网络安全设备系列

下一代防火墙

如今，企业在安全领域面临着前所未有的挑战。攻击复杂度和数量呈现指数级增长，导致企业资料、个人信息和客户数据丢失，知识产权被盗，名誉受损，生产力下降。同时，安全形势也日趋复杂。企业一直在努力解决 BYOD 变革以及联网个人设备的爆炸式增长所带来的问题。个人智能手机和平板电脑降低了网络性能和生产力，移动应用如社交媒体和视频流耗费了大量的带宽。为了解决这些网络安全和生产力挑战，部分企业选择关闭部分安全功能，来保持网络性能。

但现在，企业可以在不影响网络性能的情况下保持安全性和生产力。Dell™ SonicWALL™网络安全设备（NSA）系列下一代防火墙（NGFW）在保持网络性能的同时实现了优异的网络安全。该系列提供了一流的安全和性能，与旗舰产品 SuperMassive 下一代防火墙产品线使用了相同的架构。另外，NSA 系列还提供了 Dell 产品备受赞誉的易用性和高价值。

NSA 系列是基于多年的研发成果打造出来的，专为分布式企业、中小型企业、分支机构、校园和政府机构全新设计，在极具扩展性的设计架构中融合了极具创新意义的多核架构和荣获专利的免重组深度包检测（RFDPI®）*单通道威胁防御引擎。该产品为企业提供了业界领先的安全防护、性能和可扩展性，并支持大量并发连接，实现了低延迟，每秒处理的连接数很高，没有文件大小限制。备受推崇的独立第三方测试机构对 NSA 系列防火墙技术进行了评估，并给予了高度评价。

与其它竞争性的传统防火墙和入侵防御技术不同，NSA 系列会检测所有流量，不考虑端口或协议。凭借业界最高的后台 SSL 解密速率，NSA 系列可阻止各种先进的恶意软件。该系列的验证服务器通过细粒度应用控制，实现了带宽管理，提高了生产力，有效地执行了可接受的用户策略。不同于传统的、不支持威胁信息共享的双盒解决方案，NSA 系列集成了防火墙和 IPS，这种互联智能功能通过策略决策强化了安全效率，同时降低了管理负担和企业风险。

此外，NSA 系列防火墙提供了基于网络的恶意软件防护，并支持云援助功能，为企业提供了必不可少的基本防御层，可抵御数百万种恶意软件变体。

优点：

- 同类最佳安全保护
- 多核架构
- 超高性能
- 入侵防御
- 基于网络的反恶意软件
- 安全远程访问
- 安全无线
- URL 过滤
- 网关反垃圾邮件
- 应用控制
- 集中化管理

NSA 系列防火墙的管理非常简单，且符合成本效益，因为它们支持 Dell 公司屡获殊荣的全球管理系统（GMS）平台，该平台可通过单一的虚拟控制台管理数百乃至数千台 Dell SonicWALL 防火墙。全面的实时可视化功能可提供完整的机上和机下报告，清楚显示网络中发生的事情。

*美国专利 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Dell SonicWALL NSA 系列下一代防火墙（NGFW）采用了最新的多核硬件设计和免重组深度包检测技术保护网络远离内部和外部攻击，且不对性能构成影响。NSA 系列融合了入侵防御、内容和 URL 检测、应用智能和控制、高可用性以及其它一些先进的网络功能。

网络安全设备 NSA 220 和 220 Wireless-N

Dell SonicWALL NSA 220 为中小型企业和分支机构提供了深度的前线安全、应用和用户控制、网络生产力以及可选的 802.11n 双频无线功能。

防火墙	NSA 220 和 220 W
防火墙吞吐量	600 Mbps
IPS 吞吐量	195 Mbps
反恶意软件吞吐量	115 Mbps
全 DPI 吞吐量	110 Mbps
IMIX 吞吐量	180 Mbps
最大 DPI 连接	85,000
每秒新建连接	32,000

描述	NSA 220 和 220 W
仅指 NSA 220 防火墙	01-SSC-9750
仅指 NSA 220 Wireless-N 防火墙	01-SSC-9752
NSA 220 TotalSecure（1 年）	01-SSC-9744
NSA 220 Wireless-N TotalSecure（1 年）	01-SSC-9746
综合网关安全套件（1 年）	01-SSC-4648
网关反恶意软件/IPS（1 年）	01-SSC-4612
全天候 7x24 小时动态支持（1 年）	01-SSC-4630

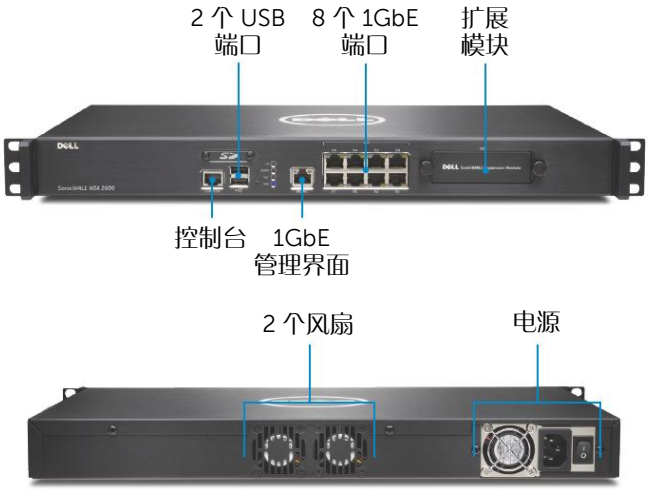
网络安全设备 NSA 250M 和 250M Wireless-N

Dell SonicWALL NSA 250M 为分支机构和分布式企业提供了深度的前线安全、应用和用户控制、网络生产力、专用模块扩展槽，以及可选的 802.11n 双频无线功能。

防火墙	NSA 250M 和 250M W
防火墙吞吐量	750 Mbps
IPS 吞吐量	250 Mbps
反恶意软件吞吐量	140 Mbps
全 DPI 吞吐量	130 Mbps
IMIX 吞吐量	210 Mbps
最大 DPI 连接	110,000
每秒新建连接	64,000

描述	NSA 250M 和 250M W
仅指 NSA 250M 防火墙	01-SSC-9755
仅指 NSA 250M Wireless-N 防火墙	01-SSC-9757
NSA 250M TotalSecure（1 年）	01-SSC-9747
NSA 250M Wireless-N TotalSecure（1 年）	01-SSC-9749
综合网关安全套件（1 年）	01-SSC-4606
网关反恶意软件/IPS（1 年）	01-SSC-4570
全天候 7x24 小时动态支持（1 年）	01-SSC-4588

