



User Guide



V.1.2 2008/03



商標聲明

所有在本書提及的商標、註冊商標,商品名稱等等均為其相關持有人所有。

智慧財產權聲明

本書所提到的商標均屬於其合法註冊之公司所有。

技術支援

威播科技提供相關網路安全技術支援,均可透過Web、E-mail 或是客服專線, 解決產品上使用的問題。

網址

威播科技的網址為: <u>WWW.BROADWEB.COM</u>,透過威播科技網站提供技術支援,提供線上下載 FAQ、技術白皮書、產品使用手冊、產品型錄及網路安全技術相關資訊。

威播網路安全服務團隊 (BSST)

威播網路安全服務團隊(BSST)網址: BSST.BROADWEB.COM 主要提供資安技術文件、資安課程教材、攻擊特徵 FAQ、攻擊資料庫最新版本 發佈消息及內容,並包含資安討論區,依據不同的主題由 BSST 指派專家提供資 安服務。

客服專線

威播科技客服專線 +886-3-610-0606。

技術服務時間

上班時間星期一至星期五,早上9:00至下午6:00,例假日及國定假日除外。



目錄

第一章 NK6000 介紹	1
1.1 NK6000 功能說明	1
1.2 BEMS SERVER 與 PLUG-IN	2
1.3 NK6000 建置範例	4
1.4 NK6000 產品系列	4
第二章 安裝與設定	6
2.1 NK6000 產品外觀	6
2.2 安裝 NK6000 設備	8
2.2.1 固定 NK6000 於標準 19"機架	8
2.2.2 連接電源	8
2.3 設定基本參數	9
2.3.1 超級終端機模式 (Hyper Terminal)	9
2.3.2 網路遠端連線模式 (Remote Connected)	
2.3.3 登入命令列模式 (Command Line Interpreter)	10
2.3.4 設定 IP 位址 (IP Address)	11
2.3.5	12
2.3.6	13
2.3.7 設定網域名稱伺服器 (DNS)	14
2.3.8 設定 BEMS 伺服器 (BEMS Server)	15
2.3.9 設定虛擬網路編號 (VLAN ID)	15
第三章 BEMS 與 PLUG-IN	17
3.1 註冊及啓動密鑰 (A/K) 下載	17
3.2 程式安裝與啓動	19
3.2.1 安裝 JRE (Java Runtime Environment)	20
3.2.2 安裝資料庫程式 (如 MySQL)	21
3.2.3 安裝 BEMS Server 主程式	22
3.2.4 啓動 BEMS Server 程式	
第四章 BEMS ADMIN CONSOLE	34
4.1 登入 Admin Console	34
4.2 系統 (System)	35
4.2.1 產品註冊 (Product Registration)	
4.2.2 安裝 Plug-in (Load Plug-in from DUC)	
4.2.3 刪除 Plug-in (Unload Plug-in)	
4.2.4 檢查升級 (Check for Update)	



4.3 使用者 (USER)	37
4.3.1 新增群組使用者 (Insert user group)	
4.3.2 <i>刪除群組使用者</i> (Remove user group)	40
4.3.3 <i>修改群組使用者</i> (Modify user group)	40
4.3.4 新增個別使用者 (Insert user)	40
4.3.5 <i>刪除個別使用者</i> (Remove user)	41
4.3.6 <i>修改個別使用者 (Modify user)</i>	41
4.4 設備 (DEVICE)	42
4.4.1 增加設備 (Insert device)	42
4.4.2 删除設備 (Remove device)	43
4.4.3 修改設備 (Modify device)	43
4.5 記錄 (LOG)	43
4.5.1 删除所有系統記錄 (Delete all system logs)	44
4.5.2 儲存記錄成檔案 (Save system logs to file)	44
4.5.3 <i>篩選系統記錄 (Filter system logs)</i>	44
第五章 NK6000 管理介面	45
5.1 登入 NK6000 管理介面	45
5.2 <i>主要操作介面</i>	
5.3 修改登入密碼	47
5.4 NK6 PLUGIN 操作	48
第六章 設備訊息	49
6.1 設備訊息 (Device Information)	49
6.1.1 設備訊息	
6.1.2 設備系統時間	51
6.1.3 <i>管理設定 (Management Setting)</i>	
6.2 連線埠設定 (Port ConFiguration)	53
第七章 物件設定	56
7.1 主機設定 (HOST CONFIGURATION)	56
7.2 虛擬網路 (VI AN CONFIGURATION)	
7.3 時程設定 (Schedul e Configuration)	
74 服務設定 (SERVICE CONFIGURATION)	61
第八音 政策管理	
δ.1 防禦政策	
8.2 以擎狩街 (SIGNATURE)	
8.3 <i>新增 修改 删除防禦收策</i>	66



www.broadweb.com	NK6000 使用手册
8.3.1 新增政策	66
8.3.2 修改 / 刪除政策	74
8.3.3 其他	74
8.4 政策群組	76
8.4.1 新增政策群組	77
8.4.2 删除政策群組	
8.4.3 修改政策群組	
第九章 即時監測	87
9.1 儀表版 (Dashboard)	
9.2 事件 (EVENT)	
9.3 <i>流量 (T</i> RAFFIC)	
9.4 利用率 (UTILITY)	
第十章 報表設定	92
10.1 事件列表 (Event List)	
10.1.1 <i>虛擬設備 (Virtual Device)</i>	
10.1.2 月曆	93
10.1.3 事件清單顯示	94
10.2 內建報表 (PREDEFINED)	94
10.2.1 <i>類型</i> (Type)	
10.2.2	
10.2.3 時間 (Time)	
10.2.4 <i>報表 (</i> Report)	
10.2.5 <i>內建報表範例 (IPS 類</i>)	
10.2.6 <i>內建報表範例 (ACL 類</i>)	
10.3 選擇查詢 (QUERY ON DEMAND)	
10.3.1 <i>類型 (Type)</i>	
10.3.2 設備 (Device List)	
10.3.3 時間 (Time)	
10.3.4	
10.3.5 選擇查詢範例 (IPS 類)	
10.4 定期報表 (SCHEDULE REPORT)	
10.4.1 排程工作	
10.4.2 報表樣本	110
第十一章系統記錄	
第十二章 NK6000 CONSOLE	



12.1 登入 Console 介面114
12.2 求助命令 (HELP)115
12.3 操作功能鍵116
12.4 系統 (System)功能群組116
12.4.1 <i>系統狀態 (All Status)</i> 117
12.4.2 <i>事件記錄 (Log)</i> 119
12.4.3 <i>變更密碼 (Password)</i> 119
12.4.4 <i>還原設定 (Reset Config)</i> 120
12.4.5 <i>停止系統 (Stop System)</i> 121
12.4.5 <i>重新啓動 (Reboot)</i> 122
12.5 設備 (Device) 功能群組123
12.5.1 網路位址 (IP)124
12.5.2 <i>網路遮罩 (</i> Netmask)125
12.5.3 <i>閘道器 (Gateway)</i> 126
12.5.4 <i>網域名稱伺服器 (DNS)</i> 127
12.5.5 TCP <i>連線逾時時間 (</i> TCP Timeout)127
12.5.6 最大系統事件記錄數量 (Max. Log)128
12.5.7 BEMS 伺服器 (BEMS Srv.)129
12.5.8 <i>連接埠設定 (Port Config)</i> 129
12.5.9 HA (High Availability)131
12.5.10
12.5.11 PING
附件一 安裝 MYSQL135



圖表目錄	
圖表 1: 電腦主機功能規格需求	3
圖表 2: NK6000 建置範例	4
圖表 3: NK6000 硬體前外觀	6
圖表 4: NK6000 硬體後外觀	6
圖表 5: NK6000 外觀燈號說明	7
圖表 6: NK6000 鎖上耳翼	8
圖表 7: NK6000 鎖上機架	8
圖表 8: NK6000 連接電源	8
圖表 9: NK6000 連接 Console 埠	9
圖表 10: 終端機模擬參數	9
圖表 11: 連結 NK6000 MGMT 埠	10
圖表 12: 命令列模式登入畫面	10
圖表 13: 命令列模式畫面	11
圖表 14: 設定 IP 位址 (IP Address) 畫面	11
圖表 15: IP 位址 (IP Address) 再次確認變更	12
圖表 16: 設定子網路遮罩 (Netmask) 畫面	12
圖表 17: 子網路遮罩 (Netmask) 再次確認變更	13
圖表 18: 設定閘道器 (Gateway) 畫面	13
圖表 19: 閘道器 (Gateway) 再次確認變更	14
圖表 20: 設定網域名稱伺服器 (DNS) 畫面	14
圖表 21: 設定 BEMS 伺服器 (BEMS Server) 畫面	15
圖表 22: 設定虛擬網路編號 (VLAN ID) 畫面	16
圖表 23: 虛擬網路編號 (VLAN ID) 再次確認變更	16
圖表 24: 連線 my.broadweb.com	18
圖表 25: 註冊帳號塡寫畫面	19
圖表 26: 正確輸入登入帳號/密碼後之畫面	19
圖表 27: 原廠光碟執行畫面	20
圖表 28: JRE 程式下載及安裝範例	21
圖表 29: MySQL 程式安裝範例	21
圖表 30: 安裝歡迎畫面	22
圖表 31: 輸入 A/K 畫面	23
圖表 32: 系統安裝參數畫面	24
圖表 33: 資料庫 (如: MySQL) 參數畫面	25
圖表 34: 管理者設定視窗	25
圖表 35: 設定遠端連線線上更新的參數畫面	26
圖表 36: HTTP Server 參數設定視窗	27
圖表 37: 傳送訊息所需的電子郵件參數設定	28



圖表	38:	Syslog 相關參數設定畫面。	.29
圖表	39:	DNSLookup 參數設定視窗	.29
圖表	40:	登入嘗試鎖定設定視窗	.30
圖表	41:	安裝目錄選擇畫面	.30
圖表	42:	需要安裝的程式 (Core 以及 Library)	.31
圖表	43:	程式安裝完畢畫面	.31
圖表	44:	建立捷徑	.32
圖表	45:	全部程式安裝完畢畫面。	.32
圖表	46:	啓動 BEMS Server 安裝成系統服務	.33
圖表	47:	於 MS-DOS 模式下手動執行	.33
圖表	48:	工具列中 BEMS Admin Console 圖示	.34
圖表	49:	BEMS Admin Console 登入畫面	.34
圖表	50:	BEMS Admin Console 畫面	.35
圖表	51:	更新網站上有 netkeeper plug-in 可供下載使用。	.36
圖表	52:	個別使用者畫面。	.37
圖表	53:	群組使用者畫面。	.37
圖表	54:	群組使用者概況 (User Group Profile)	.38
圖表	55:	Admin 權限設定畫面。	.39
圖表	56:	Config 權限設定畫面。	.39
圖表	57:	View 權限設定畫面。	.40
圖表	58:	新增使用者操作畫面	.41
圖表	59:	設備清單圖示(表格模式)	.42
圖表	60:	設備清單圖示(樹狀模式)	.42
圖表	61:	新增設備圖	.43
圖表	62:	紀錄顯示畫面	.44
圖表	63:	紀錄篩選畫面	.44
圖表	64:	瀏覽器畫面	.45
圖表	65:	操作程式下載畫面	.46
圖表	66:	登入 BEMS 管理系統畫面	.46
圖表	67:	主操作畫面說明	.47
圖表	68:	修改密碼畫面	.47
圖表	69:	NK6 Plugin 畫面	.48
圖表	70:	工具列按鍵	.49
圖表	71:	工具列按鍵	.49
圖表	72:	儲存除錯資訊	.50
圖表	73:	更新設定選項	.50
圖表	74:	設備訊息	.51
圖表	75:	設備系統時間	.51



圖表	76:	設定系統時間	.52
圖表	77:	管理設定	.52
圖表	78:	連線方式設定	.53
圖表	79:	連線埠設定畫面	.53
圖表	80:	設定連線埠畫面	55
圖表	81:	設定 HA 功能埠畫面	55
圖表	82:	主機設定 (HOST Configuration)	56
圖表	83:	新增/修改群組視窗	.57
圖表	84:	新增/修改位址視窗	.57
圖表	85:	VLAN 參數畫面	.58
圖表	86:	修改 VLAN 物件	.59
圖表	87:	時程 (Schedule) 畫面	.60
圖表	88:	新增/修改時程 (Schedule) 物件	.60
圖表	89:	服務 (Service) 設定畫面	.61
圖表	90:	新增/修改服務 (Service) 畫面	62
圖表	91:	編輯 Port 範圍	.62
圖表	92:	表格列表模式 (Table View) 畫面	.64
圖表	93:	樹狀列表模式 (Tree View) 畫面	.65
圖表	94:	新增政策畫面	.66
圖表	95:	政策屬性畫面	.67
圖表	96:	辨識條件	.67
圖表	97:	選項	.68
圖表	98:	TCP port 選項	.68
圖表	99:	UDP port 選項	.68
圖表	100	: 特徵比對模式	.69
圖表	101	:特徵型態	.69
圖表	102	l: 特徵內容	.70
圖表	103	: 攻擊反應	.70
圖表	104	:進階設定: IP 標頭	.71
圖表	105	: 進階設定: TCP 標頭	.72
圖表	106	: 進階設定: UDP 標頭	.72
圖表	107	': 進階設定: ICMP 標頭	.73
圖表	108	: 進階設定: IGMP 標頭	.74
圖表	109	: 搜尋政策	75
圖表	110	: 匯出政策儲存成檔案	75
圖表	111	: 選擇檔案匯入政策	.76
圖表	112	: 防禦政策群組畫面	.76
圖表	113	:新增政策群組	.77



圖表	114:	選擇政策偵測範圍	.77
圖表	115:	修改政策群組圖-1 (表格模式)	.78
圖表	116:	修改政策群組圖-2 (表格模式)	.78
圖表	117:	修改政策群組 (樹狀模式)	.79
圖表	118:	修改政策畫面之一	.80
圖表	119:	修改政策畫面之二	.80
圖表	120:	修改政策畫面之三	.80
圖表	121:	保護範圍與反應	.81
圖表	122:	保護範圍與反應	.82
圖表	123:	ACL 政策畫面	.83
圖表	124:	編輯 ACL 政策畫面	.84
圖表	125:	LAN 範圍定義	.85
圖表	126:	新增 LAN 端範圍	.85
圖表	127:	連線埠對映	.86
圖表	128:	定義連線埠對映	.86
圖表	129:	儀表版 (Dashboard)	87
圖表	130:	事件 (Event) 列表	.88
圖表	131:	暫停 (Pause)	.88
圖表	132:	繼續 (Resume)	88
圖表	133:	事件列表過濾	.89
圖表	134:	流量一 (Traffic)	.90
圖表	135:	流量二 (Traffic)	.90
圖表	136:	利用率 (Utility)	.91
圖表	137:	報表設定畫面	92
圖表	138:	事件列表 (Event List) 畫面	93
圖表	139:	選擇虛擬設備	.93
圖表	140:	選擇日期	.94
圖表	141:	事件列表顯示 (Event List)	94
圖表	142:	內建報表 (Predefined Report)	.95
圖表	143:	IPS 類之內建報表	.96
圖表	144:	前 10 名攻擊來源長條圖	.97
圖表	145:	前 10 名攻擊來源圓餅圖	.97
圖表	146:	前 10 名攻擊目的長條圖	.97
圖表	147:	前 10 名攻擊目的圓餅圖	.98
圖表	148:	前 10 名攻擊來源與目的長條圖	.98
圖表	149:	前 10 名攻擊來源與目的圓餅圖	.98
圖表	150:	前 10 名攻擊名稱長條圖	.99
圖表	151:	前 10 名攻擊名稱圓餅圖	.99



圖表	152:	嚴重程度統計長條圖	. 100
圖表	153:	嚴重程度統計圓餅圖	. 100
圖表	154:	攻擊種類統計長條圖	. 100
圖表	155:	攻擊種類統計圓餅圖	. 101
圖表	156:	嚴重程度趨勢圖 (Severity Trend)	. 101
圖表	157:	攻擊種類趨勢圖 (Category Trend)	. 102
圖表	158:	ACL 類之內建報表	. 102
圖表	159:	選擇查詢 (Query on Demand)	. 103
圖表	160:	選擇設備清單	. 104
圖表	161:	選擇日期	. 104
圖表	162:	查詢條件	. 105
圖表	163:	Query on Demand 長條圖	. 105
圖表	164:	Query on Demand 圓餅圖	. 105
圖表	165:	列印查詢報表	. 106
圖表	166:	定期報表 (Schedule Report)	. 106
圖表	168:	新增/編輯排程工作(頁面一)	. 108
圖表	169:	新增/編輯排程工作(頁面二)	. 109
圖表	170:	管理報表樣本	. 110
圖表	171:	新增編輯報表樣本	. 111
圖表	175:	系統訊息 (System Log) 視窗	. 112
圖表	176:	登入 (Login) 畫面	. 114
圖表	177:	Console 介面	. 115
圖表	178:	求助 (Help) 畫面	. 115
圖表	179:	系統 (System) 功能選單	. 116
圖表	180:	系統狀態 (All Status) 畫面-1	. 117
圖表	181:	系統狀態 (All Status) 畫面-2	. 118
圖表	182:	事件記錄 (Log)	. 119
圖表	183:	變更密碼 (Password) 畫面	. 120
圖表	184:	還原設定 (Reset Config) 畫面	. 121
圖表	185:	停止系統 (Stop System) 畫面-1	. 121
圖表	186:	停止系統 (Stop System) 畫面-2	. 122
圖表	187:	重新啓動 (Reboot) 畫面	. 122
圖表	188:	設備 (Device) 功能選單	. 123
圖表	189:	網路位址 (IP) 畫面	. 124
圖表	190:	網路位址 (IP) 再次確認變更	. 124
圖表	191:	網路遮罩 (Netmask) 畫面	. 125
圖表	192:	網路遮罩 (Netmask) 再次確認變更	. 125
圖表	193:	閘道器 (Gateway) 畫面	. 126



圖表	194:	間道器 (Gateway) 再次確認變更	127
圖表	195:	網域名稱伺服器 (DNS) 畫面	127
圖表	196:	TCP 連線逾時時間設定 (TCP Timeout) 畫面	128
圖表	197:	最大系統事件記錄數量 (Max Log) 畫面	128
圖表	198:	BEMS 伺服器 (BEMS Srv.) 畫面	129
圖表	199:	連接埠設定 (Port Config) 畫面	130
圖表	200:	Link Mode 子選項	130
圖表	201:	Mode 子選項	130
圖表	202:	Policy Bypass 子選項	131
圖表	203:	連接埠設定 (Port Config) 儲存詢問	131
圖表	204:	HA (High Availability) 畫面	132
圖表	205:	虛擬網路編號 (VLAN ID) 畫面	132
圖表	206:	虛擬網路編號 (VLAN ID) 再次確認變更	133
圖表	207:	Ping 功能畫面	133
圖表	208:	Ping 192.168.168.1	134



1 第一章 NK6000 介紹

本章說明

主要說明 NK6000 的主要功能及特色,並介紹應用 NK6000 的網路架構。

本章內容包含下列使用說明

章節	描述
1.1	NK6000 功能說明
1.2	BEMS Server 與 Plug-in
1.3	NK6000 建置架構範例
1.4	NK6000 產品系列

1.1 NK6000 功能說明

NK6000 超高速網路入侵防禦系統,是處理效能達到超高速 (Gigabit) 等級 的 IPS (Intrusion Prevention System) 硬體設備,可以被建置在網路系統的任何 一個地方,負責執行網路安全防禦政策,偵測網路封包的正常與否,以及阻絕不 正當的網路攻擊行為,確保網路系統的正常運作,並且有效防範企業機密外洩。 建議 NK6000 設備建置在需要極高度的安全防護網段的出入口端,以保護整個網 路系統。

NK6000 產品的主要特色有:

■ 多重功能的網路安全設備:

因應層出不窮且日新月異的網路入侵或是網路攻擊事件,NK6000 除了可防 護企業網路免於網路攻擊外,豐富的特徵碼資料庫中更包含了蠕蟲、P2P 下載 程式、及 IM 網路即時聊天程式特徵碼,網路管理者可依照企業需求開放或是加 以攔阻,這些功能可讓企業節省網路頻寬,提高員工專注力及效率,為企業帶來 更多的利潤。

■ 靈活部屬的安全防禦與虛擬 IPS 功能:

NK6000 提供了多種安全防禦運作模式,包括了 Inline-IPS / Inline-IDS / Inline-Monitor...等等運作模式,並且支援了 HA 的功能,讓 NK6000 設備可以在





既有 HA 架構之網路環境中正常運作。

NK6000 增加了虛擬 IPS (Virtual IPS)的彈性設定,使用者可以利用一台 NK6000 機器,依照實際的網路規劃,把網路埠 (Port)做不同的切割,成為虛 擬的 IPS 設備來運作,每一個虛擬的 IPS 設備可以擁有獨立的安全防禦政策, 如此運用可以增加 NK6000 在大型網路架構中的使用彈性。

■ 應用軟體安全漏洞的虛擬修補防禦能力:

NK6000 防禦網路安全的特色之一,就是提供了針對應用軟體程式的『虛擬 修補』防禦方式。

在軟體程式的漏洞被發現後,到針對該漏洞產生的攻擊手法產生,或是該漏 洞的修補程式推出之前,這一段是網路安全專家與駭客族群之間的時間競賽。即 使在漏洞的修補程式推出之後,往往還是會有使用者因為不同因素無法進行修 補,而遭受到駭客的侵擾。

威播科技研發出針對程式漏洞防禦的『虛擬修補』技術,讓即使無法進行程 式漏洞修補的客戶,還是可以在 NK6000 的保護傘下正常的運作, 免受網路攻擊 的侵擾!

BEMS (BroadWeb Extensible Management System):

BEMS 是以利用 Java 語言環境開發而成的集中控管軟體程式。所有網路安 全偵測防禦政策的設定、封包監控、安全事件回報、與事件報表的產生,均是藉 由此 BEMS Server 與 Plug-in 相互之間的搭配來完成。威播科技公司的 IPS 設 備負責接受來自 BEMS Server 的安全政策命令後確實執行,並且回報網路上發 生的事件記錄到 BEMS Server 上,供使用者進行查詢。

BSST (BroadWeb Security Service Team):

BSST (BroadWeb Security Service Team) 是由一群網路安全專家所組成,是原廠的網路安全服務團隊。任務在於鑽研駭客入侵手法,蒐集網路安全技術情報,隨時掌握各種漏洞訊息,制定最新的攻擊防禦政策、提供相關技術支援、安全技術諮詢、教育訓練等等,是客戶網路安全服務的保障。

1.2 BEMS Server 與 NK6 Plug-in

NK6000 防禦網路安全需要搭配 BEMS Server 與 NK6 Plug-in 運作而成。 網路安全偵測防禦政策的設定、網路封包監控與安全事件報表的產生,均是藉由 BEMS Server 來完成。因此在連上網路之前,須先完成 NK6000 設備的 IP 位址 等等相關參數設定,才能夠與 BEMS Server 相互溝通。



考慮資料傳遞時可能造成網路頻寬些許額外的負擔,原廠設計 NK6000 利用 設備的管理介面埠 (Management Port) 來傳遞網管資料,並且建議把 BEMS Server 與 NK6000 設備設定於同一個子網段之內,以減少網路頻寬負擔。管理 者在安裝本套系統之前,請先確定至少兩組可用之 IP 位址,分別要設定在 NK6000 設備以及政策伺服器 BEMS Server 上,等到 IP 相關參數設定完畢之 後,即可把 NK6000 設備以及政策伺服器 BEMS Server 分別安裝到網路上運 作。所有安裝或執行 BEMS Server 所需的應用程式均可在隨貨附贈的 CD 光碟 片或是網際網路上找到。

使用者自行準備的電腦主機至少需要符合以下的功能規格需求:

	最低需求	建議規格	
中央處理器(CPU)	P4-2.4G	P4-2.8G or above	
記憶體(Memory)	1GB	2GB or above	
硬碟容量(HD)	40GB	60GB or above	
網路卡(NIC)		1	
作業系統 (OS)	Microsoft Windows XP Professional		

圖表 1: 電腦主機功能規格需求

建議為了維持效能及可用性,請不要在該電腦 (PC) 或是主機 (Host) 上安 裝其他非必要之應用軟體,以確保政策伺服器 BEMS Server 的正常運作。

說明:

若電腦已經安裝了 JRE (Java Runtime Environment) 程式以及 MySQL 資料庫 程式,請直接安裝 BEMS Server 程式並依照步驟完成安裝程序即可。

原廠提供之光碟片內容如下:

- 1. 下載 JRE (Java Runtime Environment) 程式的連結。
- 2. 下載 MySQL 資料庫程式的連結。
- 3. BEMS Server 系統安裝程式。
- 4. 快速安裝手冊檔案 (Quick Installation Guide),使用手冊檔案 (User Guide)。
- 5. Adobe Reader 應用程式。

說明:

JRE 程式:可至 <u>http://java.sun.com/downloads/</u>下載適合的版本。 MySQL 資料庫程式:可至 <u>http://dev.mysql.com/</u>下載適合的版本。



建置整個 NK6000 系統可以被區分為六大部分,詳細步驟請參考快速安裝手 冊說明。

1.3 NK6000 建置範例

使用者可以把 NK6000 設備建置在需要高度安全標準要求的網路伺服器前面,或是需要高度安全的網段出入口的前面,而透過 BEMS Server 的管理,達到集中管理的目的。

以下是大型網路建置的建議架構圖:



圖表 2: NK6000 建置範例

1.4 NK6000 產品系列

型號	NK6105	NK6210C	NK6210G	NK6210F
機台高度	1U	2U	2U	2U
雙電源備援功能	無	有	有	有



	GE Copper x 7	GE Copper x 7	GBIC x 4	Fiber x 4
介面數量			GE Copper x 3	(LX/SX)
				GE Copper x 3
最大連線數	512K	1M	1M	1M
Bypass 功能	Copper Only	Copper Only	Copper Only	Fiber & Copper





本章說明

主要說明 NK6000 安裝與設定步驟。

本章內容包含下列使用說明

章節	描述
2.1	NK6000 產品外觀
2.2	安裝 NK6000 設備
2.3	設定基本參數

2.1 NK6000 產品外觀



圖表 3: NK6000 硬體前外觀



圖表 4: NK6000 硬體後外觀



機器燈號說明:

- PWR:電源顯示燈號。
- SYS:系統顯示燈號。
- E0 port: copper 介面之 IPS 的 WAN port。E0 與 E1 為成對的虛擬 IPS。
- E1 port: copper 介面之 IPS 的 LAN port。
- E2 port: copper 介面之 IPS 的 WAN port。E2 與 E3 為成對的虛擬 IPS。
- E3 port: copper 介面之 IPS 的 LAN port。
- E4 port: copper 介面之 IDS port,或是第一對 IPS (E0, E1)的映射埠 (Mirror port)。
- E5/HA port: copper 介面 IDS port, 或是設定成 HA port。
- MGMT port: 設備管理介面埠 (Management port)。

燈號	顏色	狀態	說明
	綠	亮	NetKeeper 系統啓動
FVK		滅	NetKeeper 系統關閉
eve	紅	亮	NetKeeper 系統進行程式讀取中
313		滅	NetKeeper 系統無進行程式讀取
FO		橙亮	連線埠成功連線到 1000Mbps
EU	綠橙	綠亮	連線埠成功連線到 100Mbps
~		滅	連線埠成功連線到 10Mbps
(10/100/1000)	綠	閃爍	連線埠正在傳送或接收封包
		滅	連線埠未連線
		橙亮	MGMT 埠成功連線到 1000Mbps
MGMT (10/100/1000)	綠橙	綠亮	MGMT 埠成功連線到 100Mbps
		滅	MGMT 埠成功連線到 10Mbps
	綠	閃爍	MGMT 埠正在傳送或接收封包
		滅	MGMT 埠為連線

圖表 5: NK6000 外觀燈號說明





2.2 安裝 NK6000 設備

說明 NK6000 設備的安裝到機架或是網路上的方式。

2.2.1 固定 NK6000 於標準 19"機架

NK6000 可以被固定在標準的 19 英时機櫃上。



圖表 6: NK6000 鎖上耳翼



2.2.2 連接電源

NK6000 的電源插座位於設備的背面,輸入電源電壓範圍為 100V - 240V。





2.3 設定基本參數

在對 NK6000 做安全政策設定之前,必須進入命令列模式設定 IP 位址。有兩種 方式可以連接 NK6000 設備與電腦主機 (PC):

(1). 超級終端機模式 (Hyper Terminal):

使用 Microsoft Windows XP/2000 內附之超級終端機程式,搭配使用原廠提供的 Console 線,連接電腦 (PC) 與 NK6000 的 RS-232 Console 埠。

(2). 遠端連線模式 (Remote Connected):

透過網路連線 NK6000 設備的管理介面埠 (MGMT port),使用具有 SSHv2 加密功 能之遠端連線軟體來連線。

2.3.1 超級終端機模式 (Hyper Terminal)

利用 Console 線連結 NK6000 的 console 埠與電腦主機的 serial 埠 (COM port)。 啓動 Microsoft Windows XP/2000 內建的終端機模擬程式,按下 Enter 鍵 即可進入 NK6000 設備的命令模式。終端機模擬程式的參數設定如下所示。



圖表 9: NK6000 連接 Console 埠

終端機模擬(Terminal Emulation)	VT-100, ANSI, or auto	
每秒傳輸位元(Bits Per Second)	57600	
資料位元(Data Bits)	8	
同步檢查(Parity)	None	
停止位元(Stop Bits)	1	
流量控制(Flow Control)	None	
圖表 10: 終端機模擬參數		

說明:在 Windows XP/2000 作業系統下啓動終端機模擬的步驟為:

開始

→程式集→附屬應用程式→通訊→超級終端機



2.3.2 網路遠端連線模式 (Remote Connected)

利用 UTP Cross-over 線 (對線),連結的管理介面埠 (MGMT port) 以及電腦主 機的網路卡,然後執行 SSHv2 遠端登入程式連線 NK6000 設備。



圖表 11: 連結 NK6000 MGMT 埠

2.3.3 登入命令列模式 (Command Line Interpreter)

當使用者透過超級終端機或 SSH 遠端登入程式連線至 NK6000 後,按下任意鍵後便會出現如下畫面。

login: admin Password: _			

圖表 12: 命令列模式登入畫面



說明:

- 1. NK6000預設的IP位址為: 192.168.168.221。
- 2. 預設登入的使用者名稱為 admin,密碼為 admin。

成功登入之後,即出現以下操作畫面。

< <u>S</u> >ystem <d>evice 0:</d>	3/09/06
NK6000 (c) 1999-2006 Broadweb Corp.	
Kernel 1.0.7; Sigature: 4.12	
Running 0 days 1 hours 25 mins; 2 user(s) logged on	
CPU Util.: 0%; Throughput: 0 Mbps; TCP connections: 0/512000	
Memory: 376,044 KB free, total 1,302,168 KB HD: 28,223 MB free, 5 GB used, total 34 GB	
IP: 192.168.10.1; Netmask: 255.255.0.0; Gateway: 192.168.1.1 HA: 192.168.10.2; DNS: 192.168.20.1; BEMS: 192.168.0.2	
TCP idle time limit: 20 seconds Maximum 1000 logs in 5 seconds	
< <u>S</u> >System < <u>D</u> >Device < <u>F1</u> >Help < <u>Esc</u> >Exit	16:10

圖表 13: 命令列模式畫面

2.3.4 設定 IP 位址 (IP Address) []

此功能為設定 NK6000 的網際網路地址。在 Device 功能選單中以方向鍵或快捷





統將再次詢問變更與否,按[▶]鍵確定變更 IP 位址;按[▶]鍵或[€]鍵則不變更, 預設爲不變更。

<s>ystem <d>evice</d></s>		03/08/06
Device IP Address: 192.	168.11.1	
Are y	you sure you want to change IP? (y/N)_	
		10:29

