中華資安國際
CHT Security

資安防護閘道器

（CHTS-UTM L0510A）

使用手冊

v 1.1

目錄

壹、 產品簡介.....2

貳、 產品內容物.....3

參、 資安防護閘道器硬體規格.....3

肆、 資安防護閘道器安裝架構.....6

伍、 資安防護閘道器網頁中控平台.....7

一、 儀表板.....8

二、 網路：網際網路（WAN）.....10

三、 安全防護：安全規則.....11

四、 安全防護：資安紀錄.....17

五、 進階設定：系統管理.....18

六、 進階設定：系統工具.....19

陸、 常見問題.....20

一、 資安防護閘道器的阻擋頁面，是否有提供放行功能？.....20

二、 登入資安防護閘道器的中控平台，為何瀏覽器會出現不安全的警訊？.....20

三、 忘記資安防護閘道器的網頁中控平台的密碼，該如何重設密碼？.....20

四、 資安防護閘道器有釋出新的韌體版本，如何更新韌體版本呢？.....21

五、 安裝時提供的耦合器的用途？.....21

壹、 產品簡介

資安防護閘道器是一款精巧型的防護設備，提供網頁威脅防護（Anti-WebThreat）、入侵防護（Anti-Intrusion）、檔案型病毒防護（Anti-Virus）、防火牆（Firewall）等功能，針對企業的網路訊務進行檢測，一旦識別可疑和已確認的惡意行為將進行阻斷。

圖、產品簡介

貳、 產品內容物

資安防護閘道器設備乙台、網路線乙條、AC 電源供應器乙個。

圖、產品盒裝內容物

參、 資安防護閘道器硬體規格

共配有四顆 LED 指示燈，可以顯示設備的當前運作狀態，由左至右分別為：PWR、LAN、WAN、STATE。

圖、資安防護閘道器指示燈

1. **PWR 指示燈：**顯示設備開機狀態。

燈號	對應狀態
恆亮	已開機
熄滅	未開機

2. **LAN 指示燈：**顯示設備 LAN 端裝置連線狀態。

燈號	對應狀態
恆亮 / 閃爍	LAN 端裝置連線中
熄滅	LAN 端裝置未連線

3. **WAN 指示燈：**顯示設備 WAN 端網路連線狀態。

燈號	對應狀態
恆亮 / 閃爍	WAN 端裝置連線中
熄滅	WAN 端裝置未連線

4. **STATE 指示燈：**顯示設備系統運作狀態。

燈號	對應狀態
恆亮	系統運作中
熄滅	系統準備中
閃爍	重置系統設定中

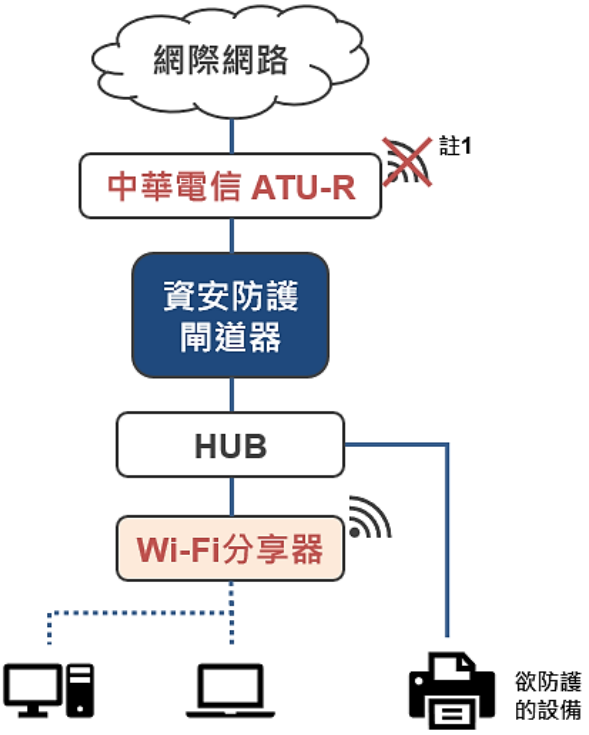
資安防護閘道器後端共配有一個按鈕與三個連接孔，由左至右，分別為：RESET 按鈕、WAN 連接孔、LAN 連接孔、DC IN 電源孔。

