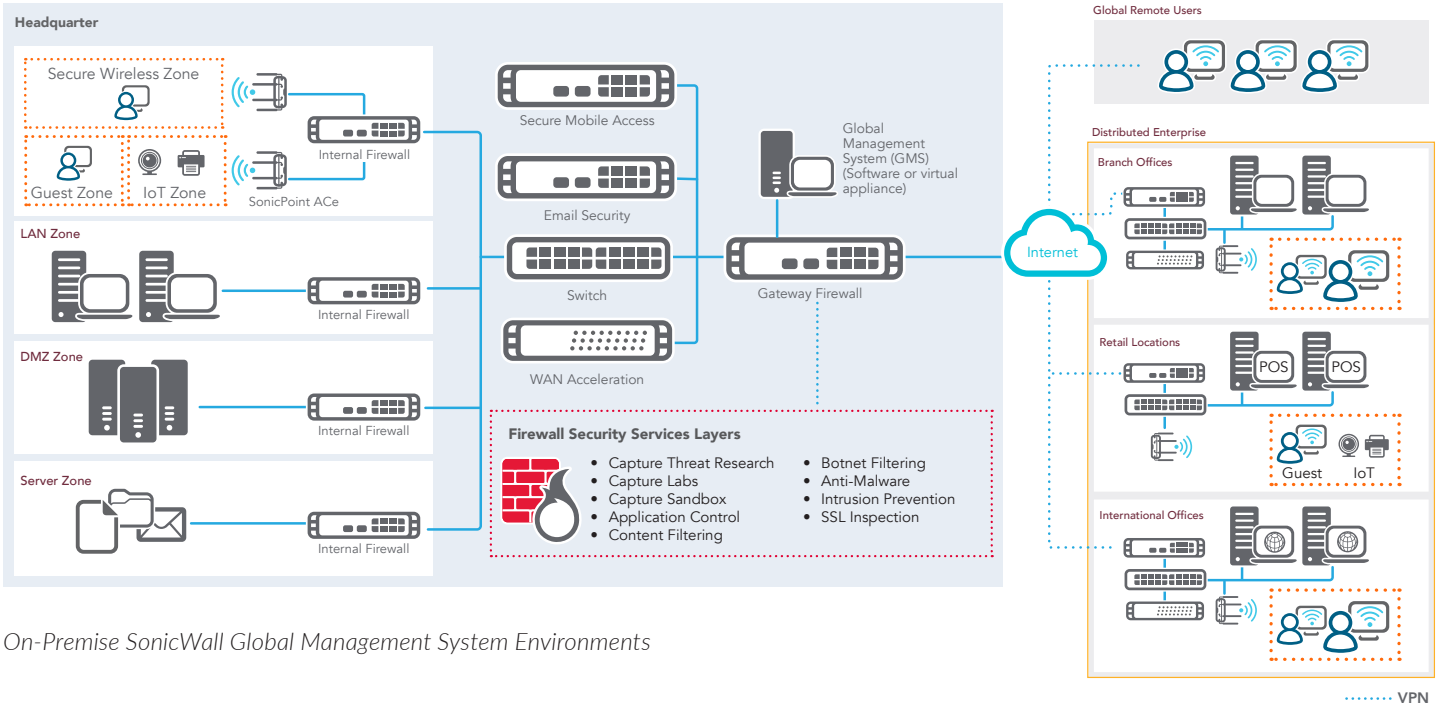
At the core of GMS is a distributed architecture that facilitates limitless system scalability. A single instance of GMS can add visibility and control over thousands of your network security devices under its management, regardless of location. At the user-experience level, the GMS universal dashboard utilizes cutting-edge user interface design and usability concepts that work together to provide consistent operator workflows across the security ecosystem.

GMS is an on-premises solution, deployable as a software or a virtual appliance. Alternatively, SonicWall Cloud Global Management System (Cloud GMS) is cloud-delivered security management and reporting platform that accelerates and simplify security management operations while increasing service agility – all at a low subscription cost.

