AW-570 UTM 設備

AW-570 是全世界第一台『多功能 UTM』，它除了一般 UTM 具備的功能外，又增加了入侵防禦 IDP、SSL VPN、Smart QOS、流量分析等獨特功能，一台設備搞定網路上所有的大小事。

幾年前的調查指出，Anti-Spam 和 Anti-Virus 是企業界最頭痛的資訊安全議題之一，病毒透過電子郵件的散播，又快又狠，讓使用者防不勝防，往往不知不覺中又當了散播病毒的幫兇。事實上網路駭客跟病毒的界線已經非常模糊，他們的目的及動機，眾說紛紜，讓人防不勝防，買了許多的資安設備，漏洞依然存在。

有鑑於此，眾至資訊結合過去在防火牆開發的經驗，推出 AW-570，期望改善使用者的困惱，並增加管理網路的方便性。

將 AW-570 架設於企業的網際網路入口處，把所有擾人的病毒及駭客，一次阻擋掉。再加上『即時流量的分析』技術，找出潛伏在內部的問題。AW-570 同時整合 Load Balance、Botnet、VPN、異常流量分析、內容過濾、URL 網頁控管與協同防禦，讓您毫無後顧之憂地捍衛網路安全。

(一) 功能特色

防火牆

AW-570 內建 SPI 技術，主動攔截、阻擋駭客攻擊，不論是 SYN、ICMP、UDP 等攻擊方式都可以阻擋。眾至資訊主要是套用合理流量的觀念，認為每個來源不會同時產生太多封包，萬一超過設定的合理封包數時，防火牆會要求將多餘的封包阻擋

物件管理技術

為了增加 AW-570 的管理便利，ShareTech 大量採用物件的觀念，任何 TCP/IP 上的管制項目都可以事先定義成一個物件，單一個內、外部 IP 位址、PORT、時間、頻寬、應用程式可以組合成物件，數個內、外部 IP 位址、Port 、應用程式也可以組合成物件。

定義每個物件後，搭配管制條例的運作，讓符合物件的網路封包允許或是拒絕通過 AW-570，降低管理的複雜度，日後管理人員要變更管理的物件，只要到定義物件的地方改變，管制條例會自動更新修改後的物件，並讓它生效執行。

IP V4 / V6 雙頻技術

IP V4 位址短缺，IP V6 的年代遲早到來，所以 ShareTech 在研發下一代 UTM 時就已經將這個趨勢整合起來，同一個網路接口，不管它被定義成 WAN 或是 LAN，都可以同時綁定 V4 或 V6 的 IP 地址，所以不管是在純 V4 的環境、V4/V6 混合、純 V6 的環境，AW-570 都一樣合用。

HTTP、FTP、MAIL 的防毒機制

病毒無孔不入，除了教育使用者不要開啟來路不明的網站、檔案外，在網路的大門口將這些有潛在威脅的網站、電子郵件、FTP ，就將它阻擋，也是一個降低風險的好方法。

防火牆內建 ClamAV 免費防毒引擎，每日自動地從網路上更新病毒碼，提供給不同的網路服務使用，藉以提高網路的性能及安全性。為了將 HTTP 掃毒時降低對使用者的效能影響，AW-570 藉由改寫 HTTP 代理軟件的軟體，自動排除不需要進入掃毒引擎的 HTTP Stream，只將可能會受病毒影響的封包導入，而不是將所有 80 Port 的網路封包導入，並且會紀錄每個網頁的掃毒狀況。

SMTP 跟 POP3 的部分也是使用 Transparent Proxy 的方式將封包導入掃毒引擎中，再將乾淨的信件內容傳給使用者，對於有病毒疑慮的郵件，管理者可以自行決定要隔離、刪除郵件。同樣的，系統會紀錄每一封信的掃毒狀況給管理者參考。

IDP 入侵防禦

IDP 它會檢查對應到 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，透過詳細的內容檢查後，符合條件的特徵碼就會被標示出來，一但發現後能夠即時地將封包阻止，讓這些穿過防火牆的惡意封包無所遁形。

一般而言，IDP 的特徵值資料庫會依照危險程度分成高、中、低三種，再讓管理者決定放行或阻擋，考量客戶端的實際網路環境及機器的運算能力，在中小型的網路架構的 IDP 設備只需要有完整的危險程度高、中 (例如，病毒、木馬程式) 的特徵值資料庫就足夠，其他屬於警告或通知性質的檢查沒必要處理。