圖、資安防護閘道器設備後端插孔

1. **RESET 按鈕：**按下 RESET 按鈕持續超過 5 秒鐘後放開，可將資安防護閘道器重置回原廠預設設定。
2. **WAN 連接孔：**將網路線的一端連接至資安防護閘道器的 WAN 連接孔，網路線的另一端連接至中華電信 ATU-R（俗稱：中華電信小烏龜）的 LAN 連接孔。
3. **LAN 連接孔：**將網路線的一端連接至資安防護閘道器的 LAN 連接孔，網路線的另一端連接至 HUB 或 Wi-Fi 分享器的 WAN 連接孔。
4. **DC IN 電源孔：**請用隨附的電源供應器，連接資安防護閘道器的 DC IN 電源孔與電源插座。

肆、 資安防護閘道器安裝架構

資安防護閘道器支援實體線路上網，與 Wi-Fi 上網的防護，只需將資安防護閘道器設備安裝在中華電信 ATU-R（俗稱：中華電信小烏龜）與欲防護的設備的中間，即可使設備獲得保護。



圖、資安防護閘道器安裝架構

註 1：請關閉中華電信 ATU-R 的 Wi-Fi 網路功能，若無關閉 ATU-R 的 Wi-Fi 網路功能，當欲防護的設備透過中華電信 ATU-R 的 Wi-Fi 訊務上網，因上網流量未流經資安防護閘道器，則資安防護閘道器無法發揮防護功能，故無法受到保護。

伍、 資安防護閘道器網頁中控平台

資安防護閘道器配有清晰易懂的網頁中控平台，讓您可透過不同網頁瀏覽器設定各項防護功能或檢視資安威脅紀錄。

1. **儀表板：**顯示資安防護閘道器所有狀態，包含設備訊息、功能狀態和資源使用率。
2. **網路：**可自行設定網路配置，如使用 DHCP 或固定 IP。
3. **安全防護：**可設定安全功能，如：防毒系統、入侵防禦、惡意網頁阻擋和防火牆。紀錄頁面可顯示每項安全功能執行動作後的紀錄。
4. **進階設定：**系統管理頁面提供使用者設定資安防護閘道器的狀態，例如備份與還原、韌體升級等；系統工具頁面提供小工具讓使用者檢查資安防護閘道器的網路連接狀態。

如欲登入設備的網頁中控平台，請先將您的電腦、手機或平板電腦連接至資安防護閘道器 LAN 端網域，開啟瀏覽器後，輸入 https://my.securegw.tw 網址[註1]，並輸入預設密碼[註2、註3]，即可進入中控平台。

