

InstantScan Content Manager

InstantScan 使用手冊

利基網路股份有限公司 Secure Networks at Layer-7

V3.1.11 (2009/12/14)

第1部	產品簡介	2
第1章	產品簡介	3
1.1	產品包裝檢查	3
1.2	硬體安裝	3
1.3	將設備連上網路	4
1.4	系統預設值 vs 範例設定	4
第2章	管理系統介紹	6
2.1	設備 技術應用	6
2.2	內容管理流程	8
2.3	設備網頁介面設計原則	9
2.4	設備圖示說明	9
2.5	工具列說明1	0
2.6	管理伺服器版本1	0
第2部	基本設定1	2
第3章	管理伺服器安裝1	3
3.1	管理伺服器軟體安裝1	3
	3.1.1 管理伺服器系統需求1	3
	3.1.2 軟體安裝程式1	4
	3.1.3 用戶端安裝	4
3.2	設定設備1	4
	3.2.1 啟動系統	5
	3.2.2 系統架構1	5
	3.2.3 系統參數設定1	5
	3.2.4 設備 網頁介面設定1	7
	新增項目1	9
	删除項目2	2
	開啟已存在的項目	3
第4章	網頁登入驗證	5
4.1	驗證的種類2	5

4.2		設定驗證類型	25
	4.2.1	Pop3(s)設定	26
	4.2.2	Imap(s)設定	27
	4.2.3	Radius 設定	28
	4.2.4	LDAP 設定	28
第5章	結合	Web Login 設定 L4/L7/Content 策略	31
5.1		需求	31
5.2		方法	31
5.3		步驟	31
	5.3.1	所有的成員都必須進行上網認證並且間隔每 8 小時就要進行一次認證 · boss 不需要認證	31
	5.3.2	讓策略規則能以 Web 認證用戶名作過濾	34
第6章	結合。	AD 設定 L4/L7/Content 策略	38
6.1		需求	38
6.2		方法	38
6.3		步驟	39
	6.3.1	讓報表中對應到 AD 用戶名	39
	6.3.2	讓報表中對應到 AD 用戶名	67
6.4		實用範例	73
	6.4.1	公司 A 部門人員架構	73
	6.4.2	AD 導入方案	73
第3部		即時監看與對象管理	83
第7章	即時約	周路監看	84
7.1		監看公司網路	84
第8章	固定對	對象 —地址/服務/排程	87
8.1		需求	87
8.2		方法	87
8.3		步驟	87
	8.3.1	地址設定	88
	8.3.2	排程設定	90
第4部		流量管理	93
第9章	流量管	^{查理} -IP 限制策略	94
9.1		設定 Per-IP Limit	94

第10章 流量	量管理−應用層(L7)策略					
10.1	0.1 應用層策略介紹					
10.2	需求					
10.3	方法					
10.4	步驟					
10.4.1	設定即時通訊軟體規則					
10.4.2	設定點對點傳輸軟體規則					
10.4.3	設定 VoIP 規則					
10.4.4	攔阻 VoIP - Skype File Transfer					
第11章 流量		110				
11.1	設定 Traffic Manager					
11.1.1	需求					
11.1.2	QoS的Per-IP功能					
11.1.3	QoS 的 Per-Session 功能					
11.1.4	QoS的Per-Net 功能					
第5部	內容管理					
第12章 內容	容管理策略					
12.1	需求					
12.2	方法					
12.3	步驟					
12.3.1	從本地端檔案載入內容策略與其群組					
12.3.2	手動編輯內容策略					
12.3.3	自動學習內容策略名單					
12.3.4	從本地端檔案匯出內容策略與其群組					
12.3.5	內容策略設定輔助工具列					
第13章 內容	客管理-網頁管理					
13.1	需求					
13.2	目的					
13.3	方法					
13.4	步驟					
第14章 容管	管理-即時通訊方案					
14.1	需求					

	14.2	方法	135
	14.3	步驟	
	14.3.1	即時通訊服務	135
	14.3.2	即時通訊群組	137
第	15章 內容	管理-即時通訊管理	139
	15.1	需求	139
	15.2	方法	139
	15.3	步驟	139
	15.3.1	新增的即時通訊使用者預設值	
	15.3.2	即時通訊聊天對象管理	140
	15.3.3	即時通訊內容過濾	142
	15.3.4	即時通訊安全防護	147
	15.3.5	除外來源端設定	149
第	16章 LDA	.P/AD 匯入範例	150
	16.1	設定 LDAP Browser 軟體	
	16.2	設定 LDAP Import – 基本設定	
	16.3	設定 LDAP Import – 進階設定	155
	16.4	LDAP 匯入疑難排解	
第(6 部	報表中心	157
第	17章 報表	中心簡介	158
	17.1	設備報表中心	
	17.2	報表設計原則	
	17.2.1	報表類別	
	17.2.2	搜尋工具	
第	18章 應用]層策略報表	162
	18.1	需求	
	18.2	方法	
	18.3	步驟	
	18.3.1	功能面報表流覽	
	18.3.2	政策面報表流覽	163
	18.3.3	個人面報表流覽	165
	18.3.4	匯出事件報表	167

第19章 即翻	诗通 訊管理報表	
19.1	需求	
19.2	方法	170
19.3	步驟	
19.3.1	功能面報表流覽	
19.3.2	政策面報表流覽	
19.3.3	個人面報表流覽	
19.3.4	匯出事件報表	
第 20 章 網頭	夏管理員報表	
20.1	需求	
20.2	方法	
20.3	步驟	
20.3.1	功能面報表流覽	
20.3.2	政策面報表流覽	
20.3.3	個人面報表流覽	
20.3.4	匯出事件報表	
第 21 章 流量	置管理員報表	
21.1	需求	
21.2	方法	
21.3	步驟	
21.3.1	頻寬面報表流覽	
21.3.2	功能面報表流覽	
21.3.3	政策面報表流覽	
21.3.4	個人面報表流覽	
第7部	資料維護與警報系統	
第 22 章 階層	骨式管理與稽核	
22.1	需求	
22.2	目的	
22.3	方法	
22.4	步驟	
22.4.1	新增使用者帳號	
22.4.2	修改使用者登入網頁介面的密碼	

第2	23 章	管理	理服務器設定					
	23.1		管理	管理服務器概述				
	23.2		管理服務器設定					
第2	24 章	側錡	禄稽核	ξ	209			
	24.1		需求					
	24.2		方法					
	24.3		步驟					
	24	4.3.1		即時通訊內容側錄				
	24	4.3.2		網頁內容側錄	210			
第2	25 章	警報	灵中心	λ	213			
	25.1		需求		213			
	25.2		目的		213			
	25.3		方法		213			
	25.4		步驟		214			
	25	5.4.1		系統記錄	214			
	25	5.4.2		設定接收系統記錄的時間	215			
	25	5.4.3		啟用即時接收系統記錄	216			
第2	26 章	系統	記維護		217			
	26.1		需求		217			
	26.2		透過	TFTP 伺服器升級韌體	217			
	26.3 備份設定檔				218			
	26.4 還原設定檔				218			
	26.5		啟用	選購的模組				
	26.6		升級	IM 引擎 / 應用程式列為 / 病毒資料庫 / URL 資料庫				
	26	6.6.1		自動升級 IM 引擎 / 應用程式列為 / 病毒資料庫 / URL 資料庫				
	26	6.6.2		手動升級應用程式列為				
	26	6.6.3		手動升級 URL 資料庫				
	26	6.6.4		在 CLI 標準模式下·恢復出廠預設值				
	26	6.6.5		在 CLI 救援模式下 · 回復出廠預設值				
	26	6.6.6		SNMP 控制設定				
附釒	录				225			
附金	象A 扌	指令	行介	面(CLI)				

A	.1	CLI 資訊清單 - 標準模式	26
A	.2	CLI 資訊清單 - 救援模式22	29
附錄	В	疑難排解	2
附錄	С	系統記錄語法	4
附錄	D	詞彙集	9
附錄	Е	索引	5

I

第1部

產品簡介

第1章

產品簡介

本章介紹您如何快速安裝設備。

員工上網不外乎用 Outlook 收信、用 Explorer 流覽網頁、用 MSN/Skype 等即時通訊(IM)跟朋友閒聊、用 KaZaA/Kuro/ezPeer 等點對點傳輸(P2P)下載非法資訊。其中·Email 與 IM 是洩密與病毒入侵的管道·而 P2P 更是頻 寬的殺手與間諜軟體的溫床。L7 Networks 的設備內容管理器·是無懼任何偽裝連線的第七層控管設備,以全球領先的 Inline 架構,依時間區段控管、側錄每個員工 IM/P2P 的細部使用行為、聊天物件、傳檔檔案型別、聊天內容關鍵字、使 用頻寬、傳檔掃毒、蠕蟲散佈等,並具備強大 IM/P2P 報表系統。除能追蹤員工洩密行為/工作績效/側錄采證外,更對目 前 Layer-4 埠號已無法反應實際流量頻寬的情況,提供了絕佳的頻寬管理與報表系統。

1.1 產品包裝檢查

編號	品名	備註		
1.	設備			
2.	L型固定鐵片			
3.	3. 螺絲組			
4.	4. 網路線 (RJ-45)			
5.	AC 電源線			
6.	RS-232 console 線			
7.	CD			

請檢查您所購買的 設備 產品包裝內容,如有遺失,請聯絡您當初購買本產品的經銷商。

表格 1-1 產品包裝專案

1.2 硬體安裝

設備 設備可以固定在標準 19 时機架上·亦可以獨立放置於桌面上。請利用包裝盒內附的螺絲組將 L 型固定鐵片鎖於 設備 上·然後將 設備 安裝於機架上。

請依以下核對清單檢查您的網路連線是否已經備妥:

1. 設備設備

2. 網路設備 – 如路由器、交換器、集線器(Hub)等。

如果您將 設備 連結到上述網路設備,請使用串線 (through)相連。

用戶端設備(CPE) - 如桌上型 PC 或筆記型電腦等。
 如果您將設備連結到上述用戶端設備,請使用跳線(cross-over)相連。

4. 將設備 RJ-45 埠連結相對應之網路線

設備系列產品的硬體規格根據您所購買的型號而有不同。當您將 設備 安裝于路由器後方時,所有進出流量皆會受其控管。 LAN 端的流量必須連接於 設備 Internal 端,而所有連外的流量必須藉由 設備 External 端與存取路由器 (access router)相連。

1.3 將設備連上網路

- 電源。首先將電源接上設備背面的電源孔,然後將另一端接上電源插座。並將開關切換至 I。請稍候約兩分鐘,設備 開機完畢後,再進行下一步連接動作。注意,設備-10 只需將變壓器的接頭接上其背後的電源孔即可啟動電源。
- 2. Console 介面。利用 RS-232 console 線·將設備 console 埠與您用來設定設備的 PC 對接。您即可透過 CLI 指令來 設定設備的系統參數。
- MGMT介面。此管理介面系用來傳送設備的設定檔封包,所以必須透過網路線與LAN 端的交換器或集線器相連,且 要與管理伺服器在同一網段底下。
- 4. Internal 介面。此介面系透過網路線與您位於 LAN 端的交換器或集線器相連,用來管理所有內部可控管的網路流量。
- 5. External 介面。此介面系透過網路線將其與存取路由器相連,用來與網際網路連線。
- 6. HA 介面。用來連接備份設備,以確保網路不因硬體或意外而中斷。
- 7. 重設鍵。用來重開機用,避免經常開關電源,而縮短軟硬體使用壽命。

1.4 系統預設值 vs 範例設定

在下表中您可比較出廠預設值與本手冊範例中所使用的 IP 設定值。請記得·INT (Internal) 連接埠與 EXT (External) 連接埠並不需要設定任何 IP。因為 Internal 連接埠是連接所有 LAN 端受 設備 控管的用戶端,而 External 連接埠為 連接對外的網路。連接埠排列順序依您所購買的型號而有不同,當您首次使用 設備 時,請進入 CLI 介面查看連接埠的排 列順序。在許可權模式中輸入 "ip show",您可以看出所有依照連接埠編號排列的連接埠,然後對照您設備上的編號, 即可以此順序來連結您的網路線。

	項目	預設設定	範例設定
Password		admin	admin
	Port No.	3	3
MGT	IP Address	192.168.1.1	192.168.168.201
	Netmask	255.255.255.0	255.255.255.0

InstantScan User Manual

	Gateway IP	192.168.1.254	192.168.168.254
	Primary DNS	0.0.0.0	168.95.1.1
	Secondary DNS	0.0.0.0	0.0.0.0
	Status	DOWN	UP
	Port No.	4	4
110	IP Address	N/A	N/A
ПА	Netmask	N/A	N/A
	Status	DOWN	DOWN
	IP Address	尚未設定	10.1.1.10
Managamant	Subnet mask	尚未設定	255.255.255.0
Server	Gateway IP	尚未設定	10.1.1.254
	Primary DNS	尚未設定	168.95.1.1
	Secondary DNS	尚未設定	N/A

表格 1-2 設備 相關系統預設值

第2章

管理系統介紹

本章節介紹如設備的設計原則與設定步驟。

2.1 設備 技術應用

設備 管理系統為一網頁應用介面,允許多個管理者同時管理一台或多台 設備裝置。您可藉由任何電腦透過網頁流覽器來 存取 設備 管理伺服器。

內容管理五步驟:生產力/安全性最大化、威脅/總持有成本最小化

現今許多網際網路使用者已經安裝了即時通訊(IM)與點對點傳輸(P2P)應用軟體。這些軟體會自動隨機跳埠,或把自 己偽裝在 HTTP 的地道裡,以規避管理者的檢查。為了讓管理者克服這個問題,「內容管理五步驟」可用來最大化生產力/ 安全性,並最小化威脅性與總持有成本。



- 随插即用即時流量偵測/學習:為了幫助管理者解決上述問題,設備提供了随插即用流量偵測來當作第一步。只需要 把網路線接起來,設備就回現場把網路流量展現在你面前。您可以看到有多少 MSN 是用 HTTP 地道來偽裝的,也 可以看到有多少 IM 正在聊天。聊天的過程會被自動記錄,以方便管理者匯入到設定中。
- 將第七層流量打回第四層:在流量偵測過後,若是列管的流量,您可以使用第七層防火牆來檔掉某些應用。在此圖中, 設備 會把在第七層亂竄的流量過濾,讓其乖乖地以第四層流量方式運行,説明您原有的第四層防火牆得以用埠號作最 基本的控制。非但如此,設備 可說明您阻擋非標準的 IM 連線。例如 MSN 會自動偵測防火牆設定,若 MSN 無法

從標準的1860埠號連出去登入,則會開始用 HTTP 代理伺服器連線出去。更有甚者,任何人都可以手動設定他要連 到哪一台 HTTP/SOCKS4/SOCKS5 代理伺服器(包括貴公司裡的 HTTP 代理伺服器)。最慘的是,員工還可以使用 流覽器連到各種不同提供 MSN 服務的網頁,繼續跟外面的人聊天。這些 設備 都可以幫助您解決。

- 互動式行為管理:設定個人化的政策。既然 設備 可以認得應用程式的各種細部行為,網管人員可以針對每個使用者 給予不同的行為許可權。使用者的資訊可以整合企業現有的使用者資料庫,例如 LDAP、Active Directory、POP3(S)、 IMAP(S)、RADIUS。
- 4. 深度內容檢測:設定進階的內容過濾功能。在此圖中,設備 可偵測/阻擋「壓縮檔裡的病毒」或「散佈在 MSN 窗口 裡的 URL 或傳檔蠕蟲」。若要做到極端的安全性,所有的對話都可以被側錄,來預防內部資訊洩漏。若使用者違反 了政策,說了些不該說的話,設備 能夠直接在「IM視窗內」警告使用者公司的 IM 使用政策
- 5. 詳細報表分析:最後,報表分析可以幫網管人員找出問題。數十種的圖形報表,包括每天/每週/每月/每季/每年的頻 寬報表、IM 使用行為、以公司部門顯示聊天側錄、違反政策情況。報表可以客制化、搜尋,且得以用 PDF/HTML/Excel 的格式,在設定的時間週期內以附加檔寄出。

三層式架構:效能、可用性、功能最大化

第七層網路設備通常要做「非常多的計算功夫」和「較好的分散架構」,以最大化效能、可用性,與功能性。設備採用了 業界最先進的三層式架構來增加效能,讓各層各司其職,完成每一個目的。



- 第七層設備:第七層設備應該要專注的是「快速地」與「準確地」執行內容檢測。如此,第七層設備裝在網路進出口 線上,才不會影響到網路的效能。
- 管理伺服器:管理伺服器要負責的是中央集中控管第七層設備,並接收來自於不同第七層設備的事件,整理於資料庫 中更進一步製作報表分析。在管理伺服器上製作報表,不會影響第七層設備的效能。
- 3. 管理用戶端:管理用戶端可用任何具備JAVA功能的流覽器連到管理伺服器。只要他連得到管理伺服器.他就可以連得 到任何架設於管理伺服器之下的第七層設備。

2.2 內容管理流程

設備 內容管理器可控管時下盛行的即時通訊軟體 (IM)、點對點 (P2P) 傳輸軟體、檔案傳輸軟體、與遠程式控制管 軟體、VoIP 軟體與網頁內容管理等等。您可以藉由這些內容管理專案來做最適當的網路管理,保障公司的網路安全、杜絕 一切藉由網際網路的便利而機密外泄的管道,更可加強員工的產能。不但可以不用全面封鎖即時通訊與點對點傳輸軟體的 使用,更可控管這些軟體,借助即時通訊、點對點傳輸軟體的時效性與便利性而達到真正公司業務往來省時又省錢的目的。 在接下來的章節中,我們將針對內容管理的細項逐一介紹。



圖表 2-1 內容管理器之管理流程

如圖表 2-1 所示,設備 將進來的流量導給流量監控監看。而當您啟用應用層策略時,所有應用軟體不管是透過 TCP 通訊協定或是代理伺服器(例如 HTTP/SOCKS)連線,企圖欺騙管理人員,其流經 設備 的封包在經過利基網路第七層辨識

引擎辨認後·再依使用者對發送該封包的 IP(來源端)與其送往的物件(目的端 IP)所定義的政策規則決定是否讓其通行,只要進來的封包符合設定的條件,就套用該政策規則。

當您啟用即時通訊管理時 · MSN/Yahoo/AIM/ICQ 等即時通訊軟體將會被規範透過正規的連接埠連線出去。也就是說 MSN 必須透過連接埠 1863、Yahoo 5050、AIM/ICQ 5190。如果即時通訊軟體透過非正規連接埠連線 · 其連線就會被 設 備 攔阻。例如 · 在應用層策略允許 MSN 連線 · 且您亦開啟即時通訊管理並允許 MSN 連線的條件下 · MSN_A 透過連接 埠 1863 · 可以正常連線;而 MSN_B 企圖透過連接埠 80 連線 · 就會被正規化的政策攔阻。

當網頁管理員也啟用時,所有透過連接埠 80 傳送的封包都會導給網頁管理員監看。管理人員可以依制定的政策做網頁內 容過濾、URL 側錄、網頁掃毒等網頁內容管理。

2.3 設備網頁介面設計原則

設備 管理系統包含下列五個視窗:

- 1. 工具列:可設定設備參數的工具,包含快速功能鍵。
- 2. 設備專案樹狀圖:包含已選擇的項目與受此專案控管的所有裝置。
- 3. 功能樹狀圖:所有 設備 的功能樹狀圖。包含監看、管理與報表系統等大項。
- 4. 內容視窗: 各項功能參數的設定視窗。接下來的章節將依序引導您設定 設備。
- 5. 狀態列:顯示所有系統操作資訊。您也可以點擊圖示 🔳 將此狀態列隱藏起來。

圖示		功能
	2	新增專案
「日列」		開啟專案
	M	顯示/隱藏 狀態列
	0	上傳設定檔
	9¥	物件群組
	_	單一物件
		除了此選定物件群組外,全部套用該通訊協定的防火牆規則。
中空油空		除了此選定物件 (範圍/子網路/主機) 外,全部套用該通訊協定的防火牆規則。
内谷伉囪	带	日期選項,可依日期期間指定顯示選定的事件記錄或報表。
	0	進階搜尋功能。可依設定的條件搜尋事件記錄。
	20	重新整理事件的時間設定。
		報表匯出設定

2.4 設備圖示說明

表格 2-1 設備 圖示說明

2.5 工具列說明

標籤	項目	說明
	Device/Group	建立新排業式群組
	Manager	建亚利袋直线杆艇
	New Project	建立新專案
File	Open Project	開啟已存在的項目
	Close Project	關閉使用中的專案
	Delete Project	刪除選取的項目
	Exit	離開使用者網頁設定介面
	Upload Configuration	上傳設定檔到裝置上
	Update IM engine	從更新中心更新特 IM 引擎
	Update pattern	從更新中心更新應用程式列為
	Update AV database	從更新中心更新病毒資料庫
Update	Update URL database	從更新中心更新 URL 資料庫
	License	如果您有購買額外模組、您必須在此填寫您的授權碼、並經過驗證後、
		才可使用。
	Option	更新中心設定
	Support I 設備 t	設備所支援的應用程式清單
	Account Manager	依使用層級·設定使用者帳號與許可權
	Change Password	更改登入密碼
Tools	Language Setting	設定語言模組,可選擇英文、繁體中文與簡體中文三種語言。
	SNMP Control	遠端監控設備的系統狀態以及網路
	Config Backup	備份現行的設定檔到本地端磁片
	Config Restore	還原已儲存的設定檔到裝置上
Help	About	顯示設備版本訊息

2.6 管理伺服器版本



步驟 2 顯示管理伺服器的版本

如右圖所示·您可以看到管理伺服器的版本與出版的日期。

第2部

基本設定

第3章

管理伺服器安裝

本章節介紹管理伺服器的軟體安裝與網路設定

3.1 管理伺服器軟體安裝

3.1.1 管理伺服器系統需求

✓ 作業系統 (OS) 至少應為 Windows 2000/2003、Windows XP 或更高等級。如果您的作業系統為英文板, 請先安裝繁體中文字型套件,否則無法正常顯示中文字型。語言套件安裝視窗將於您開始安裝管理伺服器時顯 示,請點選 Install 安裝。

Language pack installation		
To display language characters correctly you need to install the following language pack:		
Chinese Traditional		
Never install any language packs.		
Install Cancel		

圖表 3-1 語言套件安裝畫面

- ✓ 硬碟至少 80GB 以上可使用空間,建議最好有 120GB 可使用空間。
- ✓ CPU 最少是 Pentium 4 或同等級。
- ✓ 記憶體最少 256MB,建議最好 512MB 以上。
- ✓ 如果您的作業系統是 Windows XP service pack 2 · 且啟用其內建的防火牆 · 請記得依以下步驟開啟連接埠
 514、1080 和 3306。如此一來 · 所有封包的進出 · 才不會因防火牆的攔阻而有所漏失 · 管理伺服器才會正常 運作。
 - 1. 到開始 > 設定 > 網路連線。
 - 2. 點選區域連線,按滑鼠右鍵選擇內容。
 - 3. 到進階 > 設定值 > 例外。點擊新增連接埠...
 - 4. 輸入名稱與連接埠編號,點選此連接埠所使用的通訊協定(UDP或TCP)。點擊確定儲存設定值。

名稱	連接埠編碼	通訊協定	
Log Server	514	UDP	

Socks	1080	ТСР
Database Server	3306	TCP

表格 3-1 管理伺服器連接埠設定

3.1.2 軟體安裝程式

- 1. 安裝 Management Server
- 2. Management Server 版本升級
- 3. 流覽光碟
- 4. 反安裝全部(只限移除 Management Server)
- 5. 離開安裝介面

⚠ 注意:

- 當您重新安裝管理伺服器,或升級管理伺服器,請記得重新開機電腦,系統才會運作正常。詳細的安裝說明,請參考 快速安裝指南。
- 2. 如果您曾經安裝過 MySQL 與 Apache 任何的版本 · 妳必須移除您所安裝的 MySQL 與 Apache 軟體 · 請參考附錄說 明。

3.1.3 用戶端安裝

在您安裝好 設備 管理伺服器並將 設備 上的網路線連結完成後,您即可利用網頁流覽器,在網址列上鍵入 http://<管理 伺服器 IP 地址>/ 來連上管理伺服器。當您第一次透過流覽器連上管理伺服器時,Java Plug-in 將從管理伺服器端安裝 到您的用戶端電腦上。

⚠ 注意:用戶端在第一次透過流覽器連上管理伺服器時,因流覽器的因素,必須花幾分鐘時間安裝 Java plug-in 程式, 請耐心等候。

3.2 設定設備

在您開始控管 設備 設備前,請先利用設備的 console 介面,直接用 RS-232 console 線與用來設定設備用戶端的 PC 對 接。然後,透過 CLI 指令來設定設備的系統參數。之後,您可以利用 Telnet、SSH,或其它 terminal 等遠端連線方式來更 改系統參數。

3.2.1 啟動系統

將鄰近設備電源插槽的電源開關打開。在開機完成後,系統將要求您輸入 ID 與密碼。此時,預設的 ID 與密碼皆是 admin。在登入系統後,您可以利用 CLI 指令更改密碼。詳細 CLI 指令,請參閱附錄 A 說明。

3.2.2 系統架構

設備以通透模式安裝於網路上,不需更改既有的網路架構。設備管理伺服器配合設備管理系統與報表系統,提供您簡而易用的使用者管理介面來設定管理政策。網管人員可根據網路架構與公司政策來訂定各式各樣的管理政策。一台管理伺服器可同時控管多台設備,並且可接收與分析被控管的設備之事件記錄。您可將管理伺服器安置於任何網路位置。本手冊提供一個基礎的設備網路安裝架構。只要您瞭解基本的安裝原理,您即可根據貴公司的網路架構安裝您的設備。詳細的安裝範例,請參考錯誤!找不到參照來源。。



圖表 3-3 設備 系統的訊息遞送

如錯誤!找不到參照來源。所示,您必須指定 IP 位址給 1) 設備管理介面(Management 連接埠);2) 管理伺服器; 與 3)管理端 PC。設備可安裝於企業網路內部或外部。當網管人員新增一條管理規則,並將設定文件上傳,管理伺服器 立即將設定檔上傳至設備。當受到設備控管的 PC 啟用任何即時通訊(IM)軟體或點對點(P2P)傳輸軟體時,設備會將 這些事件記錄傳送給管理伺服器儲存。管理伺服器依您的時程規劃,定期產生報表寄送給網管人員分析。

3.2.3 系統參數設定

請用隨機內附的 RS-232 console 線·將設備 console介面與用來設定設備的PC之序列埠相連·您可選擇COM1埠或 COM2埠來設定設備。請參考以下超級終端機的設定範例。

終端機類型	超級終端機
每秒傳輸位	115200
數據位元	8
同步檢查	無
停止位	1
流量控制	無

表格 3-2 終端機設定

步驟 1. 設置多路橋模式 先選擇 Press(L) tol設備t·也就是鍵入L查看	Hardwar Enter Initi Validating. Setting sys Press [L] t	e ID: 338822F58646 al Key: 53179AA3E3 tem interfaces o list. (R) to rec	mfigure, (C)	to confirm. 1	szas szall- 	
然後選擇(R) to reconfigure 鍵入R設置 ports	eth0 eth1 eth2	1 2 3	UNKNOHN UNKNOHN HCT	DONN DONN DONN		
例如:設置一個2路橋的模式·在Enter interface	eth3 eth4	45	HA INT1	DOWN		
orders 後鍵入 INT2 · EXT2 · MGT · HA · INT1 ·	eth6 eth7	6 7 8	UNKNONN	DONN		
EXT1 · · ·	eth8 eth9	9 10	UNKNOHN UNKNOHN	DONN DONN		
在 Enter port orders 後鍵入 1 · 2 · 3 · 4 · 5 · 6 · · · ·	Press (L)) to list, (R)	to reconfi	gure, (C) t	o confirm. r	
注意:對每個口的設置之間都要用"·" 隔開·沒	Enter int Enter por	terface orders t orders: 1.2	INT2.EXT2	, NGT , HA . TNT '	1.EXT1	
設置到的口也要用"·"隔開。	Press (L)) to list. (R)	to reconfig	pure, (C) to	o confirm. l	
設置後再鍵入L查看確認設置無誤,最後鍵入C確	Link	Port	Na	ne	Status	
認設直元成。	cth0 eth1 eth2 clh3 eth4 eth5 clh6 eth7 eth8 clh9 Press (L	1 2 3 4 5 6 UNKNOWN UNKNOWN UNKNOWN UNKNOWN UNKNOWN	ID F H H H H H H H H H H H H H H H H H H	4T2 4T2 4T1 4T1 4KNOWN 4KNOWN 4KNOWN 4KNOWN 90me, (C) 10	DOWN DOWN DOWN DOWN DOWN DOWN DOWN DOWN	

步驟 2. 登入系統

系統預設的登入帳號密碼為 admin/admin。之後您可以根據 CLI 指令來更改密碼。

注意!!! 密碼的長度必須介於 5~20 字元間。小於 5 個字元或大於 20 個字元都會被系統拒絕。

步驟 3. 設定設備 IP 地址 鍵入en進入許可權模式。鍵入ip set指令來設定 MGT埠與 Management Server的相關IP位址。	Please enter the IP configuration for this device. IP Address 1192.168.18.181: 192.168.18.18 Metwork [255.255.25.0]: Default Bateway [192.168.18.11: 192.168.18.1 Primary DMS [202.109.14.5]: 202.109.14.5 Secondary DMS [8.0.0.0]: Your configuration is:				
	Gateway: 192.1 Primary DNS: 5 Secondary DNS: Management Ser Port Interface	68.18.1 892.189.14.5 8.0.0.0 ver: 192.168.18. 1P Address	42 Netnask	Stat	us
	1 INT2 2 EXT2 3 MGT 4 HA 5 INT1 6 EXT1 Ro you really	N/A N/A 192.168.18.18 N/A N/A N/A N/A	N/R N/A 255.255.255.8 N/A N/A N/A d save (Y/N17 (N)	UP UP DOWN UP UP	(Bridge 2) (Bridge 2) (HA Disabled) (Bridge 1) (Bridge 1)

3.2.4 設備 網頁介面設定

設備管理系統與報表系統使用Java平臺設計,需要支援Java Plug-in程式。所以用戶端必須從管理伺服器處安裝Java Plug-in,才可流覽管理伺服器網頁。當您第一次使用IE流覽器連接管理伺服器時,Java Plug-in便會自動安裝進您的電腦。 第一次登入時需要一些時間讓程式初始化,請耐心等候。

步驟 1. 連接管理伺服器 打開您的 MGTClient · 在網址列上鍵入<管 理伺服器 IP 地址>。例如·輸入 192.168.18.42 來連接管理伺服器。	連接 <u>192.168.18.42</u> Please input Management Server IP 192.168.18.42 OK Cancel	
步驟 2. 選擇語言模組 設備目前提供英文、繁體中文、簡體中文等 多種語言模組供您選擇,您可以選擇您喜愛 的語言當成網頁介面的預設語言模組。點擊 OK 進入登入畫面。	Please select your language English(US/UK/Canada/Australia) English(US/UK/Canada/Australia) Simplified Chinese(PRC/Singapore) Traditional Chinese(HK/Taiwan/Macau) French(France) Germany(German) Italian (Italy/Switzerland) Korean(Korea) Japanese(Japan)	
步驟 3. 登入 輸入 ID/Password (預設都是 admin)。通過	確認後.即可進入管理頁面。	

3.2.4.1 建立裝置/群組

步驟1選擇群組管理員	File > Device/Group Mar	nager	
點選 Device/Group Manager 選項。	Dovice/Crown Manager	CONT	
	New Droject	Ctrl-1	
	Conen Project	Ctri-O	
	Df Edit Droject	CHI 5	
	Close Project	Ctri-E	
	Delete Project	Ctrl-D	
	Evit	Ctrl X	
步驟 2 新增群組			
在 Devices 上按右鍵·然後點選 New	Group •		
步驟 3 新增群組名稱	File > Device/Group Mar	nager > New Group	
輸入此群組的名稱·然後點擊 OK 繼			
續。之後·群組名稱將顯示在螢幕上。	Enter the name of the group.		
您可以按右鍵選擇 Rename Group	-Crown information		
或 Delete Gorup 來修改或刪除此群	Name: EP1		
組。			
	19. -	OK Cancel	
步驟4 新增裝置	File > Device/Group Mar	nager > New Device	
在群組 Group_1 上按右鍵 · 然後點選			
New Device •			

	Create a new Group/Device. Add a group/device by right-click the objects.
步驟 5 編輯新裝置相關資訊	File > Device/Group Manager > New Device
輸入裝置名稱·並選擇一組已指定其管理	
伺服器的 設備裝置之 IP 位址·然後輸入	Enter a unique name and related information for the device.
具既相關貧訊。點擊 OK 儲存設定。	Device information
	Name: 🛛
注息 :您必須先透過 CLI 介围, 設定好裝 置上的 ID, 然後指定管理伺服器 ID 位	IP: 132,166,18.49
	Group: SP1 Vew
當您設定好裝置後,管理伺服器將自動獲	
取屬於其列管的 device 資訊。只要是已	
經設定過的裝置·就不可以再被設定。也	OK Cancel
就是說 · 當我已經設定好 Device_1	
192.168.11.19 · 當您要再新增裝置時 ·	
192.168.11.19將不再出現在IP欄位內了。	

新增項目

步驟 1 新增項目	File > New Project
選擇 New Project。	

	<u>File Update Tools Help</u>
	- Device/Group Manager Ctrl-T
	New Project Ctrl-P
	Den Project Ctrl-O
	Edit Project Ctrl-E
	Close Project Ctrl-C
	Delete Project Ctrl-D
	Exit Ctrl-X
步驟 2 建立新專案	File > New Project > New Project
首先・請點選項目的模式・輸入專案名稱・	
從 All Devices 欄位中選擇要加入此專案的	Create a new Project.
裝置·然後點擊 <<(左向箭頭)將點選的	Select the devices into the project.
装置加到 Selected Devices 欄位。如果您	-Select Mode
要從此專案刪除某個裝置·請點選該裝置·	General Group
然後點擊 >> (右向箭頭)即可。	-Draiget information
	Name:
	All Devices Devices Devices
	>>
	Next Step OK Cancel

專案模式	說明
General (一 般)。	您希望每台設備裝置可以擁有其個別的設定檔·每台裝置可擺放在不同的部門·且各自獨立運行· 您可以選擇此模式。
Group (群組)	當您購買 2 台或 2 台以上設備 裝置,希望簡化設定的步驟,所有裝置的設定檔共用,其報表系統 也共用。也就是說,不管您在哪一台 Device 上變更設定檔,此設定檔都會寫進基底裝置 (Base Device)的設定檔中。其它裝置只要重新載入設定檔即可獲取已更新過的設定檔。

表格 專案模式

一般專案模式

步驟1 新增一般專案模式	File > New Project
選擇 General (一般)為專案的模式,這 個模式適合大部分的案例。輸入項目名稱, 從 All Devices 欄位中選擇要加入此專案的 裝置,然後點擊 <<(左向箭頭)將點選的 裝置加到 Selected Devices 欄位。如果您 要從此專案刪除某個裝置,請點選該裝置, 然後點擊 >> (右向箭頭)即可。最後點 擊 OK 結束設定且專案會自動儲存。	Create a new Project. Enter the name of this project. New a group/device by right-click the objects. Select Mode © General Oroup Project information Name: test Selected Devices SP1: IX Devices

群組專案模式

步驟 1 新增群組專案模式	File > New Project
選擇 Group (群組)為專案的模式,這個 模式適合購買多台 設備,希望簡化設定步 驟,節省人力資源的公司。輸入項目名稱, 從 All Devices 欄位中選擇要加入此專案的 裝置,然後點擊 <<(左向箭頭)將點選的 裝置加到 Selected Devices 欄位。如果您 要從此專案刪除某個裝置,請點選該裝置, 然後點擊 >> (右向箭頭)即可。最後點 擊 Next Step 繼續下一步驟。	Create a new Project. Project micromation Marrie: Tester the reaction of the project. Devices Devices
步驟2選擇基底裝置 選擇 Base Device(基底裝置),當您選擇 基底裝置後,所有此專案內的裝置都會讀取 這個基底裝置的設定檔,且讀取的報表是所 有裝置的總和。最後點擊 OK 結束且自動 儲存設定。	File > New Project > Next Step

刪除項目

步驟1 點選刪除項目	File > Delete Project
點選 Delete Project 選項。	

	Line Update Tools Help Device/Group Manager Ctrl-T New Project Ctrl-P Open Project Ctrl-O Edit Project Ctrl-E	
	Close Project Ctrl-C	
	Exit Ctrl-X	
步驟 2 刪除項目 選擇您想刪除的項目 · 然後點擊 OK 關閉視 窗。	File > Delete Project Select a Project. Select a Project from the list below	
注意: 1. 一旦您點擊 OK 按鈕後,此專案即刻會 從系統中刪除。 2. 正在執行中的專案無法刪除,您必須先 關閉項目,才可選擇刪除項目。	Project information TEST1	
	OK Cancel	

開啟已存在的項目

步驟1 開啟項目	File > Open Project	
點選 Open Project 選項。	<u>File</u> <u>Update</u> <u>T</u> ools Help	
	- Device/Group Manager	Ctrl-T
	New Project	Ctrl-P
	/ Open Project	Ctrl-O
	📔 Edit Project	Ctrl-E
	📐 <u>C</u> lose Project	Ctrl-C
	Delete Project	Ctrl-D
	Exit	Ctrl-X
步驟 2 選擇要開啟的項目	File > Open Project	
選擇您要開啟的項目。點擊 OK 關閉窗		

□ •	Select a Project Select a Project from the 1st below	
	Project Information	
	OK Cancel	
步驟3管理設備		
現在.您可以開始管理您的設備。一個項目可	「以同時控管多台可能屬於不同群組的裝置。將滑鼠移到您要控管的裝置上點兩下‧系	
統將連接到此裝置‧並下載其設定檔。File > Open Project		

第4章

網頁登入驗證

本章介紹如何設定網頁登入驗證,讓使用者透過設備登入公司網路

設備支持 POP3(s)、IMAP(s)、Radius、LDAP 等帳號驗證方式。使用者可以您可以結合現有的 POP3(s)、IMAP (s) 郵件系統資源,讓通過驗證的使用者註冊自己的即時通訊帳號。您亦可以利用 Radius 或 LDAP 伺服器讓使用者 透過向伺服器驗證通過,取得註冊帳號的許可權。

4.1 驗證的種類

使用者必須透過流覽器完成帳號驗證。當您設定好驗證類型,使用者只要在網址列上鍵入 設備 設備的 IP 位址,驗證的視 窗就會顯示出來。

請參考下列五個步驟來設定帳號驗證:

- 1. 啟用驗證功能。
- 2. 設定驗證類別。
- 3. 設定驗證各項參數。
- 4. 透過 IE 流覽器,自動導向到設備認證網頁

4.2 設定驗證類型

4.2.1 Pop3(s) 設定

步驟 1 設定 Pop3(s)驗證	Object Manager > Web Login > Action > Auth Server > Remote >
勾選 Authentification with remote servers (啟	Pop3 (s)
用驗證)。選擇 Pop3(s)為驗證類型。輸入伺	a Statue 数 Poing a Actor Auth Server a Custom Pages
過加密(埠號 995)連線驗證·請勾選SSL。然後 上傳設定檔。	Remute D Local Astherboarder with remote servers
注意: Pop3 服務透過連接埠 110 連線而 Pop3s 服務透過連接埠 995 連線。	Cestinguy Pyru wonth many the web-login user name with those in the remote datacease choice your sub-enfortion server here. Authemation type Pactings Pathemation type Pactings Server off 152 160 1 1 Server off 152 160 1 1 Server Part 1.0 Encoption ESL

欄位	說明	範例
Server IP	Pop3(s)伺服器的 IP 地址。	10.1.1.1
Server Port	Pop3(s)伺服器資料進出的通訊埠。例如·Pop3 服務透過連接埠 110 連線而 Pop3s 服務透過連接埠 995 連線。	110
Encryption	所謂的 SSL 是利用大數值編碼的技術將資料編碼後再傳至遠端·全球資訊網 在建置之後,必須向一個有公信力的單位登入,並取得一個 Private Key, 而將另一個 Public Key 放在網路上;資料在網際網路傳輸時都是經過編碼 的資料,即使有人在中間要擷取這些經過編碼的資料,看到的都是一些毫不 具意義的亂碼,這種編碼的另一種理論基礎是,凡是經過 Public Key 編碼 過的資料,都必須利用 Private Key 才能解得開。	不啟用

表格 4-1 POP3(s)設定

4.2.2 Imap(s) 設定

步驟1 設定 Imap(s)驗證	Object Manager > Web Login > Action > Auth Server > Remote >		
勾選 Authentification with remote servers(啟	Imaps (s)		
用驗證)。選擇 Imap(s)為驗證類型。輸入伺服	Ash Sarker 然 Petry 然 Actor Ach Sarker 然 Custom Pages GRemite @ Local		
器 IP 和伺服器連接埠。如果您的伺服器需要透過			
加密(埠號 995)建線驗證,請勾選SSL。然後上 傳設定檔。	Authentic atom with remote servers		
^{២ 政 止 恤 。} 注意:Imap 服務透過連接埠 143 連線而 Imaps 服務透過連接埠 993 連線。	Cessingtor Pace wonthormath Pierweb-logith user name with those in the remote delatorse should your outremication server here. (uth endication Type: Pacel(s) © Incop(s) © LDAP (uth endication Type: © Pacel(s) © Incop(s) © LDAP Server IF 152.108.1.1		

欄位	說明	範例
Server IP	IMAP(s)伺服器的 IP 地址。	10.1.1.1
Server Port	IMAP(s)伺服器資料進出的通訊埠。例如·IMAP 服務透過連接埠 143 連線而 IMAPs 服務透過連接埠 993 連線。	993
Encryption	所謂的 SSL 是利用大數值編碼的技術將資料編碼後再傳至遠端·全球資訊網 在建置之後,必須向一個有公信力的單位登入,並取得一個 Private Key, 而將另一個 Public Key 放在網路上;資料在網際網路傳輸時都是經過編碼 的資料,即使有人在中間要擷取這些經過編碼的資料,看到的都是一些毫不 具意義的亂碼,這種編碼的另一種理論基礎是,凡是經過 Public Key 編碼 過的資料,都必須利用 Private Key 才能解的開。	SSL

表格 4-2 IMAP (s) 設定

4.2.3 Radius 設定

步驟1 設定 Radius 驗證	Object Manager > Web Login > Action > Auth Server > Remote >
如果貴公司已經有安裝 Radius 伺服器·所有的員 工資料都儲存在 Radius 伺服器中·您可以選擇 Radius 驗證類別。當使用者要自行註冊即時通訊 帳號時·設備 會連絡 Radius 伺服器提供通行驗	Radius Status Server Sector Concel Concel MultiServer Sector Concel MultiServer Sector Concel MultiServer Sector Concel Conc
^{起。} 勾選 Authentification with remote servers(啟 用驗證)。選擇 Radius 為驗證類型。輸入伺服器	- Description If you want to match the web-lugin oper name with those in the terricle database, choose your authentication server here.
IP 和伺服器連接埠。輸入與 Radius 伺服器溝通 之Secret 碼。然後上傳設定檔。	Authentituden Type OPec3(s) Olmac(t) ③ Radus OLDAP RADUS sating Server IP 192. 681.1 Server Port 1812 Server t

欄位	說明	範例
Server IP	Radius 伺服器 IP 地址。	10.1.1.2
Server Port	Rad 設備 u 伺服器資料進出的連接埠。	1812
Secret	Secret 是 Radus 伺服器與用戶端驗證的加密金鑰。也就是通訊的各方彼此間共用一把加密金鑰,並且利用該金鑰的資訊來檢驗彼此的身份。	secret

表格 4-3 Radius 設定

4.2.4 LDAP 設定

步驟1 設定 LDAP 驗證	Object Manager > Web Login > Action > Auth Server > Remote >	
如果貴公司已經有安裝 LDAP 伺服器·所有的員工 資料都儲在在 IDAP 伺服器中,你可以選擇	LDAP 熱 Status 熱 Poirs 臨 Addar	
LDAP 使用者驗證類別。當使用者要自行註冊即時	Aulh Server Custom Pages Terrols Ducal	
通訊帳號·設備會連絡 LDAP 伺服器提供使用者 驗證·使用者只要輸入帳號與密碼·設備會將此組	Authorit collon with remote sorvers	
帳號密碼傳送給 LDAP 伺服器驗證,一旦通過驗 證,即可註冊即時通訊帳號。	Description If you wants: maxing the tablecingues mame with those in the remote satebase, shoese your authentication server here.	
勾選 Authentification with remote servers(啟	Authentication Type O Port3(s) O Imat(s) O Radius I LWP	
用驗證)。選擇 LDAP 為驗證類型。輸入伺服器 IP.然後上傳設定檔。LDAP 相關設定,請參考以 下章節。	Berver IP 192, 198, 1	
欄位	說明	範例
---------------	-----------------	-----------------
Server IP	LDAP 伺服器 IP 地址	10.1.1.11
Server Domain	LDAP 伺服器的功能變數名稱	yourcompany.com

表格 4-4 LDAP 設定

InstantScan User Manual

第5章

結合 Web Login 設定 L4/L7/Content 策略

本章介紹 mailer 的設定與其應用

5.1 需求

有時企業內部並沒有架設認證伺服器 · 但網路管理人員卻需要通過認證伺服器來控制管理每個人的上網行為 · 這時設備內建的 Web 認證管理功能可以實現認證伺服器這一需求 ·

