SONICWALL

SonicWall Capture Security appliance 1000

一些客户由于合规和策略限制而不能将文件发送到云端分析，或更愿意将所有数据留在组织内部。为此，SonicWall Capture Security appliance™ (CSa) 将 Capture Advanced Threat Protection™ (ATP) 和沙箱恶意软件分析引入内部部署情景。CSa 1000 可以分析来自其他 SonicWall 产品的可疑文件，在客户保管文件的情况下快速、高精度地检测以前未曾见过的威胁。此外，借助 CSa 上的 REST API 功能，威胁情报团队、第三方安全系统以及可与已发布 API 集成的任何软件堆栈能够获得这种高效文件分析功能的好处。

CSa 结合使用基于信誉的检查、静态文件分析和 SonicWall 获得专利的 Real-Time Deep Memory Inspection™ (RTDMI) 引擎进行动态分析，确保它不仅可以提供尽可能最高的恶意文件检测率，而且能够在尽可能最短的时间内高效地完成这项工作。SonicWall 安全产品生态系统已经与云交付的 Capture ATP 分析实现完全集成，能够通过“在裁决前进行阻止”之类的功能来强制实施内联安全。当 SonicWall 产品连接到 CSa 系列而不是云 Capture ATP 时，也支持同样的功能。

RTDMI

SonicWall 正在申请专利的 Real-Time Deep Memory Inspection (RTDMI) 文件分析引擎是一种通过监控内存中应用程序的行为来分析可疑文件的新颖方法。RTDMI 可以洞察现代恶意软件为逃避网络和沙箱分析而可能部署的任何混淆或加密技术，从而对文档、可执行文件、存档文件和其他各种文件类型的攻击进行精度极高的检测。

实时防范

通过结合使用信誉和全球情报检查、静态分析和 RTDMI 技术，发挥协同效应，可以足够快地交付结果，从而使 SonicWall 产品中的“在裁决前进行阻止”等技术得以实现。由于具备这种功能，因此可以在防火墙上制定文件检测策略，以防止终端用户下载可疑文件，直到完成全面检测，并由 Capture ATP 或 CSa 作出裁决。

好处：

- 采用 RTDMI 进行基于内存的检测
- 采用信誉检查、静态分析和动态分析的多阶段分析
- 采用 API 访问进行威胁分析
- 支持广泛的文件类型
- 支持在裁决前进行阻止
- 有效确保高安全性
- 报告及基于角色的访问

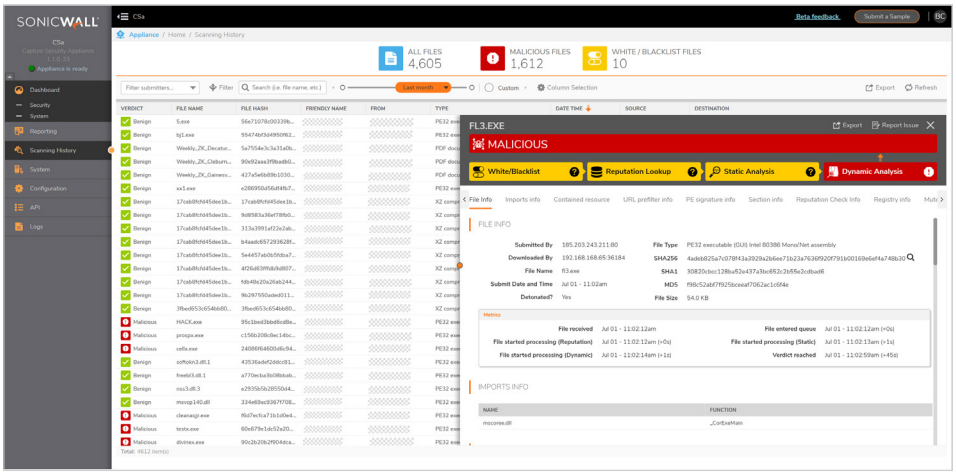
1.分析吞吐量取决于网络连接、文件类型、压缩级别，可能与公布的数字有所不同。
2.虽然没有硬性限制，但设备数量将由每个设备提交的文件数量决定。发布时的推荐范围约为 250 个设备。
3.可以运行 SonicOS 6.5.4.6 或更高版本的所有 TZ 系列、NSa 系列和 SuperMassive 系列。在 SuperMassive 9800 和 NSsp 12000 系列上不支持。