註 1：https://my.securegw.tw 中控平台不支援 IE 瀏覽器，建議請使用 Chrome、Firefox、Safari 瀏覽器。

註 2：預設密碼為設備的機身序號（SN），可於外盒或設備底部獲得此資訊，輸入時大小寫必須一致。

註 3：首次登入後，請務必於中控平台更改密碼。

一、儀表板

顯示資安防護閘道器所有狀態，包含設備訊息、功能狀態和資源使用率。

圖、儀錶板畫面

登入資安防護閘道器的網頁中控平台後，即可進入儀表板畫面，可從左側選單進入其它控制頁面。儀表板所顯示的資訊包含：

1. 裝置資訊：

1.1、 **裝置名稱**：顯示該台資安防護閘道器的名稱，可至以下路徑修改：

［系統管理］/［裝置資訊］

1.2、 **MAC**：顯示該台資安防護閘道器實體位址。

1.3、 **WAN IP**、**WAN IPv6**：顯示該台資安防護閘道器所取得的 IP（支援 IPv4 與 IPv6）。

1.4、 **特徵碼最後更新時間**：顯示最後一次更新特徵碼資料庫的日期與時間。

1.5、 **租用狀態**：顯示資安防護閘道器使用租約的狀態。

2. **狀態：**每 3 秒更新一次系統狀態。

2.1 **系統已運行：**顯示自上次設備啟動後的運行時間。

2.2 **記憶體：**顯示當前設備記憶體使用率。

2.3 **儲存空間：**顯示當前設備儲存空間使用率。

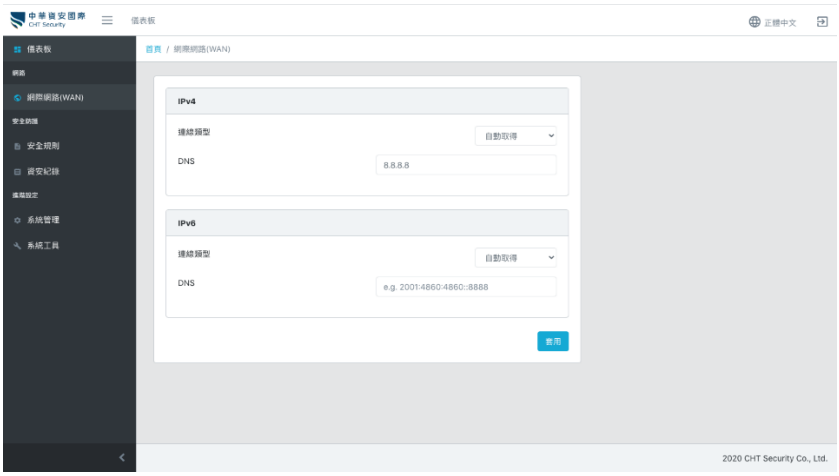
2.4 **CPU 使用率：**顯示當前設備 CPU 使用率與近期歷程。

3. 防護功能：

顯示資安防護閘道器防護功能當前的狀態，包含：防毒系統、入侵防禦、惡意網頁阻擋和防火牆。透過防護功能可快速檢視啟用狀態、各防護功能執行動作的設定、各功能所使用的特徵碼版本以及最近 24 小時內阻擋或記錄下來的威脅事件次數。

二、網路：網際網路（WAN）

在網際網路設定頁面，可以選擇連線類型為自動取得、靜態位址，或 PPPoE，以進行 IPv4 或 IPv6 的網路設置。



圖、網路：網際網路（WAN）畫面

1. **自動取得**：出廠預設值，能透過 DHCP 自動取得 IP 位址。
2. **靜態位址**：需要自行輸入正確的 IP 位址資訊。
3. **PPPoE**：需要自行輸入 HiNet 網路連線的使用者名稱與密碼。[註 1、註 2]

