

SonicWall Capture Security appliance 1000

一些客戶由於合規和策略限制而不能將文件發送到雲端分析，或更願意將所有數據留在組織內部。為此，SonicWall Capture Security appliance™ (CSa) 將 Capture Advanced Threat Protection™ (ATP)和沙箱惡意軟件分析引入內部部署情景。CSa1000可以分析來自其他SonicWall產品的可疑文件，在客戶保管文件的情況下快速、高精度地檢測以前未曾見過的威脅。此外，借助CSa上的REST API功能，威脅情報團隊、第三方安全系統以及可與已發布API集成的任何軟件堆棧能夠獲得這種高效文件分析功能的好處。

CSa結合使用基於信譽的檢查、靜態文件分析和SonicWall獲得專利的 Real-Time Deep Memory Inspection™ (RTDMI)引擎進行動態分析，確保它不僅可以提供盡可能最高的惡意文件檢測率，而且能夠在盡可能最短的時間內高效地完成這項工作。SonicWall安全產品生態系統已經與雲交付的CaptureATP分析實現完全集成，能夠通過“在裁決前進行阻止”之類的功能來強制實施內聯安全。

當SonicWall產品連接到CSa系列而不是雲Capture ATP時，也支持同樣的功能。

RTDMI

SonicWall正在申請專利的Real-Time Deep Memory Inspection (RTDMI) 文件分析引擎是一種通過監控內存中應用程序的行為來分析可疑文件的新穎方法。RTDMI可以洞察現代惡意軟件為逃避網絡和沙箱分析而可能部署的任何混淆或加密技術，從而對文檔、可執行文件、存檔文件和其他各種文件類型的攻擊進行精度極高的檢測。

實時防範

通過結合使用信譽和全球情報檢查、靜態分析和RTDMI技術，發揮協同效應，可以足夠快地交付結果，從而使SonicWall產品中的“在裁決前進行阻止”等技術得以實現。由於具備這種功能，因此可以在防火牆上制定文件檢測策略，以防止終端用戶下載可疑文件，直到完成全面檢測，並由Capture ATP或CSa作出裁決。



好處：

- 採用RTDMI進行基於內存的檢測
- 採用信譽檢查、靜態分析和動態分析的多階段分析
- 採用API訪問進行威脅分析
- 支持廣泛的文件類型
- 支持在裁決前進行阻止
- 有效確保高安全性
- 報告及基於角色的訪問

1.分析吞吐量取決於網絡連接、文件類型、壓縮級別，可能與公布的數字有所不同

2.雖然沒有硬性限制，但設備數量將由每個設備提交的文件數量決定。發布時的推薦範圍約為250個設備。

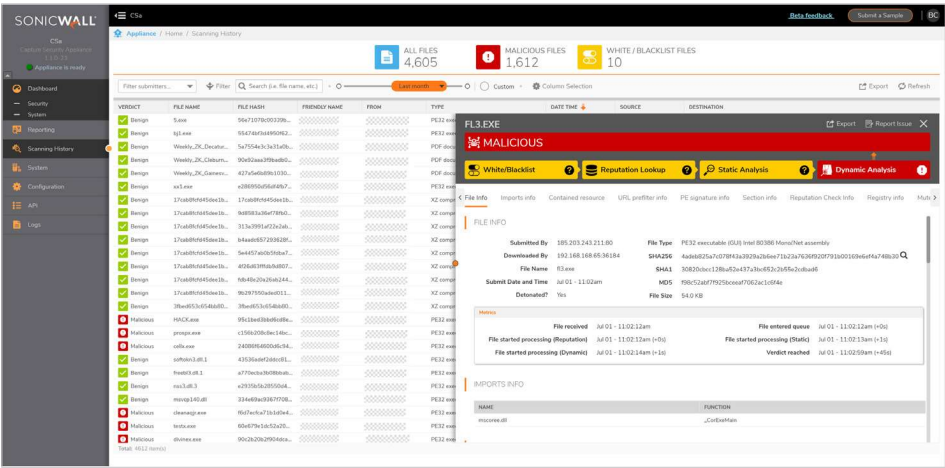
3.可以運行SonicOS 6.5.4.6或更高版本的所有TZ系列、NSa系列和SuperMassive系列。在SuperMassive 9800和NSp 12000系列上不支持。

