NK6000

Gigabit IPS

User Guide

使用手冊

V.1.2 2008/03

商標聲明

所有在本書提及的商標、註冊商標，商品名稱等等均爲其相關持有人所有。

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

威播科技的網址爲: WWW.BROADWEB.COM，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

圖表目錄

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爲，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，爲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，成爲虛擬的 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爲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

建議爲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 http://java.sun.com/downloads/ 下載適合的版本。

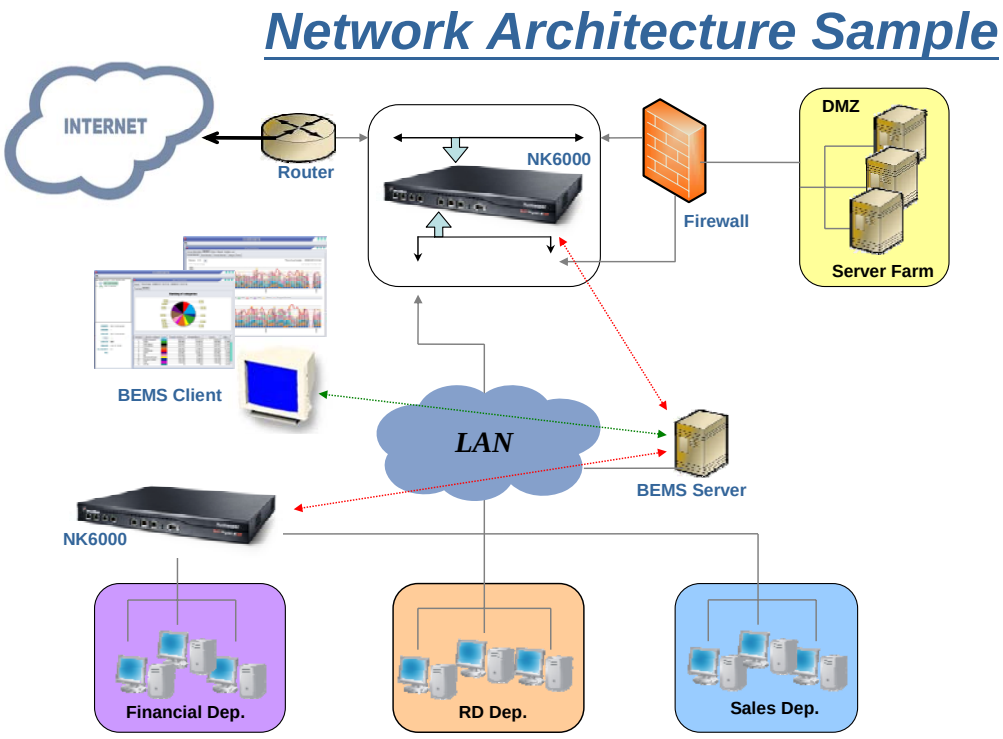
MySQL 資料庫程式: 可至 http://dev.mysql.com/ 下載適合的版本。

建置整個 NK6000 系統可以被區分爲六大部分，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

以下列出 NK6000 產品系列型號及重點資訊：

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

介面數量	GE Copper x 7	GE Copper x 7	GBIC x 4 GE Copper x 3	Fiber x 4 (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

2 第二章 安裝與設定

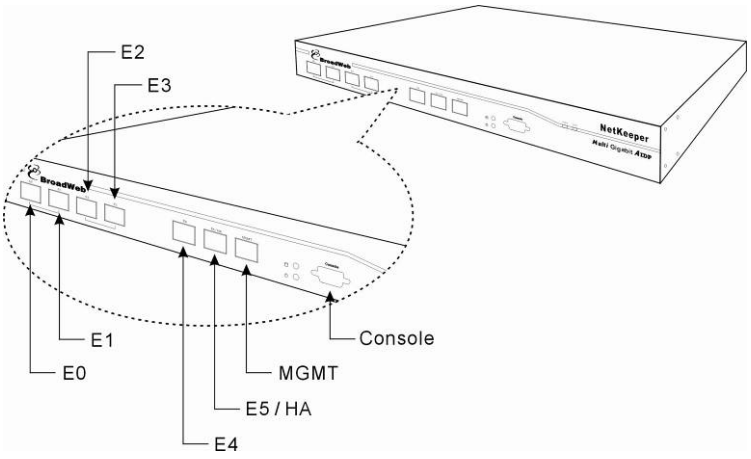
本章說明

主要說明 NK6000 安裝與設定步驟。

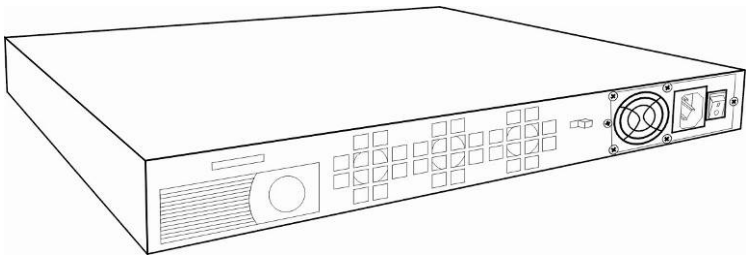
本章內容包含下列使用說明

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 爲成對的虛擬 IPS。
- E1 port：copper 介面之 IPS 的 LAN port。
- E2 port：copper 介面之 IPS 的 WAN port。E2 與 E3 爲成對的虛擬 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
PWR	綠	亮	NetKeeper 系統啓動
		滅	NetKeeper 系統關閉
SYS	紅	亮	NetKeeper 系統進行程式讀取中
		滅	NetKeeper 系統無進行程式讀取
E0 ~ E5/HA (10/100/1000)	綠橙	橙亮	連線埠成功連線到 1000Mbps
		綠亮	連線埠成功連線到 100Mbps
		滅	連線埠成功連線到 10Mbps
	綠	閃爍	連線埠正在傳送或接收封包
		滅	連線埠未連線
MGMT (10/100/1000)	綠橙	橙亮	MGMT 埠成功連線到 1000Mbps
		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 埠爲連線

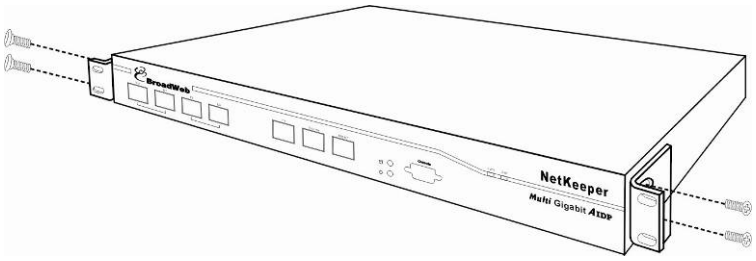
圖表 5: NK6000 外觀燈號說明

2.2 安裝 NK6000 設備

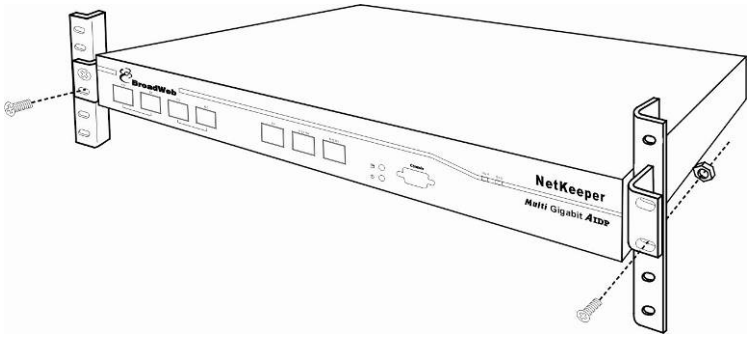
說明 NK6000 設備的安裝到機架或是網路上的方式。

2.2.1 固定 NK6000 於標準 19”機架

NK6000 可以被固定在標準的 19 英吋機櫃上。



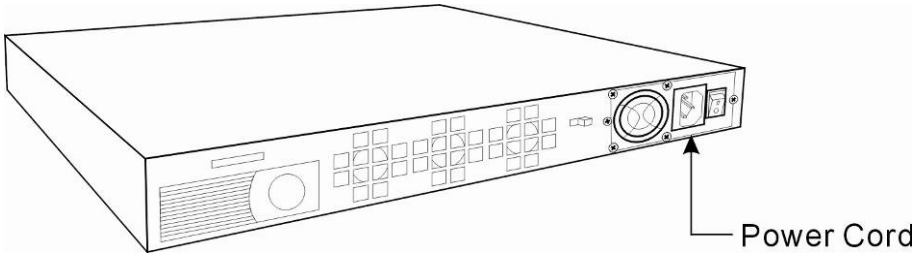
圖表 6: NK6000 鎖上耳翼



圖表 7: NK6000 鎖上機架

2.2.2 連接電源

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



圖表 8: NK6000 連接電源

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)：

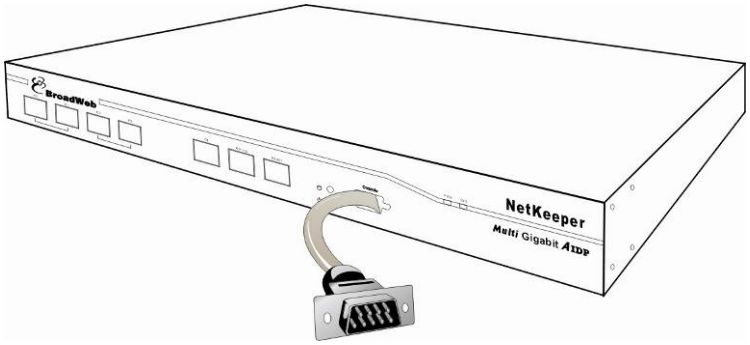
使用 Microsoft Windows XP/2000 內附之超級終端機程式，搭配使用原廠提供的 Console 線，連接電腦 (PC) 與 NK6000 的 RS-232 Console 埠。

(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

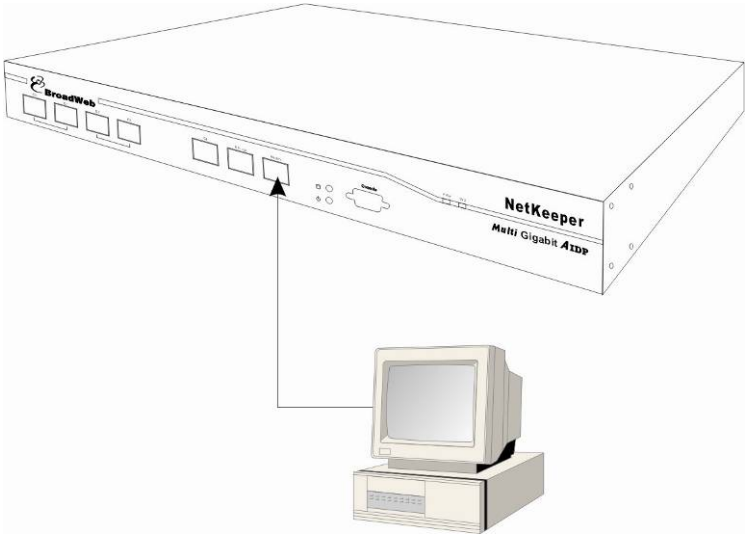
圖表 10: 終端機模擬參數

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

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)

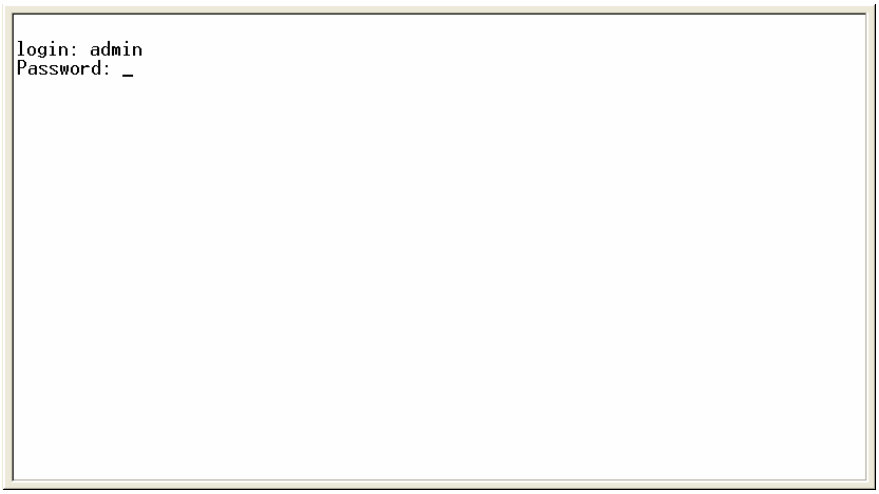
利用 UTP Cross-over 線 (對線)，連結的管理介面埠 (MGMT port) 以及電腦主機的網路卡，然後執行 SSHv2 遠端登入程式連線 NK6000 設備。



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。

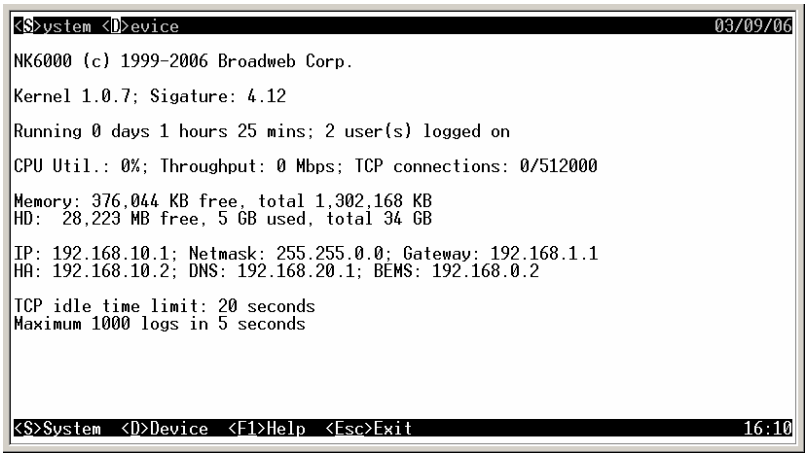


圖表 12: 命令列模式登入畫面

說明：

1. NK6000預設的IP位址爲：192.168.168.221。
2. 預設登入的使用者名稱爲 admin，密碼爲 admin。

成功登入之後，即出現以下操作畫面。



圖表 13: 命令列模式畫面

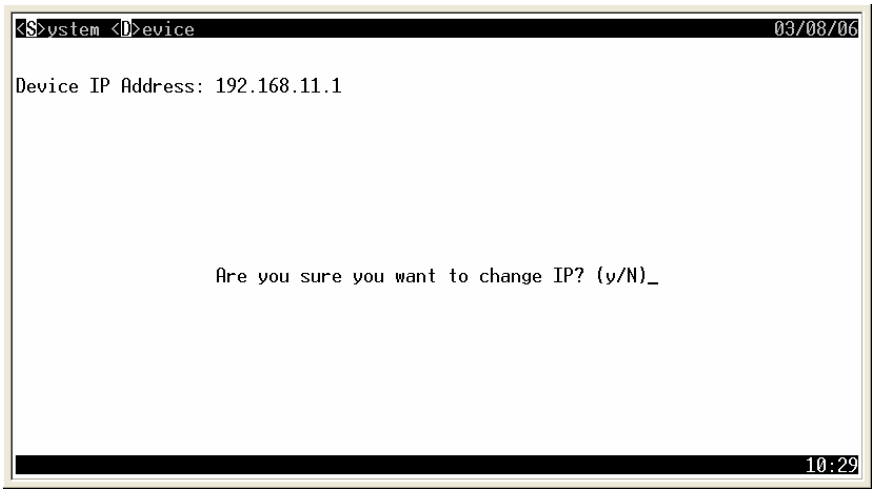
2.3.4 設定 IP 位址 (IP Address)

此功能爲設定 NK6000 的網際網路地址。在 Device 功能選單中以方向鍵或快捷鍵 I 移動到此選項並按 Enter 鍵，即可執行此功能。此功能畫面如下：

圖表 14: 設定 IP 位址 (IP Address) 畫面

執行時會顯示目前 IP 地址設定，直接輸入欲變更的 IP 位址再按 Enter 鍵，系

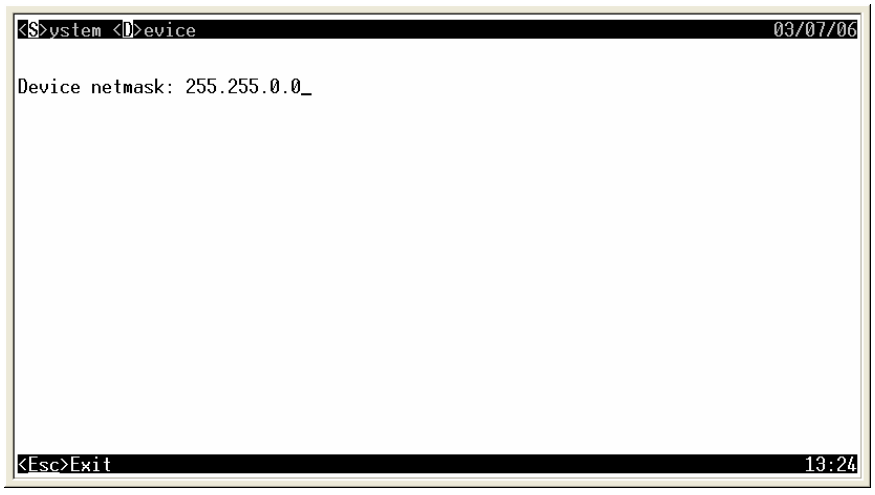
統將再次詢問變更與否，按 Y 鍵確定變更 IP 位址；按 N 鍵或 Esc 鍵則不變更，預設爲不變更。



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

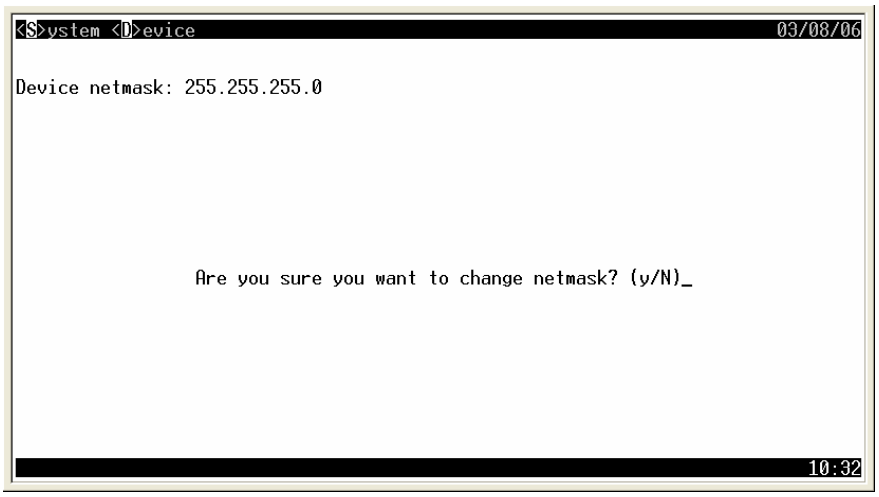
此功能爲設定 NK6000 的網路遮罩。在 Device 功能選單中以方向鍵或快捷鍵 M 移動到此選項並按 Enter 鍵，即可執行此功能。此功能畫面如下：



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 Enter 鍵，

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Esc鍵則不變更，預設爲不變更。



圖表 17: 子網路遮罩 (Netmask) 再次確認變更

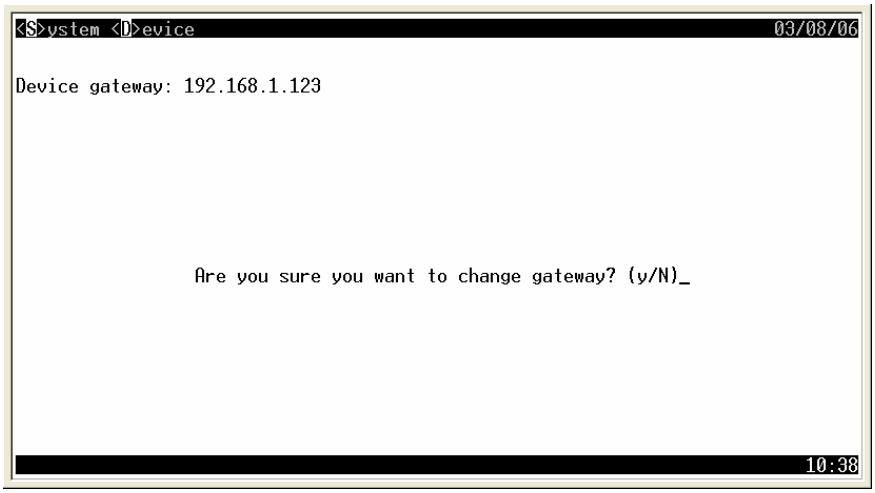
2.3.6 設定閘道器 (Gateway) G

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G移動到此選項並按Enter鍵，即可執行此功能。此功能畫面如下：

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Enter

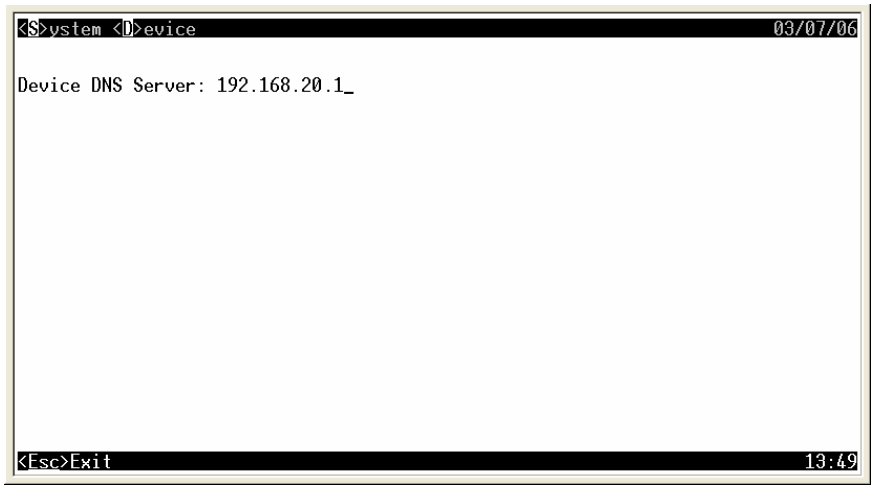
鍵，系統將再次詢問變更與否，按Y鍵確定變更閘道器設定；按N鍵或Esc鍵則不變更，預設爲不變更。



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) D

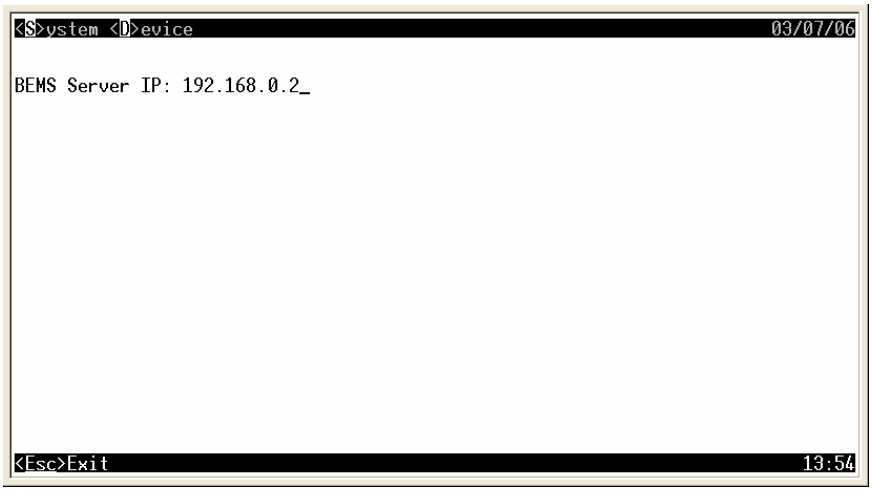
此功能爲設定 NK6000 經由何者閘道器連接至外部網路。在 Device 功能選單中以方向鍵或快捷鍵D移動到此選項並按Enter鍵，即可執行此功能。執行時會顯示目前網域名稱伺服器設定，直接輸入欲變更的網域名稱伺服器的網路位址再按Enter鍵，即可變更設定。若不變更設定則按Esc鍵取消並跳出。此功能畫面如下：



圖表 20: 設定網域名稱伺服器 (DNS) 畫面

2.3.8 設定 BEMS 伺服器 (BEMS Server) B

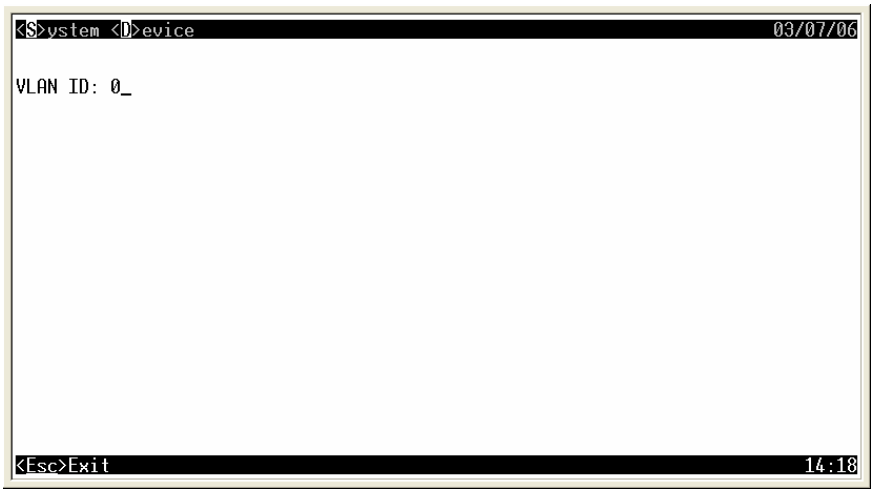
此功能爲設定 NK6000 歸屬於何者 BEMS Server 所管控。在 Device 功能選單中以方向鍵或快捷鍵 B 移動到此選項並按 Enter 鍵，即可執行此功能。執行時會顯示目前 BEMS Server 的網路位址設定，直接輸入欲變更的 BEMS Server 網路位址再按下 Enter 鍵，即可變更設定。若不變更設定則按 Esc 鍵取消並跳出。此功能畫面如下：



圖表 21: 設定 BEMS 伺服器 (BEMS Server) 畫面

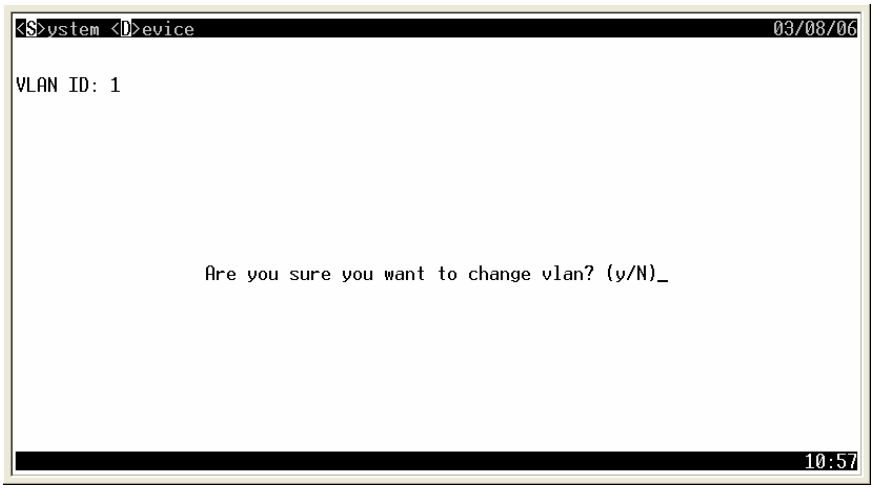
2.3.9 設定虛擬網路編號 (VLAN ID) V

此功能爲設定 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 V 移動到此選項並按 Enter 鍵，即可執行此功能。此功能畫面如下：



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 Enter 鍵，系統將會再次作確認，按 Y 鍵以確更改設定值；按 N 鍵爲不變更設定，預設爲不變更設定。



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 爲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。如果您尚未成爲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。

1. 可連結威播科技網站: www.broadweb.com，或是直接連線威播註冊網站: my.broadweb.com。
2. 第一次連線使用，請先註冊成爲一個新的客戶，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：

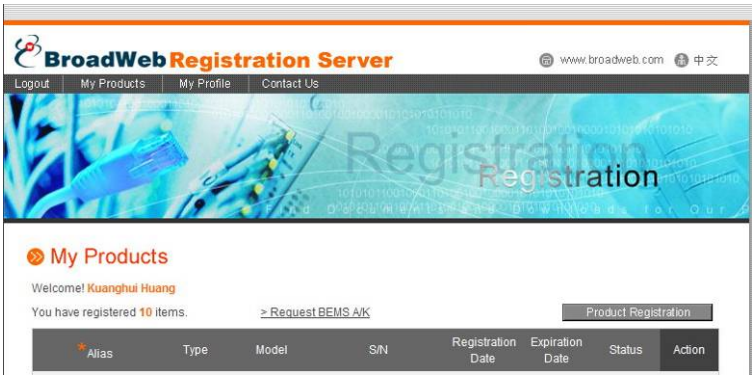
1. 登記成爲威播科技的註冊客戶，是取得BEMS啓動密鑰的必需手續。啓動密鑰內含的資訊即包含了客戶的註冊帳號，這使得BEMS管理系統可以依據使用者所註冊的產品，從威播資料更新伺服器(DUC)獲得正確的遠端升級服務，遠端升級服務包括了BEMS主程式、外掛管理模組、設備的核心程式，以及安全防禦政策等軟體的升級。
2. 產品註冊不是取得BEMS啓動密鑰的必需手續，您可以在沒有註冊任何產品的情況下，下載BEMS啓動密鑰。但是產品註冊是啓動該項產品軟體升級服務的必需手續。完成產品註冊手續之後，您可以在威播註冊網站上看到您所註冊的產品清單以及每項產品的軟體升級服務的開始與結束日期。