网络安全设备 NSA 2600

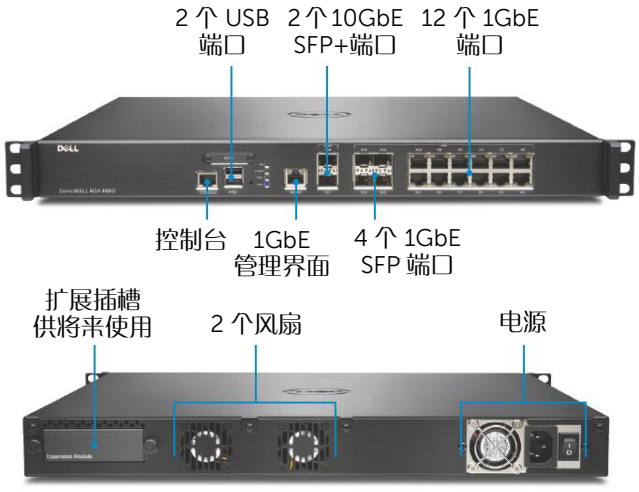


Dell SonicWALL NSA 2600 旨在解决成长型小企业、分支机构和校园的需求。

防火墙	NSA 2600
防火墙吞吐量	1.9 Gbps
IPS 吞吐量	700 Mbps
反恶意软件吞吐量	400 Mbps
全 DPI 吞吐量	300 Mbps
IMIX 吞吐量	600 Mbps
最大 DPI 连接	125,000
每秒新建连接	15,000

描述	SKU
仅指 NSA 2600 防火墙	01-SSC-3860
NSA 2600 TotalSecure（1 年）	01-SSC-3863
综合网关安全套件（1 年）	01-SSC-4453
网关反恶意软件/IPS（1 年）	01-SSC-4459
银级全天候 7x24 小时技术支持（1 年）	01-SSC-4314

网络安全设备 NSA 3600/4600

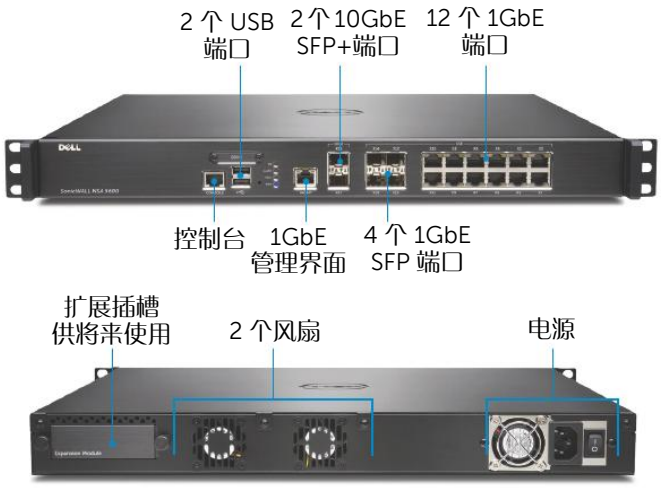


Dell SonicWALL NSA 3600/4600 尤为适合非常重视吞吐量和性能的分支机构和中小型企业环境。

防火墙	NSA 3600	NSA 4600
防火墙吞吐量	3.4 Gbps	6.0 Gbps
IPS 吞吐量	1.1 Gbps	2.0 Gbps
反恶意软件吞吐量	600 Mbps	1.1 Gbps
全 DPI 吞吐量	500 Mbps	800 Mbps
IMIX 吞吐量	900 Mbps	1.6 Gbps
最大 DPI 连接	175,000	200,000
每秒新建连接	20,000	40,000

描述	NSA 3600	NSA 4600
仅指防火墙	01-SSC-3850	01-SSC-3840
TotalSecure（1 年）	01-SSC-3853	01-SSC-3843
综合网关安全套件（1 年）	01-SSC-4429	01-SSC-4405
网关反恶意软件/IPS（1 年）	01-SSC-4435	01-SSC-4411
银级全天候 7x24 小时技术支持（1 年）	01-SSC-4302	01-SSC-4290

网络安全设备 NSA 5600

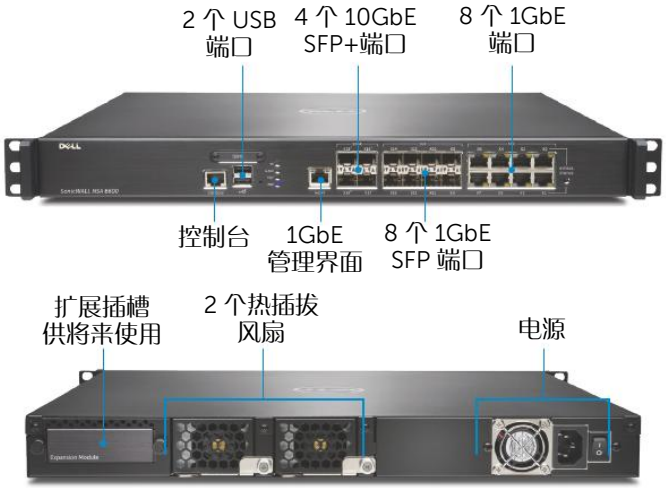


Dell SonicWALL NSA 5600 尤为适合对吞吐量要求极高的分布式企业、分支机构和企业环境。

防火墙	NSA 5600
防火墙吞吐量	9.0 Gbps
IPS 吞吐量	3.0 Gbps
反恶意软件吞吐量	1.7 Gbps
全 DPI 吞吐量	1.6 Gbps
IMIX 吞吐量	2.4 Gbps
最大 DPI 连接	500,000
每秒新建连接	60,000

描述	SKU
仅指 NSA 5600 防火墙	01-SSC-3830
NSA 5600 TotalSecure（1 年）	01-SSC-3833
综合网关安全套件（1 年）	01-SSC-4234
网关反恶意软件/IPS（1 年）	01-SSC-4240
金级全天候 7x24 小时技术支持（1 年）	01-SSC-4284

网络安全设备 NSA 6600



Dell SonicWALL NSA 6600 尤为适合对吞吐量和性能要求严苛的大型分布式企业和中央站点环境。

防火墙	NSA 6600
防火墙吞吐量	12.0 Gbps
IPS 吞吐量	4.5 Gbps
反恶意软件吞吐量	3.0 Gbps
全 DPI 吞吐量	3.0 Gbps
IMIX 吞吐量	3.5 Gbps
最大 DPI 连接	500,000
每秒新建连接	90,000

