Multi-Homing Gateway

使 用 手 册

目　　录

负载平衡器硬件安装

一、 负载平衡器硬件外部接口说明：

图 H-1 负载平衡器接孔、指示灯说明

- **Power LED**：电源显示
- **Status LED**：当 LED 灯为开始闪烁时，表示系统正在开机状态，约一分钟后系统开机程序结束，当 LED 停止闪烁，表示系统已开机成功。
- **RESET**：将负载平衡器回复到原厂默认值。
- **LAN Port**：内部网络接口，将企业内部的网络连结在此网络。
- **WAN 1/2 Port**：外部网络接口 1 / 2，与外部路由器连结。
- **DMZ Port**：非军事区网络接口，将企业内的服务器连结在此网络

二、 负载平衡器连接图：

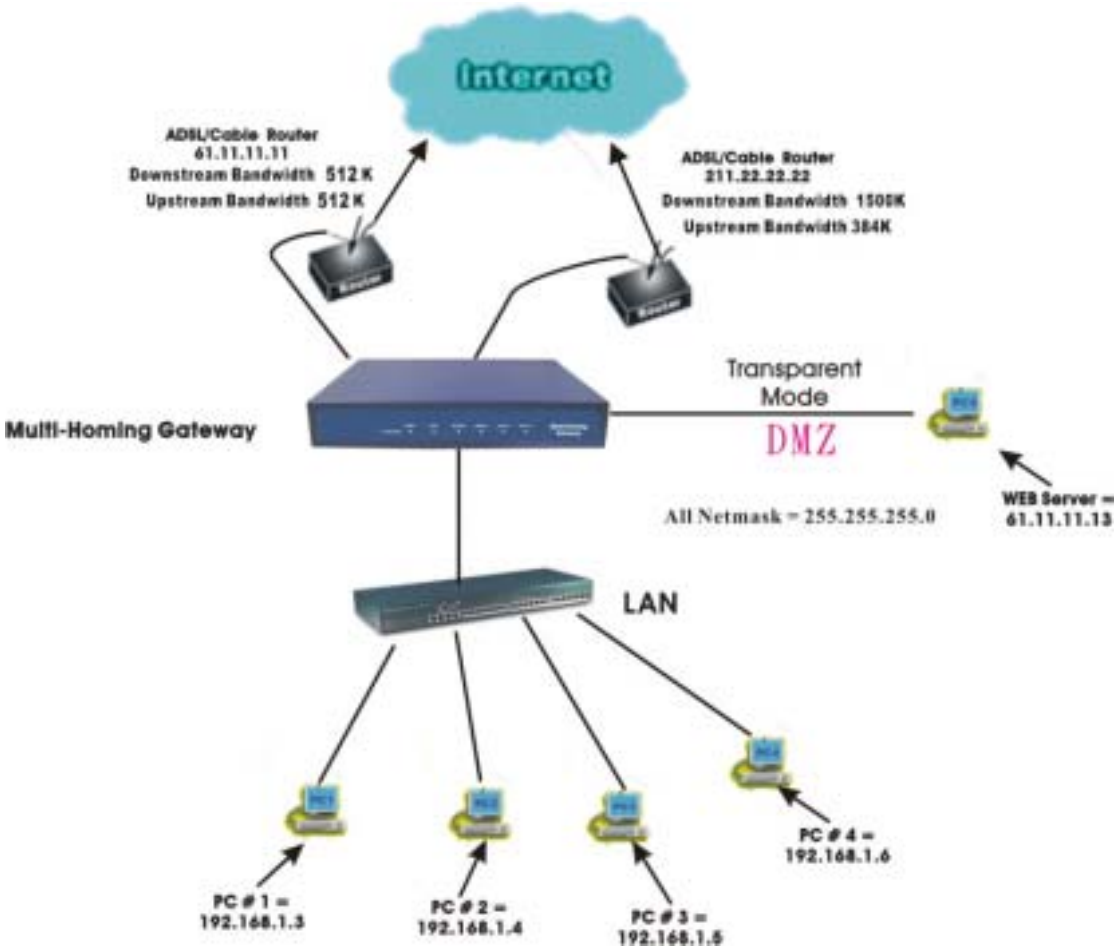


图 H-2 负载平衡连接图

■ **负载平衡器 ：**

内部端口【LAN Port】= **192.168.1.1**

外部端口【WAN 1 Port】= **61.11.11.11 (provided by ISP)**

外部端口【WAN 2 Port】= **211.22.22.22 (provided by ISP)**

非军事区端口【DMZ Port】= **61.11.11.11 (Transparent Mode)**

负载平衡器软件安装

步驟1. 首先将系统管理员的计算机和负载平衡器内部适配卡接到同一个 HUB 或 Switch，再使用浏览器（IE 或 Netscape）连结至负载平衡器。负载平衡器 Internal port 的 IP 地址内定值为 http://192.168.1.1，所以 LAN 端计算机的 IP 地址必须是 192.168.1.2 至 192.168.1.254 其中之一，子网掩码为 255.255.255.0。

步驟2. 设定新环境的 内部网络接口地址（配合公司的环境），外部网络接口地址 (由 ISP 网络公司分配)。如果新设定的 内部网络接口地址 不属于 192.168.1.0 网络，例如新 内部网络接口地址 为 172.16.0.1，管理员必须更改计算机端的 IP 地址为：172.16.0.2，或其它相同子网络的 IP 地址，此时管理员的计算机或许须重新开机，新的 IP 地址才能生效。

步驟3. 当管理员的计算机和负载平衡器的内部网络接口地址 属于 192.168.1.0 网段的网络，开启浏览器（IE 或 Netscape）连结至 http://192.168.1.1 。连上负载平衡器的 WebUI，即可开始使用浏览器设定负载平衡器的参数。

下列表格为标准虚拟 IP 地址范围，不可使用外部真实 IP 地址。

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

步驟4. 浏览器会询问使用者名称及密码，输入管理员名称与密码。*(如图 S-1)*

- 使用者名称：admin
- 密码：admin
- 点选【确定】

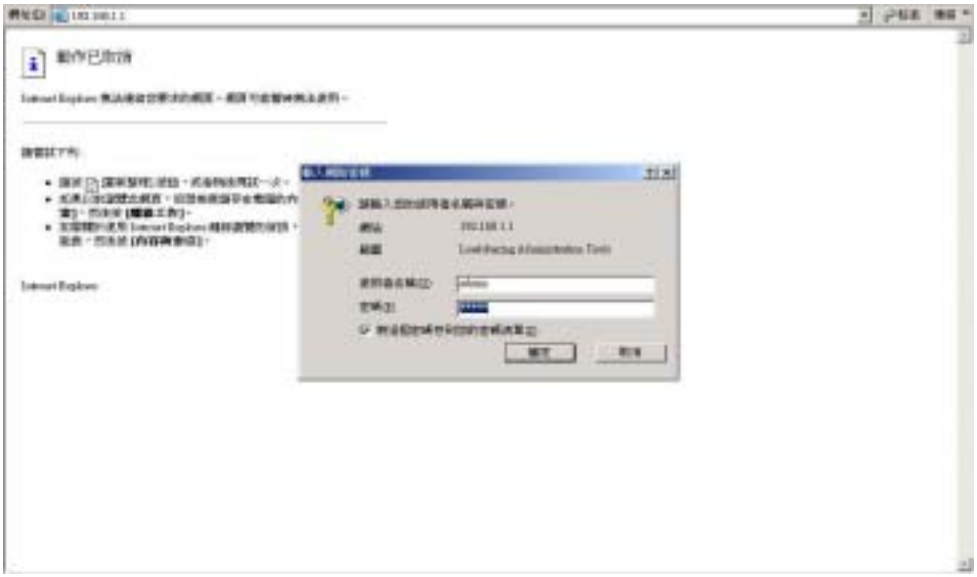


图 S-1 键入使用者名称与密码

步驟5. 进入负载平衡器软件系统主画面后，在左方的功能选项中，点选【接口地址】功能，再点选【内部网络】次功能选项。 *(如图S-2)*

■ 内部网络：

IP 地址：192.168.1.1

子网掩码：255.255.255.0

图 S-2 键入内部网络 IP 地址与子网掩码

如果新的内部网络接口地址不是 192.168.1.1，点选【OK】后，在浏览器网址字段输入新的内部网络接口地址，再重新连结负载平衡器。

步驟6. 进入负载平衡器软件系统主画面后，在左方的功能选项中，点选【接口地址】功能，再点选【外部网络】次功能选项。 *(如图S-3)*

图 S-3 外部网络接口 1 / 2 接口

步驟7. 外部网络接口 1 / 2：点选需要设定的外部网络 1 / 2 ，
点选【修改】选项。键入由 ISP 所配发的 IP 地址 ***(如图S-4)***
(例：外部网络接口地址 1)

- 外部网络路接口地址 1：
  IP 地址：211.11.11.11
  子网掩码：255.255.255.0
  预设网关：211.11.11.1
  DNS 服务器 1：168.95.1.1

图 S-4 键入外部网络 IP 地址与子网掩码

步驟8. 在左方的功能选项中，点选【管制条例】功能，再点选【内部至外部】次功能选项。

步驟9. 点选屏幕下方的【新增】管制条例功能按钮。 *（如图S-5）*

步驟10. 在出现的【新增管制条例】窗口中，键入下列相关参数：

- 来源网络地址：选择【Inside Any】
- 目的网络地址：选择【Outside Any】
- 管制动作：选择【允许】

步驟11. 按下【确定】钮。

图 S-5 至管制条例功能设定来源网络地址与目的网络地址

步驟12. 看到*图S-6* 画面即表示安装成功。最后将企业内部所有计算机的 IP 地址须设定为负载平衡器内部网络接口的同一个网域与预设网关设定为负载平衡器内部网络接口，或将内部的计算机设为自动取得 IP，企业内部网络可马上连结至网际网络存取资料，如欲使用负载平衡器的管制功能，请在【地址表】和【管制条例】功能项增加相关设定值。

图 S-6　安装设定成功画面

第一章

系 统 管 理

所谓的系统管理，广义的定义是指进出负载平衡器系统的权限、路径地址与监控等各种相关设定的管理，在本单元中则定义为管理员、系统设定与软件更新的设定与管理。

负载平衡器的管理由系统主管理员设定。系统主管理员可增加修改系统的各项设定，监控系统状态，而其它管理员（管理员名称由系统主管理员设定）仅能读取系统各项设定资料，不能予以更改。在本【系统管理】单元中：

【管理员】：系统主管理员，可依需求新增与变更次管理员人数与名单，或更改次管理员的密码。

【系统设定】：系统主管理员，可经由此功能，将先前储存的负载平衡器系统各单元设定文件，汇出至客户端硬盘中备份；或将备份的设定文件汇入至负载平衡器系统以修正/更改负载平衡器设定；以及将负载平衡器设定恢复至原出厂设定值。同时，系统主管理员也可利用此单元中的【E-Mail 设定】功能，设定负载平衡器在遭受骇客侵入时，实时自动传送警讯通知系统管理员,纪录经由【到路由分配器封包】设定此功能会将负载平衡器的所有进出封包均纪录下来方便进行管制,【重新激活路由分配器】可以重新开机激活负载平衡器。

【时间设定】：可将负载平衡器的系统时间设定为与内部使用者计算机或外部时间服务器计算机时间同步。

【Multiple Subnet】：内部网络可支持多个区段的网络地址。

【骇客预警】:建立负载平衡器各项侦测功能。系统管理员可利用此功能设定，激活负载平衡器自动侦测功能，当系统发生异常现象时，负载平衡器将会发出电子邮件警告系统管理员，同时将警告讯息显示在【警示记录】之【事件警示】窗口中。

【指定路由表】：系统管理员于此单元中，定义企业网络架构内之内部网络或外部网络，在资料封包传递至某特定网域时，所设定之网关地址。

【DHCP】：系统管理员于此单元中，定义、开启动态 IP 地址（DHCP）组态的各项参数地址与功能。

【DNS 代理服务器】：系统管理员可利用此 DNS 代理服务器功能，指定公司内部服务器的网域名称对应到内部计算机或服务器的 IP 地址。

【DDNS】：可让浮动 IP 使用者做实时更新 DNS 与 IP 对映的功能。

【语言版本】：本软件提供繁体中文和简体中文与英文三种语言版本，使用者可依个人使用的语言，于此单元中进行软件语言设定。

【管理地址】：设定不同接口的内部或外部地址，允许该特定网络地址联机至负载平衡器的接口。经由设定此功能后，非设定条例内所允许的网络地址，在企图联机负载平衡器的接口 IP 地址时，将被负载平衡器认定为非认可进入之网络地址而将其阻挡掉。

【系统注销】：执行此功能后强制系统将此联机信道断线，以防止不明人士进入负载平衡器破坏。

【软件更新】：使用者可至本公司网站上，下载最新、功能更强的软件程序，系统主管理员可利用本功能，更新负载平衡器软件，帮助您将负载平衡器发挥最大效用。

负载平衡器之【管理员】功能设定

步骤1. 在左方的功能选项中，点选【系统管理】功能，进入【管理员】设定窗口。*(如图1-1)*

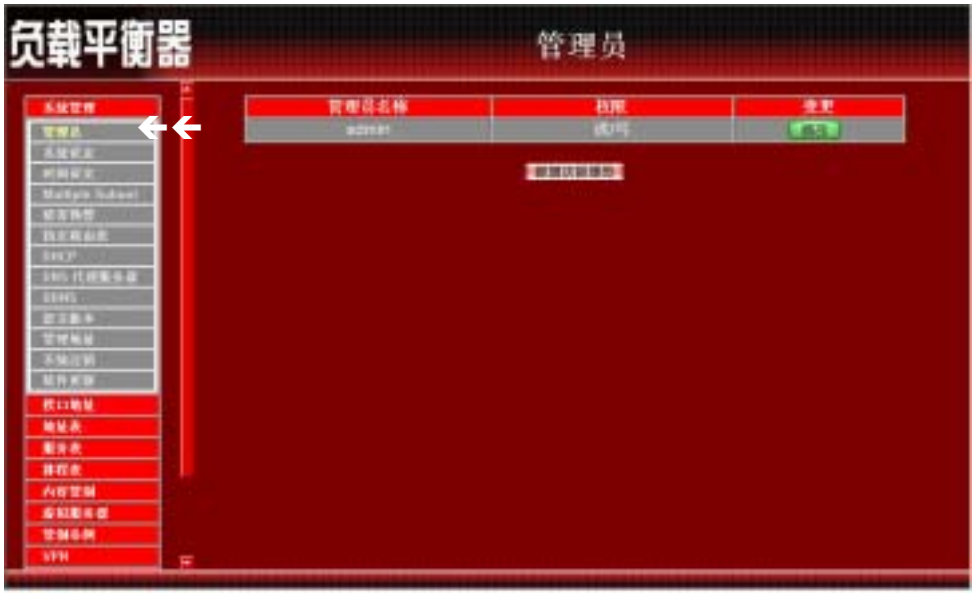


图 1-1 点选【系统管理】之【管理员】功能设定选项

步骤2. 【管理员】表格说明：

- 管理员名称：admin 为本负载平衡器预设系统管理员名称无法删除。
- 权限：本负载平衡器管理员的使用权限。可分为主管理员（可读/写）与次管理员（只读）。
- 变更：管理员之组态设定。点选表格右方【修改】功能修改主/次管理员密码，或点选【删除】功能以删除次管理员。
- 主管理员：系统主管理员。主管理员之系统使用权限为【读/写】，亦即可更改系统设定、监控系统状态、新增、删除次管理员等。
- 次管理员：次管理员。次管理员名称由主管理员设定，其系统使用权限为【读】，所有次管理员只能读取系统状态、监控系统状态，无法更改任何系统设定值。

新增次管理员

步驟1. 在【管理员】设定窗口中，点选屏幕下方【新增次管理员】功能按钮。

步驟2. 在【新增次管理员】窗口中，键入以下资料：*(如图1-2)*

- 次管理员名称：键入欲新增之次管理员名称。
- 密码：键入密码。
- 确认密码：键入与上列密码栏一致的字符串。

步驟3. 点选【确定】以登录使用者，或点选【取消】取消新增管理员。

图 1-2 新增次管理员

变更主/次管理员密码

步骤1. 在【管理员】的表格中，找到欲变更设定的管理员名称，对应至右方【变更】栏，点选【修改】。

步骤2. 在【修改管理员密码】窗口中。键入下列资料：

- 密码：键入原使用密码。
- 新密码：键入新密码。
- 确认密码：键入与上列新密码栏一致的字符串。*（如图1-3）*

步骤3. 点选【确定】修改密码，或点选【取消】取消变更设定。

图 1-3 变更管理员密码

删除次管理员

步驟1. 在【管理员】的表格中，找到欲变更设定的管理员名称，对应至右方的【变更】栏，点选【删除】。

步驟2. 屏幕上会立即产生【删除管理员】的确认对话框。*(如图1-4)*

步驟3. 依照对话框所示，点选【确定】删除该次管理员，或点选【取消】取消删除。

图 1-4 删除次管理员

负载平衡器之【系统设定】功能

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【系统设定】，进入【系统设定】工作窗口。*(如图1-5)*

图 1-5 【系统管理】功能之【系统设定】工作窗口

汇出负载平衡器组态设定档

步骤1. 在【系统设定】窗口中，点选【路由分配器组态】下【汇出系统组态文件至客户端】右方的【下载】功能按钮 。

步骤2. 在出现【档案下载】窗口中，选择【将这个档案储到磁盘】，按下确定，接着指定汇出档案所要储存的目的位置，再按下【确定】。负载平衡器设定文件即会复制至指定储存位置。*（如图1-6）*

图 1-6 选择汇出档案所要储存的目的位置

汇入负载平衡器组态设定档

步骤1. 在【系统设定】窗口中，点选【路由分配器组态】下【从客户端汇入系统组态文件】右方的【浏览】功能按钮。

步骤2. 在出现的【选择档案】窗口中，选择之前编辑储存的负载平衡器设定文件所在的目录位置，选择文件名后，再点选【开启】。*(如图1-7)*

步骤3. 点选屏幕右下方【确定】按钮，将档案汇入至负载平衡器。

图 1-7 汇入档案所在目录位置与文件名

恢复原出厂设定值

步驟1. 在【系统设定】窗口中，勾选【路由分配器组态】下【恢复至出厂设定值】。

步驟2. 点选屏幕右下方【确定】按钮。恢复负载平衡器原出厂时的设定值。*(如图1-8)*

图 1-8 勾选【恢复至出厂设定值】

设定实时警讯通知

步骤1. 勾选【**E-Mail 设定**】下之【开启电子邮件警讯通知】。开启此功能后，本负载平衡器系统在任何时候遭受骇客侵入或出现紧急事件时，将自动且实时传送警讯通知系统管理员。（各种骇客攻击侦测，可于【系统管理】之【骇客预警】功能设定。）

步骤2. 装置名称：在空格中可输入装置的名称。

步骤3. 传送者地址(非必填)：在空格中可输入传送者的名称或电子邮件。

步骤4. 邮件 SMTP 服务器：在空格中输入递送电子邮件的 SMTP 服务器 IP 地址。

步骤5. 电子邮件地址 1：在空格内输入第一位接受警讯通知的电子邮件地址。

步骤6. 电子邮件地址 2：在空格内输入第二位接受警讯通知的电子邮件地址。

步骤7. 邮件测试：点选旁边【**邮件测试**】可测试电子邮件地址 1 和电子邮件地址 2 ,输入的电子邮件是否能正确收到警讯

步骤8. 点选屏幕右下方【确定】设定警讯传送功能。*(如图1-9)*

图 1-9 开启负载平衡器实时传送警讯功能

设定 Web 管理(外部网络接口)

设定 Web 管理(外部网络接口)。提供系统管理员在任何时候改变负载平衡器的远程管理所使用的端口号。

步驟1. 在【系统设定】窗口中，【Web 管理(外部网络接口)】下【HTTP 端口号】右方的【输入字段】，填入欲变更的端口号。

步驟2. 点选屏幕右下方【确定】按钮，完成设定。*(如图1-10)*

图 1-10 设定 Web 管理

MTU 设定

提供系统管理员在任何时候改变负载平衡器的进出封包长度。

步驟1. 在【系统设定】窗口中，【MTU 设定】下【MTU】右方的【输入字段元】，输入需要改变的封包长度。

步驟2. 点选屏幕右下方【确定】按钮，完成设定。*（如图 1-11）*

图 1-11 MTU 设定

设定到负载平衡器封包

步驟1. 在【系统设定】窗口中，勾选【到路由分配器封包】下的【记录到负载平衡器封包】选项。开启此功能后，本负载平衡器系统在任何时候会将进出负载平衡器的封包纪录下来，供系统系统管理员使用。

步驟2. 点选屏幕右下方【确定】按钮，完成设定。*（如图1-12）*

图 1-12 开启记录到路由分配器封包功能

设定重新激活负载平衡器

步驟1. 重新激活负载平衡器：点选【路由分配器将被重新激活】旁边的【**重新激活**】钮。

步驟2. 屏幕上会立即产生【您确定要重新激活吗？】的确认对话框。

步驟3. 依照对话框所示，点选【确定】重新激活负载平衡器，或点选【取消】取消重新激活负载平衡器。*（如图1-13）*

图 1-13 使用重新激活路由分配器功能

系统时间设定

可将负载平衡器的系统时间设定与内部使用者的计算机或是外部时间服务器的时间同步。 *(如图 1-14)*

勾选【开启与外部时间服务器同步】。

步驟1. 可点选下拉式选单设定与 GMT 相差时间(以小时为单位)。

步驟2. 可输入外部时间服务器网络地址。

步驟3. 可设定负载平衡器的系统时间每隔多少时间与外部时间服务器自动更新负载平衡器的系统时间，也可选择输入 0 表示不自动更新。

点选 系统时间与此用户计算机同步 **【同步】**按键,则负载平衡器的系统时间会与管理负载平衡器的客户端计算机的时间同步。

图 1-14 系统时间设定

NAT 模式

可让内部网络设定多个网段地址，并可经由不同的外部地址与网际网络建立联机。
例如：公司的专线申请到多个真实 IP 地址 168.85.88.0/24，公司内部也分为许多的部门，研发部、客服部、业务部、采购部、会计室等，为了方便管理可将各部门以不同 IP 网段来区分。设定方式如下：

