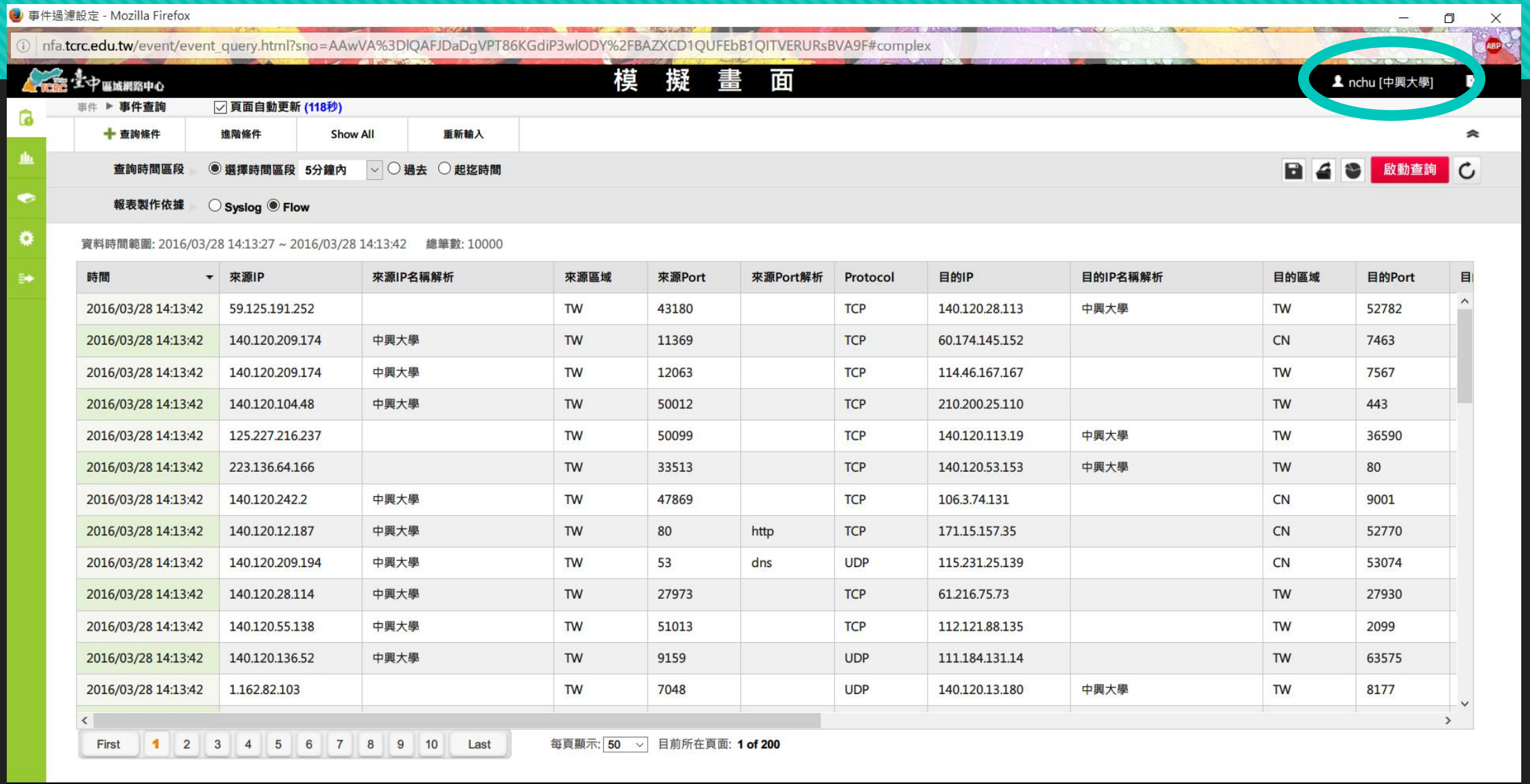
網路障礙分析與資安事件監控軟體 N-Reporter 基礎介紹

台中區網中心 鄒珮甄

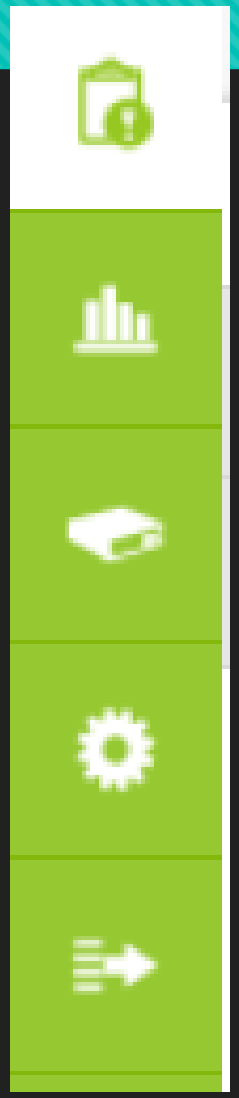
基礎畫面介紹

- 請輸入http://nfa.tcrc.edu.tw
- 輸入帳號密碼
- 不要封鎖視窗

基礎畫面介紹


事件過濾設定 - Mozilla Firefox
nfa.tcrc.edu.tw/event/event_query.html?sno=AAwVA%3DlQAFJDaDgVPT86KGdiP3wlODY%2FBAZXCD1QUFEbB1QITVERURsBVA9F#complex
臺中區域網路中心
模 擬 畫 面
nchu [中興大學]
事件 ▶ 事件查詢
頁面自動更新 (118秒)
查詢條件
進階條件
Show All
重新輸入
查詢時間區段
選擇時間區段 5分鐘內
過去
起迄時間
啟動查詢
報表製作依據
Syslog
Flow
資料時間範圍: 2016/03/28 14:13:27 ~ 2016/03/28 14:13:42 總筆數: 10000
時間 來源IP 來源IP名稱解析 來源區域 來源Port 來源Port解析 Protocol 目的IP 目的IP名稱解析 目的區域 目的Port
2016/03/28 14:13:42 59.125.191.252 TW 43180 TCP 140.120.28.113 中興大學 TW 52782
2016/03/28 14:13:42 140.120.209.174 中興大學 TW 11369 TCP 60.174.145.152 CN 7463
2016/03/28 14:13:42 140.120.209.174 中興大學 TW 12063 TCP 114.46.167.167 TW 7567
2016/03/28 14:13:42 140.120.104.48 中興大學 TW 50012 TCP 210.200.25.110 TW 443
2016/03/28 14:13:42 125.227.216.237 TW 50099 TCP 140.120.113.19 中興大學 TW 36590
2016/03/28 14:13:42 223.136.64.166 TW 33513 TCP 140.120.53.153 中興大學 TW 80
2016/03/28 14:13:42 140.120.242.2 中興大學 TW 47869 TCP 106.3.74.131 CN 9001
2016/03/28 14:13:42 140.120.12.187 中興大學 TW 80 http TCP 171.15.157.35 CN 52770
2016/03/28 14:13:42 140.120.209.194 中興大學 TW 53 dns UDP 115.231.25.139 CN 53074