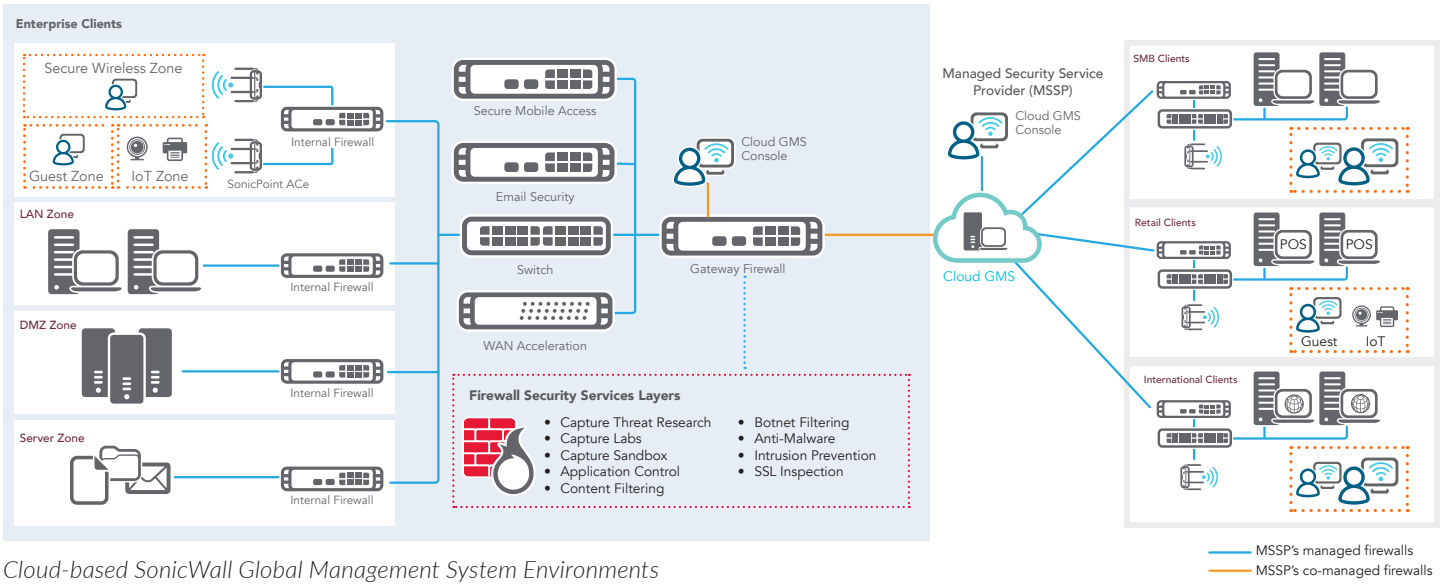


SonicWall Global Management System (GMS)

On-premise GMS provides a complete and scalable security management, analytic and reporting platform for distributed enterprises and data centers while Cloud GMS is ideal for service providers (i.e. MSP and MSSP).



