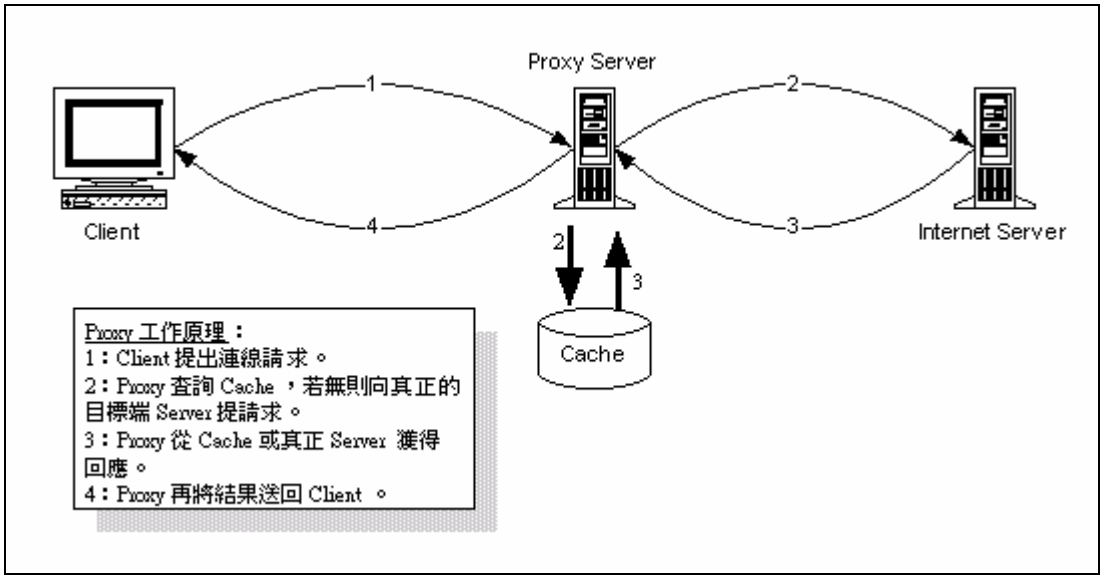
# 防火牆 NETSCREEN 10 設定說明

## 何謂防火牆

Firewall 一詞，原本是建築物上用來阻隔火災的結構，也有說是位於引擎室與駕駛艙之間的汽車部件。網路的火牆就是這麼用途的啦：將危險的、不安全的連線阻隔在您的網路之外。而我們通常說的火牆有兩種：過濾性火牆(filter) 和 代理性火牆(proxy)。若沒特別說明，我們一般所說的火牆是指過濾性火牆。

然而，從安全覺度來看，proxy 比起 filter 來說，將更加可靠：因爲它將內部與外部網路完全區隔開來了，除非它幫您做連線代理，否則別想建立連線。而且，內部網路對外部網路而言，是完全"隱形"的！除此之外，proxy 也有其非常好用的地方，比方說我們可以利用單一的連線，如使用 modem/ADU-R（ADSL），然後讓整個內部網路連接外部資源，不僅節省硬體成本，而也無需支付多個 ISP 帳號與電話線路。Proxy 的功能就是“代理”，可以分爲“程式代理”和“socks 代理”，如無特指，一般是指程式代理。

前者可以說是爲你代理所有應用軟體的連線工作：當您需要連接外部資源的時候，您的請求是直接送給 proxy ，然後，proxy 會幫您到真正的目的地去獲取，然後再轉送給您。而每一次的代理動作，它都會將資料保留一個備份，存在它的快取區去，如果再接獲相同的請求(不管是原來的機器，還是另外別的機器發出的)，它就將存於快取裡面的資料做爲回覆。有些聰明的 proxy 還能知道快取裡面的資料是否和實際目的地的資料同步呢，如果發現實際目的地的資料經過更新，它就會再次複製進自己的快取去。




Proxy 之工作原理

從上面的這個過程，我們可以看得出，proxy 還可以提高網路的存取速度哦，因爲如果資料已經在快取裡面了，其傳送都在 LAN 裡面進行，而無需經過複雜的路由程序。同時，因爲資料無需從外面重複傳遞，實際上，也令到網路的流量減少許多。而且，通過 proxy ，我們也可以省下許多 IP 位址，因爲其他機器盡可以使用私有 IP 就行了。目前正時興的網咖(Internet Cafe)，許多就是利用 proxy 來降低成本和提高 www 的瀏覽速度。另外，proxy 還可以再經由上游 proxy(或 proxy 陣列) 連接 internet ，從而再可以提高效率和安全性。

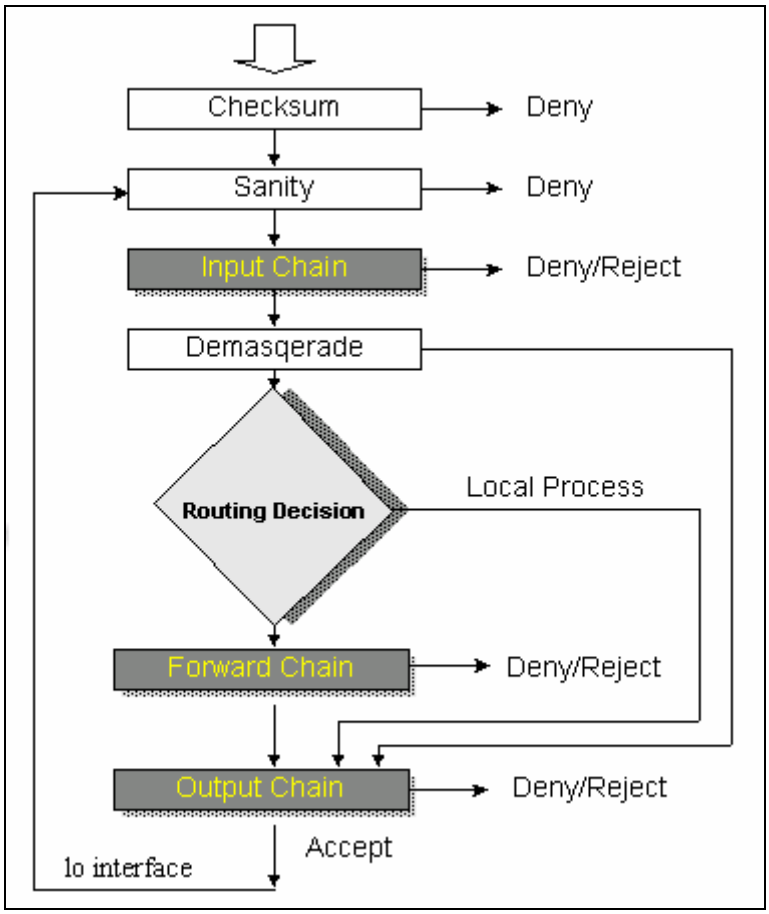
而 socks 代理呢？就好像接線生那樣，僅是將您的 TCP 連接由裡面的接口搭至外面的接口而且。還記得在“網路概念”裡面提到的 API 嗎？socks 代理其實就是代理 API 請求而已，而真正處理工作的，還是發出請求的主機本身。

這裡還要一提的是“NAT(Network Address Translation)”，它的工作原理也非常近似 socks proxy ，不過，它是利用轉換封包的位址來達到目的。如果本地網路主機要將一個封包送到外面網路，當火牆收到這個封包的時候，就會啓動 IP 僞裝功能(Masquerading)，將來源位址暫時轉換成其本身位址，然後等到接到回應封包之後，再將位址進行還原(Demasquerading)。在裡面的機器根本就無需知道這個動作，一切都由火牆處理好了。這和 Proxy 一樣，也可以節省大量的 IP 位址，而讓使用私有 IP 位址的主機也能夠存取 internet 了。因此，有人也將 NAT 稱爲 IP Proxy 。

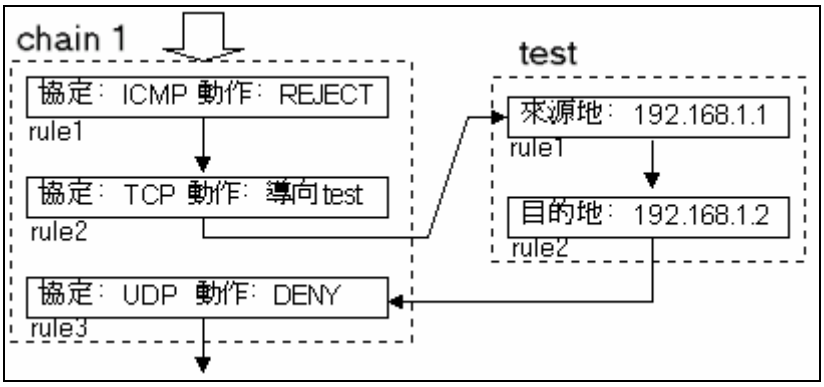
## 防火牆的運作原理

如果您對 TCP 與 IP 協定已經相當了解的話，尤其是 IP 封包和 TCP 封包格式，那麼，您將會更容易了解(過濾性)防火牆的運作：火牆會對所有經過的封包進行檢查，按照一系列規則(rule)，來決定封包的處理方式。火牆一般都會根據封包的來源和目的位址、協定、port、界面等因素進行判斷，決定是否讓封包通過。提醒一下：firewall 只管放行與否，至於要送到哪裡去，則是 routing 所負責的。

以 Linux 2.2.x 核心的 ipchains 爲例，我們可以爲火牆建立一些基本原則來定義好各種的鏈(chain)：傳入(input)、傳出(output)、轉遞(forward)、重導(redirect)、等，來決定封包的處理動作：接受(accept)、拒絕(deny)、回絕(reject)、轉遞(forward)、僞裝(masquerade)、等。在此基礎上，然後再配合實際情形設定更多規則加以限制。




我們設定規則的時候是非常多樣性的，也可以由一個 chain 導向另一個 chian ，直到符合我們的要求爲止。下面讓我們看一看一個非常陽春的規則設定例子：




當我們從一個 chain 跳到另一個自定義的 chain 的時候，如果自定義的 chain 沒有將封包剔除的話，就會回到剛才的 chain 的下一個規則去，繼續其後的規則檢查。從上例中我們可以看到：只有從 192.168.1.1 傳給 192.168.1.2 的 TCP 封包才能過關，其它諸如 ICMP 和 UDP 封包，及其他位址的封包一律會被擋掉。只要我們精心設計，不難設定出一個適合自己情形的不太鬆也不太緊的火牆的。

## 應用層防火牆

應用層防火牆是在 OSI 七層架構中第七層（應用層）運作（圖 A 爲其示意圖），它利用代理程式（Proxy）所設定的安全存取規則，儲存並轉發（Store and Forward）客戶端（Client）對伺服端（Server）提出的連線要求；組織內部欲對外界提出連線要求時，其運作原理亦同，只是方向是由內向外。此方式客戶端與伺服端雙方無法直接連線，必須透過此特別設計的安全代理程式代爲處理，避免入侵者直接連線攻擊，其優點除了提供代理服務外，在應用層也提供較好的用戶認證（除一般授權檢查外，也可以限制使用者登入／拜訪主機、登入時間等）、日誌訊息（Audit log）及過濾規則，依開發技術可以再分爲代理型（Proxy）與調適代理型（Adaptive Proxy）兩種，下面分述之：

(1) 代理型：
防火牆的安全政策／規則是在代理程式上設計，每一種被允許的服務程式都有其特定代理程式，例如，HTTP、FTP、SMTP 等服務程式，各有對應之 HTTPProxy、FTP Proxy、SMTP Proxy 代理程式來處理，其在外部網路向內部網路申請服務時發揮了中間轉接的作用，當客戶端將連線要求傳送到防火牆時，防火牆會分析其封包的內容及協定，如果政策／規則允許，則防火牆就會代表客戶端與伺服端建立一條新的連線，圖 A 爲其示意圖。

(2) 調適代理型：
它結合代理伺服器與動態封包過濾的功能，在防火牆中設定所需要的服務類型所對應的代理程式即可，防火牆中的代理程式就會接受客戶端之連線要求與要求服務之封包，並檢查封包標頭或資料，再爲該代理程式與伺服器建立新連線，而未設定代理程式之封包，則在網路層直接過濾與轉發，換言之，它結合了代理型防火牆的安全性和封包過濾式防火牆的高速度等優點，圖 B 爲其示意圖。

應用層防火牆的優點有：

如前述，在 OSI 第七層應用層代理程式的儲存並轉發客戶端對伺服端提出的連線要求，能防止直接的連線攻擊。

缺點是：

和封包過濾式防火牆相比較，則因是在應用層處理之故，速度比較慢，不適用於高速網路，例如，非同步傳輸（Asynchronous Transfer Mode，ATM）高速網路等。

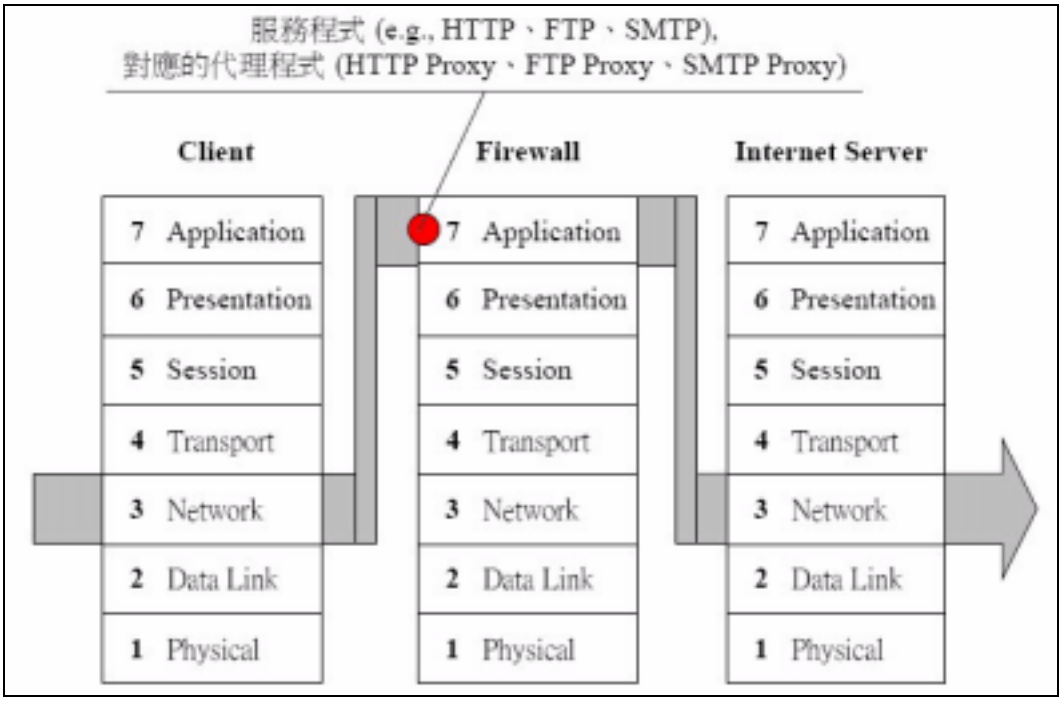



圖 A 代理型防火牆

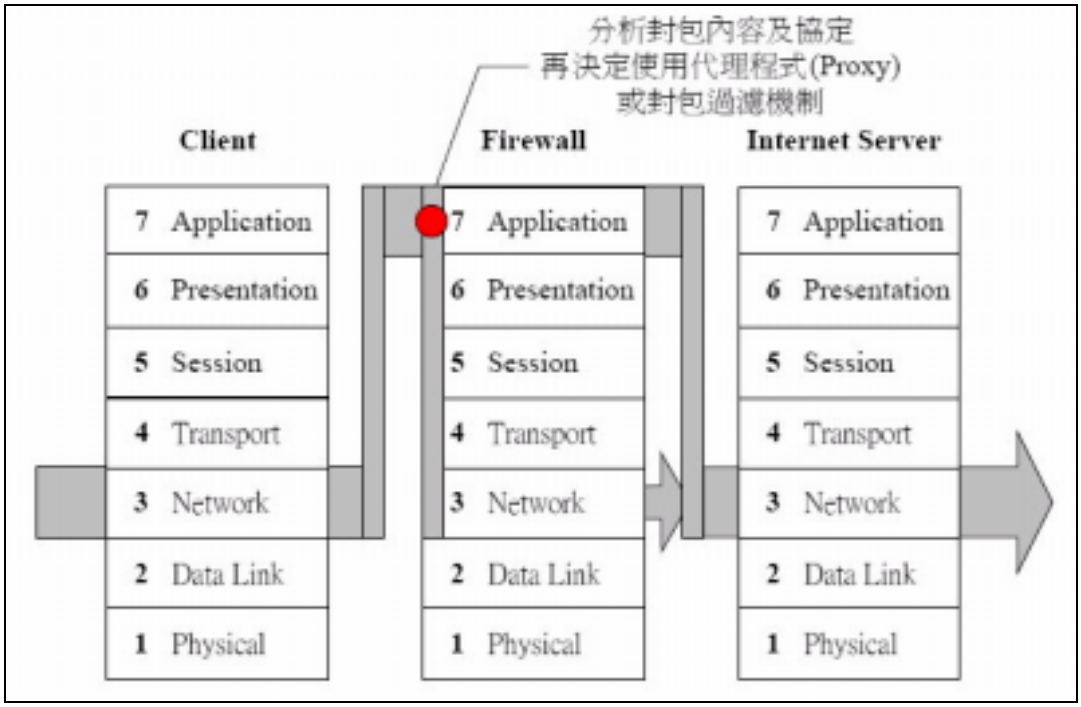



圖 B 調適代理型防火牆

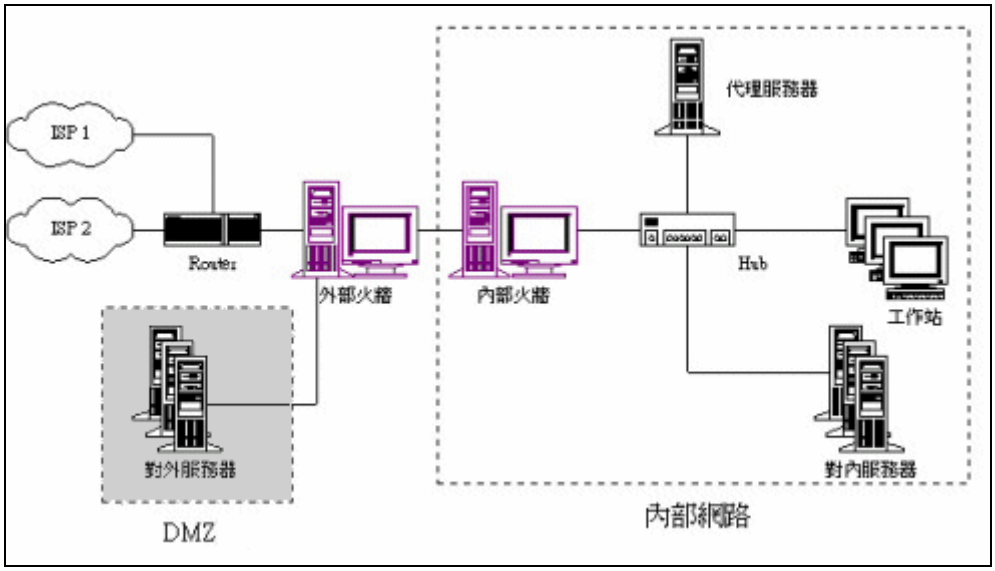
## 防火牆的設定技巧

從上面的防火牆運作來看，我們可以運用設定規則，將一些重要的主機保護起來，讓其只允許特定的網路存取，也就可以將大部份的網路入侵者致於門外。不過，對於那些絕頂駭客高手而言，還是會從您的設定漏洞攻破您的把守的，例如：他們通常會使用“取道”的方法，繞過那些被禁止的位址，以及通過不斷改變位址來逃避追蹤。有些較優秀的火牆程式，可以自動檢測一些駭客常用的攻擊方法，除了會對網路管理員發出預警之外，還可以即時切斷該等連線，和追查路徑等動作。

同時，利用不同系統來設定多個火牆，也能提高防禦能力：除非駭客對所有系統都熟悉，否則，過了一道火牆，還是過不了第二道火牆；而且由於第一道火牆的屏隔，要探測第二道火牆的難度也高許多。當然，要設定的規則就更爲複雜了，通常都會造成過於嚴厲而令到一些網路資源無法使用，或降低了網路的效能。

所以，設計一套完善的規則，其實是件極具挑戰性的事情，其後也需要不斷的測試以修補漏洞，這也是非常耗時的工作。如果對一個繁忙的網路來說，事先的測試工作就顯得非常重要了：您總不能在收到一大堆不能連線的投訴之後而關閉火牆作調試吧？

通常我們在設定火牆的時候，劃分一個“非軍事區(DMZ - Demilitarized Zone)”是非常好用的：




我們可以設定火牆，允許外部直接傳入到 DMZ 上面的伺服器，但僅限制於某些特定的協定，如 DNS、WWW、FTP、MAIL 等，同時也允許內部網路使用這些服務。但外部網路是完全禁止進入內部網路的，而內部網路則可以通過 Proxy 存取外部資源；我們也允許內部伺服器使用 rsync 協定來和 DMZ 上面的機器進行資料同步。一般我們不會將重要的資料存放在 DMZ 上面的機器，而且郵件也會在 DMZ 接收後由內部伺服器提取進來。這樣，就算那裡的機器被攻破了，也不至於損失太多。

§ 防火牆 NETSCREEN 10 設定 §

- System （設定 F/W 的系統單元）

一、Configure　F/W 主要項目設定

1. General （防禦項目與時間同步化）

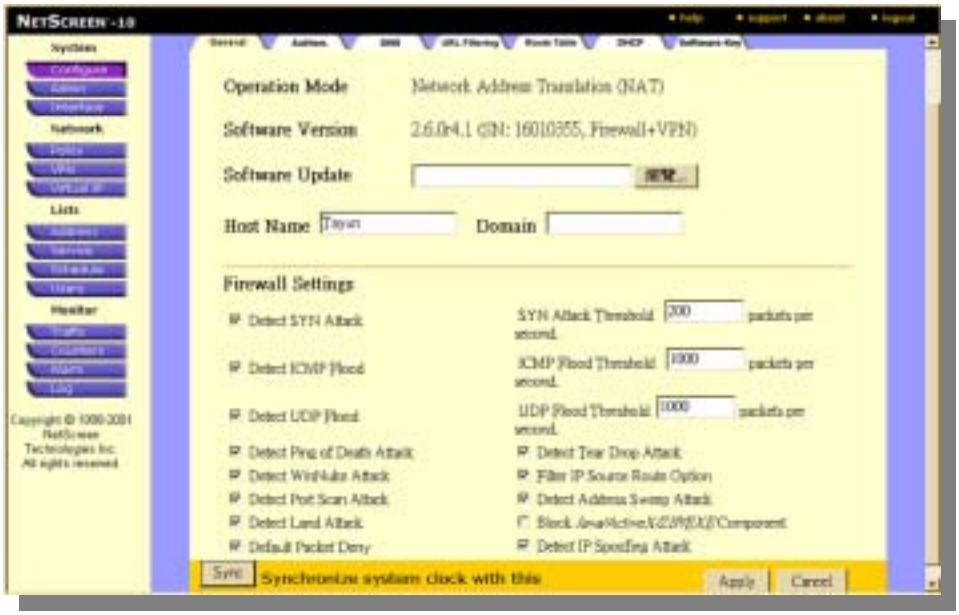



圖 FW system configure-00.jpg

Software Update：爲防火牆要更新 BIOS 的瀏覽選項

Host Name：爲防火牆的名子

Doman：爲網域名稱。（如 fromus.com.tw）

Firewall Settings：勾選的項目是可做的防禦。

（建議 Block Java /Active X/ZIP/EXE Cormponent 選項不要勾選）

Synchronize system clock with this client：將時間與你的電腦同步化。

2. Authen （進入 NetScreen 認證）

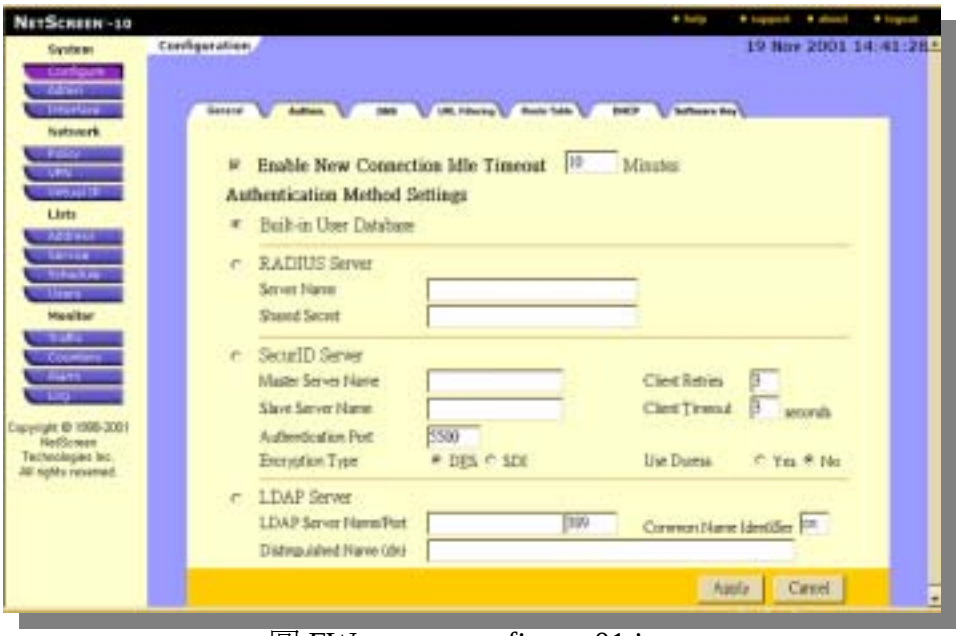



圖 FW system configure-01.jpg

**Enable New Connection Idle Timeout** ：限制時間多久 WEB 畫面 timeout。（預設值 10 分鐘）

**Authentication Method Settings**

Built-in User Database：允許登錄 netscreen 的使用者，即 System\Admin\Admin\ **Local Admin User Database 所允許的項目**。（參 P.8 頁 ~ P.9 頁）

RADIUS Server、SecurID Server、LDAP Server：登錄再確認名稱與認證機制。（如 LDAP 通訊協定的認證機制再 Microsoft WINDOWS 2000 有）

3. DNS （防火牆 DNS 參數設定）如，同 PC 上所設的 DNS 位址一樣


圖 FW system configure-02.jpg

Primary DNS Sever：爲所用之 DNS 預設位置（202.145.138.200 爲 TTN 的 DNS）。

Secondary DNS Sever：爲所用之 DNS 次要位置（210.17.1.1 爲 TTN 的 DNS）。

DNS refresh every day at:勾選課設定 DNS 多久作更新動作。

4. URL Filtering 設定限定與過濾網址（但必須另購安裝 Websense 軟體）

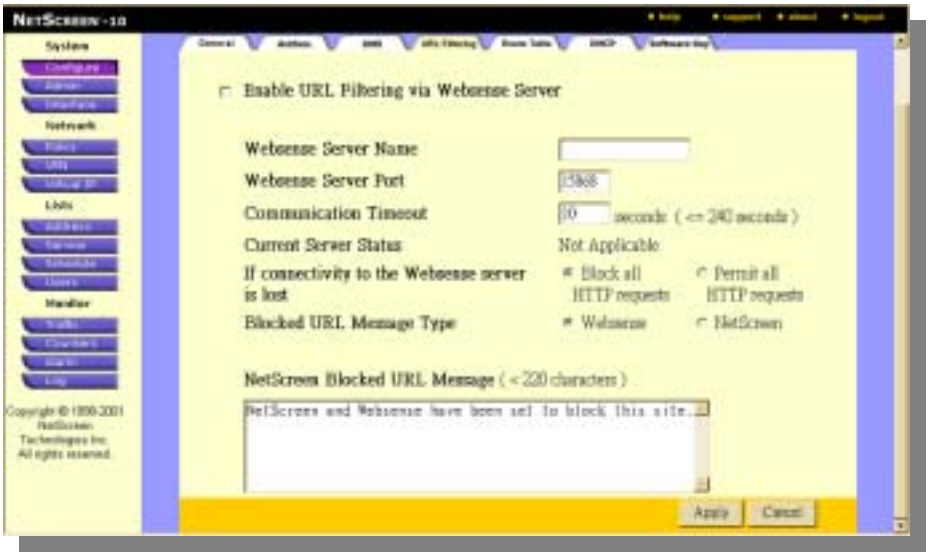



圖 FW system configure-03.jpg

Websense Server Name：爲該限定網址電腦名稱。

Websense Server Port：爲流通埠（如 hppt：\\爲 80）。

5. Router Table （路由連結點）

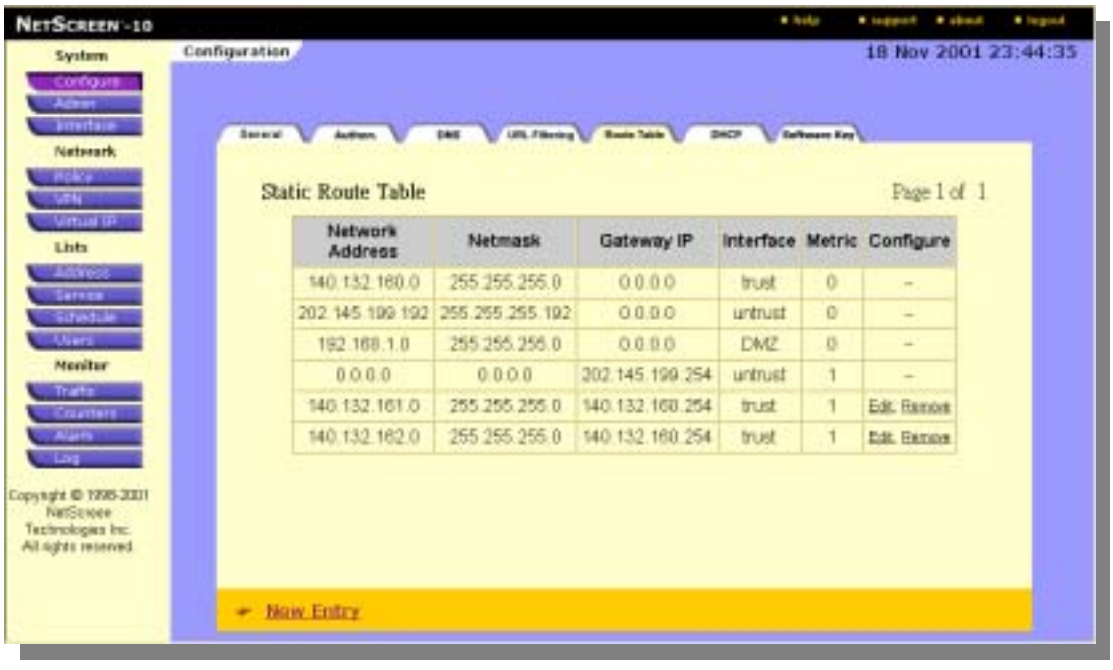



圖 FW system configure-04.jpg

建立新的連結 New Entry

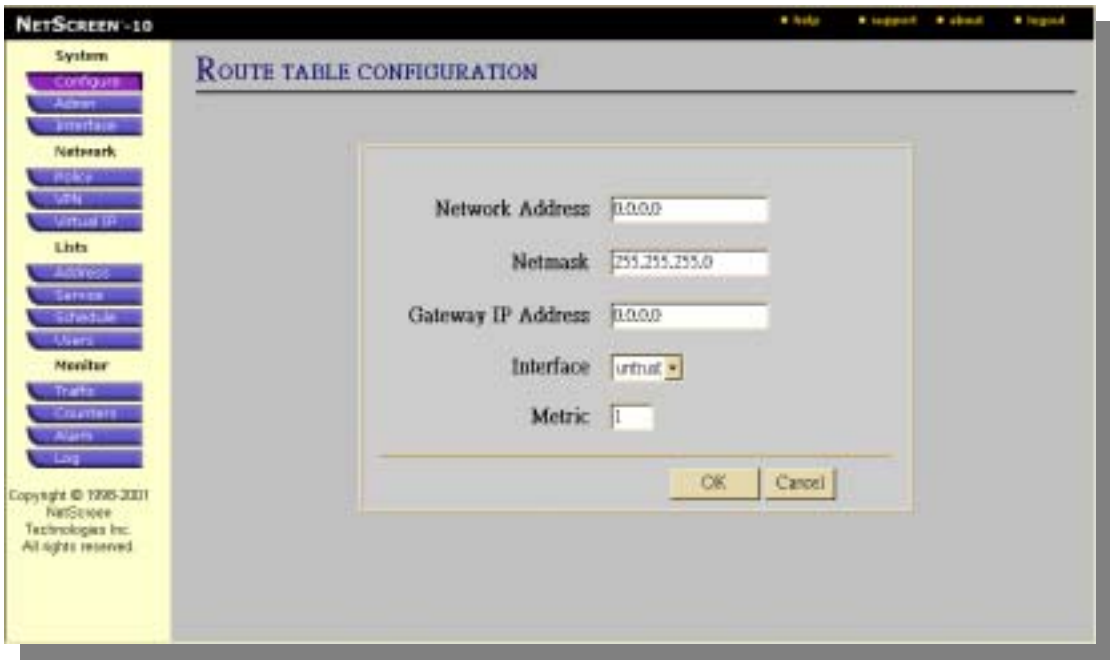



圖 FW system configure-04-1.jpg

Network Address：爲網段起點 IP 位址。

Netmask：爲網段終點 IP 位址。

Gateway IP Address：爲通訊閘道位址。

Interface：具有 trust 內部信任 、 untrust 外部信任 、DMZ 非戰區（武裝區）。

Metric：

6. DHCP （建立簡單的 DHCP Sever）

（ 若無 DHCP Sever 可在這加以設定簡易 DHCP Sever，建議以電腦主機來當 DHCP Sever 不要以此工具）

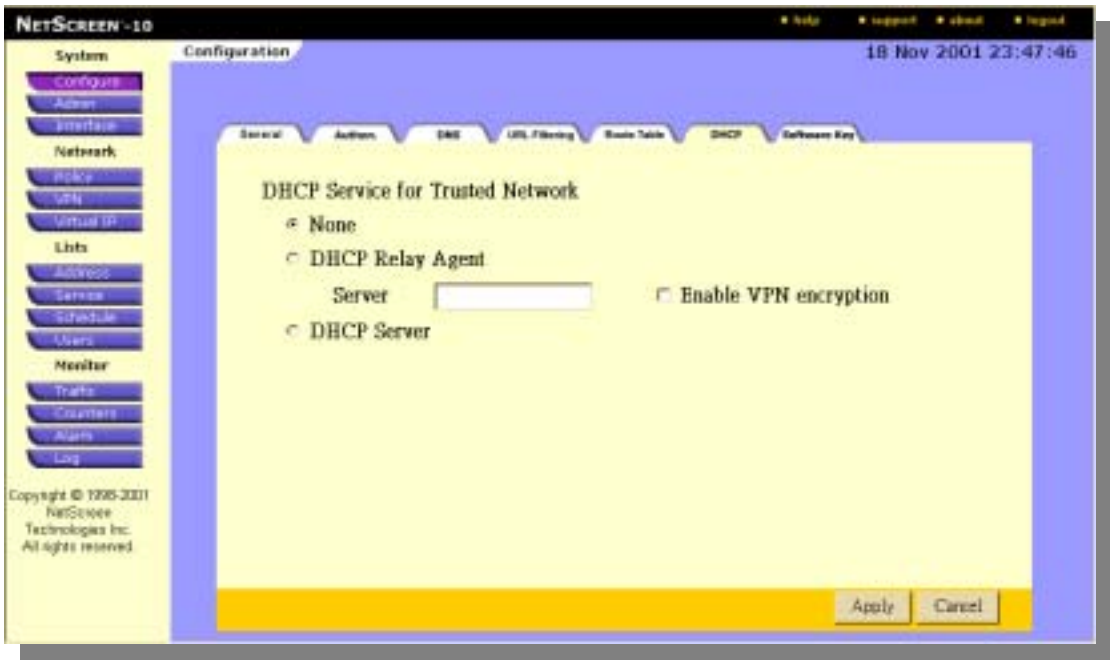



圖 FW system configure-05.jpg

None：不要加以設定。

DHCP Relay Agent Sever：代理 DHCP Sever 的 IP 位址。

Enable VPN encryption：加密。

DHCP Sever：

7. Software Key （做爲 VPN 安全機制確認）


FW system configure-06.jpg

License file Update：VPN 參數 Update。

License Information：VPN 安全機制詳細訊息。

Apply：套用。

Apply and Reset：套用並新啓動。（若 file Update 後記得先 Apply 在點選 Apply and Reset）

二、Amin 做 F/W 的管理

1. Admin （系統管理員）

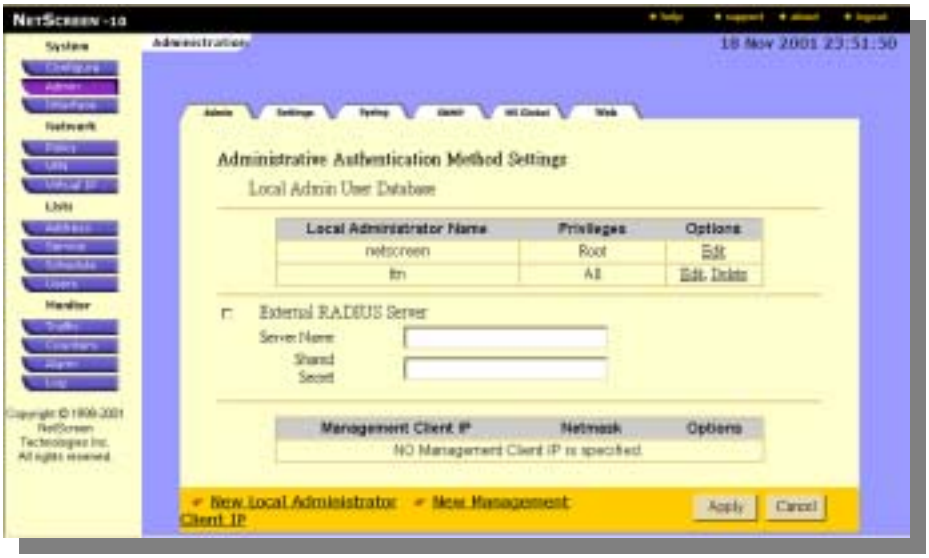



圖 FW system admin-00.jpg

Local Admin User Database：爲登綠使用者身分顯示區（root 爲最高使用權管理，原廠預設值 Login：netscreen，Password：netscreen），後面的 Edit 可以再編輯、Delete 爲撤除名稱。

