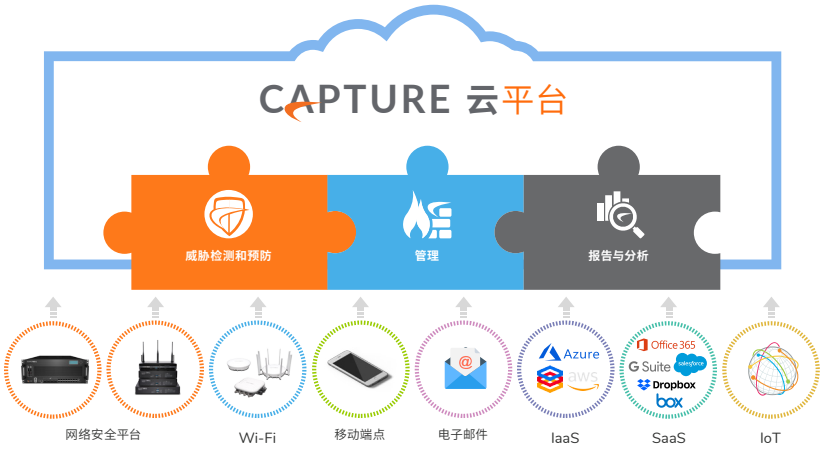
SONICWALL

SonicWall Network Security virtual (NSv) 防火墙系列

适用于公共云、私有云或混合云环境的下一代安全性

现代网络体系结构（例如虚拟化和云）的设计、实施和部署对于许多组织而言仍然是具有颠覆性的战略。实现数据中心虚拟化、迁移到云或者两者的结合显示出显著的运营和经济优势。然而，虚拟环境中的漏洞显而易见。人们经常会发现新漏洞，这些漏洞会产生严重的安全隐患和挑战。为了确保应用程序和服务以安全、高效和可扩展的方式交付，同时仍能应对对虚拟框架的各个部分（包括虚拟机（VM））有害的各种威胁，应用工作负载和数据必须成为最高优先事项。

SonicWall Network Security virtual（NSv）防火墙系列可以帮助安全团队减少这类安全风险和漏洞，这些安全风险和漏洞会严重干扰您的关键业务服务和运营。NSv 新一代虚拟防火墙集成了两种先进的安全技术，可提供最先进的威胁防御功能，使您的网络领先一步。SonicWall 正在申请专利的 Real-Time Deep Memory Inspection（RTDMI™）技术增强了我们备受赞誉的多引擎 Capture 高级威胁保护（ATP）沙箱服务。RTDMI 引擎通过直接在内存中进行检查，主动检测并阻止大众市场攻击、零日攻击和未知的恶意软件。由于采用了实时体系结构，SonicWall RTDMI 技术具有精确性，可将误报率降至最低，并可识别和缓解恶意软件攻击暴露时间小于 100 纳秒的复杂攻击。与上述技术结合使用的是 SonicWall 获得专利的*单通道免重组深度包检测（RFDPI®）引擎，它可检查防火墙上的入站和出站流量，从而检查每个数据包的每一个字节。



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

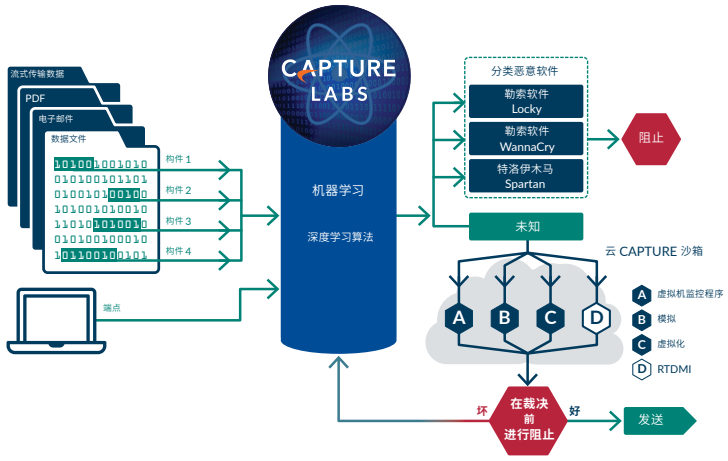
好处

公共云和私有云安全

- 具有自动实时漏洞检测和预防功能的下一代防火墙
- 正在申请专利的 Real-Time Deep Memory Inspection（RTDMI）技术
- 获得专利的免重组深度包检测（RFDPI）技术
- 完整的端到端可见性和控制力
- 应用程序智能与控制
- 分段安全性和安全性分区
- 跨私有云（ESXi、Hyper-V）和公共云（AWS、Azure）平台支持
- BYOL 和 PAYG 许可

虚拟机保护

- 使用 Capture ATP 提供零日攻击威胁防护
- 数据保密性
- 防止数据泄露的安全通信
- 流量验证、检查和监控
- 系统安全性和完整性
- 虚拟网络弹性和可用性



NSv 系列通过利用 SonicWall Capture 云平台中的创新深度学习技术，提供企业所需的自动实时漏洞检测和防御功能。该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。该平台整合了从多个来源收集的威胁情报，包括我们的 Capture ATP 以及分布在全球各地的 100 多万个 SonicWall 传感器。通过利用 SonicWall Capture 云平台以及包括入侵防御、反恶意软件和 Web/URL 过滤等功能，NSv 系列甚至可以屏蔽网关上最隐蔽的威胁。

