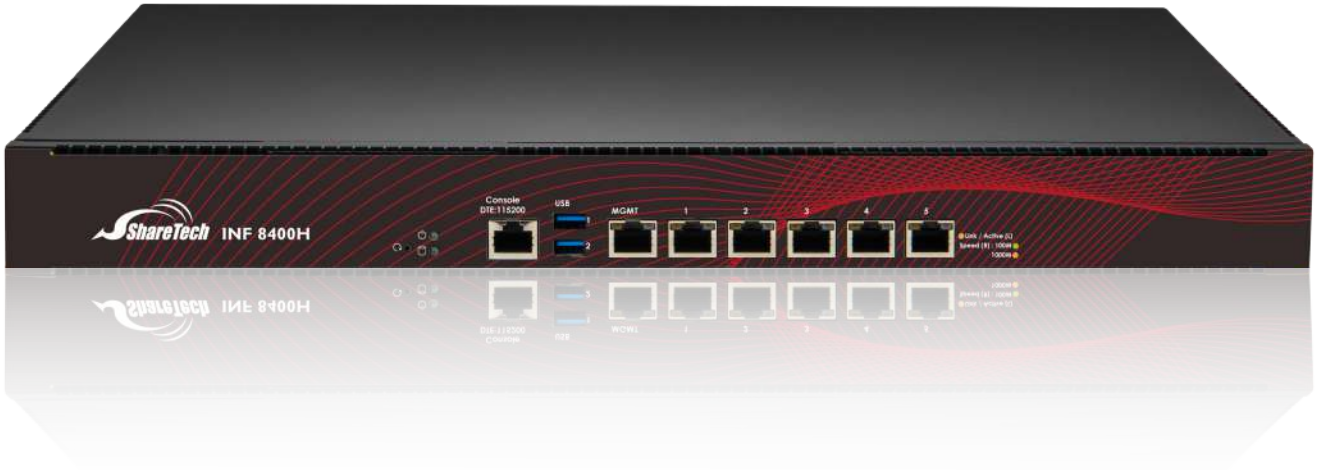
眾至內網防火牆
INF-8400H



這幾年受到疫情影響，各方對於網路運用需求日益增長，於是駭客們有了更多機會針對各式議題製作釣魚信件或惡意網址，以此來獲取使用者帳密並入侵到組織內部網路後等待時機竊取機密資料。隨著網路資安事件激增，對外部入侵或安全防護日益重視，卻似乎沒有注意到來自於內部的網路攻擊正逐漸升溫，因此現在內網安全成了營運上最重要的話題。多數機關單位對於資安防護都有基本認知，也有相關防護建置，透過防火牆或UTM作為閘道端口防護，利用IPS入侵偵測、防毒(Anti-Virus)、垃圾郵件過濾(Anti-Spam)、Sandstorm等功能抵禦來自外部的攻擊。然而值得注意的是攻擊的戰場已經轉變，駭客的攻擊途徑除了從外部，來自內網的威脅也日趨漸增。