圖表 15: IP 位址 (IP Address) 再次確認變更

2.3.5 設定子網路遮罩 (Netmask) M

此功能爲設定NK6000的網路遮罩∘在Device功能選單中以方向鍵或快捷鍵

移動到此選項並按 鍵,即可執行此功能。此功能畫面如下:



圖表 16: 設定子網路遮罩 (Netmask) 畫面

執行時會顯示目前網路遮罩設定,直接輸入欲變更的網路遮罩再按



系統將再次詢問變更與否,按^Y鍵確定變更網路遮罩設定;按^N鍵或^{ES}鍵則不 變更,預設為不變更。

NK6000 使用手册

Device netmask: 255.255.25.0
Are you sure you want to change netmask? (y/N)_
10:32

圖表 17: 子網路遮罩 (Netmask) 再次確認變更

2.3.6 設定閘道器 (Gateway) 🕒

此功能爲設定 NK6000 經由那一個閘道器連接	至外部網路。在 Device 功能選單
中以方向鍵或快捷鍵 6 移動到此選項並按 - Enter]鍵,即可執行此功能。此功能畫
面如下:	
KS>ustem KD>evice	03/07/06



圖表 18: 設定閘道器 (Gateway) 畫面

執行時會顯示目前閘道器設定,直接輸入欲變更的閘道器網路位址再按



鍵,系統將再次詢問變更與否,按[▶]鍵確定變更閘道器設定;按[▶]鍵或[№]鍵則 不變更,預設為不變更。

NK6000 使用手册

KS>ystem <d>evice</d>	03/08/06
Device gateway: 192.168.1.123	
Are you sure you want to change gateway? (v/N)	
	10.00
	10:38

圖表 19: 閘道器 (Gateway) 再次確認變更

2.3.7 設定網域名稱伺服器 (DNS) 🖻

此功能為設定 NK6000 經由何者閘道器連接至外部網路。在 Device 功能	じ選單中
以方向鍵或快捷鍵 移動到此選項並按 - Enter 鍵,即可執行此功能。執行	亍時會顯
於目前網域名稱伺服器設定,直接輸入欲變更的網域名稱伺服器的網路位址報	再按
↔ Enter 鍵, 即可變更設定。若不變更設定則按 鍵取消並跳出。此功能畫	面如下:
<pre>System <d>evice 03/07/06</d></pre>	
Device DNS Server: 192.168.20.1_	
(Esc)Exit 19:69	

圖表 20: 設定網域名稱伺服器 (DNS) 畫面



2.3.8 設定 BEMS 伺服器 (BEMS Server) 🕒

此功能為設定 NK6000 歸屬於何者 BEMS Server 所管控。在 Device 功能選單中
以方向鍵或快捷鍵 移動到此選項並按
示目前 BEMS Server 的網路位址設定,直接輸入欲變更的 BEMS Server 網路位址再
按下 ······ 鍵,即可變更設定。若不變更設定則按 鍵取消並跳出。此功能畫面
如下:

<s>ystem <d>evice</d></s>	03/07/06
BEMS Server IP: 192.168.0.2_	
ZEgoNEuit	12.5/
NESC/EXIT	10:04

圖表 21: 設定 BEMS 伺服器 (BEMS Server) 畫面

2.3.9 設定虛擬網路編號 (VLAN ID) 💟

此功能為設定 NK6000 所屬的虛擬網路編號。在 Device 功能選單中以方向鍵或

V		
快捷鍵 移動到此選項並按	 ,即可執行此功能	。此功能畫面如下:



≪S>ystem <d>evice</d>	03/07/06
VLAN ID: 0_	
<u><esc>Exit</esc></u>	14:18

圖表 22: 設定虛擬網路編號 (VLAN ID) 畫面

執行時會顯示目前虛擬網路編號設定,直接輸入欲變更的虛擬網路編號再按下

< <mark>S</mark> >ystem < D >evice		03/08/06
VLAN ID: 1		
	Hre you sure you want to change vlan? (y/N)_	
		10:57

圖表 23: 虛擬網路編號 (VLAN ID) 再次確認變更

完成了上述 IP 位址相關的設定之後,就可以連結 NK6000 與 BEMS 伺服器,並 且進行進一步的網路安全防禦政策設定。

如果需要進一步瞭解命令列模式的指令內容,請參考第13章。



3 第三章 BEMS 與 Plug-in

本章說明

主要說明 BEMS Server 以及 Plug-in 程式的安裝步驟。

本章內容包含下列使用說明

章節	描述
3.1	客戶註冊及啓動密鑰 (A/K) 下載
3.2	BEMS 管理系統安裝步驟
3.3	NK6 管理模組安裝步驟

BEMS 管理系統 (BroadWeb Extensible Management System) 是威播科技 NetKeeper 系列與其他網路設備的統一管理平台。BEMS 具有集中管理與遠端監控的 功能,它建構了一個強固而有效率的主從式架構,可以快速地將互動性高且功能豐富 的管理介面佈署到客戶端主機,使得網路管理者可以經由網路連線,從遠端對系統中 的網路設備執行設定、監控、製作報表等管理工作。

BEMS 管理系統內建帳戶與權限管理、資料庫連線管理、網路設備連線管理、系統線上升級等等功能,並且可以加載管理模組來擴充系統功能。在 BEMS 管理系統上加載 NK6000 管理模組 (NK6 Plug-in) 之後,管理者便可以透過 BEMS 管理系統客戶端介面同時管理多達 10 台的 NK6000。以下將說明安裝與啓動 BEMS 管理系統的步驟。

BEMS 管理伺服器需安裝於以 Windows 2000/XP/2003 為作業系統的電腦主機上, BEMS 管理系統客戶端程式則可以在各種作業系統的電腦主機上執行,包括Windows, Unix/Linux, MacOS 等等。

3.1 註冊及啓動密鑰 (A/K) 下載

安裝 BEMS 管理伺服器時,安裝程式將會要求使用者輸入一組啓動密鑰 (A/K, Activation Key),如果您已經是威播科技的註冊客戶,您可以直接登入威播科技的註冊網站免費下載 BEMS 的啓動密鑰。如果您尚未成為威播科技的註冊客戶,請先連線 到威播科技網站,完成客戶註冊以及產品註冊手續。

- 可連結威播科技網站: <u>www.broadweb.com</u>,或是直接連線威播註冊網站: <u>my.broadweb.com</u>。
- 2. 第一次連線使用, 請先註冊成為一個新的客戶, 並按照網頁說明依序填寫客



戶資料。

3. 回覆客戶註冊確認信後,即可完成客戶註冊手續。

第二次連線到威播註冊網站,可直接輸入使用者名稱及密碼,登入後即可繼續完成產品註冊手續,或下載 BEMS 啓動密鑰。

說明:

- 登記成為威播科技的註冊客戶,是取得BEMS啓動密鑰的必需手續。啓動密鑰 內含的資訊即包含了客戶的註冊帳號,這使得BEMS管理系統可以依據使用者 所註冊的產品,從威播資料更新伺服器(DUC)獲得正確的遠端升級服務,遠端 升級服務包括了BEMS主程式、外掛管理模組、設備的核心程式,以及安全防 禦政策等軟體的升級。
- 2. 產品註冊不是取得BEMS啓動密鑰的必需手續,您可以在沒有註冊任何產品的 情況下,下載BEMS啓動密鑰。但是產品註冊是啓動該項產品軟體升級服務的 必需手續。完成產品註冊手續之後,您可以在威播註冊網站上看到您所註冊的 產品清單以及每項產品的軟體升級服務的開始與結束日期。

注意:

在安裝BEMS管理系統時,同一組啓動密鑰僅能被使用在一台電腦主機上,如果您 需要安裝BEMS管理系統在另一台電腦主機時,請再下載一組新的啓動密鑰。



圖表 24: 連線 my.broadweb.com



🖾 my.BroadWeb.com - Microsoft Internet Explorer	
🕞 上一頁 • 🕗 · 😣 🕝 🔾 🔍 搜尋 🏠 我的最爱 🎯 🚫 • 🌦 🗷 • 💟 🌘	👌 檔案E) 編輯E) 🕇 🦹 🥂
網址(D) 💽 http://my.broadweb.com/chinese/0_1_join.php	💌 🕢 移至 👘 👻
	<u>*</u>
B	
C BroadWeb Registration Server	w.broadweb.com.tw 🚯 English
全人 聯絡我们	
	01000010101010 0 101010
Registra	rimin (
Regis	tration
	Webles for our
◎ 我的基本資料	
語域寫下列表格:	
"爲必填欄位	
Login Information	
* 帳號: 查謝此帳號是否已有人使用	>>
* 密碼:	
★ 諸西葡えーカ家孫:	
Contact mormation	
*姓:	
* 4:	
* 八司 / 第位・	
* 公明 / 単位:	
地址:	
nt:	-
I 建理 - 00_contact.php 於 www.broadweb.com.tw	

圖表 25: 註冊帳號塡寫畫面

BroadWel	Regis	tration	Server		@ www.b	roadweb.cor	m 🚯 中交
Logout My Products	My Profile	Contact Us			gistra	ation	
Souther the second seco	S Ing tems.	<u>> Request</u>	BEMS A/K		Р	roduct Regis	tration
*Alias	Туре	Model	S/N	Registration Date	Expiration Date	Status	Action
副	表 26 [.]	正確輻	入容入帳	號/密碼	後之書	面	

3.2 BEMS 管理系統安裝與啓動

BEMS 管理系統運作需要安裝的程式分別有:

- 1. 安裝 JRE (Java Runtime Environment)。
- 2. 安裝 Database 資料庫程式 (例如: MySQL)。
- 3. 安裝 BEMS 管理伺服器主程式。

將原廠提供之光碟放入光碟機後,它將會自動的執行安裝程式。如果您的系統沒 有自動執行安裝程式的話,請在光碟機目錄所在地搜尋一個『BW-BEMS.exe』的檔



案,執行它可以進行 Product Registration、BEMS Server Installation、打開並讀取 Quick Installation Guide 檔案、User Guide 檔案等等功能。



圖表 27: 原廠光碟執行畫面

3.2.1 安裝 JRE (Java Runtime Environment)

因為 BEMS 是利用 Java 語言開發而成,執行 BEMS 程式時需要 Java Runtime Environment。在選單中選擇 JRE 連線至 <u>http://java.sun.com/downloads/</u> 下載最合適的版本(原廠建議使用 JRE 1.4.2),並跟著安裝步驟一項項完成即可。







圖表 28: JRE 程式下載及安裝範例

3.2.2 安裝資料庫程式 (如 MySQL)

當 NK6000 設備偵測到網路安全事件發生時,會傳送事件紀錄給 BEMS Server,此事件紀錄會被儲存在一個資料庫當中,即所安裝的 MySQL 資料庫,方便客戶查詢歷史事件。原廠建議安裝的版本為4.1.18。

在選單中選擇 MySQL 可連線至 <u>http://dev.mysql.com/</u>下載最適合的版本,以下 是 MySQL 資料庫程式 (v4.1.18) 的安裝步驟範例:



圖表 29: MySQL 程式安裝範例

關於 MySQL 安裝過程的詳細步驟,請參見附件一:安裝 MySQL。



3.2.3 安裝 BEMS Server 主程式

執行安裝光碟,並於圖中點選 『BEMS Server Installation』,安裝程式會直接安裝 BEMS Server 主程式,其步驟圖示如下:

■ 步驟一: 安裝 BEMS Server 主程式

在選單中選擇『BEMS Server Installation』後,開始安裝 BEMS Server 程式。

•	Installation of BENIS Server	×
B a d d a d d d d d d d d d d d d d d d	♥ Welcome to the installation of BEMS 1.1.11 The homepage is at: http://www.broadweb.com/	
(Made with IzPack - http://www.izforge.com/)	Next Qui	Ð

圖表 30: 安裝歡迎畫面

■ 步驟二:BEMS 啓動密鑰設定視窗

當使用者在威播註冊網站完成註冊程序後,便可在使用者的產品專屬網頁中,下 載 BEMS 啓動密鑰(A/K)。 啓動密鑰內含的資訊可以確保每一部 BEMS Server 能夠 從威播更新伺服器(DUC)獲得正確的遠端升級服務,遠端升級服務包括了 BEMS 主程 式,外掛程式,設備的核心程式,以及安全防禦政策等軟體的升級。因此,每一組 BEMS 啓動密鑰僅可被安裝在一台 BEMS Server 上。

請將此啓動密鑰塡入設定視窗中對應的欄位。



D	Installation of BENIS Server
	Activation Key
	An activation key is required to complete the BEMS installation. You can obtain an activation key at http://my.broadweb.com/. Please enter the activation key. A/K:
(Made with IzPack - ht	tp.//www.izforge.com/)

圖表 31: 輸入 A/K 畫面

注意:

每一組 BEMS 啓動密鑰僅可被安裝在一台 BEMS Server 上。若重複將相同 BEMS 啓動密鑰安裝在不同的 BEMS Server 上,會導致特徵碼無法更新。

■ 步驟三:系統參數設定視窗

請在系統參數設定視窗中輸入 BEMS Server 名稱、用途描述、管理伺服器與客戶端之間連線傳遞資料的服務埠 (預設為 8863)。

請輸入相關參數:

- 伺服器名稱:由使用者定義
- 說明:由使用者定義
- 服務埠:客戶端 (使用者利用瀏覽器) 遠端連線管理伺服器 (BEMS Server) 時的連線埠,原廠預設值為 TCP/8863,使用者可自行修改定義。



0	Installation of BEMS Server	
	System Parameters	
	1. The server name is used to distinguish this BEMS server from the other BEMS servers, in case there are more than one BEMS installations in your organization. You may give it any name. Server Name: BEMS Server 1	
	2. An optional, brief, description of this BEMS installation may be supplied. Description:	
BinedWeb/ Extensible Monogeneen System	3. Please enter the number of the port for communication between the BEMS Management Server and Management Clients. (Default port: 8863) Server Port: 8863	
(Made with IzPack - I	http://www.izforge.com/)	it)

圖表 32: 系統安裝參數畫面

■ 步驟四:資料庫參數設定視窗

BEMS Server 需要將系統設定與事件資料儲存於資料庫伺服器中。使用者在進行此項設定之前,請先確認資料庫伺服器已經安裝完畢並正常啓動,確認無誤後,請 在資料庫參數設定視窗中輸入資料庫伺服器 IP 位址、資料庫連線服務埠、資料庫名 稱、使用者名稱及密碼。請注意,系統將依據使用者的設定測試資料庫連線,唯有連 線測試成功,BEMS 安裝程式才會進入下一個步驟。

請輸入資料庫相關參數。

- 資料庫所在的 IP 位址:例如: 192.168.168.66,如資料庫程式位在本機,則 可以輸入 localhost。
- 資料庫連線埠:0代表使用資料庫預設值。(若在安裝 MySQL 的過程指定 MySQL 使用其標準連線埠對外服務,則此欄位請輸入 0)
- 資料庫名稱:由使用者自行定義 (建議保持預設値)。
- 資料庫使用者名稱:由使用者提供。
- 資料庫使用者密碼:由使用者提供。

說明:

若是第一次安裝, 資料庫使用者名稱 請輸入 root 資料庫密碼請輸入當初安裝 MySQL 資料庫時,為 root 帳號所設定的密碼。




0	(Installation of BEMS Server)		
	Database Settings		
TO PAR	1. Please enter the IP address (or host name) of the database server.		
NIC	Database Server: localhost		
	Please enter the number of the port used to connect to the database server. Enter 0 to use the default port.		
1 miles	Database Port: 0		
S	3. Please enter the database name.		
1 teres	Database Name: bems		
BroadWeep	4. Please enter the user name used to connect to the database.		
Extensible	User Name: root		
Managerment System	5. Please enter the password used to connect to the database. Password:		
(Made with IzPack - http://www.izforge.com/)			
	Previous S Next S Q	ait)	

圖表 33: 資料庫 (如: MySQL) 參數畫面

■ 步驟五:管理者帳號設定視窗

請在管理者帳號設定視窗中輸入 BEMS 管理者的登入名稱,密碼,郵件位址, 以及關於此管理者帳號的備註說明。 登入名稱至少要有1個位元,且密碼長度至少 需要5個位元。輸入郵件位址的目的,是一旦 BEMS 系統發生了異常,將會把相關 訊息利用郵件寄送方式通知管理者。

0	Installation of BEMS Server		
	Administrator Settings		
	Please set up the user account for system administrator.		
	1. Please enter the login name for system administrator to login BEMS. You		
	can always change it later.		
	Login Name: admin		
	2. Please enter the password for system administrator to login BEMS.		
N	Password:		
A second	Retype password:		
· · · · · ·	2 Places anter the amail addrace of the system administrator		
BroadWeb	S. Tiease enter the entail autoress of the system automistrator.		
Extensible	Email Address.		
Management	4. More information about the system administrator may be supplied here.		
System	Description		
(Made with IzPack - http://www.izforge.com/)			
	G Previous 🕞 Next 😣 Qu	uit)	

圖表 34: 管理者設定視窗

■ 步驟六:遠端升級設定

BEMS Server 支援遠端升級,升級設定視窗係用以設定系統自動升級功能。當自動升級功能啓動時,BEMS Server 每天都會定時自動與威播更新伺服器連線,依據使用者的更新權限,檢查並且下載系統所使用的各項軟體,包括 BEMS Server 本身程式與相關函式庫,BEMS 外掛程式,IPS 設備的核心程式以及攻擊辨識碼等等。建議



您選擇啓動自動升級功能,以確保系統隨時擁有最新的攻擊防禦工事。 請輸入遠端升級(Update)參數設定。

- 是否啓動自動遠端升級:預設値為啓動。
- 遠端升級網站: 預設是 duc.broadweb.com
- 升級時程:預設每天凌晨4點開始進行連線,使用者可以自行調整。

0	Installation of BEMS Server	
	Update Settings	
SIL	If the auto-update function is enabled, the BEMS server will automatically download the update files and install them according to the specified schedule.	
	1. Do you want to enable the auto-update function?	
	O No	
	2. Please enter the IP address (or host name) of the update server.	
	Update Server: duc.broadweb.com	
BroadWeb/ Extensible	3. Please select an update schedule. (0 - 23) Update Schedule: 4	
Managerment Sveterm		
(Made with IzPack - http://ww	w.izforge.com/)	uit

圖表 35: 設定遠端連線線上更新的參數畫面

■ 步驟七:HTTP Server 參數設定視窗

BEMS Server 透過 HTTP Server 將管理系統客戶端的程式傳送到客戶端的電腦 中來執行。您可以在 HTTP Server 參數設定視窗中設定是否使用內建 HTTP Server (建議使用),以及 HTTP Server 的通訊埠 (預設為 80 埠)。如果 BEMS Server 上已 經安裝有其他 HTTP Server 軟體如 IIS 或 Apache,可選擇關閉不啓用內建的 HTTP Server, 並修改相關的路徑設定。

BEMS Server 安裝完成並正常啓動之後,使用者可以透過瀏覽器程式 (如 Internet Explorer),於網址列中鍵入 <u>http://<bems server IP address>/bems/</u>即可進入 BEMS 管理系統客戶端首頁畫面。



V	Installation of BENIS Server	
	HTTP Server Settings	
	The HTTP sever is needed for the system to deliver the Management Client program to the client side. You may choose to use the HTTP server built into the BEMS server or an alternative HTTP server.	
	1. Do you want to enable the built-in HTTP server?	
1.2	⊙ No	
/	2. Please specify the port number for the built-in HTTP sever.	
	HTTP Server Port: 80	
	 Please specify the root directory of the web documents. This is only needed if the built-in HTTP server is disabled. 	
BroadWeb	Root Directory: C:/Program Files/Apache Group/Apache2/htdocs/	
Extensible Management	Please enter the name of the subdirectory that is to contain the BEMS client files.	
System	Subdirectory: berns/	
(Made with IzPack - http:	n //www.izforge.com/)	
Andreas and the done may	G Previous Pext)	Quit

圖表 36: HTTP Server 參數設定視窗

■ 步驟八:Email 參數設定視窗

BEMS 管理系統有多項功能需要使用 Email 及時將適當的資訊傳送予相關人員, 如登入密碼提示、定期統計報表、系統硬碟空間不足的警示等等,只有當 Email 參數 被正確設定之後,這些功能才能正常操作。請在 Email 參數設定視窗設定 SMTP 郵件 伺服器位址及寄送郵件所使用的帳號 (Email sender) 及密碼(Sender password),如 果您所使用的 SMTP 郵件伺服器不需檢查密碼,則密碼欄位可以省略。

請輸入郵件(Email)參數設定。

- 是否啓動郵件服務:預設値為啓動。
- 郵件伺服器: 請輸入郵件伺服器 IP 位址或名稱,如 mail.broadweb.com。
- 寄件人: 請輸入用來發送郵件的帳號。
- 寄件人密碼:請輸入寄件人密碼。如果所設定的郵件伺服器不需認證,則此 欄位可以略過不填。



0	Installation of BEMS Server
	Email Settings
SE	Many system services in BEMS depends on email, such as password-recovery, alert-by-email, report-by-email, etc. To enable email-related services, please supply the following information.
	1. Do you want to enable email-related services? Ves No
	2. Please enter the IP address (or host name) of the SMTP server SMTP server mail broadweb.com
1	3. Please enter the account used for sending emails.
BroadWeb/	Email Sender: BEMS
Extensitie Management	 Please enter the password of the sender's account. It is needed only if sender authentication is required.
System	Password: Retype password:
(Made with IzPack -	http://www.izforge.com/)

圖表 37: 傳送訊息所需的電子郵件參數設定

■ 步驟九:Syslog 參數設定視窗

BEMS Server 可以將系統事件或是網路安全事件以威播特定格式(BroadWeb Syslog Format)傳送到使用者指定的 Syslog 伺服器。請在 Syslog 參數設定視窗中塡 入指定的 Syslog 伺服器的 IP 位址, Syslog Facility 的辨識碼,以及分別為不同程度 等級的資料 (INFO、WARN 及 ERROR),各依使用者需要輸入適當儲存日期長短。 請輸入 syslog 相關參數。

- Syslog 伺服器: 請輸入 syslog 伺服器所在,如在本機可輸入 localhost。
- Syslog Facility: 配合 syslog 伺服器於儲存檔時的辨識參數。
- 保存期限:區分三種等級,不同等級各有不同儲存期限。
 - 訊息(INFO)等級:預設於資料庫中儲存7天。
 - 警告(WARN)等級:預設於資料庫中儲存30天。
 - 錯誤(ERROR)等級:預設於資料庫中儲存30天。







圖表 38: Syslog 相關參數設定畫面。

■ 步驟十:DNSLookup 設定視窗

BEMS Server 提供主機名稱與 IP 位址的轉譯功能(DNS Lookup)。 安裝時需要 輸入 DNS 伺服器的所在。 此功能可以提供製作報表時的方便性,讓使用者可以直 接於報表當中讀取到主機名稱資料,而非只是 IP 位址。

請注意, 啓動此功能可能會對 BEMS Server 的效能有些微影響。

0	Installation of BENS Server	
TXX	DNSLookup Settings	
	DNSLookup is a BEMS service by which the plug-ins are able to resolve an IP address to its host name or vice versa.	
	 Do you want to enable the DNSLookup service? Yes 	
	O No	
× • • • • •	 Please enter the IP address (or host name) of the DNS server. Default DNS server will be used if no DNS server is specified here. 	
1 Acres	DNS Server:	
BroadWeb	3. Please select the maximum number of entries in the DNS cache. DNS Cache Size: 8000 •	
Management	4. Please select the time after which a DNS cache entry will be refreshed. DNS Refresh Interval : 6 hours	
System	5. Please select the time after which an unused chace entry will be removed. DNS Cache Max Age : 1 month	
(Made with IzPack - http://w	ww.izforge.com/)	
	G Previous Next 😣	Quit

圖表 39: DNSLookup 參數設定視窗

■ 步驟十一:登入嘗試鎖定設定視窗

為避免 BEMS 管理系統用戶帳號被不法之徒以嘗試錯誤的方式,猜出用戶登入密碼,您可以啓動登入嘗試鎖定(Login Retry Lockout)的功能來提升系統的安全性。一但啓動這項功能,除系統管理員以外的任何用戶帳號,如果登入密碼連續輸入錯誤達設定上限時,系統就會鎖定這個用戶帳號並拒絕其登入,直到系統管理員在管理系統



中為用戶帳號解除設定。

ww.broadweb.com

BroadWeb

0	Installation of BEMS Server	×
	Login Retry Lockout Settings	
	When the Login Retry Lockout function is enabled, the system will lockout a user account after a configured number of unsuccessful attempts by the user to log in.	
	 Do you want to enable the Login Retry Lockout function? Yes 	
	O No	
	2. Please select the number of unsuccessful login attempts allowed before	
BroadWeb Extensible Management System	the user account lockout. Login Retry Allowed : 3	
(Made with IzPack - http://v	www.izforge.com/))

圖表 40: 登入嘗試鎖定設定視窗

■ 步驟十二:指定 BEMS Server 安裝目錄。 請選擇程式安裝目錄所在。

0	Installation of BEMS Server	
Bratives Exert Sister	Select the installation path: C/Program Files/BEMS	Browse)
(Made with IzPack -	http://www.izforge.com/)	Previous 🕞 Next 😣 Quit

圖表 41: 安裝目錄選擇畫面

■ 步驟十三:選擇需要安裝的程式(全部選取)。



•	Installation of BEMS Server	
	Select the packs you want to install: Ote: greyed out packs are required.	
SE	Core	1.85 MB 5.88 MB
BroadWet Extensible Manageme Svetem	Description The BEMS core and configuration files.	
	Total space Required: Available space:	7.73 MB > 2 GB
(Made with IzPa	ack - http://www.izforge.com/)	😧 Next 😡 Quit

圖表 42: 需要安裝的程式 (Core 以及 Library)

■ 步驟十四:安裝程式完成。

•	Installation of BEMS Server	X
B as the second se	Pack installation progress:	
(Made with IzPack -	http://www.izforge.com/))

圖表 43: 程式安裝完畢畫面

■ 步驟十五:建立捷徑。



0	Installation of BEMS	Server	
	Select a Program Group for the Shortcuts:		
NJL .	Accessories		
	BroadWeb	avaata abartaut fax	
	Startup	create shortcut for	
	WinRAR	 current user 	
	Wisdom-soft ScreenHunter	🔘 all users	
BrandWeb.	BroadWeb	Reset	
Management System	▼ Create shortcut on the desktop		
(Made with IzPack -	http://www.izforge.com/)	Previous 🖓 🖓 Next 😡 G	auit

圖表 44: 建立捷徑

■ 步驟十六:安裝完成,請重新開啓電腦主機。

W Installation has completed successfully. Installation has completed su	0	Installation of BEMS Server	
	(Made with IzPack- http://www.izforge.com	 Installation has completed successfully. An uninstaller program has been created in: C:\Program Files\BEMS\Uninstaller 	€ Done

圖表 45: 全部程式安裝完畢畫面。

3.2.4 啓動 BEMS Server 程式

有兩種方式可以啓動 BEMS Server: 一是把啓動 BEMS Server 安裝成系統服務,執行 C:\Program Files\BEMS\InstallService.bat,執行後在服務內項目會增加一個 BEMS 的服務。如下圖所示:



松田市 宿案(E) 執行(A) ←→ Ⅲ ピ							11
喻服務(本機)	◎ 服務(本後)	- 19-					
	BEMS	名稱人	描述	狀態	啓動類型	登入身分	
	停止服務 重新智動服務 描述:	Selecter Application Layer G Application Manage Automatic Updates Background Intellig	通知道取的使用者及電腦系統管理警示 提供網際網路進線共用和網際網路連線 提供指派、發行、以及移称的軟體安裝 幣用重要 Windows 更新的下載员安裝 使用間圈的網路頻寬不得輸資料。	己智動	手動 手動動 動動 動	Local Serv Local Serv 本機系統 本機系統 本機系統	
	BroadWeb Extensible Management System	ClipBook ClipBook COM+ Event System	ExoadWeb Extensible Management System 智用剪贴薄帧碳器以儲存資訊並與遠端 支援「系统事件通知服務 (SEN5)」,它 管理 COM+ 元件的設定及追蹤。如果	已啓動 已啓動	自動 手動 自動 手動	本機系統 本機系統 本機系統 本機系統	
	↓延伸 √標準 /			-		_	

圖表 46: 啓動 BEMS Server 安裝成系統服務

此方式設定於每次電腦主機重新開機後均可自動啓動 BEMS Server 系統。

另外一種啓動方式是使用者手動執行,於 MS-DOS 模式下手動執行 C:\>Program Files\BEMS.bat。執行後如圖所示:

🔨 BEMS	- 🗆 ×
wrapper > Wrapper Started as Console	·
wrapper Launching a JUM	
jvm 1 Wrapper (Version 3.1.2) http://wrapper.tanukisoftware.org	
jum 1 l	<u> </u>
jvm 1 INFO [Thread-0] - ##################################	
jvm 1 🚦 INFO [Thread-0] – 🛛 BEMS started.	
jum 1 🕴 INFO [Thread-0] - Host MAC: 00-20-E0-97-3C-B8	
jvm 1 🛛 INFO [Thread-0] – [syslog.event.license_loaded] License [syst	eml is
loaded.	
jvm 1 🛛 + INFO [Thread-0] - [syslog.event.license_loaded] License [eule	en_group
l is loaded.	
jvm 1 🛛 DEBUG [Thread-0] – java.version = 1.5.0_02	
jvm 1 🛛 DEBUG [Thread-0] – java.vendor = Sun Microsystems Inc.	
jvm 1 🛛 DEBUG [Thread-0] – os.name = Windows XP	
jvm 1	ation.j
ar;lib/bjl.jar;lib/bnl.jar;lib/comm.jar;lib/connector-j.jar;lib/foxtrot.j	jar;lib/
ftp.jar;lib/itext.jar;lib/jcalendar.jar;lib/jcommon.jar;lib/jetty.jar;lib	jfreec
hart.jar;lib/jSMSEngine.jar;lib/log4j.jar;lib/mail.jar;lib/prevayler.jar;	lib/ski
nlf.jar;lib/systray4j.jar;lib/TableLayout.jar;lib/wrapper.jar	
jvm 1 🛛 DEBUG [Thread-0] – bems.version = 1.1-b2	
jvm 1 DEBUG [Thread-0] – bems.home = C:/Program Files/BEMS	
jvm 1 🛛 DEBUG [Thread-0] – bems.server_name = BEMS Server 1	
jvm 1	
jvm 1	
jvm 1 ¦ DEBUG [Thread-0] – bems.server_ip =	
jvm 1 DEBUG [Thread-0] – bems.ipv6_enabled = false	
jvm 1	
jvm 1 DEBUG [Thread-0] - bems.scheduled_update_enabled = true	
jvm 1 DEBUG [Thread-0] - bems.update_server = duc.broadweb.com	•

圖表 47: 於 MS-DOS 模式下手動執行

此方式設定於每次電腦主機重新開機後,均需由使用者手動執行,方能啓動 BEMS Server 系統。

BEMS Server 啓動之後,使用者就利用電腦主機連線進行遠端操作,以下章節將 說明操作詳細步驟。

3.3 安裝 NK6 外掛程式

搭配 NK6 外掛程式後,BEMS 管理系統即可具有 NK 6000 管理功能,並可同時 控管多達 10 台的 NK 6000 設備。



EN 98% 🔍 🖛 🔿 🖑 🥥 🖉 🕅 🖗 🖉 🔀 3:50 PM



4 第四章 BEMS Admin Console

本章說明

主要說明 BEMS Admin Console 操作步驟。

本章內容包含下列使用說明

🛃 start 👘 🧭 😂 🐚 🔾 🔮 🚳 🖉 BEMS

章節	描述
4.1	登入 Admin Console
4.2	系統 (System)
4.3	使用者 (User)
4.4	設備 (Device)
4.5	記錄 (Log)

BEMS Server 啓動後,使用者可將需要控管的 NK6000 設備增加到設備管理清 單當中以方便遠端管理。以下將說明 Admin Console 操作指令及相關參數。

4.1 登入 Admin Console

於執行 BEMS Server 電腦主機的作業系統螢幕下方工具列中會出現 Admin Console 的圖示(¹⁰),利用滑鼠雙擊之後可以登入 Admin Console 設定相關參數。

2	BE	MS Admin Console		
	$\overline{\mathcal{D}}$	User Name		
		Password		
		0⊶ Forget your p	assword?	

圖表 49: BEMS Admin Console 登入畫面

輸入名稱/使用者密碼後,可打開 BEMS Admin Console 的操作介面。共有四個



參數頁面,分別是 System(系統) / User(使用者) / Device(設備) / Log(紀錄),以下會分別說明。

說明:

- 1. 預設的登入名稱 / 登入密碼為: admin / admin
- 2. 若使用者忘記密碼,利用滑鼠點選『Forget your password?』,系統將利用 E-mail 寄送登入名稱/密碼到使用者的 E-mail 信箱。

4.2 系統 (System)

系統資訊 (System Info),紀錄 BEMS 系統相關訊息,包括版本,啓動時間,IP 位址,MAC 位址,已連線 BEMS 的設備數量,連線的使用者人數!

