產品型錄

Symantec SSL Visibility Appliance

免除加密流量產生的安全盲點

概述

提供無與倫比的加密流量能見度，對抗進階威脅

- 可自動識別所有 SSL/TLS 流量，不受通訊埠或應用程式限制
- 可找出使用 SSL 略過偵測的隱藏威脅，例如 Dyre 和 Zeus 特洛伊木馬程式、Upatre 指令與控制 (C&C) 及 VMZeus C&C 等等。

支援隱私權及合規計畫

- 選擇性解密流量，因應資料隱密性及合規要求
- 針對加密流量執行可接受使用政策

與現有安全基礎架構緊密整合

- 保持及持續擴大基礎架構的 ROI
- 支援多個網路區段，並可同時饋送主動及被動安全硬體裝置及 ProxySG

簡化管理作業

- 提供詳細記錄和警示，輕鬆找出 SSL 使用的趨勢及潛在問題
- 與管理中心整合進行組態備份、排程及同步

簡介

加密可保護資料隱私權及整合性，不過也會產生盲點，攻擊者利用 SSL 進行刺探及規避安全控管裝置。由於現今有一半以上的流量是加密的，因此在組織的安全態勢之中產生相當大的缺口，造成漏洞與風險增加及聲譽受損等問題。Symantec SSL Visibility Appliance 是加密流量管理解決方案組合的主要元件，可協助組織以符合成本效益的方式，消除環境之中的盲點，並讓安全基礎架構投資發揮最大效益。賽門鐵克可讓組織在面對加密流量時，享有所需的能見度及控制能力，確保遵循各種隱私權、法規及可接受使用政策。

提供加密流量的能見度以提升安全性

SSL Visibility Appliance 是任何組織流量管理策略之中不可或缺的元件，提供能見度協助掌握加密流量，確保攻擊無法規避偵測。賽門鐵克可識別及解密所有 SSL 連線及應用程式，涵蓋所有網路通訊埠 (即使不是常規的通訊埠也沒問題，例 HTTPS 不是 443 Port)。現有安全基礎架構可利用解密後的流量，強化偵測及保護對抗進階威脅的能力；SSL Visibility Appliance 也可負起需要大量處理的解密作業，協助提升組織網路及安全基礎架構的整體效能。

圖 1.SSL Visibility Appliance 機型 SV2800B。

支援隱私權及合規計畫

SSL Visibility Appliance 可作為有效的政策執行點，控制整個企業的 SSL 流量，不但可以降低加密流量的風險，也能維持遵循各種相關隱私權政策及法規要求。組織可利用適合政策的主機分類及 SSL 流量類型，輕鬆建立及自訂嚴僅政策，選擇性解密流量因應業務需求 (例如「不解密由企業傳出的財務或銀行流量」)。政策則可輕鬆設定，用於控制過時或脆弱的密碼及標準，例如使用 SSL v3.0 的流量。

這樣可協助組織專注於風險最高的通訊內容，有效地在安全性與資料隱密性及遵循要求之間取得平衡。這些政策也能利用賽門鐵克領先市場的全球智慧型網路 (Global Intelligence Network)，交流及更新全球 SSL 主機分類、威脅及惡意軟體的各種情報。

提供無與倫比的效能及規模

SSL Visibility Appliance 以線路速率運作，提供深入加密流量及潛在威脅的能見度，不會妨礙裝置或網路效能。硬體裝置提供：

- 線路速率網路效能；非 SSL 流量的通訊埠間延遲不到 40 毫秒。硬體裝置支援解密 9 Gbps 的 SSL 流量，適用於所有 SSL/TLS 版本及 70 種以上加密套件。
- 高連線速率/流量數：可檢測最多 800,000 個 SSL 同時會話連線，並支援每秒 30,000 個以上新會話連線交握。
- 高可用性：提供整合式的 fail-to-wire/fail-to-open 硬體，以及可設定連結狀態監控及映射，提供保證的網路可用性及網路安全。

