



主要特色

- 全新平台：「第三代」ZyWALL
- USG網路潔淨功能
(clean-traffic) 架構
- 新一代的UTM解決方案
(不包括USG 20/20W)
- 健全的hybrid VPN功能
(IPSec及SSL)
- 應用程式防火牆
(不包括USG 20/20W)
- 對社交網路應用的精密控制
- 多個WAN埠及3G備援的不中斷
網路存取
- ICSA防火牆、IPSec認證
- 全方位的報表系統
- 防垃圾郵件服務
- ZyXEL安全分佈網 (ZyXEL
Security Distribution Network,
ZSDN)

企業安全

ZyWALL整合式安全閘道器系列
(20/50/100/200/300/1000/2000 Series)

ZyWALL USG (整合式安全閘道器) 系列是標榜全新平台的「第三代」ZyWALL，能為小公司到大企業提供更強大的效能防護，以及深層封包偵測安全解決方案。僅僅一台ZyWALL USG產品便提供了狀態封包檢測 (Stateful Packet Inspection, SPI) 防火牆、防病毒、入侵偵測防禦、內容過濾、防垃圾郵件及VPN (IPSec/SSL/L2TP) 等功能。這套多層次安全設備捍衛您組織的客戶及公司記錄、智慧財產及關鍵資源，防禦來自外部及內部的威脅。

主要優勢

安全連線

資訊科技 (IT) 系統現今已普遍存在，重要性不言而喻，而大幅部署新網路技術的相關機會和風險在本質和規模上讓組織暴露於一定的危險，這種種現象迫使組織必須評估解決方案來建立更安全的基礎架構，以保障涉及寶貴資訊交換的線上交易之安全。基礎架構必須量身訂做，才能滿足擴大遠距地點及行動通訊工作者的作業需求。

主動防禦

惡意病毒、蠕蟲和攻擊程式可能癱瘓企業網路，讓業務交易停擺。除了嚴重的財務損失，您也可能面臨機密資訊洩漏的危機。由於大量發信軟體公司在網際網路上如雨後春筍般地湧現，您的網路可能受到龐大垃圾郵件 (spam) 的轟炸。如果沒有智慧型的偵測和主動防禦阻斷機制，使用者必須耗時費力地過濾冗濫的郵件信箱，而這種情節會導致生產力的嚴重損失。

遵守政策

有了眾多的檔案分享 (P2P) 和即時訊息 (IM) 應用，企業員工在上班時間要分享檔案和進行線上聊天變得更容易。快速的檔案分享不僅會因為分享包含惡意病毒的問題檔案而危及網路安全，也可能因此侵犯著作權而製造法律爭端。

網路恢復力

ISP連結失效、在閘道器上的硬體和軟體故障、VPN通道不通-這些都是IT技術人員在設計網路基礎架構時面臨的嚴重挑戰。簡言之，我們在為不中斷的營運建立高可用性的網路基礎架構時，必須考量在網路路徑上的容錯。

