SOHO/小型企業/分點辦公室專用

HiGuard Series

HiGuard XI

眾至 HiGuard 系列專為小型辦公室、分公司、零售環境提供全方位企業級的網路防護。桌上型入門級的解決方案具備成本效益、操作簡單、且佔用空間小的優勢，協助企業將安全防護擴展到組織最小單位。而小單位的資安重要性並不亞於企業總部，HiGuard XI 具備高可靠度的儲存與記憶體空間，使其性能有更大程度的發揮，支援 USB 3.2 埠口，並提供 3G/4G LTE USB 作為 WAN 網路備援。其軟體系統設計基於零信任架構 (ZTA) 為原則，除了基本 Firewall 功能，也提供 VPN 安全連線 (IPSec、SSL)、閘道安全防護機制 (Anti-Virus, IPS, Sandstorm IP, SYN Flood 防護...)、多因子驗證 (帳號管理、上網認證、SSL VPN)、協作控管 (交換器、無線 AP)、網管分析 (URL/APP 管制與資料庫、頻寬管控、上網行為管理、負載平衡) 等功能一應俱全。此外，HiGuard 系列提供地端 CMS 管理平台，Client 端能被上層 UTM 掌握其運作狀態，管理者也可透過雲端 Eye Cloud，單一介面直接監控眾至所有設備，並延伸監控交換器與無線基地台的運作狀態，讓管理者在問題發生的第一時間內，能夠有效進行錯誤排除與思考解決方案，將安全防護盡可能擴展到企業運作的每個區塊。

HiGuard XI 三大特點

SECURITY 安全	MANAGEMENT 管理	PERFORMANCE 效能
閘道防護機制 VPN安全連線	**兩步驟驗證、上網行為分析 單一平台管控**	**X86雙核硬體平台 優化記憶體與儲存空間**
• IPSec/SSL VPN加密通道 • 防毒引擎 • IPS入侵偵測防禦 • Sandstorm IP • SYN Flood防護	• 兩步驟驗證(2FA) • 頻寬、流量與應用程式管控 • 交換器協同防禦與AP管理 • CRM地端管理 (Client端) • Eye Cloud雲端管理	• 4個Gigabit高速網路埠 • 4G記憶體與32G儲存空間 • 雙核Intel CPU處理器 • NAT達1.9 Gbps效能 • USB特徵碼離線更新與還原

HiGuard XI 防護特點

SOHO 小型辦公室專用 UTM

HiGuard XI 是一款 9 吋桌機型 UTM，專為 SOHO 或小型辦公室路環境所設計，目的在於整合配置、部屬、管理與監控於單一管理平台。全系列採無風扇靜音設計，提供小型辦公室寧靜無噪音的工作環境。HiGuard XI 是經濟高效的安全防護系統，提供企業最安全的威脅管理解決方案，軟硬體優規設計可以輕鬆負載 50 人以下的網路環境，部屬簡單快速，可以減免裝置勞動力，還延伸結合兩步驟認證、無線網路解決方案，成為新一代辦公網路環境首選！

防火牆

內建 SPI 狀態封包檢查技術，利用封包檢查追蹤網路連線狀態，藉此發現網路環境中易受攻擊的弱點。系統能夠主動攔截阻斷駭客攻擊行為，如資源耗盡式的攻擊方式 (SYN Flood、ICMP Flood、UDP Flood) 等等。ShareTech 套用合理流量封包及連線數的觀念，認為每個來源在每秒不會同時產生太多封包，萬一超過所設定的合理封包數，防火牆會阻擋多餘的封包，避免影響用戶服務體驗。

高效能 NAT 處理速度

目前 ISP 業者紛紛以實惠價格提供高速穩定的網路，為了讓多數企業用戶完整體驗頻寬提升，HiGuard XI 提供高效能與穩定的運作能力，支援 4 個 Gigabit 乙太網路連接埠，1 個固定 LAN 埠與 3 個可自訂義的連接埠，NAT 的傳輸效率可達 1.9 Gbps，打破以往對於桌機型設備效能不理想的疑慮。