- 1. 讓研發部的員工都需要進行的 web 認證,沒有經過認證的都將不能上網
- 2. 讓設備產生的報表能自動與設備內建的 web 認證帳號/名稱對應
- 3. 設定策略規則時, 能以 web 認證的帳號作過濾條件

5.2 方法

- 1.1 所有的成員都必須進行上網認證並且間隔每8小時就要進行一次認證, boss 不需要認證。
 - 1.1.1 啟用 Web Auth
 - 1.1.2 新增 web 認證的帳號名和密碼
 - 1.1.3 增加 web 認證策略
- 1.2 讓策略規則能以 Web 認證用戶名作過濾
 - 1.2.1 於 L4/L7 策略的規則裡,指定 Web 認證用戶
 - 1.2.2 於 Content 策略規則裡,手動指定 Web 認證用戶
 - 1.2.3 於 Content 策略規則裡,自動匯入 Web 認證用戶

5.3 步驟

5.3.1 所有的成員都必須進行上網認證並且間隔每 8 小時就要進行一次認證 · boss 不需要認證

5.3.1.1 啟用 Web Auth

Functions >Object Manager > Web Login > Status

Status Policy Action Image: Enable Web Login Image: Enable Web Login Description Web Login allows you to authenticate users at their web browsers. Upon login, users will be notified with his time quota.
(圖 1)

5.3.1.2 新增 Web 認證帳號和密碼

步驟1 新增 Web 認證帳號和	Functions >Object Manager > Web Login > Action > Local
密碼 在 Account 欄位填入欲增加的	Status Server S Custom Pages
所有人員的帳號名稱(BOSS 除 外)·在 Password 欄位元填上密 碼·按 Add 按鍵後·帳號名和 密碼將被加入清單· 在這裡新 增加了	Remote (B) Local Description If the web-login user name does not exists in the remote authentication server, the system will lookup local u Account: shaopeng root root
shaopeng,root,admin,zhangx un,gejia 用戶.上傳設定。	admin zhangeun gejia (圖 1)

5.3.1.3 增加 Web 認證策略

步驟1 新增固定物件 BOSS	Functions >Object Manager > Static > Address > Static Object
由於 BOSS 不需要認證,首先,	
我們先得給 BOSS 這個用戶的	
PC 指定一固定 IP · 比如:	
192.168.1.88, 然後在 Static	
Object 增加這個用戶·點 OK。	

InstantScan User Manual

	Static Objects 5 Stat	it Gmups			
	-Description				
	Applied to fixed IP obje	ets who do not need to suffrentical	э.		
			10		
	Balo Objects	Bba	11 ⁻		1
	HostCEO	Mill day host			
	HostCM0	Edityour IP and ess object			
	HostChairman	Name : BOSS			
	HostViceChaima	In Type : O Bubliet O H	ange 💿 Host		
	ServerFTP	IP 192.138.1.99			
	ServerMYSQL				
	ServerSQL	CE C	acel]		
	SubnetFINANCE	RE Subnet	192 158 1 0/24 192 168 5 0/24		
	SubnetMARKETING	Subnet	192 188.6 0/24		
	Dubusden	Dishood .	100 0 831 031		
步驟 2 新增 Web 認證策略	65 Status 55 Policy 65	Action			
Policy 頁面有一條預設的策略	Description Bessions are top-dox.	n matched with the policy. Only the	first matched policy takes e	fierts.	
Guest · 這條策略預設情況下是	-				
針對全部使用者·而我們要排除	Btanus	Con	dition	101	Action
對 boss 的認證, 所以做法加下:	1 Susat	come Source		ACI	Time Gumajmup
				Inseit	peliev
在 Web Auth 的 Policy 頁面右				Delete	policy
鍵點 Insert policy 新增加一條	🚵 Status 🏙 Policy 🏙	Action			
策略·起名為 rule_BOSS · 並且	Description				
IP 選項選擇為剛才的新增加的	Bessions are top-dow	mmatched with the policy. Only the	first-matched policy takes e	flects.	
物件 BOSS · ACL 選擇為	Statue	Con	allion		Action
Allow。然後點擊 Guest 策略,	NO. Rule P	lame		ACL	Time Cuota(hour)
	Rule_Boz)	bess)	Allow		0 (uniimited)
尤ACL 選擇局 WED AUTI, IIME	2 Guert	😂 aro	prise Aut		A B HOURS

步驟 3 輸入帳號用於上網		
在員工的 PC 上·當打開 IE 時· 會自動跳轉到認證頁面·這時候 需要向管理人員索要用戶名和 密碼·填寫後方可上網	Authentication Login Usemame zhangxun	
	Password	
	Sign up	
	[[[STATUS]]]	

5.3.2 讓策略規則能以 Web 認證用戶名作過濾

5.3.2.1 於 L4/L7 策略的規則裡,指定 Web 認證用戶

步驟1 新増 Web 認證用戶	Functions > Dynamic > Dynamic Objects
步驟1新增Web認證用戶 點選Dynamie Objects裡面增 加剛才需要增加的需要認證的 使用者帳號,這裡增加了 shaopeng,zhangxun,gejia,ro ot 用戶(見圖1)·這裡可以建 立一個 Groups·把上述幾個用 戶劃到這個群組裡面·在這裡· 我們建立了一個 Group 為 RD·把 gejia,shaopeng· zhangxun 劃到 RD 這個群組裡 面(見圖2)·上傳設定。	Functions > Dynamic > Dynamic Objects ⊃ynamic Objects Accounts gejia (gejia) Shaopeng (shaopeng) Shaopeng (shaopeng) Thangxun (zhangxun) Groups (圖1)
	Functions > Dynamic > Dynamic Groups



5.3.2.2 於 Content 策略規則裡,手動指定 Web 認證用戶

步驟1新增使用者自訂 Content規則 在這裡我們需要對RD這個群組 進行IM側錄·IM所傳文檔側錄 URL側錄。首先新增一條使用者 自己定義的規則·然後在彈出的 對話方塊裡的Name的位置填 寫RD·把MSGREC·FileRec 和URLRec都選擇為Enable	Functions > C	Content Manag	er > Conter	b Profile- volume Action Web Profile Pistmurn	Sverch. stec. Virtual Groups Cothers
(圖2),上傳設定檔即可	Create a new user Schedule : Schedule : Selection of the sector of the s	() Always • RD • RD • Enable • Enable Allow Allow • Inable Allow • Inable Allow • Inable () • Inable • Inable	1) Virtual Group : Name : roup, or Web Log Disable Disable	Others RD in account Finish Can	<pre>.</pre>

5.3.2.3 於 Content 策略規則裡,自動匯入 Web 認證用戶

步驟1自動匯入 Web 認證用戶	Functions > Content Manager > Content Policy > Policy
我們可以通過自動匯入 Web 認	



第6章

結合 AD 設定 L4/L7/Content 策略

6.1 需求

- 1. 讓設備產生的報表能自動與企業現有 AD 帳號/名稱對應
- 2. 設定策略規則時, 能以 AD 帳號或 AD 群組作過濾條件

6.2 方法

- 1.1 讓報表中對應到 AD 用戶名
 - 1.1.1 於 Windows 2003 Server 新增網域控制站 (DC)
 - 1.1.2 於 Windows 2003 Serve 新增 AD 用戶
 - 1.1.3 讓 Windows 2000/XP/2003/V 設備 ta 的 PC 使用新增的 AD 帳號登入 AD 網域
 - 1.1.4 執行 AD Import
 - 1.1.5 安裝登入 script 至 AD Server
 - 1.1.6 設定 device
 - 1.1.7 將 Windows AD client 重新登入 AD · 並以 sys ad show 觀看是否成功

1.2 讓策略規則能以 AD 用戶名作過濾

- 1.2.1 於對象管理->動態物件, 匯入 AD Server 上所有用戶帳號與名稱
- 1.2.2 於 L4/L7 策略的規則裡,指定 AD 使用者
- 1.2.3 於 Content 策略規則裡,手動指定 AD 用戶或 AD 群組
- 1.2.4 於 Content 策略規則裡,自動匯入所有 AD 用戶

6.3 步驟

6.3.1 讓報表中對應到 AD 用戶名

6.3.1.1 新增網域控制站



ows 组件向导		2
indows 組件 可以添加或删除 Wind	dows 的组件。	t
要添加或删除某个组(一部分。要查看组件(牛,请单击旁边的复选框。灰色框 内容,请单击"详细信息"。	表示只会安装该组件的
组件 (C):		
🗖 🧭 Internet Exp	lorer 增强的安全配置	0.0 MB 🔼
□ QQUDDI 服务		4.9 MB —
☑ ◇ update 381整	合包	O. O MB
U Windows Medi	a Services 胆水	15.3 MB
描述: 限制用户	浏览 Internet 和 Intranet 网络	54.0 MD
新雲磁盘空间	0.7.88	
可用磁盘空间:	6979.7 MB	详细信息 (1)
	〈上一步④〉下一步④〉	取消 帮助
	(圖 1)	

"下一步"就可以完成整個	Tindows 組件向导	×
DNS 的安裝。在整個安裝過程 中請保證	Tindows 組件 可以添加或删除 Windows 的组件。	
Windows Server 2003 安裝光 碟位於光碟機中·否則會出現找 不到檔的提示·那就需要手動定	要添加或删除某个组件,请单击旁边的复选框。灰色档 一部分。要查看组件内容,诸单击"详细信息"。 组件 (<u>c</u>):	匡表示只会安装该组件的
	 □ 計算算算的网络文件和打印服务 □ ● 素引服务 ✓ 書 网络服务 ✓ 書 网络服务 	0.0 MB 0.0 MB 2.6 MB 34.4 MB
	□ 晶 远程存储 描述: 包含各种专门的、网络相关的服务和协议	4.1 MB
	所需磁盘空间: 0.7 MB 可用磁盘空间: 6979.7 MB	详细信息 (1)
	〈上一步④〉	取消 都助
	(圖2)	
	(圖2)	
	(圖2) 网络服务 要添加或删除某个组件,请单击旁边的复选框。灰色相部分。要查看组件内容,请单击"详细信息"。	
	(圖2) 网络服务 要添加或删除某个组件, 请单击旁边的复选框。 灰色 部分。要查看组件内容, 请单击"详细信息"。 网络服务 的子组件 (C):	
	(圖2) 网络服务 要添加或删除某个组件,请单击旁边的复选框。灰色相部分。要查看组件内容,请单击"详细信息"。 网络服务的子组件 (C): ■ 및 HTTP 代理上的 RPC	▲ ▲ ▲ ▲ ▲ ● <
	(圖2) 阿络服务 要添加或删除某个组件,请单击旁边的复选框。灰色标 部分。要查看组件内容,请单击"详细信息"。 网络服务 的子组件 (C): 【】 【HTTP 代理上的 RPC 【】 】 Internet 验证服务	区表示只会安装该组件的→ 0.0 MB ▲ 0.0 MB
	(圖2) 阿络服务 要添加或删除某个组件,请单击旁边的复选框。灰色 部分。要查看组件内容,请单击"详细信息"。 网络服务 的子组件 (C):	区表示只会安装该组件的→ 0.0 MB 0.0 MB 0.9 MB
	(圖2) 阿络服务 要添加或删除某个组件, 请单击旁边的复选框。灰色相 部分。要查看组件内容, 请单击"详细信息"。 网络服务 的子组件 (C): 日 日 日 日 日 日 日 日	区表示只会安装该组件的→ 0.0 MB 0.0 MB 0.9 MB 0.0 MB 0.0 MB
	(圖2) 网络服务 要添加或删除某个组件,请单击旁边的复选框。灰色都分。要查看组件内容,请单击"详细信息"。 网络服务 的子组件 (C): 日 果HTTF代理上的 RFC 日 果Internet 验证服务 日 影 Windows Internet 名称服务 (WINS) 日 动态主机配置协议 (DHCP) 日 影 简单 TCP/IP 服务	区表示只会安装该组件的→ 0.0 MB 0.0 MB 0.9 MB 0.0 MB 0.0 MB 0.0 MB
	(圖2) 阿络服务 要添加或删除某个组件, 请单击旁边的复选框。灰色标 部分。要查看组件内容, 请单击"详细信息"。 网络服务 的子组件 (C): ■ Uniternet 验证服务 ■ Uniternet 验证服务 ■ Windows Internet 名称服务 (WINS) ■ 动态主机配置协议 (DHCP) ■ 简单 TCP/IP 服务 V ■ 城名系统 (DNS)	区表示只会安装该组件的→ 0.0 MB 0.0 MB 0.9 MB 0.0 MB 0.0 MB 1.6 MB
	(圖2) 阿络服务 要添加或删除某个组件, 清单击旁边的复选框。灰色标 部分。要查看组件内容, 请单击"详细信息"。 网络服务 的子组件 (C): ■ ● HTTP 代理上的 RPC ■ ● Internet 验证服务 ■ ● Windows Internet 名称服务 (WINS) ■ ● Windows Internet 名称服务 (WINS) ■ ● 动态主机配置协议 (DHCP) ■ ● 简单 TCP/IP 服务 ▼ ● 域名系统 (DNS) 描述: 允许 RPC/DCOM 通过 Internet 信息服务器 (D	区 王 王 王 王 王 王 王 王 王 王 王 王 王
	(圖2) 阿络服务 要添加或删除某个组件,请单击旁边的复选框。灰色都分。要查看组件内容,请单击"详细信息"。 网络服务 的子组件 ©): ■ Uniternet 验证服务 ■ Internet 验证服务 ■ Internet 验证服务 ■ Nindows Internet 名称服务 (WINS) ■ Dissipation	▲ 建表示只会安装该组件的一 0.0 MB 0.0 MB 0.9 MB 0.0 MB 0.0 MB 1.6 MB 1.6 MB 1.6 MB 1.5)的 HTTP 进行通讯。
	(圖2) 阿络服务 要添加或删除某个组件,请单击旁边的复选框。灰色都分。要查看组件内容,请单击"详细信息"。 部分。要查看组件内容,请单击"详细信息"。 网络服务 的子组件(C): ● HTTP 代理上的 RPC ● ● HTTP 代理上的 RPC ● ● Internet 验证服务 ● ● Internet 指示 ● ● Internet 验证服务 ● ● Internet 值息服务器(0) ● ● Internet 信息服务器(0)	区 区 区 区 区 区 区 区 区 区 の の MB 0.0 MB 0.9 MB 0.9 MB 0.0 MB 0.0 MB 1.6 MB ↓ (IS)的 HTTP 进行通讯。
	(圖2) 网络服务 要添加或删除某个组件,请单击旁边的复选框。灰色都部分。要查看组件内容,请单击"详细信息"。 部分。要查看组件内容,请单击"详细信息"。 网络服务 的子组件(C): ● ● HTTP 代理上的 RFC ● ● Internet 验证服务 ● ● Internet 验证服务 ● ● Internet 验证服务 ● ● Windows Internet 名称服务(WINS) ● ● 动态主机配置协议(DHCP) ● ● 简单 TCP/IP 服务 ● ● 域名系统(DNS) 描述: 允许 RPC/DCOM 通过 Internet 信息服务器(DI 所需磁盘空间: 0.7 MB 可用磁盘空间: 6979.6 MB 确定	区 王 王 王 王 王 王 王 王 王 王 王 王 王

步驟 2 安裝 Active Directory	Active Directory 安装向导 🛛 🔀	
安裝完 DNS 以後,就可以進行	这些使用 Active Directory 安装向	
提升操作了·先點擊"開始—運		
行" ,輸入"Dcpromo" ,然	此向导会帮助您在这台服务器上安装 Active Directory 服务,使其成为域控制器。	
後回車就可以看到		
"Active Directory 安裝嚮導"		
直接下一步就可以了(圖1)		
這裡是一個相容性的要求,	加里你是第一次安装 Active Directory,建议你先问	
Windows 95 及 NT 4 SP3 以前	读 Active Directory 帮助里的概述。	
的版本無法登陸運行到		
Windows Server 2003 的網域	要继续,诸里击"下一步"。	
控制站,我建議大家儘量採用		
Windows 2000 及以上的作業		
系統來做為用戶端。然後點擊	<上一步(12) 下一步(12) 取消	
"下一步" (圖 2):	(圖1)	
在這裡由於這是第一台網域控	Active Directory 安装肖导 🗙	
制站,所以選擇第一項:"新域的	操作系统兼容性	
網域控制站",然後點"下一	Windows Server 2003 中改进的安全设置会影响以前版本的 Windows。	
步" (圖3):		
既然是第一台域控·那麼當然也	运行 Windows Server 2003 的域控制器使用的安全设置要求客户端和其他服务器用更安全的方式与域控制器进行通讯。	
是選擇"在新林中的域" (圖		
4):	一些旧版本的 Windows (包括 Windows 95 和 Windows NT 4.0 SP3 或更早版 木)不满足过此要求,同样,一些非 Windows 系统(包括 Apple Mac OS X 和	
在這裡我們要指定一個功能變	SAMBA 客户端)可能不满足这些要求。	
數名稱,我在這裡指定的是		
test.com(圖 5),	有关更多信息,请参阅兼容性帮助。	
這裡是指定 NetBIOS 名 · 注意		
千萬別和下面的用戶端衝突,也		
就是說整個網路裡不能再有一		
台 PC 的電腦名叫"test", 雖	< 上一步 (B) (下一步 (D) 7) 取消	
然這裡可以修改,但建議還是採		
用默認(圖 6)。	(圖2)	
在這裡要指定 AD 資料庫和日誌		
的存放位置·如果 C 盤的空間足		
夠的話·建議採用默認(圖7)。		
這裡是指定 SYSVOL 資料夾的		
位置·沒有特殊情況·不建議修		
改(圖 8):		
第一次部署時總會出現上面那		

```
Active Directory 安装向导
                                                                  X
個 DNS 註冊診斷出錯的畫面,
                        域控制器类型
主要是因為雖然安裝了 DNS,
                          请指定想要此服务器担任的角色。
但由於並沒有配置它,網路上還
沒有可用的 DNS 伺服器 · 所以
                          您想要此服务器成为新域的域控制器还是现有域的额外域控制器?
才會出現回應超時的現像,所以
                          · 新域的域控制器 (D)
在這裡要選擇:"在這台電腦上
                            选择此选项来创建新子域、新域树或新林。此服务器将成为新域中的第一
个域控制器。
安裝並配置 DNS,並將這台
                          ○ 现有域的额外域控制器 (k)
DNS 伺服器設為這台電腦的首
                           ▲ 用这个选项来处理将会删除所有在这个服务器上的本地帐户。
選 DNS 伺服器" (圖 9)。
                              所有密钥将被删除,应该在继续之前将密钥导出。
"這是一個許可權的選擇項,在
                             所有加密的数据,如 EFS-加密文件或电子邮件,应该在继续之前解
密,否则它将永远无法访问。
這裡,選擇第二項:"只與
Windows 2000 或
Window 2003 作業系統相容的
                                             < 上一步(B) 下一步(B) >
                                                              取消
許可權"·因為在上述實驗的整
個環境裡·並沒有
                                           (圖3)
Windows 2000 以前的作業系
                      Active Directory 安装向导
統存在"(可根據需要)(圖10)
                        创建一个新城
                          诸选择要创建的域的类型。
這裡是一個重點,還原密碼,設
置好以後一定要記住這個密
                          创建一个新的:
碼,因為關於活動目錄恢復需要
                          · 在新林中的域(0)]
                            如果这是您单位的第一个域或您想让新域完全独立于您当前的林,请选择这个选项。
用到這個密碼(圖11)。
這是確認畫面(圖12),請仔
                          ○ 在现有域树中的子域(C)
                            如果您想让新城成为现有域的子城,请选择此选项。例如,您可创建一个
細檢查剛剛輸入的資訊是否有
                            名为 headquarters example microsoft com 的新域作为
example microsoft com 域的子域。
誤·尤其是功能變數名稱書寫是
否正確,如果有錯誤的話可以點
                          C 在现有的林中的域树(M)
                            如果您不想使新城成为现有城的子城,请选择此选项。这将创建一个与现
上一步進入重輸·如果確認無誤
                            有树分开的、新的域树。
的話,那麼點"下一步"就正式
開安裝了(圖13):
                                             < 上一步(8) 下一步(8) >
                                                              取消
幾分鐘後·安裝完成·有時可能
要久一點,特別是 DNS 服務時
                                           (圖4)
可能會慢點。
點完成
點"立即重新啟動"。(見圖 14
和圖 15)
然後來看一下安裝了 AD 後和沒
有安裝的時候有些什麼區別,首
先第一感覺就是關機和開機的
速度明顯變慢了,再看一下登陸
```

○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	Active Directory 安装向导 🛛 🗙
「面(画10) 多出了一個"登陸到"的選擇 框·進入系統後·右鍵點擊"我	新的域名 请指定新域的名称。
的電腦"選"屬性" · 點"電 腦" (圖 17)	为新域键入一个 DNS 全名(GD: headquarters.example.microsoft.com)。 新域的 DNS 全名(2):
這樣就把普通一台 2003 Server	test. com
升級成網域主控站(DC)	R
	<上一步(B) 下一步(B) > 取消
	(圖5)
	Active Directory 安装向导 🔀
	WetBIOS 域名 请指定新域的 WetBIOS 名称。
	这个名称是早期 Windows 版本的用户用来识别新域的。单击"下一步"接受显示的名称,或输入新名称。
	域 NetBIOS 名 (D): 问题 人
	<上一步(2) 下一步(2) > 取消
	(圖6)

Active Directory 安装肖导	×
数据库和日志文件文件夹 请指定放置 Active Directory 数据库和日志文件的文件夹。	S.
基于最佳性能和可恢复性的考虑,诸将数据库和日志存放在	不同的硬盘上。
您希望在哪里保存 Active Directory 数据库? 数据库文件夹 Q):	
C. WIRDOWS WITDS	利死 (E)
您希望在哪里保存 Active Directory 日志? 日志文件夹 ①: C:\WINDOWS\WIDS	浏览 (()
<上一步@)下一:	步(图) > 取消
(圖7)	
(国,)	Y
共学的系统卷 请指定作为系统卷共享的文件夹。	X
SYSVOL 文件夹存放域的公用文件的服务器副本。SYSVOL 文件 到域中的所有域控制器。	半 夹的内容被复制
SYSVOL 文件夹必须在 NTFS 卷上。	
请输入 SYSVOL 文件夹的位置。	
文件夹位置(2):	
C: \WINDOWS\SYSVOL	浏览(B)
<上一步® 下一步	「(近) > 取消
(圖8)	

Active Directory 安装向导
DWS 社册诊断 确认 DWS 支持,或在此计算机上安装 DWS.
诊断失败
注册诊断已经运行 1 次。
警告: Active Directory 的 DWS 结构未正确配置之前,域控制器功能(如
此向导在确定此域控制器将要与其注册的 DMS 服务器是否支持动态更新时 遇到了一个错误。
○ 我已经更正了错误。再次执行 DNS 诊断测试(E)。
○ 在这台计算机上安装并配置 DNS 服务器,并将这台 DNS 服务器设为这台 计算机的首选 DNS 服务器(S)。
○ 我将在以后通过手动配置 DNS 来更正这个问题 (C)。(高级)
(圖9)
Active Directory 安装向导 X
积限 请选择用户和组对象的默认权限。
 一些服务器程序,如 Windows WT 远程访问服务,可读取域控制器储存的信息。 ○ 与 Windows 2000 之前的服务器操作系统兼容的权限 (E) 如果在 Windows 2000 之前的服务器操作系统上运行服务器程序,或在 Windows 2000 或 Windows Server 2003 操作系统上运行服务器程序,该服
● 匿名用户可读取这个域的信息。
• 只与 Windows 2000 或 Windows Server 2003 操作系统兼容的权限(图)
如果仅在 Windows 2000 或 Windows Server 2003 操作系统上运行服务器 程序,该服务器又是 Active Directory 域的成员,请选此选项。只有经 过验证的用户才能读取这个域的信息。
<上一步(B) 下一步(B) > 取消
(圖10)
(圖10)

Active Directory 安装向导 X
目录服务还原模式的管理员密码 该密码在"目录服务还原模式"下启动计算机时使用。
输入并确认您要分配给管理员帐户的密码。该帐户是该服务器用目录服务还原 模式启动时使用的。 还原模式管理员帐户与域管理员帐户不同。帐户的密码可能不同,所以一定要 记住两个帐户的密码。
还原模式密码(E): ******
· 确认密码 (C): 以****** 有关目录服务还原模式的详细信息,诸参阅 <u>Active Directory 帮助</u> 。
< 上一步 (g) 下一步 (g) > 取消
(圖11)
Active Directory 安装向导
摸要 请复查并确认选定的选项。
您选择 ①: 将这个服务翻配置成新域林中的第一个域控制器。 新域名将为 test.com。这也是新林的名称。 域的 WetBIOS 名将为 TEST 数据库文件夹: C:\WINDOWS\NTDS 日志文件文件夹: C:\WINDOWS\NTDS SYSVOL 文件夹: C:\WINDOWS\NTDS SYSVOL 文件夹: C:\WINDOWS\SYSVOL 将在这台计算机上安裝并配置 DNS 服务。将配置这台计算机使用此 DNS 服务器作为其首选 DNS 服务器。
< 上一步(1) 下一步(1) 取消 (圖12) (圖12) (目12) (日12) (12) (12) (12) (12) (12) (12) (12) (

Active Directory 安装向导
向导正在配置 Active Directory。根据您所选的选项,此过程可能要花几分钟或更长时间。
(圖13)
Active Directory 安装肖导 🛛 🔀
< 上一步(E) 完成 取消
(圖`14)
Active Directory 安装向导 🛛 🔀
必须重新启动 Windows, Active Directory 安装向导所做的改 动才能生效。 立即重新启动(E) 不立即重新启动(D)
(圖15)

登录到 Windows
Copyright © 1985-2003 Microsoft Corporation
用户名 (Ψ): Administrator 密码 (ℙ): ******* 登录到 (ℙ): TEST ● 使用拨号网络连接登录 (Ψ) ● 確定 取消 关机 (S) 选项 (Ψ) ((圖 16) 室 11 (圖 16) </th
第38 11400-0 岐中 画成 日本の更新 1244 Windows 使用以下信息在网络中标识这台计算机。 计算机描述 ①: 举例: "IIS Production Server" 或 "Accounting Server". 完整的计算机名称: www=f4b3ffc2001 test.com 域: test.com 要重新命名此计算机或加入域,单击 "更改"。 更改 (2)
(圖17)

6.3.1.2 新增 AD 用戶



xr (ビ): 」 」 が加 名(P): 本文編写(T):	
あいり エリ ひろう しい しんしょう しんしょ しんしょ	
strated (a). John	
用户登录名(U): John	N
目白谷曼名 (Windows 2000 以前版本) (W)・	43
TEST\ John	
	_
(圖3)	
新建对象 - 用户	×
-	
创建在: test.com/Users	
▲ 密码(E):	
▲ 密码(E): 離认密码(C): ******	
 密码 (ℓ): 部***** 确认密码 (ℓ): ****** □ 用户下次登录时须更改密码 (ℓ) □ 用户下次登录时须更改密码 (ℓ) 	
 ▲ 密码 (2): #***** 确认密码 (2): #***** □ 用户下次登录时须更改密码 (2) □ 用户不能更改密码 (2) □ 亦昭永 无計期 (2) 	
 密码 (£): [******] 确认密码 (£): [****** □ 用户下次登录时须更改密码 (£) □ 用户不能更改密码 (£) ☑ 密码永不过期 (£) □ 帐户已禁用 (0) 	



控制委派向导	×
用户和组 选定一个或多个您想委派控制的用户或组。	8
進定的用户和組 (S):	
添加(2) 册除(8)	
<上一步④ 下一步 ④ ▶ 取消	
(圖3)	
选择用户、计算机或组	×
选择对象类型 (<u>S</u>):	
用户、组或内置安全主体 对象类型 (0)	
查找位置 (2):	4
[test.com]位置①	1
输入对象名称来选择 (<u>示例</u>) (E):	4
John 检查名称 (C)	
高级(4) 職定 取消	
(圖4)	

控制委義向导
用户和组 选定一个或多个您想要派控制的用户或组。
选定的用户和组(S):
🖉 John (John@test.com)
凝加(<u>()</u> ,) 删除(<u>()</u>)
〈上一步 @) 下一步 @) 》 取消
(圖5)
控制委派向导
要委派的任务 您可选择常见任务或自定义您自己的任务。
 ● 委派下列常见任务 (2):
 □ 创建、删除以及管理用户帐户 □ 重设用户密码并强制在下次登录时更改密码 □ 读取所有用户信息 □ 修改组成员身份 ☑ 将计算机加入到域 □ 管理组策略链接 □ 生成策略的结果集(i+t处)
○ 创建自定义任务去委派 (C)
<上→步(2) 下→步(2) > 取消
(圖6)



6.3.1.3 讓 Windows 20 00/XP/2003/V 設備 ta 的 PC 使用新增的 AD 帳號登入 AD 網域

步驟1 設定網路屬性	Internet 协议 (ICP/IP)	属性 🛛 🛜 🔀
案例中採用的用戶端作業系統是	常规	
Windows XP 專業版(其他 windows 系統類似) · 需要大家注意的是	如果网络支持此功能,则可以获取自动指派的 IP 设置。否则, 您需要从网络系统管理员处获得适当的 IP 设置。	
的是家庭用戶·所以不能加入域·我	○ 自动获得 IP 地址 @)	
們先來設置一ト這台 XP 的網路(圖	· () 使用下面的 IP 地址(S): -	
1):	IF 地址(L):	
	子 附 掩 ሣ ① :	255 .255 .255 . 0
電脑石: MICROSOT-D5C461	默认网关 @):	192 .168 . 18 . 1
IP:192.168.18.72	○ 自动获得 DMS 服务器地址(<u>b</u>)
	●使用下面的 DNS 服务器地址	± œ:
子網路遮罩:255.255.225.0	首选 DNS 服务器 (P):	192 .168 . 18 .190
	备用 DNS 服务器(A):	
DNS 伺服器:192.168.18.190		
		高级 (1)
	(圖 1)
步驟 2 更改為域用戶	计算机名称更改	? 🔀
· 在"我的電腦"上擊右鍵·選"屬 性" · 點"電腦名" 。	可以更改这台计算机的名称 对网络资源的访问。	和成员身份。更改可能会影响
在這裡把"隸屬于"改成域,並輸 入:"test",並點確定(圖2),這 是會出現如下畫面(圖3): 輸入剛剛在域控上有許可權的帳 號,一般帳號是"Admin 設備 trator",密碼就填入它的密碼,點 確定: 出現上述畫面就表示成功加入了,然	计算机名 (C): microsof=b5c461 完整的计算机名称: microsof=b5c461. 隶属于 ④ 域 (D): test	其它 @)
後點確定(圖4)·點重啟就算 OK 了。	〇工作组 (W): WORKGROUP	 确定 取消

InstantScan User Manual

	(圖2)		
	计算机名更改 @② **		
	请输入有加入该域权限的帐户的名称和密码。		
	用户名(U): 💽 Administrator 💽 📉		
	密码(P): ******		
	计算机名更改 ×		
	文迎加入 test 域。		
	[确定]		
	(圖4)		
步驟 3 登錄 AD 網域	登录到 Windows		
來看一下登陸畫面(圖1): 美到那個"發味到"了四一司以聯擇	Microsoft-		
看到那個 豆陸到 」吧,可以選择 域登陸還是本機登陸了,在這裡選擇	Windows ^{xp}		
域"TEST" ·這樣就可以用域用戶	Copyright © 1985-2001 Microsoft Microsoft		
進行登陸了。進入系統後·在"我的			
電腦"上擊右鍵,選"屬性",點			
电烟石 (回2). 就這樣田后端已經加入到城。			
	MICROSOF-B5C461 (本机)		
	CH 确定 取消 关机 (S) 选项 (D) <<		
	(圖1)		

You make in the formation of t	Windows 使	用以下信息在网络中标识这台计 算机。
完整的计算机名称: microsof=b5c461.test.com 域: Lest.com 要使用网络标识向导去加入域并创建本地用户帐 网络 ID (A) 要重新命名此计算机或加入域,单击 "更改"。 更改 (C) 注意: 只有管理员才可更改此计算机的标识。		举例: "Kitchen Computer" 或"Mary's Computer"。
域: Lest. com 要使用网络标识向导去加入域并创建本地用户帐 网络 ID (0) 户,请单击"网络 ID"。 要重新命名此计算机或加入域,单击"更改"。 更改 (c) 要重新命名此计算机或加入域,单击"更改"。 更改 (c) 注意: 只有管理员才可更改此计算机的标识。	完整的计算机名称:	microsof-b5c461.test.com
要使用网络标识向导去加入域并创建本地用户帐 网络 ID (1) 要重新命名此计算机或加入域,单击"更改"。 更改 (C) 注意:只有管理员才可更改此计算机的标识。 确定 题) 应用 (4)	域:	test.com
要重新命名此计算机或加入域,单击"更改"。更改 (C) 不过。 注意:只有管理员才可更改此计算机的标识。	要使用网络标识向导- 户,请单击"网络 II	生加入域并创建本地用户帐 网络 ID(W)
注意:只有管理员才可更改此计算机的标识。	要重新命名此计算机	或加入域,单击"更改"。
	 注意:只有管理员才)	可更改此计算机的标识。
確定感到「取消」」		
· · · · · · · · · · · · · · · · · · ·		
		确定

6.3.1.4 於 Management Server 上配置 AD 訊息

步驟 1 配置 AD Import…		
Windows 2003 Server IP: 192.168.18.190		
Mgt Server IP: 192.168.18.45		
Mgt Server OS: Windows XP profession	File Undate Tools Help	
Device IP:192.168.18.92	🗅 🛃 🖸 Custon Report 🛐 Batch Export 🖀 AD Inport 🕼 Vpload Config	
子網路遮罩:255.255.225.0		



	🖗 Opnamic Objects 🖓 Dynamic Groups
這時候可以看到設備顯示	pSessiption-
中從 AD SERVER 抓到的 AD 的相	Mastruise can use jeccount or (proup) as a pondition or entities the policy Accounts come from
国次司。	1. After users into a nAP, before will execute a con-declingic acciptional the centre which P the account belongs to
鬧貝 	2. Users are redirected in the weaking in range of the device to tell the device which IP the account be on us to
請點擊 "Download	Draups come Frant
login.vbs and	1 After users loss in AD, heisne will execute a provided login ac pillo tall the centre which IP the account belongs to
adclient.exe",然後請把這兩	🦗 Dynamis Objecte
個檔保存好以便在接下來的步	(今) 副 Accounts (
驟中使用。	A Duest (Guest)
	▲ .bogt(.bogt)
點 Finsn 元成。	a a contra
這時設定已經結束,可以看到	- Weccon Contains
account 和 group 下已經抓取到	- W Backup Operators - W deit Publishers
的 ad server 的相關帳號資訊	왕 Disabuted DTM Users. - 양 DisAdmins
(圖 4)。	優 DinsUpdateProor 一般 Domein Admine
	∲ Comain Computers → ∲ Comain Controllers
	- 🖗 Coman Guesta - 🖗 Coman Users
	- 🖗 Emerpi se admina
	23Al leport
	(圖4)
	AD Import - Step 3/3
	Detecting
	Created 31 group(s).
	Skipped 1 group(s).
	Created 9 user(s).
	Skipped 1 user(s).
	Install login.vbs and adclient.exe on AD server
	Read installation guide
	Download login.vbs and adclient.exe
	< Back Next > Finish Cancel
	<pre>Sack Next > Finish Cancel</pre>
	(Back Next > Finish Cancel)

6.3.1.5 安裝登入 script 至 AD Server

步驟1 下載準備放到 AD Server 的檔案 假設您的AD server IP為 192.168.18.200・若您用AD的 administrator登入・您將有權 限把打開 \\192.168.18.200\netlogon\ 目錄裡。	 執行 輸入程式、資料夾、文件或網際網路資源的名稱,Windows會自動開啓。 開啓(①): M192.168.18.200/metlogon 確定 取消 瀏覽(B)
步驟2將adclient.exe放到 AD Server 若您用AD的administrator登 入・您將有權限放檔案進該目 錄。請 <u>按這裡</u> 下載adclient.exe 程式・透過網路放到 \\192.168.18.200\netlogon\ 目錄裡。	








步驟 11 確認 script 內容	■ login.vbs - 記事本 × 檔案(E) 編輯(E) 格式(O) 板視(V) 説明(H)
請確認script內容,在兩個紅框	option Explicit Dim objNetwork, objShell, objExec Dim styleer
處是否正確填入您的AD	<pre>' Create the network object = objNetwork Set objNetwork = CreateObject("wScript.Network")</pre>
Server IP與您的Mgt Server IP。若無誤誌方標。	' Get the user name. ' Anticipate that on windows 98, the user may not be logged on. strUser = objNetwork.UserName
1. 石 流跃的 行 油	' Here is the Do While Loop Do While struser = "" Wscript.Sleep 2000 ' Two Seconds struser = objNetwork.UserName Loop
	' Note the concatenation of strUser with ampersand
	'WScript.Echo "user name = " & strUser
	Set objShell = CreateObject("WScript.Shell")
	Set objExec = objShell.Exec("\192.168.18.200\hetlogon\adclient2.exe 192.168.18.111" & strUser
	Do while objExec.Status = 0
	wscript.Quit
步驟 12 刷新策略使之立即生	Command Prompt
效	Microsoft Windows L版本 5.2.3790」 <c>版權所有 1985-2003 Microsoft Corp。</c>
存檔過後,在DOS視窗中輸入	C:\Documents and Settings\Administrator>dsa.msc
GPUPDATE /FORCE以便更新	C:\Documents and Settings\Administra <mark>;or>GPUPDATE /FORCE</mark> 正在重新整理原則
策略·使剛才設定的策略能夠立 即生效。	使用者原則重新整理已完成。 電腦原則重新整理已完成。
	如果要檢查原則處理中的錯誤,請檢視事件日誌。
	C:\Documents and Settings\Administrator>

6.3.1.6 設定 device

步驟 1 設定 device AD Server IP : 192.168.18.190 Mgt Server IP: 192.168.18.45	InstantScan# sys ad ip Show/Set AD server address poll Poll all AD records from AD server show Show AD mapping information InstantScan#
Device IP: 192.168.18.92	InstantScan# sys ad ip Show/Set AD server address

poll Poll all AD records from AD server
show Show AD mapping information
InstantScan# sys ad ip 192.168.18.45
主要功能:當Device有重開機時 · 可由AD Log Server上 · 抓取以登入AD Domain
人員資訊
InstantScan# sys ad poll
手動連線AD Log Server抓取登入AD Domain人員資訊
InstantScan# sys ad show
列出目前以對應之AD Domain Users資訊,可在後面加掛IP或User Account · 單獨列
出資訊

6.3.1.7 將 Windows AD client 重新登入 AD,並以 sys ad show 觀看是否成功

步驟1AD Client 登錄 AD 網域	InstantScan# sys ad show NO. IP ADDRESS AD ACCOUNT USERNAME GROUPS
用戶端 IP:192.168.18.72	1 192,168.18.1 nestlin XXXXX8104 <rdrdrd> 2 192,168.18.72 John John John Onnain Users></rdrdrd>
Device IP:192.168.18.92	InstantScan# (圖 1)
│ 把上述 26.3.1.3 節中用戶端 PC	
接到設備 INT 埠下·EXT 埠接到	
與 AD Server(本案採用的是	
Windows 2003 Server)同一交	
換機上·並重新啟動用戶端登錄	
至域,然後用	
Console/SSH/Telnet 連到設備	
命令列 · 敲入 sys ad show (圖	
1) :	
可以看到設備已經能獲取到用	
戶端登錄的資訊。	



6.3.2 讓報表中對應到 AD 用戶名

6.3.2.1 於對象管理->動態物件, 匯入 AD Server 上所有用戶帳號與名稱



6.3.2.2 於 L4/L7 策略的規則裡,指定 AD 使用者

步驟1 於 L4 策略裡指定 AD 用	Functions > Traffic Manager > L4 Policy>Policy
戶	
點選 L4 Policy · 新增一條	
Rule [,] 在Internal IP 或 Exteranl	
IP 裡選擇 AD 用戶	

	稿 Status 篇 Policy	
	Apple actions in searched uses allowed	
	String in Sector Adam Pice	
	NO Scredule R, le Namo normal P Erizma P Service Security Profile Pice	
	1 🕅 Alvays Fuls_1 🕴 John (Jenn) 🛃 smi 🔛 vins 🗖 Alber 🖗 settut, ope	
	TE DOWN	
步驟 2 於 L7 策略裡指定 AD 用	Functions > Traffic Manager > L7 Policy>Policy	
Б	Statu: Statu:	
<i>F</i>	Elerr Cher and Alerra - Activations Lasiscentralis stone	
點選 L7 Policy · 選擇一條	Kowati	
Pule.在Internal ID 戓 External		
	Fv0. Constant France Bchecula Rula Name Internal P Edam. Protocol Socurity Profile Place	
IP 裡選擇 AD 用戶	👔 (Sanki), HBN, Suis (🚺 Jahns, 🥵 are 👍 Crassis VizBor) Han Hrands/Scimi 👩 Sick & Eq. 🧭 Satur, ppo	
	27 [139]	
	استنتب يبتنيه	

6.3.2.3 於 Content 策略規則裡,手動指定 AD 用戶或 AD 群組

步驟1點選Content Policy頁	Functions > Content Manager > Content Policy>Policy
面	
在 "Content Manager" 的	
"Content Policy" 策略規則裡	
面,可以手動添加 AD 用戶或者	

人 D 世纪立进行答响的答理	盤 Sistu	· 益 Fulty 益.	Acaum									
AD 辞組來進1] 束哈的管理	List	Virtual Group	Ŷ	1% Frefle	e l	tileb P offic	v	1		-	Seurch	
	epoty	-Schedule-	¥		cup-	- M Ptofile-	-	Web Frofile-		ic listed		
			alus	Theologic Concerning	Condition		-	5.00	ei.			
	P.O.	Sthedu e	F	Rule Name	Name	19 Frofile	-	Web Pr	ofic	- 41	tual Groups	
		atwaya	Cef	aut User	DefaultUser	Pistinum	i.	Flato	.01		Cihars	
牛踙 2 五位一体空吹	Euro	tions		tont	420200	The look large	rt	Policy S	met] • • :	ile Experi-	
少職 2 利垣—除束昭	Func	uons > (201	tentin	lanage	r > Conte	int P	oncy>	-0110	-у		
在"Content Policy"裡	1 Statur	s B Polty A	Action						_		1	
	List	Virtual Broup	*	-It: Frofie	H. Y		~		-		Saurch	
"POIICY" 選項卞的貝囬點石鍵	Apri-	Schedule	~	-Vitual O	10.p 👻	IM Profile	۲ -	Web Frofile	4	tr isted		
→ "New User"	140.	9	at.a		Condition	WEAR		Act	in .	1 3	ratual Alexand	
	1	Schedule	Def	Hule Name	Defaultiter	Di Picita Pisticui	e 0	Ateb i	2016	-	Otxers	
					400 Edd Date	Use JCot 9 User 22 All						

上頭 기 수 하는 다 이 머니	demand											
步職 3 手動指定 AD 用户												
Name 這個欄位就是我們可以	Edituser											
手動指定 AD 帳號的地方·在這裡我們填上了在 AD Server 上	Schedule : Basic —	👹 Always	~	Virtual Group :	Others	•						
創建的 AD 帳號 John · 下麵分 別是對各種許可權的設定(見圖 1 在次不在複述 · 詳細請見設備	Rule name : The Name field (Rule name : rule_1 Name : John The Name field could be AD account, AD group, or Web Login account.										
應用手冊),然後點 Fin 設備 h 後,一條 AD 帳號為 John 的策 略便加好了(見圖 2)。 匯入 AD 群組也是一樣,在 name 欄位填入 AD 群組的名稱 就可以了	IM	⊙ En ○ En	able	 Disable Disable 								
	MSN Account :	Block	~									
	Yahoo Account :	Allow	~									
	AOL Account :	Allow	*									
	ICQ Account :	Allow	*									
	IM Service :	Platin	Im			*						
	Web —— URL Rec : Web POST :	⊙ En Allow	able	O Disable								
	Web Service :	Gold	Gold									
	-	Finish Cancel										
	(圖 1)											
	NO	tatus	Condition		Action	1						
	Schedule 77. User	Rule Name	Name	IM Profie Philippe	Web Prof Protoco	le Virtual Groups						
	and a second second	1000-1	all the second s	(Prongodit)	r tansitits							

6.3.2.4 於 Content 策略規則裡,自動匯入所有 AD 帳號

步驟1 點選 Content Policy 頁	Functions > Content Manager > Content Policy>Policy
面	
在 "Content Manager" 的	
"Content Policy" 策略規則裡	
面,可以自動添加 AD 用戶和者	
AD 群組來進行策略的管理	