眾多客戶信賴並從中獲益

- CSa將來自SonicWall的Capture ATP的技術融入到各種外形規格的設備之中。Capture ATP是全球超過150,000位客戶信賴並使用的一種基於雲的服務。
- CSa還可獲得定期情報更新，與通過 SonicWall Capture ATP文件分析全球收集的威脅情報同步。

報告、分析和管理的

- CSa通過易於瀏覽的儀表板和文件分析歷史記錄，探查從所有來源提交的文件，了解提交供分析的文件的頻率、來源、裁決和其他洞察。
- 報告功能全面觀察整個組織的ATP保護，能夠安排根據不同的角色配置的定期報告。
- 管理員可以授予各種角色對CSa1000的精細訪問權限，並能夠限制對UI任何部分的訪問。
- 安全分析師可以訪問掃描歷史，並能夠修改白名單/黑名單和允許的設備，以及報告任何可疑的誤報或漏報。
- 網絡級管理員可以獲得訪問設備的操作配置的權限，但由於保密性原因，他們不能查看提交的文件及其來源。



功能特性

- 信譽和全球裁決查找（可配置）
- 採用RTDMI進行靜態分析和動態分析
- 哈希/域上的白名單/黑名單
- 可配置的計劃報告
- 基於角色的管理（可配置角色）
- 管理-通過專用管理接口或常規網絡接口的HTTPS或SSH
- SSH控制台訪問
- 日志記錄和警報
- 帶有自動白名單/黑名單的誤報和漏報報告
- 直接連接或通過VPN（IP可尋址）
- 封閉式網絡操作
- 針對文件提交和分析的REST API支持
- 帶有安全啟動和信任鏈的強化操作系統，可防止篡改
- 本地日志記錄

1.分析吞吐量取決於網絡連接、文件類型、壓縮級別，可能與公布的數字有所不同。
2.雖然沒有硬性限制，但設備數量將由每個設備提交的文件數量決定。發布時的推薦範圍約為250個設備。
3.可以運行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NSp 12000系列上不支持。

部署選項

- SonicWall CSa部署快速而簡單，只需配置基本的網絡、報告和允許的設備訪問即可開始使用
- CSa構建為IP可尋址，因此只要提交供分析的文件的設備可以訪問它，就可以部署到任何地方

