SONICWALL

# SonicWall Network Security services platform (NSsp) 12000 series

**Scalable, cutting-edge security that leverages the power of cloud intelligence.**

The SonicWall Network Security services platform (NSsp) 12000 series takes a modern approach to threat detection and prevention by combining cloud intelligence with appliance-based protection in a scalable, high-speed platform. Designed for large distributed enterprises, data centers and service providers, NSsp series next-generation firewalls (NGFWs) leverage innovative deep learning security technologies in the Capture Cloud Platform to deliver proven protection from the most advanced threats without slowing performance.

## Security for the enterprise

The volume and sophistication of today's network attacks continues to grow. Identifying and stopping unknown, zero-day threats and intrusions requires an approach that extends on-box protection with security intelligence in the cloud. Without that cloud intelligence, enterprise gateway security solutions are unable to stay ahead of today's complex threats.

The SonicWall NSsp series takes threat intelligence gathered by our dedicated Capture Labs threat research team and combines it with on-box security to deliver continuously-updated protection. SonicWall's cloud-based Capture Advanced Threat Protection (ATP) service utilizes patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology to proactively detect and block mass market, zero-day threats and unknown malware by inspecting directly in memory. Because of the real-time architecture, SonicWall RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds. Augmenting the cloud-based security is SonicWall's patented* single-pass Reassembly-Free Deep Packet Inspection (RFDPI®) engine which inspects both inbound and outbound network traffic on the firewall. By leveraging the SonicWall Capture Cloud Platform in addition to on-box capabilities including intrusion prevention, antimalware and web/URL filtering, the NSsp series is able to provide the automated, real-time breach prevention enterprise organizations need.

With the increase in the number of encrypted web connections, it's essential that NGFWs are able to inspect encrypted traffic for hidden threats. SonicWall firewalls provide complete protection by performing full decryption and inspection over hundreds of thousands of TLS/SSL and SSH encrypted connections regardless of port or protocol. The firewall looks deep inside every packet for protocol anomalies, threats, zero-days, intrusions, and even defined criteria. The deep packet inspection engine detects and prevents hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration. Inclusion and exclusion rules allow total control to customize which traffic is subjected to


## Benefits:

### Superior threat prevention and performance

- Patent-pending real-time deep memory inspection technology
- Patent reassembly-free deep packet inspection technology
- Cloud-based and on-box threat prevention
- TLS/SSL decryption and inspection
- Industry-validated security effectiveness
- Multiple 40-GbE and 10-GbE interfaces
- Dedicated Capture Labs threat research team

### Network control and flexibility

- Powerful SonicOS operating system
- Application intelligence and control
- Network segmentation and zoning
- Deployment at the network edge or data center core

### Scalability and reliability

- High DPI-SSL connection count
- Multiple configuration options
- Built-in storage module
- Redundant power supplies and fans

decryption and inspection based on specific organizational compliance and/or legal requirements.

As organizations grow, the need for scalable security takes on greater importance. SonicWall supports growing enterprise networks with a solution that eliminates concerns around the need for adding more processing power. The NSsp 12400 includes four processor modules that can be upgraded to eight, while the NSsp 12800 comes with eight processor modules out of the box.

Activating deep packet inspection functions such as IPS, antivirus, anti-spyware and TLS/SSL decryption/inspection on the firewall often slows network performance down, sometimes dramatically. NSsp series NGFWs, however, feature high-speed 40-GbE interfaces and a multi-core hardware architecture that utilizes specialized security processors. Combined with our RTDMI and RFDPI engines, this unique design eliminates the performance degradation networks experience with other firewalls.

## Network control and flexibility

At the core of the NSsp series is SonicOS, SonicWall's feature-rich operating system. SonicOS provides organizations with the network control and flexibility they require through application intelligence and control, real-time visualization, an intrusion prevention system (IPS) featuring sophisticated anti-evasion technology, high-speed virtual private networking (VPN) and additional security features.

Using application intelligence and control, network administrators can identify and categorize productive applications from those that are unproductive or potentially dangerous, and control that traffic through powerful application-level policies on both a per-user and a per-group basis (along with schedules and exception lists).

Business-critical applications can be prioritized and allocated more bandwidth while nonessential applications are bandwidth-limited. Real-time monitoring and visualization provides a graphical representation of applications, users and bandwidth usage for granular insight into traffic across the network.

