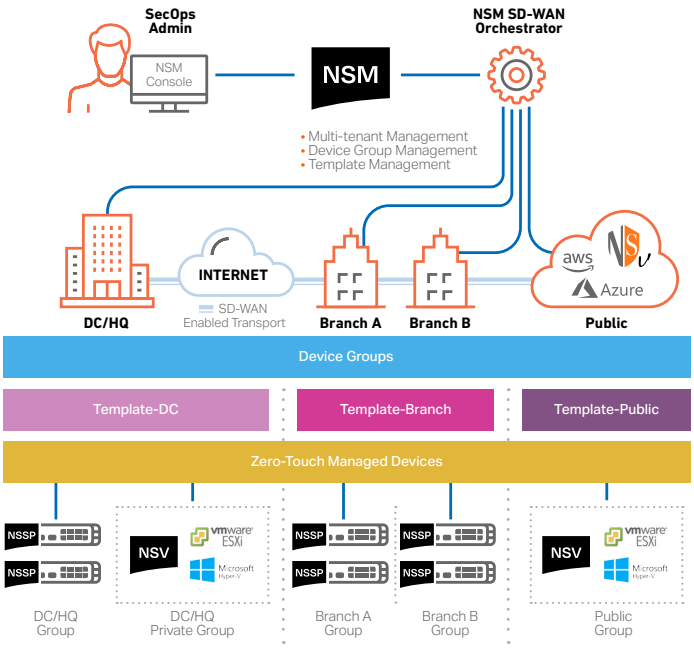
DATASHEET

Network Security Manager Cloud / Firewall Manager

Centralized firewall management that automates security at scale.

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

- Lower security management overhead with one console
- Continuous visibility into threat landscape and security posture
- Boost IT efficiency while cutting admin burnout
- Avoid costly disruption with proactive, audited policy changes

Operational

- Eliminate firewall management silos across every site
- Resolve critical issues fast with real-time health and uptime visibility
- Enforce identical configuration and policy on every managed device
- Stand up SD-WAN networks in minutes, not days

Security

- Score every firewall against a SonicWall security baseline and Tech Support Report
- Audit, approve, and commit every policy change before it ships
- Catch weak credentials and configuration drift early
- Track every policy action with full audit history
- Block unauthorized access with lockout, IP limits, and 2FA

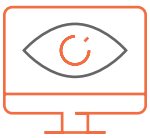
Centralized Management. Provable Security.

www.sonicwall.com/nsm

sonicwall.com

SONICWALL®

SonicWall Network Security Manager (NSM) is the multi-tenant, cloud-based and on-premises console IT and security teams use to deploy, template, and continuously audit every managed firewall. Its built-in Reporting and Analytics correlate logs across every device in a single dashboard, helping you monitor activity and catch threats before they spread. NSM simplifies compliance with consistent policy enforcement, a detailed audit trail of every configuration change, and granular reporting. Built to scale, NSM manages hundreds of firewalls across multiple tenants or locations from one place, and the cloud-based console is now integrated as the Firewall Manager with SonicWall Unified Management for a complete, seamless SonicWall experience.



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 Management lets you organize firewalls into groups, or hierarchies of groups, and push configuration templates to an entire group at once. Approved policy changes in a template apply automatically to every device group linked to it, so a single approved change rolls out consistently everywhere it belongs. Group devices by network type, location, business unit, org structure, or any combination, giving you one dynamic view for management, identification, and reporting. This keeps large, distributed fleets organized without manual bookkeeping.

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.

SONICWALL

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

NSM automates every stage of firewall management: Zero-Touch Deployment, template-based configuration push, SD-WAN and VPN orchestration, approval-gated change workflows, automatic firmware upgrades, and RESTful APIs for third-party integration. Together, these capabilities eliminate repetitive manual tasks, enforce consistent policy, and reduce human error, letting lean security teams manage hundreds of firewalls and tenants with the effort once needed for a handful, lowering operational cost while strengthening security posture.