众多客户信赖并从中获益

- CSa 将来自 SonicWall 的 Capture ATP 的技术融入到各种外形规格的设备之中。Capture ATP 是全球超过 150,000 位客户信赖并使用的一种基于云的服务。
- CSa 还可获得定期情报更新，与通过 SonicWall Capture ATP 文件分析全球收集的威胁情报同步。

报告、分析和管理

- CSa 通过易于浏览的仪表板和文件分析历史记录，探查从所有来源提交的文件，了解提交供分析的文件的频率、来源、裁决和其他洞察。
- 报告功能全面观察整个组织的 ATP 保护，能够安排根据不同的角色配置的定期报告。
- 管理员可以授予各种角色对 CSa 1000 的精细访问权限，并能够限制对 UI 任何部分的访问。
- 安全分析师可以访问扫描历史，并能够修改白名单/黑名单和允许的设备，以及报告任何可疑的误报或漏报。
- 网络级管理员可以获得访问设备的操作配置的权限，但由于保密性原因，他们不能查看提交的文件及其来源。



功能特性

- 信誉和全球裁决查找（可配置）
- 采用 RTDMI 进行静态分析和动态分析
- 哈希/域上的白名单/黑名单
- 可配置的计划报告
- 基于角色的管理（可配置角色）
- 管理 - 通过专用管理接口或常规网络接口的 HTTPS 或 SSH
- SSH 控制台访问
- 日志记录和警报
- 带有自动白名单/黑名单的误报和漏报报告
- 直接连接或通过 VPN（IP 可寻址）
- 封闭式网络操作
- 针对文件提交和分析的 REST API 支持
- 带有安全启动和信任链的强化操作系统，可防止篡改
- 本地日志记录

1.分析吞吐量取决于网络连接、文件类型、压缩级别，可能与公布的数字有所不同。
2.虽然没有硬性限制，但设备数量将由每个设备提交的文件数量决定。发布时的推荐范围约为 250 个设备。
3.可以运行 SonicOS 6.5.4.6 或更高版本的所有 TZ 系列、NSa 系列和 SuperMassive 系列。在 SuperMassive 9800 和 NSsp 12000 系列上不支持。

部署选项

- SonicWall CSa 部署快速而简单，只需配置基本的网络、报告和允许的设备访问即可开始使用
- CSa 构建为 IP 可寻址，因此只要提交供分析的文件的设备可以访问它，就可以部署到任何地方

CSa 1000 有三种主要的部署方法：

单一办公室/单一位置

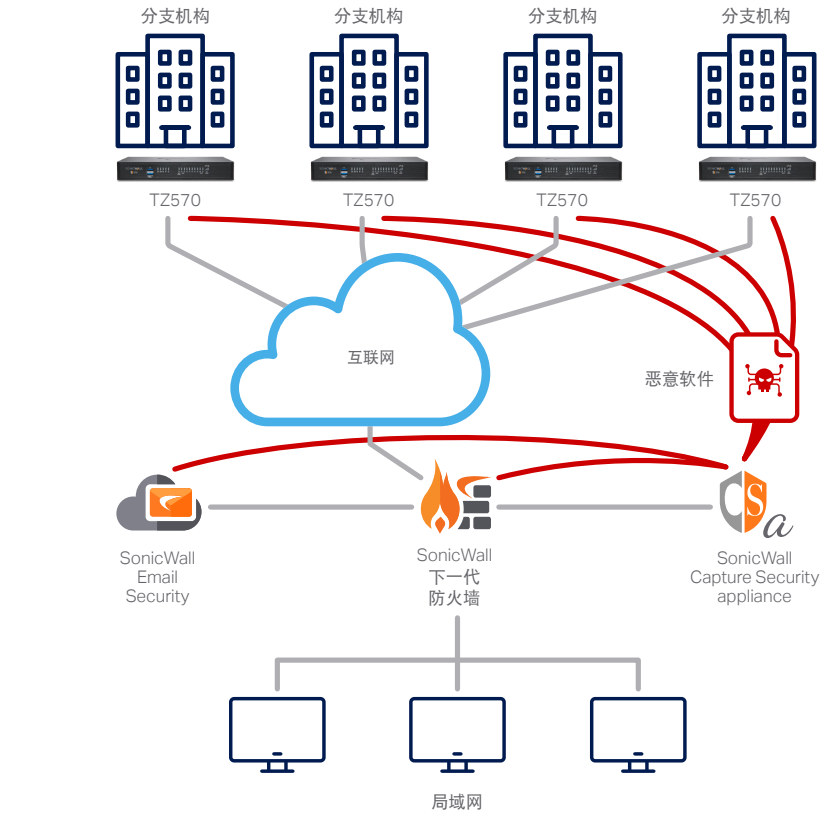
- CSa 可以部署在网络上的任何地方，只要使用它的产品能够通过 IP 访问它[1]
- 部署 CSa 后，可以将防火墙和电子邮件安全系统（其他解决方案待定）配置为将可疑文件重定向到 CSa 而非云，以进行 ATP 分析