容易管理

有了Vantage CNM (集中化網路管理)，使用者可達到以下目標：

- 容易的VPN管理及診斷能力
- 完整的安全政策及UTM管理
- 大量部署及裝置維修的整體擁有成本 (TCO) 低
- 有效的監測、警告及全方位圖解報告

這個解決方案為任何規模的企業提供了有效率的集中化管理系統，不論分公司或遠距地點有多少，都能降低營運成本。

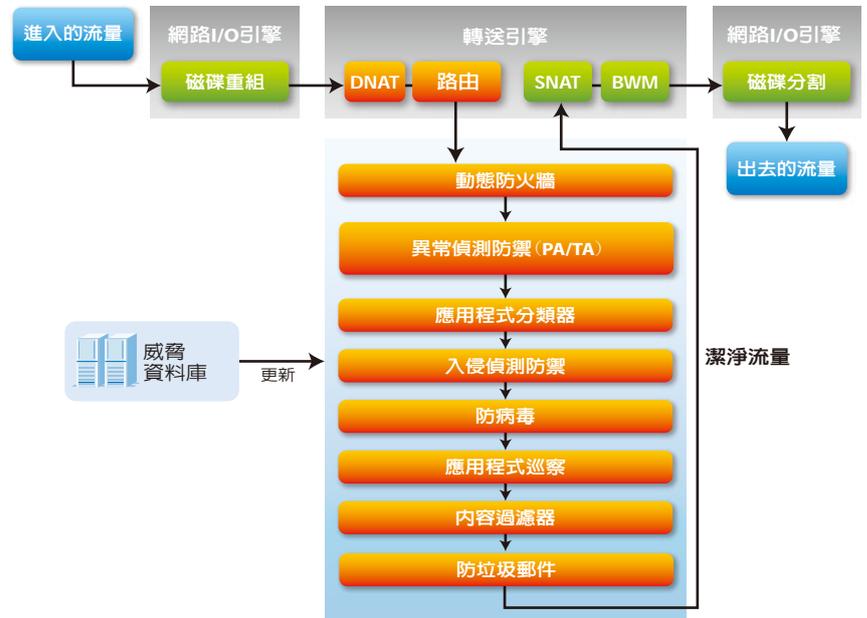
具成本效益

ZyXEL現在提供免費的軟體升級，您不需多花一毛錢便能享有完整的保護。

主要應用

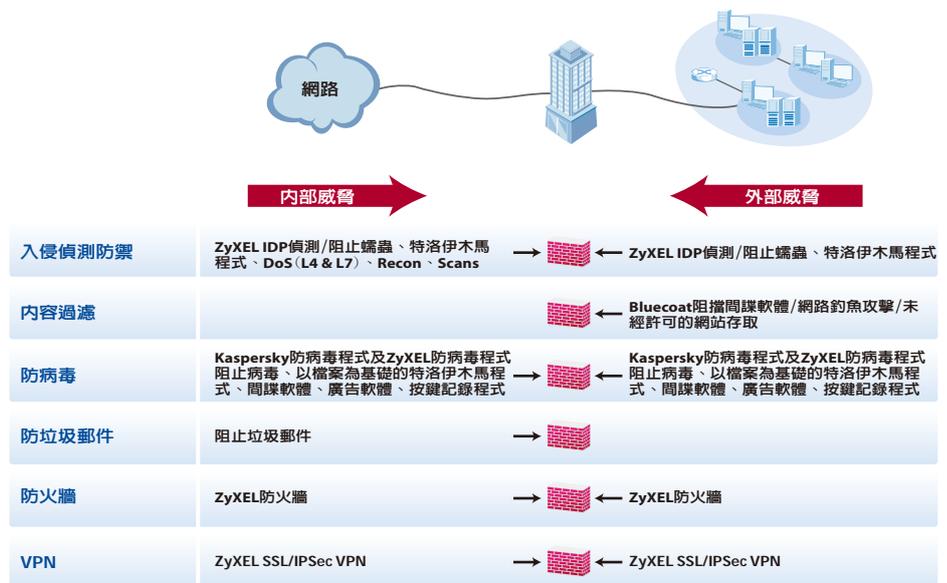
ZyWALL USG網路潔淨功能架構

The ZyWALL USG的網路潔淨功能架構能夠防禦病毒、蠕蟲、特洛伊木馬程式、間諜軟體、網路釣魚攻擊及其他新網路威脅等網路風險。有了網路潔淨功能架構，企業使用者可安心擁有潔淨安全的網路環境。



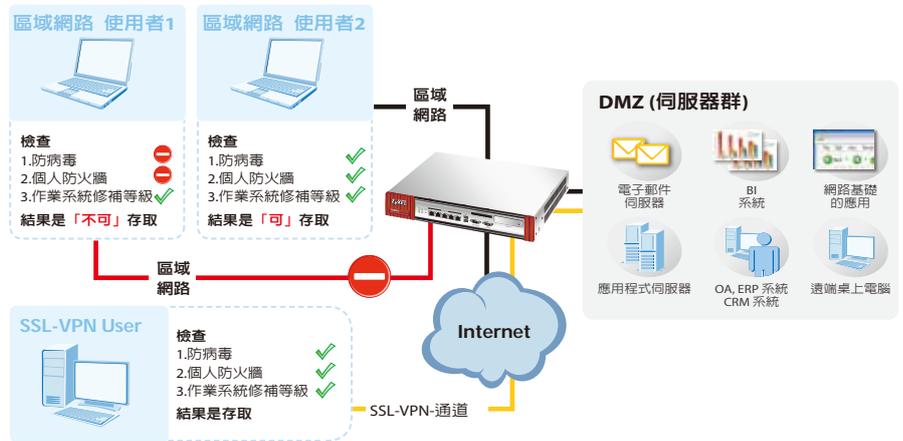
新一代的UTM解決方案

ZyWALL USG系列產品結合了硬體加速技術。在高性能SecuASIC技術及硬體加密加速器的助力下，ZyWALL USG系列為小公司和大企業實現了領先產業的績效，以及多層次的防禦威脅機制。ZyWALL USG系列提供了整合式統一威脅管理安全性功能，例如防病毒(包括Kaspersky防病毒及ZyXEL防病毒)、IDP、防垃圾郵件、內容過濾及防火牆、VPN。ZyWALL USG系列的所有產品都支援Gigabit乙太網路。



