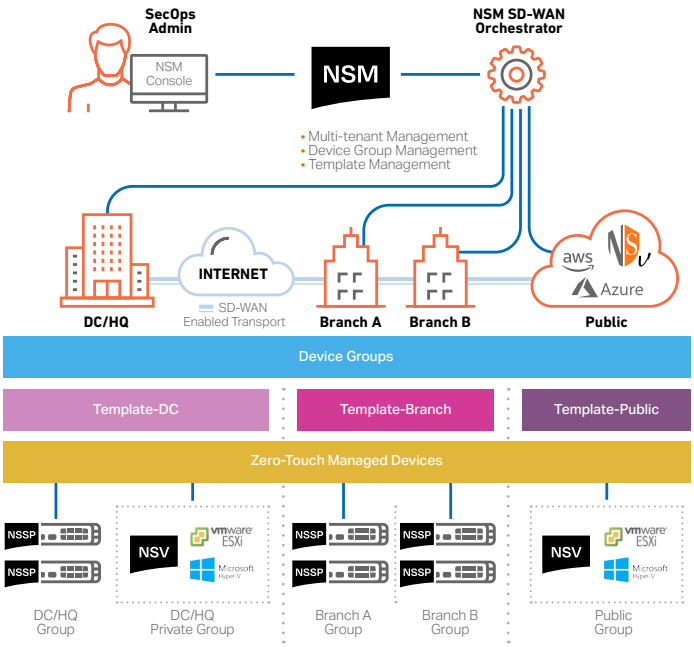
SONICWALL®

Network Security Manager On-Premise

Full control over security and compliance

Whether you're protecting a small business, a distributed enterprise, multiple businesses, or a closed network, your network security can get overwhelmed by operational disarrays, unseen risks and regulatory demands. Historically, efficient firewall management practices have mostly relied on dependable systems and operation control measures. However, frequent errors, misconfigurations and perhaps even violations of those controls remain constant challenges for well-run Security Operation Centers (SOCs).



HIGHLIGHTS

Business

- Reduced security management overhead
- Knowledge of threat landscape and security posture
- Achieve IT organization efficiency while reducing admin burnout
- Avoid costly business disruption and security incidents

Operational

- Eliminate firewall management silos
- Fast response to critical system issues, ensuring optimal network performance
- Establish consistent configuration and policy across all managed devices
- Facilitate the rapid deployment of SD-WAN networks

Security

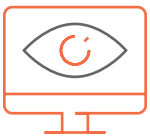
- Audit, commit, and enforce consistent security policies across all environments
- Establish consistent SD-WAN configurations across all sites
- Discover threats and respond to issues and risks quickly
- Monitor and track results of policy actions with greater clarity
- Prevent unauthorized user authentication, including insider threats

Centralized Management. Elevated Security.

www.sonicwall.com/nsm

DATASHEET

SonicWall Network Security Manager (NSM), a multi-tenant centralized firewall manager, allows you to centrally manage all firewall operations error-free by adhering to auditable workflows. Reporting and Analytics[1,2] give single-pane visibility and let you monitor and uncover threats by unifying and correlating logs across all firewalls. NSM also helps you stay compliant allowing for consistent policy enforcement across firewalls and providing detailed audit trails of every configuration change and granular reporting. The solution scales to any size organization that manages networks with hundreds of firewall devices deployed across multiple tenants or many locations. NSM does it all with less effort and time.



Be in control: Orchestrate firewall operations from one place

NSM offers you everything you need for a unified firewall management system. It empowers you with tenant-level visibility, group-based device control, and unlimited scale to manage and provision your SonicWall network security operations centrally. This includes deploying and managing all firewall devices, device groups, and tenants, synchronizing and enforcing consistent security policies, including DNS and content filtering across your environments with flexible local controls, and monitoring everything from one dynamic dashboard with detailed reports and analytics. In addition, NSM enables you to manage all of these functionalities from a single user-friendly console that can be accessed from any location using any browser-enabled device.

