特徵式木馬病毒防護監控防火牆系統

安裝與使用手冊

系統版本：2.6以上
文件修改版本： Rev 1.6

修改日期：2008.7.1

目錄

第一章 旭威防火牆系統介紹

1.1 旭威防火牆系統簡介

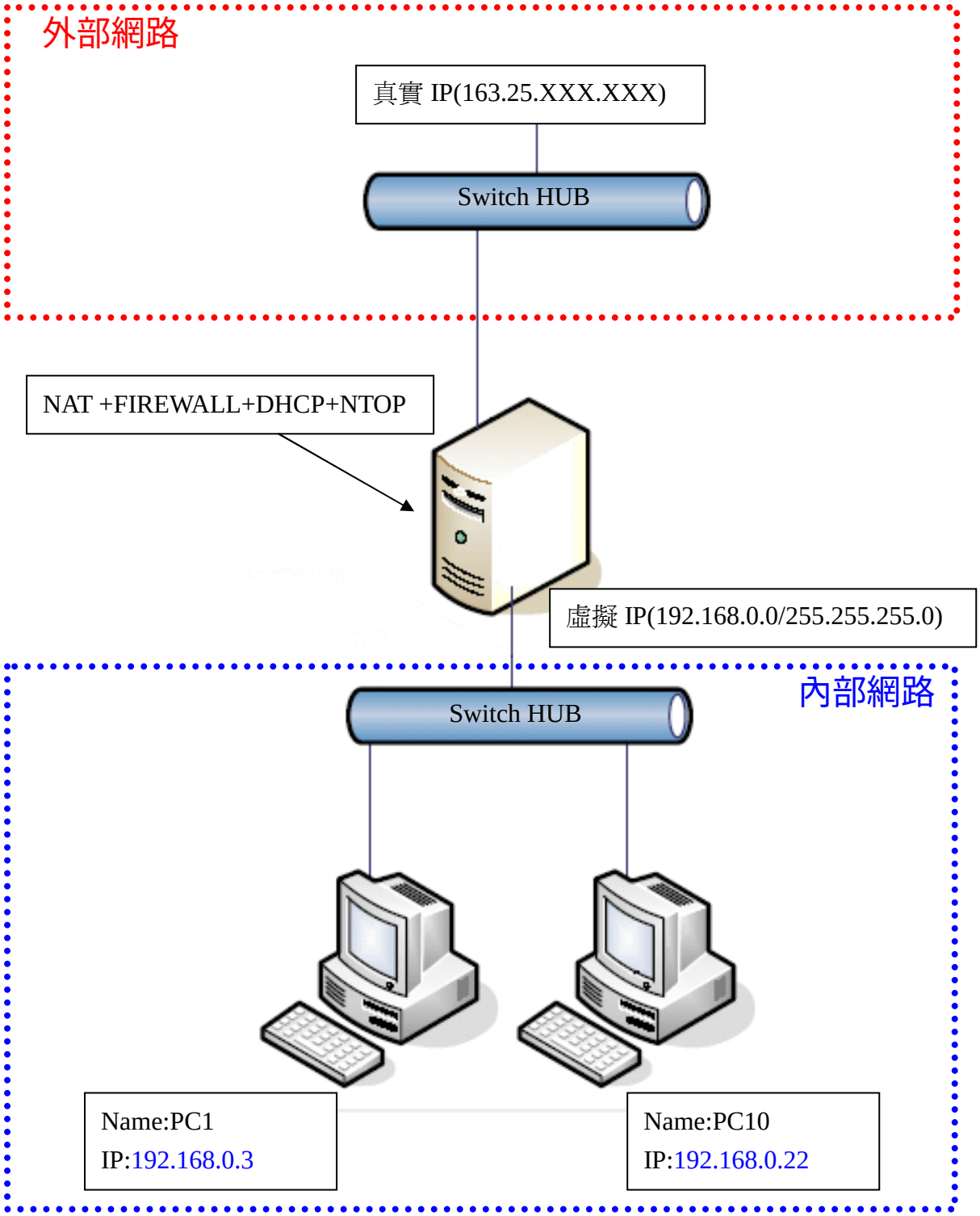
身爲一位資訊老師或是網管人員最擔心就是校內的電腦中毒了，如果它是屬於真實 IP 那到還好，因爲會被縣網的防護機制給擋下來，但是如果它是屬於虛擬 IP 的話呢？？那就可能會急得跳牆了，因爲萬一找不到又急需用網路的時候就會給他○○╳╳了。所以，難道真的要爲一粒老鼠屎然後壞一鍋粥嗎？因此，旭威電腦獨家研發的***特徵式木馬病毒防護監控防火牆系統***，針對虛擬 IP 來控管不但有類似像縣網中心的**限制連線介面**，更重要的是，維護人員還可以自行加入規則與解除限制的控管（從此不用再打電話向縣網求救與報告啦！），此系統依照設定方法（不論真假 IP 或是不同網段）不但可以了解全校的電腦上網狀況，還可明確的找出問題發生的機器。讓資訊組長輕輕鬆鬆的坐在辦公室看分析就一切搞定了。

1.2 旭威防火牆系統特點

☆系統採用 FreeBSD 核心，具有極高的效能與穩定性。
☆採用網頁遠端維護控管管理。
☆可自行設定規則、抓取時間與連結點數量。
☆可監控所有或是單一網卡（網段）。
☆具遠端管理連線限制功能。
☆管理者可自行開放已受限之電腦網路。
☆被設限電腦具通知功能（可自行更換網頁內容）。
☆網路封包監看與分析功能。
☆提供 MRTG、DHCP、NAT、PXE Boot 功能。
☆可與旭威電腦 VOD 系統整合。
☆提供 **P2P** 等行爲模式軟體的阻擋。
☆新版增加支援 **Transparent** 透通模式功能。
☆新版增加 例外清單、QOS 頻寬限制政策、網路封包擷取功能。

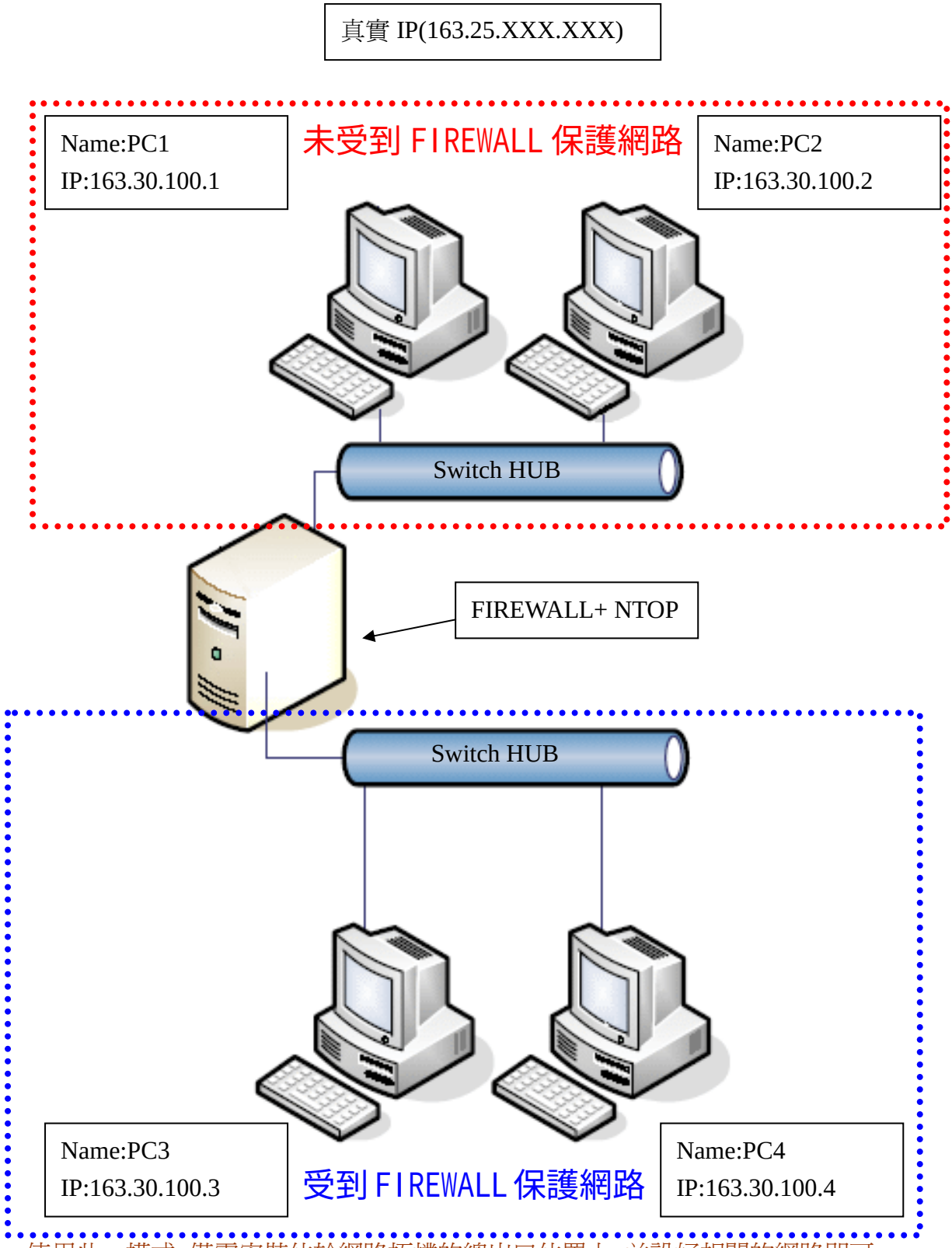
1.3 旭威防火牆 Routing / Transparent 模式的介紹與應用

