SONICWALL

Datenblatt zur SonicWall NSsp™ 15700

SonicWall Network Security Services™ (NSsp) 15700 ist eine Next-Generation Firewall-Plattform mit hoher Portdichte und schnellen Multi-Gigabit-Schnittstellen, über die mehrere Millionen Verbindungen verarbeitet und auf Zero-Day-Angriffe und komplexe Bedrohungen geprüft werden können. Diese speziell für große Konzerne, Hochschulen, Regierungsbehörden und MSSPs entwickelte Firewall eliminiert Angriffe in Echtzeit und ohne Beeinträchtigung der Performance. Sie zeichnet sich durch hohe Zuverlässigkeit aus und versorgt Organisationen unterbrechungsfrei mit Diensten.

Schnelle Firewall der Enterprise-Klasse

Im Rahmen ihrer laufenden Weiterentwicklung müssen Unternehmen mit einer konstant steigenden Zahl von verwalteten und nicht verwalteten Geräten, Netzwerken, Cloud-Workloads, SaaS-Anwendungen, Benutzern, Internetgeschwindigkeiten und verschlüsselten Verbindungen fertig werden. Wenn eine Firewall diese Bedingungen nicht ausreichend unterstützen kann, wird sie zum Engpass in der IT-Landschaft. Eine Firewall sollte aber eine Quelle der Kraft und Stärke sein und kein hinderlicher Schwachpunkt.

Die SonicWall NSsp 15700 bietet mehrere 100G/40G/10G-Schnittstellen, die zur gleichzeitigen Verarbeitung mehrerer Millionen verschlüsselter und nicht verschlüsselter Verbindungen fähig sind und eine unübertroffene Threat-Prevention-Technologie einsetzen. Angesichts der Tatsache, dass etwa 70 % aller Sessions verschlüsselt sind, ist es für die Erhaltung der Produktivität und Informationssicherheit von größter Wichtigkeit, dass eine Firewall diesen Verkehr ohne Beeinträchtigung der Endbenutzererfahrung verarbeiten und untersuchen kann.

Die einheitliche Regelschnittstelle der NSsp 15700 ermöglicht Organisationen die Erstellung von benutzerfreundlichen, intuitiven Zugangsmöglichkeiten und Sicherheitsrichtlinien über eine zentrale einheitliche Benutzeroberfläche.

Vereinfachtes Management und Reporting

Die laufende Verwaltung, Überwachung und Protokollierung von Netzwerkaktivitäten werden durch den SonicWall Network Security Manager (noch ausstehend) abgewickelt. Damit wird ein intuitives Dashboard bereitgestellt, über das Firewall-Funktionen verwaltet und Verlaufsberichte erstellt werden können – all das aus einer zentralen Quelle. Dank der einfachen Implementierung, Einrichtung und Verwaltung können Organisationen ihre TCO senken und von einem schnellen ROI profitieren.

Vorteile der SonicWall NSsp 15700:

- Hohe Portdichte
- 100-GbE-Ports
- Multi-Instance-Firewall
- Integration in On-Prem- und Cloud-basierte Sandboxen
- Bereit für die SD-Branch-Einbindung
- Verwaltung über eine zentrale Cloud- oder Firewall-basierte Benutzeroberfläche
- Integrierter und erweiterbarer Speicher
- Redundante Stromversorgung
- SonicOSX 7.0 Unterstützung
- TLS 1.3 Unterstützung
- Unterstützt Millionen von TLS-Verbindungen gleichzeitig
- Niedrige TCO

Implementierung

Next-Generation-Firewall (NGFW)

- Verwaltung von einer zentralen Konsole aus
- Leichte Integration der NSsp 15700 in das SonicWall-Ökosystem von Lösungen
- Volle Transparenz des Netzwerks mit Sicht darauf, wie Anwendungen, Geräte und Benutzer Richtlinien durchsetzen und Bedrohungen sowie Bandbreitenengpässe beseitigen
- Integration in Capture ATP mit RTDMI für Cloud-basiertes Sandboxing oder in die Capture Security Appliance für die On-Prem-Erkennung von Malware