CSa 1000 有三種主要的部署方法：

單一辦公室/單一位置

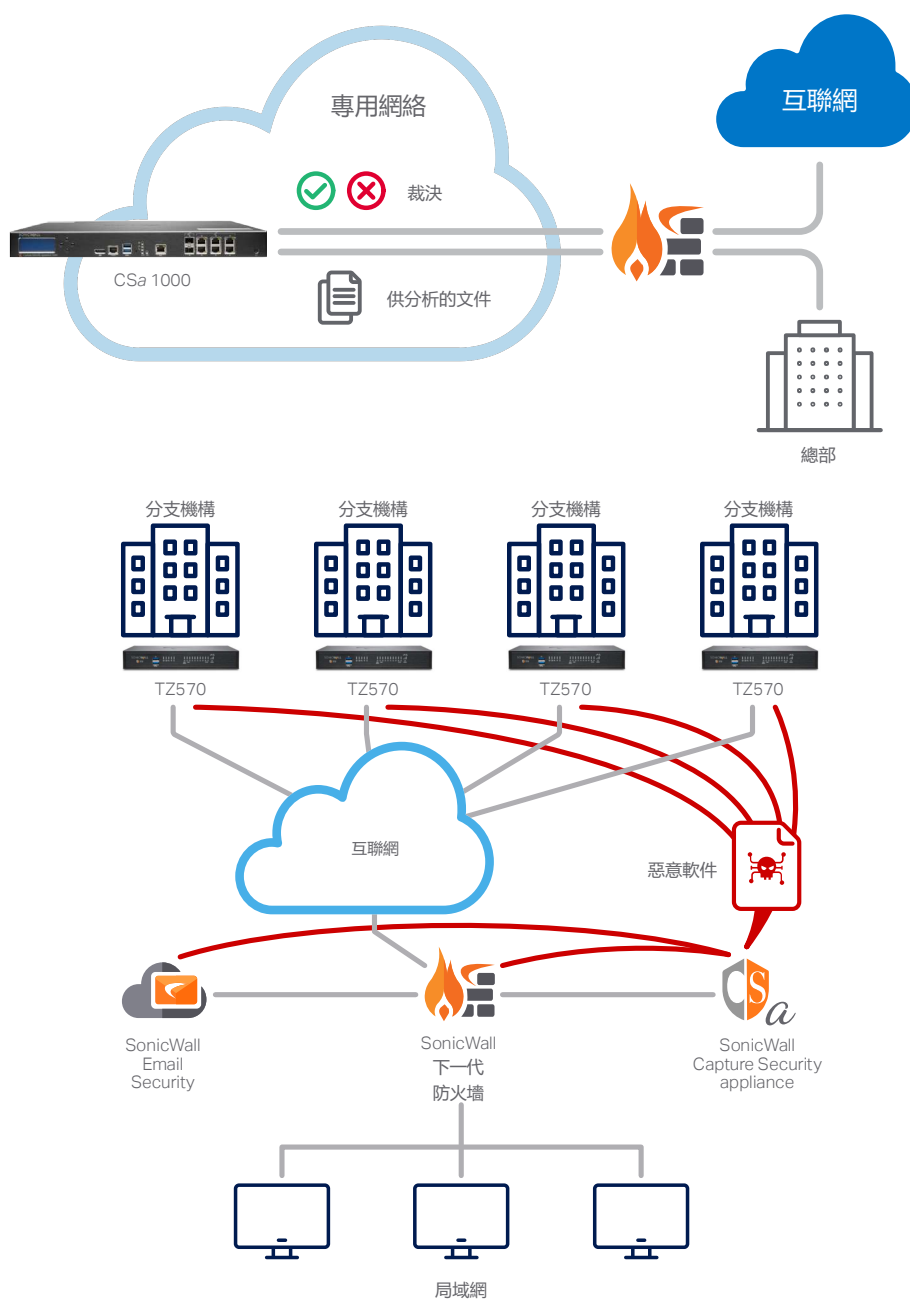
- CSa可以部署在網絡上的任何地方，只要使用它的產品能夠通過IP訪問它¹
- 部署CSa後，可以將防火牆和電子郵件安全系（其他解決方案待定）配置為將可疑文件重定向到CSa而非雲，以進行ATP分析

分布式企業/多個位置

- 可以將多個辦公室/分支機構配置為共享對單個CSa設備的訪問權限，該設備可以部署在中央總部數據中心或所有設備可訪問的遠程數據中心
- 可以直接通過互聯網或通過VPN訪問
- 可以使用GMS或基於雲的NSM集中化管理解決方案來完成指向CSa的SonicWall系統的大規模配置，以實現快速配置和部署

REST API 網關

- CSa系列具有REST API接口，可供威脅情報團隊通過其自己的腳本、Web門戶集成和其他安全產品來提交文件，以進行分析和獲得查詢結果
- 有關如何開始使用CSa的API腳本和代碼示例的說明，可在以下網站獲得：
<https://github.com/sonicwall>



