N-Reporter
DATA SHEET

new log analysis and log management tool

現今網路設備、伺服器與資安產品多能支援 Syslog 或是 Flow 流量資料的輸出功能。對 IT 人員來說，訊息完整的 Syslog Data 提供了一個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。

N-Partner 公司採用多項創新開發技術所生產的 N-Reporter 產品除了具備 Syslog/Flow 訊息蒐集、儲存、即時分析、查詢與報表製作等功能之外，其更大的特點是可以執行 Syslog 與 Flow 間的關聯性分析(Correlation)，將來自 Flow 的 L3/L4 Packet/Byte 數據與來自 Syslog 的 L7 事件內容完美結合，讓 IT 管理者完全掌握下轄網路的使用細節。N-Reporter 堪稱業界效能最優越、功能最強大、操作最親和的 Syslog 與 Flow 報表系統 + 整合分析儀(Reporter + Analyzer)。

N-Partner

2015-10-29

■軟體功能

- 使用 Web 即可進行網路的基本設定：IP Address、Gateway、DNS、NTP Server 等。
- 提供系統狀態查詢，使用者可以查詢運行版號、CPU 使用率、記憶體使用率、Syslog / Flow 資料接受量。
- 支援 IPv6 環境，同時也適用於 IPv4 與 IPv6 雙軌運行的環境。
- 不分廠牌和設備，支援各式 Syslog 資料的蒐集。
- 提供 Flow 收集的能力，如 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 (Command Line Interface)，可透過 Console 或 SSH 連線進行系統操作；Setup Page 可恢復系統的出廠值。
- Syslog 接收能力最高達 10,000EPS 以上，最高等級的 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。
- 統計 1 千萬筆 Syslog Data 的 TOP1,000 報表僅需 48 秒；搜尋 1 億筆 Flow 資料內的特定 IP 僅耗時 250 秒。
- 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 TOPN 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/V3 網路設備，系統可呈現出特定內網 IP 所在的 Switch 位置。
- 系統可下達阻擋特定 IP 指令到網路與資安設備進行聯防(註：非所有設備都支援此項功能)。
- 系統提供自動阻擋的聯防機置。可自行定義自動聯防的條件。
- 根據 Syslog/Flow 歷史用量自動學習建立 Base Line，能即時分析出發生異常突增的事件或 IP，並送出告警。
- 根據資安事件、提供即時 Security 事件報表。
- 內建圓餅、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。
- 離線報表可依工作時與工作日產生，並能設定自動寄送至指定對象。
- 可以自行訂製事件呈現的欄位和事件 PDF 輸出的欄位。
- 自訂 PDF 輸出的 LOGO 和版面。
- 提供 Windows AD 解析功能，可以將事件的 IP 解析出使用者名稱。
- 支援各類主機的使用者登入登出的稽核日誌報表：Linux、Windows server 2003 / 2008 等。
- 提供異常登入行為偵測與告警。
- 支援各類資料庫的使用者登入登出的稽核日誌報表：Oracle、MSSQL、MySQL 等。
- 支援 Windows 檔案分享的稽核日誌報表。
- 支援 WMI 方式取得 Windows Server 日誌。
- 支援資料庫備份與回復功能。
- 提供資料庫儲存天數預測功能。
- 支援 Syslog 原始的 Raw data 備份。
- 提供使用者自定動態 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。
- 完整的記錄使用者操作歷程，並提供 PDF 格式的輸出。
- 獨創最新壓縮的儲存技術，並且使用符合國際公認日誌管理標準之密碼模組 SHA-256 和 AES-256 的簽章及加密原則，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。
- 可連接外接式 NFS，擴充資料儲存空間。
- 支援 SNMP Agent，可提供系統運行狀況。
- 支援 SNMP Trap，硬體異常可以即時告警。
- 提供 Open Interface，使用者可通透 Open Interface 取得事件資訊。
- 彈性的告警通報設定，可以依不同的報表或告警種類指定不同的郵件群組。
- 與原廠保持連線狀態，可自動偵測最新韌體。

軟硬體的完美結合

N-Partner 公司 RD 團隊多年來專注於巨量資料的高效率收集、儲存以及分析領域，運用自行開發的資料庫優化技術：命名為 N-Partner《Smart DB》，可將資料搜尋與統計排序所需要的時間縮減至最短。經過實際環境的驗證，N-Reporter 統計 1 千萬筆 Syslog Data 製作成 TOP 1,000 報表僅需花費 48 秒鐘；而在 1 億筆 Flow Records 中要找尋一個或是多個特定 IP 則僅需耗時 250 秒。