Deep Packet Inspection des SSL/TLS (DPI-SSL) Verkehrs auf versteckte Bedrohungen

- Die NSsp 15700 ermöglicht die Inspektion von Millionen von gleichzeitigen TLS/SSL- und SSH-verschlüsselten Verbindungen unabhängig vom Port oder Protokoll
- Ein- und Ausschlussregeln ermöglichen die Anpassung auf Basis bestimmter organisatorischer Compliance- und/oder gesetzlicher Anforderungen
- Unterstützt TLS Cipher Suites bis TLS 1.3

Segmentierung und Netzwerke

- Betrieb über mehrere segmentierte Netzwerke, Clouds oder Servicedefiniti-onen hinweg, mit eindeutigen Vorlagen, Gerätegruppen und Richtlinien für mehrere Geräte und Mandanten
- MSSPs können auch mehrere Kunden mittels Clean-Pipe-Zugang und eindeutigen Richtlinien unterstützen

Multi-Instance-Firewall

- Multi-Instance ist die nächste Generation der Multi-Tenancy-Lösung
- Jeder Mandant wird mit dedizierten Rechnerressourcen isoliert, um einen Ressourcenmangel zu vermeiden
- Umfasst physische und logische Ports/Mandanten
- Unterstützt unabhängige Mandantenrichtlinien und Konfigurationsmanagement
- Nutzung von Versionsunabhängigkeit und High Availability (HA) Support für Mandanten

Wire-Modus-Funktionalität

- Bypass-Modus für die schnelle und relativ unterbrechungsfreie Einbindung von Firewall-Hardware in ein Netzwerk
- Inspect-Modus zur Erweiterung des Bypass-Modus ohne funktionelle Veränderung des risikoarmen, latenzfreien Paketpfads
- Secure-Modus für die aktive Zwischenschaltung der mehrkernigen Firewall-Prozessoren in den Paketverarbeitungspfad
- Tap-Modus für die Aufnahme eines wiedergespiegelten Paket-Streams über einen Switch-Port an der Firewall, wodurch die Notwendigkeit einer physischen Zwischeneinfügung eliminiert wird

Schutz vor komplexen Bedrohungen

- SonicWall Capture Advanced Threat Protection™ (ATP) wird von über 150.000 Kunden weltweit in einer Vielfalt von Lösungen eingesetzt und hilft diesen bei der Aufdeckung und Blockierung von über 1200 Formen von Malware an jedem Arbeitstag
- Bei Compliance- und Performance-sensiblen Kunden kann die NSsp 15700 mit der Capture Security Appliance (CSa) integriert werden. Diese lokale Appliance nutzt die im Arbeitsspeicher ausgeführte Dateianalysetechnologie Real-Time Deep Memory Inspection™ (RTDMI)

Capture Cloud-Plattform

- Die Capture Cloud-Plattform von SonicWall bietet kleinen wie großen Organisationen eine Cloud-basierte Lösung für Bedrohungsschutz und Netzwerkverwaltung sowie Reporting und Analysen

Content-Filtering-Services

- Die angeforderten Websites werden einem Vergleich gegen eine massive Datenbank in der Cloud unterzogen, die Millionen von bewerteten URLs, IP-Adressen und Websites enthält
- Ermöglicht die Erstellung und Anwendung von Richtlinien, die den Zugang zu Sites auf Basis individueller bzw. Gruppenidentität oder Tageszeit für über 50 vordefinierte Kategorien erlauben oder verweigern

