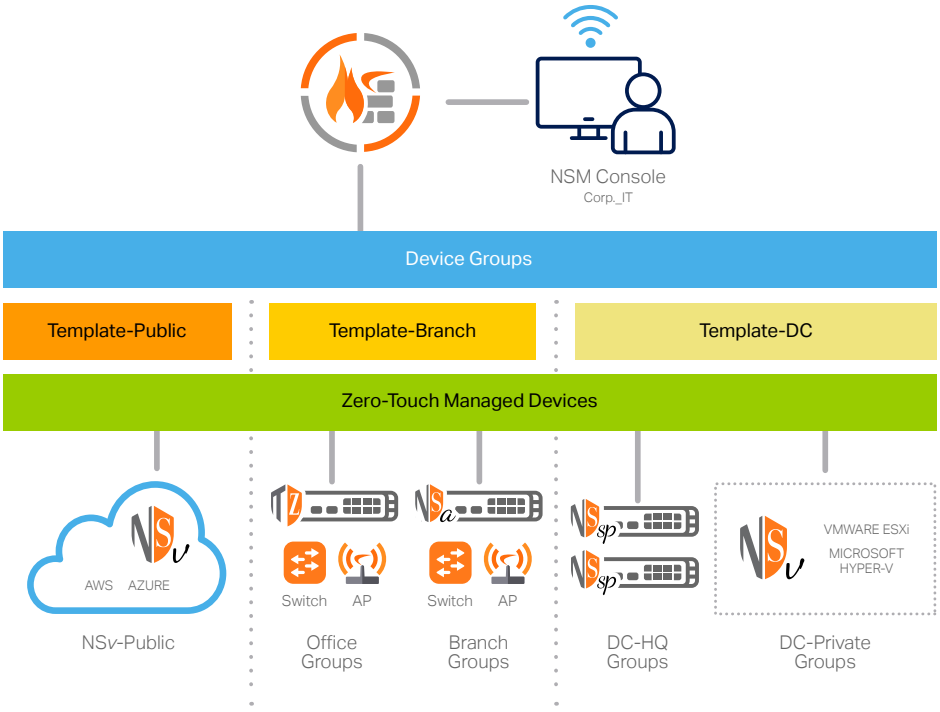
SONICWALL

Network Security Manager

Unified firewall management system that scales for any environment

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 to be constant challenges for well-run Security Operation Centers (SOCs).

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 lets you monitor and uncover threats by unifying and correlating logs across all firewalls. NSM also helps you stay compliant as it provides full audit trails of every configuration change and granular reporting. The solution scales to any size organization that manages networks with up to thousands of firewall devices deployed across many locations. NSM does it all with less effort and time.



Benefits:

Business

- Reduced security management overhead
- Knowledge of threat landscape and security posture
- Lowered CAPEX w/ SaaS

Operational

- Eliminate firewall management silos
- Onboard any number of firewalls remotely with ease
- Visibility into all security operations

Security

- Eliminate single point-of-failure with High Availability
- Audit, commit and enforce consistent security policies across all environments
- Hunt and respond to issues and risks quickly
- Make informed security policy decisions
- Prevent unauthorized access including insider threats

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 centrally manage and provision your SonicWall network security operations. These include deploying and managing all firewall devices, device groups and tenants, synchronizing and enforcing consistent security policies across your environments with flexible local controls and monitoring everything from one dynamic dashboard with detailed reports and analytics. NSM enables you to manage all 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 control isolation across all managed tenants. 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 you 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, objects and setting 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 thousands of firewall devices across many geo-locations. Templates with various firewall policies, settings and related objects are defined independently of the device. These are used by NSM to centrally and automatically push to devices or device groups that require similar configurations.

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. Also, it helps reduce the complexity, time and overhead of performing every-day security operations and administration tasks.

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

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 to comply with internal audit procedures from various functional teams. NSM enables you to improve operational efficiency, mitigate risks and eliminate misconfigurations with the compulsory approval workflow process.

Management Automation with RESTful API
NSM RESTful APIs gives your skilled security operators a standard approach to managing NSM specific features programmatically without a management web interface. It facilitates interoperability between NSM and 3rd-party management consoles to increases the efficiency of your internal security team. The API services can automate firewall operations for any managed devices. 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]

NSM interactive dashboard provides real-time monitoring and reporting and analytics data. The information helps you troubleshoot problems, investigate risks and take smart security policy actions for a more adaptive security posture.

See Everything Everywhere
NSM, combined with Analytics[1,2] gives you up to 7 days of continuous 360° visibility of your entire SonicWall security ecosystem at the tenant, group or device level. It provides a static and near-real-time analysis of all network traffic and data communication that passes 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 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 situation-awareness and valuable insight and knowledge to not only uncover security risks, but also orchestrate remediation while monitoring and tracking the results to promote and drive consistent security enforcement across your environment.

Flexible deployment
Customers can deploy NSM in various ways to best suit their operation, regulatory and budgetary requirements.

For a maintenance-free experience, NSM is available as a SaaS offering hosted by SonicWall and accessible over the internet. With NSM SaaS, you can scale on-demand while lowering your operational cost. There are no hardware and software to deploy, maintenance schedule, software customization, configurations or upgrades, downtime, depreciation and retirement costs. All of these expenses are removed and replaced with one low, predictable yearly subscription cost.

