台北海洋技術學院

Taipei College of Miritime Technology

103 年 ISO-Shaper 網路行為管理設備講習

時間:103 年 4 月 11 日下午 13:00~17:00

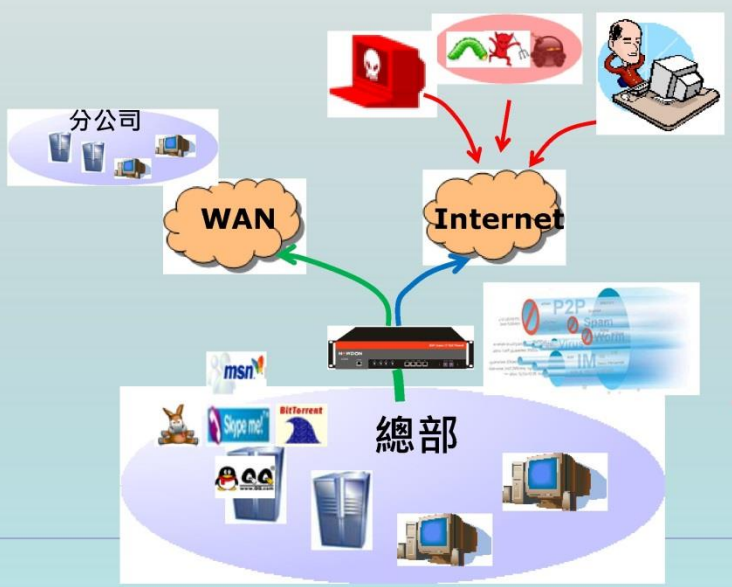
地點:台北海洋技術學院圖書館會議室

講師: 王智民 先生

正邦資訊科技股份有限公司
ISO-Shaper網路行為管理設備
2011

第七層 頻寬與內容管理防火牆

ISOshaper 的用途

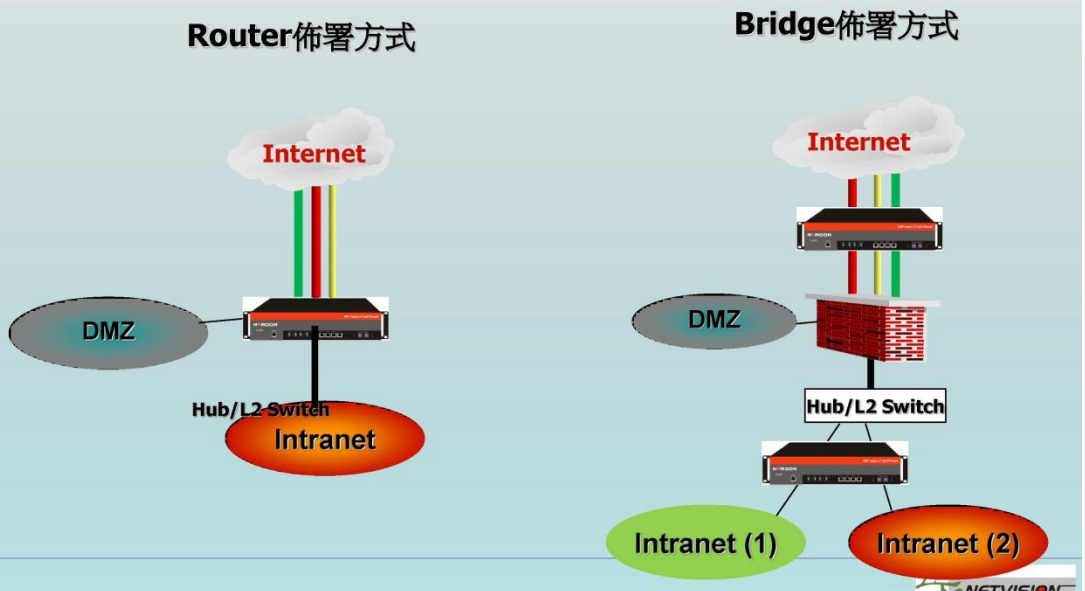


- 駭客,間諜,竊取和入侵
- DDOS攻擊和木馬
- 網路病毒和垃圾
- 內部非法入侵,越權操作
- 內部感染，傳播和攻擊
- P2P肆意占用工作頻寬
- IM洩密和影響工作
- 不良網站和瀏覽

ISO shaper 第七層 頻寬與內容管理防火牆

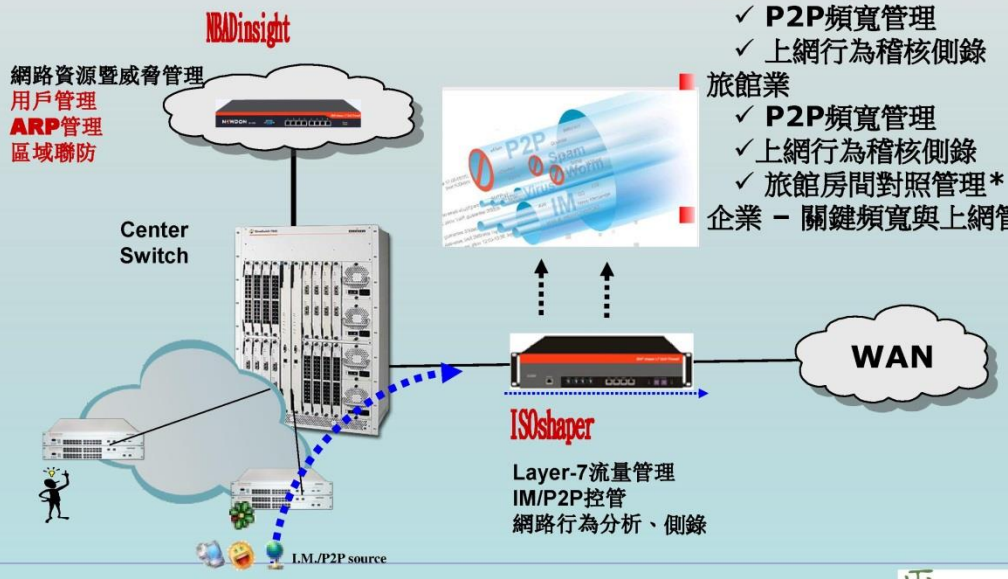
- **Network Security System**
  - VPN系統
  - 防火牆系統
- **L7 Traffic Management System**
  - 寬頻負載平衡系統 (Multi-Homed)
  - L7頻寬管理系統 (L7 P2P application QoS)
  - 流量分析與額度管理系統 (Top-N & Quota)
- **L7 application management System**
  - 上網行為管理(IM control)
  - 上網目的過濾(URL filter)
  - 上網內容側錄(Content Recorder)

路由器或橋接器部署(Router/Bridge)



ISOshaper 市場應用

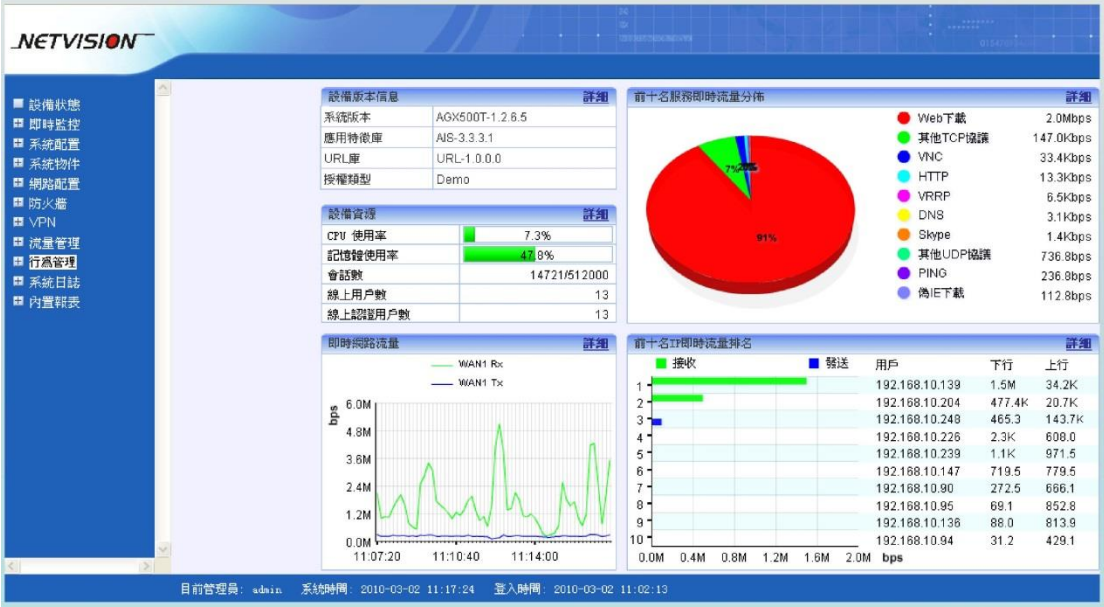
- 教育市場 – 國中小、大專
  - ✓ P2P頻寬管理
  - ✓ 上網行為稽核側錄
- 旅館業
  - ✓ P2P頻寬管理
  - ✓上網行為稽核側錄
  - ✓ 旅館房間對照管理*
- 企業 – 關鍵頻寬與上網管制



ISO-Shaper系列 優勢為何 ?產品定義是什麼 ?!

- 3A 認証,授權,計費
- Network Access Ctrl(存取)
- 控制 Source/Dest Session
- 控制 In/Outbound Qos
- 控制P2P,Stream,IM,Skype
- 控制 Service Bandwith
- 提供NAT/PAT 多對多功能
- 提供Bridge mode/Routing Mode
- 提供完整Report 統計功能
- 支援網頁過濾(URL DB)
- 支援群組權限管理(AD/LDAP)
- 支援多重認証方式
  - ✓ Web , MAC , IP , MAC+IP , VLAN ID
- 提供黑名單管制機制
  - ✓ Quota(可設 日/週/月)
  - ✓ Session(持續時間超過定義值)
  - ✓ Rate Bandwith(持續時間超過定義值)
- 黑名單提供三種懲罰模式
  - ✓ Offline(會通知user)
  - ✓ 修改來源/目的Session
  - ✓ 修改上傳/下載Bandwith
  - ✓ 可定義Day & Min 懲罰時段

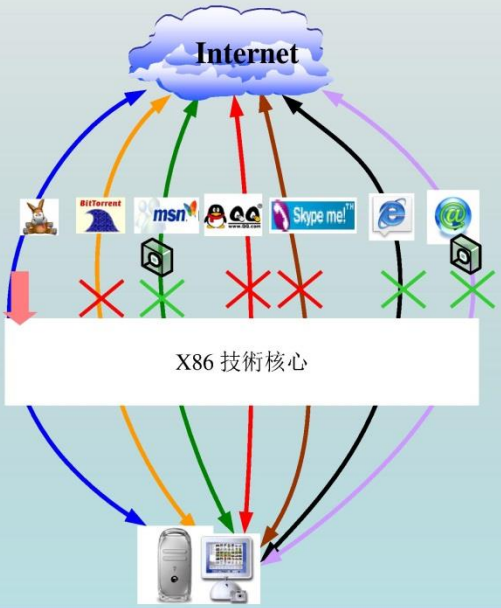
親和力管理首頁(網路狀態)



ISO系列 P2P 技術及如何解決空窗期

市面上P2P 控制技術	TCP/UDP port control	Session limit	Client Bandwidth Control	應用 Application control
Detect P2P behavior?	No	Certain degree	No	Yes
Type of P2P application recognition	No	No	No	Yes
P2P bandwidth control capabilities	No	No	No	Yes
P2P blocking	Not Really	No	No	Yes
New P2P application control support	No	Certain effect	Certain effect	Upgradeable
Ease of deployment	Easy	Difficult	Difficult	Difficult
Current P2P appliance Vendor	Yes for some	Not Really	No	Yes
x86 P2P Control appliance	Yes	Yes	Yes	Yes

網路應用內容和行為的安全管理



限速,限制連接數

部分行為限制

完全限制

監控紀錄

允許MSN聊天，不允許傳文件和視訊．
允許WEB瀏覽，不允許Email．
允許收發Email，允許附加附件．
允許使用P2P，但是限制流量．

P2P/IM/VoIP/Stream 進階管理應用

編號	服務名稱	最新速率(bps)	最近一小時總流量(Byte)	最近一小時平均速率(bps)	操作
1	TCP_ALL	↑ 682.1K, ↓129.4K	↑ 973.1M, ↓ 811.7M	↑ 2.2M, ↓1.8M	趨勢圖
2	UDP_ALL	↑ 527.9K, ↓139.2K	↑ 347.7M, ↓ 2.5G	↑ 772.7K, ↓5.6M	趨勢圖
3	DNS	↑ 567.2, ↓523.2	↑ 424.2K, ↓ 902.9K	↑ 942.6, ↓2.0K	趨勢圖
4	HTTP	↑ 39.4K, ↓57.9K	↑ 36.0M, ↓ 337.3M	↑ 80.0K, ↓749.7K	趨勢圖
5	PING	↑ 1.0K, ↓888.0	↑ 665.7K, ↓ 616.0K	↑ 1.5K, ↓1.4K	趨勢圖
6	ICMP_Timeout	0.0	0	0.0	趨勢圖
7	ICMP_Unreach	0.0	0	0.0	趨勢圖
8	ICMP_ALL	↑ 1.0K, ↓1.0K	↑ 672.8K, ↓ 1.6M	↑ 1.5K, ↓3.5K	趨勢圖
9	SMTP	↑ 210.4, ↓362.4	↑ 43.5K, ↓ 82.2K	↑ 96.7, ↓182.7	趨勢圖
10	POP3	0.0	↑ 24.6K, ↓ 54.7K	↑ 54.7, ↓121.6	趨勢圖
11	Lotus_Notes	0.0	0	0.0	趨勢圖
12	IMAP	0.0	0	0.0	趨勢圖
13	FTP	0.0	↑ 5.8K, ↓ 5.8K	↑ 12.8, ↓12.9	趨勢圖
14	TFTP	0.0	0	0.0	趨勢圖
15	Telnet	0.0	↑ 20.0K, ↓ 126.0K	↑ 44.5, ↓280.1	趨勢圖
16	SSH	0.0	0	0.0	趨勢圖
17	SSL	0.0	↑ 1.1M, ↓ 1.9M	↑ 2.4K, ↓4.2K	趨勢圖

◆P2P全部、群組、用戶(or IP)等的限制與允許

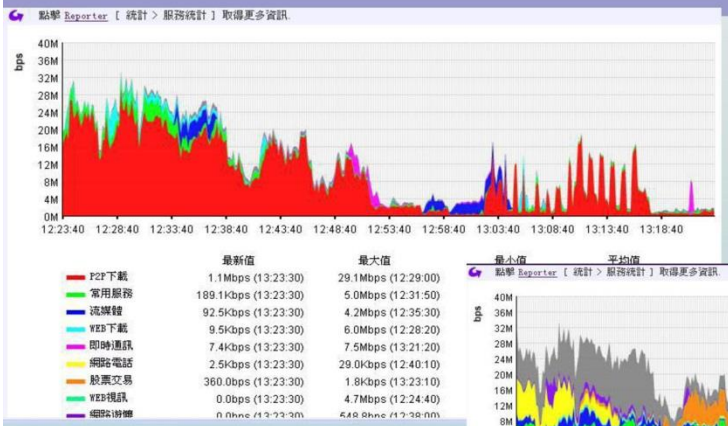
◆P2P全部、群組、用戶(or IP)等的Qos限制(UP,Down,Total)

◆P2P全部、群組、用戶(or IP)等的New Session限制

Online Game也可以管理

編號	名稱	說明
1	QQ遊戲	騰訊开发的基於QQ遊戲平臺下的以休閒遊戲爲主的遊戲
2	穿越火線	騰訊公司代理運營的一款網絡槍戰遊戲大作
3	QQ飛車	騰訊公司設計的飛車網絡遊戲
4	QQ音速	騰訊公司代理運營的"K-體育新時代"運動音樂休閒類網絡遊戲
5	QQ自由幻想	騰訊公司開發的一款大型多人MMORPG網絡遊戲
6	QQ堂	騰訊公司在2004年底開發出的一款休閒遊戲
7	英雄島	網域開發的DOTA系列遊戲所運營的大型卡通風格的戰略RPG新形態網酷遊戲
8	QQ炫舞	騰訊聯合永航科技開發的一款音樂舞蹈遊戲
9	尋仙	騰訊公司運營的一款中國美術片風格的網絡遊戲
10	QQ幻想	騰訊公司2005年度推出的一款以打怪練級爲主要升級途徑的點卡收費制2D網絡遊戲
11	QQ劇歌平臺	騰訊公司所投資開發的綠合性的網絡遊戲平臺
12	QQ西遊	騰訊推出的一款以中國四大經典名著《西遊記》爲藍本的3DMMORPG
13	地下城与勇士	騰訊運營的一款橫版格鬥過關式網絡遊戲
14	QQ三國	騰訊研發的第一款橫版MMORPG遊戲
15	熱血傳奇	盛大公司從韓國引進的基於 Internet 網路的線上角色扮演遊戲
16	傳奇世界	盛大公司推出的熱血傳奇兄弟篇
17	傳奇世界	盛趣技術有限公司開發，由盛大網路服務運營的奇幻動作類 MMORPG 網路遊戲
18	穿越Online	盛大公司運營的首款穿越題材網絡遊戲
19	功夫小子	盛大公司開發的一款格斗網絡遊戲
20	彩虹島	Actoz公司開發的一款集副本、格鬥、寵物等眾多遊戲要素的休閒遊戲
21	夢幻國度	盛大網絡研發的第一款大型卡通2D網絡角色扮演類遊戲
22	龍神傳說	盛大公司研發的一款由頂級漫畫家繪畫原畫設定的2D MMORPG網遊

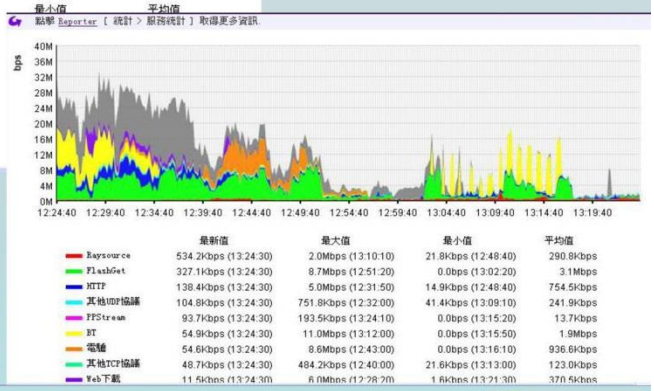
網路服務流量監視及N Top 流量排行



圖表可以明確了解網路流量狀況,對於實際應用有很大幫助

各種類服務流量數據

Service 頻寬流量管制

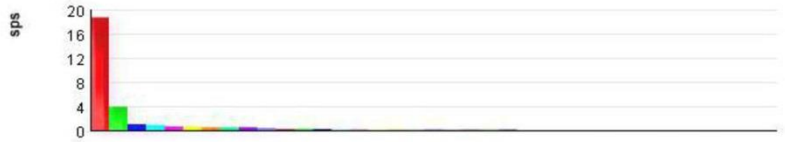


即時顯示前10名-Session 量及傳輸量排名(By ip/Username)

編號	IP 位址	用戶名	使用者群組	總	上行	下行	操作
1	172.16.3.41	zhang	软件組	677	450	227	趨勢圖 線上服務
2	172.16.3.72	172.16.3.72	软件組	608	608	0	趨勢圖 線上服務
3	172.16.3.172	172.16.3.172	软件組	204	204	0	趨勢圖 線上服務
4	172.16.3.113	172.16.3.113	软件組	62	59	3	趨勢圖 線上服務
5	172.16.3.121	172.16.3.121	软件組	45	45	0	趨勢圖 線上服務
6	172.16.161.252	172.16.161.252	其他	41	41	0	趨勢圖 線上服務
7	172.16.161.26	172.16.161.26	其他	37	37	0	趨勢圖 線上服務
8	172.16.5.5	172.16.5.5	Root	35	35	0	趨勢圖 線上服務
9	172.16.3.30	172.16.3.30	软件組	34	34	0	趨勢圖 線上服務
10	172.16.161.196	172.16.161.196	其他	30	30	0	趨勢圖 線上服務
11	172.16.5.92	172.16.5.92	測試部	29	29	0	趨勢圖 線上服務
12	172.16.3.27	172.16.3.27	软件組	23	23	0	趨勢圖 線上服務
13	172.16.2.2	172.16.2.2	其他	20	20	0	趨勢圖 線上服務
14	172.16.3.63	172.16.3.63	软件組	19	19	0	趨勢圖 線上服務
15	172.16.3.154	172.16.3.154	软件組	14	14	0	趨勢圖 線上服務

即時顯示前10名- New Session 量及傳輸量排名(By ip/Username)

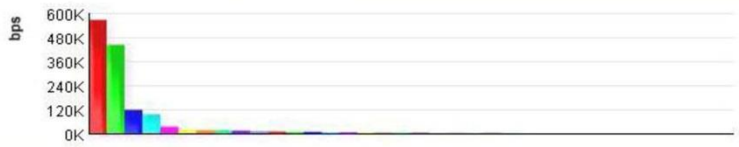
點擊 Reporter [統計 > IP 統計 > 新建會話] 取得更多資訊.