病毒過濾引擎

內建 Clam AV 免費防毒引擎，預設啟動以提供 24 小時即時更新與病毒資料庫維護，可偵測數百多萬種以上的病毒、蠕蟲、木馬程式，自動對電子郵件進行病毒掃描，透過網路每日自動更新病毒檔，還提供病毒郵件搜尋條件。管理者可以自行設定病毒碼更新時間、檢視引擎版本與更新紀錄、選擇更新病毒資料庫的伺服器，選擇對三種不同郵件動作（外對內寄信、內對外寄信、內對外收信）進行掃毒，以及設定中毒郵件的處置，包含隔離、變更副檔名稱、與變更通知信主旨。

負載平衡

負載平衡協助企業以較低的成本取得較高的頻寬，HiGuard 系列擁有至少 2 個 WAN 埠，透過負載平衡演算法自動將流量平均分配在各個線路（多條專線或 ISP 連線服務）。同時支援備線路備援 (Multi-Homing)，可自動將有問題的線路切換到其他正常線路。此外，管理者還可以利用 USB 埠，外接無線 3G/4G USB，實現無線即時備援與負載平衡機制。藉由整合多條廣域網路，協助企業打造不斷線的網路環境。

支援 SD WAN

ShareTech SD WAN 利用網際網路建立 IPSec VPN，可以當做企業專線 (MPLS) 的備援線路以降低企業成本。管理者可以利用更少的頻寬、更快的效能，輕鬆在 WAN 線路上進行部署。除了可以在中心端部屬單向運作之外，也可以建立多條 IPSec VPN 與 IP Tunnel VPN 至中心端，以線路備援機制來優化兩端點之間的連線負載，舉例如企業重要郵件採用 MPLS 專線服務、ERP 系統採用 IPSec VPN，無痛整合與切換以確保商務交流暢通。

頻寬管理功能 QoS

頻寬管理機制會在頻寬可運用範圍內，優先將剩餘頻寬進行分配，讓使用者有機會到達設定的最大頻寬。以單一或多個綁定的 ZONE 為單位，透過條例或來源 IP 進行頻寬管制，此外，也支援管理頻寬優先順序、保證最大可使用頻寬，協助網管人員控管上傳 (TX) 與下載 (RX) 的網路流量，有效減緩企業頻寬被獨佔、網路阻塞，提升服務性與頻寬使用率。

URL 資料庫管理 (一年授權)

管理使用者瀏覽的網站，不僅可以提升員工工作效率，還可以過濾惡意網站，避免使用者在不知情的狀況下遭植入惡意程式、病毒，以確保企業網路安全。HTTP 與 HTTPS 加密網站皆可被管理，與第三方廠商合作的進階 URL 資料庫，採雲端更新機制，會自動將網頁分類，管理者可以建立不同 URL 管理機制以及套用不同的阻擋訊息，阻擋記錄日誌也會被保留便於日後查詢。眾至 HiGuard 系列皆內建一年授權，客戶可自行選擇訂閱新授權，以持續獲得即時更新的 URL 網站列表。

APP 應用程式管制 (一年授權)

多半網路應用程式都與網路相連，系統元件通常被授予最廣泛的存取權限。但管理龐大的應用程式非常不容易，因為可能成為最直接的攻擊面。ShareTech 與第三方廠商合作的進階 APP 應用程式資料庫，根據應用程式的屬性進行分類，包含 P2P 軟體、VPN 與遠端控制、影音服務、VOIP、網路服務、資料共享與儲存、網站服務、社群網路、即時通訊、系統與更新、新聞媒體、購物拍賣、娛樂與藝術、運動與旅行、飲食、金融保險、賭博與色情、遊戲等等，可輕鬆控管員工使用應用軟體之權限，保護企業網路安全。眾至 HiGuard 系列皆內建一年授權，客戶可自行選擇訂閱新授權，以持續獲得即時更新的 APP 應用程式分類。