For enterprise organizations looking for advanced flexibility in their network design, SonicOS offers the tools to segment the network into zones through the use of virtual LANs (VLANs). This enables network administrators to create a virtual LAN interface that allows for network separation into one or more logical groups.

## Simplified management and reporting

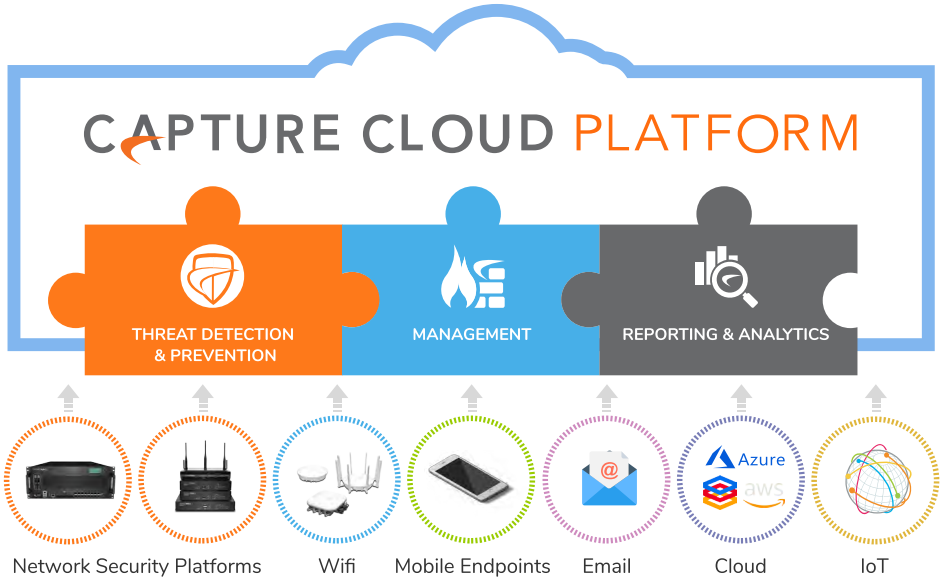
Ongoing management, monitoring and reporting of network activity are handled through the SonicWall Global Management System (GMS), providing administrators with an intuitive single pane of glass dashboard for managing all aspects of the network in real time. Together, the simplified deployment and setup along with the ease of management enable organizations to lower their total cost of ownership and realize a high return on investment.

### Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

## Capture Cloud Platform

SonicWall's Capture Cloud Platform delivers cloud-based threat prevention and network management plus reporting and analytics for organizations of any size. The platform consolidates threat intelligence gathered from multiple sources including our award-winning multi-engine network sandboxing service, Capture Advanced Threat Protection, as well as more than 1 million SonicWall sensors located around the globe.




If data coming into the network is found to contain previously-unseen malicious code, SonicWall's dedicated, in-house Capture Labs threat research team develops signatures that are stored in the Capture Cloud Platform database and deployed to customer firewalls for up-to-date protection. New updates take effect immediately without reboots or interruptions. The signatures resident on the appliance protect against wide classes of attacks, covering tens of thousands of individual threats with a single signature. In addition to the countermeasures on the appliance, NSsp firewalls also have continuous access to the Capture Cloud Platform database which extends the onboard signature intelligence with tens of millions of signatures.

Furthermore, the Capture Cloud Platform offers single pane of glass management and administrators can easily create both real-time and historical reports on network activity.

## Advanced threat protection

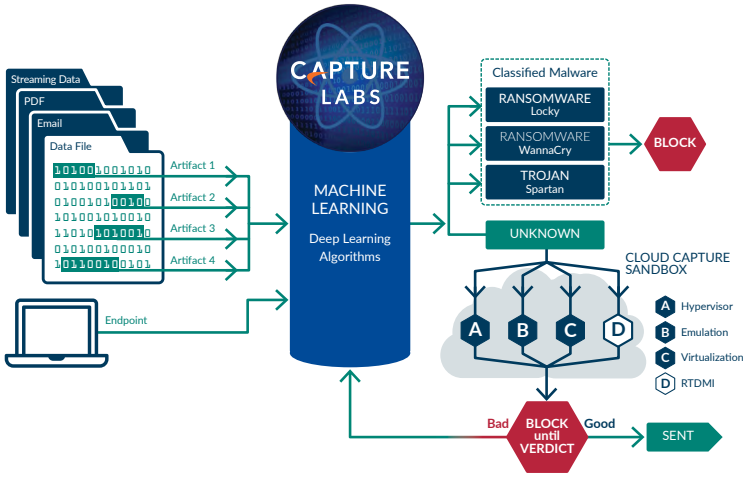
At the center of SonicWall's automated, real-time breach prevention are two advanced malware detection technologies; Capture Advanced Threat Protection™ (Capture ATP) and Capture Security appliance™ (CSa).

