



- 高安全性/高效能
- 具備IPv6金牌標章
- 健全的VPN(IPSec/SSL/L2TP)
 - EASY VPN
 - 零負擔的遠端存取方式
 - 支援智慧型手機
 - L2TP VPN(iOS/Android)
- 經ICSA認證的防火牆與IPSec VPN
- 內容過濾有效阻擋惡意程式與網頁威脅
- 強化電子郵件安全性
- 具備多個WAN以及3G網卡線路備援

Security on a New Level

-The Future Is Ahead. Stay Ahead with ZyXEL USGs.

商業網路環境內所必須面臨的安全威脅，已迅速從一般寬頻網路的攻擊發展成為癱瘓整個網路及竊取機敏資料。在如此環境中，小型企業該如何滿足此挑戰以保護他們的網路環境。

合勤ZyWALL USG100-PLUS系列，是被設計專為小型企業提供即時的檢測與多層式的網路防護，防止遭受各種網路上的威脅與攻擊。USG系列具備了SPI特徵防護防火牆、防毒軟體、入侵偵測與防禦、內容過濾、垃圾郵件防堵與VPN(支援IPSec/SSL/L2TP)等多種特色於單一設備內，除此之外，USG系列不只提供了完善的授權方式可供選擇更具備了持續性的韌體升級服務，可有效節省企業的硬體投資成本。

USG系列產品將其安全的特色融入所有連接在上面的設備，防止關鍵的資料遭受到內部或外部的威脅與攻擊，有效保護組織內的客戶與公司紀錄、智慧財產權等。

優勢

高效能與豐富的安全性

USG100-PLUS具備了高效能防火牆架構，在提供即時偵測與防止網路遭受威脅的同時還不至於犧牲效能。企業網路不僅受到完美的防護，除此之外檔案傳輸、電子郵件與資料搜索等應用都能被高速處理，在生產力與效率上也因此而獲得顯著的提升。



全面性的IPv6特色，順暢接軌未來網路環境

合勤USG防火牆系列產品具備了IPv6 金牌標章，可確保企業在未來IPv4轉IPv6的過程
中轉移順暢不間斷。USG支援dual-stack 與 IPv4 tunneling模式(6rd & 6to4傳輸通道)，
可將v6位址派發給用戶端並將v6的流量透過v4的環境傳遞，提供了各種IPv6應用程式
的網路存取方式



簡易VPN連線，降低操作成本與時間

透過架設VPN通道是一個安全連接遠端辦公室、分公司與夥伴之間的絕佳方式，但對於一般非技術人員要使用如此連線方式還必須依些繁複的設定，對他們來說是非常困難的。合勤USG系列產品提供了"EASY VPN"的解決方案，可自動將相關設定佈建至客戶端的裝置，可一舉消除在建立VPN時所帶來設定上的負擔。除此之外，USG支援iPhone/Android 以及其他智慧型手機的L2TP VPN技術，可讓員工透過行動裝置在遠端即能免費且輕鬆存取總公司的資料。

內容過濾保障網頁瀏覽安全

WWW本身即是一個非常有效率的惡意程式交換機制，因此也逐漸成為網路攻擊的主要目標。然而威脅大部分都隱藏在諸如：cookies、附掛插件與工具程式等，這使得威脅更難以被偵測到。合勤USG系列防火牆具備了領先業界的Blue Coat 與 CommTouch所提供的內容過濾解決方案，結合了全面性及數以百萬計的網址/IP位址/網域等數據資料庫，可有效降低成本並延伸防護範圍。透過此解決方案，USG設備不僅提供了即時防護阻止新興的網路威脅(惡意程式/網頁釣魚)，同時能阻擋或監控指定網址以提升員工工作效率。

強大的電子郵件防護

合勤USG 提供領先業界的Commtouch 電子郵件防護機制，可防止垃圾郵件、釣魚郵件以及病毒郵件等。透過Commtouch效能極高的經常性檢測模式(RPD)，每天都能即時分析數以百萬計的各種病毒形式以阻擋各種郵件威脅。此外，USG可根據寄件人IP位址移除超過80%非必要的郵件，並提供zero-hour的病毒防護特色，可在企業防毒軟體尚未更新至最新病毒特徵碼前做為最佳防護的選擇。