Routing Mode 屬於 NAT(Network Address Translation) 模式，意爲學生電腦爲虛擬 IP，並透過主機轉址服務上網，因此對外皆爲同一 IP，對於網路的封包分係很難真正的判斷出其真正的原因發生爲何，此種模式也最常應用於電腦教室的配置與管理。如下圖所示：



使用此一模式，需將原先提供 NAT 的伺服主機給替換，並設好相關的網路即可。

Transparent Mode 屬透通模式，或稱作橋接模式(Bridge)，意指將不改變任何的網路架構或設定，直接安裝於網路拓樸的對外出口即可。如下圖所示：



使用此一模式，僅需安裝位於網路拓樸的總出口位置上，並設好相關的網路即可。

第二章 程式的安裝與設定

2.1 支援的硬體與種類

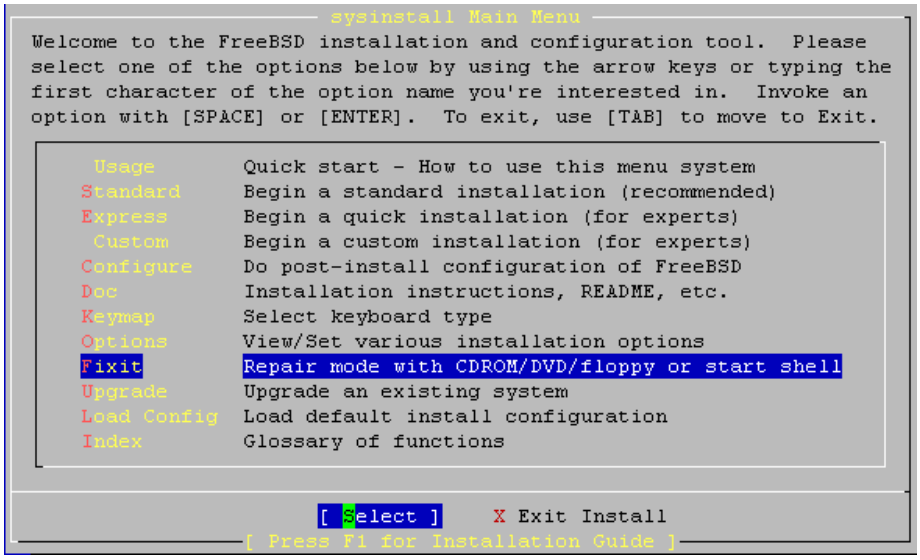
標準 Intel x86 PC 系統，支援單顆或多顆 CPU，此版提供任何介面技術的硬碟，如系統有不支援介面者，請聯絡相關技術支援，另支援的網卡種類如下表列所示：

網路卡	◎ 3COM 3C996B-T BCM5701 (Broadcom Tigon3) ◎ Intel Pro/1000 ◎ Intel i82559/i82558/i82551/i82550 ◎ DLink DL2000 ◎ Nation Semiconductor DP83820 ◎ Packet Engines Hamachi GNIC-II ◎ Packet Engines Yellowfin ◎ Realtek 8169 ◎ Marvell Yukon SK-98xx ◎ 3COM 3cR990 Typhoon ◎ AMD 8111-based ◎ Broadcom 4400 ◎ Mysom MTD-800 ◎ nForce Ethernet ◎ Sundance Alta ◎ Winbond W89c840 ◎ 3Com etherlink ◎ NE2000 ◎ Ether WOKRDS DE425 ◎ DM9102 ◎ Digital 21x4x Tulip ◎ Intel i82557/i82558 ◎ AMD PCnet32 ◎ Compaq Netlligent ◎ 100VG-AnyLan ◎ VIA Rhine ◎ Digi Intel RighSwitch SE-X ◎ Realtek 8139 ◎ SiS 900 ◎ SMC EtherPower II ◎ FA-311 DP83815 ◎ Adaptec Starfire

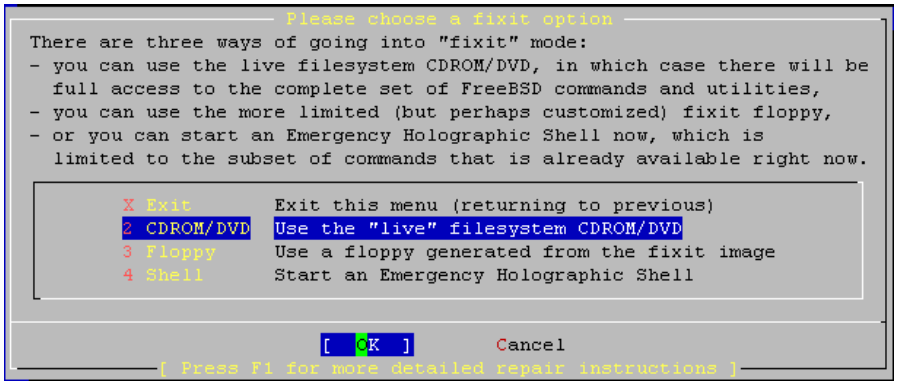
2.2 安裝

請將安裝光碟至於光碟機後，於 BIOS 設定開機順序爲 CD-ROM 優先啓動，進行開機程序，如下圖所示：（注意：此程序會將原本硬碟內資料清除，並無法再復原，請小心使用）