NSv 可以在虚拟环境中轻松部署和配置，通常是在虚拟网络（VN）或虚拟私有云（VPC）之间。这样，它就可以捕获虚拟机之间的通信和数据交换，以自动防御漏洞，同时建立严格的访问控制措施，以确保数据机密性以及虚拟机安全性和完整性。采用 SonicWall 全面的安全检查服务套件[1]，可成功消除各种安全威胁（例如，跨虚拟机或旁道攻击、基于网络的常见入侵，以及应用程序和协议漏洞）。所有虚拟机流量都受到多个威胁分析引擎的影响，包括入侵防御、网关防病毒和防间谍软件、云防病毒、僵尸网络过滤、应用程序控制和采用 RTDMI 技术的 Capture ATP 多引擎沙箱。

分段安全性

为了对高级持续性威胁（APT）产生最佳的防范效果，网络安全分段必须对高级威胁应用一套完整的动态、可实施的屏障。通过基于分段的安全功能，NSv 可以对类似的接口进行分组，并对其应用相同的策略，而不必为每个接口编写相同的策略。通过将安全策略应用到虚拟网络内部，可以配置分段，将网络资源组织成不同的分段，并允许或限制这些分段之间的流量。这样，可以严格控制对内部关键资源的访问。

NSv 会根据动态标准（如用户身份凭据、Geo-IP 位置和移动端点的安全状态等）自动执行分段限制。在扩展安全方面，NSv 还能够将多千兆网络交换整合到其安全分段策略和执行中。它将分段策略定向到整个网络中交换点的流量，并在全局范围内从单一管理平台管理分段安全执行。

由于分段的有效性取决于它们之间可以实现的安全性，因此 NSv 应用入侵防御系统（IPS）来扫描vVLANv分段上的入站和出站流量，以增强内部网络流量的安全性。对于每个分段，它都基于可实施的策略在多个接口上实施全方位的安全服务。

灵活的部署使用案例

凭借对高可用性实施的基础设施支持，NSv 可满足软件定义的数据中心的可扩展性和可用性要求。它可以确保系统的弹性、服务可靠性和法规遵从性。针对广泛的公共、私有和混合部署使用案例进行了优化，NSv 可以适应服务级别变化，并确保虚拟机及其应用工作负载和数据资产的可用性和安全性。它可以在低延迟的情况下以数 Gbps 的速度完成所有任务。

企业可获得物理防火墙的所有安全优势，同时还能获得虚拟化的运营和经济优势。这包括系统可扩展性、运营敏捷性、配置速度，以及简化管理和降低成本。

NSv 系列提供多种虚拟版本，并经过精心包装，适用于各种虚拟化和云部署使用案例。NSv 系列具备多千兆威胁防御和加密流量检测性能，可适应容量级别递增，并确保虚拟网络（VN）或虚拟私有云（VPC）的安全。该系列还能确保应用工作负载和数据资产的可用性和安全性。

集中治理

NSv部署可以采用两种方式进行集中管理，一是在内部使用 SonicWallçGlobal Management System（GMS²），二是借助 Capture Security Center²（SonicWall 的开放式、可扩展的云安全管理、监控、报告和分析平台），该平台极具成本效益，可以作为即服务产品提供。

Capture Security Center 具有无与伦比的可见性、敏捷性和功能性，能更加清晰、准确和快速地管理整个 SonicWall 虚拟和物理防火墙生态系统，所有这些均可在单一管理平台上完成。

采用 SonicOS 7 的统一策略引擎

SonicWall 统一策略引擎从 NSv 系列开始，跨 SonicWall 内部和虚拟防火墙提供各种安全策略的集成管理。

集中治理

- 为全面的安全管理、分析报告和合规建立简便的途径，以统一您的网络安全防御计划
- 自动化和关联工作流程，形成全面协调的安全治理、合规和风险管理战略

合规性

- 通过自动化 PCI、HIPAA 和 SOX 安全报告，让监管机构和审计员满意
- 自定义安全可审核数据的任意组合，以帮助您实现特定的法规合规性

风险管理

- 快速行动并跨共享安全框架推动协作、沟通和认知
- 基于时间紧迫的综合性威胁信息做出明智的安全策略决定，以提高安全方面的效率

GMS 为安全治理、合规和风险管理提供了一种全面的方法

该引擎配备一个新的 Web 界面，支持完全不同的方法，即强调用户至上的设计。

它通过可实施的警报以及简单的点击式操作就可以直观地设置上下文安全策略。

在视觉上，它也比经典界面更有吸引力。在防火墙的单窗格视图中，该界面向用户提供有关各种安全规则有效性的信息。

它可供用户以无缝方式对网关防病毒软件、反间谍软件、内容过滤、入侵防御、Geo-IP 过滤、加密流量的深度包检测等预定义规则进行修改。

借助统一策略引擎，SonicWall 提供了更加简化的体验，减少了配置错误和部署时间，从而改善了整体安全态势。

灵活的许可

NSv 支持自带设备许可证 (BYOL) 和即用即付 (PAYG) 许可。NSv 的 BYOL 许可证可以直接从 SonicWall、合作伙伴或经销商处购买。而 PAYG 许可证则可以直接从 AWS Marketplace 购买。这种类型的许可证是基于使用情况的许可证，根据使用情况按小时或按年付费。

特色

SonicOS 平台

SonicOS 体系结构是所有 SonicWall 物理和虚拟防火墙 (包括 NSv 和 NSa 系列、SuperMassive 系列和 TZ 系列) 的核心。有关特性和功能的完整列表，请参阅 SonicWall SonicOS 平台数据表。

自动防御漏洞[1]

