整合式安全

Symantec™ Gateway Security 1600 Series 硬體裝置

專為 200 位以內的使用者網路環境所設計的堅實且符合成本效益之防護方案

概觀

Symantec Gateway Security 1600 Series 是價格合理、可靠且容易管理的「整合威脅管理」(UTM)[1] 安全硬體裝置，由賽門鐵克獲獎的技術所引領，包括業界最值得信賴的防毒及入侵偵測/防禦技術。這個新一代的閘道安全硬體裝置將八個基本安全功能緊密整合，在降低安全管理複雜性的同時，帶來最大的效益；以單一、集中管理的硬體裝置提供多功能的網路安全。這個解決方案可為擁有高達 200 位使用者的獨立式 ROBO (遠端辦公室/分公司) 網路環境提供完善的整合威脅管理 (UTM)。

重要功能

- 整合完整檢測 (full-inspection) 的應用程式 Proxy 防火牆，其優於狀態式檢測 (Stateful Inspection) 防火牆的地方在於，前者會使用包括實證之即時偵測—「通訊協定異常偵測 (Protocol Anomaly Detection)」等多種技術，因此可檢測網路封包是否符合 RFC 標準) 以辨識初始攻擊 (zero-day)。
- 以價格合理的硬體裝置提供閘道病毒防護、入侵防禦、入侵偵測、垃圾郵件過濾、防間諜程式/防廣告軟體、URL 式的內容過濾 (內含針對不當網站提供的初始攻擊偵測—「動態文件檢視 (Dynamic Document Review)」，方法是套用使用多語言字典進行啓發式掃描)，以及 IPsec 和 SSL VPN 技術。
- 提供緊密結合的整合威脅管理 (UTM) 安全技術，可讓擁有高達 200 位使用者的網路環境獲得最佳的安全效益，並降低採購和管理成本。
- 結合多種初始攻擊偵測技術，包括防毒啓發式技術與 IDS/IPS 弱點攻擊攔截等技術，可精確地辨識與攔截已知及未知的攻擊、病毒和病蟲。
- 具備可擴充的政策式安全設定功能，以及可從中央主控台管理多種 Symantec Gateway Security Series 硬體裝置系列的事件/警示。
- 利用可建立低成本 Internet 服務連線，並提供預設之安全設定的「系統安裝精靈 (System Setup Wizard)」來簡化初始安裝。
- 透過支援硬體使用中/待命 (active/standby) 的備援功能，以及具備失敗接管/容錯移轉與回復功能、兩個 ISP 帳戶的頻寬聚合連結防護，以確保可靠的 Internet 存取。
- 透過 LiveUpdate˛ 來配送安全內容、即時修補程式 (hotfix) 及修正程式 (patch)，可讓您輕鬆管理數以千計的遠端網站部署。
- 提供來自網際網路安全與回應領導廠商—賽門鐵克的可靠防護。

[1] UTM 硬體裝置比標準純防火牆裝置使用更多層的安全防護。

symantec™

多功能

利用緊密整合的安全技術，Symantec Gateway Security 1600 Series 硬體裝置比其他產品更能有效地協調防護及回應，並以更優惠的價格讓您享有整合威脅管理 (UTM) 功能。這套硬體裝置緊密結合多種安全技術，包括：閘道防毒、垃圾郵件過濾技術 (特色為黑名單及啓發式的攔截)、入侵偵測及入侵預防、URL 式的內容過濾 (內含針對不當網站提供的初始攻擊偵測—「動態文件檢視」，方法是套用使用多語言字典進行啓發式掃描)、防間諜程式/防廣告軟體；以及完整檢測的應用程式 Proxy 防火牆，相較於狀態式檢測防火牆，其優點在於使用多種技術 (包括經實證的即時偵測方法—「通訊協定異常偵測」，會檢測網路封包是否符合 RFC 標準) 以辨識初始攻擊。堅實的 VPN 技術包括 IPsec (支援閘道對閘道以及用戶端對閘道的通道)，以及無用戶端 (clientless) 的 SSL 型用戶端對閘道通道，使您無須安裝及設定 IPSec 用戶端軟體。

