NetIRS 智慧型 聯合防禦網管系統

Enhance 軟體模組

身分識別與認證管理
TimeShift 時光飛梭
IP、Switch Port 回收機制
伺服器監控管理
DHCP 應用服務

最全面的進階過濾管理

縝密的身分識別認證管理，除了過濾非法使用者，亦對合法 IP 行為做即時紀錄與監控，
確保網路整體環境之安全。

NetIRS 智慧型 聯合防禦網管系統

Enhance 軟體模組 -- IP 進階控管

Enhance 軟體模組的主要功能是對 IP 做更進階的控管，以提供管理員在複雜的內部網路環境，特別是開放式空間與無線上網的環境下，能對已知或未知的使用者做到進階的過濾與管理 (User Management)，以確保網路整體環境之安全。

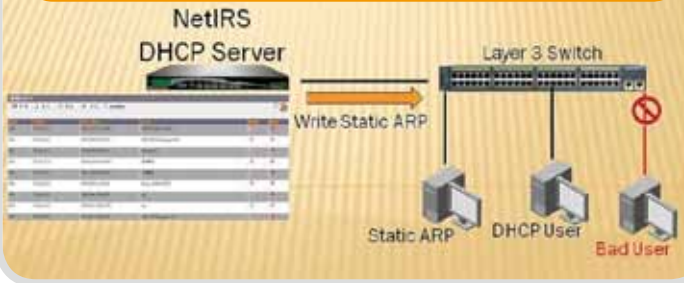
網路入口身分識別與認證管理

Enhance 軟體模組過濾使用者請求上網的方式提供三種認證模式：一、IP-MAC 鎖定功能；二、MAC Authentication；三、Web Authentication。特別的是，此三種認證模式可以獨立使用，也可以搭配管理員特殊的網路環境或要求共同存在交互使用，以達到提供彈性的使用者上網需求又能兼顧內部網路的嚴密封鎖。

IP + MAC 鎖定功能

一個 MAC 地址固定分配一個 IP 地址；只要不存在配對表上面的 IP 與 MAC 都無法使用網路。此功能可整合 DAI (Dynamic ARP Inspection)、DHCP Snooping、限制 ARP Learning 等功能，可與多種品牌的網路交換器互相搭配如 Cisco、Juniper、3COM、Extreme、Alcatel、Huawei、D-Link、SMC 等設備。同時也可新增臨時的 IP-MAC，限定有效使用時間，以方便臨時管理之需求。另外，也支援如 PDA、IP Phone 等無法輸入使用者 ID 及密碼之設備以 IP-MAC 方式認證進入網路。

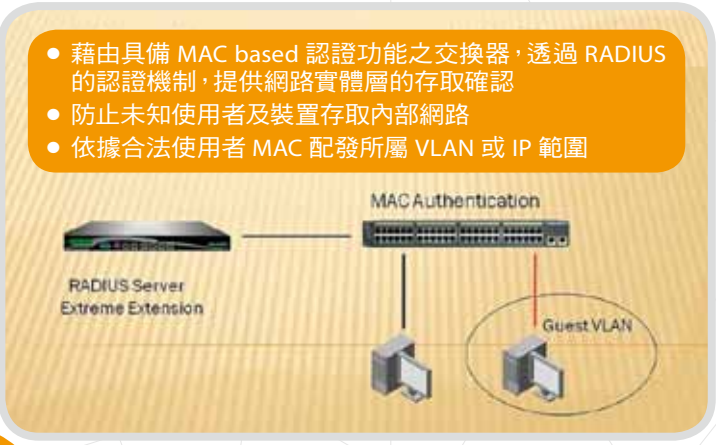
- NetIRS 自動設定 Layer 3 Switch 上的 Static ARP
- 關閉 Layer 3 Switch ARP 學習功能
- Layer 3 ARP 可經由 DHCP Snooping 取得