NSv 提供完整的高级威胁防护，包括高性能入侵和恶意软件防护，以及使用 SonicWall 的 RTDMI 技术的基于云的沙箱。

全天候安全防护[1]

NSvv可确保横向移动保护，加上入站和出站流量保护。新的威胁更新将自动推送到具有主动安全服务的防火墙，并立即生效，而无需重新启动或中断。

零日攻击防护[1]

NSv 通过针对涵盖数千个单独漏洞的最新漏洞利用方法和技术进行不断更新，以此防范零日攻击。

威胁 API

NSv 接收并利用一切专有的原始设备制造商和第三方情报源来抵御高级威胁，如零日攻击、恶意内幕交易、凭据泄露、勒索软件和高级持续性威胁。

区域保护

NSv 通过将网络划分为多个安全区域来增强内部安全性，而入侵防御服务则可以防止威胁跨越区域边界传播。创建访问规则和 NAT 策略并将其应用于通过各种接口的流量，这样可以基于各种条件允许或拒绝内部或外部网络访问。

应用程序智能与控制[1]

NSv 通过特定于应用程序的策略，可以在用户、电子邮件地址、计划和 IP 子网级别对网络流量进行精细控制。它基于应用程序独有的特定参数或模式创建签名，以此控制自定义应用程序。根据各种条件，允许或拒绝内部或外部网络访问。

防止数据泄露

NSv 提供扫描数据流中关键字的能力。这就限制了某些文件名、文件类型、电子邮件附件、附件类型、具有特定主题的电子邮件以及具有特定关键字或字节模式的电子邮件或附件的传输。

应用程序层带宽管理

NSv 可以在各种带宽管理设置中选择，以减少使用数据包监视器的应用程序对网络带宽的使用。这样可以进一步控制网络。

安全通信

NSv 确保虚拟机组之间的数据交换是安全的，包括隔离、机密性、完整性，以及通过使用分段控制这些网络内的信息流。

[1] *需要订阅 SonicWall Advanced Gateway Security Services（AGSS）。*
[2] *SonicWall Global Management System and Capture Security Center 需要单独的许可或订阅。*

访问控制

NSv 验证只有满足一组给定条件的虚拟机才能通过使用 VLAN 访问属于另一个虚拟机的数据。

用户身份验证

NSv 创建策略来控制或限制未经授权的用户对虚拟机和工作负载的访问。

数据保密性

NSv 阻止信息窃取和对受保护数据和服务的非法访问。

虚拟网络弹性和可用性

NSv 可以防止应用服务和通信中断或降级。

系统安全性和完整性

NSv 阻止未经授权接管虚拟机系统和服务。

流量验证、检查和监控机制

NSv 检测异常和恶意行为，以阻止针对虚拟机工作负载的攻击。

部署选项

针对各种私有云/公共云安全使用案例，NSv 可以部署在各种虚拟化平台和云平台上。

灵活的许可模式

SonicWall 提供永久和非永久许可模式。永久许可是一种传统的运营模式，其中防火墙和安全服务许可证必须单独购买。因此，这些许可证会分别到期。非永久许可是一种独特的模式，其中防火墙和安全服务许可证捆绑在一起，并同时到期。对于公共云部署，永久和非永久许可都以自带设备许可证 (BYOL) 模式提供。

SonicWall 非永久或订阅许可模式极为灵活和简单，因为单一 SKU 捆绑了防火墙软件和安全服务。私有云 (ESXi 和 Hyper-V) 和公共云 (AWS、Azure) 产品均可使用此模式。服务到期前会发送服务到期通知。

非永久授权模式有三种类型，即 IPS/App 控制订阅、TotalSecure 订阅和 TotalSecure 高级订阅，期限为一年。根据产品层级，NSv 软件捆绑在入侵防御系统 (IPS)、应用程序控制、支持、Capture Security Center (CSC)、Comprehensive Gateway Security Suite (CGSS) 或 Advanced Gateway Security Suite (AGSS) 的组合中。

NSv 系列系统规格

防火墙一般信息	NSv 10	NSv 25	NSv 50	NSv 100
操作系统	SonicOS[1]			
支持的虚拟机监控程序	VMware ESXi v5.5/v6.0/v6.5/v6.7，Microsoft Hyper-V Win 2012/2016，KVM Ubuntu 16.04/CentOS 7			
支持的公共云平台（实例类型）	AWS（c5.large）、Azure（Std D2 v2）			
许可	BYOL、PAYG[2]			
支持的最大 vCPU	2	2	2	2
接口计数（ESXi/Hyper-V/KVM）	8/8/8	8/8/8	8/8/8	8/8/8
最大管理/DataPlane 核心	1/1	1/1	1/1	1/1
最小内存[3]	4 GB	4 GB	4 GB	4 GB
最大内存[4]	6 GB	6 GB	6 GB	6 GB
支持的 IP/节点	10	25	50	100
最小存储	60 GB			
SSO 用户	25	50	100	100
日志记录	分析器、本地日志、Syslog			
高可用性	主动/被动			
防火墙/VPN 性能[6]	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
防火墙检查吞吐量	2 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps
完整的 DPI 吞吐量（GAV/GAS/IPS）	450 Mbps	550 Mbps	650 Mbps	750 Mbps
应用程序检查吞吐量	1 Gbps	1.25 Gbps	1.5 Gbps	1.75 Gbps
IPS 吞吐量	1 Gbps	1.25 Gbps	1.5 Gbps	1.75 Gbps
反恶意软件检查吞吐量	450 Mbps	550 Mbps	650 Mbps	750 Mbps
IMIX 吞吐量	750 Mbps	850 Mbps	950 Mbps	1100 Mbps
TLS/SSL DPI 吞吐量	650 Mbps	750 Mbps	850 Mbps	950 Mbps
VPN 吞吐量	500 Mbps	550 Mbps	600 Mbps	650 Mbps
每秒连接数	1,800	5,000	8,000	10,000
最大连接数（SPI）	2,500	6,250	12,500	25,000
最大连接数（DPI）	2,500	6,250	12,500	25,000
TLS/SSL DPI 连接数	500	1,000	2,000	4,000
VPN	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
站点到站点 VPN 隧道	10	10	25	50
IPSec VPN 客户端	10（10）	10（10）	10（25）	10（25）
包括 SSL VPN 客户端[7]	2	2	2	2
SSL VPN 客户端最大数量[7]	50	50	50	50
加密/身份验证	DES、3DES、AES（128、192、256 位）/MD5、SHA-1、Suite B、通用访问卡 （CAC）			
密钥交换	Diffie Hellman 组 1、2、5、14v			
基于路由的 VPN	RIP、OSPF、BGP			
联网	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
IP 地址分配	静态、DHCP、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			
最大 VLAN	25	25	50	50
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			
身份验证	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、内部用户数据库、终端服务、Citrix			
VoIP	SIP			
标准	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、L2TP、PPTP、RADIUS			
最大 SD-WAN 组	12	12	18	32
每个产品最大 SD-WAN 成员	24	24	36	64

