

# 入侵偵測防禦設備效能 500Mbps

## 低階入侵防禦系統

### ShareTech AW-590



AW-590 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 是機關、學校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-590，期望改善使用者的困惱，並增加管理網路的方便性。

將 AW-590 架設於單位的網際網路入口處，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-590 同時整合 Load Balance、Smart QoS、VPN、IDP、SSL VPN 和流量分析，讓您毫無後顧之憂地捍衛網路安全。

眾至資訊股份  
有限公司

台中總公司  
04-27050888

台北分公司  
02-25011185

高雄分公司  
07-2298788

免付費專線  
0800-666188

## 一、硬體規格

1. 作業系統運作不含有 Telnet, Rsh, Rlogin, 等網路服務，並且不能安裝於一般商用 NT、Unix 作業系統上，避免作業系統本身形成安全漏洞。
2. 硬體本身必須具備 10/100/1000 Mbps 乙太網路介面 6 個(含)以上，至少可以規劃成 4 個廣域網路、2 個內部網路。
3. 硬碟容量至少為 500G 以上空間，記憶體容量達 2G。
4. 符合標準 19 吋機架式規格。

## 二、軟體規格

### A. 管理功能

1. 提供以瀏覽器為管理操作，能隨時切換：繁體中/簡體中文/英文管理設定畫面。
2. 具備四個(含)以上 10/100/1000Mbps 超高速乙太網路埠，可將網路區分為 LAN(內部)、DMZ(非軍事管制區)與 WAN(外部)網路介面。
3. 提供系統效能之檢視功能，可查出 CPU、記憶體的使用率為何。
4. 提供介面狀態與 ARP 表，方便查詢連線狀況。
5. 具備手動設定時間及網路時間校正 2 項。
6. 可以設定 4 種權限的管理者，分別為 View、Read、Write 及 All (包含 View+Read+Write)。
7. 任意修改『登入標題』、『首頁標題』、『瀏覽器標題』等文字，甚至可以上傳圖形到管理介面。
8. 恢復出廠值時，可以保留介面位址，方便管理者再次進入管理介面。
9. 具備 PING、Trace route、DNS 查詢、Port 掃描等 4 種網路工具。
10. 詳細的日誌、搜尋系統，管理者所有的操作行為會被系統記錄下來，方便日後查詢。
11. 預設顯示前 12 個小時的 CPU、RAM、設備負載、網路流量圖，並可以選擇特定區間的 CPU、RAM、設備負載、網路流量圖。
12. 內部每一個使用者電腦開關機狀態及網路流量即時顯示，並可以追蹤每個使用者封包的通聯記錄。
13. 流量排行榜，統計今日使用前 1~50 名的總量統計及通訊協定比例分配圖，並且可以查詢特定時間區段的每個使用者的網路使用量及通訊協定分配圖。
14. 網路使用記錄功能，方便分析與追蹤使用狀況，含 System、Icoming、Outgoing、Intrunder Log。
15. 支援系統攻擊事件警報或記錄 (syslog)，系統記錄可以 E-mail 方式傳送給系統管理者。
16. 提供 WEB 或 JAVA 圖型化管理及報表系統。

●●●●●●●●●●  
眾至資訊股份  
有限公司

台中總公司  
04-27050888

台北分公司  
02-25011185

高雄分公司  
07-2298788

免付費專線  
0800-666188

## B. 提供防火牆基本功能

1. 採用狀態封包偵測過濾技術 (Stateful Packet Inspection)，自動偵測和阻擋 SYN Flood (DOS 或 DDOS)、Ping of Death(ICMP)、UDP Flood、Port Scan 等駭客攻擊方法，並將攻擊者及被攻擊的對象 IP 位址、Port 列表。
2. 內建 DHCP Client 及 Server 兩種功能，並可以修改 DHCP 發放 IP 位址的預設閘道。
3. 所有介面均可抵擋疾風病毒(Blaster)的攻擊。
4. 提供疾風病毒的阻擋與警告功能，並紀錄入侵時間、入侵方式及 IP 來源。
5. 支援多種網際網路服務，包含 Http, FTP, Telnet, news, SMTP, gopher 等。
6. 提供依來源地址/埠號、目的位址/埠號及網路服務功能定義交叉混合過濾之規則，限制網路之存取權限。
7. 支援防火牆安全規則 E-Mail 警示功能。
8. 支援 Dynamic DNS 動態網域名稱，即使使用 Internet 不固定 IP 仍可使用網域名稱。
9. 支援 NAT 含一對一(one-to-one)、多對一(many-to-many)方式，提供 IP 隱藏及解決 IP 不足問題。
10. 提供 PPPoE、DHCP Client 的功能，用以支援 ADSL/Cable 寬頻連線
11. 提供 Packet Filtering 封包過濾之功能。
12. 須具備 DNS Proxy 快速存取功能。
13. 內建 DNS 伺服器，可以建立 A、MX 等 DNS 服務。
14. 需具備 DHCP Server 功能，讓設備可以對 LAN 或者 DMZ 發配諸如 DNS、WINS 與 Domain Name 等資訊。
15. 提供 IP4V & V6 雙頻防火牆管理機制。

