ShareTech INF技術規格

型號	INF-8400H	INF-8600T	INF-8700C	INF-8700F
硬體規格				
機型外觀	1U	1U	1U	1U
記憶體	4G RAM	8G RAM	8G RAM	8G RAM
硬碟	240G SSD	480G SSD	480G SSD	480G SSD
網路介面	6 x Giga Ports	6 x Giga Ports 2 x 10G Fiber Ports	14 x Giga Ports	6 x Giga Ports 8 x 1G Fiber Ports
Watchdog Bypass	O	O	O	O
LAN Bypass	1組	1組	2組	2組
支援架構	Bridge	Bridge	Bridge	Bridge
適用環境	50人以下	100人以下	200-300 人	200-300 人
效能				
防火牆效能	4.2 Gbps	9 Gbps	13 Gbps	13 Gbps
最大連線數	2,000,000	2,000,000	3,000,000	3,000,000
每秒新增連線數	65,000	120,000	350,000	350,000
威脅防護效能 (同時開啟IPS、掃毒、網頁過濾)	900 Mbps	900 Mbps	1,200 Mbps	1,200 Mbps
防毒效能 (雙向)	750 Mbps	1,300 Mbps	1,600 Mbps	1,600 Mbps
IPS防禦效能	600 Mbps	1,000 Mbps	1,200 Mbps	1,200 Mbps
網路安全防護				
病毒引擎	O(ClamAV)	O(ClamAV 與一年卡巴防毒)	O(ClamAV 與一年卡巴防毒)	O(ClamAV 與一年卡巴防毒)
FTP掃毒	O	O	O	O
垃圾郵件過濾	O	O	O	O
郵件稽核過濾	O	O	O	O
IPS入侵偵測	O	O	O	O
WAF	O	O	O	O
Sandstorm惡意偵測過濾	O	O	O	O
應用程式管制	一年授權	一年授權	一年授權	一年授權
URL資料庫	一年授權	一年授權	一年授權	一年授權
異常流量分析	O	O	O	O
交換器協防管理	O	O	O	O
AP無線管控	O	O	O	O
內網防護	O	O	O	O
Geo IP 防禦	O	O	O	O
網路連線測試工具	O	O	O	O
日誌系統	O	O	O	O
頻寬管理QoS	O	O	O	O
特徵碼離線更新	O	O	O	O
威脅情報儀表	選購	O	O	O
UPS不斷線系統	O	O	O	O
雲端管控/CMS管理(Client)	O	O	O	O

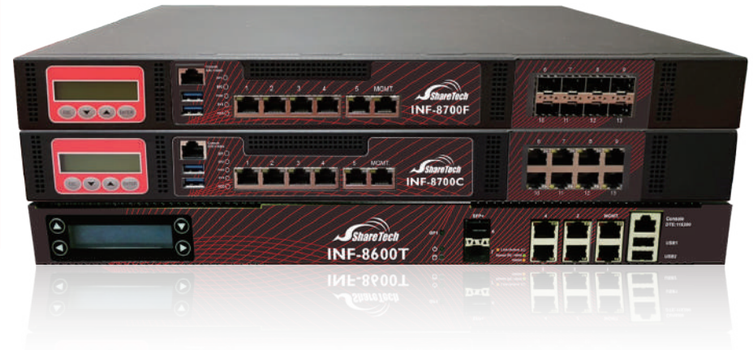
ShareTech 眾至資訊股份有限公司 ShareTech Information Co., LTD.
台中總公司 04-2705-0888 高雄分公司 07-229-8788 sales@sharetech.com.tw www.sharetech.com.tw
台北分公司 02-2501-1185 免付費專線 0800-666-188 help@sharetech.com.tw