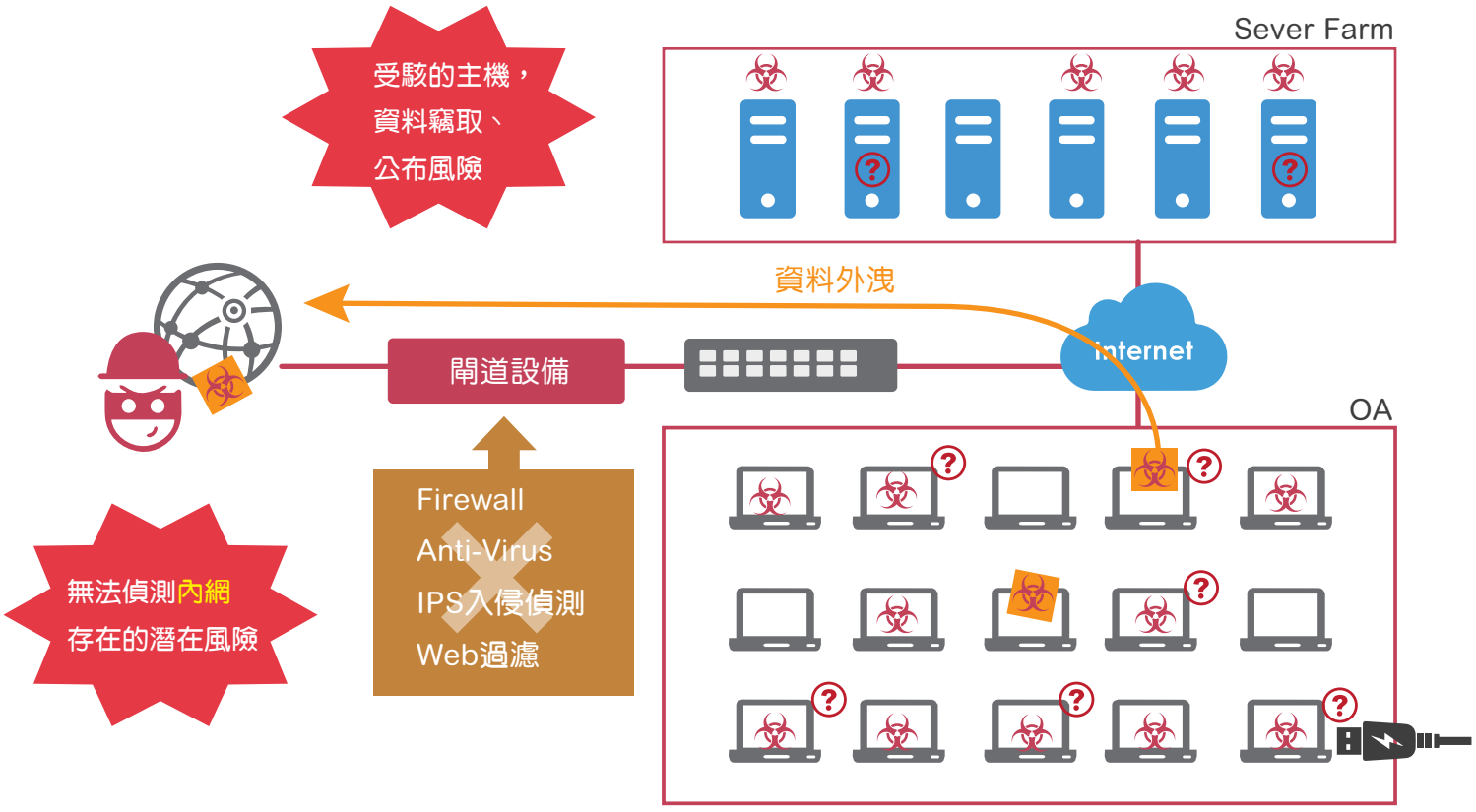


圖1：針對性的攻擊避開閘道偵測，為內網安全帶來風險。

內網面臨的安全威脅

1.伺服器系統被植入惡意程式

駭客利用網頁應用程式或公開網路伺服器上的安全漏洞在伺服器上植入惡意程式，當瀏覽人數越多、網站流量越大時，其惡意程式散播的速度也越快。

2.網路資源濫用

當網路IP位址配發不受管制、流量使用無限制時，不僅員工在工作時間聊天、看股票、玩遊戲、下載影片、瀏覽色情網站等影響工作效率，也衝擊內部網路正常使用。

3.病毒蠕蟲入侵

蠕蟲病毒攻擊模式多樣化，如：在區域內網利用感染的USB、壓縮文件、網頁目錄傳播，引起病毒蠕蟲氾濫、資料受損、網路流量異常塞車等問題，當安全措施不足的機關單位內網受到強大衝擊卻無法找到災難源頭並採取有效的處置行為時，將會帶來營運上的重大損失。

4.內網未作區段(Segment)隔離

當員工使用未經授權的個人電子產品連接到公司網路或在少許限制下存取資料的工作站時，若駭客入侵並取得控制權後，便可輕易地找到內網中有利用價值的區塊，因為多數機關單位內網並不會做區段(Segment)的隔離，一旦被滲透，門戶幾乎暢通無阻。

5.使用者不遵守資安規範

用戶中常有使用者私自接無線路由器或利用個人4G/5G無線分享方式，讓原本不允許的設備裝置連網。這樣的方式為內網帶來巨大的潛在威脅，駭客可以很輕鬆繞過閘道防火牆並悄悄地入侵，不僅重要資料可能被竊取，內網也會受病毒傳播影響而癱瘓。

6.遠端連線風險

受到疫情的影響，遠距辦公漸成為辦公常態。若要讓員工在家辦公也能與在公司上班維持相同作業方式，最簡單的方式就是利用Windows內建的遠端桌面程式，或透過TeamViewer這類軟體進行作業，但在這樣的運作下，駭客很容易透過網路掃描，找到開放的網路埠，也能利用暴力破解、帳號填充方式滲透到內網。

