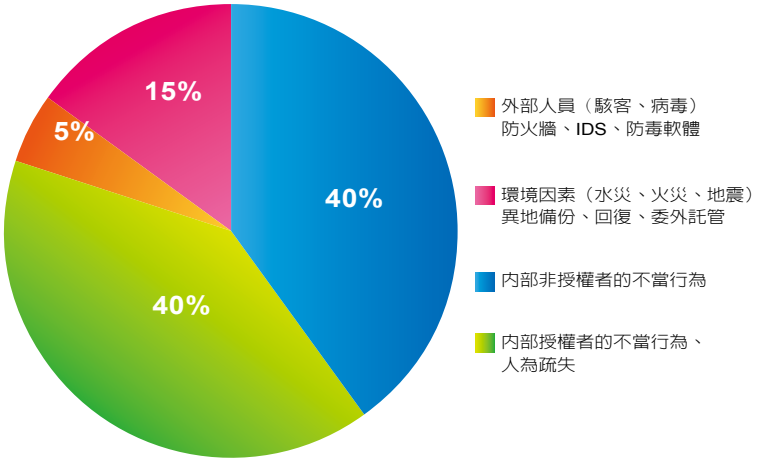
www.netaxle.com.tw

NetAgent 智慧型網路偵防系統

NetAgent 為本公司所開發針對網路第二層安全的偵防設備，採用硬體式獨立主機架構與NetAxle Labs開發之NOS嵌入式作業系統，能持續監控網路節點與事件流量並詳加記錄分析與反應；NetAgent可與NetIRS設備整合，利用智慧關連比對技術以找出有問題的第二層攻擊事件並加以解決，達成Layer2-Layer7全方位嚴密的防護。

內網偵防　唯快不破

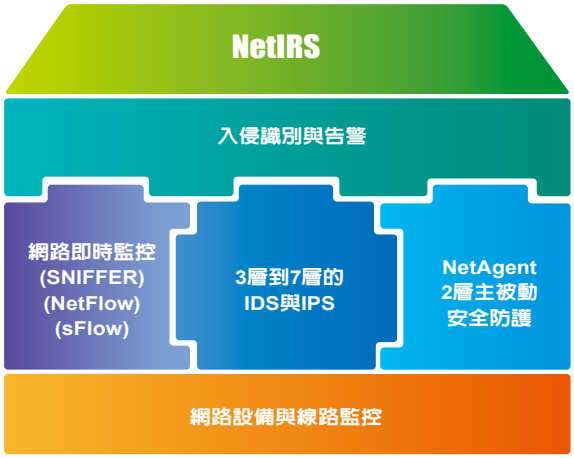


資料來源：美國FBI CSI/資策會MIC ITIS Leap Intelligence

雖然絕大多數網路都已配置了防火牆、IDS（Intrusion Detection System)／IPS（Intrusion Prevention System)，防毒軟體也是所有 PC 的標準配備，但是攻擊事件的數量仍以幾何級數增加，進而影響到網路與應用程式的使用。維繫網路安全決定於是否提供面面俱到的完整保護，然而網路安全的成敗卻決定於網路中最脆弱的一點—網路第二層攻擊。市場上幾乎所有資安產品都集中在第三層到第七層的應用偵測與防護，也因此第二層的攻擊已成為管理者最為頭痛的問題，因為大多數的網路安全設備無法有效偵測與處理第二層的攻擊封包。

第二層的網路攻擊只會出現在內部網路，在近期的研究發現，網路安全事件有80%是來自內部網路，這正說明了企業對內部網路的安全控管薄弱之處，而第二層的網路攻擊一但發生，幾乎是全面性並且立即癱瘓內部網路，而企業重金購買的資安防護設備如防火牆或IPS設備在這場戰爭中卻毫無用武之地。相同的，這種網路第二層攻擊的種類相當多，如ARP/IP Spoofing、DHCP Attack、Broadcast Storm等，單靠交換器是無法有效防堵。為解決這擾人的問題，NetAxle特別研發了NetAgent(簡稱NetAGT)系列產品，其為硬體式獨立主機架構，採用NetAxle Labs開發之NOS嵌入式作業系統，能持續監控網路環境與事件流量並詳加記錄分析與反應；經由檢測所有第二層封包流量，利用智慧關連比對技術以找出網路中所有有問題的第二層攻擊事件並加以解決。

NetAgent可與NetIRS設備整合，採用NetAxle研發技術：入侵自動反應機制(IRS–Intrusion Response System)，同時對內部網路的所有SNMP交換器執行相關安全策略，能在網路第二層攻擊發生的啓始階段就將其偵測出來並進而排除隔離出網路，快速阻斷漫延以確保網路與主機設備安全無虞。



Layer2 全方位防護

NetAgent提供的防禦模式如下：

被動防護（Reactive Protection）

當攻擊者主動發出攻擊的同時（如蠕蟲或木馬的rootkit、DoS、DDoS阻斷式攻擊…等等），在還來不及散播時，就會立即被NetAgent的監聽封包偵測出來，回應給NetIRS下指令控管隔離阻絕，並產生LOG提供NetIRS作記錄。