主動式防護

Symantec Gateway Security 1600 Series 硬體裝置能主動抵禦多種威脅，包括病毒、病蟲、間諜程式、垃圾郵件、入侵及混合式威脅，並以相容設計 (compatibility-engineered) 且由單一廠商提供的解決方案來降低採購、安裝及管理成本。藉由提供多種偵測技術 (包括通訊協定異常偵測及弱點攻擊攔截) 來精確地辨識及攔截已知及未知的 (初始) 攻擊及病蟲—這些硬體裝置便能主動防護攸關業務的網路。

可靠的 Internet 存取

為確保企業資源、合作夥伴及客戶都能使用 Internet，因此透過支援硬體使用中/待命的備援功能、具有失敗接管/容錯移轉與回復功能，以及含有頻寬聚合的 ISP 連結防護來維持連線。

容易管理及維護

完善的管理功能，可擴充安全政策設定，且能透過易於使用的 Web 型介面 (SGMI) 來管理所有安全功能的事件/警示。硬體裝置的安裝已利用「系統安裝精靈」簡化，此精靈會建立通往低成本 Internet 服務的連線，並提供預設的安全設定。此外，該硬體裝置能透過 LAN 或 WAN 連線讓本機及遠端管理更加容易。

更迅速的安全回應

迅速回應是確保企業永續營運並持續獲得重要資訊的關鍵。Symantec Gateway Security Series 硬體裝置會在可取得病毒定義檔、IDS 簽章、URL 清單及軟體修補程式時，儘速透過 LiveUpdate 取得，使您的防護保持最新，卻不會增加任何管理負擔。

整合式安全
Symantec Gateway Security 1600 Series 硬體裝置

可擴充、政策式的閘道安全功能

Symantec™ Gateway Security Advanced Manager (SGS AM) 硬體裝置選購項目會將額外的功能新增到安全閘道管理介面 (SGMI) 中。SGS AM 提供集中式的多系統政策管理、架構、記錄、警示及報表，適用於 Symantec Gateway Security 400、1600 及 5000 系列。它從 Symantec Gateway Security Series 硬體裝置合併事件資訊，然後經由中央管理主控台標準化和彙整資料，以針對企業安全狀態提供一致且全面的檢視。

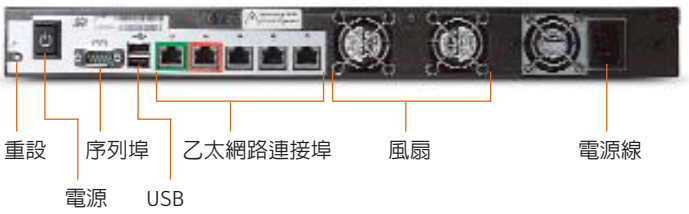
可針對幾組 Symantec Gateway Security Series 硬體裝置建立安全政策，然後自動配送至網路中的所有硬體裝置。當新威脅產生時，企業組織可以輕鬆地變更這些政策，然後將它們重新配送到部署在整個企業裡的 Symantec Gateway Security Series 硬體裝置。如此可讓企業組織維持其網路的完整性，並以近乎即時的方式回應威脅。

它藉由讓威脅更易於辨識以及透過自動通知來警示管理員，加速對安全威脅的回應，並使系統運作時間達到最長。此外，角色型的管理和高度擴充與安全的架構，使這個產品非常適用於企業與受管理的安全服務環境。

Symantec Gateway Security Advanced Manager 讓管理員能更有效地利用分散在企業內之 Symantec Gateway Security Series 硬體裝置所產生的資料。企業組織會因為強化的整體安全狀態而獲益，更快速的回應安全事件、更能做出資訊充分且智慧的決策，協助企業以更低的整體擁有成本部署安全閘道。