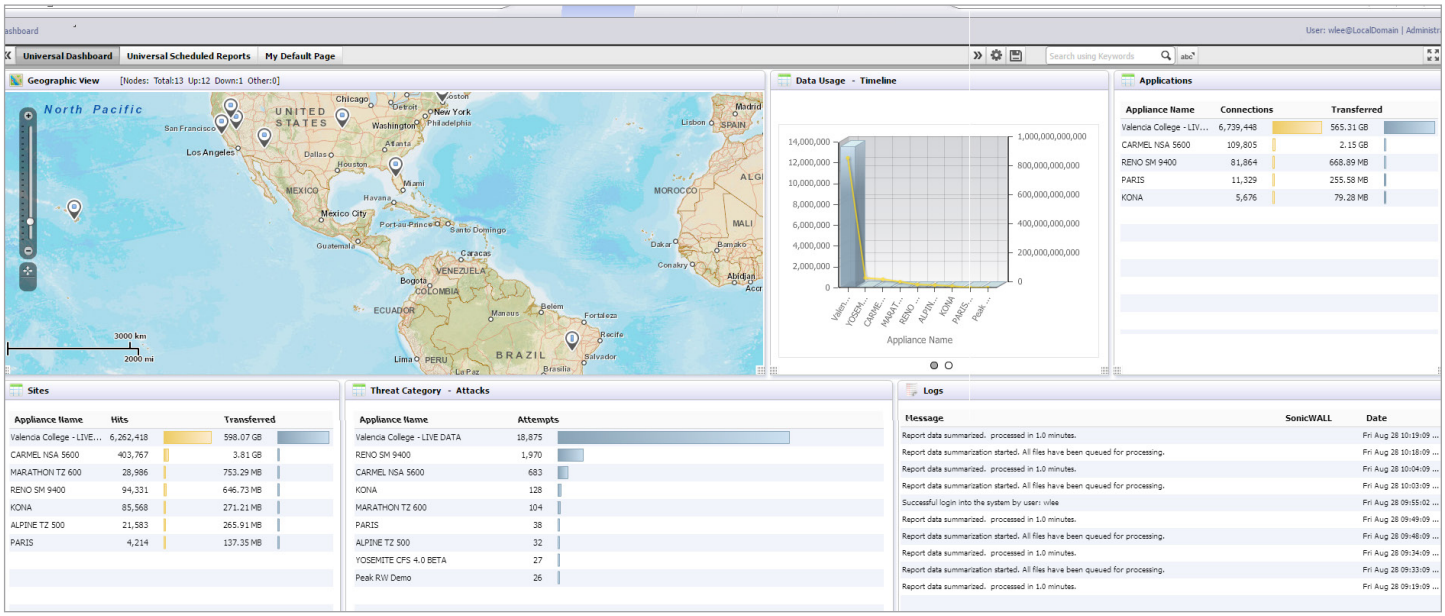
On-Premise SonicWall Global Management System Environments



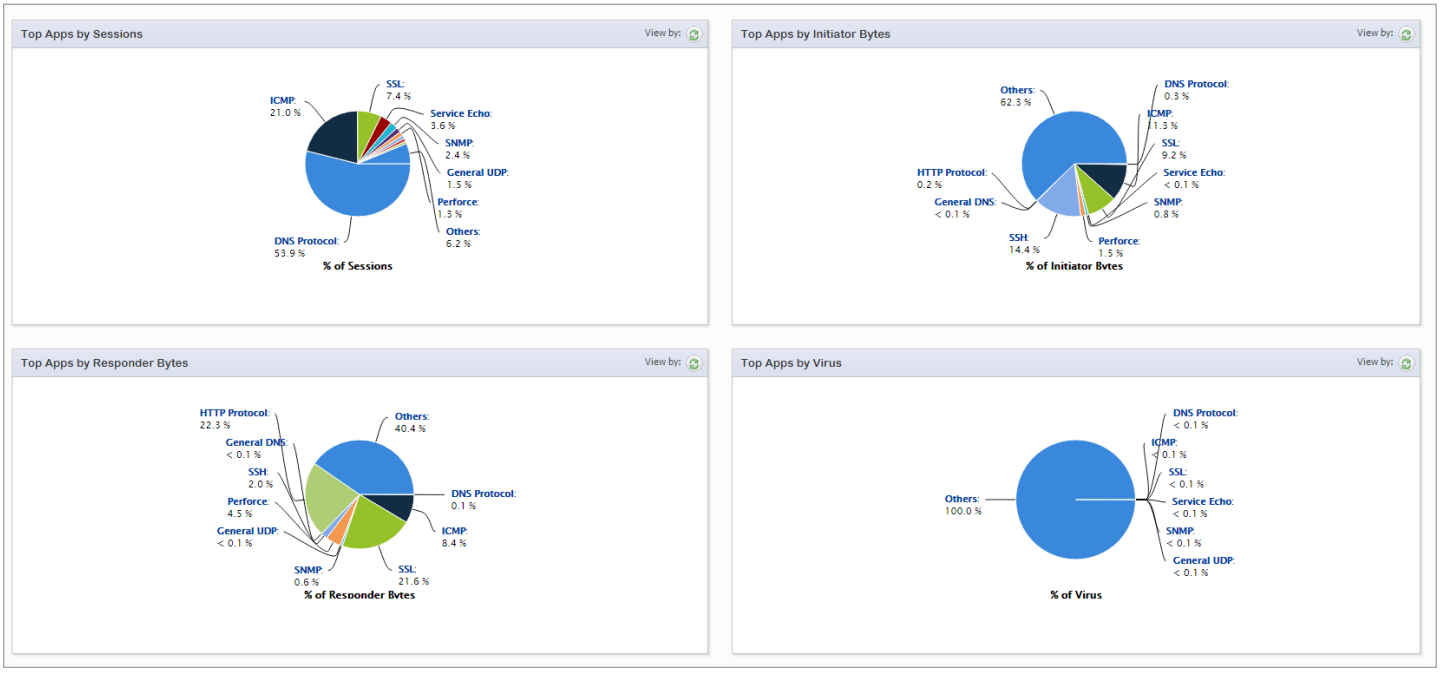
Cloud-based SonicWall Global Management System Environments

