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

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.

Deployment

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

Multi-instance Firewall (only for NSsp 15700)
- Multi-instance is the next generation of multi-tenancy
- Each tenant is isolated with dedicated compute resources to avoid resource starvation
- It features physical and logical ports/tenants
- It supports independent tenant policy and configuration management
- Leverage version independence and High Availability (HA) support for tenants

Wire Mode Functionality
- Bypass Mode for the quick and relatively non-interruptive introduction of firewall hardware into a network
- Inspect Mode to extend Bypass Mode without functionally altering the low-risk, zero latency packet path
- Secure Mode to actively interposing the firewall’s multi-core processors into the packet processing path
- Tap Mode to ingest a mirrored packet stream via a single switch port on the firewall, eliminating the need for physically intermediated insertion

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
**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)

**IoT and Application Control**

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

---

**NSsp 10700**

- 8 x 1-GbE Mgmt Ports
- 25/10/5/2.5-GbE QSFP+ Ports
- 4 x 10/5/2.5/1 Gb Cu Ports
- 16 x 1-GbE Port

---

**NSsp 11700**

- 8 x 1-GbE Mgmt Ports
- 25/10/5/2.5-GbE QSFP+ Ports
- 4 x 10/5/2.5/1 Gb Cu Ports
- 16 x 1-GbE Port
NSsp 13700

Console Port 16 x 1-GbE Ports
8 x 25/10/5/2.5-GbE Ports 4 x 10/5/2.5-GbE Cu Ports

1 GbE Mgmt USB 3.0 Port 2 x 100/40-GbE
4 x 10/5/2.5 GbE SFP/SFP+ Ports

Power button 1 TB SSD Storage Included
512GB M.2 Storage 3x Fans

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

Power button 10x fans Hot Swappable Power Adapters

512GB M.2 Storage 3x Fans
### SonicWall NSsp Series specifications

<table>
<thead>
<tr>
<th>Firewall General</th>
<th>NSsp 10700</th>
<th>NSsp 11700</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>SonicOS 7.0.1</td>
<td>SonicOS 7.0.1</td>
<td>SonicOS 7.0.1</td>
<td>SonicOSX 7.0</td>
</tr>
<tr>
<td>Interfaces</td>
<td>2x100G; 8x25G, 4x10G/5G/2.5G/1G (SFP+); 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GBe (Cu)</td>
<td>2x100G; 8x25G, 4x10G/5G/2.5G/1G (SFP+); 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GBe (Cu)</td>
<td>2x100G/40-Gbe QSFP28, 8x25/10/5/2.5-Gbe SFP28, 4x10/5/2.5-Gbe SFP+, 4x10/5/2.5/1-Gbe Cu, 16x1-Gbe Cu, 2 USB 3.0, 1 Console, 1 Mgmt. port</td>
<td>6 x 100-Gbe QSFP28, 4x40-Gbe QSFP+, 16 x 10 Ge SFP+</td>
</tr>
<tr>
<td>Total storage</td>
<td>1.5TB</td>
<td>1.5TB</td>
<td>1.5TB</td>
<td>2 x 480 GB SSD</td>
</tr>
<tr>
<td>Management</td>
<td>CLI, SSH, Web UI, REST APIs</td>
<td>CLI, SSH, Web UI, REST APIs</td>
<td>CLI, SSH, Web UI, REST APIs</td>
<td>CLI, SSH, Web UI, REST APIs</td>
</tr>
<tr>
<td>SSO Users</td>
<td>100,000</td>
<td>100,000</td>
<td>100,000</td>
<td>100,000</td>
</tr>
<tr>
<td>Access points supported (maximum)</td>
<td>512</td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
</tbody>
</table>

### Firewall/VPN Performance

<table>
<thead>
<tr>
<th>NSsp 10700</th>
<th>NSsp 11700</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall inspection throughput</td>
<td>42 Gbps</td>
<td>47 Gbps</td>
<td>60 Gbps</td>
</tr>
<tr>
<td>Threat Prevention throughput</td>
<td>27 Gbps</td>
<td>35 Gbps</td>
<td>45.5 Gbps</td>
</tr>
<tr>
<td>Application inspection throughput</td>
<td>30 Gbps</td>
<td>44 Gbps</td>
<td>57 Gbps</td>
</tr>
<tr>
<td>IPS throughput</td>
<td>28 Gbps</td>
<td>37 Gbps</td>
<td>48 Gbps</td>
</tr>
<tr>
<td>TLS/SSL inspection and decryption throughput (DPI SSL)</td>
<td>10 Gbps</td>
<td>11.5 Gbps</td>
<td>16.5 Gbps</td>
</tr>
<tr>
<td>VPN throughput</td>
<td>22.5 Gbps</td>
<td>26.7 Gbps</td>
<td>29 Gbps</td>
</tr>
<tr>
<td>Connections per second</td>
<td>280,000</td>
<td>280,000</td>
<td>280,000</td>
</tr>
<tr>
<td>Maximum connections (SPI)</td>
<td>15,000,000</td>
<td>20,000,000</td>
<td>25,000,000</td>
</tr>
<tr>
<td>Maximum connections (DPI)</td>
<td>12,000,000</td>
<td>17,000,000</td>
<td>22,000,000</td>
</tr>
<tr>
<td>Maximum connections (DPI SSL)</td>
<td>1,500,000</td>
<td>1,750,000</td>
<td>2,000,000</td>
</tr>
</tbody>
</table>