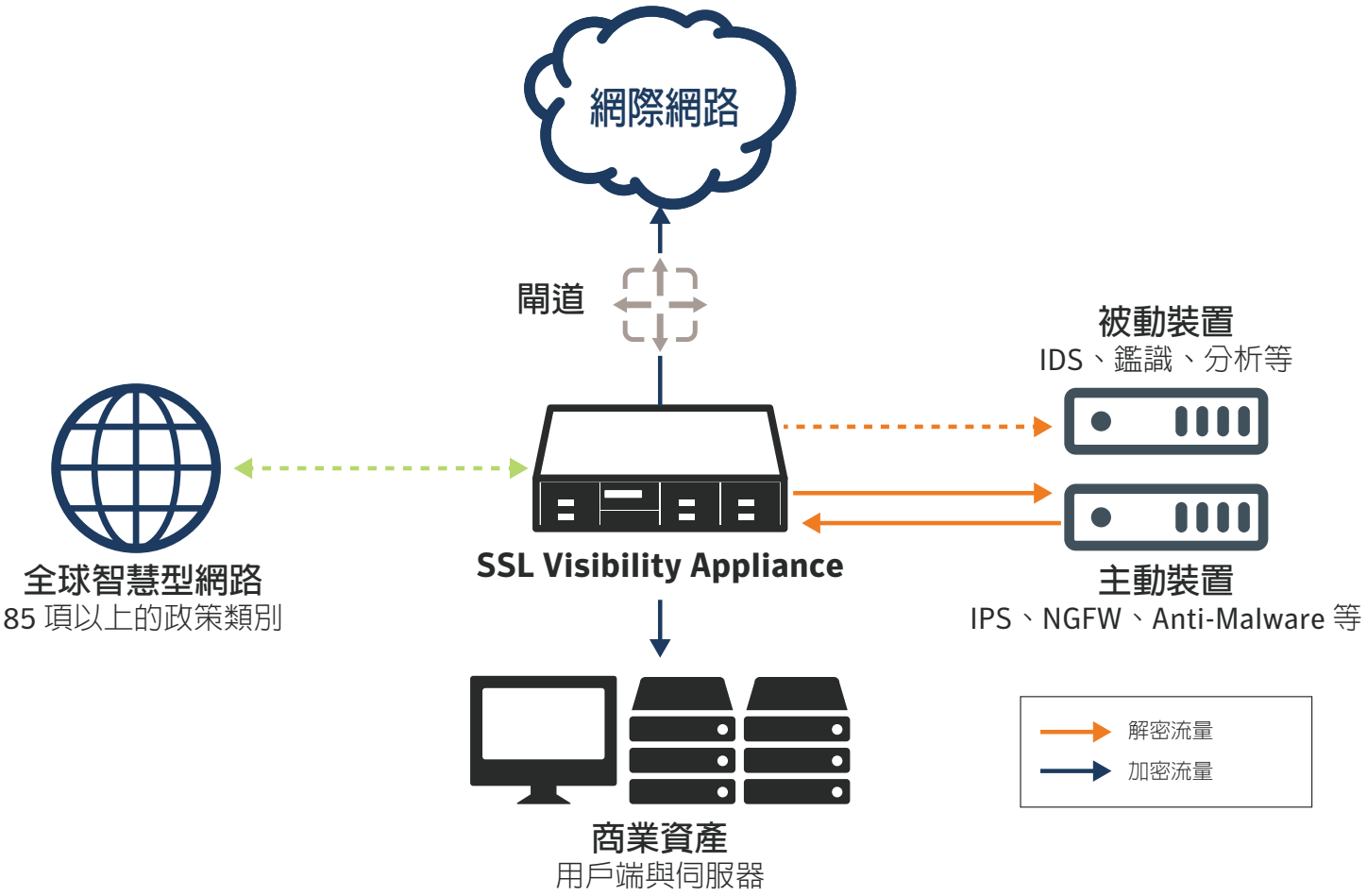
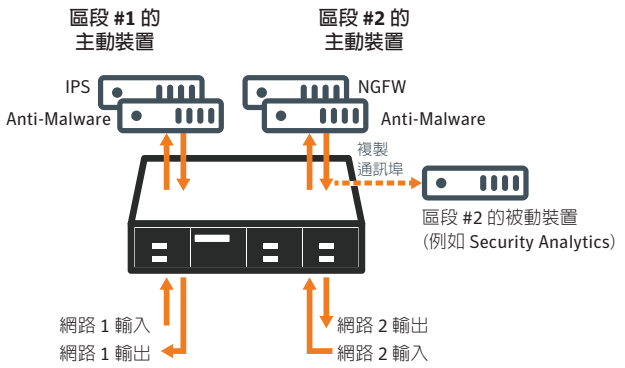