端點安全

有了新的端點安全 (Endpoint Security, EPS) 功能，管理員可輕易辨識出「壞」使用者，亦即未安裝防病毒軟體處。藉由強迫安裝防病毒軟體，ZyWALL能夠減緩病毒入侵的威脅，因此降低金錢及員工生產力的損失。除了其他軟體外，EPS尚支援Norton™ Kaspersky™及TrendMicro™ AV客戶端軟體。此外，新的EPS功能也支援個人防火牆軟體，例如Kaspersky Internet Security 2009/2010、Windows Firewall及TrendMicro PC-Cillin/Internet Security 2010。

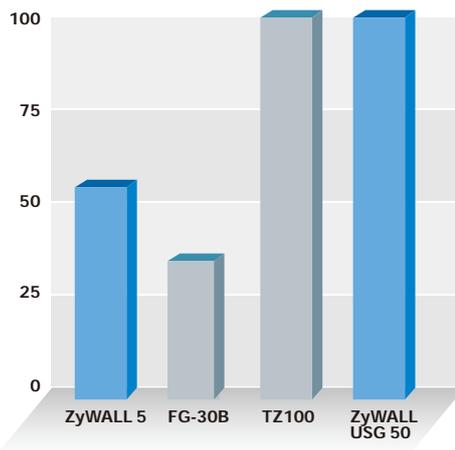


USG的新「端點安全」(End Point Security, EPS) 功能有助於確保所有用戶達到企業安全政策，亦即它會檢查AV軟體是否已安裝。

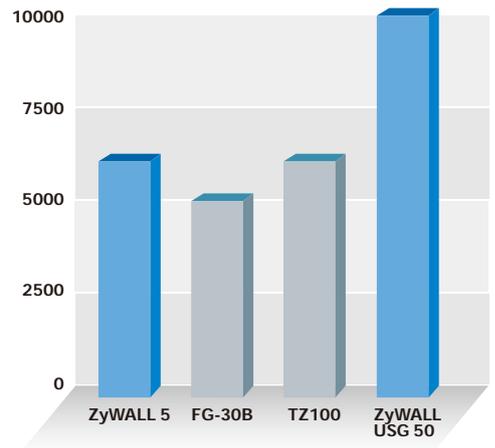
高效能

ZyXEL 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。以USG 50為例，這項產品能為小公司實現絕佳的效能。

競爭力比較：防火牆效能(以Mbps計)