Capture ATP is a cloud-based multi-engine sandbox platform, which includes Real-Time Deep Memory Inspection™ (RTDMI), virtualized sandboxing, full system emulation and hypervisor level analysis technology. CSa is an on-premises device that features RTDMI, which utilizes memory-based static and dynamic techniques for fast and accurate verdicts. Both solutions extend advanced threat protection to detect and prevent zero-day threats in a variety of SonicWall solutions such as next-generation firewalls.

Suspicious files are sent to either solution where they are analyzed using deep learning algorithms with the option to hold them at the gateway until a verdict is determined. In the case of Capture ATP, when files are identified as malicious, they are blocked, and a hash is immediately created within the Capture ATP database for all customers to leverage to block follow-on attacks. These signatures are eventually sent to firewalls to create static defenses. Results generated by CSa are not shared outside your organization for privacy and compliance reasons.

These services analyze a broad range of operating systems and file types, including executable programs, DLL, PDFs, MS Office documents, archives, JAR and APK.

For complete endpoint protection, the SonicWall Capture Client combines next-generation antivirus technology with SonicWall's cloud-based multi-engine sandbox with optional integration with SonicWall firewalls.





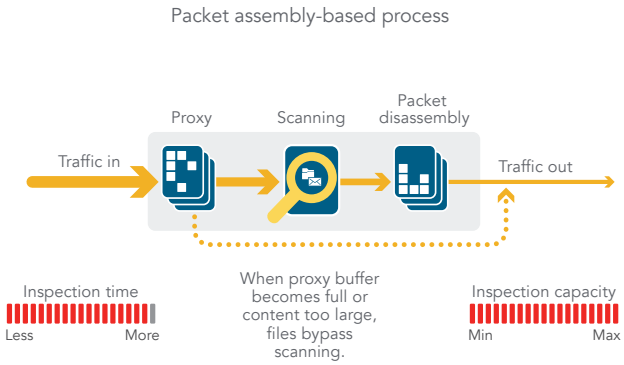

SONICWALL®

## Reassembly-Free Deep Packet Inspection engine

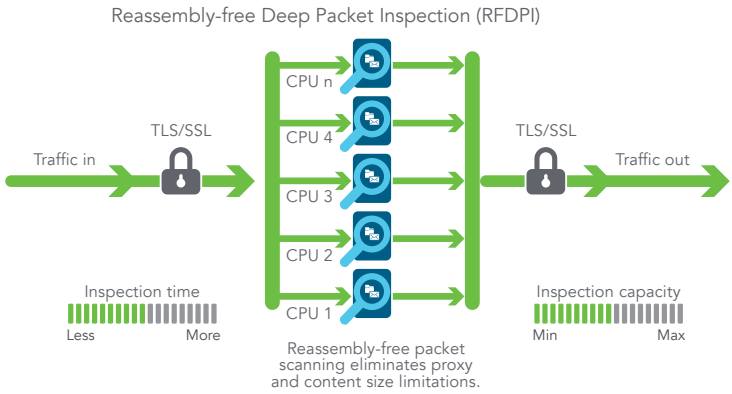
The SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) is a single-pass, low latency inspection system that performs stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. This proprietary engine relies on streaming traffic payload inspection to detect threats at Layers 3-7, and takes network streams through extensive and repeated normalization and decryption in order to neutralize advanced evasion techniques that seek to confuse detection engines and sneak malicious code into the network.

Once a packet undergoes the necessary pre-processing, including TLS/SSL decryption, it is analyzed against a single, proprietary memory representation of three signature databases: intrusion attacks, malware and applications. The connection state is then advanced to represent the position of the stream relative to these databases until it encounters a state of attack, or other "match" event, at which point a pre-set action is taken.

In most cases, the connection is terminated and proper logging and notification events are created. However, the engine can also be configured for inspection only or, in case of application detection, to provide Layer 7 bandwidth management services for the remainder of the application stream as soon as the application is identified.




