Next Generation UTM

管理者手冊

V 9.0.2.1

www.ShareTech.com.tw

目　　錄

第 1 章 安裝與訊息

1-1、硬體資訊

1-1-1、NU-840&840H

硬體外部介面說明(圖 1-1)：

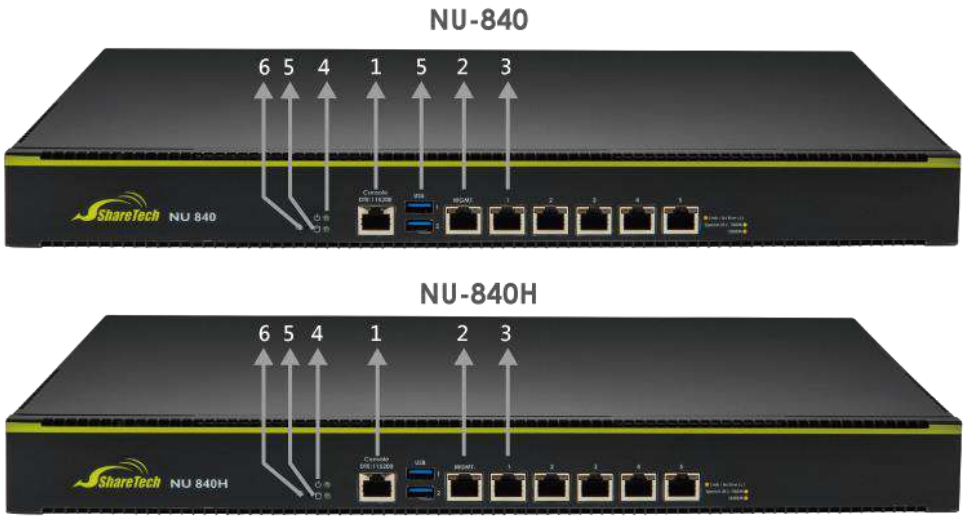


圖 1-1 NU-840&840H 正面圖示

1. Console Port：DTE 115200，主要的用途是查看系統內部網路介面設定和重置管理員密碼。

2. MGMT. Port：NU 網路管理介面，預設 IP 為 https://192.168.1.1。

3. Port 1-5：

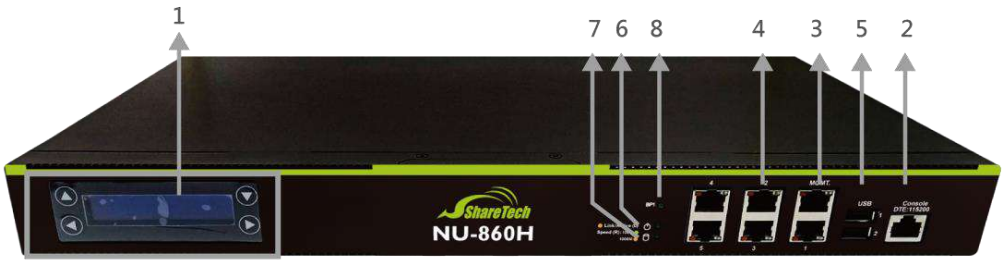
- 可自訂為內部網路介面：與內部交換器連接
- 可自訂為外部網路介面：與外部路由器連接
- 燈號：
  - 左邊：當橘燈亮起時表示該 RJ45 網路孔運作中，當橘燈閃爍時表示該 RJ45 網路孔正在傳送或接收資料。
  - 右邊：不同燈號表示不同傳輸速度，低於 10Mbps 不亮燈、達 100Mbps 時亮綠燈、達 1000Mbps 時亮橘燈。

4. Power LED 電源燈號：當亮燈時表示系統處於開機狀態。

5. HDD LED 硬碟燈號：當 LED 閃爍綠燈時，表示系統正在讀取或存入資料到內建之硬碟。

6. 重開機按鍵：利用小型的針狀物長按 5 秒按鈕後，設備會重開機。

1-1-2、NU-860H



1. LCM 顯示板：主要顯示包含

- Status (IP/Mask/Model/CPU)
- Service (DHCP/DDNS /DNS/ClamAV/SPAM/IPSecVPN)
- Maintain (Start SSH/Reset Password/Reset IP/Reboot/Power Off)

2. Console Port：DTE 115200，主要的用途是查看系統內部網路介面設定和重置管理員密碼。

3. MGMT. Port：NU 網路管理介面，預設 IP 為 https://192.168.1.1。

4. Port 1-5：

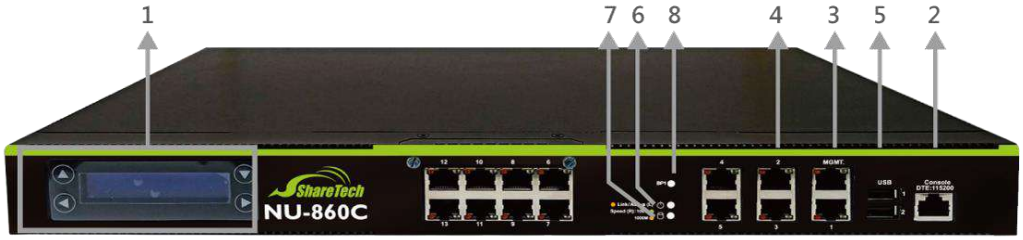
- 可自訂為內部網路介面：與內部交換器連接
- 可自訂為外部網路介面：與外部路由器連接
- 燈號：
  - 左邊：當橘燈亮起時表示該 RJ45 網路孔運作中，當橘燈閃爍時表示該 RJ45 網路孔正在傳送或接收資料。
  - 右邊：不同燈號表示不同傳輸速度，低於 10Mbps 不亮燈、達 100Mbps 時亮綠燈、達 1000Mbps 時亮橘燈。

5. Power LED 電源燈號：當亮燈時表示系統處於開機狀態。

6. HDD LED 硬碟燈號：當 LED 閃爍綠燈時，表示系統正在讀取或存入資料到內建之硬碟。

7. BP1 Bypass 燈號：當 LAN Bypass 功能啟動時，會恆亮綠燈。

1-1-3、NU-860C



1. LCM 顯示板：主要顯示包含

- Status (IP/Mask/Model/CPU)
- Service (DHCP/DDNS /DNS/ClamAV/SPAM/IPSecVPN)
- Maintain (Start SSH/Reset Password/Reset IP/Reboot/Power Off)

2. Console Port：DTE 115200，主要的用途是查看系統內部網路介面設定和重置管理員密碼。

3. MGMT. Port：NU 網路管理介面，預設 IP 為 https://192.168.1.1。

4. Port 1-13：

- 可自訂為內部網路介面：與內部交換器連接
- 可自訂為外部網路介面：與外部路由器連接
- 燈號：
  - 左邊：當橘燈亮起時表示該 RJ45 網路孔運作中，當橘燈閃爍時表示該 RJ45 網路孔正在傳送或接收資料。
  - 右邊：不同燈號表示不同傳輸速度，低於 10Mbps 不亮燈、達 100Mbps 時亮綠燈、達 1000Mbps 時亮橘燈。

5. Power LED 電源燈號：當亮燈時表示系統處於開機狀態。

6. HDD LED 硬碟燈號：當 LED 閃爍綠燈時，表示系統正在讀取或存入資料到內建之硬碟。

7. BP1 Bypass 燈號：當 LAN Bypass 功能啟動時，會恆亮綠燈。

1-1-4、NU-860T

1. LCM 顯示板：主要顯示包含

- Status (IP/Mask/Model/CPU)
- Service (DHCP/DDNS /DNS/ClamAV/SPAM/IPSecVPN)
- Maintain (Start SSH/Reset Password/Reset IP/Reboot/Power Off)

2. Console Port：DTE 115200，主要的用途是查看系統內部網路介面設定和重置管理員密碼。

3. MGMT. Port：NU 網路管理介面，預設 IP 為 https://192.168.1.1。

4. Port 1-5：

- 可自訂為內部網路介面：與內部交換器連接
- 可自訂為外部網路介面：與外部路由器連接
- 燈號：
  - 左邊：當橘燈亮起時表示該 RJ45 網路孔運作中，當橘燈閃爍時表示該 RJ45 網路孔正在傳送或接收資料。
  - 右邊：不同燈號表示不同傳輸速度，低於 10Mbps 不亮燈、達 100Mbps 時亮綠燈、達 1000Mbps 時亮橘燈。

5. SFP+(10G 光纖)網路孔

- 燈號：
  - 左邊：當燈號亮起時表示該網路孔有連接光纖模組。
  - 右邊：當燈號閃爍時表示該網路孔正經由光纖模組在傳送或接收資料。

6. Power LED 電源燈號：當亮燈時表示系統處於開機狀態。

7. HDD LED 硬碟燈號：當 LED 閃爍綠燈時，表示系統正在讀取或存入資料到內建之硬

碟。

8. BP1 Bypass 燈號：當 LAN Bypass 功能啟動時，會恆亮綠燈。

1-1-5、NU-8700C

1. LCM 顯示板：主要顯示包含

- Status (IP/Mask/Model/CPU)
- Service (DHCP/DDNS /DNS/ClamAV/SPAM/IPSecVPN)
- Maintain (Start SSH/Reset Password/Reset IP/Reboot/Power Off)

2. Console Port：DTE 115200，主要的用途是查看系統內部網路介面設定和重置管理員密碼。

3. MGMT. Port：NU 網路管理介面，預設 IP 為 https://192.168.1.1。

4. Port 1-13：

- 可自訂為內部網路介面：與內部交換器連接
- 可自訂為外部網路介面：與外部路由器連接
- 燈號：
  - 左邊：當橘燈亮起時表示該 RJ45 網路孔運作中，當橘燈閃爍時表示該 RJ45 網路孔正在傳送或接收資料。
  - 右邊：不同燈號表示不同傳輸速度，低於 10Mbps 不亮燈、達 100Mbps 時亮綠燈、達 1000Mbps 時亮橘燈。

5. Power LED 電源燈號：當亮燈時表示系統處於開機狀態。

6. HDD LED 硬碟燈號：當 LED 閃爍綠燈時，表示系統正在讀取或存入資料到內建之硬碟。

7. BP1/BP2 Bypass 燈號：當 LAN Bypass 功能啟動時，會恆亮綠燈。

1-1-6、NU-8700F

1. LCM 顯示板：主要顯示包含
   - Status (IP/Mask/Model/CPU)
   - Service (DHCP/DDNS /DNS/ClamAV/SPAM/IPSecVPN)
   - Maintain (Start SSH/Reset Password/Reset IP/Reboot/Power Off)
2. Console Port：DTE 115200，主要的用途是查看系統內部網路介面設定和重置管理員密碼。
3. MGMT. Port：NU 網路管理介面，預設 IP 為 https://192.168.1.1。
4. Port 1-5：
   - 可自訂為內部網路介面：與內部交換器連接
   - 可自訂為外部網路介面：與外部路由器連接
   - 燈號：
     - 左邊：當橘燈亮起時表示該 RJ45 網路孔運作中，當橘燈閃爍時表示該 RJ45 網路孔正在傳送或接收資料。
     - 右邊：不同燈號表示不同傳輸速度，低於 10Mbps 不亮燈、達 100Mbps 時亮綠燈、達 1000Mbps 時亮橘燈。
5. Port 6-13：
   - SFP(1G 光纖)網路孔
   - 燈號：
     - 左邊：當黃燈亮起時表示該網路孔有連接光纖模組。

■ 右邊：當橘燈亮起時表示該網路孔正經由光纖模組在傳送或接收資料。

6. Power LED 電源燈號：當亮燈時表示系統處於開機狀態。

7. HDD LED 硬碟燈號：當 LED 閃爍綠燈時，表示系統正在讀取或存入資料到內建之硬碟。

8. BP1/BP2 Bypass 燈號：當 LAN Bypass 功能啟動時，會恆亮綠燈。

1-1-7、NU-8700T

1. LCM 顯示板：主要顯示包含

- Status (IP/Mask/Model/CPU)
- Service (DHCP/DDNS /DNS/ClamAV/SPAM/IPSecVPN)
- Maintain (Start SSH/Reset Password/Reset IP/Reboot/Power Off)

2. Console Port：DTE 115200，主要的用途是查看系統內部網路介面設定和重置管理員密碼。

3. MGMT. Port：NU 網路管理介面，預設 IP 為 https://192.168.1.1。

4. Port 1-5：

- 可自訂為內部網路介面：與內部交換器連接
- 可自訂為外部網路介面：與外部路由器連接
- 燈號：

■ 左邊：當橘燈亮起時表示該 RJ45 網路孔運作中，當橘燈閃爍時表示該 RJ45 網路孔正在傳送或接收資料。

■ 右邊：不同燈號表示不同傳輸速度，低於 10Mbps 不亮燈、達 100Mbps 時亮綠燈、達 1000Mbps 時亮橘燈。

5. Port 6-9：

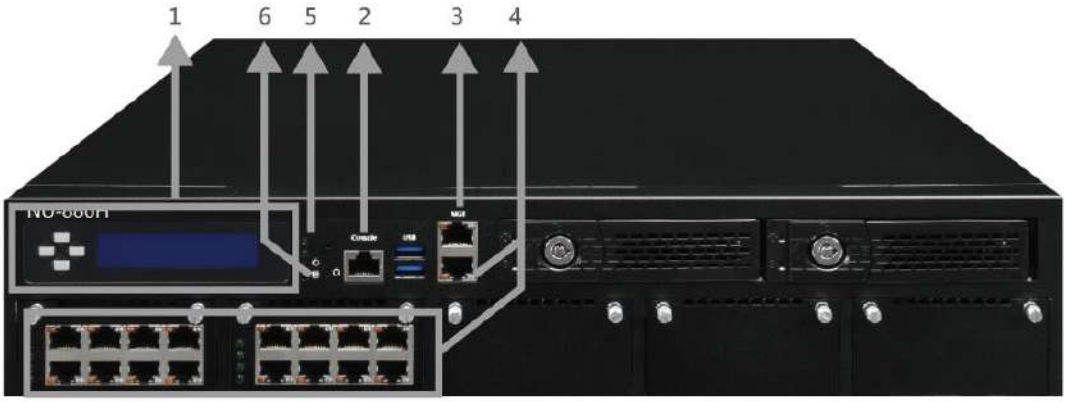
- SFP+(10G 光纖)網路孔
- 燈號：
  - 左邊：當橘燈亮起時表示該網路孔有連接光纖模組。
  - 右邊：當藍燈亮起時表示該網路孔正經由光纖模組在傳送或接收資料。

6. Power LED 電源燈號：當亮燈時表示系統處於開機狀態。

7. HDD LED 硬碟燈號：當 LED 閃爍綠燈時，表示系統正在讀取或存入資料到內建之硬碟。

8. BP1/BP2 Bypass 燈號：當 LAN Bypass 功能啟動時，會恆亮綠燈。

1-1-8、NU-880H



1. LCM 顯示板：主要顯示包含

- Status (IP/Mask/Model/CPU)
- Service (DHCP/DDNS /DNS/ClamAV/SPAM/IPSecVPN/WAF)
- Maintain (Start SSH/Reset Password/Reset IP/Reboot/Power Off)

2. Console Port：DTE 115200，主要的用途是查看系統內部網路介面設定和重置管理員密碼。

3. MGMT. Port：NU 網路管理介面，預設 IP 為 https://192.168.1.1。

4. Port 1-17：

- 可自訂為內部網路介面：與內部交換器連接
- 可自訂為外部網路介面：與外部路由器連接
- 燈號：

- 左邊：當橘燈亮起時表示該 RJ45 網路孔運作中，當橘燈閃爍時表示該 RJ45 網路孔正在傳送或接收資料。
- 右邊：不同燈號表示不同傳輸速度，低於 10Mbps 不亮燈、達 100Mbps 時亮綠燈、達 1000Mbps 時亮橘燈。

5. Power LED 電源燈號：當亮燈時表示系統處於開機狀態。

6. HDD LED 硬碟燈號：當 LED 閃爍綠燈時，表示系統正在讀取或存入資料到內建之硬碟。

1-2、第一次安裝

NG-UTM 出廠時有預設的 IP 位址及帳號密碼，管理者需要將自己的電腦 IP 位址配置跟 NG-UTM 同一個網段，並利用預設的帳號跟密碼進入設備中，進入之後再根據使用環境配置新的 IP 位址。

當管理者第一次進入設備後，建議改變預設帳號的密碼，也可以在設定完成後把預設帳號 admin 的權限縮小，管理者的權限設定在 【系統設定】 > 【管理員】介面中。

第一次安裝時的網路設定

首先將管理者的電腦和 NG-UTM 標示為 MGMT 的網路介面接到同一個 Hub 或 Switch，再使用瀏覽器 (IE、 Firefox 或 Chrome) 進入 NG-UTM 的管理介面。

NG-UTM 的 IP 地址預設值為 https://192.168.1.1，所以管理者電腦的 IP 位址必須是 192.168.1.2 至 192.168.1.254 其中之一，子網路遮罩為 255.255.255.0。

步驟**1.** 瀏覽器會詢問使用者名稱及密碼，輸入管理者名稱與密碼。

- 使用者名稱：admin
- 密碼：admin
- 可以選擇【記住登入帳號】，同一個電腦及瀏覽器下次登入時就不需要再輸入帳號跟密碼。
- 點選【確定】就可以進入管理介面。

步驟**2.** NG-UTM 會自動偵測管理者的瀏覽器語系，並自動切換語系，例如，管理者的瀏覽器使用是繁體中文，登入時就會自動切換成繁體中文，管理介面支援繁體、簡體中文跟英文語系，所以非繁體、簡體中文的瀏覽器，管理介面就會自動切換成英文語系。

步驟**3.** 登入後，如果想切換管理介面的語系，也可以在管理介面的右上角，直接選擇需要的語系，在這裡除了切換語系外，直接連到首頁、登出、管理者登入的 IP 位址跟目前有多少管理者登入，通通會在這裡顯示。如 (圖 1-2)

圖 1-2 即時更改管理介面語系

1-3、管理跟 Dashboard 模式

NG-UTM 提供 2 種操作介面，一個是管理者使用的管理介面，另一個是適合監看網路活動的 Dashboard 模式，舉凡設定、管理及記錄等動作都在管理介面中處理，Dashboard 模式除了線上即時監控外，也可以製作報表。

管理者可以在【系統設定】> 【基本設定】中的【首頁設定】選擇適當的模式，下次登入時，就會直接進入設定的模式。

1、管理介面

管理介面分成 5 大塊，分別是 Logo 區、標題區、IP 位址切換(IPV4/V6)、主選單區及設定區，除了主選單區跟設定區會因為不同管理者權限而看到不同的設定選項外，其他區域每一個管理者看到的都一樣。外，同時提供一些簡易的快速連接按鈕，直接連到首頁、登出，同時顯示管理者登入的 IP 位址跟目前有多少管理者登入設備中。（圖 1-3）

圖 1-3 選單模式

- 【Logo 區】：管理者變更這裡的圖示，讓設備除了方便辨識外，更容易凸顯企業的整體形象，圖片的格式為 150 * 90 pixel 。

  上傳圖片的地方在 【系統設定】 > 【基本設定】 > 【一般設定】 設定項目中 【更新 Logo】，圖片格式 gif 、 png、jpeg 等常見的圖片格式都可以。

- 【標題區】：區域內有 3 個區塊，分別是首頁標題、Port Information 跟管理者資訊，在首頁標題區，輸入任何標題文字，方便辨識此台設備的資訊，Port Information 顯示所有硬體 Port 的狀態，管理者資訊顯示已登入的管理者資料。

首頁標題設定的地方是在【系統設定】 > 【基本設定】 頁面中的 【一般設定】設定項目中 【首頁標題]。

■ 【IP 位址切換】：NG-UTM 是支援 IPV4/IPV6 的多功能 UTM 設備，因為 IPV4 跟 IPV6 在網路安全或是管理上稍微有點不一樣，例如，拒絕 IPV4 的 WEB 使用並不代表拒絕 IPV6 的 WEB，所以 2 個 IP 定址模式是分開管理，管理者可以在這裡切換位址，切換後所有管理介面的位址都會一併切換。

■ 【主選單】：管理介面的主選單分成 2 層，主項目、次選單，選擇次選單後在設定區會出現分頁選單，所以，最基本的設定項目是放在分頁選單中，相似功能設定的項目彙整成次選單，相同功能的次選單則彙整成一個主項目。（圖 1-4）

圖 1-4 選單層次

圖例說明：

1 : 主項目、2 : 次選單、3 : 分頁選單

一般來說，套用到整個 NG-UTM 且屬於系統管理層級的就會被分類到 【系統設定】的主項目上，再根據要設定的項目選擇對應的次選單，屬於 NG-UTM 基本的設定就安排放在【基本設定】 的次選單上，基本設定上再細分成分頁選單。

■ 【設定區】：系統所有詳細功能設定及紀錄都在此區中完成，管理者藉由主項目跟次選單的切換，更換設定項目後就進行設定。

2、Dashboard 介面

提供各種統計資訊及彙整威脅情報，讓管理者藉由圖形介面快速了解設備的狀態或是找出異常的使用者，並製作報表匯出，目前提供的統計及報表項目如下：

- 1. 威脅情報
- 2. 流量分析
- 3. 連線狀態
- 4. 防火牆防護
- 5. IPS
- 6. Web 服務
- 7. Web Control
- 8. 郵件服務
- 9. 應用程式管制
- 10. IP 地區
- 11.DNS 查詢

1-4、管理介面的首頁訊息

登入 NG-UTM 的畫面後，系統會提供豐富的訊息，讓管理者清楚目前設備的運作狀況。

1、伺服器系統資源

顯示目前設備的時間及時區，甚至是開機時間，同時也顯示設備目前的 CPU、RAM、Flash、HDD 等重要設備資源使用量，管理者能夠藉此判斷，設備是否超過負載，底下是系統資訊的說明：（圖 1-5）

伺服器系統資源	
CPU 使用率	91.5%
記憶體 使用量	82%
Flash 使用量	24%
硬碟 使用量	9%
目前連線數	3024
最大連線數	6760 (發生在: 2016-05-10 17:43:09)
每秒新連線數	66

伺服器資訊		
伺服器日期 / 時間	2016-05-17	14:50:39
現在時區	Asia/Taipei	
伺服器開機時間	14 days,0 hours,8 minutes	
伺服器型號	SDN Router	
伺服器軟體版本	9.0.0	
機器序號		

圖 1-5 系統資源

- 【目前連線數】：目前 NG-UTM 正處理的總連線數量 (Concurrent Sessions)。
- 【最大連線數】：設備曾經處理過的最大連線數量 (Maximum Sessions)，NG-UTM 同時也會標註發生的時間。

  管理者藉由最大連線數發生時間，推測系統最大負載的時間，萬一被攻擊時也可以推測被攻擊的時間。

  上述 2 個連線數都是即時資料，管理者要查詢歷史的連線數資訊，在【系統狀態】 > 【系統狀態】 > 【歷史狀態】 中有總連線數的選項可以勾選，在選定時間範圍後，NG-UTM 就會呈現歷史資料。
- 【每秒新連線數】：每秒鐘新建的連線數(New Session)。
- 【伺服器型號/軟體版本】： NG-UTM 的型號及韌體版本，韌體版本會不定期的發佈。

  管理者可以選擇手動或是自動升級，手動升級需要到 ShareTech 官網中下載韌體版本，並上傳到設備中，自動升級分成全自動跟半自動，全自動是系統會自動檢查，有新韌體發佈就會自動下載，並在管理者指定的時間下升級韌體，半自動則只會將韌體下載到設備中，升級動作需要管理者自己執行。

  詳細的設定在 【系統設定】 > 【系統升級】中。

- 【伺服器開機時間】：上次重新開機後到目前的時間，不論是管理者重新啟動或是斷電重啟，時間都會重新計算。

2、Port Information

在管理介面的標題區，有一個隱藏的資訊，Port Information ，即時顯示目前設備的所有 Port 的連線狀態，預設是收合狀態，管理者只要點選 Port information 的字樣後，NG-UTM 就會自動展開，點選任何 Port 之後會自動連結設定頁面，進階的設定在 【系統設定】 > 【網路設定】。（圖 1-6）

圖 1-6 Port Information

淺綠色代表使用中且跟其他設備連接成功，設備同時顯示連線的速度，紅色代表沒有使用，點選任何 port 後，系統會自動帶出網路設定頁面。

這裡顯示的 port 號碼跟實際機器上的 port 號碼是一致，但實際位置可能不一樣，所以管理者在配置網路區域時，必須以 **port 號碼** 為根據。在 NG-UTM 的軟體版本中，顯示的 port 數量可能會多於實際數量，設定時更需要以 port 號碼為根據。

在 【系統設定】 >【[網路設定] 中，同一個區域的網路介面會用相同色塊標示，管理者可以很快的辨識哪幾個 port 是綁定或是獨立運作。

3、管理者資訊

在管理介面標題區的最右邊是管理者資訊區域，包含切換語系、管理者自己的資訊或是查看有多少管理者同時登入設備都在這裡。

- 【切換語系】：系統會自動偵測管理者使用的瀏覽器語言，並顯示相同的語系運作，管理者可以強制切換語系。

  系統目前支援繁體中文、簡體中文跟英文語系，當瀏覽器使用的不是這 3 種語系，系統會自動切換成英文。

- 【管理者跟登入的 IP 位址】：顯示管理者登入的來源 IP 位址跟使用帳號。

  新增管理者的帳號在【系統設定】>【管理員】>【帳號管理】

- 【目前線上人數】：同時有多少人進入系統，點選數字後，會開啟新的頁面，包含每個管理者登入時間、來源 IP 位址操作內容，操作內容包含他被授予的權限所做的動作。

  這裡只能查看當下已登入的管理者所做的事情，例如，此時有 2 位管理者登入，可以查看對方目前正在做哪一些設定，當某一位管理者登出之後，這裡就不再顯示。

  查看歷史的管理者操作資訊在【日誌】>【操作日誌】。

- 【首頁 / 登出】: 提供快速的連結回到首頁或是選擇登出系統。

4、網路介面

在【網路設定】>【區域設定】中所有的區域，他的網路介面訊息跟即時流量都在這裡，管理者可以切換監看全部、已連線跟自訂的區域，自訂的選擇在【系統設定】>【基本設定】>【一般設定】>【首頁網路介面預設顯示】中勾選，即時流量會把過去 60 秒的上、下載流量動態呈現。

：代表斷線，：代表連線，系統預設會顯示所有介面的即時流量，根據需求，選擇觀看的介面。（圖 1-7）

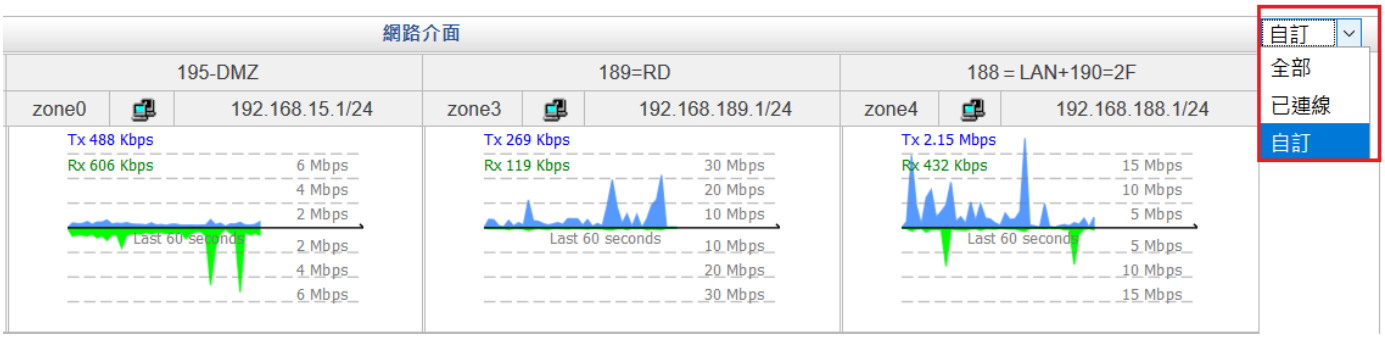


圖 1-7 網路介面即時流量

在上、下載標示上，藍色代表上傳，綠色代表下載，上、下載是以設備為出發的觀點，出網路介面的流量標示在上傳區，進入網路介面的標示在下載區。

連接網際網路的介面，例如，PPPOE，看到的上、下載流量方向是正常，反之，內部介面標示方向則是相反，標示的上傳流量就是一般認知的下載流量。

首頁上顯示的都是即時的流量資訊，就算是流量圖也只有 60 秒，管理者要查詢更長時間的流量資料，在【系統狀態】中有更多的選擇，說明如下：

A、 3 分鐘流量圖：在網路管理中，有時需要觀察某幾個介面的即時流量一段時間，藉以判斷網路是否正常運作，【系統狀態】>【系統狀態】>【介面即時流量】就能提供這樣的訊息。

B、 歷史流量圖：存在設備儲存設備的資料，能提供更長時間的紀錄資訊，【系統狀態】>【系統狀態】>【歷史狀態】中，選擇要查詢的網路介面跟時間範圍，系統就會呈現歷史的流量圖。

第 2 章 系統設定

系統設定是整台機器的基本配置，包含分配次管理者的權限、系統升級、備份還原及通知重要項目，基本上是整台設備運作的靈魂，並不是每一個進入設備的管理者都具有相同權限，只有主要管理者才有權限設定，次管理者並沒有權限設定這裡。

NG-UTM 提供多層次的管理權限，管理者權限的設定在 【系統設定】 > 【管理員】 > 【帳號管理】。 。

2-1、基本設定

2-1-1、一般設定

1、一般設定

NG-UTM 基本運作，例如，瀏覽器標題、記憶體及連線 timeout 等，管理者可以根據自己的喜好，設定瀏覽器要顯示的標題、Logo、甚至登入 NG-UTM 後，在首頁要顯示的文字，都在【一般設定】中設定。（圖 2-1）

圖 2-1 管理介面顯示設定

- 【首頁標題】：在管理介面的標題區顯示的文字，目的是讓管理者容易辨識目前使用的設備資訊，例如，台中辦公室--191 等。

  當管理者同時管理多台設備時，顯示文字就相當重要，它幫助管理者將正確配置設定到要執行的設備上，避免出錯。

- 【瀏覽器標題】：出現在管理者登入瀏覽器標題上的文字，目的讓管理者在開啟多個網頁下，快速地找出管理的設備。

- 【更新 Logo】：把原本的 ShareTech Logo 換成自己要的圖形，這個區域圖片大小有限制，最大只有 150 x 90 pixel， 最佳顯示為 150 x 90 pixel 的 GIF 圖片，管理者也可以上傳通用的 PNG、JPEG 等圖片。

- 【清除記憶體】：為了避免因為記憶體被無用的程序佔滿，導致系統運作不正常，NG-UTM 內建自動清理記憶體機制，系統預設動作是每 30 分鐘檢查系統的記憶體使用量，當記憶體超過 90% 使用量時，就會觸發清除機制，把沒有在使用的記憶體釋放，確保系統有充裕的記憶體可以使用，管理者根據使用狀態調整檢查時間跟觸發的上限值。

  另一方面，也可以指定時間讓系統定期執行檢查及清理，而不是等到記憶體滿到觸發條件之後才執行清理的動作，提高系統的穩定度，設定清理的時間通常是系統比較不忙碌的時間，例如，凌晨 0:00。

  定期清理記憶體預設是關閉，需要這樣的功能時將它啟動。

- 【Session timeout of established】：每個已經建立的 TCP 連線，多長時間內沒有傳輸資料，系統就會主動將這個 TCP 連線中斷。一般來說，通聯的雙方會在傳輸資料結束後自動將此連線中斷，一旦發生不正常結束或是被惡意攻擊時，這些 TCP 連線就會被保留在系統中佔據記憶體資源，萬一被無效連線佔據太多記憶體後，會導致正常的連線要求無法被服務，此時就需要這個機制把這些異常連線中斷掉。

  預設值為 600 秒，如果設太長 86400 秒(1 天)，系統可能會被很多空的 TCP 連線佔據記憶體資源。

  Session timeout of established 這設定值只對**已建立的 TCP 連線**有效，未完整建立的 TCP 連線跟 UDP 協定無效，UDP 協定是因為沒有三方交握機制，未完整建立的 TCP 連線就有太多可能性，DDOS 攻擊中的 SYN 攻擊就是一種消耗資源的攻擊方式。

  NG-UTM 提供 SYN 攻擊的防護，在【管制條例】>【管制規則】>【SYN 防護】中可以設定需要 SYN 保護機制的主機

- 【Pass-through Protocol】：當 NU-UTM 運用在視訊會議或是有 SIP 網路電話時，建議啟用這項功能，啟用後，對 H.323/SIP 協定的封包自動 pass，不做額外的管制。

2、Auto VPN

NG-UTM 在 9.0.1.5 版後提供 Auto VPN，Auto VPN 在建立大量且都是動態 IP 位址的 IPSec VPN 時能降低設置 IPSec VPN 的複雜度、加快 VPN 建立的速度及提高整體運作的穩定度，這個功能詳細請參考 Auto VPN 章節，這裡設定 Auto VPN 使用的通訊埠，預設值是 24088， 當 port 設為 0 代表不啟用這個功能。

3、登入失敗封鎖設定

NG-UTM 會保護自己不被猜密碼機制破解，不論是主要管理者或是次管理者使用的密碼，保護的方法就是限制每一個來源 IP 位址能夠輸入帳號、密碼的次數，當輸入錯誤的次數超過設定值，NG-UTM 就會封鎖此來源 IP 位址，避免他繼續猜密碼，被封鎖的 IP 位址必須等到設定的封鎖時間後或是另一個有主要管理者權限的人登入並執行解除封鎖後，才能將此來源 IP 位址解除鎖定。

- 【登入失敗次數超過多少暫時封鎖】：設定登入時，密碼輸入錯誤次數的限制，當同一個帳號輸入密碼錯誤超過設定次數，此來源 IP 位址將被封鎖，預設值為 0 ，代表不限制錯誤次數。

- 【多久解除被暫時封鎖的 IP】：當 IP 位址嘗試輸入密碼的次數超過後，會被 NG-UTM 封鎖不能登入一段時間，單位為分鐘，超過這個時間後，此 IP 位址又可以再次嘗試登入。

  預設值為 0 ，代表不限制 ， 即永久不解除，此 IP 位址，將不可以再登入管理介面，除非具有主要管理權限的管理者到【解除 IP 封鎖】中將這個 IP 位址解除。

- 【解除 IP 封鎖】：被封鎖的 IP 位址將會列在這裡，由主要管理者決定要不要將他解除封鎖，如果不是被永久封鎖的 IP 位址，等到超過設定在【多久解除被暫時封鎖的 IP】的時間後，系統自動解除封鎖。

4、首頁設定

當管理者登入管理介面時，NG-UTM 提供 2 個選項，一個是傳統的管理介面，另一個是 Dashboard 介面，傳統的管理介面可以對整台機器進行管理動作，Dashboard 則會以圖形介面顯示整個 NG-UTM 進出網路的流量或是駭客攻防紀錄等。

- 【首頁設定】：共有 2 個選項，管理介面跟 Dashboard，當管理者登入時，會進入哪一個畫面，預設是管理介面。

5、首頁網路介面預設顯示

主要管理者登入 NG-UTM 的管理介面時，會顯示每個網路區域(ZONE)的即時流量，當網路區域數量眾多時，對管理者來說不容易辨識，可以選擇要觀察的網路區域，降低觀察的複雜度。

- 【首頁網路介面預設顯示】：共有 3 種模式可供選擇，全部、已連線跟自訂。

  全部：所有 ZONE 介面都會列出來，不論有無啟用或是流量。

  已連線：只顯示已經連線的介面，其他沒有啟用或是連線的介面都會被隱藏。

  自訂：由管理者挑選要顯示的 ZONE，不論它是否已經連線。（圖 2-3）

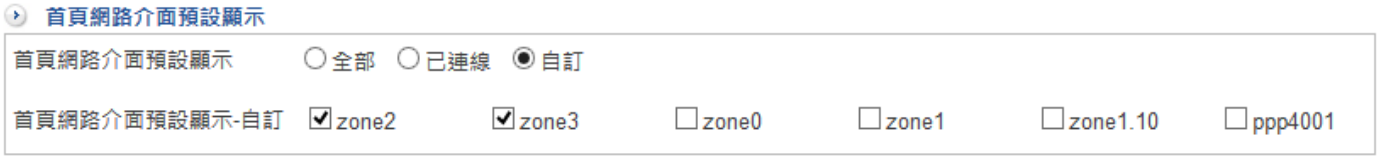


圖 2-3 選擇首頁顯示介面

預設會顯示所有的 ZONE 流量，這裡設定完成後，點選首頁，則只會出現設定的介面，在首頁也可即時選擇要觀察的 ZONE，包含全部、已連線跟自訂等選項，但下次登入時出現的預設顯示將是這裡選擇的介面。

6、Drop Session Log

管制條例中顯示封包通聯記錄的功能預設是顯示已建立的連線，通常已建立的連線代表符合管制條例的規則，但是對於違反條例的封包，系統會將它丟棄，不會有任何顯示，勾選這項功能後，系統就會將丟棄的封包紀錄。

2-1-2、DNS 解析

這裡設定 DNS 伺服器是提供給 NG-UTM 自己查詢使用，因為 NG-UTM 不一定是放在對外的閘道上，所以需要設定 DNS 伺服器查詢網域名稱，使用的 DNS 伺服器可以是 IPV4 或是 IPV6 。（圖 2-4）

- 【DNS Server 1】：NG-UTM 第一個使用的 DNS 伺服器，例如，168.95.192.1。
- 【DNS Server 2 】：NG-UTM 第二個使用的 DNS 伺服器，例如，168.95.192.1
- 【DNS Server 3 】：NG-UTM 第三個使用的 DNS 伺服器，例如，2001:b000::1

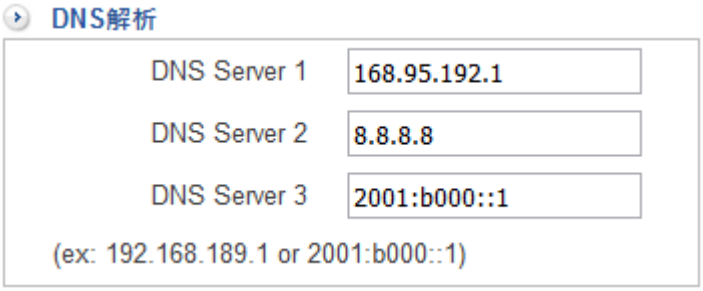


圖 2-4 DNS 伺服器

NG-UTM 需要查詢 DNS 紀錄時會先由 DNS Server 1 開始查詢，如果設定的 DNS 伺服器沒有回應，再繼續依序使用其他的 DNS 伺服器。

2-1-3、管理介面存取設定

1、管理介面存取設定

NG-UTM 使用瀏覽器設定，目前只允許使用 https 的協定進入管理介面，https 預設使用的 port 為 443，管理者依據自己的需求，可以把這個 port 改成 1 \~ 65535 中的任意號碼，當更改完成後，下次登入管理介面時就需要使用新的 port 進入。（圖 2-5）

- 【HTTPS Port】：進入 NG-UTM 管理介面使用 port 號，預設是 443，例如，NG-UTM 預設網路 IP 位址是 192.168.1.1，把它的管理 port 改為 10443，儲存後下次登入時就須使用新的 port ，https://192.168.1.1:10443。
- 【管理介面閒置多久自動斷線】：為了避免管理者登入 NG-UTM 後長期沒有登出，讓其他人藉由已登入的瀏覽器執行設定動作，在這裡設定自動閒置斷線時間，當達到閒置時間，NG-UTM 會自動將管理者的連線斷掉，如需要再進入管理介面，則需要重新登入，閒置時間的區間為 5 ~ 60 分，預設是 60 分鐘。

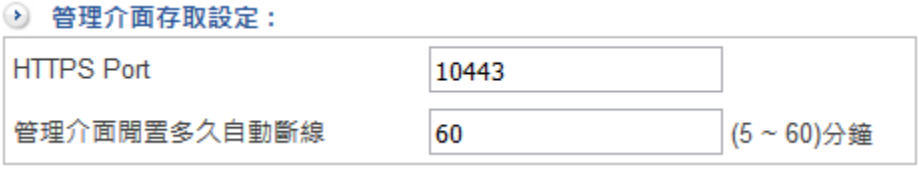


圖 2-5 HTTPS Port 及自動斷線時間

NG-UTM 可以設定多個 ZONE，每一個 ZONE 都可以設定 IP 位址，此 IP 位址就可以提供給主要管理者或是次管理者進入管理介面。

2、管理者密碼自訂規則

為了避免管理者的密碼被猜中，尤其是常被猜中的密碼 123456 或是 qazwsx 等，導致有心人士進入 NG-UTM 中為所欲為，系統提供設定密碼的複雜度跟定期的提醒管理者換密碼這 2 項措施，提高安全度，設定密碼複雜度時也會提醒是否要具備哪一些特殊的字元，例如，大寫字母，增加密碼的強度。（圖 2-6）

- 【啟用】：啟用管理者密碼管理的功能，預設是關閉。
- 【最短長度(3-16 個字元)】：設定密碼時，最短的密碼長度，從 3 ~ 16 ，由管理者決定，一般來說，越長的密碼安全性越高，但也越不容易記住。
- 【必須包含】：密碼的組合必須包含哪一些規則，這個機制是確保密碼的複雜度，避免容易被猜中，規則有大寫字母、小寫字母、數字及非英數字等 4 種，可以任選 1- 4 種組合。

  每增加一種組合，都會增加被猜中密碼的難度，相同之下，管理者自己也更難記住。 4 種組合分別是大寫字母、小寫字母、數字跟非英數字，一般情況下，由大寫字母、小寫字母、數字組合的 8 位數密碼，能提供足夠的安全性，被猜中的機率就比單純數字或是小寫字母低很多。
- 【新密碼不可包含舊密碼】：每次更改密碼時，系統會提醒管理者新設定的密碼是否跟上次一樣，如果一樣，就會提醒管理者，這項功能預設是關閉。
- 【要求修改密碼頻率】：每隔多少天，系統就會自動提醒管理者要修改密碼，預設是 90 天，0 代表關閉這項提醒的功能。

圖 2-6 管理者密碼自訂規則

2-2、時間設定

NG-UTM 的紀錄都會標註時間，所以時間的準確度很重要，系統具有自動校正時間的功能，會根據設定的時區跟時間伺服器，進行網路校正的動作。（圖 2-7）

2-2-1、設定時間與日期

1、時區與時間

- 【時區】：設定 NG-UTM 的時區，從表列的時區列表中選一個 NG-UTM 所在的時區。
- 【時間】：設定 NG-UTM 的時間。
- 【日期】：設定 NG-UTM 的日期。

自行設定時區與時間，選擇時區、時間與日期，再按下儲存，就完成設定時間的動作。

圖 2-7 設定系統時間跟時區

2、網路時間校正

將【網路時間校定】的選項啟用，並選擇網路上公開的時間伺服器或者自己輸入特定的時間伺服器，NG-UTM 每 30 分鐘跟時間伺服器校正一次，並將校正過的資料顯示在【時區與時間】中，所有跟時間伺服器校正的過程，都會記錄在【時間記錄】中。

- 【網路時間校定】：要不要啟用這項功能，預設是關閉。
- 【目前時間伺服器】：目前使用的時間伺服器。

  立即更新 ：如果需要馬上校正時間，可以按下 立即更新 按鈕，系統會立刻跟設定的時間伺服器校正資料。

  時間記錄 ：紀錄 NG-UTM 跟時間伺服器的校正資料，所有的資料會保留 3 天。。
- 【選擇時間伺服器】：按照時區，選擇適用的時間伺服器。
- 【自訂伺服器】：自行輸入使用的時間伺服器。

2-3、管理者

依照管理權限，分成主要管理者跟次管理者，主管理者具有最高權限，2 者的數量不拘，例如，預設的 admin 帳號就是預設主要管理者，NG-UTM 根據管理設備需求，可新增數個權限不一的次管理者，搭配自定義的管理者項目挑選，讓次管理者分擔主要管理者的工作內容，也可以用網路介面 (ZONE) 分配給次管理者，讓整台設備的管理更有彈性。

主要管理者的數量可以有多個，例如，由預設的主要管理者 admin 新增一個主要管理者 joy，由 joy 協助 admin 管理整台設備，此時 joy 登入後，可以改變 admin 的權限為次管理者。

為了避免因為權限設定錯誤導致沒有主要管理者，系統會自動保留最後一個具有主要管理者的帳號。在次管理者的應用情境上，設想一下幾個運作的情況，搭配自定義的管理者項目，就可以輕鬆達到要求。

A、某位管理者只能管理 VPN 的操作，例如 VPN 通道的建立，管制等，至於其他功能就不方便讓他知道太多。

B、 稽核人員可以進入 NG-UTM 中查詢被紀錄下來的資訊。

C、網管人員可以管理設備，但是沒辦法看到內容紀錄的資料。

關於管理者帳號跟權限的說明如下：

帳號管理

admin 為 NG-UTM 預設主要管理者，預設密碼為 admin，這個預設帳號無法被刪除，在第一雌安裝的情況下，需要用預設的 admin 帳號登入，此時 admin 可新增其他主要、次管理者的帳號，因為 admin 帳號在類似的網路管理者經常出現，基於安全因素，可以將它的權限限縮。

某個具備主要管理者權限的帳號，可以把預設的 admin 管理者權限修改為 Read ，不論主要管理者被修改成何種權限，NG-UTM 一定會強制保留一個具有主要管理者權限的帳號。

權限

權限分為 Read/Write/All Privileges 三種，再搭配自訂化選單功能，就能把某些項目的管理權限分配給不同的次管理者。NG-UTM 的權限配置，相當靈活，具備有 All Privileges 權限的稱之為主要管理者，具備 Read 或 Write 權限的通稱為次管理者，只有主要管理者具有新增、修改或刪除其他次管理者的權限，詳細說明如下：

【Read】：具有瀏覽功能，沒有寫入(設定)的權限，可搭配自訂化選單，讓次管理者只看到被授予看的的部分，如不搭配自訂化選單代表對整機的所有項目都具有【看】的權限。

【Write】：具有寫入、瀏覽功能，可搭配自訂化選單，次管理者就能設定被授予的項目，例如，A 次管理者被授予管理 VPN 通道，當 A 登入系統後，他左邊的選單項目只有 VPN 這個項目，其他的項目都會被隱藏。如不搭配自訂化選單代表對整機的所有項目都具有【設定】的權限。。

【All Privileges】：對整機寫入、瀏覽權限的主要管理者，因此不需要再設定自訂化選單。

2-3-1、帳號管理

帳號管理列出所有可以進入 NG-UTM 管理介面的管理者帳號及賦予權限，連他可以瀏覽或是寫入的功能項目、預計變更密碼的時間等都會列出來。

新增一個管理者

在【系統設定】>【管理員】>【帳號管理】中【新增管理者帳號及權限】按下 新增 按鈕，進入新增管理者的動作，說明如下：

- 【帳號】：新增管理者使用的帳號，任何英文跟數字的組合皆可，例如，read、joyadmin123 等。。
- 【密碼】：密碼會區分英文大、小寫，請用 3 至 64 個字元，密碼不能與帳號相同，例如，read@NG-UTM 。

  一般而言 8 位數的英文+數字組合就能提供一定程度的複雜度密碼，例如，joice735，越多位數的密碼當然會越複雜，但也更不容易記住，管理者需要在複雜度跟便利性取得平衡。
- 【密碼檢測】：NG-UTM 會自動幫您判別密碼複雜度，想讓您使用的密碼更安全可以利用下面幾種方式。

  1. 使用字母和數字混合使用。

  2. 使用特殊字元，例如 ""@""，但是冒號 "" : "" 與逗號 "" , ""禁止使用。

  3. 大小寫混合使用，例如，Joy123 的複雜度就比 joy123 高。
- 【密碼確認】：NG-UTM 需要您再次輸入設定的密碼，避免設定的密碼前後不一致。
- 【下次登入要更改密碼】：新的管理者第一次登入成功後，要不要強迫改密碼，預設是關閉。
- 【要求修改密碼頻率】：每隔多少天，系統就會自動提醒管理者要修改密碼，預設是 90 天，0 代表關閉這項提醒的功能。
- 【註解】：管理者容易辨識的描述。
- 【權限】：設定管理者的權限，共有 3 種權限可供選擇，分別是 Read 、 Write 跟 All Privileges ，選擇 Read 跟 Write 權限下，如果沒有勾選自訂化選單代表這一個管

理者可以看到所有的功能選項，因為 All Privileges 是主要管理者，選擇它時，自訂化選單會被自動隱藏。

■ 【自訂化選單】：主要管理者授予次管理者能瀏覽或管理的項目，如果沒有勾選【自訂化選單】，代表次管理員可以瀏覽整個系統。

NG-UTM 的設定架構是由主項目 + 次選單 + 分頁選單的組合，實際的設定區是在分頁選單中，只要管制次管理者能不能看到 主項目 + 次選單這 2 個項目，就可以控制它的使用權限，這 2 個項目基本上都在左邊的主選單區，所以自訂化選單 = 左邊主選單區。

範例：建立自訂化選單，並觀察 Read 跟 Write 權限的不同。

A、設定自訂化選單有「基本設定」、「訊息通知」、「區域設定」、「IP Tunnel」、「管制規則」、「位址表」等項目（圖 2-8）

圖 2-8 自訂化選單

B、具有 Read 權限的帳號登入管理介面後，他可以看到選單的項目，但是沒有【確定】或是【儲存】的按鈕。（圖 2-9）

圖 2-9 Read 權限及自訂功能

C、具有 Write 權限的帳號登入管理介面後，他可以看到選單的項目，且有【確定】或是【儲存】的按鈕。(圖 2-10)

圖 2-10 write 權限及自訂功能

2-3-2、管理者的 IP 位址

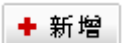
NG-UTM 可以限制來源 IP 位址進入管理介面，藉以排除不相關的人員猜測帳號、密碼的機會，預設值是空白，代表不限制來源 IP 位址，任何內、外網路來源 IP 位址都可以進入管理介面。

NG-UTM 通常會開啟 NAT 功能，所以設定來源 IP 位址必須要注意內、外網的 IP 位址，例如，設定內部的 IP 位址可以進入管理介面，但沒有設定外部網路進入的來源 IP 位址，當需要從外部網路連入系統時，就會被拒絕。

一但有 IP 位址被設定，代表啟用這一個過濾機制，只有符合的來源 IP 位址可以進入，因此在設定上管理者務必要小心，一定要確保自己的 IP 位址有被加入，以免發生無法進入管理介面。

新增第一筆來源 IP 位址時一定要加入當下管理者的來源 IP 位址，如果沒把自己加入為第一筆，儲存後，這項 IP 過濾功能就啟用，此時就會發現自己進不去(不是被允許的來源 IP 位址)。

新增一筆管理者 IP 位址

在【管理者的 IP 位址】中，點選 

按鈕。進入新增來源 IP 位址的動作，說明如下：(圖 2-11)

- 【註解】：來源 IP 位址容易辨識的名稱。
- 【IP 與網路遮罩】：可以進入管理介面的來源 IP 區段，不論是合法的 IP 位址或是 私有 IP 位址都可以，設定時要注意子網路遮罩問題，如果是合法 IP 位址，通常會用 255.255.255.255 ，代表某一個固定的 IP 位址，內部私有 IP 位址通常會用 255.255.255.0 ，代表內部某一個 區段的 來源 IP 位址。

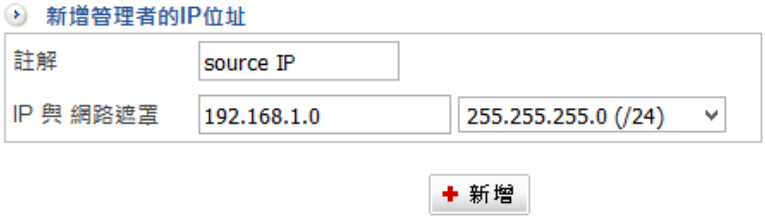


圖 2-11 設定管理者的來源 IP 位址

管理者通常會先設定自己內部網路的 IP 位址，確保自己能進入管理介面後，再去增加其他的 IP 位址，如果萬一自己的區域沒加入，就會發生無法利用進入管理介面的窘境，此時只能藉由 RS-232 介面進入把這一個功能取消，才有辦法利用網路進入管理介面。。

2-3-3、記錄清除

NG-UTM 會記錄大量的資料，包含管理者登入、登出甚至他在這一台設備的操作紀錄，還有使用者通過這台設備的使用紀錄，包含郵件、WEB/HTTPS 等，還有系統運作及防護的記錄，包含防火牆攻防紀錄、IPS 及病毒等，當這些資料累積到一定的程度，有些是按容量，有些是按時間，系統就必須把這一些資料清除掉。

記錄清除

這個地方就是【手動清除紀錄】的項目，當管理者認為需要清除某些系統紀錄時，就到這裡執行，根據不同的型號有不同的清除項目，最多有 11 個紀錄資訊。依據需求選擇適當項目清除，勾選【全選】時，就是選擇所有項目，按下清除按鈕，把已經記錄在 NG-UTM 內的資料清除掉，讓系統重新記錄。

內容記錄保留時間設定

NG-UTM 有些內建硬碟，有些是用內部的記憶卡紀錄系統資訊，有硬碟的系統，記錄最高保存時間為 36 個月(3 年)，超過 3 年的歷史資料，一定會被清除掉，沒有硬碟的設備系統會自動設定儲存上限，一般是 使用 90% 以上就會觸發清除機制。

系統的預設值為 12 個月(1 年)，管理員可以依照實際的需求在可以設定的範圍內(1~36 個月)設定要保留的時間。

一些數量比較大且跟系統運作無關的紀錄，例如，郵件過濾、流量統計跟 DNS 查詢紀錄，時間間隔會縮小。

2-4、系統升級

NG-UTM 的最新韌體資訊發佈在官網上，管理者可以在 [www.sharetech.com.tw] (http://www.sharetech.com.tw) 網站上找到最新的韌體資訊下載，升級的方式有全自動、半自動跟手動 3 種方式，【系統設定】 > 【系統升級】 > 【韌體資訊】 所設定的是全自動跟半自動，【系統設定】 > 【系統升級】 > 【軟體升級】 是手動升級。

韌體的下載有 2 種方式可以選擇，在全自動跟半自動模式下， NG-UTM 定時到更新伺服器自動檢查，有新的韌體時會自動下載到設備的儲存媒體中，讓管理者手動更新或是在設定的時間執行升級動作，手動升級模式是管理者取得最新韌體後上傳到 NG-UTM 中。

除了全自動外，半自動跟手動方式取得韌體後，一定要由管理者按下確認升級的按鈕，NG-UTM 才會執行升級動作。

2-4-1、韌體資訊

這裡設定是全自動跟半自動的升級模式，2 者最大的差別是，當檢查到新的韌體後，全自動模式會在指定時間自動執行韌體升級，半自動模式只是幫管理者下載升級韌體，由管理者登入管理介面後，按下升級按鈕，完成升級動作。(圖 2-12)

圖 2-12 NG-UTM 的韌體升級設定

3 種升級模式描述如下：

1. 手動升級：取得韌體後在 【系統設定】 > 【系統升級】 > 【軟體升級】 上傳韌體，完成升級動作。

2. 半自動模式：自動檢查及下載韌體，管理者手動更新，系統定期到更新伺服器檢查韌體，並將最新韌體自動下載到設備中，管理者登入管理介面後，按下韌體升級按鈕，執行升級動作。

3. 全自動模式：自動檢查及下載韌體，有新韌體後自動下載到設備中，並在預定時間，自動執行韌體升級動作，在執行升級動作前，可設定通知管理者，預計要執行韌體升級的時間，管理者收到郵件後如果不想升級，可以進入管理介面中暫停或是刪除升級檔。

- 【最後更新時間】：最後一次韌體資訊檢查的時間，管理員想要馬上知道此時是否有最新的韌體，可以按下 更 新 按鈕，NG-UTM 馬上跟更新伺服器檢查是否有新的韌體，如果有的話就會下載到設備中讓管理者使用。

- 【定時更新時間】：設定每天檢查的時間，這個只是檢查跟下載韌體的時間，不是軟體升級的時間。

- 【更新伺服器】：NG-UTM 檢查最新韌體的伺服器名稱，系統預設，管理者無法更改，預設網址為：autoUpdate.sharetech.com.tw。

- 【自動下載】：啟用自動下載的功能後，NG-UTM 在指定時間到更新伺服器檢查最新韌體後，自動將韌體下載 NG-UTM 中，等候管理員進一步的指令，指令有 2 種，一種是全自動升級另一種是半自動升級。

- 【自動升級韌體】：全自動升級韌體模式，首先啟用**自動下載**的功能後，此功能才能被啟用，針對自動下載的韌體，在管理者排定的時間內，執行升級動作。

  當自動升級韌體過程因為種種的因素導致升級失敗，此時這個功能就會被停用，也就是失敗之後除非管理者介入排除失敗因素，系統將不再執行自動升級韌體動作。

- 【升級韌體時間】：管理者指定韌體預訂升級的時間，執行升級動作，一般而言為了避免影響正常的使用，通常會排定在系統使用率最低的時候。

- 【自動升級通知】：當有新韌體且已經下載到 NG-UTM 中，在排定升級韌體的前幾個小時，寄出升級通知郵件通知管理者，在全自動模式下升級成功或是失敗都會寄出通知信。

  管理者郵件帳號可以設定多筆，設定管理者的郵件帳號在 【系統設定】 > 【訊息通知】 > 【訊息通知】 中的收件者項目中

- 【韌體升級紀錄】：每次韌體更新的動作，系統都會詳細記錄時間、版本、成功或是失敗，這些資料由紀錄按鈕中取得。

韌體檔案

NG-UTM 到更新伺服器的檢查後，如果有最新韌體且選擇自動下載，最新的韌體檔案就會被下載並放在系統，等候管理者的命令，當管理者決定升級後，只要在韌體升級上按下升級，系統就會開始自動執行升級動作。

通常韌體更新需 3 分鐘的時間，更新後系統將會自動重新開機，而在系統更新期間請勿關機、斷線或是離開網頁，這可能會造成 NG-UTM 不可預期之錯誤。

管理者也可以把韌體下載到本機中，在用手動的方式上傳到設備中，通常這個動作是要檢查下載檔案的 MD5 值跟網站公布的韌體 MD5 值是否一樣，當 2 者不一樣時，韌體檔案有被竄改的可能。

2-4-2、軟體升級

這是手動升級韌體機制，在韌體升級部分，除了管理者使用更新伺服器自動下載外，另一種方式就是由管理者先取得韌體後，再上傳到 NG-UTM 中。

- 【伺服器型號】：NG-UTM 的型號。
- 【目前軟體版本】：NG-UTM 的軟體版本，9.0.0.0 是最初始的版本號碼，新的板本號碼數字會比前一版的數字更大，目前的版號為 9.0.2.1。
- 【軟體升級】：選擇要上傳到 NG-UTM 中的韌體。

按下 升級 按鈕後，系統就會開始執行升級動作。

升級記錄

不論是使用自動下載後更新韌體或是由管理者上傳最新韌體到 NG-UTM 中，只要有韌體更新動作，所有的升級紀錄都會顯示在升級記錄中，包含升級的日期時間及人員等資料，例如：

2018-04-27 12:37:24 ==> 9.0.1.4 to 9.0.1.5

代表 2018-04-27 版本升級。

2018-05-24 11:09:08 ==> 9.0.1.5 fix language files

代表 2018-05-24 的更新版本是修正語系檔。

2-4-3、韌體下載紀錄

不論採用自動下載或是手動上傳，甚至升級動作是成功或是失敗，NG-UTM 會把這一些過程記錄下來，管理者可以透過【韌體下載紀錄】，找尋過去的歷史記錄，包含起始時間、結束時間、傳輸時間、版本、大小、事件等記錄。（圖 2-13）

■ 【版本/事件】：NG-UTM 成功或是失敗的事件。

起始時間	結束時間	傳輸時間	版本	大小	事件	下載
2013-06-20 11:31:51	2013-06-20 11:31:52	1 秒	2.1.8.3	23.12KB	成功	
2013-06-20 11:34:54	2013-06-20 11:35:32	38 秒	2.1.8.1	3.82MB	成功	
2013-06-20 11:46:01	2013-06-20 11:46:02	1 秒	2.1.8.2	2.06KB	成功	

圖 2-13 韌體下載搜尋

2-5、備份與還原

當設定 NG-UTM 完成且正常運作下，管理者會把所有的設定資料備份下來，並將備份檔案另外保管，以備不時之需。在相同硬體規格下，備份出來的檔案，可以匯入另一台 NG-UTM 中，達成還原的動作，儲存備份檔案有 2 個方式，一個是 USB 另一個是本機的儲存媒體。

備份動作分成手動跟全自動，手動方式在【系統備份與還原】中，全自動在【自動備份】中，所以在【系統備份與還原】中都是備份當下的設定檔。

萬一備份還原的動作仍然無法滿足，管理員可以對系統執行恢復出廠值的動作，把 NG-UTM 還原到最初的狀態，再重新設定。。

2-5-1、系統備份與還原

這裡的動作都是手動的備份與還原，系統只備份當下的設定檔。NG-UTM 的備份資料儲存有 2 種模式，USB 跟備份檔，USB 是將備份檔直接傳到 USB 裝置上，備份檔是以檔案形式存在管理者的電腦中。2 種備份方式使用目的不太一樣，在還原時做法稍微也不一樣，管理者可以 2 個都使用。

系統備份至 USB

在設備上插入 USB 的裝置，並按下備份按鈕，系統會自動偵測 USB 設備，如果存在，自動將所有設定檔複製到 USB 中，此時就可以把 USB 設備拔除，因為設備重新開機時，會檢查 USB 是否存在，如果存在則會直接進行設定檔還原動作，所以 USB 的備份就是為了快速地將設備還原成最初設定完成的狀態。

每當 NG-UTM 重新開機時，會自動偵測備份的 USB 是否存在，如果存在，自動將 USB 的備份檔載入，並執行系統還原動作，所以這個功能適用於更換故障硬體設備，把新的設備插入當初備份的 USB，就可以快速的把機器還原回原來的狀態。

系統備份

管理者在這裡按下備份鍵，就可將目前系統之設定值匯出。NG-UTM 會將整個系統的設定資料，壓縮成一個 tgz 格式的壓縮檔，當要執行還原動作時，匯入這一個檔案，系統就會回到當初備份時的狀態。（圖 2-14）

圖 2-14 系統備份

系統還原

管理者選擇想要還原的設定檔，設定檔的格式為一個 tgz 格式的壓縮檔，選擇完畢後按下確定鍵，系統會自動上傳設定檔，上傳時，NG-UTM 會自動再檢查一次設定檔是否有損壞，如果有損壞，將不會執行還原動作，只有檢查是正常的設定檔，才會將它解壓縮後還原到系統中，重新開機後，NG-UTM 就回到當初備份時的狀態。

恢復出廠預設值

管理者可以將整台設備還原到出廠值，按下【確定恢復】按鈕後，NG-UTM 會清掉所有的設定值，同時將 ZONE 0 的 ETH0 介面 IP 位址改為 192.168.1.1。

A、【恢復出廠預設值 > 保留網路介面設定】：執行恢復出廠設定值時，是否要保留原來的網路介面 IP 設定值，啟用這個選項時系統會回到出廠值，但保留所有的 IP 位址設定。

這個機制適用於網路架構是正常，但是管制動作或是內部資料太複雜，管理者就可以保留設定的網路資料，然後其他的資料通通清除後重設。

B、【恢復出廠預設值 > 格式化硬碟】：管理者可自行決定執行恢復出廠設定值時，是否順便要執行格式化硬碟的動作，如果有勾選格式化硬碟的選項，會將整顆硬碟重新格式化，此時會比單純執行恢復出廠值需要更多的時間，當 NG-UTM 執行完這一些動作後，會重新開機，開機完成，就回到系統最原始的出廠預設值。

硬碟狀態

NG-UTM 的 LOG 都是記錄在硬碟中，系統會自動檢查硬碟的狀態，並將狀態呈現在管理介面中，讓管理者輕易了解硬碟目前的情況是正常還是有發現一些問題，當硬碟故障時，不會影響網路封包的傳送、接收，但是該記錄的資料可能因為硬碟毀損而無法記錄。

2-5-2、自動備份

為了節省管理者定期執行備份動作的時間及工作，也為了保護設備資料不遺漏，NG-UTM 提供自動備份功能，管理者只要設定備份的日期與時間並選擇保留在 NG-UTM 硬碟的備份的數量，系統會依管理者設定時間自動進行備份動作，超過設定份數的舊設定檔會被自動刪除。

- 【啟用】：勾選啟用的選項後，就開始選擇執行備份的日期、時間選項。
- 【自動備份時間】：有 2 種模式可供選擇，一種是週期性日期跟時間，例如，每隔 3 天或是每隔 23 小時定期執行備份動作。另一種是自訂日期及時間，例如，每星期一的凌晨 00:00 執行備份動作。
- 【保留備份數量】：NG-UTM 會在系統上保留最新的數份設定檔，新的設定檔將會覆蓋較舊的，覆蓋的行為採取先進先出的覆蓋方式，預設值為 3 份。
- 【立即備份】：按下立即備份按鈕，系統馬上執行備份動作，並將它儲存在 NG-UTM 中，如果設定檔跟最後一次自動備份的資料一樣，也會提醒管理者

備份記錄

所有定時備份的記錄，都會被保留下來，包含備份時間、軟體版本等，管理者可以對任何自動備份下來的資料執行下列 5 種動作【下載至 USB】、【下載】、【還原】、【刪除】、【紀錄】等。

- 【下載至 USB】：將備份檔儲存在 USB 裝置上，這個好處是，當系統重新開機時，偵測到這個 USB 裝置時，會自動執行還原動作，不需要管理者再去點選系統還原的動作。
- 【下載】：把這一份備份檔下載到管理者的電腦中。
- 【還原】：管理員想讓 NG-UTM 直接回到某一時期設定檔的狀態，點選**還原**鍵，NG-UTM 會要求管理員輸入一個隨機數字，再次確認是否要執行還原動作，避免誤動作，確認無誤後會自動進行還原動作，當系統重新開機後，還原到執行自動備份的狀態，有點像時光回朔器的效果。（圖 2-15)

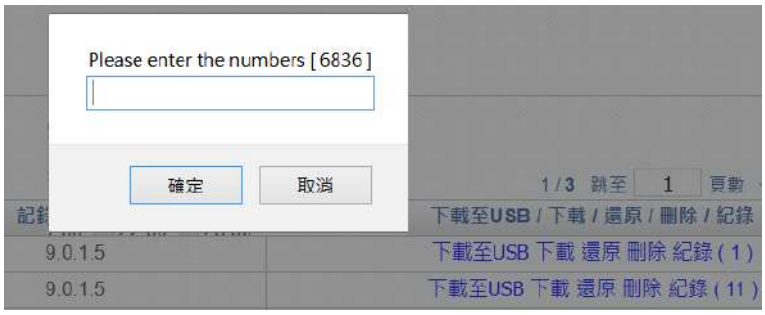


圖 2-15 系統還原

- 【刪除】：把這個備份設定檔從系統中刪除。
- 【記錄】：自動備份的設定檔跟上一個自動備份設定檔的差異項目，NG-UTM 會詳細記錄這 2 者的差異，到底改了哪一些項目，系統都會詳細記錄，方便管理者追蹤比較。（圖 2-16)

圖 2-16 NG-UTM 自動備份的差異記錄

在記錄中會留下更改時間、帳號、管理者 IP 位址、更改的項目、動作跟每個項目更改前及更改後的比較，管理者依據這一些資料判斷要不要執行還原或是找出問題的癥結。

2-6、訊息通知

NG-UTM 會用郵件通知管理者，系統發生的大大小小事件，小到備份資料成功與否，大到系統被攻擊，讓管理員可以在第一時間掌控設備及網路訊息。NG-UTM 提供的通知功能是以郵件的方式進行，因此管理員需先設定基本 SMTP 伺服器與收件者帳號，NG-UTM 才會在事件發生的第一個時間內通知指定的管理人員。

2-6-1、訊息通知

當事件發生後，NG-UTM 使用郵件通知管理人員，不同的事件可以使用不同的寄件者帳號，寄出通知信，也可以有多個收件者收到這樣的通知訊息。

訊息通知

NG-UTM 共有 24 種訊息通知的事件，每一種事件依照其類型可以做週期性的檢查或是定期性的檢查，檢查後如果發現事件有問題，就會根據管理者設定的收件者，寄出訊息通知郵件。(圖 2-17)

圖 2-17 訊息通知郵件設定

訊息通知-寄件者設定

- 【寄件者帳號】：選擇寄出通知郵件時使用的寄件者帳號，寄件帳號可以在【SMTP 伺服器設定】中設定，共有 2 種模式，自動跟指定 SMTP 帳號。

  自動

  選擇自動模式時，系統會從【SMTP 伺服器設定】中選擇跟收件者相同網域名稱的為優先，並用他寄出通知信，例如，寄件者帳號有 2 筆，一筆為 a@abcd.com，另一筆為 b@ghij.com，當收件者為 kkk@ghij.com 時，NG-UTM 會自動選 b@ghij.com 為寄件者帳號，若無任何對應關係，則使用第一筆為寄件者，寄出通知信。

  指定 SMTP 帳號

  取出【SMTP 伺服器設定】中設定的寄件者為寄件者帳號，寄出通知信。

  如果沒有任何寄件帳號在【SMTP 伺服器設定】中被設定，則不會寄出訊息通知信。

- 【收件者】：輸入訊息通知郵件的收件者，每個事件可以有多個收件者，每一個收件者一行。

- 【嘗試寄送次數】：當通知信寄出時，傳送失敗，最多會嘗試幾次傳送，設定的範圍是 1~5 次，當寄送不成功的通知郵件超過設定的次數，此封訊息通知將不會寄出。

- 【通知信語系】：選擇通知郵件的語系，共有 English、繁體中文跟簡體中文 3 種，如果語系設定不正確，有可能導致收信者收到的通知信是亂碼。

訊息通知事件

NG-UTM 目前提供 25 種的事件通知信，每一種檢查項目根據其屬性，而有不同的檢查時間及機制，例如，線路斷線與否這一個檢查項目不可能是定時檢查，他一定是週期性時間檢查。另一個範例是檢查時間的頻率，例如防火牆防護的檢查週期性就會比系統操作日誌的頻繁，免得攻擊已經過了，才發出系統通知郵件。

不論哪一種事件，發出通知訊息的郵件主旨都可以更改，管理員可以把它改成更容易讓收件者理解的主旨，例如，線路斷線的通知信郵件主旨預設為【ZONE disconnect】，它可以被改成【台北 NG-UTM 斷線】，讓收信者在收信的當下，更容易由主旨來判斷郵件的內容。

如果通知信的項目沒有被啟用，系統就不會發出這個項目的通知信，依據型號不同，25 項通知項目也不一樣，每項通知的說明如下：

1. 線路斷線：檢查廣域網路 (WAN) 對外是否暢通。
2. DDNS 更新失敗：設定的 DDNS 服務是否正常更新及運作。
3. HA 狀態切換及資料同步異常：HA 模式下，Master 跟 Slave 曾經切換或者 2 台設備的資料在同步時有異常。
4. 防火牆攻擊防護 (SYN, ICMP, UDP, PortScan)：NG-UTM 遭受到攻擊時，系統會發出通知信。
5. 異常流量 IP：Session, Zone Out (TX), Zone In (RX)：內部上網的電腦超出設定的流量。
6. 病毒阻擋 (上網,收信...)：郵件或是上網的檔案發現病毒。
7. 系統操作日誌：系統操作日誌有異動的資料。
8. 管理者使用帳號,登入錯誤事件：管理者登入時發生密碼錯誤現象。
9. SSL-VPN,上網認證,登入錯誤事件：SSL VPN 用戶登入時，帳號密碼驗證錯誤。
10. 軟體更新通知：新的韌體發佈。
11. 硬碟容量過低 (Usage over 90%) 和壞軌：硬碟可用空間太少或是有壞軌現象。
12. 自動備份系統設定檔：自動備份成功與否的通知信。
13. 協同防禦：跟交換器、無線 AP 的協同防禦阻擋通知信。
14. 資料庫異常通知：本機的資料庫異常。
15. AP 管理通知 (AP 管理請求, 連線狀態異常)：新 AP 申請加入或是有連線異常狀況。
16. 郵件流量封鎖防禦：對外大量寄信超過設定值通知信。
17. IPSec 斷線通知：IPSec VPN 斷線通知信。
18. IPSec 切換通知：SD-WAN 環境下，任何一個 IPSec 通道斷線通知信。
19. 上網認證即將到期通知：上網認證使用者的帳號即將到期。
20. 上網認證到期刪除通知：上網認證的帳號到期後，系統要將它刪除前，通知管理者。

21. 流量配額用完通知：設定流量配額下，即將用完配額。

22. UPS 記錄：跟 UPS 的通聯記錄。

23. CMS 通知 (客戶端管理請求,連線狀態異常,備份失敗,還原失敗)：CMS 運作下的通知信

24. 應用程式版本異動通知：本機的應用程式版本有新版本釋出。

25.系統空間異常：系統的儲存空間太少或是在短時間內被塞滿，發出通知。

2-6-2、訊息通知記錄

NG-UTM 會把每一次寄出的訊息通知，不論成功與否都紀錄下來，方便管理人員日後查詢。要查詢這些紀錄就在訊息通知記錄中。（圖 2-18）

訊息通知紀錄搜尋

- 【日期】：搜尋指定時間內的通知紀錄。
- 【事件】：可自選事件項目或是全部事件。
- 【收件者】：訊息通知的收件者，可以用 “*” 為萬用搜尋關鍵字，例如 *@abcd.com。

訊息通知搜尋結果　1 / 9　跳至 1 頁數、每頁 16 筆 GO　匯出　匯出全部

日期	事件	收件者	內容
2016-03-02 08:36:03	IPSec 切換通知	mandy@sharetech.com.tw	
2016-03-02 08:27:07	IPSec 切換通知	mandy@sharetech.com.tw	
2016-03-02 08:18:02	IPSec 切換通知	mandy@sharetech.com.tw	
2016-03-02 08:06:03	IPSec 切換通知	mandy@sharetech.com.tw	
2016-03-02 07:57:02	IPSec 切換通知	mandy@sharetech.com.tw	

圖 2-18 訊息通知紀錄搜尋

搜尋的結果是以紀錄的時間為排序，也可以按照事件來排序分類，點選內容中圖示後，就會出現更詳細的資料，以下為其中一筆 NG-UTM 的通知信記錄範例：（圖 2-19）

IPSec 切換通知

VPN 通道名称	时间	类型	切换
mandy	2016-03-02 08:36:03	自动	主要 >> 备援

圖 2-19 訊息通知紀錄

2-6-3、SMTP 伺服器設定

NG-UTM 寄出通知郵件時需要使用 SMTP 伺服器設定寄件帳號，如果沒有設定任何有效的寄件者帳號，則所有的通知信將無法順利寄出，管理者可以設定多筆寄件者帳號。

當【訊息通知】中的寄件者帳號選擇為自動時，且設有 2 筆以上的寄件者帳號，系統會自動比對收件者帳號中網域名稱，是否有跟寄件者帳號的網域名稱相同，如果有相同，則會挑選相同網域名稱的寄件者為寄件者帳號，若無任何相同的網域名稱，則挑出第一個有效的帳號寄出，萬一此時仍然無法寄出通知訊息郵件，會再挑第二個寄件者帳號寄出，直到達到嘗試寄送次數後，才會停止寄送通知信的動作。

新增寄件者帳號

- 【寄件者名稱】：預設的寄件者名稱為 Admin，管理者可以更改名稱，勾選【自訂名稱】後，就可以將 Admin 改成收信者容易辨識的名稱，例如，來自 NG-UTM 的通知。
- 【寄件者】：顯示在收信者的通知信郵件的寄件者名稱；例如，喬丹@台中 UTM。

  它只是顯示名稱，不是寄件者帳號，一般的郵件軟體預設會顯示寄件者名稱，如果寄件者沒有設定名稱，才會以郵件帳號當作顯示名稱。。
- 【伺服器】：SMTP 郵件伺服器主機；例如，abcd.com 或 211.22.22.22
- 【Port】：SMTP 是 TCP 25，SMTPS 是 465 或是 587，由寄件伺服器決定。
- 【帳號】：登入 SMTP 郵件伺服器的帳號，根據每一個 SMTP 郵件伺服器的不同要求，輸入帳號或是完整 email，例如 jean 或是 jean@abcd.com。
- 【密碼】：登入 SMTP 郵件伺服器寄件者帳號的密碼，例如 1234。
- 【需要驗證】：若 SMTP 郵件伺服器需要帳號認證，請勾選。
- 【TLS】：根據 SMTP 郵件伺服器的要求，寄件帳號登入的方式，選擇是否要啟動 TLS，TLS 是利用密鑰演算法在網際網路上提供身份認證與通訊保密的通訊協定。
- 【郵件寄送網域】：寄送郵件過濾時使用的寄件者網域通常需要跟收件者的網域相同，否則會發生 A 網域寄給 B 網域通知信的問題。

  例如，寄件者帳號 a@ghij.com 只會寄給 ppp@ghij.com 的收件者，這裡就填入 ghij.com，除了這個 ghij.com 網域外，此寄件者帳號不會寄出通知信郵件，預設為空白，代表任何網域都可以利用這個寄件者帳號。。

- 【指定來源位址】：某些郵件伺服器只對特定的寄件 IP 位址提供服務，要用它來寄信，就需要輸入郵件伺服器指定 IP 位址。

寄件者帳號驗證寄信

設定完成 SMTP 伺服器的寄件者帳號後，如果擔心設定的資料有誤，造成收信者無法正常的收到訊息通知郵件，NG-UTM 提供線上測試寄信功能。

在【SMTP 伺服器設定】上，NG-UTM 會列出每一個寄件者帳號的詳細資料，在【SMTP 測試郵件】區，有【測試】的按鈕，按下後系統會自動出現一個對話框，此時輸入收件者的郵件帳號。（圖 2-20）

輸入收件人郵件位址，例如，jordan@abcd.com，輸入完畢後按下確定，如果寄件者帳號設定正確，jordan@abcd.com 的郵件信箱會出現一封主旨名稱為【This is a SMTP TestMail】的信件，代表 SMTP 伺服器設定資料正確無誤，訊息通知郵件會正常的寄出。

圖 2-20 測試 SMTP 伺服器

2-7、重新啟動&關機

NG-UTM 提供 2 個按鈕執行正常開關機動作，管理者依照需求執行，另外，為提高運作的穩定度，系統可以執行定期重新開關機動作。

2-7-1、重新啟動&關機

這是 NG-UTM 正常的開關動作，系統提供 2 個按鈕，分別是【重新啟動】與【關閉】，按下重新啟動按鈕後，系統會把所有的服務關閉，重新開機，並載入預先儲存在設定檔中的資訊，按下關閉就會把 NG-UTM 按照正常程序關機。

2-7-2、自動重新啟動

系統可以週期性的自動重新啟動，重新開機的好處是清除掉不必要又佔據記憶體的不正常檔案或是暫存檔，增加系統的穩定度。週期的長度有天、周跟月 3 種，管理者可以根據自己的需求配置，一般而言，每月重新啟動一次就足夠。

- 【啟用】：啟用自動重新啟動的機制，預設值是關閉，右邊有紀錄按鈕，自動記錄重新開機的時間及成功與否。
- 【週期】：3 種週期可供選擇，天、周跟月，正常運作下每月重新開機就已經足夠。
- 【自動重啟時間】：何時執行自動重啟，一般會設在系統不會提供服務的時間。

2-8、AP 管理

首先，在談論到內網無線網路環境布局必須先了解 Thin AP 與 Fat AP 之間的差異，Thin AP 是這幾年才被提出的概念名詞，和一般無線路由器 (Fat AP) 最大不同，在於 Thin AP 功能比較單純，大多只負責無線訊號的傳遞，無法像 FAT AP 一樣進行有關管控、安全性等功能。

NG-UTM 整合無線 AP 管理功能，可以讓企業不用擔心無線網路擴充的困擾，結合無線 AP 設備，將每個 AP 通過的流量整合到 NG-UTM 的網路介面上，且 AP 彼此之間可以無縫聯繫，讓使用者在行動轉移時不會感覺到網路切換。

NG-UTM 提供了一個單獨的控制平台來管理有線與無線通聯，透由管理介面，管理員可清楚掌握每台 AP 路由器運作狀態(運作中或當機)、上傳與下載流量，與目前該 AP 路由器線上人數。最重要的管理員可直接透過控制平台直接管控每個 AP 路由器，大大減輕管理員負擔，無線 AP 管控平台可以提供強大完整無線網路保護部屬空間。

打造辦公網路環境無線熱點後，相信多數網管人員接著面臨的困擾就是該如何管控使用者利用 WiFi 上網，由於智慧型手機、平板的普及，加上 NB 筆記型電腦的廣泛使用，無線網路控管是多數企業未來必須去面對的挑戰。Thin AP 主要是傳遞無線網路訊息，對於安全的控管就比較薄弱，對於一些惡意的攻擊行為就不能有效防護，對於 WiFi 流量導到 NG-UTM 的網路環境而言，除了上述可以管控每一台無線 AP 運作狀況外，還提供身分認證機制服務，使用者利用無線上網必須通過認證，取得合法權限後才可通行。此外，透過 NG-UTM 亦可以針對無線上網之使用者進行行為控管與記錄存檔，可以限制使用者瀏覽的網頁、應用程式(即時通訊、 P2P、影音..)使用，且記錄所有使用之行為。

對於網管人員來說，以一台 NG-UTM 做為主要管理工具，透過單一管理介面，就可以管控到所有無線 AP 運作狀況，最重要的可以遠端關閉設備、下管制指令等，讓網管人員不用疲於奔命管理，大幅提高效率。除了給管理員帶來便利外，對使用者來說也可以輕鬆使用，相對地對企業網管人員來說是一個無痛導入解決方案。。

2-8-1、AP 管理設定

開啟 NG-UTM 的 AP 管理功能，預設是關閉，啟用後就可以開始加入新的被託管的 Wireless AP ，管理員可以按照不同屬性用途，把 Wireless AP 分群組，方便管理。

2-8-2、AP 管理

在 AP 管理的地方，新增被管理的 Wireless AP。（圖 2-21）

圖 2-21 新增一台無線 AP

- 【名稱】：新增被管理 AP 的名稱，任何中英文字都可以，例如，在 3F 天花板。
- 【型號】：選擇目前支援 AP 設備， AP 跟 NG-UTM 之間是用 SNMP 或是 Telnet / SSH 協議溝通，使用 Telnet / SSH 的 AP 能提供更多細項的資料，雖然 SNMP 是標準協議，但是每個 AP 都會增加自己的 SNMP 命令。

  只有經過驗證測試的 AP 才能完整呈現所有的功能，目前支援的 AP 型號及管理方式如下：

  1. Howay 2000NI : SNMP
  2. ShareTech AP-300 : SNMP
  3. Zyxel NWA1100-NH : SNMP、Telnet / SSH
  4. Zyxel NWA5123-AC : Telnet / SSH
  5. Zyxel WAC6103D-I : Telnet / SSH
  6. Zyxel NWA5123-NI : Telnet / SSH
  7. Zyxel NWA1123-ACv2 : Telnet / SSH
  8. Zyxel NWA5121-NI : Telnet / SSH。

- 【IP】：Wireless AP 的 IP 位址，例如，192.168.1.5。
- 【群組】：新增的 Wireless AP 是隸屬於哪一個已經建立的群組，同一個群組的 AP 可以套用同一個管理動作跟資料的統一派送，如果要新創一個群組，在後面空白欄內填入新群組的名稱，系統就會自動創建一個新的群組，群組名稱任何中英文+數字都可以。
- 【SNMP 埠號】：AP 用 SNMP 協定跟 NG-UTM 溝通使用的 port ，SNMP 一般是使用 161。
- 【SNMP 登入名稱 (Read)】：使用 SNMP 溝通時，使用只具有 READ 權限的帳號，一般預設是 public。
- 【SNMP 登入名稱 (Write)】：使用 SNMP 溝通時，使用只具有 WRITE 權限的帳號，一般預設是 private ， 基於安全因素，一般這個帳號都會被改掉。
- 【命令模式】：NG-UTM 使用哪一種協定跟後面的 AP 溝通，有 Telnet 跟 SSH 2 種，Telnet 為非加密的連線，所以一般都會建議使用加密的 SSH 連線。
- 【命令 Port】：Telnet 使用 TCP 23，SSH 使用 TCP 22。
- 【登入帳號】：無線 AP 的管理者帳號。
- 【登入密碼】：無線 AP 的管理者密碼。
- 【連線測試】：驗證上面的資料是否正常，NG-UTM 能跟設定的無線 AP 正常地溝通。

AP 列表

所有被管理的無線 AP 都會按照設定的群組分類，顯示每一台被管理的 Wireless AP 的狀態跟使用人數，範例如下。（圖 2-22）

- 【AP 管理請求】：每個被新增的 AP 設備，都會發出被管理的請求，當管理者接受後，才會進入 AP 設備的列表中，如果有新的 AP 要加入，這裡就會呈現數量，管理者點選後就可以加入。
- 【群組名稱】：按照群組名稱分類所有的 AP 設備
- 【狀態】：代表斷線，NG-UTM 無法跟 Wireless AP 取得聯繫，代表連線中。
- 【通道】：目前 Wireless AP 使用的無線通道，如果是自動選擇通道則會出現 Auto 字樣。
- 【SSID】：SSID 跟使用的頻帶，頻帶分成 2.4G 跟 5G 2 種，每一個不同的 Wireless AP 功能不一樣，有些只有 2.4G，有些支援 2.4G/5G 雙頻。
- 【線上人數】：每個 SSID 目前有多人正在使用。

  點選線上人數，NG-UTM 就會顯示出過去一天或是一段時間內利用這個 SSID 上網的人數統計圖，讓管理者查詢，管理者可以查詢當天跟歷史的資料。

  這個地方是根據每個 SSID 列出使用人數，在【系統狀態】 > 【連線狀態】 > 【無線成員列表】 會列出所有正在使用無線設備的設備。
- 【流量】：每個 SSID 目前的流量。

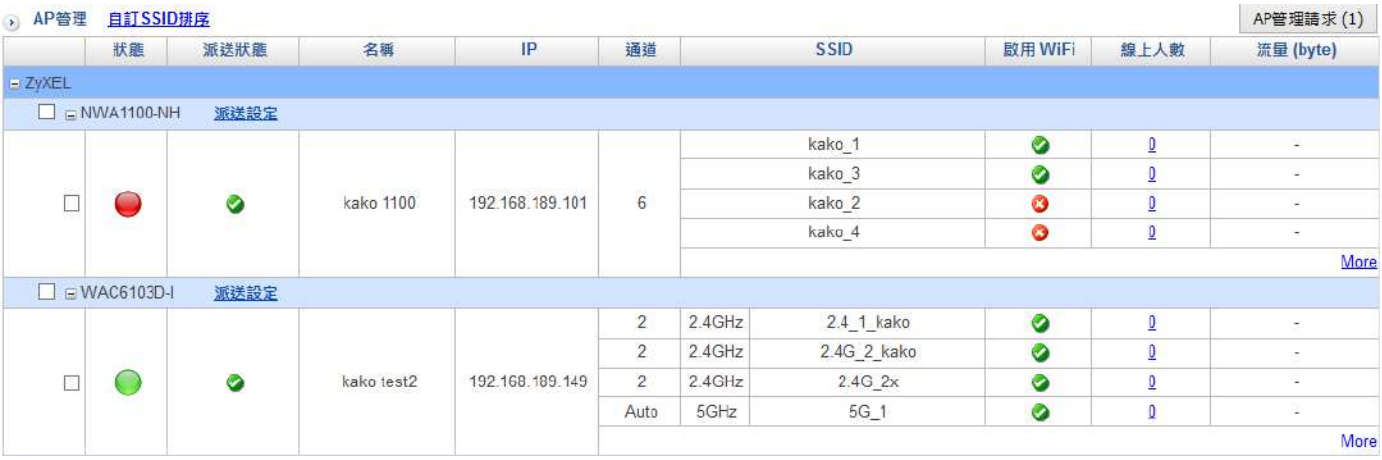


圖 2-22 無線 AP 列表

Wireless AP 設定派送

所有被管理的無線 AP 都可以用 NG-UTM，將常用的設定檔派送到無線 AP 上，例如，SSID 甚至可以更改無線 AP 上管理者的密碼，下列針對無線常用的功能解說。（圖 2-23）

- 【派送項目】：選擇要執行派送的項目，共有 AP 設定(2.4G/5G)、內部網路、管理介面密碼跟管理介面存取等。
- 【新增 SSID】：在原有的無線 AP 上再增加一組 SSID。
- 【網路模式】：使用 802.11B/G/N 中的哪一個。
- 【頻率/頻寬】：使用的通道。

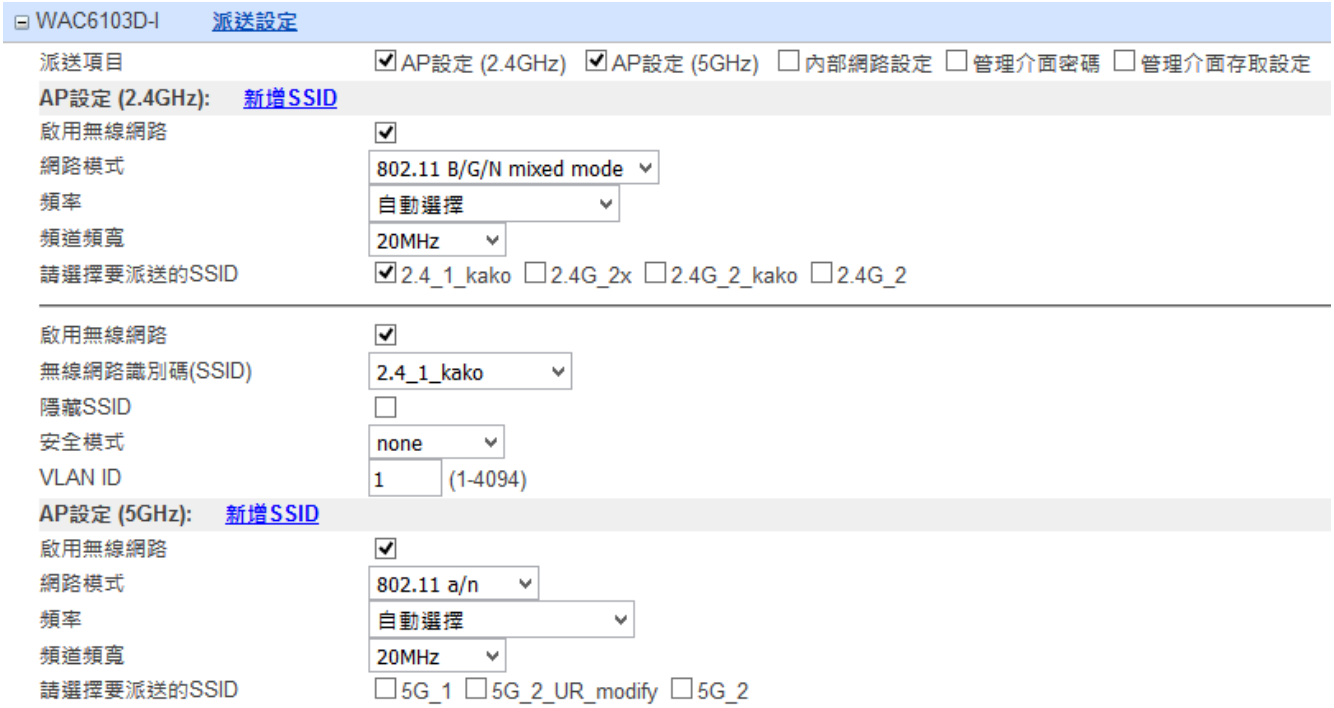


圖 2-23 無線 AP 設定派送

2-9、特徵碼更新

NG-UTM 仰賴封包特徵值比對，確認往來的封包是正常還有危害，ShareTech 會將蒐集到的特徵值定期推送到每一台設備，讓所有的資料都在最新的狀態，目前系統有 3 個自動更新的資料庫，分別是 URL 黑名單資料庫、應用程式管制規則、IPS 特徵碼。（圖 2-24）