（可在下面 New Local Administrator Client IP 新增使用者）參 P.9 頁

Extemal RADIUS Sever：設定外面使用者可登陸到內部。

Server Name：爲登陸名稱。

Shared Secret：設定登陸密碼。

（可在下面 New Management 增設登陸位址）參 P.8 頁

＊New Local Administrator Client IP 的環境說明


FW system admin-00-1.jpg

Name：登陸名稱。

New Password：密碼。

Confirm Password：確認密碼。

Privileges：ALL 完全控制、READ_ONLY 只容許讀取（瀏覽）。

＊ New Management 的環境說明

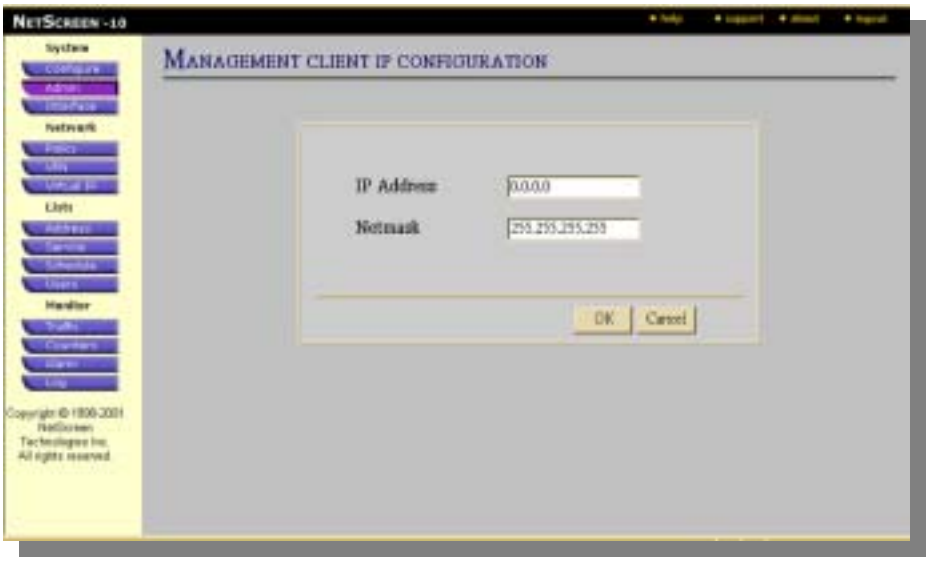



圖 FW system admin-00-2.jpg

IP Address：IP 位址。

Netmask：子網域位址。

2. Settings （工作環境設定）

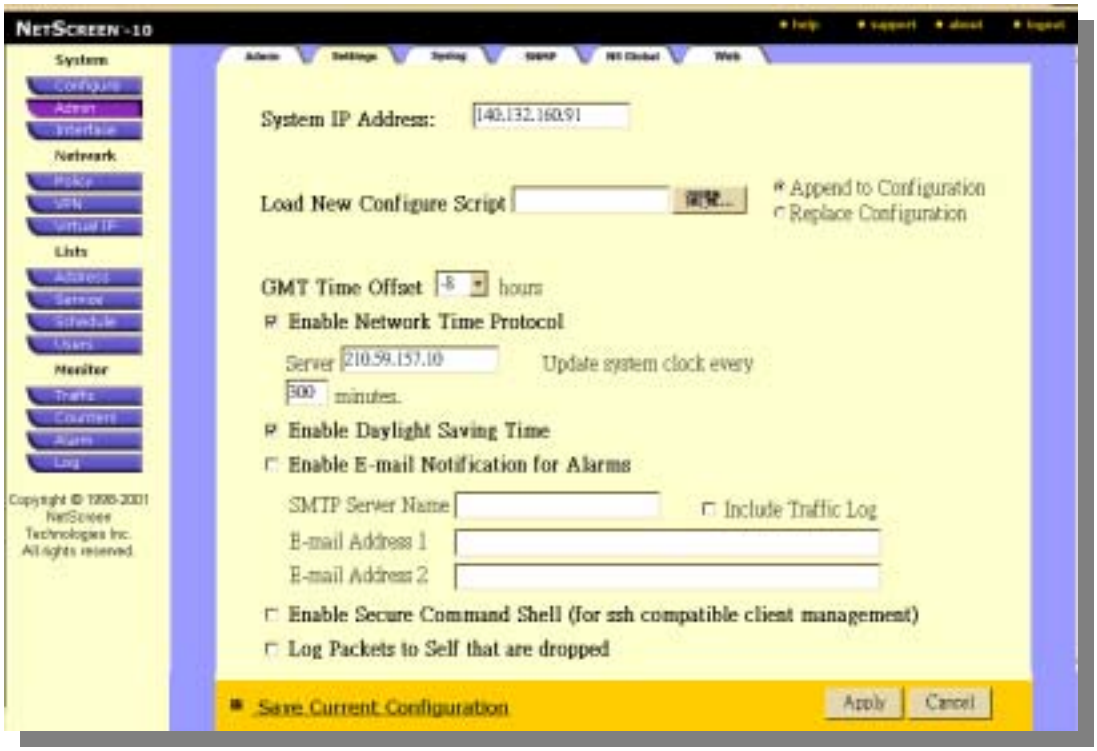



圖 FW system admin-01.jpg

System IP Address：公司內部瀏覽 F/W 設定的 IP 位址。（設定埠可參 P.14 頁）
**Load New Configure Script**　讀取所存 F/W 的參數
Append to Configuration：更新有所變更過的參數。
Replace Configuration：完全覆蓋所有變更過的參數。
GMT Time Offset：格林威治時間（台灣爲+8）。
Enable Network Time Protocol：國際電腦時間同步化。（建議勾選）
Sever Update system clock every：爲台灣政府 time sever 的 IP 所在位址。（210.59.157.10）
minutes：延遲時差。（建議 300）
Enable Daylight Saving Time：日光時間。（建議勾選）
Enable E-mail Notification for Alarms：F/W 一有狀況以 e-mail 使用管理員。
SMTP Server Name：外寄郵件 IP 位址。
Include Traffic Log：紀錄所有事件發生定將所發生存成 Log 檔寄給下方所設定的 e-mail address1 或 e-mail address2 管理人員。（建議不要勾選）
E-maill Address1：寄送郵件位址 1。
E-maill Address2：寄送郵件位址 2。
Enable Secure Command Shell（for ssh compatible client management）：若以 talnet 登錄需加解密。
Log Packets to Self that are dropped：紀錄安全封包。
Save Current Configuration：儲存目前 F/W 內部參數。

3. Syslog （系統 log 檔紀錄統計）必須而外購買 WebTrends 軟體

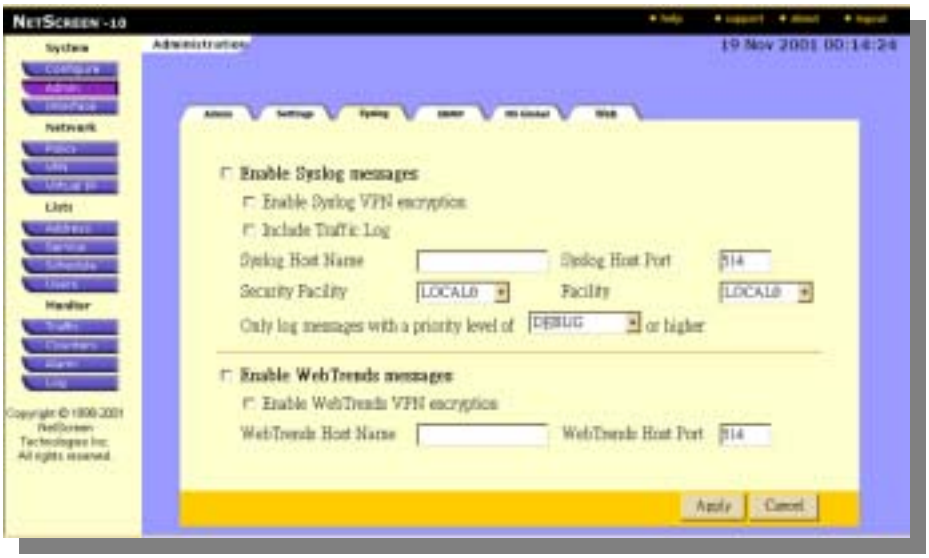



圖 FW system admin-02.jpg

**Enable Syslog messages：** 選擇登錄 Syslog 紀錄。
Enable Syslog VPN encryption：紀錄使用 VPN 通訊協定登錄。
Include Traffic Log：紀錄流量。
Syslog Host Name：登錄 Syslog 電腦名稱。
Syslog Host Port：登錄 Syslog 電腦的閘道。
Security Facility：安全機制共有 8 層。
Facility：登錄紀錄。
Only log messages with a priority level of：

**Enable WebTrends messages：**勾選使用 WebTrends 這一套網管軟體。(要另購)
Enable WebTrends VPN encryption：遠端使用 WebTrends 這一套網管軟體。
WebTrends Host Name：安裝 WebTrends 電腦 IP 位址。
WebTrends Host Port：安裝 WebTrends IP 位址所使用的通訊閘道。

PS:可到 http://www.kiwisyslog.com/index.htm 網站下載,Syslog 程式取代 WebTrends。

4. SNMP （網管分析）

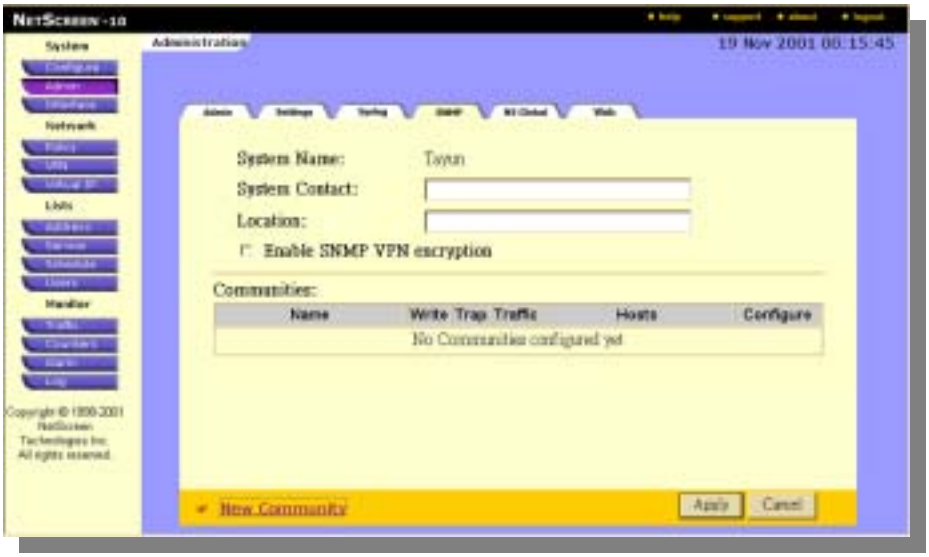



圖 FW system admin-03.jpg

System Name：

System Contact：

Location：

Enable SNMP VPN encryption：

New Community：

＊ New Community 的環境說明


圖 FW system admin-03-1.jpg

Community Name：Community 名稱。

Permissions:可勾選 Write 寫入、Trap 紀錄 、Including Traffic 。

Hosts：

5. NS Global （網管分析）其軟體要外購


圖 FW system admin-04.jpg

Enable Global Manager /PRO VPN encryption：

Enable Global Manager：

Server Name：

Server Configurtion（TCP）Port：

Server Reporting（UDP）Port：

Local Listening Port：

Enable Global PRO：

Primary IP Address：

Secondary IP Address：

Protocol Distribution：

Ethernet Statistics：

Attack Statistics：

Traffic Alarms：

Configuration Logs：

Traffic Logs：

Policy Statistics：

Flow Statistics：

Attack Alarms：

Event Alarms：

Information Logs：

Self Logs：

6. Web （設定登錄到 NetScreen 主畫面閘道）

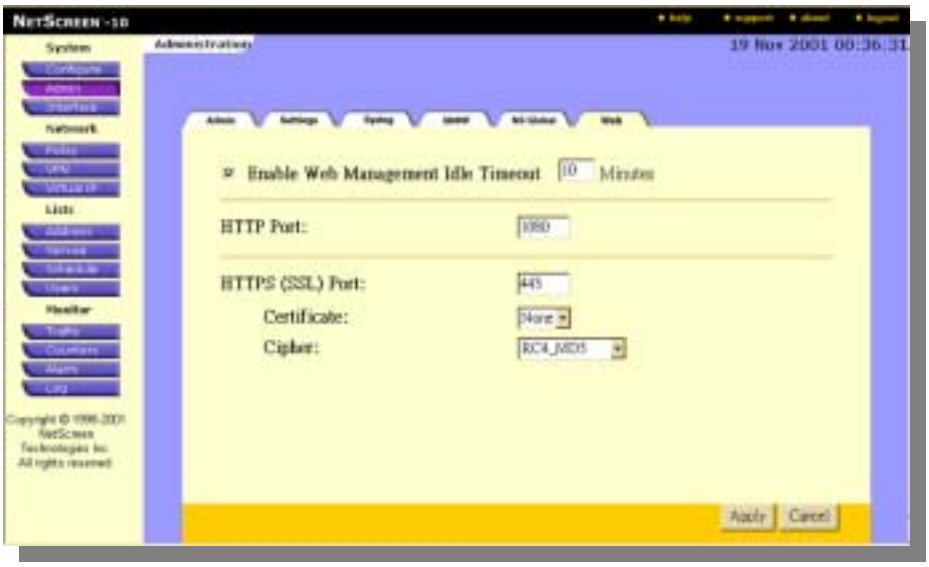



圖 FW system admin-05.jpg

Enable Web Management Idle Timeout：

HTTP Port：既爲在 system/Admin/Settings 下 System IP Address 位址的通訊埠。（區段爲 0-65535）

HTTPS（SSL）Port：加密通訊埠。

Certificate：

Cipher：加密格式。

三、Interface 做 F/W 的設定

1. Trusted （設定內部可信任 IP 對應位址）

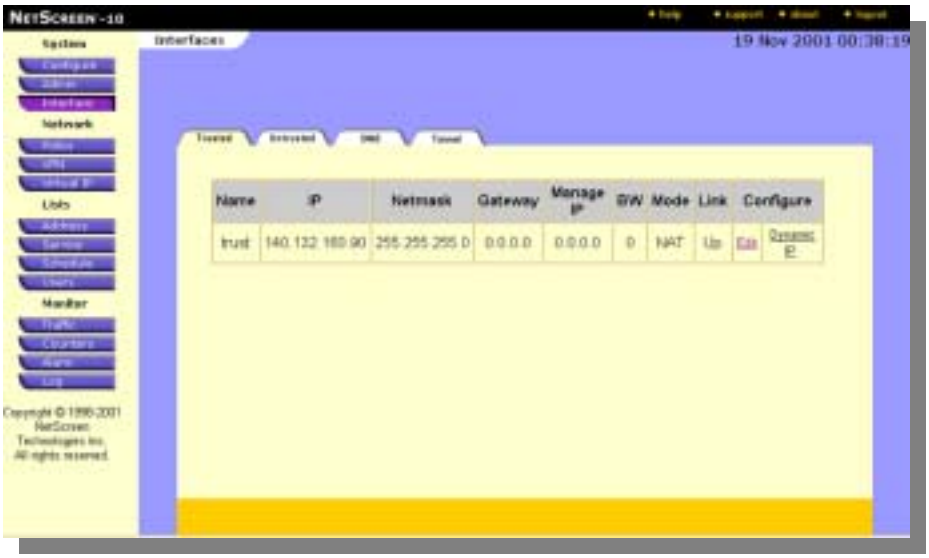



圖 FW system interface-00.jpg

Edit：編輯修改。（參 P.15 頁）

Dynamic IP ：內部員工經過 Tursted 到 Untursted 時在 Tursted 導通點產生一組動態

IP。（參 P.15 頁~P.16 頁）

＊ Edit 的環境說明


圖 FW system interface-00-1.jpg

IP Address：IP 位址。

Netmask：子網域。

Default Gateway：閘道。

Manage IP：Tursted 導通點位址。

Traffic Bandwidth：與許頻寬。

Interface Mode：當 NAT 爲虛擬網段、當 Route 爲路由網段。

**Management Services** 允許管理服務項目

SSL：加解密認證　　SCS：同 telnet 加密

NS-Global：NETSCREEN 加密　　SNMP：

NS-GlobalPRO：NETSCREEN 加密

**Other Service**：其他管理服務項目

＊ Dynamic IP Table 的環境說明


圖 FW system interface-00-2.jpg

New Entry：新增一個項目


圖 FW system interface-00-2-1.jpg

ID：編號。

**IP Address Range**

Start：動態 IP 起始位置。

End：動態 IP 起始結束。

**Port Translation**：是否任意變換。

2. Untrusted （設定外部可信任 IP 對應位址）


圖 FW system interface-01.jpg

Edit：編輯修改。（參 P.17 頁）

Mapped IP：設定合法 IP 對應內部非法 IP 位址。（參 P.17 頁~P.18 頁）

Dynamic IP：內部員工經由 Tursted 到 Untursted 時在 Untursted 導通點產生一組動態 IP。（參 P.18 頁~P.19 頁）

＊ Edit 的環境說明

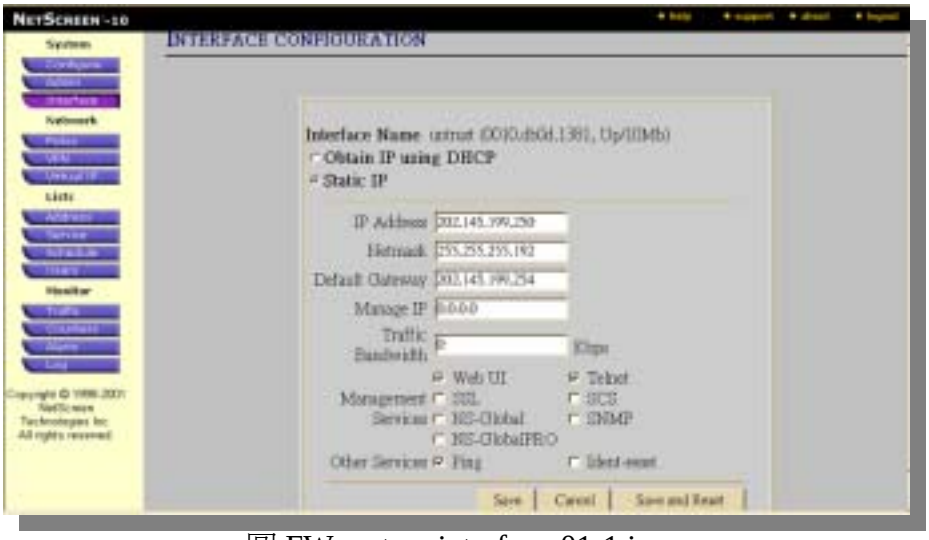



圖 FW system interface-01-1.jpg

**Obtain IP using DHCP**：動態 IP 環境設定

**Static IP**：靜態 IP 環境設定

IP Address：IP 位址。

Netmask：子網域。

Default Gateway：閘道。

Manage IP：Untrusted 導通點位址。

Traffic Bandwidth：與許頻寬。

**Management Services** 允許管理服務項目

Web UI：WEB 通訊協並　　Telnet：telnet 通訊協定

SSL：加解密認證　　SCS：同 telnet 加密

NS-Global：NETSCREEN 加密　　SNMP：

NS-GlobalPRO：NETSCREEN 加密

Other Service：其他服務項目。

＊ Mapped IP 的環境說明


圖 FW system interface-01-2.jpg

可點選 New Entry 增加一個新的 Mapped IP

New Entry：


圖 FW system interface-01-2-1g

Mapped IP Address：合法 IP 位址。

Netmask：子網域。

Host IP Address：所對應的非法 IP 位址。

＊ Dynamic IP 的環境說明


圖 FW system interface-01-3.jpg

可點選 New Entry 增加一個新的 Dynamic IP

New Entry：

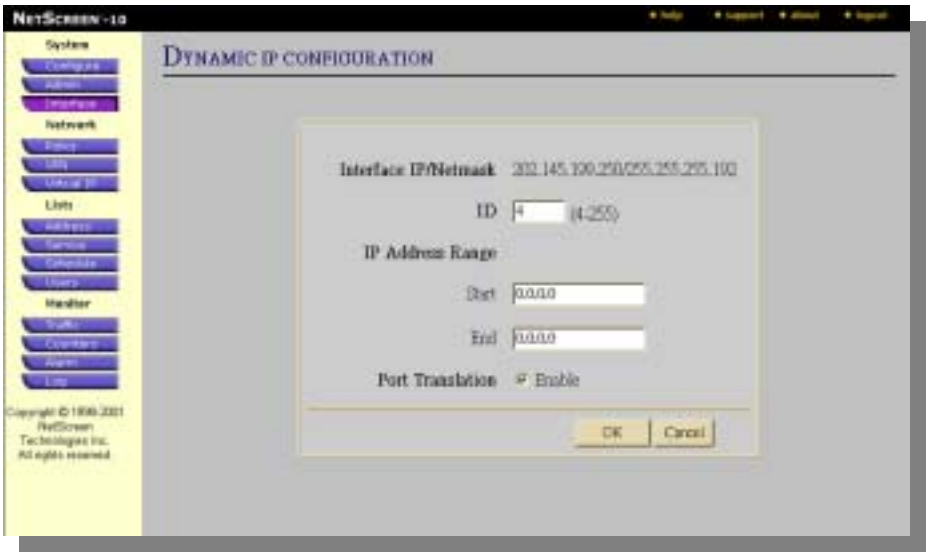



圖 FW system interface-01-3-1.jpg

ID：編號

**IP Address Range**

Stat：動態 IP 起始位置。

End：動態 IP 起始結束。

**Port Translation**：是否任意變換。

3. DMZ （設定攻防區對應位址）

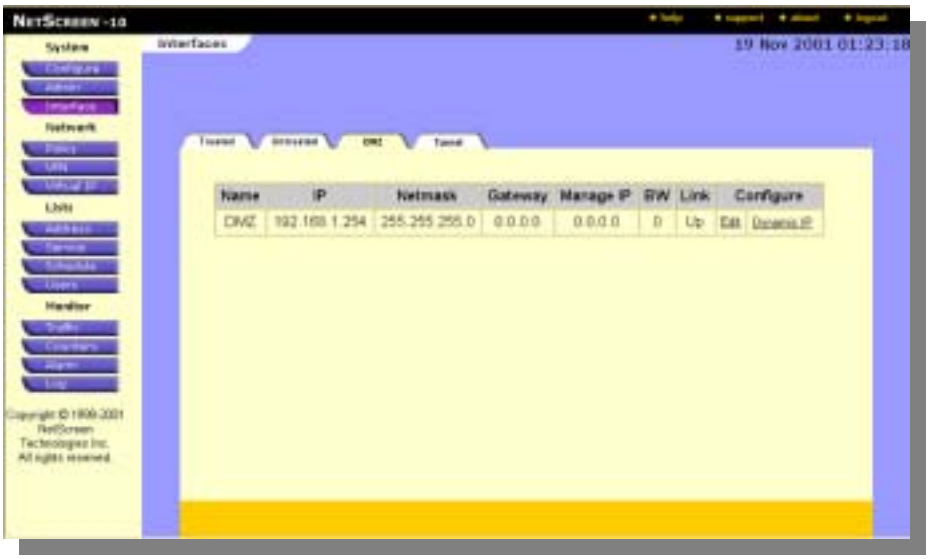



圖 FW system interface-02.jpg

Edit：編輯修改。（參 P.20 頁）

Dynamic IP：內部員工經由 Tursted 到 DMZ 時，在 DMZ 導通點產生一組動態 IP。（參 P.20 頁~P.21 頁）

＊ Edit 的環境說明

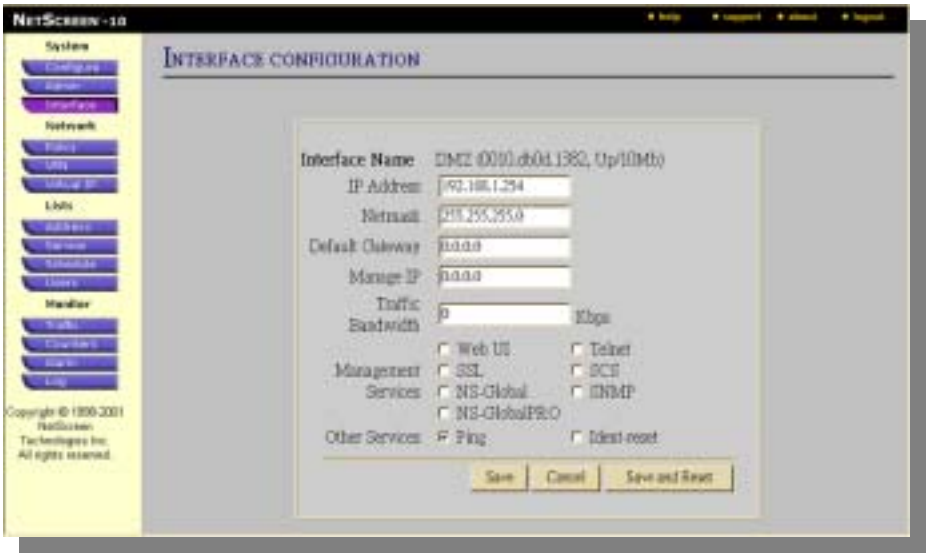



圖 FW system interface-02-1.jpg

IP Address：DMZ 非戰區所指定 IP 位址。

Netmask：DMZ 非戰區所指定 IP 子網域位址。

Default Gatway：DMZ 非戰區所指定通訊閘道。

Mange IP：DMZ 導通點位址。

Traffic Bandwidth：與許頻寬。

Management Services 允許管理服務項目

Web UI：Web 通訊協定　　Telnet：telnet 通訊協定

SSL：加解密認證　　SCS：同 telnet 加密

NS-Global：NETSCREEN 加密　　SNMP：

NS-GlobalPRO：NETSCREEN 加密

Other Services 允許管理服務項目

Ping：ping 通訊協定　　Ident-rest：同 proxy 加密

＊ Dynamic IP 的環境說明

FW system interface-02-2.jpg

可點選 New Entry 增加一個新的 Dynamic IP

＊New Entry

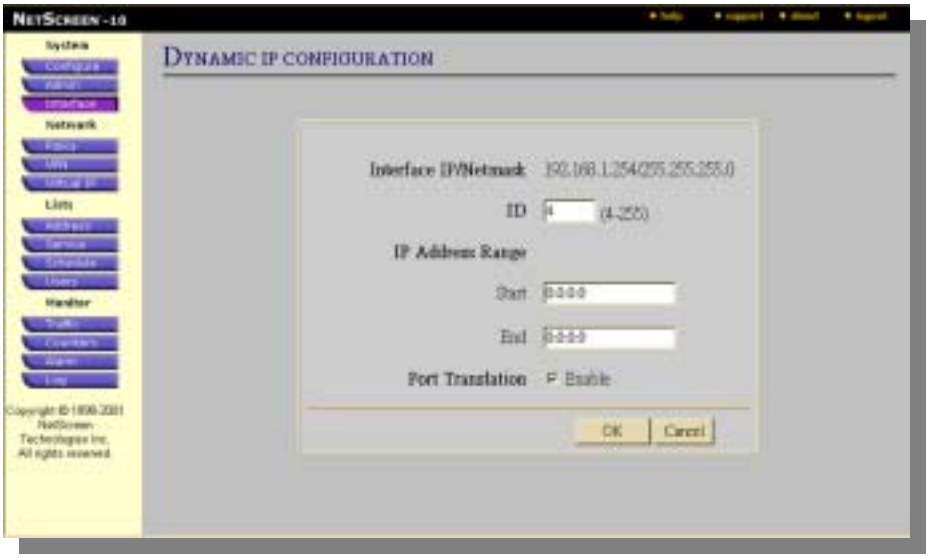



圖 FW system interface-02-2-1.jpg

ID：編號

**IP Address Range**

Stat：動態 IP 起始位置。

End：動態 IP 起始結束。

**Port Translation**：是否任意變換。

4. Tunnel （建立通道）

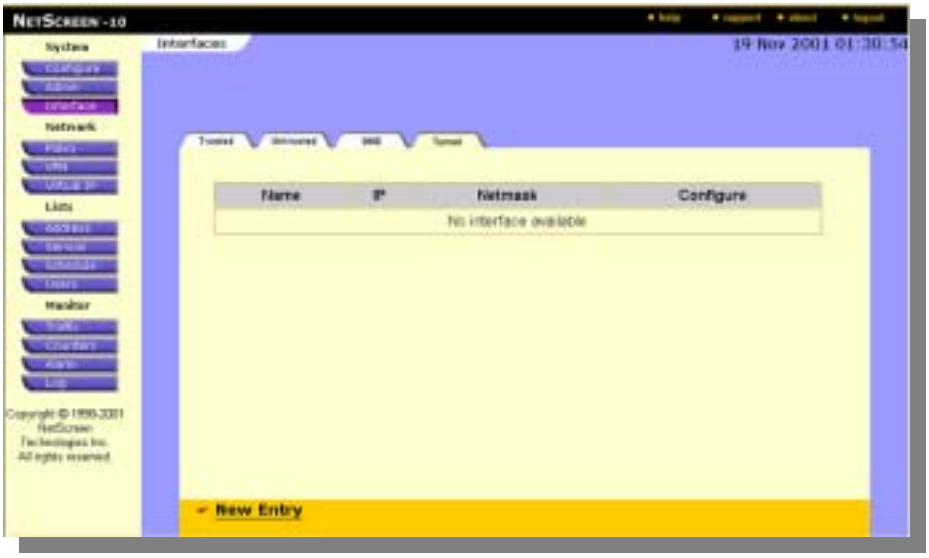



圖 FW system interface-03.jpg

可點選 New Entry 增加一個新的 Tunnel IP

＊New Entry：


圖 FW system interface-03-1.jpg

Interface Name：開放通道編號。

IP Address：開放通道 IP。

Netmask：開放通道子網域位址。

- Network （網路設定）

一、Policy　區域環境方針

1. Incoming （由 Untrusted 區域到 Trusted 區域）

PS：可在 Lists\Address 內先行設定位置在加入。（參 P.39 頁）


圖 FW network policy-00.jpg

可點選 New Entry 增加一個新的 Incoming

＊New Entry：

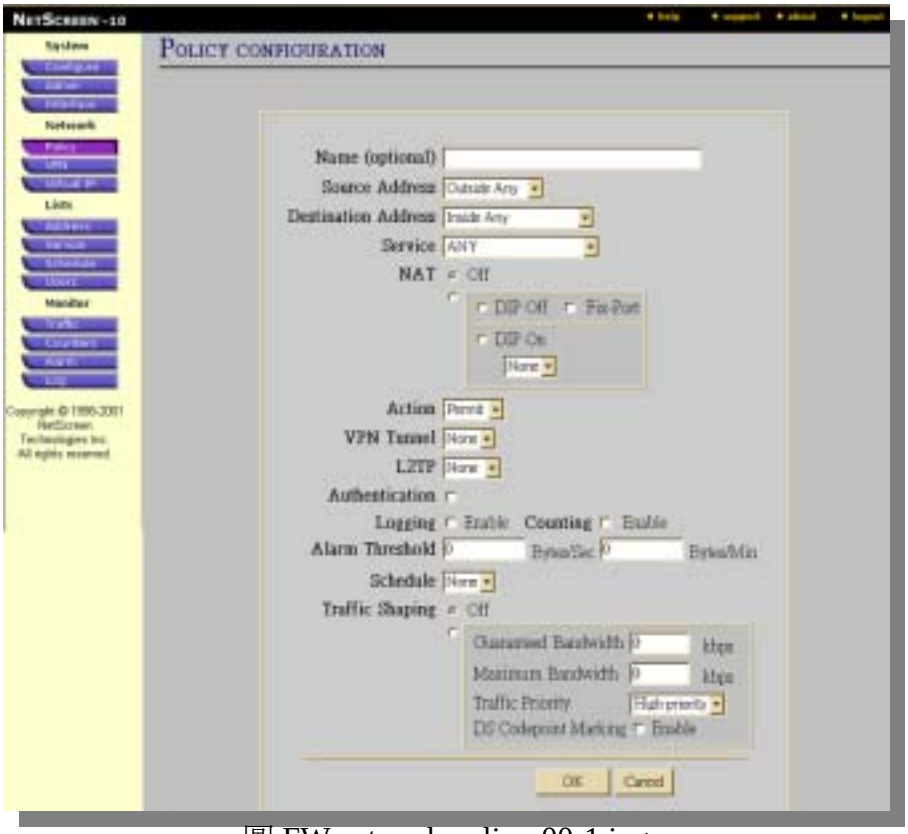



圖 FW network policy-00-1.jpg

**Name（optional）**：項目名稱。
**Source Address**：來源端（其選項可在 Lists\Address\Untrusted 新增供選擇）。
**Destination Address**：目的端。
**Service**：服務項目（內部選項可在 Lists\Service\Custom 新增供選擇）。
**NAT**
off：
Dip off：　　Fix Port：
Dip on：
**Action**：工作方式（Permit 許可、Deny 不允許、Tunnel 通道）。
**VPN Tunnel**：使用 VPN 通訊協定。
**L2TP**：當的一種；如同 PPPTP 通訊協定。
**Authentication**：再次確認 ID 與 Password。
**Logging**：事件紀錄。　　**Cunting**：連線頻寬紀錄
**Alarm Threshold**：當流量（封包）到達一數值做警訊（可選以秒或以分）。
**Schedule**：允許時段（內部選項可在 Lists\ Schedule 新增供選擇）參 P.46 頁。
**Traffic Shaping**
off：不做限制。
Guaranteed Bandwidth：保證最低頻寬。
Maximum Bandwidth：最大頻寬。
**Traffic Priority**：等級。
DiffServ Codepoint Marking：安全機制。

