F5 Secure Web Gateway Services 參考架構

為了因應重大安全性缺口、持續性滲透攻擊 (APT)，以及期望全天候、全年無休存取網際網路的「千禧世代」員工，具有遠見的 IT 組織應將 Web 存取及安全性整合為提供高性能的策略性控制點：F5 Secure Web Gateway Services。

技術白皮書

作者：David Holmes

目錄

簡介

近期最受矚目的重大安全性缺口莫過於魚叉式攻擊。此類攻擊會以特定組織的「員工」做為對象，並誘導他們將含有惡意軟體的項目下載至企業網路中。接著，該惡意軟體就會開始洩漏客戶的機密和個人識別資訊 (PII)、營業機密，或金融資產。而較新，甚或更複雜且危險的威脅更是無時不刻猖獗橫行於 Web 中。惡意軟體的現有手法還包括網頁掛馬 (Drive-by Download)、即刻威脅 (Threat Du Jour) 和水坑式攻擊 (Watering-hole Attack)。這些事件的重大程度和影響層面正迫使現今的 IT 安全性組織力圖強化與員工網際網路使用及存取相關的安全性保護網。

傳統上，組織會使用正向 Proxy 來攔截和檢查使用者的對外網際網路連線，並藉此落實旗下使用者的 Web 安全性。曾任職於大型企業網路的員工，應該都有遇過 (而且可能嘗試過加以規避) 這類型的 Proxy。儘管許多廠商已在正向 Proxy 領域中深耕十年之久，卻始終未見任何大幅度的技術進展。

保護對外存取所面臨的挑戰

雖然正向 Proxy 技術面臨停滯，安全性問題卻不會因此減少。眼前的挑戰不斷推陳出新，且特別著重於三個領域：

- 「SSL everywhere」的日益普及導致傳統的正向 Proxy 形同虛設。
- 未預期的釣魚攻擊嚴重性正在急速竄升。
- 日新月異的裝置和系統管理需求正迫使組織考慮整合旗下設備。

儘管這些變革正於世界各地持續發酵，正向 Proxy 解決方案依舊未能跟上腳步。系統管理員正在尋求可因應這些嶄新挑戰的解決方案。

在 SSL 流量和惡意軟體承載的大舉入侵下，傳統的正向 Proxy 已無用武之處，經常需要仰賴個別的補充裝置來補強解決方案。

F5 Secure Web Gateway Services

由於 F5 產品可擔任網路中的策略性控制點，因此，F5 Networks 能在組織進行應用程式交付控制的相同平台上，透過高容量、高效能的 Web 安全性來協助組織保護旗下使用者。

F5 的與眾不同之處

F5® Secure Web Gateway Services 和傳統的正向 Proxy 有何不同？兩者之間有五個主要不同之處，而這些差異也是了解 F5 解決方案如何補全 Web 安全性參考架構的關鍵所在。

- **整合的惡意軟體偵測：**傳統的正向 Proxy 解決方案會進行類似的網址篩選，但需要仰賴額外的設備或裝置來執行惡意軟體偵測。而 Secure Web Gateway Services 解決方案則會將這項功能整合至相同平台中。

- **擴充和效能：**Secure Web Gateway Services 的參考架構會提供遠超過傳統正向 Proxy 的擴充能力。如此便能透過較少的裝置來處理 Web 安全性，並降低企業的資本支出 (CapEx)。

- **SSL 攔截：**SSL 已在所有組織中日益普及，因此，透過適當的方式來攔截和檢查對外 SSL 連線也變得相形重要。傳統解決方案通常會運用 F5 Application Delivery Controller (ADC) 來執行這項功能。而將 Secure Web Gateway Services 整合至主要 ADC 平台，則可帶來整合優勢。

- **同盟單一登入：**放眼今日，F5 解決方案是市面上唯一一個整合同盟單一登入 (SSO) 的解決方案。此一成熟的 F5 技術可協助組織打造網頁驗證入口頁面，進而在每天早上進行使用者驗證，並於當日的其餘時間提供 SSO，藉此強化使用者體驗並節省寶貴的時間。

- **安全性服務的整合：**每個 F5 平台都有提供上述所有對外安全性服務。當然，對內安全性功能也一應俱全。這也意味著，網路中的策略性控制點將可提供對內和對外存取及安全性的整合。

這些差異正是 F5 Secure Web Gateway Services 得以為 Web 安全性和應用程式安全性提供出色架構的最大原因。

Secure Web Gateway 的三大基礎功能

Secure Web Gateway Services 的所有使用案例，都會以下列三項安全性功能為基礎：網址篩選、惡意軟體掃描，以及回報。

網址分類和篩選

在這三項功能之中，最基本的莫過於 Secure Web Gateway Services 所提供的網址分類和篩選。包含數十億筆網址的資料庫會每天進行評分和評估，並提供給 Secure Web Gateway Services 平台，而且每隔數分鐘便進行一次更新。這個網址分類資料庫涵蓋了裝載惡意軟體、釣魚 Proxy 或點擊綁架的網站，而且也能依據企業的專屬內容加以自訂。