特徵碼更新

名稱	版本	最後檢查日期	自動更新	功能
URL 黑名單資料庫更新	2.4.2	2018-06-19 01:10:03	☑	馬上檢查
應用程式管制規則更新	5.1.10	2018-06-19 01:10:05	☑	馬上更新
IPS 特徵碼更新	1.5.3.56	2018-06-19 01:10:13	☑	馬上檢查

圖 2-24 特徵碼更新

管理者也可以點選【馬上更新】按鈕，立刻檢查。

應用程式的特徵隨使用版本變化，判斷的特徵值就會變化，所以管理者應該套用自動檢查及更新，確保管理的應用程式能正常運作。

2-10、雲端管理服務

對多數的企業而言，管理網路的安全是一件複雜且辛苦的工作。尤其對正在成長中的企業而言，要如何能快速回應與維護所面臨的網路問題更是一項艱深的挑戰。網管人員需要的是一個簡單的管理工具，可以用來對相關的網路設備或行為進行控制，

而 EyeCloud 雲眼管理系統就是一個集中式的雲端管理設備，透過瀏覽介面可以針對旗下設備，包含防火牆、UTM、無線 AP、交換器或郵件伺服器...等，輕鬆從任何一地進行設備設定、管理、監控與問題排除。此外，EyeCloud 並整合 Line 即時通知服務，可以有效減輕網管人員工作負載量，縮短維護管理時間，提升企業競爭力。

2-10-1、雲端管理服務

在【系統設定】之【雲端管理服務】功能中，點選「啟用」雲端管理服務，就可以，若之前沒有雲端管理的帳號，請按【建立帳戶】系統會自動帶入申請機制，申請過的填寫帳號密碼「登入」，已經成功代管的說明如下：（圖 2-25）

圖 2-25 啟用中的雲端管理

- 【Server Address】：雲端管理伺服器的 IP 位址或是網域名稱。
- 【Server Port】：雲端管理伺服器跟 NG-UTM 溝通使用的 Port，預設是 TCP 2000。
- 【機器序號】：NG-UTM 的機器序號，這是唯一的號碼。
- 【最後連線時間】：NG-UTM 跟雲端管理伺服器最後一次溝通的時間。
- 【點此】：當 NG-UTM 未跟 Eyecloud 綁定下，點這一個連結，他會自動開啟管理者的瀏覽器，並將網址轉向 Eyecloud 的帳號登入頁面，此頁面可以讓管理者輸入已經申請過的 Eyecloud 帳號密碼或是新申請一個 Eyecloud 帳號跟密碼。

2-10-2、雲端管理

雲端管理的網址是 https://eyecloud.tw/，可以事先申請 Eyelcoud 的帳號，把設備託管到雲端，只要用一個 Eyecloud 帳號，就可管理多台的 NG-UTM。

1、在 https://eyecloud.tw/ ，建立新帳號（圖 2-26）

圖 2-26 建立「EyeCloud」帳戶

2、登入雲端管理系統後，新增托管的設備（圖 2-27）

圖 2-27 新增設備

3、管理托管的設備（圖 2-28）

圖 2-28 新增設備成功

在【訊息通知】>【通知項目】功能中（圖 2-29)

綠→橘：系統運作正常→ 正常連線，但設備狀態裡的其他設備 有狀態 是 變更為 off 的，例如: AP 或是交換器。

綠→黃 : 系統運作正常→ 10~20 分鐘沒有和 server 連線。

黃→紅: 10~20 分鐘沒有和 server 連線→ 20 分鐘以上沒有和 server 連線。

黃→橘: 10~20 分鐘沒有和 server 連線→ 正常連線，但設備狀態裡的其他設備是 off 的，例如: AP 或是交換器。

紅→綠: 20 以上沒有和 server 連線→ 系統運作正常。

紅→橘: 20 以上沒有和server 連線→ 正常連線，但設備狀態裡的其他設備 有狀態 是 off 的。

灰→綠: 從沒有和 server 連線過→ 系統運作正常

圖 2-29 設備狀態切換燈號解釋

解除綁定雲端管理服務

在【雲端管理服務】中點選「解除綁定」雲端管理服務，此台設備就會脫離雲端管理的機制。（圖 2-30)

圖 2-30 解除綁定雲端管理服務

就會出現此設備尚未與 EyeCloud 綁定。（圖 2-31)

圖 2-31 此設備尚未與 EyeCloud 綁訂

2-11、SSL 憑證設定

在網路傳輸資料仰賴 SSL 加密協議，NG-UTM 也是一樣，大量利用 SSL 協議，在 SSL 加密過程需要用到憑證去辨識真偽，一般而言，SSL 憑證有 Server 憑證、Root 憑證跟中繼憑證 ，不論跟合法憑證機構申請或是自己簽署的憑證，匯入操作端的電腦內，操作者的電腦就不會出現憑證錯誤的警示字眼。

2-11-1、SSL 憑證設定

憑證的來源有 3 個，一個是申請合法憑證並使用【匯入 SSL 憑證】的方式匯入，另一個在【SSL 憑證設定】選擇自行輸入，建立自己私有 SSL 憑證，最後一個是使用 Let's Encrypt 憑證，Let's Encrypt 憑證為免費發放合法憑證，但缺點是每 6 個月要重新更新一次。

1、自己私有 SSL 憑證

在【SSL 憑證設定】中選擇自行輸入，建立自己簽署的私有憑證，建立完成後可以下載並匯入操作者的電腦，則操作者的電腦就不會出現憑證錯誤的警告。以下是一個設定範例：

二碼國碼：TW

州/省別：L7FW

所在城市：TC

組織名稱：L7FW

單位名稱：L7FW

網站名稱：www.common.com

申請人員 Email：help@common.com

輸入完畢後，下載 server.csr 檔案，並將他匯入瀏覽器，則在瀏覽器的檢視憑證區可以看到下列資訊。（圖 2-32)

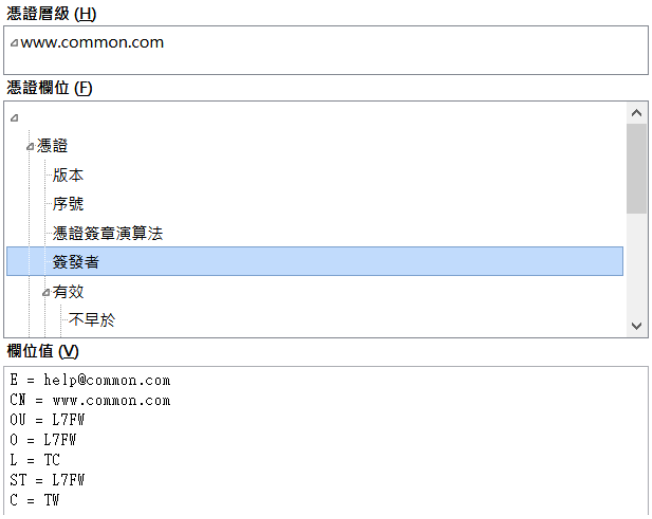


圖 2-32 檢視瀏覽器憑證

2、匯入 SSL 憑證

除了自己簽署的伺服器憑證外，也可以匯入跟外部簽署機構申請的憑證，這裡面就只有 Server 類型跟中繼憑證 2 種。

3、Let's Encrypt 憑證

Let's Encrypt 是合法的憑證發放單位，NG-UTM 可以把申請的動作簡化，管理者只要提出申請並在 DNS 伺服器上搭配設定就完成，Let's Encrypt 每次發放有效憑證時間為 6 個月，在憑證到期前自動延期。（圖 2-33)

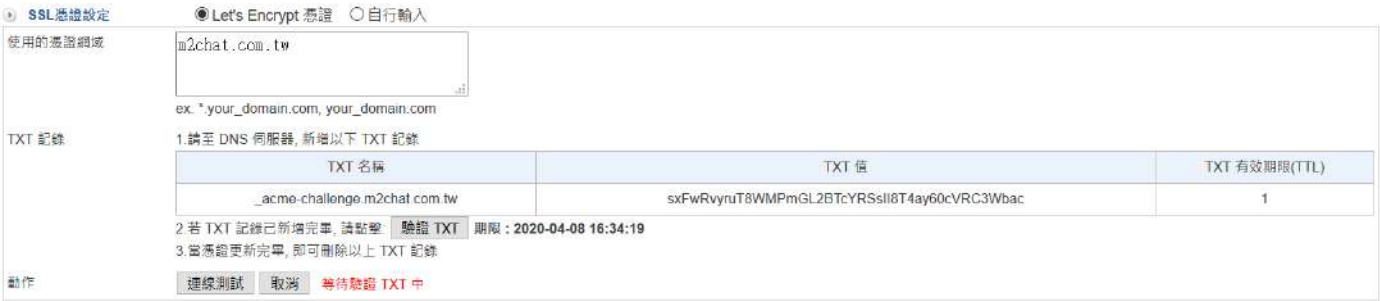


圖 2-33 申請憑證

- 【使用的憑證網域】：輸入申請的網域名稱，同時按下【申請憑證】系統就會自動向 Let's Encrypt 提出申請。
- 【TXT 紀錄】：申請成功後，Let's Encrypt 會送出（圖 2-33) TXT 值，管理者必須在 DNS 伺服器上加入一筆 TXT 紀錄，以上面範例 TXT 名稱為 _acme-challenge.m2chat.com.tw ，並在名稱上填入 TXT 值。

當 Let's Encrypt 驗證 TXT 後，合法憑證就能使用。

2-12、不斷電系統

為了避免 NG-UTM 因為臨時的斷電，導致主機板或是儲存媒體如硬碟等故障，造成設備的損毀，系統支援不斷電系統(UPS)，萬一停電後，且不斷電系統的電源低於設定值，系統會自動進入關機程序，保護裡面儲存的寶貴資料。

2-12-1、不斷電系統

NG-UTM 跟不斷電系統有 3 種連線方法，SNMP、USB 跟支援網路功能的 UPS 設備，採用 USB 跟支援網路功能的 UPS 連線時，系統會列出 ShareTech 驗證的廠牌跟型號，選擇 SNMP 則用 SNMP 協定跟 UPS 溝通。SNMP 目前支援 3 種協議分別是 SNMP v1 / v2c / v3 。管理者需要先在【連接模式】中選擇運作模式，每種運作模式的設定都不一樣。

1、USB 連接模式

USB 模式下，NG-UTM 還可以當不斷電設備跟其他設備的溝通媒介，把不斷電系統的資訊，透過網路的方式轉給網路上的設備使用。（圖 2-34)

圖 2-34 USB 連接設定

- 【型號】：選擇 UPS 的型號，共有 2 個選項，自動跟自訂。

  自動：系統自動跟設定的 IP 位址溝通，溝通後的型號會列在【UPS 資訊】中。

  自訂：從 ShareTech 驗證過的型號中選取，目前有 5 個 UPS 型號驗證過。

- 【電池低電量】：當電池的電量低於設定的比例，預設值是 80%，系統就會進入安全模式，此時會中斷對外備份的機制，並且在設定的分鐘數後進入關機程序。

- 【電池電量下限】：當不斷電系統的電池少於設定值，系統直接進入關機程序。

- 【若為高可用性模式下】：在 HA 模式下，通知另外一台設備要同步執行關機動作。

2、網路不斷電系統伺服器連接模式

- 【型號】：選擇 UPS 的型號，共有 2 個選項，自動跟自訂。

  自動：系統自動跟設定的 IP 位址溝通，溝通後的型號會列在【UPS 資訊】中。

  自訂：從 ShareTech 驗證過的型號中選取，目前有 5 個 UPS 型號驗證過。

- 【伺服器 IP 位址/埠號】：輸入不斷電系統的 IP 位址及埠號，系統會自動跟不斷電系統溝通。

- 【電池低電量】：當電池的電量低於設定的比例，預設值是 80%，系統就會進入安全模式，此時會中斷對外備份的機制，並且在設定的分鐘數後進入關機程序。

- 【電池電量下限】：當不斷電系統的電池少於設定值，系統直接進入關機程序。

- 【若為高可用性模式下】：在 HA 模式下，通知另外一台設備要同步執行關機動作。

3、SNMP v1 連接模式

- 【UPS 設備 IP】：輸入不斷電系統的 IP 位址及埠號，系統會使用 SNMP v1 協議 自動跟不斷電系統溝通，溝通後的訊息會出現在【UPS 資訊】中。

- 【電池低電量】：當電池的電量低於設定的比例，預設值是 80%，系統就會進入安全模式，此時會中斷對外備份的機制，並且在設定的分鐘數後進入關機程序。

- 【電池電量下限】：當不斷電系統的電池少於設定值，系統直接進入關機程序。

- 【若為高可用性模式下】：在 HA 模式下，通知另外一台設備要同步執行關機動作。

4、SNMP v2c 連接模式

- 【UPS 設備 IP】：輸入不斷電系統的 IP 位址及埠號。

- 【存取 SNMP 服務的帳號】：輸入不斷電系統設定的 SNMP v2c 帳號，系統會使用 SNMP v2c 協議自動跟不斷電系統溝通，溝通後的訊息會出現在【UPS 資訊】中。

- 【電池低電量】：當電池的電量低於設定的比例，預設值是 80%，系統就會進入安全模式，此時會中斷對外備份的機制，並且在設定的分鐘數後進入關機程序。

- 【電池電量下限】：當不斷電系統的電池少於設定值，系統直接進入關機程序。

- 【若為高可用性模式下】：在 HA 模式下，通知另外一台設備要同步執行關機動作。

5、SNMP v3 連接模式

- 【UPS 設備 IP】：輸入不斷電系統的 IP 位址及埠號。
- 【存取 SNMP 服務的帳號】：輸入不斷電系統設定的 SNMP v3 帳號，系統會使用 SNMP v3 協議自動跟不斷電系統溝通，溝通後的訊息會出現在【UPS 資訊】中。
- 【認證用密碼】：SNMPv3 驗證帳號時使用的密碼，驗證密碼的方式有 SHA 跟 MD5 2 種，這些資料都要跟 UPS 主機設置的一樣。
- 【傳輸用密鑰】：SNMPv3 在資料傳輸使用的加密密碼，加密模式有 DES 跟 AES 2 種，這些資料都要跟 UPS 主機設置的一樣。
- 【電池低電量】：當電池的電量低於設定的比例，預設值是 80%，系統就會進入安全模式，此時會中斷對外備份的機制，並且在設定的分鐘數後進入關機程序。
- 【電池電量下限】：當不斷電系統的電池少於設定值，系統直接進入關機程序。
- 【若為高可用性模式下】：在 HA 模式下，通知另外一台設備要同步執行關機動作。

網路不斷電系統伺服器

在 USB 及 SNMP 模式下，NG-UTM 還可以當不斷電設備跟其他設備的溝通媒介，把不斷電系統的資訊，透過網路的方式轉給網路上的設備使用。

- 【啟用】：預設不啟用這項功能，整台 UPS 只給本機使用。
- 【終端設備 IP 位址】：需要這項服務的設備端 IP 位址，當 UPS 低電量時發送通知給他。
- 【等待關機時間】：遠端設備關機需要多少時間？NG-UTM 會等待這個時間後才會進入關機程序。
- 【Ping Timeout】：NG-UTM 跟遠端設備用 ICMP (PING)的動作確認設備是否存活。

2-12-2、UPS 日誌

系統跟 UPS 溝通的紀錄都會存在這裡，包含時間記發生的事件。

2-13、CMS

CMS(Central Management System) 簡單來說，只要把中心端的設備設成 CMS Server 端，就可以管理所有外點的 NG-UTM。

CMS 跟雲端管理服務隨然都是提供類似的設備管理功能，運作上還是有點不一樣。

1、 CMS 需要中心端有固定 IP 位址或是用 DNS 的固定網名，他的目的是讓遠端的用戶端能夠找到伺服器端。

2、 CMS 的中心端需要有硬碟的 NG-UTM 設備。

3、 CMS 只能管理 NG-UTM，不能管理 ShareTech 的其他設備，例如，郵件伺服器。

ShareTech CMS 功能，具備遠端組態設定的必要功能：包括系統參數資料的備份、資料回存及設備韌體更新等，使中心端(總部)管理人員可以依照自己的需求或預設的排程來集中管理遠端多台設備，甚至透過 Log(日誌)功能更可詳實記錄所監控設備產品發生之相關事件(events)，追蹤設備的最新使用狀態。

CMS 系統的示意圖如下，（圖 2-35），每個地方的 NG-UTM 都會向總部彙整他目前的狀態、設定檔，總部的管理者就可以由總部的 NG-UTM 掌握到所有外點的即時狀態並可以介入管理。

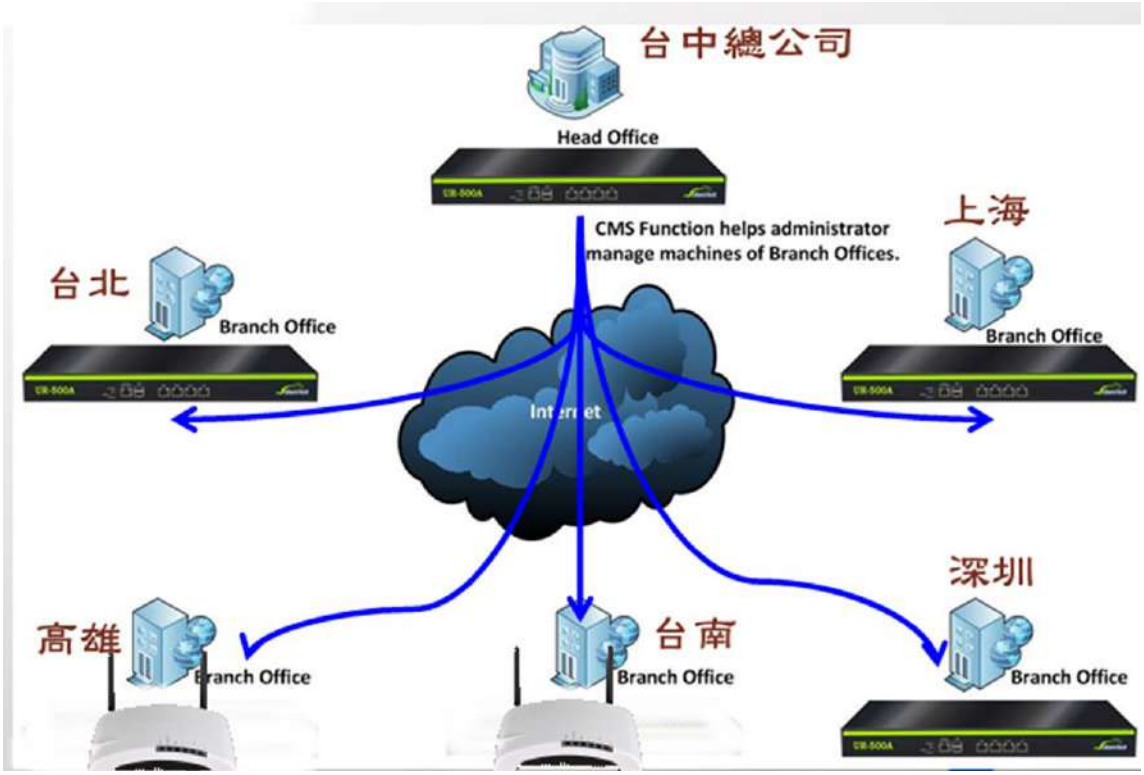


圖 2-35 CMS 示意圖

2-13-1、CMS 基本設定

每一台 UTM 防火牆的 CMS 系統都可以扮演成 Client 端或是 Server 端，如果本身沒有硬碟，則只能扮演成 Client 端。

簡單來說，CMS 運作原理相當簡單，設為 Client 端的設備定時會跟 Server 端傳送訊息並付予 Server 端管理權限。

1、設為 Client 端

當設備設為 Client 端，他會向 Server 端持續送出自己的狀態。

- 【啟用】：啟用 CMS 功能。
- 【模式】：CMS 運作模式是 Client 模式。
- 【伺服器】：CMS Server 端的域名或是 IP 位址，必須在網際網路上能夠找到的域名或是 IP 位址。範例是向 maxmax10.dyndns.org 的動態域名回報。
- 【名稱】：Client 端在 Server 端顯示的名稱，例如，UTM-台北。
- 【更新時間】：間隔多久向 Server 端更新資料，設定值為 1~ 30 分。
- 【管理者帳號】：Client 端賦予 Server 端的管理者權限，詳細的管理者權限請參照【系統設定】>【管理員】設定，Server 端的管理者就是用這個帳號登入 Client 端設備，若沒有指定管理者，則無法透過 CMS 進入管理介面。
- 【出口介面】：使用那個出口線路向 Server 端回報，系統會自動列出所有的出口線路讓管理者選擇。

2、設為 Server 端

此設備設定成 Server 端，會紀錄 Client 端送出資料，管理者只要管理 Server 端就可以管理所有的設備。

- 【啟用】：啟用 CMS 功能。
- 【模式】：CMS 運作模式是 Server 模式。

Client 設定檔自動備份至本機

當 CMS 的伺服器端，啟用定期備份 Client 的設定檔，備份的時間可以自訂週期，備份後，萬一 Client 故障或是設定錯誤，都可以透過 CMS 伺服器還原之前的設定。

- 【啟用】：啟用備份 Client 端設定檔功能。
- 【自動備份時間】：週期性的備份資料，週期性越短系統的負荷越大。
- 【備份保留數量】：備份的設定要存幾份，一般來說 5 份就已經足夠，份數越多佔的儲存空間越大。

2-13-2、CMS 監控狀態

1、接受 Client 端

每個 Client 端設定成功後對 CMS Server 端發送接管請求，Server 端的管理者需要選擇接受後，CMS Server 端才會開始處理這一個 Client 的資料。（圖 2-36)

圖 2-36 接受新的 Client 設定

2、管理 Client 端

每個 Client 可分成不同的群組，Server 端會即時地顯示目前設備的狀態，如下圖（圖 2-37)

圖 2-37 Client 列表

1、狀態：以顏色區分，代表 Client 端有定時地按照設定的時間跟 Server 端回報，橘色代表這個設備超過 3 次沒來回報資訊，紅色代表這個設備屬於斷線階段，灰色代表沒有任何更新的資料。

2、名稱：Client 端設定的名稱，預設是以 Client 端為主，但 Server 端可以依據自己的需求更改任何名稱。

3、型號：Client 端的型號。

4、IP：Client 端目前的 IP 位址。

5、即時監控：按下圖示之後，就可以利用 Client 端賦予的管理者權限，進入 Client 端的 WEB 管理畫面，空白代表 Client 端沒有授予 Server 端管理權限。

6、備份：目前儲存在 Server 端的設定檔備份份數，括弧內的就是份數，點選後就可以查看異動的資訊或是執行還原設定的動作。

7、自動備份：是否有啟動自動備份設定檔功能。

8、動作：修改/刪除 Client 端的設定。

9、紀錄：分成連線跟控制 2 個紀錄層次，連線是指 Client 端跟 Server 端的通聯紀錄，何時連線？何時斷線，控制是由 Server 端下了哪一些控制命令給 Client 端。

10、管理者可以按下【群組收合】的按鈕，即時地切換群組間的顯示訊息。

11、選定 Client 端後，按下【立即備份】按鈕，立刻執行備份的動作。

動作 -> 修改 Client 端資訊

當按下修改按鈕後，就可以修改 Client 端的顯示資訊。（圖 2-38)

1、型號 / MAC 位址： Client 端的型號及 MAC 位址，這 2 個訊息不能更改。

2、名稱：Client 端設定的名稱，預設是以 Client 端為主，但 Server 端可以依據自己的需求更改任何名稱。

3、群組：這個 Client 端是歸類在哪一個群組下，選擇已經建立的群組或是自訂，選擇自訂時，在後面的空格中填入要新增的群組名稱。

4、自動備份：是否要啟用自動備份設定檔功能。

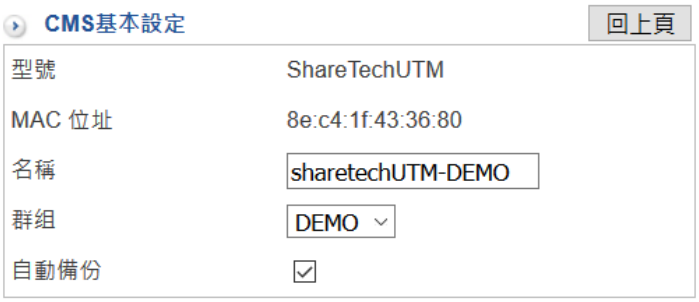


圖 2-38 修改 Client 資訊

備份-> 備份清單

CMS 系統最大的好處是可以自動且定時地將 Client 端設定檔備份下來。（圖 2-39)

1、備份時間： 何時備份這個設定檔。

2、軟體版本： Client 端備份時的版本。

3、下載：按下圖示後將這一個設定檔下載到本地端。

4、刪除：刪除這筆紀錄。

5、紀錄：這個備份檔是被修改了哪些設定。

備份時間	軟體版本	立即還原	下載	刪除	記錄
2020-04-06 21-00	9.0.2	還原			記錄
2020-04-06 19-00	9.0.2	還原			記錄

圖 2-39 備份 Client 的設定

備份 ->還原 Client 端

還原 Client 端的設定檔也是 CMS 系統的好處，他能夠快速地將 Client 端的設備還原到指定狀態，在還原時還可以指定時間執行。

1、到備份清單中選擇要還原的時間點備份下來的設定檔。

2、在【立即還原】按下【還原】按鈕，則 Server 端會將選擇備份的設定檔送到 Client 端設備。

第 3 章 網路設定

NG-UTM 並非傳統的 UTM 或是防火牆，他是以路由器為概念的 UTM，嚴格來說，它沒有防火牆的 LAN、DMZ 跟 WAN 等區別，取而代之的是 ZONE 對 ZONE 的管制，基本上，一個或是多個實體甚至虛擬的網路介面都可以組合成一個 ZONE，每一個 ZONE 進去或是出去的封包都可以執行防火牆的過濾條件。

在此章，會詳細介紹如何將一個或是多個實體網路介面甚至由 IP Tunnel 協定建立的虛擬網路介面組合成 ZONE，同時介紹如何把屬於 WAN 介面類型的 PPPOE 加入，當然屬於路由器的路由管理、VLAN 等也會說明。

3-1、區域設定

NG-UTM 預設會把 Eth0 標示為 ZONE 0，ZONE 0 跟 Eth0 的組合無法被管理者刪除，但可以把其他的實體 Port 加入 ZONE 0 中，Eth0 的預設 IPV4 的位址是 192.168.1.1。

任何一個 ZONE 有超過一個以上的實體 Port 組合時，此 ZONE 內的每一個實體 Port 會自動執行 Layer 2 的橋接器(Bridge)功能，可以很單純的想成就是一個 Switch，也就是說不需要任何設定，ZONE 內的任何 Port 彼此之間都是暢通無阻。

3-1-1、區域設定

列出目前每一個實體 Port 歸屬於哪一個 ZONE，並用顏色及數字區分，同一個 ZONE 它的顏色會一樣，當系統有任何 Port 不歸屬於任何 ZONE 時，管理者可以按下【新增區域】的按鈕，建立一個新的 ZONE，也可以在已經建立的 ZONE 中加入新的實體 Port。

如果要將某個實體 Port-X 從 ZONE 1 改成 ZONE 2，先要到 ZONE 1 把 Port-X 刪除，讓 Port-X 不屬於任何 ZONE，再到 ZONE 2 中加入 Port-X。

建立新的區域

如果有空的實體 Port 尚未被分配到 ZONE 中，管理者就可以新增加一個 ZONE，按下【新增區域】的按鈕，開始新增一個新的 ZONE。

- 【區域】：選擇新增 ZONE 的數字代號，系統以 ZONE 為前置代號，後面是數字，例如，ZONE 0、ZONE 1 ....，因為每一個實體 Port 都可以單獨成為一個 ZONE，所以最大的數字就代表此台設備擁有的實體 Port 數，挑選數字時可以任意選擇，不需要按照順序。
- 【名稱】：新增 ZONE 方便記憶的名稱，例如，會計、工程..等。
- 【顏色】：選擇 ZONE 的顏色。
- 【Port】：選擇 ZONE 的實體 Port，任何未標示數字的 Port 都可以選，也可以選擇多個 Port 組合成一個 ZONE。

選擇完畢後會回到區域列表中，NG-UTM 會把每一個區域、名稱、顏色及他擁有的實體 Port 標示出來，如果需要修改，則按下，就可以進入修改畫面，刪除則按，注意一下區域列表，只有 ZONE 0 沒有刪除的按鍵。（圖 3-1）

區域列表：（設定完成之後請點選儲存）

區域	名稱	顏色	Port	
zone0	zone0		06	
zone1	WAN		01,02	
zone2	工程		03	
zone3	LAN		04	
zone4	RD		05	

圖 3-1 區域列表

每一個 ZONE 就會出現在【網路設定】 > 【網路介面】的選單中，管理者可以針對這個 ZONE 進行網路設定。

3-1-2、線路設定

NG-UTM 的每一個 ZONE 都可以指定網卡速度，設定網卡速度有 2 個方式，一個是從【網路設定】>【區域設定】>【線路設定】 中設定，另一個進入設定的是從首頁上方的 【Port Information】，點選要設定的實體 Port 就可以調整網卡速度。

- 【區域】：這個 Port 隸屬於哪一個 ZONE。
- 【Port】：實體 Port 是在第幾個位置上。
- 【線路狀態】：目前這個 Port 有沒有連線，如果沒接任何設備，就會出現 Disconnect 字樣，正常連線則會出現 Connect 字樣。
- 【MAC 位址】：實體 Port 的 MAC 位址。
- 【Speed and Duplex Mode】：目前網卡跑的速度，及過去的連線狀態紀錄，管理者可以手動調整網卡速度，共有 10Mbps / 100Mbps / 1000Mbps ，全雙工或是半雙工等模式可以供選擇。

WAN 跟 ZONE 關係

管理建立 WAN 介面時，可以一個 ZONE(一個實體 Port)一個 WAN 線路的建置方式，也可以用一個 ZONE(一個實體 Port)外加 Switch 後接數個 WAN 線路 ，2 者差別是，前者可以詳細設定 WAN 進出的頻寬及管理，後者頻寬只能對介面管理，無法針對 ZONE 下的個別 WAN 線路設定上、下載頻寬管理。

3-2、網路介面

完成【網路設定】>【區域設定】後，所有建立的 ZONE 都會出現在【網路介面】的列表中，管理者可以開始設定 ZONE 的網路 IP 位址、連線速度等網路資訊。（圖 3-2）

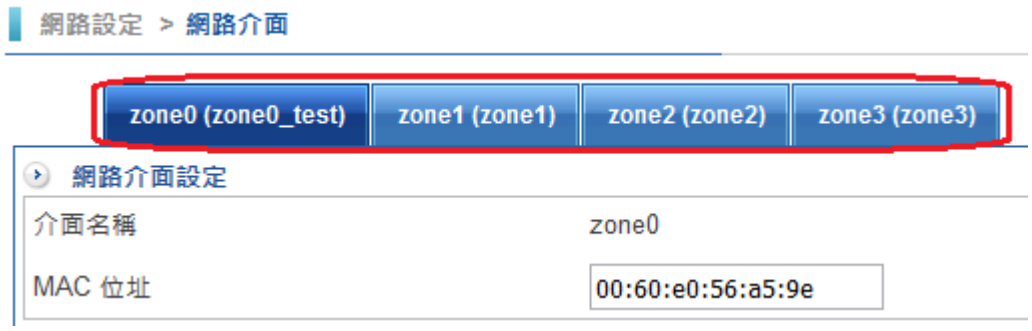


圖 3-2 在網路介面的區域列表

如前面所提，NG-UTM 會保留 ZONE 0 為預設的 ZONE，所以出現在第一個的就是 ZONE 0，其他新增的 ZONE 會按照當初給予的數字，依序排列在後方，點選上方的列表後，就可以進入網路設定。

NG-UTM 支援 SDN 控制器，除了預設的 ZONE 0 外，可以將新增加的 ZONE 交給 SDN 控制器管理，一但 ZONE 接受 SDN 控制器管理後，NG-UTM 就不會檢查這個 ZONE 內實體 Port 網路封包的傳遞， 但是當這個受 SDN 控制的 ZONE 封包要到其他 ZONE 時，NG-UTM 就會檢查封包並執行 Firewall 的工作。

網路介面設定

除了 ZONE0 外，每個 ZONE 的網路介面設定都相同，分別說明如下：（圖 3-3）

- 【介面名稱】：ZONE + 數字 組合，數字是在【區域設定】中選定。
- 【MAC 位址】：這個 ZONE 的唯一 MAC 位址，同一個 NG-UTM 管理的設備，MAC 位址不可以重複。
- 【啟用】：ZONE 0 預設是啟用狀態且不可以被關閉，其他新增加的 ZONE 有 3 個選項，關閉、STATIC 跟 DHCP。

  1、STATIC：介面的 IP 位址是在下面【介面位址 / PPPoE 撥接】新增，每個介面至少需要設定一組以上 IP 位址。

  2、DHCP：介面的 IP 位址是由 DHCP 伺服器配發，選擇後【介面位址 / PPPoE 撥接】的選項自動隱藏。
- 【MTU】：每一個封包最大的 byte 數，預設為 1500 ，設定範圍是 1400~1500。
- 【定義為外部網路】：為了簡化管理者對於 Zone 對 Zone 之間的封包流量方向，及對外路由的簡化設定，當這一個 Zone 都是對外線路的情況下，管理者可以勾選這一個項目，系統就會將預設路由往這一個 Zone 送。

  如果沒有勾選這個設定，當 NG-UTM 為閘道端設備時，管理者就要仔細的配置每一個來源 IP 位址的路由，不能有遺漏，否則就不知道往哪一邊送。

  ZONE 0 沒有這個選項。

圖 3-3 在網路介面設定

訪問控制

- 【啟用訪問】：ZONE 是否接受其他的 IP 位址查詢或是進入管理介面？共有 3 個選項，分別是 SNMP、Ping 跟 HTTPS。
- SNMP：ZONE 是否接受 SNMP 的查詢，接受後，此 ZONE 會把一些資訊，藉由 SNMP 協定送給遠端的 SNMP 伺服器。
- Ping：在 ZONE 設定的介面位址是否接受 ICMP 協定，勾選後，ZONE 上設定的 IP 位址會回應 ICMP 的封包。
- HTTPS：ZONE 是否接受 https 協定進入管理介面，勾選後，ZONE 上設定的 IP 位址都可以接受 https 服務。

防火牆防護設定

- 【防護項目】：ZONE 是否要接受防火牆的防護，啟用後，屬於這個 ZONE 上設定的介面 IP 位址，提供 SYN 攻擊、ICMP 攻擊、UDP 攻擊及 PortScan 等 4 種攻擊防護，點選 記錄 就可以查看過去駭客的攻防紀錄。

  SYN 攻擊、ICMP 攻擊、UDP 攻擊這三種的防護能力都可以在 【管理目標】>【防火牆功能】中設定，管理者可以啟用這四種的其中數種或是全部。

SDN 控制設定

NG-UTM 可以設定某一些實體 Port 成一個 ZONE 並把這個 ZONE 內網路封包的控制權交給 SDN 控制器，此設定會排除 ZONE 0 的 Eth0，將整台機器所有的實體 Port 交付給 SDN 控制器，這樣 NG-UTM 就會變成 SDN 交換器。

啟用 SDN 控制器的 ZONE 要注意，不可以在【介面位址】有綁定任何 IP 位址，否則無法啟用。

- 【簡易模式/進階模式】：2 種不同的運作模式切換，簡易模式單純設定控制器的 IP 位址及 Port 號後就可以運作，進階模式還可以區分 Out-band/In-band 的封包分別接給不同的 SDN 控制器，也可以指定多台的 SDN 控制器。
- 【啟用】： 如果介面位址有綁定 IP 位址，則無法啟用，點選啟用代表要將這個 ZONE 下的所有實體 Port 交由指定的 SDN 控制器管理。
- 【SDN 控制器模式】：在進階模式下，指定 ZONE 的 out-band 或是 in-band 要交給哪一台 SDN 控制器，可以設定成不同台的 SDN 控制器。
- 【SDN 控制器】：分成下列 2 種模式

  簡易模式：設定 SDN 控制器的 IP 位址跟 Port 號。

  進階模式：設定 SDN 控制器的 IP 位址跟 TCP Port 號，點選 ⊞ 就可以再增加第二筆 SDN 控制器。（圖 3-4）

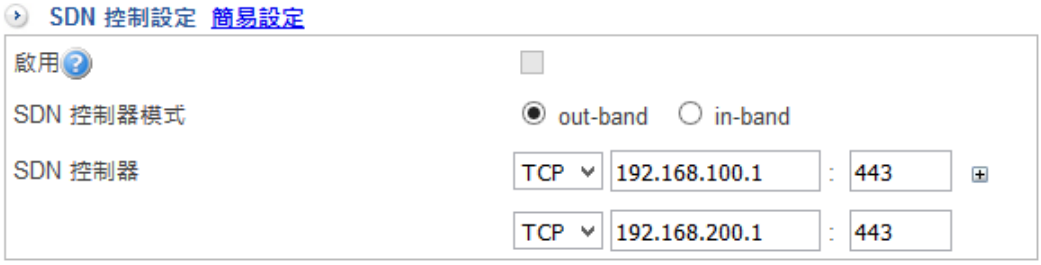


圖 3-4 SDN 控制器設定

Network Bonding 設定

NG-UTM 具有將 2 個網卡以上綁成一個網路介面的功能，這樣的好處是可以增加網路介面的頻寬，此技術就是 Network Bonding ，又可以稱之 Link aggregation、Trunking。目前支援 7 種模式，選擇適當的模式後就可以運作。

模式	名稱	說明
0	balance-rr	負載平衡模式(Round-robin policy)，依序由第一片網卡傳遞封包，就算其中一片網卡失效，也能確保網路不中斷，此功能需要交換器支援想同的機制。
1	active-backup	同一時間只有單一網卡運作，分為主要跟備援網卡，當主要斷線時由備援網卡接替，在這個模式下，不需要交換器支援。
2	balance-xor	用來源地址目的位址做 XOR 運算後傳遞，具備有負載平衡及容錯的機制。
3	broadcast	所有的網卡都會收到相同的封包，就算其中一個網卡掛了，仍可以正常運作。
4	802.3ad(LACP)	802.3ad 為交換器正式的連接聚合技術，需要交換器也支援相同的 802.3ad 功能才能運作。
5	balance-tlb	輸出的流量由主要網卡做負載平衡，輸入流量由 slave 的網卡負責，此模式不需要交換機配合。
6	balance-alb	輸出/入的流量由都做負載平衡，具備容錯機制，此模式不需要交換機配合。

Networking Bonding 啟用後需要對接交換器配合，才能讓整個機制正常運作。

介面位址 / PPPoE 撥接

定義每一個實體介面的 IP 位址，如果是 PPPoE 則會自動跳轉到 PPPoE 的設定畫面。（圖 3-5）

- 【型態】：有 2 種型態可以選擇，STATIC 跟 PPPoE，STATIC 則在下面的畫面中設定，PPPoE 則會跳轉到 PPPoE 的設定畫面，詳細請參考【網路設定】>【PPPoE 撥接】。
- 【名稱】： 容易辨識此介面的名稱，例如 Wan1:2。
- 【IP 位址】：ZONE 新增加一個 IP 位址，例如，192.168.1.1，設定後，此 IP 位址就會該 ZONE 的閘道器。
- 【網路遮罩】：IP 位址涵蓋的範圍，以一個 C 子網段為例，填入的為 255.255.255.0。
- 【預設閘道】：屬於 WAN 類型或是 ZONE 後面還有接其他的路由器，就需要填入閘道位址，內部類型 ZONE 沒有其他的路由設備就不需要。
- 【自動設定為出口線路】：就跟將 ZONE 定義成外部網路一樣的目的，這個選項為了降低管理路由上的便利，當勾選後，系統就會自動建一條出口線路的路由，任何沒有定義路由的封包將會從預設路由出去。
- 【管理 IP】：介面上的 IP 位址要不要讓管理者可以登入管理。

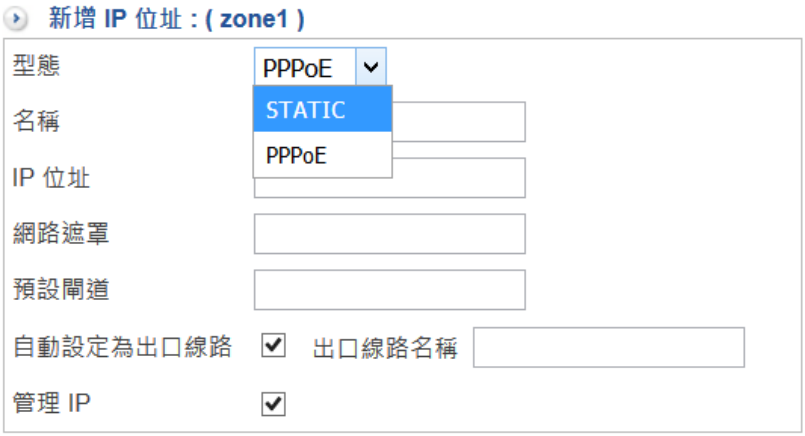


圖 3-5 網路介面 IP 位址設定

3-3、路由管理

管理者在【網路介面】>【介面位址】上設定 IP 位址跟子網路遮罩後，這筆資料就變成系統內定的路由，NG-UTM 會把所有的靜態路由表通通列出來，下圖是 IPV4 的靜態路由表。（圖 3-6）

	編號	名稱	目的網路	閘道	介面
	1	預設閘道	168.95.98.254/32		ppp4001
	2	系統內定	10.0.154.0/24		zone3.600
	3	系統內定	60.249.6.0/24		zone1
	4	系統內定	125.227.221.0/24		zone1
	5	系統內定	168.95.98.254/32		ppp4001
	6	ISP_Mail	192.168.18.0/24	192.168.195.18	zone0
	7	系統內定	192.168.186.0/24		zone2

圖 3-6 IPV4 的靜態路由表

點選主選單 MENU 上方的灰色按鈕 IPv6 ，將顯示跟設定切換到 IPV6 模式，NG-UTM 將整台設備關於 IP 顯示或是設定的模式切換到 IPV6 模式，此時就會出現 IPv4 IPv6 MENU 。

IPv4 代表目前顯示/設定的是 IPV4 的位址模式，IPv6 代表顯示/設定的是 IPV6 的位址模式。這 2 個按鈕適用於整個系統，在需要設定 IP 位址的地方，點選灰色的圖示，將會設定畫面切換成 IPV4 或是 IPV6 模式。

系統內定的路由表無法更改，要修改就需要從【網路介面】>【介面位址】上重新設定 IP 位址跟子網路遮罩，匯入跟匯出路由表限定是自行建立的路由表，系統內定的無法匯出跟匯入。

3-3-1、靜態路由

NG-UTM 除了由網路介面定義產生的內定的路由表外，可以自行加入靜態路由表，靜態路由可以指定在特定介面有效。

新增靜態路由

按下 ✚ 新增 鈕後，就開始新增靜態路由。（圖 3-7）

- 【名稱】：這個靜態路由方便記憶的名稱，例如，10 網段、預設閘道等。
- 【目的網路】：目的網路的任何一個 IP 位址，例如，10.10.10.1。
- 【網路遮罩】：目的網路的 IP 位址涵蓋的範圍，以一個 C 子網段為例，填入的為 255.255.255.0。
- 【閘道】：要往目的網路的閘道器位址。
- 【介面】：新增的路由表是要屬於哪一個介面， 在這裡用顏色區分不同的網路介面，分別是介面(ZONE)、IP 通道(IP Tunnel)、PPPoE 撥接介面、VLAN、PPTP 及 SSL VPN 等，下拉選單後，系統會列出所有已建立的介面讓管理者選擇。

圖 3-7 IPV4 新增靜態路由

如果指定介面，則這一筆路由將只會在他所屬的介面生效，若介面選擇為 NONE，路由設定將會對本機所有介面都有效，所有管理者建立的靜態路由表都可以匯出或是匯入。

3-3-2、出口線路

NG-UTM 可以把一個或是數個 ZONE 接上 WAN 的線路，如果要把 WAN 類型的線路、數據專線或是 MPLS 內部 VPN 類型的線路加在 NG-UTM 上，都需要在【出口線路】中設定，當有往外部傳輸的封包時 NG-UTM 才知道如何往下一個閘道器。

管理者事先建立數個【出口線路】後，可以把相同類型的【出口線路】綁定成一個【出口線路群組】，以 WAN 類型的【出口線路】來說，每一個【出口線路】就是一個 WAN 線路，把數個【出口線路】綁定成【出口線路群組】，就是執行線路負載平衡的工作。

1、出口線路

每一個提供網際網路連線的線路就是一個出口線路，在配置上有 2 種做法：

A、每個外線分配到一個 ZONE。

B、外部 ZONE 接一個 SWITCH，所有的外線都接到 SWITCH 上，此時就需要在【網路設定】>【網路介面】>【介面位址】上將所有外線提供的 IP 位址設定上去。

2 種方式各有優點，A 方式方便管理辨識線路及查找問題，B 方式可以接入大量的外線，超過 NG-UTM 本身 Port 的限制。

按下 ✚ 新增 鈕後，就開始新增一筆出口線路。（圖 3-8）

圖 3-8 WAN 類型的指定閘道設定

- 【名稱】：這個指定閘道方便記憶的名稱，例如，WAN-1、PPPOE-1 等。
- 【目的位址】：選填，要到這個目的網路的任何一個 IP 位址，如果沒有填入代表是 0.0.0.0/0 ，以 WAN 類型的線路來說，通常是空白。
- 【閘道】：必填，出口線路的閘道器位址。

- 【介面】：新增的出口線路是要屬於哪一個介面， 在這裡用顏色區分不同的網路介面，分別是實體網路(ZONE)、IP 通道(IP Tunnel)、PPPoE 撥接介面、VLAN、PPTP 及 SSL VPN 等，下拉選單後，系統會列出所有已建立的介面讓管理者選擇。

  【線路偵測方式】：當 ZONE 是 WAN 屬性時，會檢查線路是否斷線，檢查的方式有 2 種，ARP 或是 ICMP，每隔一段時間，NG-UTM 就會對【閘道】上設定的 IP 位址發送 ARP 或是 ICMP 封包，由對方伺服器的回應狀況判斷線路是否正常連線或是斷線，預設值為 ICMP，可以選擇 NONE，NG-UTM 就不會對閘道進行斷線的檢查，系統認為線路永遠都屬於暢通的狀態。

  當 WAN 的線路是 PPPOE，可以額外選用 PPPOE 的偵測模式，他會自動選用 DNS 方式跟 PPPOE Server 之間做線路存活測試。

- 【偵測來源 IP】：用哪一個 IP 位址當作來源 IP 位址執行線路偵測的工作，一般都是選擇這一條線路配發的 IP 位址。

- 【被偵測 IP 位址】：選填，偵測那一個目的 IP 位址判斷線路的存活，如果不填，系統預設使用出口線路配發的閘道器位址當作被偵測位址。

- 【偵測頻率】：多久時間發送一次檢查封包，預設值為 60 秒，設定的範圍是 1~999 秒。

- 【啟用備援】：當【出口線路】斷線時，把封包轉向備援的出口線路，讓【出口線路】的網路封包能夠正常的傳遞，備援的閘道可以設定 2 筆。

- 【備援閘道 1/2】：【出口線路】斷線時，封包會自動轉向備援的閘道，所謂備援的閘道就是另一個已經設定完成的【出口線路】，同時選擇備援閘道所在的 ZONE。

【啟用備援】的備援閘道功能跟【出口線路群組】所提供的線路負載平衡模式是不太相同，備援閘道沒有權重的觀念，且是指定式 1 對 1 或是 1 對 N 的備援模式，例如，原本的線路對外速度是 100Mbps，設定的備援閘道速度只有 10Mbps，原本的線路斷線後，所有 100Mbps 的網路封包都將全部塞往 10Mbps 的備援線路上，此時如果還有第 3 條線路，他並不會自動將封包轉往第 3 條線路上。

但是同樣情況在【出口線路群組】所提供的線路負載平衡上，可以依照設定的比重或是負載均衡模式，把 100Mbps 的網路封包，分配給有效的【出口線路】上，如果有三條以上的 WAN 類型線路時，可以善用【出口線路群組】。

在【出口線路】列表中，每一個 WAN 屬性的線路或是有啟用【線路偵測方式】的線路，都有斷線跟連線的紀錄可供查詢，點選 記錄 就可以查看過去的線路連線狀況，紀錄線路的斷線及連線時間。

3-3-3、出口線路群組

NG-UTM 提供線路負載平衡器的功能，把每一個【出口線路】都視為一個 WAN 類型的線路，再根據負載均衡的模式，依照權重設定，把網路封包平均分配到每一個線路中。

按下 ✚ 新增 鈕後，就開始新增一筆指定閘道群組，管理者可以根據實際的需求，設定多筆群組方便【管制條例】中選用。

- 【群組名稱】：這個出口線路群組方便記憶的名稱，例如，WAN-ALL、所有對外網路等。
- 【負載均衡模式】：網路封包的分配方式，共有四種模式可以選擇。

  1、Session：不管來源或是目的 IP 位址，按照 Session 比重分配，例如，A 線路比重 1 ，B 線路比重 2 ，則第 1 個 Session 送到 A，2/3 個送到 B，第 4 個在送到 A，以此類推。

  2、來源 IP：按照來源 IP 位址比重分配，例如，A 線路比重 1 ，B 線路比重 2 ，則同一個來源 IP 位址的第 1 個 Session 送到 A，2/3 個送到 B，第 4 個在送到 A，以此類推，不同來源 IP 位址的分配跟上面一樣。

  3、目的 IP：按照目的 IP 位址比重分配，例如，A 線路比重 1 ，B 線路比重 2 ，則到相同目的 IP 位址的第 1 個 Session 送到 A，2/3 個送到 B，第 4 個在送到 A，以此類推，每個不同目的 IP 位址的分配跟上面一樣。

  4、介面負載小優先選擇：根據的實際負載狀況分配網路封包，負載小者會分配到更多的網路封包。
- 【斷線偵測】：每隔幾秒偵測線路是否正常，作為切換線路的依據。
- 【出口線路】：這個群組使用的【出口線路】及其分配的比重，所有在【出口線路】中設定的閘道，都會出現在這裡，供管理者挑選設定。
- 【比重】：出口線路的負載能力，例如，【出口線路-A】設定的比重為 1，【出口線路-B】設定的比重為 10，NG-UTM 會先丟 1 個網路封包到【出口線路-A】後再丟 10 個網路封包到【出口線路-B】，第 12 個網路封包又往【出口線路-A】，以此類推。

3-3-4、預設閘道

當管理者沒有設定【出口線路】，在靜態路由中也沒有指定路由的目的 IP 位址，要到特定目的地的 IP 位址將無法被傳送，此目的 IP 位址將會被丟棄，為了避免這樣的情況發生，設定一個預設閘道給 NG-UTM，將所有沒有定義路由的目的 IP 位址，通通往這一個預設閘道。

在【網路設定】>【網路介面】>【網路介面設定】中勾選【定義為外部網路】，則他就是系統的預設閘道。在多條線路接到同一個 ZONE 的配置下，雖然已勾選【定義為外部網路】，管理者需要先到【出口線路】設定哪一條線路適預設閘道。

除了預設閘道，在 多 WAN 的環境，可以在設定備用閘道，當預設閘道斷線，會自動切到備用閘道上。

- 【偵測頻率】：每隔幾秒鐘，系統會偵測預設閘道是否存在，預設值為 10 秒。
- 【預設閘道 IP】：預設閘道的 IP 位址，所有沒被路由表定義的目的 IP 位址，通通往這個閘道。
- 【介面】：預設閘道屬於哪一個介面，系統會列出所有的介面讓管理者選擇。
- 【指定上網 IP】：當介面有很多個 IP 位址，用哪一個當作 NAT 位址轉換的 IP，可使用介面設定的 IP 位址或是自己定義。（圖 3-9）

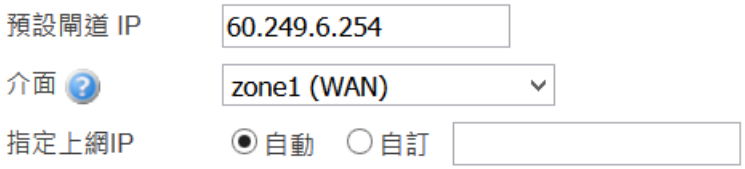


圖 3-9 預設閘道

3-3-5、動態路由

NG-UTM 支援 RIP 動態路由協議，只要指定介面跟路由周期，就可以將所有的路由協議學習起來，提供給系統使用。

- 【介面】：哪幾個實體介面要啟用 RIP 協議，可以多選。
- 【路由更新週期】：路由表更新的間隔時間，預設 30 秒，設定範圍 30-3600 秒。
- 【路由逾時設定】：超過多少時間算逾時，預設是 180 秒，設定範圍 30-3600 秒。

學習到的路由表會列在動態路由列表中。

3-4、VLAN(802.1Q)

VLAN 802.1Q 在交換器上是一個很基本的功能，他能把內部網路切割成數個獨立的子網段，每一個網段獨立運作互不相干擾，用實際的範例說明 VLAN 運作，如（圖 3-10），Switch-A 分別接了 3 個網段，192.168.1.0/24、192.168.2.0/24 跟 192.168.3.0/24， 在 Switch-A 設定 3 個不同的 VLAN ID，分別是 10、20 跟 30，這 3 個不同 VLAN ID 的電腦在 Switch-A 或是更上層的網路設備沒有設定路由之前，彼此是無法互通，同一個 VLAN ID 的電腦是可以互通。

當網路封包從 Switch-A 往上送到 NG-UTM 時，NG-UTM 就需要拆解及組合這些帶 VLAN ID 的網路封包，才會知道他下一個目的地是哪裡，如何拆解 VLAN ID 的設定就在此章節。

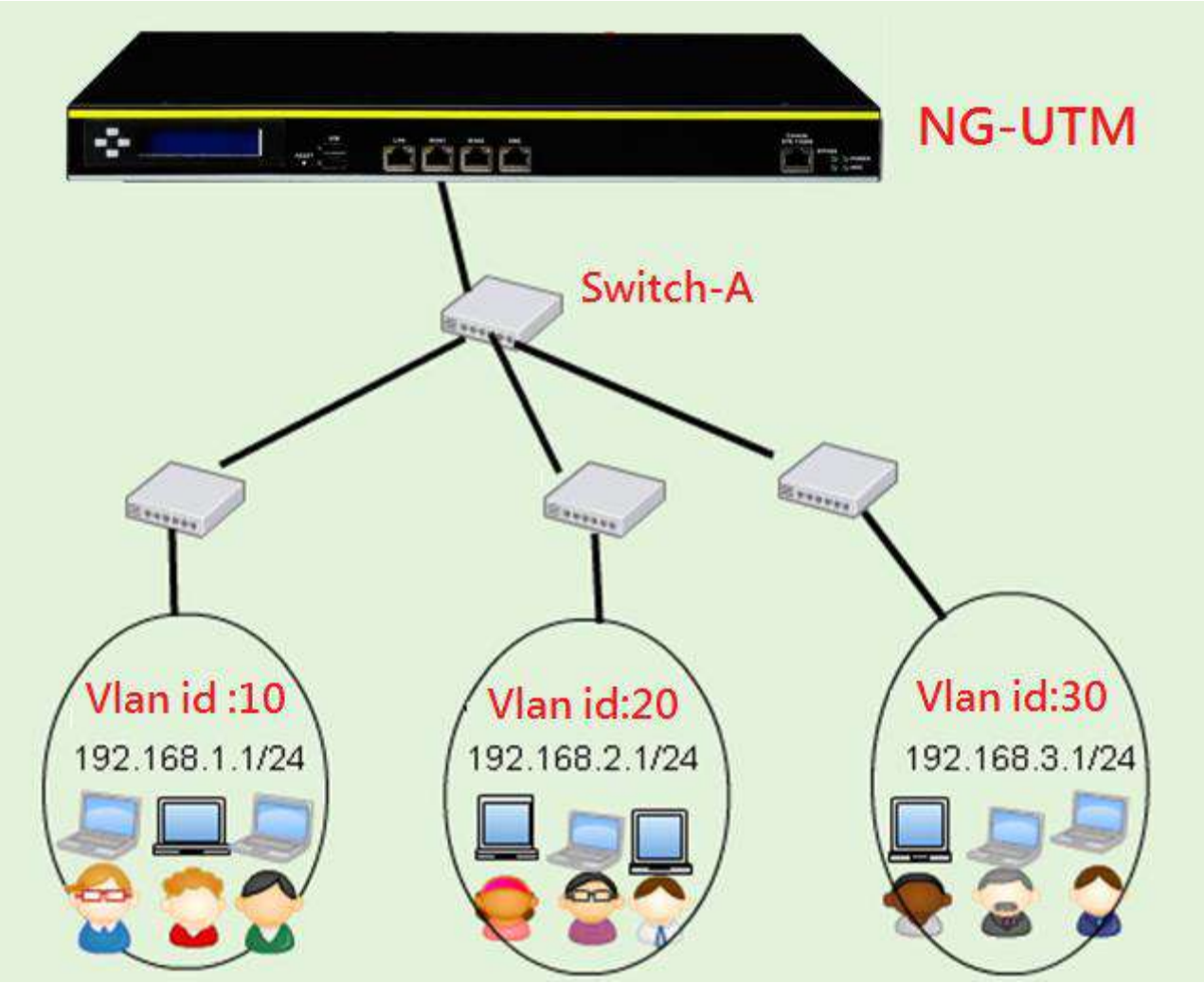


圖 3-10 VLAN 範例

NG-UTM 最高支援 4064 個 VLAN ID。

3-4-1、VLAN(802.1Q)

按下 ✚ 新增 鈕後，就開始新增 VLAN，在新增加之前，要先確認所屬的交換器目前已經配置相同的 VLAN ID 跟網路區段，網路區段可以包含 IPV4 或是 IPV6 的位址，如果這 2 個資訊無法跟對接的交換器互相符合，設定後網路封包無法正常的被拆裝及組合，網路就會不通。（圖 3-11）

- 【介面名稱】：系統預設 VLAN 的名稱就是 VLAN，無法更改，用 ID 分辨每個不同的 VLAN。
- 【啟動】：要不要啟用這個 VLAN ID？管理者可預先設定 VLAN ID，再藉由啟動功能決定要不要啟用這個 VLAN。
- 【介面】：新設的 VLAN 隸屬於哪一個區域(ZONE)，NG-UTM 會把所有的區域列出，讓管理者挑選。
- 【MTU】：每一個封包最大的 byte 數，預設為 1500 ，設定範圍是 1400~1500。
- 【VLAN ID】：給這 VLAN 一個跟別人不一樣的數字，同一台 NG-UTM 的 VLAN ID 不可以重複，數字範圍是 1~4064。
- 【IP 位址】：VLAN ID 下包含的網路 IP 位址及區段，每行一個 IP 區段，IPV4 位址跟 IPV6 位址可以同時填入。

  範例：

  192.168.1.0/24

  2001:b030:9999:abcd::1111/64

- 【訪問控制】：此 VLAN ID 的介面位址是否接受 SNMP 查詢跟 ICMP 回應，預設都是關閉。

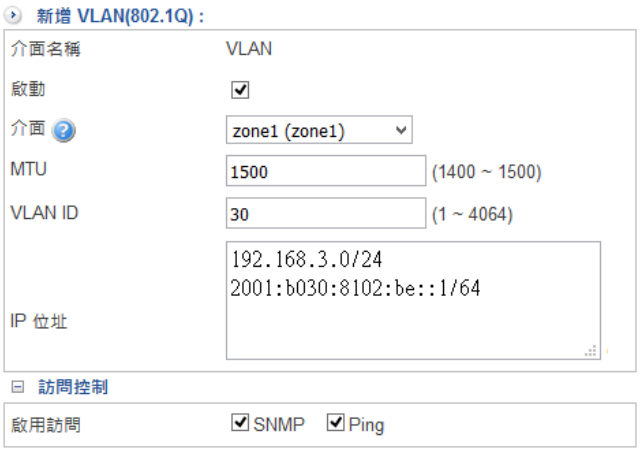


圖 3-11 VLAN 設定範例

設定完成 VLAN ID 跟網路區段後，NG-UTM 會把所有的 VLAN ID 跟所屬的 IP 位址列表出來，同時有一個起動與否的狀態顯示，出現 代表這一個 VLAN ID 目前是啟用中，出現 代表這一個 VLAN ID 目前是暫停，點選要修改的 VLAN ID 後，勾選【啟動】與否，就可以改變他的狀態。

設定完成後，NG-UTM 的介面就能夠把下層交換器的 VLAN ID 接收進來，把它拆解後根據路由設定把網路封包送到目的網路，同樣的從目的網路收到的網路封包也透過 VLAN ID 的組合送到對應的 VLAN 去。

3-5、PPPoE 撥接

在 WAN 類型的連線中，PPPoE 是很常見的撥號方式，NG-UTM 支援標準的 PPPoE 功能，不論是相同 ZONE 或是不同 ZONE 下，每一個 ZONE 都可以設定多筆 PPPoE 帳號。

按下 ✚ 新增 鈕後，就開始新增 PPPoE 帳號，在新增加之前，要先準備好 PPPoE 的帳號跟密碼，同時確認 PPPoE 線路是接在哪一個 ZONE 跟 Port 上，NG-UTM 目前支援最多 9 個 PPPoE 帳號撥接。（圖 3-12）

圖 3-12 PPPoE 範例

- 【介面名稱】：系統預設 PPPoE 撥接的名稱為 pppoe，管理者可以自行選擇 4001~4009 中任何一個數字，組合後就是 ppp4001~ppp4009，如果沒有按照命名規則，這個 PPPoE 帳號會無法正常使用。
- 【啟動】：要不要啟用這個 PPPoE 帳號？管理者可預先設定 PPPoE 帳號，再藉由啟動功能決定要不要啟用這個 PPPoE 帳號。
- 【撥接介面】：新設的 PPPoE 帳號隸屬於哪一個區域(ZONE)，NG-UTM 會把所有的定義好的區域列出，讓管理者挑選。
- 【帳號】：PPPoE 的帳號，例如，75139012@hinet.net。
- 【密碼】：PPPoE 的密碼，請注意大小寫。
- 【IPV6】：PPPoE 帳號是否有提供 IPV6 的分配模式，預設沒勾選，PPPoE 撥接只會取得 IPV4 的 IP 位址。
- 【自動新增】：在 PPPoE 模式下，為簡化設定，勾選【出口線路】跟【預設閘道】這 2 個選項後，系統會自動將它加入，就不需要再到這 2 個地方設定。

- 【線路偵測方式】：當 ZONE 是 WAN 屬性時，必須要檢查線路是否斷線，檢查的方式有 2 種，DNS 或是 ICMP，每隔一段時間，NG-UTM 就會對【被偵測伺服器 IP 位址】上設定的 IP 發送 DNS 或是 ICMP 封包，由對方伺服器的回應狀況判斷線路是否正常連線或是斷線。

  預設值為 NONE，所有的檢查過程都會紀錄下來，點選 PPPoE 帳號列表的 記錄 就可以查看過去的 PPPoE 撥接成功後，線路是否暢通與否。

- 【訪問控制】：此 VLAN ID 的介面位址是否接受 SNMP 查詢、ICMP 回應跟管理介面登入，預設都是關閉。

- 【防護項目】：這個介面要不要啟用防火牆的防護，確保不被攻擊 。

PPPoE 帳號列表中，在【啟動】欄中，出現 代表這一個 PPPoE 目前是啟用中，出現 代表這一個 PPPoE 目前是暫停，分別點選上述的圖示，就直接更改成【啟動】或是【關閉】。在【連線狀態】欄中，出現 代表撥接成功，失敗則會用 代表。（圖 3-13）

【線路偵測】跟【紀錄】欄中的 記錄 圖示，分別代表不同的紀錄資訊，【線路偵測】是 PPPoE 撥接成功後，跟網際網路的連線是否正常，【紀錄】是指 PPPoE 帳號是否能正常通過遠端 PPPoE 伺服器的認證。

PPPoE 撥接 列表

	名稱	介面名稱	啟動	撥接介面	帳號	IPv6	IP / MASK	遠端位址	連線狀態	連線時間	統計(tx/rx)	重新撥接	線路偵測	紀錄
☐	ppp4001	ppp4001	▶	zone1	75139012@hinet.net	✔	[redacted]167.123/32	168.95.98.254		12:32:53	10.46M / 73.92M	Reconnect	記錄	記錄
☐	pppoe_dynic	ppp4002	▶	zone1	75139012@hinet.net	✘	[redacted]178.12/32	168.95.98.254		1days 13:17:01	198.53M / 1.45G	Reconnect	記錄	記錄

圖 3-13 PPPoE 帳號列表

3-6、IP Tunnel

IP Tunnel 是 NG-UTM 非常特殊的功能，除了 2 台 NG-UTM 間可以透過 IP Tunnel 建立 VPN 網路外，也可以跟其他的有支援 IP Tunnel 協定的閘道器建立 IP Tunnel ，跟其他閘道器不一樣的是當 IP Tunnel 建立後，NG-UTM 還可以針對這些 Tunnel 內封包進行管制，例如，Web、SMTP 跟 POP3 可以進入 Tunnel ，其他的封包都會被拒絕。

IP Tunnel 的運作情境

參考下圖的網路架構，NG-UTM 佈署在中心端，掌管整個網路的對外連線，具有 IP Tunnel 功能的 Gateway 或是 Firewall 佈署在分點，基本的要求是分點的 POS 機或是電腦能夠安全的存取中心端的伺服器資源，例如、會計、ERP 系統等。（圖 3-14）

用 IP Tunnel 就可以快速的建立及佈署這樣需求的網路架構，在 NG-UTM 上更可以管制每一個分點的那一個應用程式可以上 Internet 或是內部網路，非這一個應用程式的服務都會被拒絕。集中管理的好處是管理者只要控制一台 NG-UTM 就可以掌握整個網路動態，因為所有的網路封包，包含中心端跟所有分點，都會經過它。

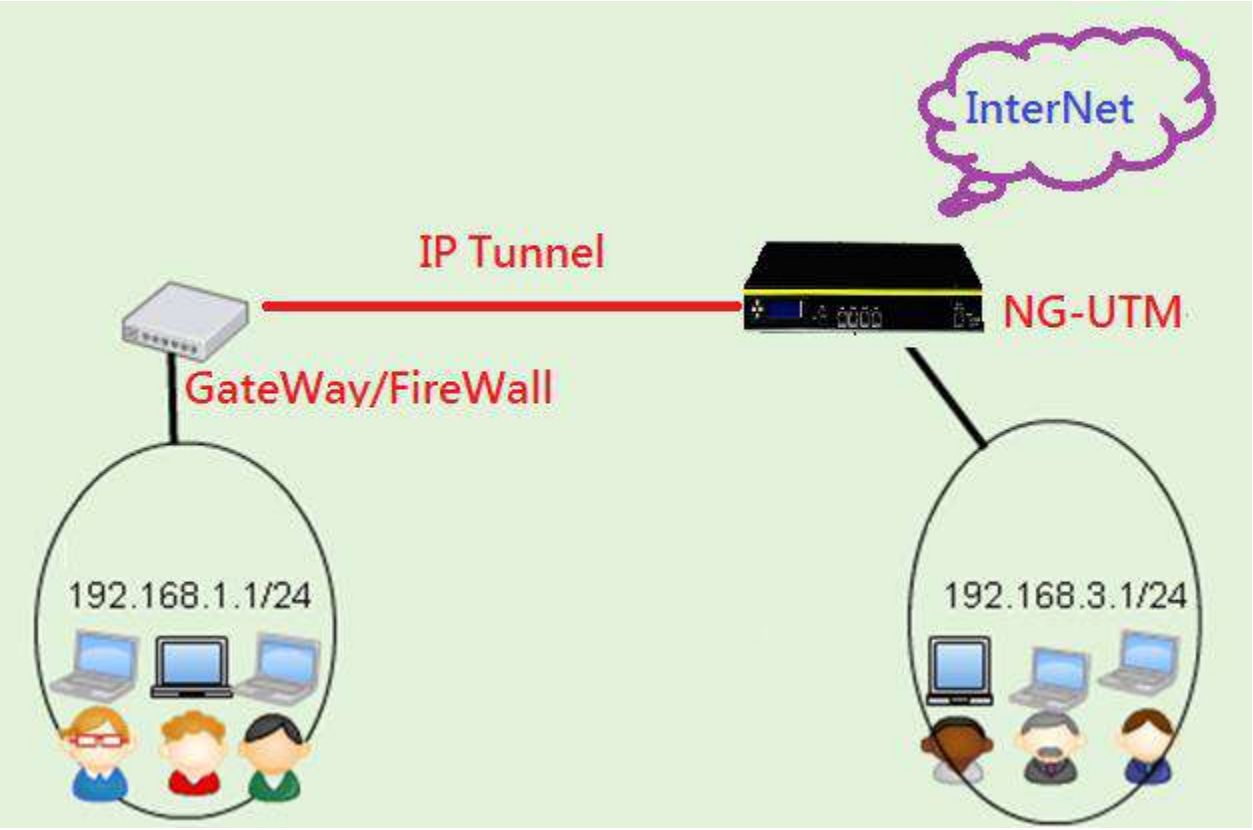


圖 3-14 IP Tunnel 運作示意圖

建立一條新的 IP Tunnel

每建立一筆 IP Tunnel ，系統會自動增加一個虛擬網路介面，類似實體 Port 的介面名稱是 Eth0、Eth1，預設的虛擬網路介面名稱為 tunl+數字，如 tunl1、tunl2，數字是系統自動加入，會從 1 開始編號，因此第一筆建立的 IP Tunnel 介面名稱就是 tunl1，第二筆就是 tunl2。

建立完成後，預設的靜態路由也自動建立，在【網路設定】>【路由管理】>【靜態路由】中就會出現一筆新的靜態路由，同時標註他的介面名稱為 tunl+數字。

也可以在【網路設定】>【路由管理】>【出口線路】中指定一個閘道，如果 NG-UTM 要當 IP Tunnel 的 Client 端，也就是要利用遠端的 IP Tunnel 上網，則需要建立【出口線路】，並在管制條例中指定哪一些服務要透過這一個 IP Tunnel 上網。

按下 新增 鈕後，就開始新增 IP Tunnel，在新增加之前，要先準備對方的 WAN IP 位址及 Tunnel 的區段。（圖 3-15）

- 【通道名稱】：任何容易辨識這個 IP Tunnel 的名稱。
- 【啟動】：要不要啟用這個 IP Tunnel ，管理者可預先設定 IP Tunnel，再藉由啟動功能決定要不要啟用這個 IP Tunnel。
- 【加密模式】：IP Tunnel 內要不要啟用加密功能，如果有啟用，每一個經過通道的封包再一次執行加密動作，共有 3 種可以選擇。

  1、NONE：IP Tunnel 不執行加密功能。

  2、GRE：IP Tunnel 用 GRE 加密 KEY 進行加解密動作。

  3、IPSEC：IP Tunnel 用 IPSEC 加密 KEY 進行加解密動作，管理者可以選擇加密的強度是 256 bit 還是 128 bit。
- 【遠地端位址】：跟 NG-UTM 建立 IP Tunnel 的遠端 IP 位址，例如：5.5.5.5。
- 【本地端位址】：NG-UTM 建立 IP Tunnel 使用的 IP 位址，這個位址需要屬於本機管轄，一般而言，在【網路設定】>【網路介面】中網路介面上有綁定的實體 Port IP 位址，例如：192.168.189.169。
- 【通道介面位址】： IP Tunnel 對內部的閘道位址，當封包被送到這個閘道位址後，會自動透過 IP Tunnel 轉到另一端。
- 【被偵測 IP 位址】：確保 IP Tunnel 的暢通，系統會自動偵測線路的斷線與否，這裡就是填入被偵測的 IP，通常是通道另一端的閘道位址。
- 【偵測頻率】：每隔多少秒執行線路偵測動作，可以設置 1-999 秒。

- 【加密格式】：選用 IPSEC 為加密協定時才會出現，有 2 種模式可以選擇。

  1、高安全：採用 AES 256 bit 為加密機制。

  2、低安全：採用 AES 128 bit 為加密機制。

- 【KEY】：GRE 跟 IPSEC 加密時，通道雙方預先設置的加密密碼，可以任何英文字母跟數字的組合。

- 【MTU】：每一個封包最大的 byte 數，預設為 1480 ，設定範圍是 1400~1500，這個預設值會比【網路設定】上預設的 1500 少，因為 IP Tunnel 需要額外的封包表頭，如果設成 1500Byte ，在加入 IP Tunnel 的表頭後，就會超過網路設定上的 MTU，導致這個封包無法傳遞成功。

圖 3-15 建立一個 IP Tunnel

3-7、中斷設定

NG-UTM 使用的 CPU 都是多核心的架構，本身提供的服務眾多，每一種服務跟網路介面的流量又都不一樣。預設上，系統會自動分配 CPU 資源給每一個服務，但是在某一些網路介面流量特別大的情況下，使用自動分配 CPU 資源的反而讓忙碌的 CPU 更忙碌，空閒的 CPU 更空閒，為了避免這樣的情況，NG-UTM 提供管理者 CPU 中斷服務，可以調整系統資源。

設定後可以到【系統狀態】>【系統狀態】>【CPU 負載】觀看每一個 CPU 的即時負載。

3-7-1、硬體中斷設定

根據實體介面的中斷要求，分配 CPU 資源，例如每一個網卡的 TX/RX 發出中斷要求時，就分配特定的 CPU 服務。（圖 3-16）

	CPU0	CPU1	CPU2	CPU3
Port01（zone1）	☐	☑	☑	☑
Port01-TxRx-0（zone1）	☐	☑	☑	☑
Port01-TxRx-1（zone1）	☐	☑	☑	☑
Port01-TxRx-2（zone1）	☐	☑	☑	☑
Port01-TxRx-3（zone1）	☐	☑	☑	☑

圖 3-16 CPU 硬體中斷

3-7-2、軟體中斷設定

用已經定義成 Zone 的介面分配 CPU 資源，他跟硬體中斷最大不同是同一個 Zone 內可能有好幾個實體 Port。（圖 3-17）

	CPU0	CPU1	CPU2	CPU3
zone0_rx-0	☑	☐	☐	☐
zone0_rx-1	☐	☑	☐	☐
zone0_rx-2	☐	☐	☑	☐
zone0_rx-3	☐	☐	☐	☑

圖 3-17 CPU 軟體中斷

第 4 章 管制條例

管制條例是整個 NG-UTM 的精隨，每一個進出 NG-UTM 的網路封包，除了劃分給 SDN 控制器管理的實體 Port 外，通通在這裡控制，甚至包含 IPSec VPN 通道、IP Tunnel 、PPTP 跟 SSL VPN 等加密的通道，也都是在這裡控制。

NG-UTM 以安全管理為首要目的，預設值「外對內、內對外」是無法連線，須於系統上設定特定條例--外對內或內對外後才可對外連線。

每一個封包進出介面時，會從第一條逐條比對是否符合管制規則，當封包的條件符合某條管制規則時，就會按該管制規則的設定，是讓它通過還是丟掉，如果選擇是它通過跟丟掉，則不會再向下檢查其他的管制規則。

當封包比對到最後一條管制規則時，仍然無法符合任何管制規則時，該封包就會被丟掉。

因為封包的比對是從第一條管制規則開始逐條比對，所以條例的先後順序就會影響整個運作，管理者在設定時必須要確認想管制的目標是否有進入相對應的管制規則中，NG-UTM 提供封包的通聯跟統計機制，通聯記錄讓管理者可驗證封包是否在符合管制規則時進入或者出去，只要點選此條管制規則上的統計，NG-UTM 就會把這個條例所有的進出封包開啟新視窗顯示。

每一條管制規則包含 3 個部分『基本設定』、『進階設定』與『防護設定』，整個管制規則用語言解釋如下：

基本設定：哪些人從哪裡來，走哪一條路到哪裡。

進階設定：檢查攜帶的東西。

防護設定：要不要保鏢保護。

對於 IPSec VPN 通道來說，應用在 Site-to-Site VPN 場景，所以管制規則相對來說簡單一些，只包含 2 個部分，『基本設定』與『進階設定』。

4-1、管制規則

一進入管制規則，NG-UTM 會把目前已經建立完成的管制規則列出來，預設會顯示每一個介面的所有管制規則，每一頁共會顯示 16 條條例，管理者可以指定想要查看的介面，則顯示的管理規則就只有來自該介面。

管制規則有 3 個頁籤，分別是 Outgoing、Incoming 跟 Advance，分成這 3 種單純簡化管理者設定的複雜度及方便閱讀與修改，每個頁籤的說明如下：

Outgoing ：內部對外部的管制規則，在 IP 位址轉換時只有 Routing 跟 NAT 可以選擇，Routing 是用在 ZONE 對 ZONE 才會用到，一般上網通常使用 NAT 模式。

Incoming：外部對內部的管制規則，在 IP 位址轉換時只有 IP 對應、Port 對應跟伺服器對應，這些對應機制都是要將封包導入內部時會用到。

Advance：進階版的管制規則，沒有內外之分由管理者決定封包的進、出規則，在 IP 位址轉換時就有所有的規則可以選擇，包含 Routing、NAT、IP 對應、Port 對應跟伺服器對應，因為它最強大同時也最複雜。

當頁籤中的管制規則有衝突時，優先權如下，簡單來說，Advance 的優先權是最高的。

內部出去的規則：Advance > Outgoing
外部進入的規則：Advance > Incoming

圖示說明

在管制規則上，會用圖示說明該條條例執行的工作，方便管理者快速辨識，圖示的說明如下：

圖 示	名 稱	說　明
	頻寬管理	頻寬管理功能已開啟。
	時間排程	啟動時間表，在設定時間範圍內自動執行條例。
	URL 管制	URL 管制功能已開啟。
	應用程式	管理哪一些應用程式，如 web、ftp、skype 等。
	掃毒管制	WEB、FTP 掃毒。
	認證	需登入帳號、密碼，才可上網連線。
	IPS	入侵偵測防禦。
	紀錄管制	HTTP、郵件的紀錄。
	電子白板	使用者必須看過電子白板的內容。
	指定閘道	從哪一個閘道走。
	防護	啟用防火牆防護。
ANY	任何協議	任何協議包含 tcp/udp/icmp 等。
TCP	tcp	tcp 通訊協議。
UDP	udp	udp 通訊協議。
ICMP	icmp	icmp 通訊協議。
	允許	NAT 運作模式，允許符合該管制條例的封包進出。

	拒絕	拒絕符合該管制條例的封包進出。
	暫停	暫停該管制條例的運作。
	啟動	啟動該管制條例的運作。
	修改	修改該管制條例的內容。
	刪除	刪除該管制條例。

管制規則顯示頁面說明

進入管制規則時，NG-UTM 會列出所有的管制規則，IPV4 跟 IPV6 的管制規則也是分開列出，預設 NG-UTM 是列出 IPV4 的管制規則，如果要切換成 IPV6 的管制規則，則在主選單上方 IPv4 IPv6 MENU 點選 IPV6，整個管制規則就會切換成 IPV6 模式，不論 IPV4 或是 IPV6 在這個頁面可讓管理者調整的項目如下：（圖 4-1）

圖 4-1 管制規則列表

- 【優先權】：NG-UTM 會從第一條 IPSec 管制規則開始執行，所以比對順序對於網路封包的通過與否有關鍵性的影響，選擇要變化優先權的管制規則並選擇數字，則此條管制規則就會插入成為選擇的優先權，例如，原本第 5 優先權的管制規則要變成第 2，在優先權上選擇 2 ，第 5 條規則就會變成第 2 條，原本的第 2 優先權管制規則就會變成第 3，以此類推。
- 【啟用】：管制規則的暫停跟啟用按鈕，管理者點選這個圖示後可以將原本啟用的管制規則暫停，原本是暫停的變成啟用。
- 【NAT】：IP 位址轉換的運作模式，空白代表 Routing 模式，DST 代表 Port 對應 ， SRC 代表 IP 對應。
- 【進階設定】：管制規則套用的進階管制項目。
- 【編輯/刪除】：修改或是刪除此條管制規則。
- 【統計】：每條管制規則進出的封包數量跟流量，暫停跟重新啟用都會把數值歸零，點選數字後，會出現符合這一個規則的所有網路封包詳細的進出記錄。

  設定管制規則後，可藉由此功能觀察封包是否進入規則中。
- 【更新】：立即更新管制條例的列表。
- 【刪除所有規則】：把所有的管制規則刪除，回到 NG-UTM 初始的狀態。

- 【計數器歸零】：把所有管制規則上【統計】欄位的數字通通歸零，重新計算。
- 【顯示來源網路介面】：選擇要查看的網路介面中管制規則，網路介面包含實體網路介面(ZONE 0，1..)、PPPoE、IP Tunnel、PPTP 跟 SSL VPN。預設觀看全部的網路介面。

當管理者在找尋網路問題時，設定的目標是否有進入管制規則中，此時就可以利用 NG-UTM 提供的網路封包即時通聯功能，點選管制規則上【統計】欄位的數字，NG-UTM 會把進出的網路封包擷取並開啟一個新的視窗讓管理者觀察。（圖 4-2）

- 【自動更新】：NG-UTM 每隔 3~30 秒，就會自動更新封包的通聯記錄，方便管理者觀察。
- 【清除】：把通聯記錄的資料全部清除掉，重新記錄跟顯示。
- 【時間】：封包通過的時間。
- 【來源 IP/Port】：通過管制規則的來源 IP 位址跟 Port。
- 【目的 IP/Port】：通過管制規則的目的 IP 位址跟 Port。
- 【通訊協定】：通過管制規則的通訊協定，有 TCP/UDP/ICMP 等 3 種協定。
- 【封包大小】：這一個連線的封包大小，單位為 Bytes。
- 【出口線路】：封包由內到外走的線路出口，如果是【-】，則是代表對方 TCP 回傳的封包。

封包通聯記錄： 每三十秒 自動更新 清除 1 / 13 跳至 1 頁數、每頁 24 筆 GO

時間	來源IP	目的 IP	通訊協定	封包大小	來源 Port	目的 Port	出口線路
2019-10-07 10:13:28	20.189.78.37	192.168.186.78	TCP	52	443	34410	-
2019-10-07 10:13:28	192.168.186.78	20.189.78.37	TCP	572	34410	443	wan1[zone1]
2019-10-07 10:13:28	192.168.186.78	20.189.78.37	TCP	1480	34410	443	wan1[zone1]
2019-10-07 10:13:28	20.189.78.37	192.168.186.78	TCP	1075	443	34410	-
2019-10-07 10:13:28	20.189.78.37	192.168.186.78	TCP	52	443	34410	-
2019-10-07 10:13:28	192.168.186.78	20.189.78.37	TCP	572	34410	443	wan1[zone1]
2019-10-07 10:13:28	192.168.186.78	20.189.78.37	TCP	1480	34410	443	wan1[zone1]

圖 4-2 管制規則的封包通聯記錄

管制規則的組合

每條管制規則由 3 個部分組合而成，分別是基本設定、進階設定跟防護設定，除了基本設定區的資料為必要填入外，另外 2 個區域的設定由管理者根據要求自行決定配置。

4-1-1、Outgoing

內部到外部的網路都在這裡管制，內部 ZONE 對 ZONE 的管制則在 Advacne 中設定。

A、Outgoing ->基本設定

每個管制規則的來源跟目的都在基本設定中定義，為了增加管理的方便性跟閱讀便利，管理者可以事先在【管理目標】 中事先定義 位址表、服務表跟應用程式，方便選擇套用，除了網路介面部分需要事先規劃外，其他的部分都有自訂方式讓管理者直接填入，例如，IP 位址、網路 Port 等。（圖 4-3）

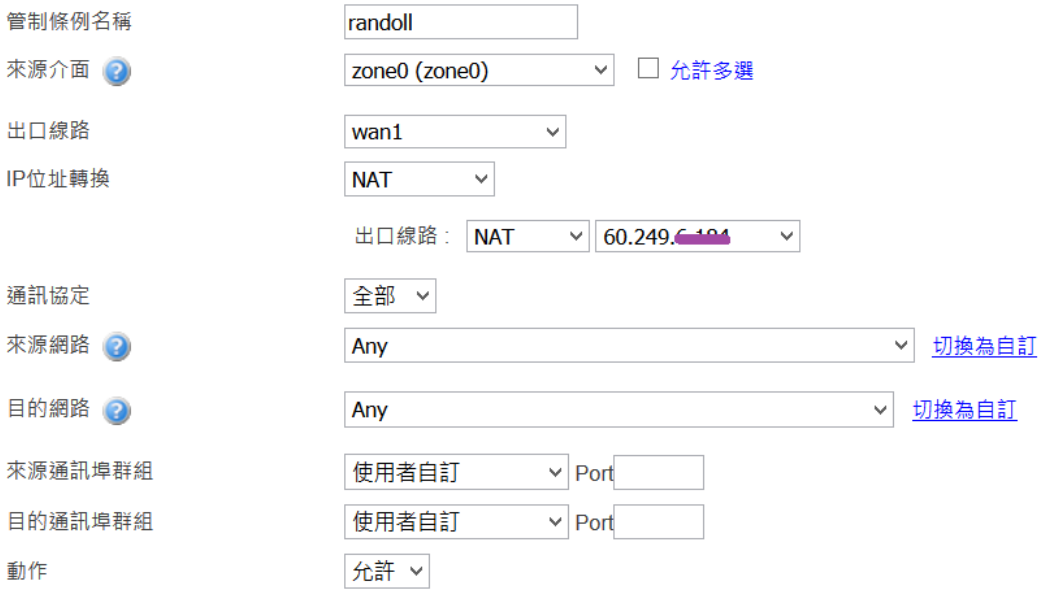


圖 4-3 管制規則的基本設定

- 【管制條例名稱】：管制規則的名稱，可以輸入任何中英文字，方便管理者辨識，例如，禁止上網。

- 【來源介面】：NG-UTM 是以 ZONE 為管理基礎，每個進出 ZONE 的網路封包都可以管理跟控制，因為這是 Outgoing 的管制，可以選擇的 ZONE 應該為內部要出去的介面，包含內部的 ZONE、PPTP、L2TP 跟 SSL VPN 的用戶端。

  網路介面分成實體介面跟虛擬介面 2 種，管理者在【網路設定】 > 【網路介面】中增加的實體介面、PPTP、L2TP 跟 SSL VPN 等都會自動加入在來源介面的選項中。

- 【出口線路 / IP 位址轉換】：參考下一個段落 Outgoing > 基本設定 > 出口線路跟 IP 轉換說明。
- 【通訊協定】：通訊協定共有 4 個選項，全部、TCP、UDP 跟 ICMP，管制規則想要管制的通訊協定是屬於哪一個類型，預設為全部。
- 【來源網路】：符合管制規則的來源 IP 位址，針對介面(ZONE)來說，就是從 NG-UTM 內部出去的 IP 位址。有 2 種模式讓管理者選擇，選項模式跟自訂模式，預設為選項模式。

選項模式

系統會自動把下列幾種來源 IP 位址加入，讓管理者選擇。

A、在 【網路設定】 > 【網路介面】 中定義的內部 ZONE。

B、在 【管理目標】 > 【位址表】 中建立的位址表或是群組

C、在各類 VPN 中分配的 IP 位址，包含 PPTP 伺服器、SSL VPN 及 L2TP 等分配給遠端用戶的 IP 位址。

自訂模式

管理者直接填入來源的 IP 位址或是 MAC 位址。

- 【目的網路】：要到達的目的 IP 位址，對 Outgoing 管制規則就是外部網路的 IP 位址，有 2 種模式讓管理者選擇，選項模式跟自訂模式，預設為選項模式。

選項模式

系統會自動加入在 【管理目標】 > 【位址表】 中建立的位址表或是群組，讓管理者選擇。

自訂 IP 位址模式

管理者直接填入來源的 IP 位址或是 MAC 位址。

同介面的 IP 可以管？

相同介面(ZONE)的不同來源跟目的 IP 位址，NG-UTM 不會管制，他的運作行為類似交換器的橋接功能，只有進、出介面(ZONE)的網路封包才會套用管制規則。

- 【來源通訊埠群組】：限制的來源通訊埠，共有 3 種可以選擇，預設服務表、自訂服務群組或是直接輸入 port，NG-UTM 會把常用的服務表列出，例如，HTTP、FTP 等，管理者為了簡化管制規則數量，把眾多服務整合出一個服務群組，這些都需要在【管理目標】中的【服務表】事先定義，定義好的管理目標就會出現在選項中，若選擇【使用者自訂】則在後面空格中自行填入 Port。

  使用注意!

  在 IPV4 的環境下，大量使用 PAT 技術，所以來源 Port 通常不固定，有可能是 1~65535 中任何一個，所以使用時請特別注意是不是要特別指定來源通訊埠，當管理者沒有指定任何群組時，預設值為全部的通訊埠。

- 【目的通訊埠群組】：限制的目的通訊埠，共有 3 種可以選擇，預設服務表、自訂服務群組或是直接輸入 port，NG-UTM 會把常用的服務表列出，例如，HTTP、FTP 等，如果管理者為了簡化管制規則數量，把眾多服務整合出一個服務群組，這些都需要在【管理目標】中的【服務表】事先定義，定義好的管理目標就會出現在選項中，若選擇【使用者自訂】則在後面空格中自行填入 Port。

  使用注意!

  在 IPV4/IPV6 的環境下，目的 Port 就是要管制的網路服務，例如只允許 HTTP 進入，則這裡就需要填入 HTTP，當管理者沒有指定任何群組時，預設值為全部。

- 【動作】：符合上述比對的封包，該如何處理，有 2 種模式可以選擇，允許跟拒絕，允許則讓封包通過，拒絕則是將封包丟棄。

  使用注意!

