內網防火牆使用手冊

章節:

第1章 安裝與訊息

1-1、硬體資訊

INF 硬體外部介面說明 ：

圖 1. 圖1-1 INF 接孔、指示燈說明¶

【LCD 顯示板】：
當設備開機完成後，顯示本機的型號、IP 位址及各項服務的啟用狀態，同時提供設備的基本命令，例如：啟用 SSH、重置管理帳號密碼跟 IP 位址、設備重新開機及關機等。

【MGMT】：
預設的管理介面，可以當作一個內網的介面使用 (LAN)，但不可以更改成 WAN、HA 或是 Bridge 介面。

【Console Port】：
使用 RS-232 的方式連接系統，提供設備基本管理命令，例如：查看網路介面、恢復出廠設定值並重置成預設的管理帳號及密碼。

【USB Port】：
透過 USB 儲存設定檔。萬一設備發生意外狀況導致無法正常運作，可透過 USB 裝置進行設定檔快速復原。

【Power LED】：
當 LED 亮綠色燈時，表示系統正在開機狀態，需大約一分鐘完成系統開機程序。

【HardDisk LED】：
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。

【Port 1~8】：
自訂網路區域。如果某個區域需要數個交換機 port，把數個 port 綁定成一個有交換器功能的 UTM，即可不另外增設交換器。

1-2、第一次安裝

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

> **Note**
>
> 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，管理者的權限設定可前往「系統設定 > 管理員」。

第一次安裝時的網路設定

• 首先將管理者的電腦和 INF 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 INF 的管理介面。

• INF 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。

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再輸入帳號跟密碼。
- 點選【確定】即可進入管理介面。

2. INF 會自動偵測管理者的瀏覽器語言，並自動切換語言，例如：管理者的瀏覽器使用繁體中文，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，非繁體、簡體中文的瀏覽器，管理介面就會自動切換成英文。

3. 登入後，可以在管理介面的右上角連到首頁、登出或切換管理介面的語言；此處也會顯示管理者登入的 IP 位址及目前有多少管理者登入。

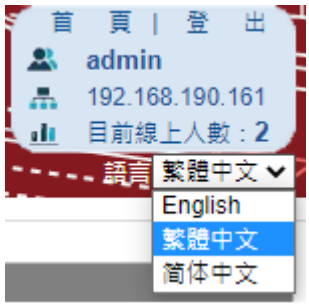


圖 2. 圖1-2 管理介面右上區域顯示¶

1-3、管理跟 Dashboard 模式

INF 提供 2 種操作介面，一種是管理者使用的管理介面，另一種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 > 首頁設定」選擇模式，下次登入時，就會直接進入此設定的模式。

1-3-1、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。

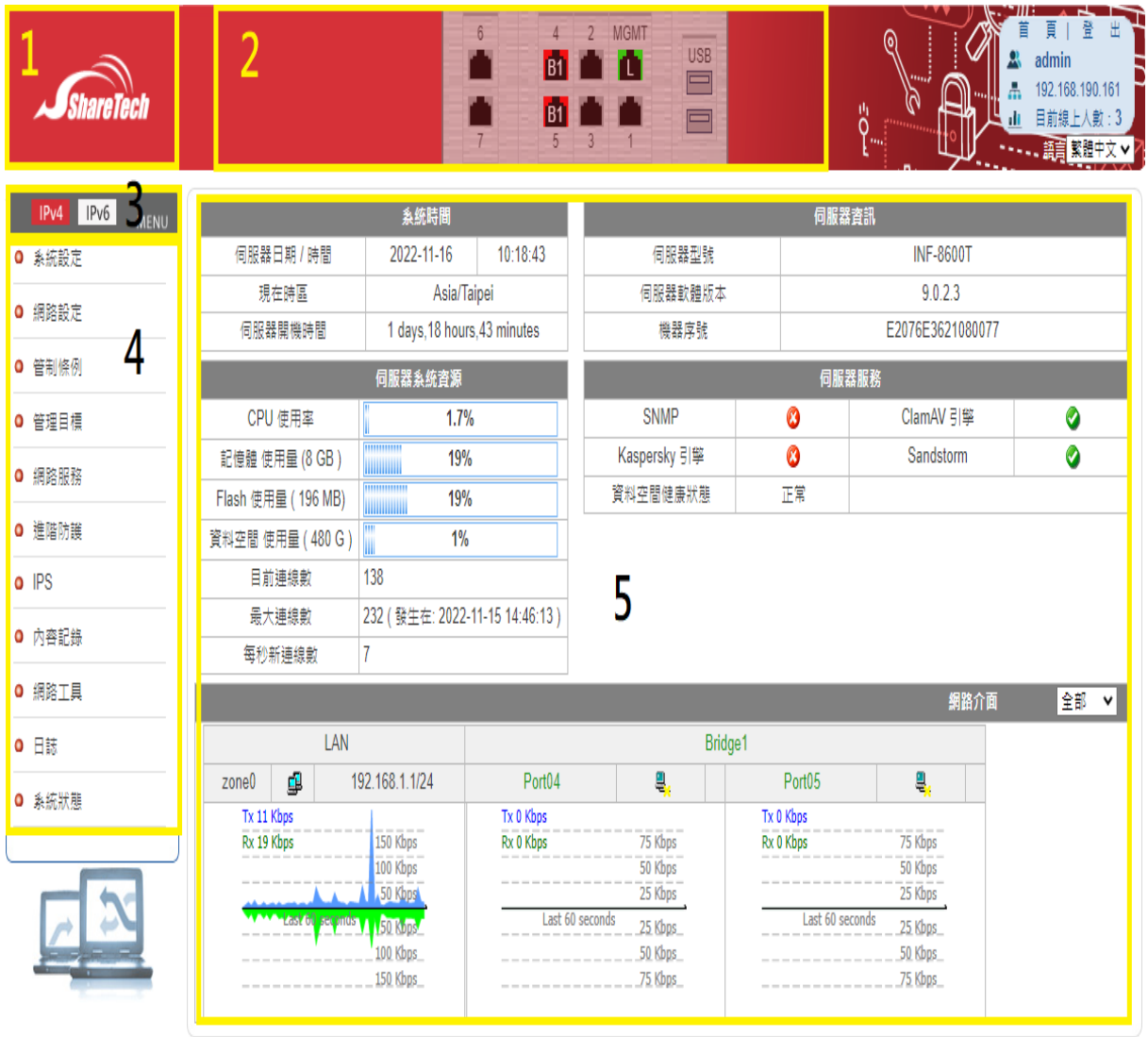


圖 3. 圖1-3 管理介面¶

1.【Logo 區】： 透過變更這裡的圖示，除了讓設備方便辨識外，更可以凸顯企業的整體形象，圖片的格式為 150 * 90 pixel 。

可前往「系統設定 > 基本設定 > 一般設定 > 更新 Logo」上傳圖片，格式包含 gif、png、jpeg。

2.【標題區】： 此區有 3 個區塊，分別是首頁標題、Port Information 跟管理者資訊。
在首頁標題區輸入標題文字，方便辨識此台設備， 1-4-2、Port Information 顯示所有硬體 Port 的狀態， 1-4-3、管理者資訊 顯示已登入的管理者資料。

首頁標題設定路徑：「系統設定 > 基本設定 > 一般設定」中的「首頁標題」。

3.【**IP 位址切換**】：INF 是支援 IPV4/IPV6 的多功能 UTM 設備，而 IPV4 跟 IPV6 在網路安全或是管理上有些差異，
例如：拒絕 IPV4 的 WEB 使用並不代表拒絕 IPV6 的 WEB，因此 2 個 IP 定址模式是分開管理的。
管理者可以在這裡切換位址，所有管理介面的位址都會一併切換。

4.【**主選單**】：管理介面的主選單分成 2 層：主項目與次選單。
選擇主項目下的次選單後，設定區會出現分頁選單進行詳細功能設定。

圖 4. 圖1-4 選單層次¶

圖1-4 說明：1. 主項目 2. 次選單 3. 分頁選單
一般來說，套用到整個 INF 且屬於系統管理層級的設定會在「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與分頁選單。

5.【**設定區**】：系統所有詳細功能設定及紀錄都在此區中完成。

1-3-2、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。

關於 Dashboard 介面操作與詳細說明，請參考 第16章 Dashboard 。

1-4、管理介面的首頁訊息

登入 INF 的畫面後，系統會提供訊息讓管理者清楚目前設備的運作狀況。

1-4-1、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 等重要資源使用量，管理者能夠藉此判斷設備是否超過負載。

系統時間		
伺服器日期 / 時間	2022-11-16	10:52:52
現在時區	Asia/Taipei	
伺服器開機時間	1 days,19 hours,18 minutes	

伺服器資訊	
伺服器型號	INF-8600T
伺服器軟體版本	9.0.2.3
機器序號	E2076E3621080077

伺服器系統資源	
CPU 使用率	0.5%
記憶體 使用量 (8 GB)	19%
Flash 使用量 (196 MB)	19%
資料空間 使用量 (480 G)	1%
目前連線數	107
最大連線數	232 (發生在: 2022-11-15 14:46:13)
每秒新連線數	0

伺服器服務			
SNMP	✗	ClamAV 引擎	✓
Kaspersky 引擎	✗	Sandstorm	✓
資料空間健康狀態	正常		

圖 5. 圖1-5 系統資源¶

各系統資源項目說明如下：

【目前連線數】：目前 INF 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)，INF 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，可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。

> **Note**
>
> 此處顯示為即時資料，若要查詢歷史的連線數資訊，在「系統狀態 > 系統狀態 > 歷史狀態」中勾選總連線數的選項，並選定時間範圍後查詢。

【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】： INF 的型號及韌體版本。

韌體版本會不定期發布，管理者可以在「系統設定 > 系統升級」設定升級方式：
· 手動升級：至 ShareTech 官網下載韌體版本，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，有新韌體發布就會自動下載，並在管理者指定的時間升級韌體；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。
可參考 2-4、系統升級 章節。

【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。

1-4-2、Port Information

在管理介面的標題區，有一個隱藏的資訊 — Port Information，即時顯示目前設備中所有 Port 的連線狀態。
預設是收合狀態，點選 Port information 的字樣後即可展開。

選擇任意 Port 之後會顯示資訊框，並會自動在設定區帶出網路設定頁面：
若 Port 顯示為綠色代表使用中且跟其他設備連接成功，同時在資訊框顯示設備連線的速度；紅色則代表沒有使用。

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，管理者可以清楚辨識哪幾個 port 是綁定的或為獨立運作。

圖 6. 圖1-6 Port Information¶

note

1. 此處顯示的 port 號碼跟實際機器上的 port 號碼是一致的，但實際位置可能會不一樣，所以管理者在配置網路區域時，必須以 port 號碼為根據。
2. 在 INF 的軟體版本中，顯示的 port 數量可能會多於實際數量，因此更需要以 port 號碼為依據進行設定。

1-4-3、管理者資訊

管理介面標題區最右邊的區域。會顯示管理者登入的 IP 位址及目前有多少管理者登入，也能操作切換語言、登出等動作。

【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。

【目前線上人數】：目前有多少人進入系統。點選顯示的數字後會開啟新的頁面，顯示目前登入的管理者與其登入的時間、來源 IP 位址及操作內容。
若要查看管理者操作資訊的歷史紀錄，可前往「日誌 > 操作日誌」。

【切換語言】：系統會自動偵測管理者使用的瀏覽器語言，並自動切換顯示相同的語言，管理者也可以自行切換。
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 種語言，則會自動切換成英文。

【首頁 / 登出】: 提供快速的連結回到首頁或是選擇登出系統。

1-4-4、網路介面

顯示「網路設定 > 區域設定」中所有區域的網路介面訊息跟即時流量，管理者可以切換查看全部、已連線跟自訂的區域。
自訂需在「系統設定 > 基本設定 > 一般設定 > 首頁網路介面預設顯示」中勾選區域。
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。

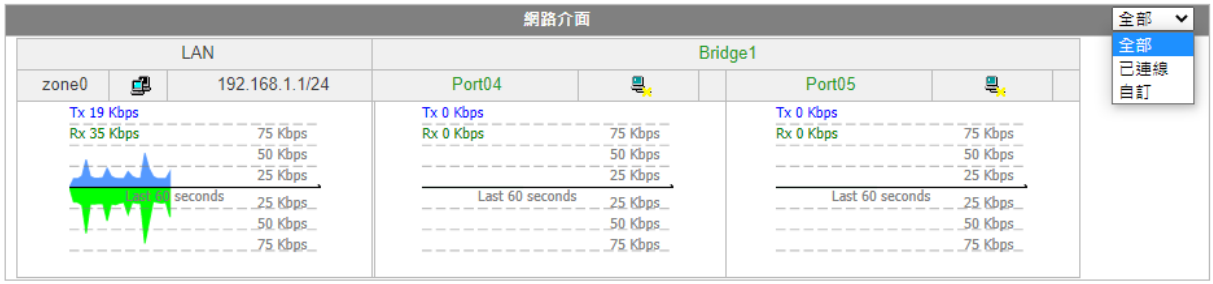


圖 7. 圖1-7 網路介面即時流量¶

藍色代表 Zone Out (TX) 流量 ， 綠色代表 Zone In (RX) 流量 。

若用上傳下載說明，上傳、下載要以設備為出發點，而非從使用者的角度。出網路介面的流量為上傳（Zone Out），進入網路介面的流量為下載（Zone In）。
連接網際網路的 WAN 介面（例如：PPPOE），上傳、下載流量方向剛好跟一般使用者角度相同；
而連接內部設備的 LAN 介面，其上傳、下載流量跟使用者角度相反，LAN 的上傳流量對於使用者角度就是下載流量。

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，如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：

A. 3 分鐘流量圖：「系統狀態 > 系統狀態 > 介面即時流量」
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，3 分鐘流量圖就能提供這樣的訊息。

B. 歷史流量圖：「系統狀態 > 系統狀態 > 歷史狀態」
儲存設備的資料，提供更長時間的紀錄資訊。可依要查詢的網路介面跟時間範圍顯示歷史流量圖。

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。
並非每個可進入設備的管理者都具有相同權限，僅主要管理者有權限進行系統設定。

INF 提供多層次的管理權限，管理者權限設定可前往「系統設定 > 管理員 > 帳號管理」。

2-1、基本設定

2-1-1、一般設定

- **一般設定**

INF 基本運作設定。例如：瀏覽器標題、記憶體及連線 timeout 等。

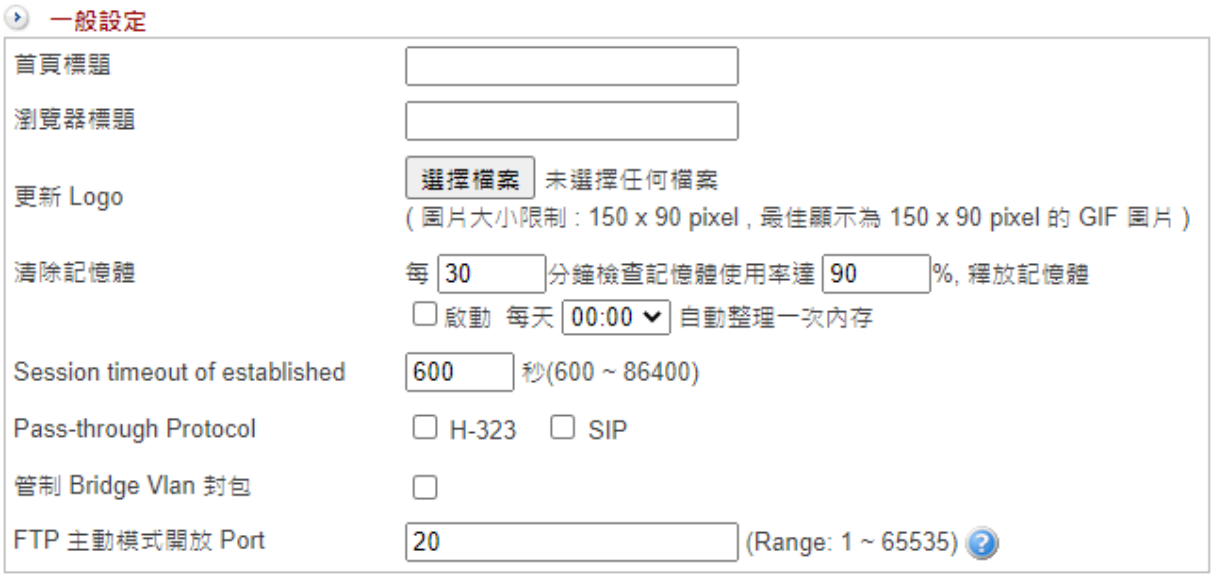


圖 8. 圖2-1 管理介面顯示設定¶

【首頁標題】：在管理介面的標題區顯示的文字。當管理者同時管理多台設備時，首頁標題可有效幫助管理者辨識並正確設定至要執行的設備上。

【瀏覽器標題】：登入管理介面的瀏覽器標題文字。設定容易辨識的標題，讓管理者在開啟多個網頁時，快速地找出此介面。

【更新 Logo】：預設為 ShareTech Logo，可以自行更換。
圖片大小限制為最大 150 x 90 pixel，最佳顯示為 150 x 90 pixel 的 GIF 圖片，也可以上傳通用的 PNG、JPEG 格式。

【清除記憶體】：為了避免記憶體被無用的程序占用，導致系統運作不正常，INF 內建自動清理記憶體機制。

系統預設為每 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。
管理者可根據使用狀態調整檢查時間跟觸發的上限值。

定期清理記憶體：預設為關閉。
可以指定時間讓系統定期執行檢查及清理，而非等記憶體達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 00:00。

【Session timeout of established】：設定每個已經建立的 TCP 連線，在多長時間內沒有傳輸資料時，系統會主動將這個 TCP 連線中斷。
預設值為 600 秒，如果設定時間太長 86400秒 (1 天)，系統可能會被很多空的 TCP 連線占據記憶體資源。

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，但若是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占據記憶體資源；
當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。

> **note**
>
> Session timeout of established 的設定只對**已建立的 TCP 連線**有效，對未完整建立的 TCP 連線及 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。
> INF 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 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。

【LAN 加速模式】：將多實體介面所綁定的虛擬介面，從 Bridge模式改為 Switch模式。不同的模式在 3-2、網路介面 會提供不同的設定。

【管制 Bridge Vlan 封包】：當防火牆位在兩交換器之間做過濾，且封包會帶 VLAN tag 時，需勾選此項讓防火牆能管制這些封包。

【FTP 主動模式開放 Port】：若內部的 FTP 伺服器使用非標準的 20 PORT 來傳輸資料，可以在此設定讓防火牆開放這個 PORT。

- **登入失敗封鎖設定**

不論是主要管理者或是次管理者，系統會限制每一個來源 IP 位址輸入錯誤的帳號、密碼的次數，當次數超過設定值，INF 就會封鎖此來源 IP 位址。
被封鎖的 IP 位址必須等到設定的封鎖時間過後，或是其他主要管理者登入並執行解除封鎖，才能將此來源 IP 位址解除鎖定。

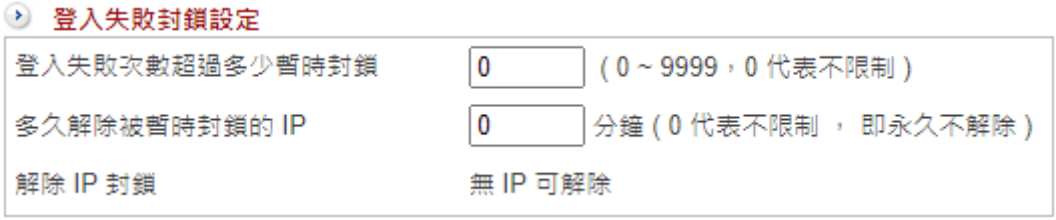


圖 9. 圖2-3 登入失敗封鎖設定¶

【登入失敗次數超過多少暫時封鎖】：
設定登入時，密碼輸入錯誤的次數限制，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 位址嘗試輸入密碼錯誤超過設定次數，會被 INF 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，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。

● 首頁設定

INF 提供 2 種操作介面，傳統的管理介面與 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 INF 進出網路的流量或是駭客攻防紀錄等。

圖 10. 圖2-4 首頁設定¶

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

● 首頁網路介面預設顯示

主要管理者登入 INF 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，此處可以設定預設顯示的網路區域。

圖 11. 圖2-5 選擇首頁顯示網路介面¶

【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。

● Drop Session Log

圖 12. 圖2-6 Drop Session Log¶

管制條例中顯示封包通聯記錄的功能。
預設僅顯示已建立的連線，通常已建立的連線代表符合管制條例的規則，而對於違反條例的封包，系統會將它丟棄且不會有任何紀錄；勾選這項功能後，系統會將丟棄的封包留有紀錄。

2-1-2、DNS 解析

這裡設定 DNS 伺服器是提供給 INF 自己查詢使用，因為 INF 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 。

【DNS Server 1】：INF 第一個使用的 DNS 伺服器，例如，168.95.192.1。

【DNS Server 2 】：INF 第二個使用的 DNS 伺服器，例如，168.95.192.1。

【DNS Server 3 】：INF 第三個使用的 DNS 伺服器，例如，2001:b000::1。

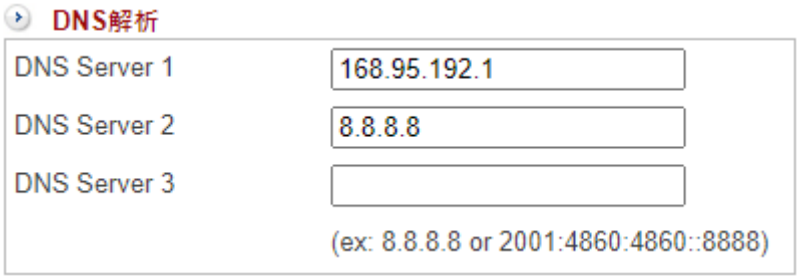


圖 13. 圖2-7 DNS 伺服器¶

INF 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，再依序使用其他的 DNS 伺服器。

2-1-3、管理介面存取設定

● 管理介面存取設定

INF 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。

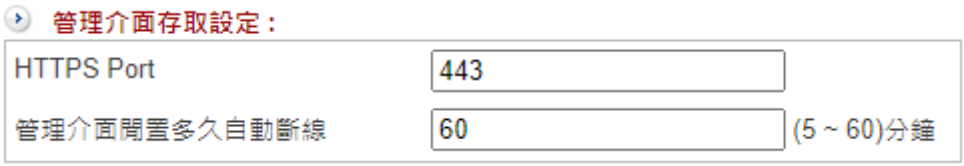


圖 14. 圖2-8 HTTPS Port 及自動斷線時間¶

【HTTPS Port】：進入 INF 管理介面使用 port 號，預設是 443。
例如：INF 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】：當超過設定的閒置時間，INF 會自動將管理者的連線中斷，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 分鐘，預設為 60 分鐘。

INF 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。

● 管理者密碼自訂規則

為了提高安全度，系統提供設定密碼的複雜度跟定期提醒管理者更換密碼這 2 項措施。

圖 15. 圖2-9 管理者密碼自訂規則¶

【啟用】：啟用管理者密碼自訂規則的功能，此預設為關閉。

【最短長度(3-16 個字元)】：設定密碼時，最短的密碼長度。一般來說，越長的密碼安全性越高。

【必須包含】：設定密碼必須包含哪一些字元，以增加密碼強度。

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，被猜中的機率相較單純數字或小寫字母的密碼低得多。

【新密碼不可包含舊密碼】：每次更改密碼時，管理者設定的新密碼不可跟舊密碼一樣，這項功能預設為關閉。

【要求修改密碼頻率】：設定每隔多少天系統會提醒管理者修改密碼，預設為 90 天；0 代表關閉這項功能。

2-2、時間設定

INF 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。

圖 16. 圖2-10 設定系統時間跟時區¶

● 時區與時間

【時區】：設定 INF 的時區，從時區列表中選一個 INF 所在的時區。

【時間】：設定 INF 的時間。

【日期】：設定 INF 的日期。

自行設定時區與時間，再按下儲存，就完成設定時間的動作。

● 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自己輸入特定的時間伺服器，INF 每 30 分鐘會跟時間伺服器校正一次。
校正過的資料顯示會在「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】：選擇是否啟用這項功能，預設為關閉。

【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 INF 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、管理員

依管理權限，分為主要管理者跟次管理者。

預設的 admin 帳號就是預設主要管理者，而主要管理者可以有多個。
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，而 Joy 也可以更改 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權限的帳號。

INF 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。

在次管理者的應用情境上，設想一下幾個運作的情況，依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 INF 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 INF 預設主要管理者，預設密碼為 admin，這個預設帳號無法被刪除。
在第一次安裝的情況下，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，
而因為 admin 在類似的網路管理者介面經常使用，基於安全考量，可以將它的權限限縮為 Read。

● 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。
INF 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權限的部分，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、瀏覽權限。
可搭配自訂化選單，讓次管理者能設定被授予權限的項目。

例如：A 次管理者被授予管理 VPN 通道，當 A 登入系統後，他左側的選單只會顯示 VPN，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】：對整機皆有寫入、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

帳號管理會列出所有可以進入 INF 管理介面的管理者帳號及權限，包含可以瀏覽或是寫入的功能項目、預計變更密碼的時間等。

● 新增管理者帳號及權限

點選 ✚ 新增 按鈕，進入新增管理者的設定，說明如下：

圖 17. 圖2-11 新增一個管理者¶

【帳號】：新增管理者使用的帳號，任何英文跟數字的組合皆可。

【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。
一般而言，8 位數的英文+數字組合就能提供一定強度的密碼。

【密碼檢測】：INF 會自動幫您判斷密碼強度。

利用下面幾種方式增加密碼安全度：
1. 英文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】：需要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，是否要強迫改密碼，預設為關閉。

【要求修改密碼頻率】：每隔多少天，系統就會自動提醒管理者修改密碼，預設為 90 天，0 代表關閉這項功能。

【註解】：新增管理者容易辨識的描述。

【兩步驟驗證】：啟用後，除了輸入原本的密碼，需再輸入由 Google Authenticator 產生的驗證碼才能登入帳號。

【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 或 Write 權限時，如沒有勾選自訂化選單代表這一個次管理者可以看到所有的功能選項。
All Privileges 即是主要管理者，因此選擇此項時，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設定的項目，如果沒有勾選，代表次管理員可以對整個系統進行瀏覽或設定。

INF 的設定架構是由主項目+次選單+分頁選單組成，實際的設定區是在分頁選單中；
只要限制次管理者可否看到主項目+次選單這 2 個項目，就可以控制他的使用權限，這 2 個項目就在左側的主選單區，所以可以理解為：自訂化選單 = 左側主選單區。

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。

自訂化選單 全選

系統設定	☑ 基本設定	☐ 時間設定	☐ 管理員	☐ 系統升級	☐ 備份與還原
	☑ 訊息通知	☐ 重新啟動&關機	☐ AP管理	☐ 特徵碼更新	☐ 雲端管理服務
	☑ SSL憑證設定	☐ 不斷電系統	☐ CMS	☐ 資料顯示筆數	
網路設定	☐ 區域設定	☐ 網路介面	☐ 路由管理	☐ VLAN(802.1Q)	☐ 中斷設定
管制條例	☐ 管制規則				
管理目標	☐ 位址表	☐ 服務表	☐ 時間表	☐ 頻寬管理	☐ 應用程式管制
	☐ URL 管理	☐ 防火牆功能			
網路服務	☐ SNMP	☐ 病毒引擎	☐ Sandstorm	☐ WEB 服務	☐ FTP 服務
	☐ 遠端記錄伺服器				
進階防護	☐ 異常IP分析	☐ 交換器管理	☐ 內網防護		
IPS	☐ IPS 設定	☐ IPS 記錄			
內容記錄	☐ WEB 記錄	☐ FTP 記錄			
網路工具	☐ 連線測試	☐ 封包擷取			
日誌	☐ 操作日誌				
系統狀態	☐ 系統狀態	☐ 連線狀態	☐ 流量分析	☐ 威脅情報儀表	

圖 18. 圖2-12 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 19. 圖2-13 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 20. 圖2-14 Write 權限及自訂功能¶

2-3-2、管理者的 IP 位址

INF 可以限制特定來源 IP 位址無法進入管理介面，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，表示不限制來源 IP 位址，任何內、外網路來源 IP 位址都可以進入管理介面。

INF 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：若設定內部的 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，則會被拒絕。

一旦有 IP 位址被設定，代表啟用此一過濾機制，只有符合的來源 IP 位址可以進入，因此設定時管理者務必確認自己的 IP 位址被加入，以免無法進入管理介面。
新增第一筆來源 IP 位址時通常會加入當下管理者的來源 IP 位址，否則儲存後就無法進入管理介面（不是被允許的來源 IP 位址）；
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。

- **設定**

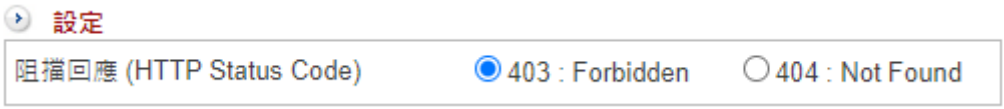


圖 21. 圖2-1 5 設定阻擋回應¶

【阻擋回應 (HTTP Status Code)】：當非設定的管理 IP 嘗試登入管理介面時，防火牆會如何回應。可選擇回應禁止連線 (403)，或是不回應 (404)。

- **新增一筆管理者 IP 位址**

在管理者的 IP 位址列表下方點選 

按鈕，進入新增來源 IP 位址的頁面，說明如下：

圖 22. 圖2-16 設定管理者的來源 IP 位址¶

【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。

2-4、系統升級

INF 的最新韌體資訊發布在官網上，管理者可以在 http://www.sharetech.com.tw 網站上找到最新的韌體資訊下載。

有全自動、半自動跟手動 3 種升級模式：
· 全自動跟半自動升級：系統設定 > 系統升級 > **韌體資訊**。
· 手動升級：系統設定 > 系統升級 > **軟體升級**。

2-4-1、韌體資訊

這裡可設定全自動或半自動的升級模式：

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。

全自動模式 ：自動檢查及下載韌體，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。

圖 23. 圖2-17 INF 的韌體升級設定¶

【最後更新時間】：最後一次韌體資訊檢查的時間。
若想知道目前是否有最新的韌體，可以按下 更 新 按鈕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，此為檢查跟下載韌體的時間，不是軟體升級的時間。

【更新伺服器】：INF 檢查最新韌體的伺服器名稱。
此為系統預設，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，INF 會在指定時間到更新伺服器檢查最新韌體並自動將韌體下載 INF 中。

【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。

Note

當自動升級韌體過程因為某些因素導致升級失敗，此時這個功能就會被停用，也就是升級失敗後管理者須排除失敗因素，否則系統將不再執行自動升級韌體動作。

【升級韌體時間】：管理者指定在此時間執行升級動作。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 INF 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，設定路徑在「系統設定 > 訊息通知 > 訊息通知 > 收件者項目」中。

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

- **韌體檔案**

INF 到更新伺服器檢查後，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，只要在韌體升級欄位按下升級，系統就會開始執行升級動作。

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 INF 不可預期之錯誤。

管理者也可以把韌體下載到本機中，再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

手動升級韌體機制：先取得韌體後，再上傳到 INF 中。

【伺服器型號】：INF 的型號。

【目前軟體版本】：INF 的軟體版本，9.0.0.0 是最初始的版本號碼，新的版本號碼數字會比前一版的數字大。

【軟體升級】：選擇要上傳到 INF 的韌體。

按下 

按鈕後，系統就會開始執行升級動作。

2-4-3、韌體下載紀錄

不論採用自動下載或是手動上傳，INF 會把韌體更新過程記錄下來，管理者可以透過【韌體下載紀錄】，找尋相關歷史記錄，包含起始時間、結束時間、傳輸時間、版本、大小、事件等。

圖 24. 圖2-18 韌體下載紀錄¶

【版本】：針對韌體版本搜尋。

【事件】：INF 韌體下載成功或是失敗的事件。

2-5、備份與還原

當設定 INF 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 INF 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 2-5-1、系統備份與還原 操作，全自動則在 2-5-2、自動備份 。

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 INF 還原到最初的狀態，再重新設定。

2-5-1、系統備份與還原

此處的動作是手動的備份與還原，系統只備份當下的設定檔。
INF 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，在還原時做法也稍微不一樣，管理者 2 種都可以使用。

● 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 設備並自動將所有設定檔複製到 USB 中，完成後請把 USB 設備拔除。
每當 INF 重新開機時，會自動偵測 USB 是否存在，如果存在，則會自動將 USB 的備份檔載入，並執行系統還原動作；
因此這個功能適用於更換故障硬體設備，把當初備份的 USB 插入新的設備，就可以快速的把機器還原回原來的狀態。

● 系統備份

按下備份鍵可將目前系統之設定值匯出。
INF 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，匯入此檔案即可。

圖 25. 圖2-19 系統備份¶

● 系統還原
管理者選擇想要還原的設定檔（ tgz 格式的壓縮檔）後按下確定鍵，系統會自動上傳設定檔。重新開機後，INF 就回到當初備份時的狀態。
上傳時，INF 會再自動檢查一次設定檔是否有損壞，若發現損壞，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。

● 恢復出廠預設值

管理者可以將整台設備還原到出廠的預設值，按下【確定恢復】按鈕後，INF 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。

· 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。
這個機制適用於網路架構正常，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，然後將其他的資料清除後重設。

· 格式化資料空間：執行恢復出廠設定值時，是否要執行格式化的動作。
如果勾選此選項，會將整個資料空間（如硬碟）格式化，此時需要較多時間執行，完成後將重新開機並回到系統最原始的出廠預設值。

● 資料空間狀態

INF 的 LOG 都是記錄在資料空間中，系統會自動檢查資料空間的狀態，並將狀態呈現在管理介面中。
當資料空間故障時，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資料空間毀損而無法記錄。

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，INF 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 INF 資料空間的備份數量，系統會依管理者的設定自動進行備份動作，超過設定份數的舊設定檔會被自動刪除。

【啟用】：勾選啟用後，就開始設定執行備份的日期、時間。

【自動備份時間】：有 2 種模式可供選擇。
· 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。
· 自訂日期及時間，例如：星期一的凌晨 00:00 執行備份動作。

【保留備份數量】：INF 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，採先進先出的覆蓋方式。

【立即備份】：按下立即備份按鈕，系統會馬上執行備份動作，並將它儲存在 INF 中。

● 備份紀錄

所有自動備份的紀錄都會被保留下來，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動作：

【下載至 USB】：將備份檔儲存在 USB 裝置上。
當系統重新開機並偵測到這個 USB 裝置時，會自動執行還原動作，不需要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】：讓 INF 直接回到某一設定檔的狀態，點選【還原】後 INF 會要求管理員輸入數字以確認是否要執行還原動作，如下圖。

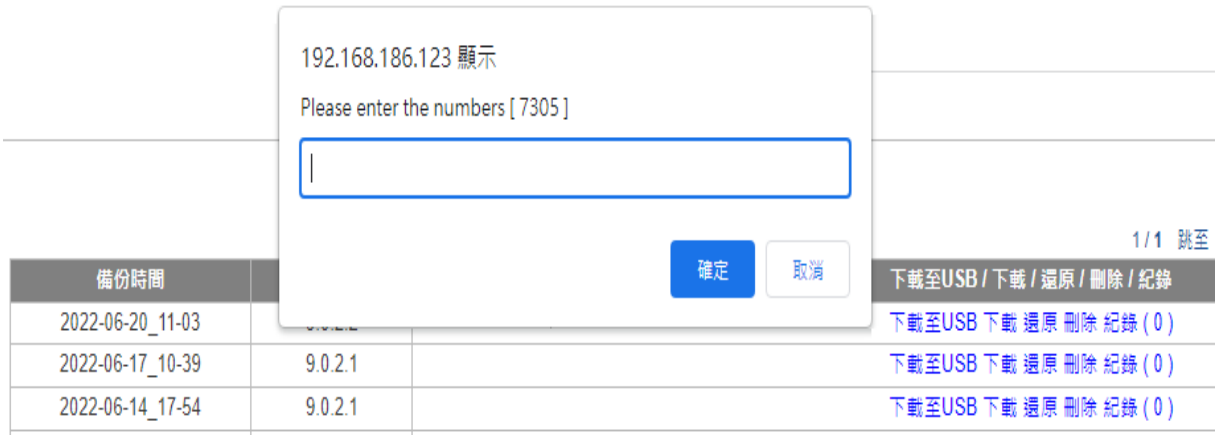


圖 26. 圖2-20 系統還原確認¶

【刪除】：把這個備份設定檔從系統中刪除。

【紀錄】：INF 會詳細記錄自動備份設定檔之間的差異項目，方便管理者追蹤比較。點選後會開啟新視窗列出詳細內容，如下圖。

圖 27. 圖2-21 INF 自動備份的紀錄¶

在記錄中有更改時間、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，管理者可依據這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

INF 會用郵件通知管理者系統發生的事件，從備份資料成功與否，到系統被攻擊等等，讓管理員可以在第一時間掌握設備及網路訊息。
INF 的通知是以郵件的方式寄送，因此管理員需先設定基本 SMTP 伺服器與收件者帳號。

2-6-1、訊息通知

可以設定不同的事件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通知訊息。

● 訊息通知

INF 共有 26 種訊息通知的事件，每一種事件依照其類型可以做週期性或定期性的檢查，檢查後如發現問題，就會根據管理者的設定來寄出訊息通知郵件。

圖 28. 圖2-22 訊息通知郵件設定¶

【寄件者帳號】：選擇寄出通知郵件時使用的寄件者帳號，寄件帳號在「SMTP 伺服器設定」頁籤中設定。

· 自動：
選擇自動模式時，系統會從【SMTP 伺服器設定】中優先選擇跟收件者相同網域名稱的寄件者。若無任何對應關係，則使用第一筆寄件者寄出通知信。

· 指定 SMTP 帳號：
以【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（換行新增）。

【嘗試寄送次數】：設定當通知信傳送失敗時，最多會嘗試傳送幾次。設定的範圍是 1~5 次，當寄送失敗超過設定的次數，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三種。如果語系設定不正確，有可能導致收信者收到的通知信為亂碼。

● 訊息通知事件

INF 目前提供 25 種的事件通知信，每一種檢查項目根據其屬性，可設定不同的檢查時間及機制。

例如：「線路斷線」這一個檢查項目一定是週期性時間檢查；「防火牆防護」的檢查週期性會比「系統操作日誌」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」，可以改為「台北 INF 斷線」。

如果檢查項目的通知沒有被啟用，系統就不會發出這個項目的通知信。
各項目逐一說明如下：

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發生異常。

4. 防火牆攻擊防護 (SYN, ICMP, UDP, PortScan)：INF 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：管理者登入時發生錯誤。

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：新的韌體發布。

11. 資料空間容量過低 (Usage over 90%) 和壞軌：資料空間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。

17. IPSec 斷線通知：IPSec VPN 斷線。

18. IPSec 切換通知：SD-WAN 環境下，任何一個 IPSec 通道斷線。

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，系統將它刪除前先通知管理者。

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. 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。

24. 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。

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。

26. 自動升級通知：設定執行自動升級前幾個小時發送通知。

2-6-2、訊息通知記錄

INF 會把每次的訊息通知（不論成功與否）都記錄下來，方便管理人員日後查詢。

● 訊息通知紀錄搜尋

【日期】：搜尋指定時間內的通知紀錄。

【事件】：可選擇特定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

圖 29. 圖2-23 訊息通知紀錄搜尋結果¶

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，欄位的 ⬍ 鍵可以更改排序方式。
點選內容欄位的圖示查看更詳細的資料。

圖 30. 圖2-24 訊息通知紀錄詳細內容¶

2-6-3、SMTP 伺服器設定

INF 寄出通知郵件時需要使用 SMTP 伺服器設定寄件帳號，如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。

● 新增 SMTP 伺服器

點選 SMTP 伺服器設定列表下方的 

圖示進入新增 SMTP 伺服器。

【寄件者名稱】：預設的寄件者名稱為 Admin，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 INF 的通知。