Memory Monitor,顯示此 BEMS Server 主機中記憶體 (memory) 使用情形。 服務資訊 (Service Info),紀錄 BEMS Server 系統所提供及正在運作的服務,例 如: TCPLogServer, UDPLogServer...等等。藍色球表示該服務正常啓動執行中,紅

色球表示此服務目前並無啓動執行。

Plug-in 資訊 (Plug-in Info),紀錄搭載在 BEMS Server 上的 Plug-in 程式,相對 應的 Plug-in 可以控管不同的設備,例如 NK Plug-in 可以用來控管 NK3000P, NK6 Plug-in 可控管 NK6000 ...等。

			BEMS Admin Cor	sole 🦯 🧕	0
4	e 🗶 🍫				
Sy:	stem 🦓 User 🎯	Device 🙀	Log		
Syste Syste IP Ad Onlin	m Info em Version: 1.1-b2 Idress: 192.16 ne Device(s): 1	8.80.246	System Uptime: MAC Address: Online User(s):	0 Day(s) 02:00:35 00-20-E0-97-3C-B8 1	
Servio	ce Info			17777K.wed	
No.	Service Name	Status	1	Remark	_
1	TCPLogServer	۲	TCP log receiv	ed: O	
2	UDPLogServer	۲	UDP log receiv	ed: O	-
3	SNMPTrapReceiver	۲	SNMP trap rece	eived: 0	
4	Poller	۲	Polling count: 3	161	
5	SMTPSender	۲	E-mail(s) sent	0	
6	SMS	0	Short Message	(s) sent: 0, received: 0	
7	DNSLookup	0	Host(s) to look	up: 0, Last lookup time:	
8	UpdateScheduler	۲	Last access:	, Last update:	
Plug-	in Info				
No.	Plug-in Name	Version	Type	Description	_
1	NetKeeperV6	0.4	0x12	NetKeeper V6 Plugin	_
2	eulen_group	0.3	0x52	Eulen Group Plugin	
3	eulen	0.3	0x51	Eulen Plugin	
					_

圖表 50: BEMS Admin Console 畫面



4.2.1 產品註冊 (Product Registration) 🙆

移動滑鼠游標點選工具列中 (Product registration),系統會透過網際網路連結到 威播科技產品註冊網站 (my.broadweb.com),可以進行註冊手續。

4.2.2 安裝 Plug-in (Load Plug-in from DUC) 🛃

BEMS Server 提供了設備管控的作業平台環境,而要完整控管設備的功能,則需要相對應的 Plug-in 程式來處理。對應控管威播網路安全系列產品所需要的 Plug-in 程式,均可以透過網際網路連線更新方式取得。

移動滑鼠點選工具列中 (Load Plug-in from DUC),BEMS Server 會透過網際網路連線到原廠的升級網站 (DUC: Data Update Center),並且自動判斷有該網站上有哪一些更新可以供下載使用。



圖表 51: 更新網站上有 netkeeper plug-in 可供下載使用。

4.2.3 刪除 Plug-in (Unload Plug-in) 😹

此功能用來刪除已經安裝的 Plug-in。請於 Plug-in Info 欄位中,點選所需要被刪除的 plug-in 名稱,按下工具列中 『刪除 Plug-in (Unload Plug-in)』即可刪除。

4.2.4 檢查升級 (Check for Update) 🐼

此功能用來檢查原廠升級網站 (DUC)上的更新資料。按下按鍵之後,系統會透過 網際網路連線回原廠的升級網站 (DUC),檢查並顯示所有可下載更新的資料,可更新 下載的包括新版本的 Plug-in 以及最新版的防禦政策等等資料。



4.3 使用者 (User)

BEMS Server 系統提供多個使用者可以連線使用,並且提供不同使用者擁有不同的權限設定。預設一個系統登入使用者名稱為 admin,密碼為 admin,此使用者擁有所有的包括新增修改刪除其他使用者的權限。

在使用者 (User) 的畫面中,可以選擇依個別使用者 (User View) 或是群組使用者 (Group View) 的方式顯示,請參考下列圖示。

•	BE	MS Admin Console	000
۲			
🚇 System 🦓 User 🞯 [Device 💕	Log	
	0	Iser View OGroup View	
No. User Name	Status	Description	
1 12345	Å		
2 admin	2	System Administrator	
2			

圖表 52: 個別使用者畫面。

•		BEMS	S Admin Console	00
	÷ 🗶 🖊			
🧐 s	ystem Kser 🍙	Device 🙀	Log	
		OUs	er View 🥑 Group View	
No.	Group Name	Members	Description	
1	admin group	2	System Administrators	

圖表 53: 群組使用者畫面。

4.3.1 新增群組使用者 (Insert user group) 🐏

按下新增群組 (Insert user group) 按鍵後,系統會出現設定畫面,如圖所示。

oadWeb www.broad	web.com	
	W	User Group Profile
	Group Name:	Read Group
	Description.	
	Privilege:	

圖表 54: 群組使用者概況 (User Group Profile)

Cancel

- 群組名稱 (Group Name):由使用者自行定義。
- 說明 (Description):由使用者自行加註此群組的說明。

OK

- 權限 (Privilege):定義此群組使用者的權限。當游標點選到該視窗,系統會 自動彈出權限選擇視窗可供點選!
 - ◆ Admin: 設定該群組擁有登入 Admin Console 的權限與否,包括下載 Plug-in, 啓動/關閉 BEMS 的服務,新增/刪除/修改管理設備,新增/刪 除/修改使用者(群組)帳號,以及刪除系統記錄的權限。
 - ◆ Config: 設定該群組擁有被管理的硬體設備的設定 (config) 權限與 否,除了區分為設備種類之外,更可以區分到同類的的設備當中,單一 設備的設定 (config) 權限與否。
 - ◆ View: 設定該群組擁有被管理的硬體設備的察看 (view) 權限與否,除 了區分爲設備種類之外,更可以區分到同類的的設備當中,單一設備的 察看 (view) 權限與否。

NK6000 使用手册

0



•			Privile	ge Editor			0
Admin	Config	View					
MAII	owed to	login Admi	n Console.				
All	owed to	download/	delete BEM	S plug-ins.			
Allı	owed to	start/stop E	BEMS servio	es.			
Allı	owed to	insert/rem	ove/modify (users.			
Allı	owed to	insert/rem	ove/modify (user group:	8.		
Allı	owed to	insert/rem	ove/modify (devices.			
Allı	owed to	delete sys	logs.				
			OK		Cancel		

圖表 55: Admin 權限設定畫面。

	Privilege Editor	
dmin Config View		
Allowed to configure all	devices;	
Allowed to configure all de	evices of the selected device ty	/pes:
Available device types:	Cho	osen device types:
NetKeeper V6	>	
Allowed to configure the s	elected devices:	
Available devices:	Cho	osen devices:
Fake NK6 (1.1.1.1)		
	>>	
	. << .	
	OK Cance	

圖表 56: Config 權限設定畫面。



0	Privilege Editor		0
Admin Config View			
Allowed to view all device	es	types:	
Available device types:		Choosen device types:	
NetKeeper V6	>>		
Allowed to view the selecter Available devices:	d devices:	Choosen devices:	
Fake NK6 (1.1.1.1)			
	0К (Cancel	

圖表 57: View 權限設定畫面。

4.3.2 刪除群組使用者 (Remove user group) 😹

需要刪除不用的群組時,使用者選擇群組名稱之後,按下工具列中刪除群組使用者 (remove user group)的按鍵後確認即可。

4.3.3 修改群組使用者 (Modify user group) 🜌

需要修改群組時,使用者選擇群組名稱之後,按下工具列中修改群組使用者 (modify user group)的按鍵後確認即可。

4.3.4 新增個別使用者 (Insert user) 🛃

按下新增個別使用者 (Insert user) 按鍵後,系統會出現設定畫面,如圖所示。



•	User Profile	0
User Name:	Test User	
Password:	*****	
E-mail:		
GSM Number:		
Group:	Read Group	
Description:		
-		
:	OK Cancel	

圖表 58: 新增使用者操作畫面

- 使用者名稱 (User Name): 由使用者自行定義。
- 密碼 (Password): 由使用者自行定義。
- 郵件地址 (E-mail): 由使用者自行定義。
- GSM 號碼 (GSM Number): 請使用者自行輸入。
- 群組 (Group): 請選擇此帳號使用者所屬的群組, 群組的定義方式, 請參考
 4.3.1 的說明。
- 說明 (Description): 該使用者的說明,請自行定義。

4.3.5 刪除個別使用者 (Remove user) 😹

需要刪除不用的使用者時,使用者選擇使用者名稱之後,按下工具列中刪除個別 使用者 (remove user)的按鍵後確認即可。

4.3.6 修改個別使用者 (Modify user) 🜌

需要修改使用者時,使用者選擇使用者名稱之後,按下工具列中修改使用者 (modify user)的按鍵後確認即可。



4.4 設備 (Device)

BEMS Server 提供了可以同時控管多台 NK6000 設備的軟體作業平台,受控管的設備均會顯示於設備 (Device) 畫面當中。在開始管理 NK6000 設備前,使用者請先把該設備加入到清單當中,完成後才能夠進行遠端管理,安全防禦政策設定,報表產出等等或是其他作業。

9		в	EMS Admin Console		
•	* * /				
0	System 🆧 Us	er 📝 Device 🕵 L	og		
			Table View OTree	View	
No.	Name	IP Address 🗠	Type	Status	Description
No. 1	Name E_Group	IP Address	Type Eulen Group	Status	Description
No. 1 2	Name E_Group Fake NK6	IP Address	Type Eulen Group NetKeeper V6	Status	Description
No. 1 2 3	Name E_Group Fake NK6 EPro_39	IP Address 0.0.0.0 1.1.1.1 192.168.168.39	Type Eulen Group NetKeeper V6 Eulen Pro	Status	Description

圖表 59: 設備清單圖示(表格模式)

- 表格模式 (Table View): 利用表格模式顯示設備清單。
- 樹狀模式 (Tree View): 利用樹狀模式,顯示設備清單。



圖表 60: 設備清單圖示(樹狀模式)

4.4.1 增加設備 (Insert device) 🐏

請利用滑鼠游標切換畫面到 device 的控制頁面底下,點選上方工具列中 (Insert device),可加入新設備。相關欄位說明如下:

- 設備名稱 (Device Name): 使用者自行定義。
- IP 位址 (IP): 該設備的 IP 位址 (ip address)。
- 類別 (Type): 該設備的類別,例如 NetKeeper, NetKeeper V6 等等。
- 根源 (Parent): 管理該設備的上層單位,例如若選擇 『BEMS Server (192.168.80.246)』,代表該設備被 IP 位址為 192.168.80.246 的 BEMS Server 所管理。
- 說明 (Description): 描述該設備的說明,內容為由使用者自行定義。



Device Name:	NetKeeper 6000		
IP:	192.168.168.222		
Туре:	NetKeeper V6		-
Parent:	BEMS Server (192.	168.80.246)	-
Description:			
		Cancel	-

圖表 61: 新增設備圖

4.4.2 刪除設備 (Remove device) 😹

需要刪除設備時,使用者選擇該設備名稱之後,按下工具列中刪除設備 (remove device) 的按鍵後確認即可。

4.4.3 修改設備 (Modify device) 🜌

需要修改設備時,使用者選擇設備名稱之後,按下工具列中修改設備 (modify device) 的按鍵後確認即可。

4.5 記錄 (Log)

此頁面記錄 BEMS 伺服器系統執行運作或是設定更改等等的事件記錄,清楚記錄事件發生的時間,事件發生的動作操作者,以及說明該事件的訊息。



		В	EMS Admin Console	
)	\$ 💊	£		
🞱 Sy	stem 🤞	😫 User 🖪 Device 🛛	🛃 Log	
No.	Туре	Date / Time	Source	Mess
1	i	2005-10-06 14:28:08	User Manager	User admin (ID: 1) login Admin Console
2	i	2005-10-06 14:21:21	User Manager	User admin (ID: 1) logout Admin Conso
3	i	2005-10-06 14:21:13	UserManager	User Test User (ID: 3) is added to the s
4	i	2005-10-06 14:20:35	User Manager	User group Read Group (ID: 2) profile is
5	i	2005-10-06 14:19:46	UserManager	User group Read Group (ID: 2) is added
6	i	2005-10-06 14:12:00	User Manager	User admin (ID: 1) login Admin Console
7	i	2005-10-06 14:11:19	Main	Network connection resumed. Host IP =
8	i	2005-10-06 14:11:13	Main	Service UpdateScheduler started.
9	i	2005-10-06 14:11:10	Main	The client files were deployed.
10	8	2005-10-06 14:11:09	Main	Failed to load plug-in eulen_group.jar b
11	i	2005-10-06 14:11:08	Main	Plug-in NetKeeperV6 (ver. 0.4) is loaded
12	i	2005-10-06 14:11:03	Main	Plug-in eulen (ver. 0.3) is unloaded.
13	i	2005-10-06 14:11:03	Main	Service DNSLookup started.
14	i	2005-10-06 14:11:03	Main	Service Poller started.
15	i	2005-10-06 14:11:03	Main	Service SNMPTrapReceiver started.
16	i	2005-10-06 14:11:03	Main	Service UDPL ogServer started

圖表 62: 紀錄顯示畫面

4.5.1 删除所有系統記錄 (Delete all system logs) 😹

按下工具列按鍵,確定之後系統將清除所有系統記錄。

4.5.2 儲存記錄成檔案 (Save system logs to file) 🛐

按下工具列按鍵後,系統會把系統記錄存成檔案,並且儲存到電腦主機當中。

4.5.3 篩選系統記錄 (Filter system logs) 🔳

此頁面記錄 BEMS Server 系統執行運作或是設定更改等等的事件記錄,清楚記錄事件發生的時間,事件發生的動作操作者,以及說明該事件的訊息

•	Sy		0		
	✓Limit visible items to: Minimum severity level is: ○Where date is after: ○Where date is before	1000 CINFO 2006 / 01 / 04 2006 / 01 / 04	OWARN	CERROR	
	OK	Reset	Cancel		

圖表 63: 紀錄篩選畫面



5 第五章 NK6000 管理介面

本章說明

主要說明 NK6000 的管理介面操作步驟。

本章內容包含下列使用說明

章節	描述
5.1	登入 NK6000 管理介面
5.2	主要操作介面
5.3	修改登入密碼
5.4	NK6 Plugin 操作

BEMS Server 啓動之後,使用者可以利用網路瀏覽器 (如 Internet Explorer 6.0) 透過網路連線到 BEMS 管理系統,進行網路安全防禦控管等等步驟。以下章節將說明 如何運用 BEMS Server 與 Plug-in 的搭配,管理 IPS 的設備,建構安全的網路環境。

5.1 登入 BEMS 管理系統客戶端程式

打開瀏覽器 (如 Internet Explorer 6.0) 連線到 BEMS Server,下載完執行 java web start 之後輸入使用者名稱及密碼之後,即可開始控管操作!請注意因為 BEMS 系統是利用 Java 語言以及 Java 環境開發而成,所以使用者的電腦請先安裝 Java Runtime Environment (JRE),以免出現 Java 的警告訊息。

步驟說明如下:

 於瀏覽器網址列鍵入 <u>http://<BEMS Server IP Address>/bems/</u>,可以連接到 BEMS Server 的顯示首頁。





2 於 BEMS Server 首頁中央,點選 here 後可以打開管理系統的登入畫面。





圖表 65: 操作程式下載畫面

在第一次進入 BEMS 管理系統時,會先由伺服器下載所需要的 JAR 檔案到電腦 中,請等候系統自動連線安裝完成即可

1	登入BEMS管理系統	000
4	管理伺服器: 用戶名稱: 用戶密碼:	192.168.168.59
	登入	取消

圖表 66: 登入 BEMS 管理系統畫面

說明:

- 1. 系統自動驗証密碼名稱是否允許登入。
- 2. 系統使用者密碼於可於 Admin Console 介面修改。

5.2 主要操作介面

操作系統介面主要由左上、左下以及右方三個視窗所組成,分別顯示『設備管理 樹狀圖』、『設備資訊』以及『Plug-in 作業視窗』。

- 設備管理樹狀圖: BEMS 伺服器可以同時控管多台設備或是設備群組,會以 樹狀圖顯示。所有在 BEMS Admin Console 介面中所加進來的 IPS 設備均 會被顯示出來。
- 設備資訊:顯示使用者於設備管理樹狀途中所點選的設備資訊,包括了設備



型號名稱、IP 位址、狀態、設備開機時間以及其他相關訊息。

管理桌面: 為控管設備的主要作業視窗,當使用者於設備管理樹狀圖中點選 兩次想要控管的設備後,所選擇設備的控管畫面將會顯示於此。



圖表 67: 主操作畫面說明

5.3 修改登入密碼 🖌

控制主畫面中提供修改登入密碼功能,請利用滑鼠游標點選『更改密碼』按鍵,系統將跳出修改密碼對話視窗。正確輸入後按下『OK』鍵後即可生效。

V	更改	次用戶密碼		0
用戶名稱:		admin		
舊 密碼 :				
新密碼:				
確認新密碼:				
	0K	:	Cancel	:

圖表 68: 修改密碼畫面



5.4 NK6 Plugin 操作

於『設備管理樹狀圖』當中,利用滑鼠游標點選使用者想要控管的 NK6000 的設備圖示兩次後,於桌面將會出現選擇對應控制的畫面。上面有設備訊息 (Device Information)、物件設定 (Objects)、防禦政策 (Policy)、即時監測 (Monitor)、報表設定 (Report)、系統事件 (System log) 等六項主要功能。以下章節將一一說明相關內容。

÷.

•	BEMS管理系统智戶論	000
*		
BEMS Server 1 (192.168.168.243)	🐨 NK6 under test (192.168.168.205)	000
 BSST NK6 (192.168.40.117) Daniel (192.168.10.250) Jerry (192.168.10.55) NK6 under test (192.168.168.205) 	2018日8日、1919年23世 約3802世 周39年23時、1919年23世 末浜市91年 2011日	
	【設備訳息] 192.168.168.205 防爆軟洗粉床 4.004 子網路建築 255.255.0.0 VLAN ID: 不輕用 閉題(P: 192.168.168.295 內接硬製坊施 正常 DNS IP 位址: 192 168 4228 最大事件記録組録: 1000 重用	
	【設備禾純時間】 (設備禾純時間) 時面: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Talpei 日光前的時間: 不發用 設定時面/日光前的時間	
	{管理設定]- SNMP 確請批評名稱: public SNMP 可說可寫批評名稱: private	
	SNMP Trap 杜幹名籍: pinate 縮號 土法 1 HostGroup_1 2 HostGroup_2	
設備類別: Netkeeper 6000 設備型號: NK-6105 設備名額: NK6 under test		
IP位址: 192.168.168.205 設備秋館: 連線	腔镜: 國大計 SNMP 連続 國大計 SSH 連続 國大計 Ping Echo 要用	
管理的時間: 13日 22:34:36 核心程式版本: 1.0.12 備註:		

圖表 69: NK6 Plugin 畫面





本章說明

主要說明管理介面中關於 NK6000 的設備設定資訊。

本章內容包含下列使用說明

章節	描述
6.1	設備訊息 (Device Information)
6.2	連線埠設定 (Port Configuration)

6.1 設備訊息 (Device Information)

打開NK6 Plug-in之後第一個畫面是『設備資訊』(Device Information)。於設備資訊畫面上方工具列中有三個按鈕分別是:



儲存設定 (Synchronize configuration to device): 將同步修改過後的設定値 (object, rule...等等相關設定) 到設備中。按下此鈕,會出現如下提示等待 畫面;完成設定,會出現如下設定成功提示畫面。

•	訊息	0
A	系統參數已設定成功!	
	確定	
	圖表 71: 工具列按鍵	

■ 儲存除錯訊息 (Save debug information): 將設備除錯資訊存檔 (如圖表 72),可提供於設備異常時分析之用。



更新設定 (Notification of update): 選擇需要的更新選項,並按下確定 (OK) 鍵即可設定成功 (如圖表 73)。

)	儲石	7			
Save <u>I</u> n: 🔼	Administrator		-		8-8- 8-6- 8-6-
 eclipse jformdesi, looksdem skeletonp vplls vpumlpro, vpworksp. 	 Cookies gner ④ Favorites o △ My Documents ro ○ ssh ○ workspace o 「開始」功能表 ace ○ 桌面 				
File <u>N</u> ame: Files of Tyne:	Tar File (tar)				
r nes or Type.				儲存	取消

圖表 72: 儲存除錯資訊

0	更新設定	0
(預設制	防禦政策]	
OB	動更新防禦政策	
• 詞	問用戶,但不自動更新	
[核心和	程式]	\neg
08	動更新核心程式	
⊙ 詢	問用戶,但不自動更新	
	確定取消	

圖表 73: 更新設定選項

於設備資訊的操作畫面中,可細分為二個不同的子項目,分別是: 『設備設定』, 『連接埠設定』。『設備設定』畫面說明如下:

6.1.1 設備訊息

描述設備的基本資訊,如 IP、Subnet Mask、DNS、Pattern version 及最大的 Log 訊息總數等。



		NK6 under test (192.168.168.205)	
翻息 物件設定	防禦政策 即時監測 報表設定 系統事	件	
1 🔜 🔮	×		
1017 HE 1017			
Harre France			
·設備訊息)]
[設備訊息] [設備IP: ·	192.168.168.205		
(設備訊息) 設備IP: 子網路遮罩: :	192.168.168.205 255.255.0.0	防禦政策版本: 4.004 VLANID: 不智用	
(設備訊息) 設備IP: 子網路速罩: : 開道 IP: : :	192.168.168.205 255.255.0.0 192.168.168.254	防禦政策版本: 4.004 VLANID: 不容用 內建硬碳状態: 正常	

圖表 74: 設備訊息

6.1.2 設備系統時間

描述 NK6000 硬體設備的系統時間。如圖 75 所示。

ſ	[設備系統時間		
	時區:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei	
	日光節約時間:	不啓用	設定時區/日光節約時間
		ואנצירי	

圖表 75: 設備系統時間

按下『設定時區/日光節約時間』按鍵,會看到如圖表 76 的連續畫面,可以設定目前的時區,以及是否要開啓及設定日光節約時間。

時區	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei	
設定模式	以絕對日期設定 ▼	
時間調整:	30 30	
開始時間:	一月 • 1 • 0:00 •	
結束時間:	一月 🔻 1 💌 0:00 💌	
	確定取消	
時區:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei	
時區:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+07:00) Bangkok, Jakarta, Hanoi	
時區: 國際	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+07:00) Bangkok, Jakarta, Hanoi (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei	
時區: 國際用日光節約時間 設定模式:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+07:00) Bangkok, Jakarta, Hanoi (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+09:00) Tokyo, Osaka, Sapporo, Seoul, Yakutsk (CMT+09:20) Adalaide Dawing	
時區: 國際用日光節約時間 設定模式:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+07:00) Bangkok, Jakarta, Hanoi (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+09:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+109:30) Adelaide, Darwin (GMT+10:00) Brisbane, Canberra, Melbourne, Sydney, Hobart	
時區: ✓啓用日光節約時間 設定模式: 時間調整:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+07:00) Bangkok, Jakarta, Hanoi (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+09:00) Tokyo, Osaka, Sapporo, Seoul, Yakutsk (GMT+09:30) Adelaide, Darwin (GMT+10:00) Brisbane, Canberra, Melbourne, Sydney, Hobart (GMT+11:00) Magadan, Solomon Is., New Caledonia	
時區: ✓啓用日光節約時間 設定模式: 時間調整: 開始時間:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+07:00) Bangkok, Jakarta, Hanoi (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+09:00) Tokyo, Osaka, Sapporo, Seoul, Yakutsk (GMT+09:30) Adelaide, Darwin (GMT+10:00) Brisbane, Canberra, Melbourne, Sydney, Hobart (GMT+11:00) Magadan, Solomon Is., New Caledonia (GMT+12:00) Fiji, Kamchatka, Marshall Is., Wellington, Auckland (GMT+13:00) Nuku'alofa	
時區: ✓啓用日光節約時間 設定模式: 時間調整: 開始時間: 結束時間:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+07:00) Bangkok, Jakarta, Hanoi (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+09:00) Tokyo, Osaka, Sapporo, Seoul, Yakutsk (GMT+09:30) Adelaide, Darwin (GMT+10:00) Brisbane, Canberra, Melbourne, Sydney, Hobart (GMT+11:00) Magadan, Solomon Is., New Caledonia (GMT+12:00) Fiji, Kamchatka, Marshall Is., Wellington, Auckland (GMT+13:00) Nuku'alofa	
時區: ●聲用日光節約時間 設定模式: 時間調整: 開始時間: 結束時間:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+07:00) Bangkok, Jakarta, Hanoi (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei (GMT+09:00) Tokyo, Osaka, Sapporo, Seoul, Yakutsk (GMT+09:30) Adelaide, Darwin (GMT+10:00) Brisbane, Canbera, Melbourne, Sydney, Hobart (GMT+11:00) Magadan, Solomon Is., New Caledonia (GMT+12:00) Fiji, Kamchatka, Marshall Is., Wellington, Auckland (SMT+13:00) Nuku'alofa	

N		
時區:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei	
✓ 啓用日光節約時間		
設定模式:	以絕對日期設定	
時間調整:	以絶對日期設定 以相對日期設定	
開始時間:	一月 🔻 1 💌 0:00 💌	
結束時間:	一月 👻 1 💌 0:00 💌	

圖表 76: 設定系統時間

6.1.3 管理設定 (Management Setting)

描述遠端連線服務的設定,包括 SSHv2, SNMP 等等遠端連線服務的相關資訊。其中的選項有:

- 是否允許遠端 SNMP 連線
- 是否允許遠端 SSHv2 連線
- 是否允許 Ping 封包回應

SNMP 9	能資社群名稱:	public								
SNMP 7	可讀可寫社群名稱:	private]				
SNMP T	irap 社群名稱:	private	主機名編		允許 SNMP 連線	允許 SSH 連線	允許 Ping		-	新增位址
1	HostGroup_1 HostGroup_2				\$	~	4		←	修改位址
									←	刪除位址
設備:	☑ 九許 SNMP 連續	\$	✔ 允許 SSH 連線	☑ 尤許 Ping E	cho		套用	- r		

圖表 77: 管理設定

說明:網路管理者可以透過該設定,限定遠端特定主機對於 IPS Managerment Port 所能連線存取的服務(SNMP、SSHv2、Ping)。

啓動遠端連線服務之後,還可以限定遠端連線的 IP 位址。於右方有三個按鍵圖 示,分別是:

 新增位址:選擇可以連線的來源主機名稱,並勾選所需連線管理設定方式, 如圖表 78 圖表 78:,按下確定鍵即設定完成。



0	管理	設定			0
管理者主機	名稱:	Host	Group_	1	
[連線方式]				
☑ 允許 SN	MP 連絡	泉			
☑ 允許 SSI	H連線				
☑ 允許 Pin	g				
-	確定	1	I	刘消	1
					_

圖表 78: 連線方式設定

- 修改位址:修改來源主機與其連線方式設定,按下確定鍵即設定完成。
- 刪除位址: 刪除選擇的 IP 來源位址與連線方式。

說明: 主機與 IP 位址 (IP Address) 的設定,請參考下一章物件 (Object) 設定。

6.2 連線埠設定 (Port Configuration)

設定 NK6000 設備中個別連線埠的模式參數設定,如圖表 79 所示。使用者可以利用連線埠的設定把一台 NK6000 設備,切割成多台不同的 IPS/IDS 虛擬設備都可以搭配不同的安全政策群組來獨立。



圖表 79: 連線埠設定畫面



參數說明如下:

- 別名 (Alias): 一個暱稱,由使用者自行定義。
- 模式 (Mode): 說明此連接埠的設定狀態是 IPS 模式, IDS 模式, IPS-Monitor 模式, 或是 IDS-Monitor 模式...等等。
 - Forward 模式: 連線埠收到封包後,會直接轉送到另一個成對的連線 埠。系統不會進行任何偵測檢查行為。
 - IPS 模式:此模式將兩個成對的連線埠視為單獨一組 IPS 設備,依照單 獨的安全防禦政策組來進行網路封包及行為分析偵測,並且根據安全政 策所訂定的防禦反應行為來確保網路安全。
 - IPS-監視模式 (IPS-Monitor): 此模式將兩個成對的連線埠視為單獨一 組 IPS 設備,依照單獨的安全防禦政策組來進行網路封包及行為分析偵 測,但是僅進行事件記錄,不阻擋封包或是干擾連線行為。
 - IDS 模式: 此模式將單一的連線埠視為一組 IDS 設備,依照單獨的安全 防禦政策組來進行網路封包及行為分析偵測,防禦反應有事件記錄以及 重置連線。
 - IDS-監視模式:此模式將單一的連線埠視為一組 IDS 設備,依照單獨的 安全防禦政策組進行網路封包及行為分析偵測,防禦反應僅有事件記錄。
 - HA 模式:此連線埠被設定成 HA 功能埠,傳送 HA 功能相關資訊。
- 防禦政策群組 (Apply Rule Set): 顯示對應使用的政策群組 (Rule Set)。
- 忽略政策檢查 (Bypass Policy Check): 是否忽略 IPS 政策檢查。
- 忽略狀態檢查 (Bypass State Inspection): 是否忽略 TCP 狀態檢查。
- 忽略封包完整性檢查 (Bypass Integrity Inspection): 是否忽略封包完整性 (Integrity) 檢查。
- 忽略碎片重組檢查 (Bypass Fragment Inspection): 是否忽略封包切割 (Fragment) 重組檢查。
- 忽略 VPN 封包檢查 (Bypass VPN Inspection): 是否忽略 VPN 封包檢查。
- 忽略 ACL 政策檢查 (Bypass ACL Inspection): 是否忽略 ACL 政策檢查。
- 忽略埠掃瞄檢查 (Bypass Port Scan Inspection): 是否忽略 Port Scan 檢查。
- 忽略 GRE 解碼 (Bypass GRE Decode): 是否忽略 GRE 封包。
- 忽略 IP 掃瞄檢查 (Bypass IP Sweep): 是否忽略 IP Sweep 檢查。
- 連線模式 (Link Mode): 顯示連接埠的實際連線狀態。