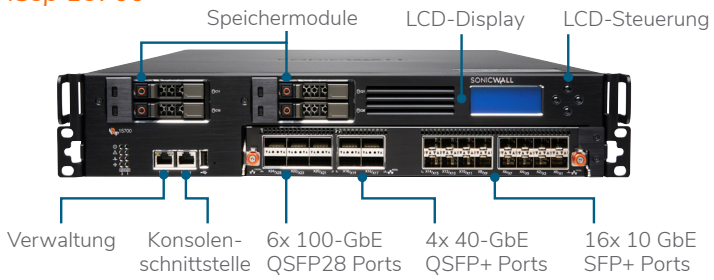
Intrusion-Prevention-System (IPS)

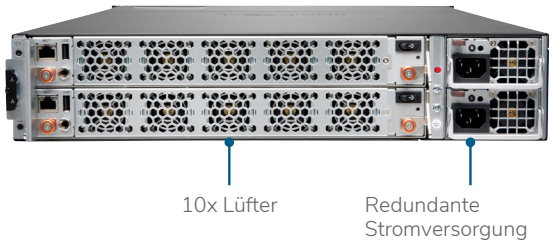
- Bietet eine konfigurierbare, leistungsstarke Deep Packet Inspection Engine für einen erweiterten Schutz von wichtigen Netzswerkdiensten, wie Web, E-Mail, Dateiübertragung, Windows Services und DNS
- Schützt vor Anwendungsschwachstellen und auch vor Würmern, Trojanern, Peer-to-Peer-Anwendungen, Spyware und Backdoor-Exploits
- Die erweiterbare Signaturdatenbank ermöglicht einen proaktiven Schutz von neu entdeckten Anwendungs- und Protokollschwachstellen
- SonicWall IPS eliminiert das kosten- und zeitaufwändige Pflegen und Aktualisieren von Signaturen für neue Attacken durch SonicWalls branchenführende Distributed Enforcement Architecture (DEA)

IoT und Anwendungskontrolle

- Die NSsp 15700 katalogisiert Tausende von Anwendungen mittels App Control und überwacht deren Verkehr über die integrierte Application-Firewall auf anomales Verhalten
- Segmentverwaltung von nicht verwalteten Geräten mit eindeutigen Management- und Zugangsprofilen

NSsp 15700





Technische Daten zur SonicWall NSsp 15700

FIREWALL ALLGEMEIN	NSsp 15700
Betriebssystem	SonicOSX 7
Schnittstellen	6x 100-GbE QSFP28, 4x 40-GbE QSFP+, 16x 10 GbE SFP+
Integrierter Speicher	2 x 480 GB SSD
Verwaltung	CLI, SSH, Web UI, REST APIs
SSO-Benutzer	100.000
Logging	Analyzer, lokale Logdatei, Syslog IPFIX, NetFlow
FIREWALL/VPN-PERFORMANCE	**NSsp 15700**
Firewall-Inspection-Durchsatz	105 GBit/s
Threat-Prevention-Durchsatz	82 GBit/s
Application-Inspection-Durchsatz	86 GBit/s
IPS-Durchsatz	76,5 GBit/s
IMIX-Durchsatz	28,5 GBit/s
Durchsatz bei TLS/SSL-Prüfung und -Entschlüsselung (DPI-SSL)	21 GBit/s
VPN-Durchsatz	32 GBit/s
Verbindungen pro Sekunde	800k
Maximale Anzahl von Verbindungen (SPI)	80M
Maximale Anzahl von Verbindungen (DPI)	50M
Maximale Anzahl von Verbindungen (DPI-SSL)	3M
VPN	**NSsp 15700**
Site-to-Site-VPN-Tunnel	25.000
IPSec-VPN-Clients (max.)	2.000 (10.000)
SSL-VPN-NetExtender-Clients (max.)	2 (3.000)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14v
Routenbasiertes VPN	RIP, OSPF, BGP
VPN-Funktionen	Dead Peer Detection, DHCP über VPN, IPSec-NAT-Traversal, redundantes VPN-Gateway, routenbasiertes VPN
Unterstützte globale VPN-Client-Plattformen	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 (integriert)
NETZWERK	**NSsp 15700**
Multi-Instance-Firewall	Maximale Mandantenzahl pro Hardware: 12
IP-Adressenzuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IP), PAT, transparenter Modus
VLAN-Schnittstellen	512
Wire-Modus	Ja
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing

Technische Daten zur SonicWall NSsp 15700

QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p
Authentifizierung	LDAP, XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix
VoIP	Volle Unterstützung für H.323-v1-5, SIP
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3
Zertifizierungen (in Bearbeitung)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall und IPS), UC APL, USGv6, CsFC
Hochverfügbarkeit	Active/Passive mit State Sync, Active/Active-DPI mit State-Sync, Active/Active-Clustering
HARDWARE	NSsp 15700
Netzteil	Zwei, redundant, 1.200 W
Lüfter	10
Eingangsspannung	100–240 V AC, 50–60 Hz
Maximaler Stromverbrauch (W)	1065
Formfaktor	Rackfähig (2 HE)
Abmessungen	68,6 x 43,8 x 8,8 (cm)
Gewicht	26 kg
WEEE-Gewicht	30,1 kg
Versandgewicht	37,3 kg
Versandabmessungen	28 x 63 x 86 (cm)
Erfüllt folgende Normen	FCC Klasse A, ICES Klasse A, CE (EMC Klasse A, LVD, RoHS), C-Tick, VCCI Klasse A, MSIP/KCC Klasse A, UL, cUL, TUV/GS, CB, Mexico UL DGN Notification, WEEE, REACH, ANATEL, BSMI
Umgebung (Betrieb/Lagerung)	0 bis 40 °C/-40 bis 70 °C
Luftfeuchtigkeit	10 bis 95 %, nicht kondensierend

Die SonicOSX Funktionen im Überblick

Firewall

- Stateful Packet Inspection
- Reassembly-Free Deep Packet Inspection
- Schutz vor DDoS-Angriffen (UDP-/ICMP-/SYN-Flood)
- IPv4-/IPv6-Unterstützung
- Biometrische Authentifizierung für den Remote-Zugriff
- DNS-Proxy
- REST-APIs
- SonicWall Switch-Integration

Einheitliche Sicherheitsrichtlinie

- Die einheitliche Richtlinie beinhaltet Regeln der Ebenen 4 bis 7:
  - Ursprungs-/Ziel-IP/Port/Service
  - Anwendungskontrolle
  - CFS/Web-Filterung
  - Single Pass Security Services-Durchsetzung
  - IPS/GAV/AS/Capture ATP
- Regelmanagement:
  - Cloning
  - Schattenregel-Analyse
  - Zelleninterne Bearbeitung
  - Gruppenbearbeitung
- Verwaltung der Ansichten
  - Verwendete/nicht verwendete Regeln
  - Aktive/inaktive Regeln
  - Abschnitte

TSL/SSL/SSH-Entschlüsselung und -Prüfung

- TLS 1.3
- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL-Steuerung
- Granulare DPI-SSL-Kontrollen nach Zone oder Regel
- Entschlüsselungsrichtlinien für SSL/TLS und SSH

Capture Advanced Threat Protection[2]

- Real-Time Deep Memory Inspection
- Cloud-basierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Dateiübermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client-Integration

Intrusion-Prevention[2]

- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- GeoIP-Durchsetzung
- Botnet-Filtering mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware[2]

- Streambasierte Malware-Scans
- Gateway-Antivirus
- Spyware-Schutz am Gateway
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- Cloud-basierte Malware-Datenbank

Anwendungsidentifizierung[2]

- Anwendungskontrolle
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Umfassende Anwendungssignaturen-datenbank

Visualisierung und Analyse des Datenverkehrs

- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung
- Cloud-basierte Analysen

Filterung von HTTP-/HTTPS-Webinhalten[2]

- URL-Filterung
- Vermeidung von Proxys
- Blockieren mithilfe von Schlüsselwörtern
- Richtlinienbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Ratingkategorien
- Content Filtering Client