  如果要使用進階設定中的功能，例如 IPS、URL 管制等，在【動作】上必須為允許，否則封包會被丟棄，當然就無法進入進階設定中。

B、Outgoing ->基本設定 -> 出口線路跟 IP 轉換

針對上面比對成功的封包，該送到哪一個出口線路，出口線路可以在【網路設定】 >【路由管理】 > 【出口線路】 或是 【出口線路群組】中設定。

- 【出口線路】：符合比對的封包，要送到哪個閘道器？管理者必須事先在 【網路設定】 > 【路由管理】 中設定 【出口線路】 或是 【出口線路群組】 設定，每一個設定的在 【出口線路】 或是 【出口線路群組】 的路由都會列出讓管理者選。預設 Default 是系統預設的閘道，管理者在 【網路設定】 >【網路介面】 > 【網路介面設定】 中勾選【定義為外部網路】，這一個 ZONE 上設定的 IP 位址就會是 Default。

  NG-UTM 的預設值為『Default』，所有的網路封包會送到【預設閘道】中。

- 【IP 位址轉換】：對於進出介面的封包要執行 NAT/PAT 或是單純的 Routing 動作，在這個地方設定，詳述如下：

  1、Routing

  選擇 Routing 模式，進出介面封包的來源 IP 位址不會被改變，此時就是一個單純的 Layer 3 的路由器，再搭配來源及目的 IP 位址管制動作，就是標準 Layer 3 核心交換器的功能。

  2、NAT

  封包出去介面時轉換成哪個 IP 位址，基本上使用 PAT (Port Address Translation) 技術，出口線路選擇是『Default』，系統在執行 PAT 時自動選擇轉換 IP 並將所有的轉換 IP 位址列出，管理者想要指定轉換 IP 時就不能使用『Default』。

  出口線路選擇是特定的閘道而不是預設的閘道，執行 NAT 動作時，管理者可以自行選擇哪一個 IP 位址是要被當成 PAT/NAT 的來源位址轉換。

  例如，在 【網路設定】 > 【出口線路】 > 【介面位址】 中設定 IP 位址是 192.168.100.0/24 ，則這裡可以設定的 IP 位址是 192.168.100.0-192.168.100.254 其中一個。

出口線路選擇的是出口線路群組，則管理者可以分別指定每個出口線路要用哪一個 IP 位址當作 PAT/NAT 的來源位址。（圖 4-4）

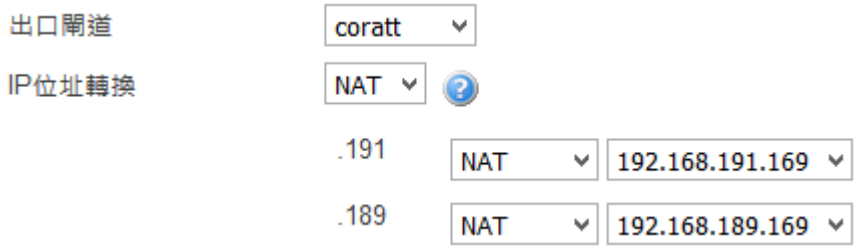


圖 4-4 多個出口線路的 PAT/NAT 設定

C、Outgoing ->進階設定

對於符合【基本設定】規則的且動作為允許的網路封包，NG-UTM 可以進行下列幾樣的額外動作，包含時間表、IPS 跟掃毒等工作，每一個項目都需要事先在相對應的【管理目標】中設定，整個管制規則才會生效。（圖 4-8）

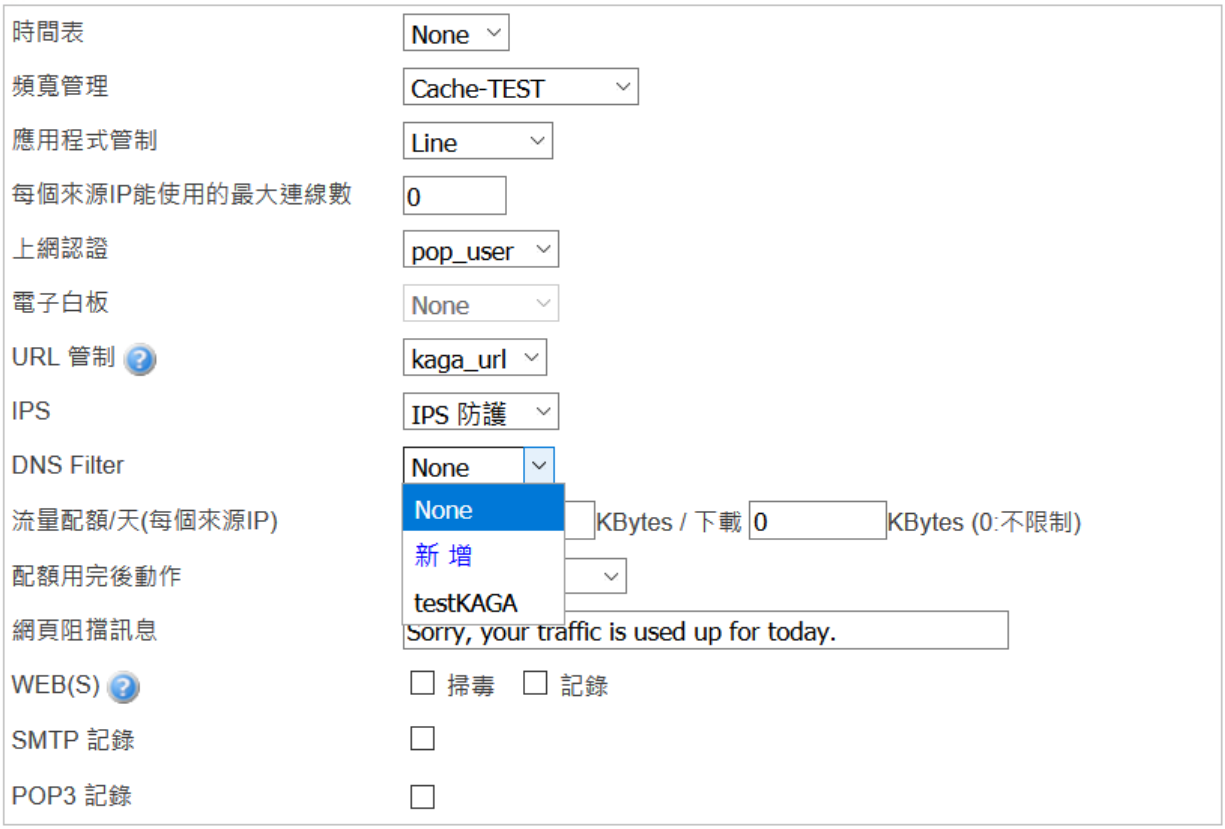


圖 4-8 管制規則進階設定

每個選項都有一個項目【新增】，當要設定的項目不在選擇中，選擇【新增】系統就會自動開啟新的頁面讓管理者快速新增管理項目，例如，要新增一筆位址表，但選擇項目中沒有，此時選擇【新增】，系統就會開新的視窗讓管理者新增位址表，而不用切換到【管理目標】>【位址表】後再按新增。

- 【時間表】：在【管理目標】>【時間表】建立要管制的時間表，整個條例只有在時間表內才會有效，時間表外則無效。
- 【頻寬管理】：在【管理目標】>【頻寬管理】建立要管制的頻寬，整個條例只使用的流量就會被限制住。
- 【應用程式管制】：在【管理目標】>【應用程式管制】建立要管制的應用程式或是群組，套用後設定的應用程式就會被阻擋或是限制使用的頻寬。
- 【每個來源 IP 能使用的最大連線數】：預設是 0，代表不管制，當設定非 0 的數字後，符合這個管制條例的每個來源 IP 位址能使用最大的連線數就會被限制。
- 【上網認證】：在【管理目標】>【上網認證】中建立認證群組，套用後，來源 IP 位址要到目的 IP 位址，都會彈跳出認證視窗，要求使用者認證。
- 【電子白板】：在【管理目標】>【電子白板】中設定使用者群組，套用後，來源 IP 位址要到介面外時，自動跳出電子白板訊息讓使用者確認。
- 【URL 管制】：在【管理目標】>【URL 管理】中設定黑名單跟白名單，套用後，黑名單的 URL 會被拒絕，白名單則允許通過。
- 【IPS】：在【IPS】>【IPS 設定】中建立一個群組，套用後，這個條例的封包就會進入 IPS 特徵值中比對，由 IPS 設定比對符合的封包是紀錄還是阻擋。
- 【DNS Filter】：啟用 DNS Filter 的功能，DNS Filter 的管制來源有 2 個，一個是 Sandstorm 另一個是自訂，這個機制可以阻擋惡意程式跟木馬網址。
- 【流量配額/天(每個來源 IP)】：這個條例中的每個來源 IP 位址能使用的上、下載量，預設值為 0，代表不限制，設定上、下載限制時，當配額使用超過，就由【配額用完後動作】中設定的動作處理。

  【配額用完後動作】：超過配額後，如何處理後續的封包要求，有 2 種選項，分別是拒絕跟繼續執行下一條。

  1、拒絕：超過配額的封包就全部丟棄，同時使用者的網頁會出現【網頁阻擋訊息】中設定的文字 。

  2、繼續執行下一條：超過配額的封包進入下一條比對，由下一個管制條例處理。

【網頁阻擋訊息】：超過配額後，使用者的網頁就會出現訊息，通知他不能再繼續使用網路的原因。

- 【WEB(S) 】：共有 2 個選項，掃毒跟紀錄，掃毒則會對所有通過的 http / https 封包執行掃毒的動作，紀錄則會記錄下 http/https 的網頁瀏覽紀錄。

  NG-UTM 內建 ClamAV 掃毒引擎是啟動，Kaspersky 掃毒引擎需要事先上傳授權碼。

  WEB 記錄不需要事先設定，啟動就生效，會記錄所有通過 NG-UTM 的 WEB 協定中 URI，不論是 http 或是 https 都會被記錄下來。

  要讓 NG-UTM 紀錄 https 的 URI 有一個前置動作，也就是要讓每一個要被記錄的使用者先匯入 NG-UTM 的 SSL 憑證，此憑證存放的位址是 https://NG-UTM 管理 IP/myca.crt ，IE / Chrome 瀏覽器均會自動執行此一憑證，Firefox 會自行管理憑證，因此使用 Firefox 時，需要再輸入一次，並將他的三個選項全部啟用。

- 【SMTP 記錄】：在【郵件管理】>【郵件過濾及記錄】中先設定要執行的項目，有掃毒、郵件稽核、垃圾郵件過濾、郵件備份等功能，每一個功能可以單獨啟用或是全選，啟用掃毒、郵件稽核、垃圾郵件過濾這 3 項功能時，還需要到【郵件管理】的【郵件掃毒】、【垃圾郵件過濾】跟【郵件稽核】項目中分別設定。

- 【POP3 記錄】：需要在【郵件管理】>【郵件過濾及記錄】中【收信的郵件掃毒、郵件稽核、垃圾信過濾、備份】事先設定要執行的項目，有掃毒、郵件稽核、垃圾郵件過濾、郵件備份等功能，每一個功能可以單獨啟用或是全選。

對於【WEB (S)】、【SMTP 記錄】、【POP3 記錄】這 3 項功能是整台 NG-UTM 都套用同一套規則，沒辦法根據每一個介面客制化規則，所以管理者只能選擇啟用或是關閉，啟用後這一個條例都是套用相同的機制。

D、Outgoing ->防護

對於進入介面的封包，要不要提供防火牆的保護，每一個管制規則都可以設定防火牆保護，但是整台 NG-UTM 只有一種防護能力的配置，防火牆的防護能力配置是在【管理目標】>【防火牆功能】中設置。（圖 4-9）

圖 4-9 管制規則的防護

4-1-2、Incoming

所有從外面進入內部 ZONE 的管制，可以在這裡設定，例如，內部有一台 ERP 伺服器，讓外面的人可以存取，就在這裡設定。

IP 位址轉換有三種運作模式，IP 對應、Port 對應、伺服器負載，每一個動作都有不同的目的，簡單來說 IP 對應就是一對一的 IP 位址對應關係，Port 對應跟伺服器負載是一對多的 IP 位址對應關係。

A、Incoming ->基本設定

IP 位址轉換有三種運作模式，IP 對應、Port 對應、伺服器負載，每一個動作都有不同的目的，簡單來說 IP 對應就是一對一的 IP 位址對應關係，Port 對應跟伺服器負載是一對多的 IP 位址對應關係。

- 【管制條例名稱】：管制規則的名稱，可以輸入任何中英文字，方便管理者辨識，例如，ERP 伺服器。
- 【來源介面】：NG-UTM 是以 ZONE 為管理基礎，每個進出 ZONE 的網路封包都可以管理跟控制，因為這是 Incoming 的管制，可以選擇的 ZONE 應該為外部要進來的介面，系統會將所有的外部網路介面列出，讓管理者選擇。
- 【 IP 位址轉換】：參考下一個段落 Incoming > 基本設定 > IP 位址轉換說明。
- 【通訊協定】：通訊協定共有 4 個選項，全部、TCP、UDP 跟 ICMP，管制規則想要管制的通訊協定是屬於哪一個類型，預設為全部。
- 【來源網路】：符合管制規則的來源 IP 位址，針對介面(ZONE)來說，就是從外面要進來 NG-UTM 的 IP 位址。有 2 種模式讓管理者選擇，選項模式跟自訂模式，預設為選項模式。

  選項模式

  系統會自動加入在 【管理目標】 > 【位址表】 中建立的位址表或是群組，讓管理者選擇。

  自訂模式

  管理者直接填入來源的 IP 位址或是 MAC 位址。
- 【目的網路】：對 Incoming 管制規則就是內部網路的 IP 位址，有 2 種模式讓管理者選擇，選項模式跟自訂模式，預設為選項模式。

選項模式

系統會自動把下列幾種來源 IP 位址加入，讓管理者選擇。

A、在【網路設定】>【網路介面】中定義的內部 ZONE。

B、在【管理目標】>【位址表】中建立的位址表或是群組

自訂 IP 位址模式

管理者直接填入來源的 IP 位址或是 MAC 位址。

- 【來源通訊埠群組】：限制的來源通訊埠，共有 3 種可以選擇，預設服務表、自訂服務群組或是直接輸入 port，NG-UTM 會把常用的服務表列出，例如，HTTP、FTP 等，為了簡化管制規則數量，把眾多服務整合出一個服務群組，這些都需要在【管理目標】中的【服務表】事先定義，定義好的管理目標就會出現在選項中，若選擇【使用者自訂】則在後面空格中自行填入 Port。

使用注意!

在 IPV4 的環境下，大量使用 PAT 技術，所以來源 Port 通常不固定，有可能是 1~65535 中任何一個，所以使用時請特別注意是不是要特別指定來源通訊埠，當管理者沒有指定任何群組時，預設值為全部的通訊埠。

- 【目的通訊埠群組】：限制的目的通訊埠，共有 3 種可以選擇，預設服務表、自訂服務群組或是直接輸入 port，NG-UTM 會把常用的服務表列出，例如，HTTP、FTP 等，如果管理者為了簡化管制規則數量，把眾多服務整合出一個服務群組，這些都需要在【管理目標】中的【服務表】事先定義，定義好的管理目標就會出現在選項中，若選擇【使用者自訂】則在後面空格中自行填入 Port。

使用注意!

在 IPV4/IPV6 的環境下，目的 Port 就是要管制的網路服務，例如只允許 HTTP 進入，則這裡就需要填入 HTTP，當管理者沒有指定任何群組時，預設值為全部。

- 【NAT】：勾選後，這個條例的來源 IP 位址會被換成內部的 IP 位址，通常是此內部介面上綁定的 IP 位址，它的使用時機為內部伺服器會管制來源 IP 位址，只開放給內部使用，當需要讓外部的人使用時，一種是改變內部伺服器的管制規則，另一種就是在條例中勾選【NAT】。

- 【動作】：符合上述比對的封包，該如何處理，有 2 種模式可以選擇，允許跟拒絕，允許則讓封包通過，拒絕則是將封包丟棄。

使用注意!

如果要使用進階設定中的功能，例如 IPS、URL 管制等，在【動作】上必須為允許，否則封包會被丟棄，當然就無法進入進階設定中。

B、Incoming ->基本設定 ->IP 位址轉換

1、IP 對應

在【網路設定】> 【網路介面】> 【外部網路 ZONE】 > 【介面位址】中設定的 IP 位址，轉換成介面內部真正提供服務的 IP 位址，是 NAT 位址轉換技術的 1 對 1 對應機制。

例如，在【外部網路 ZONE】 > 【介面位址】設定是 192.168.1.200，要對應到內部的 IP 位址是 10.10.1.200，當介面以外的人訪問 192.168.1.200 的 IP 位址時，所有的網路封包都會被自動轉換到 10.10.1.200 上。

設定 IP 對應時，在下面的空白處填入內部 IP 位址，以上面的範例就是 10.10.1.200，同時【目的網路】選擇在【網路設定】> 【網路介面】> 【外部網路 ZONE】 > 【介面位址】其中設定的 IP 位址，以上面的範例就是 192.168.1.200。同時也須勾選【來源介面】，全選所有列出來的來源介面，就可以讓所有外面的人進入，此時【來源網路】選擇 ANY，如果有限制來源 IP 位址，則在來源網路中輸入。

目的網路則選擇 IP 位址，系統自動把已經設定在【位址表】列出，方便選擇，也可按下 【切換為自訂】按鈕，直接輸入外部的 IP 位址。

2、Port 對應

Port 對應是一種 1 對多的 NAT 技術，把某一個對外的 IP 位址，根據不同的服務 Port 轉到內部不同的服務主機上，跟 IP 對應的設定觀念一樣，Port 對應也需要選擇來源介面，不是設定的來源介面無法進入，理論上，1 個合法 IP 位址，最多可分配給內部 65535 個內部 IP 位址。

選擇 Port 對應並按下修改按鈕後，NG-UTM 會出現一個新的視窗，在這個視窗中設定的 IP 位址就是內部的 IP 位址及 Port 號。（圖 4-10）

Port 對應修改

備註	通訊協定	原始目的通訊埠	轉換 IP 位址	轉換目的通訊埠	WAF	刪除
Master-WEB	TCP	HTTP Port 80	10.10.1.200	80	☑ HTTP	✕
FTP	TCP	FTP Port 21	10.10.1.100	21	☐ HTTP	✕
DNS	TCP	DNS Port 53	10.10.1.50	53	☐ HTTP	✕

圖 4-10 Port 對應設定

例如，在【外部網路 ZONE】 > 【介面位址】定義外部 IP 位址 為 192.168.1.200，伺服器 192.168.1.200 對外提供 3 種服務，WEB、FTP 跟 DNS，這 3 中服務分別對應到內部不同的主機， 10.10.1.200、10.10.1.100 跟 10.10.1.50。在 【轉換 IP 位址】上填入：

A、10.10.1.200：轉換目的通訊埠 80

B、10.10.1.100：轉換目的通訊埠 21

C、 10.10.1.50：轉換目的通訊埠 53

在【轉換目的通訊埠】中一般是跟【原始目的通訊埠】一樣，也可以設定成不一樣，設定成不一樣下，從內部使用的 Port 號跟外部使用的 Port 號就不一樣。

同時也須勾選【來源介面】，全選所有列出來的來源介面，就可以讓所有外面的人進入，此時【來源網路】選擇 ANY，如果有限制來源 IP 位址，則在來源網路中輸入。

目的網路則選擇 IP 位址，以上面的範例就是 192.168.1.200，系統自動把已經設定在【位址表】列出，方便選擇，也可按下 【切換為自訂】按鈕，直接輸入外部的 IP 位址。

WEB 類型的伺服器，NG-UTM 提供 WAF 保護機制，詳細設定請參考 【WAF】章節。

3、伺服器負載

NG-UTM 可以執行伺服器負載均衡的任務，也就是把某一個服務，平均分配給內部 2 台以上的設備，並根據設定的權重或是服務模式，分配不同的負載給不同的伺服器，跟 IP 對應的設定觀念一樣，伺服器負載也需要先選擇來源介面，不是設定的來源介面無法進入。

選擇伺服器負載並按下修改按鈕後，NG-UTM 會出現一個新的視窗，在這個視窗中定義哪一些 IP 跟 服務，執行負載均衡的工作，底下圖例是把 192.168.1.200 的 WEB 服務，依照權重設定，分配給 2 台內部伺服器，分別是 10.10.1.100 跟 10.10.1.200。（圖 4-11）

圖 4-11 伺服器負載均衡

首先確認原始目的通訊埠，可以選擇服務表中的項目，也可以自行填入 TCP Port，伺服器負載均衡機制是按照每個服務分配負載，所以每一個 Port 就需要新增一筆對應設定。

分配模式有 2 種，依序循環跟依來源 IP 2 種，每一種分配方式，都會搭配權重的觀念，分配負載給轉換 IP 位址

依序循環則是根據來源的連線要求，分配給後端的 IP 位址，例如，10.10.1.200 權重 1，10.10.1.201 權重 2，則第 1 個連線給 10.10.1.200，第 2/3 個連線給 10.10.1.201，第 4 個連線給 10.10.1.200，第 5/6 個連線給 10.10.1.201，以此類推

。

依來源 IP 則是根據來源 IP 位址分配 IP 位址，例如，第一個來源 IP 位址分配給 10.10.1.200，帶 2/3 個不同來源 IP 位址分配給 10.10.1.201，以此類推。

同時也須勾選【來源介面】，全選所有列出來的來源介面，就可以讓所有外面的人進入，此時【來源網路】選擇 ANY，如果有限制來源 IP 位址，則在來源網路中輸入。

目的網路則選擇 IP 位址，以上面的範例就是 192.168.1.200，系統自動把已經設定在【位址表】列出，方便選擇，也可按下 【切換為自訂】按鈕，直接輸入外部的 IP 位址。

C、Incoming ->進階設定

對於符合【基本設定】規則的且動作為允許的網路封包，NG-UTM 可以進行下列幾樣的額外動作，包含時間表、IPS 跟 SMTP，每一個項目都需要事先在相對應的【管理目標】中設定，整個管制規則才會生效。

每個選項都有一個項目【新增】，當要設定的項目不在選擇中，選擇【新增】系統就會自動開啟新的頁面讓管理者快速新增管理項目，例如，要新增一筆位址表，但選擇項目中沒有，此時選擇【新增】，系統就會開新的視窗讓管理者新增位址表，而不用切換到【管理目標】>【位址表】後再按新增。

- 【時間表】：在【管理目標】>【時間表】建立要管制的時間表，整個條例只有在時間表內才會有效，時間表外則無效。
- 【頻寬管理】：在【管理目標】>【頻寬管理】建立要管制的頻寬，整個條例只使用的流量就會被限制住。
- 【應用程式管制】：在【管理目標】>【應用程式管制】建立要管制的應用程式或是群組，套用後設定的應用程式就會被阻擋或是限制使用的頻寬。
- 【每個來源 IP 能使用的最大連線數】：預設是 0，代表不管制，當設定非 0 的數字後，符合這個管制條例的每個來源 IP 位址能使用最大的連線數就會被限制。
- 【IPS】：在【IPS】>【IPS 設定】中建立一個群組，套用後，這個條例的封包就會進入 IPS 特徵值中比對，由 IPS 設定比對符合的封包是紀錄還是阻擋。

  WEB 記錄不需要事先設定，啟動就生效，會記錄所有通過 NG-UTM 的 WEB 協定中 URI，不論是 http 或是 https 都會被記錄下來。

  要讓 NG-UTM 紀錄 https 的 URI 有一個前置動作，也就是要讓每一個要被記錄的使用者先匯入 NG-UTM 的 SSL 憑證，此憑證存放的位址是 https://NG-UTM 管理 IP/myca.crt，IE / Chrome 瀏覽器均會自動執行此一憑證，Firefox 會自行管理憑證，因此使用 Firefox 時，需要再輸入一次，並將他的三個選項全部啟用。
- 【SMTP 記錄】：在【郵件管理】>【郵件過濾及記錄】中先設定要執行的項目，有掃毒、郵件稽核、垃圾郵件過濾、郵件備份等功能，每一個功能可以單獨啟用或是全選，啟用掃毒、郵件稽核、垃圾郵件過濾這 3 項功能時，還需要到【郵件管理】的【郵件掃毒】、【垃圾郵件過濾】跟【郵件稽核】項目中分別設定。

對於【SMTP 記錄】、【IPS】這 3 項功能是整台 NG-UTM 都套用同一套規則，沒辦法根據每一個介面客制化規則，所以管理者只能選擇啟用或是關閉，啟用後這一個條例都是套用相同的機制。

D、Incoming ->防護

對於進入介面的封包，要不要提供防火牆的保護，每一個管制規則都可以設定防火牆保護，但是整台 NG-UTM 只有一種防護能力的配置，防火牆的防護能力配置是在【管理目標】>【防火牆功能】中設置。

4-1-3、Advance

Advance 基本上是 Outgoing 跟 Incoming 的組合體，設定時切換動作是在【IP 位址轉換】上，選擇【IP 位址轉換】後，管理介面就會切換成設定項目。當管理者要新增一條規則時，首先想到的就是 IP 位址的轉換動作，在 Advance 有 5 種規則應用時機說明如下：

A、 Routing ：通常用在內部 ZONE 對內部 ZONE 之間的管制。

B、 NAT：通常應用在內部各個 ZONE 要出去外部的管制。

C、 IP 對應：把外部 IP 位址轉到內部特定的 IP 位址，所有的 Port 都會一起轉。

D、 Port 對應：把外部 IP 位址的特定 Port 轉到內部 IP 位址的 特定 Port 上。

E、 伺服器負載：把外部 IP 位址的特定 Port 轉到內部 2 台以上不同 IP 位址的特定 Port，這 2 台不同內部 IP 位址的主機是做相同的工作，例如，WEB 伺服器。

在 Advance 的 5 種規則，已分別在 Outgoing 跟 Incoming 中說明：

A、 參考 4-1-1、 Outgoing 的 Routing 、NAT。

B、 參考 4-1-2、屬於 Incoming 的 IP 對應、Port 對應跟伺服器負載。

注意 Advance 的優先權高於 Outgoing 跟 Incoming，分別設定相同的管制條例在 Outgoing / Incoming 跟 Advance 上，只有 Advance 會生效。

4-1-4、SYN 防護

駭客常用來癱瘓伺服器 SYN 攻擊，NG-UTM 提供 SYN 防護機制，保護後面的伺服器拒絕大量不正常的 SYN 攻擊，確保服務正常運作，因為是保護後面的伺服器，所以它的設定跟 Incoming 的規則一樣，提供 IP 對應、Port 對應跟伺服器負載等 3 種 IP 位址轉換方式。

SYN 防護運作

TCP 的三方交握是用戶端要跟與伺服器間建立 TCP 連線時，用戶端與伺服器端按照順序交換資訊如下：

1、用戶端透過傳送 SYN 封包給伺服器要求建立連線。

2、伺服器回應用戶端 SYN-ACK 已抄收（acknowledge）請求。

3、用戶端回應 ACK，TCP 連線就建立完成。SYN 攻擊時用戶端不會回應 ACK。

因為駭客會送出大量的 SYN 給伺服器要求連線，佔據伺服器的資源，導致正常的 TCP 連線要求無法使用，伺服器的服務就癱瘓。

NG-UTM 的保護機制就是接手 1 ~3 步驟，確定這個連線為真之後才會將它傳給後端的伺服器，所以駭客攻擊的設備是 NG-UTM，而不是後面的伺服器。

SYN 防護切換動作是在【IP 位址轉換】上，選擇【IP 位址轉換】後，管理介面就會切換成設定項目。當管理者要新增一條規則時，首先想到的就是 IP 位址的轉換動作，在 SYN 防護有 3 種規則應用時機說明如下：

A、 IP 對應：把外部 IP 位址轉到內部特定的 IP 位址，所有的 Port 都會一起轉。

B、 Port 對應：把外部 IP 位址的特定 Port 轉到內部 IP 位址的 特定 Port 上。

C、 伺服器負載：把外部 IP 位址的特定 Port 轉到內部 2 台以上不同 IP 位址的特定 Port，這 2 台不同內部 IP 位址的主機是做相同的工作，例如，WEB 伺服器。

在 SYN 防護 的 3 種規則，已在 Incoming 中說明：參考 4-1-2、屬於 Incoming 的 IP 對應、Port 對應跟伺服器負載。

SYN 防護的進階設定只有【時間表】、【頻寬管理】、【應用程式管制】跟【每個來源 IP 能使用的最大連線數】這 4 種。

4-2、IPSec 管制

IPSec 管制規則跟其他的管制規則設定相同，只是他的選項變少也不需要選擇來源介面。

IPSec 管制顯示頁面說明

進入 IPSec 管制時，NG-UTM 會依序列出所有的管制規則，IPV4 跟 IPV6 的管制規則也是分開列出，預設 NG-UTM 是列出 IPV4 的管制規則，如果要切換成 IPV6 的管制規則，則在主選單上方 IPv4 IPv6 MENU 點選 IPV6，整個管制規則就會切換成 IPV6 模式，不論 IPV4 或是 IPV6 在這個頁面可讓管理者調整的項目如下：（圖 4-12）

- 【優先權】：NG-UTM 會從第一條 IPSec 管制規則開始執行，所以比對順序對於網路封包的通過與否有關鍵性的影響，選擇要變化優先權的管制規則並選擇數字，則此條管制規則就會插入成為選擇的優先權，例如，原本第 5 優先權的管制規則要變成第 2，在優先權上選擇 2 ，第 5 條規則就會變成第 2 條，原本的第 2 優先權管制規則就會變成第 3，以此類推。
- 【啟用】：IPSec 管制規則的暫停跟啟用按鈕，管理者點選這個圖示後可以將原本啟用的 IPSec 管制規則暫停，原本是暫停的變成啟用。
- 【編輯/刪除】：修改或是刪除此條 IPSec 管制規則。
- 【統計】：每條管制規則進出的封包數量跟流量，暫停跟重新啟用都會把數值歸零，點選數字後，會出現符合這一個規則的所有網路封包詳細的進出記錄。
- 設定管制規則後，可藉由此功能觀察封包是否進入規則中。

圖 4-12 IPSec 管制規則控制

當管理者在找尋 IPSec 網路問題時，想知道設定的目標是否有進入管制規則，此時就可以利用 NG-UTM 提供的封包即時通聯功能，點選 IPSec 管制規則上【統計】欄位的數字，此項功能就會被啟用，NG-UTM 會把進出的網路封包擷取後並開啟一個新的視窗讓管理者觀察。（圖 4-13）

- 【自動更新】：NG-UTM 每隔 3~30 秒，就會自動更新封包的通聯記錄，方便管理者觀察。
- 【清除】：把通聯記錄的資料全部清除掉，重新記錄跟顯示。
- 【時間】：IPSec 網路封包通過的時間。
- 【來源 IP/Port】：此條 IPSec 管制規則的來源 IP 位址跟 PORT。
- 【目的 IP/Port】：此條 IPSec 管制規則的目的 IP 位址跟 PORT。
- 【通訊協定】：此條 IPSec 管制規則的通訊協定，有 TCP/UDP/ICMP 等。
- 【封包大小】：這一個連線的封包大小，單位為 Bytes。
- 【出口線路】：這個封包由內到外走的線路出口，如果是【-】，則是代表對方 TCP 回傳的封包。

封包通聯記錄： 每三十秒 自動更新 清除 1 / 1 跳至 1 頁數、每頁 24 筆 GO

時間	來源IP	目的 IP	通訊協定	封包大小	來源 Port	目的 Port	出口線路
2019-10-07 10:33:36	192.168.188.81	192.168.18.154	TCP	52	4001	10001	-
2019-10-07 10:33:33	192.168.188.81	192.168.18.154	TCP	52	4001	10001	-
2019-10-07 10:33:22	192.168.188.81	192.168.18.156	TCP	52	4001	10001	-

圖 4-13 IPSec 管制封包記錄

A、IPSec 管制規則 ->基本設定

每個 IPSec 管制規則的來源跟目的都在基本設定中定義，因為專屬於 IPSec VPN 通道的管制機制，所以來源或是目的的一端就是 IPSec 通道。（圖 4-14）

圖 4-14 IPSec 管制規則的基本設定

- 【管制條例名稱】：IPSec 管制規則的名稱，可以輸入任何中英文字，方便閱讀跟理解，例如，禁止上網。
- 【通訊協定】：通訊協定共有 3 個選項，全部、TCP 跟 UDP，這個 IPSec 管制規則想要管制的通訊協定是屬於哪一個類型，預設為全部。
- 【方向】：有 2 個方向選項，【To IPSec】跟【IPSec To】，簡單來區分如下：

  To IPSec

  從內部透過 IPSec VPN 通道到遠端。

  IPSec To

  從 IPSec VPN 通道進來到內部的方向。

- 【來源網路】：根據前面的【方向】定義，來源網路就會不一樣，例如，【方向】為【To IPSec】，則來源網路是內部 ZONE 的 IP 位址，目的網路為 IPSec 另一端的 IP 位址，如【方向】為【IPSec To】，則來源網路是 IPSec VPN 通道另一端的 IP 位址，目的網路就是內部 ZONE 的 IP 位址。

  選項模式

  系統列出在【管理目標】>【位址表】中建立的位址表或是群組提供選擇的項目。

  自訂模式

  直接填入來源的 IP 位址或是 MAC 位址。

- 【目的網路】：根據前面的【方向】定義，目的網路就會不一樣，例如，【方向】為【To IPSec】，則目的網路是 IPSec VPN 通道另一端的 IP 位址，【方向】為【IPSec To】則目的網路是內部 ZONE 的 IP 位址。

  選項模式

  系統列出在【管理目標】>【位址表】中建立的位址表或是群組提供選擇的項目。

  自訂模式

  直接填入目的 IP 位址。

- 【通訊埠群組】：限制通過 IPSec VPN 通道的通訊埠，共有 3 種類別可以選擇，預設服務表、自訂服務群組跟使用者自訂，NG-UTM 會把常用的服務表列出，例如，HTTP、FTP 等，如果管理者為了簡化管制規則數量，把要眾多服務整合出一個服務群組，都需要在【管理目標】>【服務表】定義，定義好的管理目標就會出現在選項中，當然也可以自行填入 Port。

  使用注意!

  在 IPV4/IPV6 的環境下，沒有指定任何群組時，代表為全部的通訊埠。

- 【動作】：符合上述比對的封包，該如何處理，有 2 種模式可以選擇，允許跟拒絕，允許則讓封包通過並再進行進階設定中時間表或是頻寬管理的處理，拒絕則是將封包丟棄。

B、IPSec 管制規則 ->進階設定

對於符合【基本設定】規則的且動作為允許的網路封包，NG-UTM 可以進行下列 3 樣的額外動作，包含時間表、頻寬管理及 NAT(限方向為 IPSec To 的條例)。（圖 4-15）

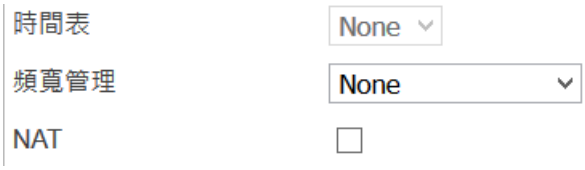


圖 4-15 IPSec 管制規則進階設定

- 【時間表】：在【管理目標】>【時間表】建立要管制的時間表，整個 IPSec 條例只有在時間表內才會有效，時間表外則無效。
- 【頻寬管理】：在【管理目標】>【頻寬管理】建立要管制的頻寬，整個條例就會被限制住，如無設定就使用到線路提供最大的頻寬。
- 【NAT】：對於從 IPSecVPN 通道進入網路介面的封包，執行 NAT 的動作，勾選後，這個條例的來源 IP 位址會被換成內部的 IP 位址，通常是此內部介面上綁定的 IP 位址，它的使用時機為內部伺服器會管制來源 IP 位址，只開放給內部使用，當需要讓外部的人使用時，一種是改變內部伺服器的管制規則，另一種就是在條例中勾選【NAT】。

4-3、SD-WAN 管制

NG-UTM 具有 SD-WAN 的功能，他能整合包含 MPLS、IP Tunnel 或是 IPSec VPN 等線路，並且分配或管理每一條線路使用的通訊協議或是頻寬，進行管制前需要先到【VPN】>【SD-WAN】把每一條使用到的通道種類事先定義好。

一個簡單的運用示意圖如下，2 點之間用 MPLS 專線，另外用網際網路的 IPSec VPN 建立第 2 條備援線路，此時管理者可以分配 2 點之間的負載分配機制，例如，MAIL 用 MPLS，ERP 用 IPSec VPN，當任何線路斷掉，另一個線路就馬上接手。（圖 4-16）

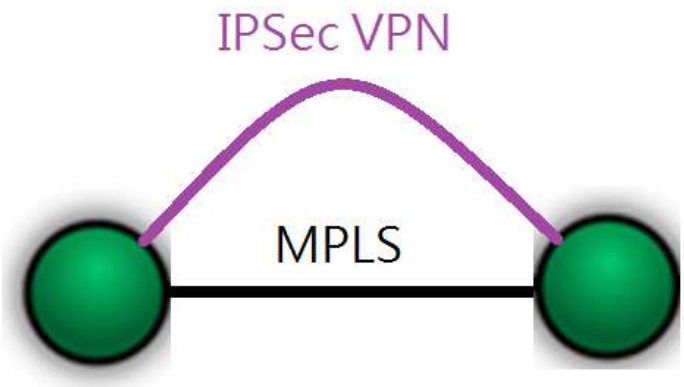


圖 4-16 SD-WAN 示意圖

除了當 MPLS 線路的備援外，也可以建立多條的 IPSec VPN 或是 IP Tunnel VPN 通道，並把 2 邊通訊需要的負載分配到合適的通道上。（圖 4-17）

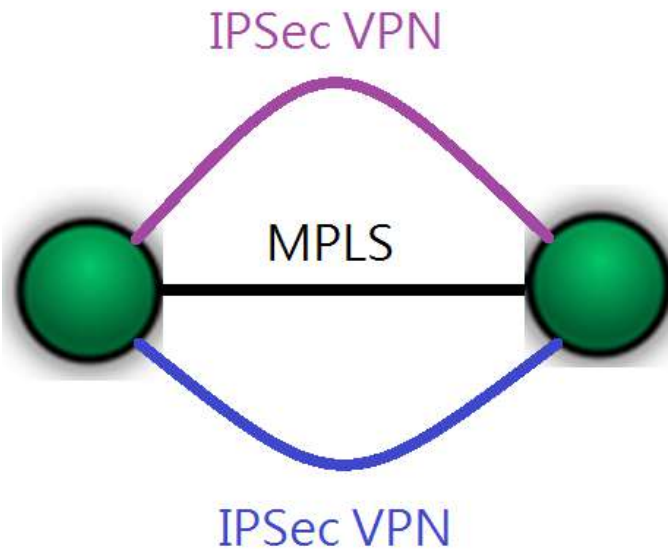


圖 4-17 多條 SD-WAN 示意圖

SD-WAN 管制顯示頁面說明

進入 SD-WAN 管制時，NG-UTM 會依序列出所有的管制規則，IPV4 跟 IPV6 的管制規則也是分開列出，預設 NG-UTM 是列出 IPV4 的管制規則，如果要切換成 IPV6 的管制規則，則在主選單上方 IPv4 IPv6 MENU 點選 IPV6，整個管制規則就會切換成 IPV6 模式，不論 IPV4 或是 IPV6 在這個頁面可讓管理者調整的項目如下：（圖 4-18）

- 【優先權】：NG-UTM 會從第一條 SD-WAN 管制規則開始執行，所以比對順序對於網路封包的通過與否有關鍵性的影響，選擇要變化優先權的管制規則並選擇數字，則此條管制規則就會插入成為選擇的優先權，例如，原本第 5 優先權的管制規則要變成第 2，在優先權上選擇 2 ，第 5 條規則就會變成第 2 條，原本的第 2 優先權管制規則就會變成第 3，以此類推。。
- 【啟用】：SD-WAN 管制規則的暫停跟啟用按鈕，點選這個圖示後可以將原本啟用的 SD-WAN 管制規則暫停，原本是暫停的變成啟用。
- 【編輯/刪除】：修改或是刪除此條 SD-WAN 管制規則。
- 【統計】：每條管制規則進出的封包數量跟流量，暫停跟重新啟用都會把數值歸零，點選數字後，會出現符合這一個規則的所有網路封包詳細的進出記錄。

  設定管制規則後，可藉由此功能觀察封包是否進入規則中。

圖 4-18 SD-WAN 管制規則控制

當找尋 SD-WAN 網路問題時，會想知道設定的目標規則是否有進入管制規則，此時就可以利用 NG-UTM 提供的網路封包即時通聯功能，點選 SD-WAN 管制規則上【統計】欄位的數字，此項功能就會被啟用，NG-UTM 會把進出的網路封包擷取並開啟一個新的視窗讓管理者觀察。（圖 4-19）

- 【自動更新】：NG-UTM 每隔 3~30 秒，就會自動更新封包的通聯記錄，方便管理者觀察。
- 【清除】：把通聯記錄的資料全部清除掉，重新記錄跟顯示。
- 【時間】：SD-WAN 網路封包通過的時間。
- 【來源 IP/Port】：此條 SD-WAN 管制規則的來源 IP 位址跟 PORT。
- 【目的 IP/Port】：此條 SD-WAN 管制規則的目的 IP 位址跟 PORT。
- 【通訊協定】：此條 SD-WAN 管制規則的通訊協定，有 TCP/UDP/ICMP 等。
- 【封包大小】：這一個連線的封包大小，單位為 Bytes。
- 【出口線路】：這個封包由內到外走的線路出口，如果是【-】，則是代表對方 TCP 回傳的封包或是 UDP 封包。

封包通聯記錄： 每三十秒 自動更新 清除 1 / 1 跳至 1 頁數、每頁 24 筆 GO

時間	來源IP	目的 IP	通訊協定	封包大小	來源 Port	目的 Port	出口線路
2019-10-07 10:26:37	192.168.188.81	192.168.100.184	TCP	52	4001	4001	TC to TP
2019-10-07 10:26:34	192.168.188.81	192.168.100.184	TCP	52	4001	4001	to_tp[gre2]

圖 4-19 SD-WAN 管制封包記錄

A、SD-WAN 管制規則 ->基本設定

每個 SD-WAN 管制規則的來源跟目的都在基本設定中定義，因為專屬於 SD-WAN 通道的管制機制，所以來源或是目的的另一端就是 SD-WAN 通道。（圖 4-20）

圖 4-20 IPSec 管制規則的基本設定

- 【管制條例名稱】：SD-WAN 管制規則的名稱，可以輸入任何中英文字，方便閱讀跟理解，例如，禁止上網。
- 【通訊協定】：通訊協定共有 3 個選項，全部、TCP 跟 UDP，SD-WAN 管制規則想要管制的通訊協定是屬於哪一個類型，預設為全部。
- 【方向】：有 2 個方向選項，【To SD-WAN】跟【SD-WAN To】，簡單來區分如下：

  To SD-WAN

  從本機要透過 SD-WAN 通道，到達 SD-WAN 另一端的連線。

  SD-WAN To

  從 SD-WAN 通道進來到本機的連線。

【來源網路】：根據前面的【方向】定義，來源網路就會不一樣，例如，【方向】為【To SD-WAN】，則來源網路是內部 ZONE 的 IP 位址，目的網路為 SD-WAN 另一端的 IP 位址，如【方向】為【SD-WAN To】，則來源網路是 SD-WAN 通道另一端的 IP 位址，目的網路就是內部 ZONE 的 IP 位址。

選項模式

事先在【管理目標】>【位址表】中建立的位址表或是群組都是可以被選擇的項目。

自訂模式

直接填入來源的 IP 位址或是 MAC 位址。

- 【目的網路】：根據前面的【方向】定義，目的網路就會不一樣，例如，【方向】為【To SD-WAN】，則目的網路是 SD-WAN 通道另一端的 IP 位址，【方向】為【SD-WAN To】則目的網路是內部 ZONE 的 IP 位址。

選項模式

事先在【管理目標】>【位址表】中建立的位址表或是群組都是可以被選擇的項目。

自訂模式

管理者直接填入目的 IP 位址。

【通訊埠或群組】：限制通過 IPSec VPN 通道的通訊埠，共有 3 種類別可以選擇，預設服務表、自訂服務群組跟使用者自訂，NG-UTM 會把常用的服務表列出，例如，HTTP、FTP 等，如果管理者為了簡化管制規則數量，把要眾多服務整合出一個服務群組，都需要在【管理目標】>【服務表】定義，定義好的管理目標就會出現在選項中，當然也可以自行填入 Port。

使用注意!

在 IPV4/IPV6 的環境下，沒有指定任何群組時，代表為全部的通訊埠。

- 【動作】：符合上述比對的封包，該如何處理，有 2 種模式可以選擇，允許跟拒絕，允許則讓封包通過並再進行進階設定中時間表或是頻寬管理的處理，拒絕則是將封包丟棄。

B、SD-WAN 管制規則 ->進階設定

對於符合【基本設定】規則的且動作為允許的網路封包，NG-UTM 可以進行下列 3 樣的額外動作，包含時間表、頻寬管理及走哪一條 SD-WAN。（圖 4-21）

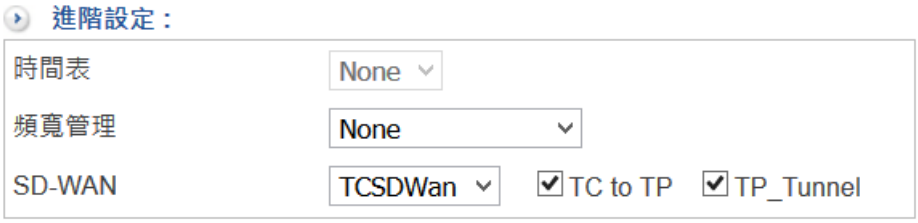


圖 4-21 SD-WAN 管制規則進階設定

- 【時間表】：在【管理目標】>【時間表】建立要管制的時間表，整個 SD-WAN 條例只有在時間表內才會有效，時間表外則無效。
- 【頻寬管理】：在【管理目標】>【頻寬管理】建立要管制的頻寬，整個條例只使用的流量就會被限制住。
- 當管制方向為 To SD-WAN 時，第 3 個選項自動切換成【SD-WAN】，當管制方向為 SD-WAN To 時，第 3 個自動切換成【NAT】，詳細說明如下：

  1、【SD-WAN】：符合基本設定的封包且動作是允許下，讓它走哪幾條線路，SD-WAN 可以由多條 IPSec VPN 通道或是 MPLS 線路組合，這一些組合需要事先 在【VPN】 > 【SD-WAN】中設定，選擇通道名稱後，系統會自動列出通道的所有 SD-WAN 線路名稱繞管理者勾選。

  2、【NAT】：對於從 IPSecVPN 通道進入網路介面的封包，執行 NAT 的動作，勾選後，這個條例的來源 IP 位址會被換成內部的 IP 位址，通常是此內部介面上綁定的 IP 位址，它的使用時機為內部伺服器會管制來源 IP 位址，只開放給內部使用，當需要讓外部的人使用時，一種是改變內部伺服器的管制規則，另一種就是在條例中勾選【NAT】。

4-4、管制規則應用範例

以實際的範例及設定步驟，說明如何使用 NG-UTM 的管制規則，管理所有的網路行為，某家公司採用 NG-UTM 為第一線的防火牆及核心交換器功能，並根據實際的網路安全架構將內部區分成 4 大塊，分別是有線區、無線網路區、對外服務區跟內部伺服器區，並把所有的對外線路整合在一個區域中，每一區的管制要求都不一樣，整體的網路架構圖如下：（圖 4-22）

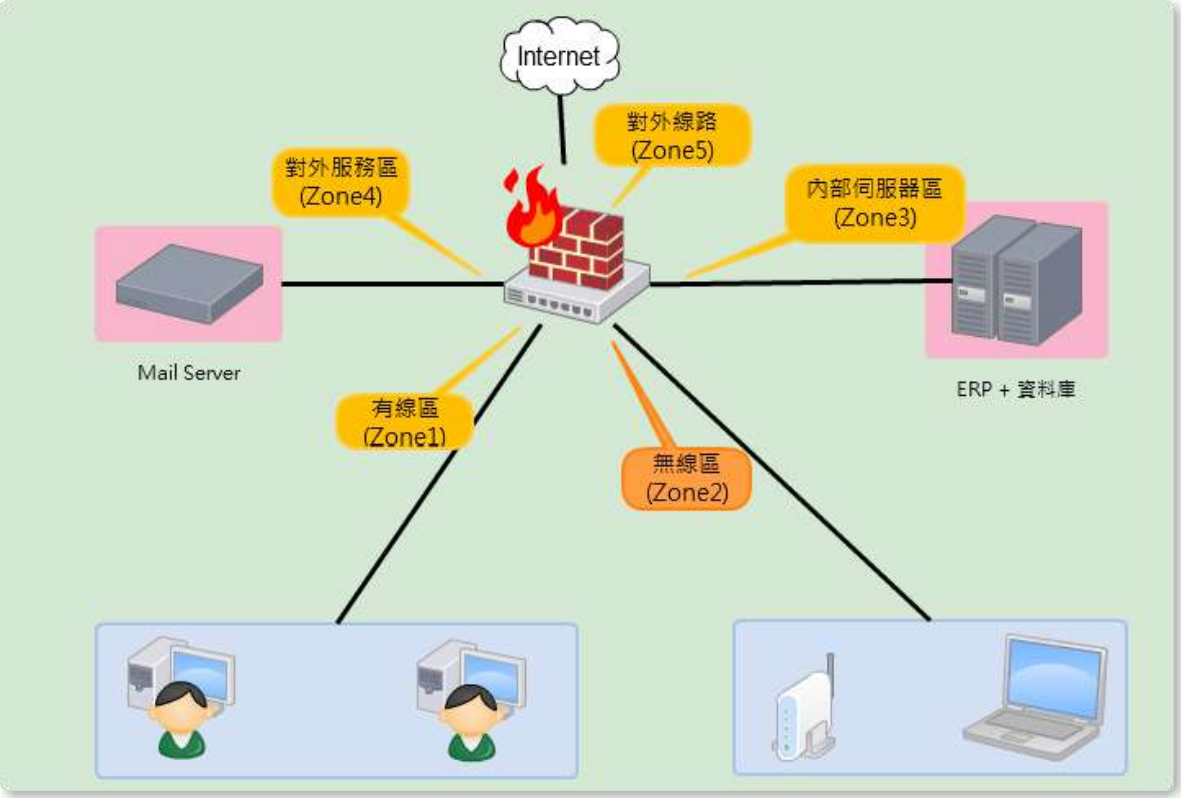


圖 4-22 管制範例網路架構圖

管制要求範例：

範例	網路介面	管理要求
1	有線區(Zone 1)	不能上黑名單 URL 跟記錄瀏覽的網站。
2	無線區(Zone 2)	上網時要認證並看電子白板，下班時間禁止上網。
3	內部伺服器區(Zone 3)	禁止上網際網路，同時只有內部特定 IP 位址能進入。
4	對外服務區(Zone 4)	只有 WEB 服務才能進出，並啟用 IPS 跟防火牆防護。
5	對外服務區(Zone 4)	只有 MAIL 服務才能進出，並啟用垃圾跟病毒郵件過濾。

共同設定

此次範例是以 NG-UTM 14 個 Giga Port 為配置範例，此台設備共有 14 個實體 Port ，代號分別是 Eth0 ~ Eth13，其中 Zone0 (Eth0) 為系統預設的 Zone，將他保留成為管理 Port，所以剩下 13 Port 可供分配，管理者根據網路狀況把所有的實體 Port 跟網路 IP 位址規劃成下表：

網路介面	數量，實體 Port	IPV4 位址	說明
有線區(Zone 1)	2 個，Eth1、Eth2	192.168.2.0/24	往下串接 L2 交換器
無線區(Zone 2)	1 個，Eth3	192.168.5.0/24	接入無線 AP
內部伺服器區(Zone 3)	3 個，Eth4~Eth6	172.16.1.0/24	郵件跟 Web 伺服器，不需要外接交換器
對外服務區(Zone 4)	5 個，Eth7~Eth11	172.16.5.0/24	ERP 跟 Data 伺服器，不需要外接交換器
對外線路(Zone 5)	2 個，Eth12、Eth13	61.22.23.24/0	只接一個外線

在『內部伺服器區(Zone 3)』跟『對外服務區(Zone 4)』中，因為要接入的伺服器數量不多，所以就可以直接入 NG-UTM 提供的網路孔中，節省交換器的使用，除了方便管理外，整體的網路速度也因為減少交換器的干擾。

步驟1. 分配置實體 Port 。

在【網路設定】>【區域設定】中按照前面的要求分配實體 Port 跟區域。（圖 4-23）

區域列表：（設定完成之後請點選儲存）

區域	名稱	顏色
zone0	zone0	
zone1	有線區	
zone2	無線區	
zone3	內部伺服器區	
zone4	對外服務區	
zone5	對外線路	

圖 4-23 定義每一個網路介面跟實體 Port

步驟2. 設定每個介面的 IP 位址。（圖 4-24）

1.在【網路設定】>【網路介面】中設定每個介面的 IP 位址跟區段。

2.新增加的區域(ZONE)自動出現在上方的頁籤中。

3.新增加的區域(ZONE)預設為 OFF，需要先設為 STATIC 並儲存。

4.在介面位址上加入規劃中的 IP 位址跟區段，除了 WAN 類型的介面需要加入預設閘道外，其他的在新增時預設閘道欄位都可以為空白，因為本身設定的 IP 位址就是 ZONE 使用者的閘道位址。

5.啟用訪問控制跟防火牆防護設定由管理者決定。

6.外部線路的 ZONE 有【定義外部網路】 的選項，勾選後這介面就會自動成為系統預設閘道的介面。

圖 4-24 設定網路介面

步驟3. 設定閘道（圖 4-25）

1.在【網路設定】>【路由管理】>【出口線路】設定對外線路。

2.如果有超過 2 個線路時，可以在【出口線路群組】中建立線路負載均衡機制。

圖 4-25 設定閘道

到目前為止，把整個 NG-UTM 在網路配置部分都完成，再來就針對每一個需求進行設置。

4-3-1、範例一：管制上網

範例一：有線區(Zone1)不能上黑名單 URL 跟記錄瀏覽的網站

步驟1. 定義黑名單 URL 來源（圖 4-26）

在【管理目標】>【URL 管理】>【黑名單設定】，新增一筆黑名單來源。

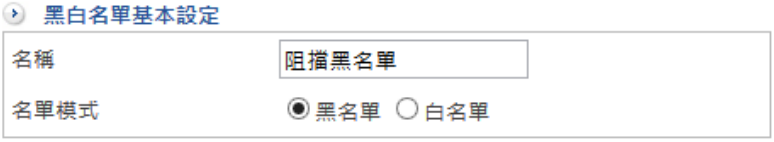


圖 4-26 建一個 URL 黑名單來源

選擇黑名單資料庫或是自訂黑名單 URL，HTTP 跟 HTTPS 的自訂黑名單是分開設定。（圖 4-27）

圖 4-27 選 URL 跟自訂黑名單

步驟2. 設定阻擋黑名單網站時要讓使用者看到的訊息（圖 4-28）

在【管理目標】>【URL 管理】>【其他設定】，設定要讓使用者看到的訊息，右邊是使用者被阻擋時網頁出現的畫面。

圖 4-28 黑名單阻擋頁面

步驟3. 建立黑名單

在【管理目標】>【URL 管理】>【URL 設定】，新增一筆黑名單名稱，名單的選擇用剛剛建立的阻擋黑名單。（圖 4-29）

圖 4-29 建立黑名單名稱

步驟4. 定 WEB/HTTPS 連線

在【網路服務】>【WEB 服務】>【WEB】檢視各項設定，包含防毒引擎、中毒時要顯示頁面、最大連線數跟加密憑證等設定。

步驟5. 管制條例套用

新增一條管制規則，來源介面為 Zone 1 有線區；動作為允許；指定閘道為對外線路，因為她是虛擬 IP 區段，要上網際網路時需要做 NAT，所以選擇來源位址轉換。（圖 4-30）

圖 4-30 管制規則的基本設定

在 URL 管制選擇剛剛的阻擋中黑名單，並啟用 WEB 掃毒跟紀錄，要啟用 SSL 的掃毒跟紀錄每一位使用者需要在個人電腦上安裝 NG-UTM 發出的根憑證。（圖 4-31）

圖 4-31 要啟用的項目

完成的管制規則。（圖 4-32）

圖 4-32 完成的管制規則

4-3-2、範例二：認證+電子白板

範例二：無線區(Zone2) 上網時要認證並看電子白板，下班時間禁止上網

步驟1. 建立認證用途的使用者帳號來源

認證的使用者來源可以是本機帳號、Radius 伺服器、AD 伺服器帳號跟郵件伺服器帳號等 4 種之一或是混合組合的帳號來源，管理者根據自己的需求配置。

說明範例中認證帳號選擇跟郵件伺服器的收信帳號相同，在【管理目標】>【上網認證】>【POP3,RAIUS 使用者】的 POP3 伺服器中指定郵件伺服器的名稱及 IP 位址等資料。（圖 4-33）

圖 4-33 POP3 伺服器帳號當作認證來源帳號

步驟2. 建立使用者群組。（圖 4-34）

圖 4-34 建立新的使用者群組

步驟3. 建立一個新的電子白板

在【管理目標】>【電子白板】中新增一筆電子白板，並且設為沒閱讀電子白板前，使用者無法上網。（圖 4-35）

圖 4-35 新建電子白板

步驟4. 電子白板版面設計

在【管理目標】>【電子白板】中選擇剛剛建立的『認證+電子白板』的版面設計。（圖 4-36）

圖 4-36 電子白板板面設計

步驟5. 認證頁面設定，套用電子白板

在【管理目標】>【上網認證】>【頁面設定】，管理者可以決定使用者登入前、後看到的資訊甚至認證成功後 URL 要不要轉到特定網址，此範例中需要使用者先看一段電子白板。（圖 4-37）

圖 4-37 套用電子白板

步驟6. 確認認證的機制

在【管理目標】>【上網認證】>【認證設定】，確認一下認證的機制，例如同一個帳號可不可以同時登入、允許使用者改密碼 ?此項功能限定本機帳號。

步驟7. 定義上班時間

在【管理目標】>【時間表】中新建一個時間表。（圖 4-38）

圖 4-38 設定上班時間

步驟8. 新增管制規則

新增一條管制規則，來源介面為 Zone 2 無線區；動作為允許；指定閘道為對外線路，因為她是虛擬 IP 區段，要上網際網路時需要做 NAT，所以選擇來源位址轉換。（圖 4-39）

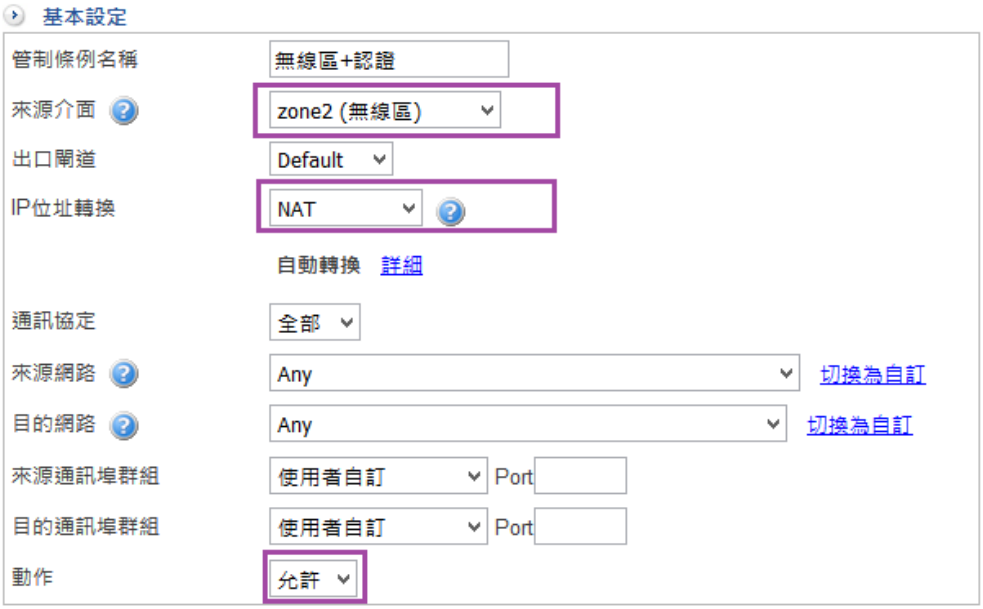


圖 4-39 管制規則基本設定

步驟9. 套用認證及時間表（圖 4-40）

圖 4-40 套用認證及時間表

步驟10. 非上班時間要拒絕。（圖 4-41）

新增第二條條例，拒絕所有連線。

圖 4-41 拒絕非上班時間的連線

步驟11. 完成的管制規則，共需要 2 條管制規則完成這一份工作，一個是上班時間，另一個是非上班時間，要注意優先權順序。（圖 4-42）

圖 4-42 完成的管制規則

4-3-3、範例三：管制 IP 進入

範例三：內部伺服器區(Zone3) 禁止上網際網路，同時只有內部特定 IP 位址能進入

建立管制規則時，在介面的選擇上，NG-UTM 能選的只有來源介面，並沒有目的介面的選項，因此在範例中，要限制某些特定的來源 IP 位址進入內部伺服器區中，除了需要事先選定來源 IP 位址外，也要事先定義目的的 IP 位址跟區段。

步驟1. 建立來源的位址表跟群組

在【管理目標】>【位址表】>【位址表】，建立可以進入 ERP 跟資料庫的人，他使用電腦跟 IP 位址，首先到位址表建立這些名單，方便管制規則選用，也可以跳過這一個項目，直接在管制規則中輸入 IP 位址，建立位址表時，可以是單一個 IP 位址，IP+MAC 位址，MAC 位址，一個網段或是 Domain。（圖 4-43）

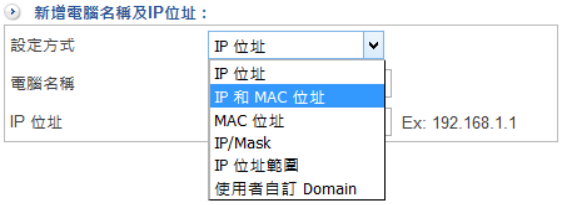


圖 4-43 建立來源位址表

在【管理目標】>【位址表】>【位址表群組】，把這一些數個不同的來源 IP 位址或是網段集合成一個群組。（圖 4-44）

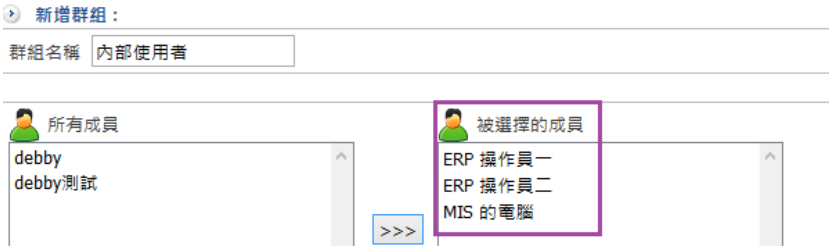


圖 4-44 建立來源位址群組

步驟2. 建立 Zone3 伺服器區的目的 IP 位址表或是區段

在【管理目標】>【位址表】>【位址表】建立新的伺服器 IP 區段。（圖 4-45）

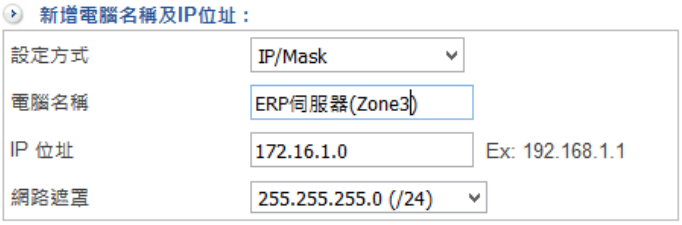


圖 4-45 建立目的位址

步驟3. 建立管制規則

此次要限制的來源介面是 Zone 1 有線區中的特定 IP 位址可以進入目的網路的特定 IP 位址，在基本設定區如下，針對符合條件的網路封包讓他進入目的網段。（圖 4-46）

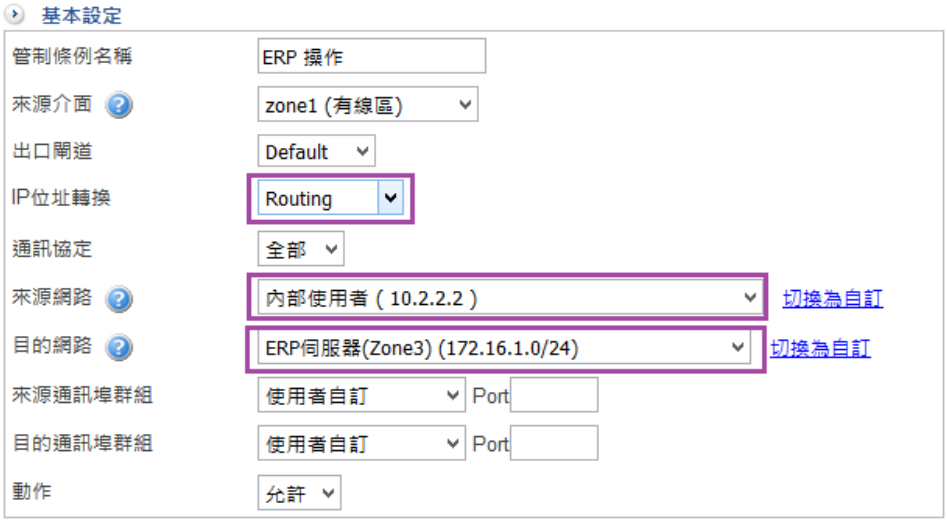


圖 4-46 完成的管制規則

步驟4. 禁止 Zone3 的網路上網（圖 4-47）

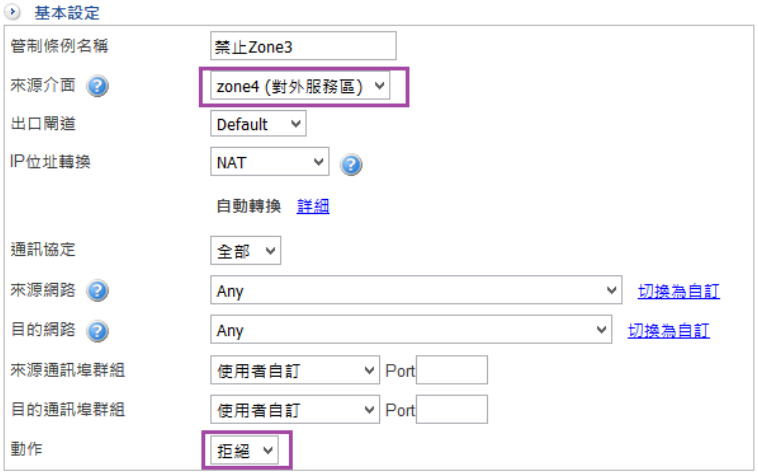


圖 4-47 禁止 Zone3 上網

步驟5. 完成後的管制規則（圖 4-48）

圖 4-48 完成的管制規則

4-3-4、範例四：Web 服務器

範例四：對外服務區(Zone4) 只有 Web 服務才能進出，並啟用 IPS 跟防火牆防護

對外的 IP 位址是在 Zone 5 上定義，而實際對外的服務是在 Zone 4 上，2 者的 IP 位址不一樣，所以管理者要事先規劃哪一些合法的 IPV4 的 IP 位址，要對應到內部的哪些 IP 位址上。

步驟1. 建立那些 Zone5 的 IP 位址是要被對應到 Zone 4 上。

在【管理目標】>【位址表】>【位址表】，建立新的對外服務 IP 位址表，建立位址表的目的是方便在管制規則中選擇套用，如果不建立位址表，也可以在管制規則中直接填入 IP 位址。（圖 4-49）

圖 4-49 建立位址表

同時也建立會在 Zone 5 提供對外服務的 2 筆 IP 位址。（圖 4-50）

圖 4-50 完成的位址表

步驟2. 建立要開放給使用者使用的服務表

在【管理目標】>【服務表】>【服務群組】建立提供對外的服務，一台是 Web Server ，另一台是 Mail Server，Web Server 同時提供 DNS Server 查詢，Web Server 的服務表範例如下：（圖 4-51）

圖 4-51 自訂服務

步驟3. 建立 IPS 保護

在【IPS】>【IPS 設定】中建立一條 IPS 的規則，阻擋高風險，其他的風險等級只要記錄就可以。（圖 4-52）

新增 IPS

群組名稱	IPS 防護
模式	◉ 初階模式 ○ 進階模式

風險程度	記錄	阻擋
⊞ High Risk (1597)	☑	☑
⊞ Medium Risk (1816)	☑	☐
⊞ Low Risk (607)	☑	☐

圖 4-52 選擇 IPS 模式及阻擋

步驟4. 建立 Web 伺服器的管制規則

在建立外部對內的對應機制時，有幾個地方需要特別注意：（圖 4-53）

1.來源介面：哪一些來源介面可以進入對外服務的伺服器區，除了原來 Zone 5 對外的網際網路上的電腦外，管理者可以再挑選，例如內部的有線區跟無線區，也要能看到自家公司的網站，這時候就要挑選這些來源介面，否則就算是內部的使用者，也無法看到網站內容，基本上沒開任何管制規則，Zone 跟 Zone 間是完全不通。

基本設定

管制條例名稱	
來源介面	☑ zone0 ☑ zone1 ☑ zone2 ☑ zone4 ☑ zone5 ☑ ppp4001 ☑ PPTP ☑ SSLVPN
出口閘道	.189
IP位址轉換	IP 對應
	172.16.5.200
通訊協定	全部
來源網路	Any 切換為自訂
目的網路	Web 伺服器 (61.22.23.20) 切換為自訂
來源通訊埠群組	使用者自訂 Port
目的通訊埠群組	Web Server Port
NAT	☐
動作	允許

圖 4-53 管制規則跟 IP 對應

2.目的網路：對外的合法 IP 位址，當從網際網路來要到目的地 IP 位址時，NG-UTM 會如何處理這一個封包，範例為 61.22.23.20。

3.目的通訊埠群組：選擇前面建立的 Web 服務群組，如果目的位址轉換的機制是選擇 Port 對應跟伺服器負載均衡，對應的 Port 會另外設置，這個地方就不需要選用，在此範例是選擇 IP 對應，所以需要選擇哪一些服務要導入對外的伺服器。

4.閘道：對外閘道。

5.IP 對應：有 3 種模式，這裡使用 IP 對應，也就是 1 對 1NAT，真正對外服務的 Web 伺服器 IP 位址是 172.16.5.200。

步驟5. 套用 IPS 防護跟防火牆防護（圖 4-54）

圖 4-54 套用 IPS 跟防火牆防護

步驟6. 建立完成的管制規則（圖 4-55）

圖 4-55 完成的管制規則

4-3-5、範例五：郵件伺服器

範例五：對外服務區(Zone4) 只有 Mail 服務才能進出，並啟用 垃圾跟病毒郵件過濾

步驟1. 定義郵件服務器的 IP 位址

在【管理目標】>【位址表】>【位址表】建立對外的郵件伺服器 IP 位址。（圖 4-56）

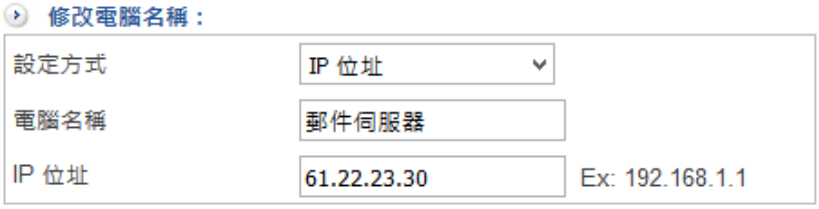


圖 4-56 建立郵件伺服器的位址表

步驟2. 啟用垃圾郵件跟掃毒功能

在【郵件管理】>【郵件過濾與記錄】>【郵件過濾與記錄】，設定要啟用的功能，並注意其他相關的配置。（圖 4-57）

圖 4-57 郵件過濾設定

步驟3. NG-UTM 為垃圾郵件閘道時，需要跟後端的設備驗證有效帳號

在【郵件管理】>【郵件過濾與記錄】>【有效帳號】中設定有效帳號的來源，並限定非定義的網域，不處理垃圾郵件過濾機制。（圖 4-58）

圖 4-58 有效帳號

管理者要注意同一台郵件伺服器中是否配置多網域，如果有則需要把每一個網域名稱都填入網域清單中，否則會出現同一台郵件服務器，A 網域會進垃圾郵件過濾，B 網域卻不會的窘境。

在有效清單設定中，預設是關閉，要避免非設定網域的郵件進入，所以將他啟用。

步驟4. 要不要啟用 SMTP 郵件防護

駭客會一直用 SMTP 寄信驗證，往往郵件伺服器承受不起這樣的攻擊，NG-UTM 可以提供後端郵件伺服器這樣的保護機制。（圖 4-59）

圖 4-59 SMTP 防護

步驟5. 確認垃圾郵件的處理方式

在【郵件管理】>【垃圾郵件過濾】>【基本設定】，設定垃圾郵件的處理方式及要不要讓使用者可以自行登入垃圾郵件區，取回被誤判的垃圾郵件。（圖 4-60）

圖 4-60 垃圾郵件設定

步驟6. 垃圾郵件清單

前面垃圾郵件處理是放在隔離區並發送清單時，管理者需要啟用清單發送機制並定下發送時間。（圖 4-61）

圖 4-61 垃圾郵件發送清單

步驟7. 中毒郵件的處理

在【郵件管理】>【郵件掃毒】>【郵件掃毒】設定掃毒引擎、跟中毒後處理方式。（圖 4-62）

圖 4-62 病毒郵件設定

步驟8. 建立 Mail 伺服器的管制規則

1.來源介面：哪一些來源介面可以進入對外服務的伺服器區，除了原來 Zone 5 對外的網際網路上的電腦外，管理者可以再挑選，例如內部的有線區跟無線區，也要能看到自家公司的網站，這時候就要挑選這些來源介面，否則就算是內部的使用者，也無法看到網站內容。（圖 4-63）

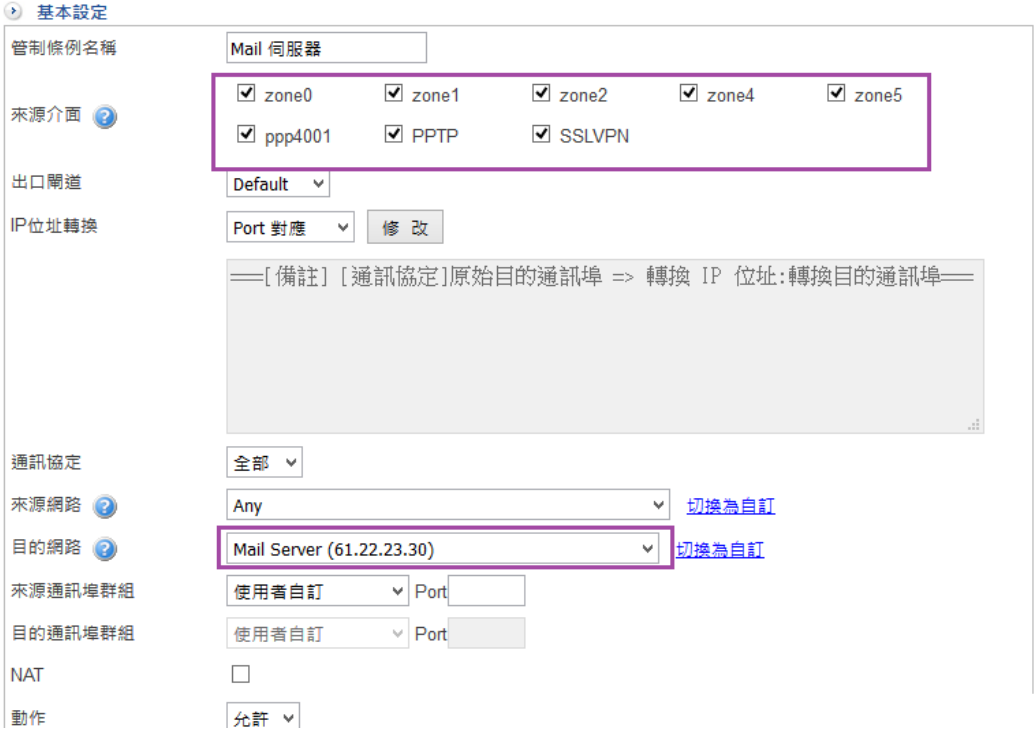


圖 4-63 管制郵件伺服器基本設定

2.目的網路：對外的合法 IP 位址，範例為 61.22.23.30。

3.閘道：對外閘道。

4.IP 對應：有 3 種模式，這裡使用 Port 對應，也就是對內 PAT 機制，真正對外服務的 IP 位址是 172.16.5.201，點選修改按鈕後會出現新的對話框，再把要提供服務的 Port 輸入，在 Mail Server 中提供 SMTP/SMTPS、POP3/POP3S、IMAP/IMAPS 及 DNS 等服務。（圖 4-64）

Port 對應修改

備註	通訊協定	原始目的通訊埠		轉換 IP 位址	轉換目的通訊埠	刪除
SMTP	TCP	使用者自訂	Port 25	172.16.5.201	25	✕
SMTPS	TCP	使用者自訂	Port 465	172.16.5.201	465	✕
POP3	TCP	使用者自訂	Port 110	172.16.5.201	110	✕
POP3S	TCP	使用者自訂	Port 995	172.16.5.201	995	✕
IMAP	TCP	使用者自訂	Port 143	172.16.5.201	143	✕
IMAPS	TCP	使用者自訂	Port 993	172.16.5.201	993	✕
DNS	UDP	使用者自訂	Port 53	172.16.5.201	53	✕
	TCP	使用者自訂	Port			✕

圖 4-64 Port 對應

使用 Port 對應時發現，來源 Port 跟目的 Port 是分開填寫，也就是說外面的 SMTP25 Port 可以轉入內部的任何 Port ， 同樣的在這個模式下，IP 位址也是可以任意轉換。

例如，61.22.23.30 的 SMTP 轉入 172.16.5.201 的 SMTP，61.22.23.30 的 POP3 轉入 172.16.5.202 的 POP3。

修改完成後顯示如下：（圖 4-65）

指定閘道　對外線路

IP位址轉換　○None ○來源地址轉換 ◉目的地址轉換

Port 對應　修 改

```
==[備註] [通訊協定]原始目的通訊埠 => 轉換 IP 位址:轉換目的通訊埠==
[SMTP] [tcp]SMTP(25) => 172.16.5.201:25
[SMTPS] [tcp]SMTP over SSL(465) => 172.16.5.201:465
[POP3] [tcp]POP3(110) => 172.16.5.201:110
[POP3S] [tcp]POP3 over SSL(995) => 172.16.5.201:995
```

圖 4-65 Port 的對應關係

步驟9. 套用 SMTP 紀錄、POP3 紀錄跟防火牆防護

SMTP 伺服器位於 Zone 4 ，所以是屬於近端。（圖 4-66）

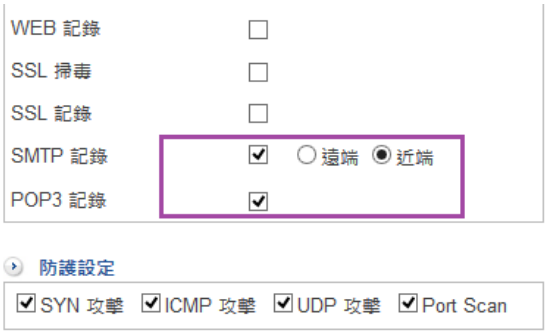


圖 4-66 套用 SMTP 跟 POP3 紀錄

步驟10. 建置完成的管制規則（圖 4-67）

圖 4-67 完成的管制規則

第 5 章 管理目標

NG-UTM 是以物件導向管理整台設備，事先定義所有的物件或是目標後，再到管制條例中禁止或是放行，除了傳統的位址表、應用程式跟 URL 可以當成管理目標外，連 ZONE 、介面位址、路由表甚至指定閘道都是管理目標，在此章，介紹的就是傳統的管理目標。

設定管理目標的目的是讓管理者在建立管制條例時，更容易辨識每一個條例的目的及用途，也可以不設定任何管理目標，直接在管制條例中輸入 IP 位址跟 Port 進行管制動作。

5-1、位址表

NG-UTM 的位址表支援 IPV4 跟 IPV6 位址模式，點選主選單 MENU 上方的灰色按鈕 IPv6 ，代表要將顯示跟設定切換到 IPV6 模式，NG-UTM 將會切換到設定 IPV6 位址模式。IPv4 代表目前顯示/設定的是 IPV4 的位址模式，IPv6 代表顯示/設定的是 IPV6 的位址模式。這 2 個按鈕適用於整個系統，在需要設定 IP 位址的地方，點選灰色的圖示，將會設定畫面切換成 IPV4 或是 IPV6 模式。

5-1-1、位址表

事先定義好為位址表，讓管制條例的建立跟理解它的目的更清楚明瞭，每一個位址表可以是單一個 IP 位址，IP 網段或是 IP 區段。

輔助選取

這個功能限定 IPV4 使用，任何設備，只要有網路封包經過 NG-UTM，不論是外部還是內部，系統都會把它紀錄下來，方便管理者建立位址表，點選 輔助選取 的圖示，列出所有的 預設電腦名稱、IP 位址跟 MAC 位址，甚至連從 DHCP 伺服器取得固定 IP 位址也可以使用，選擇要增加的 IP 或是 MAC 位址後，按下 ✚ 新增 鈕，就自動把資料加入位址表中。（圖 5-1）

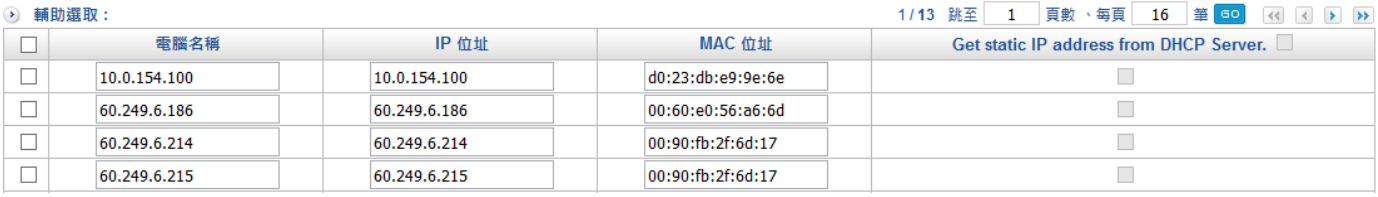


圖 5-1 選取 IP 位址

新增位址表

按下 ✚ 新增 鈕後，就開始建立位址表，總共有 6 種位址表建立方式，每一種方式都有它的使用上目的。

1、IP 位址

IPV4/IPV6 共用設定，只用 IPV4 位址或是 IPV6 位址辨識使用者，適用於每一個電腦都是使用固定 IP 位址的網路環境。

- 【電腦名稱】：這個 IP 位址的名稱，例如，張三的電腦。
- 【IP 位址】：輸入 IP 位址，例如，192.168.1.1。

2、IP 和 MAC 位址

只在 IPV4 有效，用 IPV4 位址跟 MAC 位址綁定使用者，適用於每一個電腦都是使用固定 IP 位址或是透過 DHCP 取得固定 IP 位址的網路環境，最重要的是電腦到 NG-UTM 間沒有經過 Layer 3 路由器。

- 【電腦名稱】：這個 IP 位址的名稱，例如，張三的電腦。
- 【IP 位址】：輸入 IPV4 位址，例如，192.168.1.1。
- 【MAC 位址】：這部電腦的真實 MAC 位址，例如，00:01:02:03:04:05。
- 【DHCP】：在 DHCP 環境，可以利用 DHCP 伺服器發放固定 IP 位址給同一個 MAC 位址，勾選後，代表這一部電腦會由 DHCP 伺服器發放固定的 IPV4 位址。

3、MAC 位址

只在 IPV4 有效，只用 MAC 位址綁定使用者，而不管它的 IP 位址。

- 【電腦名稱】：這個 IP 位址的名稱，例如，張三的電腦。
- 【MAC 位址】：這部電腦的真實 MAC 位址，例如，00:01:02:03:04:05。

4、IP /Mask

IPV4/IPV6 共用設定，用 IPV4 位址或是 IPV6 位址加上子網路遮罩的方式，辨識一整個區域的使用者。

- 【電腦名稱】：這個 IP 位址的名稱，例如，工程部全部的電腦。
- 【IP 位址】：輸入 IP 位址，例如，192.168.1.1。
- 【網路遮罩】：選擇適當的網路遮罩，例如，255.255.255.0/24。

5、IP 位址範圍

IPV4/IPV6 共用設定，用 IPV4 位址或是 IPV6 位址的開始 IP 位址跟結束 IP 位址，辨識一整個區域的使用者。

- 【電腦名稱】：這個 IP 位址的名稱，例如，工程部全部的電腦。
- 【開始 IP】：輸入這一個範圍的開始 IP 位址，例如，192.168.1.1。
- 【結束 IP】：輸入這一個範圍的結束 IP 位址，例如，192.168.1.100，這樣代表工程部全部電腦有 100 個 IPV4 位址。

6、使用者自訂 Domain

IPV4/IPV6 共用設定，用 Domain 的方式，辨識一整個區域的使用者，適合外部網路伺服器或是有做 Domain 正解的網路環境。

- 【電腦名稱】：這個網域的代表名稱，例如，張三的家。
- 【Domain】：輸入 Domain 資訊，可以輸入多筆網域資料，每一筆為一行，且支援萬用符號 *，例如，*.example.com 或是 example.com.*。

5-1-2、位址表群組

每一個位址表是一個單獨 IP 位址或是 IP 網段，建立好的位址表可以再組合成位址表群組，位址表群組的成員除了是位址表外，也可以是別的位址表群組，按下 新增 鈕後，就開始建立位址表群組。（圖 5-2）

- 【群組名稱】：這個位址表群組名稱，例如，2F 的電腦。
- 【所有成員】：在位址表中建立完成的位址表名稱，通通會在這裡顯示，供管理者選取。
- 【被選擇的成員】：選擇要加入這個位址表群組的位址表，再點選 >>> 就加入。
- 【所有其他群組】：已經建立在位址表群組中的位址表群組，通通會在這裡顯示，供管理者選取。
- 【被選擇的其他群組】：選擇要加入這個位址表群組的位址表群組，再點選 >>> 就加入。
- 【使用者自訂】：沒被事先定義的也可以在此區手動加入。

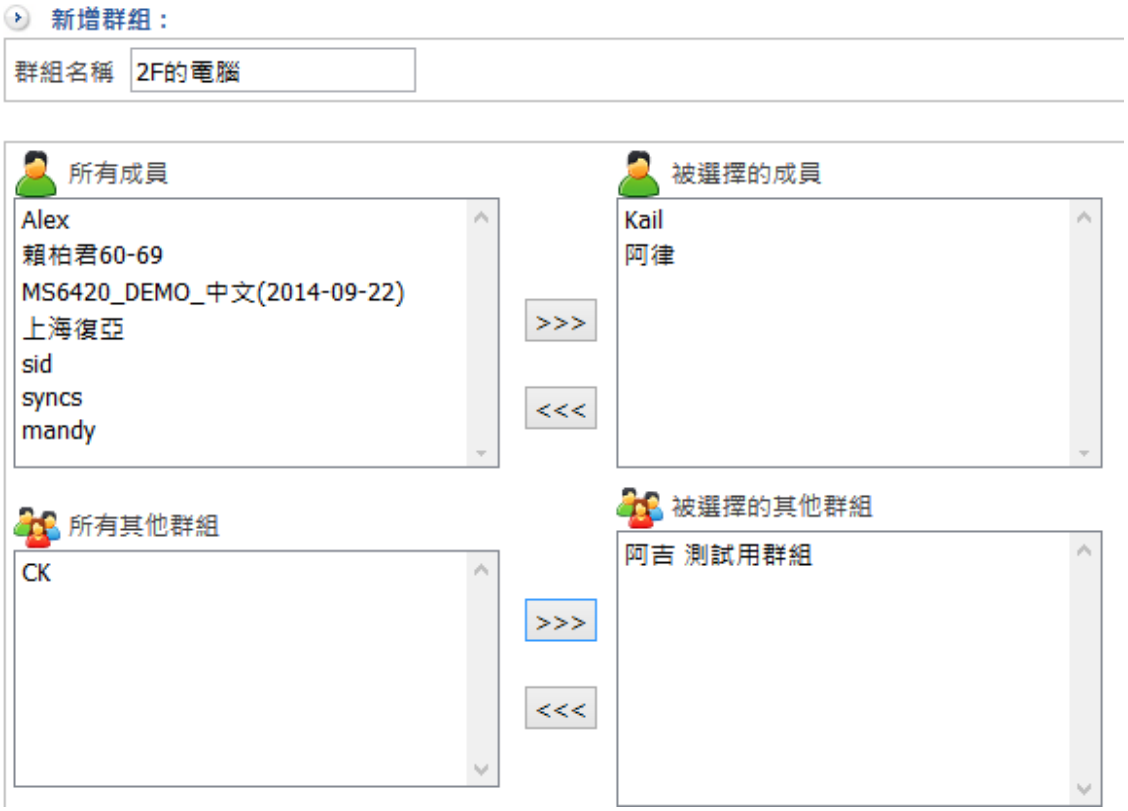


圖 5-2 選取位址表群組

5-2、服務表

TCP 協定和 UDP 協定提供各種不同的服務，每一個服務都有一個 TCP 埠(TCP Port)號碼或 UDP 埠(UDP Port)號碼代表，如 TELNET(23)，FTP(21)，SMTP(25)，POP3(110)，...等。

在輔助選取中會事先定義基本服務表，包含了比較常用已預告定義的 TCP 服務或 UDP 服務。此類服務不能修改也不可刪除。此外使用者也可依自己的需求到自訂服務表設定適當 TCP 埠和 UDP 埠號碼。在自訂服務時，客戶端埠(Client Port)設定的區間一般為 1024：65535，伺服器端埠(Server Port)號碼則是設定在 0:65535 之間。

服務表中定義的服務跟應用程式中定義的服務稍微有點不一樣，以 HTTP 協定為例，在服務表中把他定義成 TCP 80 Port 代表 HTTP 協定，但是在實際運作上，在 TCP 80 Port 的封包不一定都是 HTTP (Web)，有時跑 HTTP 的也不一定要在 TCP 80 Port 上。

在應用程式中定義的 HTTP 協定，他不會管來源跟目的 Port 號，只要封包內容是執行 HTTP(Web) 協定的，通通都算，所以應用程式對於執行協定的辨識是更準確。

如何運用服務表

系統管理者可以在【服務表】的【服務群組】選項中，新增服務群組名稱，將要提供的服務包含進去。

有了服務群組的功能，管理者在制訂管制條例時可以簡化許多流程。例如，有 10 個不同 IP 位址可以對伺服器存取 5 個不同的服務，如 HTTP、FTP、SMTP、POP3 和 TELNET，如果不使用服務群組的功能，總共需制定 10x5=50 條管制條例，但使用服務群組名稱套用在服務選項上，則只需一條管制條例即可達到 50 條管制條例的功能。