若要完整呈現 Syslog/Flow 事件與流量內容並確保統計結果的正確性，Syslog/Flow 資料的接收不容丟失。N-Reporter 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，能確保在任何情況下都不會丟失設備所輸出的 Syslog 資料；而最高等級的 Flow 模組則具備超過每秒鐘 20,000 筆以上的 Flow Records 接收能力。

除了能夠擁有高速與穩定的處理效能之外，提供簡易的維修程序亦是產品以 Appliance 架構問世的主要考量。保固期間內若硬體損壞 N-Partner 公司將以整機 RMA 方式處理，免去除錯時間的浪費。

■ 硬體功能

- ▸ All-in-One Appliance，內建專屬 OS、數據庫與應用程式
- ▸ Intel CPU Xeon E3-1231 V3 L3-8M 3.4GHz series processor
- ▸ 16 GB RAM DDR3 (supports to 32 GB of ECC unbuffered (UDIMM) DDR3-1333 / 1066 memory)
- ▸ VGA Memory 8MB
- ▸ 1GB SATA DOM
- ▸ Gigabit Ethernet ports X 2
- ▸ 1U rackmount，19 Inch Standard Wide Rack Mount Industry Server
- ▸ 100V-240V，60-50Hz AC power, Operating Temperature: 10º to 35º C (50º to 95º F),Operating Relative Humidity: 8% to 90% (non-condensing)
- ▸ Maximum Power Consumption: 350 Watts
- ▸ SATA Drives with hotswap capability, up to 4 drivers (2TB 7200 rpm HD X 4)
- ▸ Connector : USB0/1
- ▸ RAID module(optional) support levels 0, 1 and 5, up to 6T storage space

同時輸入多筆查詢條件 進行邏輯運算與製作報表

在維運的歷程中，資料查詢是大部分時間裡所需執行的工作。當接收的 Syslog/Flow 資料越來越多時，能夠支援彈性的搜尋條件輸入與快速的查詢結果呈現是使用者對報表工具的基本要求。

N-Reporter 提供智慧型的查詢功能，搭配邏輯運算概念能夠讓使用者完成各式各樣要求下的查詢工作。

事件呈現欄位及可輸入的過濾參數選項

根據 Syslog 查詢或是根據 Flow 查詢
設備 (支援單一設備或跨設備查詢)
設備的介面
時間
事件關鍵字
使用者名稱
來源 / 目的 IP(支援 CIDR 與不連續區段)
來源 / 目的 Port
來源 / 目的國家
事件嚴重等級
事件類型 (Security、Traffic、Audit、Web 等)
事件處置動作 (Block、Permit 等)
Policy ID

所謂的邏輯運算指的是多個查詢條件間以聯集 (Or) 和排除 (Not) 概念所建立的關聯性結果。舉例來說：在「事件關鍵字」的條件中採用聯集 (Or) 可以查詢多個關鍵字相關事件，或用排除 (Not) 過濾掉不想查看的事件。

N-Reporter 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。以下說明幾個操作範例：

事件關鍵字

P2P+Streaming:
表示欲同時查找含有 P2P 或是 Streaming 關鍵字的所有事件。

P2P+Streaming! BT:
表示欲同時查找含有 P2P 或是 Streaming 關鍵字的所有事件，但是需要排除 BT。

IP

192.168.1.0/24+192.168.2.0/24
表示欲同時查找這兩個網段的所有事件。

192.168.1.0/24+192.168.2.0/24
!192.168.1.100-192.168.1.200
表示欲同時查找這兩個網段的所有事件，但是過濾掉 192.168.1.100-192.168.1.200 這個區段的事件。

事件搜尋條件可以依據實際需求沒有上限的輸入，N-Partner《Smart DB》同樣給予 N-Reporter 快速查詢事件的能力，讓邏輯運算機制不會因執行大量條件比對而延遲搜尋結果的呈現。

Flow 模組進行用量分析

Flow (ex：Netflow/sFlow) 資料在網管工作中經常扮演用量分析的重要角色，IT 管理者藉由 Flow 資料了解哪個 IP 或是哪個組織單位用量最多；哪種 Protocol (ex：Port 80、Port 21) 佔去最多的頻寬資源等訊息。

N-Reporter 加裝 Flow 模組後可滿足上述 IT 管理者對於 Flow 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 或是組織單位的流量使用紀錄等。