註 1：您可以透過此連結，了解如何找到 HiNet 網路連線的使用者名稱與密碼。

註 2：選擇 PPPoE 連線後可能會無法連線至資安防護閘道器的網頁中控平台。

三、安全防護：安全規則

1. **防毒系統：**偵測並破壞病毒檔案，防止資安防護閘道器保護的設備感染病毒。

圖、安全防護：安全規則之防毒系統設定畫面

設定選項操作方法如下：

1.1、 一般設定：

1.1.1 啟用：啟用或停用「防毒系統」功能，預設為「啟用」。

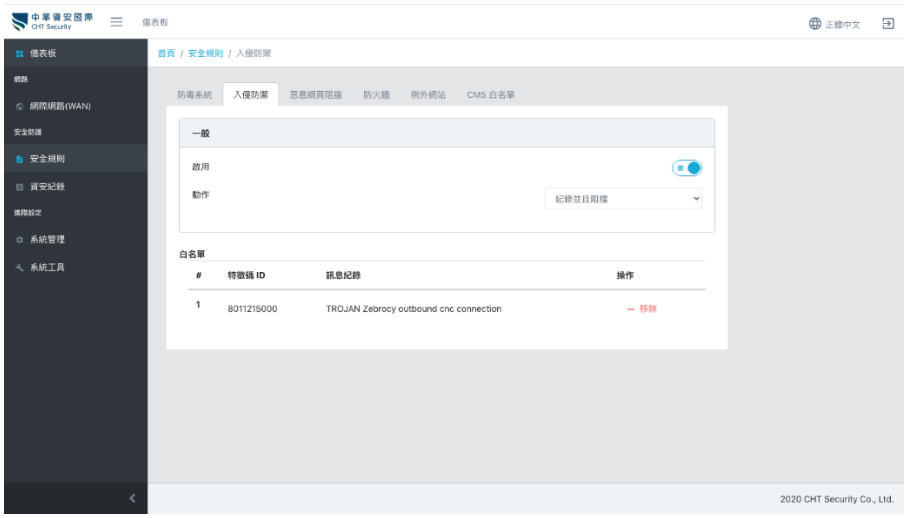
1.1.2 動作：偵測到病毒檔案後的處置措施，預設為「紀錄且破壞」。

- 紀錄：僅產生偵測到病毒檔案的紀錄。
- 紀錄並且破壞：記錄偵測結果並破壞病毒檔案，使得病毒檔案無法被正常執行。

1.2、 **進階設定：**啟用或停用雲端病毒資料庫掃描檔案功能，建議啟用以確保受到最完整的防護。

1.3、 **白名單：**顯示或移除自行加入白名單的病毒特徵碼資訊，詳細設定方式請見 [四、安全防護：資安紀錄]。

2. 入侵防禦：偵測並阻擋駭客的攻擊行為或殭屍網路的攻擊行為，以防止資安防護閘道器保護的設備遭受入侵。



圖、安全防護：安全規則之入侵防禦設定畫面

設定選項操作方法如下：

2.1 一般設定：

2.1.1 啟用：啟用或停用「入侵防禦」功能，預設為「啟用」。

2.1.2 動作：偵測入侵攻擊後的處置措施，預設為「紀錄並且阻擋」。

- 紀錄：僅產生偵測到入侵行為的紀錄。
- 紀錄並且阻擋：記錄偵測結果並阻擋入侵。

2.2 **白名單：**顯示或移除自行加入白名單的入侵行為特徵碼資訊，詳細設定方

式請見 [四、安全防護：資安紀錄]。

3. **惡意網頁阻擋**：偵測並阻擋使用者連線至釣魚網站，或連線至藏有攻擊行為的惡意網站。

圖、安全防護：安全規則之惡意網頁阻擋設定畫面

設定選項操作方法如下：

3.1 一般設定：

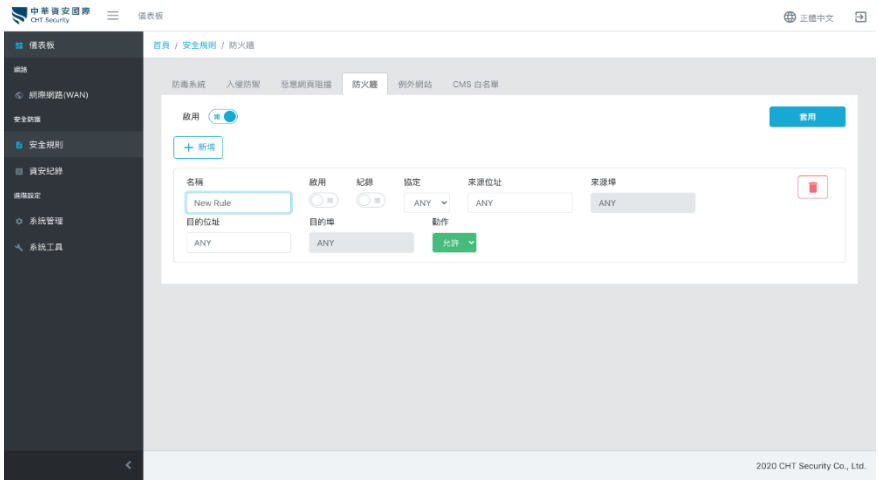
3.1.1 啟用：啟用或停用「惡意網站阻擋」功能，預設為「啟用」。

3.1.2 動作：偵測惡意網站連線後的處置措施，預設為「紀錄並且阻擋」。

- 紀錄：僅產生偵測到的連線紀錄。
- 紀錄並且阻擋：記錄偵測結果並阻擋連線。

3.2 **白名單**：顯示或移除自行加入白名單的惡意網站特徵碼資訊，詳細設定方式請見 [四、安全防護：資安紀錄]。

4. **防火牆**：能自行設定欲允許或阻擋的網路連線，規則比對順序為由上到下，當符合其中一則規則後，後續的規則將不再比對。防火牆規則可藉由滑鼠點擊拖曳，更改順序。