2016/03/28 14:13:42 140.120.28.114 中興大學 TW 27973 TCP 61.216.75.73 TW 27930
2016/03/28 14:13:42 140.120.55.138 中興大學 TW 51013 TCP 112.121.88.135 TW 2099
2016/03/28 14:13:42 140.120.136.52 中興大學 TW 9159 UDP 111.184.131.14 TW 63575
2016/03/28 14:13:42 1.162.82.103 TW 7048 UDP 140.120.13.180 中興大學 TW 8177
First 1 2 3 4 5 6 7 8 9 10 Last
每頁顯示: 50
目前所在頁面: 1 of 200

基礎畫面介紹



事件★

報表★

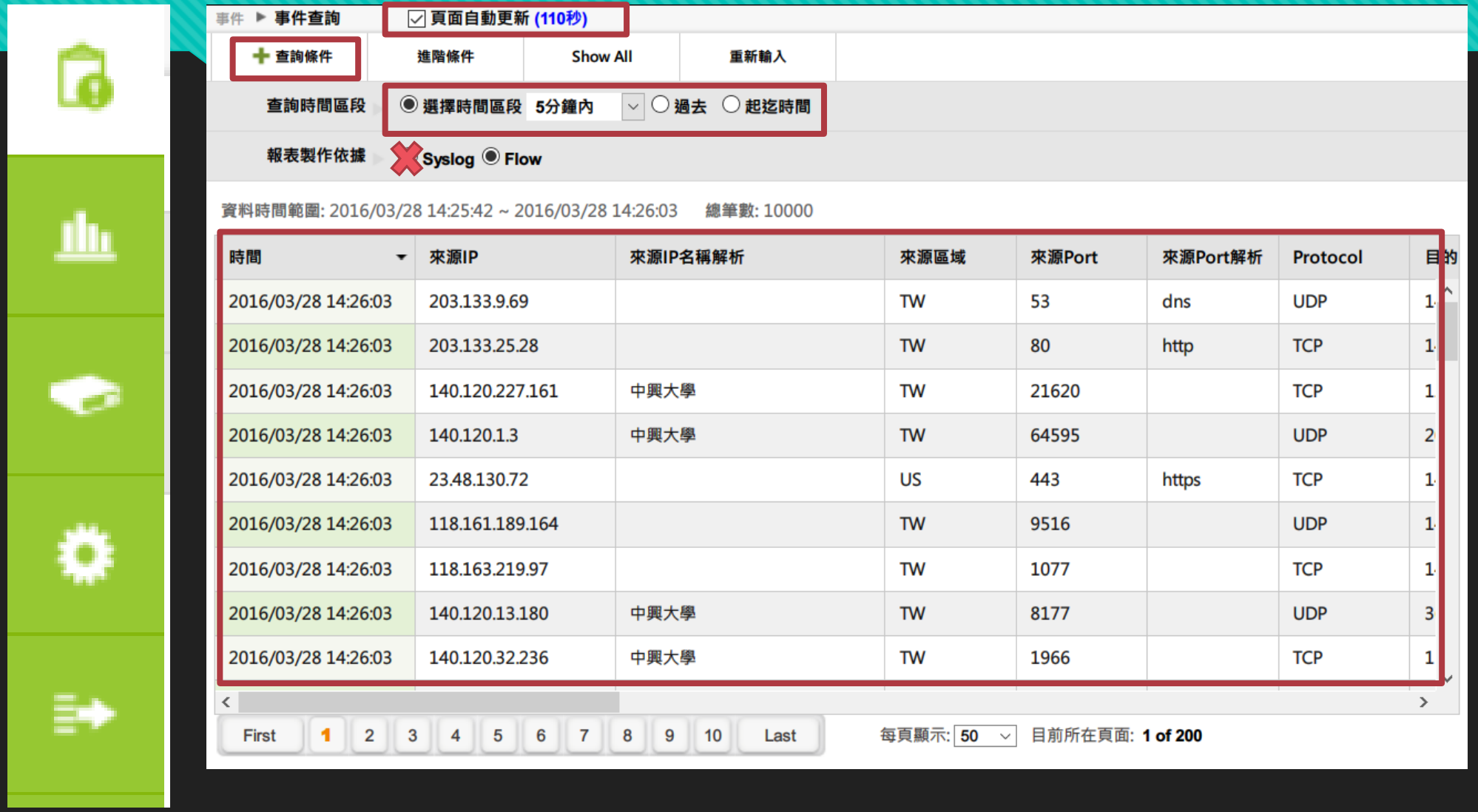
設備管理

系統管理★

收合功能視窗

基礎畫面介紹-事件

基礎畫面介紹-事件


事件 ▶ 事件查詢
頁面自動更新 (110秒)
查詢條件
進階條件
Show All
重新輸入
查詢時間區段
選擇時間區段 5分鐘內
過去
起迄時間
報表製作依據
Syslog
Flow
資料時間範圍: 2016/03/28 14:25:42 ~ 2016/03/28 14:26:03
總筆數: 10000
時間 | 來源IP | 來源IP名稱解析 | 來源區域 | 來源Port | 來源Port解析 | Protocol | 目的
2016/03/28 14:26:03 | 203.133.9.69 | | TW | 53 | dns | UDP
2016/03/28 14:26:03 | 203.133.25.28 | | TW | 80 | http | TCP
2016/03/28 14:26:03 | 140.120.227.161 | 中興大學 | TW | 21620 | | TCP
2016/03/28 14:26:03 | 140.120.1.3 | 中興大學 | TW | 64595 | | UDP
2016/03/28 14:26:03 | 23.48.130.72 | | US | 443 | https | TCP
2016/03/28 14:26:03 | 118.161.189.164 | | TW | 9516 | | UDP
2016/03/28 14:26:03 | 118.163.219.97 | | TW | 1077 | | TCP
2016/03/28 14:26:03 | 140.120.13.180 | 中興大學 | TW | 8177 | | UDP
2016/03/28 14:26:03 | 140.120.32.236 | 中興大學 | TW | 1966 | | TCP
First 1 2 3 4 5 6 7 8 9 10 Last
每頁顯示: 50
目前所在頁面: 1 of 200

基礎畫面介紹-事件

發生資安通報!