描述	SKU
仅指 NSA 6600 防火墙	01-SSC-3820
NSA 6600 TotalSecure（1 年）	01-SSC-3823
综合网关安全套件（1 年）	01-SSC-4210
网关反恶意软件/IPS（1 年）	01-SSC-4216
金级全天候 7x24 小时技术支持（1 年）	01-SSC-4278

实现深层次网络安全

Dell SonicWALL NSA 系列防火墙可为各种规模的企业提供深度网络安全。该系列采用了可扩展的多核硬件架构以及单通道、低延迟免重组深度包检测（RFDPI®）专利引擎，该引擎可扫描每个数据包的每个字节，同时保持网络的高性能。Dell SonicWALL NSA 系列比其它防火墙更为优异，它集成了支持实时 SSL 解密和检测的 RFDPI 引擎、具备先进反逃避技术的入侵防御系统（IPS），以及可利用云能力的基于网络的恶意软件防护系统。如今，企业在新型威胁出现时即可对其进行阻止。

据估计，SSL 加密导致企业对三分之一的网络流量视而不见。Dell SonicWALL NSA 系列的 SSL 解密和检测技术让 RFDPI 引擎可解密和检测每个端口上的所有网络流量。

如今，每隔一个小时就有新的恶意软件变体产生。Dell SonicWALL NSA 系列利用基于网络的恶意软件防护，让您可了解这些威胁的最新信息。该防护功能充分利用了不断更新的云数据库的能力，该库现包括超过 1300 万种恶意软件变体。

Dell SonicWALL 入侵防御服务（IPS）可帮助企业远离一系列基于网络的应用漏洞和漏洞利用程序。每天都会出现新的应用漏洞，使得 IPS 更新程序成为保持安全防护、远离新生威胁的至关重要的工具。Dell SonicWALL 大大超越了具备先进反逃避技术的入侵防御系统的传统解决方案，可扫描所有网络流量，检测蠕虫、木马、软件漏洞、后门漏洞利用程序和其它恶意攻击类型。通常，网络罪犯会试图使用复杂的算法来逃避检测，避开 IPS。Dell NGFW 提供了先进的威胁防御功能，在攻击对企业造成损害之前对隐藏攻击进行解码。通过集中关注已知的恶意流量，Dell SonicWALL IPS 可过滤掉主动错误信息，同时提高网络可靠性和性能。Dell SonicWALL IPS 旨在抵御内部和外部威胁，可监控网络流量，查找恶意或异常行为，然后根据预先制定的策略阻止或记录流量。

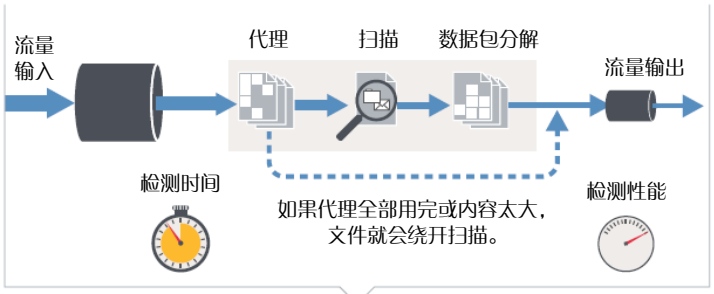
免重组深度包检测引擎

Dell SonicWALL 免重组深度包检测（RFDPI）引擎提供了出色的威胁防护和应用控制能力，且不会对性能造成影响。该引擎采用的是应用流流量有效载荷检测功能来探测 3-7 层的威胁，会让网络流接受大量重复的合规化和解密程序，以此抵御试图干扰检测引擎，然后偷偷向网络发送恶意代码的高级逃避技术。

一旦数据包经过了必需的预处理，包括 SSL 解密，即可分析出数据包是否有以下三种签名数据库的单一专用记忆表征：入侵攻击、恶意软件和应用。然后上报连接状态，显示与这些数据库有关的数据流的位置，直至提示出现攻击状态，或其它“匹配”事件，此时将采取预设行为。

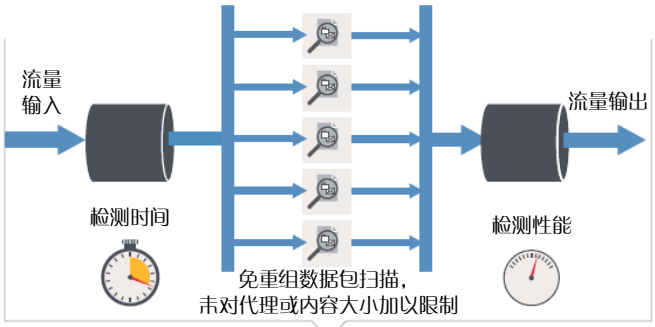
大多数情况下，连接会立即终止，随后创建正确的日志和通知事件。然而，该引擎也可配置成“仅用于检测”，或是，如果出现应用检测，只要应用得到确认，可为余下的应用流提供 7 层带宽管理服务。

数据包组装过程



一般架构

数据包免重组过程

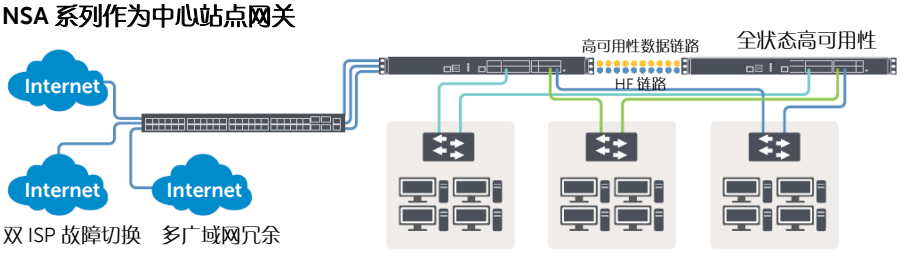


Dell SonicWALL 架构

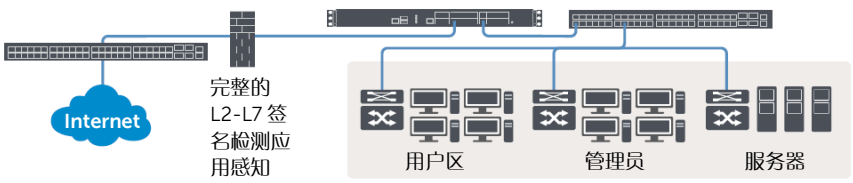
灵活和可自定义的部署选项 — NSA 系列一览

每台 Dell SonicWALL NSA 设备都采用了具突破意义的多核硬件设计和免重组深度包检测功能，在不影响网络性能的情况下实现了内部和外部网络保护。NSA 系列 NGFW 融合了高速入侵防御、文件和内容检测、支持大量先进的网络和灵活配置功能的强大的应用智能和控制功能。