使用者可以依據實際的網路環境或是特殊的應用需求,調整以上設定以達到最佳 化的使用狀態。當設備連線時,移動游標點選畫面中的連線埠圖示 (Port Icon),系 統會跳出該連線埠的詳細配置資訊,如圖表 80,81 所示。修改配置內容後,按下確 定 (OK) 鍵,即完成該連線埠的設定。



(設定)					
埠0					
別名	IPS 1				
模式	IPS模式	▼ 防禦政	、策群組	RuleSet 1	
	Forward 模式 IPS 模式 IPS 監視模式				
[選項]	IDS 模式 IDS 監視模式				
■省略政策核	查	■省略狀態檢查		■省略碎片重組檢查	
▶ 省略封包另	完整性檢查	☑省略 VPN 檢查		☑省略 ACL 政策檢查	
■省略埠掃晒	苗值測	☑省略 GRE 解碼		📓 省略 IP 掃描檢查	
連線模式	1000 Mbps 🔻	-			
		確定	取消		

圖表 80: 設定連線埠畫面

W					0
	[設定]				_
	埠5				
	別名	IDS			
	模式	HA模式			
	IP 位址	0.0	.00		
	· · · · · · · · · · · · · · · · · · ·				
	[選塤] ———				ן ך
	■省略政策檢查	Ē	■省略狀態檢查	■省略碎片重組檢查	
	■省略封包完整	管性檢查	■省略 VPN 檢查	■省略 ACL 政策檢查	
	■省略埠掃瞄値	調	■省略 GRE 解碼	■省略 IP 掃描檢查	
	連線模式	100 Mbps	▼ 全雙工		
				l	ן ע
		ſ		Ter 7 da	
			1 1 1	以7月 :	

圖表 81: 設定 HA 功能埠畫面





本章說明

主要說明物件 (Object) 的設定。

本章內容包含下列使用說明

章節	描述
7.1	主機設定 (Host Configuration)
7.2	虛擬網路設定 (VLAN Configuration)
7.3	時程設定 (Schedule Configuration)
7.4	服務設定 (Service Configuration)

7.1 主機設定 (Host Configuration)

說明如何設定主機物件。左邊為群組清單,右邊為目前選取的群組的主機位址。 上方有按鍵可以新增、修改以及刪除。

0		BEMS管理系统客户端		000
έγ.				
0		NK6 under test (192.168.168.205)		000
設備訊息 物件設定 防禦政策 即時監	測報表設定系統事件			
位址群組 VLAN 時程 服務				
HostGroup_1 HostGroup_2	編號	名稱	IP 位址 / CIDR Prefix	
	1	Host_1	192.168.20.98/32	
	2	Host_2	192.168.168.2407.24	
	0	後改位址群組	0	
	位址群組名種	: HostGroup_1		
	<u> 容</u> 動	名稱 IP 位址 / CII Host_1 192.168.20	DR Prefix 1.98 / 32	
	<u> </u>	Host_2 192.168.168	3.240/24	
		0	修改位址 🗍 🤿	
		位址名稿: Host_1		
		IPv4 - 192	.168 .20 .98 / 32	
			77 BYH	
		I		
		儲存 取消		
<u></u>	J <u>L </u>			

圖表 82: 主機設定 (HOST Configuration)



按鍵功能說明:

■ 新增 (ADD):

加入新的主機 (Host) 群組。點選後會出現新增位址群組 (Create Host Group) 的視窗。中間有按鍵可以讓使用者新增 (ADD)、修改 (EDIT) 以及 刪除 (DEL) IP 位址。將新增完畢的 IP 位址前方的啓動核取方塊打勾,即可 將此主機 (Host) 加入群組使用。未勾選者則不會被加入群組中。

)	新增位址群組	
位址群組名稱:		
啓動	名稱	IP 位址 / CIDR Prefix
0	Host_1	192.168.20.98/32
	Host_2	192.168.168.240/24
	儲存	取消

圖表 83: 新增/修改群組視窗

群組視窗按鍵功能說明:

◆ 新增主機 (ADD Host):

新增一組主機 (Host) 位址,如圖表 84,點選後會出現新增 / 修改位址 (Create / Edit Host Address) 的視窗。輸入主機 (Host) 名稱、位址、子網路遮罩 (CIDR Prefix) 後,按下儲存 (Set) 按鍵即可。

0	修改位址	
位址名稱:	行銷業務甲	
IPv4	192 . 168 . 168	.100 / 32
	儲存 取消	-

圖表 84: 新增/修改位址視窗

◆ 修改主機 (EDIT):



修改一組主機 (Host) 位址,選擇需要修改的主機名稱後,按下修改按 鍵即可進行修改編輯。

- ◆ 刪除主機 (DEL): 刪除一組主機 (Host) 位址。選擇一組欲刪除的主機 (Host) 後,按下 刪除 (DEL) 按鍵即可完成。
- 修改群組 (EDIT): 修改主機 (Host) 群組。點選後會出現修改位址群組 (Edit Host Group) 的 視窗。中間有按鍵可以讓使用者新增 (ADD)、修改 (EDIT)、 删除 (DEL) IP 位址。將新增完畢的 IP 位址前端的啓動 (Enable) 核取方塊打勾,即可將 此主機加入群組使用,未勾選則不會加入群組中。
- 刪除群組 (DEL): 刪除主機群組。選擇一組欲刪除的群組後,按下刪除 (DEL) 按鍵即可完成。

7.2 虛擬網路 (VLAN Configuration)

說明如何定義虛擬網路 (VLAN: Virtual LAN) 物件。左邊為虛擬網路物件清單, 右邊為目前選取的虛擬網路物件中有核取的虛擬網路代碼 (VLAN ID)。上方有按鍵可 以新增 (ADD)、修改 (EDIT)、刪除 (DEL) 虛擬網路物件。



圖表 85: VLAN 參數畫面



按鍵功能說明:

■ 新增 (ADD):

加入新的虛擬網路 (VLAN) 物件,如圖表 86。將啓動 (Enable) 的核取方 塊打勾,即可將此虛擬網路代碼 (VLAN ID) 加入此虛擬網路 (VLAN) 物件 中。中間可以選擇全選 (Select All) 或取消選擇 (Exclude All)。

修改 (EDIT): 修改已存在的虛擬網路 (VLAN) 物件,修改操作畫面雷同圖表 86。修改完 畢後按下儲存 (Set) 按鍵即可完成。

■ 刪除 (DEL): 刪除已存在的虛擬網路 (VLAN) 物件。選擇後按下刪除 (DEL) 按鍵即可。

Select All	Exclude All	
Enable	VLAN ID	
	1	
	2	
	3	0
N	4	
$\mathbf{\overline{\mathbf{N}}}$	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	

7.3 時程設定 (Schedule Configuration)

說明如何定義時程 (Schedule) 物件,如圖表 87。左邊為時程 (Schedule) 物件 清單,右邊藍色區域代表是目前被選取要排定時程 (Schedule) 的時段。操作畫面上 方有按鍵可以新增 (ADD)、修改 (EDIT)、刪除 (DEL) 時程 (Schedule) 物件。



a set i about handle a set i i i and i and	N	K6 under test (192	168.168.205)				00
痛訊息 · 初件設定 防禦政策 · 即時監	別一報表設定「系統事件」						
立址群組(VLAN)時程(服務)	. 🖾 🖾 🔟						
ichedule_Group_1	388	-8-	·m	:#=	1829	網五	漏分
est	0.00	~	40-	Alteres		1244	201
	1:00						
	2:00						
	3:00			-			
	4:00				-		
	5:00						
	6:00						
	7:00	-					
	8:00	-		1			
	9:00			2			
	10:00						
	11:00			7			
	12:00						
	12:00	-			-		
	14:00			17			
	15:00						
	16:00						
	17:00					· · · · · · · · · · · · · · · · · · ·	
	19:00						
	10:00						
	20:00						
	25.00						
	22:00				-		
	22.00						
	23.00						

圖表 87: 時程 (Schedule) 畫面

按鍵功能說明:

■ 新增 (ADD):

加入新的時程 (Schedule) 物件,如圖表 88。輸入時程名稱,並點選所要 排入時程的時段,即可將此時段加入此時程物件中。時段顏色改變表示該時 段已經被選取,另外也可以利用移動滑鼠進行大範圍的選取。

時程名稱: 上班時程								
	週日	週—	週二	週三	週四	週五	週六	
0:00								
1:00			3 8		1			
2:00			3 8		2		-	
3:00			3 8		1			
4:00			3 8		2			
5:00			3 6		· · · · ·			
6:00			3 8					
7:00			3 8					
8:00			1					
9:00								
10:00								
11:00								
12:00								
13:00								
14:00								
15:00								
16:00								
17:00								
18:00								
19:00								
20:00								
21:00			-					
22:00								
23:00								

圖表 88: 新增/修改時程 (Schedule) 物件


- 修改 (EDIT): 修改已存在的時程物件,修改操作畫面如圖表 88。修改設定完畢後,點選 儲存 (Set) 按鍵即可完成。
- 刪除 (DEL): 删除已存在的時程物件。選擇後按下刪除 (DEL) 按鍵即可。

7.4 服務設定 (Service Configuration)

說明如何定義服務 (Service) 物件,如圖表 89。左邊為服務 (Service) 物件清 單,右邊是此服務 (Service) 物件所對應的通信協定 (TCP/UDP/ICMP Protocol),以 及來源埠 (Source port)、目的埠 (Destination port) 範圍。上方有按鍵可以新增 (ADD)、修改(EDIT)、刪除 (DEL) 服務 (Service) 物件。

	BEMS管理系统客戶品	000
K.		
0	NK6 under test (192.168.168.205)	0.0.0
設備訊息 物件設定 防禦政策 即時監測	報表設定 系統事件	
位址群組 VLAN 時程 服務 Service A		1
Service B	SEEKDATE: ICP	
	1495t	來源埠範圍
	1	1025 ~ 65535
	4632	目的埠範回 1026 × 55535

圖表 89: 服務 (Service) 設定畫面

按鍵功能說明:

■ 新增 (ADD)、修改 (EDIT) 服務

加入新的服務 (Service) 物件或是修改已經存在的服務 (Service) 物件,如表 90。點選所要設定的通信協定 (Protocol),可以選擇 TCP、UDP 或是 ICMP。TCP 及 UDP 範圍為 0~65535, ICMP 範圍為 0~255。中間 按鍵可以新增、修改、或是刪除來源與目的埠 (port) 的範圍。



		NK6000 使用手
	新增服務	0
服務名稱:		
通訊協定:	TCP O UDP O ICMP	
編號	來源埠範圍	
1	0~65535	
編號	目的埠飯磨	
1	0 ~ 65535	

圖表 90: 新增/修改服務 (Service) 畫面

◆ 新增 (ADD)、修改(EDIT) 範圍:

選擇通信協定為 TCP 或是 UDP 時,可以新增或修改來源埠與目的 埠的範圍。

選擇通信協定為 ICMP 時,可以新增或修改 Type 及 Code 範圍。

•	新增來源	埠範圍		0
	이	~	65535	
	儲存		取消	

圖表 91: 編輯 Port 範圍

- ◆ 刪除 (DEL) 範圍: 選擇欲刪除的範圍後,按下刪除按鍵即可完成。
- 刪除 (DEL) 服務: 選擇欲刪除的服務後,按下刪除鍵即可完成。



8 第八章 政策管理

本章說明

主要說明安全防禦政策管理介面操作。

本章內容包含下列使用說明

章節	描述
8.1	防禦政策
8.2	攻擊特徵
8.3	新增/修改/刪除防禦特徵
8.4	政策群組

8.1 防禦政策

網路防禦政策是管理系統中最重要的資訊,網路防禦政策可以讓網路守護者知道 如何偵測攻擊,如何在發現攻擊後要作什麼反應,以及要保護什麼,以及何時保護。 因此,一條網路防禦政策是由偵測資訊(攻擊辨識碼、統計參數...等)、保護對象、時 程、反應、以及類別,發佈日期等等進一步資訊所組成。

攻擊特徵 (Signature) 指的是網路防禦政策當中最重要的比對資料。不管是已知 或是未知的網路異常行為,或者是程式漏洞等等,多多少少都會有一定的特徵可以被 辨識出來。只要能掌握網路封包的特徵,就可以預防駭客的網路攻擊,或是防制不正 常的網路行為發生。

系統預設防禦政策的攻擊特徵是由原廠的 BSST 所制訂。BSST (BroadWeb Security Service Team)由一群網路安全專家所組成。任務是在鑽研駭客入侵手法, 蒐集網路安全技術情報,隨時掌握各種漏洞訊息,提供給客戶永續的網路安全服務, 包括制訂最新的攻擊防禦政策、技術支援、安全技術諮詢、教育訓練等等。

8.2 攻擊特徵 (Signature)

視窗提供兩種檢視法:表格列表模式 (Table View) 與樹狀列表模式 (Tree View)。



■ 表格列表模式 (Table View): 如圖表 92,利用表格方式將所有的規則陳列 出來。上方為原廠提供的預設防禦政策。下方為使用者自訂防禦政策。

		BEMS管理系统客户最	ń .		
5		NK6 under test (192,168.1	68 205)		
波備訊息	物件設定 防禦政策	《時監測 報表設定 系統事件			
友擊特徵	政策群組				
		▲ ● 表格列表 ○ 樹狀列表			
「預設政策	疾]				
AREE A	政策發佈者	防禦政策名稱	及擊種類	嚴重程度	預設攻撃反應
1	預設政策	TCP SYN	DoS/DDoS	00000	即時監測;記錄事件, 丢棄封包;
2	領設政策	TCP Flood	DoS/DDoS	00000	即時監測;記錄事件;丟棄封包;
3	預設政策	UDP Flood	DoS/DDoS	00000	即時監測;記錄事件;丟棄封包;
4	預設政策	ICMP Flood	DoS/DDoS	66666	即時監測;記錄事件,去棄封包;
0	現就軟果	IR Flood	005/0008	00000	即時監視,記錄事件,去棄封包。 即時監測,記錄事件,去棄封包。
7	通知に取用	TCP Pod Scan	Bran	00000	NHTLER, 北京中叶, 大東封巴, 明山陸河・記録車任, 王帝共会
8	補設政策	UDP Port Scan	Scan	00000	即時際測:記錄畫件: 馬車封包:
9	預設政策	PSweep	Scan	00000	即時監測:記錄事件: 長寨村包.
10	預設政策	TCP Port SYN Scan	Scan	00000	即時監測;記錄事件; 丟棄封包.
11	預設政策	TCP Port FIN Scan	Scan	88888	即時監測;記録事件;丟棄封包;
12	預設政策	TCP Port Null Scan	Scan	00000	即時監測;記錄事件;丟藥封包;
13	預設政策	TCP PortXMas Scan	Scan	00000	即時監測;記錄事件, 丟棄封包.
14	預設政策	TCP Land	Others	66666	即時監測;記錄事件; 丟棄封包;
15	BLECON R	ICP Broadcast	DISIDUIS	000	周時監測,記錄爭汗,去集新包,
使用者定	2義政策)	1 Public Lag		1 mm m m m m	I museum
A 31995	以來號仰者 使用書字是10節		火手搓短	教里住民	開設水平以路
1	使用者正教成束		Web Attacks		RUNYSCOU, SCARONT, SECONTOL,
3	使用委定参数常	Licer Fieline	Moh Attacks		即時時期 記錄事件, 通過時間,
4	使用表定差許將	3	Web Attacks	1	別時時間 記述事件 通過対象

圖表 92: 表格列表模式 (Table View) 畫面

表格模式的欄位說明如下:

欄位	描述
編號	防禦規則序號
政策發佈者	規則制定者
	1. 預設政策: 由原廠 BSST 所建立
	2. 使用者定義政策: 爲使用者自行定義
防禦政策名稱	防禦政策的名稱
嚴重程度	攻擊嚴重程度列表,區分為五級:
	●輕微威脅
	●● :低度威脅
	◆◆◆ :中度威脅
	●●●● :高度威脅
	●●●●●:嚴重威脅
攻擊種類	系統預設値內定 16 種類攻擊特徵:
	1. Web Attacks
	2. Buffer Overflow
	3. Trojan Horse
	4. Access Control



	5. P2P
	6. Instant Messenger (IM)
	7. Virus/Worm
	8. Porn
	9. DoS/DDoS
	10. Scan
	11. ACL
	12. Mail
	13. Tunnel
	14. Stream Media
	15. File Transfer
	16. Others
預設攻擊時的	定義發現攻擊時所觸發之動作,系統提供五種動作:
反應	1. 通過 (Forward)
	2. 阻絕 (Drop)
	3. 透過郵件警告 (Warning by E-mail)
	4. 即時監控 (Monitor)
	5. 事件紀錄 (Log)

樹狀列表模式 (Tree View): 如表 93,依照每條規則所屬的類別 (Category) 來分類,點選特定的規則,可以在右邊看到此規則的詳細資料。



圖表 93: 樹狀列表模式 (Tree View) 畫面



工具列的按鍵功能說明:



8.3 新增/修改/刪除防禦政策

除了系統內建的防禦政策之外,使用者可依照實際需求新增/刪除/修改防禦政策。

8.3.1 新增政策

按下按鍵後,可以新增使用者定義的網路安全防禦政策。

攻擊名稱:		攻擊種類: Web Attacks	▼ 通訊協定: IP
受影響作業	系统: 📄全部 📄Windows 95/98	Windows 2000/XP Linu	ux EFreeBSD
	SGI Solaris	Network Device	er Unix
嚴重程度	P	1 1	1
和《金1主汉、	輕微 低度	中度 高度 嚴	重
			.1 (1917) 1
9/Fai(1981)+]			()#·(#)
封包發生		. 19	✓ 套用到 WAN 端 ● 委用到 LAN !
依據 政策	ID .	累計計算	
			~
中間 攻撃反應			
時间1 特徴2	特徵3 特徵4 特徵5 特徵6		
特徵比對模式	分辨大小寫	▼ 特徴型態	大字節序
比對位移	0 1 比對長度	0 1	
11:819526	0 1 日本	0 *	
A DISTRUCTION COMPANY			
特徵運算	4.00		

圖表 94: 新增政策畫面



- **攻擊特徵 (Signature):** 定義防禦政策內的攻擊特徵。
 - 政策屬性 (Attribute):
 - ◆ 攻擊名稱 (Name): 此名稱是作為識別之用,用來顯示在回報系統 與電子郵件之中。此欄位必須為唯一。
 - ◆ 攻擊種類 (Category): 確定此政策所防禦的攻擊是屬於何種攻擊 類別。
 - ◆ 通訊協定 (Protocol): 確定此類攻擊的通信協定,包括 TCP、UDP、 ICMP、IGMP 或 IP。如果使用者只想要偵測 IP 封包,選擇 IP 通 訊協定就可以了。
 - ◆ 受影響作業系統 (Affected OS): 指出此類攻擊是對於何種作業系統會產生影響,使用者可自訂多種選項易於辨識攻擊影響範圍,作業系統選項包含 Windows 95/98、Windows 2000/XP、Linux、 FreeBSD、SGI、Solaris、Network Device、Other Unix 或者全部。 若使用者不了解需選擇何種作業系統,則可選擇全部。此項設定目的為易於辨識該防禦政策之分類,並不會影響系統效能。

▶ 嚴重程度 (Severity): 此欄位定義欲偵測之攻擊的嚴重程度。



圖表 95: 政策屬性畫面

- 辨識條件 (Frequency): 定義封包出現的『重複率』與『週期』。
 - ◆ 『封包發生 次Ⅰ秒』: 偵測到重複性封包的個數。
 - 「每幾秒鐘』:從第一個封包被偵測到最後一個滿足重複限制封包的時間間隔。若在此週期內並無收集到足夠符合條件之的封包,此時重複計數將會被重新設置為零。
 - ◆ 統計條件。
 - 政策 ID: 依照事件 ID 統計。
 - 政策 ID + 來源 IP: 依照事件 ID 與來源位址統計。
 - 政策 ID + 目的 IP:依照事件 ID 與目的位址統計。
 - 政策ID + 來源與目的IP:依照事件ID與成對的來源目的位址 統計。

[辨識條件]			
封包發生	1 次/	0 [利	>	
依據	政策 ID	▼ 累	は計算	

圖表 96: 辨識條件



選項 (Option): 定義政策是否被啓動,以及定義此政策進行偵測判斷的 連線埠。



選擇不同的通信協定 (Protocol),封包的特徵內容定義會有區別,對於安全政策的處理操作也會有所不同,以下將分別說明欄位功能:

- (1). 一般設定:
- TCP / UDP 埠: 選擇通信協定為 TCP / UDP 時可以設定。
 - ◆ 來源埠 (Source port): TCP 或 UDP 連線來源埠。
 - ◆ 目的埠 (Destination port): TCP 或 UDP 連線目的埠。
 - ◆ 比對運算:系統提供了『忽略 (ignore)』/『等於 (equal)』/『不 等於 (not equal)』/『大於 (Greater than)』/『小於 (less than)』
 等五種比對運算欄位供使用者指定。

來源埠: 忽略 従 0 〕 至 0 〕 ▶
來源埠: 忽略 ▼ 従 0 〕 至 0 〕 ▶
來源埠: 忽略 ▼ 從 0 0 至 0 0 ▶
目的埠: 忽略 🔻 従 🛛 0 * 至 🛛 0 * 🕨

圖表 98: TCP port 選項

UDP埠	特徵	攻擊反應										
			來源埠:	忽略		Ĕ	 0 1	至	 0 (•		
			目的埠:	忽略	▼ 8	ž	0 0	至	0 (
									 1.1			

圖表 99: UDP port 選項

- 特徵內容 (Content): 定義 IP 封包的特徵與內容。最多可以定義六種不同的特徵內容。
 - ◆ 特徵比對模式:比對的字串可以是 ASCII 字串或是十六進位字串,



如果是使用十六進位值來比對時,允許比對的字母是「0」至「9」, 「A」到「F」或「a」到「f」。

- 分辨大小寫:大寫字元與小寫字元在比對上是不同的字元。此 為預設之比對方法。
- 忽略大小寫:大小寫字元在比對判別上視爲相同的字元。
- URL 字串: URL 部分將會被取出當作字串分析。比對字串中若 有問號,問號之前的字串將會視為 URL 的基本,問號之後的 字串會被視為是此 URL 字串之參數。而且,URL 比對時預設 值是忽略大小寫的,並且不會忽略空白處。
- 十六進位: 輸入內容爲十六進位字元。

時徵1 特徵2	特徴 3 特徴 4 特徴 5 特徴 6		
特徵比對模式	分辨大小寫 ▼	特徵型態	大字節序
比對位和		0 1	
20121120	不分辨大小寫	• -	
比對距離	URL字串	0 ()	
特徵運算	十六進位 マバー		
特徴		>]

圖表 100: 特徵比對模式

特徵1 特徵2 9	特徴3 特徴4 特徴5 特徴6		
特徵比對模式	分辨大小寫	▼ 特徴型態	大字節序
比對位移	0 1 比對長度	0 *	大字節序
			小字節序
吃到起角度		U .	八進制
特徵運算	等於		十進制
特徴		>	IP 字串



- ◆ 特徵型態:
 - 大字節序 (Big Endian): 依照字元順序由大到小。
 - 小字節序 (Little Endian): 依照字元順序由小到大。
 - 十六進制 (Hexidecimal): 內容為十六進位模式字串。
 - 八進制 (Octal): 內容為八進位模式字串。
 - 十進制 (Decimal): 內容為十進位模式字串。
 - IP 字串 (IP String): 內容為 IP 字串。
- ◆ 比對位移 (Offset): 比對起始點與封包籌載(payload)內容開始之間 的位移。
- ◆ 比對長度 (Depth): 比對起始點與封包內容開始之間的長度。
- ◆ 比對距離 (Distance): 比對內容與前一個比對內容之間的距離。
- ◆ 比對範圍 (Within): 比對內容所在的範圍區域。



◆ 特徵運算:系統提供『等於 (equal)』與『不等於 (not equal)』二 種比對運算欄位供使用。

說明:

- 1. 特徵一的特徵運算僅能選擇『等於 (equal)』。
- 2. 於全部的六項特徵內容欄位當中,特徵運算的『不等於 (not equal)』選項僅 能被選擇一次。

特徵:輸入比對的封包特徵,最大長度為 128 個字元。

特徵比對模式	分辨大小寫		特徵型態	大字節序	-	
比對位移	0 〕 比重	損度	0 ()			
比對距離	0 〕 比重	撤圍	0 3			
特徵運算	等於	-]				
特徴			>]		

圖表 102: 特徵內容

- 攻擊反應 (Action): 定義此安全防禦政策的反應動作。
 - ◆ 通過: 無條件放行封包通過。
 - ◆ 阻絕: 阻絕符合特徵條件的封包。若選擇通信協定為 TCP, 則可以 啓動同時中斷來源端與目的端的連線。
 - ◆ 即時監測:即時反應安全事件到即時監控畫面。
 - ◆ 記錄事件:
 - 只記錄事件,不記錄封包。
 - 記錄完整封包。
 - 僅記錄封包標頭 (前 64 bytes)。
 - ◆ 使用電子郵件警告:系統將透過電子郵件方式提出安全警告,需先 設定收件者郵件地址。

• 通過					
〕阻絕	中斷來源與目的	り端	Ŧ		
到時監測	🖸 記錄事件	不記錄封包	•	🔄 使用電子郵件警告	

圖表 103: 攻擊反應

(2). 進階設定:



- IP 封包標頭: 爲 IP 封包標頭欄位設定値參數所組成。
 - ◆ TOS 值: IP 標頭服務型態
 - ◆ IP Option: IP 封包標頭 Option 參數
 - ◆ IP 封包長度: IP 封包總長度
 - ◆ IP 標頭長度: IP 封包標頭長度
 - ◆ TTL: IP 封包存活時間欄位
 - ◆ Fragment ID: IP 封包識別欄位
 - ◆ Fragment Pointer: IP 封包分段指標
 - ◆ 檢查碼 (Checksum): IP 封包檢查碼欄位
 - ◆ Flags: DF-Don't Fragment
 MF-More Fragment
 UF-Unused Flag

IP標頭		進	楷榜與較定
TOS 值:	忽略		TOS (a) 7 6 5 4 3 2 1 0 •
IP Option :	忽略		end of option list no operation security loose source route time stamp
IP 封包長度:	忽略	-	20 🕄
IP 標頭長度:	忽略		20
TTL:	忽略	-	0
Fragment ID :	忽略		0
Fragment Offset :	忽略	-	0
檢查碼 :	忽略		0
Flags :	忽略		UF DF MF
	- - -	確定	現2治

- TCP 封包標頭: 爲 TCP 封包標頭欄位設定値參數所組成。
 - ◆ TCP 封包長度: TCP 封包總長度
 - ◆ TCP 標頭長度: TCP 封包標頭長度
 - ◆ 檢查碼 (Checksum): TCP 封包檢查碼欄位
 - ◆ SEQ: TCP 封包順序號碼
 - ◆ ACK: TCP 封包啓動號碼
 - ◆ URG Pointer: TCP 封包緊急指標
 - ◆ Windows size: TCP 封包 Windows 大小數值
 - TCP Flags: URG-urgent

 ACK-acknowledgement
 PSH-push
 RST-reset
 SYN-synchronization
 FIN-finish

Broa	adWeb
100	www.broadweb.com

		NK6000 使用手册
(進階標頭設定	
IP 標頭 TCP 標頭		
TODまt切目度	· 勿殿 - 20 *	
ICF BI BRIS		
TCP 標頭長度	: 忽略 🔻 20 🕻	
檢查碼	: 忽略 💌 0 🕽	
SEQ	: 忽略 🔽 0 🕽	
ACK	: 忽略 🔻 0	
URG Pointer	: 忽略 🔻 0 🕽	
Window Size	: 忽略 🔽 0	
Eleve	URG ACK PSH	
Flags		
	藤宇	
	NEAL AX(1)	
1		

圖表 105: 進階設定: TCP 標頭

- UDP 封包標頭: UDP 封包標頭欄位設定值參數所組成。
 - ◆ UDP 封包長度: UDP 封包總長度。
 - ◆ 檢查碼 (Checksum): UDP 封包檢查碼欄位。

峰階標頭設定
: 忽略 💌 8 📜
: 忽略 🔹 0 🕽
Terité
E AX/R

圖表 106: 進階設定: UDP 標頭

- ICMP 封包標頭: ICMP 封包標頭欄位設定值參數所組成。
 - ◆ 種類 (Type): ICMP 型態欄位。
 - ◆ Code: ICMP code 欄位。



- ◆ ID: ICMP 識別欄位。
- ◆ Sequence NO: ICMP 順序號碼。
- ◆ ICMP 封包長度: ICMP 封包總長度。
- ◆ 檢查碼 (Checksum): ICMP 檢查碼欄位。

Į.	進階標頭設定	
▶ 標頭 ICMP 標頭		
種類:	忽略 🗸	0
Code :	忽略 🔻	0
ID :	忽略 🔻	0
Sequence NO :	忽略 💌	0
ICMP 封包長度:	忽略 ▼	4
檢查碼 :	忽略 👻	0
	確定取消	:

圖表 107: 進階設定: ICMP 標頭

- IGMP 封包標頭: 爲 IGMP 封包標頭欄位設定值參數所組成。
 - ◆ 種類 (Type): IGMP 型態欄位。
 - ◆ Resp: IGMP 最大回應時間欄位。
 - ◆ IGMP 封包長度: IGMP 封包總長度。
 - ◆ 檢查碼 (Checksum): ICMP 檢查碼欄位。
 - ◆ 群組位址: IGMP 群組位址欄位。

BroadWeb www.broadweb.com	w	進階標調設定	0	NK6000 使用手册
	IP 標頭 IGMP 標題 種類: Resp: IGMP 封包長度: 檢查碼: 詳組位址:	 ②新 ▼ ②新 ▼ ②新 ▼ ②新 ▼ ②新 ▼ 0 0 0 0 	000	
		■ with a wi		

■ 一般資訊 (Info): 與政策相關的文字描述說明,方便使用者檢視政策。預設 值為空白,由使用者自行定義。

8.3.2 修改 / 刪除政策 🌌 📷

修改或是刪除所選擇的政策特徵 (Signature),使用者自行定義的政策可以被修 改或是刪除,而系統預設的政策不可以被修改或是刪除。修改政策的操作介面,請參 考8.3.1 說明。

8.3.3 其他

■ 記:根據特定字串搜尋政策。

按下按鍵後,會出現使用者輸入搜尋政策的畫面,輸入後即可快速搜尋防禦 政策。此功能提供客戶可以快速找到所需要的政策。於視窗中輸入完關鍵字後, 按下搜尋下一筆即可進行。視窗會停留在搜尋到的第一筆政策,以供使用者做進 一步的處理。



	NK6000 使用手册
0	



圖表 109: 搜尋政策

E : 匯出政策到檔案。

使用者可以利用匯出檔案的模式將政策特徵匯出。按下按鍵後可以利用此功能匯出防禦政策特徵。

•		儲存			0
Save <u>I</u> n: 🛅	Temp				
🛅 BW_Web					
C NK6					
C OTER					
I					
File <u>N</u> ame:	Save_Policy				
Files of <u>T</u> ype:	Export File (.ept)				-
			儲存	1	動消
			. 10013	<u>.</u>	

圖表 110: 匯出政策儲存成檔案

■■: 從檔案匯入政策。

使用者可以利用匯入檔案的模式將政策特徵匯入。按下按鍵後可以利用此功能匯入防禦政策特徵。

系統提供了自動化的遠端升級服務,可以利用網際網路連線原廠的升級網站,檢查並自動完成升級政策特徵。萬一使用者的網路系統無法正常連線網際網路時,也可以利用匯入匯出政策功能,達到更新防禦政策或是備份政策的目的。



				NK6000 (吏用手
0	開啓		0		
Look <u>I</u> n: 🛅	Temp	E E	8-6- 8-6-		
i BW_Web i NK6 i UnZip					
File <u>N</u> ame:	Saved_Policy				
Files of <u>T</u> ype:	Import File (.ept)				
		開啓	取消		

