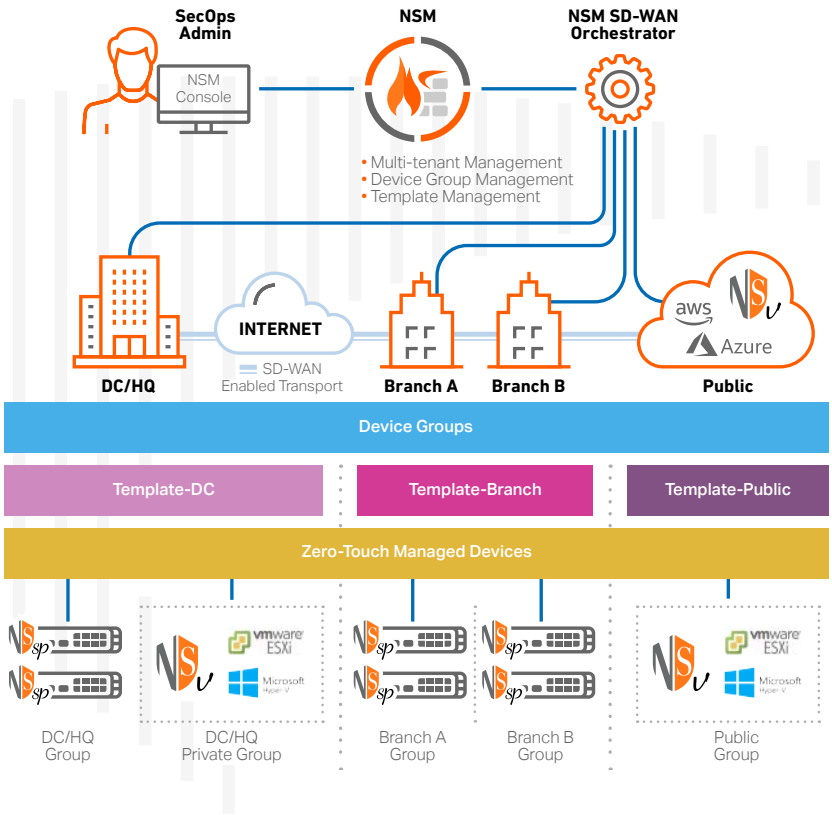
SONICWALL

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 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
- Onboard any number of firewalls remotely with ease
- 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

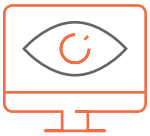
- Audit, commit and enforce consistent security policies across all environments
- Establish consistent SD-WAN configurations across all sites
- Discover threats and respond to issues and risks quickly
- Monitor and track results of policy actions with greater clarity
- Prevent unauthorized user authentication 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 as it allows for consistent policy enforcement across firewalls and provides 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 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 including DNS and content filtering across your environments with flexible local controls and monitoring everything from one dynamic dashboard with detailed reports and analytics. NSM also allows for Network Access Control via Aruba ClearPass integration. In addition, 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.

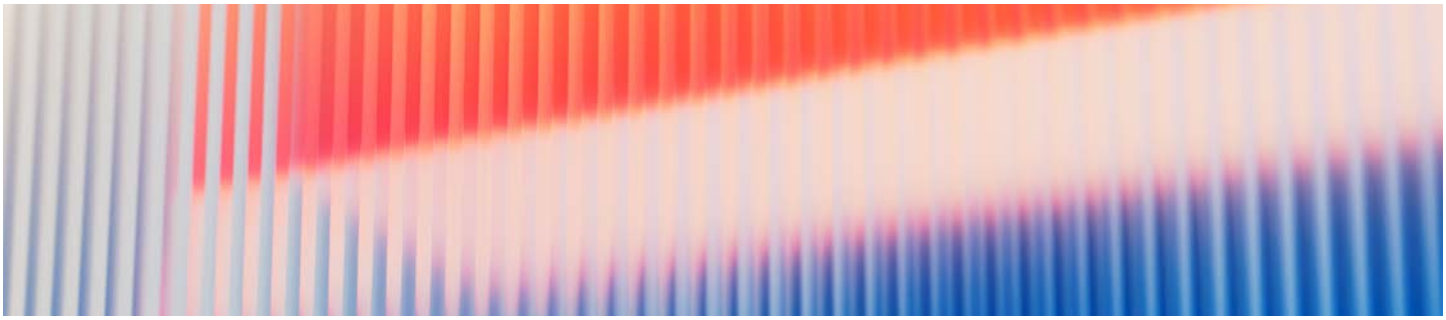
Device Group Management

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 hundreds 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.