**Competitive proxy-based architecture**

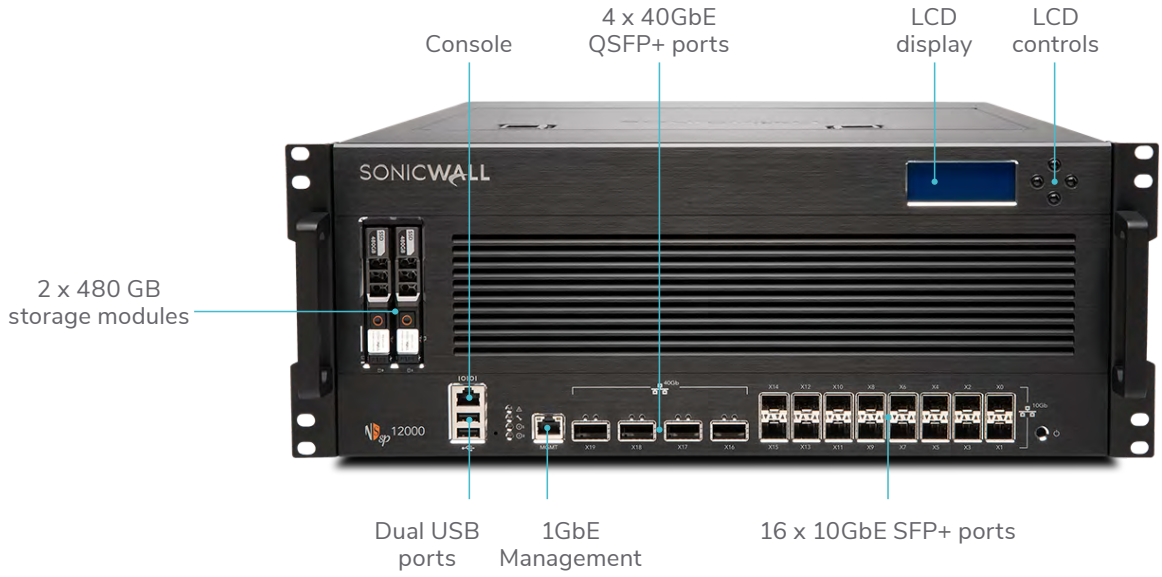


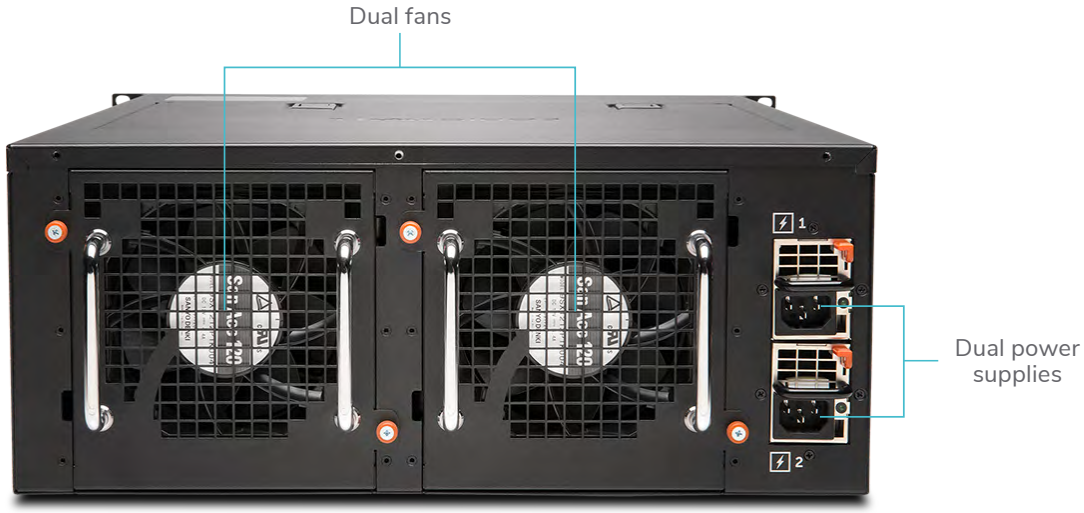

**SonicWall stream-based architecture**

## Global management and reporting

For highly regulated organizations wanting to achieve a fully coordinated security governance, compliance and risk management strategy, SonicWall provides administrators a unified, secure and extensible platform to manage SonicWall firewalls, wireless access points and WAN acceleration solutions through a correlated and auditable workstream process. Enterprises can easily consolidate the management of security appliances, reduce administrative and troubleshooting complexities, and govern all operational aspects of the security infrastructure, including centralized policy management and enforcement; real-time event monitoring; user activities; application identifications; flow analytics and forensics; compliance and audit reporting; and more. In addition, enterprises meet the firewall's change management requirements through workflow automation which provides the agility and confidence to deploy the right firewall policies at the right time and in conformance with compliance regulations. SonicWall Global Management System (GMS), SonicWall's on-premises management and reporting solution, provides a coherent way to manage network security by business processes and service levels, dramatically simplifying lifecycle management of your overall security environments compared to managing on a device-by-device basis.

