

CMS-2000

使 用 手 冊

目 錄

快速安裝.....	5
硬體安裝	6
軟體安裝	8
S.1 系統功能概述表	14
本機.....	19
系統管理.....	20
第 1 章 管理	21
1.1 管理員.....	23
1.2 管理位址.....	25
1.3 系統登出.....	26
1.4 軟體更新.....	28
第 2 章 組態	29
2.1 介面位址.....	34
2.2 系統設定.....	35
2.3 時間設定.....	41
2.4 SNMP.....	42
2.5 語言版本.....	44
第 3 章 系統監控報告	45
3.1 系統效能.....	47
3.2 事件記錄.....	48
裝置管理.....	49
第 4 章 裝置管理	50
4.1 裝置管理功能使用範例.....	53
裝置監控備份	60
第 5 章 郵件安全報告	61
5.1 統計.....	75
5.2 日誌.....	76
第 6 章 郵件歸檔報告	77
6.1 統計.....	91
6.2 歸檔.....	92
第 7 章 網站管制報告	93

7.1 統計.....	108
7.2 日誌.....	109
第 8 章 入侵防禦報告	110
8.1 統計.....	119
8.2 日誌.....	120
第 9 章 網頁應用程式報告	121
9.1 統計.....	130
9.2 日誌.....	131
第 10 章 監控記錄	132
10.1 封包記錄.....	150
10.2 事件記錄.....	152
10.3 連線記錄.....	154
10.4 病毒過濾記錄.....	155
10.5 應用程式管制記錄.....	156
10.6 連線數限制記錄.....	157
10.7 傳輸量限制記錄.....	158
遠端.....	159
管制條例選項	160
第 11 章 位址表.....	161
11.1 位址表功能使用範例.....	164
第 12 章 服務表	168
12.1 服務表功能使用範例.....	171
第 13 章 排程表	175
13.1 排程表功能使用範例.....	177
第 14 章 頻寬表	182
14.1 頻寬表功能使用範例.....	184
第 15 章 認證表	189
15.1 認證帳戶和群組功能使用範例.....	191
第 16 章 應用程式管制	195
16.1 應用程式管制功能使用範例.....	198
第 17 章 虛擬伺服器	202
17.1 虛擬伺服器功能使用範例.....	205
第 18 章 VPN	208
18.1 VPN功能使用範例.....	215
郵件安全.....	227

第 19 章 郵件安全	228
19.1 郵件安全功能使用範例.....	231
郵件 歸檔 / 稽核	240
第 20 章 郵件 歸檔 / 稽核	241
20.1 稽核.....	243
網站管制.....	252
第 21 章 網站管制	253
21.1 網站管制功能使用範例.....	257
入侵偵測防禦	264
第 22 章 入侵偵測防禦	265
22.1 入侵偵測防禦功能使用範例.....	271
網頁應用程式防火牆	278
第 23 章 網頁應用程式防火牆	279
23.1 網頁應用程式防火牆功能使用範例.....	284
SSL Web VPN.....	291
第 24 章 SSL Web VPN.....	292
24.1 SSL Web VPN功能使用範例.....	294
管制條例.....	298
第 25 章 管制條例	299
25.1 管制條例功能使用範例.....	306
即時監控.....	313
第 26 章 監控記錄	314
26.1 封包記錄.....	330
26.2 事件記錄.....	332
26.3 連線記錄.....	334
26.4 病毒過濾記錄.....	336
26.5 應用程式管制記錄.....	337
26.6 連線數限制記錄.....	338
26.7 傳輸量限制記錄.....	339
第 27 章 流量排行	340
27.1 即時流量分析.....	348
27.2 今日排行榜.....	349

27.3 歷史排行榜.....	354
第 28 章 流量圖表	355
28.1 外部網路.....	357
28.2 管制條例.....	359
第 29 章 系統狀態	361
29.1 介面狀態.....	366
29.2 系統效能.....	368
29.3 認證狀態.....	369
29.4 ARP表	370
29.5 連線狀態.....	371
29.6 DHCP用戶表	373
29.7 主機資訊.....	374

快速安裝

硬體安裝

H.1 CMS-2000 硬體外部介面說明：(如圖 H-1)

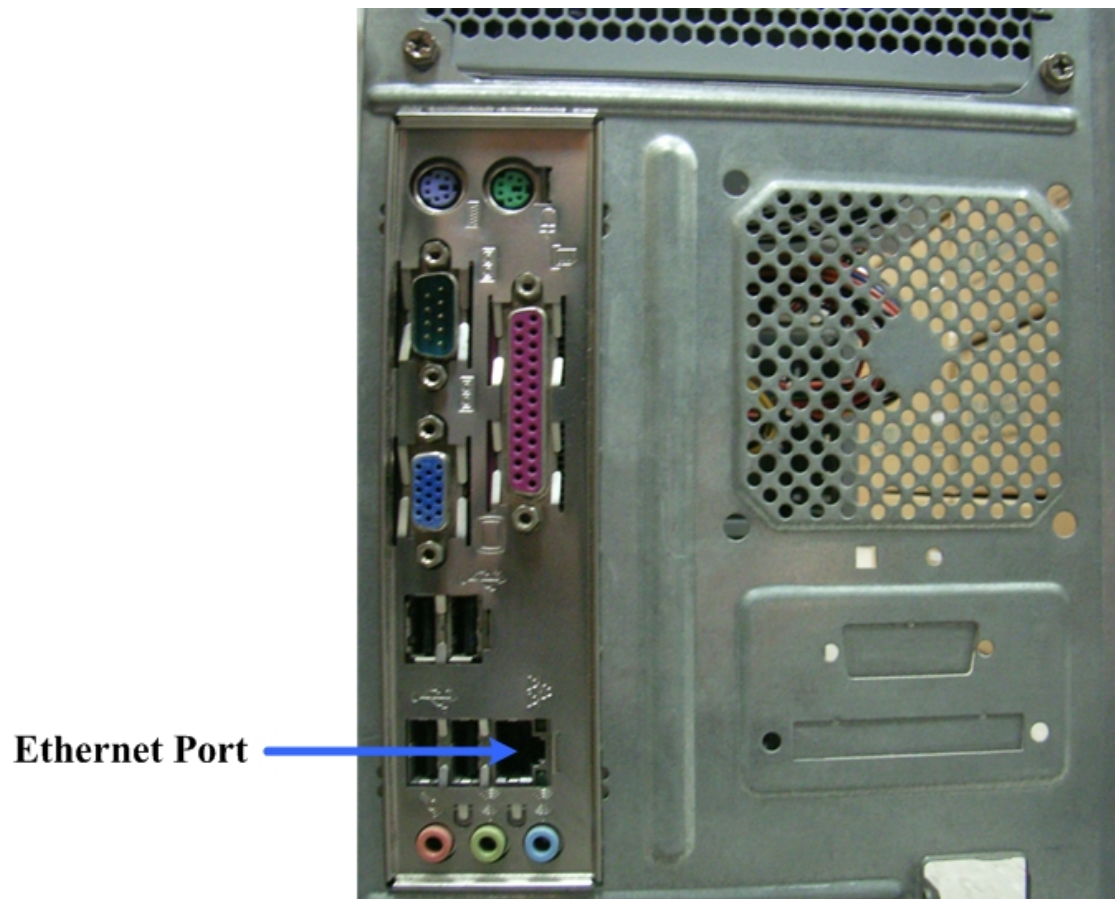


圖 H-1 CMS-2000 介面說明

- **Ethernet Port**：用來連線網路中的 UTM、MHG 設備，讓管理人員集中檢視相關運作報表和統管其設定資料。

H.2 CMS-2000 配置方法：(如圖 H-2)

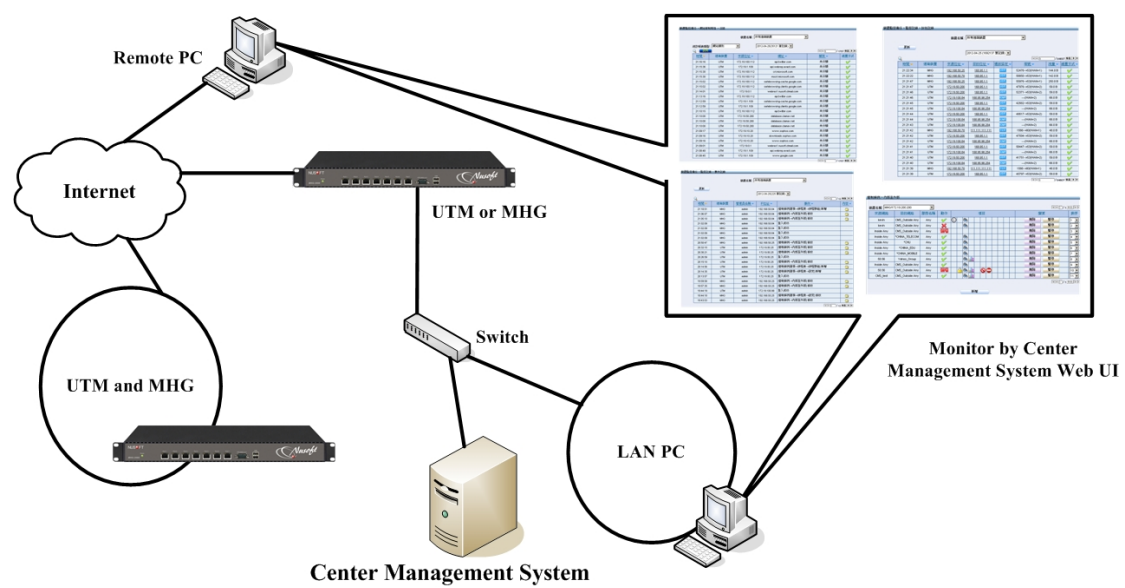


圖 H-2CMS-2000 配置圖

軟體安裝

- 步驟1. 將安裝網路卡或內建 Ethernet Port 的電腦，設定以光碟開機。
- 步驟2. 置入 CMS-2000 系統安裝光碟片，並按照顯示的指示安裝系統：
- 於開機選單選擇 First install，並按下 Enter。(如圖 S-1)
 - 於硬碟列表選擇和確認指定編號裝置，並按下 Enter。(如圖 S-2)
 - 重新格式化選定的硬碟(會清除所有資料)，然後完成系統安裝。(如圖 S-3)
 - 退出光碟片並按下任一鍵(例如：Enter)重開電腦，以正式運作 CMS-2000 系統。(如圖 S-4)

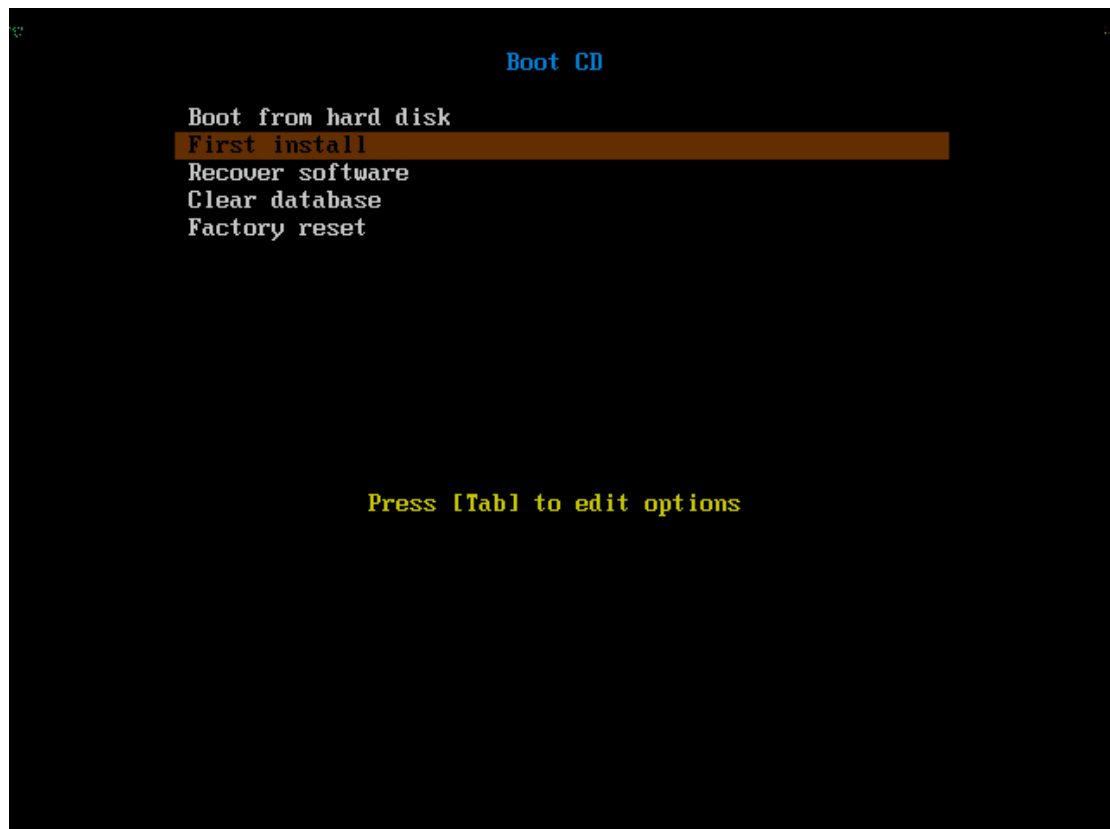


圖 S-1 選擇指定開機項目


```
#####
#                                     #
#               First install         #
#                                     #
#####

+-----+
| No.      name          size(bytes) |
+-----+
|  1       /dev/sda      30G         |
+-----+

Please select HD device No.: (1..1)1
[ Device /dev/sda selected ]

Are you sure you want to do? (y/N)y_
```

圖 S-2 選擇指定硬碟

```
Model: VMware, VMware Virtual S (scsi)
Disk /dev/sda: 32.2GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos

Number  Start   End     Size    Type    File system  Flags
  1      512B    10.0MB  10000kB primary ext2
  2      10.0MB 1034MB  1024MB  primary ext2
  3      1034MB 2058MB  1024MB  primary ext2
  4      2058MB 32.2GB  30.2GB  extended lba
  5      2058MB 2314MB  256MB   logical ext2
  6      2314MB 2442MB  128MB   logical ext2
  7      2442MB 5514MB  3072MB  logical linux-swap(v1)
  8      5514MB 26.0GB  20.5GB  logical ext3
  9      26.0GB 32.2GB  6216MB  logical ext3

=====
Formatting ext2 partition /dev/sda1....done
Formatting ext2 partition /dev/sda2....done
Formatting ext2 partition /dev/sda3....done
Formatting ext2 partition /dev/sda5....done
Formatting ext2 partition /dev/sda6....done
Making linux-swap partition /dev/sda7....done
Formatting ext3 partition /dev/sda8....done
Formatting ext3 partition /dev/sda9....done
Install firmware success!!!

Please remove CD-ROM disc and press any key to reboot your system!
```

圖 S-3 進行硬碟格式化和系統安裝作業


```
E ==> set_wf_whitelist():1009, use:0 sec
S ==> set_wf_blacklist():1018
E ==> set_wf_blacklist():1034, use:0 sec
S ==> set_wf_extension():1043
E ==> set_wf_extension():1061, use:0 sec
S ==> set_wf_mime_script():1070
E ==> set_wf_mime_script():1088, use:0 sec
S ==> set_wf_category():1097
E ==> set_wf_category():1114, use:0 sec
S ==> set_wf_group():1123
E ==> set_wf_group():1141, use:0 sec
S ==> set_wf_report():1149
E ==> set_wf_report():1162, use:0 sec
S ==> set_idp():893
E ==> set_idp():918, use:0 sec
S ==> set_idp_report():926
E ==> set_idp_report():938, use:0 sec
S ==> set_waf():943
E ==> set_waf():964, use:0 sec
S ==> set_waf_report():972
E ==> set_waf_report():984, use:0 sec
S ==> set_policy():1200
E ==> set_policy():1235, use:0 sec
S ==> set_report_setting():1243
E ==> set_report_setting():1265, use:0 sec
S ==> set_report_setting():1243
E ==> set_report_setting():1265, use:0 sec
##### Initial System [ End ] #####
INIT: Entering runlevel: 1
```

圖 S-4 CMS-2000 開機完成

- 步驟3. 將系統管理員的電腦和 CMS-2000 接到同一個 HUB 或 Switch，再使用瀏覽器（IE、Firefox、Chrome、...）連結至 CMS-2000。CMS-2000 的管理界面 IP 位址內定值為 http://192.168.1.1。
- 步驟4. 於彈跳出來的登入驗證視窗，輸入使用者名稱與密碼（預設皆為 admin）。（如圖 S-5）



圖 S-5 輸入使用者名稱與密碼



注意：

1. 務必調整 CMS-2000 主機 BIOS 的電源管理設定（POWER MANAGEMENT SETUP），將停電後再來電時的狀態（PWRON AFTER PW-FAIL）設定為開機（ON）或回到斷電之前的狀態（FORMER-STS），讓 CMS-2000 過電自動開機，避免系統停擺。
-

- 步驟5. 登入 CMS-2000 後，顯示的系統管理介面，分為兩部份：(如圖 S-6)
- 索引區：用來選擇欲操作的功能項目。(可參照 系統功能概述表)
 - 操作區：用來具體完成或顯示各項功能的設定、資訊。

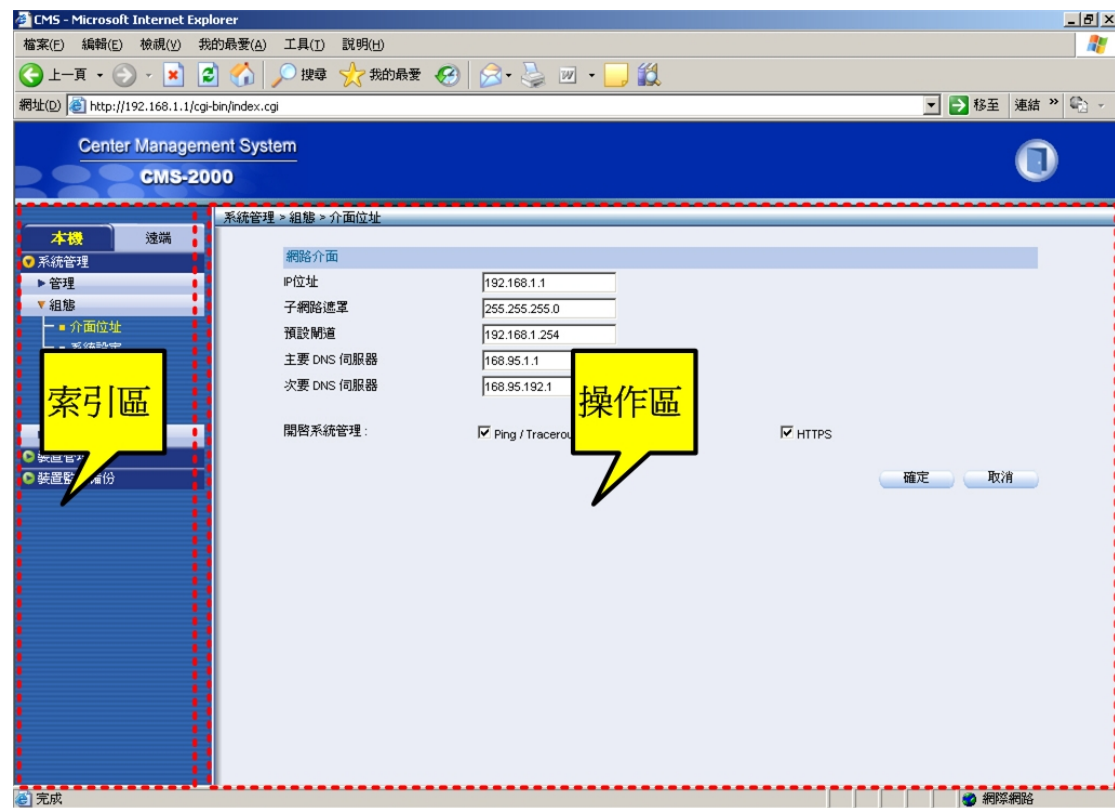


圖 S-6 CMS-2000 的系統管理介面

步驟6. 在【本機】>【系統管理】>【組態】>【介面位址】頁面中，設定網路介面位址（配合實際的網路環境做調整），如果更改後的網路介面位址不屬於系統預設網段 192.168.1.x/24，例如：網路介面位址改為 172.16.0.1（子網路遮罩 255.255.255.0），管理員必須設定電腦採用同網段且尚未被使用的 IP 位址。（如圖 S-7）

- 輸入指定的【IP 位址】、【子網路遮罩】、【預設閘道】、【主要 DNS 伺服器】、【次要 DNS 伺服器】。

圖 S-7 網路介面位址設定頁面



注意：

1. 如果更改了網路介面位址，要於瀏覽器之網址欄輸入更改後的網路介面位址，才能再登入 CMS-2000 之 Web UI。

步驟7. 在【本機】>【系統管理】>【組態】>【時間設定】頁面中，開啓與外部時間伺服器同步機制（同步的時差請依所在時區自行調整），以提供系統正確的運作時間。（如圖 S-8）

圖 S-8 系統時間設定

S.1 系統功能概述表

功能模組	功能項目		功能簡介	參照章節
本機				
系統管理	管理	管理員	用於設定管理系統的帳號。	第 1 章
		管理位址	用於指定管理 PC 的 IP 位址，僅允許特定 IP 位址登入系統。	
		軟體更新	用於更新系統的軟體版本。	
	組態	介面位址	用於設定系統網路介面的 IP 位址、子網路遮罩、預設閘道、域名解析 DNS 伺服器。	第 2 章
		系統設定	用於匯入/匯出系統設定檔、恢復出廠設定、格式化內建硬碟、開啓電子郵件警訊通知、進行管理介面連線(登入)設定、進行中央控管連線設定、設定系統各報表每頁的資料顯示筆數及重啓系統等。	
		時間設定	用於校正系統時間。	
		SNMP	用於即時取得系統的運作資訊。	
		語言版本	用於切換管理介面的語言版本，包括：繁體中文、簡體中文和英文。	
	系統監控 報告	系統效能	顯示系統運作所消耗的硬體資源。	第 3 章
		事件記錄	用於查看系統事件記錄。	
裝置管理	裝置		用於針對連線的 UTM、MHG 設備進行運作狀態檢視、設定檔備份、恢復出廠預設值等作業。	第 4 章
	群組		將連線的 UTM、MHG 設備分類、群組。	
	組態/軟體備份		用於管理匯入、備份的 UTM、MHG 設定檔和軟體。	
	組態/軟體更新		用於上傳系統匯入、備份的 UTM、MHG 設定檔或軟體到指定設備。	
裝置監控 備份	郵件安全 報告	設定	即時接收遠端 UTM 掃描郵件的結果，可以繪製成圖形化的統計報表，定時以電子郵件發送此統計報表給指定收件者；並可將其彙整成條列式的	第 5 章
		統計		
		日誌		

			文字報表。	
	郵件歸檔 報告	設定	即時接收遠端 UTM 郵件安全過濾後	第 6 章
		統計	審核、存檔信件的结果，可以繪製成	
		歸檔	圖形化的統計報表，定時以電子郵件 發送此統計報表給指定收件者；並可 將其彙整成條列式的文字報表。	
	網站管制 報告	設定	即時接收遠端 UTM、MHG 處理符合	第 7 章
		統計	網站管制特徵、規則行為的结果，可	
		日誌	以繪製成圖形化的統計報表，定時以 電子郵件發送此統計報表給指定收件 者；並可將其彙整成條列式的文字報 表。	
	入侵防禦 報告	設定	即時接收遠端 UTM 處理符合入侵特	第 8 章
		統計	徵行為的结果，可以繪製成圖形化的	
		日誌	統計報表，定時以電子郵件發送此統 計報表給指定收件者；並可將其彙整 成條列式的文字報表。	
	網頁應用 程式報告	設定	即時接收遠端 UTM 處理符合網頁應	第 9 章
		統計	用程式攻擊特徵行為的结果，可以繪	
		日誌	製成圖形化的統計報表，定時以電子 郵件發送此統計報表給指定收件者； 並可將其彙整成條列式的文字報表。	
	監控記錄	設定	用於設定封包、事件、連線、病毒過 濾、應用程式管制、連線數限制、傳 輸量限制...監控記錄的保存期限。	第 10 章
		封包記錄	即時接收遠端 UTM、MHG 流量封包 資訊。	
		事件記錄	即時接收遠端 UTM、MHG 系統事件 資訊。	
		連線記錄	即時接收遠端 UTM、MHG 系統連線 資訊。	
		病毒過濾記 錄	即時接收遠端 UTM 管制條例病毒過 濾資訊。	
		應用程式管 制記錄	即時接收遠端 UTM、MHG 管制條例 應用程式管制資訊。	
		連線數限制 記錄	即時接收遠端 UTM、MHG 管制條例 連線控管資訊。	
		傳輸量限制	即時接收遠端 UTM、MHG 管制條例	

		記錄	傳輸量控管資訊。	
遠端				
管制條例 選項	位址表	內部網路	設定適用於遠端 UTM、MHG 的內部網路、外部網路和非軍事區網路 IP 位址分類、群組。	第 11 章
		內部網路群組		
		外部網路		
		外部網路群組		
		非軍事區網路		
		非軍事區群組		
	服務表	基本服務	設定適用於遠端 UTM、MHG 的網路服務項目、群組。	第 12 章
		自訂服務		
		服務群組		
	排程表	設定	規劃適用於遠端 UTM、MHG 的網路使用排程。	第 13 章
		排程群組		
	頻寬表	設定	規劃適用於遠端 UTM、MHG 的外部網路頻寬分配設定。	第 14 章
	認證表	認證帳戶	建立適用於遠端 UTM、MHG 的上網授權驗證帳戶。	第 15 章
		認證群組		
	應用程式 管制	設定	設定適用於遠端 UTM、MHG 的即時通訊軟體、點對點軟體、影音軟體、網頁郵件、線上遊戲、通道軟體、遠端控制軟體管制規則。	第 16 章
	虛擬伺服器	IP 對應	建立適用於遠端 UTM、MHG 的內部主機對外服務 IP、連接埠設定。	第 17 章
		連接埠對應		
		連接埠對應群組		
	VPN	VPN 精靈	建立適用於遠端 UTM、MHG 的兩端點內網互連、固定電腦和特定端點內網互連之安全網路連線。	第 18 章
		IPSec 自動加密		
		PPTP 伺服器		
		PPTP 用戶端		
		Trunk		
		Trunk 群組		
郵件安全	全體化規則		設定適用於遠端 UTM 的垃圾郵件過	第 19 章

	郵件白名單		濾規則，會依序以全體化規則 > 郵件白名單 > 郵件黑名單機制掃描郵件。	
	郵件黑名單			
郵件歸檔 /稽核	稽核		設定適用於遠端 UTM 的正常郵件審核、存檔規則。	第 20 章
網站管制	網站白名單		設定適用於遠端 UTM、MHG 的 HTTP 特定網址、HTTP 特定網頁 MIME 資料/Script、FTP/HTTP 特定副檔名檔案存取管制規則。	第 21 章
	網站黑名單			
	網站類別資料庫			
	檔案傳輸管制			
	MIME/Script 管制			
	網站管制群組			
入侵偵測 防禦	異常偵測		設定適用於遠端 UTM 的異常、入侵行為偵測、管理規則。	第 22 章
	預設特徵			
	自定特徵			
網頁應用 程式防火 牆	預設特徵		設定適用於遠端 UTM 的網頁應用程式攻擊行為偵測、管理規則。	第 23 章
	自訂特徵			
SSL Web VPN	設定		設定適用於遠端 UTM、MHG 的 SSL Web VPN 連線認證規則。	第 24 章
管制條例	內部至外部		利用位址表、服務表、排程表、頻寬表、認證表、應用程式管制、虛擬伺服器、VPN、郵件過濾/歸檔/稽核、網站管制、入侵偵測防禦、網頁應用程式防火牆、SSL Web VPN 或 IM 側錄等管制項目，制定適用於遠端 UTM、MHG 內部網路、外部網路和非軍事區網路存取網路資源的權限。	第 25 章
	外部至內部			
	外部至非軍事區			
	內部至非軍事區			
	非軍事區至外部			
	非軍事區至內部			
	內部至內部			
	非軍事區至非軍事區			
即時監控	監控記錄	封包記錄	直接瀏覽遠端 UTM、MHG 儲存的流量封包資訊。	第 26 章
		事件記錄	直接瀏覽遠端 UTM、MHG 儲存的系統事件資訊。	
		連線記錄	直接瀏覽遠端 UTM、MHG 儲存的系統連線資訊。	
		病毒過濾記錄	直接瀏覽遠端 UTM 儲存的管制條例病毒過濾資訊。	
		應用程式管制記錄	直接瀏覽遠端 UTM、MHG 儲存的管制條例應用程式管制資訊。	
		連線數限制	直接瀏覽遠端 UTM、MHG 儲存的管	

		記錄	制條例連線控管資訊。	
		傳輸量限制 記錄	直接瀏覽遠端 UTM、MHG 儲存的管制條例傳輸量控管資訊。	
	流量排行	即時流量分析	直接瀏覽遠端 UTM、MHG 儲存的使用者存取網站、服務、流量資訊。	第 27 章
		今日排行榜		
		歷史排行榜		
	流量圖表	外部網路	直接顯示遠端 UTM、MHG 對外線路頻寬的使用量。	第 28 章
		管制條例	直接顯示遠端 UTM、MHG 特定管制條例頻寬的使用量。	
	系統狀態	介面狀態	直接顯示目前遠端 UTM、MHG 網路介面的設定和運作狀態。	第 29 章
		系統效能	直接顯示遠端 UTM、MHG 運作所消耗的硬體資源。	
		認證狀態	直接顯示目前遠端 UTM、MHG 透過認證授權上網的使用者清單。	
		ARP 表	直接顯示目前透過遠端 UTM、MHG 存取網路資源的 IP 和 MAC 對應資訊。	
		連線狀態	直接顯示目前遠端 UTM、MHG 內部電腦透過管制條例存取網路資源使用的連線數。	
		DHCP 用戶表	直接顯示目前透過遠端 UTM、MHG DHCP 機制取得 IP 的使用者清單。	
		主機資訊	直接顯示目前通過遠端 UTM、MHG 連線的 IP 和其對應 NetBIOS、DNS 名稱資訊。	

本機

系統管理

第1章 管理

所謂的系統管理，是指 CMS-2000 的管理員權限、管理位址、系統登出與軟體更新等設定與管理。

CMS-2000 預設之主管理員可變更系統各項設定、監控系統運作狀態及瀏覽系統各項報表內容；具有寫入、瀏覽權限的次管理員能進行和主管理員一樣的作業；不具寫入、瀏覽權限的次管理員僅能讀取系統各項設定資料，不能予以更改。

【管理員】功能概述：

管理員名稱 說明如下：

- 登入系統的驗證名稱。
- 系統預設主管理員的名稱和密碼為 **admin**，不可被刪除。

權限 說明如下：

- 主管理員有【讀/寫/瀏覽】權限。亦即具有更改系統設定、瀏覽系統報表內容、管理系統登入帳號等權限。
- 次管理員可給予唯【讀】或【讀/瀏覽】權限。亦即除了只能瀏覽系統設定外，有時也具有瀏覽系統報表內容等權限。

密碼/新密碼/確認密碼 說明如下：

- 輸入新增或修改主/次管理員之密碼。

1.1 管理員

1.1.1 新增次管理員

步驟1. 在【本機】>【系統管理】>【管理】>【管理員】頁面中，做下列設定：
(如圖 1-1)

- 按下【新增次管理員】鈕。
- 輸入指定的【次管理員名稱】、【密碼】。
- 【確認密碼】輸入和【密碼】相同的字串。
- 按下【確定】鈕，完成設定。

新增次管理員	
次管理員名稱：	<input type="text" value="sub_admin"/> (最多 30 個字元)
密碼：	<input type="password" value="*****"/> (最多 20 個字元)
確認密碼：	<input type="password" value="*****"/> (最多 20 個字元)
權限：	<input type="checkbox"/> 寫入權限 <input checked="" type="checkbox"/> 瀏覽記錄/報告權限
<div>確定 取消</div>	

圖 1-1 新增次管理員



說明：

1. 若勾選【寫入權限】和【瀏覽記錄/報告權限】，則新增之管理員為主管理員。若僅勾選【瀏覽記錄/報告權限】或不勾選此二選項，則為次管理員。

1.1.2 修改管理員密碼

步驟1. 在【本機】>【系統管理】>【管理】>【管理員】頁面中，做下列設定：
(如圖 1-2)

- 針對指定的管理員，按下【修改】鈕。
- 輸入原本的【密碼】、要置換的【新密碼】。
- 【確認密碼】輸入和【新密碼】相同的字串。
- 按下【確定】鈕，完成設定。

修改管理員密碼	
管理員名稱：	admin
密碼：	<input type="password"/> (最多 20 個字元)
新密碼：	<input type="password"/> (最多 20 個字元)
確認密碼：	<input type="password"/> (最多 20 個字元)
權限：	<input checked="" type="checkbox"/> 寫入權限 <input checked="" type="checkbox"/> 瀏覽 記錄 報告 權限
<div>確定 取消</div>	

圖 1-2 變更管理員密碼

1.2 管理位址

1.2.1 設定管理位址

步驟1. 在【本機】>【系統管理】>【管理】>【管理位址】頁面中，做下列設定：（如圖 1-3）

- 輸入管理位址【名稱】。
- 輸入允許連線的【IP 位址】。
- 輸入【子網路遮罩】（255.255.255.255 代表 1 個 IP）。
- 【開啓系統管理】勾選 Ping/Traceroute、HTTP 和 HTTPS。
- 按下【確定】鈕，完成設定。



新增管理位址

名稱：	<input type="text" value="master"/>	(最多 20 個字元)
IP位址：	<input type="text" value="163.173.56.11"/>	
子網路遮罩：	<input type="text" value="255.255.255.255"/>	
開啓系統管理：	<input checked="" type="checkbox"/> Ping / Traceroute	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS

確定 取消

圖 1-3 管理位址設定頁面



注意：

1. 管理位址若要有實際的作用，必須將 CMS-2000 網路介面的【Ping/Traceroute】、【HTTP】、與【HTTPS】功能全數關閉。
 2. 在關閉網路介面的【HTTP】與【HTTPS】功能之前，務必要設定管理位址。否則，將會發生無法透過指定介面登入系統的窘境。
-

1.3 系統登出

1.3.1 登出CMS-2000 管理介面

步驟1. 按下管理介面右上角之【系統登出】鈕，可使系統管理員隨時登出系統管理介面，避免他人更動或毀壞 CMS-2000 之設定。(如圖 1-4, 圖 1-5)

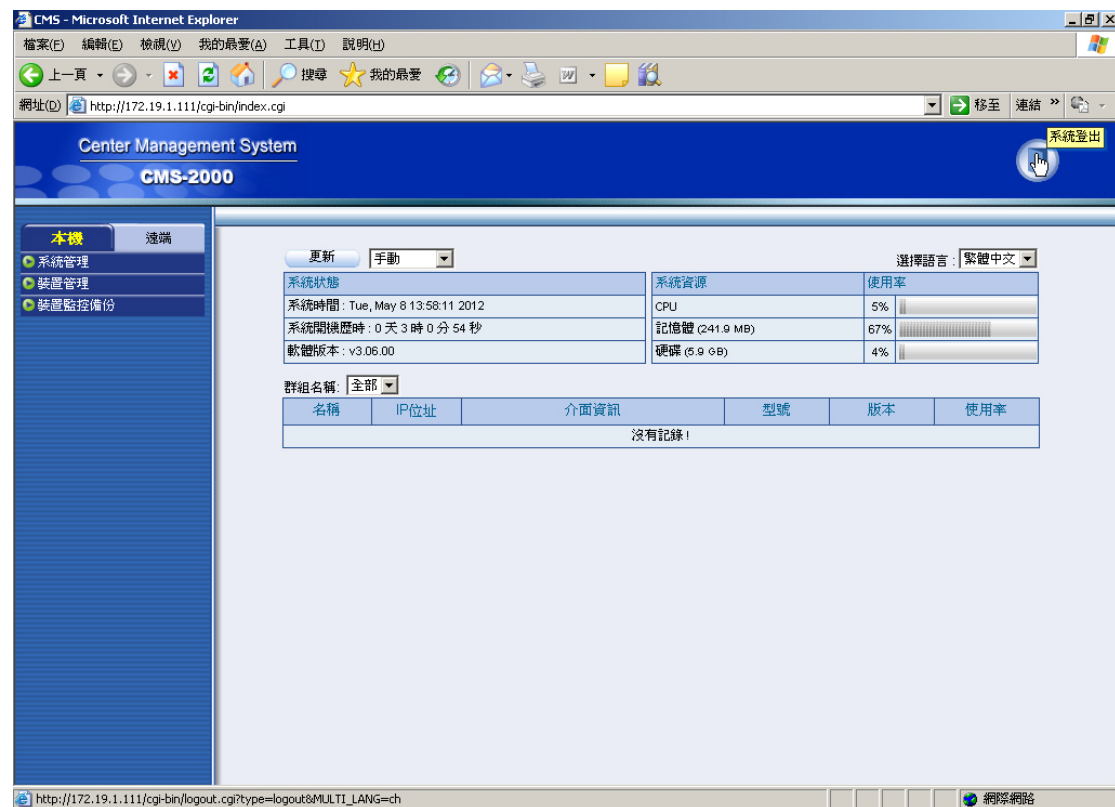


圖 1-4 登出 CMS-2000



圖 1-5 登出 CMS-2000 確認視窗

步驟2. 按下【確定】鈕，會於瀏覽器顯示登出訊息。(如圖 1-6)



圖 1-6 CMS-2000 登出訊息

1.4 軟體更新

步驟1. 在【本機】>【系統管理】>【管理】>【軟體更新】頁面中，可依下列步驟更新軟體：(如圖 1-7)

- 按下【瀏覽】鈕，選擇已下載的軟體檔案。
- 按下【確定】鈕，進行軟體更新。

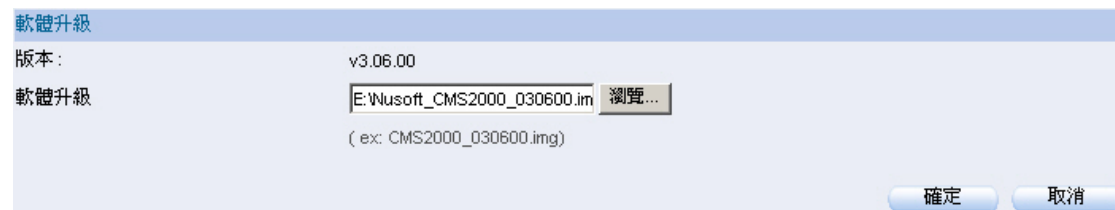


圖 1-7 更新 CMS-2000 軟體



注意：

1. 軟體更新需 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，切勿關機、斷線或是離開更新網頁，這可能會造成 CMS-2000 不可預期之錯誤。(強力建議於內部網路來更新軟體，以避免不必要的錯誤)
-

第2章 組態

所謂的系統組態，是指 CMS-2000 的介面位址、系統設定、時間設定、SNMP 和語言版本等設定。

【介面位址】功能概述：

網路介面 說明如下：

- 系統管理員可在此設定 CMS-2000 的管理介面 IP。

【系統設定】功能概述：

系統組態 說明如下：

- 系統管理員可在此匯入或匯出系統設定檔，也可在此將系統恢復至出廠設定值。

備份 / 還原系統組態檔 說明如下：

- 用來將系統設定檔複製到系統內建的指定存放空間，讓管理人員可依備份日期還原該時間點的設定；亦可避免因系統設定缺損，本地端電腦遺失設定檔而無法還原的情形。
- 系統於每日 0:00 會自動進行此設定檔備份作業，管理人員亦可手動進行即時備份作業。
- 已備份的設定檔亦可匯出至本地端電腦儲存。

格式化內建硬碟 說明如下：

- 系統管理員可在此格式化 CMS-2000 內建硬碟。

系統名稱設定 說明如下：

- 系統管理員可在此設定 CMS-2000 名稱、隸屬單位名稱和所在地址。

電子郵件警告 / 報告設定 說明如下：

- 開啓此功能後，CMS-2000 可自動以電子郵件寄送警訊通知、系統運作報告給指定收件者。

資料儲存期限設定 說明如下：

- 系統管理員可在此設定 CMS-2000 的系統效能和事件日誌保存期限。

系統管理介面登入設定 說明如下：

- 系統管理員可在任何地方以 WebUI 遠端管理 CMS-2000，並可在此變更登入 CMS-2000 所使用的埠號。

- 可在此設定系統管理員透過 WebUI 管理 CMS-2000 的閒置時間，若在登入 CMS-2000 後，持續未有管理或監控動作，當超過設定的閒置時間時，CMS-2000 會強制登出 WebUI。
- 當登入系統時輸入的驗證資料，達限定的錯誤次數；該登入系統的來源位址，於指定時間內可被阻擋。避免有心人士嘗試登入系統，竄改設定以瓦解系統運作。



注意：

1. 當 HTTP 或 HTTPS 埠號變更後，系統管理員透過瀏覽器登入 WebUI 時，要輸入相映之埠號。（如：http://172.16.1.254:8080 和 https://172.16.1.254:1025）
-

中央控管連線設定 說明如下：

- 設定讓網路中 UTM、MHG 設備連線的介面，以集中記錄相關運作報表、統管其設定資料。

系統表單顯示設定 說明如下：

- 可設定規則表（管制條例、位址表、服務表、...）、記錄清單（郵件安全日誌、網頁應用程式日誌、...）每頁的資料顯示量。

【時間設定】功能概述：

同步系統時間 說明如下：

- 可將 CMS-2000 的系統時間與系統管理員之電腦或是外部時間伺服器的時間同步化。

GMT 說明如下：

- 國際標準時間（格林威治標準時間）。

日光節約時間 說明如下：

- 啟用此功能，可調整系統時間和使用所在地實施的夏令時間之時差。日光節約時間又稱夏令時間，是將原本的標準時間撥快一個小時，分與秒不變，恢復時再撥慢一個小時。作用在於令民眾能早一個小時起床，達到早睡早起、節約能源的目的。

【SNMP】功能概述：

SNMPv3 說明如下：

- SNMP 是專門用於管理網路節點（伺服器、工作站、路由器、交換機...）的協定。網路管理員透過 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 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：
 - ◆ 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。
 - ◆ SNMPv2：改進第一版的許多安全缺陷，但執速度能不如第一版快，且無法和其相容，因此不被廣泛接受。
 - ◆ SNMPv3：修正了前兩版的問題，不僅會對所有傳輸資料進行加密，而且可使 SNMP 代理程式對管理系統做認證動作，並確保數位簽章訊息的完整性。另外，針對每項訊息還會有存取清單的限制。

安全模式 說明如下：

- SNMPv3 規定了三個認證和隱私模式：
 - ◆ 無隱私模式，即 NoAuthNoPriv。類似 SNMPv1 的明碼字串，適用於 SNMP 網路實體處於一個可信賴的環境中時。
 - ◆ 無隱私認證模式，即 AuthNoPriv。
 - ◆ AuthPriv 模式。它不僅要進行認證，而且要對 SNMP 資料進行加密。

帳戶名稱 說明如下：

- 管理系統在取得 CMS-2000 的運作資訊時，所要輸入的認證名稱。

認證協定 說明如下：

- 支援 HMAC_MD5_96、HMAC_SHA_96 認證協定。

認證密碼 說明如下：

- 管理系統在取得 CMS-2000 的運作資訊時，所要輸入的認證密碼。

加密協定 說明如下：

- 支援資料加密標準（Data Encryption Standard），是一種 NIST 標準安全加密金鑰方法，使用的加密金鑰為 56 位元。

加密码 说明如下：

- 管理系统以加密方式取得 CMS-2000 的运作资讯时，所要输入的密码。

2.1 介面位址

2.1.1 設定介面位址

步驟1. 在【本機】>【系統管理】>【組態】>【介面位址】頁面中，做下列設定：（如圖 2-1）

- 輸入指定的【IP 位址】、【子網路遮罩】、【預設閘道】、【主要 DNS 伺服器】、【次要 DNS 伺服器】。
- 按下【確定】鈕，完成設定。

網路介面	
IP位址	172.19.1.111
子網路遮罩	255.255.0.0
預設閘道	172.19.1.254
主要 DNS 伺服器	168.95.1.1
次要 DNS 伺服器	168.95.192.1
開啓系統管理：	<input checked="" type="checkbox"/> Ping / Traceroute <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 2-1CMS-2000 網路介面設定頁面

2.2 系統設定

2.2.1 下載CMS-2000 系統設定檔

步驟1. 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，做下列設定：（如圖 2-2）

- 在【系統組態】設定欄位中，按下【匯出系統組態檔至用戶端】右方的 **匯出** 鈕。
- 在【檔案下載】視窗中，按下【儲存】鈕，接著指定匯出檔案所要儲存的目的位置，再按下【儲存】鈕。CMS-2000 設定檔即會複製至指定儲存位置。



圖 2-2 匯出系統組態檔

2.2.2 匯入設定檔到CMS-2000

步驟1. 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，做下列設定：(如圖 2-3)

- 在【系統組態】設定欄位中，按下【從用戶端匯入系統組態檔】右方的【瀏覽】鈕。
- 在【選擇檔案】視窗中，【開啓】儲存在電腦的 CMS-2000 設定檔。
- 按下【確定】鈕。
- 在確認視窗中，【確定】將設定檔案匯入 CMS-2000。(如圖 2-4)

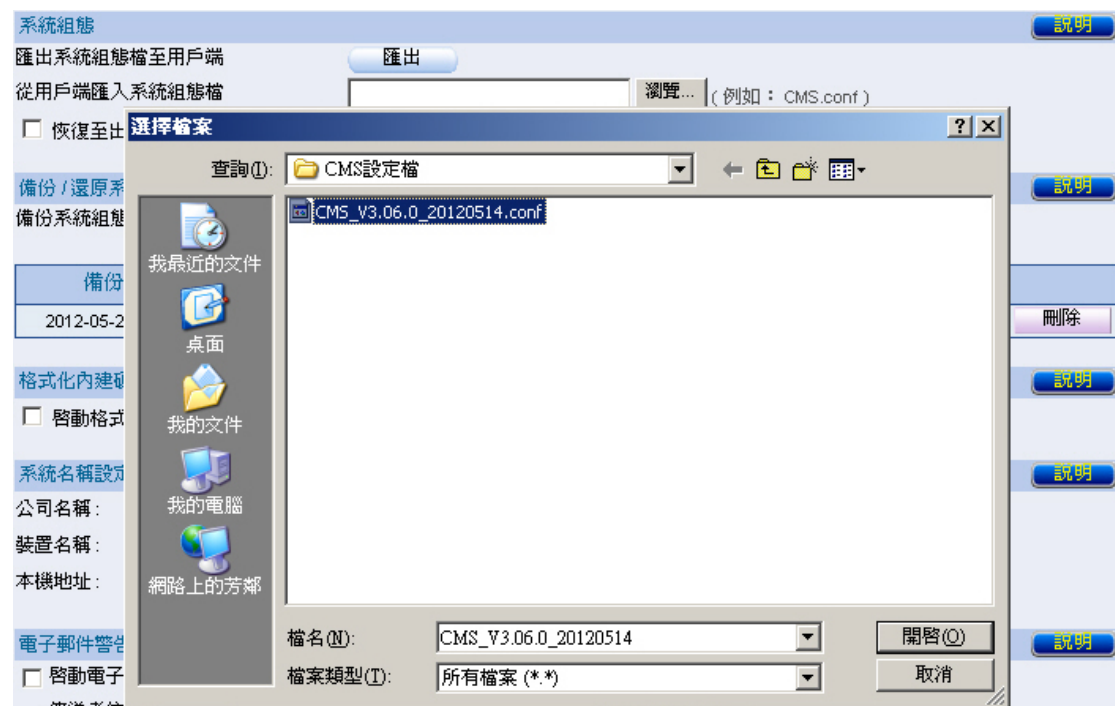


圖 2-3 匯入檔案所在目錄位置與檔名



圖 2-4 匯入設定檔確認視窗

2.2.3 將CMS-2000 恢復為出廠設定值並格式化硬碟

步驟1. 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，做下列設定：（如圖 2-5）

- 在【系統組態】設定欄位中，勾選【恢復至出廠設定值】。
- 在【格式化內建硬碟】設定欄位中，勾選【啟動格式化內建硬碟功能】。
- 按下【確定】鈕。
- 在確認視窗中，【確定】恢復 CMS-2000 為出廠時的原始設定值，並同時格式化硬碟。（如圖 2-6）

系統組態 說明

匯出系統組態檔至用戶端 匯出

從用戶端匯入系統組態檔 瀏覽... (例如: CMS.conf)

☒ 恢復至出廠設定值

備份 / 還原系統組態檔 (備份空間資訊: 已使用容量: 357KB, 剩餘可使用容量: 9MB, 總容量: 10MB) 說明

備份系統組態檔 備份目前系統組態檔

備份時間	備份檔案名稱	變更
2012-05-22 17:22:42	CMS_V3.06.0_1337707358.conf	下載 還原 刪除

格式化內建硬碟 說明

☒ 啟動格式化內建硬碟功能

圖 2-5 恢復至出廠設定值和格式化內建硬碟



圖 2-6 恢復出廠設定值確認視窗

2.2.4 設定電子郵件通知

步驟1. 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，做下列設定：（如圖 2-7）

- 在【系統名稱設定】欄位中：
 - ◆ 【公司名稱】輸入 CMS-2000 所隸屬的單位名稱。
 - ◆ 【裝置名稱】輸入 CMS-2000 的名稱。
 - ◆ 【本機地址】輸入 CMS-2000 的所在地址。
- 在【電子郵件警告 / 報告設定】欄位中：
 - ◆ 勾選【啟動電子郵件警告 / 報告】。
 - ◆ 輸入電子郵件通知的【傳送者位址】。
 - ◆ 【郵件 SMTP 伺服器】輸入遞送電子郵件的 SMTP 伺服器位址。
 - ◆ 【電子郵件位址 1】輸入第一筆接受訊息通知的電子郵件位址。
 - ◆ 【電子郵件位址 2】輸入第二筆接受訊息通知的電子郵件位址。
- 按下【確定】鈕，完成設定。

The screenshot displays the 'System Name Setting' (系統名稱設定) and 'Email Notification / Report Setting' (電子郵件警告 / 報告設定) sections of the CMS-2000 configuration interface.

系統名稱設定 (System Name Setting):

- 公司名稱 (Company Name): Nusoft Corporation (最多 20 個字元, 例如: My Company)
- 裝置名稱 (Device Name): CMS (最多 20 個字元, 例如: CMS)
- 本機地址 (Local Address): 3F.-1, No. 880, Zhongzheng Rd., Zh (最多 256 個字元)

電子郵件警告 / 報告設定 (Email Notification / Report Setting):

- ☒ 啟動電子郵件警告 / 報告 (Enable email notification / report)
- 傳送者位址 (Sender Address): root@nusoft.com.tw (最多 80 個字元, 例如: sender@mydomain.com)
- 郵件 SMTP 伺服器 (Mail SMTP Server): nusoft.com.tw (最多 80 個字元, 例如: mydomain.com)
- 電子郵件位址 1 (Email Address 1): steve@nusoft.com.tw (最多 80 個字元, 例如: user1@mydomain.com)
- 電子郵件位址 2 (Email Address 2): jack@nusoft.com.tw (最多 80 個字元, 例如: user2@mydomain.com)
- ☐ SMTP 伺服器需要驗證 (SMTP server requires authentication)
 - 帳戶名稱 (Account Name): (最多 60 個字元)
 - 密碼 (Password): (最多 60 個字元)
- 郵件測試 (Mail Test): 測試 (Test)

圖 2-7 開啓 CMS-2000 發送警告/報告信函功能



說明：

1. 按下【測試】鈕，可測試【電子郵件位址 1】和【電子郵件位址 2】，輸入的電子郵件帳號是否能正確收到警訊。

2. 當設定的【郵件 SMTP 伺服器】需要驗證才能透過其寄信時，就要啟動【SMTP 伺服器需要驗證】功能，並輸入相關的驗證設定。
-

2.2.5 重新啓動CMS-2000

步驟1. 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，做下列設定：(如圖 2-8)

- 在【重新啓動系統】設定欄位中，按下【系統將被重新啓動】右方的【重新啓動】鈕。
- 在確認視窗中，【確定】重新啓動 CMS-2000。(如圖 2-9)



圖 2-8 重新啓動系統



圖 2-9 重新啓動確認視窗

2.3 時間設定

2.3.1 CMS-2000 時間設定

步驟1. 在【本機】>【系統管理】>【組態】>【時間設定】頁面中，做下列設定：（如圖 2-10）

- 設定所在時區和 GMT 的時差。
- 勾選【開啓與外部時間伺服器同步】。
- 輸入【時間伺服器位址】。
- 輸入 CMS-2000 的時間校正頻率。
- 按下【確定】鈕，完成設定。

系統時間: Wed, May 16 15:40:55 2012

設定時區

與GMT相差 小時 [輔助選取](#)

同步系統時間

☒ 開啓與外部時間伺服器同步

☐ 開啓日光節約時間設定，從 / 至 /

時間伺服器位址 [輔助選取](#)

系統時間每 分鐘自動更新 (範圍: 0 ~ 99999, 0: 表示於開機時更新)

系統時間與您的電腦同步

圖 2-10 系統時間設定



說明：

1. 按下【系統時間與您的電腦同步】右方的【同步】鈕，CMS-2000 的系統時間會與目前連線管理的電腦時間同步。
2. 【與 GMT 相差】和【時間伺服器位址】可利用【輔助選取】進行設定。

2.4 SNMP

2.4.1 SNMP Agent設定

步驟1. 在【本機】>【系統管理】>【組態】>【SNMP】頁面的【SNMP Agent 設定】欄位中，做下列設定：（如圖 2-11）

- 輸入指定【裝置名稱】（預設為 CMS）、【裝置所在地】、【群組名稱】（預設為 public）、【聯絡人】、【註解】（預設為 CMS appliance）。
- 按下【確定】鈕，完成設定。
- 系統管理員可利用安裝於管理端電腦的 SNMP Agent 訊息接收軟體，隨時監控 CMS-2000 運作狀況。

SNMP Agent 設定	
裝置名稱：	<input type="text" value="CMS"/> (最多 255 個字元)
裝置所在地：	<input type="text" value="Taipei, Taiwan."/> (最多 255 個字元)
群組名稱：	<input type="text" value="public"/> (最多 255 個字元)
聯絡人：	<input type="text" value="root@public"/> (最多 255 個字元)
註解：	<input type="text" value="CMS appliance"/> (最多 255 個字元)
<input type="checkbox"/> 啟動 SNMPv3	
安全模式：	<input type="text" value="NoAuthNoPriv"/>
帳戶名稱：	<input type="text"/> (最多 20 個字元)
認證協定：	<input type="text" value="HMAC_MD5_96"/>
認證密碼：	<input type="text"/> (最多 15 個字元)
加密協定：	<input type="text" value="DES"/>
加密密碼：	<input type="text"/> (最多 15 個字元)

圖 2-11SNMP Agent 設定

2.4.2 SNMP Trap設定

步驟1. 在【本機】>【系統管理】>【組態】>【SNMP】頁面的【SNMP Trap 設定】欄位中，做下列設定：（如圖 2-12）

- 勾選【開啓 SNMP Trap 警訊通知】。
- 輸入指定【SNMP Trap 訊息接收位址】、【SNMP Trap 埠號】（預設為 UDP Port 162）。
- 按下【確定】鈕，完成設定。
- 系統管理員可利用安裝於管理端電腦之 SNMP Trap 用戶端軟體，隨時接收來自 CMS-2000 的異常警訊。



SNMP Trap 設定

☒ 開啓 SNMP Trap 警訊通知

SNMP Trap 訊息接收位址： (最多 255 個字元)

SNMP Trap 埠號： (範圍: 1 - 65535, 例如: 162)

SNMP Trap 測試：

圖 2-12SNMP Trap 設定



說明：

1. 系統管理員可按 鈕來測試 SNMP Trap 功能是否正常啓用。
-

2.5 語言版本

2.5.1 選擇語言版本

步驟1. 在【本機】>【系統管理】>【組態】>【語言版本】頁面中，選擇欲使用之管理介面語言版本，按下【確定】鈕。（如圖 2-13）



圖 2-13 管理介面語言版本設定

第3章 系統監控報告

用來保存和顯示 CMS-2000 的系統效能、事件記錄。

- **【系統效能】**：CMS-2000 的 CPU、硬碟以及記憶體使用率。
- **【事件記錄】**：CMS-2000 系統運作、登入、組態參數值（System Configurations）更改...記錄。

【事件記錄】功能概述：

搜尋 說明如下：

- 可依照日期、管理員名稱、IP 位址、事件類型和僅顯示有詳細內容之事件記錄等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
 - ◆ 在【本機】>【系統管理】>【系統監控報告】>【事件記錄】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 按下【搜尋】鈕。（如圖 3-1）

搜尋 事件記錄

☒ 起始 日期/時間: 2012 / 05 / 15 00 : 00
結束 日期/時間: 2012 / 05 / 16 18 : 23
管理員名稱: (最多 30 個字元)
IP位址:
事件類型:
☐ 僅顯示有詳細內容之事件記錄

搜尋

搜尋結果

2012-05-16 (9 筆記錄)

1 / 1 移至

時間 ▲	管理員名稱 ▲	IP位址 ▲	事件 ▲	內容 ▲
15:32:13	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:32:11	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:36	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:36	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:33	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:31	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:24	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:17	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:21:45	admin	172.19.20.12	[系統管理→管理→軟體更新] 成功 (v3.06.0 ==> v3.06.0)	---

1 / 1 移至

圖 3-1 搜尋特定記錄

3.1 系統效能

步驟1. 在【本機】>【系統管理】>【系統監控報告】>【系統效能】頁面中，可顯示目前或指定日期的 CMS-2000 系統 CPU、硬碟、記憶體使用狀況之相關訊息：(如圖 3-2)

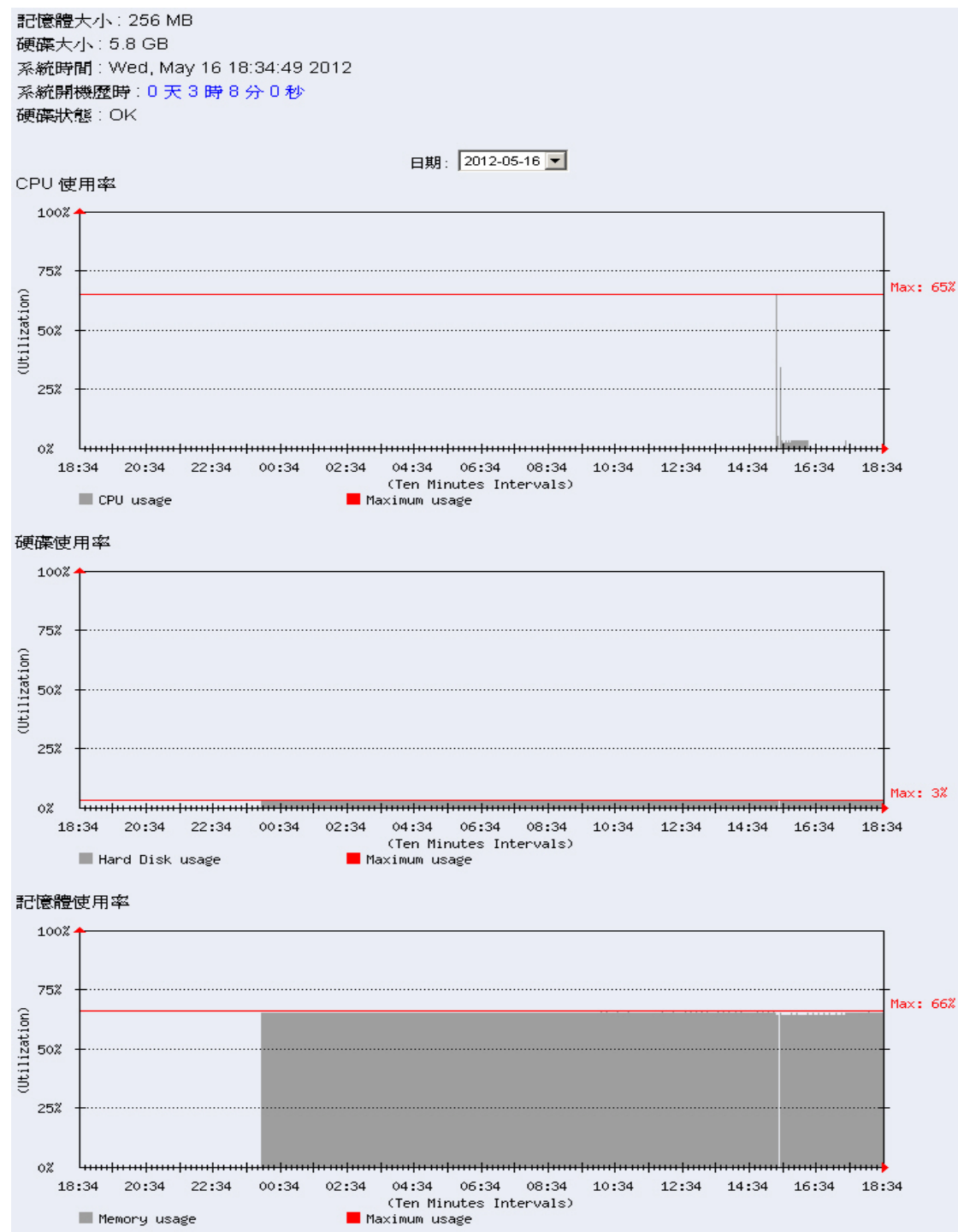



圖 3-2 系統資源使用狀態

3.2 事件記錄

3.2.1 檢視系統管理員登入和管理CMS-2000 之行爲

步驟1. 在【本機】>【系統管理】>【系統監控報告】>【事件記錄】頁面中，可顯示系統管理員登入和管理 CMS-2000 的事件記錄。(如圖 3-3)

■ 按下  鈕，CMS-2000 會顯示該筆記錄的詳細訊息。(如圖 3-4)

2012-05-16 (9 筆記錄)				
時間	管理員名稱	IP位址	事件	內容
15:32:13	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:32:11	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:38	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:36	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:33	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:31	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:24	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:31:17	admin	172.19.20.12	[系統管理→組態→時間設定] 修改	
15:21:45	admin	172.19.20.12	[系統管理→管理→軟體更新] 成功 (v3.06.0 ==> v3.06.0)	---

圖 3-3 事件記錄

http://172.19.1.111 - [事件日誌] 內容 (8) - Microsoft Internet Explorer

日期 / 時間	管理員名稱	IP位址	事件
15:32:11	admin	172.19.20.12	[系統管理→組態→時間設定] 修改

內容

修改之前

系統時間:
[設定時區](#)

與GMT相差 小時 [輔助選取](#)

同步系統時間

☒ 開啓與外部時間伺服器同步

☐ 開啓日光節約時間設定，從 / 至 /

時間伺服器位址 [輔助選取](#)

系統時間每 分鐘自動更新 (範圍: 0 ~ 99999, 0: 表示於開機時更新)

系統時間與您的電腦同步

修改之後

系統時間:
[設定時區](#)

與GMT相差 小時 [輔助選取](#)

完成

網際網路

圖 3-4 事件記錄內容

裝置管理

第4章 裝置管理

針對 CMS-2000 連線的 UTM、MHG 設備進行運作狀態檢視、設定檔備份、恢復出廠預設值等作業，並可將 CMS-2000 匯入、備份的 UTM、MHG 設定檔或軟體，上傳到指定設備。

【裝置】功能概述：

名稱 說明如下：

- 遠端 UTM、MHG 的裝置名稱，可藉此直接登入其管理介面。

IP 位址 說明如下：

- 遠端 UTM、MHG 的連線 IP 位址。

型號 說明如下：

- 遠端 UTM、MHG 設備的型號。

版本 說明如下：

- 遠端 UTM、MHG 設備使用的軟體版本。

系統效能 說明如下：

- 遠端 UTM、MHG 設備的 CPU、記憶體、硬碟使用率。

變更 說明如下：

- 修改裝置資訊、刪除連線裝置、備份裝置設定檔或將裝置恢復為出廠設定值。

【組態 / 軟體備份】功能概述：

上傳軟體 說明如下：

- 將儲存在管理者電腦的 UTM、MHG 軟體傳輸至 CMS-2000。

上傳組態檔 說明如下：

- 將儲存在管理者電腦的 UTM、MHG 設定檔傳輸至 CMS-2000。

裝置組態檔備份 說明如下：

- 備份至 CMS-2000 的連線裝置設定檔。

【組態 / 軟體更新】功能概述：

i 說明如下：

- CMS-2000 傳輸 UTM、MHG 設定檔或軟體到連線裝置的狀態。

更新時間 說明如下：

- CMS-2000 傳輸 UTM、MHG 設定檔或軟體到連線裝置的時間。

裝置 說明如下：

- CMS-2000 傳輸 UTM、MHG 設定檔或軟體到達的連線裝置。

4.1 裝置管理功能使用範例

4.1.1 將CMS-2000 匯入、備份的UTM、MHG設定檔或軟體，上傳到指定設備

步驟1. 在【本機】>【裝置管理】>【裝置】頁面中，做下列設定：

- 針對指定的連線裝置，按下【修改】鈕。(如圖 4-1)
- 輸入指定的【裝置別名】、【管理者名稱】、【管理者電子郵件】、【管理者電話】、【公司地址】。
- 按下【確定】鈕。(如圖 4-2)
- 針對指定的連線裝置，按下【組態備份】鈕。
- 【確定】連線裝置設定檔已備份至 CMS-2000。(如圖 4-3)




圖 4-1 設定連線裝置資訊

名稱	IP位址	型號	版本	系統效能	變更			
Host_Office_UTM-2000	172.19.20.11	UTM-2000	3.06.00		修改	刪除	組態備份	恢復至出廠設定值

圖 4-2 完成連線裝置資訊設定

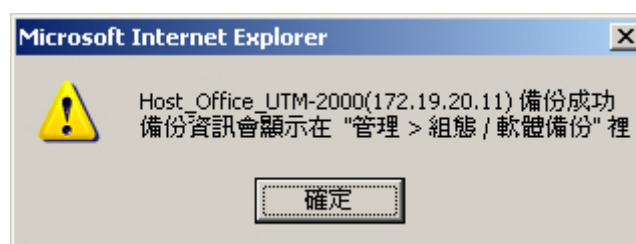


圖 4-3 連線裝置設定檔備份確認視窗



說明：

1. 建議針對所有連線裝置設定易於辨識的資訊，以利管理和監控。
2. 若同時有多台裝置和 CMS-2000 連線，在【本機】>【裝置管理】>【群組】頁面中，會自動將其整合為 GROUP_1 群組。為方便更新其軟體，可將同型號的裝置歸類、群組，並設定易於辨識的名稱。（如圖 4-4, 圖 4-5, 圖 4-6）

群組名稱：GROUP_1 (2)	修改
Host Office UTM-20...	Branch UTM-2000
群組名稱：GROUP_2	修改
群組名稱：GROUP_3	修改
群組名稱：GROUP_4	修改
群組名稱：GROUP_5	修改
群組名稱：GROUP_6	修改

圖 4-4CMS-2000 自動群組所有連線裝置

修改群組

名稱：

UTM-2000_Group

全選

反向選擇

[可選取的裝置名稱]

全選

反向選擇

[被選取的裝置名稱]

172.19.20.11

172.19.1.254

新增 >>

<< 刪除

確定

取消

圖 4-5 設定連線裝置群組

群組名稱：UTM-2000_Group (2)	修改
Host Office UTM-20...	Branch UTM-2000
群組名稱：GROUP_2	修改
群組名稱：GROUP_3	修改
群組名稱：GROUP_4	修改
群組名稱：GROUP_5	修改
群組名稱：GROUP_6	修改

圖 4-6 完成連線裝置群組設定

步驟2. 在【本機】>【裝置管理】>【組態 / 軟體備份】頁面中，做下列設定：

- 按下【上傳軟體】右方的【瀏覽】鈕。(如圖 4-7)
- 在【選擇檔案】視窗中，【開啓】儲存在電腦的 UTM、MHG 軟體。
- 按下【上傳】鈕。
- 【確定】UTM、MHG 軟體成功上傳 CMS-2000。(如圖 4-8, 圖 4-9)
- 按下【上傳組態檔】右方的【瀏覽】鈕。(如圖 4-10)
- 在【選擇檔案】視窗中，【開啓】儲存在電腦的 UTM、MHG 設定檔。
- 按下【上傳】鈕。
- 【確定】UTM、MHG 設定檔成功上傳 CMS-2000。(如圖 4-11, 圖 4-12, 圖 4-13)