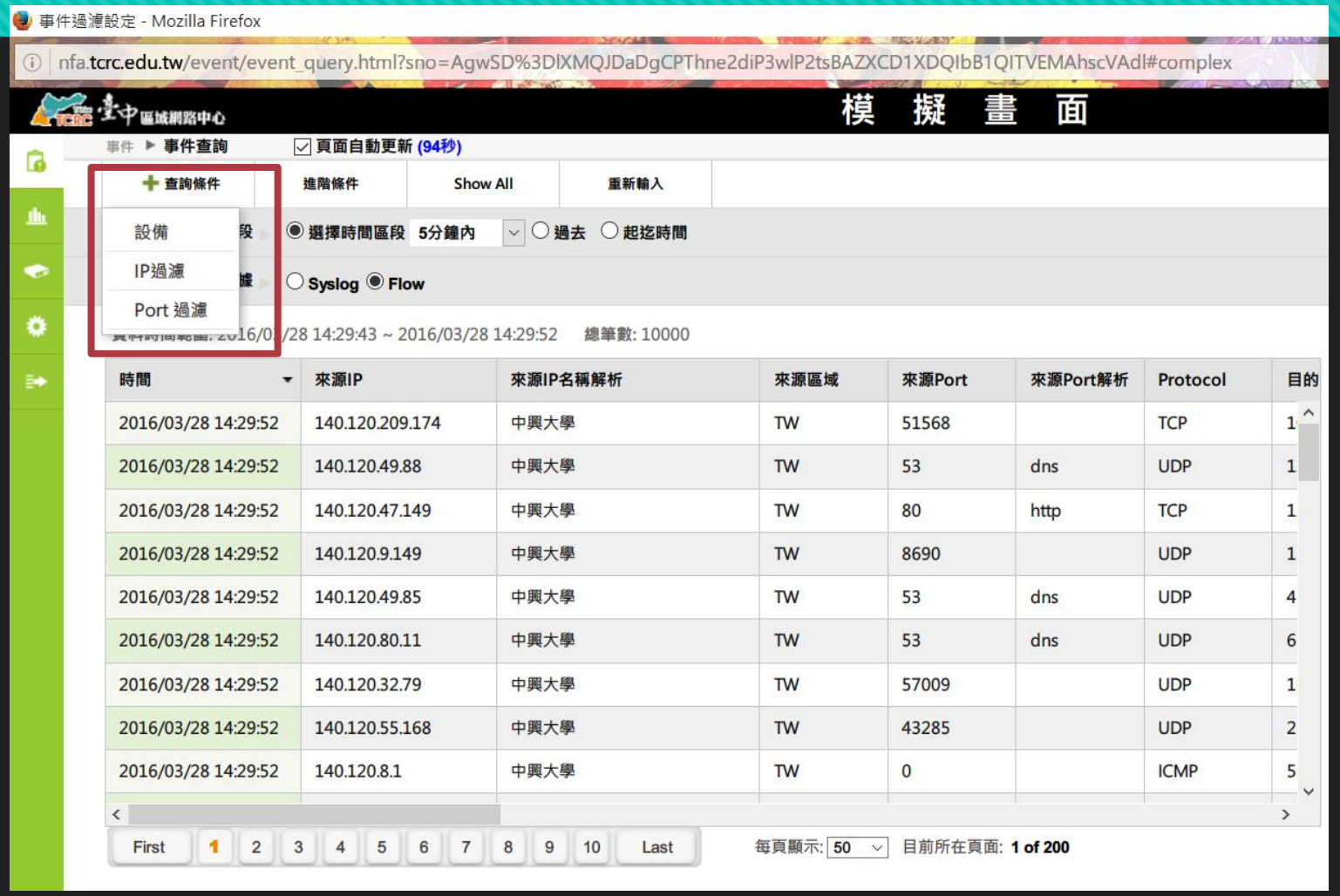
發佈編號	ASOC-INT-201603-0633	發佈時間	2016-03-03 09:17:02
事件類型	對外攻擊	發現時間	2016-03-03 09:02:06
事件主旨	通報:[國立中興大學]140.120.90.81 Telnet.Login.Brute.Force		
事件描述	ASOC 發現貴單位(國立中興大學)所屬 140.120.90.81 疑似對外進行 Telnet.Login.Brute.Force 攻擊		

基礎畫面介紹-事件

發生資安通報II

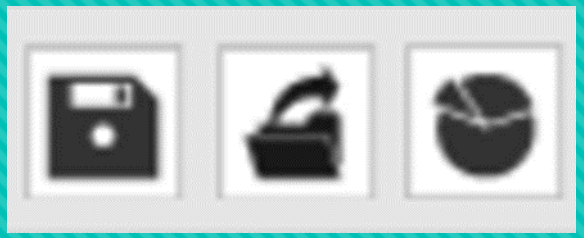
發佈編號	ASOC-INT-201603-0621	發佈時間	2016-0 3 09:16:20
事件類型	對外攻擊	發現時間	2016-03-03 08:54:11
事件主旨	通報:[中興區網中心]163.28.82.5 utm: DNS		
事件描述	ASOC 發現貴單位(中興區網中心)所屬 163.28.82.5 疑似對外進行 utm: DNS 攻擊		

