

# 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 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.

## HIGHLIGHTS

### Benefits:

- Establish a unified security governance, compliance and risk management security program
- Adopt a coherent and auditable approach to security orchestration, forensics, analytics and reporting
- Reduce risk and provide a fast response to security events
- Provide an enterprise-wide view of the security ecosystem
- Automate workflows and assures security operation compliance
- Operationalize firewalls at remote and branch offices in four easy steps with Zero-Touch Deployment
- Provision, manage and monitor SD-WAN deployment, connectivity and performance centrally
- Report on HIPAA, SOX, and PCI for internal and external auditors
- Deploy 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

- Move fast and drive collaboration, communication and knowledge across the shared security framework
- Make informed security policy decisions based on time-critical and consolidated threat information for higher level of security efficiency

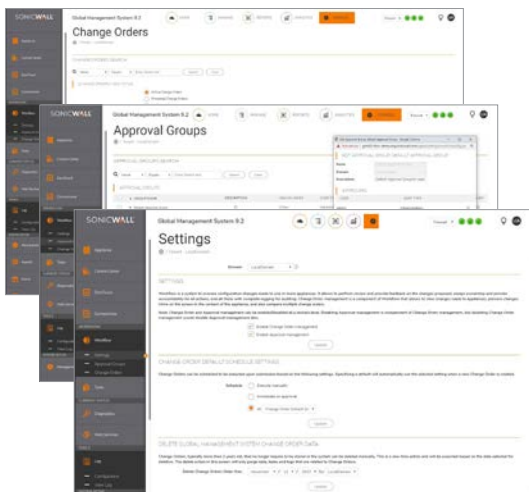
GMS provides a holistic approach to security governance, compliance and risk management

## Workflow Automation

Employing native workflow automation, GMS helps security operations conform to firewall policy change management and auditing requirements of various regulatory laws such as PCI, HIPAA and GDPR. It enables policy changes by applying a series of rigorous procedures for configuring, comparing, validating, reviewing and approving firewall policies prior to deployment.

The approval groups are flexible to comply with varying authorization and audit procedures from different types of organizations. Workflow automation programmatically deploys sanctioned security policies to improve operational efficiency, mitigate risks and eliminate errors.

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

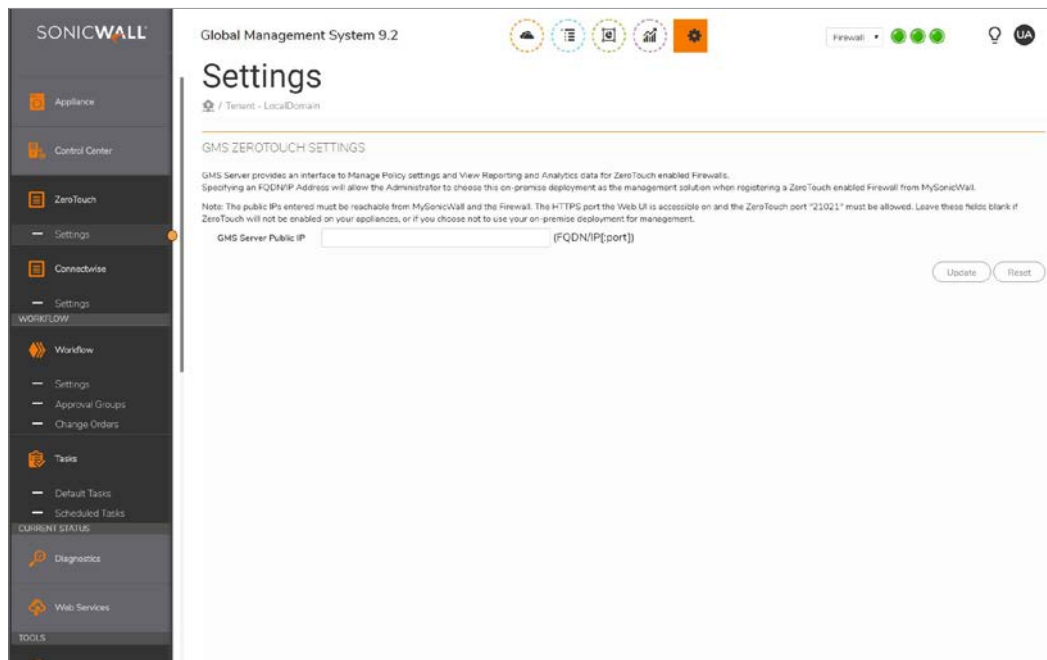


**PARTNER ENABLED SERVICES**  
Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at [www.sonicwall.com/PES](http://www.sonicwall.com/PES).