編號	IP 位址	用戶名	使用者群組	總 (sps)	上行 (sps)	下行 (sps)	操作
1	172.16.3.72	172.16.3.72	软件組	18.7	18.7	0.0	趨勢圖 線上服務
2	172.16.3.41	zhang	软件組	3.9	3.9	0.0	趨勢圖 線上服務
3	172.16.3.172	172.16.3.172	软件組	1.0	1.0	0.0	趨勢圖 線上服務
4	172.16.3.121	172.16.3.121	软件組	0.9	0.9	0.0	趨勢圖 線上服務
5	172.16.161.252	172.16.161.252	其他	0.6	0.6	0.0	趨勢圖 線上服務
6	172.16.3.113	172.16.3.113	软件組	0.6	0.6	0.0	趨勢圖 線上服務
7	172.16.2.2	172.16.2.2	其他	0.5	0.5	0.0	趨勢圖 線上服務
8	172.16.3.7	172.16.3.7	软件組	0.5	0.5	0.0	趨勢圖 線上服務
9	172.16.161.26	172.16.161.26	其他	0.5	0.5	0.0	趨勢圖 線上服務
10	172.16.3.30	172.16.3.30	软件組	0.4	0.4	0.0	趨勢圖 線上服務
11	172.16.5.130	172.16.5.130	测试部	0.2	0.2	0.0	趨勢圖 線上服務
12	172.16.3.63	172.16.3.63	软件組	0.2	0.2	0.0	趨勢圖 線上服務
13	172.16.3.13	172.16.3.13	软件組	0.2	0.2	0.0	趨勢圖 線上服務
14	172.16.161.196	172.16.161.196	其他	0.1	0.1	0.0	趨勢圖 線上服務
15	172.16.3.27	172.16.3.27	软件組	0.1	0.1	0.0	趨勢圖 線上服務

即時顯示前10名-Rate 量及傳輸量排名(By ip/Username)

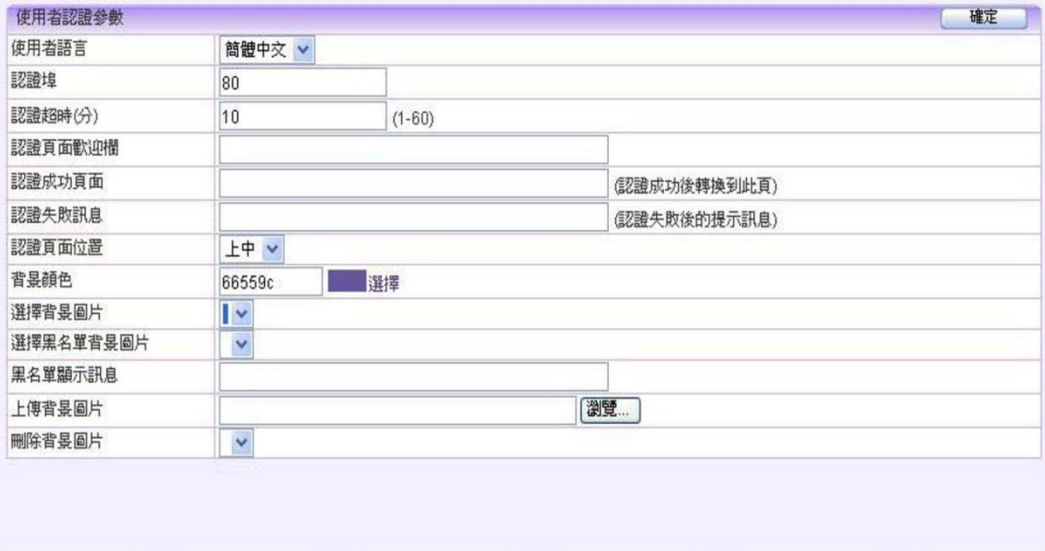
點擊 Reporter [統計 > IP 統計 > 流量統計] 取得更多資訊.



編號	IP 位址	用戶名	使用者群組	總 (bps)	上行 (bps)	下行 (bps)	操作
1	172.16.3.113	172.16.3.113	软件組	567.4K	542.5K	25.0K	趨勢圖 線上服務
2	172.16.3.41	zhang	软件組	440.3K	321.8K	118.5K	趨勢圖 線上服務
3	172.16.3.13	172.16.3.13	软件組	116.6K	108.7K	7.9K	趨勢圖 線上服務
4	172.16.3.72	172.16.3.72	软件組	94.1K	0.0	94.1K	趨勢圖 線上服務
5	172.16.3.30	172.16.3.30	软件組	33.5K	29.1K	4.4K	趨勢圖 線上服務
6	172.16.5.130	172.16.5.130	测试部	16.7K	10.0K	6.7K	趨勢圖 線上服務
7	172.16.3.32	172.16.3.32	软件組	14.5K	1.4K	13.1K	趨勢圖 線上服務
8	172.16.3.172	172.16.3.172	软件組	14.3K	4.9K	9.4K	趨勢圖 線上服務
9	172.16.3.27	172.16.3.27	软件組	13.5K	7.7K	5.8K	趨勢圖 線上服務
10	172.16.3.63	172.16.3.63	软件組	10.8K	1.2K	9.7K	趨勢圖 線上服務
11	172.16.5.92	172.16.5.92	测试部	8.5K	1.5K	7.0K	趨勢圖 線上服務
12	172.16.161.252	172.16.161.252	其他	7.5K	1.9K	5.6K	趨勢圖 線上服務
13	172.16.8.21	172.16.8.21	硬件組	7.2K	2.3K	4.8K	趨勢圖 線上服務
14	172.16.3.7	172.16.3.7	软件組	6.4K	1.6K	4.8K	趨勢圖 線上服務
15	172.16.3.154	172.16.3.154	软件組	6.3K	3.0K	3.4K	趨勢圖 線上服務

3A內容各項設定(群組繼承觀念，認証模式)

3A內容各項設定(定義Web login 資訊)



基本設定說明

- 登入設備
- 橋接模式運作範例
- 路由模式運作範例
- 流量管理運作範例
- 行為管理認證策略運作範例
- Reporter 報表查詢

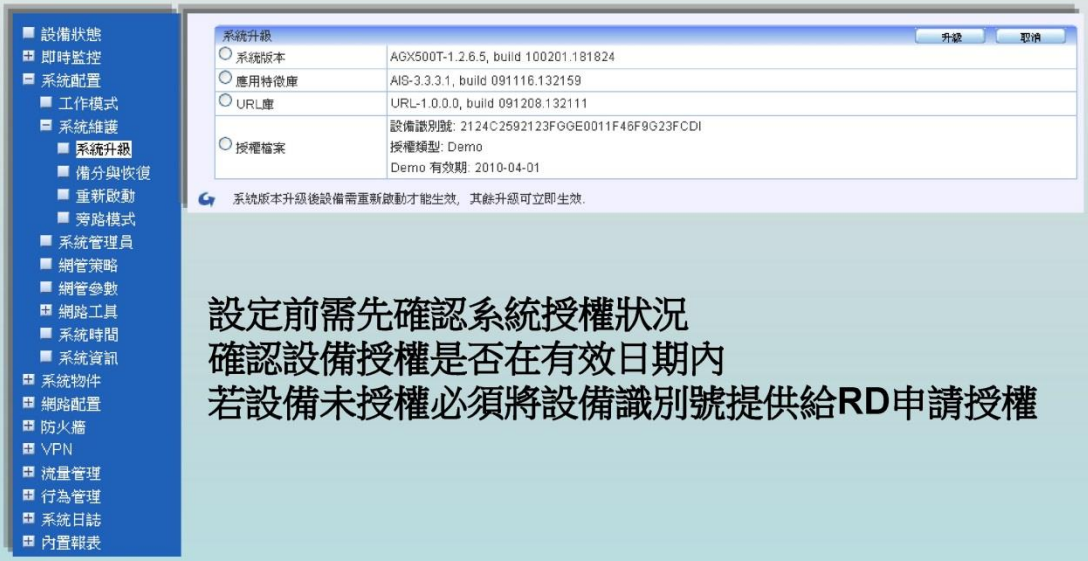
1. 登入設備

設備預設使用 LAN1 作為網管介面，LAN1 出廠IP位址為192.168.0.1/24。

URL：https:// 192.168.0.1:9090

系統預設使用 HTTPS 的登錄方式，預設的管理員帳號是admin，密碼是admin*PWD。正確輸入用戶名和密碼後， <登錄>按鈕即可進入管理介面。

授權狀況確認



設定前需先確認系統授權狀況

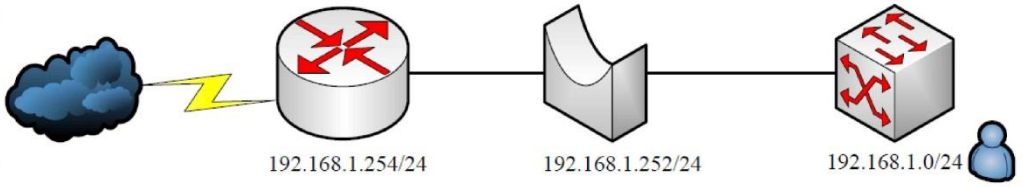
確認設備授權是否在有效日期內

若設備未授權必須將設備識別號提供給RD申請授權

2. 橋接模式運作範例

功能描述：

橋接模式是把 設備 視爲一條帶過濾功能的網路線使用，把設備接在原有閘道及內網使用者之間，不用更改網路架構和設定，這種模式於使用者可以做到完全“透明”。如下圖所示：



設定步驟：

1. [系統組態] → [工作模式] 在 <橋接器類型>中選擇希望設定的橋接 port，點選<確定>按鈕。

設定步驟：

1. [系統組態] → [工作模式] 在 <橋接器類型>中選擇希望設定的橋接 port，點選<確定>按鈕。

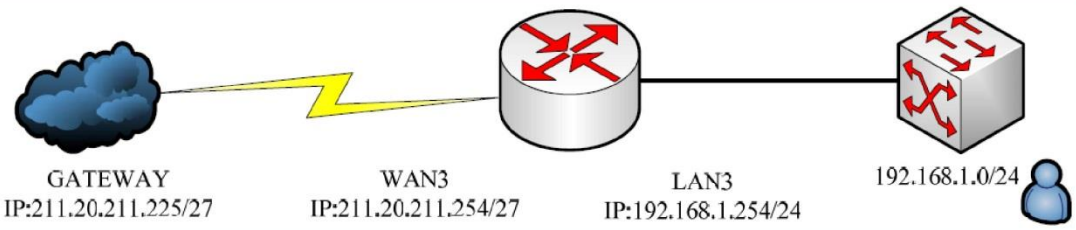
2. [網路配置] → [IP 位址配置] 點選 新增，選擇橋接器介面，IP 位址填入 192.168.1.252，子網路遮罩填入 24。

3. [網路配置] →[路由配置] → [靜態路由] 點選 新增，閘道填入 192.168.1.254。

3. 路由模式運作範例

功能描述：

此模式下設備工作類似一個路由器，可以進行路由拓撲構造。每個實體介面可以工作在不同的子網中，使 LAN 與 Internet 之間建立一個安全閘道。如下圖所示：



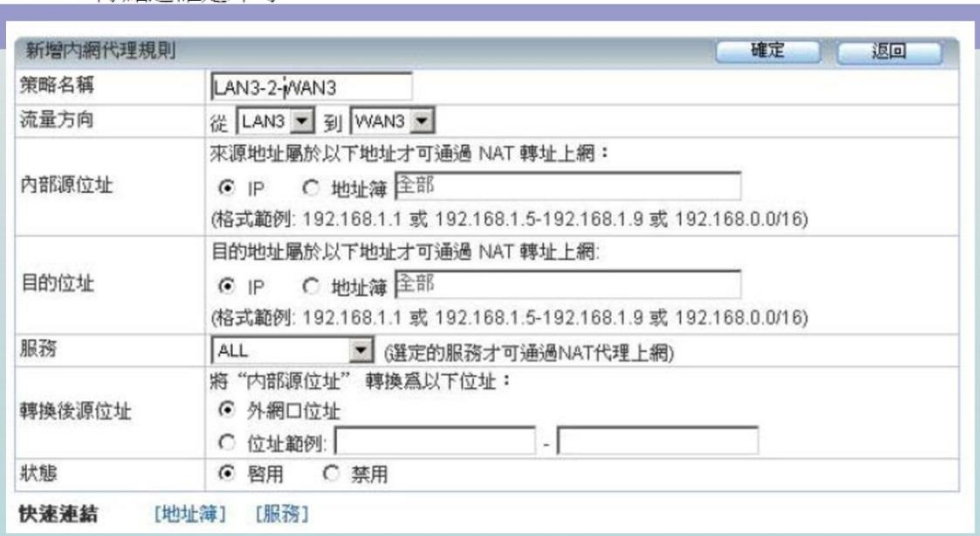
設定步驟：

1. [網路配置] → [IP 位址配置] 點選 新增，選擇 WAN3 介面，IP 位址填入 211.20.211.254，子網路遮罩填入 27。

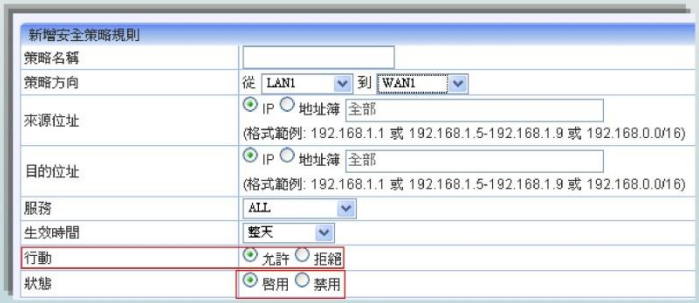
2. [網路配置] → [IP 位址配置] 點選 新增，選擇 LAN3 介面，IP 位址填入 192.168.1.254，子網路遮罩填入 24。

3. [網路配置] → [路由配置] → [靜態路由] 點選 新增，閘道填入 211.20.211.225。

4. [防火牆] → [NAT 策略] → [PAT] 點選 新增，填入策略名稱，設定流量方向從 LAN3 到 WAN3，再點選確定即可。



安全管制條例



依照服務與來源IP設定基本策略
此處僅判別允許/拒絕

4. 流量管理運作範例

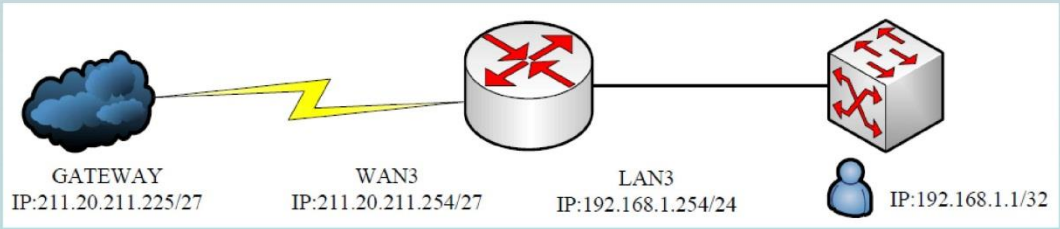
功能描述：

設備提供強大的流量頻寬管理功能，可以根據封包的來源位址、目的地址、服務類型、時間段等參數組合成各種流量，可對這些流量提供最大頻寬限制、保證頻寬、預留頻寬的功能。既能保證重要應用的服務頻寬，又能限制總上下載頻寬，還能針對服務類型、使用者群組、IP 地址等設定頻寬保證和頻寬限制。

範例需求：

保證內部 IP 192.168.1.1 上傳 512Kbps 下載 1024Kbps

如下圖所示：



設定步驟：

1. [流量管理] → [基於策略的流控] 點選 新增，填入策略名稱，選擇有效線路爲 WAN3，內部地址填入 192.168.1.1，保證頻寬上傳填入 512，下載填入 1024，再點選確定即可。

流量管理

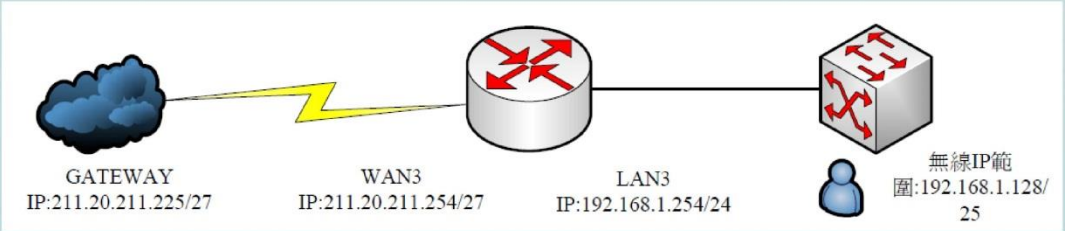
5. 行為管理認證策略運作範例

功能描述：

定義認證的條件、認證方式及使用的認證伺服器。策略規則的匹配原則是按順序從前往後匹配，即從第一條規則開始順序匹配，一旦遇到一條匹配的規則就停止，所以序號越小的規則優先順序越高。