基礎畫面介紹-事件



Step 1: 查詢條件
Step 2: IP過濾
Step 3: 啟動查詢

基礎畫面介紹-事件-查詢事件



事件 ▶ 事件查詢　□ 頁面自動更新

查詢條件 | 進階條件 | Show All | 重新輸入

查詢時間區段　○ 選擇時間區段 5分鐘內　○ 過去　◉ 起迄時間 2016/3/3 00:00 ~ 2016/3/3 05:37

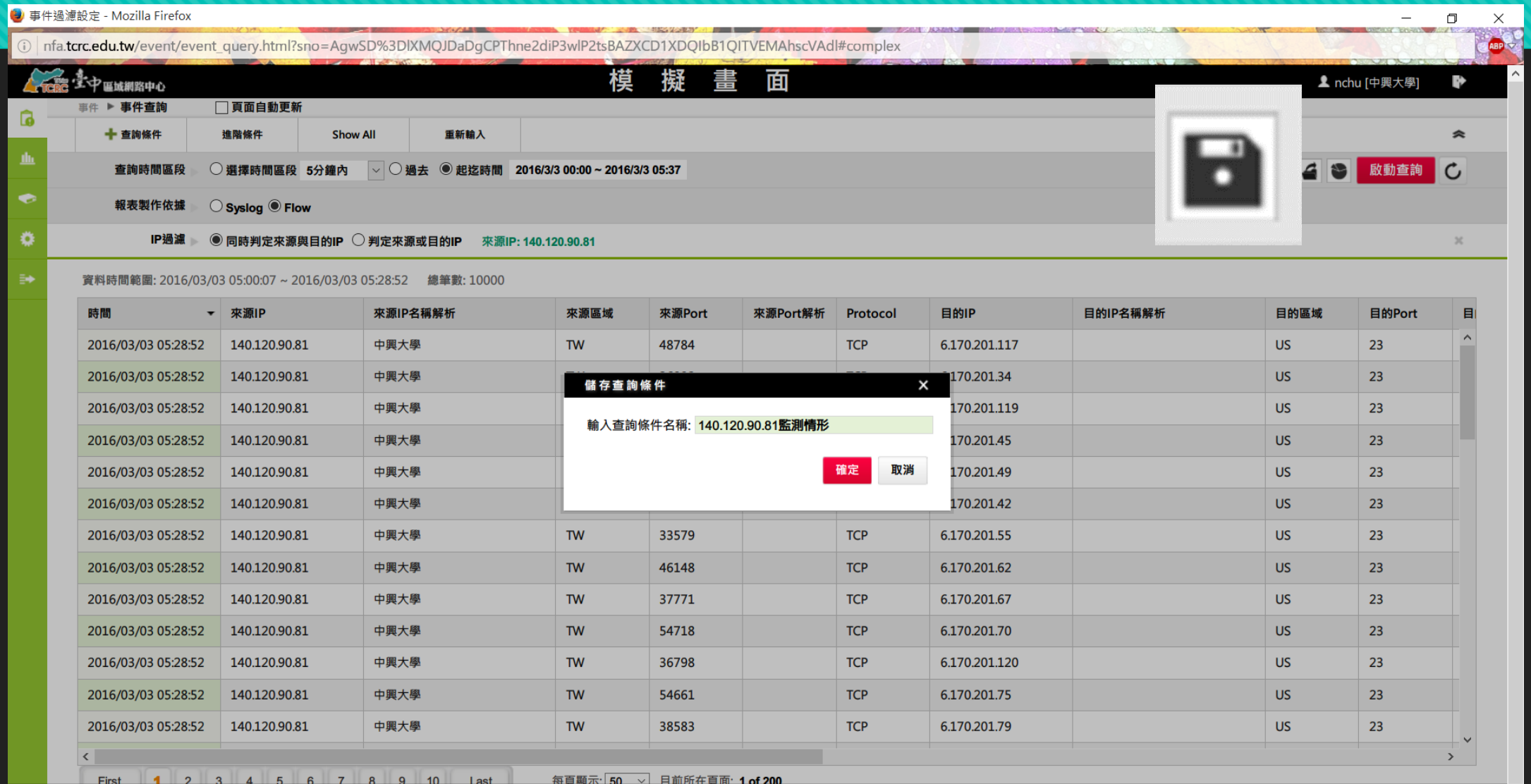
報表製作依據　○ Syslog ◉ Flow

IP過濾　◉ 同時判定來源與目的IP　○ 判定來源或目的IP　來源IP: 140.120.90.81

資料時間範圍: 2016/03/03 05:00:07 ~ 2016/03/03 05:28:52　總筆數: 10000

時間	來源IP	來源IP名稱解析	來源區域	來源Port	來源Port解析	Protocol	目的IP	目的IP名稱解析	目的區域	目的Port	目
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	48784		TCP	6.170.201.117		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	36992		TCP	6.170.201.34		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	45100		TCP	6.170.201.119		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	41744		TCP	6.170.201.45		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	53293		TCP	6.170.201.49		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	59966		TCP	6.170.201.42		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	33579		TCP	6.170.201.55		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	46148		TCP	6.170.201.62		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	37771		TCP	6.170.201.67		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	54718		TCP	6.170.201.70		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	36798		TCP	6.170.201.120		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	54661		TCP	6.170.201.75		US	23	
2016/03/03 05:28:52	140.120.90.81	中興大學	TW	38583		TCP	6.170.201.79		US	23	

