NetIRS 智慧型 聯合防禦網管系統

聯合防禦網管系統
NetIRS-BASE

最具效率的網管設備

NetIRS 系統超優的隨點即看介面，只需簡單步驟即可輕易監管網路，
大量簡化網管繁瑣作業，有效降低網管成本！

NetIRS 智慧型 聯合防禦網管系統

隨著網際網路應用的發達與普及，企業 e 化的應用更加廣泛而成熟；在複雜的網路環境裡，企業大多數都已經完成防火牆相關系統的建置，其重點為防禦外部使用者的侵略，對於內部使用者的行為卻較少著墨。然而依據調查統計資料，企業資安事件有 80% 是來自內部，因此內部網路的存取控制與監控管理就愈顯重要，而一套完善的網路安全防護，必須要含蓋以下特點：

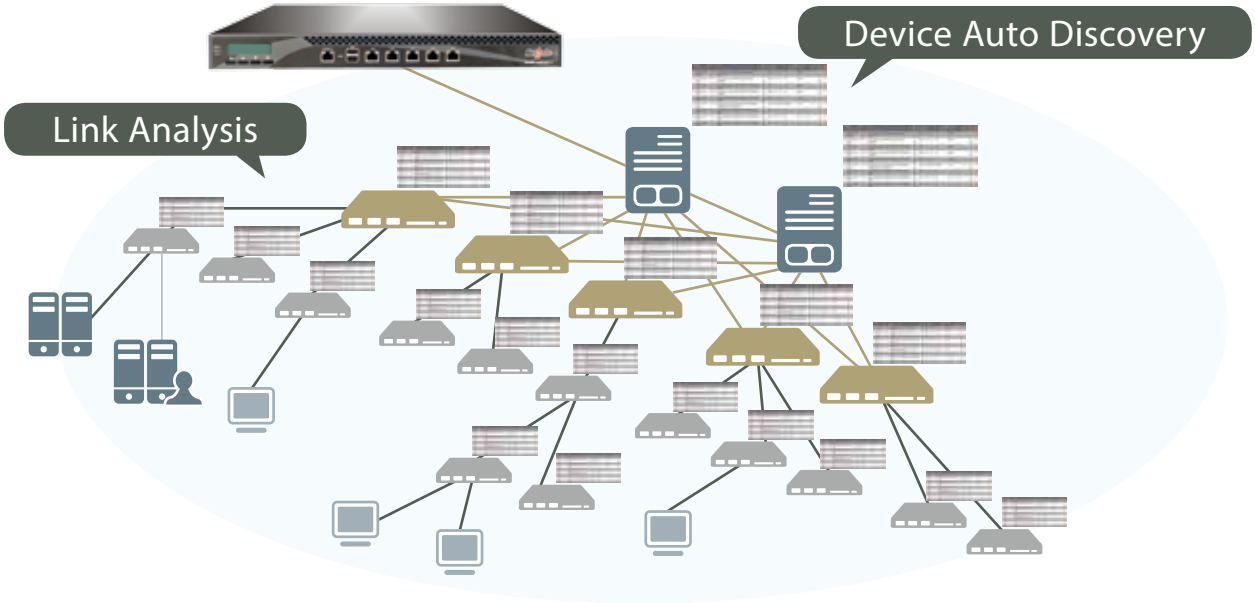
1. 確保主機服務正常：網路的最基本功能在於提供使用者可存取主機等系統上的資料與資源，一旦主機無法提供服務，則所有花費在網路上建置的設備與線路等統統等於白費，尤其現在病毒、蠕蟲相當犯濫，要如何防治是一大要務。
2. 能同時偵測與過濾網路內部與外部的節點資料流，特別是開放式空間與無線上網的使用者管理，要兼顧無障礙的上網空間又要監督未知使用者的存取控制，需能提供全方面完整的監控流程與解決方案，使防禦沒有漏洞。
3. 攻擊事件產生時，網安設備需能整合不同廠牌的資安產品以避免單一廠商的安全漏洞，為因應有限的網路管理人力與資源，在整合與操作上必須非常簡單，並進而能自動快速偵測到問題與所在，提供多樣化的告警與隔離功能。
4. 提供完整的關聯資訊操作功能，讓管理者不論在何種介面檢視網路設備或 IP，都能隨時穿梭於各功能介面，並且資訊相互連結，層層關聯，如此才能符合人性化的操作與達到最迅速、最方便的管理。
5. 提供開放式介面，能整合開發不同的應用程式，以備未來之擴充。