【寄件者】：顯示在收信者的通知信郵件的寄件者名稱。
此為顯示名稱，非寄件者帳號，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。

【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分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：當寄件者帳號 a@ghij.com 只會寄給 ppp@ghij.com 的收件者，此處填入 ghij.com，表示除了 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，INF 提供線上測試寄信功能。

在 SMTP 伺服器設定列表中，INF 會列出每一個寄件者帳號的詳細資料，按下在【SMTP 測試郵件】欄位的【測試】按鈕後輸入收件者的郵件帳號。

圖 31. 圖2-25 測試 SMTP 伺服器¶

輸入收件人郵件位址後按下確定，如果收件人的郵件信箱收到一封主旨為「This is a SMTP TestMail」的信件，代表此 SMTP 伺服器設定正常。

2-7、重新啟動&關機

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

2-7-1、重新啟動&關機

INF 正常的開關動作，系統提供 2 個按鈕：【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；按下關閉鈕就會按照正常程序關機。

2-7-2、自動重新啟動

系統可以設定週期性的自動重新啟動。重新開機可清除掉不必要且占記憶體的不正常檔案或是暫存檔，增加系統的穩定度。
有天、周跟月 3 種週期長度，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，預設為關閉。系統會自動記錄重新開機的時間及成功與否，可點選右邊的紀錄按鈕查看。

【週期】：3 種週期可選擇，天、周跟月，正常運作下設定每月重新開機一次即可。

【自動重啟時間】：何時執行自動重啟，一般會設定在非系統提供服務的時間。

2-8、AP 管理

首先，在談論到內網無線網路環境布局前必須先了解 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。

INF 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問題，
結合無線 AP 設備，將每個 AP 通過的流量整合到 INF 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。

INF 提供了一個單獨的控制平台來管理有線與無線通聯，
透過管理介面，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、目前該 AP 路由器線上人數。
最重要的是，管理員可直接透過控制平台管控每個 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且完整的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，對於安全的控管比較薄弱，無法有效防護一些惡意的攻擊行為；
而若 WiFi 流量導到 INF 的網路環境，除了可管控每一台無線 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 INF 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、影音等）使用，且記錄所有使用之行為。

對於網管人員來說，以一台 INF 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，
且最重要的是可以遠端關閉設備、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，使用者也可以輕鬆使用，對企業網管人員來說是一個無痛導入的解決方案。

2-8-1、AP 管理設定

開啟 INF 的 AP 管理功能，預設為關閉，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 管理點選 ✚ 新增 新增欲被管理的 Wireless AP。

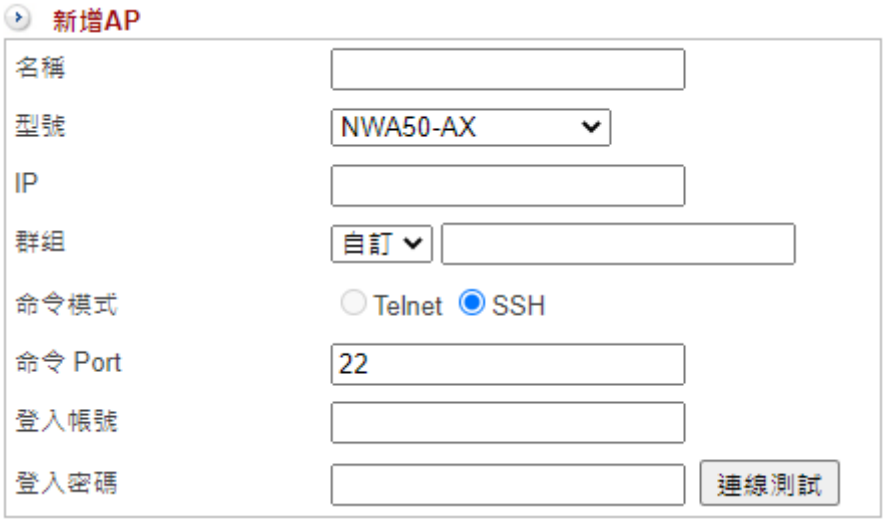


圖 32. 圖2-26 新增一台無線 AP¶

【名稱】：新增被管理的 AP 名稱，可輸入中英文字。

【型號】：選擇目前支援 AP 設備， AP 跟 INF 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 NWA5123-AC-HD：Telnet / SSH

6. Zyxel WAC6103D-I：Telnet / SSH

7. Zyxel NWA5123-NI：Telnet / SSH

8. Zyxel NWA1123-ACv2：Telnet / SSH

9. Zyxel NWA1123-ACv3：Telnet / SSH

10. Zyxel NWA1123-AC-HD：Telnet / SSH

11. Zyxel NWA1123-AC-PRO：Telnet / SSH

12. Zyxel NWA5121-NI：Telnet / SSH

13. Zyxel NWA110-AX：Telnet / SSH

【IP】：Wireless AP 的 IP 位址，例如：192.168.1.5。

【群組】：選擇新增的 Wireless AP 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且資料可以統一派送。
如要新創一個群組，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，群組名稱可輸入中英文及數字。

【SNMP 埠號】：AP 用 SNMP 協定跟 INF 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】：INF 使用哪一種協定跟後面的 AP 溝通，有 Telnet 跟 SSH 二種，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】：驗證填入的資料是否正常，INF 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。

圖 33. 圖2-27 無線 AP 列表¶

【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，INF 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顯示 Auto。

【SSID】：SSID 跟使用的頻帶，頻帶分成 2.4G 跟 5G 二種。每個不同的 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 目前有多少人正在使用。
點選線上人數，INF 就會顯示過去利用這個 SSID 上網的人數統計圖，管理者可以查詢當天或之前的歷史資料。

> **Note**
>
> 此處是根據每個 SSID 列出使用人數，而在「系統狀態 > 連線狀態 > 15-2-2、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。

● **Wireless AP 派送設定**

所有被管理的無線 AP 都可以利用 INF 將常用的設定檔派送到無線 AP 上。
例如：SSID 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。

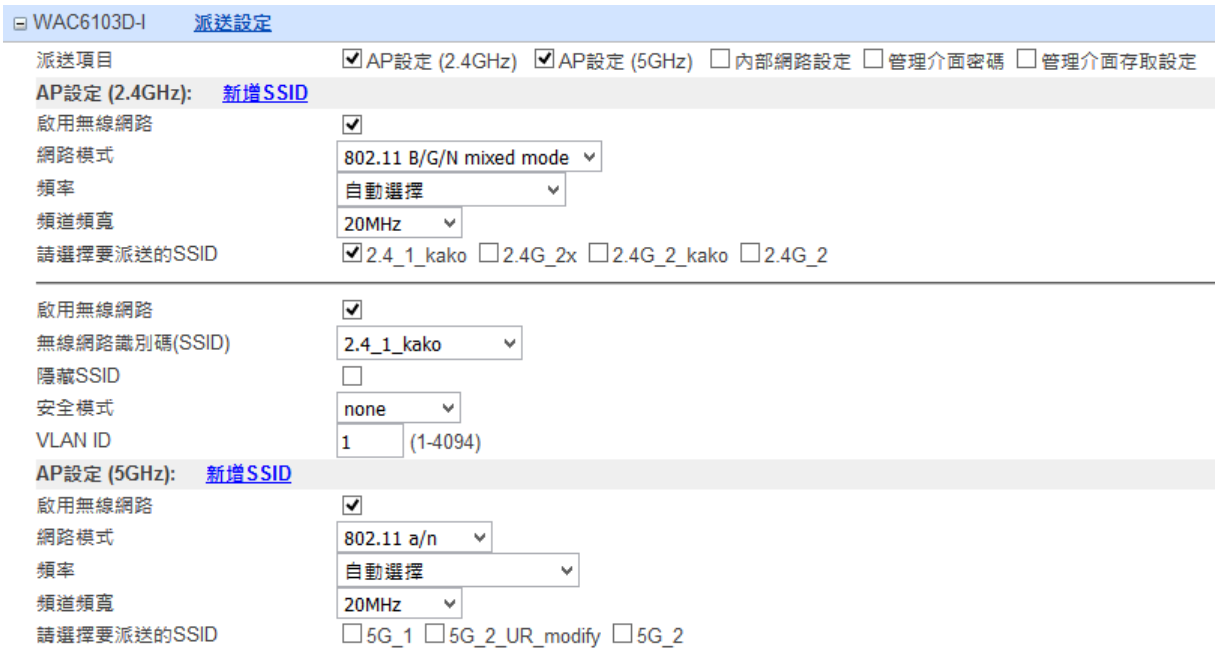


圖 34. 圖2-28 無線 AP 設定派送¶

【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】：選擇使用 802.11B/G/N。

【頻率/頻寬】：使用的通道。

2-8-3、MAC 過濾

MAC 過濾內可設定黑白名單，內容為連線裝置的 MAC 位址。設定完成後可在 AP 管理內套用。

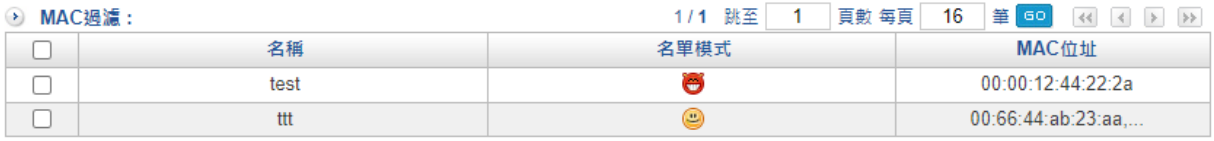


圖 35. 圖2-29 MAC 過濾列表¶

點選 ✚ 新增 按鈕，進入新增一筆 MAC 過濾設定：

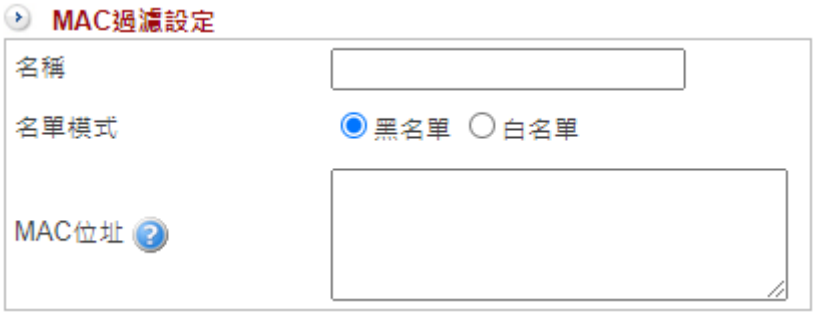


圖 36. 圖2-30 MAC 過濾設定¶

【名稱】：此筆 MAC 過濾的名稱，方便管理者辨識。

【名單模式】：黑名單或白名單。

【MAC 位址】：可設定多筆，一行一組。

2-9、特徵碼更新

INF 仰賴封包特徵值比對，確認往來的封包是否正常，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 37. 圖2-31 特徵碼更新¶

管理者也可以點選 立即更新 按鈕，立刻檢查。

應用程式的特徵隨使用版本變化，判斷的特徵值就會改變，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定、管理、監控與問題排除。
此外，EyeCloud 整合 Line 即時通知服務，可以有效減輕網管人員工作量，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 > 雲端管理服務」功能中，點選「啟用」雲端管理服務。
若之前沒有雲端管理的帳號，按下【建立帳戶】後系統會自動帶入申請機制。
如已有雲端管理的帳號，可填入帳號密碼以登入，下突圍已經成功代管的顯示畫面：

圖 38. 圖2-32 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 INF 溝通使用的 Port，預設為 TCP 2000。

【機器序號】：INF 的機器序號。

【最後連線時間】：INF 跟雲端管理伺服器最後一次溝通的時間。

【Eyecloud】： 將 INF 跟 Eyecloud 綁定。
點選後可以讓管理者綁定已經申請過的 Eyecloud 帳號密碼，或新申請一個 Eyecloud 帳號。

2-10-2、雲端管理

雲端管理的網址是 https://eyecloud.tw/，可以事先申請 Eyecloud 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 INF。

1、在 https://eyecloud.tw/ ，建立新帳號。

圖 39. 圖2-33 建立 EyeCloud 帳戶¶

2、登入雲端管理系統後，新增欲託管的設備。

圖 40. 圖2-34 新增設備¶

3、管理託管的設備。

圖 41. 圖2-35 新增設備成功¶

• 在「訊息通知 > 通知項目」可查看設備狀態：

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

紅 → 綠：20 分鐘以上沒有和 server 連線 → 系統運作正常。

紅 → 橘：20 分鐘以上沒有和 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

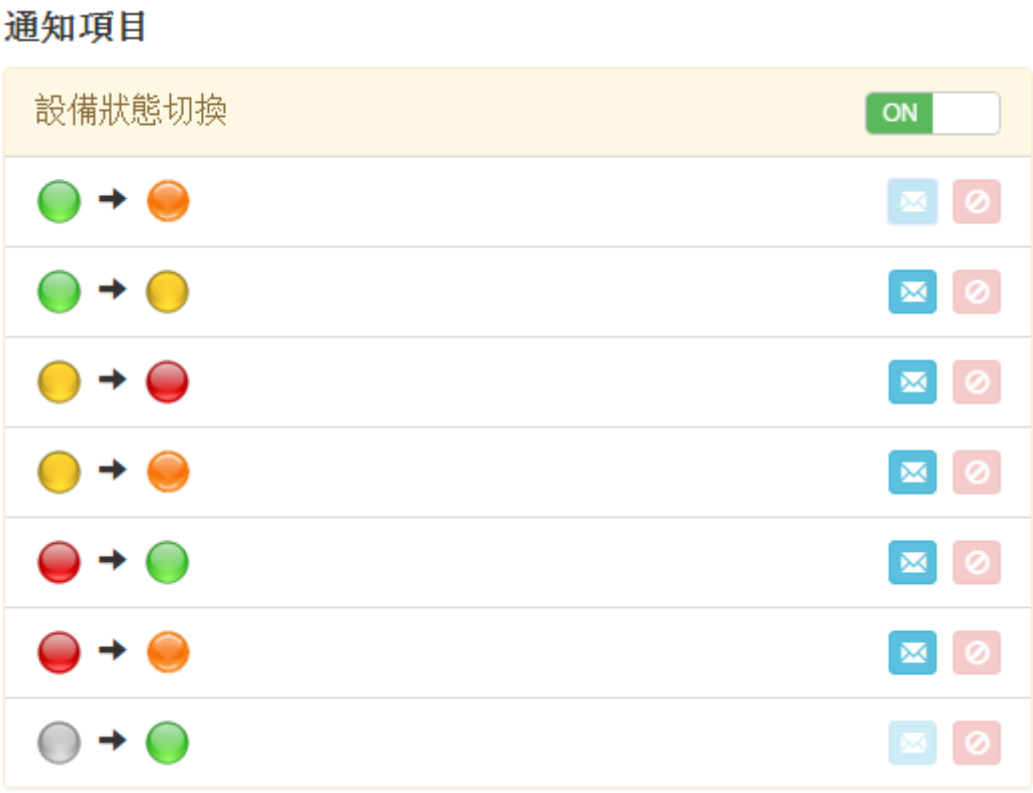


圖 42. 圖2-36 設備狀態切換燈號解釋¶

- **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 43. 圖2-37 解除綁定雲端管理服務¶

解除綁定後會顯示此設備尚未與 EyeCloud 綁定。

圖 44. 圖2-38 此設備尚未與 EyeCloud 綁訂¶

2-11、SSL 憑證設定

網路傳輸資料仰賴 SSL 加密協議，INF 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，不論是跟合法憑證機構申請或是自己簽署的憑證，匯入操作端的電腦後，操作者的電腦就不會出現憑證錯誤的警示字眼。

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，
另一個是在【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。以下為設定範例：

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，並將它匯入瀏覽器，完成後在瀏覽器的檢視憑證區可以看到下圖資訊。

圖 45. 圖2-39 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 憑證跟中繼憑證 2 種。

3、Let's Encrypt憑證

Let's Encrypt 是合法的憑證發放單位，INF 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可以。
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 46. 圖2-40 申請憑證¶

【使用的憑證網域】：輸入申請的網域名稱，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 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 INF 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，保護裡面儲存的資料。

2-12-1、不斷電系統

INF 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。

● 設定

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。

圖 47. 圖2-41 USB 連接設定¶

1. USB 連接模式

防火牆透過自己的USB介面和UPS連接

【型號】：選擇 UPS 的型號。

· 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值，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. 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。

3. 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。

4. SNMP v3 連接模式

【UPS 設備 IP】：輸入不斷電系統的 IP 位址。

【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】：SNMP v3 驗證帳號時使用的密碼，驗證密碼的方式有 SHA 跟 MD5 二種，這些資料都要跟 UPS 主機設置的一樣。

【傳輸用密鑰】：SNMP v3 在資料傳輸使用的加密密碼，加密模式有 DES 跟 AES 二種，這些資料都要跟 UPS 主機設置的一樣。

5. 網路不斷電系統伺服器連接模式

防火牆透過IP和埠號連到不斷電系統伺服器

【型號】：選擇 UPS 的型號。

· 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。

● 網路不斷電系統伺服器

在 USB 及 SNMP 模式下，INF 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 低電量時發送通知過去。

【等待關機時間】：遠端設備關機需要多少時間。INF 會等待這個時間後才會進入關機程序。

【Ping Timeout】：INF 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，包含時間及發生的事件。 如下圖

時間	
2022-07-14 15:22:02	Can not get UPS status.
2022-07-14 15:19:02	System is going to shut down.
2022-07-14 15:19:02	UPS is on battery(76%) and battery is lower than Low Battery.
2022-07-14 15:18:02	UPS is on battery(76%) and battery is lower than Low Battery.
2022-07-14 15:17:02	UPS is on battery(77%) and battery is lower than Low Battery.
2022-07-14 15:16:02	UPS is on battery(78%) and battery is lower than Low Battery.
2022-07-14 15:15:03	UPS is on battery(79%) and battery is lower than Low Battery.
2022-07-14 15:14:02	UPS is on battery(79%) and battery is lower than Low Battery.
2022-07-14 15:14:02	UPS status is changed from OB DISCHRG to OB DISCHRG LB.
2022-07-14 15:05:03	UPS status is changed from OL to OB DISCHRG.
2022-07-14 14:24:02	UPS status is changed from OL CHRG to OL.
2022-07-14 14:12:02	UPS reconnected.

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 INF。

CMS 跟雲端管理服務雖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，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 INF 設備。

3. CMS 只能管理 INF，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 ，每個地方的 INF 都會向總部彙整它目前的狀態、設定檔，
總部的管理者就可以由總部的 INF 掌握到所有外點的即時狀態並可以介入管理。

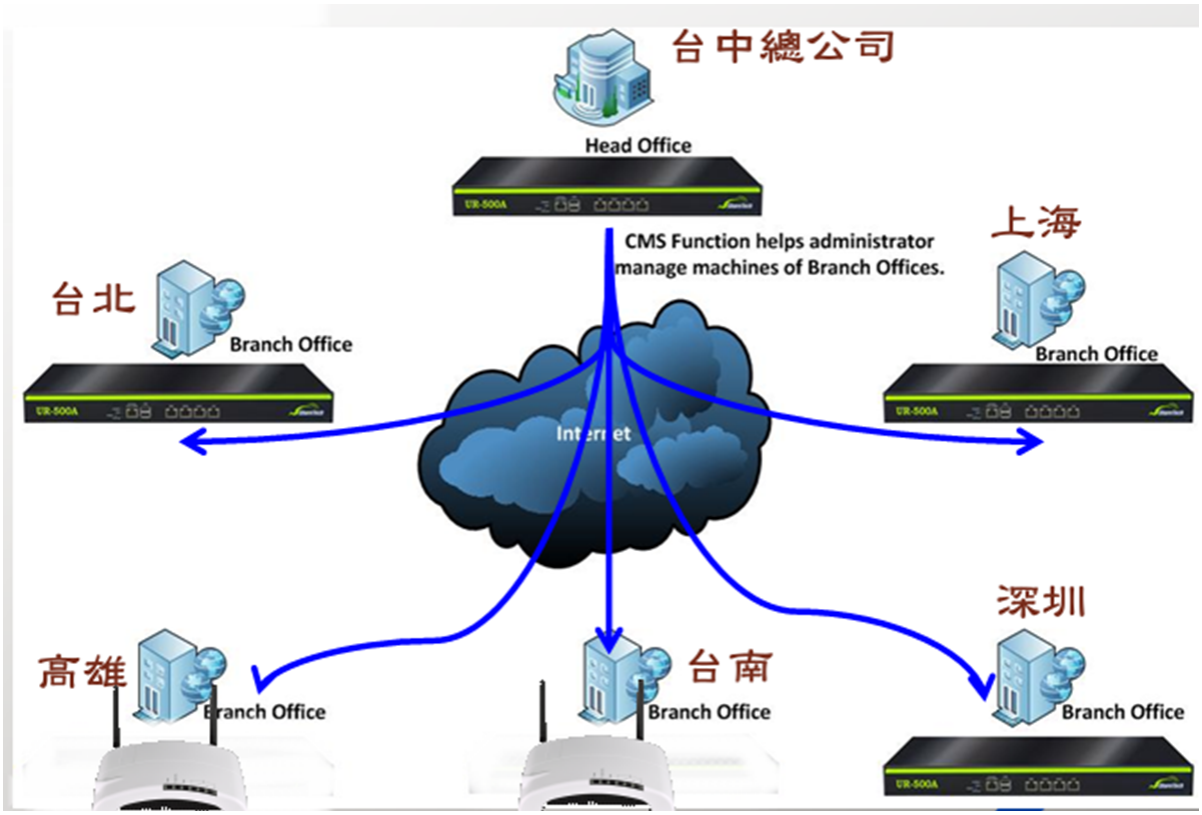


圖 48. 圖2-42 CMS 示意圖¶

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，而如果本身沒有硬碟，則只能扮演成 Client 端。

● CMS 基本設定

【啟用】：是否啟用 CMS 功能。

【模式】：CMS 運作模式是 Client 或 Server，選擇不同模式其設定項目也不同，以下分別說明。

1. 設為 Client 端

CMS 運作原理相當簡單，設為 Client 端的設備會定時跟 Server 端傳送訊息並賦予 Server 端管理權限。

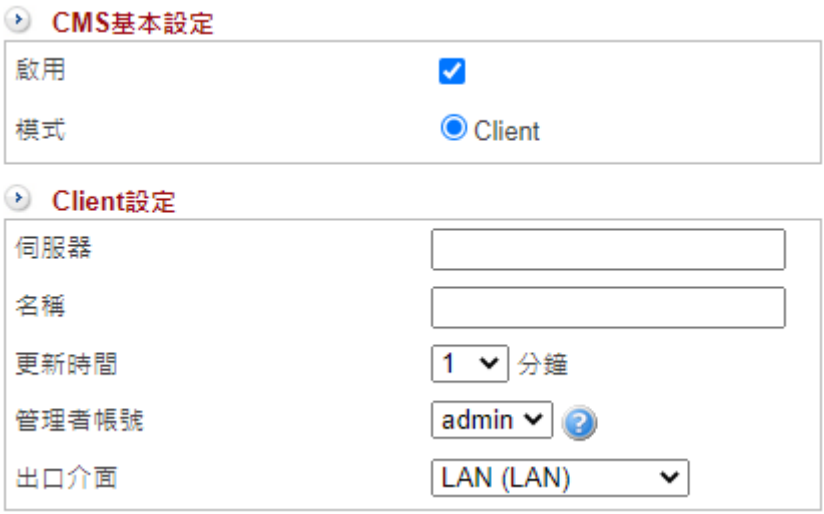


圖 49. 圖2-43 CMS 設為 Client 端¶

【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。

【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，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。
詳細的管理者權限請參照「系統設定 > 2-3、管理員 」設定。

【出口介面】：使用哪個出口線路向 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

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

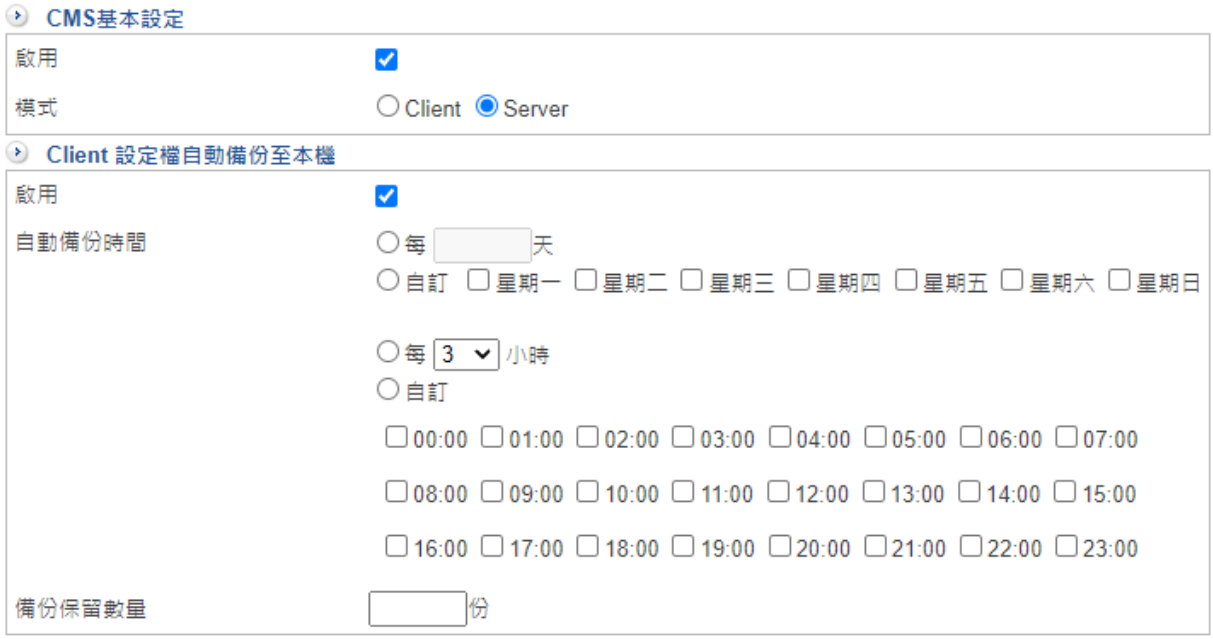


圖 50. 圖2-44 CMS 設為 Server 端¶

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】：週期性地備份資料，週期越短系統的負荷越大。

【備份保留數量】：備份的設定檔要存幾份，一般來說 5 份就已經足夠，份數越多占的儲存空間越大。

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 端的管理者選擇接受後，CMS Server 端才會開始處理這一個 Client 的資料。

圖 51. 圖2-45 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。

圖 52. 圖2-46 Client 列表¶

【狀態】：以顏色區分，綠色代表 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。

【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。

【型號】：Client 端的型號。

【IP】：Client 端目前的 IP 位址。

【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。

【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。

【自動備份】：是否有啟動自動備份設定檔功能。

【動作】：修改 / 刪除 Client 端的設定。

當按下 📝 按鈕後，就可以修改 **Client 端的顯示資訊：**

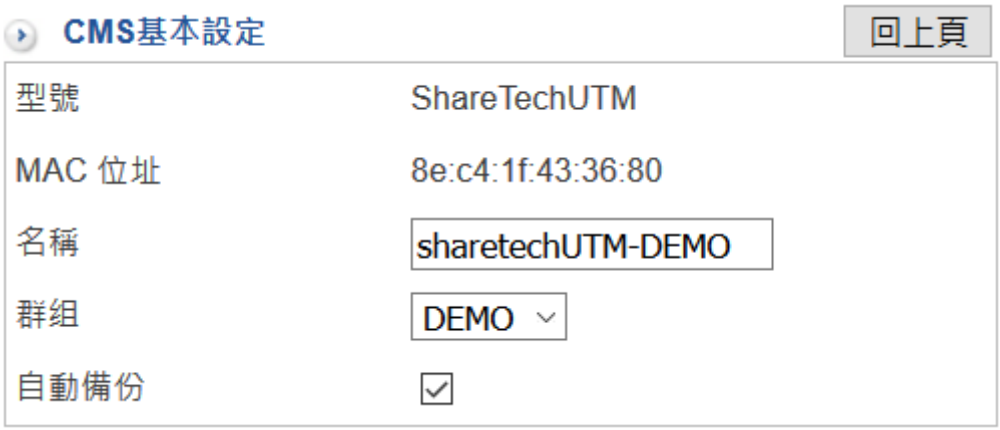


圖 53. 圖2-47 修改 Client 資訊¶

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

〖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。

〖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。

〖自動備份〗：是否要啟用自動備份設定檔功能。

【記錄】：分成連線跟控制 2 種，連線是指 Client 端跟 Server 端的通聯紀錄，控制是由 Server 端下了哪些控制命令給 Client 端。

【群組收合】：管理者可以按下【群組收合】的按鈕，切換群組間的顯示訊息。

【立即備份】：選定 Client 端後，按下【立即備份】按鈕，立刻執行備份的動作。

- **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 54. 圖2-48 備份清單-自訂備份還原設定¶

【備份時間】： 何時備份這個設定檔。

【軟體版本】： Client 端備份時的版本。

【立即還原】：還原 **Client 端的設定檔** 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. 在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。

【下載】：按下圖示後將這一個設定檔下載到本地端。

【刪除】：刪除這筆紀錄。

【記錄】：查看這個備份檔被修改了哪些設定。

第3章 網路設定

INF內網防火牆 並非傳統的 UTM 或是防火牆，它是以 SWITCH 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，
每一個ZONE都可以當成是一個 SWITCH 或是 Layer2 VLAN ，
基本上，2 個以上的實體網路介面都可以組合成一個 ZONE，每個 ZONE 進出的封包都可以執行防火牆的過濾條件。

本章會詳細介紹如何將多個實體網路介面組合成 ZONE，以及在建立ZONE時鎖需要的注意事項。

Tip

由於ZONE模擬 Layer2 SWITCH，因此 不同的ZONE之間的溝通封包，需透過前端 router 進行路由動作。
ZONE 支援封包帶 Vlan tag (RSPAN VLAN)的格式。

3-1、區域設定

INF 預設會把 MGMT 標示為 ZONE 0，ZONE 0 跟 MGMT 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，
預設 IPV4 位址是 192.168.1.1。

Tip

在同一個 ZONE 有超過一個以上的實體 Port 組合時，預設Port 與 Port 之間的封包是阻擋的，需要管制條例設定規則才會通行。

3-1-1、區域設定

區域狀態圖列出目前每一個實體 Port 歸屬於哪個 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，管理者就可以新增一個 ZONE，按下 新增區域，開始新增一個新的 ZONE：

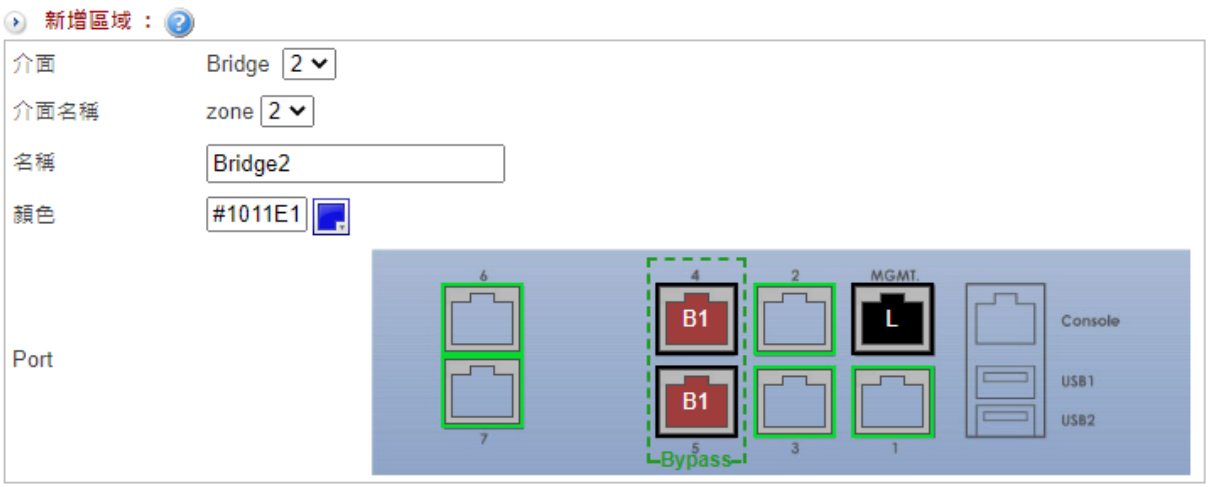


圖 55. 圖3-1 新增區域¶

【介面】：選擇數字代號。

【介面名稱】：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】：新增使 ZONE 方便記憶的名稱，例如：會計、工程等等。

【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。

Tip

在選擇Port時，如果界面被 ByPass虛線框起來，被框起來的Port 為同一組ByPass Port，支援硬體ByPass。
硬體ByPass： 此功能啟動時，同一組ByPass Port會直接導通，就像是網路線接在一起般，其啟用時機點為設備斷電或是系統偵測到異常。

新增完成後會回到區域列表中，INF 會把每一個區域、名稱、顏色及它擁有的實體 Port 標示出來。
可點選 ，進入修改，或直接刪除 （只有 ZONE 0 沒有刪除鍵）。

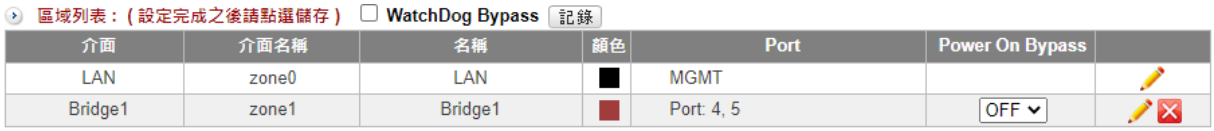


圖 56. 圖3-1 區域列表¶

列表中的每個 ZONE 會出現在「網路設定 > 3-2、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

INF 的每一個 ZONE 都可以指定網卡速度，設定網卡速度有 2 種方式，可從「網路設定 > 區域設定 > 線路設定」中設定，
或是從首頁上方的【Port Information】，點選要設定的實體 Port 就可以設定調整網卡速度。

圖 57. 圖3-1 區域設定¶

【介面】：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 有無連線。如果沒接任何設備就會顯示 Disconnected，正常連線則會顯示 Connect。

【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。

3-2、網路介面

完成「網路設定 > 區域設定」後，所有建立的介面都會出現在此處的頁籤列表中，管理者可以開始設定介面的網路 IP 位址、連線速度等網路資訊。

圖 58. 圖3-2 在網路介面的頁籤區域列表¶

如前面所提，INF 會保留 ZONE 0 為預設的 ZONE，所以出現在第一個的就是屬於 ZONE 0 的 LAN，
其他新增的介面會按照實體介面的順序，依序排列在後方，點選該頁籤後就可以進入網路設定。

3-2-1、網路介面設定

圖 59. 圖3-3 網路介面設定¶

【介面名稱】：這個介面是屬於哪個 zone（在「網路設定 > 3-1、區域設定」中定義）。

【MAC 位址】：這個介面的唯一 MAC 位址，同一個 INF 管理的設備，MAC 位址不可以重複。

【啟動】：LAN 介面預設是啟用狀態且不可以被關閉，其他新增的介面可選擇關閉、STATIC 或 DHCP。

· STATIC：介面的 IP 位址是在下方。
· DHCP：介面的 IP 位址是由 DHCP 伺服器配發。

【MTU】：每一個封包最大的 byte 數，預設為 1500 ，設定範圍是 1400~1500。

Tip

在INF建議選擇 STATIC 模式，介面位址設定IP的部份可以省略，統一透過MGMT界面管理。

3-2-2、訪問控制

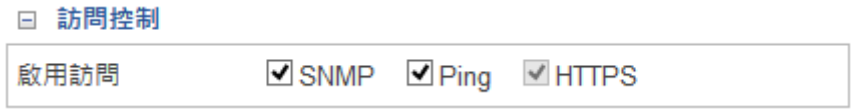


圖 60. 圖3-3 訪問控制¶

【啟用訪問】：介面是否接受其他的 IP 位址查詢或進入管理介面。

· SNMP：介面是否接受 SNMP 的查詢。勾選後，此介面會把一些資訊，藉由 SNMP 協定送給遠端的 SNMP 伺服器。
· Ping：這個介面的位址是否接受 ICMP 協定。勾選後，介面上設定的 IP 位址會回應 ICMP 的封包。
· HTTPS：這個介面是否接受透過 https 協定進入管理介面。勾選後，介面上設定的 IP 位址都可以接受 https 服務。

3-2-3、防火牆防護設定

圖 61. 圖3-3 防火牆防護設定¶

【防護項目】：此介面是否要接受防火牆的防護。針對屬於這個介面上設定的 IP 位址，提供 SYN 攻擊、ICMP 攻擊、UDP 攻擊及 Port Scan 等 4 種攻擊防護。
管理者可以啟用其中數種或是全部。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 攻擊的防護能力可以在「管理目標 > 5-8、防火牆功能 」中設定。

3-2-4、介面位址

定義每一個實體介面的 IP 位址，新增設定完成後會列表顯示。
點選 ✚ 新增 進入新增 IP 位址：

圖 62. 圖3-5 網路介面 IP 位址設定¶

【名稱】： 容易辨識此介面的名稱，例如 VLAN 1。

【IP 位址】：為介面新增一個 IP 位址，例如：192.168.10.1。

【網路遮罩】：IP 位址涵蓋的範圍，以一個 C 子網段為例，填入 255.255.255.0。

【預設閘道】：屬於 WAN 類型或是介面後面還有接其他的路由器，就需要填入閘道位址，若內部類型介面沒有其他的路由設備則不需要。

【管理 IP】：介面上的 IP 位址是否要讓管理者可以登入管理。

3-3、路由管理

於主選單 MENU 上方可切換為 IPv4 或 IPv6 模式，INF-UTM 會將整台設備關於 IP 顯示或是設定的模式切換。

3-3-1、靜態路由

管理者在「網路介面 > 」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。
系統內定的路由表無法更改，要修改就需要從「介面位址」上重新設定 IP 位址跟子網路遮罩。

INF 會把所有的靜態路由表列出來：

	編號	名稱	目的網路	閘道	介面
	1	預設閘道	192.168.186.1/32		LAN
	2	系統內定	192.168.1.0/24		LAN
	3	系統內定	192.168.186.0/24		LAN

圖 63. 圖3-6 IPV4 的靜態路由表¶

INF 除了由網路介面定義產生的內定路由表外，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。

按下 ✚ 新增 鈕後，進入新增一筆靜態路由：

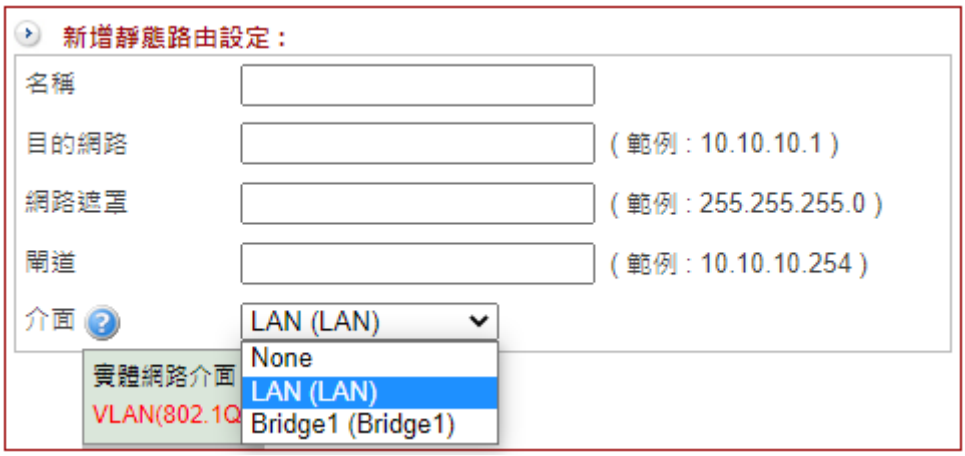


圖 64. 圖3-7 IPV4 新增靜態路由¶

【名稱】：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】：新增的路由表要屬於哪一個介面， 下拉選單後，系統會列出所有已建立的介面讓管理者選擇。
選項會用顏色區分不同的網路介面，分別是實體網路介面、IP 通道 (IP Tunnel)、GRE 通道、PPPoE 撥接介面、VLAN、PPTP 及 SSL VPN。