Step1. 選取 Fixit 選項，進行安裝資料程序。



Step2. 選取 2 CDROM/DVD 選項。



Step3. 在 #符號後面輸入 /mnt2/setup 進行資料載入。

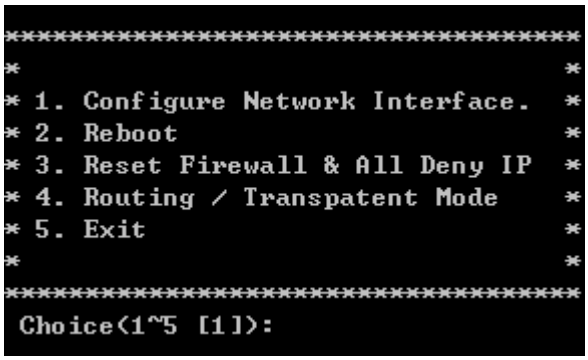
Step4. 依畫面指示，輸入預安裝的磁碟機代號及即可完成。

2.3 網路組態設定

Step1. 開完機後，系統應當出現 login: 等字樣，如無出現，表示系統沒有找到硬碟裝置！

Step2. 系統預設帳號爲 root、密碼爲 netadmin ，進行登入帳號動作。

Step3. 鍵入 setup ，即可出現下列圖示



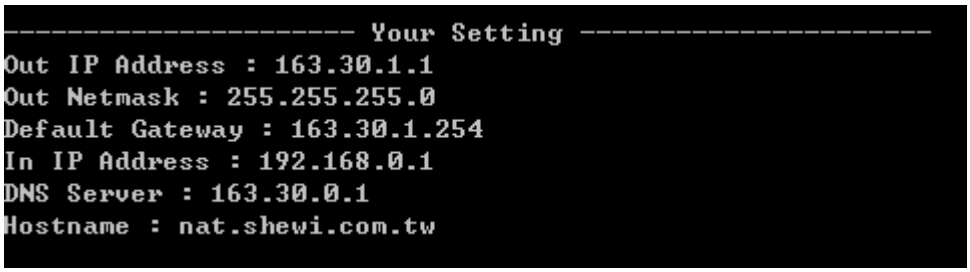
功能說明

1.	Configure Network Interface	設定網路介面與 IP 組態
2.	Reboot	重新開機
3.	Reset Firewall & All Deny IP	重新設定所有防火牆規則
4.	Routing / Transparent Mode	NAT 或透通模式切換
5.	Exit	離開

Step4.

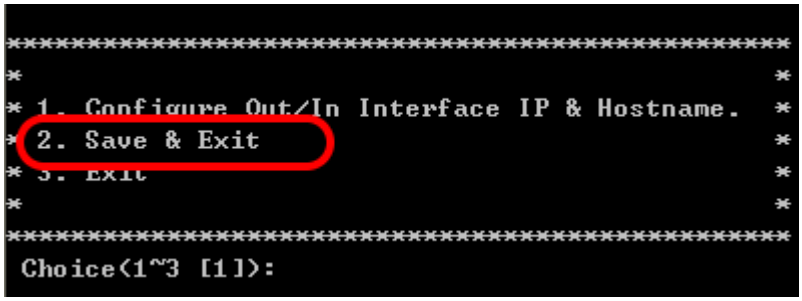
選擇 1 選項時，出現下列選項

Step5. 將其 IP 相關資訊與 DNS 位置填入



※Out IP Address 表示第一張網路卡、In IP Address 爲第二張網路卡。通常判斷方式爲主機板 PCI 插槽的順序爲主，當然，某些機種也可能有例外發生。

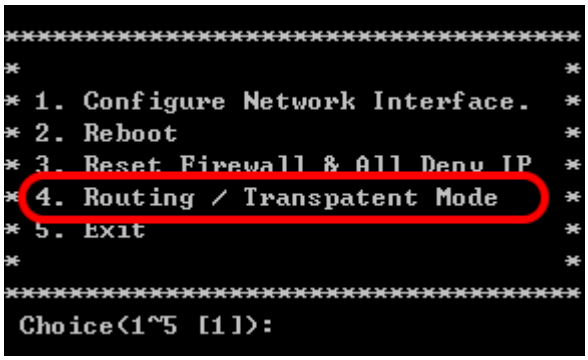
Step6. 設定完後，記得按 2 選項，即可完成網路設定



Step7. 自動重開機後，利用網頁瀏覽器作後續的設定。

2.4 Routing & Transparent 模式設定

當網路架構需切換爲不同模式運作時，請進入設定畫面，選擇 4 選項即可。



Step1. 選擇網路模式，記得要存檔，並重開機後生效。

註：Transparent Mode 狀況下，兩張的網卡 IP 皆爲一樣，就是指對外網卡的 IP 位置，同時，如有電腦發生攻擊事件時，並不會導入到自動提示回報的網頁，請注意。

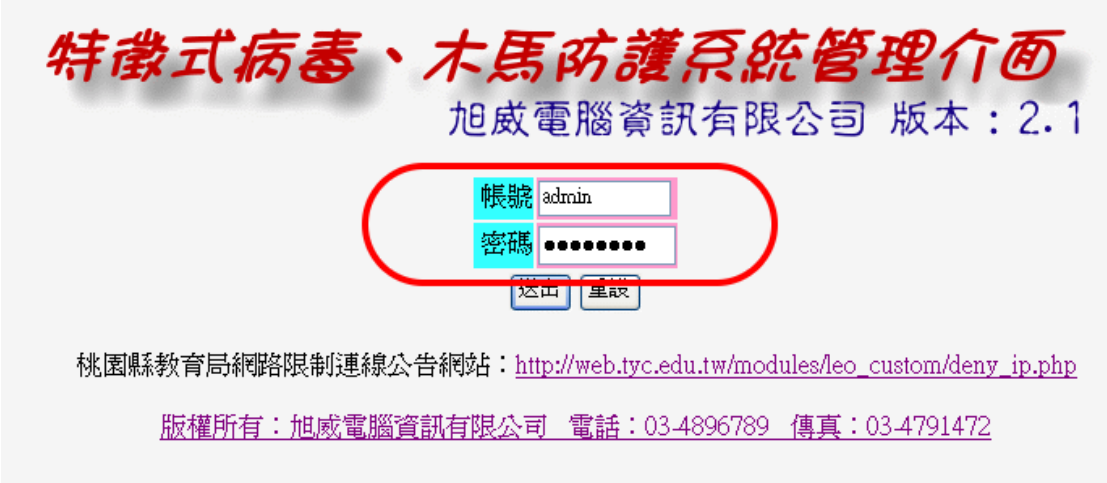
第三章 網頁的管理與應用

3.1 功能介紹與設定

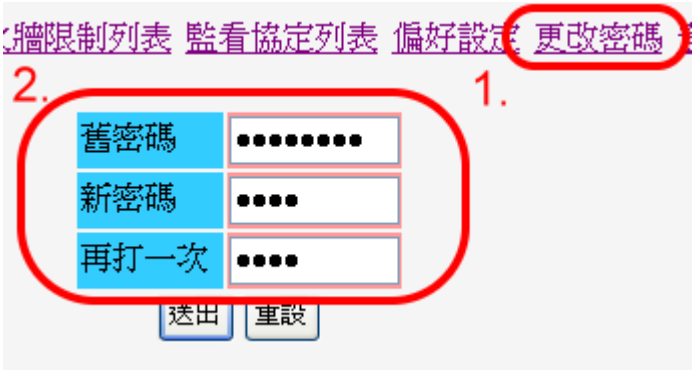
Step1. 利用瀏覽器於網址列的地方輸入原先設定外網卡的 IP 位置
(假設 IP 爲 192.168.0.1)