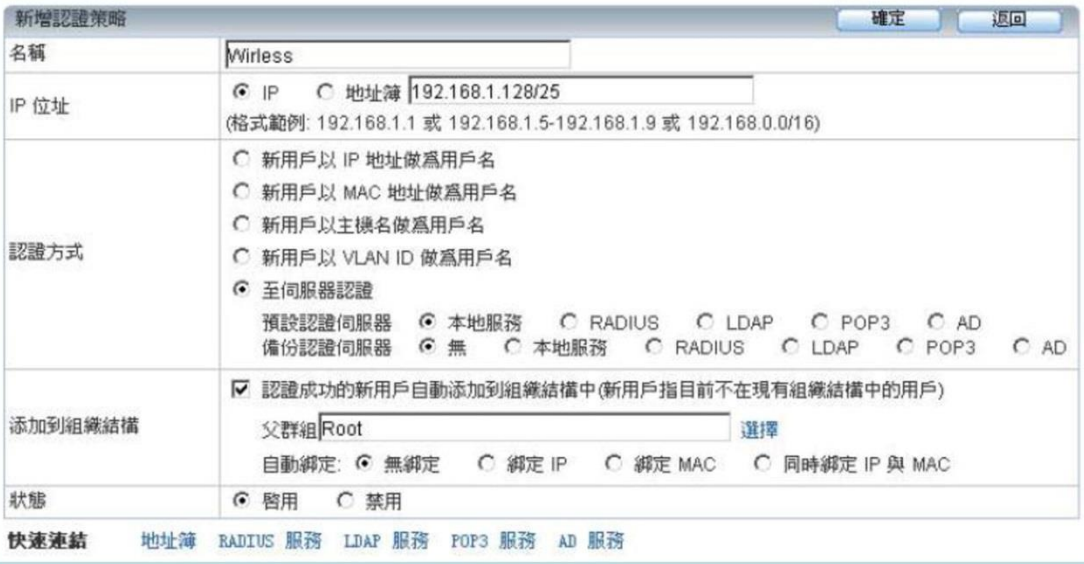
範例需求：

無線上網的 IP 須經由認證才能連外網路。



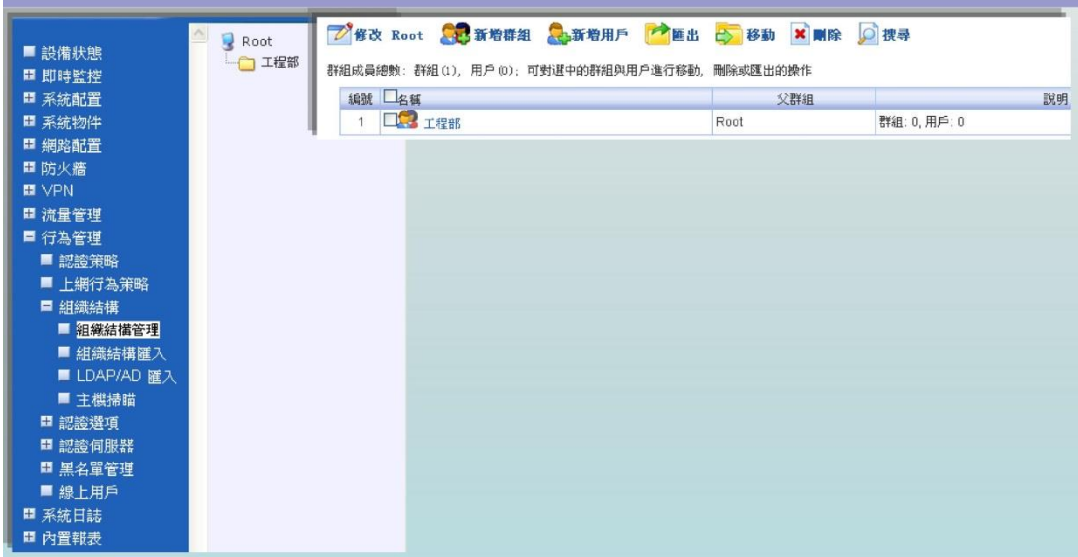
設定步驟：

1. [行爲管理] → [認證策略] 點選 新增，填入策略名稱，IP 地址填入 192.168.1.128/25，認證方式設爲至伺服器認證，再點選確定即可。

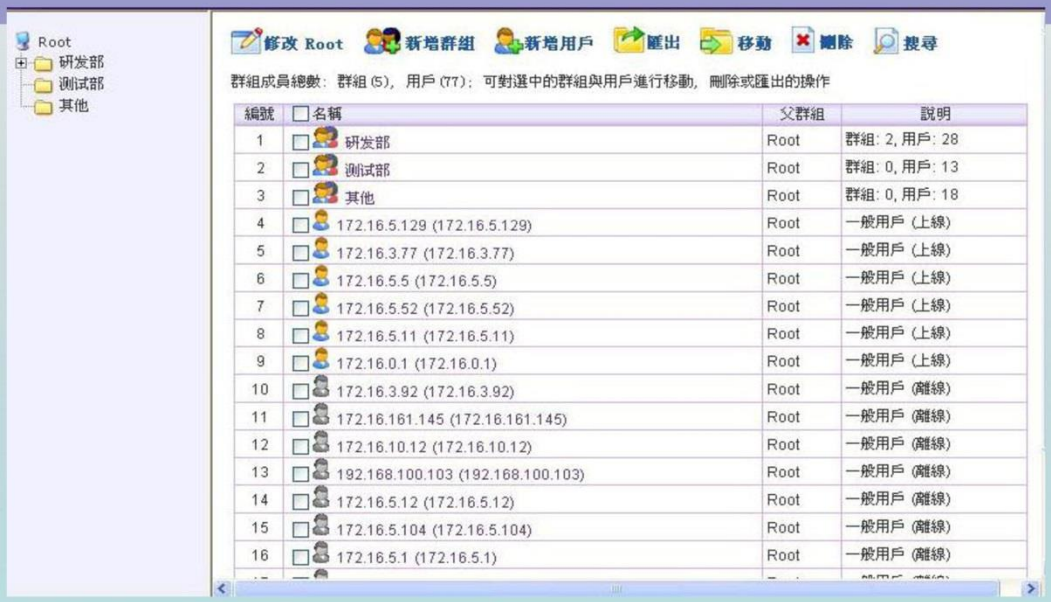


2. [行爲管理] → [組織結構] → [組織結構管理] 點選 新增用戶，填入用戶名稱，用戶類型設定爲認證用戶，認證方式填入該用戶密碼，再點選確定即可。

行為管理

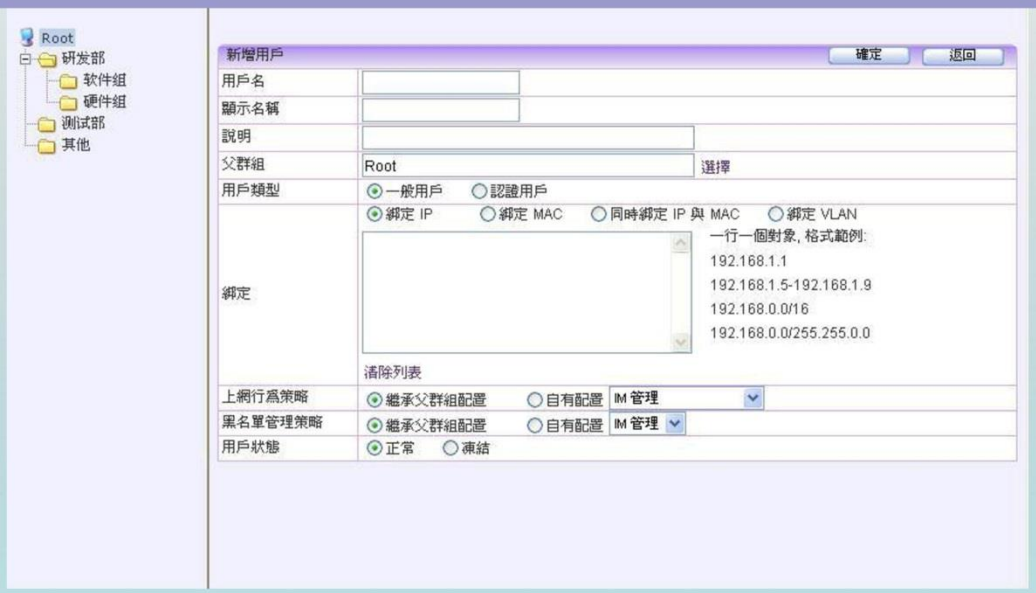


群組架構(可新增群組，用戶，設權限)



上網行為策略

群組架構(新增用戶 --- 條件)



用戶上下線使用記錄

用戶日誌查詢 [搜尋]

用戶名	
IP 位址	
時間範圍	-

用戶日誌列表 [清空]

編號	事件內容	時間
總記錄數:7405 頁碼: 1/149 下一頁		
1	用戶名: 172.16.7.1, IP 位址: 172.16.7.1, 離線	2009-11-29 13:15:08
2	用戶名: 172.16.5.103, IP 位址: 172.16.5.103, 離線	2009-11-29 13:03:17
3	用戶名: 172.16.5.88, IP 位址: 172.16.5.88, 離線	2009-11-29 13:03:01
4	用戶名: 172.16.3.32, IP 位址: 172.16.3.32, 離線	2009-11-29 12:56:32
5	用戶名: 172.16.100.130, IP 位址: 172.16.100.130, 離線	2009-11-29 12:53:53
6	用戶名: 172.16.7.1, IP 位址: 172.16.7.1, 離線	2009-11-29 12:53:28
7	用戶名: 172.16.3.105, IP 位址: 172.16.3.105, 離線	2009-11-29 12:52:24
8	用戶名: 172.16.161.239, IP 位址: 172.16.161.239, 離線	2009-11-29 12:48:12
9	用戶名: 172.16.161.242, IP 位址: 172.16.161.242, 離線	2009-11-29 12:45:15
10	用戶名: 172.16.30.43, IP 位址: 172.16.30.43, 離線	2009-11-29 12:43:31
11	用戶名: 172.16.3.63, IP 位址: 172.16.3.63, 離線	2009-11-29 12:42:44
12	用戶名: 172.16.5.17, IP 位址: 172.16.5.17, 離線	2009-11-29 12:42:06
13	用戶名: 172.16.2.4, IP 位址: 172.16.2.4, 離線	2009-11-29 12:21:42

黑名單管理機制(適用於IP , ID使用者)

新增黑名單策略 [確定] [返回]

名稱	
每日流量配額(KB)	總量 無限制 上行流量 無限制 下行流量 無限制
每週流量配額(KB)	總量 無限制 上行流量 無限制 下行流量 無限制
每月流量配額(KB)	總量 無限制 上行流量 無限制 下行流量 無限制
最大速率(Kbps)	連續 5 分鐘速率持續超過: 上傳 無限制 下載 無限制
最大會話數	連續 5 分鐘活躍會話數持續超過: 上傳 無限制 下載 無限制
管制方法	○ 強制斷線 ◉ 修改頻寬與會話數 上傳頻寬 無限制 Kbps 上行會話數 無限制 下載頻寬 無限制 Kbps 下行會話數 無限制
管制時間	1 ○ 分鐘 ◉ 小時 ○ 天
加強管制	一週內 連續進入黑名單 5 次 管制時間增加 3 倍
生效時間	整天 在生效時間內才進行黑名單的管控. 在生效時間外, 不對使用者的速率和會話進行限制, 使用者產生的流量也不記入黑名單的流量配額內.

線上用戶狀況(Session , traffic)

線上的用戶 搜尋

用戶名		用戶群組		選擇
IP 位址		MAC 位址		
登入期間	-			

在線用戶

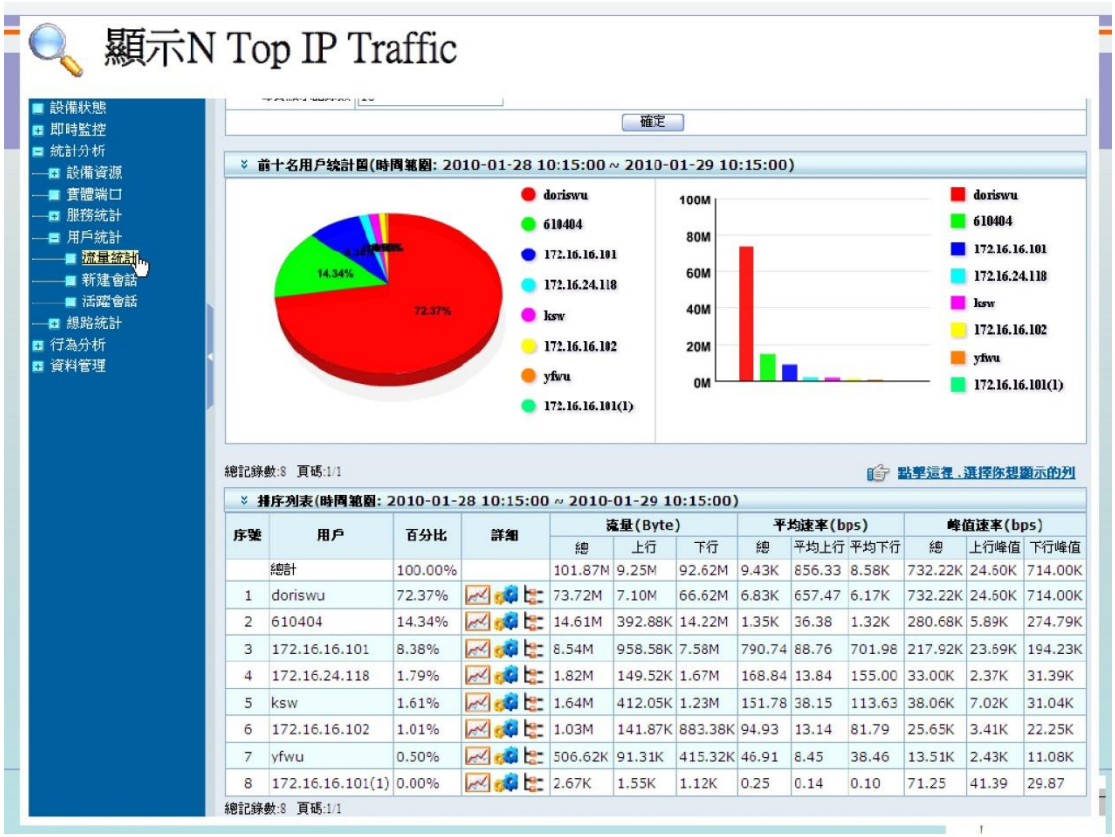
編號	用戶名/使用者群組	IP 位址/MAC 位址	實體介面	線上流量(Byte)	最新速率(bps)	活躍會話數	上線時間	操作
總記錄數:36 頁碼:1/1								
1	172.16.0.1 Root	172.16.0.1 00:18:47:04:e8:a0	LAN1	↑6.1K, ↓19.5K	↑220.0, ↓672.0	↑15, ↓0	2009-11-29 12:57:46	趨勢圖 線上服務 強制斷線
2	172.16.3.2 Root/研发部/软件组	172.16.3.2 00:18:47:04:e8:a0	LAN1	↑3.3M, ↓27.9M	↑14.0, ↓39.0	↑1, ↓2	2009-11-29 10:40:51	趨勢圖 線上服務 強制斷線
3	172.16.3.7 Root/研发部/软件组	172.16.3.7 00:18:47:04:e8:a0	LAN1	↑3.7M, ↓14.0M	↑2.6K, ↓5.2K	↑9, ↓0	2009-11-29 10:40:51	趨勢圖 線上服務 強制斷線
4	172.16.3.13 Root/研发部/软件组	172.16.3.13 00:18:47:04:e8:a0	LAN1	↑67.6M, ↓35.1M	↑124.0, ↓91.0	↑3, ↓0	2009-11-29 10:41:00	趨勢圖 線上服務 強制斷線
5	172.16.3.27 Root/研发部/软件	172.16.3.27	LAN1	↑44.4M, ↓51.0M	↑8.8K, ↓10.8K	↑30, ↓0	2009-11-29	趨勢圖 線上服務 強制

Report 記錄條件設定

內容記錄配置 確定 返回

內部位址	◉ IP ○ 地址簿 全部 (格式範例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)
即時通訊	☐登入信息 ☐通信內容
郵件記錄	☐基本信息 ☐郵件主體 ☐郵件附檔
WEB 紀錄	☐URL 位址 ☐網頁標題 ☐張貼文章信息關鍵字組過濾 ☐搜尋引擎關鍵字過濾 ☐下載檔案類型
FTP 紀錄	☐啓用記錄
會話記錄	☐啓用記錄
狀態	◉啓用 ○禁用

顯示N Top IP Traffic



序號	用户	百分比	詳細	流量(Byte)			平均速率(bps)			峰值速率(bps)		
				總	上行	下行	總	平均上行	平均下行	總	上行峰值	下行峰值
	總計	100.00%		101.87M	9.25M	92.62M	9.43K	856.33	8.58K	732.22K	24.60K	714.00K
1	doriswu	72.37%		73.72M	7.10M	66.62M	6.83K	657.47	6.17K	732.22K	24.60K	714.00K
2	610404	14.34%		14.61M	392.88K	14.22M	1.35K	36.38	1.32K	280.68K	5.89K	274.79K
3	172.16.16.101	8.38%		8.54M	958.58K	7.58M	790.74	88.76	701.98	217.92K	23.69K	194.23K
4	172.16.24.118	1.79%		1.82M	149.52K	1.67M	168.84	13.84	155.00	33.00K	2.37K	31.39K
5	ksw	1.61%		1.64M	412.05K	1.23M	151.78	38.15	113.63	38.06K	7.02K	31.04K
6	172.16.16.102	1.01%		1.03M	141.87K	883.38K	94.93	13.14	81.79	25.65K	3.41K	22.25K
7	yfwu	0.50%		506.62K	91.31K	415.32K	46.91	8.45	38.46	13.51K	2.43K	11.08K
8	172.16.16.101(1)	0.00%		2.67K	1.55K	1.12K	0.25	0.14	0.10	71.25	41.39	29.87

總記錄數:8 頁碼:1/1

顯示每個IP(User)線上-傳輸量

序號	IP 位址	用户名	用户群組	總 (bps)	上行 (bps)	下行 (bps)	操作
1	172.16.12.79			246.6K	10.2K	236.5K	趨勢圖 線上服務
2	172.16.20.20			75.9K	2.6K	73.3K	趨勢圖 線上服務
3	172.16.24.71			26.9K	9.4K	17.5K	趨勢圖 線上服務
4	192.168.1.17			26.2K	21.7K	4.5K	趨勢圖 線上服務
5	172.16.24.17			23.8K	4.9K	18.9K	趨勢圖 線上服務
6	172.16.24.1			16.3K	5.5K	10.8K	趨勢圖 線上服務
7	172.16.4.1			8.3K	3.0K	5.3K	趨勢圖 線上服務
8	172.16.20.220	172.16.20.220(1)	fcsh.khc.edu.tw	7.7K	1.9K	5.9K	趨勢圖 線上服務
9	172.16.4.2			7.1K	2.4K	4.7K	趨勢圖 線上服務
10	172.16.16.6			3.4K	881.1	2.5K	趨勢圖 線上服務
11	172.16.15.51			1.4K	280.0	1.1K	趨勢圖 線上服務
12	172.16.12.25			1.1K	967.2	177.6	趨勢圖 線上服務
13	172.16.12.125			753.1	103.2	649.9	趨勢圖 線上服務
14	172.16.24.254			500.5	213.6	286.9	趨勢圖 線上服務
15	172.16.12.101			421.1	57.1	364.0	趨勢圖 線上服務
16	172.16.12.5			84.0	69.6	14.4	趨勢圖 線上服務
17	172.16.24.120			62.9	38.7	24.3	趨勢圖 線上服務
18	192.168.1.1			22.4	22.4	0.0	趨勢圖 線上服務
19	172.16.12.23			7.5	4.8	2.7	趨勢圖 線上服務
20	192.168.1.10			0.0	0.0	0.0	趨勢圖 線上服務

即時顯示前 10 名-Session

序號	IP 位址	用戶名	用戶群組	總(sps)	上行(sps)	下行(sps)	操作
1	172.16.4.1			6.3	6.3	0.0	趨勢圖 線上服務
2	172.16.4.2			2.8	2.8	0.0	趨勢圖 線上服務
3	192.168.1.17			1.2	1.1	0.1	趨勢圖 線上服務
4	172.16.12.208			1.1	1.1	0.0	趨勢圖 線上服務
5	172.16.24.1			0.3	0.3	0.0	趨勢圖 線上服務
6	172.16.16.7			0.2	0.2	0.0	趨勢圖 線上服務
7	172.16.24.71			0.1	0.1	0.0	趨勢圖 線上服務
8	172.16.12.174			0.1	0.1	0.0	趨勢圖 線上服務
9	172.16.16.6			0.1	0.1	0.0	趨勢圖 線上服務
10	172.16.8.56			0.1	0.1	0.0	趨勢圖 線上服務
11	172.16.12.29			0.0	0.0	0.0	趨勢圖 線上服務
12	172.16.12.78			0.0	0.0	0.0	趨勢圖 線上服務
13	192.168.1.1			0.0	0.0	0.0	趨勢圖 線上服務
14	172.16.24.254			0.0	0.0	0.0	趨勢圖 線上服務