如果指定介面，則這一筆路由將只會在它所屬的介面生效；

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、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 INF，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。

除了預設閘道，在多 WAN 的環境，可以再設定備用閘道，當預設閘道斷線即會自動切到備用閘道上。

圖 65. 圖3-9 預設閘道列表¶

【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，設定範圍 1-999。

點選 ✚ 新增 後，進入新增預設閘道：

圖 66. 圖3-9 新增預設閘道¶

【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 位址或是自行定義。

3-3-3、動態路由

INF 支援 RIPv2 動態路由協議，只要指定介面跟路由週期，就可以將所有的路由協議學習起來，提供給系統使用。
學習到的路由表會列在動態路由列表中。

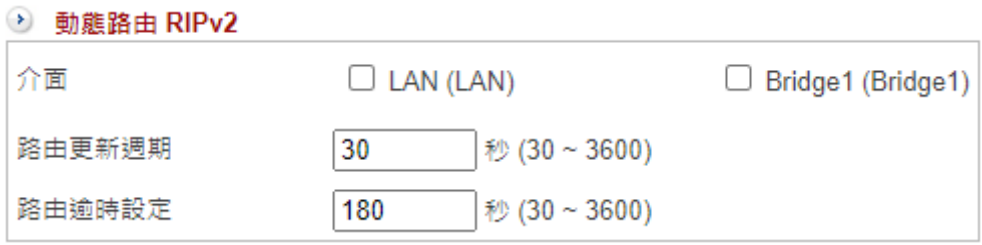


圖 67. 圖3-9 動態路由 RIPv2¶

【啟用】：是否啟用 RIP 路由協定

【介面】：選擇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，預設為 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。

3-4、VLAN(802.1Q)

VLAN 802.1Q 在交換器上是一個很基本的功能，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，
圖3-10 用實際的範例說明 VLAN 運作，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，彼此無法互通，僅同一個 VLAN ID 的電腦可以互通。

當網路封包從 Switch-A 往上送到 INF 時，INF 就需要拆解及組合這些帶 VLAN ID 的網路封包，才會知道它下一個目的地是哪裡，
本節說明如何拆解 VLAN ID 的設定。

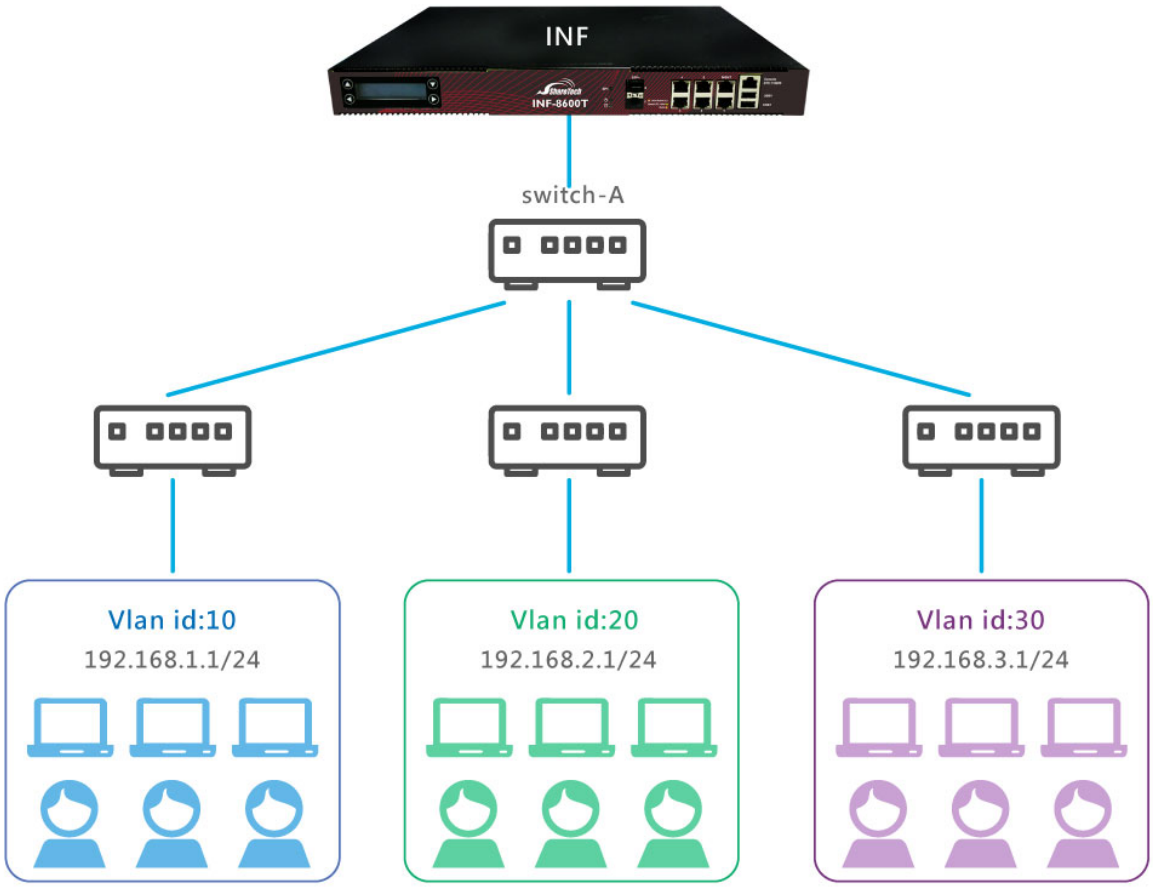


圖 68. 圖3-10 VLAN 範例¶

按下 ✚ 新增 鈕後，進入新增 VLAN：

而在新增之前，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，設定後網路封包將無法正常的被拆裝及組合，網路就會不通。

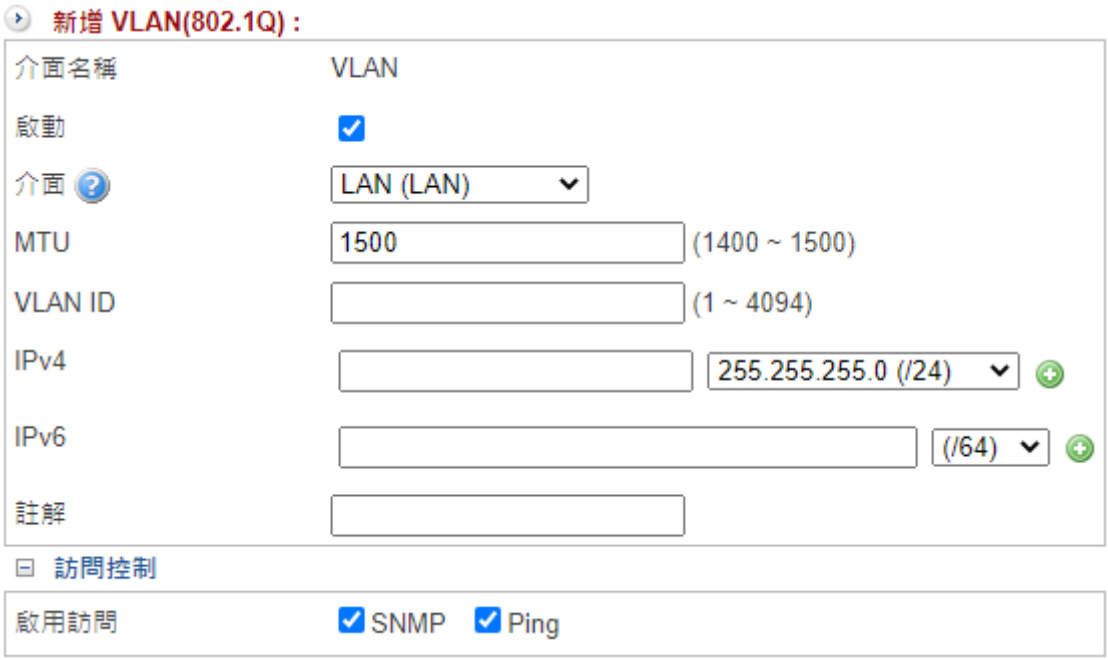


圖 69. 圖3-11 VLAN 設定範例¶

【介面名稱】：系統預設 VLAN 的名稱就是 VLAN，無法更改，僅能用 ID 分辨每個不同的 VLAN。

【啟動】：是否要啟用這個 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)，INF 會把所有的區域列出，讓管理者選擇。

【MTU】：每一個封包最大的 byte 數，預設為 1500，設定範圍是 1400~1500。

【VLAN ID】：給此 VLAN 一個數字代碼，同一台 INF 的 VLAN ID 不可以重複，數字範圍是 1~4094。

【IP 位址】：VLAN ID 下包含的網路 IP 位址及區段，可設定 IPV4 跟 IPV6 位址。

【註解】：可新增備註說明。

【啟用訪問】：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。

設定完成後，INF 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、中斷設定

INF 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。

依預設，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，
讓系統自動分配 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，INF 提供管理者 CPU 中斷服務，以調整系統資源。

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，例如當每一個網卡的 TX/RX 發出中斷要求時，就分配特定的 CPU 服務。

硬體中斷設定

啟用中斷數據載入 | 自動配置

全選		CPU0	CPU1	CPU2	CPU3
☐	Port04-TxRx-0 (Bridge1)	☑	☐	☐	☐
☐	Port04-TxRx-1 (Bridge1)	☐	☑	☐	☐
☐	Port04-TxRx-2 (Bridge1)	☐	☐	☑	☐
☐	Port04-TxRx-3 (Bridge1)	☐	☐	☐	☑
☐	Port05-TxRx-0 (Bridge1)	☑	☐	☐	☐
☐	Port05-TxRx-1 (Bridge1)	☐	☑	☐	☐
☐	Port05-TxRx-2 (Bridge1)	☐	☐	☑	☐
☐	Port05-TxRx-3 (Bridge1)	☐	☐	☐	☑
☐	LAN-TxRx-0	☑	☐	☐	☐
☐	LAN-TxRx-1	☐	☑	☐	☐
☐	LAN-TxRx-2	☐	☐	☑	☐
☐	LAN-TxRx-3	☐	☐	☐	☑

圖 70. 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，跟硬體中斷最大不同是同一個 Zone 內可能有好幾個實體 Port。

軟體中斷設定 自動配置

全選		CPU0	CPU1	CPU2	CPU3
☐	LAN_rx-0	☑	☐	☐	☐
☐	LAN_rx-1	☐	☑	☐	☐
☐	LAN_rx-2	☐	☐	☑	☐
☐	LAN_rx-3	☐	☐	☐	☑
☐	LAN_tx-0	☑	☐	☐	☐
☐	LAN_tx-1	☐	☑	☐	☐
☐	LAN_tx-2	☐	☐	☑	☐
☐	LAN_tx-3	☐	☐	☐	☑
☐	Bridge1_rx-0	☑	☐	☐	☐
☐	Bridge1_tx-0	☑	☐	☐	☐

圖 71. 圖3-17 CPU 軟體中斷¶

note

1. 自動配置：軟硬體中斷皆有自動配置選項，點選後

2. 設定後可以到「系統狀態 > 系統狀態 > 15-1-6、CPU 負載 」觀看每一個 CPU 的即時負載。

第4章 管制條例

管制條例是整個 INF 的精隨，每一個進出 INF 的網路封包，包含不同ZONE之間，同一個ZONE不同Port之間的封包接可以控管。

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中的 **基本設定** 時，就會按該管制規則的設定讓它通過或丟掉， **且不會再向下**與其他的管制規則進行比對。

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

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，INF 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，INF 就會開啟新視窗顯示這個條例所有的進出封包。

每一條管制規則包含 3 個部分「基本設定」、「通用工業協定」、「進階設定」與「防護設定」，用較白話的方式解釋：

· 基本設定：哪些人從哪裡來，走哪一條路到哪裡。

· 通用工業協定 : 工業協定 Modbus /TCP 封包的管控。

· 進階設定：檢查攜帶的東西。

· 防護設定：要不要保鏢保護。

Tip

條例預設為全部阻擋，當沒有任何條例存在時，所有封包會全部阻擋。

4-1、管制規則

一進入管制規則，INF 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，管理者可以指定查看某介面的管制規則。

- **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。
	IPS	入侵偵測防禦。
	紀錄管制	HTTP、郵件的紀錄。
	指定閘道	從哪一個閘道走。
	防護	啟用防火牆防護。
	任何協議	任何協議包含 tcp/udp/icmp 等。
	tcp	tcp 通訊協議。
	udp	udp 通訊協議。
	icmp	icmp 通訊協議。
	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，INF 會列出所有的管制規則，IPV4 跟 IPV6 的管制規則會分開列出，INF 預設顯示 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 

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 72. 圖4-1 管制規則列表¶

【優先權】：INF 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，數字越小表示越優先。

【啟用】：管制規則的暫停跟啟用按鈕，點選此處圖示後可以將原本啟用的管制規則暫停，原本暫停的改為啟用。

【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。

當管理者在找尋網路問題或想確認設定的目標是否有進入管制規則中，此時就可以利用 INF 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，INF 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）

【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 INF 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。

【條例動作】：複製某條管制規則，方便新增類似條件的規則。

【搜尋條例】：針對要查看的來源網路介面或是IP顯示管制規則，或是針對自定搜尋，針對特定條件搜尋規則。

● 管制規則的封包通聯記錄

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 73. 圖4-2 管制規則的封包通聯記錄¶

【自動更新】：INF 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 三種協定。

【封包大小】：這一個連線的封包大小，單位為 Bytes。

- **管制規則的組合**

每條管制規則由 4 個部分組合而成，分別是基本設定、通用工業協定、進階設定跟防護設定，除了基本設定區的資料必填，另外 3 個區域的設定由管理者自行決定配置。

4-1-1、管制規則設定

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 74. 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，方便管理者辨識，可輸入任何中英文字，例如：禁止上網。

【來源介面】：INF 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。
因為是 ZONE 的管制，可以在細部選擇針對那一個Port，預設不選是針對該Zone 的 所有 Port。

【通訊協定】：通訊協定共有 4 個選項，全部、TCP、UDP 跟 ICMP，選擇此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 INF 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。

- **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」中已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。

【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，
INF 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，可把眾多服務整合在一個服務群組，
這些都需要在「管理目標 > 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。

note

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，
INF 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，可把眾多服務整合出一個服務群組，
這些都需要在「管理目標 > 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。

note

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，可以選擇允許或拒絕；允許表示讓封包通過，拒絕則是將封包丟棄。

note

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。

進階設定

對於符合【基本設定】規則且【動作】設定為允許的網路封包，INF 可以進行更進階的動作，包含時間表、IPS 跟掃毒等，
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 75. 圖4-5 管制規則進階設定¶

tip

每個項目都有一個選項【新增】，當要設定的內容不在選項中，點選【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：選項中沒有想選擇的位址表，此時選【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」設定。

【時間表】：可直接在選項中點選新增，或前往「管理目標 > 時間表」設定。
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】：可直接在選項中點選新增，或前往「管理目標 > 頻寬管理」設定。
建立要管制的頻寬，整個條例每秒使用的流量會被限制。

【應用程式管制】：可直接在選項中點選新增，或前往「管理目標 > 應用程式管制」設定。
建立要管制的應用程式，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，當設定最大連線數後，符合這個管制條例的每個來源 IP 位址能使用的最大連線數就會被限制。

【URL 管制】：可直接在選項中點選新增，或前往「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】：可直接在選項中點選新增，或前往「管理目標 > IPS 設定」中建立群組。
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記錄還是阻擋。

【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，後續的封包要拒絕或是繼續執行下一條。

- 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。
- 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。
掃毒會對所有通過的 http / https 封包執行掃毒的動作；記錄則會記錄下 http/https 的網頁瀏覽紀錄。

INF 內建 ClamAV 掃毒引擎是啟動的，Kaspersky 掃毒引擎則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 INF 的 WEB 協定中 URI，不論是 http 或是 https 都會被記錄下來。

要讓 INF 記錄 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 INF 的 SSL 憑證，
此憑證存放的位址是 https://INF 管理IP/myca.crt ，IE / Chrome 瀏覽器均會自動執行此一憑證，
而 Firefox 會自行管理憑證，因此使用 Firefox 時，需要再輸入一次，並將它的三個選項全部啟用。
可參考 6-7、WEB 服務 。

note

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

防護設定

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 INF 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 76. 圖4-6 管制規則的防護¶

4-2、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 INF 的管制規則，管理所有的網路行為。
以下為實際環境常見的架構

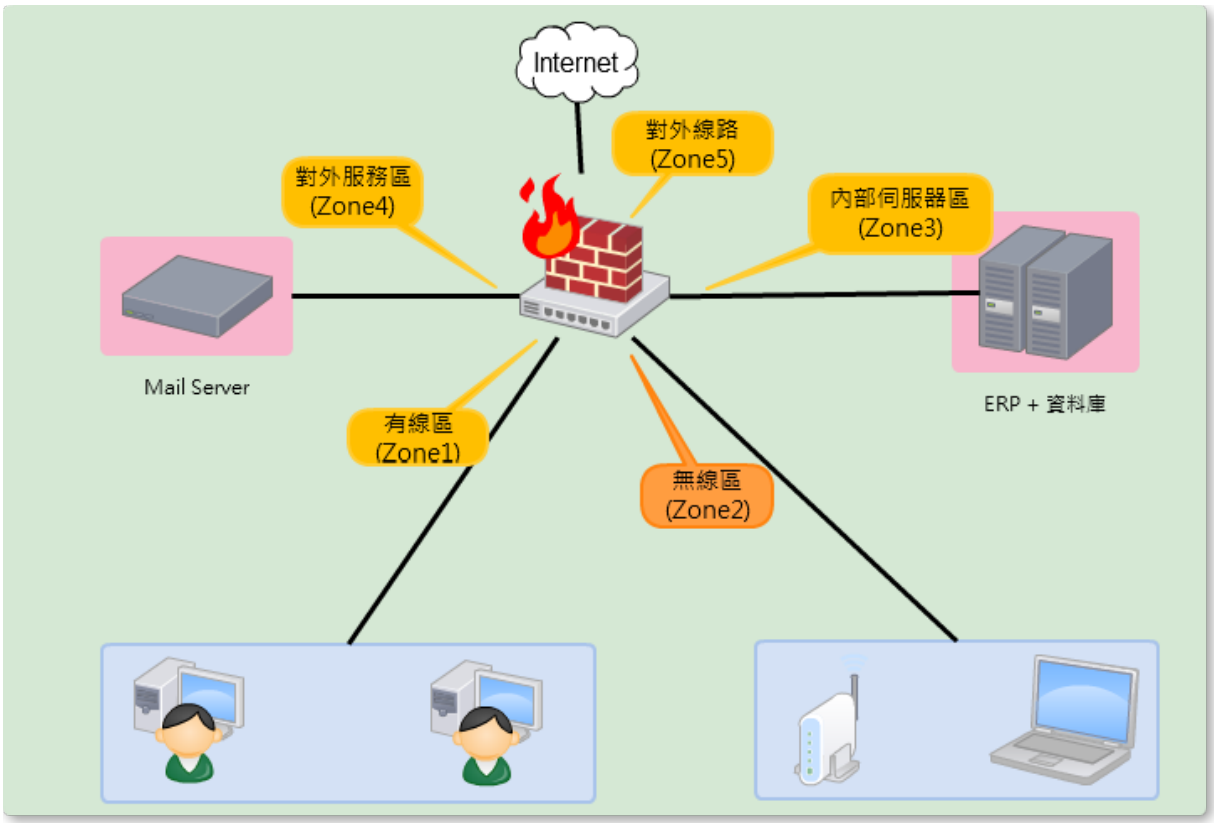
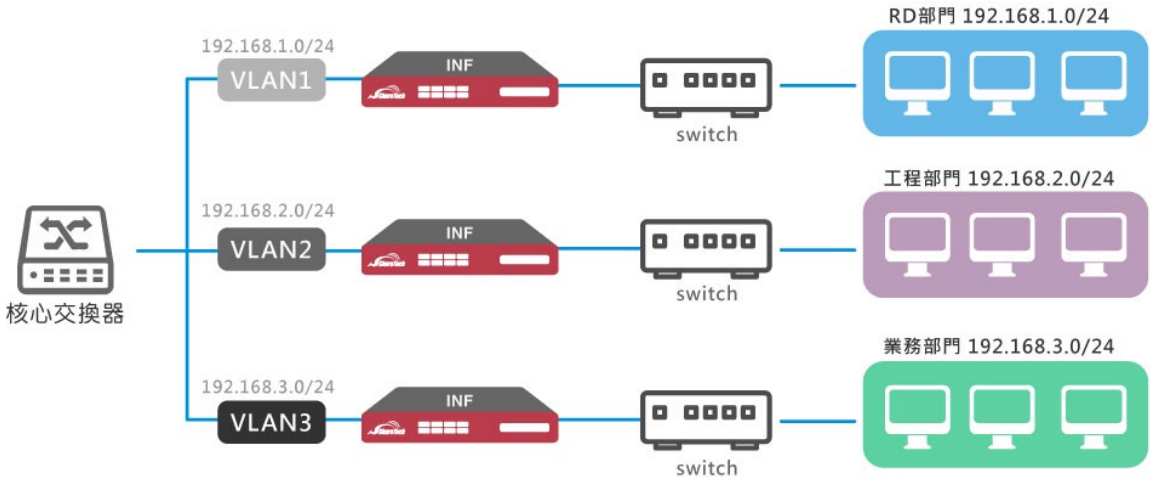


圖 77. 圖4-19 管制範例網路架構圖¶

- **管制範例：**

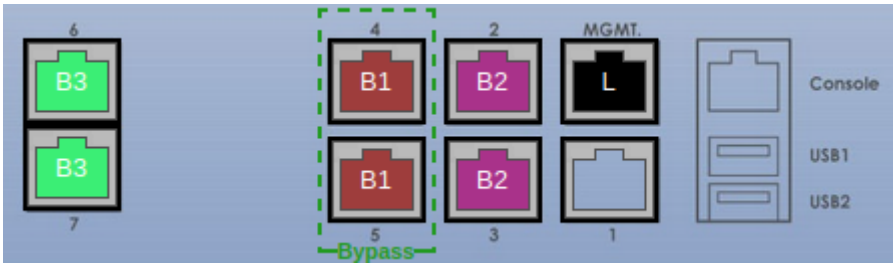
範例	環境架構	管理要求
1	不同部門	不同部門間，封包的控管。
2	跨Switch vlan	有多台Switch，針對Switch間的 Vlan Tag 封包進行管控
3	不同部門同區段	不同部門之間，隸屬與不同Switch，但區段相同時。
4	數據專線	公司內部有數據專線時，針對專線間的封包管理。

4-4-1、範例一：不同部門



這個架構下，每個部門都以不同網段區分。
在INF上可以劃出多個不同的Bridge介面，橋接在每個網段的核心交換器(core switch)和邊界交換器(edge switch)之間。
透過在條例上指定不同介面並加上如應用程式管制、流量掃毒等功能，就能達到對不同部門做相對應的管制。

1. 定義三對Bridge介面



2. 將各部門邊界交換器與核心交換器的連線接入對應的Bridge介面

3. 設定管制條例基本設定，定義受管理的介面

4. 設定管制條例進階設定、防護設定，對此條例做需要的管制、監控

設定完如下

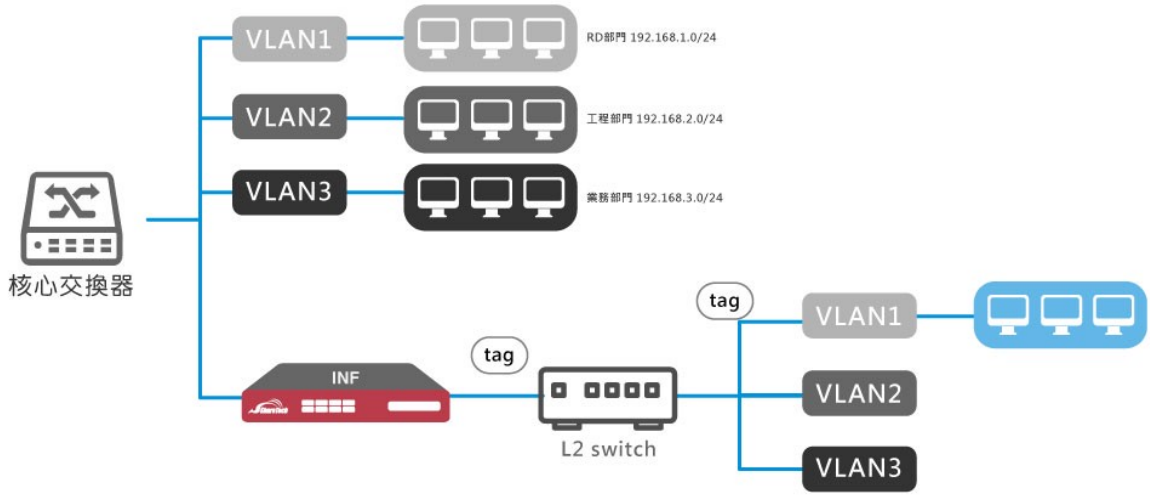
5. 也可以根據流量方向分開條例，這樣可以對進和出的流量做不同的管制、監控。

note

使用注意！

INF有 5 個 RJ45 自訂介面，兩個 SFP+ 自訂介面。若此範例要用一台 INF 達成，需有一對 Bridge 使用光電轉換。

4-4-2、範例二：跨switch VLAN



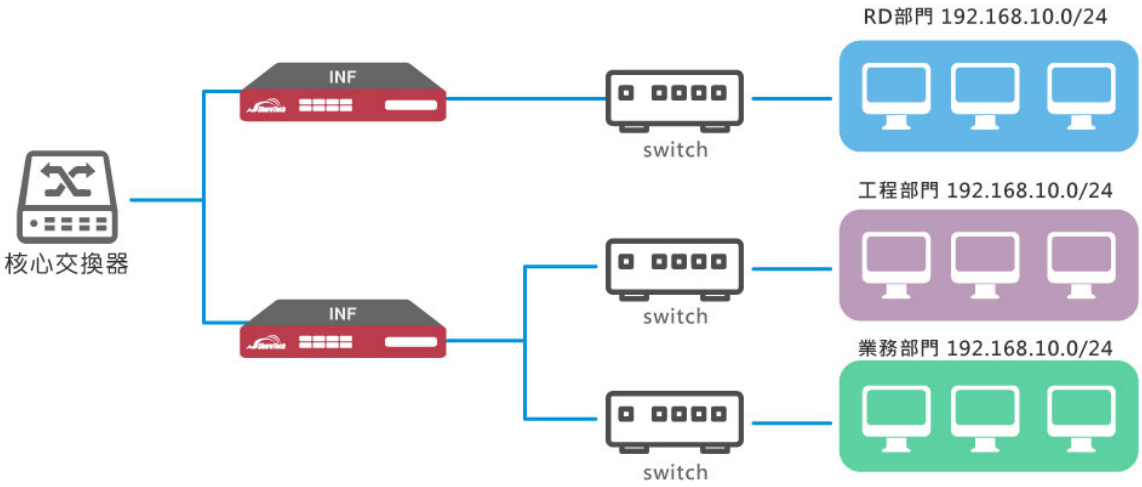
一般狀況下INF不會對帶有VLAN tag的封包做識別，
只要在 系統設定 > 基本設定 > 一般設定，勾選 管制 Bridge Vlan 封包，再配上管制條例，就能達成對tag封包的管制。

1. 建立Bridge介面後，在 系統設定 > 基本設定 > 一般設定，勾選 管制 Bridge Vlan 封包。

這樣即使來源有不同的tag，INF也可以知道封包的來源和目的IP，

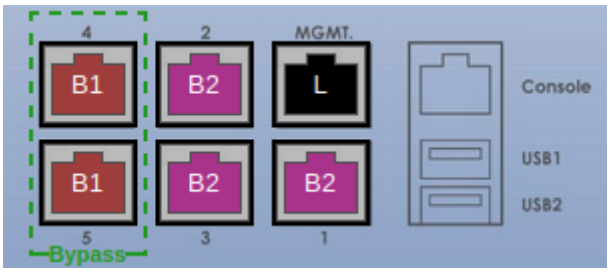
2. 這個架構下，即使是同 VLAN，只要不屬於相同 L2 switch，INF 也能使用 IP 位址達到管理效果
例如：讓192.168.3.10不能連到192.168.3.20。若 PORT 2 是接核心交換器的介面，只要指定 PORT 2 和來源、目的IP，就能達成拒絕同網段連線的管制

4-4-3、範例三：不同部門同區段



如果同一部門的 IP 來源為同一交換器但一開始沒有依照部門劃分網段，又想起到管理的作用。一樣可以將線路接進Bridge介面，再用 IP 進行管制。
除了用 IP 做管控依據，也可以搭配指定來源介面。這樣在沒有劃分網段的狀況下，同樣有管制的能力。

1. 建立多個實體介面的單一Bridge，並接上線路，如圖中的 Bridge 2



2. 建立各部門的群組

3. 建立管制規則。例如：工程部門來源為 PORT1，業務部門來源為 PORT2，INF用 PORT3 接到核心交換器。
要讓兩個部門不能互連，設定如下

設定來自 PORT1 的工程部門不能連到業務部門

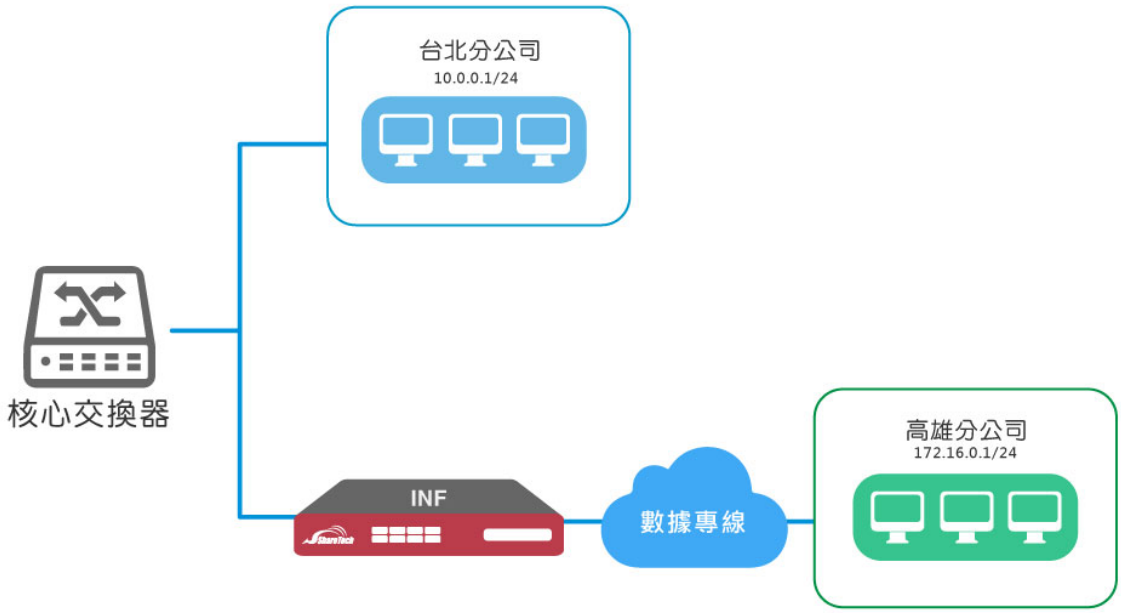
設定來自 PORT2 的業務部門不能連到工程部門

設定來自三個PORT的流量可以互通

因為條例順序的關係，部門間的流量會先被第 1 和第 2 條條例阻擋，而兩部門和核心交換器之間的流量會透過第 3 條條例通行。
若加上不在同一台 INF 管控的RD部門，同樣不可連到其他部門。則這台 INF 的條例可加上

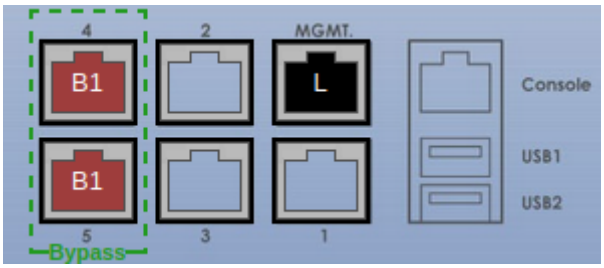
拒絕來自 PORT3(核心交換器) RD部門的流量

4-4-4、範例四：數據專線



INF 也可以應用在兩地的數據專線之間，只要將 INF 架設在專線數據機之前，就能對經過的流量進行檢測

1. 建立一對 Bridge 介面，並將線路接上



2. 建立條例讓來往的封包互通即可。另外視需求加上管制的選項

優先權	管制條例名稱	來源介面	通訊協定	來源網路	目的網路	來源埠	目的埠	動作	啟用	通用工業協定	進階設定	編輯 / 刪除	統計(Packets/Bytes)
1		Bridge1 - Port04	ANY	Any	Any								0 / 0
2		Bridge1 - Port05	ANY	Any	Any								0 / 0

第5章 管理目標

INF 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。

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

INF 支援 IPV4 跟 IPV6 位址模式，主選單 MENU 上方顯示藍色的按鈕表示目前的模式，|image177| 代表目前顯示/設定的是 IPV4 的位址模式， |image178| 代表顯示/設定的是 IPV6 的位址模式。

直接點選灰色按鈕（如 |image176| ），可將顯示跟設定切換到另一模式。

這 2 個按鈕適用於整個系統，設定時隨時切換，設定畫面會跟著切換成選擇的 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

此功能僅限 IPV4 使用。
任何設備，只要有網路封包經過 INF，不論是外部還是內部，系統都會把它記錄下來，方便管理者建立位址表。
點選|image179|的圖示，系統會列出所有記錄內的電腦名稱、IP 位址跟 MAC 位址，甚至連從 DHCP 伺服器取得的固定 IP 位址，
選擇要增加的 IP 或是 MAC 位址後，按下|image180| 鈕即可加入位址表中。

圖 78. 圖5-1 選取 IP 位址¶

● 新增位址表

按下 |image182| 鈕後，就可以開始建立位址表，首先選擇設定方式，每一種方式都有它的使用目的：

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 INF 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，代表這部電腦會由 DHCP 伺服器發放固定的 IPV4 位址。可參考 6-1-3、DHCP 固定 IP 位址 章節。

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。

此例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.*。

7、預設 Domain 黑名單

【電腦名稱】：這個網域的代表名稱，例如：張三的家。

【預設名單】：選擇預先設定的黑名單群組，讓它成為可在條例內管控的來源目的網路對象。

【Domain 測試】：輸入可疑的網址並點選「測試」，查看此網址是否在預設黑名單中。

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 |image183| 鈕後，就可以開始建立位址表群組。

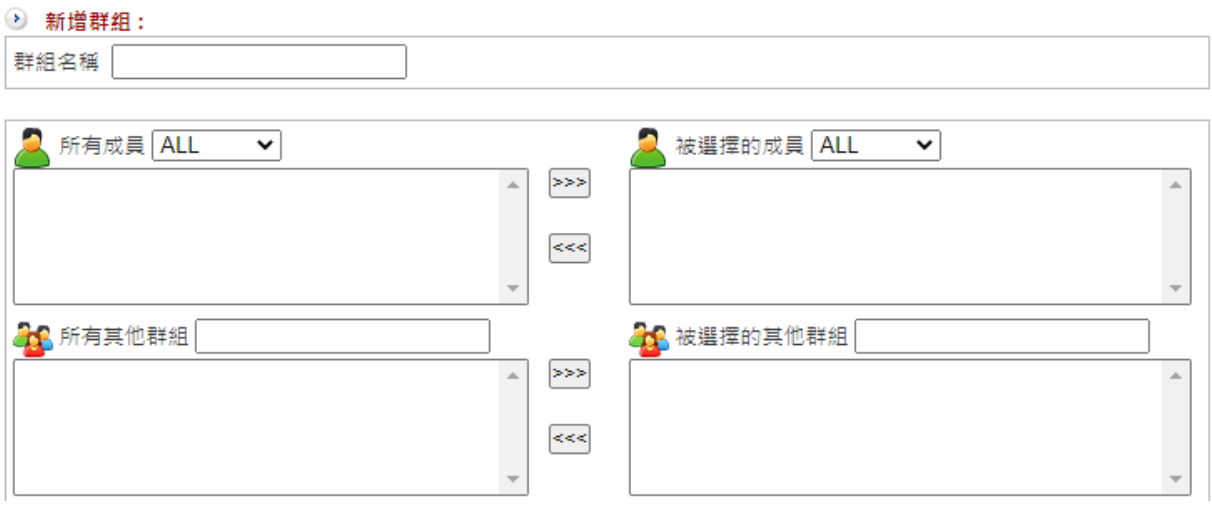


圖 79. 圖5-2 選取位址表群組¶

【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會於此顯示。

【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 |image184| 即可加入。

【所有其他群組】：已經建立的位址表群組會在這裡顯示。

【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 |image185| 即可加入。

【使用者自訂】：若沒有事先建立位址表，也可以在此區手動加入，可輸入多筆資料，每一筆為一行。

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) 等等。

在【輔助選取】中可從基本服務表中選取服務，包含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。
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不一樣，
以 HTTP 協定為例，在服務表中把它定義成 TCP 80 Port 代表 HTTP 協定，
但在實際運作上，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，不會管來源跟目的 Port 號，只要封包內容是執行 HTTP(Web) 協定的都可以，所以應用程式對於執行協定的辨識是更準確。

系統管理者可以在「服務表 > 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。
若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。

5-2-1、基本服務表

基本服務：

ANY ANY (ANY)	TCP AFPoverTCP (548)	TCP AOL (5190)	TCP BGP (179)
UDP DNS (53)	TCP FTP (21)	TCP Finger (79)	TCP GNUTella (6346)
TCP Gopher (70)	TCP H323 (NetMeeting) (1720)	TCP HTTP (80)	TCP HTTPS (443)
TCP ICQ (4000)	UDP IKE (500)	TCP IMAP over SSL (993)	TCP IMAP (143)
TCP Ident (113)	TCP L2TP (1701)	TCP LDAP Admin (3407)	TCP LDAP over SSL (636)
TCP LDAP (389)	TCP MSN Messenger (1863)	TCP NNTP (119)	UDP NTP (123)
TCP NTTP over SSL (563)	TCP POP2 (109)	TCP POP3 over SSL (995)	TCP POP3 (110)
TCP PPTP (1723)	UDP RIP (520)	TCP RLOGIN (513)	TCP Real Audio (7070)
TCP SFTP (115)	TCP SMTP over SSL (465)	TCP SMTP (25)	UDP SNMP (161)
TCP SSH (22)	UDP SYSLOG (514)	UDP TFTP (69)	TCP Telnet (23)
TCP Terminal (3389)	UDP UUCP (540)	TCP VNC (5900)	TCP WAIS (210)
TCP WINFRAME (1494)	TCP Yahoo (5050)		

圖 80. 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 INF 上。

圖示	說明
|image189|	任何服務。
|image190|	TCP服務，如：Gopher、ICQ、Ident、LDAP、NTTP over SSL、PPTP、SFTP、SSH、
|image191|	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，此頁面有 8 筆空白的欄位，管理者從編號 1 開始依序加入服務表，若要加入這個服務群組的服務項目多於 8 筆，按下|image192|後，即會新增空白的欄位。

圖 81. 圖5-4 建立服務群組¶

【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】：選取內建的基本服務表。（圖5-5）

【通訊協定】：選擇這一筆服務是使用 TCP、UDP、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，也就等於 |image193|。

- **輔助選取**

點選 |image187| 的圖示，會出現新視窗顯示 INF 內建的基本服務表，供管理者選擇。
可於視窗左上選單選擇 TCP、UDP 或是其他通訊協定，即會切換使用的通訊協定。