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

圖表 25: 註冊帳號填寫畫面



圖表 26: 正確輸入登入帳號/密碼後之畫面

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。

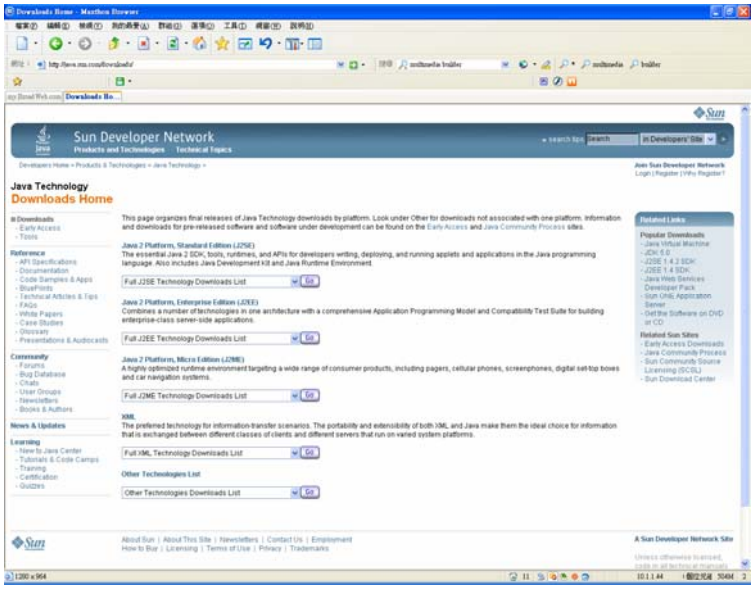
將原廠提供之光碟放入光碟機後，它將會自動的執行安裝程式。如果您的系統沒有自動執行安裝程式的話，請在光碟機目錄所在地搜尋一個『**BW-BEMS.exe**』的檔

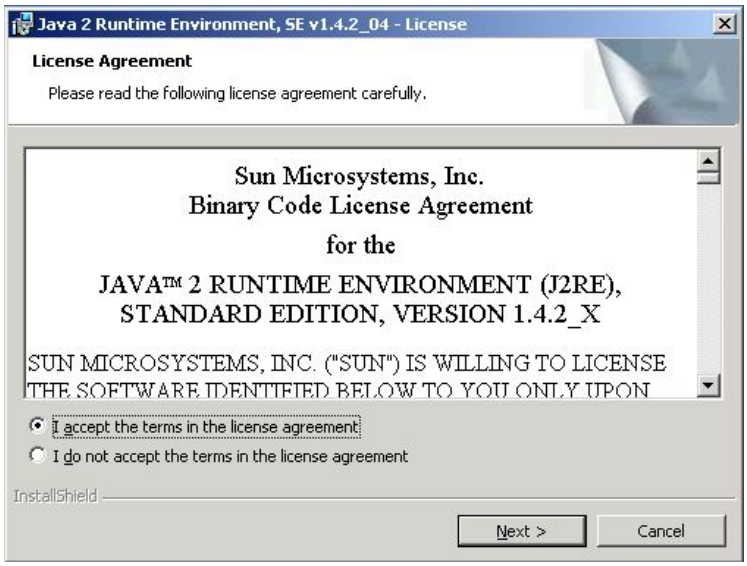
案，執行它可以進行 Product Registration、BEMS Server Installation、打開並讀取 Quick Installation Guide 檔案、User Guide 檔案等等功能。

圖表 27: 原廠光碟執行畫面

3.2.1 安裝 JRE (Java Runtime Environment)

因爲 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 http://java.sun.com/downloads/ 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。



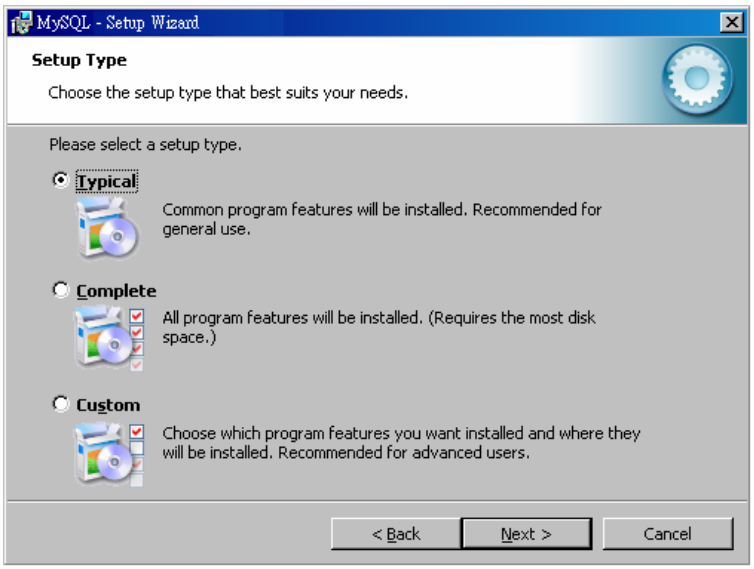


圖表 28: JRE 程式下載及安裝範例

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爲 4.1.18。

在選單中選擇 MySQL 可連線至 http://dev.mysql.com/ 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

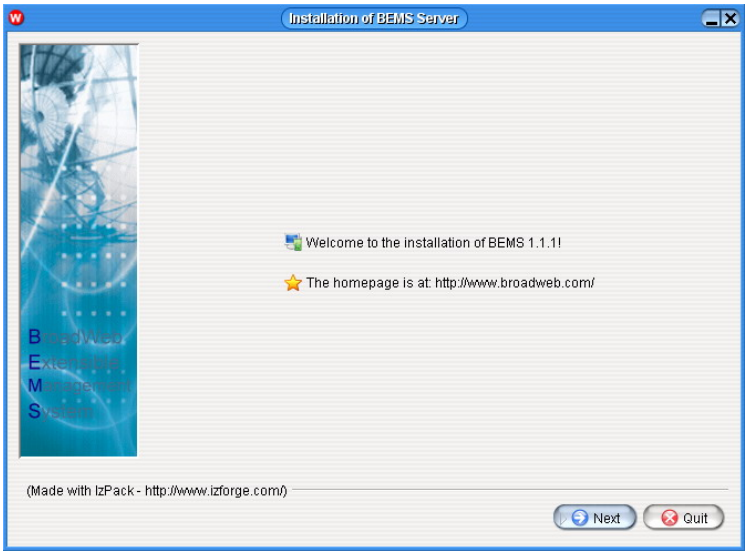
關於 MySQL 安裝過程的詳細步驟，請參見附件一：安裝 MySQL。

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。

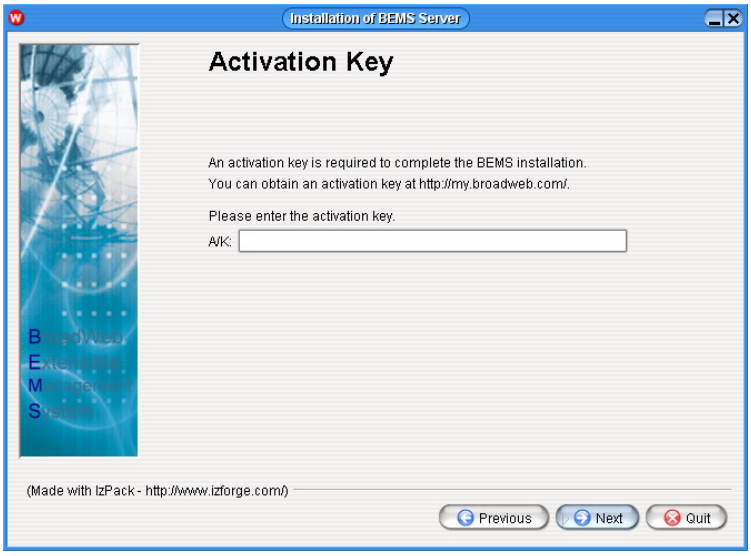


圖表 30: 安裝歡迎畫面

■ 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。

請將此啓動密鑰填入設定視窗中對應的欄位。



圖表 31: 輸入 A/K 畫面

注意：

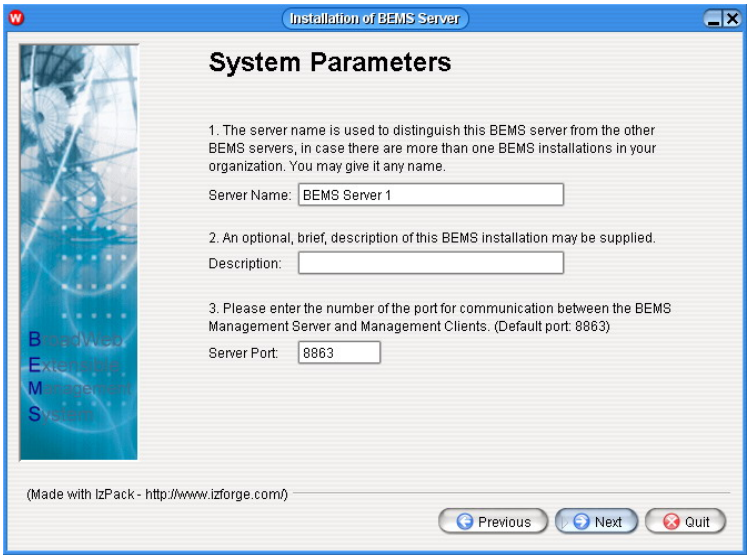
每一組 BEMS 啓動密鑰僅可被安裝在一台 BEMS Server 上。若重複將相同 BEMS 啓動密鑰安裝在不同的 BEMS Server 上，會導致特徵碼無法更新。

■ 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 (預設爲 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，原廠預設值爲 TCP/8863，使用者可自行修改定義。



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。**

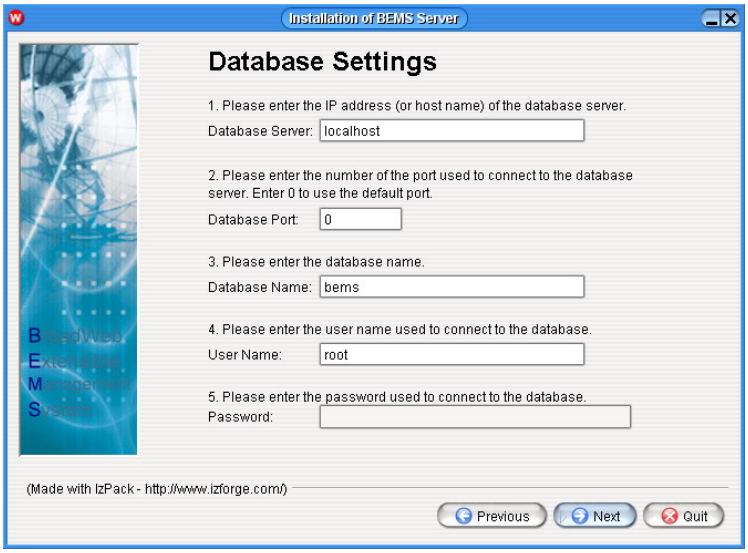
請輸入資料庫相關參數。

- 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 (建議保持預設值)。
- 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，爲 root 帳號所設定的密碼。



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。

圖表 34: 管理者設定視窗

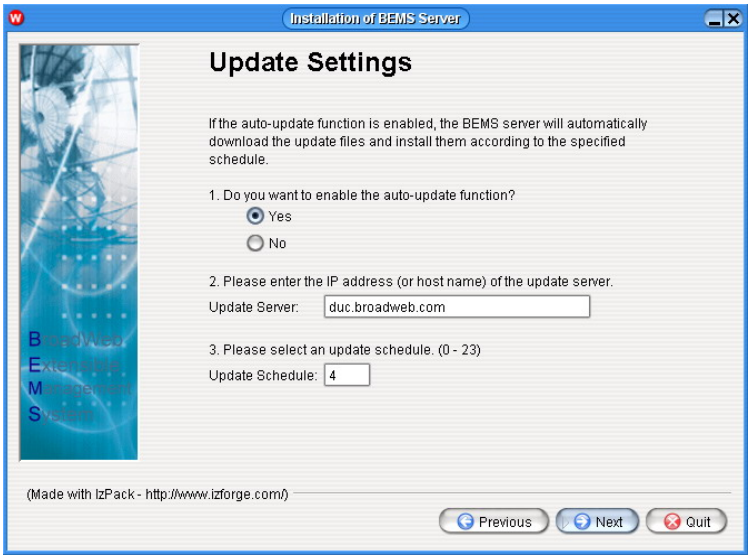
■ 步驟六：遠端升級設定

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: 預設值爲啓動。
- 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。

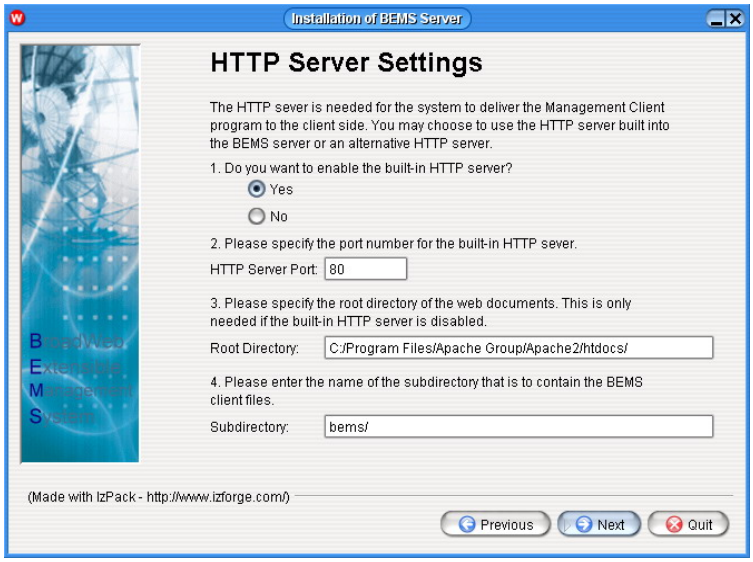


圖表 35: 設定遠端連線線上更新的參數畫面

- 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 (預設爲 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 http://<bems server IP address>/bems/ 即可進入 BEMS 管理系統客戶端首頁畫面。



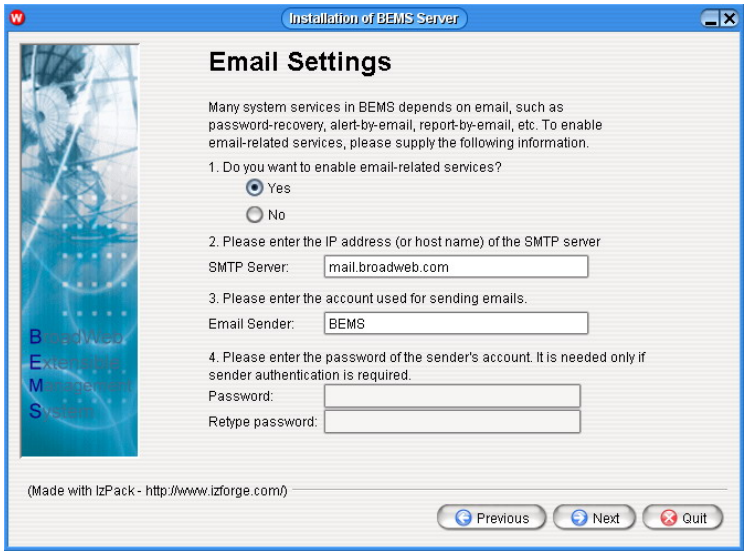
圖表 36: HTTP Server 參數設定視窗

■ 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: 預設值爲啓動。
- 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。



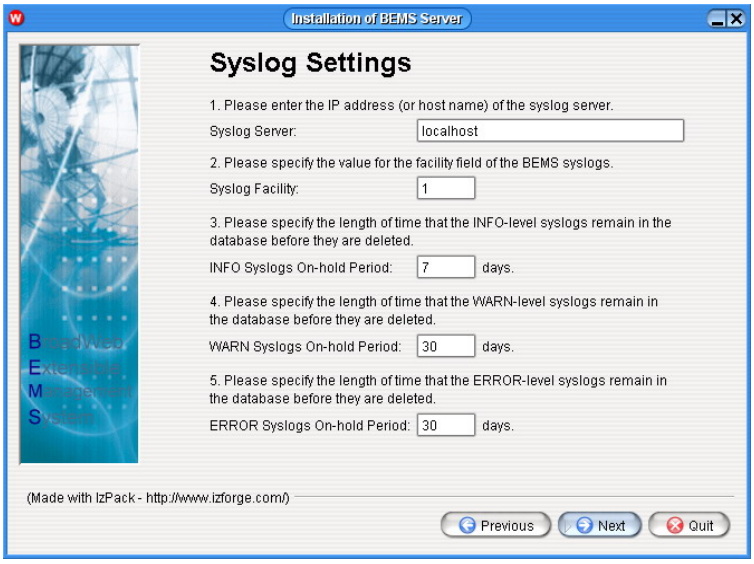
圖表 37: 傳送訊息所需的電子郵件參數設定

- 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 參數設定視窗中填入指定的 Syslog 伺服器的 IP 位址，Syslog Facility 的辨識碼，以及分別爲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。

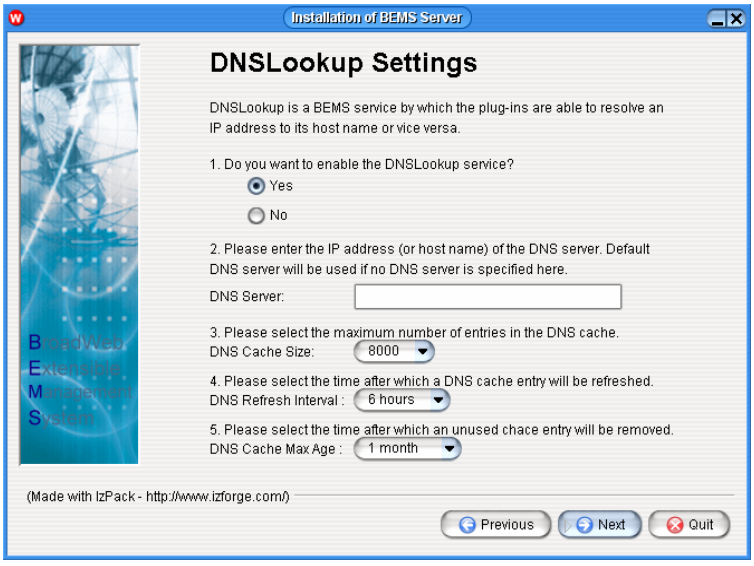


圖表 38: Syslog 相關參數設定畫面。

■ 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。

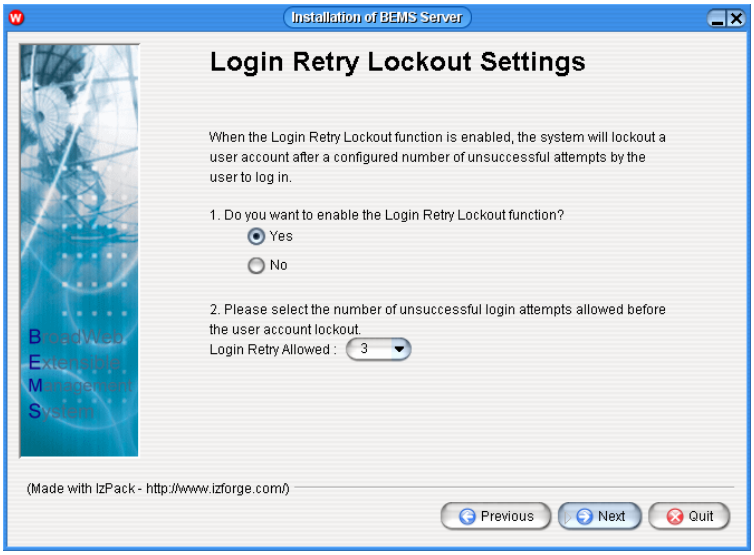


圖表 39: DNSLookup 參數設定視窗

■ 步驟十一：登入嘗試鎖定設定視窗

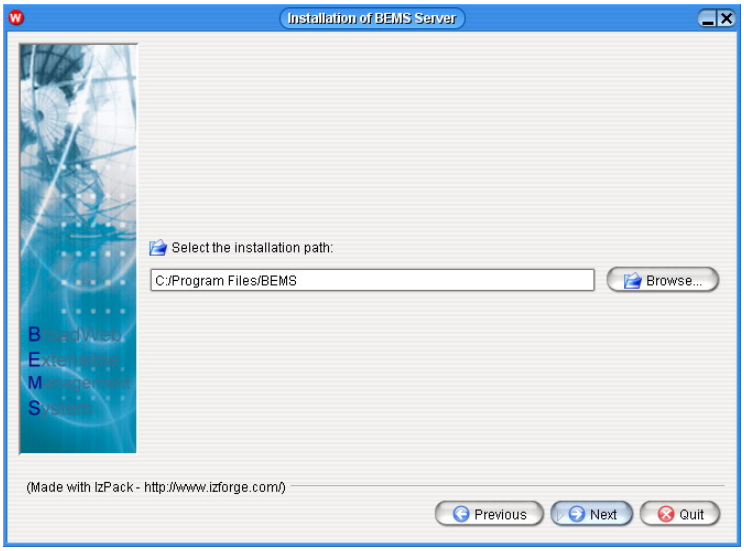
爲避免 BEMS 管理系統用戶帳號被不法之徒以嘗試錯誤的方式，猜出用戶登入密碼，您可以啓動登入嘗試鎖定(Login Retry Lockout)的功能來提升系統的安全性。一但啓動這項功能，除系統管理員以外的任何用戶帳號，如果登入密碼連續輸入錯誤達設定上限時，系統就會鎖定這個用戶帳號並拒絕其登入，直到系統管理員在管理系統

中爲用戶帳號解除設定。



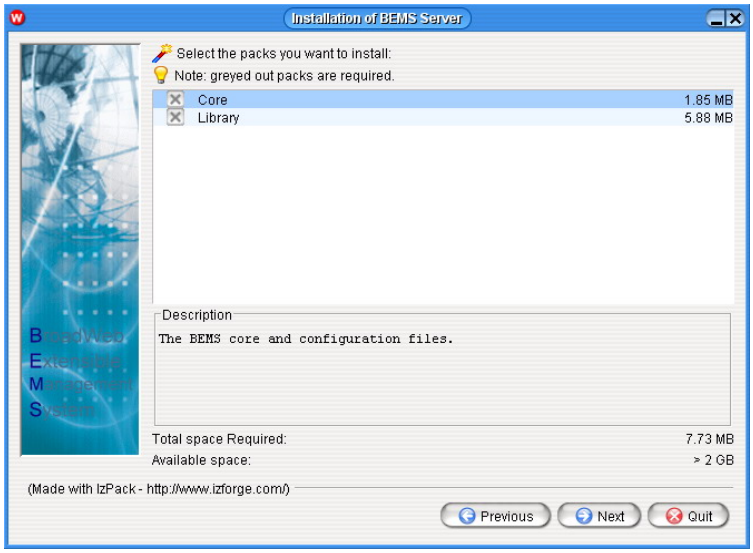
圖表 40: 登入嘗試鎖定設定視窗

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



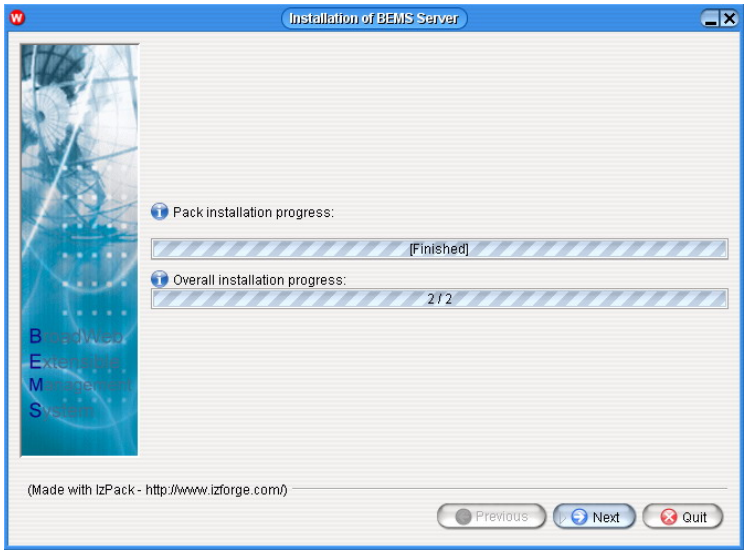
圖表 41: 安裝目錄選擇畫面

- 步驟十三：選擇需要安裝的程式(全部選取)。



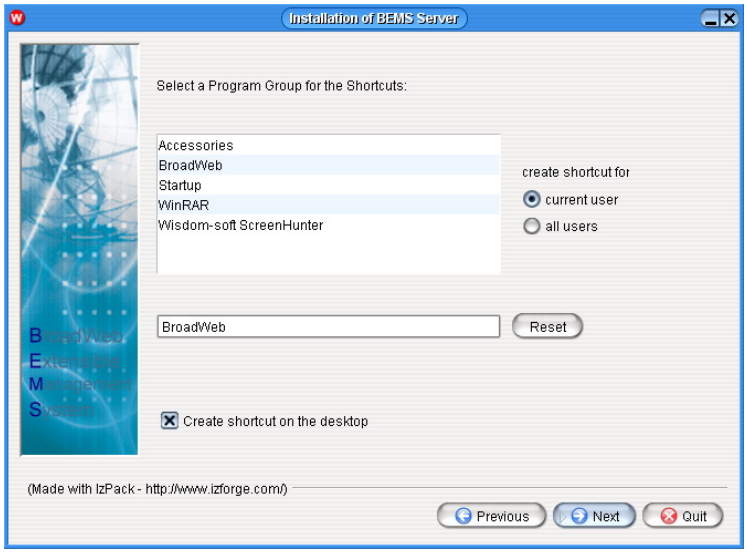
圖表 42: 需要安裝的程式 (Core 以及 Library)

- 步驟十四：安裝程式完成。



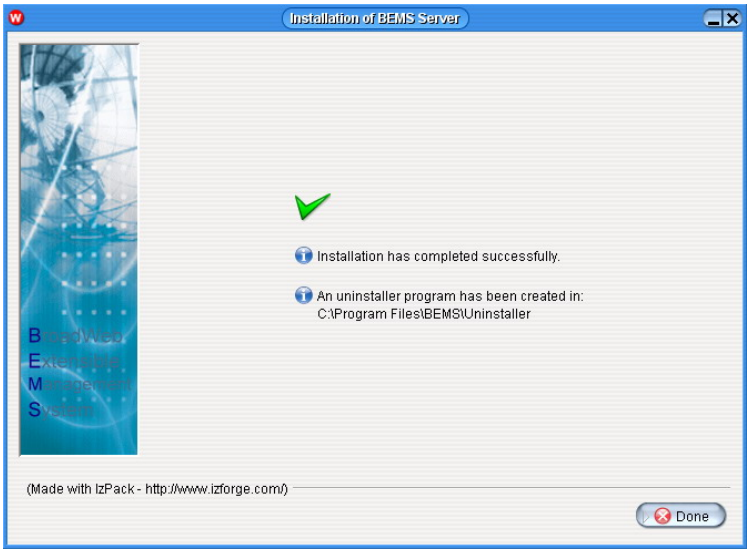
圖表 43: 程式安裝完畢畫面

- 步驟十五：建立捷徑。



圖表 44: 建立捷徑

■ 步驟十六：安裝完成，請重新開啓電腦主機。



圖表 45: 全部程式安裝完畢畫面。

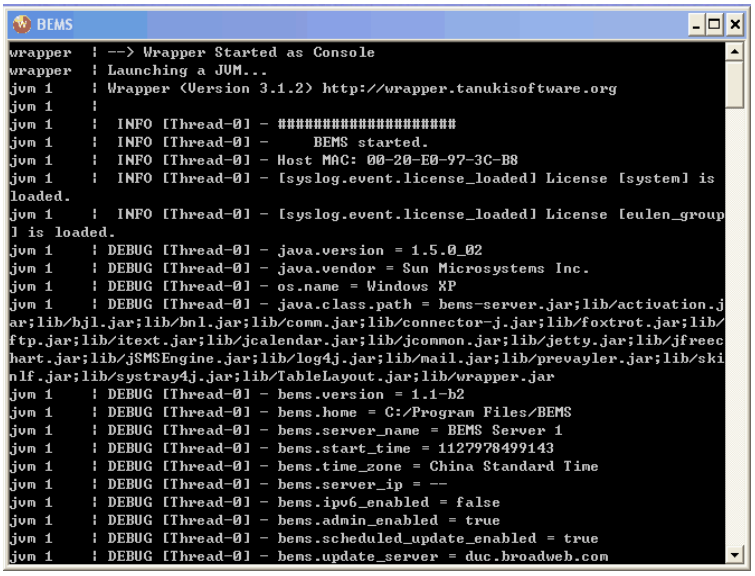
3.2.4 啓動 BEMS Server 程式

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：

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\BEMS.bat。執行後如圖所示：



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。

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

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(W)，利用滑鼠雙擊之後可以登入 Admin Console 設定相關參數。

圖表 48: 工具列中 BEMS Admin Console 圖示

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 / 登入密碼爲: 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。