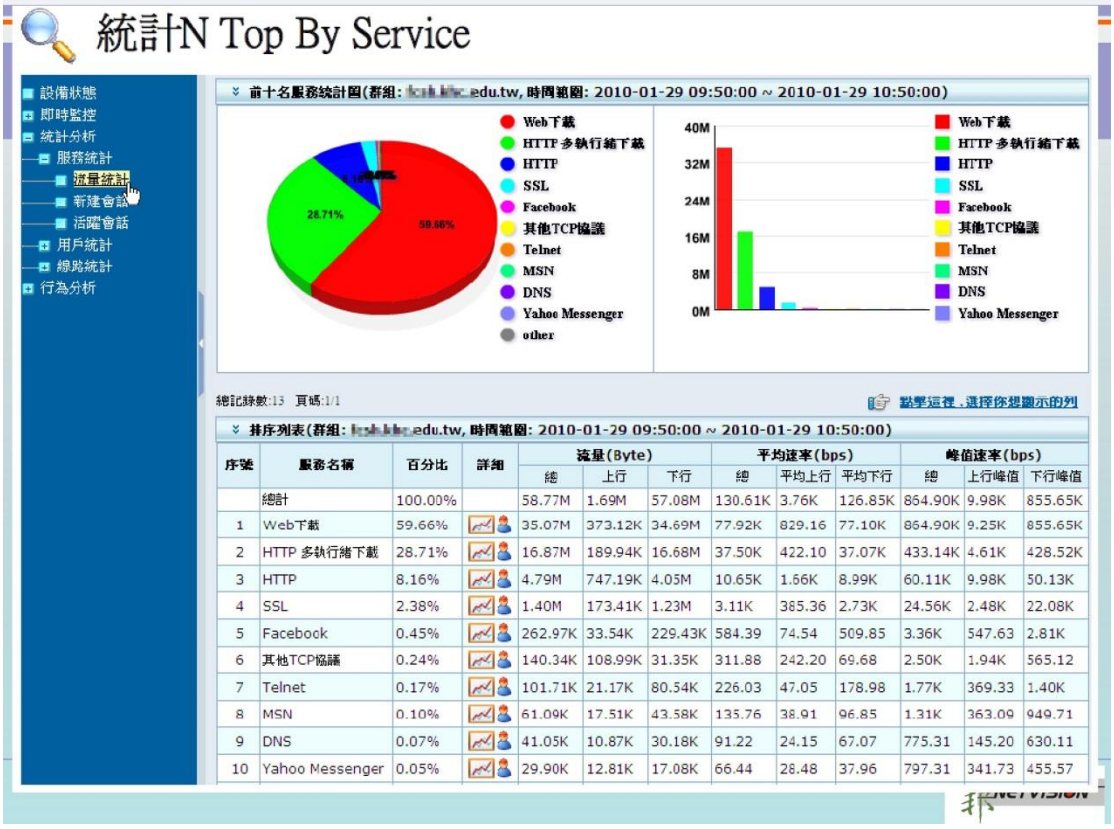
即時顯示前10名- New Session

序號	IP 位址	用戶名	用戶群組	總	上行	下行	操作
1	172.16.24.1			140	140	0	趨勢圖 線上服務
2	172.16.4.1			121	121	0	趨勢圖 線上服務
3	172.16.16.6			104	104	0	趨勢圖 線上服務
4	172.16.12.29			87	87	0	趨勢圖 線上服務
5	172.16.4.2			86	86	0	趨勢圖 線上服務
6	192.168.1.17			68	68	0	趨勢圖 線上服務
7	172.16.12.208			37	37	0	趨勢圖 線上服務
8	172.16.12.5			25	25	0	趨勢圖 線上服務
9	172.16.12.145			22	22	0	趨勢圖 線上服務
10	172.16.16.23			14	14	0	趨勢圖 線上服務
11	172.16.24.71			13	13	0	趨勢圖 線上服務
12	172.16.16.5			6	6	0	趨勢圖 線上服務
13	172.16.12.101			2	2	0	趨勢圖 線上服務
14	172.16.24.254			2	2	0	趨勢圖 線上服務
15	172.16.20.20			2	2	0	趨勢圖 線上服務
16	172.16.12.23			2	2	0	趨勢圖 線上服務
17	192.168.1.10			1	1	0	趨勢圖 線上服務
18	172.16.12.25			1	1	0	趨勢圖 線上服務
19	172.16.8.56			0	0	0	趨勢圖 線上服務
20	172.16.24.120			0	0	0	趨勢圖 線上服務

記錄每筆Session log

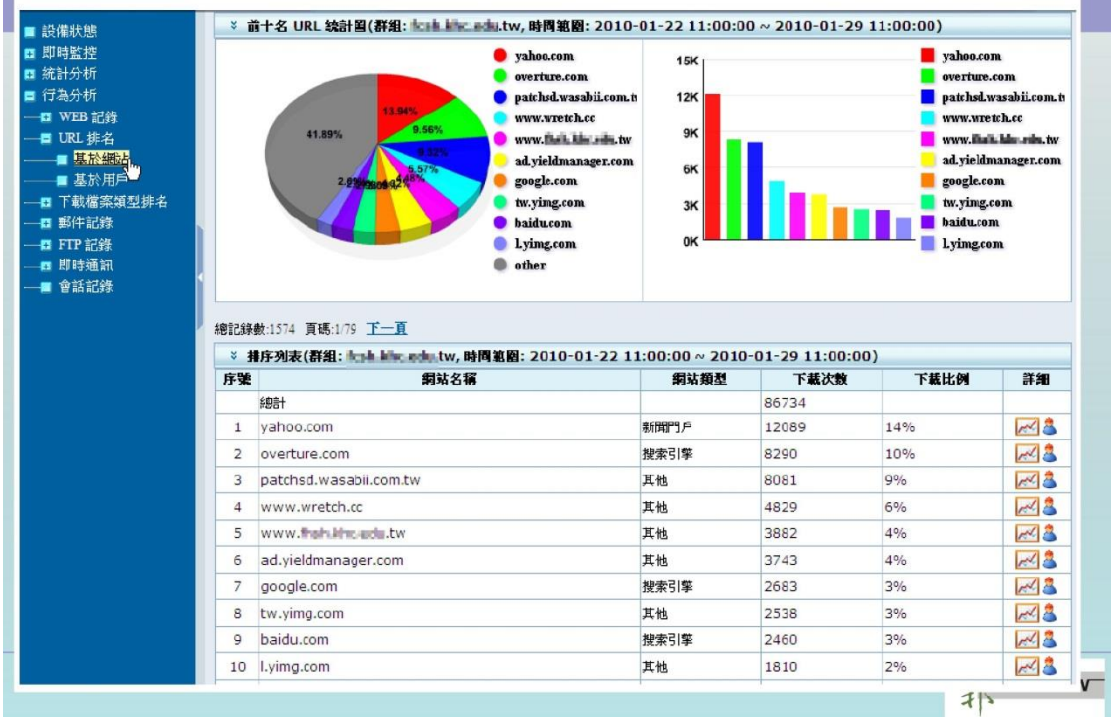
序號	來源(IP: 埠)	目的(IP: 埠)	轉換(IP: 埠)	通訊協議	服務名稱	傳送資料大小	接收資料大小	持續時間	記錄時間
1	172.16.24.1: 4211	124.108.103.68: 80	210.60.[illegible]: 4211	TCP	HTTP	8.13KB	6.2KB	122S	2010-01-29 10:52:20
2	192.168.1.17: 27771	83.223.122.70: 25	210.60.[illegible]: 27771	TCP	其他TCP協議	62B	54B	0S	2010-01-29 10:52:20
3	172.16.4.1: 57397	83.223.122.70: 53	210.60.161.254: 57397	UDP	DNS	77B	121B	30S	2010-01-29 10:52:20
4	172.16.12.79: 2686	220.228.161.115: 80	210.60.161.254: 2686	TCP	HTTP	557B	3.09KB	10S	2010-01-29 10:52:20
5	172.16.12.145: 1452	123.204.51.124: 23	210.60.[illegible]: 1452	TCP	其他TCP協議	186B	270B	128S	2010-01-29 10:52:20
6	192.168.1.17: 27771	83.223.122.70: 25	210.60.[illegible]: 27771	TCP	其他TCP協議	62B	54B	0S	2010-01-29 10:52:20
7	172.16.12.1: 1193	211.72.249.41: 80	210.60.161.254: 1193	TCP	HTTP	951B	440B	120S	2010-01-29 10:52:19
8	172.16.12.1: 1192	211.72.249.44: 80	210.60.[illegible]: 1192	TCP	HTTP	865B	846B	120S	2010-01-29 10:52:19
9	172.16.12.1: 1191	211.72.249.41: 80	210.60.161.254: 1191	TCP	HTTP	864B	840B	120S	2010-01-29 10:52:19
10	172.16.4.1: 63475	195.92.193.4: 53	210.60.161.254: 63475	UDP	DNS	85B	159B	30S	2010-01-29 10:52:19
11	172.16.4.1: 51803	195.92.67.18: 53	210.60.[illegible]: 51803	UDP	DNS	87B	161B	30S	2010-01-29 10:52:19
12	192.168.1.17: 27771	83.223.122.70: 25	210.60.[illegible]: 27771	TCP	其他TCP協議	62B	54B	0S	2010-01-29 10:52:19
13	172.16.4.1: 63760	195.92.67.18: 53	210.60.161.254: 63760	UDP	DNS	81B	155B	30S	2010-01-29 10:52:19
14	172.16.12.1: 1189	211.72.249.44: 80	210.60.[illegible]: 1189	TCP	HTTP	881B	801B	120S	2010-01-29 10:52:19
15	172.16.4.1: 59138	195.92.193.4: 53	210.60.161.254: 59138	UDP	DNS	87B	161B	30S	2010-01-29 10:52:18
16	172.16.4.1: 60054	195.92.193.4: 53	210.60.161.254: 60054	UDP	DNS	85B	159B	30S	2010-01-29 10:52:18

統計N Top By Service



序號	服務名稱	百分比	詳細	流量(Byte)			平均速率(bps)			峰值速率(bps)		
				總	上行	下行	總	平均上行	平均下行	總	上行峰值	下行峰值
	總計	100.00%		58.77M	1.69M	57.08M	130.61K	3.76K	126.85K	864.90K	9.98K	855.65K
1	Web下載	59.66%		35.07M	373.12K	34.69M	77.92K	829.16	77.10K	864.90K	9.25K	855.65K
2	HTTP 多執行緒下載	28.71%		16.87M	189.94K	16.68M	37.50K	422.10	37.07K	433.14K	4.61K	428.52K
3	HTTP	8.16%		4.79M	747.19K	4.05M	10.65K	1.66K	8.99K	60.11K	9.98K	50.13K
4	SSL	2.38%		1.40M	173.41K	1.23M	3.11K	385.36	2.73K	24.56K	2.48K	22.08K
5	Facebook	0.45%		262.97K	33.54K	229.43K	584.39	74.54	509.85	3.36K	547.63	2.81K
6	其他TCP協議	0.24%		140.34K	108.99K	31.35K	311.88	242.20	69.68	2.50K	1.94K	565.12
7	Telnet	0.17%		101.71K	21.17K	80.54K	226.03	47.05	178.98	1.77K	369.33	1.40K
8	MSN	0.10%		61.09K	17.51K	43.58K	135.76	38.91	96.85	1.31K	363.09	949.71
9	DNS	0.07%		41.05K	10.87K	30.18K	91.22	24.15	67.07	775.31	145.20	630.11
10	Yahoo Messenger	0.05%		29.90K	12.81K	17.08K	66.44	28.48	37.96	797.31	341.73	455.57