圖表 111: 選擇檔案匯入政策

8.4 政策群組

為了達成集中控管的便利性,原廠設計了運用防禦政策群組 (Rule Set) 的操作 模式,讓管理者僅需要修正一份資料之後,就可以快速更新網路防禦政策到所有的虛 擬 IPS 設備當中。系統提供最多可設定七組政策群組 (Rule Set)。

政策群組包括了預設的 IPS 防禦政策、使用者自行定義的 IPS 防禦政策、使用者 自行定義的 ACL 政策,以及連線埠對應定義等等。以下說明政策群組 (Rule Set) 的 操作模式。



圖表 112: 防禦政策群組畫面



8.4.1 新增政策群組

按下新增政策群組的按鍵,系統會跳出一個視窗供使用者可以選擇:

- 建立新的政策群組 (Create a new rule set):建立一個完全全新的政策群組。系統提供一個快速方便選擇的介面,客戶可以根據不同威脅等級以及不同分類的政策矩陣視窗中選擇所需要的。
- 複製現有的政策群組 (Duplicate an existing rule set): 選擇一個既有的政策 群組後,複製成客戶所需的政策群組。

•	新增政策群組	0
	諸選擇新增政策群組的方式:	
	●建立新的政策群組.	
	● 複製現有的政策群組.	
	上一頁 正一頁 確定 取消	

圖表 113: 新增政策群組

系統提供快速新增政策群組的方法,供使用者可以在最短的時間內完成安全政策 選擇。勾選需要加入到此政策群組的攻擊種類,以及對應的嚴重程度後,該防禦政策 就會被加入此防禦群組當中。

进择忍安管用的運動範圍.							
攻擊種類	嚴重程度						
	全部	嚴重	高度	中度	低度	輕微	
DoS/DDoS (101)							
Buffer Overflow (275)							
Access Control (527)						N	
3can (81)							
Trojan Horse (79)							
P2P(38)		I	I				
nstant Messenger (5)							
/irus/Worm (453)		I					
Porn (0)		M					
Web Attacks (37)							
Mail (0)							
File Transfer (0)		I					
Stream Media (0)		M					
Tunnel (0)							
ACL(0)							
Others (41)							

圖表 114: 選擇政策偵測範圍



8.4.2 刪除政策群組 📷

利用滑鼠游標選擇使用者所要刪除的政策群組之後,按下刪除鍵即可刪除。預設的政策群組不可被刪除。

8.4.3 修改政策群組

利用滑鼠游標選擇所要修改的政策群組之後,按下修改鍵之後可以進行修改。預設的政策群組不可被編輯。

就詳組4	名稱	RuleSet 1						
and the second second								
PS 政策	ACLI	次策 LAN 範圍定義	(埠對映定義					
	V	A 🔛 🔍	●表格列表 〇樹	狀列表				
使用者对	義政策	縦]					政策名稱:Us	er Define
優先權	啓用	政策發佈者	防禦政策名稱	攻撃種類	嚴重程度	2	.(保護新聞商	1.反應1
1	1	使用者定義政策	1	Web Attacks		_	(Prosted and	Corone 1
2		使用者定義政策	2	Web Attacks				
3	V	使用者定義政策	User Define	Web Attacks				
4	1	使用者定義政策	3	Web Attacks			優牛種	防御政策名稱
2010104	¥ 1							
預設政务	[]	70-0023/12-94	Presidents day for	Th- 10-9 4 # + 3	級音行的			
· 預設政务 優先權	₹] 啓用	政策發佈者	防禦政策名稱 下CE 2010		嚴重程度			
預設政务 優先權 WA	₹] 啓用	政策發佈者 預設政策	防禦政策名稱 TCP SYN TCP Elead	攻撃種類 DoS/DDoS DoS/DDoS	蒙 重程度			
預設政第 優先權 WA WA	₹] 啓用 ビ	政策發佈者 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS	厳重程度 ●●●●●●			
預設政第 優先權 WA WA WA	き] 啓用 ビ ビ	政策發佈者 預該政策 預該政策 預該政策 預該政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	厳重程度 ●●●●●● ●●●●●●			
優先權 WA WA WA WA WA	き] 啓用 ビ ビ	政策發佈者 預該政策 預該政策 預該政策 預該政策 預該政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood ICMP Flood ICMP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	康重程度 •••••• •••••• ••••••			
優先欄 WA WA WA WA WA	き 啓用 ダ ダ ダ ダ ダ	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood ICMP Flood ICMP Flood	攻撃種類 Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos	康亚程度 			
優先欄 WA WA WA WA WA WA WA	き 啓用 ダ ダ ダ ダ	政策發佈者 預該政策 預該政策 預該政策 預該政策 預該政策 預該政策 預該政策	防禦政策名稱 TCP Flood UDP Flood ICMP Flood ICMP Flood ICMP Flood ICMP Flood TCP Port Scan	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan	<u>厳重程度</u> 00000 00000 00000 00000 00000			
優先權 WA WA WA WA WA WA WA	き 啓用 ダ ダ ダ ダ ダ	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood ICMP Flood ICMP Flood ICP Flood TCP Port Scan UDP Port Scan	文学種類 Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Scan Scan	<u>厳重程度</u> ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			
後 で で で で 後 大 橋 WA WA WA WA WA WA WA	き 啓用 ダ ダ ダ ダ ダ ダ ダ ダ	政策發佈者 預該政策 預該政策 預該政策 預該政策 預該政策 預該政策 預該政策 預該政策	防療設策名編 TCP Flood UDP Flood ICMP Flood ICMP Flood ICMP Flood ICMP Flood ICP Port Scan UDP Port Scan UDP Port Scan	文学種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan Scan Scan	厳重程度 			
項読款対 優先欄 WA WA WA WA WA WA WA WA		政策發佈會 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防療設備名稱 TCP SYN TCP Flood ICMP Flood ICMP Flood ICMP Flood ICP Port Scan ICP Port Scan IP Sweep TCP Port Scan IP Sweep	攻撃種類 Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Scan Scan Scan Scan	厳重程度 00000 00000 00000 00000 00000 00000 00000 00000			

圖表 115: 修改政策群組圖-1 (表格模式)

and the second second									
以東朝祖名	38	RuleSet 1							
PS政策	ACLE	大策 LAN 範圍定義	/埠對映定義						
		x 🔝 🔍	→表格列表 ○樹	狀列表					
(使用者定	義政策	Ē]					政策名称・1	,	
優先權	啓用	政策發佈者	防禦政策名稱	攻擊種類	嚴重程度	F	网络第三人	Barfanet 1_	
1		使用者定義政策	1	Web Attacks		-	(PROSE HUBE	Become 1	16 16 1
2	1	使用者定義政策	2	Web Attacks					V 🚍
3	M	使用者定義政策	User Define	Web Attacks					
4		使用者定義政策	3	Web Attacks			優先權	1	防禦政策名稱
- NE BOLD- ME	1						1	SA2 SA1	
[預設政策 優先欄 ▲]	政策發佈者	防禦政策名稱	攻撃種類	嚴重程度		1 2	SA2 SA1	
(預設政策 優先欄 A] 啓用	政策發佈者	防禦政策名稱 TCP SYN	攻撃種類 DoS/DDoS	厳重程度		1 2	SA2	
【預設政策 優先欄▲ WA] 啓用	政策議佈者 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood	攻撃種類 DoS/DDoS DoS/DDoS	厳重程度 ●●●●●●		1 2	SA2	
【預読政策 優先欄▲ WA WA] 啓用 ビビ	政策發佈者 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood	攻撃極類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	厳重程度 000000 000000		1 2	SA2 SA1	
(預読政策 優先欄 A N/A N/A N/A N/A] 智用 ママママ	政策發佈者 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood ICMP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	厳重程度 ●●●●● ●●●●● ●●●●●		1 2	SA2 SA1	
【預読政策 優先欄▲ WA WA WA WA WA] 啓用 2 2 2 2 2	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策	防禦款策名稱 TCP SVN TCP Flood UDP Flood IGMP Flood	攻撃猛鎮 Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos	林王程度 000000 00000 00000 00000 00000 00000		1 2	SA2 SA1	
【預読政策 優先編 ▲ WA WA WA WA WA WA		政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood IOMP Flood IOMP Flood IP Flood	攻撃循鎖 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	厳重程度 00000 00000 00000 00000 00000 00000		1 2	5A2 5A1	
後日 後 後 大福 WA WA WA WA WA WA WA WA		政策設備者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防策設定名稱 TCP SYN TCP Flood UDP Flood ICMP Flood ICMP Flood IP Flood IP Flood TCP PortScan	攻撃猛類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan	厳重程度 ●●●●● ●●●●● ●●●●● ●●●●● ●●●●● ●●●●●		1 2	5A2 5A1	
で で で で で で で で で で で の で の で の で の で の で の で の で の で の の い べ み い べ み い べ み い べ み い べ み い べ み い べ み い べ み い べ ろ い べ ろ い べ ろ い べ ろ い べ ろ い べ ろ い べ ろ い べ ろ い べ ろ い ろ 、 、 い ろ 、 、 、 、 、 、 、 、 、 、 、 、 、		政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預 預設政策 預 預設政策	防禦政策名稱 TCP Flood UDP Flood ICMF Flood ICMF Flood IP Flood IP Flood TCP Potd Scan UDP Pott Scan	攻撃猛類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan Scan	厳重程度 		1 2	5A2 5A1	
「預設政策 優先糧」 WA WA WA WA WA WA WA WA] 啓用 マママママママママママママママママママママママママママママママママママ	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防療状況を結 TCP SVN TCP Flood UDP Flood IGMF Flood IGMF Flood TCP Port Scan UDP Port Scan IP Sweep	文学権類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan Scan Scan	献重程度 000000		1 2	<u>542</u> <u>541</u>	
で で で で で で で で で で で で で で		政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	M 増払火 名 編 TCP SYN TCP SYN TCP Flood UDP Flood ICMF Flood ICMF Flood IP Flood IP Flood TCP Pott Scan UOP Pott Scan UOP Pott Scan UOP Pott Scan COP Pott Scan IC P Pott Scan IC	攻撃猛類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan Scan Scan Scan	厳重程度 000000 000000 000000 000000 000000		1 2	<u>542</u> <u>541</u>	

圖表 116: 修改政策群組圖-2 (表格模式)



eb.com		NK6000 個	包用手冊
	修改政策群組	0	
政策群組名稱 RuleSet 1			
PS 政策 ACL 政策 LAN 範圍定義 / 埠對映定義			
C表格列表	€ ⓒ樹就列表		
● 防禁政策資料準(1994) ● 愛Web Affacks (130) ● 愛Web Affacks (130) ● 愛Trojan Horse (79) ● 愛Trojan Horse (79) ● 愛Trojan Horse (79) ● 愛P2P (38) ● 愛P1(38) ● 愛VrustWorm (453) ● 愛VrustWorm (453) ● 愛P0rn (15) ● 愛P0rn (· 政策名領: MS Windows sql Injection command · (保護範圍與反應) · (現金) · (現金)	

圖表 117: 修改政策群組 (樹狀模式)

修改政策群組時,除了可以調整使用者自行定義的 IPS 政策或是 ACL 政策中, 政策的優先順序、政策保護的範圍、安全防禦的反應行為等等之外,還可以設定網路 連線埠的特殊設定。

上方工具列按鍵功能說明:

- 過濾設定。使用者可以依照需求適度調整被啓動的安全防禦政策。
 通酬: 提升使用者定義政策優先權。向上調整優先順序一位
 - └ंटें: 降低使用者定義政策優先權。向下調整優先順序一位
- E 更改使用者定義政策選擇優先權。使用者可以針對特殊的網路環境需求而調整政策的優先順序。一旦網路封包被政策偵測比對引擎判定為有問題時,會依照高優先權的政策保護範圍、反應、以及時程而進一步處理。
- 證書政策。搜尋政策中之特殊字串。此功能提供客戶可以快速找到所需要的政策。於視窗中輸入完關鍵字後,按下搜尋下一筆即可進行。政策表格視窗會停留在搜尋到的第一筆政策,以供使用者做進一步的處理。

8.4.3.1 IPS 政策

利用滑鼠游標點選所需要修改的 IPS 政策之後,畫面右方會出現修改政策的畫面。依照不同的防禦政策類型,會有不同對應的參數設定模式供使用者選擇設定。



PS 政策	ACL	改策 LAN 範圍定義,	埠對映定義						
			●表格列表 〇樹	狀列表					
使用者》	自義政策	¥E]	196)	(政策名稱: TCP S	YN	
優先權	啓用	政策發佈者	防禦政策名稱	攻撃種類	嚴重程度	E			
1	1	使用者定義政策	1	Web Attacks		-	目的端上隈值		300÷
2		使用者定義政策	2	Web Attacks					
3		使用者定義政策	User Define	Web Attacks			來源端上隈值		300÷
4		使用者定義政策	3	Web Attacks	0				
2K BATHA	a 1						☑即時監測 ☑記錄事件	不記錄表頭	
預設政务	〔1]	政策發佈者	防雪政策名種	万能種類	蘇重程度		✓即時監測 ✓記錄事件	不記錄表頭 不記錄表頭 記錄表頭	•
預設政参 優先權 I/A	6] 啓用	政策發佈者	防禦政策名稱 TCP SYN	攻撃種類 DoS/DDoS	柴玉程度		✓即時監測 ✓記錄事件	不記錄表頭 不記錄表頭 記錄表頭	
預設政务 優先權 I/A I/A	能] 啓用	政策發佈者 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood	攻撃種類 DoS/DDoS DoS/DDoS	蒙重程度 00000		✓即時監測 ✓記錄事件	不記錄表頭 不記錄表頭 記錄表頭	•
預設政参 優先權 UA UA UA	能] 啓用	政策發佈者 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	献重程度 999999 999999 999999		✓ 用砷監測 ✓記錄事件	不記錄表頭 不記錄表頭 記錄表頭	
預設政务 愛先權 I/A I/A I/A	徒) 啓用 ビビビ	政策發佈者 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood ICMP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	蒙重程度 00000 00000 00000		《用時監測 《記錄事件	不記錄表頭 不記錄表頭 記錄表頭	
預設政會 優先權 WA WA WA WA WA	〔1] 【啓用 【ビビビビビ	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood ICMP Flood IGMP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	蒙重程度 •••••• •••••• ••••••		✓用砷酚测 ✓記錄事件	不記錄表頭 不記錄表頭 記錄表頭	
預設政會 優先權 WA WA WA WA WA	徒] 啓用 ダダダダ	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood IGMP Flood IGMP Flood IP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	●重程度 ●●●●●● ●●●●●● ●●●●●● ●●●●●● ●●●●●● ●●●●		✓ 即時監測 ✓ 記錄事件	不記錄表頭 不記錄表頭 記錄表頭	
預設政會 優先權 UA UA UA UA UA UA UA UA	徒] 啓用 マママママママ	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SVN TCP Flood UDP Flood ICMP Flood ICMP Flood IP Flood TCP Port Scan	攻撃種類 Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Scan	様面程度 00000 00000 00000 00000 00000 00000		✓ 即時監測 ✓記錄事件	不記錄表頭 不記錄表頭 記錄表頭	
資設政會 優先權 WA WA WA WA WA WA WA WA	後) 啓用 マママママママママママママママママママママママママママママママママママ	政策發佈者 預發政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood ICMP Flood ICMP Flood IP Flood TCP Port Scan UDP Port Scan	攻撃種類 DeS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan Scan	蒙重程度 		☑ 闻時監測 ☑ 記錄事件	不記錄表頭 不記錄表頭 記錄表頭	
優先權 WA WA WA WA WA WA WA WA WA WA WA	ft] 啓用 ママママママママ	政策發佈者 預於政策 預於政策 預於政策 預於政策 預於政策 預於政策 預於政策 預於政策	防療政策名稱 TCP SYN TCP Flood UDP Flood ICMP Flood ICMP Flood TCP Port Scan UDP Port Scan UDP Port Scan	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan Scan Scan	蒙重程度 00000 00000 00000 00000 00000 00000 00000 00000 00000		● (1995年) ● 記録事件	不記錄表頭 不記錄表頭 記錄表頭	-
	(E) PS	政策證佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP Flood UDP Flood ICMP Flood ICMP Flood IP Flood IP Flood IP Flood TCP Pott Scan IP Sweep TCP Pott Strin S	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan Scan Scan Scan Scan	厳重程度 000000	• (12)	● 经通知》 ● 2015年 ● 2015 ● 201 ● 2015 ●	不記錄表頭 不記錄表頭 記錄表頭	
「預読数す 優先稽 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A		政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防衛政策名稱 TCP SYN TCP Flood UDP Flood IGMF Flood IGMF Flood IGMF Flood TCP Port Scan IP Sweep TCP Port Scan IP Sweep TCP Port SYN S.	攻撃種類 DoS/DDOS DoS/DDOS DoS/DDOS DoS/DDOS DoS/DDOS DoS/DDOS Scan Scan Scan Scan Scan	様面程度 		● 经通知	不記錄表頭 不記錄表頭 記錄表頭	

圖表 118: 修改政策畫面之一

策群組名	呂稱	RuleSet 1						
28 政策	ACLE	於第一LAN 範圍定義:	/埠對映定義					
			●表格列表 〇樹	状列表				
使用者定	義政策	(t)					空管名籍 · IP Flor	hd
優先權	啓用	政策發佈者	防禦政策名稱	攻擊種類	嚴重程度	g 🕴		
1	1	使用者定義政策	1	Web Attacks	0	-	目的端上限值	1,000
2		使用者定義政策	2	Web Attacks	0			
3		使用者定義政策	User Define	Web Attacks				
4		使用者定義政策	3	Web Attacks				
20 Dame de	* 1						 ✓ 丟棄封包 ✓ 即時監測 ✓ 記錄事件 	不記錄表頭 ▼ 不記錄表頭
預設政策	き)	政策發佈者	防型政策名籍	功整種類	嚴重程度		 ✓ 丢棄封包 ✓ 即時監測 ✓ 記錄事件 	不記錄表頭 不記錄表頭 記錄表頭 記錄表頭
預設政第 優先權	き]	政策發佈者	防禦政策名稱 TCP SYN	攻撃種類 DoS/DDS	載重程度		 ✓ 丢棄封包 ✓ 即時監測 ✓ 記錄事件 	不記錄表頭 ▼ 不記錄表頭 記錄表頭
「預読政第 優先權 WA WA	₹] 	政策發佈者 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood	攻撃種類 DoS/DDoS DoS/DDoS	嚴重程度 ●●●●●● ●●●●●●		 ✓ 丢棄封包 ✓ 即時監測 ✓ 記錄事件 	不記錄表頭 ▼ 不記錄表頭 記錄表頭
預設政第 優先權 WA WA WA	き] 啓用 図	政策發佈者 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS	厳重程度 ●●●●●● ●●●●●● ●●●●●●		 ✓去棄封包 ✓即時監測 ✓記錄事件 	不記錄表頭 ▼ 不記錄表頭 記錄表頭
預設政第 優先權 UA UA UA UA	ぎ] 啓用 ダ ダ	政策發佈者 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood ICMP Flood	攻撃種類 Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos	厳重程度 ●●●●● ●●●●● ●●●●●			不記錄表頭 ▼ 不記錄表頭 記錄表頭
預設政策 愛先權 WA WA WA WA WA	*] 啓用 ダ ダ	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名編 TCP SYN TCP Flood UDP Flood ICMP Flood IGMP Flood	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	厳重程度 			不記錄表頭 ▼ 不記錄表頭 記錄表到
資設政策 優先權 WA WA WA WA WA WA	ぎ] 啓用 ダ ダ	政策設佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SVN TCP Flood UDP Flood ICMP Flood ICMP Flood IP Flood	攻撃種類 Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos	厳重程度 		✓ 丢棄封包 ✓ 即時監測 ✓ 記錄事件	不記錄表頭 ▼ 不記錄表頭 [238表頭
資設政策 優先權 WA WA WA WA WA WA WA WA	き] 啓用 ダダダダダ ダダ	政策發佈者 衝鼓政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禦政策名稱 TCP SYN TCP Flood UDP Flood IGMP Flood IP Flood IP Flood TCP Pott Scan	攻撃種類 Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Dos/DDos Scan	厳重程度 			不記錄表頭 → 不記錄表頭 記錄表頭
(預読政) 優先權 WA WA WA WA WA WA WA WA	き」 啓用 ダ ダ ダ ダ ダ ダ ダ ダ ダ ダ ダ ダ ダ	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防策改策名編 TCP SYN TCP Flood UDP Flood ICMP Flood IP Flood TCP Port Scan UDP Port Scan	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan Scan	厳重程度 60000 00000 00000 00000 00000 00000 00000		▼丢棄封包 ▼即時監測 ■記錄事件	不記錄表頭 ▼ 不記錄表頭 [238表現
「預読取算 優先權 WA WA WA WA WA WA WA WA WA WA	き」 啓用 ダ ダ ダ ダ ダ ダ ダ ダ ダ ダ ダ ダ ダ	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防禁軟束名稱 TCP Flood UDP Flood ICM Flood ICM Flood ICP Port Scan UDP Port Scan UDP Port Scan ID Sweep	攻撃種類 DoSIDDoS DoSIDDoS DoSIDDoS DoSIDDoS DoSIDDoS DoSIDDoS Scan Scan Scan	#12g 00000 00000 00000 00000 00000 00000 0000		● 活業封包 ● 即時監測 ● 記錄事件	不記錄表頭 ▼ 不記錄表頭 記錄表頭
で で で で で 後先種 WA WA WA WA WA WA WA WA WA WA	き 「 帮用 「 学 と と と と と と と と と と と と に 、 、 、 、 、 、 、 、 、 、 、 、 、	政策發佈者 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策 預設政策	防療政策名編 TCP SYN TCP Flood ICMP Flood IGMP Flood IGMP Flood ICMP Port Scan UDP Port Scan IP Sweep TCP Port SVLS	攻撃種類 DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS Scan Scan Scan Scan Scan	厳重程度 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		● 丢棄封包 ● 即時監測 ● 記錄事件	不記錄表頭 ▼ 不記錄表頭 記錄表頭

圖表 119: 修改政策畫面之二



圖表 120: 修改政策畫面之三



為了提供更彈性化的網路安全防禦,NK6000系統設計每1條 IPS 政策,都可以 對應到 32 組的防禦範圍與反應 (Scope & Action),大大提升了系統的防禦能力。預 設政策當中的防禦範圍的預設值是任何位址 (Any),反應行為的預設值請參考 8.3 『政策特徵』的說明內容。

右方防禦範圍與反應的按鍵說明如下:

新增。可新增一組防禦範圍與反應。
酬除。刪除已選擇的防禦範圍與反應。
影子優先權。向上調整優先順序一位
除低優先權。向下調整優先順序一位
許要改優先權。使用者可以調整防禦範圍與反應的優先順序。一旦網路 封包被政策偵測比對引擎判定為有問題時,會依照高優先權的防禦範圍與反 應而進一步處理。

按下右方『新增』按鍵來增加一組保護範圍與反應之後,會出現下面的編輯視窗。 於畫面之右方按下『新增』或是『編輯』按鍵後,可以於『保護範圍與反應』編輯視 窗中,編輯使用者欲設定的資料。

•	保護範圍與反應	0
SA1 SA2 test		
	確定	取消

圖表 121: 保護範圍與反應



reb.com					NK60	00 使用手册
8		Scope Action Editor			0	
名稱 SA2						
[保護範圍]						
☑來源主機	Host_1					
✔目的主機	Host_1					
✓VLAN 群組	VLAN_C	9roup_1				
[反應]						
 通過 						
☑頻寬限制	30	Kbps	☑總量限制	500	МВ	
◎阻網	中斷來源與目的端					
☑即時監測	☑記錄事件	不記錄封包 ▼	■使用電子郵件警台	ŧ		
[時程]						
	E	侍程 任何時間	1			
		確定	取消			

圖表 122: 保護範圍與反應

- 『保護範圍與反應』編輯畫面的參數說明如下:
 - 保護範圍:
 - ◆ 來源主機:指定保護封包來源位址的特定主機。主機的設定方式, 請參考 7.1 主機設定。
 - ◆ 目的主機:指定保護封包目的位址的特定主機。主機的設定方式, 請參考 7.1 主機設定。
 - ◆ VLAN 群組:指定保護特定 VLAN 群組。VLAN 群組的設定,請參考 7.2 虛擬網路設定。
 - 反應:
 - ◆ 通過:該封包將無條件被放行。
 - 頻寬限制:於封包放行時,限制保護範圍內所有觸發此攻擊特 徵的流量,且總和値不得超過「頻寬限制」欄所指定的大小。 頻寬流量每秒更新一次。
 - 總量限制:於封包放行時,限制保護範圍內所有觸發此攻擊特 徵的流量,且總和値不得超過「總量限制」欄所指定的大小。 封包總量以天為單位,每天凌晨零時更新後起算。
 - 阻絕: 直接丟棄封包, 阻絕連線 (中斷連線來源端與目的端)。
 - ◆ 即時監測: 即時顯示安全事件到即時監測的畫面中。
 - 記錄事件:記錄安全事件到系統的資料庫中。
 - 不記錄封包: 僅記錄事件,不記錄封包內容。
 - 記錄整個封包:記錄事件以及觸發事件的完整封包內容。
 - 記錄表頭:記錄事件以及觸發事件的封包表頭 (前 64 bytes)。
 - ◆ 使用電子郵件警告:利用郵件警告功能,即時反應事件給使用者。
 收件者的郵件清單,於 10.4.4 定期報表當中可以被設定。



■ 時程: 選擇反應的時間區間。時程的設定請參考 7.3 時程設定。

8.4.3.2 ACL 政策

系統提供L3/L4的防火牆連線管控政策的功能,封包在進入設備後,先經過L3 Anomaly 狀態檢查、L3/L4 ACL 政策檢查、L4 Anomaly 的狀態檢查後,才會進入 IPS 政策偵測檢查。系統預設並沒有任何 ACL 政策,由使用者自行定義。

0		修改政策群组	0
政策群組名稱	RuleSet 1		
IPS政策 ACL政	東 LAN 範圍定義 / 埠對映定義		
2 2 11			
編號		防禦政策名稱	
		確定取消	

圖表 123: ACL 政策畫面

上方工具列按鍵功能說明:



按下『新增』按鍵,系統會出現編輯 ACL 政策的畫面:

W	ACL Rule Editor	
名稱 ACL_1		
保護範圍		
○檢查 WAN 流量 ○檢查 LAN 流量	量 🕢 檢查 WAN 與 LAN 流量	
✓ 來源主機 Host A		
✓目的主機 Host A		
☑ 服務 All_P2P		
■ VLAN 群組		
反應		
⊙ 通過		
○ 頻寬限制 0	kbps 🗌 總量限制	0 KB
☑ 省略狀態檢查	🗋 省略政策檢查	雙向性
☐ 省略 TCP 重組	🗋 省略第四層以上的檢查	查
○阻絕		
■ 即時監測 ■ 記錄事件	■ 使用電子郵件警告	
- 時程		
● 即時監測 ● 記錄事件 時程	● 使用電子郵件警告	

圖表 124: 編輯 ACL 政策畫面

- 『 ACL 政策』編輯畫面的參數說明如下:
 - 名稱: 定義此政策的名稱,由使用者自行輸入定義。
 - 保護範圍:
 - ◆ 來源主機:指定封包來源位址的特定主機。主機的設定方式,請參
 考 7.1 主機設定。
 - ◆ 目的主機:指定封包目的位址的特定主機。主機的設定方式,請參
 考 7.1 主機設定。
 - ◆ 服務: 指的是網路通訊服務, 請參考7.4 服務設定。
 - ◆ VLAN 群組:指定特定 VLAN 群組。VLAN 群組的設定,請參考 7.2 虛擬網路設定。
 - 反應:
 - ◆ 通過:該封包將被放行,轉到 IPS 偵測引擎繼續檢查。
 - 頻寬限制:於封包放行時,限制此保護範圍內的所有來源位址 所佔的網路頻寬流量。流量每秒統計一次。
 - 總量限制:於封包放行時,限制此保護範圍內的所有來源位址 所傳遞的封包總量。封包總量每天統計一次,凌晨零時起算。
 - ◆ 省略狀態檢查: 忽略 TCP 狀態 (SYN;SYN-ACK;ACK) 的檢查。
 - ◆ 省略政策檢查: 忽略 IPS 政策檢查。
 - 雙向性: 忽略檢查雙向來的封包。
 - 僅來源端: 忽略檢查來源端的封包。
 - 僅目的端: 忽略檢查目的端的封包。
 - ◆ 省略 TCP 重組: 忽略破碎封包重組檢查。
 - ◆ 省略第四層以上的檢查: 忽略 IPS 引擎的政策檢查,會直接把封 包轉送出去。



- ◆ 阻絕:直接丟棄封包,阻絕連線。
- ◆ 即時監測:即時顯示安全事件到即時監測的畫面中。
- ◆ 記錄事件:記錄安全事件到系統的資料庫中。
- ◆ 使用電子郵件警告:利用郵件警告功能,即時反應事件給使用者。
 收件者的郵件清單,於 10.4.4 定期報表當中可以被設定。
- 時程: 選擇反應的時間區間。時程的設定請參考 7.3 時程設定

8.4.3.3 LAN 範圍定義 (LAN Definition)

為了解決 IP spoofing 的問題,系統提供 LAN 範圍定義功能。使用者可以事先 定義 LAN 端的 IP 位址範圍,系統將依照 LAN 端的 IP 位址範圍,偵測封包並判斷 是否有 IP spoofing 的安全事件發生。

[LAN	√範	图定義]
2		
編	諕	IP 位址 / CIDR Prefix
L		

圖表 125: LAN 範圍定義

上方工具列按鍵功能說明:

	1	新增。	可新增	LAN	端的	IP	位址	0	
•	1	編輯。	可編輯	LAN	端的	IP	位址	0	0
	M	刪除。	刪除已調	巽擇的	j lan	Ⅰ峁	∦ IP	位	址

按下『新增』按鍵,系統會出現新增 LAN 端 IP 位址的畫面。使用者需自行輸入 LAN 端的 IP 位址以及子網路遮罩 (CIDR),除了單一 IP 位址之外,亦可藉由子網路遮罩 (CIDR) 的設定方式,輸入整個子網段。

0

•	新增 LAN 範圍定義		0
	IP 位址 / CIDR Prefix 0 0 0 0	1	
	確定取消		
	NEAC 4X(H		

圖表 126: 新增 LAN 端範圍



8.4.3.4 埠對映定義 (Port Alternation)

系統提供連線埠對映定義 (Port Alternation) 功能, 滿足更彈性化的網路應用。

1 🧭 📶				
BE	IP 位址	通訊協定	原始埠	對映埠
	1P 127	通訊碼定	原始單	對映埠

圖表 127: 連線埠對映

上方工具列按鍵功能說明:



按下『新增』按鍵,系統會出現新增 LAN 端 IP 位址的畫面。輸入 IP 位址,通 信協定 (TCP / UDP),原始埠,以及對映埠後,按下確定即可。

●P版本4				
IP 位址	0.0	. 0	.0	
通訊協定	TCP	-		
原始埠	0			
對映埠	0			

圖表 128: 定義連線埠對映





本章說明

主要說明即時監測的操作介面。

本章內容包含下列使用說明

章節	描述
9.1	儀表版 (Dashboard)
9.2	事件 (Event)
9.3	流量 (Traffic)
9.4	利用率 (Utility)

9.1 儀表版 (Dashboard)

儀表版主要是顯示每一個連線埠的收送的封包狀態,並且將有偵測到有問題的封 包,利用用圓形比例圖展示出來。圖中會顯示出封包種類的所佔的比例、封包類型、 起始時間,接收與丟棄掉的總數量、平均速度、目前速度。按下『重置』鍵可以將統 計値歸零,重新開始計算。