5-2-1、基本服務表

在新增服務群組時，點選 輔助選取 的圖示時，就會自動出現 NG-UTM 內建的基本服務表，管理者只要選取想要的服務表就可以，切換 TCP 、 UDP 或是其他通訊協定，就列出使用的通訊協定 。(圖 5-3)

- 【TCP】：常用的 TCP 類型服務，例如，SSL、HTTP 等。
- 【UDP】：常用的 UDP 類型服務，例如，DNS、SNMP 等。。
- 【其他通訊協定】：其他不常使用到的服務類型，例如 ，TFTP、RDP 等。

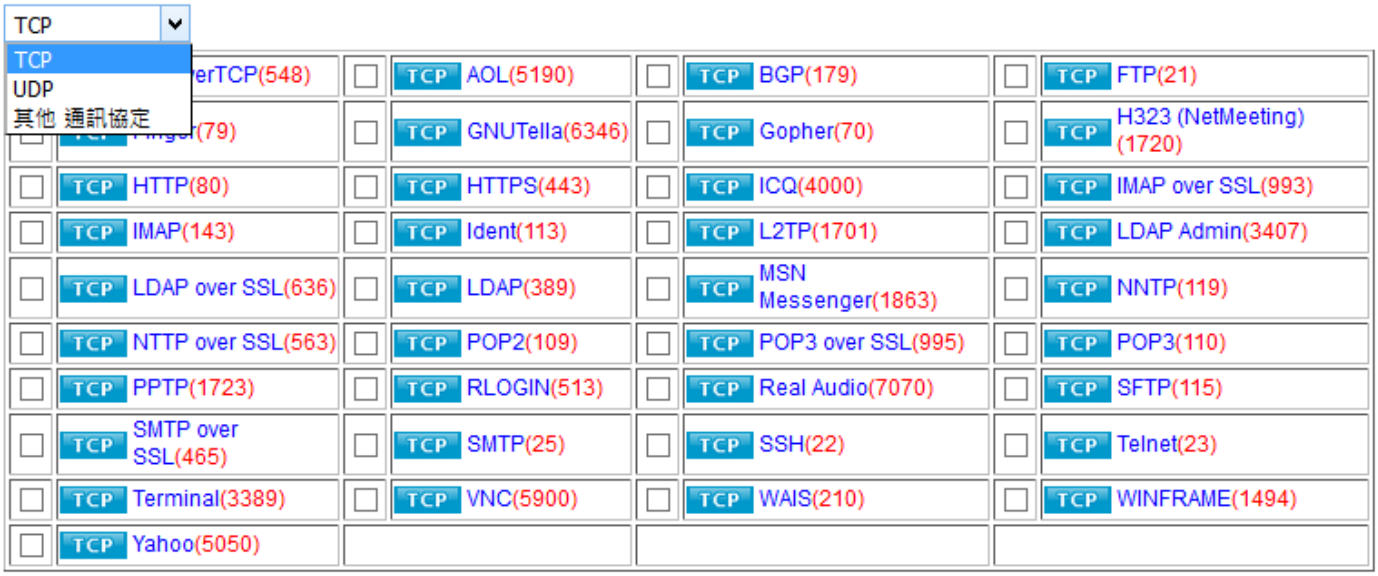


圖 5-3 基本服務表

服務表圖示說明

服務表圖示的詳細說明，這一些圖示通用在整個 NG-UTM 上。

圖示	說明
ANY	任何服務。
TCP	TCP 服務，如：Gopher、ICQ、Ident、LDAP、NTTP over SSL、PPTP、SFTP、SSH 、 Terminal 、 WINFRAME 、 AFPoverTCP 、 FTP 、 H323 、 L2TP 、 MSN Messenger、POP2、SMTP over SSL、Yahoo、AOL、Finger、HTTP、IMAP over SSL、LDAP Admin、NNTP、POP3 over SSL、RLOGIN、SMTP、VNC、BGP、GNUTella、HTTPS、IMAP、LDAPover SSL、POP3、Real Audio、Telnet、WAIS
UDP	UDP 服務，如：DNS、TFTP、NTP、SNMP、IKE、SYSLOG、RIP、UUCP 等。

5-2-2、服務群組

建立新的服務群組時，一開始會出現 8 筆空白的資訊，管理者從編號 1 開始依序加入服務表，萬一要加入這個服務群組的服務項目超過 8 個，按下 » More 後，會再多 8 筆空白的資訊。(圖 5-4)

- 【服務及服務群組名稱 】：辨識這個服務群組的名稱，例如，郵件服務器。
- 【輔助選取】：選取內建的服務表。
- 【通訊協定】：選擇這一筆服務是使用 TCP、UDP 或是自訂的通訊協定。
- 【使用的通訊埠】：通訊服務使用的開始跟結束埠號，例如，SMTP 只用 TCP 25 ，填入 25:25，POP 只用 TCP 110 ，填入 110:100，如果填入是 0:65535，代表所有埠號都滿足，他就等於 ANY 。

新增服務及服務群組：

服務及服務群組名稱 郵件伺服器 輔助選取 » More

	通訊協定	使用的通訊埠
1	◉TCP ○UDP ○自訂	25 : 25
2	◉TCP ○UDP ○自訂	110 : 110
3	○TCP ◉UDP ○自訂	53 : 53
4	◉TCP ○UDP ○自訂	:
5	◉TCP ○UDP ○自訂	:

圖 5-4 建立服務群組

建立新的服務群組後，NG-UTM 會把所有定義好的服務群組列表，同時標示他使用的埠號。(圖 5-5)

自訂服務及服務群組名稱： 1 / 1

	服務及服務群組名稱	
☐	eyecloud	TCP : 443,2000,50000:50100
☐	BBS_FTP	TCP : 9021,5000:5200
☐	FTPServer	TCP : 5201:5400,21
☐	CMS	TCP : 40000:40001
☐	MailService	TCP : 993,143,389,995,110,465,25,88,8080,8888,888,1998:1999,25 UDP : 53
☐	DemoSSLVPN	TCP : 2245
☐	DemoMail	TCP : 993,143,389,995,110,465,25

圖 5-5 服務群組列表

5-3、時間表

NG-UTM 提供系統管理者時間表的設定，管理者根據實際的需求，事先設定啟用的時間，在【管制條例】中套用時間表，讓這條例在特定時間內生效，相同的功能條例可以重複套用不同的時間表，變成 2 個不同的條例，藉以控管不同的時間需求。

時間表

時間表的設定週期有 2 種，模式一：以周為週期，定義每天生效的時間，模式二：使用者自訂週期跟時間。

- 【時間表名稱 】：辨識這個時間表的名稱，例如，白天規則、晚上規則。
- 【設定模式】：共有 2 種模式可以選取。

  模式一：以周為週期，定義每天生效的時間，有三種選擇，關閉、全天跟開始到結束時間，設定起始時間 00:00 ~ 結束時間 00:00 代表的意義就是全天。(圖 5-6)

圖 5-6 以周為週期的時間表

  模式二：使用者自訂週期跟時間，管理者設定特定日期下會生效的時間表，例如，2016 7 月 1 日開始到 2016 12 月 31 日結束。(圖 5-7)

圖 5-7 自訂週期的時間表

在管制條例列表中出現 的圖示，代表這一個條例在特定時間下才會生效。

5-4、頻寬管理

NG-UTM 可以管理經過介面的網路服務封包的傳輸速度，藉由事先規劃的頻寬表，管理者可以精準地控制每一個條例經過 ZONE 的上傳、下載的頻寬，再加上頻寬優先權的概念，讓高優先權的網路封包可以快速地通過，在配置上，有 2 種模式可以選擇，一種是每個條例的頻寬管理，另一種是這一個條例內每個來源 IP 位址的頻寬管理。

在頻寬 管理上，因為是以 ZONE 介面串起整個網路，所以需要事先定義每一個 ZONE 的上、下載速度，例如，ZONE 1 有包含 2 個實體 Port 分別是 Port A 跟 Port B，每一個實體 Port 的連線速度都為 1Gbps，在頻寬表選用上網服務 10Mbps 並套用在每個來源 IP 位址，這樣的設定代表不論從 Port A 或是 Port B 過來的 IP 位址，只要是屬於這個 ZONE 的，上傳、下載都會被限制在 10Mbps 。

設定介面速度

設定每一個介面的最快網路速度，分別是上傳、下載頻寬。這裡的上傳、下載頻寬是以實體 Port 為觀點，進去實體 Port 的網路封包為上傳，從實體 Port 送到下端設備的網路封包為下載頻寬。

這樣的配置在網路速度是對稱性(上傳跟下載的速度都一樣)的內部網路或是交換器上不會有問題，但是在非對稱性的 WAN 類型網路就有點方向性的問題，思考一下線路商提供給上傳跟下載速度，對承接網路封包的 NG-UTM 來說，剛好是相反的方向，所以對於 WAN 類型的網路，例如，ADSL，設定 ZONE 速度時就需要想一下這個方向性問題。(圖 5-8)

QoS 設定：

介面	Port	上傳速度	下載速度
zone0	06	1024000 Kbps	1024000 Kbps
zone1	01	1024000 Kbps	1024000 Kbps
zone2	02	1024000 Kbps	1024000 Kbps
zone3	03	1024000 Kbps	1024000 Kbps

圖 5-8 自訂介面的速度

NG-UTM 預設會把所有的 ZONE 上傳跟下載速度設為 1Gbps (1024Mbps=1024000Kbps)，同時把這個 ZONE 有包含哪些實體 Port 一併列出來，管理者可以修改速度，符合實際的線路狀況後儲存，這個速度就會變成設定頻寬表時最高的速度限制。

5-4-1、QoS 設定

設定頻寬表時分成保證跟最大 2 個數值，保證是指當頻寬壅塞時，他獲得的保證速度，最大是指當頻寬不壅塞時，根據優先權後可以再取得多少頻寬？優先權是 1~7 的數字，數字越低代表他的優先權越高。

頻寬運作模式有 2 種，分別是【每個條例能使用的頻寬 】跟【每個來源 IP 能使用的頻寬 】，詳細說明如下：

模式一、每個條例能使用的頻寬

當頻寬表套用在條例時，每一個進入條例的來源 IP 位址，不論是 IPV4 或是 IPV6 ，網路封包的總數上限就是頻寬表的設定值，就是大家共用這一個頻寬表分配的頻寬，例如，192.168.1.2 跟 192.168.1.3 都符合頻寬表 10Mbps / 10 Mbps 的條例，當 192.168.1.2 使用量是 9.9Mbps /9.9 Mbps 時，192.168.1.3 只能分配到 0.1Mbps / 0.1Mbps 的頻寬。

模式二、每個來源 IP 能使用的頻寬

當頻寬表套用在條例時，每一個進入條例的來源 IP 位址，不論是 IPV4 或是 IPV6 ，都可以使用到頻寬表的設定值，就是每一個 IP 位址都是頻寬表分配的頻寬，例如，192.168.1.2 跟 192.168.1.3 都符合頻寬表 10Mbps / 10 Mbps 的條例，當 192.168.1.2 最高可以用到 10Mbps / 10 Mbps，192.168.1.3 也能用到 10Mbps / 10 Mbps 的頻寬。

在這個模式下要注意一下 IP 位址數量跟分配頻寬表加總的最高值會不會超出介面能提供的最高速度，例如，這個條例估計有 100 個 IP 位址，每個人分配 20Mbps，當這 100 個 IP 通通上線且使用最高的分配頻寬時，他的總額是 100*20Mbps = 2000Mbps = 2G，這已經超過介面的最高數值 1 Gbps，這樣的狀況會導致頻寬分配不準確的情況。

設定模式則有 2 種：(圖 5-9)

基本模式

以 Zone 為單位，不管這個 Zone 包含了幾個實體介面，例如，把每一個 WAN 線路都設定獨立的 WAN Zone，則適合套用這樣模式。

進階模式

以實體網路介面當作頻寬管制基礎，例如，把 3 個線路綁成一個 WAN ZONE，選擇這個模式，會把每一個線路獨立出來讓管理者管理。

<table>
<tr><th>基本模式</th><th>進階模式</th></tr>
<tr><td>
<table>
<tr><th>介面</th><th></th></tr>
<tr><td>zone0
(zone0)</td><td>保證 0 Kbps (1~1024000)
最大 0 Kbps (1~1024000)</td></tr>
<tr><td>zone1
(WAN)</td><td>保證 10240 Kbps (1~1024000)
最大 102400 Kbps (1~1024000)</td></tr>
</table>
</td><td>
<table>
<tr><th>介面</th><th>Port</th><th></th></tr>
<tr><td>zone0
(zone0)</td><td>MGMT</td><td>保證 0 Kbps (1~1024000)
最大 0 Kbps (1~1024000)</td></tr>
<tr><td rowspan="2">zone1
(WAN)</td><td>Port01</td><td>保證 10240 Kbps (1~1024000)
最大 102400 Kbps (1~1024000)</td></tr>
<tr><td>Port02</td><td>保證 10240 Kbps (1~1024000)
最大 102400 Kbps (1~1024000)</td></tr>
</table>
</td></tr>
</table>

圖 5-9 設定模式比較

新增頻寬表

新增一筆頻寬表。(圖 5-10)

- 【QoS 名稱 】：辨識這個頻寬表的名稱，例如，白天上網、晚上開放。
- 【優先權】：當介面還有空閒的頻寬可以使用時，NG-UTM 根據優先權將剩餘的頻寬分配給使用者，讓他們有機會可以到達設定的最大頻寬。
- 【頻寬模式設定】：共有 2 種模式可以選擇，分別是【每個條例能使用的頻寬 】跟【每個來源 IP 能使用的頻寬 】，詳細說明如前面所述，預設選擇是【每個條例能使用的頻寬 】。
- 【設定模式】：共有 2 種模式可以選擇，分別是【基本模式 】跟【進階模式 】。
- 【介面-保證 】：選擇頻寬表要在哪一個介面套用，系統會提醒設定者最高的網路速度，此時設定的就是當 NG-UTM 網路壅塞，系統會保證這個條例使用者可以使用的頻寬。
- 【介面-最大 】：系統會提醒設定者最高的網路速度，此時設定的就是當 NG-UTM 網路不壅塞，根據優先權設定，系統再分配剩餘的頻寬給這個條例使用者使用的頻寬。

圖 5-10 頻寬表設定

在設定頻寬表時務必要注意設定的介面，因為 NG-UTM 是以介面為管理基礎，如果在頻寬表設定頻寬時是設定在 ZONE0 介面 ，但是在管制條例中卻是套用在其他 ZONE，這樣會導致要管理的 IP 位址或是服務無法準確的管理。

5-4-2、QoS 列表

每一個設定完成的 QoS 都會在這裡列出，方便管理者查詢。

5-5、應用程式管制

NG-UTM 是以 DPI (Deep Packet Inspection) 為基礎的 UTM，所有經過的流量都會經過 DPI 的分類及管理，使用 DPI 技術管理應用程式，跟傳統以 TCP/UDP Port 的管制更精準，以加密類型的網站 HTTPS 為例，使用 SSL 加密技術，確保瀏覽網頁內容經過網際網路後仍安全無慮，SSL 的加密是用 TCP 443 為溝通的埠號。

在以前的防火牆設計中，要管理 HTTPS 型的網站，只要把對外的 TCP 443 封掉，內部就無法瀏覽加密型的網站，但是這樣動作在目前的網路上，卻會出現問題，因為安全因素，很多網路通訊軟體開始使用 SSL 加密技術，例如，SSL VPN，封掉 TCP 443 代表 HTTPS 跟 SSL VPN 都無法使用。

為了更精準的分辨這一些應用程式，單純使用 Port 分類的就沒辦法滿足現在的網路需求，因此 NG-UTM 導入 DPI 技術，它並不是單純使用 TCP / UDP 的埠號為判斷依據，更深層的檢查封包內容，根據傳遞的內容判斷往來的封包是執行那些服務，所以這樣的判斷方式比傳統的防火牆更準確。

NG-UTM 目前能夠辨識超過 900 種的應用程式，同時也使用自動更新特徵值技術，不定期的更新這些應用程式的特徵值跟數量，管理者只需要設定好自動更新的選項，其他的就讓系統自動執行，這些應用程式同時會出現在統計分析的項目上。

因應雲端時代，很多網站提供軟體即服務(Software as a Service，SAAS)的服務，進入網站，不需要安裝任何軟體，就可以完整的使用該軟體提供的服務，例如 WebQQ，WebSkype 等，尤其是這些網站通常使用的是 HTTPS 協定或是 IPV4/IPV6 雙位址模式，管制 IPV4 位址並不代表同時封掉 IPV6 的位址，再加上用 SSL 加密技術，一般的 Firewall 或是 UTM 通常無法禁止這一類型的 SAAS 網站或是服務，造成網路管理者管理上的困擾，此時，可以搭配 NG-UTM 的另一項 URL 管理功能就可以管理這一些 SAAS 的服務。

應用程式資訊

NG-UTM 的應用程式的特徵值需要額外的授權，授權到期後，系統就不會在更新特徵值，所以管理者設定的管制項目可能有不準確的狀況，相關的啟用就需要在這裡設定。(圖 5-11)

- 【授權 】：要啟用 DPI 的應用程式需要匯入授權碼，點選【瀏覽】並匯入就完成。
- 【授權期限 】：目前應用程式的到期日。
- 【服務狀態 】：應用程式辨識是起用或是關閉。

圖 5-11 應用程式資訊

5-5-1、應用程式管制

要管理超過 900 種的應用程式管理的有一點複雜，因此 NG-UTM 根據每一個應用程式的屬性，分成 17 大類，管理者先選擇這 17 類後，再從中選擇要管理的應用程式，選擇完成數個應用程式後，給它一個名稱，建立完成後就可以到管制條例中選用，在管制條例上選用的方式跟服務表示相同。

新增應用程式管制

管理者可以新增很多筆應用程式或是某個應用程式群組內包含多種服務，建立好的服務就到管制條例中選用。

- 【群組名稱 】：辨識這個應用程式的名稱，例如，上網組、禁止的服務。
- 【動作 】：針對每一個應用程式管制，有 3 個選項分別是阻擋、阻擋+紀錄及頻寬管理，相關說明如下：
  - ◆ 阻擋：把比對符合特徵值的應用程式阻擋，不讓他使用。
  - ◆ 阻擋+紀錄：把比對符合特徵值的應用程式阻擋，並且記錄下哪一位使用者何時使用。
  - ◆ 頻寬管理：符合特徵值的應用程式進入頻寬管理機制，例如，符合 LINE/SKYPE 的應用程式，只能使用 500Kbps 的網路頻寬。
- 【搜尋】：輸入關鍵字，就可以搜尋要找的應用程式被分類在哪裡。
- 【選擇應用程式】：共有 2 種模式可以選取，全部選取或是個別選取，點選【全選 】就可以選取同一類型的的應用程式或者點選【⊞】開啟細項選取，NG-UTM 會同步顯示選取的項目(用顏色區分)及數量(5/24)。(圖 5-12)

圖 5-12 選取應用程式

建立完成的應用程式列表如下：(圖 5-13)

應用程式管制：

1 / 1

	群組名稱	項目	動作
☐	voip	影音服務與VOIP，網站服務，社群網路	阻擋+紀錄
☐	test11	影音服務與VOIP	阻擋
☐	wechat	影音服務與VOIP	阻擋+紀錄
☐	line	即時通訊	阻擋+紀錄

圖 5-13 建立好的應用程式

如何運用應用程式

建立好的應用程式需要到管制條例中再決定它的用途，例如，建立好一個應用程式群組名稱為上網，在管制條例中選擇哪一些成員要套用這一個群組，是執行允許或是禁止的動作，這一些調整通通在管制條例理運用。

5-5-2、管制紀錄

管理者設定要管理的服務群組後，到管制條例中套用，不論是允許或是禁止的動作，滿足條件的應用程式項目，都會被記錄下來，管理者可在管制紀錄中查詢特定時間內哪一些服務是被允許通過跟禁止。(圖 5-14)

時間	名稱	類別	動作	來源IP	目的IP	協定	來源埠	目的埠
06-15 15:43:58	WeChat Login	即時通訊	DROP	192.168.189.16	203.205.179.203	TCP	33976	80
06-15 15:43:54	WeChat Login	即時通訊	DROP	203.205.179.203	192.168.189.16	TCP	80	33976
06-15 15:43:39	WeChat Login	即時通訊	DROP	192.168.189.16	203.205.147.167	TCP	33984	80

圖 5-14 應用程式紀錄

5-6、URL 管理

NG-UTM 的 URL 管理，除了可管理傳統的 HTTP(Web)型的網站外，HTTPS SSL 加密型的也可以管理，管理者可設定 HTTP 類型網站黑白名單，同時系統提供預設的黑名單資料庫，讓管理者可以隨時加入，這些資料庫的資料會隨著自動更新的機制增加或是刪除，有別於 HTTP 管理方式，HTTPS 加密型的網站，只能設定黑名單，也就是禁止訪問的網址。

管理使用者瀏覽的網站，除了避免員工摸魚、增加工作效率，亦可預先過濾惡意網站，避免使用者在不知情的狀況下遭植入惡意程式、病毒，以確保網路安全，在雲端時代，惡意的資料通常先誘惑使用者點選某一個網址後，在不明就理下，安裝惡意程式到用戶端，造成資料的損失，例如，網路綁架勒索軟體就是屬於這樣類型。

當使用者瀏覽被禁止的黑名單網址後，系統會自動在使用者的瀏覽器出現預先設定的阻擋文字，提醒使用者這個網站已經被封鎖，管理者可以建立不同 URL 管理機制及套用不同的阻擋訊息，這些阻擋的紀錄也通通被記錄下來，讓管理者日後查詢。

5-6-1、URL 設定

NG-UTM 的 WEB 資料庫運作模式有 2 種，一種是黑名單資料庫，另一個是 WEB 資料庫，管理者同時只能選擇一種運作模式，如果要切換模式，就要將之前設定的資料全部刪除。底下是模式的說明：

黑名單資料庫：以 ShareTech 網路上蒐集的黑名單網站資料為主，不定期的更新這一些網站。(圖 5-15)

圖 5-15 黑名單資料庫

WEB 資料庫：ShareTech 合作廠商提供的資料庫，分類更細也更完整，其中也包含黑名單或是惡意網站，系統分成 6 大類，也會即時的更新最新的網站列表，啟用這個資料庫需要額外的授權碼。(圖 5-16)

圖 5-16 WEB 資料庫

WEB 資料庫資訊顯示目前使用的模式及其授權狀態。(圖 5-17)

- 【授權 】：要啟用 WEB 資料庫需要匯入授權碼，點選【瀏覽】並匯入就完成。
- 【模式】：目前運作的是黑名單資料庫還是 WEB 資料庫，管理者可以按【切換】按鈕，切到另一個模式。
- 【授權期限 】：目前使用資料庫的到期日。
- 【服務狀態 】：在 WEB 資料庫下，會再顯示目前是起用還是停用中。

圖 5-17 WEB 資料庫

5-6-2、黑白名單設定

URL 管理就是利用黑、白名單的建立，所謂白名單就是可以瀏覽的網址，例如，http://tw.news.yahoo.com/，當套用白名單後，管理者在套用白名單的下一條條例禁止所有的 HTTP，代表只能瀏覽白名單的網址，其他的都會被禁止。相反的黑名單的運作就是黑名單列的網址不能瀏覽，其他的都可以。

黑白名單基本設定

新增的名單運作是以黑名單還是白名單模式運作？如果選擇黑名單，比對後符合的網址，NG-UTM 就會阻擋，相反地，選擇白名單模式，就會放行。(圖 5-18)

- 【名稱 】：辨識這個黑/白名單的名稱，例如，禁止上網、只允許上班時間的網站。
- 【名單模式 】：運作模式是黑名單還是白名單。
- 【比對模式 】：提供兩種比對模式，分別為「完整」與「模糊」，完整模式為比對的網址需全部都符合才行，模糊模式是只要關鍵字有部分符合就可以了。

  例如：要封鎖 yahoo 網站

  完整模式：輸入 www.yahoo.com 將只封鎖 www.yahoo.com，但是 www.yahoo.com.tw 仍然可以正常瀏覽，此時可以用萬用字元 * 輔助，把資料改成 yahoo.com.*，就可以把 yahoo 所有相關的網站都封鎖掉。

  模糊模式：輸入 yahoo，就可以將網址中帶有 yahoo 的網址通通封鎖掉，在這樣的情況下，誤擋網站的機率相當高，以上面的為例，abcyahoo 跟 yahooabc 等不相干的網站也會被黑名單的阻擋機制擋掉，此時可以搭配萬用字元 * ，讓整個配置更有彈性。

圖 5-18 黑白名單基本設定

運作模式：黑名單資料庫

黑名單的來源可以由管理者自行輸入或是選用系統內建的黑名單資料庫，同時針對 IPV4/IPV6 甚至 HTTPS 都可以建立黑名單。

自訂黑白名單設定

- 【URL 黑名單 】：輸入黑名單的網址，例如，

  tw.news.yahoo.com/sports/

  www.pchome.com.tw

  每行為一筆黑名單，除了網址外，後面的 URI 資訊也可以加入，當選擇是完整比對時，除了網站的特定內容進不去外，其他的都可以暢行無阻。

- 【IPV4 IP 黑名單 】：輸入黑名單的 IPV4 位址，例如，

  11.12.13.14

  22.23.24.25

- 【IPV6 IP 黑名單 】：輸入黑名單的 IPV6 位址，例如，

  2001:b030:8102:bd::1

  2001:b030:8102:2001::1。

預設黑名單資料庫

當名單模式選擇【黑名單】時，才會出現，選擇【白名單】下，這一個選項就被隱藏。

黑名單的來源可以由管理者自行輸入外，系統預設 11 類黑名單資料庫，讓管理者根據實際需求選用，包含語言暴力 、線上影音 、藥品 、駭客 、成人網站 、代理過濾器 、轉頁 、後門程式 、不信任網站、暴力網站 、 非法盜版等。

為了避免自行輸入的黑名單跟資料庫內的 URL 資料庫重複，NG-UTM 有一個 URL 測試的小功能 ，點選預設黑名單設定旁的 URL 測試 圖示，就可以進入測試，例如，輸入 yahoo.com.tw 測試是否存在預設的黑名單資料庫中，結果是 不存在。(圖 5-19)

圖 5-19 URL 測試

其他黑白名單設定

NG-UTM 的黑名單設定支援群組包含群組的組合，例如，已經建立 2 個黑名單群組，分別是黑名單-A 跟黑名單-B，建立黑名單-C 時，除了黑名單-C 自己內建的之外，更可以包含黑名單-A 跟黑名單-B 中所有的黑名單設定。

當名單模式為【黑名單】時，會顯示所有【黑名單】群組提供管理者選擇，相反，名單模式為【白名單】時，只會顯示【白名單】群組。

運作模式：WEB 資料庫

目前 WEB 資料庫共有 6 大類，包含 危險及犯罪、賭、色情與暴力、政府及特殊網站、一般網路服務、生活資訊及其他等分類可以選擇，如果不知道要管制的網站被分類到哪一個群組，可以點選旁邊【URL 測試】按鈕就可以測試一下。(圖 5-20)

圖 5-20 WEB 資料庫分類

自訂黑白名單設定

根據名單模式，顯示字眼會自動切換黑名單或是白名單。

- 【URL 黑名單 】：輸入黑名單的網址，例如，

  tw.news.yahoo.com/sports/

  www.pchome.com.tw

  每行為一筆黑名單，除了網址外，後面的 URI 資訊也可以加入，當選擇是完整比對時，除了網站的特定內容進去外，其他的都可以被封鎖掉。

- 【IPV4 IP 黑名單 】：輸入白名單的 IPV4 位址，例如，

  11.12.13.14

  22.23.24.25

- 【IPV6 IP 黑名單 】：輸入白名單的 IPV6 位址，例如，

  2001:b030:8102:bd::1

  2001:b030:8102:2001::1。

5-6-3、其他設定

當使用者瀏覽黑名單網站時，NG-UTM 會出現警示畫面，畫面的文字可以由管理者自訂，管理者可以預先設計好警示畫面，也可以讓每一個黑名單都有不同的警示畫面。

預設的警示畫面

系統的預設黑名單阻擋警示設定是在【其他設定】的【預設頁面阻擋設定】中，內部的細項說明如下：(圖 5-21)

- 【阻擋結果網頁設定 】：點選【 檢視 】的按鈕就可以觀看目前的阻擋頁面效果。
- 【主題 】：黃色區塊想要顯示的文字，例如，禁止的網站。
- 【欲顯示的內容 】：需要顯示更詳細的文字說明，例如，禁止觀看否則查辦。

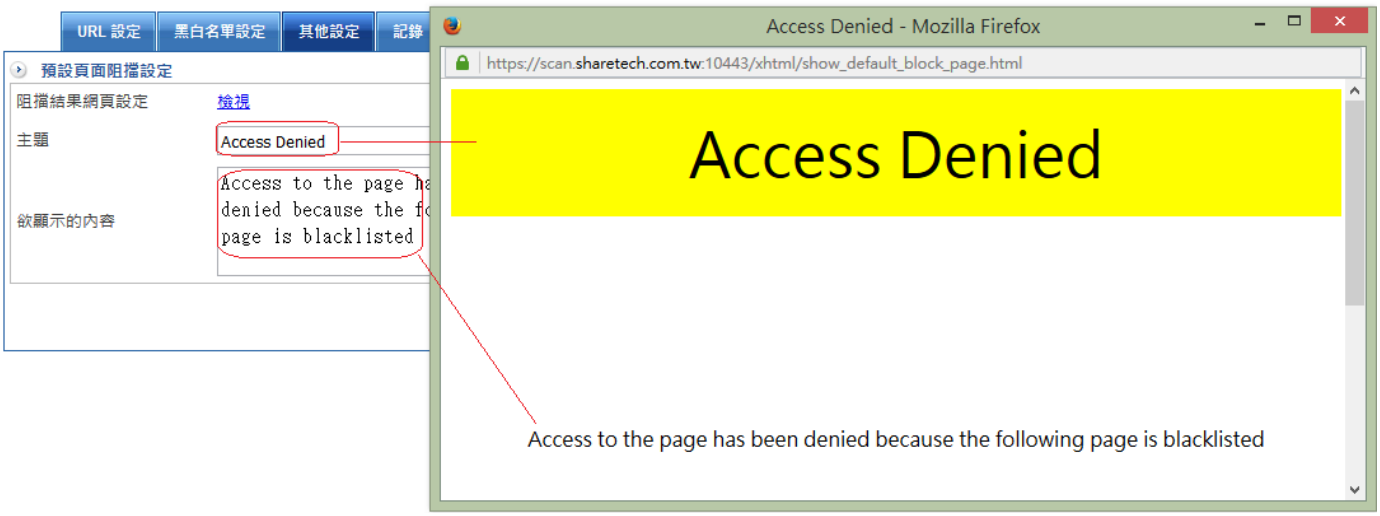


圖 5-21 預設黑名單阻擋網頁設計

URL 設定

建立黑白名單的阻擋網址後，針對黑名單部分，當 NG-UTM 阻止使用者觀看網頁後，會把使用者的瀏覽器轉向到系統預設的阻擋網頁，管理者如果覺得某一個黑名單的阻擋網頁應該跟系統預設的不一樣，可以再制定立一個阻擋顯示網頁。(圖 5-22)

- 【群組名稱 】：辨識這個黑名單的阻擋名稱，例如，禁止看的網站。
- 【啟動自訂網頁阻擋 】：預設是不啟用，這樣所有的阻擋網頁都會使用預設的阻擋網頁，啟用後，系統會另外開啟下列額外的設定項，讓管理者修改，修改的方式跟修改預設阻擋網頁的方式一樣。
- 【阻擋結果網頁設定 】：點選 檢視 的按鈕就可以觀看目前的阻擋頁面效果。
- 【主題 】：黃色區塊想要顯示的文字，例如，禁止的網站。
- 【欲顯示的內容 】：需要顯示更詳細的文字說明，例如，禁止觀看否則查辦。
- 【名單選擇 】：NG-UTM 列出所有的黑、白名單供管理者選擇。

圖 5-22 自訂黑名單阻擋網頁設計

如何運用 URL 管理

建立好的 URL 管理規則只是一些管理物件，這一些物件仍需要到管制條例中決定哪一些 IP 位址是套用這一些規則，套用的方式是執行允許或是禁止的動作，這一些調整通通在管制條例理設定。

5-6-4、記錄

管理者制定好要管理的 URL 管理後，到管制條例中套用，不論是允許或是禁止的動作，滿足條件的 URL 項目，都會被記錄下來，管理者可在紀錄中查詢特定時間內哪一些 URL 是被允許通過跟禁止。

5-7、防火牆功能

內建 SPI 技術，主動攔截、阻擋駭客攻擊，不論是 DOS、DDOS、UDP Flood 等攻擊方式都可以阻擋，甚至可以抵擋疾風病毒的攻擊，確保內部用戶的安全。

如果攻擊者不是從外部到內部，而是由內部互相攻擊呢？在 ICSA 中就沒有定義這樣的攻擊模式，可是在現實的環境中，這樣的任意攻擊卻是真實的存在。

ShareTech 套用合理流量及連線數的觀念，認為同一部電腦，不會同時產生太多的連線數，萬一超過合理的流量及連線數時，結合管制條例的運用，防火牆會要求將多餘的連線阻擋。

常見的駭客攻擊方式(阻斷服務攻擊)

SYN 攻擊

SYN Flood 是當前最流行的 DoS（拒絕服務攻擊）與 DDoS（分散式拒絕服務攻擊）的方式之一，這是一種利用 TCP 協議缺陷，發送大量偽造的 TCP 連接請求，使得被攻擊方資源耗盡（CPU 滿載或記憶體不足）的攻擊方式。

ICMP 攻擊

ICMP（Internet Control Message Protocol）是 TCP/IP 通訊協定中定義封包的一種，主要功能是用來在網路上傳遞一些簡單的控制訊號。ICMP DoS 攻擊主要有以下兩種手法： Ping of Death 與 Smurf 攻擊。

UDP 攻擊

利用 UDP 協議，發送大量偽造的 UDP 連接請求，使得被攻擊方資源耗盡（CPU 滿載、頻寬被占滿或記憶體不足）的攻擊方式。

Land 攻擊

運用 IP Spoofing 技術送出一連串 SYN 封包給目標主 機，讓目標主機系統誤以為這些封包是由自己發送的。由於目標主機在處理這些封包的時候，它自己並無法回應給自己 SYN-ACK 封包，因而造成系統當機。

Smurf 攻擊

Smurf 攻擊是以最初發動這種攻擊的程序名 Smurf 來命名。這種攻擊方法結合使用了 IP 欺騙和 ICMP 回複方法使大量網絡傳輸充斥目標系統，引起目標系統拒絕爲正常系統進行服務。

Tear Drop 攻擊

Teardrop 攻擊則是利用 IP 封包重組的漏洞。當資料經由網路傳送，IP 封包經常會被切割成許多小片段。每個小片段和原來封包的結構大致都相同，除了一些記載位移的資訊。而 Teardrop 則創造出一些 IP 片段，這些片段包含重疊的位移值。當這些片段到達目的地而被重組時，可能就會造成一些系統當機。

Ping of Death 攻擊

「Ping of Death」是經由發送過大的 ping 請求(ICMP echo request) ，以造成緩衝區溢位(Overflow)，繼而導致無法正常運作或當機。

5-7-1、防火牆功能

針對 DOS 或是 DDOS 攻擊的防護，NG-UTM 提供 SYN、ICMP 與 UDP 等 3 種協定的設定值，管理者可以根據需要適當的調整數值：（圖 5-23）

設定 SYN 攻擊設定值

允許最大流量：每一個防火牆保護的外部 IP 位址能夠承受的每秒最大封包要求，預設值是 10,000 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

允許每個來源位址最大流量：網路上同一個 IP 位址同一時間能傳送的數量，預設值是 100 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

阻擋時間：一旦防火牆判斷被攻擊，自動丟棄來自攻擊者 IP 位址封包的時間，預設是 60 秒。

設定 ICMP 攻擊設定值

允許最大流量：預設值是 10,000 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

允許每個來源位址最大流量：預設值是 100 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

阻擋時間：一旦防火牆判斷被攻擊，自動丟棄來自攻擊者 IP 位址封包的時間，預設是 60 秒。

設定 UDP 攻擊設定值

允許最大流量：預設值是 10,000 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

允許每個來源位址最大流量：預設值是 100 封包/秒，超過這個數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

阻擋時間：一旦防火牆判斷被攻擊，自動丟棄來自攻擊者 IP 位址封包的時間，預設是 60 秒。

圖 5-23 防火牆的防護設定

IP 位址封鎖

輸入直接封鎖的來源 IP 位址或是目的 IP 位址，這些位址不再經過防火牆的防護機制，所有來自這些網路的連線要求全部拒絕，以 TCP 為例，這一些 IP 位址送過來或是要送過去的 SYN 封包通通不回應或是不送出去，設定 192.168.1.1 或是 192.168.1.1/24。

IP 位址例外

跟 IP 位址封鎖相反設定，這些來源 IP 位址或是要到的目的位址，這些位址不再經過防火牆的防護機制，所有來自這些網路的連線要求全部接受，不論他的網路封包數量可能比設定值高很多。

其他項目

除了可以偵測 SYN 攻擊、ICMP 攻擊與 UDP 攻擊外，UTM 提供管理者可以阻斷網路常見的攻擊手法，像 IP Options, Land 攻擊、Smurf 攻擊、封鎖 Trace Route、封鎖 Fraggle、封鎖 Tear Drop 攻擊、封鎖 ICMP Fragment 封包、封鎖 Ping of Death 攻擊、封鎖 TCP Flags、封鎖 SYN Fragment 封包與不明封包偵測。（圖 5-24）

圖 5-24 其他項目防護設定

這些防護規則，可以套用在 NG-UTM 的介面位址上，或是每一個管制條例上，只要來自網際網路的攻擊超過設定值，NG-UTM 就會自動將攻擊者 IP 位址的封包阻擋，確保網路設備的網路安全。

5-7-2、防護記錄

NG-UTM 記錄所有攻擊行為，管理者可針對攻擊類型、攻擊來源 IP 位址、被攻擊 IP 位址進行搜尋，系統會詳細列出遭受攻擊時間、攻擊類型、協定、通訊埠、攻擊來源 IP 位址與被攻擊 IP 位址。（圖 5-25）

1 / 1

時間	類型	協定	通訊埠	介面	攻擊來源IP	被攻擊IP位址
2016-02-19 18:46:59	UDP Attack	UDP	137	zone3	192.168.188.82	192.168.188.255
2016-02-19 11:08:28	UDP Attack	UDP	137	zone3	192.168.188.91	192.168.188.255
2016-02-19 10:58:39	UDP Attack	UDP	137	zone3	192.168.188.91	192.168.188.255

圖 5-25 防火牆防護記錄

5-8、上網認證

NG-UTM 可經藉由上網認證的設定，讓使用者上網時需要輸入帳號及密碼，成功後，才可以正常的使用網路，NG-UTM 的認證機制可以使用 HTTP 或是 HTTPS，管理者可預先設定認證前、認證後使用者看到的網頁畫面，不僅如此，甚至可以把使用者瀏覽的網站轉到預先設定的網址。

提供給 NG-UTM 認證功能的帳號有四個來源，系統預設的認證帳號優先順序是「L,A,P,R」，細部說明如下：

1、 內建的本機使用者，以「L」 為代表字。

2、 外部的 Radius Server，以「R」 為代表字。

3、 外部的 POP3 伺服器，以「P」 為代表字。

4、 外部的 AD 伺服器，以「A」 為代表字。

管理者利用這四種帳號來源，建立認證機制，同時可以設定認證帳號來源的優先順序，例如，同時建立本機使用者帳號跟 AD 伺服器 2 種認證帳號來源，管理者並將認證帳號的優先來源設為「A,L,P,R」、假設 AD 伺服器跟本機使用者都有一個相同的帳號名稱為 Peter，則密碼必須是符合 AD 伺服器。

管理者希望使用者使用網際網路前，先經過認證程序，認證過後，才可以使用網路，此時就需要網路認證功能。當管制條例要求使用者認證後才能上網際網路，使用者打開網頁後，會出現要求輸入帳號密碼的視窗，輸入管理者給予的帳號密碼，正確無誤後，系統就會自動開啟預設首頁或是管理者自訂的網址。

使用者的帳號密碼來源可以從本機自建的帳號密碼、從 AD 伺服器選取的帳號密碼、Radius Server 或是從郵件伺服器來的帳號密碼。

管理者可以任意從上述的 4 種帳號來源挑選及選擇認證時的優先順序，建立完成一個使用者群組後，此時就可以在管制條例中挑選特定的使用者群組套用。當特定的來源 IP 位址要上網路時，NG-UTM 會要求這些用戶輸入帳號及密碼，認證成功後才可以使用網路。

上網認證的設定順序

要讓上網認證運作正常，有幾個預先步驟要先完成，順序如下：

【認證設定】>【頁面設定】>【決定帳號來源】>【建立使用者群組】>【管制條例套用】

5-8-1、認證設定

NG-UTM 認證時用的共同設定，每一個使用者群組都可以套用這些設定值，當然，管理者仍然可針對不同的帳號配置不同的設定值，說明如下：（圖 5-26）

- 【認證通訊埠 】：上網認證機制運作時使用的埠號，預設為 TCP 82。
- 【認證連線設定 】：導入認證畫面的使用協定，有 HTTP 跟 HTTPS 2 種可以選擇，預設是 HTTP。
- 【同時最大連線數 】：可以多少個 IP 位址跟認證伺服器同時要求認證，預設是 256 個 IP 位址，可設定範圍是 10~ 256。
- 【當閒置多久要求重登 】：使用者認證成功後，就可以上網，當這使用者多久沒有使用網路時，超過設定的時間，NG-UTM 就會要求使用者重新認證一次，預設值是 60 分，可設定範圍是 1~ 1000 分。
- 【使用者登入之後多久要求重登 】：每次使用者認證成功後，最長可以使用的時間，超過設定的時間，NG-UTM 就會要求使用者重新認證一次，預設值是 24 小時，可設定範圍是 0~24 小時，0 代表關閉這項功能，只要使用者的使用行為沒有觸發【當閒置多久要求重登 】這個機制，認證連線都是有效。
- 【允許修改密碼 】：使用者認證成功後，可不可以修改認證來源的密碼，預設是關閉，勾選後，可以修改自己的密碼，下次登入時，就可以使用新的密碼。
- 【拒絕重複登入 】：啟用這項功能後，每個帳號及密碼只允許一個 IP 位址登入，當另一個 IP 位址要求使用相同的帳號密碼時，會被 NG-UTM 的認證機制拒絕，預設是關閉，代表同一個帳號可以預不同的 IP 位址登入。
- 【登入失敗次數超過多少暫時封鎖 】：為了預防被不法使用者測試使用者密碼登入，管理者可設定當同一個帳號登入且認證失敗超過設定值時，這帳號會被暫時封鎖無法認證，預設為 0 代表功能關閉，使用者可以無限制的嘗試輸入密碼。
- 【多久解除被暫時封鎖的 IP 】：當管理者啟用【登入失敗次數超過多少暫時封鎖 】功能時，這一個機制才會生效，被封鎖的 IP 位址需要多長時間，才可以再次使用認證機制，預設為 0 代表功能關閉，不會解除被封鎖的 IP 位址，代表這一個 IP 位址被永久封鎖。
- 【登入失敗次數超過多少永久封鎖 】：管理者也可將嘗試登入的非法使用者，當其登入帳號/密碼錯誤超過設定值，把帳號永久封鎖，預設為 0 代表功能關閉，不會永久封鎖任何一個帳號。

- 【解除 IP 封鎖 】：被系統封鎖的 IP 位址，都會列在這理，管理者可將這一些被封鎖的 IP 位址解除封鎖。
- 【帳號過期通知 】：此功能限 內建的本機帳號，某個帳號有設定使用期限，當快到期前，系統會通知管理者，有哪幾個帳號即將到期，請管理者注意，預設為 0 代表功能關閉，假設定值為 3，則帳號失效前 3 天，管理者會收到通知信。
- 【帳號過期刪除 】：此功能限 內建的本機帳號，某個帳號有設定使用期限，當帳號到期後，系統自動刪除該帳號，預設為 0 代表功能關閉，也就是不會刪除任何本機帳號，假設定值為 3，則帳號失效後 3 天，此帳號就會被刪除。
- 【選擇認證模式 】：針對統內建的 4 種帳號來源，認證時優先順序，系統預設為「L,A,P,R」，依序是內建的本機使用者、外部的 Radius Server、外部的 POP3 伺服器、外部的 AD 伺服器。管理者可以調整英文字的順序，則認證優先順序就會更動。

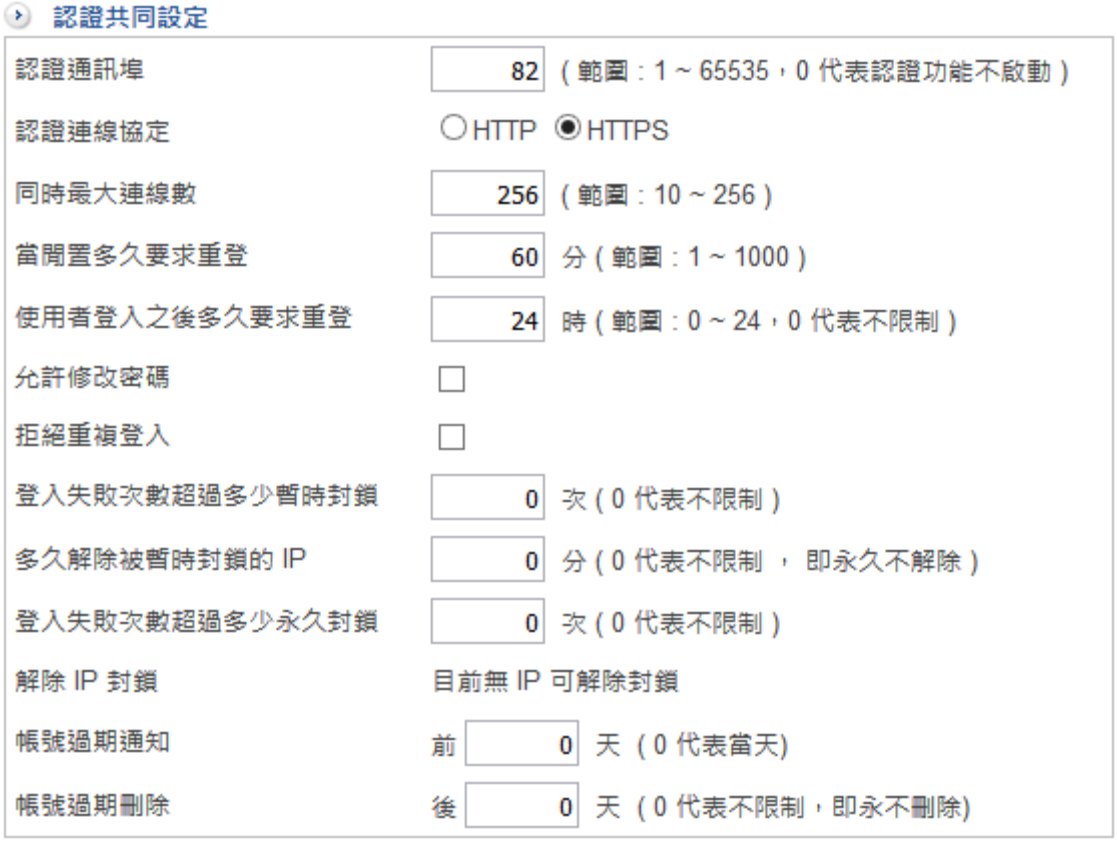


圖 5-26 認證的共同設定

5-8-2、頁面設定

管理者在這裡設定一些上網認證時出現在使用者瀏覽器上的資訊，甚至可以套用電子白板的資訊，確保使用者有看到應該看到的資訊。

頁面共用設定

這個設定會套用到整個頁面設定中。（圖 5-27）

- 【登入成功的使用者要被轉向的 URL 】：管理者可以讓登入成功的使用者開啟一個指定的網頁，例如，公司的網頁、最新消息的網站或是訊息通知的網頁，預設為空白，當使用者認證成功後，自動開啟使用者瀏覽器所設定的首頁。
- 【是否要有閱讀頁面 】：管理者可以讓登入成功的使用者開啟一個指定的網頁，並會產生一個已閱讀的按鈕讓使用者確認已經看過這一些訊息，預設為關閉。
- 【頁面預設語系 】：有 English、繁體、簡體中文 3 種選項。
- 【頁面顏色設定 】：5 個區塊的顏色可管理者挑選。

圖 5-27 認證頁面的共同設定

登入畫面設定

每個使用者登入過程會看到 2 個頁面，一個是登入頁面，也就是帳號登入時輸入帳號密碼的頁面，另一個是登入成功後，會看到的頁面，NG-UTM 提供管理者自訂這 2 個頁面的能力

Client 端登入畫面設定（圖 5-28）

- 【主旨】：在主旨區顯示的文字。例如，請輸入帳號密碼。
- 【內容】：在內容區顯示的文字。例如，這是 ABC 公司的認證系統。
- 【上傳 logo】：把 logo 區顯示的圖示換成管理者想要的圖示，預設是眾至資訊的 Logo。
- 【檢視登入畫面】：管理者檢視一下輸入文字後的效果，檢視效果之前需要先將設定的資料儲存，如果效果滿意，可以在檢視畫面中按下接受按鈕，系統就會讓這個登入畫面成為系統預設的登入畫面。

圖 5-28 認證的登入畫面及檢視

Client 端登入後畫面設定（圖 5-29）

- 【登入後訊息】：當使用者登入成功後，管理者希望他看到的訊息，例如，請不要濫用網路資源。
- 【檢視登入後畫面】：管理者檢視一下輸入文字後的效果，檢視效果之前需要先將設定的資料儲存，在檢視後的畫面會出現幾個訊息，一個是使用者目前使用的 IP 位址、Logout 跟 Change Password。
- 【Change Password】：當帳號來源是本機內建的使用者，使用者可以在登入後的畫面，自行更改認證帳號的密碼。

圖 5-29 認證的登入後畫面及檢視

套用電子白板版面設定

NG-UTM 可以讓認證的登入畫面跟電子白板完美結合，此時登入的畫面就不是剛剛檢視登入畫面中的樣式，而是電子白板的樣式，但是其中的主旨、內容跟 Logo 資料，可由管理者決定是否要沿用，在啟用這項功能之前，需要先到電子白板中建立一個群組。（圖 5-30）

- 【註解】：這個服務的名稱，例如，認證+電子白板。
- 【IP 位址】：要套用這項功能的 IP 位址，例如，192.168.1.1。
- 【網路遮罩】：子網路遮罩，例如，255.255.255.0/24 是一個 IPV4 的 C Class。
- 【套用電子白板設定】：選擇一個預先設定好的電子白板群組。
- 【顯示上網認證登入畫面】：此項功能是用電子白板取代傳統的登入畫面，但還可以把登入畫面中設定的主旨、內容及 Logo 嵌入電子白板中。
- 【預覽】：當所有設定都為完成並儲存後，NG-UTM 提供檢視功能，電子白板的檢視畫面分成電腦版跟手機板 2 種，管理者可以點選後檢視效果。

圖 5-30 認證登入結合電子白板

5-8-3、認證帳號來源

NG-UTM 的認證帳號來用共有 4 種來源，系統預設的認證帳號優先順序是「L,A,P,R」，細部說明如下：

1、 內建的本機使用者，以「L」 為代表字。

2、 外部的 POP3 伺服器，以「P」 為代表字。

3、 外部的 Radius Server，以「R」 為代表字。

4、 外部的 AD 伺服器，以「A」 為代表字。

5-8-3-1、本機使用者

建立本機使用者帳號，他的優點是可以讓使用者自行更改密碼及設定有效日期。（圖 5-31）

- 【名稱】：新增帳號的名稱，任何容易描述這個使用者的文字，例如，張三、李四，最多 16 個文字。
- 【使用者帳號】：認證時使用的帳號，限英文及數字的組合，例如，jean，最多 16 個文字。
- 【密碼】：這個帳號認證時使用的密碼，要想使你的密碼更安全，可以採取以下方法：

  使用字母和數字

  使用特殊字元(如@，但逗號與冒號不允許使用)

  混合使用大小寫

  密碼會區分英文大小寫，請用 3 至 16 個字元，不要與帳號相同，範例：@jean39
- 【密碼檢測】：根據輸入的密碼，系統自動檢測複雜度，讓管理者參考。
- 【確認密碼】：再次確認輸入密碼，避免密碼輸入錯誤造成無法登入。
- 【當下次登入時要求使用者更改密碼】：要不要讓使用者登入成功後可以修改密碼，預設是不允許。

■ 【帳號有效期限】：設定一個帳號使用期限，系統會自動帶出日期讓管理者挑選，如果空白，代表這個帳號永遠不會過期，預設是空白。

圖 5-31 建立本機使用者

本機使用者帳號列表

■ 【過期紀錄】：所有過期的帳號，全部都會列在過期紀錄中。

■ 【帳號/名稱搜尋】：當本機帳號龐大，例如，超過 50 筆資料，管理者要記得誰是誰就有一點難度，NG-UTM 提供搜尋的功能，不論是帳號或是設定的名稱，通通都可以搜尋。

■ 【匯入/匯出】：內建的本機帳號可以匯入跟匯出，便於保存。

5-8-3-2、外部 POP3 伺服器

NG-UTM 的認證帳號可以跟郵件伺服器的收信(POP3)帳號整合，讓使用者不需要背多筆帳號及密碼。（圖 5-32）

- 【POP3 伺服器網域名稱】：POP3 伺服器網域的名稱，帳號 Jean@abc.com，他的 POP3 網域名稱就是 abc.com。
- 【POP3 伺服器】：POP3 伺服器的 IP 位址或是網域的 A 紀錄名稱，例如，9.9.9.9 或是 pop.abc.com。
- 【登入帳號附加網域】：認證帳號要不要家入 POP3 伺服器網域名稱，預設是不加入，例如，某個 POP3 帳號為 jean@abc.com，當不加入附加網域時，輸入的認證帳號為 jean，選擇加入時認證帳號就變成 jean@abc.com 。
- 【通訊協定】：共有 2 種認證協定可以選擇，一個是 POP3，另一個是 IMAP，當選擇 IMAP 時要注意一下認證伺服器的 IP 位址跟網域要指向相對應的 IMAP 伺服器。
- 【安全性】：認證機制溝通時，要不要選用加密協定，預設是一般，就是沒有加密，管理者可以根據伺服器提供的連線方式，另選加密方式為 TLS 或是 SSL。
- 【通訊埠】：認證時使用的通訊埠，預設 POP3 是 110，TLS/SSL 是 443
- 【憑證】：當選擇的通訊埠是加密下，要不要忽略憑證的警示，預設為不忽略憑證警示。
- 【連線測試】：當上述的資訊都設定完成後，可以測試一下設定值是否正常運作，點選連線測試的按鈕，系統會出現一個對話框，請管理者輸入一個 POP3/IMAP 的帳號，送出後回覆測試結果。

圖 5-32 建立 POP3/IMAP 認證

5-8-3-3、外部 RADIUS 伺服器

NG-UTM 的認證帳號可以跟外部的 Radius 伺服器的帳號整合，讓使用者不需要背多筆帳號及密碼。（圖 5-33）

- 【RADIUS 名稱】：此 RADIUS 伺服器的名稱，例如，my_radius
- 【RADIUS 伺服器】：此 RADIUS 伺服器的 IP 位址或是網域名稱，例如，192.168.1.100 或是 radius.abc.com。
- 【RADIUS 伺服器通訊埠】：NG-UTM 跟 RADIUS 伺服器溝通時使用的通訊埠，預設值為 1812。
- 【密鑰】：NG-UTM 跟 RADIUS 伺服器溝通時使用的密鑰，密鑰不對認證就無法正常運作。
- 【介面】：NG-UTM 是以 ZONE 為介面，不一定每一個介面都可以跟 RADIUS 伺服器互通，因此要選擇能夠跟 RADIUS 伺服器通訊的介面，如果選擇不指定，則 NG-UTM 就會按照預設的路由表跟伺服器溝通。
- 【連線測試】：當上述的資訊都設定完成後，可以測試一下設定值是否正常運作，點選連線測試的按鈕，系統會出現一個對話框，請管理者輸入一個 RADIUS 伺服器 的帳號，送出後回覆測試結果。

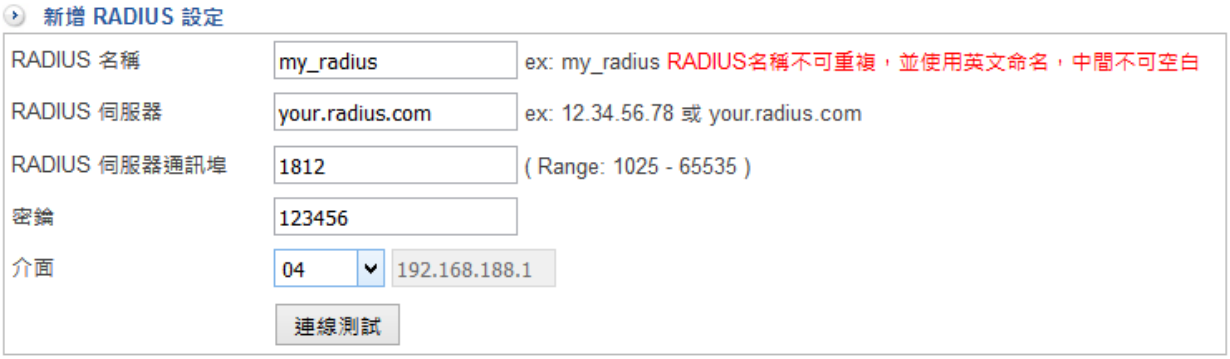


圖 5-33 建立 RADIUS 伺服器認證

5-8-3-4、外部 AD 伺服器

NG-UTM 的認證帳號可以跟外部的 AD 伺服器的帳號整合，讓使用者不需要背多筆帳號及密碼。（圖 5-34）

- 【AD 位址】：AD 伺服器的 IP 位址，例如，192.168.1.1
- 【AD 網域名稱】：AD 網域伺服器的網域名稱，例如，ad.abc.com，最多 16 個字。
- 【AD 登入帳號】：具有帳號管理權限的 AD 管理者帳號，例如，administrator，最多 16 個字。
- 【AD 登入密碼】：具有帳號管理權限的 AD 管理者的密碼。
- 【連線測試】：當輸入上述資訊後，管理者可以按一下連線測試按鈕，檢視設定的資訊是否正常。
- 【忽略的 AD 群組】：那些 AD 伺服器上的群組，該群組的使用者不具備認證帳號功能。
- 【忽略的 AD 使用者】：那些 AD 伺服器上的使用者不能用來登入認證機制。

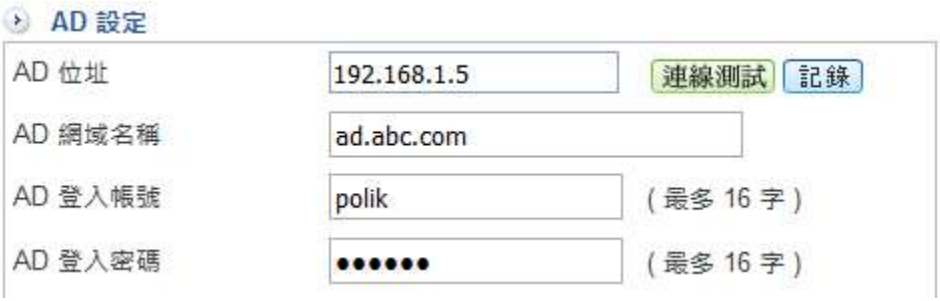


圖 5-34 AD 伺服器設定

5-8-4、使用者群組

建立認證機制的第 4 個步驟就是建立使用者群組，管理者可以建立多筆使用者群組，這些群組可套用預先設定的認證設定及帳號來源，也可以另行設定新的認證設定及帳號來源。（圖 5-35）

- 【群組名稱】：這個使用者的名稱，可以是任何文字的組合，例如，工程部群組。
- 【認證設定】：有 2 個模式可以選擇，一個是可以預先設定的認證設定，另一個是自訂設定，根據使用者特性不一樣，再次設定他的屬性，『當閒置多久要求重登』、『使用者登入之後多久要求重登』，甚至『登入成功的使用者要被轉向的 URL』都可以更改，詳細的選項說明請參考 5-8-1 的認證設定。
- 【選擇要編輯的使用者類型】：有 3 個選項可以選擇，可以混合挑選：

1.本機使用者

在這個模式下，挑選使用者，例如，本機有 200 個帳號，這個使用者群組符合其中 50 個帳號，則把這 50 個帳號挑選後加入被選擇的使用者就完成。

2.外部 POP3 伺服器

選擇預先建立的 POP3 伺服器，加入被選擇的使用者就完成。

3.外部 RAIUS 伺服器

選擇預先建立的 RADIUS 伺服器，加入被選擇的使用者就完成。

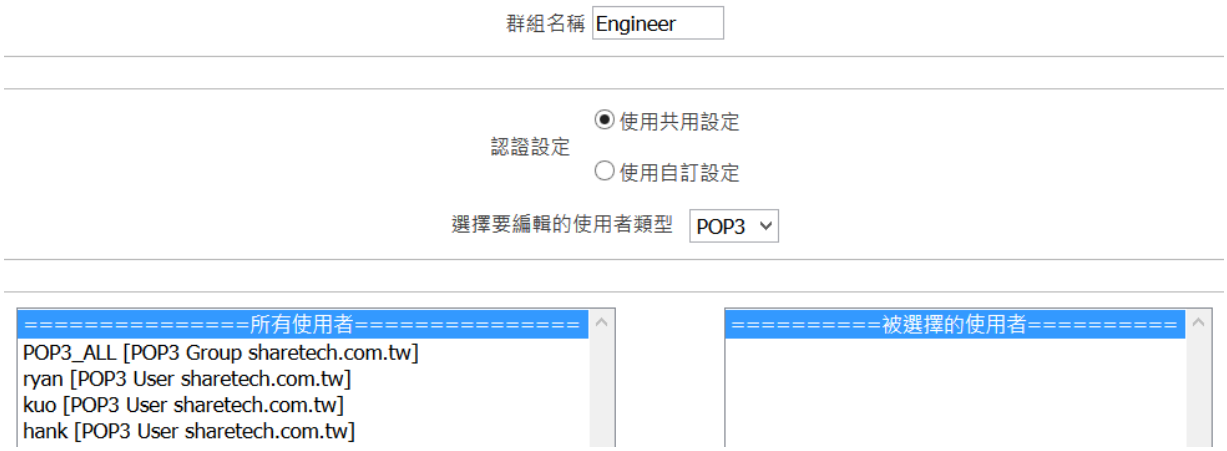


圖 5-35 認證群組設定

5-8-5、認證紀錄

每一個使用者群組的認證紀錄，不論成功、失敗都會被記錄下來，管理者可以根據 IP 位址、帳號、連線狀態或是認證帳號的來源查詢，對於認證的結果共有 6 種，login Success、login Fail、logout Success、idle logout、login Timeout 跟 admin Kick-out。（圖 5-36）

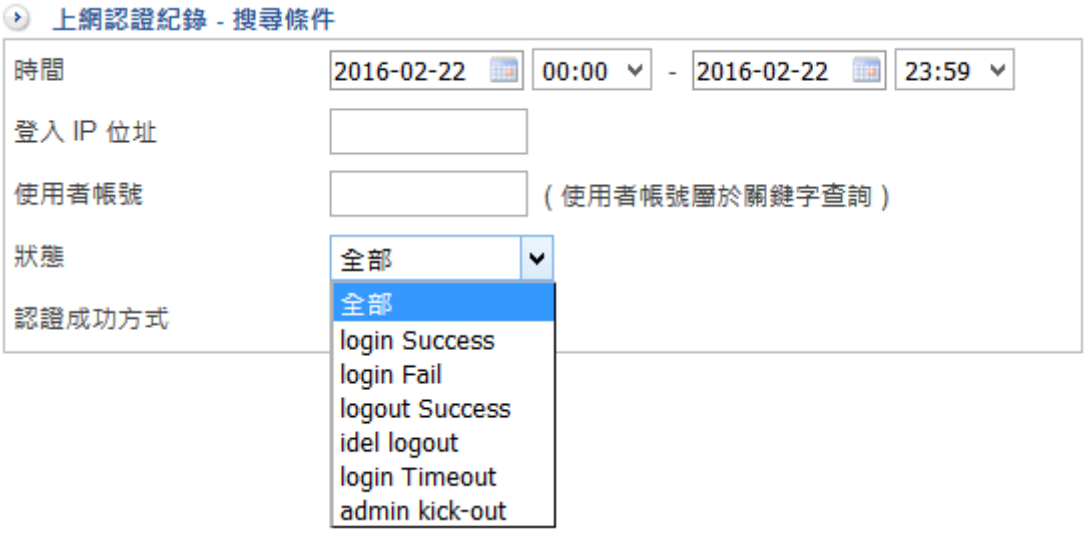


圖 5-36 認證紀錄查詢

5-8-6、認證連線狀態

列出目前利用上網認證的使用者及數量，包含群組名稱、使用者帳號、使用者 IP、剔除與群組剔除紀錄條列出來。

5-9、電子白板

現在『低頭族』越來越多，不管是坐車、搭捷運都可以看到很多人低頭玩手機、平版電腦，想起以前念書的時候也是一堆低頭族人群，不過大家都是趁著空檔努力 K 書。由於網路的快速發展，資訊的快速成長影響所有人的生活方式，進而在日常的生活、工作領域、休閒活動...都已經跟網路脫離不了關係。

以前，大多數的企業要發布訊息給所有員工知道，不是張貼公告就是就藉由 EMAIL 來通知，如果遇到一些重要訊息可能就只能緊急廣播，或藉由部門力量來快速通告。但在 21 世紀的新時代，當網路已深深影響我們生活時，利用網路快速傳播已是現在最佳傳播工具。

現今多數的上班族，上班的第一件事就是打開電腦，看看新聞，或者開啟即時通訊(MSN、QQ、SKYPE..，)跟朋友打屁、聊天，等所有這些雜事處理完時才會開工，因此，如果一些重要訊息是藉由 MAIL 通知，可能已經拖延了一些時效，時間傳達最好能即時，盡快讓所有人能掌握最新資訊。

因此，眾至網頁電子白板功能，多是當使用者打開電腦時，不管要上網瀏覽網頁或者開啟即時通訊跟朋友聊天，都必須確認看到看過公司公布的重要資訊後才可以啟用。網頁電子白板或許不能取代郵件成為主要的通報系統，但是藉由它可以讓習慣瀏覽網頁的人更快接收到最新企業訊息。

電子白板的設定順序

要讓電子白板運作正常，有幾個預先步驟要先完成，順序如下：

【建立使用者群組】>【版面設計】>【管制條例套用】

5-9-1、使用者群組

首先，需要先建立一個使用者群組，他定義閱讀訊息前跟閱讀訊息後的動作。（圖 5-37）

- 【群組名稱】：這個使用者群組的名稱，可以是任何文字的組合，例如，工程部電子白板。
- 【隔間多久彈跳一次訊息】：每隔多少小時，電子白板的訊息就會重現在使用者的網頁上，預設是 24 小時。
- 【閱讀訊息前, 阻擋全部對外連線】：使用者網頁出現電子白板的訊息後，此時要不要讓他馬上可以上網，預設是允許，管理者也可以強制要求看完電子白板的內容及按下已閱讀的按鈕後才開放使用者上網。
- 【閱讀訊息後, 網頁內容重新導向】：閱讀後要不要將使用者的網頁轉向，例如公司網站或是特定網址，空白則是使用者的瀏覽器預設網頁。

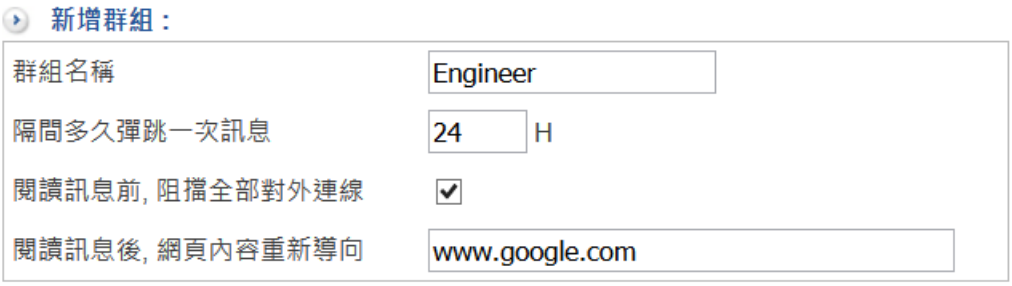


圖 5-37 電子白板群組

5-9-1-1、版面設定

NG-UTM 提供多種電子白板的樣板讓管理者設計參考，每一個樣板均可針對電腦版或是手機板在進行更細部的設計，共有 4 種樣板可供選擇，分別是基本樣板、圖片樣板、圖文樣板跟路徑連結，細項說明如下。

A. 基本樣板

手機板跟電腦版的最主要差別是整個版面的大小，基本樣板共有 3 個區塊，標題區、內文跟已讀按鈕，內容區支援標準的 HTML Tag ，把想顯示的內容輸入就可以，整個顯示檢視需要先儲存後可以按下預覽按鈕。（圖 5-38）

- 【白板標題】：輸入在標題區要顯示的文字，例如，工程部電子白板。
- 【閱讀按鈕文字】：已閱讀的按鈕文字要不要更改，點選自訂後就可以輸入文字。
- 【白板訊息內容】：輸入文字，可以使用 HTML TAG 讓閱讀內容更清楚明瞭。
- 【背景顏色】：選擇一個適當的背景色。

圖 5-38 電子白板—基本樣板

B. 圖片樣板

手機板跟電腦版的最主要差別是整個版面的大小及圖片更換的功能，圖片樣板共有 3 個區塊，標題區、圖片跟已讀按鈕，整個顯示檢視需要先儲存後可以按下預覽按鈕。（圖 5-39）

- 【白板標題】：輸入在標題區要顯示的文字，也可以設定為隱藏，如果連已閱讀按鈕都隱藏，整個電子白板為一張圖片，例如，工程部電子白板。
- 【圖片顯示】：限定電腦版，圖片區總共有幾帳。
- 【圖片變換】：圖片區的圖面每隔幾秒鐘更換一次，預設是 30 秒。
- 【圖片大小】：圖片的大小，預設值為 800X600pixel，管理者可以再調整大小。
- 【模式選擇】：限定電腦版，圖片區的圖片是隨機顯示還是每次都從第一張開始。
- 【圖片管理】：當有上傳圖片後才會開啟，讓管理者選擇圖片出來的模式，例如，隨機還是固定。
- 【隱藏閱讀按鈕】：已閱讀的按鈕是否要顯示，預設是關閉，就是不顯示，因此使用者點選圖片任何一個地方即代表已閱讀。
- 【閱讀按鈕文字】：已閱讀的按鈕文字要不要更改，點選自訂後就可以輸入文字。
- 【背景顏色】：選擇一個適當的背景色。

圖 5-39 電子白板—圖片樣板

C. 圖文樣板

手機板跟電腦版的最主要差別是整個版面的大小及圖片更換的功能，圖片樣板共有 3 個區塊，標題區、圖片+文字區跟已讀按鈕，整個顯示檢視需要先儲存後可以按下預覽按鈕。（圖 5-40）

- 【白板標題】：輸入在標題區要顯示的文字，也可以設定為隱藏，如果連已閱讀按鈕都隱藏，整個電子白板為一張圖片，例如，工程部電子白板。
- 【圖片顯示】：圖片+文字區區總共分成幾個小區塊，預設為 3 個。
- 【圖片變換】：圖片區的圖面每隔幾秒鐘更換一次，預設是 30 秒。
- 【圖片大小】：圖片的大小，預設值為 800X600pixel，管理者可以再調整大小。
- 【模式選擇】：限定電腦版，圖片區的圖片是隨機顯示還是每次都從第一張開始。
- 【隱藏閱讀按鈕】：已閱讀的按鈕是否要顯示，預設是關閉，就是不顯示，因此使用者點選圖片任何一個地方即代表已閱讀。
- 【閱讀按鈕文字】：已閱讀的按鈕文字要不要更改，點選自訂後就可以輸入文字。
- 【群組管理】：當有上傳圖片後才會開啟，讓管理者選擇圖片出來的模式。
- 【背景顏色】：選擇一個適當的背景色。

圖 5-40 電子白板—圖文樣板

D. 路徑連結

如果上述 3 種設計都無法滿足管理者的需求，電子白板可以上傳自行設定的頁面或是 NG-UTM 去抓取管理者預設存在網路上的資料，把它當作電子白板的樣本，不論那一種，都可以點選網頁範例中的原始碼，把它改成管理者要的模式就可以運用，在這個模式下，電腦版跟手機板的設定都是一樣。

模式一、HTTP 上傳

透過 HTTP 上傳預先設定好的數個檔案，再決定如何顯示。

- 【檔案管理】：根據上傳的檔案，再決定如何顯示，是固定顯示還是隨機。
- 【圖片變換】：圖片區的圖面每隔幾秒鐘更換一次，預設是 30 秒。
- 【閱讀按鈕文字】：已閱讀的按鈕文字要不要更改，點選自訂後就可以輸入文字。

模式二、FTP 伺服器

NG-UTM 到管理者預設的 FTP 伺服器中固定的目錄去抓取檔案，並按照設定的資訊顯示電子白板。

- 【系統主機 IP】：FTP 伺服器的 IP 位址，例如，192.168.10。
- 【資料夾目錄】：抓取 FTP 伺服器特定資料夾的檔案，此時需要指定資料夾的目錄，例如，\public\epaper。
- 【登入帳號】：登入 FTP 伺服器的帳號。
- 【登入密碼】：登入 FTP 伺服器的密碼，輸入完成後可以按一下連線測試，測試輸入的資料是否正常。
- 【自動更新時間】：每隔多少時間到 FTP 伺服器登入檢查是否有新檔案。
- 【立即更新】：馬上去檢查 FTP 伺服器的目錄下是否有新的檔案。
- 【檔案管理】：根據上傳的檔案，再決定如何顯示，是固定顯示還是隨機。
- 【網頁變換】：圖片區的圖面每隔幾秒鐘更換一次，預設是 30 秒。
- 【閱讀按鈕文字】：已閱讀的按鈕文字要不要更改，點選自訂後就可以輸入文字。

模式三、Samba 伺服器

NG-UTM 到管理者預設的 Samba 伺服器(網路芳鄰)中固定的目錄去抓取檔案，並按照設定的資訊顯示電子白板。

- 【系統主機 IP】：Samba 伺服器的 IP 位址，例如，192.168.10。
- 【資料夾目錄】：抓取 Samba 伺服器特定資料夾的檔案，此時需要指定資料夾的目錄，例如，\public\epaper。
- 【登入帳號】：登入 Samba 伺服器的帳號。
- 【登入密碼】：登入 Samba 伺服器的密碼，輸入完成後可以按一下連線測試，測試輸入的資料是否正常。
- 【自動更新時間】：每隔多少時間到 Samba 伺服器登入檢查是否有新檔案。
- 【立即更新】：馬上去檢查 Samba 伺服器的目錄下是否有新的檔案。
- 【檔案管理】：根據上傳的檔案，再決定如何顯示，是固定顯示還是隨機。
- 【圖片變換】：圖片區的圖面每隔幾秒鐘更換一次，預設是 30 秒。
- 【閱讀按鈕文字】：已閱讀的按鈕文字要不要更改，點選自訂後就可以輸入文字。

5-9-2、已閱讀白板使用者 IP

凡走過必留下痕跡，凡閱讀過必留下資訊，NG-UTM 網頁電子白板功能，不僅可以提供企業一套好的訊息傳播工具，更重要的它可以記錄所有使用者瀏覽訊息的情形。詳細記錄使用者閱讀電子白板訊息的主題與瀏覽時間，如果希望再次提醒使用者，還可以將它剔除，讓使用者重新再閱讀一次。（圖 5-41）

已閱讀白板使用者IP：

群組名稱	IP位址	電腦名稱	閱讀訊息時間	踢除	群組踢除
電子白板一	59.127.67.17	59.127.67.17	2016-02-22 11:01:38	踢除	踢除

圖 5-41 電子白板閱讀訊息

5-10、DNS filter

DNS filter 提供使用者的上網保護，對於設定在 DNS filter 上的域名，當使用者查詢時，系統會代理回應 0.0.0.0 給使用者，此時使用者就無法正常的使用。例如，管理者禁止內部使用者上 123abc.com 的網站，設定 123abc.com 在 DNS filter 上，當使用者要查詢時，NG-UTM 就回應 0.0.0.0 給使用者，這樣就可以達到禁止上網的動作。

DNS filter 通常會搭配 Sandstorm ，因為 Sandstrom 上面的網址通常是惡意的網站，這樣就可以避免使用者誤觸網址。

5-10-1、DNS Filter

首先，新增 DNS Filter 群組，管制的來源有 2 個，一個是 Sandstorm 上面的惡意網址，另一個是自訂。

- 【群組名稱】：設定 DNS Filter 的群組名稱。
- 【Sandstorm 服務】：DNS 管制來源為 Sandstorm 上中高風險的惡意程式網址，當使用者查詢這一些網址時，系統會回應 0.0.0.0。
- 【完整比對】：自訂要封鎖的網址，比對時採用完整比對，例如，www.123abc.com，此時，查詢這個網址時系統回應 0.0.0.0 給用戶，但是 mail.123abc.com 卻可以正常解析。
- 【模糊比對】：自訂要封鎖的網址，比對時採用完整比對，例如，123abc.com，則所有 123abc.com 的其他網址如，www.123abc.com，mail.123abc.com 都會被封鎖。

5-10-2、管制紀錄

被封鎖的 DNS 查詢紀錄都會在這裡，管理者根據時間、來源或是目的 IP 位址，就可以查詢。

第 6 章 網路服務

NG-UTM 提供一些網路服務的功能，例如 DHCP 伺服器、DDNS 服務、SNMP、DNS 伺服器、病毒引擎及 WEB 服務，每一樣服務都有其獨特的功能要求，簡述如下：

（一）【DHCP 服務】：

當啟動 DHCP 功能時，內部 PC 可透過 NG-UTM 的介面，取得 IP 位址、DNS 伺服器等資訊。

（二）【DDNS 服務】：

DDNS 是動態 DNS，通常是由第三方提供 Domain 的 服務給 WAN 不固定 IP 的主機，也就是網域名稱不變，但是 IP 位址會隨時改變。如果不固定 IP 的主機(如使用 PPPOE 的 ADSL，DHCP 的 Cable，撥接用戶)，欲架設 Web、Mail 或者 FTP 等 Server，或者使用者需要網路身份(網域名稱)者即需動態 DNS。

（三）【SNMP】：

SNMP 是專門用於管理網路節點（伺服器、工作站、路由器、交換器...）的協定。網路管理者透過 SNMP 接收到的訊息，能即時發現並解決網路問題，或協助其規劃網路資源的運用。

（四）【DNS 伺服器】：

DNS 的全稱是 Domain Name Service，是一套系統軟體，讓大家所使用及管理的電腦網路系統，能夠作領域名稱與 IP 位址之間的轉換。

（五）【病毒引擎】：

提供 ClamAV 跟 Kaspersky 掃毒引擎設定。

（六）【WEB 服務】：

NG-UTM 提供 WEB 掃毒，包含掃描圖形檔、掃毒連線數、掃描檔案大小，同時也可以針對 HTTPS 制定憑證資訊。

（七）【高可用性】：

NG-UTM 的硬體備援機制，採 Master/Backup 模式，系統正常運作的情況下網路存取皆透過指定的 MASTER 主機，同時會有一台 BACKUP 主機即時備份來自 MASTER 主機的所有資料；當目前運作中的 MAST 主機發生故障情形時，BACKUP 主機會即時取而代之成為 MASTER 主機，來保持內/外部網路不斷線，避免錯失商機。

6-1、DHCP

電腦要連上網路必須要先設定 IP 位址、子網路遮罩、路由、DNS 等。一般使用者對這些網路設定並不熟，所以要讓使用者自己去建立非常麻煩。如果企業裡有上百台的電腦，需要由網管人員去分配每一台的 IP 位址、設定電腦實在是一件痛苦的事情。因此如果有 DHCP 伺服器，網路上的電腦只要設定好自動取得 IP 位址，系統開機後就可以自動取得網路設定。網管人員就不需要一台一台去設定。

在設定 DHCP 伺服器時，我們會設定要讓使用者自動取得的 IP 位址範圍、路由、DNS，在啟動 DHCP 伺服器之後，這些資訊就會放到記憶體中等客戶端來問。當一台使用 DHCP 自動取得 IP 的電腦連上網路後，它會以廣播的方式詢問網路上有沒有 DHCP 伺服器，而 DHCP 伺服器會回應，並送給客戶端網路設定的資料。客戶端收到這些資訊後，就將它設定為自己的 IP 位址、DNS 等。

如果以 DHCP 常用的話語來說，DHCP 分配出一個 IP 的情形叫做 DHCP「出租」IP 位址 給客戶端。DHCP 的租約是有期限的，時間到了之後，客戶端就必須重新取得一次 IP 位址，不過客戶端可以要求繼續使用同一個 IP。為了避免有機器一直要求使用同一個 IP，我們也可以設定同一個 IP 最長的租期是多久。

除了動態的分配 IP 位址 外，DHCP 也可以同時設定指派固定 IP 位址。每一張網路卡都會有一個固定的網路卡位址 (MAC、Physical Address)，例如，我們可以在 FreeBSD 中使用指令 ifconfig 或是在 Windows 中使用 ipconfig/all 來看到 MAC 的資訊。以下列為例：

```
# ifconfig
fxp0: flags=88c3<UP,BROADCAST,RUNNING,NOARP,SIMPLEX,MULTICAST> mtu 1500
options=b<RXCSUM,TXCSUM,VLAN_MTU>
inet6 fe80::202:b3ff:fe48:7c74%fxp0 prefixlen 64 scopeid 0x1
inet 10.0.0.1 netmask 0xff000000 broadcast 10.255.255.255
ether 00:08:c3:96:8c:22
media: Ethernet autoselect (100baseTX <full-duplex>)
status: active
```

上列粗體部份「00:08:c3:96:8c:22」就是網路卡位址，我們可以設定某個網路卡位址一定使用固定 IP 位址，如此一來，只要這一台機器使用 DHCP 要求 IP 位址 時，DHCP 伺服器都會給它固定的位址。

NG-UTM 是已 ZONE 為介面設計的 UTM，所以每個介面包含 802.1Q Vlan 都可以設定獨立的 DHCP 伺服器，基本上實體 Port 的 DHCP 伺服器設定都一樣，VLAN 的會稍微不一樣。

6-1-1、DHCP 用戶列表

系統根據介面列出已經使用 DHCP 服務的使用者，如果有多個介面，在介面上選擇要查看的介面，系統就只會顯示該介面的 DHCP 用戶，在列表中會出現使用者的主機名稱、使用時間跟狀態，狀態是指這一個使用者是上線中還是斷線，點選圖示後會把這一個使用者加入 DHCP 的黑名單中。

6-1-2、DHCP 伺服器

選擇要設定的實體介面，例如，ZONE0，每一個介面包含實體介面 ZONE 跟虛擬的 VLAN 介面，都會列出來讓管理者選取。

- 【介面資訊】：限虛擬的 VLAN 介面，選擇 802.1Q 後，此地會出現目前虛擬 Port 的介面讓管理者挑選。
- 【IP 位址】：這個實體 ZONE 的 IP 位址或是虛擬 VLAN 的 IP 位址。

  實體 ZONE 的 IP 位址

  是在【網路設定】的【網路介面】中的【介面位址】預先設定，如果【介面位址】有超過 2 個以上，這個地方就會列出來讓管理者選擇，如果沒有管理者要的區段，就需要回到【網路設定】的【網路介面】中的【介面位址】加入。

  虛擬 VLAN 的 IP 位址

  是在【網路設定】的【VLAN802.1Q】中的【IP 位址】預先設定，如果【IP 位址】有超過 2 個以上，這個地方就會列出來讓管理者選擇，如果沒有管理者要的區段，就需要回到【網路設定】的【VLAN802.1Q】中的【IP 位址】加入。

6-1-2-1、DHCP 伺服器設定

每一個 DHCP 伺服器的詳細設定，每一個 DHCP 伺服器可以設定 2 個區段。（圖 6-1）

- 【IP 範圍 1 起始跟結束位址介面資訊】：輸入 DHCP 伺服器的開始跟結束的 IP 位址，例如，192.168.1.20、192.168.1.30，代表發放這個範圍的 11 IP 位址。
- 【IP 範圍 2 起始跟結束位址介面資訊】：輸入 DHCP 伺服器的開始跟結束的 IP 位址，例如，192.168.1.200、192.168.1.230，代表發放這個範圍的 31 IP 位址。
- 【主要/次要的 DNS】：DHCP 用戶使用的主要 DNS 伺服器，例如，8.8.8.8 跟 168.95.1.1。

- 【主要/次要的 WINS】：選填，WINS 最主要用在 Windows 內網的名稱解析，DHCP 用戶使用的主要 WINS 伺服器，例如，192.168.1.100 跟 192.168.1.200。
- 【預設租約時間】：每次 DHCP 伺服器發放 IP 位址的有效時間，預設值為 720 分(12 小時)。
- 【最大租約時間】：每次 DHCP 伺服器發放 IP 位址的最長有效時間，預設值為 720 分(12 小時)。
- 【預設閘道器】：DHCP 用戶的閘道器 IP 位址，例如，192.168.100.254。
- 【網域名稱】：選填，DHCP 用戶的閘道器的網域名稱。
- 【啟用】：要不要啟用這一個 DHCP 伺服器。

圖 6-1 VLAN DHCP 伺服器設定

6-1-3、DHCP 固定 IP 位址

在定義介面的位址表時，有一個 IP 和 MAC 位址的設定方式，其中有一個選項(Get static IP address from DHCP Server)DHCP，勾選後，這一個 MAC 位址的電腦，每次用 DHCP 伺服器取得的 IP 位址，都會是固定。（圖 6-2）

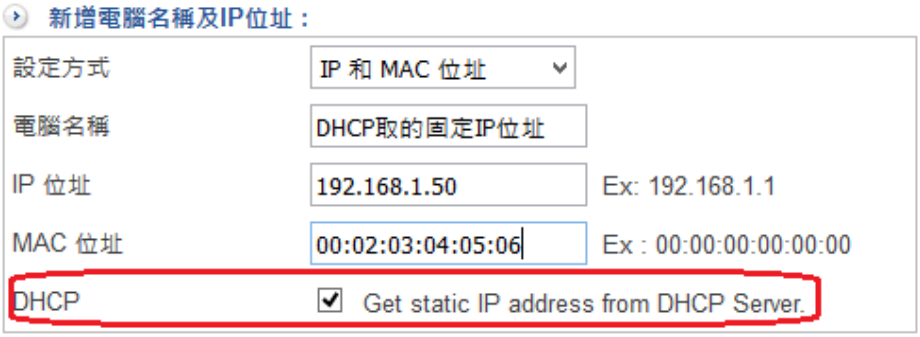


圖 6-2 DHCP 固定 IP 位址 設定視窗

在 DHCP 固定 IP 位址會出現下表。（圖 6-3）

電腦名稱	IP 位址	MAC 位址
coratt_ipmac	192.168.18.64	00:60:e0:51:ce:6a
coratt	192.168.18.64	00:60:e0:51:ce:6a

圖 6-3 DHCP 固定 IP 位址列表

6-1-4、DHCP 黑名單 MAC 位址

被列入黑名單的 MAC 位址會列在這裡，這些 MAC 位址就不能使用 DHCP 服務。

6-2、DDNS

當使用在動態 IP 位址的網路環境，DDNS 允許網際網路的使用者使用網址名稱來連線到您的伺服器，而不是使用 IP 位址，這也解決了動態 IP 位址的問題，NG-UTM 會按照設定的時間，跟提供 DDNS 服務的伺服器更新介面的 IP 位址，因此管理者只需要記住 DDNS 業者給你的網域名稱，就可以順利地連回到自己的伺服器。

DDNS 執行順序

要讓 DDNS 伺服器運作正常，有幾個預先步驟要先完成，順序如下：

1. 在“已註冊的 DDNS 服務”下拉選單，選取一個供應商來註冊。
2. 註冊完成後，跟著服務供應商的步驟申請一個網域名稱。
3. NG-UTM 的 DDNS 畫面中輸入您的 DDNS 的資料。
4. NG-UTM 自動地將您目前使用的介面 IP 位址傳送到 DDNS 伺服器上。

DDNS 伺服器設定

新增一個 DDNS 服務。（圖 6-4）

- 【開機自動啟用】：讓 DDNS 服務在開機後自動執行。
- 【服務】：選取提供 DDNS 服務的廠商。
- 【主機名稱】： 輸入申請的 DDNS 網域名稱，例如，homeLAN，後面選的就是提供服務的廠商，例如，3322.org，這樣完整的網域名稱就是 homeland.3322.org。
- 【對應介面】： 用哪一個介面的 IP 位址跟更新 DDNS 伺服器的資料。
- 【帳號】：填入您申請的 DDNS 服務的使用者名稱。
- 【密碼】：填入您申請的 DDNS 服務的密碼。
- 【註解】： 任何文字說明這個 DDNS 網域名稱。

- 【啟動】：要不要啟用這個 DDNS 網域名稱。

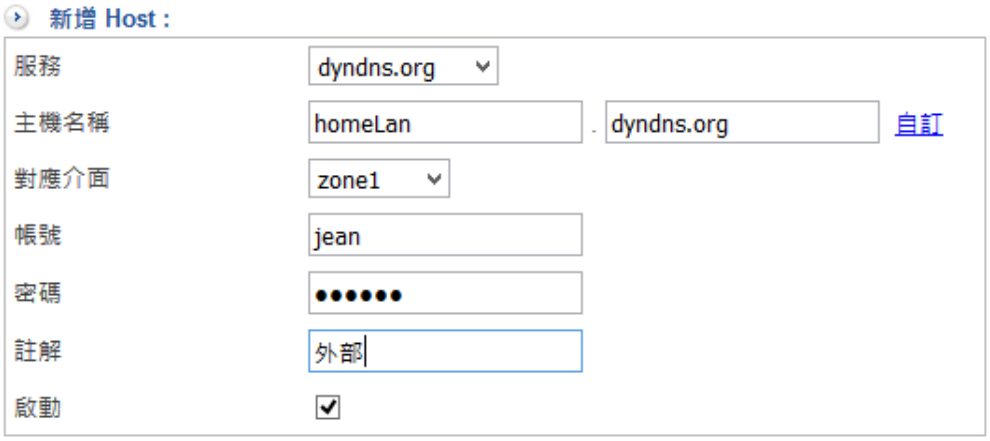


圖 6-4 DDNS 設定

DDNS 狀態

NG-UTM 會列出每一個 DDNS 網域名稱，目前的狀態。（圖 6-5）

- ：代表更新正常，：代表服務無法順利運作。
- 記錄：按鈕會顯示系統跟 DDNS 伺服器的通聯資料。
- 立即更新：讓 NG-UTM 立刻執行 DDNS 更新的動作。