圖 4-7 上傳軟體所在目錄位置與檔名



圖 4-8 等待軟體上傳

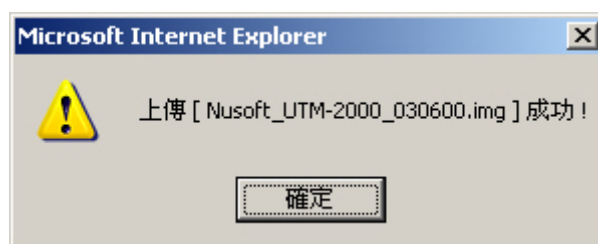


圖 4-9 軟體上傳成功確認視窗

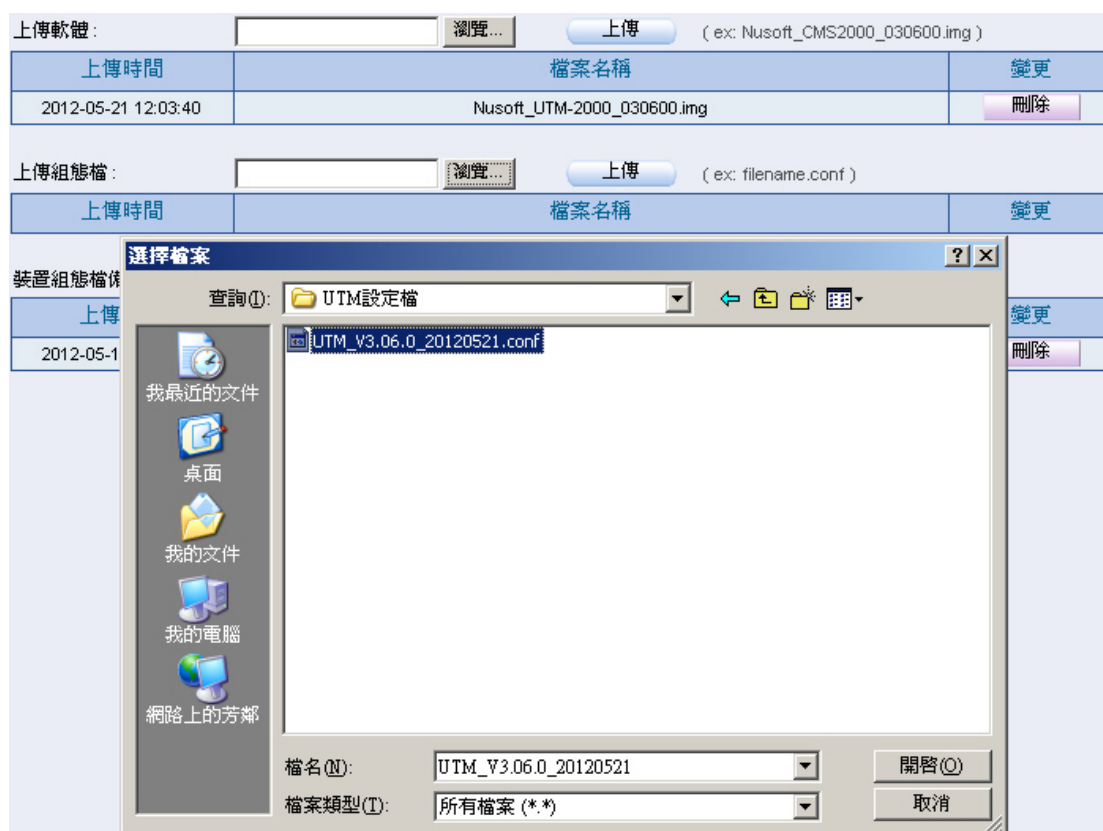


圖 4-10 上傳設定檔所在目錄位置與檔名



圖 4-11 等待設定檔上傳



圖 4-12 設定檔上傳成功確認視窗

上傳軟體： (ex: Nusoft_CMS2000_030600.img)

上傳時間	檔案名稱	變更
2012-05-21 12:03:40	Nusoft_UTM-2000_030600.img	<input type="button" value="刪除"/>

上傳組態檔： (ex: filename.conf)

上傳時間	檔案名稱	變更
2012-05-21 14:27:46	UTM_V3.06.0_20120521.conf	<input type="button" value="刪除"/>

裝置組態檔備份：

上傳時間	裝置	檔案名稱	變更
2012-05-18 15:51:22	Host_Office_UTM-2000	00:0E:2E:56:B9:95.conf	<input type="button" value="刪除"/>

圖 4-13CMS-2000 匯入、備份的 UTM、MHG 設定檔和軟體

步驟3. 在【本機】>【裝置管理】>【組態 / 軟體更新】頁面中，做下列設定：
(如圖 4-14)

- 選擇指定的【更新時間】、【上傳檔案】。
- 將指定【可選取裝置】新增至【被選取裝置】清單中。
- 按下【確定】鈕。(如圖 4-15)
- 待更新時間到達，CMS-2000 會將指定檔案傳輸至選定的連線裝置。(如圖 4-16, 圖 4-17)

圖 4-14 設定組態 / 軟體更新

i	更新時間	裝置	變更
更新執行時間	2012-05-21 17:10	Host_Office_UTM-2000 [172.19.20.11]	修改 刪除
新增			

圖 4-15 完成組態 / 軟體更新設定

i	更新時間	裝置	變更
成功	2012-05-21 17:10	Host_Office_UTM-2000 [172.19.20.11]	修改 刪除
新增			

圖 4-16 CMS-2000 更新連線裝置組態 / 軟體

更新				
2012-05-21 (6 筆記錄)				
<div> <div>1 / 1</div> <div>移至</div> </div>				
時間	管理員名稱	IP位址	事件	內容
17:19:11	admin	172.19.20.12	登入成功	---
17:11:59	CMS	192.168.112.1	Restore config by CMS	---
16:52:22	admin	172.19.20.12	登入成功	---
16:19:01	admin	172.19.20.12	登入成功	---
14:25:09	admin	172.19.20.12	[系統管理→組態→系統設定] 下載組態檔	---
14:24:48	admin	172.19.20.12	登入成功	---
<div> <div>1 / 1</div> <div>移至</div> </div>				

圖 4-17 連線裝置更新記錄

裝置監控備份

第5章 郵件安全報告

CMS-2000 可即時接收遠端 UTM 掃描郵件的結果，並做成統計報表和日誌，使企業可以瞭解到相關郵件處理的資訊。

【設定】功能概述：

垃圾 / 病毒郵件日誌保存期限 說明如下：

- 對於儲存在郵件日誌的信件記錄，可指定保留的時間，並於到期日刪除所有符合條件的記錄。

定期報告 說明如下：

- 可依選擇的報表產生時間，定時寄送報告給收件者。

歷史報告 說明如下：

- 可產生指定日期的報表並即時郵寄給收件者。
 - ◆ 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，啟動並進行【電子郵件警告 / 報告設定】，並在【本機】>【裝置監控備份】>【郵件安全報告】>【設定】頁面中，做下列設定：
 - 輸入指定【垃圾 / 病毒郵件日誌保存期限】。
 - 在【定期報告】設定欄位中，【開啓定期報告功能】並勾選年報、月報、週報和日報。
 - 按下【確定】鈕。(如圖 5-1)
 - 當時間到達時，CMS-2000 會寄送統計報表給收件者。(如圖 5-2, 圖 5-3, 圖 5-4, 圖 5-5, 圖 5-6)
 - 在【歷史報告】設定欄位中，指定要郵寄的報告日期。
 - 按下【郵寄報告】鈕。(如圖 5-7)
 - 會即時寄送相關統計報表給收件者。(如圖 5-8, 圖 5-9, 圖 5-10, 圖 5-11, 圖 5-12)



說明：

1. 郵寄定期報告，其產生方式如下：

- 【年報】：會於每年的 1 月 1 日上午 00:10 產生。
 - 【月報】：會於每月第一天的上午 00:10 產生。
 - 【週報】：會於每週第一天的上午 00:10 產生。
 - 【日報】：會於每天的上午 00:10 產生。
-

垃圾 / 病毒郵件日誌保存期限

保留時間 天 (範圍: 1 - 365)

定期報告 說明

☒ 開啓定期報告功能

☒ 年報 ☒ 月報 ☒ 週報 ☒ 日報

圖 5-1 垃圾 / 病毒郵件日誌保存期限、郵寄定期報告設定頁面

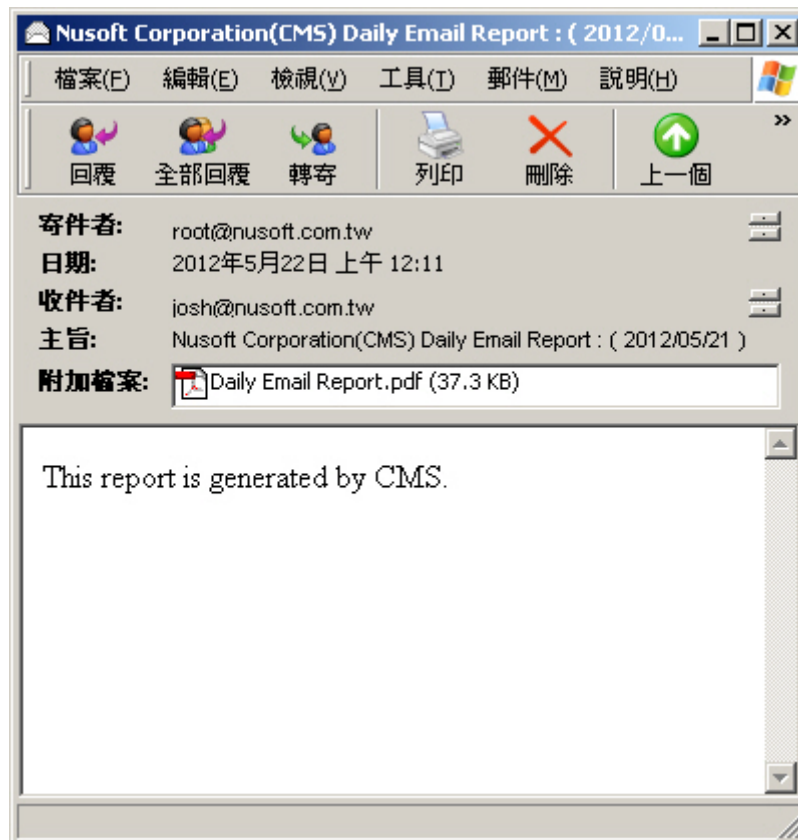
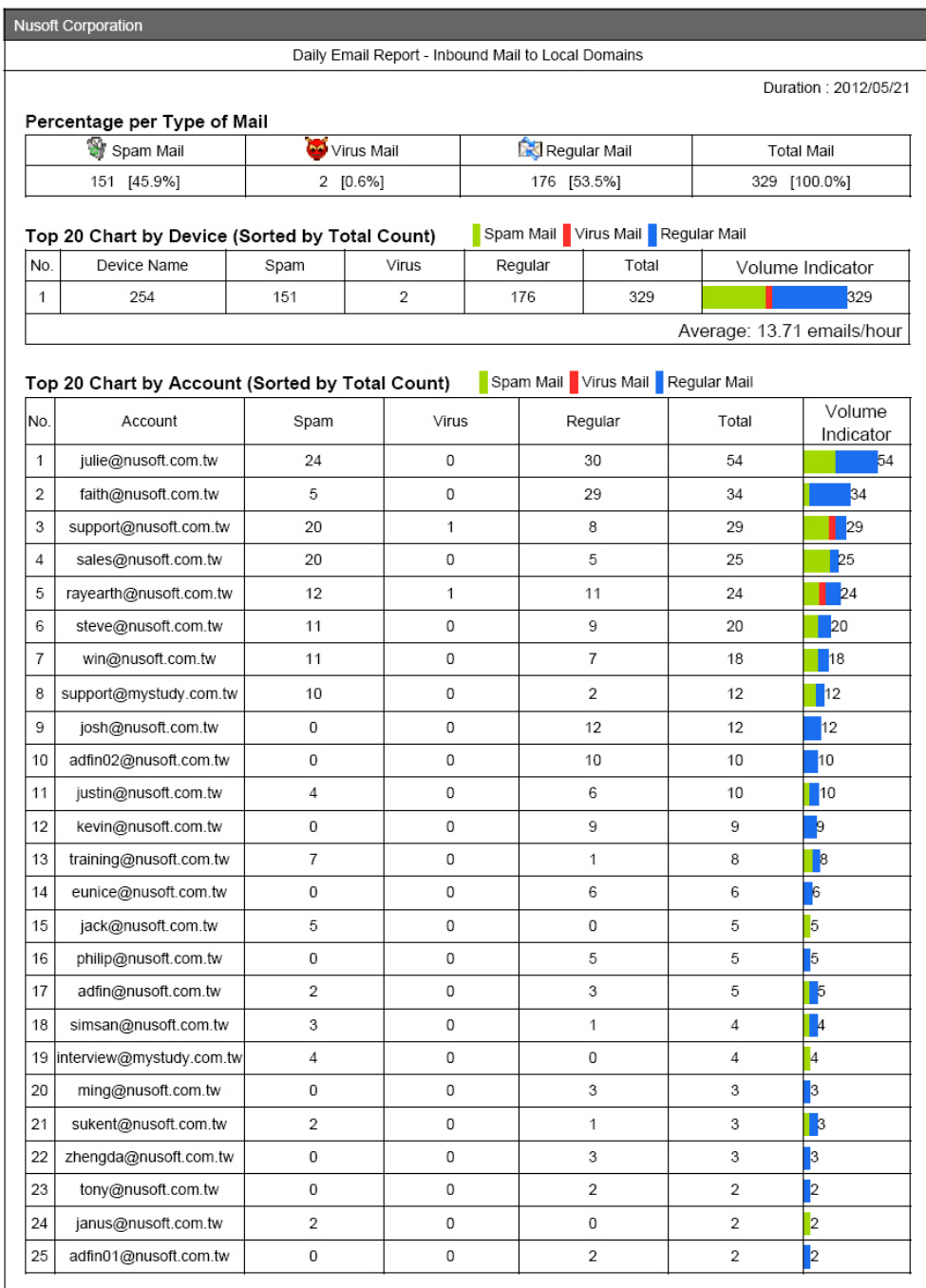


圖 5-2 收到定期報告信件



1

圖 5-3 郵件掃描定期報告內容第一頁

26	kenny@nusoft.com.tw	1	0	1	2	2
27	jackie@nusoft.com.tw	2	0	0	2	2
28	jameshihi@nusoft.com.tw	0	0	1	1	1
29	cs@nusoft.com.tw	1	0	0	1	1
30	reggie@nusoft.com.tw	0	0	1	1	1
31	kim@nusoft.com.tw	1	0	0	1	1
32	alex@nusoft.com.tw	1	0	0	1	1
33	tcin@nusoft.com.tw	0	0	1	1	1
34	emmy@nusoft.com.tw	1	0	0	1	1
35	nusoft@nusoft.com.tw	0	0	1	1	1
36	vmware@nusoft.com.tw	0	0	1	1	1
37	kongmeng@nusoft.com.tw	0	0	1	1	1
38	root@nusoft.com.tw	1	0	0	1	1
39	joy@nusoft.com.tw	0	0	1	1	1
40	andrewlai@nusoft.com.tw	0	0	1	1	1
41	ms01@mystudy.com.tw	0	0	1	1	1
42	reggie@mystudy.com.tw	1	0	0	1	1
43	kobe@nusoft.com.tw	0	0	1	1	1

Average: 13.71 emails/hour

Daily Statistics Graph

Spam Mail Virus Mail Regular Mail

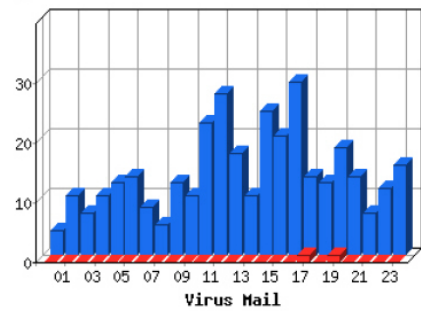
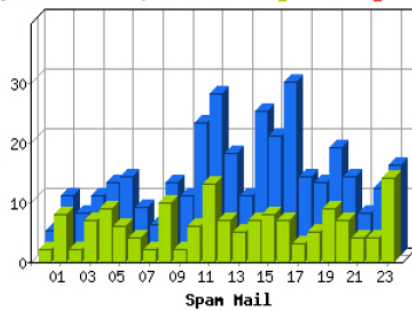






圖 5-4 郵件掃描定期報告內容第二頁

Percentage per Type of Mail

 Spam Mail	 Virus Mail	 Regular Mail	Total Mail
0 [0.0%]	0 [0.0%]	38 [100.0%]	38 [100.0%]


Top 20 Chart by Device (Sorted by Total Count)









 Spam Mail
 Virus Mail
 Regular Mail

No.	Device Name	Spam	Virus	Regular	Total	Volume Indicator
1	254	0	0	38	38	 38

Average: 1.58 emails/hour

Top 20 Chart by Account (Sorted by Total Count)

 Spam Mail
 Virus Mail
 Regular Mail

No.	Account	Spam	Virus	Regular	Total	Volume Indicator
1	julie@nusoft.com.tw	0	0	12	12	 12
2	faith@nusoft.com.tw	0	0	8	8	 8
3	kevin@nusoft.com.tw	0	0	6	6	 6
4	adfin02@nusoft.com.tw	0	0	4	4	 4
5	zhengda@nusoft.com.tw	0	0	3	3	 3
6	adfin@nusoft.com.tw	0	0	2	2	 2
7	rayearth@nusoft.com.tw	0	0	2	2	 2
8	simsan@nusoft.com.tw	0	0	1	1	 1

Average: 1.58 emails/hour

Daily Statistics Graph

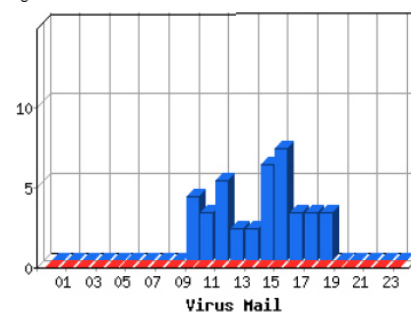
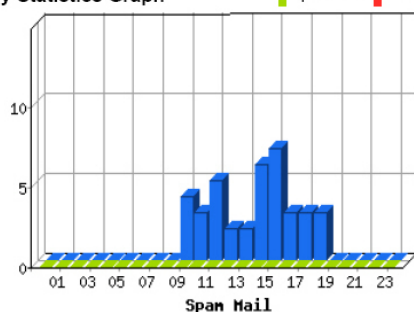
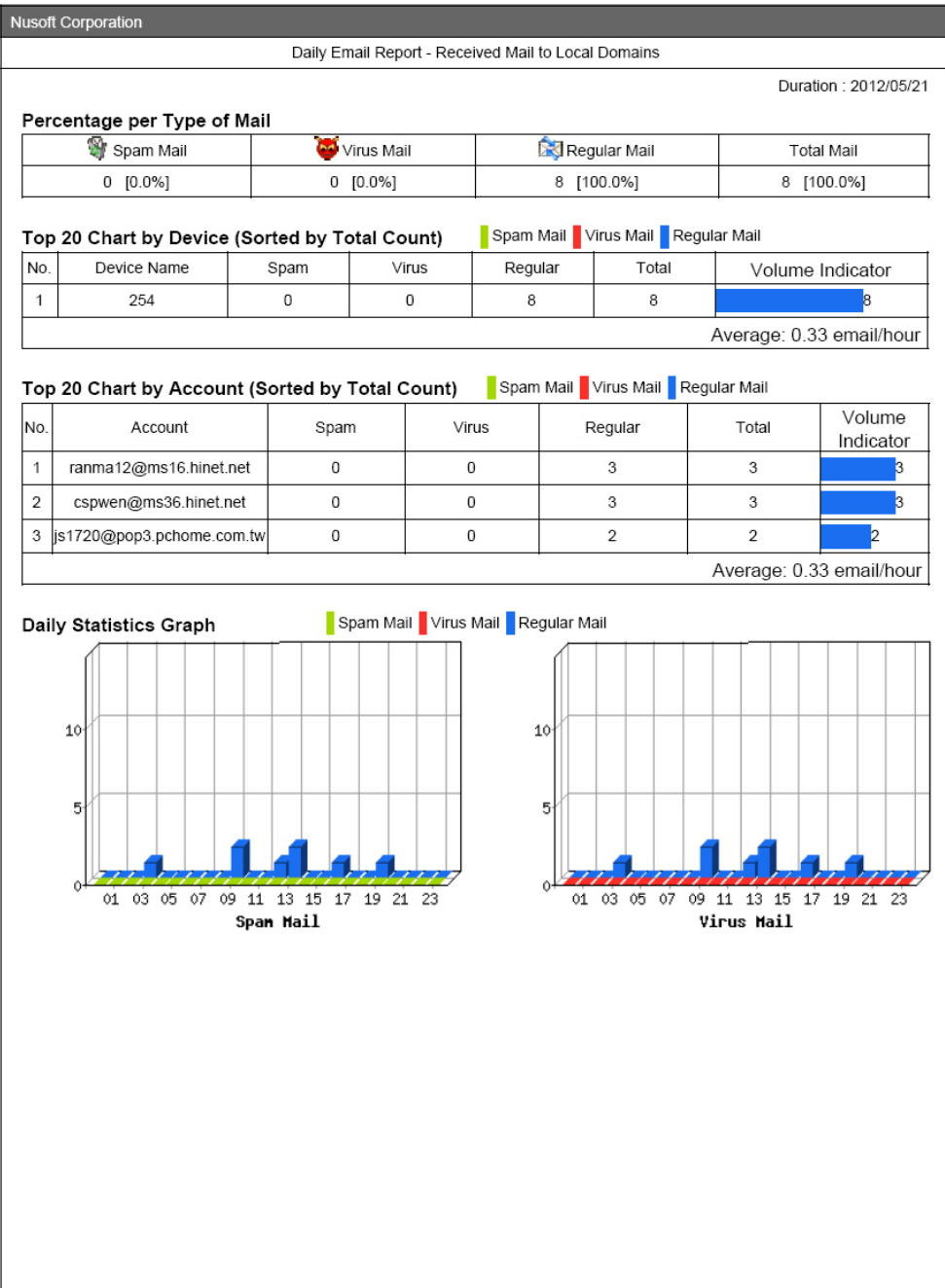
 Spam Mail
 Virus Mail
 Regular Mail


圖 5-5 郵件掃描定期報告內容第三頁



4

圖 5-6 郵件掃描定期報告內容第四頁



圖 5-7 郵寄歷史報告設定頁面

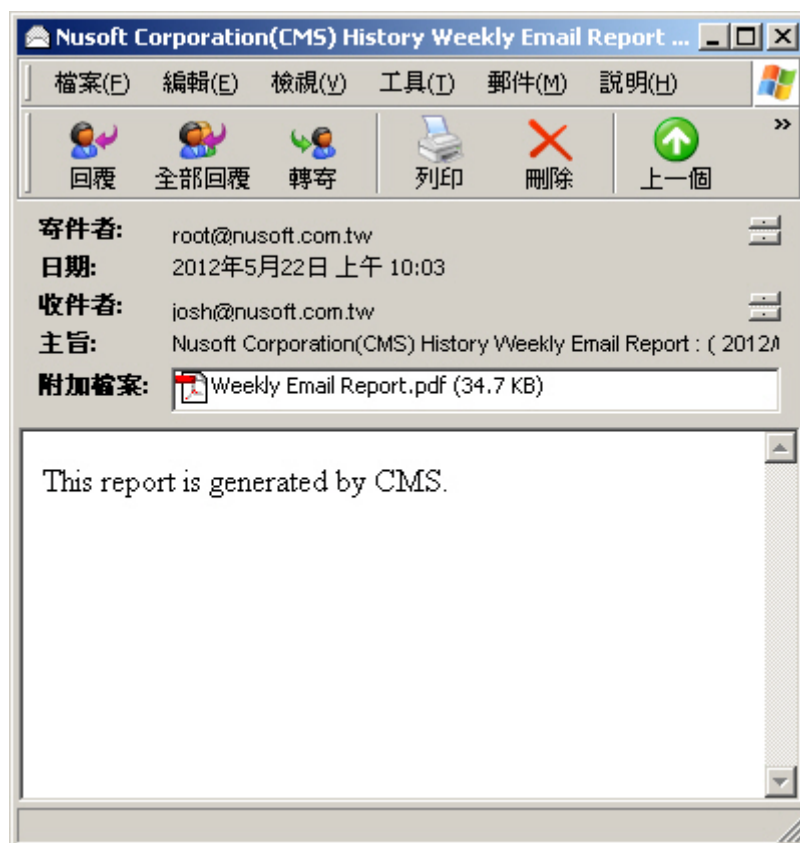
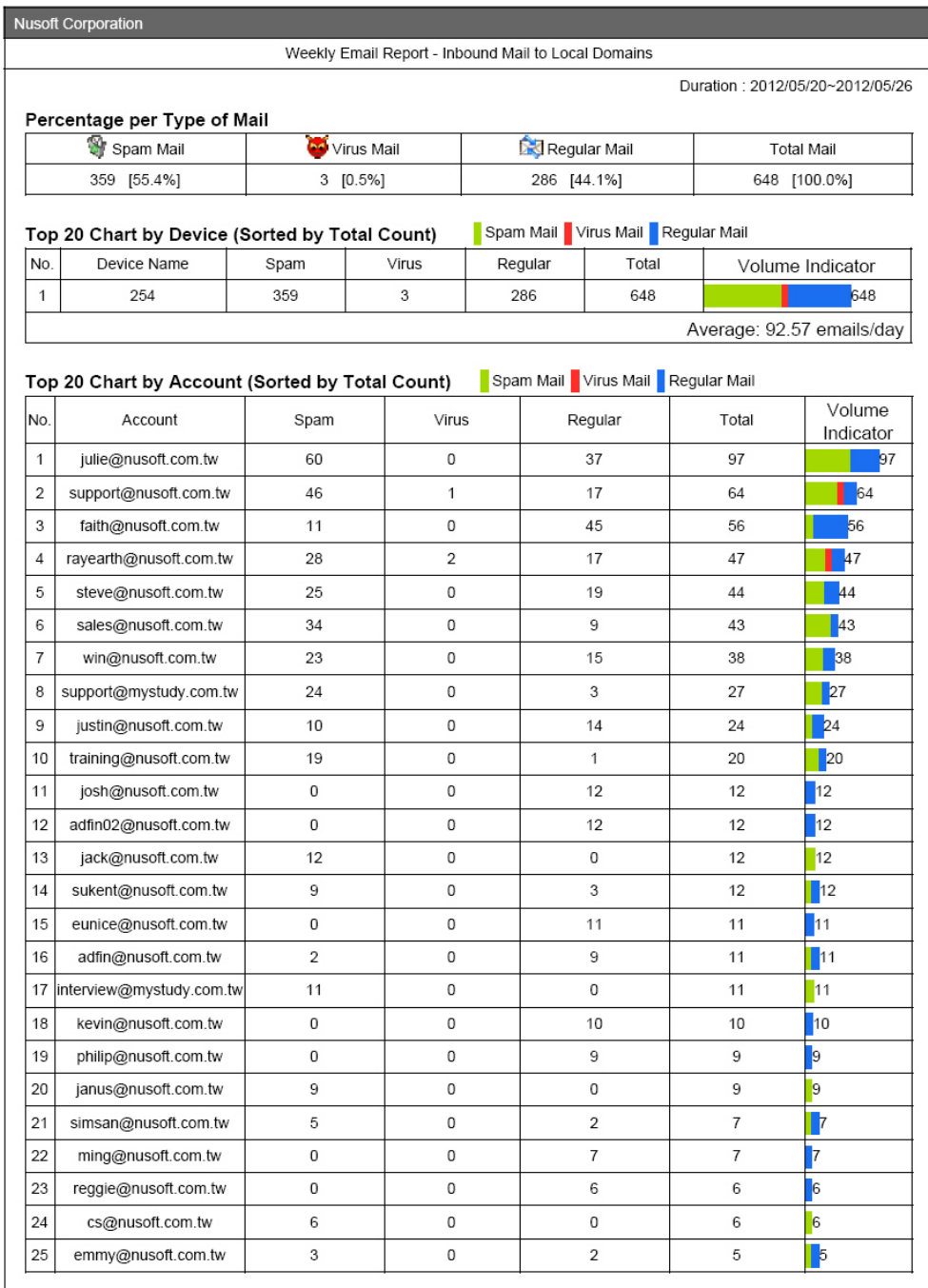


圖 5-8 收到歷史報告信件



1

圖 5-9 郵件掃描歷史報告內容第一頁

26	jackie@nusoft.com.tw	4	0	0	4	4
27	rd@nusoft.com.tw	4	0	0	4	4
28	tony@nusoft.com.tw	2	0	2	4	4
29	root@nusoft.com.tw	3	0	1	4	4
30	ms01@mystudy.com.tw	0	0	3	3	3
31	adfin01@nusoft.com.tw	0	0	3	3	3
32	kim@nusoft.com.tw	2	0	1	3	3
33	zhengda@nusoft.com.tw	0	0	3	3	3
34	nusoft@nusoft.com.tw	0	0	2	2	2
35	kenny@nusoft.com.tw	1	0	1	2	2
36	andrewlai@nusoft.com.tw	0	0	2	2	2
37	alex@nusoft.com.tw	2	0	0	2	2
38	owen@nusoft.com.tw	2	0	0	2	2
39	vmware@nusoft.com.tw	0	0	1	1	1
40	android@nusoft.com.tw	0	0	1	1	1
41	kongmeng@nusoft.com.tw	0	0	1	1	1
42	ms03@mystudy.com.tw	0	0	1	1	1
43	tcin@nusoft.com.tw	0	0	1	1	1
44	kobe@nusoft.com.tw	0	0	1	1	1
45	ejufan@nusoft.com.tw	1	0	0	1	1
46	joy@nusoft.com.tw	0	0	1	1	1
47	jameshihi@nusoft.com.tw	0	0	1	1	1
48	reggie@mystudy.com.tw	1	0	0	1	1

Average: 92.57 emails/day

Weekly Statistics Graph

Spam Mail Virus Mail Regular Mail

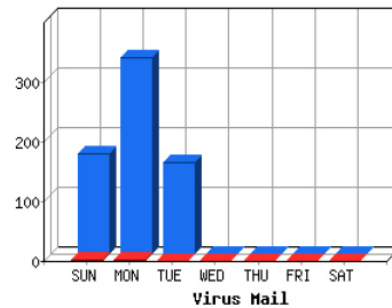
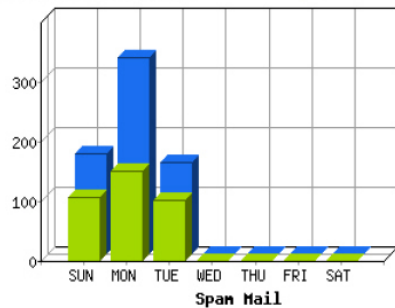
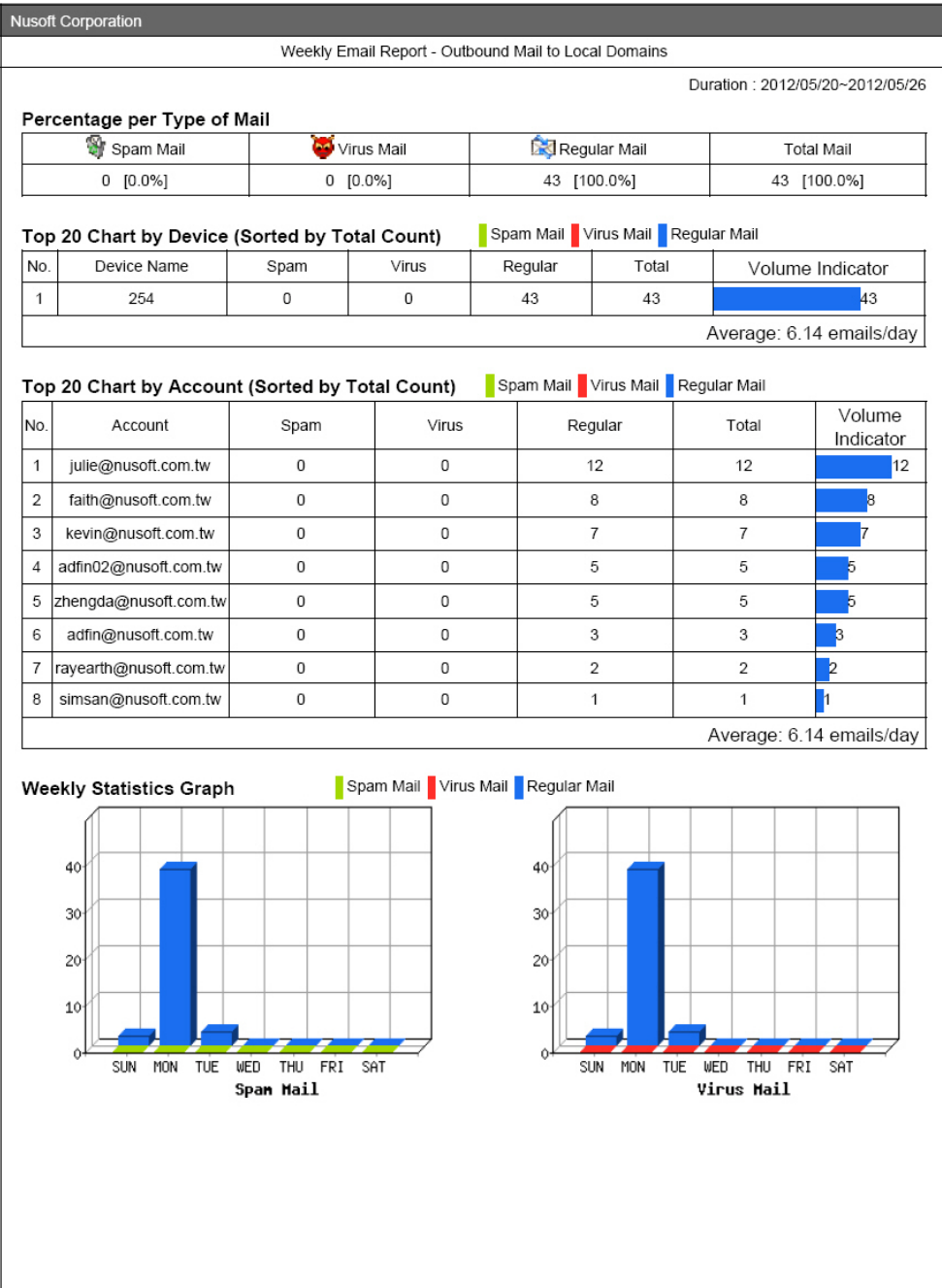




圖 5-10 郵件掃描歷史報告內容第二頁






3


圖 5-11 郵件掃描歷史報告內容第三頁

Percentage per Type of Mail

 Spam Mail	 Virus Mail	 Regular Mail	Total Mail
0 [0.0%]	0 [0.0%]	10 [100.0%]	10 [100.0%]




Top 20 Chart by Device (Sorted by Total Count)




 Spam Mail
 Virus Mail
 Regular Mail

No.	Device Name	Spam	Virus	Regular	Total	Volume Indicator
1	254	0	0	10	10	 10

Average: 1.43 emails/day

Top 20 Chart by Account (Sorted by Total Count)

 Spam Mail
 Virus Mail
 Regular Mail

No.	Account	Spam	Virus	Regular	Total	Volume Indicator
1	cspwen@ms36.hinet.net	0	0	4	4	 4
2	ranma12@ms16.hinet.net	0	0	3	3	 3
3	js1720@pop3.pchome.com.tw	0	0	3	3	 3

Average: 1.43 emails/day

Weekly Statistics Graph




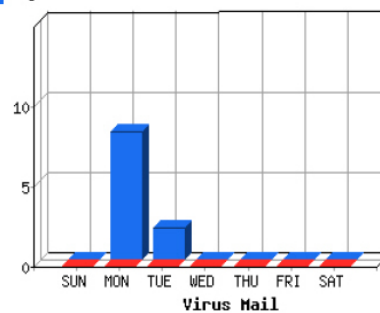
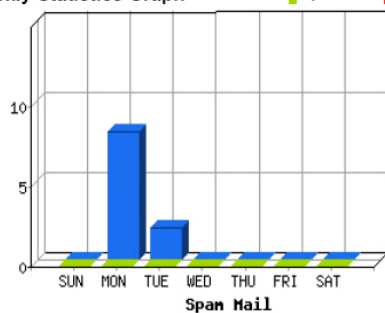
 Spam Mail
 Virus Mail
 Regular Mail


圖 5-12 郵件掃描歷史報告內容第四頁

【日誌】功能概述：

搜尋 說明如下：

- 可依照日期、裝置名稱、寄件者、寄件者 IP、收件者、附加檔案、主旨、屬性和處理方式等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- ◆ 在【本機】>【裝置監控備份】>【郵件安全報告】>【日誌】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】。
 - 【收件者】輸入郵件帳號之關鍵字。
 - 選擇指定【附加檔案】、【屬性】、【處理方式】。
 - 按下【搜尋】鈕。（如圖 5-13）

SMTP 內送郵件 POP3
SMTP 外寄郵件

搜尋 郵件記錄

☒ 起始 日期/時間: 2012 / 05 / 16 00 : 00
結束 日期/時間: 2012 / 05 / 22 19 : 33
裝置名稱: 所有遠端裝置
寄件者: (最多 100 個字元)
寄件者IP:
收件者: josh (最多 100 個字元)
附加檔案: 全部
主旨: (最多 100 個字元)
屬性: 全部
處理方式: 全部

搜尋

結果

2012-05-16 (4 筆記錄)

1 / 1 移至

時間	遠端裝置	寄件者	收件者	主旨	屬性	處理方式
21:59:27	254	apache@edmxurma...	josh@nusoft.com.tw	- 夏日變髮口下殺最低 \ 2.7 ...		
10:10:30	254	rayearth.cheng@gm...	adfin01@nusoft.com...	- Seagate授權快換中心在原價...		
10:00:28	254	vanessa_chang@ca...	josh@nusoft.com.tw	讀取: 關於 ML2500 郵件問題		
08:55:34	254	CFC@Chengday.co...	josh@nusoft.com.tw	讀取: TEST 12:25		

1 / 1 移至

圖 5-13 搜尋特定記錄



說明：

1. 於【本機】>【裝置監控備份】>【郵件安全報告】>【統計】和【日誌】報表中，可分別選擇顯示 SMTP 內送、SMTP 外寄、POP3 郵件的掃描報告。
 2. 於【本機】>【裝置監控備份】>【郵件安全報告】>【日誌】報表中，按下【寄件者】郵件地址連結，可顯示【收件者列表】報告，若按下【收件者】郵件地址連結，可顯示【寄件者列表】報告。
 3. 【本機】>【裝置監控備份】>【郵件安全報告】>【日誌】報表，可透過時間、寄件者、收件者、主旨、屬性或處理方式做排序的動作。【收件者列表】和【寄件者列表】，則可透過時間、寄件者或收件者、主旨、屬性或處理方式做排序的動作。
-

5.1 統計

步驟1. 在【本機】>【裝置監控備份】>【郵件安全報告】>【統計】頁面中，會顯示遠端 UTM 郵件掃描過後的統計報表。(如圖 5-14)

- 點選【日】，可檢視以每日 (Day) 為單位的統計報表。
- 點選【週】，可檢視以週 (Week) 為單位的統計報表。
- 點選【月】，可檢視以月 (Month) 為單位的統計報表。
- 點選【年】，可檢視以年 (Year) 為單位的統計報表。



圖 5-14 郵件掃描統計報表

5.2 日誌

步驟1. 在【本機】>【裝置監控備份】>【郵件安全報告】>【日誌】頁面中，會顯示目前遠端 UTM 郵件掃描的處理狀況。(如圖 5-15)

裝置名稱: 所有遠端裝置

SMTP 內送郵件 POP3 SMTP 外寄郵件

2012-05-22(364 筆記錄)

時間	遠端裝置	寄件者	收件者	主旨	屬性	處理方式
21:39:49	254	epaper.t9585@msa...	julie@nusoft.com.tw	- 有了遠端通報系統再也不怕...		
21:37:15	254	rh@incom.com.br	support@mystudy.c...	- 新片不斷・更新最快rosh		
21:34:52	254	tsb@mhrecv.taishinb...	steve@nusoft.com.tw	- 【集點行樂最有利2】贈品...		
21:32:34	254	patric@hddgroup.com...	faith@nusoft.com.tw	- Fw: 101.05.22 <新知傳遞者> ...		
21:26:20	254	jeremikemph@yaho...	win@nusoft.com.tw	- 對於藍藻綠藻有需求的朋友...		
21:25:07	254	snort-users-bounce...	steve@nusoft.com.tw	- Re: [Snort-users] New snort in...		
21:08:10	254	iswwwzecc@yahoo.c...	julie@nusoft.com.tw	- 韓國演藝偷拍1.5 .m f w...		
21:00:46	254	root@oms08.104.co...	faith@nusoft.com.tw	- 104應徵履歷【軟體技術...		
20:50:50	254	sentto-82719262-25...	julie@nusoft.com.tw	- [kouslv] 透過這個專案,能夠...		
20:43:44	254	returnedm@return.p...	win@nusoft.com.tw	- 5/22 21:00大折扣 PC-cillin ...		
20:42:38	254	bouncemail_8FD1F6...	eunice@nusoft.com...	- Your Ideal ERP System Realized		
20:40:16	254	sentto-82697440-25...	rayearth@nusoft.co...	- [ebebo] 透過這個專案,能夠...		
20:39:09	254	4lasizonj2v00hoccst...	steve@nusoft.com.tw	- Introducing The June Collection...		
20:36:43	254	saudeep38012@yah...	rayearth@nusoft.co...	- OMEGA型錄主qm42vhn		
20:10:31	254	sentto-81009934-12...	rayearth@nusoft.co...	- [qjllw] 【引頸期盼，終於來...		
20:10:19	254	sentto-84242516-44...	interview@mystudy...	- [mouuwo] 跨國喝咖啡全面啓...		
20:06:59	254	s00s@shu.edu.cn	julie@nusoft.com.tw	- 屈臣氏 (Watsons Water) 南...		
20:04:47	254	ekfist@yahoo.com.tw	julie@nusoft.com.tw	- 亞洲第一性感F奶爆乳...		
20:04:12	254	tmukvp@gmail.com	steve@nusoft.com.tw	- 海外成人電影 -- 中文字幕		
19:59:54	254	snort-users-bounce...	steve@nusoft.com.tw	- [Snort-users] Logging URI too l...		

圖 5-15 郵件掃描日誌

說明：

1. 【日誌】報表的相關圖示說明如下：

■ 屬性：

圖例				
代表涵義	正常郵件	垃圾郵件	病毒郵件	未掃描信件

■ 處理方式：

圖例					
代表涵義	刪除	通知收件者	傳送	儲存	已取回

■ 附加檔案：

第6章 郵件歸檔報告

CMS-2000 可即時接收遠端 UTM 審核和存查郵件的結果，並做成統計報表和日誌，方便管理者調閱以調整郵件管理政策。

【設定】功能概述：

歸檔 / 稽核郵件保存期限 說明如下：

- 對於儲存在歸檔報告的信件記錄，可指定保留的時間，並於到期日刪除所有符合條件的記錄。

定期報告 說明如下：

- 可依選擇的報表產生時間，定時寄送報告給收件者。

歷史報告 說明如下：

- 可產生指定日期的報表並即時郵寄給收件者。
 - ◆ 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，啟動並進行【電子郵件警告 / 報告設定】，並在【本機】>【裝置監控備份】>【郵件歸檔報告】>【設定】頁面中，做下列設定：
 - 輸入指定【歸檔 / 稽核郵件保存期限】。
 - 在【定期報告】設定欄位中，【開啓定期報告功能】並勾選年報、月報、週報和日報。
 - 按下【確定】鈕。(如圖 6-1)
 - 當時間到達時，CMS-2000 會寄送統計報表給收件者。(如圖 6-2, 圖 6-3, 圖 6-4, 圖 6-5, 圖 6-6)
 - 在【歷史報告】設定欄位中，指定要郵寄的報告日期。
 - 按下【郵寄報告】鈕。(如圖 6-7)
 - 會即時寄送相關統計報表給收件者。(如圖 6-8, 圖 6-9, 圖 6-10, 圖 6-11, 圖 6-12)



說明：

1. 郵寄定期報告，其產生方式如下：

- 【年報】：會於每年的 1 月 1 日上午 00:10 產生。
 - 【月報】：會於每月第一天的上午 00:10 產生。
 - 【週報】：會於每週第一天的上午 00:10 產生。
 - 【日報】：會於每天的上午 00:10 產生。
-

歸檔 / 稽核郵件保存期限

保留時間 天 (範圍: 1 - 365)

定期報告 說明

☒ 開啓定期報告功能

☒ 年報 ☒ 月報 ☒ 週報 ☒ 日報

圖 6-1 歸檔 / 稽核郵件保存期限、郵寄定期報告設定頁面

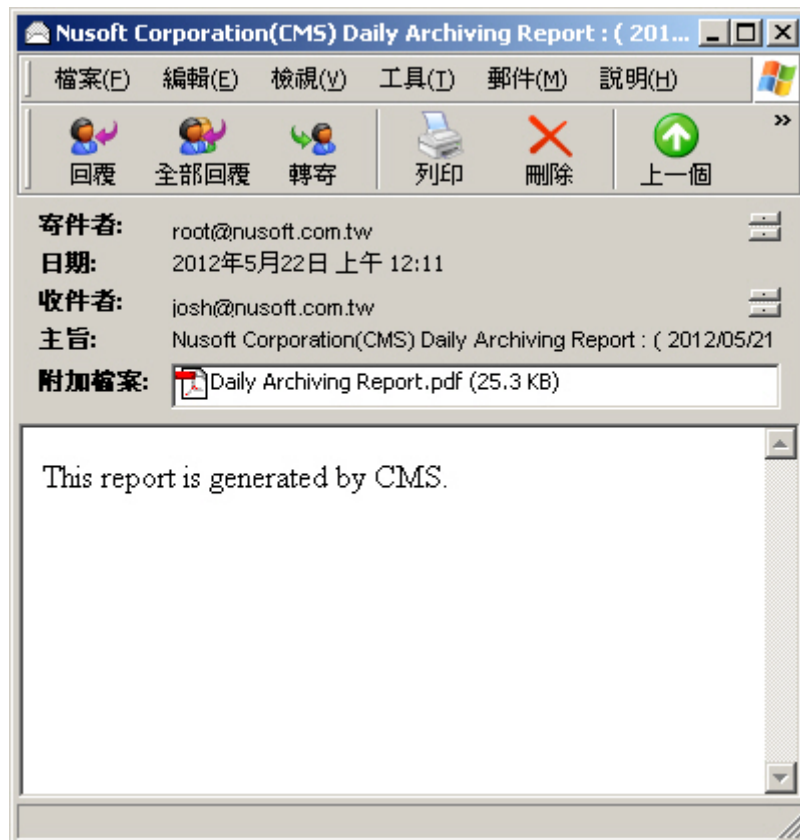


圖 6-2 收到定期報告信件

Nusoft Corporation

Daily Archiving Report - Inbound Mail to Local Domains

Duration : 2012/05/21

Total Email

Total Count of Emails	Total Volume of Emails
329	11.64 MB

Top 20 Chart by Device (Sorted by Volume)

No.	Device Name	Count	Volume	Volume Indicator
1	254	329	11.64 MB	<div></div> 11.64 MB

Top 20 Chart by Account (Sorted by Volume)

No.	Account	Count	Volume	Volume Indicator
1	julie@nusoft.com.tw	54	2.75 MB	<div></div> 2.75 MB
2	faith@nusoft.com.tw	34	1.97 MB	<div></div> 1.97 MB
3	rayearth@nusoft.com.tw	24	919.46 KB	<div></div> 919.46 KB
4	sales@nusoft.com.tw	25	866.84 KB	<div></div> 866.84 KB
5	support@nusoft.com.tw	29	810.66 KB	<div></div> 810.66 KB
6	win@nusoft.com.tw	18	781.22 KB	<div></div> 781.22 KB
7	steve@nusoft.com.tw	20	556.04 KB	<div></div> 556.04 KB
8	support@mystudy.com.tw	12	520.18 KB	<div></div> 520.18 KB
9	kevin@nusoft.com.tw	9	418.71 KB	<div></div> 418.71 KB
10	justin@nusoft.com.tw	10	363.33 KB	<div></div> 363.33 KB
11	simsan@nusoft.com.tw	4	236.19 KB	<div></div> 236.19 KB
12	adfin02@nusoft.com.tw	10	232.51 KB	<div></div> 232.51 KB
13	kongmeng@nusoft.com.tw	1	223.37 KB	<div></div> 223.37 KB
14	eunice@nusoft.com.tw	6	159.62 KB	<div></div> 159.62 KB
15	interview@mystudy.com.tw	4	155.19 KB	<div></div> 155.19 KB
16	jack@nusoft.com.tw	5	132.65 KB	<div></div> 132.65 KB
17	josh@nusoft.com.tw	12	123.59 KB	<div></div> 123.59 KB
18	training@nusoft.com.tw	8	97.80 KB	<div></div> 97.80 KB
19	philip@nusoft.com.tw	5	71.53 KB	<div></div> 71.53 KB
20	adfin01@nusoft.com.tw	2	55.64 KB	<div></div> 55.64 KB
21	sukent@nusoft.com.tw	3	51.31 KB	<div></div> 51.31 KB
22	adfin@nusoft.com.tw	5	47.79 KB	<div></div> 47.79 KB
23	alex@nusoft.com.tw	1	46.10 KB	<div></div> 46.10 KB
24	kim@nusoft.com.tw	1	29.55 KB	<div></div> 29.55 KB
25	ming@nusoft.com.tw	3	29.20 KB	<div></div> 29.20 KB
26	vmware@nusoft.com.tw	1	27.38 KB	<div></div> 27.38 KB

1

圖 6-3 郵件歸檔定期報告內容第一頁

27	kobe@nusoft.com.tw	1	27.37 KB	27.37 KB
28	zhengda@nusoft.com.tw	3	15.41 KB	15.41 KB
29	ms01@mystudy.com.tw	1	12.76 KB	12.76 KB
30	kenny@nusoft.com.tw	2	11.69 KB	11.69 KB
31	reggie@mystudy.com.tw	1	8.18 KB	8.18 KB
32	tcin@nusoft.com.tw	1	5.96 KB	5.96 KB
33	andrewlai@nusoft.com.tw	1	5.86 KB	5.86 KB
34	janus@nusoft.com.tw	2	5.34 KB	5.34 KB
35	jameshihi@nusoft.com.tw	1	5.04 KB	5.04 KB
36	tony@nusoft.com.tw	2	5.00 KB	5.00 KB
37	joy@nusoft.com.tw	1	4.57 KB	4.57 KB
38	jackie@nusoft.com.tw	2	3.83 KB	3.83 KB
39	cs@nusoft.com.tw	1	2.48 KB	2.48 KB
40	nusoft@nusoft.com.tw	1	2.34 KB	2.34 KB
41	reggie@nusoft.com.tw	1	2.05 KB	2.05 KB
42	emmy@nusoft.com.tw	1	1.54 KB	1.54 KB
43	root@nusoft.com.tw	1	1.54 KB	1.54 KB

Daily Statistics Graph

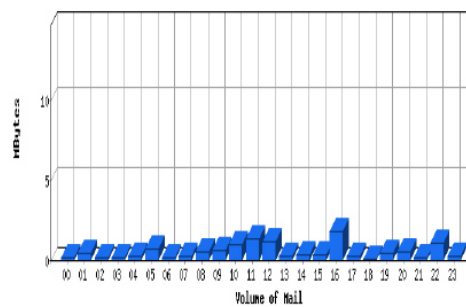


圖 6-4 郵件歸檔定期報告內容第二頁

Total Email

Total Count of Emails	Total Volume of Emails
38	1.74 MB

Top 20 Chart by Device (Sorted by Volume)

No.	Device Name	Count	Volume	Volume Indicator
1	254	38	1.74 MB	<div style="width: 100%;"></div> 1.74 MB

Top 20 Chart by Account (Sorted by Volume)

No.	Account	Count	Volume	Volume Indicator
1	adfin02@nusoft.com.tw	4	464.85 KB	<div style="width: 100%;"></div> 464.85 KB
2	julie@nusoft.com.tw	12	413.83 KB	<div style="width: 100%;"></div> 413.83 KB
3	rayearth@nusoft.com.tw	2	340.55 KB	<div style="width: 100%;"></div> 340.55 KB
4	faith@nusoft.com.tw	8	175.59 KB	<div style="width: 100%;"></div> 175.59 KB
5	simsan@nusoft.com.tw	1	170.12 KB	<div style="width: 100%;"></div> 170.12 KB
6	kevin@nusoft.com.tw	6	123.53 KB	<div style="width: 100%;"></div> 123.53 KB
7	adfin@nusoft.com.tw	2	86.53 KB	<div style="width: 100%;"></div> 86.53 KB
8	zhengda@nusoft.com.tw	3	11.40 KB	<div style="width: 100%;"></div> 11.40 KB

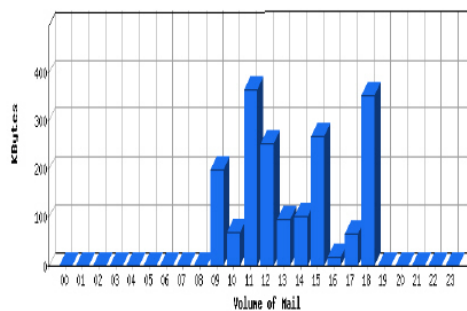
Daily Statistics Graph

圖 6-5 郵件歸檔定期報告內容第三頁

Total Email

Total Count of Emails	Total Volume of Emails
8	291.19 KB

Top 20 Chart by Device (Sorted by Volume)

No.	Device Name	Count	Volume	Volume Indicator
1	254	8	291.19 KB	291.19 KB

Top 20 Chart by Account (Sorted by Volume)

No.	Account	Count	Volume	Volume Indicator
1	ranma12@ms16.hinet.net	3	146.47 KB	146.47 KB
2	cspwen@ms36.hinet.net	3	130.19 KB	130.19 KB
3	js1720@pop3.pchome.com.tw	2	14.53 KB	14.53 KB

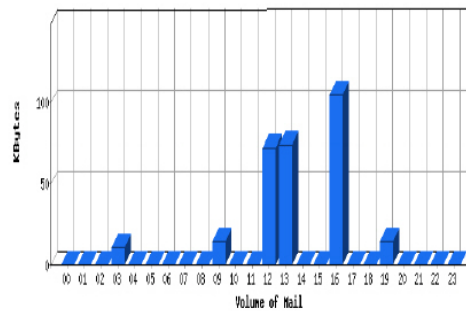
Daily Statistics Graph

圖 6-6 郵件歸檔定期報告內容第四頁



圖 6-7 郵寄歷史報告設定頁面

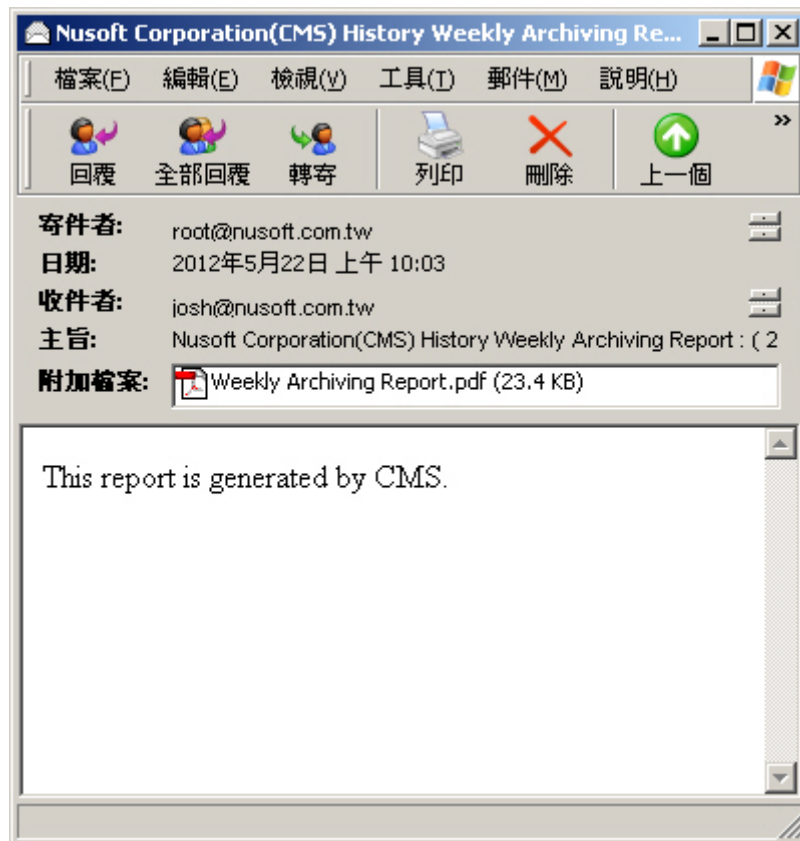


圖 6-8 收到歷史報告信件

Nusoft Corporation

Weekly Archiving Report - Inbound Mail to Local Domains

Duration : 2012/05/20~2012/05/26

Total Email

Total Count of Emails	Total Volume of Emails
648	18.92 MB

Top 20 Chart by Device (Sorted by Volume)

No.	Device Name	Count	Volume	Volume Indicator
1	254	648	18.92 MB	<div></div> 18.92 MB

Top 20 Chart by Account (Sorted by Volume)

No.	Account	Count	Volume	Volume Indicator
1	julie@nusoft.com.tw	97	3.46 MB	<div></div> 3.46 MB
2	faith@nusoft.com.tw	56	2.70 MB	<div></div> 2.70 MB
3	support@nusoft.com.tw	64	1.86 MB	<div></div> 1.86 MB
4	rayearth@nusoft.com.tw	47	1.72 MB	<div></div> 1.72 MB
5	win@nusoft.com.tw	38	1.40 MB	<div></div> 1.40 MB
6	sales@nusoft.com.tw	43	1.14 MB	<div></div> 1.14 MB
7	steve@nusoft.com.tw	44	1.02 MB	<div></div> 1.02 MB
8	support@mystudy.com.tw	27	881.35 KB	<div></div> 881.35 KB
9	justin@nusoft.com.tw	24	839.27 KB	<div></div> 839.27 KB
10	kevin@nusoft.com.tw	10	438.33 KB	<div></div> 438.33 KB
11	jack@nusoft.com.tw	12	392.99 KB	<div></div> 392.99 KB
12	interview@mystudy.com.tw	11	363.19 KB	<div></div> 363.19 KB
13	simsan@nusoft.com.tw	7	329.33 KB	<div></div> 329.33 KB
14	adfin02@nusoft.com.tw	12	320.68 KB	<div></div> 320.68 KB
15	rd@nusoft.com.tw	4	264.85 KB	<div></div> 264.85 KB
16	training@nusoft.com.tw	20	258.85 KB	<div></div> 258.85 KB
17	eunice@nusoft.com.tw	11	235.05 KB	<div></div> 235.05 KB
18	kongmeng@nusoft.com.tw	1	223.37 KB	<div></div> 223.37 KB
19	adfin01@nusoft.com.tw	3	142.15 KB	<div></div> 142.15 KB
20	josh@nusoft.com.tw	12	123.59 KB	<div></div> 123.59 KB
21	sukent@nusoft.com.tw	12	120.27 KB	<div></div> 120.27 KB
22	philip@nusoft.com.tw	9	118.66 KB	<div></div> 118.66 KB
23	kim@nusoft.com.tw	3	84.40 KB	<div></div> 84.40 KB
24	janus@nusoft.com.tw	9	83.91 KB	<div></div> 83.91 KB
25	adfin@nusoft.com.tw	11	75.58 KB	<div></div> 75.58 KB
26	alex@nusoft.com.tw	2	74.90 KB	<div></div> 74.90 KB

1

圖 6-9 郵件歸檔歷史報告內容第一頁

27	ming@nusoft.com.tw	7	59.93 KB	59.93 KB
28	owen@nusoft.com.tw	2	46.40 KB	46.40 KB
29	ms01@mystudy.com.tw	3	37.50 KB	37.50 KB
30	vmware@nusoft.com.tw	1	27.38 KB	27.38 KB
31	kobe@nusoft.com.tw	1	27.37 KB	27.37 KB
32	emmy@nusoft.com.tw	5	26.15 KB	26.15 KB
33	zhengda@nusoft.com.tw	3	15.41 KB	15.41 KB
34	cs@nusoft.com.tw	6	13.20 KB	13.20 KB
35	andrewlai@nusoft.com.tw	2	13.15 KB	13.15 KB
36	tony@nusoft.com.tw	4	12.92 KB	12.92 KB
37	root@nusoft.com.tw	4	12.76 KB	12.76 KB
38	ms03@mystudy.com.tw	1	12.35 KB	12.35 KB
39	kenny@nusoft.com.tw	2	11.69 KB	11.69 KB
40	reggie@nusoft.com.tw	6	11.63 KB	11.63 KB
41	ejufan@nusoft.com.tw	1	10.47 KB	10.47 KB
42	reggie@mystudy.com.tw	1	8.18 KB	8.18 KB
43	jackie@nusoft.com.tw	4	6.46 KB	6.46 KB
44	tcin@nusoft.com.tw	1	5.96 KB	5.96 KB
45	jameshihi@nusoft.com.tw	1	5.04 KB	5.04 KB
46	nusoft@nusoft.com.tw	2	4.66 KB	4.66 KB
47	joy@nusoft.com.tw	1	4.57 KB	4.57 KB
48	android@nusoft.com.tw	1	3.22 KB	3.22 KB

Weekly Statistics Graph

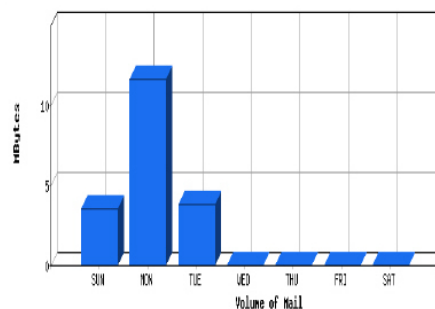


圖 6-10 郵件歸檔歷史報告內容第二頁

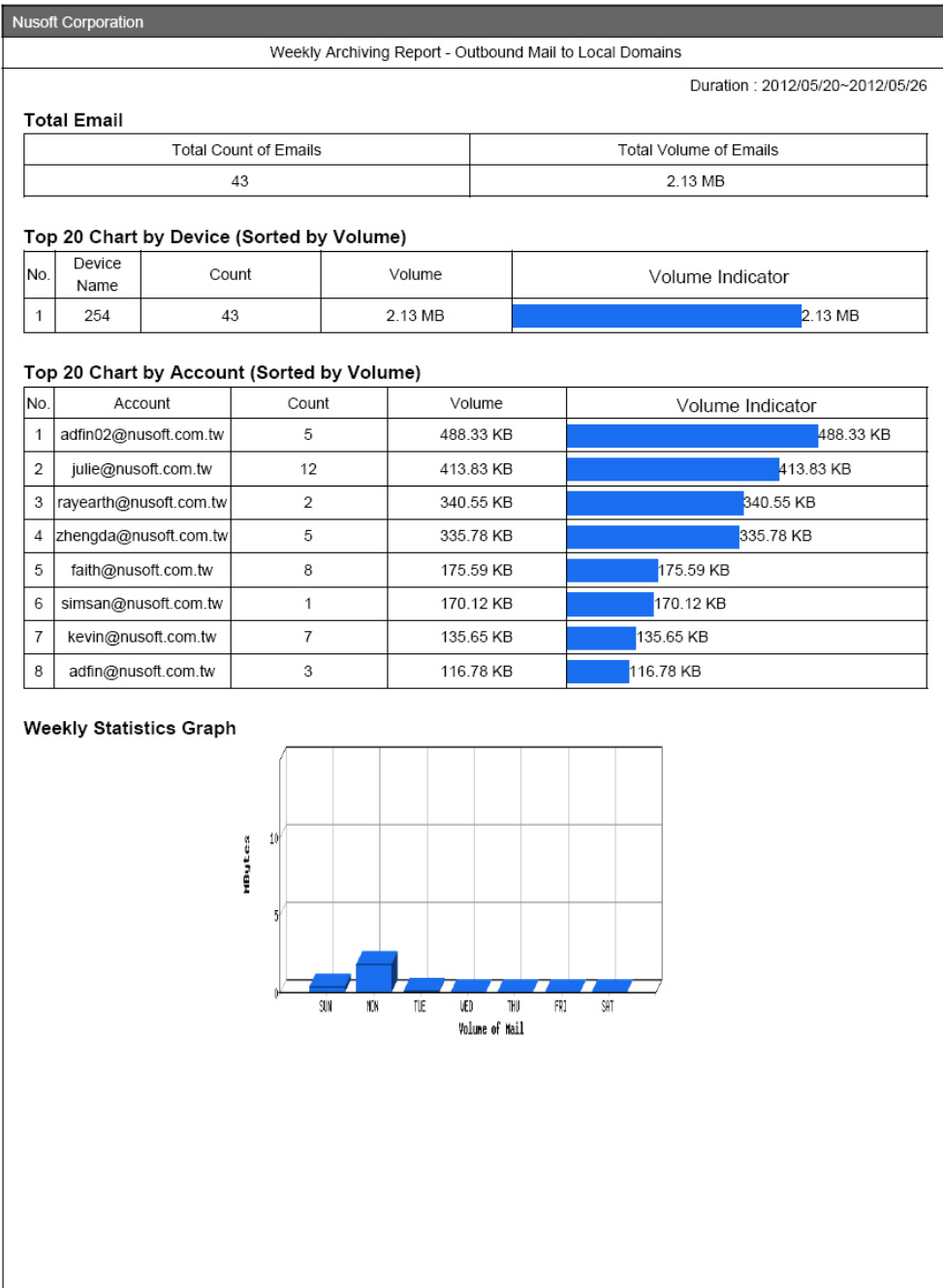



圖 6-11 郵件歸檔歷史報告內容第三頁

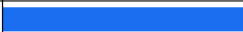
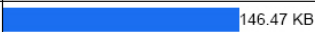

Total Email

Total Count of Emails	Total Volume of Emails
10	322.68 KB

Top 20 Chart by Device (Sorted by Volume)

No.	Device Name	Count	Volume	Volume Indicator
1	254	10	322.68 KB	 322.68 KB

Top 20 Chart by Account (Sorted by Volume)

No.	Account	Count	Volume	Volume Indicator
1	cspwen@ms36.hinet.net	4	150.75 KB	 150.75 KB
2	ranma12@ms16.hinet.net	3	146.47 KB	 146.47 KB
3	js1720@pop3.pchome.com.tw	3	25.46 KB	 25.46 KB

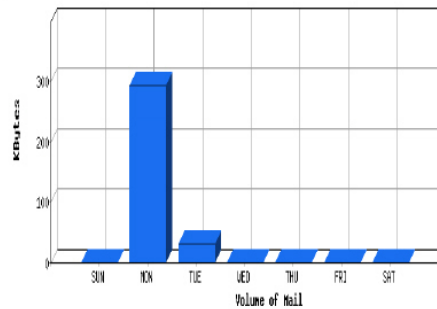
Weekly Statistics Graph

圖 6-12 郵件歸檔歷史報告內容第四頁

【歸檔】功能概述：

搜尋 說明如下：

- 可依照日期、裝置名稱、寄件者、收件者、附加檔案、主旨和處理方式等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
 - ◆ 在【本機】>【裝置監控備份】>【郵件歸檔報告】>【歸檔】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】。
 - 【收件者】輸入郵件帳號之關鍵字。
 - 選擇指定【附加檔案】、【處理方式】。
 - 按下【搜尋】鈕。（如圖 6-13）

SMTP 內送郵件 POP3
SMTP 外寄郵件

搜尋 郵件歸檔

☒ 起始 日期/時間: 2012 / 06 / 01 00 : 00
結束 日期/時間: 2012 / 06 / 10 18 : 46
裝置名稱: 所有遠端裝置
寄件者: (最多 100 個字元)
收件者: josh (最多 100 個字元)
附加檔案: 全部
主旨: (最多 100 個字元)
處理方式: 全部

搜尋

結果

2012-06-10 (1 筆記錄)

時間	遠端裝置	寄件者	收件者	主旨	處理方式
08:20:28	254	events@demand.imperv...	josh@nusoft.com.tw	- How to Defend Against Cyber Warfare	

圖 6-13 搜尋特定記錄



說明：

1. 於【本機】>【裝置監控備份】>【郵件歸檔報告】>【統計】和【歸檔】報表中，可分別選擇顯示 SMTP 內送、SMTP 外寄、POP3 郵件的審核報告。
 2. 於【本機】>【裝置監控備份】>【郵件歸檔報告】>【歸檔】報表中，按下【寄件者】郵件地址連結，可顯示【收件者列表】報告，若按下【收件者】郵件地址連結，可顯示【寄件者列表】報告。
 3. 【本機】>【裝置監控備份】>【郵件歸檔報告】>【歸檔】報表，可透過時間、寄件者、收件者、主旨或處理方式做排序的動作。【收件者列表】和【寄件者列表】，則可透過時間、寄件者或收件者、主旨或處理方式做排序的動作。
-

6.1 統計

步驟1. 在【本機】>【裝置監控備份】>【郵件歸檔報告】>【統計】頁面中，會顯示遠端 UTM 郵件歸檔的統計報表。（如圖 6-14）

- 點選【日】，可檢視以每日（Day）為單位的統計報表。
- 點選【週】，可檢視以週（Week）為單位的統計報表。
- 點選【月】，可檢視以月（Month）為單位的統計報表。
- 點選【年】，可檢視以年（Year）為單位的統計報表。