垃圾郵件過濾

垃圾郵件氾濫，讓所有的人都痛苦，AW-570 提供優秀的防護機制，確保使用者的信件乾乾淨淨，除了傳統的垃圾郵件特徵值、貝氏過濾法外，針對圖型式垃圾郵件更加上特殊的判斷機制，增加判斷的準確度。

個人或是群體的黑、白名單匯入、匯出及自動學習機制更是少不了的基本功能，將判斷的準確率提高到 95%以上。

被判斷成垃圾信件時可以做 3 種處理，「主旨加上特定文字然後傳給收件者」、「直接刪除」、「在隔離區並定時寄垃圾郵件清單給收信者」，收信者收到清單之後，可以查看信件標題，再決定要不要下載被誤判的信件。

Smart QoS 超乎你想像的頻寬管理

頻寬管理在目前的網路設備中非常常見，但是管理的好不好、準不準確有賴管理者的經驗，回到基本的問題上，為何要管理頻寬？因為頻寬不足或是公平的原則，不論是哪一種，如果買了 10Mbps 的頻寬，因為管制的機制問題，讓整體的使用量只有 2 Mbps，剩下沒使用的豈不是浪費，如果將這些頻寬適當地分配給目前正在使用的人員，就皆大歡喜。

頻寬是給有需要的人使用，基於這個原則，啟動【Smart QoS】後，UTM 會自動檢查剩餘頻寬，並將它分配給目前正在使用的人。

傳統的 QoS 都只能管理介面往外送的流量，AW-570 使用 IMQ 機制，藉由這項技術就可以管理每一個網路介面內送、外送的頻寬。當有狀況發生時，這個機制會保護設備的運作，例如：網路內部有人對外狂發封包，導致 UTM 不堪負荷，反而讓正常的封包無法運作，限制 LAN 收下網路流量的機制，就會讓設備不被攻垮。

Outbound Load Balance 對外負載平衡

AW-570 提供 2WAN ports 作多種負載平衡演算法則，當其中一條線路斷線之後，所有的網路封包會自動轉向另一條正常的線路，確保內部的用戶網路暢通，當線路恢復之後，封包又會自動分配。企業可依需求自行設定負載平衡規則，而網路存取可參照所設定的規則，執行網路流量負載平衡導引。演算法則有：自動分配、手動分配、依來源 IP 分配、依目的 IP 分配

Inbound Load Balance 對內負載平衡

AW-570 內建 Smart DNS Server，可以讓電子商務業者透過多條 ISP 線路，提供使用者更即時、快速與穩定不斷線的網際網路線上服務。

內網防護 (ARP 防偽)

對 UTM 而言，最難偵測到的攻擊類型就是廣播型的封包，如 ARP 欺騙、私架 DHCP 伺服器等，因為通訊協定的先天性缺陷，導致這一類的攻擊行為很難被偵測出來，眾至 AW-570 的 ARP 偵測機制，可以在第一時間內就找到『濫發佈』 ARP 訊息的人。另外，也可搭配協同防禦交換器的設備，可以標示出這個 IP 的實體位置，讓他無所遁形用。

異常 IP 分析

任何網路行為，不論使用者執行哪一種軟體，從網路封包的角度，大致分成上傳、下載的連線數量 (Connect Seesion)、流量 (Flow) 跟持續時間 (Time)，藉由偵測這些數量的組合，推估使用者是正常使用網路或是有異常的行為。當發現內部使用者異常行為後，管理者可以採取多種策略，例如，阻擋上網、立即限制他的最大頻寬、啟用協同防禦機制通知交換器將他封鎖或是通知管理者就好。

協同防禦 (搭配 SNMP 交換器)

協同防禦屬於 UTM 的進階防護，透過異常 IP 分析、交換器 (Switch)，即時監控內部機器的分部狀況，當內部網路發出大量異常封包時，阻擋這些封包的傳送，並協助管理人員盡速排除異常狀態，可以在事件發生的第一時間內知道哪一個電腦在哪一個交換器 PORT 上，避免企業網路癱瘓。眾至 AW-570 同防禦機制，不需要改變網路架構，不需要更昂貴的專門 Switch (具備 Layer 2 就可以)、不需要增加任何額外的偵測設備、不用改變每一個使用者的網路習慣，讓網路管理的動作變得簡單、直覺。