NetIRS 為多功能網路安全管理平台，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，基礎架構 IRS 即時入侵反應系統 (Intrusion Response System) 為 NetAxle Labs 創新研發之功能，在進行流量分析的同時，藉由 IRS 的回報，自動化建立對異常流量與攻擊封包的立即阻擋，進而與其它資安設備共同整合，達成全方位的聯合防禦網絡。除了 NetIRS 的聯合防禦網管之外，也可結合有線與無線網路，進行 IP 進階管理如使用者控管認證等、以及有線與無線共存之階層式流量地圖、擴大至 NetIRS 軟體模組之功能，並全面支援 IPv4 與 IPv6，成為最佳的網路安全運作控管之中樞 (NSOC–Network and Security Operating Center)。

聯合防禦網管系統 (NetIRS-BASE)

設備自動搜尋 (SNMP) -- 線路分析

NetIRS 系統是一套以 SNMP 為基礎的內網流量監控管理系統，可自動搜尋網路設備如路由器、交換器…等等，並具備線路分析，可將整體網路內所有連結的設備與其正確位置找出來以便歸類管理。



聯合資安設備啟動防禦機制 -- 節點定位功能

當網路發生問題時最怕找不到問題發生的地點在哪裡？NetIRS 具備網路節點定位功能，可與其它資安設備共同整合，建立一個完善的聯合資安防護網；當 IDS/IPS 等設備已找到攻擊者的 IP 或 MAC 地址，NetIRS 可在幾秒鐘內將攻擊者定位出來，若有必要，可直接隔離攻擊者。其聯合防禦的方式如下：

與防火牆或 IPS/IDS 整合讀取 LOG 加以判讀分析

NetIRS 可以搜集防火牆、IPS/IDS 等設備所產生與攻擊相關的 LOG（在這些資安設備所產生數萬筆的 LOG 之中，NetIRS 會自動過濾排除非必要的資訊，只會留取與攻擊相關的 LOG，以避免耗盡資源），並針對這些 LOG 加以分析、歸類事件輕重程度，然後自動發出警訊、主動斷線等等適當的處理。

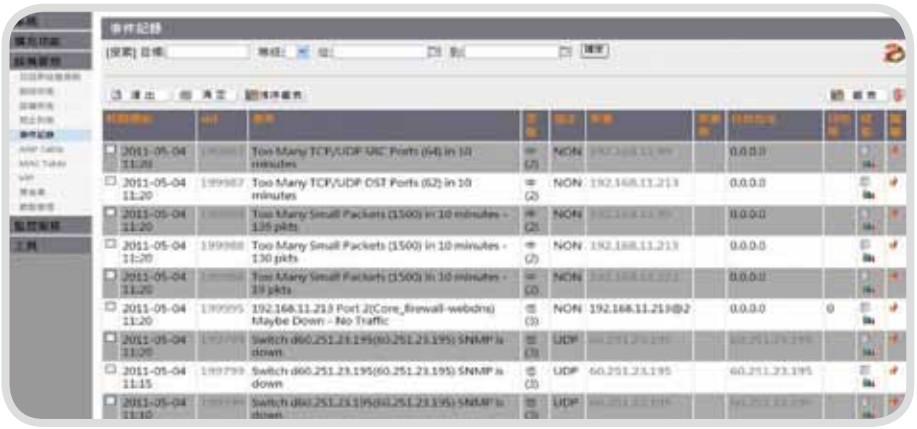
與路由器或交換器整合下 ACL 指令

NetIRS 可與支援 ACL 功能的路由器或交換器互相配合，由 NetIRS 針對異常 IP 下 ACL 指令到路由器或交換器端使其斷線。支持 IP ACL 的廠牌有 Alcatel、Cisco、Extreme、Foundry、Juniper、HP、D-Link 等等。

