



VPN 功能及獨特的驗證網域技術介紹

BiGuard SSL VPN 安全性設備

白皮書

目錄

一、前言	3
二、虛擬私有網路 (VPN) 簡介	4
IPSec VPN	4
SSL VPN	4
三、產品三合一的設計	5
四、驗證網域技術	6
五、與現有的驗證網域相容	6
六、將完整的路由技術整合於 SSL VPN 產品	9
七、總結	9

BiGuard SSL VPN 安全性設備

VPN 功能及獨特的驗證網域技術介紹

一、前言

保障企業的機密資料，一直是資訊安全議題上很重要的一環。隨著全球行動工作者比例逐漸增加，除了確保在外員工與合作夥伴遠端存取的穩定與便捷之外，遠端連線期間的資料與各種應用傳輸的安全性，涉及企業機密資料外洩的可能，嚴重者甚至可能危及企業經營。因此，如何為企業資安建立最後一道防線，圍堵網路威脅入侵可能帶來的災害，勢必成為 MIS 人員最大的挑戰。

近來，虛擬私有網路（Virtual Private Network, VPN）已成為遠端存取中最為普遍的方法。VPN 讓移動辦公的員工和遠端使用者不論在任何時間，任何地點都能使用基本的電子郵件收發、資料存取、ERP 系統或其他的應用軟體。另外，企業透過 VPN，除了可以與公司組織內的員工保持聯繫外，還能與企業合作夥伴及供應商間達到更有效的運作。

本文說明了 BiGuard SSL VPN 產品特別將 IPSec VPN 與 SSL VPN 整合在一起，因此 BiGuard SSL VPN 產品係專為安全遠端存取市場所量身訂做的安全性設備。同時也解釋 Active Directory（AD）與 Lightweight Directory Access Protocol（LDAP）這兩種認證網域技術的特點，並且介紹新增使用者如何透過 AD 或 LDAP 成功認證後，從遠端藉由 BiGuard SSL VPN 產品，來存取企業內部資源。最後，本文強調 BiGuard SSL VPN 產品，結合了 IPSec VPN 的優勢以及 SSL VPN 的能力，能達到漸進式存取控管（granular access control）和強化遠端存取安全性，而將 SSL VPN、防火牆及網路存取整合於一體的設計，使得 BiGuard SSL VPN 產品可以滿足 SOHO/SMB/SME 在安全遠端存取方面的需求。

二、虛擬私有網路（Virtual Private Network，VPN）

對於必須提供工作者從遠端存取公司資源的企業而言，提供安全性的遠端存取是關鍵的需求。不論工作者在遠端辦公室、網咖或飯店內工作，如要確保持續的生產力，就必須具備一套簡便而安全的遠端存取解決方案。VPN 技術是藉由公眾網路的運用，使遠端使用者能和企業總部、分公司之間建立加密通道，且由於 VPN 技術比傳統固接專線（leased line）或私有網路（例如 ATM、MPLS 或 Frame Relay）具有更高的安全性及成本效益，因而受到企業的歡迎與認同。其中，IPSec 及 SSL VPN 是兩種最受企業歡迎的解決方案。

IPSec VPN

透過網際網路安全性協定（IPSec）技術，可在兩個不同的地點之間建立起虛擬私有通道，以確保資料保密性、一致性及驗證使用者的存取權限。由於IPSec VPN可提供安全且具成本效益的方法，有利於各企業在不同地點之間進行連線，以滿足企業各種需求。IPSec是一項適用於在兩個可信賴網路間進行端對端（site-to-site）或點對端（client-to-site）VPN連線的理想解決方案，但仍有以下缺點：

1. 遠端使用者必須在使用電腦上安裝IPSec VPN客戶端軟體，並執行VPN組態設定。所需的安裝、維護及故障排除將對企業產生其他管理難題及成本。
2. IPSec VPN連線，可能會遇到NAT透通（NAT traversal）問題，造成遠端客戶端IPSec軟體、NAT路由器及IPSec閘道有相容性問題產生。