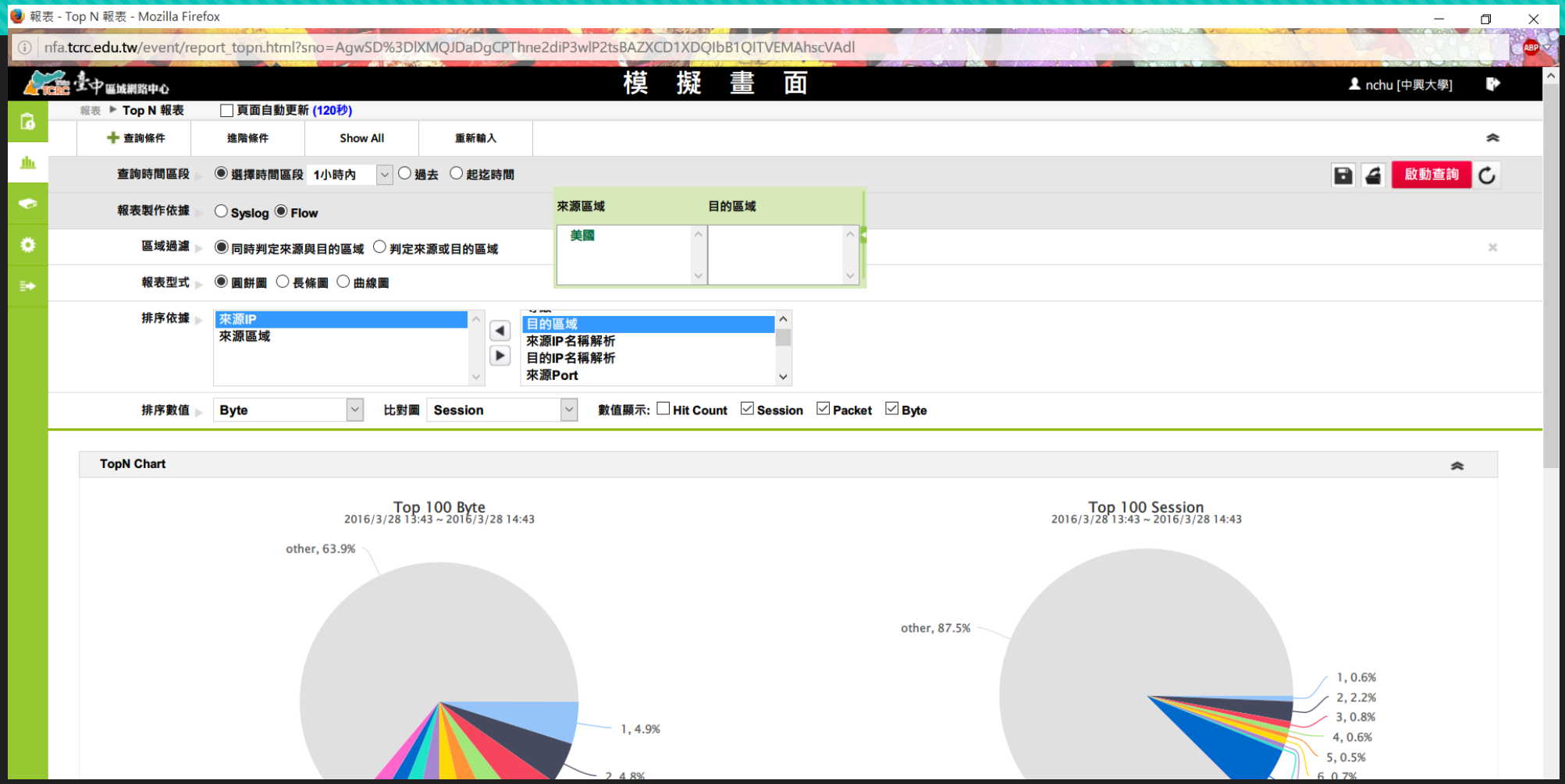
基礎畫面介紹-事件-儲存事件結果



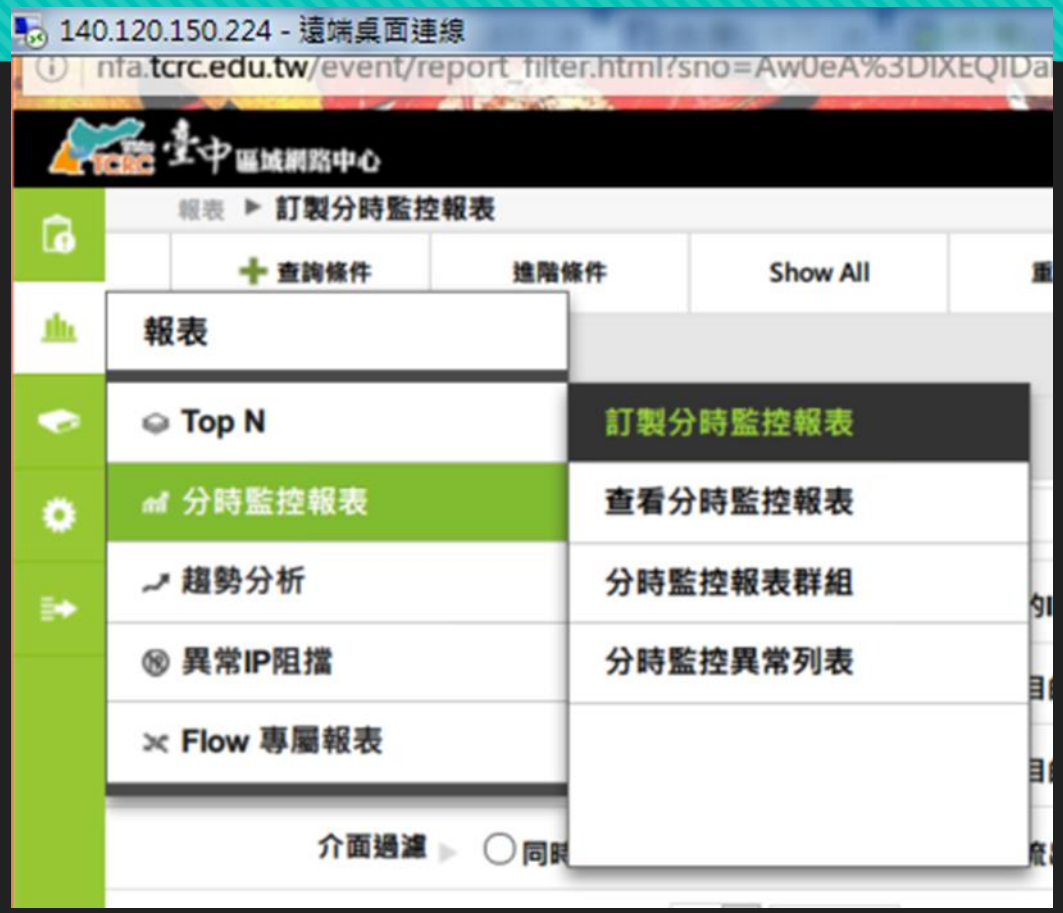
基礎畫面介紹-報表

基礎畫面介紹-報表-TOP N