Multi-Tenant Management

As your firewall environment grows, you will need a firewall management system that can scale along with that environment. NSM provides complete multi-tenant management and independent policy isolation across all managed tenants. NSM allows you to deploy configuration changes across all tenants, improving operational efficiency for MSPs/MSSPs. This separation encompasses all of NSM's management features and functions that dictate the firewall operation for each tenant. You can construct every tenant to have its own set of users, groups, and roles to conduct device group management, policy orchestration, and all other administrative tasks within the boundary of the assigned tenant account.

Device Group Management

Device Group offers an effective method for creating and managing firewall devices as groups or hierarchical groups and committing and deploying configuration templates on groups of firewalls. These allow you to synchronize and enforce policies and objects and set requirements across any selected firewall groups consistently and reliably. All approved policy changes in the template are applied automatically to all device groups linked to that template. Grouping of devices can be defined granularly based on any characteristics such as network type, location, business unit, organizational structure, or a combination of such attributes for ease of management, identification, and association.

Template Management, Commit and Deploy

NSM simplified workflows allow you to easily and quickly design, validate, audit, approve, and commit configuration templates for managing one or hundreds of firewall devices across many geolocations. Templates with various firewall policies, settings, and related objects are defined independently of the device. NSM uses these templates to centrally and automatically push to devices or device groups that require similar configurations.

Templates combined with the Template Variables allow you to centrally deploy and provision hundreds of remote firewalls and establish consistent configuration while preserving unique device-specific values per device like interface IPs, DNS Configuration, Firewall Hostname, etc. Distributed enterprises can effortlessly onboard and secure new branch and remote sites using a single template, eliminating separate manual setups for each device at every location.

SD-WAN Orchestration and Monitoring

NSM simplifies the deployment of enterprise-wide SD-WAN networks via an intuitive self-guided workflow. It centrally establishes and enforces application-based traffic and other traffic steering configurations across and between hundreds of sites, such as branch offices and retail stores. Also, NSM lets you monitor the health and performance of your whole SD-WAN environment to ensure consistent configurations, drive optimal application performance, and empower network infrastructure teams to troubleshoot and resolve issues quickly.

VPN Orchestration and Monitoring

NSM simplifies VPN configurations and policies with an easy, wizard-based, step-by-step setup process enabling system administrators to establish site-to-site connectivity and communication quickly and error-free using a repeatable self-guided workflow. In addition, VPN Monitoring helps keep an active pulse on your VPNs, giving you complete visibility into your entire VPN environment's activities, health, and performance. Network admins can leverage this information to monitor connection status, data transferred, and bandwidth consumed over those VPN tunnels. Alerts allow admins to proactively maintain the integrity of VPN connections, ensuring continuous connectivity between sites.

Be more effective: Work smarter and take security actions faster with less effort

NSM is a productivity management tool that enables you to work smarter and take security actions faster with less effort. Its design is guided by business processes and grounded on the principle of simplifying and, in some cases, automating workflows to achieve better security coordination. It also helps reduce the complexity, time, and overhead of everyday security operations and administration tasks.

Effortless Zero-Touch Deployment

Integrated into NSM is the Zero-Touch Deployment service that enables you to effortlessly deploy and operationalize SonicWall firewalls, switches, and access points at remote and branch office locations. The entire process requires minimal user intervention and is fully automated. Zero-touch-enabled devices are shipped directly to installation sites. Once registered and wired to the network, all connected devices are instantly operational, with security and connectivity occurring seamlessly. Once communication links are established with NSM, pre-provisioned device templates are automatically pushed to all connected devices. This eliminates the time, cost, and complexity of traditional on-site onboarding processes.

Error-free Change Management

NSM provides immediate access to powerful automated workflows that conform with firewall policy change management and auditing requirements of SOCs. It enables error-free policy changes by applying a series of rigorous procedures. These include configuration comparison, validation, and authorization before deployment. The approval groups are flexible in complying with internal audit procedures from various functional teams. NSM enables you to improve operational efficiency, mitigate risks, and eliminate misconfigurations through the compulsory approval workflow process.

Management Automation with RESTful API

NSM RESTful APIs give your skilled security operators a standard approach to managing NSM-specific features programmatically without a management web interface. They facilitate interoperability between NSM and third-party management consoles to increase the efficiency of your internal security team. The API services can automate firewall operations for any managed device. These include typical day-to-day tasks such as device group and tenant management, audit configurations, performing system health checks, and more.