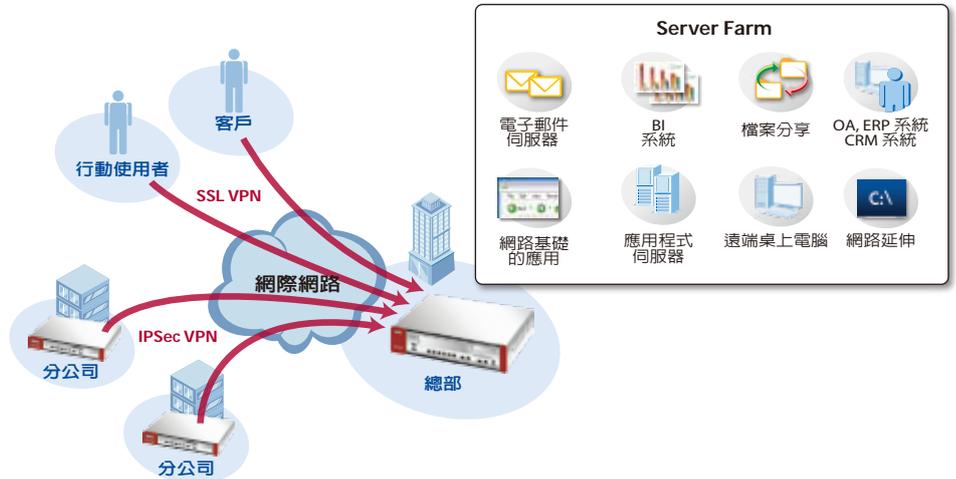
競爭力比較：Session數量



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

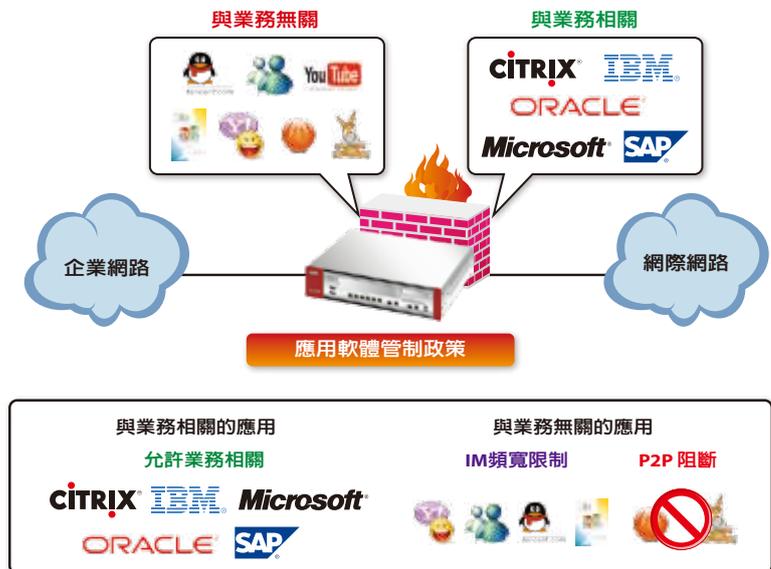
健全的hybrid VPN功能 (IPSec and SSL)

不論是何種規模的企業，ZyWALL USG系列都能透過網際網路，在遠端地點與企業資源之間提供安全的存取路徑。使用IPSec VPN，企業可保障與分公司、合作伙伴和總部之間的連線安全。經常出差的員工及電子通勤族可使用SSL或L2TP VPN來安全地存取公司網路，而不必安裝VPN軟體。ZyWALL USG系列提供了有彈性且容易的方法，讓行動員工、廠商及合作伙伴能有信心的存取公司網路資源，進而達到更高的效率。



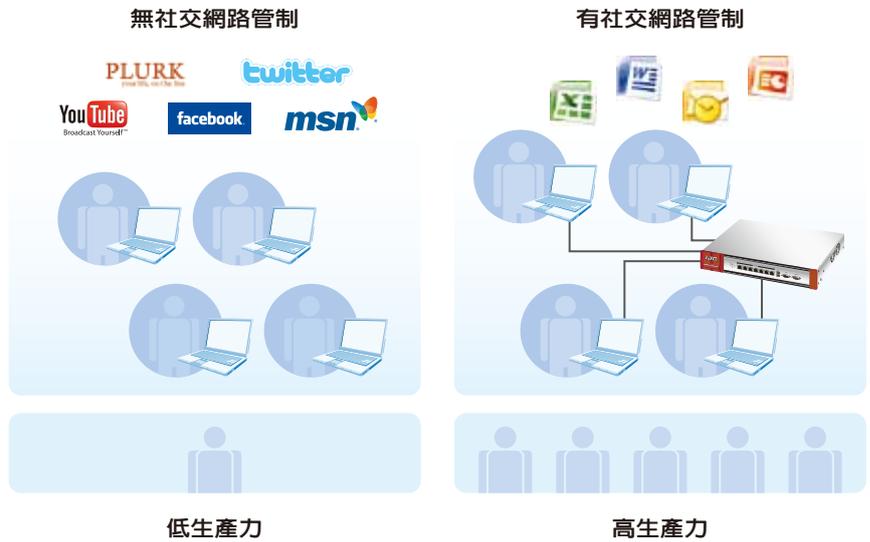
應用程式防火牆

愈來愈多網路應用程式將惡意軟體帶進您的辦公室，這種不受歡迎的軟體，尤其是IM/P2P應用軟體，可能造成頻寬浪費，甚至是系統損壞。只要使用應用程式巡察及頻寬管理功能，您可以完全掌控流量管制或速度限制等設定。