支援 IP ACL 的廠牌	支援讀取 LOG 的設備
Alcatel	Fortigate
Cisco	Snort
Extreme	GNatBox
Foundry	NetScreen IDP
Juniper	Tipping Point
HP	Dragon
D-Link	Cisco IDS
	ISS
	WatchGuard
	SonicWall
	BroadWeb
	Palo Alto
	Sourcefire

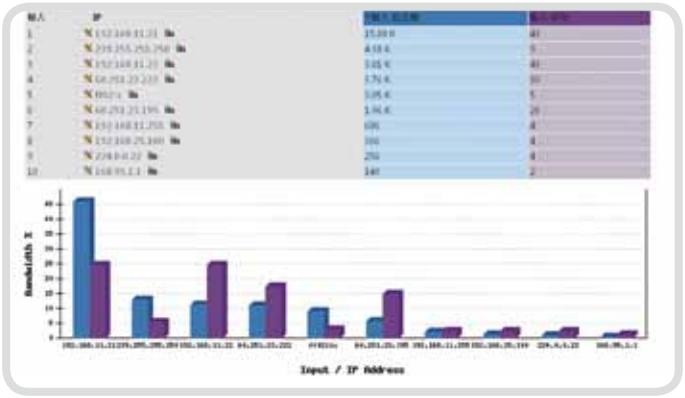
事件紀錄列表查詢

NetIRS 提供「事件紀錄」的列表供管理員查詢，管理員可依事件輕重自行設定 3 種等級（等級低者以數字 3 表示輕微、等級中者以 2 表示中等、重大事件則以 1 表示嚴重），下圖中可以清楚看見詳細的事件紀錄，如發生的時間、事件內容、等級、來源 IP、目的 IP 等等。



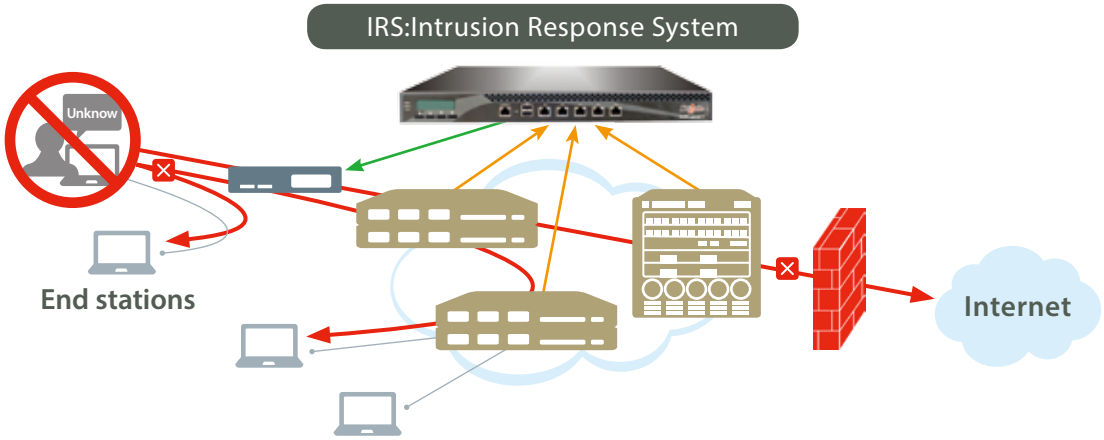
Flow 即時流量統計圖表查詢

NetIRS 系統支援 NetFlow 與 sFlow，隨時監控即時流量，可以依據 IP、Port、或 Connection 流量做排列顯示，也可接收其它不同品牌之網安設備 (如 UTM/ Switch/ Firewall/ IDS/ IPS/ Anti Virus 等) 的 Syslog 與 Trap 訊息即時加以解析，產生如長條圖或圓盤圖等分析統計圖表，並提供對應的異常流量 TopN 報表，立即通報異常 IP。