Be more aware: Investigate hidden risks with active monitoring, reporting and analytics[1,2]

The NSM interactive dashboard provides real-time monitoring, reporting, and analytics data. The information helps you troubleshoot problems, investigate risks, and take smart security policy actions for a more adaptive security posture. With real-time alerts, admins can act precisely and quickly to keep their organizations running optimally, helping them avoid costly business disruptions and security incidents.

See Everything Everywhere

NSM with Reporting and Analytics,[1,2] gives you up to 365 days, based on license type, of continuous visibility of your

SONICWALL

entire SonicWall security ecosystem at the tenant, group, or device level. It provides static and near-real-time analysis of all network traffic and data communication through the firewall ecosystem. All log data is automatically recorded, aggregated, contextualized, and presented in a meaningful, actionable, and easily consumable way. You can then discover, interpret, prioritize, and take appropriate defensive and corrective actions based on data-driven insight and situational awareness. Scheduled reporting allows you to customize your reports with any combination of traffic data. It presents up to 365 days of recorded logs at the device, device group, or tenant level for historical analysis, anomaly detection, security gaps discovery, and more. This will help you track, measure, and run an effective network and security operation.

Understand Your Risk

With added drill-down and pivoting capabilities, you can further investigate and correlate data to examine and discover hidden threats and issues with better accuracy and confidence. Using a mix of historical reporting, user- and application-based analytics, and endpoint visibility, you can thoroughly analyze various patterns and trends associated with ingress/egress traffic, application usage, user and device access, threat actions, and more. You will gain situational awareness, valuable insight, and knowledge to uncover security risks and orchestrate remediation while monitoring and tracking the results to promote and drive consistent security enforcement across your environment.

Optimize Workforce Productivity

User Analytics[1,2] gives a broad and transparent view of your workforce's web application and internet usage activities. Drilldown capabilities enable analysts to easily and quickly pivot and investigate data points of interest at the user level and establish evidence-backed policy-controlled measures for risky users and applications as they unfold in the discovery process. In addition, Productivity Reports[1,2] provide insights into employees' internet utilization and behavior over a specified period. It generates powerful snapshots and drill-down reports that classify users' web activities into productivity groups such as productive, unproductive, acceptable, unacceptable, or custom-defined groups, helping organizations better understand and control internet usage.

Flexible Deployment

You can deploy NSM On-Premises in Microsoft Azure public cloud or as a virtual appliance in a private cloud on VMWare, Microsoft Hyper-V, or KVM for total system control and compliance. These deployment options give you all the operational and economic benefits of virtualization, including system scalability and agility, speed of system provisioning, simple management, and cost reduction.

Security Capabilities

Federal, public, healthcare, pharmaceutical, and other large organizations often deploy closed networks to maintain the privacy and isolation of their mission-critical applications and most sensitive information systems, such as classified document systems, SCADA, and research facilities. NSM supports closed network environments by offering admins an offline way to onboard, license, patch, and upgrade the NSM system and firewalls under its management without contacting SonicWall License Manager and MySonicWall. For added security, NSM enforces several account access control measures to prevent unauthorized access to the NSM management interface. It grants specific administrative controls according to the user's roles and triggers account lockout based on a specified number of failed login attempts. Also, user access is only permitted when logging in from a selected list of allowed source IP addresses and secured via two-factor authentication (2FA).

Cloud Secure Edge

Cloud Secure Edge (CSE) by SonicWall is a cloud-based security solution that provides secure access to applications and data for remote and hybrid workforces. With the Cloud Secure Edge Connector integration, NSM users can access our Cloud Secure Edge technology, which offers secure private access for remote users with Zero Trust capabilities. Cloud Secure Edge integrates secure web gateways, zero-trust network access, and advanced threat protection to safeguard users and devices, regardless of location. Any organization can deploy a Cloud Secure Edge Connector starting SonicOS 7.1.2 to establish a connection to the internet and cloud clusters hosted by corporate resources. The Connector then establishes secure tunnels to the Access Tiers on the Global Edge Network.