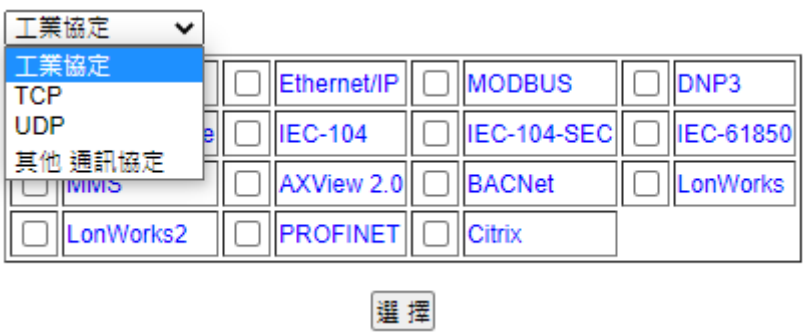


圖 82. 圖5-5 輔助選取基本服務表¶

【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。

➤ 建立新的服務群組後，INF 會把所有定義好的服務群組列表，同時標示它使用的埠號。

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 83. 圖5-6 服務群組列表¶

5-3、時間表

INF 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。

按下 |image183| 鈕，新增時間表：

時間表的設定週期有 3 種，模式一：以周為週期，設定每天生效的時間；模式二：自訂起訖日期及時間；模式三：利用圖表選取設定時間

【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 3 種模式可以選取。

· 模式一：以周為週期，設定每天生效的時間區間。
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5-7 ）

圖 84. 圖5-7 以周為週期的時間表¶

· 模式二：自訂起訖日期及時間，管理者設定特定日期下會生效的時間表，例如：2016年7月1日開始到2016年12月31日結束。（ 圖5-8 ）

圖 85. 圖5-8 自訂日期的時間表¶

· 模式三：利用圖表選擇的方式，定義每週生效的時間。和模式一不同在於，可以在一天內設定多個生效的時間區間。如下圖：
週一到週五設定的時間為06:00-11:59, 13:00-20:59，週六、日設定整天

➤ 在管制條例列表中出現|image198|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

INF 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 Zone Out (TX) / Zone In (RX) 流量，
再加上頻寬優先權的概念，讓優先權高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，另一種是此條例內每個來源 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 Zone Out (TX) / Zone In (RX) 流量，
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，Zone Out (TX) / Zone In (RX) 流量都會被限制在 10Mbps 。

5-4-1、QoS 設定

- **設定介面速度**

在此設定每一個介面的最快網路速度，分別是 Zone Out (TX) 流量、Zone In (RX) 流量。
進去實體 Port 的網路封包為 Zone In (RX) 流量，從實體 Port 送到下端設備的網路封包為 Zone Out (TX) 流量。

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 類型網路就有方向性的問題，
思考一下線路商提供的上傳跟下載速度，對承接網路封包的 INF 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 速度時就需要特別注意。

QoS 設定：

啟用	介面	Port	Zone Out (TX) 流量	Zone In (RX) 流量
☐	LAN (LAN)	MGMT	1024000 Kbps	1024000 Kbps
☐	Bridge1 (有線區)	Port04	1024000 Kbps	1024000 Kbps
		Port05	1024000 Kbps	1024000 Kbps

圖 86. 圖5-9 自訂介面的速度¶

在表格勾選啟用，表示將此介面啟用頻寬管理。
INF 預設會把所有的 Zone Out (TX) 流量、Zone In (RX) 流量設為 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，使其符合實際的線路狀況，儲存後此設定值就是設定頻寬表時最高的速度限制。

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，也可以在這邊執行修改與刪除。

● 新增頻寬表

按下列表下方的 |image183| 鈕，新增一筆 QoS :

圖 87. 圖5-10 頻寬表設定¶

【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，INF 會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。數字越低表示優先權越高。

【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】。

· 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。

圖 88. 圖5-11 基本模式¶

· 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。

圖 89. 圖5-12 進階模式¶

【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】（預設）跟【每個來源 IP 能使用的頻寬】，詳細說明如下：

· 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，也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 / 9.9Mbps 時，192.168.1.3 只能分配到 0.1Mbps / 0.1Mbps 的頻寬。

· 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，也就是每一個 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 / 10Mbps的條例，當 192.168.1.2 最高可以用到10Mbps / 10Mbps，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，
它的總額是 100*20Mbps=2000Mbps=2G，這已經超過介面的最高數值 1Gbps，這樣的狀況會導致頻寬分配不準確。

【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 INF 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 INF 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。

note

在設定頻寬表時務必要注意設定的介面，因為 INF 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。

5-5、應用程式管制

INF 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，比傳統以 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 TCP443 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，
但是現在因為安全因素，很多網路通訊軟體開始使用 SSL 加密技術，例如：SSL VPN，封掉 TCP443 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 分類就沒辦法滿足現在的網路需求，因此 INF 導入 DPI 技術，
它不是單純使用 TCP / UDP 的埠號為判斷依據，而是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。

INF 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 INF 的 5-6、URL 管理 功能管理這一些 SAAS 的服務。

5-5-1、應用程式管制

要管理超過 900 種的應用程式管理是複雜的，因此 INF 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，選擇完成後建立群組並可以到管制條例中套用。

● 應用程式資訊

INF 的應用程式的特徵值需要額外授權，授權到期後，系統不會再更新特徵值，管理者設定的管制項目就可能有不準確的狀況。

圖 90. 圖5-13 應用程式資訊¶

【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。

【授權期限】：目前應用程式的到期日。

【服務狀態】：應用程式辨識是啟用或是關閉。

● 應用程式管制

建立完成的應用程式列表如下：

	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 91. 圖5-14 建立好的應用程式¶

> **Note**
>
> 建立好的應用程式需要再到 第4章 管制條例 中決定它的用途，例如：建立一個應用程式群組，在管制條例中選擇哪些成員要套用此群組，是執行允許或是禁止。

● 新增應用程式管制

管理者可以新增很多筆應用程式，或在某個應用程式群組內包含多種服務。
按下 |image183| 鈕，新增應用程式群組：

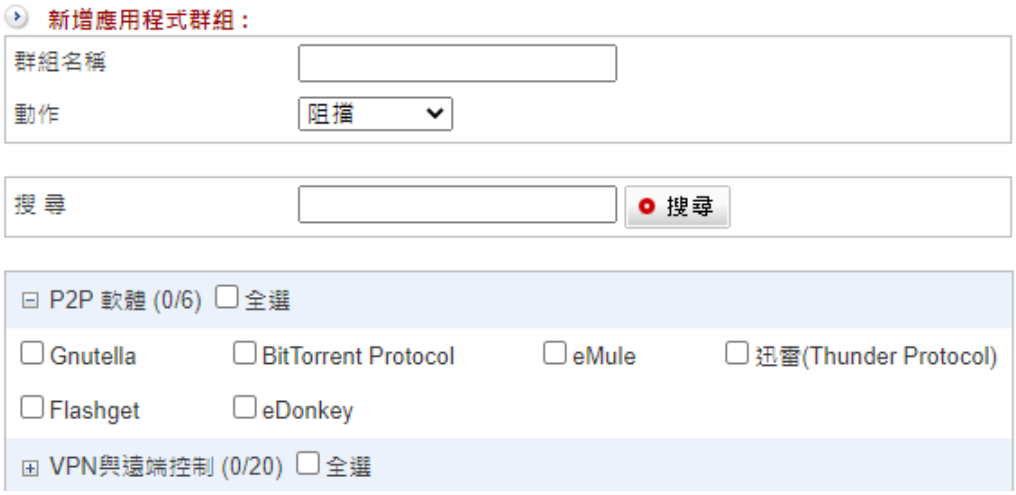


圖 92. 圖5-15 選取應用程式¶

【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 個選項分別說明如下：

· 阻擋：把比對出符合特徵值的應用程式阻擋。

· 阻擋+紀錄：把比對出符合特徵值的應用程式阻擋，並且記錄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。

【已選擇項目】：當勾選下方要管制的應用程式時，在這邊顯示已勾選的項目。可將選項收合避免影響操作。

【選擇應用程式】：每個分類下的選項可全選或個別選取，已選取的項目會用顏色區分並在該分類名稱後顯示此分類已選數量。

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，
管理者也可在管制紀錄中查詢特定時間內哪一些服務被允許通過或禁止。

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 93. 圖5-16 應用程式紀錄¶

5-6、URL 管理

INF 的 URL 管理，除了可管理傳統的 HTTP(Web) 型網站外，HTTPS SSL 加密型網站也可以管理，
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，除了可以增加工作效率之外，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。

當使用者欲瀏覽黑名單網址時，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，這些阻擋紀錄也會被記錄下來，管理者日後可以查詢。

5-6-1、URL 設定

INF 在阻止使用者觀看黑名單中設定的網頁時，會把使用者的瀏覽器轉向到預設或自訂的阻擋網頁。
管理者可以針對不同的黑名單設定頁面阻擋的顯示畫面。

按下 |image183| 鈕，新增 URL 群組：

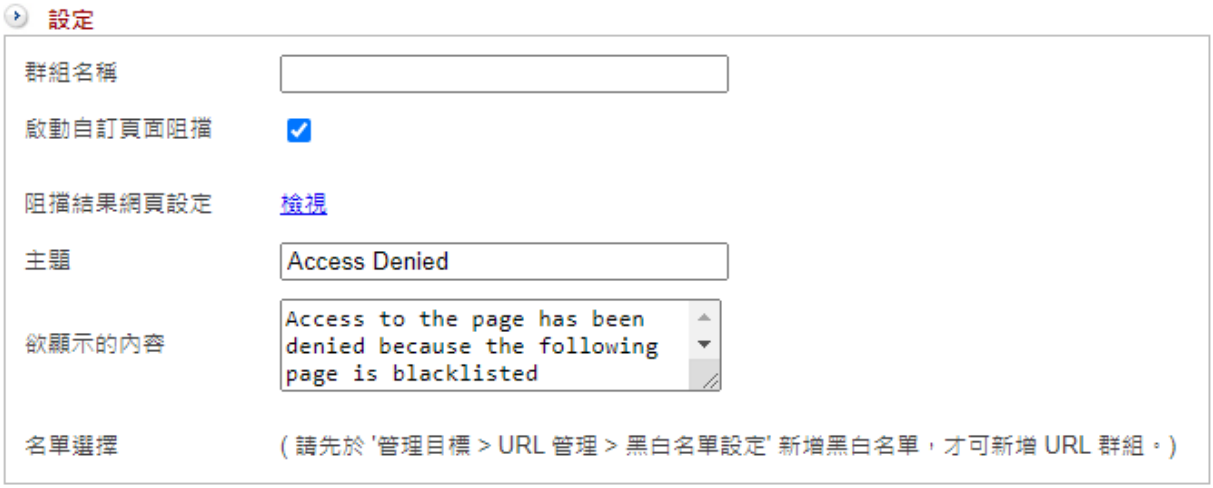


圖 94. 圖5-17 URL 設定 > 新增¶

【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】：預設沒有勾選，所有的阻擋網頁都會使用在 5-6-3、其他設定 預設的頁面阻擋設定。
啟用後，系統會展開下列設定項讓管理者修改。

【阻擋結果網頁設定】：點選檢視的按鈕就可以預覽目前的阻擋頁面設定。

【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】：INF 列出所有的黑、白名單供管理者選擇。

note

建立完成的 URL 會在【URL 設定】以表格顯示。
此處設定的管理規則只是一些管理物件，這一些物件仍需要到 第4章 管制條例 中決定哪一些 IP 位址要套用這一些規則。

5-6-2、黑白名單設定

WEB 資料庫資訊

INF 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。

1、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。
若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】按鈕測試。

圖 95. 圖5-18 WEB 資料庫設定¶

WEB 資料庫資訊顯示目前使用的模式及其授權狀態。

圖 96. 圖5-19 WEB 資料庫資訊¶

【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，可以切換到另一個模式。

【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，會顯示目前是啟用還是停用中。

2、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 97. 圖5-20 黑名單資料庫¶

黑白名單設定

所謂白名單就是可以瀏覽的網址，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。

按下 |image183| 鈕，新增黑白名單：

● 黑白名單基本設定

圖 98. 圖5-21 黑白名單基本設定¶

【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符合，模糊模式只要關鍵字部分符合。

例如欲封鎖 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，就可以將所有包含 yahoo 的網址都封鎖掉，在這樣的情況下，誤擋網站的機率相當高，
像是 abcyahoo 和 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。

● Sandstorm 服務

將 Sandstorm 會做管制的網址套用到黑名單中，可在 6-6、SandStorm 內調整風險程度來決定限制的網址量。
點選 |image210| 圖示，即可測試網址是否存在 SandStorm 資料庫。

● 自訂黑白名單設定

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。
一筆為一行，若有多筆可換行新增。

【URL 黑名單】：輸入黑名單的網址，例如： tw.news.yahoo.com/sports/ 或 www.pchome.com.tw 等等。

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

【Domain 黑名單】：依照網域來認定黑白名單，可使用特殊字元「*」來包含目標網域的所有子網域。

● 預設黑名單設定

當名單模式選擇【黑名單】時才會出現此項目，選擇【白名單】這一個項目就會被隱藏。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。

為了避免自行輸入的黑名單跟資料庫內的 URL 資料庫重複，INF 有 URL 測試的功能，點選預設黑名單設定旁的 |image210| 圖示，即可進入測試。
如圖5-22：輸入 yahoo.com.tw 測試是否存在預設的黑名單資料庫中，結果為不存在。

圖 99. 圖5-22 URL 測試¶

● 其他黑白名單設定

INF 的黑名單設定支援群組包含群組的組合，
例如：事先已經建立 2 個黑名單群組 – 黑名單 A 跟黑名單 B，
新增黑名單 C 時，除了黑名單 C 自己內建的黑名單之外，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，名單模式為【白名單】時，則只會顯示白名單群組。

5-6-3、其他設定

當使用者瀏覽黑名單網站時，INF 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：

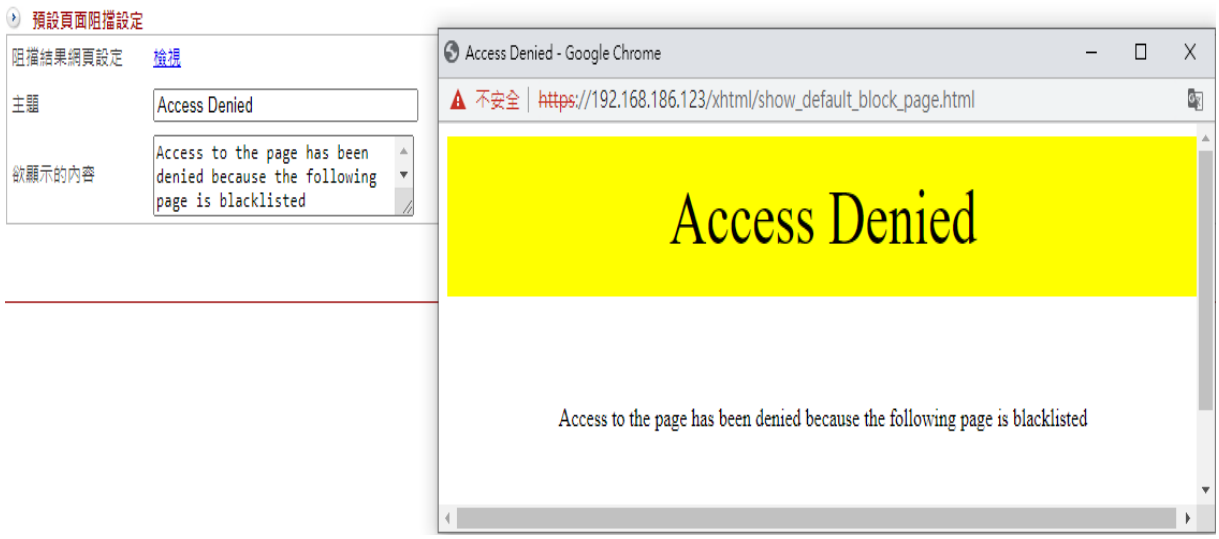


圖 100. 圖5-23 預設黑名單阻擋網頁設計¶

【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。

5-6-4、記錄

管理者制定好要管理的 URL 並到管制條例中套用後，不論是允許或是禁止的動作，只要是滿足條件的 URL 項目都會被記錄下來，管理者可在此依條件查詢。

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 中沒有定義這樣的攻擊模式，可是這樣的任意攻擊卻是真實存在。

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）

1、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。

2、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。

3、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。

4、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，它自己無法回應給自己 SYN-ACK 封包，因而造成系統當機。

5、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 回覆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。

6、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。

7、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。

Tip

影片參考｜眾至NU系列 UTM教學 防火牆防護系統.介面.條例

5-7-1、防火牆功能

針對 DOS 或是 DDOS 攻擊的防護，INF 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 101. 圖5-25 防火牆的防護設定¶

● 共用設定

【永久封鎖】：同一來源 IP 觸發下方的各種偵測超過一定次數，則會永久封鎖。次數的判定可在 5-8-2、防護記錄 內查看。被封鎖的名單會顯示在【解除IP封鎖】的連結內。

● 偵測 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，超過設定數值，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 位址每秒能傳送的數量。
預設值是 100 封包/秒，超過設定數值，防火牆就會認為受保護的 IP 位址遭受攻擊。

【當來源地址超過最大流量時的阻擋時間】：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。

● 偵測 ICMP 攻擊設定值

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

【當來源地址超過最大流量時的阻擋時間】：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。

● 偵測 UDP 攻擊設定值

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

【當來源地址超過最大流量時的阻擋時間】：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。

● IP 位址封鎖

輸入要封鎖的來源 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會 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 192.168.1.1/24。

● IP 位址例外

輸入來源 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 全部接受 ，即使它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。

圖 102. 圖5-26 其他項目防護設定¶

這些防護規則，可以套用在 INF 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，

INF 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

INF 會記錄所有攻擊行為，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。

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 103. 圖5-27 防火牆防護記錄¶

第6章 網路服務

INF 提供的網路服務功能，說明如下：

1、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。

2、病毒引擎：
提供 ClamAV 跟 Kaspersky 掃毒引擎設定。

3、Sandstorm：

4、WEB 服務：
INF 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。

5、FTP 服務：

6、遠端記錄伺服器：

6-1、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，但執行速度仍不如第一版快，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，針對每項訊息有存取清單的限制。

● 啟用 SNMP 服務

圖 104. 圖6-6 SNMP 設定¶

【開機自動啟用】：是否讓 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，管理者可修改。

【聯絡人】：聯絡人的電子郵件帳號，預設為 help@common.com。

【註解】：可填入描述文字，預設為 Firewall。

【SNMPv3】：SNMPv3 是 SNMP 的安全版本，勾選啟動後將會套用以下的安全設定。若不勾選則使用 SNMPv2。

【安全等級】：AuthPriv（認證且加密）/ AuthNoPriv（認證但不加密）/ NoAuthNoPriv（不認證且不加密）。

【用戶名稱】：使用 SNMPv3 的使用者名稱。

【認證協議】：提供 MD5/SHA 兩種認證方式，其中 SHA 較為安全。

【認證密碼】：輸入認證用的密碼。

【加密協議】：提供 DES/AES 兩種加密方式，其中 AES 較為安全。

【加密密碼】：輸入加密用的密碼。

【限制來源 IP 存取】：限制以下設定的 IP 可否存取 SNMP，或不做限制。

6-2、病毒引擎

INF 提供 2 個掃毒引擎，一個是免費的 ClamAV 跟需要付費的 Kaspersky，
預設 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它提供，上傳 Kaspersky 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 提供 24 小時更新及維護病毒資料庫，任何人發現可疑病毒可以隨時跟他們取得聯繫，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】：清除所有更新紀錄。

【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。

6-2-2、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】：清除所有更新紀錄。

【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。

6-3、SandStorm

釣魚郵件及惡意網址猖獗，使用者常誤開或誤點到惡意的網址，而這一些惡意的木馬軟體或網址並非傳統的防毒軟體可以防護的，
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 INF 在這道防線上加入新型的防護機制。

6-3-1、Sandstorm

不論是使用者誤點惡意網址或是郵件中夾帶的附檔有惡意程式，Sandstorm 會自動比對，當有比對到這些惡意行為時，INF 會主動阻擋，且 Sandstorm 的資料會自動更新，讓 INF 維持有效阻擋。

● **Sandstorm**

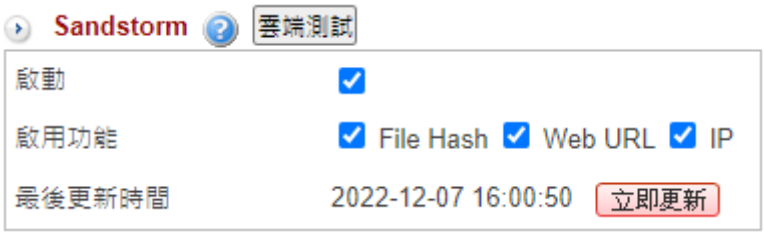


圖 105. 圖6-18 SandStorm 設定¶

【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，
而這 2 種類型分別有可能透過 WEB 或是郵件方式傳遞，管理者須確認需要的服務是 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。

【雲端測試】：點選後，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。
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。

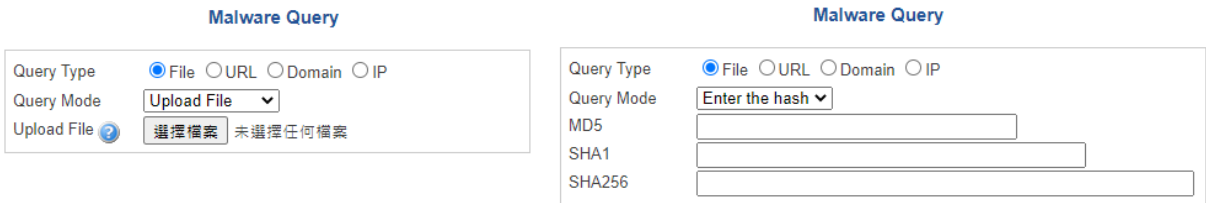


圖 106. 圖6-19 SandStorm 雲端測試¶

勾選 Sandstorm 的啟用功能後，該項目的詳細設定即會展開：

● **FILE Hash**

【版本】：目前的版本，括號內數字顯示為木馬數量。

【風險程度】：每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，若怕誤擋正常檔案傳輸，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，點選連結即可前往操作。

● 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，若怕誤擋，可以取消低風險的阻擋。

【WEB服務/郵件管理】：啟用這項功能，需要在管理介面上執行一些設定，點選連結即可前往操作。

【Url 測試】：點選後，系統會開啟另一個頁面，直接輸入 URL，資料庫會回應是否在黑名單中。

● 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，若怕誤擋，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】：點選後，系統會開啟另一個頁面，直接輸入 Domain 名稱，資料庫會回應是否在黑名單中。

6-3-2、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，系統會根據每一種攻擊特徵統計攻擊次數。
搜尋結果範例如下：

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 107. 圖6-20 Sandstorm 紀錄¶

【功能】：這筆阻擋紀錄是屬於 Sandstorm 的 3 個阻擋項目 File Hash、Web URL 跟 Domain 中的哪一類。

【惡意程式類型】：木馬或是釣魚郵件類型。

【次數】：同一個項目在統計期間內發生的次數。

如果管理者發現 Sandstorm 的阻擋誤擋了使用者正常行為，可以在啟用欄位把誤擋的項目停用，前往 Sandstorm 停用清單可查看完整停用資訊。

➤ 點選詳細的圖示，可看到內部哪個 IP 位址點了這個木馬等詳細資訊。

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 108. 圖6-21 Sandstorm 詳細紀錄¶

6-3-3、Sandstorm 停用清單

被 Sandstorm 阻擋的檔案、URL 跟 Domain 皆會詳列於此處。

6-4、WEB 服務

INF 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，使用者不需要在瀏覽器做任何設定即可運作。

HTTPS 部分因牽涉到 SSL 憑證信任，使用前管理者須在 INF 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、手機不接受非它信任的根憑證，所以 WEB 服務功能在 APPLE 系統上會失效。
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。

6-4-1、WEB

• 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。

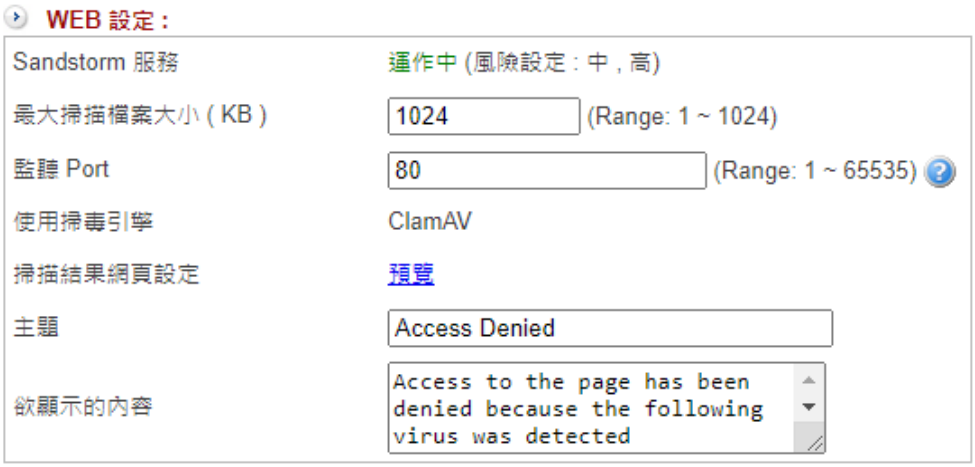


圖 109. 圖6-22 WEB 設定跟中毒網頁警示預覽¶

【最大掃描檔案大小 (KB)】：當 WEB 傳輸的檔案超過設定值，就無法執行掃毒，預設為 1024KBytes。

【監聽 Port】：哪一些 PORT 要導入 HTTP PROXY，預設為 80，管理者可以多筆輸入，例如：80,81,88，表示這些 PORT 都會導入 HTTP 檢查。

【使用掃毒引擎】：有 ClamAV 跟 Kaspersky 2 種選擇，預設是 ClamAV。
若 6-5、病毒引擎 中未啟用 Kaspersky 引擎，這邊就只會有 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。點選【預覽】可以查看輸入的主題和內容文字是否符合預期。

【主題】：輸入顯示的主題文字。

【欲顯示的內容】：輸入阻擋網頁顯示的內容。

• 加密連線設定

INF 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 管理前必須先產生 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，所以使用者在匯入憑證後不需要再設定任何瀏覽器項目。

圖 110. 圖6-23 HTTPS 設定¶

【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 INF 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，都需要再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 111. 圖6-24 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：ZONE 1 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】：原本，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；
為避免麻煩，ShareTech 提供 Windows 系統下的安裝程式，使用 3 大瀏覽器 IE、Chrome、 Firefox 的信任根憑證就可全部裝好。

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：ZONE 1 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 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。

【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。

【不導入服務來源 MAC 位址自訂】：連線若來自以下設定的 MAC 位址則不會導入 http/https 過濾。

【不導入服務來源 IP 自訂】：連線若來自以下設定的來源 IP 位址則不會導入 http/https 過濾。

【不導入服務 Domain 自訂】：連線到以下設定的網域不會導入 http/https 過濾。

【不導入服務目的 IP 自訂】：連線到以下設定的目的 IP 位址不會導入 http/https 過濾。

- **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 INF 發現這一個 IP 位址尚未安裝 SSL 憑證，就會自動將使用者的網頁轉向到下載憑證的網址。

圖 112. 圖6-25 SSL 憑證下載轉址¶

【轉址通訊埠】：使用的 PORT 號，必須是未被使用的。

【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：

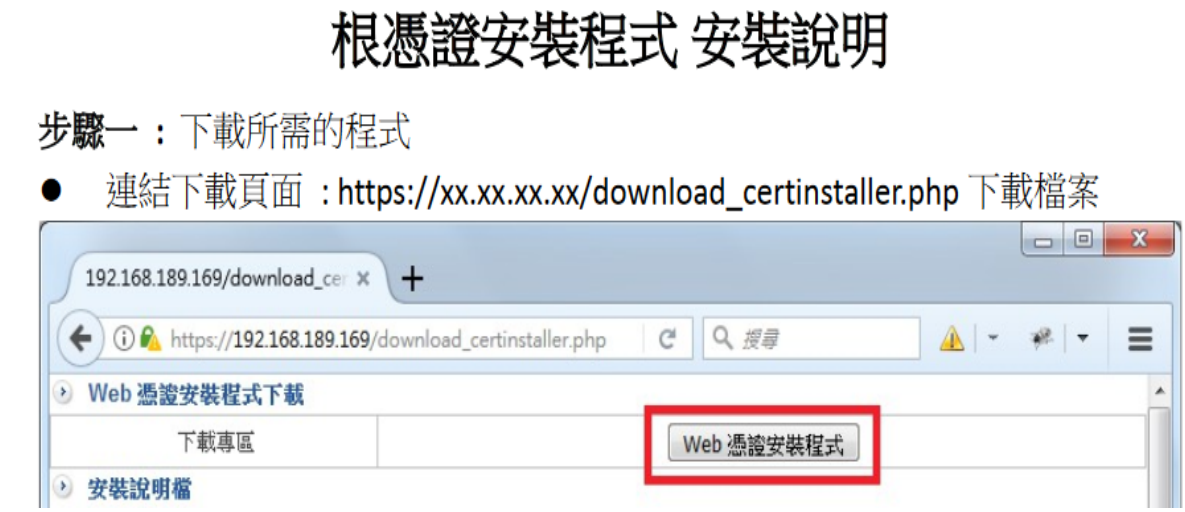


圖 113. 圖6-26 轉址網頁及安裝說明¶

- **SSL憑證資訊**

顯示目前 INF 使用的 SSL 憑證資訊，相關的憑證設定在「系統設定 > 2-11、SSL 憑證設定」，
如果 SSL 憑證有修改，每一個使用者的根憑證都需要再重新安裝及信任。

- **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。

6-4-2、HTTPS 連線記錄

選擇是否啟用 HTTPS 連線記錄，預設為關閉。
若啟用則所有透過 HTTPS proxy 連線的紀錄都會在這裡，可依條件搜尋。

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 114. 圖6-27 https 連線紀錄¶

6-4-3、白名單憑證

有一些網站或是應用程式經過 INF 後會產生憑證失敗，導致後續的服務都不能用，
此時，管理者可以將那一些失敗的憑證加入白名單，之後 INF 看到白名單的憑證，就不會進行置換的動作。

● 憑證失敗記錄

按下【搜尋】按鍵，INF 就會依條件搜尋失敗的憑證，並開啟新視窗顯示憑證失敗記錄。
可選擇憑證後按下【新增到白名單憑證】的按鈕，將這些憑證加入白名單。

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 115. 圖6-28 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。

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 116. 圖6-29 白名單憑證列表¶

6-5、FTP服務

6-6、遠端記錄伺服器

● **遠端連線設定**

INF 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 117. 圖6-33 遠端連線設定¶

【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】：設定的名稱會顯示於 syslog server ，這樣在 syslog server 就可以分辨紀錄來自哪一台設備。

● **Log 設定**

INF 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 7 種紀錄給 Syslog 伺服器，每個項目後都有不只一個的細項，由管理者自行決定。

1. 管理目標

2. 進階防護

3. 郵件管理

4. 內容記錄

5. VPN

6. 日誌

7. 系統狀態

第7章 進階防護

INF 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知道哪部電腦在哪個交換器 PORT 上，避免網路癱瘓。

協同防護的解決方案觀念很簡單，讓 UTM 跟 Switch 能夠互相溝通，提供各自優異的功能。
簡單來說，利用 UTM 偵測到的資安問題，除了本身對外的管制動作封鎖外，
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。

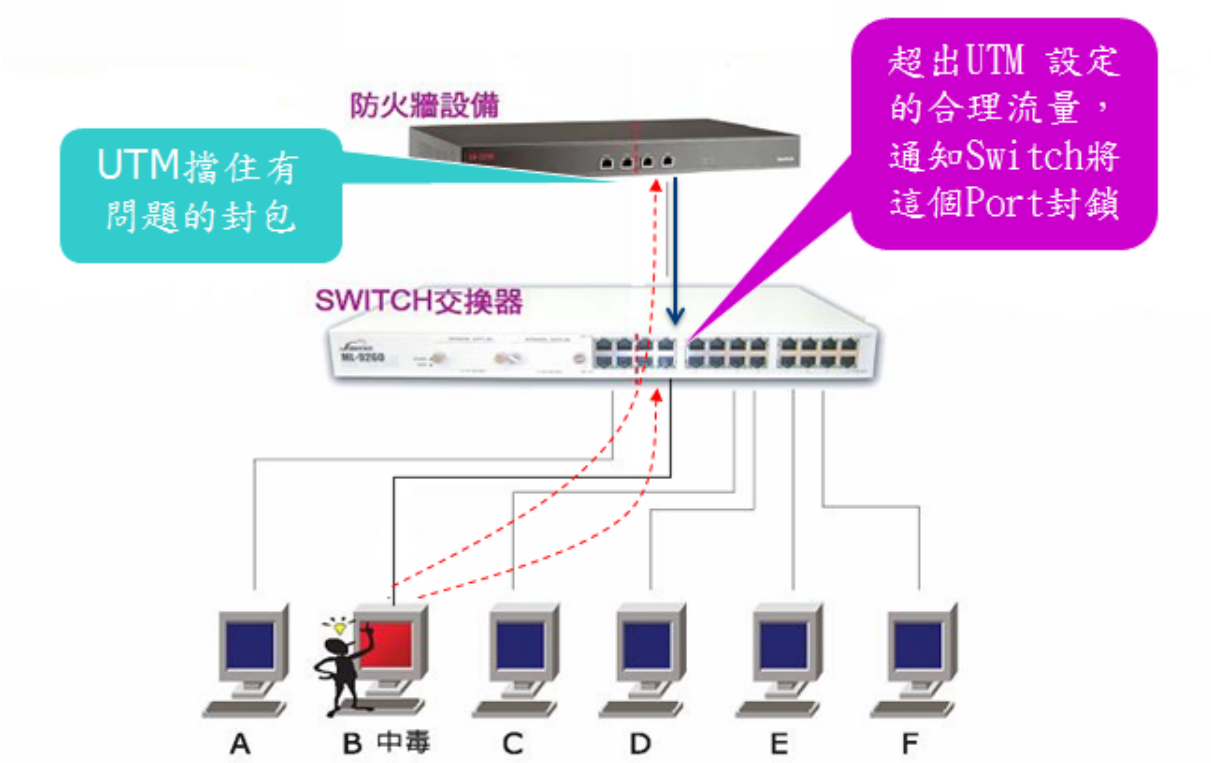


圖 118. 圖7-1 協同防禦基本概念¶

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因為費用或是部署上的問題，導致難以實行。
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範圍內。

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 INF 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，
可以採取的動作有記錄、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、記錄：
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時，
INF 會記錄觸發這個動作的事件跟來源 IP 位址。

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時，
INF 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時，
INF 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。

以看網路影片為例，大約使用 5Mbps 的下載頻寬且會持續一段時間，但是它不會占據上傳頻寬及超高的連線數，
管理者可以設定一個在正常網路行為下都不會被觸發的數值，讓 INF 幫您做第一線的把關。

當偵測到使用者異常行為後，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 關閉等處理方式，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，當有人違反規定時，可把他的頻寬縮小，讓他「慢慢地」使用網路。

在設定值的部分，紀錄設定 ≤ 通知設定 ≤ 阻擋設定。

7-1-1、共同設定

選擇偵測介面，INF 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

當有網路封包超過設定值的事件發生，INF 會記錄下當時的來源 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 INF 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。

圖 119. 圖7-2 異常 IP 分析的紀錄設定¶

【Session 量超過】：當任一個來源 IP 位址出去介面 (ZONE) 的 **網路連線數數量** 超過設定值且持續一段時間後，
INF 就會把來源 IP 位址跟超過的數值記錄下來。

【Zone Out (TX) 流量超過】：當任一個來源 IP 位址出去介面 (ZONE) 的 **Zone Out (TX) 流量** 超過設定值且持續一段時間後，
INF 就會把來源 IP 位址跟超過的數值記錄下來。

【Zone In (RX) 流量超過】：當任一個來源 IP 位址出去介面 (ZONE) 的 **Zone In (RX) 流量** 超過設定值且持續一段時間後，
INF 就會把來源 IP 位址跟超過的數值記錄下來。

7-1-3、通知設定

當有網路封包超過設定值的事件發生，INF 除了記錄下當時的來源 IP 位址、觸發數量及持續時間外，
也會馬上發出通知信，通知管理者有異常的流量發生，這個設定值適用於整個 INF 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。

圖 120. 圖7-3 異常 IP 分析的通知設定¶

【Session 量超過】：當任一個來源 IP 位址出去介面 (ZONE) 的 **網路連線數數量** 超過設定值且持續一段時間後，
INF 就會把來源 IP 位址跟超過的數值記錄下來並且發出通知信給管理者。

【Zone Out (TX) 流量超過】：當任一個來源 IP 位址出去介面 (ZONE) 的 **Zone Out (TX) 流量** 超過設定值且持續一段時間後，
INF 就會把來源 IP 位址跟超過的數值記錄下來並且發出通知信給管理者。

【Zone In (RX) 流量超過】：當任一個來源 IP 位址出去介面 (ZONE) 的 **Zone In (RX) 流量** 超過設定值且持續一段時間後，
INF 就會把來源 IP 位址跟超過的數值記錄下來並且發出通知信給管理者。

7-1-4、阻擋設定

當網路封包超過設定值的事件，INF 除了記錄下當時的來源 IP 位址、觸發數量及持續時間外，
也可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 INF 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。

圖 121. 圖7-4 異常 IP 分析的阻擋設定¶

【Session量超過】：當任一個來源 IP 位址出去介面 (ZONE) 的 **網路連線數數量** 超過設定值且持續一段時間後，
INF 就會把來源 IP 位址跟超過的數值記錄下來並且啟動預設的阻擋動作。

【Zone Out (TX) 流量超過】：當任一個來源 IP 位址出去介面 (ZONE) 的 **Zone Out (TX)** 超過設定值且持續一段時間後，
INF 就會把來源 IP 位址跟超過的數值記錄下來並且啟動預設的阻擋動作。

【Zone In (RX) 流量超過】：當任一個來源 IP 位址出去介面 (ZONE) 的 **Zone In (RX) 流量** 超過設定值且持續一段時間後，
INF 就會把來源 IP 位址跟超過的數值記錄下來並且啟動預設的阻擋動作。

● 動作

當設定值被觸發後，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：

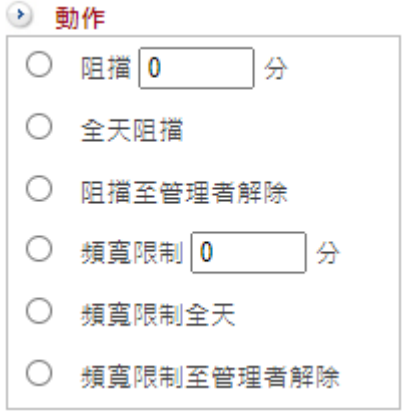


圖 122. 圖7-5 異常 IP 分析的阻擋動作¶

【阻擋數分鐘】：
異常流量可能是偶發性的，在阻擋數分鐘後，狀況就會自動會消失，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。

【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 位址阻擋一天 (24 H)，禁止出去介面 (ZONE)，但是介面內的互連封包並沒有影響。

【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)，直到管理者解除，但是介面內的互連封包並沒有影響。

【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。頻寬限制的數量則在【其他設定】中設定。

【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 H)。頻寬限制的數量則在【其他設定】中設定。

【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，直到管理者解除。頻寬限制的數量則在【其他設定】中設定。

● 其他設定

當基本設定的設定值被觸發後且選擇的動作是頻寬限制，則此處設定的頻寬數就會自動套用在出問題的電腦上。

圖 123. 圖7-6 異常 IP 分析的頻寬限制¶

【QoS 頻寬限制設定】：當任一個來源 IP 位址觸發設定值後，INF 會把這個來源 IP 位址的使用頻寬降為此設定的數值。

【網頁阻擋訊息】：執行限制頻寬時，在使用者的瀏覽網頁上出現此段文字，讓使用者知道目前已被限速中。

7-1-5、例外 IP 設定

INF 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，但是也可以針對特定的使用者，不要執行偵測動作。
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。