NSv 系列系统规格（续）

防火墙一般信息	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
操作系统	SonicOS[1]				
支持的虚拟机监控程序	VMware ESXi v5.5/v6.0/v6.5/v6.7，Microsoft Hyper-V，KVM Ubuntu 16.04/CentOS 7				
支持的公共云平台（实例类型）	AWS（c5.large）、Azure（Std D2 v2）	不适用	AWS（c5.xlarge）、Azure（Std D3 v2）	AWS（c5.2xlarge）、Azure（Std D4 v2）	AWS（c5.4xlarge）、Azure（Std D5 v2）
许可	BYOL、PAYG[2]				
支持的最大 vCPU	2	3	4	8	16
接口计数（ESXi/Hyper-V/KVM/AWS/Azure）	8/8/8/2/2	8/8/8/-/-	8/8/8/4/4	8/8/8/8/8	8/8/8/8/8
最大管理/DataPlane 核心	1/1	1/2	1/3	1/7	1/15
最小内存[3]	6 GB	6 GB	8 GB	10 GB	12 GB
最大内存[4]	6 GB	8 GB	10 GB	14 GB	18 GB
支持的 IP/节点	无限制	无限制	无限制	无限制	无限制
最小存储	60 GB				
SSO 用户	500	5,000	10,000	15,000	20,000
日志记录	分析器、本地日志、Syslog				
高可用性	主动/被动[5]				
防火墙/VPN 性能[6]	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
防火墙检查吞吐量	4.1 Gbps	5.9 Gbps	7.8 Gbps	13.9 Gbps	17.2 GBPS
完整的 DPI 吞吐量（GAV/GAS/IPS）	900 Mbps	1.6 Gbps	2.2 Gbps	4.0 Gbps	6.4 Gbps
应用程序检查吞吐量	2.3 Gbps	3.4 Gbps	4.1 Gbps	5.5 Gbps	6.4 Gbps
IPS 吞吐量	2.3 Gbps	3.4 Gbps	4.1 Gbps	5.5 Gbps	6.7 GBPS
反恶意软件检查吞吐量	900 Mbps	1.6 Gbps	2.2 Gbps	4.0 Gbps	6.6 Gbps
IMIX 吞吐量	1.5 Gbps	2.3 Gbps	2.8 Gbps	4.2 Gbps	5.3 Gbps
TLS/SSL DPI 吞吐量	1.1 Gbps	1.2 Gbps	1.8 Gbps	3.4 Gbps	5.1 GBPS
VPN 吞吐量	750 Mbps	1.4 Gbps	1.9 Gbps	4.2 Gbps	8.4 Gbps
每秒连接数	13,760	24,360	37,270	75,640	125,000
最大连接数（SPI）	225,000	1M	1.5M	3M	4M
最大连接数（DPI）	125,000	500,000	1.5M	2M	2.5M
TLS/SSL DPI 连接数	8,000	12,000	20,000	30,000	50,000
VPN	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
站点到站点 VPN 隧道	75	100	6000	10,000	25,000
IPSec VPN 客户端（最大）	50（1000）	50（1000）	2000（4000）	2000（6000）	2000（10,000）
包括 SSL VPN 客户端[7]	2	2	2	2	2
SSL VPN 客户端最大数量[7]	100	150	200	300	400
加密/身份验证	DES、3DES、AES（128、192、256 位）/MD5、SHA-1、Suite B、通用访问卡 （CAC）				
密钥交换	Diffie Hellman 组 1、2、5、14v				
基于路由的 VPN	RIP、OSPF、BGP				
联网	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
IP 地址分配	静态、DHCP、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				
最大 VLAN[8]	128	128	128	128	128
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				
身份验证	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、内部用户数据库、终端服务、Citrix				
VoIP	SIP				
标准	TCP/IP、ICMP、HTTP、HTTPS、IPSec、ISAKMP/IKE、SNMP、DHCP、L2TP、PPTP、RADIUS				
最大 SD-WAN 组	38	38	70	102	102
每个产品最大 SD-WAN 成员	76	76	140	204	204