For total system control and compliance, you can deploy NSM in Microsoft Azure public cloud or as a virtual appliance in a private cloud on VMWare, Microsoft Hyper-V or KVM. These 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 providing admins with 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 specified list of allowed source IP addresses and secured via two-factor authentication (2FA)[3].

Feature Summary

Management

- Tenant and Device Group level management
- Configuration templates
- Device grouping
- Device configuration conversion into template
- Commit and deploy wizard
- Configuration audits
- Config – Diff
- Offline Management and Scheduling
- Management of Security Firewall Policies
- Management of Security VPN Policies
- Management of SD-WAN
- Management of Security Services
- High Availability
- Configuration backups
- RESTful API
- Multi-device firmware upgrade
- Role-based administration
- Access Point and Switch Management
- Intelligent Platform Monitoring (IPM)[3]
- Multi-device certificate management

Monitoring [1,2]

- Device health and status
- License and support status
- Network/Threat summary
- Alert and notification center
- Event logs
- Topology view

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

Security

- Closed Network support
- Account lockout
- Account access control
- 2FA support[3]
- Authenticator App TFA support

Licensing and Packaging

Feature	NSM SaaS Essential	NSM SaaS Advanced	NSM On-Prem
Management	Yes	Yes	Yes
Reporting	7 days	365 days	No[2]
Analytics	No	Yes	No[2]

Product	SKU
NSM ESSENTIAL FOR SOHO 250 1YR	02-SSC-5219
NSM ADVANCED FOR SOHO 250 1YR	02-SSC-5213
NSM ESSENTIAL FOR TZ 270 1YR	02-SSC-7049
NSM ADVANCED FOR TZ 270 1YR	02-SSC-6977
NSM ESSENTIAL FOR TZ 370 1YR	02-SSC-7067
NSM ADVANCED FOR TZ 370 1YR	02-SSC-6989
NSM ESSENTIAL FOR TZ 470 1YR	02-SSC-7001
NSM ADVANCED FOR TZ 470 1YR	02-SSC-7073
NSM ESSENTIAL FOR TZ 570 1YR	02-SSC-4975
NSM ADVANCED FOR TZ 570 1YR	02-SSC-4963
NSM ESSENTIAL FOR TZ 670 1YR	02-SSC-5011
NSM ADVANCED FOR TZ 670 1YR	02-SSC-4999
NSM ESSENTIAL FOR NSa 2700 1YR	02-SSC-7166

Product	SKU
NSM ADVANCED FOR NSa 2700 1YR	02-SSC-7160
NSM ESSENTIAL FOR NSa 3600/NSa 3650 1YR	02-SSC-5299
NSM ADVANCED FOR NSa 3600/NSa 3650 1YR	02-SSC-5293
NSM ESSENTIAL FOR NSa 4600/NSa 4650 1YR	02-SSC-5325
NSM ADVANCED FOR NSa 4600/NSa 4650 1YR	02-SSC-5319
NSM ESSENTIAL FOR NSa 5600/NSa 5650 1YR	02-SSC-5347
NSM ADVANCED FOR NSa 5600/NSa 5650 1YR	02-SSC-5341
NSM ESSENTIAL FOR NSa 6600/NSa 6650 1YR	02-SSC-5365
NSM ADVANCED FOR NSa 6600/NSa 6650 1YR	02-SSC-5359
NSM MANAGEMENT ON-PREM BASE LICENSE - 5 NODES 1YR	02-SSC-6873
NSM ON-PREM MANAGEMENT - 1 NODE ADD-ON 1YR	02-SSC-6874
NSM ON-PREM MANAGEMENT - 10 NODE ADD-ON 1YR	02-SSC-6875
NSM ON-PREM MANAGEMENT - 25 NODE ADD-ON 1YR	02-SSC-6876
NSM ON-PREM MANAGEMENT - 100 NODE ADD-ON 1YR	02-SSC-6877
NSM ON-PREM MANAGEMENT - 250 NODE ADD-ON 1YR	02-SSC-6878

Multi-year SKUs and support contracts are also available. For a complete list, please contact your preferred reseller or SonicWall Sales.

[1] NSM SaaS includes reporting and analytics features.
[2] NSM On-Prem requires a separate SonicWall Analytics On-Prem install and license for the reporting and analytics features.
[3] Available only on NSM On-Prem.
[4] 365 days of Reporting and 30 days of Analytics are not supported.

Internet Browsers

- Microsoft® Internet Explorer 11.0 or higher and latest version of Microsoft Edge, Mozilla Firefox, Google Chrome and Safari

NSM On-Prem System Requirement

- Hypervisor: ESXi 7.0, 6.7, 6.5 and Hyper-V 2016, 2019
- Minimum computing resources: 4 vCPUs, 16GB Memory, 250GB Storage

Managed Devices

- NSsp 15700, NSsp 12000 Series[4], SuperMassive 9000 Series[4], E-Class NSA, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- Generation 5 appliances and firmware including non-wireless SOHO devices running SonicOS 5.9 are not supported.
- SonicWall Network Security Virtual Appliances: NSv Series
- SonicWall SonicWave, SonicPoint
- SonicWall Switch

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-NSM-US-VG-3836