MAC 認證

此方式適用於以 DHCP 來配發 IP 者。當使用者發出上網請求時，NetIRS 會先檢測其 MAC 地址是否合法，若合法，則 DHCP Server 便配發其專屬或臨時的 IP 供其上網。若 Switch 本身具備 MAC Authentication 功能，則可直接透過 Enhance 軟體模組的 RADIUS 認證機制，提供網路實體層的存取確認，對合法使用者，配發所屬 VLAN 之 IP。

- 藉由具備 MAC based 認證功能之交換器，透過 RADIUS 的認證機制，提供網路實體層的存取確認
- 防止未知使用者及裝置存取內部網路
- 依據合法使用者 MAC 配發所屬 VLAN 或 IP 範圍

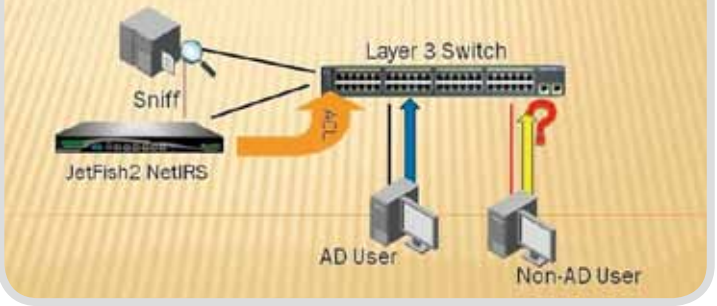


Web 網頁認證

支援 Windows Domain SSO 認證

對不受地理限制，不固定 IP 與 MAC 設備的上網用戶，就使用 Web 認證。當未授權的使用者透過 Browser 發 出上網請求時，會先在隔離區配發一組暫時的 IP 以供其輸入帳號及密碼，若認證成功，則該使用者便可取得合法的 IP，並根據管理員的網路權限設定，在範圍內使用網路。Web 認證系統亦支援 Windows Domain Single Sign On(SSO) 單一認證存取模式，使用者可直接向 Windows AD Domain（簡稱 AD）請求登錄，當 Enhance 系統監聽到 AD 登錄成功時，便配發一組合法的 IP 以供其存取網路資源；若在 Layer3 Switch 內定 ACL 隔離名單中有固定 IP 的使用者請求登錄時，Enhance 系統會自動判斷是否為合法 AD 用戶，若通過 AD 認證，Enhance 系統便會寫入 Layer3 Switch ACL 開啟使用權限，如此使用者便得以保留其原本的 IP 亦可存取該網路。後端使用者認證平台上支援 RADIUS、LDAP、POP3、IMAP4，及 SMTP 等伺服器。

- Layer 3 Switch 內定 ACL 隔離使用者存取網路
- NetIRS 監聽所有 AD 認證封包
- 若為合法 AD 用戶，寫入 Layer 3 Switch ACL 開啟使用權限 (Subnet Mode and Global Mode)



混 合式認證整合方式

以上的認證也可視用戶端的環境需求做整合性運用，如限定員工做身份識別認證，其他用戶則開放上 Internet（多用於公共場所之有線與無線網路環境下的安全控管）；或如第一次採用 WEB 認證，通過後並自動轉成 MAC 認證（目的是讓使用者只需要第一次輸入帳號密碼登入核准，以後持相同行動裝置上網就可直接登入，不須要再輸入帳號密碼）…等等混合式應用。