SSL VPN

SSL（Secure Sockets Layer）是由Netscape發明的協定，主要應用於電子商務網路交易的安全傳輸。SSL使用金鑰（例如RSA）對資料進行加解密以及驗證使用者的存取權限。它可用於防止惡意入侵、資料竊取、竊聽及網路詐騙。SSL目前已獲得一般網頁瀏覽器（諸如 IE、Netscape等）採用。使用者可於任何網路存取點使用網頁瀏覽器建立SSL VPN通道，以便存取企業內部應用程式、檔案分享及網路資料庫。對於SOHO、中小企業（SMB）以及必須隨時隨地取得資訊的使用者而言，極為便利且容易使用。SSL是一項適用於在兩個可信賴網路間，進行點對端（client-to-site）VPN連線的理想解決方案，有以下優點：

1. SSL協定內建於一般網路瀏覽器中，使用者不需安裝客戶端軟體及進行組態設定，降低了管理上的難題及支援需求。
2. SSL VPN能搭配網路應用層的協定，允許系統管理員針對各應用程式，可針對使用者制定漸進式存取控管（granular access control）政策，確保遠端使用者更高的安全性。
3. SSL VPN協定透過連線的網路應用層傳送，可減低存在於IPSec VPN的NAT相容性問題。

三、產品三合一的設計

BiGuard SSL VPN產品整合路由器、防火牆和SSL VPN成爲單一安全性產品，具備企業級解決方案的特色與強大功能，沒有複雜的設定及管理需求，亦不必額外添購路由器、硬體或個別的防火牆裝置，即可充分體驗所有遠端存取安全通訊的優勢。圖1爲BiGuard SSL VPN安全性設備擺置於企業網際網路的進入閘道點。