圖表 129: 儀表版 (Dashboard)



9.2 事件 (Event)

列出所有監測到的事件列表,如表 130。表中即時列出發生的事件時間、嚴重程度、設備 (連線埠)、攻擊名稱、來源位址、目的位址、來源埠、目的埠、通信協定 (服務)、虛擬網路編號、次數、以及攻擊時的反應等等資訊。畫面每5秒鐘更新一次。



圖表 130: 事件 (Event) 列表

工具列按鍵功能:

■ 暫停 (Pause):

暫停事件列表的即時更新。按下『暫停』鍵,圖示隨即變爲『繼續』鍵。

0					NK6 under test								
設備訊息	物件設定防禦政策	· 即時監測	1 報表設定	系統事件									
儀表板 孝	新牛 流量 利用率												
(1050 (107/00)	時間	最重程度	設備	攻擊名稱	來譚 IP	目的IP	· 東源埠/	目的埠/	通訊協定	VLAN ID	次數	攻撃反應	
1812	2006/08/23 10:3		IPS 2 (L	ICMP De	192.168.168.83	168.95.1.1	3	3	ICMP	0	1	剧時監測	
2	2006/08/23 10:3	•	IPS 2 (L	ICMP De	192.168.168.83	168.95.1.1	3	3	ICMP	0	1	即時監測	
3	2006/08/23 10:3		IPS1 (L_	Bad TCP_	192.168.168.2	192.168.168.238	4482	25	TCP	0	5	即時監測	11
4	2006/08/23 10:3		IPS 2 (L	ICMP De.	192.168.168.83	168.95.1.1	3	3	ICMP	0	1	剧時盤測	P

圖表 131: 暫停 (Pause)

■ 繼續 (Resume):

回復事件列表的即時更新。按下『繼續』鍵,圖示隨即變為『暫停』鍵。

•													C
設備訊息	物件設定 防禦政策	夏 即時監測	1 報表設定	系統事件									
康表板 3	\$ 件 流量 利用率												
19910	時間	嚴重程度	設備	攻撃名稱	來源 IP	目的 IP	來源埠/	目的埠 /	通訊協定	VLAN ID	次數	攻撃反應	T
- 編練	時間 2006/08/23 10:3	嚴重程度 ●●	設備 IPS 2 (L	攻撃名稱 CHAT M	來源 IP 192.168.20.113	目的 IP 64.4.36.55	來源埠/ 1572	目的堆/ 1863	通訊協定 TCP	VLAN ID 0	次數 1	攻撃反應 即時監測▲	-
· 建拉 10 11	时間 2006/08/23 10:3 2006/08/23 10:3	旅軍役度 ●●	設備 IPS 2 (L IPS 1 (L	攻撃名稱 CHAT M CHAT Sk	來源 IP 192.168.20.113 142.179.15.60	目的 IP 64.4.36.55 192.168.13.15	來源埠/ 1572 57346	目的堆/ 1863 4942	通訊協定 TCP TCP	VLAN ID 0	<u>検</u> 数 1 1	攻撃反應 即時監測	-
10 11 12	時間 2006/08/23 10:3 2006/08/23 10:3 2006/08/23 10:3	#重程度 ●● ●●	説情 IPS 2 (L IPS 1 (L IPS 1 (L	攻撃名稱 CHAT M. CHAT Sk. CHAT Sk.	來源 IP 192.168.20.113 142.179.15.60 69.192.209.164	目的 IP 64.4.36.55 192.168.13.15 192.168.13.15	來原埠/ 1572 57346 56737	目的堆 / 1863 4942 4943	通訊協定 TCP TCP TCP	VLAN ID 0 0	<u>次數</u> 1 1	取擊反應 即時監測	

圖表 132: 繼續 (Resume)



■ 清除:

清掉列表中所有的事件資訊,重新開始顯示。

■ 過濾:

設定事件列表要呈現的事件欄位,如圖表 133。勾選畫面要顯示出來的事件 條件,如嚴重性、Port、種類、位址等。

0	過濾		2
┌[嚴重程度]────		[虛擬設備]	
☑輕微		🗹 IPS 1 (WAN)	
☑低度		IPS 1 (LAN)	
☑中度		IPS 2 (WAN)	
☑高度		IPS 2 (LAN)	
☑嚴重		IDS	
[攻擊種類]			
⊿ DoS/DDoS		 ✓P2P	
⊠ Buffer Overflow		⊠Instant Messenger	
Access Control		ĭ	
⊠ Scan		∎Porn	
🗹 Trojan Horse		⊠ Web Attacks	
ACL		ſ⊈Tunnel	
⊠ Mail		🗹 Stream Media	
File Transfer		dthers	
[來源]			
0.0	.0	.0 / 0	
(目的)			
0 .0	.0	.0 / 0	
確定	-	取消	

圖表 133: 事件列表過濾

9.3 流量 (Traffic)

即時呈現單一設備的流量圖,利用下拉式選單可以選擇顯示單一設備 (IPS 設備 或是 IDS 設備),如圖表 134 與圖表 135 所示。流量圖分成收到的封包流量 (Received Traffic)、丟棄的封包流量 (Dropped Traffic) 以及服務流量 (Service Traffic)。畫面每5秒鐘更新一次。

■ 收到封包流量顯示:

以第四層通訊協定為分類,可選擇要以封包數量 (Packet) 或是位元數量 (Byte) 為單位。不同的通信協定將以不同的顏色表示。



■ 丟棄封包流量顯示:

以第四層通訊協定為分類,可選擇要以封包數量 (Packet) 或是位元數量 (Byte) 為單位。不同的通信協定將以不同的顏色表示。



圖表 134: 流量一 (Traffic)

■ 服務封包流量顯示:

以第七層應用協定為分類,可選擇要以連線 (Connection) 或是位元 (Byte) 位單位。不同的服務將以不同顏色的線條顯示。



圖表 135: 流量二 (Traffic)

9.4 利用率 (Utility)

提供觀察硬體的核心處理器 (CPU) 及記憶體 (Memory) 的使用情況。畫面每5 秒鐘更新一次。







圖表 136: 利用率 (Utility)





本章說明

主要說明報表系統的設定操作步驟。

本章內容包含下列使用說明

章節	描述
10.1	事件報表 (Event List)
10.2	內建報表 (Predefined Report)
10.3	選擇查詢 (Query on Demand)
10.4	定期報表 (Schedule Report)

系統提供給使用者豐富的報表查詢系統介面,功能有:

- 事件列表 (Event List): 清楚紀錄網路安全的事件清單。
- 內建報表 (Predefined Report): 內建原廠提供的報表模型,供使用者快速選擇產生所需要的網路安全報表。
- 選擇查詢 (Query On Demand): 提供彈性化的介面參數選擇畫面,因應客戶 的特殊需求,提供豐富且足以滿足客戶的個性化報表。
- 定時報表 (Schedule Report): 提供自動化定期產出報表的能力,方便使用 者快速掌握網路安全事件。



圖表 137: 報表設定畫面



10.1 事件列表 (Event List)

利用滑鼠點選『事件報表 (Event List)』的圖示之後,系統會切換到事件報表的 視窗。

按鍵說明:

回到上一頁	С
	回到上一頁

			1	EMO管理系统客户	满				•
			NK6u	nder test (192-166	(168-205)				0
编录息	物件設定 防算	题家策 即時監測 報	表說定 系统事件						
V									
成新設作	\$:		2006/08/22		加赦	489,199			
IPS - IP	98.2	E.	ACL	0	Porn		0		
_			J Migh Alline ke	450 457	DePIDDeP	6.29	6		
八月	- ÷	2006-	H INCO MUSICKS	438,457	00000000	0,20			
Sun	Mon Tuo VVI	ad Thu Fri Sat	Buffer Overflow	58	scan	11	U		
	11 22	3 4 6	Trojan Horse	0	File Transfer		0		
li a di	7 8 9	10 11 12	Access Control	7,539	Mail		0		
10		17 10 12	P2P	620	Stream Media		0		
13	14 15 1	17 18 19	Inctant Maccanoor	2 266	Tunnal		0		
20	21 2	24 25 26	instant Messenger	3,200	(uniter		0		
27	28 29 30	31	VirusAvorm	U	Others	12,86	5		
朔: 2	006/08/22	亊件總數 : 489,	199 頁次: 1/4,892						
期: 2	006/08/22	◆件總數: 489,	199 頁次: 174,892	查詢頁數: 1					
149: 2 Att.	006/08/22 【 44 】 設備名質	事件總數: 489, (44) 时間	199 頁次: 1/4,892 >> >> >> 建塑名籍	查論頁數: 1 攻擊種類	攻撃反應	束源位址	來避迫	目的位址	目的
1月月: 2 ANL 1	006/08/22 (44) 設備名編 (PS 2	事件總數: 489, ▲▲ 助問 2008-08-22 00.00.	199 頁次: 1/4,892	查詢頁數: 1 攻擊種籍 Access Control	攻撃反應 別畔勧烈,記錄事件	東源位址 :192.168.30.84	來避地 2746	目的10地 84.233.186.19	目的 80
時日:2 自社: 1 2	006/08/22 建建名解 IPS 2 IPS 2 IPS 2	事件総数: 489, ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	199 頁次: 1/4,892	查詢頁數: 1 攻擊種類 Access Control DoS/DDoS DoS/DDoS	攻撃反應 別時監測: 記錄事件 別時監測: 記錄事件	来源位址 	來避地 2746 33765 22725	目的位址 84.233.185.19 239.255.255 250	80 1900
189: 2 ARE. 1 2 3	006/08/22 建建名稱 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2	事件総数: 489, ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	199 夏次: 1/4,892	重調頁数: 1 攻撃種類 Access Control DoS/DDoS DoS/DDoS DoS/DDoS	攻撃反應 (別時監測,記録事件 即時監測,記録事件 別時監測,記録事件 問時問題,記録事件	末源位址 :	來避地 2746 33765 33765 33765	Elétyixák 84 233 186 18 239 255 255 250 239 255 255 250 239 255 255 250	80 1900 1900
期:2 創建. 1 2 3 4 5	006/08/22 設備名解 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2	事件総数: 489, ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	199 頁次: 1/4,892 建築名質 14 POLICY Web Logn/Web Pos. 51 MISC UPNP maiformed abre. 51 MISC UPNP maiformed abre. 51 MISC UPNP maiformed abre.	空詞頁数: 1 攻撃種類 Access Control DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	攻撃反應 約時監測, 記錄事件 別時監測, 記錄事件 別時監測, 記錄事件 別時監測, 記錄事件	末源位址 - 162.168.30.84 - 100.0.254 - 100.0.254 - 100.0.254 - 100.0.254	來避地 2746 33765 33765 33765 33786	E890242 84 223 185 19 239 255 255 250 239 255 255 250 239 255 255 250 239 255 255 250	80 1900 1900 1900
時間: 2 自覚 1 2 3 4 5 6	006/08/22 設備名類 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2	事件接款: 489, ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	199 頁次: 1/4,892 建築名質 14 POLICY Web LoginWibe Poss. 51 MISC UPNP maformed abve. 51 MISC UPNP maformed abve. 51 MISC UPNP maformed abve. 51 MISC UPNP maformed abve.	査論頁数: 1 攻撃種類 Access Control DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	攻擊反應 川時監測, 記錄事件 川時監測, 記錄事件 川時監測, 記錄事件 川時監測, 記錄事件 川時監測, 記錄事件	末課位址 二 192.168.30.84 二 1000.254 二 1000.254 二 1000.254 二 1000.254 二 1000.254	來選峰 2746 33765 33765 33765 33766 33766 33767	Eźbitkał 64.233.185.19 239.255.255.250 239.255.255.250 239.255.255.255 239.255.255.255.250	80 1900 1900 1900 1900 1900
188: 2 ANE 1 2 3 4 5 6 7	006/08/22 建雄名類 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2	事件技数: 499, ●付用 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00		空読員数: 1 次単種語 Acress Control Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes	攻撃反應 用時監測,記錄事件 即時監測,記錄事件 用時監測,記錄事件 用時監測,記錄事件 即時監測,記錄事件 別時監測,記錄事件	末頭位址 1 6216833084 1000254 1000254 1000254 1000254 1000254 1000254 1000254	來選絕 2746 33765 33765 33766 33766 33766 33767	E890252 84 233 186,19 239 255,255 250 239 255,255 250 239 255,255 250 239 255,255 250 239 255,255 250 239 255,255 250	Eléte 80 1 900 1 900 1 900 1 900 1 900 1 900
1期: 2 角壁 1 2 3 4 5 6 7 8	006/08/22	#ffi8at: 489, #ffi8 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00 2008-08-22 00:00	199 Ty: 1/4,892	空読頁数: 1 文筆様移 Access Control DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS DoS/DDoS	29章 瓜應 即時監約, 12時事件 即時監約, 22時事件 即時監約, 22時事件 即時監約, 22時事件 即時監約, 22時事件 即時監約, 22時事件	東源位起 二, 162.198.30.84 二, 1000.254 二, 1000.254 二, 1000.254 二, 1000.254 二, 1000.254 二, 1000.254 二, 1000.254	来選峰 2746 33765 33765 33765 33766 33766 33768 33768	Ethix32 84.233.185.18 239.255.255.255 239.255.255.255 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.255.255	80 1900 1900 1900 1900 1900 1900 1900
1期: 2 角壁 1 2 3 4 5 6 7 8 9	006/08/22 建雄名類 IPS 2 IPS 2	新行総款: 498, 2006-08-22 00:00: 2006-08-22 00:00: 2006-08-22 00:00: 2006-08-22 00:00: 2006-08-22 00:00: 2006-08-22 00:00: 2006-08-22 00:00: 2006-08-22 00:00: 2006-08-22 00:00:	199 頁次: 1/4,892 199 頁次: 1/4,892 192 14 20LCYWeb Logn/Web Pos. 1415C UPKP mathemed abre. 11MSC UPKP mathemed abre.	空波員数: 1 次単様様 Access Control Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes	收擊反應 川中監測: 注於事件 川中監測: 注於事件 川中監測: 江於事件 川中監測: 江於事件 川中監測: 江於事件 川中監測: 江於事件	★源位址 := 162168.30.84 := 100.0.254 := 100.0.254 := 100.0.254 := 100.0.254 := 100.0.254 := 100.0.254 := 100.0.254 := 100.0.254	來讀地 2746 33765 33765 33766 33768 33768 33768 33768 33768 33768	Ethtysta 84.233.185.19 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250	80 1900 1900 1900 1900 1900 1900 1900 19
a號: 2 高號: 1 2 3 4 5 6 7 8 9 10	006/08/22 建雄名類 IPS 2 IPS 2	学行総訳: 409, ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		支援 支援 支援 支援 支援 支援 支援 支援 支援 支	22章反應 川和電源1 21章中中 川和電源1 21章中中 川和電源1 21章中中 川和電源1 21章中中 川和電源1 21章中中 川和電源1 21章中中 川和電源1 21章中中 川和電源1 21章中中	市 1621633084 - 1000254 - 1000254	來讀地 2746 33765 33765 33766 33766 33768 33768 33768 33768 33768 33769 33770	E8/y0.42 0.4.233.195.18 2.39.255.255.250 2.39.255.250 2.39.255.250 2.39.255.250 2.39.255.250 2.39.255.250 2.39.2	80 1900 1900 1900 1900 1900 1900 1900 19
3時間: 2 時間: 2 3 4 5 6 7 8 9 10 11 12	006/08/22 25/6 2 % 1PS 2 1PS 2 1P	学行総数: 489, 1006-08-22 00:00 2006-08-22 00:00	199 頁次: 1/4,92 19 20(2)(Yike) Logn/Web Por- 14 PCUCYWeb Logn/Web Por- 51 MISC UPKP materned above 15 MISC UPKP mater	空流貢数: 1 文型種植 Access Control DeS/DDeS DES/DDeS DES/DDES DES/DES/DES DES/DES DES/DES DES	20並反應 川田電気(注意中作 川田電気(注意中作 川田電気)(注意中作 川田電気)(注意中作 川田電気)(注意中作 川田電気)(注意中作 川田電気)(注意中作 川田電気)(注意中作 川田電気)(注意中作	東康位址 二 162.198.30.84 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254	末譜地 2746 33765 33765 33766 33766 33768 33768 33768 33768 33769 33770 33770	Edvica k 84.233.186.19 239.255.256.250 239.255.256.250 239.256.256.250 239.256.256.250 239.256.256.250 239.256.256.250 239.256.256.250 239.256.256.256 239.256.256 239.256.256.256 24	Bátja 80 1900 1900 1900 1900 1900 1900 1900 1
1 1 2 3 4 5 6 7 8 9 10 11 12 10 11 12 10 11 12 10 11 12 13 14 5 6 7 8 9 10 10 10 10 10 10 10 10 10 10	006/08/22 建雄名類 IPS 2 IPS 2	#ft88: 489, #f88	By Ty X: 1/4,92 Det Constraints Constate Constraints Constraints Cons	空話頁数: 1 文学雑誌 水空電話 水空電話 水空電話 などの などの	20 20 20 20 20 20 20 20 20 20 20 20 20 2	末課位起 末課位起 末課位起 1962168.30.84 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254	來請地 2746 33765 33765 33766 33766 33768 33768 33768 33768 33769 33770 33770 33770 337771 337771	Elbity3.34 64.233.186.18 239.256.256.26 239.266.256.265 239.266.265.265 239.266.265.265 239.265.265.265.265 239.265.255.265.265 239.265.255.255.255 239.265.255.255.255 239.265.255.255.255.255 239.265.255.255.255.255 239.255.255.255.255.255.255.255.255.255.25	80 1900 1900 1900 1900 1900 1900 1900 19
149: 2 1 2 3 4 5 6 7 8 9 10 11 12 13 14	006/00/22 25/\$ 6.14 1952 19	●件結案: 409, ●件結案: 409, ●1006-05-22 00:00 2006-05-22 00:00	199 頁次: 11/4,92 マン・ 19 マン・ 14 PCUCYWeb Logn/Web Pco 14 PCUCYWeb Logn/Web Pco 14 MSC UPFP matiomed abor 14 MSC UPFP matiomed abor 14 MSC UPFP matiomed abor 15 MSC UPFP matiomed abor	空話見数: 1 文学様誌 Access Control DeS/DDeS DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DDES DES/DES D	20年5月 20年5月 20年5月 20年5月 2015年 11日 2015年 2015年 11日 2015 2015年 11日 2015 2015年 11日 2015 2015年 11日 2015 2015年 11日 2015 2015 2015 2015 2015 2015 2015 2015	未添位址 末162:189.30.84 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254	來讀地 2746 33765 33765 33766 33766 33768 33768 33769 33770 33770 33770 33770 33770	Ethnold 64.233.186.19 239.255.256.250 239.255.256.250 239.255.255.250	80 1900 1900 1900 1900 1900 1900 1900 19
15 15 15 15 15 15 15 15 15 15 15 15 15 1	00600/22 2%\$4 4# 198 2 198	**件總數: 489, *********************************	199 頁次: 1/4,82 文理家有 14 POLICYWeb LogarWieb Poss 14 POLICYWeb LogarWieb Poss 15 MISC UPFP materned abre 15 MISC UPFP materned abre	空話見数: 1 文学様初 Access Control Des/DDes/Des Des/DDes/DDes Des/DDes/Des/Des/Des/Des/Des/Des/Des/Des	2920.08 (19452)1 (25374) (19452)1 (25374)	市道化地 192.108.30.84 1000.254	來調理 2746 33765 33765 33766 33766 33769 33769 33770 33770 33770 33771 33777 33777 33777 33775	Behyd al: 84.233.185.18 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255.255 239.255.255.255.255.255 239.255.255.255.255.255.255.255.255.255.25	Eéti 80 1900 1900 1900 1900 1900 1900 1900 1
188 2 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	00609/22 26/24 1982 1982 1982 1982 1982 1982 1982 1982 1982 1982 1982 1982 1982 1982 1982 1982	事件接載: 489, (その) (2006-08-22 00.00, 2006-08-22 00.00, 2006-08-22 00.00, 2006-08-22 00.00, 2006-08-22 00.00, 2008-08-22 00, 2008-08-22 00, 2008-08-20 00, 2008-08-200	199 東次: 114,952	主法に見た。 1 大学様は 1 たまりため したが したが したが したが したが したが したが したが	20葉反應 川田電影(注)(古事件) 川田電影(注)(古事件) 川田電影(注)(古事件) 川田電影(注)(古事件) 川田電影(注)(古事件) 川田電影(注)(古事件) 川田電影(注)(古事件) 川田電影(江)(古事件) 川田電影(江)(古事件) 川田電影(江)(古事件) 川田電影(江)(古事件) 川田電影(江)(古事件)	東源位址 192,198,30,84 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 1000,254 102,254 1000,254	末期4年 2746 33765 33765 33767 33768 33768 33768 33768 33768 33770 33770 33777 33777 33777 33777 33777 33777 2745 80	E89103.34 64.233.185.19 239.255.255.255.255 239.255.255 239.255 239.255.255 239	E80 1900 1900 1900 1900 1900 1900 1900 19
日明: 2 編鍵. 1 2 3 4 5 6 6 7 7 8 9 10 11 11 12 13 14 15 18 17	00600/22	第件接載: 489、 ● ● ● ● ● ● ● ● ● ● ● ● ●	199 東次: 1/4,892 シングの中の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の	主法員会:1 大で学校であった。 ちょうかした。 ちょうかん ちょうん ちょうん	22250 # 1945281 213740 1945281 213740	Triff (b)/c 102,163,30,84 1000,254 1000,354 1000,354 1000,354 1000,354 1000,354 1000,354 1000,354	末額地 2746 33765 33765 33765 33766 33768 33769 33769 33769 33770 33770 33770 33777 33777 33777 33773 2746 60 2745	Behydol: 64.233.185.18 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255.255 239.255.255.255 249.255.255.255 249.255.255.255.255 249.255.255.255.255.255 249.255.255.255.255.255.255.255.255.255.25	80 1900 1900 1900 1900 1900 1900 1900 19
■ 構築: 2	006009/22 2% 4% 1/98 2 1/98	第件接載: 489, ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	199 東次: 114,952	Exist Adv. 1 2:2:2:2:4:4 Desitioned Des	22章汉族 川田電烈 126年4月 川田電烈 126年4月	TIRON 192.168.30.84 100.0.254 100.0.254 </td <td>來避绝 2746 33765 33766 33766 33766 33768 33769 33770 33770 33770 33770 33777 33777 33777 33777 33773 23773 23773 2746 80</td> <td>E89Y03 34 64.233.185.19 239.255.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255 239.255.255.255 239.255.255 239.255.255 239.255.255 239.255.255</td> <td>80 1900 1900 1900 1900 1900 1900 1900 19</td>	來避绝 2746 33765 33766 33766 33766 33768 33769 33770 33770 33770 33770 33777 33777 33777 33777 33773 23773 23773 2746 80	E89Y03 34 64.233.185.19 239.255.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255.255 239.255 239.255.255.255 239.255.255 239.255.255 239.255.255 239.255.255	80 1900 1900 1900 1900 1900 1900 1900 19

圖表 138: 事件列表 (Event List) 畫面

10.1.1 虛擬設備 (Virtual Device)