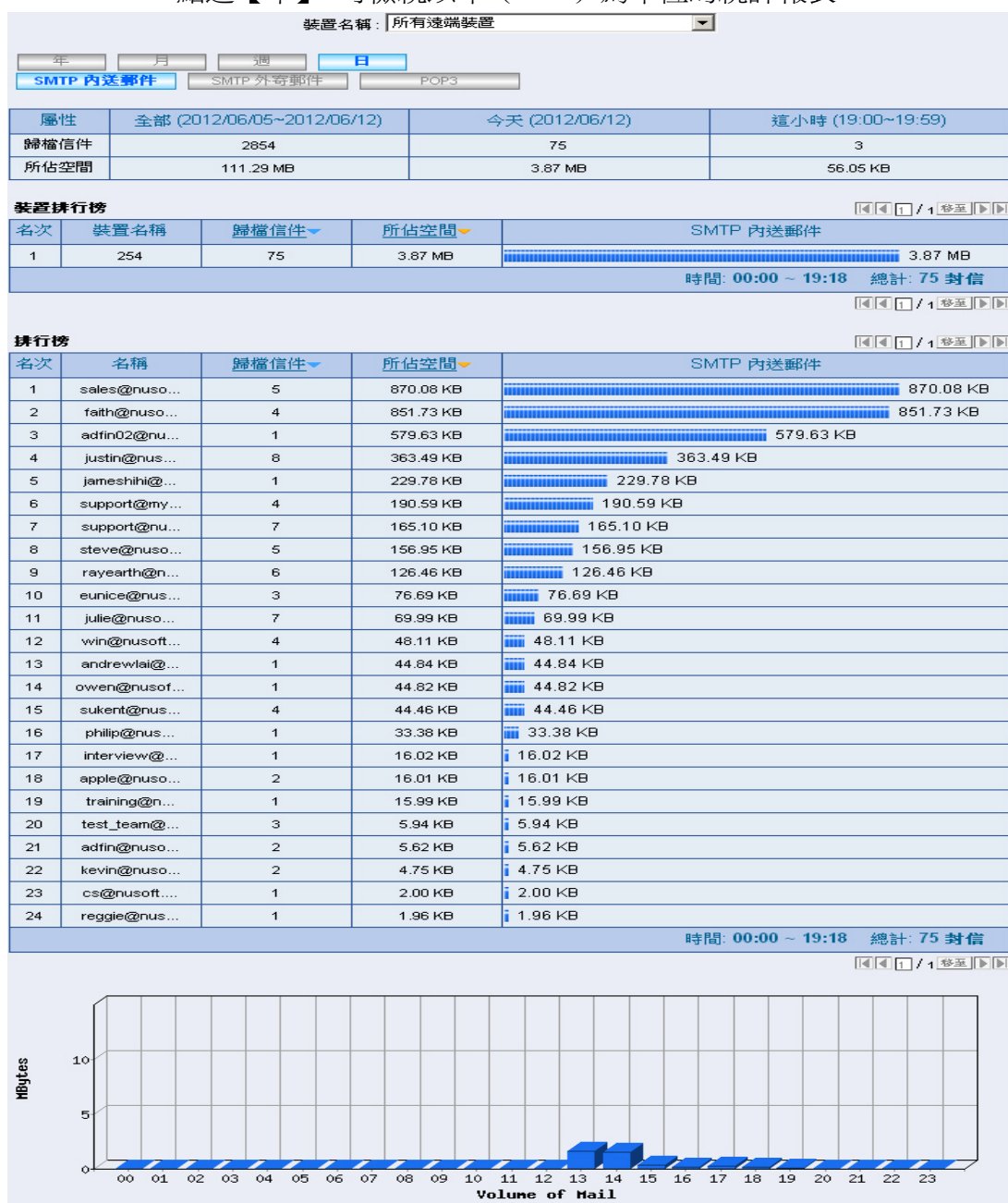


圖 6-14 郵件歸檔統計報表

6.2 歸檔

步驟1. 在【本機】>【裝置監控備份】>【郵件歸檔報告】>【歸檔】頁面中，會顯示目前遠端 UTM 郵件歸檔的狀況。(如圖 6-15)

裝置名稱: 所有遠端裝置						
<div>SMTP 內送郵件</div> <div>SMTP 外寄郵件</div> <div>POP3</div>						
2012-06-12(42 筆記錄)						
1 / 3 移至						
時間	遠端裝置	寄件者	收件者		主旨	處理方式
19:40:15	254	yam@tracking.edm.yam...	justin@nusoft.com.tw	-	【好康報你知】特選荔枝蜂蜜組 ...	
19:35:23	254	6agpukjedzp4f54in5sbie...	steve@nusoft.com.tw	-	Ciao! Up to 50% Off - Summer Sale E...	
19:23:20	254	yam@tracking.edm.yam...	philip@nusoft.com.tw	-	「關懷公益，街友慶端午」一人...	
18:03:30	254	hello@t.groupon.com.tw	justin@nusoft.com.tw	-	花蓮新開幕五星級飯店 / 高雄六星...	
18:00:25	254	clamav-users-bounces...	steve@nusoft.com.tw	-	clamav-users Digest, Vol 93, Issue 9	
17:57:31	254	soundw5@mail.cpcity.co...	julie@nusoft.com.tw	-	RE: 你好，請報價UTM1000的報價	
17:47:22	254	yam@tracking.edm.yam...	philip@nusoft.com.tw	-	寇乃馨推薦！溫控潤色粉底乳\$15...	
17:33:43	254	soundw5@mail.cpcity.co...	sales@nusoft.com.tw	-	你好，請報價UTM1000的報價	
17:05:10	254	hello@t.groupon.com.tw	justin@nusoft.com.tw	-	UNIQLO折價券 / 香蕉牛奶 / 低反發...	
17:01:43	254	bounces+23818-4346-st...	steve@nusoft.com.tw	-	Who wants to save 20+ hours worki...	
16:54:43	254	judy1219@ms64.hinet.net	julie@nusoft.com.tw		讀取: 桂圓-第一補腦的靈丹 肌肉 ...	
16:41:06	254	zqi@aolings.com	julie@nusoft.com.tw		Re: NUS-MH300	
16:27:03	254	testkevin@concept.com.t...	kevin@nusoft.com.tw	-	test c	
16:15:19	254	testkevin@perfectlink.co...	kevin@nusoft.com.tw	-	test 12345	
16:11:11	254	abramchou@ms43.url.co...	test_team@nusoft.com.tw	-	123456789	
16:08:51	254	testkevin@perfectlink.co...	test_team@nusoft.com.tw	-	test 123456789	
16:05:30	254	newsletters@techrepubl...	eunice@nusoft.com.tw	-	Five tools to keep your online reputati...	
16:04:32	254	abramchou@ms43.url.co...	test_team@nusoft.com.tw	-	qwertyuiop	
15:56:27	254	yam@tracking.edm.yam...	justin@nusoft.com.tw	-	寇乃馨推薦！溫控潤色粉底乳\$15...	
15:37:25	254	smeedmtw@em.smeefami...	ravearth@nusoft.com.tw	-	【免費活動】膳魔師、阮的肉干...	
1 / 3 移至						

圖 6-15 郵件歸檔日誌

說明：

1. 【歸檔】報表的相關圖示說明如下：

■ 處理方式：

圖例						
代表涵義	刪除	審查	延遲	歸檔	複製	傳送

第7章 網站管制報告

CMS-2000 可即時接收遠端 UTM、MHG 網站管制的結果，並做成統計報表和日誌，以便瞭解整體存取外部網站的狀況。

【設定】功能概述：

網站管制日誌設定 說明如下：

- 可指定網站管制記錄的保留時間，並於到期日刪除所有符合條件的報表。

定期報告 說明如下：

- 可依選擇的報表產生時間，定時寄送報告給收件者。

歷史報告 說明如下：

- 可產生指定日期的報表並即時郵寄給收件者。
 - ◆ 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，啟動並進行【電子郵件警告 / 報告設定】，並在【本機】>【裝置監控備份】>【網站管制報告】>【設定】頁面中，做下列設定：
 - 輸入指定網站管制日誌保留時間。
 - 在【定期報告】設定欄位中，【開啓定期報告功能】並勾選年報、月報、週報和日報。
 - 按下【確定】鈕。(如圖 7-1)
 - 當時間到達時，CMS-2000 會寄送統計報表給收件者。(如圖 7-2, 圖 7-3, 圖 7-4, 圖 7-5, 圖 7-6)
 - 在【歷史報告】設定欄位中，指定要郵寄的報告日期。
 - 按下【郵寄報告】鈕。(如圖 7-7)
 - 會即時寄送相關統計報表給收件者。(如圖 7-8, 圖 7-9, 圖 7-10, 圖 7-11, 圖 7-12)



說明：

1. 郵寄定期報告，其產生方式如下：

- 【年報】：會於每年的 1 月 1 日上午 00:15 產生。
 - 【月報】：會於每月第一天的上午 00:15 產生。
 - 【週報】：會於每週第一天的上午 00:15 產生。
 - 【日報】：會於每天的上午 00:15 產生。
-

網站管制日誌設定

保留時間 天 (範圍: 1 - 365)

定期報告 說明

☒ 開啟定期報告功能

☒ 年報 ☒ 月報 ☒ 週報 ☒ 日報

圖 7-1 網站管制日誌保留時間、郵寄定期報告設定頁面

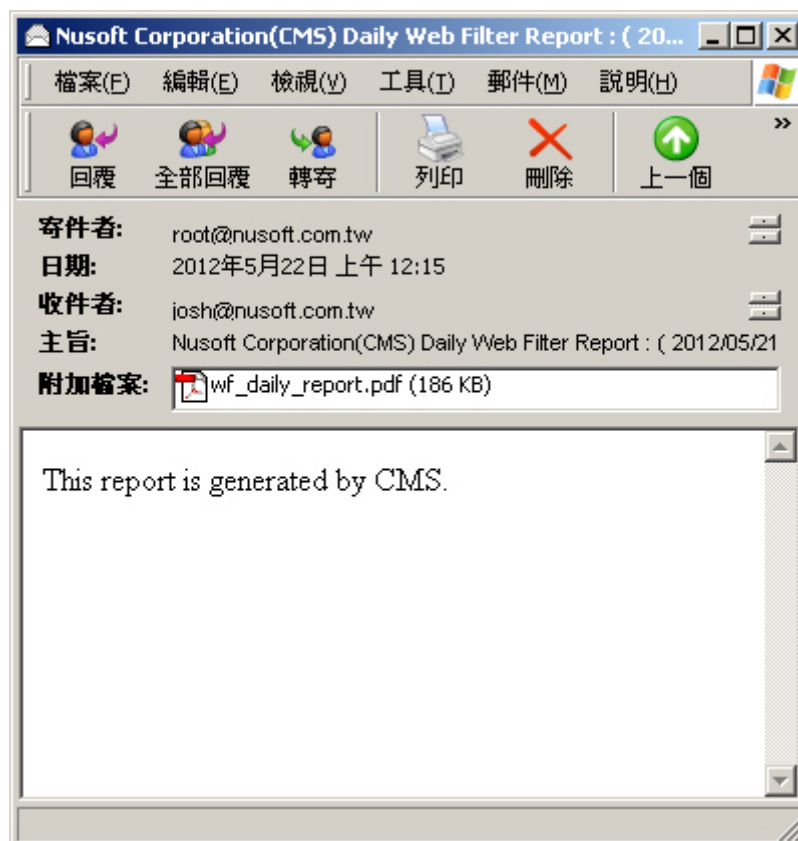


圖 7-2 收到定期報告信件

Nusoft Corporation					
Daily Web Filtering Report --- Website Category					
CMS Top Chart ■ Blocked ■ Allowed					
No.	Device Name	Blocked	Allowed	Total	Access Indicator
1	254	0	0	23172	<div style="width: 100%;"></div> 23172
Time: 2012/05/21 00:00 ~ 2012/05/21 23:59 Total: 23172 Average: 965.50 URLs/Hour					
Website Category Top Chart ■ Blocked ■ Allowed					
No.	Website Category	Blocked	Allowed	Total	Access Indicator
1	Computers & Technology	0	0	4172	<div style="width: 100%;"></div> 4172
2	Search Engines & Portals	0	0	4060	<div style="width: 100%;"></div> 4060
3	Information Security	0	0	3208	<div style="width: 100%;"></div> 3208
4	General	0	0	2178	<div style="width: 100%;"></div> 2178
5	Image Sharing	0	0	1958	<div style="width: 100%;"></div> 1958
6	Social Networking	0	0	1478	<div style="width: 100%;"></div> 1478
7	Forums & Newsgroups	0	0	905	<div style="width: 100%;"></div> 905
8	Unknown	0	0	808	<div style="width: 100%;"></div> 808
9	News	0	0	750	<div style="width: 100%;"></div> 750
10	Business	0	0	618	<div style="width: 100%;"></div> 618
11	Advertisements & Pop-Ups	0	0	590	<div style="width: 100%;"></div> 590
12	Games	0	0	366	<div style="width: 100%;"></div> 366
13	Government	0	0	349	<div style="width: 100%;"></div> 349
14	Personal Sites	0	0	296	<div style="width: 100%;"></div> 296
15	Shopping	0	0	280	<div style="width: 100%;"></div> 280
16	Entertainment	0	0	199	<div style="width: 100%;"></div> 199
17	Education	0	0	167	<div style="width: 100%;"></div> 167
18	Web-based Email	0	0	151	<div style="width: 100%;"></div> 151
19	Streaming Media & Downloads	0	0	125	<div style="width: 100%;"></div> 125
20	Finance	0	0	93	<div style="width: 100%;"></div> 93
21	Download Sites	0	0	70	<div style="width: 100%;"></div> 70
22	Travel	0	0	55	<div style="width: 100%;"></div> 55
23	Sports	0	0	54	<div style="width: 100%;"></div> 54
24	Arts	0	0	52	<div style="width: 100%;"></div> 52
25	Malware	0	0	49	<div style="width: 100%;"></div> 49
26	Fashion & Beauty	0	0	24	<div style="width: 100%;"></div> 24
27	Translators	0	0	19	<div style="width: 100%;"></div> 19
28	Chat	0	0	17	<div style="width: 100%;"></div> 17
29	Instant Messaging	0	0	17	<div style="width: 100%;"></div> 17
30	Parked Domains	0	0	14	<div style="width: 100%;"></div> 14
31	Restaurants & Dining	0	0	12	<div style="width: 100%;"></div> 12
32	Gambling	0	0	8	<div style="width: 100%;"></div> 8
33	Non-profits & NGOs	0	0	5	<div style="width: 100%;"></div> 5
34	Real Estate	0	0	5	<div style="width: 100%;"></div> 5
35	Criminal Activity	0	0	4	<div style="width: 100%;"></div> 4
36	Hacking	0	0	4	<div style="width: 100%;"></div> 4
37	Dating & Personals	0	0	3	<div style="width: 100%;"></div> 3
38	Pornography/Sexually Explicit	0	0	3	<div style="width: 100%;"></div> 3
39	Job Search	0	0	3	<div style="width: 100%;"></div> 3
40	Spam Sites	0	0	2	<div style="width: 100%;"></div> 2

1

圖 7-3 網站管制定期報告內容第一頁

41	Politics	0	0	1	1
Time: 2012/05/21 00:00 ~ 2012/05/21 23:59 Total: 23172 Average: 965.50 URLs/Hour					

Website Address Top Chart			<div></div> Blocked	<div></div> Allowed		
No.	Website Address	Blocked	Allowed	Total	Access Indicator	
1	database.clamav.net	0	1842	1842	<div></div>	1842
2	l.yimg.com	0	1086	1086	<div></div>	1086
3	203.84.192.95	0	1032	1032	<div></div>	1032
4	www.plurk.com	0	617	617	<div></div>	617
5	65.52.107.149	0	508	508	<div></div>	508
6	comet24.plurk.com	0	476	476	<div></div>	476
7	tw.yimg.com	0	444	444	<div></div>	444
8	l1.yimg.com	0	408	408	<div></div>	408
9	ap.ff.avast.com	0	386	386	<div></div>	386
10	safebrowsing.clients.goo	0	345	345	<div></div>	345
11	api.webrep.avast.com	0	343	343	<div></div>	343
12	safebrowsing-cache.google.com	0	339	339	<div></div>	339
13	www.google.com	0	330	330	<div></div>	330
14	l2.yimg.com	0	328	328	<div></div>	328
15	l3.yimg.com	0	272	272	<div></div>	272
16	www.google.com.tw	0	261	261	<div></div>	261
17	www.etax.nat.gov.tw	0	254	254	<div></div>	254
18	fxfeeds.mozilla.com	0	240	240	<div></div>	240
19	feeds2.feedburner.com	0	236	236	<div></div>	236
20	avatars.plurk.com	0	216	216	<div></div>	216
21	search.twitter.com	0	212	212	<div></div>	212
22	geo.yahoo.com	0	202	202	<div></div>	202
23	124.219.20.1	0	186	186	<div></div>	186
24	newflv.sohu.ccgslb.net	0	181	181	<div></div>	181
25	ftp.tw.debian.org	0	172	172	<div></div>	172
26	static.ak.fbcdn.net	0	171	171	<div></div>	171
27	www.google-analytics.com	0	164	164	<div></div>	164
28	www.facebook.com	0	161	161	<div></div>	161
29	119.188.27.181:8080	0	160	160	<div></div>	160
30	external.ak.fbcdn.net	0	159	159	<div></div>	159
31	nobunyaga.wasabii.com.tw	0	157	157	<div></div>	157
32	203.69.113.129	0	157	157	<div></div>	157
33	clients1.google.com	0	151	151	<div></div>	151
34	csi.gstatic.com	0	148	148	<div></div>	148
35	ad.yieldmanager.com	0	141	141	<div></div>	141
36	udn.com	0	141	141	<div></div>	141
37	newsflv.sohu.rewrite.ccg	0	141	141	<div></div>	141
38	vl.ff.avast.com	0	129	129	<div></div>	129
39	www.sophos.com	0	124	124	<div></div>	124
40	web.pts.org.tw	0	122	122	<div></div>	122
41	pagead2.googlesyndication.com	0	120	120	<div></div>	120
42	weather.noaa.gov	0	118	118	<div></div>	118
43	newsrss.bbc.co.uk	0	114	114	<div></div>	114
44	feeds.bbc.co.uk	0	113	113	<div></div>	113
45	tw.yahoo.com	0	110	110	<div></div>	110
46	googleads.g.doubleclick.net	0	105	105	<div></div>	105
Time: 2012/05/21 00:00 ~ 2012/05/21 23:59 Total: 23173 Average: 965.54 URLs/Hour						

2

圖 7-4 網站管制定期報告內容第二頁

NetBIOS Name / IP Address Top Chart					Blocked	Allowed
No.	NetBIOS Name / IP Address	Blocked	Allowed	Total	Access Indicator	
1	172.19.100.112	0	0	3766		3766
2	172.19.100.36	0	0	3274		3274
3	172.19.20.17	0	0	1995		1995
4	172.19.20.7	0	0	1253		1253
5	172.19.100.56	0	0	1203		1203
6	172.19.1.109	0	0	1076		1076
7	172.19.100.90	0	0	940		940
8	172.19.100.47	0	0	794		794
9	172.19.50.15	0	0	755		755
10	172.19.20.102	0	0	716		716
11	172.19.100.66	0	0	661		661
12	172.19.100.62	0	0	650		650
13	172.19.100.8	0	0	595		595
14	172.19.20.5	0	0	561		561
15	172.19.20.19	0	0	501		501
16	172.19.50.11	0	0	501		501
17	172.19.100.84	0	0	474		474
18	172.19.100.16	0	0	438		438
19	172.19.100.163	0	0	436		436
20	172.19.50.200	0	0	433		433
21	172.19.220.90	0	0	414		414
22	192.168.85.123	0	0	407		407
23	172.19.50.106	0	0	366		366
24	172.19.20.12	0	0	298		298
25	172.19.100.41	0	0	215		215
26	172.19.10.20	0	0	147		147
27	210.59.207.104	0	0	106		106
28	172.19.200.10	0	0	50		50
29	172.19.10.10	0	0	49		49
30	172.19.20.3	0	0	21		21
31	172.19.123.55	0	0	20		20
32	172.19.50.8	0	0	18		18
33	172.19.1.108	0	0	14		14
34	172.19.100.53	0	0	10		10
35	172.19.50.19	0	0	7		7
36	172.19.1.66	0	0	4		4
37	172.19.100.94	0	0	2		2
38	172.19.10.3	0	0	1		1
39	172.19.1.106	0	0	1		1
Time: 2012/05/21 00:00 ~ 2012/05/21 23:59					Total: 23172	Average: 965.50 URLs/Hour

圖 7-5 網站管制定期報告內容第三頁

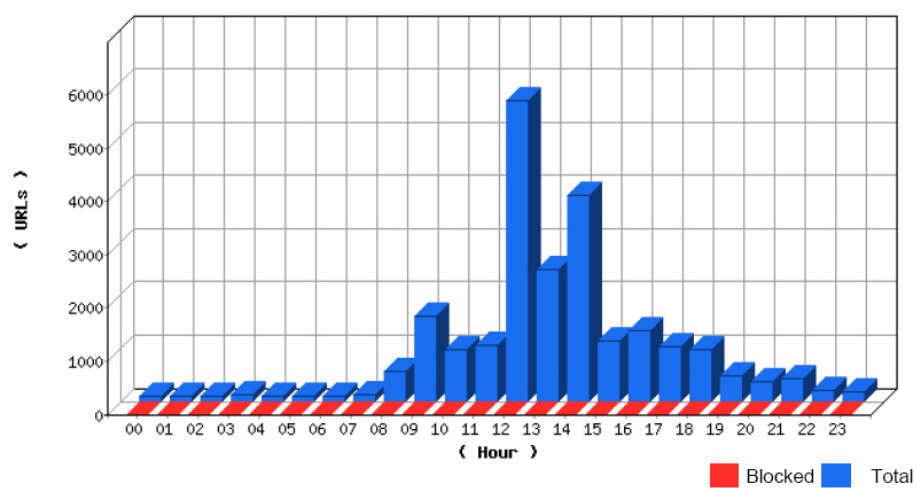


圖 7-6 網站管制定期報告內容第四頁



圖 7-7 郵寄歷史報告設定頁面

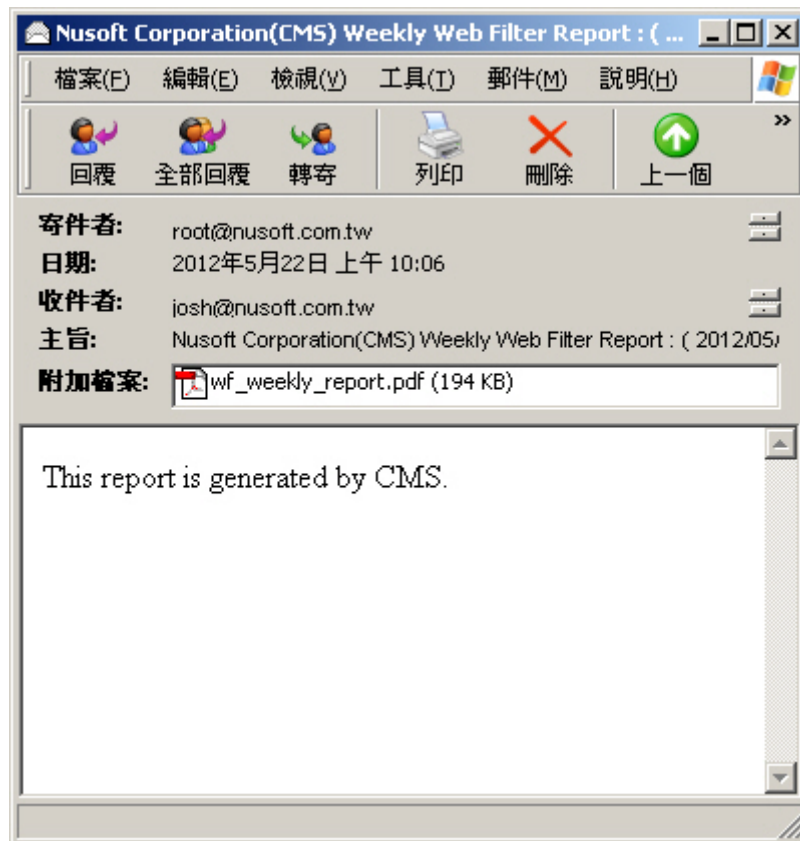



圖 7-8 收到歷史報告信件

CMS Top Chart

 Blocked
  Allowed

No.	Device Name	Blocked	Allowed	Total	Access Indicator
1	254	0	0	28935	 28935

Time: 2012/05/20(Sun) ~ 2012/05/26(Sat) Total: 28935 Average: 4133.57 URLs/Day

Website Category Top Chart

 Blocked
  Allowed







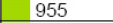
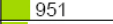
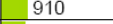
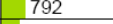
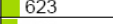
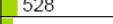
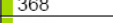
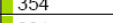


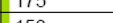
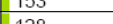






















No.	Website Category	Blocked	Allowed	Total	Access Indicator
1	Information Security	0	0	6290	 6290
2	Computers & Technology	0	0	4934	 4934
3	Search Engines & Portals	0	0	4700	 4700
4	General	0	0	2252	 2252
5	Image Sharing	0	0	2068	 2068
6	Social Networking	0	0	1574	 1574
7	Forums & Newsgroups	0	0	955	 955
8	Unknown	0	0	951	 951
9	News	0	0	910	 910
10	Business	0	0	792	 792
11	Advertisements & Pop-Ups	0	0	623	 623
12	Government	0	0	528	 528
13	Games	0	0	368	 368
14	Personal Sites	0	0	354	 354
15	Entertainment	0	0	331	 331
16	Shopping	0	0	307	 307
17	Education	0	0	175	 175
18	Web-based Email	0	0	153	 153
19	Streaming Media & Downloads	0	0	128	 128
20	Finance	0	0	93	 93
21	Download Sites	0	0	70	 70
22	Sports	0	0	65	 65
23	Arts	0	0	61	 61
24	Travel	0	0	55	 55
25	Malware	0	0	49	 49
26	Fashion & Beauty	0	0	24	 24
27	Chat	0	0	20	 20
28	Instant Messaging	0	0	20	 20
29	Translators	0	0	19	 19
30	Parked Domains	0	0	14	 14
31	Restaurants & Dining	0	0	12	 12
32	Gambling	0	0	8	 8
33	Non-profits & NGOs	0	0	5	 5
34	Real Estate	0	0	5	 5
35	Dating & Personals	0	0	4	 4
36	Criminal Activity	0	0	4	 4
37	Hacking	0	0	4	 4
38	Pornography/Sexually Explicit	0	0	3	 3
39	Job Search	0	0	3	 3
40	Spam Sites	0	0	2	 2

圖 7-9 網站管制歷史報告內容第一頁

41	Politics	0	0	1	1
42	Transportation	0	0	1	1
Time: 2012/05/20(Sun) ~ 2012/05/26(Sat) Total: 28935 Average: 4133.57 URLs/Day					

Website Address Top Chart			Blocked	Allowed		
No.	Website Address	Blocked	Allowed	Total	Access Indicator	
1	database.clamav.net	0	4392	4392	4392	
2	l.yimg.com	0	1188	1188	1188	
3	203.84.192.95	0	1032	1032	1032	
4	www.plurk.com	0	668	668	668	
5	safebrowsing.clients.goo	0	529	529	529	
6	safebrowsing-cache.google.com	0	523	523	523	
7	65.52.107.149	0	508	508	508	
8	feeds2.feedburner.com	0	488	488	488	
9	comet24.plurk.com	0	476	476	476	
10	ap.ff.avast.com	0	466	466	466	
11	tw.yimg.com	0	446	446	446	
12	l1.yimg.com	0	436	436	436	
13	fxfeeds.mozilla.com	0	423	423	423	
14	api.webrep.avast.com	0	387	387	387	
15	l2.yimg.com	0	358	358	358	
16	www.google.com	0	348	348	348	
17	www.etax.nat.gov.tw	0	320	320	320	
18	www.google.com.tw	0	316	316	316	
19	l3.yimg.com	0	302	302	302	
20	www.sophos.com	0	290	290	290	
21	web.pts.org.tw	0	251	251	251	
22	avatars.plurk.com	0	228	228	228	
23	geo.yahoo.com	0	227	227	227	
24	search.twitter.com	0	225	225	225	
25	www.google-analytics.com	0	191	191	191	
26	124.219.20.1	0	186	186	186	
27	static.ak.fbcdn.net	0	181	181	181	
28	newflv.sohu.ccsflb.net	0	181	181	181	
29	www.facebook.com	0	180	180	180	
30	vl.ff.avast.com	0	176	176	176	
31	ftp.tw.debian.org	0	172	172	172	
32	weather.noaa.gov	0	166	166	166	
33	newsrss.bbc.co.uk	0	160	160	160	
34	119.188.27.181:8080	0	160	160	160	
35	external.ak.fbcdn.net	0	159	159	159	
36	feeds.bbc.co.uk	0	158	158	158	
37	csi.gstatic.com	0	158	158	158	
38	nobunyaga.wasabii.com.tw	0	157	157	157	
39	203.69.113.129	0	157	157	157	
40	clients1.google.com	0	153	153	153	
41	pagead2.googlesyndication.com	0	146	146	146	
42	downloads.sophos.com	0	145	145	145	
43	ad.yieldmanager.com	0	144	144	144	
44	udn.com	0	141	141	141	
45	newsflv.sohu.rewrite.ccg	0	141	141	141	
Time: 2012/05/20(Sun) ~ 2012/05/26(Sat) Total: 28935 Average: 4133.57 URLs/Day						

圖 7-10 網站管制歷史報告內容第二頁

NetBIOS Name / IP Address Top Chart					Blocked	Allowed
No.	NetBIOS Name / IP Address	Blocked	Allowed	Total	Access Indicator	
1	172.19.100.112	0	0	3766		3766
2	172.19.100.36	0	0	3611		3611
3	172.19.20.17	0	0	2056		2056
4	172.19.20.7	0	0	1449		1449
5	172.19.50.15	0	0	1374		1374
6	172.19.100.56	0	0	1226		1226
7	172.19.50.11	0	0	1206		1206
8	172.19.1.109	0	0	1149		1149
9	172.19.100.163	0	0	1057		1057
10	172.19.50.200	0	0	1055		1055
11	192.168.85.123	0	0	988		988
12	172.19.100.90	0	0	983		983
13	172.19.20.102	0	0	945		945
14	172.19.100.47	0	0	822		822
15	172.19.100.62	0	0	820		820
16	172.19.100.16	0	0	760		760
17	172.19.100.66	0	0	731		731
18	172.19.100.8	0	0	725		725
19	172.19.50.106	0	0	642		642
20	172.19.20.5	0	0	580		580
21	172.19.220.90	0	0	512		512
22	172.19.20.19	0	0	501		501
23	172.19.100.84	0	0	490		490
24	172.19.10.20	0	0	356		356
25	172.19.20.12	0	0	332		332
26	172.19.100.41	0	0	217		217
27	210.59.207.104	0	0	180		180
28	172.19.10.10	0	0	99		99
29	172.19.200.10	0	0	90		90
30	172.19.20.3	0	0	67		67
31	172.19.1.108	0	0	38		38
32	172.19.100.53	0	0	26		26
33	172.19.1.66	0	0	24		24
34	172.19.123.55	0	0	20		20
35	172.19.50.8	0	0	18		18
36	172.19.50.19	0	0	7		7
37	172.19.100.94	0	0	7		7
38	172.19.10.3	0	0	3		3
39	172.19.1.106	0	0	3		3
Time: 2012/05/20(Sun) ~ 2012/05/26(Sat)					Total: 28935	Average: 4133.57 URLs/Day

圖 7-11 網站管制歷史報告內容第三頁

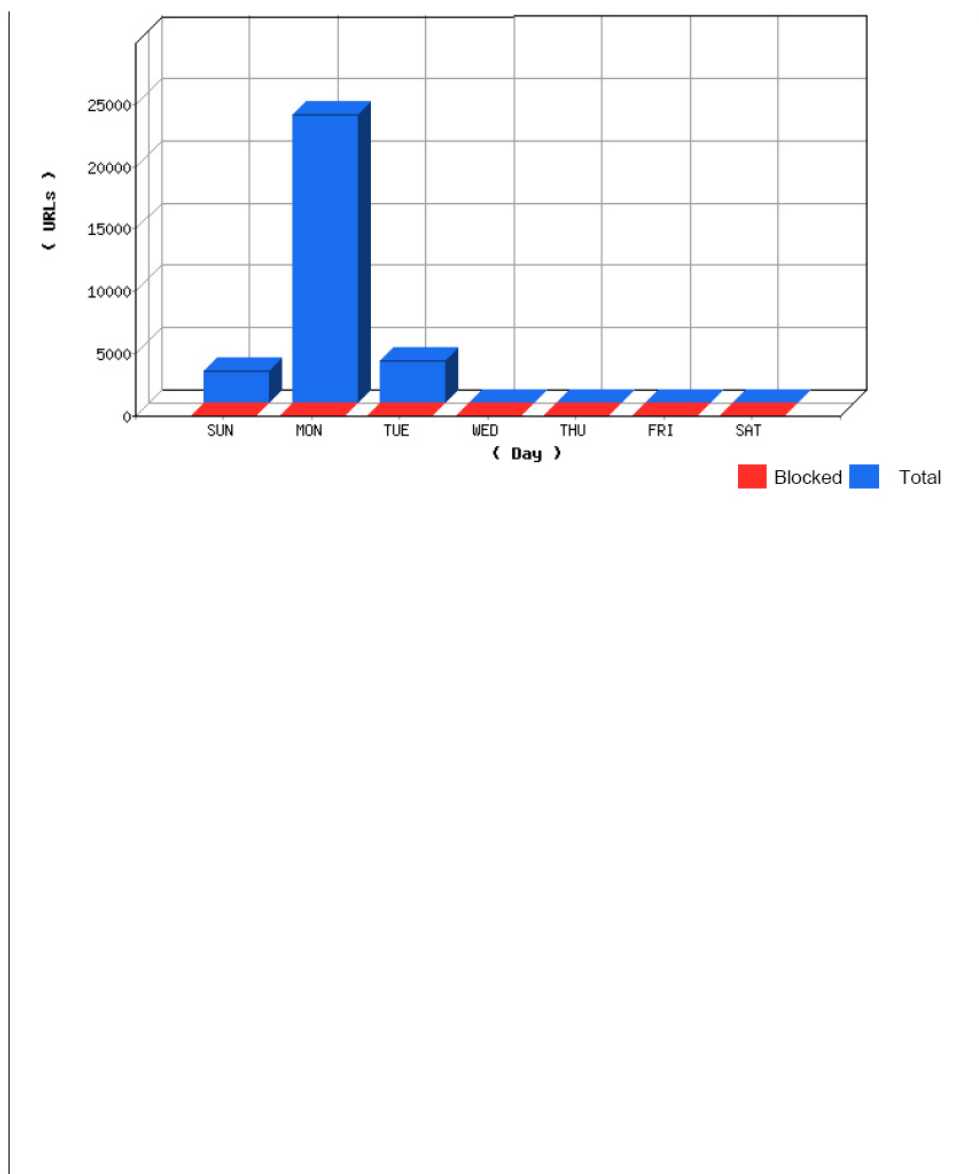


圖 7-12 網站管制歷史報告內容第四頁

【日誌】功能概述：

搜尋 說明如下：

- 網站類別：可依照日期、裝置名稱、來源位址、網址、類別和處置方式等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- 檔案傳輸（上傳）：可依照日期、裝置名稱、來源位址、網址、檔案名稱、管制規則和處置方式等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- 檔案傳輸（下載）：可依照日期、裝置名稱、來源位址、網址、檔案名稱、管制規則和處置方式等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- MIME/Script：可依照日期、裝置名稱、來源位址、網址、管制規則和處置方式等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
 - ◆ 在【本機】>【裝置監控備份】>【網站管制報告】>【日誌】的【網站類別】>【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】、【類別】、【處置方式】。
 - 按下【搜尋】鈕。（如圖 7-13）
 - 按【下載】鈕，將目前搜尋到的記錄清單即時備份到本機電腦。（如圖 7-14）

搜尋 網站類別記錄

☒ 起始 日期/時間: 2012 / 06 / 13 00 : 00
 結束 日期/時間: 2012 / 06 / 13 18 : 34
 裝置名稱: 所有遠端裝置
 來源位址: (例如: 192.168.1.10)
 網址: (最多 256 個字元)
 類別: 全部
 處置方式: 全部

搜尋

結果

2012-06-13 (19614 筆記錄) 下載

說明 1 / 981 移至

時間	遠端裝置	來源位址	網址	類別	處置方式
18:34:09	254	172.19.100.67	notify10.dropbox.com	資訊科技	✓
18:34:05	254	172.19.100.36	search.twitter.com	社交網站	✓
18:33:58	254	172.19.1.109	feeds.bbci.co.uk	新聞與媒體	✓
18:33:58	254	172.19.1.109	newsrss.bbc.co.uk	新聞與媒體	✓
18:33:58	254	172.19.1.109	fxfeeds.mozilla.com	資訊科技	✓
18:33:52	254	172.19.100.36	www.google.com	搜尋引擎與入口網路	✓
18:33:49	254	172.19.50.106	csi.gstatic.com	資訊科技, 一般	✓
18:33:49	254	172.19.50.106	translate.google.com.tw	語言翻譯	✓
18:33:26	254	172.19.100.36	emos.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:25	254	172.19.100.36	images.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:25	254	172.19.100.36	images.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:25	254	172.19.100.36	avatars.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:25	254	172.19.100.36	avatars.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:25	254	172.19.100.36	avatars.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:25	254	172.19.100.36	avatars.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:25	254	172.19.100.36	avatars.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:24	254	172.19.100.36	www.cwb.gov.tw	新聞與媒體, 政府	✓
18:33:24	254	172.19.100.36	www.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:23	254	172.19.100.36	avatars.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:32:55	254	172.19.100.36	www.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:32:46	254	172.19.20.17	djifubonholdingfund.fbs.com.tw	金融資料與服務	✓

1 / 981 移至

圖 7-13 搜尋特定記錄



說明：

1. 【本機】>【裝置監控備份】>【網站管制報告】>【日誌】的【網站類別】報表，可透過時間、來源位址、網址或類別做排序的動作。
2. 【本機】>【裝置監控備份】>【網站管制報告】>【日誌】的【檔案傳輸（上傳）】、【檔案傳輸（下載）】報表，可透過時間、來源位址、網址、檔案名稱或管制規則做排序的動作。
3. 【本機】>【裝置監控備份】>【網站管制報告】>【日誌】的【MIME/Script】報表，可透過時間、來源位址、網址或管制規則做排序的動作。

搜尋 網站類別記錄

☒ 起始 日期 / 時間: 2012 / 06 / 13 00 : 00
 結束 日期 / 時間: 2012 / 06 / 13 18 : 34
 裝置名稱: 所有遠端裝置
 來源位址: (例如: 192.168.1.10)
 網址: (最多 256 個字元)
 類別: 全部
 處置方式: 全部

搜尋

結果

2012-06-13 (19614 筆記錄) 下載

說明 1 / 981 移至

時間	遠端裝置	來源位址	網址	類別	處置方式
18:34:09	254	172.19.100.67	notify10.dropbox.com	資訊科技	✓
18:34:05	254			交網站	✓
18:33:58	254			與媒體	✓
18:33:58	254			與媒體	✓
18:33:58	254			訊科技	✓
18:33:52	254			與入口網路	✓
18:33:49	254			科技, 一般	✓
18:33:49	254			言翻譯	✓
18:33:26	254			群組, 社交網站	✓
18:33:25	254			群組, 社交網站	✓
18:33:25	254			群組, 社交網站	✓
18:33:25	254			群組, 社交網站	✓
18:33:25	254			群組, 社交網站	✓
18:33:25	254	172.19.100.36	avatars.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:25	254	172.19.100.36	avatars.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:24	254	172.19.100.36	www.cwb.gov.tw	新聞與媒體, 政府	✓
18:33:24	254	172.19.100.36	www.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:33:23	254	172.19.100.36	avatars.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:32:55	254	172.19.100.36	www.plurk.com	論壇 / 新聞群組, 社交網站	✓
18:32:46	254	172.19.20.17	djfubonholdingfund.fbs.com.tw	金融資料與服務	✓

1 / 981 移至

圖 7-14 下載搜尋到的記錄清單

7.1 統計

步驟1. 在【本機】>【裝置監控備份】>【網站管制報告】>【統計】頁面中，會顯示遠端 UTM、MHG 管制網站存取的統計報表。（如圖 7-15）

- 選擇指定【統計報表類型】。
- 點選【日】，可檢視以每日（Day）為單位的統計報表。
- 點選【週】，可檢視以週（Week）為單位的統計報表。
- 點選【月】，可檢視以月（Month）為單位的統計報表。
- 點選【年】，可檢視以年（Year）為單位的統計報表。

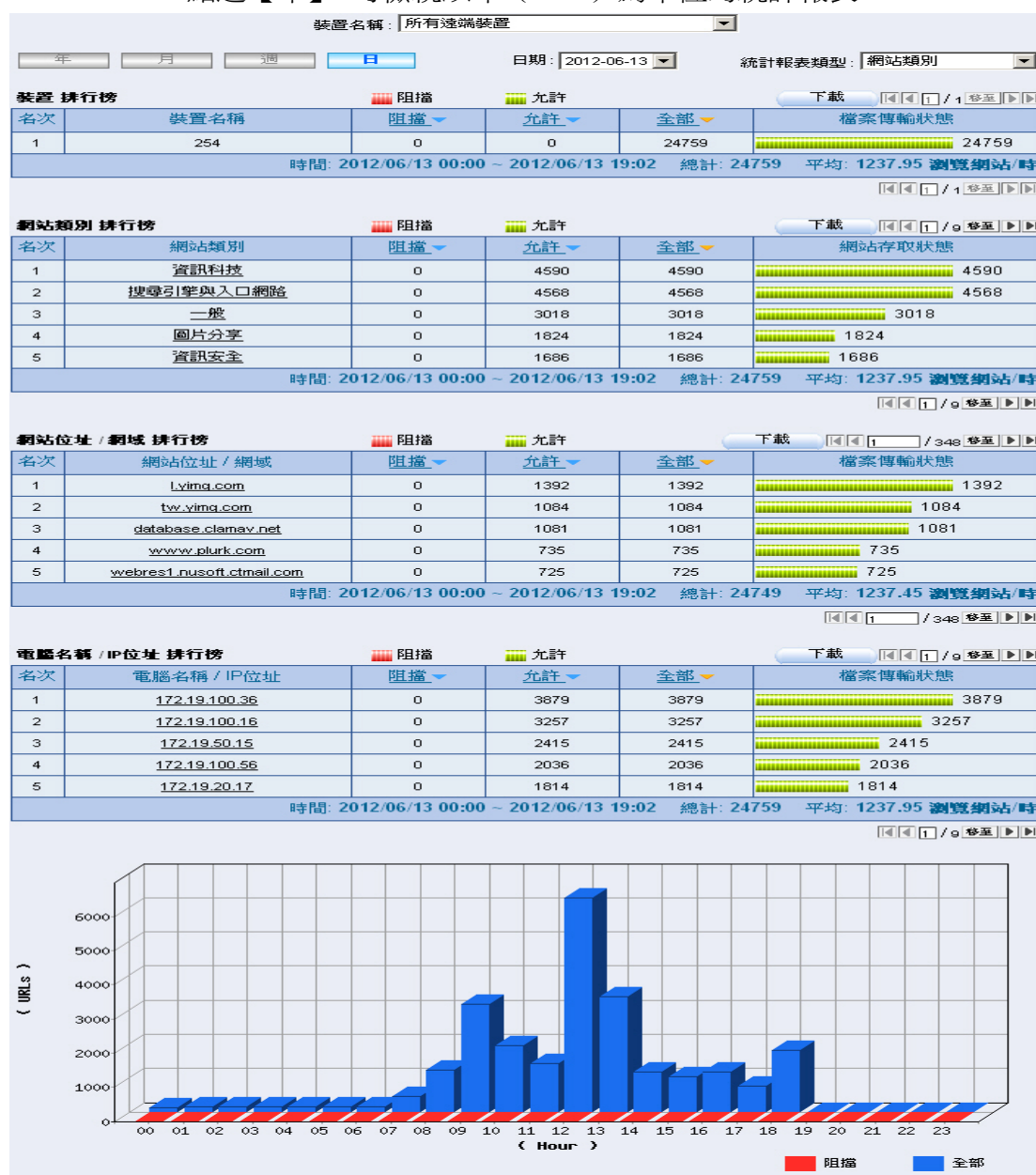


圖 7-15 網站管制統計報表

7.2 日誌

步驟1. 在【本機】>【裝置監控備份】>【網站管制報告】>【日誌】頁面中，會顯示目前遠端 UTM、MHG 的網站管制狀況。(如圖 7-16)

裝置名稱: 所有遠端裝置

統計報表類型: 網站類別 2012-06-13(20019 筆記錄)

說明

1 / 1001 移至

時間	遠端裝置	來源位址	網址	類別	處置方式
19:09:28	254	172.19.100.36	www.google.com.tw	搜尋引擎與入口網路	✓
19:09:27	254	172.19.100.41	webcache.googleusercontent.com	搜尋引擎與入口網路	✓
19:09:25	254	172.19.100.41	webcache.googleusercontent.com	搜尋引擎與入口網路	✓
19:09:24	254	172.19.100.41	webcache.googleusercontent.com	搜尋引擎與入口網路	✓
19:09:23	254	172.19.100.41	webcache.googleusercontent.com	搜尋引擎與入口網路	✓
19:09:21	254	172.19.100.41	webcache.googleusercontent.com	搜尋引擎與入口網路	✓
19:09:20	254	172.19.100.41	webcache.googleusercontent.com	搜尋引擎與入口網路	✓
19:09:19	254	172.19.100.41	www.google.com	搜尋引擎與入口網路	✓
19:09:19	254	172.19.100.41	www.google.com	搜尋引擎與入口網路	✓
19:09:19	254	172.19.100.41	webcache.googleusercontent.com	搜尋引擎與入口網路	✓
19:09:17	254	172.19.100.41	webcache.googleusercontent.com	搜尋引擎與入口網路	✓
19:09:15	254	172.19.100.63	notify10.dropbox.com	資訊科技	✓
19:09:13	254	172.19.1.109	clients1.google.com	搜尋引擎與入口網路	✓
19:09:13	254	172.19.1.109	clients1.google.com	搜尋引擎與入口網路	✓
19:09:09	254	172.19.100.36	search.twitter.com	社交網站	✓
19:08:54	254	172.19.100.36	www.plurk.com	論壇 / 新聞群組, 社交網站	✓
19:08:21	254	172.19.100.41	feeds2.feedburner.com	資訊科技, 商業	✓
19:08:21	254	172.19.100.41	web.pts.org.tw	娛樂	✓
19:08:21	254	172.19.100.41	safebrowsing-cache.google.com	搜尋引擎與入口網路	✓
19:08:21	254	172.19.100.41	fxfeeds.mozilla.com	資訊科技	✓

1 / 1001 移至

圖 7-16 網站管制日誌

第8章 入侵防禦報告

CMS-2000 可即時接收遠端 UTM 入侵偵測防禦的結果，並做成統計報表和日誌，以便瞭解整體網路資料傳輸的安全性。

【設定】功能概述：

入侵偵測防禦日誌設定 說明如下：

- 可指定入侵偵測防禦記錄的保留時間，並於到期日刪除所有符合條件的報表。

定期報告 說明如下：

- 可依選擇的報表產生時間，定時寄送報告給收件者。

歷史報告 說明如下：

- 可產生指定日期的報表並即時郵寄給收件者。
 - ◆ 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，啟動並進行【電子郵件警告 / 報告設定】，並在【本機】>【裝置監控備份】>【入侵防禦報告】>【設定】頁面中，做下列設定：
 - 輸入指定入侵偵測防禦日誌保留時間。
 - 在【定期報告】設定欄位中，【開啓定期報告功能】並勾選年報、月報、週報和日報。
 - 按下【確定】鈕。(如圖 8-1)
 - 當時間到達時，CMS-2000 會寄送統計報表給收件者。(如圖 8-2, 圖 8-3, 圖 8-4)
 - 在【歷史報告】設定欄位中，指定要郵寄的報告日期。
 - 按下【郵寄報告】鈕。(如圖 8-5)
 - 會即時寄送相關統計報表給收件者。(如圖 8-6, 圖 8-7, 圖 8-8)



說明：

1. 郵寄定期報告，其產生方式如下：

- 【年報】：會於每年的 1 月 1 日上午 00:30 產生。
 - 【月報】：會於每月第一天的上午 00:30 產生。
 - 【週報】：會於每週第一天的上午 00:30 產生。
 - 【日報】：會於每天的上午 00:30 產生。
-

入侵偵測防禦日誌設定

保留時間 天 (範圍: 1 - 365)

定期報告 說明

☒ 開啟定期報告功能

☒ 年報 ☒ 月報 ☒ 週報 ☒ 日報

圖 8-1 入侵偵測防禦日誌保留時間、郵寄定期報告設定頁面

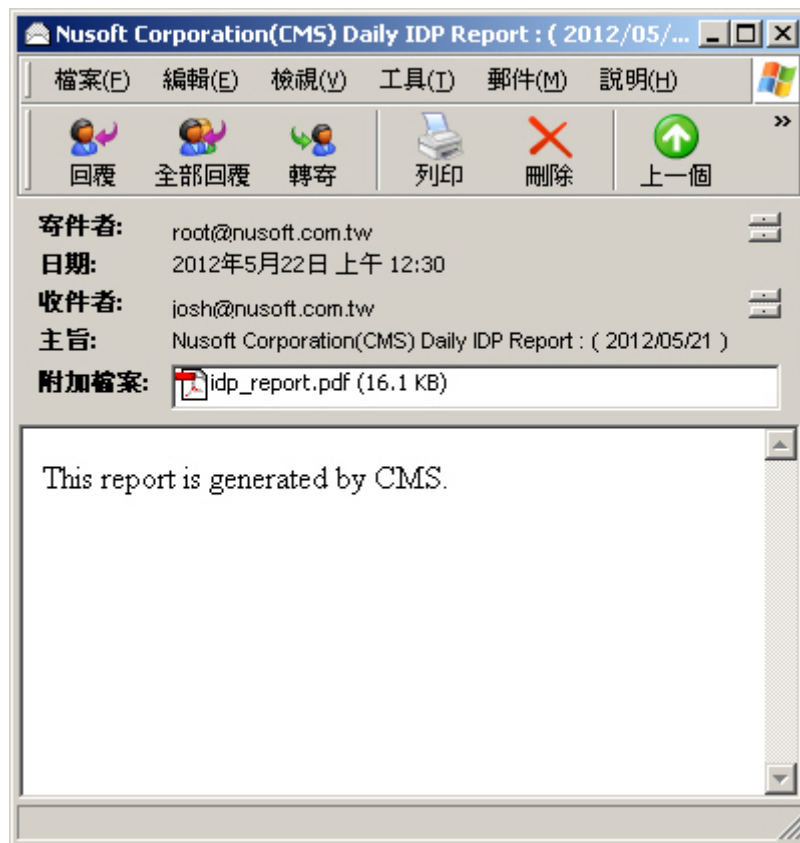


圖 8-2 收到定期報告信件

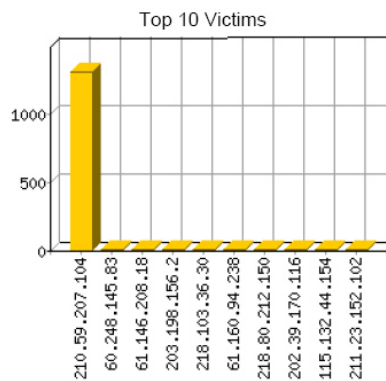
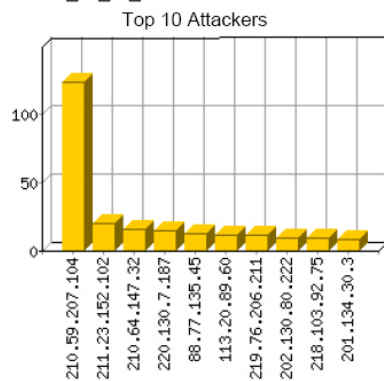
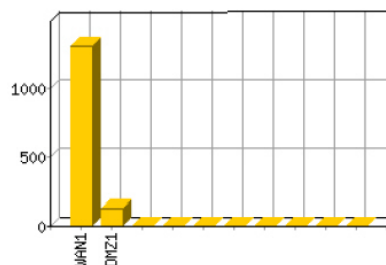
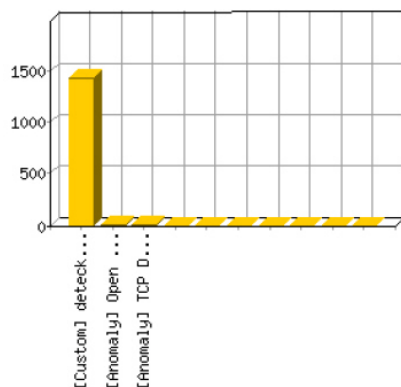
Duration	2012-05-21 00:00:00 ~ 2012-05-21 23:59:59					
Total No. of Attacks	1439					
Time of First Attack	2012-05-21 00:00:04		Time of Last Attack		2012-05-21 23:59:04	
No. of Attackers	728		No. of Victims		113	
Protocol (of attack)	TCP	639	UDP	796	ICMP	4

Top CMS Chart ■ Allowed ■ Dropped ■ Rejected

No.	Device Name	Allowed	Dropped	Rejected	No. of Attacks
1	254	1439	0	0	1439

Top Signature Chart ■ Allowed ■ Dropped ■ Rejected

No.	Signature Category	Allowed	Dropped	Rejected	No. of Attacks
1	Custom	1437	0	0	1437
2	Anomaly	2	0	0	2



Total Statistics

圖 8-3 入侵防禦定期報告內容第一頁

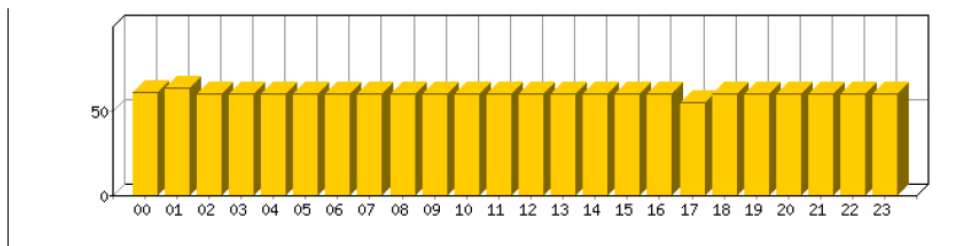


圖 8-4 入侵防禦定期報告內容第二頁



圖 8-5 郵寄歷史報告設定頁面

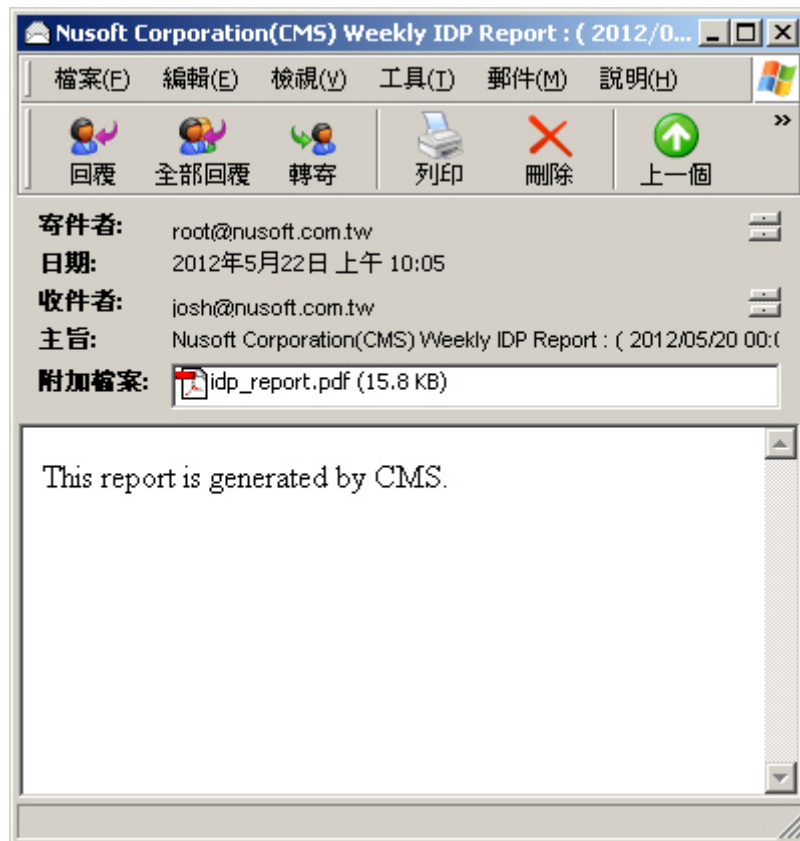


圖 8-6 收到歷史報告信件

Weekly IDP Report

Duration	2012-05-20 00:00:00 ~ 2012-05-26 23:59:59					
Total No. of Attacks	3492					
Time of First Attack	2012-05-20 00:00:04		Time of Last Attack		2012-05-22 10:04:08	
No. of Attackers	1264		No. of Victims		275	
Protocol (of attack)	TCP	1760	UDP	1715	ICMP	17

Top CMS Chart



Allowed



Dropped



Rejected

No.	Device Name	Allowed	Dropped	Rejected	No. of Attacks
1	254	3492	0	0	3492

Top Signature Chart



Allowed

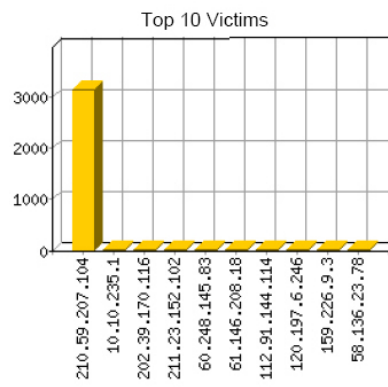
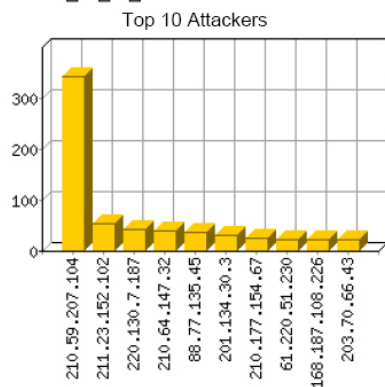
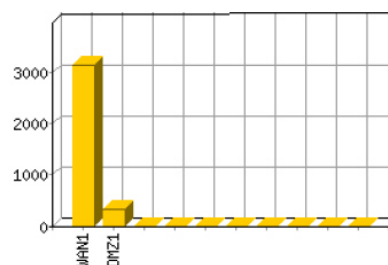
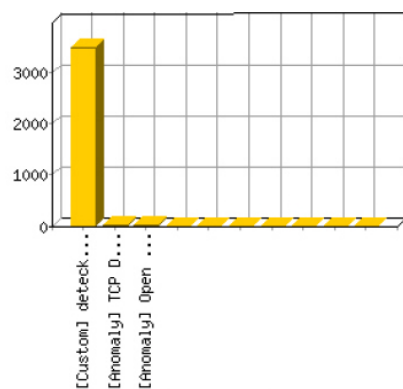


Dropped



Rejected

No.	Signature Category	Allowed	Dropped	Rejected	No. of Attacks
1	Custom	3486	0	0	3486
2	Anomaly	6	0	0	6



Total Statistics

圖 8-7 入侵防禦歷史報告內容第一頁

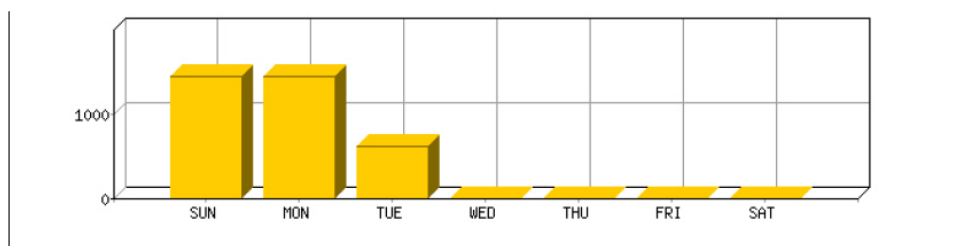


圖 8-8 入侵防禦歷史報告內容第二頁

【日誌】功能概述：

搜尋 說明如下：

- 可依照日期、裝置名稱、攻擊事件、特徵類型、攻擊地址、被攻擊地址、攻擊發生介面和風險等級等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
 - ◆ 在【本機】>【裝置監控備份】>【入侵防禦報告】>【日誌】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】。
 - 輸入異常封包和攻擊行為所屬之【攻擊事件】關鍵字。
 - 選擇指定【攻擊發生介面】、【風險等級】。
 - 按下【搜尋】鈕。（如圖 8-9）

搜索 入侵防禦報告

☒ 起始日期/時間: 2012 / 06 / 05 14 : 19
結束日期/時間: 2012 / 06 / 14 11 : 46
裝置名稱: 所有遠端裝置
攻擊事件: TCP (最多 255 個字元)
特徵類型: (最多 20 個字元)
攻擊地址:
被攻擊地址:
攻擊發生介面: 全部
風險等級: 全部

搜尋

結果

2012-06-06 (2 筆記錄)

時間	遠端裝置	攻擊事件	攻擊發生介面	攻擊地址	被攻擊地址	處理動作
11:16:08	254	[Anomaly] TCP Decoy Portscan	WAN1	122.224.3.212	210.59.207.104	✓
01:02:09	254	[Anomaly] TCP Decoy Portscan	WAN1	114.35.34.4	210.59.207.104	✓

圖 8-9 搜尋特定記錄



說明：

1. 【本機】>【裝置監控備份】>【入侵防禦報告】>【日誌】報表，可透過時間、攻擊事件、攻擊發生介面、攻擊地址、被攻擊地址或處理動作來排序。

8.1 統計

步驟1. 在【本機】>【裝置監控備份】>【入侵防禦報告】>【統計】頁面中，會顯示遠端 UTM 入侵偵測防禦的統計報表。(如圖 8-10)

- 點選【日】，可檢視以每日 (Day) 為單位的統計報表。
- 點選【週】，可檢視以週 (Week) 為單位的統計報表。
- 點選【月】，可檢視以月 (Month) 為單位的統計報表。
- 點選【年】，可檢視以年 (Year) 為單位的統計報表。

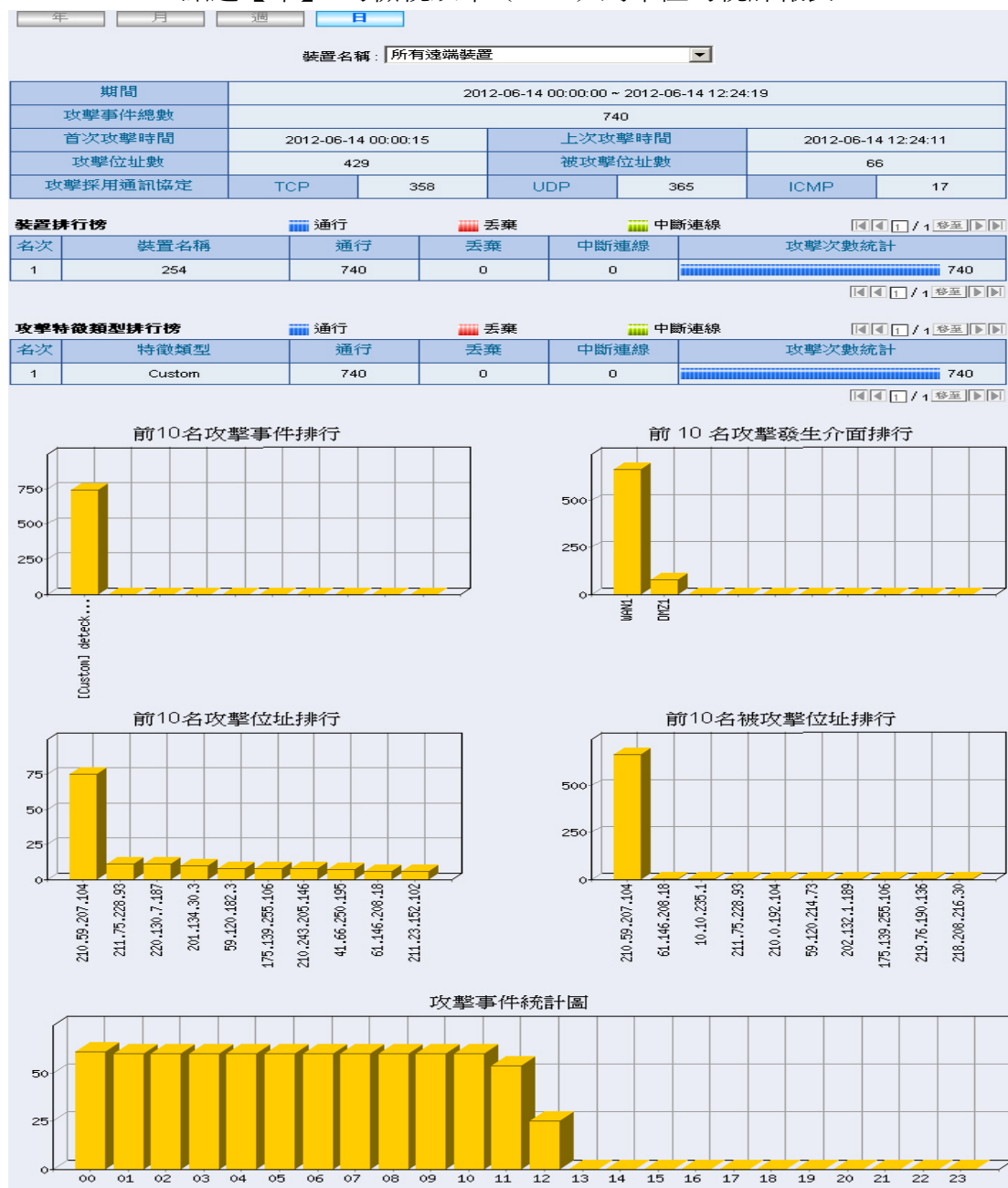


圖 8-10 入侵偵測防禦統計報表

8.2 日誌

步驟1. 在【本機】>【裝置監控備份】>【入侵防禦報告】>【日誌】頁面中，會顯示目前遠端 UTM 入侵偵測防禦的處理狀況。(如圖 8-11)

裝置名稱: 所有遠端裝置

2012-06-06 (1428 筆記錄)

34 / 72 移至

時間	遠端裝置	攻擊事件	攻擊發生介面	攻擊地址	被攻擊地址	處理動作
11:14:03	254	[Custom] deteck_all	WAN1	210.177.154.67	210.59.207.104	✓
11:15:03	254	[Custom] deteck_all	WAN1	59.148.196.232	210.59.207.104	✓
11:16:03	254	[Custom] deteck_all	WAN1	60.250.107.103	210.59.207.104	✓
11:16:08	254	[Anomaly] TCP Decoy Portscan	WAN1	122.224.3.212	210.59.207.104	✓
11:16:08	254	[Anomaly] Open Port	WAN1	122.224.3.212	210.59.207.104	✓
11:16:08	254	[Custom] deteck_all	WAN1	122.224.3.212	210.59.207.104	✓
11:17:03	254	[Custom] deteck_all	WAN1	59.125.43.223	210.59.207.104	✓
11:18:03	254	[Custom] deteck_all	WAN1	112.91.144.114	210.59.207.104	✓
11:19:03	254	[Custom] deteck_all	WAN1	59.148.196.232	210.59.207.104	✓
11:20:03	254	[Custom] deteck_all	WAN1	210.242.144.39	210.59.207.104	✓
11:21:03	254	[Custom] deteck_all	WAN1	60.251.181.16	210.59.207.104	✓
11:22:03	254	[Custom] deteck_all	WAN1	202.64.34.230	210.59.207.104	✓
11:23:03	254	[Custom] deteck_all	WAN1	175.143.49.165	210.59.207.104	✓
11:24:03	254	[Custom] deteck_all	WAN1	125.234.240.26	210.59.207.104	✓
11:25:03	254	[Custom] deteck_all	WAN1	202.82.19.249	210.59.207.104	✓
11:26:03	254	[Custom] deteck_all	WAN1	211.25.251.38	210.59.207.104	✓
11:27:03	254	[Custom] deteck_all	WAN1	211.144.213.227	210.59.207.104	✓
11:28:03	254	[Custom] deteck_all	WAN1	175.139.170.94	210.59.207.104	✓
11:29:03	254	[Custom] deteck_all	WAN1	59.59.54.138	210.59.207.104	✓
11:30:03	254	[Custom] deteck_all	WAN1	218.4.75.90	210.59.207.104	✓

