The SonicWall Network Security services platform™ (NSsp) series has next-generation firewalls with high port density and multi-gig speed interfaces, that can process several million connections for zero-day and advanced threats. Designed for large enterprise, higher education, government agencies and MSSPs, it eliminates attacks in real time without slowing performance. It is designed to be highly reliable and deliver uninterrupted services to organizations.

**HIGHLIGHTS**

**SonicWall NSsp Series**
- High port density
- 100 GbE ports
- Integrates with on-prem and cloud-based sandboxing
- Single pane of glass management
- 80+ Gbps Threat prevention throughput
- Redundant power
- Up to 100 Gbps firewall inspection throughput
- TLS 1.3 support
- Supports millions of simultaneous TLS connections
- Low TCO

**NSsp Spec Preview. View full specs »**

<table>
<thead>
<tr>
<th></th>
<th>100 GbE</th>
<th>Up to 100 Gbps</th>
<th>80M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall inspection throughput</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max Connections (NSsp 15700)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Learn more about SonicWall Gen 7 NSsp Series:**

[sonicwall.com/NSsp](sonicwall.com/NSsp)
Enterprise-Class Firewalls
As businesses evolve along with an increase in managed and unmanaged devices, networks, cloud workloads, SaaS applications, users, Internet speeds, and encrypted connections, a firewall that can’t support any one of these becomes a bottleneck. A firewall should be a source of strength and not a point of weakness. The SonicWall NSsp firewall’s multiple 100G/40G/25G/10G interfaces allow you to process several million simultaneous encrypted and unencrypted connections with unparallel threat prevention technology. With more than 70% of all sessions being encrypted, having a firewall that can process and examine this traffic without impacting the end user experience is critical to productivity and information security.

Deployed

Next-Generation Firewall (NGFW)
- Managed through a single pane of glass
- NSsp integrates with the rest of the SonicWall ecosystem of solutions
- Gain full visibility into your network to see what applications, devices, and users are doing to enforce policies as well as eliminate threats and bandwidth bottlenecks
- Integrate with Capture ATP with RTDMI for cloud-based sandboxing or Capture Security appliance for on-premise malware detection

Deep Packet Inspection of SSL/ TLS (DPI-SSL) for hidden threats
- The NSsp provides inspection for over millions of simultaneous TLS/SSL and SSH encrypted connections regardless of port or protocol
- Inclusion and exclusion rules allow customization based on specific organizational compliance and/or legal requirements
- Support for TLS cipher suites up to TLS 1.3

Segmentation and Networking
- Operate across several segmented networks, clouds, or service definitions, with unique templates, device groups, and policies across multiple devices and tenants
- MSSPs can also support multiple customers with a clean pipe along with unique policies

Advanced Threat Protection
- SonicWall Capture Advanced Threat Protection™ (ATP) is used by over 150,000 customers across the world through a variety of solutions and it helps to discover and stop over 1,200 new forms of malware each business day
- NSsp integrates with Capture Security appliance to detect and block unknown threats with on-premises sandboxing that uses Real-Time Deep Memory Inspection™ (RTDMI).

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

Content Filtering Services
- Compare requested web sites against a massive database in the cloud containing millions of rated URLs, IP addresses and web sites
- Create and apply policies that allow or deny access to sites based on individual or group identity, or by time of day, for over 50 pre-defined categories

The NSsp’s unified policy enables organizations to simply and intuitively create access and security policies in a single interface.

Simplified management and reporting
Ongoing management, monitoring and reporting of network activities are handled through the SonicWall Network Security Manager. This provides an intuitive dashboard for managing firewall operations as well as provide historical reports – from a single source. 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.
Intrusion Prevention System (IPS)

- Delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS.
- Designed to protect against application vulnerabilities as well as worms, trojans, and peer-to-peer, spyware and backdoor exploits.
- The extensible signature language provides proactive defense against newly discovered application and protocol vulnerabilities.
- SonicWall IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new attacks through SonicWall’s industry-leading Distributed Enforcement Architecture (DEA).

NSsp 13700

- Console Port
- 8 x 25/10/5/2.5 GbE Ports
- 4 x 10/5/2.5 GbE SFP/SFP+ Ports
- 16 x 1-GbE Ports
- 1 GbE Mgmt Ports
- 2 x 100/40–GbE SFP28 ports
- 4 x 10/5/2.5 GbE SFP/SFP+ Ports
- LCD display
- LCD controls
- Power button
- 512 GB Built-in Storage
- Expansion Slot (Up to 1TB)
- 3x Fans
- Power Adapters
- 10x fans
- Dual power supply

NSsp 15700

- Storage modules
- LCD display
- LCD controls
- Management Console
- 6x 100-GbE QSFP28 ports
- 4x 40-GbE QSFP+ ports
- 16x 10 GbE SFP+ ports
- 1 GbE Mgmt Ports
- 2 x 100/40–GbE SFP28 ports
- 4 x 10/5/2.5 GbE SFP/SFP+ Ports
- LCD display
- LCD controls
- Power button
- 512 GB Built-in Storage
- Expansion Slot (Up to 1TB)
- 3x Fans
- Power Adapters
- 10x fans
- Dual power supply

IoT and Application Control

- The NSsp catalogs thousands of applications through App Control and monitors their traffic for anomalous behavior.

