SONICWALL

SonicWall NSsp™ 15700
数据表

作为下一代防火墙，SonicWall 网络安全服务平台™ (NSsp) 15700 支持高端口密度和速度可达数 Gbps 的接口，因此能够处理数以百万计的连接以应对零日攻击威胁和高级威胁。该产品专为大型企业、高等教育机构，政府机构和托管安全服务提供商 (MSSP) 而设计，能够实时消除攻击而不会拖慢性能。它采用了高可靠性设计，可向组织提供绝无间断的服务。

企业级高速防火墙

随着企业的发展，托管和非托管设备、网络、云工作负载、SaaS 应用程序、用户、互联网速度和加密连接也在增加，如果防火墙不能为其中的任何一种提供支持，就会成为 IT 环境中的瓶颈。防火墙应该是力量的源泉，而不是弱点。

借助 SonicWall NSsp 15700 的多重 100G/40G/10G 接口，您可以利用无与伦比的威胁防御技术同时处理数以百万计的加密和非加密连接。由于在所有会话中有 70% 经过加密，因此拥有一个能够在不影响最终用户体验的情况下处理和检查此类流量的防火墙对于工作效率和信息安全都至关重要。

利用 NSsp 15700 的统一策略界面，组织可以在单个统一界面中简单而直观地创建访问和安全策略。

简化管理和报告

网络活动的持续管理、监控和报告均通过 SonicWall Network Security Manager 处理（待定）。这提供了一个直观的仪表板用于管理防火墙操作，也提供了来自单一来源的历史报告。该产品的部署和设置都得到了简化，而且易于管理，使得组织能够降低总体拥有成本，并实现高投资回报。

SonicWall NSsp 15700 的优势：

- 高端口密度
- 100 Gb 以太网端口
- 多实例防火墙
- 与内部和云端沙箱集成
- 支持软件定义的分支 (SD-Branch)
- 通过云或防火墙实现单一管理平台管理
- 内置和可扩展的存储
- 冗余能力
- SonicOSX 7.0 支持
- TLS 1.3 支持
- 同时支持数以百万计的 TLS 连接
- 低总体拥有成本

部署

下一代防火墙 (NGFW)

- 通过单一管理平台进行管理
- NSsp 15700 与 SonicWall 解决方案生态系统中的其他产品相集成
- 获得对您的网络的完全可见性，用于查看应用程序、设备和用户正在实施哪些操作，以便执行策略以及消除威胁和带宽瓶颈
- 与 Capture ATP 和 RTDMI 集成，供云端沙箱或 Capture 安全设备用于在内部检测恶意软件

针对隐蔽威胁的 SSL/TLS 深度数据包检测 (DPI-SSL)

- NSsp 15700 可以检查超过数百万个同时存在的 TLS/SSL 和 SSH 加密连接，而无需考虑相应的端口或协议
- 借助包含和排除规则，可以基于特定的组织合规需求和/或法律需求进行定制
- 支持多种 TLS 密码套件（最高可至 TLS 1.3）

分段和联网

- 在多个设备和租户间使用独特的模板、设备组和策略跨多个分段网络、云或服务定义执行操作
- MSSP 还可以通过一条安全的通信管道和独特的策略支持多个客户

多实例防火墙

- 多实例是下一代的多租户技术
- 每个租户都实现了隔离，拥有自己的专用计算资源，可避免资源短缺
- 它采用了物理和逻辑端口/租户
- 它支持独立的租户策略和配置管理
- 利用面向租户的版本独立性和高可用性 (HA) 支持

有线模式功能

- 旁路模式可快速且相对无中断地将防火墙硬件引入网络中
- 检查模式无需在功能上改变低风险、零延迟的数据包路径便可对旁路模式进行扩展
- 安全模式可以主动将防火墙的多核处理器插入到数据包处理路径中
- 分接模式可以通过防火墙上的单个交换机端口接收镜像数据包流，无需以物理方式在中间插入

高级威胁防护

- SonicWall Capture Advanced Threat Protection™ (ATP) 通过各种解决方案供全世界超过 15 万名客户使用，每个工作日都能帮助他们发现和阻止超过 1,200 种新的恶意软件形式
- 为了服务于对合规性和性能敏感的客户，NSsp 15700 与 Capture 安全设备 (Csa) 相集成，后者是一种采用 Real-Time Deep Memory Inspection™ (RTDMI) 这一基于内存的文件分析技术的本地设备