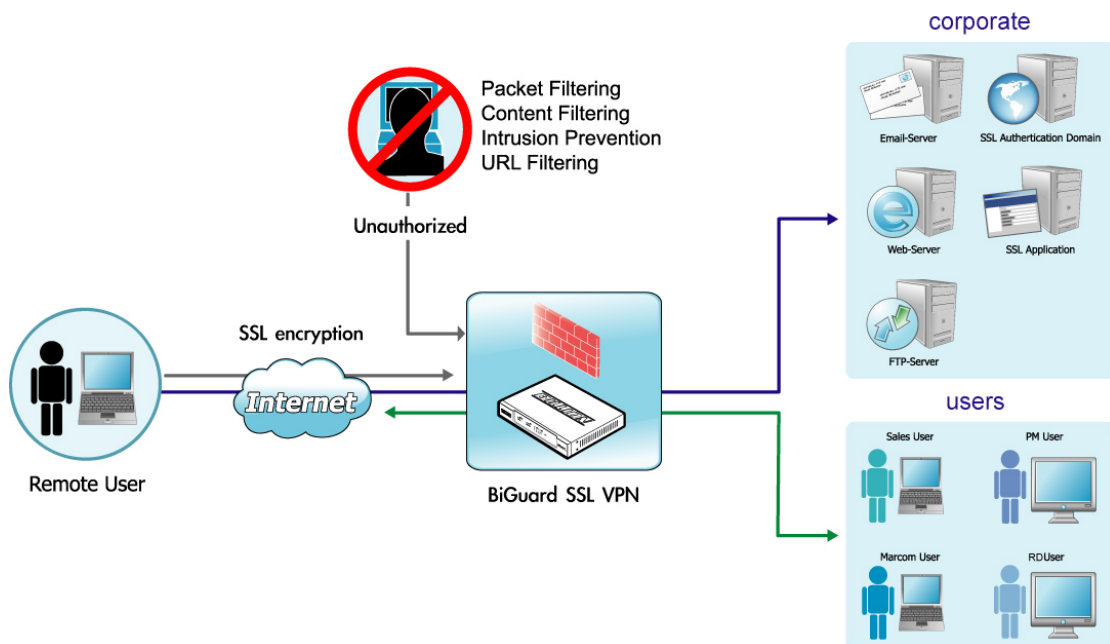


圖1 BiGuard SSL VPN安全性設備擺置點示意圖

四、驗證網域技術

企業可使用Active Directory (AD) 或Lightweight Directory Access Protocol (LDAP) 認證網域技術來提供一個在分散式網路環境裡，使用者的分層瀏覽、延展性、伸縮性和分散式安全性服務需求。AD或LDAP技術允許管理員、開發者和使用者對包含在Internet和企業內部Intranet環境中的目錄服務進行存取。AD技術也是使用LDAP作為它的核心協定，但會以網域 (Domain Name ; DN) 全名表示AD網域，如AD的一個網域 (Domain Name) 全名為 “cnc.billion-nt.hq”。而LDAP技術使用了下列不同的命名規則來定義驗證網域 (Domain Name)：由共同名稱 (Common Name; CN) 和部門名稱 (Domain Country ; DC) 等相關辨別名稱來共同組成。如 LDAP的一個BaseDN例子為 “cn=users, dc=test , dc=bgs10, dc=com, dc=tw”。BiGuard SSL VPN產品可針對這些AD DNS全名或LDAP驗證網域名稱來新增一個群組 (Group)，來控管使用者的遠端存取權限。

五、與現有的驗證網域相容

BiGuard SSL VPN產品具有彈性認證機制，對於未部署驗證網域機制的企業，可使用本地資料庫 (Local Database) 來驗證遠端使用者存取權限，如圖2。至於已部署驗證網域機制的企業，BiGuard SSL VPN產品能支援 Active Directory、LDAP、NT Domain 及RADIUS 驗證方法來驗證遠端使用者存取權限，如圖3。