34 / 72 移至

圖 8-11 入侵偵測防禦日誌

說明：

1. 【日誌】報表的相關圖示說明如下：

■ 動作：

圖例	✓	✗
代表涵義	通行	丟棄、中斷連線

■ 風險：

圖例	H	M	L
代表涵義	高風險	中風險	低風險

第9章 網頁應用程式報告

CMS-2000 可即時接收遠端 UTM 網頁應用程式攻擊處理的結果，並做成統計報表和日誌，以便瞭解整體對外服務網站的安全性。

【設定】功能概述：

網頁應用程式防火牆日誌設定 說明如下：

- 可指定網頁應用程式防火牆記錄的保留時間，並於到期日刪除所有符合條件的報表。

定期報告 說明如下：

- 可依選擇的報表產生時間，定時寄送報告給收件者。

歷史報告 說明如下：

- 可產生指定日期的報表並即時郵寄給收件者。
 - ◆ 在【本機】>【系統管理】>【組態】>【系統設定】頁面中，啟動並進行【電子郵件警告 / 報告設定】，並在【本機】>【裝置監控備份】>【網頁應用程式報告】>【設定】頁面中，做下列設定：
 - 輸入指定網頁應用程式防火牆日誌保留時間。
 - 在【定期報告】設定欄位中，【開啓定期報告功能】並勾選年報、月報、週報和日報。
 - 按下【確定】鈕。(如圖 9-1)
 - 當時間到達時，CMS-2000 會寄送統計報表給收件者。(如圖 9-2, 圖 9-3, 圖 9-4)
 - 在【歷史報告】設定欄位中，指定要郵寄的報告日期。
 - 按下【郵寄報告】鈕。(如圖 9-5)
 - 會即時寄送相關統計報表給收件者。(如圖 9-6, 圖 9-7, 圖 9-8)



說明：

1. 郵寄定期報告，其產生方式如下：

- 【年報】：會於每年的 1 月 1 日上午 00:30 產生。
 - 【月報】：會於每月第一天的上午 00:30 產生。
 - 【週報】：會於每週第一天的上午 00:30 產生。
 - 【日報】：會於每天的上午 00:30 產生。
-

網頁應用程式防火牆日誌設定

保留時間 天 (範圍: 1 - 365)

定期報告 說明

☒ 開啟定期報告功能

☒ 年報 ☒ 月報 ☒ 週報 ☒ 日報

圖 9-1 網頁應用程式防火牆日誌保留時間、郵寄定期報告設定頁面

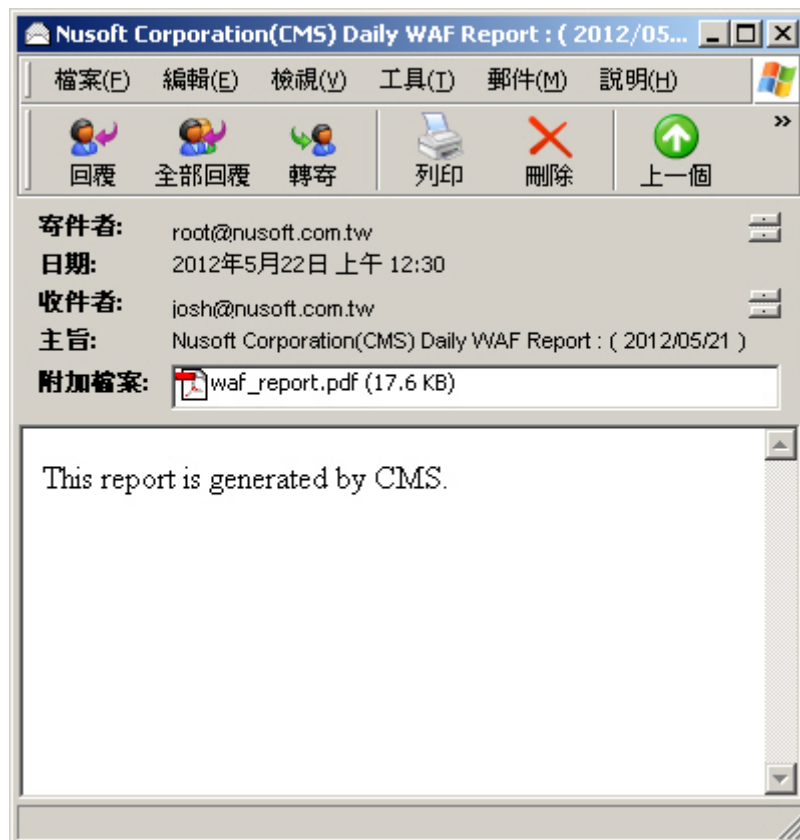


圖 9-2 收到定期報告信件

Daily WAF Report

Duration	2012-05-21 00:00:00 ~ 2012-05-21 23:59:59		
Total No. of Attacks	1326		
No. of Attackers	457	No. of URLs	545
Time of First Attack	2012-05-21 00:02:11	Time of Last Attack	2012-05-21 23:59:27

Top CMS Chart

Allowed

Dropped

No.	Device Name	Allowed	Dropped	No. of Attacks
1	254	1326	0	1326

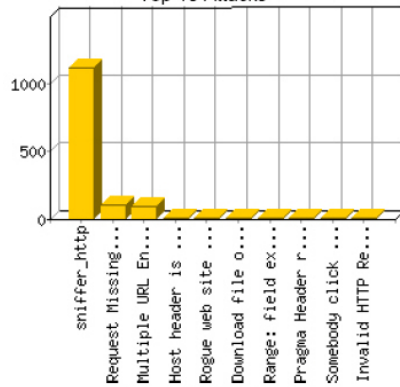
Top Signature Chart

Allowed

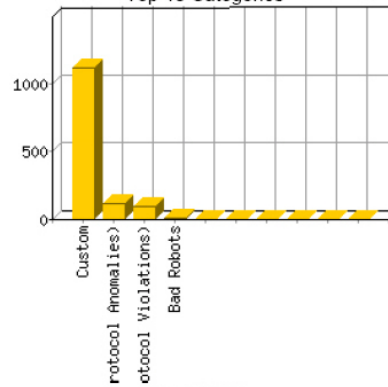
Dropped

No.	Signature Category	Allowed	Dropped	No. of Attacks
1	Custom	1123	0	1123
2	Bad Protocols (Protocol Anomalies)	109	0	109
3	Bad Protocols (Protocol Violations)	91	0	91
4	Bad Robots	3	0	3

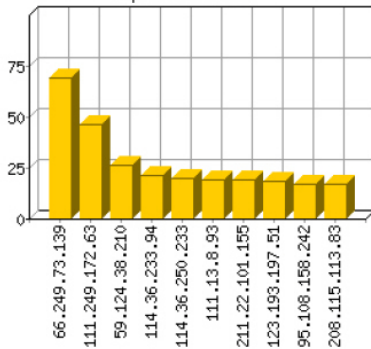
Top 10 Attacks



Top 10 Categories



Top 10 Attackers



Top 10 URLs

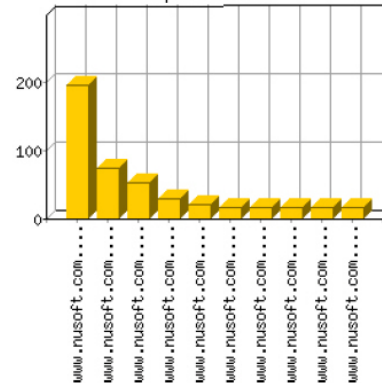


圖 9-3 網頁應用程式定期報告內容第一頁

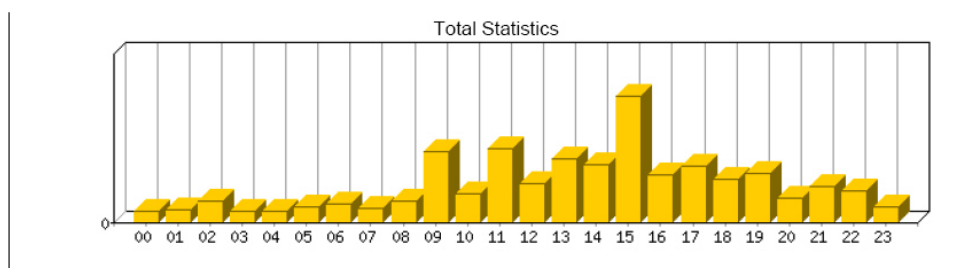


圖 9-4 網頁應用程式定期報告內容第二頁



圖 9-5 郵寄歷史報告設定頁面

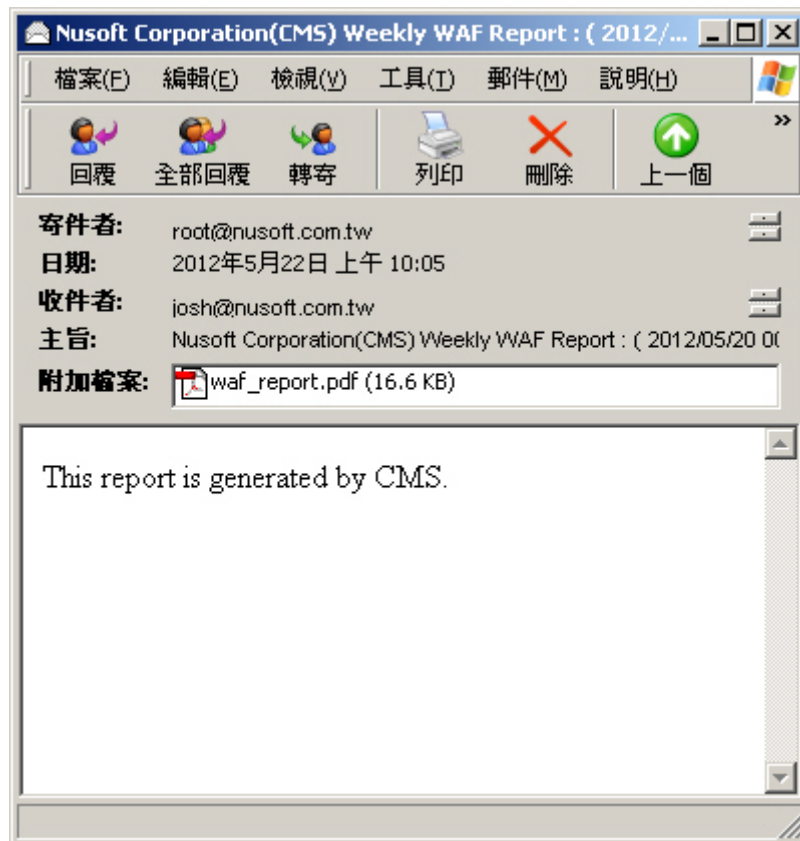


圖 9-6 收到歷史報告信件

Duration	2012-05-20 00:00:00 ~ 2012-05-26 23:59:59		
Total No. of Attacks	2685		
No. of Attackers	801	No. of URLs	1033
Time of First Attack	2012-05-20 00:01:52	Time of Last Attack	2012-05-22 10:05:12

Top CMS Chart



Allowed



Dropped

No.	Device Name	Allowed	Dropped	No. of Attacks
1	254	2685	0	2685

Top Signature Chart



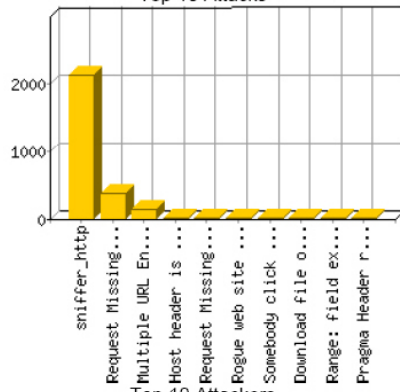
Allowed



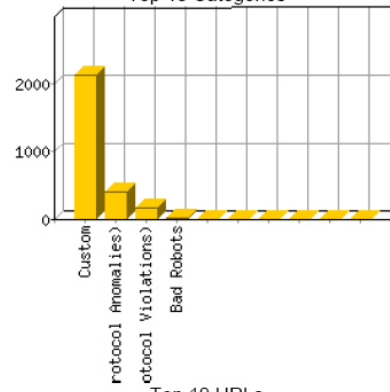
Dropped

No.	Signature Category	Allowed	Dropped	No. of Attacks
1	Custom	2136	0	2136
2	Bad Protocols (Protocol Anomalies)	392	0	392
3	Bad Protocols (Protocol Violations)	153	0	153
4	Bad Robots	4	0	4

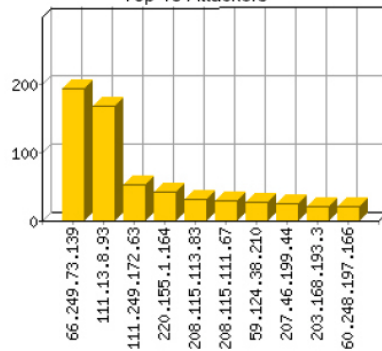
Top 10 Attacks



Top 10 Categories



Top 10 Attackers



Top 10 URLs

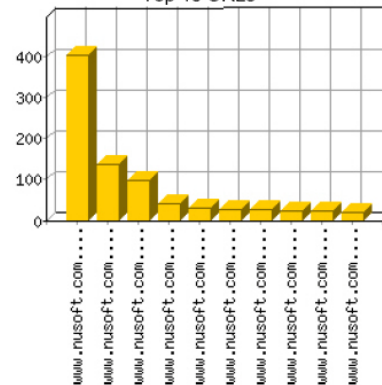


圖 9-7 網頁應用程式歷史報告內容第一頁

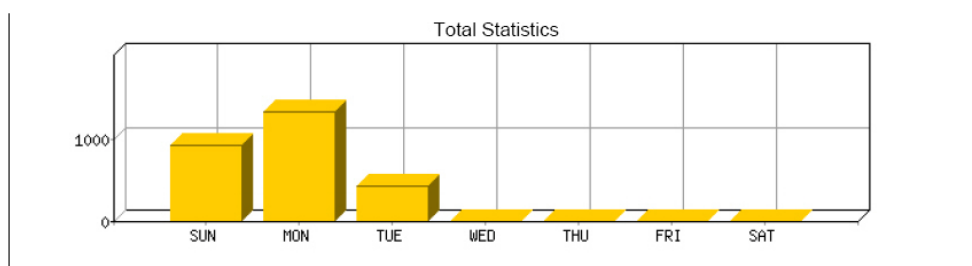


圖 9-8 網頁應用程式歷史報告內容第二頁

【日誌】功能概述：

搜尋 說明如下：

■ 可依照日期、裝置名稱、攻擊位址、連線網址、特徵類型和攻擊事件等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。

◆ 在【本機】>【裝置監控備份】>【網頁應用程式報告】>【日誌】的【搜尋】頁面中，做下列設定：

- 開啓並設定搜尋指定時間區間內的記錄。
- 選擇指定【裝置名稱】。
- 輸入攻擊行為所屬之【特徵類型】關鍵字。
- 按下【搜尋】鈕。(如圖 9-9)

搜尋

☒ 起始 日期/時間: 2012 / 06 / 05 14 : 19
結束 日期/時間: 2012 / 06 / 14 19 : 07
裝置名稱: 所有遠端裝置
攻擊位址:
連線網址: (最多 255 個字元)
特徵類型: Violations
攻擊事件: (最多 255 個字元)

搜尋

結果

2012-06-07 (82 筆記錄)

時間	遠端裝置	攻擊位址	連線網址	特徵類型	攻擊事件	處理動作
23:45:01	254	123.110.149.195	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
23:41:04	254	125.230.196.248	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
23:03:33	254	123.125.71.40	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
23:00:24	254	157.55.17.103	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
22:57:25	254	220.133.3.14	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
22:44:04	254	1.34.56.32	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
22:26:18	254	203.77.53.68	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
22:21:58	254	203.77.53.68	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
22:07:34	254	219.68.152.192	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
22:05:03	254	118.171.193.182	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
21:01:40	254	163.13.154.108	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
20:21:05	254	114.32.108.121	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
20:11:33	254	210.242.65.49	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
19:16:05	254	112.104.56.174	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
19:12:27	254	124.115.0.27	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
18:59:59	254	111.248.165.191	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
18:43:18	254	220.131.169.238	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
18:32:50	254	65.52.108.12	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
18:31:49	254	65.52.108.66	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓
18:25:10	254	220.135.48.93	http://www.nusoft.com.t...	Bad Protocols (Pr...	Multiple URL Encoding D...	✓

圖 9-9 搜尋特定記錄



說明：

1. 【本機】>【裝置監控備份】>【網頁應用程式報告】>【日誌】報表，可透過時間、攻擊位址、連線網址、特徵類型、攻擊事件或處理動作來排序。

9.1 統計

步驟1. 在【本機】>【裝置監控備份】>【網頁應用程式報告】>【統計】頁面中，會顯示遠端 UTM 網頁應用程式防火牆的統計報表。（如圖 9-10）

- 點選【日】，可檢視以每日（Day）為單位的統計報表。
- 點選【週】，可檢視以週（Week）為單位的統計報表。
- 點選【月】，可檢視以月（Month）為單位的統計報表。
- 點選【年】，可檢視以年（Year）為單位的統計報表。



圖 9-10 網頁應用程式防火牆統計報表

9.2 日誌

步驟1. 在【本機】>【裝置監控備份】>【網頁應用程式報告】>【日誌】頁面中，會顯示目前遠端 UTM 網頁應用程式防火牆的處理狀況。(如圖 9-11)

裝置名稱: 所有遠端裝置

2012-06-14 (1319 筆記錄)

1 / 66 移至

時間	遠端裝置	攻擊位址	連線網址	特徵類型	攻擊事件	處理動作
20:43:23	254	66.249.71.73	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:42:38	254	180.153.240.70	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:38:01	254	163.29.86.210	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:36:35	254	123.125.71.14	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:35:47	254	124.115.0.159	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:32:24	254	180.153.240.70	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:32:14	254	124.115.0.162	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:31:26	254	60.28.245.240	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:29:10	254	119.147.6.60	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:27:05	254	66.249.71.73	http://www.nusoft.com.tw/	Custom	sniffer_http	✓
20:26:13	254	66.249.71.73	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:24:06	254	157.55.18.23	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:20:03	254	72.14.199.50	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:19:15	254	119.147.138.100	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:19:14	254	119.147.138.100	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:18:33	254	65.52.110.22	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:15:44	254	157.55.18.23	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:13:18	254	118.160.188.237	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:12:00	254	208.115.111.67	http://www.nusoft.com.t...	Custom	sniffer_http	✓
20:09:19	254	124.115.4.192	http://www.nusoft.com.t...	Custom	sniffer_http	✓

1 / 66 移至

圖 9-11 網頁應用程式防火牆日誌

說明：

1. 【日誌】報表的相關圖示說明如下：

■ 處理動作：

圖例	✓	✗
代表涵義	通行	丟棄

第10章 監控記錄

用來即時接收遠端 UTM、MHG 的封包記錄、事件記錄、連線記錄、病毒過濾記錄、應用程式管制記錄、連線數限制記錄、傳輸量限制記錄報表。

- **【封包記錄】**：可在制定遠端 UTM、MHG **【管制條例】**時啟用，會詳細記錄通過管制條例傳送的封包資訊。
- **【事件記錄】**：遠端 UTM、MHG 系統運作、登入、組態參數值（System Configurations）更改...記錄。
- **【連線記錄】**：記錄遠端 UTM、MHG 的 VPN、PPPoE、...連線資訊；若連線發生問題時，系統管理員可憑藉此資訊，了解問題的所在。
- **【病毒過濾記錄】**：記錄所有經過遠端 UTM 管制條例，存取 HTTP/Web-Based Mail、FTP 服務時，偵測到的病毒資訊。
- **【應用程式管制記錄】**：記錄被遠端 UTM、MHG 阻擋的應用程式存取資訊。
- **【連線數限制記錄】**：記錄達到遠端 UTM、MHG 管制條例連線數限制的資訊。
- **【傳輸量限制記錄】**：記錄達到遠端 UTM、MHG 管制條例傳輸量限制的資訊。

【設定】功能概述：

監控記錄保留期限設定 說明如下：

- 對於儲存在 CMS-2000 內建硬碟的封包、事件、連線、病毒過濾、應用程式管制、連線數限制和傳輸量限制監控記錄，可指定保存的期限，並於到期日刪除所有符合條件的記錄。

【封包記錄】功能概述：

搜尋 說明如下：

- 可依照日期、裝置名稱、管制條例方向、來源位址、目的位址和目的埠號等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
 - ◆ 在【本機】>【裝置監控備份】>【監控記錄】>【封包記錄】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】、【管制條例方向】。
 - 按下【搜尋】鈕。（如圖 10-1）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如圖 10-2）

搜尋 封包記錄

☒ 起始 日期 / 時間: 2012 / 06 / 15 00 : 00
 結束 日期 / 時間: 2012 / 06 / 15 17 : 07
 裝置名稱: 所有遠端裝置
 管制條例方向: 所有方向
 來源位址:
 目的位址:
 目的埠號: - (範圍: 1 - 65535)

搜尋

結果

2012-06-15 (1342576 筆記錄)

下載

1 / 67129 移至

時間	遠端裝置	來源位址	目的位址	通訊協定	埠號	流量	處置方式
17:07:59	254	59.120.8.151	210.59.207.104	UDP	1722→1153(WAN=1)	184.0 B	✓
17:07:59	254	210.202.222.217	210.59.207.104	UDP	35532→1153(WAN=1)	152.0 B	✓
17:07:59	254	192.168.85.200	66.134.75.238	UDP	56383→53(WAN=2)	62.0 B	✓
17:07:59	254	192.168.85.200	24.30.199.7	UDP	56383→53(WAN=2)	591.0 B	✓
17:07:59	254	192.168.85.200	202.96.199.133	UDP	56383→53(WAN=2)	62.0 B	✓
17:07:59	254	192.168.85.200	202.136.254.1	UDP	56383→53(WAN=2)	62.0 B	✓
17:07:59	254	192.168.85.200	202.106.127.1	UDP	56383→53(WAN=2)	124.0 B	✓
17:07:59	254	192.168.85.200	168.95.192.1	UDP	56383→53(WAN=2)	235.0 B	✓
17:07:59	254	192.168.85.200	168.95.1.1	UDP	56383→53(WAN=2)	62.0 B	✓
17:07:59	254	172.19.50.6	66.134.75.238	UDP	34288→53(WAN=2)	58.0 B	✓
17:07:59	254	172.19.50.6	24.30.199.7	UDP	34288→53(WAN=2)	583.0 B	✓
17:07:59	254	172.19.50.6	202.96.199.133	UDP	34288→53(WAN=2)	116.0 B	✓
17:07:59	254	172.19.50.6	202.136.254.1	UDP	34288→53(WAN=2)	58.0 B	✓
17:07:59	254	172.19.50.6	202.106.127.1	UDP	34288→53(WAN=2)	58.0 B	✓
17:07:59	254	172.19.50.6	168.95.192.1	UDP	34288→53(WAN=2)	175.0 B	✓
17:07:59	254	172.19.50.6	168.95.1.1	UDP	34288→53(WAN=2)	58.0 B	✓
17:07:59	254	172.19.50.200	66.134.75.238	UDP	55151→53(WAN=2)	63.0 B	✓
17:07:59	254	172.19.50.200	24.30.199.7	UDP	55151→53(WAN=2)	593.0 B	✓
17:07:59	254	172.19.50.200	202.96.199.133	UDP	55151→53(WAN=2)	126.0 B	✓
17:07:59	254	172.19.50.200	202.136.254.1	UDP	55151→53(WAN=2)	63.0 B	✓

1 / 67129 移至

圖 10-1 搜尋特定記錄

搜尋 封包記錄

☒ 起始 日期/時間: 2012 / 06 / 15 00 : 00
 結束 日期/時間: 2012 / 06 / 15 17 : 07
 裝置名稱: 所有遠端裝置
 管制條例方向: 所有方向
 來源位址:
 目的位址:
 目的埠號: - (範圍: 1 - 65535)

搜尋

結果

2012-06-15 (1342576 筆記錄)

下載

1 / 67129 移至

時間	遠端裝置	來源位址	目的位址	通訊協定	埠號	流量	處置方式
17:07:59	254	59.120.8.151	210.59.207.104	UDP	1722→1153(WAN=1)	184.0 B	✓
17:07:59	254	210.202.222.217	210.59.207.104	UDP	35532→1153(WAN=1)	152.0 B	✓
17:07:59	254					62.0 B	✓
17:07:59	254					591.0 B	✓
17:07:59	254					62.0 B	✓
17:07:59	254					62.0 B	✓
17:07:59	254					124.0 B	✓
17:07:59	254					235.0 B	✓
17:07:59	254					62.0 B	✓
17:07:59	254					58.0 B	✓
17:07:59	254					583.0 B	✓
17:07:59	254					116.0 B	✓
17:07:59	254					58.0 B	✓
17:07:59	254					58.0 B	✓
17:07:59	254	172.19.50.6	168.95.192.1	UDP	34288→53(WAN=2)	175.0 B	✓
17:07:59	254	172.19.50.6	168.95.1.1	UDP	34288→53(WAN=2)	58.0 B	✓
17:07:59	254	172.19.50.200	66.134.75.238	UDP	55151→53(WAN=2)	63.0 B	✓
17:07:59	254	172.19.50.200	24.30.199.7	UDP	55151→53(WAN=2)	593.0 B	✓
17:07:59	254	172.19.50.200	202.96.199.133	UDP	55151→53(WAN=2)	126.0 B	✓
17:07:59	254	172.19.50.200	202.136.254.1	UDP	55151→53(WAN=2)	63.0 B	✓

1 / 67129 移至

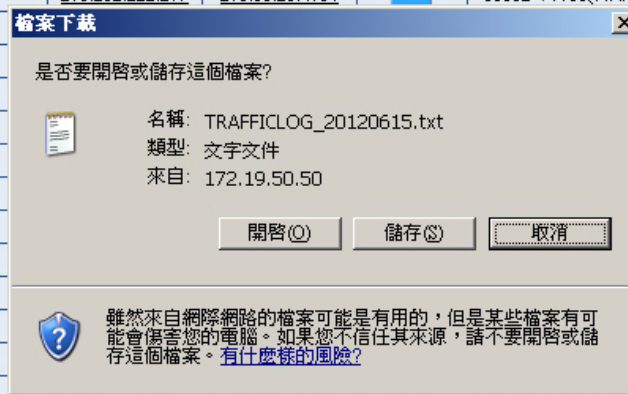


圖 10-2 下載搜尋的記錄

【事件記錄】功能概述：

搜尋 說明如下：

- 可依照日期、裝置名稱、管理員名稱、IP 位址、事件類型和僅顯示有詳細內容之事件記錄等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- ◆ 在【本機】>【裝置監控備份】>【監控記錄】>【事件記錄】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】、【事件類型】。
 - 按下【搜尋】鈕。(如圖 10-3)
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。(如圖 10-4)

搜尋 事件記錄

☒ 起始 日期 / 時間: 2012 / 06 / 15 00 : 00
 結束 日期 / 時間: 2012 / 06 / 15 18 : 48
 裝置名稱: 所有遠端裝置
 管理員名稱: (最多 30 個字元)
 IP位址:
 事件類型: 所有類型
☐ 僅顯示有詳細內容之事件記錄

搜尋

結果

2012-06-15 (166 筆記錄)

下載

3 / 9 移至

時間	遠端裝置	管理員名稱	IP位址	事件	內容
14:13:36	254	admin	172.19.20.12	登入成功	
14:03:50	254	admin	172.19.50.19	登入成功	
14:02:54	254	admin	172.19.20.12	[系統管理→管理→管理位址] 移除	
13:59:37	254	admin	172.19.20.12	[系統管理→管理→管理位址] 新增	
13:58:22	254	admin	172.19.20.12	登入成功	
13:38:57	254	admin	172.19.50.19	登入成功	
13:38:03	254	admin	172.19.20.12	登入成功	
13:01:15	254	system	127.0.0.1	寄送郵件通知 (nusoftware.com.tw)	
12:43:57	254	admin	172.19.100.84	[管制條例選項→虛擬伺服器→連接埠對應] 移除	
12:43:48	254	admin	172.19.100.84	[管制條例→外部至內部] 移除	
12:42:43	254	admin	172.19.50.15	[管制條例→外部至內部] 新增	
12:41:26	254	admin	172.19.50.15	[管制條例選項→虛擬伺服器→連接埠對應] 新增	
12:40:23	254	admin	172.19.50.15	登入成功	
12:39:08	254	admin	172.19.100.55	登入成功	
12:30:44	254	admin	172.19.50.19	登入成功	
12:29:17	254	admin	172.19.100.84	登入成功	
12:27:11	254	admin	172.19.20.12	登入成功	
12:27:01	254	system	127.0.0.1	WAN3(Port4) 連線	
12:26:42	254	system	127.0.0.1	WAN3(Port4) 斷線	
12:06:43	254	admin	172.19.50.15	登入成功	

3 / 9 移至

圖 10-3 搜尋特定記錄

搜尋 事件記錄

☒ 起始 日期 / 時間: 2012 / 06 / 15 00 : 00
 結束 日期 / 時間: 2012 / 06 / 15 18 : 48
 裝置名稱: 所有遠端裝置
 管理員名稱: (最多 30 個字元)
 IP位址:
 事件類型: 所有類型
☐ 僅顯示有詳細內容之事件記錄

搜尋

結果

2012-06-15 (166 筆記錄)

下載

3 / 9 移至

時間	遠端裝置	管理員名稱	IP位址	事件	內容
14:13:36	254	admin	172.19.20.12	登入成功	
14:03:50	254	admin	172.19.50.19	登入成功	
14:02:54	254	admin	172.19.20.12	[系統管理→管理→管理位址] 移除	
13:59:37	254	<div> <div>檔案下載</div> <div> 是否要開啓或儲存這個檔案? 名稱: Event_Log_20120615.log 類型: 文字文件 來自: 172.19.50.50 <div> 開啓(O) 儲存(S) 取消 </div> </div> <div> 雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。有什麼樣的風險? </div> </div>			
13:58:22	254				
13:38:57	254				
13:38:03	254				
13:01:15	254				
12:43:57	254				應] 移除
12:43:48	254				
12:42:43	254				
12:41:26	254				應] 新增
12:40:23	254				
12:39:08	254				
12:30:44	254				
12:29:17	254	admin	172.19.100.84	登入成功	
12:27:11	254	admin	172.19.20.12	登入成功	
12:27:01	254	system	127.0.0.1	WAN3(Port4) 連線	
12:26:42	254	system	127.0.0.1	WAN3(Port4) 斷線	
12:06:43	254	admin	172.19.50.15	登入成功	

3 / 9 移至

圖 10-4 下載搜尋的記錄

【連線記錄】功能概述：

搜尋 說明如下：

- 撥號連線：可依照日期、裝置名稱和連線類型等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- 動態 IP 位址：可依照日期、裝置名稱和連線類型等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- DHCP：可依照日期、裝置名稱和連線類型等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- PPTP Server：可依照日期、裝置名稱和連線類型等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- PPTP Client：可依照日期、裝置名稱和連線類型等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- IPSec：可依照日期、裝置名稱和連線類型等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- Web VPN：可依照日期、裝置名稱和連線類型等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- SMTP 內送郵件：可依照日期、裝置名稱、連線類型、IP 位址、寄件者、收件者、狀態和內容等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- SMTP 外寄郵件：可依照日期、裝置名稱、連線類型、IP 位址、寄件者、收件者、狀態和內容等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- POP3：可依照日期、裝置名稱、連線類型、IP 位址、帳號、狀態和內容等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
- ◆ 在【本機】>【裝置監控備份】>【監控記錄】>【連線記錄】的【IPSec】>【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】、【連線類型】。
 - 按下【搜尋】鈕。（如圖 10-5）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如圖 10-6）

搜尋 連線記錄

☒ 起始 日期/時間: 2012 / 06 / 18 00 : 00
 結束 日期/時間: 2012 / 06 / 18 17 : 58
 裝置名稱: 所有遠端裝置
 連線類型: IPSec

搜尋

結果

2012-06-18 (21033 筆記錄)

下載

1 / 1052 移至

時間	遠端裝置	連線訊息
17:58:43	UTM_TEST_測試機	"CMS_test_ipsec" #17346: ERROR: asynchronous network error report on WAN2 (sport=500) for messa...
17:58:32	UTM_TEST_測試機	"CMS_test_ipsec" #17346: ERROR: asynchronous network error report on WAN2 (sport=500) for messa...
17:58:32	UTM_TEST_測試機	ERROR: asynchronous network error report on WAN2 (sport=500) for message to 111.249.186.108 port ...
17:58:30	UTM_TEST_測試機	"CMS_test_ipsec" #17346: initiating Main Mode
17:58:30	UTM_TEST_測試機	loading secrets from "/etc/ipsec.secrets"
17:58:30	UTM_TEST_測試機	forgetting secrets
17:58:30	UTM_TEST_測試機	listening for IKE messages
17:58:30	UTM_TEST_測試機	added connection description "CMS_test_ipsec"
17:58:29	UTM_TEST_測試機	"CMS_test_ipsec": deleting connection
17:58:29	UTM_TEST_測試機	"CMS_test_ipsec": terminating SAs using this connection
17:58:29	UTM_TEST_測試機	"CMS_test_ipsec" #17345: deleting state (STATE_MAIN_1)
17:58:12	UTM_TEST_測試機	"CMS_test_ipsec" #17345: ERROR: asynchronous network error report on WAN2 (sport=500) for messa...
17:58:02	UTM_TEST_測試機	"CMS_test_ipsec" #17345: ERROR: asynchronous network error report on WAN2 (sport=500) for messa...
17:58:02	UTM_TEST_測試機	ERROR: asynchronous network error report on WAN2 (sport=500) for message to 111.249.186.108 port ...
17:57:59	UTM_TEST_測試機	"CMS_test_ipsec" #17345: initiating Main Mode
17:57:59	UTM_TEST_測試機	loading secrets from "/etc/ipsec.secrets"
17:57:59	UTM_TEST_測試機	listening for IKE messages
17:57:59	UTM_TEST_測試機	forgetting secrets
17:57:59	UTM_TEST_測試機	added connection description "CMS_test_ipsec"
17:57:59	UTM_TEST_測試機	"CMS_test_ipsec": deleting connection

1 / 1052 移至

圖 10-5 搜尋特定記錄

搜尋 連線記錄

☒ 起始 日期/時間: 2012 / 06 / 18 00 : 00
 結束 日期/時間: 2012 / 06 / 18 17 : 58
 裝置名稱: 所有遠端裝置
 連線類型: IPSec



搜尋

結果

2012-06-18 (21033 筆記錄)

下載

1 / 1052 移至

時間	遠端裝置	連線訊息
17:58:43	UTM_TEST_測試機	"CMS_test_ipsec" #17346: ERROR: asynchronous network error report on VWAN2 (sport=500) for messa...
17:58:32	UTM_TEST_測試機	"CMS_test_ipsec" #17346: ERROR: asynchronous network error report on VWAN2 (sport=500) for messa...
17:58:32	UTM_TEST_測試機	ERROR: asynchronous network error report on VWAN2 (sport=500) for message to 111.249.186.108 port ...
17:58:30	UTM_TEST_測試機	<div>檔案下載</div> <div> 是否要開啓或儲存這個檔案?  名稱: Connection_ipsec_vpn_20120618.log 類型: 文字文件 來自: 172.19.50.50 <div>開啓(O) 儲存(S) 取消</div> </div> <div>  雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。有什麼樣的風險? </div>
17:58:30	UTM_TEST_測試機	
17:58:30	UTM_TEST_測試機	
17:58:30	UTM_TEST_測試機	
17:58:30	UTM_TEST_測試機	
17:58:30	UTM_TEST_測試機	
17:58:29	UTM_TEST_測試機	
17:58:29	UTM_TEST_測試機	
17:58:29	UTM_TEST_測試機	
17:58:29	UTM_TEST_測試機	
17:58:12	UTM_TEST_測試機	N2 (sport=500) for messa...
17:58:02	UTM_TEST_測試機	N2 (sport=500) for messa...
17:58:02	UTM_TEST_測試機	e to 111.249.186.108 port ...
17:57:59	UTM_TEST_測試機	
17:57:59	UTM_TEST_測試機	loading secrets from "/etc/ipsec.secrets"
17:57:59	UTM_TEST_測試機	listening for IKE messages
17:57:59	UTM_TEST_測試機	forgetting secrets
17:57:59	UTM_TEST_測試機	added connection description "CMS_test_ipsec"
17:57:59	UTM_TEST_測試機	"CMS_test_ipsec": deleting connection

1 / 1052 移至

圖 10-6 下載搜尋的記錄

【病毒過濾記錄】功能概述：

搜尋 說明如下：

- 可依照日期、裝置名稱、來源位址、目的位址、網路服務、中毒檔案和病毒名稱等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
 - ◆ 在【本機】>【裝置監控備份】>【監控記錄】>【病毒過濾記錄】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】。
 - 按下【搜尋】鈕。(如圖 10-7)
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。(如圖 10-8)

搜尋 病毒過濾記錄

☒ 起始 日期/時間: 2012 / 06 / 05 00 : 00
結束 日期/時間: 2012 / 06 / 18 18 : 27
裝置名稱: 所有遠端裝置
來源位址:
目的位址:
網路服務: (最多 30 個字元)
中毒檔案: (最多 30 個字元)
病毒名稱: (最多 30 個字元)

搜尋

結果

2012-06-05 (1 筆記錄)

下載

1 / 1 移至

時間	遠端裝置	來源位址	目的位址	網路服務	中毒檔案	病毒名稱
17:53:02	254	172.19.50.1	www.rexswain....	HTTP	eicar.com	Eicar-Test-Signatur...

1 / 1 移至

圖 10-7 搜尋特定記錄

搜尋 病毒過濾記錄

☒ 起始日期/時間: 2012 / 06 / 05 00 : 00
 結束日期/時間: 2012 / 06 / 18 18 : 27
 裝置名稱: 所有遠端裝置
 來源位址:
 目的位址:
 網路服務: (最多 30 個字元)
 中毒檔案: (最多 30 個字元)
 病毒名稱: (最多 30 個字元)

搜尋

結果

2012-06-05 (1 筆記錄)

下載

時間	遠端裝置	來源位址	目的位址	網路服務	中毒檔案	病毒名稱
17:53:02	254	172.19.50.1	www.rexswain....	HTTP	eicar.com	Eicar-Test-Signatur...

檔案下載

是否要開啓或儲存這個檔案?

名稱: Virus_20120618.log

類型: 文字文件

來自: 172.19.50.50

開啓(O)
儲存(S)
取消

雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。[有什麼樣的風險?](#)

圖 10-8 下載搜尋的記錄

【應用程式管制記錄】功能概述：

搜尋 說明如下：

- 可依照日期、裝置名稱和來源位址等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
 - ◆ 在【本機】>【裝置監控備份】>【監控記錄】>【應用程式管制記錄】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】。
 - 按下【搜尋】鈕。（如圖 10-9）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如圖 10-10）

搜尋 應用程式管制記錄

☒ 起始 日期/時間: 2012 / 06 / 05 00 : 00
結束 日期/時間: 2012 / 06 / 18 18 : 41
裝置名稱: 所有遠端裝置
來源位址:

搜尋

結果

2012-06-15 (1 筆記錄)

下載

1 / 1 移至

時間	遠端裝置	來源位址	應用程式管制記錄
17:58:38	254	172.19.100.84	迅雷5

1 / 1 移至

圖 10-9 搜尋特定記錄

搜尋 應用程式管制記錄

☒ 起始 日期 / 時間: 2012 / 06 / 05 00 : 00
結束 日期 / 時間: 2012 / 06 / 18 18 : 41
裝置名稱: 所有遠端裝置
來源位址:

搜尋

結果

2012-06-15 (1 筆記錄)

下載

1 / 1 移至

時間	遠端裝置	來源位址	應用程式管制記錄
17:58:38	254	172.19.100.84	迅雷5

1 / 1 移至

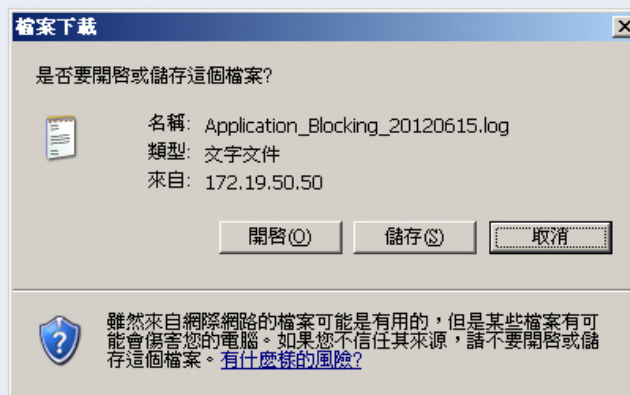


圖 10-10 下載搜尋的記錄

【連線數限制記錄】功能概述：

搜尋 說明如下：

- 可依照日期、裝置名稱和來源位址等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
 - ◆ 在【本機】>【裝置監控備份】>【監控記錄】>【連線數限制記錄】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】。
 - 按下【搜尋】鈕。（如圖 10-11）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如圖 10-12）

搜尋 連線數限制記錄

☒ 起始日期/時間: 2012 / 06 / 05 00 : 00
結束日期/時間: 2012 / 06 / 18 19 : 02
裝置名稱: 所有遠端裝置
來源位址:

搜尋

結果

2012-06-18 (1 筆記錄)

下載

1 / 1 移至

時間	遠端裝置	來源位址	管制條例方向	限制原因
18:56:33	254	172.19.20.12	內部至外部	最大連線數超過允許值

1 / 1 移至

圖 10-11 搜尋特定記錄

搜尋 連線數限制記錄

☒ 起始 日期 / 時間: 2012 / 06 / 05 00 : 00
 結束 日期 / 時間: 2012 / 06 / 18 19 : 02
 裝置名稱: 所有遠端裝置
 來源位址:

搜尋

結果

2012-06-18 (1 筆記錄)

下載

時間	遠端裝置	來源位址	管制條例方向	限制原因
18:56:33	254	172.19.20.12	內部至外部	最大連線數超過允許值

檔案下載

是否要開啓或儲存這個檔案?



名稱: Concurrent_20120618.log
 類型: 文字文件
 來自: 172.19.50.50

開啓(O)

儲存(S)

取消



雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。 [有什麼樣的風險?](#)

圖 10-12 下載搜尋的記錄

【傳輸量限制記錄】功能概述：

搜尋 說明如下：

- 可依照日期、裝置名稱和來源位址等關鍵字或特徵，來尋找儲存在 CMS-2000 內所有符合條件之記錄。
 - ◆ 在【本機】>【裝置監控備份】>【監控記錄】>【傳輸量限制記錄】的【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【裝置名稱】。
 - 按下【搜尋】鈕。（如圖 10-13）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如圖 10-14）

搜尋 傳輸量限制記錄

☒ 起始 日期/時間: 2012 / 06 / 05 00 : 00
結束 日期/時間: 2012 / 06 / 18 19 : 21
裝置名稱: 所有遠端裝置
來源位址:

搜尋

結果

2012-06-18 (1 筆記錄)

下載

1 / 1 移至

時間	遠端裝置	來源位址	管制條例方向	限制原因
18:58:35	254	172.19.20.12	內部至外部	超過每天允許傳輸量

1 / 1 移至

圖 10-13 搜尋特定記錄

搜尋 傳輸量限制記錄

☒ 起始 日期 / 時間: 2012 / 06 / 05 00 : 00
 結束 日期 / 時間: 2012 / 06 / 18 19 : 21
 裝置名稱: 所有遠端裝置
 來源位址:

搜尋

結果

2012-06-18 (1 筆記錄)

下載

時間	遠端裝置	來源位址	管制條例方向	限制原因
18:58:35	254	172.19.20.12	內部至外部	超過每天允許傳輸量

檔案下載

是否要開啓或儲存這個檔案?



名稱: Quota_20120618.log
 類型: 文字文件
 來自: 172.19.50.50

開啓(O)

儲存(S)

取消



雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。[有什麼樣的風險?](#)

圖 10-14 下載搜尋的記錄

10.1 封包記錄

10.1.1 檢視使用者透過遠端UTM、MHG存取內、外部網路資源，使用的協定及埠號

步驟1. 在【本機】>【裝置監控備份】>【監控記錄】>【封包記錄】頁面中，可顯示遠端 UTM、MHG 即時傳送至 CMS-2000 的系統封包監控記錄。（如圖 10-15）

- 點擊【來源位址】或【目的位址】連結，會彈出一視窗列出所選擇之 IP 存取網路資源時，透過之通訊協定、埠號和所使用之流量。（如圖 10-16）

裝置名稱: 所有遠端裝置							
更新							
2012-06-18 (1657405 筆記錄)							
1 / 82871 移至							
時間	遠端裝置	來源位址	目的位址	通訊協定	埠號	流量	處置方式
20:34:33	254	192.168.85.200	168.95.1.1	UDP	51238→53(WAN=2)	62.0 B	✓
20:34:33	254	172.19.50.6	168.95.1.1	UDP	60744→53(WAN=2)	58.0 B	✓
20:34:33	254	172.19.50.200	168.95.192.1	UDP	54760→53(WAN=2)	63.0 B	✓
20:34:23	254	216.155.116.210	210.59.207.104	UDP	45805→1153(WAN=1)	184.0 B	✓
20:34:23	254	172.19.50.6	66.134.75.238	UDP	36689→53(WAN=2)	58.0 B	✓
20:34:23	254	172.19.50.6	24.30.199.7	UDP	36689→53(WAN=2)	327.0 B	✓
20:34:23	254	172.19.50.6	202.96.199.133	UDP	36689→53(WAN=2)	116.0 B	✓
20:34:23	254	172.19.50.6	202.136.254.1	UDP	36689→53(WAN=2)	58.0 B	✓
20:34:23	254	172.19.50.6	202.106.127.1	UDP	36689→53(WAN=2)	58.0 B	✓
20:34:23	254	172.19.50.6	168.95.192.1	UDP	36689→53(WAN=2)	175.0 B	✓
20:34:23	254	172.19.50.200	66.134.75.238	UDP	58402→53(WAN=2)	63.0 B	✓
20:34:23	254	172.19.50.200	24.30.199.7	UDP	58402→53(WAN=2)	337.0 B	✓
20:34:23	254	172.19.50.200	202.96.199.133	UDP	58402→53(WAN=2)	126.0 B	✓
20:34:23	254	172.19.50.200	202.136.254.1	UDP	58402→53(WAN=2)	63.0 B	✓
20:34:23	254	172.19.50.200	202.106.127.1	UDP	58402→53(WAN=2)	126.0 B	✓
20:34:23	254	172.19.50.200	168.95.1.1	UDP	58402→53(WAN=2)	178.0 B	✓
20:33:07	254	192.168.85.200	168.95.1.1	UDP	59995→53(WAN=2)	62.0 B	✓
20:33:07	254	172.19.50.200	168.95.192.1	UDP	38656→53(WAN=2)	63.0 B	✓
20:33:07	254	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
20:33:06	254	172.19.50.6	168.95.1.1	UDP	60800→53(WAN=2)	58.0 B	✓

圖 10-15 封包記錄

http://172.19.50.50/cgi-bin/local_trafficlog.cgi?q=0&MULTI_LANG=ch&dt=20120618&sip=192.168.85.2 - Micros...

裝置名稱: 所有遠端裝置

更新

2012-06-18 (271865 筆記錄)

1 / 13594 移至

時間	遠端裝置	來源位址	目的位址	通訊協定	埠號	流量	處置方式
20:34:59	254	192.168.85.200	168.95.1.1	UDP	53560→53(WAN=2)	62.0 B	✓
20:34:58	254	192.168.85.200	168.95.1.1	UDP	37875→53(WAN=2)	62.0 B	✓
20:34:57	254	192.168.85.200	168.95.1.1	UDP	42043→53(WAN=2)	62.0 B	✓
20:34:56	254	192.168.85.200	168.95.1.1	UDP	36606→53(WAN=2)	62.0 B	✓
20:34:55	254	192.168.85.200	168.95.1.1	UDP	33199→53(WAN=2)	62.0 B	✓
20:34:54	254	192.168.85.200	168.95.1.1	UDP	49153→53(WAN=2)	62.0 B	✓
20:34:53	254	192.168.85.200	168.95.1.1	UDP	58948→53(WAN=2)	62.0 B	✓
20:34:52	254	192.168.85.200	168.95.1.1	UDP	45261→53(WAN=2)	62.0 B	✓
20:34:51	254	192.168.85.200	168.95.1.1	UDP	43305→53(WAN=2)	62.0 B	✓
20:34:50	254	192.168.85.200	168.95.1.1	UDP	37248→53(WAN=2)	62.0 B	✓
20:34:48	254	192.168.85.200	168.95.1.1	UDP	55206→53(WAN=2)	62.0 B	✓
20:34:48	254	192.168.85.200	168.95.192.1	UDP	55206→53(WAN=2)	235.0 B	✓
20:34:48	254	192.168.85.200	66.134.75.238	UDP	55206→53(WAN=2)	62.0 B	✓
20:34:48	254	192.168.85.200	24.30.199.7	UDP	55206→53(WAN=2)	335.0 B	✓
20:34:48	254	192.168.85.200	202.96.199.133	UDP	55206→53(WAN=2)	124.0 B	✓

完成 網際網路


圖 10-16 封包記錄過濾視窗

10.2 事件記錄

10.2.1 檢視系統管理員登入和管理遠端UTM、MHG，及遠端UTM、

MHG寄送報表、外部網路介面運作之狀況

步驟1. 在【本機】>【裝置監控備份】>【監控記錄】>【事件記錄】頁面中，可顯示遠端 UTM、MHG 即時傳送至 CMS-2000 的系統登入、管理、寄送報表、外部網路介面運作事件記錄。（如圖 10-17）

■ 按下  鈕，會顯示該筆記錄的詳細訊息。（如圖 10-18）

裝置名稱: 所有遠端裝置					
更新					
2012-06-15(175 筆記錄)					
6 / 9 移至					
時間	遠端裝置	管理員名稱	IP位址	事件	內容
11:27:07	254	admin	111.249.193.143	登入成功	
11:26:51	254	admin	172.19.20.7	[管制條例選項→VPN→PPTP 伺服器] 新增帳號	
11:19:49	254	admin	172.19.20.12	登入成功	
10:55:29	UTM_TEST_測試機	admin	172.19.100.66	[SSL Web VPN→設定] 移除	
10:55:06	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→VPN→Trunk] 移除	
10:54:44	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→虛擬伺服器→連接埠對應] 移除	
10:54:40	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→虛擬伺服器→連接埠對應群組] 移除	
10:54:35	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→虛擬伺服器→連接埠對應] 移除	
10:54:08	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→應用程式管制→設定] 移除	
10:54:06	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→應用程式管制→設定] 移除	
10:54:04	254	admin	172.19.50.21	[管制條例→內部至外部] 條例暫停	
10:53:57	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→認證表→認證帳戶] 移除	
10:53:54	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→認證表→認證帳戶] 移除	
10:53:53	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→認證表→認證帳戶] 移除	
10:53:51	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→認證表→認證帳戶] 移除	
10:53:49	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→認證表→認證帳戶] 移除	
10:53:40	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→頻寬表→設定] 移除	
10:53:38	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→頻寬表→設定] 移除	
10:53:31	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→排程表→設定] 移除	
10:52:18	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→排程表→設定] 移除	

圖 10-17 事件記錄

http://172.19.50.50 - [事件日誌] 內容 (91) - Microsoft Internet Explorer

日期 / 時間	遠端裝置	管理員名稱	IP位址	事件
06/15 10:55	UTM_TEST_測試機	admin	172.19.100.66	[管制條例選項→VPN→Trunk] 移除

內容

移除之前

i	名稱 ▲	本地端子網路	遠端子網路	VPN通道	變更
	CMS_test_ipsec_tr...	192.168.2.0 / 24	192.168.3.0 / 24	CMS_test_ipsec	修改 刪除

移除之後

i	名稱 ▲	本地端子網路	遠端子網路	VPN通道	變更
沒有記錄!					

完成

國際網路

圖 10-18 事件記錄內容

10.3 連線記錄

10.3.1 檢視遠端UTM、MHG的系統連線記錄

步驟1. 在【本機】>【裝置監控備份】>【監控記錄】>【連線記錄】頁面中，可顯示遠端 UTM、MHG 即時傳送至 CMS-2000 的系統撥號、動態 IP 位址、DHCP、PPTP Server、PPTP Client、IPSec、Web VPN、SMTP 內送郵件、SMTP 外寄郵件、POP3 連線狀況。（如圖 10-19）

裝置名稱: 所有遠端裝置

更新

連線類型: IPSec

2012-06-19(19790 筆記錄)

1 / 990 移至

時間	遠端裝置	連線訊息
16:01:48	50點兩百	"CMS_test_ipsec" #19961: initiating Main Mode
16:01:48	50點兩百	loading secrets from "/etc/ipsec.secrets"
16:01:48	50點兩百	forgetting secrets
16:01:48	50點兩百	listening for IKE messages
16:01:48	50點兩百	added connection description "CMS_test_ipsec"
16:01:48	50點兩百	"CMS_test_ipsec": deleting connection
16:01:48	50點兩百	"CMS_test_ipsec" #19960: deleting state (STATE_MAIN_I1)
16:01:48	50點兩百	"CMS_test_ipsec": terminating SAs using this connection
16:01:31	50點兩百	"CMS_test_ipsec" #19960: ERROR: asynchronous network error report on WAN2 (sport=500) for messa...
16:01:21	50點兩百	"CMS_test_ipsec" #19960: ERROR: asynchronous network error report on WAN2 (sport=500) for messa...
16:01:18	50點兩百	"CMS_test_ipsec" #19960: initiating Main Mode
16:01:18	50點兩百	loading secrets from "/etc/ipsec.secrets"
16:01:18	50點兩百	forgetting secrets
16:01:18	50點兩百	listening for IKE messages
16:01:18	50點兩百	added connection description "CMS_test_ipsec"
16:01:18	50點兩百	"CMS_test_ipsec": deleting connection
16:01:18	50點兩百	"CMS_test_ipsec": terminating SAs using this connection
16:01:18	50點兩百	"CMS_test_ipsec" #19959: deleting state (STATE_MAIN_I1)
16:01:01	50點兩百	"CMS_test_ipsec" #19959: ERROR: asynchronous network error report on WAN2 (sport=500) for messa...
16:00:50	50點兩百	"CMS_test_ipsec" #19959: ERROR: asynchronous network error report on WAN2 (sport=500) for messa...

1 / 990 移至

圖 10-19 連線記錄

10.4 病毒過濾記錄

10.4.1 檢視使用者透過HTTP/Web-Based Mail、FTP協定傳輸的檔案，經遠端UTM掃描後，阻擋的病毒記錄

步驟1. 在【本機】>【裝置監控備份】>【監控記錄】>【病毒過濾記錄】頁面中，可顯示遠端 UTM 即時傳送至 CMS-2000 的系統阻擋 HTTP/Web-Based Mail、FTP 傳輸病毒檔案記錄。(如圖 10-20)



時間	遠端裝置	來源位址	目的位址	網路服務	中毒檔案	病毒名稱
17:53:02	254	172.19.50.1	www.rexswain....	HTTP	eicar.com	Eicar-Test-Signatur...

圖 10-20 病毒過濾記錄

10.5 應用程式管制記錄

10.5.1 檢視遠端UTM、MHG阻擋的應用程式存取記錄

步驟1. 在【本機】>【裝置監控備份】>【監控記錄】>【應用程式管制記錄】頁面中，可顯示遠端 UTM、MHG 即時傳送至 CMS-2000 的系統阻擋應用程式存取記錄。（如圖 10-21）



裝置名稱: 所有遠端裝置			
更新			
2012-06-15 (1 筆記錄)			
1 / 1 移至			
時間	遠端裝置	來源位址	應用程式管制記錄
17:58:38	254	172.19.100.84	迅雷5
1 / 1 移至			

圖 10-21 應用程式管制記錄

10.6 連線數限制記錄

10.6.1 檢視達到遠端UTM、MHG限制的連線數存取記錄

步驟1. 在【本機】>【裝置監控備份】>【監控記錄】>【連線數限制記錄】頁面中，可顯示遠端 UTM、MHG 即時傳送至 CMS-2000 的系統連線數管制記錄。(如圖 10-22)



裝置名稱: 所有遠端裝置

更新

2012-06-18 (1 筆記錄)

時間	遠端裝置	來源位址	管制條例方向	限制原因
18:56:33	254	172.19.20.12	內部至外部	最大連線數超過允許值

圖 10-22 連線數限制記錄

10.7 傳輸量限制記錄

10.7.1 檢視達到遠端UTM、MHG限制的傳輸量存取記錄

步驟1. 在【本機】>【裝置監控備份】>【監控記錄】>【傳輸量限制記錄】頁面中，可顯示遠端 UTM、MHG 即時傳送至 CMS-2000 的系統傳輸量管制記錄。(如圖 10-23)



裝置名稱: 所有遠端裝置

更新

2012-06-18 (1 筆記錄)

時間	遠端裝置	來源位址	管制條例方向	限制原因
18:58:35	254	172.19.20.12	內部至外部	超過每天允許傳輸量

圖 10-23 傳輸量限制記錄

遠端

管制條例選項

第11章 位址表

用來設定位於遠端 UTM、MHG 內部網路、外部網路、非軍事區網路的 IP 位址列表，並視需求將特定 IP 位址進行群組、劃分。

這些 IP 位址可能是一個主機 IP 位址，也可能是一個網段。系統管理員可以自行設定一個易辨識的名字代表此一 IP 位址。基本上 IP 位址根據不同的網路區可分為三種：內部網路 IP 位址(Internal IP Address)、外部網路 IP 位址(External IP Address) 和非軍事區網路 IP 位址(DMZ IP Address)。當系統管理員欲將不同 IP 位址封包的過濾規則，加入相同管制條例時，可先將這些 IP 位址建立一個「內部網路群組」、「外部網路群組」或是「非軍事區群組」，以簡化設立管制條例工作程序。

【位址表】功能概述：

名稱 說明如下：

- 用於指定一個易辨識的名字代表所設定之 IP 位址。

IP 位址範圍 說明如下：

- 可以 IPv4 子網路遮罩指定、IPv6 首碼長度指定、直接輸入 IP 範圍、輸入特定 FQDN。



說明：

1. FQDN(Fully Qualified Domain Name)是由主機名稱(Hostname)和網域名稱(Domain Name)兩部份所組成。以 www.nusoft.com.tw 為例，主機名稱就是 www，網域名稱就是 nusoft.com.tw。
 2. 以往在封鎖同時對應多個 IP 的網站（例如：Facebook、Yahoo、...）時，只能逐一輸入人工查詢網站對應的 IP、網段，容易會有所遺漏，若採以 FQDN 設定外部網路位址表，系統會自動查詢網站使用的所有 IP 位址。
 3. FQDN 功能可以運用在網站黑/白名單功能鞭長莫及的地方（網站黑/白名單功能僅可管制 HTTP），例如：HTTPS、FTP。只要於外部網路位址表設定網站的 FQDN，再於管制條例中套用並封鎖之即可。
-

網際協定 說明如下：

- 位址表採用的網際網路協定，可為 IPv4 或 IPv6。

IP 位址 說明如下：

- 可以是一個主機 IP 位址，也可以是一個網段。可分為三種不同的網路區段：內部網路 IP 位址(Internal IP Address)、外部網路 IP 位址(External IP Address) 和非軍事區網路 IP 位址(DMZ IP Address)。

子網路遮罩 說明如下：

- 對應 IPv4 單一特定 IP 時，應設定為 255.255.255.255。
- 對應 IPv4 一特定網段時（例如：192.168.100.x 之 C Class 網段的 IP），應設定為 255.255.255.0。

首碼長度 說明如下：

- 對應 IPv6 單一特定 IP 時，應設定為 128。
- 對應 IPv6 一特定網段時（例如：21DA:D3:0:2F3B:2AA:FF:FE28:9C5A，前置字元是 21DA:D3:0:2F3B），應設定為 64，衍生的子網路識別碼為 21DA:D3:0:2F3B::/64。

MAC 位址 說明如下：

- 將特定單一主機之網卡 MAC 位址與其 IP 位址對應，可防止使用者更改 IP 位址，透過它條管制條例，存取非授權之網路服務。



說明：

1. 在【遠端】>【管制條例選項】>【位址表】>【外部網路群組】頁面中，*CHU、*CHINA_TELECOM、*CHINA_EDU 與*CHINA_MOBILE 分別代表中國聯通(China Unicom, CHU)、中國電信(China Telecom)、中國教育網與中國移動(China Mobile)所擁有的網路區段。可於對外連線時，依封包傳送目的位址，透過管制條例指定適當的傳輸線路，達到策略路由(PBR)的效果。
-

11.1 位址表功能使用範例

11.1.1 將遠端UTM、MHG特定內部IP位址指定給固定使用者使用，

並限制其僅能透過管制條例以FTP協定存取網路資源

步驟1. 在【遠端】>【管制條例選項】>【位址表】>【內部網路】頁面中，做下列設定：（如圖 11-1）

- 輸入使用者的【名稱】。
- 【IP 位址範圍】選擇以 IPv4 位址 / 子網路遮罩定義。
- 【網際協定】選擇 IPv4。
- 輸入使用者的【IP 位址】。
- 【子網路遮罩】輸入 255.255.255.255。（代表 1 個 IP 位址）
- 輸入使用者的【MAC 位址】。
- 按下【確定】鈕，完成設定。（如圖 11-2）

新增位址

名稱: Rayearth (最多 16 個字元)

IP位址範圍: ☒ 以 IPv4 位址 / 子網路遮罩定義 ☐ 直接定義

網際協定: IPv4

IP位址: 192.168.3.2 (例如: 192.168.1.10)

子網路遮罩: 255.255.255.255 (255.255.255.255 是指單一電腦, 255.255.255.0 是指 class C 的子網路)

MAC位址: 00:B0:18:25:F5:89

圖 11-1 設定內部網路位址表

匯出內部網路位址表至用戶端:


從用戶端匯入內部網路位址表: (最大檔案大小: 1 MBytes)

名稱	網際協定	網路介面	IP 位址	MAC位址	變更
Inside Any	---	全部	---		使用中
Rayearth	IPv4	全部	192.168.3.2 / 255.255.255.255	00:B0:18:25:F5:89	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 11-2 完成內部網路位址表設定



說明：

1. 系統管理員可【匯出】來整理和保存相關設定資料，以利未來 CMS-2000【內部網路】、【外部網路】、【非軍事區網路】位址表錯亂時，可清除規則表重新【匯入】。
 2. 系統管理員在設定位址表時，可利用點選  的方式，讓 CMS-2000 自動填入指定 IP 位址對應的 MAC 位址。
 3. 在【遠端】>【管制條例選項】>【位址表】>【內部網路】頁面中，CMS-2000 會自動預設一條 Inside Any 的位址表，此位址表代表了整個內部網路。其他如【外部網路】、【非軍事區網路】一樣有代表整個網域的 Outside Any 與 DMZ Any 預設位址表設定。
 4. 【遠端】>【管制條例選項】>【位址表】>【外部網路】與【非軍事區網路】其設定模式與【內部網路】相同；唯一的不同的是【外部網路】無法設定 MAC 位址。
-

步驟2. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 11-3）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【來源網路位址】選擇所設定的內部網路位址表規則。
- 【服務名稱】選擇 FTP。
- 按下【確定】鈕，完成設定。（如圖 11-4）

新增管制條例

分配：
☒ 裝置：UTMM72.19.20.11
☐ 群組：GROUP_1

來源網路位址：Rayearth
 目的網路位址：Outside Any
 服務名稱：FTP
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：----- None -----

動作：
☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面
 僅允許下列網路介面：
☒ (LAN1) ☐ (WAN1) ☐ (WAN2) ☐ (DMZ1)

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

網站管制：----- None -----
 應用程式管制：----- None -----

[+ 進階設定](#)

確定 取消

圖 11-3 設定限制單一使用者透過特定服務存取網路資源之管制條例

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Rayearth	Outside Any	FTP	✓		修改 刪除 暫停

1 / 1 移至

新增

圖 11-4 完成管制條例設定

步驟3. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 11-5, 圖 11-6)

匯出內部網路位址表至用戶端:

從用戶端匯入內部網路位址表: (最大檔案大小: 1 MBytes)

[輔助選取](#) ◀◀ 1 / 1 ▶▶ 移至 ▶▶

名稱 ▲	網際協定	網路介面	IP 位址	MAC位址	變更
Inside Any	---	全部	---		<input type="button" value="使用中"/>
CMS_Rayearth	IPv4	全部	192.168.3.2 / 255.255.255.255	00:B0:18:25:F5:89	<input type="button" value="修改"/>

◀◀ 1 / 1 ▶▶ 移至 ▶▶

圖 11-5 遠端 UTM、MHG 內部網路位址表設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶

來源網路	目的網路	服務名稱	動作	項目	變更	排序
CMS_Rayearth	Outside Any	FTP	✓		<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	1 ▼

◀◀ 1 / 1 ▶▶ 移至 ▶▶

圖 11-6 遠端 UTM、MHG 管制條例設定





第12章 服務表

TCP 和 UDP 協定提供各種不同的服務，每一個服務都有對應的埠號，例如：TELNET(TCP 埠 23)、SMTP(TCP 埠 25)、POP3(TCP 埠 110)、...