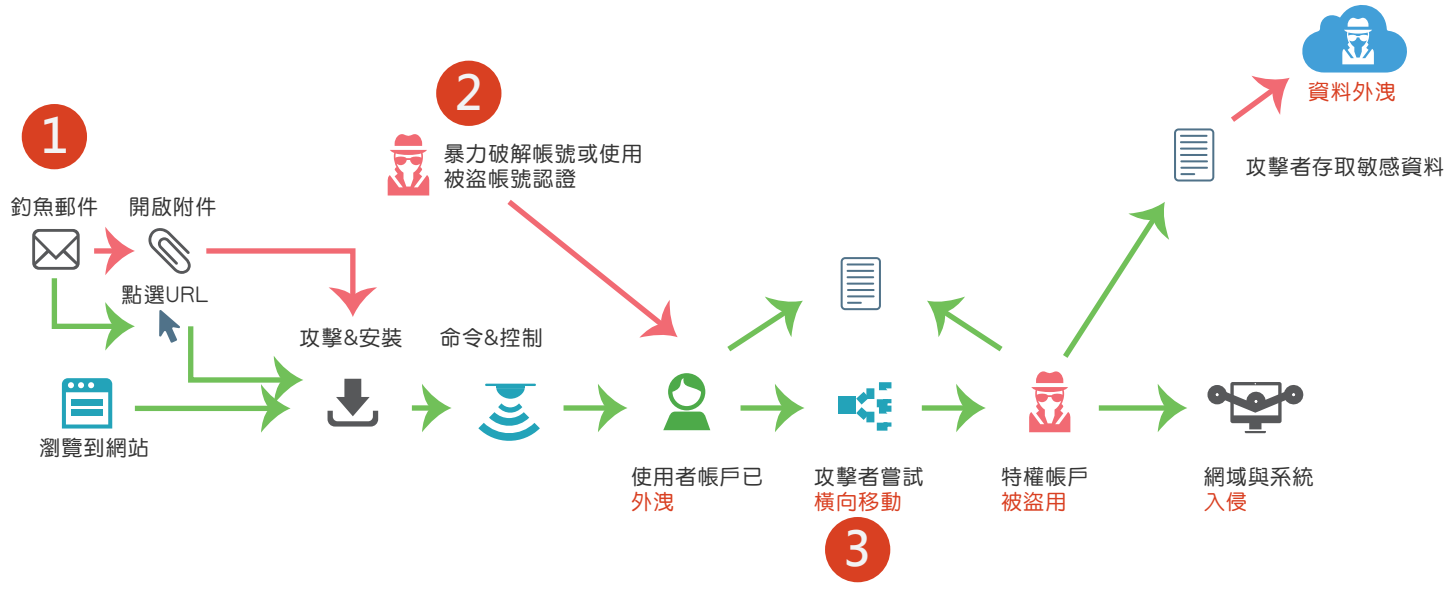


圖2：惡意攻擊者透過釣魚郵件、惡意網頁，滲透進入用戶內網

內網安全需要「內網防火牆」

內網安全是網路架構最貼近使用者，但也是最缺乏防護的一環。從網路邊界來看，如果完全沒有任何防護措施，僅僅在網路閘道口放置資安設備，就像社區大樓守衛面對進進出出的人員，如果疏忽錯放一位有風險的人員入內，當他做了非法或惡意行為時，可能就會造成社區永久的傷害。

有鑑於越來越多資安事件發生原因來自於內部網路的脆弱區段，因此原本信賴的內網也必須改以Zero Trust(零信任)來處理。第一層閘道端口防火牆的部署已經不足，只能阻絕來自外部(Internet)的病毒或攻擊，卻無法有效的過濾或阻隔經行動裝置、訪客或隨著無線區域網路、VPN、IM應用程式及郵件使用下所造成的內部網路漏洞及威脅，因此必須重新架構網路，以第二層防護、區塊防護來強化內部同區段、不同組織、不同部門之間惡意流量的傳播風險。