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. Also, it helps reduce the complexity, time and overhead of performing everyday 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 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 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 give 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 increase 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, reporting and analytics data. The information helps you troubleshoot problems, investigate risks and take smart security policy actions for a more adaptive security posture.

Admins can act with precision and quickness with real-time alerts to keep their organization running optimally, helping organizations avoid costly business disruption and security incidents.

See Everything Everywhere

NSM, combined with Analytics,[1,2] gives you up to 7 days of continuous visibility of your entire SonicWall security ecosystem at the tenant, group or device level. It provides static and near-real-time analyses 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. 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 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.

Optimize Workforce Productivity

User Analytics[1,2] gives a broad and transparent view of your workforce's web application and internet usage activities. Drill-down 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

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.

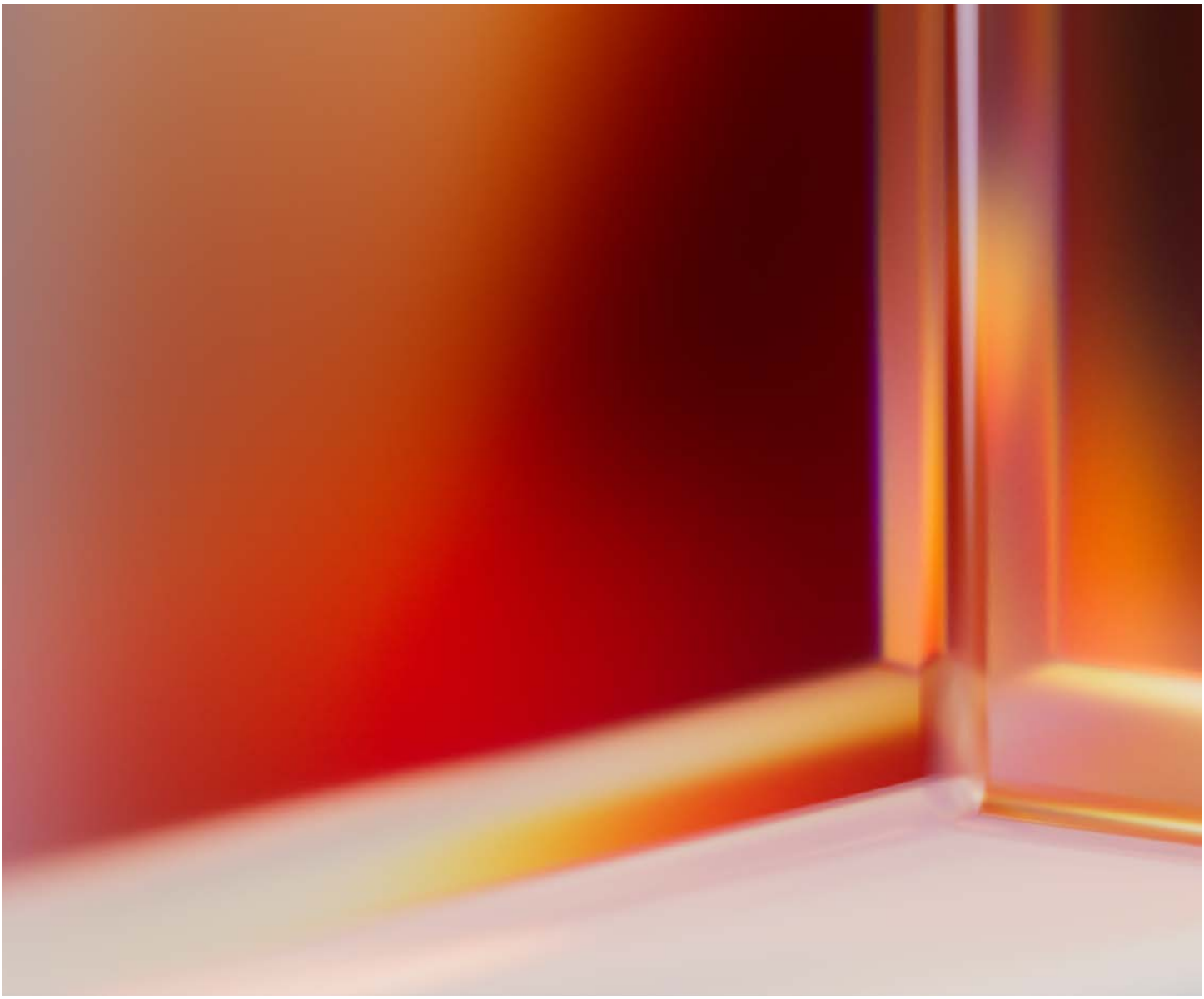
For total system control and compliance, you can deploy NSM in Microsoft Azure public cloud or as a virtual appliance in a private cloud on VMWare, Microsoft Hyper-V or KVM. These give you all the operational and economic benefits of virtualization, including system scalability and agility, speed of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