## C. Anti-SPAM 功能

1. 可以掃描郵件，不管公司的郵件伺服器是在閘道伺服器的內部、外部、非軍事區之內，甚至可以掃描外部的 POP3 伺服器。
2. 支援由外對內收信(In bound)的垃圾信件過濾及病毒掃描防護功能。
3. 可以隔離垃圾郵件，不管公司的郵件伺服器是在閘道伺服器的內部、外部或者是在非軍事區內。
4. 設備可自動提供被隔離的清單，讓使用者直接在清單內將被隔離的信件取回。
5. 提供 Client 垃圾信搜尋 Web 介面。

眾至資訊股份  
有限公司

台中總公司  
04-27050888

台北分公司  
02-25011185

高雄分公司  
07-2298788

免付費專線  
0800-666188

6. 設備可自動將規則裡的特徵學習成為垃圾郵件，或者是在非垃圾郵件。
7. 提供群組及個人黑白名單的功能，並可自行定義個人郵件過濾規則。
8. 可另行將垃圾郵件匯入，或將誤判的垃圾郵件匯出，增加判斷的能力。
9. 可將學習資料庫做匯出與匯入的動作。
10. 動在郵件的 Subject 中增中判斷的分數，若判為垃圾郵件，可再加上諸如 SPAM 等字眼。
11. 訂使用者垃圾清單傳送的時間(以小時為單位)。
12. 自行設定不接垃圾郵件清單使用者與允許寄發清單的網域。
13. 過濾 IP 位址是否在 RBL(Realtime Blackhole List)中。
14. 貝氏過濾的演算法則及啟發式郵件過濾功能。
15. ST-IP 網路信評與快速 ST-PIC 多維圖形辨識技術。
16. 指紋辨識(Finger Printing)線上即時掃描功能，結合社群用戶力量做為線上即時的垃圾郵件辨識，讓各種刻意避開貝氏過濾的垃圾信無所遁形。
17. 提供先進灰名單(Grey List)垃圾郵件預測機制，透過此機制可立即拒絕大量發送的垃圾郵件。
18. 垃圾信件的管理功能，可以針對 SMTP、POP3 為管理協定，並可設定黑名單、白名單。

#### D. Anti-Virus 功能

1. 不管公司的郵件伺服器是在閘道伺服器的內部或非軍事區內，都可針對進出的郵件進行掃毒過濾動作。
2. 可自動在郵件的 Subject 中加上諸如 Virus 等字元。
3. 可以隔離病毒郵件，不管公司的郵件伺服器是在閘道伺服器的內部、外部或者是在非軍事區內。
4. 提供中毒郵件通知信主旨設定。
5. 提供無 License 限制的掃描軟體” Clam”。
6. 具備 HTTP、SMTP、POP3 及 FTP 線上掃毒功能。
7. 針對 SMTP、POP3 等協定做病毒過濾，並自動透過網際網路每日更新病毒碼。
8. 病毒信件時可以做 2 種處理，病毒信直接刪除或將病毒清除後轉寄給收信者。
9. SMTP 掃描效能，每小時可達 13.2 萬封以上。
10. HTTP 掃描效能，每秒可達 340Mbps 以上。