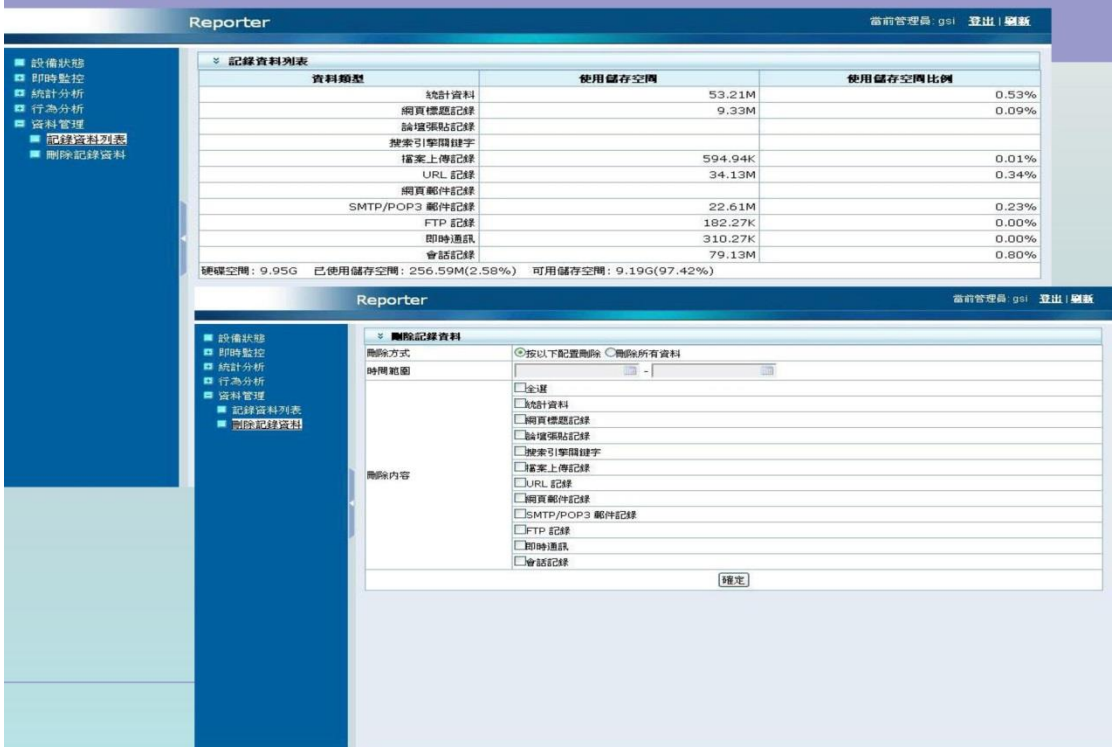
統計網站點閱率



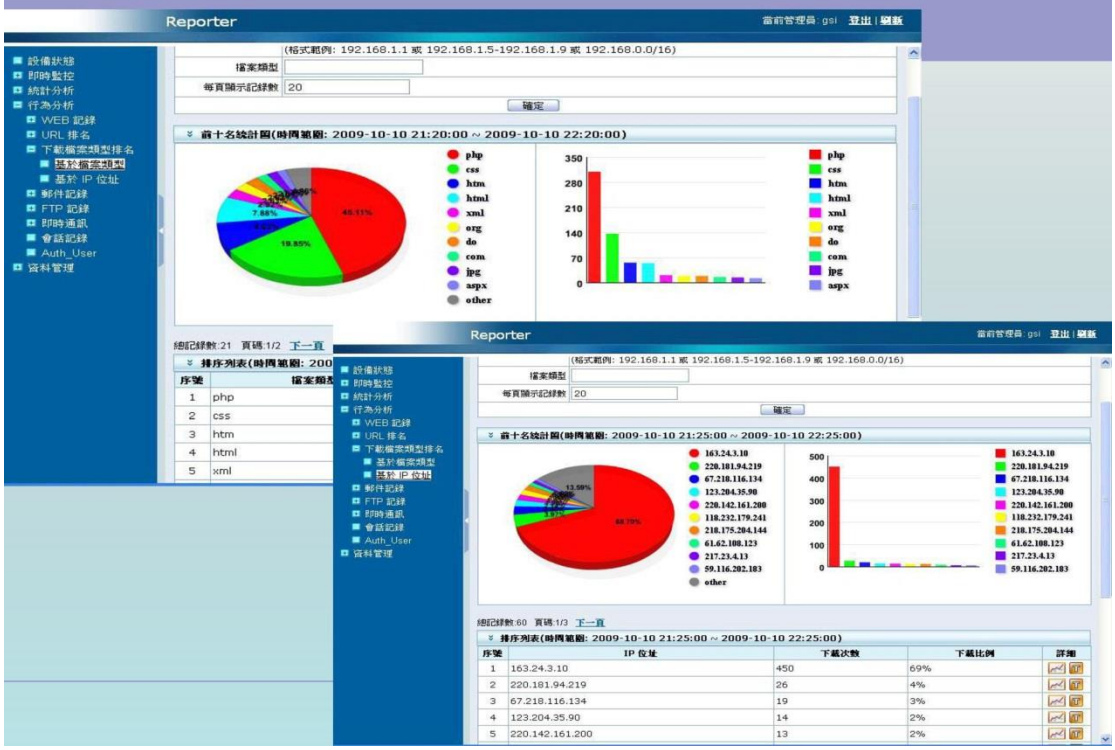
PAT Session log中可看到 sour/trans/dest三者關係

顯示每個IP(User) 線上-傳輸量/Active Session/MAC/Phy port

Log資料儲存比例及可刪除條件範圍

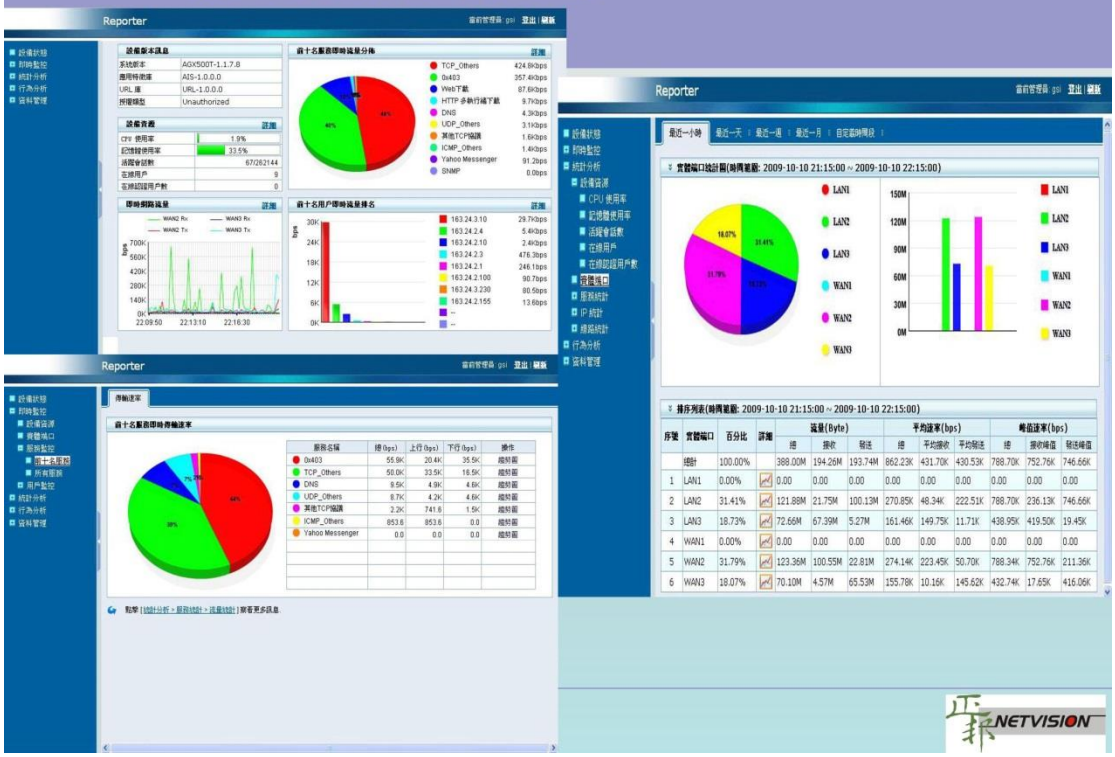


統計各下載檔案類型及下載 IP 排行

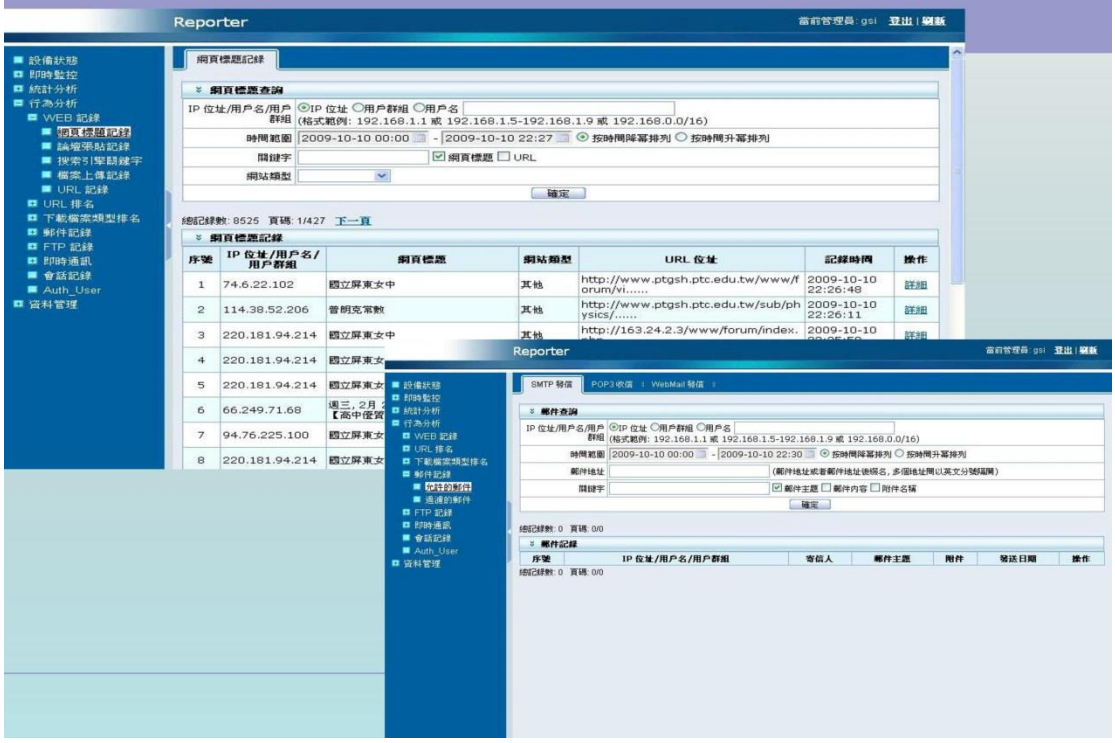


統計各Service前10名 IP

統計系統各項數據



HTTP,FTP,MSN,URL,Mail Log記錄



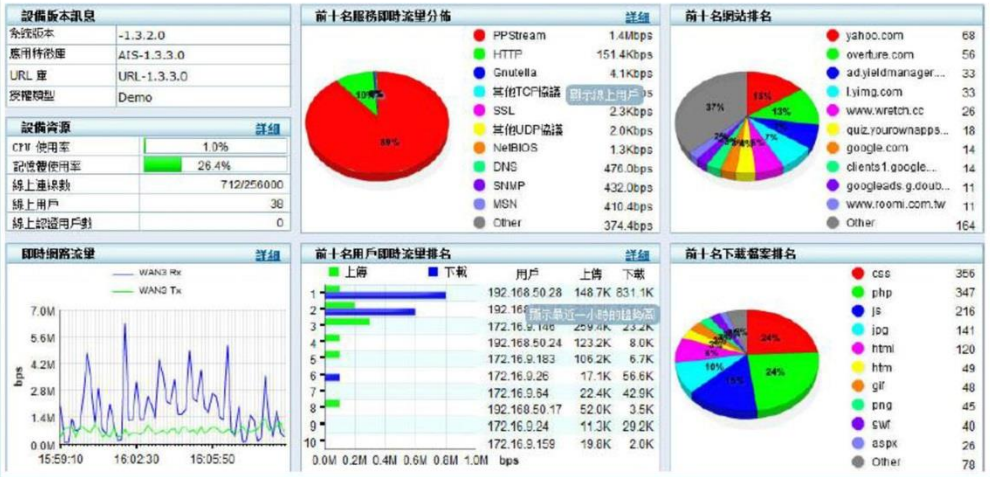
報表說明

1．設備狀態

位置：設備狀態

說明：顯示即時運作資訊。

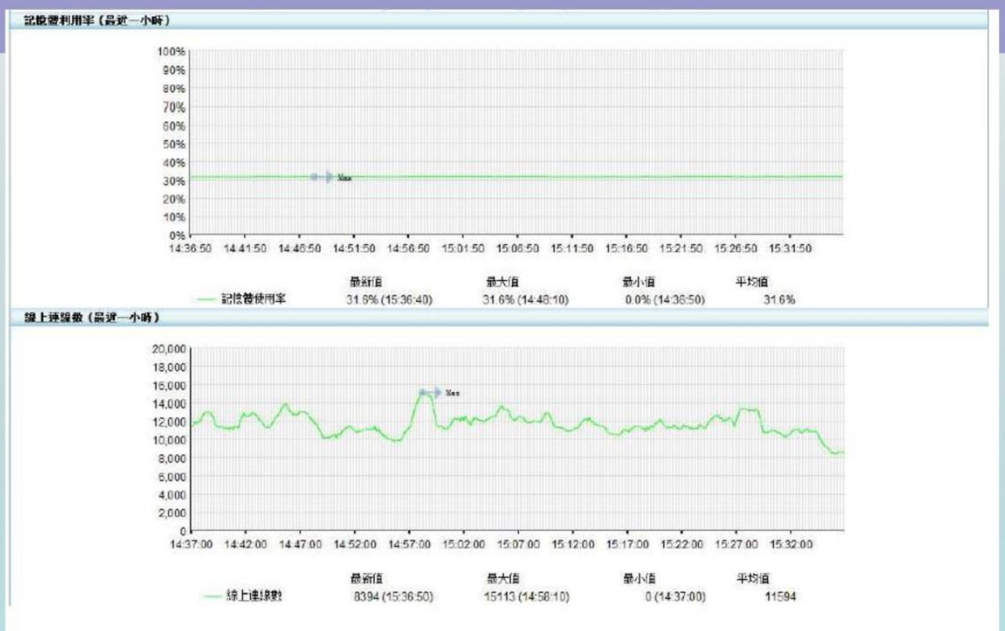
【點擊PPSteam可即時哪些使用者在使用這個服務、點擊10.10.2.30可即時顯示該用戶使用哪個服務功能】



2．即時監控

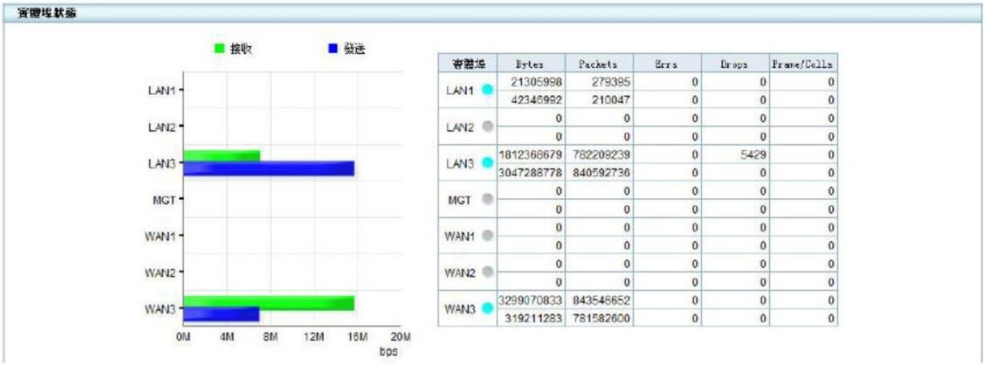
2-1．設備資源

位置：即時監控 -> 設備資源
說明：提供即時性CPU、記憶體、認證用戶、連線數、線上用戶數資訊。



2-2．實體 PORT

位置：即時監控 -> 實體Port
說明：顯示各個PORT運作狀態。
【包含上下載頻寬、封包狀況、各Port接收與發送狀態】

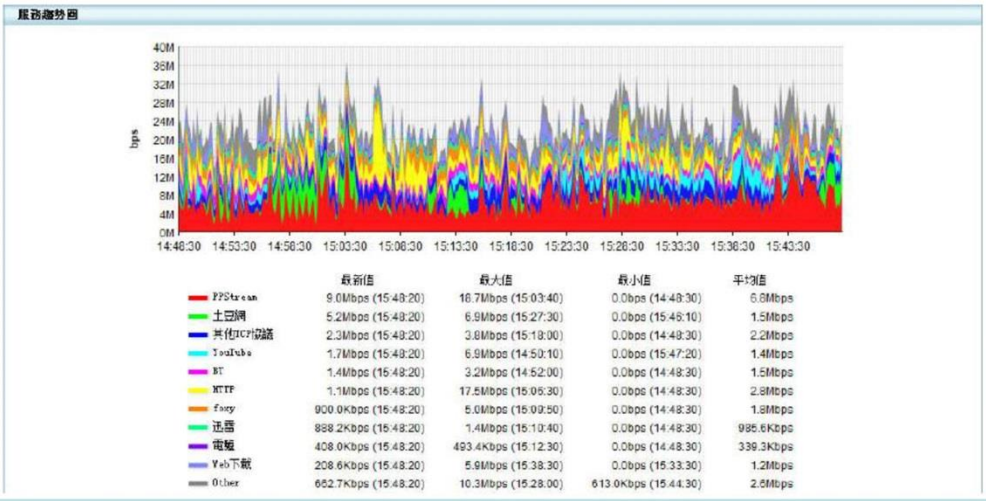


實體埠	Bytes	Packets	Errs	Drops	Frame/Cells
LAN1	21305998	279385	0	0	0
	42340992	210047	0	0	0
LAN2	0	0	0	0	0
	0	0	0	0	0
LAN3	1812368679	782209239	0	5429	0
	3047288778	840592736	0	0	0
MGT	0	0	0	0	0
	0	0	0	0	0
WAN1	0	0	0	0	0
	0	0	0	0	0
WAN2	0	0	0	0	0
	0	0	0	0	0
WAN3	3299070833	843546652	0	0	0
	319211283	781582600	0	0	0

2-3・服務監控

2-3-1・服務趨勢圖

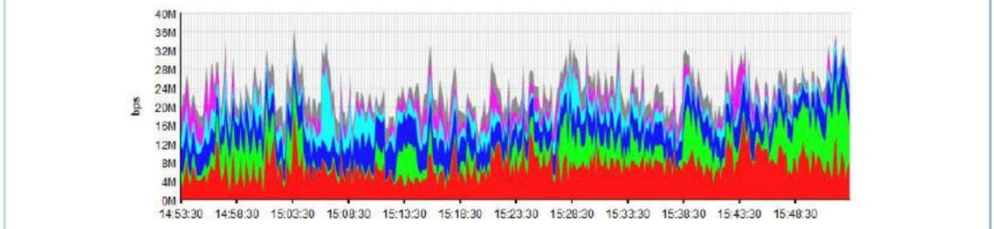
位置：即時監控 -> 服務監控 -> 服務趨勢圖
說明：顯示服務排名。



	最新值	最大值	最小值	平均值
PPStream	9.0Mbps (15:48:20)	16.7Mbps (15:03:40)	0.0bps (14:48:30)	6.8Mbps
土豆網	5.2Mbps (15:48:20)	6.9Mbps (15:27:30)	0.0bps (15:46:10)	1.5Mbps
其他TCP協議	2.3Mbps (15:48:20)	3.8Mbps (15:18:00)	0.0bps (14:48:30)	2.2Mbps
Youtube	1.7Mbps (15:48:20)	6.9Mbps (14:50:10)	0.0bps (15:47:20)	1.4Mbps
BT	1.4Mbps (15:48:20)	3.2Mbps (14:52:00)	0.0bps (14:48:30)	1.5Mbps
HTTP	1.1Mbps (15:48:20)	17.5Mbps (15:05:30)	0.0bps (14:48:30)	2.8Mbps
foxy	900.0Kbps (15:48:20)	5.0Mbps (15:09:50)	0.0bps (14:48:30)	1.8Mbps
迅雷	888.2Kbps (15:48:20)	1.4Mbps (15:10:40)	0.0bps (14:48:30)	985.6Kbps
電驢	408.0Kbps (15:48:20)	493.4Kbps (15:12:30)	0.0bps (14:48:30)	339.3Kbps
Web下載	208.6Kbps (15:48:20)	5.9Mbps (15:38:30)	0.0bps (15:33:30)	1.2Mbps
Other	652.7Kbps (15:48:20)	10.3Mbps (15:28:00)	613.0Kbps (15:44:30)	2.5Mbps

2-3-2・服務組趨勢圖

位置：即時監控 -> 服務監控 -> 服務組趨勢圖
說明：顯示服務群組排名。



	最新值	最大值	最小值	平均值
串流媒體	8.1Mbps (15:53:20)	18.8Mbps (15:03:40)	1.5Mbps (15:39:40)	1.8Gbps
WEB視訊	7.8Mbps (15:53:20)	17.1Mbps (15:53:00)	127.3Kbps (15:33:10)	6.0Gbps
P2P下載	6.5Mbps (15:53:20)	7.9Mbps (15:09:50)	3.0Mbps (15:38:00)	3.9Gbps
常用服務	902.7Kbps (15:53:20)	17.6Mbps (15:06:30)	423.2Kbps (15:45:30)	2.3Gbps
HTTP應用	554.6Kbps (15:53:20)	8.1Mbps (15:43:30)	10.4Kbps (15:00:50)	2.0Gbps
即時通訊	14.3Kbps (15:53:20)	165.4Kbps (15:18:00)	4.2Kbps (15:53:20)	3.2Gbps
網路電話	11.8Kbps (15:53:20)	220.6Kbps (15:45:10)	3.9Kbps (15:02:50)	4.4Gbps
網路遊戲	0.0bps (15:53:20)	14.7Kbps (15:01:30)	0.0bps (15:53:20)	515.4Mbps
股票交易	0.0bps (15:53:20)	21.2Kbps (15:34:40)	0.0bps (15:53:20)	1.7Gbps
網路銀行	0.0bps (15:53:20)	30.5Kbps (15:27:10)	0.0bps (15:39:40)	420.0Mbps
其他服務	1.4Mbps (15:53:20)	4.6Mbps (15:21:30)	1.1Mbps (15:53:10)	14.0Gbps
自訂普通服務	0.0bps (15:53:20)	73.6bps (14:53:30)	0.0bps (15:53:20)	210.0Mbps

2-3-3・線上服務

位置：即時監控 -> 服務監控 -> 線上服務
說明：顯示即時服務流量。

» 線上服務

序號	服務名稱	最新速率(bps)	最近一小時流量(Byte)	最近一小時平均速率(bps)	操作
1	PPStream	↑3.4M, ↓3.1M	↑1.2G, ↓2.0G	↑2.6M, ↓4.4M	趨勢圖 線上用戶
2	foxy	↑3.0M, ↓821.1K	↑180.5M, ↓641.2M	↑401.1K, ↓1.4M	趨勢圖 線上用戶
3	HTTP	↑192.1K, ↓1.7M	↑120.9M, ↓1.1G	↑268.7K, ↓2.4M	趨勢圖 線上用戶
4	其他TCP協議	↑695.6K, ↓1.1M	↑444.0M, ↓544.9M	↑986.7K, ↓1.2M	趨勢圖 線上用戶
5	YouTube	↑21.8K, ↓1.4M	↑8.4M, ↓635.1M	↑18.7K, ↓1.4M	趨勢圖 線上用戶
6	BT	↑446.2K, ↓731.1K	↑162.1M, ↓489.4M	↑360.2K, ↓1.1M	趨勢圖 線上用戶
7	視訊	↑22.8K, ↓1.1M	↑3.9M, ↓211.0M	↑8.7K, ↓468.9K	趨勢圖 線上用戶
8	迅雷	↑903.7K, ↓54.2K	↑413.3M, ↓28.2M	↑918.5K, ↓62.6K	趨勢圖 線上用戶
9	Web下載	↑12.8K, ↓901.5K	↑33.2M, ↓460.7M	↑73.8K, ↓1.0M	趨勢圖 線上用戶
10	電驢	↑336.5K, ↓64.0K	↑136.1M, ↓28.6M	↑302.5K, ↓63.5K	趨勢圖 線上用戶
11	其他UDP協議	↑185.6K, ↓193.0K	↑75.7M, ↓93.5M	↑168.2K, ↓207.8K	趨勢圖 線上用戶
12	Facebook	↑14.2K, ↓227.7K	↑6.1M, ↓85.8M	↑13.5K, ↓190.6K	趨勢圖 線上用戶
13	Gnutella	↑41.3K, ↓110.1K	↑50.8M, ↓71.0M	↑112.9K, ↓157.9K	趨勢圖 線上用戶
14	HiNet hiChannel	↑2.7K, ↓136.0K	↑1.5M, ↓68.2M	↑3.3K, ↓151.4K	趨勢圖 線上用戶

2-3-4・所有服務

位置：即時監控 -> 服務監控 -> 所有服務
說明：查看服務群組內各個服務流量與趨勢圖。

常用服務 | HTTP應用 | WEB 視頻 | P2P 下載 | 串流媒體 | 網路遊戲 | 即時通訊 |

股票交易 | 網路銀行 | 網路電話 | 其他服務 | 自定義普通服務 | 自定義特徵識別 |

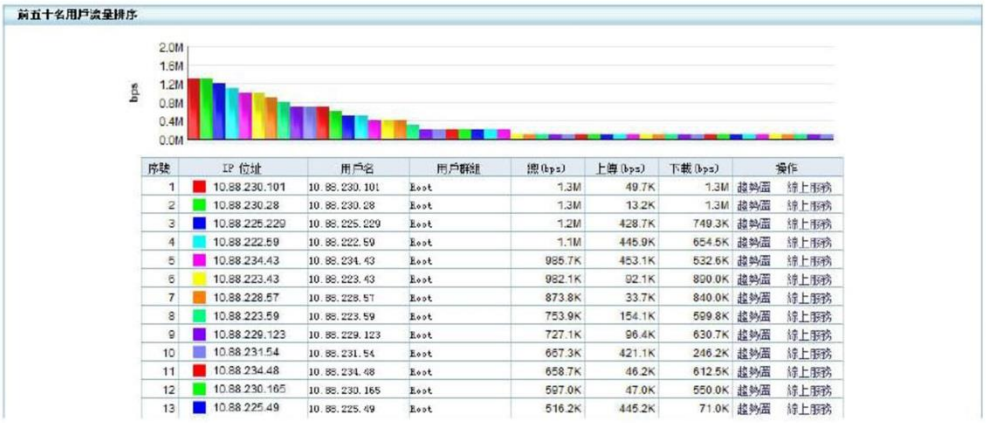
» 常用服務

序號	服務名稱	最新速率(bps)	最近一小時流量(Byte)	最近一小時平均速率(bps)	操作
1	TCP_ALL	↑2.0M, ↓13.0M	↑1.1G, ↓4.6G	↑2.5M, ↓10.1M	趨勢圖
2	UDP_ALL	↑4.5M, ↓2.4M	↑1.8G, ↓2.4G	↑4.1M, ↓5.3M	趨勢圖
3	DNS	↑1.3K, ↓4.5K	↑1.3M, ↓4.1M	↑3.0K, ↓9.0K	趨勢圖
4	HTTP	↑207.9K, ↓1.8M	↑116.7M, ↓1.0G	↑259.3K, ↓2.3M	趨勢圖
5	PING	↑1.1K, ↓1.0K	↑498.1K, ↓471.3K	↑1.1K, ↓1.0K	趨勢圖
6	ICMP_Timeout	0	0	0	趨勢圖
7	ICMP_Unreach	0	0	0	趨勢圖
8	ICMP_ALL	↑1.4K, ↓11.7K	↑526.4K, ↓4.1M	↑1.2K, ↓9.1K	趨勢圖
9	SMTP	0	0	0	趨勢圖
10	POP3	0	↑2.3K, ↓2.6K	↑5.2, ↓5.8	趨勢圖
11	Lotus_Notes	0	↑1.0M, ↓31.1K	↑2.3K, ↓69.2	趨勢圖
12	IMAP	0	0	0	趨勢圖
13	FTP	0	↓77	↓0.2	趨勢圖
14	TFTP	0	0	0	趨勢圖
15	Telnet	0	↑222.9K, ↓959.2K	↑495.3, ↓2.1K	趨勢圖