### VPN

<table>
<thead>
<tr>
<th>NSsp 10700</th>
<th>NSsp 11700</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-to-site VPN tunnels</td>
<td>6,000</td>
<td>12,000</td>
<td>12,000</td>
</tr>
<tr>
<td>IPSec VPN clients (max)</td>
<td>2000 (6000)</td>
<td>2000 (6000)</td>
<td>2000 (6000)</td>
</tr>
<tr>
<td>SSL VPN licenses (max)</td>
<td>2 (3000)</td>
<td>2 (3000)</td>
<td>2 (3000)</td>
</tr>
<tr>
<td>Encryption/authentication</td>
<td>DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA (1,256,384,512) Suite B Cryptography</td>
<td>DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography</td>
<td>DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography</td>
</tr>
<tr>
<td>Key exchange</td>
<td>Diffie Hellman Groups 1, 2, 5, 14v</td>
<td>Diffie Hellman Groups 1, 2, 5, 14v</td>
<td>Diffie Hellman Groups 1, 2, 5, 14v</td>
</tr>
<tr>
<td>Route-based VPN</td>
<td>RIP, OSPF, BGP</td>
<td>RIP, OSPF, BGP</td>
<td>RIP, OSPF, BGP</td>
</tr>
<tr>
<td>Certificate support</td>
<td>Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWall-to-SonicWall VPN, SCEP</td>
<td>Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWall-to-SonicWall VPN, SCEP</td>
<td>Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWall-to-SonicWall VPN, SCEP</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>Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN</td>
<td>Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN</td>
</tr>
</tbody>
</table>

### Networking

<table>
<thead>
<tr>
<th>NSsp 10700</th>
<th>NSsp 11700</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Instance Firewall</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>IP address assignment</td>
<td>Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay</td>
<td>Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay</td>
<td>Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay</td>
</tr>
</tbody>
</table>
# SonicWall NSsp Series specifications

## Networking

<table>
<thead>
<tr>
<th>Feature</th>
<th>NSsp 10700</th>
<th>NSsp 11700</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT modes</td>
<td>1:1, many:1, 1:many, flexible NAT (overlapping IP), PAT, transparent mode</td>
<td>1:1, many:1, 1:many, flexible NAT (overlapping IP), PAT, transparent mode</td>
<td>1:1, many:1, 1:many, flexible NAT (overlapping IP), PAT, transparent mode</td>
<td>1:1, many:1, 1:many, flexible NAT (overlapping IP), PAT, transparent mode</td>
</tr>
<tr>
<td>Logical VLAN and tunnel interfaces (maximum)</td>
<td>–</td>
<td>–</td>
<td>1024</td>
<td>–</td>
</tr>
<tr>
<td>Wire Mode</td>
<td>BGP4, OSPF, RIPv1/v2, static routes, policy-based routing</td>
<td>BGP4, OSPF, RIPv1/v2, static routes, policy-based routing</td>
<td>BGP4, OSPF, RIPv1/v2, static routes, policy-based routing</td>
<td>BGP, OSPF, RIPv1/v2, static routes, policy-based routing</td>
</tr>
<tr>
<td>Routing protocols</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>Yes</td>
</tr>
<tr>
<td>QoS</td>
<td>Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)</td>
<td>Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)</td>
<td>Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)</td>
<td>Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)</td>
</tr>
<tr>
<td>Authentication</td>
<td>LDAP (multiple domains), XAUTH/RADIUS, TACACS+, SSO, Radius accounting NTLM, internal user database, 2FA, Terminal Services, Citrix, Common Access Card (CAC)</td>
<td>LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)</td>
<td>LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)</td>
<td>LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)</td>
</tr>
<tr>
<td>Local user database</td>
<td>4,000</td>
<td>4,000</td>
<td>4,000</td>
<td>5,000</td>
</tr>
<tr>
<td>VoIP</td>
<td>Full H323-v1-5, SIP</td>
<td>Full H323-v1-5, SIP</td>
<td>Full H323-v1-5, SIP</td>
<td>Full H323-v1-5, SIP</td>
</tr>
<tr>
<td>Standards</td>
<td>TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3</td>
<td>TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3</td>
<td>TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3</td>
<td>TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3</td>
</tr>
<tr>
<td>Certifications (in progress)</td>
<td>FIPS 140-2 (with Suite B), UC APL, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall and IPS)</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>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>FIPS 140-2 (with Suite B), UC APL, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall and IPS)</td>
</tr>
<tr>
<td>High availability</td>
<td>Active/Passive with stateful synchronization</td>
<td>Active/Passive with stateful synchronization</td>
<td>Active/Passive with stateful synchronization</td>
<td>Active/Passive with stateful synchronization</td>
</tr>
</tbody>
</table>