2023.04

ShareTech

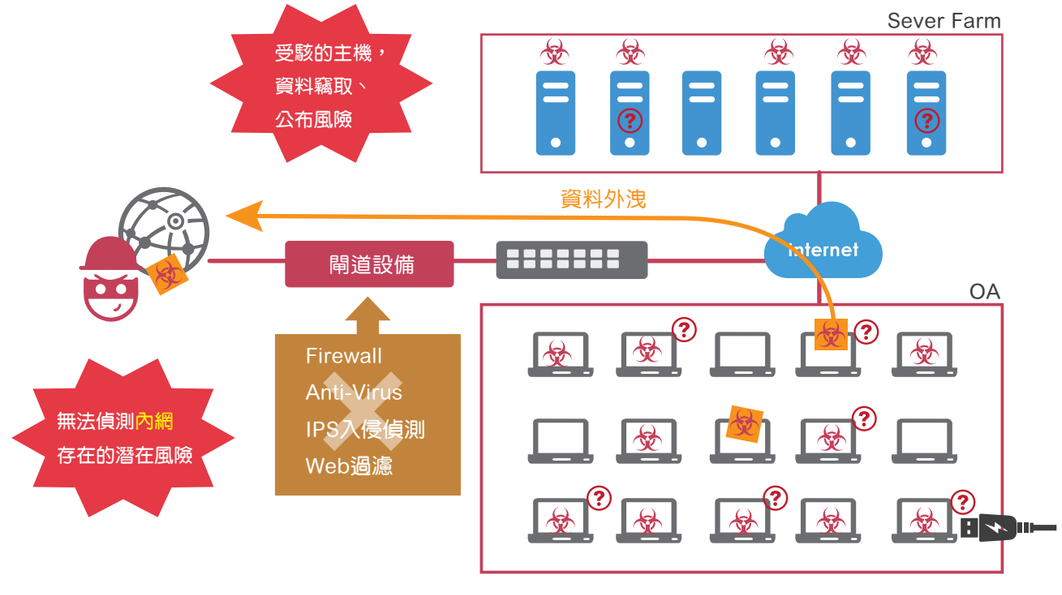
眾至內網防火牆

INF系列



企業內網常遇到風險

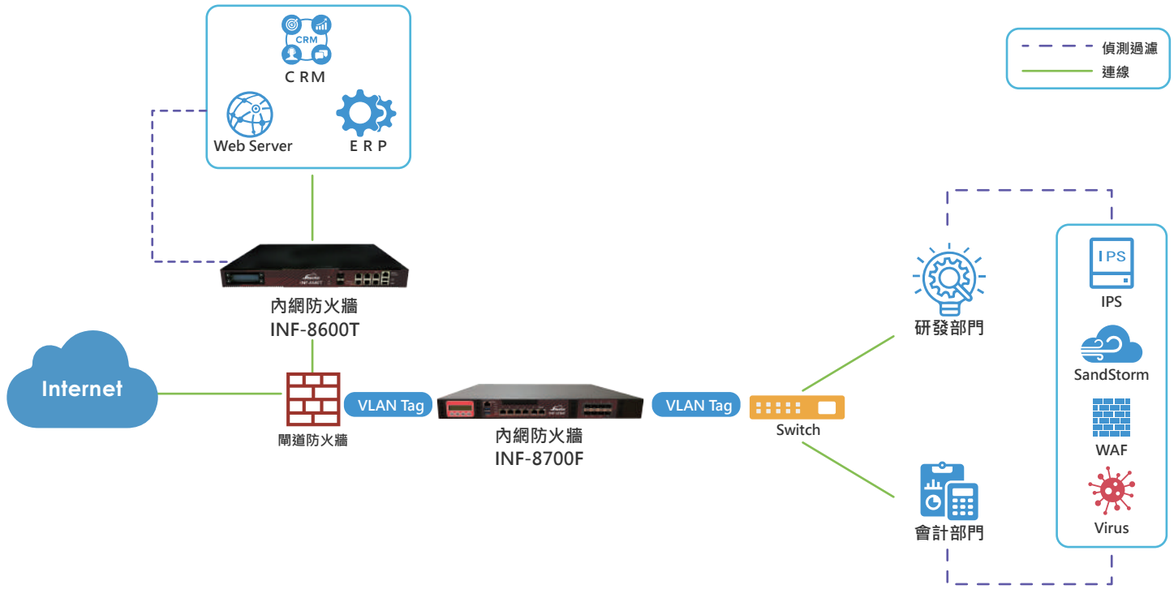
- 無法確保內網100%安全，不會遭到入侵者潛伏滲透。
- 當企業內網遭到潛入攻擊行為，無法有效及時偵測、阻擋與封阻。
- 伺服器系統被植入惡意程式
- 內網未做好區段(Segment)隔離保護
- 無法確保無線上網使用者安全
- 缺乏有效整合相關系統，使其能相互協調、互享情資資訊。
- 針對系統面臨漏洞風險時，不知道該如何進行修補與改善。
- 缺乏可視性情資資訊，提供管理者攻擊分析與相關處置動作。



ShareTech 眾至資訊股份有限公司 ShareTech Information Co., LTD.
台中總公司 04-2705-0888 高雄分公司 07-229-8788 sales@sharetech.com.tw www.sharetech.com.tw
台北分公司 02-2501-1185 免付費專線 0800-666-188 help@sharetech.com.tw