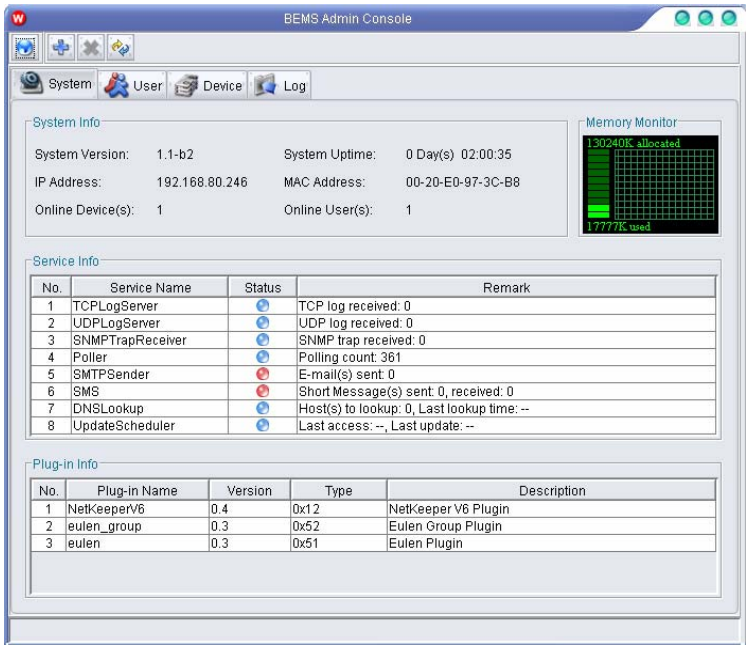
4.2 系統 (System)

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。



圖表 50: BEMS Admin Console 畫面

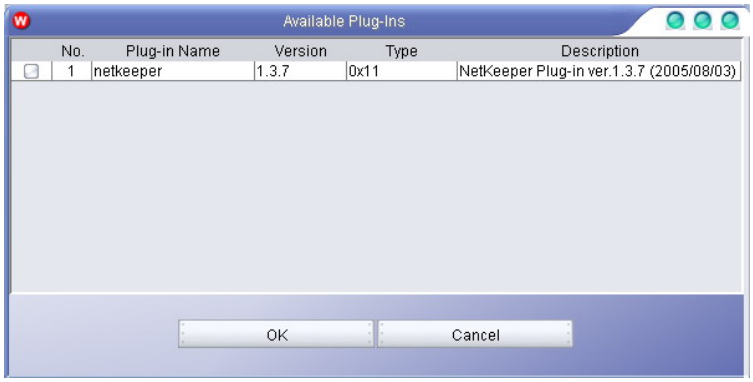
4.2.1 產品註冊 (Product Registration)

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。

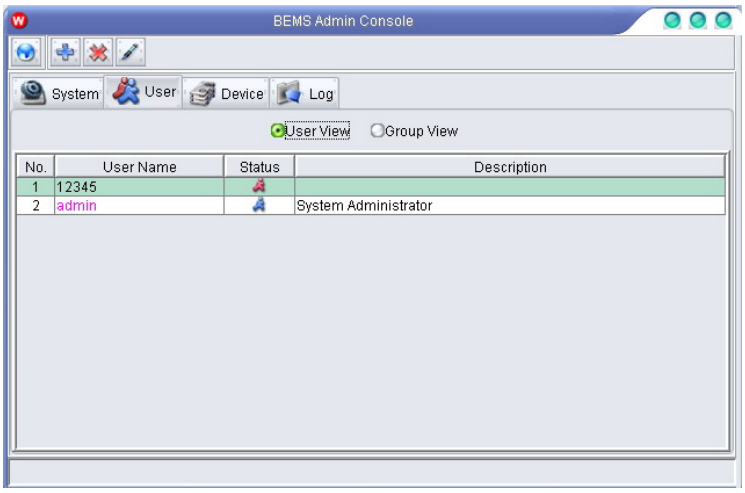
4.2.4 檢查升級 (Check for Update)

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。

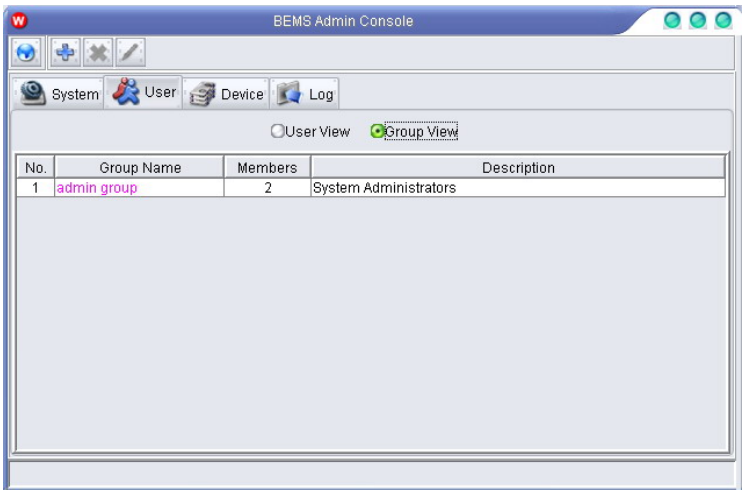
4.3 使用者 (User)

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爲 admin，密碼爲 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。



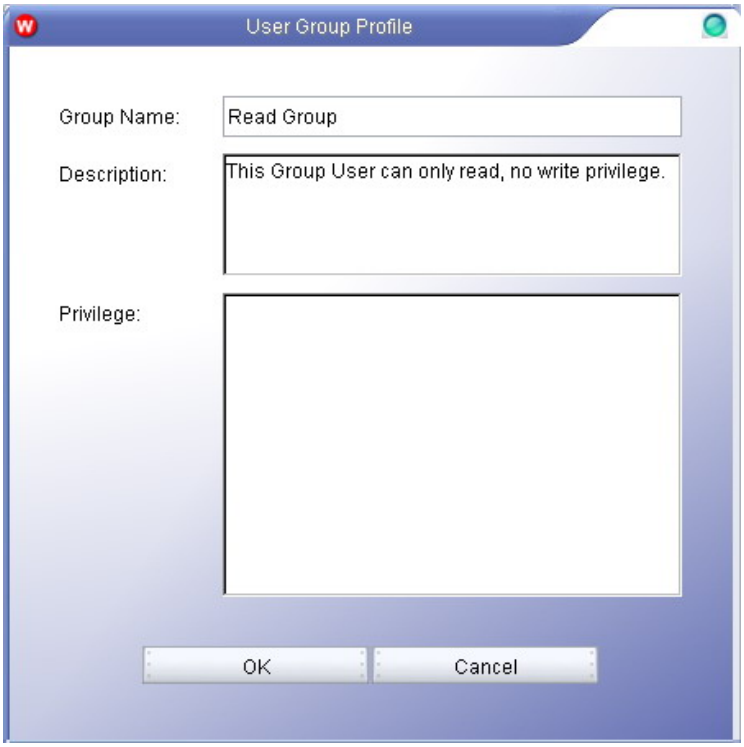
圖表 52: 個別使用者畫面。



圖表 53: 群組使用者畫面。

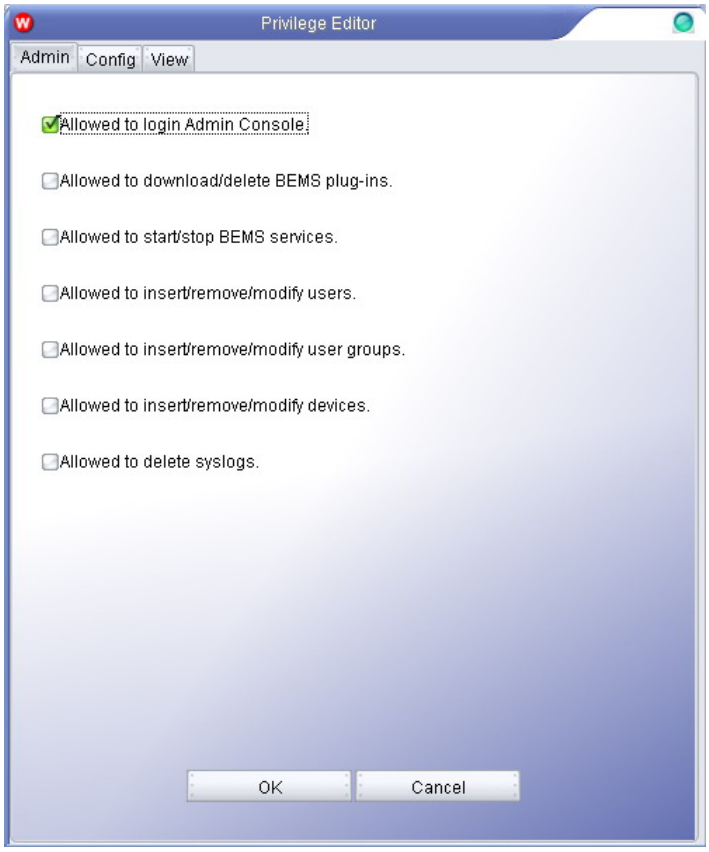
4.3.1 新增群組使用者 (Insert user group)

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。

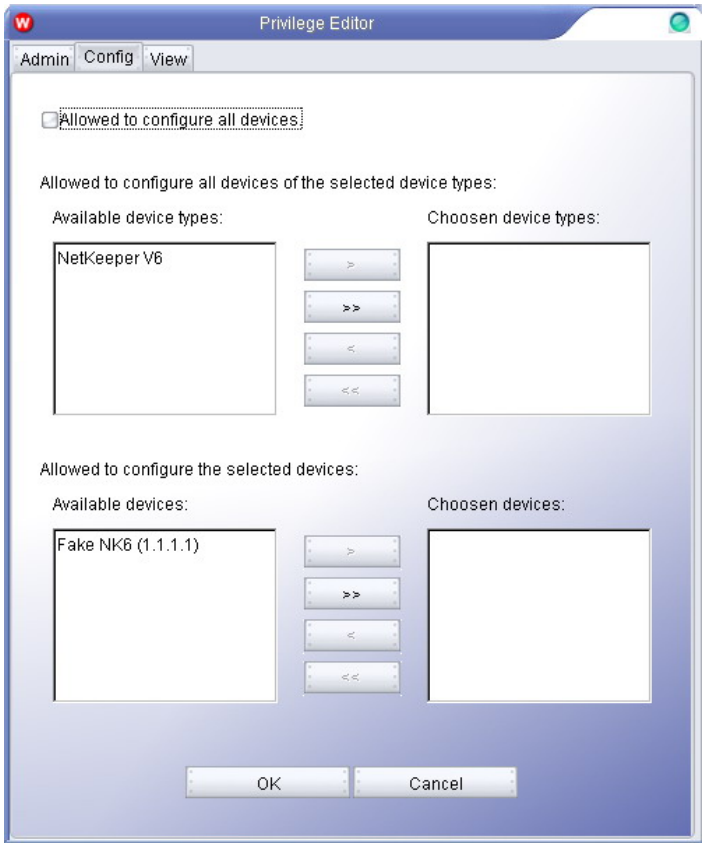


圖表 54: 群組使用者概況 (User Group Profile)

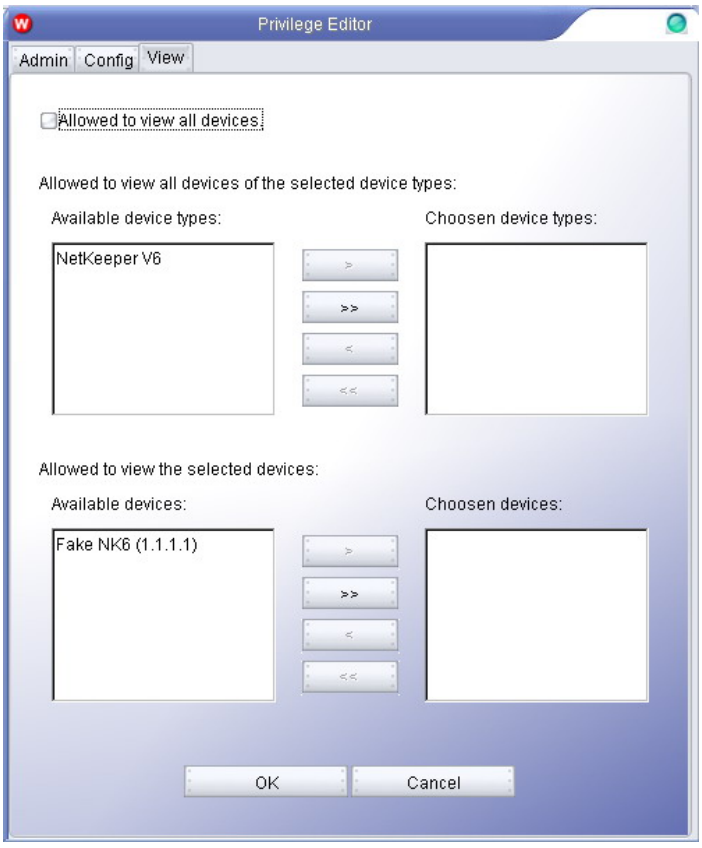
- 群組名稱 (Group Name)：由使用者自行定義。
- 說明 (Description)：由使用者自行加註此群組的說明。
- 權限 (Privilege)：定義此群組使用者的權限。當游標點選到該視窗，系統會自動彈出權限選擇視窗可供點選！
  - Admin: 設定該群組擁有登入 Admin Console 的權限與否，包括下載 Plug-in，啓動/關閉 BEMS 的服務，新增/刪除/修改管理設備，新增/刪除/修改使用者(群組)帳號，以及刪除系統記錄的權限。
  - Config: 設定該群組擁有被管理的硬體設備的設定 (config) 權限與否，除了區分爲設備種類之外，更可以區分到同類的的設備當中，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。



圖表 55: Admin 權限設定畫面。



圖表 56: Config 權限設定畫面。



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。

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)

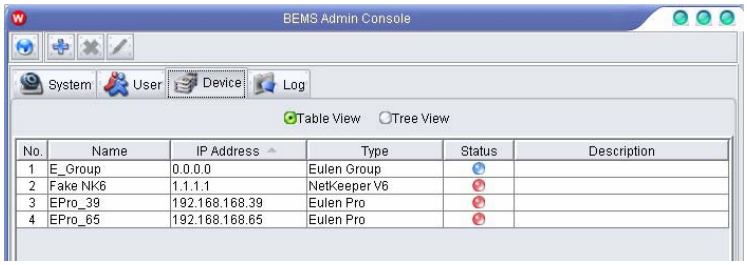
需要刪除不用的使用者時，使用者選擇使用者名稱之後，按下工具列中刪除個別使用者 (remove user) 的按鍵後確認即可。

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。

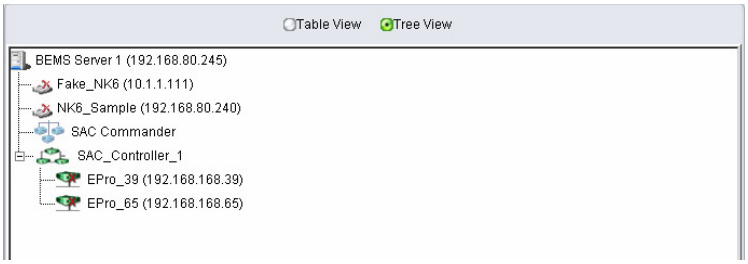
4.4 設備 (Device)

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。



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。

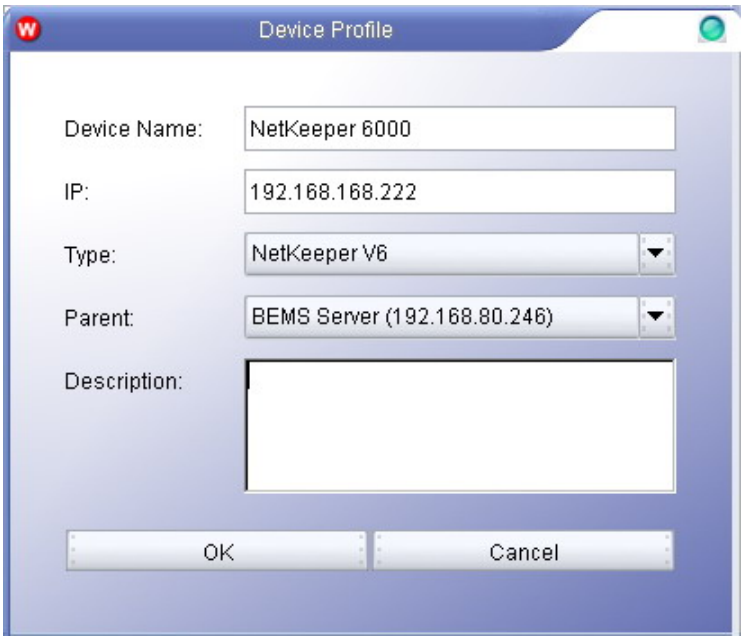


圖表 60: 設備清單圖示(樹狀模式)

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 位址爲 192.168.80.246 的 BEMS Server 所管理。
- 說明 (Description): 描述該設備的說明，內容爲由使用者自行定義。



圖表 61: 新增設備圖

4.4.2 刪除設備 (Remove device)

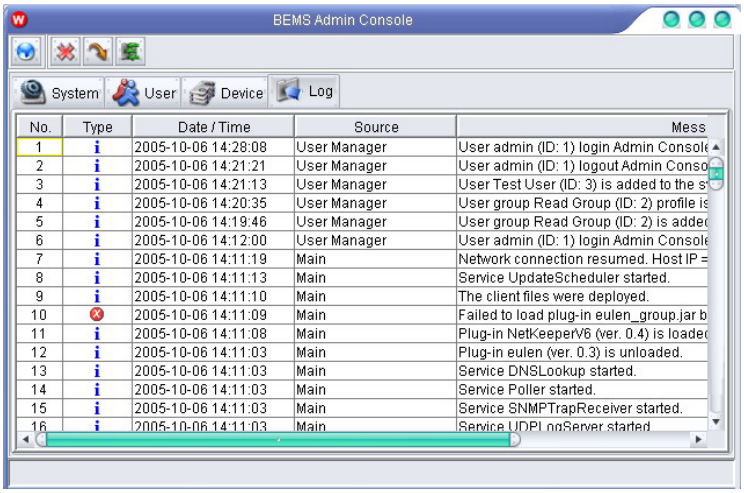
需要刪除設備時，使用者選擇該設備名稱之後，按下工具列中刪除設備 (remove device) 的按鍵後確認即可。

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。



圖表 62: 紀錄顯示畫面

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

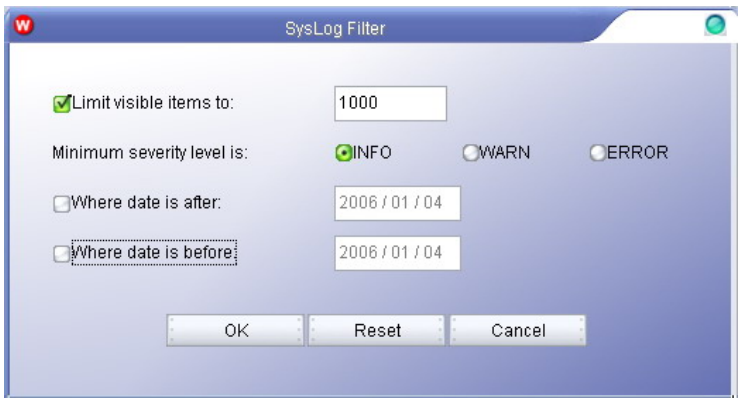
按下工具列按鍵，確定之後系統將清除所有系統記錄。

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



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

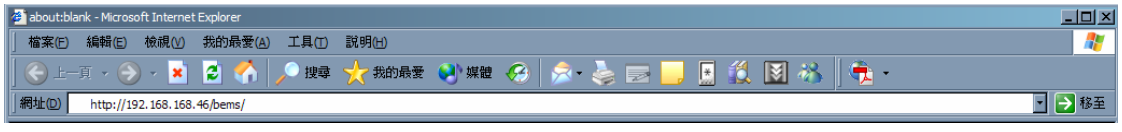
BEMS Server 啓動之後，使用者可以利用網路瀏覽器 (如 Internet Explorer 6.0) 透過網路連線到 BEMS 管理系統，進行網路安全防禦控管等等步驟。以下章節將說明如何運用 BEMS Server 與 Plug-in 的搭配，管理 IPS 的設備，建構安全的網路環境。

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！請注意因爲 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。

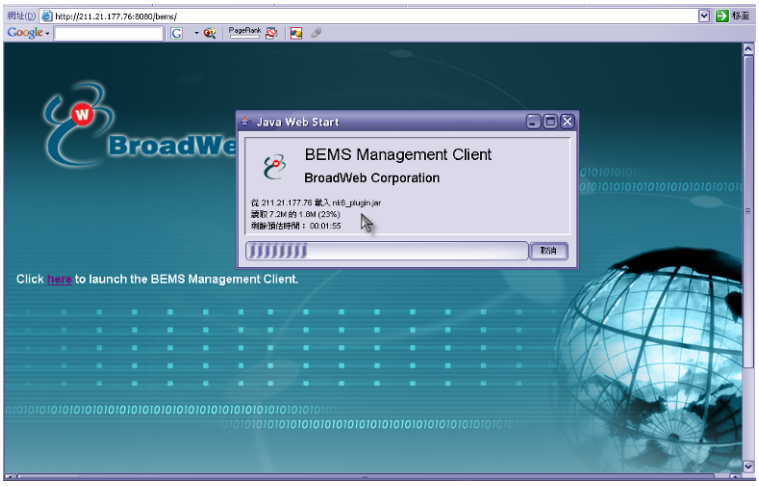
步驟說明如下：

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



圖表 64: 瀏覽器畫面

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

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。

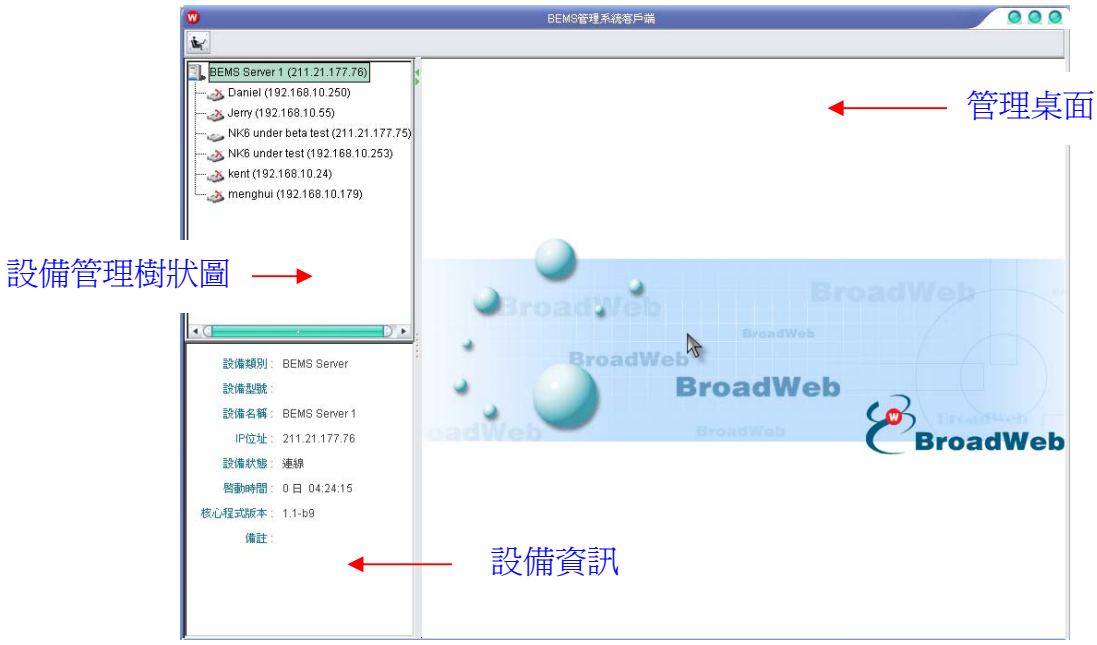
5.2 主要操作介面

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: 爲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

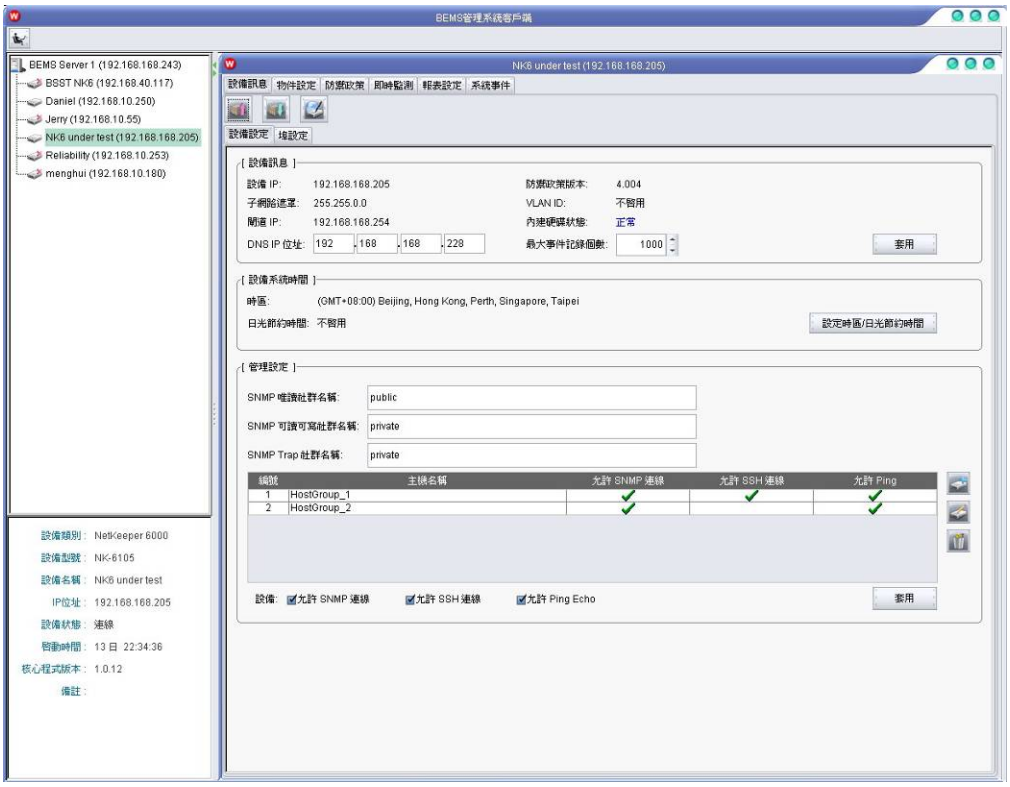
5.3 修改登入密碼

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。

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。



圖表 69: NK6 Plugin 畫面

6 第六章 設備訊息

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:

圖表 70: 工具列按鍵

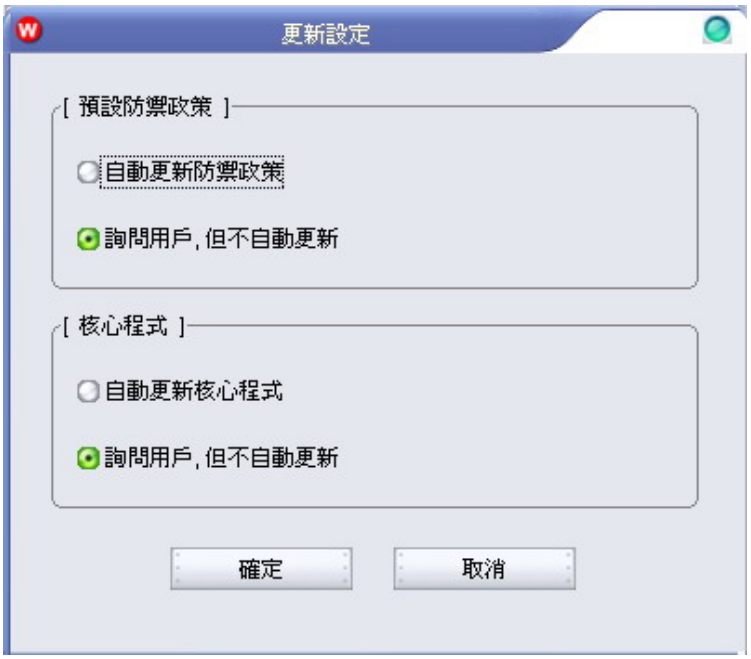
- 儲存設定 (Synchronize configuration to device): 將同步修改過後的設定值(object，rule…等等相關設定) 到設備中。按下此鈕，會出現如下提示等待畫面；完成設定，會出現如下設定成功提示畫面。

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)。

圖表 72: 儲存除錯資訊



圖表 73: 更新設定選項

於設備資訊的操作畫面中，可細分爲二個不同的子項目，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。

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。

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。

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

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。

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，每一部 IPS/IDS 虛擬設備都可以搭配不同的安全政策群組來獨立。

埠	E1	E2	E3	E4	E5	E6	E7
別名	IPS 1	IPS 1	IPS 2	IPS 2	IDS 1	IDS 2	埠 6
模式	IPS 模式	IPS 模式	IPS 模式	IPS 模式	IDS 模式	HA 模式	管理埠
防禦政策群組	RuleSet	RuleSet	RuleSet	RuleSet	Default		
忽略政策檢查							
忽略狀態檢查					✓		
忽略封包完整性檢查							
忽略碎片重組檢查							
忽略 VPN 檢查	✓	✓			✓		
忽略 ACL 政策檢查	✓	✓					
忽略埠掃瞄偵測							
忽略 GRE 解碼	✓	✓			✓		
忽略 IP 掃描檢查							

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爲。
  - IPS 模式: 此模式將兩個成對的連線埠視爲單獨一組 IPS 設備，依照單獨的安全防禦政策組來進行網路封包及行爲分析偵測，並且根據安全政策所訂定的防禦反應行爲來確保網路安全。
  - IPS-監視模式 (IPS-Monitor): 此模式將兩個成對的連線埠視爲單獨一組 IPS 設備，依照單獨的安全防禦政策組來進行網路封包及行爲分析偵測，但是僅進行事件記錄，不阻擋封包或是干擾連線行爲。
  - IDS 模式: 此模式將單一的連線埠視爲一組 IDS 設備，依照單獨的安全防禦政策組來進行網路封包及行爲分析偵測，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爲一組 IDS 設備，依照單獨的安全防禦政策組進行網路封包及行爲分析偵測，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。