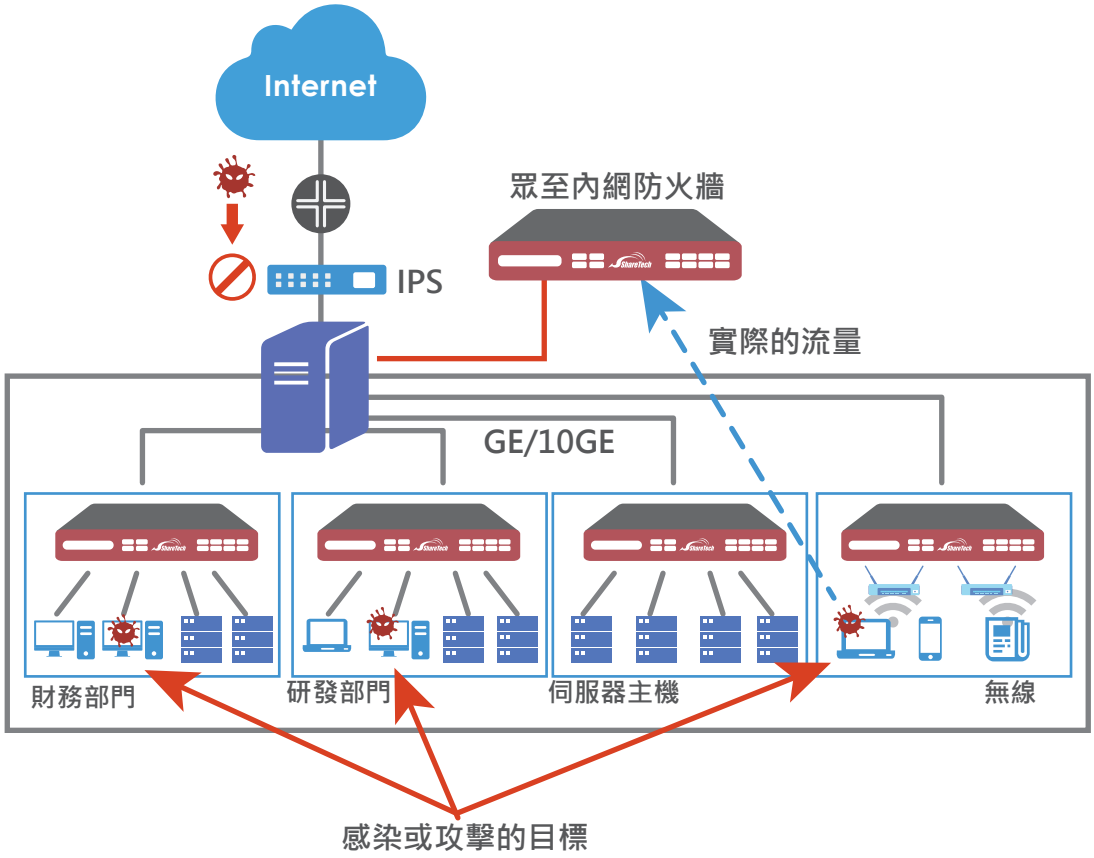


圖3：內網需以Zero Trust來處理，才能降低重要部門或主機被感染機會

考量機關單位可能因為經費及效能考量可以採取局部性的建置，保護的對象以關鍵組織部門、重要主機群或內網區段為主，在此架構下管理者需思考：

- 如何快速隔離感染源：所有的流量傳遞是否都會經過檢查(例如：病毒、IPS、Sandstorm機制偵測)。
- 適當管理政策：在不影響既有的網路架構下，讓所有流量的封包檢測能更深入檢析。
- 當遭受攻擊時如何緊急應變：如何有效主動隔離攻擊來源，確保網路運作安全。
- 交換器、AP互補協防：利用威脅情報相互協防，可以在發現受感染的使用者前，先做好智能管理將受駭者先隔離。
- 降低效能影響：現有多數機關單位內網大多為高速乙太網路環境(GB)甚至是10GB骨幹，在提高內網安全同時，是否真的能不影響目前使用者傳輸速度。
- 在封閉網路環境下，如何確保特徵值(Signatures)也能隨時提供最新資料庫服務。

眾至內部網路安全解決方案

1.降低對效能與投入成本憂慮

過往不考慮在每個網路區段前建置第二層防護關卡的考量點有二：沒有足夠預算且內網的流量遠超過網際網路流量，若將防火牆設備放到內網，當啟動所有偵測服務機制時，可能無法處理如此龐大的流量。這些問題隨著技術增進、硬體規格大幅提升，眾至內網防火牆INF-8400H利用CPU多核分工處理、SSD優化硬碟IO處理效能等，內網防火牆便可以有足夠的運行速度。