## NSsp 12000 Series




| FIREWALL | NSSP 12400 | NSSP 12800 |
|---|---|---|
| Firewall inspection throughput | 58.4 Gbps | 120.3 Gbps |
| IPS throughput | 36.8 Gbps | 73.0 Gbps |
| Anti-malware inspection throughput | 33.5 Gbps | 67.5 Gbps |
| Threat Prevention throughput | 33.5 Gbps | 67.5 Gbps |
| IMIX throughput | 14.8 Gbps | 29.0 Gbps |
| Maximum connections (DPI) | 16,000,000 | 32,000,000 |
| New connections/sec | 430,000/sec | 860,000/sec |
| Storage module | 2 x 480 GB | 2 x 480 GB |
| **DESCRIPTION** | **SKU** | **SKU** |
| NSsp firewall only | 01-SSC-1206 | 01-SSC-1207 |
| NSsp TotalSecure Advanced (1-year) | 01-SSC-7883 | 01-SSC-9139 |

## SonicOS feature summary

### Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6
- Biometric authentication for remote access
- DNS proxy
- REST APIs

### TLS/SSL/SSH decryption and inspection[1]

- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- TLS/SSL control
- Granular DPI SSL controls per zone or rule

### Capture advanced threat protection[1]

- Real-Time Deep Memory Inspection
- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated and manual submission
- Real-time threat intelligence updates
- Block until verdict
- Capture Client

### Intrusion prevention[1]

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection
- Granular IPS rule capability
- GeoIP enforcement
- Botnet filtering with dynamic list
- Regular expression matching

### Anti-malware[1]

- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- Bi-directional inspection
- No file size limitation
- Cloud malware database

### Application identification[1]

- Application control
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- Comprehensive application signature database

### Traffic visualization and analytics

- User activity
- Application/bandwidth/threat usage

### Web content filtering[1]

- URL filtering
- Proxy avoidance
- Keyword blocking
- HTTP header insertion
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- Content Filtering Client

### VPN

- Auto-provision VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire
- Route-based VPN (OSPF, RIP, BGP)

### Networking

- PortShield
- Jumbo frames
- Enhanced logging
- VLAN trunking
- RSTP (Rapid Spanning Tree Protocol)
- Port mirroring
- Port security
- Layer-2 QoS
- Dynamic routing (RIP/OSPF/BGP)
- Policy-based routing
- NAT
- DNS/DNS proxy
- DHCP server
- Bandwidth management
- Link aggregation (static and dynamic)
- Port redundancy
- A/P high availability with state sync
- A/A clustering
- Inbound/outbound load balancing
- L2 bridge, wire/virtual wire mode, tap mode
- Asymmetric routing
- Common Access Card (CAC) support

### Wireless

- WIDS/WIPS
- RF spectrum analysis
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- Floor plan view/Topology view
- Band steering
- Beamforming
- AirTime fairness
- MiFi extender
- Guest cyclic quota
- LHM guest portal

### VoIP

- Granular QoS control
- Bandwidth management
- SIP and H.323 transformations per access rule
- H.323 gatekeeper and SIP proxy support

### Management and monitoring

- GMS, Web, UI, CLI, REST APIs, SNMPv2/v3
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat Security Analytics Platform
- SonicWall access point management

### Storage

- Logs
- Reports
- Firmware backups

[1]*Requires added subscription*



SONICWALL®

## Features

### RFDPI ENGINE

| Feature | Description |
|---|---|
| Reassembly-Free Deep Packet Inspection (RFDPI) | This high-performance, proprietary and patented inspection engine performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port. |
| Bi-directional inspection | Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside. |
| Stream-based inspection | Proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams. |
| Highly parallel and scalable | The unique design of the RFDPI engine works with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks. |
| Single-pass inspection | A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture. |