IPS 入侵防禦

IPS (Intrusion Prevention System) 會檢查對應到 OSI 模型第 4 到 7 層的內容，是否有惡意的攻擊程式、病毒隱藏在 TCP/IP 的通信協定中，透過詳細的內容與行為檢查後，符合條件的特徵碼就會被標示出來，就能立刻阻止有害的網路封包攻擊內部或是從內部攻擊外部，讓穿過防火牆的惡意封包無所遁形。ShareTech 提供不定期更新的 IPS 特徵值資料庫，依照危險程度分成高、中、低三種，管理者可以自行選擇放行或阻擋。

Sandstorm

新型 ShareTech Sandstorm 防護機制可以有效偵測未知的進階惡意程式附檔 (如常見 Microsoft Word、Excel、Power Point 或 PDF)、針對性的釣魚郵件 (phishing)、與壓縮檔 (常見的 ZIP 與 RAR)。不論是使用者誤點惡意網址或郵件中夾帶的附檔有惡意程式，HiGuard 系列會著重於 IP，自動比對是否存在惡意行為，並主動進行阻擋。

無線 AP 管控

企業打造無線上網辦公環境已成為常態，因此無線 AP 被廣泛應用以實現辦公室無線網路共享。當每台 AP 之間緊密串連時，員工可享有行進間裝置連線不中斷。HiGuard 系列透過 SNMP 或非加密 Telnet/ 加密 SSH 協議，支援 AP 無線管控機制，被管理的每台 AP 會按照群組分類，在 UTM 介面中呈現登入 IP、MAC、上網時間與每個 SSID 的使用人數。此外，管理者也可以透過 UTM 主控台遠端快速重啟 AP，能夠短時間內提升無線使用者體驗、故障排除與優化無線網路維運。

完整 VPN 運用方案 (IPSec、PPTP、L2TP、SSL VPN、IP Tunnel)

提供 IPSec、PPTP、L2TP、SSL、IP Tunnel 等等 VPN 連線模式，可經由佈建於兩地間建立加密通道，具多樣化的加密方式，確保資訊傳輸的安全性。同時針對 Tunnel 之間的傳遞封包進行管制，例如：限定 Web、SMTP、POP3 服務。

- 支援 IPSec、PPTP、L2TP、SSL、GRE Tunnel 等 VPN。
- DES、3DES、AES、AES128、AES192、AES256 加密服務 SHA-1/SHA256/SHA512/MD5 認證支援。
- SSL VPN Client 支援 (Android / IOS)。
- 可透由中心端直接管控分點網路服務。

威脅情報中心 Dashboard (選購)

威脅情報中心以高度圖形化的儀表板 (Dashboard)，提供企業網管人員動態可視性的選項，能夠即時反映網路的狀態，包含 HiGuard XI 今日即時資訊 (今日最高連線、可疑連線、威脅行為)、重點風險類型分類、流量分析、動態連線狀態、防火牆防護、IPS、WEB 服務與管控、郵件服務、應用程式管制、(依國家) 分析目的來源 IP、DNS 查詢等等資訊。Drill-Down 向下鑽取報表的設計，方便網管人員從各大區塊中找出問題根源。管理者可自行設定時間模式、資料排行、IPv4/v6 切換、檔案格式下載 (PNG/PDF)，提供企業最完整的縱深防禦機制，有效降低企業遭受潛在威脅的可能性。