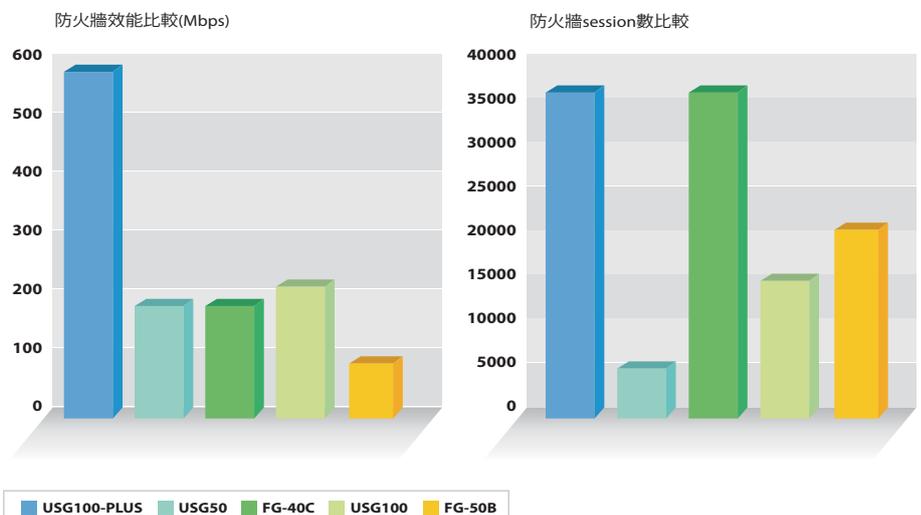
支援多款3G網卡

ZyWALL USG不僅支援多個WAN埠，也透過USB支援3G上網。透過3G連線USG設備可啟用負載平衡與線路故障備援，以提供更具高可靠度的網路連結；另外提供了更多3G網卡型號可供選擇，同時也提供了更豐富的驅動程式以滿足各種需求並節省額外支出成本。

主要應用

高效能

合勤USG系列是使用強大的整合式高效能安全(Integrated High Performance Security)架構來建立的，這是一個經證明適合高速光纖的高效能架構。這項產品提供即時的偵測功能，能夠防止網路遭受威脅，而不犧牲效能。此外，檔案下載、電子郵件往來及資訊搜尋等應用能夠以更快的速度處理，讓公司網路不僅受到安全無虞的保障，而且可大幅提升績效，改善營運生產力及效率。



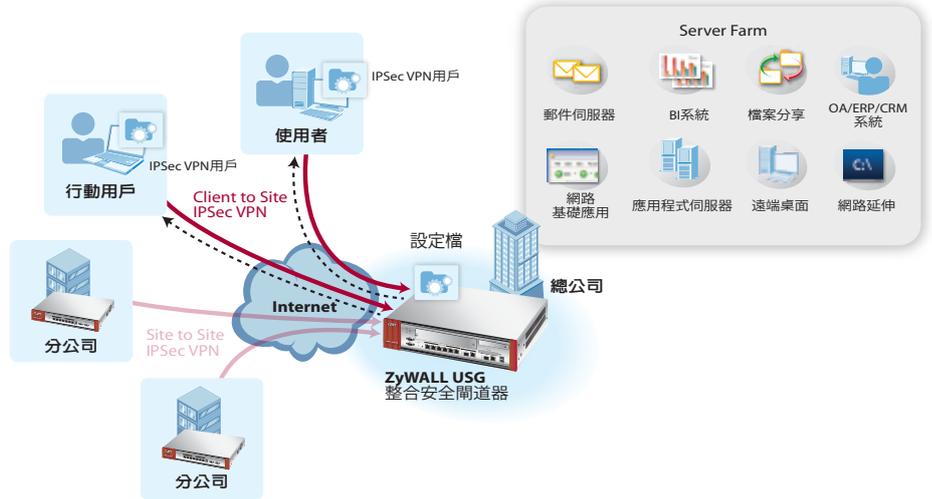
* 資料來源：來自ZyXEL、SonicWALL、Fortinet網站的效能數字

EASY VPN

零設定的遠端存取

對非技術人員來說要建立一個VPN連線可以是相當困難的，因為必須經過一些複雜的設定程序。合勤USG系列具備了"EASY VPN"的解決方案可將設定檔主動套用於客戶端的設備，屏除了繁複的設定程序並同時建立好VPN連線