2. Outgoing（由 Trusted 區域到 Untrusted 區域）

PS：可在 Lists\Address 內先行設定位置在加入。（參 P.39 頁）

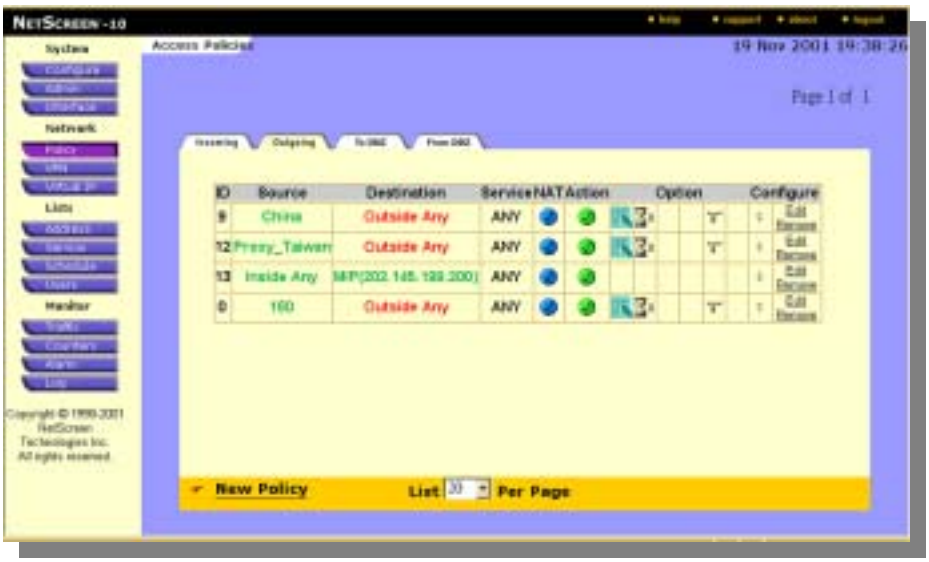



圖 FW network policy-01.jpg

可點選 New Entry 增加一個新的 Outgoing

New Entry：

設定方式和（圖 FW network policy-00-1.jpg）一樣。

3. To DMZ （由 Trusted 區域或 Untrusted 區域到 DMZ 區域）

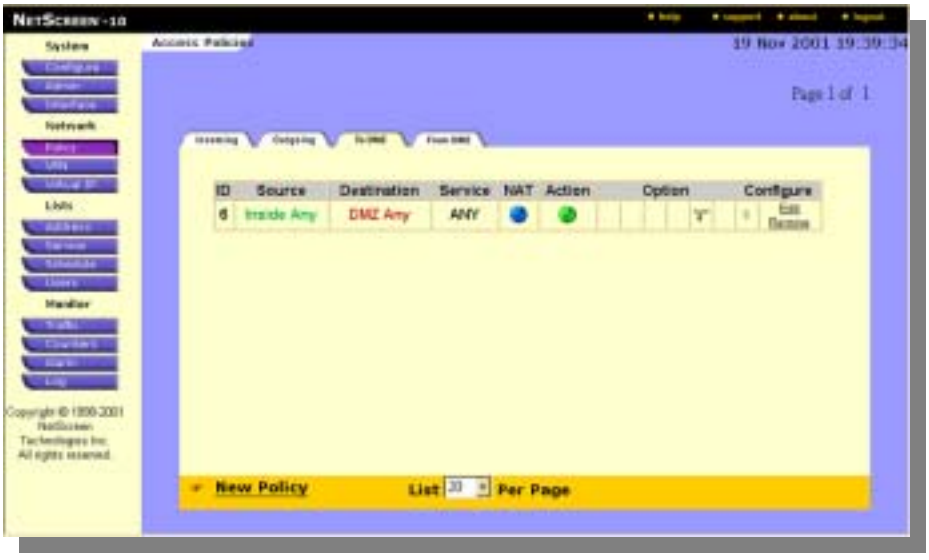



圖 FW network policy-02.jpg

可點選 New Entry 增加一個新的 To DMZ

New Entry：

設定方式和（圖 FW network policy-00-1.jpg）一樣。

4. From DMZ（由 DMZ 區域到 Trusted 區域或 Untrusted 區域）

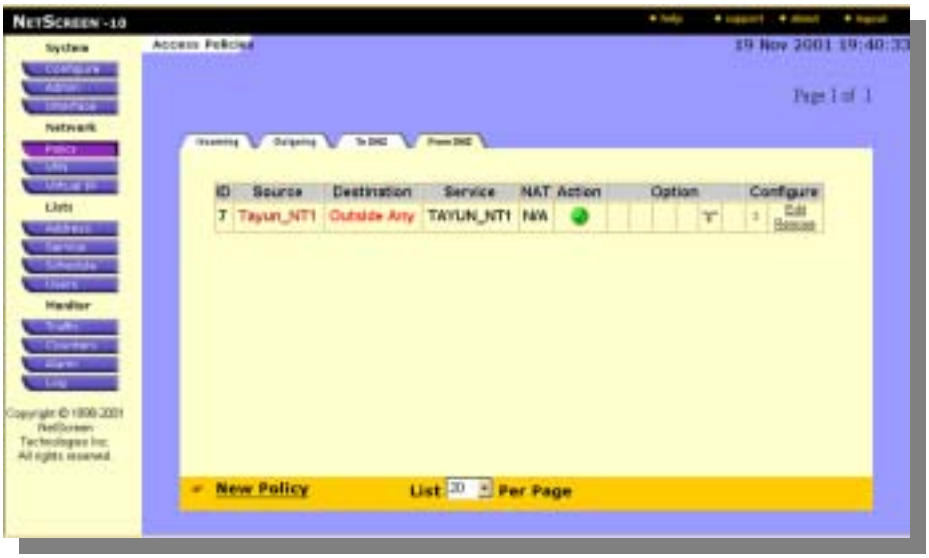



圖 FW network policy-03.jpg

可點選 New Entry 增加一個新的 From DMZ

New Entry：

設定方式和（圖 FW network policy-00-1.jpg）一樣。

二、VPN 主要功能爲當人員在外地，需使用公司電腦資源的設定介面

1. Manual Key


圖 FW network vpn-00.jpg

可點選 New Manual Key Entry 增加一個新的 Manual Key

＊New Manual Key Entry：

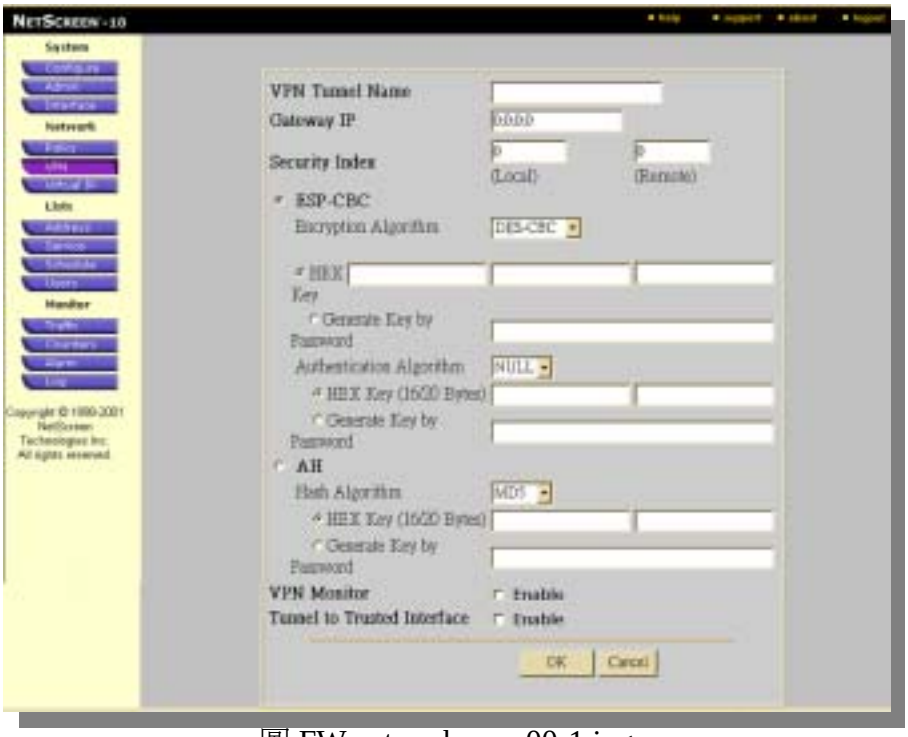



圖 FW network vpn-00-1.jpg

**VPN Tunnel Name**：

**Gateway IP**：

**Security Index**：當 Local 爲　　；當 Remote 爲　　。

**ESP-CBC**：

Encryption Algorithm

選 NULL：　　選 BES-CBC：　　選 3DES-CBC：

HEX：

Generate Key by Password：

Authentication Algorithm

選 NULL：　　選 MD5：　　選 SHA1：

HEX Key （16/20Bytes）：

Generate Key by Password：

AH：

Hash Algorithm

選 MD5：　　選 SHA1：

HEX Key（16/20Bytes）：

Generate Key by Password：

VPN Monitor：

Tunnel to trusted Interface：

2. AutoKey IKE


圖 FW network vpn-01.jpg

可點選 New AutoKey IKE Entry 增加一個新的 AutoKey IKE

＊New AutoKey IKE Entry：

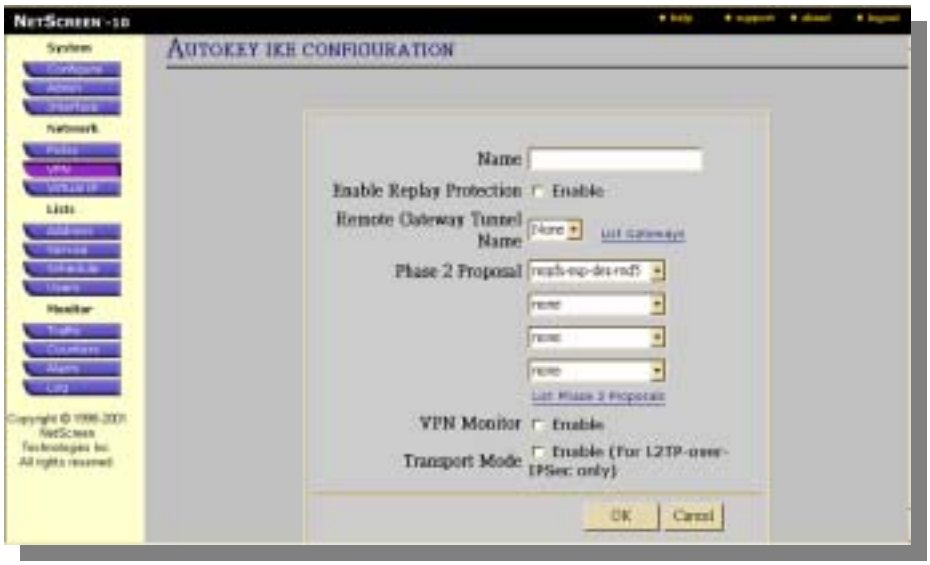



圖 FW network vpn-01-1.jpg

**Name**：

**Enable Repay Protection**：

**Remote Gateway Tunnel Name**：

List Gateways：直接跳到（Network\VPN\Gateway 畫面；圖 FW network vpn-02.jpg）

**Phase 2 Proposal** 下拉選單

Nonfs-esp-des-md5：
Nopfs-esp-des-sha：
Nopfs-esp-des-md5：
Nopfs-esp-3des-md5：
Nopfs-esp-3des-sha：
G2-esp-des-md5：
G2-esp-des-sha：
G2-esp-3des-md5：

G2-esp-3des-sha：

List Phae 2 Proposals：直接跳到（Network\VPN\P2 Proposals 畫面；圖 FW network vpn-04.jpg）

**VPN Monitor**：

**Transport Mode**：

3. Gateway


圖 FW network vpn-02.jpg

可點選 New Remote Tunnel Gateway 增加一個新的 Gateway

＊New Remote Tunnel Gateway：

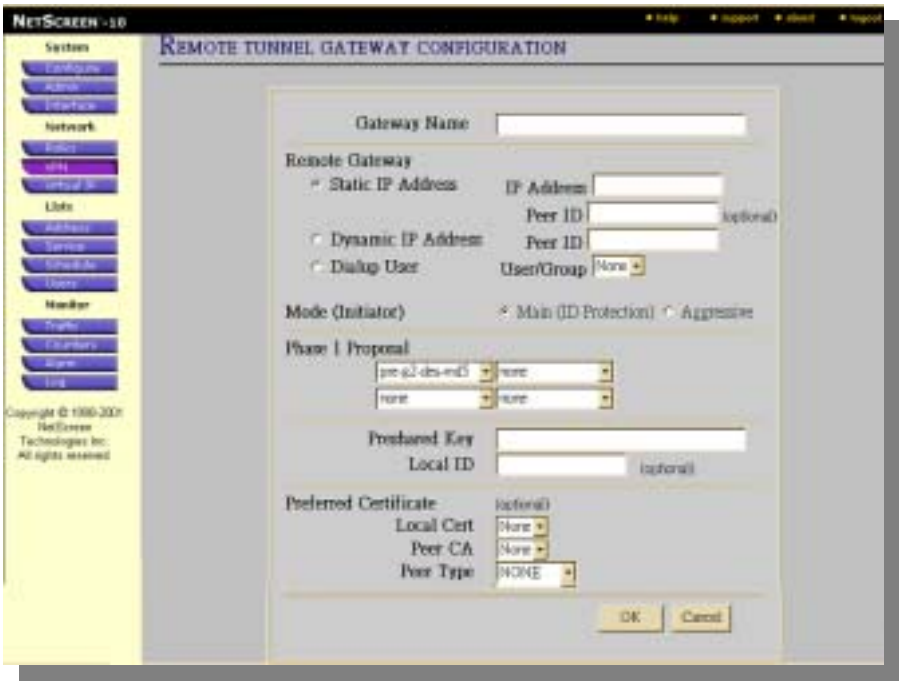



圖 FW network vpn-02-1.jpg

**Gateway Name**：Gateway 的名稱

**Remote Gateway**

Static IP Address：　　IP Address：

Dynamic IP Address：　　Peer ID（optional）：

Dialup User：　　Peer ID：

　　User/Group：

**Mode（Initiator）**

Main（ID protection）：　　Aggressive：

**Phase 1 Proposal：**

**Preshared Key：**（不可低於 8 的字）

**Local ID：**

**Preferred Certificate**

Local Cert：

Peer CA：

Peer Type：

4. P1 Proposal

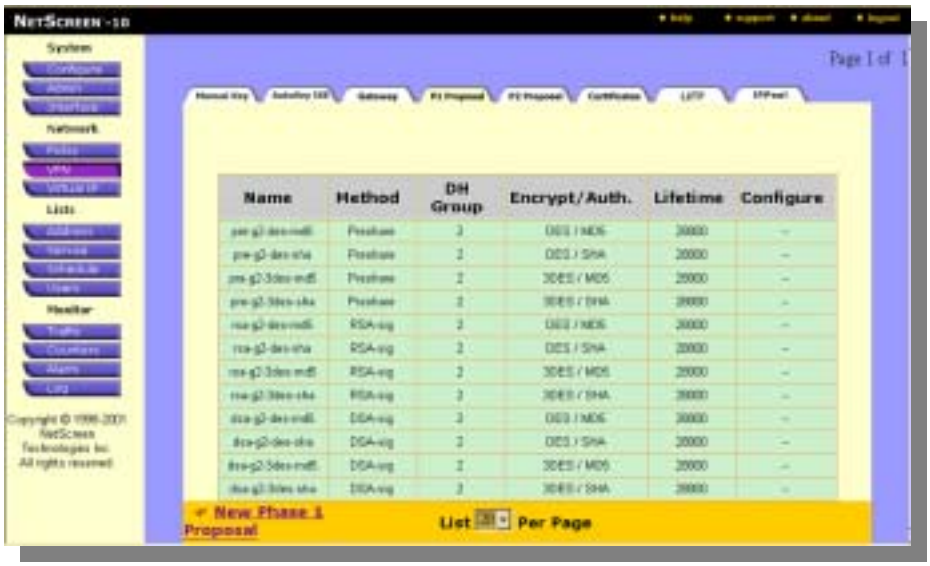



圖 FW network policy-03.jpg

可點選 New Phase 1 Proposal 增加一個新的 P1 Proposal

＊New Phase 1 Proposal：


圖 FW network vpn-03-1.jpg

**Name**：名稱

**Authentication Method**

Preshare：　　DSA-Signature：

RSA-Signature：

**DH Group**

Group1：　　Group3：

Group2：

**Encryption＆Data Intergrity**

**Encryption Algorithm**

DES-CBC：　　3DES-CBC：

**Hash Algorithm**

MD5：　　SHA-1：

下方 8 數字：

**Lifetime**：

Sec：秒　　Hours：小時

Min：分　　Day：天

5. P2 Proposal


圖 FW network vpn-04.jpg

可點選 New Phase 2 Proposal 增加一個新的 P2 Proposal

＊New Phase 2 Proposal：

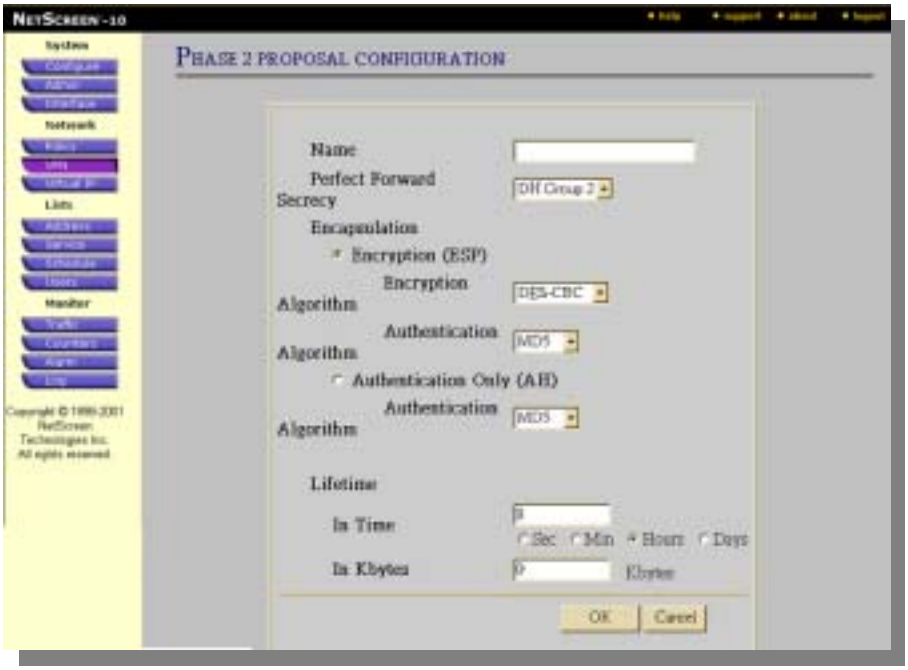



圖 FW network vpn-04-1.jpg

**Name**：

**Perfect Forward Secrecy**

NO-PFS：　　DH Grop2：

DH Grop1：　　DH Grop5：

**Encryption（ESP）**：

**Encryption**

NULL：　　DES-CBC：

3D-CBC：

**Authentication**

NONE：　　SHA-1：

MD5：

**Authentication Only（AH）**：

**Authentication**

MD5：　　SHA-1：

**In Time**：

Sec：秒　　Hours：小時

Min：分　　Days：天

**InKbytes**：

6. Certificates

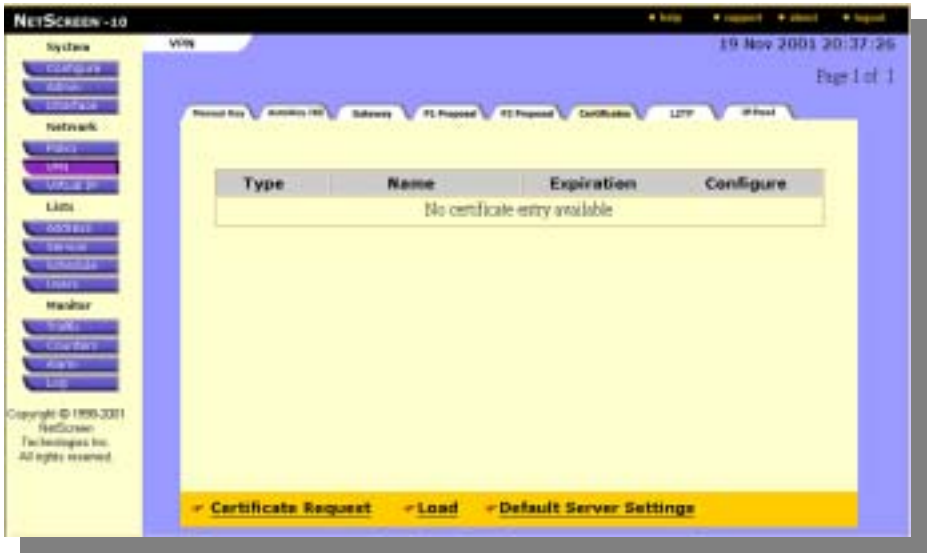



圖 FW network vpn-05.jpg

可點選 Certificate Request 增加一個新的 Certificates（圖 FW network vpn-05-1.jpg）

可點選 Load 讀取所紀錄的 Certificates（圖 FW network vpn-05-2.jpg）

可點選 Default Server Settings 設定一原定質（圖 FW network vpn-05-3.jpg）

＊Certificate Request：


圖 FW network vpn-05-1.jpg

Name：

Phone：

Unit/Department：

Organization：

County/Locality：

State：

Country：

E-mail：

IP Address：

Write Request File To

E-mail to：

Write to file：

RSA：　　DSA：

Create new key pair of：

＊Load：

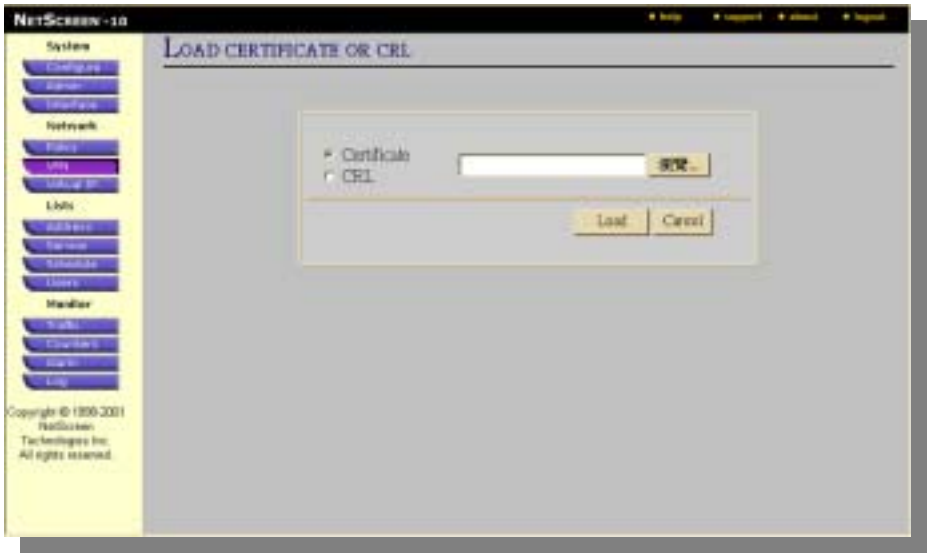



圖 FW network vpn-05-2.jpg

Certificate：

CRL：

＊Default Server Settings：

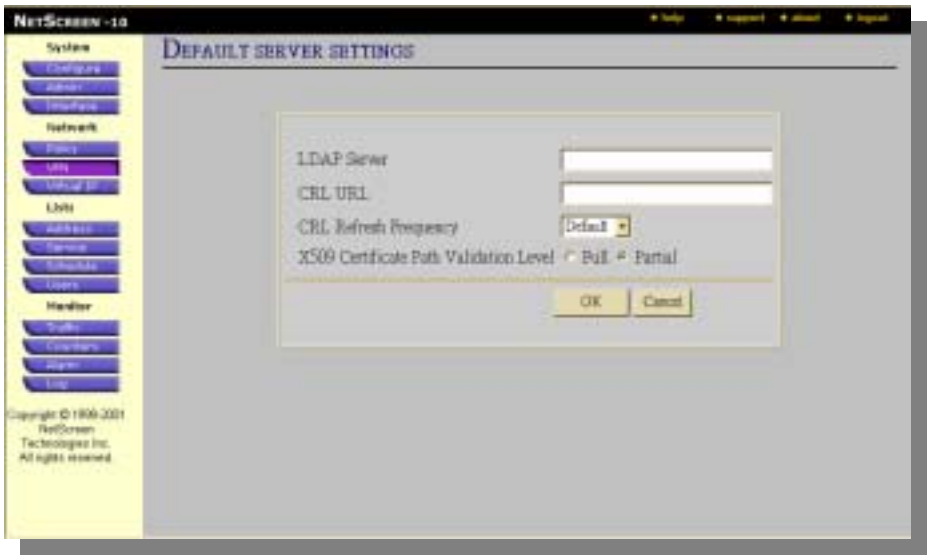



圖 FW network vpn-05-3jpg

LDAP Server：

CRL URL：

CRL Refresh Frequency

Default：　　Weekly：

Daily：　　Monthly：

X509 Cerificate Path Validation Level

Full：　　Partial：

7. L2TP


圖 FW network vpn-06.jpg

可點選 New L2TP Tunnel 增加一個新的 L2TP

＊New L2TP Tunnel：

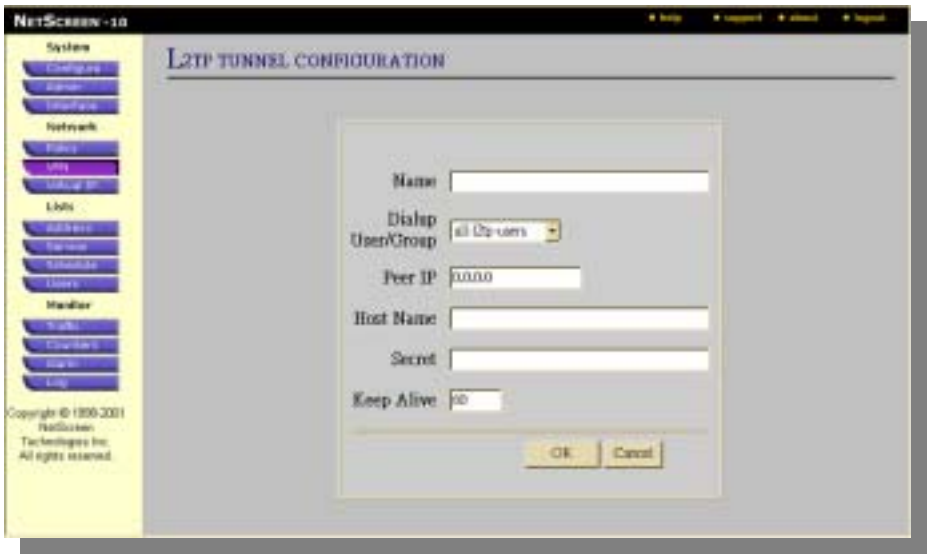



圖 FW network vpn-06-1.jpg

**Name**：

**Dialup User/Group**：

**Peer IP**：

**Host Name**：

**Secret**：

**Keep Alive**：

8. IPPool


圖 FW network vpn-07.jpg

可點選 New IPPooL 增加一個新的 IPPool

＊New IPPooL：

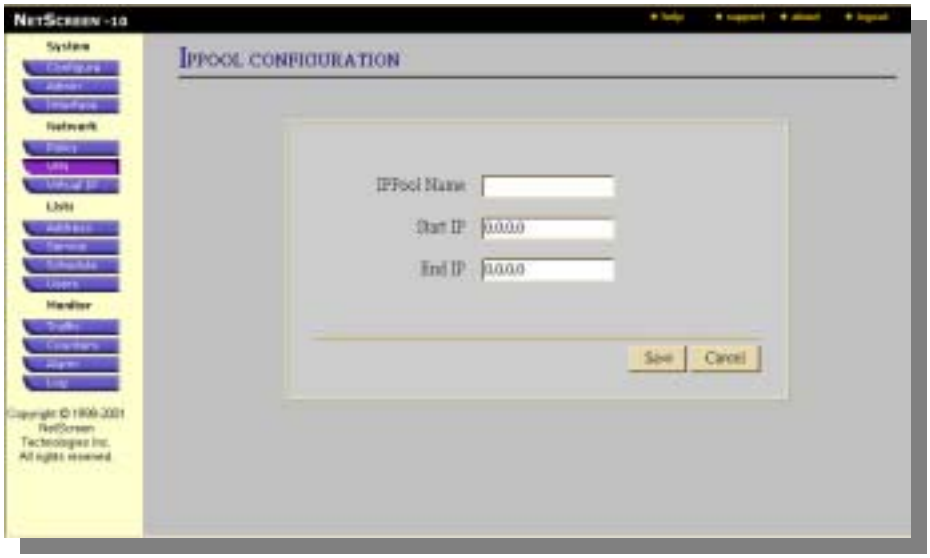



圖 FW network vpn-07-1.jpg

IPPool Name：名稱

Start IP：開始 IP 位址

End IP：結束 IP 位址

三、Virtual IP 主要功能爲當多數人員在外地，需使用公司電腦資源的設定介面
（由外部 Untrusted 到內部 Trusted 時使用 port 埠加以做分類，連接到內部電腦）
如
http://202.132.100.1：80 → 192.168.1.1
http://202.132.100.1：81 → 192.168.1.2
http://202.132.100.1：83 → 192.168.1.10

1. Virtual IP1 （第一組 Virtual IP）

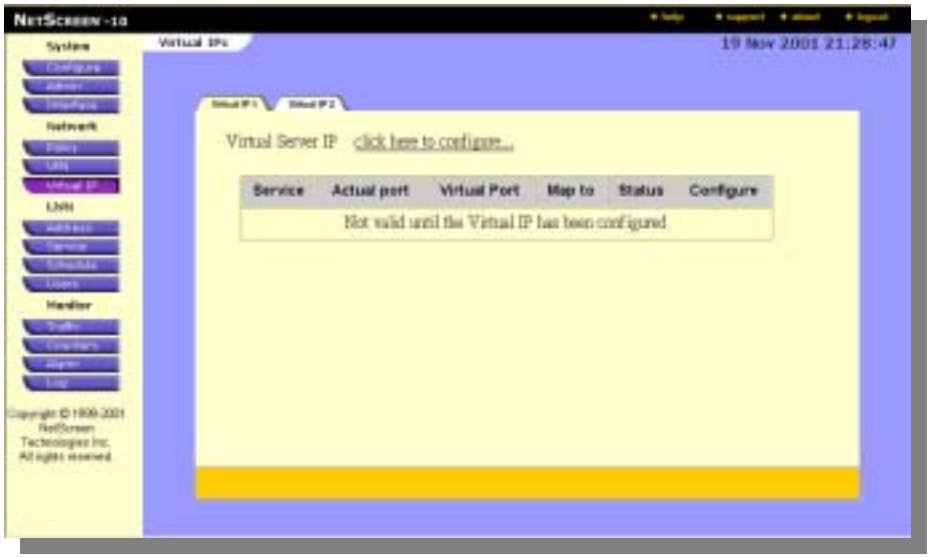



圖 FW network virtual ip-00.jpg

＊可點選 click here to configure 增加一個新的 Virtual IP1

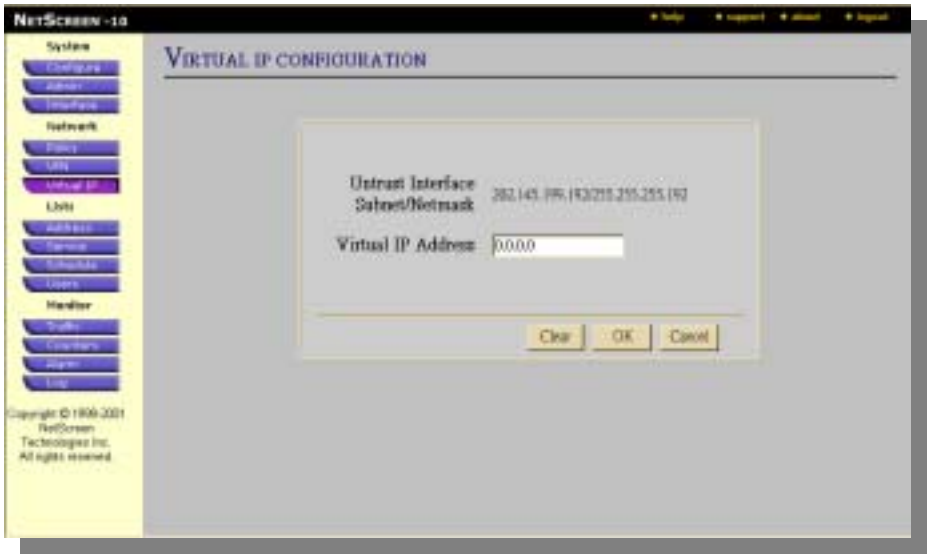



圖 FW network virtual ip-00-1.jpg

**Untrust Interface Subnet/Netmask**
**Virtual IP Address**：設定一個合法 IP。

2. Virtual IP2 （第二組 Virtual IP）

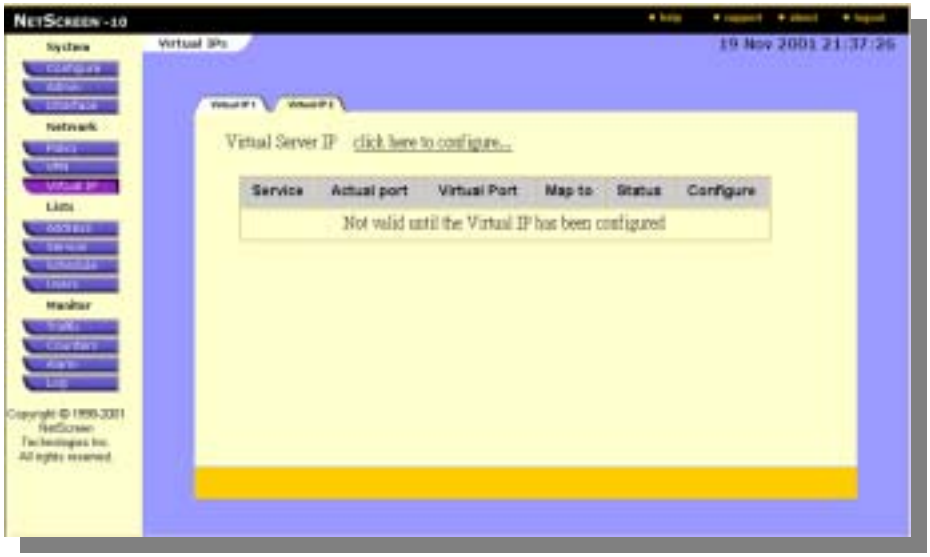



圖 FW network virtual ip-01.jpg

可點選 click here to configure 增加一個新的 Virtual IP2

＊click here to configure：

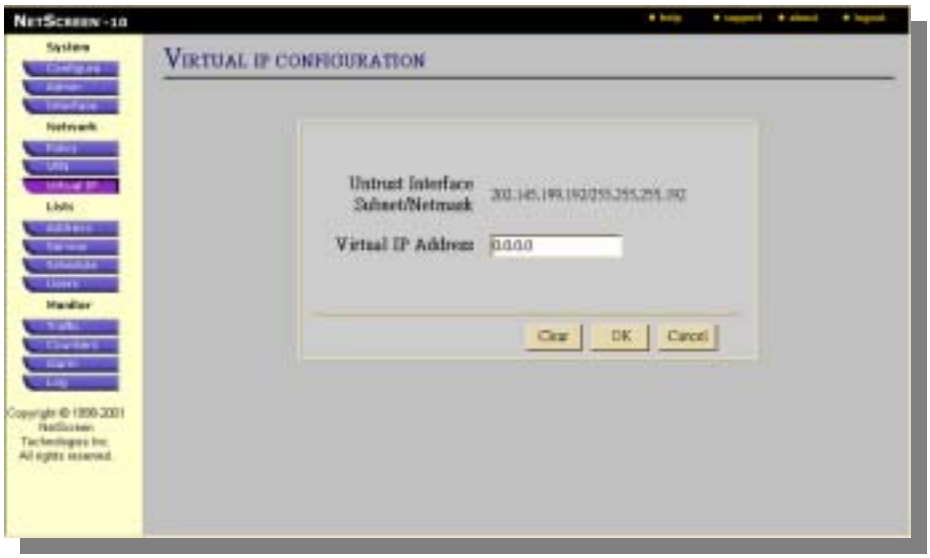



圖 FW network virtual ip-01-1.jpg

**Untrust Interface Subnet/Netmask**

**Virtual IP Address**：設定一個合法 IP。

- Lists （個別性的設定）

一、Address 定義各細項供 Network\Policy 訂定使用

1. Trusted （內部信任選項）

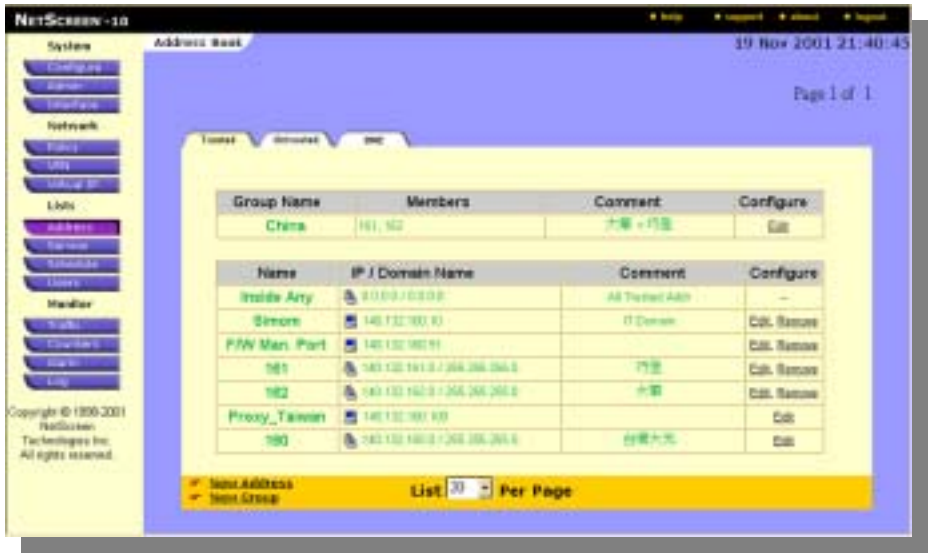



圖 FW lists addredd-00.jpg

可點選 New Address 增加一個新的 Trusted 項目（圖 FW lists addredd-00-1.jpg）
可點選 New Group 增加一個新的 Trusted 項目群組（圖 FW lists addredd-00-2.jpg）

