新一代網路維運平台

- **結合SNMP、Flow、Syslog三大網管技術**
- **支援合勤科技交換器、無線網路、防火牆監控、韌體與設定管理**
- **軟硬體完美結合，支援VM安裝版本**
- **支援多筆查詢條件，產出精密邏輯運算與報表**
- **Flow模組進行用量分析**
- **Syslog與Flow關聯性整合運用**
- **豐富多樣的即時、離線、分時報表**
- **動態即時呈現事件統計及告警現況**
- **Action模組執行聯合防禦**

傳統網管軟體只著重設備和線路狀態的監控與配置管理，進階網管系統最多再補足流量監控和記錄儲存能力，然而面對日異複雜的網路應用環境，單獨的網路監控管理已經不足以應付日常維運所遭遇到的問題。根據MIS管理人員的需求訪談統計，使用者最常遇到且難以解決的多為系統性問題。例如網路設備遭受攻擊或使用異常造 成網路效能變慢等，往往要耗費很長的時間才能找出問題根源，浪費使用者與管理人員寶貴的時間和資源。

現今網路設備、伺服器與資安產品多能支援Syslog或Flow流量資料輸出功能。對IT人員來說，訊息完整的Syslog Data提供了非常簡易的查詢基礎，而Flow Record則是了解網路用量的最佳幫手。

合勤科技ZyXEL Network Insight (ZNI) 新一代網路維運平台採用多項創新技術，除了具備Syslog／Flow訊息蒐集、儲存、即時分析、查詢與報表製作等功能之外，特點是可以執行Syslog與Flow間的關聯性分析(Correlation)，將Flow的L3/L4封包位元數據與Syslog的L7事件內容完美結合，讓IT管理者完全掌握網路使用細節。ZNI完美結合SNMP、Syslog與Flow三大網管技術，效能優越、功能強大、操作親和，真正滿足現代IT管理的網路維運平台。

優勢

軟硬體完美結合

研發團隊多年專注於巨量資料的高效率收集、儲存及分析，運用自行開發的資料庫優化技術，將資料搜尋與統計排序所需時間縮減至最短。經過實際環境的驗證，統計1千萬筆Syslog Data製作成TOP 1,000報表僅需48秒鐘；而在1億筆Flow Records中找尋一個或多個特定IP，則僅耗時250秒。要完整呈現Syslog／Flow事件與流量內容，並確保正確統計結果，Syslog／Flow資料不容丟失。ZNI提供高達每秒鐘10,000筆的 Syslog Data接收效能，可接收多達500部設備的資料；最高等級Flow模組具備超過每秒鐘20,000筆以上的Flow Records接收能力，確保在任何情況都不會丟失設備輸出的資料。

同時輸入多筆查詢條件進行邏輯運算與製作報表

維運歷程中，大部分時間需要執行資料查詢。當接收的Syslog／Flow資料越來越多，必須支援彈性的搜尋條件輸入與快速查詢結果呈現，這是使用者對報表工具的基本要求。

ZNI提供智慧型查詢功能，搭配邏輯運算概念能讓使用者完成各式各樣要求的查詢工作。邏輯運算是指多個查詢條件間以聯集(Or)和排除(Not)概念建立的關聯性結果。ZNI不僅支援「事件關鍵字」的邏輯運算，使用者亦可針對「IP」選項進行邏輯運算，事件搜尋條件可以依據實際需求沒有輸入上限。

ZNI《Smart DB》提供快速查詢事件能力，讓邏輯運算機制不因執行大量條件比對，而延遲搜尋結果的呈現。

ZNI
ZyXEL Network Insight
新一代網路維運平台

ZyXEL

ZNI
ZyXEL Network Insight 新一代網路維運平台

Flow 模組進行用量分析
Flow資料在網管用量分析的角色非常重要，IT管理者藉由Flow資料了解哪個IP或單位用量最多，或者哪種Protocol佔去最多的頻寬資源等訊息。
ZNI加裝Flow模組後，可滿足IT管理者對流量分析的需求，諸如：每日用量排行、針對特定對象長期繪製流量圖、查詢特定IP或織單位的流量使用紀錄等。
除支援路由器或交換器所送出的Netflow／sFlow／Jflow等格式外，ZNI Flow模組亦可在沒有 Flow設備的環境中， 將防火牆Traffic Syslog轉換為Flow格式進行流量分析。ZNI優化Flow資料的儲存，大幅提升查詢及報表運算效能。