1.研发部网段 192.168.1.1/24(Internal) ←→ 168.85.88.253(External)
2.客服部网段 192.168.2.1/24(Internal) ←→ 168.85.88.252(External)
3.业务部网段 192.168.3.1/24(Internal) ←→ 168.85.88.251(External)
4.采购部网段 192.168.4.1/24(Internal) ←→ 168.85.88.250(External)
5.会计室网段 192.168.5.1/24(Internal) ←→ 168.85.88.249(External)

第 1 项在接口地址设定时就设定好了，其它 4 项就必须新增在 Multiple Subnet，设定完成后每个部门就会从不同的外部 IP 地址出去，各部门的计算机设定如下

客服部　IP 地址　　：192.168.2.1
　　子网掩码：255.255.255.0
　　预设网关　：192.168.2.11

其它部门也是按照所属之区段来设定，这就是 Multiple Subnet 的 NAT 模式功能。

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【Multiple Subnet】，进入【Multiple Subnet】工作窗口。*(如图1-15)。*

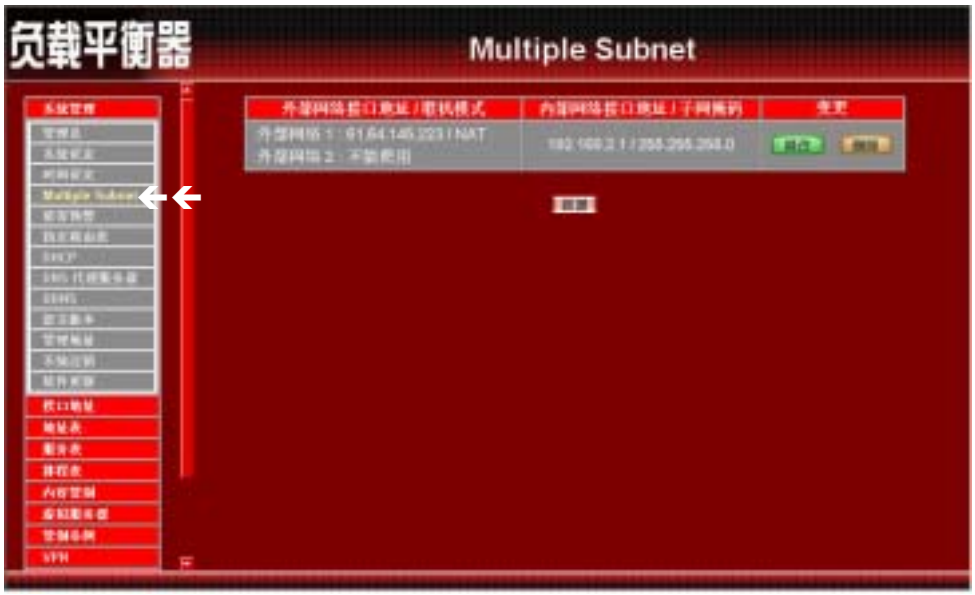


图 1-15 进入 Multiple Subnet NAT 模式功能设定

步驟2. Multiple Subnet 工作窗口名词定义：

- 外部网络接口地址/联机模式：显示目前使用外部网络之 IP 地址及联机模式（NAT 模式或是 Routing 模式）。
- 内部网络接口地址/子网掩码：内部网络之 IP 地址及屏蔽。
- 变更：变更 Multiple Subnet 中各项设定值。点选【修改】，可修改 Multiple Subnet 各项参数；点选【删除】，可删除该项设定。

新增 Multiple Subnet NAT 模式

步驟1. 点选下方【新增】Multiple Subnet 功能按钮。

步驟2. 在新增 Multiple Subnet 窗口中，键入 IP 地址。 *(如图1-16)。*

- 内部网络接口地址：键入内部网络之 IP 地址。
- 子网掩码：键入内部网络的子网掩码。
- 外部网络接口地址：选择外部网络之 IP 地址。
- 联机模式：选择联机模式 NAT 模式。(如外部网络 IP 地址仅有一个的话 如 PPPoE 。Multiple Subnet 仅能使用 NAT 模式)

步驟3. 点选【确定】新增 Multiple Subnet，或【取消】取消新增。

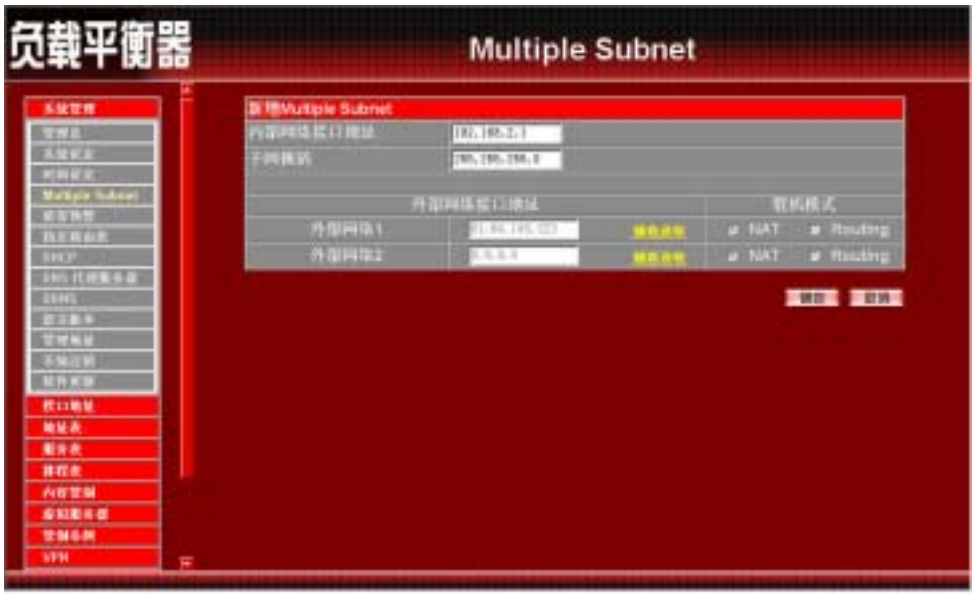


图 1-16 新增 Multiple Subnet NAT 模式

变更 Multiple Subnet NAT 模式

步驟1. 在【Multiple Subnet】的表格中，找到欲变更设定的 IP 地址，对应至右方【变更】栏，点选【修改】。

步驟2. 在【修改 Multiple Subnet】窗口中，键入新的 IP 地址。 *（如图1-17）。*

步驟3. 点选屏幕下方【确定】按钮，变更设定，或 点选【取消】取消变更。

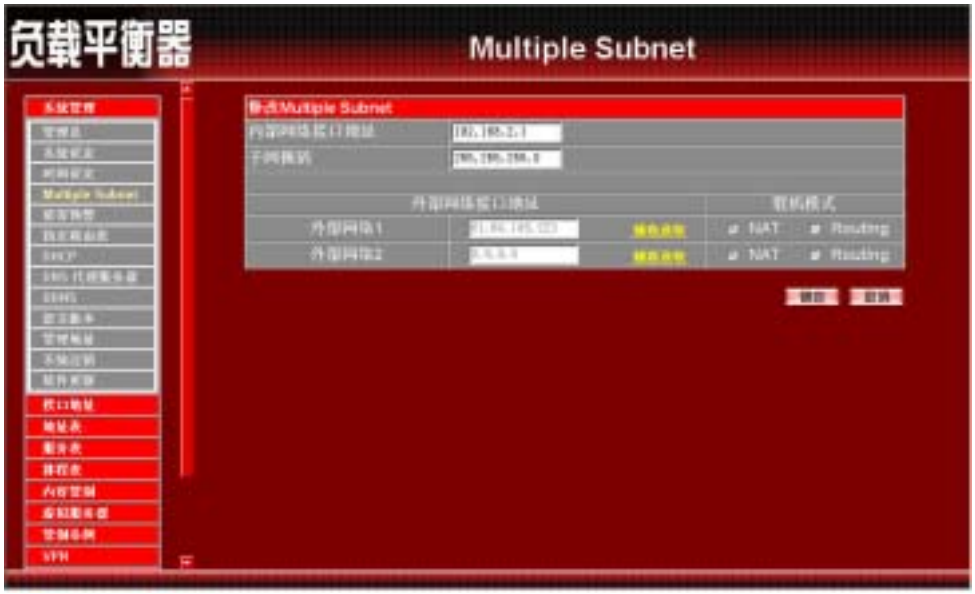


图 1-17 变更 Multiple Subnet NAT 模式

移除 Multiple Subnet NAT 模式

步驟1. 在【Multiple Subnet】的表格中，找到欲删除设定的 IP 地址，对应至右方【变更】栏，点选【删除】。

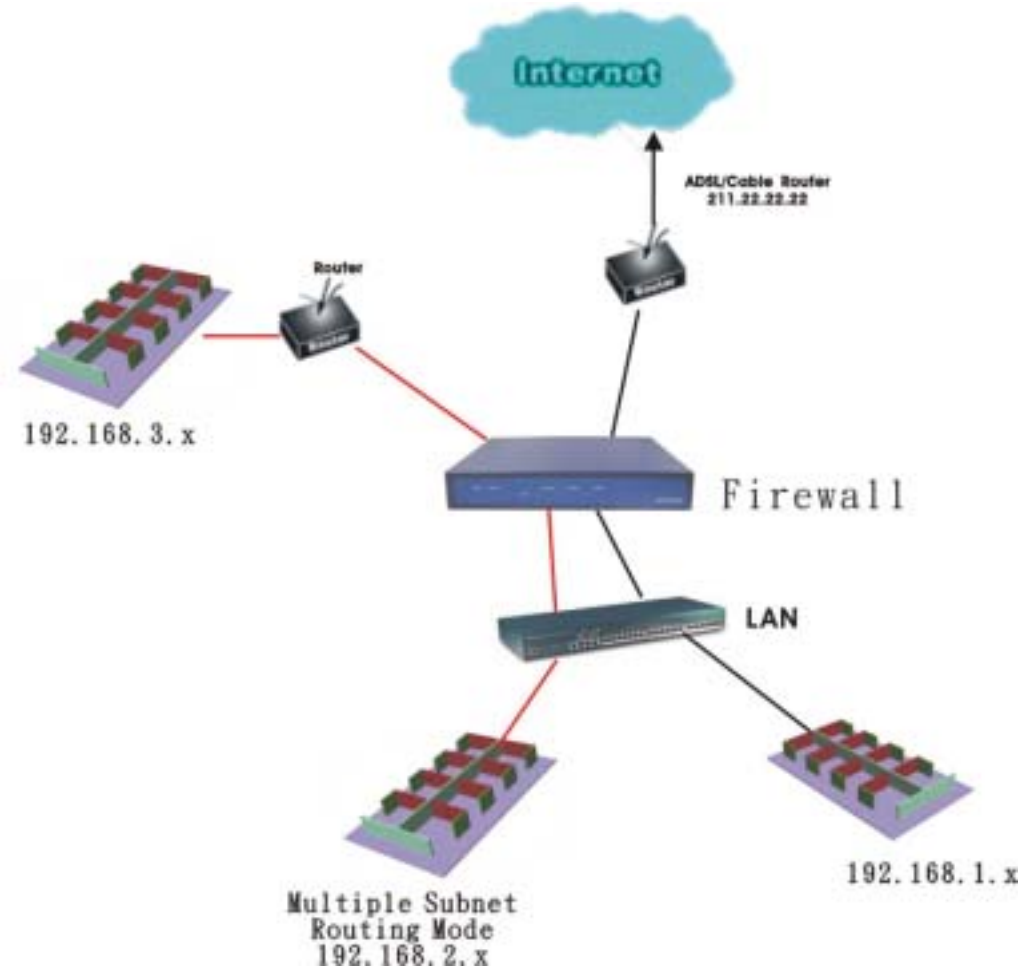
步驟2. 在【确定删除】对话框中，点选【确定】按钮，移除设定，或 点选【取消】取消移除。 *（如图1-18）。*

图 1-18 移除 Multiple Subnet NAT 模式

Routing 模式

可让公司网络在设定 Multiple Subnet Routing 模式时,连接不同网段地址,并经由不同的网段地址来建立联机沟通。

例如：公司的申请专线拥有多个 IP 地址 192.168.2.0/24，公司内部也分为许多的部门，研发部、客服部、业务部、采购部、会计室等，和不同的 IP 区段进行联机,设定 Multiple Subnet Routing 可方便整合各部门信息,。如外部网络 IP 地址需要多个以上，Multiple Subnet Routing 方能使用。



设定方式如下：

步驟1. 于左方功能选项，先点选【系统组态】，接着点选下方的【Multiple Subnet】，进入【Multiple Subnet】工作窗口。*(如图1-19)。*

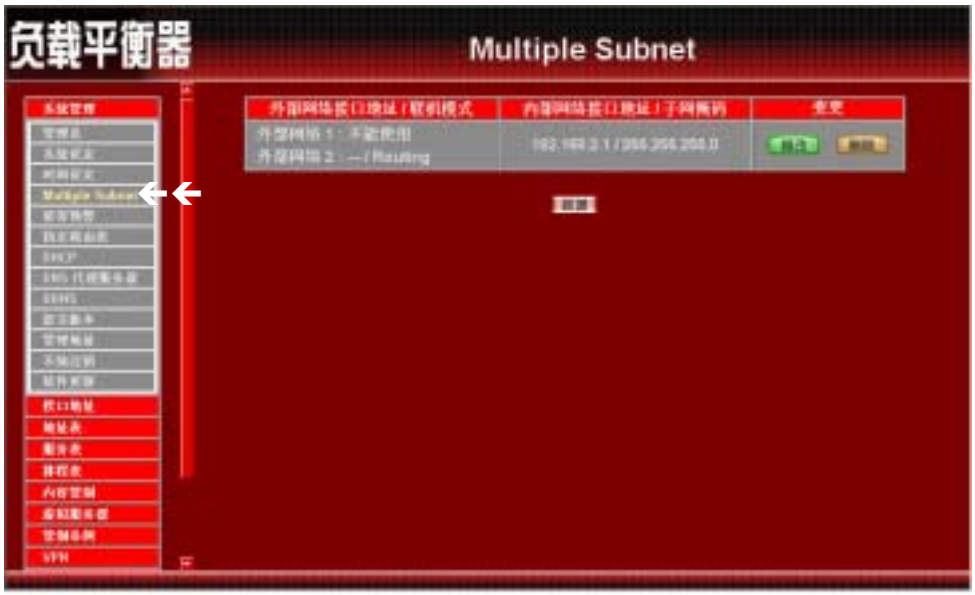


图 *1-19* 进入 Multiple Subnet Routing 模式功能设定

步驟2. Multiple Subnet 工作窗口名词定义：

- 外部网络接口地址/联机模式：显示目前使用外部网络之 IP 地址及联机模式（NAT 模式或是 Routing 模式）。
- 内部网络接口地址/子网掩码：内部网络之 IP 地址及屏蔽。
- 变更：变更 Multiple Subnet 中各项设定值。点选【修改】，可修改 Multiple Subnet 各项参数；点选【删除】，可删除该项设定。

新增 Multiple Subnet Routing 模式

步驟1. 点选下方【新增】Multiple Subnet 功能按钮。

步驟2. 在新增 Multiple Subnet 窗口中，键入 IP 地址。 *（如图1-20）*

- 内部网络接口地址：键入内部网络之 IP 地址。
- 子网掩码：键入内部网络的子网掩码。
- 外部网络接口地址：选择外部网络之 IP 地址。
- 联机模式：选择联机模式 Routing 模式。

步驟3. 点选【确定】新增 Multiple Subnet，或【取消】取消新增。

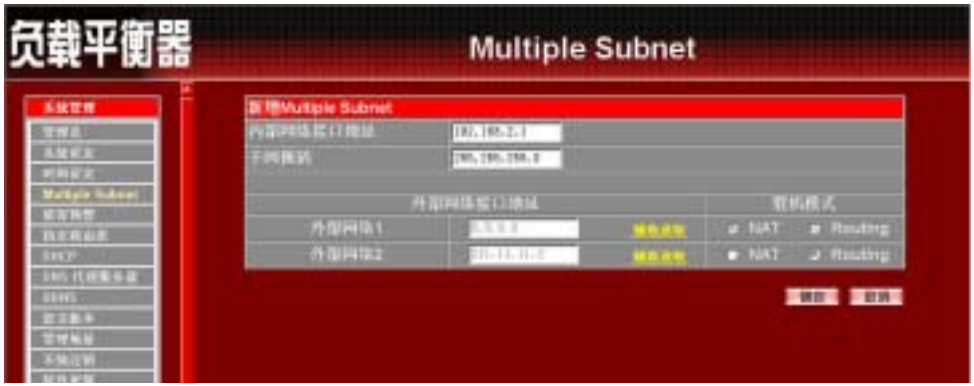


图 *1-20* 新增 Multiple Subnet Routing 模式

步驟4. 新增外部至内部管制条例， 在【外部至内部】窗口中，点选【新增】管制条例功能按钮。新增外部至内部管制条例 (如下图)

变更 Multiple Subnet Routing 模式

步驟1. 在【Multiple Subnet】的表格中，找到欲变更设定的 IP 地址，对应至右方【变更】栏，点选【修改】。

步驟2. 在【修改 Multiple Subnet】窗口中，键入新的 IP 地址。 *（如图1-21）。*

步驟3. 点选屏幕下方【确定】按钮，变更设定，或 点选【取消】取消变更。

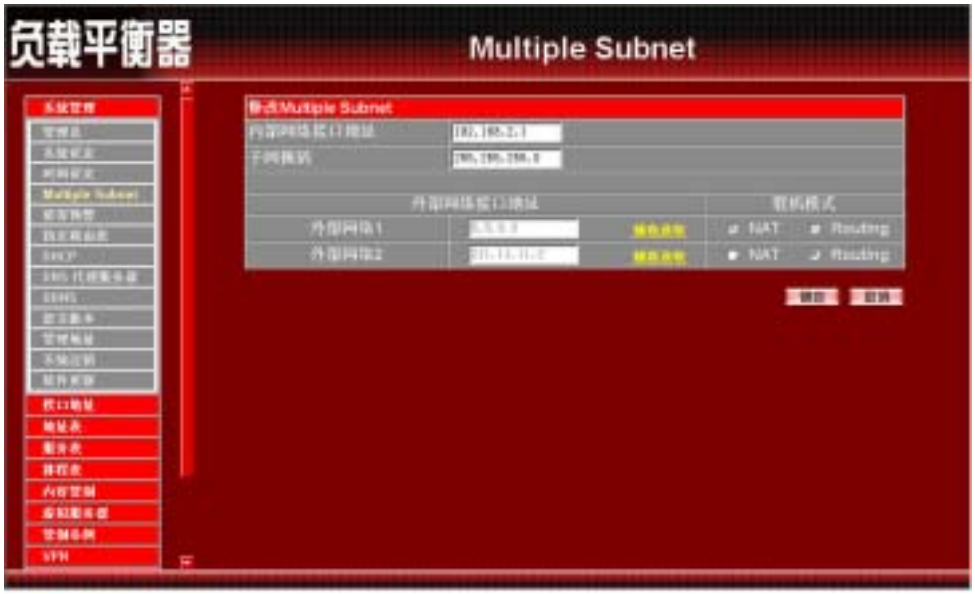


图 *1-21* 变更 Multiple Subnet Routing 模式

移除 Multiple Subnet Routing 模式

步驟5. 在【Multiple Subnet】的表格中，找到欲删除设定的 IP 地址，对应至右方【变更】栏，点选【删除】。

步驟6. 在【确定删除】对话框中，点选【确定】按钮，移除设定，或 点选【取消】取消移除。 *（如图1-22）。*

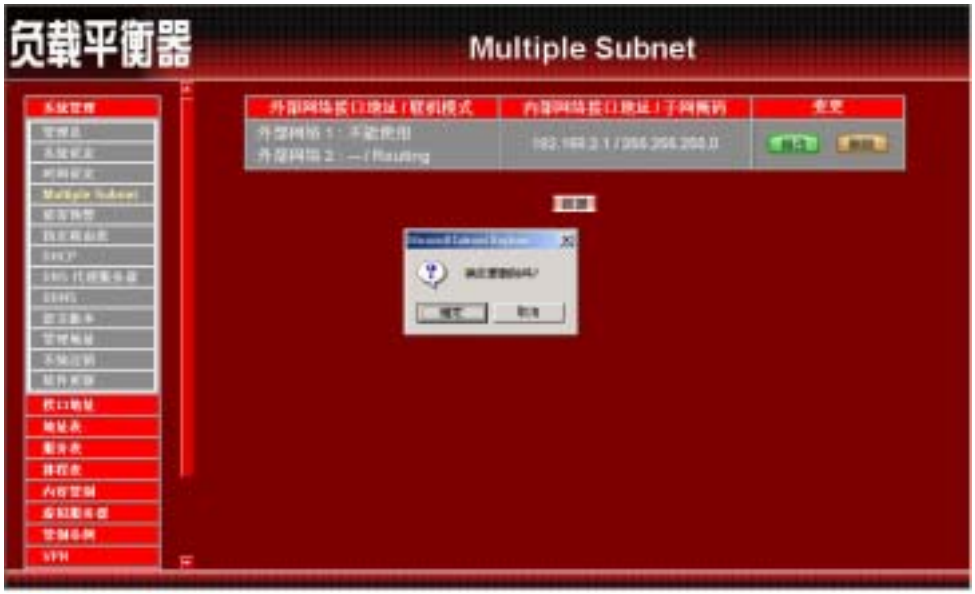


图 *1-22* 移除 Multiple Subnet Routing 模式

骇客预警功能设定

步驟1. 在左方的功能选项中，点选【系统管理】功能，再点选【骇客预警】次功能选项。

步驟2. 【骇客预警】各项侦测功能说明 *(如图1-23)*

图 1-23 设定负载平衡器骇客预警侦测功能

- 侦测 SYN 攻击：侦测当骇客连续送出TCP SYN资料封包给服务器，企图将服务器联机（Connection）资源耗光，使其它使用者无法联机成功的状况。勾选此项后，系统管理员可于右方

