SONICWALL 产品线：产品目录

下一代防火墙

高端：NS*sp* 15700

专为大型分布式企业、数据中心和托管服务提供商 (MSP) 设计的多实例防火墙，在统一策略下提供高速保护、高端口密度和真正的租户隔离

中端：NS*a* 系列

NS*a* 9650/9450/9250/6650/5650/4650/3650/2650

为中型网络、分支机构和分布式企业提供经行业验证的安全效能和性能

入门级：TZ 系列

TZ670/TZ570/TZ400/TZ350

面向中小型组织和软件定义的分支（SD-Branch）部署的集成式威胁防御和 SD-WAN 平台

虚拟化：NSv 系列

采用灵活许可模式的虚拟防火墙，可保护您的公共云和私有云基础设施的所有关键组件

无线安全

SonicWave 系列

SonicWave 432e/432i/432o/231c/224w/231o

为下一代无线设备构建的安全和性能，并通过云或防火墙进行管理

Secure Mobile Access

SMA 系列 SMA 8200v/7210/6210/500v/410/210

对网络和云资源实施根据策略强制执行的简单安全访问

访问交换机

SWS12-8/SWS12-8POE/SWS12-10FPOE/SWS14-24/SWS14-24FPOE/SWS14-48/SWS14-48FPOE

为中小型组织（SMB）和软件定义的分支（SD-Branch）部署的下一代安全连接提供智能交换

电子邮件安全系列

ESA 9000/7000/5000/虚拟机软件/云服务

多层解决方案，可防范高级电子邮件威胁

管理与分析

Capture Security Center

Global Management System (GMS)

Network Security Manager

控制和了解您的网络就是力量

Capture Security appliance (CS*a*)

内部文件测试和恶意软件预防。

Capture Client

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、沙箱、应用程序漏洞情报，以及在感染时回滚

云应用程序安全

CASB 解决方案，为 Office 365 和 G Suite 等 SaaS 应用程序提供下一代安全性，可保护电子邮件、数据和用户凭据免受高级威胁，同时实现云合规性

下一代防火墙订阅服务

基本保护服务套件为防范已知和未知威胁提供所需的所有基本安全服务。这包括采用 RTDMI 技术的 Capture 高级威胁保护、网关防病毒、入侵防御和应用程序控制、内容过滤服务、全面反垃圾邮件服务、网络可见性和全天候支持。

Advanced Gateway Security Suite (AGSS) 可用作所有物理和虚拟 SonicWall 防火墙的附加服务，用于防范最先进的和未知的威胁。

包括在 Advanced Gateway Security Suite (AGSS) 中；在 TotalSecure 高级版中与下一代防火墙相结合。

- Capture 高级威胁防护（ATP）多引擎基于云的沙箱
- 网关防病毒和反间谍软件
- 入侵防御服务
- 应用程序控制
- 内容/Web 筛选服务
- 全天候支持

安全即服务 (SECaaS)

将您的网络安全外包给我们的统包解决方案

要了解更多信息，请访问 sonicwall.com

资格认定问题

下一代防火墙

- 您是否能跟上带宽增长带来的多千兆性能需求?
- 您当前的防火墙是否能够以传入威胁的速度执行威胁检查?
- 您的绩效要求标准是什么?
- 防火墙背后的用户/网络总数是多少?
- 高峰时段的会话/连接总数是多少?
- 将有多少远程站点和用户连接到防火墙?
- 您如何衡量安全控制措施的有效性?
- 您使用哪些类型的互联网连接? 速度是多少?
- 您正在采取哪些措施来防范零日攻击等新威胁?
- 您的沙箱是否能检测和阻止隐藏在深层内存中的威胁?
- 您的沙箱包含多少个引擎?
- 您的沙箱能否在发布文件之前将文件保存在网关中?
- 您是否知道贵组织的防火墙是否正在检测 HTTPS 流量?
- 您是否曾因检测 HTTPS 流量而导致网络服务中断或停机?
- 您的虚拟防火墙是否与您的物理防火墙一样强大?
- 您如何保护自己的公共云或私有云环境的安全?
- 您是否能够在虚拟网络上实施适当的安全性分区和微分段?
- 您是否能够完全了解并控制虚拟流量?
- 您是否有兴趣将 MPLS 替换为 SD-WAN 来保护专用网络的安全，从而降低成本?