分布式企业/多个位置

- 可以将多个办公室/分支机构配置为共享对单个 CSa 设备的访问权限，该设备可以部署在中央总部数据中心或所有设备可访问的远程数据中心
- 可以直接通过互联网或通过 VPN 访问
- 可以使用 GMS 或基于云的 NSM 集中化管理解决方案来完成指向 CSa 的 SonicWall 系统的大规模配置，以实现快速配置和部署

REST API 网关

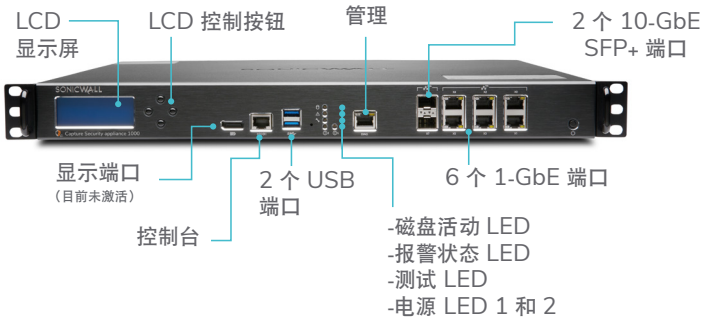
- CSa 系列具有 REST API 接口，可供威胁情报团队通过其自己的脚本、Web 门户集成和其他安全产品来提交文件，以进行分析和获得查询结果
- 有关如何开始使用 CSa 的 API 脚本和代码示例的说明，可在以下网站获得：
  https://github.com/sonicwall

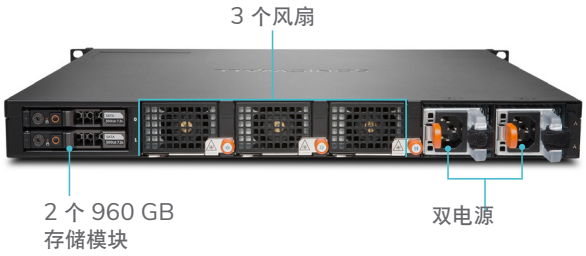


*[1]SonicWall 防火墙还需要使用 2259 端口并通过 UDP 进行访问

1.分析吞吐量取决于网络连接、文件类型、压缩级别，可能与公布的数字有所不同。
2.虽然没有硬性限制，但设备数量将由每个设备提交的文件数量决定。发布时的推荐范围约为 250 个设备。
3.可以运行 SonicOS 6.5.4.6 或更高版本的所有 TZ 系列、NSa 系列和 SuperMassive 系列。在 SuperMassive 9800 和 NSsp 12000 系列上不支持。