圖、安全防護：安全規則之防火牆設定畫面

設定選項操作方法如下：

4.1 **啟用**：啟用或停用「防火牆」功能。

4.2 **套用**：新增、修改或移除防火牆規則後，點擊「套用」開始新的規則。

4.3 **新增**：新增防火牆規則。

4.3.1 名稱：防火牆規則名稱。

4.3.2 啟用：啟用或停用該項規則。

4.3.3 紀錄：記錄或不記錄符合該項規則的連線。

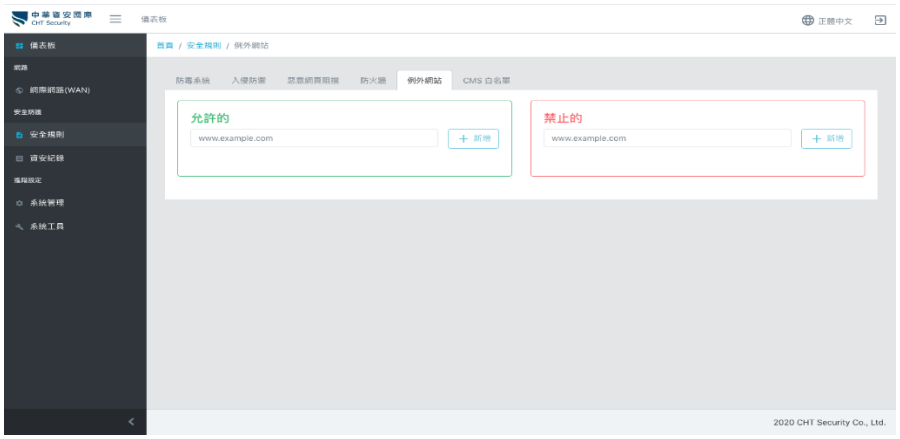
4.3.4 協定：設定允許或阻擋「TCP」、「UDP」或「任意」連線協定。

4.3.5 來源位址、來源埠、目的位址、目的埠：設定允許和阻擋的連線來源或目的。

4.3.6　動作：設定「允許」和「阻擋」。

4.3.7　移除：移除該項規則。

5. **例外網站：**能自行填入網域名稱，完全允許或完全阻擋該網域連線，不受其它安全防護功能的限制。



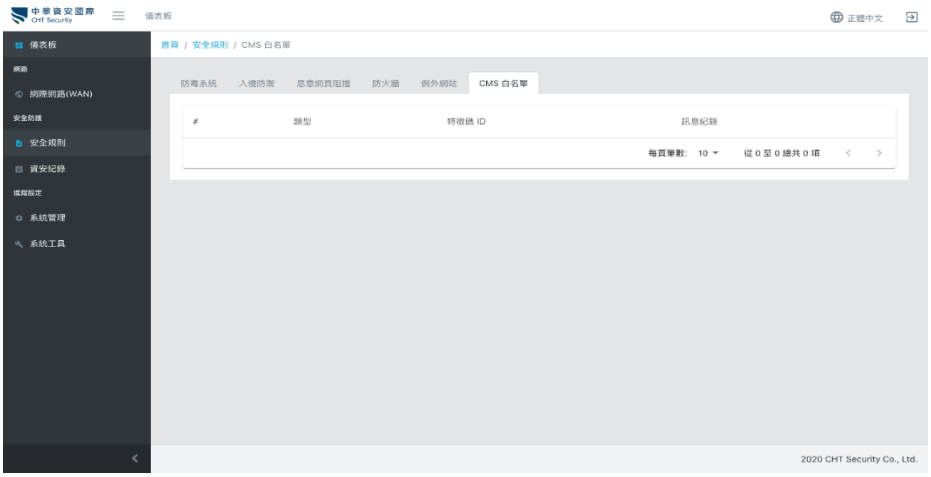
圖、安全防護：安全規則之例外網站設定畫面