點選 ✚ 新增 ，新增一筆例外 IP 設定：

圖 124. 圖7-7 例外 IP 設置¶

【IP/網路遮罩】：哪些 IP 位址不要執行異常 IP 分析，可以是一個 IP 位址或是一個網段。
例如：可輸入 192.168.1.5/32（一個 IP 位址），也可填 192.168.1.1/24（一個 C 網段）。

【類別】：有 3 個類別，記錄、通知跟阻擋，可以複選。

【備註】：關於來源 IP 位址的備註說明。

7-1-6、異常紀錄

針對所有異常行為，系統會詳細記錄其時間、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。
管理者可依條件查詢異常紀錄：

圖 125. 圖7-8 異常紀錄¶

7-1-7、阻擋清單

列出目前被 INF 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

INF 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，避免網路癱瘓。

關於管理內部網路，每個管理者的需求都不同，有人希望掌握每一個 IP 位址的流量，有人關心每一部電腦的實際位置，
再加上內部網路的網路線盤根錯節，讓管理者頭疼。

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，
佐以階層的概念，將所有的交換器分層顯示，如圖7-8 所示，要找尋出發生問題的電腦實際位置時，按圖索驥就可以。

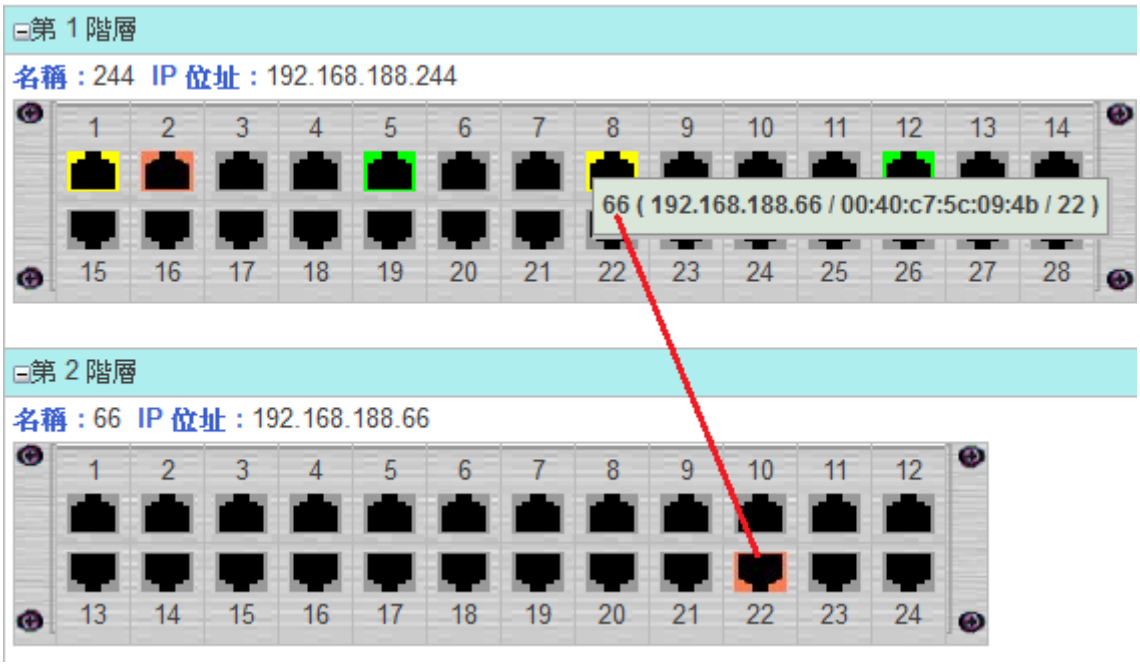


圖 126. 圖7-9 交換器的階層圖¶

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」。

● INF 支援交換器種類

INF 依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** 。

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，也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。

INF 根據不同的介面 (ZONE) 配置不同需求的交換器，
例如：ZONE 1 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 交換器就可以滿足需求。

7-2-1、Switch 設定

- **新增 Switch**

點選 ✚ 新增 ，新增交換器資料：

【介面】：新增的交換器是在哪一個介面 (ZONE)。

【交換機屬性】：新增的是哪一種交換器。依選擇的交換器屬性不同，顯示的設定選項也會有差異。

以下依交換器屬性分別說明詳細的設定方式：

A、SNMP 交換器設定

圖 127. 圖7-10 新增一台一般交換器¶

【型號】：INF 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 INF 的條件。

【名稱】：方便管理者辨識的交換器名稱，可以輸入任何中英文字，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，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】：此交換器的埠數。

【SNMP 登入名稱 (Read)】：INF 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 Read 權限的資訊。

【SNMP 登入名稱 (Write)】：INF 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「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。

B、協同防禦設定

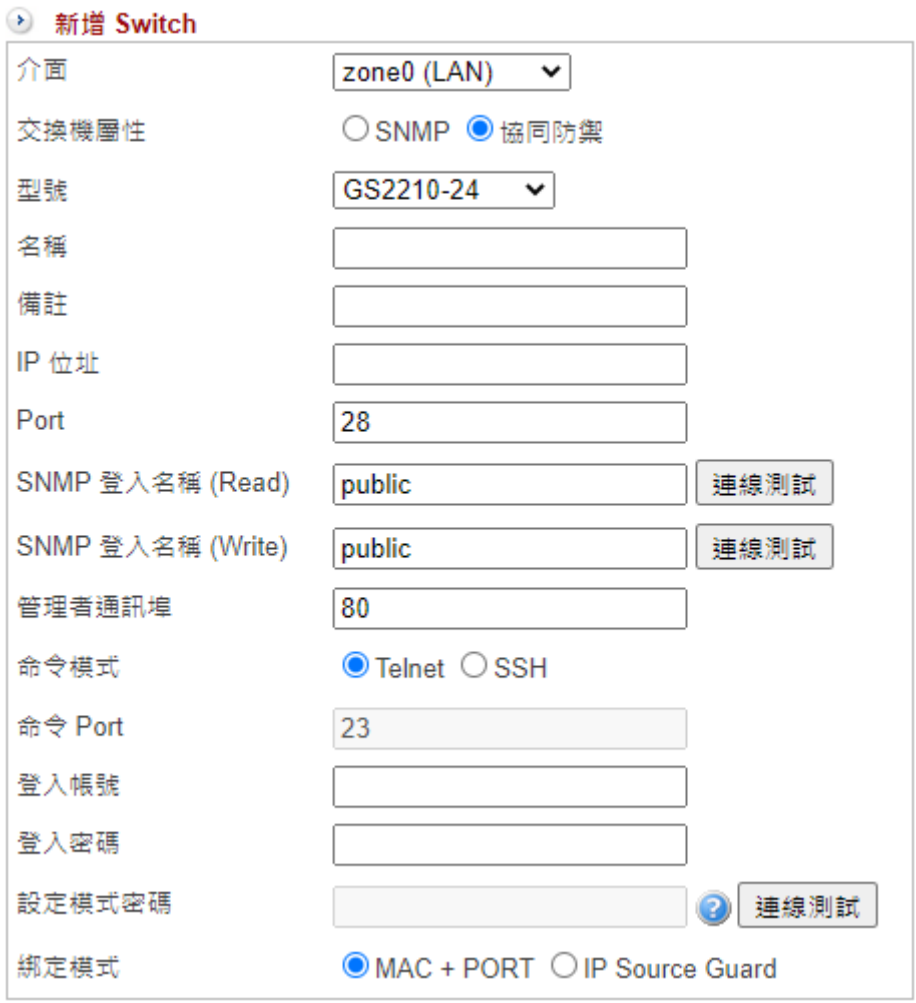


圖 128. 圖7-11 新增一台協同防禦交換器¶

【型號】：INF 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。

【名稱】：方便管理者辨識的交換器名稱，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】：交換器的 IP 位址，例如：192.168.2.55。

【Port】：此交換器的埠數。

【SNMP 登入名稱 (Read)】：INF 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 Read 權限的資訊。

【SNMP 登入名稱 (Write)】：INF 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。

【命令模式】：INF 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。

【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 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，則需要在這邊輸入，否則無法將正確的設定值加入協同防禦的交換器中。

【綁定模式】：INF 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。
並不一定每種協同防禦的交換器都支援此 3 種模式，**選擇交換器型號時，INF 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：

· 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 21 Port 上網，
當這部電腦改 IP 位址或是插入此交換器的其他 Port ，網路都會不通。

· 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 21 Port 上網，當這部電腦插入此交換器的其他 Port ，網路都會不通。

· IP Source Guard

此模式目前只支援 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，它的廣播封包通通會被禁止。

● 自動搜尋交換器

INF 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 INF 自動找尋所有介面 (ZONE) 下的 SNMP 交換器。
搜尋的結果會另外開啟視窗，找到要管理的交換器並在動作欄位按下 ，就進入交換器的設定模式。

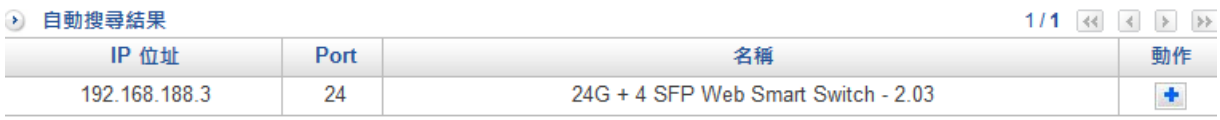


圖 129. 圖7-12 自動搜尋交換器¶

● Switch 列表

完成交換器的設定後，INF 會將所有的交換器列表，管理者可以在這裡查看設定的資訊是否正確。
點選 ，INF 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。
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。

圖 130. 圖7-13 交換器管理¶

7-2-2、網路狀態圖

對許多企業的網管人員來說查詢線路是麻煩且吃力的，尤其當線路環境很雜亂時要查出哪一台 PC 接在哪一台交換器上相對困難。

INF 結合協同防禦跟一般 SNMP 網管型的交換器，即時顯示內部網路的狀況，包含交換器之間的堆疊關係，
同時讓管理者對目前內部使用者的連線狀態一目了然，包含電腦接到哪一台交換器、是否為開機狀態，即使是串接到第二層交換器也清楚顯示。

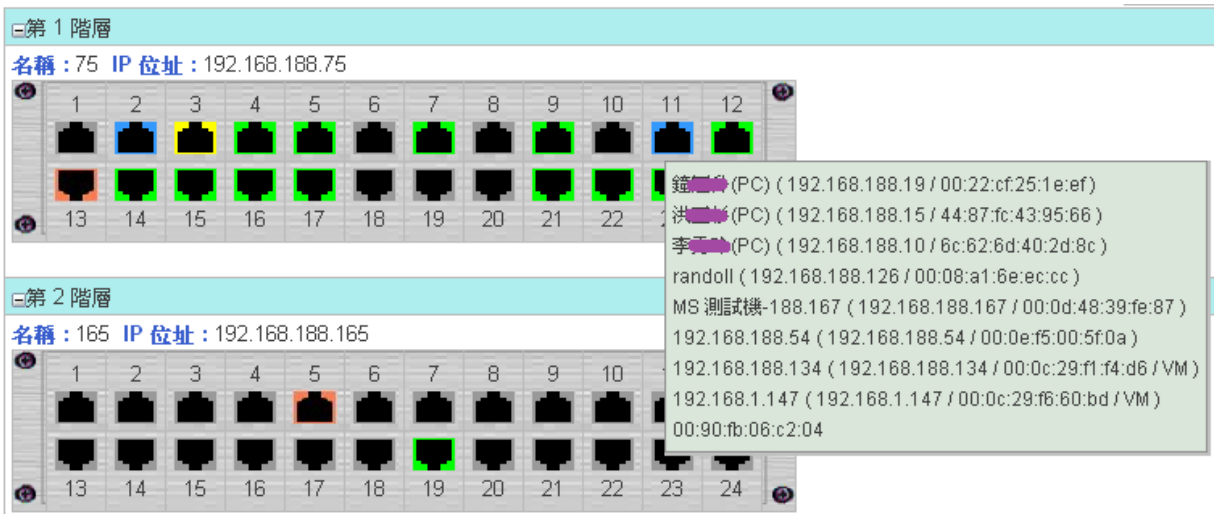


圖 131. 圖7-14 網路狀態圖¶

- **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，INF 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。

點選 ，可查看詳細圖示及名稱說明。

- **顯示方式：**

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，並可以選擇欲查看的介面 (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，可查詢這個 IP 位址在哪個交換機的第幾 PORT 上。

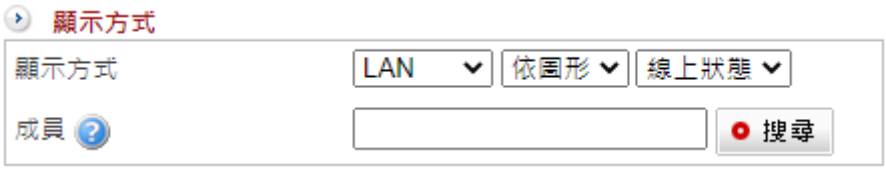


圖 132. 圖7-15 交換器跟電腦的顯示選項¶

在依圖形顯示的畫面點兩下  或  圖示，INF 介面會另開視窗顯示交換器中這個 PORT 的詳細資訊。

圖 133. 圖7-16 個別 PORT 的詳細資訊¶

【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。

【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。

【Zone Out (TX)/Zone In (RX)(bps)】：這個 IP 位址對網際網路的流入/流出流量。

7-2-3、綁定清單

為了網路安全因素或是方便內網管理，INF 的協同防禦機制可以設定在交換器的 Port 號上綁定某些特定電腦才能使用，非指定的電腦無法接上網路。

當在【Switch 設定】上設定交換器屬性為「協同防禦」，綁定模式為 IP + MAC + Port 或 MAC + Port 時，可在綁定清單做更進一步的設定。
在設定上 IP + MAC + Port 比 MAC + Port 多了一欄需輸入綁定的 IP 位址，其他的均相同，以下使用 IP + MAC + Port 說明。

● 新增綁定清單

點選 ✚ 新增 ，新增綁定清單：

圖 134. 圖7-17 綁定清單設定¶

【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。

【VLAN】：！！待確認！！

【綁定模式】：目前使用的綁定模式，是 IP + MAC + Port 或 MAC + Port。

7-2-4、IP Source Guard

INF 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。

當在【Switch 設定】上設定交換器屬性為「協同防禦」，綁定模式為 IP Source Guard 時，可在此做更進一步的設定。

● 新增 IP Source Guard 綁定

點選 ✚ 新增 ，新增一筆 IP+MAC+Port 的綁定：

圖 135. 圖7-18 新增一筆 IP source Guard 的 IP+MAC+Port 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，目前只支援 Zyxel 的交換器，例如：192.168.14.2。

【VLAN】： IP Source Guard 運作時需要搭配 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。

【Trusted Ports】：在這個 VLAN 下，哪幾個 Port 不執行 IP+MAC+Port 綁定。
在 Trusted Ports 下，任何 IP 及 MAC 位址都可以使用網路。

點選【輔助選取】，INF 就會顯示交換器的示意圖供管理者選擇，
點選屬於這個 VLAN 下的 就可以將此 Port 切換成 Trusted Port 狀態。

【輔助選取】：曾經連過交換器 VLAN 的 IP+MAC+Port 的資料，INF 可以自動將這一些資料帶入，不需再次輸入。

● 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。

在「IP Source Guard > DHCP Snooping 設定」選取欲設定的 IP 位址後，按下【設定】進入設定畫面。（圖7-20）

選擇 VLAN 前的 Box ，INF 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 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  狀態。

		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 136. 圖7-19 DHCP Snooping 設定¶

7-2-5、PoE 排程設定

INF 搭配 Zyxel 的 PoE 交換器提供供電時間管控，點選 ✚ 新增 新增排程：

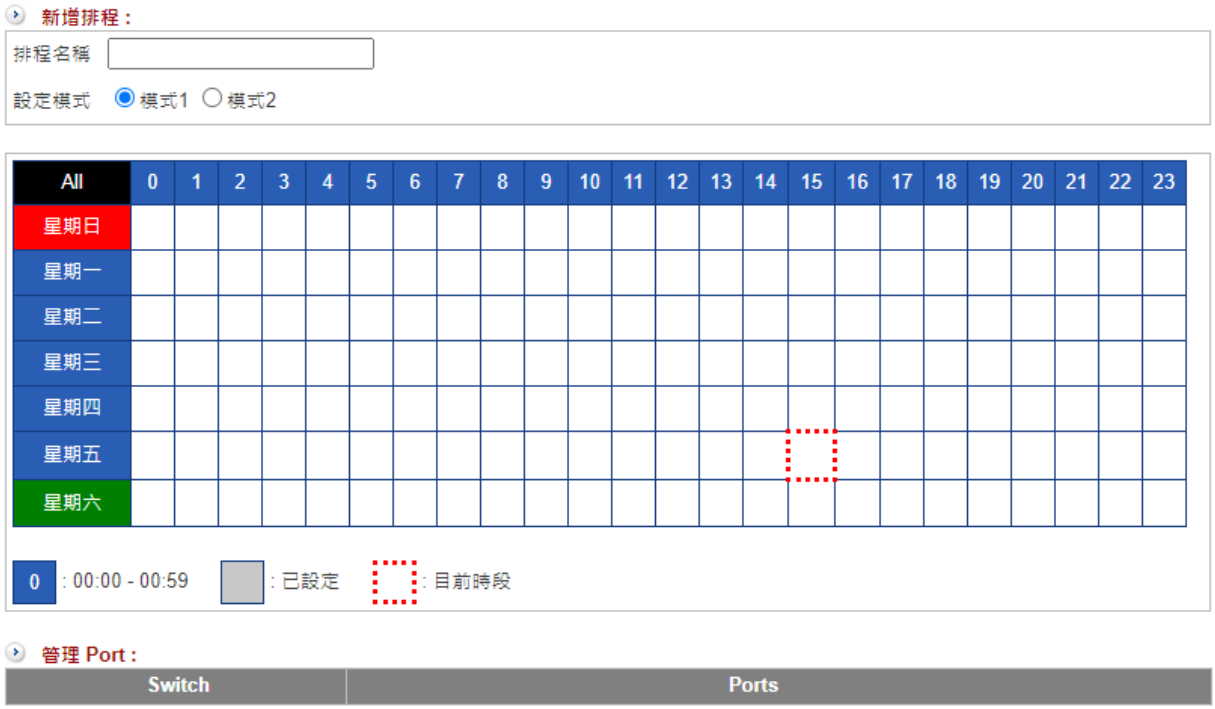


圖 137. 圖7-20 PoE 的排程設定¶

【排程名稱】：設定 PoE 排程名稱。

【設定模式】：有 2 種模式可以選擇。

- 模式一：以小時為單位，將一週的週期表列出，管理點選要管理的時間段就可以。
- 模式二：設定起訖日期時間。

【管理 Port】：系統會列出可新增 PoE 排程的交換器，在交換器下勾選要執行排程的 port。

7-3、內網防護

在內部網路的安全防護中，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，
因通訊協定的先天缺陷，導致這一類的攻擊行為難以被偵測到，
即使找到攻擊者，偵測機制也無法跟第一線的 UTM 或是交換器互相溝通，無法立即封鎖。
傳統的方式是發生問題時，到每一台交換器上拔線測試，而 INF 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，INF 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。

> **note**
>
> **封鎖選項中的「自動封鎖」與「進階封鎖」：**
> 當交換器是支援協同防禦的智慧型交換器，勾選「自動封鎖」表示當偵測機制觸發時，直接將在交換器中的預設管制 Port 的電腦封鎖；
> 如果也勾選了「進階封鎖」，因為非智慧型交換器，無法詳細管理到 Port，所以有可能發生在這個 Port 底下的其他電腦被誤封鎖。

● ARP 封包警戒值

ARP 的攻擊對 UTM 設備來說較難處理，因為 ARP 是廣播型的封包，是在尚未建立 TCP/UDP 連線前就已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，此時對方是處於 ARP 攻擊前的準備，尚未發動任何攻擊，
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。

萬一，偵測到內部有受害者出現，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，
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。

在 ARP 封包警戒值設定：

圖 138. 圖7-21 ARP 偵測機制¶

【每個來源 IP 位址每秒發送超過】：每個來源 IP 位址每秒發送超過多少個 ARP 要求，就會被 INF 視為不正常行為。

預設為 100 個，數值越大，偵測的靈敏度越低；不過相對地，靈敏度越高也越常發生誤判。

【自動封鎖】：偵測到 ARP 異常行為時，INF 主動封鎖攻擊者的交換器 PORT。

【信任位址】：輸入不執行 ARP 異常行為偵測的 IP 位址，可換行新增下一筆。

- **偽造者偵測：IP/MAC**

圖 139. 圖7-22 偽造 IP / MAC 偵測¶

INF 內建的偵測機制，可以減輕內部 IP 衝突或 MAC 衝突方面的困擾。

【IP 位址衝突偵測】：是否啟用這項功能，預設為關閉。

【自動封鎖】：偵測到 IP 位址衝突時，INF 主動封鎖偽造 IP 的電腦。

【信任位址】：輸入不執行 IP 位址衝突偵測的 IP 位址，可換行新增下一筆。

【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，INF 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，可換行新增下一筆。

- **協同防禦**

搭配在「進階防護 > 異常 IP 分析 > 7-1-4、阻擋設定 」的設定。
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 TX/RX 流量，

INF 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 140. 圖7-23 異常 IP 分析跟協同交換器連動¶

【連動異常 IP 阻擋清單 Port 關閉】：若偵測介面有 IP 出現在「異常 IP 阻擋清單」，則封鎖該 port。

【連動 IPS Port 關閉】：若偵測介面有 IP 出現在「IPS 紀錄」中，則封鎖該 port。可以設定觸發封鎖的頻率。

● 通知項目

當有觸發防護設定的事件發生時，在第一時間通知管理者處理。
可勾選的項目：連動異常 IP 阻擋、連動 IPS Port 阻擋、Arp 防護、IP 衝突、MAC 衝突。

7-3-2、ARP 紀錄

ARP 的攻擊的偵測紀錄，記錄時間、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。

圖 141. 圖7-24 ARP 攻防紀錄¶

【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。

【介面】：選擇要搜尋的內部網路介面 (ZONE)。

【事件】：搜尋全部 / 超出警戒值 / 受害者 的事件。（超出警界值：疑似為攻擊者）

【狀態】：ARP 攻擊進行中或是已經停止。

7-3-3、MAC 衝突紀錄

偽造 MAC 位址的攻防偵測紀錄，搭配協同防禦交換器，連同接入的位置都會顯示出來。

Mac 衝突列表 | 清除 | 立即更新 | 重新紀錄位址 | 1 / 2 跳至 1 頁數 每頁 16 筆 GO | 匯出 | 匯出全部

時間	Mac 位址	IP 位址	介面	接入位置	狀態	動作
2021-09-16 18:00:05	00:0d:48:26:f3:a4	192.168.1.99	zone0			
2021-09-16 18:00:05	00:0d:48:26:f3:a4	192.168.1.30	zone0		偵測到相似mac	
2021-09-16 16:20:03	00:0d:48:26:f3:a4	192.168.1.99	zone0			
2021-09-16 16:20:03	00:0d:48:26:f3:a4	192.168.1.30	zone0		偵測到相似mac	

圖 142. 圖7-25 MAC 攻防紀錄¶

【MAC 位址】：衝突的 MAC 位址。

【IP 位址】：顯示目前衝突的 IP 位址。

【接入位置】：疑似攻擊者或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 MAC 的說明。

【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。

7-3-4、IP 衝突紀錄

偽造 IP 位址的攻防偵測紀錄，搭配協同防禦交換器，連同接入的位置都會顯示出來。

IP 衝突列表 | 清除 | 1 / 1 跳至 1 頁數 每頁 16 筆 GO | 匯出 | 匯出全部

時間	Mac 位址	IP 位址	介面	接入位置	狀態	動作
2021-09-16 16:43:00	00:90:cc:de:94:2b	192.168.1.30	zone0		偵測到相似IP	
2021-09-16 16:27:20	00:0d:48:26:f3:a4	192.168.1.30	zone0		偵測到相似IP	
2021-09-16 16:19:12	00:90:cc:de:94:2b	192.168.1.30	zone0		偵測到相似IP	
2021-09-16 16:07:01	00:0d:48:26:f3:a4	192.168.1.30	zone0		偵測到相似IP	

圖 143. 圖7-26 IP 攻防紀錄¶

【MAC 位址】：顯示目前衝突的 MAC 位址。

【IP 位址】：衝突的 IP 位址。

【接入位置】：疑似攻擊者或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。

7-3-5、封鎖狀態

INF 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

INF 具備的 IPS (Intrusion Prevention System) 入侵防禦功能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。

● 為何需要 IPS ?

攻擊手法例如：SQL Slammer 是採用「緩衝溢位」(buffer overflow) 的攻擊，
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。

而狀態檢測（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，
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）。

● IPS 的運作

IPS 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，一旦發現後能夠即時地阻止封包，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，
但是越多的檢查就需要越強的運算能力，否則反而會導致網路速度緩慢。

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，
在中小型網路架構的 IPS 設備只需要有完整的危險程度高、中（病毒、木馬程式等）的特徵值資料庫就足夠了。

要讓 IPS 正常運作，步驟如下：

1. 在【IPS 設定】中，建立一個群組，在群組中指定要阻擋還是記錄有問題的特徵值。

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。

IPS 的特徵值眾多，管理者套用不同的特徵值時，有可能誤將正常的網路封包阻擋，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，INF 將所有的 IPS 事件分成高、中、低 3 種風險事件，把管制行為分成阻擋跟記錄，
管理者可以先啟用記錄功能，然後再根據實際的需要設定阻擋機制。

Tip

影片參考｜眾至NU系列 UTM教學 IPS說明與設定

8-1、IPS 設定

新增完成的 IPS 過濾設定會依群組名稱、模式、內容顯示於列表之中。
點選 ✚ 新增 ，可新增 IPS：

【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】：初階或進階模式，初階是按照特徵值的風險性，進階則是按照特徵值的類型。

· 初階模式

按照風險程度分高、中、低等級，括號內數字表示這個等級的特徵值數量，點選 ⊞ 可以觀看詳細的特徵值名稱。
可選擇每一個等級要執行的動作（記錄 / 阻擋）。

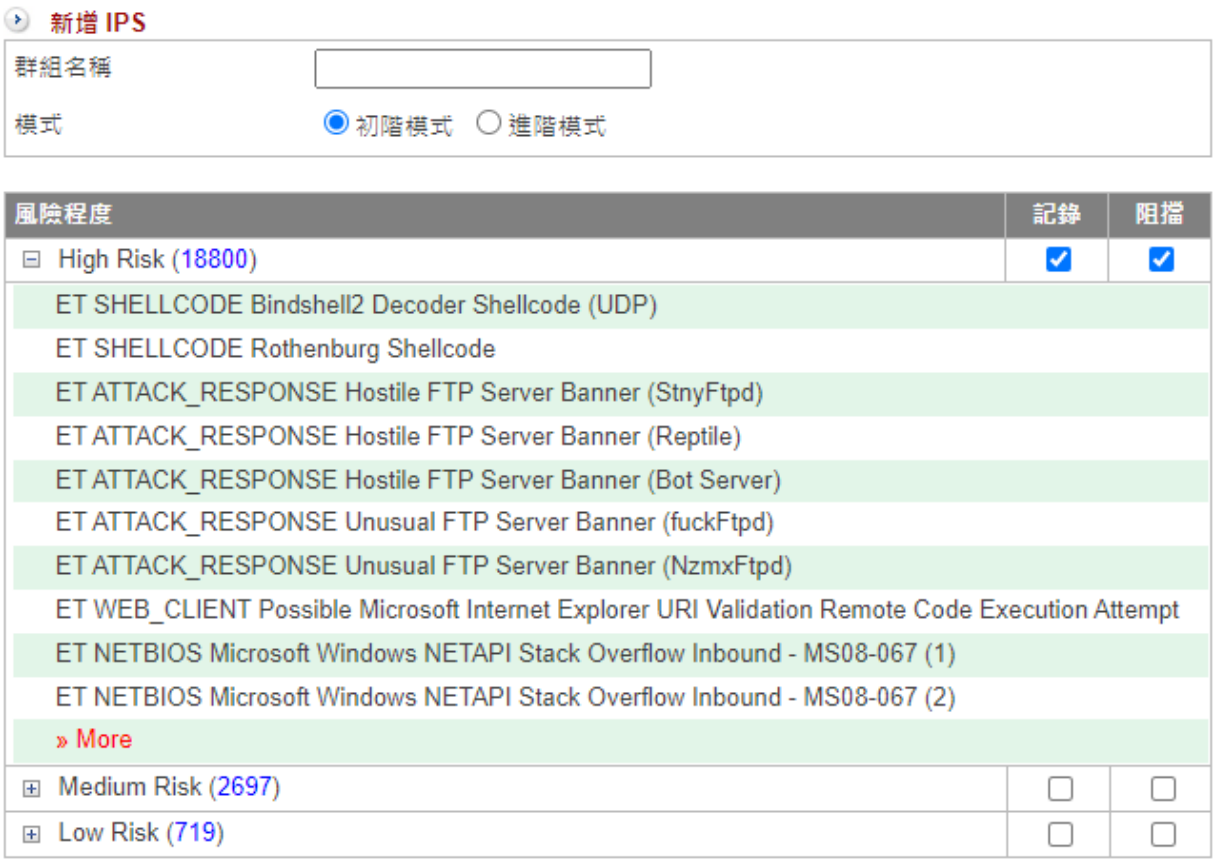


圖 144. 圖8-1 IPS 初階模式¶

· 進階模式

先選擇 IPS 特徵值分類，再根據所選的分類選擇它的風險程度是高、中、低等級。

圖 145. 圖8-2 IPS 進階模式¶

按下確定後，會依所選的分類展開該分類底下的詳細特徵值名稱，可以直接勾選整個分類也可以個別勾選要執行的動作（記錄 / 阻擋）。

8-2、IPS 記錄

每個 IPS 的阻擋事件都會被記錄下來，讓管理者可以查詢，
今日 IPS 防護紀錄 會列出從凌晨 00:00 到進入此介面當下的紀錄，管理者另可在 **IPS 紀錄搜尋** 依條件查詢 IPS 防護紀錄。

每一筆紀錄包含事件發生的時間、IPS 種類、特徵值名稱、來源 / 目的 IP 位址、協定、來源 / 目的 Port、INF 執行的動作跟分類的風險程度。

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 146. 圖8-3 IPS 阻擋及記錄¶

第9章 內容記錄

9-1、WEB 記錄

INF 可記錄 Web 的通聯紀錄，不論是 http 或是 https 協定，連掃毒過程都會被詳細地記錄下來。

9-1-1、今日 WEB 記錄

INF 會自動將通過設備的 WEB 上網紀錄（包含時間、網址等）記錄下來。

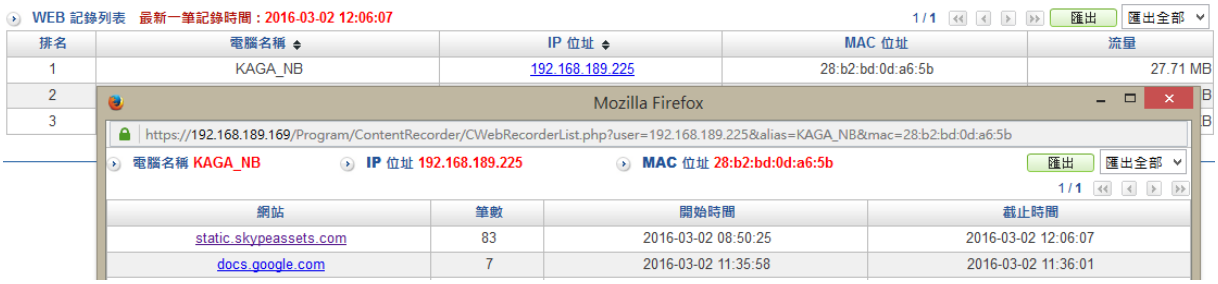


圖 146. 圖11-1 瀏覽網站列表¶

【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】：被記錄電腦的 IP 位址。

【MAC 位址】：被記錄電腦的 MAC 位址。

【上網認證帳號】：若管制條例內同時開啟 WEB 紀錄和上網認證功能，這裡會顯示此 IP 上網時認證的帳號。

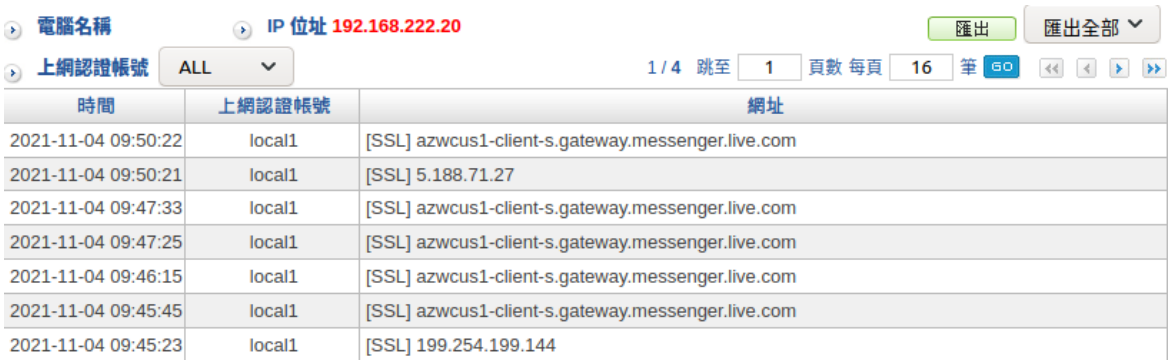
【流量】：http 協定的流量。

【匯出】：把 http 協定的資料匯出。

➤點選【IP 位址】連結後，會出現該 IP 位址更完整的上網紀錄，以「筆數」為排序依據，記錄各網站開始瀏覽時間及離開時間。

【網站】：瀏覽的網站名稱。

點選【網站】的連結後會出現這個網站被記錄幾個有效的網址列表（如下圖）。


電腦名稱　IP 位址 192.168.222.20　匯出　匯出全部

上網認證帳號 ALL　1 / 4　跳至 1　頁數 每頁 16 筆 GO

時間	上網認證帳號	網址
2021-11-04 09:50:22	local1	[SSL] azwcus1-client-s.gateway.messenger.live.com
2021-11-04 09:50:21	local1	[SSL] 5.188.71.27
2021-11-04 09:47:33	local1	[SSL] azwcus1-client-s.gateway.messenger.live.com
2021-11-04 09:47:25	local1	[SSL] azwcus1-client-s.gateway.messenger.live.com
2021-11-04 09:46:15	local1	[SSL] azwcus1-client-s.gateway.messenger.live.com
2021-11-04 09:45:45	local1	[SSL] azwcus1-client-s.gateway.messenger.live.com
2021-11-04 09:45:23	local1	[SSL] 199.254.199.144

圖 147. 圖11-2 瀏覽網址及詳細資料¶

〖時間〗：點選這個網址的時間。

〖上網認證帳號〗：此 IP 上網時認證的帳號。

〖網址〗：實際的 URL 的網址。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。

【筆數】：這個網站總共被記錄幾個有效的網址。

【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。

9-1-2、WEB 記錄查詢

可依照日期、電腦名稱、IP 位址等特徵來搜尋儲存在 INF 內所有符合條件之紀錄。

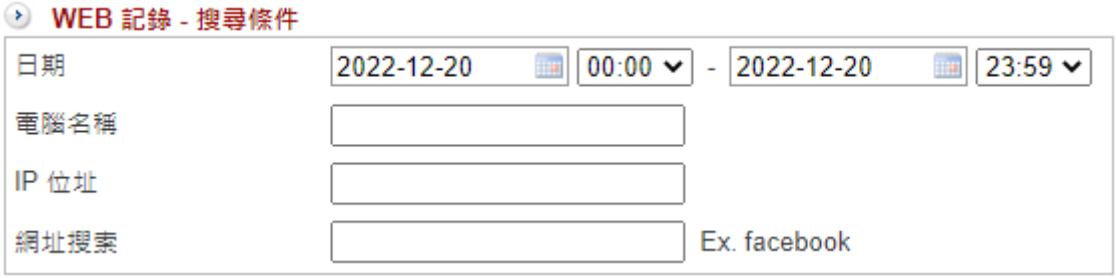


圖 148. 圖11-3 搜尋特定記錄之畫面¶

【日期】：指定時間區間內的紀錄。

【統計方式】：可選擇依 IP 統計或依上網認證統計。

· 依 IP 統計：

【電腦名稱】：以電腦名稱選定使用者。

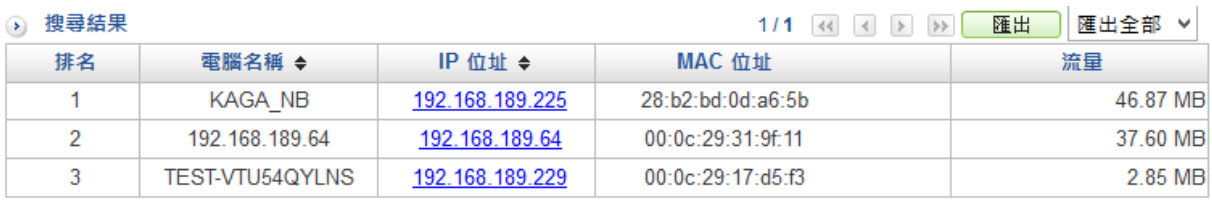
【IP 位址】：以 IP 位址選定使用者。

· 依上網認證統計：

【上網認證帳號】：系統會列出所有帳號，可選擇全部或特定帳號。

【網址搜索】：搜尋特定網址。

按下搜尋後會列出所有 WEB 紀錄查詢的結果。如同在今日 WEB 記錄列表的操作，可點選 IP 位址連結查看詳細資訊。

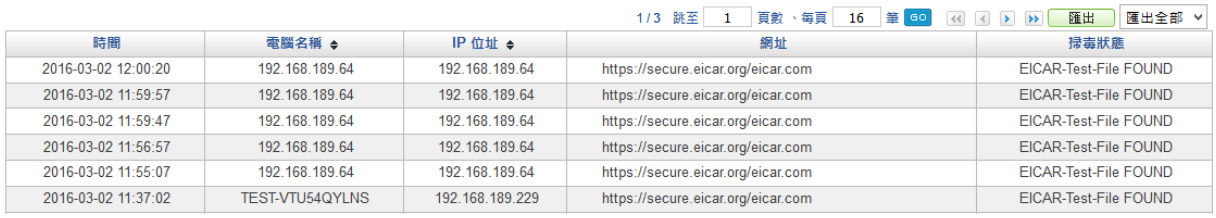


排名	電腦名稱	IP 位址	MAC 位址	流量
1	KAGA_NB	192.168.189.225	28:b2:bd:0d:a6:5b	46.87 MB
2	192.168.189.64	192.168.189.64	00:0c:29:31:9f:11	37.60 MB
3	TEST-VTU54QYLNS	192.168.189.229	00:0c:29:17:d5:f3	2.85 MB

圖 149. 圖11-4 搜尋結果列表¶

9-1-3、WEB 病毒記錄及查詢

INF 具有掃描 http/https 是否含有病毒的能力，搭配內建的 ClamAV 或是選購的 Kaspersky 掃毒引擎，
把有問題或是藏有病毒的網頁都過濾掉，這裡會列表顯示被 INF 找到的病毒紀錄。



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 150. 圖11-5 病毒紀錄列表¶

第10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 INF 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。

10-1、連線測試

10-1-1、PING

一般碰到網路不通的情況，大多會先使用 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，藉以判斷線路是否正常。