  【允许SYN最大流量】空格中，定义所有攻击IP，每秒可通过负载平衡器的最大封包数(Pkts/Sec)。

  【允许每个来源地址SYN最大流量】空格中，定义每个攻击的来源IP地址，每秒可通过负载平衡器的最大封包数(Pkts/Sec)。

  【当来源地址超过SYN最大流量时的阻挡时间】空格中，定义当每个攻击的来源IP地址，超过设定的每秒可通过负载平衡器的最大封包数(Pkts/Sec)时，会在使用者设定秒数内对此攻击来源IP封包阻挡(停止响应)。使用秒数超过后会重新开始计算封包是否超过每个来源地址SYN最大流量，如果最大流量还是超过设定值,会持续进行阻挡攻击。

- 侦测 ICMP 流量：侦测当骇客连续发出PING的资料封包，且是以广播方式（Broadcast）送给网络内每部机器的状况。勾选此项后，系统管理员可于

  【允许 ICMP 最大流量】空格中，定义所有攻击IP，每秒可通过负载平衡器的最大封包数(Pkts/Sec)。

  【允许每个来源地址 ICMP 最大流量】空格中，定义每个攻击的来源IP地址，每秒可通过负载平衡器的最大封包数(Pkts/Sec)。

  【当来源地址超过 ICMP 最大流量时的阻挡时间】空格中，定义当每个攻击的来源IP地址，超过设定的每秒可通过负载平衡器的最大封包数(Pkts/Sec)时，会在使用者设定秒数内对此攻击来源IP封包阻挡(停止响应)。使用秒数超过后会重新开始计算封包是否超过每个来源地址ICMP最大流量，如果最大流量还是超过设定值,会持续进行阻挡攻击。
- 侦测 UDP 流量：同ICMP Flood。勾选此项后，系统管理员可于

  【允许 UDP 最大流量】空格中，定义所有攻击IP，每秒可通过负载平衡器的最大封包数(Pkts/Sec)。

  【允许每个来源地址 UDP 最大流量】空格中，定义每个攻击的来源IP地址，每秒可通过负载平衡器的最大封包数(Pkts/Sec)。

  【当来源地址超过 UPD 最大流量时的阻挡时间】空格中，定义当每个攻击的来源IP地址，超过设定的每秒可通过负载平衡器的最大封包数(Pkts/Sec)时，会在使用者设定秒数内对此攻击来源IP封包阻挡(停止响应)。使用秒数超过后会重新开始计算封包是否超过每个来源地址UTP最大流量，如果最大流量还是超过设定值,会持续进行阻挡攻击。
- 侦测 Ping of Death 攻击：侦测当骇客送出的PING资料封包带有大量垃圾资料，导致某些系统收到这些资料后产生不良反应，如：执行效率变慢，或系统毁坏必须重新开机，才可正成运作的状况。
- 侦测 IP Spoofing 攻击：侦测当骇客伪造成合法的使用者企图穿越负载平衡器入侵系统。

- 侦测 Port Scan 攻击：侦测当骇客连续发出扫瞄侦测服务器开放的端口号（Port ID），当服务器对某些Port的侦测有反应时，骇客即可针对此Port攻击的状况。
- 侦测 Tear Drop 攻击：侦测当IP资料封包在传送过程中会被分段切割，而在目的地组合起来。如果攻击者送出自订的封包，强迫分段成为负值的长度，有些系统会将此负值误认为很大的数值，而将大量的资料复制进系统，导致系统损毁、停机或重新开机的状况。
- 过滤 IP Route 选择：IP封包中有个选项，可以指定封包回传时所用的目的地址，且此地址可与IP封包标头中的来源地址不同。骇客可利用此种封包伪装的IP地址进入网域中，并将网域中的资料回传给骇客。勾选这个功能，可以阻挡使用此种选项的IP封包。
- 侦测 Land 攻击：有些系统接收到来源地址与目的地址相同，来源端口号与目的端口号相同，且TCP封包标头中的「SYN」标记又被设定时，会因此处理不当而当机。勾选这个功能即可侦测此种不正常的封包。

步骤3. 勾选各项侦测功能后，点选屏幕右下方【确定】按钮。

完成此部分设定后，当系统侦测到任何异常现象时，会立即将警告讯息显示在【警示记录】之【事件警示】窗口中。系统管理员亦可于【系统设定】中开启电子邮件警讯通知功能，负载平衡器将会自动发出电子邮件警告系统管理员。

【指定路由表】设定功能

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【指定路由表】，进入【指定路由表】工作窗口。*（如图1-24）*

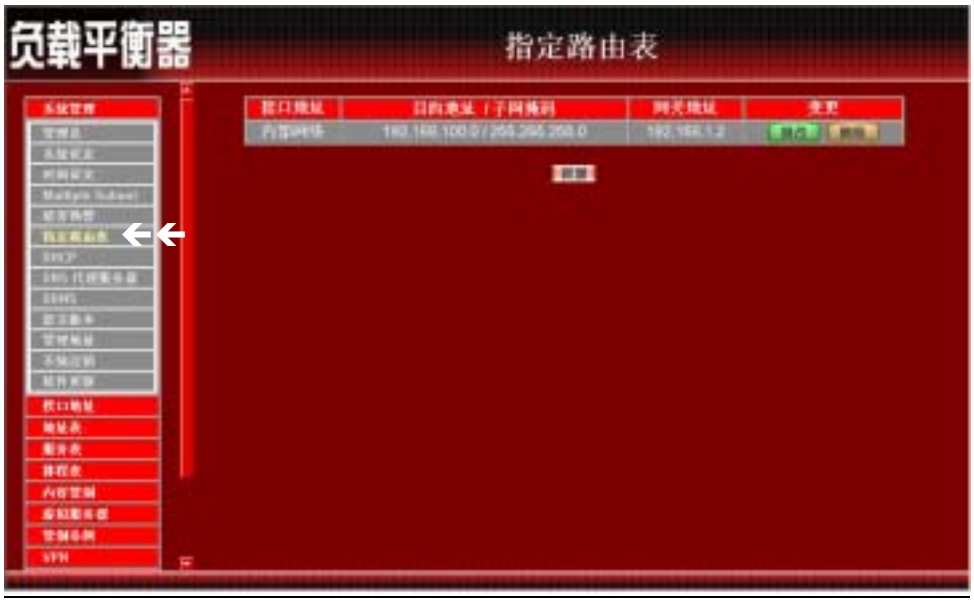


图 1-24 【指定路由表】功能设定

步驟2. 指定路由表工作窗口的表格名词定义：

- 接口地址：目的网域所属区域，为内部网络、外部网络或非军事区网络。
- 目的地址：连结目的网域之 IP 地址。
- 子网掩码：连结目的网域之子网掩码。
- 网关地址：连结目的网域之网关地址。
- 变更：变更路由表中各项设定值。点选【修改】，可修改指定路由表各项参数信息；点选【删除】，可删除该项设定。

新增网络网关

步驟1. 在【新增网络网关】窗口中，键入欲新增网络网关的目的地址、子网掩码、网关地址等资料。*(如图1-25)*

步驟2. 在接口地址的下拉选单中，选择欲连结的目的网域所属区域（内部网络、外部网络或非军事区网络)。

步驟3. 点选【确定】新增所指定的网络网关，或点选【取消】取消设定。

图 1-25 新增指定路由网关

变更指定路由表中的网络网关设定

步骤1. 在【指定路由表】的表格中，找到欲修改的网络名称，对应至右方【变更】栏，点选【修改】。

步骤2. 在出现的【变更指定路径】的窗口中，填入各项欲变更的路径地址。

步骤3. 点选【确定】修改该指定网络区域，或点选【取消】取消修改。*（如图1-26）*

图 1-26 变更指定路由表中的网关设定

删除指定路由表中的网关设定

步骤1. 在【指定路由表】的表格中，找到欲删除的网络名称，对应至右方【变更】栏，点选【删除】。

步骤2. 在【确定删除】对话框中点选【确定】执行删除设定，或点选【取消】取消删除。*（如图 1-27）*

图 1-27 删除指定路由表中的网关设定

DHCP 功能设定

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【DHCP】，进入【DHCP】工作窗口。*（如图1-28）*

图 1-28 DHCP 设定

步驟2. DHCP 设定信息：

- 子网络 ： 内部网络所属网域。
- 子网掩码 ： 内部网络所属网域屏蔽。
- 网关地址: 内部网络预设网关。
- 广播地址: 内部网络所属网域广播地址。

激活 DHCP 功能

步驟1. 勾选【激活 DHCP 服务器】。并键入下列信息 *（如图 1-29）*

- 网域名称：键入内部私有网络名称。

勾选【自动取得 DNS】：选择是否自动取得 DNS 服务器。

- DNS 服务器 1：键入欲配发 DNS 服务器 1 之 IP 地址。
- DNS 服务器 2：键入欲配发 DNS 服务器 2 之 IP 地址。
- WINS 服务器 1：键入欲配发 WINS 服务器 1 之 IP 地址。
- WINS 服务器 2：键入欲配发 WINS 服务器 2 之 IP 地址。

内部网络接口地址 ：

- 用户 IP 地址范围 1：于左边字段键入第一组可使用的起始 IP 地址；于右边字段键入第一组可使用的结束 IP 地址。（须为同一网域）
- 用户 IP 地址范围 2：于左边字段键入第二组可使用的起始 IP 地址；于右边字段键入第二组可使用的结束 IP 地址。（须为同一网域）

非军事区接口地址 ：

- 用户 IP 地址范围 1：于左边字段键入第一组可使用的起始 IP 地址；于右边字段键入第一组可使用的结束 IP 地址。（须为同一网域）
- 用户 IP 地址范围 2：于左边字段键入第二组可使用的起始 IP 地址；于右边字段键入第二组可使用的结束 IP 地址。（须为同一网域）
- 租用时间：为动态 IP 的设定租用时间。

步驟2. 点选【确定】执行 DHCP 支持功能，或【取消】取消激活 DHCP 功能。

图 1-29 激活 DHCP 功能

DNS 代理服务器功能设定

当使用者自行架设服务器，且已申请合法网域名称，为使内部网络计算机可使用该网域名称来连结此服务器，必须先于此功能中将网域名称对映至该服务器在负载平衡器后的虚拟 IP 地址。且内部网络计算机必须将其 DNS 服务器设定值定义为在负载平衡器【系统管理】接口地址中的「内部网络接口ＩＰ地址」。

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【DNS 代理服务器】，进入【DNS 代理服务器】工作窗口。*(如图 1-30)*

图 1-30 DNS 代理服务器功能

DNS 代理服务器设定信息：

- 网域名称：内部或非军事区内计算机的网域名
- 虚拟 IP 地址：该网域名称所对映之内部或非军事区（NAT 模式）虚拟 IP 地址。
- 变更：变更 DNS 代理服务器中各项设定值。点选【修改】，可修改 DNS 代理服务器各项参数；点选【删除】，可删除该项设定。

要使用负载平衡器的 DNS 服务器功能，使用者 PC 端的第一个（主）DNS 服务器一定要指向负载平衡器的 IP，也就是计算机端所设定的预设网关（Gateway）。

新增 DNS 代理服务器

步驟1. 点选下方【新增】DNS 代理服务器功能按钮。

步驟2. 在【新增 DNS 代理服务器】窗口中，键入相关参数。 *（如图 1-31）*

- 网域名 ： 键入网域名称。
- 虚拟 IP 地址 ： 键入该网域名称所对映之虚拟 IP 地址。

步驟3. 点选【确定】新增 DNS 代理服务器，或【取消】取消新增。

图 1-31 新增 DNS 代理服务器

变更 DNS 代理服务器

步驟1. 在【DNS 代理服务器】的表格中，找到欲变更设定的网域名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在【修改 DNS 代理服务器】窗口中，键入各项欲变更参数。 *（如图 1-32）*

步驟3. 点选屏幕下方【确定】按钮，变更设定，或 点选【取消】取消变更。

图 1-32 变更 DNS 代理服务器

删除 DNS 代理服务器

步驟1. 在【DNS 代理服务器】的表格中，找到欲删除设定的网域名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】DNS 代理服务器对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。 *（如图 1-33）*

图 1-33 删除 DNS 代理服务器

DDNS 功能设定

设定 DDNS，可让使用浮动 IP 的使用者直接透过负载平衡器就可以与提供 DDNS 的服务网站做动态 DNS 与 IP 地址的对映。

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【DDNS】，进入【DDNS】工作窗口。*（如图 1-34）*

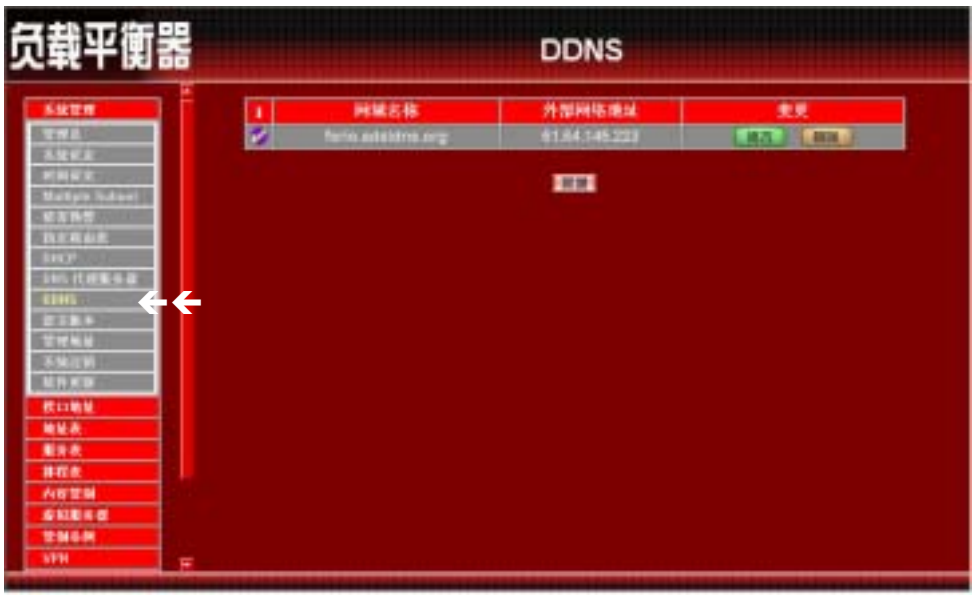


图 1-34 DDNS 功能设定

步驟2. DDNS 工作窗口名词定义：

- !：更新状态。【联机中；联机时间逾时，更新失败；更新成功；不明的错误】
- 网域名称：申请的网站名称。
- 外部网络地址：外部网络接口现在的 IP 地址。
- 变更 :变更动态 DNS 中各项设定值。点选【修改】,可修改动态 DNS 各项参数；点选【删除】，可删除该项设定。

步驟3. DDNS 使用方法：

负载平衡器里提供十家的服务厂商，使用者必须先到该网站注册后才可使用此功能，其使用规章请参阅该服务商网站。

如何注册：于左方功能选项，先点选【系统管理】，接着点选下方的【DDNS】，进入【DDNS】工作窗口，再按下新增按钮，在服务提供者的右方，按下注册去即出现该服务商的网站，注册办法请自行参阅网站说明。*(如图1-35)*

图 1-35 DDNS 服务提供者注册方法

新增 DDNS

步驟1. 点选下方【新增】DDNS 功能按钮。

步驟2. 在新窗口空栏中，键入相关信息。 *（如图 1-36）*

- 服务提供者：选择服务提供厂商。
- 注册去：到该服务厂商之网站。
- 外部网络地址：负载平衡器外部接口地址之 IP。
- 自动对映外部网络接口地址：自动将外部接口地址填入
- 选择对应的外部网络为 WAN 1 / 2。
- 使用者名称：申请时所注册的帐号。
- 密码：申请时所注册的密码。
- 网域名称：申请时所注册的名称及网域。

步驟3. 点选【确定】新增 DDNS，或【取消】取消新增。

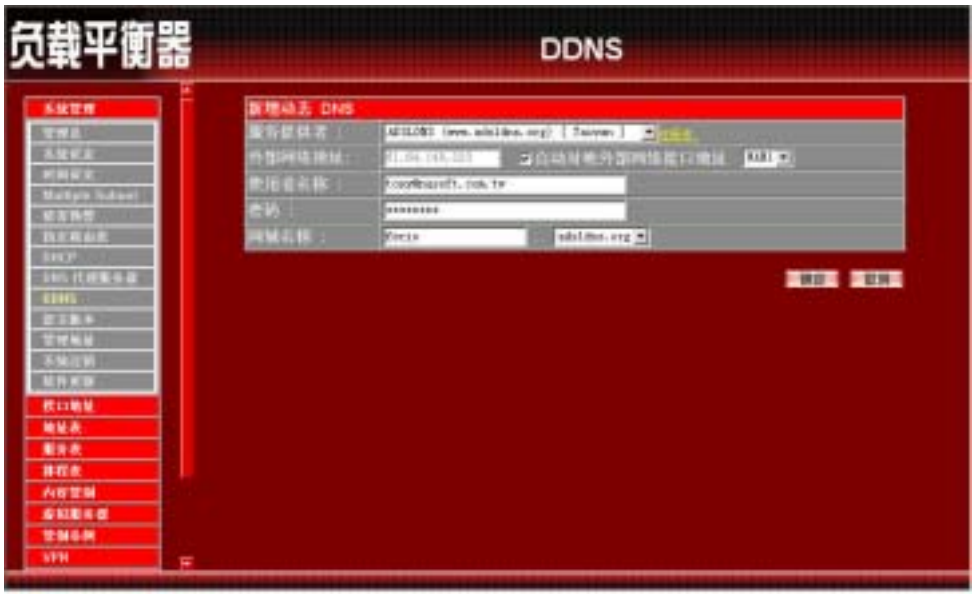


图 1-36 新增 DDNS

变更 DDNS

步骤1. 在【DDNS】的表格中，找到欲变更设定的项目，对应至右方【变更】栏，点选【修改】。

步骤2. 在【修改动态 DNS】窗口中，键入新的信息。 *(如图1-37)*

步骤3. 点选屏幕下方【确定】按钮，变更设定，或 点选【取消】取消变更。

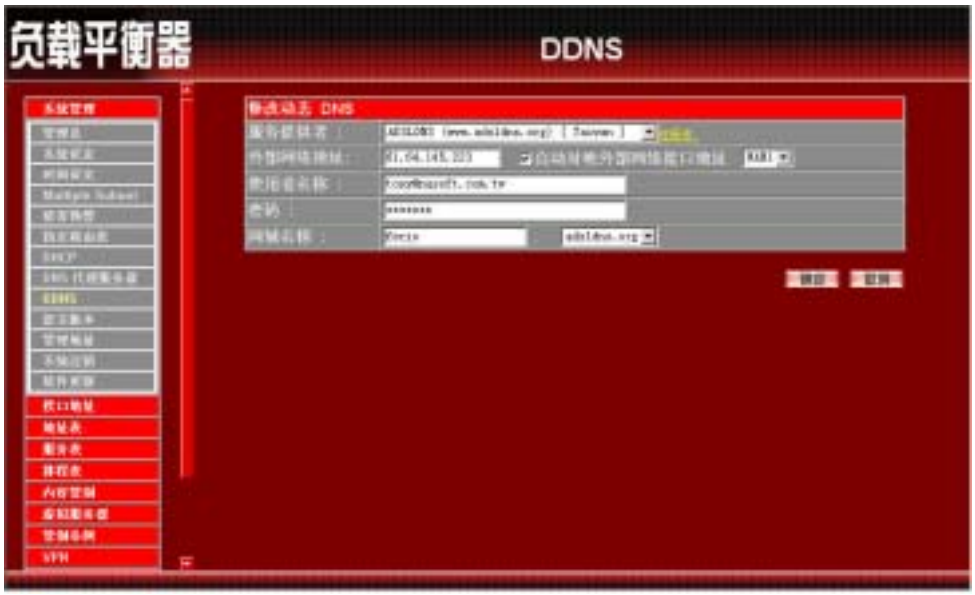


图 1-37 变更 DDNS

删除 DDNS

步驟1. 在【DDNS】的表格中，找到欲删除设定的动态 DNS，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】动态 DNS 对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。 *（如图1-38）*