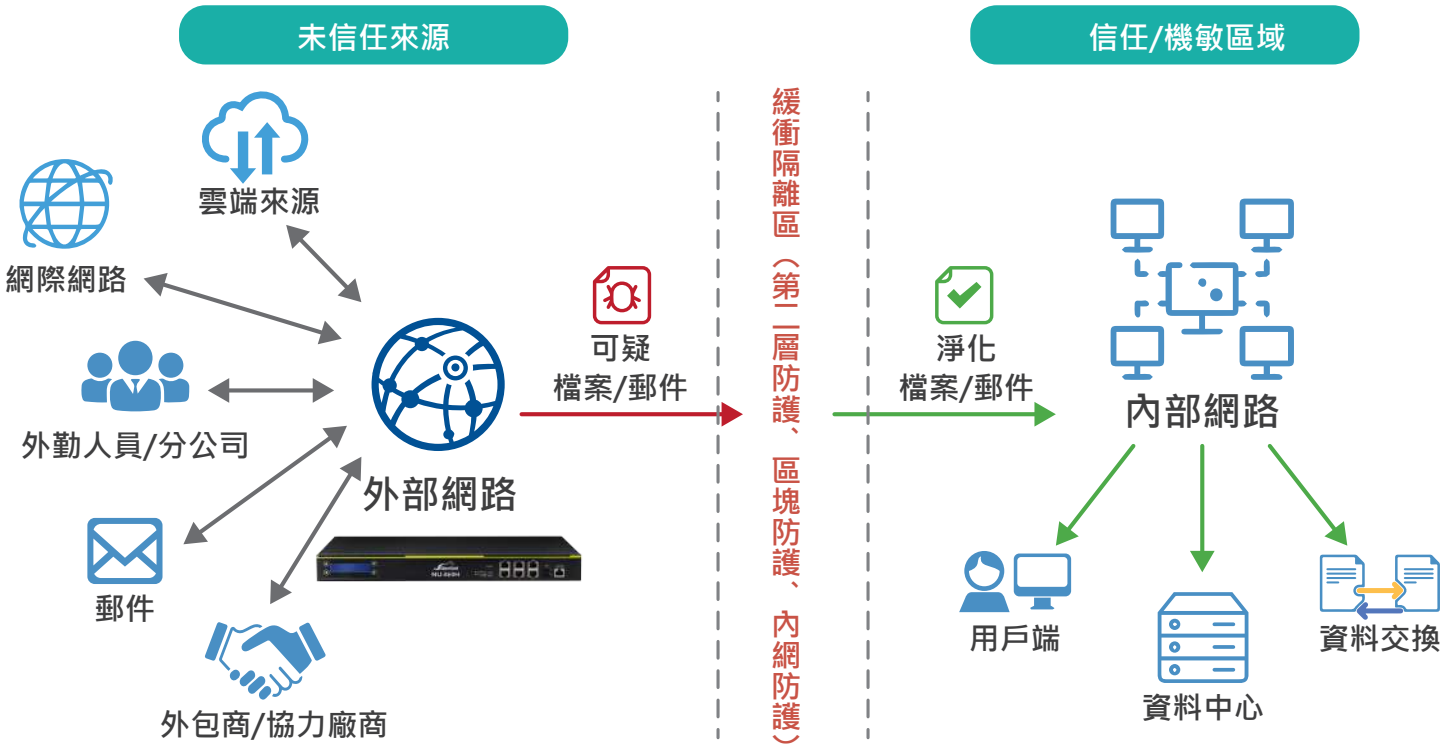


圖4：第二層防護(內網防護)機制，提升內網運作安全性

2.僅支援Bridge運作架構

INF-8400H僅支援透通橋接模式，這對多數不想改變既有架構用戶是最理想的選擇，並保護其端口之間的數據交換，過濾WAN和LAN之間的數據封包。

常見的網路架構，內部網路為了方便管控都會藉由切割VLAN，來做相關的管制。因此，VLAN的分割數量少則數個多則數十數百都有可能。針對此運用環境，眾至內網防火牆INF-8400H可對VLAN Tag封包做解析，並且無須額外設定VLAN Tag的ID，即可串在交換器中間過濾解析封包內容。

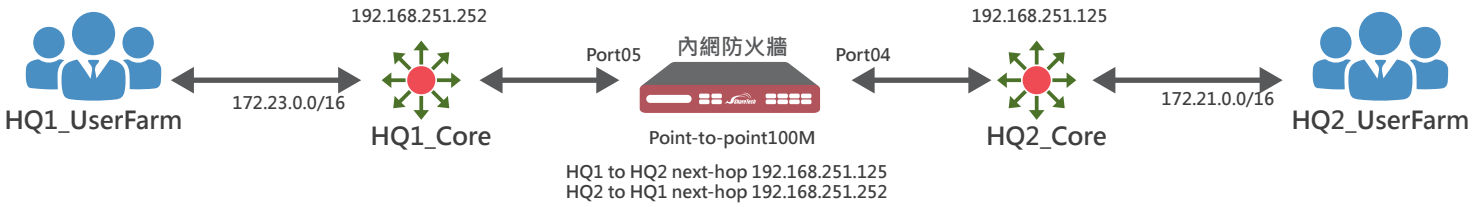


圖5：眾至內網防火牆僅支援透通運作模式

3.內網流量進行Virus、IPS、Sandstorm過濾

INF-8400H主要偵測內部網路是否有異常行為及主動阻斷攻擊的來源，具有病毒過濾、IPS偵測與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。