上は 地域ののの、 上目 FredTo 「Web P at e () E ouch	List Virtual Group	Gruch
参加	Apply -Schedule -Virtual Group -MiPtohe -Virtes Frotile Mit isset 1:0. Status Construct Aption Aption Aption 1:0. Status Construct Name Name Aption Aption 1:0. Status Rule Name Name Ibit Frotile Viet Frotile Viet Frotile Viet Frotile Viet Frotile 1:0. Status Default User DefaultUser Pistinum Pistinum Pistinum	A Annual second second second
	Status Condition Arbon 1:0. Schodule Rule Name Name Extension Via Schodule Rule Name Name Extension Via Via Schodule Rule Name Defaultuser Defaultuser Pistnum Pistnum	
PlateName Name Name Name Name Vieferfie View Point View 0 0.00 mg PlateName Charge PlateName Name Name Vieferfie View Point View 0.00 mg PlateName Charge PlateName PlateName PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Charge PlateName Plat	Schodule Rule Name Name Ust Profile Vec: Profile Value W stwars Default User DefaultUser Platnum Platnum Platnum	
Plathauth Joan Schutz	Sit stores Default. Jser Default. Jser Pistnum Plain.m.	tua Groups
步驟2 導入 AD 帳號 Functions > Content Manager > Content Policy > Policy 在 "Content Policy" -> "Policy" 選項卡頁面的右下 角·點選 "AD Book Import" Functions > Content Manager > Content Policy>Policy		Ciners
步驟 2 導入 AD 帳號 在 "Content Policy" -> "Policy" 選項卡頁面的右下 角・點選 "AD Book Import" Functions > Content Manager > Content Policy> Policy 超 2 端の 2 次 () 逆 ()		
步驟2導入AD帳號 Functions > Content Manager > Content Policy > Policy 在 "Content Policy" -> "Policy" 選項卡頁面的右下 角·點選 "AD Book Import" Functions > Content Manager > Content Policy > Policy		
步驟2導入AD帳號 Functions > Content Manager > Content Policy > Policy 在 "Content Policy" -> "Policy" 選項卡頁面的右下 角·點選 "AD Book Import" Functions > Content Manager > Content Policy > Policy		
・ 参加 ・ 参加 ・ 参加 ・ 参加 ・ 参加 ・ かいの ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		
步驟 2 導入 AD 帳號 在 "Content Policy" —> "Policy" 選項卡頁面的右下 角・點選 "AD Book Import" Functions > Content Manager > Content Policy> Policy 【はないの シーク "ソンロ ロンロー 「ジェンロー 「シーン 「シーン 「ジェンロー 「シーン 「シー 「シーン 「シー		
参照 2 導入 AD 帳號 在 "Content Policy" ー> "Policy" 選項卡頁面的右下 角・點選 "AD Book Import"		
步驟 2 導入 AD 帳號 在 "Content Policy" -> "Policy" 選項卡頁面的右下 角・點選 "AD Book Import" Functions > Content Manager > Content Policy > Policy 地設 型型型 単位化の目的 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		
步驟 2 導入 AD 帳號 在 "Content Policy" -> "Policy" 選項卡頁面的右下 角・點選 "AD Book Import" Functions > Content Manager > Content Policy > Policy 通いの意味を見ないので、 「別をしたいので、 「別をしたいので、 「別をしたいので、 「別をしたいので、 「別をしたいので、 「別をしたいので、 「別をしたいので、 「別をしたいので、 「別をしたのでは、 「別をしたのでは、 「別をしたのでは、 「別をしたのでは、 「別をしたので、 「別をしたので、 「別をしたので、 」 「別をしたので、 「別をしたので、 」 「」 「」		
歩驟 2 導入 AD 帳號 在 "Content Policy" —> "Policy" 選項卡頁面的右下 角・點選 "AD Book Import"		
プロ Book Import		
プロ Book Import		
步驟 2 導入 AD 帳號 在 "Content Policy" —> "Policy" 選項卡頁面的右下 角・點選 "AD Book Import"	🛱 D Rock Leport 🕀 Film Leport 🕀	ils Egeri
步驟 2 導入 AD 帳號 在 "Content Policy" —> "Policy" 選項卡頁面的右下 角·點選 "AD Book Import"		
在 "Content Policy" —> "Policy" 選項卡頁面的右下 角·點選 "AD Book Import"	步驟2 導入 AD 帳號 Functions > Content Manager > Content Policy>Policy	
在 "Content Policy" —> "Policy" 選項卡頁面的右下 角・點選 "AD Book Import"	Particular Status	
"Policy" 選項卡頁面的右下 角・點選 "AD Book Import" Ut virtus @ dop virt	在 "Content Policy" —>	10
POlicy 医項下貝面的右下 角・點選 "AD Book Import" No. <u>Elators Contract Meternal Structure Puterhame harre IMPerfie Web Profile Unit.al Omuss</u>	"Dolior" 避頂上百面的左下	Gord
角・點選 "AD Book Import" No. Elsous Confition Actor Actor Ac	POIICY 进境下員回的右下 Appy Bithetule: Y Yinua Goup Y Normalie: Y Yinua Profile: Y Yinua Pro	
1 🙀 -Ways Defaul User Defaul User Fleinum D. Id Others		d st@murs
	角·點選 "AD Book Import"	rar conta a
	角·點選 "AD Book Import" Actor Constant Putersanta Dentition Actor Actor Actor Actor Actor	Others
	角・點選 "AD Book Import" A Growting Puter Lange Default User Defaul	Others
	角・點選 "AD Book Import" ACtor Turing Constant Constant Not Actor Turing Putertume Name Internate State Turing Putertume Constant User Ortanit.user Flainum Const Turing Putertume Constant User Ortanit.user Flainum Const	Others
	角・點選 "AD Book Import" ACtor Floredule Pute trame transe inter-training State 1 鍵 Aways Defaul User DefaultUser Floren Containing State	Others
	角・點選 "AD Book Import" ACtor Furredule Pute trame Darre IMPortite Web Partie 1 鍵 Avarys Defaul User Defaul	Others
	角・點選 "AD Book Import" NO Elabor Overland No. No. Elabor No. No. No. Elabor No.	Differe
	角・點選 "AD Book Import" NO Elabor Ounitation Notion Storedule Puls trame Date IMPorts View Prints (1) 鍵 Always Default.laser Fleinum Octa	Differe
	角・點選 "AD Book Import"	Differe
	角・點選 "AD Book Import"	Differe
	角・點選 "AD Book Import"	Differe
	角・點選 "AD Book Import"	Differe
	角・點選 "AD Book Import"	Differe
	角・點選 "AD Book Import"	Differe
	角・點選 "AD Book Import"	Differe
	角・點選 "AD Book Import"	Differe
	角・點選 "AD Book Import"	Differe



6.4 實用範例

6.4.1 公司 A 部門人員架構

6.4.2 AD 導入方案

26.3.4.2.1 AD Group 屬 RDGROUP 者 · 上班不得用 MSN · 下班雖可用但要側錄對話並過濾關鍵字

26.3.4.2.2 AD 帳號為 John 者,所有時間都要過濾 Web 使用,包括新聞、運動、自訂 URL

26.3.4.2.3 IP 位址為 192.168.18.20~192.168.18.30 者,不作任何過濾

26.3.4.2.4 使用虛擬群組,將側錄資料以 AD 群組方式顯現

詳細步驟

步驟1選擇 Static-→Schedule-→Object	Fund		tatic	>Sch	edul	e>Ob	oject					
	NO.	Name	Sun	Non	- tue	Wed	152	E:	<u>а</u> я.	Stattime	Stor: Time	
	10	Horning		0	4	•	0	6		09.30	12.00	
		Aternoon		Q	Q	Q.	0	0		13.00	17:20	
步驟 2 添加時間策略 在這裡‧我們添加了時間策略	Fund Starter	ctions > S dress 🏠 Sched	tatic	>Sch	edul	e>Ob	ject					
worktime 作為上班時間	NO.	Name	8	un	Mon	Tue	Wed	T	u l	Fri S	at Start T	me Stap Time
	4	Noming			0	Q	0		0		00:	0 12:00
	z	Attempon			0	0	0		0	0	131	0 17:30
	3	worldime				0	9		•	•		0 18:00

步驟3 導入 AD 帳號 我們需要從 AD Server 上新建 AD 群組 AD GROUP·在這裡我 們新建的 AD 群組名稱是 RDGROUP·並把 AD 帳號 RD 添加至 RDGROUP。 然後在 UI 上點選 "Dynamic" -> "Dynamic Object" -> "AD Import" 導 入所有的 AD 帳號和群組 步驟4 設定上班策略 啟用應用層策略->在 chat 群組 裡面選擇 MSN->Schedule 選 擇 Worktime->Internal IP 選 擇 RDGROUP->Security Profile 選擇 block 或 block&log	Functions > Dynamic > Dynamic Object > AD Import
步驟 5 設定下班策略 5.1.啟用 IM 勾選 Enable IM · 為了防止 IM 透過代理 · 因此最好勾選 IM over porxy	Functions > Content Manager> IM>Status

	🚵 Status 🏥 IM Profiles 🛃 Global Policy 🛃 Options
	Enable IM Manager
	Description IM Manager allows you to manage IM behaviors/contents/peers. Matching priority: 1. Explicitly specified IM account 2. AD name 3. AD group Users out of the schedule will apply the their IM Groups' chosen IM Service.
	Exempt (Source / Destination)
	Functions > Content Manager> IM>Global Policy>IM Content>Chat
在 keywords 裡面有預設關鍵 字 · 並且可自行添加關鍵字	 Status IM Profiles Global Policy Options IM Peers IM Contents IM Security IM Messages Chat File Enable keyword filtering Keywords Sexy Confidential Sexy Cove
5.3 新增 IM 策略	Functions > Content Manager> Content Policy>Policy
在 Content Policy-→Policy 裡	
面右鍵-→New User	
Name 欄位填寫上 RDGROUP	
MSG Rec 欄位選擇 Enable	

點 Finsh 完成。	🛸 New User 🛛 🕅							
至此·3.1.2.1 的過程結束。	Create a new user							
	Schedule : C Always Virtual Group : Others							
	Basic							
	Rule name : rule 1 Name : RDGROUP							
	The Name field could be AD account, AD greater or Web Login account.							
	IM							
	MSG Rec 💿 Enable 🔿 Disable							
	File Rec : O Enable O Disable							
	MSN Account: Allow 🗸							
	Yahoo Account : Allow 🗸							
	AOL Account: Allow							
	ICQ Account: Allow							
	IM Service : Platinum							
	Web							
	URL Rec : O Enable O Disable							
	Web POST: Allow							
	Web Service : Platinum							
	Finish Cancel							
步驟 6 啟用 Web Manager	Functions > Content Manager > Web > Status							
勾選 Enable Web Manger	🚵 Status 🚵 Web Profiles 🚵 Global Policy							
	C Enshie Web Manager							
	C Labor roo Manager							
	Description							
	Web Manager allows you to filter unwanted sites during the office hours.							
	Exempt (Source / Destination)							
	Enable Exempt Sources							
	Exclude RestCEO from the web filter enforcement							
	In the wab hiter antorcement							
步驟 7 添加白訂 web 百面關鍵	Functions > Content Manager> Web>Global Policy>Web site>Custom							
· 在 Custom 百而添加 删除动体								
也 COSTON 只面 小加,								
以川应并的贬丁								



在 "Content Policy"	🛷 New User				
→ "Policy"頁面,右鍵添加一		07274			
」 個 "New User" → NAME 欄位	Create a new us				
填寫 AD 帳號 John · web	Schedule :	🗑 Always 🗠	Virtual Group :	Others	~
service 欄位元填寫步驟 8 中創	Basic —	Look of	-		
建的 "rule_john" 的許可	Rule name :	rule_1	Name :	John	
權,URL Rec 設定為 Enable 即	The Name field	could be AD account, AD	group, or they boy	an account.	
可。	IM				
到這步已經完成 3.1.2.2 的需求·	MSG Rec :	O Enable	 Disable 		
	File Rec :	O Enable	 Disable 		
	MSN Account :	Allow			
	Yahoo Account :	Allow			
	AOL Account :	Allow			
	ICQ Account :	Allow	<u>/</u>		
	IM Service :	Platinum			~
	Web —			6	
	URL Rec :	Enable	O Disable	S.	
	Web POST:	Allow			~
	Web Service :	rule_john			~
					in the second
			1	(rinsh) (salicer
步驟 10 新增 IP 群組	Functions > O	bject Manger> st	atic> Addres	s>Static Obj	ect
在"Object Manger"-→	Allanses 🙆 Schedule 🖉	no-ps			
"static" -> "Address" ->	Descrition				
"Static Object"中右鍵點擊	-opted1" feed1P / bjeck	were do not need to suffect rate			
"static Object" 目錄樹,在彈	Sama La Herconners	Type	P.		
出的右鍵功能表中選擇	HostCED HostCFO HostCFO	dd new Boot Hystur IP and associat			
│ "Add" · 在 name 欄位起一個	HosiCTO	Name [rue_1	CHAN		
有意義的名稱·然後在 IP Type		BintiF 192166.18.20	Citiza -		
│欄位點選 Range,在 Start IP 欄	Schort-TTP Schort-TTP Schort-YSO	C-00 18218-10.0			
位填寫 192.168.18.20,在 End	- Subnet*DM	OK Currel	92165.1.0/24		
IP 欄位填寫 192.168.18.30,點	 SubnetCANCEACTORE SubnetCARCETING SubnetCARCETING 	C Subret 18 C Subret 19 C Subret 19	82 184.5.024 92 188.5.024 92 188.3.024		
ОК •	- E Schrei-U	Subnel 18	82.186.2.024		
步驟 11 排除特定 IP 過濾	Functions > Co	ontent Manager>	IM >Status		
在 IM 和 Web 頁面裡的					
Exampt(Course (Destination)					
exempt(Source/Destination)					

Sources 潠佰,在點潠	Status 👫 IM Profiles 🤲 Global Policy 👫 Options
Sources 医项节正和医 Evoludo, 後面的欄位裡選擇上	
	🖃 Enable IM Manager
処增加的TUIE_I 束哈即可。	
	Description
到這裡·已經完成了 3.1.2.3 的	IM Manager allows you to manage IM behaviors/contents/peers. Matching priority:
要求。	1. Explicitly specified IM account
	2 AD name
	2 AD group
	S. AD group
	Osers out of the schedule will apply the their IM Groups' chosen IM Service.
	Exempt (Source / Destination)
	Enable Exempt Sources
	Exclude In the IM Manager enforcement
	O Include ServerHTTP win the IM Manager onforcement
	IN more service
	Filter/record IM over HTTP/SOCKS4/SOCKS5 proxy servers.
	Functions > Content Manager> Web>Status
	Status 👪 Web Profiles 👪 Global Policy
	Enable web Manager
	Description
	Web Manager allows you to filter unwanted sites during the office hours.
	Exempt (Source / Destination)
	C Enable Exempt Sources
	Exclude Free free from the web Iter enforcement
	🔿 Include 🖉 HostCTO 💉 in the web filter enforcement
步驟 12 使用虛擬群組·將側錄	Functions > Content Policy> Action
資料以 AD 群組方式顯現	-
八女旧仁座烻矸組,用尸机置做	
球到虛擬群組裡囬。	

首先在"Content Policy"	🎊 Status 🎊 Polity 🛔	à Atlan			
→ "Action" 的百面调點去錄	🕤 Virtual Groups				
	NO Group Name	Description		W Frefix	Web Profile
"Add Group"新建虛擬群	1 AE			Ne=Use:	NecUser
組·在這裡我們新建了一個 AE	2 Offrers	Default group name for t	sers' registration	Ne-Use-	NewUser
的虛擬群組(見圖1)			10 C	3.11	
其次點選 Policy 選項卡·在	(圖1)				
上述創建的 rule 1 規則裡 · 把	Functions >	Content Poli	cy> Policy		
- Vitual Group 選則為剛剛建立	🚳 Status 👫 Policy 🚮	Action			
的 AE(目園 2). 並日右键點選	List Virtual Group	-IN Profile-	-Web Frofile		Search
	Ap:t/ -Schedule-	-Mhuai Group-	-MProfie-	-Web Profile- 🗸 to List	ed
AE 規則, 選择 Edit User 進入編	NO. SI	atus Oc	nation	Actor	
輯對話方塊(見圖3)·把MSG	Echepule 1 Contactor	rule Name N	ame MiPiprie Flaisum	Wet Profile Gold A	91tual Groups
REC 點選為 Enable 狀態 (見圖	🗑 Aleays	DefauliUser Cefau	Use: Platinum	Plain.m	
4) ·設定好後·上傳配置。				2	thers
然後在 AD client 田 John 帳號	(圖2)				
	🚳 Birlus 🚳 Polky 📸	action)			
來豆球域, 亚伊用 AD client 强	List Vitual Group	It' Profile	Vob Pipfle Y		Search
送 MSN 聊天資訊,這時,我們	Apply -Schedule-	-vitusi Gm.p-	-IC Prifie-	-Web Prifie-	HQ.
可以在報表裡看見 · John 這個	NO. Brindule	Rule Name P	ndition Iome IV Profile	Action Web Profile	vitual Groups
框號已經波歸到⚠⊑的我知道	1 Stowars	nue_1 _om	Platerer New .	etid A	E 📉
喉號」。經牧蹄類到 AE 的年組作	13 Q Awars	Default user Default	User Plat Edtl.	Pladnum	Others
面(見圖 5) [。]			Delex	User	
			Delex		
	(圖3)				
到這裡·已經完成了 3.1.2.4 的					
需求・					

Edituser			
Schedule :	🕈 Always 🛛 🐱 Vi	irtual Group : AE	~
Basic —			
Rule name :	ule_1 N	lame : John	
The Name field co	uid be AD account, AD group	p, or Web Login account.	
IM			
MSG Rec :	Enable () Disable	
File Rec :	O Enable) Disable	
MSN Account :	Allow		
Yahoo Account :	Allow		
AOL Account :	Allow		
ICQ Account :	Allow		
IM Service :	Platinum		~
Web			
URL Rec :	Enable) Disable	
Web POST :	Allow		~
Web Service :	Gold		~
(圖4) Functions > Rec Fof: call For Worth 2002:07 日 Date Act: un Brt P:	oder> IM	Finish 2019 07 25 (1) 23 119 119 11 Vessage 1955 (4) -	Cancel

第3部

即時監看與對象管理

第7章

即時網路監看

本章節介紹網路監看的應用。

7.1 監看公司網路

設備 Traffic D 設備 covery (流量監控)功能,讓所有流經 設備 裝置的流量 - 覽無遺地呈現在管理者的眼前。管理者可 以藉由檢視網路流量來決定針對特定流量管理的方式,用以避免頻寬遭到員工濫用。MSN/Yahoo/ICQ/AIM 等即時通訊 軟體,當其企圖透過非正規的連接埠連線,系統將會以紅字標示,將此連線顯示在 Traffic D 設備 covery 上。透過 Traffic D 設備 covery,網管人員可即時看到整過網路的使用狀況,進而做最適當的頻寬控管。



🚵 Eumn	tery 🏙 App View 🏭 IP View 🗿	Policy View 🦄 Pipe View	
		Realtime Bandwid	ith
1.003	.104		
Der and	483 -		-TOTAL In
至 744	.178 -		-TJTAL Out
음 uav	202 -		
2 (a)	24)	<u> </u>	
ere B			
23	.621		وحواوي والمحود
100	.310		
Top Hos		Top Acclinati	or .
Top 10	tost - by Bandwidth - C	Table G Bar C Pie Top 10 Cale	ayory
	otnet	[1/2.10.102.20][93.46.0]	P2P3489.16 M
	tost 👘	(202.167.120.84)16.61 M	System (1998) N
		[10 0 132 123]18 59 M	BIDDAY 100 CB M
		[10 0 70 228]-9 77 M	EpuPit 2 M
	-	(202.197.119.107)10.24 M	Title Transfer 1.27 M
		ptp2.167.124.104(12.9.14	Elicial(2)7.47 K
		(172.16.170.100)12.34 %	■I±sternsel47.48 ×
		(202.197719.221)1174 H	■[Storia]32.63 K
	-1		
			11
在本頁,您可以查看目前的網路狀況,透過 Moni	tor > Realtime > A	App View	
每個目體確田來找到相對的使田老。	were the set View the Putton I	Polyullaw St. Fine Upru	
	Second and the second s	op	Beers Parkels Bancetith@usi
	internal P Name Count I	ort Externel P Port Pipe	In Out In Out In Out
Apolio A Apolio	atons 79010 nat 15010		10.41 G 19.40 GE2,024. 04,749.04767. 449.2 M - 503.43. 682.34. 7,990. 2.823. 203.26 (545.43.
I Fe	atwangwang 4		106.38 K 49 K 1,728 2,815 0 b 0 b
	men 80		659.36 K395.02 K 7,361 11,490 4.2 K 1.29 K
	manfie I		48.06 K 268 B 41 32 0 b 0 b
	gamedia 35		00.90 // 111.45., 196,400 000,009 54.40 K26919.
	l quetana 4 Cue 2		3 59 K 1 42 K 29 27 0h 0h 247 E 271 B 5 5 0h 0h
	amop 15		1.88 M 56.51 M 4,36U 3,873 Jb Ub
the the Er	ryshoo 1 nall 15		630 K 6.04 K 164 185 Db 0b 128 4 K 141 5 K 269 201 1503 4802 04 J
(a) (a) Er	lerprise 695		4.04 M 2.6 M 62,201 52,588 40.07 (4.17.65 P)
	emanister 73 ema 12		7.32 M 782 84 K 69,218 85,021 3818 K 10,28 K
ti- 🐼 F2	P 32301		9.29 G 11 97 G 41,020. 45,935. 178.0 H 284 98.
우 생	10.0.24.243 2		810E 578D 10 12 30 00
	- 100.26.253 1 100.34.243 79		11 56 K 2 37 M 1,563 2,068 712 b 23 44 K 895 00 K 616 M 9 349 17 751424 7716278 64
	100.35.224 120		224.30 K512.74 K 1,344 1,513 7356 25.41 K
	- 100.40.243 158 - 100.40.252 1		737 E41 .47 K 83 310 0b 0b
	- 10.0.65.237 17 10.0.75.235		288 E 1.9714 4 31 0b 0b
1.1.1	10.075 202 5		2.38 k 4.56 k 5,567 5,613 4,91 4,208 47
0.1.4	- 10.0.70.243 54 10.0.76.82 54		269.50 K 13.52 W 10,137 10,650 20.83 (853.38.)
	100.97.201 2002		580.28 K700.05 K 1,318 4,304 55 71 K 15 1 K
	E 10.0.36.232 B3		14 74 N 18 74 M 23,794 25,865 17 27 K 201.2 K
			Refreshievery 3a 👻 - Refreshitov

在這頁,可以透過具體的 IP 來找到這個人	Monitor > Re	ealtime > Ip V	'iew				
在做哪些網路應用	A Eummary A App &	Ace S PVer & Por	cy View 🖄 Fipe View	-			
		Section			Extes	Paciets	Eandwidth(boo)
	rtemaliP	Name Count Por	External P Po	1 Fine	P Gul	h Cut	10 0.0
	🛃 Hoats	80222			24.95 3 43.55 6	51675, 85,598	34D SE M 430.23 +
	庄 41 100.11	34			1.88 0(1,011.7.	21,879 22,347	232 b 1.58 k
	座 🛃 100.12	53			3.79 M 26.87 M	20,200 32,304	343.69 ((739.39 (
	座 💐 10.0.13	35			469.15 K 111.83 X	2,413 1,859	Ob Ob
	日週 100.14	53			4.19 M 4.73 M	7,469 11,283	738.3110.29.1410
	1.0.014.201	3			68.32 K 146.8 K	836 369	Ob Ob
	10.014,202				52.40 K 18.57 K	479 408	Cb Cb
	1 10.0.14.214	27			2.52 M 181.23 K	2,884 1,328	738.3110 28.8110
	E- 10.0.14.250	25			1.56 M 4.43 M	3,268 7,379	3 C b 338 b
	- CCP	2			52.85 K 20.01 K	521 1,235	0 b 330 b
	- To edonkey	1			448 B 1.31 8	56 322	2 05 05
	- → http://	1			308 B 1726 B	5 5	5 UB UB
	- bg p2pdata	2			1.19 K 3.36 8	29 114	Ub Ub
	i – 🔚 pece	1			0B 48	U 20	
	-U ppine	2			1.5 M 4.46 M	2,585 6,230	5 UB UB
	lestino 🥁	5			OB 470 8	U 12	2 00 00
	🛁 👻 unkriewn	- 11			332 B 2.1 K	22 34	0 0 0 0
	座 叠 100.19	9			241.7914 49.83 K	930 1,326	5 Ob Ob
	由 聲 100.19	21			314.92 K 0.1 M	10,114 13,238	5.43 K197.99 K
	由 登 10 C.20	- 37			24.01 M 30.57 M	00,501 70,444	1.18 M200.41 K
	自聲 100.21	327			0.147/ 1.73 M	1 16,002 12,772	2042.35 K491.44 K
	10.0.21.234	8			179.1010 1.24 M	1,940 2,500	5.3 K474.25 K
	10.0.21.235	13			2.1916 4.1 8	17 20	00 00
	10.0.21.200	13			4.65 M 50.79 K	3,653 2,488	00 00
	10.0.21,250	292			5.32 / 433.16 ×	0,384 7,387	2007.05K 17.19K
	直 肈 106.22	132			53.8 M 22.43 M	68,185 97,000	7.28 K 24.58 K
	由 聲 100.23	11			468,44 K 1.32 M	6,487 6,354	1 332.b 22.5 K
	白 肇 100.24	280			25,38 M 39.41 M	120,657 119,537	61.71.K350.83.K
	- 10.0.24.48	3			64 39 K 41 03 k	910 942	2 Oh Oh
	- 10.0.24 193	35	1		1.43 M 27.31 M	46,656 46,5 6	24 44 K211 33 K
	10.0 24.200	7			19441 K 108 93 4	3,312 2,532	Ob Oby
		nd data nita dia		Fiefre	ish every 3s 🛛 👻	Senser (Co	Batul Export

第8章

固定對象 -地址/服務/排程

本章介紹 IP 與排程的設定與使用方式。

8.1 需求

- 1. ABC 公司希望管理公司内部的所有 IP 的網路使用權限·但是·CEO 與 CTO 有完整的許可權存取網際網路的資源。
- ABC 公司的上班時間是星期一早上 8:30 12:00 · 下午 13:00 17:30 · 中午 12:00 13:00 為午休時間。依公 司政策·某些即時通訊或點對點傳輸軟體在上班時間不准使用。
- 3. 性質相同的物件最好能夠將其群組一起以方便政策規則的設定。

8.2 方法

- 點選設備對象管理員之位址·設定 CEO 的 IP 位址為 192.168.168.2 · CTO 的 IP 位址為 192.168.168.10 · 並將此 兩個都是管理階層的位址物件群組在一起。
- 2. 在對象管理員之排程設定上班時間,並將不連續的上班時間群組成一個排程。

8.3 步驟

8.3.1 地址設定

步驟 1 新增物件位址	Function > Ob	ject Manag	er > Staic > Address > Static Objects				
在 HactCEO 上坡左键,然後選擇 Edit。为了你	盤 Address 盤 Schedule 盤 Sentce						
任 HUSICEU 上投石艇,然後选择 Eult。 而」 心	State Objects a State Groups						
制定規則的便利性,設備已預設一些常用的位址物	Destruction						
件供您選擇使用·您可以直接修改預設的 IP 位	Applied to fixed IP objects w	ho do not need to authenti	cate.				
址,或將預設物件刪除,然後白行新增物件。		2350020					
	Name	Trae	IF.				
	CCC	Se Hoat	192.160.18.5				
	HISCEO	And a	192.168.100.3				
	HostCHO	Field F	1921681002				
	HostCTO	EUT E	192.168.100.1				
	HostChalman	Dawn	192.163.100.8				
	Hostyrechairman	Detete As a	192,160,100,9				
	HostMcePresident	Se Hast	192.169.100.7				
	ServerFTP Second TTP	Host Hest	192.168.100.8				
	ServerWYSQL	Host	192.163.100.9				
	ServerSQL	🖗 Hast	192.169.200.1				
	 SubnetADM SubnetFinitACF 	Subnet	192.168.4.024				
	SUBNETNANUFACTURE	Subnet	192.169.5.0/24				
	SubnetNARKETING	Subnet	192.168.6.0/24				
	SubnetRD	Subnet	192.168.2.024				
	- All and a second second	10000					
	1						
			👔 Auto Learning				
步驟 2 編輯 HostCEO	Function > Ob	ject Manag	er > Staic > Address > Static Objects				
將 HostCEO 預設的 IP 地址改成	Edit IP Address objec	t					
192.168.168.2。您亦可根據貴公司的網路架構,	Edit your IP address o	bject					
緣再此物件的夕稱與 ID 位址。							
受到此初日的石桶英 17 位址。	Name: Host	CEO	@ Uset				
IP 位址可以是 1) Subnet (子網路); 2)	IP Address : O Su	ipnet 🔾 Kange	• Host				
Range(範圍); 或 3)Host (主機)。	IP <u>192.1</u>	68.168.2					
對象HostCEO設定亦同。	ОК	Cancel					

IP Address		說明	範圍 / 格式	範例	
	IP	子網路 IP 位址	IPv4 格式	192.168.168.0	
Subnet Mask		乙烟败油军权式	24		
	(0-32)	丁納印這早	丁納떱迦早伯八	24	
Dango	Start IP 此物件範圍的起始 IP 位址。		IPv4 格式	192.168.168.1	
End IP 此物件範圍的結束 IP 位址。		IPv4 格式	192.168.168.10		
Host	IP	單一主機 IP 位址。	IPv4 格式	192.168.168.2	

表格 8-1 定義位址物件



步骤 5 上傳設定檔到裝置中 點選 Upload Configuration 選項·或者點擊 💽 圖示·將現行的設定檔上傳到裝置上。

▲ 如果某個物件已經被某個群組或某條政策規則所使用·在刪除此物件前·您必須先刪除包含此物件的位址群組或是政 策規則·否則您無法刪除此物件。

8.3.2 排程設定

步驟 1 刪除預設排程	Functio	ns > Ob	oject	Mana	iger >	Staic	> Sc	hedul	e > 0	bjects	
設備已提供您兩條預設的排程·如果預設的排程不											
符您的需求·您可以修改此排程·或者將其直接刪	🕞 Objects	🗊 Groups									
除。	NO. N	ame	s	chedules							L.
	1	WorkTime	Mo	ming, Atte	rnoon	-					
在接下來的範例中‧我們將刪除預設的排程規則‧				A	dd Group	10					
然後透過新增排程介紹您排程的設定。				E	dit Entry						
請注意·在刪除排程前請先確認排程群組或其它政				-		-					
策規則是否已經含有此排程了。		Destroyers and									
	MO No	🗊 Groups	-	then	Tue	Mart	Thu	(cr)	Qui	Charr Times	Quan Tirma
右邊的例子為排程物件已經被排程群組所使用	HCL HO	Memine	Lei	G	0	0	0	G	oar	06:38	1200
了.所以您必須先刪除排程群組.然後才可刪除排	-			0	-			0		19.00	12:00
程物件。	-	Memoon	dd Schei	tuie	~	~	~			13:00	1/ 30
		1	letete Bot	eluter							
	1		dil Entry	8							
步驟 2 在排程物件螢幕上按右鍵	Functio	ns > Oł	oject	Mana	iger >	Staic	> Sc	hedul	e > 0	bjects	
在螢幕上按右鍵,然後點擊 Add Schedule		Objects Gro	ips	Que	Mon Tuo	Wod	Thu	Eri Po	t Ptort 1	ime Stop Time	
選項。	-	NO. N	dd Eobodi	- Sun	won rue	vieu	mu	rii oa			3
		D	elete Sche	adule 4							
		E	dit Entry								
		(•

步驟 3 新增排程 輸入排程名稱。點擊 OK 關閉窗口。 ₩驟 4 編輯時間	Functions > Object Manager > Staic > Schedule > Objects
在 WH-Morning 規則的 Start Time 欄位上按	Chierra Broups
た White Moning 成点的 Statt Time 偏位工设 右鍵, 然後點躍 Edit Entry 躍頂。	NC. Name Sun Mon Tue Wed Thu Fri Sat BlantTime StopTime
	E Moming 😜 🤪 🥝 🥥 UB:30 12:00
	3 Afternoon 😜 🚱 🥹 🥥 🖓 13:00 17:30
	2 94Hittening 00.00 00.00
	Delete Schedule
	Edit Folty
步驟 5 拉選起始時間	Functions > Object Manager > Staic > Schedule > Objects
拉選 Start Time 的時與分·然後點擊 OK 關閉視 窗。	Time : Hour 8 V Min 30 V
Stop Time 的設定相同 · 請參照起始時間的設定。	
步驟 6 日期管理	Functions > Object Manager > Staic > Schedule > Objects
有將滑鼠移動到 Mon 欄位上點一下,即有一圖示	NC Name Sun Mon Tue Wed Thu Fri Sat StartTime Stop Time
◎ 顯示在表格內。接下來設定 Tue ~ Fri。	Menning 😂 🥝 🙆 🥝 08:30 12:00
	2 Afternoon 🕹 🥥 🚱 🚱 😂 1300 17:30
其它排程的設定皆相同。	2 X1++Morring (2) (2:50 12:00
步驟7流覽排程設定結果	Functions > Object Manager > Staic > Schedule > Objects
現在·我們已經設定好了兩條排程。您可以開	NC, Name Sun Kon Tue Wed Thu Fri Sat StartTime StopTime
始將這兩條排桯群組一起了。	1 Moming 🕹 😂 😂 🥹 03/20 12:00
	2 Milemaan 🥥 🥥 💭 🥥 1300 17:33
	2 94H-Moming 🕹 🤪 🤪 🚱 😡 08/30 12:00
	🖌 (NH Allemaan 🕘 😒 📀 📀 1200 17/33
步驟 8 新增群組 因為ABC公司的上班時間為 8:30~12:00 與 13:00~17:30 · 所以您必須將此兩個不連續的時間 群組在一起 · 以方便管理規則的建立 · 在螢幕上按	Functions > Object Manage > Staic > Schedule > Groups
Ⅰ 石難,然後選捧 Add Group 選填。	Delete Group Edit Entry

步骤9 輸入群組名稱 輸入群組名稱,然後點擊 OK 關閉視窗。	Functions > Object Manager > Staic > Schedule > Groups Please input group name
	Name: WorkingHours
步 驟 10 編輯群組	Functions > Object Manager > Staic > Schedule > Groups
在 WorkingHours 規則的 Schedule 欄位上按	Colects Groups
石鍵,然後選擇 Edit Entry 選項。	1 WorkingHours Empty set
	Add Group Delete Group Eat Entry
步驟 11 編輯群組	Functions > Object Manager > Staic > Schedule > Groups
在 All Schedules 欄位內選擇您要加入此群組的	Please select schedules :
程加入 Selected Schedules 欄位內。如果您要移	All Schedules Selected Schedules WH-Morning Whitemass
除某個在此群組中的排程·請在 Selected	WH-Maining
Schedules欄位中和建該排任,然後點擊 << (左向箭頭)即可移除。點擊 Fin設備h 結束設定。	>>
	Finish Cancel
步驟 12 檢視已設定的排程群組	Functions > Object Manager > Staic > Schedule > Groups
在您完成上列設定後,畫面將回到排程群組的首 更,您可以在此檢測您的訊完。	Dojects @ Groups NO. Name Schedules
具 · 心可以仕此慨悦心的故走。 	1 WorkingHours MH-Meming, WH-Afternoon
クターコート 同のに 個 辺 衣 旦 上 點選 Upload Configuration 選項・或者點擊圖示	↓ ● 上傳設定檔到裝置中。

▲ 如果某個物件群組已經被某條政策規則所使用, 在刪除此群組前, 您必須先刪除包含此群組的政策規則, 否則您無法 刪除此群組。

第4部

流量管理

第9章

流量管理-IP 限制策略

本章介紹 per-ip 與其使用方式。

由於網際網路的盛行,員工上網隨時隨地都可以上傳或下載資料/檔案,濫用頻寬的結果常導致重要訊息/檔案無法即時傳送/接收,造成公司莫大的損失。有鑒於濫用頻寬的事件頻仍,設備 流量管理員設計用來管理時下盛行的應用軟體之頻寬。 借由滑鼠拖拉的動作即可有效的控管頻寬,省時省力又大大提升網路頻寬的應用效率。

9.1 設定 Per-IP Limit

Per-IP Limit · 可以針對每個 IP 位置單獨設定對外連接數與應用軟體之頻寬。此管理器若有相同或是衝突的策略設定時 · 會視最後一筆符合的策略為有效。本範例設定所有連接數上限在 2000 條 · 上傳頻寬為 5Mbps · 下載最大頻寬量為 10Mbps · 且將 ServerHTTP 及 Admin 設備 tration 網域 · 群組起來為 UnLimitGroupy 不限對外流量 · 上下載頻寬為 100Mbps · 但此群組的 P2P 流量 · 連接不可超過 1000 條且上傳、上傳和下載流量分別為 5Mbps ·

步驟 1. 啟動 Per-IP Policy 在 Status 控制頁面中 · 勾選 Enable Per-IP Policy · 將 Per-IP Policy 功能啟 動。	Traffic Management > Per-IP Policy > Status
步縣 2. 編輯 any 的 Download 頻寬 在 Policy 頁面中 · 編輯設備預設的 Per-IP Policy 的 any 值 · 按右鍵 · 點 擊 Edit policy 設定。	Traffic Management > Per-IP Policy > Policy Status Policy Status Policy Description Table Pasted set by draw metched with the purey Only the test-metched policy lakes effects. Table Pasted set by draw metched with the purey Only the test-metched policy lakes effects. Table Pasted set by draw metched with the purey Only Test P > L3 + L7. Table Pasted policy priority Test P > L3 + L7. Eluxis other priority Test P > L3 + L7. No Fulls Heat Schoolic Secsion No Fulls Tobles Schoolic Secsion Tobles Fulls Tobles Schoolic Secsion Schoolic Secsion Lylicid Downlood Tobles Fulls Tobles Full Secsion Edit colley Delay Day

	Host Specify schedule of application Editive application and schedule settings here to help define your policy. Schedule
步驟 3. 編輯 Per-IP policy	Traffic Management > Per-IP Policy > Policy
編輯原本預設的100Mbps· (以為 5Mbps和10Mbps·按OK關閉窗口。	Specify Application
注意 · policy 設定若為數值 0 · 是表 示不受限的設定值。	Edit the application settings here to help define your policy Note: Zero means no limit. App / Service : any Session limit : 2000 Upload limit : 5 Mbps Download limit : 10 Mbps
	OK Cancel
步驟 4. 新增 Policy 在 Policy 頁面中·按右鍵點擊 Add policy·新增 Per-IP policy。	Traffic Management > Per-IP Policy > Policy Image: Particle and the second se

步驟 5. 新增 Rule_1 下的 application policy 點選剛才新增的 Rule_1 後⋅按右鍵・	Status Pointy Action Descriptor Non-Pointy commatched with the policy. Only the instructions princy takes effects. Non-Pointy princip, Per-P + 14 + 12. Status patry sends; sender + 14 + 17. Status User Status Status Status Status Non-Pointy Status Status Status Note Status Status Status Status Status Sta
點擊 Edit policy。 在彈出 Edit Per-ip Policy對話方塊裡 點選 Schedule 點選 Insert App	Note: Bancwtitith policy: Fer IP > L4 > L7; Biock policy pricitity Per-IP > L4 > L7 Biolus User Concition Action Action2 N0 Fulls Hod Scheouls Service Service Service Concition Action2 1 Rule_1 Hod Scheouls Service Service Service Concition Action2 2 Default Biology Insert policy 2000 10 Waps 10 Waps Concert 2 Default Biology Editpolicy Default Editpolicy Concert Concert
	Edit Per-IP policy Specify schedule of application Schedule Edit the application and schedule settings here to help define your policy. - Quota Schedule (Sam Session Upload Download Insect App Schedule (Sam Session Upload Download Insect App Edit App Schedule (Sam Session Upload Download Insect App Edit App Schedule (Sam Session Upload Download Insect App Edit App Schedule (Sam Session Upload Download Insect App Edit App Schedule (Sam Session Upload Download Insect App Edit App Schedule (Sam Session Upload Download Insect App Edit App Schedule (Sam Session Upload Download Insect App Edit App Starty 2000 100 Mbps Edit App Back Reve Up Back
歩驟 6. 編輯 P2P 流量策略規定 設備預設會將 L7 Policy Management 中為 P2P 分類群組起 來・此群組不可更改編輯。 拉選 P2P 群組・再設定 Session limit 為 1000・Upload limit 與 Download limit 都為 5Mbps。按 OK 確認設定 並關閉窗口。	Traffic Management > Per-IP Policy > Policy Edit your application policy Description: Rule_1_1 App / Service: P2P Bession limit: 1000 Upload limit: 5 Mbps Note: Zero means no limit. OK Cancel

步驟 7. 查看新增的 policy 當新增或修改完後 · 會立即顯示在 Policy 頁面中。 若有相同策略名稱 · 會視最後一筆符 合的策略為有效;但是 · 即使名稱不 同 · 卻與其它群組產生衝突的設定 時 · 會視設定的最小頻寬為有效策 略。舉例說明: No1 設定 FTP Transfer 的 Download 為 5 Mbps; No2 設定 FTP 的 Download 為 10 Mbps。實際 FTP 生效下載頻寬為 5 Mbps。 Traffic Management > Per-IP Policy > Policy

🕵 Status 😫 Policy 🚯 Adica

-Description Note: Persons are top-down matched with the colleg. Only the Stat-matches policy layes effects.