惡意軟體掃描

如果需要對特定內容進行額外的惡意軟體掃描，網址分類資料庫就會向 Secure Web Gateway Services 發出通知。之後，F5 解決方案就會以最常見的檔案格式 (例如 Adobe Flash 和 Adobe PDF) 來攔截和檢查惡意軟體承載和連結。

回報

系統管理員需具備檢視能力，才能訂定良好的原則，並恪守業界和政府法規。Secure Web Gateway Services 為對外 Web 存取的策略性控制點，因此，可適時扮演監控和回報 Web 使用量趨勢的角色。有些組織原則會記錄每個要求，有些則只會記錄觸發風險通知的要求。F5 解決方案可同時因應兩者，並提供常用報表 (例如，包含可識別耗用絕大多數網路頻寬之使用者的報表)。

了解外顯式和透明 Proxy

F5 Secure Web Gateway Services 可自動發揮透明的正向 Proxy 作用，讓所有使用者要求都能透過它傳遞至網際網路。透過這種方式使用解決方案時，系統管理員不用變更每個裝置的設定，或是為原則設定群組，就能攔截使用者工作階段。

Secure Web Gateway Services 也可以做為外顯式 Proxy。與透明 Proxy 模式不同的是，外顯式正向 Proxy 模式會要求系統管理員為網路中的每個目標裝置 (和使用者) 明確定義外送的正向 Proxy。雖然這個方式似乎會造成較大的系統管理員負擔，許多組織皆發現外顯式 Proxy 模式可帶來顯著、實質的安全性優勢。

Secure Web Gateway Services 會自動使用 WPAD 或 PAC 格式建立自動組態檔。不然，也可以透過群組原則或其他企業管理解決方案台推播外顯式 Proxy 的設定。

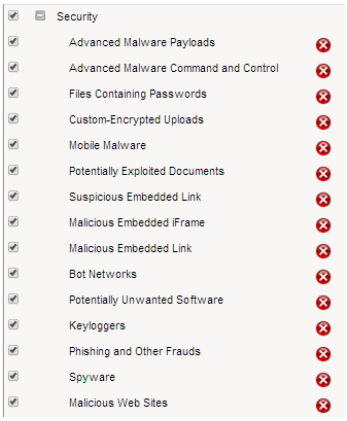

圖 1：網址資料庫的安全性分類

Websense 網址分類資料庫在 F5 Secure Web Gateway Services 中扮演著安全性引擎的角色。Websense 會每天監控數十億筆網址，以編譯這個即時威脅情報來源。

F5 客戶如何使用 Secure Web Gateway Services

Secure Web Gateway Services 參考架構預先規劃了四種常見客戶情境。這些情境並非彼此獨立，而且通常會有某些程度上的重疊。

- **內容感知的安全性：**Secure Web Gateway Services 會保護位於相似企業環境中的使用者。
- **頻寬控制：**F5 解決方案可限制媒體內容類型所耗用的頻寬，進而影響使用者行為。
- **可接受的使用原則呈現：**Secure Web Gateway Services 會要求接受可接受的使用原則，藉此協助組織提供訪客使用者專用的網路存取權，同時免除相關責任。
- **法規遵循：**與信用卡號安全性相關的支付卡產業 (PCI) 指導方針要求位於持卡人資料環境 (CDE) 中的伺服器使用正向 Proxy 來存取位於網際網路中的更新伺服器。

部署情境

為了實現客戶情境的目標，Secure Web Gateway Services 的實際部署經常可分成三個不同模式：企業、訪客存取，以及 PCI CDE DMZ。這些可支援多個客戶情境的部署情境會依照當中啟用的功能來加以區分。此外，無論為哪一個部署情境，解決方案都可提供：

- 網址分類和篩選。
- 惡意軟體掃描。
- 回報。

企業部署情境

Secure Web Gateway Services 解決方案的企業部署會包含適用於不同網路和安全性需求的多個組態設定檔。每個組織都有著獨一無二的需求，對多數組織而言，Secure Web Gateway Services 可透過分類和篩選網址、掃描內嵌惡意軟體，並選擇性遏止與生產力無關的 Web 行為，以保護組織員工產生的對外 Web 流量。

一般而言，典型的企業架構會包含 Secure Web Gateway Services 的網址篩選、惡意軟體掃描以及回報等基礎功能，再輔以一組常見的額外功能，包括：