http://192.168.0.1/admin/ 進入管理畫面。

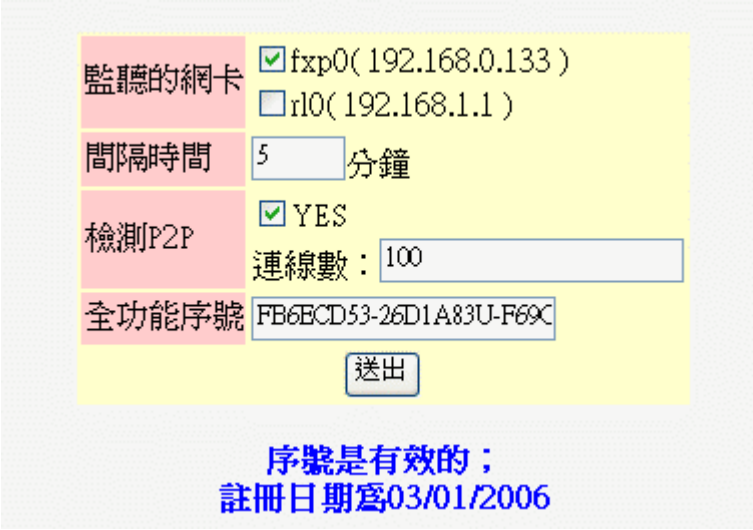
Step2. 輸入帳號 admin 與密碼 netadmin 。



Step3. 更改密碼



Step4. 偏好設定裡設定

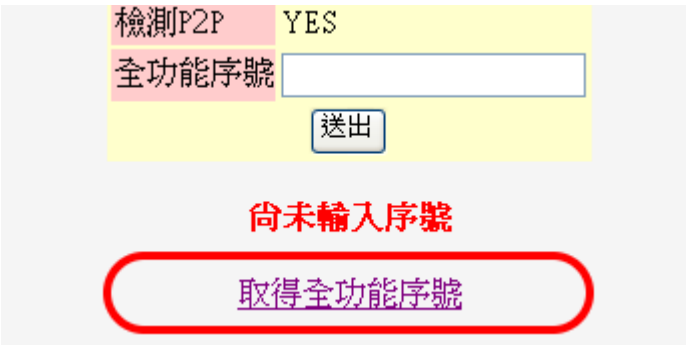


1. 監聽的網卡爲是否同時要對兩張網卡作監聽的動作，否則一般爲內網卡即可。
2. 間格時間一般爲 5 分鐘不需更改，因爲教育局的網路爲 10 分鐘偵測一次，所以設定時間一定要短少於教育局的時間，否則就沒意義了。
3. 是否對 P2P 之類的軟體作阻擋的動作，如啓用則針對其連線數超過 100 點以上才進行阻擋。
4. 序號：序號分爲正式與適用序號，序號裡內含註冊日期資料，方便查詢。
5. 設定完成後請重起防火牆即可。

3.2 產品註冊

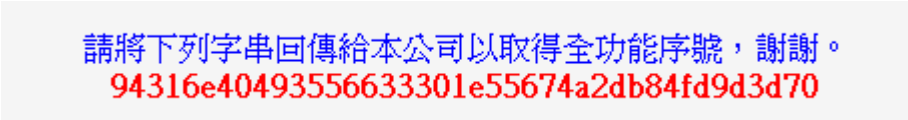
安裝好的系統是無法正常使用的，僅提供 NAT 與 DHCP 的功能，如需要試用防火牆功能皆須透過申請註冊方可使用部份或是全部功能；註冊程序非常簡單，只需依照下列步驟即可完成。

Step1. 取得系統代碼



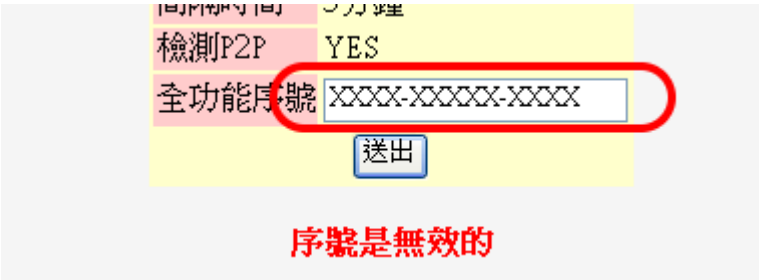
進入管理介面後，點選偏好設定裡，即可看到取得全功能序號連結。

Step2. 此序號爲網路卡 MAC 與主機板集合而成，爲獨立產生



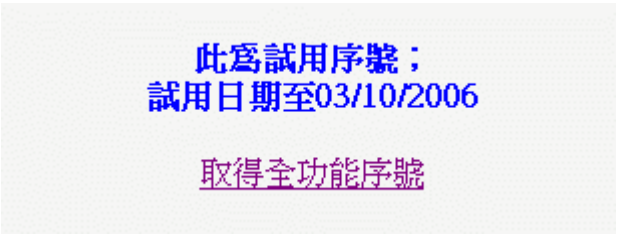
將所得到之序號利用電話、傳真或是 E-Mail 方式來取得試用序號或是購買產品，相關資訊請洽聯絡方式。

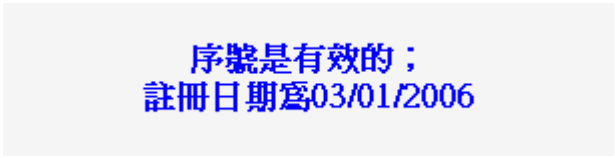
Step3. 輸入啓動序號碼



打入正確的註冊序號即可正常使用部份或是全功能防火牆

Step4. 完成註冊程序





如爲試用序號，系統會提供一組試用序號，約可使用 30 天，如上左圖示；若爲正式版則爲上右圖所示。

序號僅與主機板與網路卡 MAC Address 有關，萬一何者發生故障並且需更換時，序號會自動失效，請從新申請即可，本公司會再提供給您一組新的序號使用。

3.3 異常封包攔截設定

受管制保護內的電腦，如果發生中毒、任意掃網段、發大量封包、發送垃圾信或是非法使用 P2P 軟體存取時，皆會判定爲異常封包行爲發生，系統會自動設限相對的 IP 位置，並且會自動將使用者的電腦封包導入至限制網頁，並立即終止此 IP 對外進行網路的傳輸，讓使用者自行通知網路人員來排除。

Step1 . 設定所需檢測的 Port 與 節點數

Step2. 將常用服務埠與節點數新增或是修改即可

節點數通常爲預設 20~50 之間即可，唯讀 80 port 需 100 以上；埠號來源可參照教育局所提供即可，在此並未區分爲 TCP 或是 UDP 種類。

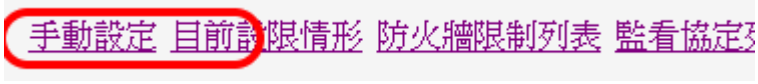
Step3. 重新啓動防火牆

重新啓動防火牆，以套用目前設定。

3.4 手動封包限制設定

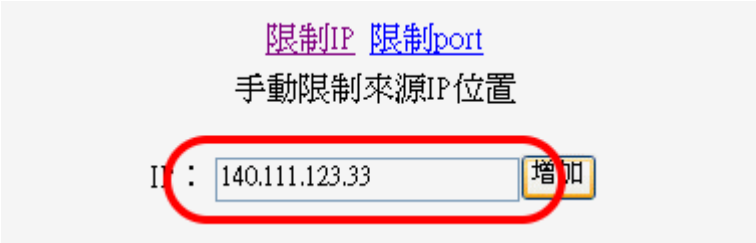
受管制保護內的電腦，如要手動限制禁止使用特定網路或是限制保護內的電腦允不允許存取對外網路皆可透過此一功能來達到其限制目的，限制種類依功能可分爲限制 IP 位置或是限制連接埠號。

Step1. 進入管理介面，進行設定



登入後選取手動設定選項。

Step2. 手動限制 IP

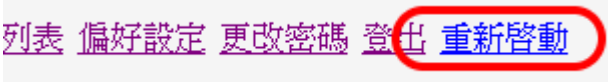


直接打入要阻擋的 IP 位置即可。
在此可提供外部 IP 或是內部 IP 位置，亦即，輸入外部 IP 時，表示保護內之所有電腦皆無法到此一 IP 位置（例：某某色情網站之類的），如輸入內部 IP 時，則表示，僅此一電腦無法進行任何的網路對外連線。

Step3. 手動限制通訊埠

將所需阻擋的通訊埠依類別 TCP 或 UDP 填入即可，上圖表示所有受到管制的電腦皆不可與外面任何一部主機作 TCP 3389 & TCP 5000 & TCP 1863 的連結，但卻可以做 TCP 80 或 TCP 21 等其他方式連結，通常用以阻擋線上遊戲或是聊天通訊軟體等等。