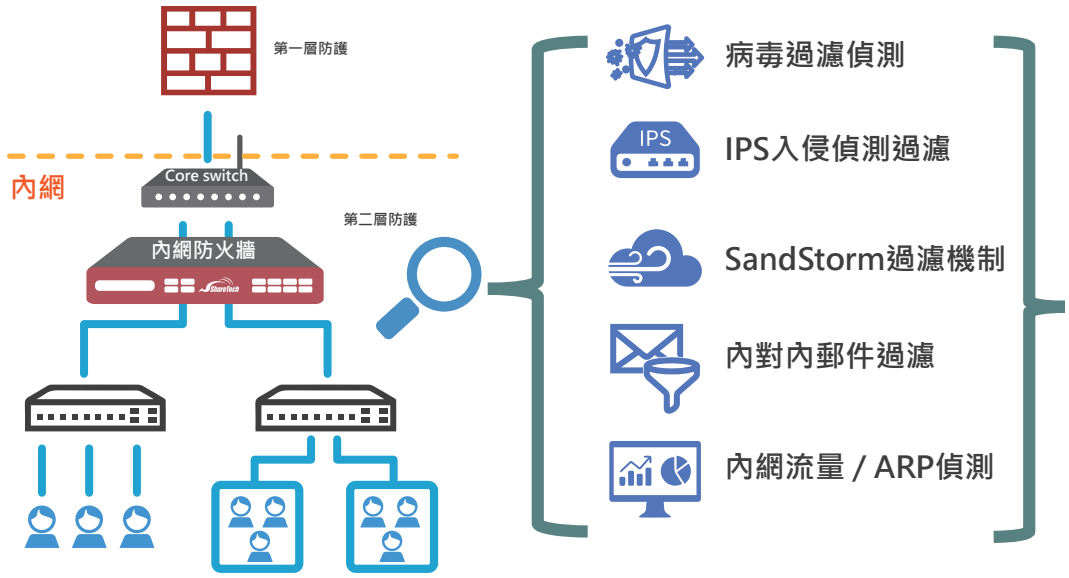


圖6：眾至內網防火牆提供多層過濾防護機制

4.交換器協防，一起守護內網安全

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，進一步偵測與判斷惡意的滲透攻擊行為。如果端點裝置被植入惡意程式或中毒，會透過內網滲透，擷取未被授權的資源或訊息，這些異常的行為會被INF-8400H所偵測並發揮即時封阻效用，將未知的風險優先隔離或封鎖該使用者的IP與MAC。

萬一內部使用者遭到ARP攻擊或被偽裝IP位址，INF-8400H與交換器協同防禦功能將攻擊者封阻在境外，藉由此防禦機制，還可記錄攻擊者的 IP位址、MAC 位址及時間，快速揪出網路中的害群之馬。

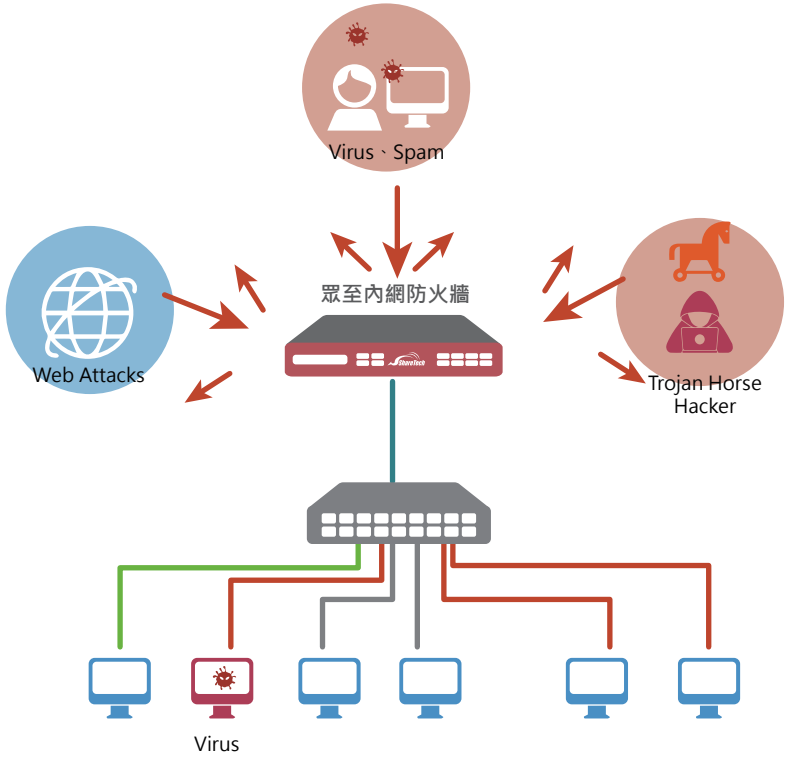


圖7：透過與交換器設備聯防降低內網攻擊威脅

整合AP與交換器後，當有流量（如異常的流量與Session、IPS）觸發內網防火牆INF-8400H的條件時，系統會主動通知交換器並關閉異常的網路孔，將災害封鎖至最小。