簡易部署ZyWall IPSec VPN用戶端
USG自動提供相關設定檔至用戶端



內容過濾——

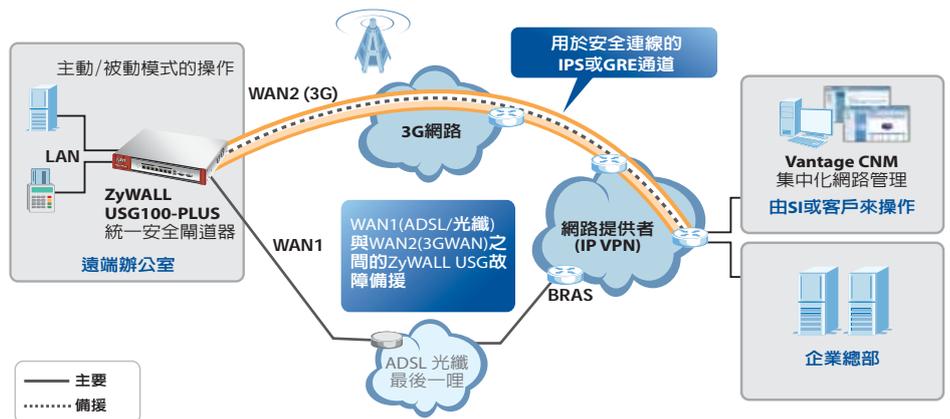
防止惡意程式與網頁潛在威脅

合勤USG提供內容過濾功能，可保護企業其用戶與網路免於遭受惡意程式威脅，諸如：間諜程式/網路釣魚的攻擊，以及P2P/IM等程式的濫用，可使企業中的電腦遠離惡意程式並保護企業網路的安全。



多個WAN埠及3G備援的不中斷網路存取

ZyWALL USG不僅支援多個WAN埠，也透過USB支援3G。這項功能促成了「主動-主動」負載分擔或「主動-被動」故障備援配置，以實現高度可靠的網路連線。



規格

型號	USG100-PLUS
產品圖片	
硬體規格	
10/100/1000 介面(銅)	4 x LAN/DMZ, 2 x WAN
USB 埠	2
卡槽	-
系統效能	
SPI 防火牆效能(Mbps) ^{*1}	600
VPN 效能(AES)(Mbps) ^{*2}	150
UTM 效能(AV+IDP)(Mbps) ^{*3}	30
無上限使用者授權	Yes
最大 Sessions ^{*4}	40,000
新 session 速率	1,000
IPSec VPN 通道同時連線數(最大)	50
SSL VPN 使用者同時連線數(最大)	25
內建 SSL VPN 用戶數	2
可客製化區	Yes
支援 IPv6	Yes
電源需求	
輸入電壓	100 - 240 V AC, 50/60 Hz, 1.2 A
電源消耗	17 W Max
外觀規格	
產品尺寸(寬X深X高)(公厘)	242 x 167 x 35.5
產品重量(公斤)	1.2
包裝尺寸(寬X深X高)(公厘)	375 x 238 x 108
包裝重量(公斤)	2.4
環境規格	
作業溫度	0°C to 40°C
儲存溫度	-30°C to 60°C
作業濕度	5% to 90% (非凝結)

備註：

*1: 測試方法: 最大效能是以 RFC 2544 (UDP 封包、1,518 位元組)。實際的效能可能視網路條件及啟動的服務而有不同。

*2: 根據 RFC 2544, 使用 1,424 位元組封包尺寸的 UDP 流量來測量 VPN (AES) 效能。

*3: 對照 1,460 位元組封包尺寸的 HTTP 協定, 使用產業標準的 Ixia IxLoad 測試工具來測量 UTM (AV+IDP) 效能。測試經多次流量往返才完成。

*4: 使用產業標準的 Ixia IxLoad 測試工具來測量最大 session。

特色

防火牆

- ICSA認證的防火牆
- 路由及透通(橋接)模式
- 以區域為基礎的存取管制表
- SPI 動態封包檢測
- 強化使用者感知政策管理
- SIP/H.323 NAT穿越
- ALG支援客戶埠

支援IPv6

- 具備IPv6 金牌標章認證
- 支援 Dual Stack模式
- 支援IPv4 Tunneling(6rd and 6to4)
- Host/Router/Firewall

虛擬私有網路(VPN)

- ICSA認證的IPSec VPN
- 演算法：AES/3DES/DES
- 驗證：SHA-1/MD5
- 關鍵管理：手動金鑰/IKE
- 完整轉發保密能力(DH群組)支援1、2、5
- IPSec NAT穿越
- 斷線偵測/中繼偵測
- PKI(X.509)認證支援
- VPN集中化支援
- 簡易精靈支援
- 自動重新連線VPN
- VPN HA(備援遠距VPN閘道器)