## Zero-Touch Deployment

Integrated into GMS is the Zero-Touch Deployment service, which simplifies and speeds the provisioning process for SonicWall firewalls at remote and branch office locations. The process requires minimal user intervention and is fully automated to operationalize firewalls at scale in four easy deployment steps.

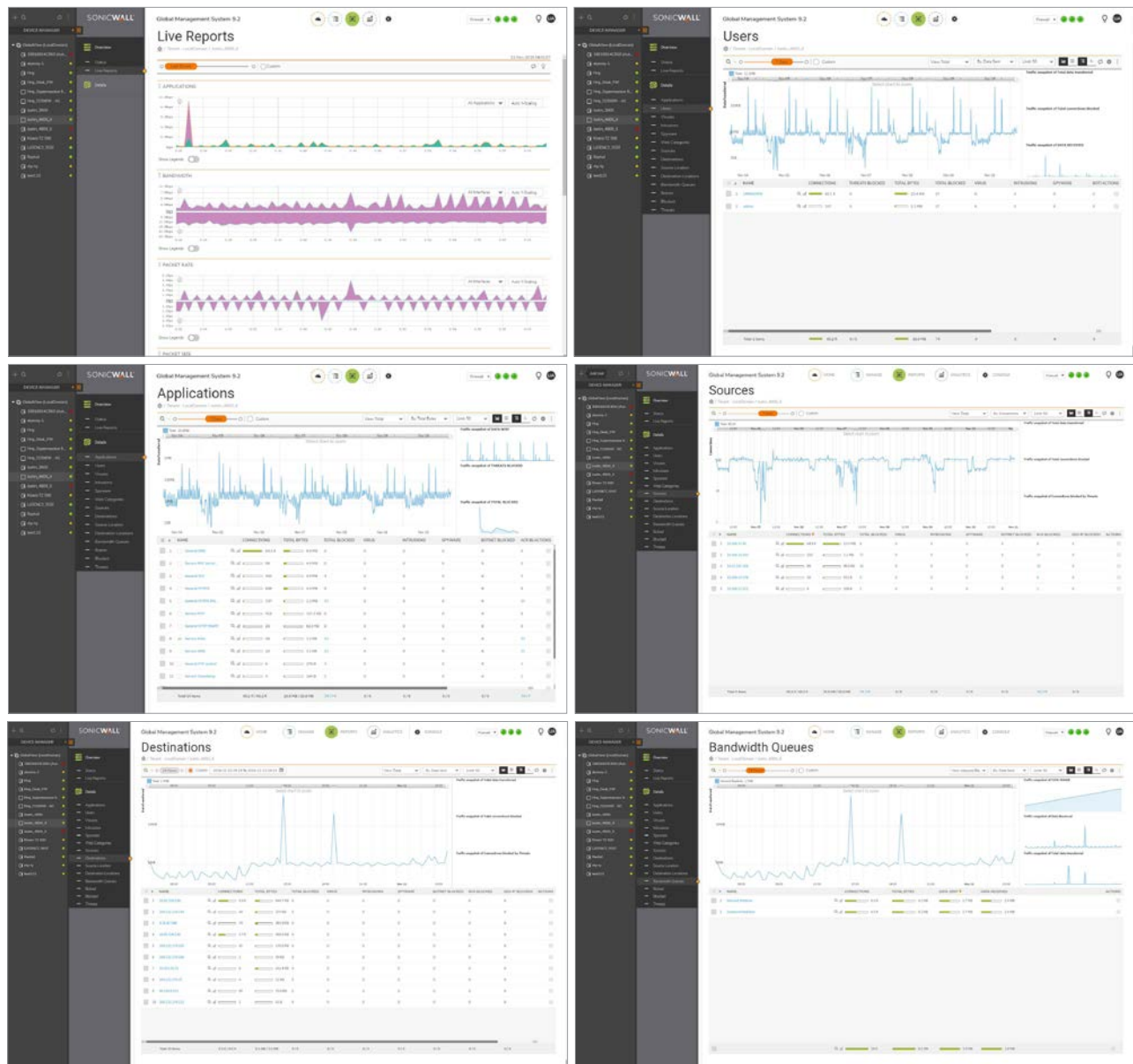
This significantly reduces the time, cost and complexity associated with installation and configuration, while security and connectivity occur instantly and automatically.