- 與企業目錄整合以進行使用者身分識別
- SSL 攔截
- 同盟 SSO

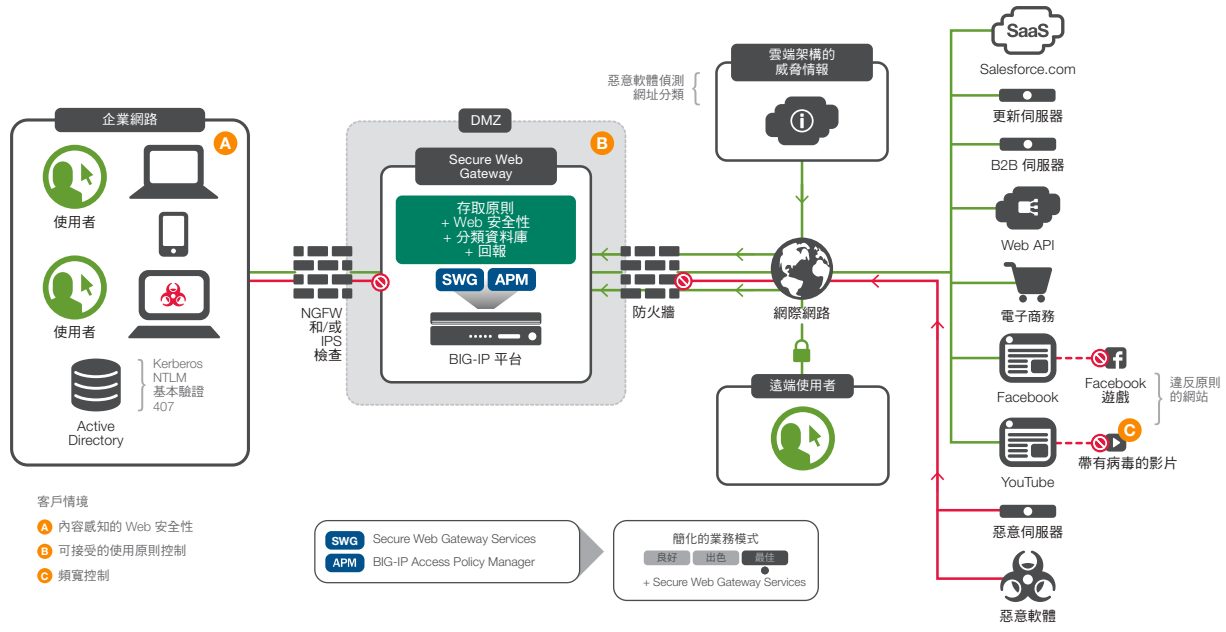

圖 2：企業部署情境，該情境可支援四個客戶情境。

使用企業目錄進行使用者身分識別

Secure Web Gateway Services 解決方案會運用其 ADC 平台固有的應用程式通訊協定理解來保護層級 7 的流量。然而，它會攔截層級 3 和 4、IP 以及 TCP 的流量。鑑於這些層級不會提供使用者對應，Secure Web Gateway Services 通訊協定可與 Microsoft Active Directory 服務協同合作，進而對應 IP 位址以及經驗證的使用者名稱。

系統管理員可以透過協調 Secure Web Gateway Services 以及 Active Directory 來查看誰於何時採取了什麼行動，以及哪一位使用者可能會感染惡意軟體。若啟用 Active Directory 通訊，要求的稽核記錄就會將與該要求相關的使用者名稱納入其中。

如果無法判斷對應 (可能是由網路中的某個惡意裝置所致)，Secure Web Gateway Services 就會針對未經驗證的連線提供三個可行方法：

1. 基於最佳安全性考量而拒絕連線。
2. 連線可與較受限制的安全性原則建立關聯。
3. 連線可導向網頁驗證入口，使用者需要於該處進行驗證 (如此一來，Secure Web Gateway Services 就能追蹤與該裝置相關的使用者)。

檢查加密流量

檢查加密的對外流量儼然已成為必要課題。隨著 HTTPS 逐漸成為預設傳輸通訊協定，系統管理員勢必要能破解這些連線，才能進行檢查。Secure Web Gateway Services 的 SSL 攔截功能會自動產生憑證，而且該憑證就如同目標網站向內部使用者所顯示的憑證一樣。而瀏覽器 (已設定為會信任解決方案的數位憑證) 則會認為自己正在與目標網站直接通訊。

雖然 SSL 是一項強大的功能，有時候，系統管理員可能無意攔截符合以下情況的連線：

- 提供網路銀行的網站 - 通常，系統管理員不會想要攔截金融機構方面的使用者資訊。
- 要求用戶端憑證驗證的網站 - 基於 SSL 通訊協定的組成方式，Secure Web Gateway Services 無法攔截需要用戶端憑證驗證的網站。
- 辨別伺服器憑證指紋的網站 - 自動化更新伺服器有時會將目標憑證內嵌於用戶端軟體中，如果使用 SSL 攔截，就會傳回錯誤。
- 高信任度 SaaS 網站 - 許多系統管理員會為常用的 SaaS 平台建立高信任度關係。而他們可以 (基於效能考量) 避免攔截和檢查連往這些服務的每一個使用者連線。