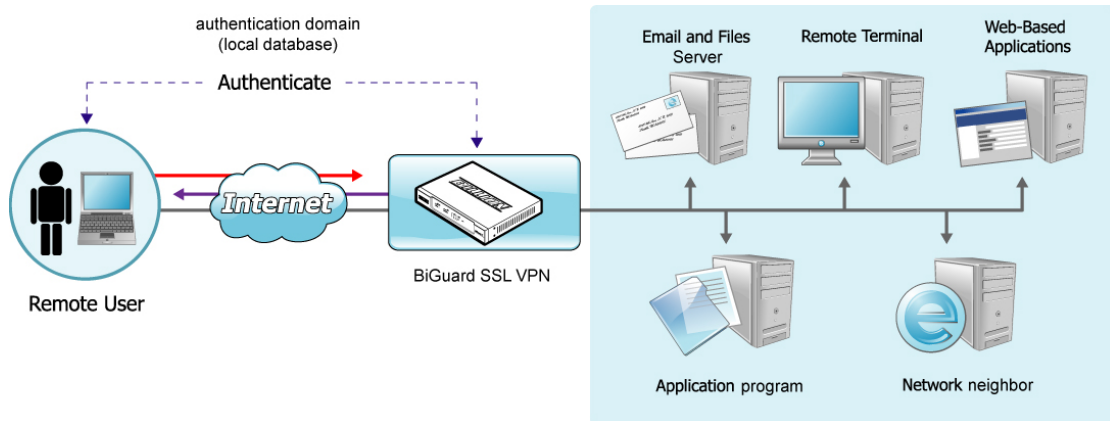


圖 2 BiGuard SSL VPN 使用本地資料庫 (Local Database) 驗證遠端使用者

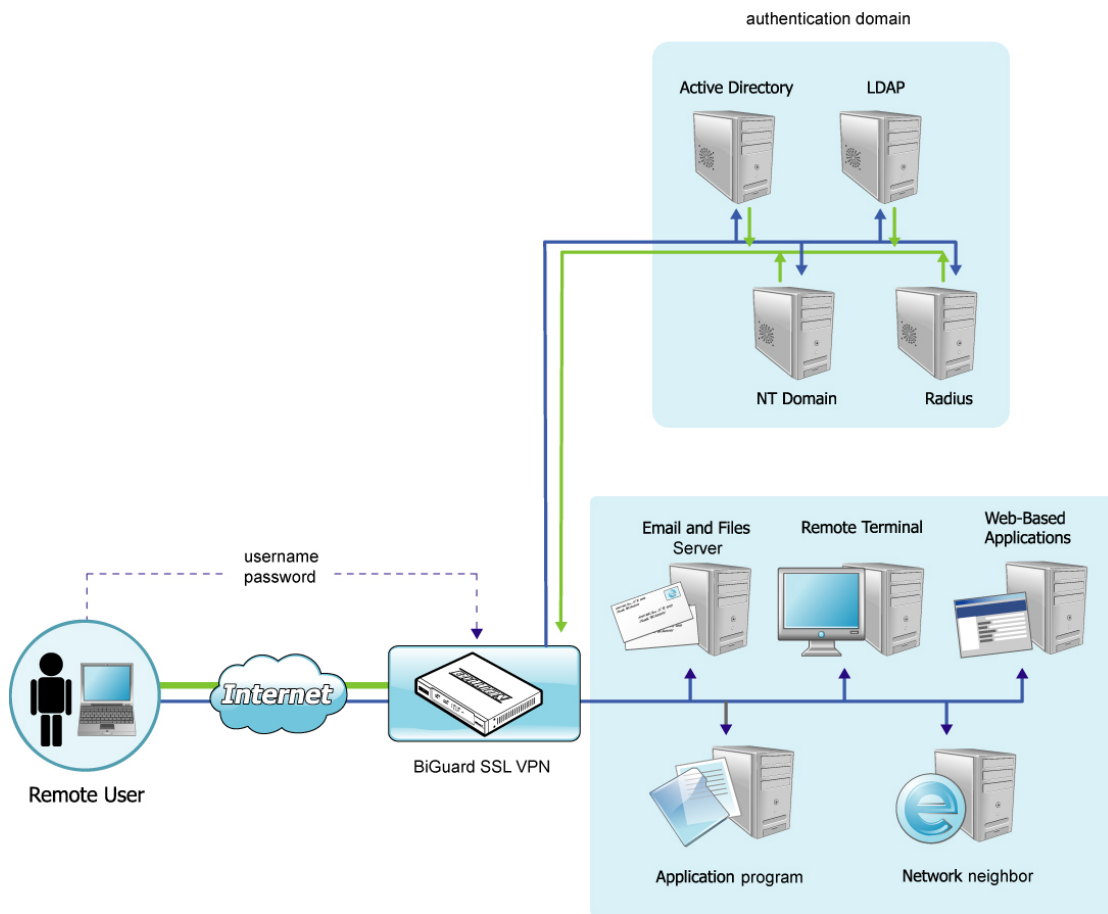


圖 3 BiGuard SSL VPN 使用驗證網域機制來驗證遠端使用者

BiGuard SSL VPN 產品的管理者能從企業內部已經設定好的 AD 或 LDAP 認證網域伺服器中撈出可遠端存取企業內部資訊之使用者資料，並且以勾選的方式快速批次新增使用者至選定的 Group 中。圖 4 為 BiGuard SSL VPN 產品欲新增使用者時，去 AD 或 LDAP 認證網域伺服器查詢目前使用者結果例子。管理者可透過查詢後網頁勾選要匯入的使用者名稱到 BiGuard SSL VPN 產品的指定 Group，亦可選擇“Select All”來匯入 AD 或 LDAP 認證網域伺服器內所有使用者名稱到 Router 內。圖 5 為按下“Apply”按鈕確認新增使用者至 Router 時，網頁執行畫面例子。往後這些新增使用者便能從遠端透過 BiGuard SSL VPN 產品，經過 AD 或 LDAP 認證網域伺服器成功認證後，來存取企業內部資源。