- **【基本服務】**：定義了常用的 TCP 和 UDP 服務，不能修改也不可刪除。
- **【自訂服務】**：用來設定欲使用的特定 TCP 和 UDP 埠。

【基本服務】功能概述：

基本服務 說明如下：

圖示	說明
	任何 TCP、UDP 服務，如：Any。
	ICMP 協定，如：PING、Traceroute。
	TCP 服務，如：AFPOverTCP、AOL、BGP、FINGER、FTP、GOPHER、HTTP、HTTPS、InterLocator、IRC、L2TP、LDAP、MSN、NetMeeting、NNTP、POP3、PPTP、Real-Media、RLOGIN、SMTP、SSH、TCP-Any、TELNET、VDO-Live、WAIS、WINFRAME、X-Windows。
	UDP 服務，如：DNS、IKE、IMAP、NFS、NTP、PC-Anywhere、RIP、SNMP、SYSLOG、TALK、TFTP、UDP-Any、UUCP。

【自訂服務】功能概述：

名稱 說明如下：

- 系統管理員可在此為自訂的服務命名。

通訊協定 說明如下：

- 設備彼此之間溝通所需求之協定，一般常用為 TCP 和 UDP。

用戶端 說明如下：

- 用戶端電腦之網卡使用的埠號，建議使用預設範圍。

伺服器端 說明如下：

- 可在此輸入所要自訂服務之埠號。



說明：

1. 在一般的情況下，用戶端電腦之網路卡的埠號，其範圍為 0-65535。建議不要修改【遠端】>【管制條例選項】>【服務表】>【自訂服務】的【用戶端】範圍。

2. 在界定埠號範圍的兩個空格內輸入不同數值，代表開啓此一區間埠號（如 15328：15333）；若兩個空格內輸入相同數值，代表開啓單一埠號（如 1720：1720）。
-

12.1 服務表功能使用範例

12.1.1 在遠端UTM、MHG建立服務群組，並限制使用者僅能透過管

制條例上網存取此群組提供之服務資源。(群組：HTTP、POP3、

SMTP、DNS)

步驟1. 在【遠端】>【管制條例選項】>【服務表】>【服務群組】頁面中，做下列設定：(如圖 12-1)

- 輸入指定服務【群組名稱】。
- 將【可選取的服務】(HTTP、POP3、SMTP、DNS)新增至【被選取的服務】清單中。
- 按下【確定】鈕，完成設定。(如圖 12-2)

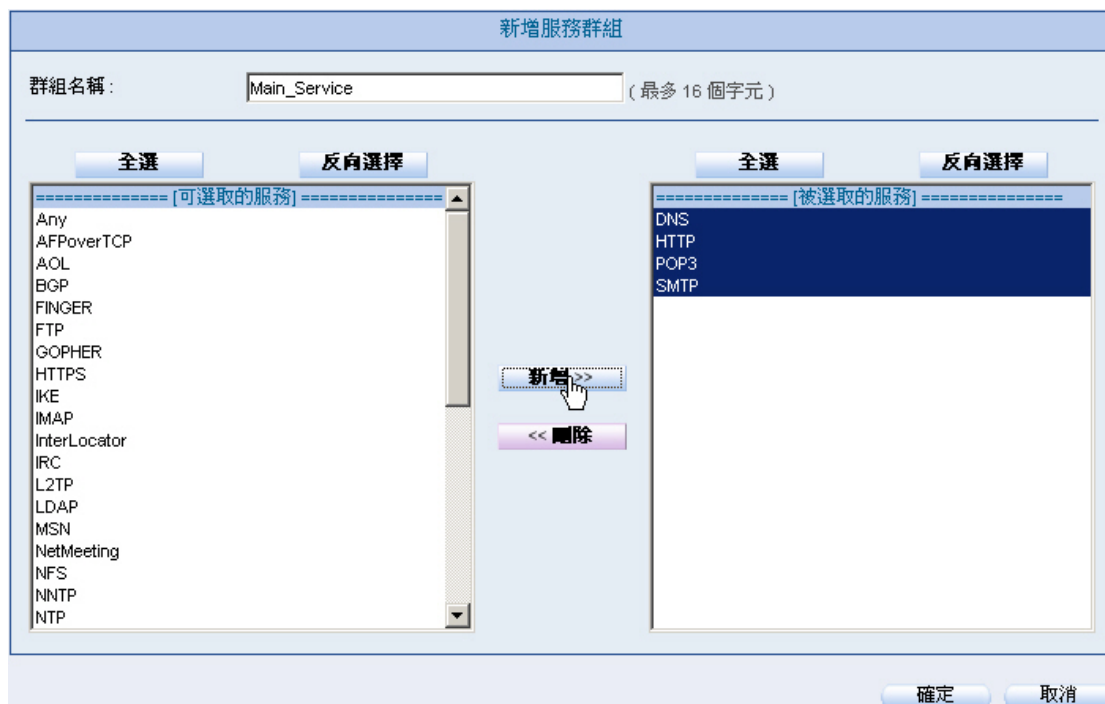


圖 12-1 設定服務群組

名稱 ▲	成員	變更
Main_Service	DNS, HTTP, POP3, SMTP	<div>修改</div> <div>刪除</div>

圖 12-2 完成服務群組設定

步驟2. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 12-3）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【服務名稱】選擇所設定的服務群組規則。
- 按下【確定】鈕，完成設定。（如圖 12-4）

新增管制條例

分配：
☒ 裝置：UTMM72.19.20.11
☐ 群組：GROUP_1

來源網路位址：Inside Any
 目的網路位址：Outside Any
 服務名稱：Main_Service
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：----- None -----

動作：
☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面
 僅允許下列網路介面：
☐ (LAN1) ☐ (WAN1) ☐ (WAN2) ☐ (DMZ1)

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

網站管制：----- None -----
 應用程式管制：----- None -----

[+ 進階設定](#)

確定 取消

圖 12-3 設定使用者存取指定網路服務之管制條例

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Inside Any	Outside Any	Main_Servi...	✓		修改 刪除 暫停

1 / 1 移至

新增

圖 12-4 完成管制條例設定

步驟3. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 12-5, 圖 12-6)

		◀◀ ◀ ◻ / 1 移至 ▶▶▶▶
名稱 ▲	成員	變更
CMS_Main_Service	DNS, HTTP, POP3, SMTP	修改
		◀◀ ◀ ◻ / 1 移至 ▶▶▶▶
新增		

圖 12-5 遠端 UTM、MHG 服務群組設定

														◀◀ ◻ / 1 移至 ▶▶▶▶			
來源網路	目的網路	服務名稱	動作	項目										變更			排序
Inside Any	Outside Any	CMS_Main...	✔											修改	刪除	暫停	1 ▼
														◀◀ ◻ / 1 移至 ▶▶▶▶			
新增																	

圖 12-6 遠端 UTM、MHG 管制條例設定

第13章 排程表

用來安排遠端 UTM、MHG 管制條例的執行時段，以便於管理網路來發揮其最大效能。

【設定】功能概述：

名稱 說明如下：

- 排程規則的辨識名稱。

排程模式 說明如下：

- 排程規則的運作模式可為：
 - ◆ 循環：以一週為基準，個別定義星期一～星期日每天的時段，讓套用此排程的管制條例持續按時管理上網權限。
 - ◆ 一次：依照年、月、日、時、分定義一期限，讓套用此排程的管制條例僅在此期限內管理上網權限。

13.1 排程表功能使用範例

13.1.1 規劃遠端UTM、MHG內部使用者，一週中每天透過管制條例

存取網路資料的有效時段

步驟1. 在【遠端】>【管制條例選項】>【排程表】>【設定】頁面中，做下列設定：

- 按下【新增】鈕。
- 輸入指定的第一段排程【名稱】。
- 選擇指定的第一段【排程模式】。
- 使用下拉式選單安排每天的第一運作時段。
- 按下【確定】鈕。(如圖 13-1)
- 再次按下【新增】鈕。
- 輸入指定的第二段排程【名稱】。
- 選擇指定的第二段【排程模式】。
- 使用下拉式選單安排每天的第二運作時段。
- 按下【確定】鈕，完成設定。(如圖 13-2, 圖 13-3)

新增排程

名稱： (最多 16 個字元)

排程模式：☒ 循環 ☐ 一次

星期	時段	
	開始時間	結束時間
星期日	<input type="text" value="Disabled"/>	<input type="text" value="Disabled"/>
星期一	<input type="text" value="12:30"/>	<input type="text" value="13:00"/>
星期二	<input type="text" value="12:30"/>	<input type="text" value="13:00"/>
星期三	<input type="text" value="12:30"/>	<input type="text" value="13:00"/>
星期四	<input type="text" value="12:30"/>	<input type="text" value="13:00"/>
星期五	<input type="text" value="12:30"/>	<input type="text" value="13:00"/>
星期六	<input type="text" value="Disabled"/>	<input type="text" value="Disabled"/>

圖 13-1 設定第一條排程表規則

新增排程

名稱: (最多 16 個字元)

排程模式: ☒ 循環 ☐ 一次

星期	時段	
	開始時間	結束時間
星期日	Disabled	Disabled
星期一	18:30	19:00
星期二	18:30	19:00
星期三	18:30	19:00
星期四	18:30	19:00
星期五	18:30	19:00
星期六	Disabled	Disabled

圖 13-2 設定第二條排程表規則

1 / 1
移至

名稱 ▲	排程模式	時間	變更
Rest_01	循環	星期日	關閉
		星期一	12 : 30 ~ 13 : 00
		星期二	12 : 30 ~ 13 : 00
		星期三	12 : 30 ~ 13 : 00
		星期四	12 : 30 ~ 13 : 00
		星期五	12 : 30 ~ 13 : 00
		星期六	關閉
Rest_02	循環	星期日	關閉
		星期一	18 : 30 ~ 19 : 00
		星期二	18 : 30 ~ 19 : 00
		星期三	18 : 30 ~ 19 : 00
		星期四	18 : 30 ~ 19 : 00
		星期五	18 : 30 ~ 19 : 00
		星期六	關閉

1 / 1
移至

圖 13-3 完成排程表設定

步驟2. 在【遠端】>【管制條例選項】>【排程表】>【排程群組】頁面中，做下列設定：（如圖 13-4）

- 輸入指定排程【群組名稱】
- 將【可選取的排程】（Rest_01、Rest_02）新增至【被選取的排程】清單中。
- 按下【確定】鈕，完成設定。（如圖 13-5）

圖 13-4 設定排程群組

名稱	成員	變更
Rest_Time	Rest_01, Rest_02	修改 刪除

圖 13-5 完成排程群組設定

步驟3. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 13-6）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【自動排程】選擇所設定的排程表規則。
- 按下【確定】鈕，完成設定。（如圖 13-7）

新增管制條例

分配：
☒ 裝置：UTM172.19.20.11
☐ 群組：GROUP_1

來源網路位址：Inside Any
 目的網路位址：Outside Any
 服務名稱：Any
 自動排程：Rest_Time
 認證名稱：None
 VPN：None

動作：
☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面
 僅允許下列網路介面：
☐ (LAN1) ☐ (WAN1) ☐ (WAN2) ☐ (DMZ1)

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

網站管制：None
 應用程式管制：None

[+ 進階設定](#)

確定 取消

圖 13-6 管制條例套用排程規則

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Inside Any	Outside Any	Any	✓		修改 刪除 暫停

1 / 1 移至

新增

圖 13-7 完成管制條例設定

步驟4. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 13-8, 圖 13-9, 圖 13-10)

名稱▲	排程模式	時間	變更
CMS_Rest_01	循環	星期日	關閉
		星期一	12:30 ~ 13:00
		星期二	12:30 ~ 13:00
		星期三	12:30 ~ 13:00
		星期四	12:30 ~ 13:00
		星期五	12:30 ~ 13:00
		星期六	關閉
CMS_Rest_02	循環	星期日	關閉
		星期一	18:30 ~ 19:00
		星期二	18:30 ~ 19:00
		星期三	18:30 ~ 19:00
		星期四	18:30 ~ 19:00
		星期五	18:30 ~ 19:00
		星期六	關閉

1 / 1 移至

新增

圖 13-8 遠端 UTM、MHG 排程表設定

名稱▲	成員	變更
CMS_Rest_Time	CMS_Rest_01, CMS_Rest_02	修改

1 / 1 移至

新增

圖 13-9 遠端 UTM、MHG 排程群組設定

來源網路	目的網路	服務名稱	動作	項目	變更	排序
Inside Any	Outside Any	Any	✓		修改 刪除 暫停	1

1 / 1 移至

新增

圖 13-10 遠端 UTM、MHG 管制條例設定

第14章 頻寬表

用來控管透過遠端 UTM、MHG 存取網路資源所使用的頻寬。可藉由管制條例運用適合的頻寬管理規則，有效分配、充分利用所能使用的頻寬。(如圖 14-1, 圖 14-2)

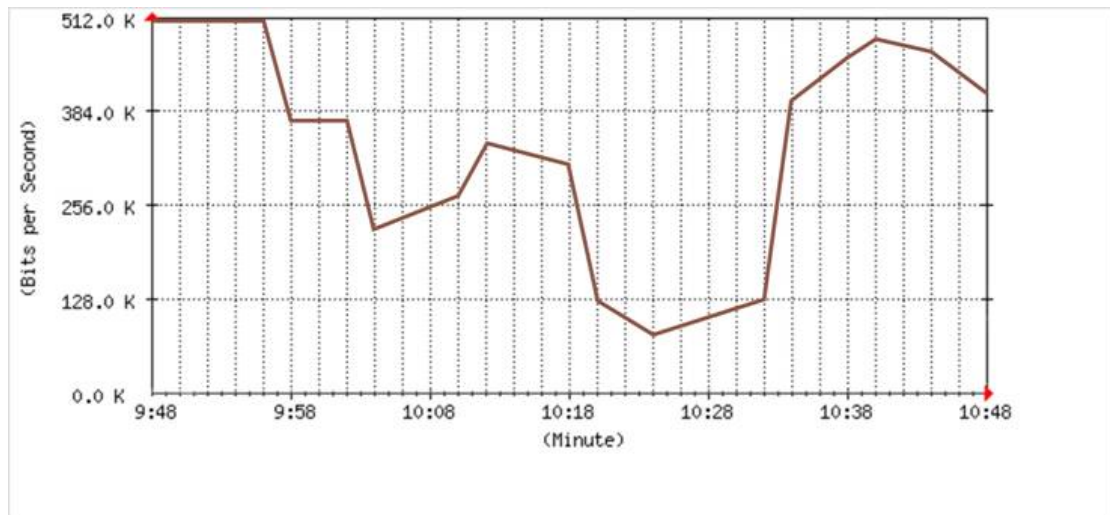


圖 14-1 未經頻寬管理的網路流量

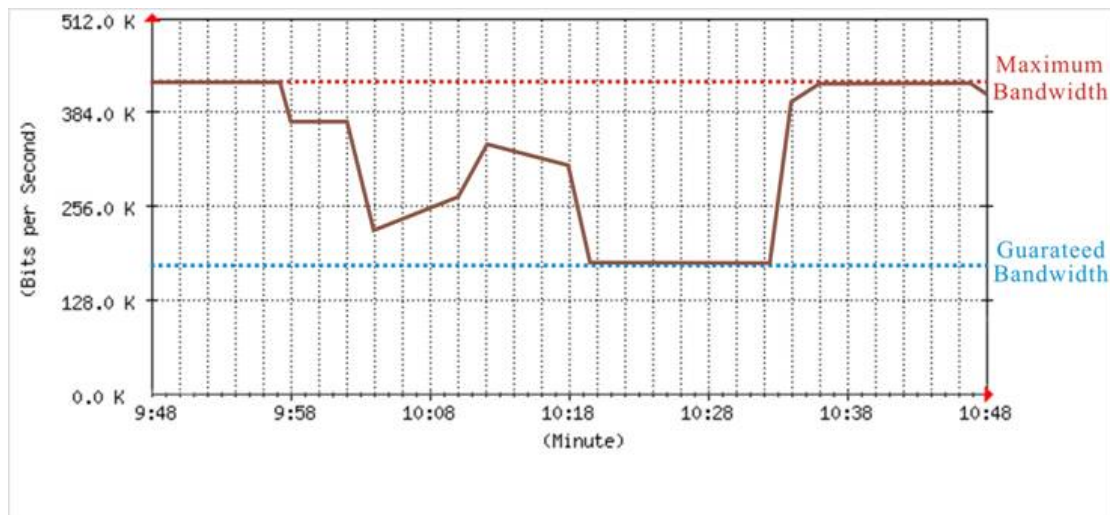


圖 14-2 經頻寬管理後的網路流量（最大頻寬：400 Kbps, 保證頻寬：200Kbps）

【設定】功能概述：

名稱 說明如下：

- 頻寬管制規則的辨識名稱。

網路介面 說明如下：

- 指設定為外部網路介面的網路埠。

下載頻寬 說明如下：

- 設定可運用的線路保證及最大下載頻寬。

上傳頻寬 說明如下：

- 設定可運用的線路保證及最大上傳頻寬。

優先權 說明如下：

- 設定未使用的下載和上傳頻寬分配優先權。

保證頻寬 說明如下：

- 在管制規則中，可使用的線路基本頻寬。

最大頻寬 說明如下：

- 在管制規則中，可使用的線路最大頻寬。

14.1 頻寬表功能使用範例

14.1.1 管制遠端UTM、MHG內部使用者對外傳輸檔案可用頻寬

步驟1. 在【遠端】>【管制條例選項】>【頻寬表】>【設定】頁面中，做下列設定：（如圖 14-3）

- 輸入頻寬表【名稱】。
- 在【網路介面】WAN1、WAN2 中，輸入所要限定之頻寬大小。
- 選擇頻寬表之【優先權】。
- 按下【確定】鈕，完成設定。（如圖 14-4）

新增頻寬表

名稱：

網路介面	下載頻寬		上傳頻寬		優先權
1 (WAN)	保證頻寬 = <input type="text" value="200"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="400"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="200"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="400"/> Kbps (範圍: 1 - 204800)	<div style="border: 1px solid black; padding: 2px; text-align: center;">中 ▼</div>
2 (WAN)	保證頻寬 = <input type="text" value="300"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="400"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="50"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="64"/> Kbps (範圍: 1 - 204800)	
3 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
4 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
5 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
6 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
7 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
8 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
9 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
10 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
11 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
12 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
13 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
14 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
15 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	
16 (WAN)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	保證頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	最大頻寬 = <input type="text" value="0"/> Kbps (範圍: 1 - 204800)	

圖 14-3 設定頻寬表

名稱 ▲	網路介面	下載頻寬	上傳頻寬	優先權	變更
Policy_QoS	1 (WAN)	保證頻寬 = 200 Kbps 最大頻寬 = 400 Kbps	保證頻寬 = 200 Kbps 最大頻寬 = 400 Kbps	中	<div>修改</div> <div>刪除</div>
	2 (WAN)	保證頻寬 = 300 Kbps 最大頻寬 = 400 Kbps	保證頻寬 = 50 Kbps 最大頻寬 = 64 Kbps		
	3 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	4 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	5 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	6 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	7 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	8 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	9 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	10 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	11 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	12 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	13 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	14 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	15 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	16 (WAN)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
					<div>新增</div>

◀◀◻▶▶

/ 1 移至 ▶▶▶

圖 14-4 完成頻寬表設定

步驟2. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 14-5）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【頻寬管理】選擇所設定的頻寬表規則。
- 按下【確定】鈕，完成設定。（如圖 14-6）

新增管制條例	
分配：	<input checked="" type="radio"/> 裝置：UTM172.19.20.11 <input type="radio"/> 群組：GROUP_1
來源網路位址：	Inside Any
目的網路位址：	Outside Any
服務名稱：	Any
自動排程：	----- None -----
認證名稱：	----- None -----
VPN：	----- None -----
動作：	<input checked="" type="checkbox"/> 允許所有外部網路介面 <input type="checkbox"/> 拒絕所有外部網路介面 僅允許下列網路介面： <input type="checkbox"/> (LAN1) <input type="checkbox"/> (WAN1) <input type="checkbox"/> (WAN2) <input type="checkbox"/> (DMZ1)
報告機制：	
封包記錄：	<input type="checkbox"/> 開啓
流量圖表：	<input type="checkbox"/> 開啓
網站管制：	----- None -----
應用程式管制：	----- None -----
<input checked="" type="checkbox"/> 進階設定 入侵偵測防禦： <input type="checkbox"/> 開啓	
病毒偵測：	<input type="checkbox"/> POP3 <input type="checkbox"/> SMTP <input type="checkbox"/> HTTP / Webmail <input type="checkbox"/> FTP
垃圾郵件過濾：	<input type="checkbox"/> POP3 <input type="checkbox"/> SMTP
郵件 歸檔 / 稽核：	<input type="checkbox"/> POP3 (僅歸檔) <input type="checkbox"/> SMTP
IM側錄：	<input type="checkbox"/> 開啓
頻寬管理：	Policy_QoS
每個來源IP最大頻寬限制：	下載頻寬 0 Kbps / 上傳頻寬 0 Kbps (0: 表示不限制)
P2P 軟體最大頻寬限制：	下載頻寬 0 Kbps / 上傳頻寬 0 Kbps (0: 表示不限制)
每個來源IP最大連線數限制：	0 (範圍: 1 - 99999, 0: 表示不限制)
最大連線數限制：	0 (範圍: 1 - 99999, 0: 表示不限制)
每個連線的傳輸量限制：	0 KBytes (範圍: 1 - 999999, 0: 表示不限制)
每個來源IP的傳輸量限制：	0 MBytes (範圍: 1 - 999999, 0: 表示不限制)
每天的傳輸量限制：	0 MBytes (範圍: 1 - 999999, 0: 表示不限制)
傳送模式：	LAN1: 自動 WAN1: 自動 WAN2: 自動 DMZ1: 自動
<input type="button" value="說明"/>	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 14-5 管制條例套用頻寬管理規則

裝置名稱: 全部 1 / 1 移至

來源網路	目的網路	服務名稱	動作	項目								變更
Inside Any	Outside Any	Any	✓									修改
1 / 1 移至												

新增

圖 14-6 完成管制條例設定



說明：

1. 系統管理員設定【頻寬表】的根據，即遠端 UTM、MHG【網路介面】>【介面位址】頁面中，設定為外部網路介面的【下載頻寬】與【上傳頻寬】，故系統管理員務必準確設定其上傳、下載頻寬。

步驟3. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 14-7, 圖 14-8)

名稱 ▲	網路介面	下載頻寬	上傳頻寬	優先權	變更
CMS_Policy_QoS	1 (LAN1)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	中	修改
	2 (WAN1)	保證頻寬 = 200 Kbps 最大頻寬 = 400 Kbps	保證頻寬 = 200 Kbps 最大頻寬 = 400 Kbps		
	3 (WAN2)	保證頻寬 = 300 Kbps 最大頻寬 = 400 Kbps	保證頻寬 = 50 Kbps 最大頻寬 = 64 Kbps		
	4 (DMZ1)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	5 (Port5)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	6 (Port6)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		
	7 (Port7)	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps	保證頻寬 = 0 Kbps 最大頻寬 = 0 Kbps		

圖 14-7 遠端 UTM、MHG 頻寬表設定

來源網路	目的網路	服務名稱	動作	項目	變更	排序
Inside Any	Outside Any	Any	✓		修改 刪除 暫停	1

圖 14-8 遠端 UTM、MHG 管制條例設定

第15章 認證表

採用內建認證帳戶和群組驗證機制，來控管透過遠端 UTM、MHG 存取網路資源的權限。

【認證帳戶】功能概述：

帳戶名稱 說明如下：

- 用於設定系統內建之認證使用者帳號。

密碼 說明如下：

- 建立認證時所需要的密碼。

確認密碼 說明如下：

- 輸入與密碼欄一致的字串。

使用者必須在下次登入時變更密碼 說明如下：

- 於啓用此後能後，內建認證帳戶進行首次認證時，會強制其變更認證密碼。

認證帳號有效日期 說明如下：

- 設定內建認證帳戶的使用期限。

15.1 認證帳戶和群組功能使用範例

15.1.1 規劃遠端UTM、MHG內部使用者必須通過管制條例之認證機制，方可連線至外部網路

制，方可連線至外部網路

步驟1. 在【遠端】>【管制條例選項】>【認證表】>【認證帳戶】頁面中，建立多筆認證帳戶。(如圖 15-1)

匯出認證帳戶表至用戶端:

從用戶端匯入認證帳戶表: (最大檔案大小: 1 MBytes)

帳戶名稱 ▲	到期日	變更
joy		<input type="button" value="修改"/> <input type="button" value="刪除"/>
john		<input type="button" value="修改"/> <input type="button" value="刪除"/>
jack		<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 15-1 認證帳戶設定



說明：

1. 系統管理員可【匯出】來整理和保存相關設定資料，以利未來 CMS-2000【認證帳戶】名單錯亂時，可清除名單表重新【匯入】。

步驟2. 在【遠端】>【管制條例選項】>【認證表】>【認證群組】頁面中，做下列設定：（如圖 15-2）

- 輸入認證群組【名稱】。
- 將指定【可選取的帳戶】新增至【被選取的帳戶】清單中。
- 按下【確定】鈕，完成設定。

圖 15-2 認證群組設定頁面

步驟3. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 15-3）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【認證名稱】選擇所設定的認證群組規則。
- 按下【確定】鈕，完成設定。（如圖 15-4）

新增管制條例

分配：
☒ 裝置：UTM172.19.20.11
☐ 群組：GROUP_1

來源網路位址：Inside Any
 目的網路位址：Outside Any
 服務名稱：Any
 自動排程：----- None -----
 認證名稱：laboratory
 VPN：----- None -----

動作：
☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面
 僅允許下列網路介面：
☐ (LAN1) ☐ (WAN1) ☐ (WAN2) ☐ (DMZ1)

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

網站管制：----- None -----
 應用程式管制：----- None -----

[+ 進階設定](#)

確定 取消

圖 15-3 管制條例套用認證規則

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Inside Any	Outside Any	Any	✓	🔒	修改 刪除 暫停

1 / 1 移至

新增

圖 15-4 完成管制條例設定

步驟4. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 15-5, 圖 15-6, 圖 15-7)

匯出認證帳戶表至用戶端:

從用戶端匯入認證帳戶表: (最大檔案大小: 1 MBytes)

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

帳戶名稱 ▲	到期日	變更
joy		<input type="button" value="修改"/>
john		<input type="button" value="修改"/>
jack		<input type="button" value="修改"/>

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 15-5 遠端 UTM、MHG 認證帳戶設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

名稱 ▲	成員	RADIUS	POP3	LDAP	變更
CMS_laboratory	joy, john, jack	✗	✗	✗	<input type="button" value="修改"/>

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 15-6 遠端 UTM、MHG 認證群組設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

來源網路	目的網路	服務名稱	動作	項目	變更	排序
Inside Any	Outside Any	Any	✔	🔒	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	1 ▼

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 15-7 遠端 UTM、MHG 管制條例設定

第16章 應用程式管制

用來控管透過遠端 UTM、MHG 使用即時通訊登入、即時通訊傳檔、點對點軟體、影音軟體、網頁郵件、線上遊戲、通道軟體和遠端控制軟體的行為。

【設定】功能概述：

應用程式特徵檔更新資訊 說明如下：

- 應用程式管制之特徵定義檔每隔 60 分鐘就會自動更新，或可手動做立即更新。同時會顯示特徵定義檔之更新時間和版本。

即時通訊登入 說明如下：

- 可阻擋使用者登入 MSN、Yahoo、ICQ/AIM、QQ、Skype、Google Talk、Gadu-Gadu、Rediff、WebIM、阿里旺旺、百度 Hi、新浪 UC、Fetion、Facebook 聊天室、Camfrog、LINE、WhatsApp 和 Viber。

即時通訊傳檔 說明如下：

- 可阻擋使用者透過 MSN、Yahoo、ICQ/AIM、QQ、Google Talk 和 Gadu-Gadu 傳送檔案。

點對點軟體 說明如下：

- 可阻擋使用者建立 eDonkey/eMule、Bit Torrent/BitConnect、WinMX、Foxy、KuGoo、AppleJuice、AudioGalaxy、DirectConnect、iMesh、MUTE、迅雷 5、GoGoBox、QQ 旋風、Ares、Shareaza、BearShare、Morpheus、Limewire、KaZaa 和 FlashGet 連線。

影音軟體 說明如下：

- 可阻擋使用者使用 PPTV 網路電視、PPS 網路電視、UUSee 網路電視、QQLive、ezPeer、快播/波波虎、Fusion、PPMate 網路電視、PiPi、暴風影音、SopCast 網路電視、CNTV 和迅雷看看軟體。

網頁郵件 說明如下：

- 可阻擋使用者登入 Gmail、Hotmail、Yahoo、Hinet、PChome、智邦、Yam 天空、Seednet、163/126/Yeah、Tom、新浪任你郵、搜狐和 QQ 網頁郵件。

線上遊戲 說明如下：

- 可阻擋使用者登入聯眾世界、QQ 遊戲和迅雷遊戲大廳軟體。

通道軟體 說明如下：

- 可阻擋使用者建立 VNN Client、無界瀏覽、Tor、Hamachi、綠盾和自由門連線。

遠端控制軟體 說明如下：

- 可阻擋使用者建立 TeamViewer、VNC、遠端桌面和 ShowMyPC 連線。

16.1 應用程式管制功能使用範例

16.1.1 限制遠端UTM、MHG內部使用者以點對點軟體存取網路上之

檔案

步驟1. 在【遠端】>【管制條例選項】>【應用程式管制】>【設定】頁面中，做下列設定：（如圖 16-1）

- 輸入應用程式管制【名稱】。
- 展開【點對點軟體】選單，勾選【全選】選項。
- 按下【確定】鈕，完成設定。（如圖 16-2）

新增應用程式管制規則

名稱: P2P_Blocking (最多 16 個字元)

- 即時通訊登入
- 即時通訊傳輸
- 點對點軟體 (☒ 全選)
 - ☒ Edonkey/eMule
 - ☒ Bit Torrent/BitConnect
 - ☒ WinMX
 - ☒ Foxy
 - ☒ KuGoo
 - ☒ AppleJuice
 - ☒ AudioGalaxy
 - ☒ DirectConnect
 - ☒ iMesh
 - ☒ MUTE
 - ☒ 迅雷5
 - ☒ GoGoBox
 - ☒ QQ旋風
 - ☒ Ares
 - ☒ Shareaza
 - ☒ BearShare
 - ☒ Morpheus
 - ☒ Linewire
 - ☒ KaZaa
 - ☒ FlashGet
- 影音軟體
- 網頁郵件
- 線上遊戲
- 通道軟體
- 遠端控制軟體
- 其他軟體

確定 取消

圖 16-1 設定點對點軟體管制

步驟2. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 16-3）

- 【分配】選擇指定的遠端 UTM、MHG。
- 選擇所設定的【應用程式管制】規則。
- 按下【確定】鈕，完成設定。（如圖 16-4）

新增管制條例

分配：
☒ 裝置：UTM172.19.20.11
☐ 群組：GROUP_1

來源網路位址：Inside Any
 目的網路位址：Outside Any
 服務名稱：Any
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：----- None -----

動作：
☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面
 僅允許下列網路介面：
☐ (LAN1) ☐ (WAN1) ☐ (WAN2) ☐ (DMZ1)

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

網站管制：----- None -----
 應用程式管制：P2P_Blocking

[+ 進階設定](#)

確定 取消

圖 16-3 管制條例套用點對點軟體管制規則

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Inside Any	Outside Any	Any	✓	<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>	<div> <div>修改</div> <div>刪除</div> <div>暫停</div> </div>

1 / 1 移至

新增

圖 16-4 完成管制條例設定

第17章 虛擬伺服器

用於將遠端 UTM、MHG 外部網路介面的真實 IP 位址，對應至內部網路設備的私有 IP 位址，以對外提供特定的網路服務。

- **【IP 對應】**：即一個外部網路真實 IP 位址的所有服務（埠號），對應到一個內部網路私有 IP 位址。
- **【連接埠對應】**：即一個外部網路真實 IP 位址，可對應到提供不同服務的多個內部網路私有 IP 位址。另外，可同時對應多個提供相同服務內容的內部網路私有 IP 位址，將尋求服務的連線循環分配給內部網路的伺服器群組。如此可減少單一伺服器的負載，降低當機的風險，提高伺服器的工作效率。
- **【連接埠對應群組】**：將**【連接埠對應】**規則群組，以特定的管制條例進行控管。

【IP 對應】功能概述：

裝置名稱 說明如下：

- 選擇和 CMS-2000 連線的裝置，將所設規則建立在該遠端 UTM、MHG。

外部網路位址 說明如下：

- 外部網路介面的真實 IP 位址。

對應到虛擬網路位址 說明如下：

- 外部網路真實 IP 位址對應的內部網路私有 IP 位址。

【連接埠對應】功能概述：

伺服器真實 IP 說明如下：

- 虛擬伺服器所採用的外部網路真實 IP 位址。

服務 說明如下：

- 虛擬伺服器可對應的服務項目名稱。

對外連線埠號 說明如下：

- 虛擬伺服器所對應的對外服務埠號。若所選擇的服務項目只有使用單一埠號時，則可在此變更其對外的埠號。（如將 HTTP 的埠號改為 8080，則外部使用者就必須以此埠號，存取所提供的 HTTP 服務）

伺服器負載平衡模式 說明如下：

- 循環分配：可將尋求服務的連線，依序分配給內部網路提供相同服務的伺服器群組；可減少單一伺服器的負載，提高伺服器的工作效率。（外部使用者若已有存取伺服器的連線，於其全部終止後遠端 UTM、MHG 尚會保留一段時間，以利使用者在限定時間內向同一台主機尋求服務）
- 備援模式：當主要伺服器發生異常或故障時，備援的伺服器會依編號順序接替主要伺服器的工作，使服務不致中斷。
- 依來源位址：辨識尋求服務的來源位址，將其連線至所設定的指定伺服器。

網路介面 說明如下：

- 用於指定虛擬伺服器之私有 IP 位址隸屬的網路介面。

伺服器虛擬 IP 說明如下：

- 虛擬伺服器所對應的內部網路私有 IP 位址。

17.1 虛擬伺服器功能使用範例

17.1.1 將遠端UTM、MHG內部提供FTP、Web、Mail等多項服務之

單一伺服器，以IP對應的方式透過管制條例來對外服務

環境設定

申請兩條有固接 IP 的 ADSL 線路，供遠端 UTM、MHG 使用。

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1 所連線路的固接 IP 為 61.11.11.10 ~ 61.11.11.14。

Port3 設為 WAN2 所連線路的固接 IP 為 211.22.22.18 ~ 211.22.22.30。

步驟1. 在遠端 UTM、MHG 內部網路中架設一提供多項服務之伺服器，其網卡 IP 設定為 192.168.1.100、DNS 設定指向於外部 DNS 伺服器。

步驟2. 在【遠端】>【管制條例選項】>【虛擬伺服器】>【IP 對應】頁面中，做下列設定：

- 選擇指定的連線【裝置名稱】。
- 輸入指定的【IP 對應名稱】。
- 【外部網路位址】選擇 WAN1 並輸入 61.11.11.12。（可輔助選取）
- 【對應到虛擬網路位址】選擇 LAN1 並輸入 192.168.1.100。（可輔助選取）
- 按下【確定】鈕，完成設定。（如圖 17-1）



新增對應IP

裝置名稱: UTM/172.19.20.11

IP對應名稱: Main_Server (最多 16 個字元)

外部網路位址: 61.11.11.12 WAN1 輔助選取

對應到虛擬網路位址: 192.168.1.100 LAN1 輔助選取

確定 取消

圖 17-1IP 對應設定頁面

步驟3. 在【遠端】>【管制條例選項】>【服務表】>【服務群組】頁面中，將伺服器所提供的服務（FTP、HTTP、POP3、SMTP）群組化（Main_Service）。（如圖 17-2）

名稱▲	成員	變更
Main_Service	FTP, HTTP, POP3, SMTP	修改 刪除

新增

圖 17-2 服務群組設定

步驟4. 在【遠端】>【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 17-3）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【目的網路位址】選擇所設定的 IP 對應規則。
- 【服務名稱】選擇所設定的服務群組規則。
- 按下【確定】鈕，完成設定。（如圖 17-4）

新增管制條例

分配：
☒ 裝置：UTM/172.19.20.11
☐ 群組：GROUP_1

來源網路位址：Outside Any
 目的網路位址：[IP對應] Main_Server(61.11.11.12)
 服務名稱：Main_Service
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：----- None -----

動作：
☒ 允許 外部至內部 連線
☐ 禁止 外部至內部 連線

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

進階設定

確定 取消

圖 17-3 設定外部使用者存取內部伺服器服務之管制條例

來源網路	目的網路	服務名稱	動作	項目	變更
Outside Any	[IP對應](61.11.11.12)	Main_Servi...	✓		修改 刪除 暫停

新增

圖 17-4 完成管制條例設定

步驟5. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 17-5, 圖 17-6, 圖 17-7)

<div> <div>1 / 1</div> <div>移至</div> </div>			
名稱 ▲	外部網路位址		變更
CMS_Main_Server	61.11.11.12	Port2 (WAN1)	192.168.1.100 / Port1 (LAN1)
<div> <div>1 / 1</div> <div>移至</div> </div>			
<div>新增</div>			

圖 17-5 遠端 UTM、MHG IP 對應設定

<div> <div>1 / 1</div> <div>移至</div> </div>		
名稱 ▲	成員	變更
CMS_Main_Service	FTP, HTTP, POP3, SMTP	修改
<div> <div>1 / 1</div> <div>移至</div> </div>		
<div>新增</div>		

圖 17-6 遠端 UTM、MHG 服務群組設定

1 / 1

移至

來源網路	目的網路	服務名稱	動作	項目								變更			排序	
Outside Any	[IP對應](61.11.11.12)	CMS_Main...	✓										修改	刪除	暫停	1 ▾

1 / 1

移至

新增

圖 17-7 遠端 UTM、MHG 管制條例設定

第18章 VPN

用來建立遠端 UTM、MHG 安全與私密的網路連線，藉以整合企業各分點網路，讓外勤人員便於連線企業網路；企業在網際網路上傳遞資料時，亦能得到最佳的保密效果。

【VPN】專有名詞概述：

Diffie-Hellman 說明如下：

- 為對稱性密碼系統，它可以讓連線兩端在完全沒有彼此任何預先資訊的條件下，透過不安全通道建立起一個金鑰，並使用此金鑰將訊息加密傳送。

RSA 說明如下：

- 為非對稱性密碼系統，使用者擁有兩把金鑰，一個為秘密金鑰，使用者須秘密收藏，為連線解密時用；另一個為公開金鑰，任何欲傳送訊息者皆可自認證中心取得，並使用此金鑰將訊息加密傳送給接收者。

Pre-Shared Key 說明如下：

- IPSec 連線時用來進行驗證的專用密碼。

ISAKMP 說明如下：

- 「IP Security Association Key Management Protocol」(ISAKMP) 就是提供一種方法讓兩台電腦建立安全性關聯 (SA)。SA(Security Association) 對兩台電腦之間進行連線編碼，指定使用哪些演算法和什麼樣的金鑰長度或實際加密金鑰。事實上 SA 不止一個連線方式：從兩台電腦 ISAKMP SA 做為起點，必須指定使用何種加密演算法 (DES、triple DES、40 位元 DES 或根本不用)、使用何種認證。

Main mode 說明如下：

- 在 IPSec 第一階段的 IKE 開始連線時，會提供兩種模式選擇，其中的一種模式就是 Main mode，會對資料交換的雙方先進行認證，Main mode 會提供六個訊息在雙方之間進行傳遞來達到認證的需求，確保與自己交流資料是對方本人，而不是偽造的。

Aggressive mode 說明如下：

- 在 IPSec 第一階段的 IKE 開始連線時，另一種認證模式就是 Aggressive mode，會對資料交換的雙方先進行認證，Aggressive mode 則僅會提供三個訊息在雙方之間進行傳遞來達到認證的需求，確保與自己交流資料是對方本人，而不是偽造的。

AH (Authentication Header) 說明如下：

- 提供 VPN 連線時的認證及選擇性認證檢測。

ESP 說明如下：

- (Encapsulated Security Payload) 提供 VPN 連線時的認證及認證檢測。並對傳送中的資料提供了機密和保護。

DES 說明如下：

- 資料加密標準 (Data Encryption Standard) 是一種 NIST 標準安全加密金鑰方法，使用的加密金鑰為 56 位元。

3DES 說明如下：

- 提供比 DES 更加安全的三重資料加密標準 (Triple Data Encryption Standard, 3DES) 安全加密金鑰方法，使用的加密金鑰為 168 位元。

AES 說明如下：

- 為高階加密模式其標準比 DES 的加密標準更加嚴謹，DES 加密金鑰長度為 56 位元，AES 加密金鑰長度則高達 128 位元、192 位元、以及 256 位元。

NULL 演算法 說明如下：

- 是一種快速又便利的連線模式來取代確保其機密性或負責身份驗證而不進行加密的動作。NULL 演算法不提供機密性也沒有提供其他任何安全服務，僅僅是一條快速方便去替換在使用 ESP 加密時的選項。

SHA1 安全雜湊演算法 (Secure Hash Algorithm, SHA) 說明如下：

- 是用於產生訊息摘要或雜湊的演算法。原有的 SHA 演算法已被改良式的 SHA1 演算法取代。可以計算出 160 位元的演算。

MD5 雜湊演算法 說明如下：

- 一種單向字串雜湊演算，其演算方式是將你給予任何長度字串，使用 MD5 雜湊演算法，可以計算出一個長度為 128 位元的演算。

GRE 通用路由協定封裝 說明如下：

- GRE 只提供了資料包的封裝，它沒有防止網路偵聽和攻擊的加密功能。所以在實際環境中它常和 VPN 一起使用，由 VPN 為用戶資料加密，給用戶提供更好的安全服務。

延伸認證 (Xauth) 說明如下：

- 會在 IPSec 第一階段和第二階段的 IKE 之間插入一個新訊息，為 IPSec 提供 Challenge/Response、Two-factor 等單向非對稱用戶認證方法。



說明：

1. 【延伸認證】會以【遠端】>【管制條例選項】>【認證表】>【認證帳戶】做為驗證依據。
-

【IPSec 自動加密】規則表概述：

名稱 說明如下：

- 用來定義 IPSec 自動加密名稱（不可重複）。

連線介面 說明如下：

- 本地端外部網路介面。

遠端閘道 說明如下：

- 遠端閘道外部網路介面位址。

IPSec 演算法 說明如下：

- 顯示目前 VPN 連線的資料加密模式。

變更 說明如下：

- 修改或刪除 IPSec 自動加密規則。(如圖 18-1)

名稱 ▲	連線介面	遠端閘道	IPSec 演算法	變更
沒有記錄！				
新增				

圖 18-1 IPSec 自動加密規則表



說明：

1. 在預設的情況下，遠端 UTM、MHG 會利用【斷線偵測機制】（Dead Peer Detection）檢查 IPSec VPN 的連線狀態。當【遠端設定】選填遠端閘道 固定 IP 位址 / 網域名稱時，可讓管理者利用【手動連線】方式來建立 IPSec VPN 連線。

【PPTP 伺服器】規則表概述：

使用者名稱 說明如下：

- PPTP 用戶端連入時所使用的驗證名稱。

變更 說明如下：

- 修改或刪除 PPTP 伺服器規則。(如圖 18-2)

使用者名稱 ▲	變更
沒有記錄！	
新增	

圖 18-2PPTP 伺服器規則表

【PPTP 用戶端】規則表概述：

使用者名稱 說明如下：

- PPTP 用戶端連入 PPTP 伺服器時所使用的驗證名稱。

伺服器 IP 位址 / 網域名稱 說明如下：

- PPTP 用戶端連入的 PPTP 伺服器網路位址。

加密認證 說明如下：

- 顯示目前 PPTP 用戶端與 PPTP 伺服器的連線傳輸，是否開啓加密認證機制。

變更 說明如下：

- 修改或刪除 PPTP 用戶端規則。(如圖 18-3)

使用者名稱 ▲	伺服器IP位址 / 網域名稱	加密認證	變更
沒有記錄！			
新增			

圖 18-3 PPTP 用戶端規則表



說明：

1. 在預設的情況下，遠端 UTM、MHG 會利用【Echo-Request】機制，檢查 PPTP VPN 的連線狀態。或讓管理者利用【手動連線】方式來建立 PPTP VPN 連線。
-

【Trunk】規則表概述：

名稱 說明如下：

- 用來定義 VPN Trunk 名稱（不可重複）。

本地端子網路 說明如下：

- 本地端欲透過 VPN 傳輸封包的子網路。

遠端子網路 說明如下：

- 遠端欲透過 VPN 傳輸封包的子網路。

VPN 通道 說明如下：

- 顯示 VPN Trunk 所包含的虛擬私人網路（VPN）通道（IPSec、PPTP 伺服器、PPTP 用戶端）。

變更 說明如下：

- 修改或刪除 VPN Trunk 規則。(如圖 18-4)

名稱 ▲	本地端子網路	遠端子網路	VPN通道	變更
沒有記錄！				
新增				

圖 18-4 VPN Trunk 規則表



說明：

1. 在【啟動 Trunk 負載平衡】機制時，會將單一連線的封包分由所整合的各 VPN 通道同時傳輸，加快完成的速度；同時，亦會依照遠端 UTM、MHG【網路介面】>【介面位址】頁面的【負載平衡模式】，自動調整資料傳送的連線、傳輸狀態。兩端點必須是支援此機制的設備，才能發揮實質效果。

【Trunk 群組】規則表概述：

名稱 說明如下：

- 用來定義 Trunk 群組名稱（不可重複）。

成員 說明如下：

- 群組欲採用相同管制條例的 VPN Trunk 規則。

變更 說明如下：

- 修改或刪除 Trunk 群組規則。(如圖 18-5)

名稱 ▲	成員	變更
沒有記錄！		
新增		

圖 18-5Trunk 群組規則表

18.1 VPN功能使用範例

18.1.1 使用兩台遠端UTM、MHG建立的IPSec VPN連線，存取特定

網段資源

環境設定

甲端點 Port1 設為 LAN1 (192.168.10.1) 為 192.168.10.x/24 網段。

Port2 設為 WAN1 (61.11.11.11) 和 ATU-R 對接，連上網際網路。

乙端點 Port1 設為 LAN1 (192.168.20.1) 為 192.168.20.x/24 網段。

Port2 設為 WAN1 (211.22.22.22) 和 ATU-R 對接，連上網際網路。

有多重網段 (192.168.85.1) 為 192.168.85.X/24 網段。

本範例以兩台遠端 UTM、MHG 做為平台操作，甲端點和乙端點建立 VPN（虛擬私人網路）連線以傳送資料。

甲端點的設定步驟如下：

步驟1. 在【遠端】>【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。（如圖 18-6）

名稱▲	連線介面	遠端閘道	IPSec 演算法	變更
沒有記錄！				
新增				

圖 18-6IPSec 自動加密頁面

步驟2. 選擇指定的連線【裝置名稱】、【名稱】輸入 VPN_A、【連線介面】選擇 WAN1。（如圖 18-7）

基本設定	
裝置名稱：	UTM172.19.20.11
名稱：	VPN_A (最多 16 個字元)
連線介面：	WAN1

圖 18-7 設定連線裝置、IPSec 名稱和外部網路介面

步驟3. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的乙端點閘道位址。(如圖 18-8)



圖 18-8 設定 IPSec 到目的位址

步驟4. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。(如圖 18-9)



圖 18-9 設定 IPSec 認證方法

步驟5. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。(如圖 18-10)

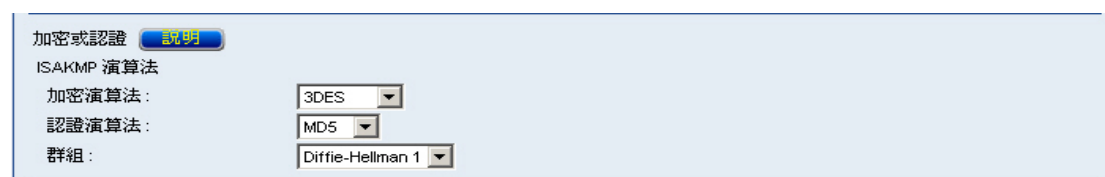


圖 18-10 設定 ISAKMP 演算法

步驟6. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。(如圖 18-11)

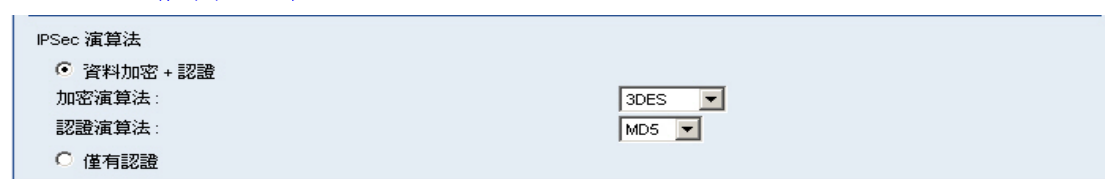


圖 18-11 設定 IPSec 演算法

步驟7. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。(如圖 18-12)



圖 18-12 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟8. 完成 IPSec 自動加密設定。(如圖 18-13)

名稱 ▲	連線介面	遠端網段	IPSec 演算法	變更
VPN_A	WAN1	211.22.22.22	3DES / MD5	修改 刪除

1 / 1 移至

新增

圖 18-13 完成 IPSec 自動加密設定

步驟9. 在【遠端】>【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：(如圖 18-14)

- 選擇指定的連線【裝置名稱】。
- 輸入所指定的【Trunk 名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入甲端點的子網路 192.168.10.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入乙端點的子網路 192.168.85.0/255.255.255.0。
- 將【可選取的通道】VPN_A 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。(如圖 18-15)

新增 Trunk

裝置名稱: UTM172.19.20.11

Trunk 名稱: IPSec_VPN_Trunk (最多 16 個字元)

本地端設定:

本地端網段所屬介面: ☒ LAN ☐ DMZ

本地端 IP 位址 / 子網路遮罩: 192.168.10.0 / 255.255.255.0

遠端設定:

☒ 遠端 IP 位址 / 子網路遮罩: 192.168.85.0 / 255.255.255.0

☐ 遠端單一電腦

VPN 通道

=====可選取的通道=====

新增 >>

<< 刪除

=====被選取的通道=====

VPN_A

測試連線IP:

☒ 顯示遠端網路芳鄰

☐ 啟動 Trunk 負載平衡

確定 取消

圖 18-14 設定 Trunk

名稱 ▲	本地端子網路	遠端子網路	VPN 通道	變更
IPSec_VPN_Trunk	192.168.10.0 / 24	192.168.85.0 / 24	VPN_A	修改 刪除

1 / 1 移至

新增

圖 18-15 完成 Trunk 設定

步驟10. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 18-16）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 18-17）

新增管制條例

分配：
☒ 裝置：UTM172.19.20.11
☐ 群組：GROUP_1

來源網路位址：Inside Any
 目的網路位址：Outside Any
 服務名稱：Any
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：IPSec_VPN_Trunk

動作：
☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

網站管制：----- None -----
 應用程式管制：----- None -----

[+ 進階設定](#)

確定 取消

圖 18-16 設定 VPN Trunk 內部至外部之管制條例

裝置名稱：全部

來源網路	目的網路	服務名稱	動作	項目	變更
Inside Any	Outside Any	Any	VPN		修改 刪除 暫停

新增

圖 18-17 完成管制條例設定

步驟11. 在【遠端】>【管制條例】>【外部至內部】功能中，做下列設定：（如圖 18-18）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 18-19）

新增管制條例

分配：
☒ 裝置：UTM172.19.20.11
☐ 群組：GROUP_1

來源網路位址：Outside Any
 目的網路位址：Inside Any
 服務名稱：Any
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：IPSec_VPN_Trunk

動作：
☒ 允許 外部至內部 連線
☐ 禁止 外部至內部 連線

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

[+ 進階設定](#)

[確定] [取消]

圖 18-18 設定 VPN Trunk 外部至內部之管制條例

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Outside Any	Inside Any	Any	允許		修改 刪除 暫停

1 / 1 移至

[新增]

圖 18-19 完成管制條例設定



說明：

1. 若【遠端設定】選擇遠端閘道 / 用戶端 採用動態 IP 位址，則【使用模式】需採用 Aggressive mode 並填入指定的【本地 ID】、【遠端 ID】，讓遠端（【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱）能以相映的設定，主動來建立正確的連線。

步驟12. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 18-20, 圖 18-21, 圖 18-22, 圖 18-23)

<div> <div>1 / 1</div> <div>移至</div> </div>						
i	名稱 ▲	連線介面	遠端閘道	IPSec 演算法	連線歷時	變更
	CMS_VPN_A	WAN1	211.22.22.22	3DES / MD5	---	<div>修改</div>
<div> <div>1 / 1</div> <div>移至</div> </div> <div>新增</div>						

圖 18-20 遠端 UTM、MHG IPSec 自動加密設定

<div> <div>1 / 1</div> <div>移至</div> </div>					
i	名稱 ▲	本地端子網路	遠端子網路	VPN通道	變更
	CMS_IPSec_VPN_...	192.168.10.0 / 24	192.168.85.0 / 24	CMS_VPN_A	<div>修改</div>
<div> <div>1 / 1</div> <div>移至</div> </div> <div>新增</div>					

圖 18-21 遠端 UTM、MHG Trunk 設定

1 / 1

移至

來源網路	目的網路	服務名稱	動作	項目										變更			排序
Inside Any	Outside Any	Any	VPN											修改	刪除	暫停	1

1 / 1

移至

新增

圖 18-22 遠端 UTM、MHG 內部至外部管制條例設定

圖 18-23 遠端 UTM、MHG 外部至內部管制條例設定

乙端點的設定步驟如下：

步驟1. 在【遠端】>【管制條例選項】>【VPN】>【IPSec 自動加密】頁面中，按下【新增】鈕。（如圖 18-24）

名稱▲	連線介面	遠端閘道	IPSec 演算法	變更
沒有記錄！				
新增				

圖 18-24IPSec 自動加密頁面

步驟2. 選擇指定的連線【裝置名稱】、【名稱】輸入 VPN_B、【連線介面】選擇 WAN1。（如圖 18-25）

基本設定	
裝置名稱：	UTM/172.19.200.11
名稱：	VPN_B (最多 16 個字元)
連線介面：	WAN1

圖 18-25 設定連線裝置、IPSec 名稱和外部網路介面

步驟3. 【遠端設定】選擇遠端閘道 固定 IP 位址 / 網域名稱，並輸入所要連線的甲端點閘道位址。（如圖 18-26）

遠端設定	
<input checked="" type="radio"/> 遠端閘道 固定IP位址 / 網域名稱：	61.11.11.11 (最多 80 個字元)
<input type="radio"/> 遠端閘道 / 用戶端 採用動態 IP位址	

圖 18-26 設定 IPSec 到目的位址

步驟4. 【認證方法】選擇 Pre-Shared Key，並輸入連線時的【預先共用金鑰】。（如圖 18-27）

認證方法：	Pre-Shared Key
預先共用金鑰：	123456789 (最多 62 個字元)

圖 18-27 設定 IPSec 認證方法

步驟5. 在【加密或認證】>【ISAKMP 演算法】欄位中，設定開始進行連線溝通時所需的演算法，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5、【群組】選擇 Diffie-Hellman 1。（如圖 18-28）

加密或認證 說明	
ISAKMP 演算法	
加密演算法：	3DES
認證演算法：	MD5
群組：	Diffie-Hellman 1

圖 18-28 設定 ISAKMP 演算法

步驟6. 在【加密或認證】>【IPSec 演算法】欄位中，設定資料傳輸時所使用的加密、認證方式，【加密演算法】選擇 3DES、【認證演算法】選擇 MD5。
(如圖 18-29)

圖 18-29 設定 IPSec 演算法

步驟7. 【進階加密】選擇 DH 1、【ISAKMP 更新週期】輸入 3600 秒、【加密金鑰更新週期】輸入 28800 秒、【使用模式】選擇 Main mode。(如圖 18-30)

圖 18-30 設定 IPSec 進階加密、ISAKMP/加密金鑰更新週期和使用模式

步驟8. 完成 IPSec 自動加密設定。(如圖 18-31)

名稱	連線介面	遠端閘道	IPSec 演算法	變更
VPN_B	WAN1	61.11.11.11	3DES / MD5	修改 刪除

圖 18-31 完成 IPSec 自動加密設定

步驟9. 在【遠端】>【管制條例選項】>【VPN】>【Trunk】頁面中，做下列設定：（如圖 18-32）

- 選擇指定的連線【裝置名稱】。
- 輸入所指定的【Trunk 名稱】。
- 【本地端網段所屬介面】選擇 LAN，並輸入乙端點的子網路 192.168.85.0/255.255.255.0。
- 【遠端設定】選擇遠端 IP 位址/子網路遮罩，並輸入甲端點的子網路 192.168.10.0/255.255.255.0。
- 將【可選取的通道】VPN_B 新增至【被選取的通道】清單中。
- 勾選【顯示遠端網路芳鄰】。
- 按下【確定】鈕，完成設定。（如圖 18-33）

圖 18-32 設定 Trunk

名稱	本地端子網路	遠端子網路	VPN通道	變更
IPSec_VPN_Trunk	192.168.85.0 / 24	192.168.10.0 / 24	VPN_B	修改 刪除

新增

圖 18-33 完成 Trunk 設定

步驟10. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 18-34）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 18-35）

新增管制條例

分配：
☒ 裝置：UTM172.19.200.11
☐ 群組：GROUP_1

來源網路位址：Inside Any
 目的網路位址：Outside Any
 服務名稱：Any
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：IPSec_VPN_Trunk

動作：
☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

網站管制：----- None -----
 應用程式管制：----- None -----

[+ 進階設定](#)

確定 取消

圖 18-34 設定 VPN Trunk 內部至外部之管制條例

裝置名稱：全部

來源網路	目的網路	服務名稱	動作	項目	變更
Inside Any	Outside Any	Any	VPN		修改 刪除 暫停

1 / 1 移至

新增

圖 18-35 完成管制條例設定

步驟11. 在【遠端】>【管制條例】>【外部至內部】功能中，做下列設定：（如圖 18-36）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【VPN】選擇所設定的 Trunk 規則。
- 按下【確定】鈕，完成設定。（如圖 18-37）

新增管制條例

分配：
☒ 裝置：UTM172.19.200.11
☐ 群組：GROUP_1

來源網路位址：Outside Any
 目的網路位址：Inside Any
 服務名稱：Any
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：IPSec_VPN_Trunk

動作：
☒ 允許 外部至內部 連線
☐ 禁止 外部至內部 連線

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

[+ 進階設定](#)

確定 取消

圖 18-36 設定 VPN Trunk 外部至內部之管制條例

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Outside Any	Inside Any	Any	VPN		修改 刪除 暫停

新增

圖 18-37 完成管制條例設定

步驟12. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 18-38, 圖 18-39, 圖 18-40, 圖 18-41)

<div> <div></div> <div></div> <div>1 / 1</div> <div>移至</div> <div></div> </div>						
i	名稱 ▲	連線介面	遠端閘道	IPSec 演算法	連線歷時	變更
	CMS_VPN_B	WAN1	61.11.11.11	3DES / MD5	---	<div>修改</div>
<div> <div></div> <div></div> <div>1 / 1</div> <div>移至</div> <div></div> </div>						
<div>新增</div>						

圖 18-38 遠端 UTM、MHG IPSec 自動加密設定

1 / 1

移至

i	名稱 ▲	本地端子網路	遠端子網路	VPN通道	變更
	CMS_IPSec_VPN_...	192.168.85.0 / 24	192.168.10.0 / 24	CMS_VPN_B	<div>修改</div>

1 / 1

移至

新增

圖 18-39 遠端 UTM、MHG Trunk 設定

<div><div></div><div></div><div>1 / 1</div><div>移至</div><div></div></div>																	
來源網路	目的網路	服務名稱	動作	項目										變更			排序
Inside Any	Outside Any	Any											修改	刪除	暫停	1 ▾	
<div><div></div><div></div><div>1 / 1</div><div>移至</div><div></div></div>																	
<div>新增</div>																	

圖 18-40 遠端 UTM、MHG 內部至外部管制條例設定

<div><div></div><div></div><div>1 / 1</div><div>移至</div><div></div></div>														
來源網路	目的網路	服務名稱	動作	項目							變更			排序
<u>Outside Any</u>	<u>Inside Any</u>	Any									修改	刪除	暫停	1 ▾
<div><div></div><div></div><div>1 / 1</div><div>移至</div><div></div></div>														
<div>新增</div>														

圖 18-41 遠端 UTM、MHG 外部至內部管制條例設定

郵件安全

第19章 郵件安全

用來過濾透過遠端 UTM 傳送之電子郵件，使用者不會收到堆積如山的垃圾信，免除從一堆無用的信件中，挑出所需要接受的訊息，或在刪除這些信件時，誤刪所需要的郵件。讓員工的工作效率提升，也不會錯失任何業務上往來溝通的訊息。

【全體化規則】功能概述：

規則名稱 說明如下：

- 用來自訂郵件評判規則之名稱。

註解 說明如下：

- 用來說明自訂規則的意義。

分類 說明如下：

- 當設定為 Spam 時，會將符合判定規則之郵件歸類為垃圾信。
- 當設定為 Ham(Non-Spam)時，會將符合判定規則之郵件歸類為非垃圾信。

處置方式 說明如下：

- 當設定 Spam 分類時，才會啟動此功能，因為只有垃圾郵件才需要被處置。
- 可將垃圾郵件儲存到隔離區、直接刪除、傳送給原收件者、轉送到指定郵件帳號或與垃圾郵件設定相同。

組合方式 說明如下：

- **And**：必須符合所有自訂規則項目之郵件，才會被判定為垃圾信或非垃圾信。
- **Or**：只要符合一條以上自訂規則項目的郵件，就會被判定為垃圾信或非垃圾信。

項目 說明如下：

- 將郵件之 Header、Body、Attach File Name、Size、mailcommand-From 和 mailcommand-To 的特徵依照所訂之條件式，來判別是否為垃圾信。
- 偵測郵件之 Header 項目可分為：Received、Envelope-To、From、To、Cc、Bcc、Subject、Sender、Reply-To、Errors-To、Message-ID、Date 和 Header。

條件 說明如下：

- 當設定 Header、Body、Attach File Name、mailcommand-From 和 mailcommand-To 項目時，其可用的條件式為：Contains、Does Not Contain、Is Equal To、Is Not Equal To、Starts With、Ends With、Exists 和 Does Not Exists。
- 當設定 Size 項目時，其可用的條件式為：More Than、Is Equal To、Is Not Equal To 和 Less Than。

郵件特徵 說明如下：

- 依所選擇的項目和條件填入相關之判斷值，例如：From 項目使用 Contains 條件，並輸入 josh 為特徵，則當寄件者之郵件帳號有 josh 字串時即會被判定為垃圾信或非垃圾信。

【郵件白名單】功能概述：

郵件帳號 說明如下：

- 用來判別有特定郵件地址之信件為非垃圾信。

郵件方向 說明如下：

- From：可用來判別信件中之寄件地址。
- To：可用來判別信件中之收件地址。

【郵件黑名單】功能概述：

郵件帳號 說明如下：

- 用來判別有特定郵件地址之信件為垃圾信。

19.1 郵件安全功能使用範例

19.1.1 於遠端UTM使用白名單與黑名單來過濾信件

環境設定

申請兩條有固接 IP 的 ADSL 線路，供遠端 UTM 使用。

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接（可用的 IP 範圍：61.11.11.10 ~ 61.11.11.14），連上網際網路。

Port3 設為 WAN2（211.22.22.22）和 ATU-R 對接（可用的 IP 範圍：211.22.22.18 ~ 211.22.22.30），連上網際網路。

Port4 設為 DMZ1（透通路由模式）連接郵件伺服器（採用 WAN1 線路 ISP 配發的可用真實 IP 位址 61.11.11.12）。

步驟1. 於遠端 UTM 非軍事區架設一郵件伺服器，其網卡 IP 設定為 61.11.11.12、DNS 設定指向於外部 DNS 伺服器、主機名稱為 nusec.com.tw。

步驟2. 在【遠端】>【管制條例選項】>【位址表】>【非軍事區網路】頁面中，做下列設定：（如圖 19-1）

名稱	網際協定	網路介面	IP 位址	MAC位址	變更
DMZ Any	---	全部	---	---	使用中
Mail_Server	IPv4	全部	61.11.11.12 / 255.255.255.255	00:0C:76:B7:96:3B	修改 刪除

圖 19-1 非軍事區網路位址表設定

步驟3. 在【遠端】>【管制條例選項】>【服務表】>【服務群組】頁面中，做下列設定：（如圖 19-2）

名稱	成員	變更
Mail_Service_01	POP3, SMTP	修改 刪除
Mail_Service_02	DNS, POP3, SMTP	修改 刪除

圖 19-2 服務群組設定

步驟4. 在【遠端】>【管制條例】>【外部至非軍事區】頁面中，做下列設定：
（如圖 19-3）

- 【分配】選擇指定的遠端 UTM。
- 【目的網路位址】選擇所設定的非軍事區網路位址表規則。
- 【服務名稱】選擇所設定的服務群組規則（Mail_Service_01）。
- 勾選 SMTP【垃圾郵件過濾】。
- 按下【確定】鈕，完成設定。（如圖 19-4）

新增管制條例

分配：
☒ 裝置：UTM172.19.20.11
☐ 群組：GROUP_1

來源網路位址：Outside Any
 目的網路位址：Mail_Server
 服務名稱：Mail_Service_01
 自動排程：None
 認證名稱：None
 VPN：None

動作：
☒ 允許 外部至非軍事區 連線
☐ 禁止 外部至非軍事區 連線

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

進階設定
 入侵偵測防禦：☐ 開啓
 網頁應用程式防火牆：☐ 開啓

病毒偵測：
☐ POP3 ☐ SMTP
 垃圾郵件過濾：
☐ POP3 ☒ SMTP
 郵件 歸檔 /稽核：
☐ POP3 (僅歸檔) ☐ SMTP

頻寬管理：
 每個來源IP最大頻寬限制：
 下載頻寬 0 Kbps / 上傳頻寬 0 Kbps (0: 表示不限制)
 每個來源IP最大連線數限制：
 0 (範圍: 1 - 99999, 0: 表示不限制)
 最大連線數限制：
 0 (範圍: 1 - 99999, 0: 表示不限制)
 每個連線的傳輸量限制：
 0 KBytes (範圍: 1 - 999999, 0: 表示不限制)
 每個來源IP的傳輸量限制：
 0 MBytes (範圍: 1 - 999999, 0: 表示不限制)
 每天的傳輸量限制：
 0 MBytes (範圍: 1 - 999999, 0: 表示不限制)

傳送模式：
 LAN1: 自動
 WAN1: 自動
 WAN2: 自動
 DMZ1: 自動

確定 取消

圖 19-3 管制條例套用非軍事區網路位址表、服務群組規則、啓用 SMTP 垃圾郵件過濾機制

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Outside Any	Mail_Server	Mail_Servic...	✓		修改 刪除 暫停

新增

圖 19-4 完成管制條例設定

步驟5. 在【遠端】>【管制條例】>【非軍事區至外部】頁面中，做下列設定：
（如圖 19-5）

- 【分配】選擇指定的遠端 UTM。
- 【來源網路位址】選擇所設定的非軍事區網路位址表規則。
- 【服務名稱】選擇所設定的服務群組規則（Mail_Service_02）。
- 【動作】選擇 WAN1。
- 勾選 SMTP【垃圾郵件過濾】。
- 按下【確定】鈕，完成設定。（如圖 19-6）

圖 19-5 管制條例套用非軍事區網路位址表、服務群組規則、啓用 SMTP 垃圾郵件過濾機制

裝置名稱: 全部												1 / 1 移至	
來源網路	目的網路	服務名稱	動作	項目								變更	
Mail_Server	Outside Any	Mail_Servic...	1								修改	刪除	暫停
1 / 1 移至													
新增													

圖 19-6 完成管制條例設定

步驟6. 在【遠端】>【郵件安全】>【郵件白名單】頁面中，做下列設定：

- 按下【新增】鈕。
- 【郵件帳號】輸入 share2k01@yahoo.com.tw。
- 【郵件方向】選擇 From。
- 按下【確定】鈕。(如圖 19-7)
- 再次按下【新增】鈕。
- 【郵件帳號】輸入 share2k01@yahoo.com.tw。
- 【郵件方向】選擇 To。
- 按下【確定】鈕。(如圖 19-8)
- 再次按下【新增】鈕。
- 【郵件帳號】輸入 josh@nusec.com.tw。
- 【郵件方向】選擇 From。
- 按下【確定】鈕。(如圖 19-9)
- 再次按下【新增】鈕。
- 【郵件帳號】輸入 josh@nusec.com.tw。
- 【郵件方向】選擇 To。
- 按下【確定】鈕，完成設定。(如圖 19-10, 圖 19-11)



圖 19-7 設定第一條郵件白名單規則



圖 19-8 設定第二條郵件白名單規則



圖 19-9 設定第三條郵件白名單規則

新增郵件白名單

郵件帳號： 說明 (*@domain.com, *: 萬用字元)

郵件方向：

確定 取消

圖 19-10 設定第四條郵件白名單規則

匯出郵件白名單至用戶端 匯出

從用戶端匯入郵件白名單 瀏覽... 匯入 (最大檔案大小: 1 MBytes)

1 / 1 移至

郵件方向 ▲	郵件帳號 ▲	變更
From	share2k01@yahoo.com.tw	修改 刪除
To	share2k01@yahoo.com.tw	修改 刪除
From	josh@nusec.com.tw	修改 刪除
To	josh@nusec.com.tw	修改 刪除

1 / 1 移至

新增

圖 19-11 完成郵件白名單設定



說明：

1. 系統管理員可【匯出】來整理和保存相關設定資料，以利未來 CMS-2000【郵件白名單】錯亂時，可清除清單內容重新【匯入】。

步驟7. 在【郵件安全】>【郵件過濾】>【郵件黑名單】頁面中，做下列設定：

- 按下【新增】鈕。
- 【郵件帳號】輸入 *yahoo*。
- 【郵件方向】選擇 From。
- 按下【確定】鈕。(如圖 19-12)
- 再次按下【新增】鈕。
- 【郵件帳號】輸入 *yahoo*。
- 【郵件方向】選擇 To。
- 按下【確定】鈕，完成設定。(如圖 19-13, 圖 19-14)

圖 19-12 設定第一條郵件黑名單規則

圖 19-13 設定第二條郵件黑名單規則

郵件方向	郵件帳號	變更
From	*yahoo*	修改 刪除
To	*yahoo*	修改 刪除

圖 19-14 完成郵件黑名單設定



說明：

1. 系統管理員可【匯出】來整理和保存相關設定資料，以利未來 CMS-2000【郵件黑名單】錯亂時，可清除清單內容重新【匯入】。
2. 【郵件帳號】可設定為完整之郵件地址（例如：josh@nusec.com.tw）或由含有【*】組成之字串（例如：*yahoo*，則代表有” yahoo” 字串之電子郵件帳號）。
3. 【郵件白名單】的權限高於【郵件黑名單】，所以遠端 UTM 在過濾垃圾郵件時，會先處理符合【郵件白名單】規則的信件，然後再將其餘信件與【郵件黑名單】規則比對。

步驟8. 在指定的遠端 UTM 中，會產生相映規則設定。(如圖 19-15, 圖 19-16, 圖 19-17, 圖 19-18, 圖 19-19, 圖 19-20)

匯出非軍事區網路位址表至用戶端:

從用戶端匯入非軍事區網路位址表: (最大檔案大小: 1 MBytes)

[輔助選取](#) ◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

名稱 ▲	網際協定	網路介面	IP 位址	MAC位址	變更
DMZ Any	---	全部	---		<input type="button" value="使用中"/>
CMS_Mail_Server	IPv4	全部	61.11.11.12 / 255.255.255.255		<input type="button" value="修改"/>

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 19-15 遠端 UTM 非軍事區網路位址表設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

名稱 ▲	成員	變更
CMS_Mail_Service_01	POP3, SMTP	<input type="button" value="修改"/>
CMS_Mail_Service_02	DNS, POP3, SMTP	<input type="button" value="修改"/>

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 19-16 遠端 UTM 服務群組設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

來源網路	目的網路	服務名稱	動作	項目	變更	排序
Outside Any	CMS_Mail_Server	CMS_Mail ...	✓		<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	1 ▼

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 19-17 遠端 UTM 外部至非軍事區管制條例設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

來源網路	目的網路	服務名稱	動作	項目	變更	排序
CMS_Mail_Server	Outside Any	CMS_Mail ...	1		<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	1 ▼

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 19-18 遠端 UTM 非軍事區至外部管制條例設定

匯出郵件白名單至用戶端

從用戶端匯入郵件白名單 (最大檔案大小: 1 MBytes)

◀◀ 1 / 1 移至 ▶▶

郵件方向 ▲	郵件帳號 ▲	變更
From	share2k01@yahoo.com.tw	<input type="button" value="修改"/> <input type="button" value="刪除"/>
To	share2k01@yahoo.com.tw	<input type="button" value="修改"/> <input type="button" value="刪除"/>
From	josh@nusec.com.tw	<input type="button" value="修改"/> <input type="button" value="刪除"/>
To	josh@nusec.com.tw	<input type="button" value="修改"/> <input type="button" value="刪除"/>

◀◀ 1 / 1 移至 ▶▶

圖 19-19 遠端 UTM 郵件白名單設定

匯出郵件黑名單至用戶端

從用戶端匯入郵件黑名單 (最大檔案大小: 1 MBytes)

◀◀ 1 / 1 移至 ▶▶

郵件方向 ▲	郵件帳號 ▲	變更
From	*yahoo*	<input type="button" value="修改"/> <input type="button" value="刪除"/>
To	*yahoo*	<input type="button" value="修改"/> <input type="button" value="刪除"/>

◀◀ 1 / 1 移至 ▶▶

圖 19-20 遠端 UTM 郵件黑名單設定

步驟9. 當來自於 yahoo 的郵件帳號，寄信給 nusec.com.tw 郵件主機上之 josh@nusec.com.tw 和 steve@nusec.com.tw 收件者帳號：