N-Reporter 的 Flow 模組除了支援路由器或交換器所送出的 Netflow/sFlow/Jflow 等格式之外，亦可在沒有 Flow 設備的環境中，將防火牆送出的 Traffic Syslog，轉換為 Flow 格式進行流量分析。N-Reporter 針對 Flow 資料的儲存進行優化，可以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 分析機制作為輔助網管工作或是符合法規要求之用。但是獨立運作的兩套設備所提供的訊息都不是全面性的，導致 IT 管理者在執行網路維運與除錯時只能往來兩套系統反覆查詢資料後，再自行比對分析找出可能的關聯性。

N-Reporter 能整合資安 Syslog 中的 L7 之使用者行為資料與 Flow 的 L3/L4 流量資訊，得到網路運作完整資訊，讓 IT 管理者完全掌握管轄網路的使用細節。例如：當 IT 管理者從 Flow 的 TOPN 排行中發現某個 IP 或是單位傳送了大量的封包，此時透過 N-Reporter 的關聯性整合功能可以快速得知這個單位的網路使用行為是甚麼內容：原來是 P2P 分享所產生巨量封包。反過來看：從第七層資安設備丟出的 Syslog 訊息中察覺到單位正遭受到 DDoS 攻擊，藉由 N-Reporter 的關聯性整合功能可以得到 DDoS 攻擊流量圖，並可以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

N-Reporter 的即時線上報表系統支援動態顯示報表內容與統計圖型。使用者可依據喜好選擇適合的圖型樣式，包括：圓餅圖、長條圖、曲線圖等。報表功能同樣支援邏輯運算概念(Or/Not)，使用者可根據各種實際的狀況邏輯結合多個過濾參數，讓報表產生的結果更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的流量週報表；資料庫存取記錄月統計等。

報表製作參數包括

事件關鍵字、來源及目的 IP、Port 等過濾條件及統計欄位

工作時段 (每日統計資料時段，如 8:00~18:00)

工作日 (可限定只統計週一到週五)

報表型態 (日報、週報、半月報、月報、 季報、半年報與年報)

定期寄送時間

指定的報表收件者

報表格式 (HTML、PDF、 XML、CSV)

離線報表定期寄送

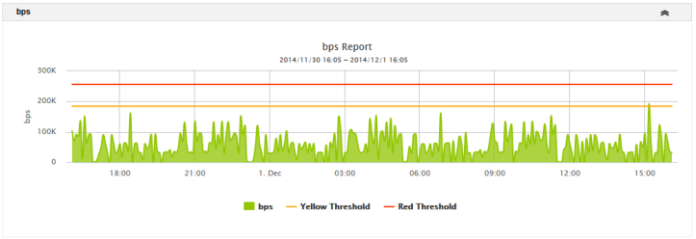
定期自動產生統計報表讓使用者無需每日手動執行報表製作與輸出的工作。N-Reporter 將根據使用者所定義的報表製作參數，寄送統計報表到指定的電子郵件帳號。

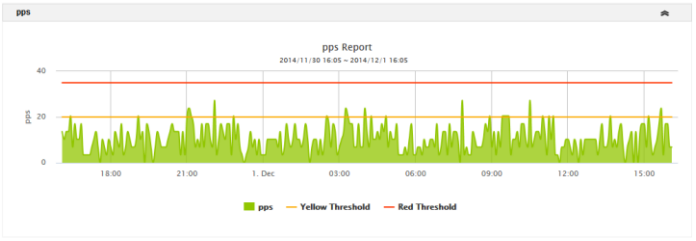
N-Reporter 針對各類主機及資料庫系統，提供符合個資法需求的稽核 (Audit) 日週月報表，包含使用者登入與登出、登入失敗及帳密猜測等稽核日誌報表。

自訂分時報表，並提供異常監控功能

管理者可使用過濾條件來定義各式的分時報表，方便長期觀察事件或是流量的變化。透過關鍵字的設定，可觀察特定事件的分時變化；例如監看「Telnet/SSH Login Fail」數量來偵測是否有帳密猜測、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。 分時報表同時也支援門檻值 (Threshold) 的設定。如此只要事件次數暴增，或者發生流量異常時，系統將主動寄發告警郵件通知管理者。