圖表 80: 設定連線埠畫面

圖表 81: 設定 HA 功能埠畫面

7 第七章 物件設定

本章說明

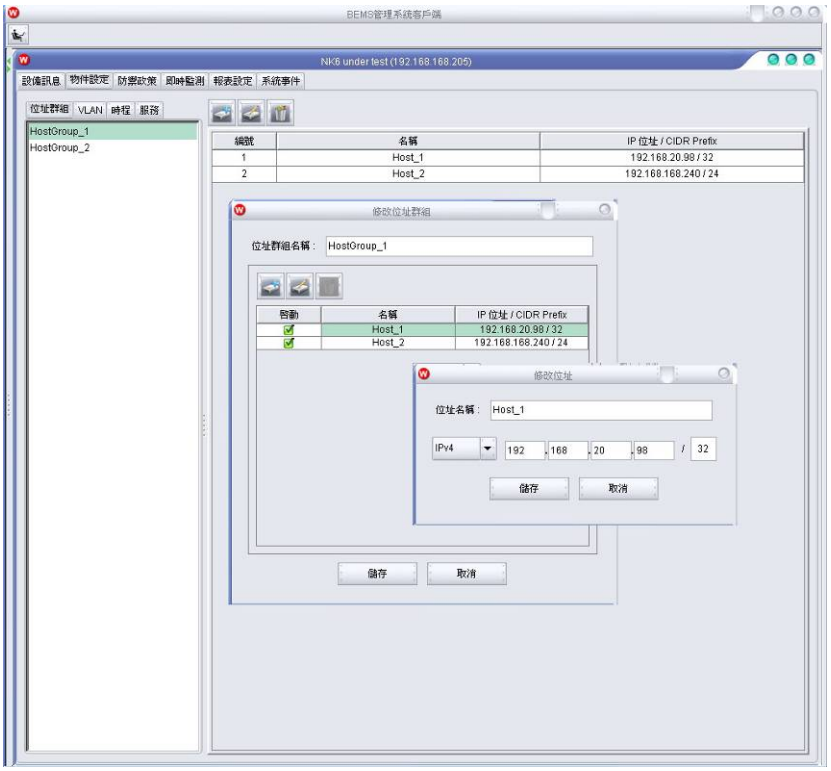
主要說明物件 (Object) 的設定。

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。左邊爲群組清單，右邊爲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。



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。

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。

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。

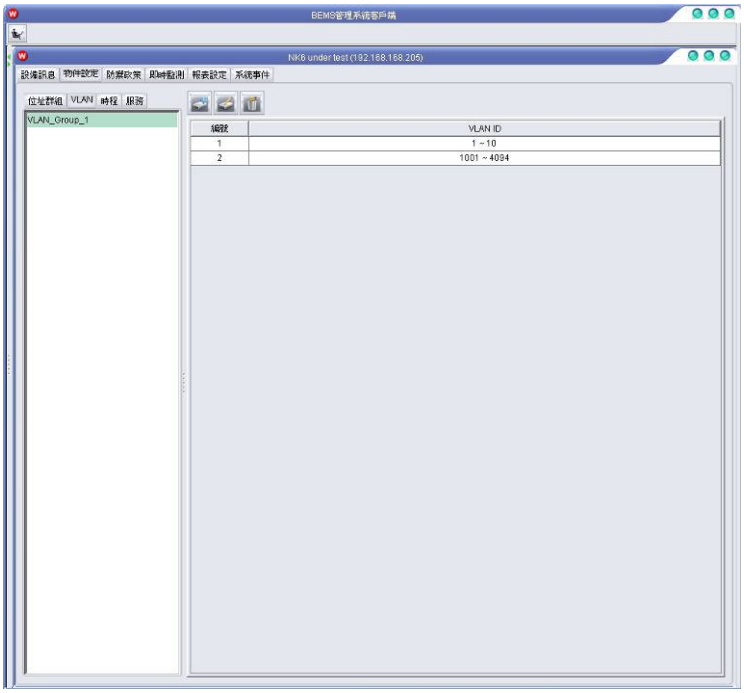
- ◆ 刪除主機 (DEL):
  刪除一組主機 (Host) 位址。選擇一組欲刪除的主機 (Host) 後，按下刪除 (DEL) 按鍵即可完成。

- ■ 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)、 刪除 (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)

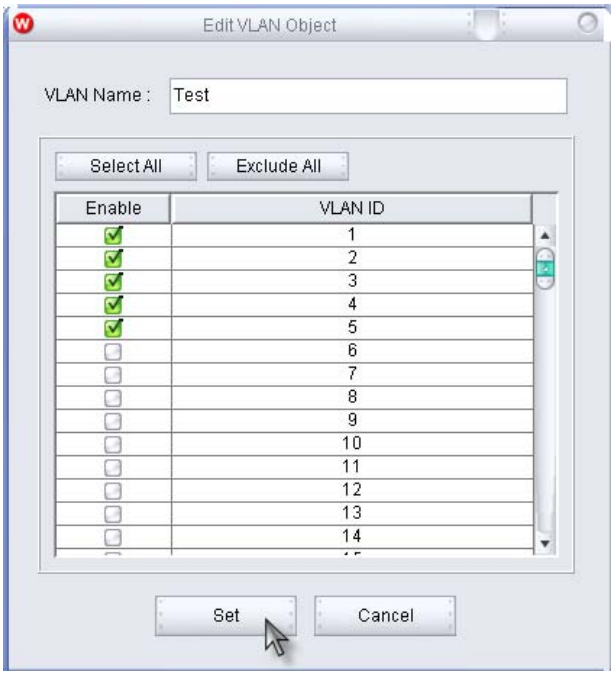
說明如何定義虛擬網路 (VLAN: Virtual LAN) 物件。左邊爲虛擬網路物件清單，右邊爲目前選取的虛擬網路物件中有核取的虛擬網路代碼 (VLAN ID)。上方有按鍵可以新增 (ADD)、修改 (EDIT)、刪除 (DEL) 虛擬網路物件。



圖表 85: VLAN 參數畫面

按鍵功能說明:

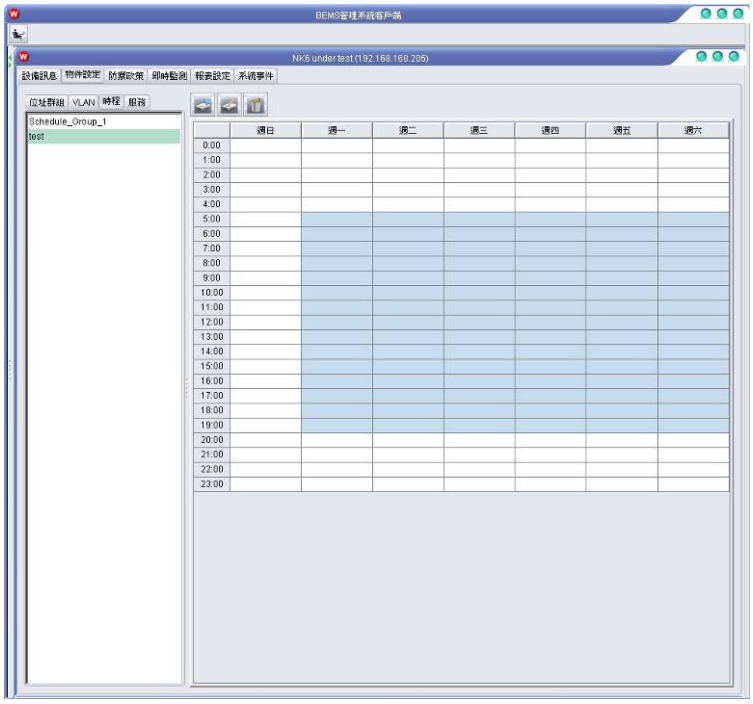
- 新增 (ADD):
  加入新的虛擬網路 (VLAN) 物件，如圖表 86。將啓動 (Enable) 的核取方塊打勾，即可將此虛擬網路代碼 (VLAN ID) 加入此虛擬網路 (VLAN) 物件中。中間可以選擇全選 (Select All) 或取消選擇 (Exclude All)。
- 修改 (EDIT):
  修改已存在的虛擬網路 (VLAN) 物件，修改操作畫面雷同圖表 86。修改完畢後按下儲存 (Set) 按鍵即可完成。
- 刪除 (DEL):
  刪除已存在的虛擬網路 (VLAN) 物件。選擇後按下刪除 (DEL) 按鍵即可。



圖表 86: 修改 VLAN 物件

7.3 時程設定 (Schedule Configuration)

說明如何定義時程 (Schedule) 物件，如圖表 87。左邊爲時程 (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。



圖表 87: 時程 (Schedule) 畫面

按鍵功能說明:

- 新增 (ADD):

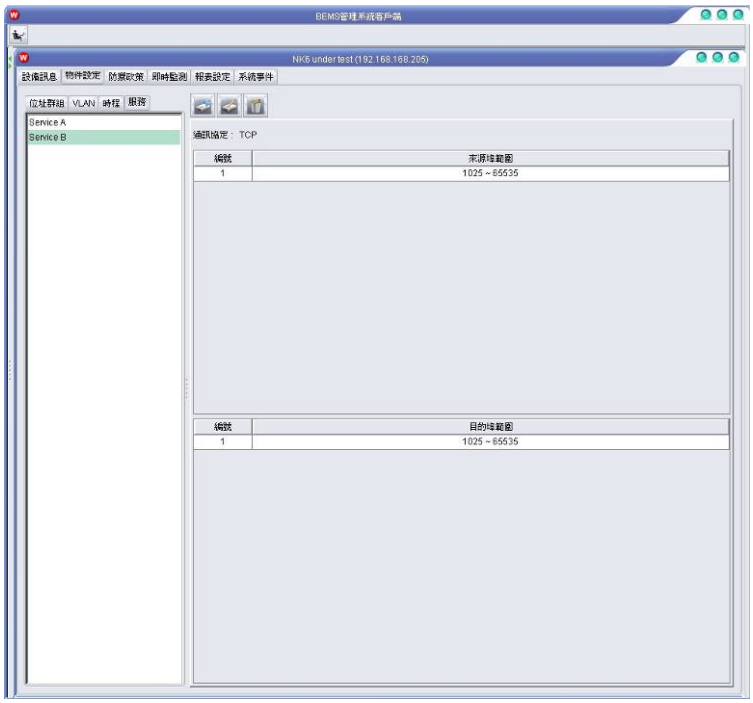
  加入新的時程 (Schedule) 物件，如圖表 88。輸入時程名稱，並點選所要排入時程的時段，即可將此時段加入此時程物件中。時段顏色改變表示該時段已經被選取，另外也可以利用移動滑鼠進行大範圍的選取。

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):
  刪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。左邊爲服務 (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。



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 範圍爲 0 ~ 65535，ICMP 範圍爲 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。

圖表 90: 新增/修改服務 (Service) 畫面

◆ 新增 (ADD)、修改(EDIT) 範圍:

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

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

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。

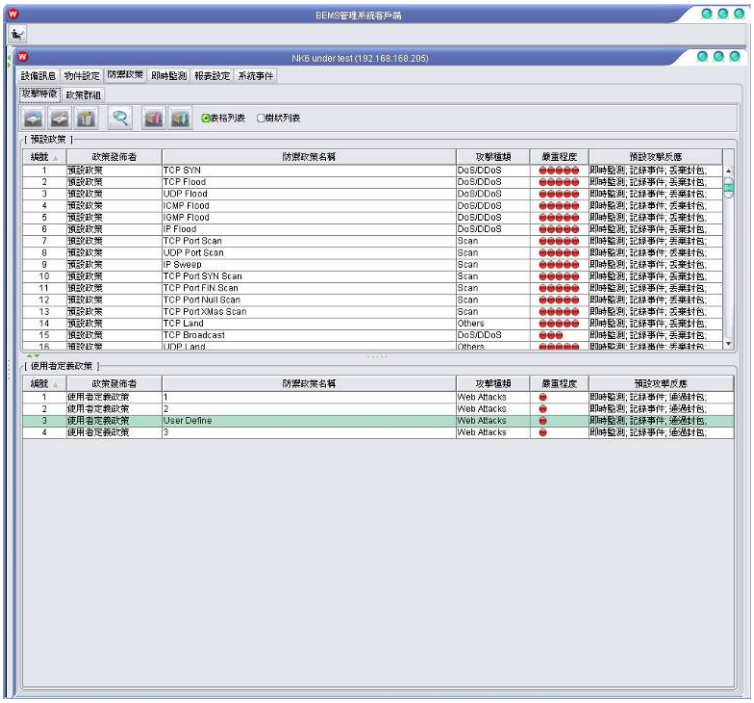
攻擊特徵 (Signature) 指的是網路防禦政策當中最重要的比對資料。不管是已知或是未知的網路異常行爲，或者是程式漏洞等等，多多少少都會有一定的特徵可以被辨識出來。只要能掌握網路封包的特徵，就可以預防駭客的網路攻擊，或是防制不正常的網路行爲發生。

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。上方爲原廠提供的預設防禦政策。下方爲使用者自訂防禦政策。



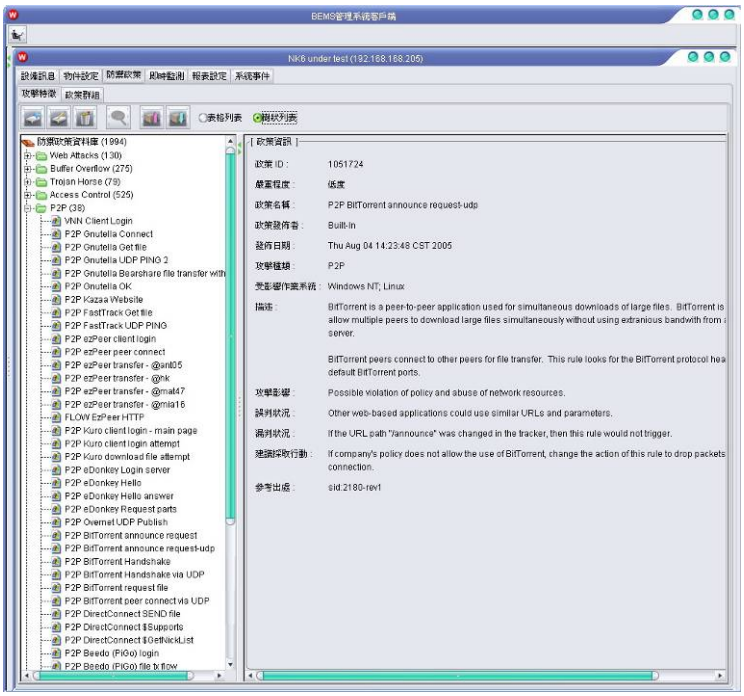
圖表 92: 表格列表模式 (Table View) 畫面

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,區分爲五級: :輕微威脅 :低度威脅 :中度威脅 :高度威脅 :嚴重威脅
攻擊種類	系統預設值內定 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
預設攻擊時的反應	定義發現攻擊時所觸發之動作，系統提供五種動作: 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:

-  : 新增政策。使用者可以依照需求新增自訂安全防禦政策。
-  : 修改政策。可以修改政策。
-  : 刪除政策。可以刪除政策。
-  : 根據特定字串搜尋政策。
-  : 匯出政策到檔案。
-  : 從檔案匯入政策。

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。

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): 此名稱是作爲識別之用，用來顯示在回報系統與電子郵件之中。此欄位必須爲唯一。
    - 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。此項設定目的爲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/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爲零。
    - 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。

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。

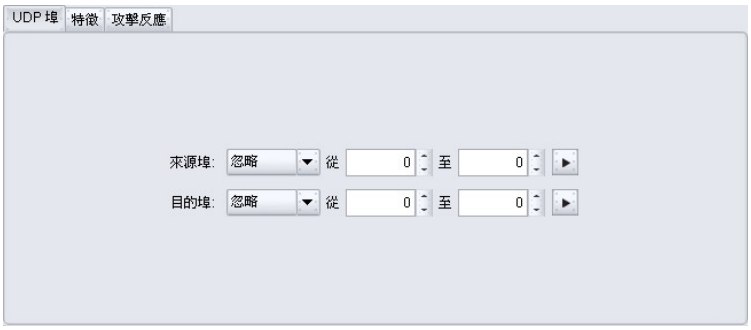
圖表 97: 選項

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: 選擇通信協定爲 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。

圖表 98: TCP port 選項



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。此爲預設之比對方法。
- 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爲 URL 的基本，問號之後的字串會被視爲是此 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。

圖表 100: 特徵比對模式

圖表 101: 特徵型態

- ◆ 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): 內容爲十六進位模式字串。
  - 八進制 (Octal): 內容爲八進位模式字串。
  - 十進制 (Decimal): 內容爲十進位模式字串。
  - IP 字串 (IP String): 內容爲 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，最大長度爲 128 個字元。

圖表 102: 特徵內容

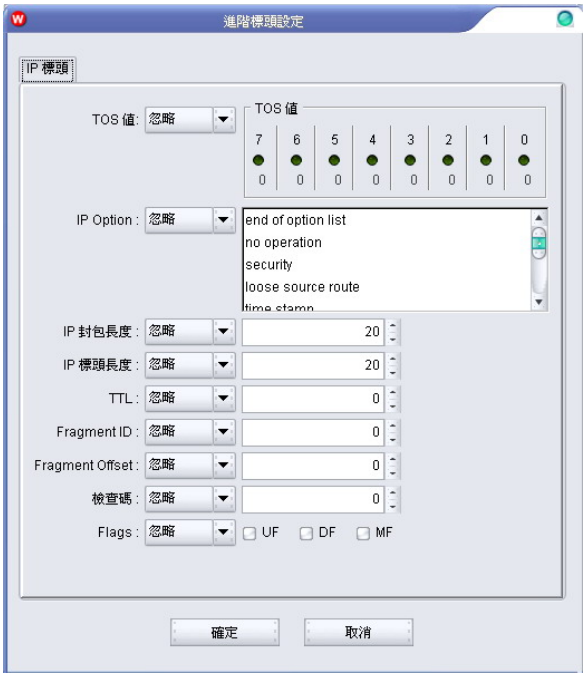
■ 攻擊反應 (Action): 定義此安全防禦政策的反應動作。

- ◆ 通過: 無條件放行封包通過。
- ◆ 阻絕: 阻絕符合特徵條件的封包。若選擇通信協定爲 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。

圖表 103: 攻擊反應

(2). 進階設定:

- IP 封包標頭: 爲 IP 封包標頭欄位設定值參數所組成。
  - 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



圖表 104: 進階設定: IP 標頭

- TCP 封包標頭: 爲 TCP 封包標頭欄位設定值參數所組成。
  - 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

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。

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。

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。

圖表 108: 進階設定: IGMP 標頭

- **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。預設值爲空白，由使用者自行定義。

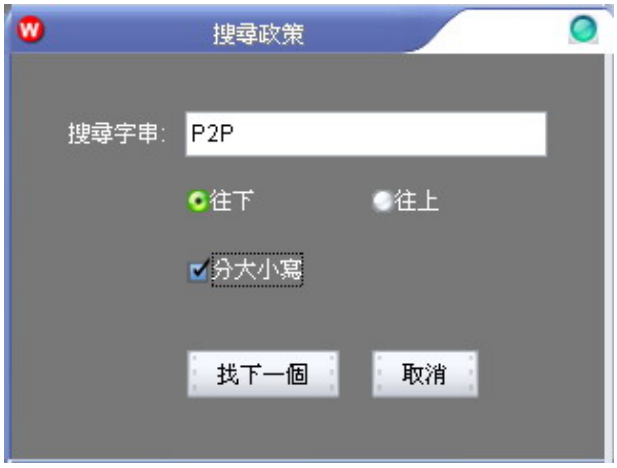
8.3.2 修改 / 刪除政策

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

- : 根據特定字串搜尋政策。

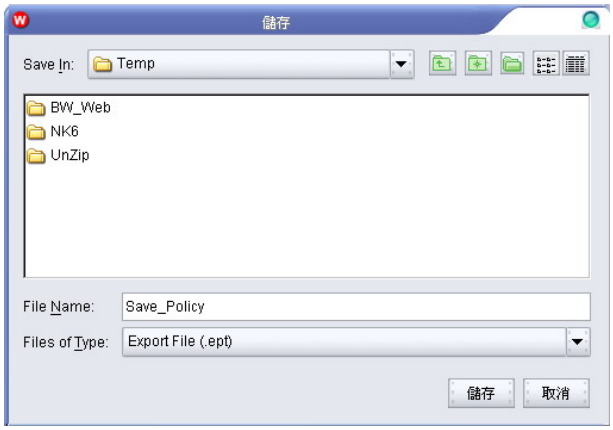
按下按鍵後，會出現使用者輸入搜尋政策的畫面，輸入後即可快速搜尋防禦政策。此功能提供客戶可以快速找到所需要的政策。於視窗中輸入完關鍵字後，按下搜尋下一筆即可進行。視窗會停留在搜尋到的第一筆政策，以供使用者做進一步的處理。



圖表 109: 搜尋政策

■  : 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。

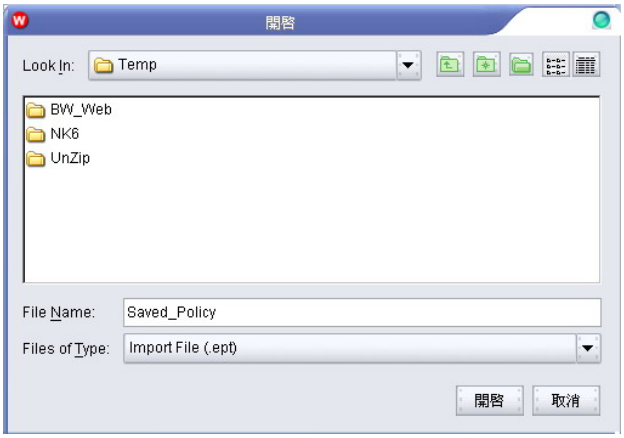


圖表 110: 匯出政策儲存成檔案

■  : 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。

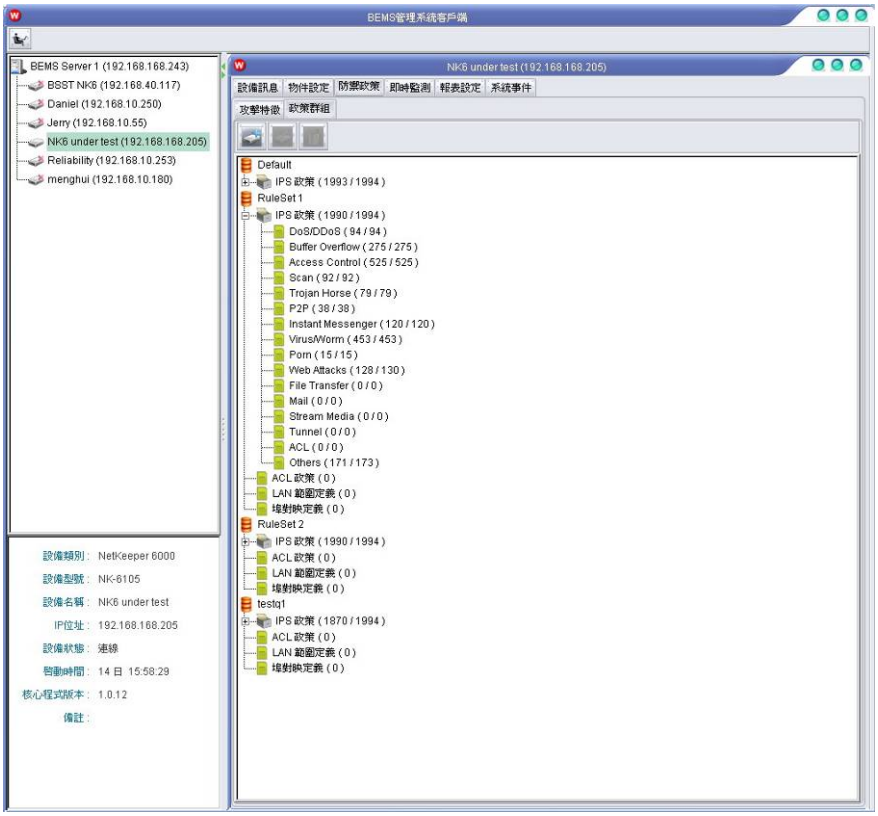


圖表 111: 選擇檔案匯入政策

8.4 政策群組

爲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。

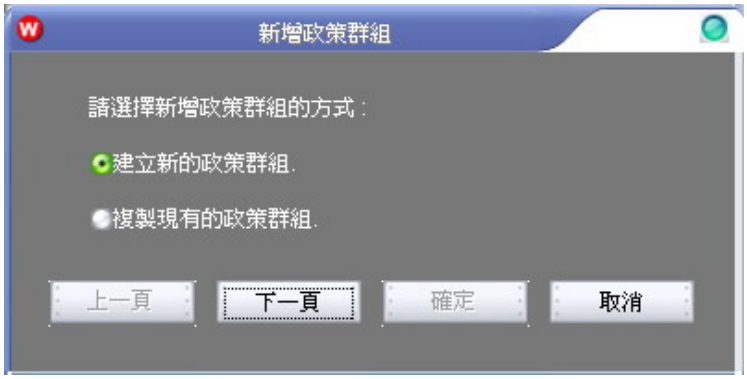


圖表 112: 防禦政策群組畫面

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。



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。

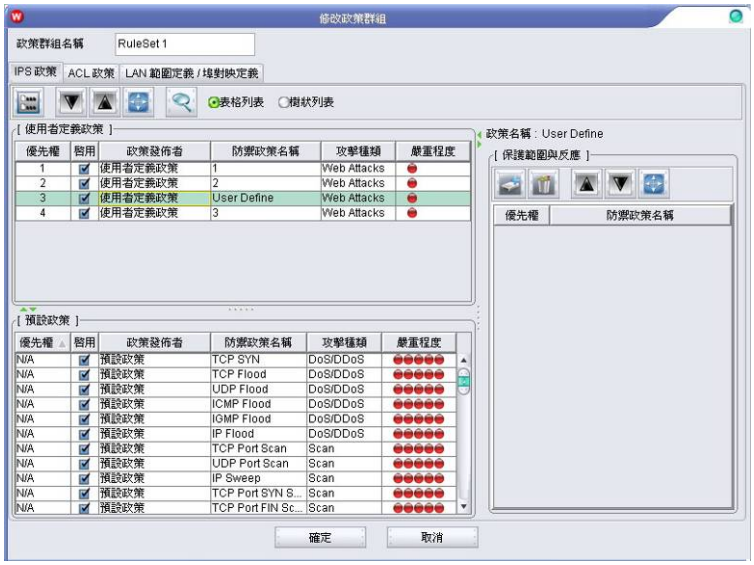
圖表 114: 選擇政策偵測範圍

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。

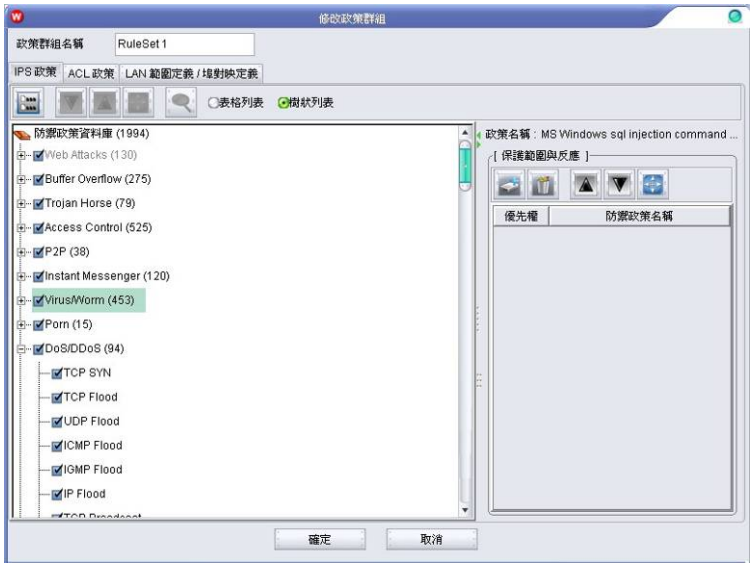
8.4.3 修改政策群組

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。



圖表 115: 修改政策群組圖-1 (表格模式)

圖表 116: 修改政策群組圖-2 (表格模式)



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、安全防禦的反應行爲等等之外，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:

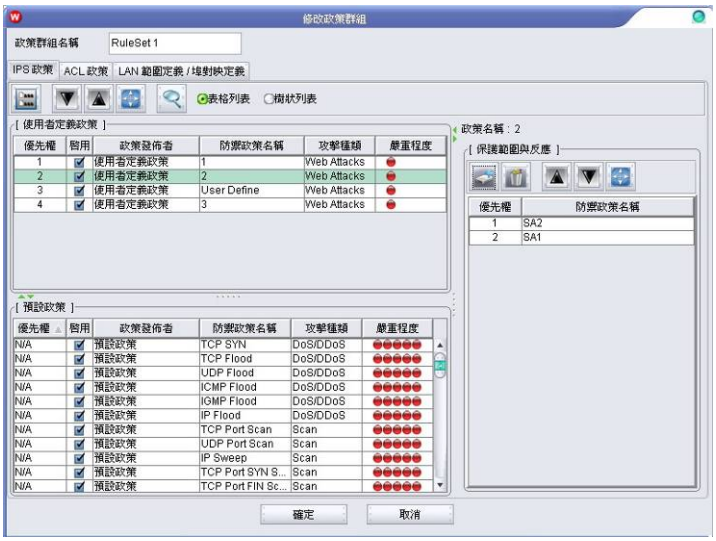
-  : 過濾設定。使用者可以依照需求適度調整被啓動的安全防禦政策。
-  : 提升使用者定義政策優先權。向上調整優先順序一位
-  : 降低使用者定義政策優先權。向下調整優先順序一位
-  : 更改使用者定義政策選擇優先權。使用者可以針對特殊的網路環境需求而調整政策的優先順序。一旦網路封包被政策偵測比對引擎判定爲有問題時，會依照高優先權的政策保護範圍、反應、以及時程而進一步處理。
-  : 搜尋政策。搜尋政策中之特殊字串。此功能提供客戶可以快速找到所需要的政策。於視窗中輸入完關鍵字後，按下搜尋下一筆即可進行。政策表格視窗會停留在搜尋到的第一筆政策，以供使用者做進一步的處理。