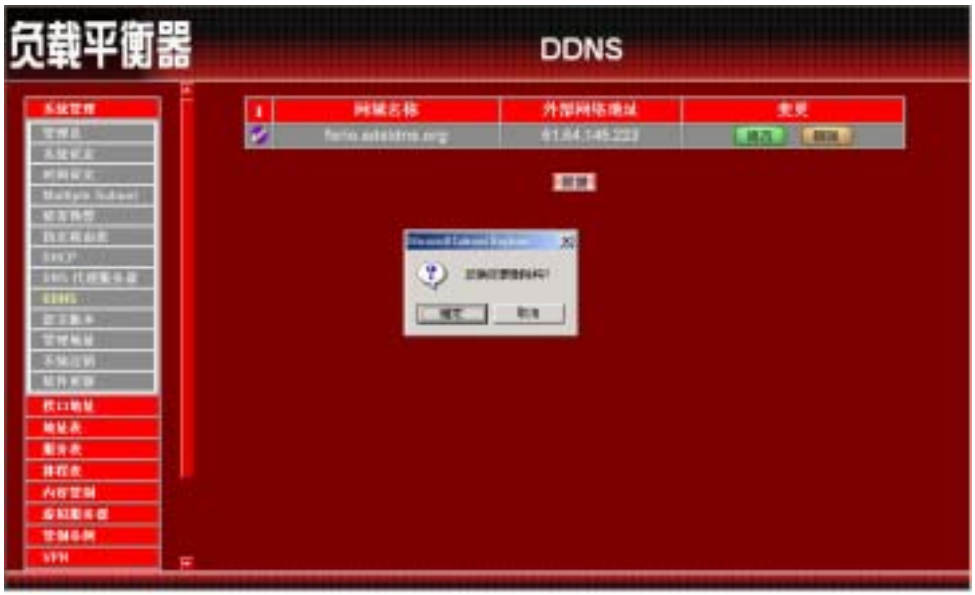


图 1-38 删除 DDNS

语言版本设定

本功能可更换负载平衡器设定画面的语言版本

步驟1. 勾选所欲使用的语言版本（繁体中文/简体中文或英文）。

步驟2. 点选【确定】更换软件的语言版本，或点选【取消】取消设定。*（如图1-39）*

图 1-39 负载平衡器软件语言版本设定

管理地址功能设定

可设定不同接口的内部或外部地址，允许该特定网络地址联机至负载平衡器的接口。经由设定此功能后，非设定条例内所允许的网络地址，在企图联机负载平衡器的接口 IP 地址时，将被负载平衡器认定为非认可进入之网络地址而将其阻挡掉。

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【管理地址】，进入【管理地址】工作窗口。*(如图 1-40)*

图 1-40 管理地址功能

步驟2. 管理地址工作窗口名词定义：

- IP 地址/子网掩码：内部或外部网络之 IP 地址及屏蔽。
- Ping：被设定 IP 地址可 Ping 外部网络接口地址。
- WebUI：允许连入负载平衡器的指定 IP 地址可透过 HTTP 联机至负载平衡器设定画面。
- 变更：变更管理地址中各项设定值。点选【修改】，可修改管理地址各项参数信息；点选【删除】，可删除该项设定。

要正确使用管理地址的相关功能，使用者必须先到【接口地址】，将与管理地址相同网络的 ***WebUI*** *与* ***HTTPS*** *功能关闭掉。也就是欲正常使用此功能，必须关闭其它有所抵触之功能项目，若忽略【接口地址】的开启设定，将造成管理地址的功能失效。*

新增管理地址

步驟1. 点选下方【新增】管理地址功能按钮。

步驟2. 在【新增管理地址】窗口中，键入相关参数。 *(如图1-41)*

- IP 地址 ： 键入允许连入的内部或外部网络之 IP 地址。
- 子网掩码：键入该网络的子网掩码。
- 服务选项：勾选允许连入负载平衡器接口的服务类型。提供 HTTP 联机和 Ping WAN Port IP 的服务。

步驟3. 点选【确定】新增负载平衡器，或【取消】取消新增。

图 1-41 新增管理地址

变更管理地址

步驟1. 在【管理地址】的表格中，找到欲变更设定的 IP 地址，对应至右方【变更】栏，点选【修改】。

步驟2. 在【修改管理地址】窗口中，键入新的 IP 地址。 *（如图1-42）*

步驟3. 点选屏幕下方【确定】按钮，变更设定，或 点选【取消】取消变更。

图 1-42 变更管理地址

删除管理地址

步驟1. 在【管理地址】的表格中，找到欲删除设定的 IP 地址，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。 *（如图1-43）*

图 1-43 删除管理地址

系统注销设定

为防止管理人员在设定或观察负载平衡器时，因故离开设定画面，而造成意图破坏人士之可乘之机，负载平衡器提供此【注销负载平衡器】功能，让设定者在执行此功能后强制系统将此联机信道断线，以防止不明人士进入负载平衡器破坏。

步驟1. 在左方的功能选项中，点选【系统注销】功能。*（如图1-44）*

步驟2. 点选【确定】执行注销负载平衡器功能，或点选【取消】取消注销。

图 1-44 注销负载平衡器设定

软件更新

升级负载平衡器软件，请先至本公司网站免费下载最新版本软件，再依下列步骤更新。更新后，无须重新设定负载平衡器系统设定值。

步骤1. 先点选左方功能选项的【系统管理】，接着点选下方的【软件更新】，进入【软件更新】工作窗口。*(如图 1-45)*

步骤2. 由屏幕上【版本】信息中，获知目前软件使用版本号码。再经由浏览器至本公司网站取得最新软件版本讯息，并将更新程序下载储存至本地端计算机的硬盘中。

步骤3. 点选【浏览】，于【选择档案】窗口中，选择最新的软件版本文件名称。

步骤4. 点选屏幕右下方【确定】功能按钮，执行软件自动更新升级。

图 1-45 负载平衡器软件更新

软件更新需 3 分钟的时间，更新后系统将会自动重新开机。

第二章

介 面 位 址

接口地址包括了负载平衡器系统的内部网络和外部网络等设定值。这些设定值在设定后会储存在接口地址文件里。

在本【接口地址】单元中：系统管理员于此单元中，依照所选择的 ISP 网络联机方式，定义企业网络架构内的内部网络和外部网络的 IP 地址、子网掩码、网关地址等接口地址。

内部网络接口地址设定

步驟1. 在左方的功能选项中，点选【接口地址】功能，再点选【内部网络】次功能选项。*(如图2-1)*

步驟2. 键入内部网络之各项接口地址设定：

- IP 地址： 键入内部网络之 IP 地址。
- 子网掩码： 键入内部网络之子网掩码。
- 开启：是否开启 Ping / WebUI 等功能

步驟3. 将所有接口地址设定好后，点选屏幕右下方【确定】按钮。

图 2-1 内部网络接口地址设定

如果负载平衡器新的 Internal IP Address 不是 192.168.1.1，则系统主管理员必须更改 PC 端的 IP Address，并重新开机才能使新的 IP 地址生效。例如：负载平衡器新的 Internal IP Address 是 172.16.0.1，则在 Browser 的网址栏位上输入新的 Internal IP Address 172.16.0.1，与负载平衡器重新联机。

外部网络接口设定

步驟1. 在左方的功能选项中，点选【接口地址】功能，再点选【外部网络】次功能选项。*(如图2-2)*

步驟2. 在负载模式下，点选下拉是选单可选择

自动分配：负载平衡器依照外部网络下载频宽,
会自动依频宽分配对外网络下载比例。
(适用不相同下载频宽的使用者)

循环分配：负载平衡器强制采用 1:1 循环分配网络下载联机。
(适用相同下载频宽的使用者)

依照流量分配：负载平衡器会照现有流量的状态来分配网络下载联机。

依照联机数：负载平衡器依照使用者设定的 **饱和联机数** 来分配对外网络联机。

依照封包数：负载平衡器依照使用者设定的封包及饱和联机数来分配对外网络联机。

- 外部网络接口：为外部网络接口 1 / 2
- 联机模式：显示目前外部网络接口联机模式
  PPPoE **设定** (ADSL **拨接使用者**)
  自动取得 IP 地址 (缆线调制解调器使用者)
  指定 IP 地址 (固接式或 ADSL 专线使用者)
- IP 地址：显示目前外部网络接口联机的 IP 地址
- 饱和联机数：设定外部网络联机数量,使用联机达设定值时即循环进入下一个外部网络联机
- 开启功能：显示是否勾选 Ping / WebUI 等功能
- 变更：修改外部网络接口设定
- 优先权：设定外部网络接口的优先使用权

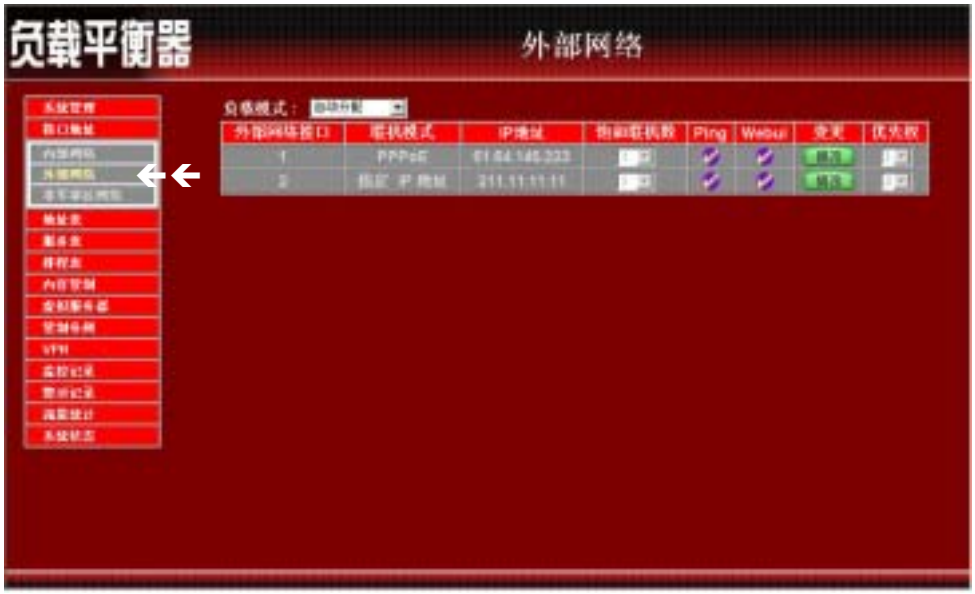


图 2-2　外部网络接口地址设定

PPPoE 设定 (ADSL 拨接使用者)

步驟1. 点选【PPPoE 设定 (ADSL 拨接使用者)】次功能选项。*(如图2-3)*

- 测试联机 IP 地址：本负载平衡器系统会自动发出侦测封包给使用者设定的 IP 地址，已确认联机状态是否正常。
  如使用者设定的 IP 地址未有响应，本负载平衡器将会重新进行联机动作，确保联机状态正常。
- 目前状态 :本负载平衡器系统会自动侦测并显现目前网络联机状态 (联机中或断线)。
- IP 地址：显示 ISP 配发的外部的 IP 地址。
- 使用者名称：ISP 配发的帐号名称。
- 密码：ISP 配发帐号的密码。
- 由 ISP 提供的 IP 地址：勾选动态 IP；或是勾选固定 IP，并键入该固定 IP 地址。
- 下载频宽：输入联机下载最大频宽。
- 上传频宽：输入联机上传最大频宽。
- 自动联机：勾选此项，当有封包到外部网络时时，将会自动联机上网。
- 闲置？分钟自动断线：原出厂值设定为 0 分钟。您可自行设定为网络闲置时，自动断线的时间，若设定值定为”0”，即表示永远维持联机状态。选择计时制的用户，最好设定自动断线时间，以节省联机费用。
- Ping：勾选此项，允许远程用户 Ping 外部网络接口地址。
- WebUI：勾选此项，允许远程用户使用 HTTP 联机至负载平衡器设定画面。

步驟2.　将所有参数设定好后，点选屏幕右下方【确定】按钮。

图 2-3　PPPoE 设定(ADSL 拨接使用者)设定

自动取得 IP 地址(缆线调制解调器使用

步驟1. 点选外部网络下方【自动取得 IP 地址(缆线调制解调器使用者)】。 *(如图2-4)*

- 测试联机 IP 地址：本负载平衡器系统会自动发出侦测封包给使用者设定的 IP 地址，已确认联机状态是否正常。
  如使用者设定的 IP 地址未有响应，本负载平衡器将会重新进行联机动作，确保联机状态正常。
- IP 地址：显示 ISP 配发的外部的 IP 地址。
- MAC 地址 (某些 ISP 要求输入)：某些 ISP 需输入 MAC 地址。(按下右方【填入使用者 MAC 位置】按钮可自动取得)
- 用户名称 (某些 ISP 要求输入)：某些 ISP 要求输入配发的帐号名称。
- 网域名称：某些 ISP 要求输入的网域名称。
- 使用者名称（DHCP+ 网络协议使用）：ISP 配发的帐号名称。
- 密码（DHCP+ 网络协议使用）：ISP 配发帐号的密码。
- 下载(上传)频宽：输入联机下载(上传)最大频宽。
- 更新:：要求重新取得外部 IP 地址。
- 释放:：要求释放已取得外部 IP 地址。
- Ping：勾选此项，允许远程用户 Ping 外部网络接口地址。
- WebUI：勾选此项，允许远程用户使用 HTTP 联机至负载平衡器设定画面。

步驟2.　将所有参数设定好后，点选屏幕右下方【确定】按钮。

图 2-4　自动取得 IP 地址(缆线调制解调器使用者)设定

指定 IP 地址(固接或 ADSL 专线使用者)

步驟1. 点选外部网络下方【指定 IP 地址 (固接式或 ADSL 专线使用者)】。 *(如图2-5)*

- 测试联机 IP 地址：本负载平衡器系统会自动发出侦测封包给使用者设定的 IP 地址或网址，以确认联机状态是否正常。
  如使用者设定的 IP 地址未有响应，本负载平衡器将会重新进行联机动作，确保联机状态正常。
- IP 地址：键入 ISP 配发的固定 IP 地址。
- 子网掩码 键入 ISP 配发的子网掩码。
- 预设网关：键入 ISP 配发的预设网关地址。
- DNS 服务器 1/2：键入 ISP 所配发的 DNS 1/2 服务器地址。(*详见附注*)
- 下载频宽：输入联机下载最大频宽
- 上传频宽：输入联机上传最大频宽
- Ping：勾选此项，允许远程用户 Ping 外部网络接口地址。
- WebUI：勾选此项，允许远程用户使用 HTTP 联机至负载平衡器设定画面。

步驟2． 将所有接口地址设定好后，点选屏幕右下方【确定】按钮。

图 2-5 指定 IP 地址(固接或 ADSL 专线使用者)设定

若自行架设 DNS 服务器，需先至【虚拟服务器】功能中，将原先 DNS 服务器的真实 IP 地址对应至内部或非军事区 DNS 服务器的虚拟 IP 地址，而在此处 DNS 服务器地址中，则必需键入内部或非军事区 DNS 服务器的虚拟 IP 地址。

外部网络接口 2 设定方法

步驟1. 在左方的功能选项中，点选【接口地址】功能，再点选【外部网络】次功能选项,再点选外部网络接口中变更 1/2 修改。

设定外部网络接口 2 时,需将外部网络 2 〔开启〕 方可进行设定…其余设定均同外部网络设定方法。(如图 2-6)

图 2-6 外部网络 2 设定方法

非军事区网络接口设定

步驟1. 在左方的功能选项中，点选【接口地址】功能，再点选【非军事区网络】次功能选项。*(如图2-7)*

图 2-7 非军事区网络设定

步驟2. 设定非军事区网络接口时,需将非军事区网络选项【**开启**】选择 NAT Mode 或是 DMZ_Transparent Mode 进行设定

- IP 地址 ： 键入非军事区之 IP 地址。
- 子网掩码: 键入非军事区之子网掩码。
- Ping：勾选此项，激活负载平衡器允许内（外）部网络所有接口地址 Ping。
- WebUI：勾选此项，激活非军事区接口地址联机至负载平衡器设定画面。

步驟3. 将所有接口地址设定好后，点选屏幕右下方【确定】按钮。

第三章

位 址 表

本负载平衡器在此单元中提供系统主管理员，定义内部网络、内部网络群组、外部网络、外部网络群组、非军事区网络、非军事区网络群组的接口地址。

【地址表】纪录的 IP 地址可能是一个主机 IP 地址，也可能是一个网域多个 IP 地址。系统管理员可以自行设定一个易辨识的名字代表此一 IP 地址。基本上 IP 地址根据不同的网络区可分为三种：内部网络 IP 地址(Internal IP Address)、外部网络 IP 地址(External IP Address) 和非军事区网络 IP 地址(DMZ IP Address)。当系统管理员欲将不同 IP 地址封包的过滤规则，加入相同管制条例时，可先将这些 IP 地址建立一个「内部网络群组」、「外部网络群组」或是「非军事区网络群组」，以简化设立管制条例工作程序。

如何运用地址表

有了易辨识的 IP 地址的名称后，同时地址群组名称也已显示在地址表上，系统管理员在设定管制条例时，就可选用此地址表名称，套用在管制条例的来源地址(Source Address)或目的地址(Destination Address)。所以地址表的设定应该在管制条例的设定之前，如此在设定管制条例时，才可在地址表中挑出正确的 IP 地址名称。

地址表之【内部网络】功能

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【内部网络】次功能选项。 *(如图3-1)*

图 3-1 内部网络地址功能设定

步驟2. 内部网络工作窗口之表格名词定义：

- 名称：内部网络计算机名称。
- IP：内部网络计算机 IP 地址。
- 子网掩码：子网掩码。
- MAC 地址：内部网络计算机 IP 地址对应的 MAC 地址。
- 变更：变更内部网络中各项设定值。点选【修改】，可修改内部网络各项参数信息；点选【删除】，可删除该项设定。

在内部网络窗口中，若是某个地址表成员已被加入管制条例或网络群组之中。则在【变更】字段中，将会出现【使用中】文字，无法进行修改或删除的变更设定。

新增内部网络地址

步驟1. 点选【新增】功能按钮。

步驟2. 在新增地址窗口中，键入新内部网络地址之网络名称、IP 地址、子网掩码、MAC 地址等各项参数值。 *（如图3-2）*

步驟3. 勾选【从 DHCP 服务器取得固定 IP 地址】，可使此 MAC 地址每次皆取得同一 IP 地址。

步驟4. 点选屏幕下方【确定】按钮，新增指定的内部网络，或点选【取消】取消设定。

图 3-2 新增内部网络地址

若欲使用【从 DHCP 服务器取得固定 IP 地址】功能，必须先键入 MAC 地址，此功能才可生效。

变更内部网络地址

步驟1. 在【内部网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在【变更地址】窗口中，键入各项欲变更的路径地址。 *（如图3-3）*

步驟3. 点选屏幕右下方【确定】按钮，变更设定，或点选【取消】取消变更。

图 3-3 变更内部网络位置

删除内部网络地址

步驟1. 在【内部网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】内部网络地址对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。 *（如图3-4）*

图 3-4 删除内部网络地址设定

内部网络群组功能设定

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【内部网络群组】次功能选项。 *(如图3-5)*

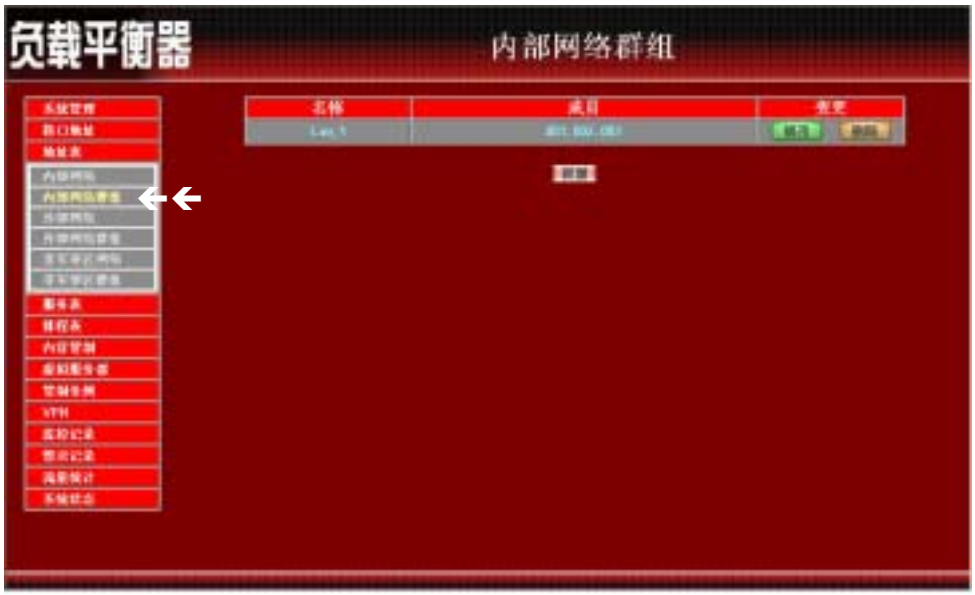


图 3-5 内部网络群组功能设定

步驟2. 内部网络群组工作窗口之表格名词定义：

- 名称：内部网络群组名称。
- 成员：该群组成员。
- 变更：变更内部网络群组中各项设定值。点选【修改】，可修改内部网络群组各项参数信息；点选【删除】，可删除该群组。

在【内部网络群组】工作窗口中，若是某个网络群组已被加入管制条例中，【变更】栏中会出现【使用中】文字，而无法进行修改或删除设定。需先至管制条例删除该项设定，才可进行变更设定。

新增内部网络群组

步驟1. 在内部网络群组窗口中，点选【新增】内部网络群组功能按钮。

步驟2. 在出现的新增位置群组窗口中 *（如图3-6）*

可选取的地址：显示内部网络所有组员名单。
被选取的地址：显示登录至新群组的组员名单。

- 名称：键入新群组名称。
- 新增组员：由【可选取的地址】选单中，点选欲登录之组员名称，再点选【Add＞＞】，将该成员加入新群组组员名单中。
- 删除组员：在【被选取的地址】选单中，点选欲删除之组员名称，再点选【＜＜Remove】，将该组员由群组中删除。