Capture 云平台

- SonicWall 的 CAPTURE 云平台可为任何规模的企业提供基于云的威胁防御和网络管理以及报告与分析。

内容过滤服务

- 将所请求的网站与云端的庞大数据库进行比较，该数据库中包含数以百万计的已评定 URL、IP 地址和网站
- 为超过 50 个预定义的类别创建和应用策略，这些策略将基于个人或群组的身份或者按一天中的时间允许或拒绝访问网站

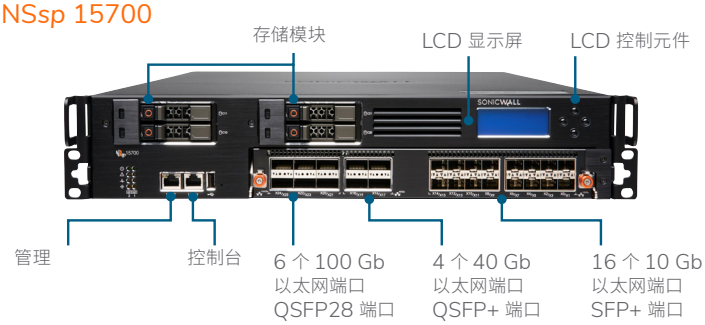
入侵防御系统 (IPS)

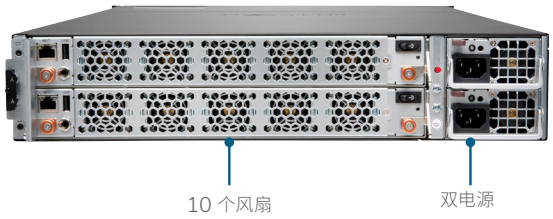
- 提供一个可以配置的高性能深度数据包检查引擎，以便对诸如 Web、电子邮件、文件传输、Windows 服务和 DNS 等关键网络服务进行更广泛的保护
- 用于防止应用程序漏洞以及蠕虫、木马、点对点传输、间谍软件和后门攻击
- 可扩展签名语言可针对新发现的应用程序和协议漏洞提供主动防御
- 通过 SonicWall 行业领先的分布式强制实施架构 (DEA)，SonicWall IPS 可以免除因维护和更新签名而产生的昂贵耗时的负担，从容应对新的攻击。

物联网 (IoT) 和应用程序控制

- NSsp 15700 通过应用程序控制对数以千计的应用程序进行编目，并通过板载的应用程序防火墙监控它们的流量以检测异常行为
- 使用独特的管理和访问配置文件从非托管设备管理分段

NSsp 15700





SonicWall NSsp 15700 规格

防火墙一般信息	NSsp 15700
操作系统	SonicOSX 7
接口	6 个 100 Gb QSFP28 以太网端口，4 个 40 Gb QSFP+ 以太网端口，16 个 10 Gb SFP+ 以太网端口
内置存储	2 个 480 GB 固态硬盘
管理	CLI、SSH、Web 用户界面、REST API
SSO 用户	100,000
日志记录	分析器、本地日志、Syslog、IPFIX、NetFlow
防火墙/VPN 性能	**NSsp 15700**
防火墙检查吞吐量	105 Gbps
威胁防御吞吐量	82 Gbps
应用程序检查吞吐量	86 Gbps
IPS 吞吐量	76.5 Gbps
IMIX 吞吐量	28.5 Gbps
TLS/SSL 检查和解密吞吐量 (DPI SSL)	21 Gbps
VPN 吞吐量	32 Gbps
每秒连接数	800k
最大连接数 (SPI)	80M
最大连接数 (DPI)	50M
最大连接数 (DPI SSL)	3M
VPN	**NSsp 15700**
站点到站点 VPN 隧道	25,000
IPSec VPN 客户端（最大）	2,000 (10,000)
SSL VPN NetExtender 客户端（最大）	2 (3,000)
加密/身份验证	DES、3DES、AES（128、192、256 位）/MD5、SHA-1、Suite B Cryptography
密钥交换	Diffie Hellman 组 1、2、5、14v
基于路由的 VPN	RIP、OSPF、BGP
VPN 功能	失效对端检测、VPN 上的 DHCP、IPSec NAT 遍历、冗余的 VPN 网关、基于路由的 VPN
支持的全球 VPN 客户端平台	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（嵌入版）
联网	**NSsp 15700**
多实例防火墙	每硬件最大租户数量：12
IP 地址分配	静态（DHCP、PPPoE、L2TP 和 PPTP 客户端）、内部 DHCP 服务器、DHCP 中继
NAT 模式	一对一、多对一、一对多、灵活的 NAT（重叠 IP）、PAT、透明模式
VLAN 接口	512
有线模式	是
路由协议	BGP、OSPF、RIPv1/v2、静态路由、基于策略的路由
QoS	带宽优先级、最大带宽、有保障带宽、DSCP 标记、802.1p

