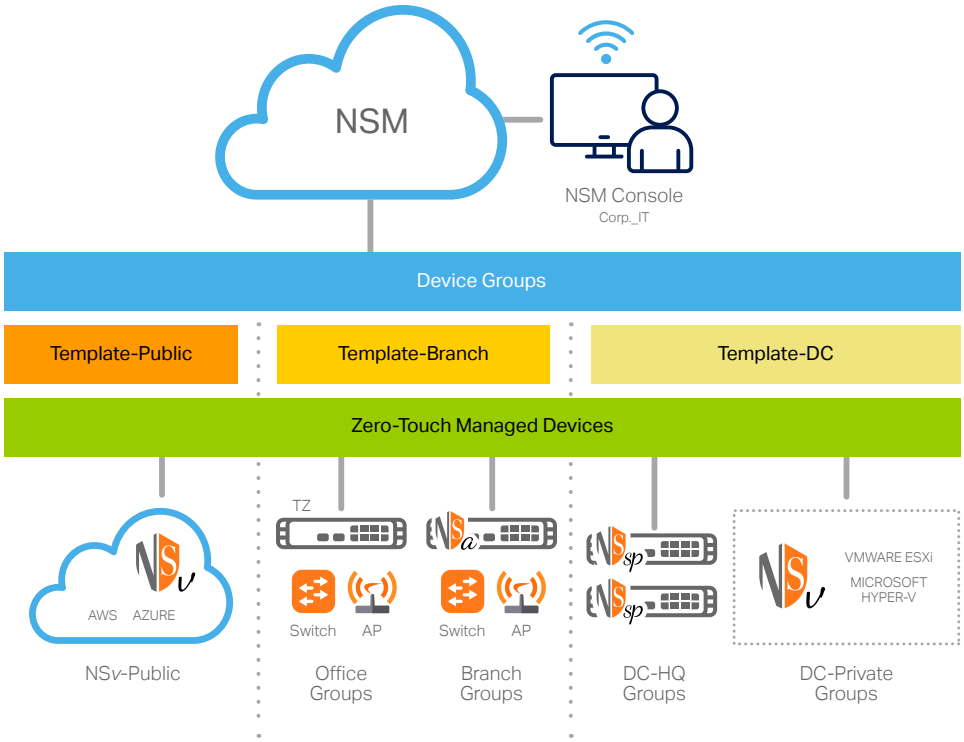
SONICWALL

Network Security Manager

Unified firewall management system that scales for any environment

Whether you're protecting a small business, a distributed enterprise, or multiple businesses, your network security can get overwhelmed by operational disarrays, unseen risks and regulatory demands. Historically, good firewall management practices have mostly relied upon robust and dependable system and operational control measures. However, common 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. Its native analytic engine gives 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 trail of every configuration changes and granular reporting. NSM scales to any size organization managing networks with up to thousands of firewall devices deployed across many locations — and 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

- No HW/SW to deploy
- Eliminate firewall management silos
- Onboard any number of firewalls remotely with ease
- Visibility into all security operations

Security

- Audit, commit and enforce consistent security policies across all environments
- Hunt and respond to issues and risks quickly
- Make informed security policy decisions

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. This includes 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 do all this from a single user-friendly cloud native console that can be accessed from any location using any browser-enabled device.

Multi-Tenant Management
As your firewall environment grows with complex multi-cloud and multi-location tenants that have differing security needs for each network segment, 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 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 group or hierarchical groups and committing and deploying configuration templates on groups of firewalls. This allows you to synchronize and enforce common policies, objects, and/or setting requirements across any selected firewall groups in a consistent and reliable manner. All approved policy changes in the template are automatically applied to all device group linked to that template. Grouping of devices can be granularly defined based on any characteristics such as network type, location, business unit, organizational structure, or a combination of relative 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 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 independent of the device and are used by NSM to centrally and automatically push to devices or device groups that requires 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, while reducing 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 which 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 unpacked, registered, wired to the network, and powered, 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 zero-touch enabled devices. This eliminates 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 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. NSM programmatically deploys fully validated and audited security policies to improve operational efficiency, mitigate risks and eliminate misconfigurations and human errors.

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 are used to automate firewall operations for any managed devices. This includes common day-to-day tasks such tenant, 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

NSM interactive dashboard is loaded with real-time monitoring, reporting, and analytics data to help troubleshoot problems, investigate risks and guide smart security policy decisions and policy actions for a stronger adaptive security posture.