步驟3. 点选【确定】执行新增群组；或点选【取消】取消新增。

图 3-6 新增内部网络群组

变更内部网络群组设定

步驟1. 在内部网络群组窗口中，找到欲变更设定的网络群组名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在出现的变更地址群组窗口中 *（如图3-7）*

- 名称：键入新群组名称。
- 新增组员：由【可选取的地址】选单中，点选欲登录之组员名称，再点选【Add＞＞】，将该成员加入新群组组员名单中。
- 删除组员：在【被选取的地址】选单中，点选欲删除之组员名称，再点选【＜＜Remove】，将该组员由群组中删除。

步驟3. 点选【确定】执行变更群组；或点选【取消】取消变更。

图 3-7 变更内部网络群组设定

删除内部网络群组

步驟1. 在【内部网络群组】的表格中，找到欲删除的内部网络群组，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】内部网络群组对话框中，点选【确定】按钮，删除设定，或点选【取消】取消删除。 *（如图3-8）*

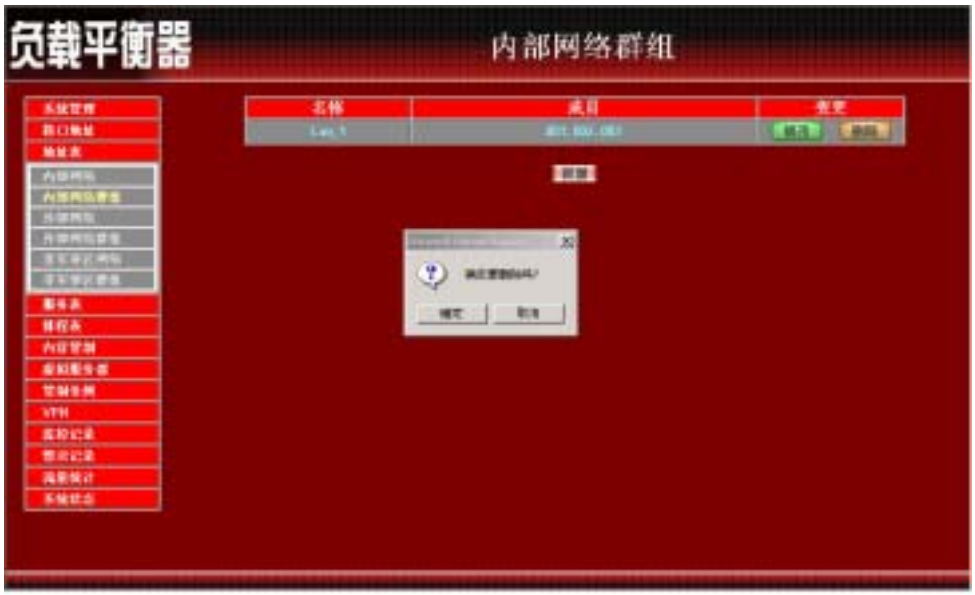


图 3-8 删除内部网络群组

外部网络功能设定

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【外部网络】次功能选项。 *(如图3-9)*

图 3-9 外部网络设定功能

步驟2. 外部网络工作窗口之表格名词定义：

- 名称：外部网络名称。
- IP 地址/子网掩码：连结目的网域之 IP 地址与子网掩码。
- 变更：变更外部网络中各项设定值。点选【修改】，可修改外部网络各项参数；点选【删除】，可删除该项设定。

在外部网络窗口中，若是某个地址表成员已被加入管制条例或网络群组之中，【变更】栏中会出现【使用中】文字，无法进行修改或删除的变更设定。

新增外部网络地址

步驟1. 点选【新增】外部网络地址功能按钮。

步驟2. 在【新增位置】窗口中，键入新外部网络各项参数值。 *（如图3-10）*

步驟3. 点选屏幕下方【确定】按钮，新增指定外部网络，或点选【取消】取消设定。

图 3-10 新增外部网络地址

变更外部网络地址

步驟1. 在【外部网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在【变更地址】窗口中，键入各项欲变更的路径地址。 *（如图3-11）*

步驟3. 点选屏幕下方【确定】按钮，变更设定，或 点选【取消】取消变更。

图 3-11 变更外部网络地址

删除外部网络地址

步驟1. 在【外部网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】外部网络地址对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。 *（如图3-12）*

图 3-12 删除外部网络地址

外部网络群组功能设定

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【外部网络群组】次功能选项。 *(如图3-13)*

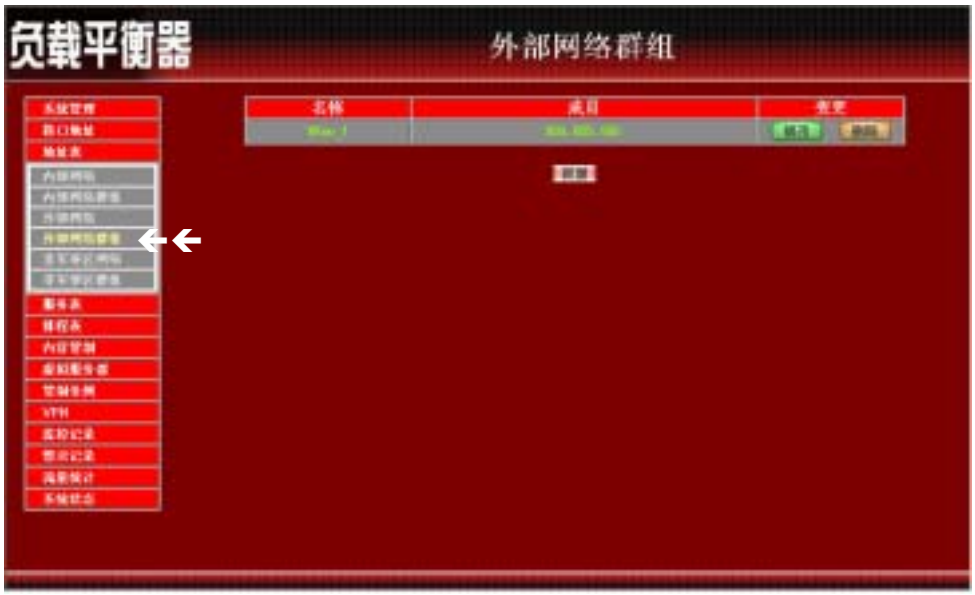


图 3-13 外部网络群组功能设定

步驟2. 外部网络群组工作窗口之表格名词定义：

- 名称：外部网络群组名称。
- 成员：该群组成员。
- 变更：变更外部网络群组中各项设定值。点选【修改】，可修改外部网络群组各项参数；点选【删除】，可删除该群组。

在【外部网络群组】工作窗口中，若是某个网络群组已被加入管制条例中，在【变更】栏会出现【使用中】文字，无法进行修改或删除的变更设定，需先至管制条例删除该向设定，才可进行变更设定。

新增外部网络群组

步驟1. 在外部网络群组窗口中，点选【新增】外部网络群组功能按钮。

步驟2. 在出现的新增地址群组窗口中 *(如图3-14)*

可选取的地址：显示外部网络所有组员名单。
被选取的地址：显示登录至新群组的组员名单。

- 名称：键入新群组名称。
- 新增组员：由【可选取的地址】选单中，点选欲登录之组员名称，再点选【Add＞＞】，将该成员加入新群组组员名单中。
- 删除组员：在【被选取的地址】选单中，点选欲删除之组员名称，再点选【＜＜Remove】，将该组员由群组中删除。

步驟3. 点选【确定】执行新增群组；或点选【取消】取消新增。

3-14 新增外部网络群组

变更外部网络群组设定

步驟1. 在外部网络群组窗口中，找到欲变更设定的网络群组名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在出现的变更地址群组窗口中 *（如图3-15）*

- 名称：键入新群组名称。
- 新增组员：由【可选取的地址】选单中，点选欲登录之组员名称，再点选【Add＞＞】，将该成员加入新群组组员名单中。
- 删除组员：在【被选取的地址】选单中，点选欲删除之组员名称，再点选【＜＜Remove】，将该组员由群组中删除。

步驟3. 点选【确定】执行变更群组；或点选【取消】取消变更。

3-15 变更外部网络群组设定

删除外部网络群组

步驟1. 在【外部网络群组】的表格中，找到欲删除的外部网络群组，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】外部网络群组对话框中，点选【确定】按钮，删除设定，或点选【取消】取消删除。 *（如图3-16）*

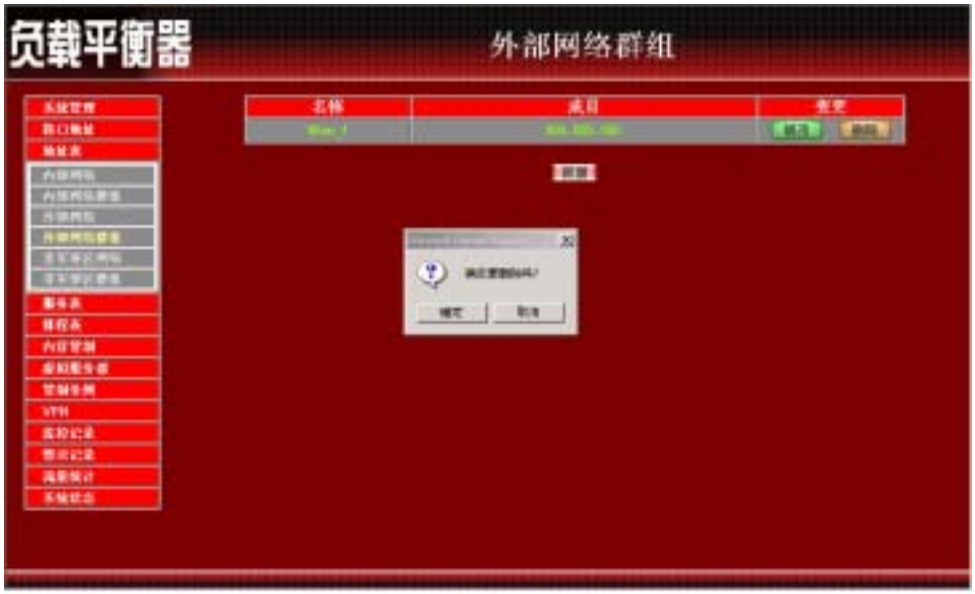


图 3-16 删除外部网络群组

非军事区网络功能设定

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【非军事区网络】次功能选项。 *（如图3-17）*

图 3-17 非军事区网络设定功能

步驟2. 非军事区网络工作窗口之表格名词定义：

- 名称：非军事区网络名称。
- IP 地址/子网掩码：连结目的网域之 IP 地址与子网掩码。
- MAC 地址：非军事区网络计算机 IP 地址对应的 MAC 地址。
- 变更：变更非军事区网络中各项设定值。点选【修改】，可修改非军事区网络各项参数；点选【删除】，可删除该项设定。

在非军事区网络窗口中，若是某个地址表成员已被加入管制条例或网络群组之中，【变更】栏中会出现【使用中】文字，无法进行修改或删除的变更设定。

新增非军事区网络地址

步骤1. 点选【新增】非军事区网络地址功能按钮。

步骤2. 在【新增位置】窗口中，键入新非军事区网络各项参数值。 *（如图3-18）*

步骤3. 点选屏幕下方【确定】按钮，新增指定非军事区网络，或点选【取消】取消设定。

图 3-18 新增非军事区网络地址

变更非军事区网络地址

步驟1. 在【非军事区网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在【变更地址】窗口中，键入各项欲变更的路径地址。 *（如图3-19）*

步驟3. 点选屏幕下方【确定】按钮，变更设定，或 点选【取消】取消变更。

图 3-19 变更非军事区网络地址

移除非军事区网络地址

步驟1. 在【非军事区网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定移除】非军事区网络地址对话框中，点选【确定】按钮，移除设定，或 点选【取消】取消移除。 *(如图3-20)*

图 3-20 移除非军事区网络地址

非军事区网络群组功能设定

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【非军事区网络群组】次功能选项。 *(如图3-21)*

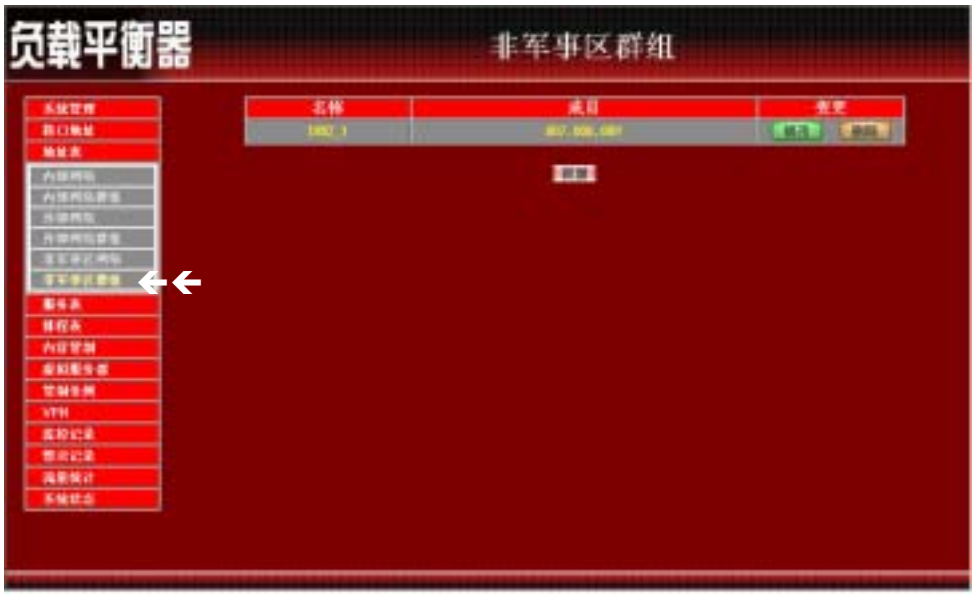


图 3-21 非军事区网络群组功能设定

步驟2. 非军事区网络群组工作窗口之表格名词定义：

- 名称：非军事区网络群组名称。
- 成员：该群组成员。
- 变更：变更非军事区网络群组中各项设定值。点选【修改】，可修改非军事区网络群组各项参数；点选【删除】，可删除该群组。

在【非军事区网络群组】工作窗口中，若是某个网络群组已被加入管制条例中，在【变更】栏会出现【使用中】文字，无法进行修改或删除的变更设定，需先至管制条例移除该向设定，才可进行变更设定。

新增非军事区网络群组

步驟1. 在非军事区网络群组窗口中，点选【新增】功能按钮。

步驟2. 在出现的新增地址群组窗口中 *（如图3-22）*

可选取的地址：显示非军事区网络所有组员名单。
被选取的地址：显示登录至新群组的组员名单。

- 名称：键入新群组名称。
- 新增组员：由【可选取的地址】选单中，点选欲登录之组员名称，再点选【Add＞＞】，将该成员加入新群组组员名单中。
- 移除组员：在【被选取的地址】选单中，点选欲移除之组员名称，再点选【＜＜Remove】，将该组员由群组中移除。

步驟3. 点选【确定】执行新增群组；或点选【取消】取消新增。

图 3-22 新增非军事区网络群组

变更非军事区网络群组设定

步驟1. 在外部网络群组窗口中，找到欲变更设定的网络群组名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在出现的变更地址群组窗口中 *（如图3-23）*

- 名称：键入新群组名称。
- 新增组员：由【可选取的地址】选单中，点选欲登录之组员名称，再点选【Add＞＞】，将该成员加入新群组组员名单中。
- 移除组员：在【被选取的地址】选单中，点选欲移除之组员名称，再点选【＜＜Remove】，将该组员由群组中移除。

步驟3. 点选【确定】执行变更群组；或点选【取消】取消变更。

图 3-23 变更非军事区网络群组设定

移除非军事区网络群组

步驟1. 在【非军事区网络群组】的表格中，找到欲移除的非军事区网络群组，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定移除】外部网络群组对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。 *（如图3-24）*

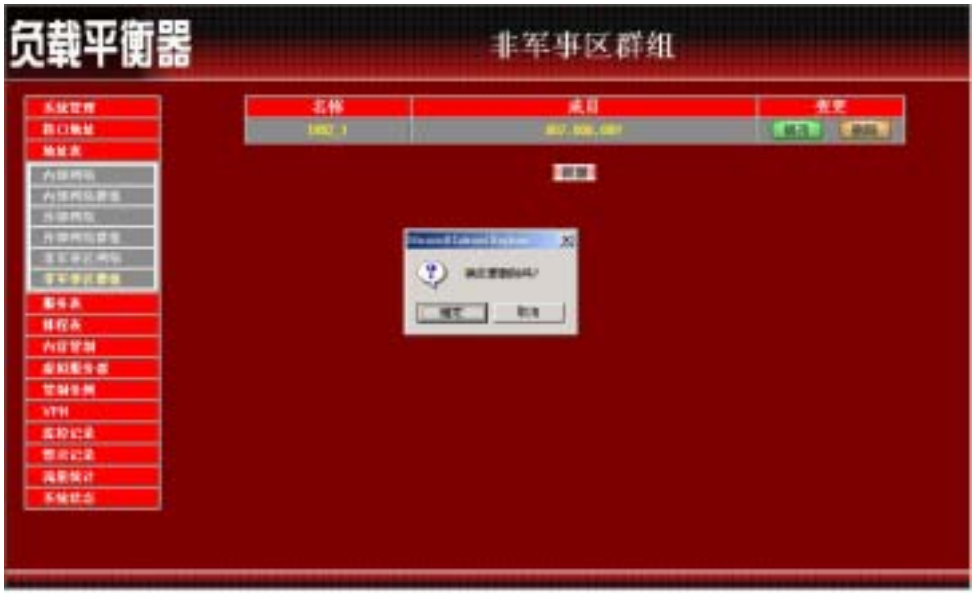


图 3-24 移除非军事区网络群组

第四章

服 务 表

TCP 协议和 UDP 协议提供各种不同的服务，每一个服务都有一个 TCP 端口(TCP Port)号码或 UDP 端口号码代表，如 TELNET(23)，FTP(21)，SMTP(25)，POP3(110)，…等。本产品的服务包含两个部分 ： 基本服务表和自订服务表，比较常用的 TCP 服务或 UDP 服务已预告定义在基本服务表，此类服务不能修改也不可删除。另外使用者也可依自己的需求到自订服务表设定适当 TCP 端口和 UDP 端口号码。在自订服务时，客户端端口(Client Port)设定的区间一般为 1024：65535，服务器端端口(Server Port)号码则是设定在 0:65535 之间。

本负载平衡器在此单元中，将一些常用的网络服务列入各项表列的服务选单中（基本服务、自订服务与服务群组）。系统主管理员只需依照下列操作说明，将网络协议与出入端口号码定义在各种网络通讯应用中，客户端即可与各种不同服务器联机，传输资料。

如何运用服务表

系统管理员可以在【服务表】的【服务群组】选项中，新增服务群组名称，将要提供的服务包含进去。有了服务群组的功能，管理员在制订管制条例时可以简化许多流程。例如，有 10 个不同 IP 地址可以对服务器存取 5 个不同的服务，如 HTTP、FTP、SMTP、POP3 和 TELNET，如果不使用服务群组的功能，总共需制订 10x5=50 条管制条例，但使用服务群组名称套用在服务选项上，则只需一条管制条例即可达到 50 条管制条例的功能。

服务表之【基本服务】功能

步骤1. 在左方的功能选项中，点选【服务表】功能，再点选【基本服务】次功能选项。*（如图 4-1）*

图 4-1 基本服务表

步骤2. 基本服务表窗口表格内图标与名词名称定义：

图标	说明
ANY	任何服务。
TCP	TCP 服务，如：FTP、FINGER、HTTP、、HTTPS 、IMAP、SMTP、POP3、ANY、AOL、BGP、GOPHER、InterLocator、IRC、L2TP、LDAP、NetMeeting、NNTP、PPTPReal、 Media、RLOGIN、SSH、TCP ANY、TELNET、VDO Live、WAIS、WINFRAME、X-WINDOWS、AFPoverTCP、Real-Media 等。
UDP	UDP 服务，如：IKE、DNS、NTP、IRC、RIP、SNMP、SYSLOG、TALK、TFTP、UDP-ANY、UUCP、PC-Anywhere 等。
ICMP	ICMP 服务，如：PING、TRACEROUTE 等。

自订服务功能设定

步驟1. 在左方的功能选项中，点选【服务表】功能，再点选【自定服务】次功能选项。*(如图 4-2)*

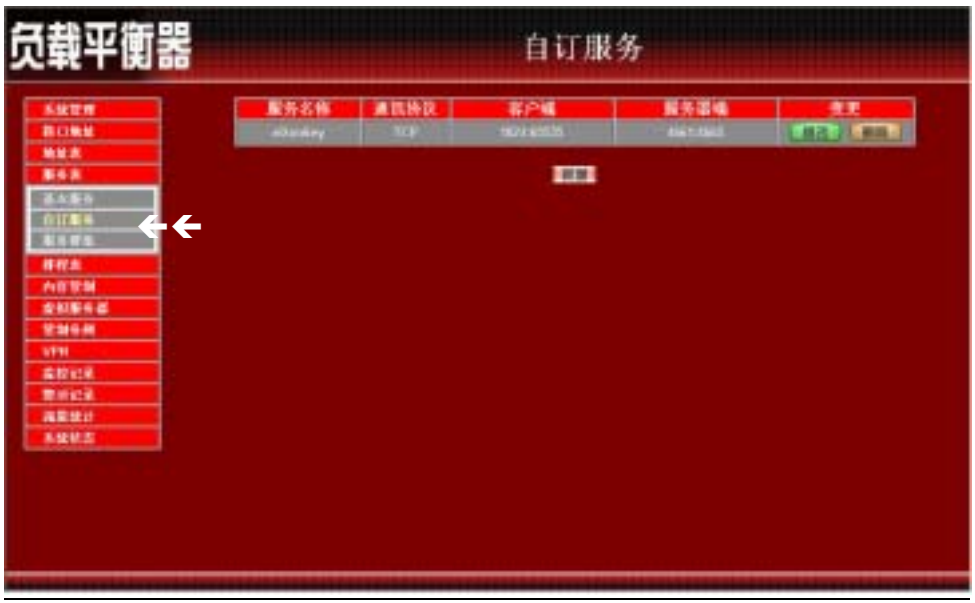


图 4-2 自订服务功能设定

步驟2. 自订服务工作窗口之表格名词定义：

- 服务名称：自订服务项目名称。
- 通讯协议：【基本设定】中所使用的网络协议。如 TCP、UDP，或其它（请选择代码）。
- 客户端：自定服务项目中之客户端的出入端口范围。
  在客户端两个空格内输入的 port 号如为不同端口号，则是开启端口号为两个空格内输入 port 号的中间范围。
  在客户端两个空格内输入的 port 号如为相同端口号，则是开启端口号为同一个 port 号