Be more aware: See every risk clearly[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 into your entire SonicWall security ecosystem at the tenant, group, or device level. It provides static and near-real-time analysis

SONICWALL

of all network traffic and data communication moving 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

NSM helps surface hidden risks, flag vulnerabilities in configuration errors, and provide real-time visibility into firewall activity to accelerate response. Advanced analytics and drill-down capabilities let you correlate events across users, applications, and traffic to quickly identify and remediate threats.

Credential Auditor: Automatically checks firewall passwords and keys against publicly known credential databases.

Configuration Auditor: Checks system settings against best practices to reduce security gaps and misconfigurations.

Security Insights

Continuously scores every managed firewall against a SonicWall security baseline. It combines Configuration Auditor results with Tech Support Report (TSR) analysis in a single dashboard, surfacing misconfigurations and compliance gaps before they can be exploited.

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.

One console. Every firewall. Provable security at scale

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.

Licensing and Packaging

Licensing		
Features	**Advanced Protection**	**Managed Protection**[7]
Advanced Reporting	7 Days	30 Days
Advanced Analytics	7 Days	30 Days
Managed Firewall & Enhanced Support		✓

Management

Feature	Cloud 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	✓
Security Insights[1]	✓
Tenant grouping in firewall inventory view	✓

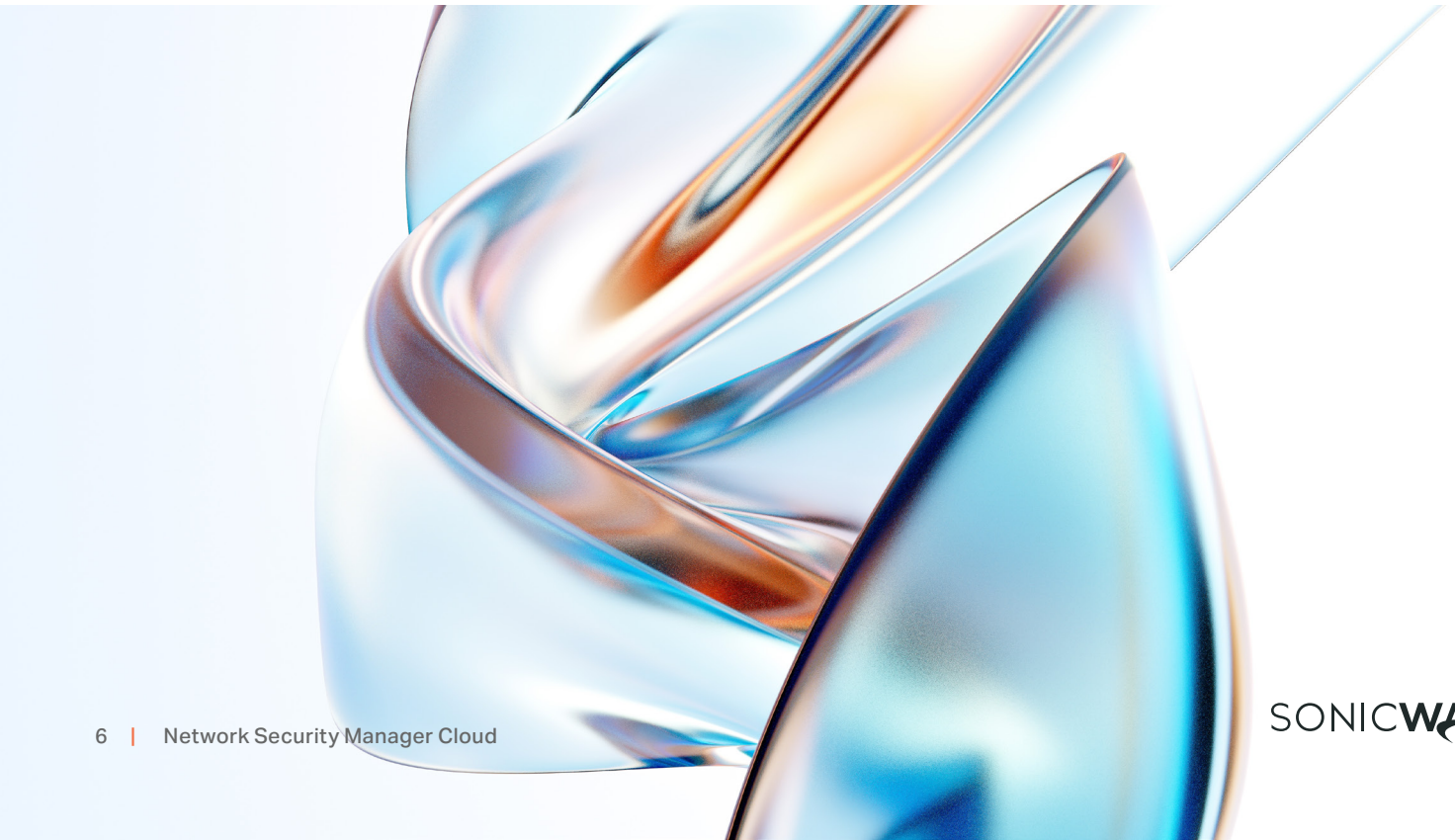
Licensing and Packaging cont'd

Reporting

Feature	Cloud Advanced Reporting and Analytics for 7, 30, 90, and 365 days
Group/Tenant Level Dashboard	✓
Capture ATP (Device Level)	✓
Capture Threat Assessment (Device Level)	✓
Productivity Reports[4]	✓
VPN Reports	✓
Custom Reports	✓
Schedule Report (Flow, CTA and Management)	✓
Firewall connectivity and Uptime status	✓
Firewall Up-Time Summary Report	✓
Firewall Audit Log Retention	✓
Attack Reports	✓
Web Activity Report	✓
Custom Branding in PDF Reports (MSP/MSSP)	✓

Analytics

Feature	Cloud Advanced Reporting and Analytics for 7, 30, 90, and 365 days
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