NSA 系列作为中心站点网关



NSA 系列作为内联的 NGFW 解决方案

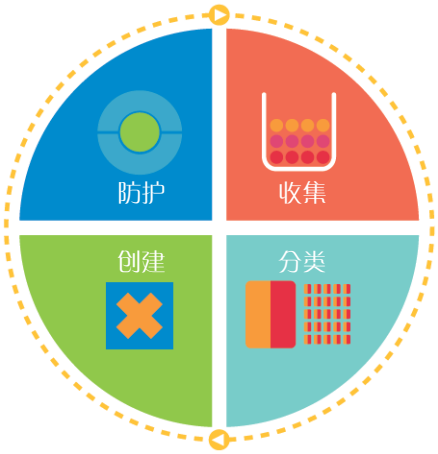


安全和防护

Dell SonicWALL 企业内部专门成立的 Dell SonicWALL 威胁研究团队正致力于研发可部署于现场防火墙的防御措施，以获得最新的安全防护能力。该团队在全球采用了超过 100 万个传感器，来收集恶意软件样本，并对最新威胁信息进行遥测反馈，这些信息随后会集成到入侵防御、反恶意软件和应用检测系统。

Dell SonicWALL NGFW 客户可获得不断升级的全天候威胁防御能力，新的更新软件会立即生效，无需重启，亦不会造成业务中断。设备上的签名旨在抵御各种攻击类型，包含数以万计的、拥有单一签名的单独威胁。

除设备的防御措施外，NSA 设备还可访问 Dell SonicWALL CloudAV Service（基于云的防病毒服务）。Dell SonicWALL CloudAV Service 包含 1200 多万个签名，增强了机载智能签名功能。防火墙可通过专用的轻量协议来访问 CloudAV 数据库，强化设备的检测能力。利用 Geo-IP 和僵尸网络过滤功能，Dell SonicWALL NGFW 可阻止来自危险域或整个区域的流量，降低网络的风险预测。

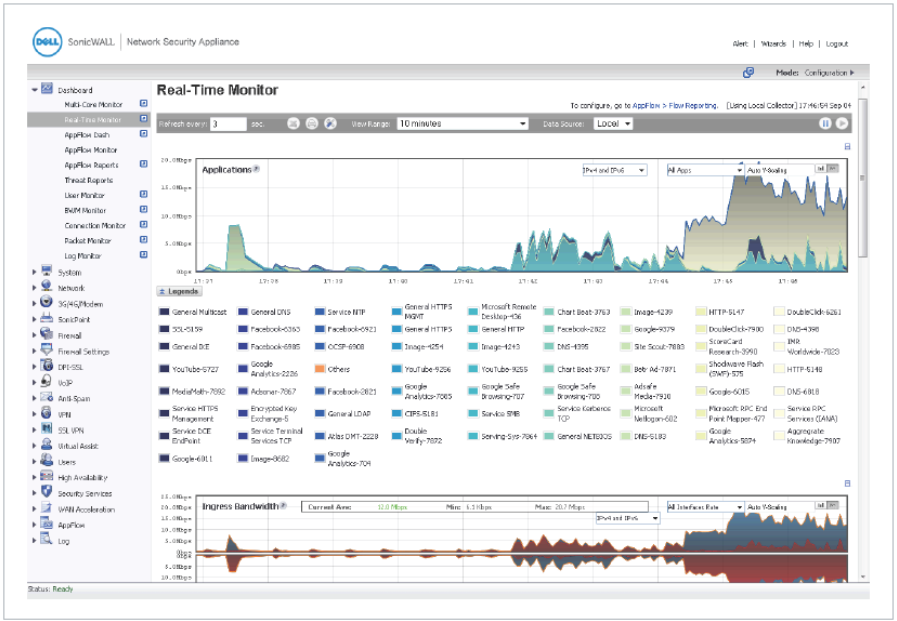


应用智能和控制

应用智能功能会通知管理员有关跨越网络的应用流量的信息，以便他们可根据业务优先级安排应用控制，遏制非生产力应用和阻止具有潜在危险的应用。实时可视化功能可识别流量异常，立即启动防御措施，阻止入站或出站攻击或预防性能瓶颈。

Dell SonicWALL 应用流量分析提供了有关应用流量、带宽利用率和安全威胁的深入细致的信息，以及强大的故障解决能力和取证能力。此外，安全的单点登录（SSO）功能简化了用户体验，提高了生产力，减少了服务台呼叫次数。

Dell SonicWALL 全球管理系统（GMS®）通过直观的 web 化界面简化了应用智能和控制管理。



功能

RFDPI 引擎	
功能	**描述**
免重组深度包检测（RFDPI）	这款荣获专利的高性能检测引擎可基于数据流进行双向流量分析，不采用代理或缓冲，用于查找入侵尝试、恶意软件，并对应用流量（不管其端口所在）进行识别。
双向检测	可同时扫描入站和出站流量中的威胁，确保网络未被利用来发布恶意软件，即使是网络中出现感染设备时也不会成为发布攻击的平台。
基于数据流的检测	较少使用代理和非缓冲的检测技术为处理数百万并发网络流量的 DPI 提供了超低延迟性能，没有文件和数据流大小方面的限制，可用于通用协议和原始 TCP 数据流。
高度并行、可扩展	RFDPI 引擎的独特设计配合多核架构，可提供高 DPI 吞吐量以及极高的新会话创建速率，来处理要求严苛的网络的流量尖峰。
单通道检测	单通道 DPI 架构可同时扫描恶意软件、入侵尝试，并进行应用识别，大大降低了 DPI 延迟，确保所有威胁信息在一个架构内都是相互关联的。

入侵防御	
功能	**描述**
基于防御措施的安全防护	紧密集成的入侵防御系统（IPS）可利用签名和其它防御措施来扫描数据包有效负载，查找漏洞和漏洞利用程序，覆盖了大量攻击和漏洞。
自动签名更新	Dell SonicWALL 威胁研究团队将不断深入研究，将更新程序添加至广泛的 IPS 防御措施列表中，该表目前纳入了 50 多种攻击类别。新的更新程序可立即生效，无需重启，亦不会造成业务中断。
区内 IPS 保护	通过将网络分为多个支持入侵防御的安全区域，增强了内部安全防护，阻止威胁在区域边界散布。
僵尸网络命令和控制（CnC）检测和阻止	识别和阻止源自本地网 bots 的命令和控制流量发送到已被确认为正在发布恶意软件或是已知 CnC 点的 IP 和域。
协议滥用/异常检测和防御	识别和阻止会滥用协议以偷偷躲避 IPS 的攻击。
零天攻击防御	利用针对最新漏洞利用方法和技术（包括数千种漏洞利用程序）的不断更新的更新程序，保护网络远离零时攻击。
反逃避技术	广泛的数据流合规化、解密和其它技术确保威胁不会在 2-7 层利用逃避技术在未经检测的情况下进入网络。