請注意，用戶端憑證驗證無法相容於透明 SSL Proxy。此外，舉凡與憑證相關的服務，或是驗證伺服器憑證指紋的任何服務 (例如 Microsoft Windows Update)，也無法相容於透明 SSL Proxy。如果網站會要求用戶端憑證驗證，或是其他無法相容於透明 SSL Proxy 的功能，系統管理員可以建立列出允許網站的自訂類別，指出可以略過哪些檢查。SSL 攔截所應略過的網站終究是有待系統管理員訂定和管理的原則決策。

適用於 Secure Web Gateway Services 的 F5® iApps® 範本可用來管理 SSL 攔截所應略過的網站類別。

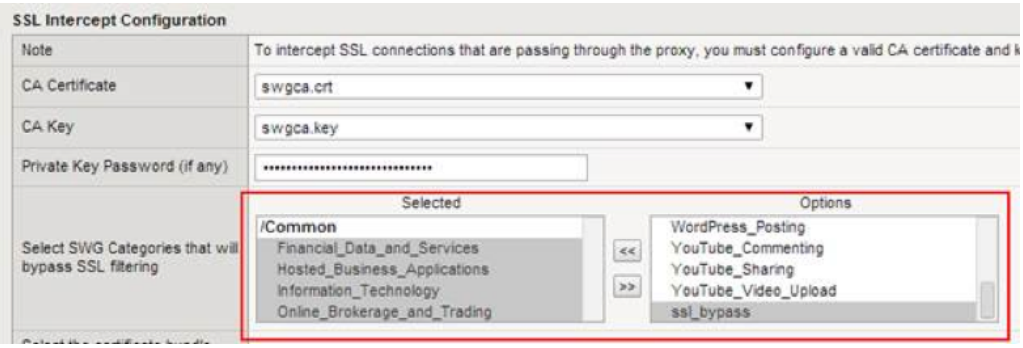

圖 3：以 iApps 範本管理 SSL 所應略過的類別

將安全性視為企業原則

現代化瀏覽器和搜尋引擎都有提供篩選模式，可預防搜尋結果顯示裝載已知惡意軟體的網站。Google 採用的技術名為 SafeSearch，而 Microsoft 採用的技術則為 SmartScreen 篩選工具。

如果使用者無法使用這些安全模式瀏覽器，惡意軟體和惡意網址就有可能藏身於未受篩選的搜尋結果中。此外，多數搜尋引擎都已採用「僅限 SSL」的模式，這也增加了透過 Web 安全性提供安全搜尋的難度。Secure Web Gateway Services 可偵測和封鎖內嵌於這些搜尋結果中的連結，有效落實適用於全公司的安全搜尋原則。

提供同盟 SSO

同盟 SSO 為 Secure Web Gateway Services 最強大的功能之一。只要加以設定，解決方案就能和企業 SSO 工具相互運作 (透過 SAML 和其他技術)，將網際網路存取登入轉換成企業入口網站和軟體即服務 (SaaS) 應用程式的已驗證存取。如此一來，即可提供原則架構的控制和監控，進而掌握哪些使用者可以在何時存取哪個網站，以及當中涉及哪些風險。

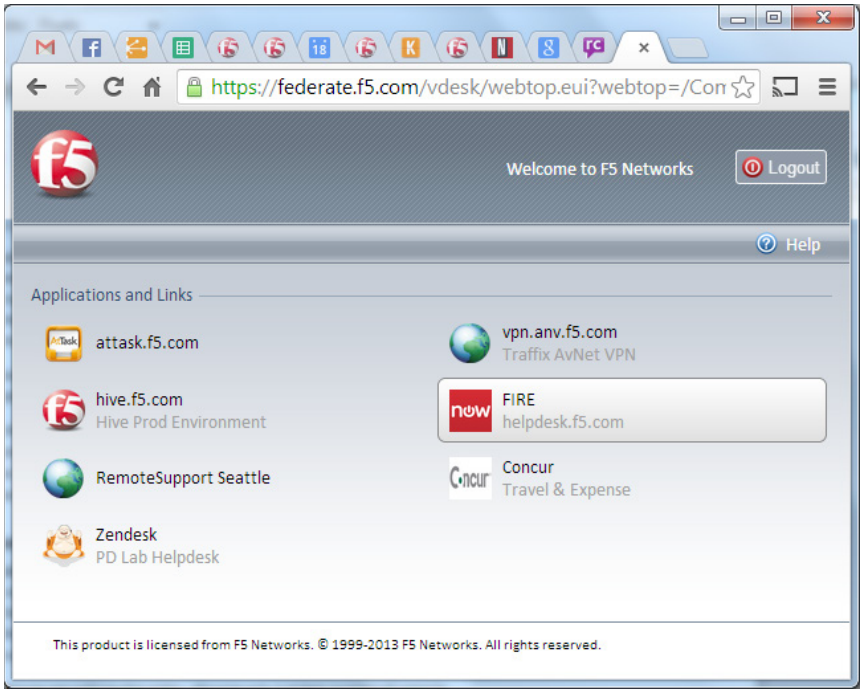

圖 4：提供同盟 SSO 的每日登入頁面範例

假設某個組織有 20 個位於雲端的整合式 SaaS 應用程式。Secure Web Gateway Services 的同盟 SSO 功能就能在不要求使用者重新輸入憑證的情況下，自動驗證 20 個服務的每一名使用者。這不僅可以節省時間，更重要的是，它可以將驗證整合成整合單一服務，盡可能省下密碼管理所耗費的心力。