Syslog 與 Flow 間的關聯性整合運用
過去IT管理者需要分別建置Syslog儲存系統與Flow分析機制，以輔助網管工作或符合法規要求。但是兩套設備獨立運作，無法提供全面性的訊息，導致IT管理者在網路維運與除錯時，只能往來兩套系統反覆查詢資料，再自行比對分析，找出關聯性。
ZNI整合資安Syslog的L7使用者行為資料與Flow的L3/L4流量資訊，得到網路運作完整資訊，讓IT管理者完全掌握網路使用細節。例如，當IT管理者從Flow的 TOP-N排行發現某個IP或單位傳送大量封包，此時透過ZNI的關聯性整合功能，可以快速得知這個單位網路使用行為（例如P2P分享所產生巨量封包）。反之，從第七層資安設備提供的Syslog訊息中察覺某單位遭受DDoS攻擊，可以藉由ZNI關聯性整合功能得到DDoS攻擊流量圖，並進一步追查攻擊來源IP，以進行防禦，也可以得知DDoS對內部的影響範圍。

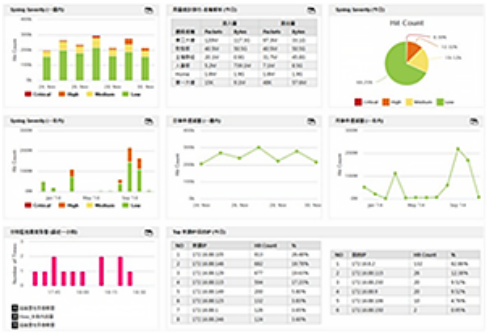
豐富多樣的即時線上報表
ZNI即時線上報表系統支援動態顯示報表內容與統計圖型。使用者可選擇π狀圖、長條圖、曲線圖等適合樣式。報表功能同樣支援邏輯運算概念(Or/Not)，使用者可根據實際狀況，邏輯結合多個過濾參數，讓報表產生結果貼近使用者的真實所需。例如伺服器遭受嚴重攻擊事件日報表、員工使用社群網站與串流影音流量週報表、資料庫存取記錄月統計等。

定期寄送離線報表
定期自動產生統計報表讓使用者無需重複手動執行報表製作與輸出。ZNI根據使用者定義的報表製作參數，將統計報表寄送到指定電子郵件帳號。
針對各類主機及資料庫系統，ZNI提供符合個資法需求的稽核(Audit)日週月報表，包含使用者登入登出、登入失敗及帳密猜測等稽核日誌報表。

自訂分時報表，提供異常監控功能
管理者可使用過濾條件定義各式分時報表，方便長期觀察事件或流量變化。透過關鍵字設定，可觀察特定事件的分時變化；例如監看「Telnet/SSH Login Fail」數量偵測是否發生帳密猜測、監看半夜連線某主機次數及流量來偵測是否異常、「Port 445」連線及流量監控來偵測是否感染蠕蟲等。 分時報表同時支援門檻值(Threshold)設定。一旦事件次數暴增或發生流量異常時，系統將主動寄發告警郵件通知管理者。
加裝Flow模組的分時報表，可於同一分時報表畫面裡，同步繪製事件、bps、pps和session的曲線圖，方便使用者交叉比對分析。

異常登入行為報表
分析全網主機登入行為，一旦察覺異常登入行為立即通知管理者，提供針對主機的第二道安全防禦，大幅降低駭客入侵成功率及造成的危害。

動態即時呈現事件統計及告警現況
ZNI提供使用者自定動態儀表板(Dashboard)，以一目瞭然的方式呈現最即時的資訊。使用者可以依需求以最適用的方式，將系統運作現況、事件統計排行、即時趨勢分析、異常告警等資訊排列在專屬儀表板即時監看。儀表板呈現的異常，也能直接以點選方式到達該頁面進一步處理。



Action模組執行聯合防禦

ZNI具備優越的即時異常分析能力，使用者可以運用分析結果，進行進階管理處置。搭配Action模組，可以快速鎖定內網的異常IP發生在交換器的哪個介面上，IT管理者就能視影響網路的嚴重程度，準確執行管制作為，讓網路立即恢復正常運作。至於來自網外的攻擊，則可將IP封鎖指令下達位於Internet入口的網路或資安設備，進行第一時間防禦。ZNI Action模組搭配即時趨勢分析功能是察覺並阻擋DDoS攻擊最有效的解決方案！

內建人工智慧，根據歷史紀錄自動產出趨勢分析報表

ZNI具備優越的即時異常分析能力，使用者可以運用分析結果，進行進階管理處置。搭配Action模組，可以快速鎖定內網的異常IP發生在交換器的哪個介面上，IT管理者就能視影響網路的嚴重程度，準確執行管制作為，讓網路立即恢復正常運作。至於來自網外的攻擊，則可將IP封鎖指令下達位於Internet入口的網路或資安設備，進行第一時間防禦。ZNI Action模組搭配即時趨勢分析功能是察覺並阻擋DDoS攻擊最有效的解決方案！

Action模組執行聯合防禦

ZNI內建人工智慧科技能根據Syslog／Flow歷史資料，自動找出發生次數、封包數或Byte數異常突增的事件或IP，並將異常突增內容主動寄發通知郵件給IT管理者，以利第一時間處置網路的異常狀況。藉由行為偵測與分析功能，使用者無需猜測與預設合理的門檻值，即可充分掌握網路值得注意的變化， 讓維運工作更輕鬆容易。ZNI不僅是功能強大的事件查詢與報表製作系統，更是能真正做到趨勢分析的維運平台。