功能

威胁防御	
功能	**描述**
基于网络的恶意软件防护	Dell SonicWALL RFDPI 引擎可扫描所有入站、出站和区内流量，在经所有端口传输的和 TCP 数据流的长度和大小不限的文件中查找病毒、木马、键盘记录程序和其它恶意软件。
CloudAssist 恶意软件保护	位于 Dell SonicWALL 云服务器的不断更新的数据库，包含 1200 多万种威胁签名，以此为基准，可增强机载签名数据库的功能，使 RFDPI 能识别并抵御大量威胁。
全天候安全更新	Dell SonicWALL 威胁研究团队可对新威胁进行分析，并每周 7 天、每天 24 小时不间断地发布防御措施。新的威胁更新程序将自动发送至支持主动安全服务的防火墙，程序将立即生效，无需重启，亦不会造成业务中断。
SSL 解密和检测	解密和检测传输过程中的 SSL 流量，不采用代理，即可查找恶意软件、入侵尝试和数据泄露，然后采用应用、URL 和内容控制策略，抵御 SSL 加密流量中隐藏的威胁。
双向原始 TCP 检测	RFDPI 引擎可双向扫描任何端口上的原始 TCP 数据流，阻止试图悄悄穿越传统安全系统（这类系统主要用于保障少数已知端口的安全）的攻击。
广泛的协议支持	可识别通用协议如 HTTP/S、FTP、SMTP、SMBv1/v2 和其它不会在原始 TCP 中发送数据的协议，解密有效负载来检测恶意软件，即使它们未基于标准的已知端口运行。

应用智能和控制	
功能	**描述**
应用控制	控制应用，或单种应用功能，RFDPI 引擎可根据不断扩展的、现包含 4300 多种应用签名的数据库来识别这些应用或功能，提高网络安全性，增强网络生产力。
自定义应用识别	根据网络通信中某一应用特有的参数或格式来创建自定义签名，控制自定义应用，实现对网络的进一步控制。
应用带宽管理	限制或优先处理某些应用或应用类别，以最大限度地提高关键应用的可用带宽，同时消除或减少不需要的应用流量。
On-box/off-box 流量可视化	利用 NetFlow/IPFix 的实时 on-box 应用流量可视化和 off-box 应用流量报告功能，识别带宽利用率，分析网络行为。
细粒度控制	根据调度表、用户组、排除列表和一系列行为（通过集成 LDAP/AD/Terminal Services/Citrix，支持 SSO 用户识别），控制应用，或应用的特定组件。

功能

防火墙和网络	
功能	**描述**
状态包检测	检测和分析所有网络流量，使其满足防火墙访问策略。
DDoS/DoS 攻击防御	SYN 泛滥保护功能使用了 3 层 SYN 代理程序和 2 层 SYN 黑名单技术，实现了对 DOS 攻击的防御。此外，它可经 UDP/ICMP 泛滥保护和连接速率限制来抵御 DOS/DDoS 攻击。
灵活的部署选项	NSA 系列可采用传统 NAT、2 层桥接、有线模式和网络触摸模式部署。
高可用性/集群	NSA 系列支持具备状态同步化功能的 Active/Passive、Active/Active DPI 和 Active/Active 集群高可用性模式。Active/Active DPI 可将深度包检测负载卸载到无源设备的核心，以提高吞吐量。
广域网负载均衡	使用基于轮循（Round Robin）、Spillover 或 Percentage 的方法对多个广域网接口进行负载均衡。
基于策略的路由	根据协议创建路由，将流量发送至优先广域网连接，一旦出现运行中断，可及时转移至备用广域网。
高级 QoS	利用 802.1p 和 DSCP 标签和重新映射网络中的 VoIP 流量，确保关键的业务通信。
H.323 网守和 SIP 代理支持	要求所有入站呼叫都必须经过 H.323 网守或 SIP 代理程序的验证，防止垃圾呼叫。

管理和报告	
功能	**描述**
全球管理系统（GMS）	采用 Dell SonicWALL GMS，可经单个界面直观的管理控制台监控、配置和报告多台 Dell SonicWALL 设备的情况，以降低管理成本和复杂性。
强大的单设备管理	除提供了全面的 CLI 和 SNMPv2/3 支持外，直观的 web 化界面实现了快速、方便的部署。
IPFIX/NetFlow 应用流报告	可经由 IPFIX 或 NetFlow 协议导出应用流量分析和使用率数据，利用 Dell SonicWALL Scrutinizer 或其它支持带扩展的 IPFIX 和 NetFlow 的工具来检测和报告实时和历史数据。

虚拟专用网	
功能	**描述**
支持站对站连接的 IPSec VPN	高性能 IPSec VPN 让 NSA 系列可用作数千个大型网站、分支机构或家庭办公室的 VPN 集线器。
SSL VPN 或 IPSec 客户端远程访问	利用无客户端 SSL VPN 技术或易于管理的 IPSec 客户端，经各种平台轻松访问电子邮件、文件、电脑、内联网和应用。
冗余 VPN 网关	使用多个广域网时，主要的和备用的 VPN 可配置来支持所有 VPN 会话的无缝的自动故障转移和故障恢复。
基于路由的 VPN	可经 VPN 链接执行动态路由，经替换路线无缝重新传输流量，确保出现临时性 VPN 信道故障时的连续正常运行时间。

功能

内容/上下文感知

功能	描述
用户行为追踪	通过无缝集成 AD/LDAP/Citrix/Terminal Services SSO，配合通过 DPI 获取的大量信息，实现用户识别和行为追踪。
GeoIP 国家流量识别	识别和控制发送至或源自特定国家的网络流量，抵御来自已知或可疑威胁行为源的攻击，或调查来自该网络的可疑流量。
定期表达式 DPI 过滤	通过定期的表达式匹配，识别和控制经网络传输的内容，避免数据泄露。

SonicOS 功能概述

防火墙
- 免重组深度包检测
- SSL 的深度包检测
- 状态包检测
- TCP 重组
- 秘密模式
- 通用访问卡（CAC）支持
- DOS 攻击防御
- UDP/ICMP/SYN 泛滥保护