Note: Rendwidth policy priority: Fer-IE + 1.4 + 17; Block policy priority: Fer-IE + 1.4 + 1.7

6	rat.s	User	Con	ifirin		Att	ion.			Action 7	
-9C.	Rue .	Host	Bchedule	Ber-ica	Session	Uclose	Download	Quota	Session	Upload	Down.
	Buls 4	The set last to sure	and all some	Comp.	2000	1007/bps	100 Mbps				
	HURST &	Second Supervision	all on when	C 1221	1000	5 Mode	d Okps				
1	Cefault \$	any any	Al-Ris	🕒 ərə	2000	5 Mades	10 Maps	-	1		
		A CONTRACTOR OF A CONTRACTOR OFTA CONT	and the second second second		1		A CONTRACTOR OF A				

警告,設備 策略管理順序如下:

Per-IP Policy > L7 Policy > L4 Policy

第10章

流量管理-應用層(L7)策略

本章節介紹七層策略的設定。

10.1 應用層策略介紹

根據 2005 年 5 月 Gartner 提出的「Application Delivery and Web L7 Are Ready to Converge」報告中指出,現今所有的網路攻擊事件中,約有 75%的攻擊事件是瞄準應用程式層,我們可以發現網路攻擊已經不僅是單純的掃瞄網段或主機, 而是以企業必須開啟的連接埠為發動攻擊開端,為了確保網路安全,「應用層策略(L7)」是最佳的防禦方式。

應用層策略只是一個防禦環節,最重要的還是相對應的防禦政策。所以應用層策略必須根據其所需保護的應用程式定義不同的防禦政策。以目前應用程式網頁化的趨勢而言,小至網頁郵件、大至整個企業的 ERP 系統,都可以透過流覽器使用, 我們可以想見網頁伺服器攻擊的比例將會越來越高,而防護難度也相對提升。設備的應用層策略系將所有通過該裝置的應 用軟體加以辨識控管,讓企業阻絕一些不必要的應用,且透過頻寬控管,讓企業內部的網路可發揮其最大的功效。

10.2 需求

- 1. CEO 與 CTO 擁有完整的許可權可以使用網際網路資源。
- 2. 除了 MSN 以外,上班時間不允許使用其它即時通訊軟體。
- 3. 除了 Skype 以外,上班時間不允許使用其它點對點傳輸軟體。
- 4. 上班時間·R&D 部門不允許使用 Skype 傳檔。

10.3 方法

- 1. 允許所有來自 CEO 與 CTO 的網路流量。
- 2. 除了 CEO 與 CTO 外,員工在上班時間內只允許使用 MSN,其餘即時通訊軟體一律攔阻。
- 3. 除了 CEO 與 CTO 外,員工在上班時間內只允許使用 Skype 傳送簡訊與檔案,其餘點對點傳輸軟體與 VoIP 一律攔 阻。
- 4. 上班時間不允許 R&D 部門的員工透過 Skype 傳檔。

10.4 步驟

1. 啟用應用層策略、設定上班時間排程、允許所有來自 Boss 群組的網路流量、允許 MSN 並攔阻其餘即時通訊軟體的 使用。

- 2. 允許 Skype 並攔阻其餘點對點傳輸軟體的使用。
- 3. 上班時間,攔阻 R&D 部門的 Skype 檔案傳輸。

⚠ 注意:

- 1. 如果您選擇讓某個應用軟體通過設備,不管其來源端/目的端的 IP 位元址為何,所有屬於該應用軟體的流量皆可通過 設備。
- 2. 如果 設備 擺放在貴公司防火牆外,且透過防火牆轉址,因設備本身設計上的考慮,您無法透過特定的 IP 控管任何 應用軟體。且 Traffic D 設備 covery 上所看到的來源端 IP 都是防火牆的 WAN 端 IP,無法顯示其真實的 IP。

10.4.1 設定即時通訊軟體規則

步驟1 啟用應用層策略	Functions > Traffic Management > L7 Policy	
	24 States 25 Fate-	
勾選 Enable L/ Policy。	(F Enable L ^y Folce	
	Cescription IN Device Per-D = 1.4 + 1.7 2 Up notice type the ministric match Cet meetbes: on tryin Never in central sertion asses drop	•
	Derbuda 🛃 Hossorro 💌 tam inc "7 policy — im finite Sing fi	
	Cetaul Traft Fice	
步驟 2 列舉 Chat 群組	Functions > Traffic Management > L7 Policy>	Policy
在搜尋丁旦列上選擇 L設備t Chat · 列舉所有屬於	A Shis A City	
	La -CalegoryProtoci Appy -Scheque Security In-	dire- 🐱 utistid 🔤 🖌 🟹
Chat 群組的規則。	Calcure A Cantern	6100
	NO. eName Intern. Edom. Protocol	Secu t/ Frontic Filte
	👷 🙀 Email 🛛 R/NGE 🕂 are 🛒 are 🦉 theb Hip Range Oct	📽 Allow 🙉 High 🧖
	💿 🙀 FileTranel DOVINL. 🗟 any 🛱 any 🥻 theb-Hp Dovinican(zionanissellisonmetri)	🕷 Allow 🕄 🏚 High
	👔 🍯 pop // DEO_L. 🐏 any 🕮 any 🙋 Web-Hip Viceo(hamp4/swittamy)	🕷 Allow 🕺 High
	📅 😥 🙀 Turinel 🔤 EFRONY. 🐏 my 😫 any 🔮 Web-Hip Provolitips Aproxy combilities (🕷 Allow 🕺 High
	121 · · · · · · · · · · · · · · · · · ·	🔹 Alow 🕄 Hgh
	🗤 👹 -waya OPG_Role_T 😫 my 😫 my 🕼 EnaleFOPG	📲 Alaw 🕺 High
	· · · · · · · · · · · · · · · · · · ·	# Alow Q High
	20 🖉 Avaga (T. P.Js.) . 🖳 er- 🚆 ang 🍯 (nelsanslas) (T.	🖉 Alaw 💽 Malde
	27 餐 Awaya ENB Sue : 壁 an- 壁 any 目 FielTransfer-BNB	# Alow @High
	왕 - waya PP. P. Ja. 1 및 arr 및 any 및 Vo P-STP	# Allow \$1 High
	22 A HWAYA RTCP_SUB_1 A A RT BE ANY A VOP-STCP	# Allow St High
	a www.s EKYPE_HUIS_1 as any as only as one-skipe	allacy the High
	What's EXTERIES and an address the second	
	and an extremulting and an	a dian gi High
	27 W Away H332 Bile 1 W an W an With D 2320 Hills star Street	
	A ANTER U CAL BU, Water Water Called Unit	
	A ANALY VIPEUSTES, Way Way Wine Ware star	a diaza 🔒 Hab
步驟3選擇排程	Functions > Traffic Management > L7 Policy>	Policy

在丁目列上選擇∆nnly WorkingHours 排程,將	截 thue 截 2007	
	List 🕒 Chat. 💌Proseco 🐱 ApthySchedule 😿Securito 😿Traitio-	- 🚽 to i sted 🛛 🔞 🛣
此排在复用在所有 Cnat 群組中。您亦可以手動選	State State	Action
擇每條應用程式列為的排程。	Schedule Eule Same Intern Extern 🔐 Hover Protocol 🔅	Security Profile Pipe
	1 資 Always MEN Rule : 陸 any 陸 any 和國 exacyture OritianWi-andsetSaim) @	Altw R Hor
	왕 Always MENEL = Rul 陸 suy 환 suy 위험 #5-Matrics · · · · · · · · · · · · · · · · · · ·	Allw Gitign
	👔 Abaya VA-00 Rue (🕼 any 🐺 any 🖓 any 🖓 ang ramerane cal no T-liar Mianda Sami 🙍	Alter Atter
	· · · · · · · · · · · · · · · · · · ·	Altwork (Ching)
	Avays DMPP_aus_1 🚔 any 🚔 any 🖓 Chel-COTP(Coundle FeleCam) 🖉	FAILW KR (197
	A Alwaye KO_ROB_1 😫 any 🛃 Shee DO	ALW Strige
	Avays Occus Roo. San	Aller Marings
	a waa oo taa a a a a a a a a a a a a a a a	All and a second
	a Amara Oldariare, a ann a ann a Chairean Ianna ann an Aonaichtean ann ann ann ann ann ann ann ann ann	
	a share (0.00_00e_1 a an a an a Chet/Pote/P)	Aller Dian
	The Alterna PCE Calls 1 Marry Marry ChatGood State Co.	New garage
	12 W Abree Al off Class Warr & Chate Manuffronting & Chate	Nitras Distant
	All and All and EFTIN Rule Likers and All and	Nine all the
	Markey DOBHCY St. Markey Markey Markey Markey	Miner and Har
	15 Webraue 1 (Webraue 1995) and 1995 and 1995 and 1995 and 1995	Aller Aller
	Window One gan gan gan gan an a	Miner Star
	Register hereichter Bran II aus bereichte Artaget	200-7 0 5 0.5
考味 (KOSS 结调起码外,时有处混体 IP 使用则	The second	
時通訊軟體都套用選定的應用層策略規則。	2 Wurkin, W241 LL_Adi, Stub A & any & Crist Van-rik 3 Wurkin, K4LO_Lake, Crist, Warkin, K4LE, Crist, Warkin, Warkin, Warkin, Warkin, Crist, Warkin, Warkin	Alaz Gilgh
時通訊軟體都套用選定的應用層策略規則。	2 Wuthin, W241 LL_Adt, Study A and W Chel-Wan-tle 3 Wuthin, W1400_subc, Core 4 Wuthin, W1400_subc, Core 5 Wuthin, W1400_subc, Core 6 Wuthin, W1400_subc, Core 7 Wuthin, M01_Pute_1 8 Wuthin, M01_Pute_1 9 Wuthin, M01_Pute_1 9<	Alazy Giligh
時通訊軟體都套用選定的應用層策略規則。	2 Wuthin, WARTEL_AL, AL, SUDA S, any S, CheFWan-tle 3 Wuthin, KHCO_Aule_1 SuDA S, any S, CheFWan-tle 4 Wuthin, KHCO_Aule_1 Surg S, any S, CheFWan-tle 5 Wuthin, KHCO_Aule_1 Surg S, any S, CheFWan-tle 6 Wuthin, KHCO_Aule_1 Surg S, any S, CheFWan-tle 7 Wuthin, KHC_Aule_1 Surg S, any S, CheFWan-tle 8 Wuthin, SHC_Aule_1 Surg S, any S, CheFWan-tle 9 Wuthin, SHC_Aule_1 Surg S, any S, CheFOO, Surg S, and Surg S, ang	Alazy Giligh
時通訊軟體都套用選定的應用層策略規則。	2 Wuthin, W241 LL_Adi, St0 A & any & CheF Wan-tle 3 Wuthin, S4100_st0e; Cm Any & CheF Wan-tle 4 Wuthin, S4100_st0e; Cm Any & CheF Wan-tle 5 Wuthin, ADL_Pare_1 Org_stors HattS-C (HastC-C) FM muthConstruction) 6 Wuthin, ADL_Pare_1 Org_stors HattS-C (HastC-C) FM muthConstruction) 7 Wuthin, ORT_FALE_1 Org_stors HattS-C (HastC-C) FM muthConstruction) 8 Wuthin, ORT_FALE_1 Org_stors HattS-C (HastC-C) FM muthConstruction) 9 Wuthin, ORT_FALE_1 HattS-C (HastC-C) FM muthConstruction) Image: Anny & CheFCO (HastC-C) FM muthConstruction) 9 Wuthin, ORT_FALE_1 HattS-C (HastC-C) FM muthConstruction) Image: Anny & CheFCO (HastC-C) FM muthConstruction) 9 Wuthin, ORT_FALE_1 Within ORT_FALE_1 Within ORT_FALE_1 Image: Anny & CheFCO (HastConst Line) Image: Anny & CheFCO (HastCons	Alazy Giligh
時通訊軟體都套用選定的應用層策略規則。	2 Wuthn, W241 LL_Adt, St0 A & any & CheF Ven-tle 3 Wuthn, V4100_40le, any & CheF Ven-tle 4 Wuthn, ADL_Pare_1 Org_tors HustCat(HustCat) 5 Wuthn, ADL_Pare_1 Org_tors HustCat(HustCat) 6 Wuthn, ADL_Pare_1 Org_tors HustCat(HustCat) 7 Wuthn, ADL_Pare_1 Org_tors HustCat(HustCat) 8 Wuthn, ADL_Pare_1 Org_tors HustCat(HustCat) 9 Wuthn, ADL_Pare_1 Org_tors HustCat(HustCat) 9 Wuthn, ORL_Pare_1 Org_tors HustCat(HustCat) 9 Wuthn, ORL_Pare_1 Org_tors HustCat(HustCat) 9 Wuthn, ORL_Pare_1 Org_tors 9 Wuthn, ORL_Pare_1 Wuthn, ORLAGE 9 Wuthn, ORL_Pare_1 Wuth, Samy & CheFOC Test and the function of the func	Alazy Giligh
時通訊軟體都套用選定的應用層策略規則。	2 Wuthn, W241 LL_Adt, Stork A any & Chek Vennik 3 Wuthn, K4100_stork, any & Chek Vennik 4 Wuthn, K4100_stork, any & Chek Vennik 5 Wuthn, K4100_stork, any & Chek Vennik 6 Wuthn, K4100_stork, any & Chek Vennik 7 Wuthn, K4100_stork, any & Chek Vennik 8 Wuthn, K4100_stork, any & Chek Vennik 9 Wuthn, K4100_stork, any & Chek Vennik 9 Wuthn, CHE Jau & Hes any & Chek Col ration 9 Wuthn, CHE Jau & Hes any & Chek Col ration 9 Wuthn, CHE Jau & Hes any & Chek Col ration 9 Wuthn, CHE Jau & Hes any & Chek Col ration 9 Wuthn, CHE Jau & Hes any & Chek Col ration 9 Wuthn, CHE Jau & Hes any & Chek Col ration 9 Wuthn, CHE Jau & Hes any & Chek Col ration 9 Wuthn, CHE Jau & Hes any & Chek Col ration	Alazy Giligh
時通訊軟體都套用選定的應用層策略規則。	2 Wuthin, WARTEL, Ad. Stork A any M Chairwards 3 Wuthin, KAD, Pare, I Org. Cost Warten, KAD, Pare, I 4 Wuthin, KAD, Pare, I Org. Cost Hast, Schler, Hast, Schler, I, Hast, Schler, Hast, Schl	 Aloy Gligh
時通訊軟體都套用選定的應用層策略規則。 步驟 5 選擇安全行為(Security Profile) 在工具列的 Security 選項上選擇套用 Block 在 所有即時通訊應用軟體上,但是請記得之後要將 MSN 的 Security 選擇Allow。因為依公司規定, 上班時間允許使用 MSN。	2 Wuthn, WARLE, add. Stable & any CheFMan-tle 3 Wuthn, ADL, Pare 1 Ong Coss Host Coll (1) State 1 (1) S	Alory Alligh Alory Alligh
A Status & "Inter		
---	--	
List 🕒 Chet 😺Potocol+ 😺Spredule- 💌Spredule- 💌Spredule-	2 4 1	
Satus Constitut - Ation		
NO. Sthedule Revenue Interna P Edent. Security P offe	Ppe	
🦛 via	-tpin	
2 🎆 Workin, MBNRUE_Ruis, 🌺 Bost 🚉 any 🐔 ChacMarFile 🔹 Allew 👘 Allew	-lph	
💦 🖓 Works n., WHOOL P., le_1 🎭 Boss 😰 any 🍙 Char Yahoo (Yahoo Trillian Miranda Samo) 🕷 Alber 🕋 🕋	-lgh	
🔺 🍓 Works (ACL_Ruis_1) 🏘 Boss 😫 bry 👔 Char ACLAOL/MUT Itom CQT ItilianMir (# Mis+ 👔	-lph	
5 🎆 Workn MP2_Rule_1 🙀 Eoss 🕺 my 🐉 CharXMP2(Coople Tabbaam) 🗰 Alcer 😭	-tgh	
6 🚮 Workin, Jab, Rule 1 🎆 Boss 😫 mr. 🖨 Changia 👘 Alc.+ 🚳 -	-lph	
🚮 Worken, POCHATROOL, 🥵 Eose 😫 any 🤗 Char-OOChatRoom 🖉 Alei-+ 🚳	-igh	
0 🐺 Warkin, pOWEDW, Roll, 🥵 Date: 🔛 eny 🏘 Char-OD Mediad (re than selen/bace/blace) 🗰 Ale 🤟 🚳	-1gh	
🕴 🎆 Wincin (1923–1982), K. 🎆 Duss 🔛 any 🎆 Char-OD-thared Fras 💿 All.— 🚳	-igh	
💿 🐻 Wincin, PAUU_Liule_1 🥵 Liule_ 🔯 Shar-Geol(Dedu-Geolu/Geo	1gh	
11 🐻 Wincon 100 (Pade 1 🌾 Disse 🐼 way 😺 Char400 (Sins 100) 👘 All w 🕼	192	
📅 🌆 Winkin POPo Rate 1 🥵 Enek-Carolycepothty) 👘 Alliw 🔞	ign	
10 🎆 Winnen 🤤 Heann (2000) 🥵 Ense 🥵 ense 🏀 Charab Heann (2000) Charab Heann (2000) Charab Heann (2000) 🎼 🚳 All 👾 🚳	igh	
14 🎆 Winken (FETCH) Rula 🥵 Enss 🕼 are 🥃 Charled in(Cristanibia Failin) 🔹 Alti 🔞	-iqi	
15 🦓 Warkin DDS-099, Ru 🥵 Eass 👰 are 🔭 Char-DoSrow 💮 Allow 🔞	-igk	
16 😹 Wite-en, LAUA-AUX, Ru, 🏘 Eness 😰 are 💁 Chast Lava-aves 🖉 Allow 🚳	-lgk	
17 🐻 Werkin, WEBDL, Rula 1 🍓 Boss 🗱 any 🕴 Chark/WEBDW/2EN Webmessenge/eBBU. 🔹 Alter 🍂	-ligh	
所有即時涌訊應用軟體上。使所有即時涌訊軟體的	2	
所有即時通訊應用軟體上。使所有即時通訊軟體的	266	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 A A	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 (A) (a)	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 A A	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 (A) (A) 2 (B) (A)	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 1 現2004年 2014年10日 2014年10月10日 2014年10月10日11月10日 2014年10月10日10月10日10月	2 (A) (A) 2 (B) (A)	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 (A) (a) > po 10 ⁹ 10 ⁹ 10 ⁹ 10 ⁹ 10 ⁹ 10 ⁹	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 1 現代的的 2011日 2018日本 20	12 A	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 1 現 2004年 2014 2014年1211日1日1日日本ののの日日の日本の2014年12日日本の1日日の日本の2014年12日日	12 A	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 1 現 2004年 2014 2014年219日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日	2 A	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 1 現 2004年 2014日21 単位2014年 1月11日日1日1日日1日日1日日1日日1日日1日日1日日1日日1日日1日日1日	2 A A	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 1 現 2004年 2014日21 単位化 1000000000000000000000000000000000000	2 A A	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 1 現代加速 Web Same Herall/Eden. Protect Part Protect Part Part Protect Part Part Part Part Part Part Part Par	2 A A	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 A C	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 ¹⁰ ²⁰ ²⁰ ²⁰ ²⁰ ²⁰ ²⁰ ²⁰ ²	2 A	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 A) (*) *pp tip*	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 A) 'pp igp	
fn有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 A A 'pp ig ig igp igp igp	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 Util Craft		
fn 有 即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。	2 A A 'pp ig ig igf igf igf	
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 ND Educe Protect Act and a bit and an and a bit and		
所有即時通訊應用軟體上。使所有即時通訊軟體的 頻寬限制為 Middle 類別。 NO Use Orating Protection Oracle Protection	2 A	

-			1000		and of the	154
NO	Statu:	3		Condition		stion
	Schepula Rule Nam	e internati	P Entern	Protocol	Bacuity Profile	Ppa
	Workin, visk_Rule_1	Bots	env	Chat MBN(:/SNOrfflien/Milanda(Galm)	 Black £ log 	🚉 tviddia
	Workin . SISHFILE_R	I. 🅵 Boss	建 307	🚯 Chat ManFila	💁 Black S. log	🕷 vidėla
	// Workin, WAHCO_Fuk	_ Boss	翻: any	🔐 Chat Yahoo (Yahoo (Ti Hanviranda/Gaim)	🌒 Black S. log	📸 krisičio
	👷 Workin . KOL_Rule_1	Boss	Se ony	🏨 ChekACL(ACLARY THEN/COTT Harryin.	 Black S. Iog 	🚔 telakie
	👷 Workin, CorFP_R. Io.	1 🔮 Boss	Se any	Chat Xt:PP(Google TaildGain)	 Black & log 	🚉 tritidio
	Workin, SQ_Rulo_1	Bots	Sei any	🙆 Chat Qû	. BChal XVH	
	Workin, SOCHATRO). 🕵 Bocs	any any	🖗 Chat G1ChalReam	👩 g(Gougle T	ak,Gami
	Workin, COMEDIA_R	u. 👧 Bocs	Se any	🛤 Chat QC Modia(File Tians/ed//o col/-Itieo)	 Black & log 	🙈 reiddie
	👷 Workin, GOSHARE_P	t. 🛃 Boss	🖳 any	🕅 Chat Q2 Shared Files	🦚 Black S. log	🚔 tritidio
	👷 Warkin , GADU_Rule,	1 🕵 Boss	Se any	👼 Chat Gadu; Sait. Gas uKadu Mirans a/G	🐠 Black S. log	🕷 relatio
	👷 Warkin, UC_Rula_1	Bots	St ony	🥁 Chat UC(Sina UC)	🤹 Black S. log	🚔 kriskis
	Workin, POPO_R.Io,	1 🛃 Boos	Se any	😂 Chat POPO; sepat 53;	 Black S. log 	📸 telelele
	👷 Warkin , ALMAN 9404	· Boss	Se 207	🙁 Ohat ALMangAtang (Toobao AL WangM.	🌒 Black S. Iog	🙈 telekle
	Workin, FETTON_Rul	👥 Bots	any any	🍃 Ohat Fation; Chinamabile Fation)	a Black S. log	🙈 tritidio
	Workin, DOSHOW_R	👧 Bots	Ste eng	🤭 Chat DeShow	o Black S. log	🙈 Madic
	Workin, LAWILWAL	u. 👧 Bocs	92 ang	🚮 Chat LavaLava	a Black S. log	🙈 retaide
	Workin, WERM Sult	Bots	19 - and	Chot WEBIC/MEN Menmers engerieBud	a Black Slott	A Printie

	欄位	說明	範圍 / 格式	範例
L設備t	Group	依群組搜尋所有應用層策略規則·並列舉搜尋結果。	所有設備定義的群 組	Chat
	Schedule	將選取的排程規則套用在所列舉的清單中。	使用者定義	WorkingHours
Apply to l	Security Profile	將選取的安全行為規則套用在所列舉的清單中。	Allow / Block	Block
設備 ted.	Traffic Profile	將選取的頻寬類別規則套用在所列舉的清單中。	High / Middle / Low	Middle

表格 10-1 應用層策略功能列

欄位	說明	範圍 / 格式	範例
Src	進入設備之封包的來源端 IP 地址。請注意 · 圖示 Ser 指的是除了 Boss 這個位址群組外的其餘 IP 位址。	Subnet / Range / Host	🍪 Boss
Dst	進入設備之封包的目的端 IP 位元址。請注意 · 圖示 Ser 指的是除了 Boss 這個位址群組外的其餘 IP 位址。	Subnet / Range / Host	any
Protocol	通訊協定類別,或是可受 設備 控管的應用程式類別。	所有可控管的通訊 協定	Chat-MSN
Security Profile	控管應用程式的使用行為。	Allow / Block	Allow
Traffic Profile	在流量管理員中所定義的頻寬類別。	High / Middle / Low	Middle

表格 10-2 應用層策略欄位說明

10.4.2 設定點對點傳輸軟體規則

步骤 1 啟用應用層策略	Functions > Traffic Management > L7 Policy>Policy						
	🕼 Shius 🚵 Fuite						
勾選 Enable L/ Policy。	Enable LT Paler						
	Cestipion 1 Putry order Terch + L4 + L1. 2 Up putry order to potentiate instant 3 El needlass on try in Never to word serviceness and p						
	Cetaul Trate Pice						
步驟 2 列舉 P2P 群組	Functions > Traffic Management > L7 Policy>Policy						
▲ 在工具列之 Group 上選擇 L設備t P2P 。所有P2P	a the star						
的注册社会照一大教育上	List 🖬 PaP 😽Puluote 🖌 AppyConstale- 🤟Cerumbe- 👻Tradio- 😼 C. Islan, 12 🗐 🖓						
的肩单就曾閷小仕宝希上。	-Celean-A						
	Web e Name Internal IF Edom Pictocol Security Profile Filoe						
	🖕 🕼 (
	2						
	KEY_R. 🛃 ary 🕮 any 🚯 P3P eDanker/eDanker/Cremetie/Ullo/Aa. 🖉 Mow 🌒 High						
	TUT POP STIM FLB TTORRENT FLORKEY, FLASHOFT WINKY						
	😸 🦉 AMWA EZPEERPLUS, FASTERACK, GNUTELLA, KURG, EIRECTCONNECT. 🖉 MWA 🔒 High						
	6 🖉 AW32 CPENET ARES, BOULSEEK, GOBCOGY KUGOO 🔹 Allaw 🔒 High						
	A State And A State						
	Alway CEFEDOWALDAD COPONTA						
	·····································						
	 						
	11 👹 Awaya 🖓 PEN-1lut. 🌺 ary 🔛 any 👹 Pel-Opent (Coasadooace) 🛛 👹 Alow 🔍 High						
	🙀 🖗 Alazza 🕹 4.5 👹 ary 📓 Pal-Alasza 🖉 Alazza 👰 High 🚽						
	10 餐 Awaya 100.00.4、 桑 ars 操 any 李 PalSG nO-aas						
	🚳 🙀 - Avaga (- COCODE: 2) 🥥 ar a 🔯 any 🛅 (- ST-CocDuring) 🛛 💰 Alaw 🛛 🔃 Option						
	📑 👹 Alwaya (1960) Rule 🦉 ary 🕼 Alway 👯 Alway 🙀 P2P40.gui 💣 Alway 🚳 Alway						
	ne 🙀 Awaya (FICC Gulain 🖉 ara 🕼 any 🧒 PCP-Pign(Pign(Cliftan)) 🛛 👩 Alaw 🔍 High						
	17 🙀 Awaya 19000 Rula 1 🥰 ara 🛱 any 📴 PSP-PonsiFean/Fearin) 🛛 💣 Alow 🔍 High						
	🔄 11 🦉 Awaga - DODOWALCA 🤯 arv - 🛱 any 🕜 PDP-00Do-rinad - 👩 Allow - 🤱 High - 🧕						

上廠 9 選擇排理	Functions > Traffic Management > 17 Policy > P		
灭棘 3 海洋排性	Functions > frame wanagement > L7 Policy>P	oncy	
在工具列上選擇 WorkingHours 排程,將此排程套	A Biths A Polky		
- 田左砾右 DOD 群组由。你亦可以手动逐一避埋海今	List 🔮 P3P 😿 -Protocol- 🚽 Apply -Bahad. Ia- 😪 -Bacurty- 😴 -Traffa	to listed 2 🔏 👔	
用住所有 FZF 矸租中。您你可以于勤处一选择週口	Status Status	action	
選定政策的排程。	Schedule Rule Name Interne P Letern Vervor	GeoungPhote Pipe	
	😸 Awaya (DINLEL Pule) 👹 any 🖓 are 🔂 complexity of lact Sitina	6 Al - 🚯 igi 🧉	
	😵 🥹 Awaya DITORIENT. 🚑 any 👰 any 🖗 any 🖉 Millionia Different Fillionials Lines .	🔿 Alt 🛩 💦 int	
	🙀 Alwaya EDONATE R 👰 ang 🕎 ang 🕎 ang 🖓 ang EDONATE ROMAN (FDorkey) (FDo	⊛Alt~ @_ip	
	🔧 🙀 Akonya 🛛 FLAEHDET: R. 👰 any 🖓 any 🚺 929-FlashCell(FlashCellTunTu)	● Alt~ 🕅 Hitt	
	5 餐 Always Allwhy_Rule_1 委 any 🖉 any 🚮 205/26n/x	& Allow 🕼 High	
	🔥 🙀 Aways EZFEERFLUS 🌉 any 🙀 any 🧔 P2P-azFearPlus	🐔 Alicer 🙀 -ion	
	📝 🦉 Always - FASTTRACK, , 🌉 any – 🗱 any – 🚮 P2P-Fasthacki; kazas (Sycksten Mech)	🐔 Allow 🍂 High	
	👘 🖗 Always (ONLITELLA, R., 🌲 any 🖉 any 🔮 229- Shutella; Soxytoz Peon BearsharelOn .	🔹 Alicer 🙀 - Igr	
	b 響 Always KUR0_Rulo_1 製 any - 製 any - 副 P2P-Kurd	🚓 Alicer 🍂 High	
	🔐 🖓 Always DIRECTOONL 🙊 any - 💐 any - 😹 P2P Line::ConnectDirectDor	🐔 Allow 🍂 High	
	🗤 🔯 Always OPENFT_Rul. 🛃 any – 🛒 any – 👹 P2P-OperFT(Crazzalikoas))	🐔 Alle= 🌒 🙀 – Igh	
	12 🖉 Always ARES 🔮 any 🖉 any 🖉 P2P ares	🔹 Aller 🔗 -tgh	
	113 🚳 Always SOULSEEN, 🛃 ang 🖉 ang 🤟 P2P BoulBook	Allew 😹 High	
	14 🚳 Always (9081091) R. 🕷 ark 🖉 art 🖪 P2P 365609	Aller & Hot	
	15 W Always KUGCO Sule & any W on C 222 Suppo	Nite Rite	
	10 B Always FIGC Buls 1 Start Ware 222-200/200/100Eau)	Nice Rent	
	17 St elegent FOCO P. le 1 St and St an 2728-2000/PropPs-2000	Alter - Int	
	a Alvera (DD00%) D4 Alvera (Alvera (D225) CD1-emand	A New Country	
	The second	BOARDAN BOARDAN	
		1.2	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源	Functions > Traffic Management > L7 Policy > P		
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且 在 上 一 章 節 中 我 們 已 建 立 一 群 組 Boss	Functions > Traffic Management > L7 Policy>P		
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源・ 且在上一章節中我們已建立一群組 Boss (HostCEO HostCTO)。選擇圖云 ♥Boss,音味著	Functions > Traffic Management > L7 Policy > P	olicy	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且 在 上 一 章 節 中 我 們 已 建 立 一 群 組 Boss (HostCEO, HostCTO)。選擇圖示 ^{愛 Boss} · 意味著	Functions > Traffic Management > L7 Policy>P	olicy w witcled. 12 A A Action Becany Prove C Attwo Action	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且 在 上 一 章 節 中 我 們 已 建 立 一 群 組 Boss (HostCEO, HostCTO)。選擇圖示 ♥Boss · 意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點	Functions > Traffic Management > L7 Policy>P	olicy w witcled. 12 ∡ ∡ Action Security You's Pice C +Live & Lingh ● Allow & Lingh	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 ♥Boss ·意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點	Functions > Traffic Management > L7 Policy>P	vilities. 12 x x Action Security Traine C +Low Strain ≪ +Low Strain ≪ how Strain	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且 在 上 一 章 節 中 我 們 已 建 立 一 群 組 Boss (HostCEO, HostCTO)。選擇圖示 ♥Boss ·意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy>P State State State State State State State State State State State State State State State State State State	vilities. 12 x x Action Security Prote C ALW & Lings ← ALW & Lings ← ALW & Lings ← ALW & Lings ← ALW & Lings	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源, 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 ^{愛Boss} .意味著 除了 Boss 這個群組外,所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy>P State Party Lot P2P Protocol Apply State Protocol Mo State Mo State Mo Protocol Mo Protocol Mo State Mo Protocol Mo Protocol Mo Protocol Protocol Protocol <	viteted. 12 x x Action Security frame Dice Action Security frame Dice Action A	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源, 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 ♥Boss,意味著 除了 Boss 這個群組外,所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy>P State Par Par Protocol Apply Schedule State Par Protocol Apply State Par State Par <	viited. 12 A A Action Becarity Protect C Attwork C Lingh C Attwor	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 ♥Boss ·意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy>P State ************************************	viicled, 12 A A Action Security Profes C ALAN & Ligh A ALAN & Ligh A ALAN & Ligh A ALAN & High A ALAN & High	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 愛Boss ·意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy>P State ************************************	Alber Phan	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且 在 上 一 章 節 中 我 們 已 建 立 一 群 組 Boss (HostCEO, HostCTO)。選擇圖示 ^{愛Boss} · 意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy>P State ************************************	viieles, 12 A A Acton becarity from Acton becarity from Acton Ac	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且 在 上 一 章 節 中 我 們 已 建 立 一 群 組 Boss (HostCEO, HostCTO)。選擇圖示 ^{愛 Boss} · 意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy>P State ************************************	viieles, 12 A A Acton Security *urine Acton Security *urine Acton Acton Acton Acton Atom Ato	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且 在 上 一 章 節 中 我 們 已 建 立 一 群 組 Boss (HostCEO, HostCTO)。選擇圖示 ைBoss · 意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	State Point State Point Let P2P Protocol Apple State Point Sta	Alber Bigh Alber Bigh	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且 在 上 一 章 節 中 我 們 已 建 立 一 群 組 Boss (HostCEO, HostCTO)。選擇圖示 ைBoss · 意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy>P State State P3P Protocol Apple State P3P Protocol P3P	Alber Alber Albert Albe	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源 · 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 ைBoss · 意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy>P State State P2P Protocol Apple State P2P Protocol Apple State	Alber	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源, 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 ♥Boss ·意味著 除了 Boss 這個群組外,所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy > P State State Condition Condition On Horseol Apply State State On Horseol On Horseol <th< td=""><td>Alber Alber Alber</td></th<>	Alber	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源, 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 ♥Boss .意味著 除了 Boss 這個群組外,所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy > P State Or distant Or distant </td <td>Alber Alber Alber</td>	Alber	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源, 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 ♥Boss .意味著 除了 Boss 這個群組外,所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy > P State State State Protocol Apply Scherule - Protocol State State Or office Protocol Apply Scherule - Protocol Or office Office Of	Alow Alay Alow Alay	
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源, 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 ♥Boss . 意味著 除了 Boss 這個群組外,所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy > P State State State Protocol Apply Scherulz Scouth- Traffic No Protocol Apply Scherulz Scouth- Traffic No Protocol On ddian No Protocol Scouth- Traffic No Protocol Scouth- Traffic No Protocol Scouth- Traffic No Protocol Protocol Protocol No Protocol Protocol Protocol No Protocol Protocol Protocol Protocol Protocol Protocol Protocol Protocol Protocol Protocol <th c<="" td=""><td>Alow Alay Alow Alay</td></th>	<td>Alow Alay Alow Alay</td>	Alow Alay Alow Alay
步驟 4 選擇來源端 IP 因為CEO與CTO有完整的許可權存取網際網路資源. 且在上一章節中我們已建立一群組 Boss (HostCEO, HostCTO)。選擇圖示 愛Boss . 意味著 除了 Boss 這個群組外 · 所有來源端 IP 使用點對點 傳輸軟體都套用選定的應用層策略規則。	Functions > Traffic Management > L7 Policy > P State State State Protocol Apply Scherule Security Thrifte State State State On ddan State On ddan State On ddan State On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan On ddan	Alber Alber	

步骤 5 選擇安全行為	Functions > Traffic Management > 17 Policy>P	olicy
		oney
在上具列的 Security Profile 選項上選擇套用	List Pap - Propiou - Apolic - Schedule Security Infic-	• • 12 Ister. 12 🗛 🗛
Block 在所有點對點傳輸軟體。	Status Condition - Jecunty-	Action
	NU. Schedule Eulemanne Marria P Edern	Ensurity Profile Files
	👘 Workin, SUNLEL Rule, 🧙 Bose, 👙 arv 🌾 P29-XLinial/Au 👩 Block 6. op	🗑 Allaw 🙀 Hah 🔮
	😸 🦉 Workin, EITTORSENT 🍓 Boss 🚑 arv 🔀 P29-Eltorsmößitomertißitometullore.	🕷 Alaw 🔍 🕄 High
	👘 🖓 Workin, EDONICEY, R. 💩 Bosk, 👙 arv 🌾 P2P-eConkey(eConkey(eXonepektuleVa)	💣 Allaw 🔍 🕄 High
	💦 🕷 Workin, FLASHGET, P. 🚭 Bosk, 👙 ark, 🚺 F2P-FlashGaljElashGaljTucTub	💣 Alaw 🔍 High
	📑 🦝 Winkin - WitchY Rule 1 🙅 Brisk 👙 ark 📝 P2R-Wanny	💣 Allow 🔍 High
	🐘 🦓 Wirkin, EZEEEEELUS, 🥵 Disk, 👰 ars, 🍈 E22-azEaar?us	🗑 Alaw 🔍 🔍 High
	👘 🖉 Worker, FASTTRACK . 🧔 Anse 🥥 ark 🌃 P29-Esstrack/Kasas/Srok-Lenitiesr) 👘	🔮 Alaw 🔍 🔍 High
	🔲 🛛 🖓 Wirkin - ONUTEL A.G. 👺 Disk. 👰 ark 🔮 P23-Ormata;EctypeFeedFeedFeedFeedFeedFeedFeedFeedFeedFe	💣 Alaw 🔍 🕄 High
	🐘 🦝 Worsen, DUPO Pute t 🥵 Dose, 🥥 ary 🕞 P22-Koro	🕷 Alaw 🔍 🔍 High
	💷 🐻 Wirken DEFCIOON 🧔 Disk 🥥 ary 🍺 P2%DirectConnect(D	🔹 -low 🔍 Ugh
	🔢 🚮 Workin OPENIT_Dul 🥵 Dusk 🥔 ary 🎁 P2%-Dom(T)Crazesi-Cease)	💣 Alaw 🔍 🔍 High
	🕕 🦝 Wirkin 🖅 🥵 Disk 🖓 ary 🙆 P2N-58	💣 Alaw 🔍 🔍 High
	👘 🖓 Mursin, 2000 G.T.K., 🥵 Duss, 🤮 ary 🔶 P2N-SudSeek	🕷 -tow 🔍 Og High
	🚮 🖓 Winkin (GOODOOT_P. 🥵 Duse 🖓 any 🧧 P256 Duoge	🕷 -low 🔍 Ngh
	🔐 🖓 Markin, 165600_Gale, 👹 Duke 🔮 kry 🚱 129-Kagaa	🕷 Allow 🕺 High
	🔐 🦝 Yurkin, 1960_R.Jeji 🥵 Buse 🔮 ary 🥑 P2APigu(Figu/1988au)	🔹 +low 🕺 High
	👔 🖓 Marka, POCO_Role_1 🕵 Bussi 😫 ary 🛐 P2A-Paca)/Scar-PA-Panti	🕷 Alow 🕺 High
	👔 🖓 Wirkin, 200309/ALOA, 🥸 Boss 🔮 any 🥥 P2/400D0milias	🖝 -low 🕺 High 🔰
在工具列的 Traffic Profile 選項上選擇套用 Low 類 別在所有點對點傳輸軟體上。使所有即時通訊軟體的	List P3P V -Protection Apply -Stabular -Stabular -Stabular	v lates. 12 A A
	san Status Condition Taffe	Action
頻寬限制為 Low 類別。	Schedule Rule Name Plema Pledent, Fiolocol RHigh	h Pronte Prote
	🚯 Muran 2023 11 Pute 🚱 Duss 👹 are 🤇 P2Nunei(MurlerD2, 1/e) 🔂 Corr	C SQ 11.06
	🚳 Worken (111-005:EN) 🚱 Duss 🚱 ar y 👘 P2-46it escol/Homer(111: marviore	e -low QHab
	🚯 etnikan EDOMOTY P. 😨 Dinak 🥥 ark 🌾 P22-aConkas(aConkasOsamateMutaVa	🕷 Alow 🛛 🕄 High
	Amerin FLASHOFT P Sonse Stars 1 P2%-EachGeltEachGeltTucTu	MAINS QHigh
	👬 Workin, MithNY, Pulk 1 🕸 Bosk, 👙 are 🚮 P25-Wanny	Alow 🕄 Hah
	Workin EZFEERFLUS A Boss A o P29-40FAM-9 US	Alow SLHgh
	🚜 Workin, FAS TRACK, 🧟 Braz 👹 ars 🚺 P29-Fastrack(Kazaa@rokslanit/earr)	Alow 👯 High
	👫 Weikin, ION, TELIA, R. 🌨 Bose 👹 ary 🖉 P29-Orutal a Foryrat Feer Ee archarsion	Alow 😫 High
) 編 WorkinKURO_R.le_1 全Boss 髪ary 目 P2P-Kuro	Alow St.Hgh
	🚓 we (n., DRECTION) 🐞 Bost 🔮 ary 🔰 P2P. Directionnet/CliectConnect/C	Alow SL Hgh
	🦓 vio vin. (OPENFT_Rul. 🌚 Basa 😻 ary 👹 P2P OtenFT(Croznal-Leasy)	Allow Migh
	12 A WO JII. WREB Bass & ary M F2P fres	Aloc: MHgh
	ary 🍄 P2º BollBeck	Aloc: MHgh
	ang woo .m.,0080000'_R. ∰ Bos: ∰ ary 0 P2P 0:Booly	Alou: 🖬 High
	ary 👯 workin., KUGCO_Rula., 👥 Basa 🔮 ary 💘 P2P Kupoo	n Aloc: MHgh
	(1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	Millow: St High
	We workin, FUCO Pute 1 Se Bass AP ark W P2P PosoPocoPP Point	1000 WLHah

10.4.3 設定 VoIP 規則

步骤 1 啟用應用層策略	Functions > Traffic Management > L7 Policy>Policy
勾選 Fnable I 7。	2 Salas 2 Fully
	F Enable L7 Palce
	Description 1.10.1 synamler "level + 1.5 + 1.5. 2.12 putier type du = 1 fast moleth 1.10.1 synamler "level + 1.5 + 1.5. 2.12 putier type du = 1 fast moleth 1.10 puti
步 驟 2 列舉 VoIP 群組	Functions > Traffic Management > L7 Policy>Policy
	Saux & fuir-
任工具则之 Group 工選择 L设饰T VOLP。所有	(at a 172 a -bintant- a Anne -Sintennie a -Security a -bains a indexed (*) 4* 2*
VoIP 的清單就會顯示在螢幕上。	
	NO Crat Condition Ation Ation
	🕴 🕹 🖥 Eminet 🖉 Bullat. 🥵 Boos 🔮 env 🎸 P3P-Kurlei (kunistit), Situte) 💿 Alla= 🕷 Lave
	👔 👷 Fistratsf 🛛 ARENT. 🥵 Boss 🔮 any 🦙 P3P-B torreth/Bittorian/Bitxornal/uTorret. 🔹 Alia= 🙀 Law
	1 V F28 KEY R. S Boss Billion Vie P2F-aDonkey/aDonkey/Overnatizet/Us/Vie. Allo= 🖗 Low
	SP 1023 0UC-4L VOIEBUSTER
	🖉 Waldin and a man
	💥 Wardin, EZPEERPLUE, 😻 Boos 🔮 anv 🔗 PSF-azPearFlus 💿 Ala- 🗰 Law
	Workin, FASTTRACK, Se Boos any P2P.Fastrack)(czaa/broksteri Hosh) Alla-
	Windta VICO Duk Data Guran DDP Vica
	10 Wende TIPETTO'N Bass Bran U BED Districtionart/D
	11 W Workin, OPE-FT Ru, Stars Stars P2P-OpenFT/Crataa(Keeas)
	12 all Workin, pRES 🔐 Boos 🚇 any 🏤 P2P-bres 🔹 alla- 📸 Law
	13 👷 Worldin, BOLLBEEK, . 🚳 Boos 🏨 any 🤟 P3P-SoulBack 💿 Alla= 🙀 Law
	14 👹 Worldin, DOEODOry_F., 🏶 Boos 🏨 any 🧧 PSF-GeBoogy 💿 stilo= 🗰 Law
	15 👷 Workin, KUDOO_Rule, 👹 Boos 👹 any 🔃 P3P-Kugoo 💿 Alia= 🗰 Law
	10 👷 Vichin, Pioo_Rule_: 👹 Boos 👹 cm/ 👩 PSP. Pigo(Pigo(108ac) 🛛 🕢 Allow 🕷 Loow
	17 😹 Wandan, POCO_Fiula_ 🕵 Boos 🔮 any 🗹 PSP. Poco(Feco/Fe/Polint) 💿 Alia= 🕷 Law
	18 👷 Worldn : SQDSWNLCA 🧶 Boos 👰 any 🎧 PSP-QQDa+rload 💿 Alla= 🕷 Law
步驟 3 選擇排程	Functions > Traffic Management > L7 Policy>Policy
	St Cause Ma Date-
在上具列上選擇 WorkingHours 排程,將此排程	ist And a literate a fine thread a function of the state of the state
套用在所有 VoIP 群組中。您亦可以手動選擇每條	-Schecke-
座田程式列为政策的排程 。	NO Scherula Picklame (report Picklam) Alexet Princip
ルは「T11キュレン」「「同区大山」」ない。	1 2 News RTF_Ruit_1 2 are 1 and 1 an
	😰 🕼 Netys RTCP_Rule_1 😻 my 🗱 mr 👹 RHMaining 💿 Nice 🏨 High
	👔 🗑 Meays BKY2E_Rule_1 🔮 my 😫 and 📴 VOMOScore 🔹 👘 Mice 🚳 High
	1 @ Always SKYPEFLE_R. 壁 any 壁 any 道 VolP-SkypeFle Transfer 《 Alka- @ Figh
	a 🗑 Newys SK72EOUT_4. 壁 my 壁 ang 🕲 Volt-SkapeCol 🔹 Noe 🚳 Ligh
	👔 Alexys GP_Rite_1 😫 are 😫 and 😰 VolkGDWEN VocePation VoceMagal. 💿 Alte- 🚱 righ
	🕼 Alexys (D?) [P.Ja_1] 😰 are 🔯 any 🚳 Volf4 (DZ)(NetMeakop/Yoecom) 🛛 🚳 Alexy 🕼 rob
	If Always If 2, D, Is_1 If any If any If 2, D, Is_1 If any