簡單易用的操作介面與管理功能

透過Web介面即可進行操作與管理。此外，使用者亦可透過 FTP、NFS 、SMB等方式進行資料庫或復原。

功能特色

軟體功能

- 支援Web介面網路基本設定：IP Address、Gateway、DNS、NTP Server 等。
- 提供系統狀態查詢，包含運行版號、CPU使用率、記憶體使用率、Syslog／Flow資料接受量。
- 支援IPv6環境，同時適用於IPv4與IPv6雙軌運行環境。
- 不分廠牌和設備，支援各式Syslog資料蒐集。
- 提供Flow收集能力，包含Netflow V5/V9、sFlow V4/V5、JFlow等，或以防火牆TrafficLog進行流量分析。
- 支援中文Web(HTTP/HTTPS)操作介面，使用者權限可分為管理者與一般使用者。
- 提供CLI，可透過Console或SSH進行系統操作；可回復系統出廠預設值。
- Syslog接收能力高達10,000EPS以上，最高等級Flow模組接收能　力最高達每秒20,000筆Flow Records。
- 可輸入多筆查詢條件進行邏輯運算(or/not)，條件包括事件關鍵字、IP、嚴重等級等各項參數，輸入條件數無限制。
- 支援IP網段名稱解析對應功能，在事件及報表中呈現IP及網段名稱
- 不壓縮資料時，可儲存高達6億筆Syslog Data。提供資料壓縮技術，壓縮比高達8倍，大幅度提升儲存空間利用率。
- 內建Flow分析與統計功能，能自動繪製流量圖(Packet/Byte)並產生用量TOP-N表。
- 具備Flow異常流量智能分析功能，即時分析異常流量(DDoS、Host Scan、Port Scan等)。
- 支援SNMPV1/V2網路設備。
- 支援系統下達阻擋特定IP指令到網路與資安設備，進行聯防。（註：非所有品牌設備均支援本功能）
- 支援根據Syslog／Flow歷史用量自動學習建立Base Line，能即時分析異常突增事件或IP，並送出告警。
- 提供即時資安事件報表。
- 內建π型、長條、曲線圖等多種圖型式樣，可依需求客製化報表。
- 支援報表Drill Down深入查閱行為。
- 支援依工作時與工作日產生離線報表，並自動寄送至指定對象。
- 支援自訂事件呈現欄位和事件PDF輸出欄位。
- 支援自訂PDF輸出LOGO和版面。
- 支援Windows AD解析功能，可以根據事件IP解析使用者名稱。
- 支援Linux、Windows 2003、Windows 2008等主機的使用者登入登出稽核日誌報表。
- 提供異常登入行為偵測與告警。
- 支援Windows檔案分享稽核日誌報表。
- 支援資料庫備份與復原功能。
- 提供資料庫儲存天數預測功能。
- 支援Syslog原始資料（Raw data）備份。
- 提供使用者自定動態儀表板（Dashboard），即時呈現告警現況及事件統計等資訊
- 支援 Access List Control，限制可執行管理的IP白名單。
- 支援完整記錄使用者操作歷程，並提供PDF格式輸出。
- 支援獨創最新壓縮儲存技術，符合國際公認NIST800-92日誌管理標準之密碼模組SHA-256和ES-256簽章及加密原則，確保資料的完整性和不可否認性。
- 提供CPU、風扇和硬碟狀態監控，主動通知管理者異常告警。
- 支援連接外接式NFS，擴充資料儲存空間。
- 支援 SNMP Agent，提供系統運行狀況。
- 支援 SNMP Trap，提供硬體異常即時告警。
- 支援Open Interface，使用者可藉由Open Interface取得事件資訊。
- 提供彈性告警通報設定，可依不同報表或告警種類指定郵件群組。

ZyXEL

ZNI
ZyXEL Network Insight 新一代網路維運平台

硬體規格

- IEEE 802.1D 擴展樹協定 (STP)
- All-in-One Appliance，內建專屬OS、數據庫與應用程式
- Intel CPU Xeon E3-1230 V2 L3-8M 3.3GHz series processor
- 16 GB RAM DDR3 (可擴充支援32 GB ECC unbuffered (UDIMM) DDR3-1333 / 1066 memory)
- VGA Memory 8MB
- 1GB SATA DOM
- Gigabit Ethernet網路埠X2
- 19吋1U標準機架安裝
- 電源需求：100V-240V，60-50H AC
- 操作溫度：10°C～35°C；操作濕度：8%～90%（非凝結）
- 最大功耗：350 Watts
- SATA硬碟支援熱抽換，最高可擴充至8TB（2TB 7200 rpm HD X 4）

5-100-01215002 08/15