入侵防御
- 基于签名的扫描
- 自动签名更新
- 出站威胁防御
- IPS 例外列表
- 基于 GeoIP 和声誉的过滤
- 定期表达式匹配

反恶意软件
- 基于数据流的恶意软件扫描
- 网关防病毒
- 网关反间谍软件
- SSL 解密
- 双向检测
- 无文件大小限制
- CloudAV 威胁数据库

应用控制
- 应用控制
- 应用组件阻塞
- 应用带宽管理
- 自定义应用签名创建
- 应用流量可视化
- 数据泄露防御
- 经 NetFlow/IPFIX 进行应用报告
- 用户行为追踪（SSO）
- 全面的应用签名数据库

Web 内容过滤
- URL 过滤
- 反代理程序技术
- 关键字阻塞
- 带宽管理 CFS 速率分类
- 带应用控制功能的统一策略模式
- 56 种内容过滤类别

VPN
- 支持站对站连接的 IPSec VPN
- SSL VPN 或 IPSec 客户端远程访问
- 冗余 VPN 网关
- 针对 iOS 和 Android™设备的 Mobile Connect
- 基于路由的 VPN（OSPF, RIP）

网络
- 动态路由
- SonicPoint 无线控制器
- 基于策略的路由
- 高级 NAT
- DHCP 服务器
- 带宽管理
- 链路聚合
- 端口冗余
- 支持状态同步化的 A/P 高可用性
- A/A 集群
- 入站/出站负载均衡
- L2 桥接、有线模式、触摸模式、NAT 模式

VoIP
- 高级 QoS
- 带宽管理
- VoIP 流量的 DPI
- H.323 网守和 SIP 代理支持

管理和监控
- Web GUI
- 命令行界面（CLI）
- SNMPv2/v3
- Off-Box 报告（Scrutinizer）
- 集中化管理和报告
- 日志
- Netflow/IPFix 导出
- 应用流量可视化
- 集中化策略管理
- 单点登录（SSO）
- Terminal Service/Citrix Support
- Solera Networks Forensics 集成

NSA 系列系统规格

	NSA 220/W	NSA 250M/W
操作系统	SonicOS 5.9	
安全核心	2 个	
1GbE 接口	7 个 1GbE 接口	5 个 1GbE 接口
管理界面	CLI, SSH, GUI, GMS	
内存（RAM）	512 MB	512 MB
扩展	2 个 USB，SD 卡	1 个模块接口，2 个 USB，SD 卡
防火墙检测吞吐量 [1]	600 Mbps	750 Mbps
全 DPI 吞吐量 [2]	110 Mbps	130 Mbps
应用检测吞吐量 [2]	195 Mbps	250 Mbps
IPS 吞吐量 [2]	195 Mbps	250 Mbps
反恶意软件检测吞吐量 [2]	115 Mbps	140 Mbps
IMIX 吞吐量 [3]	180 Mbps	210 Mbps
VPN 吞吐量 [3]	150 Mbps	200 Mbps
每秒连接数	2,200	3,000
最大连接（SPI）	85,000	110,000
最大连接（DPI）	32,000	64,000
可支持的 SonicPoints 数量（最大数量）	16	16
单点登录（SSO）用户	250	250[4]
VPN	**NSA 220/W**	**NSA 250M/W**
点对点隧道	25	50
IPSec VPN 客户端（最大数量）	2（25）	2（25）
SSL VPN 许可证（最大数量）	2（15）	2（15）
加密/验证	DES, 3DES, AES（128、192、256 位）/MD5, SHA-1	
密钥交换	Diffie Hellman Groups 1, 2, 5, 14	
基于路由的 VPN	RIP, OSPF	
网络	**NSA 220/W**	**NSA 250M/W**
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	1 对 1，多对 1，1 对多，灵活的 NAT（重复的 IPS），PAT，透明模式	
VLAN 接口	25	35
路由协议	BGP，OSPF，RIPv1/v2，静态路由，基于策略的路由，组播	
QoS	带宽优先级、最大带宽、保证带宽、DSCP 标记、802.1p	
认证	XAUTH/RADIUS，活动目录，SSO，LDAP，Novell，内部用户数据库，终端服务，Citrix	
VoIP	全 H323-v1-5，SIP	
标准	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3	
认证	VPNC，ICSA 防火墙，ICSA 防病毒	
待定认证	FIPS 140-2，通用标准 EAL1+	
通用访问卡（CAC）	支持	
无线	**NSA 220/W**	**NSA 250M/W**
标准	802.11a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS	
虚拟访问点（VAP）5 个 – 天线（5dBi 全向性）	室外则增至三倍，可分开	
发射功率–802.11a/802.11b/802.11g	15.5dBm max/18dBm max/17dBM @ 6Mbps, 13dBM @ 54Mbps	
发射功率–802.11n (2.4GHz)/802.11n（5.0GHz）	19dBm MCS 0, 11dBm MCS 15/17dBm MCS 0, 12dBm MCS 15	
无线电接收机敏感度–802.11a/802.11b/802.11g	-95dBm MCS 0, -81dBm MCS 15/-90dBm @ 11Mbps/-91dBm @ 6Mbps, -74dBm @ 54 Mbps	
无线电接收机敏感度–802.11n (2.4GHz)/802.11n (5.0GHz)	-89dBm MCS 0, -70dBm MCS 15/-95dBm MCS 0, -76dBm MCS 15	
硬件	**NSA 220/W**	**NSA 250M/W**
电源	36W 外部	
风扇	无风扇/1 个内部风扇	2 个内部风扇
输入功率	100-240VAC, 60-50Hz	
最大功耗（W）	11/15	12/16
外形	台式机/可用的 1U 机架配件	
尺寸	7.125 x 1.5 x 10.5 英寸（18.10 x 3.81 x 26.67 厘米）	
重量	1.95 磅/0.88 千克/2.15 磅/0.97 千克	3.05 磅/1.38 千克/3.15 磅/1.43 千克
WEEE 重量	3.05 磅/1.38 千克/3.45 磅/1.56 千克	4.4 磅/2.0 千克/4.65 磅/2.11 千克
装运重量	7 4.35 磅/4.7 磅	5.6 磅/5.9 磅
主要要求	FCC A 级, CE (EMC, LVD, RoHS), C-Tick, VCCI A 级, MSIP/KCC A 级, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI, GOST-R (NSA 220), CU (NSA 250M)	
工作环境	40-105°F，0-40°C	
湿度	5-95%，无冷凝	