Step4. 重新啓動防火牆



重新啓動防火牆，以套用目前設定。

防火牆保護內被設限的電腦，當瀏覽網頁時，提供主動畫面提示訊息，如下圖

註：當電腦出現此畫面後，務必透過管理者方可解除限制，即使用戶端從新安裝系統也一樣。

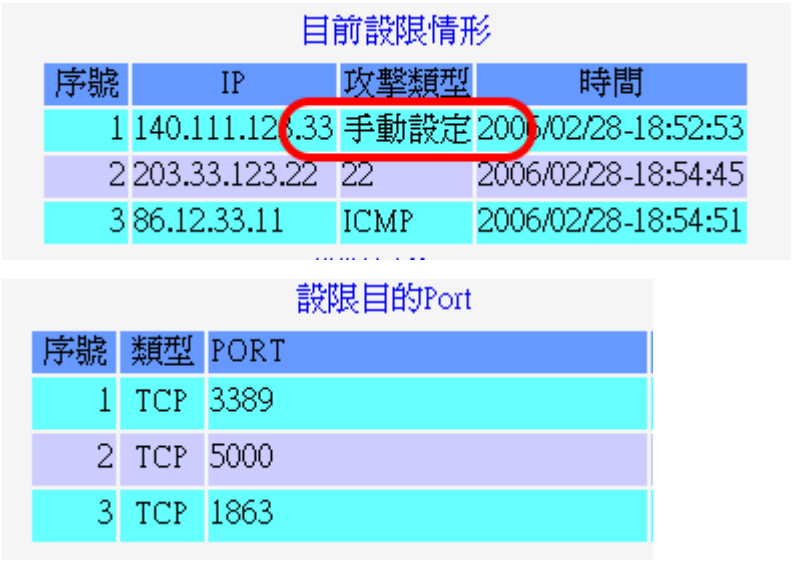
3.5 解除設限的 IP & Port

解除程序非常簡單，只需透過管理介面，登入帳號後即可解除被設限的 IP 位置或通訊連接埠。

Step1. 目前設限情形

Step2. 被設限 IP 位置與異常行為種類

Step3. 手動限制與通訊埠的部份



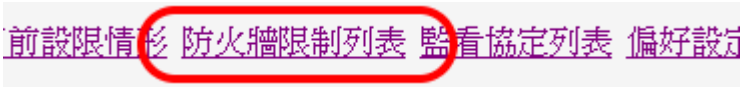
目前設限情形

序號	IP	攻擊類型	時間
1	140.111.123.33	手動設定	2006/02/28-18:52:53
2	203.33.123.22	22	2006/02/28-18:54:45
3	86.12.33.11	ICMP	2006/02/28-18:54:51