[1]目前支持 SonicOS 6.5.4。
[2]PAYG 目前仅在 AWS 上可用。
[3]禁用巨型帧的内存。
[4]启用巨型帧的内存。巨型帧需要额外的内存。Azure 和 AWS 不支持巨型帧。
[5]在 VMware ESXi 平台和 Microsoft Hyper-V 上提供高可用性，而在 Azure 和 AWS 上不支持高可用性。
[6]发布的性能数据符合规格，实际性能可能会因基础硬件、网络条件、防火墙配置和已激活的服务而异。性能和容量也可能会因基础虚拟化基础设施而异，我们建议在您的环境中进行其他测试，以确保满足您的性能和容量要求。使用运行带有 VMware vSphere 6.5 的 SonicOSv 6.5.0.2 的 Intel Xeon W 处理器（W-2195 2.3GHz、4.3GHz Turbo、24.75M 缓存）观察到的性能指标。
[7]增加的 SSL VPN 编号仅可从 SonicOS 6.5.4.4-44v-21-723 固件及更高版本获得。
[8]Azure 和 AWS 上不支持 VLAN 接口。
测试方法：基于 RFC 2544 的最大性能（用于防火墙）。使用行业标准的 Spirent WebAvalanche HTTP 性能测试和 Ixia 测试工具，对完整的 DPI/网关 AV/反间谍软件/IPS 吞吐量进行测量。通过多个端口对使用多个流量进行测试。根据 RFC 2544，使用 1418 字节数据包大小的 UDP 流量测量 VPN 吞吐量。所有规格和功能均可能随时更改。

特色

RFDPI 引擎	
功能	**描述**
免重组深度包检测 （RFDPI）	这种高性能、专有且获得专利的检查引擎无需代理或缓冲即可执行基于流的双向流量分析，可发现入侵尝试和恶意软件，并识别应用程序流量，而不受端口限制。
双向检测	同时扫描入站和出站流量中是否存在威胁，以确保网络不会被用于传播恶意软件，并在受感染的机器被带入时，不会成为攻击的发射平台。
基于数据流的检查	无代理、不需缓冲的检查技术为数百万个同步网络流的 DPI 提供超低延迟性能，而不会引入文件和流的大小限制，并且可应用于常见协议以及原始 TCP 流。
高并行性和可扩展性	RFDPI 引擎的独特设计与多核体系结构配合，可提供高 DPI 吞吐量和极高的新会话建立率，以应对要求苛刻的网络中的流量高峰。
单通道检查	单通道 DPI 体系结构同时扫描是否存在恶意软件、入侵和应用程序识别，可大幅降低 DPI 延迟，并确保所有威胁信息在单一体系结构中相关联。

防火墙和网络	
功能	**描述**
REST API	允许防火墙接收并利用一切专有的原始设备制造商和第三方情报源来抵御高级威胁，如零日攻击、恶意内幕交易、凭据泄露、勒索软件和高级持续性威胁。
有状态数据包检查	检查、分析所有网络流量并使其符合防火墙访问策略。
高可用性[1]	NSv 系列支持具有同步状态的主动/被动（A/P）。
DDoS/DoS 攻击防护	SYN 防洪保护利用第 3 层 SYN 代理和第 2 层 SYN 黑名单技术提供对 DoS 攻击的防御。此外，它还通过 UDP/ICMP 防洪保护和连接速率限制来防御 DoS/DDoS。
支持 IPv6	互联网协议版本 6（IPv6）正处于取代 IPv4 的早期阶段。使用 SonicOS，硬件将支持过滤和有线模式的实现。
灵活的部署选项	NSv 系列可以在传统的 NAT、二层桥接、有线和网络分接模式下部署。
WAN 负载平衡	使用轮循机制、溢出法或百分比法对多个 WAN 接口进行负载平衡。
高级服务质量（QoS）	通过 802.1p、DSCP 标记和网络上 VoIP 流量的重新映射，确保关键通信。
支持 SIP 代理	通过要求 SIP 代理对所有来电进行授权和身份验证，阻止骚扰来电。
生物身份验证	支持指纹识别等不易复制或共享的移动设备身份验证，以安全地对访问网络的用户身份进行身份验证。
开放式身份验证和社交登录	允许来宾用户使用其来自社交网络服务（例如 Facebook、Twitter 或 Google+）的凭据登录，并使用直通式身份验证通过主机的无线、LAN 或 DMZ 区域访问互联网和其他来宾服务。

管理和报告	
功能	**描述**
基于云的内部管理	SonicWall 设备的配置和管理可使用 SonicWall Capture Security Center 通过云实现，也可以使用 SonicWall Global Management System（GMS）在内部实现。
强大的单一设备管理功能	除了全面的命令行界面和对 SNMPv2/3 的支持外，基于 Web 的直观界面还可实现快捷的配置。
IPFIX/NetFlow 应用程序流报告	通过 IPFIX 或 NetFlow 协议导出应用程序流量分析和使用情况数据，以便使用 SonicWall Scrutinizer 等工具或其他支持 IPFIX 和 NetFlow 扩展的工具进行实时和历史监控和报告。