## Reporting

GMS offers a broad range of pre-defined reports as well as the flexibility to create custom reports using any combination of auditable data to acquire various use case outcomes. These outcomes include big-picture and detailed awareness of network events, user activities, threats, operational and performance issues, security efficacy, risks and security gaps, compliance readiness, and even post-mortem analysis. Every report is designed, with the collective input from many years of SonicWall customer and partner collaborations. This provides the deep granularity, scope and knowledge of syslog and IPFIX/NetFlow data needed to track, measure and run an effective network and security operation.

Intuitive graphical reports simplify managed appliance monitoring. Administrators can easily identify traffic anomalies based on usage data for a specific timeline, initiator, responder or service. They can also export reports to a Microsoft® Excel® spreadsheet, portable document format (PDF) file or directly to a printer for regular business review.



## 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.<br><br>All granular details of any changes made are historically preserved to help with compliance, audit trailing, and troubleshooting. |
| Zero-Touch Deployment                          | Simplifies and speeds the deployment and provisioning of SonicWall firewalls remotely using the cloud. Automatically pushes policies; performs firmware upgrades; and synchronizes licenses.                                                                                                                                                                                                                                                                                                                                   |
| SD-WAN Provisioning                            | Centrally provision, manage and monitor SD-WAN deployment and connectivity with ease across a distributed enterprise environment.                                                                                                                                                                                                                                                                                                                                                                                              |
| 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.                                                                                                                                                                                                                                                                                                                                      |
| Closed Network Support                         | Deploy GMS in closed environments, such as highly protected government networks. All license keysets and signature files from SonicWall backend services are packaged, encrypted and securely transferred to the local file system, where GMS can access, upload and then push required updates to all managed security appliances.                                                                                                                                                                                            |
| Intelligent Platform Monitoring (IPM)          | Monitor and alert health and status of GMS system in real-time to proactively remediate critical system conditions as they arise. This assures GMS run reliably and continuously at peak performance.                                                                                                                                                                                                                                                                                                                          |

## 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 |

## SECURITY REPORTING AND ANALYTICS (CONTINUED)

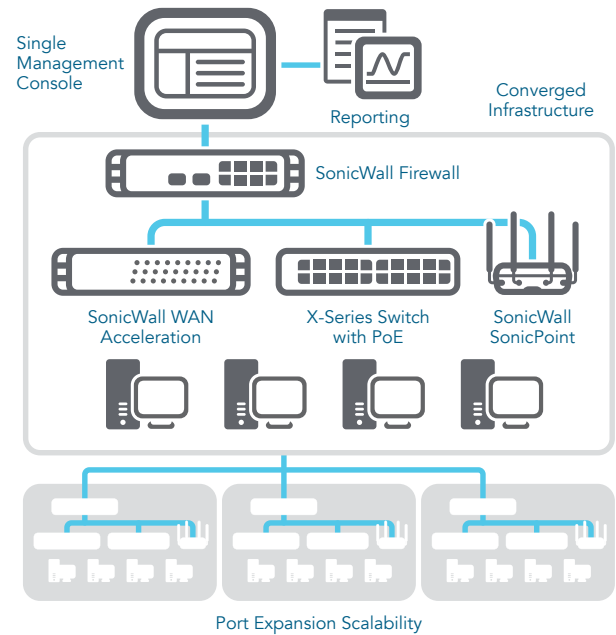
| Feature                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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: <ul style="list-style-type: none"><li>• Data Usage &gt; Initiators</li><li>• Data Usage &gt; Responders</li><li>• Data Usage &gt; Details</li><li>• User Activity &gt; Details</li><li>• Web Activity &gt; Initiators</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 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. <ul style="list-style-type: none"><li>• A Real-Time Viewer with drag and drop customization</li><li>• A Real-Time Report screen with one-click filtering</li><li>• A Top Flows Dashboard with one-click View By buttons</li><li>• A Flow Reports screen with five additional flow attribute tabs</li><li>• A Flow Analytics screen with powerful correlation and pivoting features</li><li>• A Session Viewer for deep drill-downs of individual sessions and packets.</li></ul> |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## AUTHENTICATION SECURITY