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。

圖表 118: 修改政策畫面之一

圖表 119: 修改政策畫面之二



圖表 120: 修改政策畫面之三

爲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)，反應行爲的預設值請參考 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。
-  : 刪除。刪除已選擇的防禦範圍與反應。
-  : 提升優先權。向上調整優先順序一位
-  : 降低優先權。向下調整優先順序一位
-  : 更改優先權。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爲有問題時，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。

圖表 121: 保護範圍與反應

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，且總和值不得超過「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，且總和值不得超過「總量限制」欄所指定的大小。封包總量以天爲單位，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。

圖表 123: ACL 政策畫面

上方工具列按鍵功能說明:

-  : 新增。可新增防火牆連線管控政策 (ACL)。
-  : 編輯。可編輯防火牆連線管控政策 (ACL)。
-  : 刪除。刪除已選擇的政策。

按下『新增』按鍵，系統會出現編輯 ACL 政策的畫面:

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)

爲了解決 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。

圖表 125: LAN 範圍定義

上方工具列按鍵功能說明:

■  : 新增。可新增 LAN 端的 IP 位址。

■  : 編輯。可編輯 LAN 端的 IP 位址。。

■  : 刪除。刪除已選擇的 LAN 端 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。

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。

圖表 127: 連線埠對映

上方工具列按鍵功能說明:

-  : 新增。可新增對映連線埠。
-  : 編輯。可編輯對映連線埠。
-  : 刪除。刪除已選擇的對映連線埠。

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。

圖表 128: 定義連線埠對映

9 第九章 即時監測

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』鍵可以將統計值歸零，重新開始計算。

圖表 129: 儀表版 (Dashboard)

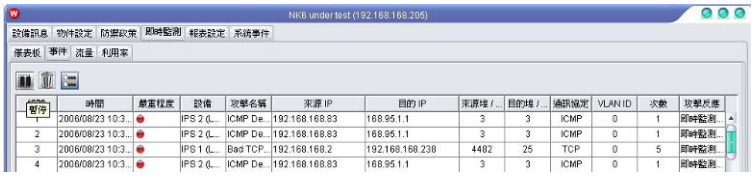
9.2 事件 (Event)

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。



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，圖示隨即變爲『暫停』鍵。

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。

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

■ 丟棄封包流量顯示:

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

圖表 134: 流量一 (Traffic)

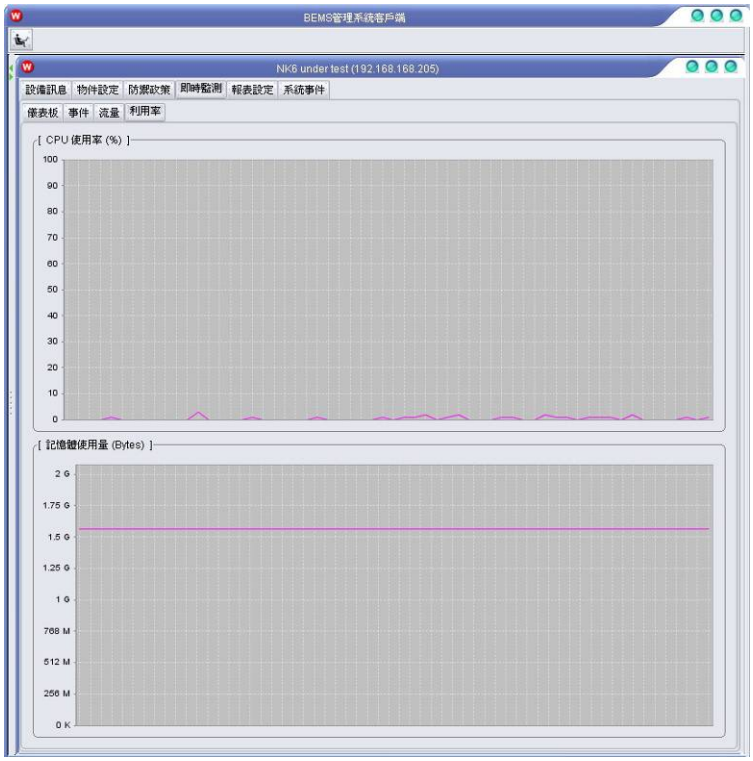
■ 服務封包流量顯示:

以第七層應用協定爲分類，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)

10 第十章 報表設定

本章說明

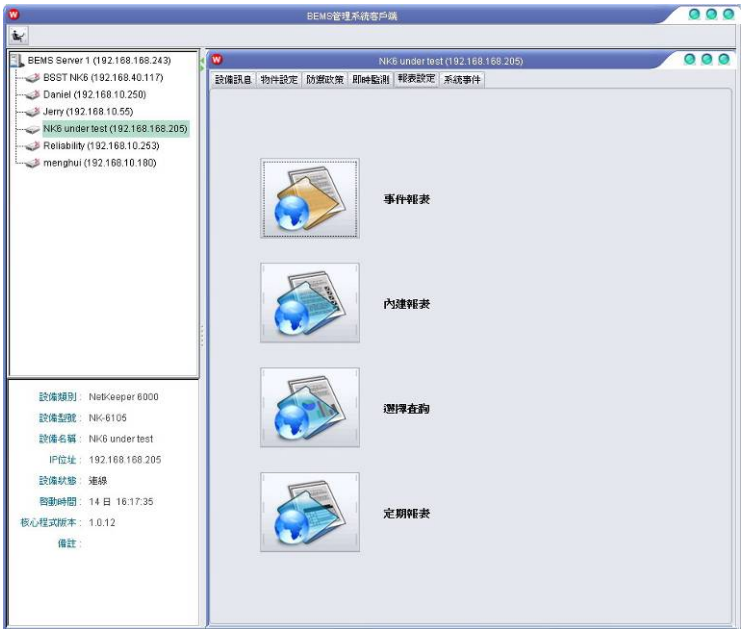
主要說明報表系統的設定操作步驟。

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。



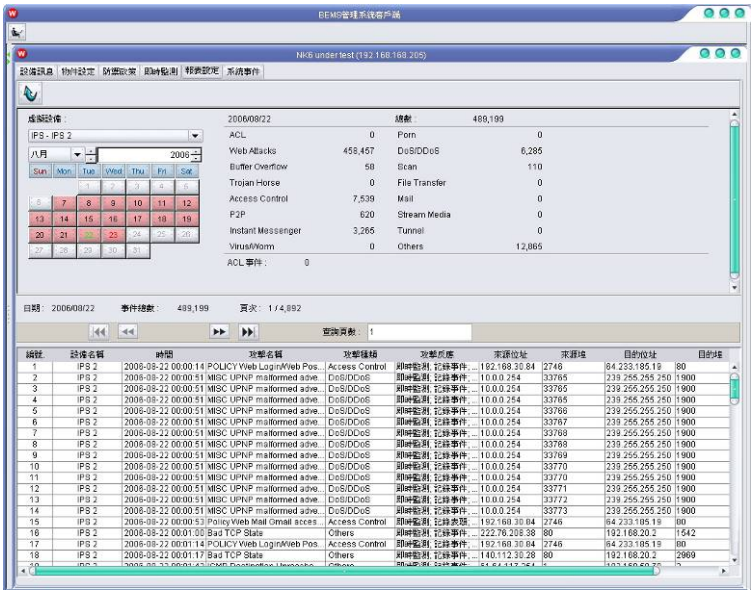
圖表 137: 報表設定畫面

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:

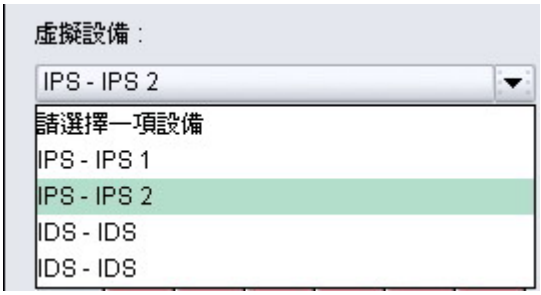
■  : 回到上一頁。



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。



圖表 139: 選擇虛擬設備

10.1.2 月曆

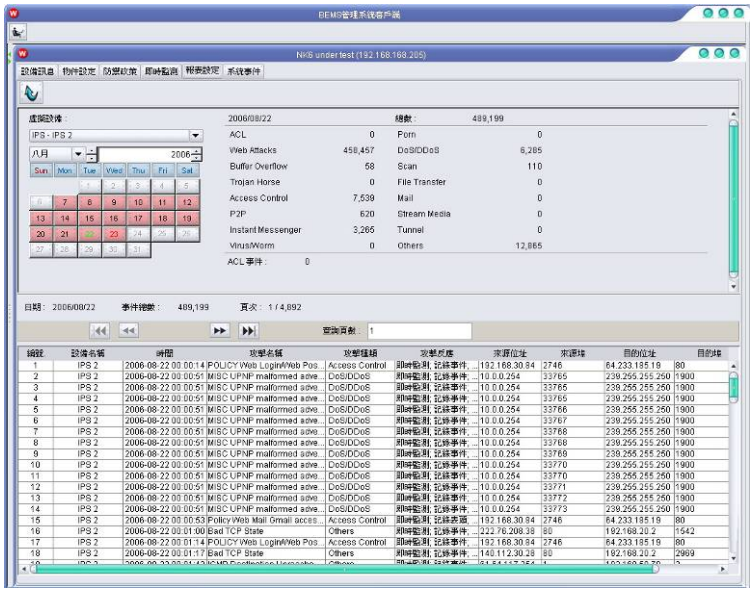
選完設備後，使用者可自行選擇日期來顯示事件列表。以一天爲最小統計單位。

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一一顯示出來，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。



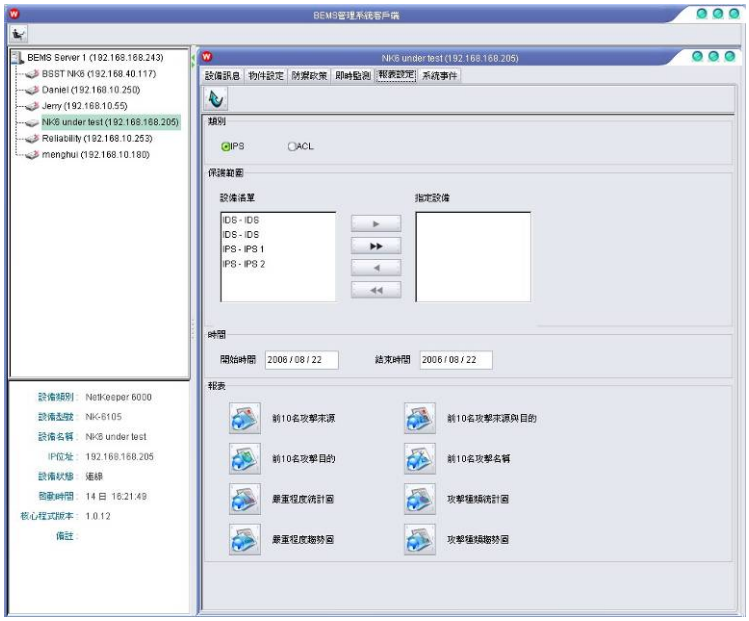
圖表 141: 事件列表顯示 (Event List)

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。

按鍵說明:

■  : 回到上一頁。



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。

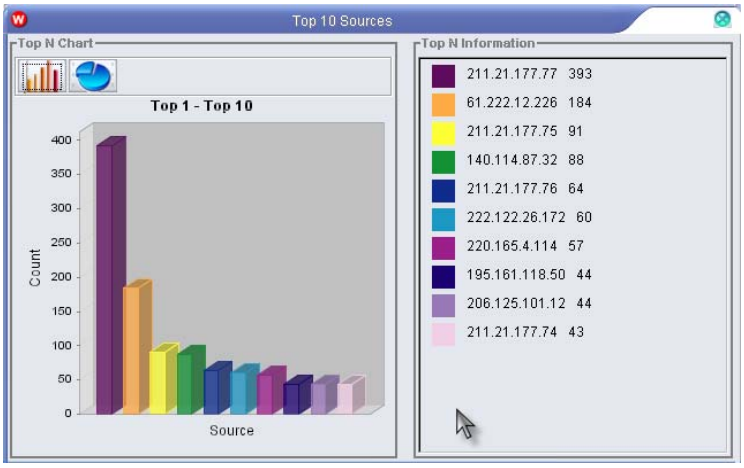
10.2.5 內建報表範例 (IPS 類)

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。

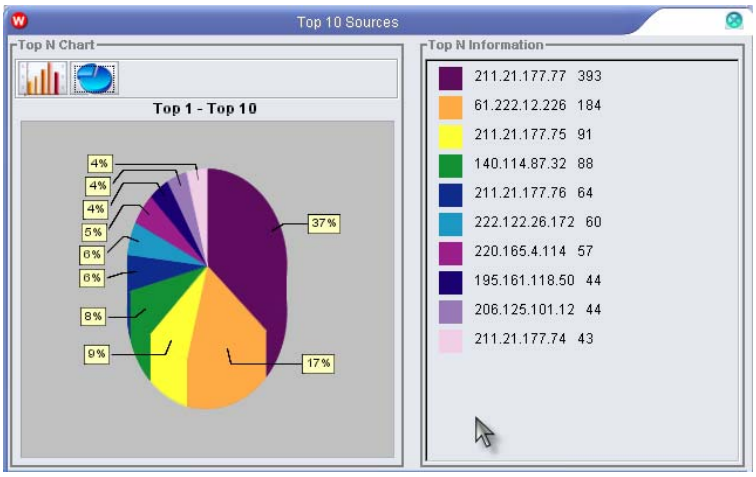
圖表 143: IPS 類之內建報表

- 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。



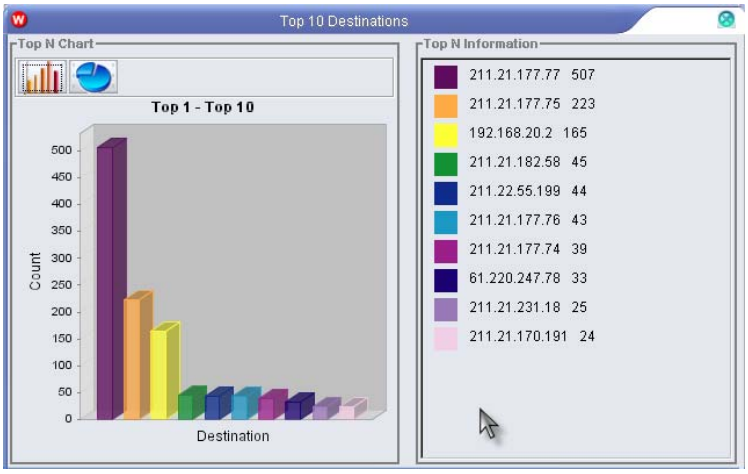
圖表 144: 前 10 名攻擊來源長條圖



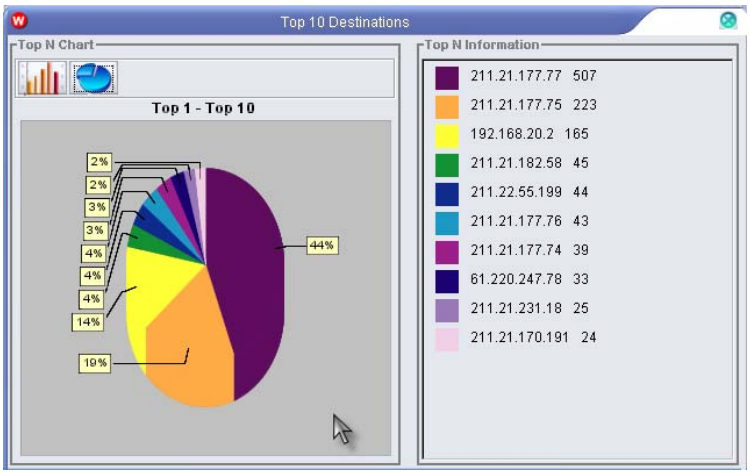
圖表 145: 前 10 名攻擊來源圓餅圖

■ 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。



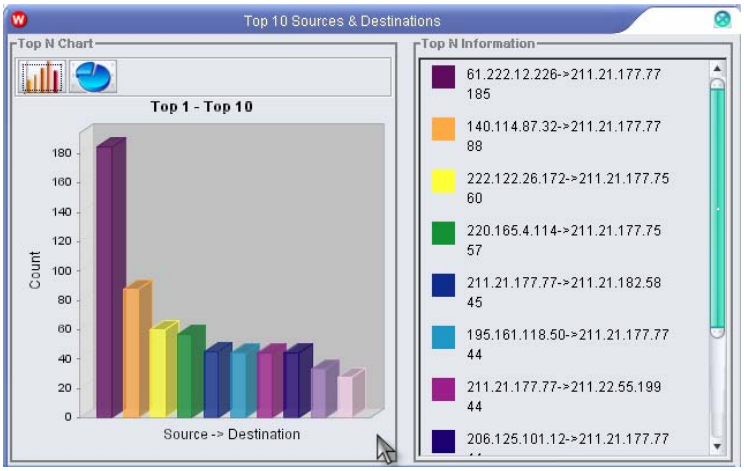
圖表 146: 前 10 名攻擊目的長條圖



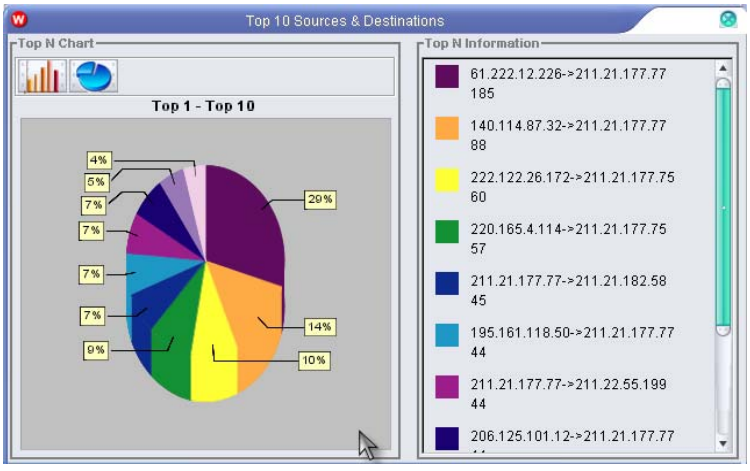
圖表 147: 前 10 名攻擊目的圓餅圖

■ 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。



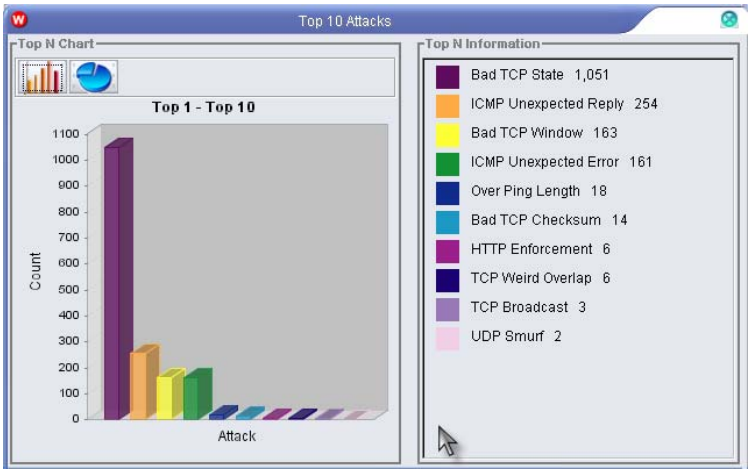
圖表 148: 前 10 名攻擊來源與目的長條圖



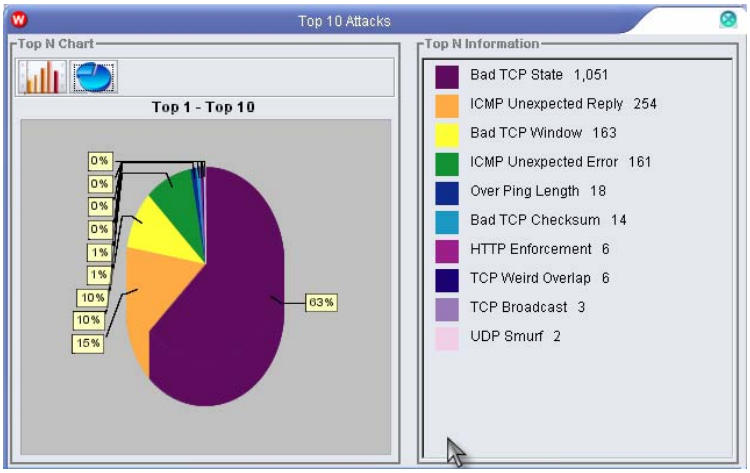
圖表 149: 前 10 名攻擊來源與目的圓餅圖

■ 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。



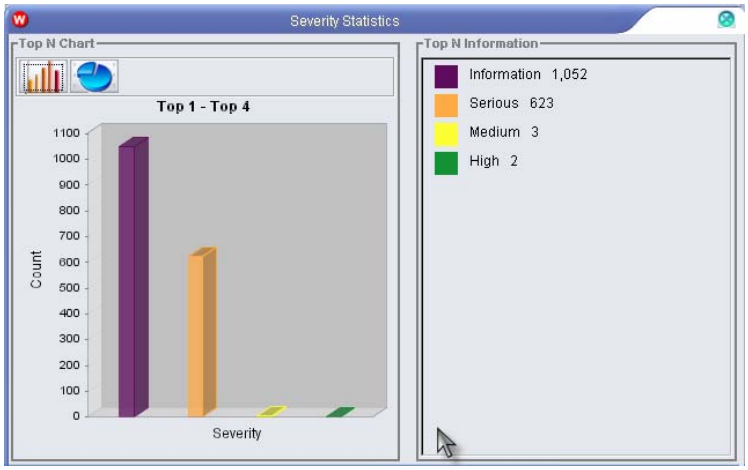
圖表 150: 前 10 名攻擊名稱長條圖



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。

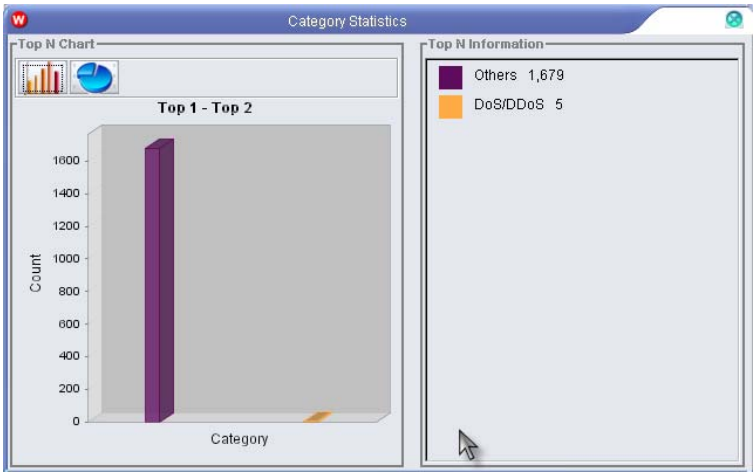


圖表 152: 嚴重程度統計長條圖

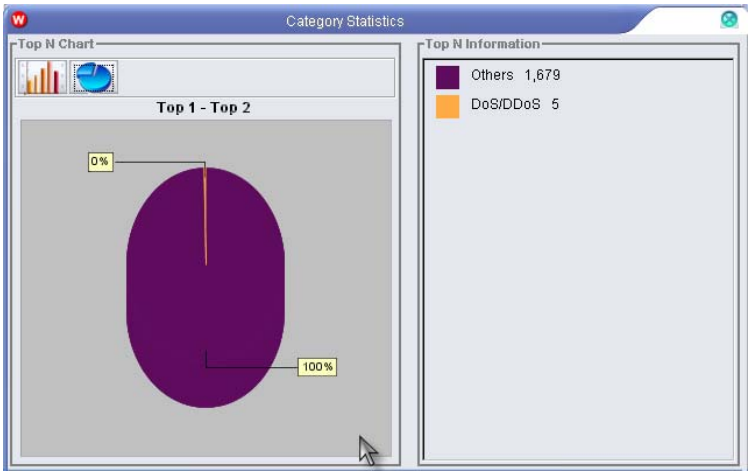
圖表 153: 嚴重程度統計圓餅圖

■ 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。



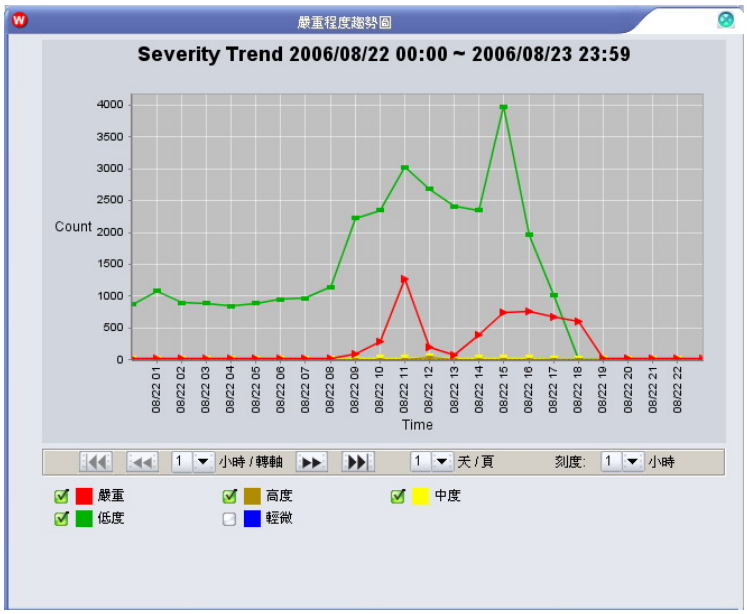
圖表 154: 攻擊種類統計長條圖



圖表 155: 攻擊種類統計圓餅圖

■ 嚴重程度趨勢圖

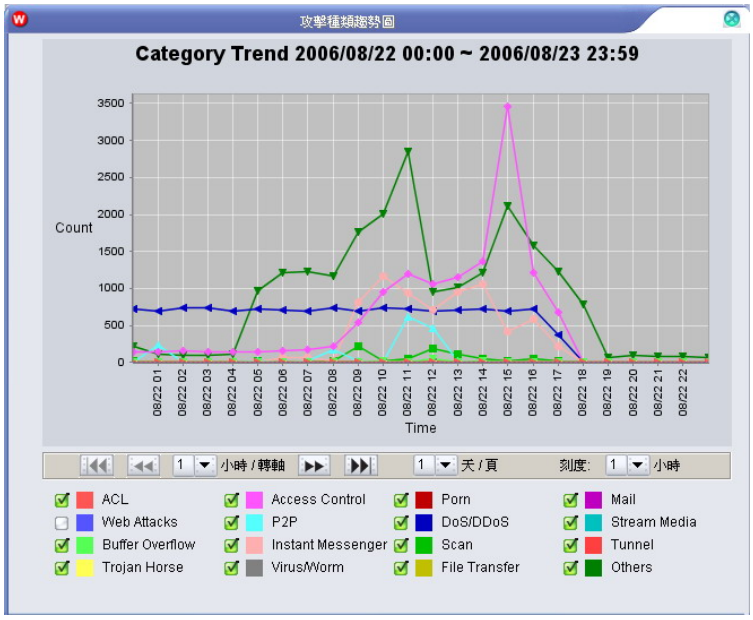
利用曲線圖繪出不同時間點的攻擊數量，不同顏色的線代表不同的嚴重性等級。可利用左右箭頭按鍵來控制所要看的時間點，左右箭頭按鍵中間可設定每次移動的間隔。並可設定每個頁面顯示幾天的資料量，以及多久間隔劃一次節點。



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。



圖表 157: 攻擊種類趨勢圖 (Category Trend)

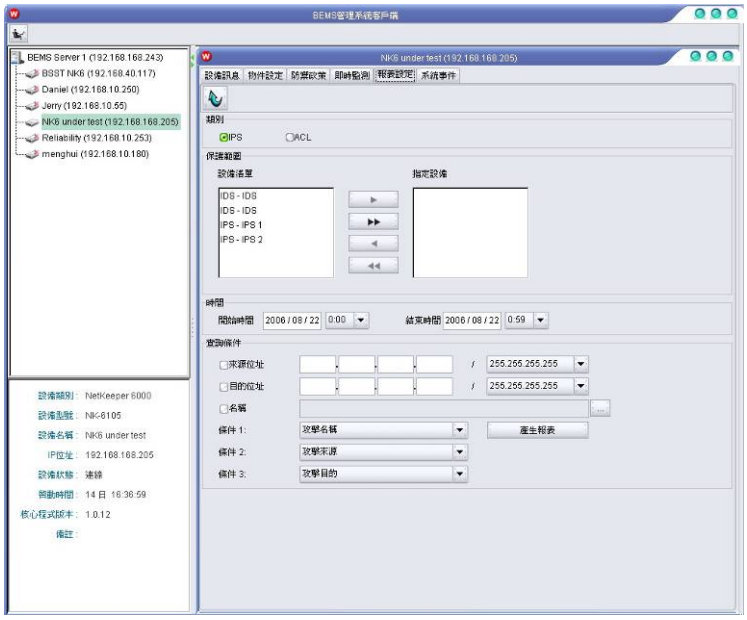
10.2.6 內建報表範例 (ACL 類)

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。



圖表 159: 選擇查詢 (Query on Demand)

按鍵說明:

■  : 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。

圖表 160: 選擇設備清單

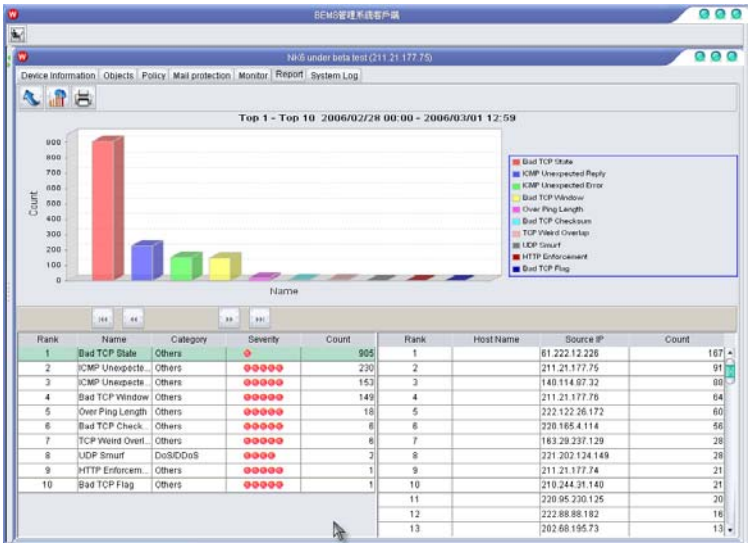
圖表 161: 選擇日期

- 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。

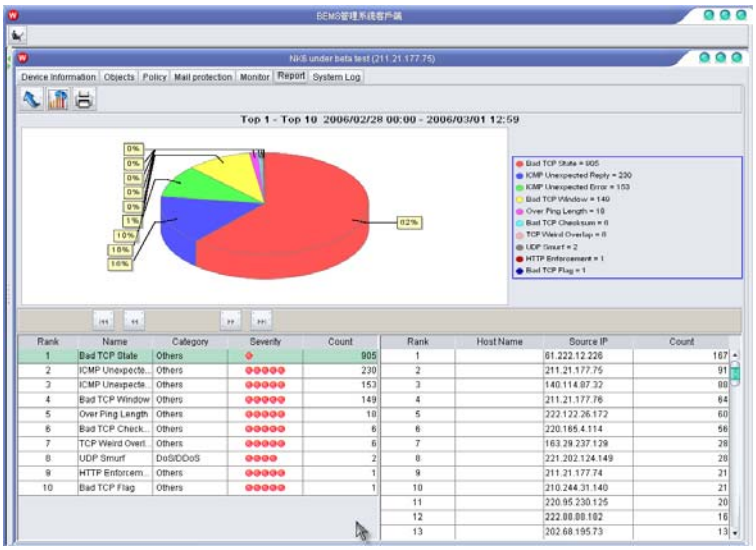
圖表 162: 查詢條件

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，右下方爲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。

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。



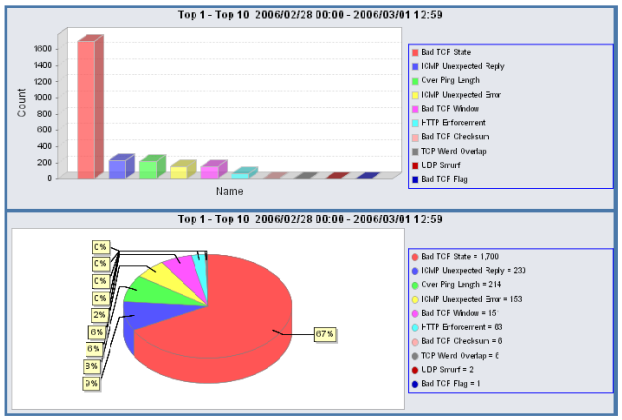
圖表 163: Query on Demand 長條圖



圖表 164: Query on Demand 圓餅圖

Name

NetKeeper Device IP : NK-6

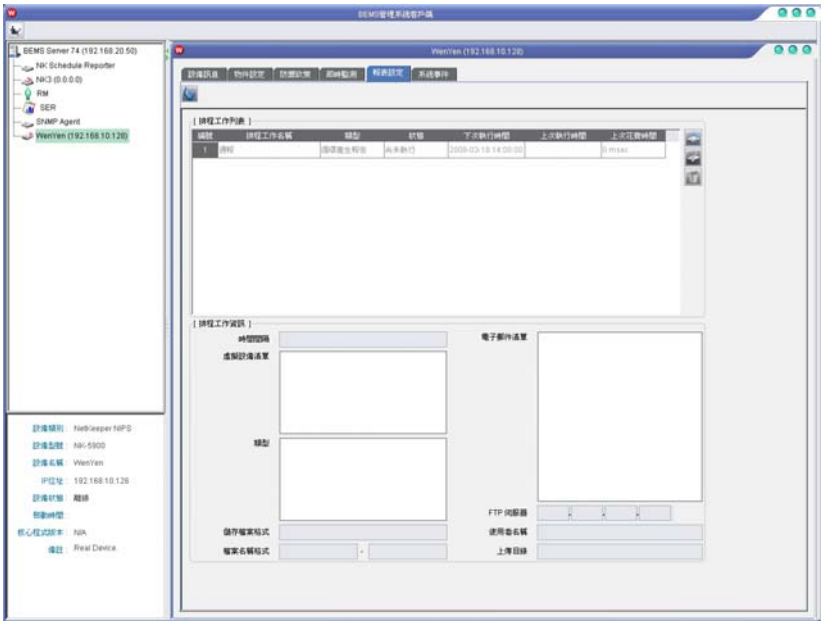


Rank	Name	Category	Severity	Count
1	Bad TCP State	Others	Information	1,700
2	ICMP Unexpected Reply	Others	Serious	230
3	Over Ping Length	Others	Serious	214
4	ICMP Unexpected Error	Others	Serious	153
5	Bad TCP Window	Others	Serious	151
6	HTTP Enforcement	Others	Serious	63
7	Bad TCP Checksum	Others	Serious	6
8	TCP Weird Overlap	Others	Serious	6
9	UDP Smurf	DoS/DDoS	High	2
10	Bad TCP Flag	Others	Serious	1
11	Fake ICMP Error Message	Others	Serious	1

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:

-  : 回到上一頁。

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。

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。

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。

圖表 168: 新增/編輯排程工作(頁面二)

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。

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。

圖表 170: 新增編輯報表樣本

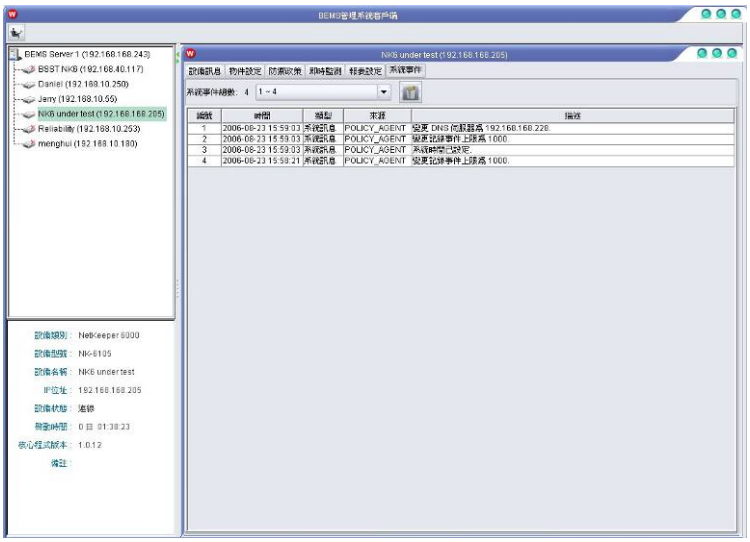
用戶設定好參數後，按下確定即完成新增報表樣本。

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：



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): 設備傳遞訊息爲無效訊息。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，例如因爲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：

-  : 刪除紀錄，刪除已選擇之系統紀錄。使用者可選取某些特定的系統紀錄後，刪除該筆紀錄資料，或是直接刪除全部紀錄。

12 第十二章 NK6000 Console

本章說明

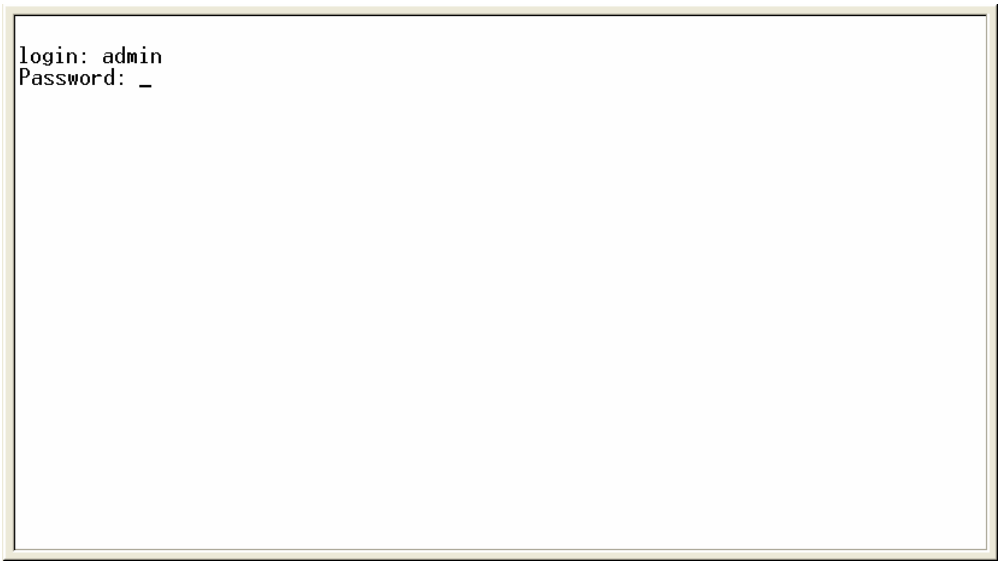
主要說明 NK6000 Console 介面功能與操作步驟。

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

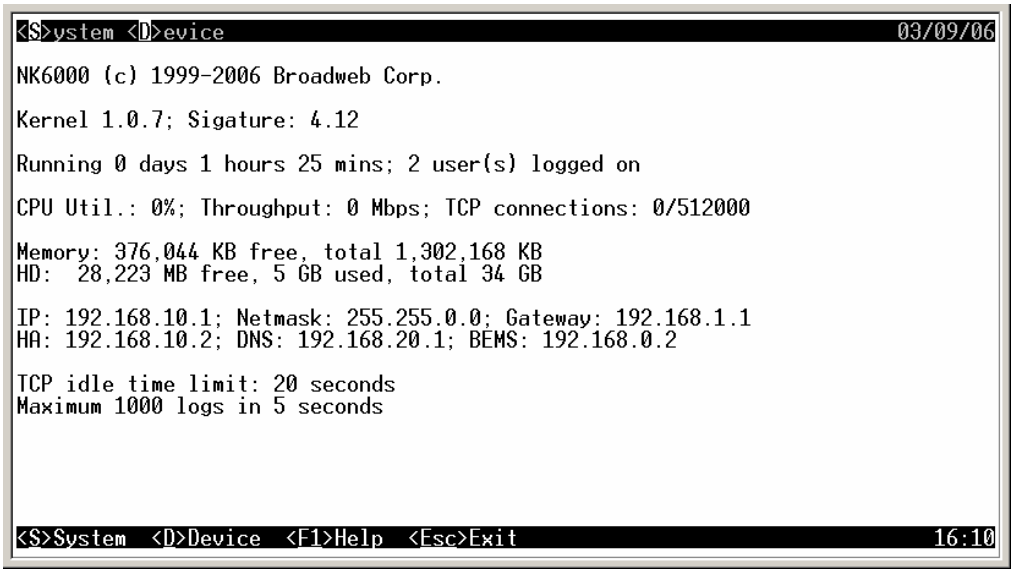
於登入提示出現後，如圖表所示，輸入帳號/密碼『admin / admin』，即可進入 NK6000 的 Console 介面。



圖表 172: 登入 (Login) 畫面

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

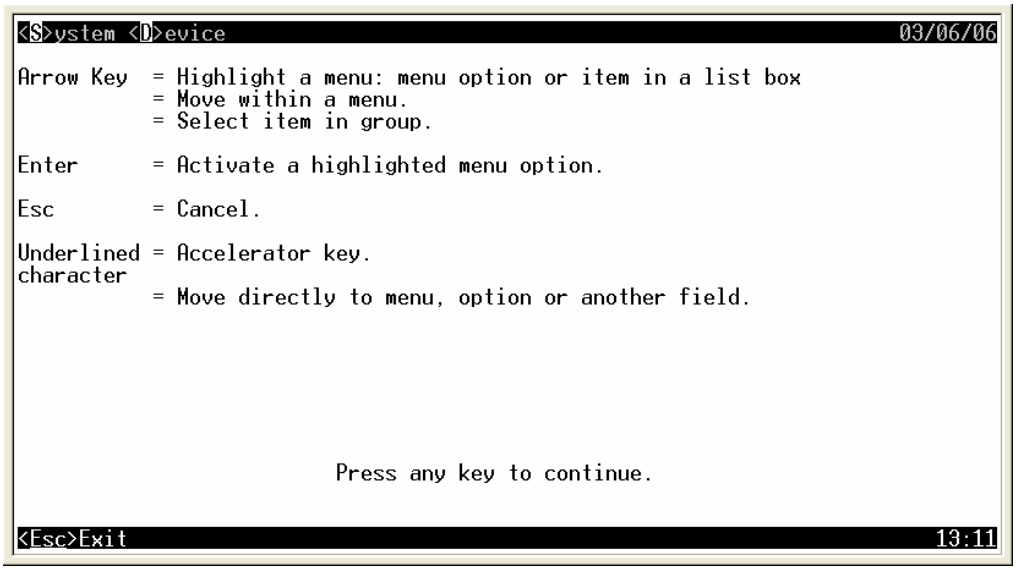
(Device) 選單與日期。主視窗中顯示有 NK6000 韌體 (BroadWeb NK Kernel)、防禦政策 (Signature) 等等的版本資訊、系統負載、網路設定及相關資訊。快捷功能列顯示有目前視窗可用的功能及系統時間。



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 爲操作功能鍵，詳細說明請參考 12.3 操作功能鍵。Underlined character 爲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。



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:

↑ ↓ ← →	**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 S

此功能群組爲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:

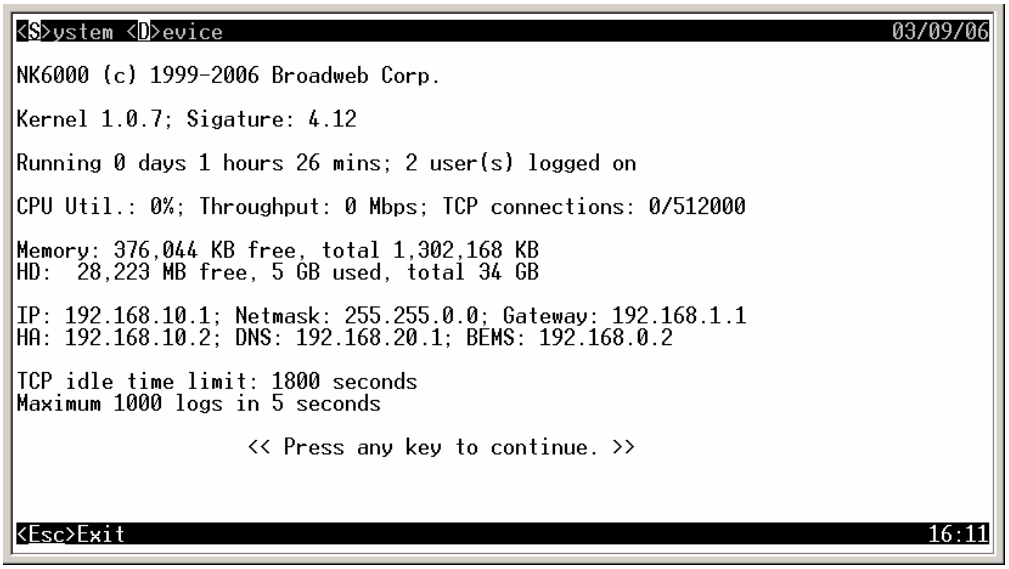
- All Status (系統狀態): 顯示系統硬體設備狀態資訊與各埠狀態資訊。
- Log (事件紀錄): 顯示系統事件記錄。
- Password (變更密碼): 變更管理者密碼。
- Reset Config (還原設定): 還原設定值成原廠出廠設定值。
- Stop System (停止系統): 停止 NK6000 運作並且關機。
- Reboot (重新啓動): 將 NK6000 重新啓動。

圖表 175: 系統 (System) 功能選單

12.4.1 系統狀態 (All Status) A

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 Enter 鍵，即可執行此功能。此功能執行中可按 Esc 鍵返回上層或按 S 鍵、D 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 核心版本爲 1.0.7、特徵檔案版本爲 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 使用率爲 0%、檢測效能爲 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 位址爲 192.168.10.1、網路遮罩爲 255.255.0.0、閘道器爲 192.168.1.1、對應的 HA 主機：192.168.10.3、DNS 伺服器爲 192.168.20.1、BEMS 伺服器爲 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。

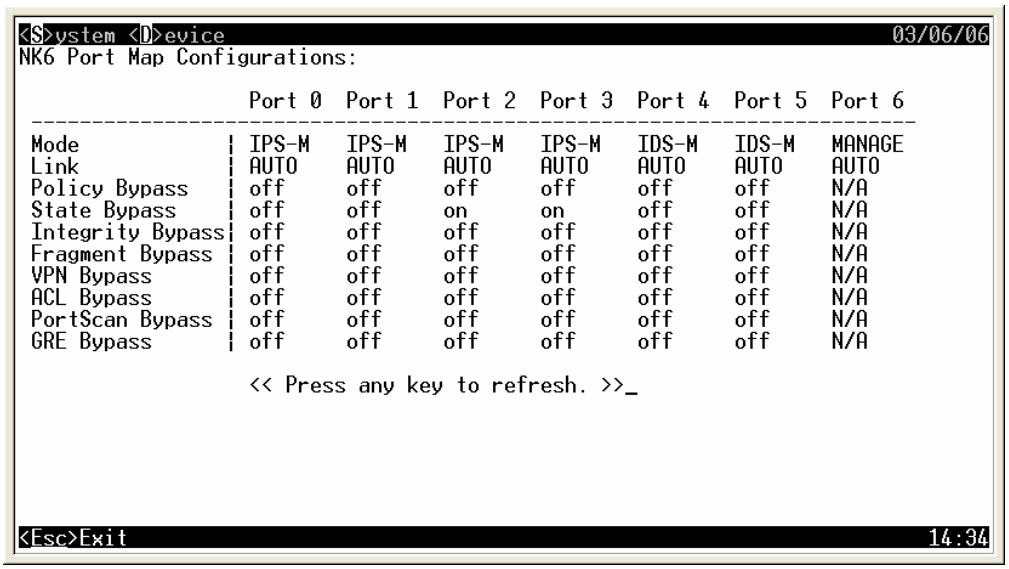


圖表 176: 系統狀態 (All Status) 畫面-1

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，爲 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)、1000F (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 爲忽略。
- 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 爲忽略。
- 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 爲忽略。
- Fragment Bypass: 系統偵測網路封包時，是否忽略 Fragment (切割) 之封包，on 爲忽略。
- VPN Bypass: 系統偵測網路封包時，是否忽略 VPN (虛擬私人網路)，on 爲忽略。
- ACL Bypass: 系統偵測網路封包時，是否忽略 ACL (存取控制清單) 的設定，on 爲忽略。
- PortScan Bypass: 系統偵測網路封包時，是否忽略 PortScan (連接埠掃描攻擊)，on 爲忽略。
- GRE Bypass: 系統偵測網路封包時，是否忽略 GRE 通信協定的連線，on 爲忽略。

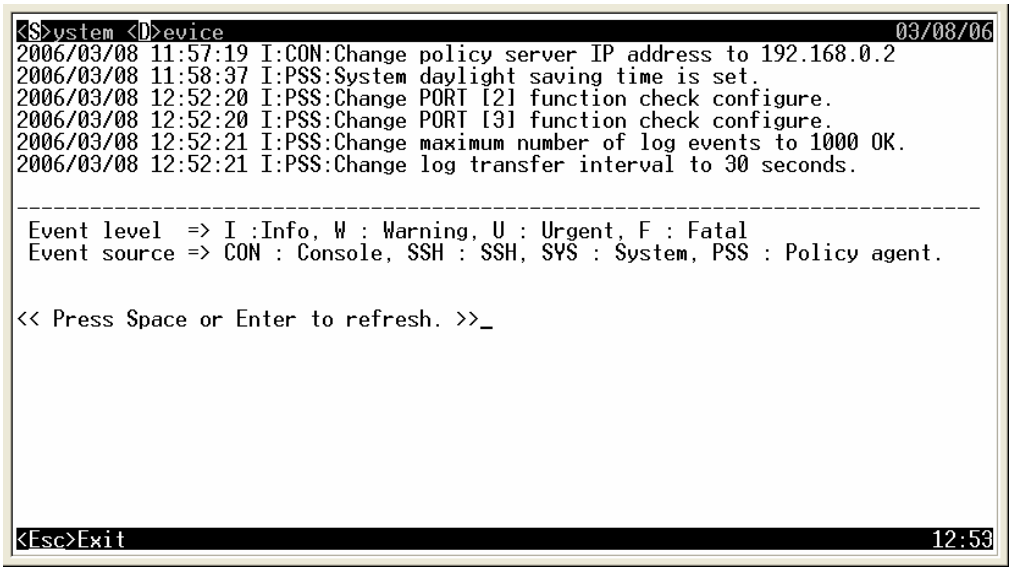


圖表 177: 系統狀態 (All Status) 畫面-2

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) L

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 L 移動到此選項並按 Enter 鍵，即可執行此功能。執行中可用空白鍵或 Enter 鍵更新記錄，Esc 鍵返回上層或按 S 鍵、D 鍵跳至功能選單。此功能畫面如下:



圖表 178: 事件記錄 (Log)

如圖中所示，NK6000 的事件紀錄的格式爲:

- 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。

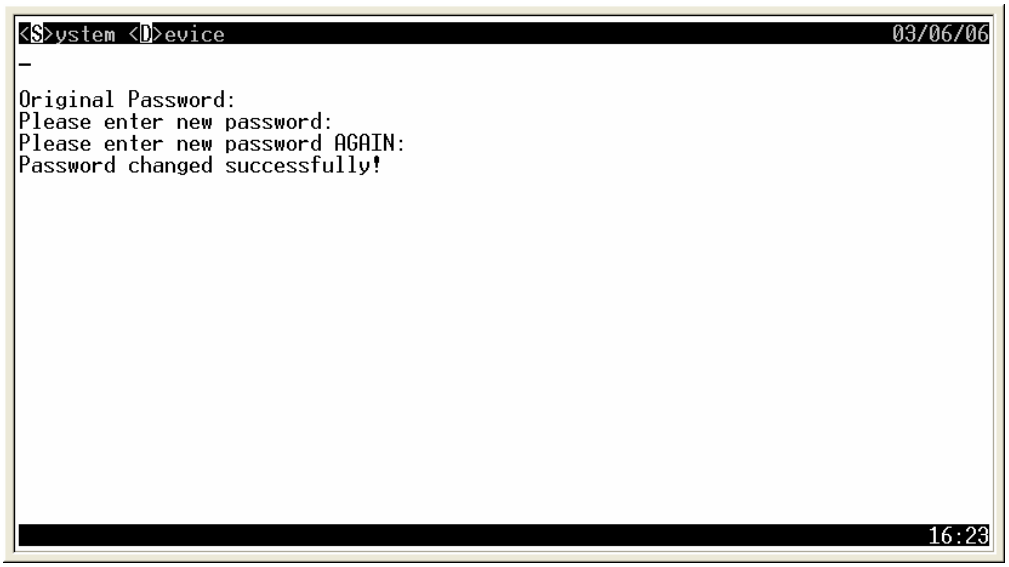
事件等級區分: 資訊 (I:Info)，警告 (W:Warning)，緊急 (U:Urgent)，致命 (F:Fatal)。

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) P

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 P 移動

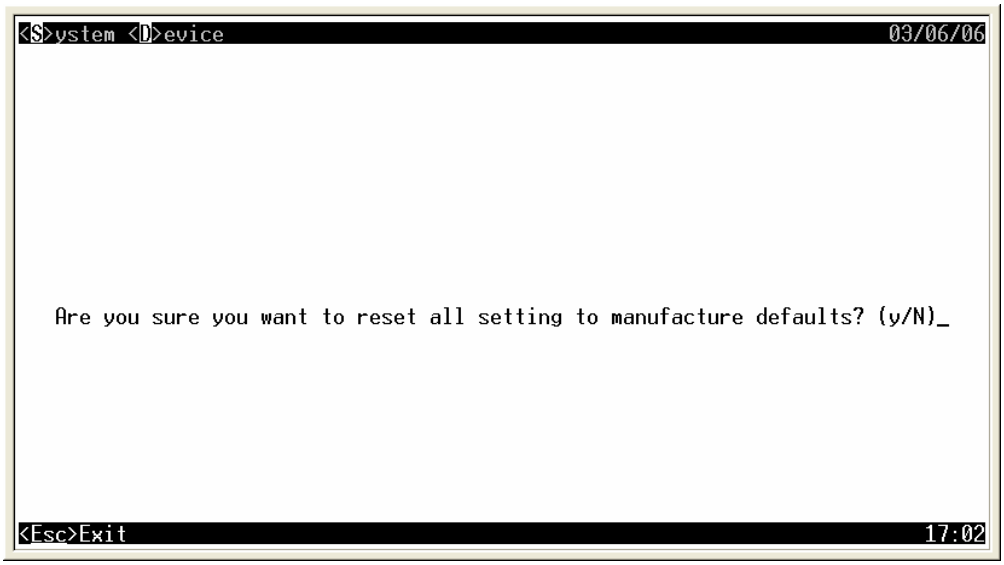
到此選項並按Enter鍵，即可執行此功能。首先系統會提示輸入原本的密碼，確認後會提示輸入新密碼，系統將會再確認一次新密碼，變更成功即出現『Password changed successfully!』字樣，失敗則出現『Password mismatch』字樣。此功能畫面如下:



圖表 179: 變更密碼 (Password) 畫面

12.4.4 還原設定 (Reset Config) E

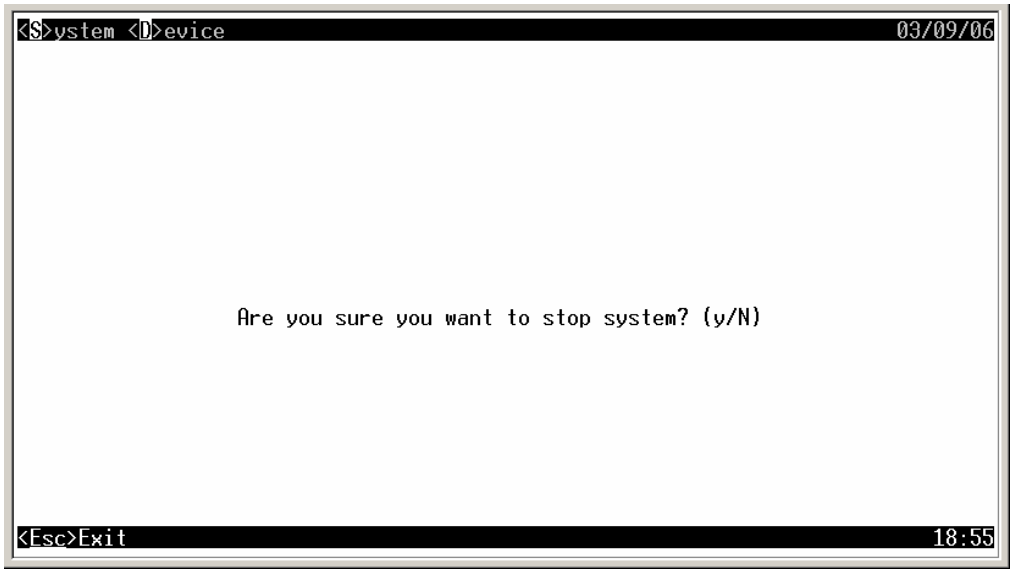
此功能可還原設定值至原出廠值。在 System 功能選單中以方向鍵或快捷鍵E移動到此選項並按Enter鍵，即可執行此功能。執行後系統會詢問是否還原設定，按Y鍵確定還原；按N鍵或Esc鍵保留目前設定，預設爲保留目前設定。此功能畫面如下:



圖表 180: 還原設定 (Reset Config) 畫面

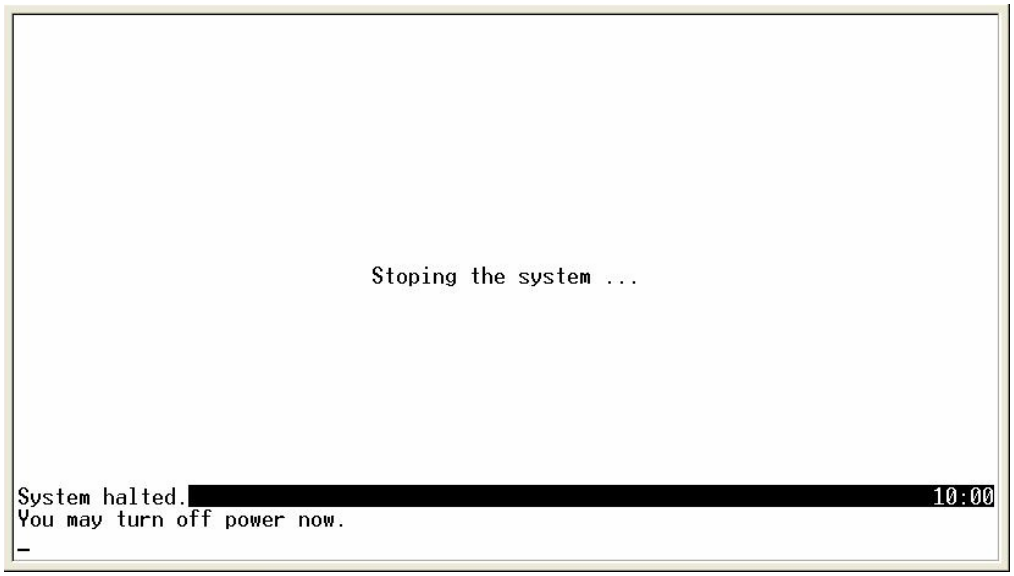
12.4.5 停止系統 (Stop System) S

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 S 移動到此選項並按 Enter 鍵，即可執行此功能。此功能畫面如下:



圖表 181: 停止系統 (Stop System) 畫面-1

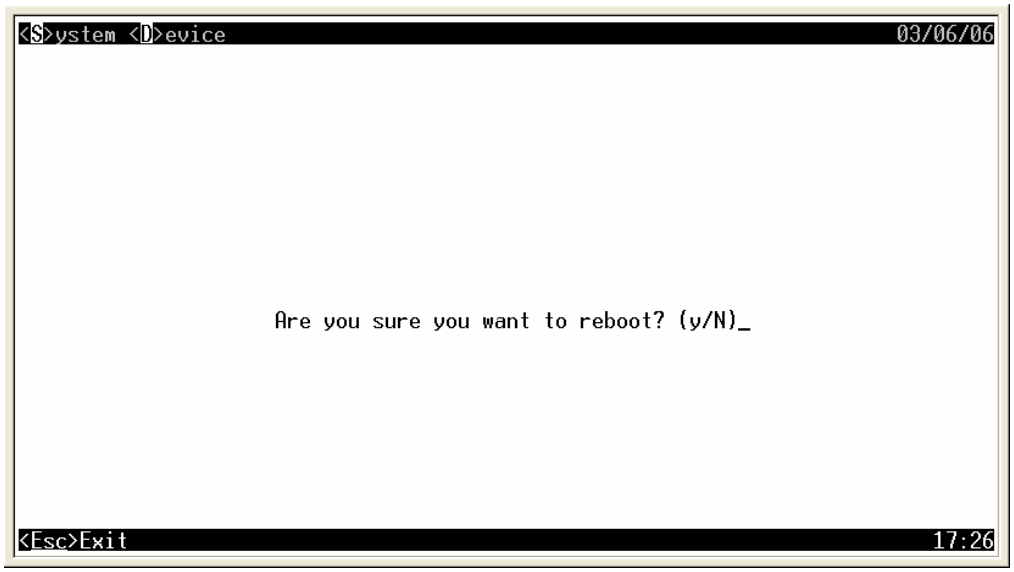
執行後系統會詢問是否停止，按 Y 鍵確定停止，當停止後，出現如下圖『You may turn off power new』字樣，即可關掉主機電源；按 N 鍵或 Esc 鍵繼續運作，預設爲繼續運作。



圖表 182: 停止系統 (Stop System) 畫面-2

12.4.5 重新啓動 (Reboot) R

此功能爲重新啓動 NK6000。在 System 功能選單中以方向鍵或快捷鍵R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動，按Y鍵確定重新啓動；按N鍵或Esc鍵繼續運作，預設爲繼續運作。此功能畫面如下:



圖表 183: 重新啓動 (Reboot) 畫面

12.5 設備 (Device) 功能群組 D

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 D 鍵，可以移動至 Device 功能群組，選單選項有:

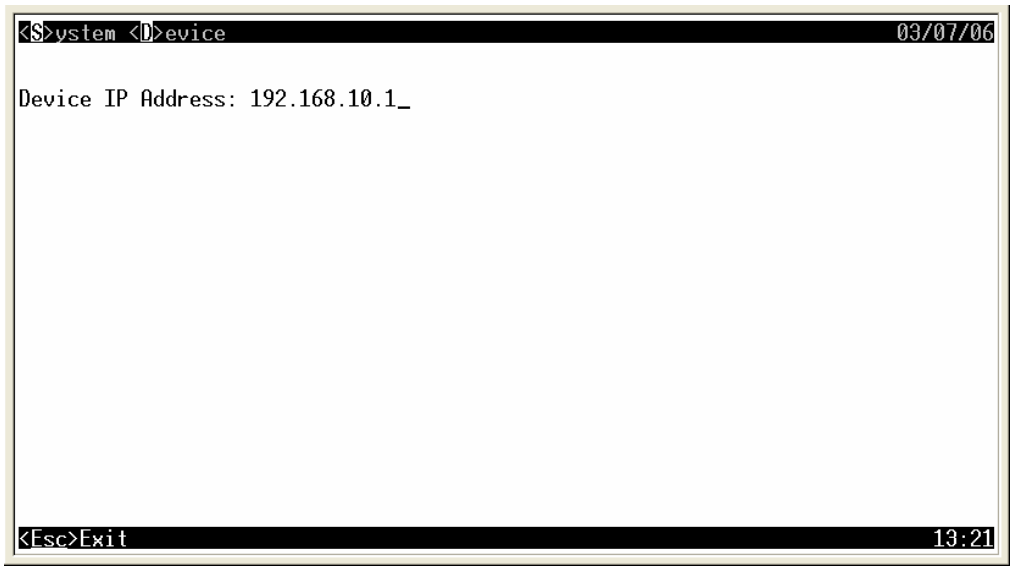
- IP (網路位址): 設定 NK6000 的網際網路地址。
- Netmask (網路遮罩): 設定 NK6000 的網路遮罩。
- Gateway (閘道器): 設定 NK6000 經由何者 Gateway 連接至外部網路。
- DNS (網域名稱伺服器): 設定 NK6000 使用何者 DNS 伺服器。
- TCP timeout (TCP 連線逾時時間): 設定經由 NK6000 的 TCP 連線逾時限制。
- Max. Log (最大系統事件記錄數量): 設定 NK6000 最多存放的系統事件記錄數量。
- BEMS Srv. (BENS 伺服器): 設定 NK6000 歸屬於何者 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

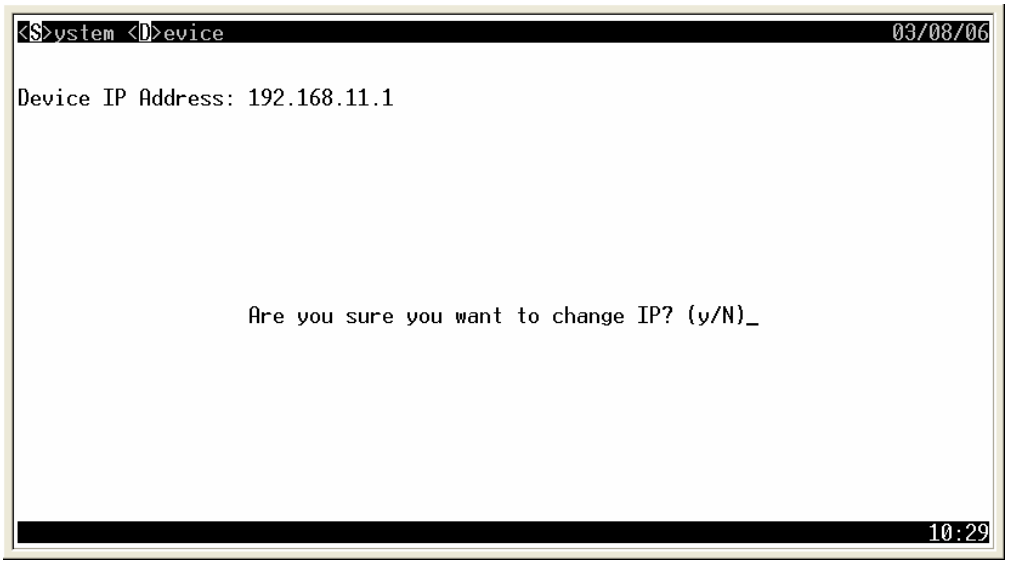
12.5.1 網路位址 (IP) I

此功能爲設定 NK6000 的網際網路位址。在 Device 功能選單中以方向鍵或快捷鍵 I 移動到此選項並按 Enter 鍵，即可執行此功能。此功能畫面如下:



圖表 185: 網路位址 (IP) 畫面

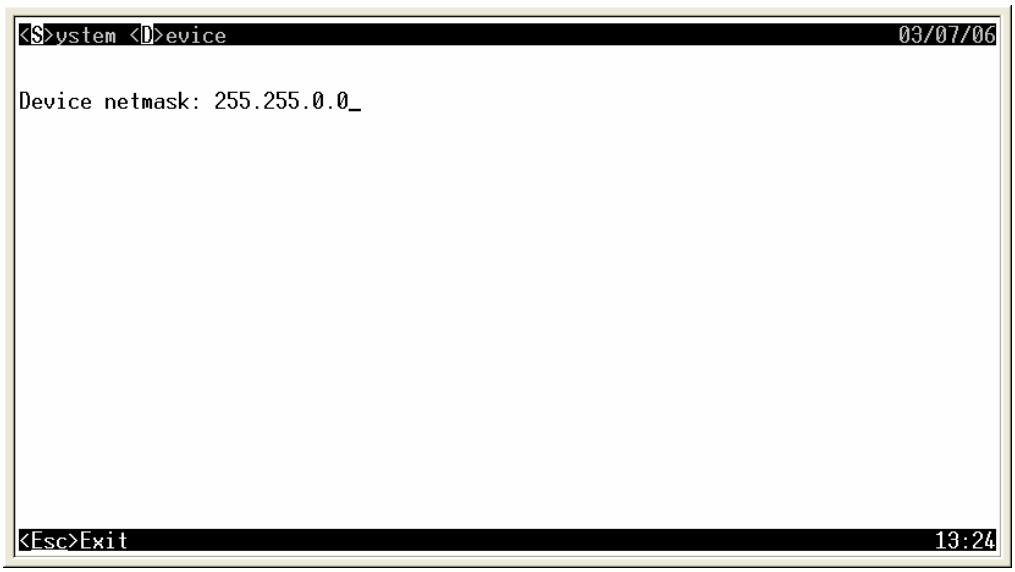
執行時會顯示目前 IP 位址設定，直接輸入欲變更的 IP 位址再按 Enter 鍵，系統將再次詢問變更與否，按 Y 鍵確定變更 IP 位址；按 N 鍵或 Esc 鍵則不變更，預設爲不變更。



圖表 186: 網路位址 (IP) 再次確認變更

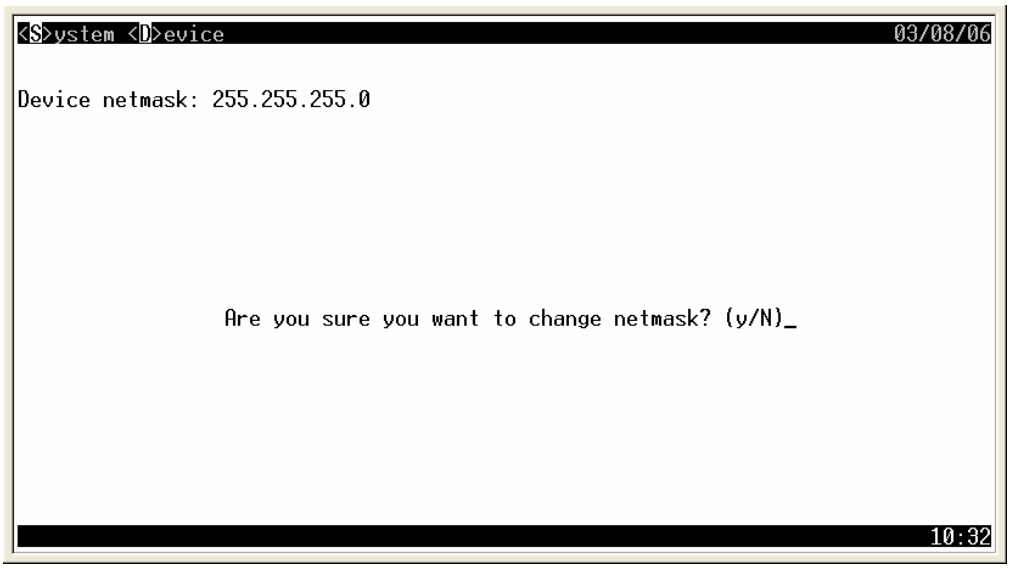
12.5.2 網路遮罩 (Netmask) M

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 M 移動到此選項並按 Enter 鍵，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 Y 鍵確定變更網路遮罩設定；按 N 鍵或 Esc 鍵則不變更，預設爲不變更。



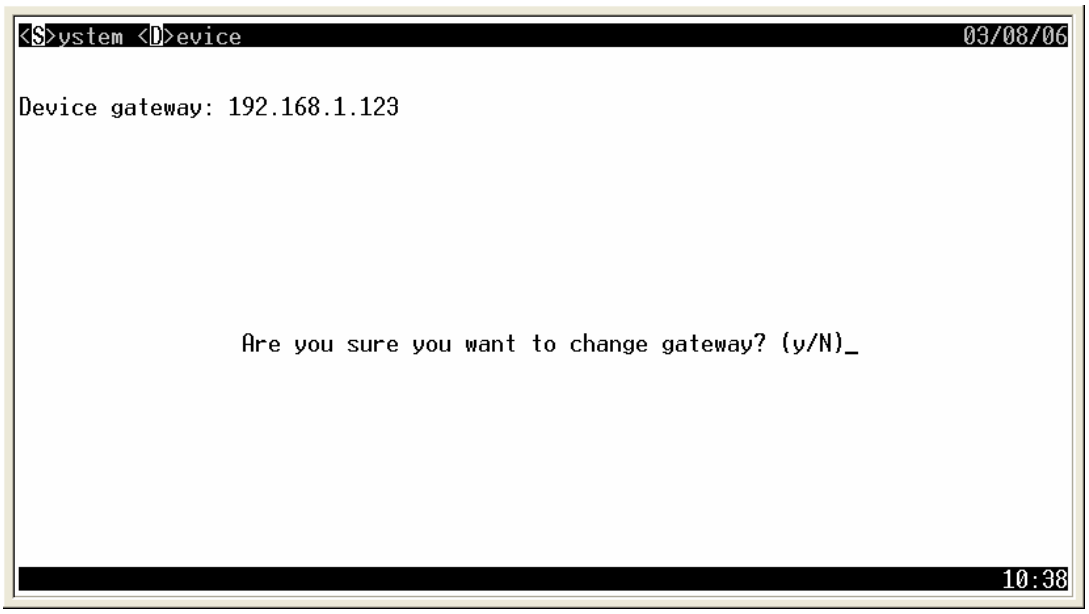
圖表 188: 網路遮罩 (Netmask) 再次確認變更

12.5.3 閘道器 (Gateway) G

此功能爲設定 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 G 移動到此選項並按 Enter 鍵，即可執行此功能。此功能畫面如下:

圖表 189: 閘道器 (Gateway) 畫面

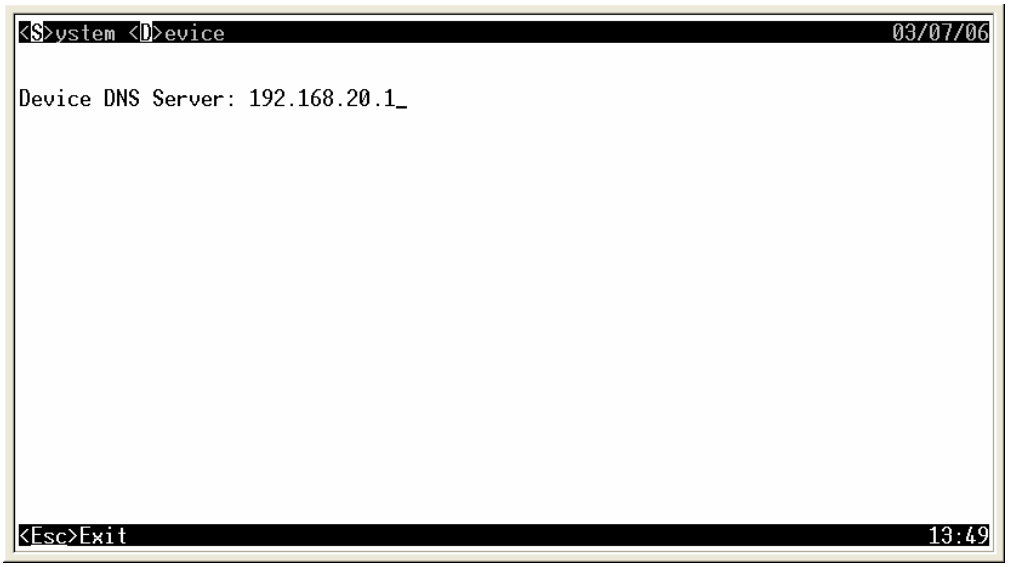
執行時會顯示目前閘道器設定,直接輸入欲變更的閘道器網路位址再按 Enter 鍵，系統將再次詢問變更與否，按 Y 鍵確定變更閘道器設定；按 N 鍵或 Esc 鍵則不變更，預設爲不變更。



圖表 190: 閘道器 (Gateway) 再次確認變更

12.5.4 網域名稱伺服器 (DNS) D

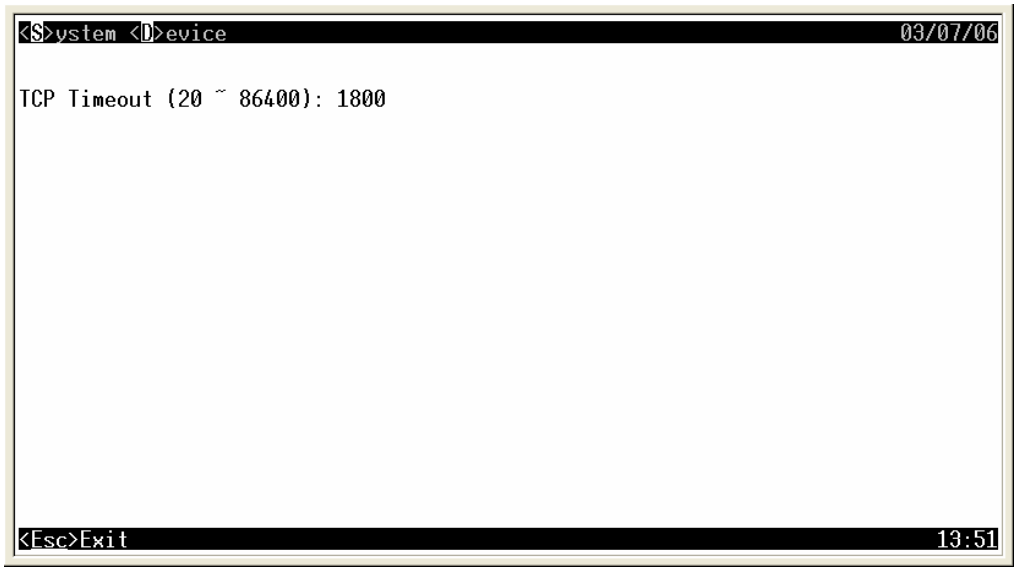
此功能爲設定 NK6000 經由何者閘道器連接至外部網路。在 Device 功能選單中以方向鍵或快捷鍵 D 移動到此選項並按 Enter 鍵，即可執行此功能。執行時會顯示目前網域名稱伺服器設定，直接輸入欲變更的網域名稱伺服器的網路位址再按下 Enter 鍵，即可變更設定。若不變更設定則按 Esc 鍵取消並跳出。此功能畫面如下:



圖表 191: 網域名稱伺服器 (DNS) 畫面

12.5.5 TCP 連線逾時時間 (TCP Timeout) T

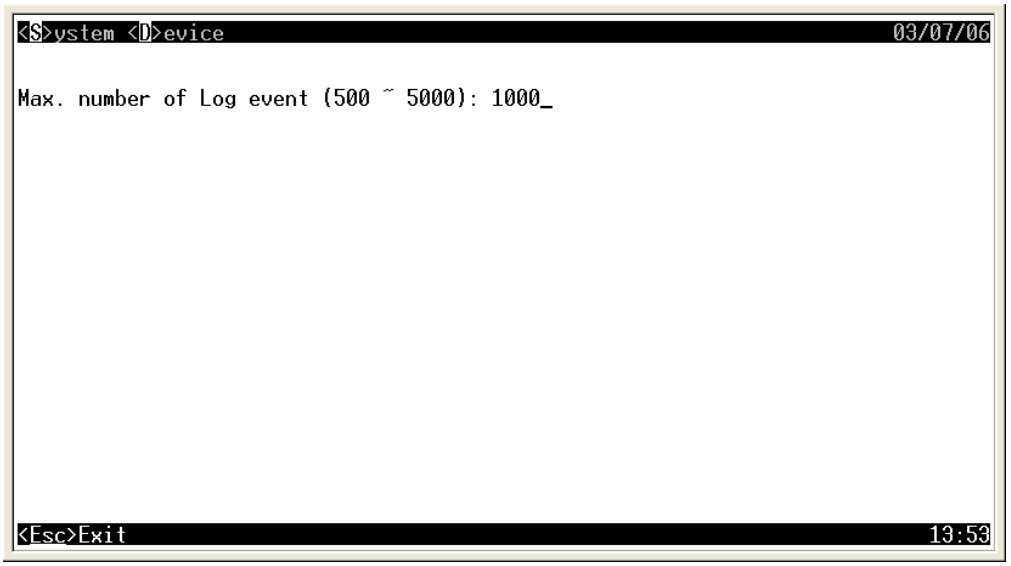
此功能爲設定經由 NK6000 的 TCP 連線逾時限制。在 Device 功能選單中以方向鍵或快捷鍵 T 移動到此選項並按 Enter 鍵，即可執行此功能。執行時會顯示目前 TCP 連線逾時限制設定，此設定以秒爲單位，直接輸入欲變更的逾時限制再按下 Enter 鍵，即可變更設定。若不變更設定則按 Esc 鍵取消並跳出。此功能畫面如下:



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) L

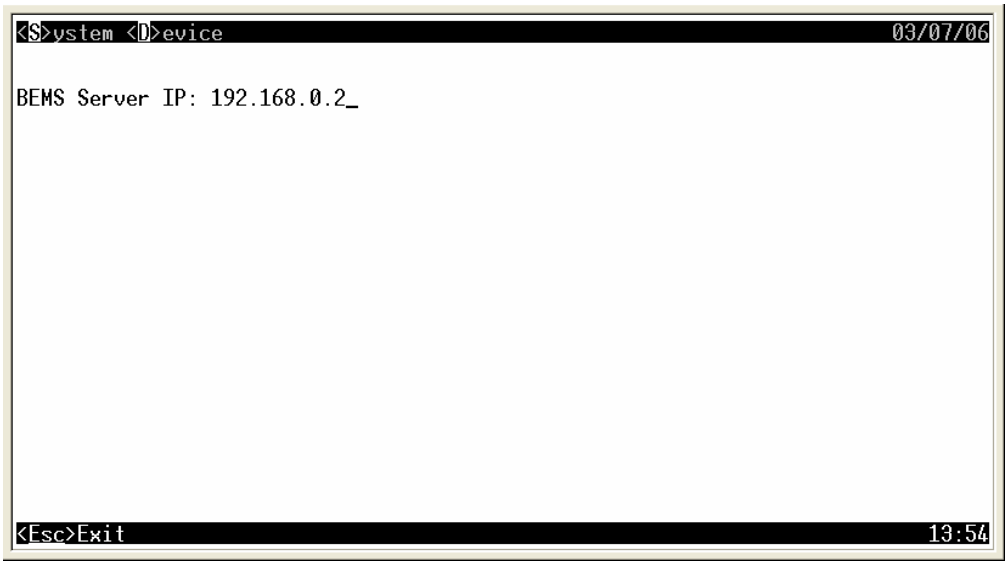
此功能爲設定 NK6000 最多存放的系統事件記錄數量。在 Device 功能選單中以方向鍵或快捷鍵 L 移動到此選項並按 Enter 鍵，即可執行此功能。執行時會顯示目前最大系統事件記錄存放數量的設定，直接輸入欲變更的最大存放數量設定再按下 Enter 鍵，即可變更設定。若不變更設定則按 Esc 鍵取消並跳出。此功能畫面如下:



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.) B

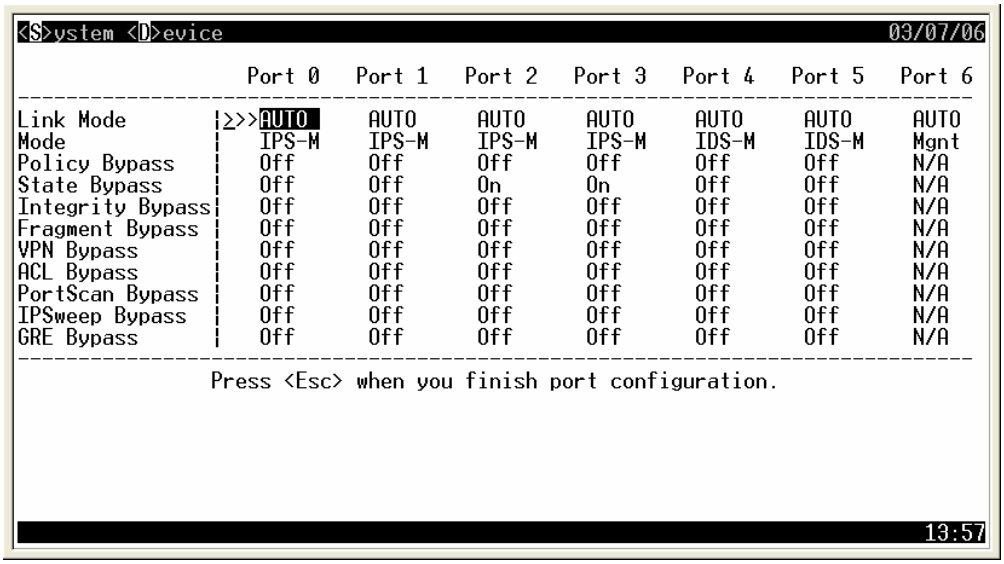
此功能爲設定 NK6000 歸屬於何者 BEMS 伺服器所管控。在 Device 功能選單中以方向鍵或快捷鍵 B 移動到此選項並按 Enter 鍵，即可執行此功能。執行時會顯示目前 BEMS 伺服器的網路位址設定，直接輸入欲變更的 BEMS 伺服器網路位址再按下 Enter 鍵，即可變更設定。若不變更設定則按 Esc 鍵取消並跳出。此功能畫面如下:



圖表 194: BEMS 伺服器 (BEMS Srv.) 畫面

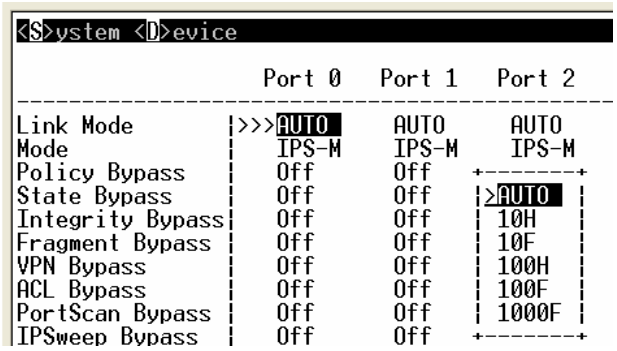
12.5.8 連接埠設定 (Port Config) C

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 C 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:

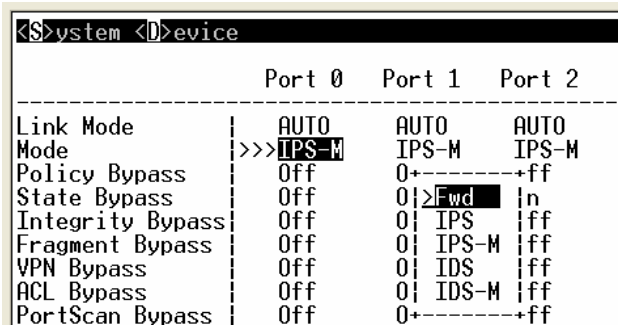


圖表 195: 連接埠設定 (Port Config) 畫面

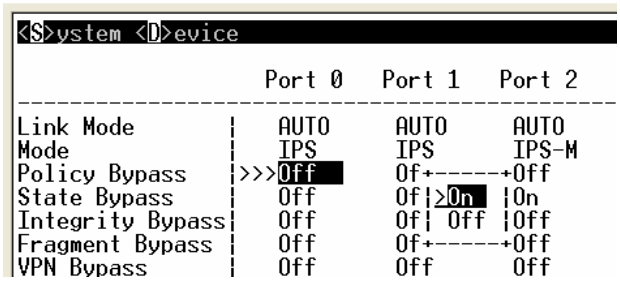
Port Config 於連線模式、偵測模試與各功能忽略與否的設定中各擁有子選項，其操作方式是相同的，可以利用方向鍵移動至要變再按下 Enter 鍵，則會出現子選項，如下圖表，再以上下方向鍵選擇所欲變更之設定，再按 Enter 鍵即可變更設定。若不變更設定則按 Esc 鍵取消並跳出。此功能畫面如下:



圖表 196: Link Mode 子選項

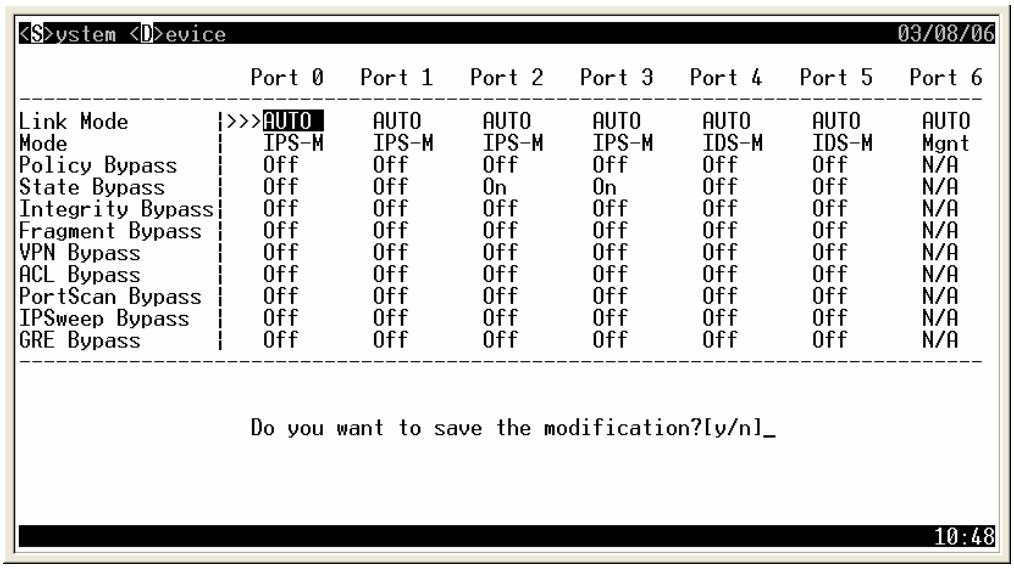


圖表 197: Mode 子選項



圖表 198: Policy Bypass 子選項

當設定完畢，按Esc鍵欲結束設定時，系統將會詢問是否儲存已修改的設定，按Y鍵確定儲存已修改的設定；按N鍵則不儲存，此選項無預設值。



圖表 199: 連接埠設定 (Port Config) 儲存詢問

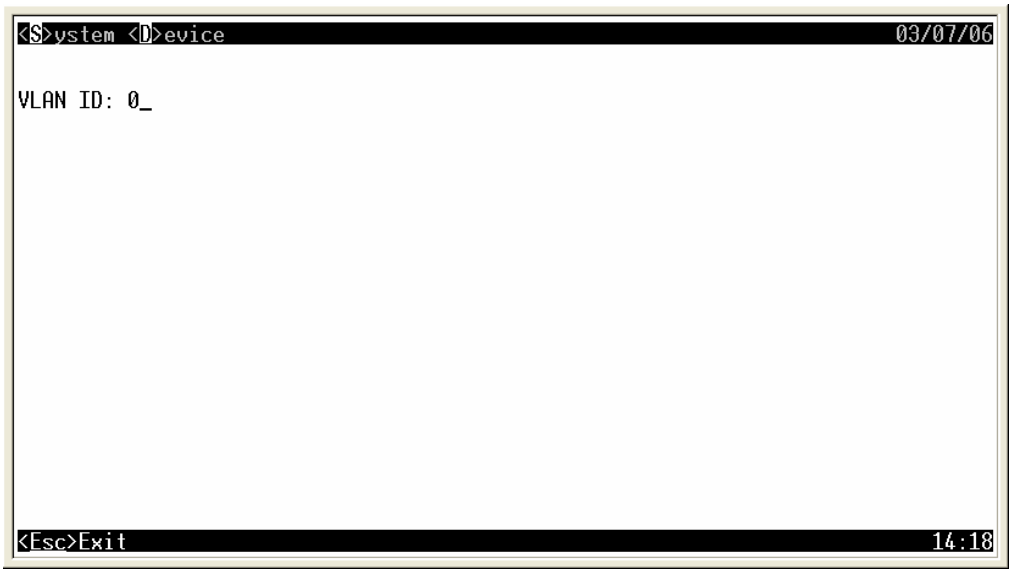
12.5.9 HA (High Availability) H

此功能爲設定本機 High Availability 對應的 NK6000 型設備。在 Device 功能選單中以方向鍵或快捷鍵H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Enter鍵，即可變更設定。此功能畫面如下:

圖表 200: HA (High Availability) 畫面

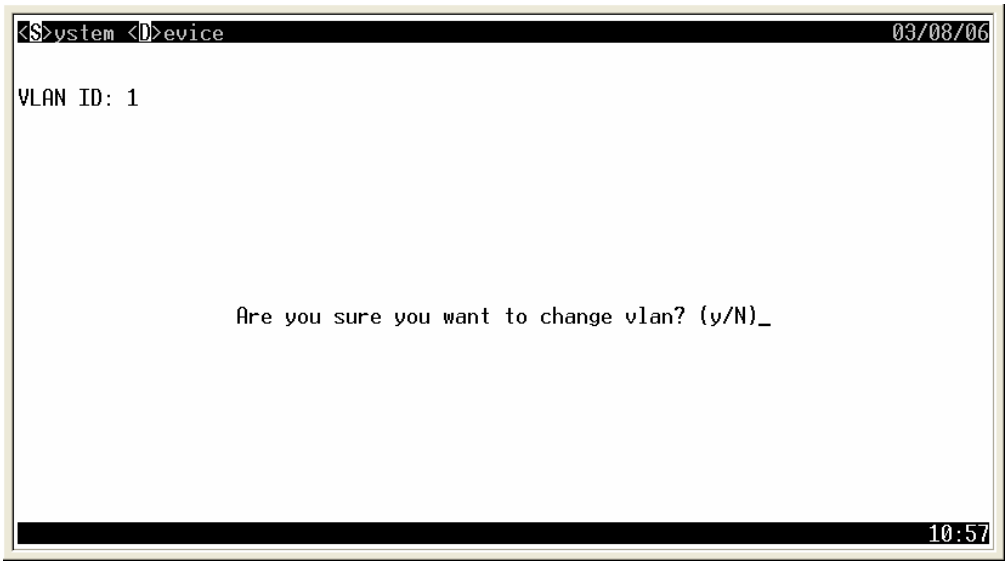
12.5.10 虛擬網路編號 (VLAN ID) V

此功能爲設定 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 V 移動到此選項並按 Enter 鍵，即可執行此功能。此功能畫面如下:



圖表 201: 虛擬網路編號 (VLAN ID) 畫面

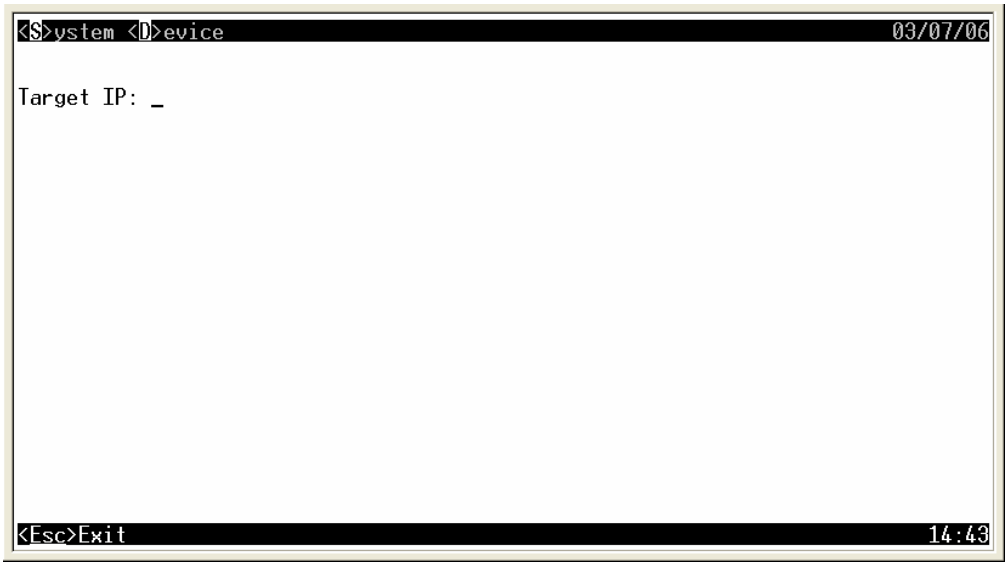
執行時會顯示目前虛擬網路編號設定，直接輸入欲變更的虛擬網路編號再按下 Enter 鍵，系統將會再次作確認，按 Y 鍵以確更改設定值；按 N 鍵爲不變更設定，預設爲不變更設定。



圖表 202: 虛擬網路編號 (VLAN ID) 再次確認變更

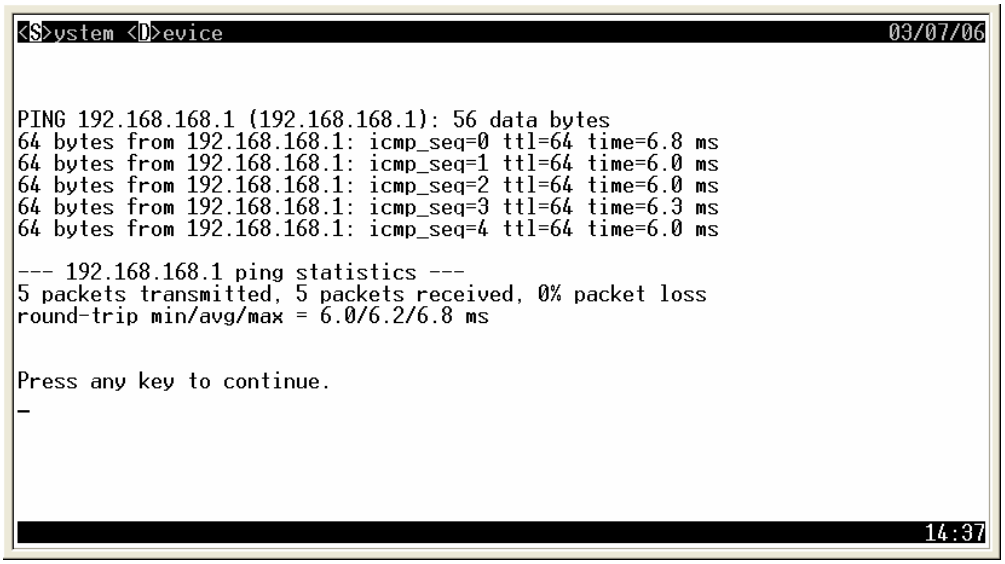
12.5.11 PING

此功能爲 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 Enter 鍵，即可執行此功能。此功能畫面如下:



圖表 203: Ping 功能畫面

執行後，輸入欲作 Ping 測試的 IP 位址，再按下 Enter 鍵，即可在主視窗中得知是否能連線到該 IP 位置。操作範例如下。

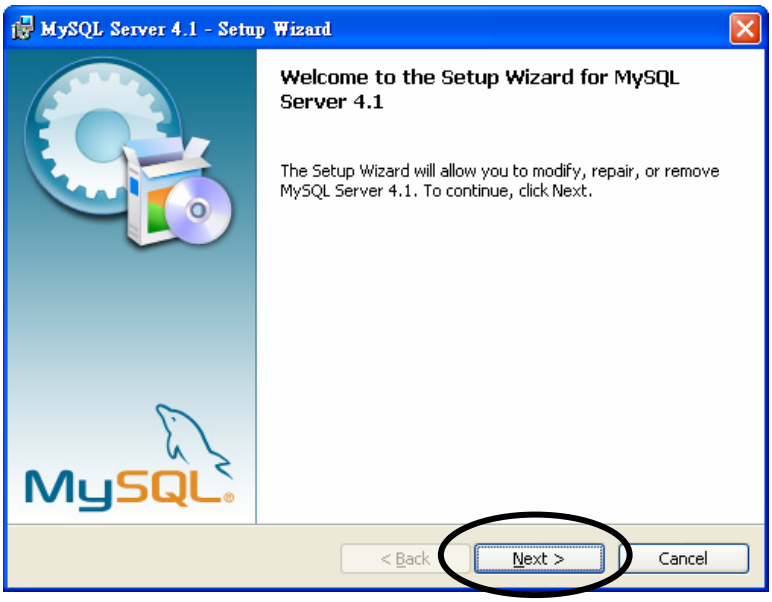


圖表 204: Ping 192.168.168.1

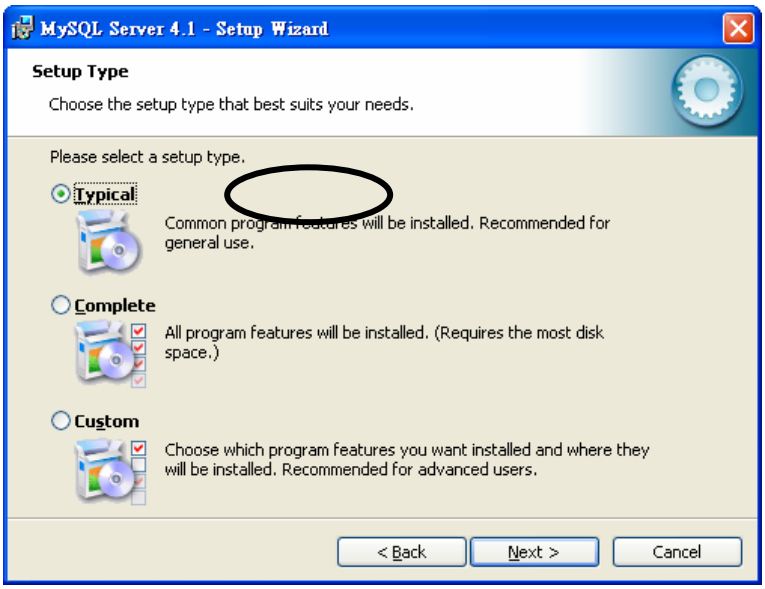
附件一 安裝 MySQL

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 不會自動爲使用者呼叫 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。

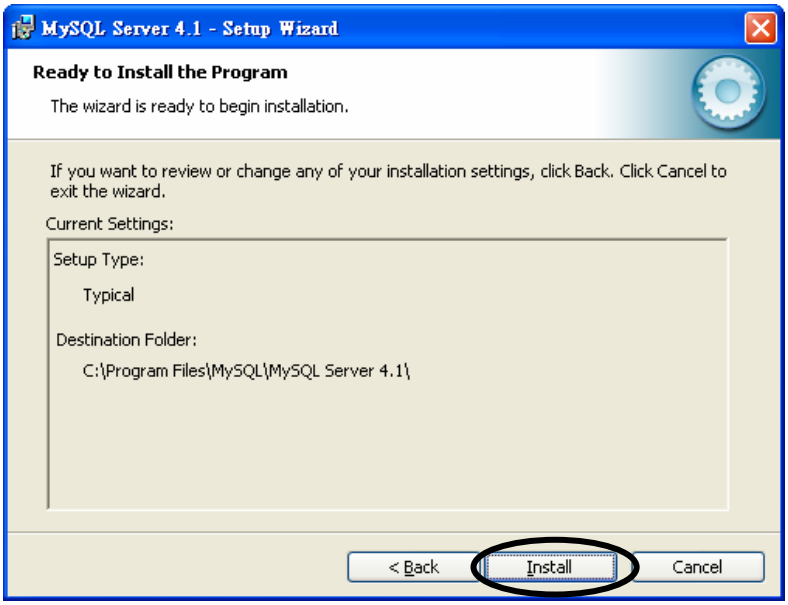
1. 執行 MySQL 安裝程式，出現以下畫面。按 **Next**。



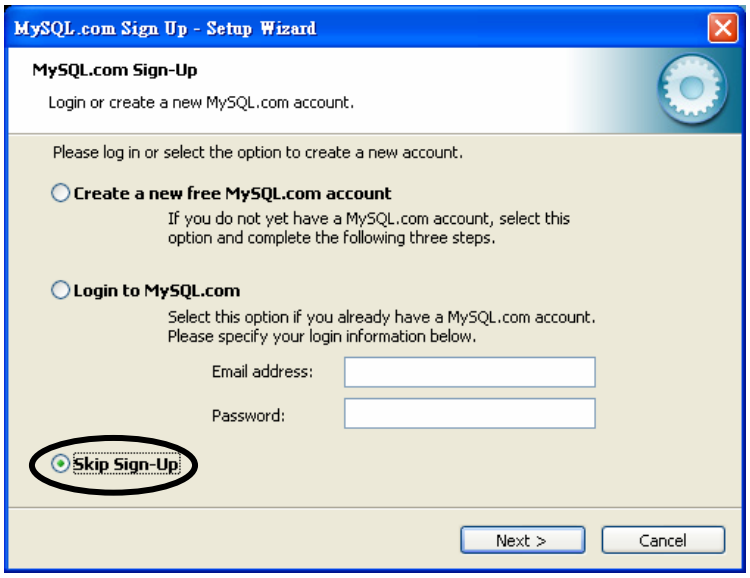
2. 核選 **Typical**



3. 按 **Install**

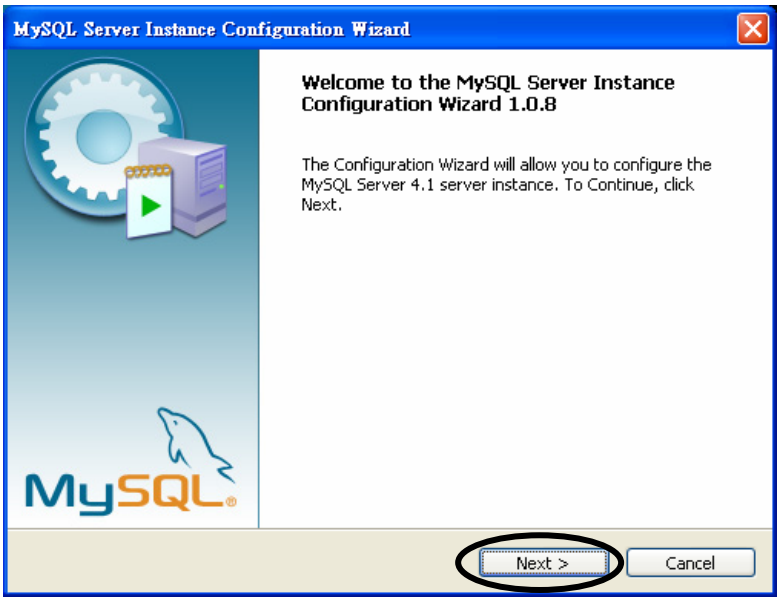


4. 點選 **Skip Sign-Up**

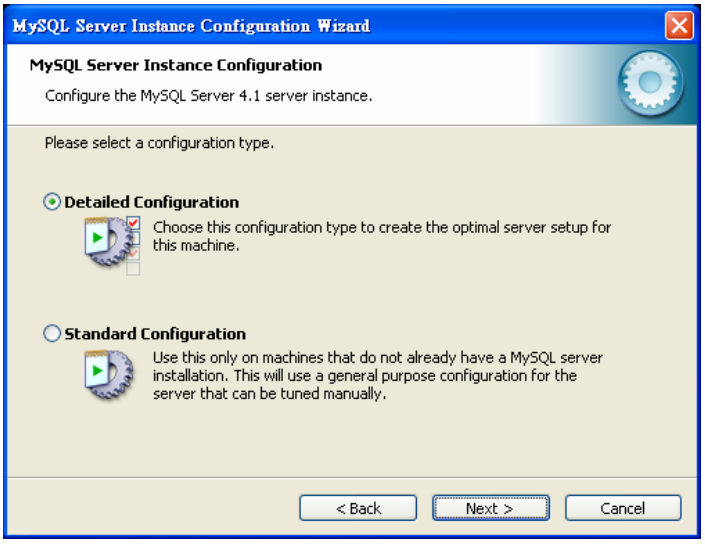


5. 核選 **Confugure the MySQL Server now**，再按 **Finish**。

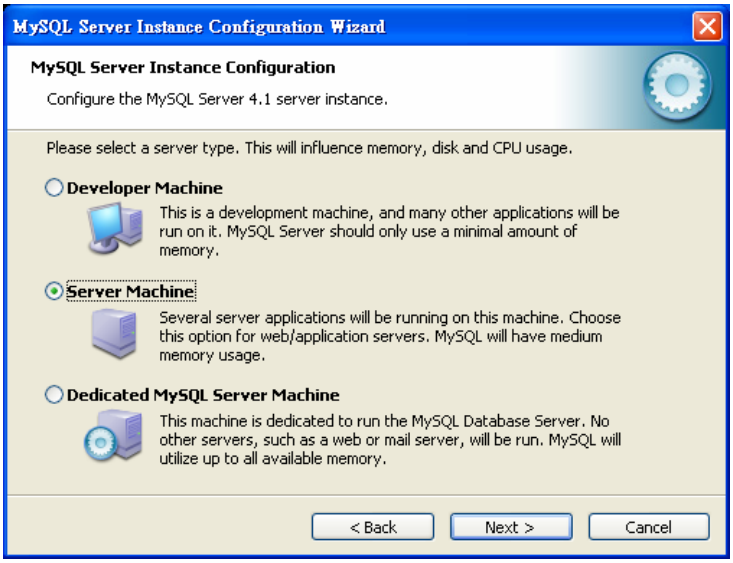
6. 點選 **Next**。



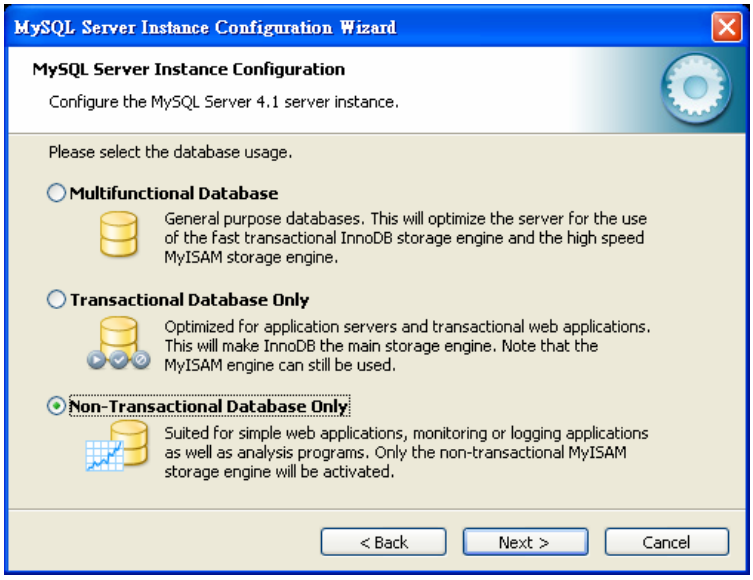
7. 核選 **Detailed Configuration**。



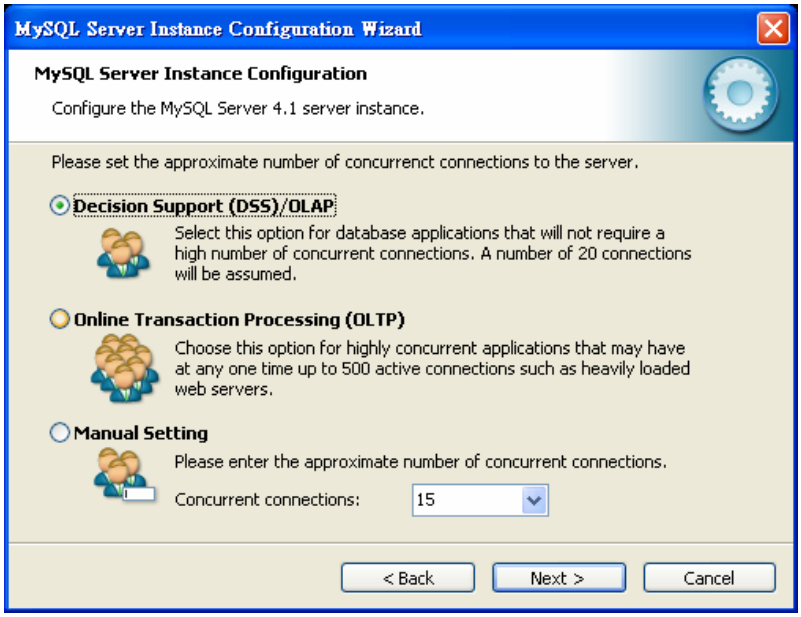
8. 核選 **Server Machine**。



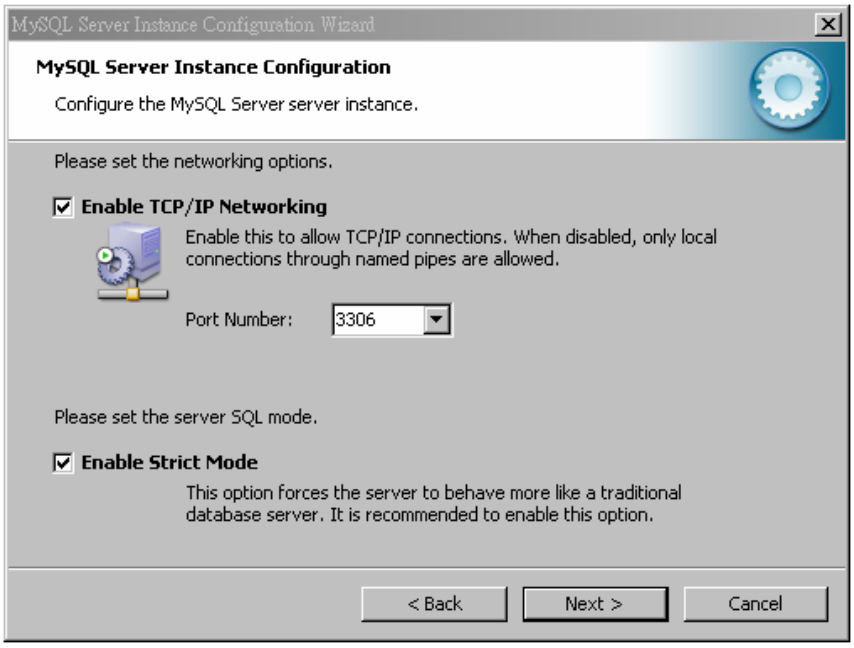
9. 核選 **Non-Transactional Database Only**。



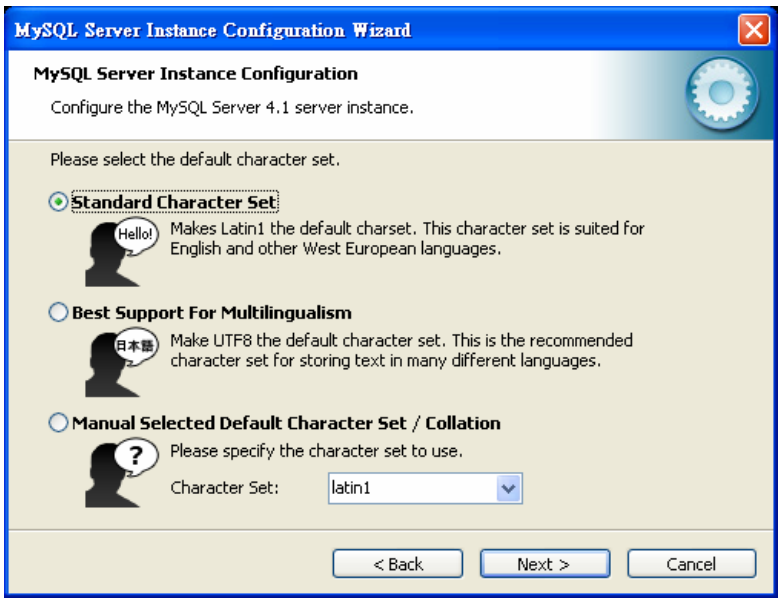
10. 核選 **Decision Support (DSS)/OLAP**。



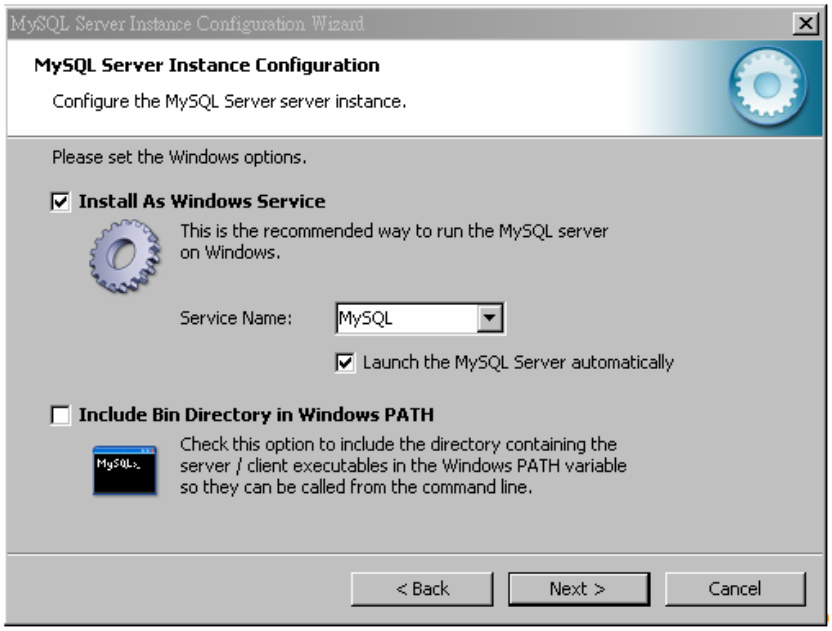
11. 核選 **Enable TCP/IP Networking**。**Port Number** 保持預設值 **3306**。核選 **Enable Strict Mode**。



12. 核選 **Standard Character Set**。



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



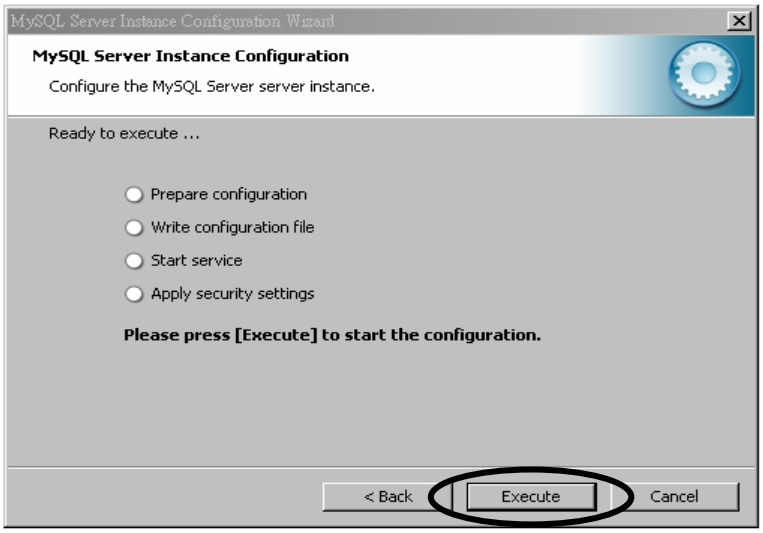
14. 核選 **Modyfy Security Settings**。請爲 MySQL 資料庫的 root 帳號自行設定一個密碼，如下圖：

說明：

請牢記您爲 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。



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 服務的狀態爲「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