＊New Address：

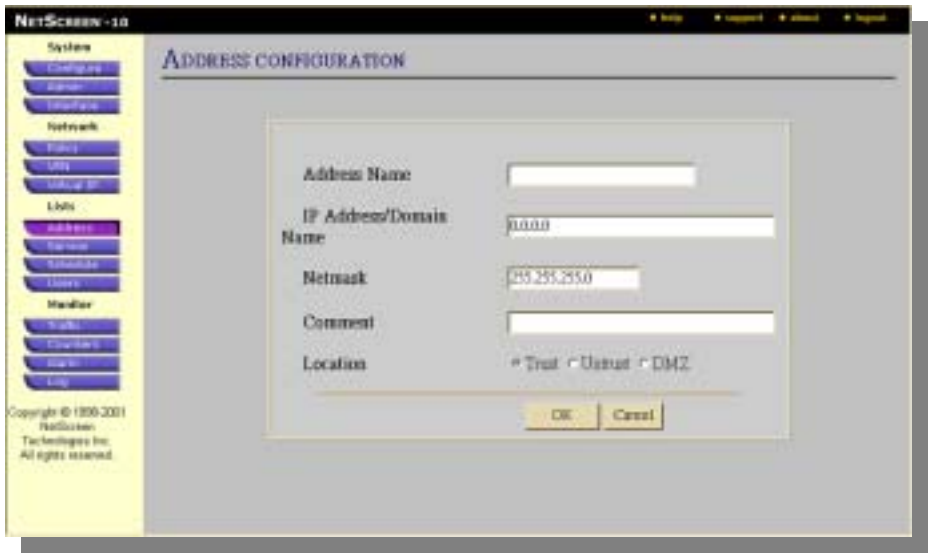



圖 FW lists addredd-00-1.jpg

**Address Name**：項目名稱。

**IP Address/Domain Name**：內部信任的 IP 位址。

**Netmask**：內部信任的子網域位址。

**Comment**：備說明註欄。

**Location** 將所要定義的 IP 放置於何區域裡。（預設值爲所定義的 Trust 區域爲區域）

Trust： Untrust：

DMZ：

＊New Group：


圖 FW lists addredd-00-2.jpg

**Group Name**：項目群組名稱。

**Comment**：備註說明欄。

左方塊：定義群組選項

右方塊：New Address 增加一個新的 Trusted 項目

2. Untrusted （外部信任選項）

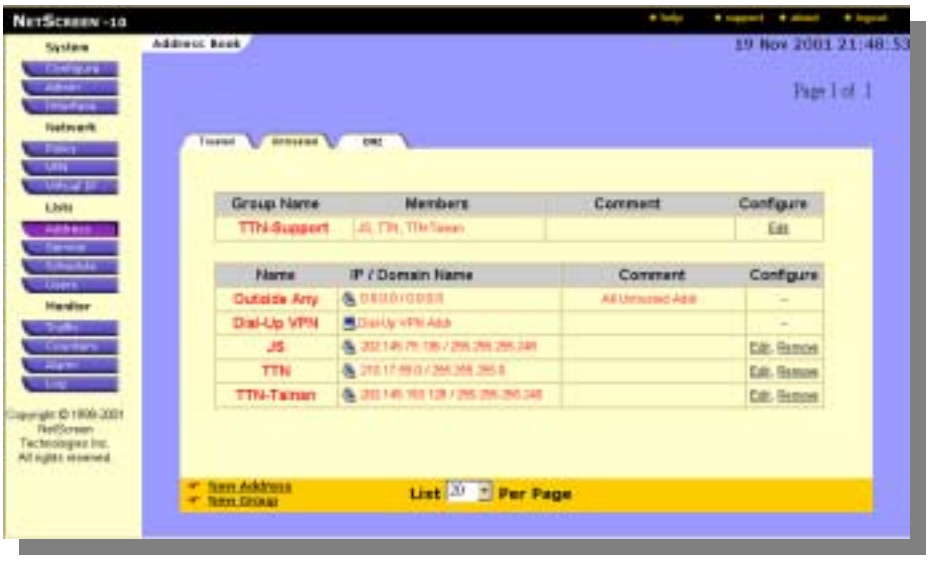



圖 FW lists addredd-01.jpg

可點選 New Address 增加一個新的 Untrusted 項目（圖 FW lists addredd-01-1.jpg）

可點選 New Group 增加一個新的 Untrusted 項目群組（圖 FW lists addredd-01-2.jpg）

＊New Address：

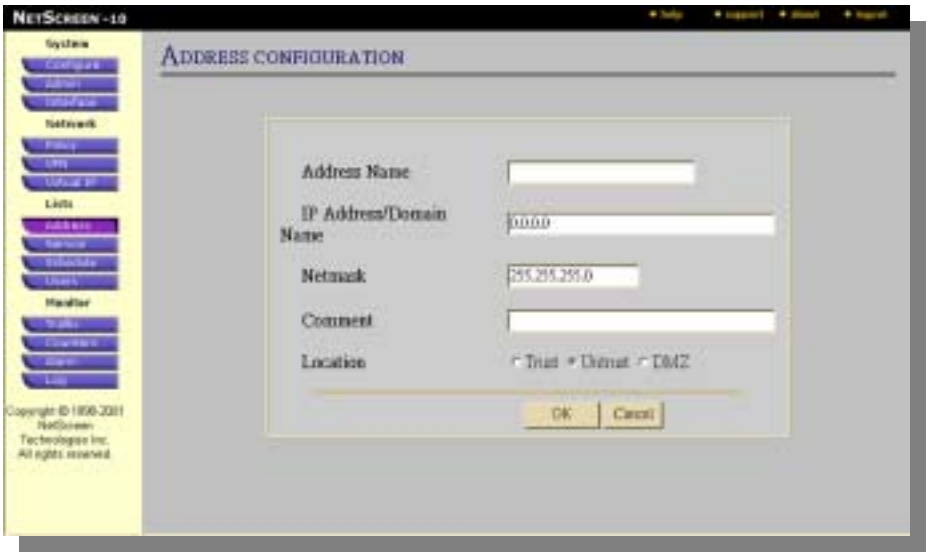



圖 FW lists addredd-01-1.jpg

**Address Name**：項目名稱。
**IP Address/Domain Name**：外部信任的 IP 位址。
**Netmask**：外部信任的子網域位位址。
**Comment**：備註說明欄。
**Location** 將所要定義的 IP 放置於何區域裡。（預設值爲所定義的 Untrust 區域爲區域）
Trust：　　DMZ：
Untrust：

＊New Group：

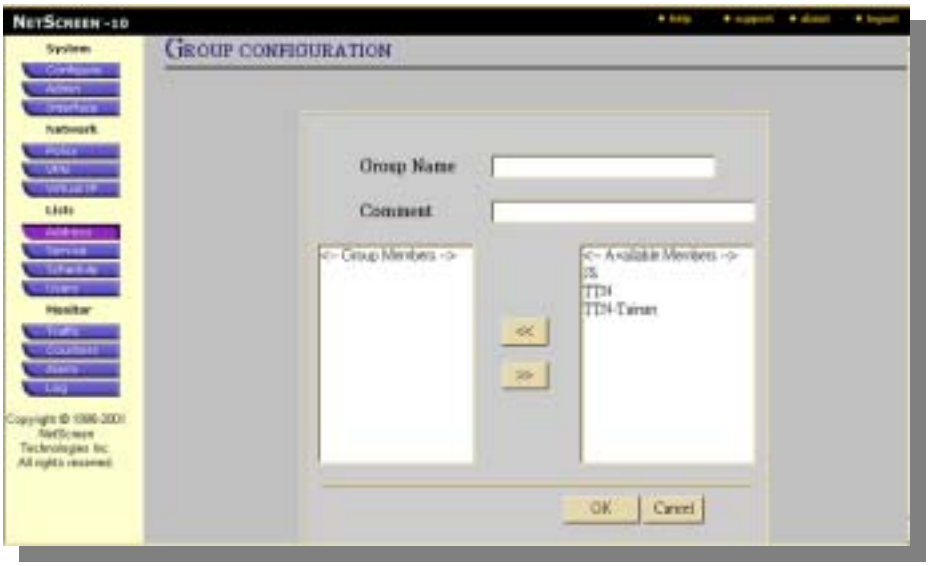



圖 FW lists addredd-01-2.jpg

**Group Name**：項目群組名稱。
**Comment**：備註說明欄。
左方塊：定義群組選項

右方塊：New Address 增加一個新的 Untrusted 項目

3. DMZ （攻防區選項）

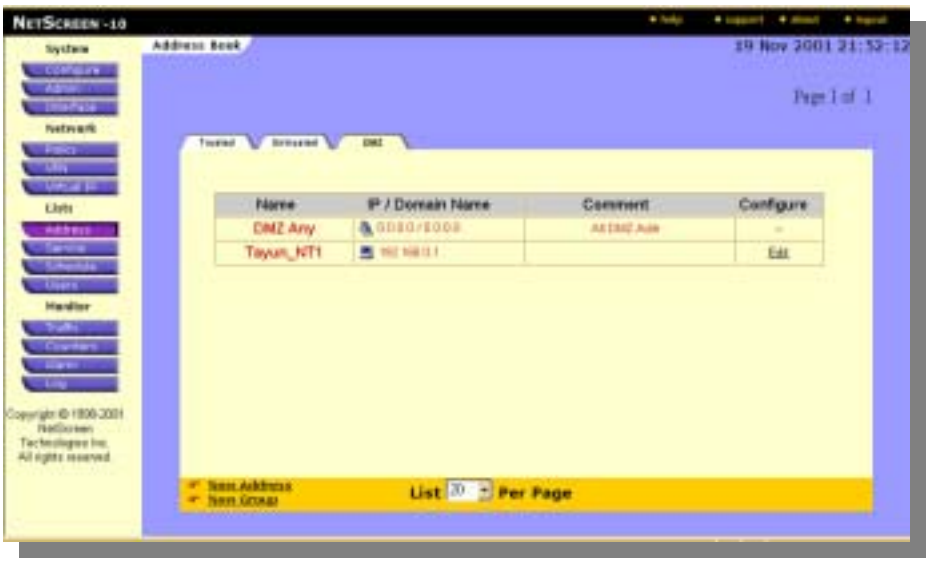



圖 FW lists addredd-02.jpg

可點選 New Address 增加一個新的 DMZ 項目（圖 FW lists addredd-02-1.jpg）

可點選 New Group 增加一個新的 DMZ 項目群組（圖 FW lists addredd-02-2.jpg）

＊New Address：

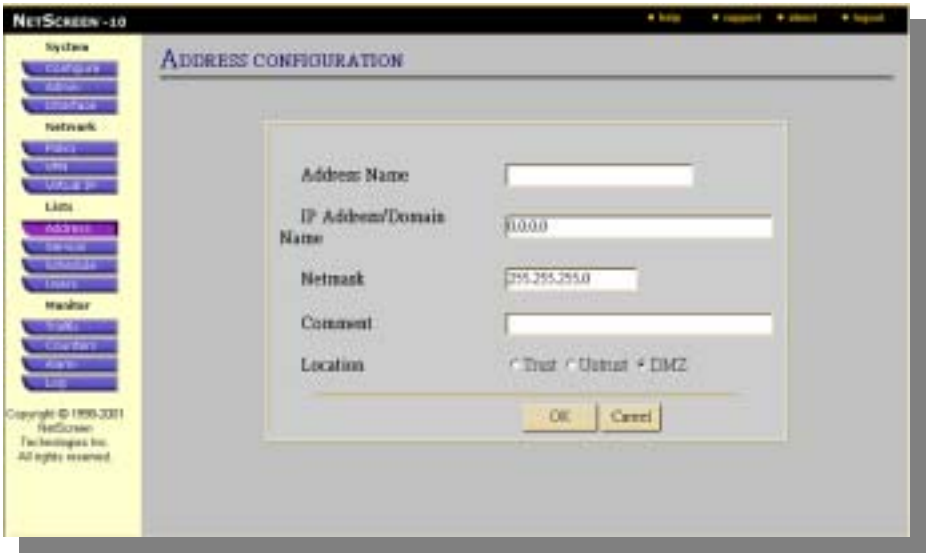



圖 FW lists addredd-02-1.jpg

**Address Name**：項目名稱

**IP Address/Domain Name**：DMZ 的 IP 位址。

**Netmask**：DMZ 的子網域位址。

**Comment**：備註欄。

**Location** 將所要定義的 IP 放置於何區域裡。（預設值爲所定義的 DMZ 區域爲區域）

Trust： DMZ：

Untrust：

＊New Group：

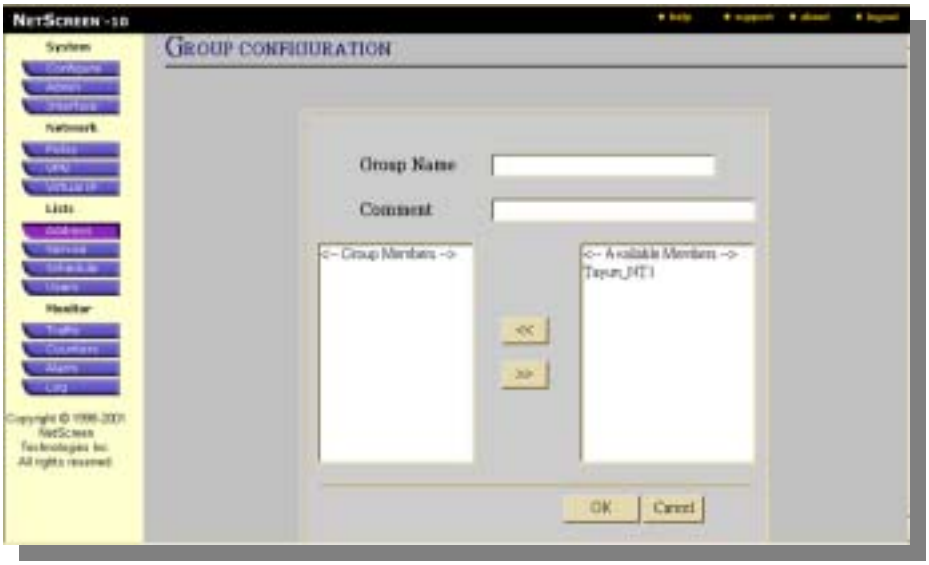



圖 FW lists addredd-02-2.jpg

**Group Name**：項目群組名稱。

**Comment**：備註說明欄。

左方塊：定義群組選項

右方塊：New Address 增加一個新的 DMZ 項目

二、service（各種服務）

1. Pre-defined （各種通訊協定服務）

PS：可將滑鼠一置所在通訊項目，其說明便會秀出相關資訊。

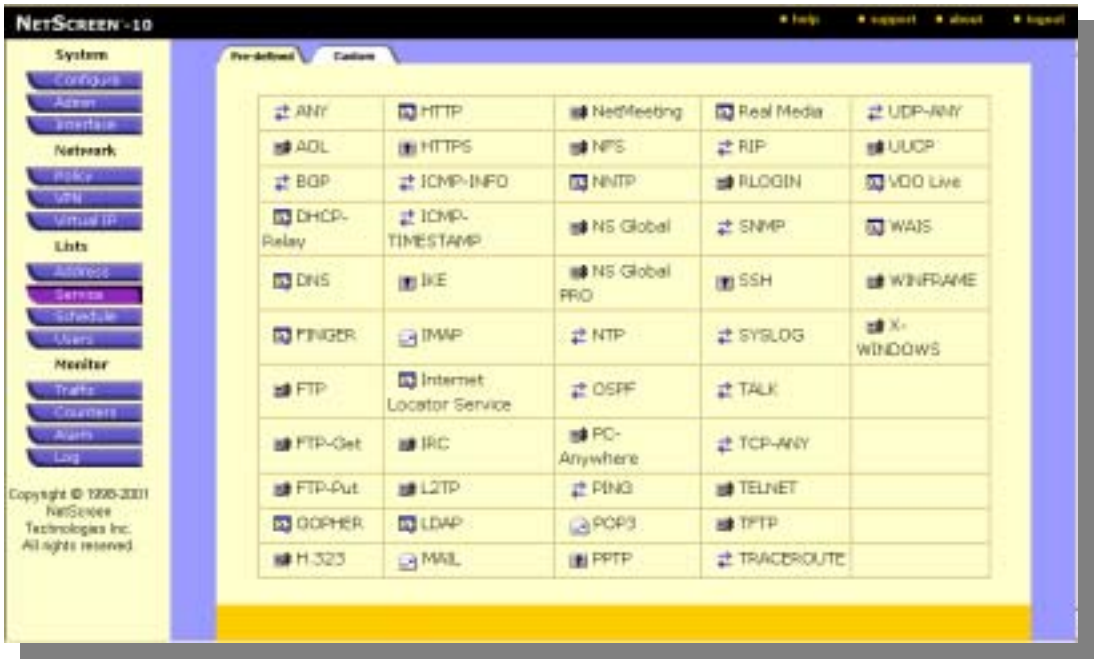



圖 FW lists service-00.jpg

2. Custom （自訂通訊協定服務項目）

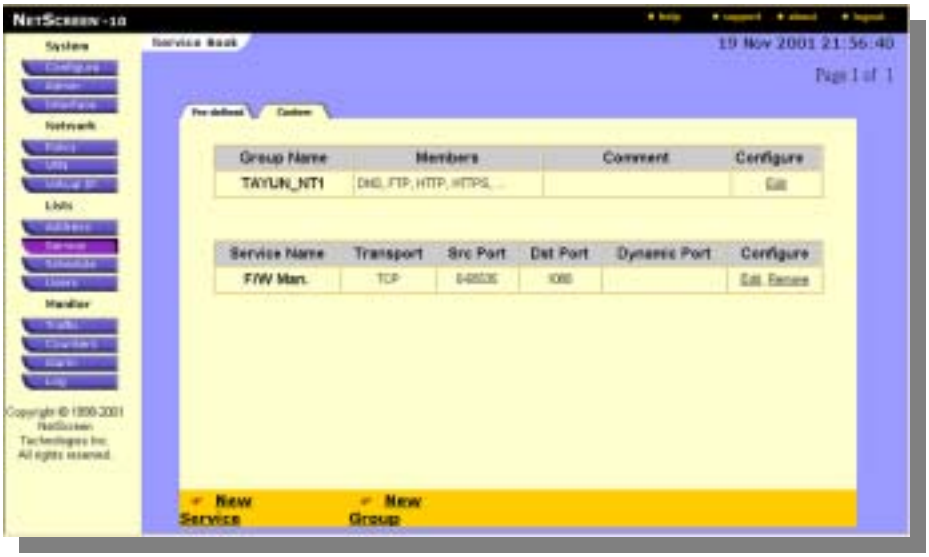



圖 FW lists service-01.jpg

可點選 New Service 增加一個新的 Custom 項目（圖 FW lists service-01-1.jpg）

可點選 New Group 增加一個新的 Custom 項目群組（圖 FW lists service-01-2.jpg）

＊New Service：


圖 FW lists service-01-1.jpg

**Sevvice Name**：所要自訂通訊協定名稱。

**Source Port** 起始值 port 數值。（0 ~ 65535）

Low：建議爲 0。　　High：建議爲 65535。

**Destination Port** 所要定義的通訊協定範圍。（如，HTTP 爲 80 可定義 Low：70 、High：90）

Low：　　High：

**Transport** 一些比較特殊的 port ID 編號。（建議以預設值 TCP：6 爲準）

TCP：　　Other：

UDP：

UDP 下方空格欄：封包物件數

1~8 項目：

＊New Group：

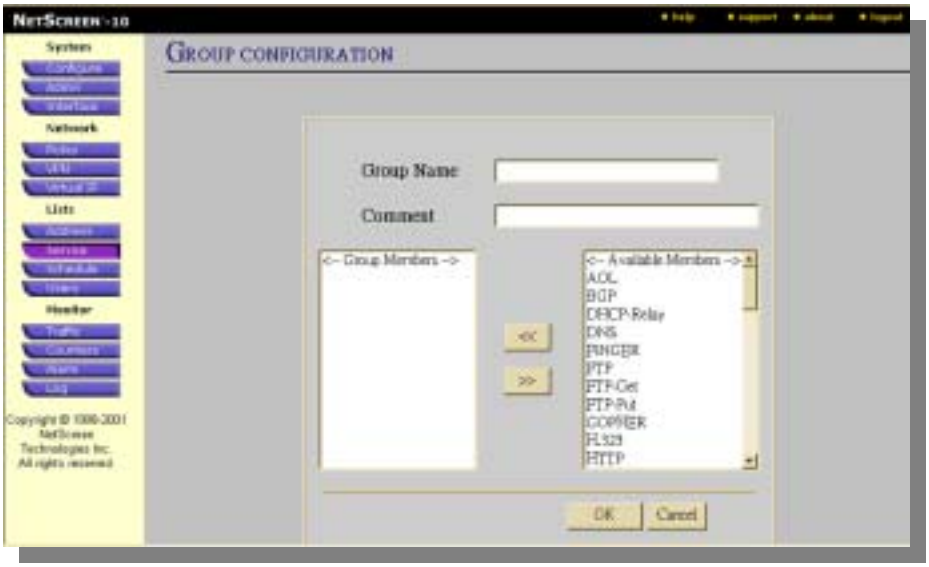



圖 FW lists service-01-2.jpg

**Group Name**：項目群組名稱。

**Comment**：備註說明欄。

左方塊：自訂群組選項

右方塊：Service\Per-defined 的各種項目表單

三、Schedule （時間的准許）即設定時段是否可做的通訊協定

1. Schedule （時間排程）

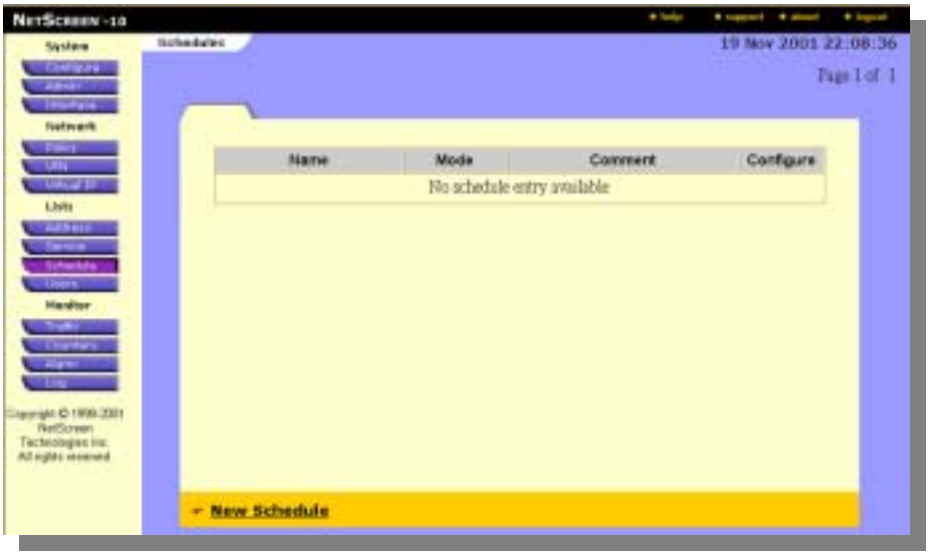



圖 FW lists schedule-00.jpg

可點選 New Schedule 增加一個新的 Schedule 項目

＊New Schedule：

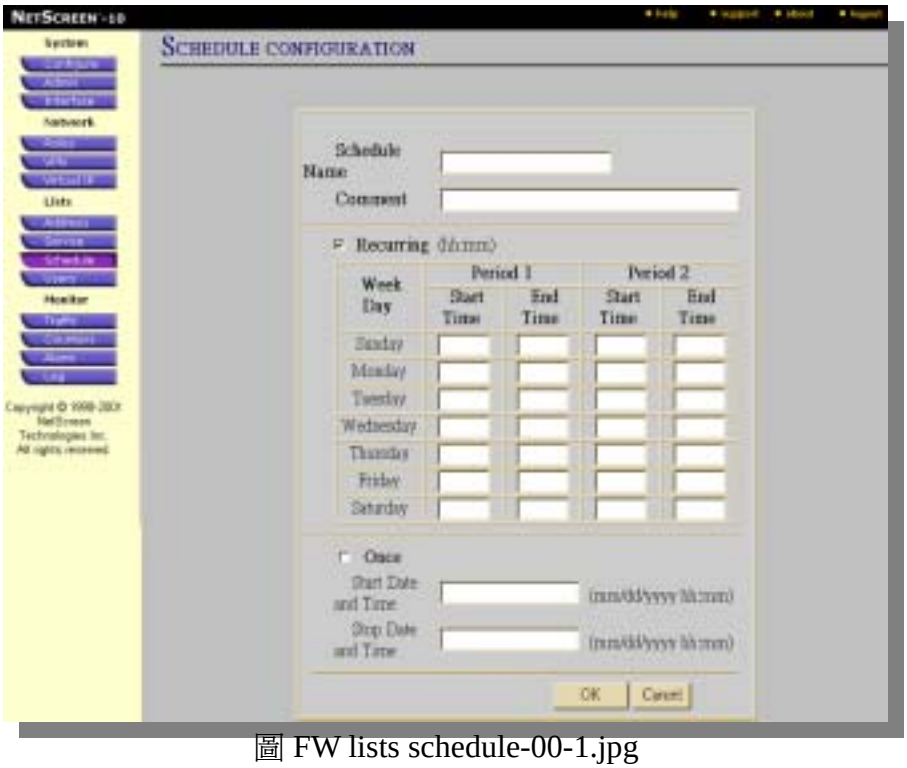



圖 FW lists schedule-00-1.jpg

**Schedule Name**：定義時間的准許名稱。

**Comment**：備註說明欄。

**Recurring**：啓動格林威治時間（小時與分鐘）

**Period1**：上午時段　　**Period2**：下午時段

Stat Time：開始時間　　End Time：結束時間

Sunday：星期日　　Thursday：星期四
Monday：星期一　　Friday：星期五
Tuesday：星期二　　Saturday：星期六
Wednesday：星期三
**Once**：是否啓動
Start Date and Time：啓動開始時間。
Stop Date and Time：啓動結束時間。

四、Users

1. Users

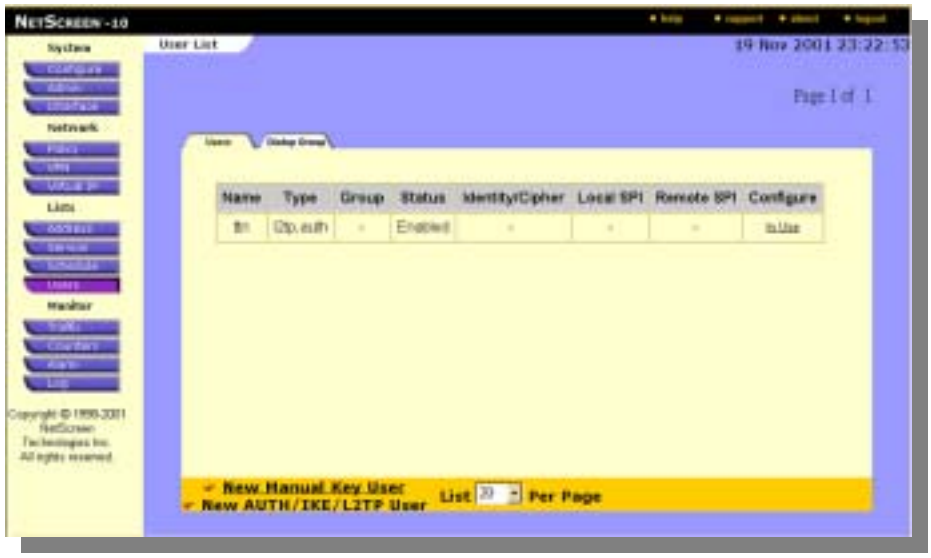



圖 FW lists users-00.jpg

可點選 New Manual Key User 增加一個新的 Users 項目（圖 FW lists users-00-1.jpg）
可點選 New AUTH / IKE / L2TP User 增加一個新的　　（圖 FW lists users-00-2.jpg）

＊New Manual Key User：


圖 FW lists users-00-1.jpg

**User Name**：名稱

**User Group**：群組

**Security Index**

Local：　　Remote：

**Esp**：

Encryption Algorithm

NULL：　　3DES-CBC：

DES-CBC：

HEX：

Generate Key By Password：

AuthenticationAlgorithm

NULL：　　SHA-1：

MD5：

HEX Key（16/20 Bytes）：

Generate Key by Password：

**AH**：

Hash Algorithm

MD5：　　SHA-1：

HEX Key（16/20 Bytes）：

Generate Key by Password：

＊New AUTH / IKE / L2TP User：

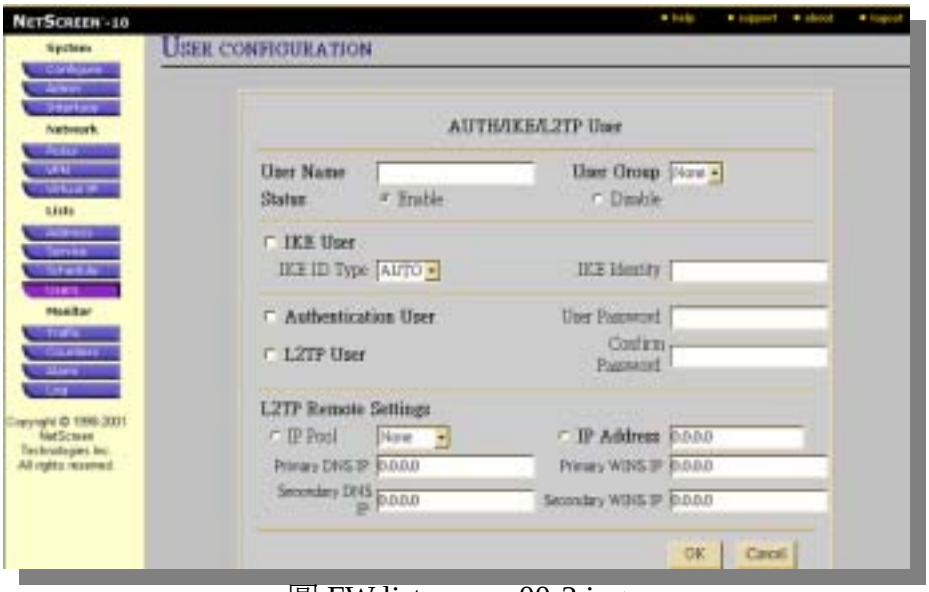



圖 FW lists users-00-2.jpg

**User Name**：名稱
**User Group**：使用群組
None 不加以定義
Status：身分
Enable：賦予
Disable：無資格
**IKE User**：
IKE ID Type
AUTO：
IKE Identity：
**Authentication User**：是否認證。
User Password：使用者密碼
**L2TP User**：是否使用 L2TP2 定義方式。
Confirm Password：確定密碼
**L2TP Remote Settings** 設定 L2TP2 定義方式。
IP Pool
None：不加以定義
**IP Address**：IP 位址
Primary DNS IP：第一組 DNS IP 位址。
Primary WINS IP：第一組 WINS IP 位址。
Secondary DNS IP：第二組 DNS IP 位址。
Secondary WINS IP：第二組 WINS IP 位址。