CSa 1000





SonicWall CSa 1000 规格

功能特性	
信誉和全球威胁查找吞吐量（每小时文件数）[1]	12,000
真实文件混合吞吐量（每小时文件数）[1]	2,500
动态分析 (RTDMI) 吞吐量（每小时文件数）[1]	300
最大文件大小	100 MB
支持的最大设备数[2]	基于性能
最大存档扫描深度	3
REST API 支持	是
支持的 SonicWall 设备	TZ、NSa 和 SuperMassive（运行 SonicOS 6.5.4.6 及更高版本）[3] Email Security 10.X NSsp 15000 系列 - 待定 NSv 系列（7.X 及更高版本）- 待定
支持的文件类型	.cpl .dll .drv .exe .elf .ocx .scr .sys .doc .dot .wbk .docx .docm .dotx .dotm .docb .xls .xlt .xlm .xlsx .xlsm .xltx .xltm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .pptx .pptm .potx .potm .ppam .ppsx .ppsm .sldx .sldm .o .dylib .bundle .dmg .pdf .jar .apk .rar .bz2 .bzip2 .7z .xz .gz .zip
数据保留期	不受限制，受存储限制
存储	2 个 1TB SSD (RAID 1)
接口	(6)-端口 1GE、(2)-端口 10Gb SFP+、(2) USB、(1) 控制台
专用端口管理	是 (X0)
认证	FIPS 140-2 待定
产品特点	
外形规格	1U
尺寸	17.0 x 16.5 x 1.75 英寸（43 x 41.5 x 4.5 厘米）
设备重量	18.3 磅（8.3 千克）
加密数据加速 (AES-NI)	是
MTBF（@ 25° C 或 77° F），以小时计算	129,601
电源	双电源，可热插拔
输入额定值	100-240 VAC，1.79 A
功耗	114 W
总散热	389 BTU
环境	WEEE、欧盟 RoHS、中国 RoHS
非运行冲击	110 g，2 msec
排放	FCC、ICES、CE、C-Tick、VCCI；MIC
安全	TUV/GS、UL、CE PSB、CCC、BSMI、CB 方案
工作温度	0° C 至 40° C（32° F 至 104° F）
TPM	是

1.分析吞吐量取决于网络连接、文件类型、压缩级别，可能与公布的数字有所不同。
2.虽然没有硬性限制，但设备数量将由每个设备提交的文件数量决定。发布时的推荐范围约为 250 个设备。
3.可以运行 SonicOS 6.5.4.6 或更高版本的所有 TZ 系列、NSa 系列和 SuperMassive 系列。在 SuperMassive 9800 和 NSsp 12000 系列上不支持。

产品	SKU
Capture Security Appliance CSA 1000	02-SSC-2853
Capture Security Appliance CSA 1000 带情报更新和支持捆绑包 - 1 年	02-SSC-5637
Capture Security Appliance CSA 1000 带情报更新和支持捆绑包 - 3 年	02-SSC-5638
Capture Security Appliance CSA 1000 带情报更新和支持捆绑包 - 5 年	02-SSC-5639

服务（CSa 1000 运行时需要。所有向 CSa 发送文件的设备都必须有 Capture ATP 许可）	SKU
针对 SonicWall CSa 1000 的情报更新、激活和支持 1 年	02-SSC-4712
针对 SonicWall CSa 1000 的情报更新、激活和支持 2 年	02-SSC-4713
针对 SonicWall CSa 1000 的情报更新、激活和支持 3 年	02-SSC-4714
针对 SonicWall CSa 1000 的情报更新、激活和支持 4 年	02-SSC-4715
针对 SonicWall CSa 1000 的情报更新、激活和支持 5 年	02-SSC-4716
针对 SonicWall CSa 1000 的情报更新、激活和支持 6 年	02-SSC-4717

REST API 激活（仅 REST API 运行才需要此服务。 必须应用在“情报更新、激活和支持”服务之上）	SKU
适用于 SonicWall Capture Appliance CSA 1000 的 REST API 激活 1 年	02-SSC-4706
适用于 SonicWall Capture Appliance CSA 1000 的 REST API 激活 2 年	02-SSC-4707
适用于 SonicWall Capture Appliance CSA 1000 的 REST API 激活 3 年	02-SSC-4708
适用于 SonicWall Capture Appliance CSA 1000 的 REST API 激活 4 年	02-SSC-4709
适用于 SonicWall Capture Appliance CSA 1000 的 REST API 激活 5 年	02-SSC-4710
适用于 SonicWall Capture Appliance CSA 1000 的 REST API 激活 6 年	02-SSC-4711

1.分析吞吐量取决于网络连接、文件类型、压缩级别，可能与公布的数字有所不同。
2.虽然没有硬性限制，但设备数量将由每个设备提交的文件数量决定。发布时的推荐范围约为 250 个设备
3.可以运行 SonicOS 6.5.4.6 或更高版本的所有 TZ 系列、NSa 系列和 SuperMassive 系列。在 SuperMassive 9800 和 NSsp 12000 系列上不支持。

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-CSa-US-COG-2099