SSL VPN

- 用戶端安全遠距存取
- 支援反向代理模式及完整通道模式
- 統一政策施行
- 支援雙因素驗證
- 可客製化的使用者入口

入侵偵測防禦

- 路由及透通(橋接)模式
- 區域基礎的IDP檢測
- 可客製化的防護設定檔
- 可防禦超過2000種攻擊
- 自動更新特徵碼
- 客戶端特徵碼

- 協定異常偵測與保護
- 流量異常偵測與保護
- 異常訊務偵測與保護
- DoS/DDoS保護

防毒

- 支援Kaspersky及ZyXEL防病毒程式
- 以串流為基礎的防毒引擎
- 以區域為基礎的防毒政策
- 支援HTTP/FTP/SMTP/POP3/IMAP4協定
- 自動更新病毒特徵碼
- 無檔案大小限制
- 支援黑名單/白名單

應用程式巡察

- 應用軟體、IM/P2P、多媒體串流、VoIP存取
- IM的細節存取控制(聊天、檔案傳送、視訊)
- 應用程式及IM/P2P頻寬控制
- 支援使用者驗證
- IM/P2P特徵碼自動更新
- 支援超過15個目錄的IM及P2P
- 即時統計報告
- 最大/保證頻寬

防垃圾郵件

- 區對區防護
- 透過SMTP/POP3協定攔截郵件
- 支援POP3/SMTP 連接埠設定
- 以寄件者IP信譽為基礎的過濾方式
- 支援Commtouch RPD查詢
- 零時差的病毒攻擊防禦
- 支援 X-Header
- 支援黑名單/白名單
- 支援DNSBL檢查
- 支援垃圾郵件標籤
- 統計報告

高可用性

- 主動-被動模式
- 裝置故障偵測與通知
- 支援ICMP與TCP ping檢查
- 連結監測
- 自動同時配置

內容過濾(BlueCoat / Commtouch)

- 社交網路管制
- 網頁安全—BlueCoat 安全瀏覽
- URL阻擋、關鍵字阻擋
- 已設定檔為基礎的設定方式
- 排除名單(黑名單與白名單)
- 封鎖 java applet、cookies及active X
- 動態URL過濾資料庫(BlueCoat/Commtouch)
- 支援無限使用者授權
- 警告訊息客製化，重新轉向URL位址。

網路

- 路由模式/橋接模式/混合模式
- L2連接埠群組功能
- 乙太網路/PPPoE
- NAT/PAT
- 支援802.1Q tagged VLAN
- 虛擬介面(alias介面)
- 以政策為基礎的路由方式(使用者感知)
- 以政策為基礎的NAT(SNAT)
- 支援動態路由(RIP v1/v2, OSPF)
- 支援DHCP客戶端/伺服器/中繼
- 動態DNS支援
- 支援2埠以上WAN Trunk(USG 50/100/200)
- 每主機session數限制
- 保證頻寬
- 最大頻寬
- 優先頻寬使用



驗證

- 本地使用者資料庫
- 支援微軟AD
- 支援外部LDAP/RADIUS使用者資料庫
- 用於IPSec VPN的Xauth over RADIUS
- 強迫使用者驗證(透過驗證)
- IP/MAC位址定位
- Syslog(傳送到最多四個伺服器)
- 電子郵件警報(傳送到最多兩個伺服器)
- 即時流量監測
- 內建的每日報告
- 支援進階報告(Vantage Report)
- 支援集中化網路管理(CNM)Vantage可管理

系統管理

- 以角色為基礎的管理
- 多重管理員登入
- 多國語言網路介面(HTTPS/HTTP)
- 物件為基礎配置
- 指令行介面(console/web console/SSH/TELNET)
- SNMP v2c(MIB-II)
- 系統配置回覆
- 透過FTP/FTP-TLS/web GUI升級韌體

記錄/監測

- 全方位的本地日誌記錄

認證

- EMC
- FCC Part 15(Class B)
- CE EMC (Class B)

支援3G網卡列表

請參考 http://www.zyxel.com/products_services/smb_security_appliances_and_services.shtml

並找到以下路徑: ZyWALL Unified Security Gateways → USG product pages to see the 3G Card Compatibility List for supported USB devices