### FIREWALL AND NETWORKING

| Feature | Description |
|---|---|
| REST APIs | Allows the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats. |
| Stateful packet inspection | All network traffic is inspected, analyzed and brought into compliance with firewall access policies. |
| High availability/clustering | The NSsp series supports Active/Passive (A/P) with state synchronization, Active/Active (A/A) DPI and Active/Active clustering high availability modes. Active/Active DPI offloads the deep packet inspection load to cores on the passive appliance to boost throughput. |
| DDoS/DoS attack protection | SYN flood protection provides a defense against DoS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DoS/DDoS through UDP/ICMP flood protection and connection rate limiting. |
| IPv6 support | Internet Protocol version 6 (IPv6) is in its early stages to replace IPv4. With SonicOS, the hardware will support filtering and wire mode implementations. |
| Flexible deployment options | The NSsp series can be deployed in traditional NAT, Layer 2 bridge, wire and network tap modes. |
| WAN load balancing | Load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods. |
| Advanced quality of service (QoS) | Guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network. |
| H.323 gatekeeper and SIP proxy support | Blocks spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy. |
| Biometric authentication | Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user identity for network access. |
| Open authentication and social login | Enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication. |

### MANAGEMENT AND REPORTING

| Feature | Description |
|---|---|
| Global Management System (GMS) | Configuration and management of SonicWall appliances is available on-premises using SonicWall Global Management System (GMS). |
| Powerful single device management | An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive command-line interface and support for SNMPv2/3. |
| IPFIX/NetFlow application flow reporting | Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools such as SonicWall Analytics or other tools that support IPFIX and NetFlow with extensions. |

### VIRTUAL PRIVATE NETWORKING (VPN)

| Feature | Description |
|---|---|
| Auto-provision VPN | Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically. |
| IPSec VPN for site-to-site connectivity | High-performance IPSec VPN allows the NSsp series to act as a VPN concentrator for thousands of other large sites, branch offices or home offices. |
| SSL VPN or IPSec client remote access | Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms. |
| Redundant VPN gateway | When using multiple WANs, a primary and secondary VPN can be configured to allow seamless, automatic failover and failback of all VPN sessions. |
| Route-based VPN | The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes. |

| CONTENT/CONTEXT AWARENESS | |
|---|---|
| Feature | Description |
| User activity tracking | User identification and activity are made available through seamless AD/LDAP/Citrix1/Terminal Services1 SSO integration combined with extensive information obtained through DPI. |
| GeoIP country traffic identification | Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address. Eliminates unwanted filtering of IP addresses due to misclassification. |
| Regular expression DPI filtering | Prevents data leakage by identifying and controlling content crossing the network through regular expression matching. Provides the ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address. |

## Breach prevention subscription services

| CAPTURE ADVANCED THREAT PROTECTION | |
|---|---|
| Feature | Description |
| Multi-engine sandboxing | The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation, and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity. |
| Real-Time Deep Memory Inspection (RTDMI) | This patent-pending cloud-based technology detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. By forcing malware to reveal its weaponry into memory, the RTDMI engine proactively detects and blocks mass-market, zero-day threats and unknown malware. |
| Block until verdict | To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined. |
| Broad file type and size analysis | Supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments. |
| Rapid deployment of signatures | When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWall Capture ATP subscriptions and Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours. |
| Capture Client | Capture Client is a unified client platform that delivers multiple endpoint protection capabilities, including advanced malware protection and support for visibility into encrypted traffic. It leverages layered protection technologies, comprehensive reporting and endpoint protection enforcement. |

| CAPTURE SECURITY APPLIANCE (CSa) | |
|---|---|
| Feature | Description |
| Compliance-centered malware detection | Analyze suspicious files in your own environment without sending files or results to a third-party cloud. |
| Built-in integrations | CSa supports out of the box integrations with other security solutions (firewalls and email security) from SonicWall. |
| Near real-time protection | SonicWall's patented RTDMI technology helps detect malware quickly, even for previously unknown malware, that CSa can enable the block until verdict capability on SonicWall next-generation firewalls. |
| Deployment | CSa can be configured on a private network directly connected to a singular edge firewall or be reachable over the Internet directly or using VPN by branch firewalls. |

| ENCRYPTED THREAT PREVENTION | |
|---|---|
| Feature | Description |
| TLS/SSL decryption and inspection | Decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in encrypted traffic Included with security subscriptions for all NSsp series models. |
| SSH inspection | Deep packet inspection of SSH (DPI-SSH) decrypts and inspect data traversing over SSH tunnel to prevent attacks that leverage SSH. |

| INTRUSION PREVENTION | |
|---|---|
| Feature | Description |
| Countermeasure-based protection | Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. |
| Automatic signature updates | The SonicWall Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take immediate effect without any reboot or service interruption required. |

| | |
|---|---|
| Intra-zone IPS protection | Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries. |
| Botnet command and control (CnC) detection and blocking | Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points. |
| Protocol abuse/anomaly | Identifies and blocks attacks that abuse protocols in an attempt to sneak past the IPS. |
| Zero-day protection | Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits. |
| Anti-evasion technology | Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7. |