SONICWALL

Licensing and Packaging

Licensing	
Features	**Advanced Protection**
Advanced Reporting	7 Days
Advanced Analytics	7 Days

Management	
Feature	**NSM On-Premise Management**
Tenant	✓
Device Inventory	✓
Push policy at the group level	✓
Device Group	✓
Templates	✓
Commit and Deploy (Workflow Automation)	✓
Configuration Audit	✓
Config Diff	✓
Auto Sync Configurations	✓
Workflow Automation	✓
API	✓
Zero-Touch Deployment	✓
SD-WAN Orchestration and Monitoring	✓
VPN Orchestration and Monitoring	✓
Task scheduling	✓
Backup/Restore	✓
Firmware upgrades	✓
Access Point and Switch Management from Firewall	✓
Advanced DNS Filtering*	✓
Network Access Control	✓
Reputation-based content filtering*	✓
Integration with Cloud Secure Edge Connector	✓
Firewall Migration App	✓
One-Click Management	✓
Offline Firewall View	✓

*Must have NSM On-Prem Base license to add on reporting and analytics license

SONICWALL

Licensing and Packaging cont'd

Reporting	
Feature	**NSM On-Premise Advanced Reporting and Analytics for 7 and 365 days[2]**
Group/Tenant Level Dashboard	✓
Capture ATP (Device Level)	✓
Capture Threat Assessment (Device Level)	✓
Productivity Reports4	✓
VPN Reports	✓
Custom Reports	✓
Schedule Report	✓
(Flow, CTA and Management)	✓
Firewall Up-Time Summary Report	✓
Attack Reports	✓

Analytics	
Feature	**NSM On-Premise Advanced Reporting and Analytics for 7 and 365 days[2]**
User-based analytic	✓
Application analytics	✓
Network forensic and threat hunting using drill-down and pivots	✓

SONICWALL

Feature Summary

Management

- Integration with Cloud Secure Edge Connector
- Network Access Control (NAC)
- Tenant and Device Group level management
- Configuration templates
- Device grouping
- Device configuration conversion into template
- Commit and deploy the wizard
- Firewall Migration Capability
- Configuration audits
- Config – Diff
- Offline Management and Scheduling
- Management of Security firewall policies
- Management of Security VPN policies
- Administration of SD-WAN
- Synchronization of Security Services
- High Availability
- Configuration backups
- RESTful API
- Multi-device firmware upgrade
- Automatic Firmware Upgrades
- Role-based administration

Monitoring[1,2]

- Device health and status
- License and support status
- Network/Threat summary
- Alert and notification center
- Offline Device Monitoring
- Event logs
- Topology view
- Local Firewall Change Alerts

Analytics[1,2]

- User-based activities
- Application usage
- Cross-product visibility with Capture Client
- Real-Time Dynamic Visualization
- Drill-down and pivoting capabilities

Reporting[1,2]

- Scheduled PDF reports - Tenant/ Group/Device level
- Customizable reports
- Centralized logging
- Multi-Threat report
- User-Centric report
- Application Usage report
- Bandwidth and Services reports
- Per User Bandwidth Reporting
- Productivity Reports
- Firewall Up-Time Summary Report
- Attack Reports
- VPN Usage Reports

Security

- Closed Network support
- Account lockout
- Account access control
- 2FA support
- Authenticator App TFA support

*Supported on SonicOS 7.1 and above

SONICWALL

NSM On-Premises System Requirement

- Hypervisor: ESXi 7.0, 8.0, 2019, 2022, Microsoft Hyper-V, and KVM
- Public Cloud: Azure
- Minimum computing resources: 4Core vCPUs, 16 GB RAM Memory, 250GB Storage

Managed Devices[5]

- NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp
- 12000 Series, SuperMassive 9000 Series, NSa Series, TZ Series, TZ80, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NSv Series
- Support for SonicWave includes Wi-Fi[6] enabled access points[4]
- SonicWall Switch[4]

[1] NSM On-Premise 3.0 natively supports reporting and analytics. It now has feature parity with NSM SaaS.
[2] On-Premise does not support reporting and analytics for Gen6/Gen6.5 products.
[3] Requires AGSS/CGSS license enabled on Generation 6/6.5 Firewalls
[4] Managed only when connected to an NSM managed Firewall.
[5] All products that are end-of-life are not supported on NSM.
[6] Gen 6 Hardware is not supported for NSM On-Premise Reporting and Analytics.

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