- 服务器端：自定服务项目中之服务器端的出入端口范围。
  在服务器端两个空格内输入的 port 号如为不同端口号，则是开启端口号为两个空格内输入 port 号的中间范围。
  在服务器端两个空格内输入的 port 号如为相同端口号，则是开启端口号为同一个 port 号
- 变更：变更服务表中各项设定值。点选【修改】，可修改服务表各项参数；点选【删除】，可删除该项设定。

 *在自订服务工作窗口中，若是某个服务已被加入管制条例或服务群组之中。【变更】栏会出现【使用中】，而无法进行修改或删除的变更设定，需先至管制条例或服务群组中，删除该项设定，才可执行变更。*

新增自订服务

步驟1. 在【自订服务】表格中，点选【新增】功能按钮。

步驟2. 在出现的新增自订服务窗口中 *(如图4-3)*

- 服务名称：输入新服务名称。
- 通讯协议：勾选【基本设定】中所使用的网络协议。如 TCP、UDP，或其它（请选择代码）。
- 客户端： 输入新服务之客户端的出入端口范围。

  在客户端两个空格内输入的 port 号如为不同端口号，则是开启端口号为两个空格内输入 port 号的中间范围。

  在客户端两个空格内输入的 port 号如为相同端口号，则是开启端口号为同一个 port 号
- 服务器端：输入新服务之服务器端的出入端口范围。

  在服务器端两个空格内输入的 port 号如为不同端口号，则是开启端口号为两个空格内输入 port 号的中间范围。

  在服务器端两个空格内输入的 port 号如为相同端口号，则是开启端口号为同一个 port 号

步驟3. 点选【确定】执行新增服务；或点选【取消】取消新增。

图 4-3 新增自订服务

变更自订服务

步驟1. 在【自订服务】窗口中，找到欲变更设定的服务名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在出现的变更自订服务窗口中 *（如图4-4）*

- 服务名称：输入新服务名称。
- 通讯协议：勾选【基本设定】中所使用的网络协议。如 TCP、UDP，或其它（请选择代码）。
- 客户端： 输入新服务之客户端的出入端口范围。
  在客户端两个空格内输入的 port 号如为不同端口号，则是开启端口号为两个空格内输入 port 号的中间范围。
  在客户端两个空格内输入的 port 号如为相同端口号，则是开启端口号为同一个 port 号
- 服务器端：输入新服务之服务器端的出入端口范围。
  在服务器端两个空格内输入的 port 号如为不同端口号，则是开启端口号为两个空格内输入 port 号的中间范围。
  在服务器端两个空格内输入的 port 号如为相同端口号，则是开启端口号为同一个 port 号

步驟3. 点选【确定】执行变更服务；或点选【取消】取消变更。

图 4-4 变更自订服务

删除自订服务

步驟1. 在【自订服务】窗口表格中，找到欲变更设定的服务名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【删除服务】确定对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。*（如图4-5）*

图 4-5 删除自订服务

服务群组功能设定

步驟1. 在左方的功能选项中，点选【服务表】功能，再点选【服务群组】次功能选项。*(如图 4-6)*

图 4-6 服务群组功能设定

步驟2. 服务群组工作窗口之表格名词定义：

- 群组名称：所有已设定之服务群组名称。
- 服务名称：该服务群组服务项目。
- 变更：变更服务群组中各项设定值。点选【修改】，可修改服务群组各项参数；点选【删除】，可删除该群组。

在【服务群组】工作窗口中，若是某个服务群组已被加入管制条例中，则在【变更】栏会出现【使用中】，而无法进行修改或删除的变更设定，需先至管制条例中，删除该项设定，才可执行变更。

新增服务群组

步驟1. 在服务群组窗口中，点选【新增】功能按钮。

步驟2. 在出现的新增服务群组窗口中 *(如图4-7)*

可选取的服务：显示所有有效的服务项目。
被选取的服务：显示针对新增服务群组所选择的服务项目。

- 名称：键入新服务群组名称。
- 新增服务项目：在【可选取的服务】选单中，点选欲增加的服务项目名称，再点选【Add＞＞】，将该服务项目加入新群组。
- 删除服务项目：在【被选取的服务】字段中，点选欲删除之服务项目名称，再点选【＜＜Remove】，将该服务项目自群组中删除。

步驟3. 点选【确定】执行新增群组；或点选【取消】取消新增。

图 4-7 新增服务群组

变更服务群组

步驟1. 在内部网络群组窗口中，找到欲变更设定的网络群组名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在出现的变更服务群组窗口中 *（如图4-8）*

- 名称：键入新群组名称。
- 新增组员：由【可选取的服务】选单中，点选欲登录之组员名称，再点选【Add＞＞】，将该成员加入新群组组员名单中。
- 删除组员：在【被选取的服务】选单中，点选欲删除之组员名称，再点选【＜＜Remove】，将该组员由群组中删除。

步驟3. 点选【确定】执行变更群组；或点选【取消】取消变更。

图 4-8 变更服务群组

删除服务群组

步驟1. 在【服务群组】的表格中，找到欲删除的服务群组，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】服务群组确认对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。*（如图 4-9）*

图 4-9 删除服务群组

第五章

排 程 表

本负载平衡器在此单元中提供系统主管理员，在排程表中定义网络系统连结与执行的时间区段，以便在【管制条例】功能中，选择特定时间内开放资料封包的出入。利用排程表的自动执行功能，系统管理员可以节省许多时间，同时让网络系统发挥最大的效能。

如何运用排程表

系统管理员可利用排程表功能，设定系统在多个不同的时间区段内，自动执行设定封包流向的【管制条例】功能。

排程表功能设定

步驟1. 在左方的功能选项中，点选【排程表】功能。*(如图5-1)*

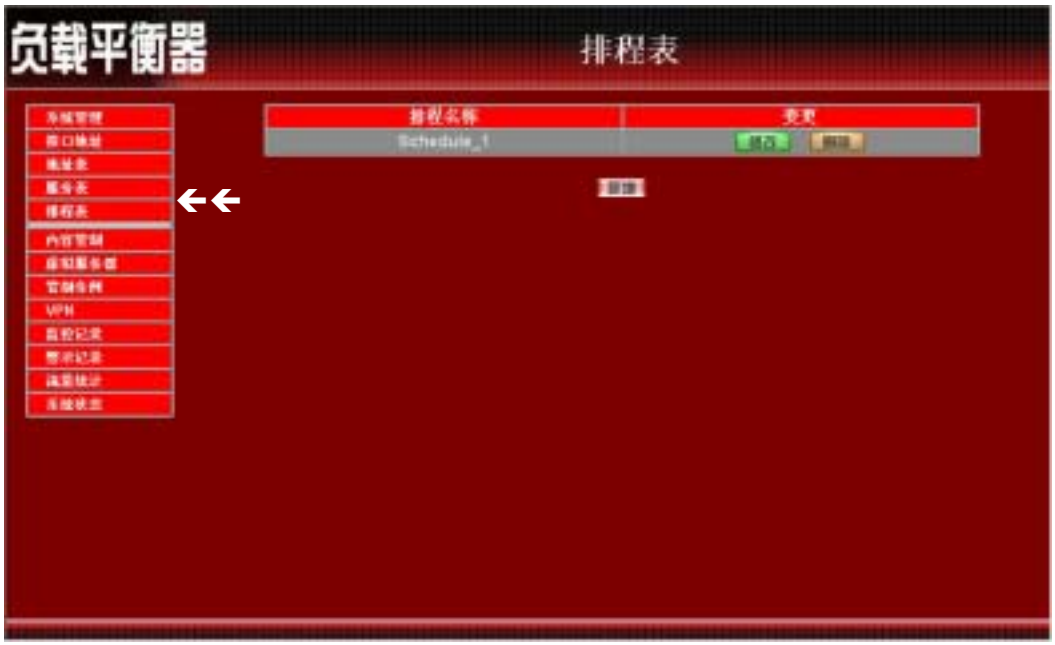


图 5-1 排程表功能设定

步驟2. 排程表工作窗口之表格名词定义：

- 排程名称：管理者所定义之排程表名称。
- 变更：变更排程表中各项设定值。点选【修改】，可修改排程表各项参数；点选【删除】，可删除该项设定。

在排程表工作窗口中，若是某个排程已被加入【管制条例】之中。【变更】栏会出现【使用中】，而无法进行修改或删除的变更设定，需先至【管制条例】中，删除该项设定，才可执行变更。。

新增排程表

步驟1. 点选【新增】功能按钮。

步驟2. 在出现的【新增排程】窗口中 *(如图5-2)*

- 排程名称：输入新排程名称。
- 时段：在每周特定日期的表格内，于【起始时间】与【结束时间】的下拉选单中，点选有效执行的时间范围。

步驟3. 点选【确定】执行新增排程表；或点选【取消】取消新增。

图 5-2 新增排程表

制订排程表时，【起始时间】字段，必须小于【结束时间】字段，否则无法进行新增或修改的设定。

变更排程表

步驟1. 在【排程表】窗口中，找到欲变更设定的排程表名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在出现的变更排程窗口中，键入新排程表名称，并设定排程表时间范围 *（如图5-3）*

步驟3. 点选【确定】执行变更；或点选【取消】取消变更。

图 5-3 变更排程表

删除排程表

步驟1. 在【排程表】窗口表格中，找到欲变更设定的排程表名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【删除排程表】确定对话框中，点选【确定】按钮，删除设定，或点选【取消】取消删除。*（如图5-4）*

图 5-4 删除排程表

第六章

内 容 管 制

内容管制分为「网站管制」与「Script 管制」两种。

（一）【网站管制】：系统管理员可使用完整网域名称、关键词、万用字符（〝～〝及〝＊〞）针对特定网站作「开放」或「限制」进入的设订。

（二）【Script 管制】：管制 Popup、ActiveX、Java、Cookie「开放」或「限制」执行。

如何运用内容管制

系统管理员可使用完整网域名称、关键词、万用字符（〝～〝及〝＊〞）针对特定网站作「开放」或「限制」进入的设订。

网站管制功能设定

设定管制的网站，系统管理员可使用完整网域名称、关键词、万用字符（〝～〝及〝＊〞）针对特定网站作「开放」或「限制」进入的设订。

步驟1. 于左方功能选项，先点选【内容管制】，接着点选下方的【网站管制】，进入【网站管制】工作窗口。*(如图6-1)*

图 6-1 进入网站管制功能设定

步驟2. 网站管制工作窗口名词定义：

- 网站名称：受到负载平衡器管制进入或仅开放进入的网域名称。
- 变更：变更网站管制中各项设定值。点选【修改】，可修改网站管制各项参数；点选【删除】，可删除该项设定。

步驟3. 网站管制使用方法：

符号说明：〝～〞表示开放；〝＊〞表示万用字符。

限制无法进入特定网站：在新增网站管制功能的网站名称中，键入欲禁止网站的「完整网域名称」、或「关键词」。如：www.yahoo.com 或 yahoo。

仅开放特定网站可进入：

1. 先将欲开放网站一一加入网站管制中，新增时，必须于「完整网域名称」、或「关键词」前加入表示开放进入的符号〝～〞。(如：～www.yahoo.com 或～yahoo)。
2. 在所有欲开放的网站设定完成后，于最后一条欲开放的网站管制后，新增一条全部禁止的指令，亦即在网站名称中，仅键入〝＊〞。*注意！*此全部禁止的指令必须永远放置于最后。*(如下图)*
3. 若欲新增开放网站，必须先将全部禁止指令删除，再键入新网域名称，完成后，再重新加入全部禁止指令。

新增网站管制

步驟1. 点选下方【新增】网站管制功能按钮。

步驟2. 在新增网站管制窗口，网站名称空栏中，键入欲管制进入的网址或关键词。 *（如图6-2）*

步驟3. 点选【确定】新增网站管制，或【取消】取消新增。

图 6-2 新增网站管制

变更网站管制

步驟1. 在【网站管制】的表格中，找到欲变更设定的网站名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在【修改网站管制】窗口中，键入新网站的网址。 *(如图 6-3)*

步驟3. 点选屏幕下方【确定】按钮，变更设定，或 点选【取消】取消变更。

图 6-3 变更网站管制

删除网站管制

步驟1. 在【网站管制】的表格中，找到欲删除设定的网站名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】网站管制对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。 *（如图6-4）*

图 6-4 删除网站管制

Script 管制功能设定

步驟1. 在左方的功能选项中，点选【内容管制】功能，再点选【Script 管制】次功能选项。

步驟2. 【Script 管制】各项侦测功能说明 *(如图 6-5)*

图 6-5 负载平衡器 Script 管制功能设定

- Popup 管制：可阻挡自动弹跳出的窗口。
- ActiveX 管制：可阻挡 ActiveX 封包。
- Java 管制：可阻挡 Java 封包。
- Cookie 管制：可阻挡 Cookie 封包。

步驟3. 勾选各项侦测功能后，点选屏幕右下方【确定】按钮。

完成此部分设定后，当系统侦测到管制现象时，负载平衡器将会自动阻档。

第七章

虚 拟 伺 服 器

负载平衡器将企业内部网络与网际网络(Internet) 分隔成内部网络与外部网络，因IP地址已不够分配，企业内的内部网络为了有足够的IP地址分配给每一台计算机，大都是将计算机设定成私有IP地址（ Private IP Address)，透过负载平衡器的NAT (Network Address Translation) 功能，转换成真实IP地址(Real IP Address)，如果对外提供服务的服务器是置于内部网络时，它的私有IP地址将无法让外部的使用者直接联机使用。

对于此类问题，可使用本负载平衡器的虚拟服务器功能得以解决，所谓虚拟服务器是将负载平衡器外部接口子网络的一个真实IP地址设成虚拟服务器IP地址，藉由负载平衡器IP转换的功能，将外部使用者寻求服务的联机，由虚拟服务器IP地址转换成内部网络实际提供服务服务器的私有IP地址。

虚拟服务器还拥有一项特色，一对多的对映功能，即一个外部接口的虚拟服务器 IP 地址可对映到四部提供相同服务的内部网络服务器的私有 IP 地址，因虚拟服务器提供负载平衡(Load Balance)功能，可将寻求服务的联机，依权值比重分配给内部网络的服务器群组，如此可减少服务器的负载，降低当机的风险，提高服务器的工作效率。

于本章节，将针对【IP 对映】、【虚拟服务器 1/2/3/4】作详细的介绍与使用说明：

【IP 对映】：因为内部网络是透过 NAT（Network Address Translation）机制转换的私有 IP 地址，如果服务器放于内部网络时，它的 IP 地址是属于私有 IP（Private IP）地址；外部网络的使用者无法直接连上其私有 IP 地址，必须先连接上外部接口子网络真实 IP（Real IP）地址，再由真实 IP 地址对映到内部网络私有 IP 地址，对映的方式有「IP 对映」与「虚拟服务器」两项。「IP 对映」是一对一对映，即一个外部接口真实 IP 地址的所有服务，对映到一个内部网络私有 IP 地址。

【虚拟服务器 1/2/3/4】：虚拟服务器是一对多对映，即一个外部接口真实 IP 地址，对映到 1～4 个内部网络私有 IP 地址，并提供【服务表】中基本服务之项目。

如何运用虚拟服务器

虚拟服务器和IP对映是因NAT转换机制而产生IP地址对映方式，他们是运用于【管制条例】中【由外部至内部网络】的管制条例，虚拟服务器和IP对映两者功能相当类似，都是以真实IP地址对映到私有IP地址（和NAT转换方式相反）实际的服务器是放在私有IP地址上，但是它们之间仍有些差异性存在：

- 虚拟服务器可以对映到内部多台服务器，IP对映只能对映到一台内部服务器，并且虚拟服务器有负载平衡（Load Balance）功能，将服务的联机对映到不同的服务器主机。
- 虚拟服务器只能对映内部实际服务器某一种服务项目，而IP对映可对映到实际服务器所有服务。

无论是 IP 对映或是虚拟服务器，都是运用将外部接口虚拟服务器的 IP 地址转换成内部网络实际提供服务的服务器的私有 IP 地址的功能，使得外部网络的使用者可由与虚拟服务器的 IP 地址寻求服务联机而顺利的使用内部网络的服务器。

IP 对映功能设定

步驟1. 在左方的功能选项中，点选【虚拟服务器】功能，再点选【IP 对映】次功能选项。 *（如图7-1）*

图 7-1 IP 对映功能设定

步驟2. IP 对映表格说明：

- 外部网络地址：外部网络 IP 地址。
- 对映到虚拟网络地址：该外部网络对映至内部服务器之虚拟网络所指定的 IP 地址。
- 变更：变更 IP 对映各项设定值。点选【修改】，可修改 IP 对映各项参数；点选【删除】，可删除该项设定。

新增 IP 对映

步驟1. 在 IP 对映窗口中，点选【新增】功能按钮。

步驟2. 在出现的新增对映 IP 窗口中，键入下列相关参数 *（如图 7-2）*

- 外部网络地址：键入外部网络地址。
- 对映到虚拟网络地址：键入该外部网络对映至虚拟网络的指定 IP 地址。

步驟3. 点选屏幕右下方【确定】按钮，新增指定的 IP 对映，或点选【取消】取消新增。

图 7-2 新增 IP 对映

变更 IP 对映

步驟1. 在【IP 对映】窗口中，找到欲变更设定的 IP 对映，对映至右方【变更】栏，点选【修改】。

步驟2. 在出现的【修改对映 IP】窗口中，键入欲变更的参数值 *（如图 7-3）*

步驟3. 点选屏幕下方【确定】按钮，变更指定的 IP 对映设定，或点选【取消】取消变更设定。

图 7-3 变更 IP 对映

若在【外部至内部】管制条例中的目的地址，已设定某 IP 对映，则无法对该条 IP 对映作变更之动作。

删除 IP 对映

步驟1. 在【IP 对映】窗口中，找到欲变更设定的 IP 对映列，对映至右方【变更】栏，点选【删除】。

步驟2. 在【删除 IP 对映】确定对话框中，点选【确定】按钮，删除设定，或点选【取消】取消删除。 *（如图 7-4）*

图 7-4 删除 IP 对映

虚拟服务器 1/2/3/4 功能设定

步驟1. 在左方的功能选项中，点选【虚拟服务器】功能，再点选【虚拟服务器 1/2/3/4】次功能选项。 *（如图 7-5）*

图 7-5 虚拟服务器功能设定

步驟2. 虚拟服务器窗口内名词定义说明：

- 虚拟服务器真实 IP：此虚拟服务器所设定的外部网络 IP 地址。若尚未设定，可点选【选择】功能按钮，即可新增新虚拟服务器地址，若欲变更，则直接点选该【虚拟服务器真实 IP 地址】后，键入新 IP 地址。
- 服务名称（端口号）：此虚拟服务器所提供的服务项目名称。
- 外部网络端口号 :此虚拟服务器所提供的服务项目所代表之 TCP 端口号码或 UDP 端口号码。
- 服务器虚拟 IP：此虚拟服务器所对映的虚拟网络 IP 地址。
- 变更：变更虚拟服务器之各项服务设定值。点选【修改】，可修改 IP 对映各项参数；点选【删除】，可删除该项设定。

本虚拟服务器功能提供四个外部接口真实 IP 地址，亦即最多可设定四个虚拟服务器（由此功能选项之虚拟服务器 1/2/3/4 中设定）。系统管理员可点选虚拟服务器 1/2/3/4 工作窗口中，【虚拟服务器真实 IP】新增或变更虚拟服务器之 IP 地址；新增或变更该虚拟服务器服务设定，则点选下方【新增】功能或变更栏的【修改】按钮。

新增虚拟服务器真实 IP

步驟1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选虚拟服务器真实 IP【选择】功能按钮。

步驟2. 在【新增虚拟服务器 IP】窗口，由【虚拟服务器真实 IP】键入可使用外部网络 1/2 的 IP 地址。*（如图 7-6）*

步驟3. 点选【确定】执行新增虚拟服务器真实 IP；或点选【取消】取消新增。

7-6 新增虚拟服务器真实 IP

变更虚拟服务器 IP 地址

步骤1. 在【新增虚拟服务器 IP】窗口，由【虚拟服务器真实 IP】所使用外部网络 IP 地址中， 变更 IP 地址。*(如图7-7)*

步骤2. 点选【确定】执行变更虚拟服务器 IP 地址；或点选【取消】取消变更。

图 7-7 变更虚拟服务器 IP 地址

删除虚拟服务器 IP 地址

步骤1. 在【新增虚拟服务器 IP】窗口，由【虚拟服务器真实 IP】，清除 IP 地址。*（如图7-8）*

步骤2. 点选【确定】执行删除虚拟服务器 IP 地址；或点选【取消】取消删除。

图 7-8 删除虚拟服务器 IP 地址

虚拟服务器服务设定

步驟1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选虚拟服务器表格下方【新增】功能按钮。

步驟2. 在【虚拟服务器组态】设定对话框中 *(如图 7-9)*

图 7-9 虚拟服务器组态窗体

- 虚拟服务器真实 IP：显示此虚拟服务器所设定的外部网络 IP 地址。
- 服务名称（端口号）：此虚拟服务器所提供的服务项目及其代码。在此下拉选单内所列的服务项目名称，皆为【服务表】功能内所定义。
- 外部网络端口号：此虚拟服务器所提供的服务项目的代码。
- 负载平衡服务器：负载平衡服务器编号。
- 服务器虚拟 IP：此虚拟服务器所对映的内部服务器 IP 地址。最多可设定 4 台计算机的 IP 地址，可达到负载平衡的功能。