SonicWall NSsp 15700 规格

身份验证	LDAP、XAUTH/RADIUS、SSO、Novell、内部用户数据库、终端服务、Citrix
VoIP	全 H.323-v1-5、SIP
标准	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、PPPoE、L2TP、PPTP、RADIUS、IEEE 802.3
认证（进行中）	ICSA 防火墙、ICSA 防病毒软件、FIPS 140-2、Common Criteria NDPP（防火墙和 IPS）、UC APL、USGv6、CsFC
高可用性	主动/被动（包括状态同步）、主动/主动 DPI（包括状态同步）、主动/主动集群
硬件	**NSsp 15700**
电源	冗余式双电源，1,200W
风扇	10
输入功率	100-240 VAC，50-60 Hz
最大功耗 (W)	1065
外形规格	2U 机架（可安装）
尺寸	68.6 x 43.8 x 8.8 (cm)
重量	26 Kg
WEEE 重量	30.1 Kg
装运重量	37.3 Kg
装运尺寸	28 x 63 x 86 (cm)
主要监管标准	FCC A 类、ICES A 类、CE（EMC A 类、LVD、RoHS）、C-Tick、VCCI A 类、MSIP/KCC A 类、UL、cUL、TUV/GS、CB、墨西哥 UL DGN 通知、WEEE、REACH、ANATEL、BSMI
环境（操作/储藏）	32° 至 105°F（0° 至 40°C）/-40° 至 158°F（-40°至 70°C）
湿度	10-95%，无凝结

SonicOSX 功能摘要

防火墙

- 有状态数据包检查
- 免重组深度包检测
- DDoS 攻击防护 (UDP/ICMP/SYN 洪水攻击)
- IPv4/IPv6 支持
- 面向远程访问的生物身份验证
- DNS 代理
- REST API
- SonicWall 交换机集成

统一安全策略

- 统一策略整合了第 4 层到第 7 层的规则:
  - 来源/目标 IP/端口/服务
  - 应用程序控制
  - CFS/Web 过滤
  - 单通道安全服务强制实施
  - IPS/GAV/AS/Capture ATP
- 规则管理:
  - 克隆
  - 影子规则分析
  - 单元格内编辑
  - 群组编辑
- 管理视图
  - 已使用/未使用的规则
  - 活动/活动中的规则
  - 分区

TLS/SSL/SSH 解密和检查

- TLS 1.3
- 针对 TLS/SSL/SSH 的深度数据包检查
- 包含/排除对象、群组或主机名
- SSL 控制
- 按区域或规则精细控制 DPI-SSL
- 针对 SSL/TLS 和 SSH 的解密策略

Capture 高级威胁防护[2]

- Real-Time Deep Memory Inspection
- 云端多引擎分析
- 虚拟化沙箱
- 虚拟机监控程序级分析
- 全系统模拟
- 广泛的文件类型检查
- 自动和手动提交
- 实时威胁情报更新
- 在裁决前进行阻止
- Capture Client 集成

入侵防御[2]

- 基于签名的扫描
- 自动签名更新
- 双向检测
- 精细的 IPS 规则功能
- GeoIP 强制实施
- 利用动态列表过滤僵尸网络
- 正则表达式匹配

反恶意软件[2]

- 基于数据流的恶意软件扫描
- 网关防病毒软件
- 网关反间谍软件
- 双向检测
- 不限制文件大小
- 云端恶意软件数据库

应用程序识别[2]

- 应用程序控制
- 应用程序带宽管理
- 创建定制的应用程序签名
- 防止数据泄露
- 通过 NetFlow/IPFIX 进行应用程序报告
- 综合式应用程序签名数据库