設定選項操作方法如下：

5.1 依據需求，將網域名稱填入「允許的」或「禁止的」下的輸入框，並點擊「新增」即開始該項例外規則。

5.2 若欲移除例外規則，點擊該項規則旁的「移除」即可生效。

6. **CMS 白名單：**當中華資安國際的防護小組為資安防護閘道器設定共用的安全規則後，將會顯示白名單於「CMS 白名單」頁面。

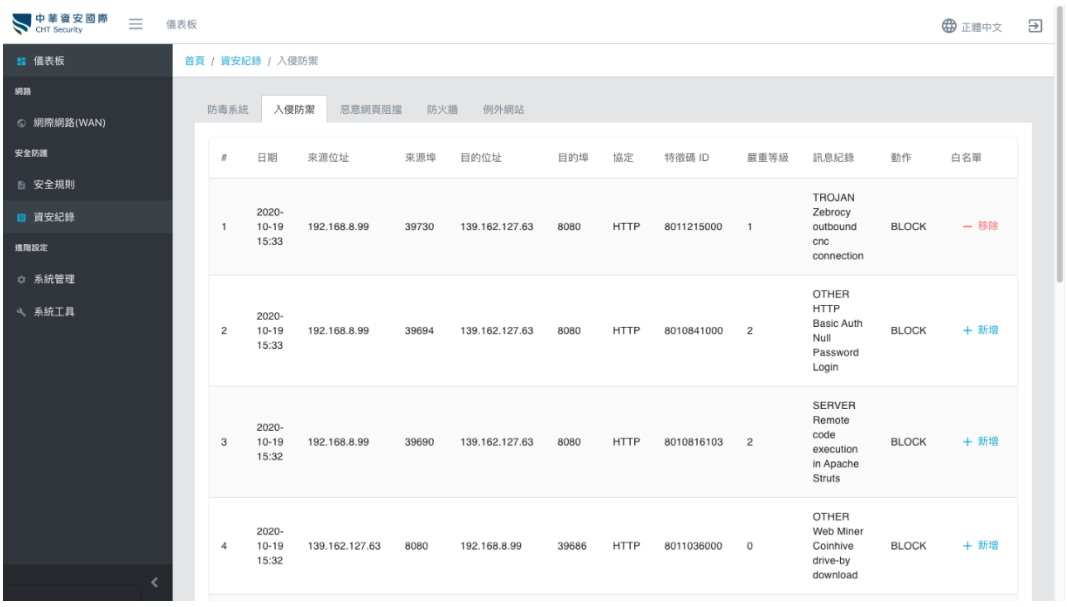


圖、安全防護：安全規則之 CMS 白名單設定畫面

四、安全防護：資安紀錄

「資安紀錄」頁面下分別以不同分頁顯示「防毒系統」、「入侵防禦」、「惡意網頁阻擋」、「防火牆」與「例外網站」所偵測、摧毀檔案、阻擋連線或允許連線的近期歷史紀錄。

若「防毒系統」、「入侵防禦」或「惡意網頁阻擋」紀錄中含有您不希望摧毀的檔案或阻擋的連線，可以點擊該項紀錄最右側的「新增」，將該檔案或該連線加入白名單。若需從白名單移除，也可以點擊「移除」或從 [安全防護] / [安全規則] 下的對應白名單中移除。