圖 6-5 DDNS 狀態

6-3、SNMP

SNMP 是專門用於管理網路節點（伺服器、工作站、路由器、交換器...）的協定。網路管理者透過 SNMP 接收到的訊息，能即時發現並解決網路問題，或協助其規劃網路資源的運用。

SNMP 介紹

SNMP 管理的網路有三個構成要素：被管理的設備、代理、網路管理系統（NMSs，Network-management systems）。

目前 SNMP 有 3 種版本：

1.SNMPv1：欠缺加密及認證功能，皆以明碼傳送字串，使任何人皆可輕易攔截密碼，安全性備受爭議。

2.SNMPv2：改進第一版的許多安全缺陷，但執行速度能不如第一版快，且無法和其相容，因此不被廣泛接受。

3.SNMPv3：修正了前兩版的問題，不僅會對所有傳輸資料進行加密，而且可使 SNMP 代理程式對管理系統做認證動作，並確保數位簽章訊息的完整性。另外，針對每項訊息還會有存取清單的限制。

啟用 SNMP 服務

- 【開機自動啟用】：讓 SNMP 服務在開機後自動執行。
- 【裝置名稱】： 輸入 SNMP 的顯示名稱，例如，OfficeUTM。
- 【裝置所在地】：預設為 Taipei, Taiwan，可以是任何英文字。
- 【登入名稱】：預設為 public，只有讀的權限，管理者可已修改。
- 【聯絡人】：聯絡人的電子郵件帳號，預設為 help@common.com。
- 【註解】：預設為 Firewall，填入能描述的文字。

6-4、DNS 伺服器

網路是由無限多的電腦連線所構成，為了確保資料流動的正確性，每台電腦都有「固定而且單一」的「位址」，即是 IPV4 是 0～255 數字所組成的 IP 位址，IPV6 則是由 0000:FFFFF 6 個區段組合。

隨著連線主機的增加，對於一般使用者來說 IP 的位址不適合記憶與管理，因此會有 Domain 的出現。就像我們每個人一出生都會有一組身分證字號，但是一大串的身分證號碼難記憶，因此就會有名字或別名出現，方便稱呼。

網址是由主機名稱與網域名稱兩部分組合而成。例如：網路中文名稱為：www.ShareTech.com.tw，透過 DNS 解析，即可以指到：211.22.160.28 這台主機，因此我們不必要記誦這串難記的數碼，只要輸入網域名稱就可以連上該網站。而 www.ShareTech.com.tw 與 211.22.160.28 之間的對應，中間就需要 DNS Server 來轉換了。

我們可以知道，網路上是用 IP 來定址的，如果要使用讓人好記的 Domain Name 來連結，就要先在一台 DNS 伺服器上紀錄該網域內的名稱資料和 IP 的對應記錄，供人查詢出相對應的 IP。

為了達到這個功能，必須將不同的「紀錄」設定在 DNS 裡，目前比較常用的紀錄有 A、MX、CNAME、NS 等紀錄。以下分別說明這四種基本紀錄的用途與解說。

NG-UTM 支援 Inbound Loadbalance 機制，Inbound Loadbalance 就是利用 DNS 查詢的機制，當第一個來詢問 www.abc.com 時回應 WAN -1 線路位址，第二個來詢問時回應 WAN -2 線路位址，這樣就將服務平均分配在不同的線路上，達到負載均衡的目的。

要達成 Inbound Load balance 則網域名稱的解析權利必須在 NG-UTM 上。

DNS 名稱說明：

1. A 紀錄

IPV4 位址，主機名稱和其 IPV4 位址的對應關係，例如：www.ShareTech.com.tw 對應的 IPV4 位址為 211.22.160.28，當我們在瀏覽器輸入 www.ShareTech.com.tw ，透過 DNS 解析會找到 211.22.160.28 的 IP V4 位址，如果在網址直接輸入 211.22.160.28，也是可以找到網站主機。

A 紀錄是沒有數量限制，不同的 A 紀錄可已指向同一個 IPV4 位址，以上述的網站為例，可以再建立一筆 A 紀錄 www2.ShareTech.com.tw 對應到 IP V4 位址 211.22.160.28。

2. AAAA 紀錄

IPV6 位址，主機名稱和其 IPV6 位址的對應關係，例如：www.ShareTech.com.tw 對應的 IPV6 位址為 2001:288:502b::1，當我們在瀏覽器輸入 www.ShareTech.com.tw ，透過 DNS 解析會找到

2001:288:502b::1 的 IPV4 位址，如果在網址直接輸入 2001:288:502b::1，也是可以找到網站主機。

AAAA 紀錄是沒有數量限制，不同的 AAAA 紀錄可已指向同一個 IPV4 位址，以上述的網站為例，可以再建立一筆 AAAA 紀錄 www2.ShareTech.com.tw 對應到 IP 位址 2001:288:502b::1。

3. MX 紀錄

MX 紀錄主要的目的是讓郵件能正常的收發，讓寄件者得知負責接收郵件伺服器位址為何？通常負責處理接收的郵件伺服器會有兩台以上，所以會設定這兩台以上郵件伺服器的優先順序。設定 MX 紀錄的好處在於當您的郵件伺服器更換時，只需要修改 DNS 紀錄就可以了，對方的郵件主機不會理會您是用哪一台電腦來負責郵件交換。。

Host：指的是網域或主機名稱，也就是郵件地址@符號後面的部份，寫給這個名稱的郵件會被送到 host 欄位指定的郵件伺服器。

優先權：與某一台主機或網域有關的 MX 紀錄可能不只一個，所以需設定 Mail Server 的優先順序。當有人寄信到 jean@ShareTech.com.tw 時，會把信寄到 ms1.ShareTech.com.tw 這台主機上面，如果無反應時，就會將信寄到 ms2.ShareTech.com.tw 這台主機上。

Mail Server：通常指的是主機名稱，假設您架設為 Mail Server，您的主機名稱通常為 mail.ShareTech.com.tw。

設完 MX 記錄後，需注意是否有設定其相對應的 A 記錄或是 AAAA 紀錄。

4. CNAME 紀錄

「Nickname 別名」，可以給和網路位址(A)相對應之網域名稱，使用另外一個(或多個)網域名稱讓外面查詢。

nickname 別名：這個主機名稱的另外一個別名，nickname 可以是任何有效的主機名稱。

host: 這裡是主機的正式名稱。這個主機名稱必須是正式的主機名稱，不可以是別名。

在網址輸入 www.ShareTech.com.tw 或 web.ShareTech.com.tw 都會到達同個網站 (211.22.160.28)，其實 CNAME 紀錄就好像是 A 紀錄的分身，幫已存在的 A 紀錄設定其他的名字。

5. NS 紀錄

告訴其他 DNS Server 指定哪些伺服器作為網域或子網域的網域名稱解析伺服器。

6-4-1、網域設定

在 DNS 伺服器設定鐘，目前比較常用的紀錄有 A、MX、CNAME、NS 等紀錄。

DNS 伺服器建立步驟

要建立 DNS 伺服器，需要下列幾個步驟要先完成，順序如下：

1. 在【網域設定】中，輸入 DNS 網域及主伺服器 IP 位址。
2. 建立常用的 A、AAAA、MX、CNAME、NS 等紀錄。
3. 設定接受代理查詢的 IP 位址。

1、網域設定

上層的 DNS 伺服器服務商在管理者申請網域時，會要求一個固定 IPV4 的位址，這一個位址就是網域位址，當其他的 DNS 伺服器查詢管理者申請的網域時，會把這些查詢資料全部轉到這個 IP 位址上，再由管理者在此建立的 DNS 伺服器回應屬於這個網域下的 A、AAAA、MX、CNAME、NS 等紀錄。

建立一個全新的 DNS 伺服器網域，於【網域設定】中，新增下列資料。（圖 6-6）

- 【網域名稱】：申請的網域名稱，例如，def.com。
- 【網域位址】：首先需決定由哪一個介面回應外界 DNS 伺服器的查詢，這個 IP 位址，需要網際網路上能夠訪問到的固定 IPV4 位址，這個 IP 位址通常也是管理者在上層 DNS 伺服器申請時填入的 IP 位址。例如，由 ZONE 1 的 12.13.14.15 負責回應外界的 DNS 查詢要求，
- 【主伺服器名稱】：申請網域的主 DNS 名稱，例如，dns.def.com，系統會主動加入 2 個紀錄，一個是 SOA 紀錄，另一個是 A 紀錄。
- 【主伺服器位址】：申請網域的主 DNS 名稱的 IP 位址，此位址會自動加入 A 紀錄中。例如，12.13.14.15，則 A 紀錄中預設就會有一筆 dns.def.com 的 A 紀錄 IP 位址就是這裡填入的 12.13.14.15。
- 【擁有者的電子郵件地址】：輸入網域管理者的郵件，例如，jean@def.com

- 【資料更新時間】：DNS 的紀錄更新時間，預設是 10800 秒。
- 【資料重傳間隔】：DNS 的紀錄重傳間隔時間，預設是 3600 秒。
- 【資料過期時間】：DNS 的紀錄過期時間，預設是 604800 秒。
- 【預設資料有效期限】：DNS 的紀錄更新時間，預設是 38400 秒。
- 【建立對應反查網域】：啟用建立對應反查網域時，管理者需要輸入 DNS 反查的 IP 位址，這個功能只限定擁有一個 C 網域(256 個固定 IP 位址)的用戶，少於這個數量，一般都由 ISP 幫客戶做 DNS 反解。

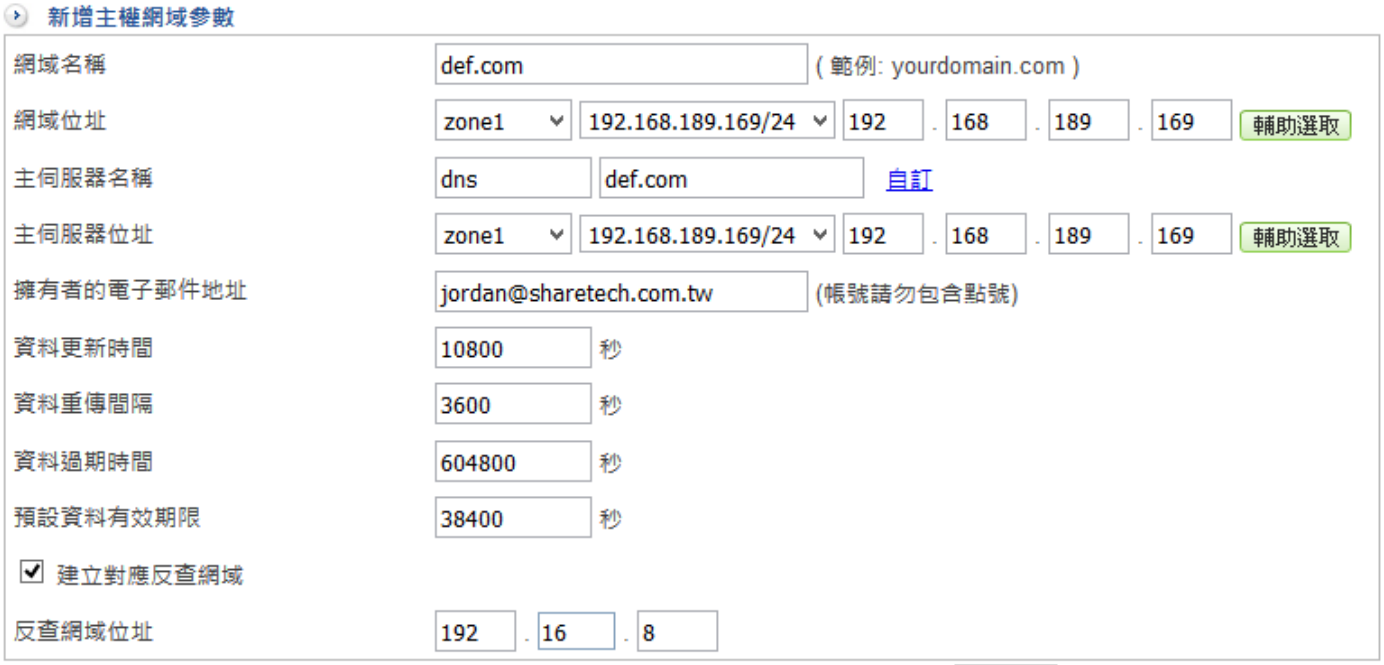


圖 6-6 建立 DNS 網域

建立 DNS 伺服器紀錄

完成基本的 DNS 伺服器之後，NG-UTM 會自動建立一個 DNS 伺服器列表，在狀態欄的 ，進入新增、刪除及修改所有的 A 紀錄、AAAA 紀錄、MX 紀錄、CNAME 等資料，當網域設定完成後，系統會自動建立 DNS 伺服器的對應 A 紀錄及 NS 紀錄，這 2 個數值就是在網域設定中輸入的 IP 位址。（圖 6-7）

圖 6-7 網域設定完成後 DNS 預設的紀錄

新增 A 紀錄

在新增資源記錄中，點選 ，代表要增加這個網域下的 A 紀錄。（圖 6-8）

- 【名稱】：建立新的 A 紀錄，英文跟數字的組合，例如，郵件伺服器要用名稱，mail.def.com。
- 【預設有效期限】：這筆 A 紀錄的有效期限。
- 【位址】：第一個欄位的 ANY，代表任何人來查詢這筆 A 紀錄，會回應後面欄位輸入的 IP 位址，第二欄位之後是選擇介面及 IP 位址，如果 DNS 是提供服務給外面查詢，這個介面需要是對外有效的介面及 IP 位址，如果 這筆 A 紀錄只是提供給內部使用，則可以是內部能訪問到的介面跟位址。
- 【DNS 備援】：當同一筆 A 紀錄設定 2 個不同 IP 位址，查詢不到 A 紀錄時，回應備援 A 紀錄 IP 位址，通常是在線路負載均衡或是 Server Load Balance 上使用。

圖 6-8 建立一筆 A 紀錄

新增 AAAA 紀錄

AAAA 記錄就是 IPV6 位址模式下的 A 記錄，在新增資源記錄中，點選 AAAA ，代表要增加這個網域下的 AAAA 紀錄，他的設定跟 A 紀錄一樣，只是 IP 位址選為 IPV6。

- 【名稱】：建立新的 AAAA 紀錄，英文跟數字的組合，例如，郵件伺服器要用名稱，mail.def.com。
- 【預設有效期限】：這筆 AAAA 紀錄的有效期限。
- 【位址】：第一個欄位的 ANY，代表任何人來查詢這筆 AAAA 紀錄，會回應後面欄位輸入的 IP 位址，第二欄位之後是選擇介面及 IP 位址，如果 DNS 是提供服務給外面查詢，這個介面需要是對外有效的介面及 IP 位址，如果 這筆 AAAA 紀錄只是提供給內部使用，則可以是內部能訪問到的介面跟位址。
- 【DNS 備援】：當同一筆 AAAA 紀錄設定 2 個不同 IP 位址，查詢不到 AAAA 紀錄時，回應備援 AAAA 紀錄 IP 位址，通常是在線路負載均衡或是 Server Load Balance 上使用。

線路負載均衡用的 A 紀錄跟 AAAA 紀錄

當同一個 A/AAAA 紀錄有 2 個不同的 IP 位址，代表要啟用 Inbound Loadbalance 的機制，選擇要啟用線路負載均衡的 A/AAAA 記錄，並點選他的狀態欄的 ，進入新增第二筆 A/AAAA 紀錄，在正查位址資料區點選新增，頁面會再度出現新增 A/AAAA 紀錄的設定畫面，建立第 2 筆的 A/AAAA 紀錄，因為是執行線路負載均衡，所以它的 IP 位址當然是另一組。

設定完同一個 A/AAAA 紀錄 2 組以上不同的 IP 位址後，在下方的 View 與回應位址區會出現 **any(負載平衡)** 字樣，管理者在這個區域設定每一個線路分擔的比例，共有 2 個模式可供選擇，一個是優先權模式，另一個是比例模式。（圖 6-9）

- 【優先權模式】：管理者藉由優先權跟權重的分配，把線路負載分配到適當的線路上，例如，第一條線路 100M，第 2 條線路 200M，希望外面訪問時多使用第 2 條線路，因此可以把線路 2 優先權設為 1 ，把權重設為 5，這樣大部分的使用量就會跑到線路 2 上面。

- 【比例模式】：管理者單純藉由權重的分配，把線路負載分配到適當的線路上，例如，第一條線路 100M，第 2 條線路 200M，希望外面訪問時多使用第 1 條線路，因此可以把線路 1 權重設為 10 ，線路 2 權重設為 1，這樣大部分的使用量就會跑到線路 1 上面。

圖 6-9 線路負載均衡設定

線路負載均衡的 A/AAAA 紀錄沒有數量的限制，只要有不同的線路跟 IP 位址都可以設定並啟用。

新增 MX 紀錄

在新增資源記錄中，點選 MX ，代表要增加這個網域下的 MX 紀錄，MX 記錄有優先權的觀念，數字越低代表優先權越高，如果同一個網域有 2 筆以上的 MX 紀錄，郵件服務器通常會優先高的 A/AAAA 紀錄主機溝通，使用 MX 一般而言，要先定義好 A /AAAA 紀錄，才能在選擇設定 MX 紀錄。（圖 6-10）

- 【網域名稱】：郵件伺服器用的網域名稱。
- 【預設有效期限】：這筆 MX 紀錄的有效期限。
- 【郵件伺服器】：郵件伺服器的 A/AAAA 紀錄，例如，mail.def.com。這個 A/AAAA 紀錄必須能夠查詢到，否則郵件無法正常傳遞跟接收。
- 【優先權】：優先權，可以填入 1 以上的數字，一般而言數字越低，優先權越高，例如，mail1.def.com 的優先權設為 5，mail2.def.com 的優先權設為 10。當外界要寄郵件寄信給 def.com 的郵件主機時，會先跟 mail1.def.com 要求寄信，除非 mail1.def.com 不回應(掛了)，才會由 mail2.def.com 回應。

圖 6-10 MX 紀錄

設定 MX 紀錄時，記得 MX 紀錄一定要有相對應的 A/AAAA 紀錄，否則郵件伺服器無法找到相對應的郵件主機位址，回應外界的要求。（圖 6-11）

MX

網域名稱	預設有效期限	優先權	郵件伺服器
def.com	38400	10	mail.def.com

NS

網域名稱	預設有效期限	名稱伺服器
def.com	38400	dns.def.com

A

名稱	預設有效期限	位址
def.com	38400	192.168.189.169(zone1)(any)
dns.def.com	38400	192.168.189.169(zone1)(any)
mail.def.com	38400	192.168.189.169(zone1)(any)...

圖 6-11 MX 紀錄跟 A/AAAA 紀錄

新增 NS 紀錄

當新建立一個網域時，自動就會建立一筆 NS 跟 A 記錄給 NS 使用，管理者也可以再新增其他筆 NS 記錄，在新增資源記錄中，點選 NS，代表要增加這個網域下的 NS 紀錄，一般而言，要先定義好 A/AAAA 紀錄，才能在選擇設定 NS 紀錄。（圖 6-12）

- 【網域名稱】：郵件伺服器用的網域名稱。
- 【預設有效期限】：這筆 NS 紀錄的有效期限。
- 【名稱伺服器】：名稱伺服器的 A/AAAA 紀錄，例如，dns2.def.com。這個 A/AAAA 紀錄必須能夠查詢到，否則用到這個 DNS 查詢時無法正常查詢。

MX

網域名稱	預設有效期限	優先權	郵件伺服器
def.com	38400	10	mail.def.com

NS

網域名稱	預設有效期限	名稱伺服器
def.com	38400	dns.def.com

A

名稱	預設有效期限	位址
def.com	38400	192.168.189.169(zone1)(any)
dns.def.com	38400	192.168.189.169(zone1)(any)
mail.def.com	38400	192.168.189.169(zone1)(any)...

圖 6-12 NS 跟 A/AAAA 記錄

新增 CNAME 紀錄

在新增資源記錄中，點選 CNAME ，代表要增加這個網域下的 CNAME 紀錄，一般而言，要先定義好 A 紀錄，才能在選擇設定 CNAME 紀錄。

- 【名稱】：使用 CNAME 的名稱，例如，mail2.def.com。
- 【預設有效期限】：這筆 NS 紀錄的有效期限。
- 【實際名稱】：當查詢 CNAME 時，實際回應的 A/AAAA 紀錄，例如，mail.def.com。這個 A/AAAA 紀錄必須能夠查詢到，否則用到這個 DNS 查詢時無法正常查詢。

  以上述範例，當外界查詢 mail2.def.com 時，會自動轉給 mail.def.com，實際上執行工作的是 mail.def.com，但這個網域名稱因為種種因素不希望外界知道她真實的名稱，此時可以用 CNAME 的機制，把她隱藏起來。

新增 TXT 紀錄

在新增資源記錄中，點選 TXT ，代表要增加這個網域下的 TXT 紀錄，每一個網域只可以有一個 TXT 紀錄，但是 SPF 中指定的 IP 位址卻可以多筆，SPF 是郵件傳送過程中，對方收信者確認你是這一個郵件伺服器的使用者。

- 【網域名稱】：輸入要採用 SPF 的網域名稱，例如，def.com。
- 【預設有效期限】：這筆 NS 紀錄的有效期限。
- 【SPF 設定】：在 TXT 欄位中 SPF 的紀錄，例如，ip4:12.13.14.15/24，代表 IPV4 12.13.14.15 這個 C 網段的 IP 位址都是正常的郵件服務器。

2、DNS 查詢介面

內建的 DNS 伺服器可以接受使用者的代理查詢，例如，內部的使用者可以將 DNS 伺服器指向 NG-UTM 的介面，當使用者要查詢 www.abc.com 時，NG-UTM 會代理這項 DNS 查詢服務，並將結果回應給內部的使用者，在【DNS 服務】>>【介面設定】中，新增下列資料。（圖 6-13）

- 【開放介面查詢】：管理者決定哪一個介面接受查詢或是代理查詢。
- 【接受代理查詢服務的 IP 位址】：指 NG-UTM 要幫內部的 IP 位址或是區段，做代理查詢，如果設定為 192.168.188.110，表示 NG-UTM 只允許此 IP 做代理查詢，而它就不用在連到外部去查詢 DNS 了，支援 IPV4/IPV6 位址。
- 【接受網域抄送的 IP 位址】：NG-UTM 具有 DNS Server 功能，而要不要讓其他的 DNS Server 抄寫我們的資料做備份，只要輸入其 IP 即表是允許它抄寫。例如：輸入 192.168.188.100 代表把我們上面 DNS 資料抄寫到它的主機上。

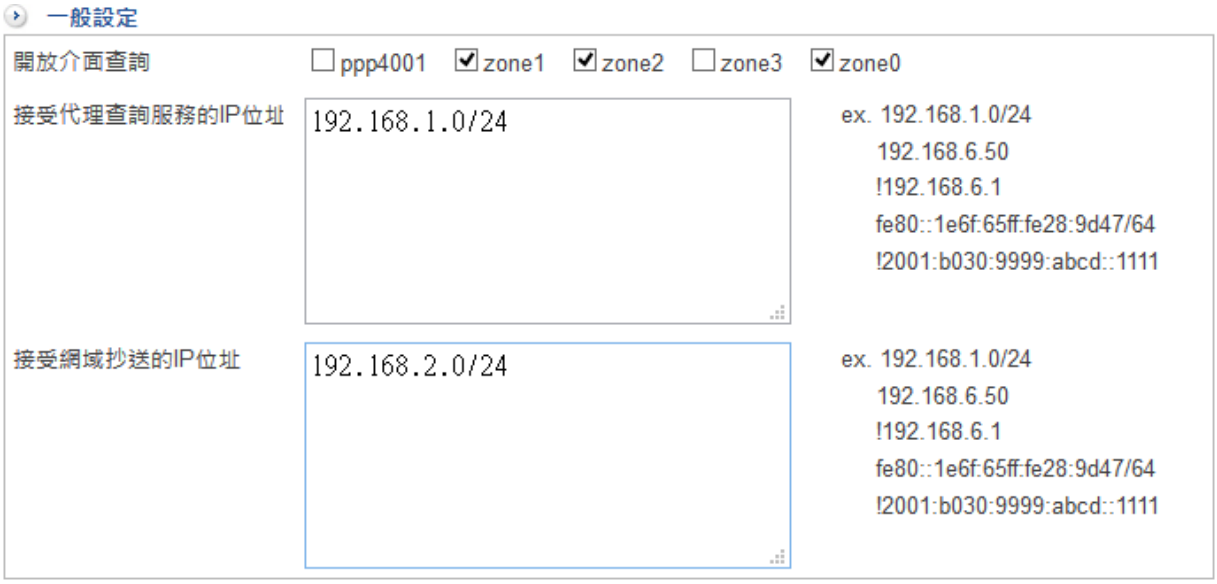


圖 6-13 代理查詢

6-4-2、View 設定

哪一個 IP 位址可以查詢內建的 DNS 伺服器，預設是 ANY，也就是任何一個來源 IPV4/IPV6 的 IP 來查詢，DNS 伺服器都會回應，如果對於某些 A/AAAA 紀錄希望只有特定網段的來源 IP 位址才可以查詢到，則可以在這裡建立這一些來源 IP 位址，並把他套用在 DNS 的紀錄上。（圖 6-14）

- 【View 名稱】：View 的名稱。
- 【來源 IP 位址】：接受查詢服務的 IP 位址，支援 IPV4/IPV6 位址，可以多筆資料輸入。

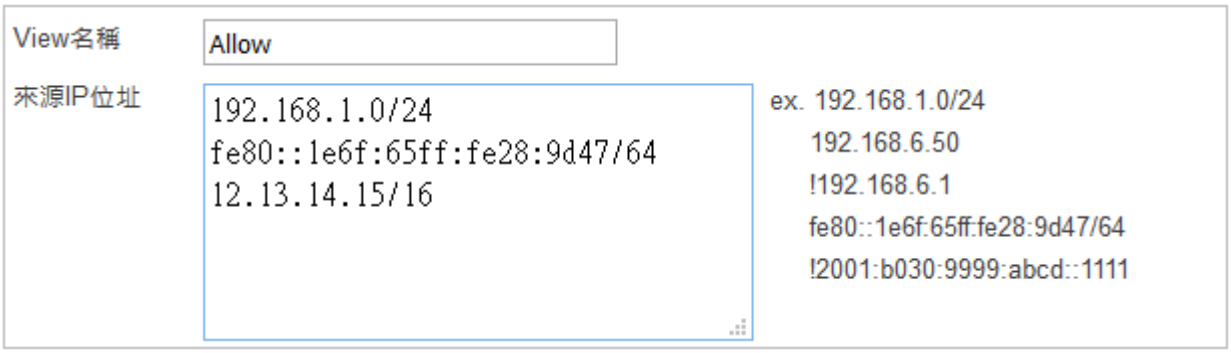


圖 6-14 DNS View 設定

設定完成後，在 DNS 伺服器的【網域設定】中，新增一筆 A/AAAA 紀錄就可以選擇這筆資料，這樣代表只有屬於 Allow 這一個群組的來源 IP 位址可以查訊。（圖 6-15）

圖 6-15 DNS View 回應

6-4-3、介面設定

NG-UTM 的 DNS 伺服器服務除了扮演自己網域的 DNS 解析外，也可以扮演一般公用 DNS 伺服器常有的代理查詢跟網域抄寫功能，代理查詢就是使用者查詢的網域資訊，當本機的 DNS 伺服器沒有資料時，會自動向外部 DNS 查詢，並將查詢結果轉給使用者，網域抄寫就是將自己 DNS 伺服器的資料複寫給別的 DNS 伺服器。（圖 6-16）

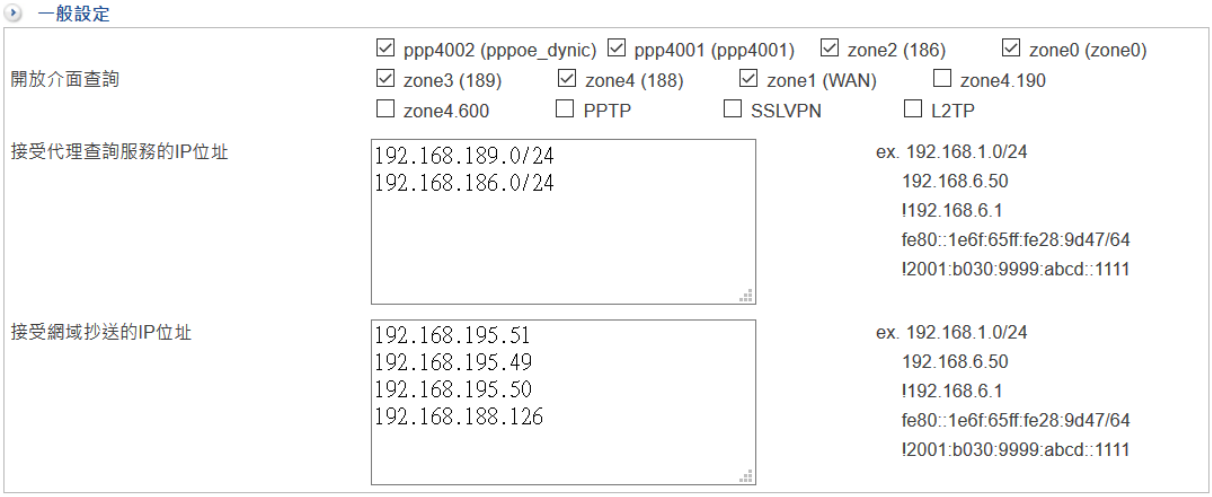


圖 6-16 DNS 介面設定

- 【開放介面查詢】：接受從哪一些介面進來的 DNS 查詢，沒有被勾選的介面他的 DNS 查詢都會被拒絕。
- 【接受代理查詢服務的 IP 位址】：接受代理查詢服務的 IP 位址，支援 IPV4/IPV6 位址，可以多筆資料輸入。
- 【接受網域抄送的 IP 位址】：接受網域抄送的 IP 位址，支援 IPV4/IPV6 位址，可以多筆資料輸入。

6-5、病毒引擎

NG-UTM 提供 2 個掃毒引擎，一個是免費的 ClamAV 跟需要付費的 Kaspersky 掃毒引擎，預設上 ClamAV 掃毒引擎是開啟的，所以在管理介面套用的掃毒機制就是由他提供，上傳 Kaspersky 掃毒引擎的授權後，主要的掃毒引擎就會換成 Kaspersky。

6-5-1、ClamAV 掃毒引擎

ClamAV 全名是 Clam Antivirus，它跟 Linux 一樣強調公開程式碼、免費授權等觀念，ClamAV 24 小時更新及維護病毒資料庫，任何人發現可疑病毒也可以隨時跟她們取得聯繫，立刻更新病毒碼。

- 【ClamAV 掃毒引擎目前狀態】：預設都是啟用，也沒有關閉的選項。
- 【引擎版本】：目前使用的掃毒引擎版本，例如，ClamAV 0.98.4。
- 【更新紀錄】：每次掃毒引擎的更新紀錄都會列在這裡。
- 【清除紀錄】：把更新紀錄清除掉。
- 【病毒碼自動更新時間】：每次更新病毒資料庫的時間，預設為 6 小時，設定範圍是 1~24 小時。
- 【ClamAV Database mirrors】：選擇更新病毒資料庫的伺服器。
- 【立即更新】：馬上更新病毒資料庫。
- 【更新紀錄】：

6-5-2、Kaspersky 掃毒引擎

Kaspersky 掃毒引擎需要授權碼才能生效。

- 【Kaspersky 掃毒引擎目前狀態】：預設是關閉，需要上傳授權文件才可以啟用。
- 【引擎版本】：目前使用的掃毒引擎版本。
- 【病毒碼數量】：顯示最新的病毒碼數量。
- 【更新紀錄】：每次掃毒引擎的更新紀錄都會列在這裡。
- 【病毒碼自動更新時間】：每次更新病毒資料庫的時間，預設為 6 小時，設定範圍是 1~24 小時。
- 【清除紀錄】：把更新紀錄清除掉。
- 【立即更新】：馬上更新病毒資料庫。
- 【Licenses】：上傳掃毒引擎的授權文件。

6-6、SandStorm

釣魚郵件肆虐及惡意的網址流竄，使用者往往不小心誤開或是誤點惡意的網址，而這一些惡意的木馬軟體或是網址並不是傳統的病毒軟體可以防護的，防火牆是安全的第一道(由外對內)也是最後一道(由內對外)防線，所以 NG-UTM 在這道防線上加入新型的防護機制。

6-6-1、Sandstorm

不論是使用者誤點惡意網址、網址中有惡意程式或是郵件中夾帶的附檔有惡意程式，Sandstorm 會自動比對，當有比對到這一些惡意行為時，NG-UTM 會主動阻擋，Sandstorm 的資料會自動更新，讓 NG-UTM 維持的阻擋力。

1、Sandstorm

設定 Sandstorm 啟用的功能，有 3 個項目分別是 File Hash、Web URL 跟 Domain。（圖 6-17）

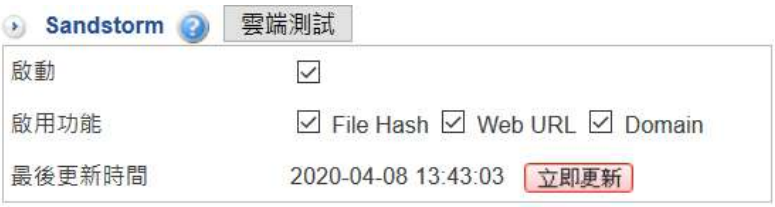


圖 6-17 SandStorm 設定

- 【雲端測試】：管理者可以上傳檔案或是 URL、網址到 Sandstorm 中比對是否在黑名單資料庫中，點選【雲端測試】，系統會開啟另一個頁面，選擇要比對的項目後上傳檔案或是輸入 URL、網址，資料庫就回應是否為在黑名單中。（圖 6-18）

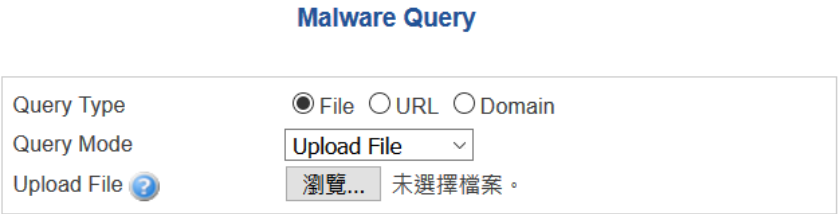


圖 6-18 SandStorm 雲端測試

- 【啟用功能】：Sandstorm 可以掃描 2 種類型的木馬程式，一個是檔案類型另一個是網址類型，而者 2 種類型分別有可能透過 WEB 或是郵件方式傳遞，管理者需要確認需要的服務是 2 者都要還是特定一種。

  檔案類型跟 URL 分別在 WEB 或是郵件中都會存在，管理者需要在不同地方設置，這裡會用超連接讓管理者快速進入設定。

- 【最後更新時間】：Sandstorm 會定期去資料庫拉最新的資料，按下【立即更新】可以馬上更新黑名單的資訊。

2、FILE Hash

- 【版本】：目前的版本及木馬數量，括弧內的就是木馬數量。
- 【風險程度】：每一個樣本都會被歸類為高、中、低 3 種風險，管理者可以根據自己的需求調整，如果怕誤檔正常檔案傳輸，就可以取消低風險的阻擋。
- 【WEB/郵件服務】：啟用這項功能後，需要在管理介面上執行一些設定，這裡把需要設定的網頁連結，方便管理者操作。

3、Web URL

- 【版本】：目前的版本及木馬數量，括弧內的就是木馬數量。
- 【風險程度】：每一個樣本都會被歸類為高、中、低 3 種風險，管理者可以根據自己的需求調整，如果怕誤檔，就可以取消低風險的阻擋。
- 【WEB/郵件服務】：啟用這項功能，需要在管理介面上執行一些設定，這裡把需要設定的網頁連結，方便管理者操作。
- 【Url 測試】：點選【Url 測試】後，系統會開啟另一個頁面，直接輸入 URL，資料庫就回應是否為在黑名單中

4、Domain

- 【版本】：目前的版本及阻擋網址數量，括弧內的就是數量。
- 【風險程度】：每一個樣本都會被歸類為高、中、低 3 種風險，管理者可以根據自己的需求調整，如果怕誤檔，就可以取消低風險的阻擋。
- 【DNS】：啟用這項功能，需要在管理介面上執行一些設定，點選後直接進入 DNS Filter 的管理頁面。
- 【Domain 測試】：點選【Domain 測試】後，系統會開啟另一個頁面，直接輸入 Domain 名稱，資料庫就回應是否為在黑名單中

6-6-2、Sandstorm 紀錄

管理者根據日期、功能、服務類型、風險程度或是 IP 位址等條件搜尋後的結果如下，系統會根據每一種攻擊特徵統計攻擊次數。（圖 6-19）

	日期	功能	惡意程式類型	目標資訊	風險程度	次數	詳細	啟用
☐	2020-04-08 13:39:29	Domain	Malware	nengchima.com	高	4		
☐	2020-04-06 18:35:10	URL	Malicious host	storage.googleapis.com/	低	63		
☐	2020-04-06 17:42:55	URL	Phishing	e.dtscout.com/e/	低	5		

圖 6-19 Sandstorm 紀錄

- 【功能】：Sandstorm 有 3 個阻擋項目分別是 File Hash、Web URL 跟 Domain，這筆阻擋紀錄是屬於哪一類。
- 【惡意程式類型】：木馬或是釣魚郵件類型。
- 【次數】：同一個項目在在統計期間內發生的次數。

如果管理者覺得 Sandstorm 的阻擋誤擋了使用者正常行為，可以在啟用那一個欄位把誤擋的項目停用，這樣就可以避免誤擋，相關的停用資訊，可以在 Sandstorm 停用清單中找到。

點選詳細的圖示，內部哪一個 IP 位址點了這個木馬的行為通通詳細列出。（圖 6-20）

惡意程式資訊：

功能:	URL
惡意程式類型:	Malicious
風險程度:	中
URL:	crl.starfieldtech.com/sfroot-g2.crl

詳細： 1 / 1 跳至 1 頁數 、每頁 16 筆 GO

日期	服務類型	IP	目標
2019-10-04 08:39:11	Web	192.168.190.241	http://crl.starfieldtech.com/sfroot-g2.crl
2019-10-04 08:34:11	Web	192.168.190.241	http://crl.starfieldtech.com/sfroot-g2.crl
2019-10-04 08:33:11	Web	192.168.190.241	http://crl.starfieldtech.com/sfroot-g2.crl

圖 6-20 Sandstorm 詳細紀錄

6-6-3、Sandstorm 停用清單

被 Sandstorm 阻擋的檔案、URL 跟 Domain 會列在這裡。

6-7、WEB 服務

NG-UTM 可掃描 HTTP 跟 HTTPS 的通訊協定，並檢查傳遞的內容是否含有病毒，除了能夠檢查這 2 種協定的封包外，也能把使用者瀏覽的網址紀錄下來，方便管理者日後查詢跟管理，HTTP/HTTPS 的掃描跟紀錄方式是採用 Transparent Proxy 模式，使用者不需要再瀏覽器做任何設定即可以運作。

HTTPS 部分牽涉到 SSL 憑證信任，使用前管理者在 NG-UTM 產生一個 SSL 根憑證，再將這個根憑證安裝到使用者的電腦上。

在信任根憑證上不同的作業系統有不同的做法，一般而言，APPLE 公司的電腦、手機不接受非他信任的根憑證，所以 WEB 服務功能在 APPLE 系統上是失效。Windows 系統信任的根憑證及 Firefox 信任的根憑證也在不同地方，使用上要特別注意使用的瀏覽器信任存放在哪裡的根憑證。

6-7-1、WEB 設定

設定 HTTP 掃毒使用的掃毒引擎，管理者根據網路的實際狀況，配置相關的規格，讓 WEB 服務運作正常。（圖 6-21）

- 【最大掃描檔案大小 (KB)】：當 WEB 傳輸的檔案超過設定值，就不執行掃毒，預設是 1024KBytes。
- 【監聽 Port】：哪一些 PORT 要導入 HTTP PROXY，預設是 80，管理者可以多筆輸入，例如，80,81,88，代表這 3 個 PORT 都會導入 HTTP 檢查。
- 【使用掃毒引擎】：共有 ClamAV 跟 Kaspersky 2 種可供選擇，預設是 ClamAV。
- 【掃描結果網頁設定】：當發現病毒時，出現的警告訊息給使用者。
- 【主題】：輸入顯示的主題文字，可以是任何文字。
- 【欲顯示的內容】：輸入阻擋網頁的內容。
- 【預覽】：點選預覽後可以比對輸入文字是否符合管理者的設計。

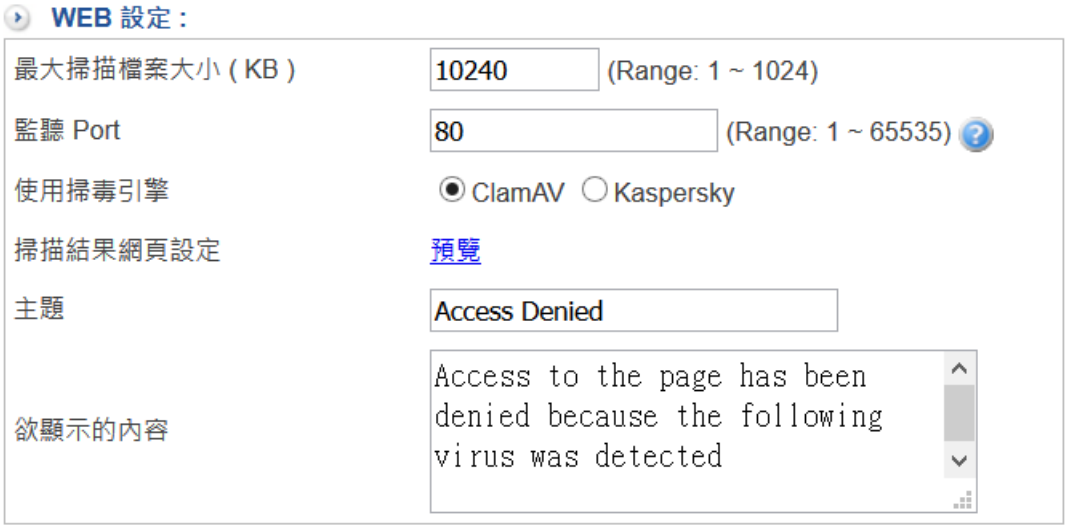


圖 6-21 WEB 設定跟中毒網頁警示預覽

加密連線設定

NG-UTM 除了可以對 HTTP 進行管理外，對於 HTTPS 也可以執行掃毒及網站的管理，要進行 HTTPS 管理前必須產生 SSL 的根憑證，並把這個憑證匯入每一個使用者的電腦中，HTTPS 也是使用 Transparent Proxy 技術，所以使用者不需要設定任何瀏覽器項目，除了匯入憑證外。

- 【加密連線監聽 Port】：哪一些 PORT 要導入 HTTPS PROXY，預設是 443，管理者可以多筆輸入，例如，443,8443,888，代表這 3 個 PORT 都會導入 HTTPS 檢查。
- 【憑證產生時間】：目前本機產生的根憑證時間。
- 【下載 SSL 憑證】：按下載就可以把 NG-UTM 本機的根憑證下載到管理者的電腦中，管理者再將這憑證傳給使用者，如果有修改 SSL 根憑證的內容，都需要在重新產生根憑證並下載，按下【重新產生憑證】就會出現對話框。（圖 6-22）

圖 6-22 重新產生憑證

- 【憑證下載連結】：管理者也可以給每一個使用者一個 URL，讓使用者點選之後，自己安裝憑證，這個連結組合有三個部分

  1. 網路介面 IP 位址或網域 ，例如，ZONE1 介面 IP 位址是 192.168.1.254。
  2. 在【網路介面及路由 > 網路介面 > HTTPS Port】中設定的 PORT，預設是 443。
  3. myca.crt 是根憑證的名稱

  在這個範例中，下載的 URL 就是 https://192.168.1.254:443/myca.crt ，使用者點選後就會自動安裝憑證。

- 【憑證安裝程式下載連結】：當使用者切換不同瀏覽器，信任的根憑證也要對應式的匯入，為了避免這個麻煩，ShareTech 提供 Windows 系統下的安裝程式，執行這個安裝程式使用 3 大瀏覽器 IE、Chrome、Firefox 的信任根憑證就全部裝好。

  管理者給每一個使用者一個 URL，讓使用者點選之後，自己下載安裝程式，這個連結組合有三個部分

  1. 網路介面 IP 位址或網域 ，例如，ZONE1 介面 IP 位址是 192.168.1.254。
  2. 在【網路介面及路由 > 網路介面 > HTTPS Port】中設定的 PORT，預設是 443。
  3. download_certinstaller.php 就是安裝程式的頁面。

  在這個範例中，下載的 URL 就是 https://192.168.1.254:443/download_certinstaller.php ，使用者點選後就會自動下載安裝程式，執行安裝程式後，需要的根憑證就安裝完畢。（圖 6-23）

圖 6-23 HTTPS 設定

- 【Apple 裝置不導入服務】：Apple 的信任憑證清單無法新增，使用 https proxy 時會導致無法連線，勾選後所有 Apple 的設備都不會進入 https proxy 中。
- 【不導入服務 Domain 自訂】：不導入 http/https 過濾的網站。
- 【不導入服務 IP 自訂】：不導入 http/https 過濾的 IP 位址。
- 【導入服務 Domain 自訂】：導入 http/https 過濾的網站
- 【導入服務 IP 自訂】：導入 http/https 過濾的 IP 位址。

憑證安裝程式設定

為了方便使用者下載 SSL 憑證，當使用者要瀏覽網頁時，如果 NG-UTM 發現這一個 IP 位址尚未安裝 SSL 憑證，就會將使用者的網頁自動轉向到下載憑證的網址，方便使用者操作。（圖 6-24）

圖 6-24 SSL 憑證下載轉址

- 【轉址通訊埠】：使用的 PORT 號，必須是沒被使用的。
- 【通訊協定】：使用 http 還是 https 當作轉址的協定。
- 【來源 IP 位址】：哪一些來源 IP 的人才會使用這項服務，不是這個 IP 範圍的人就不受影響。
- 【已瀏覽 IP】：哪一些 IP 已瀏覽過。

當設定的來源 IP 尚未安裝 SSL 憑證，他瀏覽的網頁會被自動轉址到下列的網頁，網頁中有 Web 憑證安裝程式及安裝說明。（圖 6-25）

圖 6-25 轉址網頁及安裝說明

SSL 憑證資訊

顯示目前 NG-UTM 使用的 SSL 憑證資訊，相關的憑證設定在【系統設定】>【SSL 憑證設定】>【SSL 憑證設定】中，如果 SSL 憑證有修改，每一個使用者的根憑證都需要在重新安裝及信任。

匯入 SSL 憑證

匯入 SSL 憑證，包含自行輸入或是申請的合法憑證。

6-7-2、HTTPS 連線紀錄

所有透過 HTTPS proxy 連線的紀錄都會在這裡，預設是關閉。（圖 6-26）

HTTPS紀錄列表　1 / 7018　跳至 1 頁數，每頁 16 筆 GO　匯出　匯出全部

時間	HTTPS名稱	介面	來源 IP	目的 IP
2018-06-20 17:45:49	demohiguardx.ddns.net	zone2	192.168.186.40	125.224.245.21
2018-06-20 17:45:49	demohiguardx.ddns.net	zone2	192.168.186.40	125.224.245.21
2018-06-20 17:45:49	demohiguardx.ddns.net	zone2	192.168.186.40	125.224.245.21
2018-06-20 17:45:49	demohiguardx.ddns.net	zone2	192.168.186.40	125.224.245.21

圖 6-26 https 連線紀錄

6-7-3、白名單憑證

有一些網站或是應用程式經過 NG-UTM 後會產生憑證失敗，導致後續的服務都不能用，此時，管理者可以到這裡，將那一些失敗的憑證加入白名單中，下次 NG-UTM 看到白名單的憑證，就不會進行置換的動作，使用者的服務就不會收受到影響。

尋找失敗憑證

按下【搜尋】按鍵，NG-UTM 就會列出這一段時間內失敗的憑證，選擇要加入白名單憑證後按下【新增到白名單憑證】的按鈕後就完成。（圖 6-27）

憑證失敗記錄　1 / 1　匯出　匯出全部

時間	來源 IP	目的 IP	網域	次數
2018-06-20 10:00:03	192.168.189.225	216.58.200.35	ssl.gstatic.com	8
2018-06-20 09:59:58	192.168.189.225	172.217.160.67	www.google.com.tw	16
2018-06-20 09:59:57	192.168.189.225	172.217.24.4	www.google.com	3
2018-06-20 09:59:05	192.168.189.225	172.217.160.99	ssl.gstatic.com	8

圖 6-27 失敗的憑證

白名單憑證列表

新增的白名單憑證會列表如下。（圖 6-28）

白名單憑證列表

目的 IP	網域
54.169.185.6	24h.pchomeapp.com
210.242.43.176	24h.m.pchome.com.tw
210.242.216.53	shopping.pchome.com.tw
216.58.200.40	www.googletagmanager.com
210.242.43.154	ecvip.pchome.com.tw
210.242.216.52	a.ecimg.tw
104.107.54.70	www.global-ebanking.com
103.227.227.18	cobank.tcb-bank.com.tw

圖 6-28 白名單憑證列表

6-8、高可用性

NG-UTM 提供高可用性（High Availability）功能，使用 2 台相同的 NG-UTM，一台為 Master，另一台為 Backup，萬一 Master 主機發生故障，馬上由 Backup 設備接手，讓網路封包不會發生斷線情況，維持企業的運作。

管理人員亦可立即獲得高可用性切換的訊息，來對原本故障的主機做修復保養的工作，使其能夠盡快恢復運作，來保障網路永續通暢。

NG-UTM 的 HA 架構為 Active-Backup 模式，也就是說 2 台設備只有一台是在工作中，另一台是 Standby 狀態，只有工作中的設備故障後，Backup 的主機會立刻接手所有的網路流量。

啟用高可用性之前，要先到【網路設定】>【區域設定】中指定哪一個 Port 為 HA Port。

高可用性-Master

- 【啟用】：要不要啟用 HA 功能。
- 【模式】：這一台設備的角色是 Master 主機。
- 【管理 IP】：啟用 HA 後，2 台設備會產生一個共同的虛擬 IP 位址，不論哪一台設備運作，除了可以用原始設備的 IP 位址進入外，也可以用這一個共同的虛擬 IP 位址管理設備，這一個虛擬的 IP 位址就是管理 IP。

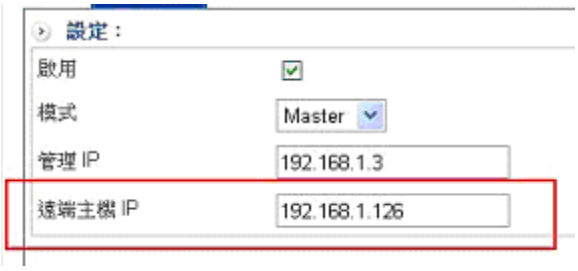
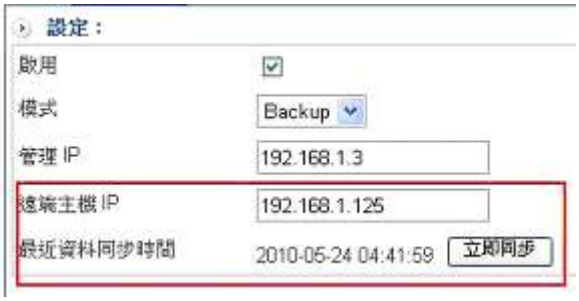
  設定管理 IP 位址時要注意，必須跟原來介面的 IP 位址是同一個網段，否則會無法進入。例如，原來介面的實體 IP 位址是 192.168.1.1/24，則管理 IP 位址就可以設為 192.168.1.5。
- 【遠端主機 IP】：當運作模式為 Master 時，這一個 IP 位址就是 Backup 主機的實際 IP 位址。

高可用性-Backup

- 【啟用】：要不要啟用 HA 功能。
- 【模式】：這一台設備的角色是 Backup 主機。
- 【管理 IP】：啟用 HA 後，2 台設備會產生一個共同的虛擬 IP 位址，不論哪一台設備運作，除了可以用原始設備的 IP 位址進入外，也可以用這一個共同的虛擬 IP 位址管理設備，這一個虛擬的 IP 位址就是管理 IP。

設定管理 IP 位址時要注意，必須跟原來介面的 IP 位址是同一個網段，否則會無法進入。例如，原來介面的實體 IP 位址是 192.168.1.1/24，則管理 IP 位址就可以設為 192.168.1.5。

- 【遠端主機 IP】：當運作模式為 Backup 時，這一個 IP 位址就是 Master 主機的實際 IP 位址。

Master 主機	Backup 主機
	

2 台主機開啟 HA 後，介面 IP 位址必須在同網段內的不同 IP 位址，否則會造成 IP 位址衝突。以上表為例，當本機設為 Master，遠端主機位址設為 192.168.1.126，則 192.168.1.126 就是 Backup 主機，NG-UTM 會向遠端主機 192.168.1.126 檢查型號群組和版本是否相同，檢查成功後才可以做同步動作。

Backup 主機， 會顯示最近資料同步時間，NG-UTM HA 的 Backup 主機每隔間 5 分鐘向 Master 要求同步資料，管理者也可以手動按立即同步。

註 1、當 HA 切換至 Backup，在 Backup 主機所做的任何修改設定，Master 復原起來後，系統不會向 Backup 同步回差異資料。如果需要將 Backup 的資料同步回 Master，可以將二台角色做互換， Master 改為 Backup，Backup 改為 Master， 這樣資料就會以最初設定的 Backup 為準。

註 2. 不會被同步的資料， 如下：

內容記錄器錄下的資料

系統操作日誌

系統/網路狀態圖

電腦成員列表

流量分析資料

6-9、遠端紀錄伺服器

遠端連線設定

NG-UTM 可以把 封包的通聯記錄用 Syslog 的方式送出給外部的 Syslog 伺服器，讓 Syslog Server 將這一些資訊保存或是進一步分析。（圖 6-29）

- 【啟用】：要不要啟用 Syslog 功能。
- 【Server IP】：遠端 Syslog 的 IP 位址，例如，192.168.1.100。
- 【Server Port】：遠端 Syslog 使用的 Port，預設為 UDP 514。
- 【設備主機名稱】：以甚麼名稱送出，在 syslog server 就會出現這一個設定的名稱，這樣在 syslog server 就可以分辨紀錄來自哪一台設備。

Log 設定

NG-UTM 能送出 2 種格式的 syslog，一個是標準 Syslog 格式，一個是 CEF 格式，使用哪一種格式由 Syslog Server 決定。

Log 項目

- 目前可以送出 6 種紀錄給 Syslog 伺服器，每個項目後都有不只一個的細項，由管理者決定。

  1、管理目標

  2、進階防護

  3、郵件管理

  4、內容記錄

  5、日誌

  6、系統狀態

第 7 章 進階防護

NG-UTM 可透過異常 IP 分析跟交換器（Switch）的協同防護，即時監控內部機器的分部狀況，於內部網路發出大量異常封包時，阻擋此類封包的傳送，並協助管理人員盡速排除異常狀態，可以在事件發生的第一時間內知道哪一個電腦在哪一個交換器 PORT 上，避免企業網路癱瘓。

協同防護的解決方案觀念很簡單，讓 UTM 跟 Switch 能夠互相溝通，貢獻自己優異的功能，簡單來說，利用 UTM 偵測到的不合理的資安問題，除了本身對外的管制動作外封鎖外，再利用 SNMP 或是 TELNET/SSH 的命令通知 SWITCH 執行簡單的 PORT 封鎖/管制。既可以不改變使用者的任何使用習慣，又可以在第一時間發現異常時，將出問題的電腦封鎖在一個小範圍內，如（圖 7-1）。

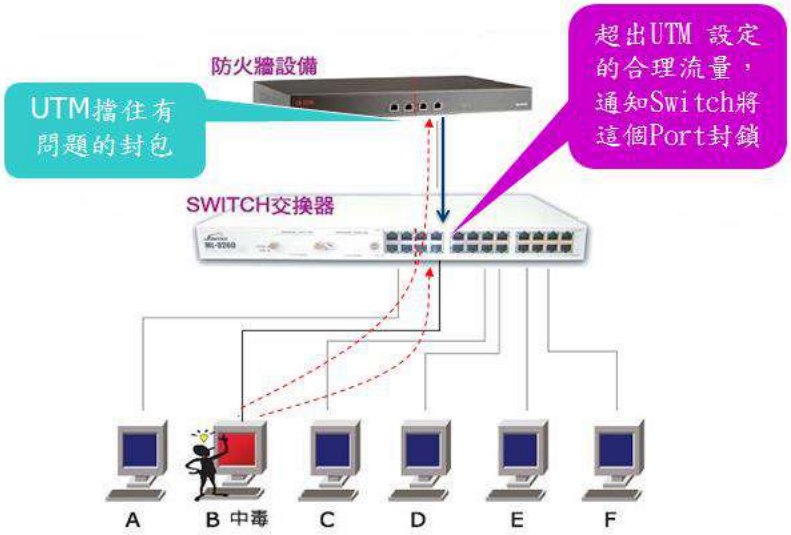


圖 7-1 協同防禦基本概念

一般而言，Layer 2 且支援 SNMP 協定的交換器在市價上是可以被接受的範圍，所以我們的解決方案不會有聽起來很好，但要實際做到時因為費用或是佈署上的問題，導致『曲高和寡』的困境。就算因為費用的因素，無法全面換成這樣的交換器，也可以將內網的渾沌區域限制在一個小小的範圍。

如果選擇協同防禦的交換器，則可以執行 IP-PORT-MAC 互鎖的功能。

7-1、異常 IP 分析

當 NG-UTM 偵測到介面跟介面間的網路封包傳遞有不正常連線數量、上下載流量時，可以採取 3 個動作，紀錄、通知跟阻擋，管理者可以 3 個全選或是任選其一二，確保網路能夠正常運作。

1.紀錄：

從介面出去或是進入介面的連線數、上下載流量超過設定值，NG-UTM 會記錄觸發這個動作的事件跟來源 IP 位址，管理者事後可以透過查詢知道何時發生。

2.通知：

從介面出去或是進入介面的連線數、上下載流量超過設定值，NG-UTM 會記錄觸發這個動作的事件跟來源 IP 位址，同時根據設定的方式，通知管理者。

3.阻擋：

從介面出去或是進入介面的連線數、上下載流量超過設定值，NG-UTM 會記錄觸發這個動作的事件跟來源 IP 位址，同時根據設定的方式阻擋這個行為繼續發生。

不論使用者執行哪一種軟體，從網路封包傳輸的角度，分成幾個現象，上傳、下載的連線數量(Connect Session)、流量(Flow)跟持續時間(Time)，藉由偵測這些數量的組合，推估使用者是正常使用網路或是有異常的行為。

當發現偵測出使用者異常行為後，管理者可以採取多種策略，例如，阻擋上網、立即限制他的最大頻寬、啟用協同防禦機制通知交換器將他封鎖或是通知管理者就好。

以看網路影片為例，它使用約 5Mbps 的下載頻寬且會持續一段時間，但是它不會占據你的上傳頻寬及超高的連線數，管理者可以設定一個正常網路行為下都不會被觸發的數值，讓 NG-UTM 幫你做第一線的把關。

萬一，真的有人觸發了上限值，管理者可以採取限制頻寬、封鎖或是通知交換器將這一個 PORT 關閉的三種處理方式，管理者可以針對自己的需求採取對應的處理原則，例如對於出租型的宿舍網路，屬於非常強制類型，有人違反規定時，把它的頻寬縮小，讓它可以『慢慢地』使用網路。

在設定值部分，紀錄設定 =< 通知設定 =< 阻擋設定。

7-1-1、共同設定

選擇異常 IP 的偵測介面，NG-UTM 會把所有設定好的介面列出，讓管理者勾選，只有啟動的介面才會有偵測服務。

7-1-2、紀錄設定

當網路封包超過設定值的事件，NG-UTM 紀錄下當時的來源 IP 位址跟觸發數量及持續時間，讓管理者事後查詢，這個設定值適用於整個 NG-UTM 的所有介面(ZONE)。

基本設定

內部電腦出去介面(ZONE)外的異常流量偵測值。

- 【Session 量超過】：每一個來源 IP 位址，出去介面(ZONE)的網路連線數數量，當超過設定值且持續一段時間後，NG-UTM 就會把來源 IP 位址跟超過的數值紀錄下來，例如，設定 Session 超過【100】，持續【120】秒，介面(ZONE)內部任一 IP 位址對外的連線超過 100 個且持續 120 秒，就會被紀錄。
- 【上傳流量超過】：每一個來源 IP 位址，出去介面(ZONE)的上傳頻寬，當超過設定值且持續一段時間後，NG-UTM 就會把來源 IP 位址跟超過的數值紀錄下來，例如，設定上傳流量超過【100】，持續【120】秒，介面(ZONE)內部任一 IP 位址對外的上傳頻寬超過 100Kbps 個且持續 120 秒，就會被紀錄。
- 【下載流量超過】：每一個來源 IP 位址，出去介面(ZONE)的下載頻寬，當超過設定值且持續一段時間後，NG-UTM 就會把來源 IP 位址跟超過的數值紀錄下來，例如，設定下載流量超過【100】，持續【120】秒，介面(ZONE)內部任一 IP 位址對外的下載頻寬超過 100Kbps 個且持續 120 秒，就會被紀錄。（圖 7-2）

圖 7-2 異常 IP 分析的紀錄設定

7-1-3、通知設定

當網路封包超過設定值的事件，NG-UTM 除了紀錄下當時的來源 IP 位址跟觸發數量及持續時間，外，也會馬上發一個通知信，通知管理者，有一個異常的流量發生，這個設定值適用於整個 NG-UTM 的所有介面(ZONE)。

基本設定

內部電腦出去介面(ZONE)外的異常流量偵測值。

- 【Session 量超過】：每一個來源 IP 位址，出去介面(ZONE)的網路連線數數量，當超過設定值且持續一段時間後，NG-UTM 就會把來源 IP 位址跟超過的數值紀錄下來並且發出通知信給管理者，例如，設定 Session 超過【200】，持續【120】秒，介面(ZONE)內部任一 IP 位址對外的連線超過 200 個且持續 120 秒，就會被紀錄且通知。
- 【上傳流量超過】：每一個來源 IP 位址，出去介面(ZONE)的上傳頻寬，當超過設定值且持續一段時間後，NG-UTM 就會把來源 IP 位址跟超過的數值紀錄下來並且發出通知信給管理者，例如，設定上傳流量超過【200】，持續【120】秒，介面(ZONE)內部任一 IP 位址對外的上傳頻寬超過 200Kbps 個且持續 120 秒，就會被紀錄且通知。
- 【下載流量超過】：每一個來源 IP 位址，出去介面(ZONE)的下載頻寬，當超過設定值且持續一段時間後，NG-UTM 就會把來源 IP 位址跟超過的數值紀錄下來並且發出通知信給管理者，例如，設定下載流量超過【200】，持續【120】秒，介面(ZONE)內部任一 IP 位址對外的下載頻寬超過 200Kbps 個且持續 120 秒，就會被紀錄且通知。（圖 7-3）

圖 7-3 異常 IP 分析的通知設定

7-1-4、阻擋設定

當網路封包超過設定值的事件，NG-UTM 除了紀錄下當時的來源 IP 位址跟觸發數量及持續時間，外，並啟動預設的阻擋動作，阻止這樣的情形持續發生，這個設定值適用於整個 NG-UTM 的所有介面(ZONE)。

基本設定

內部電腦出去介面(ZONE)外的異常流量偵測值。

- 【Session 量超過】：每一個來源 IP 位址，出去介面(ZONE)的網路連線數數量，當超過設定值且持續一段時間後，NG-UTM 就會把來源 IP 位址跟超過的數值紀錄下來並且啟動預設的阻擋動作，例如，設定 Session 超過【300】，持續【120】秒，介面(ZONE)內部任一 IP 位址對外的連線超過 300 個且持續 120 秒，就會被紀錄且啟動預設的阻擋動作。
- 【上傳流量超過】：每一個來源 IP 位址，出去介面(ZONE)的上傳頻寬，當超過設定值且持續一段時間後，NG-UTM 就會把來源 IP 位址跟超過的數值紀錄下來並且啟動預設的阻擋動作，例如，設定上傳流量超過【300】，持續【120】秒，介面(ZONE)內部任一 IP 位址對外的上傳頻寬超過 300Kbps 個且持續 120 秒，就會被紀錄且啟動預設的阻擋動作。
- 【下載流量超過】：每一個來源 IP 位址，出去介面(ZONE)的下載頻寬，當超過設定值且持續一段時間後，NG-UTM 就會把來源 IP 位址跟超過的數值紀錄下來並且啟動預設的阻擋動作，例如，設定下載流量超過【300】，持續【120】秒，介面(ZONE)內部任一 IP 位址對外的下載頻寬超過 300Kbps 個且持續 120 秒，就會被紀錄且啟動預設的阻擋動作。（圖 7-3）

圖 7-3 異常 IP 分析的阻擋設定

動作

當前面的設定值被觸發後，管理者可以針對有異常行為的電腦進行的動作，共有 6 種預設的處置方式，分別敘述如下：

1、阻擋數分鐘

異常流量可能是偶發性的，所以阻擋數分鐘後，症狀就會自動會消失，所以將這個來源 IP 位址，暫時阻擋幾分鐘，讓他不能出去介面(ZONE)，但是介面內的互連封包並沒有影響。

2、全天阻擋

異常行為已經嚴重違反網路使用規定，將這個來源 IP 位址阻擋個一天(24:00)，禁止出去介面(ZONE)，以示懲罰，但是介面內的互連封包並沒有影響。

3、阻擋至管理者解除

異常行為已經嚴重違反網路使用規定，將這個來源 IP 位址禁止出去介面(ZONE)，以示懲罰，一直到跟他跟管理者說明原因或是狀況解除後才可以再出去，但是介面內的互連封包並沒有影響。

4、頻寬限制數分鐘

異常流量已經造成網路流量不公平分配，因此將這個來源 IP 位址限制使用網路頻寬數分鐘，限制的數量則在【其他設定】中設定。

5、頻寬限制全天

異常流量已經造成網路流量不公平分配，因此將這個來源 IP 位址限制使用網路頻寬整天(24:00)，限制的數量則在【其他設定】中設定。

6、頻寬限制至管理者解除

異常流量已經造成網路流量不公平分配，因此將這個來源 IP 位址限制使用網路頻寬，直到管理者認為狀況解除再另行開放，限制的數量則在【其他設定】中設定。（圖 7-4）

圖 7-4 異常 IP 分析的阻擋動作

其他設定

當前面的設定值被觸發後且選擇的動作是頻寬限制，則在這裡的頻寬數就會自動套用在出問題的電腦上。

- 【QoS 頻寬限制設定】：每一個來源 IP 位址觸發設定值後，不論是觸發哪一項，連線數或是上、下載頻寬，NG-UTM 會把這個來源 IP 位址的使用頻寬降為表列的數值，例如，200Kbps，則他會被限制在這一個頻寬下慢慢的執行。
- 【網頁阻擋訊息】：選擇限制頻寬時，會在使用者的瀏覽網頁上出現設定的文字，讓使用者知道目前是被限速中。（圖 7-5）

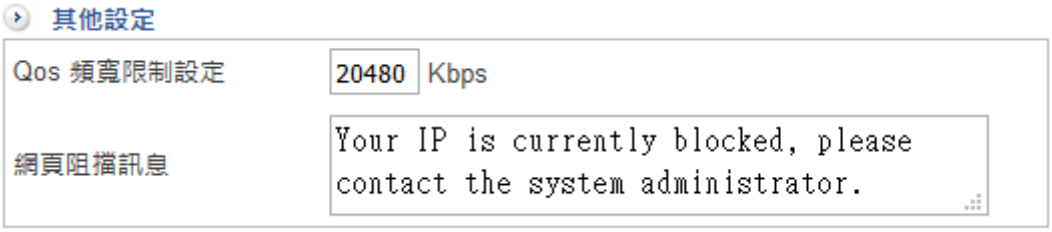


圖 7-5 異常 IP 分析的頻寬限制

7-1-5、例外 IP 設定

NG-UTM 可以針對異常的 Session、上傳流量、下載流量進行記錄、通知與阻擋，但是針對特定的使用者，不要做執行偵測動作該怎麼辦呢？利用例外 IP 設定方式，管理者可以設定哪一些 IP 位址不要執行異常 IP 分析的工作。

- 【IP/網路遮罩】：那一些 IP 位址不要執行異常 IP 分析，可以單一個 IP 位址或是一個網段，例如，192.168.1.5/32 就是一個 I P 位址，192.168.1.1/24 就是一個 C 網段
- 【類別】：分成 3 個類別，紀錄、通知跟阻擋，可以複選。
- 【備註】：來源 IP 位址的備註說明。（圖 7-6）

圖 7-6 例外 IP 設置

7-1-6、異常紀錄

針對所有異常行為，系統會詳細記錄其異常行為時間、來源 IP 位址、管制動作、觸發事件、實際量、持續時間及管制時間。（圖 7-7）

圖 7-7 異常紀錄

7-1-7、阻擋清單

列出目前被 NG-UTM 阻擋的來源 IP 位址，管理者具有權限放行這些被管制的 IP 位址。

7-2、交換器管理

當 NG-UTM 可透過交換器（Switch），即時監控內部機器的分部狀況，於內部網路發出大量異常封包時，阻擋此類封包的傳送，並協助管理人員盡速排除異常狀態，避免企業網路癱瘓。

如何管理內部網路每一個管理者想要的需求都不一樣，有人關心每一個 IP 位址的流量，有人關心每一部電腦的實際位置在哪裡，再加上內部網路的網路線的盤根錯覺，讓每一位管理者頭疼。

ShareTech 的交換器管理把這一切都簡單化了，以 UTM 的 LAN 或是 DMZ 為出發點，把每一個交換器的 Uplink 跟 Downlink 標示出，佐以階層的觀念，將所有的交換器分層顯示，如（圖 7-8）所示，要找尋出問題的電腦實際位置時，按圖索驥就可以了。

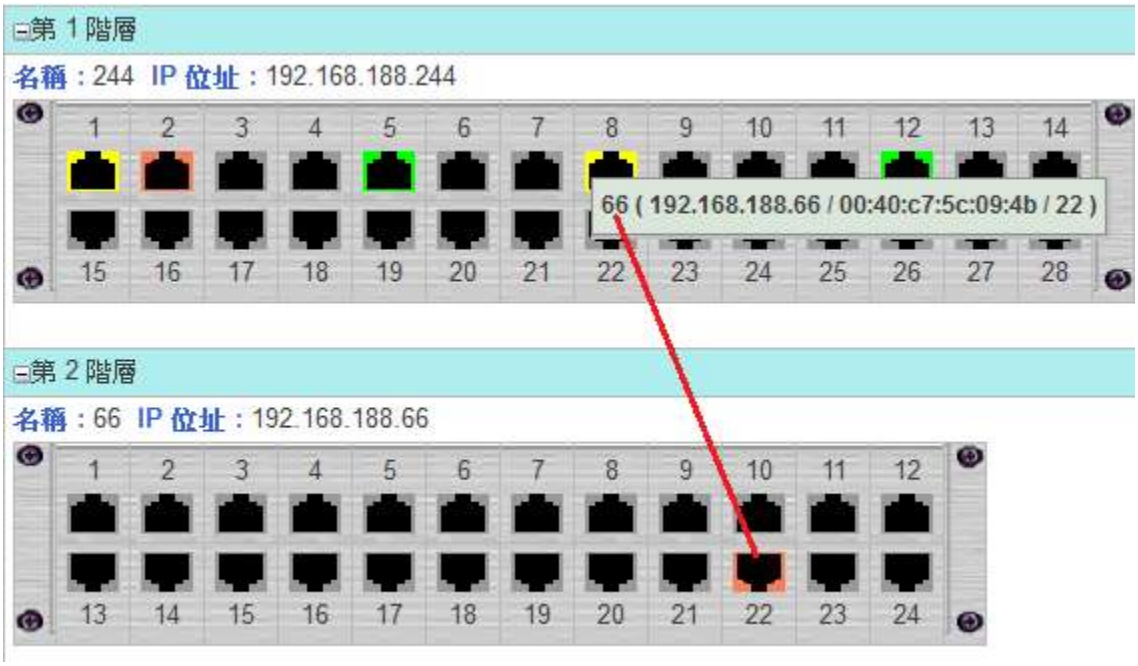


圖 7-8 交換器的階層圖

以圖形介面的方式顯示每一個 IP 位址的交換器 PORT 之後，就會讓內部網路的真實架構一目了然，例如，哪幾個交換器間是彼此互接，此時，再搭配 UTM 的位址表管理圖像，讓網路管理不再只是 IP 位址的虛擬管理，每一個 IP 接在哪一個交換器 PORT，能不能自己更換 IP 位址，每一個管理動作都是”有圖有真相”。

NG-UTM 支援交換器種類

NG-UTM 根據不同的功能需求及現場環境，支援 2 種交換器類型，一般標準 SNMP 網管型跟支援進階協同防禦的核心交換器，2 種交換器提供的功能不一樣，一般標準的 SNMP 交換器可以顯示網路狀態圖，協同防禦型的核心交換器除了可以顯示網路狀態圖外，可以根據管理者的設定，在交換器上自動阻擋有問題的電腦。

NG-UTM 根據不同的介面(ZONE)配置不同需求的交換器，例如，ZONE1 是內部網路區域，使用的電腦數眾多，所以配置具有協同防禦的核心交換器跟一般標準的 SNMP 交換器，ZONE2 是內部伺服器使用區，只要搭配一般標準的 SNMP 交換器就可以滿足要求。

7-2-1、Switch 設定

啟用交換器管理時，需要新增交換器的資料，首先進入【進階防護】之【交換器管理】>【Switch 設定】新增設備。

- 【介面】：新增的交換器是在哪一個介面(ZONE)，例如，內部網路 ZONE1。
- 【交換器屬性】：新增的交換器是屬於哪一種交換器，管理者必須事先了解交換器種類，是只能顯示網路圖的一般標準 SNMP 交換器或是支援協同防禦的核心交換器，底下分別說明詳細的設定方式。

A、SNMP 交換器設定

- 【型號】：NG-UTM 會列出已經測試過且運作正常的一般 SNMP 交換器讓管理者選擇，如果要新增的交換器不在支援的名單中，請選擇『一般 SNMP』，一般來說，只要支援網管型的交換器通常可以滿足 NG-UTM 的條件。
- 【名稱】：這個交換器的名稱方便管理者辨識，可以輸入任何中英文字的組合，例如，2F 的工程部。
- 【備註】：交換器的備註，方便管理者辨識，可以輸入任何中英文字的組合，例如，工程部的測試區。
- 【IP 位址】：交換器的 IP 位址，例如，192.168.1.66
- 【Port】：此一般 SNMP 交換器總共的埠數，例如，一般 SNMP 交換器的埠數為 24 則填入 24。
- 【SNMP 登入名稱 (Read)】：NG-UTM 使用 SNMP 協定跟交換器溝通時具有 Read 權限的名稱，一般 SNMP 類型的交換器預設值為『public』，設定完成後可以按下【連線測試】按鈕，驗證交換器是否接受這一個名稱查詢 Write 權限的資訊。

- 【SNMP 登入名稱 (Write)】：NG-UTM 使用 SNMP 協定跟交換器溝通時具有 Write 權限的名稱，一般 SNMP 類型的交換器預設值為『private』，設定完成後可以按下【連線測試】按鈕，驗證交換器是否接受這一個名稱查詢 Write 權限的資訊。
- 【管理者通訊埠】：進入交換器的管理介面使用的埠號，一般來說是 80。（圖 7-9）

圖 7-9 新增一台一般交換器

B、協同防禦設定

- 【型號】：NG-UTM 會列出已經測試過且運作正常的協同防禦交換器，目前支援的品牌如 Zyxel、Cisco、Juniper 及 H3C 等，管理者需要從中挑選支援的交換器名稱。
- 【名稱】：這個交換器的名稱方便管理者辨識，可以輸入任何英文字，例如，1F。
- 【備註】：交換器的備註，方便管理者辨識，可以輸入任何中英文字的組合，例如，核心交換器。
- 【IP 位址】：協同防禦交換器的 IP 位址，例如，192.168.2.55。
- 【命令模式】：NG-UTM 用哪一種通訊協定跟協同防禦的交換器溝通，支援 2 種模式，Telnet 跟加密的 SSH 2 種，管理者需要根據協同防禦交換器的需求，選擇適當的通訊模式。
- 【命令 Port】：根據前面【命令模式】選的通訊模式，例如，Telnet 是 23 、加密的 SSH 是 22，這個數值不可以更改。

- 【登入帳號】：使用命令模式登入協同防禦交換器的帳號，例如，root 或是 admin。
- 【登入密碼】：使用命令模式登入協同防禦交換器的密碼，例如，password。
- 【設定模式密碼】：使用命令模式登入協同防禦交換器進行設定時，是否還有另一層密碼保護，如果有，則需要加入，否則無法將正確的設定值加入協同防禦的交換器中。（圖 7-10）

圖 7-10 新增一台協同防禦交換器

- 【綁定模式】：NG-UTM 跟協同防禦交換器之間可以有 3 種綁定，分別是 IP+MAC+PORT、MAC+PORT 及 IP Source Guard，並不一定每一種協同防禦的交換器都支援上面 3 種，選擇交換器型號時，NG-UTM 就會列出此型號支援的模式提供給管理者選擇，詳細的模式說明如下：

1、IP+MAC+PORT

在這個模式下，使用者的 IP 跟 MAC 位址綁定在協同防禦交換器 PORT 上，不是綁定的電腦無法透過協同防禦交換器上網，例如，綁定 IP 位址 192.168.2.99 且 MAC 位址為 00:01:02:03:04:05 的電腦只能透過協同防禦的第 21Port 上網，當這部電腦改 IP 位址或是插入此交換器的其他 Port ，網路都不通。

2、MAC+PORT

在這個模式下，使用者的 MAC 位址綁定在協同防禦交換器 PORT 上，不是綁定的電腦無法透過協同防禦交換器上網，例如，MAC 位址為 00:01:02:03:04:05 的電腦只能透過協同防禦的第 21Port 上網，當這部電腦插入此交換器的其他 Port ，網路都不通。

3、IP Source Guard

這個模式目前只支援 Zyxel 品牌的交換器，除了傳統的 IP+MAC+PORT 綁定外更可以結合 VLAN 的運作，讓綁定的運作更具有彈性。

IP Source Guard 的交換器具有禁止內部私架 DHCP 伺服器(DHCP Snooping)的功能，私架的 DHCP 伺服器往往會成為內部網路不固定的網路安全威脅因素之一，具備 IP Source Guard 的交換器可以指定 DHCP 伺服器使用的 Port，當其他 Port 有 DHCP 伺服器時，他的廣播封包通通會被禁止。（圖 7-11）

圖 7-11 協同防禦交換器的綁定模式

- 【SNMP 登入名稱 (Read)】：NG-UTM 使用 SNMP 協定跟交換器溝通時具有 Read 權限的名稱，交換器預設值為『public』，設定完成後可以按下【連線測試】按鈕，驗證交換器是否接受這一個名稱查詢 Write 權限的資訊。
- 【SNMP 登入名稱 (Write)】：NG-UTM 使用 SNMP 協定跟交換器溝通時具有 Write 權限的名稱，交換器預設值為『private』，設定完成後可以按下【連線測試】按鈕，驗證交換器是否接受這一個名稱查詢 Write 權限的資訊。
- 【管理者通訊埠】：進入交換器的管理介面使用的埠號，一般來說是 80。

自動搜尋交換器

NG-UTM 提供自動搜尋交換器的功能，在 Switch 列表中，按下【自動搜尋】的按鈕，讓 NG-UTM 自動幫你找尋所有介面(ZONE)下的 SNMP 交換器，搜尋的結果會另外開啟視窗，將要管理的交換器在動作下方按下 ，就進入交換器的設定模式，設定好帳號密碼、埠號等資訊及指定運作的介面(ZONE)，就完成增加交換器的工作。（圖 7-12）

自動搜尋結果 1 / 1

IP 位址	Port	名稱	動作
192.168.188.3	24	24G + 4 SFP Web Smart Switch - 2.03	

圖 7-12 自動搜尋交換器

完成交換器的設定後，NG-UTM 會將所有的交換器列表，管理者在這裡查看設定的資訊是否正常或是直接點選 ，NG-UTM 會根據管理者設定的模式，開啟另一個視窗直接進入交換器的管理介面。（圖 7-14），此功能讓管理者可以用統一的介面管理內部所有的交換器。

Switch 列表 1 / 1 自動搜尋

介面	交換機屬性	名稱	IP 位址	Port	管理者通訊埠	動作
zone0	SNMP	2F工程	192.168.1.66	80		
zone0	協同防禦	1F	192.168.2.55	28		

圖 7-14 交換器管理

7-2-2、網路狀態圖

對企業來說，對許多網管人員來說最麻煩的就是查線路，尤其當線路環境很亂時候要查出哪一台 PC 接在哪一台交換器上面尤其痛苦。

NG-UTM 結合協同防禦跟一般 SNMP 網管型的交換器，把內部網路的狀況，即時顯示出來，包含交換器之間的堆疊關係，用哪 2 個交換機的 Port 當成堆疊，同時讓管理者可以一目了然知道目前內部使用者的連線狀態，包含電腦接到哪一台交換器，是否有開機，就算是串接到第二層交換器也可同樣顯示出來。（圖 7-15）

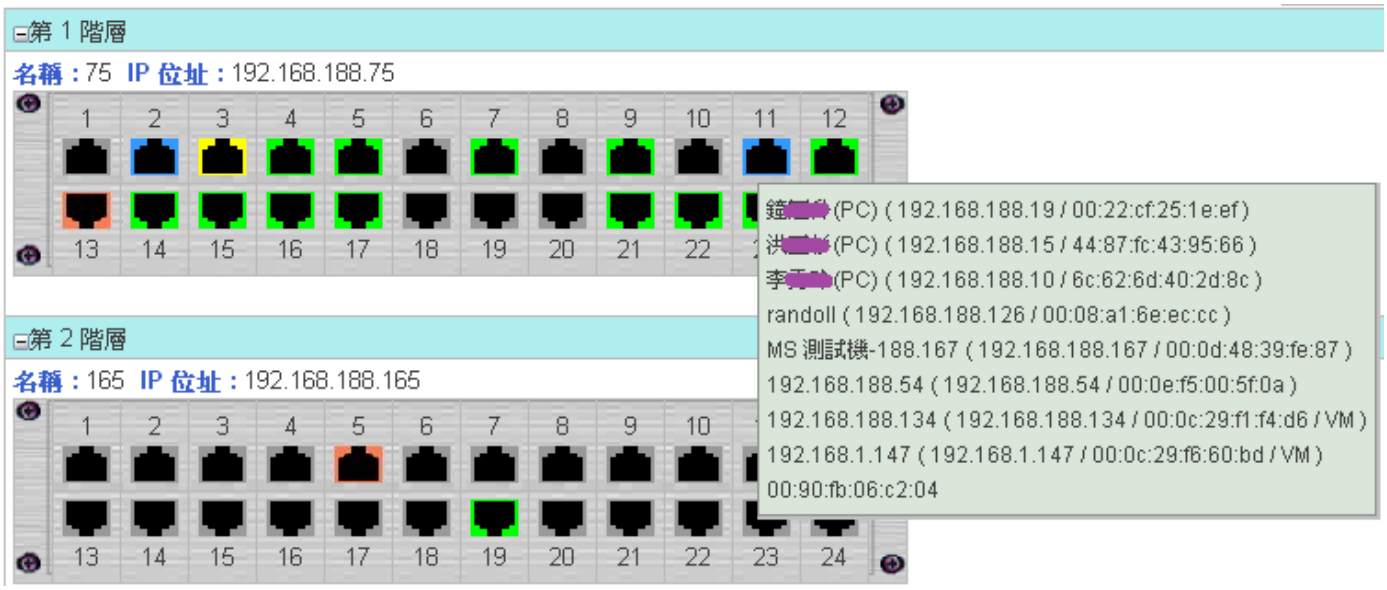


圖 7-15 網路狀態圖

圖示說明：

Up Link Down Link：不同階層之間一定是由 Up Link+Down Link 配對組合，NG-UTM 會顯示交換器的上、下層堆疊關係。

Dump Switch：這個交換機 Port 接一台以上無網管的交換器。

On：這個交換機 Port 有接一台 PC 且目前是開機狀態。

立即更新：按下立即更新按鈕將會把所有狀態更新。

在顯示方面，查看交換器跟電腦之間的組合，可以用 3 種方式呈現，依照圖形（圖 7-15）、依照清單或是依照 IP 顯示，並可以選擇查看的介面(ZONE)。

設定排程更新的時間，讓網路狀態及時更新，同時具有搜尋功能，在搜尋的欄位輸入 IP 位址後，NG-UTM 會幫管理者找出這一個 IP 位址在哪一個交換機的第幾 PORT 上。（圖 7-16）

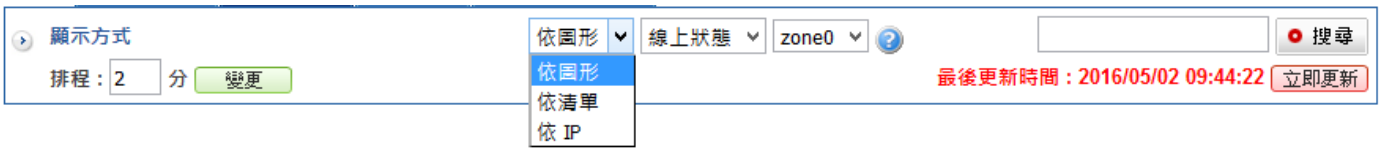


圖 7-16 交換器跟電腦的顯示選項

點選  或是  的圖標，NG-UTM 介面會顯示交換器中這一個 PORT 的更詳細的資料。（圖 7-17）

- 【向上對接孔】：指定這一個 PORT 對 UP link PORT。
- 【啟用/關閉】：將這一個 PORT 整個開啟或是關閉。
- 【In / Out】：整個 PORT 的流入/流出流量。
- 【對外網路上傳/下載流量】：這個 IP 位址對網際網路的流入/流出流量。
- 【綁定】：當交換器是協同防禦時，管理者可以將這個 IP/MAC 鎖在這個 PORT 上。

綁定	名稱	IP 位址	Mac 位址	對外網路 上傳/下載(bps)	接入位置
	192.168.1.89	192.168.1.89	00:0c:29:36:d2:2a	-- / --	
	192.168.1.144	192.168.1.144	00:0c:29:74:b2:4f	-- / --	
	192.168.1.56	192.168.1.56	00:0c:29:97:7d:16	-- / --	
	192.168.1.90	192.168.1.90	00:0c:29:d0:7d:00	-- / --	
	192.168.1.26	192.168.1.26	00:0c:6e:b5:f8:a5	-- / --	

圖 7-17 個別 PORT 網路狀態圖

7-2-3、綁定清單

管理者為了網路安全因素或是方便內網管理，在交換器的 Port 號上綁定某些特定電腦才能使用，不是指定的電腦，就無法接上網路，NG-UTM 的協同防禦機制，就可以滿足這樣的需求。

首先根據 Switch 設定上的綁定模式，而有不同的設定方式，在綁定模式上除了 Zyxel 的交換器多一個 Ip Source Guard 的選項外，綁定模式有 2 種，一種是 IP + MAC + Port 另一種是 MAC+ Port ，在設定上 IP + MAC + Port 比 MAC + Port 需要多輸入綁定的 IP 位址，其他的均相同，以 IP + MAC + Port 為說明。

首先，在綁定清單上選擇前要執行的協同交換器 IP 位址。

新增綁定清單

- 【IP 位址】：要被綁定的 IP 位址，例如，192.168.2.96。要注意一下，這部電腦不論是設定用 DHCP 或是固定 IP，只要 IP 位址一改變，就無法存取網路資源。
- 【MAC 位址】：要被綁定的 MAC 位址，例如，02:03:04:05:06:07。如果不是這一個 MAC 位址的電腦，無法接上網路。
- 【協同防禦】：這部電腦是被綁定在哪一台協同防禦的交換器上。
- 【Port】：這部電腦是被綁定在協同防禦交換器上的第幾埠，例如，24 埠。
- 【綁定模式】：目前使用的綁定模式，是 IP + MAC + Port 或 MAC + Port。（圖 7-18）

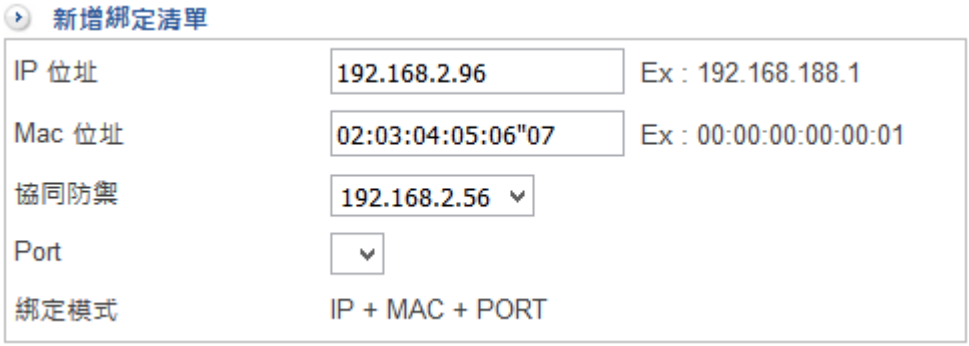


圖 7-18 綁定清單設定

7-2-4、IP Source Guard

NG-UTM 搭配 Zyxel 的交換器提供另一種 IP + MAC + Port 的綁定模式，IP Source Guard ，除了可以執行 IP + MAC + Port 的綁定外，另外提供 DHCP snooping 的機制，確保內部私自架設的 DHCP 伺服器無法運作，IP Source Guard 運作時需要搭配 VLAN ，所以需要先在交換器上設定完成相關的 VLAN。

新增 IP Source Guard 綁定

點選 IP Source Guard 上的新增按鈕，新增一筆 IP+MAC+Port 的綁定

- 【協同防禦】：選擇要執行 IP+MAC+Port 綁定的協同防禦交換器 IP 位址，例如，192.168.14.2，目前只支援 Zyxel 的交換器。
- 【VLAN】：選擇要執行 IP+MAC+Port 綁定的 VLAN，系統會列出所有運作中的 VLAN 讓管理者選取，例如，VLAN1。
- 【Trusted Port】：在這個 VLAN 下，哪幾個 Port 不執行 IP+MAC+Port 綁定，不執行的 Port 就稱之為 Trusted Port，在 Trusted Port 下，任何 IP 及 MAC 位址都可以使用網路，點選【輔助選取】，NG-UTM 就會顯示交換器的示意圖，讓管理者選擇，點選屬於這個 VLAN 下的就可以將此 Port 切換成 Trusted Port 的狀態。
- 【輔助新增】：曾經連過交換器 VLAN 的 IP+MAC+Port 的資料，NG-UTM 可以自動將這一些資料帶入，省下管理者的輸入資料時間。（圖 7-19）

