SONICWALL

SonicWall NSsp™ 15700 Datasheet

The SonicWall Network Security services platform™ (NSsp) 15700 is a next-generation firewall 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.

Enterprise-Class High-Speed Firewall

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 in the IT landscape. A firewall should be a source of strength and not a point of weakness.

The SonicWall NSsp 15700's multiple 100G/40G/10G interfaces allow you to process several million simultaneous encrypted and unencrypted connections with unparallel threat prevention technology. With 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 15700's unified policy interface enables organizations to simply and intuitively create access and security policies in a single unified interface.

Simplified management and reporting

Ongoing management, monitoring and reporting of network activities are handled through the SonicWall Network Security Manager (pending). 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.

SonicWall NSsp 15700 Benefits:

- High port density
- 100 GbE ports
- Multi-instance firewall
- Integrates with on-prem and cloud-based sandboxing
- Single pane of glass management through cloud or firewall
- Redundant power
- SonicOSX 7.0 support
- TLS 1.3 support
- Supports millions of simultaneous TLS connections
- Low TCO

Deployment

Next-Generation Firewall (NGFW)

- Managed through a single pane of glass
- NSsp 15700 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 15700 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

Mutli-Instance Firewall

- 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
- For compliance and performance-sensitive customers, the NSsp 15700 integrates with Capture Security appliance (CSa), a local device based on the memory-based file analysis technology, 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

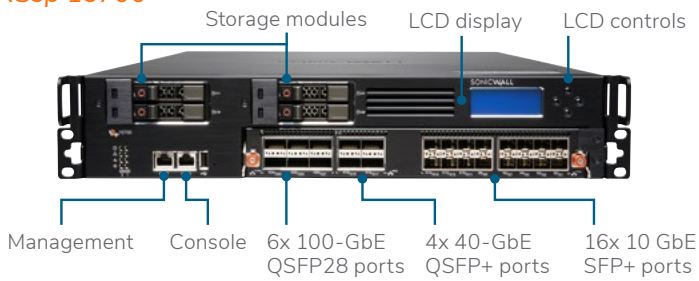
Intrusion Prevention System (IPS)

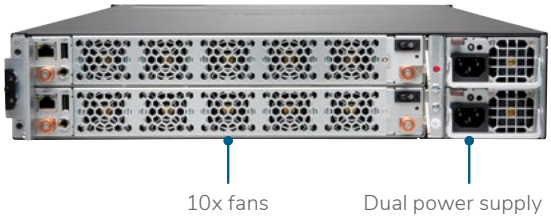
- Delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS
- Designed to protect against application vulnerabilities as well as worms, trojans, and peer-to-peer, spyware and backdoor 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 15700 catalogs thousands of applications through App Control and monitors their traffic for anomalous behavior through the on-board Application Firewall
- Segment managed from unmanaged devices with unique management and access profiles

NSsp 15700





SonicWall NSsp 15700 specifications

FIREWALL GENERAL	NSsp 15700
Operating System	SonicOSX 7
Interfaces	6 x 100-GbE QSFP28, 4 x 40-GbE QSFP+, 16 x 10 GbE SFP+
Built-in storage	2 x 480 GB SSD
Management	CLI, SSH, Web UI, REST APIs
SSO Users	100,000
Logging	Analyzer, Local Log, Syslog, IPFIX, NetFlow
FIREWALL/VPN PERFORMANCE	**NSsp 15700**
Firewall inspection throughput	105 Gbps
Threat Prevention throughput	82 Gbps
Application inspection throughput	86 Gbps
IPS throughput	76.5 Gbps
IMIX throughput	28.5 Gbps
TLS/SSL inspection and decryption throughput (DPI SSL)	21 Gbps
VPN throughput	32 Gbps
Connections per second	800k
Maximum connections (SPI)	80M
Maximum connections (DPI)	50M
Maximum connections (DPI SSL)	3M
VPN	**NSsp 15700**
Site-to-site VPN tunnels	25,000
IPSec VPN clients (maximum)	2,000 (10,000)
SSL VPN NetExtender clients (maximum)	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
VPN features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN
Global VPN client platforms supported	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
NetExtender	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
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)
NETWORKING	**NSsp 15700**
Multi-Instance Firewall	Max Tenants per Hardware: 12
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 IP), PAT, transparent mode
VLAN interfaces	512
Wire Mode	Yes
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing

SONICWALL®

SonicWall NSsp 15700 specifications

QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p
Authentication	LDAP, XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix
VoIP	Full H.323-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 15700
Power supply	Dual, Redundant, 1,200W
Fans	10
Input power	100-240 VAC, 50-60 Hz
Maximum power consumption (W)	1065
Form factor	2U Rack Mountable
Dimensions	68.6 x 43.8 x 8.8 (cm)
Weight	26 Kg
WEEE weight	30.1 Kg
Shipping weight	37.3 Kg
Shipping dimensions	28 x 63 x 86 (cm)
Major Regulatory	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
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)
Humidity	10-95% non-condensing

SonicOSX 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/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[2]

- 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[2]

- 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[2]

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

Application identification[2]

- 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[2]

- 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 architecture
- 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[1] (static and dynamic)
- Port redundancy[1]
- A/P high availability with state sync
- A/A clustering[1]
- 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
- SonicExpress mobile app support
- SNMPv2/v3
- Centralized management and reporting with SonicWall Global Management System (GMS)[2]
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat security analytics platform
- Application and bandwidth visualization
- IPv4 and IPv6 management

[1] Not supported on NSv Series firewalls
[2] Requires added subscription.

Product	SKU
SONICWALL NSSP 15700	02-SSC-2722
ESSENTIAL GATEWAY SECURITY SUITE BUNDLE FOR NSSP 15700 1YR	02-SSC-4739
ESSENTIAL GATEWAY SECURITY SUITE BUNDLE FOR NSSP 15700 3YR	02-SSC-4740
ESSENTIAL GATEWAY SECURITY SUITE BUNDLE FOR NSSP 15700 5YR	02-SSC-4741
24X7 SUPPORT FOR NSSP 15700 1YR	02-SSC-4733
24X7 SUPPORT FOR NSSP 15700 3YR	02-SSC-4734
24X7 SUPPORT FOR NSSP 15700 5YR	02-SSC-4735

Bundles	SKU
SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION 1YR	02-SSC-4764
SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION 3YR	02-SSC-4766
SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION 5YR	02-SSC-4765

Accessories	SKU
10GB-SR SFP+ SHORT REACH FIBER MODULE MULTI-MODE NO CABLE	01-SSC-9785
10GB-LR SFP+ LONG REACH FIBER MODULE SINGLE-MODE NO CABLE	01-SSC-9786
10GB SFP+ COPPER WITH 1M TWINAX CABLE	01-SSC-9787
10GB SFP+ COPPER WITH 3M TWINAX CABLE	01-SSC-9788
1GB-SX SFP SHORT HAUL FIBER MODULE MULTI-MODE NO CABLE	01-SSC-9789
1GB-LX SFP LONG HAUL FIBER MODULE SINGLE-MODE NO CABLE	01-SSC-9790
1GB-RJ45 SFP COPPER MODULE NO CABLE	01-SSC-9791
SONICWALL SFP+ 10GBASE-T TRANSCEIVER COPPER RJ45 MODULE	02-SSC-1874

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

© 2020 SonicWall Inc. ALL RIGHTS RESERVED. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Datasheet-NSsp15700-US-COG-2378