● **Ping 偵測設定：**

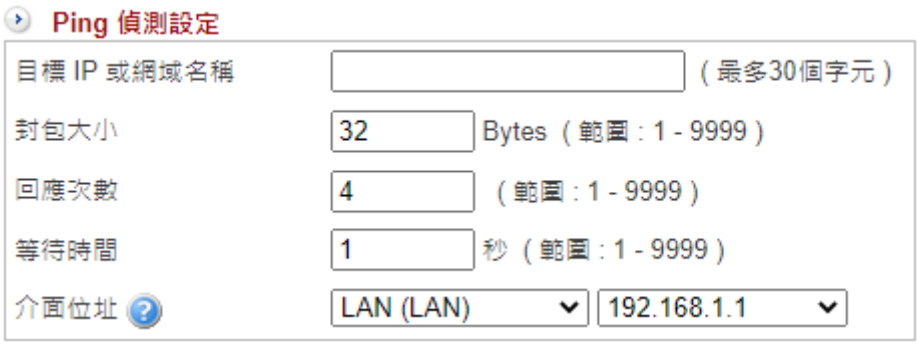


圖 151. 圖13-1 PING 測試工具及輸出資訊¶

【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 1~9999。

【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。

【等待時間】：ICMP 等待回應的間隔時間，超過此設定時間就會視為斷線，預設是 1 秒，設定範圍是 1~9999。

【介面位址】：選擇要送出這個測試封包的介面跟帶出去的 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。

10-1-2、Trace route

Trace route 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。當網路不通時，除了用 PING 檢查以外，
若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，就會使用 Traceroute 這一個工具，目前只支援 IPV4 位址。

● **Traceroute 偵測設定：**

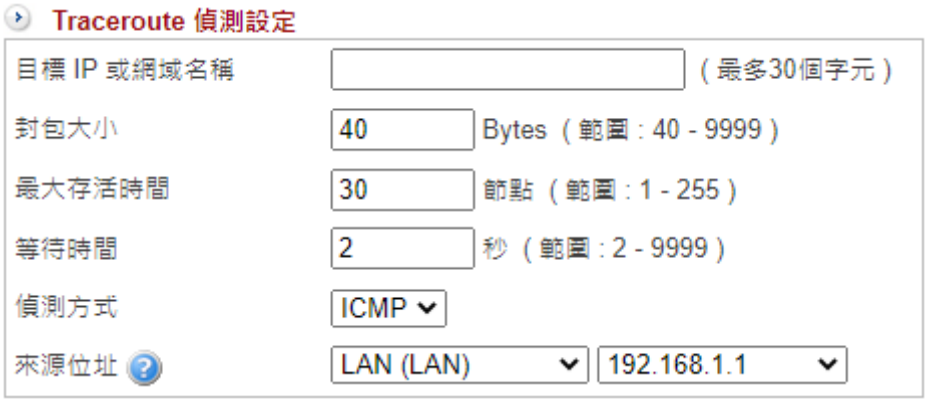


圖 152. 圖13-2 Tracer route測試工具及輸出資訊¶

【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 ~9999。

【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】：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。

【偵測方式】：用哪一個通訊協定送出偵測封包，可以選擇 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帶出去的 IP 位址。

10-1-3、DNS Query

查詢 DNS 的詳細資料，可以依 DNS 的 ANY、SOA、NS、A、AAAA、MX、CNAME、PTR 等類型查詢，
管理者可以使用本機或是特定的 DNS 伺服器作為查詢依據。

● **DNS 查詢工具設定：**

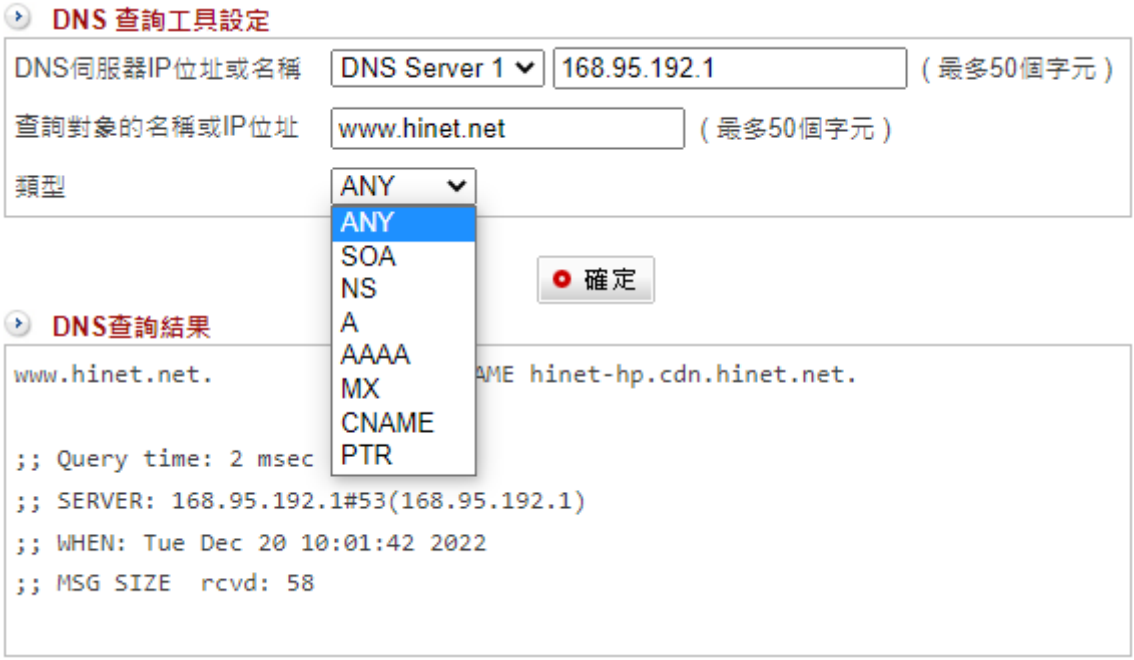


圖 153. 圖13-3 DNS 測試工具及輸出資訊¶

【DNS 伺服器 IP 位址或名稱】：可以選用 INF 使用的 DNS 伺服器或是自行輸入其他的 DNS 伺服器。

【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，例如：168.95.1.1 或是 www.hinet.net。
輸入網域名稱是選擇正查，輸入 IP 位址則是屬於反查。

【類型】：查詢 DNS 的 ANY、SOA、NS、A、AAAA、MX、CNAME、PTR 等資料。

10-1-4、Port Scan

利用 INF 去掃描遠端電腦是否開放常用 PORT。

圖 154. 圖13-4 DNS 測試工具及輸出資訊¶

【輸入 IP 位址或域名】：輸入查詢的主機 IP 位址或是域名。

【掃描服務】：選擇欲掃描的是預設或自訂 Port。

【來源位址】：查詢時使用的 Zone 跟 IP 位址。

【查詢結果】：有開放的 Port 會顯示為 OK ，沒開放則顯示 FAIL 。

10-1-5、 IP Route

顯示整個 INF 的路由表，讓管理者參考。

10-1-6、Interface Information

INF 可以顯示每個 Zone 內綁定的位址區段、使用者 IP 及 MAC 位址。

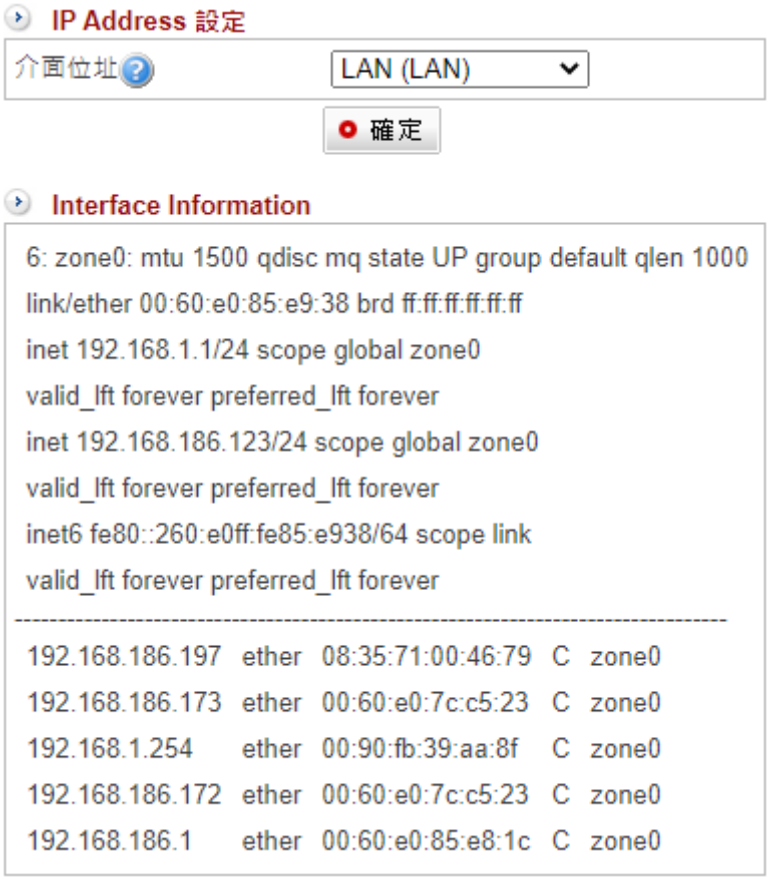


圖 155. 圖13-5 介面資訊¶

10-1-7、Wake Up

INF 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。

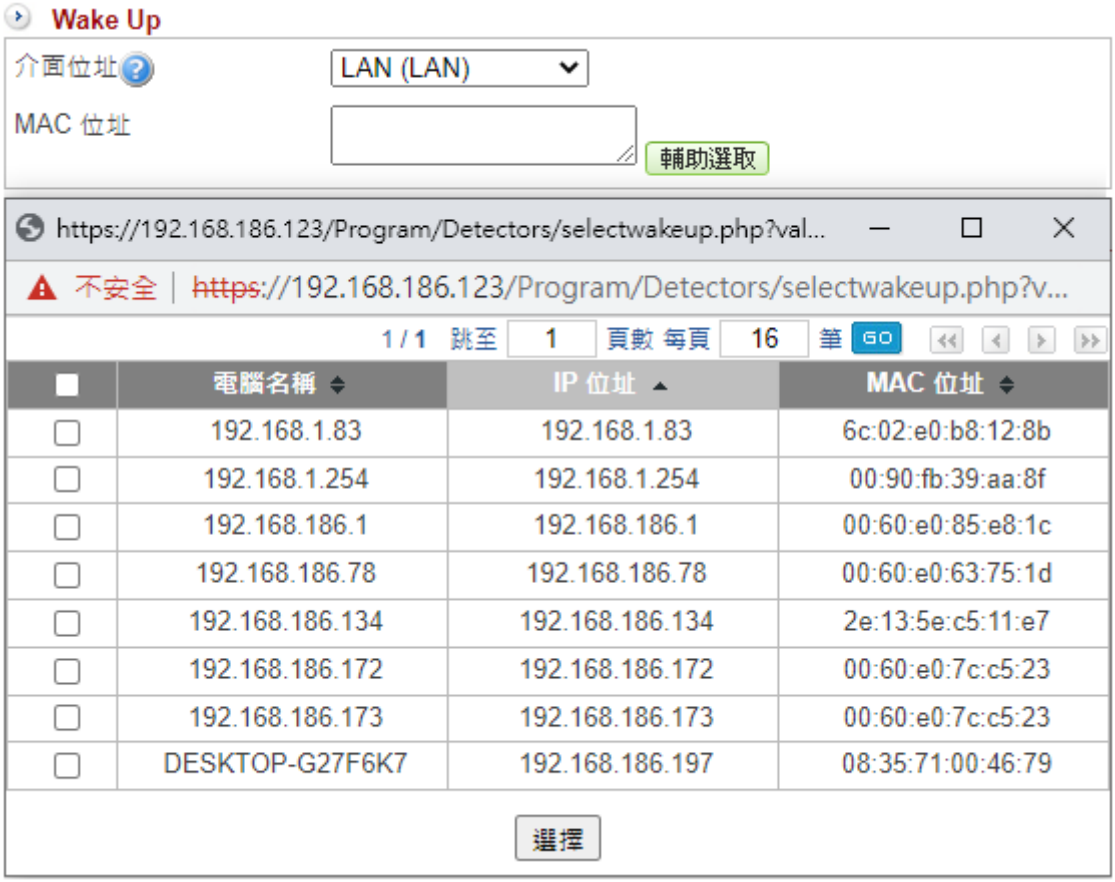


圖 156. 圖13-6 Wake Up 設定¶

【介面位址】：要執行 Wake Up 的電腦屬於哪一個介面。

【MAC 位址】：要執行 Wake Up 電腦的 MAC 位址，可以進入 輔助選取 勾選。

10-1-8、SNMP

INF 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。

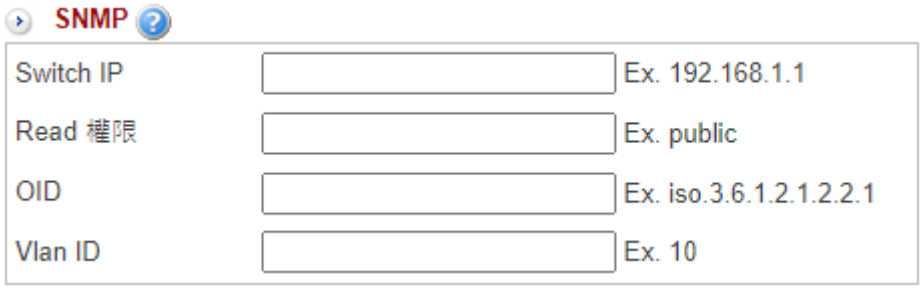


圖 157. 圖13-7 SNMP 查詢交換器資訊¶

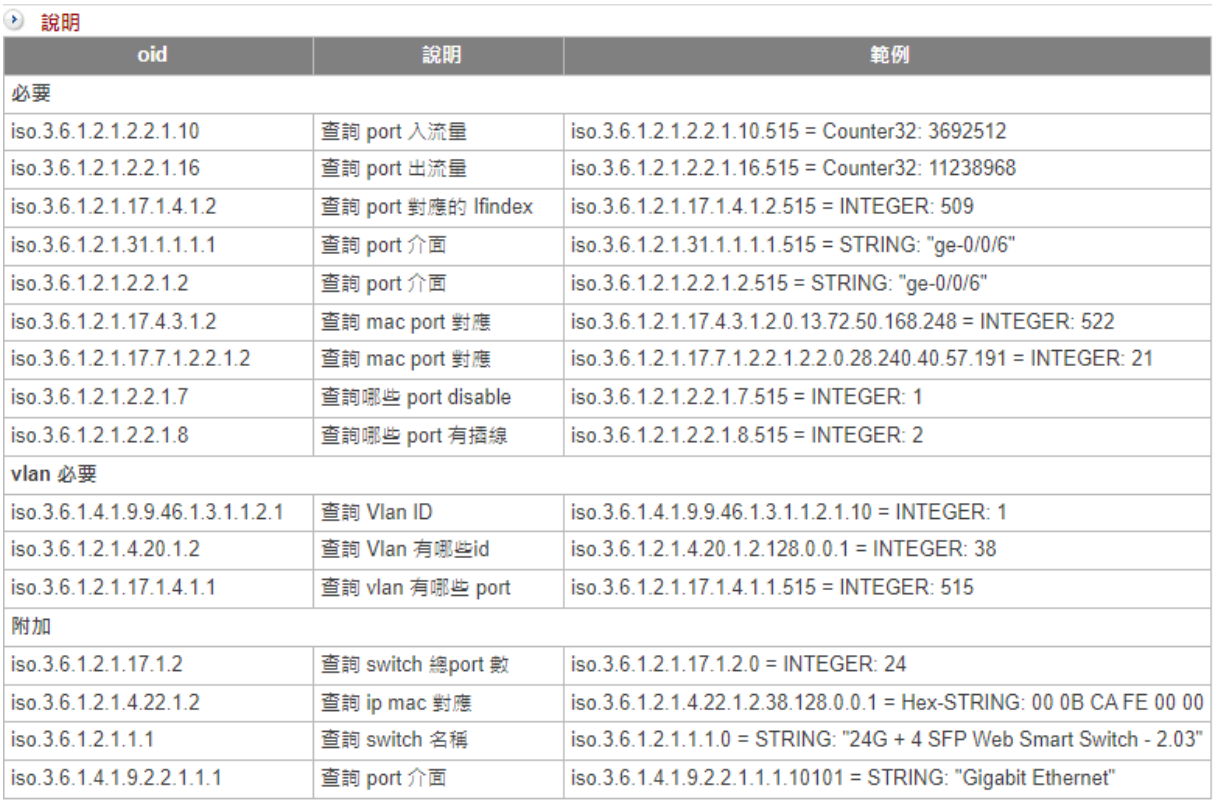
【Switch IP】：要向哪一個交換器查詢，填入交換器的 IP 位址。

【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 識別代碼的方式去查詢。

【Vlan ID】：Switch 是隸屬於哪一個 Vlan 。

點選 可查看 OID 說明：



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 158. 圖13-8 可查詢 OID¶

10-2、封包擷取

INF 提供自動定時抓封包的工具，把封包記錄下來之後，管理者可到「已完成列表」頁籤中查看、下載。
方便管理者在找網路問題時，針對封包進行分析。

10-2-1、排程中列表

在排程中列表下方點選 ✚ 新增 即可新增排程：

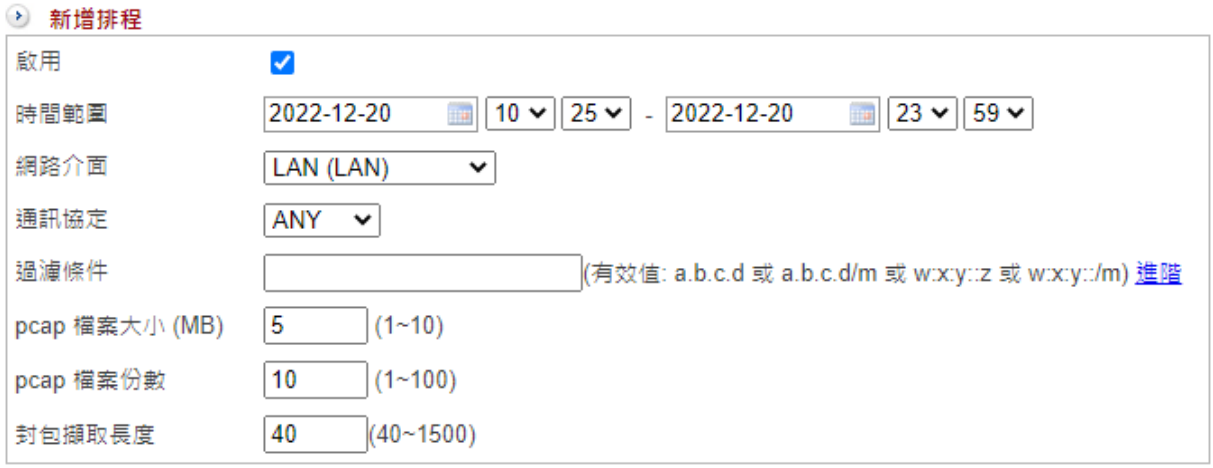


圖 159. 圖13-9 封包擷取設定¶

【啟用】：是否啟用抓取封包功能。

【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】：全部抓取還是指定 TCP、UDP、ICMP、ARP 類型的封包。

【過濾條件】：2 種模式，簡易版填入 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)】：每一個記錄下來的檔案大小，設定範圍是 1-10 MB。

【pcap 檔案份數】：總共記錄幾份，設定範圍是 1-100 份，要注意儲存空間。
以最大值計算，10MB*100=1000MB=1G，系統必須有 1G 的空間可以儲存，如果設定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。

10-2-2、已完成列表

成功抓取的網路封包會顯示於此列表，點選 記錄 按鈕，就可以進入查看詳細資訊並將這個檔案下載到操作者的電腦端。

圖 160. 圖13-10 封包擷取列表¶

第11章 日誌

INF 會詳實地把每位管理者登入系統後所執行的任何項目（包含登入失敗的事件）都記錄下來，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。

11-1、操作日誌

11-1-1、日誌

任何權限的管理者（View、Read、Write、View-Read-Write）在 INF 的所有操作都會被詳細地記錄。
包含發生的時間、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 12 個月。
點選欄位項目的 ⬍ 可以更改排序方式。


日誌列表 1 / 10 跳至 1 頁數 每頁 16 筆 GO 匯出 匯出全部

時間	帳號	IP 位址	管理 IP	功能路徑	動作	內容
2022-12-20 09:15:17	admin	192.168.190.161	192.168.186.123	允許登入	登入	Login Successful
2022-12-19 12:03:58	admin	192.168.186.173	192.168.186.123	管制條例 > 管制規則 > 管制規則	新增	管制條例名稱
2022-12-19 12:03:45	admin	192.168.186.173	192.168.186.123	管制條例 > 管制規則 > 管制規則	修改	管制條例名稱
2022-12-19 12:03:37	admin	192.168.186.173	192.168.186.123	管制條例 > 管制規則 > 管制規則	新增	管制條例名稱
2022-12-19 12:03:03	admin	192.168.186.173	192.168.186.123	管制條例 > 管制規則 > 管制規則	刪除	管制條例名稱
2022-12-19 12:03:01	admin	192.168.186.173	192.168.186.123	管制條例 > 管制規則 > 管制規則	刪除	管制條例名稱
2022-12-19 09:56:08	admin	192.168.186.173	192.168.186.123	管制條例 > 管制規則 > 管制規則	修改	管制條例名稱

圖 161. 圖14-1 日誌列表¶

【時間】：該事件發生的時間。

【帳號】：執行動作的管理者帳號。

【IP 位址】：管理者帳號使用的 IP 位址。

【管理 IP】：此帳號由哪個防火牆的 IP 位址登入介面。

【功能路徑】：管理者進入的管理介面路徑。

【動作】：管理者執行的動作，登入、新增、修改、刪除、搜尋、下載等。

【內容】：執行動作前後的詳細內容，INF 會列出修改前跟修改後的差異項目。

11-1-2、日誌搜尋

可依照特定 IP 位址或相關事件特徵，搜尋儲存在 INF 內所有符合條件之紀錄。

圖 162. 圖14-2 事件搜尋¶

【帳號】：系統會列出所有管理者帳號，可選擇全部或特定帳號。

【IP 位址】：管理者帳號的 IP 位址。

【管理 IP】：防火牆的 IP 位址。

【時間】：選擇要查詢的時間範圍。

【事件】：全選或勾選要查詢的事件紀錄。

第12章 系統狀態

使用者可隨時由系統狀態查看 INF 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，也有歷史資訊提供給管理者查詢。

系統狀態有 4 個主項目：

1、系統狀態： 顯示目前 INF CPU 負載、記憶體負載、系統負載，也可以查詢每個介面的 TX/RX 流量。

2、連線狀態： 記錄 INF 之連線使用情況，包含上線數量、封包的紀錄等。

3、流量分析： 根據 PORT、應用程式或是 DNS 的使用量統計查詢。

4、Dashboard： 也就是威脅情報儀表，以圖形的方式顯示各項統計資訊。於 第16章 Dashboard 詳細說明。

12-1、系統狀態

12-1-1、系統狀態

顯示從現在到過去 24 小時的統計資料，有【**CPU 負載圖**】、【**記憶體負載圖**】、【**系統負載圖**】。

【**CPU 負載圖**】：顯示 INF 過去 24 小時 CPU 目前使用狀況。點選【顯示更多】會列出每個 CPU 的統計圖。

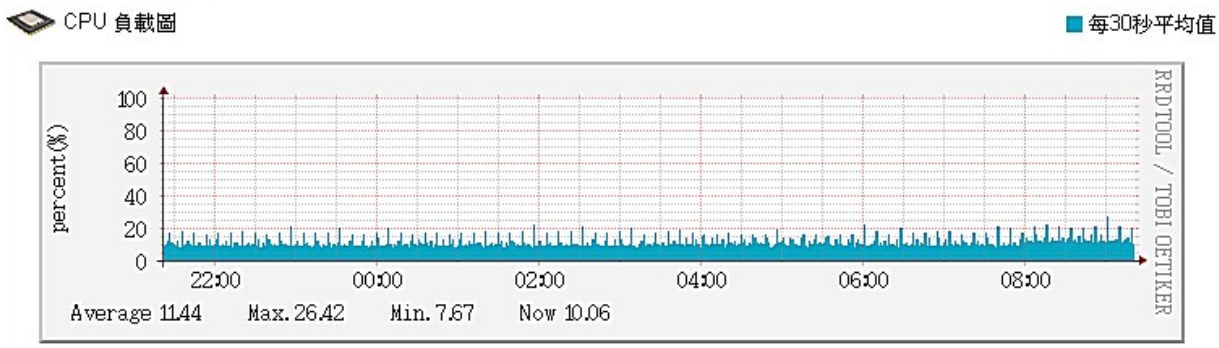


圖 163. 圖15-1 CPU 負載¶

【**記憶體負載圖**】：顯示 INF 過去 24 小時記憶體使用狀況。

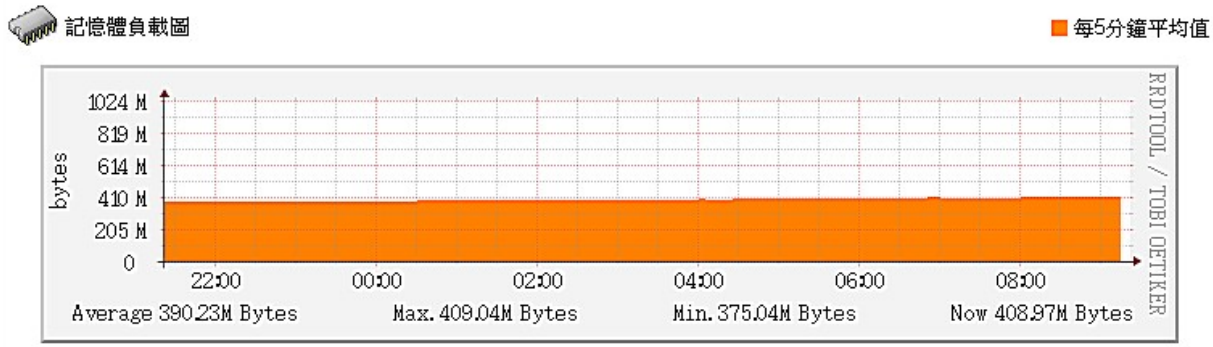


圖 164. 圖15-2 記憶體負載¶

【**系統負載圖**】：顯示 INF 系統過去 24 小時的系統負載。

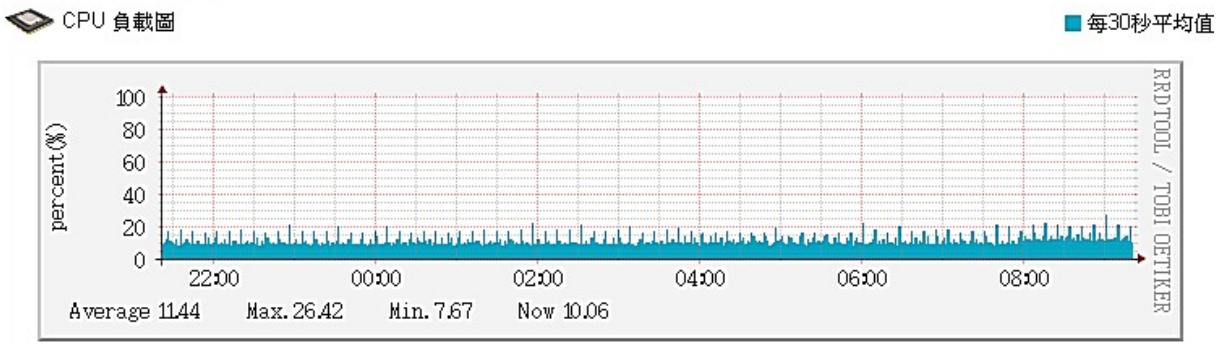


圖 165. 圖15-3 系統負載¶

12-1-2、網路流量

顯示目前 INF 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。
顯示藍色為 Zone Out (TX) 流量，就是從介面出去的流量 ； 綠色則是 Zone In (RX) 流量，表示進入介面的流量 。

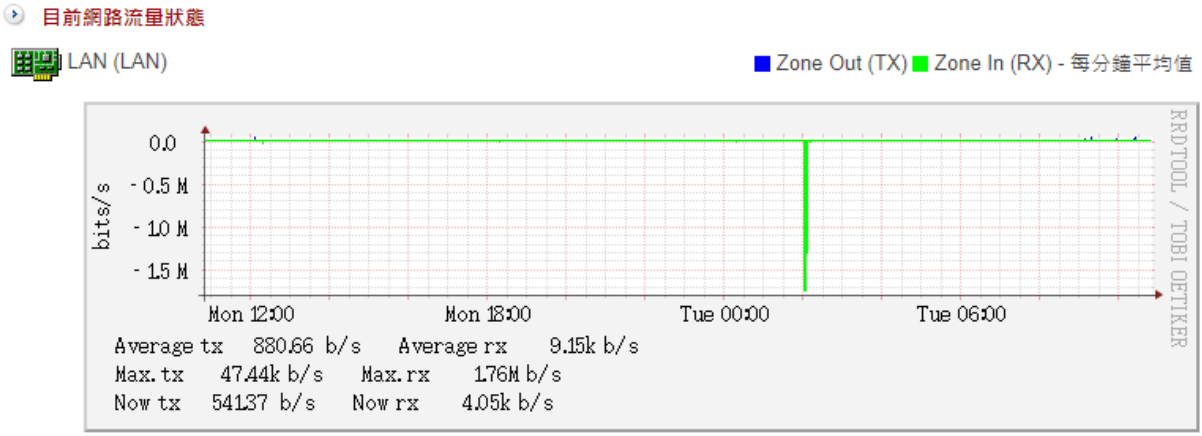


圖 166. 圖15-4 網路介面流量¶

> **Note**
>
> 對於 WAN 類型的介面，它的統計流量方向跟線路提供商的上下載是不同的方向。

12-1-3、連線狀態

INF 提供過去 48 小時上線人數跟總連線數圖表，讓管理者快速地掌握過去一段時間內的狀態，在「歷史狀態」頁籤中可以搜尋更長時間的狀態變化。

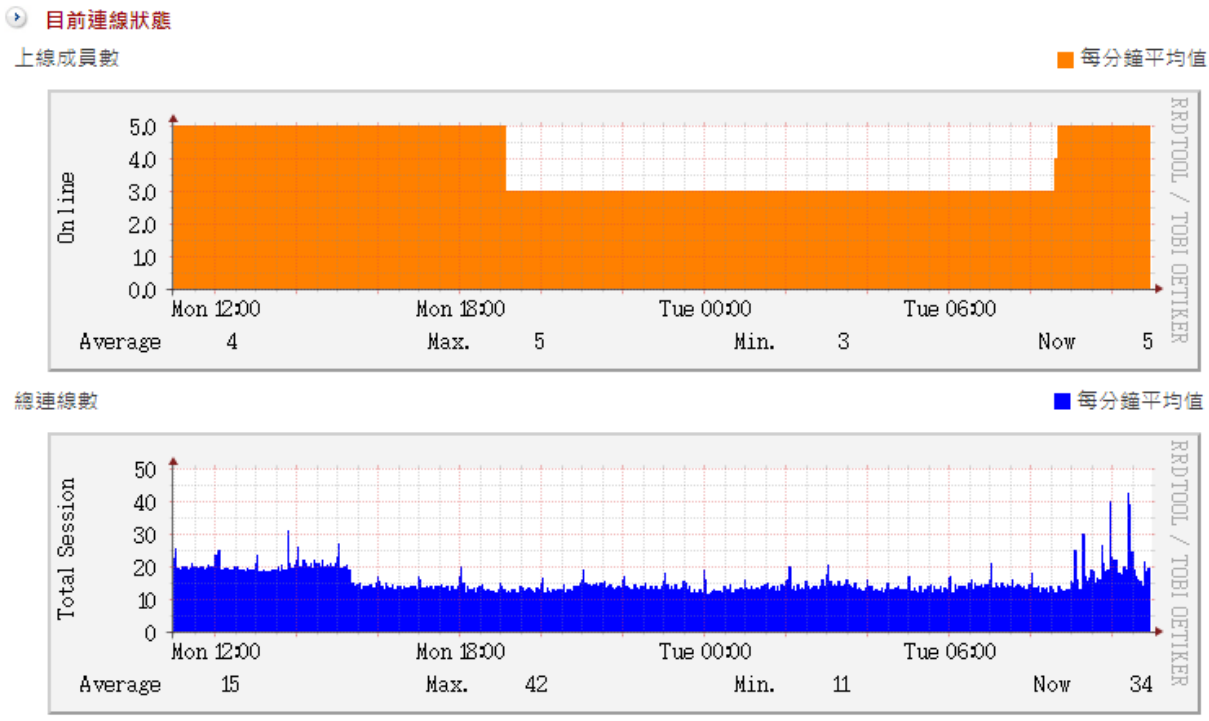


圖 167. 圖15-5 過去 48 小時的連線紀錄¶

12-1-4、歷史狀態

管理者選擇查詢目標及時間區間後，INF 會自動顯示這一段時間的各項統計圖表。
這個功能可以讓管理者從中分析過去一段時間是否有出現問題，並從問題中找出可能的解決方式。

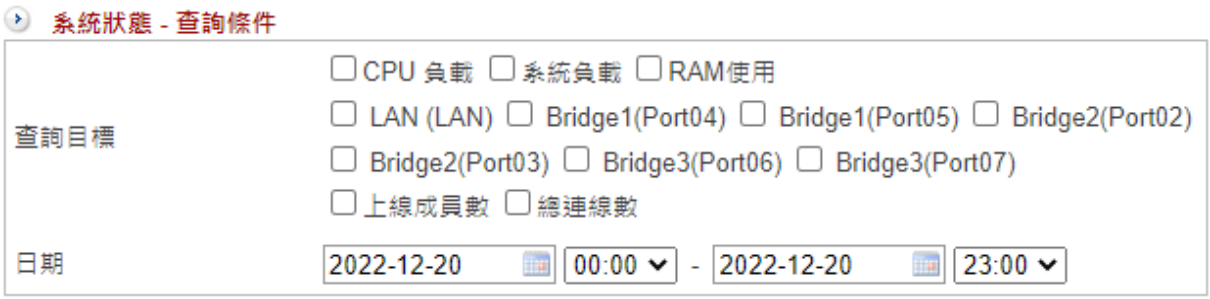


圖 168. 圖15-6 歷史資料搜尋¶

【查詢目標】：選擇要查詢的目標，目前可以選擇 CPU、RAM、系統負載、介面流量（系統會列出所有網路介面讓管理者勾選）、上線成員數跟總連線數。

【日期】：選擇欲搜尋的日期與時間，例如：2015-04-05 00:00 ~ 2016-04-05 23:00 代表要查詢一年的歷史狀態。

12-1-5、介面即時流量

有別於「網路流量」是統計過去 24 小時的流量，這裡顯示的介面即時流量是近 3 分鐘的資料。
不僅可以看實體介面，也可以查看虛擬介面的即時流量，例如：IP Tunnel、PPPOE，最多可以同時看 2 個介面。

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。
顯示藍色為 Zone Out (TX) 流量，就是從介面出去的流量 ； 綠色則是 Zone In (RX) 流量，表示進入介面的流量 。

圖 169. 圖15-7 即時流量¶

> **Note**
>
> 對於 WAN 類型的介面，它的統計流量方向跟線路提供商的上下載是不同的方向。

12-1-6、CPU 負載

管理者可以藉由這項功能得知每一個 CPU 的即時負載情況。
例如：若發現系統資源有吃單顆 CPU 的狀況發生，可以從「網路設定 > 3-7、中斷設定」將它的網路流量分配到其他 CPU 中。

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	99.75%	0.00%	0.25%	0.00%	0.00%	0.00%	0.00%	0.25%
cpu0	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
cpu1	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
cpu2	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
cpu3	99.00%	0.00%	0.00%	1.00%	0.00%	0.00%	0.00%	1.00%

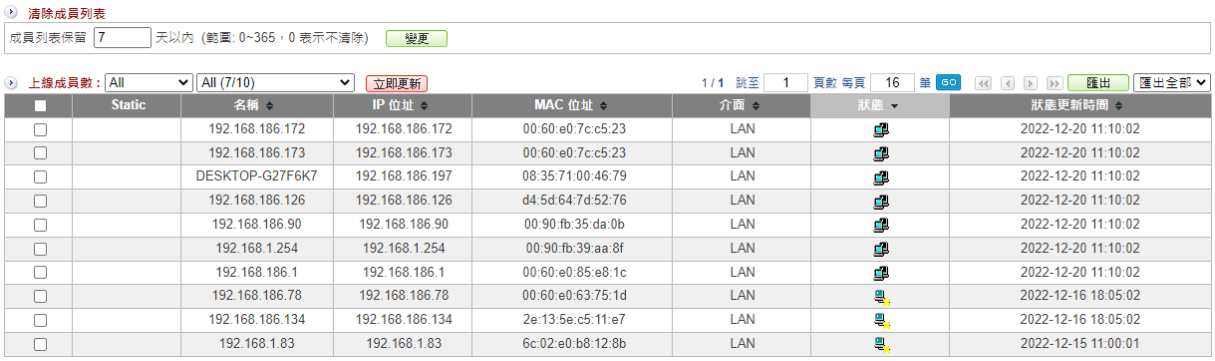
圖 170. 圖15-8 CPU 即時統計¶

12-2、連線狀態

連線狀態會記錄成員列表、無線成員列表及連線追蹤，有經驗的管理者可以藉此判斷某部電腦是否有問題。
成員列表會記錄 7 天內（預設值）經過 INF 所有介面下的 IP 位址資訊；
連線追蹤則是詳細記錄每一個來源 IP 位址的連線數量統計跟實際使用的封包通聯紀錄。

12-2-1、成員列表

顯示通過 INF 介面下的所有 IP 資訊。如果是內部網路，還可以判斷是否為開機狀態、從哪個網路介面連線。點選 ⬍ 可改變排序方向。


清除成員列表

成員列表保留 7 天以內 (範圍: 0~365，0 表示不清除) 變更

上線成員數： All All (7/10) 立即更新 1 / 1 跳至 1 頁數 每頁 16 筆 GO 匯出 匯出全部

	Static	名稱	IP 位址	MAC 位址	介面	狀態	狀態更新時間
☐		192.168.186.172	192.168.186.172	00:60:e0:7c:c5:23	LAN		2022-12-20 11:10:02
☐		192.168.186.173	192.168.186.173	00:60:e0:7c:c5:23	LAN		2022-12-20 11:10:02
☐		DESKTOP-G27F6K7	192.168.186.197	08:35:71:00:46:79	LAN		2022-12-20 11:10:02
☐		192.168.186.126	192.168.186.126	d4:5d:64:7d:52:76	LAN		2022-12-20 11:10:02
☐		192.168.186.90	192.168.186.90	00:90:fb:35:da:0b	LAN		2022-12-20 11:10:02
☐		192.168.1.254	192.168.1.254	00:90:fb:39:aa:8f	LAN		2022-12-20 11:10:02
☐		192.168.186.1	192.168.186.1	00:60:e0:85:e8:1c	LAN		2022-12-20 11:10:02
☐		192.168.186.78	192.168.186.78	00:60:e0:63:75:1d	LAN		2022-12-16 18:05:02
☐		192.168.186.134	192.168.186.134	2e:13:5e:c5:11:e7	LAN		2022-12-16 18:05:02
☐		192.168.1.83	192.168.1.83	6c:02:e0:b8:12:8b	LAN		2022-12-15 11:00:01

圖 171. 圖15-9 成員列表¶

【成員列表保留】：通過 INF 的 IP 位址要保留幾天，預設值為 7 天，設定範圍是 0~365，0 代表不清除這些紀錄資料。

【上線成員數】：第一個選單顯示該介面偵測到的 IP，第二個選單根據不同網段再分類。也可以選擇 All 顯示全部。
括號內數字顯示為這個網段內（上線成員數/共有幾位成員），
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 INF 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。

【Static】：在 5-1、位址表 中，將此 IP 與 MAC 位址綁定，此欄位就會顯示為 ✅，表示此裝置是固定的。

【名稱】：該部電腦的 NETBIOS 名稱，可以在管理目標的 5-1、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。

12-2-2、無線成員列表

透過 AP 上網的使用者會被列表在這裡（在「系統設定 > 2-8、AP 管理 」加入 UTM 管理的設備），
除了可以得知 SSID 外，還可以判斷是否為開機狀態、從哪個 AP 連線。點選 ⇕ 可改變排序方向。