有些 SAML 身分識別提供者 (IdP) 可以使用 NTLM 進行透明化登入，讓使用者再也不用輸入其使用者名稱和密碼。使用者只會在首次存取網頁驗證入口時看到快速的瀏覽器重新導向畫面，而且只要一登入桌面，就不用再輸入使用者名稱和密碼。

透過 SAML IdP 將網頁驗證入口轉換為日常同盟頁面。

端點檢查

Secure Web Gateway Services 的存取原則允許用戶端檢查收集和驗證使用者系統資訊。這些用戶端檢查是確保遠端工作者已在個人電腦和筆記型電腦中安裝防毒和反惡意軟體服務的一大關鍵。這項原則可以在授予網路資源存取權之前套用至特定安全性層級。

頻寬控制

Secure Web Gateway Services 可透過以內容類型 (例如串流媒體)、網址類別、應用程式或通訊協定 (例如 FTP) 為基準的頻寬控制來協助組織改變使用者行為。頻寬限制選項相當適合用在組織有意加以抑制，進而協助改變使用者行為的低容量連結以及特定內容類型 (佔用頻寬) 上。

雖然頻寬配額 (在指定時間內使用的頻寬總量) 所提供的控制較不即時，但也能達成相同的目的 (避免使用佔用頻寬的應用程式)。

- **限制有病毒的影片，但不會禁止所有娛樂：**Secure Web Gateway Services 可辨識和分類成千上萬的娛樂性質網站。系統管理員不僅能使用這個類別控制娛樂性質網站的存取，還能控管允許的存取次數。舉例來說，假設某位員工因工作所需而必須定期存取影片網站，但組織不想要讓員工觀看各種帶有病毒的影片 (進而導致該類型影片在辦公室中流竄)，即可派上用場。

  Secure Web Gateway Services 能使用 Websense 帶有病毒的影片網址類別來落實這項原則。這個經常更新的類別會列出目前的熱門影片，以供系統管理員輕鬆設定原則，進而達成每天只允許特定檢視次數的目的。有著此一問題的作業勢必會對 Secure Web Gateway Services 所提供的控制層級愛不釋手。

- **提供有關 Netflix 的控制：**Secure Web Gateway Services 可控制的另一個娛樂網站類型則是 Netflix 等媒體串流網站。有些組織想要無時不刻對所有使用者封鎖這類型的網站。有些組織則只想在下班之後的時間允許需要留守但不必處理事務的員工存取這些網站。因此，系統管理員可以根據群組來落實不同的原則。

訪客存取部署情境

提供訪客存取的功能是 Secure Web Gateway Services 部署情境較為與眾不同之處。若使用此一部署方式，F5 解決方案就會保護訪客專用的網際網路存取，而訪客則包括存取訪客無線網路的賓客，或是使用專屬承包商網路的獨立承包商。

儘管 Secure Web Gateway Services 可驗證訪客使用者，大多數的組織只會要求訪客使用者接受條款，然後仰賴 Secure Web Gateway Services 保護該名使用者免受惡意網站或內嵌惡意軟體所擾。