SONICWALL®
## SonicWall NSsp 13700 and 15700 specifications

<table>
<thead>
<tr>
<th>Firewall General</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>SonicOS 7.0</td>
<td>SonicOSX 7.0</td>
</tr>
<tr>
<td>Interfaces</td>
<td>2x100/40-Gbe QSFPP28, 8x25/10/5/2.5-Gbe SFP28, 4x10/5/2.5-Gbe SFP+, 4x10/5/2.5/Gbe Cu, 16x1-Gbe 2 USB 3.0, 1 Console, 1 Mgmt. port</td>
<td>6 x 100-Gbe QSFPP28, 4 x 40-Gbe QSFPP+, 16 x 10 Gbe SFP+</td>
</tr>
<tr>
<td>Built-in storage</td>
<td>1.5 TB M.2</td>
<td>2 x 480 GB SSD</td>
</tr>
<tr>
<td>Management</td>
<td>CLI, SSH, Web UI, REST APIs</td>
<td></td>
</tr>
<tr>
<td>SSO Users</td>
<td>100,000</td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td>Analyzer, Local Log, Syslog, IPFIX, NetFlow</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firewall/VPN Performance</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall inspection throughput$^1$</td>
<td>60 Gbps</td>
<td>105 Gbps</td>
</tr>
<tr>
<td>Threat Prevention throughput$^2$</td>
<td>45.5 Gbps</td>
<td>82 Gbps</td>
</tr>
<tr>
<td>Application inspection throughput$^2$</td>
<td>57 Gbps</td>
<td>86 Gbps</td>
</tr>
<tr>
<td>IPS throughput$^3$</td>
<td>48 Gbps</td>
<td>76.5 Gbps</td>
</tr>
<tr>
<td>IMIX throughput</td>
<td>20 Gbps</td>
<td>28.5 Gbps</td>
</tr>
<tr>
<td>TLS/SSL inspection and decryption throughput (DPI SSL)$^2$</td>
<td>16.5 Gbps</td>
<td>21 Gbps</td>
</tr>
<tr>
<td>VPN throughput$^3$</td>
<td>29 Gbps</td>
<td>32 Gbps</td>
</tr>
<tr>
<td>Connections per second</td>
<td>170K</td>
<td>800K</td>
</tr>
<tr>
<td>Maximum connections (SPI)</td>
<td>14M</td>
<td>80M</td>
</tr>
<tr>
<td>Maximum connections (DPI)</td>
<td>12M</td>
<td>50M</td>
</tr>
<tr>
<td>Maximum connections (DPI SSL)</td>
<td>1.5M</td>
<td>3M</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VPN</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-to-site VPN tunnels</td>
<td>12,000</td>
<td>25,000</td>
</tr>
<tr>
<td>IPSec VPN clients (max)</td>
<td>2,000 (6,000)</td>
<td>2,000 (10,000)</td>
</tr>
<tr>
<td>SSL VPN licenses (max)</td>
<td>2 (3,000)</td>
<td></td>
</tr>
<tr>
<td>Encryption/authentication</td>
<td>DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography</td>
<td></td>
</tr>
<tr>
<td>Key exchange</td>
<td>Diffie Hellman Groups 1, 2, 5, 14v</td>
<td></td>
</tr>
<tr>
<td>Route-based VPN</td>
<td>RIP, OSPF, BGP</td>
<td></td>
</tr>
<tr>
<td>VPN features</td>
<td>Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN</td>
<td></td>
</tr>
<tr>
<td>Global VPN client platforms supported</td>
<td>Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10</td>
<td></td>
</tr>
<tr>
<td>NetExtender</td>
<td>Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE</td>
<td></td>
</tr>
<tr>
<td>Mobile Connect</td>
<td>Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Networking</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Instance Firewall</td>
<td>N/A</td>
<td>Max Tenants per Hardware: 12</td>
</tr>
<tr>
<td>IP address assignment</td>
<td>Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay</td>
<td></td>
</tr>
<tr>
<td>NAT modes</td>
<td>1:1, many:1, 1:many, flexible NAT (overlapping IP), PAT, transparent mode</td>
<td></td>
</tr>
<tr>
<td>VLAN interfaces</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>Wire Mode</td>
<td>–</td>
<td>Yes</td>
</tr>
<tr>
<td>Routing protocols</td>
<td>BGP4, OSPF, RIPV1/v2, static routes, policy-based routing</td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)</td>
<td></td>
</tr>
</tbody>
</table>
## SonicWall NSsp 13700 and 15700 specifications