使用者自行選擇想要顯示事件列表的虛擬設備名稱。虛擬設備的設定請參考 6.2 章節說明。

虛擬設備:	
IPS - IPS 2	
諸選擇一項設備	
IPS-IPS1	
IPS - IPS 2	
IDS - IDS	
IDS - IDS	

醫擇虛擬設備

10.1.2 月曆

選完設備後,使用者可自行選擇日期來顯示事件列表。以一天爲最小統計單位。



月曆上顯示紅色的日期表示該天有網路安全事件紀錄,可以被選擇,其餘則無。



圖表 140: 選擇日期

10.1.3 事件清單顯示

選擇完虛擬設備與日期之後,系統會搜尋資料庫並且把網路安全事件——顯示出來,右上方則是事件的統計資訊。使用者可以利用左右按鍵選擇換頁。

_									
0	-		NK6 u	nder test (192.168	1168.205)				
備訊息	物件設定「防禦	(政策 即時監護 報告	設定「系统事件						
V									
成領知	•		2006/08/22		總數:	489,199			
IPS - IP	PS 2	+	ACL	0	Porn		0		
nн	الترج ا	2006	Web Attacks	458,457	DoSIDDoS	6,28	5		
103		2000	Buffer Overflow	58	Scan	11	0		
Sun	Mon Tue VVe	o Thu Fri Sat	Traign Horno		Ello Transfor		0		
	1 2	3 4 5	nojan Hurse	0	rite mansier				
6	7 8 9	18 11 12	Access Control	7,539	Mail		0		
13	14 15 16	17 18 19	P2P	620	Stream Media		0		
20	31 20	1 14 1 1X 1 12 1	Instant Messenger	3,265	Tunnel		0		
20	21 20		VinisiWarm	0	Others	17.86	6		
Lanning P.	Country Associate Street	Gen Editoria (II)	+ C/ 19735						
[其]]: 21	006/08/22	李件锦载: 489,19	99 頁次: 1/4,892						
期: 21	006/08/22	李件铭数: 489,11	99 頁次: 1/4,892	查詢頁數: 1					
49: 21 492	005/08/22 【 【 設備名編	李件裕数: 489,19 (44) (时間)	93 頁次: 1/4,892	查論頁數 1 攻擊種類	波撃反應	來源位址	來運場	目的位址	目的
49: 21 492	005/08/22 	事件語数: 489,11 	39 頁次: 1 / 4,892 ▶ ▶ ▶ 秋型名類 4 POUCY Web LoginWeb Pos.	登論頁数 1 攻撃種類 Access Control	攻撃反應 即時監測, 記錄事件	來源位址 ,	來源場 2746	目的位址 64.233.185.19	目的 80
期日: 21 和12 2	005/08/22 建始名朝 IPS 2 IPS 2	李件總数: 489,11 → → 第間 2006-08-22 00 00:1 2006-08-22 00 00:5 2006-08-22 00 00:5	39 頁次: 1/4,892	室論頁数 1 攻撃種類 Access Control DeS/DDoS	攻撃反應 即時監測, 記錄事件 別時監測, 記錄事件	來順位址 	來2世地 2746 33765	目的位址 64.233.185.19 239.255.255.255	目的 80 1900
43: 21 ABE 1 2 3	006/08/22 設備名編 IPS 2 IPS 2 IPS 2 IPS 2	●け能数: 489,11 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	33 頁次: 1 (4,892 数型約4 4 POLICY Web LoginWeb Pos. MISC UPNF malformed adve. MISC UPNF malformed adve. MISC UPNF malformed adve.	空政百赦 1 攻撃種類 Access Control DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS	攻撃反應 即時監測:記錄事件 和時監測:記錄事件 即時監測:記錄事件	家原位址 	來這更堆 2746 33765 33765 33765	目的位述 64.233.185.19 239.255.255.250 239.255.255.260	80 1900 1900
期: 21 時間: 21 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	005/08/22 設備名編 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2	★/+ Heat: 489,11 ★489,11 ★489,11 ★100 2006.08.22.00.00;5 2005.08.20.00,5 2005.	33 頁次: 114,892 東京: 114,892 東京和福祉 4 POLICY Web LoginWeb Pos. MISC UPNF malformed adve. MISC UPNF malformed adve. MISC UPNF malformed adve.	宮油頁数 1 攻撃種類 Access Control DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS	取筆反應 即時限測,記錄事件 即時限測,記錄事件 即時限測,記錄事件 即時限測,記錄事件	来原位址 	來讓時 2746 33765 33765 33766 33766	目的位3上 64.233.185.19 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250	80 1900 1900 1900 1900
戦号: 21 開発 1 2 3 4 5 6	006/08/22 設備名編 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2	★/† //ext 489,11 ●/† //ext 489,11 ●/↑ 2006-08-22 00 00.1 2006-08-22 00 00.5 2006-08-22 00 00.5 2006-08-22 00 00.5 2006-08-22 00 00.5 2006-08-22 00 00.5 2006-08-22 00 00.5 2006-08-22 00 00.5	ag 真次: 1/4,892 建築名籍 4 POLICY Web Login/Web Pos. MISC UPNF malformed side. MISC UPNF malformed side. MISC UPNF malformed side.	空論百数 1 次学経経 Access Control DeS/DDoS DeS/DDoS DeS/DDoS DeS/DDoS DeS/DDoS DeS/DDoS	攻擊反應 即時股別, 記錄事件 即時股別, 記錄事件 即時股別, 記錄事件 即時股別, 記錄事件 和時報別, 記錄事件	末順位並 192168-30.84 10.0.254 10.0.0254 10.0.0254 10.0.0254 10.0.0254	家(原5年 2746 33765 33765 33766 33766 33766 33767	E80034 64,233,185,19 239,255,255,250 239,255,255,250 239,255,255,250 239,255,255,250	80 1900 1900 1900 1900 1900
1 2 3 4 5 6 7	006/08/22 	*(†1958): 409,11 2006-08-22 00 00:1 2006-08-22 00 00:5 2006-08-22 00 00:5 2006-08-22 00 00:5 2006-08-22 00 00:5 2006-08-22 00 00:5 2006-08-22 00 00:5	田子 114,892 田子 114,892 田子 114,892 田子 144,892 田 144,992 田 144,992 田 144,992 田 144,992 田 144,992 田 144,992	世法百般 1 次年経経 Access Control DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS	按单点库 即时能用: 記錄事件 用时能用: 記錄事件 即时能用: 記錄事件 即时能用: 記錄事件 即时能用: 記錄事件 即时能用: 記錄事件	東原位地 192168.30.84 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254	東道王章 2746 33765 33765 33766 33766 33766 33768	B00036 64.233.155.19 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250	目的 80 1900 1900 1900 1900 1900
H3: 21	006/08/22 25済名4 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2 IPS 2	*/filex: 489,11 */file 2006-08-22 00 00:1 2006-08-22 00 00:5 2006-08-22 00 00:5 2006-08-22 00 00:5 2006-08-22 00 00:5 2006-08-22 00 00:5 2006-08-22 00 00:5	ag 百次: 1/4,892 シンジン (14,892) シンジン (14,892) を見たいのでは、 はないのでは、 はないのでは、 はないのでは、 したいので、 したいのでは、 したいのでは、 したいのでで、 したいのでで、	空談頁象 1 次型種類 Access Control DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS DeS/DDeS	20 年50 度 即時間月、20 年年代 用時間月、20 年年代 用時間月、20 年代 用時間月、20 年代 用時間月、20 年代 用時間月、20 年代 用時間月、20 年代 用時間月、20 年代	東厚位址 192168.3034 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254	求证更非 2746 33765 33765 33765 33766 33766 33768 33768	目的位注 64.233.185.19 238.255.255.250 238.255.255.250 238.255.255.250 238.255.255.250 238.255.255.250 238.255.255.250	80 1900 1900 1900 1900 1900 1900 1900
H3: 21	006/08/22 設備名編 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2	*/+/## 489,11 */*********************************	B T ≪ 1/4,892	文学 は 大 なた なた なた なた なた なた の より した した した した した した した し	安装反席 104年2月12日本14 104年2月12日本14 104年2月12日本14 104年2月12日本17 104年2月12日本17 104年2月12日本14 104年2月12日本14 104年2月12日本14	末原位地 132168.30.34 - 100.0254 - 100.0254 - 100.0254 - 100.0254 - 100.0254 - 100.0254 - 100.0254 - 100.0254	來讀維 2746 33765 33765 33766 33766 33768 33768 33768 33768	Biblicitz 64.233.185.19 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260 239.255.255.260	目的 1900 1900 1900 1900 1900 1900 1900 190
期: 21 期理: 21 1 2 3 4 5 6 7 8 9 10	006/08/22 22/44/4 1PS 2 1PS 2	*#####: 489,11 *### 2006.08.22.01.00; 2006.08.20; 2006.08.20; 2006.08.20; 2006.08.20; 2006.08.20; 2006.08.20; 2006.08.	Type 1/4,892 System 2	室政育会1 水空などのIF00 De5/DDe5	20単反應 用时程息1,226年71 用时程息1,226年71 用时程息1,226年71 用时程息1,226年71 用时程息1,226年71 用时程息1,226年71 用时程息1,226年71 用时程息1,226年71 用时程息1,226年71 用时程息1,226年71	東原位北 192168.30.94 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254	жцёле 2746 33765 33766 33766 33768 33768 33768 33768 33769 33770	E89(03)2 64,233,185,18 238,255,255,250 238,255,255,250 239,255,255,250 239,255,255,250 239,255,255,250 239,255,255,250 238,255,255,255,255,255,255,255,255,255,25	80 1900 1900 1900 1900 1900 1900 1900 19
期: 21 期: 21 1 2 3 4 5 5 6 7 8 9 10 11	006/08/22 建建体化物 IPS 2 IPS 2 I	#F#1882: 489,11 #C #182 2006.08.22 00 00.1 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5 2006.08.22 00 00.5	Text 1/4.992 T	またすまた	安禁反應 (1) 4 4 5 4 5 4 5 4 5 4 5 4 5 4 5 5 5 5 5	東原位社 192188.3034 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254	來運炸 2746 33765 33765 33766 33766 33768 33768 33768 33768 33770	間的位地	80 1900 1900 1900 1900 1900 1900 1900 19
143: 21 12 3 4 5 6 7 8 9 10 11 12	006000/22 設備名稱 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2 IPS2	Strike 409,11 Image: 1 100-00-22 00 00-1 2006-00-22 00 00-1 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2 2006-00-22 00 00-2 2000-00-22 00 00-2	Try 1/4,992 Water Water Second Se		20 単反應 四十年3月、22 本部 中午2月、23 本部 中午2月、24 本部 中午2月、24 本部 中午2月、24 本部 中午2月、24 本部 中午2月、24 本部 中午2月 中午2日、24 本部 中午2日 中午2日、24 本部 中午2日 中午3日 中子3日 中子	末単位地 末日100.0264 100.0264 100.0264 100.0254 100.0254 100.0254 100.0254 100.0254 100.0254 100.0254 100.0254 100.0254 100.0254 100.0254 100.0264	來讓那篇 2746 33766 33766 33766 33768 33768 33768 33768 33770 33770 33770	890034 64.233 165 18 238.265 255 250 238.265 255 250	80 1900 1900 1900 1900 1900 1900 1900 19
143: 21 1 2 3 4 5 6 7 8 9 10 11 12 13	006000/22 設備名領 IPS2	Fifteen 409,11 ■ ■ 2006 06-22 00 001 2000 062 200 005 2006 06-22 00 005 2000 062 200 005 2006 06-22 00 005 2006 062 200 005 2006 06-22 00 005 2006 062 200 005 2006 06-22 00 005 2006 062 200 005 2006 062 200 005 200 006 2006 062 200 005 200 005 2006 062 200 005 200 005 2006 062 200 005 200 005 2006 062 200 005 200 005 2006 062 200 005 200 005 2006 062 200 005 200 005 2006 062 200 005 200 005	Role 11499 Role 1149	室政育会. 1 次学年4月 人をress Control Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes	20年5月 20日前日 2015年 2015 2015 2015 2015 2015 2015 2015 2015	末原位地 192188.3084 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254	求調報 2746 33765 33766 33766 33766 33768 33768 33768 33768 33770 33770 33777 33777		80 1900 1900 1900 1900 1900 1900 1900 19
(#3: 2) 692 1 2 3 4 5 6 7 8 9 10 11 12 13 14 	006/08/22 22/清希緒 IPS2	Strikes: 409,11 Image: Control of the strike strine strike strike strike strine strike strike strike	Tex: 114,992 T	空油戸会: 1 北学年経 クロジアクロジ クロジ クロジ クロジ クロジ クロジ クロジ クロジ クロジ クロジ	2845.8 Dete 91, 223, 844 Horsen, 223, 844 Horsen, 223, 844 Horsen, 223, 844 Horsen, 223, 844 Horsen, 223, 844 Horsen, 235, 845 Horsen, 235, 845 Hor	##fift# 102.168.30.34 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254 10.0.254	東道海 第746 第3765 第3765 第3766 第3766 第3768 第3768 第3768 第3770 第3778 第3777 第3777 第3777 第3777	800034 64.233.165.18 230.245.545.200 230.245.245.240 230.245.245.240 230.245.245.240 230.245.245.240 230.245.245.240 230.245.245.240 230.245.245.240 230.245.245.240 230.245.245.240 230.245.245.240 230.245.245.240	Eléty 80 1900 1900 1900 1900 1900 1900 1900 1
188: 21 12 3 4 5 6 7 8 9 10 11 12 13 14 15 12 13 14 15 10 10 11 12 13 14 15 10 10 10 10 10 10 10 10 10 10	2006/00/22 20 / / / / / / / / / / / / / / / / / / /	Fiftees 489,11 ■ ■ 2006 06-22 00 001 200 000-22 00 005 2006 06-22 00 005 2000 06-22 00 005 2006 06-22 00 005 2000 06-22 00 005 2006 08-22 00 005 2000 08-22 00 005 2006 08-22 00 005 2000 08-22 00 005 2006 08-22 00 005 2000 08-22 00 005 2006 08-22 00 005 200 006 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005 2006 08-22 00 005 200 005	TRX: 114.892 TV	室政育会. 1 次学種語 人を:ses Control Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes Des/DDes	20.单反体 [Date:34] 21.4本14 用加量24] 22.4本14 用加量24] 22.4本14	東原位地 192168.3034 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254 100.0.254	次(部) 第746 第765 第765 第765 第766 第766 第768 第768 第770 第3770 第3770 第3777 第3777 第3777 第3777 第3777 第3777 第3776	B0%032 64.233.185.19 239.295.255.250 239.295.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.255.250 239.295.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.255.250 239.255.250 2	80 1900 1900 1900 1900 1900 1900 1900 19
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 10 11 12 13 10 11 12 10 10 10 10 10 10 10 10 10 10	00600072 Big Anii IPS 2 IPS	High (1993) High (199	Tex: 1/4,992 T	2000 F 40:000 1 2000 F 40:000 0 0.62/000-65 0 0.62/000-65 0 0.62/000-65 0 0.62/000-65 0 0.62/000-65 0 0.62/000-65 0 0.62/000-65 0 0.62/000-65 0 0.62/000-65 0 0.62/000-65 0 0.62/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-65 0 0.63/000-	20. 单反压 10. 中化31, 21. 43. 中小 11. 12. 12. 12. 13. 23. 13. 13. 13. 13. 13. 13. 13. 13. 13. 1	##fift# 102.168.30.34 10.0.254 20.0.254 10.0.254 20.0.254 10.0.254 20.0.254 20.0.254 10.0.254 20.0.254 20.0.254 10.0.254 20.0.254		目的位法 64.233.185.19 (236.256.255.260 (236.256.255.260) (236.256.255.260) (236.256.255.260) (236.256.255.260) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.255.250) (236.255.250) (236.255.250) (236.255	80 1900 1900 1900 1900 1900 1900 1900 19
448: 21 448: 21 1 1 2 3 4 4 5 6 7 8 8 9 10 11 12 13 14 15 16 17 16 17	006/00/22 建備名第 1P8 2 1P8 2	Image: state Image: state 2000-08-22 00 001 2000-08-22 00 001 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005 2000-08-22 00 005	TAX: 114,902 T	200 0.0 1 XX25244 1 Access Control 0.65/DDo6 Do6/DDo6 0.65/DDo6 Do6/DDo6	20 10 10 10 10 10 10 10 10 10 10 10 10 10	末頃位生 192188.3084 1000.264 1000.264 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254 1000.254	水(野油 2746 33765 33765 33765 33768 33768 33768 33768 33768 33768 33770 33770 33770 33777 33777 33777 33777 33777 2746 80 2746	Bellyiúsia 1230,225,125,220 230,225,255,220 230,225,255,220 230,225,255,220 230,225,255,220 230,225,255,250 230,225,255,250 230,225,255,250 230,225,255,250 230,226,255,255,250 230,226,255,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,226,255,250 230,250,255,250 230,250,255,250 230,250,255,250 230,250,255,250 230,250,255,250 230,250,255,250 230,250,255,250 230,250,255,250 230,350,255,250	目約 80 1900 1900 1900 1900 1900 1900 1900 1

圖表 141: 事件列表顯示 (Event List)

10.2 內建報表 (Predefined)

利用滑鼠點選『內建報表 (Predefined』的圖示之後,系統會切換到內建報表的 視窗。

BroadWeb	web.com			NK600	0 使用毛冊
按鍵說明: ■ []	回到上一頁	0		111000	
	ELNS Server 1 (192.168.182.243) ELNS Server 1 (192.168.10.177) ELNS Server 1 (192.168.10.255) Action and rear (192.168.10.255) Action and rear (192.168.10.255) Action and rear (192.168.10.185) Amagenetic (192.168.10.185)	B26888 初日記定 約第65年 月66281 B26888 初日記定 約第65年 月66281 B26888 初日記定 約第65年 月66281 B2688 B2	SFF 構 NK-S under test (192, 168, 169, 205) WK-RE20E (本名中か)		
	設備期時): NetKooper 6000 設備当時: NetKooper 6000 設備当時: NetS Under test IPR先: 192168-86.05 設備収載 編集 融資時間: 14日 18.21.49 後心程式成本: 10.12 備証:	 総合納税 2000/09/22 総表 総合 約10名次年2月 約10名次年2月 約10名次年2月 第10名次年3月 第二位成場ける 東重位成場時る 	 総理時間 2006/09/22 総計 10 4 次学末源外目的 総計 10 4 次学本等 取学経済物計画 取学経済物分画 		

圖表 142: 內建報表 (Predefined Report)

10.2.1 類型 (Type)

使用者自行選擇想要顯示的事件類型,有兩大類型可供選擇,一是入侵防禦政策類 (IPS),一是防火牆連線控制類 (ACL)。

10.2.2 設備 (Device List)

選擇完類型後,使用者可自行選擇想要產出報表的虛擬設備。選擇後的虛擬設備 會出現在畫面右方清單當中。

10.2.3 時間 (Time)

選擇完類型、虛擬設備之後,使用者可以自行選擇想要製作報表的時間區間(以 天爲最小單位)。移動滑鼠游標到開始時間或是結束時間的方格中,月曆選擇畫面會自 動出現以供選擇。

10.2.4 報表 (Report)

選擇完類型、虛擬設備以及時間區間之後,使用者可以利用滑鼠選擇系統內建的 報表格式。



- 前 10 名攻擊來源 (TOP 10 Source): 依安全事件紀錄中的來源 IP 位址排 行,顯示前 10 名事件紀錄報告。
- 前 10 名攻擊目的 (TOP 10 Destination): 依安全事件紀錄中的目的 IP 位址 排行,顯示前 10 名事件紀錄報告。
- 前 10 名攻擊來源與目的 (TOP 10 Source & Destination): 依安全事件紀錄 中的來源 IP 位址與目的 IP 位址排行,顯示前 10 名事件紀錄報告。
- 前 10 名攻擊名稱 (TOP 10 Attacks): 依安全事件紀錄中的攻擊事件名稱排 行,顯示前 10 名事件紀錄報告。
- 嚴重程度統計圖 (Severity Statistics): 依安全事件紀錄中的嚴重程度產出統 計報告。
- 攻擊種類統計圖 (Category Statistics): 依安全事件紀錄中的分類程度產出 統計報告。
- 嚴重程度趨勢圖 (Severity Trend): 依安全事件紀錄中的嚴重程度產出趨勢 報告。
- 攻擊種類趨勢圖 (Category Trend): 依安全事件紀錄中的分類程度產出趨勢 報告。

10.2.5 內建報表範例 (IPS 類)

內建 IPS 類報表共有八種:前 10 名攻擊來源、前 10 名攻擊目的、前 10 名攻擊 來源與目的、前 10 名攻擊名稱、嚴重程度統計圖、攻擊種類統計圖、嚴重程度趨勢 圖以及攻擊種類趨勢圖。



圖表 143: IPS 類之內建報表

■ 前 10 名攻擊來源

列出累計前 10 名的來源位址,如圖表 144,利用長條圖顯示累計的數量。 如圖表 145,利用圓形圖顯示所佔的比例。圖示右方利用不同顏色代表 IP 位址。








圖表 145: 前 10 名攻擊來源圓餅圖

■ 前 **10** 名攻擊目的

列出累計前 10 名的目的地位址,各有長條圖 (圖表 146) 與圓餅圖 (圖表 147) 顯示。圖示右方利用不同顏色代表 IP 位址。



圖表 146: 前 10 名攻擊目的長條圖





圖表 147: 前 10 名攻擊目的圓餅圖

■ 前10名攻擊來源與目的

列出累計前 10 名的相同來源位址以及目的位址,各有長條圖 (圖表 148) 與 圓餅圖 (圖表 149) 顯示。圖示右方利用不同顏色代表成對的 IP 位址。





圖表 149: 前 10 名攻擊來源與目的圓餅圖



前 10 名攻擊名稱

列出累計前 10 名的攻擊種類,各有長條圖 (圖表 150) 與圓餅圖 (圖表 151) 顯示。圖示右方利用不同顏色代表不同的攻擊種類。



圖表 150: 前 10 名攻擊名稱長條圖



圖表 151: 前 10 名攻擊名稱圓餅圖

■ 嚴重程度統計圖

列出不同嚴重性等級的統計值,各有長條圖 (圖表 152) 與圓餅圖 (圖表 153) 顯示。圖示右方利用不同顏色代表的不同的嚴重性等級。



•

8

NK6000 使用手册 0 -Top N Chart Top N Informat Information 1,052 Serious 623 Top 1 - Top 4 Medium 3 1100 -1000 High 2 900 800 700 Count 600 500 400 300 200 100 0 Severity 圖表 152: 嚴重程度統計長條圖 Severity Statistics Top N Chartop N Information Information 1,052 Top 1 - Top 4 Serious 623 Medium 3 0% High 2



圖表 153: 嚴重程度統計圓餅圖

攻擊種類統計圖

列出不同攻擊種類的統計值,各有長條圖 (圖表 154) 與圓餅圖 (圖表 155) 顯示。畫面右方利用不同顏色代表攻擊種類。



圖表 154: 攻擊種類統計長條圖





圖表 155: 攻擊種類統計圓餅圖

■ 嚴重程度趨勢圖

利用曲線圖繪出不同時間點的攻擊數量,不同顏色的線代表不同的嚴重性等 級。可利用左右箭頭按鍵來控制所要看的時間點,左右箭頭按鍵中間可設定每次 移動的間隔。並可設定每個頁面顯示幾天的資料量,以及多久間隔劃一次節點。



圖表 156: 嚴重程度趨勢圖 (Severity Trend)

■ 攻擊種類趨勢圖

利用曲線圖繪出不同時間點的攻擊數量,不同顏色的線代表不同的攻擊種 類。可利用左右箭頭按鍵來控制所要看的時間點,左右箭頭按鍵中間可設定每次 移動的間隔。並可設定每個頁面顯示幾天的資料量,以及多久間隔劃一次節點。





10.2.6 內建報表範例 (ACL 類)

內建 ACL 類報告共有三種,前 10 名事件來源 (TOP 10 Source)、前 10 名事件 目的 (TOP 10 Destination)、前 10 名事件來源與目的 (TOP 10 Source & Destination)。報表內容及格式畫面與 IPS 類報表雷同,請參考 10.2.5 說明。



圖表 158: ACL 類之內建報表

10.3 選擇查詢 (Query on Demand)

利用滑鼠點選『選擇查詢 (Query On Demand)』的圖示後,系統會切換到選擇 查詢的視窗。



veb.com		NK6000 使用手册
₩ ₩	BEMS管理系统客戶構	
 BEMS Sever 1 (192.168.168.243) BEMS Sever 1 (192.168.04.0117) Danie (192.168.10.250) Mary (192.168.10.550) Rotical and the several se	Philis under test (192,163,163,265) R2株式R2 19/1号21: 55 第402年、月時報道書 11/1年232年、「新品書作 101 101 101 101 101 101 101 101 101 101 101 102 103 104 105 <tr< th=""><th></th></tr<>	
設備期刻: NetKeeper6000 設備規程: Ne-6105 設備を描: Ne-8105 設備な路: 連結 開始時間: 445 (163659 核心症実成年: 1.0.12 増証:	」目的思想: / / 255.255.255 合稿 信件 1: 記録年間 ▼ 值件 2: 記録年間 ▼ 備件 3: 記録目的 ▼	

圖表 159: 選擇查詢 (Query on Demand)



■ 🛃: 回到上一頁。

10.3.1 類型 (Type)

使用者自行選擇想要查詢的事件類型,有兩大類型可供選擇,一是入侵防禦政策類 (IPS),一是防火牆連線控制類 (ACL)。

10.3.2 設備 (Device List)

選擇完類型後,使用者可自行選擇想要產出報表的虛擬設備。選擇後的虛擬設備 會出現在畫面右方清單當中。

10.3.3 時間 (Time)

選擇完類型、虛擬設備之後,使用者可以自行選擇想要查詢紀錄的時間區間 (以 小時爲最小單位)。

10.3.4 查詢條件 (Query Conditions)

選擇完類型、虛擬設備、時間區間之後,使用者可以設定想要查詢的紀錄條件, 選擇完畢後按下『產生報表 (Generate)』按鍵即可產生報表。



- 來源 IP 位址 (Source IP): 輸入特定的事件來源 IP 位址, 使用者可以查詢 到特殊來源 IP 位址的事件紀錄。
- 目的 IP 位址 (Destination IP): 輸入特定的事件來源 IP 位址, 使用者可以 查詢到特殊目的 IP 位址的事件紀錄。
- 事件名稱 (Name): 輸入特定的攻擊事件名稱, 使用者可以查詢到特殊事件 的紀錄。
- 顯示順序條件 (Criterion):系統提供以上三相順序條件 (來源/目的/名稱) 可供選擇,產出的報表將依照此三項順序條件依序逐一顯示。

條件選擇完畢後,按下『產生報表 (Generate)』按鍵,系統會依照順序條件而產 生第一層查詢後的報表視窗。使用者可以再利用游標點選新視窗中列表裡面的欄位, 則可以繼續產生下一層的報表視窗。

10.3.5 選擇查詢範例 (IPS 類)

- 保護範圍:選擇設備清單,如圖表 160,利用中間的按鍵來選擇虛擬設備。
- 日期:點選圖中的日期方塊,會跳出如圖表 161 的日曆可供點選日期。

没備清單	指定設備	
IDS - IDS	IPS-IPS1	
IDS - IDS	IPS - IPS 2	

圖表 160: 選擇設備清單

•					0
March	₹÷				2006 ÷
Sun Mon	Tue	Wed	Thu	Fri	Sat
09		1	2	3	4
10 5 6	7	81	9	10	11
11 12 13	14	15	16	17	18
12 19 20	21	22	23	24	25
13 26 27	28	29	30	31	

圖表 161: 選擇日期

查詢條件:可設定使用者想要的條件,如來源位址、目的地位址等,如圖表
 162,按下『產生報表 (Generate)』即會產生查詢報表。



	1	255.255.255.255	
	1	255.255.255.255	
			:
攻擊名稱	-	產生報表	-
攻擊來源	-		
攻擊目的	•		
	文字名稱 文字本源 文字目的	□ · · · □ · · · 反擊名類 · · 反擊不原 · 反擊目的 ·	/ 255.255.255.255 / 255.255.255.255 / 255.255.255 / 255.255.255 / 255.255 / 文學名稱 文學目的

圖表 162: 查詢條件

查詢報告畫面如圖表 163,上方長條圖顯示不同種類的累計值,左下方有不同種類的排名,右下方為特定攻擊種類當中的詳細事件列表。圖示的上方有按鍵可更換顯示圖形,如圖表 164,利用原型比例圖來展現不同種類所佔的比例。

000 000 🔦 🔐 😸 Top 1 - Top 10 2006/02/28 00:00 - 2006/03/01 12:59 800 700 600 600 400 Bad TCP State CMP Unexpecte Dad TCP Windo Diver Ping Died TCP (300 200 100 . Name Use Bad TCP State Others ICMP Unexpecte Others rate Unexpecte Others others Source # 61.222.12.226 211.21.177.75 140114.07.32 211.21.177.76 222.122.26.172 220.165.4.114 163.20.237.129 221.302.124.149 211.21.177.34 210.944.31.140 220.95.230.125 222.88.88.189 Category Seventy Count Rank Rank 167 * 91 99 64 60 56 28 28 21 21 20 16 13 905 Ind TCP State ICMP Unexpette ICMP Unexpette Bad TCP Window Over Ping Length Bad TCP Check TCP Weind Overl UDP Smurf 153 149 18 Others Others Others Others DoS/DDoS em. Bad TCP Flag 222.88.88.182 202.68.195.73 12 De

查詢的結果並可列印成網頁檔 (HTML),進一步儲存或是匯出,如圖表 165。

圖表 163: Query on Demand 長條圖



圖表 164: Query on Demand 圓餅圖



Name NetKeeper Device IP : NK-6



圖表 165: 列印查詢報表

10.4 定期報表 (Schedule Report)

除了提供豐富的報表供查詢外,另外系統也提供定期寄送報表的功能。使用者可以利用滑鼠點選『定期報表 (Schedule Report)』的圖示後,系統會切換到定期報表的視窗。



圖表 166: 定期報表 (Schedule Report)



排程工作列表顯示所有已經建立的排程工作,每一列顯示該排程工作目前的狀 態。如果排程工作未被啓用,則會以淺灰色顯示。

點選排程工作列表中的排程工作,下方排程工作資訊頁面會顯示被點選工作的詳 細設定資訊。

按鍵說明:



10.4.1 排程工作

排程工作用來定期產生報表,藉由產生多份排程工作,用戶能定義出不同時間範 圍匯整而成的報表。每一個排程工作都有自己獨立的設定值而不會互相影響,用戶能 更簡單地定義出自己需要的定期報表。

在排程工作列表右邊的工具列用來管理排程工作,用戶能新增,編輯和刪除排程工作。

マ花费时间	-
90	4
	10

圖表 167: 排程工作管理工具列

排程工作設定介面第一頁,需要設定的欄位如下:

- 排程工作
 - ◆ 啓動排程工作: 若未啓動排程工作,則該工作將不會執行。
 - ◆ 排程工作名稱: 建議使用容易表達出該工作意圖的文字當作排程工作名 稱。
- 設定排程類型
 - ◆ 排程類型:若選擇循環產生報告,排程工作將會定期產生報告。若選擇
 只產生一次報告,排程工作在第一次產生報告後便停止執行。
 - ◆ 時間範圍:決定資料的時間範圍。循環報告也會利用時間範圍決定出下
 一次的執行時間。
- 設定執行時間:設定排程工作下一次的執行時間。
- 虛擬設備:選取要產生報告的虛擬設備清單。



報表:點選編輯報表樣本選取預設報表樣本或使用者自訂樣本。一個排程工作可以選取多個報表樣本。

🔞 編輯排程工作	0
~[排程工作]	
密動排程工作 资格 图 资格 图 资格 图 资格 图 资格 资格	
排程工作名稱	
[設定排程類型]	
排程類型 通循環產生報告	☑只產生一次報告
時間範圍 💽小時: 1	○日: 1 💌
□週報	◎月報
執行時間 年: 2008 ÷ 月: 3 ÷	日: 18 - 小時: 14 -
[虛擬設備]	
諸選擇欲查詢的虛擬設備	已選擇查詢的虛擬設備
IPS-IPS1(LAN)	
IPS - IPS 1(WAN)	
IPS - IPS 2(LAN)	
IPS - IPS 3(WAN)	
[報表])
編輯報表様本	
取消	下一步 > 確定

圖表 167: 新增/編輯排程工作(頁面一)

- 輸出檔案
 - ◆ 儲存檔案格式:使用者可以決定產生的檔案格式。一個排程工作不能同時產生多種格式的報告檔案。
 - ◆ 檔案名稱格式:系統能自動在檔案名稱後面加上時間字串。
 - ◆ 檔案名稱:產生報告檔案的名稱。
- 收件者:定義自動報表所要傳送的使用者,以及傳送的方式。系統提供了利用 E-mail 的模式或是 FTP 的模式來儲存報表。
 - ◆ 啓動 E-mail 模式:需填寫收件者的郵件地址。
 - ◆ 啓動 FTP 模式: 需填寫:
 - ◆ FTP 伺服器: FTP 伺服器 IP 位址。



- ◆ 使用者名稱: FTP 伺服器登入使用者名稱。
- ◆ 密碼: FTP 伺服器登入密碼。
- ◆ 上傳目錄: 指定檔案上傳的的目錄所在。
- 預覽:此功能提供給使用者在設定完畢定期報表的產生格式之後,可以先利用此介面產生暫時性的報表進行檢查,也可以把該報表先存到系統的硬碟當中。請使用者選擇產生報表的起始時間、結束時間、以及存檔的檔名及位置後,按下『製作 (Generate)』即可產生報表存檔供使用者檢查。

0	編輯排程工作		0
-[輸出檔案]			
儲存檔案格式 💽 HTML	_ OPDF	OCSV	
檔案名稱格式 🕑自動命	命名(檔案名稱+日期)	○固定名稱	
	檔案名稱		
[收件者]			
图格用郵件通知			
			-
			11
			_
FIP 伺服器 U			
使用者名稱			
密碼			
上傳目錄			
従 年:	2008 - 月: 3 -	日: 18 小	時: 12 -
到 年: []	2008 月: 3 日	日: 18 小	時: 12
Głaz Zukar			
	Cocuments and SettingSKP-L		
取消	1 《上一步 1	下一步 > 1	旋
	表 168: 新增/編輯排利	程工作(百面二)	

正確輸入以上兩頁面的欄位後,選擇確定即完成編輯排程工作。



10.4.2 報表樣本

報表樣本將彙集成的原始資料,轉換成有特殊意義的統計資料,透過統計資料能 讓用戶更快找出有意義的資訊。每一個計畫工作可以指派多種報表樣本,除了系統內 建的報表樣本外,用戶也可以定義自己的報表樣本。

10.4.2.1 管理報表樣本

管理報表樣本介面如下圖表,透過右邊的工具列來建立或刪除用戶自訂的報表樣 本,系統預設的報表樣本不能被刪除。

上方頁面顯示已經加入計畫工作的報表樣本。

下方頁面顯示系統預設報表樣本的細部設定,比如選擇 Category Trend,則下方 頁面呈現要顯示在報表上的攻擊種類。

•	管理報表様本
~[様本]	全部選取 全部取消
	Top-N Source IPs Top-N Destination IPs Top-N Rules Severity Statistics System Log Category Statistics Severity Trend
N = [10 🕂 (最小值:10 最大值:100)
	確定 取消

圖表 169: 管理報表樣本

選擇好想要加入計畫工作的報表樣本後,按下確定即完成。

10.4.2.2 建立報表樣本

透過右邊工具列,使用者可以新增/編輯使用者自訂報表樣本。

- 樣板名稱:代表此報表樣版的名稱,使用者自行定義。
- 描述:此模組的說明,內容由使用者自行定義。
- 選擇欄位: 可供選擇的有:



- ◆ IPS/ACL: 資料庫中紀錄的事件型態。
- ◆ 選擇顯示在報表內的欄位。
- 限制條件:用來篩選事件的條件。
 - ◆ 名稱: 指定特定的名稱,可選擇等於或是不等於。
 - ◆ 來源位址:指定特定的來源 IP 位址,可選擇等於或是不等於。
 - ◆ 目的位址:指定特定的目的 IP 位址,可選擇等於或是不等於。
 - ◆ Group By 依照所選條件完成群組。
 - ◆ Order By: 依照所選條件排序。
 - ◆ Dsecend: 選擇後由大到小排序,如未選擇則採取由小到大排序。
 - ◆ Filter By Action: 根據政策反應設定來篩選出符合的事件。
 - ◆ Limit: 限制資料筆數。

)		新	增報表様本		
羕板名稱					
苗述					
-[選擇欄)	位)				
🕑 IPS	🖸 全部	🖸 名稱	🖸 來源位址	🖸 目的位址	
OACL	日時間	🖸 來源埠	🖸 目的埠	🖸 總數	
[限制條]	件]				
🖸 名稱		相等			>
🖸 來源位	址	相等 🔻			
🖸 目的位	址	相等			
🖸 Group	ву	修改			
🖸 Order	Ву	修改	DESC		
🖸 Filter I	By Action	 通過 			
		◯丢棄封包	日中間	液源端 🖸	中斷目的端
		🕘 即時監測			
		🔲 使用電子	郵件警告		
		🖸 記錄事件	不記錄	封包	-
🖸 Limit		[1 🕂 紀錄
			≠ :] [:	Bracker []	
		確入	E	取消	

圖表 170: 新增編輯報表樣本

用戶設定好參數後,按下確定即完成新增報表樣本。



11 第十一章 系統記錄

本章說明

主要說明系統紀錄 (System Log) 的介面。

本介面顯示系統操作紀錄。NK6000 設備開機完成並且連線 BEMS 伺服器成功之後,NK6000 設備會自動將系統記錄傳送到 BEMS 伺服器,系統運作以及設定操作相關的紀錄將儲存於 BEMS 伺服器的資料庫當中。客戶端的畫面如下:

11.112管理系统管户请	00
茶該事件總數: 4 1 ~ 4	
1 2006-06-21155901 (Highs POLCY, ACENT SEE TWA (BESS) 52:06160.226 2 2006 06-21155901 (Highs) (Highs POLCY, ACENT SEE 2018/H 1998) (Highs) 3 2006 06-21155901 (Highs POLCY, ACENT SEE 2018/H 1998) (Highs) 4 2006 06-21153911 (Highs) POLCY, ACENT SEE 2018/H 1998 (1000)	
	Notiounderstadt, 022188.10.0200) RASKAL, Phylodize, Rinkskal, Handszel, Rinkskal, Phylodizer, Rinkskal, Handszel, Rinkskal, Handszel, Rinkskal, Phylodizer, Ademin, Kardiszkal, Handszel, Rinkskal, Handszel, R

圖表 171: 系統訊息 (System Log) 視窗

頁面顯示及功能說明如下:

- 類型 (Type):
 - ◆ 無效的 (INVALID): 設備傳遞訊息為無效訊息。只要設備傳遞的訊息不 是屬於 INFO/WARN/URGEN 以上三種類型,將會被歸屬於無效的訊息。
 - ◆ 系統事件資訊 (INFO): 主要紀錄 BEMS 系統本身的設定修改,或是 IPS 設備的設定修改,或是使用者登入登出等等使用者想要看到的訊息。訊息 (INFO) 顯示均不會影響 BEMS 系統本身或是 IPS 設備的運作。
 - ◆ 系統警告 (WARN): 主要反應可能出現影響系統本身運作的警告,例如 因為使用者的操作而停止服務,導致操作畫面無法順利顯示的情形。警 告 (WARN) 顯示使用者看到的可能出現問題,但是並不影響整個 BEMS 系統的運作。
 - ◆ 系統緊急 (URGEN): 主要反應出已經會影響 BEMS 系統運作的錯誤操 作。例如系統某些主服務已經因爲程式錯誤執行而停止運作等等訊息。



- 時間 (Time): 顯示系統紀錄的時間,預設值是由 NK6000 系統開機連線 BEMS 伺服器後的時間起算,一直紀錄到目前的時間為止,此時間主要取決 於資料庫的儲存能力。資料庫 (例如: MySQL) 的空間愈大,則可以紀錄的 資料就愈多,時間就愈久遠。
- 來源 (Source): 顯示操作記錄的來源。
 - ◆ SSH User: 使用 SSHv2 連線的操作紀錄。
 - ◆ Console: 利用 Console 連線的操作紀錄。
 - ◆ System: 系統本身運作的紀錄。
 - ◆ Policy Engine: 防禦政策引擎運作的紀錄。
- 訊息 (Message): 描述系統記錄的內容。