新增虚拟服务器服务设定

步骤1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选虚拟服务器表格下方【新增】功能按钮。

步骤2. 在【虚拟服务器组态】对话框中，键入下列参数 *（如图 7-10）*

图 7-10 新增虚拟服务器服务

- 虚拟服务器真实 IP：显示此虚拟服务器所设定的外部网络 IP 地址。
- 服务名称（端口号）：点选下拉选单内所列服务项目名称，此部分窗体内容皆为【服务表】功能中所定义之服务项目。
- 外部网络端口号：无须填写，点选上方服务名称时，系统会直接显示该服务项目代码。
- 负载平衡服务器：负载平衡服务器编号。
- 服务器虚拟 IP：此虚拟服务器所对映的内部服务器 IP 地址。最多可设定 4 台计算机的 IP 地址，可达到负载平衡的功能。

步骤3. 点选【确定】执行新增虚拟服务器服务；或点选【取消】取消新增。

系统主管理员可依需求，点选【虚拟服务器】工作窗口中的【新增】服务控制按钮，增加虚拟服务器的服务项目，并在设定【管制条例】前，完成所有虚拟服务器必须提供的服务项目。否则，于管制条例的服务名称中将不会显现，而无法选择。

变更虚拟服务器服务设定

步骤1. 在【虚拟服务器 1（或 2、3、4）】窗口中，由显示该虚拟服务器服务项目的表格中，找到欲变更设定的服务名称，对映至右方【变更】栏，点选【修改】。

步骤2. 在【虚拟服务器组态】窗口，键入欲变更的参数值 *（如图 7-11）*

图 7-11 变更虚拟服务器服务设定

- 虚拟服务器真实 IP：显示此虚拟服务器所设定的外部网络 IP 地址。
- 服务名称（端口号）：点选下拉选单内所列服务项目名称，此部分窗体内容皆为【服务表】功能中所定义之服务项目。
- 外部网络端口号：无须填写，点选上方服务名称时，系统会直接显示该服务项目代码。
- 负载平衡服务器：负载平衡服务器编号。
- 服务器虚拟 IP：此虚拟服务器所对映的内部服务器 IP 地址。最多可设定 4 台计算机的 IP 地址，可达到负载平衡的功能。

步骤3. 点选【确定】执行变更虚拟服务器服务；或点选【取消】取消变更。

若在【管制条例】中的目的网络，已设定某条虚拟服务器，则无法对该条虚拟服务器作变更动作。须先删除该项设定，才可执行变更设定。

删除虚拟服务器服务设定

步骤1. 在【虚拟服务器 1（或 2、3、4）】窗口中，由虚拟服务器服务项目的表格中，找到欲变更设定的服务名称，对映至右方【变更】栏，点选【删除】。

步骤2. 在【删除虚拟服务器】窗口，点选【确定】执行删除虚拟服务器 IP 地址；或点选【取消】取消删除。 *（如图 7-12）*

图 7-12 删除虚拟服务器服务设定

若在【管制条例】中的目的网络，已设定某条虚拟服务器，则无法对该条虚拟服务器作删除之动作。须先删除该项设定，才可执行删除动作。

第八章

管 制 条 例

负载平衡器经由管制条例的参数设定，可以控管资料封包的过滤规则。管制条例的参数包含有来源网络地址、目的网络地址、服务名称、管制动作、流量监控、流量统计、内容管制、自动排程及最高流量警示值等。系统管理员可以由这些参数，管理、设定不同出入端口间的资料传送以及服务项目，哪些网络对象、网络服务或应用程序的封包该予以拦截或放行。

本负载平衡器依据不同来源地址的资料封包，将管制条例设定功能区分为下列六项，以便利系统主管理员，针对不同资料封包的来源 IP、来源端口、目的 IP、目的端口制订管制规则。

（一）【内部至外部】：来源网络地址是在内部网络区，目的网络地址是在外部网络区。系统管理员在此功能中，制订内部网络至外部网络间所有封包的管制、服务项目的管制规则。

（二）【外部至内部】：来源网络地址是在外部网络区，目的网络地址是在内部网络区（如 IP 对映、虚拟服务器）。系统管理员在此功能中，制订外部网络至内部网络间所有封包的管制、服务项目的管制规则。

（三）【外部至非军事区】：来源网络区是外部网络区，目的网络区是在非军事区区（如 IP 对映、虚拟服务器）。系统管理员在此功能中，制订外部网络至非军事区间所有封包的管制、服务项目的管制规则。

（四）【内部至非军事区】：来源网络区是内部网络区，目的网络区是在非军事区区。系统管理员在此功能中，制订内部网络至非军事区间所有封包的管制、服务项目的管制规则。

（五）【非军事区至内部】：来源网络区是非军事区区，目的网络区是在内部网络区。系统管理员在此功能中，制订非军事区至内部网络间所有封包的管制、服务项目的管制规则。

（六）【非军事区至外部】：来源网络区是非军事区区，目的网络区是在外部网络区。系统管理员在此功能中，制订非军事区至外部网络间所有封包的管制、服务项目的管制规则。

如何运用管制条例

管制条例所需设定的参数包含有：来源网络地址、目的网络地址、服务名称、管制动作、流量监控、流量统计、内容管制、自动排程及最高流量警示值等。其中，来源网络和目的网络和 IP 地址对映的名称必需先在【地址表】定义。而服务项目，若属于【基本服务】项目中，则可直接使用，如果是属于自订服务，则必须先在【服务表】中的【自订服务】定义其服务项目名称和其对映的端口号(Port Number)。

在制订【外部至内部网络】和【外部至非军事区网络】条例时，它的目的地址为 1 对 1 对映的 IP 地址或是虚拟服务器 IP 地址，此部分需在【虚拟服务器】项目中定义，而非在【地址表】制订。

管制条例操作指引

步驟1. 至【地址表】中，定义来源网络与目的网络的名称、地址。

步驟2. 至【服务表】中，定义服务项目。

步驟3. 至【虚拟服务器】中，定义对映 IP 或虚拟服务器名称地址。（此步骤仅于定义【外部至内部网络】和【外部至非军事区网络】需操作。）

内部至外部管制条例功能设定

来源网络地址是在内部网络区，目的网络地址是在外部网络区。系统管理员在此功能中，制订内部网络至外部网络间所有封包的管制、服务项目的管制规则。

步骤1. 在左方的功能选项中，点选【管制条例】功能，再点选【内部至外部】次功能选项。 *（如图 8-1）*

图 8-1 内部网络至外部网络功能设定

步骤2. 管制条例表格说明（由内部网络至外部网络）：

- 编号：所设定之管制条例编号，此处编号由 1 开始。
- 来源网络：已于【地址表】之【内部网络】功能中所指定的内部网络地址，或所有内部网络地址。
- 目的网络：已于【地址表】之【外部网络】功能中所指定的外部网络地址，或所有外部网络地址。
- 服务名称：指定外部网络服务器提供的服务项目。
- 管制动作：指定内、外部网络进出负载平衡器资料封包的准许与拒绝动作。

- 监控功能：指定内、外部网络进出负载平衡器资料封包的各种监控功能。第一栏为流量监控功能，第二栏为流量统计功能，第三拦为内容管制功能，第四栏为自动排程功能，第五栏为最高流量警示值功能。当该栏出现图标即表示该项监控功能已激活，反之，若未有任何图标，则监控功能未开启。（图标说明如下方表格。）
- 变更：变更内部网络中各项设定值。点选【修改】，可修改内部网络各项参数信息；点选【删除】，可删除该项设定。
- 移动：该项管制条例之编号排列次序。由下拉选单中点选编号，可移动该项管制条例次序。

管制条例图标说明：

图 示	名 称	说　　明
	准许	准许指定的所有内部到所有外部网络 资料封包进出。
	监控	准许指定的内部到外部网络 1 资料封包进出。
	监控	准许指定的内部到外部网络 2 资料封包进出。
	拒绝	拒绝指定的所有内部到所有外部网络资料封包进出。
	流量监控	流量监控功能已开启。
	流量统计	流量统计功能已开启。
	内容管制	已激活内容管制所制订管制功能。
	自动排程	已激活排程表所制订时间范围内自动执行功能。
	流量警示	最高流量警示功能已开启。

备注：

1. 检视系统之流量监控记录  ，点选屏幕左方【监控记录】下之【流量监控】选项，系统使用与操作方式，请翻阅第十章。
2. 检视系统之流量统计纪录  ，点选屏幕左方【流量统计】选项，使用与操作方式，请翻阅第十二章。
3. 检视系统之内容管制  ，点选屏幕左方【内容管制】选项，使用与操作方式，请翻阅第六章。
4. 负载平衡器自动执行时间范围之排程  ，修改排程时间，点选屏幕左方【排程表】选项，使用与操作方式，请翻阅第五章。
5. 检视流量之警示记录  ，点选屏幕左方【警示记录】下之【流量警示】选项，系统使用与操作方式，请翻阅第十一章。

新增内部至外部管制条例

步驟1. 在【内部至外部】窗口中，点选【新增】功能按钮。

步驟2. 在出现的【新增管制条例】窗口中，键入下列相关参数 *（如图8-2）*

图 8-2 新增内部网络至外部网络管制条例

- 来源网络地址：由下拉选单中点选内部网络名称。
  此部分下拉选单所显示的内部网络名称为：【地址表】之【内部网络】所设定的内部网络地址。若要新增选项需至【地址表】之【内部网络】功能窗口中设定，此处无法新增。
- 目的网络地址：由下拉选单中点选外部网络名称。
  此部分下拉选单所显示的外部网络名称为：【地址表】之【外部网络】所设定的外部网络地址。若要新增选项需至【地址表】之【外部网路】功能窗口中设定，此处无法新增。
- 服务名称：由下拉选单中点选服务功能。此部分下拉选单所显示的服务功能项目为：(一)【服务表】中的【基本服务】功能，如：ANY、AOL、AUTH.....等多项服务可供选择；(二) 系统管理员已于【服务表】之【自订服务】或【服务群组】所定义之服务功能项目。

- 管制动作,外部网络端口：由下拉选单中点选指定的内、外部网络 1 / 2 资料封包进出的准许或拒绝。可选择【允许】；或【拒绝】。
- 流量监控：勾选【开启】，开启流量监控记录功能。
- 流量统计：勾选【开启】，开启流量统计功能。
- 内容管制：勾选【开启】，开启内容管制功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。此警示记录将记录于【警示记录】之【流量警示】中。

步驟3. 点选屏幕下方【确定】按钮，新增指定的内部网络，或点选【取消】取消设定。

 *若要变更本单元【内部至外部】表格内管制条例次序，可于表格右方【移动】栏，下拉选单中点选编号，即可移动该项管制条例。*

变更内部至外部管制条例

步骤1. 在【内部至外部】窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【修改】。

步骤2. 在出现的【变更管制条例】窗口中，键入下列相关参数。 *(如图 8-3)*

图 8-3 变更内部网络至外部网络管制条例

- 来源网络地址：由下拉选单中点选内部网络名称。
  此部分下拉选单所显示的内部网络名称为：【地址表】之【内部网络】所设定的内部网络地址。
- 目的网络地址：由下拉选单中点选外部网络名称。
  此部分下拉选单所显示的外部网络名称为：【地址表】之【外部网络】所设定的外部网络地址。
- 服务名称：由下拉选单中点选新服务项目。
- 管制动作,外部网络端口：由下拉选单中点选指定的内、外部网络 1 / 2 资料封包进出的准许或拒绝。可选择【允许】；或【拒绝】。
- 流量监控：勾选【开启】，开启流量监控记录功能。
- 流量统计：勾选【开启】，开启流量统计功能。

- 内容管制：勾选【开启】，开启内容管制功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。此警示记录将记录于【警示记录】之【流量警示】中。

步骤3. 点选屏幕下方【确定】按钮，变更指定的至外部网络管制条例，或点选【取消】取消变更。

若要变更或新增下拉选单的选项，需至各选项的原始设定单元重新设定。

- *来源网络→【地址表】之【内部网络】；*
- *目的网络→【地址表】之【外部网络】；*
- *服务表内的服务名称→【服务表】之【基本服务】、【自订服务】或【服务群组】。*

删除内部至外部管制条例

步骤1. 在【内部至外部】窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【删除】。

步骤2. 在【删除管制条例】确定对话框中，点选【确定】按钮删除设定，或点选【取消】取消删除。 *（如图 8-4）*

图 8-4 删除内部网络至外部网络管制条例

外部至内部管制条例功能设定

在设定外部至内部管制条例时，必须在【虚拟服务器】中，先设定好各项参数。虚拟服务器设定请参考第七章。

来源网络地址是在外部网络区，目的网络地址是在内部网络区。系统管理员在此功能中，制订外部网络至内部网络间所有封包的管制、服务项目的管制规则。

步驟1. 在左方的功能选项中，点选【管制条例】功能，再点选【外部至内部】次功能选项。 *（如图 8-5）*

图 8-5 外部网络至内部网络管制条例功能设定

步驟2. 管制条例表格说明（由外部网络至内部网络）：

- 来源网络地址：已于【地址表】之【外部网络】功能中所指定的外部网络地址，或所有外部网络地址。
- 目的网络地址：已于【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】功能中所指定的 IP 对映网络地址，或虚拟服务器网络地址。
- 服务名称：虚拟服务器（或 IP 对映）提供的服务项目。
- 管制动作：由下拉选单中点选外部网络对虚拟服务器（或 IP 对映）资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。

- 监控功能：指定内、外部网络 1/2 进出负载平衡器资料封包的各种监控功能。第一栏为流量监控功能，第二栏为流量统计功能，第三栏为自动排程功能，第四栏为最高流量警示值功能。当该栏出现图标即表示该项监控功能已激活，反之，若未有任何图标，则监控功能未开启。（图标说明如下方表格。）
- 变更：变更至内部网络中各项管制条例设定值。点选【修改】，可修改各项相关参数值；点选【删除】，可删除该项设定。
- 移动：该项管制条例之编号排列次序。由下拉选单中点选编号，可移动该项管制条例次序。

管制条例图标说明：

图 示	名 称	说　　明
	准许	准许指定的所有外部到内部网络资料 封包进出。
	拒绝	拒绝指定的所有外部到内部 网络资料封包进出。
	流量监控	流量、事件监控功能已开启。
	流量统计	流量统计功能已开启。
	自动排程	已激活排程表所制订时间范围内自动执行功能。
	流量警示	最高流量警示功能已开启。

备注：

1. 检视系统之流量监控记录  ，点选屏幕左方【监控记录】下之【流量监控】选项，系统使用与操作方式，请翻阅第十章。
2. 检视系统之流量统计纪录  ，点选屏幕左方【流量统计】选项，使用与操作方式，请翻阅第十二章。
3. 负载平衡器自动执行时间范围之排程  ，修改排程时间，点选屏幕左方【排程表】选项，使用与操作方式，请翻阅第五章。
4. 检视流量之警示记录  ，点选屏幕左方【警示记录】下之【流量警示】选项，系统使用与操作方式，请翻阅第十一章。

新增外部至内部管制条例

步驟1. 在【外部至内部】窗口中，点选【新增】功能按钮。

步驟2. 在出现的【新增管制条例】窗口中，键入下列相关参数 *(如图8-6)*

图 8-6 新增外部网络至内部网络管制条例

- 来源网络地址：由下拉选单中点选外部网络名称。
  此部分下拉选单所显示的外部网络名称为：已在【地址表】之【外部网络】所设定的外部网络地址。若要新增需至【地址表】之【外部网络】功能窗口中设定，此处无法新增。
- 目的网络地址：由下拉选单中点选内部网络名称。
  此部分下拉选单所显示的内部网络名称为：已在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所设定的 IP 对映网络地址，或虚拟服务器网络地址。若要新增选单内的选项需至【虚拟服务器】功能窗口中设定（新增方法请详见第七章虚拟服务器），此处无法新增。

- 服务名称：由下拉选单中点选服务项目。
  此部分下拉选单所显示的服务项目为：系统管理员已在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所定义之该 IP 对映，或该虚拟服务器的服务项目。若要新增或修改选单内的服务项目选项，需至【虚拟服务器】工作窗口中设定（新增方法请详见第七章 虚拟服务器），此处无法修改。
- 管制动作：由下拉选单中点选外部网络对虚拟服务器（或 IP 对映）资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。
- 流量监控：勾选【开启】，开启流量监控功能。
- 流量统计：勾选【开启】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。此警示记录将记录于【警示记录】之【流量警示】中。

步驟3. 点选【确定】执行新增群组；或点选【取消】取消新增。

 *若要变更本单元【外部至内部】表格内管制条例次序，可于表格右方【次序】栏，下拉选单中点选编号，即可移动该项管制条例。*

变更外部至内部管制条例

步驟1. 在【外部至内部】窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【修改】。

步驟2. 在出现的【变更管制条例】窗口中，键入各项欲变更之参数值 *（如图 8-7）*

图 8-7 变更外部网络至内部网络管制条例

- 来源网络：由下拉选单中点选已在【地址表】之【外部网络】所设定的外部网络地址名称。
- 目的网络：由下拉选单中点选已在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所设定的 IP 对映网络地址，或虚拟服务器网络地址名称。
- 服务名称：由下拉选单中点选已在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所定义之该 IP 对映，或该虚拟服务器的服务项目。
- 管制动作：由下拉选单中点选外部网络对虚拟服务器（或 IP 对映）资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。
- 流量监控：勾选【激活】，开启流量监控功能。

- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。此警示记录将记录于【警示记录】之【流量警示】中。

步驟3. 点选【确定】执行变更管制条例；或点选【取消】取消变更。

若要变更或新增下拉选单的选项，需至各选项的原始设定单元重新设定。

- *来源网络→【地址表】之【外部网络】；*
- *目的网络→【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】的网络地址；*
- *服务项目→【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】提供的服务项目。*

删除外部至内部管制条例

步驟1. 在【外部至内部】窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【删除】。

步驟2. 在【删除管制条例】确定对话框中，点选【确定】按钮，删除设定，或点选【取消】取消删除。 *（如图8-8）*

图 8-8 删除外部网络至内部网络管制条例

外部至非军事区管制条例功能设定

步驟1. 在左方的功能选项中，点选【管制条例】功能，再点选【外部至非军事区】次功能选项。 *（如图 8-9）*

图 8-9 外部网络至非军事区网络管制条例功能设定

管制条例表格说明（由外部网络至非军事区）：

- 编号：所设定之管制条例编号，此处编号由 1 开始。
- 来源网络地址：【地址表】之【外部网络】功能中所指定的外部网络地址，或所有外部网络地址。
- 目的网络地址 :于【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】功能中，所指定的网络地址。
- 服务名称：由下拉选单中点选已在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所定义之该 IP 对映，或该虚拟服务器的服务项目。
- 管制动作：指定外部网络与非军事区进出负载平衡器资料封包的准许与拒绝动作。

- 监控功能：指定外部网络与非军事区进出负载平衡器资料封包的各种监控功能。第一栏为流量监控功能，第二栏为流量统计功能，第三栏为自动排程功能，第四栏为最高流量警示值功能。当该栏出现图标即表示该项监控功能已激活，反之，若未有任何图标，则监控功能未开启。（图标说明如下方表格。）
- 变更：变更外部网络与非军事区中各项管制条例设定值。点选【修改】，可修改各项参数信息；点选【删除】，可删除该项设定。
- 移动：该项管制条例之编号排列次序。由下拉选单中点选编号，可移动该项管制条例次序。

管制条例图标说明：

图 示	名 称	说　　明
	准许	准许指定的所有外部到非军事区网络资料 封包进出。
	拒绝	拒绝指定的所有外部到非军事区 网络资料封包进出。
	流量监控	流量监控功能已开启。
	流量统计	流量统计功能已开启。
	自动排程	已激活排程表所制订时间范围内自动执行功能。
	流量警示	最高流量警示功能已开启。

备注：

1. 检视系统之流量监控记录  ，点选屏幕左方【监控记录】下之【流量监控】选项，系统使用与操作方式，请翻阅第十章。
2. 检视系统之流量统计纪录  ，点选屏幕左方【流量统计】选项，使用与操作方式，请翻阅第十二章。
3. 负载平衡器自动执行时间范围之排程  ，修改排程时间，点选屏幕左方【排程表】选项，使用与操作方式，请翻阅第五章。
4. 检视流量之警示记录  ，点选屏幕左方【警示记录】下之【流量警示】选项，系统使用与操作方式，请翻阅第十一章。

新增外部至非军事区管制条例

步驟1. 在【外部至非军事区】窗口中，点选【新增】功能按钮。

步驟2. 在出现的【新增管制条例】窗口中，键入下列相关参数 *（如图 8-10）*

图 8-10 新增外部网络至非军事区管制条例

- 来源网络地址：由下拉选单中点选内部网络名称。
  此部分下拉选单所显示的内部网络名称为：【地址表】之【外部网络】所设定的外部网络地址，与所有外部网络地址。若要新增选项需至【地址表】之【外部网络】功能窗口中设定，此处无法新增。
- 目的网络地址：由下拉选单中点选非军事区名称。
  此部分下拉选单所显示的外部网络名称为：已于【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】功能中，所设定的网络地址。若要新增选项需至【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】功能功能窗口中设定，此处无法新增。