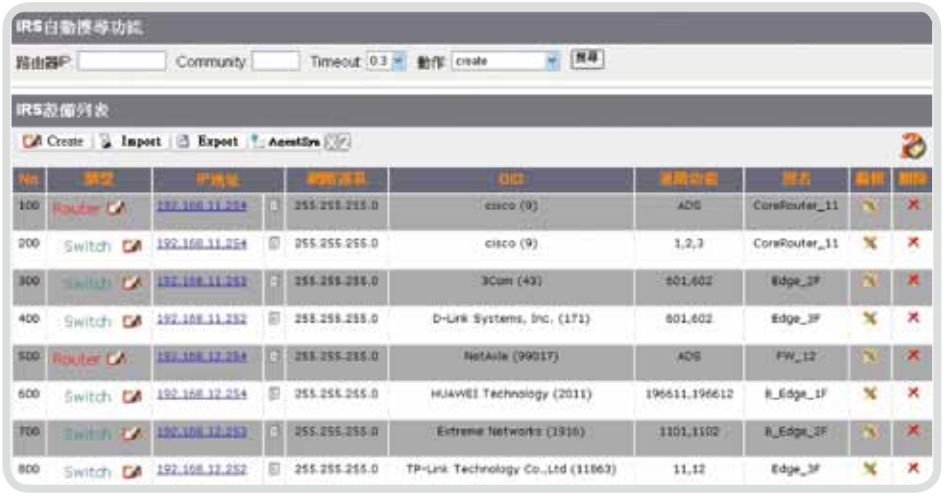
DHCP 應用服務

Enhance 軟體模組提供豐富的 DHCP 應用服務，包括有 DHCP Server、Static DHCP IP-MAC Mapping、DHCP relay、DHCP report 四大部份。DHCP Server 提供 IP 位址的發放；Static DHCP IP Map 則可以根據特定的 MAC 發放特定的 IP，如果管理員已有大量的 IP-MAC 對照表，Enhance 系統亦提供上傳的公用程式以便匯入資料，同時提供 [Learning] 自動學習功能，將兩者資料整併一齊。DHCP relay 主要的目的是讓 NetIRS 可以使用外部的 DHCP Server，讓 client 端可將其 DHCP request 傳導 (relay) 至指定的 DHCP Server。DHCP report 則讓管理員可了解 DHCP 的使用狀況。

NetIRS 系統之 IP-MAC 中央控管

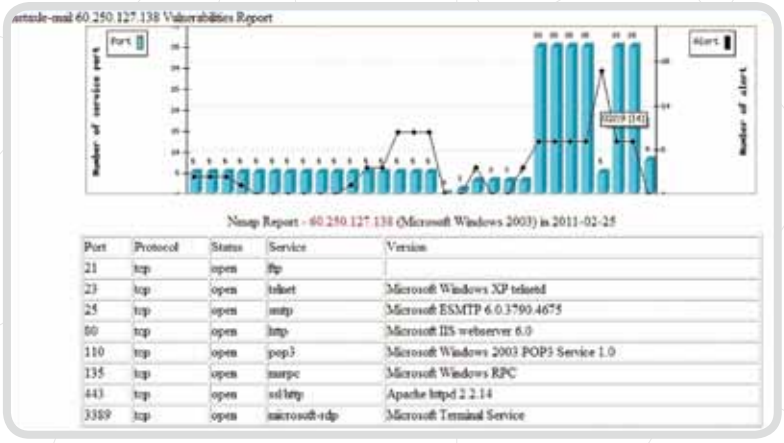
節點管理

Enhance 軟體模組提供節點管理 (Node Manager) 功能，可依據 Group(群組)、Subnet、Device(設備) 等分類進行管理，並支援各種廠牌的 SNMP Switch。節點管理可監測設備的 CPU 與 Memory，可設定告警的程度與等級，也可自動偵測設備的 Private OID、或列出相關的 OID 供管理員直接點選，設定與操作都相當簡易而便利。



伺服器監控

伺服器監控 (Host Monitor) 服務，支 援 TCP Service、UDP Service、ICMP Ping 等傳輸協定，可觀察如 TCP 協定中，各種服務的版本與對應的通訊埠口，同時監督其服務的狀態，必要時可產生告警，所以也可偵測網頁是否遭到篡改並產生入侵紀錄與防禦動作。伺服器監控服務可結合 Script Management 功能，若伺服器非硬體或人力因素導致當機時，管理員可啟動遠端伺服器使之重新開機、恢復運作。



TimeShift（時光飛梭）節點線上監控

TimeShift 時光飛梭節點線上監控功能，主要為觀察某特定 IP 近期或某特定時段的網路使用狀況，包含該 IP 是幾月幾日上線、上線的時數與次數、從哪一個連接埠位址、配對的 MAC 位址等資訊，可經由 TimeShift 功能判斷出來。