保護和回報訪客存取連線的機制大多與企業部署情境並無不同。不過，無線網路訪客的限制會較為寬鬆 (例如，不會套用生產力鎖定)，而承包商的限制可能會較為嚴謹。

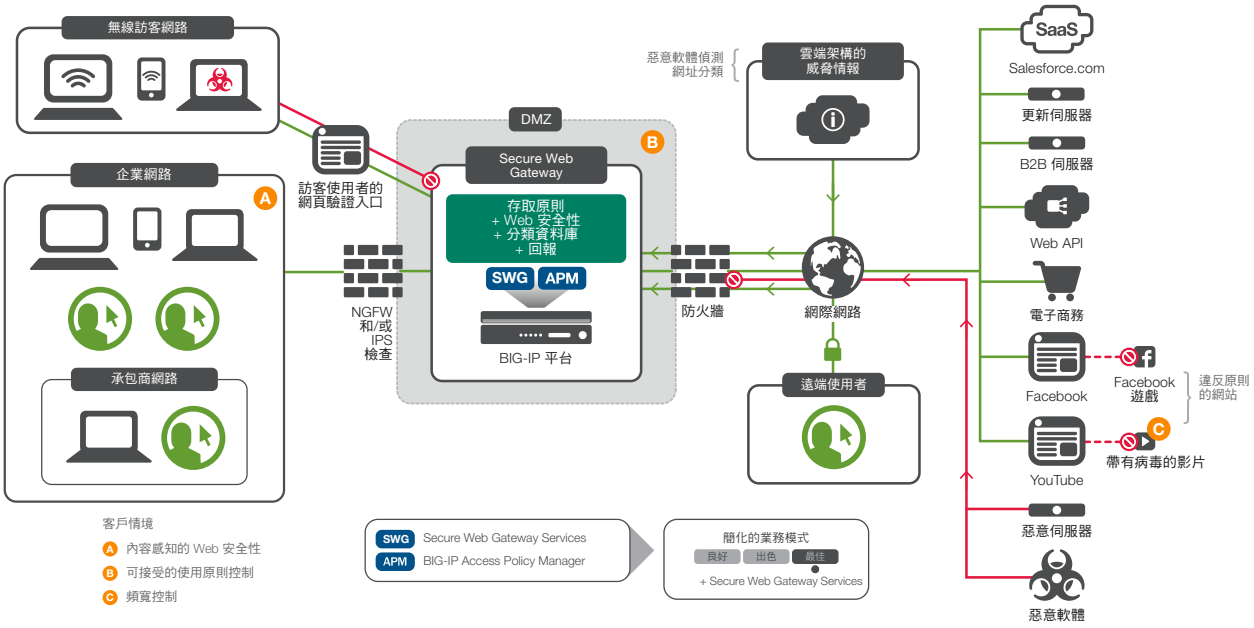

圖 5：使用網頁驗證入口的訪客存取部署

適用於訪客存取的一般 Secure Web Gateway Services 部署會涉及幾項常見功能的啟用，包括：

- 透明 Proxy 模式。
- 網頁驗證入口。
- 網址篩選。
- 惡意軟體掃描。
- 回報。

雖然上述功能皆相當重要，此一模式的最大不同之處則非網頁驗證入口莫屬。

網頁驗證入口

網頁驗證入口的概念就好比登入咖啡店或飯店的訪客無線網路存取點。使用者必須透過網頁驗證入口頁面登入網路。有時候，網頁驗證入口會要求提供憑證 (例如飯店房號) 以收取費用。在多數情況下，網頁驗證入口 (至少) 會要求使用者接受服務條款。

只要要求使用者同意可接受的使用原則，組織就能將某些責任轉移至該使用者身上。通常，使用原則會告知使用者不得欺騙封包、攻擊其他電腦或網路，或是監控其他使用者流量。如果使用者違反規定並因而產生訴訟，組織就能聲明一切肇因於該使用者並未遵守使用原則。

PCI CDE DMZ 部署情境

這個情境的目的在於透過部署 Secure Web Gateway Services 來滿足 PCI 安全性指導方針之規定。舉例來說，Secure Web Gateway Services 經常會用來建立符合 PCI DSS 規範的持卡人資料環境 (CDE)。PCI DSS 標準的 1.3.7 章節表示：如果 CDE 當中的任何伺服器會連線至網際網路，就必須使用正向 Proxy 控制來保護這些伺服器。在 CDE 中部署 Secure Web Gateway Services 不僅可滿足此項規定，還能保護對外的連線和通訊。

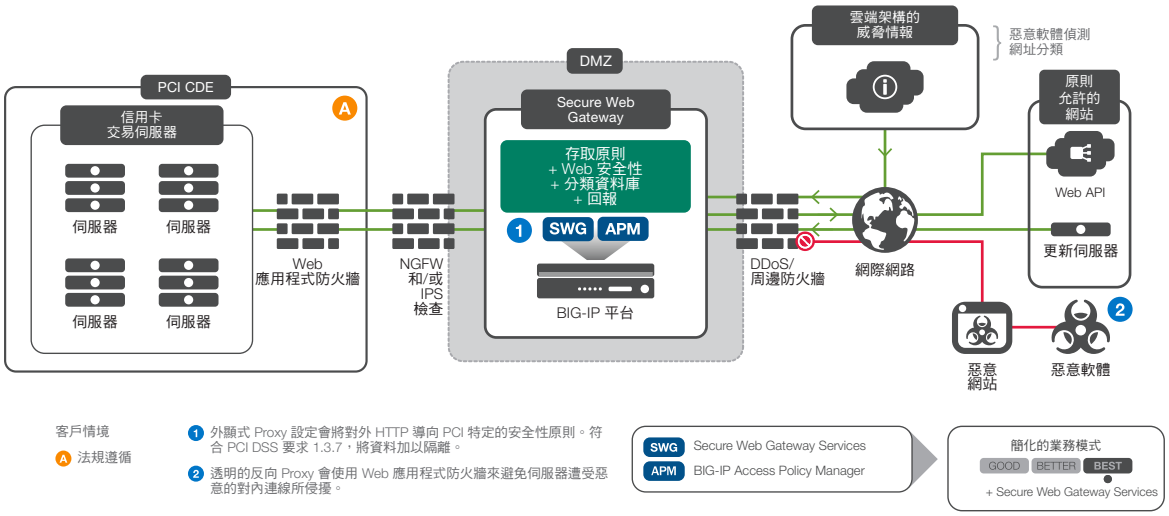

圖 6：F5 解決方案的 PCI CDE 部署

在這些案例中，安全性系統管理員的目標就應該放在盡可能進行 Proxy，以縮小威脅範圍。如果環境中的伺服器終究還是遭受危害，惡意軟體感知 Proxy 就能讓攻擊者難以將攻擊工具載入至該伺服器中。