| Feature                                | Description                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account lockout                        | Account lockout policy disables a GMS user account if incorrect passwords are entered after a specified number of allowed attempts during a given period. This helps prevent attackers from guessing users' passwords and reducing the chance of successful attacks gaining unauthorized access to protected assets and data on the network. |
| Password Complexity                    | The password complexity policy sets the minimum guidelines considered important for a strong password to log in and access the GMS system.                                                                                                                                                                                                   |
| Admin access to specific address range | Customers will be able to control admin access to specific IP address ranges.                                                                                                                                                                                                                                                                |

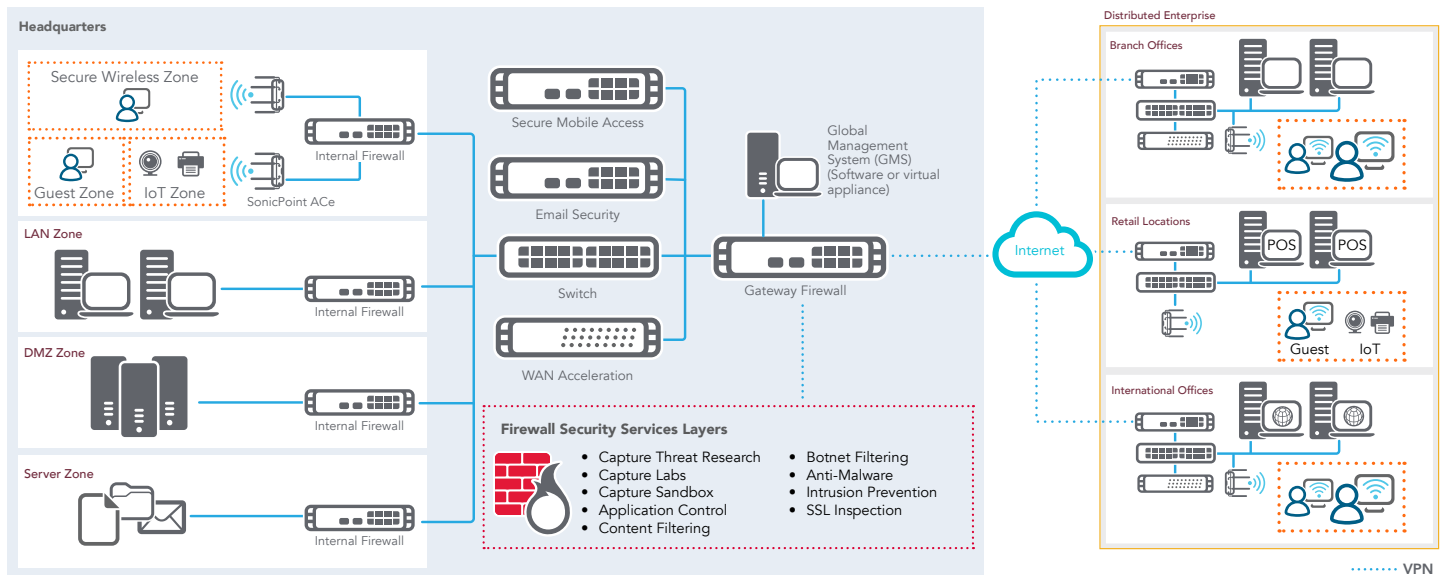
## Scalable distributed architecture

GMS is an on-premises solution, deployable as a software or a virtual appliance. At the core of GMS is a distributed architecture that facilitates limitless system availability and 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 customer-facing level, its highly interactive universal dashboards, loaded with real-time monitoring, reporting, and analytics data, help guide smart security policy decisions, and drive collaboration, communication and knowledge across the shared security framework. With an enterprise-wide view of the security environment and real-time security intelligence reaching the right people in the organization, accurate security policies and controls actions can be made towards attaining a stronger adaptive security posture.