多種隔離方式 -- Switch Port Shutdown 最安全

NetIRS 因具備即時入侵反應系統 (IRS：Intrusion Response System)，在發現有異常事件通知時，可自動利用節點定位功能 (Node Locator) 將有異常的節點封鎖隔離，以確保網路的安全。NetIRS 對異常行為提供四種隔離方式：1、Switch Port Shutdown 可說是最安全的防禦機制，因為一旦攻擊者的 switch port 被關閉後，攻擊者已完全失去網路連線，當然不可能再攻擊網路。2、Create ACL (IP ACL 與 MAC ACL)：若為網外使用者，則直接在路由器或交換器上寫入。3、Move to Quarantine VLAN (隔離至虛擬網路隔離區)。4、Create ARP (產生 ARP 過濾表)。



多重告警機制

NetIRS 支援 5 種告警方式，管理員可以自行設定如嚴重等級的事件以 SMS 簡訊發送至管理員手機、中等程度的事件顯示在 E-Mail、而輕微事件者則直接紀錄在 Syslog 或 Trap 裡以備不時之需，如此經過歸類後的告警便可大大幫助管理員得到最迅速的資訊並做正確的處置。

SMS 告警支援中文與雙向回應

NetIRS 的 SMS 簡訊告警不但支援中文顯示，還可雙向溝通。當系統發出簡訊告知管理員某人被斷線時，管理員可以立即回撥手機通知 NetIRS 釋放該使用者，如此雙向回應讓管理員即使不在電腦旁也能立即處理緊急事件，甚為便利！

關聯資訊 -- 人力比不上自動化

在諾大的企業網路裡，要如何快速地把 EVEN 事件找出來，查出它在哪裡、甚至是誰，是非常麻煩、耗時耗力的，萬一這是個嚴重事件，等到管理員好不容易查出它來之後想斷線，卻已經來不及了！

NetIRS 可以與附加的軟體模組整合，將所有的分析資料、流量、地圖等等資訊互相關聯，讓管理員不論在 NetIRS 的任何操作頁面，只要點選想觀察的 IP，就會出現一個小視窗，列出關聯此 IP 所有可監控的資訊 (視附加的軟體模組功能而定) 供管理員直接點選監控，相當快速方便。