## THREAT PREVENTION

| Feature | Description |
|---|---|
| Gateway anti-malware | The RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams. |
| Capture Cloud malware protection | A continuously updated database of tens of millions of threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats. |
| Around-the-clock security updates | New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions. |
| Bi-directional raw TCP inspection | The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports. |
| Extensive protocol support | Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decodes payloads for malware inspection, even if they do not run on standard, well-known ports. |

## APPLICATION INTELLIGENCE AND CONTROL

| Feature | Description |
|---|---|
| Application control | Control applications, or individual application features, that are identified by the RFDPI engine against a continuously expanding database of over thousands of application signatures, to increase network security and enhance network productivity. |
| Custom application identification | Control custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network. |
| Application bandwidth management | Granularly allocate and regulate available bandwidth for critical applications or application categories while inhibiting nonessential application traffic. |
| Granular control | Control applications, or specific components of an application, based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration. |

## CONTENT FILTERING

| Feature | Description |
|---|---|
| Inside/outside content filtering | Enforce acceptable use policies and block access to websites containing information or images that are objectionable or unproductive with Content Filtering Service. |
| Enforced Content Filtering Client | Extend policy enforcement to block internet content for Windows, Mac OS, Android and Chrome devices located outside the firewall perimeter. |
| Granular controls | Block content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups. |
| Web caching | URL ratings are cached locally on the SonicWall firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second. |

## ENFORCED ANTIVIRUS AND ANTI-SPYWARE

| Feature | Description |
|---|---|
| Multi-layered protection | Utilize the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block, viruses entering network through laptops, thumb drives and other unprotected systems. |
| Automated enforcement option | Ensure every computer accessing the network has the appropriate antivirus software and/or DPI-SSL certificate installed and active, eliminating the costs commonly associated with desktop antivirus management. |
| Automated deployment and installation option | Machine-by-machine deployment and installation of antivirus and anti-spyware clients is automatic across the network, minimizing administrative overhead. |
| Next-generation antivirus | Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and roll back to a previous uninfected state. |
| Spyware protection | Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they transmit confidential data, providing greater desktop security and performance. |