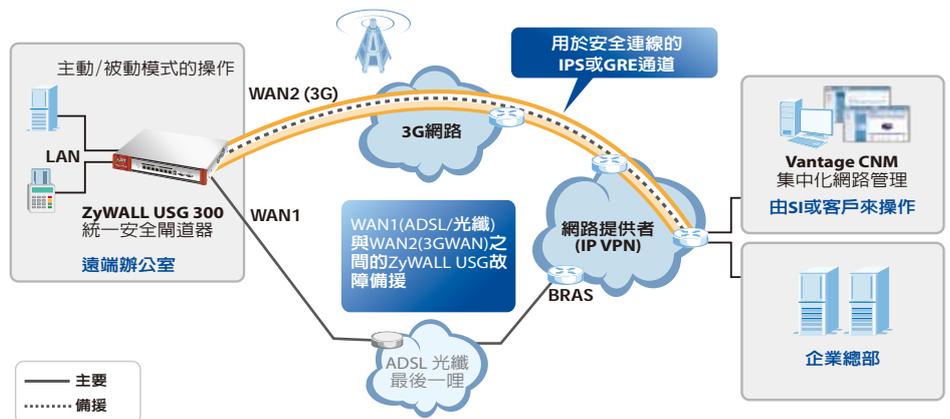
對社交網路應用的精密控制

諸如Facebook、Twitter及Youtube等社交網路應用，已成為人們快速聯繫並分享資訊的網路現象。如果沒有靈活的管理，社交網路應用將侵蝕掉業務生產力。ZyWALL USG能確保網際網路不被濫用，防止頻寬浪費或違反人力資源政策。ZyWALL USG能對社交網路應用提供精密控制。



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或PCMCIA卡支援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。



防垃圾郵件服務

ZyXEL的防垃圾郵件服務透過統一的安全架構，去除垃圾郵件、網路釣魚攻擊、病毒及惡意軟體威脅，而不會漏掉正當的訊息。有了ZyXEL的防垃圾郵件服務，企業可節省處理不當郵件的時間和資源，進而降低營運成本。



ZyXEL安全分散式網路 (ZSDN) 能確保對新威脅做出快速反應

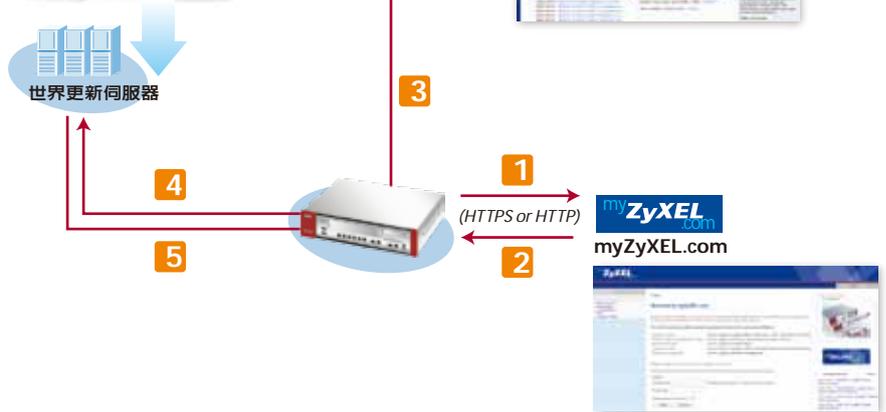
ZSDN提供最新的保護

- myZyXEL.com網站提供便利、集中化的方法來登記所有ZyWALL單位及安全服務。
- ZyXEL安全更新伺服器全年無休地運作，自動傳送更新的簽名資料庫到世界各地的ZyWALL單位。
- mySecurityZone入口提供全方位、可搜尋的病毒和系統弱點相關資訊，且提供豐富的資訊資源，讓客戶隨時知道最新的弱點和對策。

ZyXEL 安全應變團隊



安全資訊中心 (電子郵件佈告欄)