圖 1.Symantec SSL Visibility Appliance 可協助您集中管理加密流量。

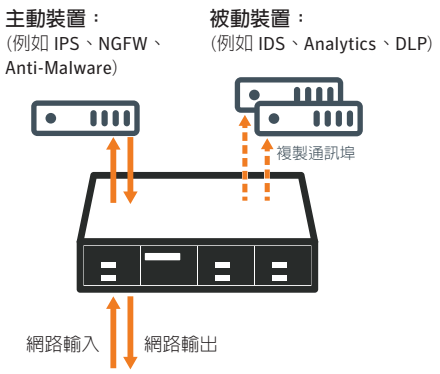
與現有基礎架構緊密整合

SSL Visibility Appliance 可在現有基礎架構中輕鬆部署，無需使用重複的安全硬體裝置，或重新打造網路基礎架構。硬體裝置提供：

- 提升基礎架構 ROI：強化網路及安全硬體裝置的效能及現有功能，卸載解密作業，並提供加密流量的能見度，協助現有資安設備看見隱的威脅。
- 網路透明度：部署 SSL Visibility Appliance 對終端系統及串接網路元件都是透明的。其中不需要重新設定網路、變更 IP 位址或拓撲，或修改用戶端 IP 及網頁瀏覽器設定。



- 彈性的部署選項：支援多個 in-line 或 tap 區段，饋送一個以上的主動或被動附加硬體裝置 (支援的區段數量，依不相同機型而定)。



- 複製通訊埠：SSL Visibility Appliance 能夠透過未使用的網路埠，傳送複本至許多裝置。這樣可讓組織將所有流量 (解密及非 SSL) 饋送至額外其他的被動式安全設備被動裝置。
- 應用程式保護：以產生 TCP 串流的方式，將解密的純文字傳送至安全硬體裝置，並包含當初接收時的封包標頭。這樣可讓新一代防火牆 (NGFW)、入侵偵測/預防系統 (IDS/IPS)、資料遺失預防 (DLP) 系統及安全分析等應用程式和硬體裝置，擴展範圍及提供保護，對抗隱藏在之前加密流量之中的威脅。以上作業無需附加安全工具的任何特殊軟體或功能。SSL Visibility Appliance 饋送 ProxySG 時，必須執行 4.x 版軟體，而 ProxySG 必須執行 6.7.2.x 或更新版軟體。
- 完整支援：提供完整的 inbound 及 outbound SSL 階段作業能見度；支援非對稱流量路由網路；檢測 outbound SSL 流量時支援多種重簽憑證授權中心 (CA)；可匯入許多伺服器金鑰/憑證配對，以檢測外往內企業 SSL 伺服器的 inbound SSL 流量。
- 輸入彙整：在一個被動區段中可彙整多個網路 tap 的流量給需要的設備進行檢測。

簡化管理作業

SSL Visibility Appliance 易於設定及管理，提供：

- 單一裝置管理：提供功能強大、以 SSL 維護安全且易於使用的網頁式使用者介面 (UI) 用於設定及管理。
- 集中管理：可讓 Symantec Management Center 管理多個硬體裝置，進行盤點及系統效能監控、運作狀態監控、組態備份及排程作業，以及組態同步。Management Center 也支援基於角色控管存取權限(RBAC)。
- 電子郵件警示：設定記錄觸發警示，可透過電子郵件立即轉送，或每隔一段時間傳送給指定的網路管理員。
- SSL 階段作業識別：提供階段作業記錄，詳細說明所有 SSL 流量、是否解密檢測，並允許偵測可疑的 SSL 趨勢或樣式。
- Syslog 報告：支援最多 8 台遠端 Syslog 伺服器，協助強化分散式環境之中的報告與記錄應用程式。
- SNMP 支援能力：可由第三方裝置透 SNMP v3 標準進行監控和管理。