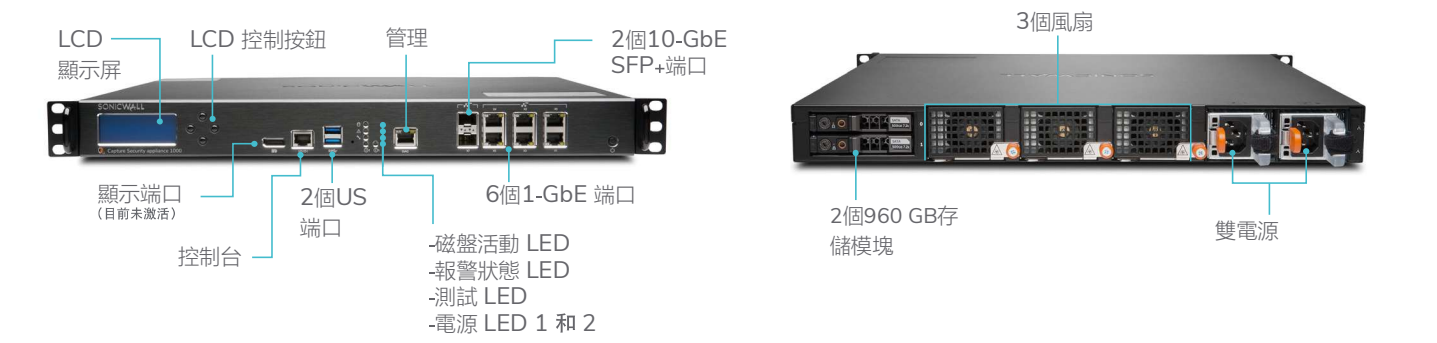
* ¹SonicWall防火牆還需要使用2259端口並通過UDP進行訪問

1.分析吞吐量取決於網絡連接、文件類型、壓縮級別，可能與公布的數字有所不同。

2.雖然沒有硬性限制，但設備數量將由每個設備提交的文件數量決定。發布時的推薦範圍約為250個設備。

3.可以運行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NSp 12000系列上不支持。

CSa 1000



SonicWall CSa 1000 規格

功能特性	
信譽和全球威脅查找吞吐量 (每小時文件數) ¹	12,000
真實文件混合吞吐量 (每小時文件數) ¹	2,500
動態分析(RTDMI)吞吐量 (每小時文件數) ¹	300
最大文件大小	100 MB
支持的最大設備數 ²	基於性能
最大存檔掃描深度	3
REST API 支持	是
支持的 SonicWall設備	TZ、NSa 和 SuperMassive (運行 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
支持的文件類型	.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 .bzp2 .7z .xz .gz .zip
數據保留期	不受限制, 受存儲限制
存儲	2 個 1TB SSD (RAID 1)
接口	(6)-端口 1GE、(2)-端口 10Gb SFP+、(2) USB、(1) 控制台
專用端口管理	是 (X0)
認證	FIPS 140-2 待定
產品特點	
外形規格	1U
尺寸	17.0 x 16.5 x 1.75 英寸 (43 x 41.5 x 4.5 厘米)
設備重量	18.3 磅 (8.3 千克)
加密數據加速 (AES-NI)	是
MTBF (@ 25° C 或 77° F) , 以小時計算	129,601
電源	雙電源, 可熱插拔
輸入額定值	100-240 VAC, 1.79 A
功耗	114 W
總散熱	389 BTU
環境	WEEE、歐盟 RoHS、中國 RoHS
非運行沖擊	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
工作溫度	0° C 至 40° C (32° F 至 104° F)
TPM	是

1.分析吞吐量取決於網絡連接、文件類型、壓縮級別, 可能與公布的數字有所不同。
2.雖然沒有硬性限制, 但設備數量將由每個設備提交的文件數量決定。發布時的推薦範圍約為250個設備。
3.可以運行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。

產品	SKU
Capture Security Appliance CSA 1000	02-SSC-2853
Capture Security Appliance CSA 1000 帶情報更新和支持捆綁包 - 1 年	02-SSC-5637
Capture Security Appliance CSA 1000 帶情報更新和支持捆綁包 - 3 年	0 -SSC-5638
Capture Security Appliance CSA 1000 帶情報更新和支持捆綁包 - 5 年	02-SSC-5639

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

REST API 激活 (僅 REST API 運行才需要此服務。必須應用在“情報更新、激活和支持”服務之上)	SKU
適用於 SonicWall Capture Appliance CSA 1000 的 REST API 激活 1 年	02-SSC-4706
適用於 SonicWall Capture Appliance CSA 1000 的 REST API 激活 2 年	02-SSC-4707
適用於 SonicWall Capture Appliance CSA 1000 的 REST API 激活 3 年	02-SSC-4708
適用於 SonicWall Capture Appliance CSA 1000 的 REST API 激活 4 年	02-SSC-4709
適用於 SonicWall Capture Appliance CSA 1000 的 REST API 激活 5 年	02-SSC-4710
適用於 SonicWall Capture Appliance CSA 1000 的 REST API 激活 6 年	02-SSC-4711

1.分析吞吐量取決於網絡連接、文件類型、壓縮級別，可能與公布的數字有所不同。
2.雖然沒有硬性限制，但設備數量將由每個設備提交的文件數量決定。發布時的推薦範圍約為250個設備
3.可以運行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NSp 12000系列上不支持。

關於 SonicWall

SonicWall 為超分布式時代和每個人都遠程辦公、每個人都移動辦公、每個人都都不太安全的工作現實提供了Boundless Cybersecurity。通過了解未知、提供實時可見性並實現經濟學突破，SonicWall為世界各地的大型企業、政府和中小企業彌補了網絡安全業務缺口。有關詳情，請訪問 www.sonicwall.com