- 1 登記與啓用**
 1. 登入
 2. MAC
 3. RegType (試驗)
 4. 授權金鑰
- 2 1. SKU**
 2. 到期日

- 3 檢查政策與建議**
- 4 請求下載**
- 5 下載簽名**

登記中心

規格

機種	SB			SMB				
	ZyWALL USG 20W	ZyWALL USG 20	ZyWALL USG 50	ZyWALL USG 100	ZyWALL USG 200	ZyWALL USG 300	ZyWALL USG 1000	ZyWALL USG 2000
產品照片								
特色	<ul style="list-style-type: none"> • 小型企業的整合式安全閘道器 (1~5個PC使用者) • 全Gigabit乙太網路介面設計 • 高效能多層次威脅防禦 • Hybrid VPN(IPSec、SSL)保障連線安全 • USB埠支援3G，提供WAN備援 • 802.11b/g/n無線AP 	<ul style="list-style-type: none"> • 小型企業的整合式安全閘道器 (1~5個PC使用者) • 全Gigabit乙太網路介面設計 • 高效能多層次威脅防禦 • Hybrid VPN(IPSec、SSL)保障連線安全 • USB埠支援3G，提供WAN備援 	<ul style="list-style-type: none"> • 小型企業的整合式安全閘道器 (1~10個PC使用者) • 全Gigabit乙太網路介面設計 • 高效能多層次威脅防禦 • Hybrid VPN(IPSec、SSL)保障連線安全 • 用於多個ISP連結及負載平衡的多個WAN埠 	<ul style="list-style-type: none"> • 中型企業的整合式安全閘道器 (10~25個PC使用者) • 高效能多層次威脅防禦 • Hybrid VPN (IPSec、SSL及L2TP) 保障與總部的連線安全 • 支援Kaspersky及ZyXEL防病毒程式 	<ul style="list-style-type: none"> • 中型企業的整合式安全閘道器 (25~50個PC使用者) • 高效能多層次威脅防禦 • Hybrid VPN (IPSec、SSL及L2TP) 保障與總部的連線安全 • 支援Kaspersky及ZyXEL防病毒程式 • 可彈性選購OTP埠 	<ul style="list-style-type: none"> • 中型企業的整合式安全閘道器 (50~75個PC使用者) • 提供Hybrid VPN (IPSec/SSL VPN) 及健全的UTM安全服務 • 高效能多層次威脅防禦 • 個人化安全網路政策引擎提供了存取粒度能力 • 有目標、文本基礎且集中化的絕佳管理 	<ul style="list-style-type: none"> • 中型企業的整合式安全閘道器 (75~200個PC使用者) • 提供Hybrid VPN (IPSec/SSL VPN) 及健全的UTM安全服務 • 高效能多層次威脅防禦 • 關鍵任務應用不中斷運作 • 有目標、文本基礎且集中化的絕佳管理 	<ul style="list-style-type: none"> • 中型企業的整合式安全閘道器 (200~500個PC使用者) • 提供光纖介面的Gigabit防火牆 • 可擴充的VPN/UTM效能 • 支援Kaspersky及ZyXEL防病毒程式 • 電源備援模組
硬體規格								
10/100/1000 介面 (銅)	4 x LAN/DMZ, 1 x WAN	4 x LAN/DMZ, 1 x WAN	4 x LAN/DMZ, 2 x WAN	5 x LAN/DMZ, 2 x WAN	5 x LAN/DMZ, 2 x WAN, 1 x OPT	7	5	6
Dual Personality GbE (SFP/RJ45)	-	-	-	-	-	-	-	2
USB 埠	1	1	2	2	2	2	2	2
SEM 槽 (安全延伸模組)	-	-	-	-	-	-	-	1
卡槽	-	-	-	1	1	2	1	1
802.11b/g/n	是	-	-	-	-	-	-	-
2x2 天線	是	-	-	-	-	-	-	-
系統容量與效能								
SPI 防火牆效能 ¹ , Mbps	150	150	180	180	250	300	400	2,000
VPN 效能 (3DES) ² , Mbps	75	75	90	90	90	130	180	600 ¹⁴
UTM 效能 (AV+IDP) ³ , Mbps	-	-	24	30	40	80	100	400 ¹⁵
WiFi 效能, Mbps ⁷	80	-	-	-	-	-	-	-
無上限使用者授權	是	是	是	是	是	是	是	是
最大Sessions ⁶	6,000	6,000	10,000	20,000	40,000	60,000	500,000	1,000,000
新 Session 速率	900	900	1,000	1,000	1,000	1,500	12,000	20,000
IPSecVPN通道同時連線數 (最大)	5	5	5	50	100	200	1,000	2,000
SSL VPN 使用者同時連線數 (最大)	1	1	5	5	10	25	250	750 ^{11,12}
包含SSL VPN使用者	1	1	2	2	2	2	5	5
可客製化區	是	是	是	是	是	是	是	是
電源需求								
輸入電壓	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50 - 60 Hz, 1.2 A	100 - 240 V AC, 50/60 Hz, 0.55 - 0.3 A	100 - 240 V AC, 50/60 Hz, 1 A Max	100 - 240 V AC, 50 - 60 Hz, 3 - 6 A
額定功率	最大16 W	15 W Max	17 W Max	20 W Max	20 W Max	35 W Max	80 W Max	200 W Max
環境規格								
操作溫度	0°C 至 40°C	0°C 至 40°C	0°C 至 40°C	0°C 至 40°C	0°C 至 40°C	0°C 至 40°C	0°C 至 40°C	0°C 至 40°C
儲存溫度	0°C 至 40°C	0°C 至 40°C	0°C 至 40°C	-30°C 至 60°C	-30°C 至 60°C	-30°C 至 60°C	-30°C 至 60°C	-30°C 至 60°C
操作濕度	20% 至 95% (非凝結)	20% 至 95% (非凝結)	20% 至 95% (非凝結)	5% 至 90% (非凝結)	5% 至 90% (非凝結)	20% 至 90% (非凝結)	5% 至 90% (非凝結)	5% 至 90% (非凝結)
實體規格								
尺寸, (寬) × (深) × (高)公釐	216 x 140 x 33	216 x 140 x 33	242 x 167 x 35.5	242 x 175 x 35.5	242 x 175 x 35.5	430 x 201 x 42	431 x 292 x 43.5	430 x 487 x 89
重量, 公斤	0.42	0.38	1.2	1.2	1.2	2.8	4.7	10.5