TimeShift 時光飛梭節點線上監控功能，主要為觀察某特定 IP 近期或某特定時段的網路使用狀況，包含該 IP 是幾月幾日上線、上線的時數與次數、從哪一個連接埠位址、配對的 MAC 位址等資訊，可經由 TimeShift 功能判斷出來。

◀ 在 Enhance 系統下，管理員只要在 IP 節點列表中點選欲查詢的特定 IP，即出現該 IP 資料功能視窗，其中就包含該 IP 的 TimeShift 以及其對應 MAC 地址的 TimeShift 供管理員選擇，因為當下所看見的 IP 與其對應 MAC 地址，不表示過去六個月兩者也會有相同的行為模式。

TimeShift 時光飛梭節點上線監控功能，特別適用於個資法案在舉證某 IP 於線上操作次數與時間的軌跡紀錄，這樣具體的紀錄儲存將是對企業在維護內部資安上的一大利器，因為多數的資安設備都無法只針對單一 IP 做歷史性監控，遇到需要調閱時，只能人工從一堆報表裡逐一尋找，還必須自行分析判斷；而 TimeShift 時光飛梭只需管理員用點選的方式，系統便自動將該異常 IP 的歷史上線紀錄做 TimeShift，讓管理員一目了然，輕鬆以對。

◀ 圖中，時間軸最下層顯示某 IP 在某年某月的上線次數；中間層將時間軸放大顯示某月某日的上線次數；最上層顯示該 IP 每次上線的起始時間與結束的時間，並以藍色線段突顯上線的時段。

◀ 圖中，點選 IP，可進一步查出此 IP 關聯的設備，與使用者的細部資料。

進階防火牆功能

Enhance 軟體模組可同時啟動兩種封包過濾與分析及動態檢測之能力，也提供各種通訊協定的進階封包過濾選項 (包括 TTL、ToS/DSCP、Time 等)，以及完全支援 FTP(active/passive) 協定可動態產生 FTP 連線的防火牆規則。透過完整的動態檢測設計，也使得攻擊者無法進行 SYN/FIN/RST flooding 攻擊。另外 Enhance 軟體模組的 TCP Defender 功能，可有效阻擋各類 TCP 攻擊及作業系統特徵掃瞄 (Fingerprint，包括 SYN/FIN/XMAS/NULL 等特徵掃瞄、Land 攻擊、SYN/FIN/ACK/RST flooding 攻擊等)。

Policy Based NAT

提供 Policy Based NAT 的防火牆功能，可依據 Source IP、Destination IP、Protocol、Source Port、Destination Port、ToS、DSCP、Day/Time 定義 Policy 規則，提供一對一、多對一、多對多的對應與 DNAT。

IM 與 P2P 控管

內建 IM 與 P2P 應用服務控管功能，防止端點因使用如 Skype、MSN、eDonkey 等等傳輸軟體時附帶散播的木馬程式與病毒蠕蟲，監測範圍含蓋網路層 Layer7，亦包含 VoIP 全方位管理。

Policy Based TARPIT

提供 TARPIT 煙暮欺敵防入侵系統，利用偽裝 IP 與服務 (如 Web、FTP、Mail、Telnet 等) 以混淆駭客並進而達成隱藏內部伺服器與鎖定駭客掃瞄工具；Enhance 軟體模組遇到掃瞄探測時會咬住對方的程式，並施放給對方假的網路埠號碼以混淆其攻擊行為，保護伺服器的安全並能做到凍結駭客的攻擊。