主動防護（Proactive Protection）

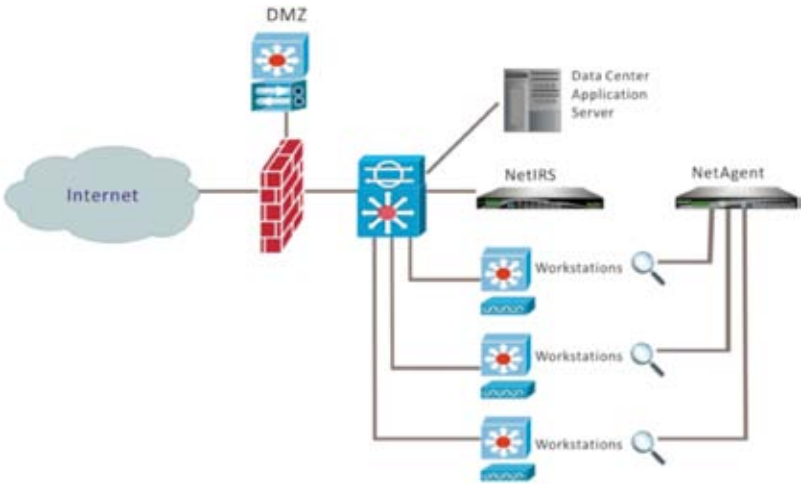
當網路內部某主機的病毒或蠕蟲並非以攻擊為主，而是潛藏在合法的網域裡面做隱形式攻擊，面臨這種隱形式攻擊，即便是具備監聽功能的高檔交換器也判斷不出來的。最常看到的隱形式攻擊種類多為ARP/IP Spoofing、DHCP Attack、Broadcast Storm，例如非法DHCP Server、非法Gateway IP、非法IP盜用、ARP欺騙；中毒的機器會回應所有ARP Request所要求的IP解析為自己的MAC地址，進而癱瘓整體網路。NetAgent提供以下的主動防護以隔絕這類型攻擊的發生：

一、DHCP 防護

防止駭客冒充DHCP Server。NetAgent不僅可以偵測出非法的DHCP Server，還可以將所有非法的DHCP Server的IP耗盡，使其喪失DHCP Server功能，同時也能直接將非法的DHCP Server 隔離起來，杜絕弊端。

二、動態ARP防護

防止ARP欺騙(ARP Spoofing)。由於防火牆/IPS入侵偵測設備都設置在核心路由交換器之後，根本沒有機會接觸到ARP封包，因此對ARP 攻擊是束手無策，就算有也僅止於出口控制，無法由網路底層第一時間阻斷此類攻擊；NetAgent不但可以在第一時間快速偵測到非法的ARP攻擊，並能自動隔離從未授權的主機裡發送出來的ARP廣播包，杜絕ARP欺騙。



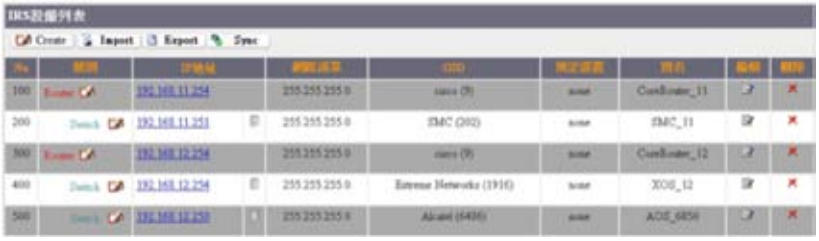
三、非法動態IP的鎖定與終結

防止偽造IP流竄。由於NetAgent會主動掃瞄合法IP位址，所以一旦駭客使用偽造IP位址企圖登入網路時，便會立刻被NetAgent發現並終結。

網路設備控制與監測

- **網路存取控制**

NetAgent可以自動歸類並顯示網路設備，如直接標示某IP設備的類別為[Router]或[Switch]，並顯示其位址、廠牌與別名，讓管理者一目了然。再進一步點選某IP設備後，可顯示該設備所有介面的使用狀況，並可線上即時開啓與關閉網路埠。