2-4．用戶監控

2-4-1．流量分析

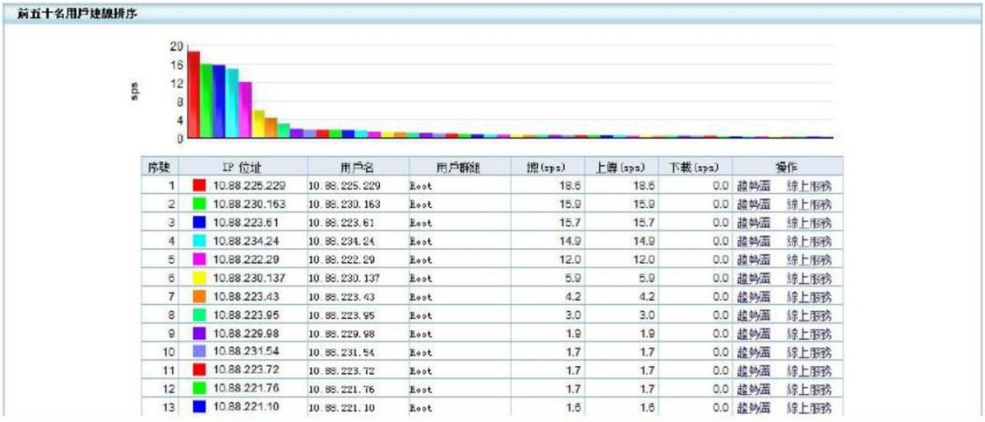
位置：即時監控 -> 用戶監控 -> 流量分析
說明：顯示用戶流量。



序號	IP 位址	用戶名	用戶群組	總(bps)	上傳(bps)	下載(bps)	操作
1	10.88.230.101	10.88.230.101	Root	1.3M	49.7K	1.3M	趨勢圖 線上服務
2	10.88.230.28	10.88.230.28	Root	1.3M	13.2K	1.3M	趨勢圖 線上服務
3	10.88.225.229	10.88.225.229	Root	1.2M	428.7K	749.3K	趨勢圖 線上服務
4	10.88.222.59	10.88.222.59	Root	1.1M	445.9K	654.5K	趨勢圖 線上服務
5	10.88.234.43	10.88.234.43	Root	985.7K	453.1K	532.6K	趨勢圖 線上服務
6	10.88.223.43	10.88.223.43	Root	982.1K	92.1K	890.0K	趨勢圖 線上服務
7	10.88.228.57	10.88.228.57	Root	873.8K	33.7K	840.0K	趨勢圖 線上服務
8	10.88.223.59	10.88.223.59	Root	753.9K	154.1K	599.8K	趨勢圖 線上服務
9	10.88.229.123	10.88.229.123	Root	727.1K	96.4K	630.7K	趨勢圖 線上服務
10	10.88.231.54	10.88.231.54	Root	667.3K	421.1K	246.2K	趨勢圖 線上服務
11	10.88.234.48	10.88.234.48	Root	658.7K	46.2K	612.5K	趨勢圖 線上服務
12	10.88.230.165	10.88.230.165	Root	597.0K	47.0K	550.0K	趨勢圖 線上服務
13	10.88.225.49	10.88.225.49	Root	516.2K	445.2K	71.0K	趨勢圖 線上服務

2-4-2．連線分析

位置：即時監控 -> 用戶監控 -> 連線分析
說明：顯示用戶連線數。



序號	IP 位址	用戶名	用戶群組	總(sps)	上傳(sps)	下載(sps)	操作
1	10.88.225.229	10.88.225.229	Root	18.6	18.6	0.0	趨勢圖 線上服務
2	10.88.230.163	10.88.230.163	Root	15.9	15.9	0.0	趨勢圖 線上服務
3	10.88.223.61	10.88.223.61	Root	15.7	15.7	0.0	趨勢圖 線上服務
4	10.88.234.24	10.88.234.24	Root	14.9	14.9	0.0	趨勢圖 線上服務
5	10.88.222.29	10.88.222.29	Root	12.0	12.0	0.0	趨勢圖 線上服務
6	10.88.230.137	10.88.230.137	Root	5.9	5.9	0.0	趨勢圖 線上服務
7	10.88.223.43	10.88.223.43	Root	4.2	4.2	0.0	趨勢圖 線上服務
8	10.88.223.95	10.88.223.95	Root	3.0	3.0	0.0	趨勢圖 線上服務
9	10.88.229.98	10.88.229.98	Root	1.9	1.9	0.0	趨勢圖 線上服務
10	10.88.231.54	10.88.231.54	Root	1.7	1.7	0.0	趨勢圖 線上服務
11	10.88.223.72	10.88.223.72	Root	1.7	1.7	0.0	趨勢圖 線上服務
12	10.88.221.76	10.88.221.76	Root	1.7	1.7	0.0	趨勢圖 線上服務
13	10.88.221.10	10.88.221.10	Root	1.6	1.6	0.0	趨勢圖 線上服務

2-4-3・線上連線

位置：即時監控 -> 用戶監控 -> 線上連線
說明：顯示用戶連線數。

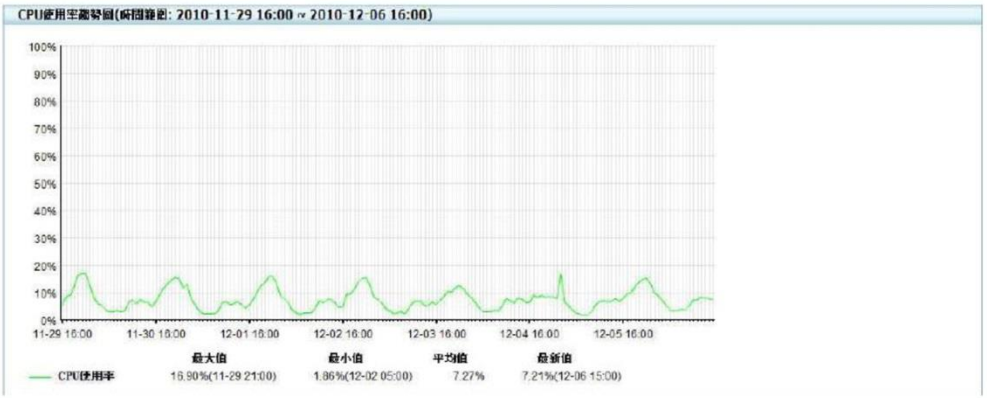
序號	IP 位址	用戶名	用戶群組	總	上傳	下載	操作
1	10.88.223.61	10.88.223.61	Root	2074	2074	0	趨勢圖 線上服務
2	10.88.234.24	10.88.234.24	Root	1212	1212	0	趨勢圖 線上服務
3	10.88.225.229	10.88.225.229	Root	940	940	0	趨勢圖 線上服務
4	10.88.222.29	10.88.222.29	Root	778	778	0	趨勢圖 線上服務
5	10.88.230.163	10.88.230.163	Root	686	686	0	趨勢圖 線上服務
6	10.88.223.43	10.88.223.43	Root	374	374	0	趨勢圖 線上服務
7	10.88.231.54	10.88.231.54	Root	228	228	0	趨勢圖 線上服務
8	10.88.230.137	10.88.230.137	Root	185	185	0	趨勢圖 線上服務
9	10.88.221.35	10.88.221.35	Root	173	173	0	趨勢圖 線上服務
10	10.88.229.102	10.88.229.102	Root	171	171	0	趨勢圖 線上服務
11	10.88.221.10	10.88.221.10	Root	162	162	0	趨勢圖 線上服務
12	10.88.231.35	10.88.231.35	Root	117	117	0	趨勢圖 線上服務
13	10.88.230.109	10.88.230.109	Root	107	107	0	趨勢圖 線上服務

3・統計分析

3-1・設備資源

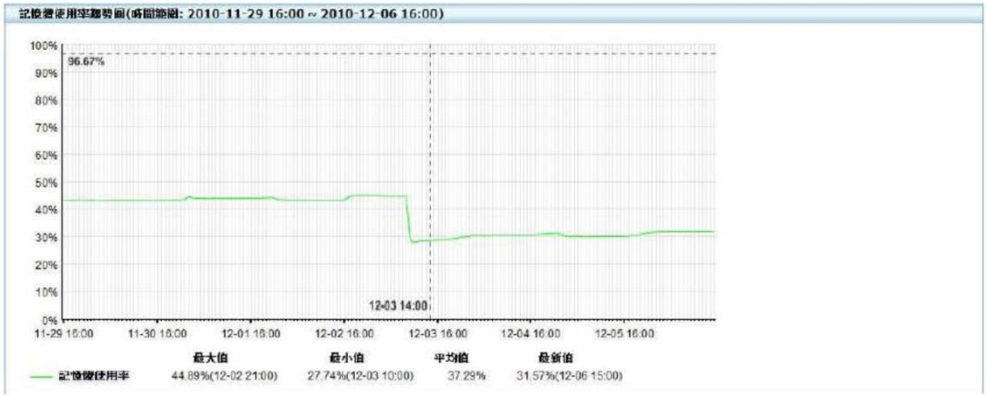
3-1-1・CPU 使用率

位置：統計分析 -> 設備資源 -> CPU使用率
說明：查詢最近一小時、一天、一周、一月、或自定義時間查詢CPU運作資訊。



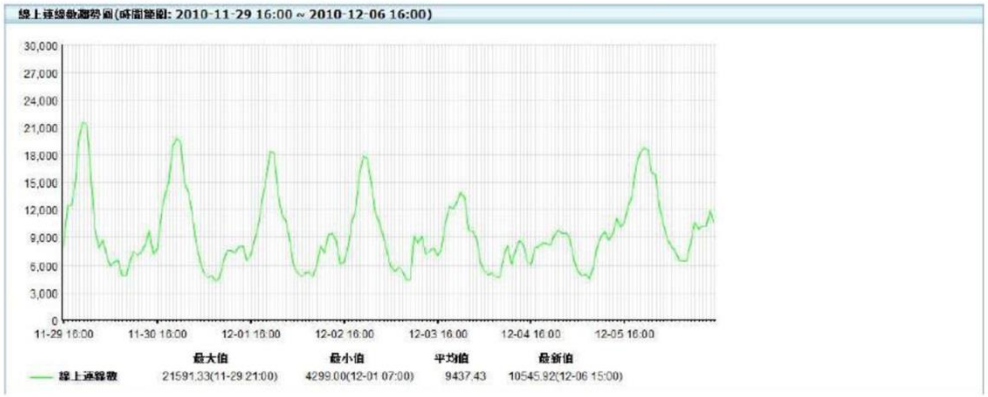
3-1-2．記憶體使用率

位置：統計分析 -> 設備資源 -> 記憶體使用率
說明：查詢最近一小時、一天、一周、一月、或自定義時間查詢記憶體運作資訊。



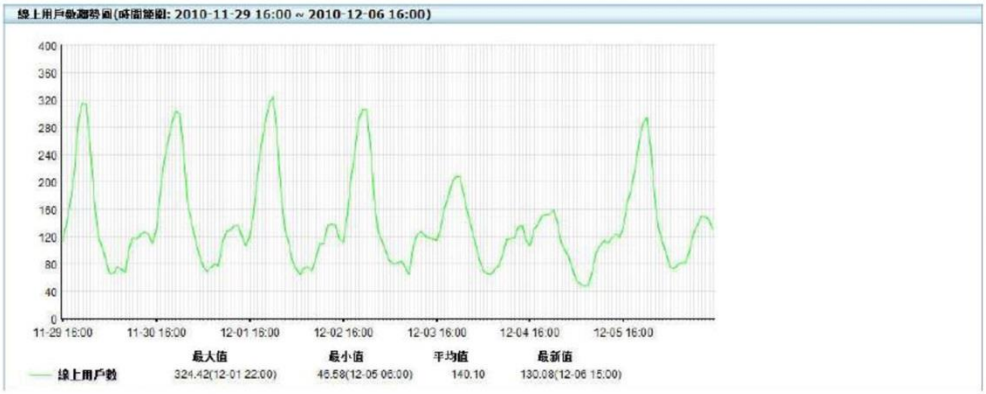
3-1-3．線上連線數

位置：統計分析 -> 設備資源 -> 線上連線數
說明：查詢最近一小時、一天、一周、一月、或自定義時間查詢活躍會話運作資訊。



3-1-4．線上用戶

位置：統計分析 -> 設備資源 -> 線上用戶
說明：查詢最近一小時、一天、一周、一月、或自定義時間查詢線上用戶運作資訊。



3-1-5．在線認證用戶數

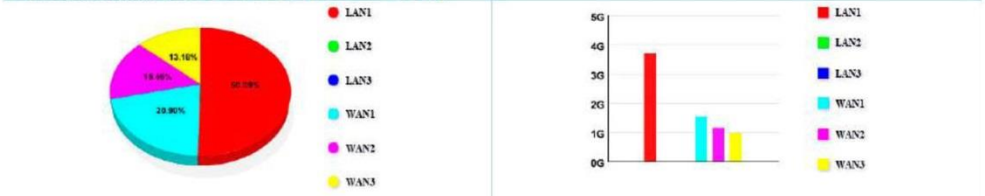
位置：統計分析 -> 設備資源 -> 在線認證用戶數
說明：查詢最近一小時、一天、一周、一月、或自定義時間查詢在線認證用戶運作資訊。

3-2・實體 Port

位置：統計分析 ->實體Port

說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢Port使用量。

實體端口統計圖(時間範圍: 2010-06-08 12:00:00 ~ 2010-06-08 13:00:00)



排序列表(時間範圍: 2010-06-08 12:00:00 ~ 2010-06-08 13:00:00)

序號	實體端口	百分比	詳細	流量(Byte)			平均速率(bps)			峰值速率(bps)		
				總	接收	發送	總	平均接收	平均發送	總	接收峰值	發送峰值
	總計	100.00%		7.36G	3.70G	3.66G	16.35M	8.21M	8.13M	9.86M	5.31M	9.09M
1	LAN1	50.39%		3.71G	394.91M	3.31G	8.24M	877.58K	7.36M	9.86M	2.17M	9.09M
2	LAN2	0.00%		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
3	LAN3	0.00%		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
4	WAN1	20.90%		1.54G	1.31G	224.11M	3.42M	2.92M	498.03K	4.95M	4.64M	1.77M
5	WAN2	15.55%		1.14G	1.09G	51.93M	2.54M	2.43M	115.40K	5.46M	5.31M	188.98K
6	WAN3	13.16%		968.25M	895.82M	72.43M	2.15M	1.99M	160.95K	4.04M	3.82M	233.30K

3-3・服務統計

3-3-1・流量統計

位置：統計分析 -> 服務統計 -> 流量統計

說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢流量。

設計條件

群組 [選擇]

排序對象 ◉總流量 ○上傳流量 ○下載流量
(以此參數作為排序的對象，按此參數的統計值來計算百分比)

服務選擇 服務類型 ALL 服務名稱 ALL

組合條件選擇 ○用戶 ○協議:

每頁顯示記錄數 20

[確定]

前十名服務統計圖(排序對象: 總流量; 時間範圍: 2010-12-08 16:00 ~ 2010-12-08 17:00)

排序列表(排序對象: 總流量; 時間範圍: 2010-12-08 16:00 ~ 2010-12-08 17:00)

總記錄數: 64 頁碼: 1/4 下一頁

序號	服務名稱	百分比	詳細	流量(Byte)			平均速率(bps)			峰值速率(bps)		
				總	上傳	下載	總	上傳	下載	總	上傳	下載
	總計	100.00%		12.16G	2.59G	9.57G	27.03M	5.75M	21.27M			
1	PPStream	29.22%		3.55G	1.06G	2.49G	7.90M	2.35M	5.54M	12.43M	2.92M	9.77M
2	HTTP	14.02%		1.71G	123.25M	1.58G	3.79M	273.89K	3.52M	8.47M	346.16K	8.15M
3	Web下載	13.99%		1.70G	43.48M	1.66G	3.78M	96.62K	3.68M	7.18M	156.02K	7.03M

3-3-2・新建連線

位置：統計分析 -> 服務統計 -> 新建連線
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢連線數。

排序列表(排序對象：總新建連線數；時間範圍: 2010-12-08 16:10 ~ 2010-12-08 17:10)

總記錄數：64 頁碼：1/4 下一頁

序號	服務名稱	百分比	詳細	新建連線數			新建連線平均速率(sps)			新建連線峰值速率(sps)		
				總	上傳	下載	總	上傳	下載	總	上傳	下載
	總計	100.00%		426.83K	426.83K	1	118.56	118.56	0.00			
1	BT	26.71%		114.02K	114.02K	0	31.67	31.67	0.00	79.88	79.88	0.00

3-3-3・線上連線

位置：統計分析 -> 服務統計 -> 線上連線
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢連線數。

排序列表(排序對象：總平均線上連線數；時間範圍: 2010-12-08 16:10 ~ 2010-12-08 17:10)

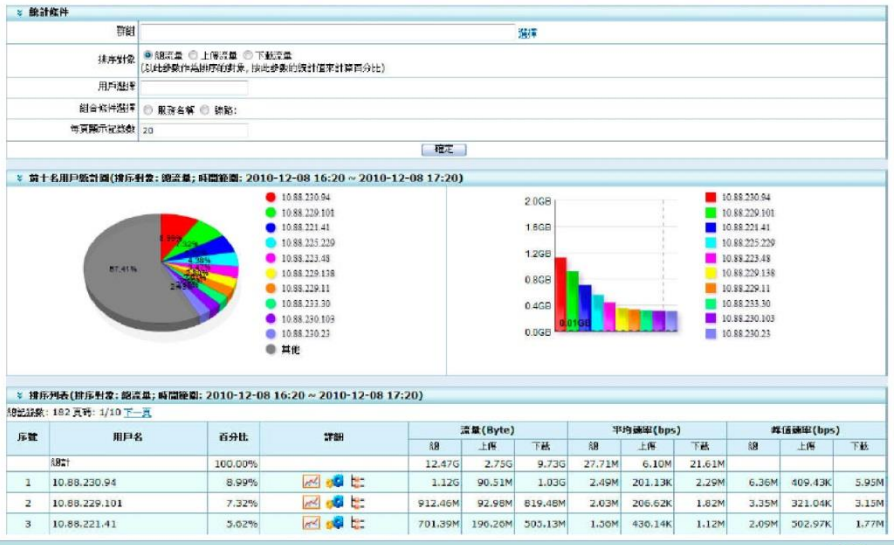
總記錄數：64 頁碼：1/4 下一頁

序號	服務名稱	百分比	詳細	平均線上連線數			峰值線上連線數		
				總	上傳	下載	總	上傳	下載
	總計	100.00%		10.50K	10.50K	1.01			
1	HTTP	17.99%		1.89K	1.89K	0.00	3.33K	3.33K	0.00