## 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.



On-Premise SonicWall Global Management System Environments



## Feature summary

### Reporting

- Comprehensive Set of Graphical Reports
- Compliance Reporting
- Customizable Reporting with Drill Down Capabilities
- Centralized Logging
- Multi-threat Reporting
- User-centric Reporting
- Application Usage Reporting
- Granular Services Reporting
- New Attack Intelligence
- Bandwidth and Services Report per Interface
- Reporting for SonicWall Firewall Appliances
- Reporting for SonicWall SRA SSL VPN Appliances
- Universal Scheduled Reports
- Next-generation Syslog and IPFIX Reporting
- Flexible and Granular Near Real-Time Reporting
- Per User Bandwidth Reporting
- Client VPN Activity Reporting
- Detailed Summary of Services over VPN Report
- Rogue Wireless Access Point Reporting
- SRA SMB Web Application Firewall (WAF) Reporting

### Management

- Ubiquitous Access
- Alerts and Notifications
- Diagnostic Tools
- Multiple Concurrent User Sessions
- Offline Management and Scheduling
- Management of Security Firewall Policies
- Management of Security VPN Policies
- Management of Email Security Policies
- Management of Secure Remote Access/SSL VPN Policies
- Management of Value Added Security Services
- Define Policy Templates at the Group Level
- Policy Replication from Device to a Group of Devices
- Policy Replication from Group Level to a Single Device
- Redundancy and High Availability
- Provisioning Management
- Scalable and Distributed Architecture
- Dynamic Management Views
- Unified License Manager
- Command Line Interface (CLI)
- Web Services Application Programming Interface (API)
- Role Based Management (Users, Groups)
- Universal Dashboard
- Backup of preference files for firewall appliances
- SD-WAN
- Zero-Touch Deployment
- Closed network support
- Firewall Sandwich support

### Monitoring

IPFIX Data Flows in Real time  
SNMP Support  
Active Device Monitoring and Alerting  
SNMP Relay Management  
VPN and Firewall Status Monitoring  
Live Syslog Monitoring and Alerting

### Authentication Security

Account lockout  
Password Complexity  
Admin access to specific address range

## 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<sup>1</sup>

- Windows Server 2016 and 2019
- 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, 5.5, or 7.0
- Use the GMS Capacity Calculator to determine the hardware requirements for your deployment.

### VMware Hardware Compatibility Guide:

[www.vmware.com/resources/compatibility/search.php](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)

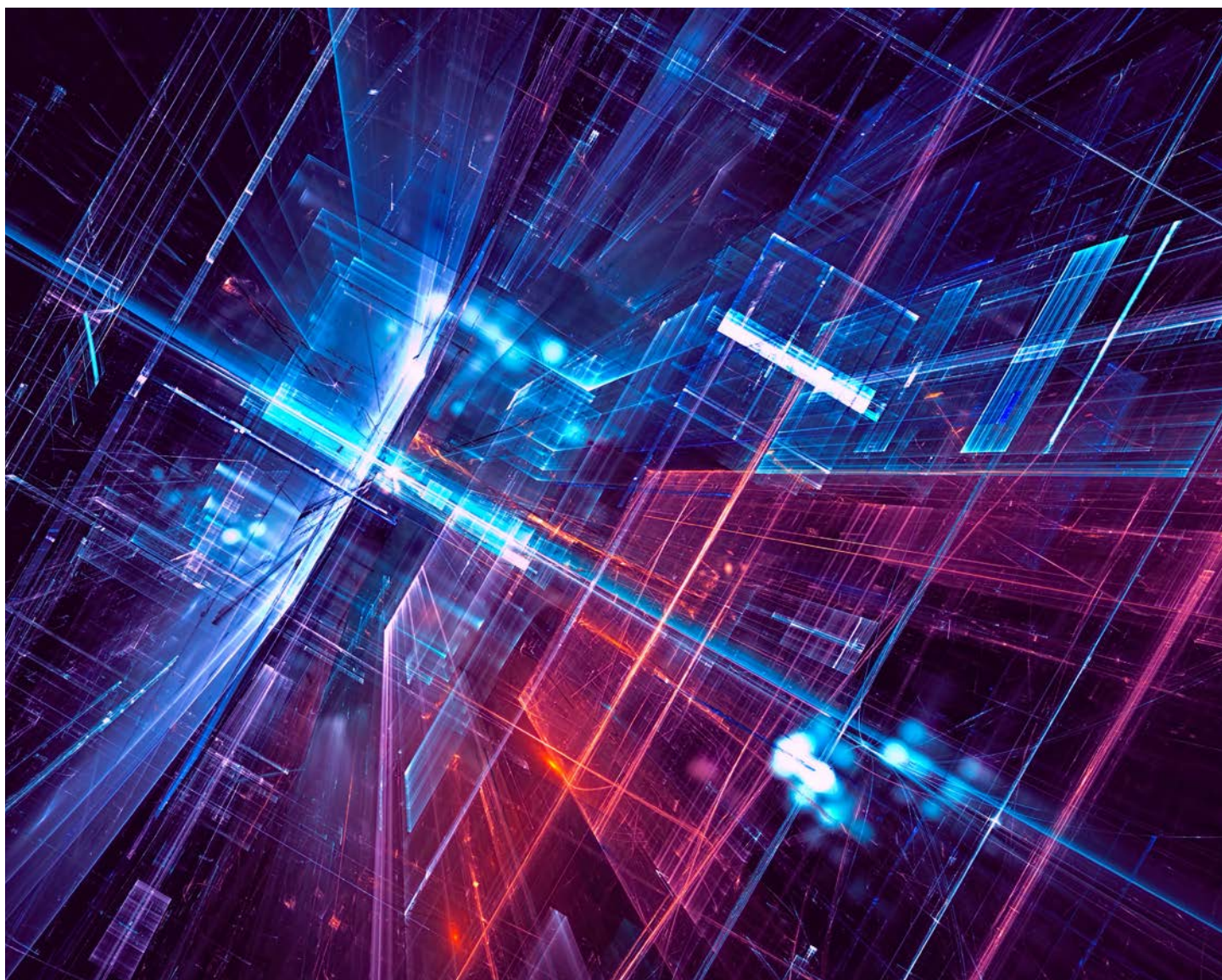
## Supported SonicWall appliances managed by GMS\*

