

# NetAuditor

Network Traffic Analyzer

Datasheet

## 主要功能

### ◆ 流量統計

提供來源/目的 IP、時間、封包大小、服務埠等資訊，並可依時間進行過濾及呈現。

### ◆ 自訂群組流量統計

提供將流量依分區或使用群組進行分類，方便管理者依群組進行流量統計。

### ◆ 異常行為分析

流量過高、連線數過多、疑似中毒等的行為告警與紀錄。

### ◆ 支援 Snort 規則

管理者可根據企業內的資安需求，自行匯入與調整規則內容。

### ◆ 多樣化權限

可依據管理所需，新增/修改角色權限，並指派各個管理員權限。

### ◆ 系統狀態資訊

### ◆ 系統備份與還原

### ◆ 韌體更新

簡易並且快速的更新機制，只需透過網頁上傳即可完成更新。

NetAuditor 是專業級的網路流量分析解決方案，可協助您瞭解企業內部網路流量的使用狀態和用戶端的使用習慣，並提供簡易又有彈性的操作介面，讓您能快速的查詢及分析流量資料。NetAuditor 幫您隨時掌握網路流量的即時狀態，管理者可由此提供的分析資訊，運用來提升網路頻寬的使用效能及傳輸品質。

NetAuditor 利用持續不斷的高速擷取技術，無時無刻監聽及分析企業整體的網路流量，進而統整提供多項記錄功能，包含網路頻寬使用率(包含主機端對內、對外或特定服務的流量)、曾到訪的 Web 統計分析、網路傳輸量分析...等。並依據臨界值的設定，當網路出現符合監控規則的異常行為，或是流量傳輸行為在某時段超過允許臨界值時，系統會自動且快速的產出警訊統計及列表，讓管理者能第一時間得知網路異常行為的活動。

## 產品特色：

- ✓ 同時支援 IPv4 及 IPv6 解析
- ✓ 異常事件的判斷與告警
- ✓ 管理者與群組權限自訂化
- ✓ 高速擷取分析能力
- ✓ 群組、主機、服務流量分析
- ✓ 中、英文語系介面

## What

• 由Mirror、sFlow或NetFlow導入的流量中取得IP相關資訊，包含Source/Destination的IP、Port、Protocol...等相關資訊。

## When

• 針對每一筆記錄的連線資訊，提供其發生時間點。

## Where

• 由系統定義的分區設定及使用者群組設定，將IP分佈在那些分區及屬於那些使用者群組進行分類，以方便視別。

## How

• 即時依設定的Snort規則檔，比對封包特徵，或依流量臨界值設定，監測是否超過設定限額，將其紀錄在統計資料及警報列表。

# NetAuditor

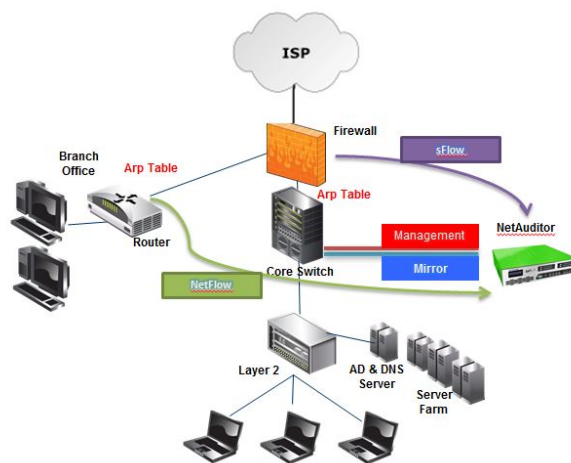


## ❖ 連線總覽

提供即時流量/連線數據統計分析資訊，亦可利用時間區段、使用者群組、通訊協定等多種過濾選項，進行篩選及呈現；透過簡易直覺的圖形介面，MIS 人員可馬上瞭解企業內部網路的使用狀態，如：TopN 的用戶端、網路的對內、對外數據，以及尖峰時段的內部網路使用行為等，進而得知網路資源的分配狀態。

## ❖ 支援多種資料來源

接收 Port Mirror 導入的流量進行分析，其流量亦可用於 Snort 異常分析，依據匯入/自訂的規則來即時判斷是否有網路攻擊行為，另外同時支援接收並分析由路由器、交換器或防火牆等設備導出 Netflow 或 Sflow 格式的流量。透過以上功能可以全面涵蓋外點或分公司的流量統計與分析，無需另外加裝硬體或軟體代理設備。



IP 位址	對內	對外	內部	總覽		
10.1.1.118	65.6 MB	1.4 MB	15.7 KB	67.0 MB		
10.1.1.105	20.6 MB	1.1 MB	19.3 KB	21.7 MB		
10.1.1.115						
10.1.1.112						
10.1.1.111						
10.1.1.245						
10.1.1.112						
10.1.1.243						
10.1.1.112						
10.1.1.106						
10.1.1.123						
10.1.1.111	10.1.1.118	123.205.250.81	外部	0.8 MB	45.9 MB	46.7 MB
10.1.1.245	10.1.1.118	139.175.107.17	外部	485.2 KB	27.8 MB	28.3 MB
10.1.1.112	10.1.1.118	139.175.107.14	外部	323.1 KB	18.2 MB	18.5 MB
10.1.1.243	10.1.1.118	139.175.107.99	外部	90.3 KB	320.2 KB	410.4 KB
10.1.1.112	10.1.1.118	139.175.107.29	外部	5.8 KB	82.5 KB	88.4 KB
10.1.1.106	10.1.1.118	74.125.204.19	外部	15.1 KB	37.4 KB	52.4 KB
10.1.1.111	10.1.1.118	139.175.107.39	外部	45.8 KB	3.3 KB	49.0 KB
10.1.1.111	10.1.1.118	139.175.107.108	外部	28.5 KB	12.3 KB	40.8 KB
10.1.1.111	10.1.1.118	239.255.255.250	外部	36.0 KB	0	36.0 KB
10.1.1.111	10.1.1.118	139.175.107.103	外部	1.6 KB	33.2 KB	34.8 KB

## ❖ 歷史記錄/報表

內含總覽記錄、主機排行記錄、使用者群組記錄、通訊協定記錄、TCP/UDP 埠號記錄...等，多種查詢報表，內容包括來源 IP、目的 IP、通訊埠、通訊協定、對內、對外...等，並可依各種需求自訂搜尋條件，取得專屬的紀錄、報表資訊。



一休資訊科技股份有限公司

新北市三重區 241

重新路五段 609 巷 4 號 4 樓

電話：02-7716-8868 / 傳真：02-2999-8440

EQ Information Technologies Inc.

New Taipei City 241, Taiwan

4<sup>th</sup> Floor, No.4, Ln.609, Sec.5, Chongxin Rd, Sancong

TEL:886-2-7716-8868 / FAX:886-2-2999-8440