BotNet 協同防禦

ShareTech 的 UTM 兼具 BotNet 功能，因為本身兼具 NAT 的功能，當內部的使用者利用郵件伺服器寄出垃圾信件或是直接對外，UTM with BotNet 的偵測設備都可以明確地指出，哪一台才是真正的攻擊來源，也才有辦法將有危害的網路封包直接封鎖。萬一，UTM 的 BotNet 阻擋事件發生後，特定電腦仍然持續的對外攻擊，為確保 UTM 的 CPU 資源不會被浪費在同一件事情上，管理者可以啟用 BotNet 的協同防禦機制，將有問題的電腦 Switch Port 直接關閉，不僅可以節省 UTM 的資源，也確保內部網路不會被這個殭屍病毒持續危害。

IP/MAC/Port 互鎖

在某些敏感度比較高的網路環境，例如軍方、政府單位、研究機構等，不希望使用者任意地更換 Switch 的實體位置，以下面的使用者 A(IP:192.168.100.5，MAC:05:51:62:53:02:03)為範例，透過 AW-570 可以將它定位在 Switch 第 3Port 孔，如果他換到任何 Switch 的不同孔位，設備就會不通。

認證 Authentication

提供本機使用者/AD/POP3 認證授權機制，可協助網管人員與監控企業內部所有使用者帳號，在確認使用者的 ID 的有效授權之後，才能允許其使用網路，讓企業可以有效管理網路使用資源。

內容過濾

提供 Web Filter(網頁過濾)功能，能阻擋工作端存取不當網頁(如色情、暴力)和攻擊性網頁(如駭客、病毒)，且能自設過濾條件，阻擋不當網站。

URL 資料庫管理

AW-570 內建「雲端 URL 資料庫」，自動將網頁分類，管理者只要針對有害的 URL 網進行防堵，可以輕鬆管制，不需要再逐一輸入網站 IP 位址、關鍵字…來阻擋。任意點選有害的 URL 網址是罪惡的淵源，最好的防堵方式是禁止使用網路，如果無法全面禁止，使用時時更新的 URL 資料庫就是最好的防護機制。

DNS 伺服器

UTM 內建 DNS 伺服器，將煩人的 A RECORD、MX 等設定，通通交給內部的 DNS 伺服器，DNS 不僅可以支援 IPV4 的名稱解析，連 IPV6 的部分也一併搞好，進階的部分更可以做到相同的網域名稱不同的 IP 位址回應及 InBound 負載平衡。

IPSec、PPTP VPN 連接及管制

UTM 採用的 IPSec 軟體，完全遵照 IPSec 的標準定義，確保跟其他支持 IPSec 協定的設備互聯互通，目前支援手工密鑰交換方式(PreShare Key)，同時支援 DES、3DES、AES、Blowfish、Twofish 等多種加密演算法及 MD5、SHA 等認證算法。

PPTP VPN 遵循 RFC 相關標準要求，支援 MS-CHAP 和 MS-CHAP V2 身分認證及 MPPE 加密演算法。

對於所有透過 VPN 通道進入內部或是要從內部到 VPN 遠端的所有封包，利用特有的管制條例機制，管理封包進出的時間、頻寬、通訊服務等，這個機制確保內部不會因為遠端 VPN 的連接，而感染網路病毒或是占據所有的頻寬。

SSL VPN 連接及管制

SSL VPN 是一種具有安全加密保護的虛擬私人網路技術，可以讓使用者在外地使用電腦的時候，就像是在區域網路裡面使用電腦一樣，可以使用任何只有在區域網路內才能使用的資源，如 ERP、進銷存或是限定來源 IP 位址的圖書查詢系統，又因為將資料加密，所以在網際網路上無法解析傳輸的內容，確保雙方傳輸資料的安全性。

SSL VPN 具備有管制功能，對於遠端用戶而言，管制有 2 個方向，一個是進入內部網路，另一個是透過 VPN Server 上網際網路(可以選擇啟用或是關閉這項功能)，這 2 個管制方向都可以管制遠端用戶使用的頻寬、通訊服務及時間。

應用程式管制

網路軟體千變萬化，靠傳統 IP 及 PORT BASE 的機制，無法管制現在的軟體，但是每一個網路應用軟體在起始的溝通過程中會出現一定的特徵，這類的特徵可能是要求輸入帳號密碼，或是 Client 跟 Server 溝通的程序，它會反映在網路封包上，藉由抓取前 2000 Bytes 的網路封包分析，就可以成功辨識出使用的軟體，這樣避免全面的封包擷取，增加網路負擔，又能正確地分辨使用的軟體。