步驟 4 選擇來源端 IP	Functions > Traffic Management > L7 Policy>F	Policy	
	A Since M. Policy	,	
因為CEO與CIO有元整的計可催存取網際網路貨	List 🕒 Va P 🗸 -Primaca - V Apply -Schedule- 🗸 -Security- V -Traffi	- v istes	12 [A] [A]
源,且在上一章節中我們已建立一群組 Boss	Satis Constor		n
(HostCEO, HostCTO) ∘選擇圖示 鬡 ^{Boss} · 意味	School.ie Ruie Fame Hiema P Ede Protocol	Security Profile	Fice
著除了 Boss 這個群組外,所有來源端IP使用點對	A We should BTCF_R. Ic_1	Alter 🔒	Hgh
點傳輸軟體都套用選定的應用層策略規則。	3 🦝 WorkhSKITE_R.to_1 🚾 Gr Soss HostCEO HostCFC	🕷 Alecc 🛛 🐊	LHgh
	4 🦉 Wolkin., SKIPEFLE_P. 🖉 Court 🖏 any 💽 VolP-Skype File Transfor	Alou:	Hgh
	SIR Storen SIR Suis 1 SIR Suis 1	Aloc: 👥	Hab
	7 📑 Weinn H333 Rule 1 📓 Bet 🖉 🖉 arr 🌚 VolP-H323): etcestingPotycom	Alow 🕄	LHgh
	8 - 關 Warkin, UUCALL_Rut, 委 any 委 ary ④ VolP-U_Call	🗑 Alow 🙀	Hah
	11 🦝 Workin, POFBUETER 👼 any 🖉 ark 🥥 VolP-VolPBustar	e Alow 🚯	LH gh
步驟 5 選擇安全行為 在工具列的 Security Profile 選項上選擇套用 Block 在所有點對點傳輸軟體上。	Functions > Traffic Management > L7 Policy>F	Policy	12 A
	Schedula P. Jo Name Internal IP Entern.	Socurty Profile	Ppp
	2 Workin, RTCP_Rule_1 2 Boss 2 on 2 VoP-RTCP	♦ Allo=	k - Igh
	1 🔊 Workin, SKYPE_Rule_1 🧟 Boos 🕸 am 🔞 Vo P-Skape	🔹 Alla= 🔗	k Iph
	4 副 Workin,SKYPEFLE_R、 編 Boos 译 any 🔤 Vo P-Skype File Transfer	e Alla-	k ⊢rph
	Workin, SKY2EOUT_S, Gelleves Starry To VolFSkypeOut	Alter St	2 - tgh
	1 Wulen 102: Pole 1 @ Does Lang Wul + Ozbite Hole and Pole area	Alu- (3	t ign
	n 🔄 Winkin USCAL Ru 🙋 Base 👺 sing 🔿 Va PADO si	6 AD- 0	ki ish
	💉 💐 Wellin VOPAUSTE 🧕 😵 🔤 🥵 ang 😡 Vort-Vorta, star	6 Alti- 13	R High
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。	Functions > Traffic Management > L7 Policy>F Status Folce List VCIP Status Folce ND Status Notific All Nome Internal IP Enem. Notific All Strengt Status Notific All Stren	Policy a policid a p	2 (A) () 0 200 2 -1gr 2 -1gr
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為	Functions > Traffic Management > L7 Policy>F Statis Folse Statis Folse NO Folse Schedue Role Mann NO Folse NO Schedue NO Schedue NO Schedue Notan	Policy	13 AX (a) 0 Ppe 4-197 4-197 4-197 4-197 4-197 4-197 4-197 4-197 4-197
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 →驟 7 調整 Skype 的安全行為 依公司政策允許員工上班使用 Skype ·所以您必須	Functions > Traffic Management > L7 Policy>F Statis Folicy Statis Folicy ND Exhecuse Statis Folicy ND Exhecuse Statis Folicy ND Exhecuse Statis France Notifin Strip Statis Strip Notifin Strip Statis Strip Notifin Strip Statis Strip Notifin Strip Statis Strip Notifin Strip Strip Strip Notifin Strip Notifin Strip Notifin Strip Notif	Policy	-3 A (s) Ppe -1gr -1gr -1gr -1gr -1gr -1gr -1gr -1gr -1gr -1gr
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為 依公司政策允許員工上班使用 Skype、所以您必須 手動調整 Skype 的安全行為到 Allow 的狀態。	Functions > Traffic Management > L7 Policy>F Status Folicy Status Folicy ND Efelus Status Folicy ND Efelus Status Folicy ND Efelus ND Efelus ND Efelus Northin, STP_Sulp_1 Stass Northin, STP_Sulp_1 Stass Northin, STP_Sulp_1 Stass Northin, STP_Sulp_1 Stass Northin, StPPERLE,R. Stass Northin, UOPERLE,R.	Policy Control island du Protection Bitck & og Bitck & og Bit	-3 A a -9 pe -9 pr -9 pr -
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為 依公司政策允許員工上班使用 Skype ·所以您必須 手動調整 Skype 的安全行為到 Allow 的狀態。 這樣 Skype 的流量才可以通過設備。	Functions > Traffic Management > L7 Policy>F Status Folicy Status Folicy ND Status Status Folicy Notifin. Status Notifin. Nocestatus	Policy Colicy	12 (A) (A) 10 2 pp 2 -1gr 2 -1gr
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為 低公司政策允許員工上班使用 Skype・所以您必須 手動調整 Skype 的安全行為到 Allow 的狀態。 這樣 Skype 的流量才可以通過設備。	Functions > Traffic Management > L7 Policy>F Status Folcy Status Folcy Status Folcy NO Elalus Status Folcy Notation Folcy Notation Status	Policy Colicy	12 (A) (A) 10 2 pp 4 -1gr 4 -1gr 4 -1gr 4 -1gr 4 -1gr 4 -1gr 4 -1gr 4 -1gr 4 -1gr 4 -1gr 5 -1gr 7 - 1gr 4 -1gr 4 -1gr
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為 低公司政策允許員工上班使用 Skype ·所以您必須 手動調整 Skype 的安全行為到 Allow 的狀態。 這樣 Skype 的流量才可以通過設備。	Functions > Traffic Management > L7 Policy>F Status Folcy List VCIP Elaus Creation NO Schedue Schedue Protocol NO Schedue Schedue Protocol NO Schedue Schedue Protocol NO Schedue Schedue Rule Nome Notifin Schedue Notifin <	Policy Colicy	12 (A) (A) Ppe 4-1gr
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為 低公司政策允許員工上班使用 Skype・所以您必須 手動調整 Skype 的安全行為到 Allow 的狀態。 這樣 Skype 的流量才可以通過設備。	Functions > Traffic Management > L7 Policy>F State State Folice List VCP Flate ND Echecule Rule Name The train ND Echecule Rule Name The train ND Echecule Rule Name The train NO Echecule Rule Name The train NO Echecule Rule Name The train Protoco Rule Name The train Rule Name Rule Name <td< th=""><th>Policy Colicy Colicy</th><th>12 x x 12 x x 14 - 197 14 - 197</th></td<>	Policy Colicy	12 x x 12 x x 14 - 197 14 - 197
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為 依公司政策允許員工上班使用 Skype、所以您必須 手動調整 Skype 的安全行為到 Allow 的狀態。 這樣 Skype 的流量才可以通過設備。	Functions > Traffic Management > L7 Policy>F Statis Folicy Ital VCIP Elsius Cradian ND Ensure Workin Stream Stream Stream Workin Stream Stream Stream Workin Stream Workin Stream Stream Stream Stream Stream Stream Stream	Policy Let v fallstad de v Prote v fallstad e Elcka og	
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為 依公司政策允許員工上班使用 Skype・所以您必須 手動調整 Skype 的安全行為到 Allow 的狀態。 這樣 Skype 的流量才可以通過設備。	Functions > Traffic Management > L7 Policy>F Status Folicy List VCIP Elsius Cradian ND Elsius Cradian France Northin Stream Protein Stream Northin Stream Stream VCIP-Elspee Northin Stream Stream Northin Northin Stream	Policy L- Policy	
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為 依公司政策允許員工上班使用 Skype ·所以您必須 手動調整 Skype 的安全行為到 Allow 的狀態。 這樣 Skype 的流量才可以通過設備。	Functions > Traffic Management > L7 Policy>F Status Folicy Ist VSP Edus Cradian ND Edus Status Folicy Ist VSP Status Folicy ND Edus Status Folicy Ist VSP Status Folicy Status Status Status	Policy L of listed du Protection Block & og Block	
步驟 6 選擇頻寬類別 在工具列的 Traffic Profile 選項上選擇套用 High 在所有點對點傳輸軟體上。使所有即時通訊 軟體的頻寬限制為 High 類別。 步驟 7 調整 Skype 的安全行為 依公司政策允許員工上班使用 Skype ·所以您必須 手動調整 Skype 的安全行為到 Allow 的狀態。 這樣 Skype 的流量才可以通過設備。	Functions > Traffic Management > L7 Policy>F Status Folicy Ist VCIP Status Folicy ND Status Status Folicy Northin Status	Policy Colicy	

10.4.4 攔阻 VoIP - Skype File Transfer



步驟 4 上傳設定檔

當設定好以上的政策規則後,請記得上傳設定檔到設備裝置上,否則當您重新連上裝置後,現行的設定檔就會被系統清除。 選擇 Upload Configuration 選項,或者點擊圖示 🙆 上傳現行的設定檔。

步骤 5 Skype傳檔的事件記錄	Functions	> Repo	rts > L7 > E	vent Vi	ew			
由右圖我們可以看出·RD 部門 IP 192.168.17.58	Functional View	Policy View	Personal View Ev	ent View				
企圖透過 Skype 傳檔·但被 設備 攔阻下來的事	Date : 2006-05-01	• ОК	🕺 🔣 💷					
件記錄。	Date	Application	Description	Protocol	Src IP	Src Port	Dst IP	Dst Port
	2006-05-18 13:59:38	skypefile	[BLOCK] skypefile	UDP	192.168.17.58	25991	192.168.17.56	16249

① 設定小技巧:

- 1. 如果您要選取/取消選取某條規則時,只要利用 < Ctrl > + < 滑鼠左鍵 > 在該規則的編號上點一下即可轉換選取的 動作。
- 如果在編輯應用層策略時,某條規則呈現淡黃色背景時,代表您已選取該條規則。如果您希望透過篩選工具列套用選 定的政策在所有的通訊協定上時,請將滑鼠移到第一條規則上,按滑鼠左鍵往下拉,當所有規則的背景都呈現淡黃色 時,代表所有規則已被選取。
- 3. 如果您要選取排列不連續的規則,您可以按住 < Ctrl >,然後透過滑鼠在選取的規則上點一下即可。

第11章

流量管理-頻寬通道策略

11.1 設定 Traffic Manager

11.1.1 需求

由於在 TCP/IP 網路環境中,所有流量都是"一視同仁",使得這些流量先搶先贏,越傳越大,導致網路頻寬在很多時候被少數人的垃圾流量佔用(比如 p2p),而無法保證正常的業務應用。因此為了保證網路頻寬分配的公平性,我們開發了針對每個 IP、每個 session 和每個網段來平均分配頻寬的功能。一下就來通過實例介紹一下此功能

11.1.2 QoS 的 Per-IP 功能

在 QoS 下的 per-IP 的功能針對每個 IP 來平均分配頻寬,保證每個 IP 頻寬都一樣。

實例:甲公司有 100 名員工 100 台 PC·另外有在電信 IDC 機房託管一台 server 以用作 WEB/FTP/MAIL 服務·公司內部 有 4M ADSL 公網頻寬可以使用·公司會通過 FTP 方式來更新網站內容以及開通每人的 FTP 帳號給每人存放工作資料。為 了讓大家用 FTP 傳檔時不會佔用整個頻寬·部門領導決定把 4M 頻寬專門劃分出一條 2M 的管道分配給 FTP 應用·並且同 時刻最多只能有 5 個人平均分配這 2M 頻寬進行 FTP 傳檔以保證傳檔的速度不會很慢。其他人要等到這 5 人中的某人 ftp 應用結束才能進行相應操作,另外 2M 頻寬做其他正常工作使用。具體設置如下:

步驟1 啟動 QoS Policy	QoS Policy>Status
步驟1 啟動 QoS Policy 勾選 Enable QoS Policy	Outside Service Status Status Status

步驟 2 編輯頻寬	QoS Policy>Action> QoS Tree
在頁面中滑鼠右鍵點擊 default-pipe,彈出選擇,再滑鼠右鍵點 擊·點選 add new pipes 來新增管線並 對管線頻寬進行設置。 將 Pipe Name 設為 1・Upload 和 Download 的 Guaranteed 都設為 2Mbps·將 Rate control among flows within th 設備 pipe 勾選;在 Flow type 中拉選 Per-IP·將 Max #flows 設 置成 5・設置完成後點選 OK 再次點選 add new pipes 將剩餘 的 2M 頻寬分配完・將 Pipe Name 設 為 2	Strace shall pipes of Selon's, gipt Image: Selon's, gipt Effit as remetaris by right-clicking the selecter pipe Note: These selects some pipe potofie that has inhered from this default the. You can only actual parameters but cannot modify the tree hierarchy unless you remove all pipe profile Deveload Mb(s) Image: Selecter actual pipe profile Optime the pipe: Corp pe parameters. Image: Selecter actual pipe profile Optime the pipe: Corp pe parameters. Image: Selecter actual pipe actual pipe Optime the pipe: Corp pe parameters. Image: Selecter actual pipe actual pipe Optime the pipe: Corp pe parameters. Upped Mb(s) Optime the pipe. Corp pe parameters. Optime the pipe. Upped Mb(s) Optime the pipe. Corp pe parameters. Optime the pipe. Upped Mb(s) Optime the pipe. Corp pe parameters. Optime the pipe. Upped. Most pipe. Corp pe parameters. Optime the pipe. Corp pe parameters. Optime the pipe. Corp pe bander. Optime the pipe. Deven
步驟 3:新增 Pipe Profile	Bitsis Carefilian No Bitsis Carefilian Addia Carefilian Addia Bitsis Carefilian Addia Bitsis Carefilian Page Profile Description



11.1.3 QoS 的 Per-Session 功能

在 QoS 下的 per-session 功能是根據每個 session 來平均分配頻寬,如果一個 IP 比其他 IP 多開了很多 session,那他得 到的頻寬就會比其他 IP 多。

實例:甲部門經上次使用了設備的 QoS 的 Per-IP 功能發現效果很好·所以領導決定就將 pipe 1 作為專供下載使用的管道· 為了使頻寬分配更具公平和靈活性·保證對頻寬需求大的人能夠得到更多的頻寬·部門領導決定使用 per-session 功能來 分配頻寬·具體設置如下:

步驟 1 啟動 QoS Policy 勾選 Enable QoS Policy	QoS Policy>Statu	Schools and a state provides soched a state provides soched a state provides soched a state provide parameters. solare es from the sebast tree the LALX selectures	
步驟 2 編輯頻寬 右鍵點擊 Policy · 點選 Edit th 設 備 profile · 彈出對話方塊後右鍵點擊 default-pipe · 點選 Edit child pipes ; 在對話方塊中選擇 pipe 1 · 右鍵點	QoS Policy> Policy Status Poley (action) Description Right-striking here allows you to ad You can create pipe another with dit Note: If schedules are overlapped, t	Cy bodd Pipe Profiles from the Dataset Tree Profil krent schedales, is former profile has lower priority Constition	e Arison
擊選擇 Edit pipe parameters · Flow type 中拉選 Per- session · 設置完成後 點選 OK	Bathedule	Interface Extractingence	Pipe Profile Description Net Description Editive profile Description profile
	Provi Tree 2 (d r 4) Mark B 2 (d r 2) Mark 1 (2 r 2) Mark 2 (d r 2) Mark	Up load barritividit prover.	Dewnload bandwidh 1 - (18 %) Bendwidh:: 2 Moly
		2-000%) Bondwidth: 2 Mark Dt Cascal	2 - (15 %) Bandwedlin: 2 Main

	Edit parameters by righi-olio	king the selected pipe.		
	Note: The tree hierarchy is in	heriled from the default	ine so only severa	al parameters are adjustab
	Name 1	Opload I 2	Abrs	2 Download Mors
	2	2	Add new	pipe
			Delete thi	s pipe
	Estivation raffe			
	Pipe Name 1	1		
	Upload		r	
	Cuaranteed 2	Mb;s)Rsman 0	Referenced amo	ng lows when this pipe.
	Domiwis-sitshis cancelon t	it ministration	Flow type [Fer Session 🧧 Nemesk 💷
	Max tendericiti	Wape@?ac 1000	Via: Allowe,	0 (0.5mlmtec)
	Pho:ty 1	(0.h.gh=st.p. ori-i	Vin fire cals:	0 (Auto)
	Cowrited			
	Queranised 2	Mtcs/P=man_0	I Sats ported area	cultes = thut be as a
	Tomers-sideble concerdent	o minisparent	Fin-tyse	Por Stosion
	Max transformath	Waps@Vac10000	Nax-Ric+s	10 Onlimited)
	Printy 1	(0 h gh=st p-od-)	Nix 100/rate	f (Multi)
	Ľ		<u>.</u>	(@)[0a:
步驟 3:啟動 L7 Policy	L7 Policy>Status			
勿避 Epoble 17 Policy,將 Put	Status Policy			
勾进 Ellable L/ Policy,府 Put	Enable L7 Police			
unmatched traffic into 設置成 2				
	Description Policy order: Per-IP + L4 + L7 2 L7 policy order: top-down first mab 3. Set needle so policy to News to an	ch sid performace skop.		•
		And the first firster		
	Contras Revenue to	a cut the f's boach.		
	Default Traffic Pipe	-		
	Put unmatchea traffic into : 🔮 2 😁	J	Data - Di Longo	
				and the second states
步驟 4:設置 FTP 應用的管線	L7 Policy>Policy			
 拉彈 Traffic 講所有應田 Pine 铅署	Status Pokcy			
	List -Category- 🖌 -Protocol-	Azoly -Schesure-	-Becurity-	-Traffic- v to listent
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	NO. Batedute Rule Name In	Condition	en Protocol	Action Action Profile Pile
拉選 Protocol 選擇 FTP·將其 Pipe	Alexyr 144100_Rale_1	any 🕮 are 🤐 Chathadanay	noof it is the second of the s	CAlm C2
	🗧 🧐 Alwayt ADL_Role_1 🖷	any 🕮 are 🛔 ChatAGU(AD)	WM TROVICO/TREAMED	anda. 🕷 Allan 🙀 2
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Always DMPP_Rule_1	any Ware O Charlosophia	ogre Takfönin)	CAIN Q2
	Minage DOCKNTROOM	any Mare (@ chab@chap	eo/8	a Alian (C)
	Contestin Para 1	any 🕮 are 🕅 Charlos Medi	efite TransferVision/Vision)	e Alma 🙊 2
	alinaya DOSHARE, Rus 👰	any Se and M Chat DO Shar	id Film da Dada Kabathian da Sur	Alter R 2
	U BAMer US, Role, 1	any ann of ChatUCODeal	0	Ales RZ
	11 (B Almen POPO_Rule_1 🗳	any 🖳 any 🥹 Chairmongo	po163)	Alan 😪 2
	Always ALMANONAND .	any 🗟 any 🤲 ChabAL/Wang	Wang(Taobao ALIWangWan	a Alex Sta
	The second section put of	and the same of campage	- art (2 m (83 %)	B. C. M.

	Status	Palks						
	List -Collegory- V THE Appy					-Sphedule- 🖌 -Security- 🖌 -Tra	nid.	
	NO	1	Bhadus	lan.		Condition	2	1506
		Schedule	Rule Name	intim.	Edam.	Protocol	Security Profile	Pipe
	al the second	C	In man	at 14	100.00	C. LIN IMPROVING	10 10 10 10 10 10 10 10 10 10 10 10 10 1	
步驟 5:上傳設定								
點擊 🧯 上傳設定								

11.1.4 QoS 的 Per-Net 功能

在 QoS 下的 per-Net 功能是根據每個網段來平均分配頻寬

實例:公司老總覺得頻寬分配在實際工作應用中的效果很好,非常讚賞這樣的做法,於是決定將公司新投入的 20M 頻寬專 門劃分出 10M 平均分配給各部門做檔案傳輸專用管道,公司有 5 個部門,每個部門分屬不同的網段,為保證網路傳送速 率,需限制最多只能有 3 個網段同時進行下載傳輸檔,於是公司網管使用了 QoS 下的 per-Net 功能,按網段來平均分配 頻寬,具體設置如下:

步驟1 啟動 QoS Policy	QoS Policy>Status
勾選 Enable QoS Policy	Bitles Painty Provide Cool Protor Coordination Table to cool and the cool as scheduled to the protons Table to cool and the cool as scheduled to the protons State to cool and the cool as scheduled to the protons State to cool and the cool as scheduled to the protons State to cool and the cool as scheduled to the protons State to cool and the cool as scheduled to the protons State Cool and the cool and the cool as scheduled to the debuilt bee Image: A cool and the cool and the cool and the debuilt bee Image: A cool and the cool and the cool and the debuilt bee Image: A cool and the cool and the cool and the debuilt bee Image: A cool and the cool and the cool and the debuilt bee Image: A cool and the cool and the cool and the debuilt bee Image: A cool and the cool and the cool and the debuilt bee Image: A cool and the cool
步驟2編輯頻寛	QoS Policy>Action> QoS Tree
在頁面中滑鼠右鍵點擊 default-pipe,彈出選擇,再滑鼠右鍵點 擊·點選 add new pipes 來新增管線並 對管線頻寬進行設置。	
將 Pipe Name 設為 1 · Upload 和 Download 的 Guaranteed 都設為 10 · 將 Rate control among flows	

within th 設備 pipe 勾選;在 Flow	n Zdiring child pipes of deforth_pipe 🛪
type 中拉選 Per-Net · 將 Max #flows	Edit parameters by right-clicking the selected proe
設置成 3·Netmask 設置為 24·設置	Note: There exists some pipe profile that has inherited from this default free.
完成後點選 OK	You can only adjust parameters but cannot modify the tree hierarchy unless you remove all pipe profiles
	Name Upload Mb/s Download Mb/s
	Add nev pipe Exit p pe parametere Determine piper OK Concel
	Editor. rupe Estr
	Fite Name (1
	-Other
	Custan feed (10)/hpeekertain 10 P Rate control among fows within his p.p.
	Comoversate is bendvalih from ny careni. Forekper: Per Net: Netmack: [1] Marchanetweite: Comoversate in the optimized i
	Prindly
	Diemosto Buaranteed 10 rebosilitation 10
	Eerrov avalacie bandvitith form motarent. Errorse Eerrov avalacie bandvitith form motarent. Errorse Eerrov avalacie bandvitith form motarent.
	Disc bandwidth: [1] Hops (Disc 00.0) Kosc #Tross 3 (1-500.1)
	Priority: 1 (0 trigheol priority) Min flow rate: 2.32 tripp (0, lo)
	OK Cursal
步驟 3:新增 Pipe Profile	QoS Policy> Policy
滑鼠右鍵點擊彈出對話方塊·點選 Add	Steps Policy Action
2 now profile 巫新增 Pine Profile	Description Riotic ricking have above you to added til Pipe Profiles from the Datast Tree Profile
a new prome 浓新項 Fipe Frome	You can create gipe profiles with different schedules.
	Note: It schedules are sweltapped, the former profile has lower priority
	NO Datas Canditan Astox
	Address and a second and a se
	Editor profes
步驟 4:啟動 L7 Policy	L7 Policy>Status
〜 勿躍 Epoble I 7 Dolicy 悠 Dut	
今选 Eliable L/ Policy,府 Pul	
unmatched traffic into 設置成 2	

	Status Policy		
	El Enable L7 Policy		
	Ouscription Policy order: Per-P + LA + L7 L7 policy order: Top-down finitimatch S Bet neereless policy to leave to avoid performance strop. Exercic Secure / Destination Exercic Sec		
步驟 5:設置 FTP 應用的管線	L7 Policy>Policy		
拉選 Traffic 講所有應用 Pipe 設置	teatus Policy List -CategoryProtocol Apply -SchedureSecurityTra	Ar- 😽 toiska	
成 2。	NO. Blatus Condition Tra	Action	
	Sthedule Rule Name Intern. Edem. Protocol	Profile Pipe	
拉選 Protocol 選擇 FTP · 將其 Pipe 設	👔 😸 Almaya 🕬 100_fisik_1 🕮 any 🕮 ang 🥥 Chab'tahon('rabool'Titlian(Misanda/Sain)	Alen 😪 2	
罢为 1	· · · · · · · · · · · · · · · · · · ·	Alm 2	
且₼↓	· 博 Aleman (SMPP_Rode_1) 壁 any 壁 ang () Chark/SMPP(Google Tablicain)	@ Alm (\$2	
	😸 Always: DO_Rule_1 🐯 any 🐯 ang 🧑 Stat DD	@ Alme 1 2	
	영 Aways DOCHATROCH 분 ary 분 are 🖉 Sat DOCSaRison	Also 🙀 J	
	Minays DOMERCH_Rate_TE any E are M Charlos Media/Fee TuedeoValae/View)	S Alama SC 2	
	· · · · · · · · · · · · · · · · · · ·	· Alm · · · · · · · · · · · · · · · · · · ·	
	0 Babuerr BADU_Rele_1 De ary Bary Bab Cash (Badu Badu Kadu Marada Babe)	Man R2	
	U 通 Alvera UC_Role_1 壁 are 健 are gd ChatUC(Sea UC)	Alen Miz	
	11 😸 Always POPO_Rule_1 😤 any 🗟 ang 🍪 ChakPOPO(popo165)	Alen St 2	
	😸 Always - PLINSHOWAHO, 🕎 aty 🔮 aty 🕐 (StabAL/WangWang/Taxbao AL/WangWang)	Alter St 2	
	11 (@ Always FETIDS_Pole_1) mary mary (@ ChabTelloc(Chinamathe Federa)	Alm M2	
	Status Policy		
	List -Calagony- V CITTE V Appy -Schedule- V -Security- V -Traffic-	to tisted	
	Condition	AcSoe	
	NU Bohazula Plute Name Infam Edam Protocol Be	curity Profile Pige	
	1 S Alway TTP_Tala_5 E are E are S fileTransferTTP	41w (41	
步驟 6:上傳設定			
點擊 上傳設定			

第5部

內容管理

第12章

內容管理策略

12.1 需求

- 1. 管理者導入已經設定好的內容策略的設定。
- 2. 管理者想將已設定好的內容策略備份存檔。

12.2 方法

- 1. 選擇"File Import"將編輯好的內容策略設定導入。
- 2. 選擇"File Export"將編輯好的內容策略匯出儲存成檔案。

12.3 步驟

當您啟用即時通訊管理,並上傳設定檔到 設備 裝置上時,內容策略立即受 設備 控管。設備 提供您三個方法來編輯內容 策略的清單:1) 從現存的 AD 伺服器匯入使用者資料(詳見第25章 AD 設定與應用);2) 將現有資料庫匯出的文字 檔匯入使用者資料;3) 手動自行編輯使用者清單。

管理者可以自行定義預設使用者的行為模式為攔阻或是允許通行。以下的範例,將介紹您如何設定內容策略。

12.3.1 從本地端檔案載入內容策略與其群組

可以將既有的資料庫按照內容策略的欄位元排列方式將資料匯出並存成純文字檔·然後藉由檔案匯入的方式將內容策略的 資料匯入。

步驟 1 可匯入的純文字檔	Functions > Content Manager > Content Policy > Policy> File
您從既有的資料庫匯出的文字檔必需依據右圖的	Import
格式・欄位與欄位間要用逗號分開。請注意・名	root, boss, Alvays, Others, disable, disable, *, *, *, *, *, Platinum, disable, allow, Platinum
稱是主索引鍵,不可重複,所以在您透過檔案匯	Buill, MIS, MINBYS, BUNELS, PHABLE, PHODIE, 2, 2, 2, 3, 7, 15, 1501,000, Flatton, Flatton, Flatton,
入使用者資料前,請檢查資料是否有重複、欄位	
是否符合要匯入的目標欄位。	



步驟3 選擇要匯入的欄位 一般情況是全部勾選所有的核取方塊,然後勾選 Would you like to overwrite ex設備ting users? 覆寫已存在的使用者,點擊 OK 進入下 一個視窗。	Functions > Import	 Content Manager > Content Policy > Policy> File Please select the columns which you want to import. Name Description Schedule Group Msg Record Sthe Provide
	E	MSN Account Yahoo Address ICQ Address AOL Address IM Service URL Record Web POST Web Service UWeb Service URL Record
步驟4選擇要匯入的檔案 選擇您要匯入的文字檔·然後點擊 Open 開始匯 入動作。	Look In:	My Documents
	File <u>N</u> ame: Files of <u>Typ</u> e:	Import test.txt All Files Open Cancel

步驟 5 匯入成功	Functions >	· Content I	/anager >	· Content P	olicy > Polic	:y> File
│ │	Import					
	inport					
訊息告訴您進人成功。點擊 Close 完成設定。		Import Mess	age			
		Line1: import is	s done.			
		Line2: import is Import complete	s done. te.			
						<u></u>
					Close	
步骤 6 顯示檔案匯入的結果	Functions >	· Content I	/anager >	Content P	olicy > Polic	:y> File
當匯入資料後.您可以在本頁檢視匯入結果。請	Import					
 注意·匯入的資料其設定都是預設值,網管人員	N0	Elatus	Constion		Arlan	
	Schedule 1 & Abvava	Pule Name	Name	W Profile Platnum	eVeb Frofile Platnum	Vitual Orcups Officers
必須視情沉調整母位元内容策略的規則。	2 🙀 Always	rris	acimin	Patnum	Patnum	Offers
	Always	Cefault User	DefaultJeer	Painum	P atnum	Of ers
步驟7上傳設定檔	1					
│選擇 Upload Configuration 或點擊圖示 💌 將	設定檔上傳到裝	置上。				

12.3.2 手動編輯內容策略

步驟1 新增內容策略 F	unc	tions > Co	on	itent N	lanage	r > Content	Policy >	Policy	
在 Content Policy 視窗上按右鍵,然後選擇	월 Fratua 월 Poliky 월 Actino								
New User •	List	Virt. al Group	y	M Profile	- 4	-Vielo Frofile			Search
	Арр у	-Schedue	~		oup 👻	-it: Frofile	-Web Profile-	🚽 to lister	1
	NO.	Star	IIR		Condition			rion	
	1	Schedule		Ruis Name	Hanne	Iti Frofie Pistenni	(s)db	Profile	Vidual Groups
	2	🖉 ribuces	17	15	acimin	Pictinum	Pla	tinum:	Others
	3	Atress	0	efeull User	DəfaulUser	Pistirum	Pla	tinum	Others
					Edr U Edr U Dewis	sar sar staar Al			

步骤 2 輸入相關資訊	Functions >	Content M	anager >	Content P	olicy > Policy	/
翰入相關資訊後(欄位含義請看下麵介紹)。點擊	Create a new up	ar.				
OK 關閉窗口。	Schedule :	at 1971 Adways	Virtual Grou	up : Others	~	
	Basic	and a control of the	-0 - 222-222	e Licoles		
	Rule name :		Name	1		
	The Name field o	could be AD account, A	D group, or Web i	.ngin account.		
	IM					
	MSG Rec	🔿 Enable	💿 Disable			
	File Rec :	🔿 Enable	Oisable			
	MSN Account:	Allow	*		115	
	Yahoo Account :	Allow	*			
	AOL Account:	Allow	*			
	ICQ Account :	Allow	*			
	IM Service :	Platinum			~	
	Web					
	URL Rec :	🔿 Enable	 Disable 			
	Web POST.	Allow			~	
	Web Service :	Platinum			~	
				Pinish	Cancel	
步驟 3 檢視已編輯好的內容策略	Functions >	Content M	anager >	Content Po	olicy > Policy	/
	NO	Etatus	Condition		Action	
利增加的內谷來哈的設定卻定項設置,納官八貝	NU. Schedu	le Rule Name	Name	IC Froßie	Web Profile	Virtual Groups
必須視情況調整每位元內容策略的規則。	🖬 Ahvays	bose	7007	Patirum	Pistirum	Clhars
	😨 🖬 Atways	mis	acimin	Patrum	Platinum	Cihers
	🥶 Always	🛩 poweruser	ten	Palnum	Plateom	Clhers
	Atrops	Default User	DefaulUse:	Palnum	Plalicum	Clhars
歩聯4上傳設定檔 選擇 Upload Configuration 或點擊圖示 ፩ 將	設定檔上傳到裝				7100400	

欄位	說明	範圍/格式	範例
Schedule	啟用或取消內容策略政策規則的時間。	Always / Never / 使用者 定義	Always
Group	使用者定義的內容策略群組。	使用者定義	boss
Msg Rec.	即時通訊訊息側錄器。當您開啟時‧所有即時通 訊訊息都會被側錄。	🥥 (啟用)/ 🗢 (取消)	0
File Rec.	即時通訊檔案側錄器。當您開啟時‧所有即時通 訊檔案都會被側錄。	🥥 (啟用)/ 🗢 (取消)	0
Rule Name	内容策略規則名稱。	使用者定義	Rule_1

Name	内容策略的名稱。	使用者定義	сео
MSN account	MSN 帳號。	MSN 帳號格式	ceo@hotmail.com
YAHOO account	Yahoo 帳號。	Yahoo 帳號格式	ceo1111
ICQ account	ICQ 帳號。	ICQ 帳號格式	
AOL account	AOL 帳號。	AOL 帳號格式	Ceo111
IM Service	即時通訊使用行為許可權。	使用者定義	Platinum

表格 12-1 內容策略欄位說明

12.3.3 自動學習內容策略名單

為了讓管理者能夠快速設定使用者的即時通訊帳號,設定了即時通訊帳號自動學習的功能。管理者只要利用即時通訊記錄 器上側錄到的帳號,即可按右鍵選擇帳號匯入的方式即可。詳細設定,請參照下表說明。

步驟1 匯入所有使用者	Functions > Auditor > IM
在 Non_IM_Users (非 IM Users 清單上的帳號)上按右鍵,選擇您要將即時通訊帳號匯入的方式。 注意,已經加入的群組或即時通訊使用者就不可以再次 匯入帳號了。也就是說,當您將 Non_IM_Users 的帳號匯入 IM Users 清單內, 則系統將會自動將該帳號顯示為 IM Users 上所 設定的名稱。記錄器上所顯示的樹狀圖,第一層為 群組、第二層為 設備內部的即時通訊帳號、第三 層為該帳號與其它帳號之間的通訊記錄。	Date : 2006-05-01 V OK OF INDEXT OF INDEXT. TO BE INDEXT OF INDEXT OF INDEXT OF INDEXT OF INDEXT OF INDEXT OF INDEXT. TO BE INTENDED AND A DATA INTOXIC INTENT. TO BE INTOXIC INTENT OF INDEXT. TO BE INTOXIC INTOXI
	Reload Clear

欄位	說明
Import all accounts to IM User using IP as	將所有已記錄的帳號匯入內容策略中·並以其傳送/接收訊息者的
username	IP 為使用者名稱。
Import all accounts to IM User using hostname	將所有已記錄的帳號匯入內容策略中‧並以其傳送/接收訊息者的主
as username	機名稱為使用者名稱。
Clear records	清除所有通訊記錄。

表格 12-1 自動帳號學習 - 匯入所有非內容策略清單上的帳號



Field	Description	Example	
Import as a pow IM usor	將選定的即時通訊帳號·以新增一筆新規則的	4286963	
	方式匯入內容策略清單內。		
Import as an ox 沿借 ting IM Usor	將選定的即時通訊帳號·匯入已存在的內容策	- Friend	
	略清單內。	EVdII	
Import to IM Licer using ID as username	將選定的即時通訊帳號·依其 IP 位址命名匯	192.168.168.10	
	入內容策略清單內。		
Import to IM User using hostname as	將選定的即時訊帳號,依其主機名稱稱匯入內	APC Evan	
username	容策略清單內。	ABC-EVAII	
Clear records	清除選定帳號的所有記錄。		

表格 12-2 自動帳號學習 - 匯入選定的非內容策略清單上的帳號

12.3.4 從本地端檔案匯出內容策略與其群組

為了避免不可預期的因素,造成已設定好的內容策略設定檔損毀,您可隨時將內容策略匯出成檔案儲存,以備不時之需。

步驟1 檔案匯出	Fun	ctions > C	Content N	Manager	> Content	Policy > Policy	
■P.费 File Fuelente 医山中空等略容约1		Eb	105	Condition		Action	
點擊 File Export 進山內谷東哈貝科。	NU.	Schedule	Rula Nama	Name	12 Frofile	Web Profile	virual Groups
	1	S N=3/2	0066	1007.	Platnum	Platnum	Clhere
		(a) N=0/S	ms	acimin	Pialinum	Platrum	Cihara
		the majo	DafaultUser	DefaultUppr	Piatrum	Plattrum	Citors
		W. C. C.					
	4			Ę	St 10 Jack Lepen	🔹 🔁 File Lepert 🗎	S file Squet
步驟 2 輸入要儲存的檔案	Fun	ctions > C	Content N	Manager	> Content	Policy > Policy	
在 File Name 欄位內輸入要儲存的檔案·然後點	> File Export						
墼 Save 儲存。			-				
		Save (n:	My Docu	ments		- 6 6 6 8	8 8-
		filelik	5	My S	kype Received Fil	es SkypeSetup.exe	
		ICQ L	Lite	Syma Syma	antec	technical.txt	
		MSN	Messenger §	i 🖾 Test		Vs.rar	11.50
		My M	fusic	□ vs		Yahoo! Briefcase.	url
		My P	ictures	WAL	L		
		My R	eceived Files	🗋 Insta	ntblock-db.txt		
		•			- 6 1 16		
		File Nam	e: fileExpo	ort			
		Files of 7	All Film	5			
		Files of 1	she. All thes	,			
						Save Car	ncel
步 驟 3 匯出完成	Fun	ctions > C	Content M	Manager	> Content	Policy > Policy	
當檔案匯出成功後·將有如右圖的訊息告知您。請	>	- ile Export	t	5			
點擊 OK 結束設定。		•					
				Expo	ort Complete.		

12.3.5 內容策略設定輔助工具列

為了加速內容策略的設定,設備提供下列設定輔助工具列: 1) 列舉(L設備t) 選定的專案。所有選定的群組/服務將 被列舉在螢幕上。2) 套用(Apply) 選定的專案到列舉的內容策略清單中。



欄位		說明	範圍 / 格式	範例
L設備也	Virtual Group	列舉選定的群組在內容策略清單上。	使用者定義的群組	Boss
	IM Profile	列舉選定的服務在內容策略清單上。	使用者定義的服務	Glod
	Web Profile	列舉選定的服務在 Web 清單上。	使用者定義的服務	
	Schedule	套用選定的排程到列舉的內容策略清單上。	使用者定義的排程	Always
	Virtual Group	套用選定的群組在內容策略清單上。	使用者定義的群組	
Apply to l 铅借	IM Profile	套用選定的 MSN 規則到列舉的內容策略清單上。	使用者定義的服務	Bronze
ted.	Web Profile	套用選定的服務在 Web 清單上。	使用者定義的服務	Bronze
Search		此搜尋功能讓您利用關鍵字快速尋找特定的規則。		

表格 12-2 內容策略輔助設定工具列

InstantScan User Manual

第13章

內容管理-網頁管理

本章節介紹 IntantScan 的網頁管理功能與其設定。

13.1 需求



圖表 13-1 透過網頁過濾防止員工流覽被禁止的網站

1. 如圖表 13-1 所示 · PC1_1 正在流覽 WebServer3 的網頁 · 網頁的內容包含 cookies · Java applets · Java scripts 或者 ActiveX 物件等 · 這些內容也許包含惡意程式伺機竊取使用者資料 · 所以 · 您希望能夠禁止 PC1_1 下載這些 禁止流覽的組件 ·



圖表 13-2 透過網頁過濾禁止員工流覽 WebServer3 的網頁

 如圖表 13-2 所示·PC1_1 在上班時間流覽禁止流覽 WebServer3 的網頁。這些網頁內容也許包含股票市場資訊、 暴力或色情,且會浪費公司網際網路的頻寬,降低員工生產力。所以,您希望透過設定 設備就可以攔阻 PC1_1 流 覽這些類型的網站。

13.2 目的

- 1. 移除網頁內含的 cookies、Java applet、ActiveX 對象等。
- 2. 防止員工連上禁止流覽的網站。

13.3 方法

- 1. 設定要過濾的網頁元件,例如 cookies 或 Java applets。
- 2. 設定網頁過濾。當流覽網頁時,設備會根據設定的規則檢查網域、網址或關鍵字來判斷是否放行網頁流量。

13.4 步驟

步驟1 啟用網頁過濾 勾選 Enable Web Manager。 請注意,當您套用網頁過濾時,系統將自動勾選過 濾所有流經標準 HTTP(80埠號)的網頁流量。若 想要將某些人除外,可勾選 Enable Exempt Sources,其中Exclude是除外,Inlcude是只對選 定的人進行Web過濾。	Content Manager > Web > Status
步驟 2 編輯Web Profiles 決定Web Profiles的各個許可權等級。 你可以新增Web Profiles · 或者編輯現有Web Profiles。	Content Manager > Web > Web Profiles Status Void Profiles Classif Profes Non Elected Cologenes Provincer 2 Orid Pet Met. Kib IM Discotter, Induct Manage, Chat Noon Provincer 2 Orid Pet Met. Kib IM Discotter, Induct Manage, Chat Noon Petrophysics Sports, Sports, Status, Void IM, Bing, Discotter, Some, Induct Manage, HEMS, Shoss, Panagaight, Sports, Sports, Status, Chat Noon 2 Silver Petrophysics Sports, Status, Edit Benkics Parms, Induct Manage, HEMS, Shoss, Panagaight, Sports, Sports, Sports, Sports, Status, Sports, Status, Sports, Sports, Status, Sports, Sports, Status, Sports, Status, Sports, Status, Sports, Status, Sports, Status, Sports, Status, Sports, Track, Trace, King Web Met, Status, Status, Fort, Induct Manager, HEMS, Paris, Induct Manager, Manager, Paris, Induct Manager, Paris, Induct Manager, Paris, Induct Manager, Paris, Induct Manager, P
步驟3 編輯Silver Web Profiles 將您想要阻擋的Web database網站種類 · 加到 Silver 等級的Web Profiles · 若用戶被指定為此 Service者 · 連到這幾種網頁時 · 就會被阻擋 ·	Edit Service Name : Silver Blocked Categories Web Mail Web IM Blog Discussion Game Instant Message NEWS Photo Pornography Sports Stocks Finish Cancel

步驟 4 於Content Policy > Policy 加入用 戶	Functions > Console > User Console	
你可以從AD Import進來使用者資料,然後讓使用 者登入時自動讓系統得知AD登入,並對其後的 Web Profiles作相對應的過濾。 系統內建DefaultUser,任何沒有比對身份到的 Web流量,都會給予設定的Web Profiles。	And Corcups NO Group Nome Description No Group Nome Christian Control of Statul group Name for control registration Christian Control of Statul group Name for control registration	Cleb Protife Fladin.m Sold Silver Domose NewViser
步骤 5 訂定信任的網域 勾選 Enable Trusted Destination。然後新增 信任的網域群組與網功能變數名稱稱。	Content Manager > Web > Global Policy>Web Sites	> Trusted Des
請輸入信任的網功能變數名稱稱。注意,如果 您所輸入的網功能變數名稱稱無法被 DNS 伺服器辨識,這筆網功能變數名稱稱將會被忽 略。再則是,如果您啟用太多的網功能變數名 稱稱,在開始網頁過濾時將需要較長的時間來 作名稱辨識。	Freedottine Tor Hoas Instead alles listed here will not be filtered by the Web Manager	

欄位	說明	範圍 / 格式	範例
Enable Exempt Sources	啟用用除外來源端。	啟用 / 不啟用	啟用
Exclude from the web filter enforcement	所列舉的 IP 位址除外 · 其餘的電腦皆強 制執行網頁過濾。也就是說當您選擇 Boss 時·除了 CEO 與 CTO 外的 IP 都 需要執行網頁過濾。	啟用 / 不啟用	啟用 / Boss
Include in the web filter enforcement	網頁過濾只適用於所列舉的電腦。	啟用 / 不啟用	不啟用

表格 13-1 除外來源端欄位說明

步驟 6 客制化 URL 關鍵字攔阻	Functions > Content Manager > Web > Global Policy>Web Sites>
步驟 6 客制化 URL 關鍵字攔阻 勾選 Custom_URL · 攔阻任何包含關鍵字清單之 URL 位址。設備 已預設一些常用的關鍵字,如不 敷需求您可以在螢幕上按右鍵新增/修改/刪除關鍵 字群組/關鍵字。	Functions > Content Manager > Web > Global Policy>Web Sites> Custom

欄位	說明	範圍 / 格式	範例
URL Keywords	如果您要流覽的 URL 網址出現所輸入的關鍵 字·當您利用網際網路連上此網址後·此 URL 的內容將會被設備攔阻。	文字字串	Adv/advert 設備 e/adsrv/ banner/splash

表格 13-2 URL 關鍵字過濾

步驟7 網頁物件特徵過濾	Functions > Content Manager > Web > Global Policy>Web
勾選 Enable Object Blocking。然後勾選要利用特 徵過濾的網頁物件。當您啟用此功能後.透過PC1_1 流覽網頁可能還可以看到這些物件。這可能是因為 網頁暫存(cache)所致。請清除所有網頁流覽器 內的網頁暫存記憶.關閉流覽器。重新開啟流覽 器.然後重連網頁即可。	Status Methods Methods <

欄位	說明	範例		
啟用物件特徵攔阻	選擇以下的網頁元件以作為網頁之特徵過濾。	啟用		

ActiveX	過濾包含 ActiveX 的網頁。	啟用
Java	過濾包含 Java 的網頁。	啟用
Cookies	過濾包含 Cookies 的網頁。	啟用

表格 13-3 網頁特徵過濾

欄位	說明	範圍 / 格式	範例	
Enable Keyword Blocking	啟用網頁內容關鍵字攔阻。	啟用 / 不啟用	啟用	
Stop transferring the web page when the same keyword appears for <u>times</u> .	當勾選關鍵字攔阻,如果您要開啟的網頁中含有本 頁所列舉的關鍵字,此網頁將會被攔阻而無法正常 顯示。"限關鍵字每出現 次" 意味著只要關鍵字 出現等於或大於所輸入的數字時,攔阻要開啟的網 頁。例如,只要關鍵字出現5次,攔阻該網頁。	啟用 / 不啟用 數字	啟用 5 次	
Keywords	輸入您想攔阻的關鍵字。	文字字串	adv advert 設 備 e adsrv banner splash	

表格 13-4 網頁關鍵字過濾

第14章

容管理-即時通訊方案

14.1 需求

- 1. 網管人員希望依照工具性質來定義每位元員工的即時通訊行為之許可權。
- 2. 所有員工將依工作性質分成許多不同的群組,以方便網管人員控管其網路之使用。

14.2 方法

- 1. 定義即時通訊服務,讓管理者可以視使用者需求為其選擇適當的服務。
- 2. 將每個員工分配到其適合的群組中。

14.3 步驟

14.3.1 即時通訊服務

步驟 1 預設即時通訊服務	Fun	unctions >Content Manager > IM > IM Profiles											
預設即時通訊服務如右圖所示。你可依照您的需		Name	LOGIN	FILE_TRAN	FILE_SHARI	APP_SHARI	PHOTOSWAP	VOICE	WEBCAM	WHITEBOARD	REMOTE_A	GAME	HANDWRIT
		Platinum	۲	0	<u></u>	0	0	۲	0	<u></u>	9	۲	e
求修改或删除預設服務規則。	2	Gold	0	0	9	9	۲	۵	۲	۲	۲	•	•
注意,如果某條即時通訊服務規則已被其它規則	3	Sliver	۲	۲	۲	۲	۲	۲	۲	٥	•	•	•
使用了,您不可以直接删除此提削,如欲删除,	- 4	Bronze	۵	۲	0	۵	٢	•	۰	۰	•	•	•
	5	Normal	۲	٢	۰	•	•	۲	٢	٢	•	•	•
請先刪陈所有已包含此服務規則的具它規則。 		NewUser	•	•	•	•	•	•	•	•	•	•	•
步骤 2 新增即時通訊服務 Functions > Content Manager > IM > IM Profiles													
<u> </u>	N0.	Name	LOGIN	FILE_TRAN	FILE_SHARL	APP_SHARI	PHOTOSWAP	VOICE	WEBCAM	WHITEBOARD	REMOTE_A	GAME	HANDWRIT
剂涡锅炒到研防遮积减汤工及石 <u>碎</u> 流及 <u>和</u> 运	1	Platinum	٢	9	9	9	0	۲	9	•	9	۵	•
New Service •	2	Gold	۲	۲	۲	۲	۲	۲	۲	۲	۲	۰	•
	з	Silver	٢	۲	۲	٢	۲	۲	۲	۰	•	۰	•
	4	Bronze	٢	0	0	۲	0	•	۰	۰	۰	۰	•
	5	Normal	۲	•	•	•	•	•	•	٥	•	۰	•
	6	NewUser	٢	۰	۰	•	٥	۰	۰	٥	۰	۰	•
				Ne De	w Service lete Service lete All								