圖 7-19 新增一筆 IP source Guard 的 IP+MAC 綁定

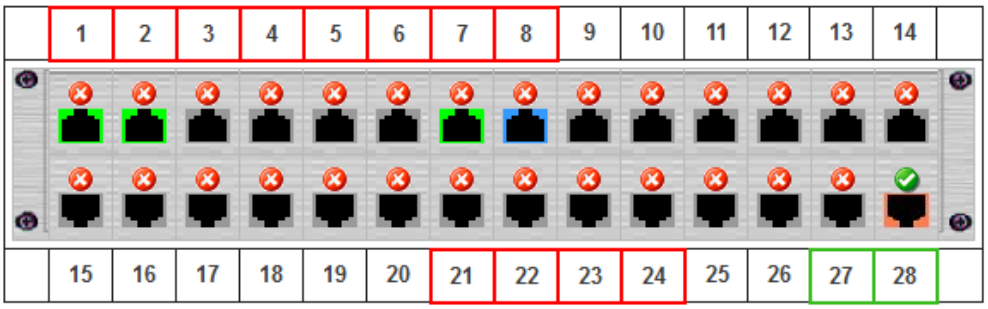
新增 DHCP Snooping 設定

IP Source Guard 可以確保每一個 VLAN 底下私自架設的 DHCP 伺服器都無法正常運作，只有公司允許的 DHCP 伺服器才有辦法發放 IP 位址，因此管理者需要事先知道每一個不同 VLAN 的 DHCP 伺服器是接在交換器的第幾個實體 Port。

進入 IP Source Guard 上的設定，NG-UTM 會開啟新的設定畫面。（圖 7-20）選擇 VLAN 前的 Box ，NG-UTM 就會將屬於此 VLAN 的實體 Port 用紅色跟綠色框列出，其中紅色框代表是 Untagged Port ，綠色是 Tagged Port。

不執行 IP+MAC+Port 綁定的 Port 就稱之為 Trusted Port，在 Trusted Port 下，任何 IP 及 MAC 位址都可以使用網路，啟用 DHCP Snooping 功能時必須要注意，此 VLAN 下必須要有一個 Trusted Port，點選屬於這個 VLAN 下的就可以將此 Port 切換成 Trusted Port 的狀態。

名稱：test IP 位址：192.168.14.2 備註：test



		vlan name	vlan id	Ports	啟用
	◉	1	1	Tagged: 27,28 Untagged: 1,2,3,4,5,6,7,8,21,22,23,24	☑
	○	QQ	10	Tagged: 27,28 Untagged: 9,10,11,12	☑
	○	AA	20	Tagged: 27,28 Untagged: 13,14,15,16	☐

圖 7-20 DHCP Snooping 設定

7-2-5、PoE 排程設定

NG-UTM 搭配 Zyxel 的 PoE 交換器提供供電時間管控，按下【新增】就會出現排程。（圖 7-21）

- 【排程名稱】：給設定的 PoE 排程名稱。
- 【設定模式】：有 2 種模式可以選擇，
  - ◆ 模式一：以每個小時為單位，將一周的周期表列出，管理點選要管理的時間段就可以。
  - ◆ 模式二：以連續性的時間段，如下所示：

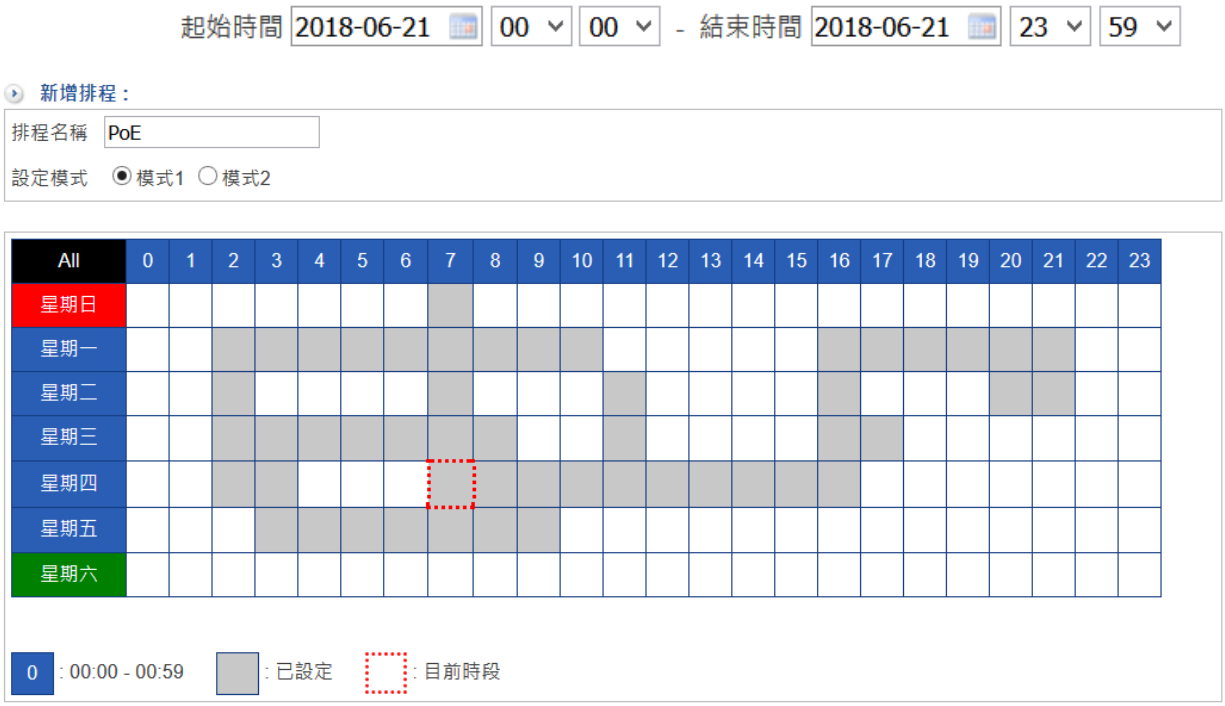


圖 7-21 PoE 的排程設定

7-3、內網防護

對內部網路的安全考量上，最難偵測到的攻擊類型就是廣播型的封包，如 ARP 欺騙、私架 DHCP 伺服器等，因為通訊協定的先天性缺陷，導致這一類的攻擊行為很難被偵測出來，就算找到了攻擊者，因為偵測機制無法跟第一線的 UTM 或是交換器互相溝通，無法做立即的封鎖，傳統的方式是發生問題時，請人到每一台交換器上拔線測試外，別無他法，NG-UTM 提供一些工具，阻止類似的攻擊。

當啟用協同防禦的交換器後，NG-UTM 提供進階的內網防護機制，保護內部網路的安全，這些機制包含 ARP 防護、偽造 IP 偵測、偽造 MAC 偵測跟異常 IP 阻擋連動，搭配介面(ZONE)的選擇，把想要的偵測機制套用在介面(ZONE)上。

7-3-1、防護設定

偵測介面

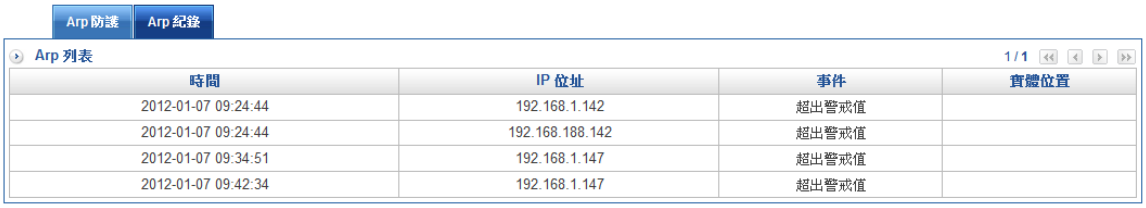
選擇內網防護要套用的網路介面(ZONE)，管理者可以選擇一個以上的介面執行偵測機制，通常這個機制是套用在內部網路。

交換器是 NG-UTM 列表中的智慧型交換器，也就是在交換器圖示中出現  ，當觸發的偵測機制發生時，就直接在這個 Port 上的電腦直接封鎖，如果選擇進階封鎖，圖示為  ，因為他非智慧型交換器，無法詳細的管理到 Port，所以有可能發生皆在這一個 Port 底下的電腦都被誤封鎖。

ARP 封包警戒值

ARP 的攻擊防護對 UTM 設備來說比較難以處理，因為 ARP 是用廣播封包的方式處理，在尚未建立 TCP/UDP 連線前就先存在的網路溝通方式。

ShareTech 的 ARP 偵測機制，可以在第一時間內就找到『濫發』 ARP 訊息的人，此時他只是處於 ARP 攻擊前的準備，尚未發動任何攻擊，站在管理者的角度，它是在合法跟非法的邊緣，搭配協同防禦交換器的設備，可以標示出這個 IP 的實體位置，讓他無所遁形。（圖 7-22）



時間	IP 位址	事件	實體位置
2012-01-07 09:24:44	192.168.1.142	超出警戒值	
2012-01-07 09:24:44	192.168.188.142	超出警戒值	
2012-01-07 09:34:51	192.168.1.147	超出警戒值	
2012-01-07 09:42:34	192.168.1.147	超出警戒值	

圖 7-22 ARP 攻防紀錄

萬一，偵測到內部有受害者出現了，管理者就可以合理的懷疑，曾經" 濫發" ARP 訊息的 IP 位址可能是攻擊者的候選人，管理者可以啟用協同防禦的機制，將攻擊者的交換器 PORT 封鎖掉，把攻擊者堵在他自己的網路卡上，不讓他繼續危害他人。

進入 ARP 封包警戒值設定。

- 【每個來源 IP 位址】：每個來源 IP 位址每秒發送超過多少個 ARP 要求，就會被 NG-UTM 視為不正常行為，預設為 100 個，數值越大偵測的靈敏度越低，相反地，靈敏度越高也越常發生誤判的動作。
- 【自動封鎖】：偵測到 ARP 異常行為時，NG-UTM 主動封鎖使用者繼續濫發 ARP 封包。
- 【信任位址】：輸入不做 ARP 異常行為偵測的 IP 位址，例如，192.168.1.100。（圖 7-23）

圖 7-23 ARP 偵測機制

IP/MAC

內部 IP 衝突或是 MAC 衝突也是一件困擾網路管理者的事情，NG-UTM 內建的偵測機制，可以減輕管理者這方面的困擾。

- 【IP 位址衝突偵測】：要不要啟用這項功能，預設是關閉。
- 【自動封鎖】：偵測到 IP 位址衝突時，NG-UTM 主動封鎖偽造 IP 的電腦。
- 【信任位址】：輸入不做 IP 位址衝突偵測的 IP 位址，例如，192.168.1.100。
- 【MAC 位址衝突偵測】：MAC 位址偵測的頻率，預設為每 3 小時偵測一次。
- 【自動封鎖】：偵測到 MAC 位址衝突時，NG-UTM 主動封鎖偽造 MAC 的電腦。
- 【信任位址】：輸入不做 MAC 位址衝突偵測的 MAC 位址，例如，00:01:02:03:04:05。（圖 7-24）

圖 7-24 偽造 IP / MAC 偵測

協同防禦

在【進階防護】中的【異常 IP 分析】中有一個【阻擋設定】，在內網防護上搭配協同防禦的交換器可以執行連動機制，當內部使用者超過使用的連線數或是上、下載頻寬，NG-UTM 會自動通知交換器，執行封鎖的動作，該部電腦就無法繼續使用。（圖 7-25）

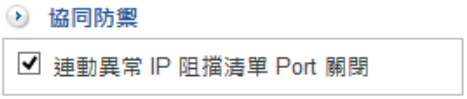


圖 7-25 異常 IP 分析跟協同交換器連動

通知項目

發生上面的事件時，NG-UTM 要不要在第一時間內通知管理者處理，選擇要通知的項目即可，目前有連動異常 IP 阻擋、Arp 防護、IP 衝突、MAC 衝突等 4 種。

7-3-2、ARP 紀錄

ARP 的攻擊的偵測紀錄，紀錄時間、IP 位址、MAC 位址、事件、接入位置、狀態與動作，並分辨出攻擊者跟受害者，讓管理者可以介入調查。

- 【IP 位址】：哪一個 IP 位址發出大量 ARP 封包攻擊別人或是接受到大量的 ARP 封包的受害者。
- 【事件】：分辨出疑似攻擊者或是受害者，疑似攻擊者會用 超出警界值字眼，讓管理者區分狀態。
- 【狀態】：ARP 攻擊進行中或是已經停止。（圖 7-26）

Arp 列表 清除 1 / 14 1 GO

時間	IP 位址	Mac 位址	事件	接入位置	狀態	動作
2013-10-17 13:35:10	172.16.1.146	00:00:00:00:00:01	受害者		已停止 (2013-10-17 13:38:10)	
2013-10-17 12:35:10	172.16.1.146	00:00:00:00:00:01	受害者		已停止 (2013-10-17 12:38:10)	
2013-10-17 11:33:00	172.16.1.146	00:00:00:00:00:01	受害者		已停止 (2013-10-17 11:38:09)	
2013-10-17 10:33:00	172.16.1.146	00:00:00:00:00:01	受害者		已停止 (2013-10-17 10:38:09)	
2013-10-16 09:53:24	172.16.7.154	00:0c:29:ed:fe:c9	超出警戒值	,12	已停止 (2013-10-16 09:56:24)	

圖 7-26 ARP 攻防紀錄

7-3-3、MAC 衝突紀錄

偽造 MAC 位址的攻防偵測紀錄都會被記錄下來，搭配協同防禦交換器，連同接入的位置都會顯示出來，方便管理者介入調查。

- 【MAC 位址】：哪一個 MAC 位址偽造另一個 MAC 位址。
- 【IP 位址】：這個偽造者的 IP 位址。
- 【接入位置】：疑似攻擊者或是受害者是在協同防禦交換器上的哪一個實體埠上。
- 【重新記錄位址】：把 MAC 位址的資料全部清除，重新學習並開始統計偽造資訊。
- 【狀態】：偽造 MAC 的說明。（圖 7-27）

Mac 衝突列表 清除 1 / 32 1 GO 立即更新 重新紀錄位址

時間	Mac 位址	IP 位址	接入位置	狀態	動作
2013-10-16 19:05:03	00:0c:29:99:eb:c2	172.16.7.145	juniper-ex2200,14		
2013-10-16 19:05:03	00:00:00:00:00:11 >> 00:0c:29:99:eb:c2	172.16.7.141	juniper-ex2200,13	偵測到相似mac	
2013-10-16 19:00:05	00:0c:29:99:eb:c2	172.16.7.145	juniper-ex2200,14		

圖 7-27 MAC 攻防紀錄

7-3-4、IP 衝突紀錄

偽造 IP 位址的攻防偵測紀錄都會被記錄下來，搭配協同防禦交換器，連同接入的位置都會顯示出來，方便管理者介入調查。

- 【IP 位址】：哪一個 IP 位址偽造另一個 IP 位址。
- 【IP 位址】：這個偽造者的 IP 位址。
- 【接入位置】：疑似攻擊者或是受害者是在協同防禦交換器上的哪一個實體埠上。
- 【狀態】：偽造 IP 的說明。（圖 7-28）

IP 衝突列表 清除 1 / 9 1 GO

時間	Mac 位址	IP 位址	接入位置	狀態	動作
2013-09-24 17:33:22	54:04:a6:9a:b7:02	172.16.7.7	Juniper-ex2200,8		
2013-09-24 17:33:22	00:0c:29:ed:fe:c9	172.16.7.7		偵測到相似IP	
2013-09-24 17:33:03	54:04:a6:9a:b7:02	172.16.7.7	Juniper-ex2200,8		

圖 7-28 IP 攻防紀錄

7-3-5、封鎖狀態

NG-UTM 提供進階的內網防護機制，保護內部網路的安全，包含 ARP 防護、偽造 IP 偵測、偽造 MAC 偵測跟異常 IP 阻擋連動，如果有任何 IP / MAC 違反存取規則而被封鎖，所有的資訊都會顯示在這裡，管理者也可以在這裡執行解除封鎖的動作。

第 8 章 IPS

NG-UTM 具備的 IPS（Intrusion Prevention System) 入侵防禦功能，IPS 可以立刻檢查網路封包是否含有攻擊/入侵的特徵值，並立刻阻止有害的網路封包攻擊內部或是從內部攻擊外部。

為何要 IPS？

狀態檢測（Stateful Inspection）防火牆可以檢視對應 OSI 模型第 2 到第 4 層通訊協定的內容，他最常檢視及控管的項目為：Source IP Address（來源 IP 位址）、Destination IP Address（目的 IP 位址）、Source Port Number（來源埠號）、Destination Port Number（目的埠號）、以及 Flag Fields（旗標欄位）。

例如，SQL Slammer 採用「緩衝溢位」(buffer overflow)的攻擊手法，因為防火牆開了 SQL 通訊埠，所以外界的人可以進到內部的 SQL Server，攻擊者再利用緩衝溢位攻擊的程式碼，就可以攻擊內部的 SQL 伺服器，竊取他想要的資料。

IPS 的運作

IPS 它會檢查對應到 OSI 模型第 4 到 7 層的內容，是否有惡意的攻擊程式、病毒，隱藏在 TCP/IP 的通信協定中，透過詳細的內容檢查後，符合條件的特徵碼就會被標示出來，一但發現後能夠即時地將封包阻止，讓這些穿過防火牆的惡意封包無所遁形。

IPS 跟 Firewall 的差別就是 IPS 會做內容或行為檢查，IPS 的優劣就在於特徵值資料庫的多寡及更新速度，也就是說 IPS 的資料庫有越多的特徵值，意味它能辨識越多不正常的內容或網路行為，但是事情總不是如此完美，越多的檢查就需要越強的運算能力，否則好處沒嘗到，反而付出網路速度緩慢的後果。

一般而言，IPS 的特徵值資料庫會依照危險程度分成高、中、低三種，再讓管理者決定放行或阻擋，考量客戶端的實際網路環境及機器的運算能力，在中小型的網路架構的 IPS 設備只需要有完整的危險程度高、中(例如，病毒、木馬程式)的特徵值資料庫就足夠，其他屬於警告或通知性質的檢查沒必要處理。

IPS 使用步驟

要讓 IPS 正常運作，需要下列步驟，順序如下：

1. 在【IPS 設定】中，建立一個群組，在群組中指定要阻擋還是紀錄有問題的特徵值。
2. 在【管制條例】中選擇來源 /目的 IP 位址後再套用預先建立的群組。

因為 IPS 的特徵值眾多，管理者套用不同的特徵值之間，有可能將正常的網路封包阻擋，造成誤判斷的情況，本來為了安全才使用 IPS 反而造成網路不順暢。

為了避免這樣的狀況，NG-UTM 事先將所有的 IPS 事件分類，分成 高、中、低 3 種風險事件，把管制行為分成阻擋跟紀錄，為了避免誤擋網路封包，管理者可以先啟用紀錄功能，然後再根據實際的需要設定阻擋機制。

建立新群組

每個 IPS 群組可選擇 2 種模式，初階模式跟進階模式，2 個模式套用的特徵值都一樣，只是初階模式 NG-UTM 事先按照特徵值的風險程度分成高、中、低三種，方便管理者挑選，進階模式則是按照特徵值的屬性分類，例如，病毒型、木馬型等，管理者再根據要阻擋/紀錄的類型或是其中的單一特徵值進行挑選。

- 【群組名稱】：IPS 群組的名稱，可以是任何文字的組合，例如，高風險阻擋。
- 【模式】：2 種模式可供選擇，初階跟進階，初階是按照特徵值的風險性，進階則是按照特徵值的類型。

模式一、初階模式（圖 8-1）

共分 3 個等級，按照風險程度分高、中、低，點選 ⊞ 可以觀看詳細的特徵值名稱，每一個等級可選阻擋或是紀錄，括弧中的是這一個分類的特徵值數量。

風險程度	記錄	阻擋
⊟ High Risk (1597)	☑	☑
Adware/Calla.A.1-3		
Adware/Calla.A.1-4		
» More		
⊞ Medium Risk (1816)	☑	☐
⊞ Low Risk (607)	☑	☐

圖 8-1 IPS 初階模式

模式二、進階模式（圖 8-2）

按照 IPS 特徵值分類，每一個分類的特徵值都可單獨選擇是紀錄或是阻擋，點選 ⊞ 就可以看到更詳細的資訊，括弧中的是這一個分類的特徵值數量。

分類	記錄	阻擋
⊟ AntiVir(12)	☑	☐
Adware/Calla.A.1-3	☑	☑
SPR/Fraud.IdBoan.C-1	☑	☐
TR/Dldr.FakeAler.AB-1	☑	☐
⊞ DNS(952)	☑	☐
⊞ ET DROP(228)	☑	☐
⊞ ET MALWARE(903)	☑	☐

圖 8-2 IPS 進階模式

今日 IPS 紀錄

每個 IPS 的阻擋事件，都會被記錄下來，讓管理者可以查詢，首先出現的是今日的 IPS 防護紀錄，從凌晨 00:00 到目前的事件，管理者另可在 IPS 紀錄搜尋查詢今日以前的 IPS 防護紀錄。（圖 8-3）

每一筆紀錄包含是件發生的時間、IPS 種類、特徵值名稱、來源 /目的 IP 位址、協定、來源 /目的 Port、NG-UTM 執行的動作跟他分類的風險程度。

IPS記錄搜尋結果　1 / 1　匯出　匯出全部

時間	分類	事件	來源 IP	目的 IP	協定	來源埠	目的埠	動作	風險程度
2016-02-18 14:36:29	ET MALWARE	Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)	10.0.154.100	54.193.111.93	TCP	44985	80	阻擋	High
2016-02-18 14:31:24	ET MALWARE	Hex Encoded IP HTTP Request - Likely Malware	192.168.188.110	192.30.252.153	TCP	49422	80	記錄	Medium
2016-02-18 14:26:38	ET MALWARE	Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)	192.168.188.92	54.85.182.70	TCP	52605	80	阻擋	High
2016-02-18 11:36:29	ET MALWARE	Suspicious Mozilla User-Agent - Likely Fake (Mozilla/4.0)	10.0.154.100	54.193.111.93	TCP	44985	80	阻擋	High
2016-02-18 11:31:24	ET MALWARE	Hex Encoded IP HTTP Request - Likely Malware	192.168.188.110	192.30.252.153	TCP	49422	80	記錄	Medium

圖 8-3 IPS 阻擋及記錄

第 9 章 WAF

NG-UTM 具備的 WAF (Web Application Firewall) 功能，WAF 可以提供對外服務的網頁伺服器進階的保護，不論駭客對於網頁伺服器常用的手法有 SQL Injection 、Cross-site Scripting Attack 等，WAF 都可以將他們阻隔在網頁伺服器之外，一般駭客攻擊網頁伺服器的目的為癱瘓或是竊取網頁資料庫內的重要資料庫資訊。

網頁伺服器有 2 個協定，一個是 HTTP，另一個是 HTTPS，WAF 的運作有如代理伺服器，如果後端的網頁伺服器是 HTTPS 協定，則需要將他的憑證資料匯入 WAF 伺服器，否則外面的使用者瀏覽網頁時會出現憑證錯誤的狀況，HTTP 協定就不需要額外的設定。

啟用的步驟

WAF 的啟用有 3 個步驟：管制條例把 http / https 轉入內部網頁伺服器並把 WAF 啟用、匯入憑證(http 省略)及選擇啟用 WAF 項目。

1、 在管制條例的管制規則中的 Incoming 或是 Advance 建有將 HTTP 或是 HTTPS 導入內部網頁伺服器的管制條例，並啟用 WAF 功能，詳細設定 WEB 的管制條例請參考第 4-3-4 章。如（圖 9-1）所示，內部的伺服器是 https://192.168.189.151。

圖 9-1 管制條例啟用 WAF

2、 到 WAF ->網站管理 ，NG-UTM 就會自動列出目前有啟用 WAF 機制的伺服器，HTTPS 需要匯入網站伺服器的憑證，HTTP 就不需要任何額外設定。

3、 到 WAF ->WAF 設定啟用 WAF 並選擇管制項目及規則。

9-1-1、WAF 設定

NG-UTM 的 WAF 分成 19 個大項，每一個項目都有更多的細項，管理者可以依據自己的需求配置，處理的方式有 2 種，記錄跟阻擋，記錄是將符合規則的行為記錄後放行，記錄是方便管理者日後查詢，阻擋則是符合規則的行為直接阻擋，所以後端的網頁伺服器就不會收到這個從外部過來的服務要求。（圖 9-2）

第一次啟用 WAF 功能時，怕誤擋造成使用者瀏覽網頁伺服器不順，可以單獨啟用【記錄】處理方式，然後在 WAF 記錄中查詢有哪一些規則被觸發，因為 WAF 的規則比較嚴謹，如果網頁伺服器的程式寫法不是按照標準安全的規則寫，都會被阻擋，也就是這一些不按照標準安全的程式書寫方式，讓駭客們有機可乘，WAF 就是做這些漏洞的補救。

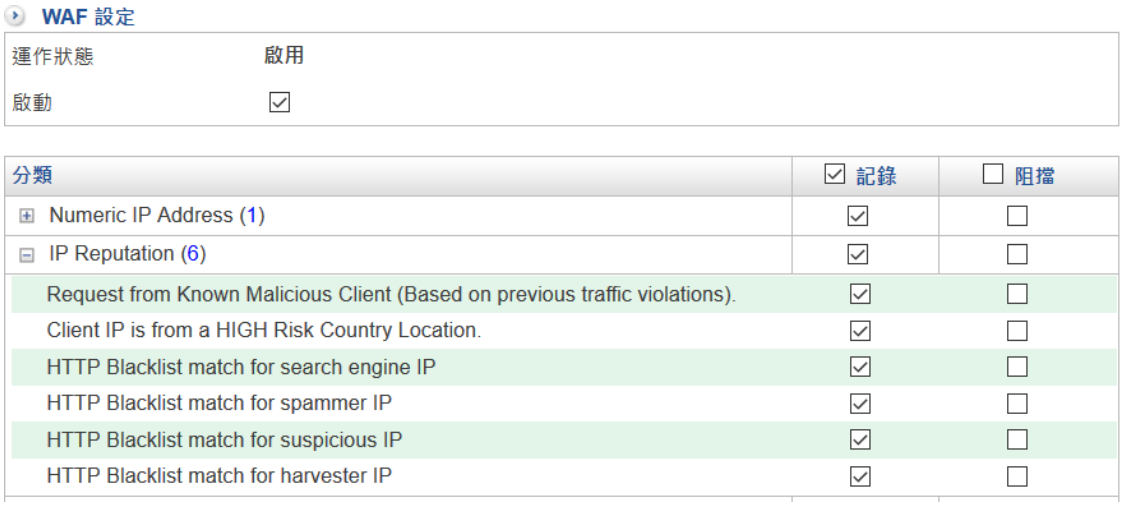


圖 9-2 WAF 啟用及規則

- 【啟動】：啟用 WAF 功能。
- 【異常連線封鎖】：當同一來源 IP 位址每分鐘觸發超過設定的次數，暫時封鎖這個來源 IP 位址，設定範圍是 0 ~ 9999，0 表示不封鎖。
- 【多久解除異常連線封鎖】：當來源 IP 位址觸發異常連線後，系統多久解除封鎖，設定範圍是 0 ~ 9999，0 表示不解除封鎖。
- 【永久封鎖】：異常連線封鎖次數超過幾次，就將這個 IP 位址永久封鎖， 設定範圍是 0 ~ 9999，0 表示沒有永久封鎖。
- 【封鎖 IP】：點選後出現目前被封鎖的來源 IP 位址，管理者可以解除單一個或是全部的封鎖 IP。

分類

共有 19 大項，括弧內就是這一項目的子項目數量，以下圖為例，（圖 9-3）Numeric IP Address(1) 裡面只有一個規則就是 Host header is a numeric IP address ，這一個的意思就是瀏覽者帶過來的 Request 是用 IP 位址，而不是常見的網域名稱。

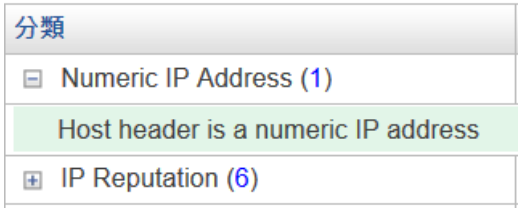


圖 9-3 WAF 規則分類

- 【記錄 / 阻擋】：符合規則的項目處理方式，只記錄還是阻擋。

9-1-2、網站管理

每一個在管制條例中啟用 WAF 服務的網頁伺服器都會列表在這裡，他預先按照據實際提供服務的內部網頁伺服器 IP 位址列表，而不是根據外面導入的 IP，例如在管制條例中有 2 個規則分別啟用 WAF 功能。

www.def.com (合法 IP : 1.1.1.1) → 內部網頁伺服器 (虛擬 IP : 192.168.1.1)

www.def.com (合法 IP : 2.2.2.2) → 內部網頁伺服器 (虛擬 IP : 192.168.1.1)

1 個網對外服務的網站 www.def.com ，因為做線路負載平衡所以有 2 個對外 IP 位址，分別是 1.1.1.1 / 2.2.2.2 ，到最後都導向內部的 1 個網頁伺服器 192.168.1.1 ，則在網站管理只會出現 192.168.1.1 這一個主機 IP。（圖 9-4）

主機 IP	主機通訊埠	連線協定	伺服器名稱	憑證資訊	修 改
192.168.195.89	80	HTTP	www.def.com	--	
192.168.189.151	443	HTTPS	www.defg	Local Certificate	

圖 9-4 網站列表

- 【主機 IP】：內部實際網頁伺服器的 IP 位址。
- 【主機通訊 Port】：網頁伺服器使用的通訊 Port，一般而言 80 是 http，443 是 https，管理者也可以根據網路環境改變 Port，例如 ： 8080 、 8000 、 8443 等。
- 【通訊協定】：網頁伺服器使用的通訊協定，一般而言 80 是 http，443 是 https，https 協議就需要匯入【原】網頁伺服器使用的憑證，如果沒匯入憑證使用者的瀏覽器就會出現憑證錯誤的警告。
- 【伺服器名稱】：網頁伺服器的名稱，如果是空白，則將外部連線需求直接轉給網頁伺服器，如果後端的網頁伺服器支援多台的 Virtual Host，則需要填入實際使用的 Virtual Host ，讓後端的網頁伺服器有 SNI 可以分辨，這些動作都可以透過 進行修改。HTTP 網站名稱（圖 9-5）

圖 9-5 HTTP 網站名稱

■ 【憑證資訊】：https 協定需要把後端伺服器的憑證匯入 WAF 中，在【伺服器、憑證列表】中按下 就可以進行修改，每一個 Virtual Host ，都需要匯入相對應的憑證。（圖 9-6）

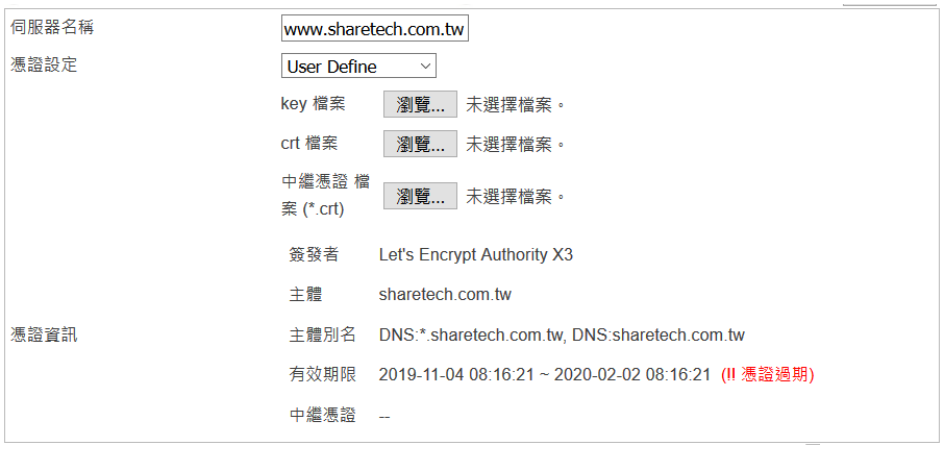


圖 9-6 HTTPS 網站名稱及匯入憑證

■ 【憑證設定】：後端伺服器的憑證使用的來源有 2 個，Local Certificate 跟 User Define，User Define 是匯入後端伺服器既有的憑證，在 Key 檔案、crt 檔案中匯入原本伺服器的憑證檔，Local Certificate 是使用 NG-UTM 的憑證檔。

9-1-3、阻擋頁面

WAF 在運作時，後端往往有很多伺服器，每一台伺服器的內容不一定一樣，在阻擋時呈現給使用者的資料也會不一樣，這些阻擋訊息可以在這裡設定。

預設阻擋頁面設定

系統會預設阻擋頁面，管理者可以點選【阻擋結果網頁設定】中的檢視，就可以查看，對於需要自定阻擋頁面的伺服器則在【自訂阻擋頁面伺服器】中，首先，選擇需要自訂阻擋頁面伺服器，系統會自動列出已經建立的伺服器讓管理者勾選，勾選後在上面輸入名稱跟阻擋資訊，儲存後就完成設定。（圖 9-7）

圖 9-7 WAF 阻擋頁面設定

9-1-4、WAF 白名單

有些網站在程式設計過程會觸發 WAF 規則，但是改程式又是複雜的問題，如果違反的是低風險的規則，管理者可以將它設為白名單，則系統在比對時就不會套用它。（圖 9-8）

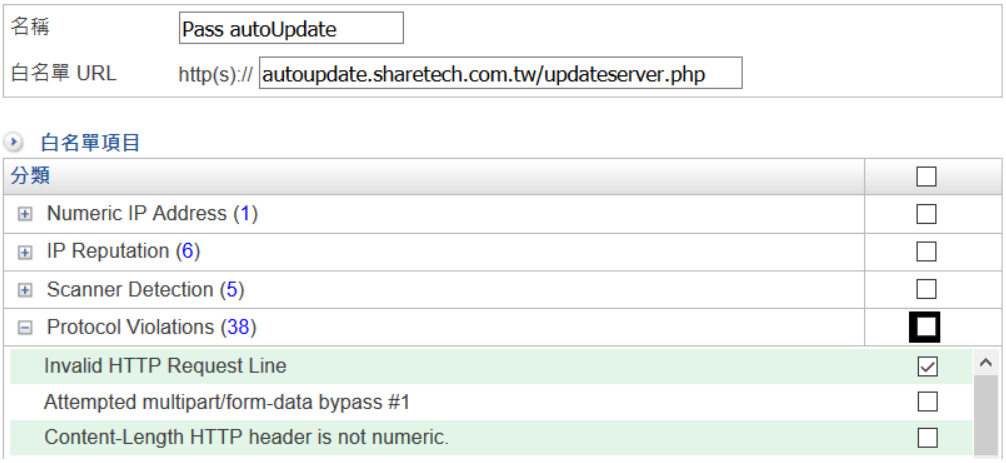


圖 9-8 WAF 白名單設定

- 【名稱】：白名單的名稱。
- 【白名單 URL】：哪一個 URL 觸發 WAF 規則且想把它設為白名單，在這裡填入 URL 就可以。
- 【白名單項目】：觸發的是哪一個項目，勾選後這個 URL 的白名單項目就不會檢查。

管理者可以在 WAF 阻擋紀錄中找尋誤檔的項目，直接在紀錄中加入白名單就可以。

9-2-1、WAF 記錄

每一個被 NG-UTM 的 WAF 分析到的規則，都會列表在這裡，管理者可以從中去找出目前駭客是使用哪一種手法攻擊。（圖 9-9）

紀錄列表　1 / 8　跳至 1　頁數 每頁 16 筆 GO　匯出　匯出全部

日期	動作	來源 IP	Url	目的主機	分類	事件	連線次數	白名單
2020-04-08 15:34:56	阻擋	179.13.219.219	http://125.227.221.21	192.168.195.89:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2020-04-08 14:34:44	阻擋	45.56.78.64	http://60.249.6.185/dbgeng.dll	192.168.195.89:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2020-04-08 14:18:21	阻擋	143.255.243.182	http://60.249.6.185:80	192.168.195.89:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2020-04-08 14:14:01	阻擋	67.200.231.19	http://127.0.0.1/cgi-bin/mainfunction.cgi	192.168.195.89:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	

圖 9-9 WAF 記錄

- 【動作】：有記錄跟阻擋 2 種，系統用顏色區分，紛紅色為紀錄的項目，白色為記錄。
- 【來源 IP】：攻擊者的來源 IP 位址。
- 【URI】：被攻擊的 URI，管理者可以知道那一個 URI 被攻擊，如果是自己的網頁程式寫不標準引起的假攻擊事件，藉此可以去調整。
- 【目的主機】：有啟用 WAF 服務的 實際網頁伺服器 IP 位址。
- 【分類】：那一種 WAF 攻擊項目。
- 【事件】：分類中的哪一個細項引起的攻擊。
- 【連線次數】：同一個來源 IP 位址的攻擊次數。
- 【白名單】：管理者確認這是 WAF 誤檔，點選白名單後這一個規則就會自動設為白名單。

9-2-2、WAF 封鎖記錄

每一個被 NG-UTM WAF 封鎖的來源 IP 位址都在這裡查詢。

第 10 章 郵件管理

NG-UTM 對通過所有介面的郵件可以進行管理，不論郵件伺服器是架設在內部或是外部，在郵件管理章節中，以【近端】代表郵件伺服器是架設在 NG-UTM 的內部，網際網路上的寄件者利用 NG-UTM WAN 類型的線路，將郵件寄到內部郵件伺服器中，相反的【遠端】代表郵件伺服器是架設在網際網路上，當內部使用者透過 WAN 類型的網路去寄信，不僅是寄信的郵件可以被管理，內部的使用者用 POP3 協定到網路上收信，也可以被 NG-UTM 攔截跟管理。

NG-UTM 在郵件處理上的角色扮演有點像是郵件閘道器，可以對於進、出的郵件執行下列之一或是全部的功能：

1.郵件掃毒：對於進、出的郵件，進行掃毒。

2.垃圾郵件過濾：對於進、出的郵件，進行垃圾郵件過濾。

3.郵件稽核：對於進、出的郵件，進行郵件稽核，經郵件管理者放行後郵件才會寄出。

4.郵件備份：對於進、出的郵件，進行備份，方便日後查詢。

5.郵件通聯記錄查詢：詳細記錄郵件伺服器對郵件伺服器的 SMTP 對話紀錄，方便管理者找出無法收、送郵件的問題點。

典型的應用範例如示意圖。(圖 10-1)

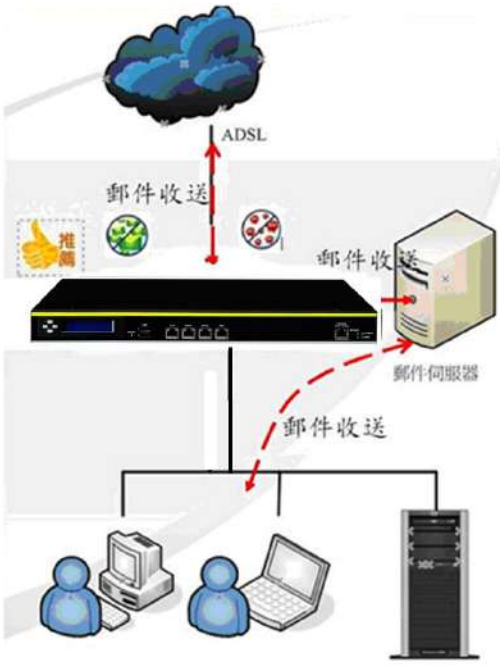


圖 10-1 一般企業郵件伺服器規劃架構

10-1、郵件過濾與紀錄

NG-UTM 對於進、出的郵件要啟用掃毒、垃圾郵件過濾、郵件稽核跟備份中哪一些功能，在這裡可以讓管理者選擇，因為它是屬於郵件閘道器的功能，本身並沒有郵件使用者的帳號，所以 NG-UTM 需要跟後端的郵件伺服器驗證是不是有這一個使用者。

除了郵件的基本進、出的郵件管理外，如果有駭客攻擊郵件伺服器，NG-UTM 也可以提供保護，例如，某個來源 IP 位址一直對郵件伺服器傳送垃圾郵件，當超過合理(預先設定的流量)後，NG-UTM 就會拒絕這個來源 IP 位址的寄信要求。

10-1-1、郵件過濾與紀錄

NG-UTM 具有郵件閘道器功能，所謂郵件閘道器就是利用郵件代理的技巧，將所有的信件攔到 NG-UTM 的中，經過垃圾郵件、病毒、稽核、紀錄等機制後，再將原來的郵件轉給原來的郵件伺服器，補足原來郵件伺服器功能不足的地方。

因為 NG-UTM 本身不是郵件伺服器，對於要將垃圾郵件通知的信件寄給收信者，需要借重原來的郵件伺服器提供有效帳號。

郵件過濾功能啟用

以 NG-UTM 的觀點，郵件的進、出共有 3 個主要動作，一個是外部對**內部(近端)**的郵件伺服器寄信，另一個是內部對**外部(遠端)**的郵件伺服器寄信，最後一個是內部到外部的郵件伺服器收信，每一個動作可以獨立選擇要執行的功能。（圖 10-2）

SMTP 近端的郵件掃毒、郵件稽核、垃圾信過濾、備份

- 【啟用功能】：啟用外部對近端郵件伺服器的功能，有全選、掃毒、郵件稽核、垃圾郵件過濾跟郵件備份等選項。

SMTP 遠端的郵件掃毒、郵件稽核、垃圾信過濾、備份

- 【啟用功能】：啟用外部對近端郵件伺服器的功能，有全選、掃毒、垃圾郵件過濾跟郵件備份等選項，它比其他的功能少郵件稽核的功能。

收信的郵件掃毒、郵件稽核、垃圾信過濾、備份

- 【啟用功能】：啟用外部對近端郵件伺服器的功能，有全選、掃毒、郵件稽核、垃圾郵件過濾跟郵件備份等選項。

SMTP 記錄設定

NG-UTM 能夠對每一封信的 SMTP 通聯記錄進行詳細的紀錄，包含郵件伺服器對郵件伺服器的溝通，如果管理者要找出某一封郵件無法成功寄出的原因時，SMTP 通聯記錄也會詳細記錄，此項功能可以由管理者決定要不要啟用，或者是部分啟用。

- 【近端】： 有 3 個選項，關閉、接受跟全部，預設是關閉，選擇接受的 SMTP 紀錄時，只紀錄允許跟對方溝通的 SMTP 紀錄，其他被 SMTP 阻擋掉的不會記錄下來，這樣可省下一些不必要的紀錄。
- 【遠端】：有 3 個選項，關閉、失敗跟全部，預設是關閉，選擇失敗的 SMTP 紀錄時，只紀錄跟對方溝通的 SMTP 過程中紀錄，其他正常寄出的信不會記錄下來，這樣可省下一些不必要的紀錄。
- 【記錄類型】：可記錄簡單或詳細版，要找寄信問題時可以選擇詳細版。

圖 10-2　郵件過濾功能啟用

郵件紀錄相關設定

NG-UTM 執行郵件備份時，對於超過設定範圍的郵件要不要備份，這個功能限在外部對內部(近端)的郵件伺服器寄信跟內部對外部的郵件伺服器(遠端)寄信，或是內部到外部的郵件伺服器收信這 3 個功能中有啟用郵件備份時才會生效。（圖 10-3）

- 【郵件檔案備份】：郵件檔案大於設定值，備份郵件時附件不會被記錄下來。預設值為 0，代表不限制。
- 【收信】：郵件檔案大於設定值，備份郵件時附件不會被記錄下來，預設值為 640KB，代表檔案超過 640KB 不做掃毒、垃圾郵件過濾，只進行黑白名單處理。

更換來源 IP 位址為設備 IP

這個功能限制在只對外部對內部(近端)的郵件伺服器寄信時有效，NG-UTM 屬於郵件閘道器的功能，當他代理郵件並將他執行掃毒、垃圾郵件過濾後，郵件還是需要傳給原來的郵件伺服器，此時傳送給原來郵件伺服器的來源 IP 位址是要用 NG-UTM 介面的 IP 位址還是原始寄件伺服器的 IP 位址。

- 【SMTP 近端寄信】：啟動代表會用 NG-UTM 的介面 IP 位址為來源 IP 位址，傳送給郵件伺服器。關閉則代表會用原始寄件的郵件伺服器的 IP 位址當作來源 IP 位址。

放行攜帶主旨

這個功能限制在郵件備份功能下，郵件經由管理者放行後，被放行的郵件要不要在主旨上插入一段文字，讓他跟原始的郵件有差別，讓管理者跟使用者知道，這是一封被放行的郵件。

- 【加入主旨】：啟動代表會在放行郵件加入一個預設的文字，預設是關閉。
- 【主旨內容】：插入一個時間戳記，例如，$Y-$m-$d $H:$i:$s 代表會在放行郵件主旨最前面插入 2016-5-31 12:12:30 時間戳記。

垃圾郵件清單、稽核通知信的連線設定

這個功能限制在啟用垃圾郵件過濾跟郵件稽核這 2 項功能有啟用下，當使用者收到 NG-UTM 寄出的垃圾郵件清單或是稽核管理者收到要稽核放行郵件清單時，點選放行郵件時使用的 IP 位址或是網域名稱。

- 【IP 位址或 Domain】：可設 NG-UTM 的介面 IP 位址或是網域名稱。
- 【通訊埠】：預設為 443，管理者可以按下變更後更改。

圖 10-3　郵件過濾進階項目設定

10-1-2、有效帳號設定

NG-UTM 當作郵件閘道器時，因為本身沒有郵件帳號，如果沒有跟後面(近端)的郵件伺服器做帳號的整合，會收下非郵件伺服器的郵件在佇列中，這些在佇列中的垃圾郵件並沒有辦法送出，當佇列中的垃圾郵件數量多時，會造成 NG-UTM 的負擔。

為了降低這些非本機的郵件，因此 NG-UTM 有 2 種作法，一種是把郵件帳號匯入，另一種是即時的登入郵件伺服器檢查帳號是否存在，即時的檢查機制適用於後端的郵件伺服器是 Microsoft Exchange 伺服器且帳號是跟 AD 伺服器整合。

郵件帳號匯入的方式有自動增加跟手動匯入 2 種方式，NG-UTM 也可以啟用自動學習帳號機制，自動加入。

SMTP 寄信需要驗證/不需要驗證

郵件伺服器對於要寄信的使用者，當使用 SMTP 去寄信時會要求使用者認證，確保不會被當成寄垃圾郵件的跳板，目前大部分的郵件主機設定都是需要認證，但有一些只是對內部服務的郵件主機或是已經建立 Mail Relay 關係的郵件主機，不一定會啟用 SMTP 認證，所以管理者必須知道所 NG-UTM 郵件閘道器所代理的網域是否需要 SMTP 驗證寄信，並根據這樣的屬性，在不同的地方輸入有效帳號驗證。

有效郵件設定(需驗證)

後端的郵件主機需要進行 SMTP 寄信驗證時，在這裡加入代理的網域跟帳號，只要填入網域名稱，所有經過閘道器且成功到後端郵件主機的帳號就會自動到有效帳號的名單中。（圖 10-4）

- 【啟用】：要不要啟用有效帳號的新增功能。
- 【學習啟用】：NG-UTM 會自動學習合法、有效的帳號到郵件帳號中，例如，NG-UTM 的郵件閘道器收到一封寄給 jean@abc.com 的郵件，把它轉送給後端的郵件伺服器，如果後端的郵件主機接受這一封郵件，則 Jean@abc.com 這個帳號就會自動加入有效帳號中，下次寄給她的郵件就不需要進行驗證。
- 【網域清單】：把後端郵件伺服器的網域填入就可，例如，abc.com，如果有多網域就每一行一個網域，如果 NG-UTM 收到要求寄給 def.com ，但是 def.com 沒在網域清單中，則 NG-UTM 會拒絕這一個郵件。
- 【郵件帳號】：填入合法的郵件帳號，例如，jean@abc.com。
- 【匯入】：管理者可以將郵件主機的郵件帳號匯出後，一次性的匯入系統中。

圖 10-4　手動加入有效帳號

有效郵件設定(不需驗證)

後端的郵件主機需要進行 SMTP 寄信時，不需要驗證，在這裡加入代理的網域跟帳號，只要填入網域名稱，所有經過閘道器且成功到後端郵件主機的帳號就會自動到有效帳號的名單中。

- 【啟用】：要不要啟用有效帳號的新增功能。
- 【網域清單】：把後端郵件伺服器的網域填入就可，例如，abc.com，如果有多網域就每一行一個網域，如果 NG-UTM 收到要求寄給 def.com ，但是 def.com 沒在網域清單中，則 NG-UTM 會拒絕這一個郵件。
- 【郵件帳號】：填入合法的郵件帳號，例如，jean@abc.com。
- 【匯入】：管理者可以將郵件主機的郵件帳號匯出後，一次性的匯入系統中。

有效郵件設定(Exchange Server)

後端的郵件主機如果是 Microsoft 的 Exchange Server 時，需要進行 SMTP 寄信驗證時，一定需要 SMTP 驗證，帳號的驗證有 2 種方式，手動匯入及自動跟 AD 伺服器同步。

手動匯入是 Exchange Server 單獨運作，並沒有跟 Microsoft AD 伺服器進行帳號的整合，在這個情況下，管理者需要在這裡加入代理的網域跟帳號，只要填入網域名稱，所有經過閘道器且成功到後端郵件主機的帳號就會自動到有效帳號的名單中。

自動跟 AD 伺服器同步選項下，藉由 NG-UTM 去 AD 伺服器同步取得使用者帳號，並把他加入有效帳號中。

- 【啟用】：要不要啟用有效帳號的新增功能。
- 【同步啟用】：預設為關閉，在關閉的情況下，管理者需要填入網域清單及郵件帳號或者用匯入的方式增加有效郵件帳號。
- 【網域清單】：限【同步啟用】是關閉下的功能，把後端郵件伺服器的網域填入就可，例如，abc.com，如果有多網域就每一行一個網域，如果 NG-UTM 收到要求寄給 def.com ，但是 def.com 沒在網域清單中，則 NG-UTM 會拒絕這一個郵件。
- 【郵件帳號】：限【同步啟用】是關閉下的功能，填入合法的郵件帳號，例如，jean@abc.com。
- 【匯入】：限【同步啟用】是關閉下的功能，管理者可以將郵件主機的郵件帳號匯出後，一次性的匯入系統中。
- 【同步啟用】：設為啟動，管理者點選新增 Exchanger Server 的按鈕，NG-UTM 會出現 AD 伺服器的 IP 位址、網域名稱、管理者帳號密碼，並選擇要加入的群組就可以完成設定，另有 連線測試 跟 記錄 可以讓管理者驗證設定的資料是否正常，另可以設定同步週期，每幾分鐘到 AD 伺服器取得最新的帳號資料。（圖 10-5）

圖 10-5 AD 跟有效帳號

有效清單設定

- 【允許非有效清單網域通過】：管理者是否允許沒設在有效清單的網域通過，預設值是關閉，只有表列在清單中的網域才會接受，啟動下是任何網域都可以寄送。

- 【阻擋日誌】：點選 記錄 會顯示，哪些寄件者嘗試利用 SMTP 協定，經過 NG-UTM 的郵件過濾機制後，到後端的郵件伺服器。(圖 10-6)

阻擋日誌　匯出　清除　1 / 1

日期	寄件者 IP	寄件者	收件者	狀態
2012-01-09 13:56:56	192.168.188.23	<>	1	非有效網域
2012-01-09 13:39:43	192.168.188.23	<>	aa	非有效網域
2012-01-09 12:28:04	192.168.188.23	aa	aa	非有效網域
2012-01-09 12:26:44	"192.168.188.23"	"aa	"aa	非有效網域

圖 10-6 阻擋紀錄

註 1：當啟動有效帳號啟用功能後，凡是未建置在【有效帳號 E-mail】欄位的帳號都會被系統直接隔離刪除，因此，當啟用此功能時需特別注意有效帳號 email 名單的建立。

註 2：帳號名單除了可單筆建立外，NG-UTM 亦提供快速匯入方式，可將檔案存為.txt、.csv 檔。

10-1-3、灰名單與 IP 反解設定

灰名單過濾功能只要是過濾垃圾郵件行為，一般來說廣告業者在第一次發送廣告信件時，如果收件者拒收，就不會再發送第二次，而灰名單過濾主要就是發揮這種特性，對於第一次陌生寄送的帳號都拒收。

正常的郵件主機，在信件第一次發送失敗時，會在傳送第二次、第三次，則灰名單過濾機制在正常郵件第二次寄送時就會收下信件，往後此寄件者的來信都不會做阻擋，除非使用者有將它列入黑名單或其他判別條件中。

灰名單原理：（圖 10-7）

灰名單方法非常簡單，它僅專注於郵件傳遞的三項信息

1 寄件者來源 IP

2 寄件者

3 收件者

如果灰名單系統從未見過這三項組合時，就會在一定阻隔時間(初值 300 秒)內『暫時』拒絕這封信件傳遞，寄件方將會收到如下錯誤訊息

> 450 <收件者>: Recipient address rejected: Greylisted, see http://postgrey.schweikert.ch/help/ShareTech.com.tw.html

對於正常郵件伺服器而言，這並不會造成太大問題，因為它明瞭 450 只是暫時拒絕接收，因此會在稍後重複嘗試遞送；而對於垃圾郵件發送系統，通常是採用：發後不管、偽造寄件者、變換 IP 的方法，這些正是灰名單機制可以有效攔阻的。

反過來說，只要見過這三項組合，且達到一定阻隔時間後和重試時間(初值 2 天)內，信件就會享有一段有效期限(初值 35 天)內被正常收下，而且在此期間內收到信件後，此期限會再被延長。

灰名單的副作用，由於初次收信會阻隔一段時間，所以正常信件實際收到時效將稍被延遲，延 遲時間將視寄件方的郵件伺服器的重送機制而定；同時因為這樣的關係，可能造成後寄信件比前面信件早到的特殊現象，不過這都僅限於初次通信時發生。

處理流程如下圖

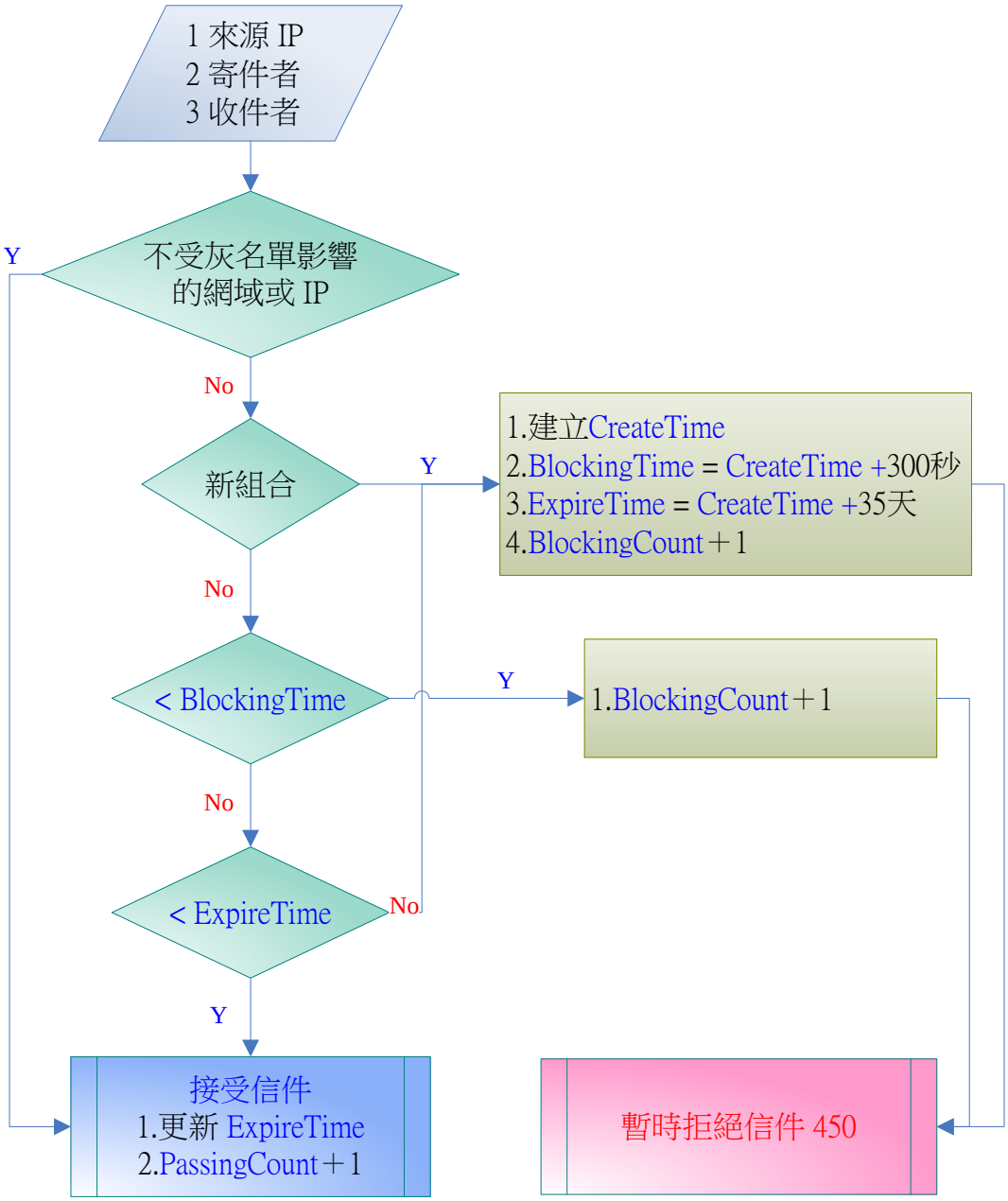


圖 10-7 郵件處理程序

參考資料：http://projects.puremagic.com/greylisting/whitepaper.html

灰名單設定（圖 10-8）

- 【灰名單啟用】：要不要啟用灰名單的功能，預設是關閉。
- 【收信延遲時間】：拒絕第一次 SMTP 連線後間隔多久後接受第 2 次 SMTP 寄信，預設值為 15 秒，設定範圍是 1~1000 秒。
- 【阻擋日誌】：紀錄灰名單阻擋的紀錄，包含時間、寄件者 IP 位址、寄件者跟收件者，這個紀錄大於 100Kbytes 後，NG-UTM 會自動清除。

IP 反解設定

網域名稱對 IP 位址有 2 個 DNS 專有名稱：正解和反解，正解就是把網域名稱解析成 IP 位址，例如，www.yourdomain.com，DNS 就會幫我們翻譯成 211.22.160.28 就是正解的功能，反解是把 IP 位址轉成網域名稱，例如，211.22.160.28 反解成 www.yourdomain.com。

- 【IP 反解驗證功能】：預設是關閉。
- 【未驗證通過處理方式】：當 NG-UTM 無法透過 IP 反解機制找到相對應的網域名稱，此寄件者很有可能是濫發垃圾郵件或是他的網域伺服器沒設定 IP 反解，管理者可以選擇下列 3 種之一處理這類型的郵件。

1. 直接刪除：這一封郵件一定是垃圾郵件，刪掉他。
2. 直接隔離：這一封郵件可能是垃圾郵件，把它先放在隔離區中。
3. 增加垃圾郵件分數：增加垃圾郵件的分數，再由總分決定是不是垃圾郵件，預設增加 5 分，設定範圍是 1~20 分。

共同設定

為了避免客戶發送信件遭受灰名單的阻擋，可以先將企業用戶網域或 IP 先加入信任名單設定 IP 位址或區段，這一些區段的寄件者，都不會進入灰名單或是要求 IP 反解，這一些 IP 位址或是網域名稱可以藉由匯入/匯出的機制保留或是還原資料，格式如下，每一行一筆：

192.168.0.0/16

192.168.1.22

Trust.domain

圖 10-8 灰名單跟 IP 反解

10-1-4、流量封鎖防禦設定

灰名單過濾垃圾郵件的發送技術越來越進步，網路的使用者往往不知道自己已經受害被當成垃圾郵件的跳板而不知。

傳統的 firewall 或是 UTM 甚至 IPS 並沒有辦法阻擋這樣的行為，因為從網路的觀點，這是管理者允許的網路行為，一旦 ISP 業者發現並封鎖 對外 IP 時，才去找 LOG 紀錄，分析那一個設備才是跳版。

NG-UTM 的異常發送郵件偵測及阻擋將這一方面的技術發揮到極致，一旦有人被當跳板，立刻阻擋。

認證異常

一般正常寄信不會在短短的時間內發送大量的信件，利用這個特徵值，管理者可以設定防禦機制，假設 UTM 在 120 秒內收到同一個來源 IP 或是帳號對外發送超過 10 封信，就可以認定他是被植入木馬，此時將對外發信的動作阻擋特定時間。（圖 10-9）

- 【使用者認證異常情形】：要不要啟用異常寄件流量的封鎖，預設是啟用。
- 【認證異常規則設定】：怎樣的條件才是異常，預設值是 120 秒內，同一來源 IP 位址嘗試寄信，但是認證失敗 10 次，NG-UTM 就會認為這一個寄件者或是寄件 IP 位址嘗試攻擊或是猜測使用者密碼，處理動作就是拒絕這個來源 IP 位址或是寄件者 600 秒。

圖 10-9 流量封鎖防禦設定

流量封鎖防禦（圖 10-10）

當寄件者觸發封鎖條件後，NG-UTM 有 2 種封鎖機制，根據寄件者帳號封鎖或是根據寄件者的 IP 位址封鎖。

依據寄件者封鎖

- 【依據寄件者封鎖】：要不要啟用寄件異常流量的封鎖，預設是關閉。
- 【此 IP 範圍才檢查寄件者】：啟用寄件異常流量的封鎖後，怎樣的條件才是異常，預設值是 100 秒內，同一來源 IP 位址嘗試寄信，但是認證失敗 10 次，NG-UTM 就會認為這一個寄件者或是寄件 IP 位址嘗試攻擊或是猜測使用者密碼，處理動作就是拒絕這個來源 IP 位址 600 秒。
- 【寄件者例外清單】：啟用寄件異常流量的封鎖後，針對表列的寄件者不會執行寄件者檢查，其他的寄件者檢查，簡單來說就是白名單寄件者。
- 【寄件者網域例外清單】：啟用寄件異常流量的封鎖後，針對表列的網域不會執行寄件者檢查，其他的網域檢查，簡單來說就是白名單網域名稱。

依據 IP 位址封鎖

- 【依據 IP 封鎖】：要不要啟用寄件者異常流量的 IP 位址封鎖，預設是關閉。
- 【寄件者 與 IP 規則設定】：啟用依據 IP 封鎖後，針對表列的 IP 位址或是區段才會執行寄件者檢查，其他的 IP 位址不檢查，簡單來說就是黑名單 IP 位址。

圖 10-10 異常寄件者封鎖

共用設定

對於符合系統異常偵測規則之來源，管理者可以設定封鎖的時間、例外 IP 清單與封鎖防禦紀錄，並可以針對例外清單進行匯入/匯出的工作。（圖 10-11）

- 【每次封鎖時間】：觸發異常流量封鎖時，封鎖 IP 位址或是寄件者的時間，預設值為 600 秒。
- 【IP 例外清單】：IP 位址白名單，這些來源 IP 位址都不會被封鎖。

圖 10-11 流量封鎖共用設定

點選 記錄 會有詳細的封鎖紀錄及狀態，包含日期時間、寄件者 IP 位址、寄件者跟封鎖類型。(圖 10-12)

日期	IP	寄件者	封鎖類型	封鎖狀態	解除封鎖
2012-02-20 11:12:46	192.168.1.142	chaio@sharetech.com.tw	sender	已解除	-

圖 10-12 IP 封鎖防禦紀錄

10-1-5、SMTP 封鎖 IP

SMTP 封鎖 IP 跟流量封鎖 IP 防禦是不一樣的防護機制，流量封鎖 IP 防禦最主要防禦寄件者帳號被猜測密碼，此時的 SMTP 溝通已經完成並且進入傳送郵件階段，但是在 SMTP 溝通之前，駭客利用大量的 SMTP 請求，目的是癱瘓郵件伺服器，這樣的防護機制就由 SMTP 封鎖 IP 來處理。

- 【啟用】：要不要啟用異常 SMTP 封鎖機制，預設是啟用。
- 【封鎖中 IP】：被封鎖的異常 IP 位址會被封鎖 600 秒，這裡會顯示剩餘的封鎖時間及 IP 位址。

10-2、郵件掃毒

郵件病毒肆虐，讓人防不勝防，對於熟悉病毒運作原理的網管人員，接收到有問題的郵件時，例如特殊的圖片，網址超連結，*.exe..等檔案，通常不會貿然的點選，感染病毒的機會就少很多。

但是對於大部分的使用者而言，要分辨正常跟有問題的電腦執行檔或是網址超連結，是一件相當困難的事，點選或是執行後才知道問題，這時候只能仰仗本身電腦防毒軟體抵擋最後一關了，如果連這一關都擋不住，只能求助於網管人員了。

NG-UTM 的防毒功能，就是避免上述的情況發生，有問題的郵件一進入 UTM 設備後，藉由內部病毒過濾引擎，將有問題的郵件隔離或是刪除，不必送至使用者的郵箱，當然就降低使用者感病毒的機會。

啟動郵件掃毒時會比較耗費硬體資源，如 CPU、RAM 等，如果整個網路環境已經建立類似防毒牆的郵件閘道器，專責掃毒，則此項功能可以關閉。

目前 NG-UTM 內建 ClamAV 掃毒引擎跟選購 Kaspersky 掃毒引擎，針對中毒的郵件，統統會被歸類在「病毒信件隔離區」中，管理者可以透過病毒郵件的列表，看到病毒隔離區的信件，什麼時間、什麼人寄給那一個人、主旨為何、中毒的檔案為何、中了那一種病毒，管理者可以輸入選項搜尋特定郵件。

10-2-1、郵件掃毒

NG-UTM 內建的掃毒引擎掃出來由夾帶病毒的郵件，NG-UTM 可以將它的檔案改名跟郵件主旨改掉，提醒收信者小心這一封郵件。

基本設定(圖 10-13)

- 【啟動郵件掃毒】：啟動郵件掃毒功能。
- 【使用掃毒引擎】：選擇掃毒引擎，預設會選擇 ClamAV 掃毒引擎，可以選購 Kaspersky。
- 【不掃描的檔案】：建立不掃瞄的檔案名稱（jpg、gif 等），增加郵件處理的速度，NG-UTM 解析接收的郵件，如果夾帶檔案的副檔名跟設定的一樣，掃毒系統就會跳過這個病毒檢查程序，進入下一個郵件處理程序，每一不掃描副檔名為一行。
- 【最大掃描檔案大小（KB）】：當郵件的附件超過設定的大小後，掃毒引擎就不會掃描這一封郵件。

中毒郵件處理方式

- 【隔離中毒信件】：當選擇隔離中毒郵件時，該郵件的收信者不會收到這一封郵件，預設是關閉，代表郵件收信者會收到一封中毒郵件通知信，通知信的檔名跟主旨如下列描述。
- 【中毒郵件儲存副檔名為】：將中毒郵件的夾帶檔案的檔名改掉，例如，virus，避免收信者誤執行該檔案。
- 【中毒郵件通知信主旨】：將中毒郵件的主旨改掉，例如，郵件中毒，提醒收件者。

圖 10-13 設定中毒郵件處理方式

10-2.2、病毒信件隔離區

於【郵件掃毒】中的【病毒信件隔離區】功能中，搜尋下列資料。

- **搜尋**的條件如下：

  【收件日期】：有病毒的郵件進入隔離區的時間，可以指定時間區間。

  【寄件者】：是誰寄出病毒的郵件。

  【寄件者 IP】：寄件者 IP 位址。

  【收件者】：這一封病毒信的收件者。

  【郵件主旨】：病毒信件的主旨。

  【郵件大小】：病毒信的檔案大小。

10-3、垃圾郵件過濾

垃圾郵件的氾濫，不僅造成工作效率的低落，病毒、木馬郵件甚至會導致網路安全的疑慮，所以防範垃圾郵件成為郵件系統不得不做的事情。

NG-UTM 內建垃圾郵件的過濾功能，使用者不會收到堆積如山的垃圾信，免除從一堆無用的信件中，挑出所需要接受的訊息，或在刪除這些信件時，誤刪所需要的郵件，讓員工的工作效率提升，也不會錯失任何業務上往來溝通的訊息。

判斷垃圾郵件的機制，最怕的動作就是誤判斷，將原本正常的信件判斷成垃圾信，所以都有事後補救的方法，只是這個辦法是由管理者還是由個別的使用者來做。

UTM 防火牆會在設定的時間內，寄一封個人的垃圾郵件通知信給使用者，其中會列出時間、寄件者、收件者、主旨、綜合垃圾郵件判斷分數等資料，如果使用者覺得信件被誤判，直接下載該檔案就可以。

★範例

NG-UTM 是用整封郵件行為，並將它轉換成綜合判斷分數，一般垃圾郵件評分如下所示：

0.1 MIME_HTML_ONLY BODY: Message only has text/html MIME parts

0.0 HTML_MESSAGE BODY: HTML included in message

2.2 HTML_IMAGE_ONLY_02 BODY: HTML: images with 0-200 bytes of words

0.7 MIME_HTML_NO_CHARSET RAW: Message text in HTML without chareset

1.9 MIME_HEADER_CTYPE_ONLY ‘Content-Type found without required MIME headers

1.6 FORGED_MUA_OUTLOOK Forged mail pretending to be from MS Outlook

X-Spam-Status: Yes，hits=6.5 required=6.0 tests=FORGED_MUA_OUTLO

針對信件的行為給予不同的分數，例如：某個收件者收到一封信，在信件的本文中只有網址超連接，沒有其他的文字說明，在一般的郵件而言，它很有可能是要誘惑收信者點選某一個特定網站，有相當程度上它可能會是垃圾郵件，所以以上述的例子，給予 0.1 分。

將這些判斷行為的分數統統加總起來，就是這封郵件的垃圾郵件分數，分數越高，是垃圾郵件的可能性高。

以上面的範例來說，加總為 0.1+0.0+2.2+0.7+1.9+1.6 = 6.5，再根據管理者的設定，6.5 分是不是垃圾郵件。

對於垃圾郵件的處理方法共有 3 種，主旨加入提示文字、放在隔離區、刪除，詳細的說明會在「垃圾郵件處理方式」中說明。

10-3-1、基本設定

對於垃圾郵件的過濾機制及想要減少誤判的機會，管理者可以在這裡詳細的設定，一開始如果不知道如何調整，可以全部使用預設值，再根據使用者的回饋訊息，調整細項功能，例如，評分的大小，就算系誤判了，把正常郵件歸類為垃圾郵件，郵件收件者仍然可以自行登入垃圾信取回機制的網頁，自行取回遭到誤判的郵件。

垃圾郵件過濾基本設定（圖 10-14）

- 【目前垃圾郵件過濾狀態】：目前 NG-UTM 的垃圾郵件過濾機制的運作狀態，是【正常運作中..】或是停止運作，因為有些垃圾郵件的判斷機制會使用網路去檢查最新的 IP 位址狀況，網路不通的情況下，這個地方會顯示停止運作的狀態。
- 【垃圾郵件過濾】：垃圾郵件過濾這項功能目前是設定為啟動或是關閉。
- 【通過 SMTP 認證使用者所發出信件的垃圾郵件過濾】：啟動後，郵件伺服器對於使用 SMTP 認證成功的寄件者所有的傳送接收郵件，不會再進入垃圾郵件的過濾程序。他的主要原因是一旦通過 SMTP 認證，確認這個使用者是正常郵件伺服器寄出的郵件，所以會寄出垃圾郵件的機會相對減少一些。

  假設選擇關閉，但萬一是郵件帳號的 SMTP 帳號密碼被猜中，則可能寄出大量的垃圾郵件出去，所以管理者必須要根據郵件伺服器的密碼帳號強度，決定這一項功能要關閉或是啟動。
- 【**最大**掃描檔案大小】：預設值為 512 Kbytes，郵件超過這個大小，垃圾郵件過濾機制將不會掃描整封郵件。
- 【垃圾郵件學習共享】：團結力量大，啟用這項功能時，會把介於正常跟垃圾郵件的灰色地帶郵件轉到雲端的學習機制，藉由大資料學習的方式，讓學習後的特徵值自動下載到 NG-UTM 中，下次再比對時，就讓正常郵件分數更低，垃圾郵件的分數更高。

圖 10-14 垃圾信辨識引擎的基本設定

垃圾信辨識引擎的設定及狀態（圖 10-15）

對於垃圾郵件的過濾引擎，NG-UTM 總共提供 3 種辨識機制，由管理者決定要啟用哪幾個？其中 ST-IP 網路信評的機制，需要透過網路跟提供 SPAM-IP 位址過濾的網站進行更新，當網路斷線時，這一項功能則無法啟用。

- 【ST-IP 網路信評】：這個功能參照垃圾郵件系統的黑名單 IP 位址資料庫，如果寄件者的 IP 位址來自於被列入黑名單 IP 位址資料庫的 IP 位址，那他是垃圾郵件的比率就相當高，

  如果寄件者的 IP 位址是動態的，是垃圾郵件的比率也是相當高的，掃描引擎需要網路暢通才能使用，所以選擇啟動時要注意，NG-UTM 對外的網路是否正常，預設值是啟動。

- 【貝氏過濾法】：貝氏過濾法是將信件之內文以貝氏資料庫之規則來評分，分數越高者其越有可能是垃圾信件。一般來說「貝氏過濾法」會有個資料庫，當一封信件進入系統的時候會把信件分解成單詞，比對目前「貝氏過濾法資料庫」，分析以往的經驗，來判別此封信件為垃圾信件的機率，且貝氏過濾資料庫具有自動學習的功能，可以依照不同企業收信的狀態來調整最適合的過濾條件，預設值是啟動。

- 【貝氏過濾自動學習機制】：是否要啟動垃圾郵件過濾機制中貝氏過濾法的自動學習機制，預設值是啟動。

圖 10-15 垃圾信辨識引擎的設定

垃圾郵件處理方式

NG-UTM 是用垃圾郵件分數決定如何處理被判斷成垃圾郵件的信，管理者可以依據本身的需求設定判斷分數，原則上分數設的高，代表使用者必須容許較多的垃圾郵件，一開始設定分數時可以將它的分數稍微調高一下，例如 7～8 分，管理者再根據使用者的反應，或是實際自己郵箱的運作情況調整，如此就可以調整到適合公司運作的垃圾郵件判斷分數。

對於垃圾郵件的處理方法共有 4 種，這 4 個動作的垃圾郵件分數可以分別設定，管理者可以從 4 個處理方式中任意組合處理，這 4 種處理方式如下：（圖 10-16）

1.僅作資料分析。

2.主旨加入提示文字然後傳給使用者。

3.放在垃圾郵件隔離區，定時寄送垃圾郵件清單給使用者。

4.直接刪除

垃圾郵件處理方式->僅作資料分析

NG-UTM 執行完垃圾郵件分析後，完封不動的將郵件傳遞給後端的郵件伺服器，不會改變郵件標題或是把它放入隔離區中，因為 NG-UTM 具有郵件防火牆的功能，所以此項功能除了能提供郵件的統計資料給 Dashboard 外，也可以保護後端的防火牆免於垃圾郵件業者的攻擊或是測試。

- 【垃圾郵件分數大於】：設定垃圾郵件分數大於【 】分以上為垃圾郵件，此分數單純給統計報表統計垃圾郵件的數量。

垃圾郵件處理方式->主旨加入提示文字然後傳給使用者

- 【主旨加入文字後傳給收件者】：當 NG-UTM 判斷成垃圾信後，在信件主旨上要加的文字，預設是【Spam-Mail】，管理者可以改成想要的任何文字，當然也可以是空白文字。

  設成空白文字時是並不會影響使用者的收信內容，但是被判斷成垃圾信件的信件會顯示在「流量統計」的日誌中，管理者可以先藉由這些日誌分析，誤判的比率及實際應該設定的垃圾郵件分數為何？讓整體的判斷機制更準確。

- 【垃圾郵件分數大於】：設定垃圾郵件分數大於【 】分以上為垃圾郵件，此時會執行【主旨加入文字後傳給收件者】的動作，預設值是 5 分。

- 【垃圾郵件主旨提示文字】：設定垃圾郵件主旨提示文字，預設為【Spam-Mail】，可以自訂任何中英文字。

垃圾郵件處理方式->放在垃圾郵件隔離區並發送清單

- 【垃圾郵件在隔離區並發送清單】：當 NG-UTM 判斷成垃圾信後，郵件並不會後送件伺服器，而是把這封郵件放在隔離區中，並定時的發送垃圾郵件通知清單給使用者，讓使用者知道哪一些郵件是被隔離的，在清單中，使用者可以直接按下取回的按鈕，將此封被誤判的郵件取回。

  垃圾郵件在隔離區保留天數設為【7】天，超過這個日期，垃圾郵件會被刪除。

- 【垃圾郵件分數大於】：設定垃圾郵件分數大於【 】分以上為垃圾郵件，此時會執行【垃圾郵件在隔離區並發送清單】的動作，預設值是 15 分。

垃圾郵件處理方式->直接刪除

- 【直接刪除】：當 NG-UTM 判斷成垃圾信後，郵件並不會後送件伺服器，而是把這封郵件放在刪除區中，在刪除區的郵件並不會通知使用者有郵件被放在此區中，只有管理者可以進入刪除區，取回郵件。

  垃圾郵件在隔離區保留天數設為【7】天，超過這個日期，垃圾郵件會被刪除。

圖 10-16 垃圾郵件的處理方式

垃圾郵件隔離區/刪除區

被 NG-UTM 判斷成垃圾郵件的郵件，如果管理者選擇放在隔離區，則郵件收件者會定時的收到垃圾郵件清單，如下範例。（圖 10-17）

	日期	寄件者	收件者	主旨	大小	分數	處理	個人化規則
☐	2016-02-29 17:04:56	hxoqieakl@ms76.hin...	jordan@sharetech.co...	約女同事登山後強迫她拍裸照...	1.9 KB	0	垃圾信	取回 加入黑名單 加入白名單
☐	2016-02-29 17:08:53	erwi@yub.com	cn@sharetech.com.tw	高效仓储管理与工厂物料配送	8.0 KB	62	垃圾信	取回 加入黑名單 加入白名單
☐	2016-02-29 17:24:21	upxbhkzqvdm@ms49...	bbs@sharetech.com.tw...	蘿莉淫蕩白衣天使	1.8 KB	21.91	垃圾信	取回 加入黑名單 加入白名單
☐	2016-02-29 17:50:06	zanlwfhr@ms14.hinet...	sales@sharetech.com.tw	淫蕩熟女喜歡玩雙穴齊插！mcm...	1.9 KB	0	垃圾信	取回 加入黑名單 加入白名單

高效仓储管理与工厂物料配送

圖 10-17 垃圾郵件的通知信

郵件收件者可以點選右端的按鈕取回被誤判的垃圾郵件或是將這一封信的寄件者加入個人的黑白名單中，下次這個寄件者寄來的郵件就照使用者自己本身的黑白名單處理。在【隔離區】可以搜尋被判斷為垃圾郵件的郵件，搜尋的條件如下：

【收件日期】：垃圾郵件進入隔離區的時間，可以指定時間區間。

【寄件者 IP】：寄件者 IP 位址。

【寄件者】：是誰寄出垃圾郵件。

【郵件大小 KB】：垃圾郵件的檔案大小。

【收件者】：這一封垃圾郵件的收件者。

【垃圾郵件分數】：垃圾郵件分數的區間。

【病毒】：垃圾郵件是否含有病毒。

【郵件主旨】：垃圾郵件的主旨。

被 NG-UTM 判斷成垃圾郵件的郵件，如果管理者選擇放在刪除區，則郵件收件者不會收到這些垃圾郵件通知，只有管理者可以到隔離區中，當管理者在隔離區中搜尋到被誤判斷的郵件時，可以直接放行給原來郵件的收件者，在刪除區的收尋條件如下：

【收件日期】：垃圾郵件進入刪除區的時間，可以指定時間區間。

【寄件者 IP】：寄件者 IP 位址。

【寄件者】：是誰寄出垃圾郵件。

【郵件大小 KB】：垃圾郵件的檔案大小。

【收件者】：這一封垃圾郵件的收件者。

【垃圾郵件分數】：垃圾郵件分數的區間。

【病毒】：垃圾郵件是否含有病毒。

【郵件主旨】：垃圾郵件的主旨。

Client 垃圾信搜尋 Web 介面

以往郵件被垃圾郵件過濾到隔離區或是刪除區的信件，要重新取回需要管理者協助幫忙，就算有垃圾郵件清單的協助，萬一忘記或是想要查詢數天前的垃圾郵件，困擾管理人員跟使用者，NG-UTM 為了節省這一些維護上的困擾，允許使用者可自行透過 Web 介面，搜尋自己的郵件，只要在 NG-UTM 介面 IP 位址後面加上/spam.php，就可以登入個人的隔離區，搜尋並取回郵件。

例如，NG-UTM 管理介面位址為 http://192.168.1.1，則進入 Client 垃圾信搜尋介面需輸入 http://192.168.1.1/spam.php，登入後就可以。（圖 10-18）

- 【允許 Client 使用信件搜尋介面】：是否要讓使用者可以登入這個垃圾郵件搜尋系統，預設是關閉，啟用後需要設定使用者登入個人垃圾郵件搜尋系統的認證機制，通過認證後才可以進入。
- 【登入失敗次數超過多少暫時封鎖】：使用者登入垃圾郵件搜尋系統時，輸入帳號密碼失敗超過多少次，管理介面就會封鎖這個 IP 位址，這個功能是避免發生猜測帳號密碼的事情，預設為 0，0 代表不啟用這樣功能。
- 【多久解除被暫時封鎖的 IP】：當 IP 位址被封鎖後，隔多久才可以再登入，預設為 0，代表不封鎖所有的 IP 位址。
- 【解除 IP 封鎖】：當 IP 位址被封鎖後，會把 IP 位址列在這裡，管理者可以立刻的解除被封鎖的 IP 位址。

圖 10-18 使用者登入垃圾郵件搜尋設定

Client 信件搜尋 Web 介面，登入伺服器設定

因為 NG-UTM 本身沒有郵件伺服器的帳號密碼，所以使用者登入時需要一組帳號密碼，這一組帳號密碼可以跟原本的郵件伺服器整合，這樣不論使用者會是管理者，只要記住一組帳號就可以，在 NG-UTM 按下新增按鈕。（圖 10-19）

- 【網域】：原本郵件伺服器的網域名稱。
- 【伺服器位址】：郵件伺服器的 IP 位址。
- 【登入帳號附加網域】：是否要幫使用者自動添加網域名稱，減少使用者輸入的字串，例如，郵件帳號為 jean@abc.com，啟用這項功能後，使用者登入時只需要登入 jean 及密碼，如果這項功能是關閉，則輸入 jean@abc.com 及密碼。
- 【通訊服務】：用 POP3 或是 IMAP 通訊協定跟後端的郵件伺服器溝通。
- 【安全性】：在安全性上，NG-UTM 用哪一種協議跟後端的郵件伺服器溝通，共有三種選項不加密、TLS 跟 SSL ，預設值是不加密。
- 【通訊埠】：TCP 埠號，POP3 是 110，IMAP 是 143，如果選擇是 TLS / SSL，則是 POPS 是 995 跟 IMAPS 是 993，IMAP 的 TLS 也是使用 143，選擇不同的通訊協定他的 PORT 號就不一樣。
- 【憑證】：是否忽略憑證的警示，因為溝通時使用的 SSL 憑證都不是正常憑證機構簽發的憑證，所以會有警示訊息，建議忽略。
- 設定完成後可以按下連線測試按鈕驗證剛剛的設定值是否正常運作。

圖 10-19 Client 登入郵件伺服器認證

進入 Client 垃圾信搜尋 WEB 介面。(圖 10-20)

例如，NG-UTM 管理介面位址為 http://192.168.1.1，則進入 Client 垃圾信搜尋介面需輸入 http://192.168.1.1/spam.php ，此時輸入郵件伺服器的帳號跟密碼。

圖 10-20 進入使用者端垃圾信搜尋介面

登入後，使用者可藉由 NG-UTM 提供的搜尋條件(包含收件日期、寄件者 IP、方向、寄件者、郵件大小、收件者、垃圾郵件分數、病毒、郵件主旨)快速搜尋遭到誤判的垃圾郵件。

使用者亦可透過這裡的【個人設定】，建立個人黑、白名單帳號。並可針對黑名單帳號寄來的郵件再設定處理方式，包含在主旨加入文字後傳送給收件者或直接刪除兩種方式。（圖 10-21）

圖 10-21 新增個人帳號的黑名單及處理方式

10-3-2、垃圾郵件通知

定時地將隔離區的垃圾郵件郵寄清單給每個使用者，由使用者自行決定是不是垃圾郵件，減少郵件伺服器或是管理者的人為誤判。

管理者可以決定要不要啟動這項功能，如果不啟用，被歸類在隔離區的垃圾郵件就只能靠管理者幫使用者搜尋、下載。

啟動後，NG-UTM 就會在《傳送時間》的設定時間，寄發一封垃圾郵件通知信給使用者。

以一天為周期性的時間，每個小時為最小的單位，管理者可以彈性的設定傳送垃圾郵件清單的時間，例如，管理者可以設定 每天早上 8 點及中午 12 點，下午 5 點傳送清單。這樣不僅增加彈性，更能降低總體的垃圾郵件數量。

NG-UTM 寄送垃圾郵件清單的主旨，管理者可以輸入任何中英文，設定主旨的最主要目的就是讓使用者容易分辨正常信件跟垃圾郵件清單信件。

對於內部的特定帳號，他不想要收到任何的垃圾郵件清單，可以在這個地方，輸入完整的內部 e-mail 帳號，每一行為一筆帳號。

使用者垃圾郵件清單傳送設定

使用者垃圾郵件清單傳送設定，在建立垃圾郵件清單傳送之前需至『管理者』－『SMTP 伺服器設定』完成相關設定，讓 NG-UTM 能夠寄信給郵件伺服器的帳號。針對每一個使用者的垃圾郵件清單，可以新增的項目如下：（圖 10-22）

- 【使用者垃圾郵件清單傳送】：要不要開啟這項功能。
- 【傳送時間】：選取垃圾郵件清單傳送時間，1～24 小時每一個小時可以選一次，也可以按下【立即傳送】按鈕，將目前已經在隔離區的垃圾郵件，以清單的方式將它馬上寄出。
- 【垃圾郵件清單主旨】：設定郵件清單主旨，例如：垃圾郵件通知。

■ 【不接收垃圾郵件清單者】：郵件清單主旨設定不接收垃圾郵件清單者，每一行為一個帳號。需輸入完整的 e-mail，並以 Enter 鍵來換行區隔。也可以選擇【接收垃圾郵件清單者】，代表這一些帳戶才接收清單，其他的就不送出。

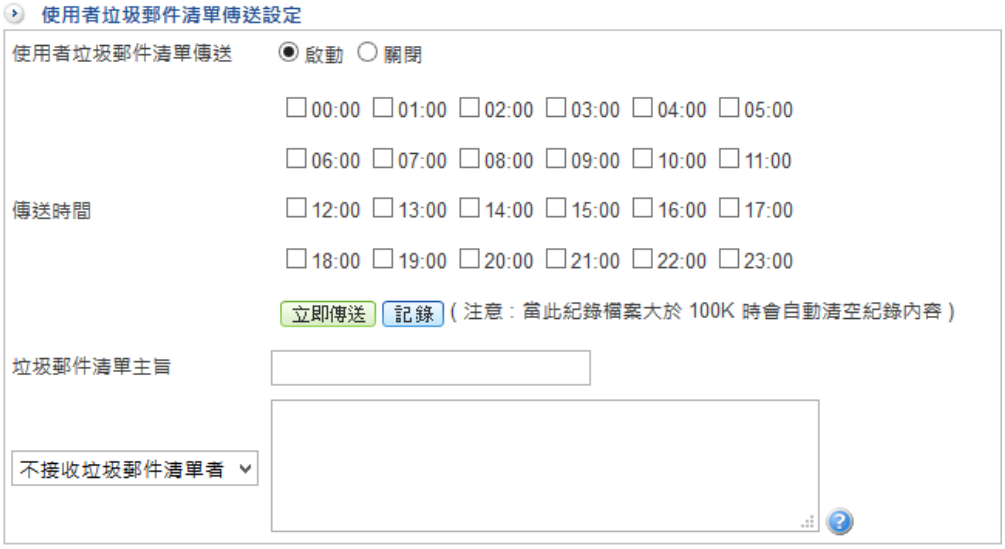


圖 10-22 使用者垃圾郵件清單傳送設定

註 1：使用者收到一封垃圾郵件清單，寄件者帳號為 root，這是由系統自動產生，但是寄件者的 IP 位址卻是管理者可以自行定義，通常會設為這台郵件伺服器的外部 IP 位址或是網域名稱（mail.yourdomain.com）。

註 2：【使用者垃圾郵件清單傳送】管理者可以決定要不要啟動這項功能，如果不啟用，被歸類在隔離區的垃圾郵件就只能靠管理者幫使用者搜尋、下載。啟動後，NG-UTM 就會在《傳送時間》的設定時間，寄發一封垃圾郵件通知信給使用者。

註 3：【傳送時間】如果帳號很多，而且每個帳號的在隔離區的垃圾郵件又特別多，它會導致在製作、寄發垃圾郵件清單時郵件伺服器的忙碌狀態，所以縮短清單寄發的時間，把負載平均分配。按【立即傳送】按鍵，會馬上傳送一份垃圾郵件清單至使用者的個人信箱。

註 4：【不接受垃圾郵件清單者】對於內部的特定帳號，他不想要收到任何的垃圾郵件清單，可以在這個地方，輸入完整的內部 e-mail 帳號，每一行為一筆帳號，當郵件伺服器在郵寄垃圾郵件清單時，就會將這些帳號排除在外。

管理者垃圾郵件清單傳送設定

管理者垃圾郵件清單傳送設定，在建立垃圾郵件清單傳送之前需至『管理者』－『SMTP 伺服器設定』完成相關設定，讓 NG-UTM 能夠寄信給郵件伺服器的帳號，管理者垃圾郵件清單傳送設定。

- 【管理者垃圾郵件清單傳送】：要不要開啟這項功能。
- 【傳送時間】：選取垃圾郵件清單傳送時間，1～24 小時每一個小時可以選一次，也可以按下【立即傳送】按鈕，將目前已經在隔離區的垃圾郵件，以清單的方式將它馬上寄出。
- 【垃圾郵件清單主旨】：設定郵件清單主旨，例如：垃圾郵件通知。
- 【接收垃圾郵件清單者】：郵件清單主旨設定接收垃圾郵件清單者，每一行為一個帳號。需輸入完整的 e-mail，並以 Enter 鍵來換行區隔，代表這一些帳戶才接收清單，其他的就不送出。