眾至資訊股份  
有限公司

台中總公司  
04-27050888

台北分公司  
02-25011185

高雄分公司  
07-2298788

免付費專線  
0800-666188

## E. 提供 IDP 入侵偵測防禦功能

1. 特徵資料庫(Signature Database)必須提供至少 2,000 個以上預設攻擊模式，並可主動線上更新。
2. 預設的『特徵資料庫』可允許用戶自行修改它的 Action。
3. Action 的模式至少要有兩種：Accept、drop
4. 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
5. 提供威脅攻擊記錄及報表查詢功能，以方便分析。
6. 報表查詢可查看以下記錄：時間、事件、群組名稱、風險程度、介面、來源 IP、目的 IP、協定、來源埠與目的埠。
7. AW-590 具備下列幾種入侵攻擊事件回應能力：發送 TCP Reset 中斷入侵攻擊連線或隔離入侵者、丟棄攻擊封包或移除攻擊流量、紀錄攻擊事件或封包。
8. 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

## F. 提供負載平衡(Load Balance)機制

1. 具備整合不同 ISP 的線路同時並存且能互為備援之功能，至少支援兩條(含)以上線路，並同時提供 Inbound 與 Outbound 之負載平衡。
2. 支援各種型態之網路線路，包含 T1、E1 專線、ADSL 及 Cable Modem 等。
3. 可整合不同 ISP 及 WAN 線路，使進出 Internet 的資料流量提供承載分配及容錯備援，可自動偵測避開中斷的線路，確保廣域網路連線暢通，並至少可支援 100Mbps(含)以上之對外頻寬。
4. 至少支援 4 種(含)以上之負載平衡方法：自動分配、手動分配、依來源 IP 分配、依目的 IP 分配。
5. 擁有多個 WAN 埠，利用負載平衡演算法自動平均分配流量於各線路上。並具備線路備援 (Multi-Homing)功能。使用負載平衡功能可發揮線路最大使用效益，讓企業網路無斷線之憂。
6. 具有對內負載平衡與對外負載平衡功能。
7. 不論是內部到外部或是外部到內部，都將平均分配流量各線路上，即使其中一條線路故障了也不受影響，使企業網路不中斷，保持在一個穩定又暢通的網路環境。

眾至資訊股份  
有限公司

台中總公司  
04-27050888

台北分公司  
02-25011185

高雄分公司  
07-2298788

免付費專線  
0800-666188

8. 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。

### G. 頻寬管理(QoS)功能

1. 可依策略設定頻寬需求，如位址/群組/服務，甚至針對單一 MAC 客戶等。
2. 可設定最多、保證之頻寬及優先權(Priority)
3. 需具有頻寬管控功能，可針對所有網路介面、任何 TCP、UDP Port 及其任意組合、不同 IP 位址、時間或網卡卡號做頻寬管理，並設定上載、下載的保證頻寬、最大頻寬及 1~7 種優先權限
4. 針對不同的網路使用者與應用服務，提供最大可使用之頻寬(Max Bandwidth)、最低保證頻寬(Guaranty Bandwidth)及傳輸優先權(priority)，以便使每個連線都能達到最佳服務。
5. 提供 Smart QoS，包含每個條例使用的頻寬、每個內部來源 IP 能使用的頻寬、每個外部來源 IP 能使用的頻寬。
6. 可自行設定 Smart QoS 可用流量。

### H. 提供 VPN site-to-site / Client-to-site 功能

1. 內建 IPSec、PPTP Server / Client 的軟體，並提供 VPN 穿透能力。
2. 支援 168-bit(3DES)、AES128/196/256 之加解密功能。
3. 提供 256(含)以上之 VPN 通道(Tunnels)
4. 支援 Key management: manual and automated(AutoKey IKE)
5. 支援 Authentication: MD5 and SHA-1
6. 支援測試 IP 功能(Keep Alive IP / GRE)
7. 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。
8. 支援 Aggressive mode，並提供顯示這端網路芳鄰。
9. 支援 VPN 認證功能，並且針對 VPN 提供頻寬管理與排程的能力。
10. 內建標準 IPSec VPN 加密虛擬網路連線功能，當相同兩部以上設備連接及認證後，即形成私人虛擬網路，並可以顯示個別 VPN 通道的建立連線通聯記錄。
11. 內建 PPTP Server / Client 功能，並可以顯示個別 VPN 通道的登入及登出時間
12. 支援 SSL VPN(Web VPN)功能，使用者可利用 Web VPN 連線至內部網路。
13. 提供 VPN、SSL VPN 管制功能。
14. 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