Security Capabilities

Any organization can deploy the SonicOS 7.1.2 as a Cloud Secure Edge Connector" that can establish a connection to internet and cloud clusters hosted by corporate resources. The Connector then establishes secure tunnels to the Access Tiers on the Global Edge Network. With the Cloud Secure Edge Connector integration, NSM users have access to our Cloud Secure Edge technology to offers secure private access for remote users with Zero Trust 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

- Integration with Cloud Secure Edge Connector
- Network Access Control (NAC) with Aruba Clearpass
- 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
- Administration of SD-WAN
- Synchronization 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
- Productivity Reports
- Firewall Up-Time Summary Report

Security

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

Licensing and Packaging

Management			
Feature	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Premises[2]**
Tenant	Yes	Yes	Yes
Device Inventory	Yes	Yes	Yes
Push policy at the group level	Yes	Yes	Yes
Device Group	Yes	Yes	Yes
Templates	Yes	Yes	Yes
Commit and Deploy (Workflow Automation)	Yes	Yes	Yes
Configuration Audit	Yes	Yes	Yes
Config Diff	Yes	Yes	Yes
Workflow Automation	Yes	Yes	Yes
API	Yes	Yes	Yes
Zero-Touch Deployment	Yes	Yes	Yes
SD-WAN Orchestration and Monitoring	Yes	Yes	Yes
VPN Orchestration and Monitoring	Yes	Yes	Yes
Task scheduling	Yes	Yes	Yes
Backup/Restore	Yes	Yes	Yes
Firmware upgrades	Yes	Yes	Yes
Access Point and Switch Management	Yes	Yes	Yes
Advanced DNS Filtering*	No	Yes	No
Network Access Control with Aruba Clearpass*	Yes	Yes	Yes

*Supported on SonicOS 7.1 and above

Licensing and Packaging cont'd

Management			
Reputation-based content filtering*	Yes	Yes	Yes
Integration with Cloud Secure Edge Connector	Yes	Yes	No

Reporting			
Feature	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Premises[2]**
Group/Tenant Level Dashboard	Yes	Yes	No
Capture ATP (Device Level)	Yes	Yes	Yes
Capture Threat Assessment (Device Level)	Yes	Yes	Yes
Productivity Reports[5]	No	Yes	No
VPN Reports	No	Yes	No
Custom Reports	Yes	Yes	No
Schedule Report (Flow, CTA and Management)	Yes (Except flow report)	Yes	Yes
Days of reporting data	7 days (Basic reporting)	365 days	365 days
Firewall Up-Time Summary Report	Yes	Yes	Yes

Analytics			
Feature	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Premises[2]**
User-based analytic	No	Yes	Yes
Application analytics	No	Yes	Yes
Network forensic and threat hunting using drill-down and pivots	No	Yes	Yes

System Requirements

Internet Browsers

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

NSM On-Premises System Requirement

- Hypervisor: ESXi 7.0, 8.0, 2019, 2022, and KVM
- Public Cloud: Azure
- Minimum computing resources: 4 vCPUs, 24 GB Memory for managing 1-500 firewalls, 250GB Storage

Managed Devices

- NS*sp* 15700, NS*sp* 13700, NS*sp* 12000 Series[4], SuperMassive 9000 Series[4], NSA Series, NS*a* 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: NS*v* Series
- SonicWall SonicWave[6], SonicPoint
- Support for SonicWave includes Wi-Fi6 enabled access points
- SonicWall Switch

[1] NSM SaaS includes reporting and analytics features.
[2] NSM On-Premises requires a separate SonicWall Analytics On-Premises install and license for the reporting and analytics features.
[3] Available only on NSM On-Premises.
[4] 365 days of Reporting and 30 days of Analytics are not supported.
[5] Requires AGSS/CGSS license enabled on Generation 6/6.5 Firewalls, Essential Protection license on Generation 7 Firewalls
[6] Support for SonicWave includes Wi-Fi6 enabled access points

Deploy and manage all your firewalls, connected switches and access points, all in one easy-to-use interface.

www.sonicwall.com/nsm

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

SONICWALL®