虚拟专用网络（VPN）	
功能	**描述**
自动配置 VPN	通过在 SonicWall 防火墙之间自动进行初始站点到站点的 VPN 网关配置，同时又可立即自动实现安全性和连接性，简化并减少了复杂的分布式防火墙部署，将繁琐的操作化为无形。
用于站点到站点连接的 IPSec VPN	高性能 IPSec VPN 使 NSv 系列可以充当数千个其他大型站点、分支机构或家庭办公室的 VPN 集中器。
SSL VPN 或 IPSec 客户端远程访问	利用无客户端的 SSL VPN 技术或易于管理的 IPSec 客户端，可以轻松地从各种平台访问电子邮件、文件、计算机、内网网站和应用程序。
冗余的 VPN 网关	当使用多个 WAN 时，可以将主 VPN 和辅助 VPN 配置为允许所有 VPN 会话进行无缝、自动故障转移和故障恢复。
基于路由的 VPN	通过 VPN 链路执行动态路由的功能可通过备用路由在端点之间无缝地重新路由流量，从而在 VPN 隧道发生临时故障时确保连续的正常运行时间。

[1] *目前 AWS 和 Azure 不支持高可用性*

内容/上下文感知	
功能	**描述**
用户活动跟踪	通过无缝的 AD/LDAP/Citrix1/Terminal Services1 SSO 集成提供用户身份识别和活动。 与通过 DPI 获得的大量信息相结合。
GeoIP 国家/地区流量识别	识别和控制进出特定国家/地区的网络流量，以防止来自已知或可疑威胁活动来源的攻击，或调查源自网络的可疑流量。能够创建自定义国家/地区和僵尸网络列表，以覆盖与 IP 地址相关的错误国家/地区或僵尸网络标记。消除了由于分类错误而对 IP 地址进行的不必要过滤。
正则表达式 DPI 过滤	通过正则表达式匹配来识别和控制跨网络的内容，防止数据泄露。能够创建自定义国家/地区和僵尸网络列表，以覆盖与 IP 地址相关的错误国家/地区或僵尸网络标记。

防御漏洞订阅服务

CAPTURE 高级威胁保护	
功能	**描述**
多引擎沙箱	多引擎沙箱平台，包括虚拟化沙箱、全系统模拟和虚拟机监控程序级别分析技术，可执行可疑代码并分析行为，从而提供对恶意活动的全面可见性。
Real-Time Deep Memory Inspection（RTDMI）	这项正在申请专利的基于云的技术可以检测并阻止具有以下特征的恶意软件：不表现出任何恶意行为并通过加密方式隐藏其攻击。RTDMI 引擎通过强制恶意软件将其攻击暴露在内存中，可以主动检测并阻止大众市场攻击、零日攻击和未知恶意软件。
在裁决前进行阻止	为了防止可能为恶意的文件进入网络，将发送到云进行分析的文件保存在网关上，直到确定裁决为止。
广泛的文件类型和大小分析	支持对各种文件类型进行单独或成组分析，包括可执行程序 （PE）、DLL、PDF、 MS Office 文档、存档、JAR 和 APK 以及包括 Windows、Android、Mac OS X 在内的多种操作系统及多浏览器环境。
快速部署签名	当一个文件被识别为恶意文件时，会立即在 48 小时内将签名部署到具有 SonicWall Capture ATP 订阅和网关防病毒和 IPS 签名数据库以及 URL、IP 和域名信誉数据库的防火墙。
Capture Client	Capture Client 是一个统一的客户端平台，可提供多端点保护功能，包括高级恶意软件防护和对加密流量可见性的支持。它利用分层保护技术、全面的报告和端点保护强制实施。
加密威胁防范	
功能	**描述**
TLS/SSL 解密和检查	无需代理即可实时解密和检查 TLS/SSL 加密流量是否存在恶意软件、入侵和数据泄露，并应用应用程序、URL 和内容控制策略，防范隐藏在加密流量中的威胁。包含在所有 NSv 系列机型的安全订阅中。
SSH 检查	针对 SSH 的深度包检测（DPI-SSH）可解密并检查通过 SSH 隧道传输的数据，防止利用 SSH 的攻击。
入侵防御	
功能	**描述**
基于对策的保护	紧密集成的入侵防御系统（IPS）已涵盖广泛的攻击和漏洞，它利用签名和其他对策来扫描数据包有效负载，寻找漏洞和攻击。
自动签名更新	SonicWall 威胁研究团队持续研究并部署 IPS 对策详尽列表的更新，其中涵盖 50 多种攻击类别。新的更新立即生效，无需重新启动，服务也不会中断。
区内 IPS 防护	将网络划分为多个具有入侵防御功能的安全区域，并防止威胁跨区域边界传播，从而增强内部安全性。
僵尸网络命令和控制（CnC）检测和阻止	识别并阻止从本地网络中的机器人发送到被标识为传播恶意软件或属于已知 CnC 点的 IP 和域的命令和控制流量。
协议滥用/异常情况	识别并阻止滥用协议企图越过 IPS 的攻击。
零日攻击防护	通过针对涵盖数千个单独漏洞的最新漏洞利用方法和技术进行不断更新，以此保护网络免遭零日攻击。
反规避技术	广泛的流规范化、解码和其他技术确保威胁不会在第 2-7 层中利用规避技术在未被发现的情况下进入网络。
威胁防御	
功能	**描述**
网关反恶意软件	RFDPI 引擎扫描所有入站、出站和区内流量，从而在所有端口和 TCP 流中发现不限长度和大小的文件中的病毒、特洛伊木马、键记录器和其他恶意软件。
Capture 云恶意软件防护	SonicWall 云服务器上有一个持续更新的数据库，其中包含数千万个威胁签名，用于增强机载签名数据库的功能，为 RFDPI 提供广泛的威胁覆盖范围。
全天候安全更新	新的威胁更新将自动推送到域中具有主动安全服务的防火墙，并立即生效，而无需重新启动或中断。
双向原始 TCP 检查	RFDPI 引擎能够对任何端口上的原始 TCP 流进行双向扫描，防止恶意软件通过专注于保护几个熟知端口的过时安全系统进行偷袭的攻击。
广泛的协议支持	识别 HTTP/S、FTP、SMTP、SMBv1/v2 等不以原始 TCP 方式发送数据的常见协议，并解码有效负载以便对恶意软件进行检查，即使这些有效负载不在标准、熟知的端口上运行。