2. Dialup Group


圖 FW lists users-01.jpg

可點選 New Group 增加一個新的 Dialup Group 項目

＊New Group：

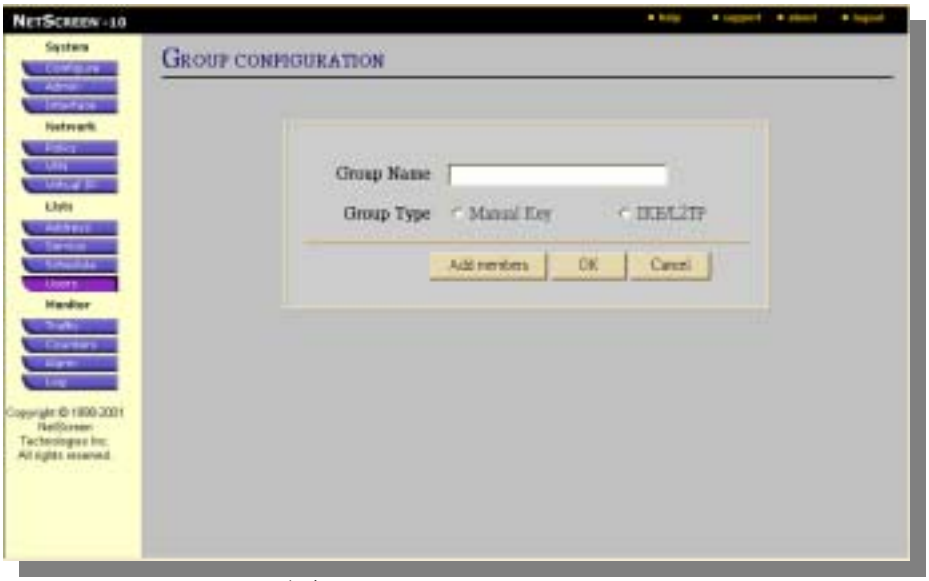



圖 FW lists users-01-1.jpg

Group Name：名稱

Group Type

Manual Key：　　IKE/L2TP：

- Monitor（防火牆狀況進出監測）

一、Traffic 防火牆流通狀況

1. Policy （現階段方針）


圖 FW monitor traffic-00.jpg

2. Interface（連繫裝置）


圖 FW monitor traffic-01.jpg

可點選 Update Now

二、Counters（檢視各區域的通訊協定狀況）

1. Counters （檢視各區域的通訊協定狀況）


圖 FW monitor counters-00.jpg

PS：可點選「View Count Details...」前面小紅點瀏覽其狀況。

三、Alarm（警報）

1. Traffic Alarm （流量警報）主要爲攻擊內部


圖 FW monitor alarm-00.jpg

2. event Alarm（進出情況警報）主要爲攻擊外部

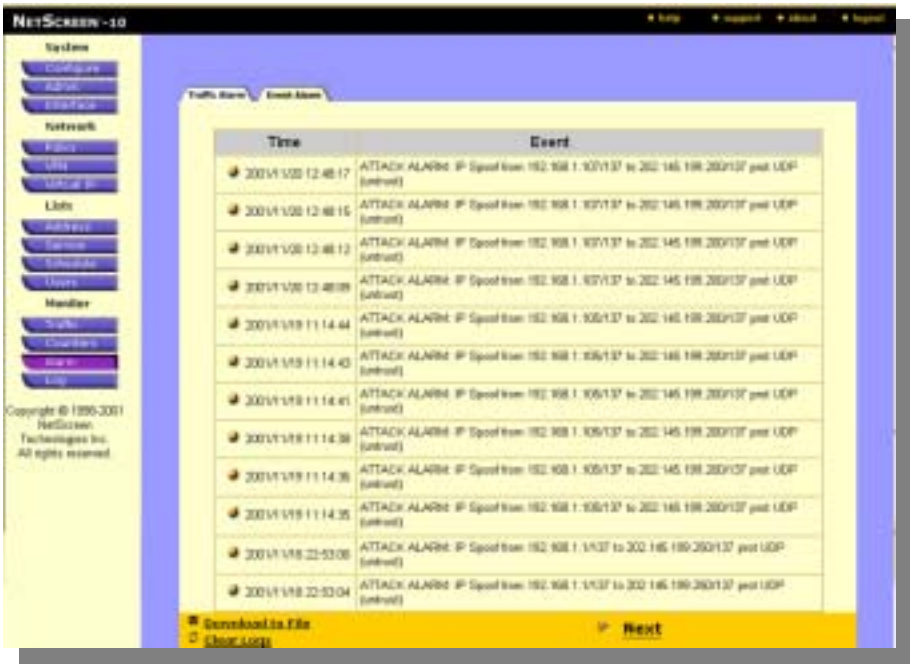



圖 FW monitor alarm-01.jpg

可點選 Download to File 下載紀錄目前狀況加以儲存

可點選 Clear Logs 清除目前所紀錄的狀況

四、Log （事件紀錄）

1. Traffic Log （流量紀錄）

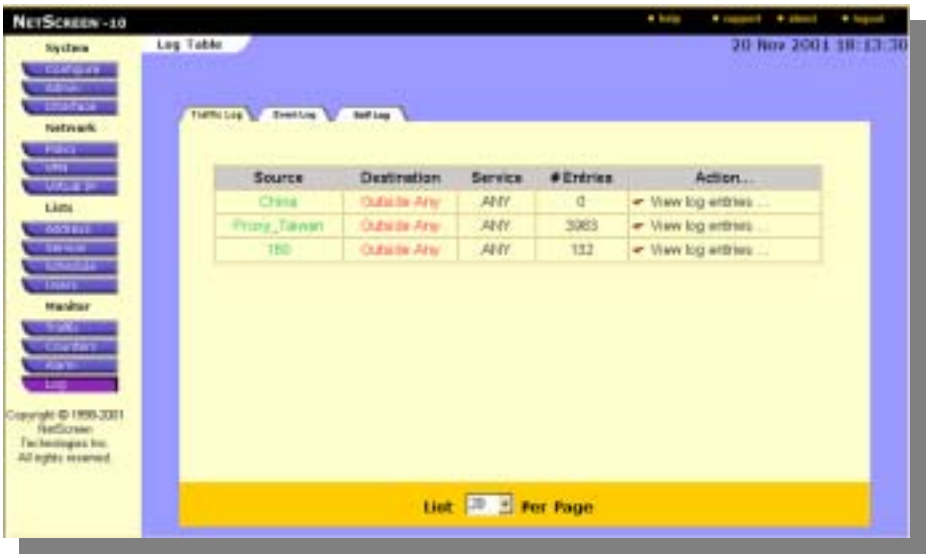



圖 FW monitor log-00.jpg

2. Event Log （重大事件紀錄）

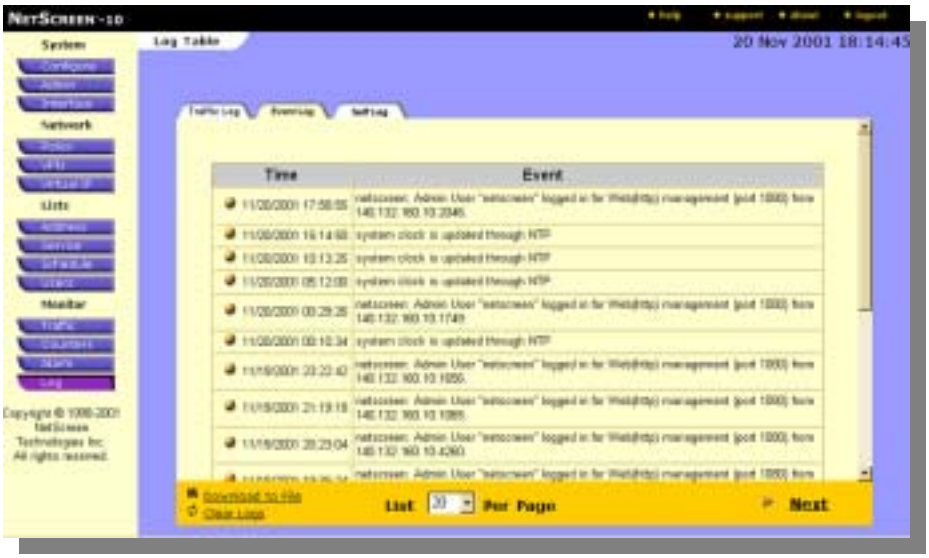



圖 FW monitor log-01.jpg

可點選 Download to File 下載紀錄目前狀況加以儲存

可點選 Clear Logs 清除目前所紀錄的狀況

3. Self Log（安全紀錄）

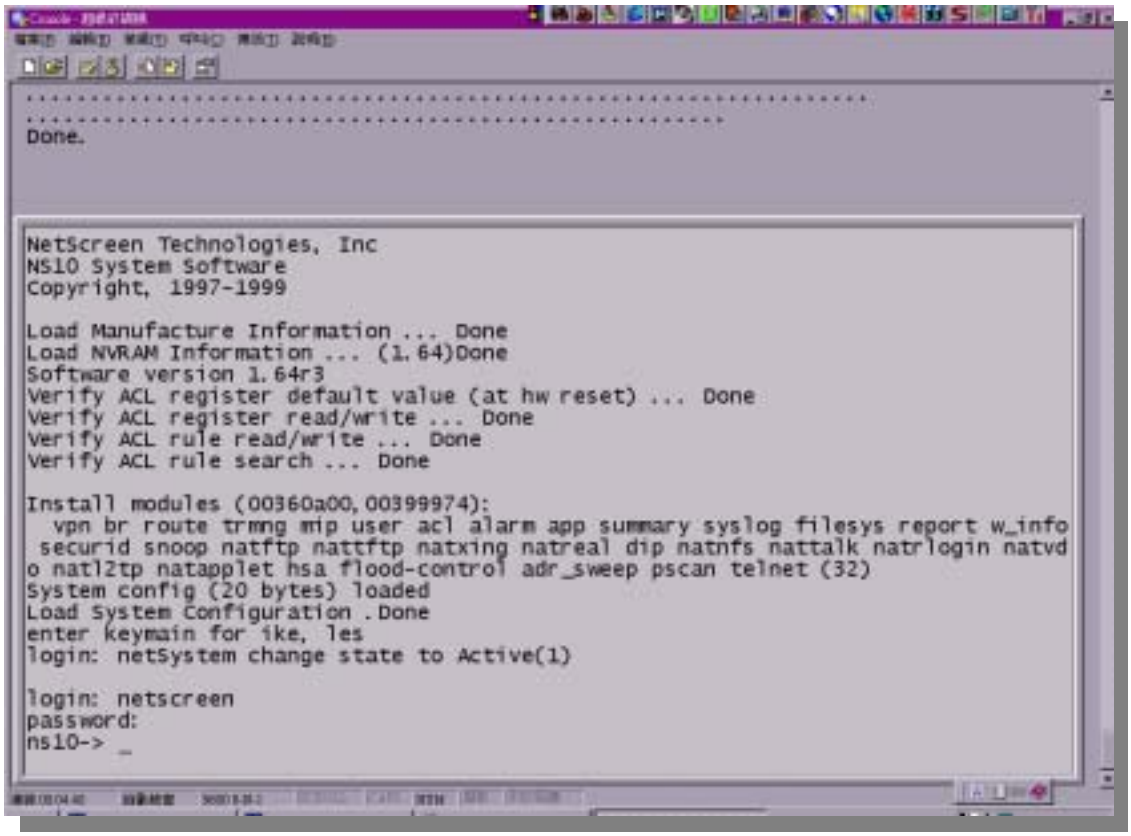

圖 FW monitor log-02.jpg

可點選 Download to File 下載紀錄目前狀況加以儲存

可點選 Clear Logs 清除目前所紀錄的狀況

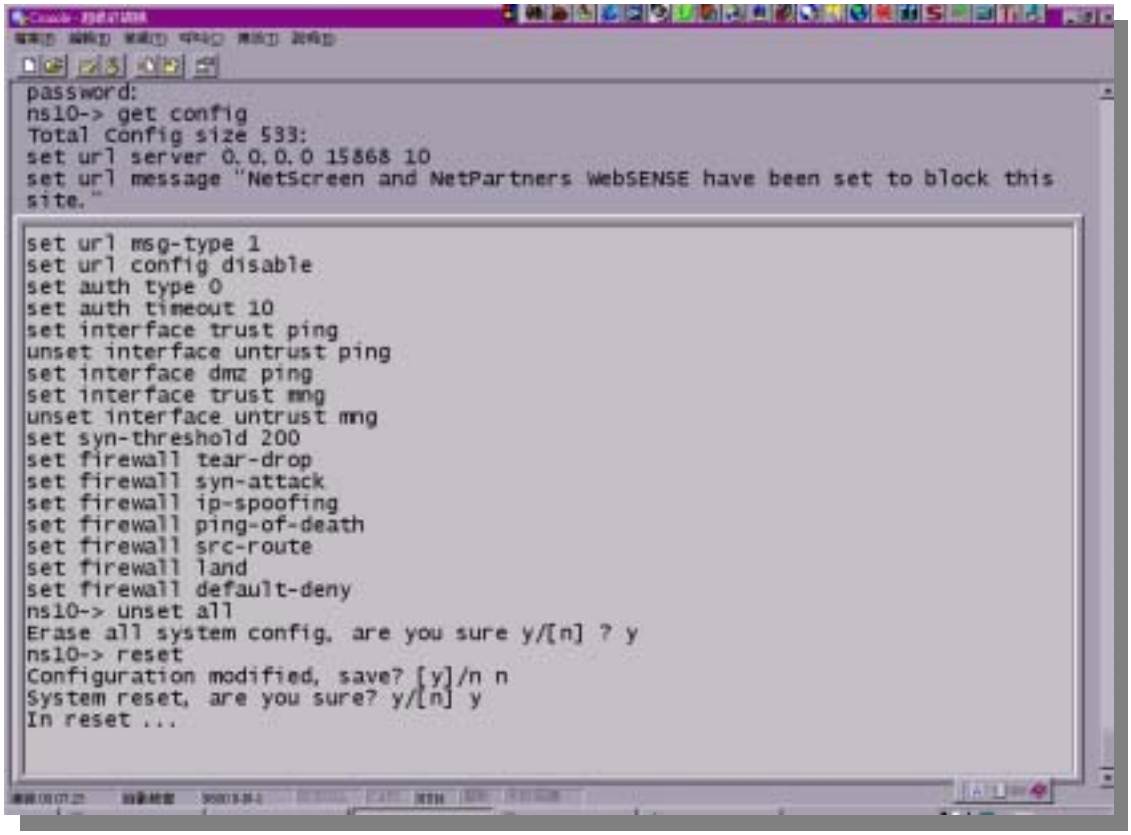
## 附件一：Netscreen firewall 簡易設定步驟

使用隨設備所附的 console cable 連接到 Netscreen console 與電腦的 com port
速率設爲 9600 參數 n,8,1(也就是都用預設值)
使用終端機程式或是 Telix 等終端機軟體即可看到 Netscreen 的狀態如下圖
**登入的帳號及密碼預設都是小寫的 netscreen**




進入後即可看到 > 符號,此時可對 firewall 下指令,
如果要看目前設備內的設定值就打 get config
將可以看到如下圖資訊

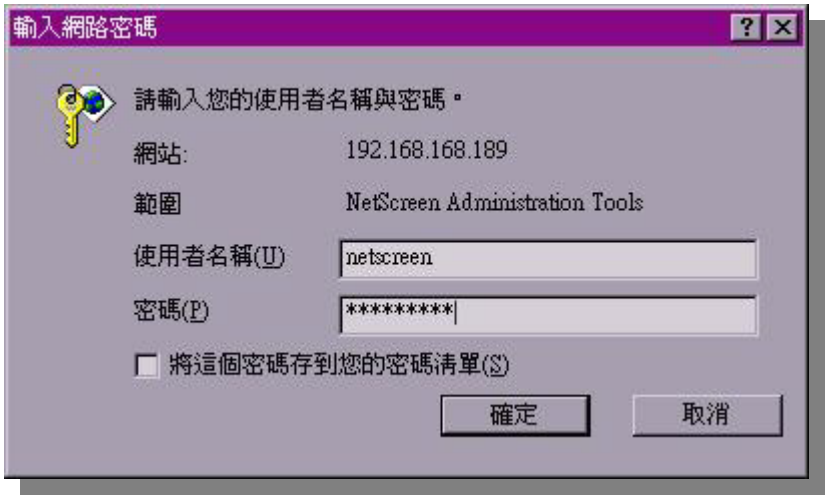
**要將設定清除恢復成預設值就打 unset all**
再打 reset 將機器重新啓動才會生效,問你是否要儲存回答 no 不要儲存
這樣才會清得掉
也一併參考下圖



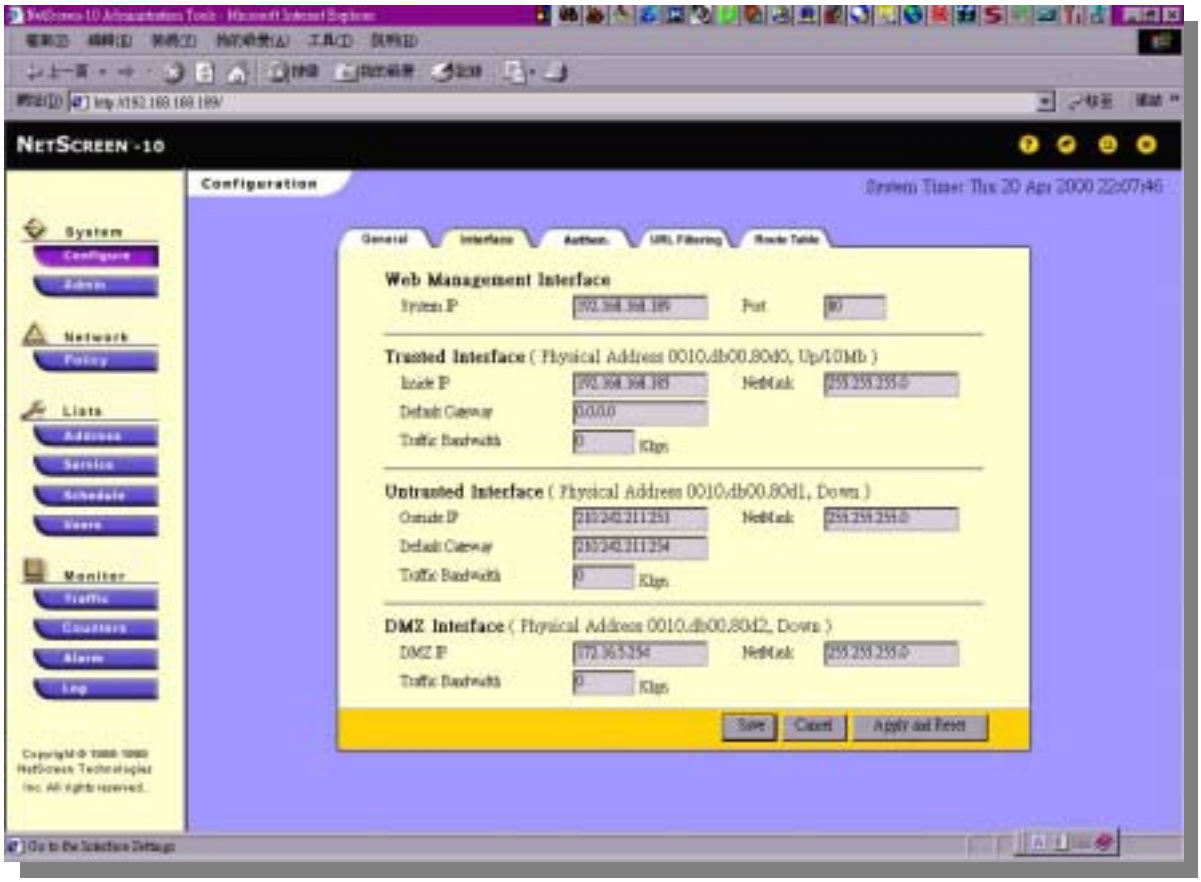

Netscreen 可以由瀏覽器來操作而且較快速方便
清空成爲預設值後，我們只需要下一行指令
指定了 firewall 的 IP 後就可以都用瀏覽器來管理,十分簡單
舉例：如果 Netscreen firewall 的 IP 是 192.168.168.189 的話,就下一行指令

**set admin sys-ip 192.168.168.189**

輸入 **save** 就可以儲存目前設定
之後就可以開瀏覽器在網址打入 Netscreen 的 IP 位置：192.168.168.189
在此需輸入的帳號及密碼仍然都是小寫的 netscreen
按 enter 後即可進入 web 操作介面



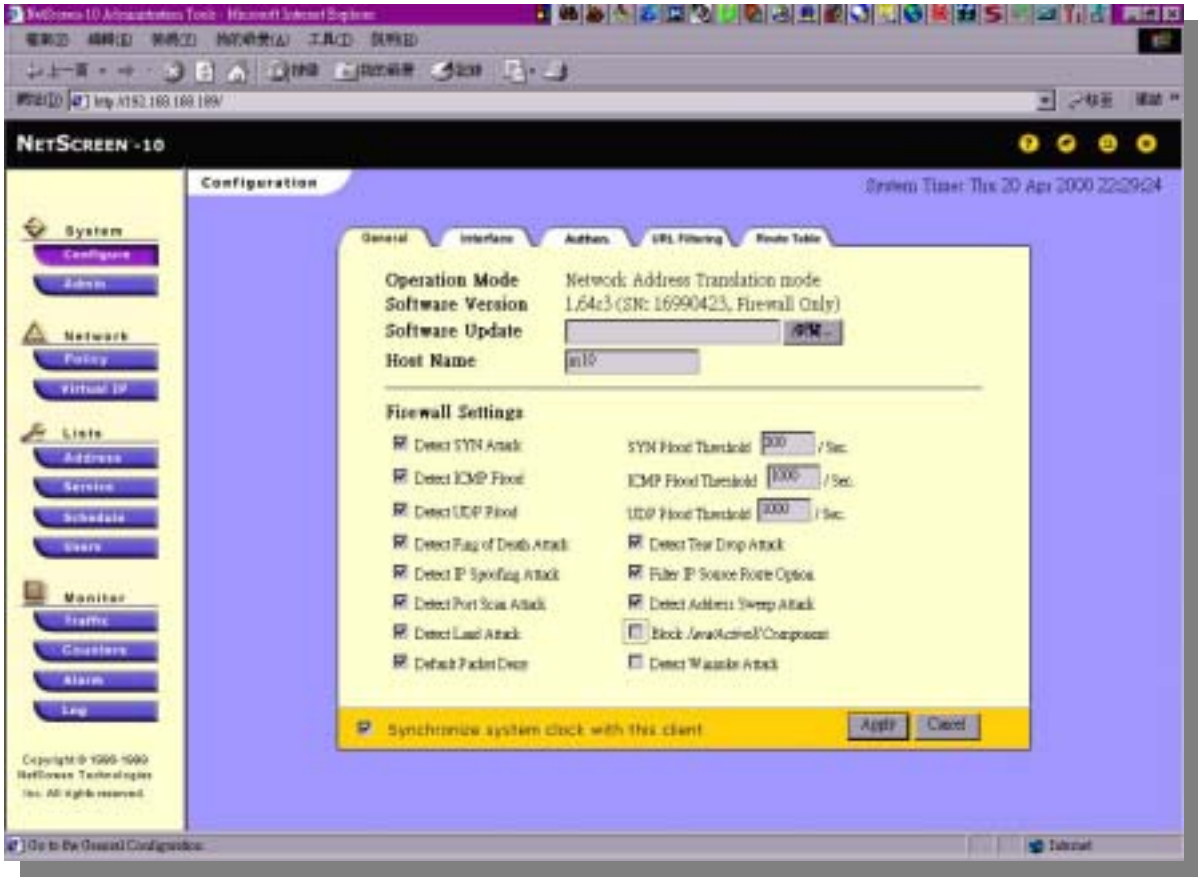
接下來**設定各個介面的 IP 位置**：點選左邊的 Configuration
在 trusted interfac inside IP 打入你的 firewall IP 與網路遮罩(mask)
untrusted interface outside IP 打入 untrust 的 IP 與 mask
在這邊的 default gateway 輸入 router 的 LAN 端 IP
DMZ interface 內也輸入你的網路伺服主機(web,ftp..等)那段的 IP 位置與 mask




輸入完成後按右下方的 Apply and Reset
再回答確定即可生效
此時系統需要重新啓動大約會花一分鐘的時間此期間不要操作瀏覽器
稍後一分鐘畫面出現 ok 訊息將瀏覽器重新整理就可以看到新的畫面

接下來設定可以防禦的選項與時間同步

按左方的 Configure 後選 General 那頁
可以看到 firewall setting 中有勾選的項目即是目前可做的防禦
視需要加以勾選
下方有一個時間同步的選項,Synchronize system clock with this client
可將時間與你的電腦同步
如此日後閱讀 log 紀錄時比較好對照時間




接下來我們需要將被管理的對象一一在 firewall 內建立起來

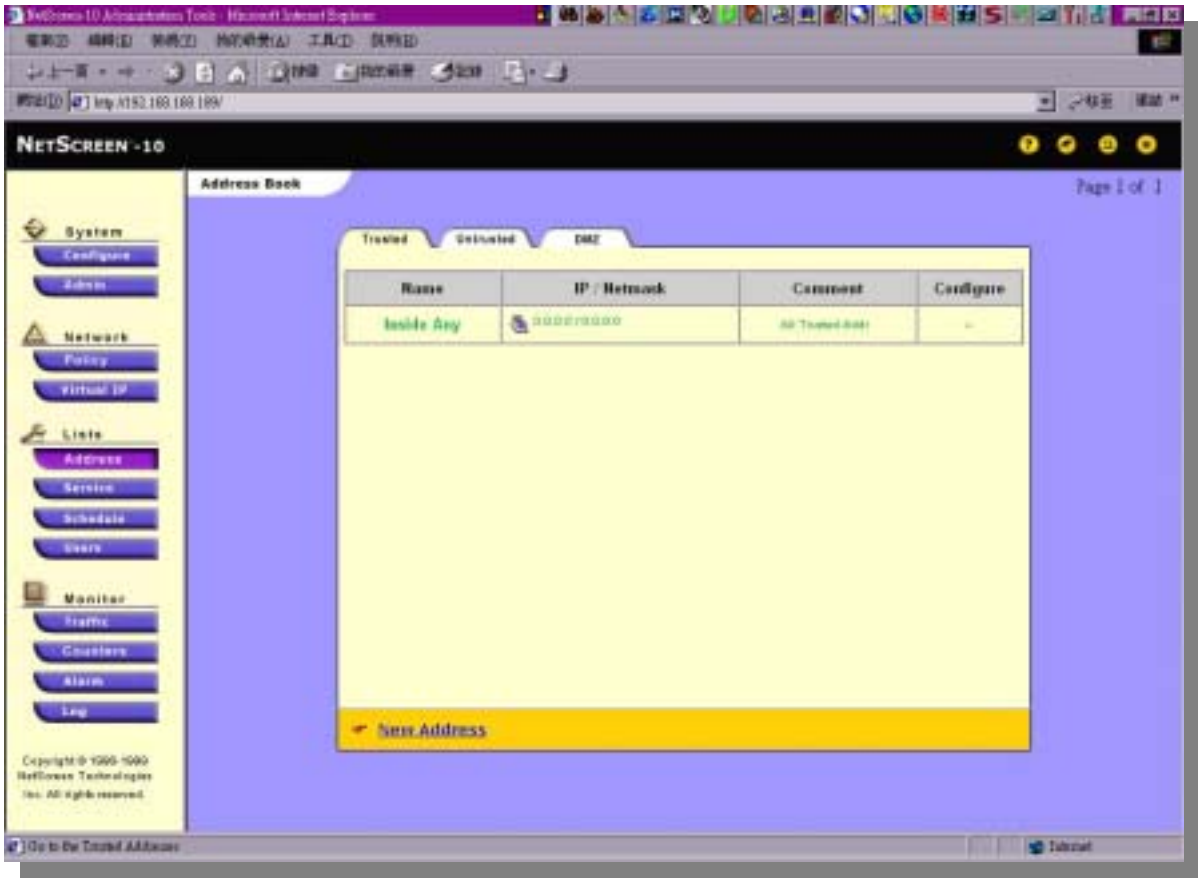
Netscreen firewall 只可以依 IP 來作管理,也就是要先**設定 Address**：

按左方的 Address 將出現下圖：

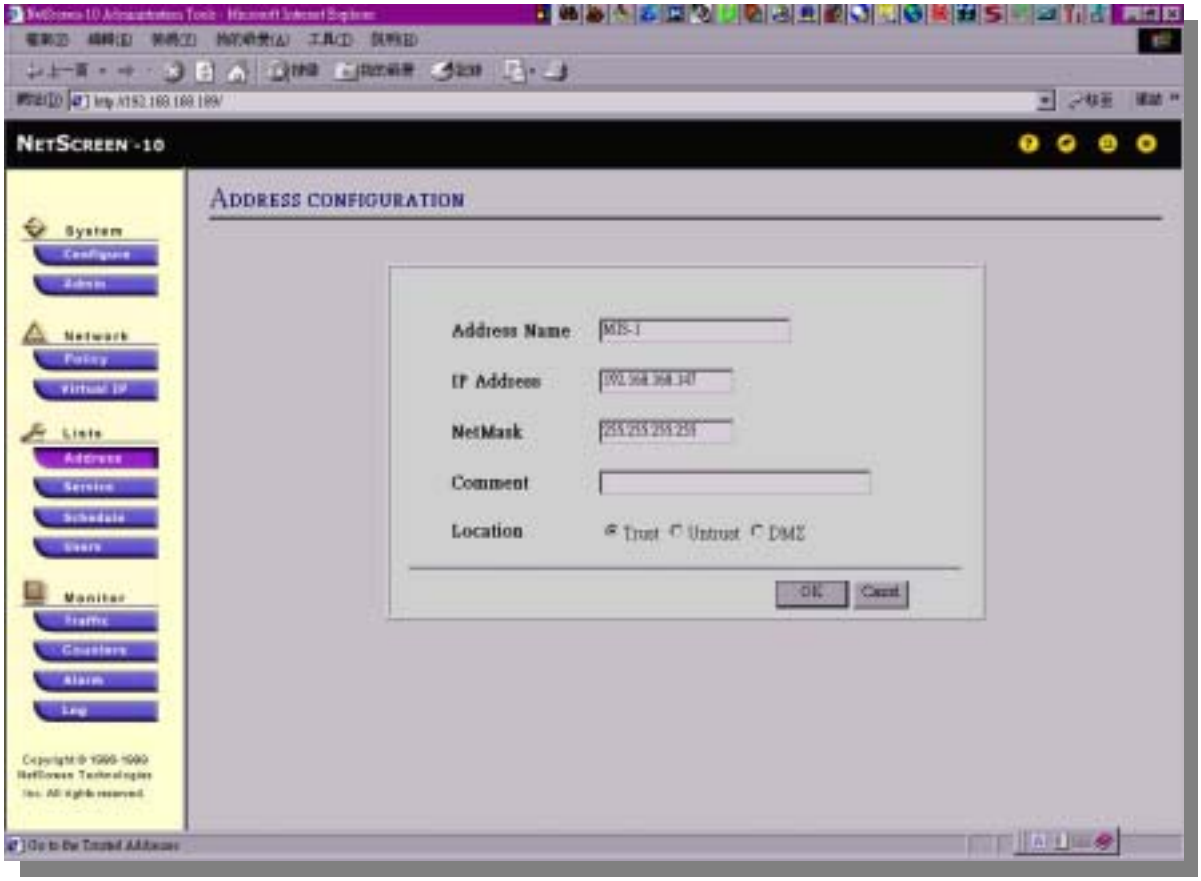
裡面的 Trusted Untrusted DMZ 三個選單預設值都是空的
在 Trusted 這邊建立的對象是你內部網路的主機或 PC
一般是使用非法(虛擬)的 IP

在 Untrust 這邊建立的是在 internet 上出現的有合法 IP 的主機
所以這邊都應該是合法的,可以上 internet 或外部網路的 IP

在 DMZ 這邊設定的則是你自己要提供服務的主機的 IP
例如是你的 web server 或 ftp server
此三個界面的 IP 是不同的網段

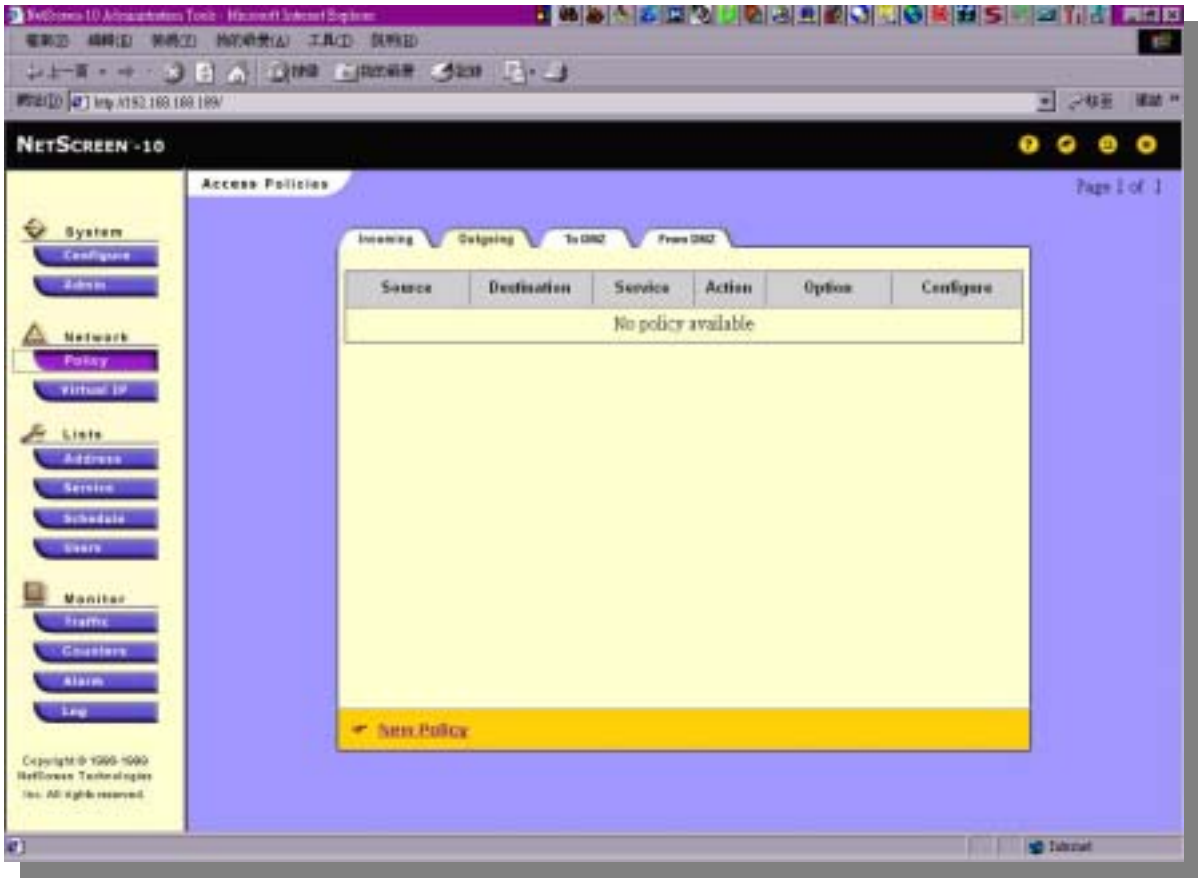



按下 New Address 即可新增一個對象

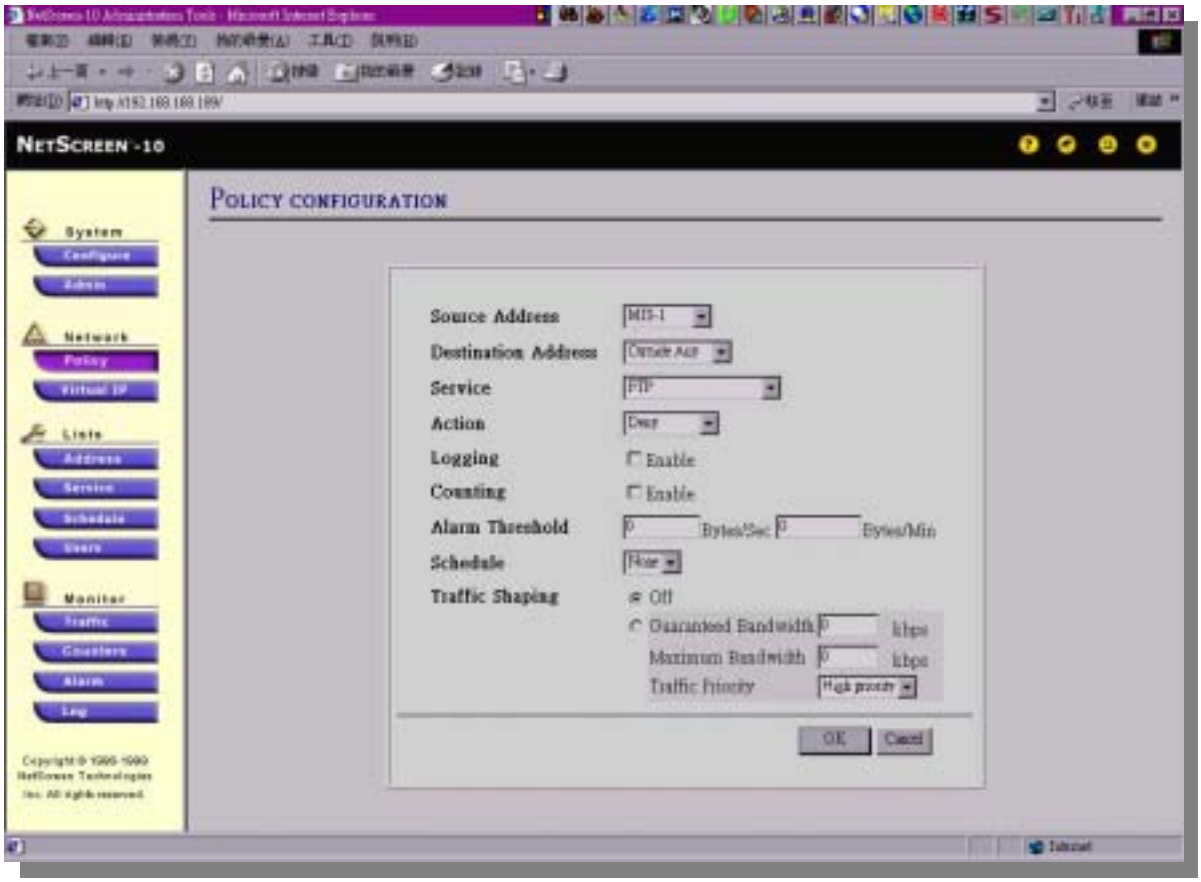


其中 Address Name 可以自己定英數字組成的名稱如 MIS-1(請不要打中文)
這個名稱將在訂定 policy 中可被選取
IP 打入這台主機的位置如 192.168.168.147
如果 NetMask 打的是 255.255.255.255 的話就是指這一部主機而已
如果 NetMask 打 255.255.255.0 就是指整個 192.168.168.0 網段的所有機器
此方法雖然可以簡化設定不用重複輸入位置但是自己也需特別注意是否規劃正確
Location 就是選擇這個 IP 是在 Netscreen 的哪個一介面裡,注意不要弄錯