SONICWALL®

Context-sensitive dashboards display a variety of informational widgets, such as geographical maps, syslog reports, bandwidth summaries, top websites accessed, or the data that is most relevant to specific users.



Intuitive graphical reports simplify managed appliance monitoring. Easily identify traffic anomalies based on usage data for a specific timeline, initiator, responder or service. Export reports to a Microsoft® Excel® spreadsheet, portable document format (PDF) file or directly to a printer.



S = Standard
N = Not available

Feature Summary			
Solution		GMS (On-Premise)	GMS (Cloud)
	Reporting	S	S
	Policy Management	S	S
	Monitoring	S	S
Deployment Options			
	Deployable as Virtual Appliance	S	Cloud
	Deployable as Software Application	S	Cloud
	Deployable for management and reporting in an IPv6 network	S	S
Reporting			
	Comprehensive Set of Graphical Reports	S	S
	Compliance Reporting	S	N
	Customizable Reporting with Drill Down Capabilities	S	S
	Centralized Logging	S	S
	Multi-threat Reporting	S	S
	User-based Reporting	S	S
	Application Usage Reporting	S	S
	New Attack Intelligence	S	S
	Bandwidth and Services Report per Interface	S	S
	Reporting for SonicWall UTM Firewall Appliances	S	S
	Reporting for SonicWall SRA SSL VPN Appliances	S	N
	Universal Scheduled Reports	S	N
	Next-generation Reporting	Syslog and IPFIX	IPFIX
	Flexible and Granular Near Real-Time Reporting	S	S
	User-centric Reporting	S	S
	Per User Bandwidth Reporting	S	S
	More Granular Services Reporting	S	S
	Client VPN Activity Reporting	S	N
	More Detailed Summary of Services over VPN Report	S	N
	Rogue Wireless Access Point Reporting	S	N
	SRA SMB Web Application Firewall (WAF) Reporting	S	N
Management			
	Ubiquitous Access	S	S
	Alerts and Notifications	S	S
	Diagnostic Tools	S	S
	Multiple Concurrent User Sessions	S	S
	Offline Management and Scheduling	S	S
	Management of Security Firewall Policies	S	S
	Management of Security VPN Policies	S	S
	Management of Email Security Policies	S	N
	Management of Secure Remote Access/SSL VPN Policies	S	N
	Management of Value Added Security Services	S	S

S = Standard
N = Not available

Feature Summary			
Solution		GMS (On-Premise)	GMS (Cloud)
Management con't			
	Define Policy Templates at the Group Level	S	S
	Policy Replication from Device to a Group of Devices	S	S
	Policy Replication from Group Level to a Single Device	S	S
	Redundancy and High Availability	S	S
	Provisioning Management	S	S
	Scalable and Distributed Architecture	S	S
	Dynamic Management Views	S	S
	Unified License Manager	S	S
	Command Line Interface (CLI)	S	N
	Web Services Application Programming Interface (API)	S	N
	Role Based Management (Users, Groups)	S	S
	Universal Dashboard	S	N
	Backup of preference files for firewall appliances	S	S
Monitoring			
	IPFIX Data Flows in Real time	S	S
	SNMP Support	S	N
	Active Device Monitoring and Alerting	S	S
	SNMP Relay Management	S	N
	VPN and Firewall Status Monitoring	S	S
	Live Syslog Monitoring and Alerting	S	N