【成員列表保留】：通過 INF 的 IP 位址要保留幾天，預設值為 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。

【AP 名稱】：此 AP 的名稱。

【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。

12-2-3、連線追蹤

藉由網路封包的分析及追蹤，分析每一個使用者的網路使用行為。
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、TX 流量、RX 流量、詳細紀錄。

● 查詢條件

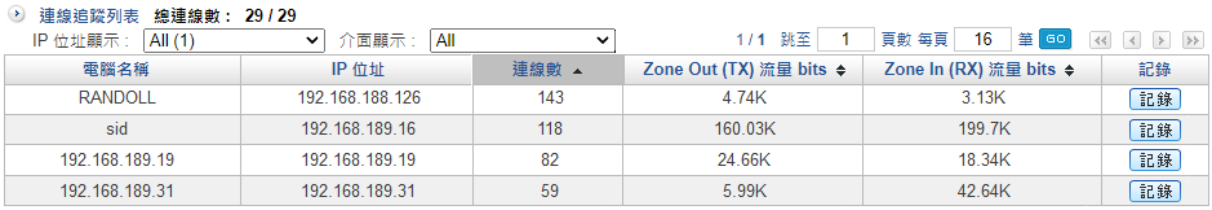
【顯示】：可依照來源 IP 或目的 IP 來顯示表格，也就是連線追蹤列表內顯示的 IP 為來源或目的端。

【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。

【更新頻率】：設定每隔幾秒會更新此頁面。

● 連線追蹤列表


連線追蹤列表 總連線數： 29 / 29
IP 位址顯示： All (1) 介面顯示： All 1 / 1 跳至 1 頁數 每頁 16 筆 GO

電腦名稱	IP 位址	連線數	Zone Out (TX) 流量 bits	Zone In (RX) 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 172. 圖15-10 連線數及流量列表¶

【總連線數】：顯示當下經過 INF 的連線數 / 全部連線數。
例如：1245/1976，代表所有經過 INF 的總連線數為 1976 條，但在這一個介面的統計總數是 1245 條，其他的連線數是分布在其他介面。

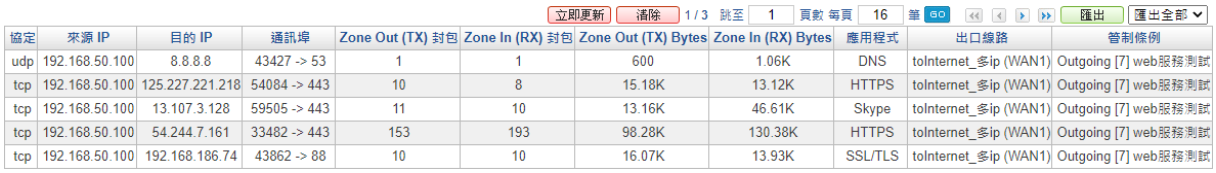
【電腦名稱】：顯示目前該電腦的 NetBIOS 名稱或是位址表中定義的名稱，如果都沒有則顯示 IP 位址。

【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。

【Zone Out (TX)/ Zone In (RX) 流量 bits】：這個 IP 讓防火牆 傳送/接收 的 bit 數量。

在要查看的電腦資料按下 記錄 按鈕後，會出現這部電腦近 3 分鐘的詳細封包通聯訊息，如下圖。



立即更新 清除 1 / 3 跳至 1 頁數 每頁 16 筆 GO 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	管制條例
udp	192.168.50.100	8.8.8.8	43427 -> 53	1	1	600	1.06K	DNS	toInternet_多ip (WAN1)	Outgoing [7] web服務測試
tcp	192.168.50.100	125.227.221.218	54084 -> 443	10	8	15.18K	13.12K	HTTPS	toInternet_多ip (WAN1)	Outgoing [7] web服務測試
tcp	192.168.50.100	13.107.3.128	59505 -> 443	11	10	13.16K	46.61K	Skype	toInternet_多ip (WAN1)	Outgoing [7] web服務測試
tcp	192.168.50.100	54.244.7.161	33482 -> 443	153	193	98.28K	130.38K	HTTPS	toInternet_多ip (WAN1)	Outgoing [7] web服務測試
tcp	192.168.50.100	192.168.186.74	43862 -> 88	10	10	16.07K	13.93K	SSL/TLS	toInternet_多ip (WAN1)	Outgoing [7] web服務測試

圖 173. 圖15-11 使用者連線狀態¶

【立即更新】：按下後可以馬上更新通聯封包的連線數資訊。

【清除】：清除所有的資料，重新顯示通聯封包。

【匯出】：將此資料表匯出。

【協定】：此連線使用何種協定，通常為 TCP 或是 UDP。

【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，而若協定是 UDP，大約可推測是 DNS 協定。

【Zone Out (TX)/Zone In (RX) 封包】：這筆連線讓防火牆 傳送/接收 的封包數。

【Zone Out (TX)/Zone In (RX) Bytes】：這筆連線讓防火牆 傳送/接收 的 byte 數。

【應用程式】：這個連線是使用哪個應用程式，INF 會依據內建的 900 種 DPI 分類這些應用程式。

【出口線路】：這個連線用哪一個出口線路到網際網路。

【管制規則】：這個連線套用的管制規則。

12-3、流量分析

INF 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。

Tip

影片參考｜眾至NU系列 UTM教學 流量分析介紹、流量分析設定

12-3-1、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，點選列表中的資料後可以看到該使用者使用的應用程式等詳細資訊。

圖 174. 圖15-12 流量排行統計條件¶

【預設載入時間範圍】：點選流量排行頁籤後系統會根據此設定的時間範圍顯示統計資料於下方列表，可選擇今天、1 小時、不顯示。
預設是「今天」（從 00:00 ~），選擇「1 小時」表示只統計最近 1 個小時的資料，如果資料多會延遲開啟網頁的時間，
選擇「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，即可馬上切換。

【連線類型】：統計以來源 IP 位址或是目的 IP 位址的連線，切換後按下【搜尋】即會將結果顯示於下方列表。

【統計方式】：使用 IP 位址或是上網認證的帳號為統計基礎，預設為依 IP 統計。

【時間範圍】：統計的時間範圍，可選擇今天或 1 小時。

選擇搜尋條件後所有透過 INF 流量的統計資訊會列表於下方。點選欄位項目的 ⬍ 可改變排序方向。

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 175. 圖15-13 使用者流量排行¶

【電腦名稱】：電腦的 NETBIOS 名稱。

【IP 位址】：電腦的 IP 位址。

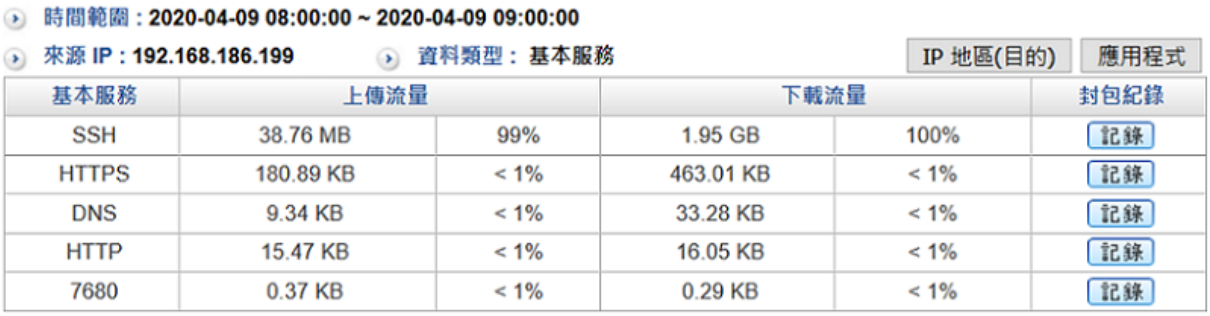
【MAC 位址】：電腦的 MAC 位址。

【上網認證】：這個 IP 位址若有使用上網認證就會顯示帳號，如果沒有就會顯示空白。

【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。

在列表中，點選任一筆電腦或 IP 位址的資料，就可以查看上、下載流量是被哪些應用程式或通訊協定佔用比例等詳細資訊，如下圖。



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 176. 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 種資料類型，基本服務與應用程式分類。
管理者可以用右側的切換按鈕切換，如果這裡出現的是「基本服務」則切換按鈕就會是「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，點選後資料類型就會切換成 IP 目的地區。

點選每筆資料的 記錄 按鈕，INF 顯示這個統計項目更詳細的資訊，如每個時間段的上、下載流量，出口線路跟使用的管制條例。

時間範圍：2021-10-20 00:00:00 ~ 2021-10-20 16:10:05
來源 IP：192.168.50.100　基本服務：HTTPS　返回
1 / 125 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
2021-10-20 16:06:53	67	tcp	192.168.50.100	125.227.221.218	55966->443	2.12 KB	1.84 KB	toInternet_多ip (WAN1)	Outgoing [7] web服務測試
2021-10-20 16:06:27	219	tcp	192.168.50.100	192.229.232.200	50266->443	3.22 KB	9.85 KB	toInternet_多ip (WAN1)	Outgoing [7] web服務測試

圖 177. 圖15-15 詳細的通聯記錄¶

【持續時間】：某個連線的時間長度。

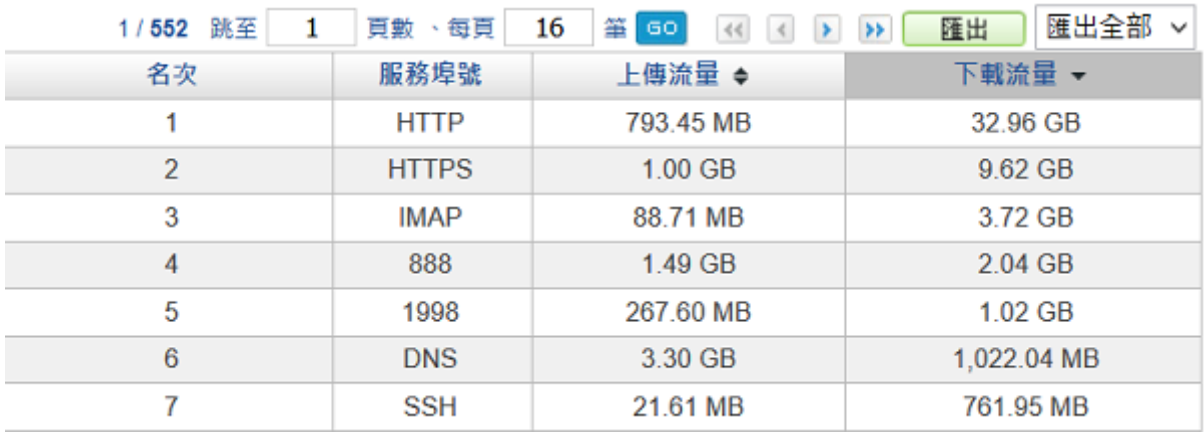
【上傳/下載流量】：某個連線累積的上傳、下載流量。

【出口線路】：使用哪個出口線路。

【管制規則】：使用哪個管制條例。

12-3-2、流量排行 By Port

顯示在統計時間範圍內 INF 的總通訊協議流量排行榜，流量分別可以用上傳、下載流量進行排序。
點選欄位項目的 ⬍ 可改變排序方向。

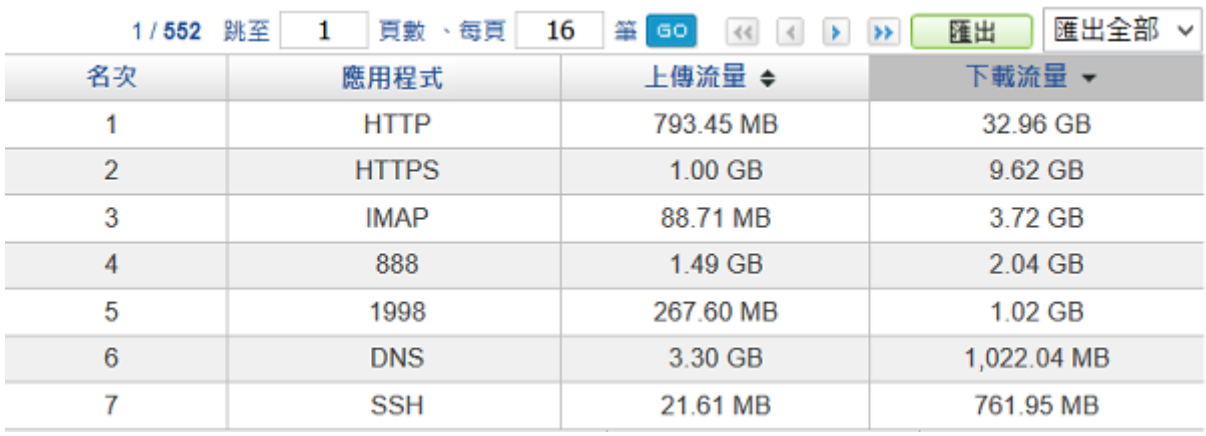


名次	服務埠號	上傳流量	下載流量
1	HTTP	793.45 MB	32.96 GB
2	HTTPS	1.00 GB	9.62 GB
3	IMAP	88.71 MB	3.72 GB
4	888	1.49 GB	2.04 GB
5	1998	267.60 MB	1.02 GB
6	DNS	3.30 GB	1,022.04 MB
7	SSH	21.61 MB	761.95 MB

圖 178. 圖15-16 Port 流量統計¶

12-3-3、流量排行 By APP

顯示在統計時間範圍內 INF 的總應用程式流量排行榜，例如：用 LINE、HTTPS 跟 SKYPE 等應用程式使用的總量，並列成排行榜，
流量分別可以用上傳、下載流量進行排序，點選欄位項目的 ⬍ 可改變排序方向。
INF 預設不會顯示無法辨識的應用程式，若希望無法辨識的應用程式也要顯示，則需要勾選【顯示 Unknown】。



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 179. 圖15-17 APP 流量統計¶

12-3-4、流量排行 By Location

顯示在統計時間範圍內 INF 整台的目的 IP 位址的地區資訊，並根據地區統計總使用量。流量分別可以用上傳、下載流量進行排序，點選欄位項目的 ⬍ 可改變排序方向。

1 / 1 跳至 1 頁數 每頁 16 筆 GO 匯出 匯出全部

名次	IP 地區	上傳流量	下載流量
1	日本	10.08 MB	97.56 MB
2	美國	4.09 MB	17.85 MB
3	other	2.28 MB	14.40 MB
4	臺灣	4.40 MB	11.17 MB
5	英國	275.01 KB	10.34 MB

圖 180. 圖15-18 地區流量統計¶

12-3-5、流量排行查詢

查詢前 10 ~ 500 名的流量排行，可調整的條件項目如下：

【日期】：欲查詢的日期與時間範圍。

【連線類型】：分來源跟目的 2 種連線類型。

【查詢條件】：來源 IP、目的 IP 位址、目的 Port、上網認證、應用程式、IP 地區、出口線路。

【查詢排名】：系統預設顯示前 10 名的列表，可於下拉選單選擇其他排行數量。

按下【搜尋】後，查詢結果會顯示於下方列表，如下圖：

查詢結果：

查詢排名	前 10 名
日期	2021-10-21 00:00 ~ 2021-10-21 23:00

匯出

電腦名稱	IP 位址	MAC 位址	上網認證	上傳流量	下載流量
192.168.50.100	192.168.50.100	6c:02:e0:b8:f1:fc		23.40 MB	162.52 MB
192.168.186.1	192.168.186.1	00:60:e0:85:e7:ec		0.23 KB	0.00 KB

圖 181. 圖15-19 流量排行搜尋結果¶

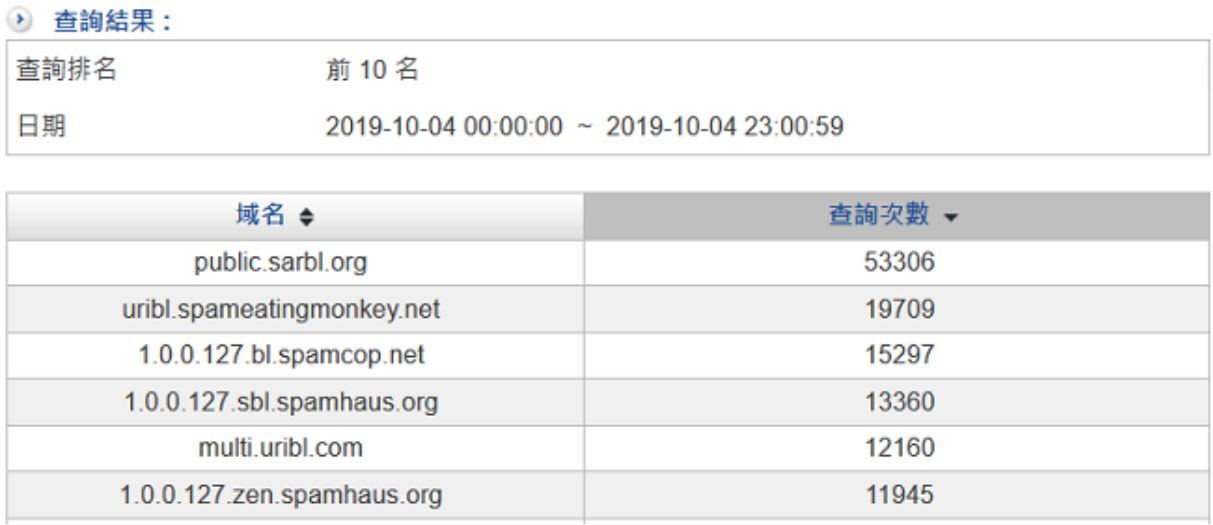
12-3-6、流量配額查詢

在管制條例中設有每個 IP 位址能使用的流量總額，可在此查詢使用者的流量歷史紀錄。

12-3-7、DNS 排行查詢

DNS 是網路連線的第一個動作，透過統計 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。
可依日期、統計方式及查詢條件進行查詢，統計方式有三種：依域名 / 依 DNS 伺服器 / 依來源 IP，三種統計方式的查詢結果如下：

1. 依域名： 統計內部對外 DNS 查詢的域名及次數排行。



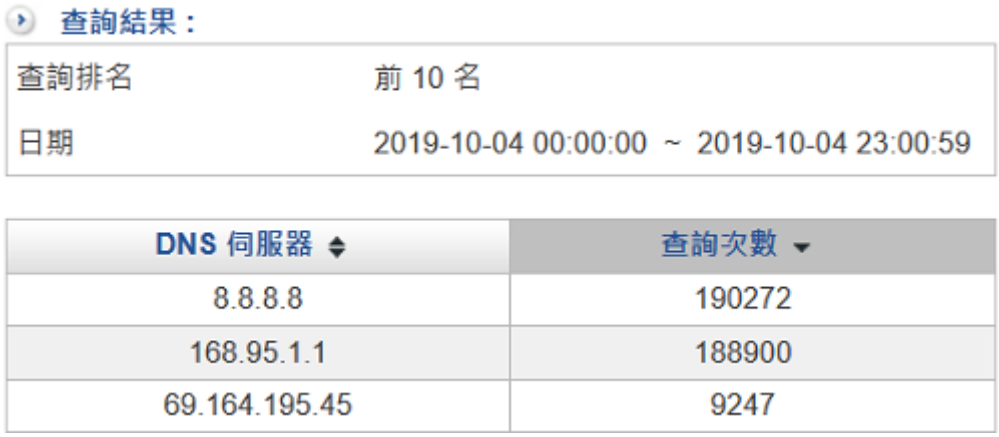
查詢結果：

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 182. 圖15-20 網域跟次數¶

2. 依 DNS 伺服器： 統計使用的 DNS 伺服器次數排行。



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 183. 圖15-21 DNS 伺服器跟次數¶

3. 依來源 IP： 統計內部 IP 使用 DNS 查詢的次數排行。

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 184. 圖15-22 內部的 DNS 查詢次數¶

第13章 Dashboard

跟傳統 UTM的數據呈現方式不同，INF 的 Dashboard（威脅情報儀表）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，便於管理者找出問題的根源。

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。

此處的功能列表可以操作：

1. 時間：可以選擇 24 小時模式或自訂範圍。
2. 排行：設置各項目的統計排行數量。預設為 10，表示會顯示前 10 名的數據。
3. IPV4/IPV6：切換目前的位址。
4. PNG/PDF：依選擇的檔案格式下載目前顯示的統計資料。
5. 刷新：重新整理。

Tip

影片參考｜眾至NU系列 UTM教學 Dashboard介紹、Dashboard報表與配送

13-1、威脅情報

顯示 INF 的攻防紀錄。首頁的威脅情報分成即時資訊跟依風險類型分類的攻防資訊，即時資訊顯示今日最高連線、可疑連線等，
依風險類型分類的攻防資訊可以依今日或本月份把病毒防護、垃圾郵件、IPS、防火牆防護跟各種管制羅列出來，同時跟最近五個月內的月份做簡單的比較。

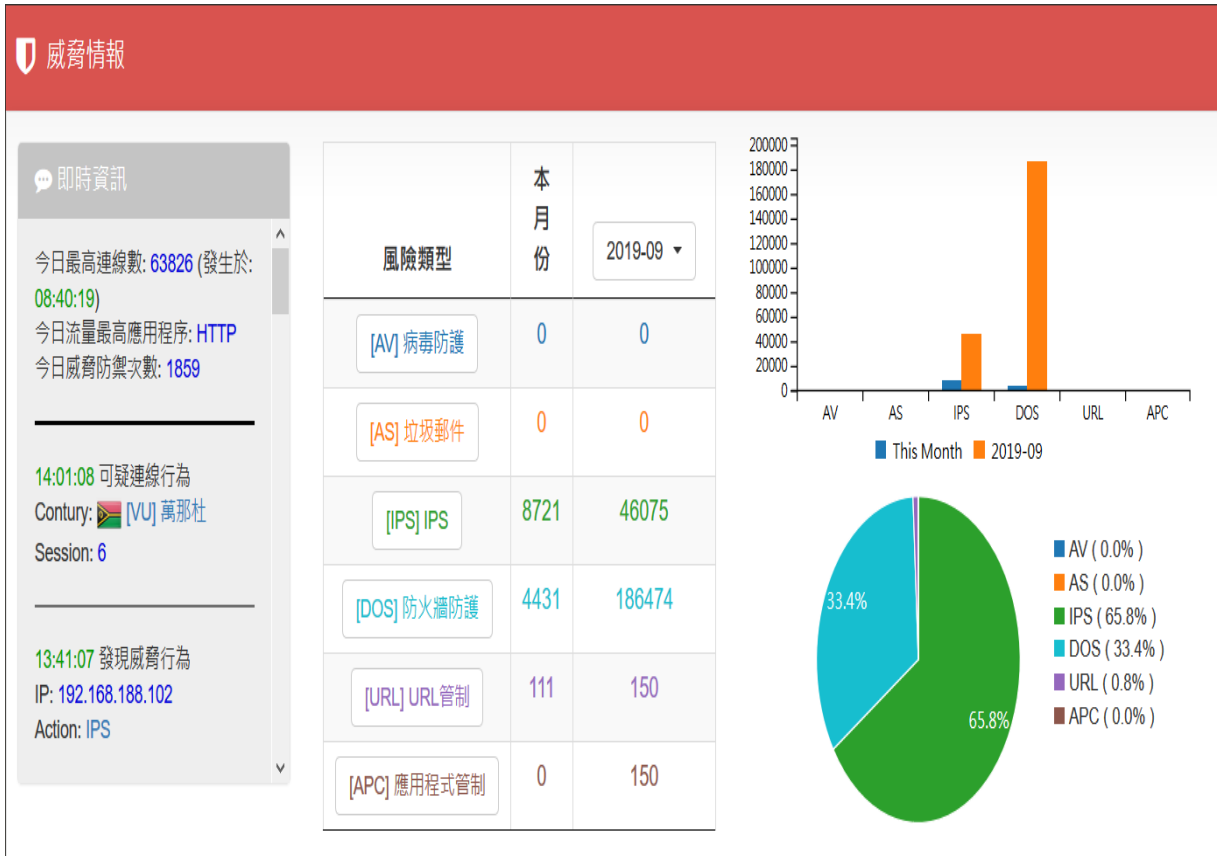


圖 185. 圖16-1 威脅情報 Dashboard¶

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，即會開啟新視窗顯示更完整的資訊，包含區域圖、圓餅圖及各風險類型的排行列表。

13-2、流量分析

INF 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其使用的應用程式並統計它的使用量，
Dashboard 的流量分析 (Application) 會將這一些統計數據以圖形介面呈現。

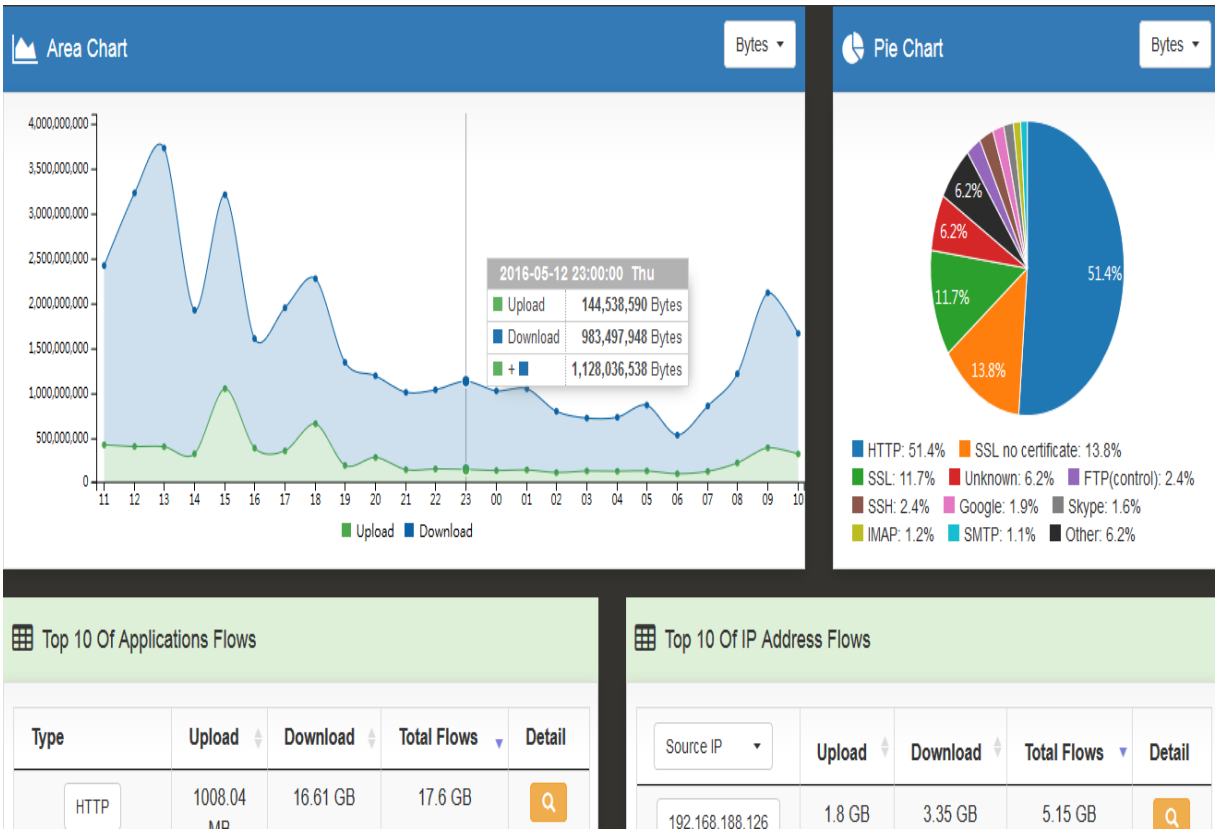


圖 186. 圖16-2 Applications 的 Dashboard¶

【區域圖】：過去 24 小時內，以小時為基本單位，進出 INF 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。

以上圖為例，點選 18:00 的流量，系統會自動統計 17:30~18:30 經過 INF 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，如下圖。
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。

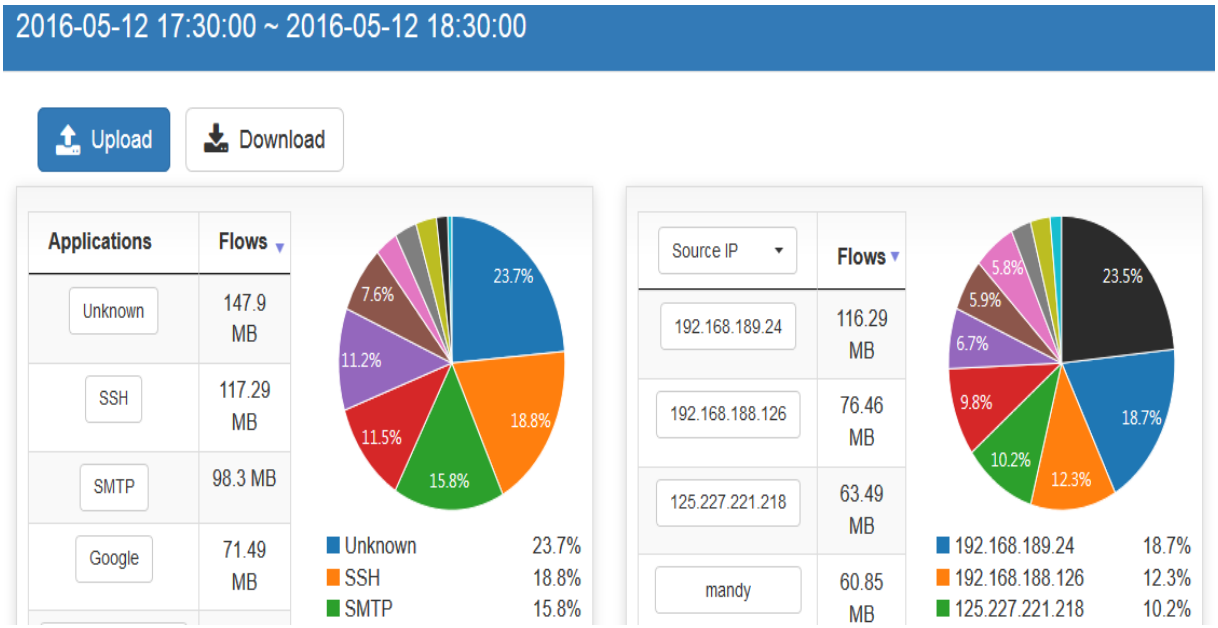


圖 187. 圖16-3 每小時的應用程式使用量分析¶

【圓餅圖】：每一個應用程式的分布比例。

【前 10 名 應用程序流量】：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，系統會自動在【區域圖】分析這一個應用程式在過去 24 小時內的分布。

點選每個應用程式詳細欄位的圖示  ，進入更詳細的統計分析，以點選 SSH 為例：INF 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。

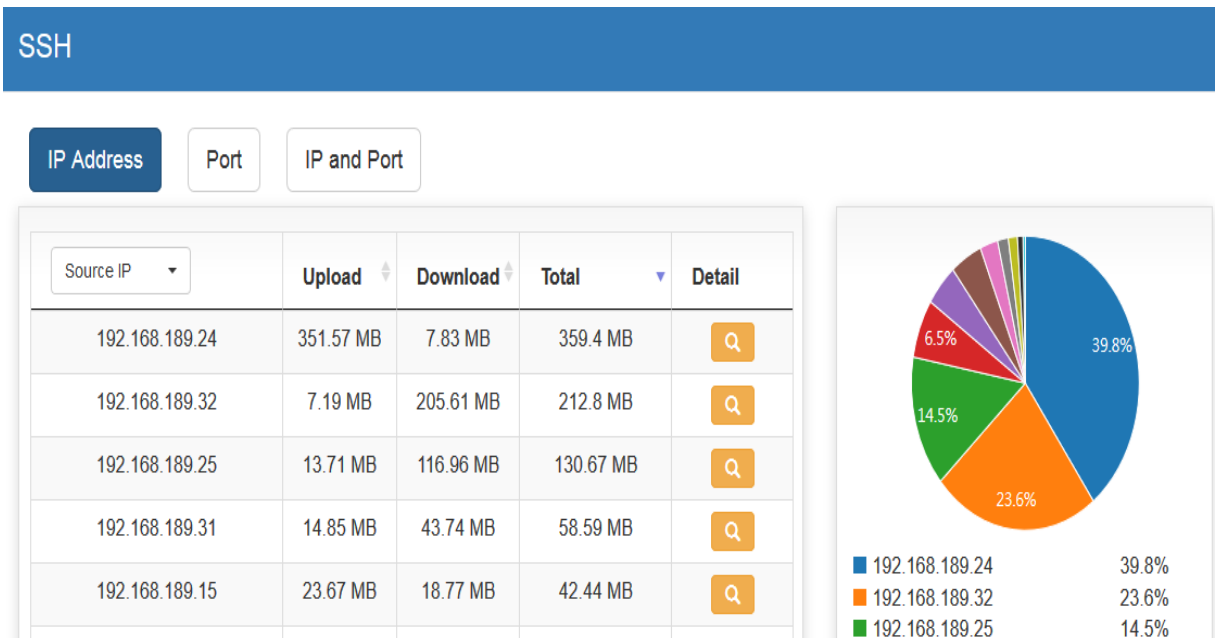


圖 188. 圖16-4 應用程式使用量分析¶

再點選每個 IP 位址後詳細欄位的圖示  ，則會顯示這一個來源 IP 位址使用 SSH 到哪裡、使用量分別是多少。

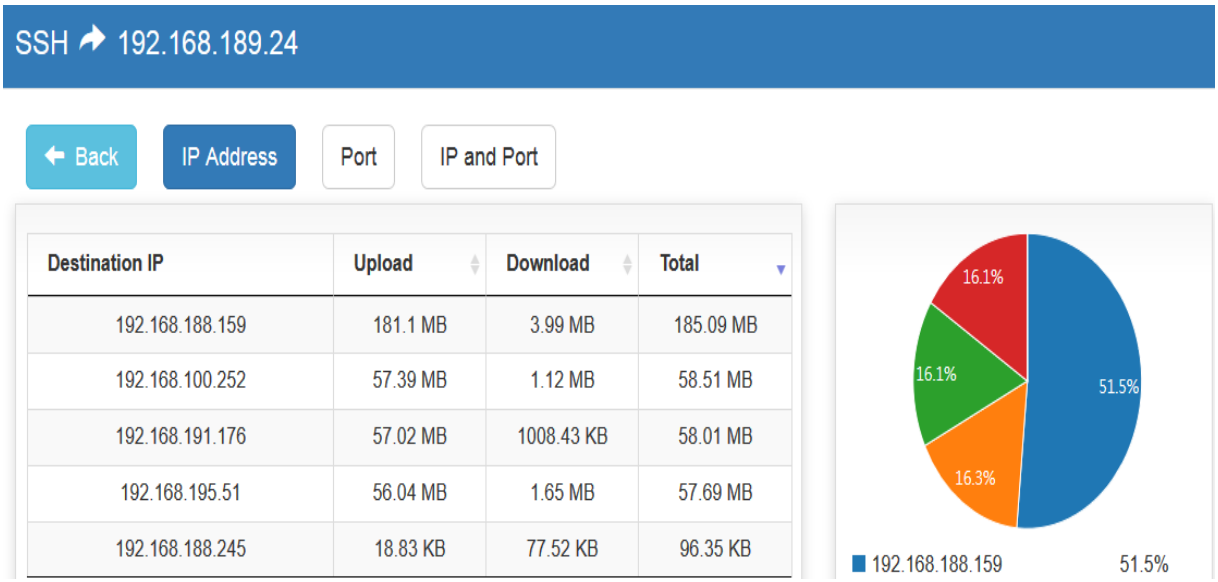


圖 189. 圖16-5 應用程式來源目的 IP 位址使用量分析¶

【前 10 名 IP 地址流量】：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，系統會自動在【區域圖】分析這一個 IP 位址在過去 24 小時內的使用量分布，

跟前面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。

13-3、連線狀態

INF 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。
在動態顯示的圖形上，預設是統計所有的數量後再去計算它佔的比例，如果管理者想要剔除某些資料量進入總量的統計，只要在圓餅圖旁點選該項目，則 INF 就會自動剔除其資料並重新統計數量分配。

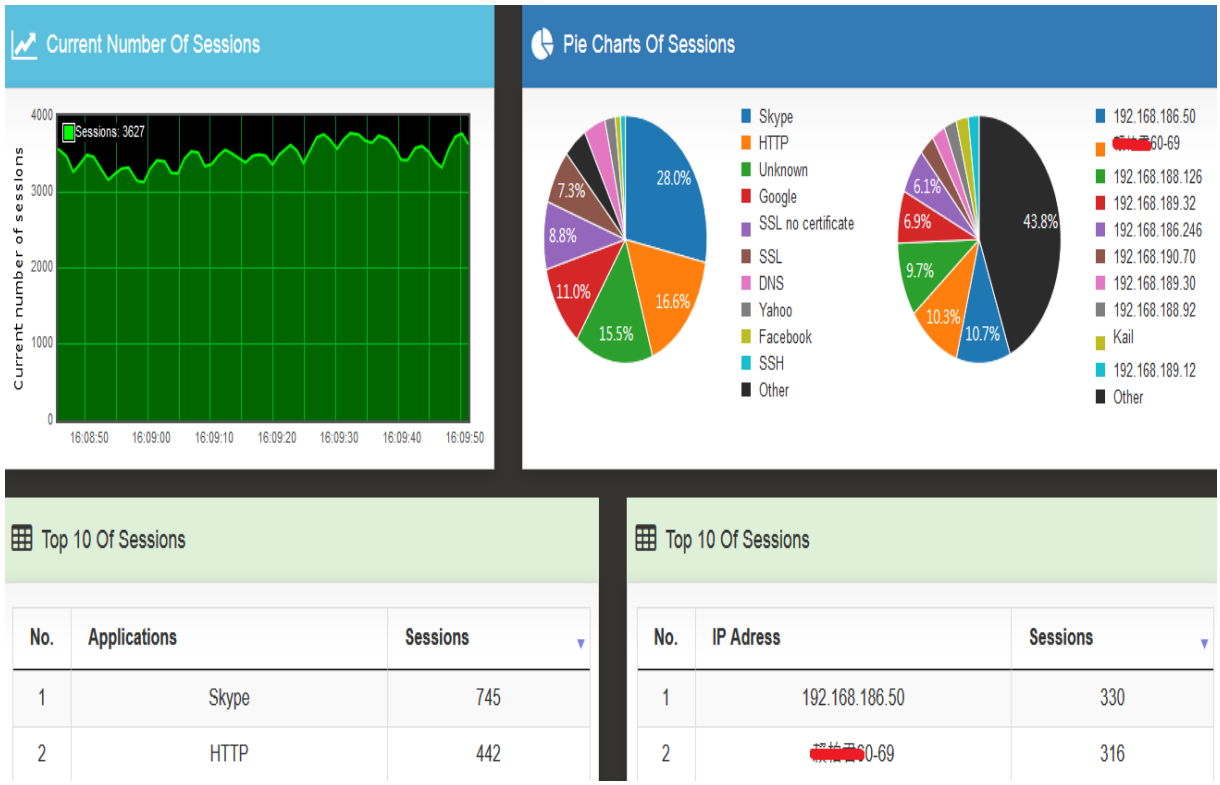


圖 190. 圖16-6 即時連線數統計¶

【圓餅圖】：根據應用程式跟連線數量統計，並顯示它的分布比例。

13-4、防火牆防護

欲查看防火牆防護的統計資訊需要事先確認以下動作：

1.「管理目標 > 防火牆功能」中其他項目必須要勾選。

2. 系統預設會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，INF 就會自動執行統計分析。

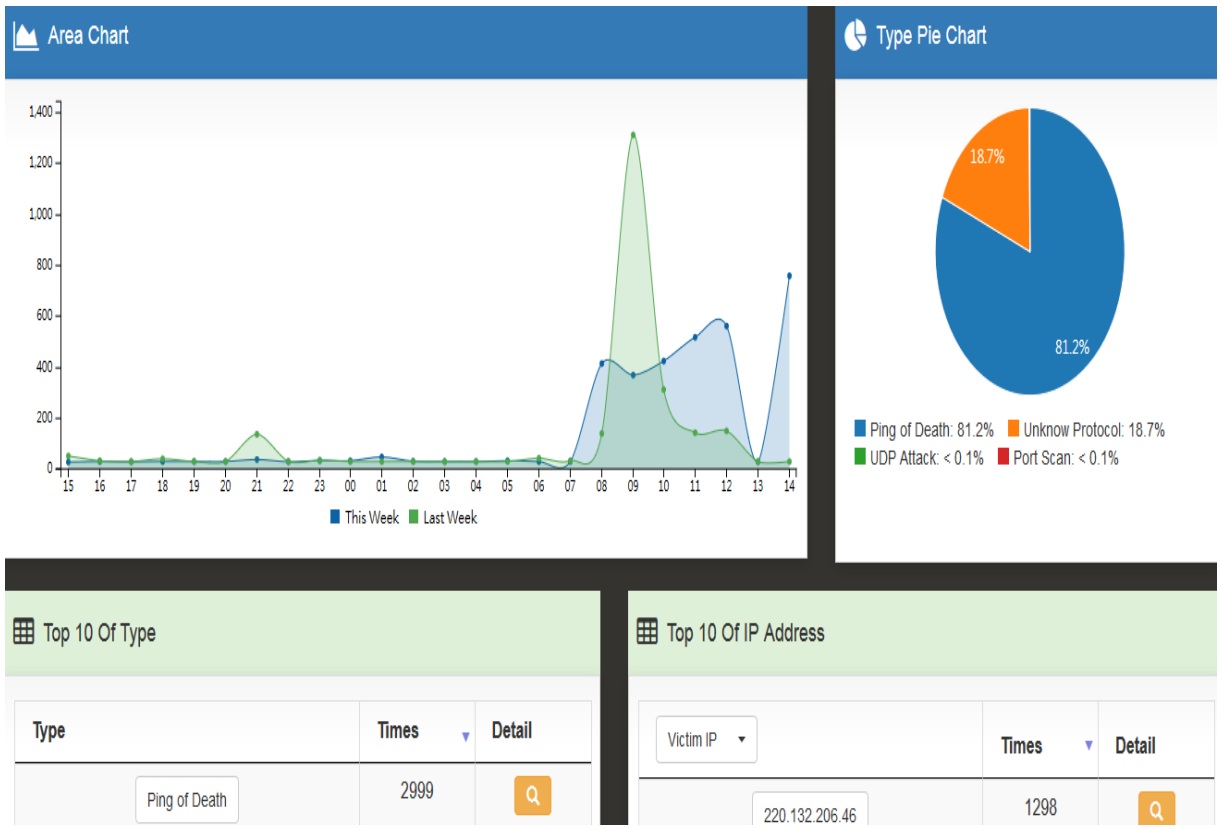


圖 191. 圖16-7 防火牆攻防紀錄¶

【圓餅圖】：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，點選詳細欄位的圖示  ，都可以繼續 Drill Down 更詳細的資訊。