	SV800-250M-C	SV800 - 500M-C	SV1800-C/-F	SV2800B	SV3800B	SV3800B-20
使用 3.X 系列軟體的效能						
Total Packet Processing Capability	8 Gbps	8 Gbps	8 Gbps	20 Gbps	40 Gbps	40 Gbps
SSL Inspection Throughput	250 Mbps	500 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	9 Gbps
Cut-through Latency	<40µs	<40µs	<40µs	<40µs	<40µs	<40µs
Concurrent SSL Flow States	20,000	20,000	100,000	200,000	400,000	800,000
Full Handshake RSA 1024 bit	1,000 per second	2,000 per second	7,500 per second	10,500 per second	12,500 per second	30,000 per second
Full Handshake RSA 2048 bit	1,000	2,000	3,000	3,000	6,000	6,000
Full Handshake ECDHE256	500	1,000	3,500	6,000	8,000	11,000
SSL Session Log Entries	32,000,000	32,000,000	32,000,000	32,000,000	32,000,000	32,000,000
使用 4.X 系列軟體的效能						
Total Packet Processing Capability	8 Gbps	8 Gbps	8 Gbps	20 Gbps	40 Gbps	40 Gbps
Classic segment Inspection capacity	220 Mbps	450 Mbps	1.30 Gbps	2.80 Gbps	4.20 Gbps	7.30 Gbps
Proxy segment Inspection capacity	0.2 Gbps	0.4 Gbps	0.9 Gbps	2.6 Gbps	3.9 Gbps	6.6 Gbps
Concurrent SSL Flow States	20,000	20,000	100,000	200,000	400,000	800,000
New Full Handshake RSA 1024 bit	1,000 per second	2,000 per second	7,300 per second	10,500 per second	12,500 per second	25,000 per second
New Full Handshake RSA 2048 bit	1,000	2,000	3,500	4,500	5,700	5,800
New Full Handshake SSL ECDHE	450	900	2,800	6,000	8,000	12,000
SSL Session Log Entries	32,000,000	32,000,000	32,000,000	32,000,000	32,000,000	32,000,000
規格						
Configurations	Network Interfaces: Fixed 8 x 1 Gbps Copper	Network Interfaces: Fixed 8 x 1 Gbps Copper	Network Interfaces: Fixed 8 x 1 Gbps Copper or 8 x 1 Gbps Fiber (SX)	Network Interfaces: 3 Netmod Slots - Various 1 Gbps and 10 Gbps Interface Options	Network Interfaces: 7 Netmod Slots - Various 1 Gbps and 10 Gbps Interface Options	
Power Supplies	1 x 150W	1 x 150W	1+1 Redundant 450W	1+1 Redundant 750W	1+1 Redundant 750W	
Management Interfaces	1x RJ45	1x RJ45	1x RJ45	1 x RJ45	1 x RJ45	
Manageability	SNMP v1, v2c and v3 supported; GETs and TRAPs supported across multiple Symantec MIBs; SETs supported only for the System Group					
Display	LCD 16 x 2 Char. Display	LCD 16 x 2 Char. Display	LCD 16 x 2 Char. Display	LCD 16 x 2 Char. Display	LCD 16 x 2 Char. Display	
Operating Temperature	5°C to 40°C	5°C to 40°C	5°C to 40°C	10°C to 35°C	10°C to 35°C	
Storage Temperature	-10°C to 60°C	-10°C to 60°C	-10°C to 60°C	-10°C to 60°C	-10°C to 60°C	
Dimensions (in.) H x W x D	1.75 x 8 x 12.75	1.75 x 8 x 12.75	1.75 x 17 x 20	1.75 x 17.5 x 29	3.5 x 17.5 x 29	
Regulatory and Environmental Standards/Compliance	CE (EN55022, EN55024, EN60950), FCC part 15 class A, UL60950-1					
Certifications	None	None	FIPS 140-2 level 2 for the SV180B, SV2800, SV2800B, SV3800, SV3800B and SV3800B-20 models. These models also have Common Criteria NDPP and SOGIS certification and are in process for EAL3+. These models also have UC/APL certification.			
Modes of Operation (per network segment)	Passive-Tap, Passive-Inline, Active-Inline Fail to Network (FTN) and Fail to Appliance (FTA), ProxySG segment (4.x only)					
Visibility Modes	Controlled-client (Re-sign) Mode [In-line Only], Controlled-server (Known-key) Mode. A full list of Modes is available in the Administrator Guide.					
Encryption	TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0, SSLv3, partial SSLv2					
Public Key Algorithms	RSA, DHE, ECDHE					
Symmetrical Key Algorithms	AES, AES-GCM, 3DES, DES, RC4, ChaCha20-Poly1305, Camellia					
Hashing Algorithms	MD5, SHA-1, SHA-2, SHA256, SHA384					
RSA Keys	512 to 4096 bits					
軟體						
Software Licensing	A Symantec License is required for inspection activation for each appliance. Please refer to the Licensing section within the Symantec Support portal. Host Categorization is an optional, subscription-based service that requires an additional license per appliance.					

Symantec™ 台北市信義區忠孝東路 5 段 68 號 29 樓 | +886 2 8729 9277 | +886 2 8729 9257 | **www.symantec.com/zh/tw**