Capture Client

- 您的端点是否需要针对勒索软件和加密威胁提供一致的高级保护?
- 跨所有端点遵守策略和执行许可证管理的难易程度如何?
- 您是否为端点的可见性和安全状况的管理而烦恼?
- 您的端点安全产品是否连接到沙箱环境?
- 您能否对端点上安装的应用程序进行编目，并知道其中包含多少个漏洞?
- 您目前的解决方案是否能持续监控系统的运行状况?
- 您是否可以将勒索软件导致的损坏回滚到先前已知的干净状态?
- 您是否有能力阻止未知和可能受感染的设备与端点连接?

云应用程序安全

- 您是否使用 O365 或 G Suite?
- 您是否使用 Proofpoint 或 Mimecast 来保护 O365/G Suite 的安全?
- 您是否扫描内部 O365 电子邮件?
- 贵组织使用多少个经过批准的 SaaS 应用程序?
- 对于存储在 SaaS 应用程序中的数据，您在保持合规方面是否遇到困难?
- 您如何知道用户的凭据是否遭到攻击?
- 您是否了解谁在何时何地访问数据? （自带设备 (BYOD)）

无线安全

- 您的员工/合作伙伴/客户是否抱怨 Wi-Fi 性能低下?
- 在任何时候，无线用户的最大数量是多少?
- 您是否担心在网络中添加安全无线解决方案的成本?
- 您对 802.11ac Wave 2 无线标准的熟悉程度如何?
- 您是否需要灵活性来管理接入点 - 云与防火墙管理?
- 您是否有效地规划了您的 Wi-Fi 网络?
- 您是否需要将接入点与防火墙解除绑定?
- 您是否担心在您的 Wi-Fi 网络中提供高级安全功能?
- 访客服务对您来说重要吗?
- 您是否需要为访客登录提供定制的访客登录门户?

访问交换机

- 您是否需要能够接入千兆流量的交换机来支持启用 PoE 的设备?
- 具有统一可见性和管理的统一安全态势对您来说是否很重要?
- 对于使用 SonicWall 生态系统的第三方交换机，您是否面临解决方案挑战?

Secure Mobile Access

- 您目前的远程员工访问策略是什么?
- 对于采用零信任网络访问方法，您有什么想法?
- 您如何让用户安全访问内部和云托管的公司资源以及应用程序?
- 您是否了解访问您网络的每个用户和每台设备?
- 您目前如何保护您的关键业务 Web 财产和 Web 服务器?

电子邮件安全

- 您是否担忧勒索软件、鱼叉式网络钓鱼和企业电子邮件泄露等高级电子邮件威胁?
- 您当前的电子邮件安全解决方案是否可提供高级威胁防护功能?
- 您是否担忧包含机密信息的电子邮件可能被泄露?
- 您是怎样遵守通用数据保护条例 (GDPR)、萨班斯 - 奥克斯利法案 (SOX)、格雷姆-里奇-比利雷法案 (GLBA) 或 HIPAA 等法规的?
- 您是否有兴趣向您的客户提供托管电子邮件安全服务? (MSSP)

管理与分析

- 通过将您的安全解决方案统一到一个通用管理平台下，提供单一管理平台体验，您可以解决哪些问题?
- 您在管理自己的安全基础设施时遇到哪些经济和运营挑战?
- 您对自己展现网络安全合规性（如 PCI、HIPPA 和 GDPR）方面的能力有多大信心?
- 如果您能够更好地检测并快速、准确地响应威胁和风险，这会如何改变您的安全状况?
- 借助全面了解网络威胁和您的业务面临的风险，您和您的领导团队将获得什么价值?

深度内存检查

SonicWall Real-Time Deep Memory Inspection (RTDMI™) 引擎是一项正在申请专利的技术，通过深层内存检测实时主动检测并阻止未知的大众市场恶意软件。该引擎现在可与 SonicWall Capture 高级威胁防护 (ATP) 云沙箱服务一起使用，并且可识别和缓解甚至最隐蔽的现代威胁，包括未来的 Meltdown 漏洞。

要了解更多信息，请访问 sonicwall.com

SONICWALL®