- 若寄件者帳號為 share2k01@yahoo.com.tw 時，則此二收件者帳號皆會收到由此寄件者帳號寄來之信件。
- 若是來自其他的 yahoo 寄件者帳號（share2k003@yahoo.com.tw）時，則只有 josh@nusec.com.tw 會收到由此寄件者帳號寄來之信件，寄給 steve@nusec.com.tw 的信件則會被判定為垃圾郵件並儲存在隔離區。

步驟10. 當來自於 nusec.com.tw 的郵件帳號，寄信給 yahoo 郵件主機上之 share2k01@yahoo.com.tw 和 share2k003@yahoo.com.tw 收件者帳號：

- 若寄件者帳號為 josh@nusec.com.tw 時，則此二收件者帳號皆會收到由此寄件者帳號寄來之信件。
- 若是來自其他的 nusec.com.tw 寄件者帳號（steve@nusec.com.tw）時，則只有 share2k01@yahoo.com.tw 會收到由此寄件者帳號寄來之信件，寄給 share2k003@yahoo.com.tw 的信件則會被判定為垃圾郵件並儲存在隔離區。

郵件 歸檔 / 稽核

第20章 郵件 歸檔 / 稽核

可將透過遠端 UTM 傳輸的郵件，依其特性做審核和存查的動作，有效控管郵件的進出。

【稽核】功能概述：

規則名稱 說明如下：

- 用來自訂郵件審核規則之名稱。

註解 說明如下：

- 用來說明自訂規則的意義。

組合方式 說明如下：

- **And**：必須符合所有自訂規則項目之郵件，才會被判定是否要稽核。
- **Or**：只要符合任一自訂規則項目的郵件，就會被判定是否要稽核。

處置方式 說明如下：

- 可將郵件直接刪除、留待指定管理者審查、於指定時間送出、傳送給原收件者或複製到特定信箱。

郵件歸檔 說明如下：

- 可將符合判定規則之郵件做存查的動作。

項目 說明如下：

- 將郵件之 From、To、Subject、Body、Attach File Name、Size、mailcommand-From 和 mailcommand-To 的特徵依照所訂之條件式做審核。

條件 說明如下：

- 當設定 From、To、Subject、Body、Attach File Name、mailcommand-From 和 mailcommand-To 項目時，其可用的條件式為：Contains、Does Not Contain、Is Equal To、Is Not Equal To、Starts With、Ends With、Exists 和 Does Not Exists。
- 當設定 Size 項目時，其可用的條件式為：More Than、Is Equal To、Is Not Equal To 和 Less Than。

郵件特徵 說明如下：

- 依所選擇的項目和條件填入相關之判斷值，例如：From 項目使用 Contains 條件，並輸入 josh 為特徵，則當寄件者之郵件帳號有 josh 字串時即符合審核的標準。

20.1 稽核

20.1.1 於遠端UTM審核往來的信件

環境設定

申請兩條有固接 IP 的 ADSL 線路，供遠端 UTM 使用。

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1（61.11.11.11）和 ATU-R 對接（可用的 IP 範圍：61.11.11.10 ~ 61.11.11.14），連上網際網路。

Port3 設為 WAN2（211.22.22.22）和 ATU-R 對接（可用的 IP 範圍：211.22.22.18 ~ 211.22.22.30），連上網際網路。

Port4 設為 DMZ1（透通路由模式）連接郵件伺服器（採用 WAN1 線路 ISP 配發的可用真實 IP 位址 61.11.11.12）。

步驟1. 於遠端 UTM 非軍事區架設一郵件伺服器，其網卡 IP 設定為 61.11.11.12、DNS 設定指向於外部 DNS 伺服器、主機名稱為 nusec.com.tw。

步驟2. 在【遠端】>【管制條例選項】>【位址表】>【非軍事區網路】頁面中，做下列設定：（如圖 20-1）

匯出非軍事區網路位址表至用戶端:

從用戶端匯入非軍事區網路位址表: (最大檔案大小: 1 MBytes)

名稱	網際協定	網路介面	IP 位址	MAC位址	變更
DMZ Any	---	全部	---	---	<input type="button" value="使用中"/>
Mail_Server	IPv4	全部	61.11.11.12 / 255.255.255.255	00:0C:76:B7:96:3B	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 20-1 非軍事區網路位址表設定

步驟3. 在【遠端】>【管制條例選項】>【服務表】>【服務群組】頁面中，做下列設定：（如圖 20-2）

名稱	成員	變更
Mail_Service_01	POP3, SMTP	<input type="button" value="修改"/> <input type="button" value="刪除"/>
Mail_Service_02	DNS, POP3, SMTP	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 20-2 服務群組設定

步驟4. 在【遠端】>【管制條例】>【外部至非軍事區】頁面中，做下列設定：
（如圖 20-3）

- 【分配】選擇指定的遠端 UTM。
- 【目的網路位址】選擇所設定的非軍事區網路位址表規則。
- 【服務名稱】選擇所設定的服務群組規則（Mail_Service_01）。
- 勾選 SMTP【郵件歸檔 / 稽核】。
- 按下【確定】鈕，完成設定。（如圖 20-4）

圖 20-3 管制條例套用非軍事區網路位址表、服務群組規則、啓用 SMTP 郵件歸檔/稽核機制

裝置名稱: 全部

1 / 1

移至

來源網路	目的網路	服務名稱	動作	項目							變更
Outside Any	Mail_Server	Mail_Servic...	✔							<div>修改</div> <div>刪除</div> <div>暫停</div>	

1 / 1

移至

新增

圖 20-4 完成管制條例設定

步驟5. 在【遠端】>【管制條例】>【非軍事區至外部】頁面中，做下列設定：
（如圖 20-5）

- 【分配】選擇指定的遠端 UTM。
- 【來源網路位址】選擇所設定的非軍事區網路位址表規則。
- 【服務名稱】選擇所設定的服務群組規則（Mail_Service_02）。
- 【動作】選擇 WAN1。
- 勾選 SMTP【郵件歸檔 / 稽核】。
- 按下【確定】鈕，完成設定。（如圖 20-6）

圖 20-5 管制條例套用非軍事區網路位址表、服務群組規則、啓用 SMTP 郵件歸檔/稽核機制

來源網路	目的網路	服務名稱	動作	項目
Mail_Server	Outside Any	Mail_Servic...	↑	

圖 20-6 完成管制條例設定

步驟6. 在【遠端】>【郵件 歸檔 / 稽核】>【稽核】頁面中，做下列設定：

- 按下【新增】鈕。
- 【規則名稱】輸入 Mail_Delivery。
- 【註解】輸入 Deliver Mail To User。
- 【組合方式】選擇 Or。
- 【處置方式】選擇傳送。
- 啟用【郵件歸檔】功能。
- 於第一條【項目】選擇 From，【條件】選擇 Contains，【郵件特徵】輸入 share2k01。
- 按【下一列】鈕。
- 於第二條【項目】選擇 To，【條件】選擇 Contains，【郵件特徵】輸入 share2k01。
- 按【下一列】鈕。
- 於第三條【項目】選擇 From，【條件】選擇 Contains，【郵件特徵】輸入 josh。
- 按【下一列】鈕。
- 於第四條【項目】選擇 To，【條件】選擇 Contains，【郵件特徵】輸入 josh。（如圖 20-7）
- 按下【確定】鈕，完成設定。（如圖 20-8）

規則名稱: (最多 16 個字元) 註解: (最多 20 個字元)

組合方式: 處置方式:

☒ 郵件歸檔 (當無勾選此選項時，符合此條件的信件將不歸檔)

項目	條件	郵件特徵 (最多 30 個字元)	變更
<input type="text" value="From"/>	<input type="text" value="Contains"/>	<input type="text" value="share2k01"/>	<input type="button" value="刪除"/>
<input type="text" value="To"/>	<input type="text" value="Contains"/>	<input type="text" value="share2k01"/>	<input type="button" value="刪除"/>
<input type="text" value="From"/>	<input type="text" value="Contains"/>	<input type="text" value="josh"/>	<input type="button" value="刪除"/>
<input type="text" value="To"/>	<input type="text" value="Contains"/>	<input type="text" value="josh"/>	<input type="button" value="下一列"/> <input type="button" value="刪除"/>

圖 20-7 設定第一條稽核規則

1 / 1 移至

規則名稱	處置方式	註解	郵件歸檔	變更	排序
Mail_Delivery		Deliver Mail To User		<input type="button" value="修改"/> <input type="button" value="刪除"/>	<input type="text" value="1"/>

1 / 1 移至

圖 20-8 完成第一條稽核規則設定

步驟7. 於【遠端】>【郵件 歸檔 / 稽核】>【稽核】頁面中，做下列設定：

- 按下【新增】鈕。
- 【規則名稱】輸入 Mail_Deletion。
- 【註解】輸入 Delete Mail。
- 【組合方式】選擇 Or。
- 【處置方式】選擇刪除。
- 啓用【郵件歸檔】功能。
- 於第一條【項目】選擇 From，【條件】選擇 Contains，【郵件特徵】輸入 yahoo。
- 按【下一列】鈕。
- 於第二條【項目】選擇 To，【條件】選擇 Contains，【郵件特徵】輸入 yahoo。（如圖 20-9）
- 按下【確定】鈕，完成設定。（如圖 20-10）

規則名稱: Mail_Deletion (最多 16 個字元) 註解: Delete Mail (最多 20 個字元)

組合方式: Or 處置方式: 刪除

☒ 郵件歸檔 (當無勾選此選項時，符合此條件的信件將不歸檔)

項目	條件	郵件特徵 (最多 30 個字元)	變更
From	Contains	yahoo	刪除
To	Contains	yahoo	下一列 刪除

確定 取消

圖 20-9 設定第二條稽核規則

說明

規則名稱	處置方式	註解	郵件歸檔	變更	排序
Mail_Delivery		Deliver Mail To User		修改 刪除	1
Mail_Deletion		Delete Mail		修改 刪除	2

新增

圖 20-10 完成第二條稽核規則設定

說明：

- 於【稽核】規則設定中，【處置方式】僅能選擇【刪除】、【審查】、【延遲】、【傳送】或【複製】其中一種。
- 經遠端 UTM【郵件安全】>【郵件過濾】和【病毒偵測】後，允許傳送的郵件，在【稽核】功能中，會依其設定條例之順位來做審核。

3. 在【Outlook Express】信件匣中任選一郵件，按下滑鼠右鍵選擇【內容】，並於彈出視窗的【詳細資料】頁面中，會顯示該封信所有表頭項目，可用來當作【稽核】之【條件】和【項目】設定時之參考值。（如圖 20-11）



圖 20-11 郵件之詳細資料

步驟8. 在指定的遠端 UTM 中，會產生相映規則設定。(如圖 20-12, 圖 20-13, 圖 20-14, 圖 20-15, 圖 20-16, 圖 20-17)

匯出非軍事區網路位址表至用戶端:

從用戶端匯入非軍事區網路位址表: (最大檔案大小: 1 MBytes)

[輔助選取](#) ◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

名稱 ▲	網際協定	網路介面	IP 位址	MAC位址	變更
DMZ Any	---	全部	---		<input type="button" value="使用中"/>
CMS_Mail_Server	IPv4	全部	61.11.11.12 / 255.255.255.255		<input type="button" value="修改"/>

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 20-12 遠端 UTM 非軍事區網路位址表設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

名稱 ▲	成員	變更
CMS_Mail_Service_01	POP3, SMTP	<input type="button" value="修改"/>
CMS_Mail_Service_02	DNS, POP3, SMTP	<input type="button" value="修改"/>

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 20-13 遠端 UTM 服務群組設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

來源網路	目的網路	服務名稱	動作	項目	變更	排序
Outside Any	CMS_Mail_Server	CMS_Mail ...	✓		<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	1 ▼

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 20-14 遠端 UTM 外部至非軍事區管制條例設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

來源網路	目的網路	服務名稱	動作	項目	變更	排序
CMS_Mail_Server	Outside Any	CMS_Mail ...	1		<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	1 ▼

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 20-15 遠端 UTM 非軍事區至外部管制條例設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

規則名稱	處置方式	註解	郵件歸檔	變更	排序
Mail_Delivery		Deliver Mail To User	✓	<input type="button" value="修改"/> <input type="button" value="刪除"/>	1 ▼

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 20-16 遠端 UTM 第一條稽核規則設定

說明

1 / 1

移至

規則名稱	處置方式	註解	郵件歸檔	變更		排序
Mail_Delivery		Deliver Mail To User		修改	刪除	1
Mail_Deletion		Delete Mail		修改	刪除	2

1 / 1

移至

新增

圖 20-17 遠端 UTM 第二條稽核規則設定

步驟9. 當來自於 yahoo 的郵件帳號，寄信給 nusec.com.tw 郵件主機上之 josh@nusec.com.tw 和 steve@nusec.com.tw 收件者帳號：

- 若寄件者帳號為 share2k01@yahoo.com.tw 時，則此二收件者帳號皆會收到由此寄件者帳號寄來之信件。
- 若是來自其他的 yahoo 寄件者帳號（share2k003@yahoo.com.tw）時，則只有 josh@nusec.com.tw 會收到由此寄件者帳號寄來之信件，寄給 steve@nusec.com.tw 的信件則會被刪除。

步驟10. 當來自於 nusec.com.tw 的郵件帳號，寄信給 yahoo 郵件主機上之 share2k01@yahoo.com.tw 和 share2k003@yahoo.com.tw 收件者帳號：

- 若寄件者帳號為 josh@nusec.com.tw 時，則此二收件者帳號皆會收到由此寄件者帳號寄來之信件。
- 若是來自其他的 nusec.com.tw 寄件者帳號（steve@nusec.com.tw）時，則只有 share2k01@yahoo.com.tw 會收到由此寄件者帳號寄來之信件，寄給 share2k003@yahoo.com.tw 的信件則會被刪除。

網站管制

第21章 網站管制

用來控管遠端 UTM、MHG 內部使用者瀏覽網頁時存取的網站、檔案、MIME/Script，避免摸魚降低工作效率、在不知情的狀況下遭植入惡意程式（病毒）。

- **【網站白名單】**：系統管理員可透過完整網域名稱、關鍵字或萬用字元（*），設定開放存取的特定網址。
- **【網站黑名單】**：系統管理員可透過完整網域名稱、關鍵字或萬用字元（*），設定阻擋存取的特定網址。
- **【網站類別資料庫】**：系統管理員可針對網站分類，設定阻擋存取的規則。（須付費使用）
- **【檔案傳輸管制】**：管制直接透過 http 或 ftp 協定從網路下載、上傳特定副檔名之檔案。
- **【MIME/Script 管制】**：管制網頁 Pop-up Window、ActiveX Control、Java Applet、Browser Cookie 的存取權限，和網頁傳送的資料型態。
- **【網站管制群組】**：系統管理員可組合所設定的**【網站白名單】**、**【網站黑名單】**、**【網站類別資料庫】**、**【檔案傳輸管制】**或**【MIME/Script 管制】**項目，制定網站管制規則。

【網站白名單】功能概述：

名稱 說明如下：

- 網站白名單規則的辨識名稱。

URL 說明如下：

- 設定允許存取的特定網址關鍵字。
- 若將其設為*，則代表允許存取任何網址。

排除檔案傳輸管制 說明如下：

- 可透過允許連結的網址存取所限制的檔案。

【網站黑名單】功能概述：

名稱 說明如下：

- 網站黑名單規則的辨識名稱。

URL 說明如下：

- 設定阻擋存取的特定網址關鍵字。
- 若將其設為*，則代表阻擋存取任何網址。

【網站類別資料庫】功能概述：

名稱 說明如下：

- 網站類別規則的辨識名稱。

網站類別 說明如下：

- 可分為非法、情色、賭博與遊戲、社會與經濟、互動與服務、休閒嗜好、教育新知、其他等類別，於各大類別中包含了所屬的網站類型。
- 可組合特定的網站類型來設置管制規則。



說明：

1. 遠端 UTM、MHG 管制網站存取的規則比對順序：**【網站白名單】→【網站黑名單】→【網站類別資料庫】**。
-

【檔案傳輸管制】功能概述：

名稱 說明如下：

- 檔案傳輸管制規則的辨識名稱。

預設之副檔名 說明如下：

- 可阻擋使用者透過 HTTP 或 FTP 協定傳輸遠端 UTM、MHG 預設副檔名之檔案。

自訂之副檔名 說明如下：

- 可阻擋使用者透過 HTTP 或 FTP 協定傳輸自訂副檔名之檔案。

禁止傳遞所有檔案 說明如下：

- 可阻擋使用者透過 HTTP 或 FTP 協定傳輸任一預設和自訂副檔名之檔案。

禁止分段傳檔 說明如下：

- 可限制使用者將檔案分割，透過 HTTP 或 FTP 協定同時以多條連線傳輸。

【MIME/Script 管制】功能概述：

名稱 說明如下：

- MIME/Script 管制規則的辨識名稱。

阻擋的 Script 說明如下：

- Pop-up Window：可阻擋瀏覽網頁時自動彈跳出視窗。
- ActiveX Control：可阻擋執行網頁內嵌的 ActiveX 控制項。
- Java Applet：可阻擋執行網頁內嵌的 Java 程序。
- Browser Cookie：可阻擋網站儲存特定資訊於使用者電腦。

Mime 類型 說明如下：

- MIME（Multipurpose Internet Mail Extensions，多用途網際網路郵件擴展）是一個網際網路標準，它擴展了電子郵件標準，使其能夠支援二進位格式附件、非 ASCII 字元等多種格式的訊息。在 HTTP 協定中也使用了 MIME 的框架。
- MIME 規定了用於表示各樣資料類型的符號化方法。

- MIME 的內容類型 (Content-Type) 表頭 (Header) 是用於指定訊息類型，通常呈現的方式為 Type/Subtype。

- ◆ Type 的種類有：

- Text：用於標準化表示文字訊息，可以是多種字元集或格式的文字訊息。
- Multipart：用於整合多個文件為一個訊息，這些文件可以是不同類型的資料。
- Application：用於傳輸應用程式或二進位資料。
- Message：用於封裝一個電子郵件訊息。
- Image：用於傳輸靜態圖片資料。
- Audio：用於傳輸音訊或聲音資料。
- Video：用於傳輸動態影像資料，可以是與音訊編輯在一起的視訊資料。

- ◆ Subtype 用於指定 Type 的細部種類，常見的有：

- text/plain (純文字文件)。
- text/html (HTML 文件)。
- application/xhtml+xml (XHTML 檔案)。
- image/gif (GIF 圖像)。
- image/jpeg (JPEG 圖像)。
- image/png (PNG 圖像)。
- video/mpeg (MPEG 影像)。
- application/octet-stream (任意的二進位資料)。
- application/pdf (PDF 檔案)。
- application/msword (Microsoft Word 文件)。



注意：

1. 【網站白名單】、【網站黑名單】、【網站類別資料庫】、【檔案傳輸管制】和【MIME/Script 管制】規則皆要群組後，方能為【管制條例】所引用。
-

21.1 網站管制功能使用範例

21.1.1 使用網站白名單與黑名單來限制遠端UTM、MHG內部使用者

存取特定網址

步驟1. 在【遠端】>【網站管制】>【網站白名單】頁面中，做下列設定：

- 按下【新增】鈕。
- 輸入指定【名稱】。
- 【URL】輸入第一條允許連線的網址關鍵字。（例如：yahoo）
- 按下【確定】鈕。（如圖 21-1）
- 再次按下【新增】鈕。
- 輸入指定【名稱】。
- 【URL】輸入第二條允許連線的網址關鍵字。（例如：google）
- 按下【確定】鈕，完成設定。（如圖 21-2, 圖 21-3）

圖 21-1 設定第一條網站白名單規則

圖 21-2 設定第二條網站白名單規則

匯出網站白名單至用戶端：

從用戶端匯入網站白名單： (最大檔案大小: 1 MBytes)

名稱 ▲	URL ▲	檔案存取	變更
url_1	yahoo	✗	<input type="button" value="修改"/> <input type="button" value="刪除"/>
url_2	google	✗	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 21-3 完成網站白名單設定



說明：

1. 系統管理員可【匯出網站白名單至用戶端】來整理和保存相關設定資料，以利未來 CMS-2000【網站白名單】錯亂時，可清除清單內容重新【從用戶端匯入網站白名單】。

步驟2. 在【遠端】>【網站管制】>【網站黑名單】頁面中，做下列設定：（如圖 21-4）

- 輸入指定【名稱】。
- 【URL】輸入*（代表任一字元），用來阻擋連線任何網址。
- 按下【確定】鈕，完成設定。（如圖 21-5）

圖 21-4 設定網站黑名單

名稱 ▲	URL ▲	變更
url_3	*	修改 刪除

圖 21-5 完成網站黑名單設定

說明：

1. 系統管理員可【匯出網站黑名單至用戶端】來整理和保存相關設定資料，以利未來 CMS-2000【網站黑名單】錯亂時，可清除清單內容重新【從用戶端匯入網站黑名單】。

步驟3. 在【遠端】>【網站管制】>【網站管制群組】頁面中，做下列設定：（如圖 21-6）

- 輸入指定群組【名稱】。
- 將【可選取的網站白名單】新增至【已選取的網站白名單】。
- 將【可選取的網站黑名單】新增至【已選取的網站黑名單】。
- 按下【確定】鈕，完成設定。（如圖 21-7）

新增群組

名稱: URL_Blocking_Group (最多 21 個字元)

網站類別: None

檔案傳輸管制 (上傳): None

檔案傳輸管制 (下載): None

MIME / Script 管制: None

網站白名單

全選 反向選擇

=====[可選取的網站白名單]=====

=====[已選取的網站白名單]=====

url_1

url_2

新增 >>

<< 刪除

網站黑名單

全選 反向選擇

=====[可選取的網站黑名單]=====

=====[已選取的網站黑名單]=====

url_3

新增 >>

<< 刪除

確定 取消

圖 21-6 設定網站管制群組

名稱 ▲	管制項目	變更
URL_Blocking_Group	白名單: url_1, url_2 黑名單: url_3 網站類別: --- 檔案傳輸管制 (上傳): --- 檔案傳輸管制 (下載): --- MIME / Script 管制: ---	<div>修改</div> <div>刪除</div>

新增

圖 21-7 完成網站管制群組設定

步驟4. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 21-8）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【網站管制】選擇所設定的網站管制群組規則。
- 按下【確定】鈕，完成設定。（如圖 21-9）
- 使用者僅能經由此管制條例連結含有 yahoo 和 google 關鍵字的網址。

新增管制條例

分配：

☒ 裝置：UTM172.19.20.11
☐ 群組：GROUP_1

來源網路位址：

Inside Any

目的網路位址：

Outside Any

服務名稱：

Any

自動排程：

----- None -----

認證名稱：

----- None -----

VPN：

----- None -----

動作：

☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面
 僅允許下列網路介面：
☐ (LAN1) ☐ (WAN1) ☐ (WAN2) ☐ (DMZ1)

報告機制：

☐ 封包記錄
☐ 流量圖表

網站管制：

URL_Blocking_Group

應用程式管制：

----- None -----

[+ 進階設定](#)

確定 取消

圖 21-8 管制條例套用網站管制規則

裝置名稱: 全部	1 / 1 移至									
來源網路	目的網路	服務名稱	動作	項目						變更
Inside Any	Outside Any	Any	✓							修改 刪除 暫停
1 / 1 移至										
新增										

圖 21-9 完成管制條例設定

步驟5. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 21-10, 圖 21-11, 圖 21-12, 圖 21-13)

匯出網站白名單至用戶端:

從用戶端匯入網站白名單: (最大檔案大小: 1 MBytes)

名稱	URL	檔案存取	變更
CMS_url_1	yahoo	✗	<input type="button" value="修改"/>
CMS_url_2	google	✗	<input type="button" value="修改"/>

圖 21-10 遠端 UTM、MHG 網站白名單設定

匯出網站黑名單至用戶端:

從用戶端匯入網站黑名單: (最大檔案大小: 1 MBytes)

名稱	URL	變更
CMS_url_3	*	<input type="button" value="修改"/>

圖 21-11 遠端 UTM、MHG 網站黑名單設定

名稱	管制項目	變更
CMS_URL_Blocking_Gr	白名單: CMS_url_1, CMS_url_2 黑名單: CMS_url_3 網站類別: --- 檔案傳輸管制 (上傳): --- 檔案傳輸管制 (下載): --- MIME / Script 管制: ---	<input type="button" value="修改"/>

圖 21-12 遠端 UTM、MHG 網站管制群組設定

來源網路	目的網路	服務名稱	動作	項目	變更	排序
Inside Any	Outside Any	Any	✓	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	1

圖 21-13 遠端 UTM、MHG 管制條例設定

入侵偵測防禦

第22章 入侵偵測防禦

遠端 UTM 可即時偵測異常流量、掃描異常封包內容，並加以阻絕、隔離、干擾或發出警訊通知管理者，以預防可疑程式碼入侵目標主機。所以當遠端 UTM 偵測到來自內部或外部的攻擊行為時，可即時提供保護網路與阻絕攻擊行為的措施，使企業網路依然可運行暢通，並提高資訊傳輸的安全性。

針對各種不同的攻擊行為，提供相對應的比對規則，包含三個部份：異常偵測、預設特徵和自訂特徵。

- **【異常偵測】**：會隨著定義檔的更新，來針對目前所能發現的異常封包與流量做偵測和防禦。
- **【預設特徵】**：亦會隨著定義檔的更新，來針對目前所能發現的入侵模式做偵測和防禦。
- **【自訂特徵】**：讓使用者可依自己的需求，來偵測和防禦**【預設特徵】**、**【異常偵測】**以外的攻擊行為及異常封包、流量。

【異常偵測】功能概述：

異常偵測設定 說明如下：

- 可分為 SYN flood、UDP flood、ICMP flood、port scanning 和 http inspect 等異常偵測機制。(如圖 22-1)
- 可針對特定封包所產生之異常流量或行為，做通行、丟棄、中斷連線、記錄或警示的控管動作。

異常偵測設定

☐ 開啓 SYN flood 偵測

流量臨界值: 300 封包數 / 秒 (範圍: 1 - 1000超過此值時系統將會予以阻擋) [說明](#)

阻擋時間: 60 秒 (範圍: 1 - 3600)

處理動作: 通行

事件通知: ☐ 記錄 ☐ 警示

☐ 開啓 UDP flood 偵測

流量臨界值: 300 封包數 / 秒 (範圍: 1 - 1000超過此值時系統將會予以阻擋) [說明](#)

阻擋時間: 60 秒 (範圍: 1 - 3600)

處理動作: 通行

事件通知: ☐ 記錄 ☐ 警示

☐ 開啓 ICMP flood 偵測

流量臨界值: 300 封包數 / 秒 (範圍: 1 - 1000超過此值時系統將會予以阻擋) [說明](#)

阻擋時間: 60 秒 (範圍: 1 - 3600)

處理動作: 通行

事件通知: ☐ 記錄 ☐ 警示

☐ 開啓 port scanning 偵測

阻擋時間: 60 秒

處理動作: 通行

事件通知: ☐ 記錄 ☐ 警示

☐ 開啓 HTTP 偵測

處理動作: 通行

事件通知: ☐ 記錄 ☐ 警示

確定 取消

圖 22-1 異常偵測設定頁面

【預設特徵】功能概述：

入侵偵測防禦特徵 說明如下：

- 可分為 Attack Responses、Backdoor、Bad Traffic、Chat、DDoS、DNS、DoS、Exploit、Finger、FTP、ICMP、IMAP、Info、Media、Misc、MySQL、NetBIOS、NNTP、Oracle、Policy、POP2、POP3、RPC、Rservices、Scan、Shellcode、SMTP、SNMP、Spyware、SQL、Telnet、TFTP、Web Attacks、Web CGI、Web Client、Web Coldfusion、Web IIS、Web Misc、Web PHP、X11 和 Other 等類別，於各大類別中包含了所屬的攻擊特徵。(如圖 22-2)
- 可針對符合攻擊特徵的封包，做通行、丟棄、中斷連線、記錄或警示的控管動作。

入侵偵測防禦特徵總數：2818

特徵啟用數量：0

H：高風險 **M**：中風險 **L**：低風險

<input type="checkbox"/>	特徵名稱	風險等級	處理動作	記錄	警示	變更
<input type="checkbox"/>	Attack Responses (17)					
<input type="checkbox"/>	Backdoor (74)					
<input type="checkbox"/>	Bad Traffic (12)					
<input type="checkbox"/>	Chat (30)					
<input type="checkbox"/>	DDos (33)					
<input type="checkbox"/>	DNS (19)					
<input type="checkbox"/>	Dos (19)					
<input type="checkbox"/>	Exploit (76)					
<input type="checkbox"/>	Finger (13)					
<input type="checkbox"/>	FTP (70)					
<input type="checkbox"/>	ICMP (115)					
<input type="checkbox"/>	IMAP (39)					
<input type="checkbox"/>	Info (10)					
<input type="checkbox"/>	Media (10)					
<input type="checkbox"/>	Misc (59)					
<input type="checkbox"/>	MySQL (2)					
<input type="checkbox"/>	NetBIOS (202)					
<input type="checkbox"/>	NNTP (13)					
<input type="checkbox"/>	Oracle (298)					
<input type="checkbox"/>	Policy (21)					
<input type="checkbox"/>	POP2 (4)					
<input type="checkbox"/>	POP3 (27)					
<input type="checkbox"/>	RPC (128)					
<input type="checkbox"/>	Rservices (13)					
<input type="checkbox"/>	Scan (20)					
<input type="checkbox"/>	Shellcode (21)					
<input type="checkbox"/>	SMTP (59)					
<input type="checkbox"/>	SNMP (17)					
<input type="checkbox"/>	Spyware (307)					
<input type="checkbox"/>	SQL (44)					
<input type="checkbox"/>	Telnet (13)					
<input type="checkbox"/>	TFTP (11)					
<input type="checkbox"/>	Web Attacks (46)					
<input type="checkbox"/>	Web CGI (349)					
<input type="checkbox"/>	Web Client (19)					
<input type="checkbox"/>	Web Coldfusion (35)					
<input type="checkbox"/>	Web IIS (115)					
<input type="checkbox"/>	Web Misc (327)					
<input type="checkbox"/>	Web PHP (126)					
<input type="checkbox"/>	X11 (2)					
<input type="checkbox"/>	Other (3)					

確定

取消

圖 22-2 預設特徵設定頁面

【自訂特徵】功能概述：

名稱 說明如下：

- 系統管理員可在此為自訂的特徵命名。

網際協定 說明如下：

- 設定欲偵測和防禦的網際協定（IPv4、IPv6）。

通訊協定 說明如下：

- 設定欲偵測和防禦的通訊協定（TCP、UDP、ICMP、IP）。

來源 IP 位址 / 子網路遮罩 說明如下：

- 設定攻擊端電腦使用的 IP 位址。

來源埠號 說明如下：

- 設定攻擊端電腦使用的埠號（範圍 1~65535）。

目的 IP 位址 / 子網路遮罩 說明如下：

- 設定被攻擊端電腦的 IP 位址。

目的埠號 說明如下：

- 設定被攻擊端電腦的埠號（範圍 1~65535）。

風險等級 說明如下：

- 設定符合自訂特徵之封包的威脅性。

處理動作 說明如下：

- 設定符合自訂特徵之封包的處理動作。

事件通知 說明如下：

- 比對到符合自訂特徵之封包時，可進行記錄和警示動作。

進階選項 說明如下：

- 可針對所有通過遠端 UTM 傳送的 Inbound 和 Outbound 封包來做過濾。
- 設定是否要依照封包內容特徵的大小寫來做過濾。

內容 說明如下：

- 設定欲偵測的封包內容特徵。

22.1 入侵偵測防禦功能使用範例

22.1.1 於遠端UTM偵測異常封包和流量，並搭配自訂特徵和預設特

徵來偵測和防禦攻擊行為

步驟1. 在【遠端】>【入侵偵測防禦】>【異常偵測】頁面中，做下列設定：（如圖 22-3）

- 啟用並設定各偵測機制。
- 按下【確定】鈕，完成設定。

異常偵測設定

☒ 開啓 SYN flood 偵測

流量臨界值: 300 封包數 / 秒 (範圍: 1 - 1000超過此值時系統將會予以阻擋) [說明](#)

阻擋時間: 60 秒 (範圍: 1 - 3600)

處理動作: 通行

事件通知: ☒ 記錄 ☒ 警示

☒ 開啓 UDP flood 偵測

流量臨界值: 300 封包數 / 秒 (範圍: 1 - 1000超過此值時系統將會予以阻擋) [說明](#)

阻擋時間: 60 秒 (範圍: 1 - 3600)

處理動作: 通行

事件通知: ☒ 記錄 ☒ 警示

☒ 開啓 ICMP flood 偵測

流量臨界值: 300 封包數 / 秒 (範圍: 1 - 1000超過此值時系統將會予以阻擋) [說明](#)

阻擋時間: 60 秒 (範圍: 1 - 3600)

處理動作: 通行

事件通知: ☒ 記錄 ☒ 警示

☒ 開啓 port scanning 偵測

阻擋時間: 60 秒

處理動作: 通行

事件通知: ☒ 記錄 ☒ 警示

☒ 開啓 HTTP 偵測

處理動作: 通行

事件通知: ☒ 記錄 ☒ 警示

確定 取消

圖 22-3 異常偵測設定

步驟2. 在【遠端】>【入侵偵測防禦】>【預設特徵】頁面中，做下列設定：（如圖 22-4）

- 選擇要使用的特徵。
- 按下【確定】鈕，完成設定。

入侵偵測防禦特徵總數：2818
特徵啟用數量：2818

H：高風險
 M：中風險
 L：低風險

<input type="checkbox"/>	特徵名稱	風險等級	處理動作	記錄	警示	變更
<input checked="" type="checkbox"/>	Attack Responses (17)					
<input checked="" type="checkbox"/>	Backdoor (74)					
<input checked="" type="checkbox"/>	Bad Traffic (12)					
<input checked="" type="checkbox"/>	Chat (30)					
<input checked="" type="checkbox"/>	DDos (33)					
<input checked="" type="checkbox"/>	DNS (19)					
<input checked="" type="checkbox"/>	Dos (19)					
<input checked="" type="checkbox"/>	Exploit (76)					
<input checked="" type="checkbox"/>	Finger (13)					
<input checked="" type="checkbox"/>	FTP (70)					
<input checked="" type="checkbox"/>	ICMP (115)					
<input checked="" type="checkbox"/>	IMAP (39)					
<input checked="" type="checkbox"/>	Info (10)					
<input checked="" type="checkbox"/>	Media (10)					
<input checked="" type="checkbox"/>	Misc (59)					
<input checked="" type="checkbox"/>	MySQL (2)					
<input checked="" type="checkbox"/>	NetBIOS (202)					
<input checked="" type="checkbox"/>	NNTP (13)					
<input checked="" type="checkbox"/>	Oracle (298)					
<input checked="" type="checkbox"/>	Policy (21)					
<input checked="" type="checkbox"/>	POP2 (4)					
<input checked="" type="checkbox"/>	POP3 (27)					
<input checked="" type="checkbox"/>	RPC (128)					
<input checked="" type="checkbox"/>	Rservices (13)					
<input checked="" type="checkbox"/>	Scan (20)					
<input checked="" type="checkbox"/>	Shellcode (21)					
<input checked="" type="checkbox"/>	SMTP (59)					
<input checked="" type="checkbox"/>	SNMP (17)					
<input checked="" type="checkbox"/>	Spyware (307)					
<input checked="" type="checkbox"/>	SQL (44)					
<input checked="" type="checkbox"/>	Telnet (13)					
<input checked="" type="checkbox"/>	TFTP (11)					
<input checked="" type="checkbox"/>	Web Attacks (46)					
<input checked="" type="checkbox"/>	Web CGI (349)					
<input checked="" type="checkbox"/>	Web Client (19)					
<input checked="" type="checkbox"/>	Web Coldfusion (35)					
<input checked="" type="checkbox"/>	Web IIS (115)					
<input checked="" type="checkbox"/>	Web Misc (327)					
<input checked="" type="checkbox"/>	Web PHP (126)					
<input checked="" type="checkbox"/>	X11 (2)					
<input checked="" type="checkbox"/>	Other (3)					

圖 22-4 預設特徵設定

步驟3. 在【遠端】>【入侵偵測防禦】>【自訂特徵】頁面中，做下列設定：（如圖 22-5）

- 輸入指定的特徵【名稱】。
- 選擇指定的【網際協定】、【通訊協定】。
- 輸入指定的【來源埠號】、【目的埠號】。
- 選擇指定的【風險等級】、【處理動作】。
- 【事件通知】勾選記錄和警示。
- 【進階選項】勾選無方向性和不區分大小寫。
- 輸入欲偵測的封包【內容】特徵。
- 按下【確定】鈕，完成設定。（如圖 22-6）

圖 22-5 設定自訂特徵

名稱	風險等級	處理動作	記錄	警示	變更
Software_Crack	H	丟棄	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	修改 刪除

新增

圖 22-6 完成自訂特徵設定



說明：

1. 【內容】可直接填入要偵測的字串，或將其轉換為十六進位的 ASCII 碼（例如：cracks 可轉換為 \x63\x72\x61\x63\x6b\x73）。

步驟4. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：（如圖 22-7）

- 【分配】選擇指定的遠端 UTM。
- 開啓【入侵偵測防禦】。
- 按下【確定】鈕，完成設定。（如圖 22-8）

新增管制條例

分配：
☒ 裝置：UTM1 72.19.20.11
☐ 群組：GROUP_1

來源網路位址：Inside Any
目的網路位址：Outside Any
服務名稱：Any
自動排程：----- None -----
認證名稱：----- None -----
VPN：----- None -----

動作：
☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面
僅允許下列網路介面：
☐ (LAN1) ☐ (WAN1) ☐ (WAN2) ☐ (DMZ1)

報告機制：
封包記錄：☐ 開啓
流量圖表：☐ 開啓

網站管制：----- None -----
應用程式管制：----- None -----

☒ 進階設定
入侵偵測防禦：☒ 開啓

病毒偵測：☐ POP3 ☐ SMTP ☐ HTTP / Webmail ☐ FTP
垃圾郵件過濾：☐ POP3 ☐ SMTP
郵件 歸檔 / 稽核：☐ POP3 (僅歸檔) ☐ SMTP

IM 側錄：☐ 開啓

頻寬管理：----- None -----
每個來源IP最大頻寬限制：下載頻寬 0 Kbps / 上傳頻寬 0 Kbps (0: 表示不限制)
P2P 軟體最大頻寬限制：下載頻寬 0 Kbps / 上傳頻寬 0 Kbps (0: 表示不限制)
每個來源IP最大連線數限制：0 (範圍：1 - 99999, 0: 表示不限制)
最大連線數限制：0 (範圍：1 - 99999, 0: 表示不限制)
每個連線的傳輸量限制：0 KBytes (範圍：1 - 999999, 0: 表示不限制)
每個來源IP的傳輸量限制：0 MBytes (範圍：1 - 999999, 0: 表示不限制)
每天的傳輸量限制：0 MBytes (範圍：1 - 999999, 0: 表示不限制)

傳送模式：
LAN1：自動
WAN1：自動
WAN2：自動
DMZ1：自動

說明

確定 取消

圖 22-7 管制條例啓用入侵偵測防禦機制

裝置名稱：全部

來源網路	目的網路	服務名稱	動作	項目	變更
Inside Any	Outside Any	Any	✓		修改 刪除 暫停

新增

圖 22-8 完成管制條例設定

步驟5. 在指定的遠端 UTM 中，會產生相映規則設定。(如圖 22-9, 圖 22-10, 圖 22-11, 圖 22-12)

異常偵測設定

☒ 開啓 SYN flood 偵測

流量臨界值:

300

封包數 / 秒 (範圍: 1 - 1000超過此值時系統將會予以阻擋)

說明

阻擋時間:

60

秒 (範圍: 1 - 3600)

處理動作:

通行

事件通知:

☒ 記錄

☒ 警告

☒ 開啓 UDP flood 偵測

流量臨界值:

300

封包數 / 秒 (範圍: 1 - 1000超過此值時系統將會予以阻擋)

說明

阻擋時間:

60

秒 (範圍: 1 - 3600)

處理動作:

通行

事件通知:

☒ 記錄

☒ 警告

☒ 開啓 ICMP flood 偵測

流量臨界值:

300

封包數 / 秒 (範圍: 1 - 1000超過此值時系統將會予以阻擋)

說明

阻擋時間:

60

秒 (範圍: 1 - 3600)

處理動作:

通行

事件通知:

☒ 記錄

☒ 警告

☒ 開啓 port scanning 偵測

阻擋時間:

60

秒

處理動作:

通行

事件通知:

☒ 記錄

☒ 警告

☒ 開啓 HTTP 偵測

處理動作:

通行

事件通知:

☒ 記錄

☒ 警告

確定

取消

圖 22-9 遠端 UTM 異常偵測設定

入侵偵測防禦特徵總數：2819

特徵啟用數量：2819

H：高風險 **M**：中風險 **L**：低風險

<input type="checkbox"/>	特徵名稱	風險等級	處理動作	記錄	警告	變更
<input checked="" type="checkbox"/>	Attack Responses (17)					
<input checked="" type="checkbox"/>	Backdoor (74)					
<input checked="" type="checkbox"/>	Bad Traffic (13)					
<input checked="" type="checkbox"/>	Chat (30)					
<input checked="" type="checkbox"/>	DDos (33)					
<input checked="" type="checkbox"/>	DNS (19)					
<input checked="" type="checkbox"/>	Dos (19)					
<input checked="" type="checkbox"/>	Exploit (76)					
<input checked="" type="checkbox"/>	Finger (13)					
<input checked="" type="checkbox"/>	FTP (70)					
<input checked="" type="checkbox"/>	ICMP (115)					
<input checked="" type="checkbox"/>	IMAP (39)					
<input checked="" type="checkbox"/>	Info (10)					
<input checked="" type="checkbox"/>	Media (10)					
<input checked="" type="checkbox"/>	Misc (59)					
<input checked="" type="checkbox"/>	MySQL (2)					
<input checked="" type="checkbox"/>	NetBIOS (202)					
<input checked="" type="checkbox"/>	NNTP (13)					
<input checked="" type="checkbox"/>	Oracle (298)					
<input checked="" type="checkbox"/>	Policy (21)					
<input checked="" type="checkbox"/>	POP2 (4)					
<input checked="" type="checkbox"/>	POP3 (27)					
<input checked="" type="checkbox"/>	RPC (128)					
<input checked="" type="checkbox"/>	Rservices (13)					
<input checked="" type="checkbox"/>	Scan (20)					
<input checked="" type="checkbox"/>	Shellcode (21)					
<input checked="" type="checkbox"/>	SMTP (59)					
<input checked="" type="checkbox"/>	SNMP (17)					
<input checked="" type="checkbox"/>	Spyware (307)					
<input checked="" type="checkbox"/>	SQL (44)					
<input checked="" type="checkbox"/>	Telnet (13)					
<input checked="" type="checkbox"/>	TFTP (11)					
<input checked="" type="checkbox"/>	Web Attacks (46)					
<input checked="" type="checkbox"/>	Web CGI (349)					
<input checked="" type="checkbox"/>	Web Client (19)					
<input checked="" type="checkbox"/>	Web Coldfusion (35)					
<input checked="" type="checkbox"/>	Web IIS (115)					
<input checked="" type="checkbox"/>	Web Misc (327)					
<input checked="" type="checkbox"/>	Web PHP (126)					
<input checked="" type="checkbox"/>	X11 (2)					
<input checked="" type="checkbox"/>	Other (3)					

確定

取消

圖 22-10 遠端 UTM 預設特徵設定

名稱▲	風險等級	處理動作	記錄	警示	變更
CMS_Software_Crack	H	丟棄▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	修改 刪除

新增

圖 22-11 遠端 UTM 自訂特徵設定

																	1 / 1 移至	
來源網路	目的網路	服務名稱	動作	項目										變更			排序	
Inside Any	Outside Any	Any	✓												修改	刪除	暫停	1
																	1 / 1 移至	
新增																		

圖 22-12 遠端 UTM 管制條例設定

網頁應用程式防火牆

第23章 網頁應用程式防火牆

遠端 UTM 可即時偵測外部使用者存取對外服務網站的應用程式（ASP、PHP、CGI、JSP、...）之封包內容，以預防針對網頁應用程式漏洞的攻擊行為。當遠端 UTM 偵測到外部使用者嘗試進行對外服務網站的應用程式弱點攻擊時，可即時阻絕攻擊行為以保護網站，讓企業適時針對網站進行安全性補強作業。

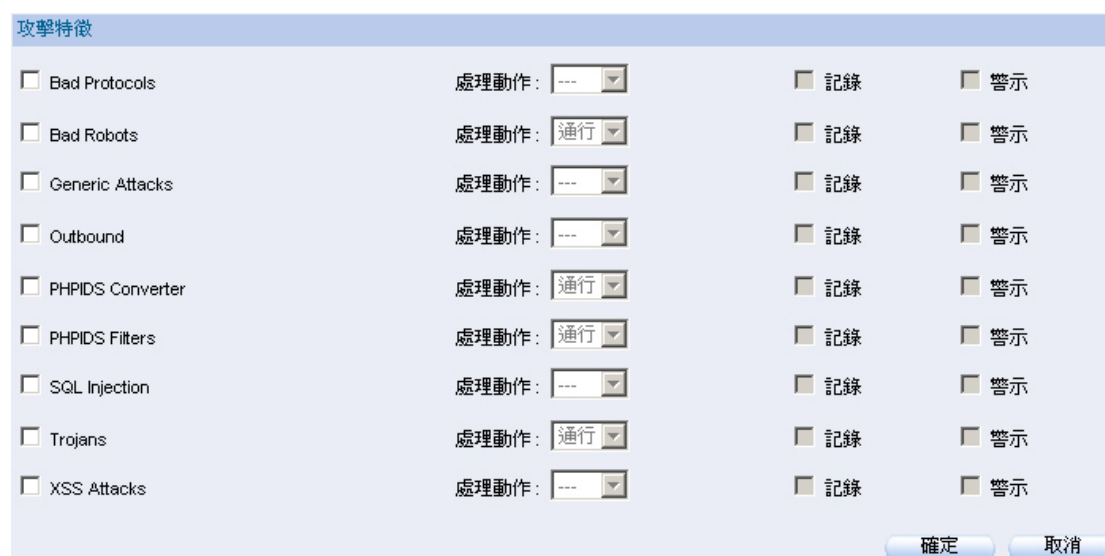
針對各種不同的攻擊行為，提供相對應的比對規則，包含兩個部份：預設特徵和自訂特徵。

- **【預設特徵】**：會隨著定義檔的更新，來針對目前所能發現的攻擊模式做偵測和防禦。
- **【自訂特徵】**：讓使用者可依自己的需求，來偵測和防禦**【預設特徵】**以外的攻擊行為。

【預設特徵】功能概述：

攻擊特徵 說明如下：

- 可分為 Bad Protocols、Bad Robots、Generic Attacks、Outbound、PHPIDS Converter、PHPIDS Filters、SQL Injection、Trojans 和 XSS Attacks 等類別，於各大類別中包含了所屬的攻擊特徵。（如圖 23-1）
- 可針對符合攻擊特徵的封包，做通行、丟棄、記錄或警示的控管動作。



攻擊特徵

<input type="checkbox"/> Bad Protocols	處理動作：---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警示
<input type="checkbox"/> Bad Robots	處理動作：通行	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警示
<input type="checkbox"/> Generic Attacks	處理動作：---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警示
<input type="checkbox"/> Outbound	處理動作：---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警示
<input type="checkbox"/> PHPIDS Converter	處理動作：通行	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警示
<input type="checkbox"/> PHPIDS Filters	處理動作：通行	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警示
<input type="checkbox"/> SQL Injection	處理動作：---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警示
<input type="checkbox"/> Trojans	處理動作：通行	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警示
<input type="checkbox"/> XSS Attacks	處理動作：---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警示

確定 取消

圖 23-1 預設特徵設定頁面

【自訂特徵】功能概述：

名稱 說明如下：

- 系統管理員可在此為自訂的特徵命名。

處理動作 說明如下：

- 設定符合自訂特徵之封包的處理動作。

事件通知 說明如下：

- 比對到符合自訂特徵之封包時，可進行記錄和警示動作。

處理階段 說明如下：

- 可選擇在存取網頁的 Request Headers、Request Body、Response Headers 或 Response Body 階段，進行偵測動作。

變數 說明如下：

- 針對指定的 ARGS、ARGS_NAMES、ARGS_GET、ARGS_GET_NAMES、ARGS_POST、ARGS_POST_NAMES、FILES_NAMES、FILES_SIZES、AUTH_TYPE、REMOTE_ADDR、REMOTE_HOST、REMOTE_USER、REQUEST_LINE、REQUEST_HEADERS、REQUEST_HEADERS_NAME、REQUEST_COOKIES、REQUEST_COOKIES_NAME、REQUEST_BODY、RESPONSE_HEADERS、RESPONSE_HEADERS_NAME、RESPONSE_CONTENT_TYPE、RESPONSE_STATUS 或 RESPONSE_BODY 等網頁存取表頭、內容識別代碼進行偵測動作。

運算子 說明如下：

- 設定比對網頁識別代碼傳輸的表頭、內容資料之判別式。
- 可以利用@符號來指定使用的比對方法（預設是採用正規表示法）。
 - ◆ @rx waf：以正規表示法比對傳輸的資料是否包含 waf 字串。
 - ◆ @gt 100：傳輸的資料是否大於 100Byte。
 - ◆ @lt 100：傳輸的資料是否小於 100 Byte。
 - ◆ @eq 100：傳輸的資料是否等於 100 Byte。
 - ◆ @ge 100：傳輸的資料是否大於或等於 100 Byte。
 - ◆ @le 100：傳輸的資料是否小於或等於 100 Byte。



說明：

1. 正規表示法 (Regular Expression)，是指一個用來描述或者匹配一系列符合某個句法規則的字符串，其運用的基礎字符彙整如下：

RE 字符	意義與範例
^	代表字串的起始字元。
	例如：^A
	代表以 A 開頭的字串 Abc, Aaa。
\$	代表字串的結束字元。
	例如：A\$
	代表以 A 結尾的字串 bcA, aaA。
.	代表『任意一個』字元，一定是一個任意字元。
	例如：e.e
	代表字串可以是 eve, eae, eee, e e，但不能僅有 ee；亦即 e 與 e 中間『一定』僅有一個字元，而空白字元也是字元。
\	跳脫字符，將特殊符號的特殊意義去除。
	例如：\.
	代表含有.號的字串 www.nusoft。

*	重複零個或多個的前一字元。
	<p>例如：ess*</p> <p>代表含有 es, ess, esss 等等的字串。注意，因為*可以是 0 個，所以 es 也是符合帶搜尋字串。另外，因為*為重複『前一個字元』的符號；因此，在*之前必須要緊接著一個字元(例如：a*)。</p>
\{n,m\}	<p>連續 n 到 m 個的『前一字元』。</p> <p>若為 \{n\} 則是連續 n 個的前一字元；若是 \{n,\} 則是連續 n 個以上的前一字元。</p>
	<p>例如：go\{2,3\}g</p> <p>代表在 g 與 g 之間有 2 個到 3 個的 o 存在的字串，亦即 goog, gooog。</p>
[]	字元集合的特殊字符的符號。
	<p>例 1：g[ld]</p> <p>代表含有 gl 或 gd 的字串</p> <p>需要特別留意的是，在[]當中『謹代表一個待搜尋的字元』，亦即[af]代表 a 或 f 的意思。</p> <p>例 2：[0-9]</p> <p>代表含有任意數字的字串。需特別留意，在字元集合[]中的減號-是有特殊意義的，他代表兩個字元之間的所有連續字元(例如：所有大寫字元則為[A-Z])。</p> <p>例 3：oo[^t]</p> <p>代表字串可以是 oog, ood 但不能是 oot，^在[]內時，代表的意義是『反向選擇』的意思(例如：我不要大寫字元，則為[^A-Z])。</p>
+	重複『一個或一個以上』的前一字元。
	<p>例如：go+d</p> <p>代表 god, good, good, ...的字串。o+代表『一個以上的 o』。</p>
?	『零個或一個』的前一字元。
	<p>例如：go?d</p> <p>代表 gd, god 這兩個字串。o? 代表『空的或 1 個 o』。</p>
	用或(or)的方式找出數個字串。
	<p>例如：gd good</p> <p>代表 gd 或 good 這兩個字串。</p>
()	找出『群組』字串。
	<p>例 1：g(la oo)d</p> <p>代表 glad 或 good 這兩個字串，因為 g 與 d 是重複的，所以，我就可以將 la 與 oo 列於()當中，並以 來分隔開來。</p>

	<p>例 2：A(xyz)+C</p> <p>代表開頭是 A 結尾是 C，中間有一個以上的 "xyz" 字串的意思。</p>
--	--

變換函數 說明如下：

- 針對透過網頁傳輸的資料可做特定轉換再行比對。
 - ◆ t.toLowerCase：轉換傳輸的資料為小寫字元。
 - ◆ t.urlDecode：轉換傳輸的資料為 URL 編碼值（例如：waf = %77%61%66）。
 - ◆ t.removeWhitespace：刪除傳輸資料中所有的空白字元。

23.1 網頁應用程式防火牆功能使用範例

23.1.1 於遠端UTM以自訂特徵和預設特徵來偵測和防禦攻擊行為

環境設定

申請兩條有固接 IP 的 ADSL 線路，供遠端 UTM 使用。

Port1 設為 LAN1（192.168.1.1，NAT / 路由模式）和內部網路連接，為 192.168.1.x/24 網段。

Port2 設為 WAN1 所連線路的固接 IP 為 61.11.11.10 ~ 61.11.11.14。

Port3 設為 WAN2 所連線路的固接 IP 為 211.22.22.18 ~ 211.22.22.30。

步驟1. 在遠端 UTM 內部網路中架設一提供網頁服務之伺服器，其網卡 IP 設定為 192.168.1.100、DNS 設定指向於外部 DNS 伺服器。

步驟2. 在【遠端】>【管制條例選項】>【虛擬伺服器】>【連接埠對應】頁面中，做下列設定：（如圖 23-2）



名稱 ▲	伺服器真實IP	服務	伺服器虛擬IP	變更
Web_Server	61.11.11.12	HTTP	192.168.1.100	修改 刪除

圖 23-2 連接埠對應設定

步驟3. 在【遠端】>【網頁應用程式防火牆】>【預設特徵】頁面中，做下列設定：（如圖 23-3）

- 選擇並設定要使用的特徵。
- 按下【確定】鈕，完成設定。

攻擊特徵			
<input checked="" type="checkbox"/> Bad Protocols	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> Protocol Violations	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Protocol Anomalies	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Bad Robots	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Generic Attacks	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> OS Command Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Coldfusion Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> LDAP Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> SSI Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Email Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> HTTP Request Smuggling	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> HTTP Response Splitting	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Remote File Inclusion	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Prequalify Request Matches	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Session Fixation	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> File Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Command Access	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Command Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> PHP	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Outbound	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> Response Detection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> IFrame Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Malware Domain	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> ASP/JSP Leakage	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> PHP Leakage	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Statistics Display	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> SQL Leakage	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> IIS Leakage	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Directory Listing	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> PHPIDS Converter	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> PHPIDS Filters	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> SQL Injection	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> SQL Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> SQL Injection Weak	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Trojans	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> XSS Attacks	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> XSS Attacks	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> IE XSS Filters	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告

圖 23-3 預設特徵設定

步驟4. 在【遠端】>【網頁應用程式防火牆】>【自訂特徵】頁面中，做下列設定：（如圖 23-4）

- 輸入指定的特徵【名稱】。
- 選擇指定的【處理動作】。
- 【事件通知】勾選記錄和警示。
- 選擇指定的【處理階段】。
- 輸入指定的【變數】。
- 【運算子】輸入[a-z]{1}[1-2]{1}[0-9]{8}（以正規表示法比對包含 a155968142, s255689148, e255893146, ...的資料）。
- 【變換函數】輸入 t:lowercase（轉換傳輸的資料為小寫字元）
- 按下【確定】鈕，完成設定。（如圖 23-5）

圖 23-4 設定自訂特徵

名稱▲	處理動作	記錄	警示	變更
Security_ID_Number	丟棄	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	修改 刪除

圖 23-5 完成自訂特徵設定

步驟5. 在【遠端】>【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 23-6）

- 【分配】選擇指定的遠端 UTM。
- 選擇對外開放網頁服務的【目的網路位址】和【服務名稱】。
- 開啓【網頁應用程式防火牆】。
- 按下【確定】鈕，完成設定。（如圖 23-7）

新增管制條例	
分配：	<input checked="" type="radio"/> 裝置：UTM/172.19.20.11 <input type="radio"/> 群組：GROUP_1
來源網路位址：	Outside Any
目的網路位址：	[連接埠對應] Web_Server(81.11.11.12)
服務名稱：	HTTP (80)
自動排程：	----- None -----
認證名稱：	----- None -----
VPN：	----- None -----
動作：	<input checked="" type="checkbox"/> 允許 外部至內部 連線 <input type="checkbox"/> 禁止 外部至內部 連線
報告機制：	
封包記錄：	<input type="checkbox"/> 開啓
流量圖表：	<input type="checkbox"/> 開啓
<input checked="" type="checkbox"/> 進階設定	
入侵偵測防禦：	<input type="checkbox"/> 開啓
網頁應用程式防火牆：	<input checked="" type="checkbox"/> 開啓
病毒偵測：	<input type="checkbox"/> POP3 <input type="checkbox"/> SMTP
垃圾郵件過濾：	<input type="checkbox"/> POP3 <input type="checkbox"/> SMTP
郵件 歸檔 /稽核：	<input type="checkbox"/> POP3 (僅歸檔) <input type="checkbox"/> SMTP
頻寬管理：	----- None -----
每個來源IP最大頻寬限制：	下載頻寬 [0] Kbps / 上傳頻寬 [0] Kbps (0: 表示不限制)
每個來源IP最大連線數限制：	[0] (範圍: 1 - 99999, 0: 表示不限制)
最大連線數限制：	[0] (範圍: 1 - 99999, 0: 表示不限制)
每個連線的傳輸量限制：	[0] KBytes (範圍: 1 - 999999, 0: 表示不限制)
每個來源IP的傳輸量限制：	[0] MBytes (範圍: 1 - 999999, 0: 表示不限制)
每天的傳輸量限制：	[0] MBytes (範圍: 1 - 999999, 0: 表示不限制)
傳送模式：	LAN1 : 自動 WAN1 : 自動 WAN2 : 自動 DMZ1 : 自動
<input type="button" value="說明"/>	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 23-6 管制條例啓用網頁應用程式防火牆機制

裝置名稱: 全部 1 / 1 移至

來源網路	目的網路	服務名稱	動作	項目								變更		
Outside Any	[連接埠對應](61.11.11.12)	HTTP	✓									修改	刪除	暫停

1 / 1 移至

新增

圖 23-7 完成管制條例設定



說明：

1. 【網頁應用程式防火牆】係避免外部使用者，針對架設於遠端 UTM 內部（LAN 或 DMZ）對外提供網頁服務的主機，進行網頁應用程式弱點攻擊。

步驟6. 在指定的遠端 UTM 中，會產生相映規則設定。(如圖 23-8, 圖 23-9, 圖 23-10, 圖 23-11)

名稱▲	伺服器真實IP	服務	伺服器虛擬IP	變更
CMS_Web_Server	61.11.11.12 Port2 (WAN1)	HTTP	192.168.1.100 (LAN)	修改

新增

圖 23-8 遠端 UTM 連接埠對應設定

攻擊特徵

<input checked="" type="checkbox"/> Bad Protocols	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> Protocol Violations	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Protocol Anomalies	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Bad Robots	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Generic Attacks	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> OS Command Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Coldfusion Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> LDAP Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> SSI Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Email Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> HTTP Request Smuggling	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> HTTP Response Splitting	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Remote File Inclusion	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Prequalify Request Matches	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Session Fixation	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> File Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Command Access	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Command Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> PHP	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Outbound	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> Response Detection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> IFrame Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Malware Domain	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> ASP/JSP Leakage	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> PHP Leakage	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Statistics Display	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> SQL Leakage	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> IIS Leakage	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Directory Listing	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> PHPIDS Converter	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> PHPIDS Filters	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> SQL Injection	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> SQL Injection	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> SQL Injection Weak	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> Trojans	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> XSS Attacks	處理動作: ---	<input type="checkbox"/> 記錄	<input type="checkbox"/> 警告
<input checked="" type="checkbox"/> XSS Attacks	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告
<input checked="" type="checkbox"/> IE XSS Filters	處理動作: 通行	<input checked="" type="checkbox"/> 記錄	<input checked="" type="checkbox"/> 警告

確定 取消

圖 23-9 遠端 UTM 預設特徵設定

/ 1 移至

名稱 ▲	處理動作	記錄	警示	變更
CMS_Security_ID_Number	丟棄 ▼	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>修改</div> <div>刪除</div>

/ 1 移至

新增

圖 23-10 遠端 UTM 自訂特徵設定

/ 1 移至

來源網路	目的網路	服務名稱	動作	項目	變更	排序
Outside Any	[連接埠對應]61.11.1...	HTTP			<div>修改</div> <div>刪除</div> <div>暫停</div>	1 ▼

/ 1 移至

新增

圖 23-11 遠端 UTM 管制條例設定

SSL Web VPN

第24章 SSL Web VPN

由於網際網路的普遍應用，企業遠端安全登入的需求也與日俱增。對於使用者而言，最方便安全的解決方案莫過於 SSL Web VPN，用戶端只要使用標準的瀏覽器，就可直接透過 SSL 安全加密協定傳輸資料。

【VPN】專有名詞概述：

DES 說明如下：

- 資料加密標準（Data Encryption Standard）是一種 NIST 標準安全加密金鑰方法，使用的加密金鑰為 56 位元。

3DES 說明如下：

- 提供比 DES 更加安全的三重資料加密標準（Triple Data Encryption Standard, 3DES）安全加密金鑰方法，使用的加密金鑰為 168 位元。

AES 說明如下：

- 為高階加密模式其標準比 DES 的加密標準更加嚴謹，DES 加密金鑰長度為 56 位元，AES 加密金鑰長度則高達 128 位元、192 位元、以及 256 位元。

【設定】功能概述：

名稱 說明如下：

- SSL Web VPN 連線認證規則的辨識名稱。

使用之認證帳戶或群組 說明如下：

- SSL Web VPN 連線驗證時比對的【遠端】>【管制條例選項】>【認證表】>【認證帳戶】、【認證群組】規則。

24.1 SSL Web VPN功能使用範例

24.1.1 建立讓外部用戶端和遠端UTM、MHG建立SSL Web VPN連線的規則

步驟1. 在【遠端】>【管制條例選項】>【認證表】>【認證帳戶】和【認證群組】頁面中，做下列設定：（如圖 24-1, 圖 24-2）

匯出認證帳戶表至用戶端:

從用戶端匯入認證帳戶表: (最大檔案大小: 1 MBytes)

帳戶名稱 ▲	到期日	變更
joy		<input type="button" value="修改"/> <input type="button" value="刪除"/>
john		<input type="button" value="修改"/> <input type="button" value="刪除"/>
jack		<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 24-1 認證帳戶設定

名稱 ▲	成員	RADIUS	POP3	LDAP	變更
laboratory	joy, john, jack	✗	✗	✗	<input type="button" value="修改"/> <input type="button" value="刪除"/>

圖 24-2 認證群組設定

步驟2. 在【遠端】>【SSL Web VPN】>【設定】頁面中，做下列設定：（如圖 24-3）

- 輸入所指定的 SSL Web VPN 連線認證規則【名稱】。
- 【使用之認證帳戶或群組】選擇所設定的認證帳戶、群組規則。
- 按下【確定】鈕，完成設定。（如圖 24-4）

新增 SSL Web VPN 認證方式

名稱: (最多 20 個字元)

使用之認證帳戶或群組:

確定 取消

圖 24-3 設定 SSL Web VPN 認證

SSL Web VPN 認證方式設定

名稱 ▲	使用之認證帳戶或群組	變更
Web_VPN_Connection	laboratory	修改 刪除

新增

圖 24-4 完成 SSL Web VPN 認證設定

步驟3. 在【遠端】>【管制條例】>【外部至內部】頁面中，做下列設定：（如圖 24-5）

- 【分配】選擇指定的遠端 UTM、MHG。
- 【VPN】選擇所設定的 SSL Web VPN 規則。
- 按下【確定】鈕，完成設定。（如圖 24-6）

新增管制條例

分配：
☒ 裝置：UTM172.19.20.11
☐ 群組：GROUP_1

來源網路位址：Outside Any
 目的網路位址：Inside Any
 服務名稱：Any
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：[Web VPN] Web_VPN_Connection

動作：
☒ 允許 外部至內部 連線
☐ 禁止 外部至內部 連線

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

[+ 進階設定](#)

確定 取消

圖 24-5 設定 SSL Web VPN 外部至內部之管制條例

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Outside Any	Inside Any	Any	VPN		修改 刪除 暫停

新增

圖 24-6 完成管制條例設定

步驟4. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 24-7, 圖 24-8, 圖 24-9, 圖 24-10)

匯出認證帳戶表至用戶端:

從用戶端匯入認證帳戶表: (最大檔案大小: 1 MBytes)

帳戶名稱 ▲	到期日	變更
joy		<input type="button" value="修改"/>
john		<input type="button" value="修改"/>
jack		<input type="button" value="修改"/>

圖 24-7 遠端 UTM、MHG 認證帳戶設定

名稱 ▲	成員	RADIUS	POP3	LDAP	變更
CMS_laboratory	joy, john, jack	✗	✗	✗	<input type="button" value="修改"/>

圖 24-8 遠端 UTM、MHG 認證群組設定

SSL Web VPN 組態設定

SSL Web VPN: ☒ (加密演算法: AES-128, 連線埠號 TCP: 443 和 TCP: 1194)

配給用戶端的IP位址範圍: 192.168.53.0 / 255.255.255.0

SSL Web VPN 認證方式設定

名稱 ▲	使用之認證帳戶或群組	硬體認證	SSL 應用	變更
CMS_Web_VPN_Connection	CMS_laboratory	✗	✗	<input type="button" value="修改"/>

圖 24-9 遠端 UTM、MHG SSL Web VPN 認證設定

來源網路	目的網路	服務名稱	動作	項目	變更	排序
Outside Any	Inside Any	Any	VPN		<input type="button" value="修改"/> <input type="button" value="刪除"/> <input type="button" value="暫停"/>	1 ▼

圖 24-10 遠端 UTM、MHG 管制條例設定



說明：

1. 在遠端 UTM、MHG 【SSL Web VPN】>【設定】頁面中，要先啓用 SSL Web VPN 功能，才可讓外部使用者依照所設規則建立連線。

管制條例

第25章 管制條例

封包在通過遠端 UTM、MHG 前，需要比對是否符合管制條例（由第一條規則開始，依序往下比對）。當封包符合某條管制條例的規則時，就會按該管制條例來傳送，而不會再向下比對其他的管制條例。如封包無法符合任何管制條例時，該封包就會被攔截。

管制條例的參數包含有來源網路位址、目的網路位址、服務名稱、自動排程、認證名稱、VPN、動作、封包記錄、流量圖表、網站管制、應用程式管制、入侵偵測防禦、網頁應用程式防火牆、病毒偵測、垃圾郵件過濾、郵件歸檔/稽核、IM 側錄、頻寬管理、每個來源 IP 最大頻寬限制、P2P 軟體最大頻寬限制、每個來源 IP 最大連線數限制、最大連線數限制、每個連線的傳輸量限制、每個來源 IP 的傳輸量限制、每天的傳輸量限制、傳送模式等。系統管理員可以由這些參數，管理、設定不同出入埠間的資料傳送以及服務項目，哪些網路物件、網路服務或應用程式的封包該予以攔截或放行。

遠端 UTM、MHG 依據不同來源位址的資料封包，將管制條例設定功能區分為下列八項，以便系統主管理員，針對不同資料封包的來源 IP、來源埠、目的 IP、目的埠制訂管制規則。

- **【內部至外部】**：來源網路位址是內部網路區，目的網路位址是外部網路區。系統管理員在此功能中，訂定內部網路至外部網路間所有封包的管制、服務項目的管制規則。
- **【外部至內部】**：來源網路位址是外部網路區，目的網路位址是內部網路區（如：IP 對應、連接埠對應）。系統管理員在此功能中，訂定外部網路至內部網路間所有封包的管制、服務項目的管制規則。
- **【外部至非軍事區】**：來源網路位址是外部網路區，目的網路位址是非軍事區（如：IP 對應、連接埠對應）。系統管理員在此功能中，訂定外部網路至非軍事區間所有封包的管制、服務項目的管制規則。
- **【內部至非軍事區】**：來源網路位址是內部網路區，目的網路位址是非軍事區。系統管理員在此功能中，訂定內部網路至非軍事區間所有封包的管制、服務項目的管制規則。
- **【非軍事區至外部】**：來源網路位址是非軍事區，目的網路位址是外部網路區。系統管理員在此功能中，訂定非軍事區至外部網路間所有封包的管制、服務項目的管制規則。

- **【非軍事區至內部】**：來源網路位址是非軍事區，目的網路位址是內部網路區。系統管理員在此功能中，訂定非軍事區至內部網路間所有封包的管制、服務項目的管制規則。
- **【內部至內部】**：來源網路位址是內部網路區，目的網路位址是內部網路區。系統管理員在此功能中，訂定內部網路至內部網路間所有封包的管制、服務項目的管制規則。
- **【非軍事區至非軍事區】**：來源網路位址是非軍事區，目的網路位址是非軍事區。系統管理員在此功能中，訂定非軍事區至非軍事區間所有封包的管制、服務項目的管制規則。