步驟 3 輸入新服務名稱	Functions > Content Manager > IM > IM Profiles												
輸入新增服務的名稱,然後點擊 OK 關閉視窗。	Please input service name Tin OK Cancel												
步驟 4 開啟適用此規則的即時通訊行為	Functions > Content Manager > IM > IM Profiles												
新增的即時通訊服務規則預設為禁止所有即時通	NO.	Name Platinum	LOGIN	FILE_TRAN.	FILE_SHARI.	APP_SHARL	PHOTOSWA	P VOICE	WEBCAM	WHITEBOAR	D REMOTE_A.	. GAME	HANDWRIT
訊行為·所以當您新增一條規則即要調整其預設	2	Gold	0	0	0	0	0	0	0	0	0	•	•
設定。	3	Silver	۲	0	0	0	۲	0	۲	•	•	•	•
	4	Bronze	۲	۲	۲	۲	۲	•	•	•	•	•	•
出現即可。	5	Normal	<u> </u>	•	•	•	•	•	•	•	•	•	•
	7	NewUser	•	•	•	•	•	•	•	•	•	•	•
	Functions > Content Manager > IM > IM Profiles												
	NO.	Name	LOGIN	FILE_TRAN.	FILE_SHARI.	APP_SHARI.	. PHOTOSWAR	P VOICE	WEBCAM	WHITEBOAR	D REMOTE_A	GAME	HANDWRIT
啟用 Login、FileTransfer、與 Voice。	1	Platinum	•	•	•	•	•	•	•	•	0	•	•
	2	Gold	<u></u>	<u></u>	0	0	<u></u>	<u></u>	<u></u>	<u></u>	©	•	•
	4	Bronze	0	0	0	0	0	•	•	•	•	•	•
	5	Normal	۲	•	•	•	•	•	•	•	•	•	•
	6	Tin	۲	۲	•	•	•	0	•	•	•	•	•
	7	NewUser	٥	•	•	•	•	•	•	•	•	•	•
步骤 6 變更即時通訊服務規則名稱	Fur	nction	s > C	onten	t Mar	nager	> IM	> IM	Profil	es			
在選取的規則上按右鍵·然後點選 Edit Entry。	NO.	Name Platinum	LOGIN	FILE_TRAN	FILE_SHARI	APP_SHARL	PHOTOSWAP	VOICE	WEBCAM	WHITEBOARI	D REMOTE_A	GAME	HANDWRITE
	2	Gold	٥	٥	٥	٢	0	0	0	0	0	•	•
	3	Sliver	۵	۲	٥	۲	۲	۲	۲	•	•	•	•
	4	Bronze	•	0	•	0	•	•	•	•	•	•	•
	5 6	Tin	0	0	0	0	0	0	0	0	0	•	0
	7	New Servic Delete Service	ce vice	•	•	•	•	•	•	•	•	•	•
		Delete Sele Delete All	ected										
		Edit Entry	ht D										
步驟 7 編輯服務名稱	Fur	nction	s > C	onten	t Mar	nager	> IM	> IM	Profil	es			
輸入您要修改的服務名稱·點擊 OK 關閉視窗。		1											
	Please input service name												
	opeeu												
	OK Cancel												
步驟 8 刪除服務 Functions > Cont

將滑鼠移到要刪除的服務規則上按右鍵·點選 Delete Service 或 Delete Selected 即可刪除 此服務。

Functions > Content Manager > IM > IM Profiles LOGIN FILE_TRAN... FILE_SHARI... APP_SHARL PHOTOSY NO Name VOICE WEBCAM WHITEBOARD REMOTE_A... GAME HANDWR Platinum ۲ 0 0 0 0 0 0 ۲ 0 0 0 Gold ٢ ٢ ٢ ٢ ۲ ٢ ٢ ٢ ٢ • • Sliver ٢ ٢ 0 0 0 0 ۲ • ٠ ٠ ٠ 0 0 ۲ ۲ ۲ • • ٠ ۰ ۰ Bronze • ٢ ٠ ٠ ٠ ۰ ٠ ۰ ٠ ٠ ٠ ۰ Normal 0 • Tin 0 • 0 0 • 0 0 • Delete Service • • • • • • • • • Delete All

步驟 9 上傳設定檔到裝置上

選擇 Upload Configuration 或者點擊圖示 💽 ·將現行的設定檔上傳到裝置上。

即時通訊使用行為	說明
登入	允許使用者登入即時通訊軟體與其它即時通訊使用者線上傳送訊息。
檔案傳送	允許即時通訊使用者與其它使用者傳送或接收檔案。
檔案分享	允許即時通訊使用者與其它使用者分享檔案。
應用程式分享	允許即時通訊使用者與其它使用者分享應用程式。
相片分享	允許即時通訊使用者與其它使用者分享相片。
語音	允許即時通訊使用者與其它使用者使用語音交談。
影像	允許即時通訊使用者與其它使用者透過視訊交談。
白板	允許即時通訊使用者與其它使用者透過白板書寫筆記、畫圖或傳送簡訊。
遠程協助	允許即時通訊使用者與其它使用者使用遠端協助功能。
遊戲	允許即時通訊使用者與其它使用者互相玩線上遊戲。
手寫	允許即時通訊使用者透過手寫功能傳遞訊息。

表格 14-1 可管理的即時通訊使用行為

14.3.2 即時通訊群組



步驟 2 編輯群組說明	Functions > Content Manager > Content Policy	
將滑鼠移到 Boss 規則的說明欄	盤 Sales 懿 1007 懿 Allen	
位上按右鍵,然後選擇 Edit	(j) Vitast Croups VO. Group Name Descriptor MProfile Web Profile	
Group •	1 Low Seven Seven	
	2 Chen Defait group name for used nog deather East Straus Duetter Nuetter Nuetter	
	Deere Croup Deere Al	
	Functions > Content Manager> Content Policy	
ケ Contant 潤位内給入你再为		
此群組做的說明·然後點擊 OK	Edit group	
繼續。	Name : Boss	
	Description : Full permission	
	IM	
	IM Service : Platinum 🔽	
	Web	
	Web Service : Platinum	
	Finish Cancel	
步驟 4 設定此群組的預設服	Functions > Content Manager> Content Policy	
務	A line & futer	
選擇此群組的預設服務。営即	White Sectors NO Group Name Description IM Profile Web Profile	
時通訊使田規則排程已過,多	et Bret	
約2000000000000000000000000000000000000	2 Other Default group sums for year spiritulies	
該群組的即時通訊使用者上。	Bi-or Bro ver Microna Mic-ul/ser	
步驟 5 上傳設定檔		
選擇 Upload Configuration 或點	點擊圖示 💽 將設定檔上傳到裝置上。	

⚠ 注意:

除了手動建立即時通訊群組外 · 您也可以透過 AD Import 或者 File Import 的方式 · 從既有的資料庫中匯入群組資料 · 請參閱以下章節 ·

第15章

內容管理-即時通訊管理

15.1 需求

- 1. 為了設定的方便,需要調整新增即時通訊使用者的預設值。
- 在上班時間,員工只可以使用 MSN,且需要被側錄存證,其餘即時通訊軟體一率禁止。當員工使用某些即時通訊軟 體被阻檔時,需要知道其違反了哪項政策規則。
- 3. 因工作性質關係,研發部 RD 在上班時間不准與公司外的人員聊天。
- 所有傳送的即時通訊訊息與檔案都需要作內容過濾·避免員工利用即時通訊的便利在上班時間聊工作之外的事情與傳送不必要的檔案·浪費公司網路頻寬。
- 5. 所有傳送接收的檔案都需要掃毒,以保護公司內部的電腦。
- 6. 因為管理部門的 CEO 與 CTO 有特殊的需求,所以不列入即時通訊管理控管的範圍。

15.2 方法

- 1. 在 Functions > Content Manager > IM > Options 頁面上設定新增加的即時通訊使用者預設值。
- 2. 在 Functions > Content Manager > Content Policy 頁面設定即時通訊使用者的政策。
- 3. 在 Functions > Content Manager > IM > Global Policy > IM Peers 頁面設定 RD 群組不可以與 Non_IM_User 聊天。
- 4. 在 Functions > Content Manager > IM > Global Policy > IM Contents 頁面設定要過濾的訊息與檔案 · 並啟用設定。
- 5. 在 Functions > Content Manager > IM > Global Policy > IM Security 頁面啟用防毒與防蠕蟲功能。
- 在 Functions > Content Manager > IM > status > Exempt Sources/Destination 頁面設定 · Boss (CEO/CTO) 的連線都避開即時通訊管理的控管。

15.3 步驟

15.3.1 新增的即時通訊使用者預設值

步驟 1 調整即時通訊使用者預設值	Functions > Content Manager > IM > Options	
為了配合即時通訊使用者的政策 · 所以調整 New	📸 Status 🐘 M P offec 🚮 Global Policy 🎒 Opdans	
IM User 的設定值為: Schedule: WorkTime Group: Others	New User Schling.	_
Msg Record: enable	FieRec: OEtabe	
File Record: enable	HRN Account - Invo	
MSN:Allow	=OLAxozurit.	
YAHOO: Block	100 sectors: Allow v 19 Sectors: Flathrum v	
ICQ: Block		
設備L: Block	URL Rec @ Enable C Clobe West 2007 Tow	
Service: Platinum	Web Berts : Flatinum	
當您設定好此預設值後·往後增加的即時通訊使用		
者都會套用此設定。		

15.3.2 即時通訊聊天對象管理

步驟1 啟用即時通訊管理	Functions > Content Manager > IM > Status
勾選 Enable IM。	Ne Status Ne offec M Global Policy 動 Options
	Time to B' Nanoger
	-Description
	It Manager allows you to manage to bahadarskamtantskaars. Natching priority:
	1 Excluding operated Wiscopurk
	2.AC rame
	8 VC than
	Users our little schedule will appeille her Michaels chosen 19 Service
	Brampt (Bo, roc / Deschallori)
	Erable Everript Bources
	🔿 Eixil.de 🖉 GroupEmployee 💌 from the IN Manager enforcement.
	🔿 Induse 🔄 Serveri-TTP 🔤 in the IM Manaper antarcement
	-R tog prov
	Filentecore Mic-or HTTF/800K84/800K86 providences.

步骤 1 新增即時通訊聊天物件規則	Functions > Content Manager >	IM > Global Policy >	IM Peer
	NO. User 1	User 2	Permission
府洞面移到 IN Peel 的宝希上按石蜒,	1 😽 ANY	😌 ANY	🔹 allow
Peer •			
	Add Peer		
步驟2 選擇 User1	Functions > Content Manager >	IM > Global Policy >	IM Peer
在 User 1 欄位上選擇 RD。	NO. User 1	User 2	Permission
	1 😽 ANY	- Second	🐞 allow
	2 ANY ALL_IM_USER	Se ANY	🐞 allow
	RD .		
	Sources		
	issaa 🗨	r	
步驟 3 選擇 User2	Functions > Content Manager >	IM > Global Policy >	IM Peer
在 User2 欄位上選擇 NON IM USER。	NO. User 1	User 2	Permission
	1 ^{See} RD	💛 ANY 🗖	🔹 allow
	2 😽 ANY	ANY	🔹 allow
		► 10	
		Servare Servare	
		🧧 issaa 📃	·
步骤 4 攔阻 RD 與 NON IM User間的對	Functions > Content Manager >	IM > Global Policy >	IM Peer
新	NO. User 1	User 2	Permission
	1 😂 RD	😻 NON_IM_USER	🔹 allow 👻
在 Perm設備SION 欄位上选择 deny。	2 😔 ANY	Se ANY	allow
步骤 5 檢視新增的即時通訊聊天物件規則	Functions > Content Manager >	IM > Global Policy >	IM Peer
檢視已新增的聊天物件規則。	NO. User 1	User 2	Permission
	1 😻 RD	Son Im_User	oj deny
	2 ANY	🤟 ANY	💰 allow
步骤6上傳設定檔			
選擇 Upload Configuration 或點擊圖示 📧 將	設定檔上傳到裝置上。		



15.3.3 即時通訊內容過濾

15.3.3.1 關鍵字過濾

步驟1 啟用關鍵字過濾	Functions > Content Manager > IM > Global Policy >IM Contents >	
勾選 Enable keyword filtering。	Chat	
	Enable keyword filtering	
	Keywords	
	🖽- 🥅 🦉 Dirty Words	
	🖽- 🥅 📴 Name	
	🖽- 🥅 📴 Confidential	
	🖽- 🥅 📴 Sexy	
	🖅- 🥅 📴 Love	
	⊡- 🥅 📴 Stock	

ような」は前間の空	Functiones, Content Menoren, INA, Clobal Dalines, INA Contents	
步聯 ∠ 新瑁關鍵子	Functions > Content Manager > IM > Global Policy >IM Contents >	
將滑鼠移到 IM Contents > Chat 的螢幕上按右	Chat	
鍵·點選 Add Group。	Enable keyword filtering	
	C C Keywords	
	E- Dirty Add Group	
	⊡- 🔄 📴 Name Edit Group	
	🖽- 🥅 🎯 Confi 🛛 Delete Group	
	E- Sexy Add Keyword	
	Edit Keyword	
	⊡- □ III Stock	
	Delete Reymond	
步驟 3 輸入關鍵字群組名稱	Functions > Content Manager > IM > Global Policy >IM Contents >	
輸入關鍵字群組名稱,然後點擊 確定 繼續。	Chat	
	Please input the group name	
	Stock	
	OK Cancel	
步驟4 新增關鍵字	Functions > Content Manager > IM > Global Policy > IM Contents >	
在剛剛新增的群组上按右鍵,然後點選 Add	Chat	
	Enable keyword filtering	
	🔲 🧊 Keywords	
	🗄 - 🔲 🇊 Dirty Words	
	🕀 🔄 🍞 Name	
	⊞ /∰ Confidential	
	Add Group	
	Delete Group	
	Odd Kossiord	
	Edit Keyword	
	Delete Keyword	

Functions > Content Manager > IM > Global Policy > IM Contents >
Chat
Stock
OK Cancel
設定檔上傳到裝置上。
マ 又要忙了 Conversation □□ × File Edit Actions Tools Help
Invite Send Files Video Voice Activities Games
To: 又要忙了 <tsai282863@hotmail.com></tsai282863@hotmail.com>
Second Angel says:
又要忙了 savs:
Policy violation! Some word(s) of the sentence you are trying to send/receive is not allowed.
Search
Last message received at 5:04 PM on 6/5/2006.

15.3.3.2 檔案類型過濾

步驟1 啟用檔案類型過濾	Functions > Content Manager > IM > Global Policy >IM Contents >
勾選 Enable file-type filtering。	File
	TEnable file-type filtering
	🔲 🧊 File Types
	🖻 🔲 🗊 Audio
	🖻 🔲 🧊 Compression
	🖭 🔲 🧊 Image
	🖽 🔲 🧊 Office
	🕀 🗔 🧊 Source
	🕀 🗔 🧊 Risk
	🖽 🔲 🧊 Video
	🖻 🛄 📑 XML

步驟 2 新增檔案類型	Functions > Content Manager > IM > Global Policy > IM Contents >
「 將滑鼠移到 IM Contents > File 的螢幕上按右	File
鍵·點選 Add Type。	✓ Enable file-type filtering
	Image: File Type Image: Fold Type <td< th=""></td<>
步驟3 輸入檔案類型	Functions > Content Manager > IM > Global Policy > IM Contents >
輸入檔案類型·然後點擊 確定 繼續。	
	File Type Delete Type File Type File Type File Type File Type File Type Delete Type File Type File Type Delete Type File Type Delete Type File Type File Type Delete Type File Type File Type Delete Type File Type File Type File Type File Type Delete Type File
步驟 4 新增檔案名稱	Functions > Content Manager > IM > Global Policy > IM Contents >
在剛剛新增的檔案類型上按右鍵·然後點選 Add	File
File Name •	✓ File Types ✓ File Types ✓ Compression ✓ Compression ✓ Office ✓ Office ✓ Source ✓ Yideo ✓ Yuteo ✓ Yuteo ✓ Yuteo ✓ Yuteo ✓ Yuteo ✓ Yuteo ✓ Yuteo



15.3.4 即時通訊安全防護

15.3.4.1 防毒 (Anti-Virus)

步骤1 啟用 ClamAV 防毒 勾選 Enable ClamAV Anti-Virus·然後選擇您希 望 設備 掃描的最大檔案大小。例如 500K·當傳 送的檔案大小是 500K 以下才掃毒,超過 500K 的檔案一律放行。	Functions > Content Manager > IM > Global Policy > IM Security > Anti-Virus PEnable ClamAV Anti-Virus Max file size to scan 500K
步驟 2 上傳設定檔	
選擇 Upload Configuration 或點擊圖示 🔊 將	設定檔上傳到裝置上。
步驟3 傳送/接收的檔案含有病毒的警告訊息 當使用者傳送/接收的檔案含有病毒時・在您或聊天物件接收檔案後・系統將會在即時通訊視窗內傳送警告訊息告知設備內部的使用者。	Year and the state of th

15.3.4.2 防蠕蟲 (Anti-Worm)

步驟 1 啟用第七層防蠕蟲 勾選 Enable L7 Anti-Worm。	Functions > Content Manager > IM > Global Policy > IM Security > Anti-Worm
步驟 2 上傳設定檔	
選擇 Upload Configuration 或點擊圖示 🝥 將	設定檔上傳到裝置上。
步驟3 傳送/接收的URL/檔案含有病毒的警告訊息 當使用者傳送/接收的URL/檔案含有電腦蠕蟲時·系統將會在即時通訊視窗內傳送警告訊息告知設備內部的使用者。	#那邪氣 - Conversation - IX File Edit Actions Tools Help File Edit Actions Tools Help File Edit Actions Tools Welp File Edit Actions Tools Help Invite Send Files Video Voice Activities Games Send Files Video Voice Activities Games To: #\$\$\$ File Edit Actions the states is set to Oot To Leach. Test says: bedroom-thongs.pif #TF和氣 says: Security Warning! A computer Worm is detected. You are not allowed to send/receive this URL/file. A @ + ① Voice Clip ② Winks + 🖸 + 🚳 + 100 Search Last message received at 3:23 PM on 6/6/2006.

15.3.5 除外來源端設定

步驟1 啟用除外來源端	Functions > Content Manager > IM > Exempt Source
勾選 Enable Exempt Sources · 然後選擇 Exclude Boss from the IM enforcement 。在上 面的章節我們已提過 Boss (包含 CEO 與 CTO)有完整的許可權存取網際網路 · 所以將其列 入除外來源 · 避開即時通訊管理的控管。	 Enable Exempt Sources Exclude Boss from the IM Manager enforcement Include ServerHTTP in the IM Manager enforcement
步骤 2 上傳設定檔 選擇 Upload Configuration 或點擊圖示 🗾 將設定檔上傳到裝置上。	

欄位	說明	範圍 / 格式	範例
Enable Exempt Sources	啟用除外來源功能。	啟用 / 不啟用	啟用
Exclude from IM enforcement	所列舉的 IP 位址除外·其餘的電腦皆強制執行即時通訊管理政策。	所有 Object 位址/ 群組清單	Boss
Include in IM enforcement	即時通訊管理政策只適用於所列舉的電 腦。	所有 Object 位址/ 群組清單	

表格 15-1 除外來源端欄位解釋

第16章 LDAP/AD 匯入範例

LDAP 代表 Lightweight Directory Access Protocol (輕量目錄存取協定)。在 LDAP 的協定之中,很像硬碟目錄結構 或倒過來的樹狀結構。LDAP 的根就是全世界,第一級是屬於國別(countries)性質的層級,之後可能會有公司 (organization)的層級,接著是部門(organizationalUnit),再來為個人。而就像個人檔案,每個人都會有所謂的顯 名(d設備 tingu 設備 hed name,簡稱 dn), dn 可能類似 cn=John Smith,ou=Accounts,dc=myCompany,dc=tw。

針對 LDAP Import 這個功能,因其本身的複雜性,所以有許多使用者可能不甚瞭解如何設定。在此,我們提供詳盡的設 定範例,希望提供使用者設定時的參考。

在使用 LDAP Import 這個功能之前,要先確認您現在用來操作使用者介面的電腦是否可以透過 LDAP 這個 Protocol,連線到貴公司的 LDAP 伺服器(例如: ActiveDirectory、OpenLDAP 等)。建議您先用一套 LDAP Browser 的軟體來測 試是否可以連線到 LDAP 伺服器上,您可以在 <u>http://www-unix.mcs.anl.gov/~gawor/ldap/</u> 這裡找到這套軟體以及更 多 LDAP 相關資訊。以下的範例為我們在上列網站上下載 Browser282b2.zip,解壓縮後執行。

16.1 設定 LDAP Browser 軟體



步 驟 2 啟用 LDAP Browser 軟體	🤹 Connect 🛛 🔀
啟動 LDAP Browser 的軟體後 · 您可以看到如右	Session List Quick Connect
圖的畫面·點擊 New 建立新的連線(Session)。	Session List: Edit Copy Delete
	Rename Connect Cancel
步驟3輸入連線的名稱	🌲 New Session
▲ \ 此連須的夕孫。	Name Connection Options
₩J/\LL2E前水口\石件H。	Session Name: LDAPServer Save Cancel
步驟4a設定 LDAP 伺服器連線參數 –	👙 Edit Session 🔀
OpenLDAP	Name Connection Options
輸入 LDAP 伺服器的 IP 位址或網址、連接埠與	Host Info
您在伺服器上所設定的 Base DN。如果不確定	Host: 141.211.14.62 Port: 389 Version: 2 -
Base DN 為何,可以嘗試用 Fetch DNs 來自動	Base DN: ou=people,dc=umich,dc=edu
取得Base DN。請注意,當您使用 Fetch DNs	Fetch DNs/ 此值与 LDAP Browser 最上
時 · 所擷取到的 Base DN 為最上層的 Base	User Info / 层的值相对应
DN。為了確保 LDAP Import 時資料的正確性,	User DN: cn=Directory Manager append base DN
請務必確認使用者資料所存放的 Base DN 為	Password:
何。一般而言 · OpenLDAP 使用者資料會儲存在	Save Cancel
ou=People 的路徑目錄下。	

InstantScan User Manual

	🕹 LDAP Browser/Editor v2.8.2 - Odan://Idan itd nmich edu/on=people.dc=nmich.dc=edul. 🔲 🗖 🗙
	File Edit View LDIF Help
	Image: Second
	Crient A J Brown 1 Crient A J McNamara 2 Crient A N Dingle 1 Crient A R Krachenberg 1
	Constant Sector 1
	Constant Contraction Constant Contraction
	Ready.
步驟 4b 設定 LDAP 伺服器連線參數 –	👙 Edit Session 🔀
ActiveDirectory	Name Connection Options
輸入 LDAP 伺服器的 IP 位址或網址、連接埠與	Host Info
您在伺服器上所設定的 Base DN。如果不確定	Host: 10.17.17.3 Port: 389 Version: 3 🗸
Base DN 為何,可以嘗試用 Fetch DNs 來自動	Base DN: CN=Users,DC=AD,DC=yourCompany,DC=com
取得Base DN。請注意‧當您使用 Fetch DNs	Fetch DNs / 此值与StDAP Browser A最加加 bind
時,所擷取到的 Base DN 為最上層的 Base	User Info 层的值相对应
DN。為了確保 LDAP Import 時資料的正確性,	User DN: administrator append base DN
請務必確認使用者資料所存放的 Base DN 為	Password: *******
何。一般而言·ActiveDirectory 使用者資料會儲	Save Cancel
存在cn=Users (ActiveDirectory)的路徑目錄	
h •	LDAP Browser\Editor y 2.8.2 - [Idap://10.17.17.3/CN=Users,DC=AD,DC=L7-Networks
	CN=Users,DC=AD,DC=yourCompany,DC=com
	CN=Cert Publishers
	← CTCN=DnsAdmins = CN=DnsUpdateProxy =
	←
	←
	← C CN=Domain Users
	CN=Enterprise Admins
	CN=Exchange Services
	CheGroup Policy Creator Owners
	Ready. 31 entries returned.

步驟 5 a 取消匿名綁定設定 - OpenLDAP	👙 Edit Session 🔀
取消勾選匿名綁定(anonymous bind) · 然後在	Name Connection Options
User DN 那邊輸入管理者的帳號與密碼。	Host Info
注意:在Open LDAP中您所輸入的 User DN必須	Host: 141.211.14.62 Port: 389 Version: 2 V
為 cn=[yourAccount] · 例 如 cn=Directory	Base DN: ou=people,dc=umich,dc=edu
Manager •	Fetch DNs SSL Anonymous bind
	User Info
	User DN: cn=Directory Manager append base DN
	Password
	Save Cancel
步驟 5b 取消匿名綁定設定 -	🌲 Edit Session 🔀
ActiveDirectory	Name Connection Options
取消勾選匿名綁定 (anonymous bind) · 然後在	Host Info
User DN 那邊輸入管理者的帳號與密碼。	Host: 10.17.17.3 Port: 389 Version: 3 ▼
	Base DN: CN=Users,DC=AD,DC=yourCompany,DC=com
	Fetch DNs SSL Anonymous bind
	- User Info
	Password:
	Save Cancel
步驟 6 進階設定	👙 Edit Session 🛛 🔀
在 Options 這邊有些其它相關的設定,可以視你	Name Connection Options
的需求去調整。一般而言不需要更動。	LDAP Settings
	Referrals: Manage V Handle
	Deref. Aliases: V Never Always Searching Finding
	Vitor Soldings
	Sort Tree: No sorting Ascending Descending
	Save Cancel



16.2 設定 LDAP Import - 基本設定

步驟 1 設定 LDAP Import 參數	A: OpenLDAP
設定伺服器的 IP、連接埠·以及管理者的帳號密	
碼。並且設定伺服器上的 Base DN。	

步驟 2 選擇 LDAP 伺服器類型	AD Import
<i>文</i>卿 ∠ 選择 LDAP 问版 研知 選擇您的LDAP Server類型,選擇正確的Server類 型,會幫您做好預設篩選使用者與群組資訊的方 式。如果您需要自行調整LDAP內容參數,請參考 進階設定中的說明。	Please setup your AD server Server Setting "Server IP: "Server IP: 192.168.17.254 "Port: 388 "User DN: stor.cn=users.dc=I7,dc=com Password: "Base DN: dc=I7,dc=com Server Type ActiveDirectory 2000 ActiveDirectory 2003
	Delete all objects OK Cancel B: ActiveDirectory
	Please setup your AD server Server Setting 'Server IP: 192.156.17.254 'User DN: ator,cn=users,dt=17,dc=com 'Base DN: dt=17,dc=com 'Server Type
	Delete all objects OK Cancel

16.3 設定 LDAP Import - 進階設定





16.4 LDAP 匯入疑難排解

問題一:為何我無法連到我的 LDAP 伺服器?

答:首先要先確認伺服器的 IP 與連接埠是否正確。如果沒有錯誤的話,可以用 telnet <ip> <port>的方式,看看是否能正常連接。在操作 UI 的電腦與 LDAP 伺服器之間是否有防火牆阻擋?LDAP 伺服器設定是否有開放許可權,讓外部的電腦存取(access)資料?(關於 LDAP 伺服器要怎麼設定存取許可權,請洽詢你的 LDAP 伺服器軟體供應商。

問題二:為何匯入成功,卻沒有新增任何使用者資料?

答:這可能是因為你所指定要匯入資訊的位置錯誤,或者篩檢程式的條件設定有誤,以致於沒有任何資訊符合條件。

問題三:為何我所匯入的使用者數量比我存在 LDAP 伺服器上的還要少?

答:因為多數 LDAP 伺服器會設定一次查詢(query)中·能回應結果(result)的數量上限·如果希望能正常匯入所有使 用者的資料·必須要修改你所使用的 LDAP 伺服器的參數。請參照 http://www.ldapbrowser.com/forum/viewtopic.php?t=14 的討論·或者請洽詢你的 LDAP 伺服器軟體供應商。



報表中心

第17章

報表中心簡介

本章介紹 設備報表中心。

17.1 設備報表中心

設備 提供客戶隨選即用人性化的使用者介面,除了易於設定的管理系統外,更提供使用者簡潔易懂的報表中心。讓使用 者可以依據需求定義報表搜尋方式、查詢各式各樣的排行榜資料、更可依功能面、政策面與個人面作特殊的搜尋與排行。 除此之外,更有事件記錄的資料可供使用者查詢。

17.2 報表設計原則

17.2.1 報表類別

目前 設備 依功能列分成五種報表:

- 1. 應用層策略報表:可檢視與查詢所有應用層策略通訊協定的排行榜與事件記錄。
- 2. 即時通訊管理報表:可檢視與查詢所有即時通訊行為的排行榜與事件記錄。
- 3. 網頁管理員報表:可檢視與查詢所有網頁流量的圖形報表與事件記錄。
- 4. 流量管理員報表:可檢視與查詢每日、每週、每月、每季與每年的流量排行榜與事件記錄。
- 5. 系統管理員報表:可檢視與查詢所有系統的操作資訊。詳見錯誤!找不到參照來源。系統紀錄的說明。

所有報表,除了系統管理員報表外,皆依其性質分成四個類別:

- 1. 功能面 (Funcational View): 依功能作用排行。
- 2. 政策面(Policy View): 依使用者所制定的政策排行,也可以說是管理面的報表。
- 3. 個人面(Personal View):依個別使用的狀況排行,也可以說是個人化的報表。
- 4. 事件面(Event View):所有行為動作的事件記錄。

17.2.2 搜尋工具

為了加速使用者在尋找特定事件記錄或報表的速度,設備 搜尋工具列可以讓您依日期或特定的關鍵字搜尋你要的資訊。



步聚1 搜尋期間設定 報表中心上所顯示的日期期間為您在安裝管 理伺服器時所選擇的資料分割期間。可分成 1)每週2)每月3)每季·三種期間。如右圖 所示·分割期間為每個月。所以日期顯示會以 每個月的第一天為主·例如2006-06-01。同 理類推。 注意·為了確保資料搜尋的速度與保留資料的 完整性·在資料分割後,當您選擇每週/每月/ 每季後,您無法跨周/月/季搜尋。	Date : 2006-06-01 V OK S I I I I I I I I I I I I I I I I I I
步縣 2 重新整理報表與事件記錄時間設定 點擊圖示 診 設定重新整理報表與事件記錄的時 間。	Date : 2006-06-01 V OK OR Refresh Time .
步骤 3 選擇重新整理時間 選擇 10 seconds · 然後點擊 OK 完成設定。一旦 您套用這個設定 · 往後每 10 秒鐘系統會根據您所 選擇的時間重新整理報表與事件紀錄的資料。	Refresh Time Refresh Time Customize the time to refresh all reports and events. 10 seconds OK
步驟 4 進階搜尋 點擊圖示 (建階)。	Date : 2006-06-01 V OK Advanced

步驟 5 選擇搜尋日期	Choose the interested columns to be filtered
勾選 Date。在此您可以縮小搜尋的範圍。也就是	V Date
說當你資料分割是以每月為主,你可以在當月內選	✓ TopN
挥	User
计	From
闪进倖授等的起始时间兴起来时间。	2006-06-01
	То
	2006.06.10
	ОК
步骤 6 輸入要流覽的排名數	Filter Dialog
勿選 TopNI 預設上,多效顯示的低右車件的排名	Choose the interested columns to be filtered.
	V Date Set the Top N
列衣,如未您只需安刖 N 石排石列衣, 您可以任	Loare Set the Top N User
Ŋ衣,知未恋只需要用 N 石排石列衣,您可以在 空格內輸入您想要流覽的數目。	∠ Date Set the Top N ∠ TopN Top
网表·知未您只需要用 N 石排石列表,您可以住 空格內輸入您想要流覽的數目。	Set the Top N Top Top Top Top Top Top Top To
>>>□ >>□ >>□ →□ ス・ ¹ →□ ス・ ¹ □ →□ ス・ ¹ →□ →	Set the Top N User Top 10
ула, чи未恋只需要加 N 石排石列衣, 芯可以在 空格內輸入您想要流覽的數目。	Set the Top N Set the Top N Top 10
▶刘衣·知未恋只需要用 N 石排石列衣, 您可以住 空格內輸入您想要流覽的數目。	Set the Top N User
ула, чи未恋只需要加 N 石拼石列衣, 芯可以在 空格內輸入您想要流覽的數目。	Set the Top N User
Ŋ衣,知未芯只需要用 N 石排石列衣,芯可以在 空格內輸入您想要流覽的數目。	Set the Top N User
內茲·知未忘只需要用 N 石拼石列衣, 您可以住 空格內輸入您想要流覽的數目。	Set the Top N USer
УЛА·ЯЛКОСЛЕНИЯ 空格內輸入您想要流覽的數目。	Set the Top N User
УЛ花·ЯТ茶芯只需要用 N 石拼石列衣, 芯可以在 空格內輸入您想要流覽的數目。	Set the Top N USer I User Set the Top N
УЛ花·ЯЛ禾芯只需要用 N 石拼石列衣, 芯可以在 空格內輸入您想要流覽的數目。	Set the Top N USer
ула, яи未恋只需要加 N 石拼石列衣, 恋可以在 空格內輸入您想要流覽的數目。	Set the Top N Set the Top N Set the Top N Top Top Top Top Top Top Top To
УЛА·ЯЛКОСЛЕНИЯ 2014 2014 2014 2014 2014 2014 2014 2014	Set the Top N Set the Top N Set the Top N
ула, ялалах, такала ула, такала, такал	Set the Top N Set the Top N Set the Top N Top Top Top Top Top Top Top To

步縣7 細部搜尋 如果您希望做更細部的搜尋·您可以特定的細 部搜尋項目。例如:user、receiver、sender、 application、action 等等,視您所選擇的報 表專案而定。	Filter Dialog. Image: Choose the interested columns to be filtered. Image: Date Image: Set the User Image: Date Image: S	
	ОК	

第18章

應用層策略報表

本章介紹應用層策略報表的應用。

18.1 需求

- 1. 有鑒於網路頻寬的濫用頻繁,管理人員希望獲得哪些通訊協定被企圖非法使用的統計資料。
- 2. 管理人員希望知道前 10 名使用 skype 被 設備 攔阻的排行榜。
- 3. 管理人員希望知道使用者 (IP: 192.168.17.58) 前 10 名被攔阻的通訊協定排名。
- 4. 管理人員希望將事件記錄儲存成 Excel 檔,可以依據自己的需求產生其它的報表格式。

18.2 方法

- 1. 到 Reports > L7 > Funcational View > Top Blocked Protocol 檢視圖形報表。
- 2. 到 Reports > L7 > Policy View > Top Blocked Users of Application · 並于 Advanced 上勾選 Application 選擇 skpye。
- 3. 到 Reports > L7 > Personal View > Top Blocked Applications of User · 並點擊 Advanced 設定搜尋 source IP 192.168.17.58。
- 4. 到 Reports > L7 > Event View · 點擊 Export · 選擇資料匯出類型為 Excel 。

18.3 步驟

18.3.1 功能面報表流覽



報表專案	說明
Top Blocked Protocols	經常被攔阻的通訊協定排行。也就是企圖非法闖關的通訊協定排行。
Top Blocked Users	經常被攔阻的使用者排行。也就是企圖非法使用某些通訊協定的使用者排行。



18.3.2 政策面報表流覽



報表專案	說明
Top Blocked Users of Application	經常因違法使用通訊協定的使用者排行。

表格 18-2 政策面報表說明

步驟 2 進階搜尋報表	Reports > L7 > Policy View > Top Blocked Users of Application >
勾選 Application · 然後在 Application 列表上勾選 Skype。點擊 OK 流覽結果。	Advanced

Choose the interested columns to be filtered.
Application Set the Application Set the Application Application Application Set the Application Application Set the Application Application Set the Application

報表專案	說明	範例
Date	可設定要搜尋的資料之期間。注意,這個期間的有效範圍為當您在管理伺服器所 設定的資料分割週期,超過資料分割週期的期間設定是無效的。也就是當您所設 定的資料分割週期為每個月分割一個表格,您所選擇的搜尋期間就不可以超過該 月的範圍。預設上,這個日期期間會依當周的日期為主,如果您在報表畫面上看 不到過去的圖表,請在此選擇適當的日期。	2006/06/01 ~ 2006/06/30
ТорN	您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆,請填入 10。	10
Application	您希望流覽哪些使用者經常違法使用某些通訊協定的排行。可複選。	skype

表格 18-3 應用層策略 - 政策面報表進階搜尋說明

步驟 3 流覽設定的結果	Reports > L7 > Policy View > Top Blocked Users of Application
右圖為因為企圖非法使用 Skype 的使用者排名。	



18.3.3 個人面報表流覽



報表專案	說明	
Top Blocked Protocols of User	特定的使用者所違法使用的通訊協定排行。	

表格 18-4 應用層策略 - 個人面報表說明

步驟 2 進階搜尋報表	Reports > L7 > Personal View > Top Blocked Protocols of User >
勾選 Src IP · 然後在 Src IP 欄位上輸入	Advanced
192.168.17.58。點擊 OK 流覽結果。	Filter Dialog
	Choose the interested columns to be filtered.
	✓ Date Set the Src IP
	Src IP
	Src IP
	192.168.17.58
	ОК

報表專案	說明	範例
Date	可設定要搜尋的資料之期間。注意,這個期間的有效範圍為您在管理伺服器所設定的資料分割週期,超過資料分割週期的期間設定是無效的。也就是當您所設定的資料分割週期為每個月分割一個表格,您所選擇的搜尋期間就不可以超過該月的範圍。預設上,這個日期期間會依當周的日期為主,如果您在報表畫面上看不到過去的圖表,請在此選擇適當的日期。	2006/06/01 ~ 2006/06/30
ТорN	您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆,請填入 10。	10
Src IP	您希望查詢的使用者,其經常違法使用而被攔阻的通訊協定排行。	192.168.17.58

表格 18-5 應用層策略 - 個人面報表進階搜尋說明

步驟 3 流覽搜尋結果	Reports > L7 > Personal View > Top Blocked Protocols of User
右圖使用者 192.168.17.58 企圖非法使用的通訊	
協定排行表。	



18.3.4 匯出事件報表

步驟1 匯出事件報表	Reports >	L7 > E	event View				
點擊圖示 🕕 進階設定。	Functional View Date : 2006-06-01	Policy View OK	Personal View Event View				
	Dete	Application	Deservet	Drotocol	Ore ID	Ore Devt	Det ID
	2006-06-12 11:53:11	vahoo	IBLOCK1 vahoo	TCP	192.168.17.58	2994	216.155.193.169
	2006-06-12 11:53:11	vahoo	[BLOCK] Normalization - vahoo	тср	192.168.17.58	2994	216.155.193.169
	2006-06-12 11:52:41	vahoo	IBLOCK1 vahoo	TCP	192 168 17 58	2993	216 155 193 169
	2006 06 12 11:52:21	aol	[BLOCK] pol	TCD	64 42 200 90	5100	102 169 17 59
	2000-00-12 11.32.21	uphoo	[DLOCK] abi		403 460 47 50	2004	246 455 402 460
	2000-00-12 11:32:11	yanuu		TCP	192.100.17.30	2991	210.155.195.109
	2006-06-12 11:51:41	yanuu	[BLUCK] yanuu	TOP	192.108.17.58	2990	210.133.193.101
	2006-06-12 11:51:06	msn	[BLOCK] msn	ТСР	192.168.17.58	2989	65.54.239.20
	2006-06-12 11:39:35	msn	[BLOCK] Normalization - msn	тср	192.168.17.58	2972	65.54.195.185
	2006-06-12 11:39:25	msn	[BLOCK] Normalization - msn	тср	192.168.17.58	2972	65.54.195.185
	2006-06-12 11:39:20	msn	[BLOCK] Normalization - msn	тср	192.168.17.58	2972	65.54.195.185
	2006-06-12 11:39:18	msn	[BLOCK] Normalization - msn	тср	192.168.17.58	2972	65.54.195.185
	2006-06-12 11:37:48	msn	[BLOCK] Normalization - msn	TCP	192.168.17.58	2945	65.54.195.185
	2006-06-12 11:37:39	msn	[BLOCK] Normalization - msn	тср	192.168.17.58	2945	65.54.195.185
	2006-06-12 11:37:34	msn	[BLOCK] Normalization - msn	тср	192.168.17.58	2945	65.54.195.185
	2006-06-12 11:37:31	msn	[BLOCK] Normalization - msn	тср	192.168.17.58	2945	65.54.195.185
	2006-06-12 11:36:04	msn	[BLOCK] Normalization - msn	тср	192.168.17.58	2915	65.54.195.185 👻
	•						
步驟 2 選擇匯出報表的專案 勾選您要匯出的報表專案·然後勾選會出報表的類 型為 Excel·點擊 OK 繼續。	Reports >	L7 > E	event View > Exp	oort			

Select the reports to make form	
Choose export file type HTML PDF EXCEL Load Setting Save Setting OK Cancel	

欄位 / 按鈕	說明	範例
L7	應用層策略可以匯出的事件記錄。	AF Events
Choose export file type	選擇要匯出報表的格式。有三種檔案類型可供選擇: 1) HTML 2) PDF 3) EXCEL (提供原始事件資料,可 供使用者自行制定報表。)	EXCEL
Button		
Load Setting	將之前已儲存的報表設定檔載入。	
Save Setting 儲存報表設定檔。		
OK 套用設定。		
Cancel	ncel 取消設定並關閉窗口。	

表格 18-6 應用層策略 - 報表匯出欄位說明

步驟3 儲存報表

選擇您要儲存報表的資料夾,然後點擊 Save 完成設定。

第19章

即時通訊管理報表

本章介紹即時通訊管理報表的應用。

19.1 需求

- 1. 管理人員希望知道前 10 名合法的即時通訊使用者排行。
- 2. 管理人員希望知道合法傳送檔案的即時通訊使用者排行。
- 3. 管理人員希望知道 RD "Evan" 合法使用的即時通訊行為。
- 4. 管理人員希望將事件記錄儲存成 Excel 檔,可以依據自己的需求產生其它的報表格式。

19.2 方法

- 1. 到 Reports > IM > Funcational View > Top Allowed Users 檢視圖形報表。
- 2. 到 Reports > IM > Policy View > Top Allowed Users of Service, 並於進階搜尋上勾選 Action 選擇 file。
- 3. 到 Reports > IM > Personal View > Top Allowed Services of User, 並於進階搜尋的 User 欄位填入 Evan。
- 4. 到 Reports > IM > Event View · 點擊 Export · 選擇資料匯出類型為 Excel ·

19.3 步驟

19.3.1 功能面報表流覽



欄位	說明
IM Service	依管理者所設定的即時通訊服務規則·定義其服務與使用者之間的關係。即時通訊服務報表可分成: 1) 被許可的服務排行),2) 被攔阻的服務排行),3) 被許可的使用者排行,4) 被攔阻的使用者排行。
IM Peer	依管理者所設定的即時通訊聊天物件規則·定義聊天物件彼此之間的關係。聊天物件報表可分成兩 大類:1)因發起聊天被攔阻之使用者/群組排行);2)因回應聊天被攔阻之使用者/群組排行。
IM Content	依管理者所設定的即時通訊內容過濾(關鍵字過濾、檔案過濾).可檢視非法關鍵字與檔案的使用 情形。可分成:1)被攔阻關鍵字的使用者排行;2)被攔阻的關鍵字排行;3)傳送檔案被攔阻的使用 者排行;4)被攔阻的檔案名稱排行。
IM Security	依管理者所設定的即時通訊安全防護所產生的報表,可檢視病毒/蠕蟲排行、遭受攻擊的目的端排 行,與發送病毒攻擊的來源端排行。

表格 19-1 即時通訊管理 - 報表專案說明



InstantScan User Manual



19.3.2 政策面報表流覽

步骤 1 流覽被允許使用即時通訊的使用者排	Reports > IM > Polic	y View > Top Allow	ed Users of Service	
名	Functional View Policy View Pe	rsonal View Event View		
點擊 Top Allowed Users of Service。然後點擊	Date : 2006-06-01 - OK	3 🔀 💷		
圖示 🧕 進階設定。	Cop Plotwed Users of Bandre Cop Plotwed Users of Bandre Cop Plotwed Users of Keyword Top Blocked Users of Keyword Top Blocked Users of Virus Top Blocked Users of Worm	5 10 16 20 25 90	Ved Users of Service Counts 95 40 46 60 65 60 66 70 75 90	35 00
		= 42865963 = Evan =vindydance88 = 17manuabost = ylvu829 = 17lest@notmail.com = violet_026@notmail.com		
		User	Counts	
		42088960	06	-
		Evan	37	1
		ujoželaoro00	5	
		Trianualtest	3	
		ylwu823	2	
	E	1. Znavezon telek	1410.00	

報表專案	說明
Top Allowed Users of Service	可依搜尋的服務,查詢被允許使用此服務的使用者排行。
Top Blocked Users of Service	可依搜尋的服務,查詢因使用此服務而被攔阻的使用者排行。
Top Blocked Users of Keyword	可依搜尋的關鍵字,查詢因傳送訊息內容含有此關鍵字而被攔阻的使用者排行。
Top Blocked Users of File	可依搜尋的檔名·查詢因傳送此檔名而被攔阻的使用者排行。
----------------------------	--------------------------------
Top Blocked Users of Virus	可依搜尋的病毒·查詢因傳送/接收此病毒而被攔阻的使用者排行。
Top Blocked Users of Worm	可依搜尋的蠕蟲,查詢因傳送/接收此蠕蟲而被攔阻的使用者排行。