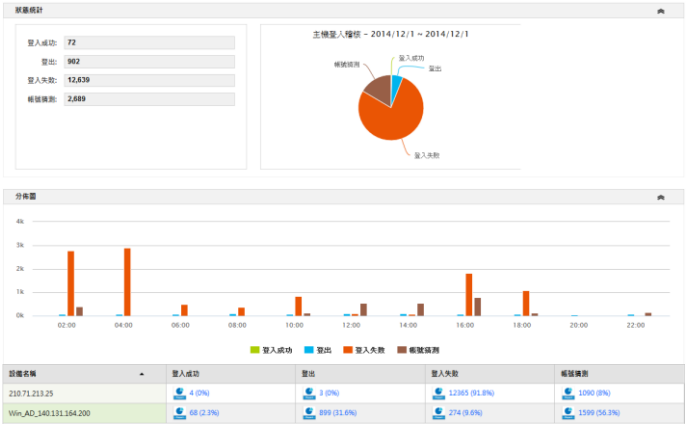
加裝 Flow 模組的分時報表，可以在同一個分時報表畫面裡，同步繪製事件、bps、pps 和 session 的曲線圖方便使用者進行交叉比對分析。





異常登入行為報表

分析全網的主機登入行為，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，大幅減少駭客入侵成功率及所造成的危害。



▲主機稽核報表，追踪主機的登入/登出/帳密猜測次數及發生時間

智能稽核功能

帳號密碼猜測

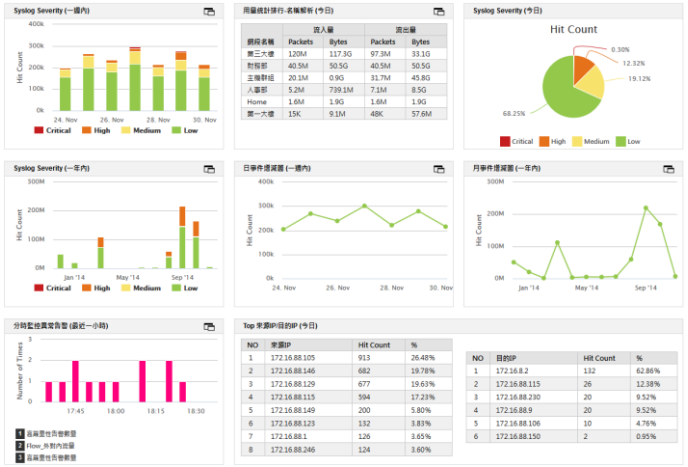
可疑 IP 登入成功

改變登入 IP

Dashboard：
動態即時呈現事件統計及告警現況

N-Reporter 提供使用者自定動態 Dashboard，以一目瞭然的方式提供最即時的資訊。

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的儀表板上，進行即時的監看。Dashboard 上所呈現的異常，也能直接以點選的方式到達該頁面進一步處理。



Action 模組執行聯合防禦

N-Reporter 擁有優越的即時異常分析能力，使用者可以運用這些有用的分析結果進行更進階的管理處置。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 管理者就能夠視影響網路的嚴重程度準確地執行更進一步的管制作為，讓網路立即恢復正常運作。至於來自網外的攻擊，則可將 IP 封鎖指令下達至位於 Internet 入口處的網路或是資安設備，進行第一時間的防禦。

使用者也可以根據事件的關鍵字、定義自動阻擋的條件。系統即可主動分析定義的條件，一旦條件達到門檻值時，自動阻擋該異常的 IP 於聯防的設備上。

N-Reporter 的 Action 模組搭配即時趨勢分析功能是發掘並阻擋 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

N-Reporter 內建的人工智慧科技能根據蒐集到的 Syslog/Flow 歷史資料自動找出發生次數、Packet 數或 Byte 數異常突增的事件或 IP，並將發生異常突增的內容主動寄發通知郵件給 IT 管理者以利於第一時間處置網路中的的異常狀況。藉由 Behavior Based 偵測與分析功能，使用者無需猜測與預設合理的門檻值，即可充分掌握網路環境裡值得注意的變化，讓維運工作顯得更輕鬆容易。N-Reporter 不僅是功能強大的事件查詢與報表製作系統，更是一部能真正做到趨勢分析的 Analyzer。

簡單易用的操作介面與管理功能

透過 Web 介面即可進行 N-Reporter 的操作與管理。此外，使用者亦可以將 N-Reporter 資料庫中的資料透過以下方式進行備份或是回復： FTP、NFS 、SMB

Syslog 與 Flow 轉發功能

使用者可以自行定義將收到的 Syslog 轉發至第三方設備。也提供 Flow 的轉發功能。

通過 NIST CAVP 密碼模組

通過符合國際公認推薦密碼模組 FIPS 140-2，並使用 AES & SHA 的加密原則，確保資料的完整性和不可否認性。

http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html#2416
http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.htm#2073

採購與銷售合作：sales@npartnertech.com

技術諮詢：support@npartnertech.com

TEL: +886-4-23752865

FAX: +886-4-23757458