【管制條例】功能概述：

來源網路位址（來源網路）& 目的網路位址（目的網路）說明如下：

- 來源網路位址（來源網路）與 目的網路位址（目的網路）是以遠端 UTM、MHG 為觀察點。主動連線的一端為來源網路位址，被連線的一端為目的網路位址。
- 點擊管制條例列表中的【來源網路】、【目的網路】欄位，可即時修改所套用的【位址表】、【IP 對應】、【連接埠對應】、【連接埠對應群組】設定。

服務名稱 說明如下：


- 為該管制條例所管制的服務項目。可以選用系統預設，或是選用系統管理員所自訂的服務項目。
- 點擊管制條例列表中的【服務名稱】欄位，可即時修改所套用的【服務表】設定。

項目 說明如下：


- 顯示該管制條例之各項監控功能是否已啟動，若該項功能已啟動則會出現該功能的代表圖示。（圖示說明如下方表格）

圖 示	名 稱	說 明
	自動排程	已啟動排程表所制訂時間範圍內自動執行功
	認證名稱	認證功能已運作。
	封包記錄	封包記錄功能已運作。
	流量圖表	流量圖表功能已運作。
	入侵偵測防禦	已啟動入侵偵測防禦功能。
	網站管制	網站管制功能已開啓。
	應用程式管制	已啓用應用程式管制功能。
	網頁應用程式防火牆	已啓用網頁應用程式防火牆功能。
	病毒偵測、垃圾郵件過濾、郵件歸檔/稽核	已啟動病毒偵測、垃圾郵件過濾、郵件歸檔/稽核功能。
	頻寬管理	頻寬管理功能已開啓。
	IM 側錄	已啟動 MSN、QQ、YAHOO 傳訊內容記錄功能。
	傳送模式	已設定透過指定埠傳輸的封包，要轉換成特定 IP 或以使用者電腦 IP 位址連上網路。

自動排程 說明如下：

- 設定該條管制條例的運作時間。
- 點擊管制條例列表中的，可即時修改所套用的【排程表】設定。

認證名稱 說明如下：







- 使用者必須通過認證，才可經由該管制條例連線。
- 點擊管制條例列表中的，可即時修改所套用的【認證表】設定。

VPN 說明如下：


- 將 SSL Web VPN、套用至 VPN Trunk 的 IPSec 和 PPTP VPN 連線傳輸封包，經由該管制條例控管。

動作 說明如下：


- 指定資料封包經由遠端 UTM、MHG，允許傳送的路徑（WAN1、WAN2、...）或禁止傳送。（圖示說明如下方表格）

圖 示	名 稱	說 明
	允許所有外部網路介面	允許符合該管制條例的封包從 WAN1、WAN2、...進出。
	允許 WAN1	允許符合該管制條例的封包從 WAN1 進出。
	允許 WAN2	允許符合該管制條例的封包從 WAN2 進出。
	允許 VPN	允許符合該管制條例的 VPN 連線封包進出。
	拒絕所有外部網路介面	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。


封包記錄 說明如下：

- 記錄通過該條管制條例所有封包使用的協定、埠號、來源位址、目的位址、...。
- 點擊管制條例列表中的，可即時查閱相關封包記錄。


流量圖表 說明如下：

- 將通過該條管制條例的網路流量繪製成圖表。
- 點擊管制條例列表中的，可即時查閱相關流量圖表。

網站管制 說明如下：

- 可管制透過網頁（HTTP）和 FTP 存取的網路資源、連線的特定網站。
- 點擊管制條例列表中的 ，可即時修改所套用的【網站管制】設定。

應用程式管制 說明如下：

- 可管制即時通訊、點對點軟體、影音軟體、網頁郵件、線上遊戲、通道軟體和遠端控制軟體的連線。
- 點擊管制條例列表中的 ，可即時修改所套用的【應用程式管制】設定。

入侵偵測防禦 說明如下：

- 通過該條管制條例的封包，皆會透過入侵偵測防禦機制過濾。

網頁應用程式防火牆 說明如下：

- 通過該條管制條例過濾執行網頁應用程式的行為。

病毒偵測 說明如下：

- 偵測通過該條管制條例，以 POP3 和 SMTP 協定傳送的郵件、HTTP/Web-Based Mail 和 FTP 協定存取的檔案，是否有夾帶病毒。

垃圾郵件過濾 說明如下：

- 偵測通過該條管制條例，以 POP3 和 SMTP 協定傳送的郵件，是否為垃圾信。


郵件歸檔/稽核 說明如下：

- 判斷通過該條管制條例，以 POP3 和 SMTP 協定傳送的郵件，經病毒偵測和垃圾郵件過濾允許傳送後，是否要稽核、歸檔。

IM 側錄 說明如下：

- 記錄通過該條管制條例，以 MSN、QQ、YAHOO 傳送的訊息內容。

頻寬管理 說明如下：

- 設定該條管制條例的最大頻寬與保證頻寬（頻寬由符合該管制條例之使用者共享）。
- 點擊管制條例列表中的 ，可即時修改所套用的【頻寬表】設定。

每個來源 IP 最大頻寬限制 說明如下：

- 限定每個 IP 透過管制條例存取網路資源時，可用的頻寬。



說明：

1. 當【每個來源 IP 最大頻寬限制】使用量的總和，達到【頻寬管理】所賦予的資源量時，將無法提供頻寬給新的連線，做傳輸的動作。
 2. 當管制條例僅進行【每個來源 IP 最大頻寬限制】時，可使每位使用者，擁有相等的頻寬，穩定的存取網路資源。
-

P2P 軟體最大頻寬限制 說明如下：

- 限定以【遠端】>【管制條例選項】>【應用程式管制】的點對軟體透過管制條例存取網路資源時，可用的頻寬。

每個來源 IP 最大連線數限制 說明如下：

- 指定每個 IP 透過管制條例存取網路資源的同時連線數。如連線數超過設定值，則超過的連線無法建立成功。

最大連線數限制 說明如下：

- 指定管制條例允許的同時連線數。如連線數超過設定值，則超過的連線無法建立成功。



說明：

1. 當【每個來源 IP 最大連線數限制】的設定值，大於【最大連線數限制】的設定值時，所有通過該管制條例的連線數，皆會受限於【最大連線數限制】。
-

每個連線的傳輸量限制 說明如下：

- 該管制條例中，每個連線可使用的最高流量（KBytes）

每個來源 IP 的傳輸量限制 說明如下：

- 該管制條例中，每個 IP 每天可使用的最高總流量（MBytes）

每天的傳輸量限制 說明如下：

- 該管制條例中，每天可使用的最高總流量（MBytes）。

傳送模式 說明如下：

- 封包於外部網路、內部網路、非軍事區間，有下列傳輸模式：
 - ◆ 自動：來源位址直接轉換為遠端 UTM、MHG 的預設網路介面位址，進行傳輸的動作。
 - ◆ 路由：依原本來源（目的）位址透過遠端 UTM、MHG 網路介面進行傳輸的動作。
 - ◆ NAT：來源位址轉換為隸屬於遠端 UTM、MHG 網路介面相同網段的其他指定位址，進行傳輸的動作。



說明：

1. 在遠端 UTM、MHG【網路介面】>【介面位址】頁面中，外部網路【介面類型】的【NAT 模式】，旨在設定所有對外封包的統一位址轉換；【管制條例】的 NAT【傳送模式】則可再根據特定的來源網段進行個別指定的轉址。
-

暫停 說明如下：

- 用於停止該管制條例的作用。

排序 說明如下：

- 由於每一個封包在通過遠端 UTM、MHG 時，是由前至後逐條檢查是否符合管制條例。由此可變更管制條例之編號，以更動管制條例的優先順序。

25.1 管制條例功能使用範例

25.1.1 禁止遠端UTM、MHG內部使用者存取特定網路資源

步驟1. 在【遠端】>【網站管制】>【檔案傳輸管制】、【MIME/Script 管制】與【網站管制群組】頁面中，做下列設定：（如圖 25-1, 圖 25-2, 圖 25-3）

副檔名清單: [修改](#) ◀◀ 1 / 1 ▶▶ 移至 ▶▶

[說明](#)

名稱 ▲	副檔名	變更
All_extend	exe, zip, rar, iso, bin...	修改 刪除

◀◀ 1 / 1 ▶▶ 移至 ▶▶

[新增](#)

圖 25-1 檔案傳輸管制設定

Mime 類型清單: [修改](#) ◀◀ 1 / 1 ▶▶ 移至 ▶▶

[說明](#)

名稱 ▲	阻擋的 Script	阻擋的 MIME 類型	變更
All_Script_MIME	Window Popup...	application/msword, application/octet-stream...	修改 刪除

◀◀ 1 / 1 ▶▶ 移至 ▶▶

[新增](#)

圖 25-2MIME/Script 管制設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶

名稱 ▲	管制項目	變更
Web_Blocking_Group	白名單: --- 黑名單: --- 網站類別: --- 檔案傳輸管制 (上傳): All_extend 檔案傳輸管制 (下載): All_extend MIME / Script 管制: All_Script_MIME	修改 刪除

◀◀ 1 / 1 ▶▶ 移至 ▶▶

[新增](#)

圖 25-3 網站管制群組設定

步驟2. 在【遠端】>【管制條例選項】>【應用程式管制】>【設定】頁面中，
做下列設定：（如圖 25-4，圖 25-5）

新增應用程式管制規則

名稱： (最多 16 個字元)

☒ 即時通訊登入 (☒ 全選)

<input checked="" type="checkbox"/> MSN	<input checked="" type="checkbox"/> Yahoo	<input checked="" type="checkbox"/> ICQ/AIM	<input checked="" type="checkbox"/> QQ
<input checked="" type="checkbox"/> Skype	<input checked="" type="checkbox"/> Google Talk	<input checked="" type="checkbox"/> Gadu-Gadu	<input checked="" type="checkbox"/> Rediff
<input checked="" type="checkbox"/> WebIM	<input checked="" type="checkbox"/> 阿里旺旺	<input checked="" type="checkbox"/> 百度Hi	<input checked="" type="checkbox"/> 新浪UC
<input checked="" type="checkbox"/> Fetion	<input checked="" type="checkbox"/> Facebook聊天室	<input checked="" type="checkbox"/> Camfrog	<input checked="" type="checkbox"/> LINE
<input checked="" type="checkbox"/> WhatsApp	<input checked="" type="checkbox"/> Viber		

☒ 即時通訊傳檔

☒ 點對點軟體 (☒ 全選)

<input checked="" type="checkbox"/> Edonkey/eMule	<input checked="" type="checkbox"/> Bit Torrent/BitConnect	<input checked="" type="checkbox"/> WinMX	<input checked="" type="checkbox"/> Foxy
<input checked="" type="checkbox"/> KuGoo	<input checked="" type="checkbox"/> AppleJuice	<input checked="" type="checkbox"/> AudioGalaxy	<input checked="" type="checkbox"/> DirectConnect
<input checked="" type="checkbox"/> iMesh	<input checked="" type="checkbox"/> MUTE	<input checked="" type="checkbox"/> 迅雷5	<input checked="" type="checkbox"/> GoGoBox
<input checked="" type="checkbox"/> QQ旋風	<input checked="" type="checkbox"/> Ares	<input checked="" type="checkbox"/> Shareaza	<input checked="" type="checkbox"/> BearShare
<input checked="" type="checkbox"/> Morpheus	<input checked="" type="checkbox"/> Limewire	<input checked="" type="checkbox"/> KaZaa	<input checked="" type="checkbox"/> FlashGet

☒ 影音軟體

☒ 網頁郵件

☒ 線上遊戲

☒ 通道軟體

☒ 遠端控制軟體

☒ 其他軟體

圖 25-4 設定應用程式管制

應用程式特徵檔更新資訊

最近查詢時間：2012/07/05 15:00:01 (每小時自動更新特徵定義檔)

特徵定義檔版本：7.4.1 (更新於 2012/07/03 17:00:03)

立即更新特徵定義檔 (使用 TCP 埠號：80 和 UDP 埠號：53)

應用程式管制規則

1 / 1

名稱 ▲	應用程式	變更
IM_P2P_Blocking	MSN, Yahoo, ICQ/AIM, QQ, Skype, Google Talk, Gadu-Gadu, Rediff, W...	<input type="button" value="修改"/> <input type="button" value="刪除"/>

1 / 1

圖 25-5 完成應用程式管制設定

步驟3. 在【遠端】>【管制條例選項】>【位址表】>【外部網路】、【外部網路群組】頁面中，做下列設定：（如圖 25-6, 圖 25-7）

匯出外部網路位址表至用戶端:

從用戶端匯入外部網路位址表: (最大檔案大小: 1 MBytes)

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

名稱 ▲	網際協定	IP位址 / 子網路遮罩	變更
Outside Any	---	---	<input type="button" value="使用中"/>
Remote_Server1	IPv4	61.219.38.98 / 255.255.255.255	<input type="button" value="修改"/> <input type="button" value="刪除"/>
Remote_Server2	IPv4	202.1.237.21 / 255.255.255.255	<input type="button" value="修改"/> <input type="button" value="刪除"/>

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

圖 25-6 外部網路位址設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

名稱 ▲	成員	變更
*CHU	---	<input type="button" value="使用中"/> <input type="button" value="刪除"/>
*CHINA_TELECOM	---	<input type="button" value="使用中"/> <input type="button" value="刪除"/>
*CHINA_EDU	---	<input type="button" value="使用中"/> <input type="button" value="刪除"/>
*CHINA_MOBILE	---	<input type="button" value="使用中"/> <input type="button" value="刪除"/>
WAN_Group	Remote_Server1, Remote_Server2	<input type="button" value="修改"/> <input type="button" value="刪除"/>

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

*CHINA_TELECOM, *CHU, *CHINA_EDU 和 *CHINA_MOBILE

圖 25-7 外部網路位址群組設定

- 步驟4. 在【遠端】>【管制條例】>【內部至外部】頁面中，做下列設定：
- 按下【新增】鈕。
 - 【分配】選擇指定的遠端 UTM、MHG。
 - 【目的網路位址】選擇所設定的外部網路位址群組規則。（以 IP 做阻擋的動作）
 - 【動作】勾選拒絕所有外部網路介面。
 - 按下【確定】鈕。（如圖 25-8）
 - 再次按下【新增】鈕。
 - 【分配】選擇指定的遠端 UTM、MHG。
 - 【網站管制】選擇所設定的網站管制群組規則。
 - 【應用程式管制】選擇所設定的應用程式管制規則。
 - 按下【確定】鈕，完成設定。（如圖 25-9, 圖 25-10）

新增管制條例	
分配：	<input checked="" type="radio"/> 裝置：UTM172.19.20.11 <input type="radio"/> 群組：GROUP_1
來源網路位址：	Inside Any
目的網路位址：	WAN_Group
服務名稱：	Any
自動排程：	----- None -----
認證名稱：	----- None -----
VPN：	----- None -----
動作：	<input type="checkbox"/> 允許所有外部網路介面 <input checked="" type="checkbox"/> 拒絕所有外部網路介面 僅允許下列網路介面： <input type="checkbox"/> (LAN1) <input type="checkbox"/> (WAN1) <input type="checkbox"/> (WAN2) <input type="checkbox"/> (DMZ1)
報告機制：	
封包記錄：	<input type="checkbox"/> 開啓
流量圖表：	<input type="checkbox"/> 開啓
網站管制：	----- None -----
應用程式管制：	----- None -----
+ 進階設定	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 25-8 設定阻擋連線指定外部網路位址之管制條例

新增管制條例

分配：
☒ 裝置：UTMM172.19.20.11
☐ 群組：GROUP_1

來源網路位址：Inside Any
 目的網路位址：Outside Any
 服務名稱：Any
 自動排程：----- None -----
 認證名稱：----- None -----
 VPN：----- None -----

動作：
☒ 允許所有外部網路介面 ☐ 拒絕所有外部網路介面
 僅允許下列網路介面：
☐ (LAN1) ☐ (WAN1) ☐ (WAN2) ☐ (DMZ1)

報告機制：
 封包記錄：☐ 開啓
 流量圖表：☐ 開啓

網站管制：Web_Blocking_Group
 應用程式管制：IM_P2P_Blocking

[+ 進階設定](#)

圖 25-9 管制條例套用網站、應用程式管制規則

裝置名稱: 全部

來源網路	目的網路	服務名稱	動作	項目	變更
Inside Any	WAN_Group	Any	✗		修改 刪除 暫停
Inside Any	Outside Any	Any	✓		修改 刪除 暫停

圖 25-10 完成管制條例設定



說明：

1. 管制條例的拒絕動作可阻擋符合該管制條例的封包進出，系統管理員可將該管制條例置於第一位階，來阻止使用者與特定 IP 連線。

步驟5. 在指定的遠端 UTM、MHG 中，會產生相映規則設定。(如圖 25-11, 圖 25-12, 圖 25-13, 圖 25-14, 圖 25-15, 圖 25-16, 圖 25-17)

副檔名清單: [修改](#) ◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

[說明](#)

名稱 ▲	副檔名	變更
CMS_All_extend	exe, zip, rar, iso, bin...	修改

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

[新增](#)

圖 25-11 遠端 UTM、MHG 檔案傳輸管制設定

Mime 類型清單: [修改](#) ◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

[說明](#)

名稱 ▲	阻擋的 Script	阻擋的 MIME 類型	變更
CMS_All_Script_MIME	Window Popup...	application/msword, application/octet-stream...	修改

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

[新增](#)

圖 25-12 遠端 UTM、MHG MIME/Script 管制設定

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

名稱 ▲	管制項目	變更
CMS_Web_Blocking_Gr	白名單: --- 黑名單: --- 網站類別: --- 檔案傳輸管制 (上傳): CMS_All_extend 檔案傳輸管制 (下載): CMS_All_extend MIME / Script 管制: CMS_All_Script_MIME	修改

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

[新增](#)

圖 25-13 遠端 UTM、MHG 網站管制群組設定

應用程式特徵檔更新資訊

最近查詢時間: 2012/07/05 19:00:01 (每小時自動更新特徵定義檔)

特徵定義檔版本: 2.8.0 (更新於 2012/07/05 19:00:01)

立即更新特徵定義檔 (使用 TCP 埠號: 80 和 UDP 埠號: 53) [立即更新](#) [測試連線](#)

應用程式管制規則

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

名稱 ▲	應用程式	變更
CMS_IM_P2P_Blocking	MSN, Yahoo, ICQ/AIM, QQ, Skype, Google Talk, Gadu-Gadu, Rediff, W...	修改

◀◀ 1 / 1 ▶▶ 移至 ▶▶▶▶

[新增](#)

圖 25-14 遠端 UTM、MHG 應用程式管制設定

匯出外部網路位址表至用戶端：

從用戶端匯入外部網路位址表： (最大檔案大小: 1 MBytes)

◀◀ 1 / 1 移至 ▶▶▶

名稱▲	網際協定	IP位址 / 子網路遮罩	變更
Outside Any	---	---	<input type="button" value="使用中"/>
CMS_Remote_Server1	IPv4	61.219.38.98 / 255.255.255.255	<input type="button" value="修改"/>
CMS_Remote_Server2	IPv4	202.1.237.21 / 255.255.255.255	<input type="button" value="修改"/>

◀◀ 1 / 1 移至 ▶▶▶

圖 25-15 遠端 UTM、MHG 外部網路位址設定

◀◀ 1 / 1 移至 ▶▶▶

名稱▲	成員	變更
*CHU	---	<input type="button" value="使用中"/> <input type="button" value="刪除"/>
*CHINA_TELECOM	---	<input type="button" value="使用中"/> <input type="button" value="刪除"/>
*CHINA_EDU	---	<input type="button" value="使用中"/> <input type="button" value="刪除"/>
*CHINA_MOBILE	---	<input type="button" value="使用中"/> <input type="button" value="刪除"/>
CMS_WAN_Group	CMS_Remote_Server1, CMS_Remote_Server2	<input type="button" value="修改"/>

◀◀ 1 / 1 移至 ▶▶▶

*CHINA_TELECOM, *CHU, *CHINA_EDU 和 *CHINA_MOBILE

圖 25-16 遠端 UTM、MHG 外部網路位址群組設定

◀◀ 1 / 1 移至 ▶▶▶

來源網路	目的網路	服務名稱	動作	項目	變更	排序
Inside Any	CMS_WAN_Group	Any	✗		<input type="button" value="修改"/> <input type="button" value="刪除"/>	<input type="button" value="暫停"/> 1
Inside Any	Outside Any	Any	✓	⊘ ⊘	<input type="button" value="修改"/> <input type="button" value="刪除"/>	<input type="button" value="暫停"/> 2

◀◀ 1 / 1 移至 ▶▶▶

圖 25-17 遠端 UTM、MHG 管制條例設定

即時監控

第26章 監控記錄

用來直接瀏覽遠端 UTM、MHG 所儲存的封包記錄、事件記錄、連線記錄、病毒過濾記錄、應用程式管制記錄、連線數限制記錄、傳輸量限制記錄報表。

- **【封包記錄】**：可在制定遠端 UTM、MHG **【管制條例】**時啟用，會詳細記錄通過管制條例傳送的封包資訊。
- **【事件記錄】**：遠端 UTM、MHG 系統運作、登入、組態參數值（System Configurations）更改...記錄。
- **【連線記錄】**：記錄遠端 UTM、MHG 的 VPN、PPPoE、...連線資訊；若連線發生問題時，系統管理員可憑藉此資訊，了解問題的所在。
- **【病毒過濾記錄】**：記錄所有經過遠端 UTM 管制條例，存取 HTTP/Web-Based Mail、FTP 服務時，偵測到的病毒資訊。
- **【應用程式管制記錄】**：記錄被遠端 UTM、MHG 阻擋的應用程式存取資訊。
- **【連線數限制記錄】**：記錄達到遠端 UTM、MHG 管制條例連線數限制的資訊。
- **【傳輸量限制記錄】**：記錄達到遠端 UTM、MHG 管制條例傳輸量限制的資訊。

【封包記錄】功能概述：

搜尋 說明如下：

■ 可依照日期、管制條例方向、排序、來源位址、目的位址和目的埠號等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。

◆ 在【遠端】>【即時監控】>【監控記錄】>【封包記錄】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：

- 開啓並設定搜尋指定時間區間內的記錄。
- 選擇指定【管制條例方向】、【排序】。
- 按下【搜尋】鈕。（如圖 26-1）
- 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如

圖 26-2)

搜尋 封包記錄

☒ 起始 日期 / 時間: 2012 / 07 / 09 00 : 00
結束 日期 / 時間: 2012 / 07 / 09 20 : 35
管制條例方向: 所有方向
排序: All
來源位址:
目的位址:
目的埠號: - (範圍: 1 - 65535)

搜尋

結果

2012-07-09 (3449964 筆記錄)

下載

1 / 172499 移至

時間	來源位址	目的位址	通訊協定	埠號	流量	處置方式
20:35:37	83.25.159.236	210.59.207.104	TCP	18756→80(WAN=1)	841.0 B	✓
20:35:37	79.187.60.90	210.59.207.104	TCP	2688→80(WAN=1)	841.0 B	✓
20:35:37	220.130.155.11	210.59.207.104	TCP	2505→80(WAN=1)	841.0 B	✓
20:35:37	220.128.209.194	210.59.207.104	TCP	3358→80(WAN=1)	841.0 B	✓
20:35:37	211.72.81.206	210.59.207.104	TCP	2675→80(WAN=1)	841.0 B	✓
20:35:37	211.23.199.139	210.59.207.104	TCP	2762→80(WAN=1)	841.0 B	✓
20:35:37	200.107.67.26	210.59.207.104	TCP	4915→80(WAN=1)	841.0 B	✓
20:35:37	175.180.65.30	210.59.207.104	TCP	2576→80(WAN=1)	841.0 B	✓
20:35:37	163.22.72.94	210.59.207.104	TCP	3037→80(WAN=1)	841.0 B	✓
20:35:37	163.22.145.126	210.59.207.104	TCP	2265→80(WAN=1)	841.0 B	✓
20:35:37	125.67.126.81	210.59.207.104	TCP	2917→80(WAN=1)	841.0 B	✓
20:35:36	84.121.220.6	210.59.207.104	TCP	3542→80(WAN=1)	841.0 B	✓
20:35:36	80.55.73.142	210.59.207.104	TCP	1782→80(WAN=1)	841.0 B	✓
20:35:36	80.53.87.170	210.59.207.104	TCP	1681→80(WAN=1)	841.0 B	✓
20:35:36	218.86.28.83	210.59.207.104	TCP	1065→80(WAN=1)	841.0 B	✓
20:35:36	218.7.204.130	210.59.207.104	TCP	3795→80(WAN=1)	841.0 B	✓
20:35:36	210.68.117.127	210.59.207.104	TCP	2711→80(WAN=1)	841.0 B	✓
20:35:36	200.46.252.194	210.59.207.104	TCP	1484→80(WAN=1)	841.0 B	✓
20:35:36	189.19.67.234	210.59.207.104	TCP	1967→80(WAN=1)	853.0 B	✓
20:35:36	114.32.242.26	210.59.207.104	TCP	4081→80(WAN=1)	841.0 B	✓

1 / 172499 移至

圖 26-1 搜尋特定記錄

搜尋 封包記錄

☒ 起始 日期 / 時間: 2012 / 07 / 09 00 : 00
 結束 日期 / 時間: 2012 / 07 / 09 20 : 35
 管制條例方向: 所有方向
 排序: All
 來源位址:
 目的位址:
 目的埠號: - (範圍: 1 - 65535)

搜尋

結果

2012-07-09 (3449964 筆記錄)

下載

1 / 172499 移至

時間	來源位址	目的位址	通訊協定	埠號	流量	處置方式
20:35:37	83.25.159.236	210.59.207.104	TCP	18756→80(WAN=1)	841.0 B	✓
20:35:37	79.187.60.90	210.59.207.104	TCP	2688→80(WAN=1)	841.0 B	✓
20:35:37	220.130.155.11	210.59.207.104	TCP	2505→80(WAN=1)	841.0 B	✓
20:35:37	220.128.209.194	210.59.207.104	TCP	3358→80(WAN=1)	841.0 B	✓
20:35:37	211.72.81.1				.0 B	✓
20:35:37	211.23.199.1				.0 B	✓
20:35:37	200.107.67.1				.0 B	✓
20:35:37	175.180.65.1				.0 B	✓
20:35:37	163.22.72.1				.0 B	✓
20:35:37	163.22.145.1				.0 B	✓
20:35:37	125.67.126.1				.0 B	✓
20:35:36	84.121.220.1				.0 B	✓
20:35:36	80.55.73.1				.0 B	✓
20:35:36	80.53.87.1				.0 B	✓
20:35:36	218.86.28.1				.0 B	✓
20:35:36	218.7.204.1				.0 B	✓
20:35:36	210.68.117.127	210.59.207.104	TCP	2711→80(WAN=1)	841.0 B	✓
20:35:36	200.46.252.194	210.59.207.104	TCP	1484→80(WAN=1)	841.0 B	✓
20:35:36	189.19.67.234	210.59.207.104	TCP	1967→80(WAN=1)	853.0 B	✓
20:35:36	114.32.242.26	210.59.207.104	TCP	4081→80(WAN=1)	841.0 B	✓

1 / 172499 移至

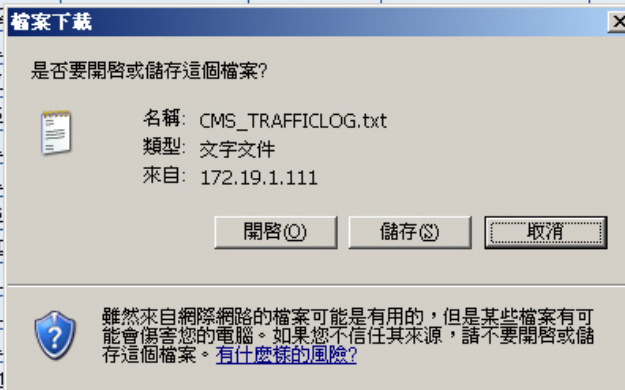


圖 26-2 下載搜尋的記錄

【事件記錄】功能概述：

搜尋 說明如下：

- 可依照日期、管理員名稱、IP 位址、事件類型和僅顯示有詳細內容之事件記錄等關鍵字或特徵，來尋找儲存在遠端 UTM·MHG 所有符合條件之記錄。
 - ◆ 在【遠端】>【即時監控】>【監控記錄】>【事件記錄】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 選擇指定【事件類型】。
 - 按下【搜尋】鈕。（如圖 26-3）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如圖 26-4）

搜尋 事件記錄

☒ 起始 日期 / 時間: 2012 / 05 / 10 11 : 00
結束 日期 / 時間: 2012 / 07 / 10 11 : 22
管理員名稱: (最多 30 個字元)
IP位址:
事件類型: 所有類型
☐ 僅顯示有詳細內容之事件記錄

搜尋

結果

2012-07-10 (28 筆記錄)

下載

1 / 2 移至

時間	管理員名稱	IP位址	事件	內容
11:12:16	admin	172.19.50.19	登入成功	---
10:25:39	admin	172.19.20.12	登入成功	---
10:00:01	system	127.0.0.1	寄送郵件通知 (nusoft.com.tw)	---
09:49:05	admin	172.19.20.7	登入成功	---
09:26:26	admin	172.19.50.19	登入成功	---
09:25:43	admin	172.19.50.19	登入成功	---
09:25:43	admin	172.19.50.19	登入成功	---
09:25:37	admin	172.19.50.19	登入成功	---
09:25:37	admin	172.19.50.19	登入成功	---
09:25:36	admin	172.19.50.19	登入成功	---
09:25:36	admin	172.19.50.19	登入成功	---
09:25:36	admin	172.19.50.19	登入成功	---
01:27:23	admin	220.133.110.173	登入成功	---
01:27:01	admin	220.133.110.173	登入成功	---
01:27:00	admin	220.133.110.173	登入成功	---
01:25:31	admin	220.133.110.173	登入成功	---
01:25:31	admin	220.133.110.173	登入成功	---
01:25:30	admin	220.133.110.173	登入成功	---
01:24:15	admin	220.133.110.173	登入成功	---
01:24:15	admin	220.133.110.173	登入成功	---

1 / 2 移至

圖 26-3 搜尋特定記錄

搜尋 事件記錄

☒ 起始 日期/時間: 2012 / 05 / 10 11 : 00
 結束 日期/時間: 2012 / 07 / 10 11 : 22
 管理員名稱: (最多 30 個字元)
 IP位址:
 事件類型: 所有類型
☐ 僅顯示有詳細內容之事件記錄

搜尋

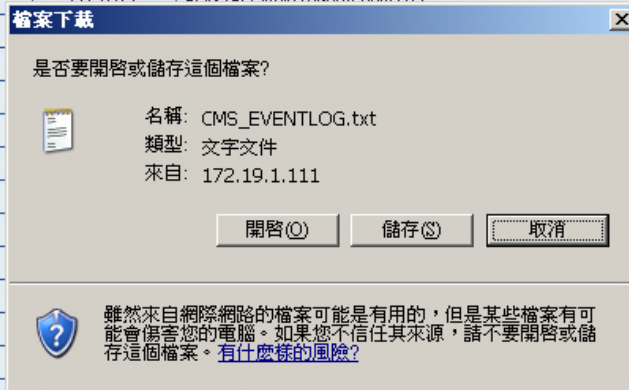
結果

2012-07-10 (28 筆記錄)

下載

1 / 2 移至

時間	管理員名稱	IP位址	事件	內容
11:12:16	admin	172.19.50.19	登入成功	---
10:25:39	admin	172.19.20.12	登入成功	---
10:00:01	system	127.0.0.1	發送郵件通知 (nmssoft.com.tw)	---
09:49:05	admin			---
09:26:26	admin			---
09:25:43	admin			---
09:25:43	admin			---
09:25:37	admin			---
09:25:37	admin			---
09:25:36	admin			---
09:25:36	admin			---
09:25:36	admin			---
01:27:23	admin			---
01:27:01	admin			---
01:27:00	admin	220.133.110.173	登入成功	---
01:25:31	admin	220.133.110.173	登入成功	---
01:25:31	admin	220.133.110.173	登入成功	---
01:25:30	admin	220.133.110.173	登入成功	---
01:24:15	admin	220.133.110.173	登入成功	---
01:24:15	admin	220.133.110.173	登入成功	---



1 / 2 移至

圖 26-4 下載搜尋的記錄

【連線記錄】功能概述：

搜尋 說明如下：

- 撥號連線：可依照日期等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
- 動態 IP 位址：可依照日期等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
- DHCP：可依照日期等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
- PPTP Server：可依照日期等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
- PPTP Client：可依照日期等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
- IPSec：可依照日期等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
- Web VPN：可依照日期等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
- SMTP 內送郵件：可依照日期、IP 位址、寄件者、收件者、狀態和內容等關鍵字或特徵，來尋找儲存在遠端 UTM 所有符合條件之記錄。
- SMTP 外寄郵件：可依照日期、IP 位址、寄件者、收件者、狀態和內容等關鍵字或特徵，來尋找儲存在遠端 UTM 所有符合條件之記錄。
- POP3：可依照日期、IP 位址、帳號、狀態和內容等關鍵字或特徵，來尋找儲存在遠端 UTM 所有符合條件之記錄。
- ◆ 在【遠端】>【即時監控】>【監控記錄】>【連線記錄】的指定【遠端裝置】>【IPSec】>【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 按下【搜尋】鈕。(如圖 26-5)
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。(如圖 26-6)

搜尋 連線記錄

☒ 起始 日期 / 時間: 2012 / 05 / 11 00 : 00
 結束 日期 / 時間: 2012 / 07 / 10 16 : 09

搜尋

結果

2012-06-05(25994 recorders)

下載

1 / 1300 移至

時間	連線訊息
10:13:29	terminating all conns with alias='1111'
10:07:04	terminating all conns with alias='1111'
10:05:31	terminating all conns with alias='1111'
10:03:34	packet from 111.249.204.247:500: initial Main Mode message received on 220.135.197.227:500 but no connection has b...
10:03:34	packet from 111.249.204.247:500: received Vendor ID payload [Dead Peer Detection]
10:03:34	packet from 111.249.204.247:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
10:03:34	packet from 111.249.204.247:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already usin...
10:03:34	packet from 111.249.204.247:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
10:03:31	packet from 111.249.176.164:500: initial Main Mode message received on 220.135.197.227:500 but no connection has b...
10:03:31	packet from 111.249.176.164:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
10:03:31	packet from 111.249.176.164:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already usin...
10:03:31	packet from 111.249.176.164:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n] meth=106, but already us...
10:03:31	packet from 111.249.176.164:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] meth=108, but already usin...
10:03:30	packet from 111.249.176.164:500: received Vendor ID payload [RFC 3947] method set to=109
10:03:30	packet from 111.249.176.164:500: received Vendor ID payload [Dead Peer Detection]
10:03:30	packet from 111.249.176.164:500: received Vendor ID payload [Openswan (this version) 2.6.23]
10:03:30	packet from 210.177.210.178:500: received and ignored informational message
10:03:30	packet from 210.177.210.178:500: ignoring Delete SA payload: not encrypted
10:03:21	packet from 111.249.176.164:500: initial Main Mode message received on 220.135.197.227:500 but no connection has b...
10:03:21	packet from 111.249.176.164:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]

1 / 1300 移至

圖 26-5 搜尋特定記錄

搜尋 連線記錄

☒ 起始 日期 / 時間: 2012 / 05 / 11 00 : 00
結束 日期 / 時間: 2012 / 07 / 10 16 : 09

搜尋

結果

2012-06-05(25994 recorders)

下載

1 / 1300 移至

時間	連線訊息
10:13:29	terminating all conns with alias='1111'
10:07:04	terminating all conns with alias='1111'
10:05:31	terminating all conns with alias='1111'
10:03:34	packet from 111.249.204.247:500: initial Main Mode message received on 220.135.197.227:500 but no connection has b...
10:03:34	packet from 111.249.204.247:500: received Vendor ID payload [Dead Peer Detection]
10:03:34	packet from
10:03:34	packet from
10:03:34	packet from
10:03:31	packet from
10:03:31	packet from
10:03:31	packet from
10:03:31	packet from
10:03:31	packet from
10:03:31	packet from
10:03:31	packet from
10:03:30	packet from
10:03:30	packet from
10:03:30	packet from
10:03:30	packet from
10:03:30	packet from
10:03:30	packet from 210.177.210.178:500: ignoring Delete SA payload: not encrypted
10:03:21	packet from 111.249.176.164:500: initial Main Mode message received on 220.135.197.227:500 but no connection has b...
10:03:21	packet from 111.249.176.164:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]

1 / 1300 移至

檔案下載

是否要開啓或儲存這個檔案?

名稱: CMS_CONNECTIONLOG.txt
類型: 文字文件
來自: 172.19.1.111

開啓(O)

儲存(S)

取消

雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。[有什麼樣的風險?](#)

圖 26-6 下載搜尋的記錄

【病毒過濾記錄】功能概述：

搜尋 說明如下：

- 可依照日期、來源位址、目的位址、網路服務、中毒檔案和病毒名稱等關鍵字或特徵，來尋找儲存在遠端 UTM 所有符合條件之記錄。
 - ◆ 在【遠端】>【即時監控】>【監控記錄】>【病毒過濾記錄】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 按下【搜尋】鈕。（如圖 26-7）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如

圖 26-8)

搜尋 病毒過濾記錄

☒ 起始 日期 / 時間: 2012 / 05 / 29 00 : 00
結束 日期 / 時間: 2012 / 07 / 13 14 : 26
來源位址:
目的位址:
網路服務: (最多 30 個字元)
中毒檔案: (最多 30 個字元)
病毒名稱: (最多 30 個字元)

搜尋

結果

2012-06-26 (1 筆記錄)

下載

時間	來源位址	目的位址	網路服務	中毒檔案	病毒名稱
10:21:02	kang_auth	eicar.org	HTTP	eicar.com	Eicar-Test-Signature.U...

圖 26-7 搜尋特定記錄

搜尋 病毒過濾記錄

☒ 起始 日期/時間: 2012 / 05 / 29 00 : 00
 結束 日期/時間: 2012 / 07 / 13 14 : 26
 來源位址:
 目的位址:
 網路服務: (最多 30 個字元)
 中毒檔案: (最多 30 個字元)
 病毒名稱: (最多 30 個字元)

搜尋

結果

2012-06-28 (1 筆記錄)

下載

1 / 1 移至

時間	來源位址	目的位址	網路服務	中毒檔案	病毒名稱
10:21:02	kang_auth	eicar.org	HTTP	eicar.com	Eicar-Test-Signature.U...

檔案下載

是否要開啓或儲存這個檔案?



名稱: CMS_VIRUSLOG.txt
 類型: 文字文件
 來自: 172.19.1.111

開啓(O)

儲存(S)

取消



雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。[有什麼樣的風險?](#)

圖 26-8 下載搜尋的記錄

【應用程式管制記錄】功能概述：

搜尋 說明如下：

- 可依照日期和來源位址等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
 - ◆ 在【遠端】>【即時監控】>【監控記錄】>【應用程式管制記錄】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 按下【搜尋】鈕。（如圖 26-9）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如圖 26-10）

搜尋 應用程式管制記錄

☒ 起始 日期/時間: 2012 / 05 / 16 00 : 00
結束 日期/時間: 2012 / 07 / 13 14 : 36
來源位址:

搜尋

結果

2012-07-05 (5 筆記錄)

下載

時間	來源位址	應用程式管制記錄
21:55:11	PUREXP	Edonkey/eMule
18:55:13	PUREXP	迅雷5
10:59:35	LINUX-CD20	QQ登入
10:27:25	PUREXP	QQ登入
10:09:49	172.19.50.5	QQ登入

圖 26-9 搜尋特定記錄

搜尋 應用程式管制記錄

☒ 起始 日期 / 時間: 2012 / 05 / 16 00 : 00
 結束 日期 / 時間: 2012 / 07 / 13 14 : 36
 來源位址:

搜尋

結果

2012-07-05 (5 筆記錄)

下載

時間	來源位址	應用程式管制記錄
21:55:11	PUREXP	Edonkey/eMule
16:55:13	PIRFXP	迅雷5
10:59:35		登入
10:27:25		登入
10:09:49		登入

檔案下載

是否要開啓或儲存這個檔案?

名稱: CMS_APPLICATION_BLOCKING_LOG.txt
 類型: 文字文件
 來自: 172.19.1.111

雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。[有什麼樣的風險?](#)

圖 26-10 下載搜尋的記錄

【連線數限制記錄】功能概述：

搜尋 說明如下：

- 可依照日期和來源位址等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
 - ◆ 在【遠端】>【即時監控】>【監控記錄】>【連線數限制記錄】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 按下【搜尋】鈕。（如圖 26-11）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如圖 26-12）

搜尋 連線數限制記錄

☒ 起始 日期 / 時間: 2012 / 05 / 25 00 : 00
結束 日期 / 時間: 2012 / 07 / 13 14 : 43
來源位址:

結果

2012-06-28 (1 筆記錄)

1 / 1 移至

時間	來源位址	管制條例方向	限制原因
10:36:31	kang_auth	內部至外部	最大連線數超過允許值

1 / 1 移至

圖 26-11 搜尋特定記錄

搜尋 連線數限制記錄

☒ 起始 日期 / 時間: 2012 / 05 / 25 00 : 00
結束 日期 / 時間: 2012 / 07 / 13 14 : 43
來源位址:

搜尋

結果

2012-06-28 (1 筆記錄)

下載

1 / 1 移至

時間	來源位址	管制條例方向	限制原因
10:36:31	kang_auth	內部至外部	最大連線數超過允許值



1 / 1 移至

圖 26-12 下載搜尋的記錄

【傳輸量限制記錄】功能概述：

搜尋 說明如下：

- 可依照日期和來源位址等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
 - ◆ 在【遠端】>【即時監控】>【監控記錄】>【傳輸量限制記錄】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：
 - 開啓並設定搜尋指定時間區間內的記錄。
 - 按下【搜尋】鈕。（如圖 26-13）
 - 按【下載】鈕，將目前搜尋到的記錄檔即時備份到本機電腦來。（如

圖 26-14)

搜尋 傳輸量限制記錄

☒ 起始 日期 / 時間: 2012 / 05 / 25 00 : 00
結束 日期 / 時間: 2012 / 07 / 13 14 : 48
來源位址:

搜尋

結果

2012-06-26 (1 筆記錄)

下載

1 / 1 移至

時間	來源位址	管制條例方向	限制原因
10:37:54	kang_auth	內部至外部	超過每天允許傳輸量

1 / 1 移至

圖 26-13 搜尋特定記錄

搜尋 傳輸量限制記錄

☒ 起始 日期 / 時間: 2012 / 05 / 25 00 : 00
結束 日期 / 時間: 2012 / 07 / 13 14 : 48
來源位址:

搜尋

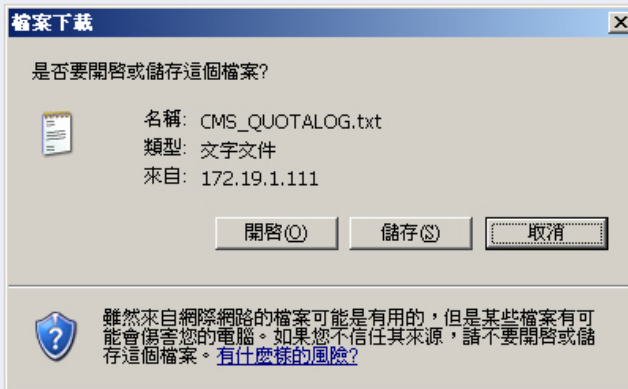
結果

2012-06-28 (1 筆記錄)

下載

1 / 1 移至

時間	來源位址	管制條例方向	限制原因
10:37:54	kang_auth	內部至外部	超過每天允許傳輸量



1 / 1 移至

圖 26-14 下載搜尋的記錄

26.1 封包記錄

26.1.1 檢視使用者透過遠端UTM、MHG存取內、外部網路資源，使用的協定及埠號

步驟1. 在【遠端】>【即時監控】>【監控記錄】>【封包記錄】的指定【遠端裝置】頁面中，可顯示遠端 UTM、MHG 所儲存的系統封包監控記錄。

(如圖 26-15)

- 點擊【來源位址】或【目的位址】連結，會彈出一視窗列出所選擇之 IP 存取網路資源時，透過之通訊協定、埠號和所使用之流量。(如圖 26-16)
- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由遠端 UTM、MHG 清除。(如圖 26-17)

遠端裝置: Branch_UTM-2000 (172.19.1.254)

更新

1 / 8948 移至

時間	來源位址	目的位址	通訊協定	埠號	流量	處置方式
12:17:50	84.241.38.178	210.59.207.104	TCP	23996→80(WAN=1)	747.0 B	✓
12:17:50	61.28.37.220	210.59.207.104	TCP	2777→80(WAN=1)	978.0 B	✓
12:17:50	61.220.51.230	210.59.207.104	TCP	3193→80(WAN=1)	1.1 KB	✓
12:17:50	60.250.107.103	210.59.207.104	UDP	32993→1153(WAN=1)	152.0 B	✓
12:17:50	60.248.1.133	210.59.207.104	TCP	2234→80(WAN=1)	1.2 KB	✓
12:17:50	222.210.27.188	210.59.207.104	TCP	42155→80(WAN=1)	160.0 B	✓
12:17:50	218.6.145.176	210.59.207.104	TCP	3021→80(WAN=1)	978.0 B	✓
12:17:50	187.172.80.82	210.59.207.104	TCP	4218→80(WAN=1)	1.2 KB	✓
12:17:50	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	33.0 B	✓
12:17:50	124.13.206.112	210.59.207.104	UDP	3148→1153(WAN=1)	184.0 B	✓
12:17:50	117.56.104.66	210.59.207.104	TCP	21359→80(WAN=1)	1.2 KB	✓
12:17:50	115.214.239.137	210.59.207.104	TCP	3865→80(WAN=1)	1.2 KB	✓
12:17:50	111.253.217.243	210.59.207.104	TCP	4254→80(WAN=1)	1.2 KB	✓
12:17:49	92.247.113.134	210.59.207.104	TCP	3869→80(WAN=1)	1.2 KB	✓
12:17:49	87.139.157.251	210.59.207.104	TCP	1561→80(WAN=1)	1.1 KB	✓
12:17:49	83.228.41.21	210.59.207.104	TCP	2164→80(WAN=1)	1.1 KB	✓
12:17:49	79.175.67.169	210.59.207.104	TCP	1938→80(WAN=1)	1.1 KB	✓
12:17:49	79.175.67.169	210.59.207.104	TCP	1937→80(WAN=1)	1.2 KB	✓
12:17:49	60.248.1.133	210.59.207.104	TCP	2233→80(WAN=1)	1.1 KB	✓
12:17:49	59.120.153.184	210.59.207.104	TCP	1611→80(WAN=1)	1.2 KB	✓

清除

1 / 8948 移至

圖 26-15 封包記錄

http://172.19.1.111 - [封包記錄] 內部至外部 - Microsoft Internet Explorer

更新 手動

1 / 167 移至

時間	來源位址	目的位址	通訊協定	埠號	流量	處置方式
12:21:24	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:23	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:22	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:21	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:20	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:19	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:18	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:17	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:16	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:15	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:14	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:13	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:12	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:11	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:10	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:09	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:08	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓
12:21:07	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	66.0 B	✓

完成 網際網路

圖 26-16 封包記錄過濾視窗

遠端裝置: Branch_UTM-2000 (172.19.1.254)

更新

1 / 8948 移至

時間	來源位址	目的位址	通訊協定	埠號	流量	處置方式
12:17:50	84.241.38.178	210.59.207.104	TCP	23996→80(WAN=1)	747.0 B	✓
12:17:50	61.28.37.220	210.59.207.104	TCP	2777→80(WAN=1)	978.0 B	✓
12:17:50	61.220.51.230	210.59.207.104	TCP	3193→80(WAN=1)	1.1 KB	✓
12:17:50	60.250.107.103	210.59.207.104	UDP	32993→1153(WAN=1)	152.0 B	✓
12:17:50	60.248.1.133	210.59.207.104	TCP	2234→80(WAN=1)	1.2 KB	✓
12:17:50	222.210.27.188	210.59.207.104	TCP	42155→80(WAN=1)	160.0 B	✓
12:17:50	218.6.145.176	210.59.207.104	TCP	3021→80(WAN=1)	978.0 B	✓
12:17:50	187.172.80.82	210.59.207.104	TCP	4218→80(WAN=1)	1.2 KB	✓
12:17:50	172.19.100.84	168.95.98.254	ICMP	---(WAN=2)	33.0 B	✓
12:17:50	124.13.206.112	210.59.207.104	UDP	31153→1153(WAN=1)	184.0 B	✓
12:17:50	117.56.104.66	210.59.207.104	TCP	3021→80(WAN=1)	1.2 KB	✓
12:17:50	115.214.239.137	210.59.207.104	TCP	3021→80(WAN=1)	1.2 KB	✓
12:17:50	111.253.217.243	210.59.207.104	TCP	3021→80(WAN=1)	1.2 KB	✓
12:17:49	92.247.113.134	210.59.207.104	TCP	3021→80(WAN=1)	1.2 KB	✓
12:17:49	87.139.157.251	210.59.207.104	TCP	3021→80(WAN=1)	1.1 KB	✓
12:17:49	83.228.41.21	210.59.207.104	TCP	2164→80(WAN=1)	1.1 KB	✓
12:17:49	79.175.67.169	210.59.207.104	TCP	1938→80(WAN=1)	1.1 KB	✓
12:17:49	79.175.67.169	210.59.207.104	TCP	1937→80(WAN=1)	1.2 KB	✓
12:17:49	60.248.1.133	210.59.207.104	TCP	2233→80(WAN=1)	1.1 KB	✓
12:17:49	59.120.153.184	210.59.207.104	TCP	1611→80(WAN=1)	1.2 KB	✓

清除

Microsoft Internet Explorer 您確定要刪除？ 確定 取消


圖 26-17 清除封包記錄

26.2 事件記錄

26.2.1 檢視系統管理員登入和管理遠端UTM、MHG，及遠端UTM、

MHG寄送報表、外部網路介面運作之狀況

步驟1. 在【遠端】>【即時監控】>【監控記錄】>【事件記錄】的指定【遠端裝置】頁面中，可顯示遠端 UTM、MHG 所儲存的系統登入、管理、寄送報表、外部網路介面運作事件記錄。(如圖 26-18)

■ 按下  鈕，會顯示該筆記錄的詳細訊息。(如圖 26-19)

遠端裝置: Branch_UTM-2000 (172.19.1.254)

更新

2012-06-28 (158 筆記錄)

◀◀ 2 / 8 移至 ▶▶

時間	管理員名稱	IP位址	事件	內容
18:33:27	admin	172.19.50.21	[管制條例→內部至外部] 修改	
18:32:44	admin	172.19.50.21	[管制條例→內部至外部] 修改	
18:32:32	admin	172.19.50.21	登入成功	---
18:32:00	admin	172.19.50.21	[監控報告→網路偵測→封包側錄] 修改	
18:16:50	admin	172.19.50.21	登入成功	---
18:16:49	admin	172.19.50.21	登入成功	---
18:16:09	admin	172.19.50.21	[監控報告→網路偵測→封包側錄] 修改	
18:15:57	admin	172.19.50.21	登入成功	---
18:13:32	admin	172.19.50.21	[監控報告→網路偵測→封包側錄] 下載組態檔	---
18:12:31	admin	172.19.50.21	[監控報告→網路偵測→封包側錄] 修改	
18:12:14	admin	172.19.50.21	[管制條例→內部至外部] 修改	
18:12:00	admin	172.19.50.21	[管制條例選項→位址表→外部網路群組] 新增	
18:11:47	admin	172.19.50.21	[管制條例選項→位址表→外部網路] 新增	
18:09:39	admin	172.19.50.21	[監控報告→網路偵測→封包側錄] 下載組態檔	---
18:08:58	admin	172.19.50.21	[監控報告→網路偵測→封包側錄] 修改	
18:08:47	admin	172.19.50.21	[管制條例→內部至外部] 修改	
18:08:30	admin	172.19.50.21	[管制條例選項→位址表→外部網路] 修改	
18:07:08	admin	172.19.50.21	[監控報告→網路偵測→封包側錄] 下載組態檔	---
18:06:37	admin	172.19.50.21	[監控報告→網路偵測→封包側錄] 修改	
18:06:23	admin	172.19.50.21	[管制條例→內部至外部] 修改	

◀◀ 2 / 8 移至 ▶▶

圖 26-18 事件記錄

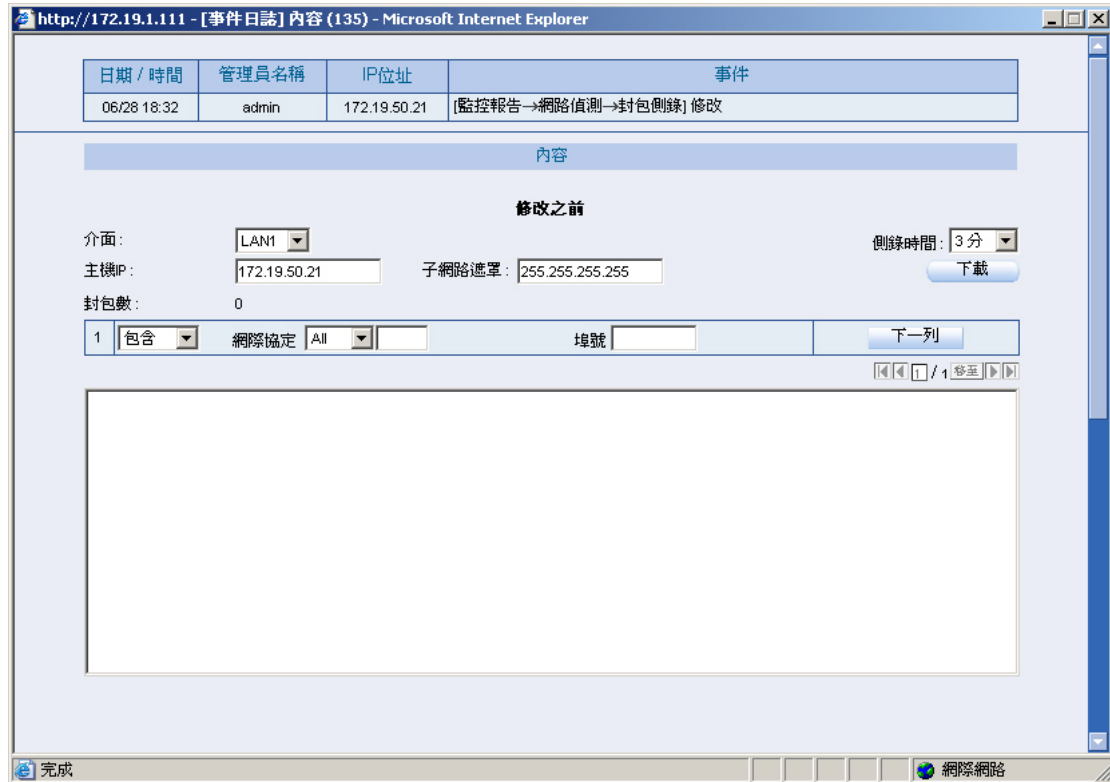


圖 26-19 事件記錄內容

26.3 連線記錄

26.3.1 檢視遠端UTM、MHG的系統連線記錄

步驟1. 在【遠端】>【即時監控】>【監控記錄】>【連線記錄】的指定【遠端裝置】頁面中，可顯示遠端 UTM、MHG 所儲存的系統撥號、動態 IP 位址、DHCP、PPTP Server、PPTP Client、IPSec、Web VPN、SMTP 內送郵件、SMTP 外寄郵件、POP3 連線狀況。(如圖 26-20)

- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由遠端 UTM、MHG 清除。(如圖 26-21)

遠端裝置: Branch_UTM-2000 (172.19.1.254)

更新

連線類型: IPSec 2012-07-16(11173 recorders)

3 / 559 移至

時間	連線訊息
17:12:19	packet from 111.249.182.44:500: initial Main Mode message received on 220.135.197.227:500 but no connection has be...
17:12:19	packet from 111.249.182.44:500: received Vendor ID payload [Dead Peer Detection]
17:12:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
17:12:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
17:12:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using ...
17:11:49	packet from 111.249.182.44:500: received Vendor ID payload [Dead Peer Detection]
17:11:49	packet from 111.249.182.44:500: initial Main Mode message received on 220.135.197.227:500 but no connection has be...
17:11:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
17:11:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
17:11:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using ...
17:11:19	packet from 111.249.182.44:500: initial Main Mode message received on 220.135.197.227:500 but no connection has be...
17:11:19	packet from 111.249.182.44:500: received Vendor ID payload [Dead Peer Detection]
17:11:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
17:11:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using ...
17:11:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
17:10:49	packet from 111.249.182.44:500: initial Main Mode message received on 220.135.197.227:500 but no connection has be...
17:10:49	packet from 111.249.182.44:500: received Vendor ID payload [Dead Peer Detection]
17:10:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
17:10:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using ...
17:10:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108

清除

3 / 559 移至

圖 26-20 連線記錄

遠端裝置: Branch_UTM-2000 (172.19.1.254)

更新

連線類型: IPSec 2012-07-16(11173 recorders)

3 / 559 移至

時間	連線訊息
17:12:19	packet from 111.249.182.44:500: initial Main Mode message received on 220.135.197.227:500 but no connection has be...
17:12:19	packet from 111.249.182.44:500: received Vendor ID payload [Dead Peer Detection]
17:12:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
17:12:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
17:12:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using ...
17:11:49	packet from 111.249.182.44:500: received Vendor ID payload [Dead Peer Detection]
17:11:49	packet from 111.249.182.44:500: initial Main Mode message received on 220.135.197.227:500 but no connection has be...
17:11:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
17:11:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
17:11:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using ...
17:11:19	packet from 111.249.182.44:500: received Vendor ID payload [Dead Peer Detection]
17:11:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
17:11:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using ...
17:11:19	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108
17:10:49	packet from 111.249.182.44:500: initial Main Mode message received on 220.135.197.227:500 but no connection has be...
17:10:49	packet from 111.249.182.44:500: received Vendor ID payload [Dead Peer Detection]
17:10:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
17:10:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using ...
17:10:49	packet from 111.249.182.44:500: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03] method set to=108

清除

3 / 559 移至

圖 26-21 清除連線記錄

26.4 病毒過濾記錄

26.4.1 檢視使用者透過HTTP/Web-Based Mail、FTP協定傳輸的檔案，經遠端UTM掃描後，阻擋的病毒記錄

步驟1. 在【遠端】>【即時監控】>【監控記錄】>【病毒過濾記錄】的指定【遠端裝置】頁面中，可顯示遠端 UTM 所儲存的系統阻擋 HTTP/Web-Based Mail、FTP 傳輸病毒檔案記錄。(如圖 26-22)

- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由遠端 UTM 清除。(如圖 26-23)



圖 26-22 病毒過濾記錄



圖 26-23 清除病毒過濾記錄

26.5 應用程式管制記錄

26.5.1 檢視遠端UTM、MHG阻擋的應用程式存取記錄

步驟1. 在【遠端】>【即時監控】>【監控記錄】>【應用程式管制記錄】的指定【遠端裝置】頁面中，可顯示遠端 UTM、MHG 所儲存的系統阻擋應用程式存取記錄。(如圖 26-24)

- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由遠端 UTM、MHG 清除。(如圖 26-25)



圖 26-24 應用程式管制記錄



圖 26-25 清除應用程式管制記錄

26.6 連線數限制記錄

26.6.1 檢視達到遠端UTM、MHG限制的連線數存取記錄

步驟1. 在【遠端】>【即時監控】>【監控記錄】>【連線數限制記錄】的指定【遠端裝置】頁面中，可顯示遠端 UTM、MHG 所儲存的系統連線數管制記錄。(如圖 26-26)

- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由遠端 UTM、MHG 清除。(如圖 26-27)



圖 26-26 連線數限制記錄



圖 26-27 清除連線數限制記錄

26.7 傳輸量限制記錄

26.7.1 檢視達到遠端UTM、MHG限制的傳輸量存取記錄

步驟1. 在【遠端】>【即時監控】>【監控記錄】>【傳輸量限制記錄】的指定【遠端裝置】頁面中，可顯示遠端 UTM、MHG 所儲存的系統傳輸量管制記錄。(如圖 26-28)

- 按下【清除】鈕，於顯示之刪除資料確認視窗中，按下【確定】鈕後，可將記錄即時由遠端 UTM、MHG 清除。(如圖 26-29)



圖 26-28 傳輸量限制記錄



圖 26-29 清除傳輸量限制記錄

第27章 流量排行

系統管理員可利用即時流量分析、今日排行榜和歷史排行榜功能，來了解使用者透過遠端 UTM、MHG 傳輸的網路流量和進行的網路活動。

- **【即時流量分析】**：可顯示進行傳輸的來源位址、網路服務之即時流量。
- **【今日排行榜】**：可顯示當天特定時段內進行傳輸的來源位址、目的位址、網路服務之累積流量。
- **【歷史排行榜】**：可顯示指定時間範圍內進行傳輸的日期、來源位址、目的位址、網路服務之累積流量。

【即時流量分析】功能概述：

來源位址 說明如下：

- 可顯示經遠端 UTM、MHG 進行傳輸的來源位址之即時流量。
- 來源位址：表示封包傳輸時的來源位址。
- 流量：表示該來源位址傳輸的資料量。
- 可將來源位址的資料傳輸總量，與其個別資料傳輸量列出比例值。

網路服務 說明如下：

- 可顯示經遠端 UTM、MHG 進行傳輸的網路服務之即時流量。
- 網路服務：表示封包傳輸時採用的通訊協定和埠號。
- 流量：表示透過該網路服務傳輸的資料量。
- 可將網路服務的資料傳輸總量，與其個別資料傳輸量列出比例值。

【今日排行榜】功能概述：

您可以拖曳 游標 / 游標間紅色區塊 來選擇欲統計的時間 說明如下：

- 可方便觀察特定時段內的流量統計資料。

來源位址 說明如下：

- 可顯示當天特定時段內，經遠端 UTM、MHG 進行傳輸的來源位址之累積流量。
- 來源位址：表示封包傳輸時的來源位址。
- 下載流量 / 上傳流量：表示該來源位址上傳/下載的資料量。
- 可將來源位址的資料傳輸總量，與其個別資料傳輸量列出比例值。

目的位址 說明如下：

- 可顯示當天特定時段內，經遠端 UTM、MHG 進行傳輸的目的位址之累積流量。
- 目的位址：表示封包傳輸時的目的位址。
- 下載流量 / 上傳流量：表示該目的位址上傳/下載的資料量。
- 可將目的位址的資料傳輸總量，與其個別資料傳輸量列出比例值。

網路服務 說明如下：

- 可顯示當天特定時段內，經遠端 UTM、MHG 進行傳輸的網路服務之累積流量。
- 網路服務：表示封包傳輸時採用的通訊協定和埠號。
- 下載流量 / 上傳流量：表示透過該網路服務上傳/下載的資料量。
- 可將網路服務的資料傳輸總量，與其個別資料傳輸量列出比例值。

【歷史排行榜】功能概述：

更新 說明如下：

- 可依照日期、來源位址、目的位址或網路服務等條件，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
 - ◆ 在遠端 UTM、MHG **【系統管理】>【組態】>【系統設定】** 頁面中，啟動並進行**【電子郵件警告 / 報告設定】**，並在**【遠端】>【即時監控】>【流量排行】>【歷史排行榜】**的指定**【遠端裝置】**頁面中，做下列設定：
 - 選擇**【來源位址】**。
 - 設定搜尋指定時間區間內的記錄。
 - 按下**【更新】**鈕。(如圖 27-1)
 - 按下**【郵寄報告】**鈕。
 - 會即時寄送相關統計報表給收件者。(如圖 27-2, 圖 27-3)
 - 按**【下載】**鈕，將目前搜尋到的記錄清單即時備份到本機電腦。(如圖 27-4)
 - 按下**【清除全部】**鈕，於顯示之刪除資料確認視窗中，按下**【確定】**鈕後，可將記錄即時由遠端 UTM、MHG 清除。(如圖 27-5)



圖 27-1 搜尋特定記錄

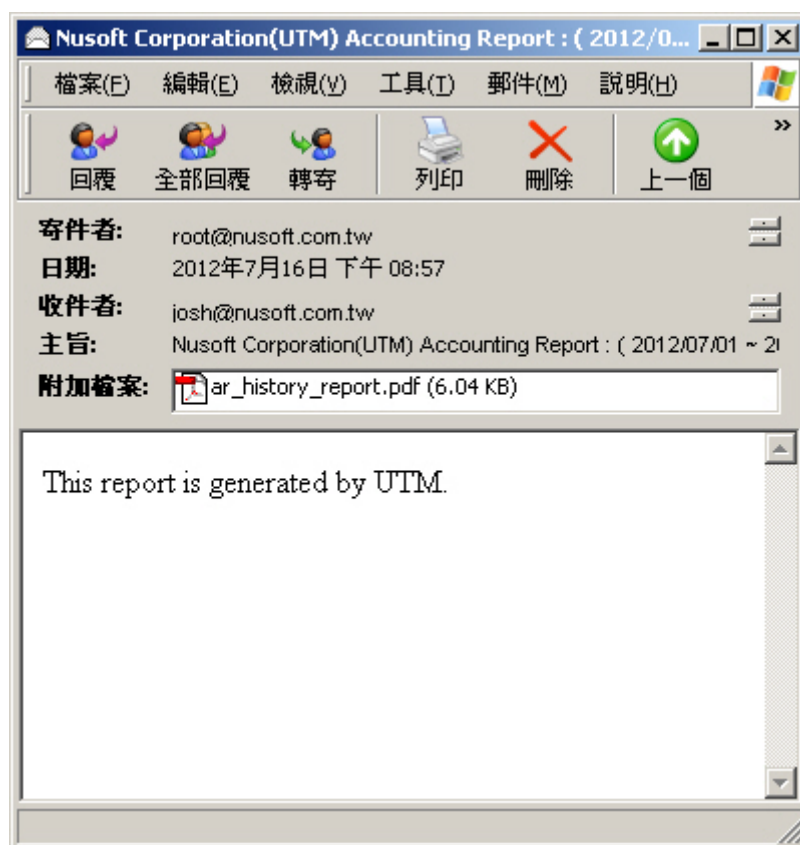


圖 27-2 收到搜尋報告信件

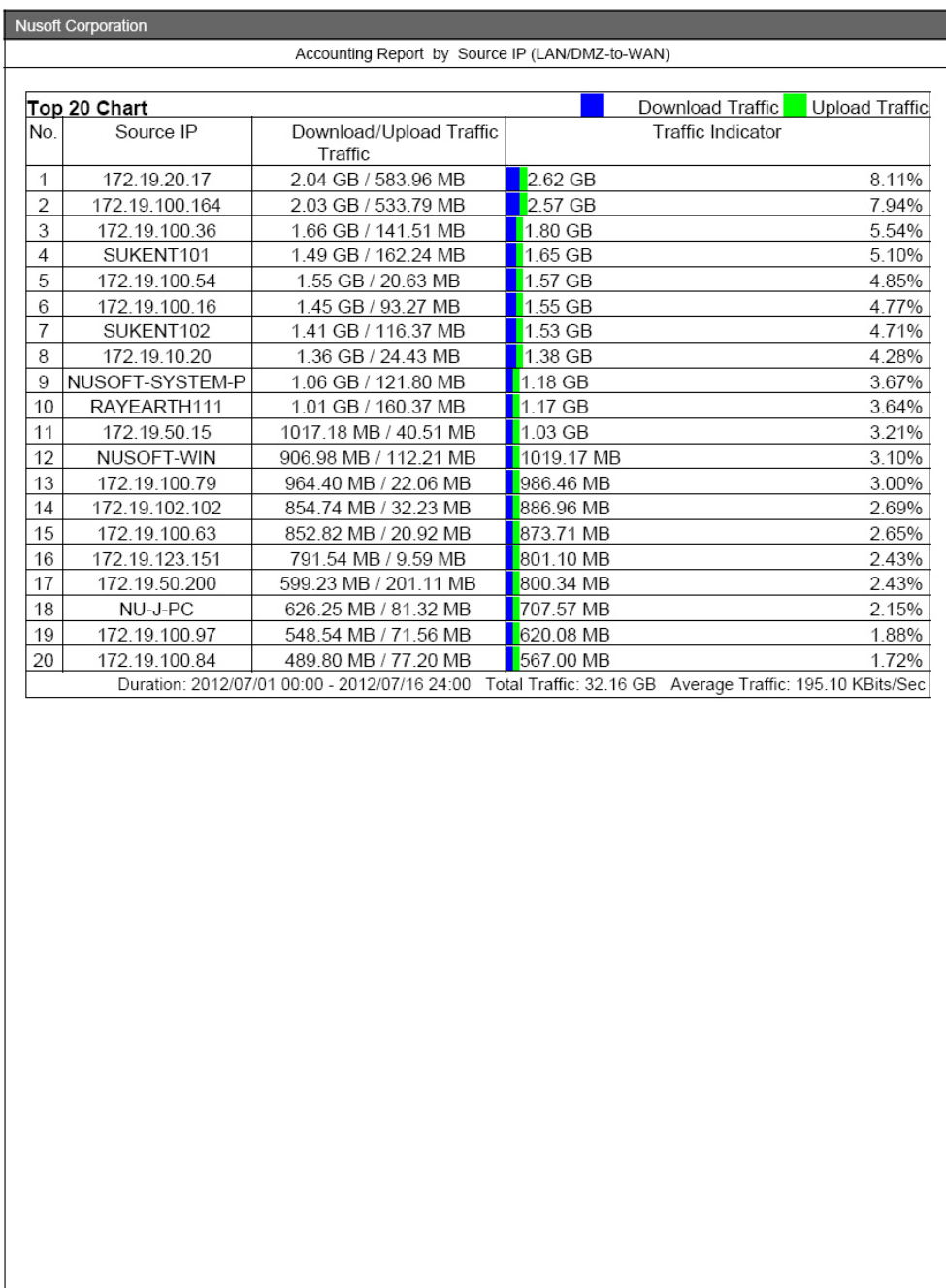


圖 27-3 流量排行搜尋報告內容



圖 27-4 下載搜尋的記錄



圖 27-5 清除歷史流量排行記錄

27.1 即時流量分析

步驟1. 在【遠端】>【即時監控】>【流量排行】>【即時流量分析】的指定【遠端裝置】頁面中，會顯示經遠端 UTM、MHG 進行傳輸的來源位址、網路服務之即時流量。（如圖 27-6）