硬體規格

為符合具有小型辦公室效能需求之企業組織，以及擁有 ROBO 網路環境的大型企業之需求，Symantec Gateway Security 1600 Series 提供兩種完全整合的機型，不僅能提供可靠的安全管理，也提供優惠的價格及絕佳的效能。Symantec Gateway Security 1600 Series 可符合擁有高達 200 名使用者之辦公室所需的安全及效能需求，並且在搭配使用 Symantec Gateway Security 5600 Series 後，還可以將業界領先的整合威脅管理 (UTM) 功能擴展到最廣的企業網站範圍。



圖為 Symantec Gateway Security 1660。

Symantec Gateway Security 1620 共有三個乙太網路連接埠。

symantec.

整合式安全
Symantec Gateway Security 1600 Series 硬體裝置

機型		1620	1660
建議使用者		內含無限制的節點授權 可保護高達 100 個節點	內含無限制的節點授權 可保護高達 200 個節點
安全功能	整合威脅管理 (UTM)—下列安全功能經過全面整合，達到最大的效益，且更容易管理，複雜性也較低：		
	完整檢測防火牆 (Full inspection firewall)	具備完整檢測功能的多種防火牆技術，適用於：HTTP/HTTPS、FTP、SMTP、POP3、CIFS、Telnet、含 T.120 支援的 H323、DNS、NBdgram 及 NNTP。透過自訂的 Proxy 也能保護其他服務。此外，也提供電路等級分析、緩衝區溢位攔截、通訊協定異常偵測、URL 特徵比對/攔截，以及網路位址轉譯 (NAT)	
	閘道防毒	超過 70,000 個病毒定義檔，用於掃描 HTTP、SMTP、POP3 及 FTP 流量。根據政策過濾郵件	
	垃圾郵件過濾	具備白/黑名單及關鍵字攔截功能的啓發式防護	
	擴充的防護	500 個以上的定義檔，抵禦惡作劇軟體、間諜程式、廣告軟體及其他非病毒引起的風險	
	入侵偵測	超過 3,100 個可動態更新的特徵資料	
	入侵預防	攔截已知、未知 (初始) 及 DoS 攻擊，也能攔截 P2P 及即時通訊威脅	
	內容過濾	完整的 URL 清單，內含超過 30 個種類 4 百萬個項目；以及動態文件檢視技術—針對不當的網站提供的初始攻擊偵測，方法是套用一種使用多語言字典進行啓發式掃描	
	最高安全層級整合	其他競爭者採用拼湊的多功能解決方案，無法提供緊密安全功能整合所具備的下列優點： • 防火牆及 IDS/IPS 功能可針對入侵偵測、防禦及對策進行溝通與協調。 • 防火牆及防毒功能可進行溝通與協調，不讓受感染的資料 (郵件、檔案及網頁) 通過防火牆。 • 內容過濾及存取控制可進行協調，以限制存取 URL，加上現在有了「動態文件檢視」之後，還能在 HTML 文件層級強制執行政策。	
	虛擬私有網路	IPsec 及/或無用戶端 (SSL) 的 VPN 都有強化的「VPN-only」介面設定支援，適用於無線網路安全。內含 Client VPN v9 CD-ROM	
	驗證	針對雙重認證 (multi-factor) 的通訊協定提供驗證支援，例如 Radius、LDAP、AD 及 RSA Secure ID 或 PKI 憑證	
	用戶端政策遵循 (Client Compliance)	確保透過 IPsec 或無用戶端 SSL VPN 從遠端連線的使用者已適當地啓用其「賽門鐵克個人防火牆」及「賽門鐵克防毒」主機的防護	
	授權	每個硬體裝置啓用套件都包含無限的授權，適用的功能如下：防火牆、防毒、垃圾郵件過濾、防間諜程式、入侵偵測、入侵防禦、內容過濾、閘道對閘道 VPN 通道，以及高可用性	
	用戶端對閘道 VPN Sessions (Client-to-Gateway VPN Sessions)	內含的 Client VPN 軟體，可安裝在無限個用戶端上。Client VPN 的授權適用於閘道上同時並存的階段作業。內含 1 個 IPsec 或無用戶端 SSL 階段作業。可使用 5 及 25 個階段作業的附加授權	
硬體功能	乙太網路介面 10/100/1000 RJ45	(3) 1 個內部介面、1 個外部介面， 以及 1 個多用途介面[2]	(5) 1 個內部介面、1 個外部介面， 以及 3 個多用途介面[2]
	記憶體	512 MB	768 MB
	硬碟 (內含)	40 GB	40 GB
	加密加速	否	是，AES 及 3DES
	其他介面	1 序列，2 USB	1 序列，2 USB
效能	狀態式防火牆傳輸量	100 Mbps	200 Mbps
	應用層檢測防火牆傳輸量	80 Mbps	160 Mbps
	VPN 傳輸量	20 Mbps AES	100 Mbps AES
	防火牆+防毒傳輸量	30 Mbps	60 Mbps
	最大 IPsec VPN 通道	30	125
	同時連線數	25,000	50,000