## NS*sp* series system specifications

| FIREWALL GENERAL | NSsp 12400 | NSsp 12800 |
|---|---|---|
| Operating system | SonicOS 6.5.1.8 | |
| Security processing cores | 128 | 256 |
| Interfaces | 4 x 40-GbE QSFP+, 16 x 10-GbE SFP+, 1 GbE Management, 1 Console | 4 x 40-GbE QSFP+, 16 x 10-GbE SFP+, 1 GbE Management, 1 Console |
| Built-in storage | 2 x 480 GB | |
| Management | CLI, SSH, Web UI, GMS, REST APIs | |
| SSO users | 110,000 | 110,000 |
| Maximum access points supported | 128 | 128 |
| Logging | Analyzer, Local Log, Syslog, IPFIX, NetFlow | |
| **FIREWALL/VPN PERFORMANCE** | **NSsp 12400** | **NSsp 12800** |
| Firewall inspection throughput[1] | 58.4 Gbps | 120.3 Gbps |
| Threat Prevention throughput[2] | 33.5 Gbps | 67.5 Gbps |
| Application inspection throughput[2] | 45.5 Gbps | 91.0 Gbps |
| IPS throughput[2] | 36.8 Gbps | 73.0 Gbps |
| Anti-malware inspection throughput[2] | 33.5 Gbps | 67.5 Gbps |
| IMIX throughput | 14.8 Gbps | 29.0 Gbps |
| TLS/SSL decryption and inspection throughput (DPI SSL)[2] | 8.1 Gbps | 17.6 Gbps |
| VPN throughput[3] | 24.5 Gbps | 47.0 Gbps |
| Connections per second | 430,000/sec | 860,000/sec |
| Maximum connections (SPI) | 40,000,000 | 80,000,000 |
| Maximum connections (DPI) | 16,000,000 | 32,000,000 |
| Maximum connections (DPI SSL) | 1,300,000 | 2,600,000 |
| **VPN** | **NSsp 12400** | **NSsp 12800** |
| Site-to-site VPN tunnels | 25,000 | 25,000 |
| IPSec VPN clients (max) | 2,000 (10,000) | 2,000 (10,000) |
| SSL VPN NetExtender clients (max) | 2 (3,000) | 2 (3,000) |
| Encryption/Authentication | DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography | |
| Key exchange | Diffie Hellman Groups 1, 2, 5, 14v | |
| Route-based VPN | RIP, OSPF, BGP | |
| **NETWORKING** | **NSsp 12400** | **NSsp 12800** |
| IP address assignment | Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay | |
| NAT modes | 1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode | |
| VLAN interfaces | 512 | 512 |
| Routing protocols | BGP, OSPF, RIPv1/v2, static routes, policy-based routing | |
| QoS | Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p | |
| Authentication | LDAP, XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC) | |
| VoIP | Full H323-v1-5, SIP | |
| Standards | TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 | |
| Certifications (in progress) | ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall and IPS), UC APL, USGv6, CsFC | |
| High availability | Active/Passive with State Sync, Active/Active DPI with State Sync, Active/Active Clustering | |
| **HARDWARE** | **NSsp 12400** | **NSsp 12800** |
| Power supply | Dual, Redundant, 1,200W | |
| Fans | Dual, Removable | |
| Input power | 100-240 VAC, 50-60 Hz | |
| Maximum power consumption (W) | 679 | 965 |
| MTBF @25°C in hours | 113,114 | 91,118 |
| MTBF @25°C in years | 12.9 | 10.4 |
| Form factor | 4U Rack Mountable | |
| Dimensions | 24.0 x 16.9 x 7.1 in (61 x 43 x 18 cm) | |
| Weight | 59.3 lb (26.9 kg) | 67.2 lb (30.5 kg) |
| WEEE weight | 67.7 lb (30.7 kg) | 75.6 lb (34.3 kg) |
| Shipping weight | 83.1 lb (37.7 kg) | 91.1 lb (41.3 kg) |
| Major regulatory | FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL | |
| Environment (Operating/Storage) | 32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C) | |
| Humidity | 10-95% non-condensing | |

[1] *Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.*
[2] *Full DPI/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs. Threat Prevention throughput measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled. DPI SSL performance measured on HTTPS traffic with IPS enabled.*
[3] *VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change.*
**Future use. All specifications, features and availability are subject to change.*

## NSsp 12000 series ordering information

| NSsp 12400 | SKU |
|---|---|
| NSsp 12400 TotalSecure Advanced Edition (1-year) | 01-SSC-7883 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall management and reporting, Shadow IT Visibility, and 24x7 Support for NSsp 12400 (1-year) | 01-SSC-6588 |
| Capture Advanced Threat Protection for NSsp 12400 (1-year) | 01-SSC-6598 |
| Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSsp 12400 (1-year) | 01-SSC-7853 |
| 24x7 Support for NSsp 12400 (1-year) | 01-SSC-6384 |
| Content Filtering Service for NSsp 12400 (1-year) | 01-SSC-7698 |
| **NSsp 12800** | **SKU** |
| NSsp 12800 TotalSecure Advanced Edition (1-year) | 01-SSC-9139 |
| Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall management and reporting, Shadow IT Visibility, and 24x7 Support for NSsp 12800 (1-year) | 01-SSC-6591 |
| Capture Advanced Threat Protection for NSsp 12800 (1-year) | 01-SSC-7178 |
| Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSsp 12800 (1-year) | 01-SSC-7879 |
| 24x7 Support for NSsp 12800 (1-year) | 01-SSC-6498 |
| Content Filtering Service for NSsp 12800 (1-year) | 01-SSC-7850 |
| **MODULES AND ACCESSORIES*** | **SKU** |
| NSsp 12000 Series Processor Module | 01-SSC-1211 |
| NSsp 12000 Series SSD Module | 01-SSC-1212 |
| NSsp 12000 Series System Fan | 01-SSC-1213 |
| NSsp 12000 Series AC Power Supply | 01-SSC-1215 |

**Please consult with your local SonicWall reseller for a complete list of supported SFP and SFP+ modules*

## Regulatory model numbers:

NSsp 12400/12800 – 4RK02-0C0

## 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-NSsp-US-COG-2466