NetIRS Base 功能特點

- 提供 IPv6 功能 : IPv4/IPv6 dual stack, DHCPv6。
- 提供網路設備自動搜尋功能，可輕易的將整體網路內所有連結的設備找出來並加以歸類，方便管理者進行管理；並支援各廠牌的 SNMP 交換器協定，如 CDP(Cisco Discovery Protocol)、EDP(Extreme Discovery Protocol)、LLDP(Link Layer Discovery Protocol)。
- 提供 sFlow Probe 與支援 NetFlow/sFlow analyzer 功能，可監看分析網路服務，並可接收其它不同品牌之網安設備 (如 UTM/ Switch/ Firewall/ IDS/ IPS/ Anti Virus 等) 的 Syslog 與 Trap 訊息並做即時的解析。
- 支援 Behavior Base 封包監測與辨視功能，進而分析是否有異常或攻擊事件。
- 可搜集防火牆、IPS/IDS 等設備所產生與攻擊相關的 LOG，並加以分析、歸類事件輕重程度，然後自動發出警訊、主動斷線等等適當的處理；支援的廠牌有 BroadWeb、Cisco IDS、Dragon、Fortigate、GNatBox、ISS、Netscreen IDP、Snort、SonicWall、Tipping Point、Watch Guard。
- 可針對異常 IP 下 ACL 指令到路由器或交換器端使其斷線；支援配合 IP ACL 的廠牌有 Alcatel、Cisco、Extreme、Foundry、Juniper、HP、D-Link 等等。
- 提供「事件紀錄」列表，事件可依輕重自行設定 3 種等級以便歸類 (如輕微、中等、嚴重)；列表中有詳細的資訊如顯示發生的時間、事件內容、等級、來源 IP、目的 IP、與嚴重等級等。
- 提供多種異常流量 TopN 事件分析表查詢與圖形化如圓盤圖、長條圖等統計功能。
- 支援即時入侵反應系統 (IRS：Intrusion Response System)，當 NetIRS 系統發現有異常事件通知時，可自動利用節點定位功能 (Node Locator) 將有異常的節點封鎖隔離，以確保網路的安全；節點定位功能可同時支援 IPv6/IPv4。
- 提供 Switch port shutdown、ARP、下 ACL 指令、ARP/IP Spoofing 等多種隔離方式，並自動依照優先順序逐步執行隔離動作，不需做任何設定。
- 提供如 Syslog、Trap、Web、E-Mail、SMS 等多重告警機制；SMS 簡訊告警支援中文顯示與雙向溝通模式。
- 提供關聯資訊，可與 NetIRS 的軟體模組整合，將所有的分析資料、流量、地圖等資訊互相關聯；只要點選 IP，就會列出關聯此 IP 所有可監控的軟體資訊連結。
- 介面埠不需鎖定特殊用途，每埠均可自由定義與使用為 LAN、WAN、DMZ、Authentication 網路類型與路由模式。
- 可配合 NetAgent 設備以支援 Layer2 攻擊偵測防禦;例如:假冒 Gateway IP、ARP 攻擊、Broad cast 攻擊、非法 DHCP 伺服器等。
- 支援 SNMP v1/v2c/v3。
- 支援 SSH v1/v2。
- 支援 NTP 功能。
- 支援 VRRP 備援系統功能，支援 active-active H.A.。
- 提供 Secure Web(HTTPS-SSL 加密) 與 CLI 管理介面。

NetIRS 產品規格表

產品型號	JetFish2-C	JetFish2-E	JetFish2-S	JetFish2-X
				
記憶體	1G	2G	4G	8G
Flash	1G	2G	4G	8G
網路介面	4 * 100/1000Tx	6 * 100/1000Tx	6 * 100/1000Tx	4-port 100/1000Tx, 4-port SFP
802.1q	V	V	V	V
效能	無數目限制	無數目限制	無數目限制	無數目限制
型式	1U 19 吋機架型	1U 19 吋機架型	1U 19 吋機架型	2U 19 吋機架型
功能	NetIRS 聯合防禦系統 Base 基本系統 · 設備自動搜尋 (SNMP) · 即時流量統計與報表查詢 (支援 NetFlow/sFlow) · 異常流量分析 (TopN) · 節點定位功能 · 判讀資安設備的攻擊封包 (Syslog) · Switch Port Shutdown 與 ACL 等多種隔離方式 · 多重告警方式			

軟體模組	NMS	Enhance	FlowAnalyzer	WLAN (Wireless LAN)	WOT (Wheel Of Time)
功能	· 線路與流量分析報表 · 伺服器監控 · 階層式流量地圖 · 流量地圖六宮格 · 內網 GPS -- IP 定位系統	· 身份識別與認證管理 · TimeShift 時光飛梭 · IP、Switch Port 回收機制 · 進階防火牆功能 · 節點管理 · 伺服器監控 · DHCP 應用服務	· 歷史流量統計與報表查詢 (NetFlow/ sFlow) · 歷史異常流量分析 (TopN) · 歷史 Syslog 封包紀錄 · 歷史報表定時回報 · 可整合 NMS 模組 · 可產生歷史流量地圖動畫播放 · 需加裝硬碟於 NetIR 機器主體	* **需已購買 NMS 模組方可加購** · 整合 Aruba、Cisco 無線網路 · 無線有線統合流量地圖 · 無線 AP 分析報表 · 無線使用者分析報表 · 無線網路節點定位	· 應用程式服務與網路延遲分析 (latency) · 應用程式即時與歷史延遲追蹤 (latency) · 可整合伺服器監控 · 可整合流量地圖

最具效率的網管設備

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