若要充分發揮 PCI CDE DMZ 的安全性，系統管理員可以設定自訂類別，以建立列出允許網站的清單。

在 Secure Web Gateway Services 中，受保護的一般 DMZ 部署會涉及啟用基本功能，以及添加外顯式或透明 Proxy 模式功能。

使用外顯式 Proxy 保護 DNS 服務

外顯式 Proxy 的其中一個安全性優勢，在於 Proxy 會成為所有外部要求的預設名稱伺服器。這樣一來，系統管理員就可以卸除由內部 DNS 伺服器為外部位址提供服務的功能，進而縮小名稱服務的威脅範圍。舉例來說，假設攻擊者已從外部對應網路，並發現內部 DNS 名稱伺服器 intra.example.com。只要已卸除由內部伺服器為外部位址提供服務的功能，攻擊者就無法對它的快取下毒手。

將 Secure Web Gateway Services 使用在外顯式模式時，可將其附加至外部 DNS 伺服器。如此一來，就不用以企業的內部 DNS 伺服器做為外部解析來源。在這個情況下，只要加以設定，即可讓內部 DNS 不再轉發外部資源的要求 (因為它們將交由 Secure Web Gateway Services 處理)。這可望縮小威脅範圍，並保護內部 DNS 不會遭受快取感染。

查詢大小寫隨機處理

查詢大小寫隨機處理會透過隨機變更名稱大小寫，然後確保回應的大小寫會與修改後的要求完全相同，進而為名稱查詢添加另一層的安全性。舉例來說，如果使用者要求 www.example.com 的位址，執行查詢大小寫隨機化的服務 (例如 Secure Web Gateway Services) 就會將查詢變更為 wWw.EXamPle.com。處理回應期間會進行檢查，以確保回應中的大小寫也與其相符。這有助於避免攻擊者透過提供假的熱門網站 (例如 Google Mail 或金融機構) 要求回應來偷渡位址。

依據部署情境劃分的客戶情境

這三個基本部署情境皆可支援四個常見客戶情境，為組織提供最切合其目標的組態選項。

部署情境	內容感知的安全性	頻寬控制	可接受的使用原則呈現	法規遵循
企業	●	●	●	—
訪客存取	●	●	●	—
PCI CDE DMZ	—	—	—	●

圖 7：部署情境如何支援各種客戶情境

從 Microsoft Forefront TMG 移轉

對許多組織而言，Microsoft Forefront Threat Management Gateway (TMG) 的終止不啻為轉換至 F5 Secure Web Gateway Services 的契機。

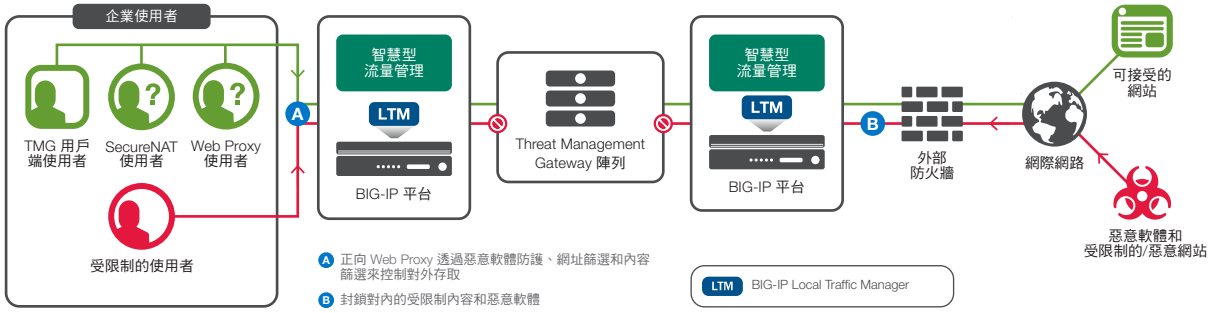

圖 8：Microsoft TMG 陣列在一般企業網路中的定位

由於緊鄰 TMG 的 F5 BIG-IP® Local Traffic Manager™ (LTM) 裝置可以啟用正向 Proxy 功能，因此 F5 解決方案的表現遠比單純替換 TMG 來得出色。正向 Proxy 已整合至 BIG-IP 中，不僅能降低企業的資本支出 (CapEx) 和營運支出 (OpEx)，還可望提升效能。