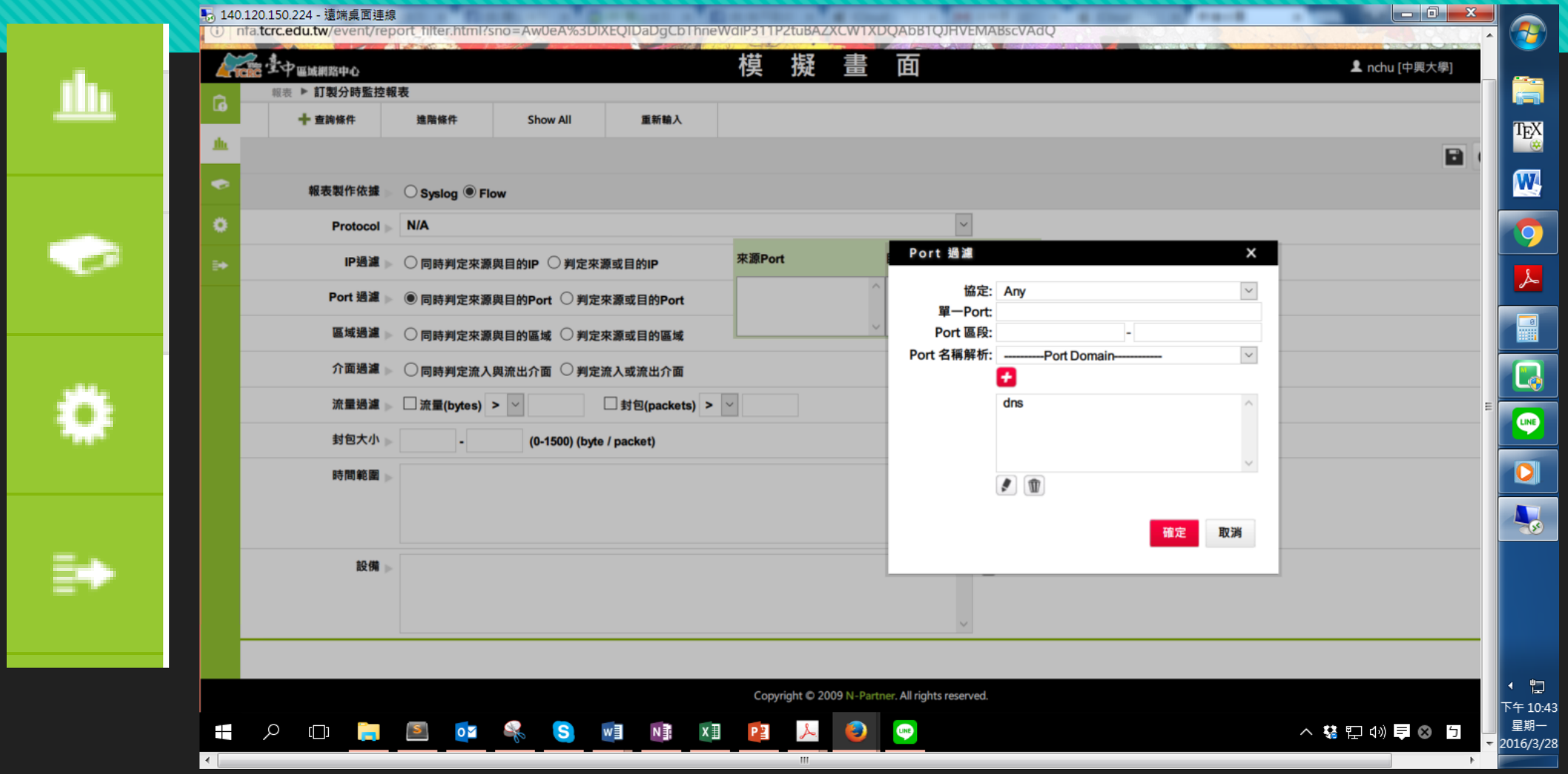
基礎畫面介紹-報表-TOP N-查詢美國到校流量



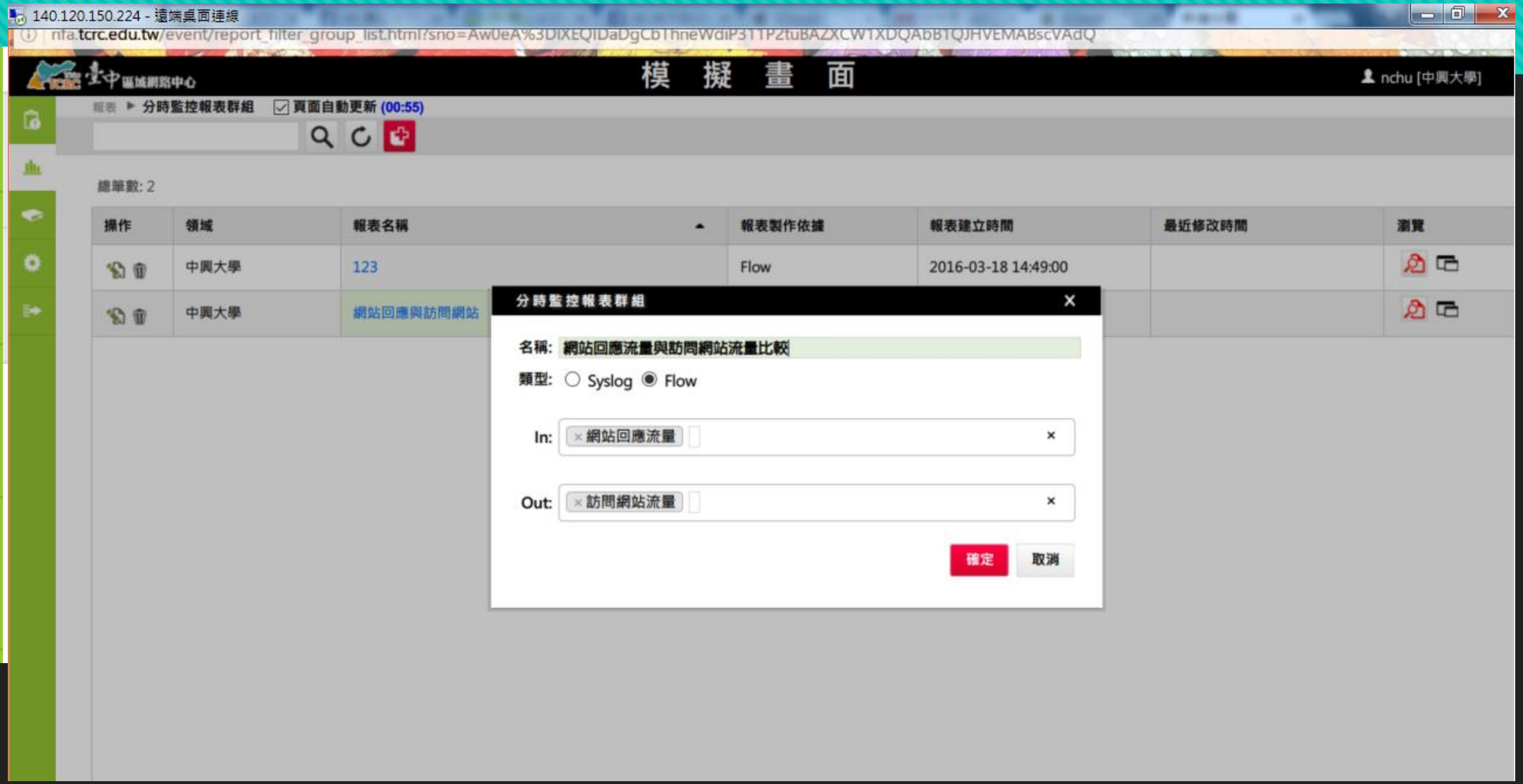
基礎畫面介紹-報表-分時監控報表