設限目的Port

序號	類型	PORT
1	TCP	3389
2	TCP	5000
3	TCP	1863

Step4. 選擇防火牆限制列表進行解除設限動作



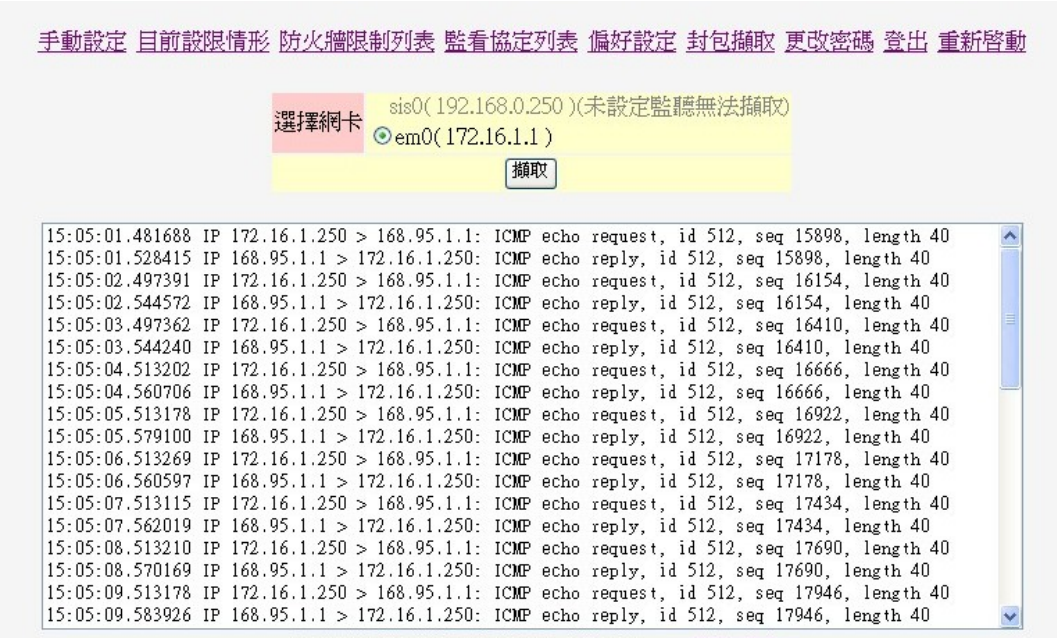
Step5. 點選所需解除 IP 或通訊埠即可

序號	停權IP	功能
1	140.111.123.33	解除
2	203.33.123.22	解除
3	86.12.33.11	解除

3.6 例外清單、QOS 頻寬限制政策、網路封包擷取

此功能爲自行設定白名單，方便下層網路架設 IP 分享器或是封包分析監測軟體應用時，不至於發生誤判的可能。

此功能爲設定簡易 QOS 頻寬功能，可自由限制每部電腦的網路流量管理。



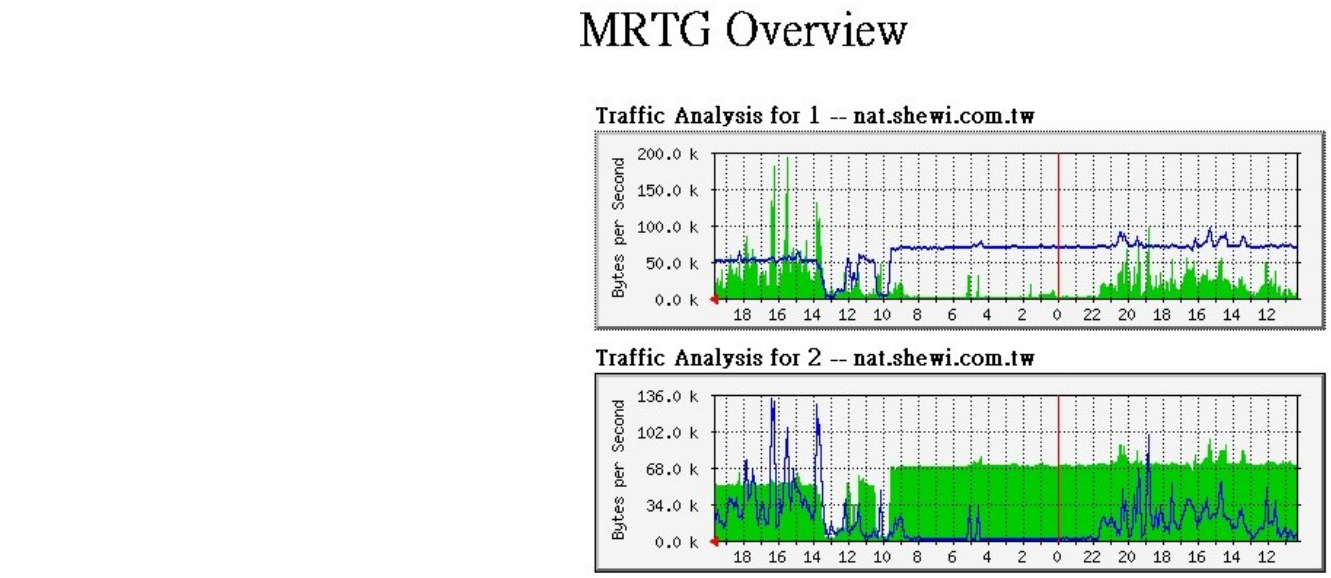
此功能爲封包擷取畫面，讓網管人員更方便的了解目前網路的問題。

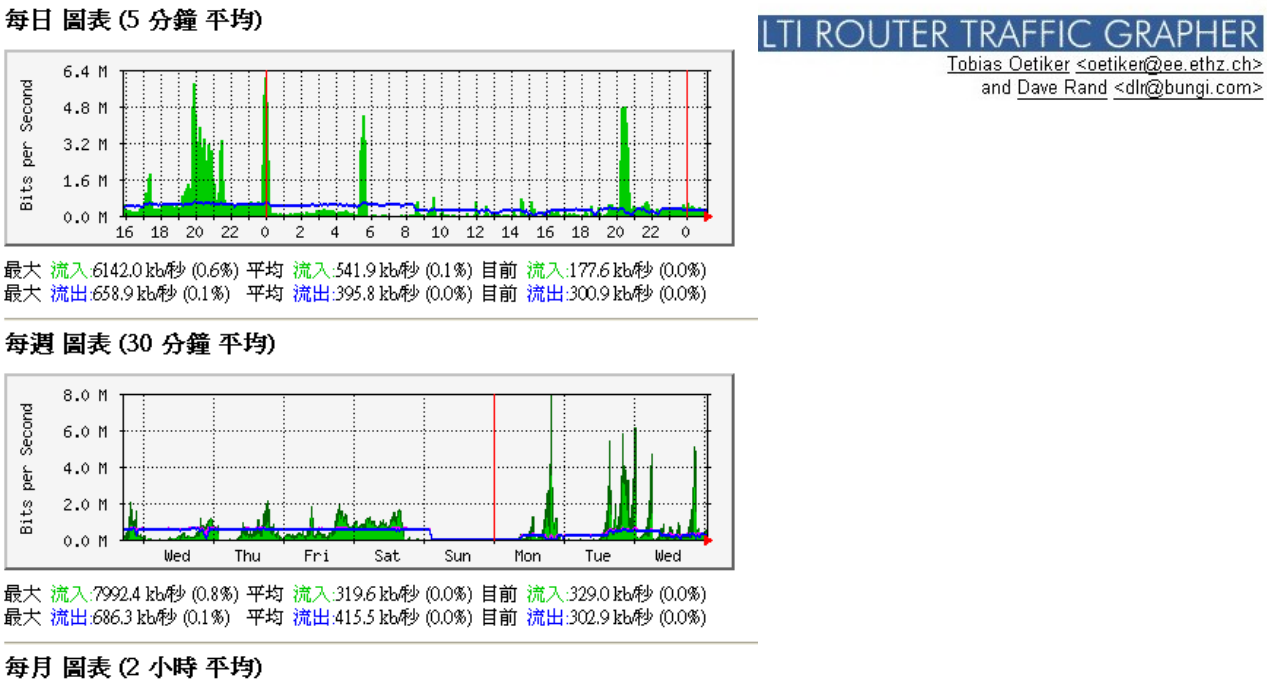
第四章 其他功能說明

防火牆本身除了針對異常行爲或是手動加入限制規則外，另提供一些管理人員常用的一些工具，以利找出問題背後發生的真正原因與解決辦法

4.1 MRTG 流量監視

透過瀏覽器打入網址 http://192.168.0.1 會顯示 MRTG 的流量圖表



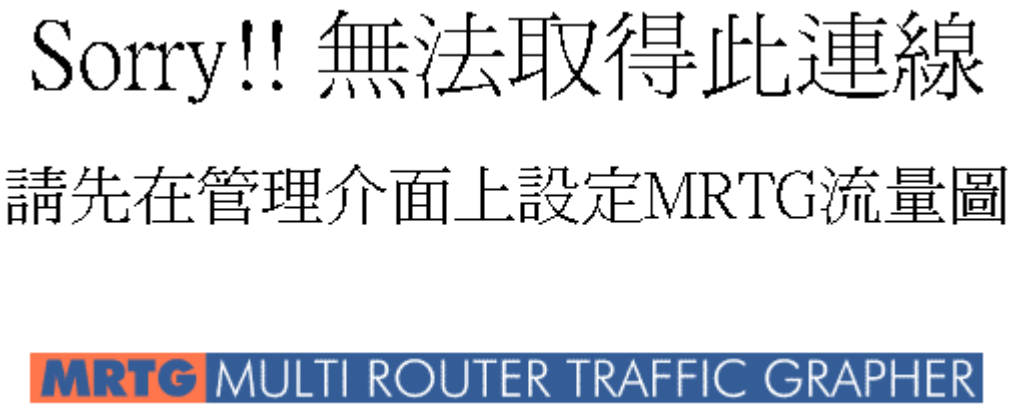


LTI ROUTER TRAFFIC GRAPHER

Tobias Oetiker <oetiker@ee.ethz.ch>