圖、安全防護：資安紀錄畫面

五、進階設定：系統管理

「系統管理」頁面提供下列功能調整資安防護閘道器的系統設定：

1. **裝置資訊：**設定資安防護閘道器裝置名稱。
2. **備份＆復原設定：**下載資安防護閘道器當前各項設定，或將先前備份的設定檔復原回資安防護閘道器。
3. **更新韌體：**自動檢查韌體版本是否為最新版，或手動上傳並安裝韌體。
4. **Email 通知：**設定 SMTP 伺服器資訊，以啟用電子郵件通知功能。
5. **Syslog：**設定 Syslog 伺服器以回傳資安防護閘道器各項紀錄，此項功能為較大規模的網路管理進階功能。
6. **更改密碼：**變更資安防護閘道器的網頁中控平台登入密碼，若忘記密碼，需將資安防護閘道器設備重新設定。
7. **ACL：**設定能夠存取網頁控制介面的裝置 IP 位址。

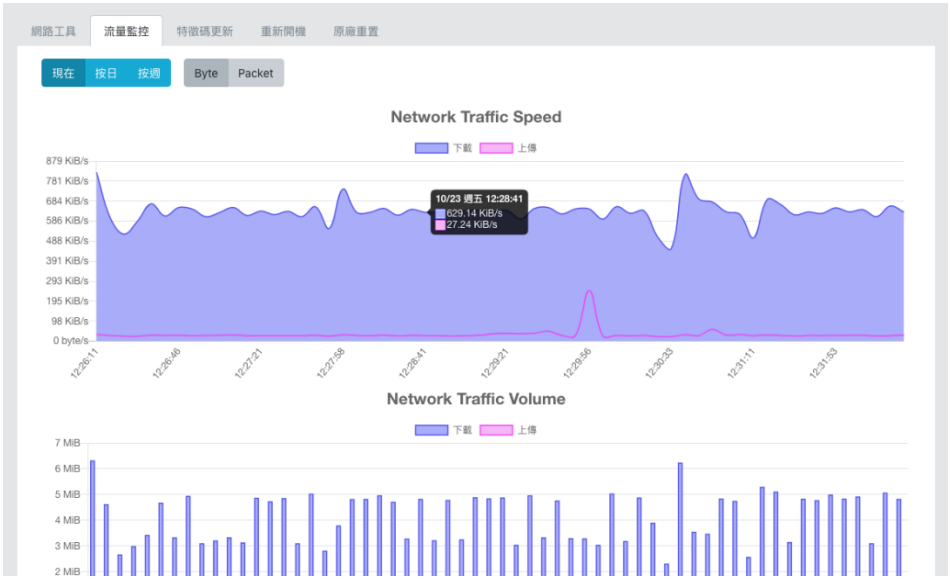
為降低資安防護閘道器受到外來入侵的威脅，預設僅開放同網域下的裝置以內部網路 IP 登入網頁控制介面。若您需要從其它網域連線至資安防護閘道器網頁控制介面，或需要在資安防護閘道器上使用 PPPoE 並取得外部網路 IP，請務必提前將欲連線至資安防護閘道器所使用的裝置 IP（建議為靜態位址）新增至 ACL 存取控制清單中。