[1] 测试方法：最大性能应符合 RFC 2544 的规定（用于防火墙）。实际性能可能会因网络状况和使用的服务而有所差异。[2] 全 DPI/网关防病毒/反间谍软件/IPS 吞吐量使用行业标准 Spirent WebAvalanche HTTP 性能测试和 Ixia 测试工具进行测量。测试是采用穿越多个端口对的多点流量完成的。[3] VPN 吞吐量是使用符合 RFC 2544 规范、数据包大小为 1280 字节的 UDP 流量进行测定的。所有规格、功能和可用性可随时变更。[4] 请查看最新的 SonicOS 5.9 版本，了解最新的 SSO 用户数量。*供将来使用。

NSA 系列系统规格

	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
操作系统	SonicOS 6.1				
安全核心	4 个	6 个	8 个	10 个	24 个
10GbE 接口	—	2 个 10GbE SFP+端口			4 个10GbE SFP+端口
1GbE 接口	8 个 1GbE 接口	4 个 1GbE SFP 端口 12 个 1GbE 端口			8 个 1GbE SFP 端口，8 个 1GbE 接口（1 个 LAN 旁通对）
管理界面	1 个 1GbE，1 个控制台				
内存（RAM）	2.0 GB			4.0 GB	
扩展	1 个扩展插槽（背后）*，SD 卡*				
防火墙检测吞吐量 [1]	1.9 Gbps	3.4 Gbps	6.0 Gbps	9.0 Gbps	12.0 Gbps
全 DPI 吞吐量 [2]	300 Mbps	500 Mbps	800 Mbps	1.6 Gbps	3.0 Gbps
应用检测吞吐量 [2]	700 Mbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
IPS 吞吐量 [2]	700 Mbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
反恶意软件检测吞吐量 [2]	400 Mbps	600 Mbps	1.1 Gbps	1.7 Gbps	3.0 Gbps
IMIX 吞吐量 [3]	600 Mbps	900 Mbps	1.6 Gbps	2.4 Gbps	3.5 Gbps
SSL 检测和解密（DPI SSL）[2]	200 Mbps	300 Mbps	500 Mbps	800 Mbps	1.3 Gbps
VPN 吞吐量 [3]	1.1 Gbps	1.5 Gbps	3.0 Gbps	4.5 Gbps	5.0 Gbps
每秒连接数	15,000	20,000	40,000	60,000	90,000
最大连接（SPI）	225,000	325,000	400,000	750,000	750,000
最大连接（DPI）	125,000	175,000	200,000	500,000	500,000
可支持的 SonicPoint 数量（最大）	32	48	64	96	96
单点登录（SSO）用户	250	500	1,000	2,500	4,000
VPN	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
点对点隧道	75	800	1,500	4,000	6,000
IPSec VPN 客户端（最大数量）	10（250）	50（1,000）	500（3,000）	2,000（4,000）	2,000（6,000）
SSL VPN 许可证（最大数量）	2（25）	2（30）	2（30）	2（50）	2（50）
加密/验证	DES, 3DES, AES（128、192、256 位）/MD5, SHA-1				
密钥交换	Diffie Hellman Groups 1, 2, 5, 14				
基于路由的 VPN	RIP, OSPF				
网络	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
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	1 对 1，多对 1，1 对多，灵活的 NAT（重复的 IPS），PAT，透明模式				
VLAN 接口	50	50	200	400	500
路由协议	BGP，OSPF，RIPv1/v2，静态路由，基于策略的路由，组播				
QoS	带宽优先级，最大带宽，保证带宽，DSCP 标记，802.1p				
认证	XAUTH/RADIUS，活动目录，SSO，LDAP，Novell，内部用户数据库，终端服务，Citrix				
VoIP	全 H323-v1-5，SIP				
标准	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
认证	VPNC，ICSA 防火墙，ICSA 防病毒				
待定认证	FIPS 140-2，通用标准 EAL1+				
通用访问卡（CAC）	待定				
硬件	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
电源	200W	单个固定电源，250W			
风扇	双固定电源				双冗余热插拔风扇
输入功率	100-240 VAC, 60-50 Hz				
最大功耗（W）	49.4	74.3	86.7	90.9	113.1
外形	1U 机架式				
尺寸	1.75 x 10.25 x 17 英寸 （4.5 x 26 x 43 厘米）	1.75 x 19.1 x 17 英寸 （4.5 x 48.5 x 43 厘米）			
重量	10.1 磅（4.6 千克）	13.56 磅（6.15 千克）			14.93 磅（6.77 千克）
WEEE 重量	11.0 磅（5.0 千克）	14.24 磅（6.46 千克）			19.78 磅（8.97 千克）
装运重量	14.3 磅（6.5 千克）	20.79 磅（9.43 千克）			26.12 磅（11.85 千克）
主要要求	FCC A 级，CE（EMC, LVD, RoHS），C-Tick，VCCI A 级，MSIP/KCC A 级，UL，cUL，TUV/GS，CB，Mexico CoC by UL，WEEE，REACH，ANATEL，BSMI，CU				
工作环境	32-105°F，0-40°C				
湿度	10-90%，无冷凝				
MTBF（年）	20.2	16.8	16.0	15.4	13.3

[1]测试方法：最大性能应符合 RFC 2544 的规定（用于防火墙）。实际性能可能会因网络状况和使用的服务而有所差异。[2]全 DPI/网关防病毒/反间谍软件/IPS 吞吐量使用行业标准 Spirent WebAvalanche HTTP 性能测试和 Ixia 测试工具进行测量。测试是采用穿越多个端口对的多点流量完成的。[3]VPN 吞吐量是使用符合 RFC 2544 规范、数据包大小为 1280 字节的 UDP 流量进行测定的。所有规格、功能和可用性可随时变更。*供将来使用。