表格 19-2 即時通訊管理 - 政策面報表說明



報表專案	說明	範例
Date	可設定要搜尋的資料之期間。注意,這個期間的有效範圍為當您在管理伺服器所 設定的資料分割週期,超過資料分割週期的期間設定是無效的。也就是當您所設 定的資料分割週期為每個月分割一個表格,您所選擇的搜尋期間就不可以超過該 月的範圍。預設上,這個日期期間會依當周的日期為主,如果您在報表畫面上看 不到過去的圖表,請在此選擇適當的日期。	2006/06/01 ~ 2006/06/30
ТорN	您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆,請填入 10。	10
Action	即時通訊服務的搜尋條件。可依搜尋的即時通訊服務·查詢使用此即時通訊服務 而被允許/被攔阻的使用者排行。	File

表格 19-3 即時通訊管理 - 政策面報表進階搜尋說明



19.3.3 個人面報表流覽



報表專案	說明
Behavior Stat 設備 tics	可流覽所搜尋的使用者,其使用即時通訊細部行為的分佈狀況、累積服務分佈與 該使用者的使用的服務比例。
Top Allowed Services of User	依搜尋的使用者·查詢其合法使用的服務排行。
Top Blocked Services of User	依搜尋的使用者·查詢其違法使用的服務排行。

Top Blocked Initiators of User	依搜尋的使用者·查詢其因發起聊天而被攔阻的使用者排行。
Top Blocked Responders of User	依搜尋的使用者·列出因回應聊天要求而被攔阻的使用者排行。
Top Blocked Keywords of User	依搜尋的使用者·查詢其被攔阻的關鍵字排行。
Top Blocked Files of User	依搜尋的使用者·查詢其被攔阻的檔案排行。
Top Viruses from User	依搜尋的使用者·查詢其發送的病毒種類排行。
Top Viruses toward User	依搜尋的使用者·查詢其遭受的病毒種類排行。
Top Worms from User	依搜尋的使用者·查詢其發送的蠕蟲種類排行。
Top Worms toward User	依搜尋的使用者·查詢其遭受的蠕蟲種類排行。

表格 19-4 即時通訊管理 - 個人面報表說明



報表專案	說明	範例
Data	可設定要搜尋的資料之期間。注意 · 這個期間的有效範圍為您在管理伺服器時所	2006/06/01 ~
Dale	設定的資料分割週期·超過資料分割週期的期間設定是無效的。也就是當您所設	2006/06/30

	定的資料分割週期為每個月分割一個表格·您所選擇的搜尋期間就不可以超過該	
	月的範圍。預設上·這個日期期間會依當周的日期為主·如果您在報表畫面上看	
	不到過去的圖表·請在此選擇適當的日期。	
ТорN	您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆,請填入 10。	10
User	查詢使用者(在此指的是 IM User) · 列舉此使用者所使用的合法服務排名。	192.168.17.58

表格 19-5 即時通訊管理 - 個人面報表進階搜尋說明



19.3.4 匯出事件報表

步驟1 匯出事件報表	Reports > IM > Event View
點擊圖示 🕕 進階設定。	

		D DC	E 135			
	Functional View Policy View	Personal View	Event View			
	Date : 2006-06-01 🔻 OK	🛛 🕺 🛃 🛛				
	Date Application	Action	User	Description	Protocol	Sr
	2006-06-14 16:10:00 msn	login	Evan	[ALLOW] CHAT MSN login	тср	207.46.2.1 🔺
	2006-06-14 16:06:41 msn	login	Evan	[ALLOW] CHAT MSN login	тср	207.46.24.
	2006-06-14 16:01:12 icq	login	42866963	[ALLOW] CHAT ICQ login	тср	64.12.25.1
	2006-06-14 16:01:04 aol	login	I7manualtest	[ALLOW] CHAT AOL login	тср	64.12.161.
	2006-06-14 16:00:26 msn	login	Evan	[ALLOW] CHAT MSN login	тср	207.46.24.
	2006-06-14 16:00:23 msn	login	Evan	[ALLOW] CHAT MSN login	тср	207.46.24.
	2006-06-14 14:09:42 ica	login	42866963	FALLOWI CHAT ICQ login	тср	64.12.25.1
	2006-06-13 17:41:50 msn	whiteboard	Evan	ALLOWI CHAT MSN whiteboard	тср	64.4.37.17
	2006-06-13 17:33:34 msn	remoteassist	Evan	IALLOWI CHAT MSN remoteassist	TCP	207.46.27
	2006-06-13 17:33:11 msn	message	Evan	IALLOWI CHAT MSN message	тср	192 168 1
	2006.06.13 17:32:54 men	woice	Evan		тср	207.46.27
	2000-00-13 17:32:34 1151	voice	Evan	IALLONG CHAT MON VOICE	TCD	402.460.4
	2000-00-10 17:01:00 mist	90000	Evdfi		TCP	192,108,1
	2006-06-13 17:31:29 msn	message	Evan	ALLOW CHAT MSN message	TOP	192.168.1
	2006-06-13 15:56:38 msn	login	Evan	[ALLOW] CHAT MSN login	ICP	207.46.4.2
	2006-06-13 14:31:39 msn	login	Evan	[ALLOW] CHAT MSN login	тср	207.46.24.
	2006-06-13 11:11:52 icq	message	42866963	[ALLOW] CHAT ICQ message	тср	64.12.25.1 -
型為 Excel·點擊 OK 繼續。	Select the reports to ma Manager Manager E	vents				
	Choose export file type	EXCEL ave Setting	ОК	Cancel		

欄位 / 按鈕			說明	範例	
IM			即時通訊管理可以匯出的事件記錄。	AF Events	
Choose	export	file	選擇要匯出報表的格式。有三種檔案類型可供選擇:	EXCEL	

type	1) HTML 2) PDF 3) EXCEL (提供原始事件資料,可 供使用者自行制定報表。)	
Button		
Load Setting	將之前已儲存的報表設定檔載入。	
Save Setting	儲存報表設定檔。	
ОК	套用設定。	
Cancel	取消設定並關閉窗口。	

表格 19-6 即時通訊管理 - 報表匯出欄位說明

步驟3 儲存報表

選擇您要儲存報表的資料夾,然後點擊 Save 完成設定。

第20章

網頁管理員報表

本章節介紹網頁管理員報表的應用。

20.1 需求

- 1. 管理人員希望知道前 10 名存取網站排名。
- 2. 管理人員希望知道因違反網頁管理員政策的控管類別(content_object)而被攔阻的網站排名。
- 3. 管理人員希望知道 192.168.17.58 這台電腦到目前為止的前 10 名存取網頁排名。
- 4. 管理人員希望將事件記錄儲存成 Excel 檔,可以依據自己的需求產生其它的報表格式。

20.2 方法

- 1. 到 Reports > Web Manager > Funcational View > Top Access Sites 檢視圖形報表。
- 2. 到 Reports > Web Manager > Policy View > Top Blocked Sites of Reason · 並於進階搜尋上勾選 Function Type 選擇 content_object 。
- 3. 到 Reports > Web Manager > Personal View > Top Access Sites of User · 並於進階搜尋的 Src IP 欄位填入 192.168.17.58。
- 4. 到 Reports > Web Manager > Event View · 點擊 Export · 選擇資料匯出類型為 Excel ·

20.3 步驟

20.3.1 功能面報表流覽

步驟1 點擊存取網站排名項目	Reports > Web Manager > Functional View > Top Access Sites
點擊 Top Access Sites。	



項目	說明	
Session D 設 備 tribution	可查詢每日、每週、每月的流覽/回應網頁的連線次數與流量分佈狀況。每日以 24 小時為單 位·每週與每月皆以日期為單位。	
Client Stat 設備 tic	可查詢網頁流覽網頁/上傳/下載與因流覽網頁而被攔阻的使用者排行。	
Site Stat 設備 tic	ite Stat 設備 tic 可查詢熱門存取網站/上傳網站/下載網站/被攔阻的網站排行。	
Request Stat 設備 tic 可查詢網頁流覽的存取方法/通訊協定/網域等的比例。		
Response Stat 設備 tic 可查詢網頁回應內容型別/流量等的比例。		

表格 20-1 網頁管理員 - 功能面報表專案說明

步驟 2 進階搜尋報表	Reports > Web Manager > Functional View > Top Access Sites
勾選 TopN·然後在 Top 欄位上輸入 10。點擊 OK 流覽結果。	



20.3.2 政策面報表流覽

步驟 1 流覽被攔阻的網站排名	Reports > Web Manager > Policy View > Top Blocked Sites of
點擊 Top Blocked Sites of Reason。然後點擊圖 示 🙆 進階設定。	Reason



報表專案	說明
Top Request Users of Site	可依搜尋的網站,查詢經常流覽此網站的使用者排行。
Top Upload Users of Site	可依搜尋的網站,查詢經常上傳此網站的使用者排行。
Top Download Users of Site	可依搜尋的網站·查詢經常下載此網站的使用者排行。
Top Blocked Users of Site	可依搜尋的網站‧查詢因流覽此網站而被攔阻的使用者排行。
Top Blocked Users of Reason	可依搜尋的控管類別‧查詢因違反此控管類別政策而被攔阻的使用者排行。
Top Blocked Sites of Reason	可依搜尋的控管類別,查詢因違反此控管類別政策的網站排行。

表格 20-2 網頁管理員 - 政策面報表說明

步驟 2 進階搜尋報表	Reports > Web Manager > Policy View > Top Blocked Sites of
勾選 Function Type, 然後在 Function Type 列	Reason > Advanced
表上點選 content_object。點擊 OK 流覽結果。	

報表專案	說明	範例
Date	可設定要搜尋的資料之期間。注意,這個期間的有效範圍為當您在管理伺服器 所設定的資料分割週期,超過資料分割週期的期間設定是無效的。也就是當您 所設定的資料分割週期為每個月分割一個表格,您所選擇的搜尋期間就不可以 超過該月的範圍。預設上,這個日期期間會依當周的日期為主,如果您在報表 畫面上看不到過去的圖表,請在此選擇適當的日期。	2006/06/01 ~ 2006/06/30
ТорN	您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆,請填入 10。	10
Function Type	網頁管理員報表的細部搜尋條件。可依搜尋的控管類別(Function Type)· 查詢所有違反控管類別政策的網站排名。	content_object

表格 20-3 網頁管理員政策 - 面報表進階搜尋說明

步驟3流覽設定的結果	Reports > Web Manager > Policy View > Top Blocked Sites of
右圖為因違反控管類別政策而被攔阻的網站排名。	Reason



20.3.3 個人面報表流覽



報表專案	說明
Session D 設備 tribution of User	可依搜尋的使用者(IP),查詢此使用者每日、每週、每月的流覽/回應網頁的連線次數與流量分佈狀況。每日以 24 小時為單位,每週與每月皆以日期為單位。
Site Stat 設備 tic	可依搜尋的使用者(IP)·查詢此使用者存取網站/上傳/下載與流覽違法的網站排 行。

Request Stat 設備 tic	可依搜尋的使用者(IP)·查詢此使用者經常存取網站/上傳網站/下載網站/被攔 阻的網站排行。
Response Stat 設備 tic	可依搜尋的使用者(IP)·查詢此使用者網頁流覽的存取方法/通訊協定/網域等的 比例。

表格 20-4 網頁管理員 - 個人面報表說明



報表專案	說明	範例
Date	可設定要搜尋的資料之期間。注意,這個期間的有效範圍為您在管理伺服器所設定的資料分割週期,超過資料分割週期的期間設定是無效的。也就是當您所設定的資料分割週期為每個月分割一個表格,您所選擇的搜尋期間就不可以超過該月的範圍。預設上,這個日期期間會依當周的日期為主,如果您在報表畫面上看不到過去的圖表,請在此選擇適當的日期。	2006/06/01 ~ 2006/06/30
ТорN	您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆,請填入 10。	10
Src	查詢使用者(在此指的是使用者的 IP),查詢此使用者的存取網站排行。	192.168.17.58

表格 20-5 網頁管理員 - 個人面報表進階搜尋說明



20.3.4 匯出事件報表

步驟1 匯出事件報表	Reports > Web Manager > Event View		
■ 點擊圖示 🔰 進階設定。	Functional View Personal View Event View		
	Date: 2006-06-01 V OK OK		
	Date Web Site Unction Type Message Src IP		
	2006-06-15 13:10:50 ar.atwola.com url_record ar.atwola.com/content/80/0/H7pTL 192.168.17.58 2Luf0_kw3xmij8W/rsns8a9RRNke 8_SAqLzKBa609jmULHVa8jgFKtiL6 9KXxB92suHm7GFSxCAAzjxHgh-J vcqpm/zKgLAE0M0WyQY\$/sol		
	2006-06-15 13:10:50 ar.atwola.com content_object [BLOCK] Cookie object 192.168.17.58		
	2006-06-15 13:10:50 ar.atwola.com content_object [BLOCK] Cookie object 192.168.17.58		
	2006-06-15 13:10:50 ar.atwola.com content_object [BLOCK] Cookie object 192.168.17.58		
	2006-06-15 13:10:50 ar.atwola.com url_record ar.atwola.com/image/93169980/icq 192.168.17.58		
	2006-06-15 12:02:22 iveupdate.symantecliveupdate.url_record liveupdate.symantecliveupdate.co 192.168.17.58 m/avenge \$201.5\$20microdefs25\$ 20nav2005_microdefsb.curdefs_s symallanguages_livetri.zip		
	2006-06-15 12:02:22 liveupdate.symantecliveupdate.url_record liveupdate.symantecliveupdate.co 192.168.17.58 m/navnt\$202005_11.0.11_chinese		
	2006-06-15 12:02:22 liveupdate.symantecliveupdate.url_record liveupdate.symantecliveupdate.co 192.168.17.58 m/avenge\$201.5\$20microdefs25\$ 20nav2005_microdefsb.nov_symal languages_livetri.zip		

步骤 2 選擇匯出報表的專案	Reports > Web Manager > Event View > Export
勾選您要匯出的報表專案,然後勾選會出報表的類型為 Excel,點擊 OK 繼續。	Select the reports to make form Web Manager Report Web Manager Events Web Filter
	Choose export file type HTML PDF EXCEL Load Setting Save Setting OK Cancel

欄位 / 按鈕	說明	範例	
Web Manager	網頁管理員可以匯出的事件記錄。	Web Manager Events	
		Web Filter	
Choose export file type	選擇要匯出報表的格式。有三種檔案類型可供選擇: 1) HTML 2) PDF 3) EXCEL (提供原始事件資料,可 供使用者自行制定報表。)	EXCEL	
Button			
Load Setting	將之前已儲存的報表設定檔載入。		
Save Setting	儲存報表設定檔。		
ОК	套用設定。		
Cancel	取消設定並關閉窗口。		

表格 20-6 網頁管理員 - 報表匯出欄位說明

步驟3 儲存報表

選擇您要儲存報表的資料夾·然後點擊 Save 完成設定。

第21章

流量管理員報表

本章節介紹流量管理員報表的應用。

21.1 需求

- 1. 管理人員希望知道 2006 年 6 月份的頻寬使用狀況。
- 2. 管理人員希望知道 2006 年 6 月 15 日網路進出總流量最大的前 5 名使用者排行。
- 3. 管理人員希望知道 2006 年 6 月 15 日使用 FTP 與 HTTP 等應用軟體的最大總流量之使用者排行。
- 4. 管理人員希望知道 2006 年 6 月 15 日使用者 (192.168.17.58) 使用的應用軟體之最大總流量排行。

21.2 方法

- 1. 到 Reports > Traffic Manager > Bandwidth View > Monthly Report > Monthly Bandwidth 檢視圖形報表。
- 2. 到 Reports > Traffic Manager > Functional View > Daily Totoal Traffic > Daily Top Total Traffic by User · 並於進 階搜尋上的 TopN 欄位上填入 5。
- 3. 到 Reports > Traffic Manager > Policy View > Daily Top Total Traffic by User of Application · 並於進階搜尋的 Application 欄位選擇 ftp 與 http。
- 4. 到 Reports > Traffic Manager > Personal View > Daily Top Total Traffic by Application of User · 並於進階搜尋上 勾選 Sip · 然後填入 IP 位址 192.168.17.58。

21.3 步驟

21.3.1 頻寬面報表流覽

步驟1 點擊每月頻寬折線圖	Reports > Traffic Manager > Bandwidth View > Monthly Report >
點擊 Monthly Bandwidth。	Monthly Bandwidth



欄位	說明	
Daily Report	查詢每日頻寬狀況·依應用程式/頻寬類別/應用程式類別等分類方式·方便查詢對內頻寬/對外頻寬/ 總頻寬的流量。	
Weekly Report	查詢每週頻寬狀況·依應用程式/頻寬類別/應用程式類別等分類方式·方便查詢對內頻寬/對外頻寬/ 總頻寬的流量。	
Monthly Report	查詢每月頻寬狀況·依應用程式/頻寬類別/應用程式類別等分類方式·方便查詢對內頻寬/對外頻寬/ 總頻寬的流量。	
Yearly Report	查詢每年頻寬狀況·依應用程式/頻寬類別/應用程式類別等分類方式·方便查詢對內頻寬/對外頻寬/ 總頻寬的流量。	

表格 21-1 流量管理員 - 頻寬面報表專案說明

21.3.2 功能面報表流覽

步驟1 點擊每日最大流量之使用者排行	Reports > Traffic Manager > Functional View > Daily Traffic Report
在工具列上的 Day 欄位選擇 2006-06-15 · 點擊	> Daily Totoal Traffic > Daily Top Total Traffic by User
OK 繼續 · 點擊 Daily Top Total Traffic by	
User.然後點擊圖示 🙆 進階設定。	





21.3.3 政策面報表流覽



報表專案	說明
Traffic Daily Report	可查詢每日流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。
Traffic Weekly Report	可查詢每週流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。

Traffic Monthly Report	可查詢每月流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。
Traffic Quarterly Report	可查詢每季流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。
Traffic Yearly Report	可查詢每年流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。



步驟 2 進階搜尋報表 Reports > Traffic Manager > Policy View > Traffic Daily Report > Daily Total Traffic > Daily Top Totoal Traffic by User of Application 勾選 Application · 然後在 Application 列表上勾 選ftp與http。點擊OK流覽結果。 Filter Dialog -Choose the interested columns to be filtered. TopN Application Set the Application Application 🗌 🖉 Application elia 🗊 eci es 🐨 ares directionment 🔄 📑 edonkay 🛄 🖉 expeter CPI II to D 🛄 🐺 grutella 🔄 📑 h323 B hopster OK

報表專案	說明	範例
ТорN	您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆,請填入 10。	10
Application	應用軟體的搜尋條件。可依搜尋的應用軟體,查詢使用此即時應用軟體的使用者 排行。(可複選)	File

表格 21-3 流量管理員 - 政策面報表進階搜尋說明

步驟 3 流覽設定的結果	Reports > Traffic Manager > Policy View > Traffic Daily Report >
右圖為最常使用 ftp 與 http 應用軟體的使用者	Daily Total Traffic > Daily Top Totoal Traffic by User of Application
排行。	



21.3.4 個人面報表流覽



報表專案	說明
Traffic Daily Report	可依選擇的使用者·查詢其每日流量與封包數的對內/對外/總流量/總封包數排行與應用軟體排行。
Traffic Weekly Report	可依選擇的使用者·查詢其每週流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。

Traffic Report	Monthly	可依選擇的使用者·查詢其每月流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。
Traffic Report	Quarterly	可依選擇的使用者·查詢其每季流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。
Traffic Year	ly Report	可依選擇的使用者·查詢其每年流量與封包數的對內/對外/總流量/總封包數的使用者排行與應用軟體排行。

表格 21-4 流量管理員 - 個人面報表說明



報表專案	說明	範例
Date	可設定要搜尋的資料之期間。注意,這個期間的有效範圍為您在管理伺服器時所 設定的資料分割週期,超過資料分割週期的期間設定是無效的。也就是當您所設 定的資料分割週期為每個月分割一個表格,您所選擇的搜尋期間就不可以超過該 月的範圍。預設上,這個日期期間會依當周的日期為主,如果您在報表畫面上看 不到過去的圖表,請在此選擇適當的日期。	2006/06/01 ~ 2006/06/30
ТорN	您在報表畫面上希望看到的排行數。如果您希望只看前 10 筆,請填入 10。	10
Sip	查詢使用者(在此指的是來源端的 IP 位址) · 查詢此使用者所使用的應用軟體 流量排行。	192.168.17.58



表格 21-5 流量管理員 - 個人面報表進階搜尋說明

第7部

資料維護與警報系統

第22章

階層式管理與稽核

本章介紹設備階層式管理與稽核的設計與應用。

22.1 需求

面對層出不窮的資安事件,企業為解決資安問題不能單由技術面著手,應藉由建立完整管理系統以有效解決資安問題。根 據政府資通會報規定:政府部會中A、B級單位需在民國97年以前通過BS7799認證。由此可見,BS7799內容的適用性 與重要性。此外,由於BS7799巨細彌遺的說明企業控管資訊安全所應採取的步驟及應制訂哪些應變措施。由此可見,BS 7799 是一套完整的計畫,能有效建構資訊安全防護機制。IT 專業人員可將這套資訊安全標準規則當作藍圖,依其導引制 定企業的安全政策與程式。設備內容管理器,為符合BS7799的規範,説明企業執行BS7799計畫,特地設計階層式管 理與稽核系統。

22.2 目的

內容管理因牽涉到個人隱私與公司機密·在處理上需要特別小心謹慎。設備 階層式管理與稽核·利用許可權控管資安內容· 將風險降到最低與資安防護效果最大化·將管理與稽核人員分開·各司其職且相互合作。

22.3 方法

設備目前規劃三種許可權群組,分別為:

- 1. Admin:最高管理人員,擁有最高許可權,可制定管理政策與流覽側錄訊息。
- 2. Manager:管理人員,可制定管理政策但無法流覽側錄訊息。
- 3. Audit:稽核人員,可流覽側錄訊息,但無法制定管理政策。

22.4 步驟

在您第一次登入 設備 內容管理器時,您可以在帳號管理員編輯可存取管理伺服器的帳號與密碼。借由設定的許可權階層 式控管 設備,讓貴公司確保員工個人隱私與公司機密,更能符合公司稽核的需求。

22.4.1 新增使用者帳號

步骤 1 管理帳號設定		
選擇 Account Manager(帳號管理員)選項。		
步驟 2 新增使用者帳號	Tools > Account Manager > User > Add User	
設備 可同時多人連接控管·您可在		
Account Manager (帳號管理員) 建立可		
存取管理伺服器的帳號·包含使用者與其		



欄位	說明	範例
Name(名稱)	可存取管理伺服器的使用者帳號名稱。	test
	可存取管理伺服器的使用者群組,可分成三種授權群組:	
	1. admin(最高管理人員):可設定設備、流覽報表與查看側錄記錄等所有權限。	
	2. manager(管理人員):監督人員,可依管理人員給予開放的許可權來設定設備、	
Group(辞組)	流覽報表與查看側錄記錄。	manager
	3. audit(稽核人員):只可查看側錄記錄·但無法設定設備。	
	注意:群組不可增刪修改。	
		test
Description(抽処)	□ ずT 至J Ψ長 5ሺ F J F 和 元 中月 。	account

表格 22-1 帳號管理員

步驟3 編輯帳號	Tools > Account Manager > User > Add User
請輸入您要新增的帳號名稱、對此帳號的	
描述、與其密碼·並選擇所屬群組。	

	Enter a unique name	e and related information for the user.
	-User Information-	
	Name :	Itaat
	(NATION)	lest
	Group :	1770 IN 1770
	cribup.	Manager ⊻
	Description	Manager
	Description :	Audit
	Password -	
	i assivora :	
	Confirm :	[
		Advanced
	4	
		OK Cancel
步驟 4 設置添加 Project(專案)	Project Permission	Config Permissi
在 All groups(全部群組)欄裡依需求選	Please select the pro	ojects allowed to be opened by this user.
擇管理設備·點選>>鍵添加到 Selected	-All groups	- Selected groups
groups(已選擇的群組)欄裡.如右圖添	IS-19	18-500
選設備-500則是允許此帳號可以管理查	IS-500	
看設備設備-500	Markey Sec.	
		>>>
		~
		Finish Cancel

步驟 5 修改許可權	Project Permission Config Permissi Log Permission
用戶可以通過 Advanced 的功能自己來定 義管理許可權。右圖是 manager 的許可 權更改對話方塊,可以根據需要自行修改。 注:manager(管理員)和 Auditor(稽 核員)可以更改許可權,admin(最高管理 員)擁有全部許可權,不可以更改。	 Please select the permissions for configuration by this user. Browse Config Allow this user to browse all configurations. Edit Config Allow this user to edit all configurations.
	Rinish Cancel
	Project Permission Config Permissi Log Permission
- 歩骤 6 帳號建立成功資訊	Project Permission Contig Permissi Lug Permission Please select the groups whose private logs are allowed to be viewed by this user. Browse Recorders Allow this user to browse all recorders. All groups Others Non_IM_Users Finish Cancel
步聯 6 帳號建立成切員訊 當您建立帳號成功 · 將有如右圖的視窗通 知您新增成功。	The user is added successfully.
步骤 7 顯示已增加的帳號	Tools > Account Manager > User
當您成功建立帳號‧您可以在 Account	
Manager (帳號管理員) 的視窗上看到這	

筆資料。	Account Manager Levels	Name admin mis audit test	Group Admin Manager Audit Manager	Description Administrator Manager Auditor manager
步驟 8 刪除帳號 欲刪除某筆帳號 · 只要點選此筆資料 · 然 後按右鍵 · 選擇 Delete User (刪除使用 者) 。	Tools > Account Account Manager Levels	nt Manager Name admin mis audit	> User > D Group Admin Manager Audit Add U Dele	elete User Description Administrator Manager Auditor User te User

22.4.2 修改使用者登入網頁介面的密碼

步骤1 點選更改密碼	Tools > Change Password
選擇 Change Password(更改密碼)選項。	te Tools Help Account Manager Change Password Change Setting SNMP Control Config Backup Config Restore
步驟 2 輸入新的密碼 輸入 Old Password (舊的密碼)與 New	Tools > Change Password

Password (新的密碼) · 然後在 Confirm (確認)欄位內再次輸入新的密碼。點擊 OK	Enleryour old password and new password.	
完成設定。	Password Old Password: Prene New Password: Prene Confirm:	
	ОК Саясеі	

第23章

管理服務器設定

本章介紹管理服務器的設定與其應用

23.1 管理服務器概述

在管理伺服器安裝完成 · 且重開機後 · 有一小圖示 🦃 (mailer) 將會顯示在伺服器的右下角 · 請將滑鼠移到圖示上 · 點兩下 · mailer 的功用如下 :

- 系統資訊:查詢 CPU/Memory 使用狀態、資料庫/HTTP/管理伺服器的存取目錄、管理伺服器的 IP/MAC 等相關資訊。
- 郵件警告:設定郵寄伺服器與自訂電子郵件警告內容。
- ▶ FTP 備份:設定 FTP 伺服器、資料備份時間與備份類型、並選擇備份狀態。
- 報表中心:可選擇報表寄發的時間、格式、報表收件者與選擇報表的來源(裝置)。在設定報表中心前,請在裝置上設定匯出報表的專案,相關設定請參考章節。
- ▶ 系統記錄:設定系統操作記錄的收件者,與希望收到的系統記錄的嚴重等級。

詳細設定說明·參請考以下的說明。

23.2 管理服務器設定

在管理伺服器安裝完成,且重開機後,有一小圖示,上會顯示在伺服器的右下角。請將滑鼠移到圖示上,點兩下。

步驟 1 系統資訊	mailer > System Info
在這個頁面上·您可以看到 CPU 與記憶體的使用情 況,還有一些管理包服器的存故位罢,網路訊自等,	InstantScan-MySQL connected V2.1
況‧還有一些管理伺服器的存放位置、網路訊息等。	System Info E-Mail Alext FTP Setup Report Center System CPU Usage CPU Usage Hetory Memory Usage Mail Alext FTP Setup Provide Hetory Management Server Info Database Server Service on [C:UTNetworks/Apache/A
	Management Server : Service on (C:UZNetworks) Network Hie Description-Readekt RTLB139 Family PCI Fast Ethemat NIC - Packet Scheduler Miniport Addressr00.05A1.35 AE:5E DhrpEinable4-0 ByAdresslut=192.168.17.120 ByMark=255.295.295.0 2006r10/20 1±47:06.44:52 [Management Servet]: Management Servet Started, 2006r10/20 1±47:06.454 [Management Servet]: Management Servet Started, 2006r10/20 1±47:06.4554 [Management Servet]: Report[No device has been chosen, 2006r10/20 1±47:06.4554 [Management Servet]: Report[No device has been chosen, 2006r10/20 1±47:06.4554 [Management Servet]: Report[No device has been chosen,

步驟 2 設定郵件伺服器	Mailer > E-Mail Alert > Edit
點擊 Edit 按鍵。選擇 By Local Server 選項。輸入 DNS 伺服器 IP 位址,並在 Check Time(min)欄	LastaréScan-MySQL cerenected V2.1
位上鍵入系統檢查是否有警告信件的時間。如果您希 望透過 SMTP 伺服器寄送警告信件,請點選 By SMTP Server 選項。您可以點擊 Test,然後在彈跳 出來的視窗內輸入收件者的電子郵寄地址,最後點擊 OK,測試連線狀態。	System Info E-Mail Alert FTP Simup Report Center Systog Asut Mail Server Satup Meri Receiver Deer Agp Action E-Mail DRS Server FIGURE 1.1 Deer Agp Action E-Mail User Name FIGURE 1.1 Select Bother Bother DRS Server FIGURE 1.1 Select Bother Bother Date Name FIGURE 1.1 Select Bother Bother Date Name FIGURE 1.1 Select Bother Bother Chack Tamalyminitie FIGURE Early Early Early Early Test FIGURE Early Early Early Early
步驟 3 客制化郵件訊息 將游標移到文字方塊中要加入變數的位置·點擊變數 (\$Date、\$App、\$Action、\$User)。	2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 上午 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 L+ 09 50-54 (Management Server) Popurt/Bio device has been chrasen. 2000/10/20 L+ 09 50-54 (Management Server) Popurt/Bio device has been chrasen. </th
	Mail Server Server Over Age Action E44al DHS Server D005 05.11 D006 Mail Manager DHS Server D005 05.11 D006 Mail Manager DHS Server D005 05.11 D006 Mail Manager Description DHS Server D005 05.11 D006 Book Description DHS Server D005 05.11 D006 Book Book Description DHS Server D005 05.11 D006 Book Book Book Description DHS Server D005 05.11 DHS Server Book Book <td< th=""></td<>

變數名稱	說明	範例
\$Date (日期)	違反政策事件發生的日期。	2005/01/01 10:10:00
\$App (應用軟體)	IM使用者違反政策時所使用的IM軟體。	MSN
\$Action (使用行為)	不合法的IM使用行為。	file transfer
\$User (使用者帳號)	違反政策的IM使用者帳號。	user@host.your.com

表格 23-1 警告信件內的變數設定

步驟 4 預覽警告郵件內容	Mailer > E-Mail Alert > Customize Mail > Preview
當您設定好警告信件內容‧可點擊 Preview 預覽。關 閉預覽視窗繼續下一步。	Preview × Subject: [L7 Networks] You are not allowed to do MSN's file transfer!! Hi user@host.your.com ,This is a message from the IT department. The MSN file transfer you were trying to access is forbidden at 2005/01/01 10:10:00. Please strictly follow the company's policy. For more help, email IT Support Desk.
步驟 5 FTP 設定	Mailer > FTP Setup > FTP Schedule
在本頁‧您可設定利用FTP備份記錄的方式。勾選 Enable FTP Backup‧然後勾選 Backup only。	Instant/Some My/SQL connected V2.1 Image: Connected
您可以選擇FTP自動備份的時間 1) 每日 2) 每週 3) 每月。點擊 Daily · 然後選擇15:00。換句話說 · 每天下午 3 點 · 系統會開始透過 FTP 備份當天的事 件記錄。	FTP Cpro Production IF Each FTP Backup Production IF Each Production Production
步驟 6 設定備份類型 請在 Backup Type 選擇資料備份類型。當您要還原	Mailer > FTP Backup > Backup Type
您已被份的資料,請點擊 Get Bakup L 設備 t 按鈕,	Evelopition E-Val Al-at ETD Selas Depart Center S-salas Al-at ETD Selas
然後選擇要從 FTP 伺服器上下載的路徑·點擊 Restore 開始資料庫或檔案還原。	Production Production
	2015/10/11 丁 11:20 54 [Management Sensed] [Pep of N. device has been cruster 2015/10/11 丁 11:33 54 [Management Sensed] [Pep of N. device has been cruster 2015/10/11 丁 11:34 54 [Management Sensed] [Pep of N. device has been cruster 2015/10/11 丁 11:34 54 [Management Sensed] [Pep of N. device has been cruster



止雨 10 洼穴/健方多纮記錄	InstantScan-MySQL connected V2.2					
步驟 10 清空/储存系統記錄 在狀態欄內按右鍵。您可選擇清空事件記錄或者將紀 錄儲存到硬碟上。	System Info	E-Mail Alert	FTP Setup	Report Center	Syslog	About
	1 第006/10/20 上午 11:22	27 (Managament	Sérrer) Managan	vent Server Started.		er Log áz.

▲ 如果您不小心關閉 mailer · 您可以在桌面或 C 磁槽根目錄 · L7 Networks 資料夾內找到檔案 mailer.exe · 移動您 的滑鼠 · 在 mailer.exe 圖示上點兩下 · 即可開啟它 · Mailer 預設儲存的路徑為 C:/L7Network ·
第24章

側錄稽核

本章節介紹即時通訊與網頁的側錄。

24.1 需求

為符合 BS7799 的規範, 説明企業執行 BS7799 計畫, 設備 階層式管理與稽核系統能夠保護使用者的隱私, 免於一般人 随便流覽其聊天資訊。然而, 當有洩密情況發生時, 這些測錄資料亦可供稽核人員隨時采證, 防範員工不法的舉動而危及 公司。所以只有管理人員與稽核人員可以看到側錄的內容, 網管人員只可以設定 設備, 無法進入側錄系統。目前側錄共有 兩大類:

- 1) 即時通訊內容側錄:使用者使用的即時通訊軟體 MSN/Yahoo/ICQ/設備L 皆可即時側錄傳送的訊息與檔案,並以紅 字標示違法的關鍵字與傳檔檔案名。
- 2) 網頁網址側錄:使用者流覽的網頁即時側錄。可以查詢使用者流覽網頁的狀況與其合法性。

24.2 方法

- 1. 到 Auditor > IM Recorder 檢視側錄內容。
- 2. 到 Auditor > Web Recorder 檢視側錄內容。

24.3 步驟

24.3.1 即時通訊內容側錄

步驟4 即時通訊內容側錄

只有管理人員與稽核人員可以看到側錄內容。當您打開即時通訊側錄器後·將有類似右圖的訊息顯示。即時通訊側錄器以樹狀結構顯示。 第一層為群組·第二層為在此群組內的使用者·第三者為與此使用者聊天的對象·第四層為側錄到的訊息。如果您已經設定使用者規則· 經由同一使用者規則內的所有帳號所傳送/接收的訊息內容都會顯示在同一個視窗內。當使用者不在即時通訊使用者群組內時·將會以 Non_IM_Users 顯示·所有側錄到的訊息會依使用者的即時通訊帳號逐條顯示。

側錄如右圖所示:

- 1. 關鍵字過濾: 關鍵字以紅字顯示。
- 2. 檔案傳送:可將滑鼠移到檔案名上,點一下檔案,將其儲存在本地端電腦上,並開啟流覽。
- 3. 檔案過濾:違反檔案傳送規則的檔案名稱會以紅字顯示,並禁止使用者傳檔。

欄位	說明	範例
Date	傳送訊息的日期與時間。	2006-06-19 13:20:12

From	傳送訊息的使用者。當您在 IM User 上已有設定此使用者,則在此 欄位會顯示您所設定的使用者名稱,否則將顯示即時通訊帳號。	Evan
Nick (只適用MSN)	傳送訊息的使用者的昵稱。此昵稱為您在 MSN 即時通訊帳號所設 定的顯示名稱。	Test
То	接收訊息的使用者。當您在 IM User 上已有設定此使用者,則在此欄位會顯示您所設定的使用者名稱,否則將顯示即時通訊帳號。	Angel
Nick (只適用MSN)	接收訊息的使用者的昵稱。此昵稱為您在 MSN 即時通訊帳號所設 定的顯示名稱。	一個半小時新竹<->宜蘭
Message	即時通訊訊息內容。	stock

表格 24-1 即時通訊側錄內容欄位說明

24.3.2 網頁內容側錄

步驟1 流覽的網頁側錄	Auditor >	Web Reco	order > R	equest																																				
當您在 Web Manager > Status 頁面上開啟	Side: 2005-06-81 +	* 🧕 📶																																						
5	Net NetepstRepet	Calo Motor	d Hvit Dra	UNI	Deters	21.14	Die Port	DellP	Did Port																															
URI Recorder,所有您要流覽的網頁將會被記錄在	C S Vid-Minigar Events	2080-06-10 14:00.31 get	www.websies.com	time and the second	1963.08	102,168,17.08	18153	210.153,40.34	88 *																															
	To Prospersa	2086-06-15 14:40:27 get	ange Lying com	As ping conditions straphs as 200500171201.com	108.8	182.190.17.58	38.80	8438.908.210																																
這個側錄頁面上。		2085-06-19 14:40:24 put	maje Lyleig com	An piration distance have	122.0	182.180.17.58	1071	61.05.905.219	60																															
		2186-06-1914-90223 (08	anyyohie.com	confighty_off	205.4	182,198,12.58	name i	88.142.187.380	840 -																															
		2088-06-12 18:0023 (eff	www.anden.com	1	256.0	102.108.17.00	1000	88,142,107,188	14																															
		2085-36-18 18 89:29 (eff	Parloging observes	A gi Lin Argin cut	848.0	102.005.17.00	1983	282.43.195.151	94																															
		2006-06-18 14:40:29 prf	Personal and a second	ituri	455.0	182,160,17,58	NERG	282.43.195.52	94																															
		2086-06-19 14:40:20 gut	Withouten	interating lapset to "Mipolary	452.0	182,199,17,58	5995	20104196242	-																															
		2080.06.19.18.0020 get	NUTEVARIAGEN	Professor Standing and Party Strength	897.0	182.169.17.58	1998	20184190302	60																															
		2084-06-10 14:00.17 (64	Perception and	if an los teges and	847.8	182, 188, 17,98	1987	282.63.195.191	20																															
																																	2086-06-19 14:40:17 get	heurdiyaliwa.com	interacting lighter in the strange	60.5	102,108,17,58	CORT.	20184,196,242	86
		2086-06-19 14:40:15 gut	created for yellocal user for e-both	ida europataneta elle flaticita	444.0	182,190,17.58	596	81213167.2%	88																															
		2080.06-1014.0015 get	stight yeloccos	radoplayler.cll	10.0	182,160,12.58	5791	88,162276,280	30																															
																																	2088-08-19 14:00:15 and	matyatos.com/bi	1	635.8	182,168,17,88	1681	282.43.195.13	10
																																2088-06-13 14:40:15 pot	hereiyebea.com	divisional Papiliago (matil/folige finado Livelino a caracteri	816.0	102,165,17.68	1880	283.84.196.242	88	
										2086-06-19 14:42:15 get	fyr,anhosucore	ball	655.0	182,190,17,58	1290	202.43,195.52	84																							
																																2085-06-19 14:10:15 get	Nurdyahoscare	Performs The Report Mater Processie on community	897.9	182,199,17.58	6790	203.84.186.242	80	
		2004/06/19 18:0017 get	hypegoare	Investorment of an	/98.8	182,160,17.58	1/94	28184.196.97	10																															
		2088-06-10 14:40 12 804	Profescore	Abuitude01031ad, secart	258.0	382,165,17,68	1785	28585.196.57	88																															
		2005-06-19 14:40:12 pet	heating.com	Mechanol001031ad_muaif	258.0	182,168,17.58	1792	29384.196.97	60																															
		2086-06-19 18:40:11 gut	hisking.com	Invitorial mugh	258.0	182,160,17,58	5790	200344196.97	86																															
		2089-06-1914/9211 84	hustegone	Multipolit_staft	162.0	182.100.12.68	1089	28184.196.8V	H																															
		THE OWNER AND ADDRESS AND	Barrana casa	The Rockshold State of Taxaban	171.9	107 100 17 18	in the later	Second states and	100																															

欄位	說明	範例
Date	發送流覽網頁要求的時間。	2006-6-19 14:40:24
Method	method 用以規範表單被送出時,所採用的 HTTP method,預設值是 GET。POST 方法是將 資料包裝在 HTTP 標頭內傳送給 Web server; 而 GET 方法則是將資料直接加在 URI 之後。使 用 GET method 所能傳遞的資料有限(連同 URI 共 255 字元),在需要上傳大量資料或檔案時,	get

	必須使用 POST method。	
Web Site	要流覽的網站。	us.js1.yimg.com
URI	Uniform Resource Identifiers 的縮寫·資源識別 字串·是用於在網路環境中識別檔、可供下載的檔 案、各式服務及電子郵箱等等的各式資源。	/us.yimg.com/lib/common/lsmfonts_20040826.css
Bytes	發送流覽要求的網頁流量。	322
Src IP	發送流覽要求的來源端 IP 地址。	192.168.17.58
Src Port	發送流覽要求的來源端連接埠。	1811
Dst IP	欲流覽的網站之 IP 地址。	64.86.106.216
Dst Port	欲流覽的網站之連接埠。	80

表格 24-2 網頁側錄 - 流覽欄位說明

步驟 2 回應的網頁側錄	Auditor >	• Web Recorder >	> Resp	oonse					
用來儲存 request (要求) 生成的 response(回	Bate: 2080.06.01 +	· · · · · · · · · · · · · · · · · · ·	Tana and	and a strength of these	- Date	0.0	5.0.0	list.	0.4
(m)。同應的網百多位以上網百法暨要求發生時、	E S Web Manager Events	2008-05-19-14:48:27 (m.jsf.ateq.com	290	jest'cos	6101.8	192,108,17,58	3810	84.06 106.218	00 -
應 / " 闫愿的构只尔低以上构只加見女不及工时 '	To Photosel	Distance in the second second program in	290	beat to six	1055.0	10.16.17.58	1811	81.06.108.216	100
料库的同库岬百卢会油侧稳大洁用百五人	CI MORECOLDER	2858-85-10 18-PE IN INCOMENCE	200	maging?	891.8	192.108.17.58	3290	202.43.195.02	100
到應的凹應網貝也曾被側銶仕這個貝囬工。		2008-95-15 14:49-12 (wylengioten	290	mapping	257.0	192.108.17.58	1794	20184.195.07	80
		2006-05-19 14:48 12 he yeng.com	290	mappipi	157,0	192.108.17.58	1290	20184.196.57	90
		2009-0510 101812 (a parecon	280	and the	157.0	10.16.17.59	1210	20184.19037	- 10
		2006-80-10 18:88 12 (wyleng.com)	290	wap-yr	256.8	187.108.17.88	3790	20181.00.07	-
		2006-86-15 14;42 11 Incentions	200	integrigif	1316.8	10.98.17.58	1781	20184.19587	100
		2005-85-15 14:48 11 (wu/ingucors	290	application/e-anvanceant	2948.8	100.108.17.58	1780	203.84.195.57	10
		2005-85-19 HORE 11 Inciding com	240	and the second	110010	10.108.17.58	1287	203.84.185.87	94
		2018-00-10 12-20-11 Depletg.com	200	mappi	2010.0	107.108.17.58	1780	20184.183.97	-
		2006-85-15 164211 (w.a2ping.com	290	application/s prescript	2453.8	182.468.57.58	1285	203.84.195.08	10
		2006-05-15-14:42.11 (w.a2)#rsp.cmt	290	inside lat	\$27.0	192.158.17.59	1794	203.84.195.08	80
		2006-85-19 18:8811 Iwgiing.com	200	inapoli	2907.8	192,108,17.69	1283	203.81.183.97	90
		2005-00-10 Mail 11 Payling-com	290	in a propi	2507.8	18.16.17.68	1282	20184.195.07	80
		2006-35-19 10:48-11 In alphoacers	290	integrigit.	537.6	192.108.17.50	19281	205.84,195.08	88
		2004-85-19-14:42.11 fw.a2;#rsp.cms	290	(expip)	\$17.0	192.168.17.59	1280	203.84.195.98	80
		DB08.85.19 12:8211 (wyleng.com	290	inspig!	2905.8	102.108.17.59	2776	20284.181.97	-00
		2008-85-10 1048-11 (wyleng-com	290	Report	28(6.2	192-158-17.88	1276	203.84.185.07	80
		2006-05-15-14:49-11 (w.a2.phog.com	290	inceptof.	524.0	132.106.17.58	477E	205.84.195.58	80
		2006-85-15 14:48-11 (w.s2)#sq.cms	290	magnigf.	1015.0	192.108.17.50	1271	203.84.195.98	00
		2004-05191602111xg80g.com	200	ana poper	13/3.8	10.108.17.59	2276	20184.181.97	
		2008-85-10 1048-11 (wjerg.com	200	spatication/s d'activate	138043.0	10.108.17.88	1274	211.84,184,07	-
		2008-05-15 14:4209 (wyeng.com	290	ineptories:	3887.8	192.968.17.50	6773	293.84.195.87	00
		2006-05-19-14:48:09 keyling.com	290	interpription (5657.8	192.158.17.50	1772	233.84.195.97	80
		DODERN TR STORED Revenues	140	lenker lere	12/2.8	192.56.17.58	1771	30184.18182	10