AW-570 運用封包特徵值技術，辨識使用的軟體種類，並把它適當的分類，包含【P2P 軟體】、【即時通訊軟體】、【WEB 應用】、【娛樂軟體】、【其他】等 5 大類，可以針對所需要的管制項目做成管制目標，套用在管制條例上，就可以有條理的管制或是開放特定的應用程式。

Bridge、NAT 混合模式

網路基礎建置一直在進步改變，如果客戶的網路環境因為當初的建置不足，例如，當初只是用簡單的 IP 路由器，提供上網功能，一段時間後，導致安全上的疑慮或是因為網路應用內容變化，需要補足缺少的功能，如 Mail SPAM、Mail Virus、Web Virus 等或是頻寬、應用程式的管理、阻擋，甚至想要紀錄郵件、WEB 等資料。

針對這些需求，AW-570 可以將 DMZ 介面採取橋接(Bridge) 模式，藉由 AW-570 提供的豐富功能，滿足日新月異的網路世界上安全的要求，橋接(Bridge) 模式可以確保用戶的環境，不會因為要提高安全等級而破壞現有網路的完整性。

多樣的 Multi-Subnet

傳統上，大一點的網路架構，都會配置 Layer 3 交換器，此時就可以將網路分組的重責大任給交換器處理，但是對於不大不小的網路架構，就可以用 Multi-Subnet 來幫忙。

把 AW-570 的 LAN 或是 DMZ 的網路接口，想像成可以綁定不同子網路的 L3 交換器，並將所有的網路封包都經由 AW-570 路由交換，這樣不管企業網路如何成長了，在必要的時候，增加一個子網路，就可以滿足成長時的需求了。

功能強大的 NAT、PAT

IPV4 位址在可預見的數年內會全部耗盡，所以 NAT 的功能在目前網路環境中，處處可見，AW-570 提供豐富的 NAT 功能，不論是 1:1 的地址映射、1:N 的位址轉換，或是內部出去的 PAT，套用上管制條例後馬上生效。

好用的工具

AW-570 提供多種網路測試工具，包含 PING、Traceroute、DNS 查詢，Port 查詢等工具，在 PING、Traceroute 這 2 樣工具，還可以分別在不同網路介面執行。例如可以在 LAN 介面上 PING、Traceroute 內部網路上任何一部電腦。

管理簡單，簡單管理

滿足網路管理的基本要求，使用 Web 方式設定和更新軟體，操作畫面可隨時切換為繁體中文／簡體中文／英文，並具有設定檔匯入、匯出的功能，並可以隨意開啟／關閉 ping/ http/ https 的遠端操控服務。

任意修改的『登入標題』、『首頁標題』、『瀏覽器標題』等文字，甚至上傳圖形到管理介面，讓管理者一進入畫面，就知道目前正在設定哪一台設備。

以歷史為鏡，鑑古知來

歷史資料重不重要？見仁見智，但是所有的網路攻擊或是異常，往往不是突然發生，我們只是在發生嚴重後果時才意識到它的存在，所以將歷史資料去無存菁備份

在設備中，提供管理者查詢分析，或許可以避免下一場更大的災難。

雙作業系統，永保安康

雙作業系統不僅提高設備運作的穩定度，更給遠端的網路管理者(一般是指系統集成商)服務的保證，當正常的開機系統故障時，可以進入備援的作業系統，將一切恢復成最初的出廠狀況，在出廠狀況下，設備可以維持系統最原始的運作如上網、管制...。後續再利用軟體升級機制，將設備升級到最新的韌體版本。

(二) 硬體規格

■ 網路介面

4WAN / 1LAN / 1DMZ

■ 網路速度

10/100/1000 Mbps

■ 硬碟容量

SATA 250G

■ 系統管理

使用瀏覽器進行管理設定(HTTP & HTTPS)

■ 安規認證

CE、FCC

■ 使用環境

作業環境溫度：0℃ ~ 40℃
作業環境濕度：5% ~ 95% RH

■ 產品尺寸

44mm(高)×440mm(寬)×320mm(深)

■ 電源

100V~240V / 150W

■ 機型

1U 機架型

如有任何需要，歡迎和我們聯絡

銳吉科技有限公司
Http://www.rayji.com.tw
電話：04-26332215 傳真：04-26332216
E-Mail：service@mail.rayji.com.tw