NSA 系列订购信息

产品	SKU
NSA 220 TotalSecure（1 年）	01-SSC-9744
NSA 220 Wireless-N TotalSecure（1 年）	01-SSC-9746
NSA 250M TotalSecure（1 年）	01-SSC-9747
NSA 250M Wireless-N TotalSecure（1 年）	01-SSC-9749
NSA 2600 TotalSecure（1 年）	01-SSC-3863
NSA 3600 TotalSecure（1 年）	01-SSC-3853
NSA 4600 TotalSecure（1 年）	01-SSC-3843
NSA 5600 TotalSecure（1 年）	01-SSC-3833
NSA 6600 TotalSecure（1 年）	01-SSC-3823
NSA 220W 和 220 Wireless-N 技术支持和安全产品订购	**SKU**
综合网关安全套件 – 应用智能、威胁防御和内容过滤，支持 NSA 220（1 年）	01-SSC-4648
威胁防御 – NSA 220 的入侵防御、网关防病毒、网关反间谍软件、基于云的防病毒（1 年）	01-SSC-4612
针对 NSA 220 的动态支持（1 年）	01-SSC-4630
NSA 220 的内容过滤高级企业版（1 年）	01-SSC-4618
针对 NSA 220 的全面的反垃圾服务（1 年）	01-SSC-4642
NSA 250M 和 250M Wireless-N 技术支持和安全产品订购	**SKU**
综合网关安全套件 – 应用智能、威胁防御和内容过滤，支持 NSA 250M（1 年）	01-SSC-4606
威胁防御 – NSA 250M 的入侵防御、网关防病毒、网关反间谍软件、基于云的防病毒（1 年）	01-SSC-4570
针对 NSA 250M 的动态支持（1 年）	01-SSC-4588
NSA 250M 的内容过滤高级企业版（1 年）	01-SSC-4576
针对 NSA 250M 的全面的反垃圾服务（1 年）	01-SSC-4600
NSA 2600 技术支持和安全产品订购	**SKU**
综合网关安全套件 – 应用智能、威胁防御和内容过滤，支持 NSA 2600（1 年）	01-SSC-4453
威胁防御 – NSA 2600 的入侵防御、网关防病毒、网关反间谍软件、基于云的防病毒（1 年）	01-SSC-4459
针对 NSA 2600 的银级全天候 7x24 小时技术支持（1 年）	01-SSC-4314
NSA 2600 的内容过滤高级企业版（1 年）	01-SSC-4465
针对 NSA 2600 的全面的反垃圾服务（1 年）	01-SSC-4471
NSA 3600 技术支持和安全产品订购	**SKU**
综合网关安全套件 – 应用智能、威胁防御和内容过滤，支持 NSA 3600（1 年）	01-SSC-4429
威胁防御 – NSA 3600 的入侵防御、网关防病毒、网关反间谍软件、基于云的防病毒（1 年）	01-SSC-4435
针对 NSA 3600 的银级全天候 7x24 小时技术支持（1 年）	01-SSC-4302
NSA 3600 的内容过滤高级企业版（1 年）	01-SSC-4441
针对 NSA 3600 的全面的反垃圾服务（1 年）	01-SSC-4447
NSA 4600 技术支持和安全产品订购	**SKU**
综合网关安全套件 – 应用智能、威胁防御和内容过滤，支持 NSA 4600（1 年）	01-SSC-4405
威胁防御 – NSA 4600 的入侵防御、网关防病毒、网关反间谍软件、基于云的防病毒（1 年）	01-SSC-4411
针对 NSA 4600 的银级全天候 7x24 小时技术支持（1 年）	01-SSC-4290
NSA 4600 的内容过滤高级企业版（1 年）	01-SSC-4417
针对 NSA 4600 的全面的反垃圾服务（1 年）	01-SSC-4423

NSA 系列订购信息

NSA 5600 技术支持和安全产品订购	SKU
综合网关安全套件 – 应用智能、威胁防御和内容过滤，支持 NSA 5600（1 年）	01-SSC-4234
威胁防御 – NSA 5600 的入侵防御、网关防病毒、网关反间谍软件、基于云的防病毒（1 年）	01-SSC-4240
针对 NSA 5600 的金级全天候 7x24 小时技术支持（1 年）	01-SSC-4284
NSA 5600 的内容过滤高级企业版（1 年）	01-SSC-4246
针对 NSA 5600 的全面的反垃圾服务（1 年）	01-SSC-4252
NSA 6600 技术支持和安全产品订购	**SKU**
综合网关安全套件 – 应用智能、威胁防御和内容过滤，支持 NSA 6600（1 年）	01-SSC-4210
威胁防御 – NSA 6600 的入侵防御、网关防病毒、网关反间谍软件、基于云的防病毒（1 年）	01-SSC-4216
针对 NSA 6600 的金级全天候 7x24 小时技术支持（1 年）	01-SSC-4278
NSA 6600 的内容过滤高级企业版（1 年）	01-SSC-4222
针对 NSA 6600 的全面的反垃圾服务（1 年）	01-SSC-4228
模块及附件*	**SKU**
10GBASE-SR SFP+短距离模块	01-SSC-9785
10GBASE-LR SFP+长距离模块	01-SSC-9786
10GBASE SFP+ 1M 双轴电缆	01-SSC-9787
10GBASE SFP+ 3M 双轴电缆	01-SSC-9788
1000BASE-SX SFP 短距离模块	01-SSC-9789
1000BASE-LX SFP 长距离模块	01-SSC-9790
1000BASE-T SFP 铜线模块	01-SSC-9791
NSA 220/250M 机架配件	**SKU**
NSA 220 机架配件	01-SSC-9212
NSA 250M 机架配件	01-SSC-9211
NSA 250M 扩展模块	**SKU**
针对 NSA 250M 系列的 4 端口 GbE 扩展模块	01-SSC-8619
2 端口 SFP 模块	01-SSC-8826
1 端口 T1/E1 模块 M1	01-SSC-8829
1 端口 ADSL Annex A 模块 M1	01-SSC-8827
1 端口 ADSL Annex B 模块 M1	01-SSC-8828
带 LAN 旁路组件 M1 的 2 端口 GbE	01-SSC-8830
管理和报告	**SKU**
Dell SonicWALL GMS 10 节点软件许可证	01-SSC-3363
Dell SonicWALL GMS E-Class 全天候 7x24 小时 10 节点软件支持（1 年）	01-SSC-6514
Dell SonicWALL Scrutinizer 虚拟设备，为 5 个节点提供流量分析模块软件许可证（包含 1 年的全天候 7x24 小时软件支持）	01-SSC-3443
Dell SonicWALL Scrutinizer，为 5 个节点提供流量分析模块软件许可证（包含 1 年的全天候 7x24 小时软件支持）	01-SSC-4002
Dell SonicWALL Scrutinizer，为 5 个节点提供高级报告模块软件许可证（包含 1 年的 7x24 小时软件支持）	01-SSC-3773

*请联系 Dell 安全产品 SE，了解可支持的 SFP 和 SFP+模块的详细信息。

可管理型号：

NSA 220–APL24-08E
NSA 220 W–APL24-08F
NSA 250M–APL25-090
NSA 250M W–APL25-091
NSA 2600–1RK29-0A9
NSA 3600–1RK26-0A2
NSA 4600–1RK26-0A3
NSA 5600–1RK26-0A4
NSA 6600–1RK27-0A5

欲了解更多信息，请登录 www.sonicwall.com

Dell Software
5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
如果您是在北美以外的地区，请登录网站查看当地办事处信息。

DellSW 538-09/13