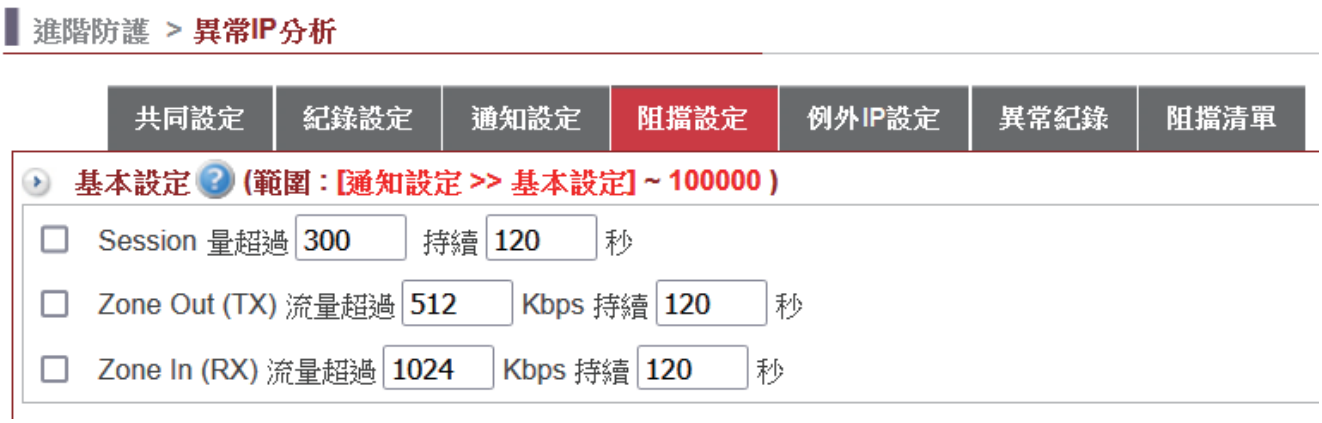


圖8：眾至內網防火牆可針對異常流量進行阻擋

5.強化內網無線上網安全

結合內建的認證機制，所有經由無線連線的封包亦會經過病毒特徵檢測、IPS入侵偵測、Sandstorm偵測過濾，不需要再另尋其他無線網安解決方案，即可落實有線與無線網路的整合控管與資安防禦。