<table>
<thead>
<tr>
<th>Networking</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td>LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)</td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong></td>
<td>Full H323-v1-5, SIP</td>
<td></td>
</tr>
<tr>
<td><strong>Standards</strong></td>
<td>TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3</td>
<td></td>
</tr>
<tr>
<td><strong>Certifications (in progress)</strong></td>
<td>FIPS 140-2 (with Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall and IPS)</td>
<td></td>
</tr>
<tr>
<td><strong>High availability</strong></td>
<td>Active/Passive with stateful synchronization</td>
<td></td>
</tr>
</tbody>
</table>

### Hardware

<table>
<thead>
<tr>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power supply</strong></td>
<td>2x350W</td>
</tr>
<tr>
<td><strong>Fans</strong></td>
<td>3 (removable)</td>
</tr>
<tr>
<td><strong>Input power</strong></td>
<td>100-240 VAC, 50-60 Hz</td>
</tr>
<tr>
<td><strong>Maximum power consumption (W)</strong></td>
<td>181.2</td>
</tr>
<tr>
<td><strong>Form factor</strong></td>
<td>1U Rack Mountable</td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td>43 x 32.5 x 4.5 (cm)</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>9.1 Kg</td>
</tr>
<tr>
<td><strong>WEEE weight</strong></td>
<td>11 Kg</td>
</tr>
<tr>
<td><strong>Shipping weight</strong></td>
<td>14.9 Kg</td>
</tr>
<tr>
<td><strong>Environment (Operating/Storage)</strong></td>
<td>32°-105°F (0°-40°C)/-40° to 158°F (-40° to 70°C)</td>
</tr>
<tr>
<td><strong>Humidity</strong></td>
<td>0-90% R.H non-condensing</td>
</tr>
</tbody>
</table>

### Regulatory

<table>
<thead>
<tr>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regulatory model numbers</strong></td>
<td>1RK54-118</td>
</tr>
<tr>
<td><strong>Major Regulatory</strong></td>
<td>FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, ANATEL, BSMI</td>
</tr>
</tbody>
</table>

1. Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.
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.
SonicOSX and SonicOS feature summary

Firewall
- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6 support
- Biometric authentication for remote access
- DNS proxy
- REST APIs
- SonicWall Switch integration
- Layer 7 rules:
  - Application Control
  - Single Pass Security Services enforcement
  - IPS/GAVAS/Capture ATP
- Rule management:
  - Cloning
  - Shadow rule analysis
  - In-cell editing
  - Group editing
- Managing views
  - Used/un-used rules
  - Active/in-active rules
- Sections

Unified Security Policy
- Unified Policy combines Layer 4 to Layer 7 rules:
  - Source/Destination IP/Port/Service
  - Application Control
  - CFS/Web Filtering
  - Single Pass Security Services enforcement
  - IPS/GAVAS/Capture ATP
- Rule management:
  - Cloning
  - Shadow rule analysis
  - In-cell editing
  - Group editing
- Managing views
  - Used/un-used rules
  - Active/in-active rules
- Sections

TLS/SSL/SSH decryption and inspection
- TLS 1.3
- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Granular DPI-SSL controls per zone or rule
- Decryption Policies for SSL/TLS and SSH

Capture advanced threat protection
- 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 integration

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

Application identification
- 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
- Cloud-based analytics

HTTP/HTTPS Web content filtering
- URL filtering
- Proxy avoidance
- Keyword blocking
- Policy-based filtering (exclusion/inclusion)
- HTTP header insertion
- Bandwidth manage CFS rating categories
- 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
- Multi-instance firewall (only on NSsp 15700)
- PortShield
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- Link aggregation (static and dynamic)
- Port redundancy
- A/IPv high availability with state sync
- Inbound/outbound load balancing
- High availability – Active/Standby with state sync
- Wire/virtual wire mode, tap mode, NAT mode
- Asymmetric routing

Voice over Internet Protocol (VoIP)
- Granular QoS control
- Bandwidth management
- DPI for VoIP traffic
- H.323 gatekeeper and SIP proxy support

Management and monitoring
- Web GUI
- Command line interface (CLI)
- Zero-Touch registration & provisioning
- Rest API
- SonicExpress mobile app support
Management and monitoring cont’d

- SNMPv2/v3
- Centralized management and reporting with SonicWall Network Security Manager (NSM)
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- Application and bandwidth visualization
- IPv4 and IPv6 management

1. Requires added subscription