[2] 多用途介面可設定為：第二個外部介面，以達到雙重 ISP 頻寬聚合/失敗接管、一個內部介面、一個 DMZ 介面、一個僅限 VPN 的無線網路安全連接埠，或一個通往熱待機 (hot-standby) 硬體裝置的同步連結。

symantec™

整合式安全

Symantec Gateway Security 1600 Series 硬體裝置

機型		1620	1660
高可用性	ISP 連結防護	自動連結失敗偵測，流量失敗接管/容錯移轉與回復，這是藉由連結通訊協定/連接埠針對兩個外部連線進行負載平衡來達成的	
	硬碟防護	熱待機硬體裝置備援功能，可自動同步化設定及狀態	
	熱待機授權	有特別折扣的熱待機授權及維護軟體套件	
	備用元件	無	無
	可現場置換的元件	無	無
網路功能	連接低成本的 Internet 服務	可針對下列項目設定每一個連接埠：PPPoE、PPTP、DHCP、靜態 IP、動態 DNS，以及具備 MTU 調整功能的 MAC 位址複製	
	彈性的 IP 定址	可在機上設定的 DHCP 伺服器，任何定義的內部介面或 VLAN 都受支援；也支援 DHCP 轉接	
	VLAN 支援	802.1q 可用於高達 16 個 VLAN 的 VLAN 標記支援	
	動態路由	OSPFv2 及 RIPv2 通訊協定支援	
控制項及指示器	前方面板指示器	綠色 LED 表示電源、磁碟活動、就緒及乙太網路活動 (每個連接埠)；琥珀色 LED 表示注意	
	控制項	電源開關，多功能重設按鈕	
管理	簡易安裝	系統安裝精靈、網路連線精靈及預設的安全政策設定簡化了安裝	
	系統管理介面	透過內部或外部連接埠建立網路瀏覽器連線，使硬體裝置的設定更容易，也能輕鬆檢視即時系統狀態和圖形化的報表	
	LiveUpdate	賽門鐵克的全球伺服器網路會自動傳遞兩種更新： 1) 軟體修補程式及即時修補程式 2) 病毒及間諜程式定義檔、IPS 特徵資料及內容過濾的安全內容更新 URL 清單及垃圾郵件過濾字典	
集中式管理	Symantec Gateway Security Advanced Manager Appliance	可選購的硬體解決方案，可針對整個企業內數以千計的 Symantec Gateway Security 硬體裝置進行最佳化，達到集中式管理、記錄、警示及報表等功能	
	Policy-based security configuration	Multiple policies can be created/modified and automatically downloaded to appropriate appliance groups	
	事件管理	透過彙整、正規化、減少與視覺化來將事件資料轉換為可供行動參考的安全資訊	
	監控及警示	彈性且可自訂的警示，可根據預先設定的臨界值 (threshold) 設定以通報偵測到的重大事件，並立即透過多種警示機制來傳遞通知	
	角色型管理	可針對集中式管理主控台提供多層級的角色型存取，將管理員類別的功能限制為只能採取特定動作	
實體規格	可置於桌上	提供塑膠腳墊	
	機架式 (Rackmountable)	19 吋機架高度為 1U，提供掛載的支架	
	尺寸	17" 寬 x 1.75" 高 x 10" 深 (431.8 公釐寬 x 44.3 公釐高 x 254 公釐深)	
	重量	11.5 磅 (5.22 公斤)	12.0 磅 (5.44 公斤)
	出貨重量	17.1 磅 (7.76 公斤)	17.6 磅 (7.98 公斤)
電源規格	輸入 AC 電源	90–240 VAC / .55 A	
	輸入頻率	47–63 Hz	
	一般功率	31 瓦特	35 瓦特
	最大電源功率特	250 瓦特	250 瓦特
環境規格	操作溫度 (高度 0–1000 公尺)	0˚C–40˚C，32˚F–104˚F	
	操作溫度 (高度1000–2000 公尺)	0˚C–35˚C，32˚F–95˚F	
	儲存溫度	-20˚C–70˚C`，-4˚F–149˚F	
	操作溼度	15 到 90% (非凝結)	
	儲存溼度	15 到 90% (非凝結)	
	高度	0–2000 公尺	
	散熱	兩個底架風扇，一個電源供應器風扇，CPU 散熱裝置	