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: 附SEM-DUAL/SEM-VPN模組。

*5: 附SEM-DUAL模組。

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

*7: 11N無線網路標準僅支援20MHz頻寬模式

特色

防火牆

- ICSA認證的防火牆
- 路由及透明(橋接)模式
- 區域基礎的存取管制表
- 動態封包檢測
- NAT、PAT
- 政策基礎NAT
- 虛擬區域網路標籤
- 個人化安全網路政策施行
- SIP/H.323 NAT穿越
- ALG支援客戶埠

虛擬私有網路 (VPN)

- ICSA認證的IPSec VPN
- PPTP、L2TP、IPSec
- 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

- 無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 (IDP) (不包括USG 20/20W)

- 路由及透明(橋接)模式
- 區域基礎的IDP檢測
- 可客製化的保護剖繪
- 防禦2000攻擊
- 自動簽名更新
- 客戶簽名
- 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

防病毒 (USG 20/20W除外)

- 支援Kaspersky及ZyXEL防病毒程式
- 串流基礎的防病毒引擎
- 區域基礎的AV保護
- 支援HTTP/FTP/SMTP/POP3/IMAP4協定
- 自動簽名更新
- 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、串流應用媒體、VoIP存取精密控制
- 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簽名自動更新
- 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協定透明攔截郵件
- 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 (不包括USG 50/20/20W)

- 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

- 社交網路管制
- 網頁安全—ZyXEL安全瀏覽
- URL阻斷、關鍵字阻斷
- Profile基礎設定
- 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發動)
- 支援無限使用者授權
- 警告訊息客製化，並改變URL方向。

網路

- 路由模式/橋接模式/混合模式
- 第二層埠群組功能
- 乙太網路/PPPoE
- 標籤化VLAN(802.1Q)
- 虛擬介面(alias介面)
- 政策基礎路由(個人化)
- 政策基礎NAT(SNAT)
- 動態路由(RIP v1/v2, OSPF)
- DHCP客戶端/伺服器/中繼
- 動態DNS支援
- WAN Trunk超過2埠
- 每主機session限制
- 保證頻寬
- 最大頻寬
- 優先頻寬使用

驗證

- 地方使用者資料庫
- Microsoft Windows有效目錄整合
- 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(透明驗證)
- IP/MAC位址定位

系統管理

- 以角色為基礎的管理
- 多管理員登入
- 多語言網路GUI(HTTPS/HTTP)
- 頻外管理(AUX)
- 目標基礎配置
- 命令行介面(console/web console/SSH/TELNET)
- SNMP v2c(MIB-II)
- 系統配置回返
- 透過FTP/FTP-TLS/web GUI升級韌體

記錄/監測

- 全方位的局部日誌記錄
- 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
- 進階報告(Vantage Report)
- 集中化網路管理(CNM) Vantage可管理

配件

安全性擴充模組 (僅USG 2000)