多重路由及線路之負載與備援

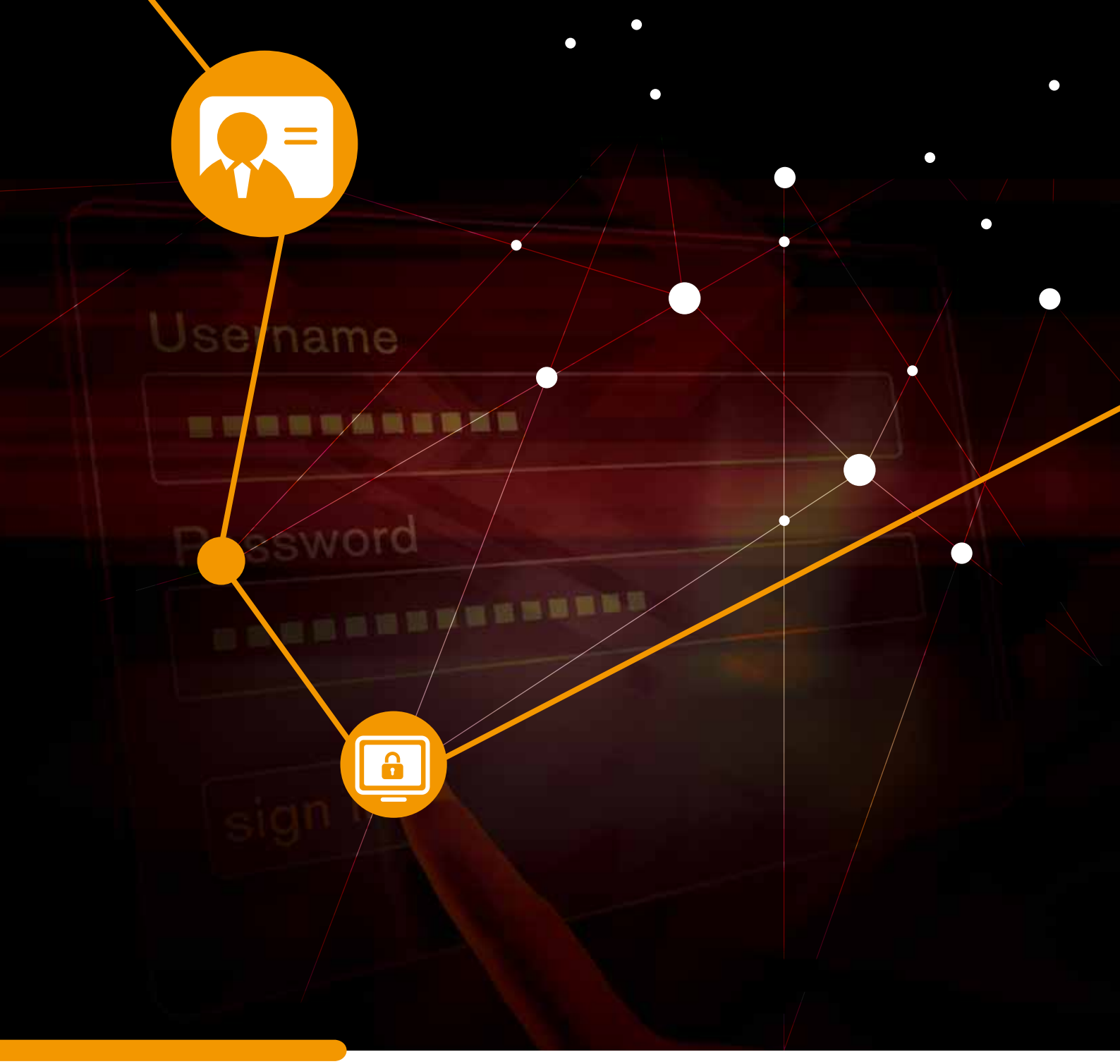
提供多個網路介面，管理者可依照不同的需求定義每個埠不同之路由網段 (Routed mode)、橋接模式 (Bridged mode)、甚至 Hybrid 混合模式 (Mix Routed with Bridged Mode)，因此除了規劃 DMZ 及 Intranet 所需的網路埠外，其餘埠皆可規劃為對外的寬頻連線，同時連接到多家 ISP 網路，以建立對外路徑的負載平衡或備援連結容錯的目的，並支援虛擬介面 (Virtual IP) 與 802.1Q 功能，每個介面可設定多組 IP 地址，使聯結數不受實體連接埠之限制，各 VLAN / Subnet 可使用不同安全機制。Enhance 軟體模組同時具備完整之路由系統，包括 Static Route、Policy Route、RIPv1/v2、OSPF、BGP-4、IS-IS、DVMRP、PIM 等 Unicast 與 Multicast 路由功能，透過這些路由功能讓 NetIRS 防禦系統得以完美佈署在網際網路上。