- **SonicWall Network Security Appliances:** SuperMassive E10000 and 9000 Series, E-Class NSA, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- **SonicWall Network Security Virtual Appliances:** NSv Series
- **SonicWall Secure Mobile Access (SMA) appliances:** SMA 100 Series
- SonicWall Email Security appliances
- All TCP/IP and SNMP-enabled devices and applications for active monitoring

\*SonicWall appliances running version 7.1.1 or higher are not supported by GMS

## Global Management System (GMS) ordering information

| Product                                                          | SKU         |
|------------------------------------------------------------------|-------------|
| SONICWALL GMS 5 NODE SOFTWARE LICENSE                            | 01-SSC-3311 |
| SONICWALL GMS 10 NODE SOFTWARE LICENSE                           | 01-SSC-7662 |
| SONICWALL GMS 25 NODE SOFTWARE LICENSE                           | 01-SSC-3350 |
| SONICWALL GMS 1 NODE SOFTWARE UPGRADE                            | 01-SSC-7664 |
| SONICWALL GMS 5 NODE SOFTWARE UPGRADE                            | 01-SSC-3301 |
| SONICWALL GMS 10 NODE SOFTWARE UPGRADE                           | 01-SSC-3303 |
| SONICWALL GMS 25 NODE SOFTWARE UPGRADE                           | 01-SSC-3304 |
| SONICWALL GMS 100 NODE SOFTWARE UPGRADE                          | 01-SSC-3306 |
| SONICWALL GMS 250 NODE SOFTWARE UPGRADE                          | 01-SSC-0424 |
| SONICWALL GMS 1000 NODE SOFTWARE UPGRADE                         | 01-SSC-7675 |
| SONICWALL GMS CHANGE MANAGEMENT AND WORKFLOW                     | 01-SSC-6524 |
| SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 1 NODE (1 YR)    | 01-SSC-6514 |
| SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 5 NODE (1 YR)    | 01-SSC-3334 |
| SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 10 NODE (1 YR)   | 01-SSC-3336 |
| SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 25 NODE (1 YR)   | 01-SSC-3337 |
| SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 100 NODE (1 YR)  | 01-SSC-3338 |
| SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 250 NODE (1 YR)  | 01-SSC-6524 |
| SONICWALL GMS E-CLASS 24X7 SOFTWARE SUPPORT FOR 1000 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 SonicWall

[SonicWall](#) is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.



**SonicWall, Inc.**  
1033 McCarthy Boulevard | Milpitas, CA 95035  
Refer to our website for additional information.  
[www.sonicwall.com](http://www.sonicwall.com)

SONICWALL®

© 2024 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non-infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.