HiGuard XI 功能說明

基本防火牆功能

- **路由管理**：支援靜態、動態路由、出口線路 (群組)、和預設閘道。
- **IPv4/v6**：支援 IPv4、IPv6、與 IPv4/IPv6 雙堆疊，管理者可以一鍵快速切換模式。
- **虛擬 VLAN 802.1Q**：可以將內部網路切割成數個獨立的子網段，運作不相干擾。
- **虛擬伺服器**：讓外部網路 IP 可以對應到內部 IP。
- **GEO IP**：位址表群組支援依據區域國家當目的 / 來源套用條例，針對區域性 IP 進行管理。
- **網路服務**：HiGuard 系列支援 DHCP、DDNS、SNMP、DNS Proxy。
- **阻斷服務 (DoS)、分散式阻斷服務 (DDoS) 攻擊防禦**：支援偵測 SYN、ICMP、UDP 攻擊。
- **VPN**：IPSec、PPTP、L2TP VPN、SSL VPN、IP Tunnel。
- **SD WAN**：支援出口線路或 VPN 通道，可以以任意組合綁定，並依照特性分配比重。
- **IP Tunnel**：2 台眾至設備可透過 IP Tunnel 建立 VPN，並針對封包進行管制。
- **Auto VPN**：在大量且動態 IP 位址的 IPSec VPN 情況下，降低設置複雜度與提高穩定度。
- **日誌**：HIGuard XI 包含操作日誌、安裝精靈、系統設定、網路設定、管制條例、管理目標、網路服務、進階防護、IPS、郵件管理、VPN。

網路威脅防護與郵件過濾

- **ClamAV 防毒引擎**：HiGuard XI 支援免費即時更新，病毒資料庫達百萬筆。
- **IPS 防護與特徵資料庫**：HiGuard XI 支援眾至自行維護 IPS 資料庫，依危險程度分高、中、低三種。
- **Sandstorm**：HiGuard 系列支援 Sandstorm IP 阻擋項目。
- **異常 IP 分析**：偵測介面間封包傳遞連線數或上下載流量，可採取記錄、通知、阻擋等動作。
- **郵件過濾與紀錄**：HIGuard XI 支援郵件掃毒功能、SMTP 通聯記錄查詢、病毒信件隔離區、和郵件記錄查詢。

網頁管理

- **TLS 加密協議**：支援 IPv4/v6 TLS v1.3。
- **DPI**：所有流量都會經過 DPI 的分類管理，比傳統 TCP/UDP 埠管制更精確。
- **WEB 服務**：HiGuard XI 支援 HTTPS 掃毒與網站管理、SSL 憑證安裝程式、資訊與匯入、HTTPS proxy 連線紀錄、白名單憑證。
- **URL 管理**：與第三方合作資料庫，支援多達 6 大類的黑名單與惡意網站列表。訂閱授權可享有即時資料庫更新，免費版資料庫則同韌體版本釋出時程更新。
- **應用程式管理**：與第三方合作資料庫，支援多達 17 類的最新應用程式。訂閱授權可享有即時資料庫更新，免費版資料庫則同韌體版本釋出時程更新。

存取認證與流量管理

- **上網認證機制**：支援本機使用者、Radius/POP3/AD 伺服器。可自訂使用者群組，提供認證記錄與連線狀態。
- **兩步驟認證 (2FA)**：整合 Google/Microsoft Authenticator 達成輔助驗證，支援兩步驟認證有三個部分：帳號管理、上網認證、SSL VPN。
- **負載平衡**：監控內送 (Inbound) 和外送 (Outbound) 流量，將每個出口線路都視為一個 WAN 線路，依照權重設定，平均分配網路封包到每一個線路。
- **頻寬管理 QoS**：提供保證頻寬、最大頻寬限制、優先權。

縱深防禦管理

- **交換器協同防禦：**支援一般標準 SNMP 網管型 & 進階協防核心交換器 (交換器拓樸圖)。
  ZYXEL 交換器支援 IP Source Guard (IP+MAC+Port 綁定模式)，可設定 DHCP Snooping 和 PoE 交換器排程。
- **無線 AP 管理：**顯示 AP 狀態與使用人數，可以利用 HiGuard XI 將常用設定檔派送到所管理的無線 AP。
- **內網防護：**支援 ARP 廣播型封包偵測機制、IP & MAC 偽造者偵測、通知紀錄、和封鎖狀態。