如果被管理的 address 都已經設定完成就可以進入 **Policy 設定**
按左方的 Policy 鍵將出現下列選單
從內部(trusted)出去到 internet 要在 Outgoing 設定
讓外界(untrusted)存取我們要在 Incoming 設定
不論哪一邊(trusted or untrusted)要去存取 DMZ 要在 To DMZ 設定
若從 DMZ 出去到 trust 或是 untrusted 端都在 From DMZ 設定



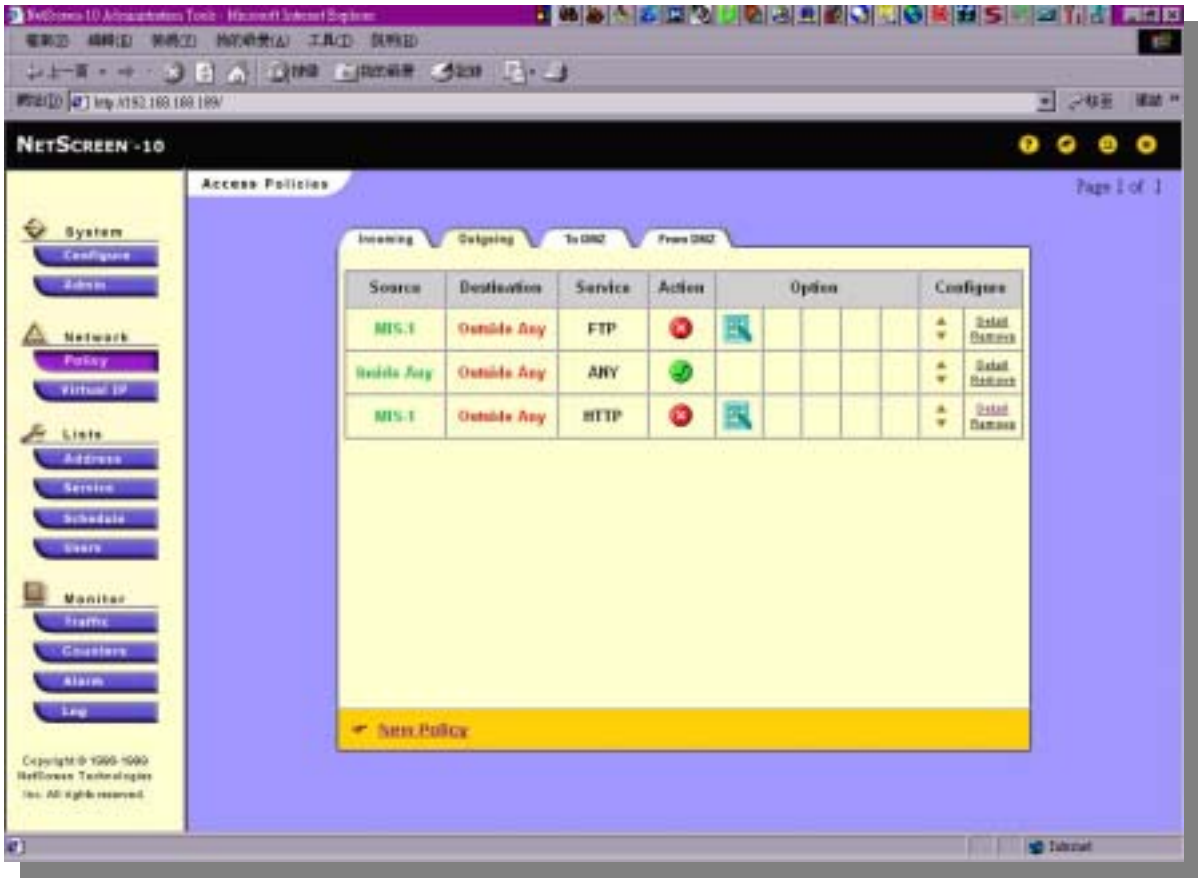

依上述法則你要設定的種類後按下該頁
選下方的 New Pollicy 即可新增一個進出管制設定
如下圖




每一個進出管制 policy 至少都有四個參數要選擇
可以在各個下拉選單中作選擇　以設定 outgoing 爲例
Source :你要管理的對象 例如剛剛建立的 MIS-1
Destination :要去的目的地 例如 outside any 就是所有的外界主機
Service:加以管制的服務種類,內建已經有很多標準的網路服務種類如 FTP
Action:設定允許(Permit)或拒絕(Deny)或是需要經過身分辨識(Authenticate)
如果需要將此活動紀錄,可以再勾選 logging

上列設定即是『不允許 MIS-1 對任何外部的主機進行 FTP』

Netscreen 的 policy 的觀念是
**越前面頁數；越上面一列的 policy 優先度越高**
如果下面的 policy 與前面的相衝突，仍已先設的爲準
如下圖所示
第一行已設定不允許作 FTP
第二行雖然允許所有的服務均可通過，但是因爲第一行之故仍是無法做 FTP
第三行雖然不允許 HTTP 服務通過，但是第二行已經允許所有服務通過故第三行的設定還是無效
其他以此類推

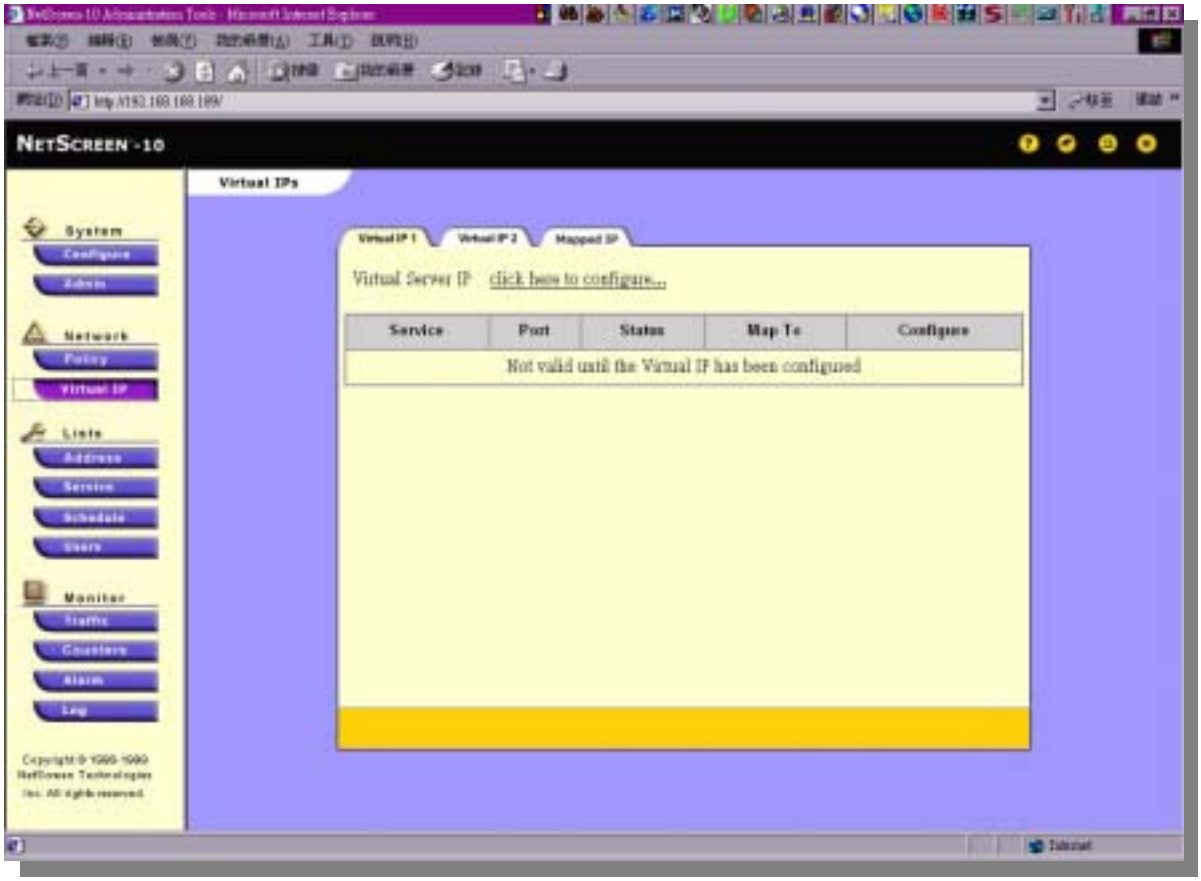


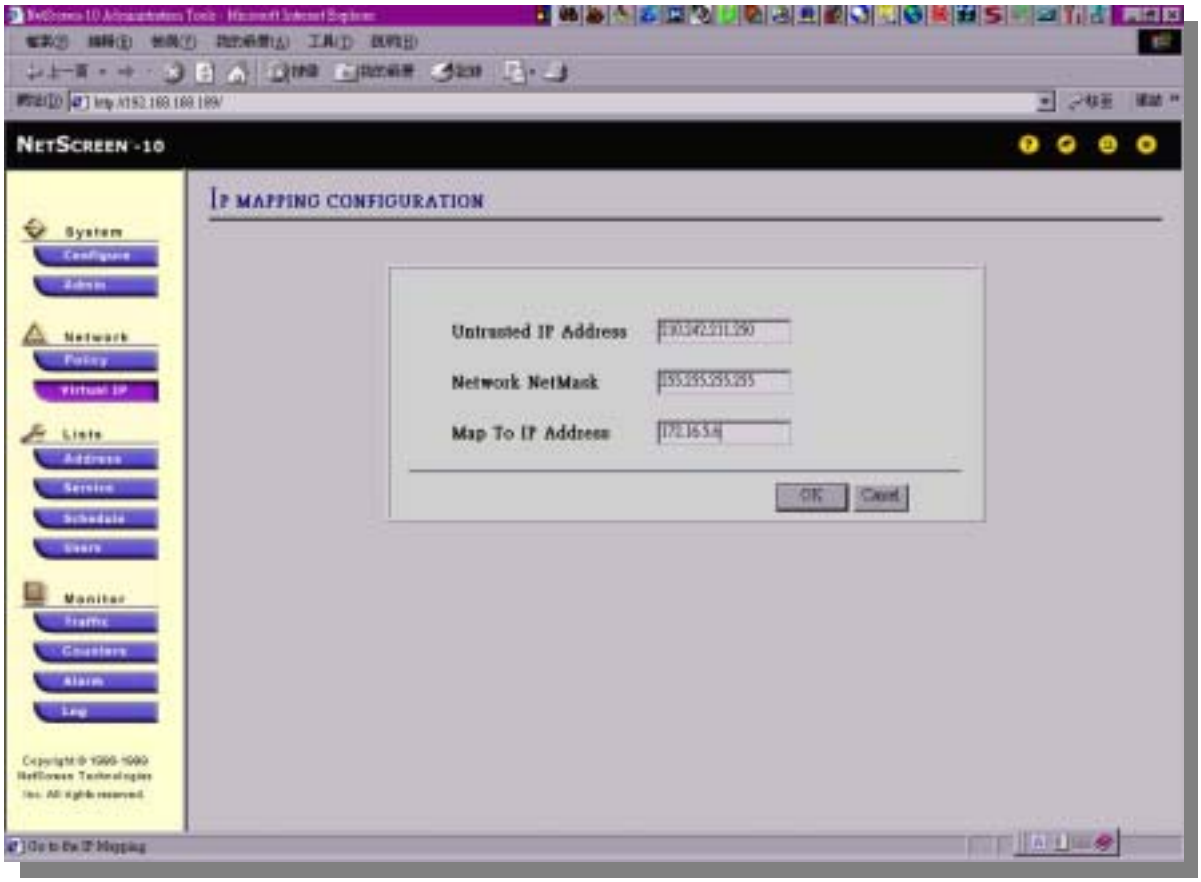

如果要調整某一列設定的高低順序，就按最右側 Configure 裡面倒數第二格的
三角形上(提高)或下(降低)鍵，按一次可調整一個順位。直到符合需求爲止
若要將此設定清除就按最右邊的 remove。按 Detail 可以進入修改設定

如果我有伺服器放在 DMZ 段由於 DMZ 的機器不能被 internet 的人存取
必須要有合法的 IP 對應到 untrusted 才可以

點選在左方的 Virtual IP,會出現下頁的圖
選擇 **Mapped IP**
按下方的 New Entry 來新增一個對應的 IP 位置
第一行是指對應出來的合法 IP 如 210.242.211.250
中間 255.255.255.255 代表是一對一的對應
第三行就是你在 DMZ 網段中 server 的 IP
如 172.16.5.6

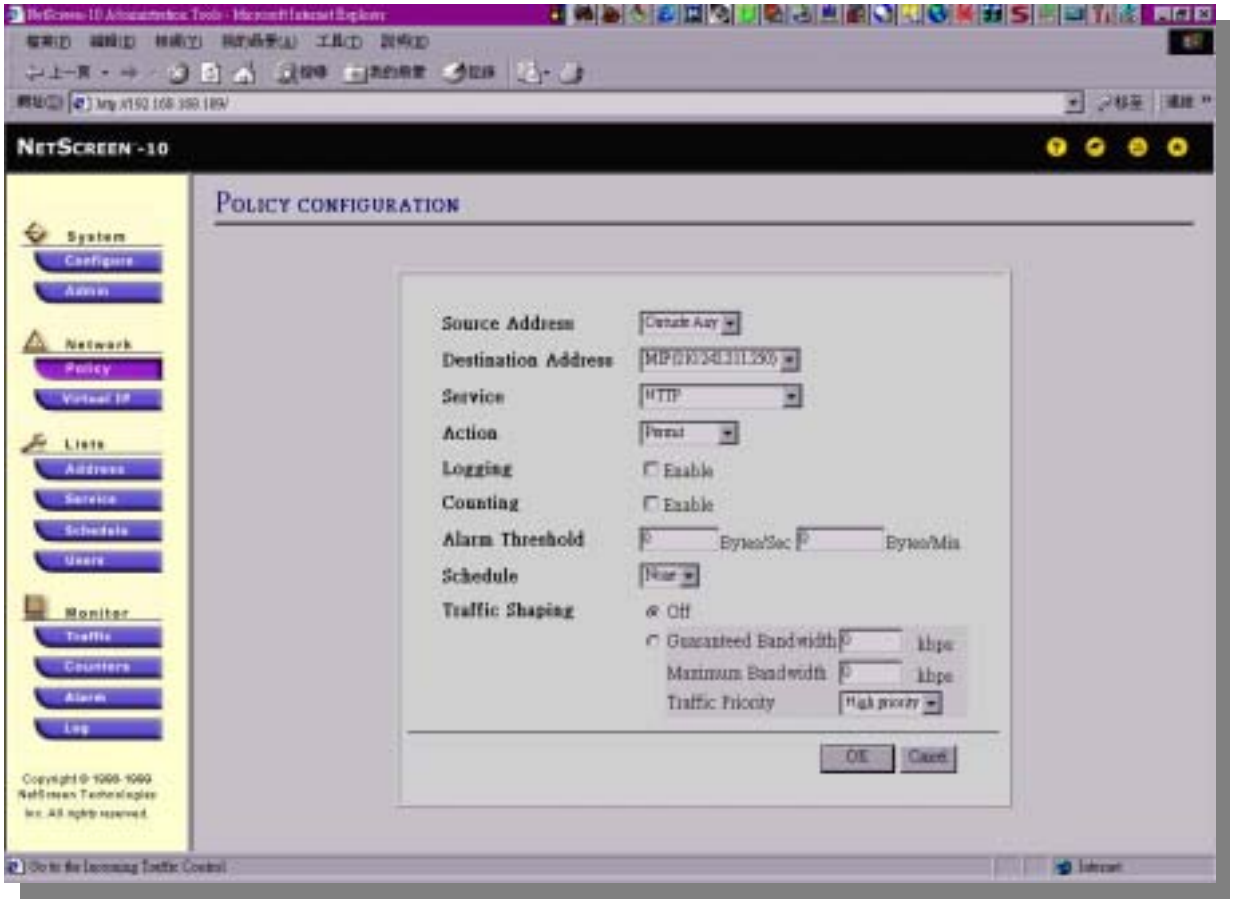
其他所有要讓 internet 存取的主機一樣以此原則一一在 Virtual IP 中的 Mapped IP 建立
再至 Policy 中限制可以對它做的存取


NETSCREEN -10
Virtual IPs
System
Configure
Admin
Network
Policy
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Virtual IP 1
Virtual IP 2
Mapped IP
Virtual Server IP
click here to configure...
Service
Port
Status
Map To
Configure
Not valid until the Virtual IP has been configured


NETSCREEN -10
IP MAPPING CONFIGURATION
System
Configure
Admin
Network
Policy
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Untrusted IP Address
Network NetMask
Map To IP Address
OK
Cancel

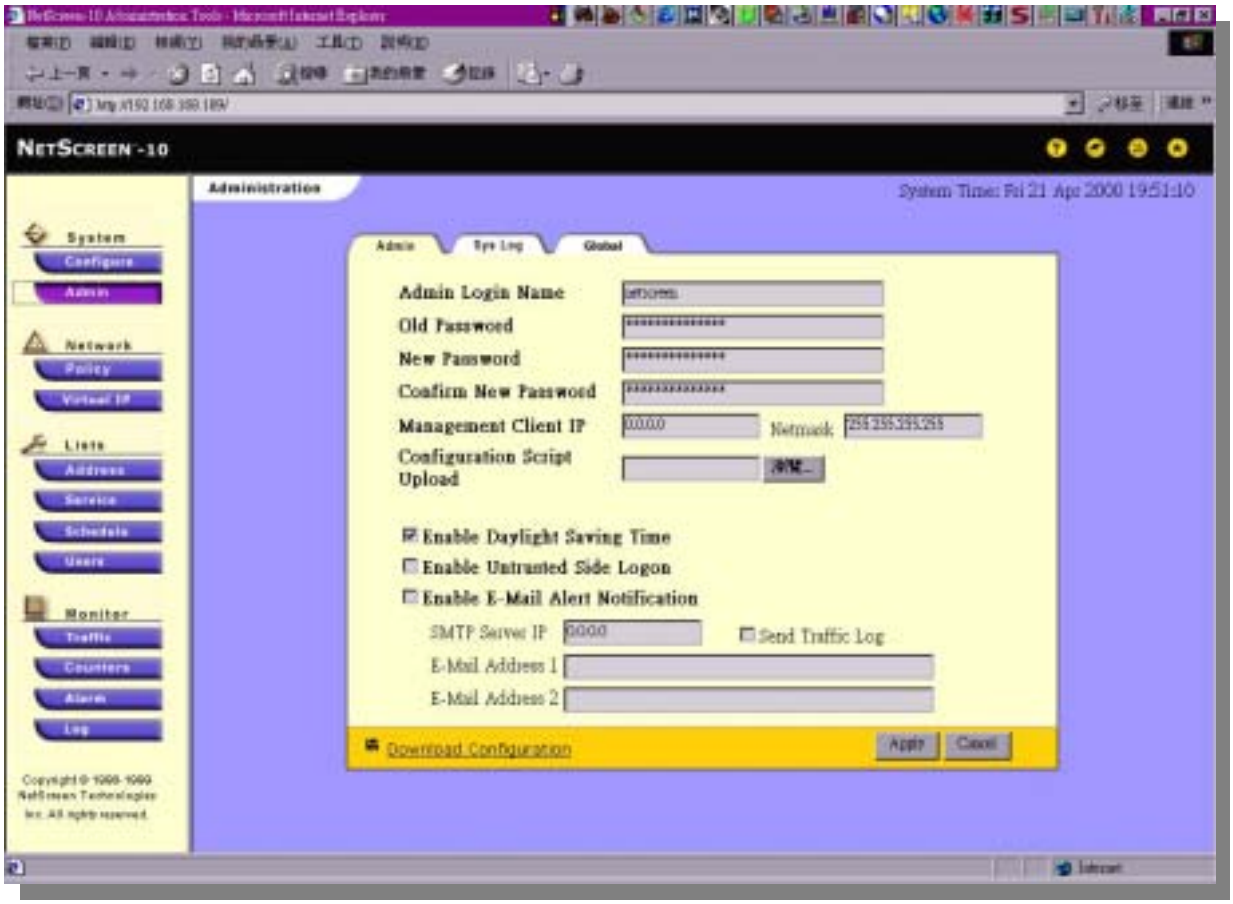
製作人：蘇嘉文

有設完 mapped IP 後，就可以在 Policy 中決定外界可以對這個 IP 存取的限制
如下即是設定『外界僅可以對此伺服器作 HTTP(web)的存取』




如果需要將目前設定儲存備份，到左方的 Admin 中按下
即可在第一頁 Admin 看到最下方的 Download configuration
按下後會出現儲存視窗，可將其存爲一般文字檔.txt

如果有設定檔要讀進 Netscreen，一樣在此頁的 Configuration Scrip Upload 中按下瀏覽
找出硬碟上儲存的設定檔按確定就可以讀進來
重新啓動後就可以生效




注意事項

**自行設定的帳號及密碼若遺忘只有送回原廠一途**

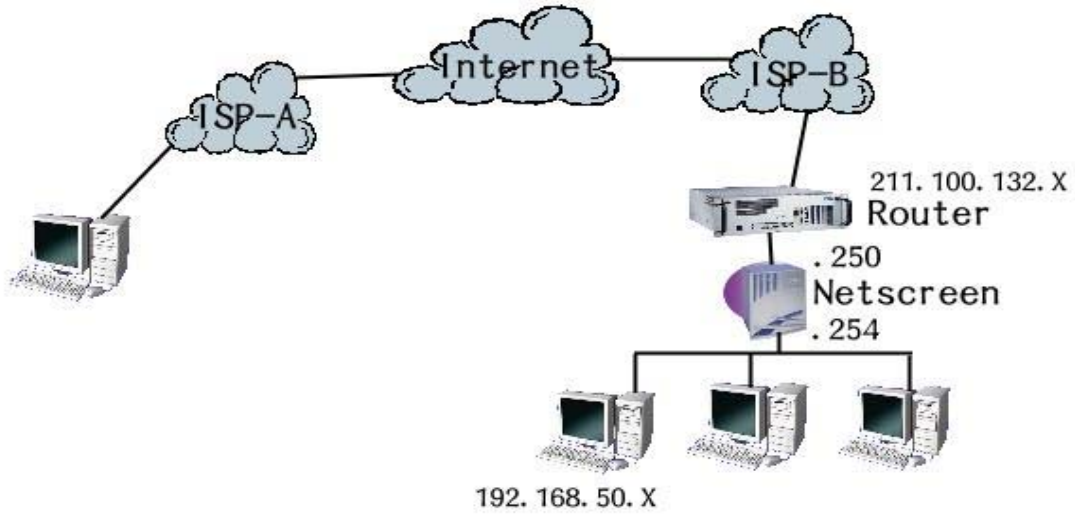
**絕對不可自行拆卸機殼**

進行設定檔讀取時不可中斷

若需要升級新版韌體請聯絡經銷商之工程師

## 附件二：**Netscreen Remote 應 用(一)**

※因公在外，連上當地 ISP 後，使用 Netscreen Remote 存取內部資源。舉例如



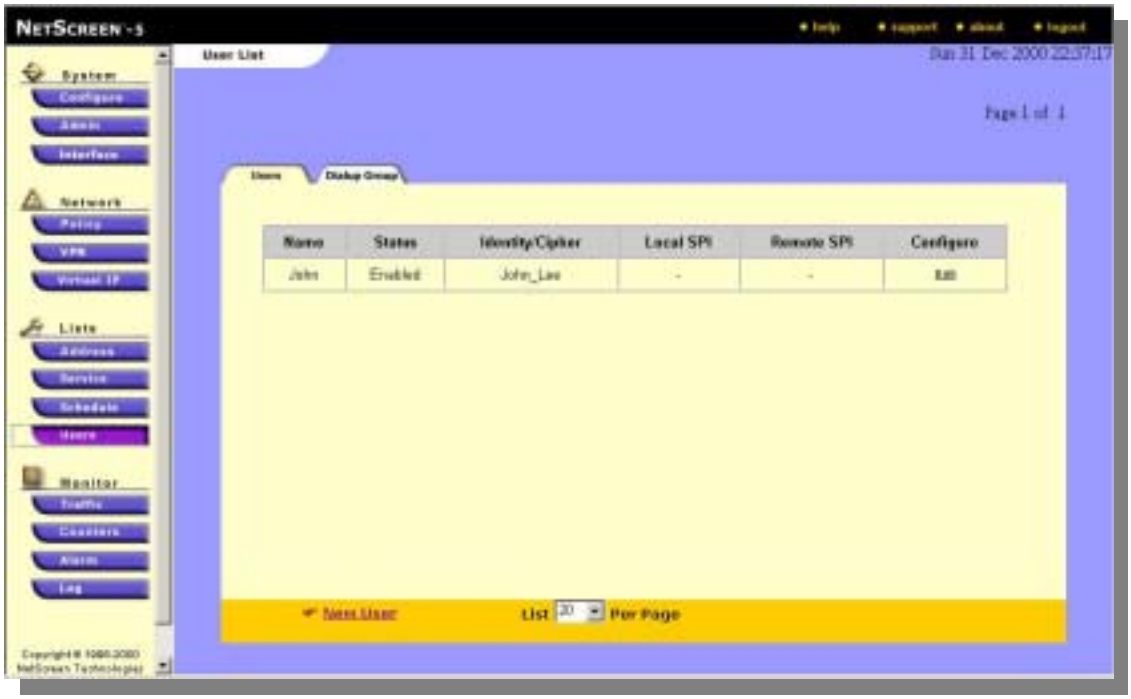

圖一：

如上圖所示，當你因公出差至外地，你可以只連上當地之 ISP，利用 Netscreen Remote 連回公司之 Netscreen Firewall，即可存取內部之網路資源。與傳統撥回公司比較起來，一可節省可觀之撥接費用，再則透過訊息加密可確保資料之安全性。本例中 Netscreen Firewall 使用 2.5 版之 OS，Netscreen Remote 使用 5.X 版之軟體。VPN 採用 Preshare Key，加密採用 DES，Authenticate 採用 MD5。

※設定步驟 Netscreen Firewall

1、點選 VPN/User/New User 可看到如下畫面：
於 User Name 處輸入使用者名稱如 ”John”，點選 IKE Dynamic Peer，於 Identity 處輸入此使用者之識別名稱如 “John_Lee”，


於最下方按下 “Apply”後即出現如下畫面：



2、點選 VPN/Gateway/New Remote Gateway 出現如下畫面：

於 NAME 處輸入 Gateway 名稱如 “G-John”。選取 Dialup User，於 User/Group 下拉選取 Dialup User John，併選取 Aggressive Mode。於 phase 1 proposal 下拉選單選取 phase1 proposal，如 pre-g2des-md5。於 Preshare Key 處輸入與 Netscreen Remote 相互擁有之 Key，最低不得少於 8 個字

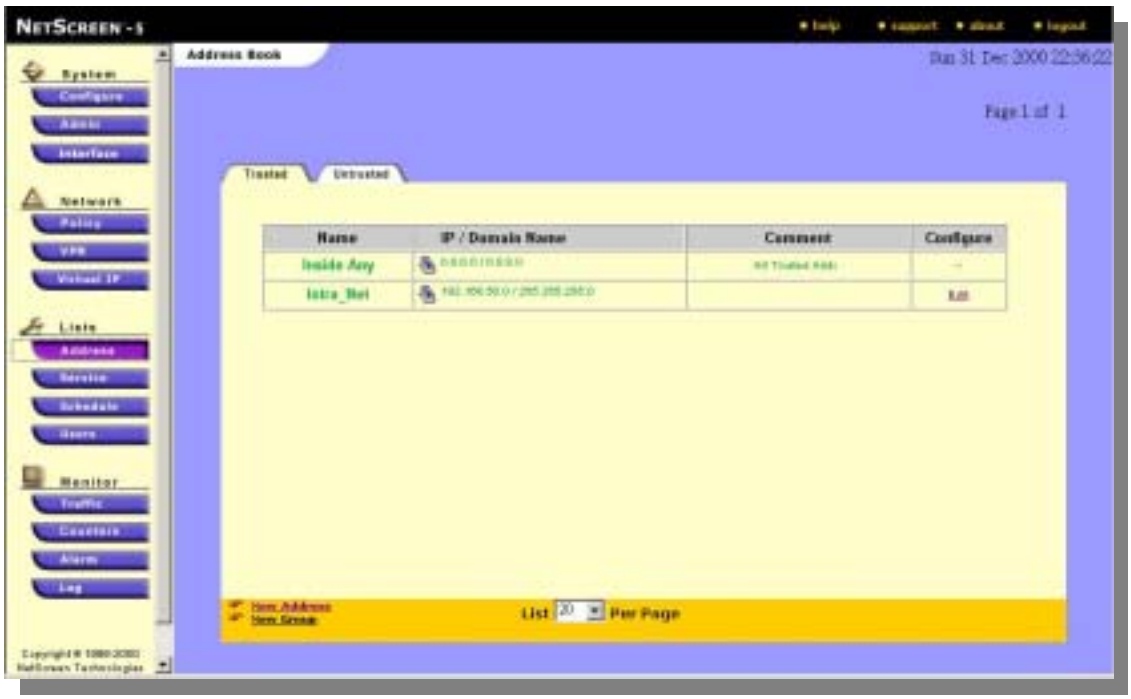

按下 ok 後，出現如下畫面：

3、點選 VPN/Auto Key IKE/NEW Antokey IKE Entry，出現如下畫面：

於 NAME 處輸入此 VPN 之名稱如 “V-John”，Enable Replay Protection 勾選或不勾選，於 Remote Gateway Tunnel NAME 處選取 “G-John”，於 Phase2 Propasal 處選取 “nopfs-esp-des-md5”


按下 ok 後出現如下畫面：


4、點選 Address/Trusted/New Address 輸入 Trusted net 之資訊，ok 後出現如下畫面


NETSCREEN - 5
Address Book
Trusted
Untrusted
Name
IP / Domain Name
Comment
Configure
Inside Any
Intra_Net
Edit
List
Per Page