- Integration with Sonicwall Unified Management
- Network Access Control (NAC)
- Tenant and Device Group level management
- Configuration templates
- Device configuration conversion into template
- Firewall migration app
- Configuration Auditor
- Config – Diff
- Offline management and scheduling
- Management of firewall and VPN security policies
- Administration of SD-WAN
- Synchronization of security services
- Password protected configuration backups
- RESTful API
- Multi-device firmware upgrade
- Automatic firmware upgrades
- Role-based administration
- Credential auditor
- Automated remediation and reset of local user passwords and TOTP key bindings

Monitoring[1,2]

- Device health and status
- License and support status
- Firmware upgrade 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]

- Security Assessment Report
- 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 reports
- Attack Reports
- VPN Usage Reports
- Web Activity Report
- Custom branding in PDF reports (MSP/MSSP)

Security

- Closed Network support
- Account lockout
- Account access control
- 2FA support
- Authenticator App TFA support
- Security Insights: configuration scoring dashboard
- Firewall audit log retention

SONICWALL®

System Requirements

Internet Browsers

- The latest versions of Microsoft Edge, Mozilla Firefox, Google Chrome, and Safari

Managed Devices[5]

- NSsp 15700, NSsp 13700, NSsp 11700, NSsp 107000, NSsp 12000 Series[6], SuperMassive 9000 Series[6], NSa Series, TZ Series, TZ80.
- SonicWall Network Security Virtual Appliances: NSv Series
- Support for SonicWave includes Wi-Fi 6 enabled access points[4]
- SonicWall Switch[4]

[1] Available with Security Suites starting with EPSS, or as part of NSM Basic Licensing
[2] NSM Cloud includes reporting and analytics features.
[3] Only legacy reporting and analytics licenses are supported for Gen6/Gen6.5 products
[4] Managed only when connected to an NSM managed Firewall.
[5] All products that are end of life are not supported on NSM.
[6] NSM Advanced licenses are not supported for these models
[7] Supported on SonicOS 7.1 and above

Deploy and manage all firewalls from one easy-to-use interface.

www.sonicwall.com/nsm

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

© 2026 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.

Datasheet - NSM 4.0 SaaS 12254

sonicwall.com

SONICWALL®