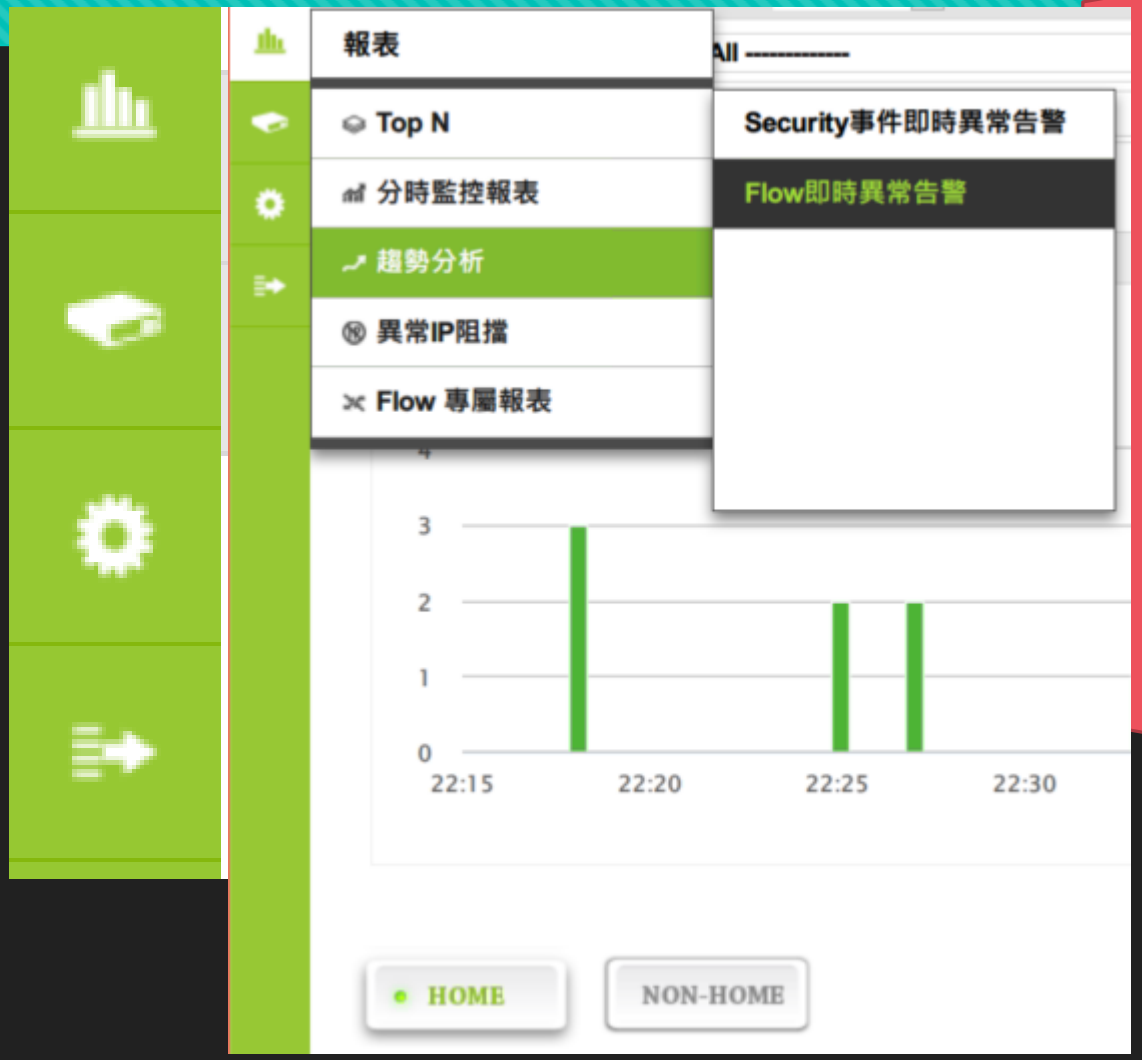
基礎畫面介紹-報表-分時監控報表-訂製分時監控報表-DNS監控

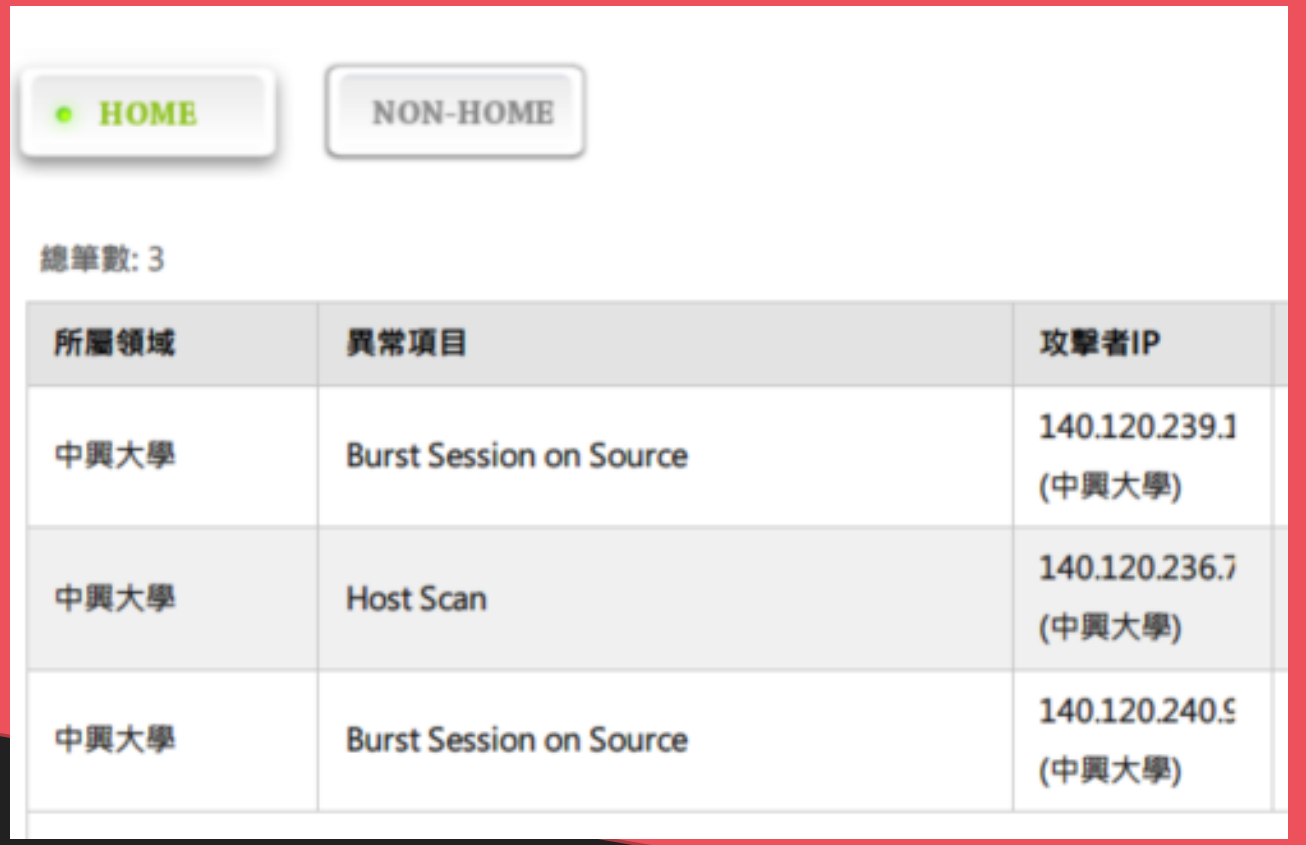


基礎畫面介紹-報表-分時監控報表群組