3-4・用戶分析

3-4-1・流量統計

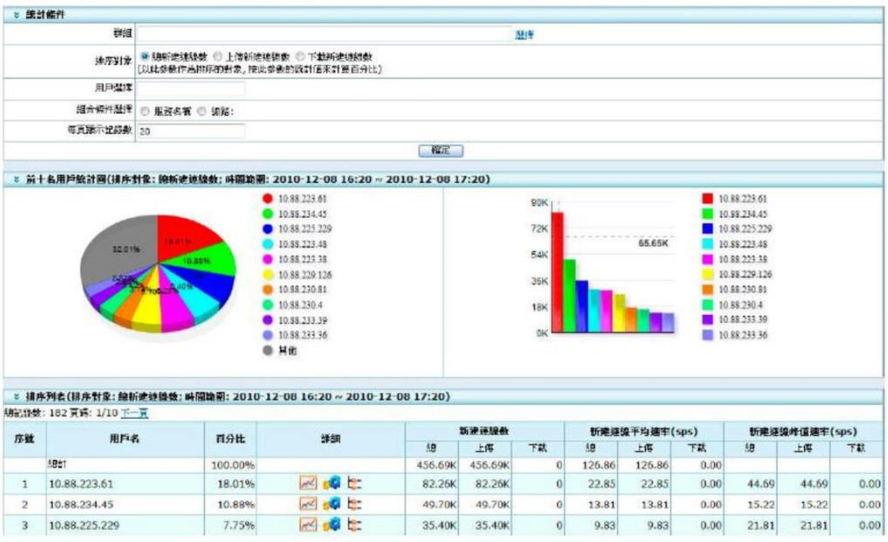
位置：統計分析 -> 用戶分析 -> 流量統計
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢流量。



序號	用戶名	百分比	詳細	流量(Byte)			平均速率(bps)			峰值速率(bps)		
				總	上傳	下載	總	上傳	下載	總	上傳	下載
	總計	100.00%		12.47G	2.75G	9.73G	27.71M	6.10M	21.61M			
1	10.88.230.94	8.99%		1.12G	90.51M	1.03G	2.49M	201.13K	2.29M	6.36M	409.43K	5.95M
2	10.88.229.101	7.32%		912.46M	92.98M	819.48M	2.03M	206.62K	1.82M	3.35M	321.04K	3.15M
3	10.88.221.41	5.62%		701.39M	196.26M	505.13M	1.56M	436.14K	1.12M	2.09M	502.97K	1.77M

3-4-2・新建連線

位置：統計分析 -> 用戶分析 -> 新建連線
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢連線數。



序號	用戶名	百分比	詳細	新建連線數			新建連線平均速率(sps)			新建連線峰值速率(sps)		
				總	上傳	下載	總	上傳	下載	總	上傳	下載
	總計	100.00%		456.69K	456.69K	0	126.86	126.86	0.00			
1	10.88.223.61	18.01%		82.26K	82.26K	0	22.85	22.85	0.00	44.69	44.69	0.00
2	10.88.234.45	10.88%		49.70K	49.70K	0	13.81	13.81	0.00	15.22	15.22	0.00
3	10.88.225.229	7.75%		35.40K	35.40K	0	9.83	9.83	0.00	21.81	21.81	0.00

3-4-3・線上連線

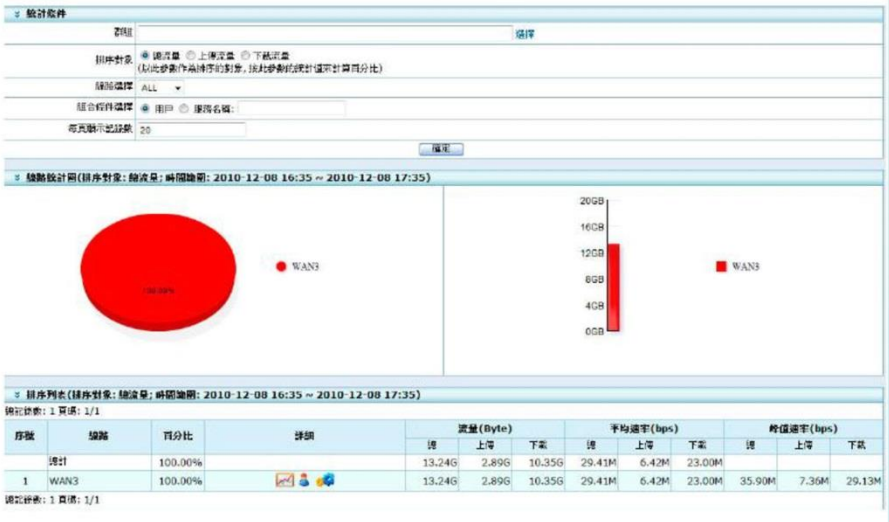
位置：統計分析 -> 用戶分析 -> 線上連線
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢連線數。

序號	用戶名	百分比	詳細	平均線上連線數			峰值線上連線數		
				總	上傳	下載	總	上傳	下載
	總計	100.00%		10.34K	10.34K	1.00			
1	10.88.223.61	11.18%		1.16K	1.16K	0.00	2.04K	2.04K	0.00
2	10.88.234.45	9.39%		971.36	971.36	0.00	1.19K	1.19K	0.00
3	10.88.225.229	8.45%		873.59	873.59	0.00	1.28K	1.28K	0.00

3-5・線路統計

3-5-1・流量統計

位置：統計分析 -> 線路分析 -> 流量統計
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢流量。

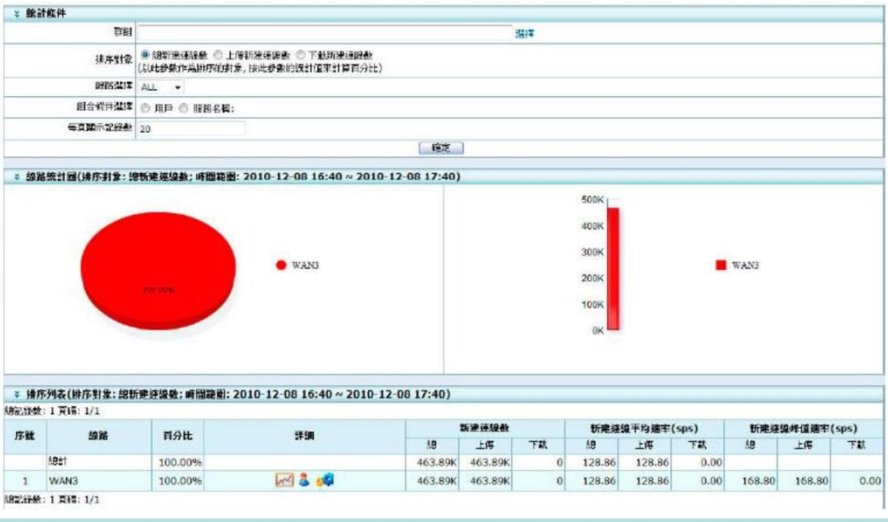


序號	線路	百分比	詳細	流量(Byte)			平均速率(bps)			峰值速率(bps)		
				總	上傳	下載	總	上傳	下載	總	上傳	下載
	總計	100.00%		13.24G	2.89G	10.35G	29.41M	6.42M	23.00M			
1	WAN3	100.00%		13.24G	2.89G	10.35G	29.41M	6.42M	23.00M	35.90M	7.36M	29.13M

總記錄數: 1 頁碼: 1/1

3-5-2・新建連線

位置：統計分析 -> 線路分析 -> 新建連線
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢會話量。



3-5-3・線上連線

位置：統計分析 -> 線路分析 -> 線上連線
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢連線數。

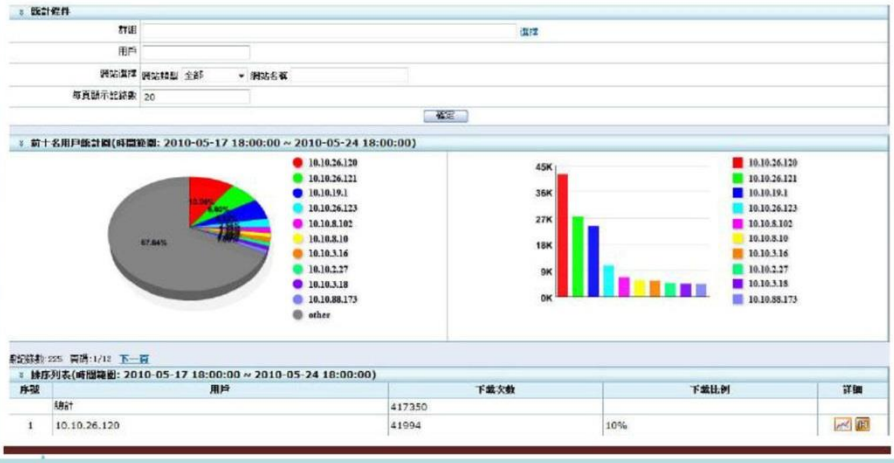
3-6・URL 排名

3-6-1・基於網站

位置：統計分析 -> URL排名 -> 基於網站
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢網站排名。

3-6-2・基於用戶

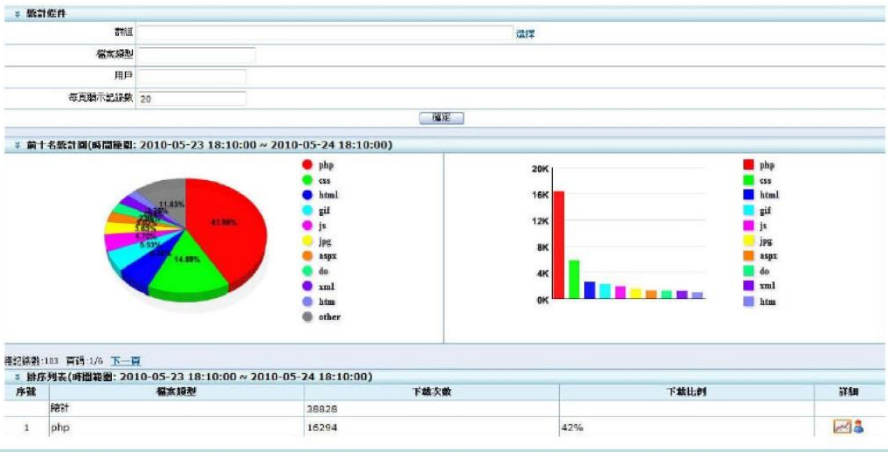
位置：統計分析 -> URL排名 -> 基於用戶
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢用戶排名。



3-7・下載檔案類型排名

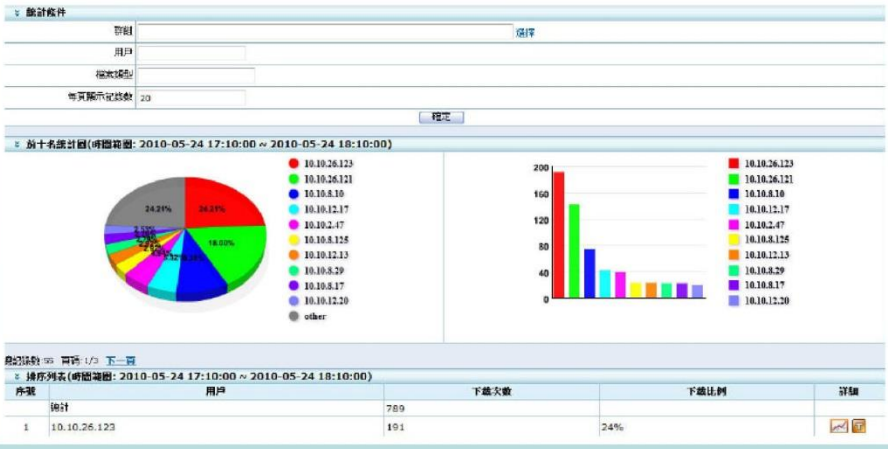
3-7-1・基於檔案類型

位置：統計分析 -> URL排名 -> 基於網站
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢網頁檔案排名。



3-7-2・基於用戶

位置：統計分析 -> URL排名 -> 基於用戶
說明：顯示最近一小時、一天、一周、一月、或自定義時間查詢用戶排名。



4・行為分析

4-1・Web 記錄

4-1-1・網頁標題記錄

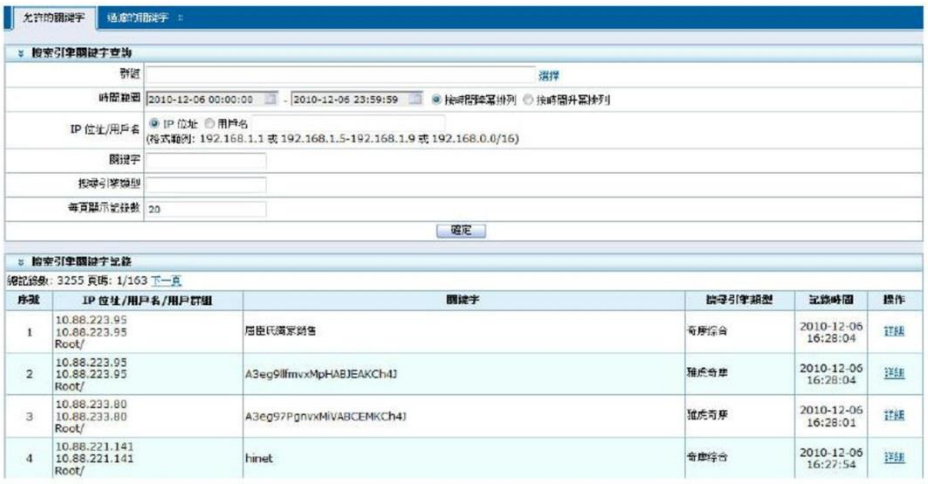
位置：行為分析 -> Web記錄 -> 網頁標題記錄
說明：查詢用戶使用網頁搜尋紀錄。

4-1-2・論壇發文/評論紀錄

位置：行為分析 -> Web記錄 ->論壇發文/評論紀錄
說明：查詢用戶使用張貼文章記錄。

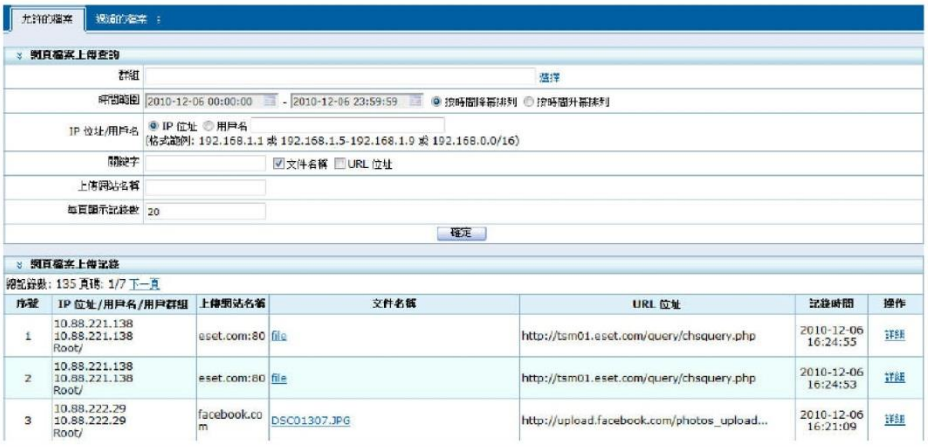
4-1-3．搜索引擎紀錄

位置：行為分析 -> Web記錄 -> 搜尋引擎紀錄
說明：查詢用戶使用搜尋關鍵字記錄。



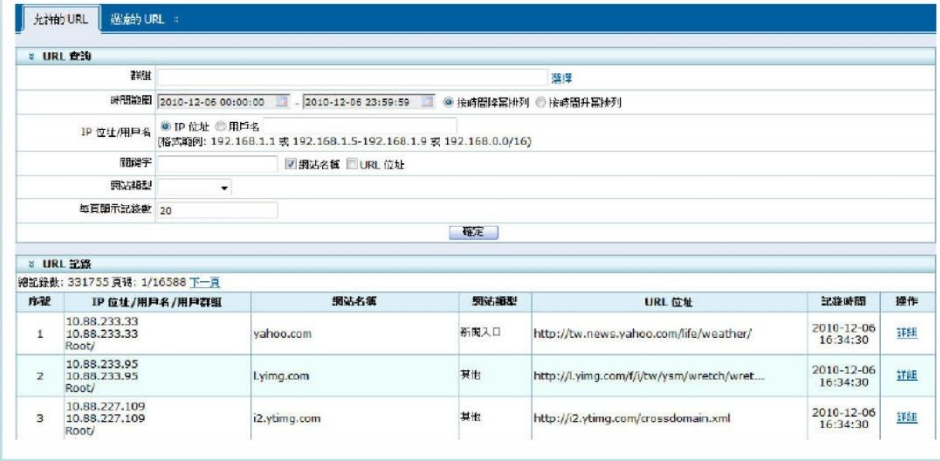
4-1-4．網頁檔案上傳記錄

位置：行為分析 -> Web記錄 -> 網頁檔案上傳記錄
說明：查詢用戶上傳檔案紀錄。



4-1-5 · URL 記錄

位置：行為分析 -> Web記錄 -> URL 記錄
說明：查詢用戶 URL記錄。



4-2 · 郵件記錄

4-2-1 · 允許的郵件

位置：行為分析 -> 郵件記錄 -> 允許的郵件
說明：查詢郵件內容。

4-2-2 · 過濾的郵件

位置：行為分析 -> 郵件記錄 -> 過濾的郵件
說明：查詢過濾郵件。

4-3 · FTP 記錄

4-3-1 · 允許的 FTP 傳輸

位置：行為分析 -> FTP 記錄 -> 允許的FTP傳輸
說明：查詢用戶登入、上下載記錄。

4-3-2・過濾的 FTP 傳輸

位置：行為分析 -> FTP 記錄 -> 過濾的FTP傳輸
說明：查詢用戶過濾上下載記錄。

4-4・即時通訊

4-4-1・MSN

位置：行為分析 -> 即時通訊 -> MSN
說明：查詢MSN登入、聊天、檔案傳輸記錄。

4-4-2 · QQ

位置：行為分析 -> 即時通訊 -> QQ
說明：查詢QQ登入記錄。

4-4-3 · Yahoo

位置：行為分析 -> 即時通訊 -> Yahoo
說明：查詢Yahoo即時通登入、聊天、檔案傳輸記錄。

4-4-4 · ICQ

位置：行為分析 -> 即時通訊 -> ICQ
說明：查詢ICQ登入、聊天、檔案傳輸記錄。

4-5 · 連線記錄

位置：行為分析 -> 連線記錄
說明：查詢用戶各個連結來源與目的、對外PORT的顯示、服務種類的區分。

序號	來源(IP: 埠)	目的(IP: 埠)	轉換(IP: 埠)	協議類型	服務名稱	傳送資料大小	接收資料大小	線上時間	記錄時間
1	10.88.229.4: 4139	60.199.252.179: 80		TCP	HTTP	778B	762B	140Sec	2010-12-06 16:53:30
2	10.88.233.93: 1575	125.46.41.163: 80		TCP	360軟件更新	1.7KB	40.1KB	121Sec	2010-12-06 16:53:30
3	10.88.231.54: 22905	75.61.69.105: 44516		UDP	Skype	107B	424B	30Sec	2010-12-06 16:53:30
4	10.88.234.54: 1449	203.84.197.77: 80		TCP	HTTP	10.0KB	189.9KB	39Sec	2010-12-06 16:53:30
5	10.88.233.44: 10044	183.12.99.132: 47757		UDP	其他UDP協議	3.2KB	44.7KB	481Sec	2010-12-06 16:53:30
6	10.88.234.24: 59744	71.74.159.133: 37485		TCP	Gnutella	638B	531B	121Sec	2010-12-06 16:53:30
7	10.88.234.24: 59742	122.108.6.195: 38239		TCP	Gnutella	637B	932B	121Sec	2010-12-06 16:53:30
8	10.88.221.7: 1036	113.31.31.198: 80		TCP	HTTP	801B	441B	120Sec	2010-12-06 16:53:30
9	10.88.225.8: 1267	203.84.197.9: 80		TCP	HTTP	3.5KB	1.6KB	180Sec	2010-12-06 16:53:30

4-6．阻斷紀錄

4-6-1．防火牆阻斷

位置：行為分析 -> 阻斷紀錄 -> 防火牆阻斷
說明：安全策略阻擋紀錄。

防火牆阻斷

防火牆阻斷查詢

時間範圍 2010-12-01 00:00:00 - 2010-12-01 23:59:59 ◉ 按時間降冪排列 ○ 按時間升冪排列

IP 位址 來源 IP 位址: 目的 IP 位址:
(格式範例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)