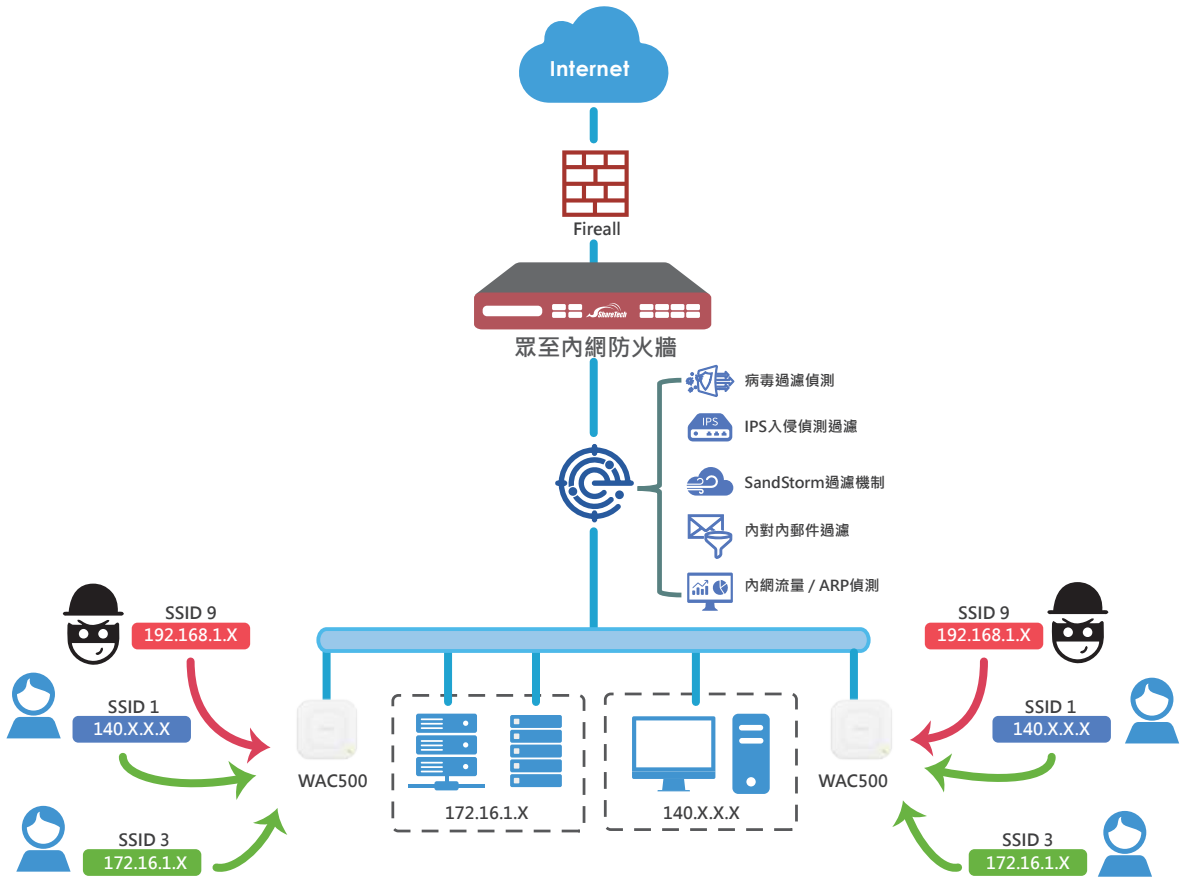


圖9：內網有線、無線安全一併管控、協防

6.Geo IP Detection

具備以國家別或地域名稱來制定流量過濾、阻擋政策功能(Location / GeoIP / Geography)，允許管理者可以以國家別或地域名稱來制定流量過濾、阻擋政策功能，可主動過濾大量或大範圍的異常國際網路連線(例如：北韓、菲律賓)。

7.內網流量頻寬管理QoS

除了提供最大頻寬、優先順序管理之外，還能夠保證頻寬功能。若將頻寬管理針對個人化頻寬管理使用時，可將頻寬管理功能所預留的頻寬，再分配給內網的其他使用者，可有效防範頻寬獨占現象。協助網管人員控管內部網路流量，有效減緩機關單位網路的阻塞、提升服務性與頻寬使用率。

8.視覺化Dashboard威脅儀表板(選購)

眾至瞭解Log保存對機關單位的重要性，所以INF-8400H支援CEF標準事件格式，管理者可以更方便管理與備份所有設備Log，必要時可以藉由像Graylog、LogServer進行資料查詢，此外，INF-8400H可選購視覺化Dashboard威脅儀表板。

▪ 威脅情報統計

統計多種風險威脅，包含病毒攻擊、垃圾郵件攻擊、IPS入侵偵測、DOS攻擊、URL管制風險與應用程式管制風險。

▪ 網路流量分析

擷取所有流經網路交換器的所有封包，容許管理者為強化安全來檢視、搜尋所有流量。包括HTTP、SSL/TLS、HTTP、Unknown等相關流量。

▪ 整合Syslog、Flow與威脅儀表

使用者不需要再額外採購流量分析與日誌軟體，透由統一監控畫面讓管理者可以一目了然完整監控。

▪ 強化事件關聯

事件關聯報告能針對內網防火牆INF-8400H所蒐集的風險數據、流量分析、連線狀態，定義可能的病毒或使用者可疑活動。

▪ Log稽核與查詢

管理者能依使用者IP、名稱和應用程式追蹤網路活動，建立更多詳細辨識的分析報告。

▪ 豐富的報表分析

管理者可以自訂TOP N報表，包含設備狀態、流量分析、郵件分析、入侵防護分析、網頁分析、防護分析、應用程式管制分析、Web Control分析、IP地區、DNS查詢與威脅情報。報表類型可以天、周、月、季類型呈現。

9.支援CMS管理功能與雲端管理平台(Eye Cloud)

為了便利管理多台內網防火牆，除了可以透過內建CMS管理外，亦可透過ShareTech雲端管控平臺 (Eye Cloud Management System) ，IT管理員只要登入雲管理平臺，可統一監看所有內網防火牆，包含內部的無線基地台跟交換器的即時狀況。

◆中央管控設備可以管理不同的佈署，提供了完整檢視及控制遠端設備的功能。

◆雲偵測系統，可偵測web、smtp相關服務，當發生異常狀況時可透由line或郵件通知。

◆提供防護排行相關資訊

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	480G 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	X	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	4.2Gbps	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)	550 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				
閘道防護	O	O(內建一年防毒)	O(內建一年防毒)	O(內建一年防毒)
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	O	O	O	O
URL資料庫	O	O	O	O
異常流量分析	O	O	O	O
交換器協防管理	O	O	O	O
內網防護	O	O	O	O
AP無線管控	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
威脅情報儀表	選購	O	O	O
UPS不斷電系統	O	O	O	O
雲端管控/CMS管理(Client)	O	O	O	O

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