and Dave Rand <dlr@bungi.com>

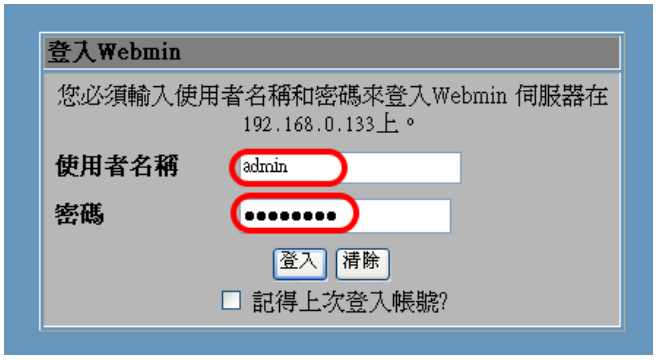
設定方法請依照下列方式：

Step1. http://192.168.0.1



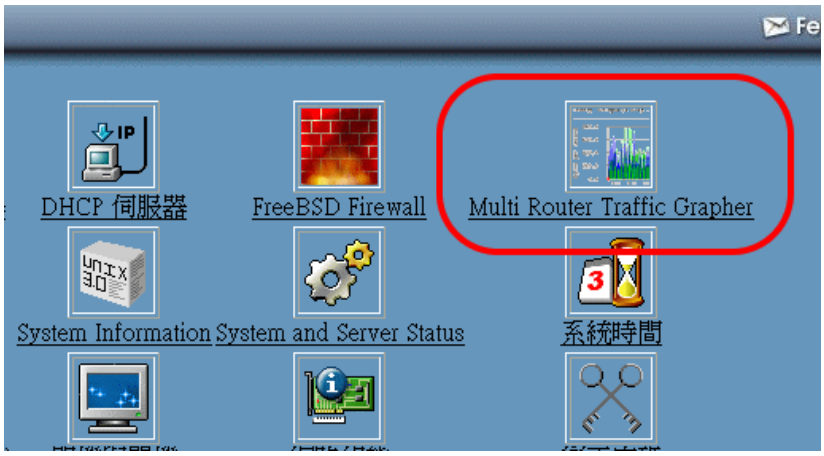
尚未設定時看到的畫面。

Step2. http://192.168.0.1:10000



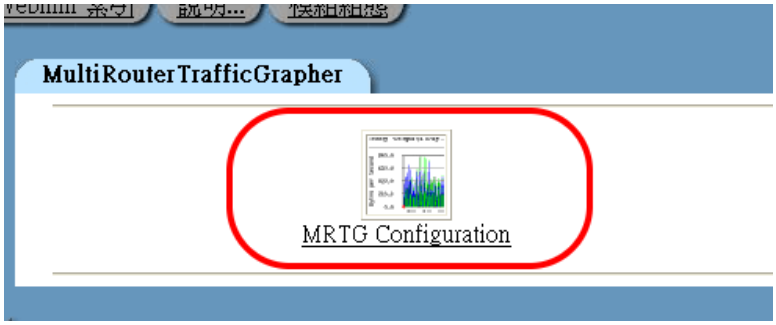
輸入預設號密碼 admin : netadmin

Step2. 設定 MRTG 流量圖



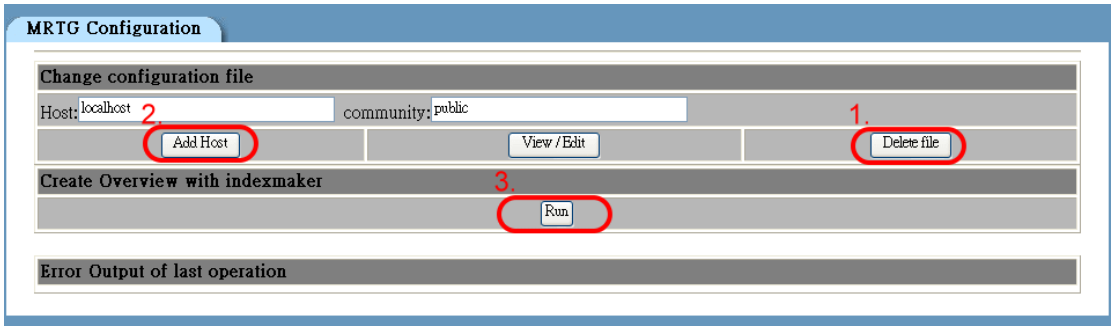
點選 Multi Router Traffic Geapher 選項

Step3. 設定 MRTG 流量圖



點選 MRTG Configuration 選項

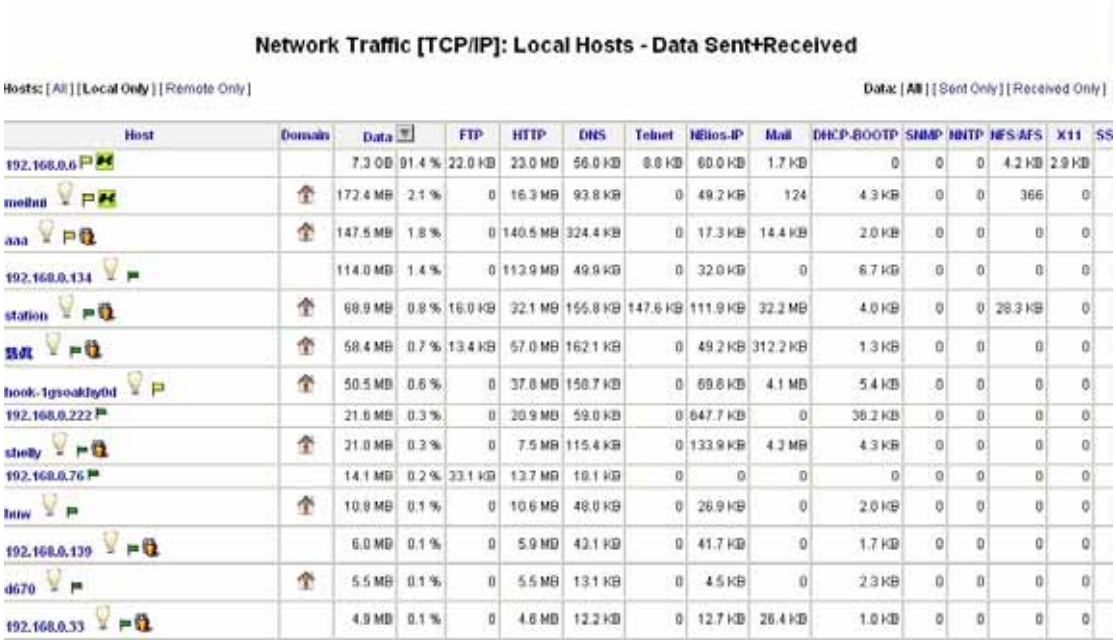
Step4. 設定 MRTG 流量圖



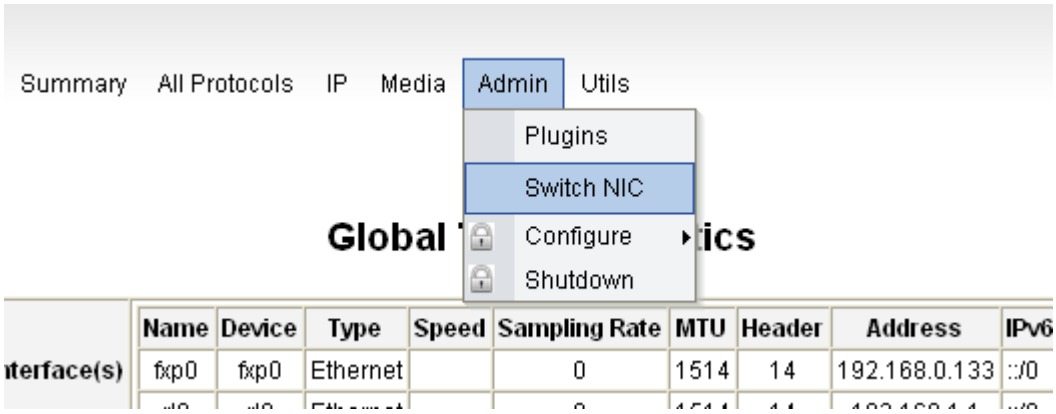
依照步驟，即可完成設定，回到網頁，等候 5 分鐘，就會有流量圖案出來囉。

4.2 NTOP 3.1 封包狀態分析

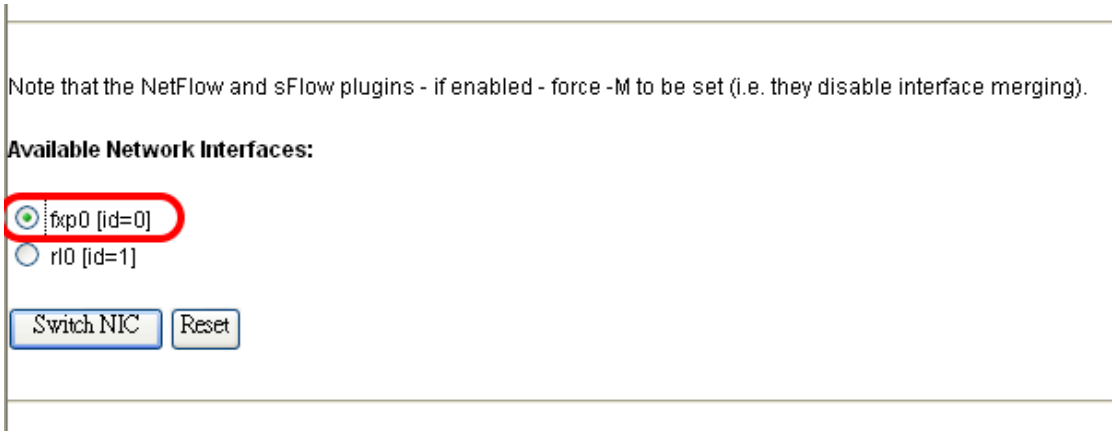
透過瀏覽器打入網址 http://192.168.0.1:3000 會顯示 NTOP 的封包分析圖表