協議及埠 協議種類

每頁顯示記錄數 20

確定

防火牆阻斷記錄

總記錄數: 361 頁碼: 2/19 第一頁 上一頁 下一頁

序號	來源(IP: 埠)	目的(IP: 埠)	協議種類	封包長度	策略名稱	記錄時間
21	220.191.180.126: 36864	192.168.1.1: 4875	ICMP	92	Deny	2010-12-01 17:50:19
22	83.234.148.125: 5632	192.168.1.19: 53216	ICMP	28	Deny	2010-12-01 17:49:50
23	212.174.243.178: 0	192.168.1.10: 256	ICMP	28	Deny	2010-12-01 17:49:41
24	222.89.243.121: 45054	192.168.1.11: 1433	TCP	40	Deny	2010-12-01 17:47:47
25	124.125.125.213: 0	192.168.1.14: 256	ICMP	28	Deny	2010-12-01 17:38:55
26	72.167.162.215: 36105	192.168.1.11: 80	TCP	48	Deny	2010-12-01 17:37:29
27	184.106.172.104: 5086	192.168.1.252: 5060	UDP	447	Deny	2010-12-01 17:36:29
28	184.106.172.104: 5086	192.168.1.1: 5060	UDP	446	Deny	2010-12-01 17:36:28
29	66.249.71.136: 49557	192.168.1.23: 80	TCP	60	Deny	2010-12-01 17:35:34
30	66.249.71.136: 49557	192.168.1.23: 80	TCP	60	Deny	2010-12-01 17:35:10

4-6-2．流量管理阻斷

位置：行為分析 -> 阻斷紀錄 -> 流量管理阻斷
說明：流量管理阻擋紀錄。

流量管理阻斷

流量管理阻斷查詢

時間範圍 2010-12-01 00:00:00 - 2010-12-01 23:59:59 ◉ 按時間降冪排列 ○ 按時間升冪排列

IP 位址 來源 IP 位址: 目的 IP 位址: 轉換 IP:
(格式範例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)

服務或協議 ○ 服務名稱 ○ 協議及埠:

每頁顯示記錄數 20

確定

流量管理阻斷記錄

總記錄數: 1262 頁碼: 4/64 第一頁 上一頁 下一頁

序號	來源(IP: 埠)	目的(IP: 埠)	轉換(IP: 埠)	協議類型	服務名稱	封包長度	策略名稱	記錄時間
61	172.16.15.118: 12983	182.61.129.55: 8899		UDP	PPStream	73	computer172.16.9.0	2010-12-01 17:36:03
62	172.16.12.208: 1750	72.14.203.148: 80	[redacted].254: 1750	TCP	YouTube	592	computer172.16.9.0	2010-12-01 17:35:57
63	172.16.12.208: 1742	74.125.11.97: 80	[redacted].254: 1742	TCP	YouTube	1500	computer172.16.9.0	2010-12-01 17:35:53
64	172.16.12.208: 1732	72.14.203.148: 80	[redacted].254: 1732	TCP	YouTube	592	computer172.16.9.0	2010-12-01 17:35:49
65	172.16.12.208: 1724	72.14.203.148: 80	[redacted].254: 1724	TCP	YouTube	592	computer172.16.9.0	2010-12-01 17:35:44
66	172.16.15.118: 12983	125.46.40.50: 8400		UDP	PPStream	173	computer172.16.9.0	2010-12-01 17:35:43
67	172.16.12.208: 1708	72.14.203.148: 80	[redacted].254: 1708	TCP	YouTube	592	computer172.16.9.0	2010-12-01 17:35:38
68	172.16.15.118: 12983	182.61.129.55: 8899		UDP	PPStream	73	computer172.16.9.0	2010-12-01 17:35:03
69	172.16.15.118: 12983	125.46.40.11: 8400		UDP	PPStream	147	computer172.16.9.0	2010-12-01 17:34:48
70	172.16.16.10: 1108	72.14.203.102: 80	[redacted].254: 1108	TCP	YouTube	404	computer172.16.9.0	2010-12-01 17:34:44

4-6-3・行為管理阻斷

位置：行為分析 -> 阻斷紀錄 -> 行為管理阻斷
說明：行為管理阻擋紀錄。


行為管理阻斷

行為管理阻斷查詢

時間範圍 2010-12-01 00:00:00 - 2010-12-01 23:59:59 ◉ 按時間降冪排列 ○ 按時間升冪排列

IP 位址 來源 IP 位址: 目的 IP 位址: 轉換 IP:
(格式範例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)

服務或協議 ◉ 服務名稱 ○ 協議及埠:

每頁顯示記錄數 20

確定

行為管理阻斷記錄

總記錄數: 12 頁碼: 1/1

序號	來源(IP: 埠)	目的(IP: 埠)	轉換(IP: 埠)	協議類型	服務名稱	封包長度	記錄時間
1	192.168.0.5: 52674	116.214.4.25: 80	211.20.233.246: 52674	TCP	其他TCP協議	890	2010-12-01 18:24:27
2	192.168.0.5: 52668	116.214.4.25: 80	211.20.233.246: 52668	TCP	其他TCP協議	845	2010-12-01 18:24:18
3	192.168.0.5: 52659	116.214.4.25: 80	211.20.233.246: 52659	TCP	其他TCP協議	851	2010-12-01 18:24:08
4	192.168.0.5: 52622	64.4.45.62: 1863	211.20.233.246: 52622	TCP	其他TCP協議	190	2010-12-01 18:23:56
5	192.168.0.5: 52616	64.4.45.62: 1863	211.20.233.246: 52616	TCP	其他TCP協議	190	2010-12-01 18:23:53
6	192.168.0.5: 52602	64.4.45.62: 1863	211.20.233.246: 52602	TCP	其他TCP協議	66	2010-12-01 18:23:44
7	192.168.0.5: 52442	64.4.61.82: 1863	211.20.233.246: 52442	TCP	MSN	46	2010-12-01 18:23:40
8	192.168.0.5: 52442	64.4.61.82: 1863	211.20.233.246: 52442	TCP	MSN	45	2010-12-01 18:23:27
9	192.168.0.5: 52442	64.4.61.82: 1863	211.20.233.246: 52442	TCP	MSN	45	2010-12-01 18:23:19
10	192.168.0.5: 52442	64.4.61.82: 1863	211.20.233.246: 52442	TCP	MSN	45	2010-12-01 18:23:16

5・資料管理

5-1・紀錄資料列表

位置：資料管理 -> 紀錄資料列表
說明：記錄Reporter訊息，硬碟使用量。

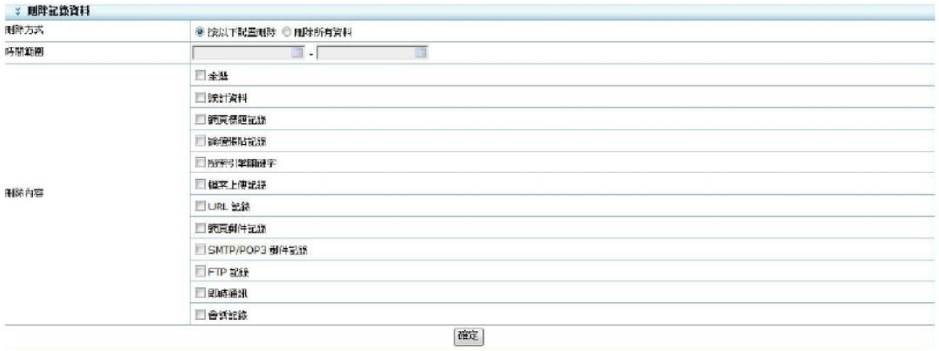

記錄資料列表

資料類型	使用儲存空間	使用儲存空間比例
統計資料	864.63M	2.13%
網頁瀏覽記錄	22.20M	0.05%
詢問單點記錄		
搜索引擎關鍵字	2.12M	0.01%
檔案上傳記錄		
URL 記錄	138.11M	0.34%
網頁郵件記錄	1.06M	0.00%
SMTP/POP3 郵件記錄	5.08M	0.01%
FTP 記錄	857.09K	0.00%
即時通訊	1.64M	0.00%
會話記錄	329.74M	0.81%

總硬盤空間: 40.51G 已使用儲存空間: 1.42G(3.51%) 可用儲存空間: 37.03G(96.49%)

5-2．刪除紀錄資料

位置：資料管理 -> 刪除記錄列表
說明：清除記錄資訊。



5-3．資料備份

5-3-1．備份伺服器

位置：資料管理 -> 資料備份 -> 備份伺服器
說明：備份伺服器設定。

5-3-2．自動備份

位置：資料管理 -> 資料備份 -> 自動備份
說明：自動備份模式設定。

5-3-3．手動備份

位置：資料管理 -> 資料備份 -> 手動備份
說明：手動選擇時間備份。

5-3-4．備份列表

位置：資料管理 -> 資料備份 -> 備份列表
說明：備份檔案查詢。

6．報表管理

6-1．報表列表

位置：報表管理 -> 報表列表
說明：產生每日、每周、每月、每年報表。

6-2．報表配置

位置：報表管理 -> 報表配置
說明：報表記錄開關。

6-3．手動報表

位置：報表管理 -> 手動報表
說明：增加自定義時間範圍報表。

7．個人行為

7-1．綜合

位置：個人行為 -> 綜合
說明：依照組織結構產生的群組區分項目上網行為。

即時通訊

MSN

MSN 帳號	登入次數	聊天記錄數	傳輸檔案數
[redacted]@hotmail.com	1	0	0
[redacted]@yahoo.com.tw	1	0	0
[redacted]@hotmail.com	2	146	0

QQ

QQ 帳號	登入次數	聊天記錄數	傳輸檔案數

Yahoo

Yahoo 帳號	登入次數	聊天記錄數	傳輸檔案數

ICQ

ICQ 帳號	登入次數	聊天記錄數	傳輸檔案數

郵件記錄

郵件記錄

郵件帳號	發信數	收信數
[redacted]@yahoo.com.tw - yahoo 郵箱	2	0

FTP 記錄

FTP 記錄

登入次數	上傳檔案數	下載檔案數
0	0	0

7-2 · Web 紀錄

位置：個人行為 -> Web紀錄
說明：依照組織結構產生的群組區分項目上網行為。

7-3．即時通訊

位置：個人行為 -> 即時通訊
說明：依照組織結構產生的群組區分項目上網行為。

7-4．郵件紀錄

位置：個人行為 -> 郵件紀錄
說明：依照組織結構產生的群組區分項目上網行為。

7-5．FTP 紀錄

位置：個人行為 -> FTP紀錄
說明：依照組織結構產生的群組區分項目上網行為。

8．Reporter 搜尋範例 & 查詢應用

範例 1

查詢應用：即時掌控服務類型應用在哪些使用者上。
【點擊 MSN 可以立即顯示哪些用戶在使用，當出現 FOXY、BT..等服務時，立即掌握用戶線況】

範例 2

查詢應用：即時掌控使用者應用在哪些服務類型上。

【點擊用戶名稱可以立即顯示用戶在使用的服務，監控用戶上行、下行是否大量異常】

範例 3

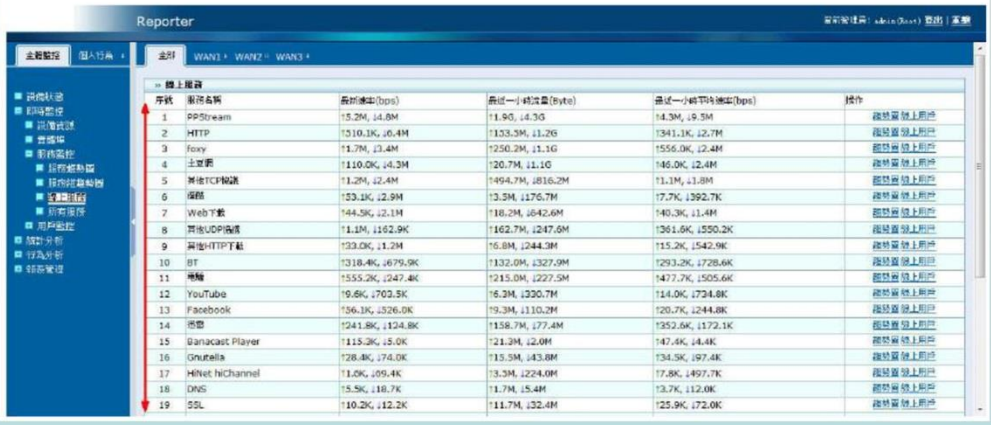
查詢應用：即時掌控連線數異常飆高。

【是否有異常金字塔飆高情況，Reporter 內統計分析>設備資源可以顯示時、日、月狀況】

範例 4

查詢應用：即時掌控服務類型上是否異常。

【顯示主要流量使用在哪個服務，發現異常時可以點擊在線用戶隨時了解用戶 IP 馬上處理或阻擋】



範例 5

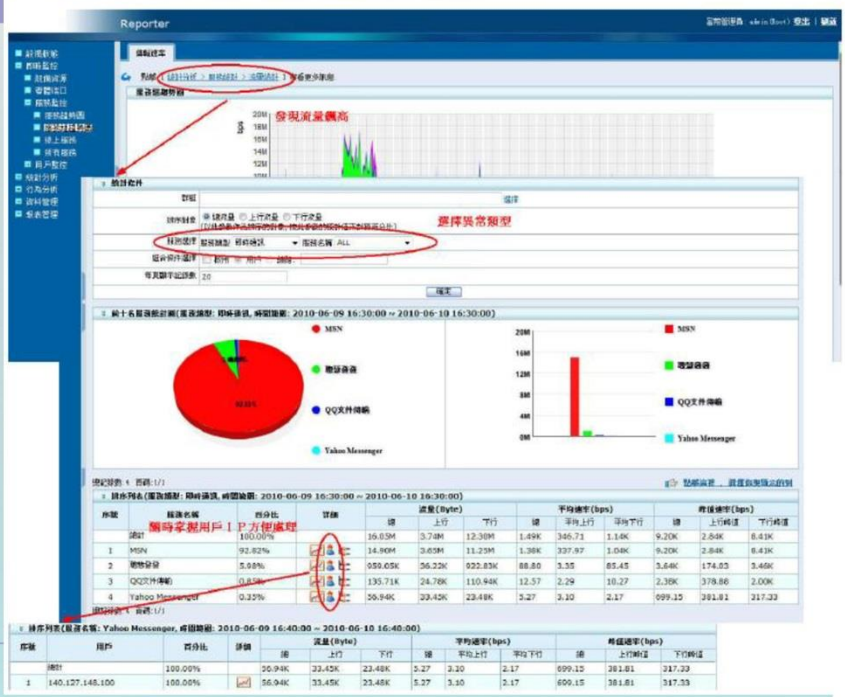
查詢應用：即時掌控所有服務類型流量與使用狀況

【查詢線上有在使用的服務，區分類型方便查找，可以有效防止頻寬占用。】

範例 6

搜尋範例：針對服務類型占用頻寬查詢到用戶 IP

【利用服務群組了解頻寬異常，往下搜尋原因與用戶資訊。】



範例 7

搜尋範例：針對上下載占用頻寬查詢

【直接搜尋服務或用戶名，使用哪些 port 進出 NAT 為哪個 IP。】

範例 8

搜尋範例：針對中毒大量異常 port 發送查詢

【了解異常金字塔飆高情況，比對用戶與時間點，搜尋歷史用戶使用情況。】

序號	來源(IP:埠)	目的(IP:埠)	轉換(IP:埠)	通訊協定	服務名稱	傳送資料大小	接收資料大小	連線時間	記錄時間
1	140.127.146.99:445	218.172.80.110:2748	未轉換	TCP	其他TCP協議	108B	54B	61S	2010-06-05 01:32:28
2	140.127.146.99:55030	203.188.197.10:25	未轉換	TCP	UUCall	1.92KB	1.06KB	120S	2010-06-04 22:38:30
3	140.127.146.99:445	202.144.216.35:49800	未轉換	TCP	其他TCP協議	216B	162B	120S	2010-06-04 22:21:03
4	140.127.146.99:80	202.144.216.35:49799	未轉換	TCP	其他TCP協議	162B	108B	120S	2010-06-04 22:21:03
5	140.127.146.99:445	61.223.13.145:2503	未轉換	TCP	其他TCP協議	108B	54B	60S	2010-06-04 19:26:02
6	140.127.146.99:80	60.250.140.123:46891	未轉換	TCP	其他TCP協議	108B	54B	65S	2010-06-04 16:51:41
7	140.127.146.99:445	59.104.123.172:53089	未轉換	TCP	其他TCP協議	108B	162B	10S	2010-06-04 15:19:50
8	140.127.146.99:80	59.104.123.172:53091	未轉換	TCP	其他TCP協議	108B	108B	10S	2010-06-04 15:19:50
9	140.127.146.99:445	118.232.40.194:61246	未轉換	TCP	其他TCP協議	270B	216B	124S	2010-06-04 14:11:34
10	140.127.146.99:80	218.163.156.67:49668	未轉換	TCP	其他TCP協議	108B	54B	60S	2010-06-04 12:35:16
11	140.127.146.99:445	203.79.199.4:56361	未轉換	TCP	其他TCP協議	132B	66B	60S	2010-06-04 11:47:35
12	140.127.146.99:80	218.165.24.76:8465	未轉換	TCP	其他TCP協議	162B	216B	14S	2010-06-04 09:59:13
13	140.127.146.99:445	59.124.197.67:60426	未轉換	TCP	其他TCP協議	198B	162B	124S	2010-06-04 08:36:30
14	140.127.146.99:80	59.124.197.67:60422	未轉換	TCP	其他TCP協議	198B	162B	124S	2010-06-04 08:36:29
15	140.127.146.99:445	59.124.197.67:60406	未轉換	TCP	其他TCP協議	198B	162B	122S	2010-06-04 08:36:27
16	140.127.146.99:80	114.36.53.193:1108	未轉換	TCP	其他TCP協議	324B	270B	194S	2010-06-04 08:20:37
17	140.127.146.99:50138	72.14.203.121:80	未轉換	TCP	HTTP	719B	438B	120S	2010-06-04 07:58:14
18	140.127.146.99:54564	72.14.203.121:80	未轉換	TCP	HTTP	1.63KB	26.56KB	120S	2010-06-04 07:58:14
19	140.127.146.99:445	118.166.245.187:1511	未轉換	TCP	其他TCP協議	613B	1.27KB	277185	2010-06-04 04:51:57
20	140.127.146.99:80	61.230.74.76:3178	未轉換	TCP	HTTP	3.1KB	943B	379905	2010-06-04 00:17:54

範例 9

查詢應用：NAT 轉換 IP 與時間對照

【透過 IP 用戶名查詢 NAT 為哪個 IP 對外、依照服務類、詳細時間點】

範例 10

搜尋範例：查詢用戶線上即時通訊所有資訊

【包括 Web 瀏覽紀錄、論壇發文記錄、檔案上下傳與 URL 記錄..等】

範例 11

查詢應用：防火牆被阻擋 IP，策略名稱與時間對照

【透過 IP 來源資料，顯示被阻擋的 IP、哪一個策略條件、詳細時間點】

範例 12

查詢應用：流量管理被阻擋 IP，NAT 轉換、使用服務、策略名稱與時間對照

【透過 IP 來源資料，顯示被阻擋的 IP、哪一個策略條件、詳細時間點】

範例 13

查詢應用：行為管理被阻擋 IP，策略名稱與時間對照

【透過 IP 來源資料，顯示被阻擋的 IP、哪一個服務名稱、詳細時間點】

Thank You

Q&A

簽到單

博鉅資訊股份有限公司

網路實務研習營簽到表

日期：103 年 4 月 11 日下午 13:00～17:00
地點：台北海洋技術學院圖書館會議室
講師：王智民先生

單位	與會人員	簽名
圖資中心主任	陳建宏	陳建宏
圖資中心網路組	蔡慧貞	蔡慧貞
圖資中心資訊組	蔡彥志	蔡彥志
圖資中心資訊組	張哲偉	張哲偉
圖資中心資訊組	郭子傑	郭子傑