symantec™

整合式安全
Symantec Gateway Security 1600 Series 硬體裝置

Model		1620	1660
法規遵循	安全認證	UL、cUL、CB、TUV/GS、NOM、KONCAR、SABS、SASO、SII	
	EMC 認證	FCC Class A、CE Class A、C-Tick、VCCI Class A、CISPR Class A、ICES Class A、BSMI、MIC	
支援及服務系統需求	硬體保固	每個硬體裝置都有一年可退回原廠的硬體保固	
	軟體保固	內含 30 天的軟體保固	
	金級維護	產品啓用套件包含 3 個月的金級維護 (Gold Maintenance)，並提供正常上班時間的電話支援服務、進階硬體更換、軟體升級保證 (upgrade insurance) 及內容更新。每種內容更新類型都有擴充及更新可用	
	白金級支援 (Platinum Support Extends)	將金級電話支援延長到下班後及週末，並允許存取白金級的數位服務 (E-services)	
	DeepSight™ 早期預警	選用的服務，針對全世界即將發生的網路攻擊提供自訂化且完善的警示，也提供攻擊前的預防對策。	
系統需求	Symantec Gateway Security 1600 Series 硬體裝置本身包含所有軟體並且已預先載入系統。透過安全的網路連線達到管理目的，因此可使用任何執行支援之網路瀏覽器版本的系統來管理硬體裝置。		

更多資訊

請造訪我們的網站

http://enterprisesecurity.symantec.com

如您想跟產品專員諮詢此產品

若您需要任何一個分公司的聯絡電話或相關資訊，請造訪我們的網站。

關於賽門鐵克

賽門鐵克是提供解決方案以協助個人與企業確保資訊安全性、可用性與完整性的全球領導廠商。賽門鐵克總部位於美國加州 Cupertino 市，並在全球 40 個以上的國家地區設有營運據點。如需更多資訊，請造訪：

www.symantec.com.tw

台灣賽門鐵克股份有限公司

地址：台北市 105 南京東路五段 188 號 2F-7

電話：(02) 8761-5800

傳真：(02) 2742-2838

地址：台北市 110 基隆路一段 200 號 20F

電話：(02) 8722-7000

傳真：(02) 2345-5009

www.symantec.com.tw

DS-00303-TW