10-3-3、垃圾郵件自動學習

垃圾信的學習機制要不要啟動，啟動後郵件伺服器就會定時地在時間內，將黑名單學習帳號、白名單學習帳號的信件匯入垃圾信學習資料庫中，下次有同樣的郵件進來時，就會根據學習機制自動判斷。（圖 10-23）

- 【定時自動學習功能】：要不要開啟自動學習這項功能，預設是關閉。
- 【垃圾信多久學習一次】：預設是 12 個小時，設定範圍是 1～24 小時，也可以按【立即學習】按鍵，將黑名單學習帳號、白名單學習帳號的信件匯入垃圾信學習資料庫中
- 【黑名單學習】：所有寄到這個信箱的信件，資料庫會學習這封信的內容特徵，並且將這個寄件者、寄件者 IP 位址列入黑名單，而被歸類為黑名單，下次 NG-UTM 收到這個寄件者寄來的信會直接被歸類為垃圾信件。

  按下垃圾郵件的學習紀錄按鍵，會顯示黑名單學習帳號的信件匯入垃圾信學習資料庫中的所有學習紀錄，包含學習的總筆數、學習日期、從幾封信中學習到幾筆資料。

  提供匯入黑名單學習帳號檔，檔案大小上傳建議不要超過 64MB
- 【白名單學習】：所有寄到這個信箱的信件，資料庫會學習這封信的內容特徵，並且將這個寄件者、寄件者 IP 位址列入白名單，而被歸類為白名單，下次 NG-UTM 收到這個寄件者寄來的信就不會被歸類為垃圾信件。

  按下垃圾郵件的學習紀錄按鍵，會顯示白名單學習帳號的信件匯入垃圾信學習資料庫中的所有學習紀錄，包含學習的總筆數、學習日期、從幾封信中學習到幾筆資料。

  提供匯入黑名單學習帳號檔，檔案大小上傳建議不要超過 64MB
- 【清除垃圾信學習資料庫】：清空所有的學習紀錄，重頭開始。

■ 【安裝預設學習資料庫】：線上取得垃圾信學習資料庫的資料，這一台 NG-UTM 就不需要重新建立自己的學習資料庫。

圖 10-23 垃圾郵件自動學習

註 1：垃圾信的學習機制要不要啟動，啟動後郵件伺服器就會定時地在時間內，將黑名單學習帳號、白名單學習帳號的信件匯入垃圾信學習資料庫中，預設值是(啟動)。

註 2：【垃圾信多久學習一次】預設是 3 個小時，設定範圍是 1～24 小時，也可以按【立即學習】按鍵，將黑名單學習帳號、白名單學習帳號的信件匯入垃圾信學習資料庫中。

註 3：【學習紀錄】按下垃圾郵件的學習紀錄按鍵，會顯示黑名單學習帳號、白名單學習帳號的信件匯入垃圾信學習資料庫中的所有學習紀錄，包含學習的總筆數、學習日期、從幾封信中學習到幾筆資料。

10-3-4、個人黑白名單

個人黑白名單

NG-UTM 可以建立 2 種黑、白名單，個人跟系統，在優先權上，個人的黑白名單會比系統的黑白名單更優先，不論哪一種類型的黑白名單資料庫，建立完成後，管理者都可以匯出跟匯入這一些黑、白名單。（圖 10-24）

黑、白名單的組合是以文字檔的方式，一行一筆資料，以下列範例說明：

Ruser,Black,White

jean@abcd.com, “bbb@pp.com”,” ppp@ll.com”

jean@abcd.com,” ” ,ccc@ll.com

apple@abcd.com,” ooo@pp.com” ,” ”

第一行為保留字，資料是從第二行後開始計算，以上面 3 筆為例，帳號 jean@abcd.com 有 1 筆黑名單 bbb@pp.com 跟 2 筆白名單分別是 ppp@ll.com 跟 ccc@ll.com，帳號 apple@abcd.com 則只有一筆黑名單 ooo@pp.com，沒有白名單。管理者可以定期將個人黑白名單匯出，隨時建立備份準備。

並針對黑名單帳號寄來的郵件可以再設定處理方式，包含在主旨加入文字後傳送給收件者或直接刪除兩種方式，尤其是主旨加入文字，可以讓他跟系統的垃圾信判斷機制出現的文字不一樣，這樣使用者就知道這個判斷是根據哪一個基準。

每一個黑白名單建立完成後，管理者可以看到下列的資料，

個人黑白名單列表 注意，個人黑白名單的內容長度上限為 65535 個字元 1 / 1

註解	帳號	黑名單	白名單	黑名單處理方式	編輯 / 刪除
黑白	jean@abcd.com	po@pol.com	lk@def.com	垃圾郵件主旨提示文字	

圖 10-24 個人黑白名單列表

10-3-5、系統黑白名單

NG-UTM 的系統黑、白名單，又在細分成 2 個來源，分別是寄件者跟收件者的黑、白名單他的匯出及匯入規則跟個人的一樣，但是在寄件者的黑名單處理部分，又可更細分成下列 3 種。

1. 主旨加入文字後傳給收件者　垃圾郵件主旨提示文字，在這裡直接輸入要標示的文字，例如，黑名單資料庫。

2. 直接隔離，符合的寄件者郵件，立刻送入隔離區。

3. 直接刪除，符合的寄件者郵件，立刻送入刪除區。

系統的白名單部分，除了可以用帳號管理外，也可以列出 IP 位址，利用信任 IP 位址機制，將來自跟 IP 位址的郵件，通通列為白名單，不會再進入垃圾郵件過濾。

在收件者為基礎的白名單上，分成網域跟寄件者帳號，來自設定的網域或是郵件帳號通通會自動視為白名單，不會再進入垃圾郵件過濾機制。（圖 10-25）

圖 10-25 系統白名單網域及帳號

註 1：【黑名單】（ * @abcd.com ），所有從 abcd.com 網域寄出的信件統統被列入垃圾信件。（ spam@domain.com ）寄件者是 spam@domain.com 的信件從，統統被列入垃圾信件。所有從黑名單中寄給本機網域的信件，都會被列為垃圾信件，不管其信件內容為何，所以設定時要小心。

註 2：【白名單】（ * @xyz.com ）所有從 xyz.com 網域寄出的信件不會被列入垃圾信件。（ sales@domain.com ）寄件者是 slaes@domain.com 的信件從，不會被列入垃圾信件。

註 3：【信任的 IP 位址】被設定的信任 IP 位址寄出的寄件者，統統會被加入白名單中。192.168.100：代表 192.168.100.0/24 這個區段的寄件者 IP 所寄的信件，都不會被列入垃圾郵件。211.22.160.30：代表 211.22.160.30/32 這個寄件者 IP 所寄的信件，不會被列入垃圾郵件。

10-3-6、郵件內文過濾

一般的垃圾郵件都針對特徵值，NG-UTM 除了一般特徵值比對外，針對郵件內文中如果有惡意的網址，會跟自己的黑名單資料庫進行比對，當比對到後，管理者可以針對這類型的郵件進行處置。

比對資料來源有 3 個，分別是自訂的黑、白名單， URL 資料庫跟 Sandstorm 資料庫，自訂黑、白名單跟 URL 資料庫都只能比對郵件內文中是否有不正當的網址，Sandstorm 除了比對網址外還會比對夾帶的附件檔案，是否含有惡意的木馬程式。（圖 10-26）

圖 10-26 郵件內文比對設定

- 【更新時間】：內建惡意網址的資料庫最近的更新時間，按下【立即更新】就可以馬上更新。
- 【內文連結過濾機制】：管理者可自己決定要不要啟用這項功能。
- 【內文連結過濾自訂白名單】：自行輸入 URL 的白名單。
- 【內文連結過濾自訂黑名單】：自行輸入 URL 的黑名單。
- 【內文連結過濾項目】：共有 16 項 URL 資料庫，括弧內的是這個分類共有幾筆網址。
- 【內文連結過濾測試】：點選後系統會開啟新的頁面，輸入 URL 網址，確認是否存在系統的黑名單中。
- 【Sandstorm 服務】：在郵件內文比對中加入 Sandstorm 惡意木馬程式比對，在後面的【URL 測試】中可以輸入網址，比對是否已經在資料庫中。

- 【內文連結過濾處理方式】：比對到後，這一封郵件該如何處理，注意收信類型的郵件，只能增加分數而不能直接刪除或是放在隔離區。

  ◆直接刪除：把這一封信直接刪除。

  ◆轉到垃圾郵件隔離區：直接放在隔離區，也不下放給使用者。

  ◆增加垃圾郵件分數：增加垃圾郵件分數，再由垃圾郵件總分來區分如何處理。

10-4、郵件稽核

網路的快速發展，讓 e-mail 普遍使用於企業及各機關團體及學校中，然而藉由 e-mail 發生洩密案件卻層出不窮。這些多是對於 e-mail 不當的使用，除了可能造成商業資訊外洩外，嚴重的會影響企業商譽受損及內部士氣低落並造成網路頻寬之消耗造成員工生產力降低等困擾。

電子郵件在網路運用上所衍生安全性的漏洞為現今企業不容忽視的一環。眾至資訊提供網路及電子郵件稽核解決方法。可以針對企業聯外電子郵件，進行即時完整紀錄(包含外寄郵件)，同時提供高效率、警示、分析，產生管理稽核報表，可以讓企業快速導入，使主管迅速掌握企業員工電子郵件各種誤殺、濫用、洩密或者密件暗傳等使用行為。藉由有效的「管理」取得在「效率」、「安全」間的平衡點。

可將透過 NG-UTM，依其郵件特性做稽核的動作，有效控管郵件的進出。

10-4-1、稽核過濾設定

郵件稽核功能是 NG-UTM 跟其他的 UTM 不一樣的地方，針對通過 NG-UTM 的郵件進行內容的稽核過濾，並按照是先規畫的處理行為，處理郵件的下一個動作。

- 【過濾器名稱】：設定過濾器名稱，給這個郵件稽核過濾器的名稱。
- 【啟動】：點選啟動後，設定的過濾器功能才會生效，例如，可以將預先要作的過濾功能先設定好，但是不啟用，等到要執行時，將它啟用就可以。
- 【備註】：給予這個過濾器一個更詳細的說明，管理者不需要查看過濾器的內容，就可以瞭解這個過濾條件的功能為何？

過濾器條件

針對下列的郵件內容設定條件，以（AND）或是（OR）的邏輯來決定下面幾項過濾條件是不是全部要符合或是只要有一項符合就有效。標示【*】的條件可以輸入特殊定義字，【！】表示【非】的意思，【null】表示【沒有】，多個條件可以用【，】的符號隔開，它代表【OR】。

只輸入【null】字元，表示當信件沒有主旨文字時。在來源 IP 輸入【！192.168.1.】表示寄件者來源不是介於 192.168.1.0~192.168.1.255 之間。【反向】代表跟設定值相反的意義。如果過濾條件是空白，代表這項條件就不列入邏輯判斷的依據。

過濾器條件->組合條件為 AND

所有的條件都符合時，過濾器才會生效，並將此信件依照「處理方式」及「進階處理」的設定方式處理它，範例：

在過濾條件《寄件人包含》中設定【@yourdomain.com】，《郵件主旨包含》中設定【報價單】，這 2 項資料，其他都沒有輸入資料，它就代表 yourdomain.com 的任何一個帳號往外寄信時，只要信件的主旨有包含【報價單】這 3 個字，就符合過濾條件。

過濾器條件->組合條件為 OR

只需其中一個過濾條件的任何一個符合，過濾器就會將此信件依照「處理方式」及「進階處理」的設定處理它，範例：

在過濾條件《寄件人包含》中設定【@yourdomain.com】，《郵件主旨包含》中設定【報價單】，它就代表 yourdomain.com 的任何一個帳號寄信、收信，或是傳送、接收郵件的主旨有【報價單】這 3 個字，就符合過濾條件。

過濾器條件->反向

符合過濾條件的相反，例如，填入在寄件者包含的地方填入，jean@abcd.com，並選擇反向，代表只要是寄件者不是 jean@abcd.com 就符合條件。

- 【條件組合方式】：根據過濾條例特性選擇 AND / OR 的組合。
- 【寄件者包含】：設上要過濾的寄件者帳號就可以，這裡所指的寄件者不光是內部網域的互寄帳號，也包含外部郵箱寄給內部網域的信。其中外部郵箱代表是寄件者。範例，abc@google.com 寄給 sales@yourdomain.com ，abc@google.com 就是寄件者。
- 【收件者包含】：設上要過濾的收件者帳號就可以，這裡所指的收件者不光是內部網域的互寄帳號，內部網域寄給外部郵箱的信，其中外部郵箱就代表是收件者。範例，sales@yourdomain.com 寄給 abc@google.com，abc@google.com 就是收件者。
- 【寄件來源 IP 包含】：填入 IP 位址，所有從這些 IP 位址寄的信件都符合過濾器設定條件，這個地方也可以設上邏輯條件。範例，【192.168.1】 代表 192.168.1.0~192.168.1.255 的 IP 位址，【！192.168.2】 代表不屬於 192.168.2.0~192.168.2.255 的 IP 位址。
- 【郵件表頭包含】：填入要過濾的郵件表頭內容。
- 【郵件主旨包含】：填入要過濾的郵件主旨，例如（報價單），所有外寄、內送的郵件主旨出現這 3 個字就符合過濾規則，不論它原來的主旨是（新聞報價單據）或是（報價單單是一個笑話），都是符合的。
- 【郵件內容包含】：填入要過濾的郵件內容，例如（最新設計圖）字樣，如果內容有含這些文字就符合過濾器設定條件，郵件內容是郵件的本文，不包含郵件所夾帶的檔案，郵件夾帶檔案的內容無法用這個功能判斷，目前只能用整封信件的大小及郵件附件檔名作為判斷依據。
- 【郵件容量大於】：郵件容量大於多少 Bytes，包含所夾帶的檔案，就符合過濾器設定條件，通常郵件的容量大小是指整封信件的原始格式的大小。

- 【郵件附件檔名包含】：郵件附件檔名可以含有特定字元，例如，（報價單），也就是所有的信件，只要附帶檔案的檔案名稱有（報價單），就符合過濾器設定條件，不論是（2008 最新報價單.DOC）或是（報價單據.pdf）。

- 【個資過濾】：稽核機制可以更詳細的稽核郵件內容，只要是 DOC/PDF 類型的文件裡有特殊的關鍵字，就滿足過濾條件，目前可以過濾的資料，如：身分證字號、出生日期、電話號碼、行動電話號碼、信用卡卡號、電子郵件等，並設定權重，加總權重後讓管理者決定該如何處理這一封疑似洩漏個資的郵件。（圖 10-27）

圖 10-27 個資過濾

處理方式

符合過濾條件的郵件，要怎樣處理，管理者針對不同的過濾條件，可以設定不同的處置，例如，當寄件者是 jean@abcd.com 時，郵件直接刪除；當收件者是 jordan@abcd.com 時，把他的郵件抄送副本給 admin@abcd.com。（圖 10-28）

- 【垃圾郵件過濾】：符合過濾條件的郵件，在垃圾過濾動作上共有 2 個選項，增減垃圾郵件分數跟不做垃圾信過濾

增減垃圾郵件分數

NG-UTM 提供貝氏過濾法將信件之內文以貝氏資料庫之規則來評分，分數越高者其越有可能是垃圾信件。一般來說「貝氏過濾法」會有個資料庫，當一封信件進入系統的時候會把信件分解成單詞，比對目前「貝氏過濾法資料庫」，分析以往的經驗，來判別此封信件為垃圾信件的機率，且貝氏過濾資料庫具有自動學習的功能，可以依照不同企業收信的狀態來調整最適合的過濾條件。但是針對特定字眼、主旨，企業可能要增加其垃圾郵件分數，可在處理方式做郵件。

分數的增減。例如：針對「色情」要增加其過濾分數 50 分，可直接輸入 50。如要降低過濾分數 50 分則輸入「-50」即可。

不做垃圾信過濾

對於內部網域的特定收件者，不希望郵件伺服器幫他作垃圾郵件、病毒信件的過濾，可以在【收件者包含】中填入特定帳號，NG-UTM 就不會進行垃圾信過濾機制。

- 【直接隔離】：依過濾器所定條件，公司對於機密性的資料總是害怕員工會藉由 email 傳到外部，如果沒有一個妥善的郵件管理工具，那麼這些機密性的文件就不具有安全性。

  因此，管理者可以在過濾條件設定所列管標題、文字內容，例如：「報價單」，則內部使用者寄送到外部，只要有涵蓋報價單的內容都會直接隔離。寄信者不會收到隔離的清單，只有管理者透由稽核過濾隔離區掌握這些直接隔離的信件。

- 【直接刪除】：對於符合過濾條件的郵件，直接刪除，無法將郵件送達最終的收件者，郵件將進入「進階處理」的程序。

- 【IP 封鎖】：直接封鎖寄件者 IP 位址。

- 【移除符合條件的附件】：凡是符合上述過濾條件，勾選「移除符合條件的附件」，則系統會自動刪除其附件檔。
- 【抄送副本】：針對符合過濾條件的信件，將這封信轉寄給特定的收件者，不論是外部寄給內部、內部互寄、內部寄給外部的所有信件，統統會轉寄，連同夾帶的檔案也會一併轉寄。
- 【通知功能】：跟「抄送副本」不一樣，符合過濾條件的信件，這個選項只會主動寄一封事先設定好主旨的通知信，給特定的收件者，至於符合過濾條件的信件內容、夾帶檔案，並不會轉寄給設定的帳號，管理者可以在這裡設定通知信的主旨、通知信的收件者或者要不要通知原來的寄件者。
- 【停止處理更多規則】：「停止處理更多規則」，並不是真得不做任何動作，因為郵件伺服器的過濾器是依照順序向下執行，例如，設有 10 條規則，在沒有【停止處理更多規則】下，每一個郵件都會經過 10 個過濾規則，如果的 5 條符合過濾規則且有選擇【停止處理更多規則】，則這一封郵件只會比對 5 個過濾規則。

圖 10-28 過濾處理方式

如果稽核過濾條件筆數過多，也可以利用整批快速匯入方式，以 csv 檔建立，匯入名稱依序為 serial_id、filter_title、match_header、match_sender、match_receiver、match_sender_ip、match_subject、match_body、match_attachment_name、action_to_carbon_copy、note、advise_subject、advise_receiver、audit_auditor、audit_agent、audit_subject、action_to_separate、is_need_all_conditions_hold、is_sender_match_local_domain、is_receiver_match_local_domain、is_check_fake_sender、 size_over、action_to_delete、action_to_ignore_spam、action_to_adjust_spam_score、action_to_ip_block、action_to_remove_attachment、is_ignore_other_filter、is_not_match_sender、is_not_match_receiver、is_not_match_header、is_not_match_subject、is_not_match_body、is_not_match_sender_ip、is_not_match_attachment_name、advise_sender、action_to_audit、is_need_all_receiver_hold、is_need_all_subject_hold、is_need_all_body_hold、is_need_all_attachment_name_hold

10-4-2、稽核進階設定

稽核進階設定是針對稽核過濾設定中的 IP 封鎖機制，提供管理者更詳細的阻擋設定，在稽核過濾設定中的過濾條件觸發且管理者選擇 IP 封鎖這個處理動作，NG-UTM 才會執行封鎖，管理者可以在這裡設定例外 IP 位址、例外寄件者跟執行解封鎖。

IP 封鎖設定

- 【每次阻隔時間(秒)】：符合過濾條件的郵件，且處理動作是執行 IP 封鎖，NG-UTM 會把這一個 IP 位址列入黑名單中，拒絕他的連線，預設值是 600 秒。
- 【永久阻隔次數】：當觸發阻擋次數超過設定值時，則會這個 IP 位址將會被 NG-UTM 永久拒絕連線，預設值是 3 次。
- 【IP 例外清單】：輸入不會被拒絕連線的 IP 位址，就是稽核過濾的白名單 IP 位址，一行一組設定，IPV4/IPV6 皆可以，格式如下：

  10.1.1.0/16

  fe80::1e6f:65ff:fe28:9d47/64

- 【寄件者例外清單】：輸入不會被稽核過濾拒絕的寄件者帳號，就是稽核過濾的白名單寄件者帳號，一行一組設定，格式如下：

  jean@abcd.com

  pol@defg.com

- 【解除 IP 封鎖】：當 IP 位址被拒絕連線時，管理者可以在這個地方將這個 IP 位址解除封鎖。
- 【IP 封鎖記錄】：每個被稽核過濾機制封鎖的紀錄，不論是 IP 位址或是寄件者帳號，都會記錄在這裡，包含出發的時間跟事件，當此紀錄檔案大於 100K 時會自動清空紀錄內容。

10-4-3、稽核過濾隔離區

任何經過 NG-UTM 的稽核過濾的郵件，只要被隔離機制觸發的事件，都可以在稽核過濾隔離區中查詢，管理者可以依照郵件的時間、寄件者、收件者、主旨甚至過濾器名稱等資料查詢。

10-5、郵件紀錄查詢

NG-UTM 可將所有經過它傳送、接收的信件，統統紀錄起來，紀錄的郵件包含內容、附檔等，被紀錄下來的郵件會放在本機的硬碟中，管理者進入郵件查詢系統後，根據搜尋的條件找到目標郵件後，可以再放行給郵件收件者或是把它下載到管理者的電腦中。

除了搜尋郵件的功能外，萬一郵件是被 NG-UTM 本身的防禦機制，例如，垃圾郵件過濾、病毒跟稽核過濾等阻擋，這裡也可以找到被哪一種機制阻擋掉。

NG-UTM 會把所有被紀錄的信件在這裡列出來，方便管理者查詢，信件的進出及紀錄，郵件管理者並且有權限針對此封郵件執行放行、下載等工作。

10-5-1、今日郵件列表

NG-UTM 會把今天進出的郵件列表出來，按照時間排序，讓管理者查看，列表項目的詳細說明如下：（圖 10-29）

圖 10-29 紀錄郵件列表

- 【日期】：郵件進入 NG-UTM 的日期及時間。
- 【寄件者 IP】：寄件者的 IP 位址。
- 【收件者 IP】：收件者的 IP 位址。
- 【方向】：郵件進出方向，總共有 3 個方向，：【外部進入內部郵件伺服器(近端)】、：【內部到外部郵件伺服器寄信(遠端)】、：【內部到外部郵件伺服器收信】。
- 【寄件者】：寄件者的郵件帳號。
- 【收件者】：郵件的收件者帳號。
- 【主旨】：此封郵件的主旨。
- 【郵件大小】：郵件的大小容量。

- 【遞送狀態】：傳送是否成功還是被對方的郵件伺服器拒絕，共有成功、拒絕、接受、失敗跟加密 5 種。
- 【病毒】：郵件是否含有病毒。
- 【分數】：郵件被垃圾郵件過濾機制判斷的分數。
- 【處理】：垃圾郵件的處理方式是【主旨加入文字】、【隔離區】或是【刪除區】，正常郵件則會是空白。
- 【 】：此封郵件是否有包含附件。
- 【詳細】：此封郵件在 NG-UTM 的郵件處理程序的詳細資料，例如，垃圾信的過濾、病毒信過濾、稽核過濾器的處理方式等。（圖 10-30）

郵件

收件日期	2016-03-01 10:20:00
寄件者	abcd@test.com.tw
郵件主旨	稻盛和夫《成功的要義》：持續不斷抱持著「無論如何都要成功」的強烈意念，就能邁向成功之路。
大小(位元組)	9
病毒	
SPAM	8.2分 (隔離)
記錄	-

收件者

過濾器(抄送副本)	收件者	狀態	使用者清單通知	處理方式	執行者	處理日期
	aaa@aaa.com.tw	正常				

圖 10-30 郵件的詳細處理過程

- 【下載】：此封郵件是否曾經被管理者下載到管理者的電腦中。
- 【放行】：將此封郵件是否曾經被管理者放行給收件者。
- 【郵件】：是否要將此封郵件的寄件者加入系統的白名單中。

處理行為

管理者可以點選列表中的幾封或這是全部郵件，執行下列的動作。

- 【下載】：將選擇的郵件下載到管理者的電腦中。
- 【刪除】：將選擇的郵件從 NG-UTM 的紀錄中刪除。
- 【放行】：將此封郵件放行給收件者，所以使用者將會再收到同樣的郵件。
- 【加入系統白名單】：將選擇郵件的寄件者加入系統的白名單，下次就不會被判斷成垃圾郵件。
- 【加入黑名單學習】：將選擇郵件的寄件者加入系統的黑名單，下次直接拒絕，會被判斷成垃圾郵件。
- 【匯出】：將選擇的郵件紀錄匯出到管理者的電腦中。

10-5-2、郵件紀錄查詢

在「郵件紀錄查詢」功能中，管理者可以搜尋過 UTM 設備的所有郵件，不論是內部寄出還是外面寄進來的郵件，搜尋條件詳細說明如下。（圖 10-31）

- 【收件日期】：填入要查詢的日期區間。
- 【資料來源】：選擇本機資料還是已經備份到外面儲存媒體中的資料。
- 【寄件者 IP】：寄件者的 IP 位址。
- 【收件者 IP】：收件者的 IP 位址。
- 【傳遞方向】：可選定內對外寄信、內對外收信或外對內。
- 【寄件者】：寄件者的電子郵件帳號。
- 【郵件大小 KB】：郵件的檔案大小，可以設定郵件大小的區間條件。
- 【收件者】：這一封郵件的收件者。
- 【垃圾郵件處理方式】：信件是屬於正常信件或是垃圾郵件，有沒有被隔離。
- 【垃圾郵件分數】：垃圾郵件被判斷的分數，可以設定分數的區間條件。
- 【病毒】：垃圾郵件是否含有病毒。
- 【過濾器】：是否有啟動過濾器功能。
- 【遞送狀態】：郵件的傳遞情況，共有成功、拒絕、接受、失敗跟加密 5 種選項。
- 【郵件主旨】：郵件的主旨文字。

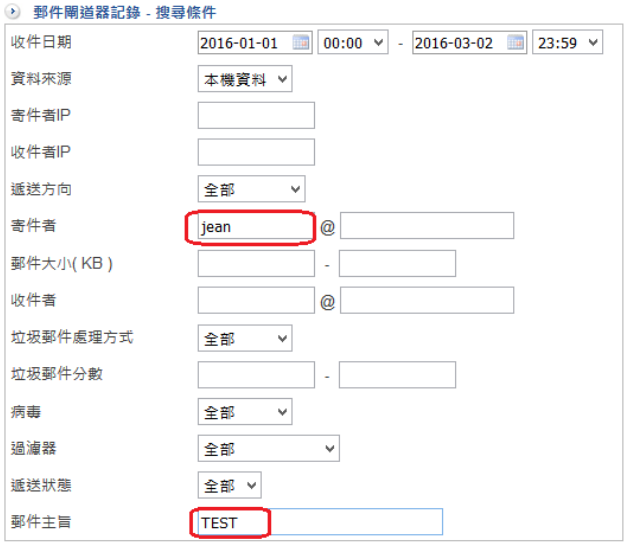


圖 10-31 搜尋郵件

10-6、SMTP 通聯記錄查詢

在「SMTP 通聯記錄查詢」功能，管理者可以搜尋每一封信詳細的 SMTP 通聯記錄，藉以判斷寄信不成功時的依據。（圖 10-32）

- 【收件日期】：填入要查詢的日期區間。
- 【寄件者】：寄件者的電子郵件帳號。
- 【郵件大小 KB】：郵件的檔案大小，可以設定郵件大小的區間條件。
- 【收件者】：這一封郵件的收件者。
- 【傳送狀態】：共有成功、拒絕、接受、失敗跟加密 5 種。

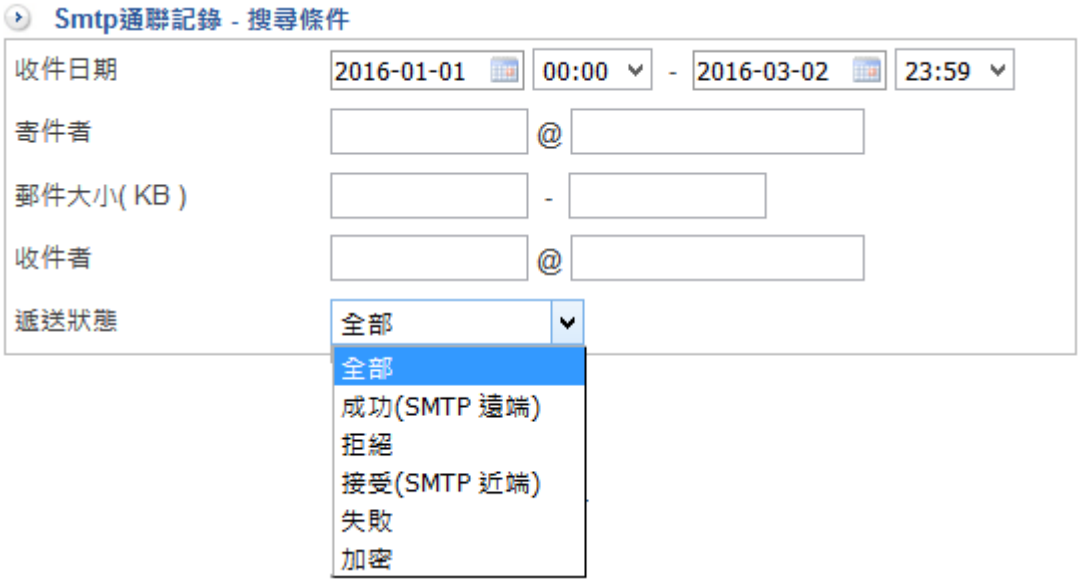


圖 10-32 搜尋郵件

簡單版 SMTP 紀錄

NG-UTM 預設的紀錄類型就是簡單版的 SMTP 記錄，搜尋後的列表如下，會把無法傳送的原因列在傳送訊息中，這是簡單版的 SMTP 紀錄，只是出現最後無法通聯的原因。（圖 10-33）

- 【傳送訊息】：顯示傳送不成功的原因。

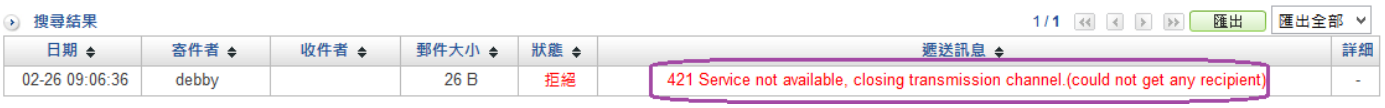


圖 10-33 搜尋郵件

詳細版 SMTP 紀錄

如果在 【郵件管理】>【郵件過濾與紀錄】>【SMTP 記錄設定】>【紀錄類型】選擇是詳細，則 NG-UTM 會在列表的【詳細】中讓管理者點選，一封郵件 SMTP 的通聯範例如下：（圖 10-34）

SMTP 連線詳細紀錄

日期	2012-03-02 12:01:49
寄件者	rookieswu@sharetech.com.tw
收件者	01@maxmax10.dyndns.org
大小(位元組)	0
傳遞狀態	拒絕
回應訊息	554 <01@maxmax10.dyndns.org>: Relay access denied

通訊過程

```
(01:49) > 220 ESMTP MAIL Server (SMTP PROXY)
(01:49) < EHLO scan.sharetech.com.tw
(01:49) > 250-smtp.passthru
(01:49) > 250-SIZE 5120000
(01:49) > 250-VRFY
(01:49) > 250-ETRN
(01:49) > 250-AUTH LOGIN PLAIN
(01:49) > 250 8BITMIME
```

圖 10-34 詳細的 SMTP 紀錄

第 11 章 內容記錄

NG-UTM 可記錄 Web 的通聯記錄，不論是 http 或是 https 協定，都會被詳細的紀錄下來，連掃毒過程也會被記錄下來。

11-1-1、今日 WEB 紀錄

NG-UTM 會自動將通過設備的 WEB 上網紀錄，包含時間、網址等紀錄下來，管理者只需要點選被紀錄下來的網址列，就會開啟新視窗，顯示使用者當時瀏覽的網頁內容。被紀錄的網址列表如下：（圖 11-1）

- 【排名】：按照傳輸的總流量，總流量是 HTTP 跟 HTTPS 的加總。
- 【電腦名稱】：該部電腦的電腦名稱。
- 【IP 位址】：被紀錄電腦的 IP 位址。
- 【MAC 位址】：被紀錄電腦的 MAC 位址。
- 【流量】：http 協定的流量。
- 【匯出】：把 http 協定的資料匯出。

點選【IP 位址】後，會出現更完整的訊息，它是以『筆數』為排序依據，紀錄哪一個網站的開始瀏覽時間及最後離開的時間。

- 【網站】：瀏覽的網站名稱。
- 【筆數】：這個網站總共被紀錄幾個有效的網址。
- 【開始時間】：這個網站開始瀏覽的時間。
- 【截止時間】：這個網站結束瀏覽的時間。

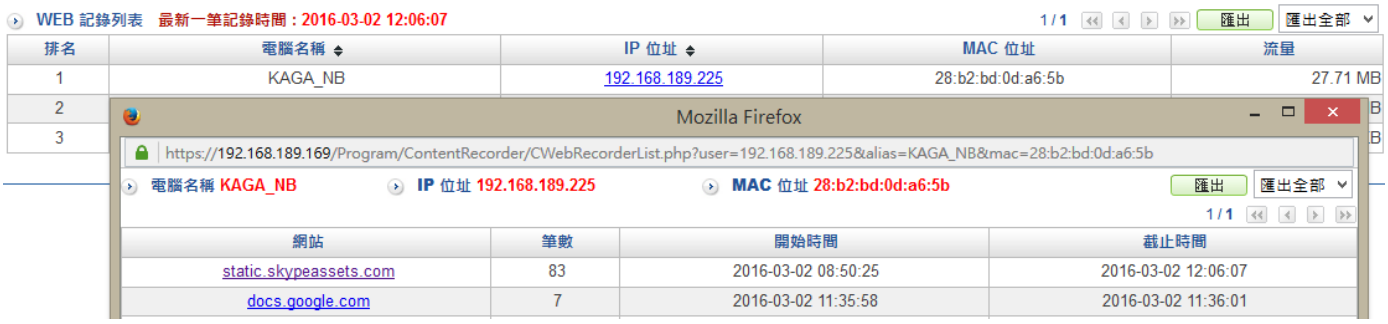


圖 11-1 瀏覽網站列表

點選【網站】後會出現這個網站被紀錄幾個有效的網址列表。（圖 11-2）

- 【時間】：點選這個網址的時間。
- 【網址】：實際的 URL 的網址。
- 【掃毒狀態】：如果有啟動 WEB/FTP 掃毒，它會紀錄這個網址是否有病毒，『OK』代表網址沒有毒。
- 點選網址後會開啟新視窗，顯示當時使用者正在瀏覽的網頁資訊。

電腦名稱 KAGA_NB　IP 位址 192.168.189.225　MAC 位址 28:b2:bd:0d:a6:5b　上一頁

網站 docs.google.com　1 / 1　匯出　匯出全部

時間	網址	掃毒狀態
2016-03-02 11:36:01	https://drive.google.com/doclist/offline/cacheupdater?delete_cache=0	--
2016-03-02 11:36:01	https://docs.google.com/offline/cacheupdate?ouid=uccce3d759691dfca	--
2016-03-02 11:36:00	https://docs.google.com/offline/cacheupdate?ouid=uccce3d759691dfca	--
2016-03-02 11:36:00	https://docs.google.com/offline/cacheupdate?ouid=uccce3d759691dfca	--
2016-03-02 11:36:00	https://docs.google.com/offline/cacheupdate?ouid=uccce3d759691dfca	--
2016-03-02 11:36:00	https://docs.google.com/offline/cacheupdate?ouid=uccce3d759691dfca	--

圖 11-2 瀏覽網址及詳細資料

11-1-2、WEB 紀錄查詢

可依照日期、電腦名稱、IP 位址等特徵，來尋找儲存在 NG-UTM 內所有符合條件之紀錄。（圖 11-3）

- 【日期】：設定搜尋指定時間區間內的紀錄。
- 【電腦名稱】：以【電腦名稱】選定使用者。
- 【IP 位址】：以【IP 位址】選定使用者。
- 【Web 紀錄保留】：WEB 紀錄要保留多久，按下【搜尋】鈕。

WEB 記錄 - 搜尋條件

日期　2016-03-02　00:00　-　2016-03-02　23:59

電腦名稱

IP 位址

網址搜索　Ex. facebook

圖 11-3 搜尋特定記錄之畫面

- 列出所有 WEB 紀錄查詢的結果。（圖 11-4）
- 如前面操作，點選 IP 位址、網站名稱或是網址，就會出現瀏覽的網頁。

搜尋結果　1 / 1　匯出　匯出全部

排名	電腦名稱	IP 位址	MAC 位址	流量
1	KAGA_NB	192.168.189.225	28:b2:bd:0d:a6:5b	46.87 MB
2	192.168.189.64	192.168.189.64	00:0c:29:31:9f:11	37.60 MB
3	TEST-VTU54QYLNS	192.168.189.229	00:0c:29:17:d5:f3	2.85 MB

圖 11-4 搜尋結果列表

11-1-3、WEB 病毒紀錄及查詢

NG-UTM 具有掃描 http/https 的病毒能力，搭配內建的 ClamAV 或是選購 Kaspersky 掃毒引擎，把有問題或是藏病毒的網頁通通過濾掉，這裡就會顯示被 NG-UTM 找到的病毒列表。（圖 11-5）

1 / 3　跳至 1 頁數、每頁 16 筆 GO　匯出　匯出全部

時間	電腦名稱	IP 位址	網址	掃毒狀態
2016-03-02 12:00:20	192.168.189.64	192.168.189.64	https://secure.eicar.org/eicar.com	EICAR-Test-File FOUND
2016-03-02 11:59:57	192.168.189.64	192.168.189.64	https://secure.eicar.org/eicar.com	EICAR-Test-File FOUND
2016-03-02 11:59:47	192.168.189.64	192.168.189.64	https://secure.eicar.org/eicar.com	EICAR-Test-File FOUND
2016-03-02 11:56:57	192.168.189.64	192.168.189.64	https://secure.eicar.org/eicar.com	EICAR-Test-File FOUND
2016-03-02 11:55:07	192.168.189.64	192.168.189.64	https://secure.eicar.org/eicar.com	EICAR-Test-File FOUND
2016-03-02 11:37:02	TEST-VTU54QYLNS	192.168.189.229	https://secure.eicar.org/eicar.com	EICAR-Test-File FOUND

圖 11-5 病毒列表

第 12 章 VPN

NG-UTM 可以用 VPN 方式建立安全的網路連接，以整合企業的各個遠地網路與全球外勤人員遠地個人電腦，提供公司企業與遠端使用者一個安全便利的網路加密方式，讓企業在網際網路上傳遞資料時，得到最佳的效能及保密效果。

在實務上每一種 VPN

NG-UTM 支援 3 種 VPN 協定，分別是 IPSec、PPTP 跟 SSL VPN，每種他的屬性跟定位不太一樣，IPSec 強調在 Tunnel 部分，PPTP 跟 SSL VPN 最主要是讓外部的使用者利用網際網路安全地連入內部網路。廣義來說，在主選單網路設定中 IP Tunnel 也是一種 VPN 連線模式，他也可以選用 IPSec 的加密模式，但是他有一點是屬於 Tunnel 性質，所以把他歸類到虛擬介面中。

VPN 種類說明如下：

1、IPSec VPN Tunnel：系統管理者可以利用 IPSec 協定，建立 Site to Site 的 VPN 通道，通道 2 端的溝通資料，都會以 DES、3DES、AES 的加密方式，無法讓其他人就算攔截通道的封包也無法順利解出其中傳遞的內容。

2、PPTP 伺服器：管理者可於此單元建立 PPTP 的撥接帳號，讓外部的使用者可以使用 NG-UTM 內部的資源。

3、SSL VPN 伺服器：管理者可於此單元建立 SSL VPN 的撥接帳號，讓外部的使用者可以使用 NG-UTM 內部的資源。

如何管理 VPN 通聯

建立虛擬私有網路驗證 Virtual Private Network (VPN)，需先在 IPSec VPN 中建立 Tunnel、PPTP 伺服器跟 SSLVPN 伺服器建立帳號，如果要管理這一些外點，IPSec VPN 在主選單的管制條例中 IPSec 管制建立管理規則，PPTP 跟 SSL VPN 則在主選單的管制條例中管制規則中實現 。

12-1、IPSec Tunnel

建立一條 IPsec VPN Tunnel 需要 2 端的設定都一致才有辦法連線成功，每一個連線需要設定的資訊說明如下：

IPSec 通道設定

- 【啟動 】：這一條 IPSec Tunnel 目前的狀態是啟用還是暫停中。（圖 12-1）
- 【VPN 通道名稱 】：IPSec VPN Tunnel 的名稱，此名稱可以是任何中英文文字，方便管理者辨識。
- 【本地 IP 位址 】：哪一個 IP 位址或是網域要接受 IPSec VPN Tunnel 的封包，通常指的是外部網路的 IP 位址。
- 【遠端 IP 位址 】：遠端 IPSec VPN Tunnel 的 IP 位址或是網域名稱，如果不知道遠端的這一些資訊，就使用動態 IP 位址，如果有多條 IPSec VPN 通道的外部 IP 都是動態，要注意他們的 Preshare Key 都要一樣。
- 【啟用備援 】：這一條 IPSec VPN Tunnel 要不要啟動備援服務。

  萬一主要的 IPSec VPN Tunnel 斷線時，會自動啟用備援線路的 Tunnel，確保所有的服務不中斷，當勾選備援設定時就進入設定畫面。
- 【斷線多就切換 】：當主要的 IPSec VPN Tunnel 斷線多久後切換到備援線路，預設值是 5 分鐘。
- 【備援本地 IP 位址 】：哪一個 IP 位址或是網域要當備援線路，接受 IPSec VPN Tunnel 的封包。
- 【備援遠端 IP 位址 】：備援線路的遠端 IPSec VPN Tunnel 的 IP 位址或是網域名稱，如果不知道遠端的這一些資訊，就使用動態 IP 位址。

圖 12-1 建立 IPSec VPN 通道

IPSec VPN 互連的網段

一般來說，IPsec VPN 通道相連的 2 端是不同的內網區段，且通常是連續，例如，192.168.1.0/24 到 192.168.2.0/24。如果 2 端有不連續的網段，要互連，可以按下 ，增加互連的網段，例如，A 點是 192.168.1.0/24 跟 172.16.1.0/24 要到 B 點 192.168.2.0 跟 172.16.2.0/24 ，他們都要利用相同的 IPSec VPN 通道。（圖 12-2）

- 【多通道模式 】：啟用多通道模式，
- 【本地端網路 】： 本地端的那一個網段要跟對方網段要利用 IPSec VPN 通道互連，例如，192.168.1.0/24，按下 就可以再追加新的網段 。
- 【遠端網路 】：IPSec VPN 通道的遠端網段，例如 192.168.61.0/24，按下 就可以再追加新的網段。

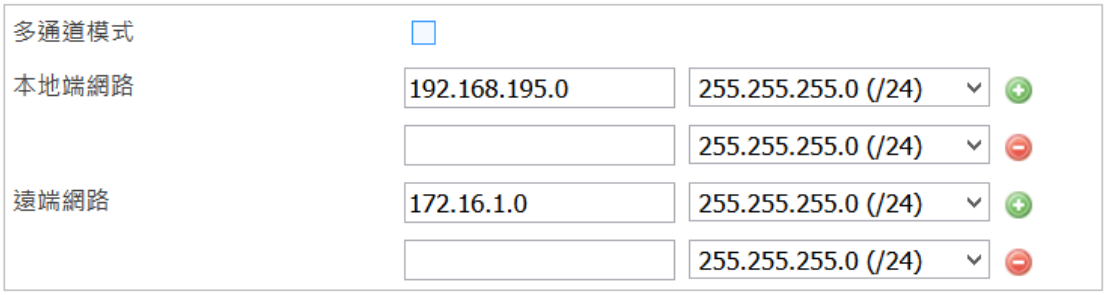


圖 12-2 IPSec VPN 通道內部網段

多通道模式

多通道運作模式就是把相連 2 個內部網段的封包，分配到 2 條以上的 IPSec VPN 通道中，達到類似線路負載平衡的機制，不過這一個運作有一個前提，管理者要輸入雙方的通道 ID，一般的通道 ID 是在外部網路 IP 位址前加入 @，例如，@1.1.1.1 或是@vpn.dyndns.org。

- 【本地端 ID 】： 使用 IPSec VPN 通道的本地端外部網路 IP 位址，前面加@，例如，@1.1.1.1 。
- 【遠端 ID 】：使用 IPSec VPN 通道的遠端外部網路 IP 位址，前面加@，例如，@vpn.abc.org。

本地端網路		遠端網路		本地端 ID (域名)	遠端 ID (域名)	
192.168.1.0	255.255.255.0 (/24)	192.168.2.0	255.255.255.0 (/24)	@1.1.1.1	@vpn.abc.org	
192.168.1.0	255.255.255.0 (/24)	192.168.2.0	255.255.255.0 (/24)	@2.2.2.2	@ppp.abc.org	
	255.255.255.0 (/24)		255.255.255.0 (/24)	@	@	
	255.255.255.0 (/24)		255.255.255.0 (/24)	@	@	

圖 12-3 IPSec VPN 多通道

IPSec 通道加密資訊

共有 2 個區塊，一個是 IKE (Phase I)，另一個是 IPSec 設定。（圖 12-4）

IPSec Phase 1 設定

- 【IKE】：有 2 種可以選 V1 或是 V2，IKE V2 是新的協議，設定前要注意，2 端的 IKE 要一致。
- 【連線模式 】：有 2 種模式可以選擇，一個是主要模式(main mode)，另一個是野蠻模式(aggressive mode)，通常是選用主要模式，用野蠻模式下，所有的 VPN 通道都會共用一組 Preshare Key 。
- 【Preshare Key 】：IPSec VPN Tunnel 建立時，雙方進行連線時用來進行 IPSec 加密用的金鑰。
- 【ISAKMP 演算法 】：「IP Security Association Key Management Protocol」(ISAKMP) 就是提供一種方法供兩個設備建立安全性關聯 (SA)。

SA 的說明

SA(Security Association) 對兩台電腦之間進行連線編碼，指定使用哪些演算法和什麼樣的金鑰長度或實際加密金鑰。事實上 SA 不止一個連線方式：從兩台電腦 ISAKMP SA 作為起點，必須指定使用何種加密演算法 (DES、triple DES、AES)、使用何種封包驗證 MD5 或是 SHA1。

DES/3DES 的說明

3DES 提供比 DES(加密金鑰爲 56 位元)，更加安全的三重資料加密標準(Triple Data Encryption Standard,3DES) 安全加密金鑰方法，使用的加密金鑰爲 168 位元

AES 的說明

為高階加密模式其標準比 DES 的加密標準更加嚴謹，DES 加密金鑰長度為 56 位元，AES 加密金鑰長度則高達 128 位元、192 位元、以及 256 位元。

MD5 的說明

一種單向字串雜湊演算，其演算方式是將你給予任何長度字串， 使用 MD5 雜湊演算法，可以計算出一個長度為 128 位元的演算。

SHA 的說明

是用於產生訊息摘要或雜湊的演算法，原有的 SHA 演算法已被改良式的 SHA1 演算法取代，可以計算出 160 位元的演算。

- 【本地 ID】：預設會自動帶本地端的 IP 位址當作 ID，管理者也可以輸入一組域名當作本地端 ID，系統會自動在前端加入@符號，送到遠端，例如，@1.1.1.1 或是 @ghi.com，設定時一定要注意，2 端的資料一定要互相對稱。
- 【遠端 ID】：預設會自動認為遠端的 ID 是連線的 IP 位址，管理者輸入一組域名當作遠端 ID，系統會自動在前端去除@符號，認為是遠端送來本地端的 ID，例如，@2.2.2.2 或是@def.com，設定時一定要注意，2 端的資料一定要互相對稱。
- 【IKE SA 生存時間】：根據 ISAKMP 演算法計算出的 SA，他的有效時間，超過這個時間，系統會自動在產生另一個 SA，取代前面的，預設是 3 小時，最長可以設定 24 小時。

IPSec Phase 2 設定

- 【IPSec 演算法】：指定使用何種加密演算法 (DES、triple DES、AES)、使用何種封包驗證 MD5 或是 SHA1。
- 【Perfect Forward Secrecy (PFS)】：指定使用何種加密演算法 (DES、triple DES、AES)、使用何種封包驗證 MD5 或是 SHA1。
- 【IPSec SA 生存時間】：根據 IPSec 演算法計算出的 SA，他的有效時間，超過這個時間，系統會自動在產生另一個 SA，取代前面的，預設是 3 小時，最長可以設定 24 小時。

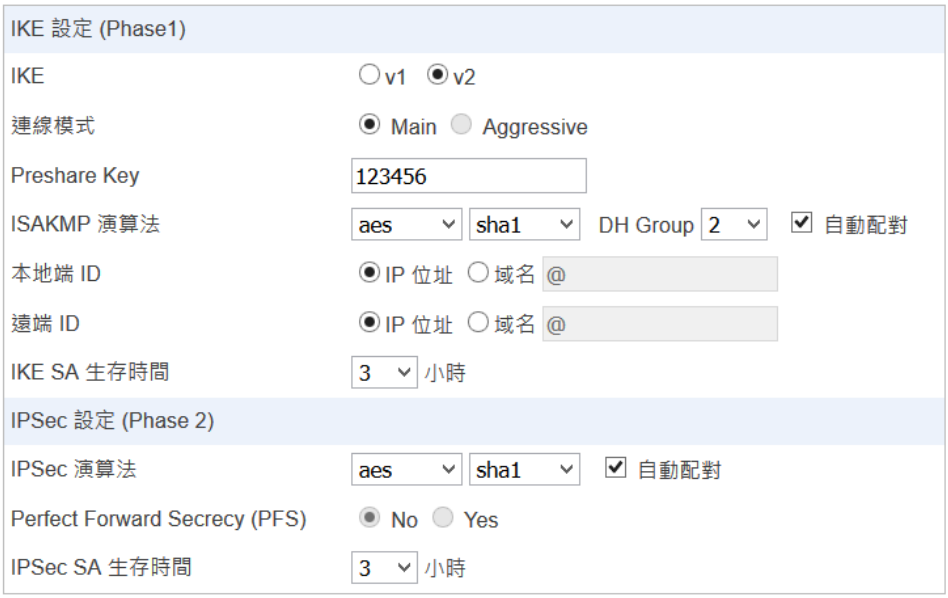


圖 12-4 IPSec VPN 通道加密

IPSec 其他設定（圖 12-5）

- 【Dead Peer Detection】：DPD 是一種自動偵測 VPN 斷線機制的標準協定，可自動判別 VPN 另一方的 IPSec 通道是否正常運作中，判斷有 IPSec 通道有問題時，針對這條 VPN 通道可以做下列 3 個動作，Hold、Clear、Restart，Hold 就是繼續等待，Clear 則是把相關的資訊清除掉等待重新連線，Restart 則是直接將 VPN 重新連線。

- 【關閉網路芳鄰】：建立 IPSec VPN 通道後可以讓 2 方的網段利用網路芳鄰協定查詢電腦名稱，預設是啟用，也就是允許網路芳鄰的封包通過 VPN 通道到另外一端，管理者可以把它關閉。

圖 12-5 IPSec VPN 通道其他設定

範例：兩台 NG-UTM 建立的 IPSec VPN 連線，存取特定網段的資源

甲公司　**WAN IP 為 61.11.11.11，LAN IP 為 192.168.188.0/24**

乙公司　**WAN IP 為 211.22.22.22，LAN IP 為 192.168.200.0/24**

IPSec VPN Tunnel 連線環境架構圖（圖 12-6）

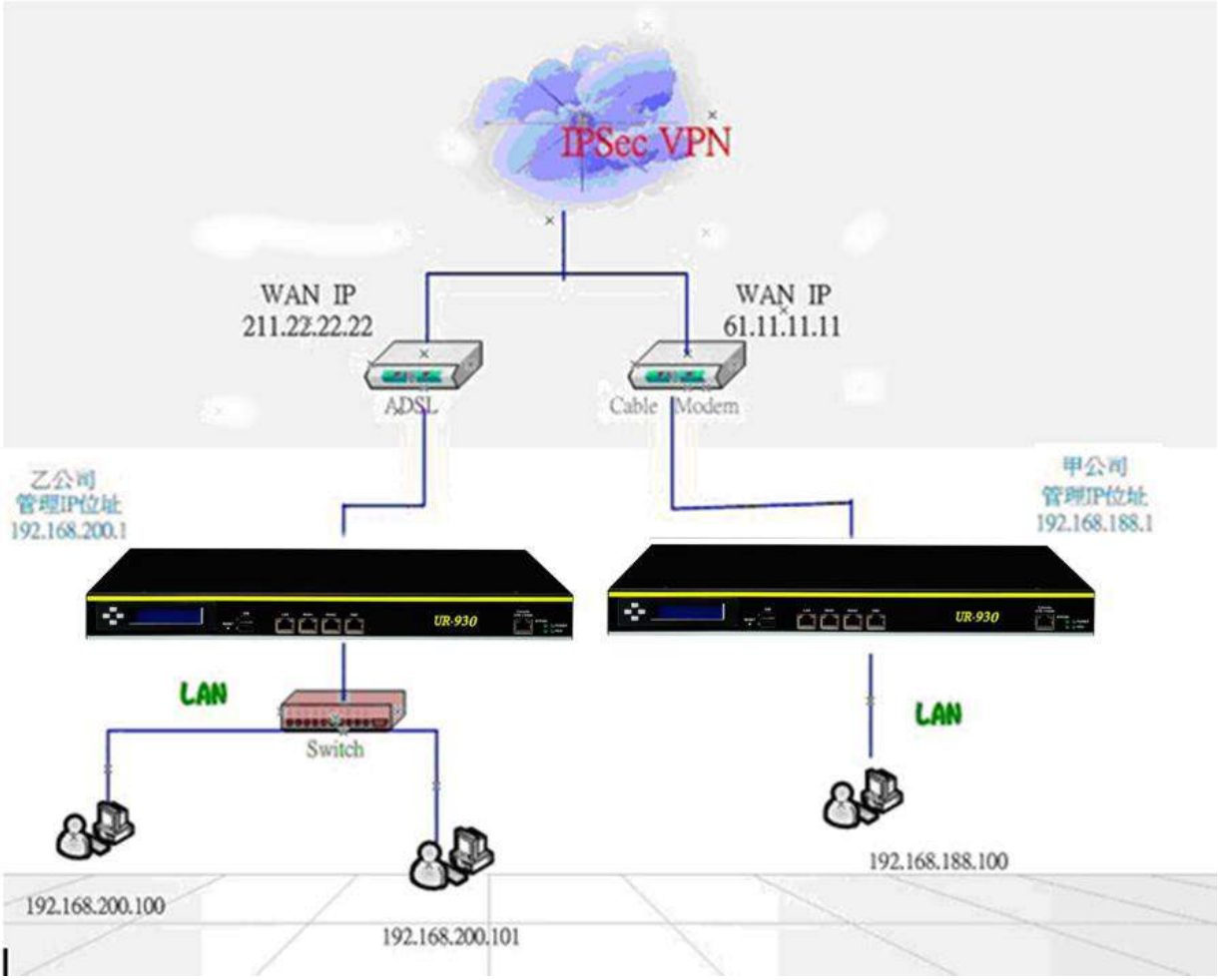


圖 12-6 IPSec VPN 連線之架設環境

甲公司的設定

進入甲公司的 NG-UTM 設定，系統預設值的部分就不列出。

- 【啟動 】：選擇啟用。
- 【VPN 通道名稱 】：到乙公司連線。
- 【本地 IP 位址 】：61.11.11.11。
- 【遠端 IP 位址 】：211.22.22.22。
- 【本地端網路 】：192.168.188.0/24。
- 【遠端網路 】：192.168.200.0/24。
- 【啟用備援 】：不要啟動備援服務。

IPSec Phase 1 設定

- 【連線模式 】：主要模式(main mode)。
- 【Preshare Key 】：123456789。
- 【ISAKMP 演算法 】：AES / SHA-1，DH Group2。

IPSec Phase 2 設定

- 【IPSec 演算法】：AES / SHA-1，DH Group2。

IPSec 其他設定

- 【Dead Peer Detection】：Restart。

乙公司的設定

進入乙公司的 NG-UTM 設定，系統預設值的部分就不列出。

- 【啟動 】：選擇啟用。
- 【VPN 通道名稱 】：到甲公司連線。
- 【本地 IP 位址 】：211.22.22.22。
- 【遠端 IP 位址 】：61.11.11.11。
- 【本地端網路 】：192.168.200.0/24。
- 【遠端網路 】：192.168.188.0/24。
- 【啟用備援 】：不要啟動備援服務。

IPSec Phase 1 設定

- 【連線模式 】：主要模式(main mode)。
- 【Preshare Key 】：123456789。
- 【ISAKMP 演算法 】：AES / SHA-1，DH Group2。

IPSec Phase 2 設定

- 【IPSec 演算法】：AES / SHA-1，DH Group2。

IPSec 其他設定

- 【Dead Peer Detection】：Restart。

2 端的差異部分如紫色區塊，這 2 個地方必須要確認清出並輸入正確，如果網段或是外部 IP 位址設錯，將會導致 VPN 連線無法成功。

VPN 通道控制方法

建立完成的 IPSec VPN Tunnel 會列表，如下圖：（圖 12-7）

IPSec VPN 通道： 1 / 1

VPN 通道名稱	本地 IP 位址	本地端介面	本地端網路	狀態	遠端 IP 位址	遠端網路	phase 1	phase 2	運作時間	啟動	切換	編輯 / 刪除	記錄
coratt	192.168.191.169		192.168.1.0/24		192.168.191.170	192.168.61.0/24	des-md5	des-md5	00:24:18		-		記錄
mandy	192.168.191.169	zone2	192.168.1.0/24		Dynamic IP	172.16.10.0/24	des-md5	des-md5	--		主要		記錄

圖 12-7 IPSec VPN 通道控制

- 【本地端介面】：目前 IPSec VPN 使用的實體介面。
- 【狀態】：：代表斷線，：代表連線。
- 【啟動】：控制 IPSec VPN 啟動與暫停的按鈕，：代表目前是啟動中，：這一條 VPN 被暫停。
- 【切換】：這一條 VPN 通道是主要的還是備援。
- ：代表修改這個通道的設定。
- 【紀錄】：記錄：這一條 VPN 的通聯記錄，IPSec VPN 通道如果跟對方有溝通紀錄，按下去會開啟新視窗，資料是照時間排序，最新的訊息在最後一頁。（圖 12-8）

通道名稱：甲公司連線　每三十秒　自動更新　export　clear　1 / 23　1　GO

時間	號碼	事件
2010-04-23 16:50:03		terminating SAs using this connection
2010-04-23 16:50:03		terminating SAs using this connection
2010-04-23 16:50:03		terminating SAs using this connection
2010-04-23 16:50:03	#2	initiating Main Mode

圖 12-8 IPSec Tunnel 的通聯記錄

12-2、Auto VPN

建立一條 IPsec VPN Tunnel 的步驟繁瑣，尤其是要對應 2 端的 ID，使用網段等，當 IPSec VPN 通道數量多時，往往不太容易辨識或是弄錯，尤其是遠端 IP 多是動態 IP 位址下，IPSec VPN 的穩定度備受考驗。

ShareTech 提出 Auto VPN 架構，他是建構在 IPSec VPN 的基礎上，簡化設定邏輯，讓 VPN 部署時方便又快速，他基本組成有 2 個

AutoVPN Server：設定 IPSec VPN 的條件，並產生一個辨識碼，這個辨識碼是要給 Client 端使用。

AutoVPN Client：拿到 Auto VPN Server 端給的辨識碼，輸入 AutoVPN 的 IP 位址，就完成 Client 的設定。

12-2-1、Auto VPN Server 設定

在 AutoVPN Server 建立一條新通道時，除了【辨識碼】外，其他的都跟傳統的 IPSec VPN 通道建立的方式一樣。（圖 12-9）

- 【辨識碼】：每建一個 VPN 通道，系統會自動產生一個獨一無二的辨識碼，將這個辨識碼複製後傳給 Auto VPN Client 端。

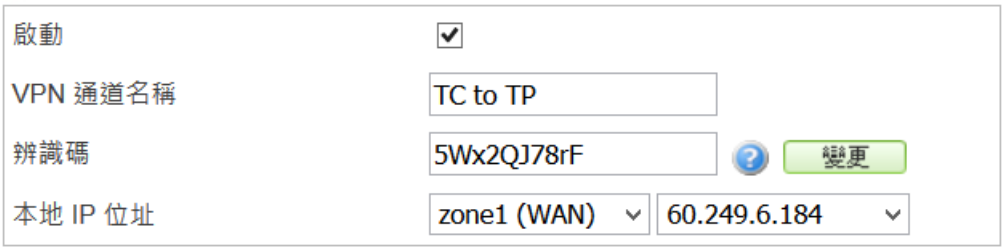


圖 12-9 Auto VPN 設定

12-2-2、Auto VPN Client

當獲得 AutoVPN Server 的【辨識碼】後，就可以到遠端的 AutoVPN Client 端設定，在 Client 端就沒有 IPSec VPN 的繁雜設定。（圖 12-10）

- 【啟動】：啟用這條 VPN 設定。
- 【VPN 通道名稱】：這一條 VPN 通道容易辨識的名稱。
- 【Server IP】：Auto VPN 的外部 IP 位址。
- 【辨識碼】：輸入 Auto VPN Server 給的獨一無二的辨識碼。
- 【本地 IP 位址】：要使用那一個 IP 建立 VPN 通道。

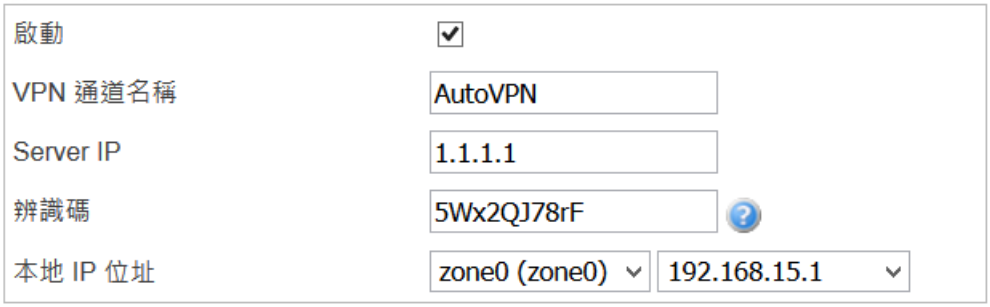


圖 12-10 Auto VPN Client 端設定

建立完成的 VPN 通道 列表如下，

- 【AutoVPN 狀態】：：代表 Client 連線正常，：代表 Client 尚未連線。
- 【狀態】：：代表斷線，：代表連線。
- 【啟動】：控制 IPSec VPN 啟動與暫停的按鈕，：代表目前是啟動中，：這一條 VPN 被暫停。

VPN 的繁雜設定。（圖 12-11）

圖 12-11 Auto VPN Client 端設定

12-3、PPTP 伺服器

PPTP 協定在每一個作業系統中，例如，Windows、Linux 都有現成的撥接軟體可以使用，輸入管理者預先給的帳號密碼後，就可以藉由 PPTP VPN 連線，透過網際網路進入 NG-UTM 內部。

使用 PPTP 功能在 NG-UTM 中有幾個步驟：

1.啟用 PPTP 伺服器

2.建立帳號

3.到管制條例的管制規則中建立 PPTP 用戶可以存取的網路資源

12-3-1、PPTP 伺服器

建立 PPTP 伺服器的第一個動作就是啟用 PPTP 伺服器，讓遠端用戶可以利用 PPTP 的撥接軟體跟 NG-UTM 的 PPTP 伺服器建立加密的 VPN 連線，以下為其設定步驟：（圖 12-12）

- 【啟用】：要不要啟用 PPTP 伺服器。
- 【啟動壓縮加密】：要不要在 PPTP 通道中啟用壓縮。
- 【分配的 IP 位址範圍】：要分配給撥進來用戶端分配的 IP 位址及範圍，例如，10.1.1.1~10.1.1.10。
- 【DNS1/2】：分配給遠端用戶端的 DNS 伺服器位址。
- 【WINS1/2】：分配給遠端用戶端的 WINS 伺服器位址。

圖 13-8 PPTP 伺服器設定

12-3-2、新增帳號

在【新增帳號】選項，在此要建立用戶端的撥入帳號。（圖 12-13）

- 【啟動】：要不要啟用這個帳號。
- 【帳號】：PPTP 用戶端撥入使用的帳號，例如，jordan。
- 【密碼】：PPTP 用戶端撥入使用的密碼。
- 【用戶端的 IP 位址】：PPTP 用戶端撥入使用的 IP 位址，除了可以由 PPTP 伺服器按照設定的範圍分配外，管理者也可以針對特定的帳號，給予特定的 IP 位址或是範圍。
- 【自行輸入 IP 位址】：在【用戶端的 IP 位址】中選擇自行輸入 IP 位址時就會出現，例如 192.168.1.5。

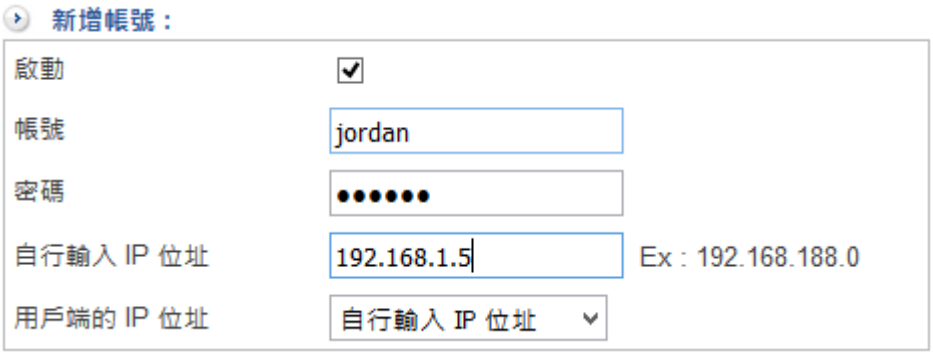


圖 12-13 建立 PPTP 帳號

12-3-3、PPTP 帳號列表

建立好的 PPTP 帳號會在【PPTP 帳號列表】中出現，管理者可以在此控制，每一個 PPTP 帳號的啟用與關閉。（圖 12-14）

- 【帳號】：PPTP 用戶端撥入使用的帳號。
- 【狀態】：：代表斷線，：代表連線。
- 【啟動】：控制 PPTP VPN 啟動與暫停的按鈕，：代表目前是啟動中，：這一個 PPTP 帳號是被暫停，點選暫停用戶無法利用 PPTP 它來撥接。

PPTP 伺服器列表： 目前上線成員數：0 1 / 1

帳號	狀態	啟動	編輯 / 刪除	記錄
coratt				記錄
test				記錄
csko				記錄
kaga				記錄
debby				記錄

圖 12-14 PPTP 帳號列表控制

- 【紀錄】：記錄：這一條 VPN 的通聯記錄，PPTP 用戶如果有撥入，在此會顯示其撥接紀錄，按下去會開啟新視窗。

PPTP 紀錄

- 【時間】：PPTP 用戶端撥入開始的時間。
- 【遠端網路 IP】：PPTP 用戶端使用的 IP 位址。
- 【事件】：PPTP 用戶端撥入開始或是結束事件，結束的事件系統會自動計算總共使用的時間，單位是『小時:分』，低於 1 分鐘的時間統統被紀錄成 00:00。

12-4、SSL VPN Server

SSL VPN 是一種具有安全加密保護的虛擬私人網路技術，可以讓使用者在外地使用電腦的時候，就像是在區域網路裡面使用電腦一樣，可以使用任何只有在區域網路內才能使用的資源，如 ERP、進銷存或是限定來源 IP 位址的圖書查詢系統，又因為將資料加密，所以在網際網路上無法解析傳輸的內容，確保雙方傳輸資料的安全性。

SSL VPN 具備有管制功能，對於遠端用戶而言，管制有 2 個方向，一個是進入內部網路，另一個是透過 VPN Server 上網際網路(可以選擇啟用或是關閉這項功能)，這 2 個管制方向都可以管制遠端用戶使用的頻寬、通訊服務及時間。

使用 SSL VPN 時，需要從 VPN 伺服器端下載軟體及憑證，SSL VPN 用戶端軟體使用綠色軟體的技術，所以不需要任何安裝動作，直接執行就可以運行，所以使用者可以將軟體跟憑證放在任何移動的儲存設備，如 USB 等，然後在任何電腦設備上執行。

Client 端取得 SSL Client 端軟體及憑證 URL

用戶端可以登入 SSL VPN 伺服器端取得 SSL VPN 用戶端軟體及憑證，因為 NG-UTM 的用戶端軟體跟憑證是綁定在一起，用戶下載之後，解壓縮後就可以執行。

預設的網址是 https:// 【網路介面 IP 位址或網域】：【網路介面及路由 > 網路介面 > HTTPS Port】/sslvpn.php。

範例：介面的管理 IP 位址及 Port 是 https://211.2.2.2:8443 則取得的網址下：https://211.2.2.2:8443/sslvpn.php

12-4-1、SSL VPN 設定

SSL VPN 預設是關閉，要啟用前需要點選【修改伺服器設定值】才會將設定畫面開啟。

SSL VPN 伺服器設定

- 【服務狀態】：可以啟動或是關閉。（圖 12-15）
- 【本機使用的介面】：選擇提供 SSL VPN 服務的介面跟他的 IP 位址，按輔助選取的按鈕可以提示管理者，哪一個介面跟 IP 位址目前還可以選擇。

  這裡的介面跟 IP 位址是可以複選，例如，ZONE 1 的 IP 位址 11.12.13.14 跟 ZONE 2 的 IP 位址 23.24.25.26 都提供 SSL VPN 撥入的服務。
- 【本機使用通訊埠】：哪幾個 PORT 號讓 SSL VPN 的用戶端撥入，管理者可以設定一個 PORT 或是一個範圍的 PORT，例如，387-387，代表只有 387 接受 SSL VPN，如果設定值是 387-400，代表這一個範圍的 PORT 都接受 SSL VPN 撥入。

  這個用戶端跟伺服器端溝通的埠號，切記，一定要跟 WAN 的管理介面錯開。
- 【同時最大連線數】：最多可以讓幾個人同時用 SSL VPN，預設值是 20。
- 【VPN IP 範圍】：SSL VPN 用戶端取得的 IP 位址範圍，例如，10.8.0.0 /255.255.255.0，VPN IP 範圍不可與內部的網段相同。
- DNS Server ：SSL VPN 用戶連線成功後配發的 DNS 伺服器。
- Wins Server ：SSL VPN 用戶連線成功後配發的 wins 伺服器。

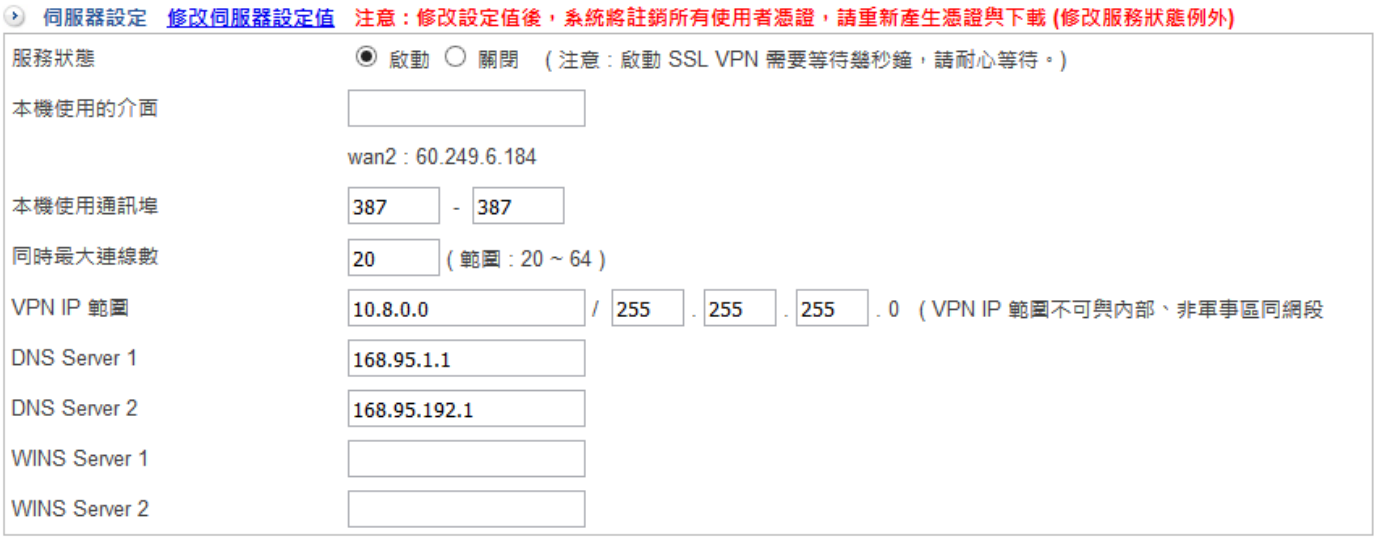


圖 12-15 SSL VPN 伺服器設定

憑證設定

SSL VPN 用戶端使用的憑證是由 SSL Server 簽發，伺服器要簽發憑證時需要填入一些資訊，憑證機制再利用這一些資訊製作憑證給使用者，每個欄位都必須輸入最少一個文字，不可為空白，如果更改這個欄位的任何一個字元，每個使用者的憑證都需要重新下載。（圖 12-16）

圖 12-16 憑證設定

12-4-2、Client SSL VPN 列表

新增一個 SSL VPN 用戶前，要先到上網認證的地方增加一個認證群組，並選擇群組成員，如何產生群組成員，請參考第 5-8 節，上網認證中使用者群組說明。

增加使用者群組後，可以在 Client SSL VPN 列表終新增一個認證群組，在認證群組中會出現剛剛在上網認證設定使用者群組。（圖 12-17）

- 【註解】：任何可以描述這一個 SSL VPN 用戶端的文字，例如，SSLVPN-TEST。
- 【認證群組】：顯示在第 5-8 節，上網認證中建立的使用者群組且尚未被套用過。
- 【連線成功時顯示訊息之網址】：希望 SSL VPN 撥接成功後，自動轉向哪一個網頁，如果沒有設定，則使用使用者瀏覽器預設的網址。

圖 12-17 新建一個 SSL VPN 認證列表

增加一個認證群組後，Client SSL VPN 列表會把所有的 SSL 用戶端列出來。（圖 12-18）

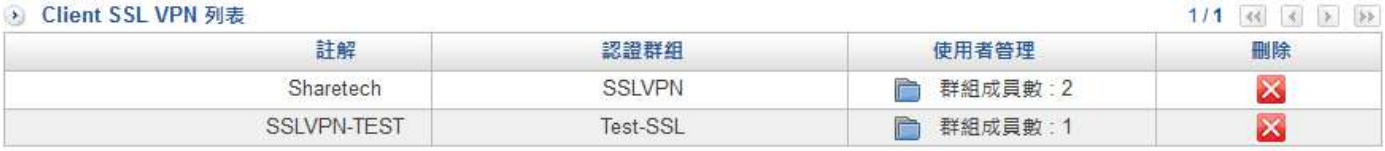


圖 12-18 SSL VPN 用戶列表

取得憑證

每當管理者更改憑證伺服器中的任何文字，對於已經建立的 SSLVPN 用戶，所有的憑證都需要重新產生，只要按下【重新取得憑證】的按鈕，NG-UTM 就會將所有的憑證更新一次，使用者重新下載後就可以使用。（圖 12-19）

按下 就可以查看目前憑證。

- 【使用者帳號】：在增加群組時，所加入的使用者。
- 【註銷憑證】：將該使用者的憑證取消，使用者就無法撥入，如果希望讓使用者又再次能使用，則需要重新取得憑證。
- 【重新取得憑證】：將該使用者的憑證取消或是憑證的內容重新設定，用者就無法撥入，此時使用者則需要重新取得憑證。
- 【下載】：下載用戶端軟體跟憑證。
- 【設定使用者固定 IP 位址】：針對這個 SSL VPN 用戶端，每次撥接成功後， 伺服器端分配的固定的 IP 位址給他，點選 進入選擇 IP 位址的頁面，選擇一個尚未被分配的 IP 位址給這個使用者。
- 【暫停使用】：憑證暫時停用，此使用者的憑證依然有效，只是不讓他具有撥入權限，只要讓他恢復使用，恢復使用不需要重新取得憑證使用者就可以使用。
- 【設定使用者固定 MAC 位址】：管理者可以在此填入這一個 SSLVPN 用戶的 MAC 位址，避免因為帳號密碼或是憑證被別人竊取後的資安漏洞，確保撥入的用戶電腦是管理者認可的，空白代表撥入時不會檢查 MAC 位址。

  點選 進入填寫 MAC 位址的頁面，如果用戶端有多個網卡，SSL VPN 用戶端會自動抓取第一個網路卡的 MAC 位址當作比對的對象。

圖 12-19 SSL VPN 用戶資料修改

SSL VPN 用戶端使用

使用者可自行登入 NG-UTM 的 SSLVPN 用戶端軟體下載 SSLVPN 軟體，下載的網址就 https://介面 IP 位址:port/sslvpn.php。

步驟**1.** 用 https://SSL SERVER /sslvpn.php 下載檔案。（圖 12-20）

圖 12-20 SSL VPN 用戶端軟體及憑證下載

步驟**2.** 下載 SSL VPN 的用戶端及憑證檔案，並將他另存新檔，下載完畢可以將檔案解壓縮在任何地方。（圖 12-21）

圖 12-21 儲存 SSL VPN 用戶端軟體

步驟**3.** 在解壓縮地方執行 SSL VPN 的用戶端，openvpn-gui-1.0.3-en.exe。

步驟**4.** 軟體會自動執行，執行後在右下角會出現一個小圖示

 ，按下滑鼠右鍵。

步驟**5.** 選擇 EDIT Config，使用者可以選擇語系，更改 SSL VPN Server 或是 埠號，也可以選擇要不要從遠端上網際網路，如果沒有勾選從遠端上網，則除了遠端的 LAN、DMZ 區段的 IP 會走 SSL VPN 通道外，其他的都會走本地端。（圖 12-22）

圖 12-22 修改 SSL VPN 用戶端

步驟**6.** SSL VPN 連線，輸入管理者給的帳號及密碼，這個帳號及密碼跟剛剛下載軟體及憑證的帳號密碼是一樣的。（圖 12-23）

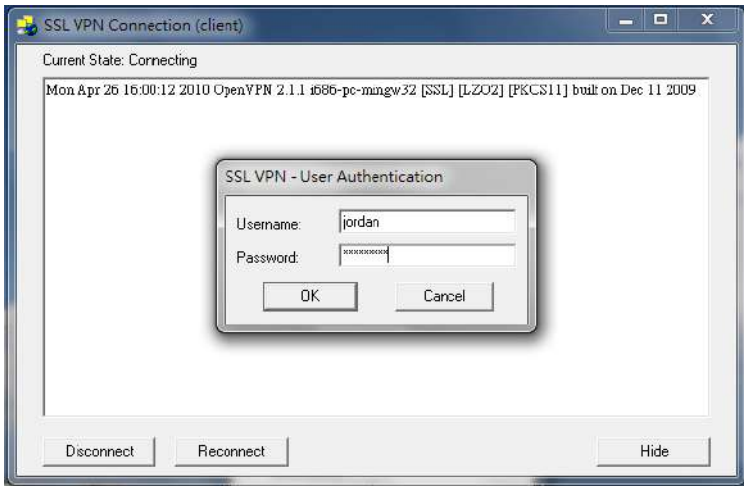


圖 12-23 SSL VPN 用戶端登入

步驟**7.** SSL VPN 連線後 ，在原來的小圖標會由紅色轉成綠色，代表 SSL VPN 已經完成連線。（圖 12-24）

圖 12-24 SSL VPN 用戶登入成功

11-4-3、VPN 紀錄

每一個 SSL VPN 的連線紀錄在 NG-UTM 中都有詳細的紀錄。（圖 12-25）

- 【啟動拒絕連線紀錄】：要不要將 SSL VPN 伺服器的拒絕紀錄下來，管理者可以選擇啟動或是關閉，當啟用後，所有撥接不成功的紀錄通通會被紀錄下來，管理者可以按下 紀錄按鈕 查詢相關資訊。
- 【目前上線成員數】：總共有多少 SSLVPN 上線。
- 【踢除】：對於已經用 SSLVPN 連線的使用者，管理者可以強制讓他離線，點選踢除+用戶名稱，就可以讓他離線。

每一個可以用 SSL VPN 撥入的帳號都會出現在使用者列表中，在每一個使用者的 記錄 處，知道用戶何時登入登出。

圖 12-25 SSL VPN 用戶列表

12-5、L2TP

NG-UTM 支援 L2TP VPN，L2TP 提供 IPSec VPN 的 Preshare key 加密機制，提供比 PPTP 更強的加密保護。

12-5-1、帳號列表

建立好的 L2TP 帳號會在【帳號列表】中出現，管理者可以在此控制，每一個 L2TP 帳號的啟用與關閉。

12-5-2、基本設定

L2TP 是建立在 IPSec 加密技術的基礎之上，所以要事先設定 Preshare Key 跟要分配的 IP 位址範圍。（圖 12-26）

- 【啟動】：要不要啟用 L2TP 伺服器。
- 【分配的 IP 位址範圍】：要分配給撥進來用戶端分配的 IP 位址及範圍，例如，10.1.1.1~10.1.1.10。
- 【第一個 DNS 伺服器】：分配給遠端用戶端的 DNS 伺服器位址。
- 【第二個 DNS 伺服器】：分配給遠端用戶端的 DNS 伺服器位址。
- 【介面 IP】：哪個外部介面 IP 要當 L2TP 撥進來的 IP 位址，點選【輔助選取】後，系統會列出所有可以提供的外部介面，勾選後就可以提供給 L2TP VPN 的用戶撥入，可以勾選多個外部介面。
- 【Preshare Key】：在 L2TP 上使用的加密密碼。

圖 12-26 L2TP 設定

建立帳號

L2TP 撥入時需要的帳號跟密碼。（圖 12-26）

- 【啟動】：要不要啟用這個帳號。
- 【帳號】：給撥進來用戶的帳號，例如，lt2ptest。
- 【密碼】：此帳號的密碼。
- 【用戶端的 IP 位址】：有 2 種選項，使用配給的 IP 位址或是自行輸入 IP 位址。

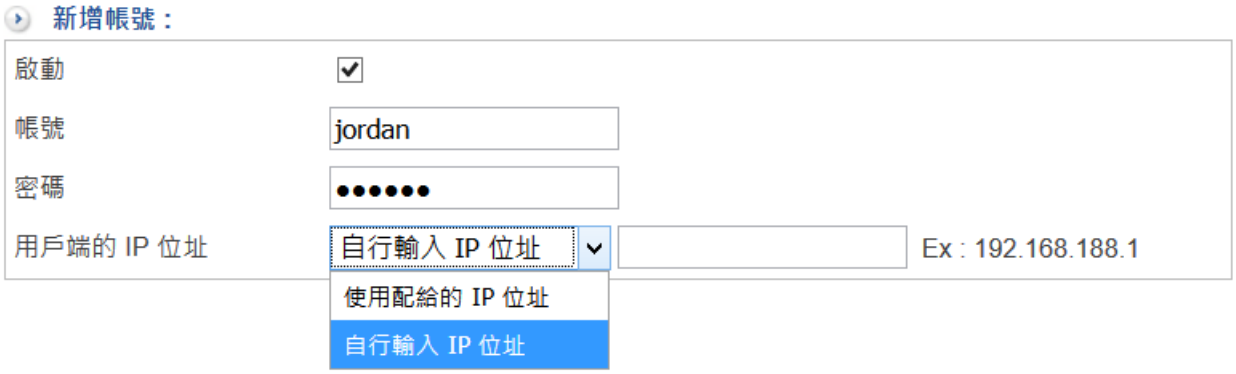


圖 12-26 L2TP 設定

建立完成的帳號，按下【紀錄】按鈕就可以知道這個帳號使用狀態。（圖 12-27）

圖 12-27 L2TP 帳號列表

12-6、SD-WAN

NG-UTM 支援 SD-WAN 功能，SD-WAN 可以把出口線路或是 VPN 通道的任意組合綁定成一個通道控制機制，綁定同時，還可以指定負載分配的比重。（圖 12-28）

- 【群組名稱】：SD-WAN 的名稱。
- 【比重】：負載分配比例，如果使用 3 個線路當作負載線路，分別設成 A 線路 ：1、B 線路：2、C 線路：3，則第一個封包往 A 線路送，第 2、3 個往 B 線路送，第 4、5、6 封包往 C 線路送，第 7 個再往 A 線路，以此類推。
- 【VPN 通道】：用 IPSec VPN 建立的通道。
- 【出口線路】：接在 NG-UTM 上的實體線路。

  NG-UTM 提供 SD-WAN 功能，可以混用 VPN 通道跟出口線路，只要確認任何通道都可以單獨到遠端後，就可以混用並按照線路特性分配比重。

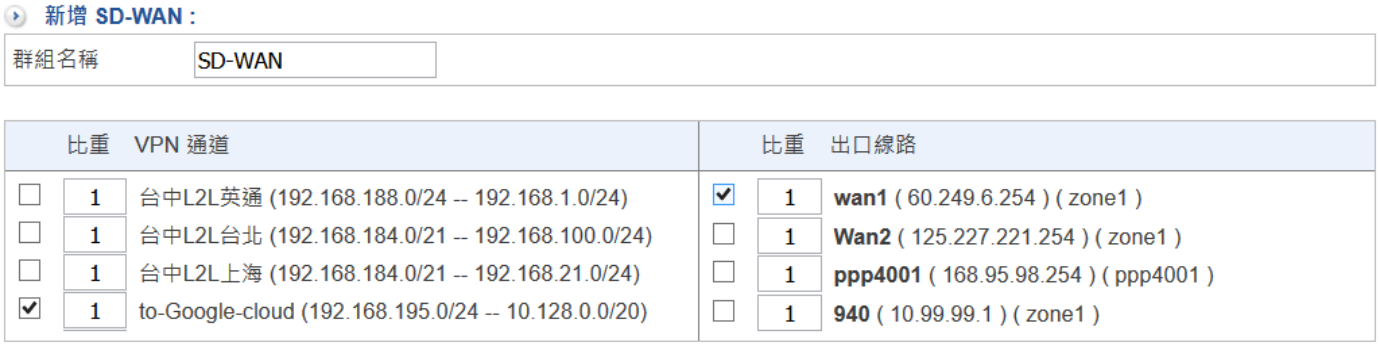


圖 12-28 SD-WAN 比重分配

SD-WAN 建立完成後的列表，到目前為止只是定義好線路，這些線路能跑那些協議則需要到管制條例中的 SD-WAN 管制處理。（圖 12-29）

圖 12-29 SD-WAN 列表

第 13 章 網路工具

管理者可由系統提供的網路工具，主動發送偵測封包，確認 NG-UTM 對外的線路品質跟 DNS 查詢是否正常，目前提供幾種工具讓管理者運用，分別是 PING、Trace route、DNS 查詢、Port Scan、Wake up 跟 SNMP，其中 PING 支援 IPV4/V6 2 種位址模式。

13-1、連線測試

13-1-1、PING 的使用

一般碰到網路不通的情況，很自然的就會使用 PING（Windows 跟 Linux 都相同）這個命令來檢查自己跟對方網路是否暢通，PING 這個命令使用 ICMP 協定，在固定的時間送出特定大小的 ICMP 封包，同時量測對方電腦的回應時間，藉以量測線路是否正常。（圖 13-1）

- 【目標 IP 或網域名稱】：切換 MENU 選單的 IPV4/IPV6 按鈕可以切換要測試的 IP 位址模式，以 IPV4 為例，輸入待檢測的 IP 位址或是網域名稱都可以，例如，168.95.1.1 或是 www.hinet.net。
- 【封包大小】：每次送出的 ICMP 協定封包大小，預設是 32 Bytes，設定範圍是 1 ~9999Bytes。
- 【回應次數】：送出多少次的測試封包，預設是 4 次，設定範圍是 1 ~9999 次。
- 【等待時間】：ICMP 等待回應的間隔時間，超過這一個時間就會視為斷線，預設是 1 秒，設定範圍是 1~9999 秒。
- 【介面位址】：選擇要送出這個測試封包的介面跟他帶出去的 IP 位址。
- 【出口線路】：要從這一個介面位址的哪一個閘道送出測試封包。


```
PING 168.95.1.1 (168.95.1.1) from 192.168.189.169 : 32(60) bytes of data
40 bytes from 168.95.1.1: icmp_seq=1 ttl=249 time=3.42 ms
40 bytes from 168.95.1.1: icmp_seq=2 ttl=249 time=2.99 ms
40 bytes from 168.95.1.1: icmp_seq=3 ttl=249 time=1.97 ms
```

圖 13-1 PING 測試工具及輸出資訊

13-1-2、Trace route 的使用

Trace route，它可顯示封包從來源到目的地網絡所經過的路由器的 IP 位址，一般碰到網路不通的情況，除了用 PING 檢查自己跟對方網路是否暢通外，如果想知道到目的地前會經過哪幾個路由器或是網路不通到底是斷在哪裡，此時就會使用這一個工具，目前他只支援 IPV4 位址。（圖 13-2）

- 【目標 IP 或網域名稱】：輸入待檢測的 IP 位址或是網域名稱都可以，例如，168.95.1.1 或是 www.hinet.net。
- 【封包大小】：每次送出的 ICMP/UDP/TCP 協定封包大小，預設是 40 Bytes，設定範圍是 40 ~9999Bytes。
- 【最大存活時間】：最大可以量測經過幾個路由器，預設是 30，設定範圍是 1 ~255 個路由器。
- 【等待時間】：ICMP 等待回應的間隔時間，超過這一個時間就會視為斷線，預設是 2 秒，設定範圍是 2~9999 秒。
- 【偵測方式】：用哪一個通訊協定送出偵測封包，可以選 ICMP/UDP/TCP，預設是 ICMP。
- 【來源位址】：選擇要送出這個測試封包的介面跟他帶出去的 IP 位址。
- 【出口線路】：要從這一個介面位址的哪一個閘道送出測試封包。


```
traceroute to 168.95.1.1 (168.95.1.1), 30 hops max, 40 byte packets
 1  192.168.189.1 (192.168.189.1)  0.744 ms  0.790 ms  0.829 ms
 2  h254.s98.ts.hinet.net (168.95.98.254)  4.756 ms  4.916 ms  4.996 ms
 3  tc-c6r2.router.hinet.net (168.95.145.54)  4.710 ms  4.796 ms  4.799 ms
 4  tchn-3011.hinet.net (220.128.16.234)  7.784 ms  7.794 ms  7.793 ms
 5  220-128-32-129.HINET-IP.hinet.net (220.128.32.129)  4.582 ms  4.589 ms  4.594 ms
 6  dns.hinet.net (168.95.1.1)  4.393 ms  5.461 ms  5.275 ms
```