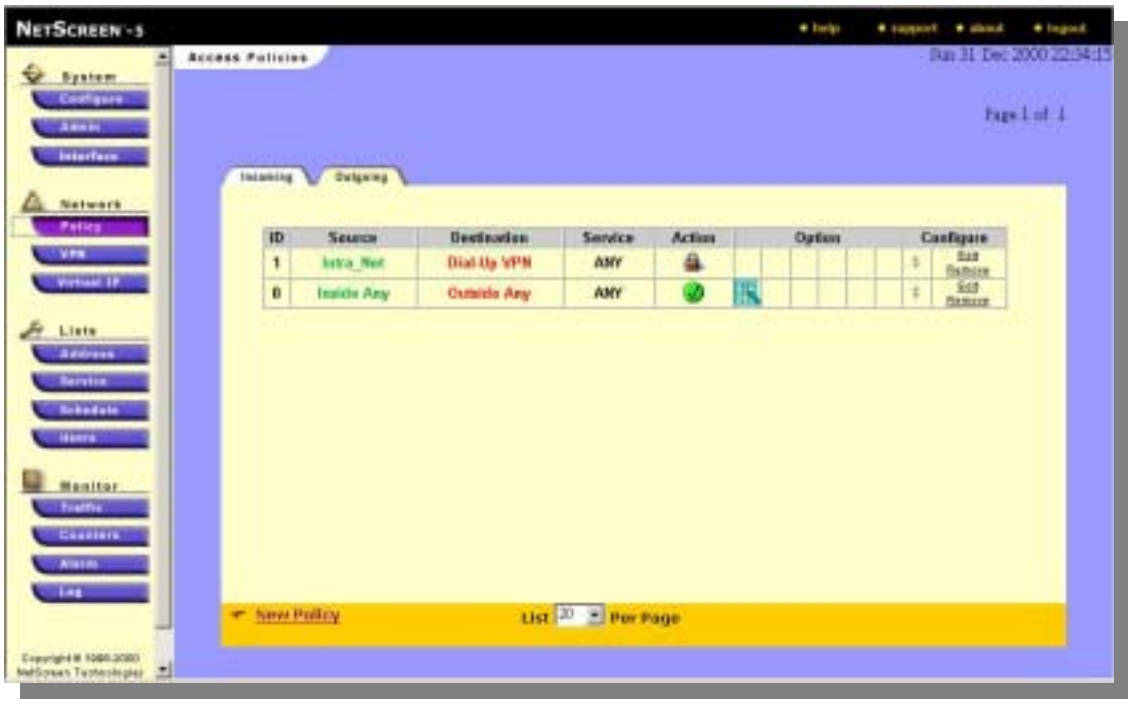
5、點選 Policy/outgoing/New Policy 出現如下畫面

於 Source Address 選取 Intra-Net,於 Destination Address 選取 Dial-up VPN

於 Service 處選取 ANY,於 Action 處選取 Tunnel

於 VPN Tunnel 選取 V-John

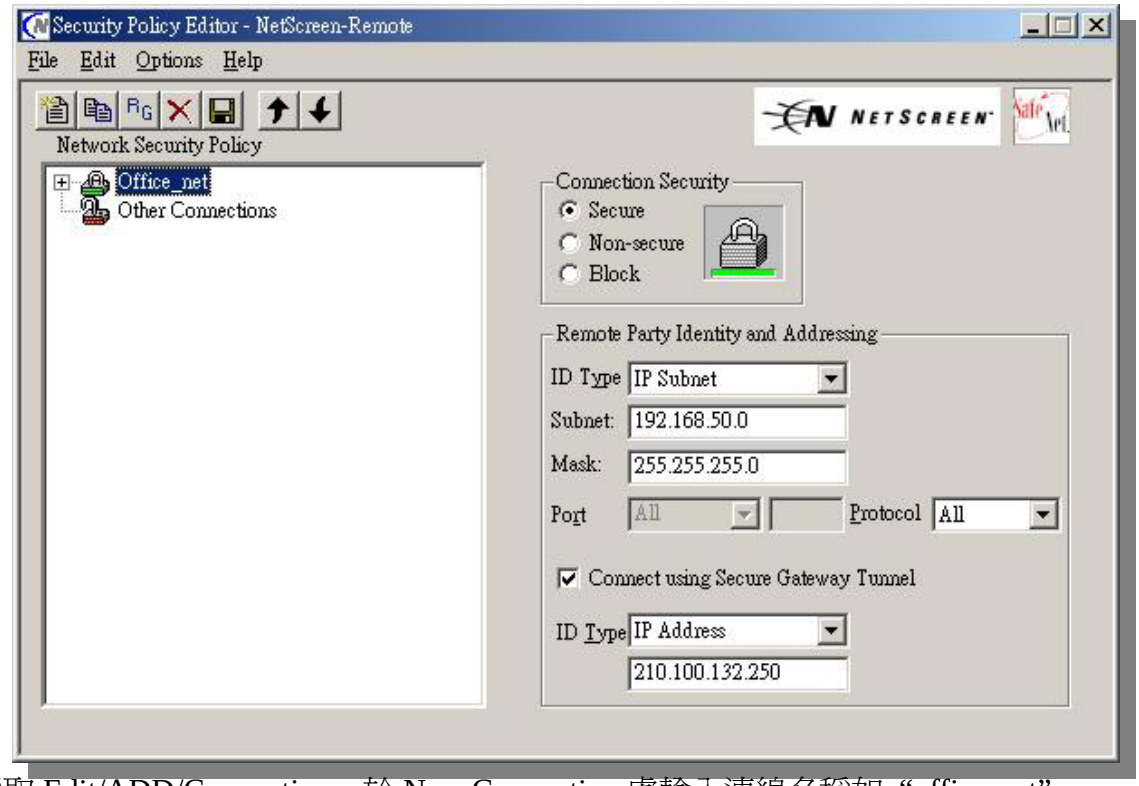

選取 ok 後出現如下畫面



6、將此 policy 上移至最前面。

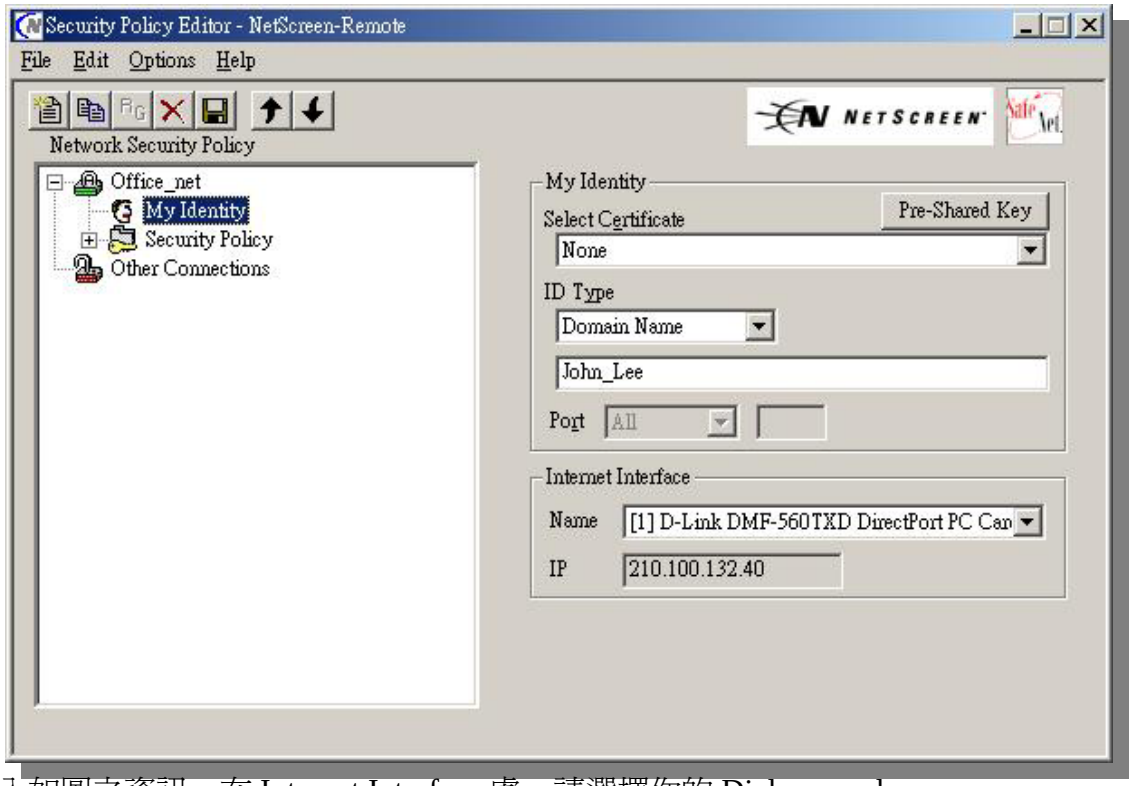
## ※ 設定步驟---Netscreen Remote

1、叫出 Security policy editor，如圖



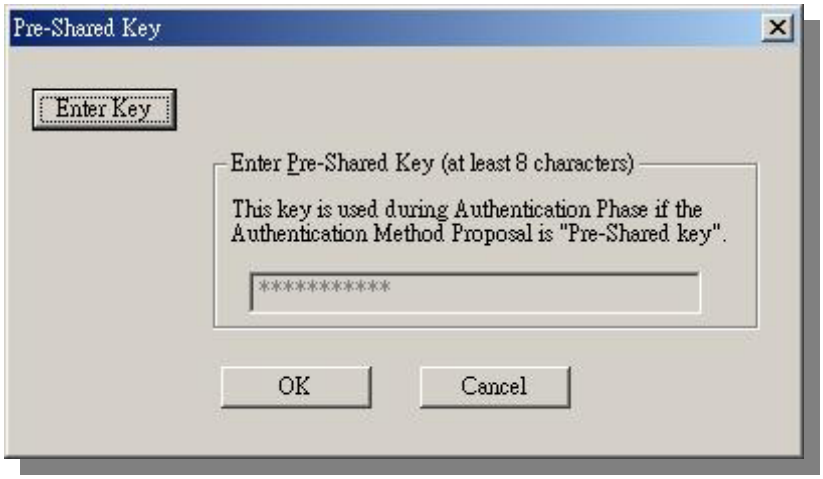

選取 Edit/ADD/Connection，於 New Connection 處輸入連線名稱如 “office-net” 並輸入如畫面上之資訊。

2、按下 “office-net”左邊之“十”鍵，出現如圖



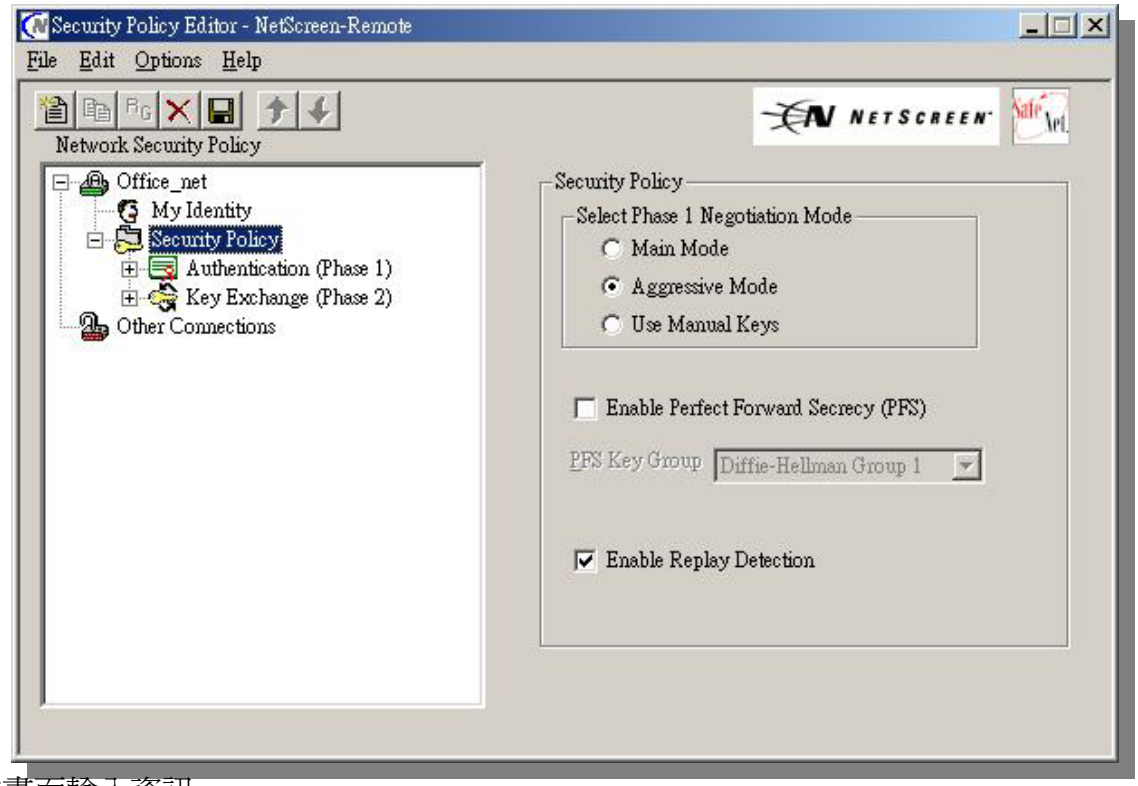

輸入如圖之資訊，在 Internet Interface 處，請選擇你的 Dial-up modem。

3、按下 Preshare key 按鍵出現如下畫面



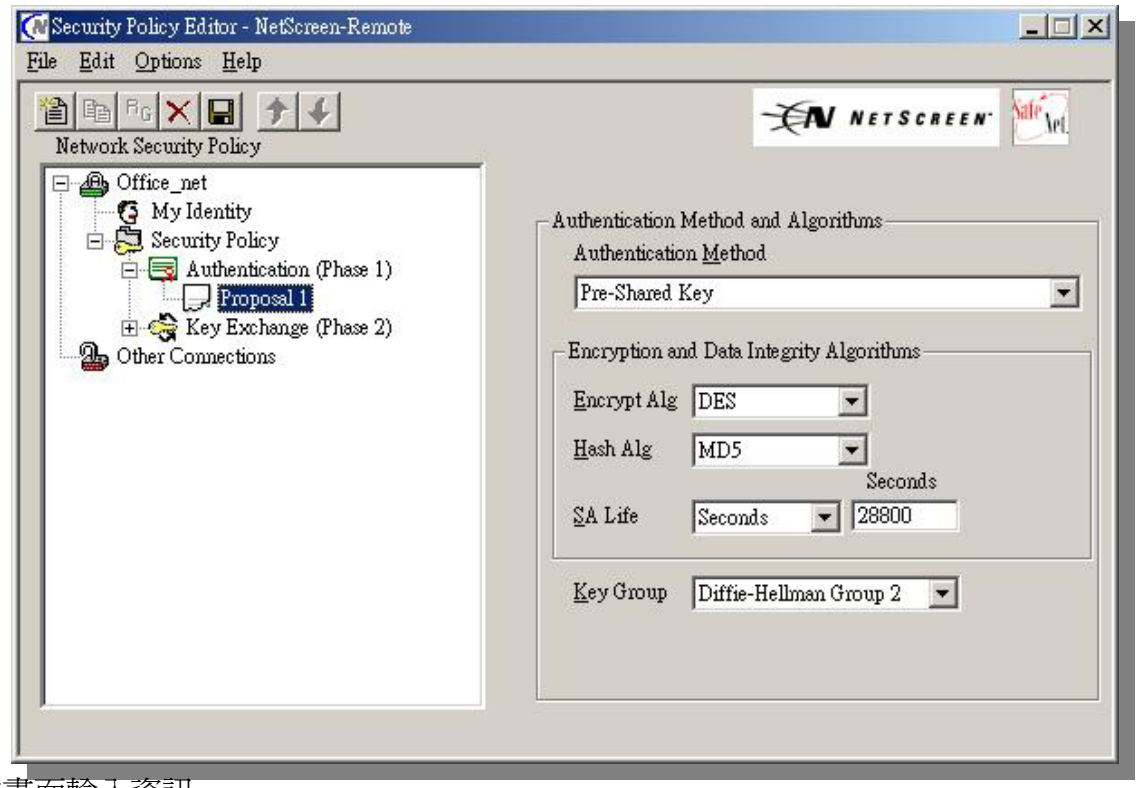

按下 Enter key 後輸入先前在 Netscreen Firewall 中輸入之 key

4、按下 Security policy 左邊“十”鍵，出現如下畫面


Security Policy Editor - NetScreen-Remote
File Edit Options Help
Network Security Policy
Office_net
My Identity
Security Policy
Authentication (Phase 1)
Key Exchange (Phase 2)
Other Connections
NETSCREEN
Security Policy
Select Phase 1 Negotiation Mode
Main Mode
Aggressive Mode
Use Manual Keys
Enable Perfect Forward Secrecy (PFS)
PFS Key Group
Diffie-Hellman Group 1
Enable Replay Detection

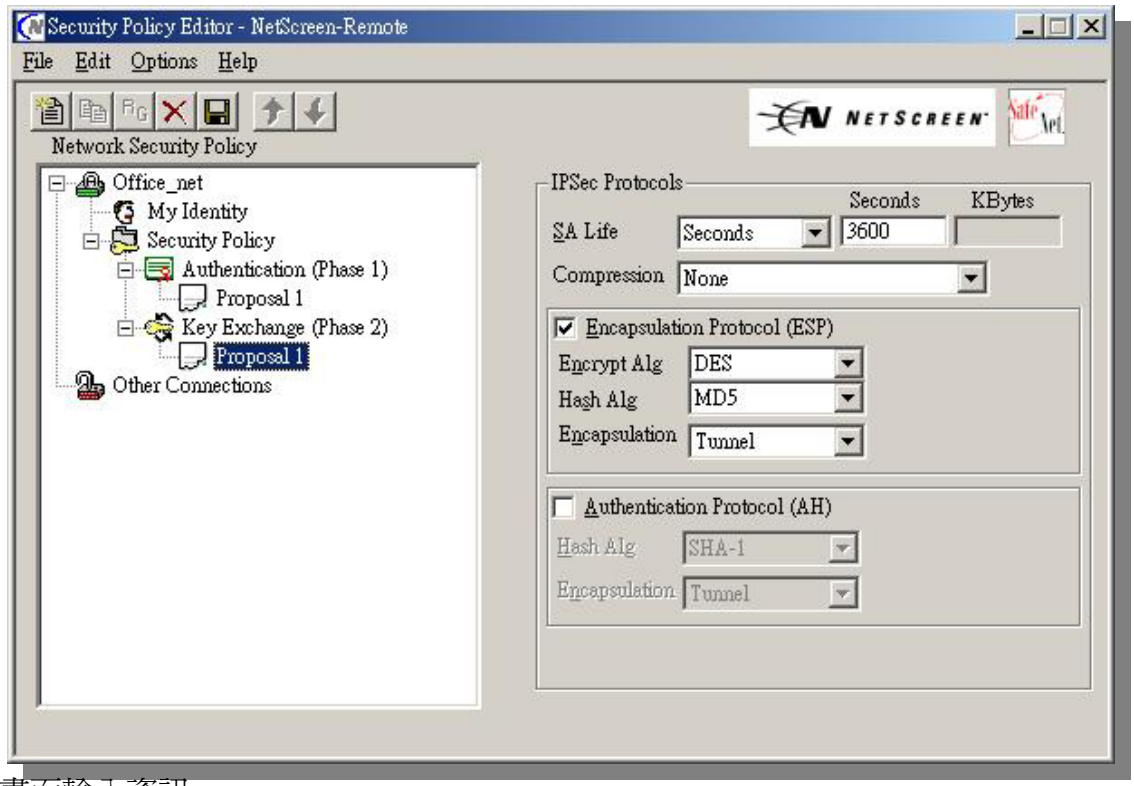
依畫面輸入資訊。

5、按下 Authentication(phase1) 左邊“十”鍵，出現如下畫面




依畫面輸入資訊。

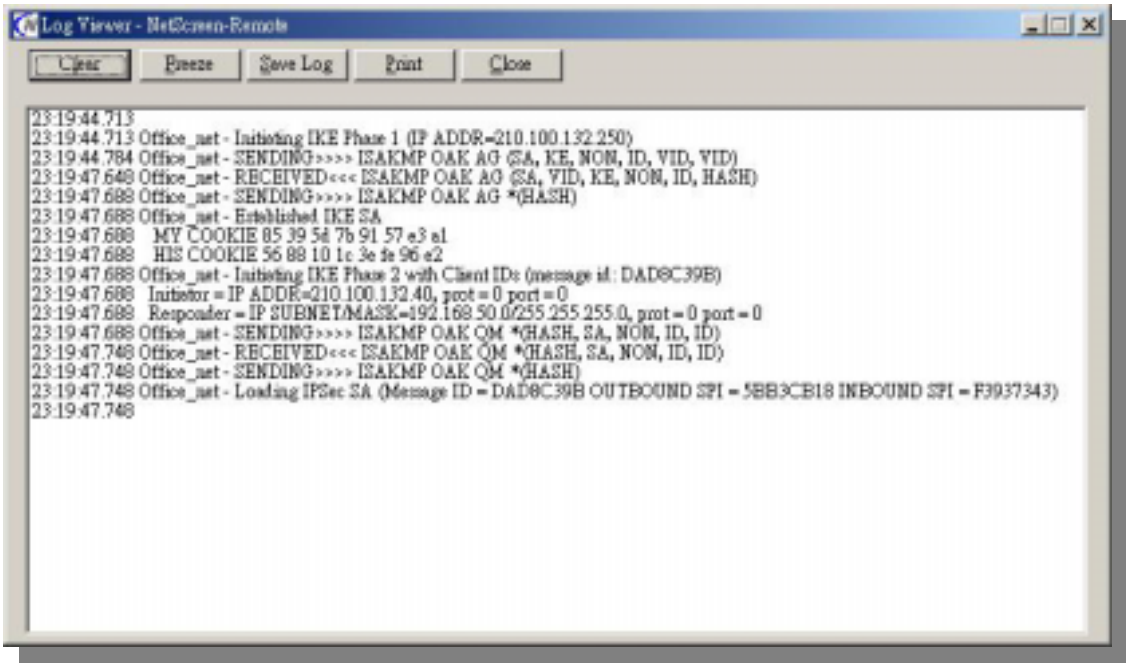
6、按下 Key Exchange(phase2) 左邊“十”鍵，出現如下畫面




依畫面輸入資訊。

※ 測試

開啓 Dos 視窗，執行 ping 192.168.50.254，前 2~3 次可能失敗，但幾次後就會得到回應。另外可叫出 Log viewer，如果設定成功則可看到類似之畫面。如圖



## 附件三：Netscreen VPN site to site 設定

**Firmware:3.0.0r2.0**

如圖所示,NS-A 與 NS-B 皆爲 NS-5XP、NATmode。

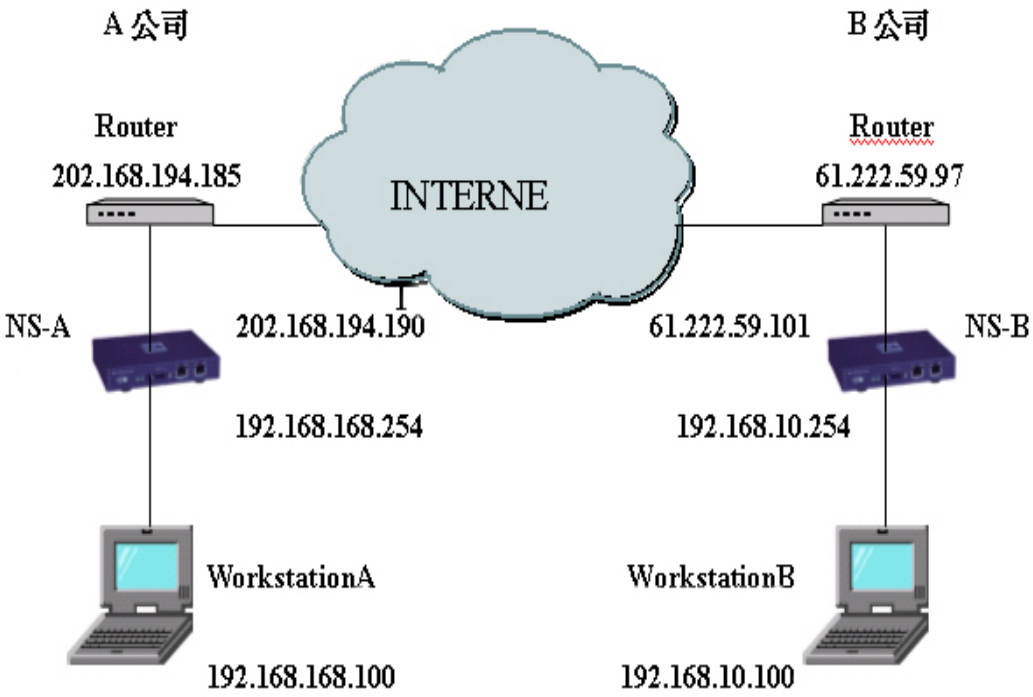
**NS-A Untrust ip** 爲 202.168.194.190

Trust ip 爲 192.168.168.254；private ip 網段爲 192.168.168.0.。

**NS-B Untrust ip** 爲 61.222.59.101

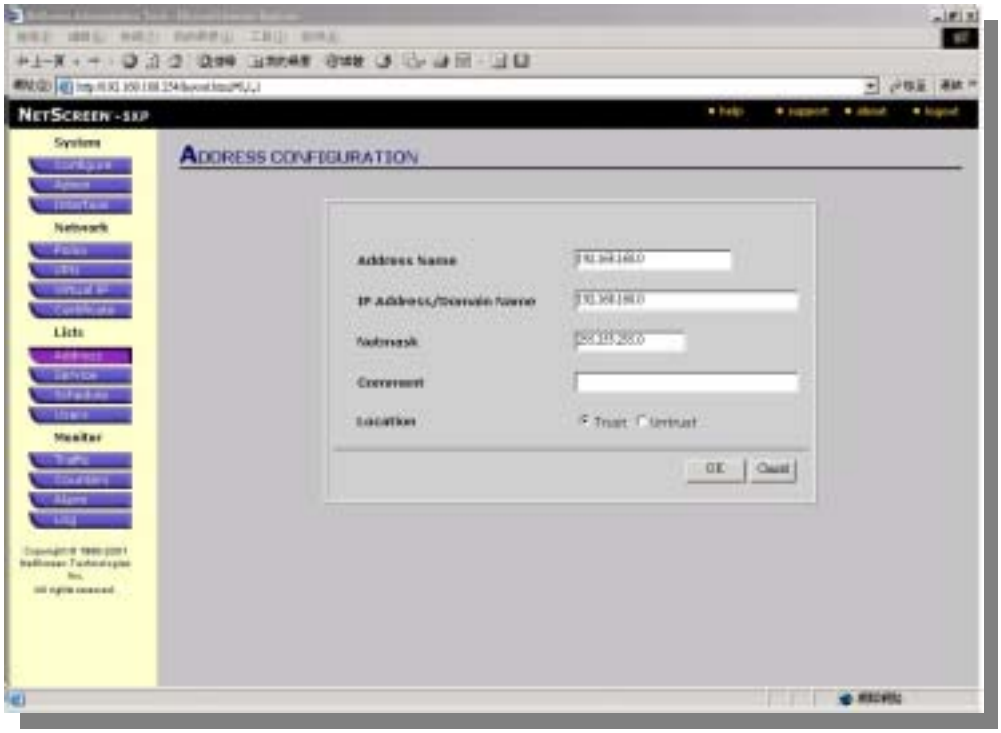
Trust ip 爲 192.168.10.254；private ip 網段爲 192.168.10.0.。

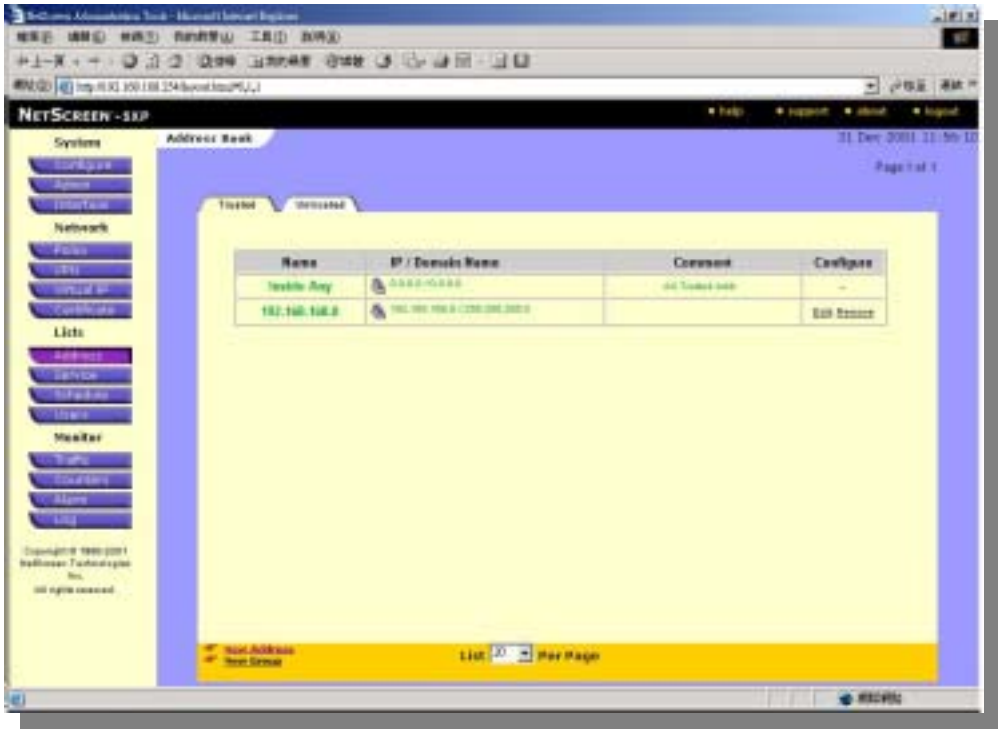
現在欲建立 NS-A 與 NS-B VPN tunnel,使 A 公司與 B 公司兩個內部網段能透過 VPN 相互存取.其設定方法如下：



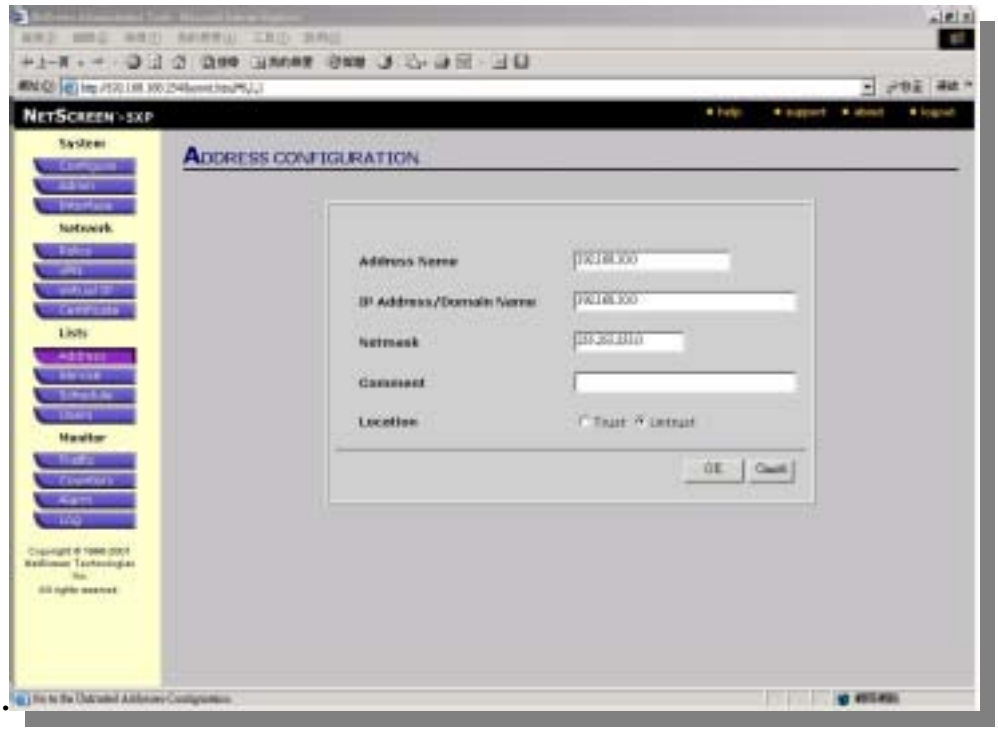
# NS-A 設定

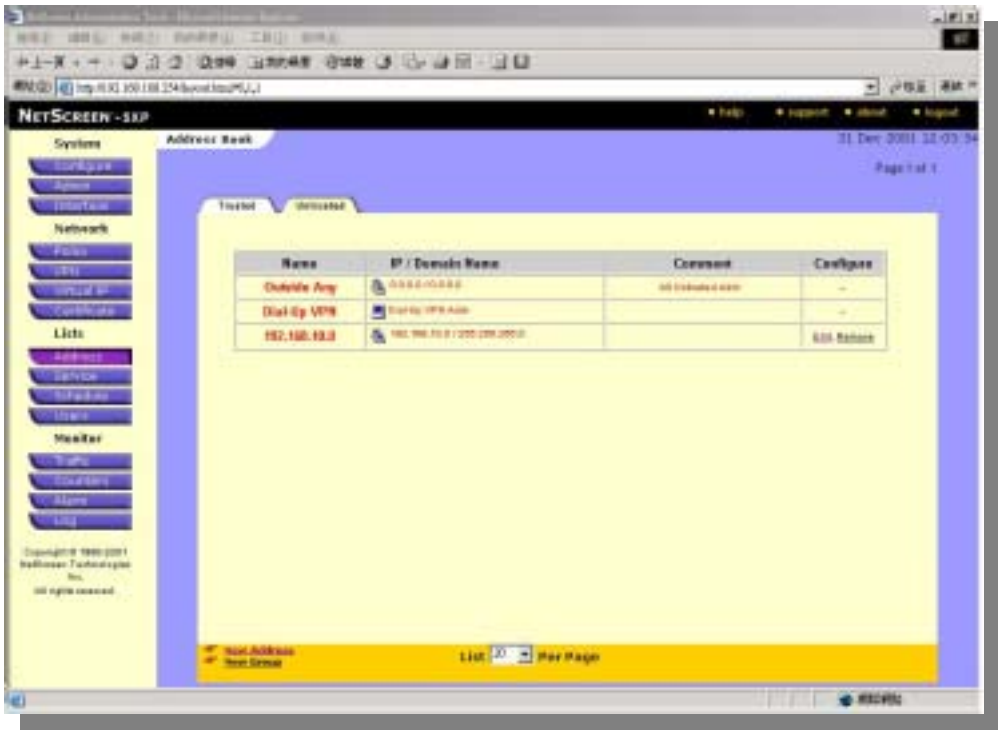
**1.** 進入 address>trust 選項,點選 new address 定義 A 公司之內部網段 ip 位址 192.168.168.0



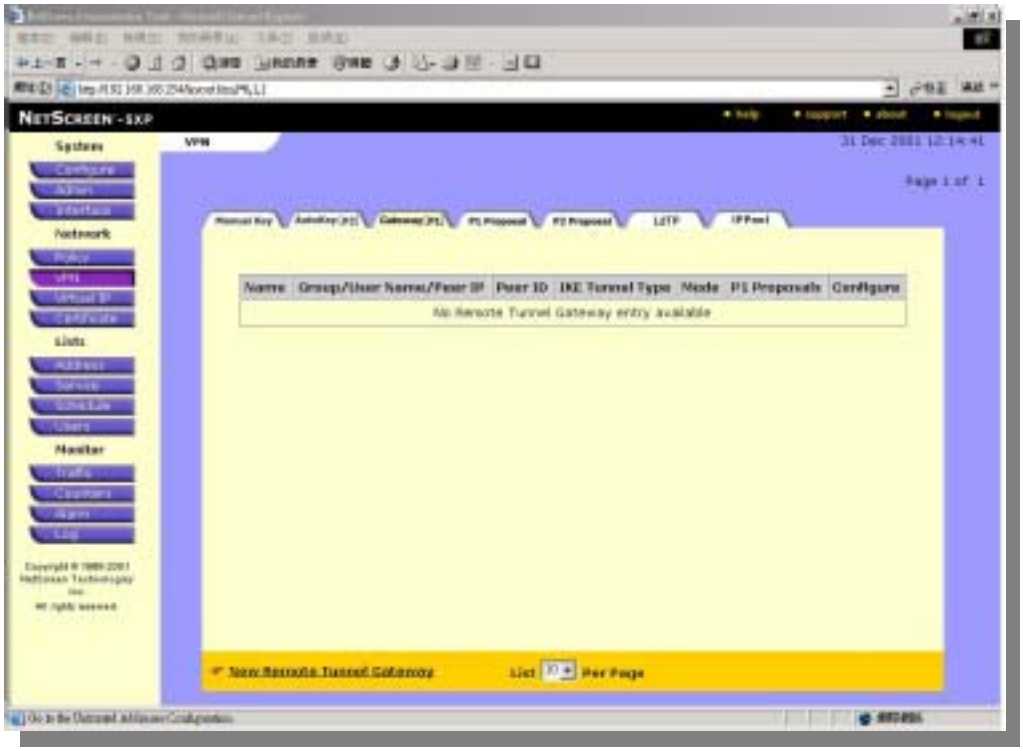



**2.** 進入 address>untrust 選項,點選 new address 定義 B 公司之內部網段 ip 位址 192.168.10.0

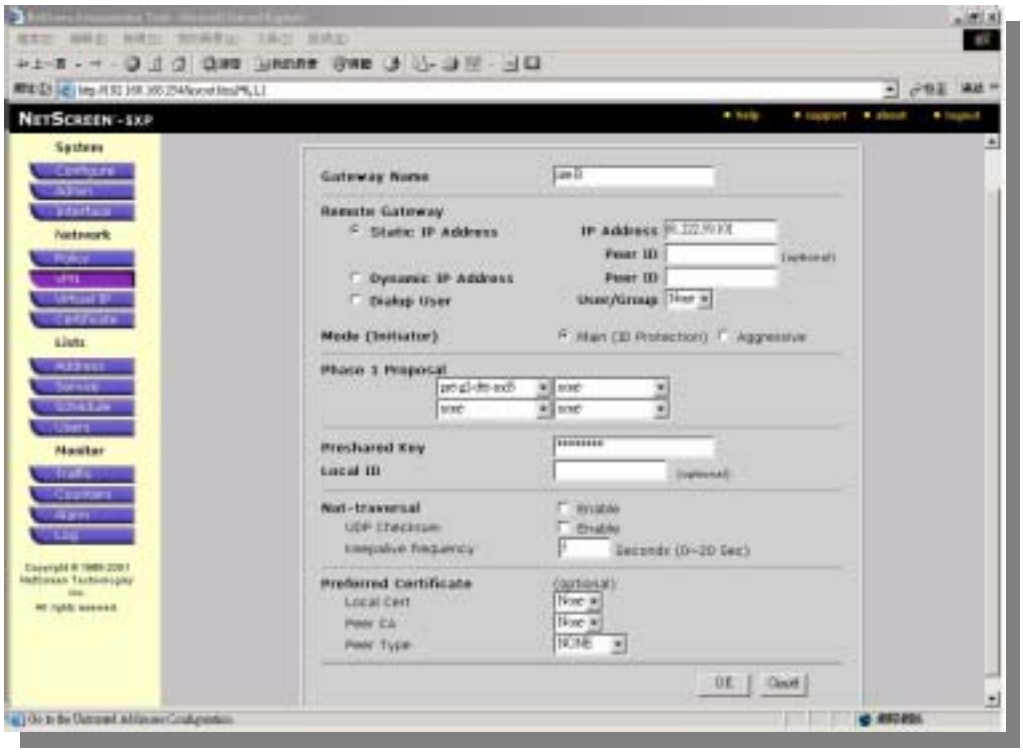


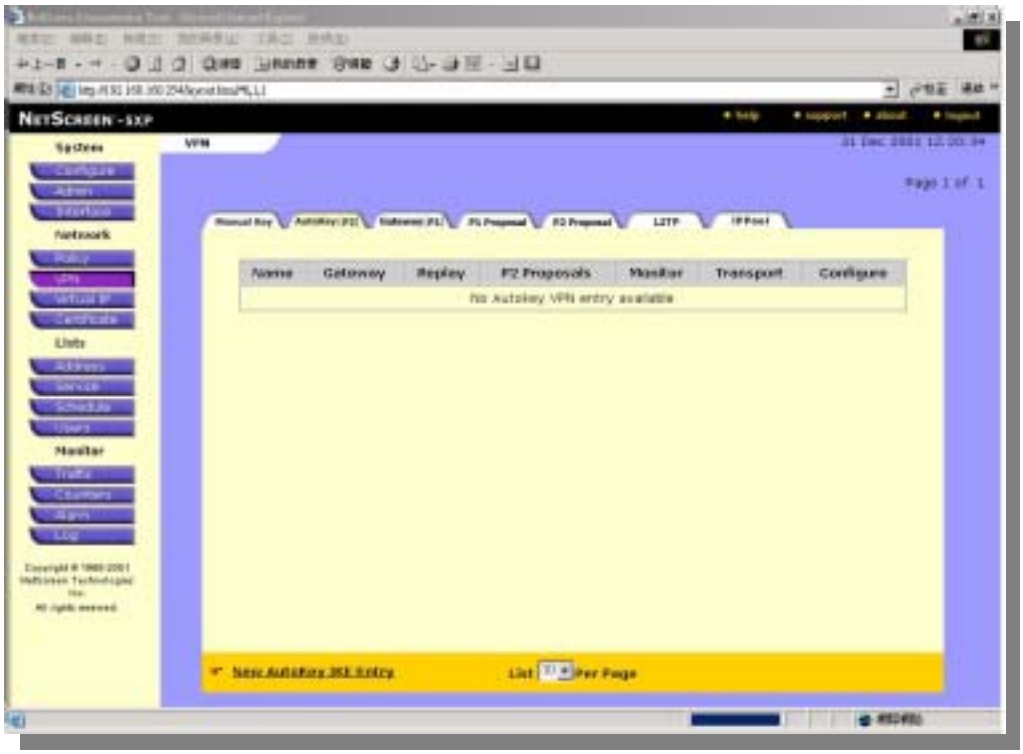
**3.**進入 VPN>Gateway>New Remote Tunnel Gateway