Minimum system requirements

Below are the minimum requirements for SonicWall GMS with respect to the operating systems, databases, drivers, hardware and SonicWall-supported appliances:

Operating system[1]

Windows Server 2016

Windows Server 2012 Standard 64-bit

Windows Server 2012 R2 Standard 64-bit (English and Japanese language versions)

Windows Server 2012 R2 Datacenter

Hardware requirements

Use the GMS Capacity Calculator to determine the hardware requirements for your deployment.

Virtual appliance requirements

Hypervisor: ESXi 6.5, 6.0 or 5.5

Use the GMS Capacity Calculator to determine the hardware requirements for your deployment.

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

Supported databases

External databases: Microsoft SQL Server 2012 and 2014

Bundled with the GMS application: MySQL

Internet browsers

Microsoft® Internet Explorer 11.0 or higher (do not use compatibility mode)

Mozilla Firefox 37.0 or higher

Google Chrome 42.0 or higher

Safari (latest version)

GMS gateway

SonicWall SuperMassive™ E10000 Series, SonicWall SuperMassive™ 9000 Series, E-Class Network Security Appliance (NSA), and NSA Series

Supported SonicWall appliances managed by GMS

SonicWall Network Security Appliances: SuperMassive E10000 and 9000 Series, E-Class NSA, NSA, and TZ Series appliances®

SonicWall Secure Mobile Access (SMA) appliances: SMA Series and E-Class SRA

SonicWall Email Security appliances

All TCP/IP and SNMP-enabled devices and applications for active monitoring

Global Management System (GMS) ordering information	
Product	**SKU**
SNWL CLOUD GMS MANAGEMENT WORKFLOW AND REPORTING LIC FOR TZ 1YR	01-SSC-3435
SNWL CLOUD GMS MANAGEMENT, WORKFLOW AND REPORTING LIC FOR NSA 1YR	01-SSC-3879
SNWL CLOUD GMS MANAGEMENT AND WORKFLOW LIC FOR TZ/SOHO 1YR	01-SSC-3664
SNWL CLOUD GMS MANAGEMENT AND WORKFLOW LIC FOR NSA 1YR	01-SSC-3665
SONICWALL GMS 5 NODE SOFTWARE LICENSE	01-SSC-7680
SONICWALL GMS 10 NODE SOFTWARE LICENSE	01-SSC-3363
SONICWALL GMS 25 NODE SOFTWARE LICENSE	01-SSC-3311
SONICWALL GMS 1 NODE SOFTWARE UPGRADE	01-SSC-7662
SONICWALL GMS 5 NODE SOFTWARE UPGRADE	01-SSC-3350
SONICWALL GMS 10 NODE SOFTWARE UPGRADE	01-SSC-7664
SONICWALL GMS 25 NODE SOFTWARE UPGRADE	01-SSC-3301
SONICWALL GMS 100 NODE SOFTWARE UPGRADE	01-SSC-3303
SONICWALL GMS 250 NODE SOFTWARE UPGRADE	01-SSC-3304
SONICWALL GMS 1000 NODE SOFTWARE UPGRADE	01-SSC-3306
SONICWALL GMS CHANGE MANAGEMENT AND WORKFLOW	01-SSC-0424
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 1 NODE (1 YR)	01-SSC-7675
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 5 NODE (1 YR)	01-SSC-6524
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 10 NODE (1 YR)	01-SSC-6514
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 25 NODE (1 YR)	01-SSC-3334
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 100 NODE (1 YR)	01-SSC-3336
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 250 NODE (1 YR)	01-SSC-3337
SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 1000 NODE (1 YR)	01-SSC-3338

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

DataSheet-SonicWallGlobalManagementSystem-US-VG-MKTG305