Select Account(s) to add <<First <Prev Page 6 / 8 Next> Last>>

Select all <input type="checkbox"/>		Change group			
#	Selected	User Name	Add to group	Status	
51	<input type="checkbox"/>	otis	Test		
52	<input type="checkbox"/>	otischang	Test		
53	<input type="checkbox"/>	pattywu	Test		
54	<input type="checkbox"/>	petershih	Taipei_2K	Existed	
55	<input type="checkbox"/>	porcupinechen	Taipei_2K	Existed	
56	<input type="checkbox"/>	pqanj	Taipei_2K	Existed	
57	<input type="checkbox"/>	pqatest	Taipei_2K	Existed	
58	<input type="checkbox"/>	raymondwu	Test		
59	<input type="checkbox"/>	riachang	Taipei_2K	Existed	
60	<input type="checkbox"/>	robert	Test		

Apply Cancel

圖 4 新增使用者時，認證網域伺服器查詢目前使用者的範例

Select Account(s) to add <<First <Prev Page 1 / 8 Next> Last>>

Select all <input type="checkbox"/>		Change group			
#	Selected	User Name	Add to group	Status	
1	<input checked="" type="checkbox"/>	otis	Test	Succeed!	
2	<input checked="" type="checkbox"/>	otischang	Test	Succeed!	
3	<input checked="" type="checkbox"/>	pattywu	Test	Succeed!	
4	<input checked="" type="checkbox"/>	raymondwu	Test	Succeed!	
5	<input checked="" type="checkbox"/>	robert	Test	Succeed!	
6	<input type="checkbox"/>	Administrator	Test		
7	<input type="checkbox"/>	Guest	Test		
8	<input type="checkbox"/>	IUSR_2K-SERVER	Test		
9	<input type="checkbox"/>	IUSR_2K-SERVER2	Test		
10	<input type="checkbox"/>	WAM_2K-SERVER	Test		

Apply Clear

Microsoft Internet Explorer

Account(s) added successfully!

確定

圖 5 確認新增使用者至 Router 時，網頁執行畫面範例

六、將完整的路由技術整合於SSL VPN產品

BiGuard SSL VPN產品已整合完整的路由技術，包括靜態路由、動態路由、RIP1/RIP2、靜態WAN連線、DHCP客戶端WAN連線以及PPPoE WAN連線。此外，該產品也支援大部分的頻寬管理控制系統、Dynamic Domain Name System、Virtual伺服器、DHCP伺服器、硬體DMZ、多重NAT以及SNTP，同時還支援完整的登入及監測，包括系統記錄、電子郵件警示通知及攻擊記錄，以及系統狀態監測。BiGuard SSL VPN產品支援最先進的防火牆功能，包括靜態封包檢測Stateful Packet Inspection (SPI)、Denial of Service (DoS) 防範、封包過濾 (Packet Filter)、攻擊偵測 (Intrusion Detection)、URL filters 以及Java Applet/ActiveX/Cookie阻斷。該安全性設備也支援使用連接ISP最廣泛的WAN存取協定。

七、總結

SSL VPN 技術能支援免客戶端軟體之遠端存取、不需繁瑣的系統管理，而且可以讓行動工作者經由瀏覽器介面從任何地方存取應用程式。SSL VPN 支援與 IPsec VPN 相同的安全層級，而此協定的性質讓它成為安全遠端存取的解決方案。BiGuard SSL VPN 安全性設備以尖端的 SSL 技術為基礎，結合了所有 IPsec VPN 在安全性及連接性方面的優勢以及 SSL VPN 能力，能達到漸進式存取控管 (granular access control) 和強化遠端存取安全性，而且沒有 NAT 相容性的問題。除此之外，此一全方位設計將 SSL VPN、防火牆及網路存取整合於一體，讓 BiGuard SSL VPN 安全性設備成為 SOHO/SMB/SME 使用者具成本效益及彈性的投資的方案，以滿足其安全遠端存取的需求。

BiGuard SSL VPN安全性設備白皮書

Copyright © Billion Electric Co., Ltd. 版權所有

BiGuard 產品註冊網站：www.biguard.com

技術支援：support@billion.com

www.billion.com