欄位	說明	範例
Date	回應流覽網頁要求的時間。	2006-06-19 14:40:24
Web Site	要流覽的網站。	Us_js1.yimg.com
Status Code	狀態碼值·表示網頁流覽的成功或失敗。	200
Content Type	網頁內容型別標示。	Text/css
Bytes	回應流覽需求的網頁流量。	1053.0

InstantScan User Manual

Src IP	流覽網頁要求的來源端 IP 地址。	192.168.17.58
Src Port	流覽網頁要求的來源端連接埠。	1811
Dst IP	欲流覽的網站之 IP 地址。	64.86.106.216
Dst Port	欲流覽的網站之連接埠。	80

表格 24-3 網頁側錄 – 回應欄位說明

第25章

警報中心

25.1 需求

- 1. 網管人員希望知道過去所有系統執行狀態,不希望有非法設定。
- 2. 網管人員每天必須核對系統操作記錄,但是希望簡化並縮減核對的程式。
- 3. 網管人員希望即時收到 alert (警告)與 critical (嚴重) 等級的事件記錄,希望當系統有問題時,能即時提 供解決之道。

25.2 目的

- 1. 網管人員希望知道過去所有系統的管理動作。
- 2. 網管人員希望每天收到設備的記錄報表。
- 3. 網管人員希望即時收到嚴重等級以上的系統記錄。

25.3 方法

- 1. 透過系統記錄的追蹤,您可以檢視管理動作的合法與否。
- 2. 透過 mailer 接收電子郵件。設定每天定時自動寄送記錄檔給網管人員。
- 3. 在 mailer 上啟用透過 e-mail 即時寄送系統記錄。

25.4 步驟

25.4.1 系統記錄

步驟3 檢視系統記錄	Functions > Re	ports > Syst	tem	Ma	nager			
您可以在 Functions > Reports > System	Date : 2006-06-01 💌	ок 🧕 🔀 🕯						
Manager 頁面上流覽所有的系統記錄。系統記錄	System Manager Report	Date	Tier	LD	SYE Message	SYS User	From	15
	E T Events	2008-06-07 14:07:55	Client	\$27	Download configuration	admin	192.160.17.56	-
化承里性分化 5 個寺級。	Aleri XV Coloral	2006-06-07 14:07:50	Client	\$27	Download configuration	sutmin	192.169.17.56	
Δlort (Maming	2006-06-07 13:15:50	Chent	\$27	Download configuration	admin	192.168.17.56	
	Notification	2006-06-07 13:15:46	Chent	\$27	Download configuration	admin	192.168.17.56	
Critical (嚴重)	- 11 Internation	2006-06-07 11:36:12	Chent	\$27	Download configuration	admin	10.180.50.3	
· · ·		2006-06-07 11:35:52	Cirent	\$27	Download configuration	admin	10.180.50.3	
Warning (警示)		2006-06-06 17:17:31	Client	528	Upload configuration	admin	192.168.17.56	
		2006-06-06 16:15:34	Client	S28	Upload configuration	admin	192.168.17.56	
NOTIFICATION (注息)		2006-06-06 19:42:24	Client	S28	Upload configuration	admin	192.168.17.56	
Information (信自)		2006-06-06 15:24:05	Client	S28	Upload coofiguration	admin	192.168.17.56	
Information (旧志)		2006-06-06 15:10:11	Client	S28	Upload configuration	admin	192.168.17.56	-
	1	4			1		10	F
系統記錄詳細資訊請參考 錯誤!找不到參照來 源 。。								

欄位	說明	
Date	系統事件記錄產生的日期與時間。	
Tier	產生系統記錄的層級。因為設備 屬於三層式架構·所以有 Device 層、Management Server 層·與 Client 層。	
LID	系統記錄的編號。	
SYS Message	系統記錄的操作說明,	
SYS User	登入並操作此 設備 的使用者帳號。	
From	造成此系統事件的來源端。	

表格 25-1 系統記錄說明

25.4.2 設定接收系統記錄的時間

步骤1 設定系統記錄的輸出格式	Functions > Reports > System Manager > Export
在 Reports > System Manager 的頁面上按圖示 ■ 。選擇您有接收的報表類型,然後勾選輸出報 表的檔案類型,最後點擊 Save Settings。以後如 果您升級韌體,只要點擊 Load Settings,就可將 之前的設定載入了。	Select the reports to make form System Manager Report Events Of The Critical Of
	Choose export file type
	HTML PDF PEXCEL
	Load Setting Save Setting OK Cancel
步骤 2 設定接收系統記錄的時間	Mailer > Report Center
在 mailer > Report Center 上選擇希望接收系統	InstantScan Management Server MySQL connected V2.0 -
記錄報表的時間、報表格式及勾選要接收哪個裝置	
上的系統記錄。最後輸入報表接收者的電子郵件信	System Info E-Mail Alert FTP Selup Report Center Systog About
71	Daily C Waskiy C Marthly Device IP 192.16B.168.201
	Format
	Report receiver former
	File Nerre ND5 Checksum File Size

25.4.3 啟用即時接收系統記錄

步驟1 啟用透過電子郵件傳送系統記錄	mailer > Syslog							
勾選 Enable/D設備able Send Syslog By	InstantScan Management ServerMySQL connected Y2.0 -							
勾選 Enable/D 設備 able Send Syslog By Email · 拉選您要即時接收系統記錄的嚴重性 · 然 後輸入報表接收者的電子郵件帳號。 設定完成後 · 每當有符合設定的事件記錄產生 · 您 便可即時接收電子郵件寄送的系統記錄警告信件。	InstandScan Management Server: -MySQL connected V2:0 -							

第26章

系統維護

本章介紹系統維護。

26.1 需求

- 設備讓您可以隨時更新韌體與資料庫以符合當前的網路狀態。新的功能、新的攻擊、新的 URL 資料庫,與新的病 毒定義都需要不定時更新,所以本章介紹如果透過 TFTP 伺服器與網頁介面更新設備。
- 2. 當您忘記密碼、韌體或設定檔損毀,您可以透過網頁介面或是 console 介面將韌體恢復到出廠預設值。但當您忘記密碼時,您只可以透過 console 介面,利用救援模式恢復出廠預設值。
- 3. 當您設定好設備後,為避免因不明原因而造成設定檔損毀,所以您可以將現行的設定檔備份,以備不時之需。

26.2 透過 TFTP 伺服器升級韌體

步驟1 設定 TFTP 伺服器	
將 TFTP 伺服器置於 C:\ 槽底下。將所有韌體副	
檔名為 bin 的檔案也放在一起。將這台有安裝	N/A
tftp 伺服器的 PC 之 IP 地址設定與設備 LAN1	
端的 IP 在同一個網段。登入 設備 console 介	
面。輸入" en" 進入許可權模式。	

步驟 2 升級韌體

輸入 ip tftp upgrade image < FILENAME > 192.168.168.170。完成後,設備 將會重開機。相關 CLI 指令,請參考附錄 A 說明。

步驟 3 檢查更新後的韌體設定	======================================	9 Information ====================================
待重開機完成·請用sys ver檢查所有相關設定是否正確。	Firmware Version: Building Time: Hardware ID: Serial Number: ======== Engines/ pattern engine: virus db engine: im-engine: pattern: virus database: url database:	Uersion 3.0.04 20080926-20:07:05 EFEE4BE373F6940CDE0977DA 01591D876FC797ADF7192D16 00D0C99CAA66 10dules Uersion ====================================

26.3 備份設定檔



26.4 還原設定檔

步驟1 還原設定檔	Tools > Config Restore
在工具列上點擊 Tools · 然後點選 Config Restore。	Iools Connig Restore Image: Setting and the setting of the se
	Config Restore

步聯2選擇要還原的設定檔 請選擇要還原的設定檔·然後點擊 Restore 完成 設定。	Tools > Co Look In:	nfig Restore
	File <u>N</u> ame:	050705.bcf
	Files of Type:	CBC Backup Config File (.bcf)
		Restore Cancel

26.5 啟用選購的模組

當您購買設備時,只有標準的L7 模組、Traffic Manager 模組、IM 模組與 Object Manager 模組。如果您有選購 Web Manager,您必須透過使用者介面上傳 Web Manager 模組的 License Key 來啟用它,否則您無法使用 Web Manager,且也無法在 UI 上面看到這個模組。

步驟1 連上註冊網頁	Update > License
在工具列上的 update · 點選 License ·	Update Tools Help
	🧔 Upload configuration
	🔘 Update pattern
	😸 Update URL database
	🔓 License
	License Status
	Coption
步驟 2 輸入 License Key	Update > License
輸入您所選購模組的授權碼,然後點擊 OK 繼續。	License Key 🔀
	Please input Lincense Key :
	License Key : 3L-40418-D5E9A-5B924-3A40C-D6C81
	OK Cancel



26.6 升級 IM 引擎 / 應用程式列為 / 病毒資料庫 / URL 資料庫

26.6.1 自動升級 IM 引擎 / 應用程式列為 / 病毒資料庫 / URL 資料庫

步驟 1 自動更新設定	Update > Option
點擊 Option 。	Update Tools Help
	🧔 Upload configuration
	💮 Update pattern
	😹 Update URL database
	License
	License Status
	G Option
步驟 2 輸入更新中心資料	Update > Option > General
輸入更新中心的位址·您亦可以點擊 Default 按鈕	Update Option
來獲得預設的更新中心網址。然後選擇連線方式	General
如果貴公司透過 proxy 伺服器連上網路·請點選	General Update Center
伺服器的 IP 位址、伺服器連接埠與您的使用者名	Cocation: update.L7.com.tw
稱 和密碼。點擊 Advanced 設定更新項目與排	Advanced Default
程。	Connection
	Direct Connect to Internet
	Manual Proxy Configuration
	User name: yOserName Password:
	OK Cancel

步驟 3 啟用自動更新	Update > C	Dption > Advanced
勾選 enable auto update · 並勾選要自動更新的	Update Optio	n 🛛 🛛
項目。點擊 Schedule 設定更新排程。	and the second s	Advanced
	General	-Auto-update
	*	renable auto update
	Advanced	Pattern VIII II engine VIII DB VIII DB
		scheduling update Schedule
		OK Cancel
步驟 4. 設定更新排程	Update > 0	Dption > Advanced > Schedule
選擇 Weekly · 然後選擇每週自動更新的時間與日		Daily
期。點擊 OK 完成設定。		⊖ Daily
		set update time : Hour : 5 💌 Min : 45 💌
		Weakh
		Weekly
		set update time : Hour : 20 💌 Min : 0 💌
		Monday
		OK Cancel
		On Gener

步驟 1 從 UI 上手動升級應用程式列為	Update > Update p	attern		
點擊 Update pattern。		Update	<u>T</u> ools Help	
		🧔 Uple	oad configuration	
		🔅 Upd	ate pattern	
		😹 Upd	ate URL database	
		🔓 Lice	ense	
		🚡 Lice	ense Status	
		🍈 Opt	ion	
步驟 2 更新應用程式列為	Update > Update p	attern		
點擊 OK 開始更新應用程式列為。				
		Current pa	ttern version is 2.1.01.150	
		Do you wa	nt to upgrade pattern now?	
			OK Cancel	

26.6.2 手動升級應用程式列為

26.6.3 手動升級 URL 資料庫

步驟 1 從 UI 上手動升級 URL 資料庫	Update > Update URL database			
點擊 Update URL database。		<u>U</u> pdate	Tools	Help
		🍯 Uplo	oad con	figuration
		🔅 Upd	late pat	tern
		😹 Upd	late URI	L database
		🔓 Lice	ense	
		🚡 Lice	ense Sta	atus
		🍈 Opti	ion	



26.6.4 在 CLI 標準模式下,恢復出廠預設值

步骤3 恢復出廠預設值

在 CLI 模式下鍵入 sys resetconf now,按 Enter 後,系統將重新開機,所有設定將回復到出廠預設值。

26.6.5 在 CLI 救援模式下,回復出廠預設值

步驟 4 進入安全模式	Press ctrl+e in 5 secs to start with emergency kernel. Enter emergency mode.
在 5 秒的倒數計時內,按 ctrl+e,進入救援	
模式。在這個核心模式中,您可以利用 tftp 指	(Emergency Mode) login as "admin", no password
令來安裝韌體或者將設定檔回復到出廠預設	[EMERGENCY] TOGIN: admin [EMERGENCY]> en
值·甚至您忘記密碼也可以在這個模式下操	lEMERGENCY]# disable Turn off privileged mode command
作。	exit Exit command shell in Configure/Display IP related settings
輸入 sys resetconf now · 系統將重新開機將 設定檔回復到出廠預設值。	sys Configure system parameters [EMERGENCY]# sys resetconf now Config reset to default. System will reboot now

26.6.6 SNMP 控制設定

步驟 1 開啟 SNMP 控制視窗	Tools > SNMP Control
點選 Tool Bar 上面的 Tools 選項 · 就會跳出	
選單·點選 SNMP Control 選項之後·就會跳	
出 SNMP 的控制介面。	

InstantScan User Manual

	Tools Help Account Manager Account Manager Change Password Example Setting Language Setting SNMP Control Source Config Backup Example Setting Restore
步驟 2 設定 SNMP 控管 只要在介面上設定好 SNMP 各項參數 · 您就 可以透過 SNMP 管理員遠端監控設備的系 統狀態、網路狀態等。	Tools > SNMP Control
	Trap community: [rap-comm Trap destination: 192.168.40.5

欄位	說明	範例
啟用 SNMP	啟用 SNMP 遠程監控。	啟用
系統名稱	設備裝置名稱。	WALL-1.yourCompany.com
系統位置	設備安裝的位置。	Office
連絡人信息	控管設備 的網管人員。	m 設備
Get community	透過社群可以獲得 SNMP 的資訊。這裡的 get community 類 似密碼·用來做身份驗證用。	public-ro
Set Community	透過社群可以獲得 SNMP 的資訊。這裡的 set community 類似密碼,用來做身分驗證。	private-rw
信賴的主機	可以透過 設備 獲得或設定社群的 IP 地址。	192.168.1.5
Trap community	傳送 SNMP trap 的社群。	trap-comm
Trap destination	透過設備傳送 SNMP trap 的 IP 位址。	192.168.1.5

附錄

附錄 A 指令行介面(CLI)

您可以利用 web 介面 (http/https) 來設定設備,除此之外,當遇到緊急時刻,您亦可利用 console/ssh/telnet 遠端連線 方式來更改或查詢設定。CLI 指令是非常有用的工具,它可以讓您設定或更改所有介面的 IP 位址、將設定檔重設成出廠預 設值或者是重開機。我們將所有 CLI 指令整理成以下表格,以供您參考。

A.1 CLI 資訊清單 - 標準模式

當您透過 console/telnet/SSH 連上設備 · 必須使用 CLI 指令來設定設備 · 您可依據以下表格所描述的指令來完成設備的設定 ·

主要指令	次要指令	範例	指令說明
?		?	顯示所有指令主選單
enable (en)		enable	開啟許可權模式指令
exit (ex)		exit	離開 CLI 介面
ір			設定相關 IP 參數
	ping	ip ping 202.11.22.33	發送 ICMP 回應需求訊息
	traceroute	ip traceroute 202.11.22.33	這查路由到目的地址所經過的路徑
sys			設定系統參數
	status (st)	sys status	顯示系統與網路狀態
	version (ver)	sys version	顯示設備韌體版本資訊

非許可權模式 Non-privileged mode

表格 A-1 標準模式下的非許可權模式

▲ 注意:如果您不曉得某個指令的參數·您可以在指令後空一格打問號"?" 例如: "ip?" 。所有ip底下可能的參數就 會顯示出來。。

許可權模式 Privileged mode

主要指令	次要指令	範例	指令說明
?		?	顯示所有指令的主選單
d 設備 able (d 設 備)		d 設備 able	關閉許可權模式
exit (ex)		exit	離開 CLI 介面
ір			設定相關 IP 參數
	ifset	ip ifset INTF1	顯示或變更網路介面設定
	ping	ip ping 202.11.22.33	發送 ICMP 回應需求訊息
	set	ip set	設定設備相關 IP 地址
	show	ip show	顯示所有網路設定
	tftp (upgrade)	ip tftp upgrade image <filename> 192.168.168.170.</filename>	從 tftp 伺服器處升級韌體
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所經過的路徑
sys			設定系統參數
	date	sys date	顯示/設定目前系統時間
	halt	sys halt now	關機
	highavail	sys highavail set	High-Availability 相關參數設定
	module	sys module	更新/還原系統模組設定
	password	sys password	變更管理員密碼
	reboot	sys reboot now	重開機
	resetconf	sys resetconf now	重設系統設定檔成出廠預設值
	sessionlog	sys ressionlog on	Session 記錄的設定
	showmac	sys showmac	顯示網路卡的 MAC 位址
	status (st)	sys status	顯示系統狀態
	tcpdump	sys tcpdump management	傾印 (dump) 流經的封包
	uptime	sys uptime	顯示設備正常運作的時間
	version (ver)	sys version	顯示設備韌體版本

表格 A-2 標準模式下的許可權模式

完整的 sys module 與 ip tftp upgrade 指令 · 請參閱下表。

首碼指令	第二指令	第三指令	字尾指令	範例	指令說明
		flushstate		sys module flushstate	手動清除系統內閒置 不用的連線
		query		sys module query	詢問模組版本
			all	sys module restore all	復原系統應用程式列 為/特徵碼/病毒資料 庫
		restore	av	sys module restore av	復原系統病毒和蠕蟲
			pattern	sys module restore pattern	復原系統應用程式列 為
sys	module		signature	sys module restore	復原系統特徵碼
			set	sys module setting set	更改更新伺服器設定
		setting	show	sys module setting show	顯示更新伺服器設定
			all	sys module update all	更新系統應用程式列 為/特徵碼/病毒資料 庫
		update	av	sys module update av	更新系統病毒和蠕蟲
			pattern	sys module update	更新系統應用程式列 ^为
			signature	sys module update	更新系統特徵碼
		c	FILENAME	ip tftp upgrade firmware	從 tftp 伺服器處升級
ip tftp upgrad		firmware	tftp server IP address	<filename> 192.168.168.170</filename>	部體
	upgrade	image	FILENAME tftp server IP	ip tftp upgrade image <filename> 192.168.168.170</filename>	從 tftp 伺服器處升級 image 檔
		module	FILENAME tftp server IP	ip tftp upgrade module <filename> 192.168.168.170</filename>	從 tftp 伺服器處升級 系統模組

表格 A-3 Sys module 與 IP tftp 指令說明

⚠ 注意 · IP TFTP upgrade字尾指令意義如下:

WORD: tftp 伺服器IP地址。

FILENAME: 升級設定檔或韌體的image檔案名稱。

完整 sys sessionlog 指令,請參閱下表。

首碼指令	第二指令	第三指令	字尾指令	範例	指令說明
	Off		sys sessionlog off	關閉系統記錄	
sys	vs Sessionlog	On		sys sessionlog on	啟用系統記錄
	Status		sys sessionlog status	系統記錄狀態	

表格 A-5 sys tcpdump 指令說明

完整 sys tcpdump 指令,請參閱下表。

首碼指令	第二指令	第三指令	字尾指令	範例	指令說明
sys tcpdump		External	dump	sys tcpdump external dump	傾印流經 external 端的封包
			interactive	sys tcpdump external interactive	依交談模式列舉流經 external 端的封包
	tcpdump	tcpdump Internal	dump	sys tcpdump internal dump	傾印流經 internal 端的封包
			interactive	sys tcpdump internal interactive	依交談模式列舉流經 internal 端的封包
		Management	dump	sys tcpdump management dump	傾印流經 management 端的 封包
			interactive	sys tcpdump management	依交談模式列舉流經 management 端的封包

表格 A-6 sys tcpdump 指令說明

A.2 CLI 資訊清單 - 救援模式

如果原始韌體因某些意外而損毀,您需要利用救援模式將韌體回復到出廠預設值。將設備重新開機後,在 5 秒鐘的倒數程式內按 <ctrl> + e 鍵,請輸入 admin 後進入救援模式。

非許可權模式 Non-privileged mode

主要指令 次要	指令 範例	指令說明
------------	----------	------

?		?	顯示所有指令主選單
enable (en)		Enable	開啟許可權模式指令
exit (ex)		Exit	離開 CLI 介面
ір			設定相關 IP 參數
	ping	ip ping 202.11.22.33	發送 ICMP 回應需求訊息
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所經過的路徑
sys			設定系統參數
	date	sys date	顯示目前系統時間

表格 A-7 救援模式之非許可權模式

許可權模式 Privileged mode

主要指令	次要指令	範例	指令說明
?		?	顯示所有指令主選單
d 設備 able (d 設 備)		D 設備 able	關閉許可權模式
exit (ex)		Exit	離開 CLI 介面
ір			設定相關 IP 參數
	ping	ip ping 202.11.22.33	發送 ICMP 回應需求訊息
	set	ip set	設定 device 的 IP 地址
	show	ip show	顯示所有網路設定
	tftp (upgrade)	ip tftp upgrade image <filename> 192.168.168.170.</filename>	從 tftp 伺服器處升級韌體 (相關設定與標準模式 同)
	traceroute	ip traceroute 202.11.22.33	追查路由到目的地址所經過的路徑
sys			設定系統參數
	date	sys date	顯示目前系統時間
	halt	sys halt now	關機
	reboot	sys reboot now	重開機

resetconf	sys resetconf now	重設系統設定檔成出廠預設值
resetpasswd	sys resetpasswd	變更管理員密碼
showmac	sys showmac	顯示網路卡的 MAC 位址

表格 A-8 救援模式之許可權模式

附錄 B

疑難排解

1. 安裝設備後為什麼 MSN 或 Yahoo 都無法登入?

答: 您可能碰到以下幾種情況:

- 1-1 啟動 IM 功能後 User 無法登入 MSN
 - A. 先到 Report 中的 L7 查看 log 狀況,是否被設備所阻擋?為何被擋?
 - B. 如果用戶端的 MSN 無法登入是因為走 port 80 · 而我們只允許用戶端走正常連線的 1863 · 請在用戶端的
 PC 上·把 MSN 中的進階選項 TCP 打勾 · 取消勾選其它如 SOCKS · SOCKS 5 · HTTP Proxy 選項 ·
 - C. 到防火牆端開1條規則 ※= > LAN TO WAN Service: 1863 Allow
- 1-2 啟動 IM 功能後 User 無法登入 Yahoo
 - A. 先到 Report 中的 L7 查看 log 狀況,是否被設備所阻擋?為何被擋?
 - B. 如果用戶端的 Yahoo 無法登入是因為走連接埠 80 · 而我們只允許用戶端走正常連線的 5050 · 請在用戶
 端的 PC 上 · 把 Yahoo 中的網路連線設定選擇第一項 不需使用代理伺服器 · 這時請勿選擇其它選項 ·
 - C. 到防火牆端開1條規則 = > LAN TO WAN Service: 5050 Allow。

2. 如何知道目前設備的網路處理效能?

答:進入 Console 模式下,輸入指令 sys status,可瞭解本裝置的 CPU Loading、Concurrent Sessions 等等。

3. 如果我設定 Auto update pattern[,]那我如何得知目前最新 pattern 有哪些變動?

答: 在管理介面點選 Update > Support I 設備 t · 系統會自動開啟 IE 流覽器告知您目前使用的 pattern 版本與其 所支援的通訊協定。

4. 最新版本的 Pattern 或 URL database 要怎樣更新呢?

答:

- 4-1 在管理介面的工具列上點選您要更新的項目 · 例如 Update > Update Pattern/Database ·
- 4-2 在 console 模式中輸入 sys module update all 或逐項更新 (例如 sys module update pattern)。在此之前 · 請先確認您的對外網路是暢通的。

5. 如何更新韌體呢?

答: 首先請先接洽您購買本裝置的經銷商·向其取得最新韌體·然後在 Console 模式下輸入指令 ip tftp upgrade image <檔案名稱> (例如: ip tftp upgrade image filename.bin 192.168.1.10)。至於怎麼設定 tftp 伺服器與如何從 tftp 伺服器升級韌體·請參考本手冊章節錯誤! 找不到參照來源。。

6. 管理伺服器為什麼都收不到記錄?

答:請依下列步驟檢查您的設定:

- 6-1 請確認在 console 模式中已經設定好本裝置對應的管理伺服器 IP 位址了。
- 6-2 請確認管理伺服器是否有安裝個人防火牆。

6-3 如有啟動防火牆·請於防火牆設定中開啟三個讓管理伺服器與本裝置間溝通用的連接埠(514、1080與3306)。

6-4 如果上述3 個步驟都排除後,最後請確認在服務選項中的 LogServer 之服務是否已經啟動了。

7. 為什麼我在 Console 下都看不到畫面?

- 答:
 - 7-1 請確認終端機選項中·每秒傳輸位是否選擇 115200。超級終端機上的設定值為(8 資料位元、1 停止位元、無同 位檢查、115200 每秒傳輸位)。
 - 7-2 假如步驟 7-1 的設定皆已完整,還是無法進入 console 畫面。那麼請準備-台 PC 或筆記型電腦與管理埠對接, 然後 Ping 管理埠的 IP (出廠預設值為 192.168.1.1)查看 Request 是否有回應。
 - 7-3 如果步驟 7-2 也 ping 不到管理埠之 IP·那麼請直接將本裝置連接到網路上·測試網路是否斷線來測試硬體開機 問題·再進一步確認硬體是否有損壞。
 - 7-4 依上述步驟 3,將本裝置連接到網路上,請依以下結果處理後續事宜:
 - A. 網路正常:請更換 Console 線。
 - B. 網路斷線:請用 RMA 方式聯絡原廠。

附錄 C

系統記錄語法

系統記錄語法

設備: time=2005-01-10 12:57:27; mod=SYS; sev=<1|2|3|4|5>; tier=<TIER>; lid=<LID>; msg=<Message>; by=<user|system>; from=<IP|console|system>;

嚴重等級	Level name
1	Alert (警告)
2	Critical (嚴重)
3	Warning (警示)
4	Notification (注意)
5	Information (信息)

TIER	LID	Message	Severity
	A01	Login success	Information
	A01	Login fail, m 設備 s password	Information
	A02	Change password	Information
	A04	A new user <user> has been added</user>	Notification
Client	A05	User <user> has been deleted.</user>	Notification
tier=1	A07	Login user <user> login failed due to invalid user name</user>	Information
	S25	Backup configuration file by admin	Warning
	S26	Restore configuration file by admin	Warning
	S27	Download configuration	Warning
	S28	Upload configuration	Warning
Mgtsvr	L01	Database 設備 full	Critical
tier=2	L02	Database 設備 cleanup	Critical

	L03	Backup database to 192.168.17.130	Warning
	L04	Send report to user@yourCompany.com	Information
	L05	Restore database from 192.168.1.1	Warning
	L06	Send alert to user@yourCompany.com	Information
	M01	Change E-Mail Alert setting	Notification
	M02	Change FTP Backup setting	Notification
	M03	Change Report Center setting	Notification
	M04	Change Syslog setting	Notification
	A03	Login success	Information
	A03	Login fail, m 設備 s password	Information
	A06	Change password	Information
	S01	Device Startup	Warning
	S02	Device Reboot	Critical
	S03	MGT set to192.168.17.114	Notification
	S04	Gateway IP set to 192.168.17.254	Notification
	S05	Primary DNS set to 10.1.1.1	Notification
	S06	Secondary DNS set to 168.95.1.1	Notification
Device	S07	Management server set to 192.168.17.112	Notification
tier=3z	S08	System time updated to 2005-09-04 12:00:00	Notification
	S09	Factory reset to default settings	Warning
	S10	Firmware upgraded to version X.X.XX	Warning
	S10	Firmware upgrade has failed	Critical
	S11	L7 pattern updated to version X.X.XX.XXX	Warning
	S11	L7 pattern update has failed	Critical
	S12	IM signature updated to version X.X.XX.XXX	Warning
	S12	IM signature update has failed	Critical
	S13	AVDB updated to version X.X.XX.XXX	Warning
	S13	AVDB update has failed	Critical

	S14	Enable L7	Notification
Ī	S14	D 設備 able L7	Notification
ſ	S15	Enable IM	Notification
ſ	S15	D 設備 able IM	Notification
Ī	S16	Enable Traffic Manager	Notification
Ī	S16	D 設備 able Traffic Manager	Notification
Ī	S17	Enable HA	Critical
Ī	S17	D 設備 able HA	Critical
Ī	S18	HA mode changed to AA	Critical
Ī	S18	HA mode changed to AS	Critical
ſ	S19	HA type changed to master	Critical
Ī	S19	HA type changed to slave	Critical
Ī	S20	HA monitored node <node_name> failed</node_name>	Warning
Ī	S21	HA control changed to master	Alert
Ī	S21	HA control changed to slave	Alert
	S22	HA Virtual IP Address: 192.168.17.100	Notification
ſ	S23	HA In-Ping-Nodes: 192.168.17.111	Notification
Ī	S24	HA Ex-Ping-Nodes: 192.168.17.254	Notificaiton
ſ	S29	URLDB	
ſ	S31	L7 pattern updated to version X.X.XX.XXX	Warning
Ī	S31	L7 pattern update has failed(error code:XX)	Critical
ſ	S32	reserved for future using	
	S33	AVDB updated to version X.X.XX.XXX	Warning
ſ	S33	AVDB update has failed(error code:XX)	Critical
Ī	S34	URLDB updated to version X.X.XX.XXX	Warning
Ī	S34	URLDB update has failed(error code:XX)	Critical
Ī	S35	IM engine updated to version X.X.XX	Warning
	S35	IM engine has failed(error code:XX)	Critical

S36	L7 engine updated to version X.X.XX	Warning
S36	L7 engine update has failed(error code:XX)	Critical
S37	reserved for future using	
S38	Antivirus database engine updated to version X.X.XX	Warning
S38	Antivirus database engine update has failed(error code:XX)	Critical
S39	URL database engine updated to version X.X.XX.XXX	Warning
S39	URL database engine update has failed(error code:XX)	Critical
S40	reserved for future using	
S41	L7 pattern restored to version X.X.XX.XXX	Warning
S41	L7 pattern restore has failed(error code:XX)	Critical
S42	reserved for future using	
S43	AVDB restored to version X.X.XX.XXX	Warning
S43	AVDB restore has failed(error code:XX)	Critical
S44	URLDB restored to version X.X.XX.XXX	Warning
S44	URLDB restore has failed(error code:XX)	Critical
S45	IM engine restored to version X.X.XX.XXX	Warning
S45	IM engine restore has failed(error code:XX)	Critical
S46	L7 engine restored to version X.X.XX	Warning
S46	L7 engine restore has failed(error code:XX)	Critical
S47	reserved for future using	
S48	Antivirus database engine restored to version X.X.XX	Warning
S48	Antivirus database engine restore has failed(error code:XX)	Critical
S49	URL database engine restored to version X.X.XX	Warning
S49	URL database engine restore has failed(error code:XX)	Critical
S50	reserved for future using	
ςε1	\$SWID	
221	(Update Successfully. Update database and then respond a new SWID.)	
S52	\$SWID	

	(Keep old license. Don't need to update database and then respond the old SWID.)	
S53	Request 設備 rejected	
S54	Invalid HWID	
S55	Th 設備 device 設備 not reg 設備 tered	
S56	Th 設備 license 設備 invalid	
S57	Th 設備 license has been reg 設備 tered	
S58	Th 設備 license cannot be used on th 設備 device	
S59	Can not connect to database	
S60	No such device	
S61	Can not connect to device	
S62	Unable to clear database table	
S63	Filter L 設備 t error	
S64	Post parameters error	
S65	Post value 設備 invalid	
S66	Invalid software ID	
S67	Execute SQL command fail	
S68	No version obtained	
S69	No such database	
S70	Backup database fail	
S71	Restore database fail	
S72	Unmatched pattern version	
S73	Software ID was reset to trial version	
S74	Invalid checksum	
S75	Can not find backup SQL scheme	
S76	Enable Web Manager	Notification
S76	D 設備 able Web Manager	Notification

表格 D-1 系統記錄格式說明

附錄 D

詞彙集

DDoS (分段式阻斷服務, D 設備 tributed Denial-of-Service)

DDoS 是 DoS 的一種變形,因為它是透過網路分散來源的技巧,所以將之稱作分散式 DoS (D 設備 tributed DoS,簡稱 DDoS) 攻擊。

DoS (Denial of Service)

DoS 是一種入侵程式,可以讓電腦無法直執行某些動作,或者無故當機。與一般駭客入侵不同的是,DoS 攻擊並不會讓電腦內部資料遭到竊取或竄改,而是以癱瘓主機為目的。

FTP (檔案傳輸協定 File Transfer Protocol)

FTP 是在傳輸控制協定 (TCP/IP) 網路使用的一種檔案通訊協定 · 定義如何將一個電腦系統 · 連接現有的網路 (Network) · 以便存取網路上的系統資源 · 其主要工作是提供檔案非錄清單 · 負責檔案傳輸與轉換工作 ·

H.323

H.323 規範是在 1996 年經國際電信聯盟認定,可以解決多媒體傳輸所要求的即時性與連續性問題。其主要內容是在定義 分封切換式網路上終端機之間的壓縮和解壓縮標準、通話程式及媒體傳輸等協定,同時也定義了在分封切換式網路上的終 端如何與傳統的電話網絡互相通話的機制。H.323 界定語音及視訊的壓縮 / 解壓縮設備,雙方溝通的設定與控制。在語音 方面,它支援多種標準,其中以 G.711 為主;至於視訊方面,H.323 則支援 H.261 與 H.263 兩種主要的視訊壓縮 / 解壓 縮標準。

IM (即時通訊, Instant Messaging)

即時通訊是一種聊天應用,透過網際網路即時地與他方使用者傳送文字簡訊,現在更可以傳送檔案、語音、視訊或玩網路 遊戲等。

IPS (異常偵測·Anomaly-Based IPS)

異常偵測則是對使用者或網路流量先建立一個「正常」的行為·再對通過的封包去做比對·假如超過正常行為的門檻值就 是視為異常。此種做法的優點是可以偵測未知型態的入侵·但是誤判率會表較高。

IP Spoofing (IP 地址欺偽)

InstantScan User Manual

這是一種攻擊者得知主機位址之後,利用外部封包攻擊主機的方法,由於封包 (Packet) 的來源位址和內部封包一樣,因此主機 (Host) 會認為這是來自內部的封包,因而允許進行連結 (Link),這種攻擊方法也會被內部破壞者使用。

LDAP (Lightweight Directory Access Protocol)

LDAP 是 Lightweight Directory Access Protocol 的簡稱 · 是目前最流行的目錄服務 (Directory Service, DS) 存取協定。

License Key (授權碼)

設備由多個模組組成,某些模組必須購買授權碼並於開機時輸入此授權碼才可以啟用該服務。

P2P (點對點, Peer-To-Peer)

這是一種傳輸模式,以點對點的方式傳輸訊息,例如曾經瘋狂流行過的 Napster (Napster),就是以點對點的方式傳輸, 使用者在對方提供的檔案伺服器上直接上傳或下載 (Download) 樂曲; P2P 架構要比主從架構 (Client/Server) 簡 單便宜,因為無須太多高深的技術就可以執行,不過當網路負擔太重的啥喉,傳輸的狀況就不會比主從架構理想。

Port

資料 (Data) 進入或出去的一個接連點。

Protocol (通訊協定)

一個議定主要的就是幾個通信處理之間·要被交換的一些訊息格式和訊息內涵的一組協約或規則·讓實施和使用更加方便· 在一些複雜的網路 (Network) 中·高階議定可以用一種分層的方式來使用一些低階議定。

RADIUS (遠端認證撥接使用者服務, Remote Authentication Dial-In User Service)

RADIUS 是被許多網際網路服務供應商 (設備 P) 所使用的認證與記帳系統。當你撥入設備 P時,你必須輸入你的使用 者名稱和密碼。這個資訊被傳送到 RADIUS 伺服器 (Server),查看資訊是否正確,並授權設備 P 系統的存取。雖然 RADIUS 不是一個公認的標準,但是它的規格是由網際網路工程工作團隊所維持。

RDP (遠端桌面協議 · Remote Desktop Protocol)

RDP 是 Windows 終端機伺服器和用戶端用來彼此通訊的通訊協定。用戶端會利用它將按鍵輸入及滑鼠點按資訊傳送到 伺服器,而伺服器則會利用此協定將顯示 資訊傳送給用戶端。

Router (路由器)

路由器又稱為路徑器·使用者在網路層上連接不同網路所用的硬體與軟體·路由器與橋接器 (Bridge) 的功能類似·借 著將許多較小的網路連結在一起·以便有效擴充網路。路由器可以連接使用不同網際網路通訊協定 (IP) 和傳輸方法的 區域網路 (LAN) 。

RS-232

RS-232 為 EIA 標準,是裝置間連結資料最普遍的方式。

Scan

Scan 可以是連接埠、IP 或弱點掃描。駭客掃埠來尋找入侵的目標。他們可能使用 TCP connect() call、SYN 掃描(half-open scanning)、Nmap 等等。

Severity

入侵攻擊的嚴重性被定義成最低到最嚴重 5 個等級,其對預設對應的動作視其嚴重性而定。

Signature

特徵碼是辨識惡意程式之獨特的行為模式。

Smurf Attack

Smurf 攻擊者將偽造來源的 ICMP echo request 封包送到 IP broadcast addresses · 而來源地址設成被害者的位址 · 造成 broadcast 位址回傳大量的 ICMP echo reply 封包給被害者 · 使被害者的網路擁塞甚至中斷。

Spam (垃圾信件)

Spam 原是一種美國肉罐頭的商標 · 隨著網際網路 (Internet) 的出現 · 而被用來指稱垃圾電子郵件 (E-mail) · 這 類垃圾郵件內含許多使用者可能不想看的商業廣告 · 並傳送給大量的收件人 · 用於動詞時 · 則是指將許多使用者不想要的 訊息 (message (MESG) (MSG)) · 貼在相關的郵件或網頁上 ·

Spoofing (欺偽)

指的是以未經過授權的身份,在網路 (Network) 上從事傳輸動作,通常是惡意的行為。

SSL (Secured Socket Layer)

SSL 是將公開金鑰的加密技術加入合併到網景領航員 (Netscape Navigator) 的網路流覽器 (Browser) 裡面,還有 網景公司商業用的伺服器 (Server)裡,且目前大多數的網路 (Network) 伺服器與流覽器也已經採用 SSL。SSL 的 加密與解密過程當中,必須透過密碼簿中的金鑰才能將亂碼完全解開,為了確保使用者拿到的金鑰安全性與公正性,金鑰 必須透過具有公信力的伺服器認證中心認證。

SYN Attack

此種攻擊方式主要是利用 TCP 連結的 three way handshaking 的缺陷。在 TCP/IP 通訊協定中·傳輸雙方 (A、B) 的連結方式是·A 會從特定連接埠送出一個 SYN 封包給 B 的特定連接埠·而此時 B 會響應一個 SYN-ACK 的封包給 A·如果順利到達·A 會再回送一個 ACK 的封包給 B 作確認。在完成這些程式之後·A 與 B 便能確認彼此的連結·此時連線建立·雙方能夠溝通·並傳送與收發資料。SYN 這類攻擊讓 TCP 協議無法完成三次握手協議;

TCP (傳輸控制協議 Transm 設備 sion Control Protocol)

TCP/IP 是一組用來連接網際網路 (Internet) 上主機 (Host)的協定標準。TCP 相當於開放系統互相連線參考模型的 第四層 (運輸層)協議,而 IP 則相當於 OSI/RM 的第三層(網路層)協定。但 TCP/IP 通常是指一組完整的網路通訊協定。

Teardrop

Teardrop attack 的目的不是要去偷取你電腦中的資料,而是要讓使用者的電腦當機無法繼續使用。利用封包重組時的弱點,當資料經由網路傳送,IP 封包經常會被切割成許多小片段。每個小片段和原來封包的結構大致都相同,除了一些記載 位移的資訊。而 Teardrop 則創造出一些 IP 片段,這些片段包含重迭的位移值。當這些片段到達目的地而被重組時,可能 就會造成一些系統當機。當它檢查到後面片段的資料長度大於重迭的資料片段時,重迭部份將會被略過,但是後面的片段 的資料長度小於重迭的資料片段時,使得資料片段長度太小,當接收到傳來的封包時,只會去檢查是否太長,是否應該捨 棄重迭多餘的部分,但卻不會去檢查是否太短而造成了錯誤.

Telnet

終端機 (terminal(T)(TERM)(TML)) 模擬程式是遠端登入的網際網路通訊協定 (IP)・使電腦使用者可與伺服器 (Server) 做互動式的連結,並存取 (Access) 遠端網站。

Terminal Emulator (終端機模擬器)

容許在個人電腦和主機電腦或裝置間做同步資料傳送,而資料則以主機可接受的格式來交換。。

TFTP (簡單檔案傳輸協定 Trivial File Transfer Protocol)

TFTP 是 TCP/IP Protocol 中的一員,和 FTP 一樣是傳輸檔案用,但是 FTP 是使用 TCP,但是 TFTP 是使用 UDP 來傳輸,使用 UDP 是不作傳輸資料正確性的驗證,所以實際的檔案傳輸是不會使用到 TFTP,然而若您是經常使用網路設備如 Terminal Server、Router 或是 SNMP Hub 的話,那您便可能需要使用 TFTP 來 Upgrade 網路設備的 Firmware 或 Software。

Transparent Mode (透通模式)

產品的複雜作業情形已被隱藏起來,使用者使用產品時一點都不會覺得有何困難,而且操作容易。一般的透通模式裝置, 容易安裝於任何網路架構底下,且不需要改變既有的網路設定。

Transport (傳輸模式)

IPsec 封裝機制的一種 · 傳輸模式即是所謂的 Host-to-Host 的封裝機制 · 亦即由連線兩端主機對其交換的 IP 封包以前段 所述的 AH 或(及) ESP 做安全保護 · 兩通訊主機皆須實作有 IPsec 。

Trojan (特洛伊木馬, Trojan Horse)

顧名思義·特洛伊木馬是一種看似無害其實會隱藏起來在電腦內部作怪的程式。它以合法功能的面貌偽裝·將病毒碼放在 一個外表看起來十分正常的程式當中·等到適當的時機才開始破壞的動作。特洛伊木馬一種惡性程式碼 (Malicious code) ·但和病毒 (Virus) 最大的不同是·特洛伊通常不會自我複製·大多用來竊取電腦密碼。

UDP (使用者資料流程通協議, User Datagram Protocol)

UDP 是傳輸層通訊方法或通信協定,用於傳送短暫需求的少量資料。這個通信協定可提供資料傳輸量有限的服務,因此不需要驗證目的端是否已接收動作的應用程式資料通訊機制。

UID (使用者識別碼, User IDentification)

一種碼,具有惟一性,可以用來識別一個系統的使用者。

URL (統一資源定位器, Uniform Resource Locator)

指明某個體所在位置的標準方式,所謂某個體,通常是指網際網路 (Internet) 上的網頁,至於其它的個體我們在下麵 說明。全球資訊網 (WWW) 以 URL 作為網址的格式。在超檔標示語言 (HTML) 的檔中,利用 URL 來指定超連結 (Hyperlink) 的目標位置,通常這個目標位置就是另一個 HTML 檔 (而且還可能儲存在另一台電腦上)。

Virus (病毒)

病毒是一種程式,一種會將自己附加在其它程式裡面的軟體,當附加程式被執行的時候,病毒程式也跟著啟動。病毒具有 傳播和感染的特性,可能會造成系統損害、刪除程式或者資料。病毒通常會附著在可執行檔或開機磁片、磁片,甚至硬碟 分割磁區,不過必須附加在其它程式中才能感染另一台電腦,某些病毒也會借著電子郵件 (E-mail) 感染其它電腦。

VPN (私有虛擬網路, Virtual Private Network)

VPN 是通道 (Tunneling)、加密 (Encryption)、身分辨認 (Authentication)、存取控制 (Access Control)等 技術·及經由 Internet、管理式 IP 網路、或網路供應商骨幹來傳遞資料等服務之眾多專案的綜合體。VPN 能利用公用網 絡來建立與遠端使用者、分支辦公室及夥伴建立專屬連結。如果企業想要有一個安全有保障的廣域網路絡環境· VPN 可 以透過目前的公眾網路·在網路上劃分出一條類似私有專線所提供的通道·即所謂的 VPN 的主要元件 – Tunneling·企 業包括 Internet、企業內網際網路、 企業外部網路的使用者都可以在通過安全認證後, 在這個通道內不受時間與地點限制, 享有其所需的網路服務。

Vulnerability (弱點)

系統或應用程式容易被攻擊的點。

WAN (Wide Area Networks)

廣域網路絡是能在廣大地理區域傳輸資料的電腦網路·它是由一些透過電信服務連接的區域網路組成。與區域網路不同點 在於·它們使用的規約不相同·傳輸速率比區域網路低。

Worm (電腦蠕蟲)

電腦蠕蟲也可說是電腦病毒的一種,與病毒不同的是,蠕蟲不會感染寄生在其它檔案。蠕蟲的主要特性是會自我複製並主動散播到網路系統上的其它電腦裡面。就像蟲一樣在網路系統裡面到處爬竄,所以稱為「蠕蟲」。

WWW (World Wide Web)

網際網路的通稱。
附錄 E







InstantScan User Manual