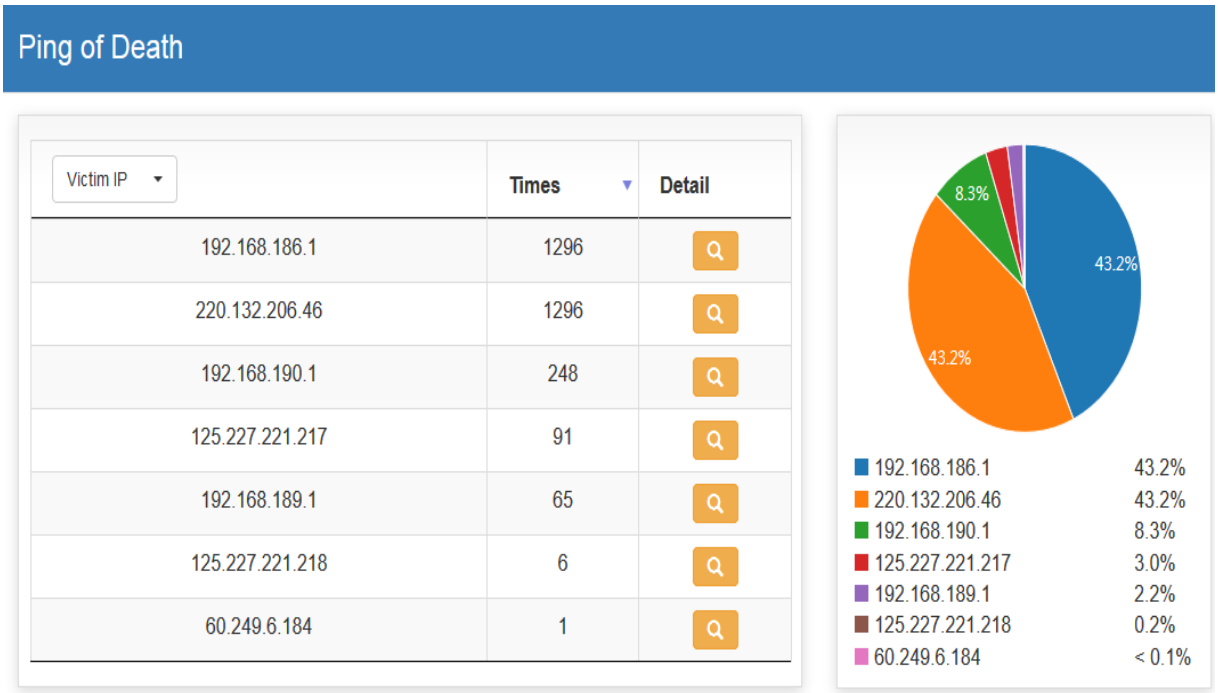


圖 192. 圖16-8 防火牆詳細紀錄¶

13-5、IPS

欲查看 IPS 的統計資訊需要事先確認以下動作：

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，INF 就會自動執行統計分析。

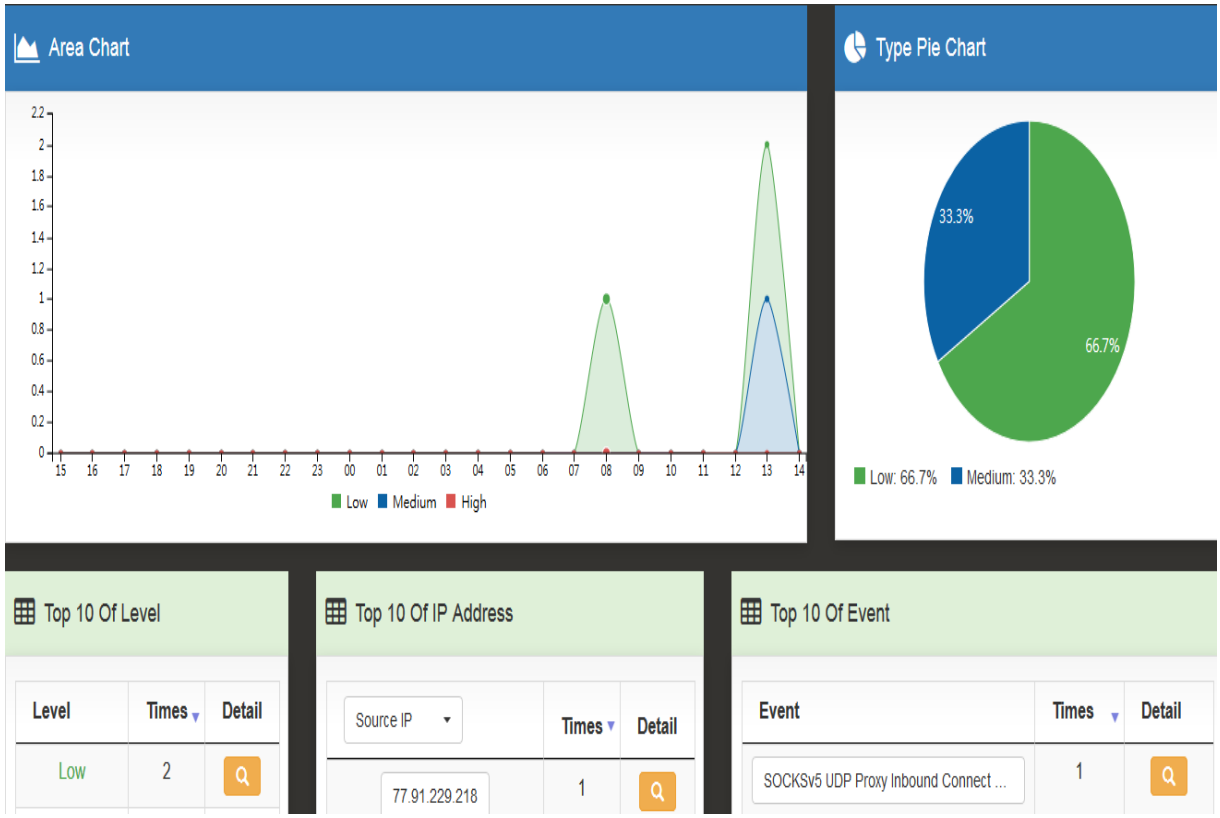


圖 193. 圖16-9 IPS 的統計¶

【圓餅圖】：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，依據風險程度、攻擊或是受害的 IP 位址及攻擊種類，點選詳細欄位的圖示  ，都可以繼續Drill Down 更詳細的資訊。

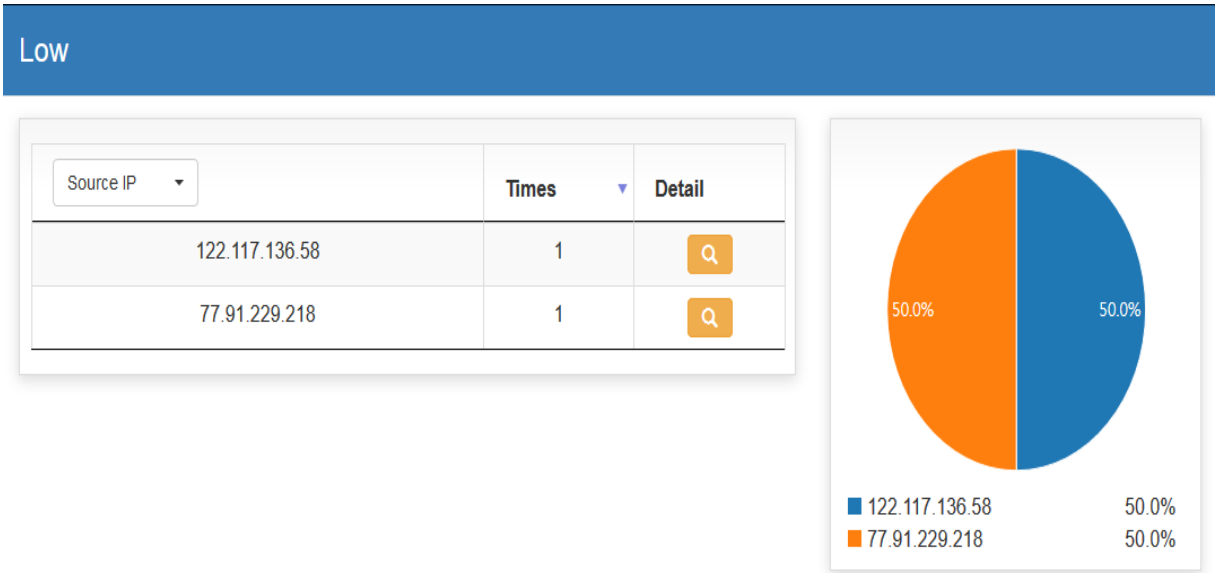


圖 194. 圖16-10 IPS 攻防詳細資料¶

13-6、Web 服務

欲查看 Web 的統計資訊需要事先確認：

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。

滿足此條件後，INF 就會自動執行統計分析。

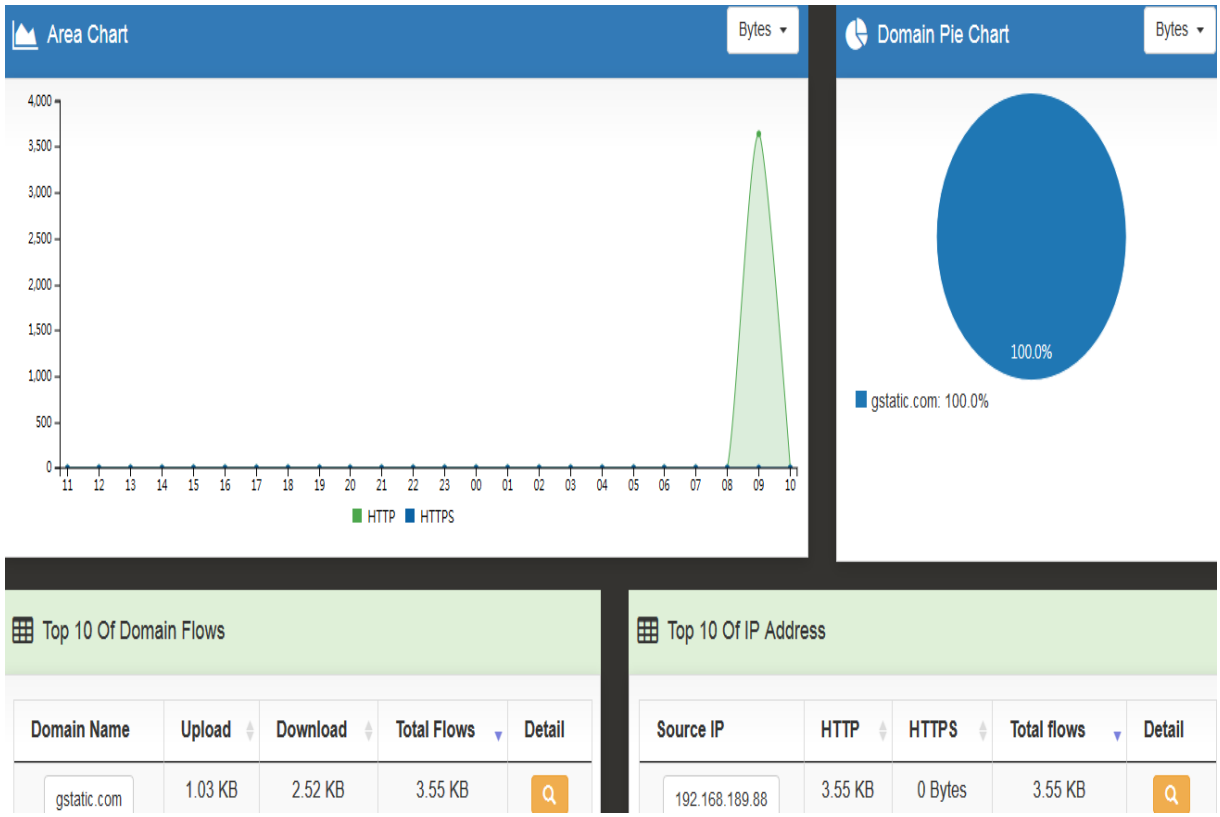


圖 195. 圖16-11 Web 的統計¶

【圓餅圖】：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，點選詳細欄位的圖示  ，都可以繼續 Drill Down 更詳細的資訊。

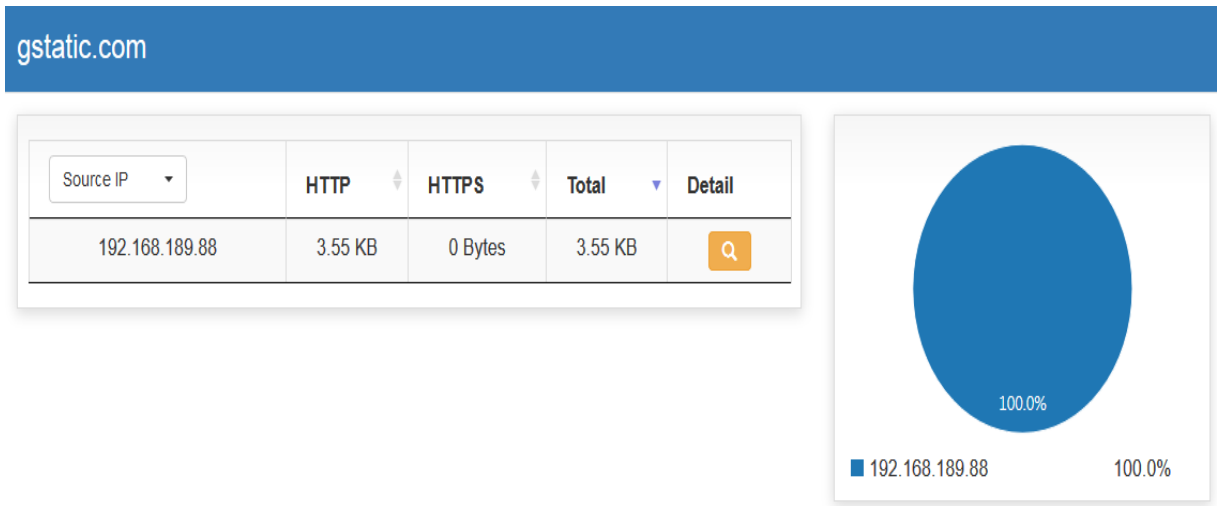


圖 196. 圖16-12 Web 的詳細分布¶

13-7、Web Control

欲查看 Web Control 的統計資訊需要事先確認：

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。

滿足此條件後，INF 就會自動執行統計分析。

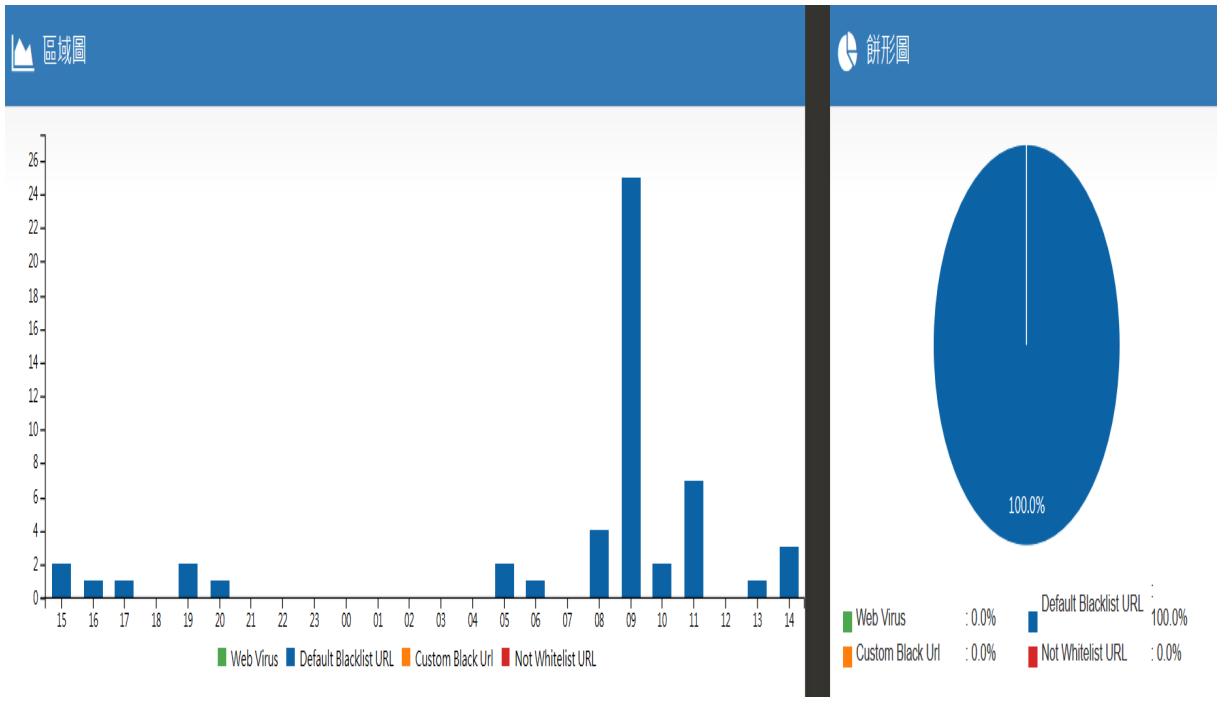


圖 197. 圖16-13 Web 的統計¶

【圓餅圖】：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。

13-8、郵件服務

欲查看 MAIL 的統計資訊有幾個地方需要事先確認以下動作：

1.「郵件管理 > 垃圾郵件過濾 > 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，INF 就會自動執行統計分析。

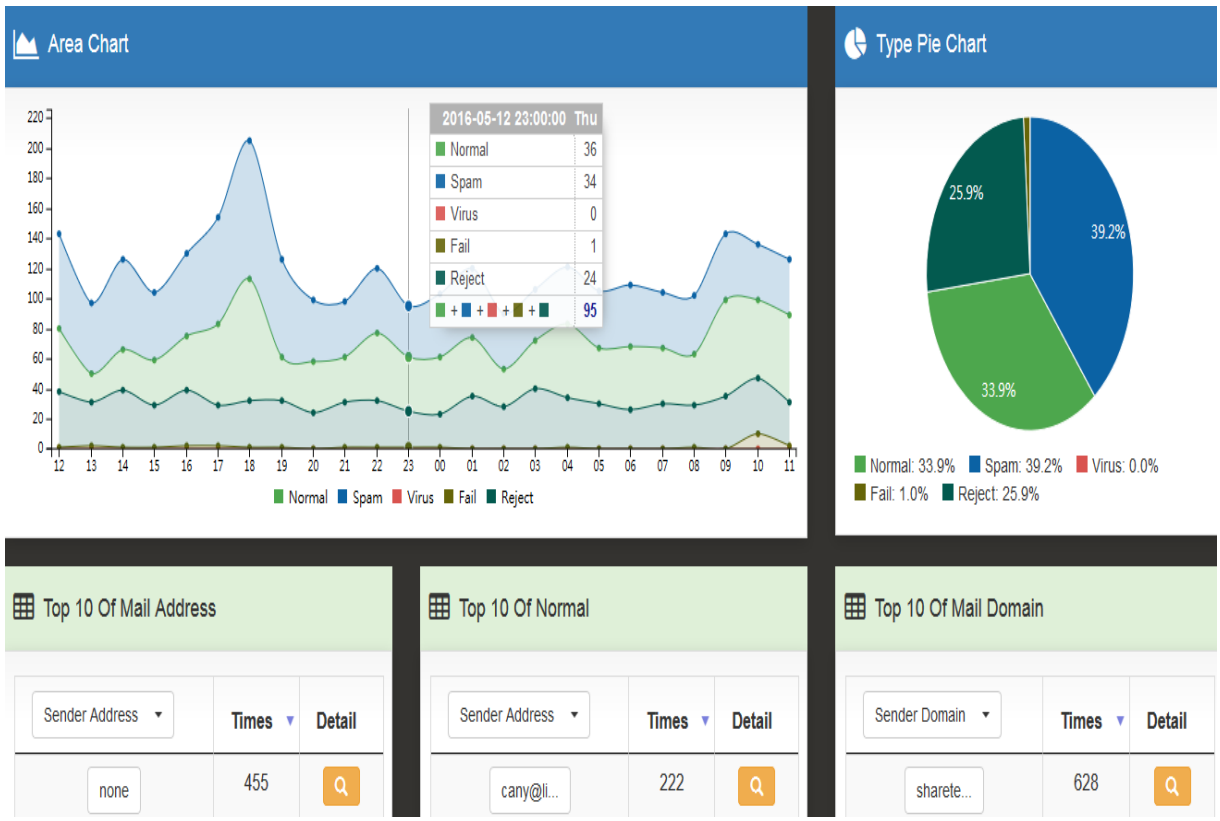


圖 198. 圖16-14 Mail 使用量分析¶

【區域圖】：過去 24 小時內，以小時為基本單位，進出 INF 的所有郵件總和的統計，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。 再點選郵件每一個項目都可以繼續追查更詳細的使用情況。

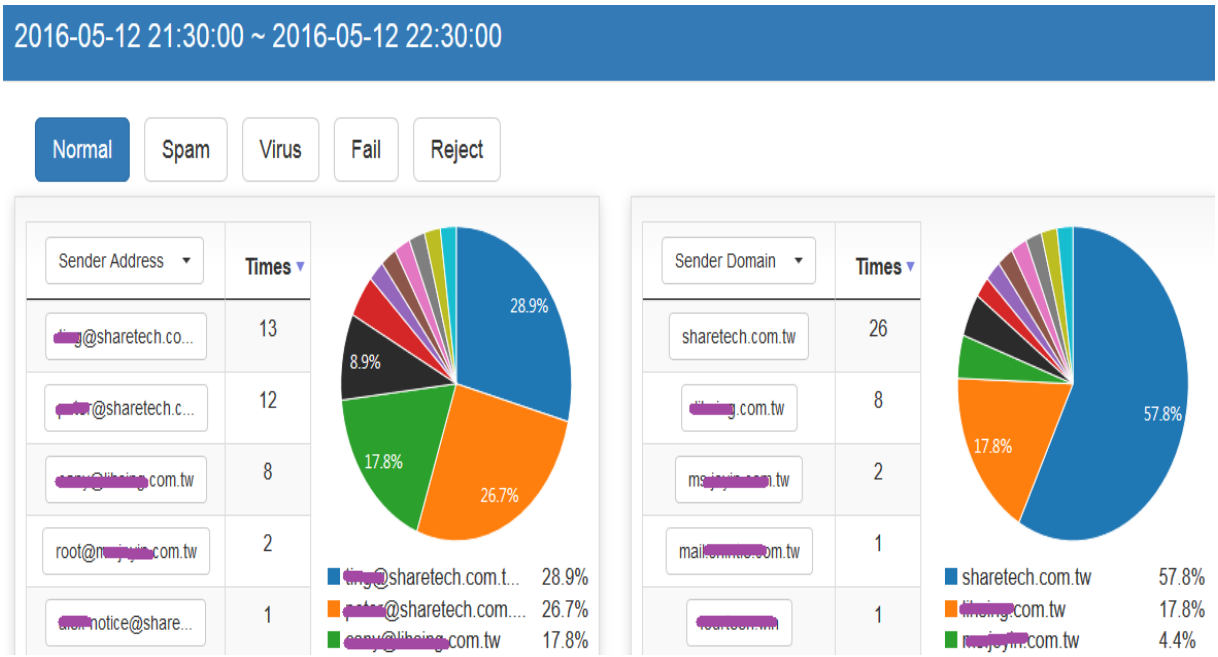


圖 199. 圖16-15 每小時 Mail 使用量分析¶

【圓餅圖】：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，點選詳細欄位的圖示  ，都可以繼續 Drill Down 更詳細的資訊。
如下圖呈現寄件者 Peter@sharetech.com.tw 寄給 hotmail.com 中 sharetech-peter@hotmail.com 的帳號，包含寄信時間、主旨、大小等資訊。

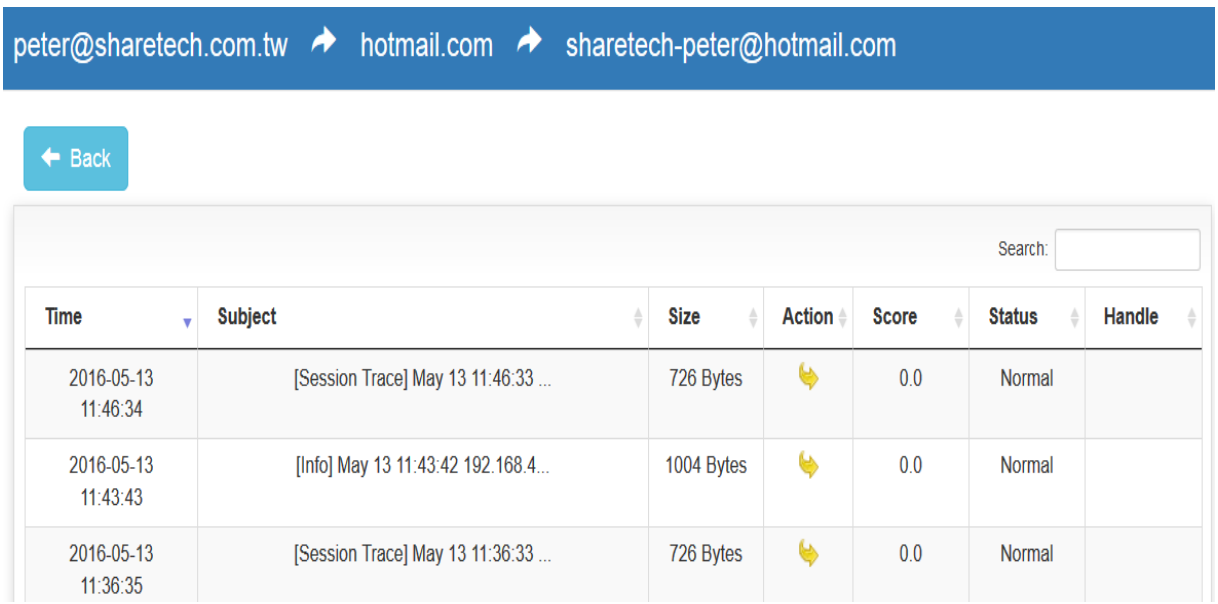


圖 200. 圖16-16 Mail 原始資訊¶

13-9、應用程式管制

（待補）

13-10、IP 地區

統計透過 INF 的目的跟來源地區（依國家）。

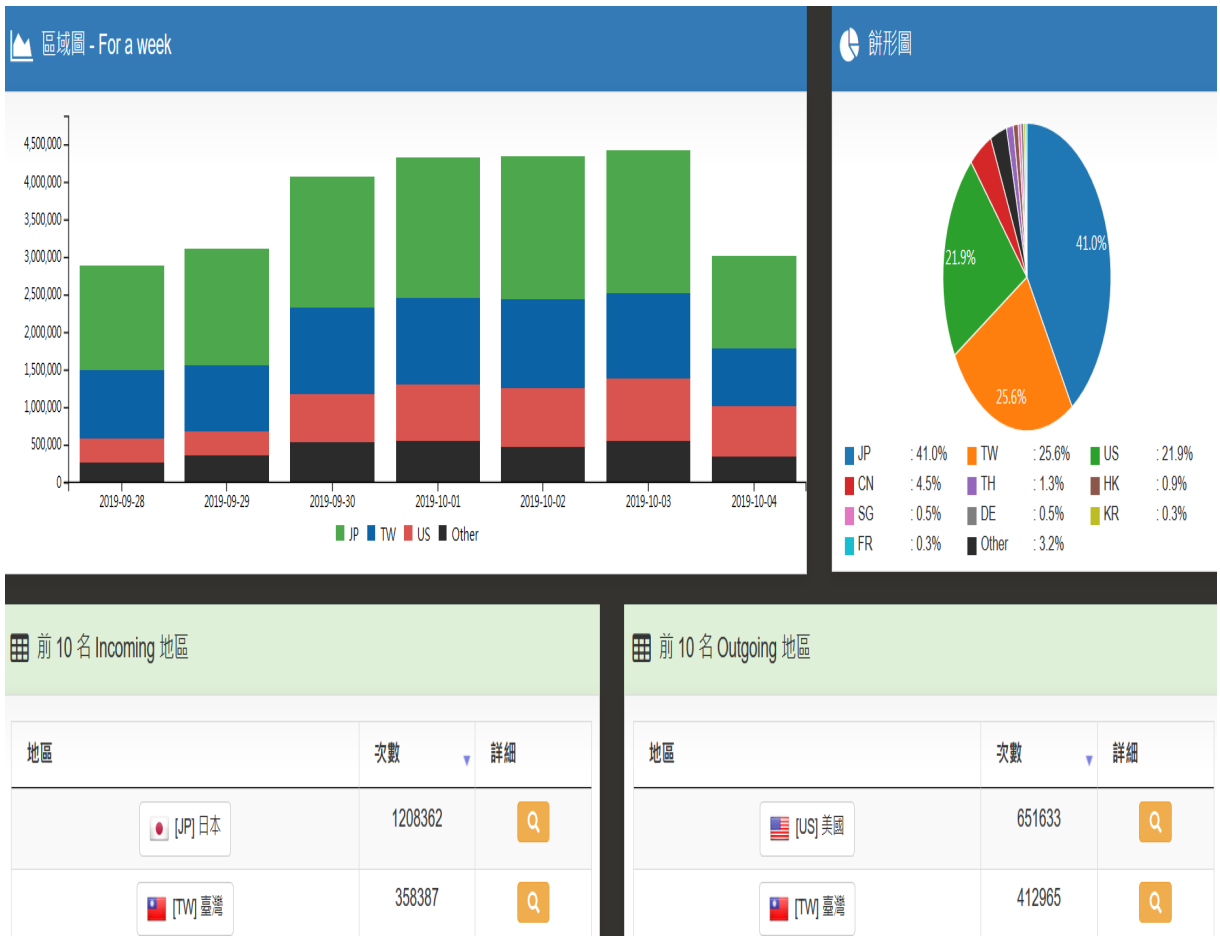


圖 201. 圖16-17 IP 地區查詢¶

13-11、DNS 查詢

統計透過 INF DNS 查詢的目的跟使用的 DNS 伺服器。

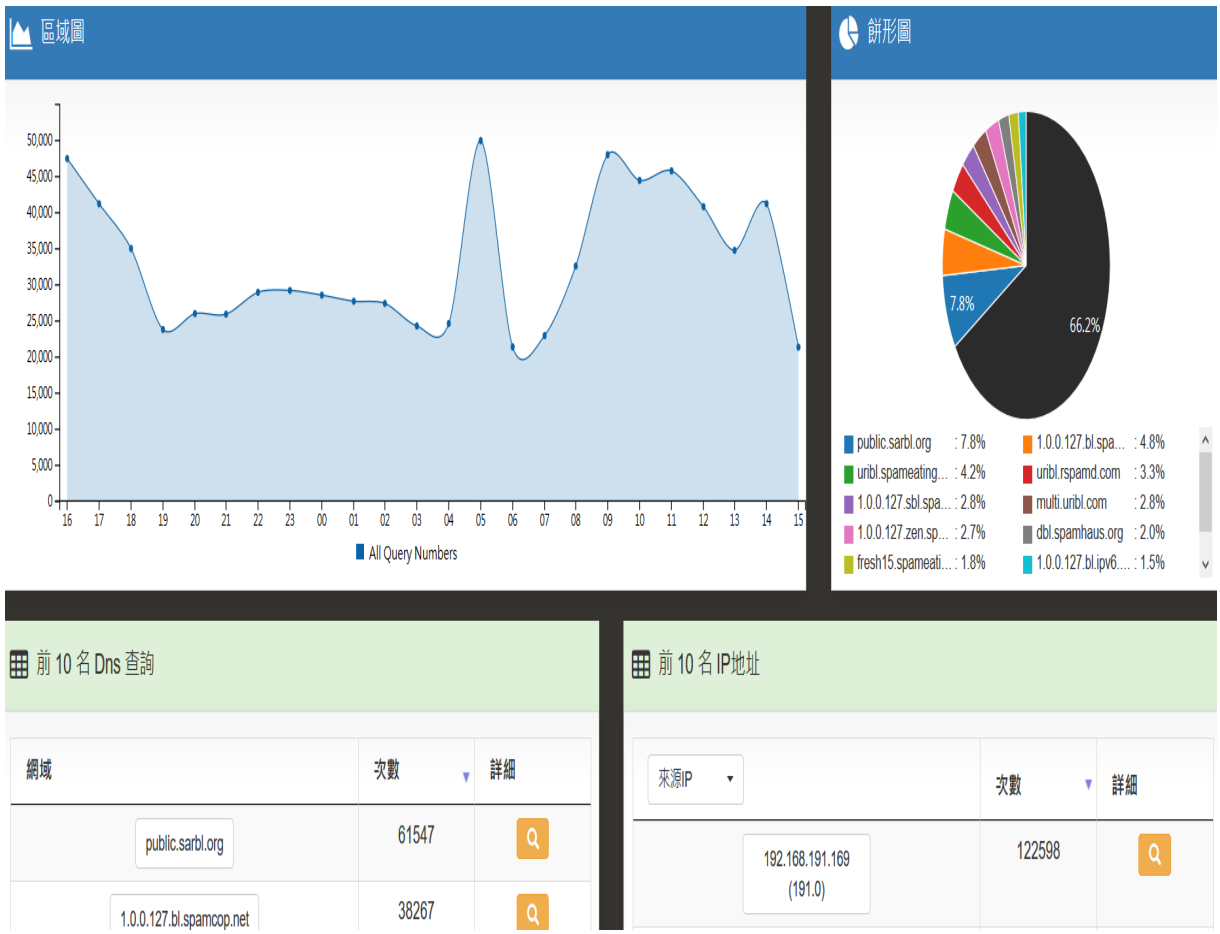


圖 202. 圖16-18 DNS 查詢¶

13-12、統計

手動設定查詢條件，點選查詢後將呈現管理者想要看到的資訊圖表。

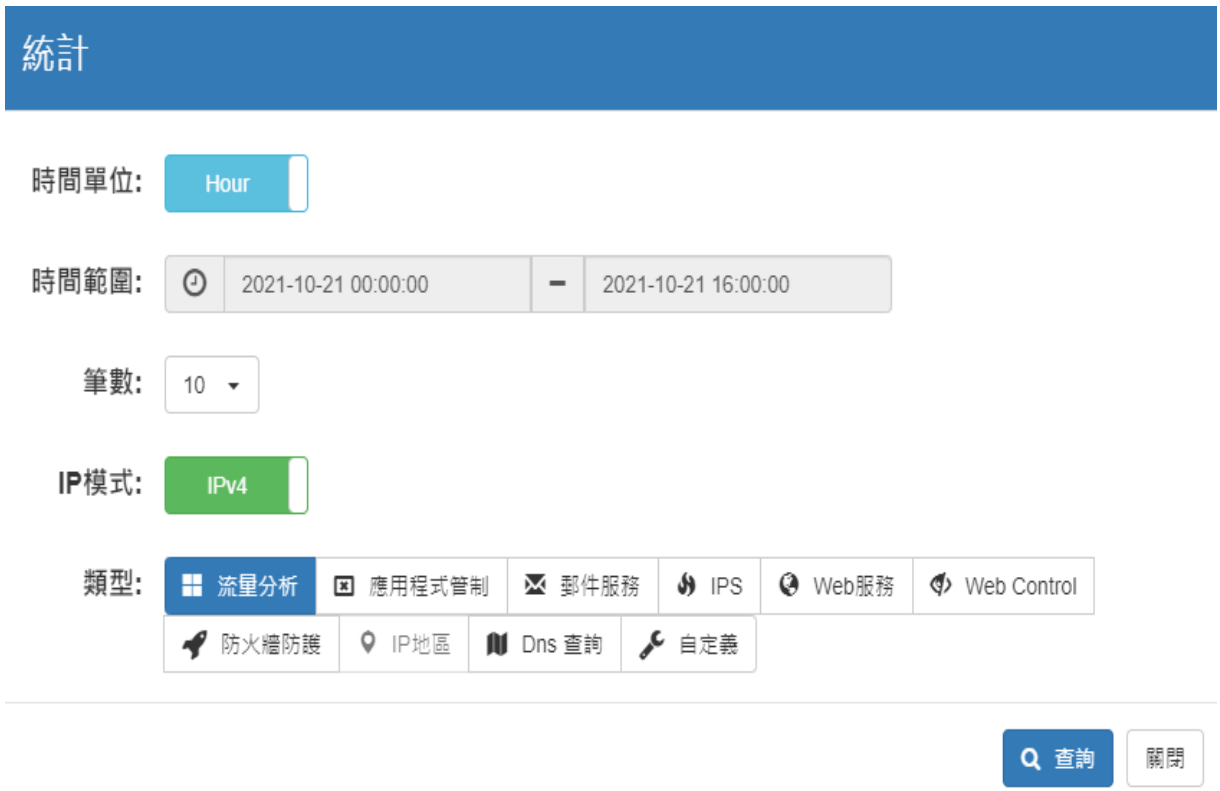


圖 203. 圖16-19 查詢統計¶

13-13、報表

將統計的資訊產生報表，可以設定寄給指定的管理者。先在 2-6、訊息通知 中設定 SMTP 伺服器後，可以於此選擇要收到報表的帳號。

圖 204. 圖16-20 報表設定¶