应用程序智能与控制

功能	描述
应用程序控制	控制应用程序或单个应用程序功能，这些应用程序或功能由 RFDPI 引擎根据包含超过数千种应用程序签名的不断扩展的数据库进行识别，以增强网络安全性并提高网络生产力。
自定义应用程序识别	通过基于应用程序在其网络通信中独有的特定参数或模式创建签名来控制自定义应用程序，以便进一步控制网络。
应用程序带宽管理	严格分配和调整关键应用程序或应用程序类别的可用带宽，同时抑制不必要的应用程序流量。
精细控制	通过 LDAP/AD/Terminal Services/Citrix 集成，基于计划表、用户组、排除列表和一系列具有完全 SSO 用户识别功能的操作控制应用程序或应用程序的特定组件。

内容过滤

功能	描述
内部/外部内容过滤	强制实施可接受的使用策略，并阻止对 HTTP/HTTPS 网站的访问，这些网站包含的信息或图像对于内容过滤服务和内容过滤客户端来说令人反感或毫无价值。
强制实施内容过滤客户端	扩展策略强制实施范围，以阻止位于防火墙外围的 Windows、Mac OS、Android 和 Chrome 设备的互联网内容。
精细控制	使用预定义的类别或任何类别的组合来阻止内容。过滤可以按一天当中的时间安排，如上学期间或工作时间，并应用于单个用户或组。
Web 缓存	URL 评级缓存在 SonicWall 防火墙本地，因此，后续访问频繁访问过的网站的响应时间只需几分之一秒。

强制实施防病毒和反间谍软件

功能	描述
多层保护	利用防火墙功能作为外围的第一层防御，再加上端点防护，以阻止病毒通过笔记本电脑、U 盘和其他不受保护的系统进入网络。
自动强制实施选项	确保每台访问网络的计算机都已安装并激活了适当的防病毒软件和/或 DPI-SSL 证书，从而免除了通常与桌面防病毒管理相关的费用。
自动部署和安装选项	防病毒和反间谍软件客户端通过网络逐个自动部署和安装，从而最大程度地减少了管理开销。
新一代防病毒软件	Capture Client 使用静态人工智能 （AI）引擎在威胁执行前确定它们，并回滚到以前的未感染状态。
间谍软件防护	强大的间谍软件防护功能可以在台式机和笔记本电脑传输机密数据之前，扫描并阻止在台式机和笔记本电脑上安装各种间谍软件程序，从而提高台式机和笔记本电脑的安全性和性能。

SonicOS 功能摘要

全局控制

- 集中控制 IPv6 可见性
- 全局禁用 IPv6 流量处理
- 禁用默认 VPN 策略、配置屏幕和自动生成的规则

登录和用户安全

- 基于 IP 地址范围的登录尝试锁定用户
- 从 CLI 锁定用户
- 首次登录时强制更改密码
- 支持双因素身份验证 (TOTP)
- 来宾用户策略零接触门户支持
- 支持来宾服务 IPv6
- 支持 TACACS+ 会计
- 所有用户的配额控制
- 动态僵尸网络 HTTP 身份验证

联网和系统

- SD-WAN 支持
- DNS 安全/DNS sinkhole 支持
- 通过 TCP DNS 的 FQDN
- 针对 NAT 的 FQDN 地址对象
- DHCPv6 中继
- 针对 H.323 VoIP 应用程序层网关的 IPv6 寻址模式
- 多控制平面 (CP) 核心支持
- 具有数据平面卸载功能的 HTTP/HTTPS 重定向
- IP 帮助程序卸载到数据平面
- 本地存储上的固件备份
- 高可用性加密
- 高可用性固件上传支持
- 基于策略的静态路由和动态路由优化
- 性能/吞吐量提高
- 监视程序功能可监视防火墙运行状况
- 增强了可扩展性，可通过 VPN 编号的隧道接口进行高级路由
- 基于 OSS Noklava v10.5.0 ASN.1 编译器更新 H.323 库
- 任务线程优先级更新
- 数据平面上的 SSLVPN 和书签

安全服务

- Capture ATP 在裁决精细控制前进行阻止
- Capture ATP 针对非 HTTP 协议显示友好的文件名
- CFS 阻止单个 YouTube 视频
- 同时支持 HTTPS 内容过滤和 DPI-SSL
- 下一代防病毒 (SentinelOne) 和 DPI-SSL 强制实施
- Wan DDOS 防护性能提升

策略/对象

- 访问规则增强
- 基于应用程序的路由
- 动态地址对象
- CFS 策略排除
- 基于策略的 HTTPS 内容过滤对象
- 内容过滤器对象中支持 URI 列表组
- 针对 HTTP 请求的 CFS 自定义标头插入
- 针对规则和对象的 UUID
- 针对 CFS 策略的 UUID
- 针对 NAT 策略的源 MAC 覆盖