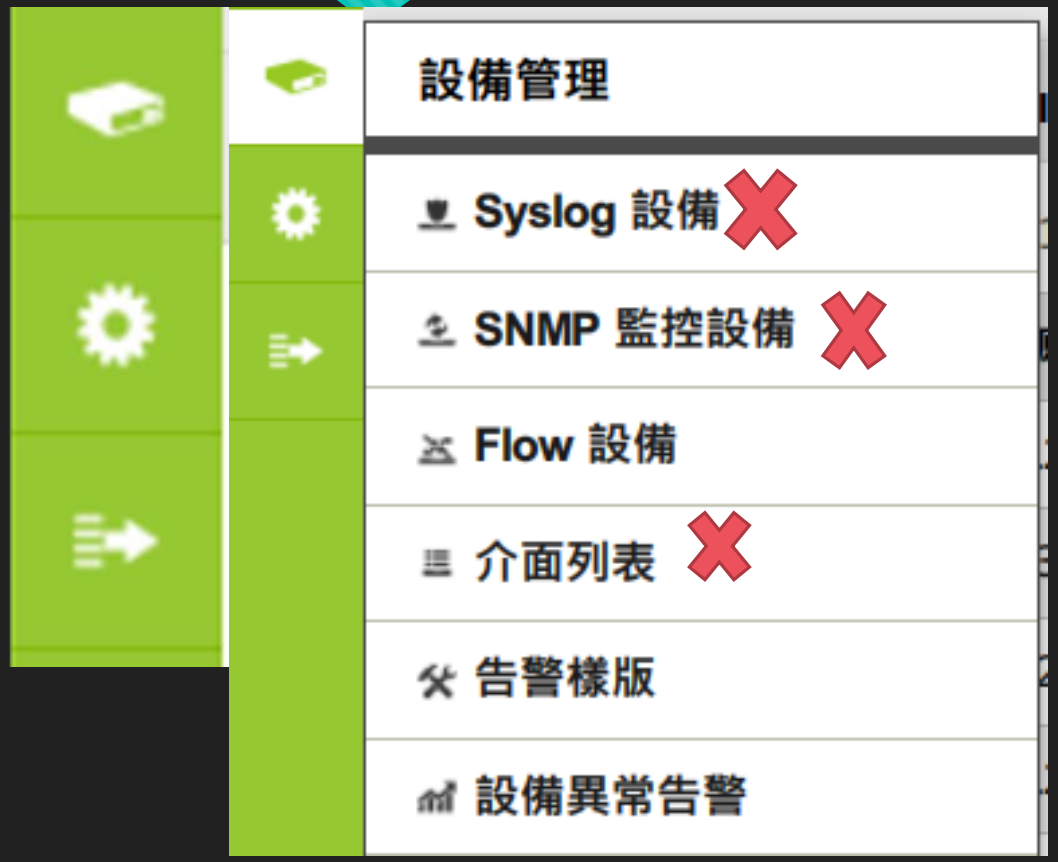


基礎畫面介紹-報表-趨勢分析





基礎畫面介紹-設備管理



基礎畫面介紹-系統管理


系統管理
系統管理
使用者管理
IP名稱解析
Port 名稱解析
告警通報設定
操作歷程
偏好設定
Dashboard