工具列按鍵說明:

 Implication

 Implication





12 第十二章 NK6000 Console

本章說明

主要說明 NK6000 Console 介面功能與操作步驟。

本章內容包含下列使用說明

章節	描述	
12.1	登入 Console 介面	
12.2	求助命令	
12.3	操作功能鍵	
12.4	系統 (System) 功能	
12.5	設備 (Device) 功能	

12.1 登入 Console 介面

於登入提示出現後,如圖表所示,輸入帳號/密碼『admin / admin』,即可進入 NK6000的 Console 介面。

login: admin Password: _			

圖表 172: 登入 (Login) 畫面

NK6000 Console 介面如下圖表所示,上方黑色橫桿為功能列,中間為主視窗, 下方黑色橫桿為可用功能的快捷功能列。在功能列顯示有系統 (System) 選單、設備



(Device) 選單與日期。主視窗中顯示有 NK6000 韌體 (BroadWeb NK Kernel)、防禦 政策 (Signature) 等等的版本資訊、系統負載、網路設定及相關資訊。快捷功能列顯 示有目前視窗可用的功能及系統時間。

 Image: System <D>evice
 03/09/06

 NK6000 (c) 1999-2006 Broadweb Corp.
 Kernel 1.0.7; Sigature: 4.12

 Running 0 days 1 hours 25 mins; 2 user(s) logged on
 CPU Util.: 0%; Throughput: 0 Mbps; TCP connections: 0/512000

 Memory: 376,044 KB free, total 1,302,168 KB
 HD: 28,223 MB free, 5 GB used, total 34 GB

 IP: 192.168.10.1; Netmask: 255.255.0.0; Gateway: 192.168.1.1

 HA: 192.168.10.2; DNS: 192.168.20.1; BEMS: 192.168.0.2

 TCP idle time limit: 20 seconds

 Maximum 1000 logs in 5 seconds

 (S>System <D>Device <F1>Help <Esc>Exit

圖表 173: Console 介面

12.2 求助命令 (Help) 🗈

當使用者對於 Console 介面不熟悉或疑惑時,可利用此功能查詢操作方法。在快捷功能鍵列出現 <F1>Help 字樣時,即可按下按鍵,取得求助資訊,如下圖,Arrow Key、Enter、Esc 為操作功能鍵,詳細說明請參考 12.3 操作功能鍵。Underlined character 為功能列或快捷功能列上,字元有底線者,其作用在於快速切換至該選單或該功能。

< <mark>S</mark> >ystem <	>evice 03/06/06
Arrow Key	= Highlight a menu: menu option or item in a list box = Move within a menu. = Select item in group.
Enter	= Activate a highlighted menu option.
Esc	= Cancel.
Underlined	= Accelerator key.
character	= Move directly to menu, option or another field.
	Press any key to continue.
K <u>Esc</u> >Exit	13:11

圖表 174: 求助 (Help) 畫面



12.3 操作功能鍵

NK6000 Console 操作方式非常容易上手,介面以視窗方式呈現,以鍵盤操作。 其操作功能鍵如下:

Ť↓← →	方向鍵: 移動並選取「功能列」選單中的選項。
Enter	Enter 鍵:執行已選取的選項。
Esc	Esc 鍵: 取消。

12.4 系統 (System)功能群組 🗈

此功能群組為系統相關資訊與設定。在主畫面下按下按鍵,可以移動至系統 (System)功能群組,選單選項有:

- All Status (系統狀態):顯示系統硬體設備狀態資訊與各埠狀態資訊。
- Log (事件紀錄):顯示系統事件記錄。
- Password (變更密碼): 變更管理者密碼。
- Reset Config (還原設定): 還原設定値成原廠出廠設定値。
- Stop System (停止系統):停止 NK6000 運作並且關機。
- Reboot (重新啓動):將 NK6000 重新啓動。

KS>vstem KD>evice All Status Log Password Reset Config Stop System Reboot
< <u>A</u> >All Status <l>Log <p>Password <e>Reset <s>Stop System <r>Reboot <esc>Exit 15:42</esc></r></s></e></p></l>

圖表 175: 系統 (System) 功能選單

BroadWeb

NK6000 使用手册

12.4.1 系統狀態 (All Status) 🚹

此功能顯示系統軔體版本、硬體設備狀態資訊與各連線埠的狀態資訊。在 System 功能選單中以方向鍵或快捷鍵 A 移動到此選項並按 J Enter 鍵,即可執行此功能。 此功能執行中可按 鍵返回上層或按 2 鍵、 2 鍵跳至功能選單。其畫面如下, 在此畫面中顯示的:

- 版本資訊: NK6000 核心版本為 1.0.7、特徵檔案版本為 4.12。
- 迄今運作時間:0天1小時26分;目前有兩位使用者登入。
- 系統效能資訊: CPU 使用率為 0%、檢測效能為 0Mbps、目前存在 TCP 連線 0 筆、最大允許 TCP 連線數 512,000 筆
- 儲存媒體資訊:記憶體剩餘 376,044KB,總共 1,302,168KB、儲存空間剩餘 28,223MB,已使用 5GB,總共 34GB。
- 網路設定: IP 位址為 192.168.10.1、網路遮罩為 255.255.0.0、開道器為 192.168.1.1、對應的 HA 主機: 192.168.10.3、DNS 伺服器為 192.168.20.1、 BEMS 伺服器為 192.168.0.2。
- 控管之網路資訊: TCP 連線閒置時限 1800 秒、最大事件記錄每 5 秒 1000 筆。



圖表 176: 系統狀態 (All Status) 畫面-1

此時按下任意鍵以繼續顯示下頁。如下圖所示,第二頁顯示 NK6000 各個連接埠的設定值,主視窗中上方橫列的項目有 Port 0 ~ Port 6,為 NK6000 中的七個連接埠的埠號;左側縱列的項目有:

■ Mode: 連接埠的偵測模式設定。



- Link: 連接埠的連線速率,有 AUTO (自動偵測速率)、10H (10Mbps 半雙工)、10F (10Mbps 全雙工)、100H (100Mbps 半雙工)、100F (100Mbps 全 雙工)、100F (1000Mbps 全雙工)。
- Policy Bypass:系統偵測網路封包時,是否忽略 Policy (偵測政策)的設定, on 為忽略。
- State Bypass: 系統偵測網路封包時,是否忽略 State (連線狀態)的正確 性, on 為忽略。
- Integrity Bypass:系統偵測網路封包時,是否忽略 Integrity (網路異常使用) 之封包, on 為忽略。
- Fragment Bypass: 系統偵測網路封包時,是否忽略 Fragment (切割) 之封 包, on 為忽略。
- VPN Bypass: 系統偵測網路封包時,是否忽略 VPN (虛擬私人網路), on 為 忽略。
- ACL Bypass: 系統值測網路封包時,是否忽略 ACL (存取控制清單)的設定, on 為忽略。
- PortScan Bypass:系統偵測網路封包時,是否忽略 PortScan (連接埠掃描 攻擊), on 為忽略。
- GRE Bypass: 系統偵測網路封包時,是否忽略 GRE 通信協定的連線, on 為忽略。

< <mark>S≻ystem <</mark> D≻evice NK6 Port Map Confi	guration	is:					03/06/0
	Port Ø	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Mode Link Policy Bypass State Bypass Integrity Bypass Fragment Bypass VPN Bypass ACL Bypass PortScan Bypass GRE Bypass	IPS-M AUTO off off off off off off off	IPS-M AUTO off off off off off off off	IPS-M AUTO off off off off off off off	IPS-M AUTO off off off off off off off	IDS-M AUTO off off off off off off off	IDS-M AUTO off off off off off off off	Manage Auto N/A N/A N/A N/A N/A N/A N/A N/A
< <u>Esc</u> ≻Exit	<< Pres	s any ke	y to ref	resh. >>	-		14:3

圖表 177: 系統狀態 (All Status) 畫面-2

此時按下任意鍵均可顯示更新後的系統資訊。



12.4.2 事件記錄 (Log) 此功能顯示系統事件記錄。在 System 功能選單中以方向鍵或快捷鍵 移動到 L Enter J Enter 鍵,即可執行此功能。執行中可用空白鍵或 此選項並按 鍵更新記 D 键跳至功能選單。此功能書面如下: 錄, 鍵返回上層或按 03/08/06 <<mark>S</mark>>ystem <D>evice 2006/03/08 11:57:19 I:CON:Change policy server IP address to 192.168.0.2 2006/03/08 11:58:37 I:PSS:Change PORI [2] function check configure. 2006/03/08 12:52:20 I:PSS:Change PORI [2] function check configure. 2006/03/08 12:52:21 I:PSS:Change PORI [3] function check configure. 2006/03/08 12:52:21 I:PSS:Change maximum number of log events to 1000 OK. 2006/03/08 12:52:21 I:PSS:Change log transfer interval to 30 seconds. Event level => I :Info, W : Warning, U : Urgent, F : Fatal Event source => CON : Console, SSH : SSH, SYS : System, PSS : Policy agent. << Press Space or Enter to refresh. >>_ <<u>Esc</u>>Exit 12:53

圖表 178: 事件記錄 (Log)

如圖中所示,NK6000的事件紀錄的格式為:

- 年/月/日: yyyy/mm/dd。顯示記錄日期。
- 時/分/秒: hh/mm/ss。顯示記錄時間。
- 事件等級: Event level。顯示事件記錄等級。
- 事件來源: Event source。顯示事件記錄發生來源。
- 訊息內容: Message。顯示事件記錄之內容。

事件等級區分: 資訊 (I:Info), 警告 (W:Warning), 緊急 (U:Urgent), 致命 (F:Fatal)。

事件來源區分: 操縱臺 (CON:Console), SSH 連線 (SSH:SSH), 系統 (SYS:System), 政策精靈 (PSS:Policy agent)。

12.4.3 變更密碼 (Password) [Password]

此功能用以變更管理者密碼。在 System 功能選單中以方向鍵或快捷鍵 — 移動



到此選項並按 ^{→ ■} 鍵,即可執行此功能。首先系統會提示輸入原本的密碼,確認 後會提示輸入新密碼,系統將會再確認一次新密碼,變更成功即出現『Password changed successfully!』字樣,失敗則出現『Password mismatch』字樣。此功能畫 面如下:



圖表 179: 變更密碼 (Password) 畫面

12.4.4 還原設定 (Reset Config) [

此功能可還原設定値至原出廠値。在 System 功能選單中以方向鍵或快捷鍵 移動到此選項並按 · Enter 鍵,即可執行此功能。執行後系統會詢問是否還原設定, 按 鍵確定還原;按 ^N鍵或 ^{Esc} 鍵保留目前設定,預設爲保留目前設定。此功能 畫面如下:





12.4.5 停止系統 (Stop System) [[®]

此功能爲停止 NK6000 運作,並關機。在 System 功能選單中以方向鍵或快捷鍵



鍵確定停止,當停止後,出現如下圖『You may 執行後系統會詢問是否停止,按 turn off power new』字樣,即可關掉主機電源;按[▶]鍵或[▶]鍵繼續運作,預設為 繼續運作。





圖表 182: 停止系統 (Stop System) 畫面-2

12.4.5 重新啓動 (Reboot) 🔳

<<u>Esc</u>>Exit

此功能爲重新啓動 NK	K6000。在 System 功能選單中以方向鍵或快捷鍵	移動
到此選項並按 🗝 Enter 鍵	,即可執行此功能。執行後系統會詢問是否重新啓認	勆,按
▲ 鍵確定重新啓動;按【	▶ 鍵或 鍵繼續運作,預設為繼續運作。此功能	畫面如
下:		
< S ≻ystem < D ≻evice	03/06/06	Ĩ

Are you sure you want to reboot? (y/N)_

圖表 183: 重新啓動 (Reboot) 畫面

17:26



12.5 設備 (Device) 功能群組 🖻

此功能群組用以設定設備的網路設定值,並含有 PING 工具以供使用這測試網路

設定。在主畫面下按下 建,可以移動至 Device 功能群組,選單選項有:

- IP (網路位址):設定 NK6000 的網際網路地址。
- Netmask (網路遮罩): 設定 NK6000 的網路遮罩。
- Gateway (閘道器):設定 NK6000 經由何者 Gateway 連接至外部網路。
- DNS (網域名稱伺服器):設定 NK6000 使用何者 DNS 伺服器。
- TCP timeout (TCP 連線逾時時間): 設定經由 NK6000 的 TCP 連線逾時限 制。
- Max. Log (最大系統事件記錄數量): 設定 NK6000 最多存放的系統事件記錄數量。
- BEMS Srv. (BENS 伺服器): 設定 NK6000 歸屬於何者 BEMS 伺服器所管 控。
- Port Config (連接埠設定): 設定 NK6000 各個連接埠。
- HA (High Availability):設定本機 High Availability 連接埠對應的 NK6000 設備 IP 位址。
- VLAN ID (虛擬網路編號):設定 NK6000 所屬的虛擬網路編號。
- PING: 網路連線測試工具。

選項的功能操作在往後各個子節將詳細介紹。



圖表 184: 設備 (Device) 功能選單





圖表 186: 網路位址 (IP) 再次確認變更

10:29



12.5.2 網路遮罩 (Netmask) 🔳

此功能爲設定NK6000的網路遮罩∘在Device功能選單中以方向鍵或快捷鍵

移動到此選項並按 ,即可執行此功能。此功能畫面如下:



圖表 187: 網路遮罩 (Netmask) 畫面

執行時會顯示目前網路遮罩設定,直接輸入欲變更的網路遮罩再按^{↓▲ Enter} 〕鍵, 系統將再次詢問變更與否,按[♥] 鍵確定變更網路遮罩設定;按[№] 鍵或^{Esc} 鍵則不 變更,預設為不變更。



圖表 188: 網路遮罩 (Netmask) 再次確認變更



12.5.3 閘道器 (Gateway) 🕒

此功能為設定 NK6000 經由何者閘道器連接至外部網路。在 Device 功能選單中

以方向鍵或快捷鍵 移動到此選項並按 ,即可執行此功能。此功能畫面 如下:



鍵,系統將再次詢問變更與否,按[→]鍵確定變更閘道器設定;按[→]鍵或[∞]鍵則 不變更,預設為不變更。

< <mark>S</mark> ≻ystem <d>evice</d>	03/08/06
Device gateway: 192.168.1.123	
Hre you sure you want to change gateway? (y/N)_	
	10:38



圖表 190: 閘道器 (Gateway) 再次確認變更

12.5.4 網域名稱伺服器 (DNS) 🖻
此功能為設定 NK6000 經由何者閘道器連接至外部網路。在 Device 功能選單中
以方向鍵或快捷鍵 移動到此選項並按 ,即可執行此功能。執行時會顯
示目前網域名稱伺服器設定,直接輸入欲變更的網域名稱伺服器的網路位址再按下
➡ mm 鍵,即可變更設定。若不變更設定則按 鍵取消並跳出。此功能畫面如下:
KS>ystem KD>evice 03/07/06 Device DNS Server: 192.168.20.1_
圖表 191: 網域名稱伺服器 (DNS) 畫面

12.5.5 TCP 連線逾時時間 (TCP Timeout) []

此功能為設定經由NK6000的TCP連線逾時限制。在Device功能選單中以方向 鍵或快捷鍵 移動到此選項並按 # Enter 鍵,即可執行此功能。執行時會顯示目 前TCP連線逾時限制設定,此設定以秒為單位,直接輸入欲變更的逾時限制再按下 # Enter 鍵,即可變更設定。若不變更設定則按 ^{Esc} 鍵取消並跳出。此功能畫面如下:





圖表 192: TCP 連線逾時時間設定 (TCP Timeout) 畫面

12.5.6 最大系統事件記錄數量 (Max. Log) 🕒

此功能為設定 NK6000 最多存放的系統事件記錄數量。在 Device 功能選	單中以
方向鍵或快捷鍵 移動到此選項並按 即可執行此功能。執行時	會顯示
目前最大系統事件記錄存放數量的設定,直接輸入欲變更的最大存放數量設定	再按下
↓ Enter 鍵,即可變更設定。若不變更設定則按	面如下:
S>ystem <d>evice 03/07/06</d>	
Max. number of Log event (500 ~ 5000): 1000_	

圖表 193: 最大系統事件記錄數量 (Max Log) 畫面



12.5.7 BEMS 伺服器 (BEMS Srv.) 🕒

此功能為設定 NK6000 歸屬於何者 BEMS 伺服器所管控。在 Device 功能選單中
以方向鍵或快捷鍵 移動到此選項並按 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
示目前 BEMS 伺服器的網路位址設定,直接輸入欲變更的 BEMS 伺服器網路位址再
按下━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
如下:

< <u>S</u> >ystem <d>evice</d>	03/07/06
BEMS Server IP: 192.168.0.2_	
	10 54
K <u>ESC</u> >Ex1t	13:54

圖表 194: BEMS 伺服器 (BEMS Srv.) 畫面

12.5.8 連接埠設定 (Port Config) []

此功能爲設定NK6000各個連接埠。在Device功能選單中以方向鍵或快捷鍵

移動到此選項並按 ,即可執行此功能。執行時會顯示目前各個連接埠的連線模式 (Link Mode)、偵測模式 (Mode) 及各功能忽略與否 (例如: Policy Bypass、 State Bypass 等等)的設定。此功能詳細釋義請參考 12.4.1 系統狀態 (All State)。操作介面如下圖示:



< <mark>S</mark> >ystem <d>evice</d>							03/07/06
	Port Ø	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Link Mode Mode Policy Bypass State Bypass Integrity Bypass Fragment Bypass VPN Bypass ACL Bypass PortScan Bypass IPSweep Bypass GRE Bypass	≥>> <mark>AUTO</mark> IPS-M Off Off Off Off Off Off Off Off Off	AUTO IPS-M Off Off Off Off Off Off Off Off Off	AUTO IPS-M Off On Off Off Off Off Off Off Off	AUTO IPS-M Off On Off Off Off Off Off Off Off	AUTO IDS-M Off Off Off Off Off Off Off Off Off	AUTO IDS-M Off Off Off Off Off Off Off Off Off	AUTO Mgnt N/A N/A N/A N/A N/A N/A N/A N/A N/A
P	ress <esc></esc>	when you	ı finish p	oort confi	iguration.		13:57

圖表 195: 連接埠設定 (Port Config) 畫面

Port Config 於連線模式、偵測模試與各功能忽略與否的設定中各擁有子選項,其

操作方式是相同的,可以利用方向鍵移動至要變再按下^{+-Enter}鍵,則會出現子選

若不變更設定則按 鍵取消並跳出。此功能畫面如下:

< <u>S</u> >ystem < <u>D</u> >evice							
	Port Ø	Port 1	Port 2				
Link Mode	i>>>auto	AUTO	AUTO				
Mode	IPS-M	IPS-M	IPS-M				
Policy Bypass	0ff	Off	++				
State Bypass	l Off	Off	l≥AUTO				
Integrity Bypass	0ff	Off	10H				
Fragment Bypass	l Off	Off	10F				
VPN Bypass	i Off	Off	100H				
ACL Bypass	l Off	Off	100F				
PortScan Bypass	i Off	Off	1000F				
IPSweep Bypass	0ff	Off	++				

圖耒	196.	Link	Mode	子彈頂
回衣	190.	LIIIK	mode	丁进归

Port ØPort 1Port 2Link ModeAUTOAUTOAUTOMode>>>IPS-MIPS-MIPS-MPolicy BypassOff0++ffState BypassOff0 >IWdInIntegrity BypassOff0 IPSIffFragment BypassOff0 IPS-MIffVPN BypassOff0 IDSIffACL BypassOff0 IDS-MIffPortScan BypassOff0 IDS-MIff	< <mark>S</mark> >ystem < D >evice				
Link Mode AUTO AUTO AUTO Mode >>> IPS-M IPS-M IPS-M Policy Bypass Off O++ff State Bypass Off O >Fwd n Integrity Bypass Off O IPS ff Fragment Bypass Off O IPS-M ff VPN Bypass Off O IDS ff ACL Bypass Off O IDS-M ff PortScan Bypass Off O++ff		Port Ø	Port 1 Port 2		
	Link Mode Mode Policy Bypass State Bypass Integrity Bypass Fragment Bypass VPN Bypass ACL Bypass PortScan Bypass	AUTO >>> IPS-M Off Off Off Off Off Off Off	AUTO AUTO IPS-M IPS-M O++ff O ≥Fwd n O IPS ff O IPS-M ff O IDS ff O IDS ff O IDS-M ff O++ff		

圖表 197: Mode 子選項



		D. CATCO					
			Port Ø	Port 1	Port 2		
	Link Mode Mode Policy Byp State Bypa Integrity Fragment B VPN Bypass	ass > ss Bypass ypass	AUTO IPS >> Off Off Off Off Off	AUTO IPS Of+ Of¦≥ On Of¦ Of Of+ Off	AUTO IPS-M +Off IOn f Off +Off Off		
	围	表 198: 日	Policy Byp	oass 子選	項		
設定完畢,按 確定儲存已修ī	■ 鍵欲線 改的設定	詰束設定 ; 按 ▶	四時,系統 建則不	統將會議 儲存,止	可問是否 比選項無	儲存已候 預設値	修改的設 。
< <mark>S</mark> ≻ystem < <mark>D</mark> ≻evic	e						03/08/06
1	Date O	Dan 1	Dow 1 O	Dam± 1	Dont /	DoutE	Daw + C
Link Mode Mode Policy Bypass State Bypass Integrity Bypass Fragment Bypass VPN Bypass ACL Bypass PortScan Bypass IPSweep Bypass GRE Bypass	Port 0 IPS-M Off Off Off Off Off Off Off Of	Port 1 AUTO IPS-M Off Off Off Off Off Off Off Off Off	Port 2 AUTO IPS-M Off On Off Off Off Off Off Off Off	Port 3 AUTO IPS-M Off Off Off Off Off Off Off Off Off	Port 4 AUTO IDS-M Off Off Off Off Off Off Off Off Off Of	Port 5 AUTO IDS-M Off Off Off Off Off Off Off Off Off Of	Port 6 AUTO Mgnt N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A
Link Mode Mode Policy Bypass State Bypass Integrity Bypass Fragment Bypass YPN Bypass ACL Bypass PortScan Bypass IPSweep Bypass GRE Bypass	Port 0 >>> <mark>AUTO</mark> IPS-M Off Off Off Off Off Off Off Off Off	Port 1 AUTO IPS-M Off Off Off Off Off Off Off Off Off	Port 2 AUTO IPS-M Off On Off Off Off Off Off Off off off	Port 3 AUTO IPS-M Off Off Off Off Off Off Off Off Off	Port 4 AUTO IDS-M Off Off Off Off Off Off Off Off Off Of	Port 5 AUTO IDS-M Off Off Off Off Off Off Off Off	Port 6 AUTO Mgnt N/A N/A N/A N/A N/A N/A N/A N/A N/A

12.5.9 HA (High Availability)

此功能為設定本機 High Availability 對應的 NK6000 型設備。在 Device 功能選單中以方向鍵或快捷鍵 移動到此選項並按 , 即可執行此功能。執行時會顯示目前對應的 HA 設備 IP 位址,直接輸入欲變更的 HA 設備 IP 位址,再按下 , 即可變更設定。此功能畫面如下:





圖表 200: HA (High Availability) 畫面

12.5.10 虛擬網路編號 (VLAN ID) 💟

此功能為設定 NK6000 所屬的虛擬網路編號。在 Device 功能選單中以方向鍵或

快捷鍵 移動到此選項並按	┛ Enter 鍵,	即可執行此功能。	此功能畫面如下:
--------------	------------	----------	----------

<s>ystem <d>evice</d></s>	03/07/06
VLAN ID: 0_	
K <u>Esc</u> >Exit	14:18

圖表 201: 虛擬網路編號 (VLAN ID) 畫面

執行時會顯示目前虛擬網路編號設定,直接輸入欲變更的虛擬網路編號再按下 → Enter 鍵,系統將會再次作確認,按 鍵以確更改設定値;按 鍵為不變更 設定,預設為不變更設定。


NK6000 使用手册



圖表 202: 虛擬網路編號 (VLAN ID) 再次確認變更

12.5.11 PING

此功能為 NK6000 所提供的網路連線測試工具。在 Device 功能選單中以方向鍵

移動到此選項並按	〕鍵	,	即可執行此功能。	c	此功能書面如下:
沙玛山匹克亚汉	- yt				此め府と里山がー・

< <mark>S</mark> >ystem <d>evice</d>			03/07/06
Target IP: _			
K <u>Esc</u> >Exit			14:43
	圖表 203: Ping 功	能畫面	
行後,輸入欲作 Pir	ng 測試的 IP 位址,再	按下	〕 鍵,即可在主視
能連線到該 IP 位置	。遍作簕例加下。		



NK6000 使用手册

<s>ystem <d>evice</d></s>	03/07/06
PING 192.168.168.1 (192.168.168.1): 56 data bytes 64 bytes from 192.168.168.1: icmp_seq=0 ttl=64 time=6.8 ms 64 bytes from 192.168.168.1: icmp_seq=1 ttl=64 time=6.0 ms 64 bytes from 192.168.168.1: icmp_seq=2 ttl=64 time=6.0 ms 64 bytes from 192.168.168.1: icmp_seq=3 ttl=64 time=6.3 ms 64 bytes from 192.168.168.1: icmp_seq=4 ttl=64 time=6.0 ms	
192.168.168.1 ping statistics 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 6.0/6.2/6.8 ms	
Press any key to continue. —	
	14:37

圖表 204: Ping 192.168.168.1



附件一 安裝 MySQL

從 BEMS 1.1 版本起, MySQL 資料庫安裝程式將不再內含在出貨光碟片中。BEMS installer 不會自動為使用者呼叫 MySQL 安裝程式。使用者需要自行下載 MySQL 程式 (原廠建議使用 MySQL 4.1.18 版)並自行安裝、設定 MySQL。

1. 執行 MySQL 安裝程式,出現以下畫面。按 Next。



2. 核選 Typical





3. 按 Install

🕞 MySQL Server 4.1 - Setup Wizard 🛛 🛛 🔀
Ready to Install the Program The wizard is ready to begin installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard. Current Settings:
Setup Type:
Typical Destination Folder:
C:\Program Files\MySQL\MySQL Server 4.1\
< <u>B</u> ack Install Cancel

4. 點選 Skip Sign-Up

MySQL.com Sign Up - Setup Wizard	
MySQL.com Sign-Up Login or create a new MySQL.com account.	0
Please log in or select the option to create a new account. Create a new free MySQL.com account If you do not yet have a MySQL.com account, select this option and complete the following three steps.	
O Login to MySQL.com Select this option if you already have a MySQL.com account. Please specify your login information below.	
Email address:	
Next > (Cancel



5. 核選 Confugure the MySQL Server now,再按 Finish。



6. 點選 Next。





7. 核選 Detailed Configuration。



8. 核選 Server Machine。

MySQL Server Instance Configuration Wizard	×		
MySQL Server Instance Configuration Configure the MySQL Server 4.1 server instance.			
Please select a server type. This will influence memory, disk and CPU usage.			
• Server Machine Several server applications will be running on this machine. Choose this option for web/application servers. MySQL will have medium memory usage.			
O Dedicated MySQL Server Machine			
This machine is dedicated to run the MySQL Database Server. No other servers, such as a web or mail server, will be run. MySQL will utilize up to all available memory.			
<pre></pre>			



9. 核選 Non-Transactional Database Only。



10. 核選 Decision Support (DSS)/OLAP。

MySQL Server Instance Configuration Wizard				
MySQL Server Instance Configuration Configure the MySQL Server 4.1 server instance.				
Please set the approximate number of concurrenct connections to the server. • Decision Support (DSS)/OLAP • Select this option for database applications that will not require a high number of concurrent connections. A number of 20 connections will be assumed. • Online Transaction Processing (OLTP) • Choose this option for highly concurrent applications that may have at any one time up to 500 active connections such as heavily loaded web servers. • Manual Setting • Please enter the approximate number of concurrent connections. • Concurrent connections:				
< Back Next > Cancel				



11. 核選 Enable TCP/IP Networking。Port Number 保持預設值 3306。核選 Enable Strict Mode。



12. 核選 Standard Character Set。

MySQL Server Instance Configuration Wizard	×			
MySQL Server Instance Configuration Configure the MySQL Server 4.1 server instance.				
Please select the default character set.				
Character set for storing text in many different languages. Manual Selected Default Character Set / Collation Please specify the character set to use. Character Set: latin1				
< Back Next > Ca	ancel			





13. 維持預設值: 核選 Install As Windows Service; Service Name: MySQL; 核選 Launch the MySQL Server automatically。

MySQL Server Insta	nce Configuration Wizard	×
MySQL Server Configure the I	Instance Configuration MySQL Server server instance.	
Please set the	Windows options.	
🔽 Install As	Windows Service	
Constant of the second	This is the recommended way to run the MySQL server on Windows.	
	Service Name: MySQL	
	Launch the MySQL Server automatically	
🔲 Include Bi	in Directory in Windows PATH	
MySQL2	Check this option to include the directory containing the server / client executables in the Windows PATH variable so they can be called from the command line.	
	< Back Next > Cancel	

14. 核選 **Modyfy Security Settings**。請為 MySQL 資料庫的 root 帳號自行設定一個 密碼,如下圖:

MySQL Server Insta			×	
MySQL Server Configure the	Instance Configuratio MySQL Server server inst	n ance.		
Please set the	security options.			
🔽 Modify Se	curity Settings			
	New root password:	*****	Enter the root password.	
root	Confirm:	*****	Retype the password.	
		🔲 Enable root a	access from remote machines	
🔲 Create An	Anonymous Account			
This option will create an anonymous account on this server. Please note that this can lead to an insecure system.				
		< Back	Next > Cancel	

說明:

請牢記您為 MySQL root 帳號所設定的密碼。安裝 BEMS 時(圖表 33),會需要您輸入 root 帳號的密碼。若密碼不符合, BEMS 無法順利安裝。



15. 按 Execute,完成 MySQL 資料庫的安裝步驟。

MySQL Server Instance Configuration Wizard	×
MySQL Server Instance Configuration Configure the MySQL Server server instance.	\bigcirc
Ready to execute	
 Prepare configuration Write configuration file Start service Apply security settings 	
Please press [Execute] to start the configuration.	
< Back Execute	Cancel

說明:

在完成 MySQL 安裝後,電腦會自動建立一個 MySQL 服務,請確認 MySQL 服務的狀態為「啓動」,再繼續 BEMS 的安裝。

_名稱 △	描述	狀態	啓動類型	登入身分
🖏 IPSEC Services	管理	已啓動	自動	本機系統
🍓 Logical Disk Manager	偵測	已啓動	自動	本機系統
🍓 Logical Disk Manager Administrativ	設定…		手動	本機系統
🍓 Messenger	在用…		已停用	本機系統
🍓 MS Software Shadow Copy Provider	管理		手動	本機系統
🎭 MySQL		已啓動	自動	本機系統
🍓 Net Logon	支援…		手動	本機系統
🍓 NetMeeting Remote Desktop Sharing	讓經…		手動	本機系統
🏶 Network Connections	管理	已啓動	手動	本機系統
🎭 Network DDE	爲動…		已停用	本機系統
🍓 Network DDE DSDM	訊息…		已停用	本機系統
🍓 Network Location Awareness (NLA)	收集…	已啓動	手動	本機系統
🍓 Network Provisioning Service	在網…		手動	本機系統
🍓 NT LM Security Support Provider	爲沒		手動	本機系統
🍓 Office Source Engine	儲存		手動	本機系統
🍓 pcAnywhere Host Service	"Allo		手動	本機系統