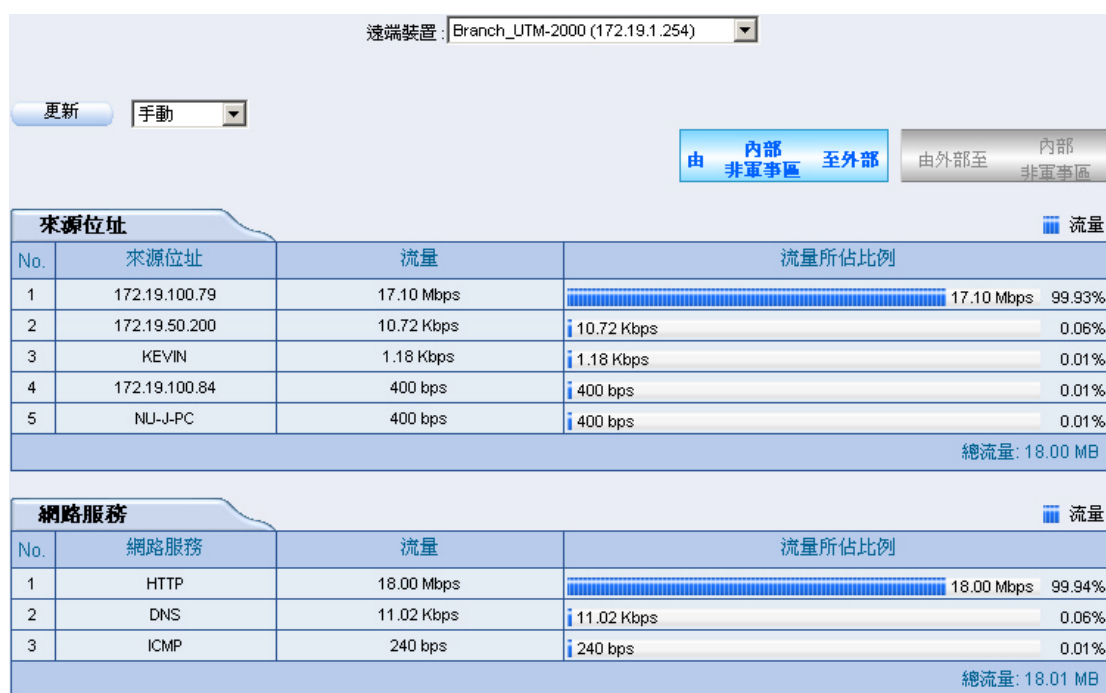


圖 27-6 即時流量排行榜

27.2 今日排行榜

步驟1. 在【遠端】>【即時監控】>【流量排行】>【今日排行榜】的指定【遠端裝置】頁面中，會顯示當天特定時段內，經遠端 UTM、MHG 進行傳輸的來源位址、目的位址、網路服務之累積流量。(如圖 27-7)

- 可使用滑鼠拖曳畫面上方的滑動鈕來設定統計時間，左邊滑動鈕為起始時間，右邊滑動鈕為終止時間。調整時間區間後，遠端 UTM、MHG 將會自動統計區間內的流量，來源位址、目的位址與網路服務排行榜也會隨著時間點改變而同步調整。(如圖 27-8)
- 在來源位址排行榜點擊【來源位址】連結，會跳出視窗顯示傳輸資料時，該來源位址連線的目的位址、透過的網路服務。(如圖 27-9)
- 在目的位址排行榜點擊【目的位址】連結，會跳出視窗顯示傳輸資料時，連線該目的位址的來源位址、透過的網路服務。(如圖 27-10)
- 在網路服務排行榜點擊【網路服務】連結，會跳出視窗顯示傳輸資料時，透過該網路服務連線的來源位址、目的位址。(如圖 27-11)

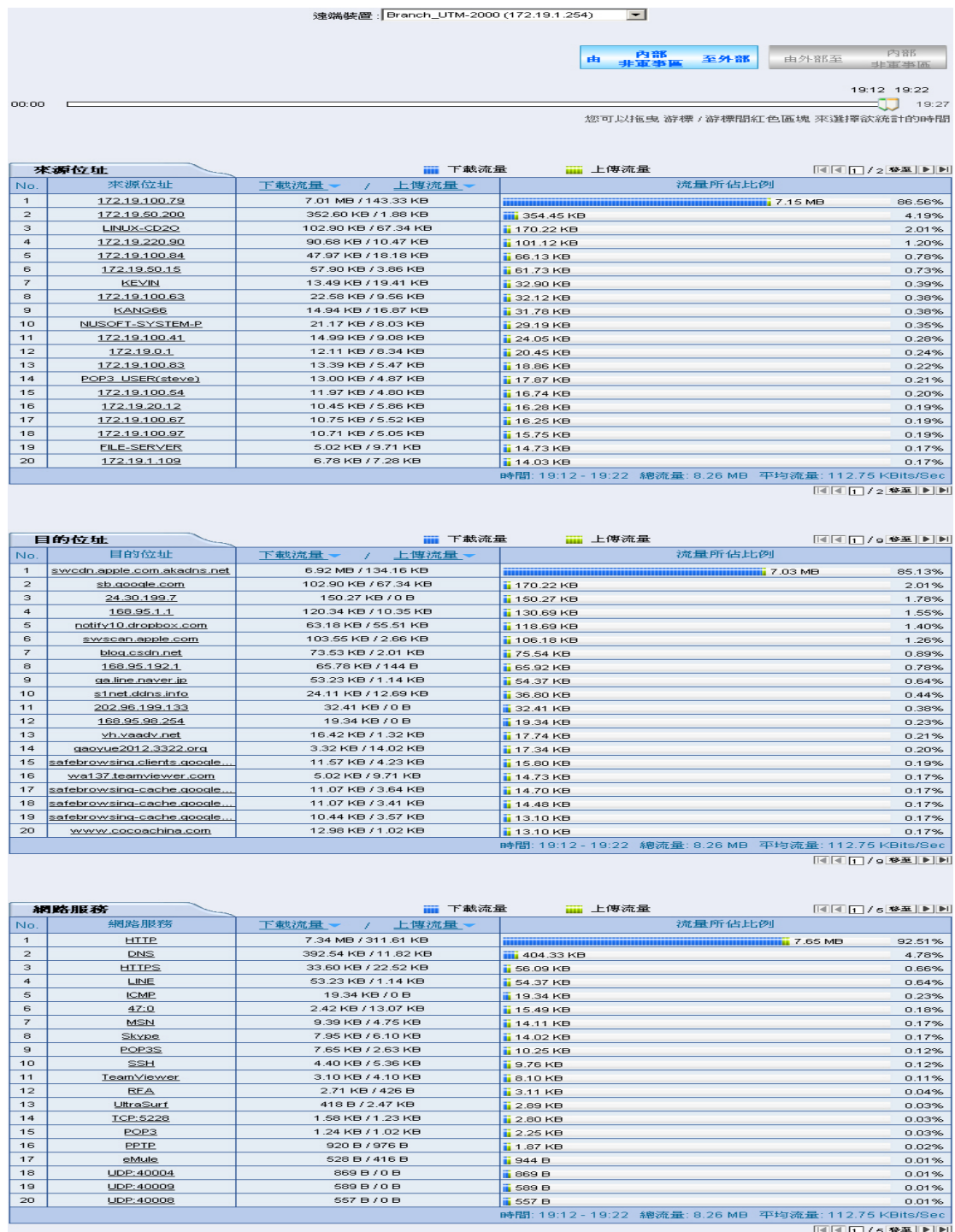


圖 27-7 今日排行榜

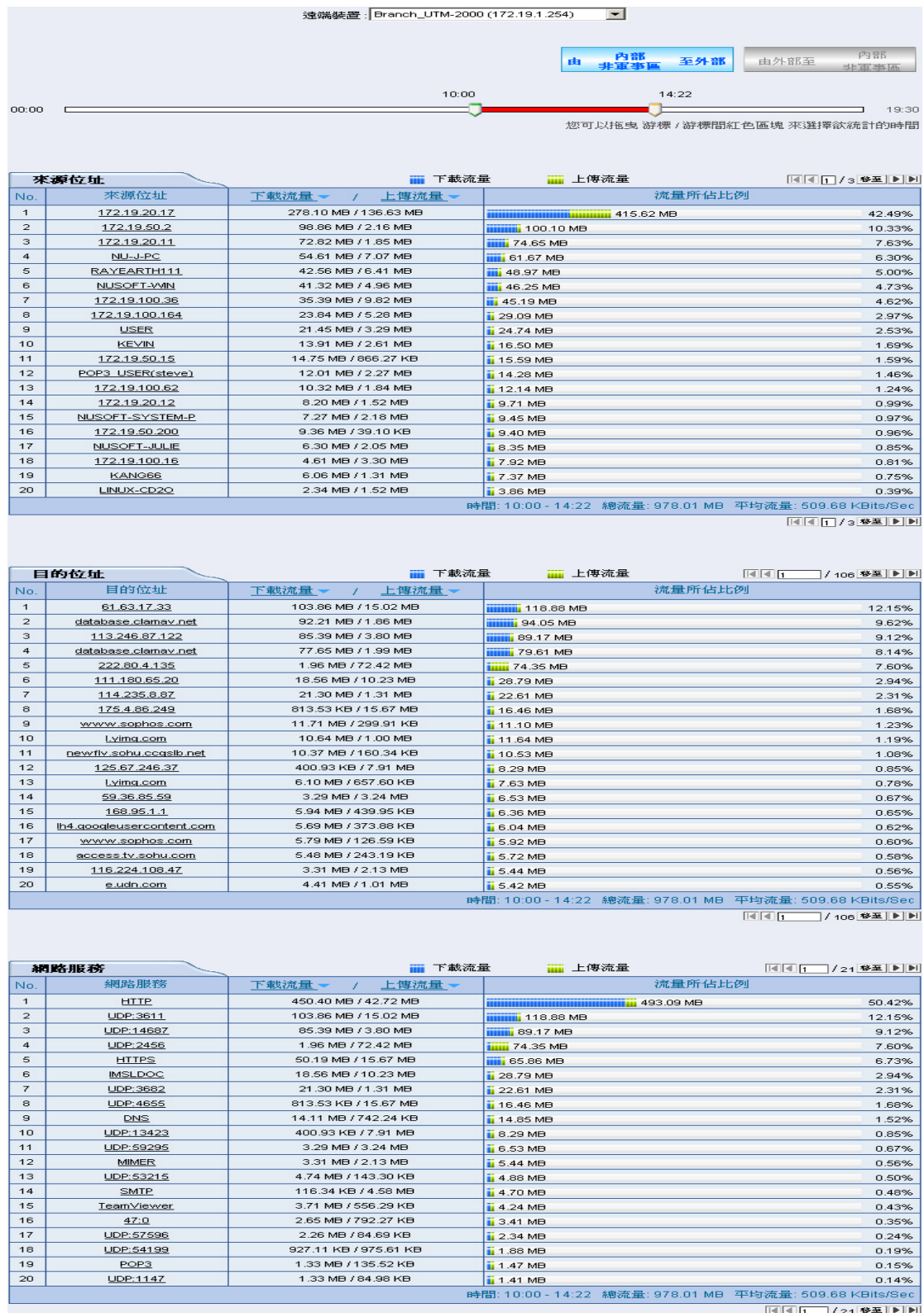


圖 27-8 指定時間區間的今日排行榜

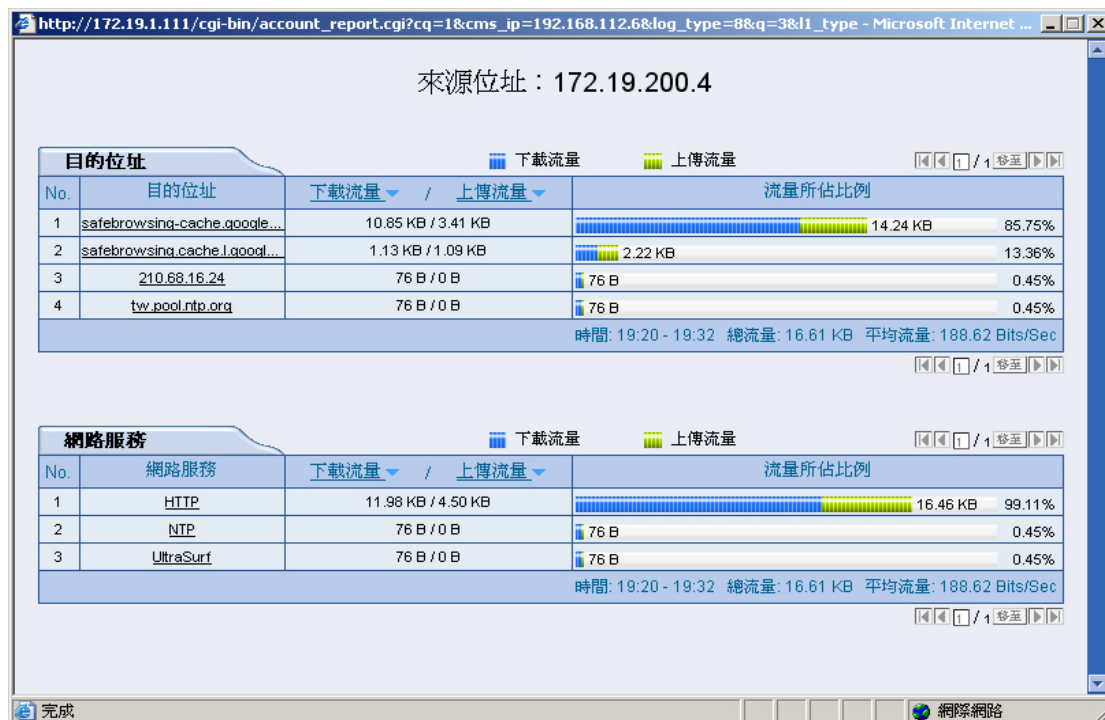


圖 27-9 傳送資料時來源位址連線的目的位址、透過的網路服務

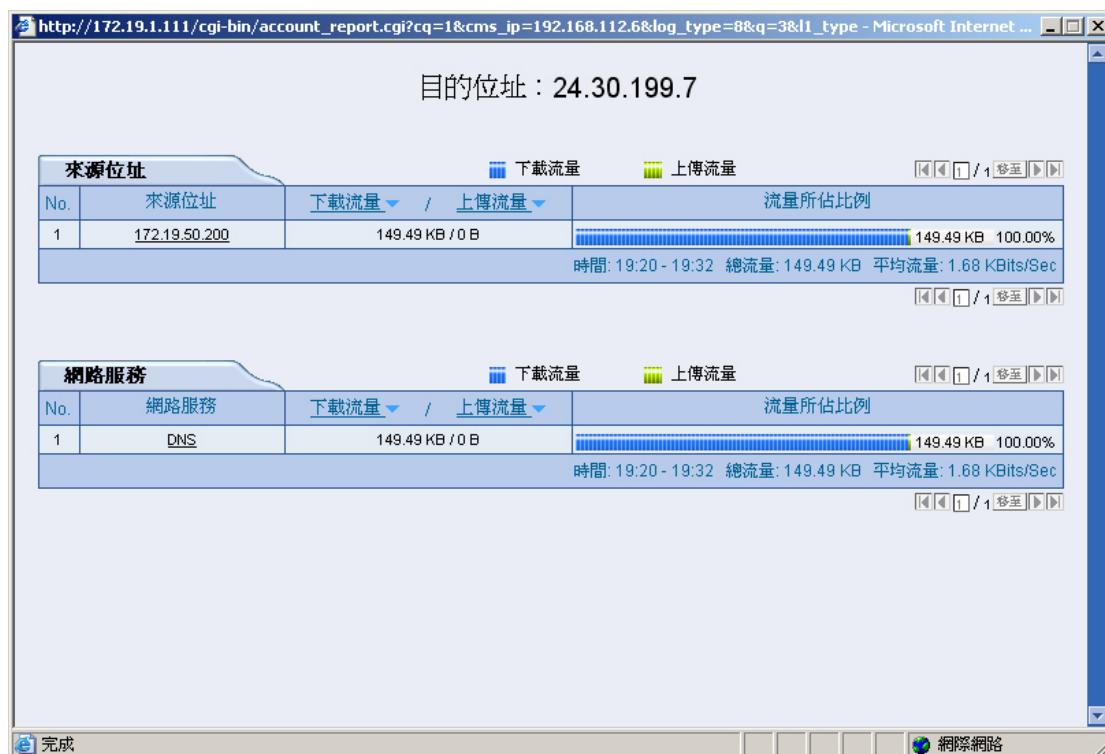


圖 27-10 傳送資料時連線目的位址的來源位址、透過的網路服務

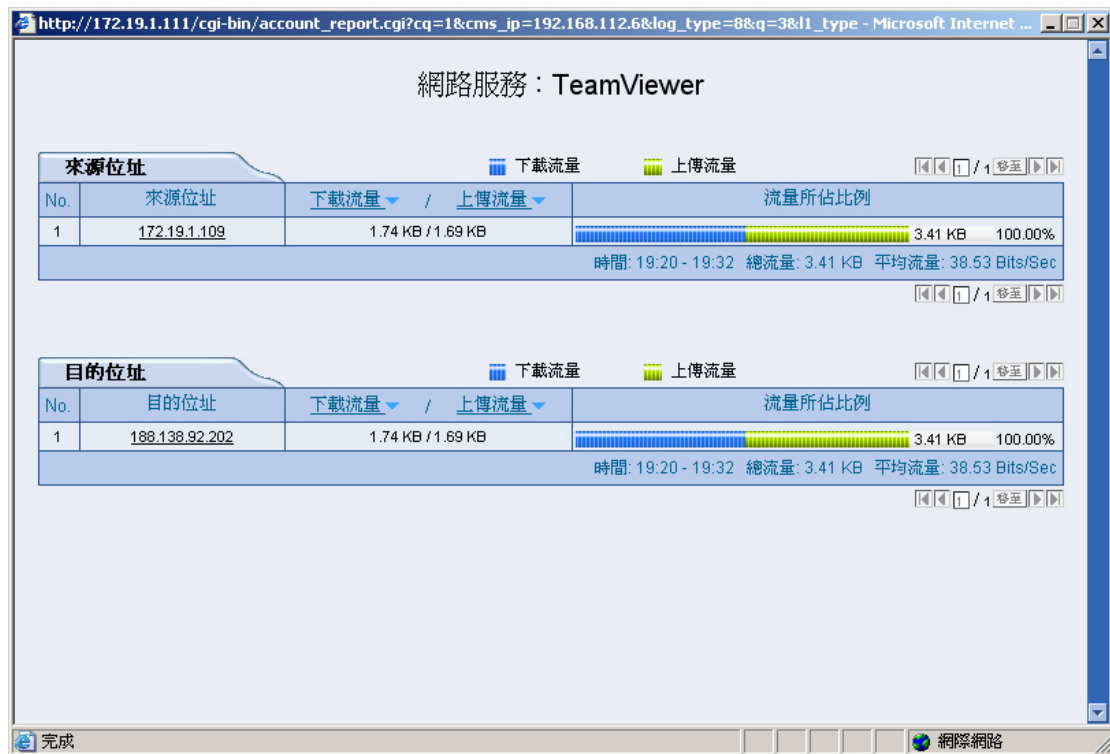


圖 27-11 傳送資料時透過特定網路服務連線的來源位址、目的位址

27.3 歷史排行榜

步驟1. 在【遠端】>【即時監控】>【流量排行】>【歷史排行榜】的指定【遠端裝置】頁面中，可顯示指定時間範圍內，經遠端 UTM、MHG 進行傳輸的日期、來源位址、目的位址、網路服務之累積流量。(如圖 27-12)

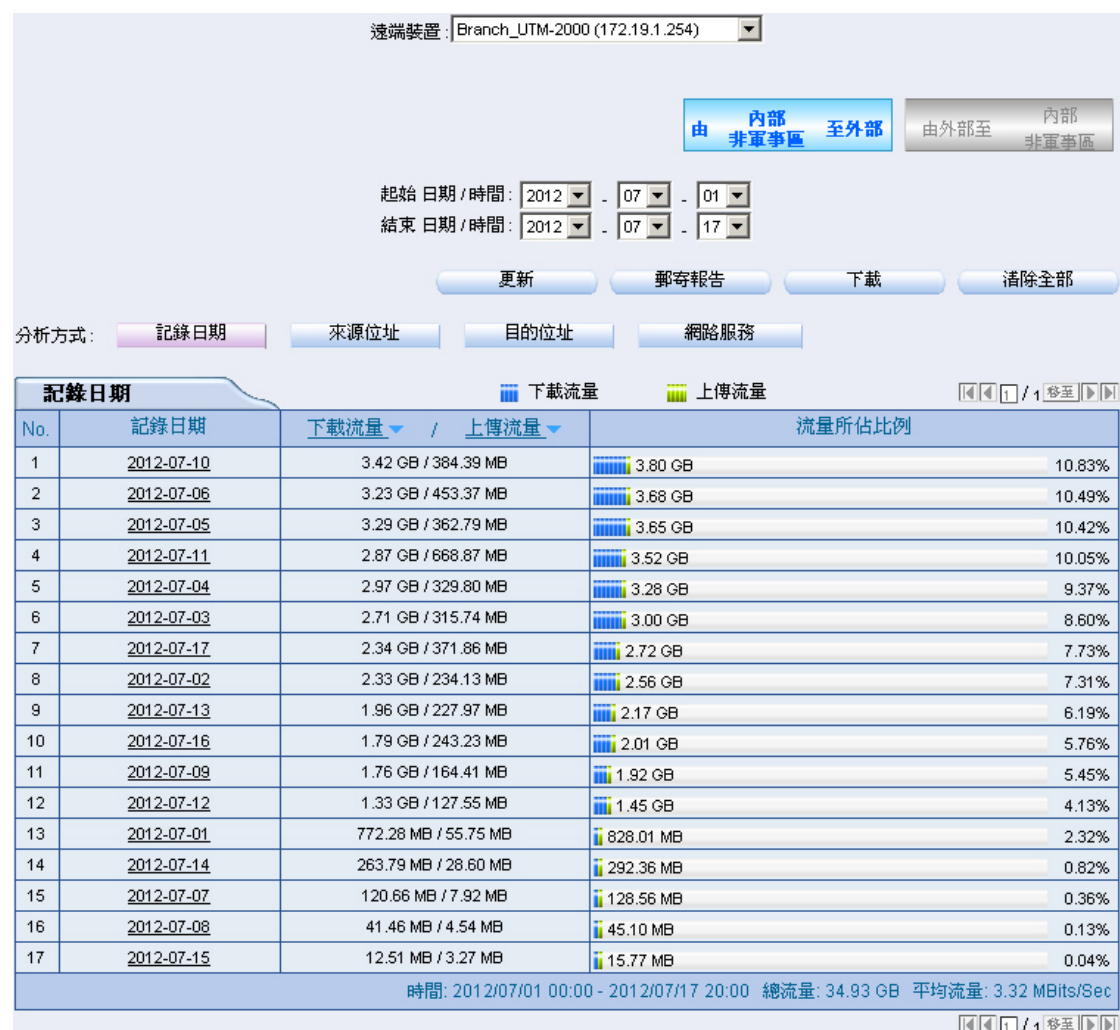


圖 27-12 歷史排行榜

第28章 流量圖表

用於統計遠端 UTM、MHG 外部網路介面或是所設定的管制條例之封包與資料傳輸流量，讓系統管理員了解網路流量狀況。

- **【外部網路】**：經過外部網路介面下載/上傳的資料量、接收/傳送的封包量統計資料。
- **【管制條例】**：經過管制條例下載/上傳的資料量、接收/傳送的封包量統計資料。

【流量圖表】功能概述：

流量統計圖表 說明如下：

- 縱座標：網路流量。
- 橫座標：時間。

管制條例方向 / 來源網路 / 目的網路 / 服務名稱 / 動作 說明如下：

- 條列進行流量統計的管制條例規則。

時間 說明如下：

- 可分別檢視以分、時、日、週、月、年為時間單位的流量統計。



說明：

1. 當檢視時間選擇為：

- 【分】：流量統計圖表會每分鐘更新一次。
 - 【時】：流量統計圖表會每小時更新一次。
 - 【日】：流量統計圖表會每日更新一次。
 - 【週】：流量統計圖表會每週更新一次。
 - 【月】：流量統計圖表會每月更新一次。
 - 【年】：流量統計圖表會每年更新一次。
-

Bits/sec Bytes/sec 使用率 累計（全部） 說明如下：

- 系統管理員可由此變換統計圖的流量計算標準。
 - ◆ Bits/sec：每秒鐘傳送的資料位元。
 - ◆ Bytes/sec：每秒鐘傳送的資料位元組。
 - ◆ 使用率：流量佔遠端 UTM、MHG 外部網路介面設定的最大下載/上傳頻寬之比例。
 - ◆ 累計（全部）：單位時間內所累加的資料傳輸量。

28.1 外部網路

步驟1. 在【遠端】>【即時監控】>【流量圖表】>【外部網路】的指定【遠端裝置】頁面中，找到欲檢視的外部網路介面名稱，對應至右方【時間單位】欄：（如圖 28-1, 圖 28-2）

- 點選【分】，可檢視以每分鐘（Minute）為單位的流量統計圖表。
- 點選【時】，可檢視以每小時（Hour）為單位的流量統計圖表。
- 點選【日】，可檢視以每日（Day）為單位的流量統計圖表。
- 點選【週】，可檢視以每週（Week）為單位的流量統計圖表。
- 點選【月】，可檢視以每月（Month）為單位的流量統計圖表。
- 點選【年】，可檢視以每年（Year）為單位的流量統計圖表。

遠端裝置: Branch_UTM-2000 (172.19.1.254)						
外部網路	時間單位					
WAN1	分	時	日	週	月	年
WAN2	分	時	日	週	月	年
WAN3	分	時	日	週	月	年
All WAN	分	時	日	週	月	年

圖 28-1 外部網路流量統計頁面

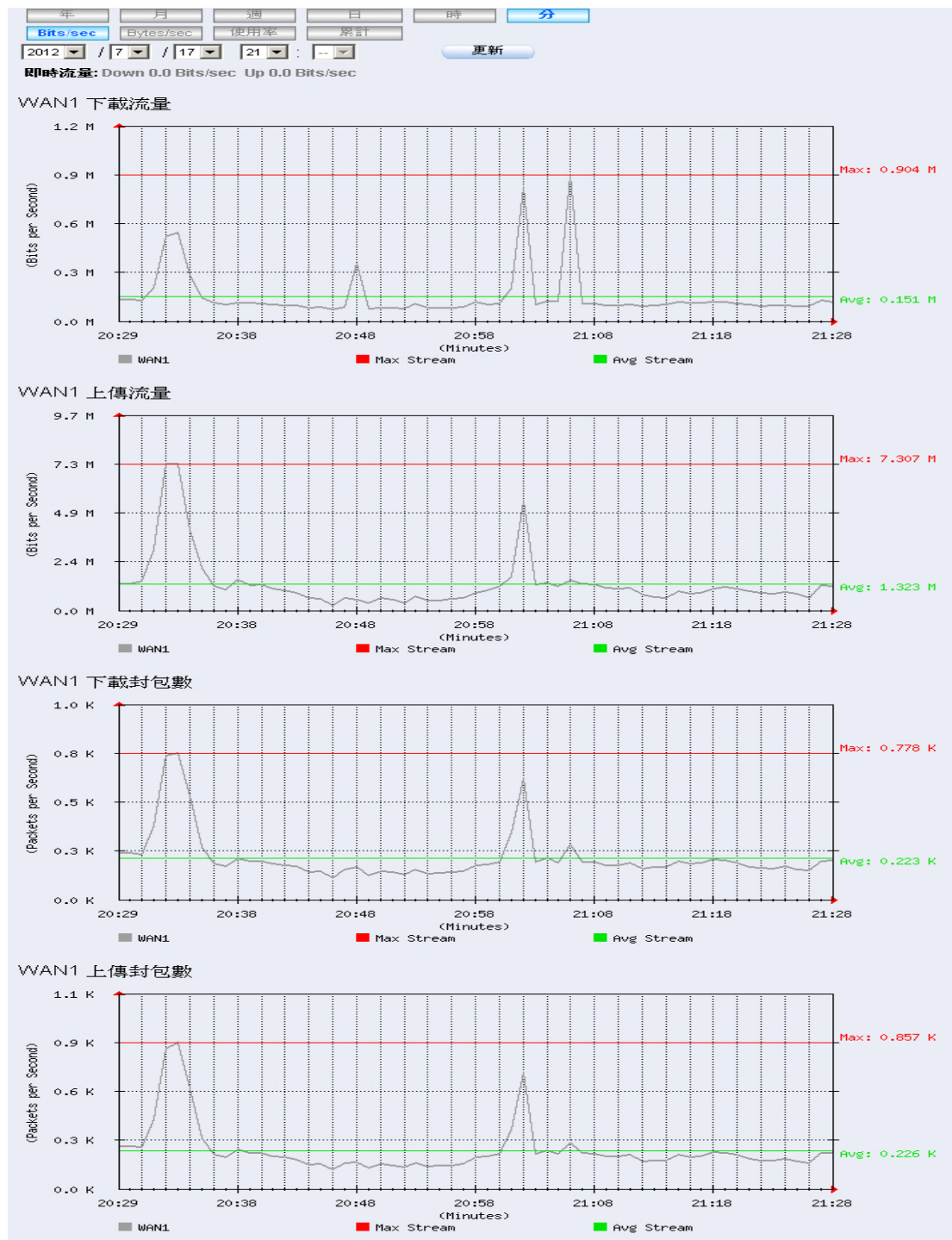


圖 28-2 外部網路流量統計圖



說明：

1. 當設定遠端 UTM、MHG【網路介面】>【介面位址】為外部網路介面時，其對應的外部網路流量統計機制也會隨之啟用。
2. 可檢視指定時間開始記錄的流量統計圖。

28.2 管制條例

步驟1. 當【管制條例】有開啓【流量圖表】功能時，在【遠端】>【即時監控】>【流量圖表】>【管制條例】的指定【遠端裝置】頁面中，找到欲檢視的管制條例，對應至右方【時間】欄：（如圖 28-3, 圖 28-4）

- 點選【分】，可檢視以每分鐘（Minute）為單位的流量統計圖表。
- 點選【時】，可檢視以每小時（Hour）為單位的流量統計圖表。
- 點選【日】，可檢視以每日（Day）為單位的流量統計圖表。
- 點選【週】，可檢視以每週（Week）為單位的流量統計圖表。
- 點選【月】，可檢視以每月（Month）為單位的流量統計圖表。
- 點選【年】，可檢視以每年（Year）為單位的流量統計圖表。

遠端裝置: Branch_UTM-2000 (172.19.1.254)

管制條例方向: 全部

管制條例方向	來源網路	目的網路	服務名稱	動作	時間
內部至外部	50.35	Outside Any	Any	✓	分時日週月年
內部至外部	steve	Outside Any	Any	1	分時日週月年
內部至外部	mailserver	Outside Any	DNS	2	分時日週月年
內部至外部	mailserver	Outside Any	Any	1	分時日週月年
內部至外部	Inside Any	Outside Any	Any	2	分時日週月年
外部至內部	Outside Any	[連接埠對應](22...	VoIP	✓	分時日週月年
外部至內部	Outside Any	[連接埠對應群組]...	mail server service...	✓	分時日週月年
外部至內部	Outside Any	[連接埠對應群組]...	HTTP, video_89, HT...	✓	分時日週月年
外部至內部	Outside Any	[連接埠對應](20...	BBB_service	✓	分時日週月年
外部至非軍事區	Outside Any	DATABASE_Server	HTTP	✓	分時日週月年
外部至非軍事區	Outside Any	DATABASE_Server	pushupdate	✓	分時日週月年
外部至非軍事區	Outside Any	[連接埠對應](22...	pushupdate	✓	分時日週月年
外部至非軍事區	Outside Any	[連接埠對應](22...	HTTP	✓	分時日週月年
外部至非軍事區	Outside Any	[連接埠對應](20...	HTTP	✓	分時日週月年
外部至非軍事區	Outside Any	WEBServer	HTTP	✓	分時日週月年
內部至非軍事區	Inside Any	DMZ Any	rsync	✓	分時日週月年
內部至非軍事區	Inside Any	DMZ Any	Any	✓	分時日週月年
非軍事區至外部	DMZ Any	Outside Any	Any	1	分時日週月年
非軍事區至外部	DMZ Any	Outside Any	Any	✓	分時日週月年
非軍事區至內部	DMZ Any	Inside Any	Any	✓	分時日週月年

圖 28-3 管制條例流量統計頁面

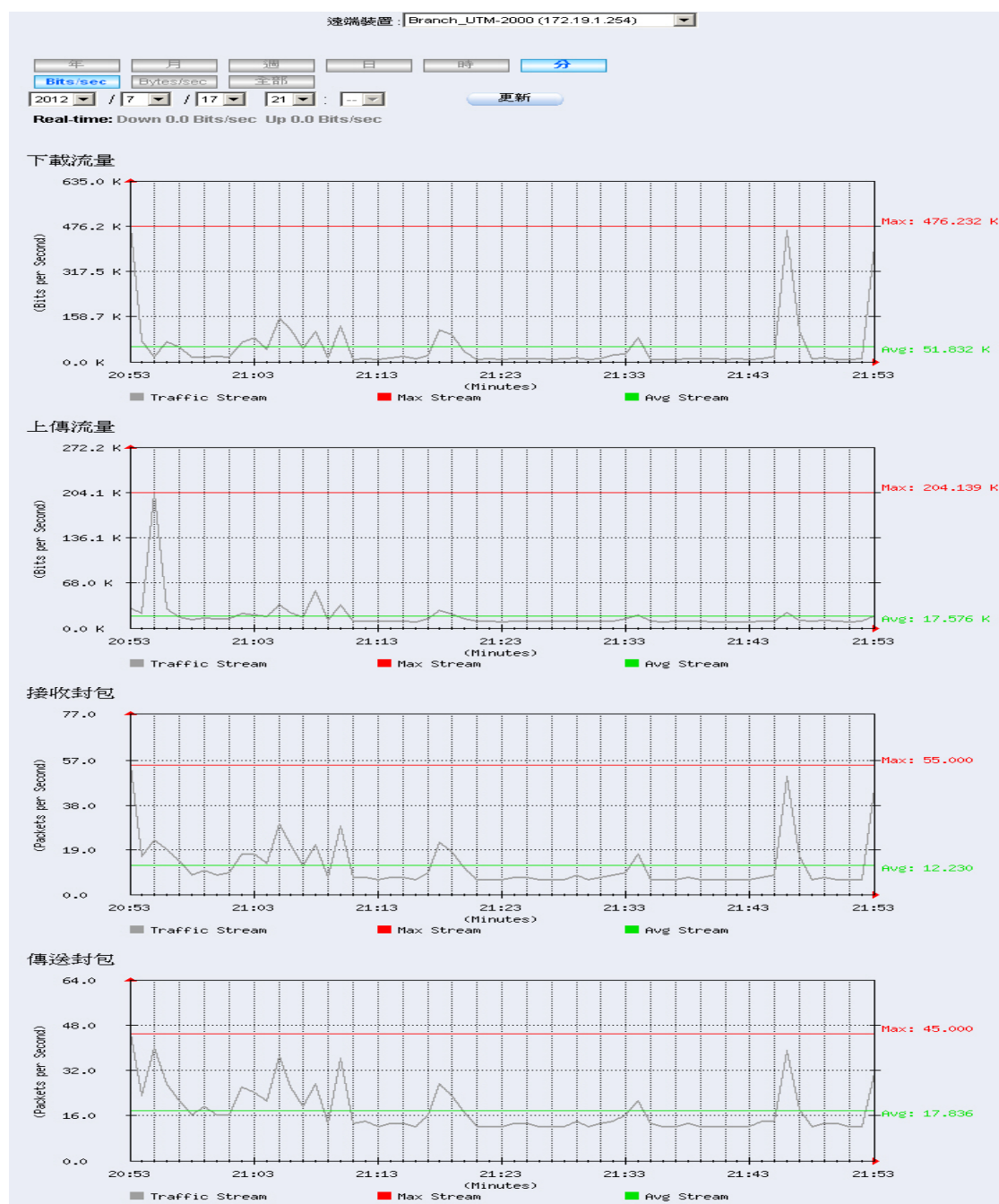


圖 28-4 管制條例流量統計圖



說明：

1. 若欲進行管制條例流量統計，系統管理員須於【管制條例】啟動【流量圖表】功能。
2. 管制條例流量統計的【管制條例方向】可分為：內部至外部、外部至內部、外部至非軍事區、內部至非軍事區、非軍事區至外部、非軍事區至內部、內部至內部、非軍事區至非軍事區。
3. 可檢視指定時間開始記錄的流量統計圖。

第29章 系統狀態

系統管理員可隨時得知遠端 UTM、MHG 的網路介面狀態、系統效能、認證狀態、ARP 表、連線狀態、DHCP 用戶表、主機資訊等各項資訊。

- **【介面狀態】**：顯示遠端 UTM、MHG 的所有網路介面狀態。
- **【系統效能】**：顯示遠端 UTM、MHG 的 CPU、硬碟以及記憶體的使用率。
- **【認證狀態】**：記錄遠端 UTM、MHG 之認證機制使用情況。
- **【ARP 表】**：記錄透過或與遠端 UTM、MHG 建立連線的設備之 IP、MAC 位址對應資訊。
- **【連線狀態】**：記錄目前所有透過遠端 UTM、MHG 管制條例傳輸封包的連線。
- **【DHCP 用戶表】**：記錄遠端 UTM、MHG 內建 DHCP 伺服器配發 IP 的狀況。
- **【主機資訊】**：記錄通過遠端 UTM、MHG 的連線 IP 和其對應 NetBIOS、DNS 名稱資訊。

【ARP 表】功能概述：

搜尋 說明如下：

- 可依照網際協定、目前 IP 位址、MAC 位址和介面等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
 - ◆ 在【遠端】>【即時監控】>【系統狀態】>【ARP 表】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：
 - 選擇指定【網際協定】、【介面】。
 - 按下【搜尋】鈕。（如圖 29-1）

遠端裝置: Branch_UTM-2000 (172.19.1.254)

搜尋 ARP 表

網際協定: IPv4
目前IP位址: (例如: 192.168.1.1)
MAC位址:
介面: WAN1

搜尋

結果

靜態 ☐

靜態 <input type="checkbox"/>	NetBIOS 名稱	目前IP位址 ▲	MAC位址 ▲	介面 ▲	變更
<input type="checkbox"/>	---	210.59.207.254	00:90:1a:3b:cf:fe	WAN1	刪除

確定

圖 29-1 搜尋特定記錄

【連線狀態】功能概述：

搜尋 說明如下：

- 可依照管制條例方向、排序、網際協定、來源位址、目的位址和埠號等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
 - ◆ 在【遠端】>【即時監控】>【系統狀態】>【連線狀態】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：
 - 選擇指定【管制條例方向】、【排序】、【網際協定】。
 - 按下【搜尋】鈕。（如圖 29-2）

遠端裝置: Branch_UTM-2000 (172.19.1.254)

搜尋 連線狀態

管制條例方向: 外部至內部
排序: 5
網際協定: IPv4
來源位址:
目的位址:
埠號: -> (範圍: 1 - 65535)

搜尋

結果

1 / 1 移至

<input type="checkbox"/>	網際協定 ▾	連線資料	起始時間 ▾	流量 ▾	管制條例方向
<input type="checkbox"/>	TCP	Original: 49.217.152.96:42667 -> download.nusoft.com.tw:291 Reply: 172.19.100.53:291 -> 49.217.152.96:42667	17:14:43	938.0 B	✓

1 / 1 移至

阻擋 ☒

圖 29-2 搜尋特定記錄

【DHCP 用戶表】功能概述：

搜尋 說明如下：

- 可依照網際協定、IP 位址和 MAC 位址等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。
 - ◆ 在【遠端】>【即時監控】>【系統狀態】>【DHCP 用戶表】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：
 - 選擇指定【網際協定】。
 - 按下【搜尋】鈕。（如圖 29-3）

遠端裝置: Branch_UTM-2000 (172.19.1.254)

搜尋 DHCP 用戶表

網際協定: IPv4
IP位址: (例如: 192.168.1.1)
MAC位址:

搜尋

結果

1 / 1 移至

NetBIOS 名稱	IP位址 ▲	MAC位址 ▲	租用時間	
			起始	結束
---	172.19.100.32	48:5b:39:c9:89:af	---	---
---	172.19.100.51	00:50:bf:13:11:86	---	---
NMXDSOOGRDJ	172.19.20.10	00:13:d4:8c:9f:9b	---	---
---	172.19.200.4	00:0c:76:b7:96:3b	2012/07/18 14:08:20	2012/07/19 02:08:20

1 / 1 移至

圖 29-3 搜尋特定記錄

【主機資訊】功能概述：

搜尋 說明如下：

- 可依照主機類型、IP 位址和名稱等關鍵字或特徵，來尋找儲存在遠端 UTM、MHG 所有符合條件之記錄。

◆ 在【遠端】>【即時監控】>【系統狀態】>【主機資訊】的指定【遠端裝置】>【搜尋】頁面中，做下列設定：

- 選擇指定【主機類型】。
- 按下【搜尋】鈕。（如圖 29-4）

遠端裝置: Branch_UTM-2000 (172.19.1.254)

搜尋 DNS

主機類型:

IP位址:

名稱:

搜尋

結果

DNS	全選	全部取消	刪除
<input type="checkbox"/> www.yahoo.com 106.10.170.118	<input type="checkbox"/> www.yahoo.com 87.248.112.181	<input type="checkbox"/> www.yahoo.com 87.248.122.122	<input type="checkbox"/> tw.yahoo.com 119.160.246.241
<input type="checkbox"/> static.ak.facebook.com 58.26.1.88	<input type="checkbox"/> static.ak.facebook.com 58.26.1.75	<input type="checkbox"/> static.ak.fbcdn.net 58.26.1.65	<input type="checkbox"/> static.ak.facebook.com 58.26.1.74
<input type="checkbox"/> static.ak.facebook.com 58.26.1.97	<input type="checkbox"/> profile.ak.fbcdn.net 117.104.139.50	<input type="checkbox"/> profile.ak.fbcdn.net 117.104.139.10	<input type="checkbox"/> fbcdn-sphotos- a.akamaihd.net
<input type="checkbox"/> profile.ak.fbcdn.net 117.104.139.57	<input type="checkbox"/> ga.line.naver.jp 119.235.235.91	<input type="checkbox"/> mystudy.dyndns.org 203.69.6.23	<input type="checkbox"/> s- static.ak.facebook.com
<input type="checkbox"/> api.twitter.com 199.59.150.9	<input type="checkbox"/> api.twitter.com 199.59.150.41	<input type="checkbox"/> search.twitter.com 199.59.149.243	<input type="checkbox"/> api.twitter.com 199.59.148.20
<input type="checkbox"/> search.twitter.com 199.59.148.11	<input type="checkbox"/> search.twitter.com 199.59.148.84	<input type="checkbox"/> webres1.nusoft.ctmail. 103.5.198.219	<input type="checkbox"/> search.twitter.com 199.59.150.10
<input type="checkbox"/> maps.google.com 173.194.72.101	<input type="checkbox"/> maps.google.com.tw 173.194.72.102	<input type="checkbox"/> maps.google.com 173.194.72.113	<input type="checkbox"/> stats.update.microsoft. 207.46.21.58
<input type="checkbox"/> plus.google.com 74.125.31.113	<input type="checkbox"/> plus.google.com 74.125.31.138	<input type="checkbox"/> plus.google.com 74.125.31.139	<input type="checkbox"/> maps.google.com 173.194.72.138
<input type="checkbox"/> localhost 127.0.0.1	<input type="checkbox"/> iou9527.no-ip.biz 118.160.254.66	<input type="checkbox"/> alias6.phx2-aud-mta- out2.cnet.com	<input type="checkbox"/> gg.google.com 74.125.31.101
<input type="checkbox"/> www.plurk.com 74.120.121.80	<input type="checkbox"/> www.plurk.com 74.120.121.83	<input type="checkbox"/> www.plurk.com 74.120.121.34	<input type="checkbox"/> c301.cloudmark.com 208.83.137.114
<input type="checkbox"/> s3.lockergnome.com 216.137.55.77	<input type="checkbox"/> d1ros97qkrwjf5.cloudfr 216.137.55.123	<input type="checkbox"/> d297h9he240fqh.cloud 216.137.55.150	<input type="checkbox"/> ourregularlyscheduledp 173.254.26.56
<input type="checkbox"/> tpdownload2.macrome 58.26.1.72	<input type="checkbox"/> content.yieldmanager.e 58.26.1.73	<input type="checkbox"/> twitter.com 199.59.150.7	<input type="checkbox"/> static.adzerk.net 216.137.55.82
<input type="checkbox"/> www.amazon.com 72.21.194.1	<input type="checkbox"/> www.apartments.com 74.119.98.50	<input type="checkbox"/> www.apartmenttherap 173.255.203.88	<input type="checkbox"/> twitter.com 199.59.148.82
<input type="checkbox"/> kona.kontera.com 58.26.1.42	<input type="checkbox"/> static.ak.facebook.com 58.26.1.83	<input type="checkbox"/> a0.twimg.com 184.169.75.33	<input type="checkbox"/> gazebosreview.16mb.c 31.170.164.109
<input type="checkbox"/> av.vimeo.com 58.26.1.91	<input type="checkbox"/> liveupdate.symanteclive 58.26.1.41	<input type="checkbox"/> www.etsy.com 96.16.234.37	<input type="checkbox"/> www.theweddingidea 70.38.11.59
<input type="checkbox"/> imagecdn.getprismatic. 216.137.55.243	<input type="checkbox"/> d297h9he240fqh.cloud 216.137.55.74	<input type="checkbox"/> imagecdn.getprismatic. 216.137.55.64	<input type="checkbox"/> static.ak.facebook.com 58.26.1.58
<input type="checkbox"/> suvendugiri.wordpress 72.233.2.58	<input type="checkbox"/> suvendugiri.wordpress 76.74.254.123	<input type="checkbox"/> suvendugiri.wordpress 74.200.243.251	<input type="checkbox"/> track.stetag.us 58.26.1.80
<input type="checkbox"/> nusoft.com.tw 210.59.207.105	<input type="checkbox"/> juststopscreaming.com 97.74.55.1	<input type="checkbox"/> code.jquery.com 72.21.91.19	<input type="checkbox"/> imagecdn.getprismatic. 216.137.55.118
<input type="checkbox"/> www.thesuburbanmor 50.23.234.64	<input type="checkbox"/> www.squidoo.com 64.225.155.21	<input type="checkbox"/> suvendugiri.wordpress 76.74.254.120	<input type="checkbox"/> suvendugiri.wordpress 74.200.244.59
<input type="checkbox"/> www.wikihow.com 173.203.142.18	<input type="checkbox"/> img1.etsystatic.com 124.40.41.47	<input type="checkbox"/> www.panasonic.ro 124.40.41.92	<input type="checkbox"/> login.wordpress.com 72.233.104.107
<input type="checkbox"/> www.florencefinds.co 79.170.44.81	<input type="checkbox"/> cdn.makezine.com 81.22.38.99	<input type="checkbox"/> s2.wp.com 68.232.44.111	<input type="checkbox"/> mrdavemartin.files.wor 72.233.104.107
<input type="checkbox"/> www.gravatar.com 68.232.44.219	<input type="checkbox"/> makezine.com 208.201.239.101	<input type="checkbox"/> makezine.com 208.201.239.100	<input type="checkbox"/> allapparel.biz 64.71.34.115
<input type="checkbox"/> cdn.stumble- upon.com	<input type="checkbox"/> cdn.api.twitter.com 118.215.191.144	<input type="checkbox"/> www.facebook.com 69.171.237.32	<input type="checkbox"/> dollarstorecrafts.com 108.162.197.57
<input type="checkbox"/> r.twimg.com 199.59.150.12	<input type="checkbox"/> stats.wordpress.com 74.200.247.59	<input type="checkbox"/> stats.wordpress.com 76.74.248.163	<input type="checkbox"/> p.typekit.net 117.18.237.119
<input type="checkbox"/> stats.wordpress.com 74.200.247.187	<input type="checkbox"/> static.parsely.com 216.137.55.148	<input type="checkbox"/> static.parsely.com 216.137.55.125	<input type="checkbox"/> makeprojects.com 75.101.159.182
			<input type="checkbox"/> r.twimg.com 199.59.148.89
			<input type="checkbox"/> stats.wordpress.com 216.151.210.122
			<input type="checkbox"/> d297h9he240fqh.cloud 216.137.55.178
			<input type="checkbox"/> 1.gravatar.com 68.232.44.121
			<input type="checkbox"/> www.makershed.com 69.49.188.152
			<input type="checkbox"/> stats.wordpress.com 72.233.111.159
			<input type="checkbox"/> d297h9he240fqh.cloud 216.137.55.201

圖 29-4 搜尋特定記錄

29.1 介面狀態

步驟1. 在【遠端】>【即時監控】>【系統狀態】>【介面狀態】的指定【遠端裝置】頁面中，會顯示目前遠端 UTM、MHG 各網路介面運作之相關訊息：（如圖 29-5）

遠端裝置: Branch_UTM-2000 (172.19.1.254)							
系統連線數目: 7617				系統開機歷時: 0 天 21 時 48 分 36 秒			
介面編號	1	2	3	4	5	6	7
介面定義	LAN1	WAN1	WAN2	WAN3	DMZ1	WAN4	DMZ2
模式	NAT	固定IP	撥號連線	撥號連線	透通路由模式	固定IP	透通橋接模式
外部網路連線狀態							
連線速率	1000Mb/s	100Mb/s	100Mb/s	100Mb/s	100Mb/s		
雙工模式	全雙工	全雙工	全雙工	全雙工	全雙工		
網路頻寬（上傳/下載）Kbps		4096 / 4096	10240 / 2048	4096 / 2048		204800 / 204800	
下載流量比例		90%	10%	0%			
上傳流量比例		98%	2%	0%			
連線歷時			4:01:27	21:46:27			
MAC位址	00:90:0B:14:B1:46	00:90:0B:14:B1:4B	00:90:0B:14:B1:4A	00:90:0B:14:B1:49	00:90:0B:14:B1:48	00:90:0B:14:B1:47	
IPv4位址	172.19.1.254	59.124.36.162	114.32.109.246	114.37.82.95		172.39.1.1	
子網路遮罩	255.255.0.0	255.255.255.240	255.255.255.255	255.255.255.255		255.255.0.0	
IPv4預設閘道		59.124.36.161	168.95.98.254	168.95.98.254		172.39.1.254	
IPv6位址	2001:0DB8:0:F101::1	2001:0DB8:1FF:F101::2					
首碼長度	64	64					
IPv6預設閘道		2001:0DB8:1FF:F101::1					
DNS伺服器 1		168.95.1.1	168.95.1.1	168.95.1.1		168.95.1.1	
DNS伺服器 2		168.95.192.1	168.95.192.1	168.95.192.1		168.95.192.1	
接收封包數（成功 / 錯誤）	3011470,0	22209204,0	2636762,0	84527,0	17517723,0	0,0	0,0
傳送封包數（成功 / 錯誤）	3470591,0	21343726,0	2056879,0	72681,0	18370979,0	0,0	0,0
Ping	✓	✓	✓	✓	✓	✓	✗
HTTP	✓	✓	✓	✓	✓	✓	✗
HTTPS	✓	✓	✓	✓	✓	✓	✗
Telnet	✓	✗	✗	✗	✗	✗	✗
SSH	✗	✗	✗	✗	✗	✗	✗

圖 29-5 介面狀態



說明：

1. 【系統開機歷時】：遠端 UTM、MHG 開機歷時。
2. 【系統連線數目】：顯示目前通過遠端 UTM、MHG 建立的連線數。
3. 【模式】：為該網路介面的連線模式。
4. 【外部網路連線狀態】：顯示該外部網路介面的連線狀態。
5. 【網路頻寬（上傳/下載）Kbps】：顯示該外部網路介面所能使用的最大下載 / 上傳頻寬（為系統管理員在遠端 UTM、MHG【網路介面】>【介面位址】頁面中，設定的外部網

路介面頻寬)。

6. **【下載流量比例】**：遠端 UTM、MHG 依照各外部網路介面的流量，所分配的下載比例。
 7. **【上傳流量比例】**：遠端 UTM、MHG 依照各外部網路介面的流量，所分配的上傳比例。
 8. **【連線歷時】**：當外部網路介面的連線模式為撥號連線 / 動態 IP 位址時，會於此欄位顯示其連線歷時。
 9. **【MAC 位址】**：該網路介面之 MAC Address。
 10. **【IPv4 位址 / 子網路遮罩】**：為該網路介面之 IPv4 位址與網路遮罩設定。
 11. **【IPv4 預設閘道】**：顯示該外部網路介面之 IPv4 通訊閘道位址。
 12. **【IPv6 位址 / 首碼長度】**：為該網路介面之 IPv6 位址與首碼長度設定。
 13. **【IPv6 預設閘道】**：顯示該外部網路介面之 IPv6 通訊閘道位址。
 14. **【DNS 伺服器 1】**：外部網路介面可用來解析網域名稱的主要 DNS 伺服器。
 15. **【DNS 伺服器 2】**：外部網路介面可用來解析網域名稱的次要 DNS 伺服器。
 16. **【接收封包數 (成功/錯誤)】**：顯示該介面所接收之正常、錯誤封包數。
 17. **【傳送封包數 (成功/錯誤)】**：顯示該介面所傳送之正常、錯誤封包數。
 18. **【Ping/Tracert / HTTP / HTTPS / Telnet / SSH】**：顯示使用者能否從該網路介面 Ping/Tracert 到遠端 UTM、MHG；或是透過 HTTP、HTTPS、Telnet、SSH 協定登入其 UI。
-

29.2 系統效能

步驟1. 在【遠端】>【即時監控】>【系統狀態】>【系統效能】的指定【遠端裝置】頁面中，可顯示目前或指定日期的遠端 UTM、MHG 系統 CPU、硬碟、記憶體使用狀況之相關訊息：(如圖 29-6)



圖 29-6 系統資源使用狀態

29.3 認證狀態

步驟1. 在【遠端】>【即時監控】>【系統狀態】>【認證狀態】的指定【遠端裝置】頁面中，會顯示目前遠端 UTM、MHG 認證機制之相關訊息：(如圖 29-7)

遠端裝置: Branch_UTM-2000 (172.19.1.254)

IP位址	認證名稱 ▲	登入時間 ▲	變更
172.19.100.85	POP3_USER(steve)	2012/07/04 12:31:32	刪除

圖 29-7 認證狀態



說明：

1. 【IP 位址】：認證使用者 IP 位址。
2. 【認證名稱】：認證使用者採用的認證帳號。
3. 【登入時間】：使用者進行認證的起始時間。(年/月/日 時/分/秒)。

29.4 ARP表

步驟1. 在【遠端】>【即時監控】>【系統狀態】>【ARP 表】的指定【遠端裝置】頁面中，可顯示在 IPv4、IPv6 網際協定下，目前透過或與遠端 UTM、MHG 建立連線之設備的 NetBIOS 名稱、IP 位址、MAC 位址和所屬網路介面之相關訊息：（如圖 29-8）

遠端裝置: Branch_UTM-2000 (172.19.1.254)

ARP防偽程式（防範“ARP病毒/欺騙/攻擊”專用） [下載](#) [說明](#)

網際協定: IPv4

靜態 ☐

靜態 <input type="checkbox"/>	NetBIOS 名稱	目前IP位址 ▲	MAC位址 ▲	介面 ▲	變更
<input type="checkbox"/>	---	210.59.207.106	00:0c:76:b7:97:7e	DMZ1	刪除
<input type="checkbox"/>	---	210.59.207.104	00:0e:2e:56:b9:92	DMZ1	刪除
<input type="checkbox"/>	---	172.19.50.11	00:1d:60:28:82:f5	LAN1	刪除
<input type="checkbox"/>	---	172.19.20.17	00:1d:92:40:74:c8	LAN1	刪除
<input type="checkbox"/>	---	172.19.100.16	48:5b:39:c9:89:b3	LAN1	刪除
<input type="checkbox"/>	WWW	172.19.1.66	20:cf:30:93:c2:e6	LAN1	刪除
<input type="checkbox"/>	---	172.19.100.36	00:1d:92:40:78:ad	LAN1	刪除
<input type="checkbox"/>	---	172.19.100.25	48:5b:39:c9:85:25	LAN1	刪除
<input type="checkbox"/>	---	172.19.50.200	00:60:e0:4f:10:5c	LAN1	刪除
<input type="checkbox"/>	KANG66	172.19.100.66	54:04:a6:57:48:ea	LAN1	刪除
<input type="checkbox"/>	NUSOFT-M2K	172.19.123.41	00:18:f3:4b:20:90	LAN1	刪除
<input type="checkbox"/>	NUSOFT-JULIE	172.19.20.19	20:cf:30:93:c1:d8	LAN1	刪除
<input type="checkbox"/>	ADFIN05	172.19.20.5	00:13:d4:8c:ca:1f	LAN1	刪除
<input type="checkbox"/>	---	172.19.220.90	00:0c:29:a1:47:a1	LAN1	刪除
<input type="checkbox"/>	---	172.19.100.41	00:40:f4:49:29:15	LAN1	刪除
<input type="checkbox"/>	USER	172.19.20.13	20:cf:30:93:c2:f4	LAN1	刪除
<input type="checkbox"/>	---	172.19.100.21	bc:ae:c5:18:ea:d6	LAN1	刪除
<input type="checkbox"/>	---	172.19.1.101	00:0c:29:73:56:2a	LAN1	刪除
<input type="checkbox"/>	---	172.19.1.111	00:0c:29:a3:c7:b8	LAN1	刪除
<input type="checkbox"/>	NUSOFT-SYSTEM-P	172.19.100.47	bc:ae:c5:55:19:a5	LAN1	刪除

新增 確定

圖 29-8 ARP 表



說明：

1. 【NetBIOS 名稱】：該設備之網路識別名稱。
2. 【目前 IP 位址】：該設備之網路 IP 位址。
3. 【MAC 位址】：該設備之網路卡識別號碼。
4. 【介面】：該設備所屬網路介面。
5. 遠端 UTM、MHG【靜態】ARP 表功能和提供的【ARP 防偽程式】，必須同時搭配使用，可分別綁定遠端 UTM、MHG 和用戶端彼此的 IP 及 MAC 位址對應，避免內部代回封包導致的網路異常情形。

29.5 連線狀態

步驟1. 在【遠端】>【即時監控】>【系統狀態】>【連線狀態】的指定【遠端裝置】頁面中，可顯示在 IPv4、IPv6 網際協定下，目前透過遠端 UTM、MHG 管制條例傳輸封包的連線：（如圖 29-9）

- 點選【來源位址】連結，可顯示其存取網路資源時，透過之埠號和所使用之流量。（如圖 29-10）

遠端裝置: Branch_UTM-2000 (172.19.1.254)

網際協定: IPv4

來源位址	持續時間	總流量	連線數
172.19.50.200	00:03:00	57.1 KB	229
RAYEARTH111	11:38:22	2.4 MB	78
NUSOFT-M2K	04:31:06	72.8 KB	40
KEVIN	00:34:16	152.9 KB	34
172.19.100.36	09:25:39	1.2 MB	20
60.54.248.162	00:01:19	18.2 KB	16
175.139.238.120	00:01:40	12.9 KB	11
NU-J-PC	09:21:34	914.7 KB	11
59.125.65.213	06:26:12	11.7 KB	10
111.249.195.93	09:02:08	283.2 MB	10
MYCHAT-9AD55F6A	00:00:28	148.2 KB	10
61.244.239.61	00:01:26	9.8 KB	9
218.16.57.183	00:01:15	9.8 KB	9
111.249.207.148	00:01:21	10.1 KB	9
163.24.77.115	00:01:19	9.9 KB	9
61.64.143.95	06:26:36	10.0 KB	9
60.249.96.162	00:01:21	10.3 KB	9
220.133.122.33	00:01:16	10.3 KB	9
122.116.117.12	00:01:17	10.2 KB	9
212.202.229.64	00:01:28	10.2 KB	9

圖 29-9 系統連線狀態

遠端裝置: Branch_UTM-2000 (172.19.1.254)

1 / 12 移至

<input type="checkbox"/> 網際協定	連線資料	起始時間	流量	管制條例方向
<input type="checkbox"/> UDP	Original: 172.19.50.200:51164 -> 66.134.75.238:53 Reply: 66.134.75.238:53 -> nusoft.com.tw:51164	18:46:26	58.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:59576 -> 168.95.1.1:53 Reply: 168.95.1.1:53 -> nusoft.com.tw:59576	18:46:25	292.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:59576 -> 202.96.199.133:53 Reply: 202.96.199.133:53 -> nusoft.com.tw:59576	18:46:25	116.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:59576 -> 202.136.254.1:53 Reply: 202.136.254.1:53 -> nusoft.com.tw:59576	18:46:25	58.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:59576 -> 66.134.75.238:53 Reply: 66.134.75.238:53 -> nusoft.com.tw:59576	18:46:25	58.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:59576 -> 24.30.199.7:53 Reply: 24.30.199.7:53 -> nusoft.com.tw:59576	18:46:25	327.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:59576 -> 168.95.192.1:53 Reply: 168.95.192.1:53 -> nusoft.com.tw:59576	18:46:25	175.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:59576 -> 202.106.127.1:53 Reply: 202.106.127.1:53 -> nusoft.com.tw:59576	18:46:25	58.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:39166 -> 168.95.1.1:53 Reply: 168.95.1.1:53 -> nusoft.com.tw:39166	18:46:24	292.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:39166 -> 202.96.199.133:53 Reply: 202.96.199.133:53 -> nusoft.com.tw:39166	18:46:24	116.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:39166 -> 202.106.127.1:53 Reply: 202.106.127.1:53 -> nusoft.com.tw:39166	18:46:24	58.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:39166 -> 168.95.192.1:53 Reply: 168.95.192.1:53 -> nusoft.com.tw:39166	18:46:24	175.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:39166 -> 202.136.254.1:53 Reply: 202.136.254.1:53 -> nusoft.com.tw:39166	18:46:24	58.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:39166 -> 66.134.75.238:53 Reply: 66.134.75.238:53 -> nusoft.com.tw:39166	18:46:24	58.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:39166 -> 24.30.199.7:53 Reply: 24.30.199.7:53 -> nusoft.com.tw:39166	18:46:24	327.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:57486 -> 168.95.1.1:53 Reply: 168.95.1.1:53 -> nusoft.com.tw:57486	18:46:23	292.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:57486 -> 202.136.254.1:53 Reply: 202.136.254.1:53 -> nusoft.com.tw:57486	18:46:23	58.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:57486 -> 66.134.75.238:53 Reply: 66.134.75.238:53 -> nusoft.com.tw:57486	18:46:23	58.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:57486 -> 202.96.199.133:53 Reply: 202.96.199.133:53 -> nusoft.com.tw:57486	18:46:23	116.0 B	2
<input type="checkbox"/> UDP	Original: 172.19.50.200:57486 -> 168.95.192.1:53 Reply: 168.95.192.1:53 -> nusoft.com.tw:57486	18:46:23	175.0 B	2

1 / 12 移至

阻擋 ☒

圖 29-10 系統連線過濾頁面

29.6 DHCP用戶表

步驟1. 在【遠端】>【即時監控】>【系統狀態】>【DHCP 用戶表】的指定【與端裝置】頁面中，記錄在 IPv4、IPv6 網際協定下，遠端 UTM、MHG 內建的 DHCP 伺服器配發 IP 之情況：（如圖 29-11）

遠端裝置: Branch_UTM-2000 (172.19.1.254)

網際協定: IPv4

NetBIOS 名稱	IP位址 ▲	MAC位址 ▲	租用時間	
			起始	結束
---	172.19.100.32	48:5b:39:c9:89:af	---	---
---	172.19.100.51	00:50:bf:13:11:86	---	---
NMXDSOOGRDJ	172.19.20.10	00:13:d4:8c:9f:9b	---	---
---	172.19.200.4	00:0c:76:b7:96:3b	2012/07/18 14:08:20	2012/07/19 02:08:20

圖 29-11 DHCP 用戶表



說明：

1. 【NetBIOS 名稱】：接受遠端 UTM、MHG 配發 IP 的設備之網路識別名稱。
2. 【IP 位址】：遠端 UTM、MHG 所配發給該設備之動態 IP 位址。
3. 【MAC 位址】：該動態 IP 位址所對應之 MAC 位址。
4. 【租用時間】：該動態 IP 位址之有效時間(起始 / 結束時間)（年/月/日/時/分/秒）。

29.7 主機資訊

步驟1. 在【遠端】>【即時監控】>【系統狀態】>【主機資訊】的指定【遠端裝置】頁面中，可顯示在 IPv4 網際協定下，通過遠端 UTM、MHG 的連線 IP 位址和其對應 NetBIOS、DNS 名稱資訊。(如圖 29-12, 圖 29-13)

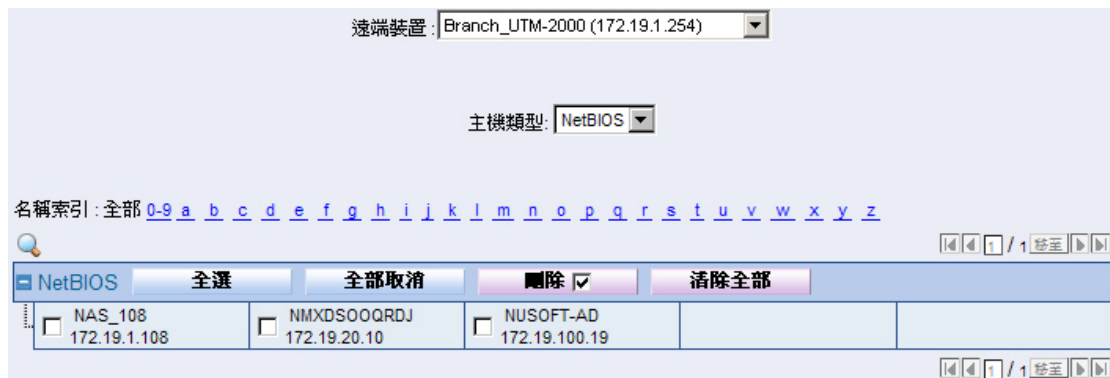


圖 29-12 NetBIOS 主機列表

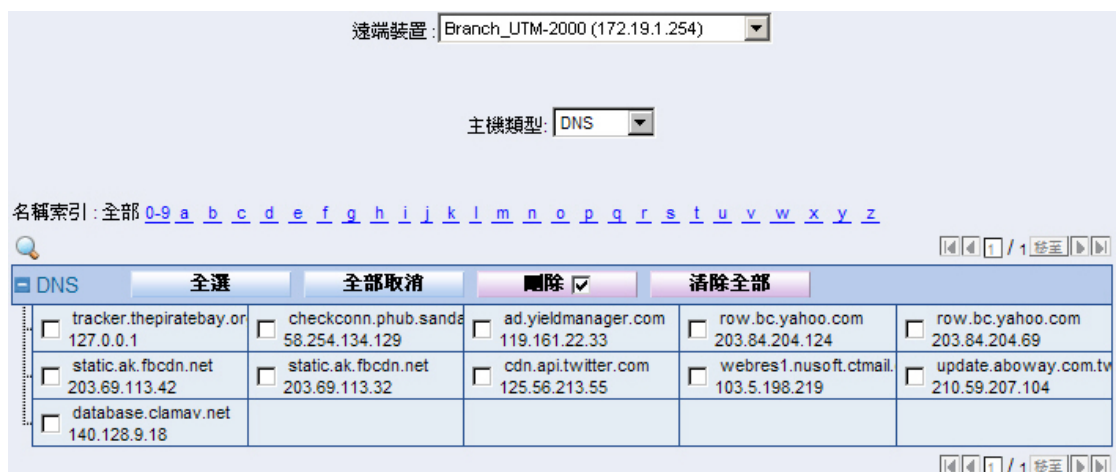


圖 29-13 DNS 主機列表