VPN

- Auto-Provisioning für VPNs
- IPSec-VPN für Site-to-Site-Konnektivität
- Remote-Zugriff per SSL-VPN und IPSec-Client
- Redundantes VPN-Gateway
- Mobile Connect für iOS, Mac OS X, Windows, Chrome, Android und Kindle Fire
- Routenbasiertes VPN (OSPF, RIP, BGP)

Netzwerk

- Multi-Instance-Architektur
- PortShield
- Jumbo-Frames
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Portspiegelung
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- Regelbasiertes Routing (ToS/metrisch und ECMP)
- NAT
- DHCP-Server
- Bandbreitenverwaltung
- Link-Aggregation[1] (statisch und dynamisch)
- Port-Redundanz[1]
- Hochverfügbarkeitsmodus A/P mit State-Sync
- A/A-Clustering[1]
- Lastausgleich für ein- und ausgehenden Datenverkehr
- Hochverfügbarkeit – Active/Standby mit State-Sync
- Wire/Virtual Wire-Modus, Tap-Modus, NAT-Modus
- Asymmetrisches Routing

VoIP

- Granulare QoS-Kontrolle
- Bandbreitenverwaltung
- DPI für VoIP-Datenverkehr
- H.323-Gatekeeper- und SIP-Proxy-Support

Verwaltung und Überwachung

- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- Registrierung und Bereitstellung mittels Zero Touch-Deployment
- Support für mobile SonicExpress-Apps
- SNMPv2/v3
- Zentralisierte Verwaltung und zentrales Reporting mittels SonicWall Global Management System (GMS)[2]
- Logging
- NetFlow-/IPFIX-Export
- Cloud-basiertes Konfigurationsbackup
- BlueCoat Security Analytics Plattform
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung

[1] Wird auf NSv Series Firewalls nicht unterstützt
[2] Erfordert zusätzliches Abo.

Produkt	Artikelnummer
SONICWALL NSSP 15700	02-SSC-2722
ESSENTIAL GATEWAY SECURITY SUITE BÜNDEL FÜR NSSP 15700 1 JAHR	02-SSC-4739
ESSENTIAL GATEWAY SECURITY SUITE BÜNDEL FÜR NSSP 15700 3 JAHRE	02-SSC-4740
ESSENTIAL GATEWAY SECURITY SUITE BÜNDEL FÜR NSSP 15700 5 JAHRE	02-SSC-4741
24/7 SUPPORT FÜR NSSP 15700 1 JAHR	02-SSC-4733
24/7 SUPPORT FÜR NSSP 15700 3 JAHRE	02-SSC-4734
24/7 SUPPORT FÜR NSSP 15700 5 JAHRE	02-SSC-4735

Bündel	Artikelnummer
SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION 1 JAHR	02-SSC-4764
SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION 3 JAHRE	02-SSC-4766
SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION 5 JAHRE	02-SSC-4765

Zubehör	Artikelnummer
10GB-SR SFP+ KURZSTRECKEN-FASERMODUL MULTI-MODE OHNE KABEL	01-SSC-9785
10GB-LR SFP+ LANGSTRECKEN-FASERMODUL MULTI-MODE OHNE KABEL	01-SSC-9786
10GB SFP+ KUPFER MIT 1M TWINAX-KABEL	01-SSC-9787
10GB SFP+ KUPFER MIT 3M TWINAX-KABEL	01-SSC-9788
1GB-SX SFP NAHVERKEHR-FASERMODUL MULTI-MODE OHNE KABEL	01-SSC-9789
1GB-LX SFP FERNVERKEHR-FASERMODUL MULTI-MODE OHNE KABEL	01-SSC-9790
1GB-RJ45 SFP KUPFERMODUL OHNE KABEL	01-SSC-9791
SONICWALL SFP+ 10GBASE-T TRANSCEIVER KUPFER RJ45-MODUL	02-SSC-1874

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

Datasheet-NSsp15700-US-COG-2378