●●●●●●●●●●  
眾至資訊股份  
有限公司

台中總公司  
04-27050888

台北分公司  
02-25011185

高雄分公司  
07-2298788

免付費專線  
0800-666188

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。

### I. 支援 5 大類應用程式管理

1. P2P 類至少包含 eDonkey、Bit Torrent、Kazaa、Napster、Imesh 等 5 種軟體。
2. 即時通訊類至少包含 MSN、Yahoo、AIM、QQ、Skype、GoogITalk 等 6 種軟體。
3. WEB 應用至少可以管制針對特定副檔名下載管理、WEB MAIL、Video、Audio 禁用。
4. 娛樂軟體管制至少包含 DOOM、Xbox、BattleField、Quake 等 4 種軟體。
5. 其他軟體管制至少包含 Citrix、PC anywhere、VNC、RDP、Code\_red、Nimda 等 6 種軟體。
6. 提供 FTP 及 HTTP 的下載(Download)及上傳(Upload)管制, 可針對 HTTP 的 Audio & Video 進行控管, 甚至可針對 exe、zip、scr、doc 等 20 種以上的副檔名進行管制

### J. 內容記錄

1. 詳細的郵件通聯記錄查詢, 只要信件通過設備, 就會將郵件的通聯紀錄存下來。
2. WEB 紀錄, 紀錄使用 WEB 紀錄, 設備會將瀏覽過的 URL 記錄下來, 如果啟用 WEB 防毒, 會將掃毒狀況顯示出來。
3. FTP 紀錄, 紀錄 FTP 傳輸檔案, 如果啟用 FTP 防毒, 會將被紀錄下來的檔案及掃描狀況, 一併顯示。
4. MSN 紀錄, 紀錄 MSN 的對話及傳輸的檔案名稱及內容, 甚至可以在對話中插入警示文字。
5. IM 紀錄, 紀錄 Yahoo、ICQ、IRC、Gadu、Jabber 等 5 種的對話內容。
6. 郵件紀錄, 紀錄 SMTP、POP3 信件內容及傳輸的附加檔案, 不論郵件伺服器主機放置於網際網路上的任何地方。

### K. 提供策略管理(Policy Management)

1. 設定的管制條例可以加上註解, 並且可以任意移動執行順序, 對於內至外的封包, 可以觀察詳細的通聯記錄。
2. 可依來源地址、目的地址 (IP 或 MAC 位址或任意組合的群組) 及網路服務功能 (Port、頻寬、時間、防毒、使用介面及內容紀錄) 定義過濾之規則, 限制網路之存取權限。
3. 更動管理目標設定值前, 不需要將已套用的管制條例暫停, 更改後新的設定值馬上生效。

眾至資訊股份  
有限公司

台中總公司  
04-27050888

台北分公司  
02-25011185

高雄分公司  
07-2298788

免付費專線  
0800-666188

4. 具備 URL-Blocking(網址-關鍵字過濾)功能，並可配合排程過濾(Time-Scheduler 24 Hours × 7 Days)。
5. 提供頻寬限量(Bandwidth Quota Control)功能，可依連線數目(Per Session)或依每日(Per day)針對某人(或群組)或某服務(或群組)做頻寬分配與限量傳輸。
6. 提供認證功能，可內建帳號密碼(Local Data Base)，或將詢問轉向內部 RADIUS SERVER。
7. 管理者可以任意從自訂的帳號密碼、從 AD 伺服器選取的帳號密碼或是從郵件伺服器來的帳號密碼來源挑選組合，組合的名稱就是一個認證群組，此時就可以在管制條例中挑選特定的認證群組套用。
8. 支援將認證需求轉向給 POP3、AD、RADIUS 伺服器。
9. 提供位址表功能，可以單獨針對 IP、IP+MAC 綁定，來制定管制條例。
10. 可進行 VPN 管制，包含管制通訊協定、頻寬管理與時間表。
11. 提供 Web-Based 之設定與管理介面，以管理及控制本設備各種之設定。
12. 政策，包括安全規則、頻寬管理、VPN 及 Multi-WAN 負載平衡等策略。
13. 提供依來源位址/埠號、目的位址/埠號及網路服務定義交叉混合過濾之規則。

#### L. 維護保固

1. 攻擊特徵引擎免費升級服務。
2. 提供防毒更新軟體免費更新。
3. 提供無限人數使用版權。
4. 具備新版本軟體無限期免費更新服務、報表管理軟體與特徵資料庫免費更新服務。
5. 支援網路設備 HA(High Availability)備援功能，使單機發生故障無法運作時，備援設備可接續網路運作。

眾至資訊股份  
有限公司

台中總公司

04-27050888

台北分公司

02-25011185

高雄分公司

07-2298788

免付費專線

0800-666188