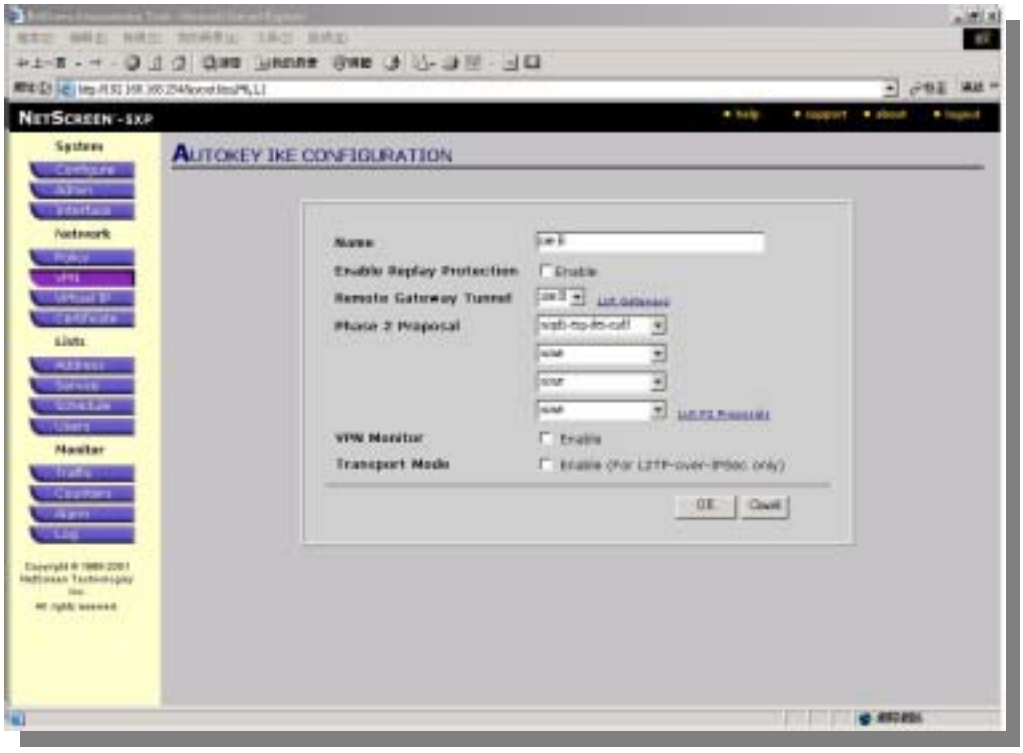

**4.**Gate**w**ay name 爲 siteB,IP address 爲 B 公司的 Netscreen untrust ip,61.59.35.90;Mode 採用預設之 Main Mode;Phase 1 Proposal 爲設定加密與認證的方法(註 1);Preshare key 設定輸入 87654321(註 2):以上設定完後,按下 ok



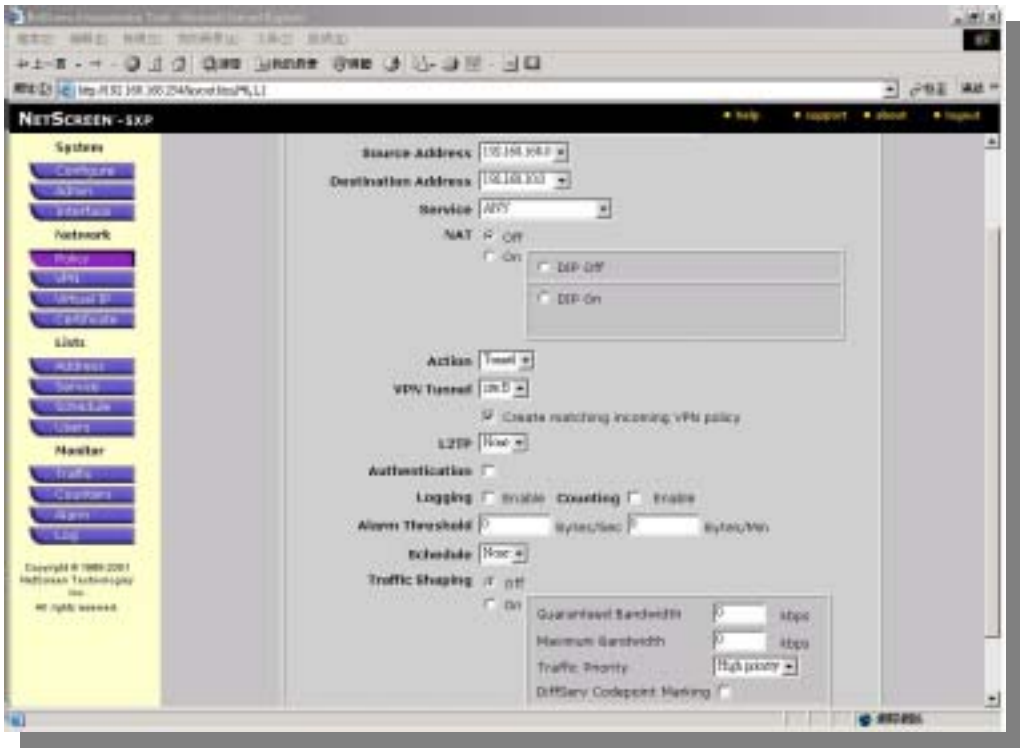
**5.**點選 Autokey>New Autokey IKE Entry



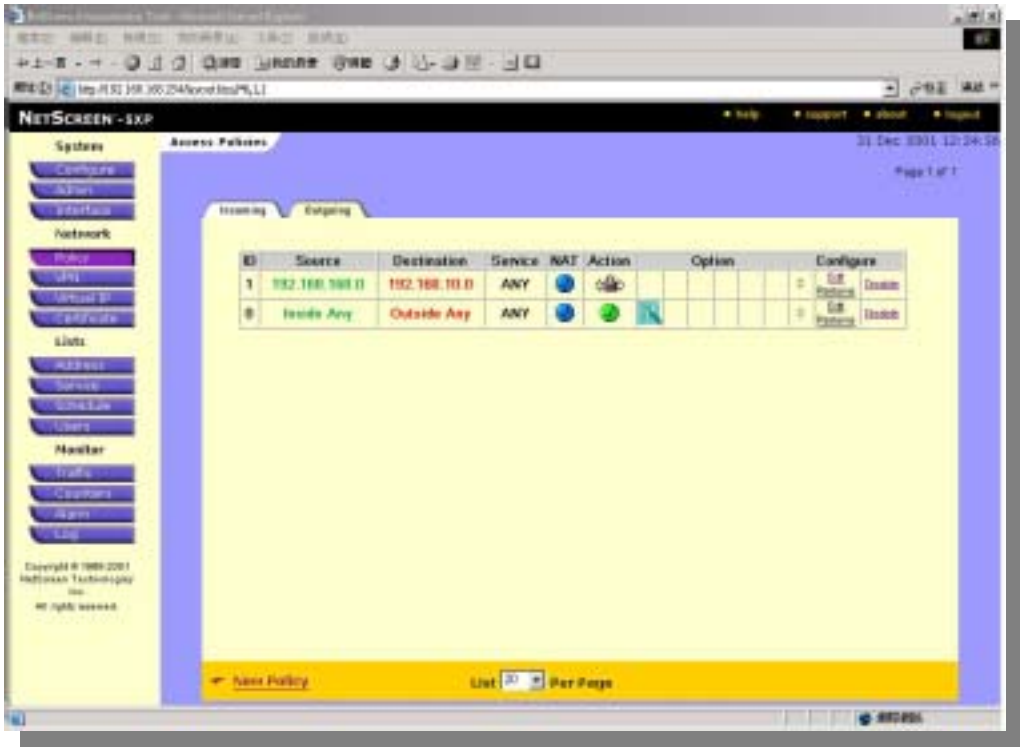

**6**.輸入 Name,siteB,按下 ok



**7.**進入 Policy>Outgoming>New Policy,Source Address 爲 192.168.168.0， Destination Address 爲 192.168.10.0,Service 爲 any,Action 選 Tunnel,
VPN tunnel 選剛建好之 site B.勾選 Create matching incoming VPN policy 按下 ok 後即可.

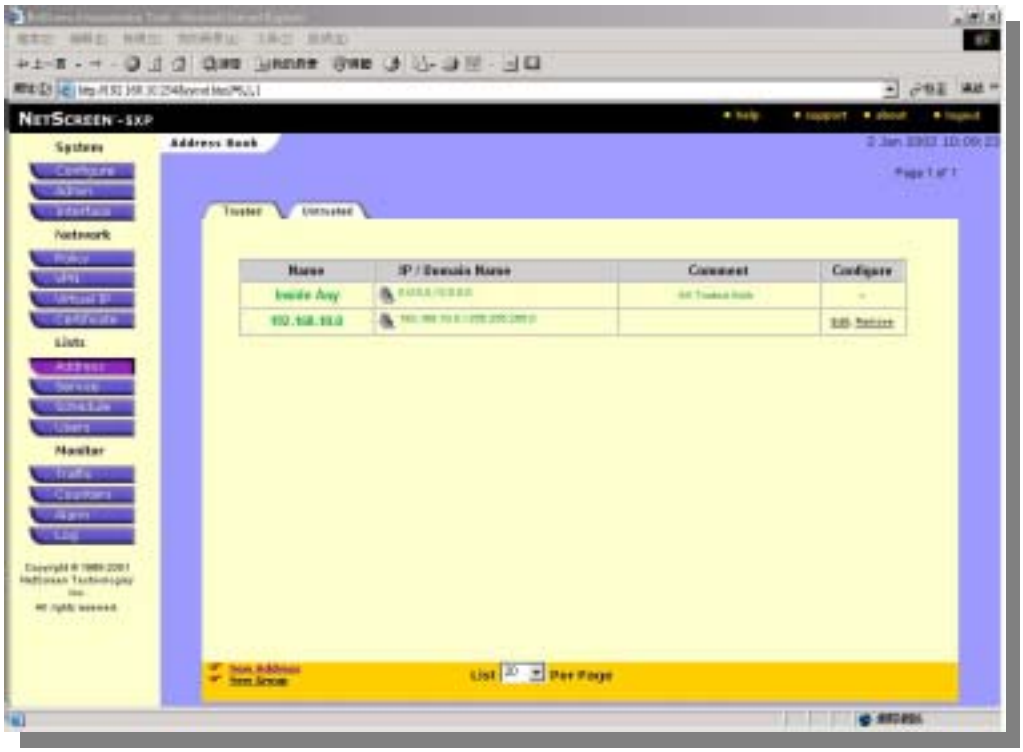



**8.**將 VPN policy 移置最上層,即完成 siteA 設定(註 3)

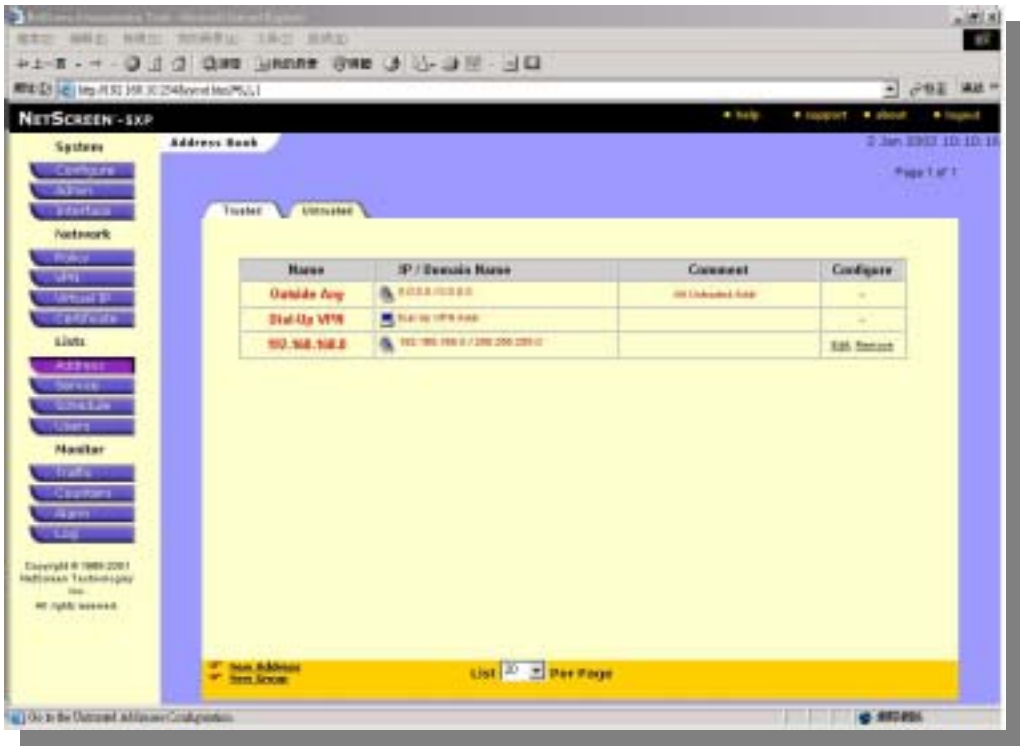


# NS-B 設定

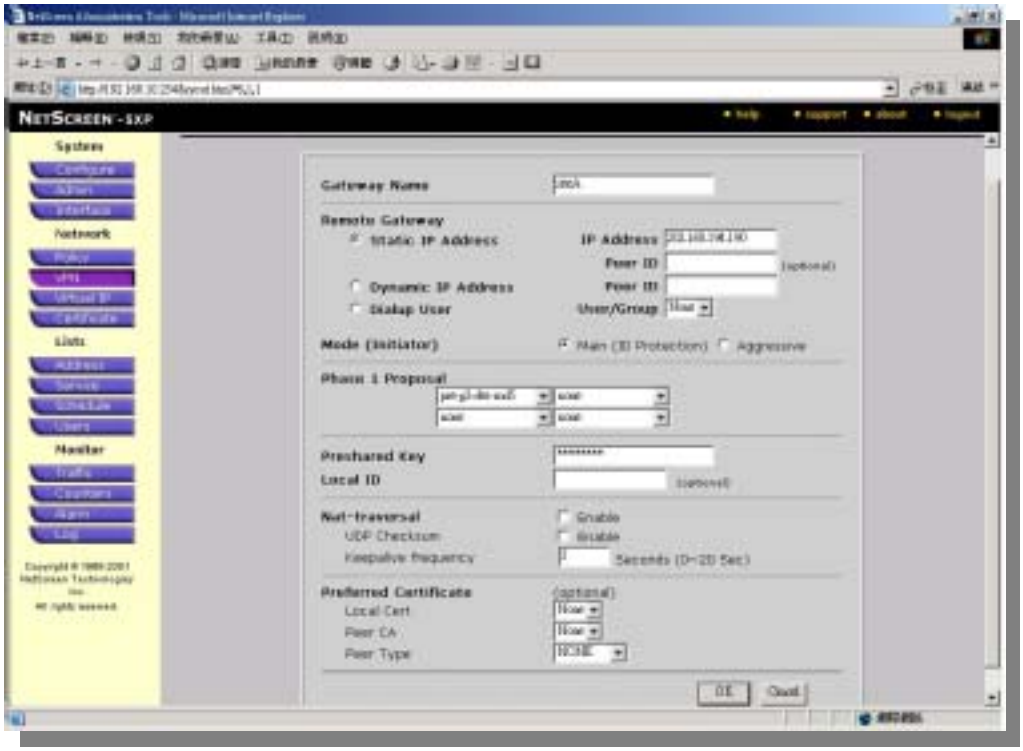
**1.** 進入 address>trust 選項,點選 new address 定義 B 公司之內部網段 ip 位址 192.168.10.0



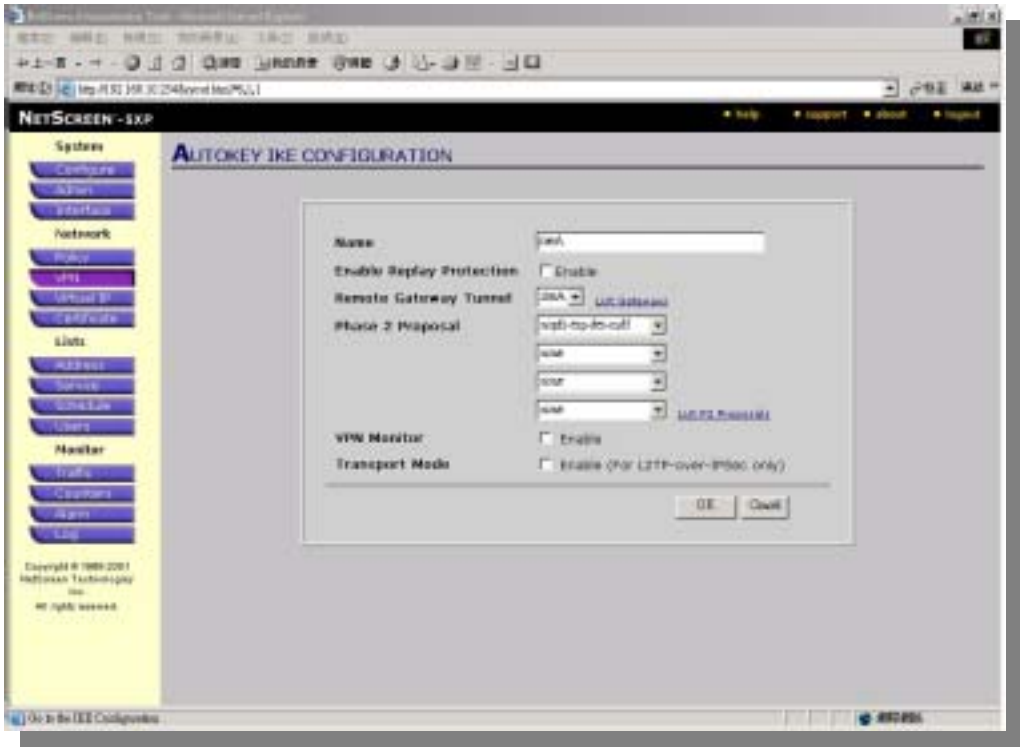

**2.** 進入 address>untrust 選項,點選 new address 定義 A 公司之內部網段 ip 位址 192.168.168.0



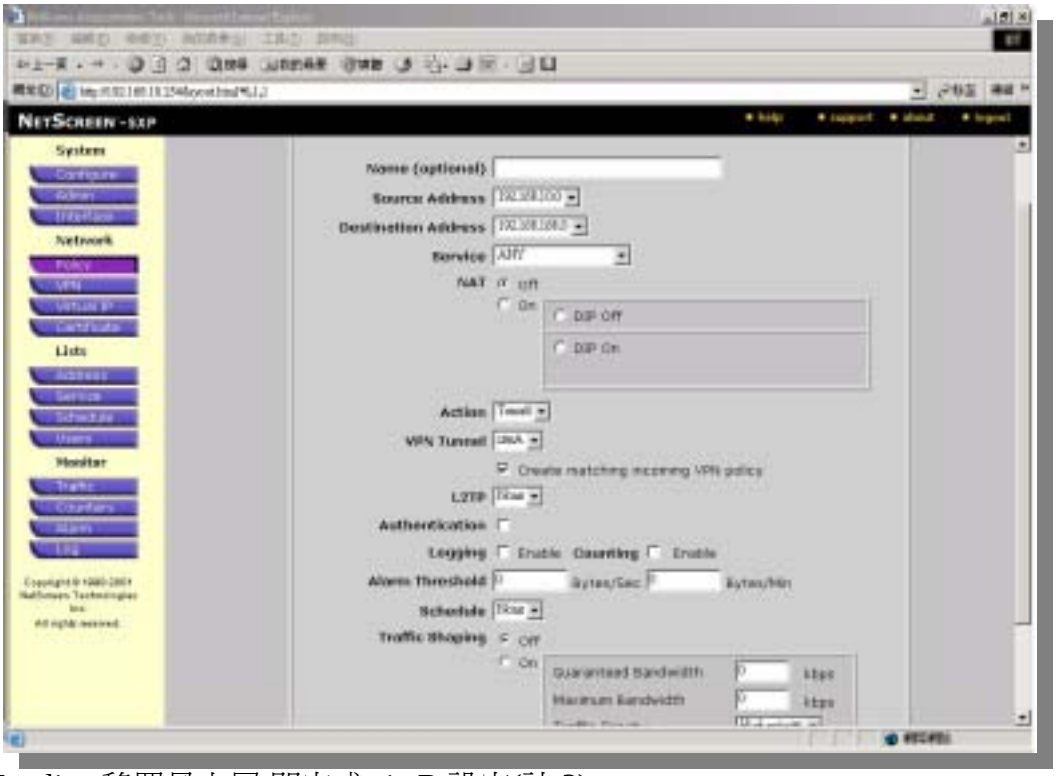
**3.**進入 VPN>Gateway>New Remote Tunnel Gateway, Gateway name 爲 siteA,IP address 爲 A 公司的 Netscreen untrust ip,210.134.101.254;Mode 採用預設之 Main Mode;Phase 1 Proposal 爲設定加密與認證的方法(註 1);Preshare key 設定輸入 87654321(註 2):以上設定完後,按下 ok.



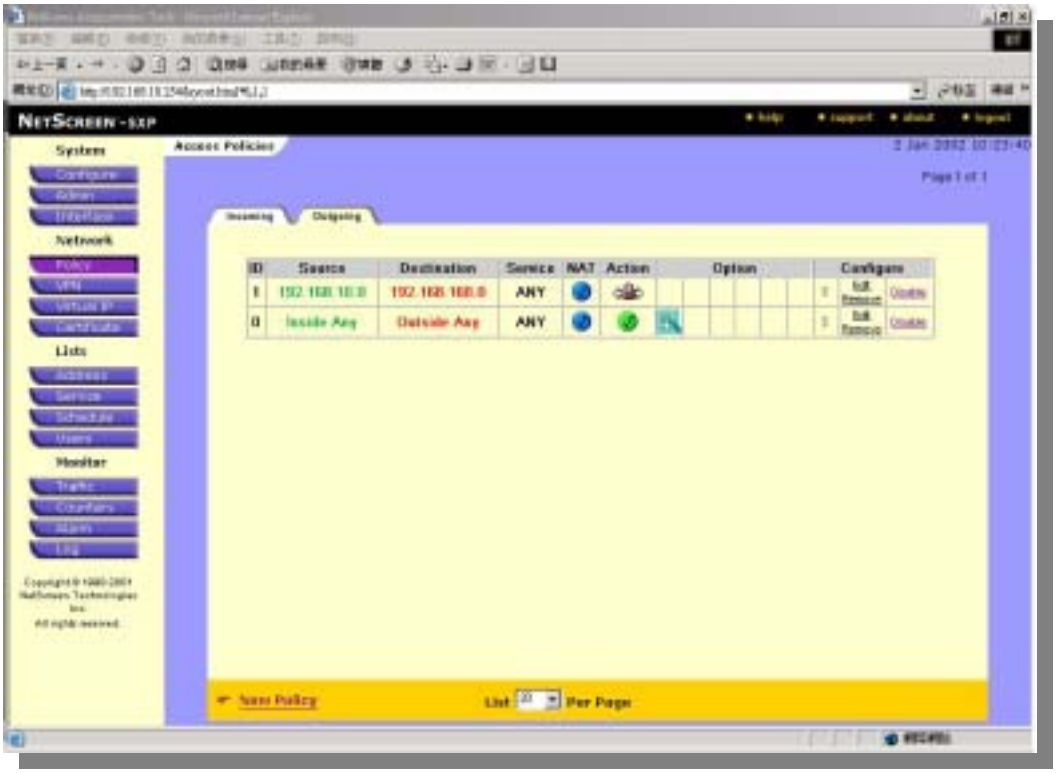

**4.**點選 Autokey>New Autokey IKE Entry, 輸入 Name,siteA,按下 ok.



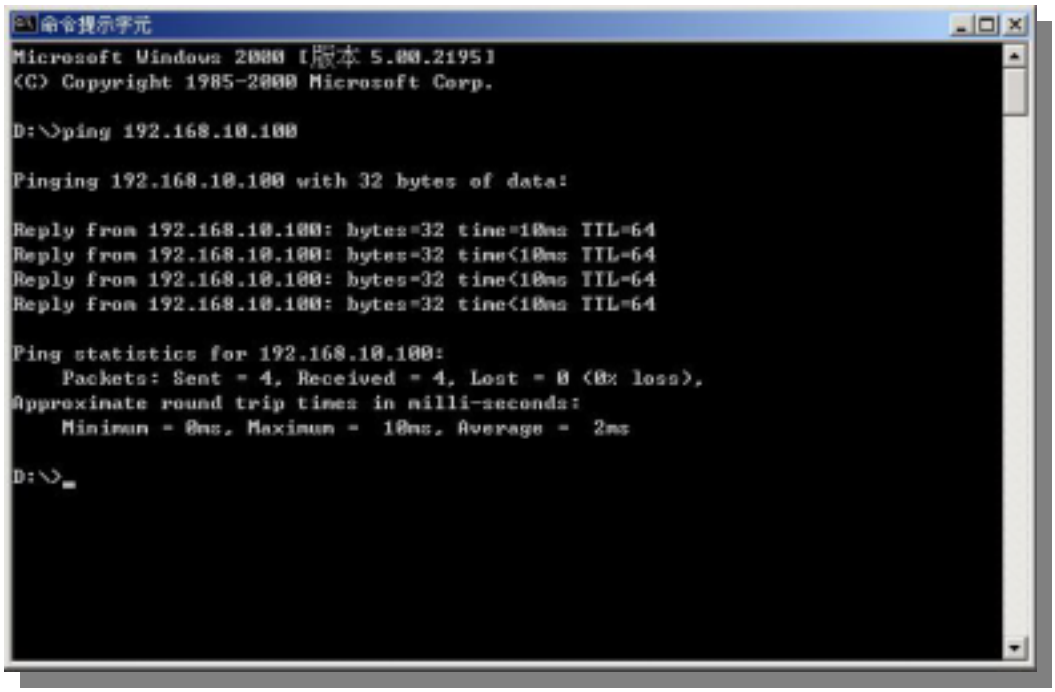
**5.** 進入 Policy>Outgoming>New Policy,Source Address 爲 192.168.10.0,Destination Address 爲 192.168.168.0,Service 爲 any,Action 選 Tunnel,VPN tunnel 選剛建好之 siteA.勾選 Create matching incoming VPN policy,按下 ok 後即可




**6.**將 VPN policy 移置最上層,即完成 siteB 設定(註 3)



當 siteA 與 siteB 設定完後,VPN tunnel 已建置完成,192.168.168.0 與 192.168.10.0 的網段可經由在加密與認證的 tunnel 透過 internet 傳遞資料.
測試方法即 WorkstationA(192.168.168.100) ping WorkstationB(192.168.10.100 能成功 ping 到.




如欲更詳細的解說與設定,可參考隨貨附上的光碟片,內附 Netscreen Concepts&Examples 的 PDF 檔(約 11.5MB),或是到 Netscreen 網站上下載到最新相關手冊.

**註 1.**此處爲設定加密認證的方式,重點在於 NS-A 與 NS-B 必需使用相同的加密認證方式.

**註 2.**preshare key 可輸入數字與英文符號,不可輸入中文與符號,有分大小寫,最大可到 31 個字元.NS-A 與 NS-B preshare key 必需相同.

**註 3.**必須將所有 VPN Policy 移至 Policy 最上層,Incoming 與 Outgoing Policy 皆要上移.

# 附件（四）何謂 DMZ

1、DMZ

DMZ 術語來自於軍事領域，原意爲禁止任何軍事行爲的區域即非軍事區。在技術領域，DMZ 最初被定義爲防火牆的外部介面和外部路由器的內部介面之間的網路段。後來 DMZ 的定義進一步演化，是指爲不信任系統提供服務的孤立網路段。現在 IT 人員用這個術語來指兩個防火牆之間的網段，或是連接防火牆的“死端”的網路。

不管 DMZ 的種種定義，它的目的就是把敏感的內部網路和其他提供訪問服務的網路分離開，爲網路層提供深度的防禦。防火牆上的策略和訪問控制系統定義限制了通過 DMZ 的全部通信資料。相反，在 Internet 和企業內部網之間的通信資料通常是不受限制的。

2、DMZ 的主要作用

DMZ 的主要作用是減少爲不信任客戶提供服務而引發的危險。DMZ 可以爲你的主機環境提供網路級的保護，它還把公衆主機設備和私有網路設施分離開來。例如，如果你公司有一個 WEB 站點，任何人可以通過瀏覽器和它連接。沒有 DMZ 配置時，你的主機系統位於防火牆的外部（暴露在 Internet 上）或位於公司內部網中的網路段上。前一種情況你的 WEB 主機對所有攻擊都是開放的，沒有任何防禦。後一種情況會導致其他的內部資源受到攻擊。通過 DMZ 可以在保護內部網路時，同時保護到 Internet 伺服器。

DMZ 在保護企業內部其他資源的安全方面也發揮重要作用，當有些資源僅供少數人訪問時，可以把相應系統隔離，從而提供安全性。

一個內部的 DMZ 是上面我們提及的自我服務的 HR 企業內部互聯網的理想模型。DMZ 保護了 WEB 應用程式伺服器和資料庫系統。

大多數人認爲防火牆提供的是堅固無比的防護，實際上，內部網路和主機的安全通常並不是那樣的堅固。在一個非 DMZ 系統中，提供給 Interent 的服務產生了許多漏洞，使其他主機極易受到攻擊。

解決問題的方法之一是把沒有包含敏感資料，擔當代理資料訪問職責的主機放置於 DMZ 中。通過應用程式的介面（例如：WEB 站點），或通過網路協定（例如：HTTP 或 SQLnet）可以實現上述方法。在網路中資料從應用層分離提供了附加的安全，因爲實施 DMZ 的系統不會把包含商業資料的內部系統直接暴露給網路攻擊。攻擊者取得初步入侵成功後要面臨 DMZ 設置的新的障礙。

## 附件（五）何謂 SSL

SSL（Secure Socket Layer Protocol）網路資料傳輸的安全協定：
爲了避免交易相關資料於傳輸過程被截取破壞等因素，Netscape Communications 公司 1995 年 6 月所提出了這個協定，使傳輸資料時得以確保資料的隱密性、完整性、身份的確認，目前已經成爲一種開放性的安全標準機制。也爲大多數電子商務網站所採用。

SSL 能夠讓主從式架構的應用（瀏覽器和 Web 伺服器）安全的進行溝通，簡單來說就是建立起客戶端和伺服器之間的安全通道。

SSL 是介於傳輸層（Transport Layer）與應用層（Application Layer）之間的安全機制，它能對 TCP/IP 以上（如 http、telnet、ftp 等）的網路協定作資料的加密，而其所採用到的密碼技術有兩種：訊息加密和解密、數位簽章與簽證技術。

一般電腦上的瀏覽器（IE 或 Netscape 等）皆有支援 SSL 技術，且會以「https://」和「http://」來區分是否是支援 SSL 的網頁，其中的「s」就是「Secure」的意思。

SSL 包含 SSL Record Protocol 、Handshake Protocol、Change Cipher Spec Protocol 等幾個部份。其中 Record Protocol 是 SSL 的底層協定，功能是將資料加以壓縮加密轉換成 MAC（Message Authentication Code），當接收者確認後會再將其解壓及解密。

Handshake Protocol 屬於 SSL 的上層協定，負責雙方通訊的安全參數。而 Change Cipher Spec Protocol 只有在使用者需更改到其所加密資料的密碼時才會用到。

目前線上購物方面，商家的伺服器上必需有 SSL 的「數位憑證」才能在網路上以 SSL 的安全機制進行交易，而 SSL 所使用的是 RSA 公司授權的「公開金鑰加密法」，一般皆必需申請私人「數位憑證」加裝於伺服器上才能支援 SSL。

基本上 SSL 提供：資料的機密性、伺服器的個體識別、客戶端的個體識別三種安全防護。
由於 SSL 是直接將資料（如信用卡號及個人資料）加密，單單在客戶端與商家間建立安全通道，如此除了很容易將資料暴露在別人面前外，此種簡單的加密技術也容易被不法駭客以「Traffic Analysis 攻擊法」所侵犯。

另外因爲 IP 並未加密，其來源及目的位置也會輕易被知道，或從 TCP 的 Port 號碼及資料量大小來分析是何種應用，其資料都很容易被竊取。

因此要如何才能夠更安全的在網路上進行交易便成了極受重視的問題。目前認定 SET（安全電子交易標準）比 SSL 更安全，不過因爲 SET 申請手續複雜，所以在市場上並不如 SSL 普遍。

## 附件（六）何謂 SET 電子安全交易規則

在網路電子交易安全的要求不斷地被提出後，爲了達到交易安全及符合市場的經濟效益成本考量，一些世界性的發卡認證組織如 VISA、MasterCard 及國際資訊電腦公司如 IBM、Microsoft、Netscape、GTE、Terisa 和 Verisign 等，共同制定了電子安全交易（Secure Electronic Transactions 簡稱 SET）規格。

它是一個用來保護在任何網路上付款交易的開放規格，以保護任何開放型網路上個人和金融資訊的隱密性。

電子安全交易規格（SET）有幾項基本要件：

1. 數位電子證書

數位電子證書是 SET 的核心，因爲它提供了簡易的方法來讓交易的雙方能夠彼此信任。數位電子證書利用訊息加密的方式，將交易訊息轉換或加密成需要使用鑰匙（KEY）的密碼，要解釋或轉換該訊息，接收者就需要擁有一把密碼鑰匙才可。

2. 數位電子簽名

數位電子簽名係利用公開鑰匙加密（public key cryptograohy）的製碼技術所延伸出的另一項電子安全交易要件。

讓我們以最簡單的方式解釋數位電子簽名：志明在網路上需要向申請電子證書的銀行證明自己的身分，志明只需利用私人鑰匙送出一項訊息送給發卡銀行，銀行再以數位證書上的公開鑰匙加以解密，如果銀行能成功解開這項訊息，就能證明網上交談的客戶就是志明本人。這種驗明客戶正身的動作及技術專家稱爲「電子數位簽名」。

SET 是使用訊息的加密方式，而非通道的加密方式，對消費者或商家都來得要有保障。因爲 SET 會將一個購物的要求拆成兩個部份－訂單資訊（Order Information，OI）與付款資訊（Payment Information，PI），每個訊息都會再經過一個訊息摘要演算，分送給不同層級(消費者、商家、收單銀行、發卡銀行及 CA〔電子證書管理中心〕)、，並使用對稱與非對稱式的加密方式，也採用一對公開與私人金鑰的認證方式，不同層級所能看到的資訊並不相同，也因此具有絕佳的交易安全性與穩私性。

目前網路安全管理機制最常見的方式就是「密碼」。由於密碼在網路交易上並無任何可供辨識之實體存在，且交易雙方均持有相同的密碼，若僅依靠密碼作爲身份辨識之依據，其危險程度相當高。例如：駭客入侵網站取得密碼資料或猜中用戶的密碼（用戶常用自己的生日、身份證字號、電話號碼設定密碼），駭客即可代表客戶對網站進行交易。此外，缺乏事後不可否認交易的功能，亦是密碼機制無法廣泛運用於電子商務的主要原因之一。

爲改善上述密碼之缺點，目前業界大多採用 RSA 非對稱式亂碼技術確保網路交易安全。此一技術是目前業界及學界公認最安全已成熟之技術。在此機制中，每個用戶均擁有一把公開金鑰（public key）及一把私密金鑰（private key）。這兩把金鑰並不相同，但互相對應。其特性如下：

＊ 經過私密金鑰加密過之資訊僅能由對應之分開金鑰正確解密。

＊ 無法利用公開金鑰推算出私密金鑰。

基於此特性，我們可使用私密金鑰對資料進行數位簽章（digital signature）之工作。並使用公開金鑰對資料進行驗證簽章之動作。只要資料經過數位簽章後，任何對資料之竄改均可於驗證簽章時檢查出來；如此一來，數位簽章即能與傳統印鑑具備相同的功能。由於私密金鑰能代表使用者簽署電子文件；因此，使用者必須妥善保管私密金鑰，正如同保存印章一樣。在擁有可供運用的 PKI 應用技術後，即須依賴憑證機構簽發憑證，供網路交易使用，確保雙方權益。