DPI-SSL/DPI-SSH

- 基于 DPI-SSL 动态云的白名单
- DPI-SSH 阻止 SSH 端口转发
- DPI-SSH 阻止 X11 转发
- 在数据包镜像/数据包捕获中保留 SSL 解密端口
- 按区域精细控制 DPI-SSL
- 基于访问规则的 DPI-SSL 控制
- DPI-SSL 客户端阻止或允许过期的 CA 证书
- TLS 证书状态请求扩展
- 支持本地 CRL
- 增强的 DPI-SSL 证书验证
- 支持与 ECDSA 相关的密码
- 支持联邦认证的 OpenSSL LTS 发行版

记录、监控和报告

- 能够验证 DPI 是否在特定数据包上执行
- 针对应用程序控制的文件名和 URI 日志记录
- 向管理员显示登录记录
- 配置审核
- 记录 TCP 连接的 NAT 映射
- FTP 支持日志自动化
- 针对 NSv 的 Capture Security Center（CSC）报告和分析支持
- Capture ATP 记录电子邮件发件人/收件人
- 捕获威胁评估客户端增强 (SWARM v3)
- 重置 SFR（SWARM）统计数据的功能
- 为 SonicFlow 报告选择输出语言的选项

API

- SonicOS API 阶段 1
- SonicOS API 身份验证支持
- SonicOS API 阶段 2
- LHM RESTful API

SonicOS Web 管理 UI

- SonicOS 全局搜索
- 改进内容页面可用性
- 每个用户客户端 UI 首选项存储
- 将友好名称固定到 SonicOS Web 管理屏幕
- 重构的 SonicOS Web 界面布局

NSv 系列订购信息

产品	ESXI SKU	HYPER-V SKU	AZURE SKU	AWS SKU	KVM SKU
SonicWall NSv 10 Virtual Appliance TotalSecure 高级版 (1 年)	01-SSC-5875	02-SSC-1387	02-SSC-3426	02-SSC-3452	02-SSC-3494
SonicWall NSv 25 Virtual Appliance TotalSecure 高级版 (1 年)	01-SSC-5923	02-SSC-1395	02-SSC-3454	02-SSC-3464	02-SSC-3497
SonicWall NSv 50 Virtual Appliance TotalSecure 高级版 (1年)	01-SSC-5926	02-SSC-1399	02-SSC-3470	02-SSC-3474	02-SSC-3504
SonicWall NSv 100 Virtual Appliance TotalSecure 高级版 (1 年)	01-SSC-5929	02-SSC-1405	02-SSC-3480	02-SSC-3489	02-SSC-3513
SonicWall NSv 200 Virtual Appliance TotalSecure 高级版 (1 年)	01-SSC-5950	02-SSC-1412	02-SSC-0868	02-SSC-0906	02-SSC-3519
SonicWall NSv 300 Virtual Appliance TotalSecure 高级版 (1 年)	01-SSC-5964	02-SSC-1420	—	—	02-SSC-3526
SonicWall NSv 400 Virtual Appliance TotalSecure 高级版 (1 年)	01-SSC-6084	02-SSC-1427	02-SSC-0888	02-SSC-0912	02-SSC-3531
SonicWall NSv 800 Virtual Appliance TotalSecure 高级版 (1 年)	01-SSC-6101	02-SSC-1429	02-SSC-0889	02-SSC-0914	02-SSC-3533
SonicWall NSv 1600 Virtual Appliance TotalSecure 高级版 (1 年)	01-SSC-6109	02-SSC-1436	02-SSC-0895	02-SSC-0921	02-SSC-3540
产品	ESXI SKU	HYPER-V SKU	AZURE SKU	AWS SKU	KVM SKU
SonicWall NSv 10 Virtual Appliance TotalSecure 高级版 (3 年)	01-SSC-5873	02-SSC-1386	02-SSC-3427	02-SSC-3453	02-SSC-3491
SonicWall NSv 25 Virtual Appliance TotalSecure 高级版 (3 年)	01-SSC-5890	02-SSC-1397	02-SSC-3457	02-SSC-3465	02-SSC-3498
SonicWall NSv 50 Virtual Appliance TotalSecure 高级版 (3 年)	01-SSC-5924	02-SSC-1398	02-SSC-3471	02-SSC-3472	02-SSC-3505
SonicWall NSv 100 Virtual Appliance TotalSecure 高级版 (3 年)	01-SSC-5928	02-SSC-1404	02-SSC-3478	02-SSC-3486	02-SSC-3514
SonicWall NSv 200 Virtual Appliance TotalSecure 高级版 (3 年)	01-SSC-5951	02-SSC-1411	02-SSC-0866	02-SSC-0903	02-SSC-3515
SonicWall NSv 300 Virtual Appliance TotalSecure 高级版 (3 年)	01-SSC-5965	02-SSC-1419	—	—	02-SSC-3523
SonicWall NSv 400 Virtual Appliance TotalSecure 高级版 (3 年)	01-SSC-6089	02-SSC-1426	02-SSC-0887	02-SSC-0911	02-SSC-3527
SonicWall NSv 800 Virtual Appliance TotalSecure 高级版 (3 年)	01-SSC-6102	02-SSC-1428	02-SSC-0891	02-SSC-0913	02-SSC-3538
SonicWall NSv 1600 Virtual Appliance TotalSecure 高级版 (3 年)	01-SSC-6108	02-SSC-1435	02-SSC-0897	02-SSC-0920	02-SSC-3542

*有关 SKU 的完整列表，请咨询您当地的 SonicWall 经销商

关于 SonicWall

在每个人都远程办公、每个人都移动办公、每个人都不太安全的工作现实中，SonicWall 为超分布式时代提供了 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。有关更多信息，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-NSvVirtualFirewalls-US-VG-2088