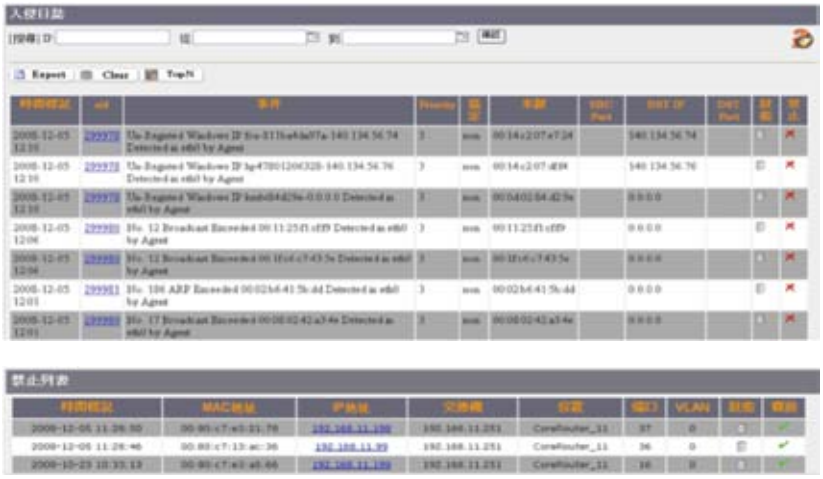


- **IP-MAC鎖定**

不需更改現有設備與架構，NetAgent會經由監控所有網路使用狀況，利用IP-MAC鎖定功能，確保合法使用者才能使用網路。MAC-IP配對表可線上編輯與使用輸出輸入方式管理，也可與NetIRS同步，管理者只需利用NetIRS即可做集中控管。IP-MAC 管控可依各VLAN彈性選擇寬鬆管控與嚴格管控。

- **即時入侵反應系統** Intrusion Response System—IRS

NetAgent系統偵測到網路第二層攻擊時，除了紀錄事件發生的資訊外，同時配合節點定址功能回報系統，主動將有異常的節點透過交換器網路埠封鎖，立即防止異常事件在內部網路漫延。



NetAgent 功能特點

- 每個介面可獨立監控一個VLAN網路中的Layer 2異常封包，此VLAN可包含多個IP網段。
- 具備Rate-based、Rule-based、與Behavior-based事件偵測能力。
- 異常封包包含：IP衝突與盜用、IP/ARP Spoofing、ARP 掃瞄、廣播風暴、非法DHCP伺服器偵測。
- 可自動耗盡非法DHCP伺服器的所有 IP，使非法DHCP伺服器功能失效。
- 支援MAC與IP地址定位功能，可自動找出單一MAC、單一IP、與整個IP網段中所有IP所連接的交換器連接埠。
- 支援監控Router、Switch、Firewall、Mainframe、Server/Host、IDP/IPS、Web Cache、DataBase、與所有SNMP功能設備。
- 提供日誌資料與攻擊行為收集功能，依據收集資料關連分析以判別是否有異常行為。
- 支援標準Syslog訊息模式，支援 SHA-1 HASHING，日誌收集符合NIST日誌管理標準。
- 提供日誌資料搜尋功能，可依時間、來源、目的、關鍵字、IP與服務埠進行搜尋。
- 提供設備與設備異動報表，可與NetIRS自動同步。
- 支援IRS(Intrusion Response System)功能，可依據所偵測到的攻擊自動到所對應的交換器網路埠將其鎖住，並支援所有SNMP標準功能交換器–3COM、Alcatel、Cisco、Extreme、Foundry、Huawei、D-Link、SMC等。
- 可與NetIRS整合以納管多台NetAgent設備與提供統一中央控管機制，並提供多種通知機制–E-mail、SMS(簡訊)、Trap、MSN、與Syslog訊息模式。
- 提供異常事件分析報表及TopN排行報表，並以Pie與Bar chart 圖形方式呈現。
- 提供HIPAA國際標準報表，報表並能以HTML顯示與CSV格式儲存。
- 利用Open URL功能，提供客製化報表功能，並可依據事件等級即時產生報表或告警。
- 可將Syslog資訊滙出或轉送至其他主機做備份，透過Open URL功能可完成手動與自動定期備份或特定時間備份。
- 支援SNMP v1/v2c/v3管理功能。
- 提供Secure Web (HTTPS—SSL加密)與CLI管理介面。
- 可設定多組管理帳號與權限，進行系統操作與管理。
- 支援SSH v1/v2。
- 支援NTP 功能。

NetAgent Professional 軟體模組

- 支援802.1Q功能。
- 提供DHCP Server功能，可整合IP-MAC鎖定機制。
- 支援VIP白名單功能。
- 提供Netflow Probe功能。
- 提供NAT設備偵測功能。

產品型號	JetFish2-A4	JetFish2-A8
		
功能規格		
記憶體	512M	1G (Up to 2G)
Flash	512M (Up to 4G)	1G (Up to 8G)
網路介面	4＊100/1000Tx	8＊100/1000Tx
旁路功能	內建	內建
系統性能		
事件處理數	512/秒	1024/秒
流量數	2000/秒	4000/秒
運作模式	SPAN, Monitor	SPAN, Monitor
系統功能		
型式	1U 19吋機架型	1U 19吋機架型
Web UI	英/繁/簡	英/繁/簡
軟體模組(選購)		
名稱	NetAgent Professional Module	

捷宇網安股份有限公司
NetAxle Network Security Corp.
TEL:+886 2 2346 1063
FAX:+886 2 2346 1064
www.netaxle.com.tw