## Hardware

<table>
<thead>
<tr>
<th>Feature</th>
<th>NSsp 10700</th>
<th>NSsp 11700</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply</td>
<td>2x350W</td>
<td>2x350W</td>
<td>2x350W</td>
<td>Dual, Redundant, 1,200W</td>
</tr>
<tr>
<td>Fans</td>
<td>3 (removable)</td>
<td>3 (removable)</td>
<td>3 (removable)</td>
<td>10</td>
</tr>
<tr>
<td>Redundant Power Supply</td>
<td>100-240 VAC, 50-60 Hz</td>
<td>100-240 VAC, 50-60 Hz</td>
<td>100-240 VAC, 50-60 Hz</td>
<td>100-240 VAC, 50-60 Hz</td>
</tr>
<tr>
<td>Maximum power consumption (W)</td>
<td>155.3</td>
<td>155.3</td>
<td>181.2</td>
<td>1135.0</td>
</tr>
<tr>
<td>Total heat dissipation</td>
<td>529.57 BTU</td>
<td>529.57 BTU</td>
<td>617.89 BTU</td>
<td>3870.35 BTU</td>
</tr>
<tr>
<td>Form factor</td>
<td>1U Rack Mountable</td>
<td>1U Rack Mountable</td>
<td>1U Rack Mountable</td>
<td>2U Rack Mountable</td>
</tr>
<tr>
<td>Dimensions</td>
<td>43 x 32.5 x 4.5 (cm) 16.9 x 12.8 x 1.8 in</td>
<td>43 x 32.5 x 4.5 (cm) 16.9 x 12.8 x 1.8 in</td>
<td>43 x 32.5 x 4.5 (cm) 16.9 x 12.8 x 1.8 in</td>
<td>68.6 x 43.8 x 8.8 (cm)</td>
</tr>
<tr>
<td>Weight</td>
<td>9.1 Kg</td>
<td>9.1 Kg</td>
<td>9.1 Kg</td>
<td>26 Kg</td>
</tr>
<tr>
<td>WEEE weight</td>
<td>11 Kg</td>
<td>11 Kg</td>
<td>11 Kg</td>
<td>30.1 Kg</td>
</tr>
<tr>
<td>Shipping weight</td>
<td>14.9 Kg</td>
<td>14.9 Kg</td>
<td>14.9 Kg</td>
<td>37.3 Kg</td>
</tr>
<tr>
<td>Environment (Operating/Storage)</td>
<td>32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)</td>
<td>32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)</td>
<td>32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)</td>
<td>32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)</td>
</tr>
<tr>
<td>Humidity</td>
<td>0-90% R.H non-condensing</td>
<td>0-90% R.H non-condensing</td>
<td>0-90% R.H non-condensing</td>
<td>10-95% non-condensing</td>
</tr>
</tbody>
</table>

## Regulatory

<table>
<thead>
<tr>
<th>Feature</th>
<th>NSsp 10700</th>
<th>NSsp 11700</th>
<th>NSsp 13700</th>
<th>NSsp 15700</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory model numbers</td>
<td>1RK54-118</td>
<td>1RK54-119</td>
<td>1RK54-118</td>
<td>2RK05-0FE</td>
</tr>
<tr>
<td>Major Regulatory</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>
<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>
<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>
<td>FCC Class A, ICES Class A, CE (EMC Class A, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico UL DGN notification, 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 with UDP traffic using 1418 byte packet size AESGCMAC16-256 Encryption 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

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/GAV/AS/Capture ATP
- Rule management:
  - Cloning
  - Shadow rule analysis
  - In-cell editing
  - Group editing
- Managing views
  - Used/Un-used rules
  - Active/Inactive 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

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 management 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/P 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

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)¹
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- Application and bandwidth visualization
- IPv4 and IPv6 management

¹ Requires added subscription