回收 IP、Switch Port

NetIRS 具備相當完整的 IP 管理功能，其內建的 DHCP 應用服務，可以指定特定的 MAC 發放給特定的 IP，也可支援企業既有的 DCHP Server。它除了可以防止非固定 IP 發放所產生的 IP 衝突之外，也可以防止 IP 被非法盜用；對於發出去的每個固定 IP 都有明確的「關聯紀錄」，並且會主動顯示許久未被使用的 IP，提供管理員決定是否要回收以便再度利用。上述的管理功能也同樣完整應用在 Switch 的每個連接埠上，使閒置的 Switch Port 也能透過 NetIRS 系統操作，簡單而輕易地關閉回收。

Enhance 軟體模組功能

- 同時支援 IPV4、IPV6、有線及無線網路認證之安全防禦閘道功能，可直接控管終端電腦設備網路存取政策。
- 具備身份識別與認證管理功能，支援 IP-MAC 鎖定功能、MAC Authentication、Web Authentication、與交互混合應用認證模式。
- 可新增臨時的 IP-MAC，限定有效使用時間，以方便臨時管理之需求。
- 認證模式支援不同品牌之有線與無線網路設備；交換器支援品牌如 Cisco、Juniper、3COM、Extreme、Netscreen、Alcatel、Huawei、TippingPoint、Fortigate、SonicWall、Snort 等設備；無線網路支援如 PDA、IP Phone 等設備。
- 支援使用者以 Browser 認證方式達成身份認證，使用者無需安裝任何軟體。
- 身份識別與存取控管：支援 AD、LDAP、RADIUS、POP3(S)、IMAP4(S)、SMTP(S) 等認證伺服器，使用者通過認證後才能獲得網路使用權，未經認證設備無法使用網路資源或重導至認證網頁。
- 認證服務提供 Windows Client 軟體，並支援 Single Sign On 應用，可整合 Windows AD Domain 達成一次性簽入。
- 使用者帳號可依角色類別給定不同權限並限定其網路存取範圍與規則。
- 提供 DHCP Server、Static DHCP IP-MAC Mapping、DHCP relay、DHCP report 等豐富的 DHCP 應用服務。
- 提供節點管理 (Node Manager) 功能，可依據 Group、Subnet、Device 等分類進行管理，並支援各種廠牌的 SNMP Switch。節點管理可監測設備的 CPU 與 Memory，可設定告警的程度與等級，也可自動偵測設備的 Private OID、或列出相關的 OID 供管理員直接點選。
- 支援伺服器監控 (Host Monitor)，並支援 TCP Service、UDP Service、ICMP Ping 等傳輸協定。伺服器監控服務可結合 Script Management 功能，若伺服器非硬體或人力因素導致當機時，管理員可啟動遠端伺服器使之重新開機、恢復運作。
- 提供時光飛梭 (TimeShift) 節點線上監控功能，可觀察某特定 IP 近期或某特定時段的網路使用狀況，包含幾月幾日上線、上線的時數與次數、從哪一個連接埠位址、配對的 MAC 位址等資訊。
- 標示出固定 IP 與 Switch Port 未被使用的閒置時間，供管理員決定是否要回收以便再度利用。
- 支援 802.1x/SNMP 交換器。



NETWORK SECURITY PIONEER

www.netaxle.com.tw

捷宇網安股份有限公司

NetAxle Network Security Corp.

台北市松山路 421 號 3 樓之 2

TEL : + 886 2 23461063

FAX: + 886 2 23461064

授權經銷商