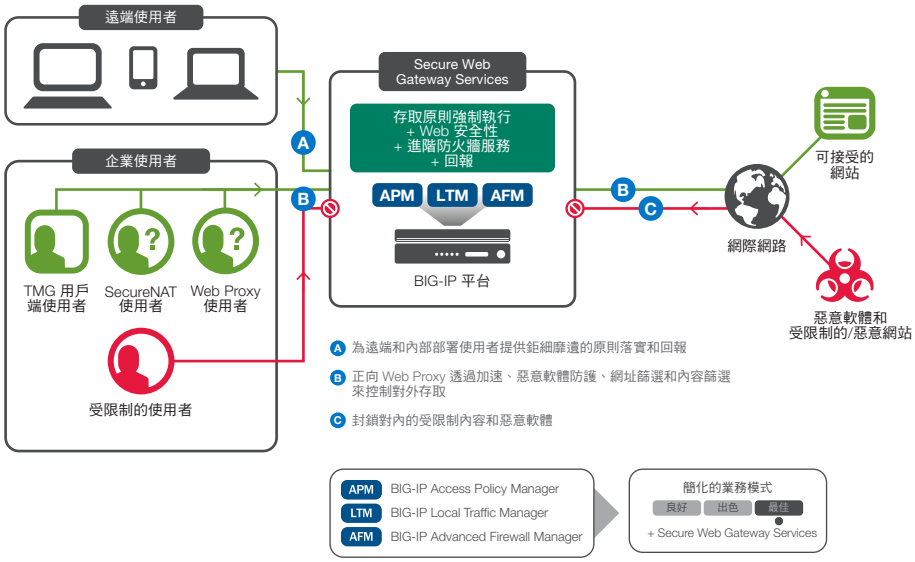

圖 9：從 TMG 移轉至 Secure Web Gateway Services 後的網路

調整解決方案平台的大小

如同所有 F5 解決方案一樣，Secure Web Gateway Services 可部署至 F5 產品組合的任何平台中。我們的服務工程師可協助 F5 客戶判斷現有平台是否足以運行 Secure Web Gateway Services。

方法	BIG-IP 2200	BIG-IP 5200	BIG-IP 10200
外顯式篩選、掃描 (每秒交易數)	1,800	5,700	8,300
僅外顯式篩選 (每秒交易數)	9,800	37,000	45,000
透明篩選、掃描 (每秒交易數)	1,700	5,600	8,300
僅透明篩選 (每秒交易數)	11,200	40,000	41,000

圖 10：F5 平台規模

授權和同時上線使用者

每個 F5 平台都會指派同時上線的工作階段限制，以確保最佳的使用者體驗。不同大小的網頁也會對 Secure Web Gateway Services 的效能帶來不同影響。熱門 F5 平台的最佳同時上線授權使用者數量會介於 100 到 30,000 人之間。

F5 平台	Secure Web Gateway 同時上線連線
VIPRION 2400	30,000
10000 系列	20,000
7000 系列	15,000
5000 系列	10,000
4000 系列	5,000
2200	1,000
VE	100

圖 11：熱門 F5 平台的同時上線使用者授權 (以 16 KB 的平均頁面大小為基礎)

結論

這份參考架構說明了 F5 Secure Web Gateway Services 如何為任職於大型企業、中小企業，以及付款處理資料中心的 IT 系統管理員提供協助。

- 許多組織正在使用 F5 解決方案來保護內部使用者的 Web 安全。該解決方案的網址分類和篩選可避免使用者淪為惡意軟體網站的犧牲者，並遏止與生產力無關的網際網路使用。鉅細靡遺的安全性原則部署則能為內部承包商提供更嚴謹的安全性防護。
- 不少小型企業正在運用 Secure Web Gateway Services，在不必承擔額外責任的情況下，為來訪賓客提供網際網路存取。
- 眾多付款處理資料中心則會使用 Secure Web Gateway Services 建立 PCI CDE DMZ，並藉此保護付款伺服器。

F5 Secure Web Gateway Services 解決方案可將眾多服務整合至組織部署至網路以做為策略性控制點的單一平台中。

在今日的嚴峻環境中，儘管魚叉式攻擊、網頁掛馬 (Drive-by Download)、水坑式攻擊 (Watering-hole Attack) 和持續性滲透攻擊 (APT) 層出不窮，價值絕非唯一考量。唯有採取更健全的安全性手段 解決方案才能發揮作用。SSL 攔截和惡意軟體掃描可有效補全安全性藍圖、縮小威脅範圍，並簡化 IT 系統管理員的工作。

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
企業總部
info@f5.com

F5 Networks
亞太地區
apacinfo@f5.com

F5 Networks Ltd.
歐洲 / 中東 / 非洲
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

Solutions for an application world.