如需監看內或外網路卡的資料，可於 Admin 選項裡的 Switch NIC 進行切換



圖一



圖二

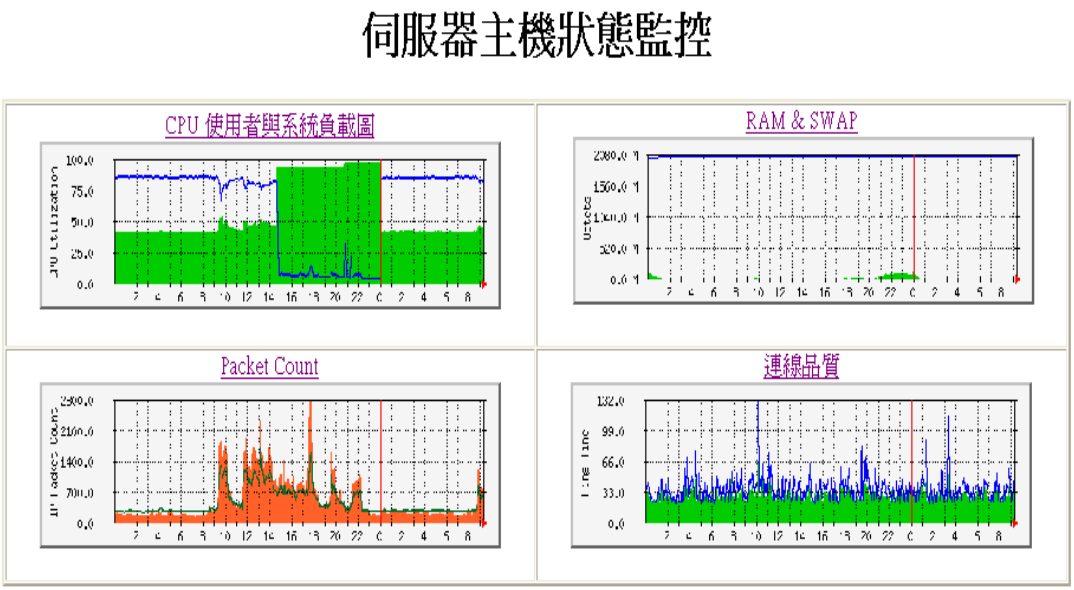
註：1.所有資料統計皆爲一天，既當天僅提供 0~24 點之間的流量-。

2.防火牆設定爲 Transparent Mode 時，不分內外網路卡流量，以總流量表示。

4.3 系統狀態表

透過瀏覽器打入網址 http://192.168.0.1/phpSysInfo/ 會顯示系統狀態資料。

透過瀏覽器打入網址 http://192.168.0.1/sysinfo/ 會顯示系統狀態資料。



4.4 進階設定

Webmin 管理介面請務必更換密碼，更換方式如下：透過管理介面進入 http://192.168.0.1:10000

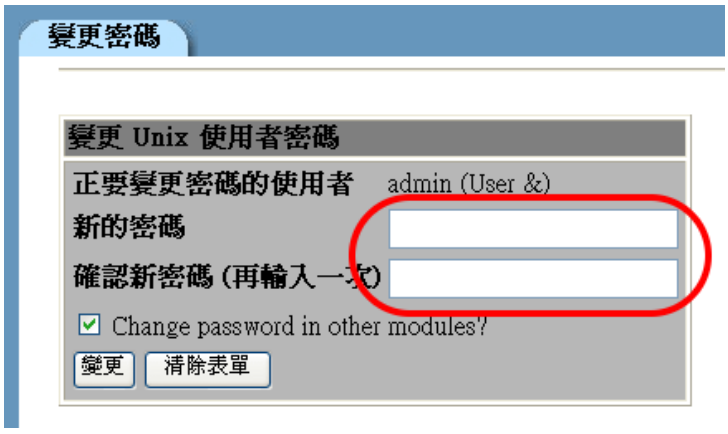
Step1. 變更密碼

點選 變更密碼 選項

Step2. 變更密碼

點選 admin 帳號 (如果可能的話，請連同 root 一併更改。)

Step3. 變更密碼



鍵入 新的密碼 並點選變更按鈕即可完成密碼更換。

細部參數的設定

防火牆本身除了網頁式管理外，還提供另外更細部的選項，設定方法如下(通常可不更改，使用預設即可。)

Step1. 以 Console 方式登入

登入後切換目錄至 /usr/local/etc/mrtg/admin/ 底下

以文字編輯器修改 config.php 參數檔

Step2. 參數檔內容如下 vi config.php

```
<?php
$optionFile = "option.txt";
$filename = "data.txt";
$denyFile = "deny.txt";
$tmpFile = "tmp.txt";
$webuser = "www";
$p2pCheck = true;
$p2pLimit = 100;
//server ip and port. DON'T MODIFY THIS
$localAddress = "127.0.0.1";
$localPort = "3125";
//admin config
$session = 30;//min                                          //閒置多久後自動登出
$adminName = "admin";                                        //管理者的帳號
$adminpw = "d92899c8cba68c81bf496197c4f0fdcb0dd44d26";       //管理者的密碼(編碼過)
//present that why can't connect outside network.
$denyMsgHost = "127.0.0.1";
$denyMsgHostPort = "81";
//where can browse webpage
$haveRestriction = "1";                                      //0 表示任何地方都可存取防火牆網頁
$autoDetectAllowNetwork = "1";// 1=Yes;0=No                  //1 表示自動偵測可存取的網段(預設
                                                               爲網路卡所存在的網段)
$allowNetwork = "192.168.0,192.168.60,10.10.10";             // 手動加入可遠端控管的 IP 位置，當上
                                                               一選項設定爲 0 時，才有作用
$NIC = "rl0";
$duration = "5";
$serialNumber = "F6ECBD53-2U6D1A83-F691G713-C99DB44D-50B76501-D42E641432--1871347210";
?>
```

上述的 where can browse webpage 裡面表示設定網頁存取與否，如無法存取時則會出現 **【您無權限使用此服務。】** 字樣。

第五章 問題與討論

5.1 已知問題

5.1.1 電腦主機沒有任何問題，卻還是被設限？

此發生的原因通常爲，有問題的電腦使用者自行更換 IP 位置，導致這個位置被封鎖了(如使用者使用 P2P 軟體被封鎖後又自行更換 IP 位置)，正好這個 IP 又被配發到其他正常的電腦。

5.1.2 防火牆內另存在著 NAT 的網路架構環境？

會造成防火牆的誤判，以爲此一 IP 流量與行爲模式異常，並針對其封鎖，進而導致 NAT 底下的電腦全部被設限。

5.1.3 會不會發生防火牆已經設限了但教育局也接著設限的可能嗎？

有的，因爲瞬間攻擊封包過大，防火牆本身是分析 5 分鐘內的資料，所以 5 分鐘內的封包皆會傳到教育局的主機，所以會發生 5 分鐘後，防火牆先阻擋，而後十分鐘後，教育局卻阻擋防火牆對外的 IP(此行爲理論判斷，應不會發生，但實際上有可能發生，即使發生了，管理者也知道是哪部電腦出了問題之類的)。

5.1.4 對整體網路效能有無影響？

不會，因是爲收集 5 分鐘之內的封包再做分析的判定，並不像高階防火牆做封包即時性全檢的動作，需要很高速的硬體或設備。

5.1.5 有沒有誤判的可能？

應當是會發生，假使誤判時，可先解除，如果電腦確實有異狀，也會於下 5 分鐘之後被設限。(疑似有些軟體會先做網路的檢測等等，譬如 sniffer 封包分析、資產軟體等等。)

5.2 試用版功能的限制

除了時間試用參數外，試用版與正式版最大的差別在於兩項功能，其一爲手動增加限制 IP 與通訊埠的功能；其二爲當主機發生問題進而導致防火牆對其設限後，沒有提供解除的功能，亦即僅會阻擋而已，但不提供管理者對受限電腦做解除的動作，但是當主機進行重新開機的動作以後就會自動解除所有設限。

5.3 自動封鎖與自動解除限制

當異常行爲發生後，主機會分析完封包後並自動加以阻擋，直到管理者手動解除設限或是主機重新開機後，才會自動清除被受限的主機。

但如果當限制是由手動增加的方式，如手動新增 IP 或是通訊埠等，除非管理者下達解除命令外，即使主機重新開機，受限皆還是存在的。

5.4 備忘錄

第六章 聯絡方式

旭威電腦資訊有限公司

Shewi Computer CD.,LTD.

電話：03-4896789
傳真：03-4791472
地址：桃園縣龍潭鄉中正路 117 號
統一編號：86370255
Mail：service@shewi.com.tw