機種	SEM-DUAL	SEM-VPN
產品照片		
特色	<p>針對需要完整安全功能的客戶，包括VPN及UTM威脅防禦功能。SEM-DUAL提供ZyWALL USG 2000平台的完全馬力，且其VPN及UTM效能強大。</p> <ul style="list-style-type: none"> 用於UTM加速的SecuASIC CIP-3001 (防病毒及IDP) 大幅提昇VPN效能的進階VPN Crypto 	<p>針對有密集VPN應用需求，以便在中央地點建立強大的VPN集中器，並需要最高度冗位的客戶。專精於VPN應用程式，SEM-VPN能加速VPN效能。</p> <ul style="list-style-type: none"> 大幅提昇VPN效能的進階VPN Crypto
系統效能		
VPN 效能 (AES) ^{*7}	400 Mbps	400 Mbps
UTM 效能 (AV+IDP) ^{*8}	400 Mbps	100 Mbps
最大IPSec VPN 隧道	2,000	2,000
最大SSL VPN 使用者	750	750
環境規格		
操作溫度	0°C 至 40°C	0°C 至 40°C
儲存溫度	-30°C 至 60°C	-30°C 至 60°C
操作濕度	5% to 90% (非凝結)	5% to 90% (非凝結)
實體規格		
尺寸, (寬) × (深) × (高)公釐	199.2 x 212 x 36.3	199.2 x 212 x 36.3
重量, 公克	410	410

備註：

*7: 有1,460位元組封包的VPN (AES) HTTP協定。測試經多次流量往返才完成。

*8: 使用產業標準的Ixia IxLoad測試工具來測量UTM (AV+IDP) 效能。

收發器

機種名稱	連線	波長	最大傳輸距離	光纖組數	雷射傳輸器特徵		接收器特徵	
					最大發射功率	最小發射功率	光纖接收器敏感度	最大輸入功率
SFP-SX-D	LC	850 nm	550 m	7.5 dB	-4 dBm	-9.5 dBm	-17 dBm	-3 dBm
SFP-LX-10-D	LC	1310 nm	10 km	10.5 dB	-3 dBm	-9.5 dBm	-20 dBm	-3 dBm
SFP-LHX1310-40-D	LC	1310 nm	40 km	21 dB	+3 dBm	-2 dBm	-23 dBm	-3 dBm
SFP-ZX-80-D	LC	1550 nm	80 km	24 dB	+5 dBm	0 dBm	-24 dBm	-3 dBm

軟體授權

產品	期間	ZyXEL 防毒	Kaspersky 防毒	入侵偵 測防禦	內容 過濾器	資安管理軟體 Vantage CNM	集中式報表軟體 Vantage Report
USG 2000	1年	是	是	是	是	所有ZyWALL機種 支援: 10個節點 25個節點 50個節點 100個節點 300個節點 1000個節點	所有ZyWALL機種 支援: 1台裝置 5台裝置 25台裝置 100台裝置
	2年	是	是	是	是		
USG 1000	1年	是	是	是	是		
	2年	是	是	是	是		
USG 300	1年	是	是	是	是		
	2年	是	是	是	是		
USG 200	1年	是	是	是	是		
	2年	是	是	是	是		
USG 100	1年	是	是	是	是		
	2年	是	是	是	是		
USG 50	1年	是*	是	是	是		
	2年	是*	是	是	是		
USG 20	1年	-	-	-	是		
	2年	-	-	-	是		
USG 20W	1年	-	-	-	是		
	2年	-	-	-	是		

*:2011年第一季上市

產品	SSL VPN 通道數	IPSec VPN Client用戶端授權數
USG 2000	5至50個	對於用戶端PC 1個用戶端軟體授權 5個用戶端軟體授權 10個用戶端軟體授權 50個用戶端軟體授權
	5至250個	
	5至750個	
	50至250個	
	50至750個	
	250至750個	
USG 1000	5至25個	
	5至50個	
	5至250個	
	25至50個	
	25至250個	
	50至250個	
USG 300	2至10個	
	2至25個	
	10至25個	
USG 200	2至10個	
USG 100	2至5個	
USG 50	2至5個	
USG 20	-	
USG 20W	-	

支援3G卡

3G卡不包含在內。請造訪<http://www.zyxel.com/web/>，找到以下路徑：
網路安全設備 → 整合式安全閘道器 → 單一USG產品頁面，便可查詢支援USB裝置的3G
卡相容列表。

For more product information, visit us on the web at www.ZyXEL.com



Copyright © 2010 ZyXEL Communications Corp. All rights reserved. ZyXEL, ZyXEL logo are registered trademarks of ZyXEL Communications Corp. All other brands, product names, or trademarks mentioned are the property of their respective owners. All specifications are subject to change without notice.