中央管理與Dashboard

- **Eye Cloud 雲端管理系統：**可即時監測眾至全系列設備，並延伸監控無線 AP、交換器，分一般、VIP、經銷商三種權限，HiGuard 系列 v9023 版本以上支援派送設定檔 (Config.) 與韌體更新功能，管理者可依據站點為單位，選擇防火牆系列、設備、設定檔或韌體、派送時間，建立派送任務條例。
- **地端 CMS：**HiGuard 系列支援 Client 端定時傳送訊息給 Server 端，設定檔可以被定時自動備份。
- **Dashboard 威脅情報中心：**HiGuard 系列可選購高度圖形化的儀表板，可定期產生各類行報表，包括統計、排行與圖表。

其他

- **運作模式：**Transparent Bridge、Transparent Routing、NAT。
- **操作介面：**自主化管理介面、顯示網路流量與駭客攻防紀錄的Dashboard介面(HiGuard系列需選購Dashboard)。
- **網路檢測工具：**提供Ping、Trace Route、DNS Query、Port Scan、IP Route、Wake Up、SNMP等檢測連線工具。
- **遠端記錄伺服器：**封包通聯記錄可以透過Syslog訊息格式傳送至外部Syslog伺服器，以便資料保存或進階分析。
- **設定精靈(Wizard)：** 協助管理者簡化首次五項設定: LAN、WAN、URL黑名單、防護設定、和郵件管理。
- **分權管理：**依管理權限分為主要管理者(admin)跟次管理者，分Read / Write / All Privileges 三種權限。
- **管理者密碼自訂：**密碼長度限制、字元組合要求、不可沿用舊密碼、變更頻率要求。
- **中斷設定：**支援硬體中斷(CPU)與軟體中斷(ZONE)兩種方式，協助管理者調整系統資源。
- **USB離線特徵碼更新：** HiGuard XI支援項目有IPS、預設APP與URL黑名單、ClamAV防毒、Sandstorm IP。
- **電子白板：**HiGuard XI支援電子白板，以確保公司重要資訊被使用者瀏覽過才可以啟用網頁瀏覽。
- **高可用性：**HiGuard XI 支援 Active-Passive高可用性模式。
- **保固與韌體：**兩年保固服務與韌體免費升級。

HiGuard 技術規格

型號	HIGUARD VI	HIGUARD XI
硬體規格		
建議使用人數	50人以下	50人以下
記憶體 / 儲存空間	4G / 32G	4G / 32G
GE RJ45 網路介面	1 LAN + 3自訂埠	1 LAN + 3自訂埠
USB埠 3.2	2	2
Console (RJ45)	1	1
電源供應與耗瓦	110-240 /12V ; 40W	110-240 /12V ; 40W
燈號顯示	Power/System	Power/System
處理效能		
防火牆效能	1.9 Gbps	1.9 Gbps
最大連線數	200,000	200,000
每秒新連線數	65,000	65,000
掃毒效能	X	800 Mbps
VPN處理效能	380 Mbps	380 Mbps
軟體功能		
設定精靈	O	O
防火牆	O	O
防毒引擎	X	Clam AV
兩步驟驗證	O	O
SD WAN	O	O
頻寬管理與負載平衡	O	O
異常流量分析	O	O
URL管理與資料庫	內建一年	內建一年
APP管理與資料庫	內建一年	內建一年
IPS防禦與資料庫	X	O
WEB服務	X	O
內網防護	O	O
交換器協同防禦	O	O
無線AP管理	50台	50台
高可用性	X	O
電子白板	X	O
威脅情報中心	選購	選購
VPN	IPSec、PPTP、L2TP VPN、SSL VPN、IP Tunnel	
中央管控	Eye Cloud雲端管理系統 & 地端 CMS Client端	