See Everything Everywhere
NSM reporting, analytics and risk monitoring dashboard 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 static and near-real-time analysis of all network traffic and data communication

that pass through the firewall ecosystem. All log data is automatically recorded, aggregated, contextualized and presented in a meaningful, actionable and easily consumable way that lets you discover, interpret, prioritize and take appropriate defensive and corrective actions based on data-driven insight and situational awareness. Scheduled reporting allows you to fully customize your reports with any combination of auditable 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 fully 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.

Feature Summary

Management

- Tenant and Device Group level management
- Configuration templates
- Device grouping
- 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 Value-Added Security Services
- Redundancy and High Availability
- Backup of Preference Files for Firewall Appliance
- RESTful API
- Firmware upgrade
- Role-based administration
- Access Point and Switch Management

Monitoring

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

Analytics

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

Reporting

- 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

Licensing and Packaging

Features	Essential	Advanced
Manage hundreds of devices per tenant	Yes	Yes
Multi-tenant Management	Yes	Yes
Device Inventory	Yes	Yes
Push policy at the group level	Yes	Yes
Device Group	Yes	Yes
Templates	Yes	Yes
Commit and Deploy	Yes	Yes
Configuration Audit	Yes	Yes
Config Diff	Yes	Yes
Workflow Automation	Yes	Yes
API	Yes	Yes
Zero-Touch Deployment	Yes	Yes
Task scheduling	Yes	Yes

Features	Essential	Advanced
Backup/Restore	Yes	Yes
Firmware upgrades	Yes	Yes
Access Point and Switch management	Yes	Yes
Days of reporting data	7 days	365 days
Group/Tenant Level Dashboard	Yes	Yes
Capture ATP (Device Level)	Yes	Yes
Capture Threat Assessment (Device Level)	Yes	Yes
Group Level Visibility and Reporting	Yes	Yes
Scheduled reports (Device Group level)	Yes	Yes
User-based analytic	No	Yes
Application analytics	No	Yes
Threat analytics	No	Yes
Drill-down and pivots	No	Yes

Product	SKU
NSM ESSENTIAL FOR SOHO 250 1YR	02-SSC-5219
NSM ADVANCED FOR SOHO 250 1YR	02-SSC-5213
NSM ESSENTIAL FOR TZ 350 1YR	02-SSC-5239
NSM ADVANCED FOR TZ 350 1YR	02-SSC-5231
NSM ESSENTIAL FOR TZ 400 1YR	02-SSC-5263
NSM ADVANCED FOR TZ 400 1YR	02-SSC-5257
NSM ESSENTIAL FOR TZ 500 1YR	02-SSC-5183
NSM ADVANCED FOR TZ 500 1YR	02-SSC-5177
NSM ESSENTIAL FOR TZ 570 1YR	02-SSC-4975
NSM ADVANCED FOR TZ 570 1YR	02-SSC-4963
NSM ESSENTIAL FOR TZ 600 1YR	02-SSC-5201
NSM ADVANCED FOR TZ 600 1YR	02-SSC-5195
NSM ESSENTIAL FOR TZ 670 1YR	02-SSC-5011
NSM ADVANCED FOR TZ 670 1YR	02-SSC-4999
NSM ESSENTIAL FOR NS*a* 2600/NS*a* 2650 1YR	02-SSC-5281
NSM ADVANCED FOR NS*a* 2600/NS*a* 2650 1YR	02-SSC-5275
NSM ESSENTIAL FOR NS*a* 3600/NS*a* 3650 1YR	02-SSC-5299
NSM ADVANCED FOR NS*a* 3600/NS*a* 3650 1YR	02-SSC-5293
NSM ESSENTIAL FOR NS*a* 4600/NS*a* 4650 1YR	02-SSC-5325
NSM ADVANCED FOR NS*a* 4600/NS*a* 4650 1YR	02-SSC-5319
NSM ESSENTIAL FOR NS*a* 5600/NS*a* 5650 1YR	02-SSC-5347
NSM ADVANCED FOR NS*a* 5600/NS*a* 5650 1YR	02-SSC-5341
NSM ESSENTIAL FOR NS*a* 6600/NS*a* 6650 1YR	02-SSC-5365
NSM ADVANCED FOR NS*a* 6600/NS*a* 6650 1YR	02-SSC-5359

Multi-year SKUs and support contracts are also available.

Internet Browsers

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

[1] Supports firewalls running SonicOS version 6.x or 7.x.
[2] 365 days of Reporting and 30 days of Analytics are not supported.

NSM's Managed Devices[1]

- SonicWall Network Security Appliances: SuperMassive 9000 Series[2], E-Class NSA, NS*sp* 12000 Series[2], NS*a* Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NS*v* 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.

Datasheet-NSM-US-COG-2114

SONICWALL®

Connection we solve IT™

Contact an Account Manager for more information.
1.800.800.0014 ■ www.connection.com/Sonicwall