六、進階設定：系統工具

提供下列功能，讓您能檢測或排除資安防護閘道器的系統問題：

1. **網路工具**：提供＂ping＂、＂traceroute＂、＂nslookup＂等指令檢測資安防護閘道器網路連線問題。

2. **流量監控**：即時顯示資安防護閘道器的網路流量以檢測是否有不正常的行為。



圖、進階設定：系統工具之流量監控畫面

3. **特徵碼更新**：無法透過網路連線自動更新特徵碼時，手動更新特徵碼資料庫。

4. **重新開機**：重新啟動資安防護閘道器。

5. **原廠重置**：重置資安防護閘道器所有設定至原廠預設值。

陸、 常見問題

一、資安防護閘道器的阻擋頁面，是否有提供放行功能？

A：沒有，為確保用戶的連線安全，因此阻擋頁面沒有提供放行的功能。若有發現被誤攔阻，除可透過 SOC 電話（02）2344-3693 進行申訴外，也可透過資安防護閘道器的網路監控平台 [安全防護：安全規則] / [例外清單] 進行解除。

圖、資安防護閘道器阻擋畫面

二、登入資安防護閘道器的中控平台，為何瀏覽器會出現不安全的警訊？

A：因瀏覽器不認得資安防護閘道器的中控平台（https://my.securegw.tw）網頁憑證，故會跳出此告警訊息，您可安心前往資安防護閘道器的網頁中控平台。

三、忘記資安防護閘道器的網頁中控平台的密碼，該如何重設密碼？

A：目前尚未提供重新設定密碼的功能。但您可以透過以下方式將密碼恢復成預設密碼：按下資安防護閘道器後方的 RESET 按鈕持續超過 5 秒鐘後放開，設備將回到出廠設定，即可將密碼恢復成預設密碼。重新設定前，若需保留原有設定，建議您可撥打 SOC 電話（02-2344-3693）協助您處理。

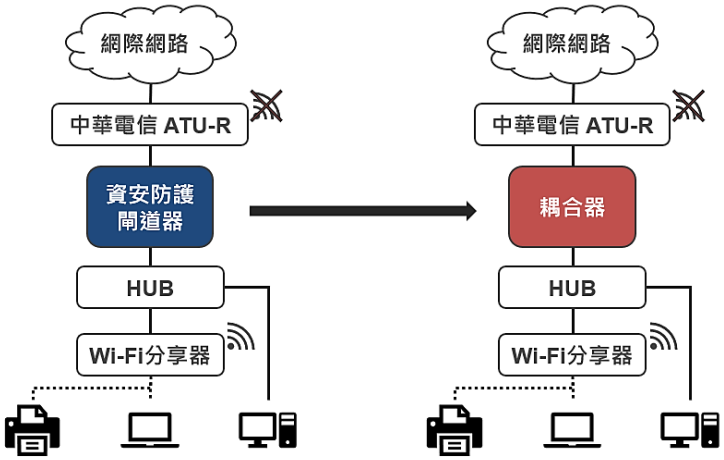
四、資安防護閘道器有釋出新的韌體版本，如何更新韌體版本呢？

A：只需重啟資安防護閘道器設備，設備將會自動更新成新的韌體版本。重啟設備後，進入資安防護閘道器的網頁中控平台 https://my.securegw.tw，選擇［儀表板］／［裝置資訊］查看韌體版本是否已經進行更新。

五、安裝時提供的耦合器的用途？

A：當發生網路異常時，您可透過耦合器初步判斷網路異常狀態屬於線路本身的問題，或資安防護閘道器的問題。可依下列步驟初步判斷問題原因：

1. 請將資安防護閘道器 WAN 端連接孔的網路線移除，並將移除下來的網路線接頭連接至耦合器一端。
2. 請將資安防護閘道器 LAN 端連接孔的網路線移除，並將移除下來的網路線接頭連接至耦合器的另一端。
3. 若網路恢復正常，請撥打 SOC 電話（02-2344-3693）處理設備問題。
4. 若網路仍未恢復正常，請聯繫中華電信客服（0800-080-365）處理網路問題。



圖、介接耦合機說明