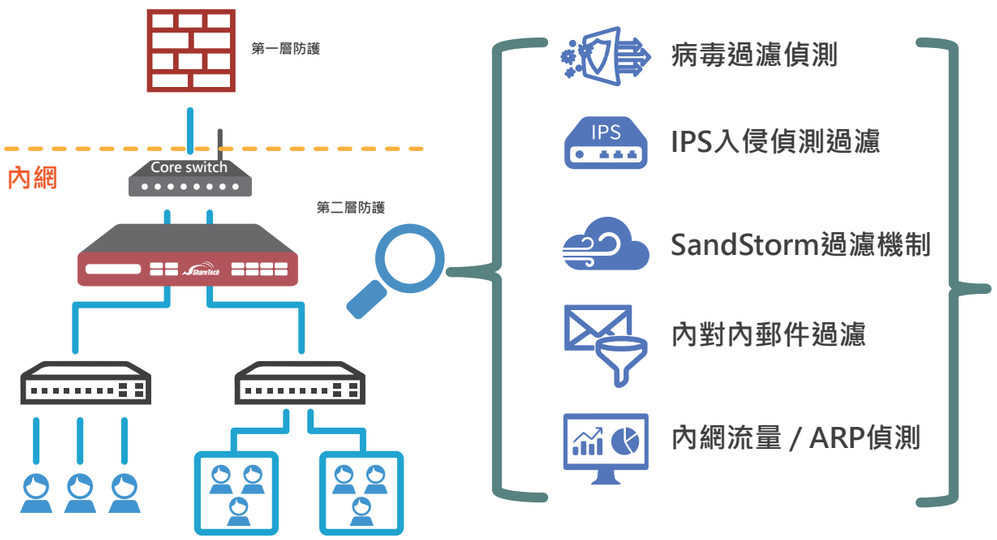
眾至內網防火牆INF系列，降低企業內網資安風險

眾至ShareTech內網防火牆提供安全防護、偵測、情資、回應與協防的組合。它有別於新世代防火牆設計概念，將防護偵測拉至內網體系，提供更高的可視性、可偵測相關聯的威脅攻擊，同時採用智能協防和示警功能來幫助偵測可疑的事件。



特點一：降低內網遭受零時差攻擊機會

眾至內網防火牆主要在於偵測內部網路是否有異常行為及主動阻斷攻擊的來源。大部分的網通設備都只能在閘道端在封包經過設備狀況下進行偵測、分析與隔離措施，但是對於網路內部的感染或攻擊行動，這些資安設備就無法做有效的阻嚇。眾至內網防火牆透過內建病毒過濾、IPS偵測、WAF與Sandstorm過濾，除了警戒監測異常連線行為外，還肩負過濾病毒活動與降低駭客攻擊。



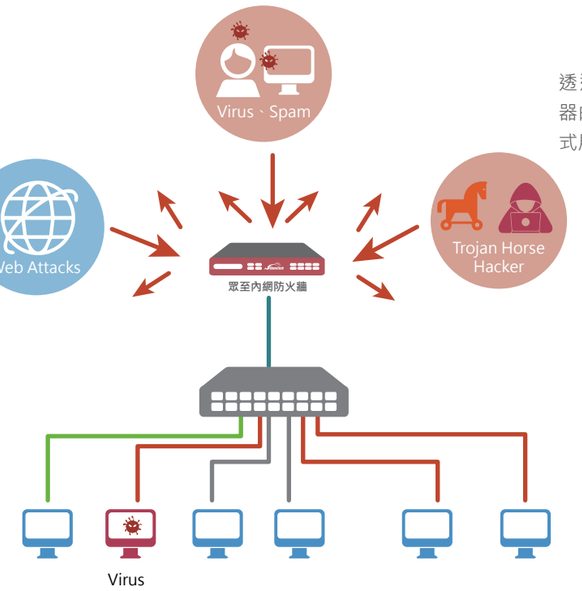
特點二：保護重要伺服器與主機

眾至內網防火牆INF系列具備針對各類 Web 應用攻擊的檢測和防禦能力，如蠕蟲威脅、駭客攻擊、SQL 注入、跨網站攻擊等，滿足對檢測、防禦能力在廣度和深度上的要求。內建「WAF網頁應用防護」，用來加強原本防火牆對網站防護的不足之處；WAF是針對Layer 7層級的封包內容進行過濾判斷，若為合法的連線即允許連入，可疑的連線就會在此被拒絕。

特點三、與交換器協防，一起守護內網安全

一旦偵測到受保護的區段內有任何異常的行為，並被判斷為感染或攻擊行為時，透過眾至內網防火牆將感染源或有攻擊者的所有封包主動阻斷或隔離。此外，進階結合交換器，IT管理者可以透過網路拓樸圖，瞭解交換器架構的布建與各節點的使用狀況，同時取得資料進行儀表分析，讓IT透過視覺化的管理，進一步偵測與判斷惡意的滲透攻擊行為。

當內網防火牆偵測到風險時，透過與交換器設備聯防機制來手動或自動屏蔽，在第一時間降低內網攻擊威脅。



透過交換器拓樸圖將每一個交換器的Uplink跟Downlink以分層方式展示出，利於網管人員管。

特點四：掌握最完整情資全貌

眾至內網防火牆內建Dashboard威脅情報儀表，是為內網安全專門設計，能提供有用的資訊，讓設備裡面的紀錄與事件資料，能夠簡化並集中進行分析、彙整、儲存、查詢與報表製作。透過眾至Dashboard，管理者可以為強化安全來檢視、搜尋所有流量，並透過事件關聯定義可能的風險來源或可疑的活動。

威脅情報分析儀表(Dashboard)特點：

- 威脅情報統計
- 網路流量分析
- 整合Syslog、Flow與威脅儀表
- 強化事件關聯
- Log稽核與查詢
- 豐富的報表分析