圖 13-2 Tracer route 測試工具及輸出資訊

13-1-3、DNS Query 的使用

查詢 DNS 的詳細資料，可以查詢 DNS 的 ANY、SOA、NS、A、MX、CNAME、PTR 等資料，管理者可以使用本機或是特定的 DNS 伺服器作為查詢依據。（圖 13-3）

- 【DNS 伺服器 IP 位址或名稱】：可以選用 NG-UTM 使用的 DNS 伺服器或是自行輸入其他的 DNS 伺服器。例如，8.8.8.8。
- 【查詢對象的名稱或 IP 位址】：輸入待查詢的 IP 位址或是網域名稱都可以，輸入網域名稱這是選擇正查，輸入 IP 位址則是屬於反查，例如，168.95.1.1 或是 www.hinet.net。
- 【類型】：查詢 DNS 的 ANY、SOA、NS、A、MX、CNAME、PTR 等資料。

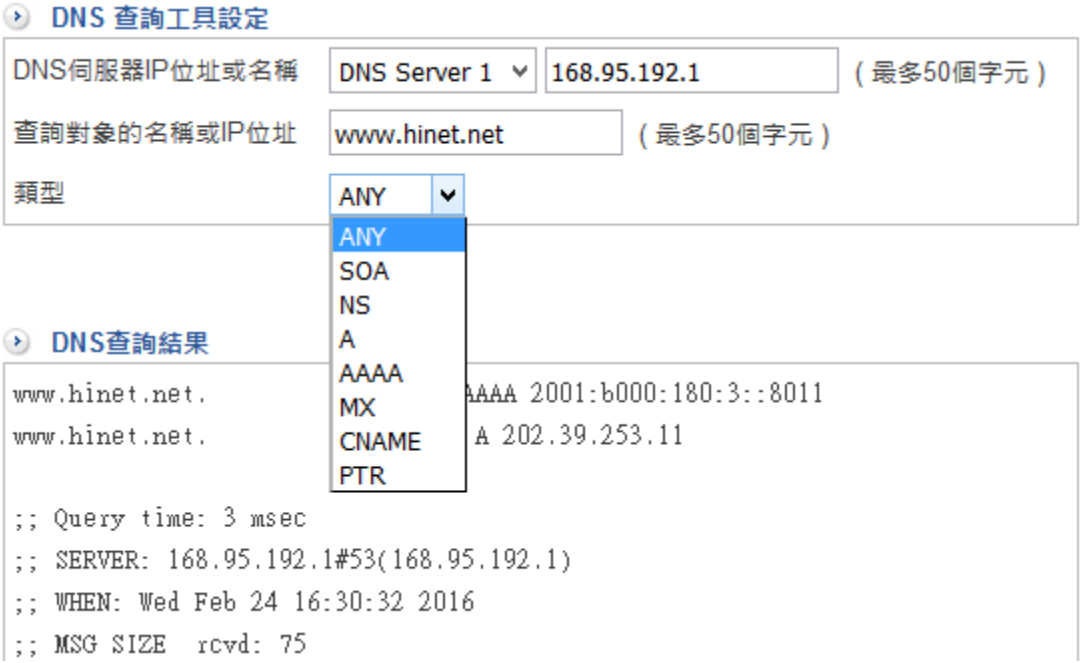


圖 13-3 DNS 測試工具及輸出資訊

13-1-4、Port Scan

利用 NG-UTM 去掃描遠端電腦是否有開放的常用的 PORT。（圖 13-4）

- 【輸入 IP 位址或域名】：輸入查詢的主機 IP 位址或是域名，例如，8.8.8.8。
- 【來源位址】：查詢時使用的 Zone 跟 IP 位址。
- 【查詢結果】：有開放的 Port 會出現 OK 文字，如果沒開放則出現 FAIL。

圖 13-4 DNS 測試工具及輸出資訊

13-1-5、IP Route

整個 NG-UTM 的路由表，讓管理者參考。

13-1-6、Interface Information

NG-UTM 可以顯示每一個 Zone 內的綁定的位址區段、使用者 IP 及 MAC 位址。（圖 13-5）

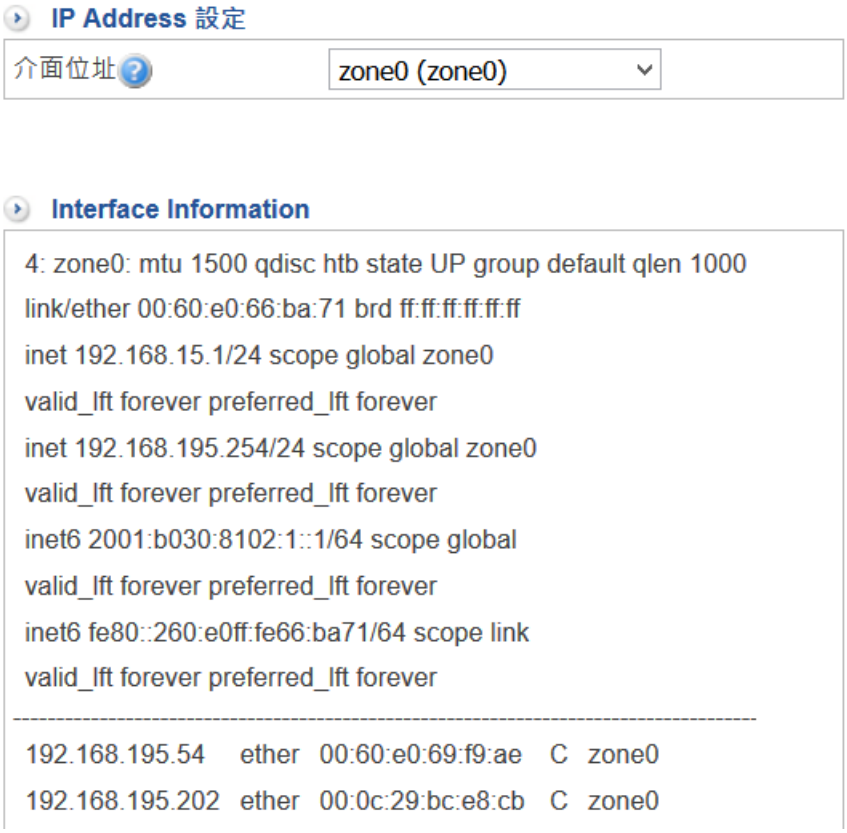


圖 13-5 介面資訊

13-1-7、Wake Up

NG-UTM 可以執行 Wake Up 遠端電腦的工作，只要填入遠端電腦的 MAC 位址，按下確定後，系統會自動送出 Wake Up 封包給遠端的電腦，管理者也可以按【輔助選取】，直接選要喚醒的電腦。（圖 13-6）

- 【介面位址】：要執行 Wake Up 的電腦是屬於哪一個介面。
- 【MAC 位址】：要執行 Wake Up 電腦的 MAC 位址，如果不知道可以按下【輔助選取】按鈕選取。

圖 13-6 Wake Up 設定

13-1-8、SNMP

NG-UTM 用 SNMP 協議去查詢交換器的資訊，包含每一個 Port 的即時流量或是 Vlan ID 等。

- 【Switch IP】：要向哪一個交換器查詢，填入交換器的 IP 位址。
- 【Read 權限】：因為只是要執行查詢動作，只需要 Read 權限的密碼就可以。
- 【OID】：要查詢的資料，SNMP 都是以 OID 的方式去查詢。（圖 13-7）

oid	說明	範例
必要		
iso.3.6.1.2.1.2.2.1.10	查詢 port 入流量	iso.3.6.1.2.1.2.2.1.10.515 = Counter32: 3692512
iso.3.6.1.2.1.2.2.1.16	查詢 port 出流量	iso.3.6.1.2.1.2.2.1.16.515 = Counter32: 11238968
iso.3.6.1.2.1.17.1.4.1.2	查詢 port 對應的 Ifindex	iso.3.6.1.2.1.17.1.4.1.2.515 = INTEGER: 509
iso.3.6.1.2.1.31.1.1.1.1	查詢 port 介面	iso.3.6.1.2.1.31.1.1.1.1.515 = STRING: "ge-0/0/6"
iso.3.6.1.2.1.2.2.1.2	查詢 port 介面	iso.3.6.1.2.1.2.2.1.2.515 = STRING: "ge-0/0/6"
iso.3.6.1.2.1.17.4.3.1.2	查詢 mac port 對應	iso.3.6.1.2.1.17.4.3.1.2.0.13.72.50.168.248 = INTEGER: 522
iso.3.6.1.2.1.17.7.1.2.2.1.2	查詢 mac port 對應	iso.3.6.1.2.1.17.7.1.2.2.1.2.2.0.28.240.40.57.191 = INTEGER: 21
iso.3.6.1.2.1.2.2.1.7	查詢哪些 port disable	iso.3.6.1.2.1.2.2.1.7.515 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.8	查詢哪些 port 有插線	iso.3.6.1.2.1.2.2.1.8.515 = INTEGER: 2
vlan 必要		
iso.3.6.1.4.1.9.9.46.1.3.1.1.2.1	查詢 Vlan ID	iso.3.6.1.4.1.9.9.46.1.3.1.1.2.1.10 = INTEGER: 1
iso.3.6.1.2.1.4.20.1.2	查詢 Vlan 有哪些id	iso.3.6.1.2.1.4.20.1.2.128.0.0.1 = INTEGER: 38
iso.3.6.1.2.1.17.1.4.1.1	查詢 vlan 有哪些 port	iso.3.6.1.2.1.17.1.4.1.1.515 = INTEGER: 515
附加		
iso.3.6.1.2.1.17.1.2	查詢 switch 總port 數	iso.3.6.1.2.1.17.1.2.0 = INTEGER: 24
iso.3.6.1.2.1.4.22.1.2	查詢 ip mac 對應	iso.3.6.1.2.1.4.22.1.2.38.128.0.0.1 = Hex-STRING: 00 0B CA FE 00 00
iso.3.6.1.2.1.1.1	查詢 switch 名稱	iso.3.6.1.2.1.1.1.0 = STRING: "24G + 4 SFP Web Smart Switch - 2.03"
iso.3.6.1.4.1.9.2.2.1.1.1	查詢 port 介面	iso.3.6.1.4.1.9.2.2.1.1.1.10101 = STRING: "Gigabit Ethernet"

圖 13-7 可查詢 OID

- 【Vlan ID】：Switch 是隸屬於哪一個 Vlan 。

13-2、封包擷取

有時在找網路問題時，需要抓封包分析，NG-UTM 提供自動定時抓封包的工具，方便管理者把封包錄下來，事後到【已完成列表】中下載就可以。

13-2-1、排程中列表（圖 13-8）

- 【啟用】：啟用抓取封包功能。
- 【時間範圍】：指定抓取封包的時間範圍。
- 【網路介面】：要抓網路封包的介面，隸屬於哪一個 Zone。
- 【通訊協定】：全抓還是指定 TCP 、UDP 類型的封包。
- 【過濾條件】：2 種模式，簡易版是填入 IP 位址或是區段就可以，進階版可以下完整的 tcpdump 的命令。
- 【pcap 檔案大小(MB)】：每一個錄下來的檔案大小，設定範圍是 1-10MB。
- 【pcap 檔案份數】：總共錄幾份，設定範圍是 1-100 份，要注意一下儲存空間，以最大值計算，10MB*100 = 1000MB = 1G ，系統必須有 1G 的空間可以儲存，如果有設了好幾個排程同時抓封包，此時就必須要計算可用的空間。
- 【封包擷取長度】：每個封包擷取時的最大長度，一般的網路 MTU 都是 1500。

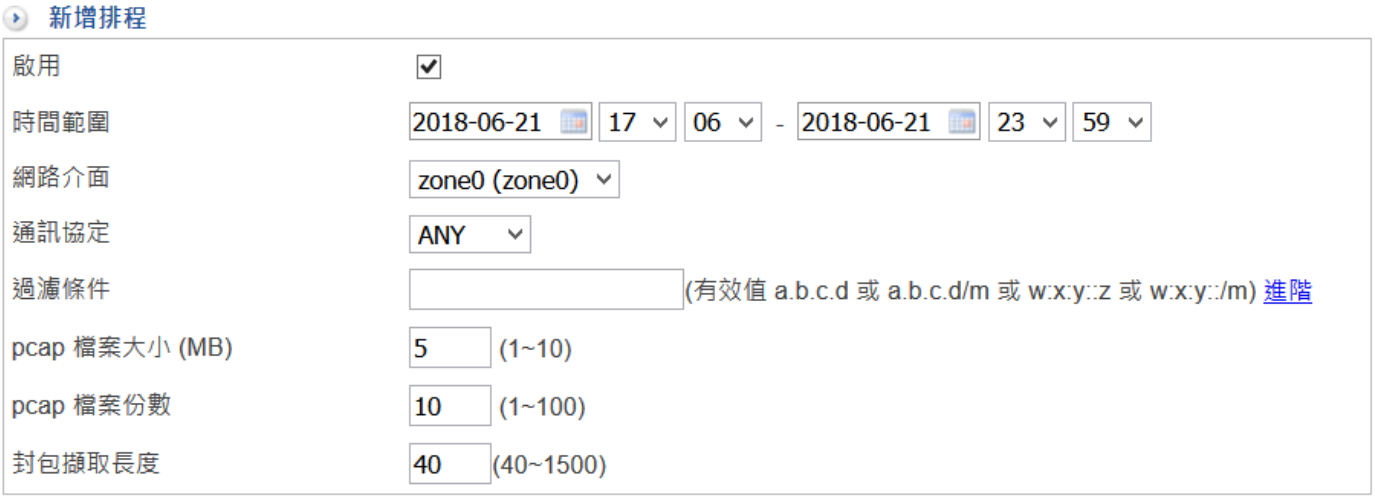


圖 13-8 封包擷取設定

13-2-2、已完成列表

成功抓取的網路封包會列表在這裡，點選【紀錄】按鈕，就可以將這個檔案下載到操作者的電腦端。（圖 13-9）

已完成列表 1 / 1

時間範圍	網路介面	通訊協定	過濾條件	pcap 檔案大小	pcap 檔案份數	封包擷取長度	記錄	刪除
09/28 15:37 ~ 09/28 23:59	188	ANY	-nn	10	1	1500	記錄	

圖 13-9 封包擷取列表

第 14 章 日誌

NG-UTM 會忠實的把每一位管理者登入系統後所執行的任何項目通通紀錄下來，甚至包含登入失敗的事件也會記錄下來，這樣做的優點是方便管理者事後追蹤自己或是其他管理者的操作是否正常，留這樣的依據也方便做時光回朔的動作。

14-1-1、日誌

把所有的事件按照事件發生的 時間、登入帳號、登入 IP 位址、功能路徑、動作跟操作的內容，事件最久可保留一年(12 個月)。

查詢登入事件的詳細資料，任何權限的管理者（View、Read、Write、 View-Read- Write），在 NG-UTM 做的任何事情（新增、修改、刪除、查詢、下載）都會在這裡詳細的紀錄，點選 ⬍ 還可以根據英文字母或是大小排序。（圖 14-1）

- 【時間】：發生該事件的時間。
- 【帳號】：那個管理者帳號，觸發這個事件。
- 【IP 位址】：管理者者帳號使用的 IP 位址。
- 【功能路徑】：管理者進入那一個管理畫面。
- 【動作】：管理者執行的動作，分成（登入、新增、修改、刪除、搜尋、下載）等。
- 【內容】：管理者執行的動作前及後的詳細內容，NG-UTM 會列出修改前跟修改後的差異項目讓管理者比較。

日誌列表　1 / 75　跳至 1 頁數、每頁 16 筆 GO

時間	帳號	IP 位址	功能路徑	動作	內容
2016-02-24 16:33:39	admin	192.168.189.245	網路服務 > DNS伺服器 > View設定	編輯	View名稱
2016-02-24 16:32:20	admin	192.168.189.245	網路服務 > DNS伺服器 > 介面設定	編輯	接受網域抄送的IP位址
2016-02-24 16:32:20	admin	192.168.189.245	網路服務 > DNS伺服器 > 介面設定	編輯	接受代理查詢服務的IP位址
2016-02-24 16:30:48	admin	192.168.189.18	管制條例 > 安全策略 > 安全策略	修改	管制條例名稱
2016-02-24 16:30:29	admin	192.168.189.18	允許登入	登入	Login Successful
2016-02-24 16:12:45	admin	192.168.189.23	允許登入	登入	Login Successful
2016-02-24 15:36:16	admin	192.168.189.245	允許登入	登入	Login Successful

圖 14-1 日誌列表

14-1-2、日誌搜尋

可依照特定 IP 位址或相關事件特徵，來尋找儲存在 NG-UTM 內所有符合條件之記錄。（圖 14-2）

- 【帳號】：查詢哪一個管理者帳號。
- 【IP 位址】：用哪一個 IP 位址登入系統。
- 【事件】：要查詢的是哪一個事件，當然也可以全選。

圖 14-2 事件搜尋

第 15 章 系統狀態

使用者可隨時由系統狀態中，得知 NG-UTM 的資源統計圖，如 CPU、RAM、硬碟等，同時也可以獲得網路即時連線資訊及其統計資料，除了即時資訊外，也有歷史的資訊提供給管理者查詢。

系統狀態有 4 個主要的項目，分別是系統狀態跟連線狀態，說明如下：

（一）【系統狀態】：顯示目前 NG-UTM CPU 使用率，負載、記憶體負載，系統負載，每個介面的上下傳流量也可以查詢上述資訊的歷史流量。

（二）【連線狀態】：記錄 NG-UTM 之連線使用情況，包含上線數量、封包的紀錄等。

（三）【流量分析】：根據 PORT、應用程式或是 DNS 的使用量統計查詢。

（四）【Dashboard】：以圖形的方式顯示各項統計資訊。

15-1、系統狀態

15-1-1、系統狀態

【系統狀態】之【系統狀態】功能中，會顯示從現在到過去 24 小時的統計資料，總結來說有【CPU 負載圖】、【記憶體負載圖】、【系統負載圖】等 3 種。

- 【CPU 負載圖】：顯示 NG-UTM 過去 24 小時 CPU 目前使用狀況。（圖 15-1）
- 點選顯示更多則會列出每一個 CPU 的統計圖。

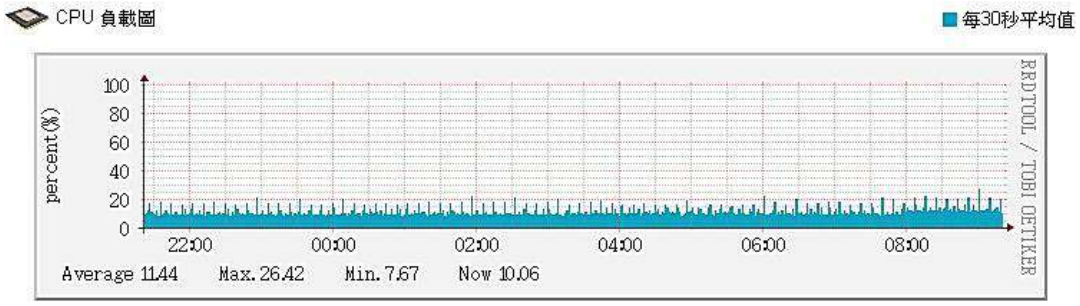


圖 15-1 CPU 負載

- 【記憶體負載圖】：顯示 NG-UTM 過去 24 小時記憶體使用狀況。（圖 15-2）

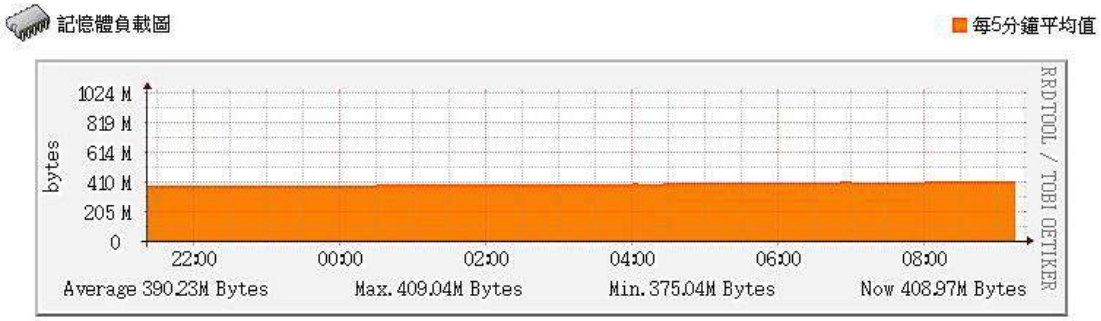


圖 15-2 記憶體負載

- 【系統負載圖】：顯示 NG-UTM 系統過去 24 小時的系統負載。（圖 15-3）

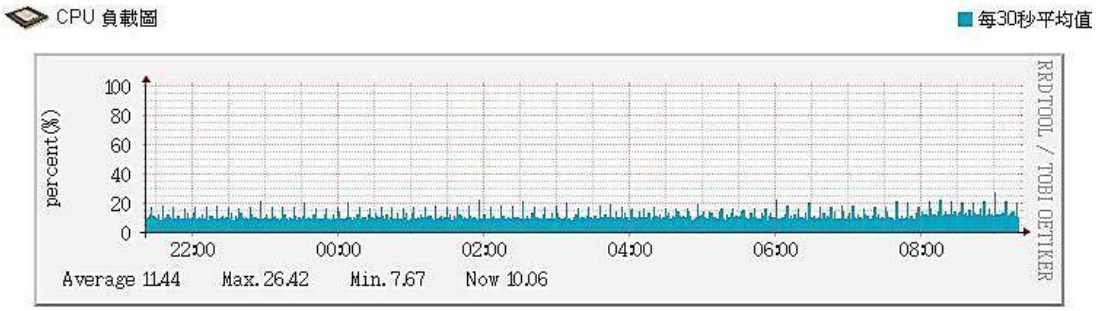


圖 15-3 系統負載

15-1-2、網路流量

於【系統效能】之【網路流量】功能中，會顯示目前 NG-UTM 所有介面過去 24 小時的網路流量，流量的統計是以介面為主，如果介面有 2 個 1G 的實體線路，滿載時，這個介面最高會顯示 2G 的流量，在顯示上藍色（圖形上方）是上傳流量，就是進入介面的流量，綠色（圖形下方）是下載流量，就是從介面出去的流量，對於是 WAN 類型的介面，他的統計流量方向跟線路提供商的上下載是不同的方向。（圖 15-4）

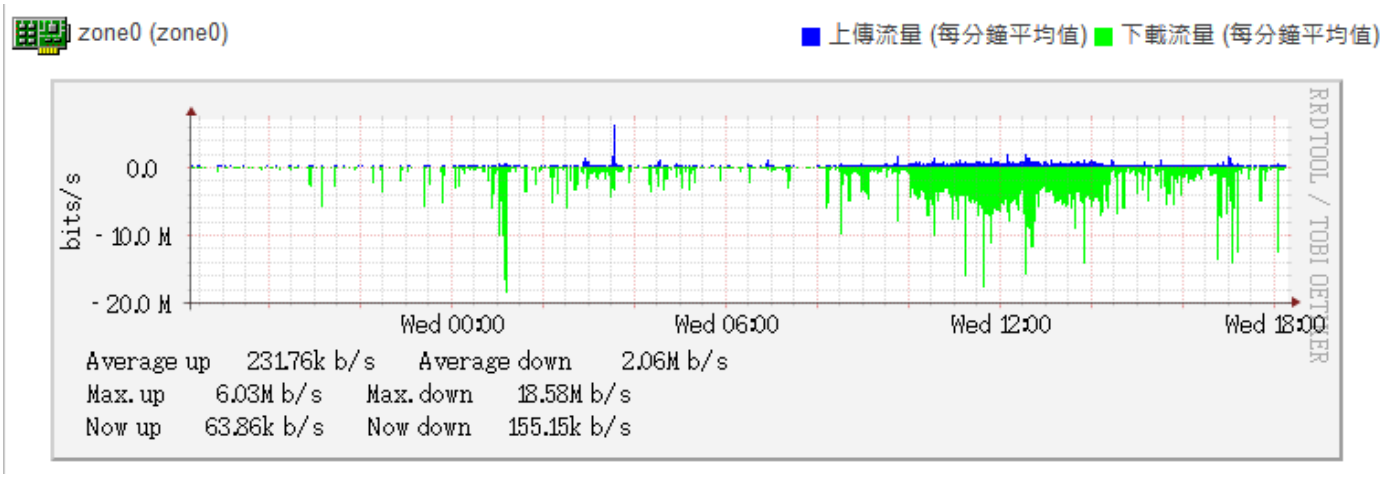


圖 15-4 網路介面流量

15-1-3、連線狀態

NG-UTM 提供過去 48 小時的上線人數跟連線數的圖表，讓管理者快速地掌握過去一段時間內的變化，當然在 15-1-4、歷史狀態中可以提供更長時間的搜尋。（圖 15-5）

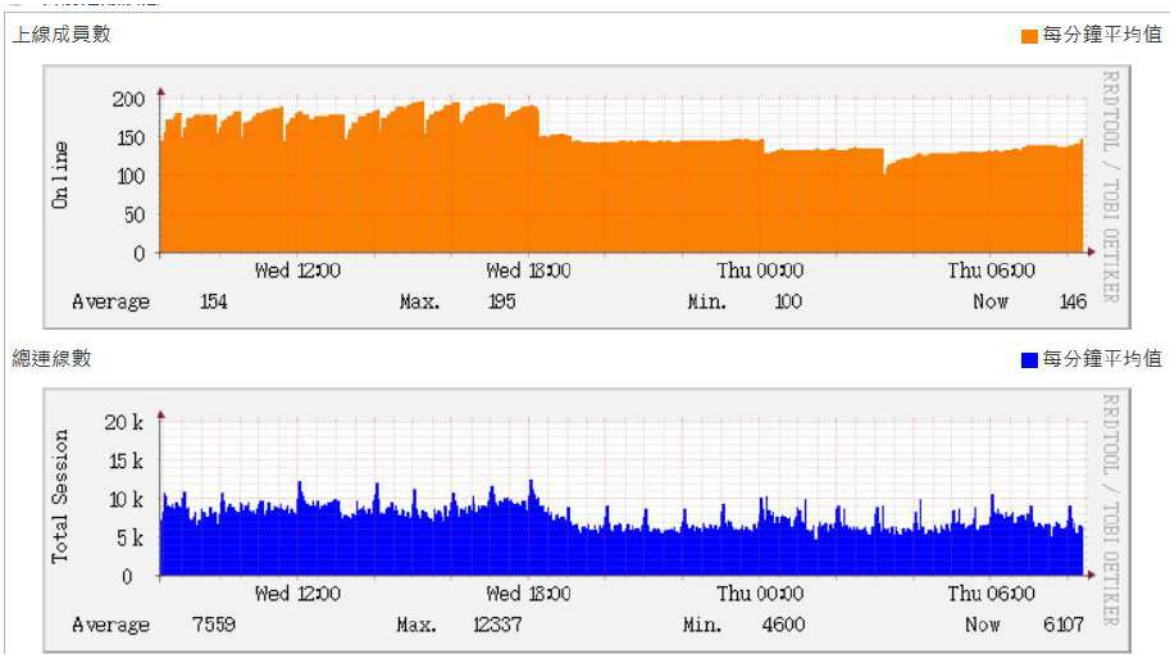


圖 15-5 過去 48 小時的連線紀錄

15-1-4、歷史狀態

顯示 CPU、RAM、系統負載跟每一個介面的歷史流量統計，管理者選擇時間區間後，NG-UTM 會自動顯示這一段時間的圖表，這個功能可以讓管理者去分析過去的哪一段時間是有問題，並從問題中找出可能的解決方式。（圖 15-6）

- 【查詢目標】：選擇要查詢的目標，目前可以選擇 CPU、RAM、系統負載跟介面流量，上線成員跟總連線數，在介面部分系統會列出所有的網路介面讓管理者勾選。
- 【日期】：選搜尋日期，例如，2015-04-05 00：00 ~ 2016-04-05 23：00 代表要查詢一年的使用情況。

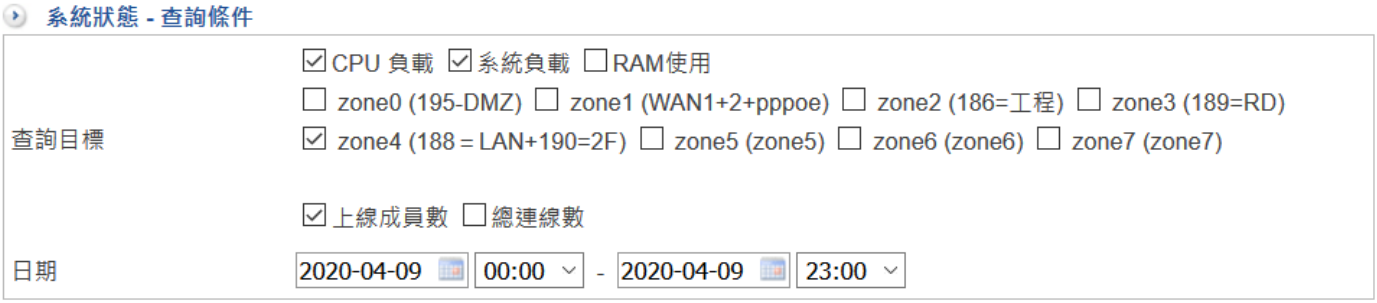


圖 15-6 歷史資料搜尋

15-1-5、介面即時流量

有別於【網路流量】功能中的過去 24 小時流量統計，這裡會顯示介面的即時流量是過去 3 分鐘的流量，不僅是可以看實體介面的即時流量，虛擬介面，例如 IP Tunnel、PPPOE 的即時流量也都可以查看，最多可以同時看 2 個介面。（圖 15-7）

流量的統計是以介面為主，如果介面有 2 個 1G 的實體線路，滿載時，這個介面最高會顯示 2G 的流量，在顯示上藍色是上傳流量，就是進入介面的流量，綠色下載流量，就是從介面出去的流量，對於是 WAN 類型的介面，他的統計流量方向跟線路提供商的上下載是不同的方向。

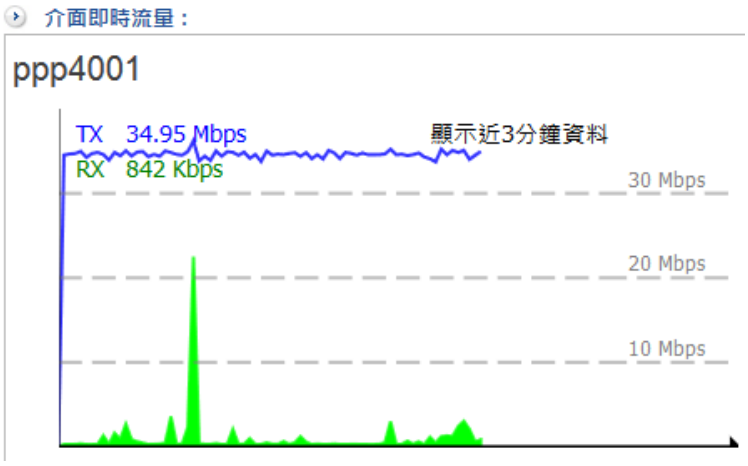


圖 15-7 即時流量

15-1-6、CPU 負載

【系統狀態】之【CPU 負載】功能中，每一個 CPU 的即時負載情況，管理者可以藉由這樣功能查知，系統資源是否有吃單顆 CPU 的情況，萬一有吃單顆 CPU 的情況時，可以從【網路設定】之【中斷設定】將他的網路流量分配到其他 CPU 中。（圖 15-8）

名稱	閒置	使用者	系統	Nice	I/O	硬中斷	軟中斷	CPU 使用率
平均負載	97.14%	1.04%	0.78%	0.26%	0.00%	0.00%	0.78%	2.86%
cpu0	96.91%	2.06%	1.03%	0.00%	0.00%	0.00%	0.00%	3.09%
cpu1	95.88%	1.03%	1.03%	1.03%	0.00%	0.00%	1.03%	4.12%
cpu2	98.95%	1.05%	0.00%	0.00%	0.00%	0.00%	0.00%	1.05%
cpu3	95.88%	2.06%	0.00%	1.03%	0.00%	0.00%	1.03%	4.12%

圖 15-8 CPU 即時統計

15-2、連線狀態

連線狀態會記錄 3 件事情，一個是成員列表、無線成員列表及連線追蹤，成員列表會記錄 7 天內(預設值)，經過 NG-UTM 的所有介面下 IP 位址資訊，連線追蹤則是詳細記錄每一個來源 IP 位址他的連線數量統計跟實際使用的封包通聯記錄，尤其是封包通聯紀錄，有經驗的管理者可以藉由連線數量跟通聯記錄判斷某一步電腦是否有問題。

15-2-1、成員列表

【連線狀態】之【成員列表】功能中，會顯示通過 NG-UTM 的介面下所有 IP 資訊，如果是內部網路下，還可以判斷是開機或是關機狀態？從那一個網路介面來？也可以按照大小排序。（圖 15-9）

- 【成員列表保留】：通過 NG-UTM 的 IP 位址要保留幾天，預設值是 7 天，設定範圍是 0 ~365，0 代表不清除這些紀錄資料。
- 【目前上線成員數】：按照網路區段統計，例如，All(141/220)，代表過去 7 天內有 220 個 IP 位址經由設定的網介面，通過 NG-UTM 到另一個介面，目前有 141 個 IP 位址上線中。
- 【介面顯示】：選擇要顯示的介面，包含實體介面跟 802.1Q 的 VLAN。
- 【名稱】：該部電腦的 NETBIOS 名稱，可以在管理目標的位址表中自定義名稱。
- 【IP 位址】：該部電腦的 IP 位址。
- 【MAC 位址】：該部電腦的 MAC 位址。
- 【介面】：該部電腦的來源介面，包含實體介面跟 802.1Q 的 VLAN。
- 【狀態】：：代表電腦開機中，：代表電腦關機中。
- 【狀態更新時間】：所有更新時間訊息。
- 【】：按照大小排序。

圖 15-9 成員列表

15-2-2、無線成員列表

在系統設定中 AP 管理加入 UTM 管理的設備，透過 AP 上網的使用者會被列表在這裡，除了可以得知 SSID 外，還可以判斷是開機或是關機狀態？從那一個 AP 來？

- 【成員列表保留】：通過 NG-UTM 的 IP 位址要保留幾天，預設值是 7 天，設定範圍是 0 ~365，0 代表不清除這些紀錄資料。
- 【目前上線成員數】：目前有幾個 IP 位址透過 AP 上線中。
- 【SSID】：AP 使用的 SSID，同一個 AP 可能會有多個 SSID。
- 【IP 位址】：該部電腦的 IP 位址。
- 【MAC 位址】：該部電腦的 MAC 位址。
- 【狀態】：：代表電腦開機中，：代表電腦關機中。
- 【狀態更新時間】：所有更新時間訊息。
- 【】：按照大小排序。

15-2-3、連線追蹤

藉由網路封包的分析及追蹤，分析每一個使用者網路使用行為，分析的資料是從電腦開機到關機，每個用戶利用網路，在幾點幾分，花了多少時間、作了哪些事情。

此主要是以來源端名稱作為分類，顯示目前所有使用者之紀錄，包含 IP 位址、連線數、上傳流量、下載流量、紀錄(紀錄所使用協定、來源 IP、目的 IP、通訊埠、上傳封包、下載封包、上傳 Bytes、下載 Bytes)。

【連線狀態】之【連線追蹤】功能中，會顯示目前 NG-UTM 內網電腦所有使用者上傳、下載流量統狀態：（圖 15-10）

- 【總連線數】：顯示當下經過 NG-UTM 的連線數，顯示的格式為 ，這個頁面連線數總和/全部連線數，例如，1245/1976，代表所有經過 NG-UTM 的總連線數為 1976 條，但在這一個頁面的統計總數是 1245 條，其他的連線數是分布在其他頁面。
- 【來源 IP 】：輸入要查看的來源 IP 位址，空白代表全部。
- 【目的 IP】：輸入要查看的目的 IP 位址，空白代表全部。
- 【電腦名稱】：顯示目前該電腦的 NetBIOS 名稱或是位址表中定義的名稱，如果都沒有則顯示 IP 位址。
- 【IP 位址】：該部電腦的 IP 位址。
- 【連線數】：該部電腦目前對外已經建立的連線數。
- 【上傳流量】：該部電腦目前的上傳流量，單位是 bps，bits/Second。
- 【下載流量】：該部電腦目前的下載流量，單位是 bps，bits/Second。

連線追蹤列表 總連線數： 1146 / 1919 來源IP 目的IP 每三十秒 立即更新

1 / 17 跳至 1 頁數，每頁 24 筆 GO

電腦名稱	IP 位址	連線數	上傳流量 bits	下載流量 bits	記錄
RANDOLL	192.168.188.126	143	4.74K	3.13K	記錄
sid	192.168.189.16	118	160.03K	199.7K	記錄
192.168.189.19	192.168.189.19	82	24.66K	18.34K	記錄
192.168.189.31	192.168.189.31	59	5.99K	42.64K	記錄

圖 15-10 連線數及流量列表

- 【立即更新 】：按下後可以馬上更新連線數資訊。

選擇要查看的電腦後，按下【紀錄】按鈕後，會出現這部電腦前 3 分鐘的詳細的封包通聯訊息，在應用程式區，NG-UTM 按照每個連線的應用程式分類。（圖 15-11）

- 【Clear all 】：清除所有的資料，重新顯示通聯封包。
- 【Refresh 】：按下後可以馬上更新通聯封包的連線數資訊。
- 【匯出 】：將資料表匯出，讓管理者可以用其他的統計方式處理。
- 【來源 IP 】：該部電腦的 IP 位址。
- 【目的 IP】：這一個連線的目的 IP 位址。
- 【通訊埠】：來源及目的通訊埠，例如，62506>53，代表來源 PORT 是 62506，目的 PORT 是 53，再從協定中用 UDP，大約可以看的出來他是 DNS 協定。
- 【上傳/下載封包】：這個連線的上傳/下載封包量，例如，37/36，代表上傳 37 個封包，下載 36 封包，再從協定 TCP 來看，這是屬於正常的封包行為，如果這 2 個數字差異很大，例如，6000/2，代表封包有去無回，2/6000 代表來的多但回不了，在這 2 種情況下，都是有問題的連線，有可能是線路品質不好或是被攻擊甚至去攻擊別人，管理者就可以注意一下這樣的電腦。
- 【上傳/下載 Bytes】：這個連線的上傳/下載量。
- 【應用程式】：這個連線是使用哪個應用程式，NG-UTM 會按照內建的 900 種 DPI 分類這些應用程式。
- 【出口線路】：這個連線是用哪一個出口線路到網際網路。
- 【管制規則】：這個連線是套用管制規則的哪一條?

refresh clear all 1 / 4 跳至 1 頁數，每頁 24 筆 匯出 匯出全部

協定	來源 IP	目的 IP	通訊埠	Zone Out (TX) 封包	Zone In (RX) 封包	Zone Out (TX) Bytes	Zone In (RX) Bytes	應用程式	出口線路	管制規則
tcp	192.168.190.106	103.243.172.110	58938 -> 443	11	18	22.47K	221.01K		-	-
tcp	192.168.190.106	103.243.172.110	58963 -> 443	7	4	13.94K	44.07K	Online Certificate Status Protocol	wan1 (zone1)	Outgoing [30] 2F-190
udp	192.168.190.106	108.177.97.156	53153 -> 443	19	18	42.59K	76.13K	Google.com	Wan2 (zone1)	Outgoing [30] 2F-190
tcp	192.168.190.106	210.176.156.41	58813 -> 443	26	32	164.95K	103.24K	Online Certificate Status Protocol	Wan2 (zone1)	Outgoing [30] 2F-190
tcp	192.168.190.106	31.13.87.38	58783 -> 443	142	249	266.96K	3.21M	Facebook	Wan2 (zone1)	Outgoing [30] 2F-190

圖 15-11 使用者連線狀態

15-3、流量分析

NG-UTM 提供流量的統計分析，可以讓管理者按照流量、應用程式或者是 TCP Port 來查看每一個 IP 的使用狀況。

15-3-1、流量排行

流量排行能讓管理者查詢每一個使用者使用網路的狀況並依照使用流量排序，點選每個使用者後可以看到使用的應用程式等資訊。

- 【預設載入時間範圍】：點選流量排行頁籤後系統根據設定的時間範圍統計，預設是今天(從 00:00 ~)，另一個選項是只統計最近 1 個小時的資料，如果資料多會延遲開啟網頁的時間，管理者可以選第 3 個選項，不顯示，則進入流量排行時系統不會出現任何統計數字，按下【變更】按鈕後，馬上切換。
- 【連線類型】：統計資料是以來源 IP 位址或是目的 IP 位址統計排序，切換後按下【搜尋】按鍵就切換統計方式。
- 【統計方式】：使用 IP 位址或是上網認證的帳號為統計基礎，預設是 IP 位址。
- 【時間範圍】：統計的時間範圍，只有今天跟 1 個小時 2 個選項。（圖 15-12）

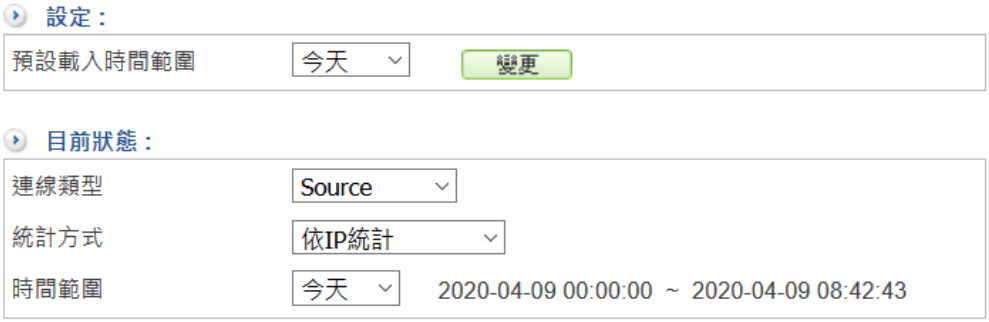


圖 15-12 流量排行統計條件

選擇搜尋條件後所有透過 NG-UTM 流量的統計資訊會列表，可以在連線類型中指定按照來源 IP 位址統計或是目的 IP 位址統計，預設是用來源 IP 位址統計，如果有套用上網認證部分，也可以利用帳號來分析。（圖15-13）

- 【電腦名稱】：電腦的 NETBIOS 名稱。
- 【IP 位址 】：電腦的 IP 位址。
- 【MAC 位址 】：電腦的 MAC 位址。
- 【上網認證】：這個 IP 位址有使用上網認證就會顯示帳號，如果沒有就是空白。
- 【上傳流量 KBytes】：累積的上傳量，單位為 K/M/G bytes。
- 【下載流量 KBytes】：累積的下載量，單位為 K/M/G bytes。

電腦名稱	IP 位址	MAC 位址	上網認證	上傳流量	下載流量
JEAN-PC	192.168.190.70	1c:6f:65:ab:54:1f		97.67 MB	3.48 GB
192.168.190.116	192.168.190.116	08:35:71:ea:c2:dd		45.66 MB	1.54 GB
192.168.188.126	192.168.188.126	1c:6f:65:d2:e0:18		204.43 MB	1.25 GB

圖 15-13 使用者流量排行

在列表中，點選任一個電腦或是 IP 位址，就可以更詳細察看，上、下載流量是被那些應用程式或是通訊協定佔用比例。（圖15-14）

時間範圍：2020-04-09 08:00:00 ~ 2020-04-09 09:00:00
來源 IP：192.168.186.199　資料類型：基本服務　IP 地區(目的)　應用程式

基本服務	上傳流量		下載流量		封包紀錄
SSH	38.76 MB	99%	1.95 GB	100%	記錄
HTTPS	180.89 KB	< 1%	463.01 KB	< 1%	記錄
DNS	9.34 KB	< 1%	33.28 KB	< 1%	記錄
HTTP	15.47 KB	< 1%	16.05 KB	< 1%	記錄
7680	0.37 KB	< 1%	0.29 KB	< 1%	記錄

圖 15-14 使用者流量分析

- 【時間範圍】：統計流量的時間範圍。
- 【IP 位址 】：根據來源或是目的 IP 位址為統計。
- 【資料類型 】：有 2 種，基本服務跟應用程式分類，管理者可以用右邊的切換按鈕切換，如果這裡出現的是【基本服務】則切換按鈕是【應用程式】，反之亦然。
- 【IP 地區(目的)】：顯示來源 IP 位址到訪的目的主機所在的地區，點選後下面的列表就會切換成 IP 目的地區。
- 【基本服務/應用程式】：顯示服務的種類，基本服務就會用 http/https，應用程式就是用 LINE、SKYPE 等。

點選每個顯示列表的【紀錄】按鈕，NG-UTM 顯示這個統計項目的更詳細資訊，如每個時間段的上、下載流量，出口線路跟使用的管制條例。（圖 15-15）

- 【持續時間】：某個連線的時間長度。
- 【上、下傳流量】：某個連線累積的上、下載流量。
- 【出口線路】：使用哪個出口線路。
- 【管制規則】：流量是使用哪個管制條例。

時間範圍：2018-06-21 00:00:00 ~ 2018-06-21 17:42:12

來源 IP：192.168.190.116　　基本服務：HTTPS　　返回

1 / 321　跳至 1 頁數、每頁 16 筆 GO　匯出　匯出全部

日期	持續時間 (s)	協定	來源 IP	目的 IP	通訊埠	上傳流量	下載流量	出口線路	管制規則
2018-06-21 03:10:11	41	tcp	192.168.190.116	139.162.97.147	48851->443	2.04 KB	4.48 KB	wan1 (zone1)	Outgoing [30] 2F-190
2018-06-21 07:38:23	42	tcp	192.168.190.116	52.229.171.202	6445->443	2.01 KB	5.81 KB	Wan2 (zone1)	Outgoing [30] 2F-190
2018-06-21 07:38:24	166	tcp	192.168.190.116	40.77.228.242	50432->443	11.22 KB	52.62 KB	Wan2 (zone1)	Outgoing [30] 2F-190
2018-06-21 07:38:24	165	tcp	192.168.190.116	40.77.228.242	59262->443	12.84 KB	98.03 KB	wan1 (zone1)	Outgoing [30] 2F-190
2018-06-21 07:38:24	40	tcp	192.168.190.116	23.103.189.158	6447->443	1.02 KB	4.39 KB	Wan2 (zone1)	Outgoing [30] 2F-190

圖 15-15 詳細的通聯記錄

15-3-2、流量排行列表 By Port

顯示NG-UTM 整台的在統計時間範圍內總通訊協議流量排行榜，例如，用 HTTP (TCP 80)、HTTPS(TCP 443)統計使用的總量，並列成排行榜，流量分別可以用上傳、下載流量進行排序。（圖15-16）

1 / 552 跳至 1 頁數，每頁 16 筆 GO 匯出 匯出全部

名次	服務埠號	上傳流量	下載流量
1	HTTP	793.45 MB	32.96 GB
2	HTTPS	1.00 GB	9.62 GB
3	IMAP	88.71 MB	3.72 GB
4	888	1.49 GB	2.04 GB
5	1998	267.60 MB	1.02 GB
6	DNS	3.30 GB	1,022.04 MB
7	SSH	21.61 MB	761.95 MB

圖 15-16 Port 流量統計

15-3-3、流量排行列表 By APP

顯示NG-UTM 整台的在統計時間範圍內總應用程式流量排行榜，例如，用 LINE、HTTPS跟 SKYPE 等使用的總量，並列成排行榜，流量分別可以用上傳、下載流量進行排序，NG-UTM 預設不會顯示無法辨識的應用程式，管理希望顯示無法辨識的應用程式，則需要勾選【顯示Unknown】。（圖15-17）

1 / 552 跳至 1 頁數，每頁 16 筆 GO 匯出 匯出全部

名次	應用程式	上傳流量	下載流量
1	HTTP	793.45 MB	32.96 GB
2	HTTPS	1.00 GB	9.62 GB
3	IMAP	88.71 MB	3.72 GB
4	888	1.49 GB	2.04 GB
5	1998	267.60 MB	1.02 GB
6	DNS	3.30 GB	1,022.04 MB
7	SSH	21.61 MB	761.95 MB

圖 15-17 APP 流量統計

15-3-4、流量排行列表 By Location

顯示 NG-UTM 整台的在統計時間範圍內目的 IP 位址的地區資訊，並根據地區統計總使用量。

15-3-5、流量排行查詢

查詢前 10 ~ 500 名的使用者，排行項目如下：

1、日期

2、連線類型：分來源跟目的 2 種連線類型。

3、來源 IP 跟目的 IP 位址及 Port。

4、上網認證帳號。

5、應用程式。

6、IP 地區。

7、出口線路。

預設，系統會顯示前 10 名的列表。（圖15-18）

查詢結果：

查詢排名	前 10 名
日期	2018-06-22 00:00:00 ~ 2018-06-22 23:00:00

電腦名稱	IP 位址	MAC 位址	上網認證	上傳流量	下載流量
192.168.191.187	192.168.191.187	*		1.84 GB	356.20 MB
59.125.127.22	59.125.127.22			7.31 MB	354.05 MB
192.168.100.252	192.168.100.252			70.29 MB	347.54 MB
59.125.95.19	59.125.95.19			7.04 MB	334.23 MB

圖 15-18 流量排行搜尋

15-3-6、流量配額

在管制條例中設定每個 IP 位址能使用的流量總額，當使用者超過這個限制後，可以在這裡查詢。

15-3-7、DNS查詢排行查詢

DNS 是網路連線的第一個動作，藉由統計 DNS 的紀錄可以知道對外連線的目的，甚至可以藉此找到不合法的網路行為。選擇查詢日期及統計方式就完成，有3種統計方式。

1、 依域名

依照內部對外 DNS 查詢最多的域名統計，在特定時間內網域跟次數列表。（圖15-19）

查詢結果：

查詢排名	前 10 名
日期	2019-10-04 00:00:00 ~ 2019-10-04 23:00:59

域名	查詢次數
public.sarbl.org	53306
uribl.spameatingmonkey.net	19709
1.0.0.127.bl.spamcop.net	15297
1.0.0.127.sbl.spamhaus.org	13360
multi.uribl.com	12160
1.0.0.127.zen.spamhaus.org	11945

圖 15-19 網域跟次數

2、 依 DNS 伺服器

以照使用的 DNS 伺服器排名。（圖 15-19）

查詢結果：

查詢排名	前 10 名
日期	2019-10-04 00:00:00 ~ 2019-10-04 23:00:59

DNS 伺服器	查詢次數
8.8.8.8	190272
168.95.1.1	188900
69.164.195.45	9247

圖 15-19 DNS 伺服器跟次數

3、 以來源IP

內部哪一個 IP 用 DNS 查詢的次數最多。（圖 15-20）

查詢結果：

查詢排名	前 10 名
日期	2019-10-04 00:00:00 ~ 2019-10-04 23:00:59

來源 IP	查詢次數
192.168.191.169	76850
192.168.195.49	42827
192.168.195.53	35060

圖 15-20 內部的 DNS 查詢次數

第 16 章、Dashboard

NG-UTM 的 Dashboard 提供跟傳統 UTM 不一樣的數據呈現方式，以圖形的方式，提供網路流量、內容及駭客攻防紀錄等資訊，並以 Drill Down 的方式，提供管理者找出問題的根源。

目前 Dashboard 提供下列幾個模塊，Application(應用程式分析)、Mail(郵件分析)、IPS、Web(網頁流量)、Defense(駭客攻防紀錄)跟 Session(即時連線)，進入 Dashboard 的首頁，上方是每一個模塊的切換，其中功能配置是切回傳統的管理介面。

在動態顯示的圖形上，預設是統計所有的數量後再去計算他佔的比例，如果管理者想要剔除某些資料量不要讓他進入總量的統計，只要點選該項目，則 NG-UTM 就會自動剔除他的資料量並重新統計他的數量分配。

16-1-1、威脅情報

威脅情報把目前 NG-UTM 的攻防紀錄用簡單明白的方式讓管理者知道整個狀況，分成 2 大區塊，即時攻防資訊跟歷史的攻防資訊，即時資訊把最近的攻擊列表出來，歷史部分則依照約月份把病毒防護、垃圾防護、IPS、防火牆防護跟各種管制羅列出來，同時跟上個月做一個簡單的比較。（圖 16-1）

圖 16-1 威脅情報 Dashboard

首頁的威脅情報是概約式的統計，如果要看更詳細的資訊，點擊上方的威脅情報圖示，有更完整的資訊，如果想把統計資料以 PDF 或是 PNG 的方式呈現，右上角的 PDF 跟 PNG 圖示點擊後系統就會將資料匯出指定格式。

16-1-2、流量分析(Applications)

NG-UTM 是以 DPI 為建構的基本核心，每一個進出設備的網路連線都會被辨識他使用的應用程式並統計他的使用量，Dashboard 的 Application 就會將這一些統計數據已圖形介面呈現，（圖 16-2）。

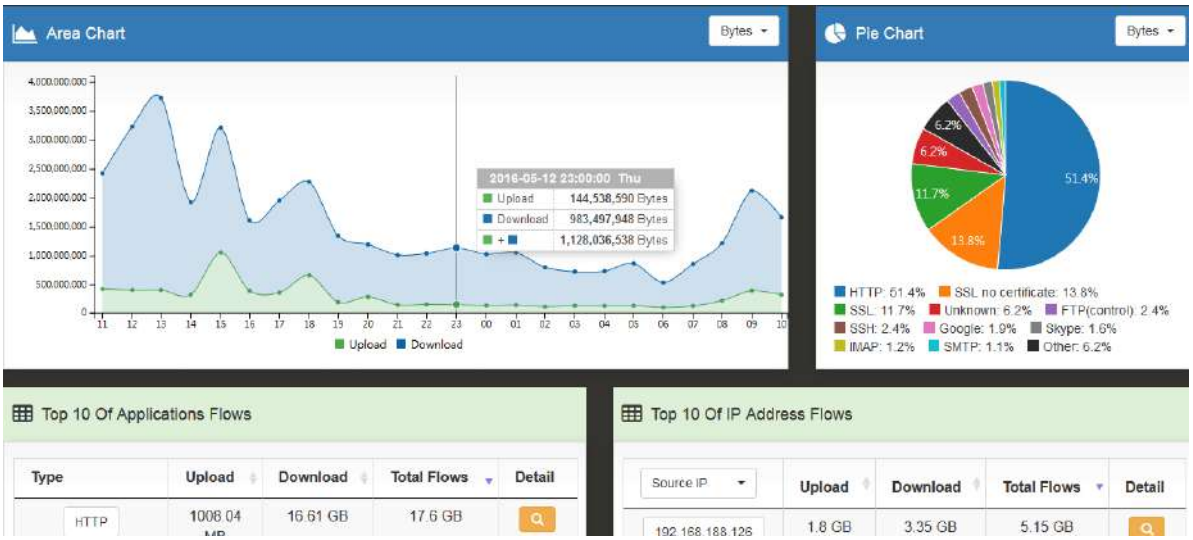


圖 16-2 Applications 的 Dashboard

- 【Area Chart】：過去 24 小時內，以小時為基本單位，進出 NG-UTM 的所有流量(上傳/下載)總和的統計，點選每個小時的統計數字後，Dashboard 會列出這一個小時內所有應用程式的使用量分配，如（圖 16-3）。

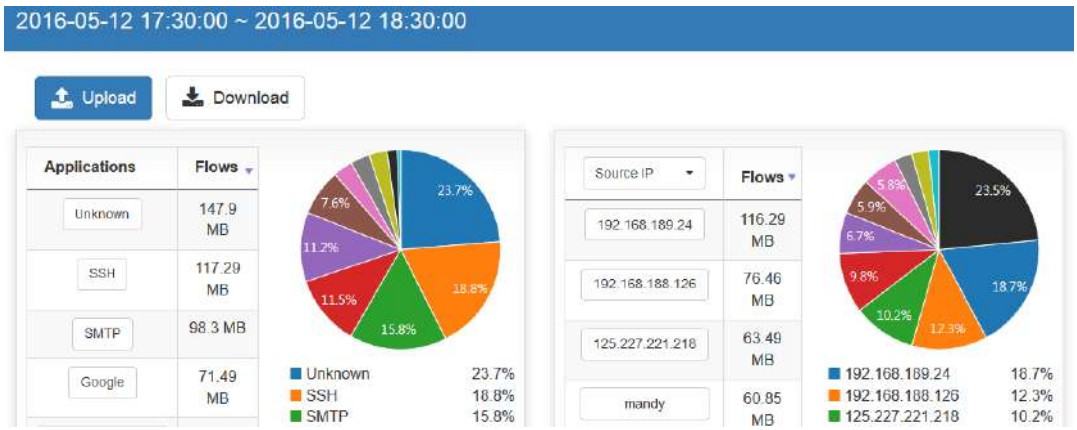


圖 16-3 每小時的應用程式使用量分析

以上圖為例，點選 18 點的流量，系統會自動統計 17:30~18:30 經過 NG-UTM 的上傳跟下載流量，並根據使用的應用程式跟來源 IP 位址進行分類，點選表列的應用程式或是來源 IP 位址，可以繼續 Drill Down 更詳細的資訊。

- 【Pie Chat】：每一個應用程式的分布比例。
- 【Top 10 of Applications Flow】：列出過去 24 小時內前 10 種使用量最多的應用程式，點選應用程式的種類，系統會自動分析這一個應用程式在過去 24 小時內他的分布。

點選每個應用程式 Detail 中的 圖示  ，進入更詳細的統計分析，以點選 SSH 為例，NG-UTM 會統計過去 24 小時內，哪一些來源或是目的 IP 位址的使用者用過這一個應用程式或者是這個應用程式使用的 Port 分布，如（圖 16-4）。

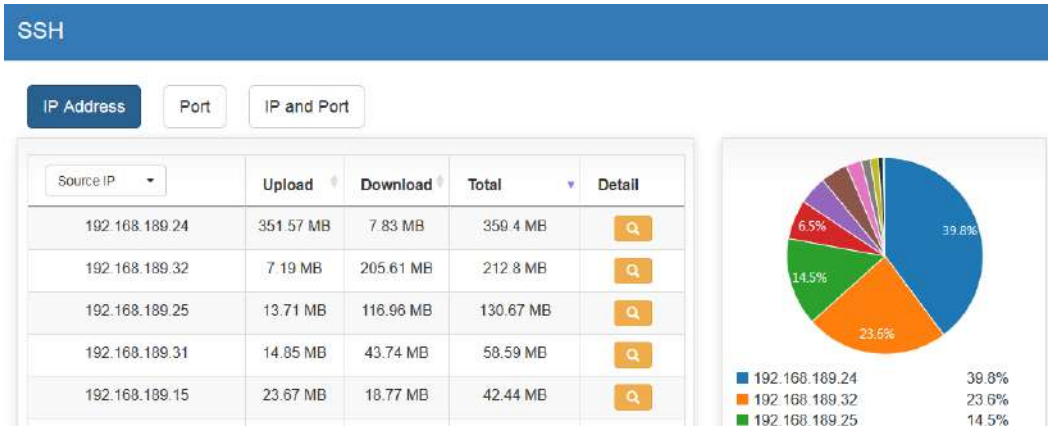


圖 16-4 應用程式使用量分析

再點選每個 IP 位址後 Detail 中的 圖示 ，則會顯示這一個來源 IP 位址使用 SSH 到哪裡，他的使用量分別是多少，如（圖 16-5）。

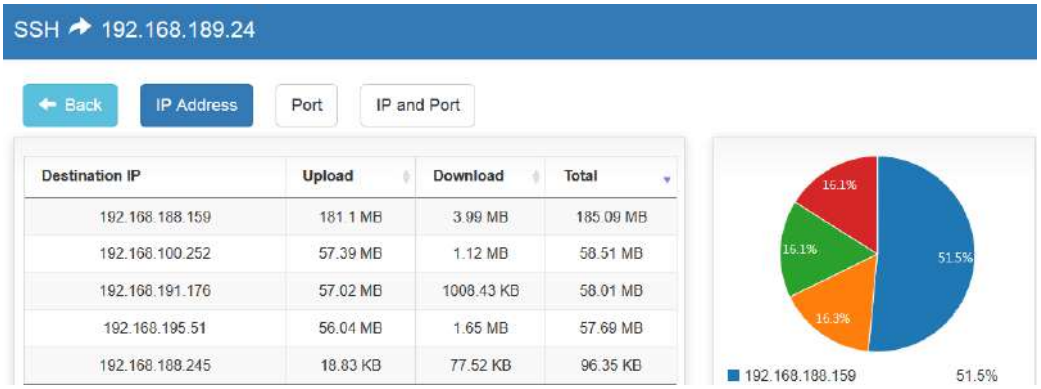


圖 16-5 應用程式來源目的 IP 位址使用量分析

- 【Top 10 of Address Flow】：列出過去 24 小時內前 10 名使用量最大的來源或是目的 IP 位址，點選 IP 位址後，系統會自動分析這一個 IP 位址在過去 24 小時內他的使用量分布，跟前面的以應用程式分類的查詢方式一樣，只不過這個地方是以來源/目的 IP 位址為查詢依據，例如，來源 IP 位址 192.168.188.126 的使用者在過去 24 小時內用過哪一些應用程式，這一些應用程式的使用量是多少?

16-1-3、連線狀態

NG-UTM 能看到所有經過的即時連線數，並根據應用程式分類每一個應用程式跟統計每一個來源 IP 位址的即時連線數量，這個功能最容易找出當下連線異常的使用者，如（圖 16-6）。

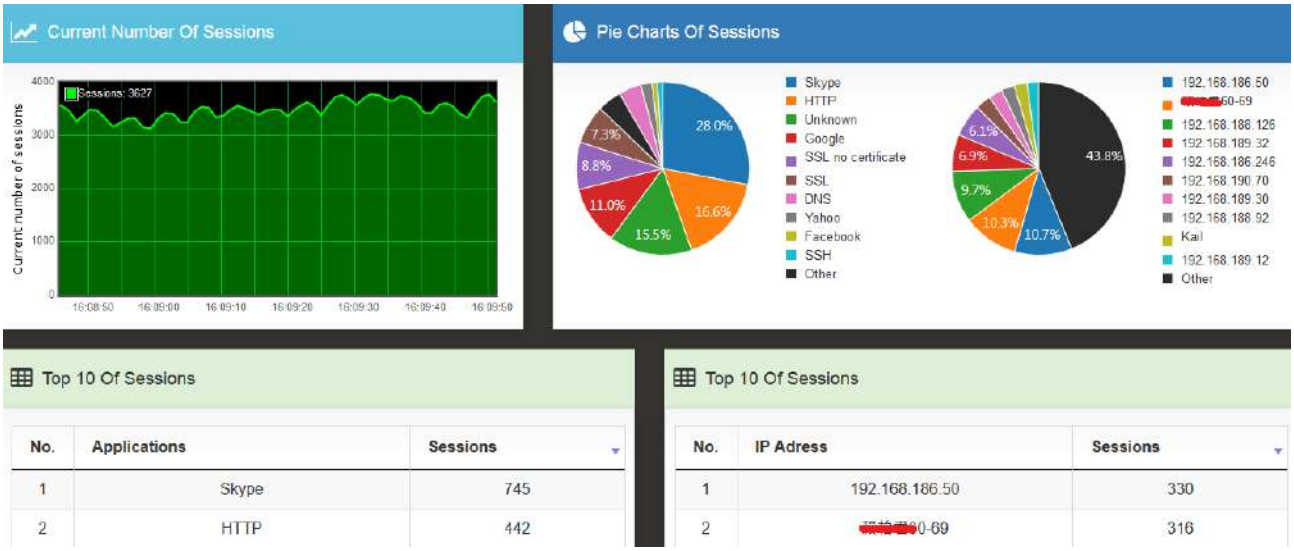


圖 16-6 即時連線數統計

- 【Pie Chart】：根據應用程式跟連線數量統計，並顯示它的分布比例。

16-1-4、防火牆防護

要讓 NG-UTM 能看到 Defense (駭客攻防紀錄)的統計資訊有幾個地方需要事先啟用。

1. 【管理目標】>【防火牆功能】中其他項目必須要有勾選。

2. 系統預設會統計針對本機的駭客攻防紀錄進行統計，當管理者在【管制條例】使用者進出網路的介面，有一條條例是套用防護設定，則 Dashboard 也會統計這一些紀錄。

滿足上面 2 個條件後，NG-UTM 就會自動執行統計分析，在 Dashboard 點選 Defense 就會看到，如（圖 16-7）。

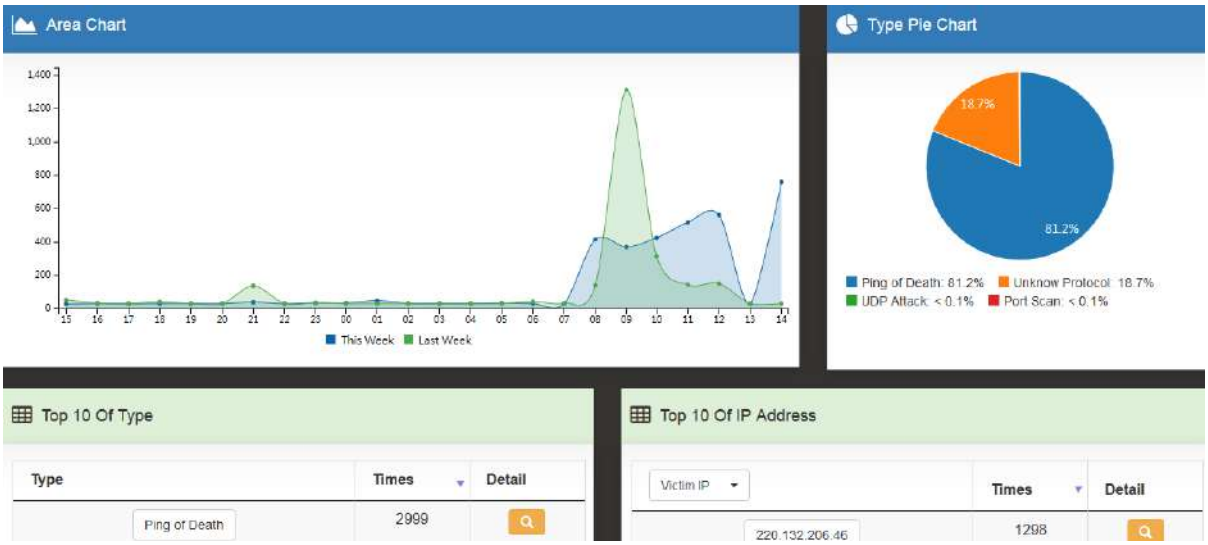


圖 16-7 防火牆攻防紀錄

- 【Pie Chart】：根據攻擊種類分類，並顯示它的分布比例。
- 【Top 10】：共有 2 種分類，分別是攻擊種類跟攻擊/受駭的 IP 位址，點選每一樣的圖示  ，都可以繼續 Drill Down 更詳細的資訊，下圖為例（圖 16-8）。

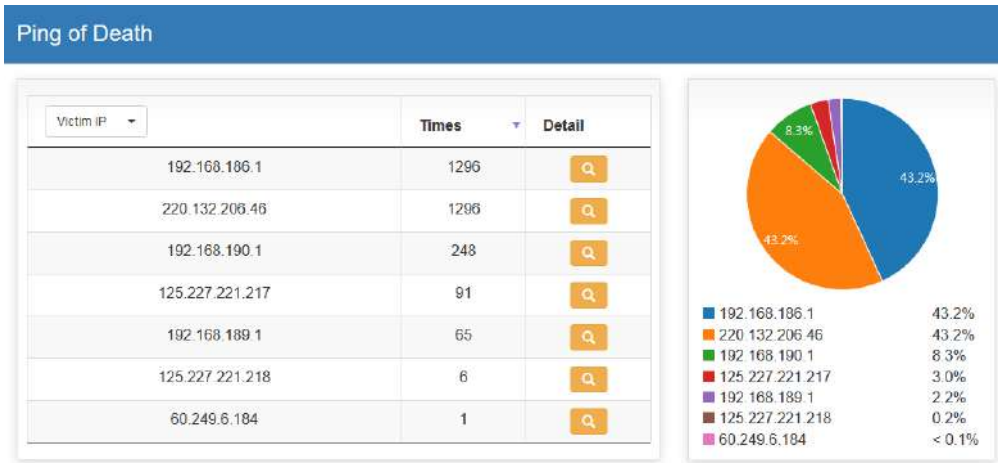


圖 16-8 防火牆詳細紀錄

16-1-5、IPS

要讓 NG-UTM 能看到 IPS 的統計資訊有幾個地方需要事先啟用。

1. 【IPS】>【IPS 設定】中至少要啟用紀錄功能

2. 【管制條例】使用者進出網路的介面，必須要有一條條例是套用在 IPS 設定的項目。

滿足上面 2 個條件後，NG-UTM 就會自動執行統計分析，在 Dashboard 點選 IPS 就會看到，如（圖 16-9）。

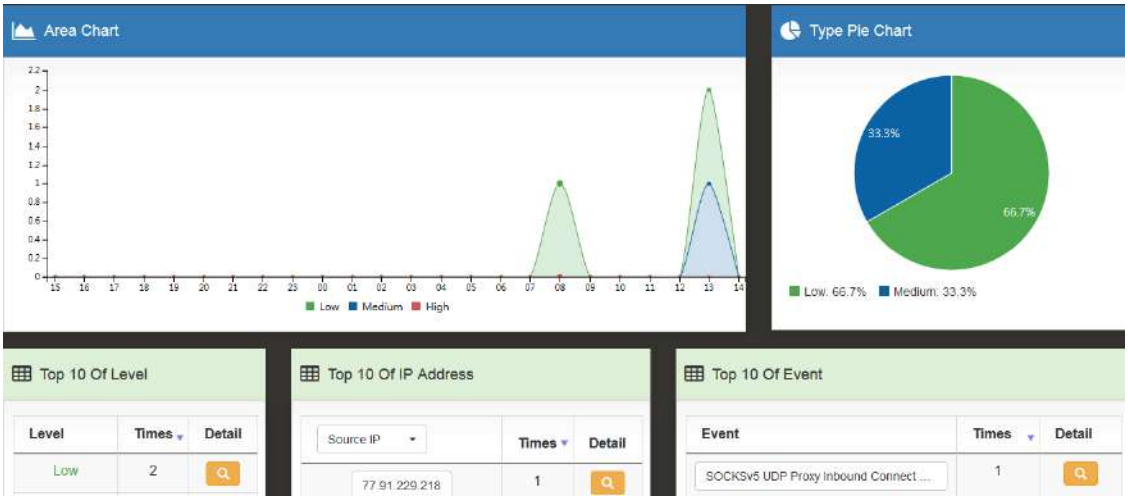


圖 16-9 IPS 的統計

- 【Pie Chart】：根據特徵值的風險程度分類，分成高、中、低 3 種，並顯示它的分布比例。
- 【Top 10】：共有 3 種分類，依據分險等級、攻擊或是受害的 IP 位址及攻擊種類，點選每一樣的圖示  ，都可以繼續 Drill Down 更詳細的資訊，下圖為例（圖 16-10）。

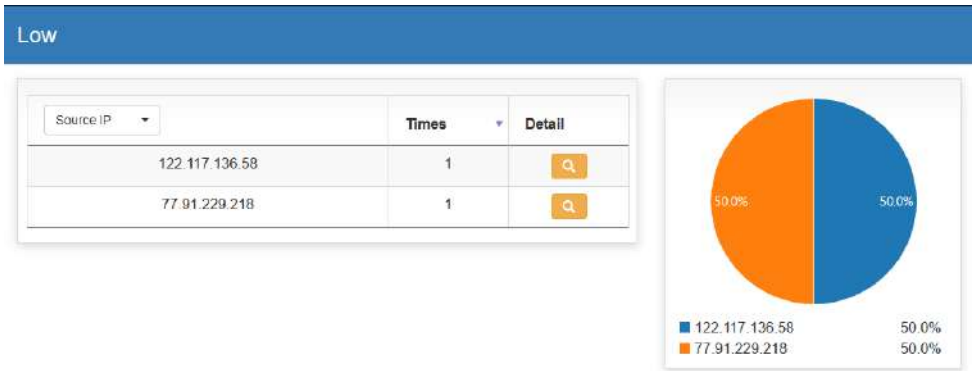


圖 16-10 IPS 攻防詳細資料

16-1-6、Web 服務

要讓 NG-UTM 能看到 Web 的統計資訊有一個地方需要事先啟用。

1.【管制條例】使用者進出網路的介面，必須要有一條條例有勾選 Web 紀錄的項目。

滿足上面 條件後，NG-UTM 就會自動執行統計分析，在 Dashboard 點選 Web 就會看到，如（圖 16-11）。

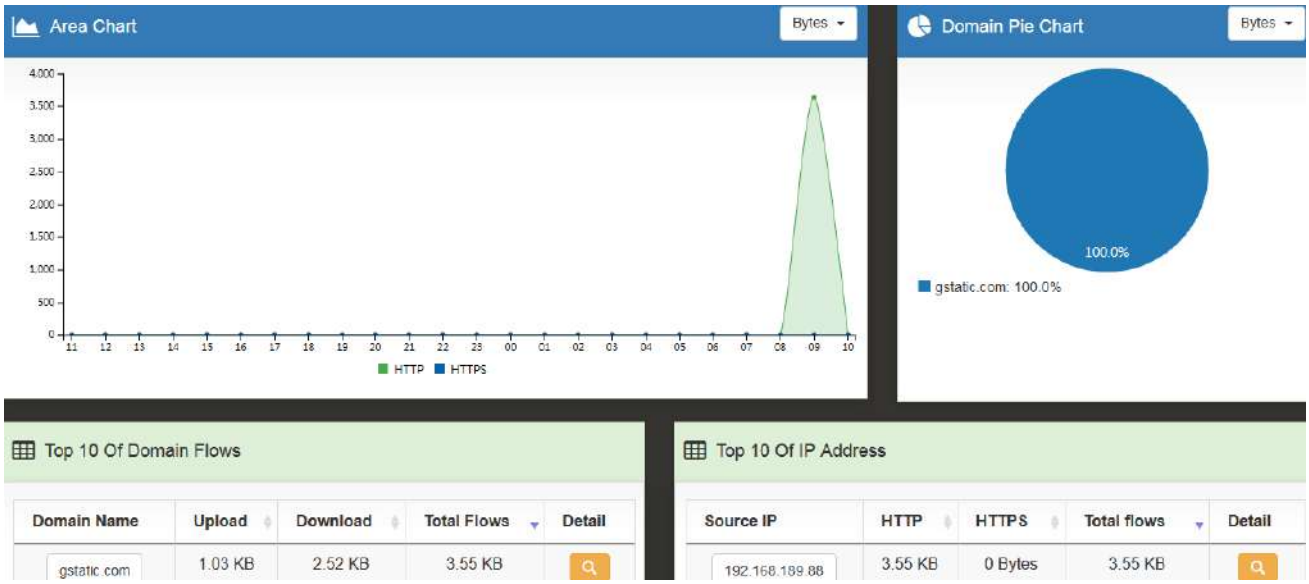


圖 16-11 Web 的統計

- 【Pie Chart】：根據 Web(包含 HTTP 跟 HTTPS 的總和)網站分類，並顯示它的分布比例。
- 【Top 10】：共有 2 種分類，分別是造訪網站的前 10 名跟使用 WEB 量的前 10 名，點選每一樣的圖示  ，都可以繼續 Drill Down 更詳細的資訊，下圖為例（圖 16-12）。

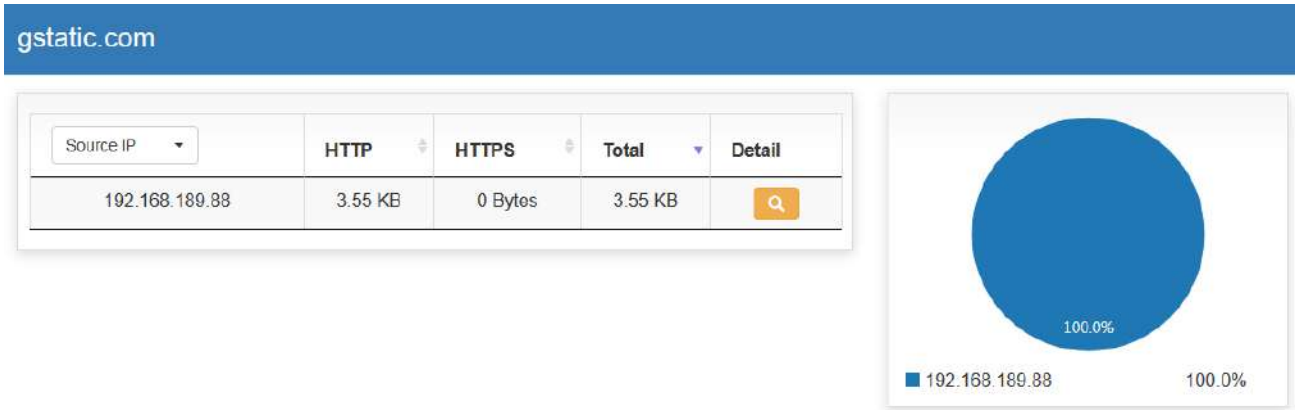


圖 16-12 Web 的詳細分布

16-1-7、Web Control

要讓 NG-UTM 能看到 Web 的統計資訊有一個地方需要事先啟用。

1.【管制條例】使用者進出網路的介面，必須要有一條條例有勾選 Web 紀錄的項目。

滿足上面 條件後，NG-UTM 就會自動執行統計分析，在 Dashboard 點選 Web 就會看到，如（圖 16-13）。

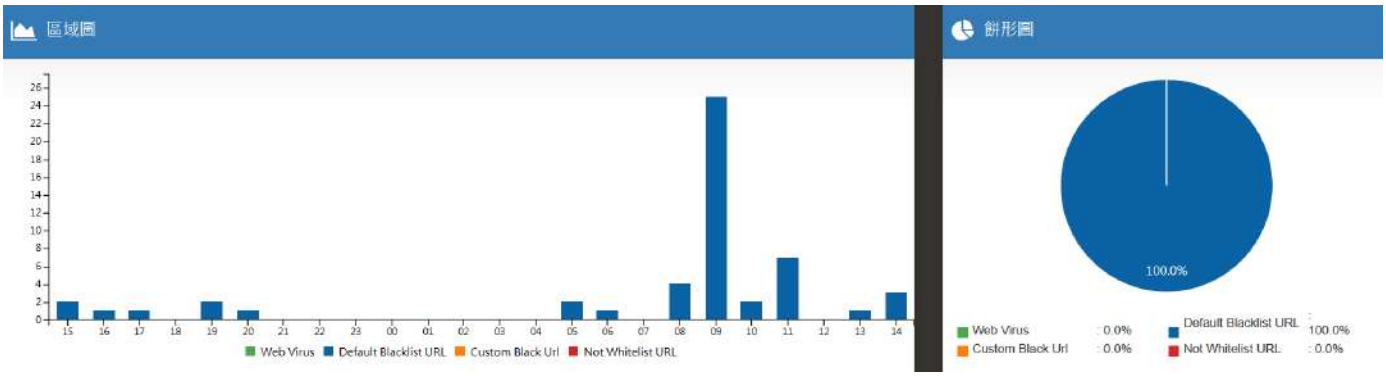


圖 16-13 Web 的統計

- 【Pie Chart】：根據 Web(包含 HTTP 跟 HTTPS 的總和)觸發黑名單資料庫或是惡意程式的網址，做出統計。

16-1-8、郵件服務

要讓 NG-UTM 能看到 MAIL 的統計資訊有幾個地方需要事先啟用。

1. 【郵件管理】>【垃圾郵件過濾】中【垃圾郵件處理方式】必須啟用其中一樣，如果管理者不想改變原有的機制，只想作分析用，則可以選僅作資料分析。

2. 【管制條例】使用者進出網路的介面，必須要有一條條例是啟用 SMTP 紀錄。

滿足上面 2 個條件後，NG-UTM 就會自動執行統計分析，在 Dashboard 點選 Mail 就會看到，如（圖 16-14）。

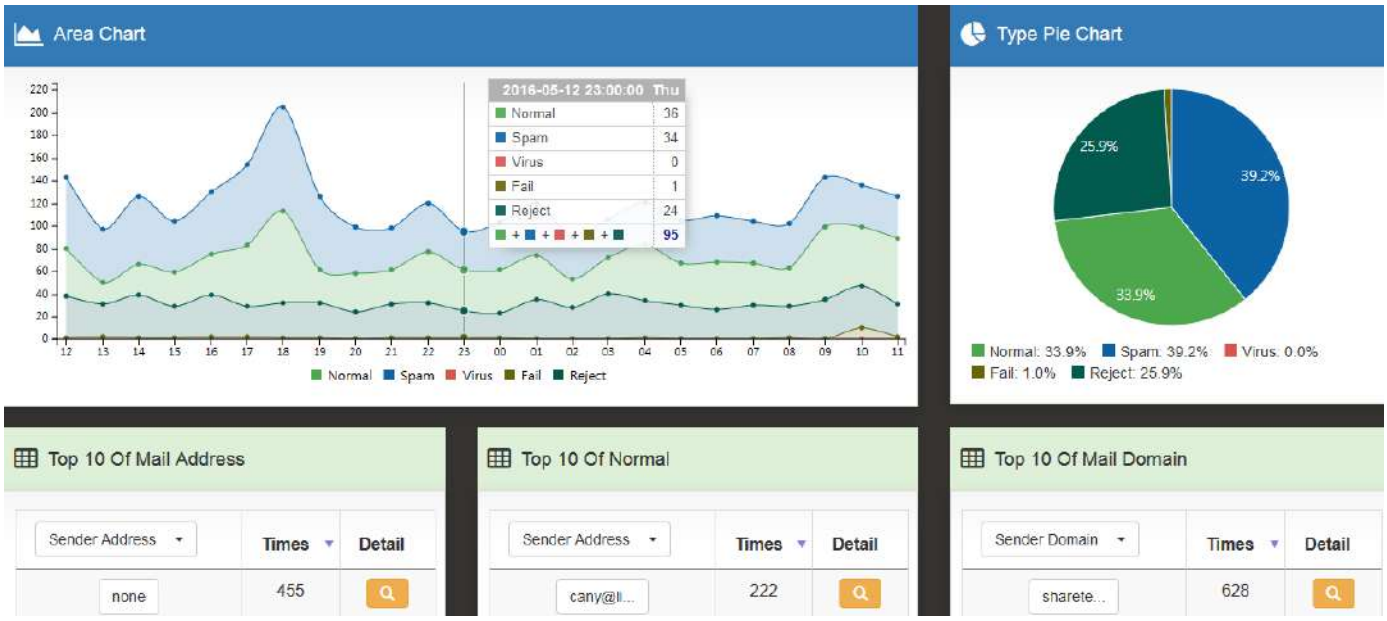


圖 16-14 Mail 使用量分析

■ 【Area Chart 】：過去 24 小時內，以小時為基本單位，進出 NG-UTM 的所有郵件總和的統計，他顯示正常郵件、垃圾郵件、病毒郵件、連線失敗跟拒絕對方連線的統計數值，點選每個小時的統計數字後，Dashboard 會列出這一個小時內所有郵件的使用量分配，如（圖 16-15）。

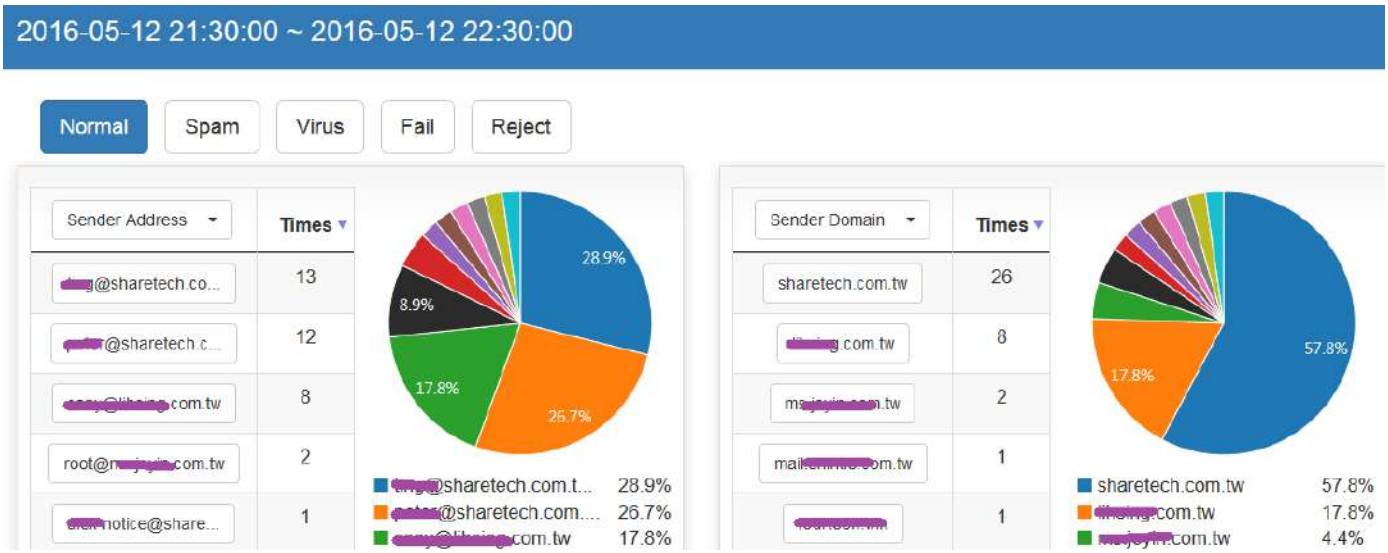


圖 16-15 每小時 Mail 使用量分析

點選郵件每一個項目都可以繼續追查更詳細的使用情況。

■ 【Pie Chart】：正常郵件、垃圾郵件、病毒郵件、連線失敗跟拒絕對方連線這 5 種郵件的統計分析。

■ 【Top 10】：共有 7 種 Top 10 的統計分析，點選每一樣的圖示  ，都可以繼續 Drill Down 更詳細的資訊，下圖為例（圖 16-16），可以呈現寄件者 Peter@sharetech.com.tw 寄給 hotmail.com 中 sharetech-peter@hotmail.com 的帳號，他寄信時間、主旨、大小等資訊。

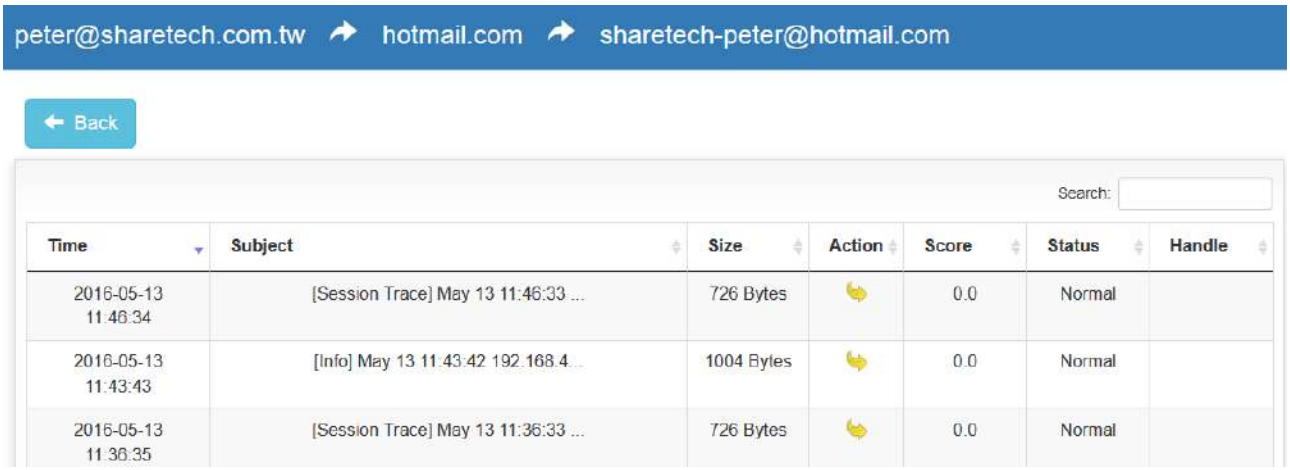


圖 16-16 Mail 原始資訊

16-1-9、IP 地區

統計透過 NG-UTM 的目的跟來源地區依照國家別。（圖 15-36）。

圖 16-17 IP 地區查詢

16-1-10、DNS 查詢

統計透過 NG-UTM DNS 查詢的目的跟使用的 DNS 伺服器。（圖 16-18）。

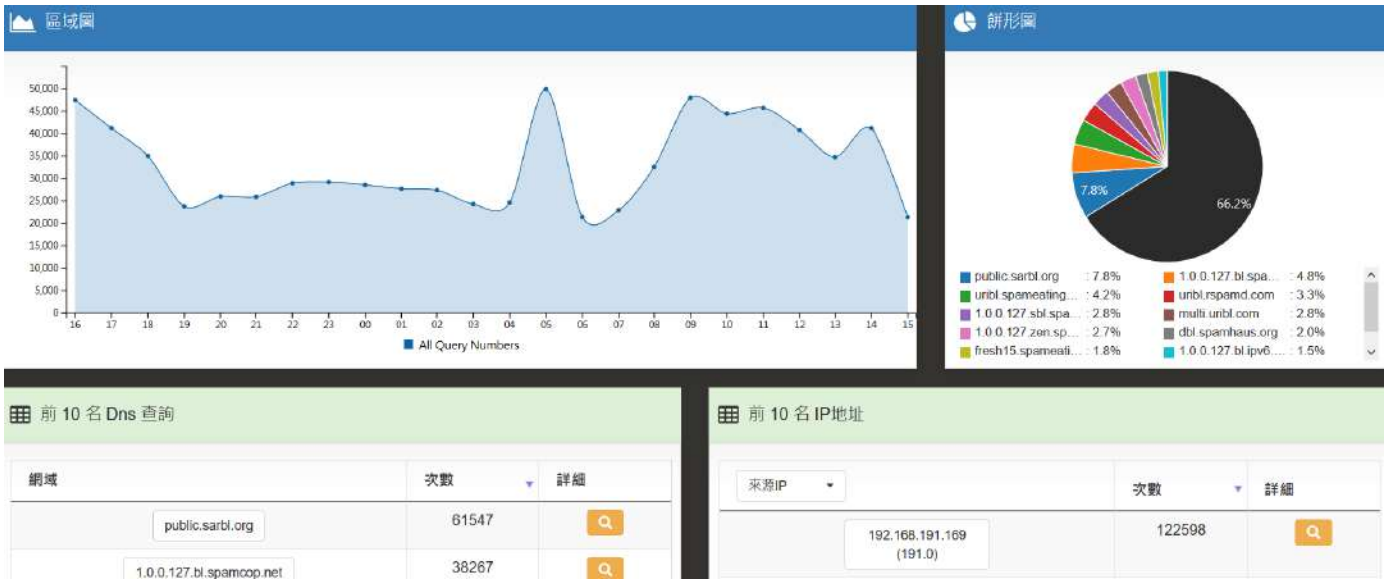


圖 16-18 DNS 查詢