流量可视化和分析

- 用户活动
- 应用程序/带宽/威胁使用情况
- 云端分析

HTTP/HTTPS Web 内容过滤[2]

- URL 过滤
- 代理规避
- 关键字拦截
- 基于策略的过滤 (排除/包含)
- HTTP 标头插入
- 带宽管理 CFS 评级类别
- 内容过滤客户端

VPN

- 自动配置 VPN
- 用于站点到站点连接的 IPSec VPN
- SSL VPN 和 IPSec 客户端远程访问
- 冗余的 VPN 网关
- Mobile Connect for iOS、Mac OS X、Windows、Chrome、Android 和 Kindle Fire
- 基于路由的 VPN (OSPF、RIP、BGP)

联网

- 多实例体系结构
- PortShield
- 巨型帧
- 路径 MTU 发现
- 增强日志记录
- VLAN 中继
- 端口镜像
- 第 2 层 QoS
- 端口安全
- 动态路由 (RIP/OSPF/BGP)
- 基于策略的路由 (ToS/metric 和 ECMP)
- NAT
- DHCP 服务器
- 带宽管理
- 链路聚合[1] (静态和动态)
- 端口冗余性[1]
- 主动/被动 (A/P) 高可用性 (包括状态同步)
- A/A 集群[1]
- 入站/出站负载平衡
- 高可用性 - 主动/备用 (包括状态同步)
- 有线/虚拟有线模式、分接模式、NAT 模式
- 非对称路由

VoIP

- 精细 QoS 控制
- 带宽管理
- 用于 VoIP 流量的 DPI
- H.323 Gatekeeper 和 SIP 代理支持

管理和监控

- Web 图形用户界面
- 命令行界面 (CLI)
- 零接触注册与配置
- SonicExpress 移动应用程序支持
- SNMPv2/v3
- 利用 SonicWall Global Management System (GMS)[2] 进行集中化管理和报告
- 日志记录
- Netflow/IPFix 导出
- 云端配置备份
- BlueCoat 安全分析平台
- 应用程序和带宽可视化
- IPv4 和 IPv6 管理

[1] Nsvv 系列防火墙对此不提供支持
[2] 需要额外订阅。

产品	SKU
SONICWALL NSSP 15700	02-SSC-2722
NSSP 15700 基本网关安全套件捆绑包（1 年）	02-SSC-4739
NSSP 15700 基本网关安全套件捆绑包（3 年）	02-SSC-4740
NSSP 15700 基本网关安全套件捆绑包（5 年）	02-SSC-4741
针对 NSSP 15700 的全天候支持（1 年）	02-SSC-4733
针对 NSSP 15700 的全天候支持（3 年）	02-SSC-4734
针对 NSSP 15700 的全天候支持（5 年）	02-SSC-4735

捆绑包	SKU
SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION（1 年）	02-SSC-4764
SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION（3 年）	02-SSC-4766
SONICWALL NSSP 15700 TOTALSECURE ESSENTIAL EDITION（5 年）	02-SSC-4765

配件	SKU
10GB-SR SFP+ 短程光纤模块，多模式，不带电缆	01-SSC-9785
10GB-LR SFP+ 长程光纤模块，单模式，不带电缆	01-SSC-9786
10GB SFP+ 铜制模块，带 1 米双轴电缆	01-SSC-9787
10GB SFP+ 铜制模块，带 3 米双轴电缆	01-SSC-9788
1GB-SX SFP 短程光纤模块，多模式，不带电缆	01-SSC-9789
1GB-LX SFP 长程光纤模块，单模式，不带电缆	01-SSC-9790
1GB-RJ45 SFP 铜制模块，不带电缆	01-SSC-9791
SONICWALL SFP+ 10GBASE-T 收发器铜制 RJ45 模块	02-SSC-1874

关于 SonicWall

SonicWall 为超分布式时代和每个人都远程办公、每个人都移动办公、每个人都不太安全的工作现实提供了 Boundless Cybersecurity。通过了解未知、提供实时可见性并实现经济学突破，SonicWall 为世界各地的大型企业、政府和中小企业弥补了网络安全业务缺口。有关详情，请访问 www.sonicwall.com。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
有关详情，请访问我们的网站。
www.sonicwall.com

Datasheet-NSsp15700-US-COG-2378