- 服务名称：由下拉选单中点选服务项目。此部分下拉选单所显示的服务项目为：系统管理员在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所定义之该 IP 对映，或该虚拟服务器指定的服务项目。若要新增或修改选单内的服务项目选项，需至【虚拟服务器】工作窗口中设定（新增方法请详见第七章虚拟服务器），此处无法修改。
- 管制动作：由下拉选单中点选外部网络与非军事区间资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。
- 流量监控：勾选【激活】，开启流量监控功能。
- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。

步驟3. 点选屏幕下方【确定】按钮，新增指定外部至非军事区管制条例，或点选【取消】取消新增。

若要变更本单元【外部网络至非军事区】表格内管制条例次序，可于表格右方【移动】栏，下拉选单中点选编号，即可移动该项管制条例。

变更外部至非军事区管制条例

步驟1. 在【外部至非军事区】工作窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【修改】。

在出现的【变更管制条例】窗口中，键入欲变更的相关参数 *（如图 8-11）*

图 8-11 变更外部网络至非军事区管制条例

- 来源网络地址：由下拉选单中点选外部网络名称。
  此部分下拉选单所显示的外部网络名称为：【地址表】之【外部网络】所设定的外部网络地址。
- 目的网络地址：由下拉选单中点选非军事区名称。
  此部分下拉选单所显示的外部网络名称为：已于【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】功能中，所设定的网络地址。
- 服务名称：由下拉选单中点选新服务项目。此部分下拉选单所显示的服务项目为：系统管理员在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所定义之该 IP 对映，或该虚拟服务器指定的服务项目。

- 管制动作：由下拉选单中点选外部网络与非军事区间网络资料封包进出的准许或拒绝。
- 流量监控：勾选【激活】，开启流量监控功能。
- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。

步骤2. 点选屏幕下方【确定】按钮，变更指定外部至非军事区管制条例，或点选【取消】取消变更。

若要变更或新增下拉选单的选项，需至各选项的原始设定单元重新设定。

- *来源网络→【地址表】之【外部网络】；*
- *目的网络→【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】所对映之 IP；*
- *服务项目→【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】提供的服务项目。*

移除外部至非军事区管制条例

步驟1. 在【外部至非军事区】工作窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【删除】。

步驟2. 在【移除管制条例】确定对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。 *（如图 8-12）*

图 8-12 移除外部网络至非军事区管制条例

内部至非军事区管制条例

步驟1. 在左方的功能选项中，点选【管制条例】功能，再点选【内部至非军事区】次功能选项。 *（如图 8-13）*

图 8-13 内部网络至非军事区管制条例功能设定

步驟2. 管制条例表格说明（由内部网络至非军事区）：

- 编号：所设定之管制条例编号，此处编号由 1 开始。
- 来源网络：【地址表】之【内部网络】功能中所指定的内部网络地址，或所有内部网络地址。
- 目的网络：【地址表】之【非军事区】功能中所指定的非军事区地址，或所有非军事区地址。
- 服务名称：指定非军事区服务器提供的服务项目。
- 管制动作：指定内部网络与非军事区进出负载平衡器资料封包的准许与拒绝动作。

- 监控功能：指定内部网络与非军事区进出负载平衡器资料封包的各种监控功能。第一栏为流量监控功能，第二栏为流量统计功能，第三栏为自动排程功能，第四栏为最高流量警示值功能。当该栏出现图标即表示该项监控功能已激活，反之，若未有任何图标，则监控功能未开启。（图标说明如下方表格。）
- 变更：变更内部网络至非军事区中各项管制条例设定值。点选【修改】，可修改各项参数；点选【删除】，可删除该项设定。
- 移动：该项管制条例之编号排列次序。由下拉选单中点选编号，可移动该项管制条例次序。

管制条例图标说明：

图 示	名 称	说　　明
	准许	准许指定的所有内部到非军事区网络资料 封包进出。
	拒绝	拒绝指定的所有内部到非军事区 网络资料封包进出。
	流量监控	流量监控功能已开启。
	流量统计	流量统计功能已开启。
	自动排程	已激活排程表所制订时间范围内自动执行功能。
	流量警示	最高流量警示功能已开启。

备注：

1. 检视系统之流量监控记录  ，点选屏幕左方【监控记录】下之【流量监控】选项，系统使用与操作方式，请翻阅第十章。
2. 检视系统之流量统计纪录  ，点选屏幕左方【流量统计】选项，使用与操作方式，请翻阅第十二章。
3. 负载平衡器自动执行时间范围之排程  ，修改排程时间，点选屏幕左方【排程表】选项，使用与操作方式，请翻阅第五章。
4. 检视流量之警示记录  ，点选屏幕左方【警示记录】下之【流量警示】选项，系统使用与操作方式，请翻阅第十一章。

新增内部至非军事区管制条例

步骤1. 在【内部至非军事区】窗口中，点选【新增】功能按钮。

步骤2. 在出现的【新增管制条例】窗口中，键入下列相关参数 *（如图8-14）*

图 8-14 新增内部网络至非军事区管制条例

- 来源网络地址：由下拉选单中点选内部网络名称。
  此部分下拉选单所显示的内部网络名称为：【地址表】之【内部网络】所设定的内部网络地址，与所有内部网络地址。若要新增选项需至【地址表】之【内部网络】功能窗口中设定，此处无法新增。
- 目的网络地址：由下拉选单中点选非军事区名称。
  此部分下拉选单所显示的内部网络名称为：【地址表】之【非军事区】功能中所指定的非军事区地址，或所有非军事区地址。
  若要新增选项【地址表】之【非军事区】功能窗口中设定，此处无法新增。

- 服务名称：由下拉选单中点选服务项目。此部分下拉选单所显示的服务项目为：（一）【服务表】中的【基本服务】功能，如：ANY、AOL、AUTH…..等多项服务可供选择；（二）系统管理员已于【服务表】之【自订服务】或【服务群组】所定义之服务功能项目。若要新增或修改选单内的服务项目选项，需至【服务表】工作窗口中设定，此处无法修改。
- 管制动作：由下拉选单中点选指定的内部网络与非军事区间资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。
- 流量监控：勾选【激活】，开启流量监控功能。
- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。

步驟3. 点选【确定】执行新增指定的内部至非军事区网络管制条例；或点选【取消】取消新增。

若要变更本单元【内部至非军事区】表格内管制条例次序，可于表格右方【次序】栏，下拉选单中点选编号，即可移动该项管制条例。

变更内部至非军事区管制条例

步驟1. 在【内部至非军事区】工作窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【修改】。

步驟2. 在出现的【变更管制条例】窗口中，键入欲变更的相关参数 *（如图8-15）*

图 8-15 变更内部网络至非军事区管制条例

- 来源网络地址：由下拉选单中点选内部网络名称。
  此部分下拉选单所显示的内部网络名称为：【地址表】之【内部网络】所设定的内部网络地址。
- 目的网络地址：由下拉选单中点选非军事区名称。
  此部分下拉选单所显示的非军事区网络名称为：已于【地址表】之【非军事区】功能中所指定的非军事区地址，或所有非军事区地址。
- 服务名称：由下拉选单中点选新服务项目。此部分下拉选单所显示的服务项目为：(一)【服务表】中的【基本服务】功能，如：ANY、AOL、AUTH.....等多项服务可供选择；(二) 系统管理员已于【服务表】之【自订服务】或【服务群组】所定义之服务功能项目。

- 管制动作：由下拉选单中点选指定的内部网络与非军事区间网络资料封包进出的准许或拒绝。
- 流量监控：勾选【激活】，开启流量监控功能。
- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。

步骤3. 点选屏幕下方【确定】按钮，变更指定的内部至非军事区网络管制条例，或点选【取消】取消变更。

若要变更或新增下拉选单的选项，需至各选项的原始设定单元重新设定。

- *来源网络→【地址表】之【内部网络】；*
- *目的网络→【地址表】之【非军事区网络】；*
- *服务项目→【服务表】之【基本服务】、【自订服务】或【服务群组】。*

移除内部至非军事区管制条例

步驟1. 在【内部至非军事区】工作窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【删除】。

步驟2. 在【移除管制条例】确定对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。 *（如图 8-16）*

图 8-16 移除内部网络至非军事区管制条例

非军事区至外部管制条例

步驟1. 在左方的功能选项中，点选【管制条例】功能，再点选【非军事区至外部】次功能选项。 *（如图 8-17）*

图 8-17 非军事区至外部网络管制动作设定功能

步驟2. 管制条例表格说明（由非军事区至外部网络）：

- 编号：所设定之管制条例编号，此处编号由 1 开始。
- 来源网络：已于【地址表】之【非军事区】功能中所指定的非军事区地址。
- 目的网络：可选择网络区为，已于【地址表】之【外部网络】所指定的外部网络地址。
- 服务名称：指定外部网络服务器提供的服务项目。
- 管制动作：指定非军事区和外部网络进出负载平衡器资料封包的准许与拒绝动作。
- 监控功能：指定非军事区、外部网络间进出负载平衡器资料封包的各种监控功能。第一栏为流量监控功能，第二栏为流量统计功能，第三拦为内容管制功能，第四栏为自动排程功能，第五栏为最高流量警示值功能。当该栏出现图标即表示该项监控功能已激活，反之，若未有任何图标，则监控功能未开启。（图标说明如下方表格。）

- 变更：变更非军事区至外部网络中各项管制条例设定值。点选【修改】，可修改各项参数；点选【删除】，可删除该项设定。
- 移动：该项管制条例之编号排列次序。由下拉选单中点选编号，可移动该项管制条例次序。

管制条例图标说明：

图 示	名 称	说　　明
	准许	准许指定的所有非军事区到外部网络 资料封包进出。
	监控	准许指定的非军事区到外部网络 1 资料封包进出。
	监控	准许指定的非军事区到外部网络 2 资料封包进出。
	拒绝	拒绝指定的所有非军事区、外部网络 资料封包进出。
	流量监控	流量监控功能已开启。
	流量统计	流量统计功能已开启。
	内容管制	已激活内容管制所制订管制功能。
	自动排程	已激活排程表所制订时间范围内自动执行功能。
	流量警示	最高流量警示功能已开启。

备注：

1. 检视系统之流量监控记录  ，点选屏幕左方【监控记录】下之【流量监控】选项，系统使用与操作方式，请翻阅第十章。
2. 检视系统之流量统计纪录  ，点选屏幕左方【流量统计】选项，使用与操作方式，请翻阅第十二章。
3. 检视系统之内容管制  ，点选屏幕左方【内容管制】选项，使用与操作方式，请翻阅第六章。
4. 负载平衡器自动执行时间范围之排程  ，修改排程时间，点选屏幕左方【排程表】选项，使用与操作方式，请翻阅第五章。
5. 检视流量之警示记录  ，点选屏幕左方【警示记录】下之【流量警示】选项，系统使用与操作方式，请翻阅第十一章。

新增非军事区至外部管制条例

步驟1. 在左方的功能选项中，点选【管制条例】功能，再点选【非军事区至外部】次功能选项。

步驟2. 点选【新增】功能按钮。

步驟3. 在新窗口中，键入新管制条例各项参数值。 *（如图8-18）*

图 8-18 新增非军事区至外部网络管制条例

- 来源网络地址：由下拉选单中点选非军事区名称。
  此部分下拉选单所显示的非军事区名称为：已在【地址表】之【非军事区】所设定的非军事区地址，或所有非军事区地址。若要新增需至【地址表】之【非军事区】功能窗口中设定，此处无法新增。

- 目的网络地址：由下拉选单中点选外部网络名称。
  此部分下拉选单所显示的外部网络名称为：【地址表】之【外部网络】功能中所指定的外部网络地址，或所有外部网络地址。若要新增需至【地址表】之【外部网络】功能窗口中设定，此处无法新增。

- 服务名称：由下拉选单中点选服务项目。
  此部分下拉选单所显示的服务项目为：(一)【服务表】中的【基本服务】功能，如：ANY、AOL、AUTH.....等多项服务可供选择；(二)系统管理员已于【服务表】之【自订服务】或【服务群组】所定义之服务功能项目。若要新增或修改选单内的服务项目选项，需至【服务表】工作窗口中设定，此处无法修改。
- 管制动作：由下拉选单中点选指定的非军事区与外部网络间资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。
- 流量监控：勾选【开启】，开启流量监控记录功能。
- 流量统计：勾选【开启】，开启流量统计功能。
- 内容管制：勾选【开启】，开启内容管制功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。此警示记录将记录于【警示记录】之【流量警示】中。

步驟4. 点选屏幕下方【确定】按钮，新增指定的非军事区至外部网络管制条例，或 点选【取消】取消新增。

若要变更本单元【非军事区至外部网络】表格内管制条例次序，可于表格右方【移动】栏，下拉选单中点选编号，即可移动该项管制条例。

变更非军事区至外部管制条例

步驟1. 在【非军事区至外部】的表格中，找到欲变更设定的网络名称，对映至右方【变更】栏，点选【修改】。

步驟2. 在【变更管制条例】窗口中，键入各项欲变更的参数。 *（如图8-19）*

图 8-19 变更非军事区至外部网络管制条例

- 来源网络地址：由下拉选单中点选非军事区名称。
  此部分下拉选单所显示的非军事区名称为：已在【地址表】之【非军事区】所设定的非军事区地址，或所有非军事区地址。
- 目的网络地址：由下拉选单中点选外部网络名称。
  此部分下拉选单所显示的外部网络名称为：【地址表】之【外部网络】功能中所指定的外部网络地址，或所有外部网络地址。
- 服务名称：由下拉选单中点选服务项目。
  此部分下拉选单所显示的服务项目为：(一)【服务表】中的【基本服务】功能，如：ANY、AOL、AUTH.....等多项服务可供选择；(二)系统管理员已于【服务表】之【自订服务】或【服务群组】所定义之服务功能项目。

- 管制动作：由下拉选单中点选指定的非军事区与外部网络间资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。
- 流量监控：勾选【开启】，开启流量监控记录功能。
- 流量统计：勾选【开启】，开启流量统计功能。
- 内容管制：勾选【开启】，开启内容管制功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。此警示记录将记录于【警示记录】之【流量警示】中。

步骤3. 点选屏幕下方【确定】按钮，变更指定的非军事区至外部网络管制条例，或 点选【取消】取消变更。

若要变更或新增下拉选单的选项，需至各选项的原始设定单元重新设定。

- *来源网络→【地址表】之【非军事区网络】；*
- *目的网络→【地址表】之【外部网络】；*
- *服务项目→【服务表】之【基本服务】、【自订服务】或【服务群组】。*

移除非军事区至外部管制条例

步驟1. 在【非军事区至外部】工作窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【删除】。

步驟2. 在【移除管制条例】确定对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。 *（如图 8-20）*

图 8-20 移除非军事区至外部网络管制条例

非军事区至内部管制条例

步驟1. 在左方的功能选项中，点选【管制条例】功能，再点选【非军事区至内部】次功能选项。 *（如图 8-21）*

图 8-21 非军事区至内部网络管制动作设定功能

步驟2. 管制条例表格说明（由非军事区至内部）：

- 编号：所设定之管制条例编号，此处编号由 1 开始。
- 来源网络：已于【地址表】之【非军事区】功能中所指定的非军事区地址。
- 目的网络：可选择网络区为，已于【地址表】之【内部网络】所指定的内部网络地址。
- 服务名称：指定内部网络服务器提供的服务项目。
- 管制动作：指定非军事区、内部网络进出负载平衡器资料封包的准许与拒绝动作。

- 监控功能：指定非军事区、内部网络间进出负载平衡器资料封包的各种监控功能。第一栏为流量监控功能，第二栏为流量统计功能，第三栏为自动排程功能，第四栏为最高流量警示值功能。当该栏出现图标即表示该项监控功能已激活，反之，若未有任何图标，则监控功能未开启。（图标说明如下方表格。）
- 变更：变更非军事区至内部网络中各项管制条例设定值。点选【修改】，可修改各项参数；点选【删除】，可删除该项设定。
- 移动：该项管制条例之编号排列次序。由下拉选单中点选编号，可移动该项管制条例次序。

管制条例图标说明：

图 示	名 称	说　　明
	准许	准许指定的所有非军事区到内部网络 资料封包进出。
	拒绝	拒绝指定的所有非军事区到内部网络 资料封包进出。
	流量监控	流量监控功能已开启。
	流量统计	流量统计功能已开启。
	自动排程	已激活排程表所制订时间范围内自动执行功能。
	流量警示	最高流量警示功能已开启。

备注：

4. 检视系统之流量监控记录  ，点选屏幕左方【监控记录】下之【流量监控】选项，系统使用与操作方式，请翻阅第十章。
5. 检视系统之流量统计纪录  ，点选屏幕左方【流量统计】选项，使用与操作方式，请翻阅第十二章。
6. 负载平衡器自动执行时间范围之排程  ，修改排程时间，点选屏幕左方【排程表】选项，使用与操作方式，请翻阅第五章。
5. 检视流量之警示记录  ，点选屏幕左方【警示记录】下之【流量警示】选项，系统使用与操作方式，请翻阅第十一章。

新增非军事区至内部管制条例

步驟1. 在左方的功能选项中，点选【管制条例】功能，再点选【非军事区至内部】次功能选项。

步驟2. 点选【新增】功能按钮。

步驟3. 在新窗口中，键入新管制条例各项参数值。 *（如图8-22）*

图 8-22 新增非军事区至内部网络管制条例

- 来源网络地址：由下拉选单中点选非军事区名称。
  此部分下拉选单所显示的非军事区名称为：已在【地址表】之【非军事区】所设定的非军事区地址，或所有非军事区地址。若要新增需至【地址表】之【非军事区】功能窗口中设定，此处无法新增。
- 目的网络地址：由下拉选单中点选内部网络名称。
  此部分下拉选单所显示的内部网络名称为：【地址表】之【内部网络】功能中所指定的内部网络地址，或所有内部网络地址。若要新增需至【地址表】之【内部网络】功能窗口中设定，此处无法新增。

- 服务名称：由下拉选单中点选服务项目。
  此部分下拉选单所显示的服务项目为：(一)【服务表】中的【基本服务】功能，如：ANY、AOL、AUTH.....等多项服务可供选择；(二)系统管理员已于【服务表】之【自订服务】或【服务群组】所定义之服务功能项目。若要新增或修改选单内的服务项目选项，需至【服务表】工作窗口中设定，此处无法修改。
- 管制动作：由下拉选单中点选指定的非军事区与内部网络间资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。
- 流量监控：勾选【激活】，开启流量监控功能。
- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。

步驟4. 点选屏幕下方【确定】按钮，新增指定的非军事区至内部网络管制条例，或 点选【取消】取消新增。

若要变更本单元【非军事区至内部网络】表格内管制条例次序，可于表格右方【移动】栏，下拉选单中点选编号，即可移动该项管制条例。

变更非军事区至内部管制条例

步骤1. 在【非军事区至内部】的表格中，找到欲变更设定的网络名称，对映至右方【变更】栏，点选【修改】。

步骤2. 在【变更管制条例】窗口中，键入各项欲变更的参数。 *（如图8-23）*

图 8-23 变更非军事区至内部网络管制条例

- 来源网络地址：由下拉选单中点选非军事区名称。
  此部分下拉选单所显示的非军事区名称为：已在【地址表】之【非军事区】所设定的非军事区地址，或所有非军事区地址。
- 目的网络地址：由下拉选单中点选内部网络名称。
  此部分下拉选单所显示的内部网络名称为：【地址表】之【内部网络】功能中所指定的内部网络地址，或所有内部网络地址。
- 服务名称：由下拉选单中点选服务项目。
  此部分下拉选单所显示的服务项目为：(一)【服务表】中的【基本服务】功能，如：ANY、AOL、AUTH.....等多项服务可供选择；(二)系统管理员已于【服务表】之【自订服务】或【服务群组】所定义之服务功能项目。

- 管制动作：由下拉选单中点选指定的非军事区与内部网络间资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。
- 流量监控：勾选【激活】，开启流量监控功能。
- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。

步驟3. 点选屏幕下方【确定】按钮，变更指定的非军事区至内部网络管制条例，或 点选【取消】取消变更。

若要变更或新增下拉选单的选项，需至各选项的原始设定单元重新设定。

- *来源网络→【地址表】之【非军事区网络】；*
- *目的网络→【地址表】之【内部网络】；*
- *服务项目→【服务表】之【基本服务】、【自订服务】或【服务群组】。*

移除非军事区至内部管制条例

步骤1. 在【非军事区至内部】工作窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【删除】。

步骤2. 在【移除管制条例】确定对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。 *（如图8-24）*

图 8-24 移除非军事区至内部网络管制条例

第九章

VPN

本负载平衡器采 VPN 方式建立安全与私密的网络通讯服务，结合远程用户认证辨识系统，以整合企业的各个远地网络与全球外勤人员远地个人计算机，提供公司企业与远程使用者一个安全便利的网络加密方式， 让企业在网际网络上传递资料时，得到最佳的效能及保密效果，更节省管理者管理太多钥匙的麻烦。

【IPSec 自动加密】:系统管理员可于此单元以加密功能建立联机两端以固定标准方式交换网络加密钥匙码，并设定 IPSec Lifetime（加密钥匙更新周期），亦可以 Perfect Forward Secrecy（进阶加密）功能，激活负载平衡器系统自动随机选取更新无法被判读入侵的加密钥匙码。

【PPTP 服务器】:系统管理员可于此单元建立 VPN-PPTP 服务器的相关功能设定。
【PPTP 客户端】:系统管理员可于此单元建立 VPN-PPTP 客户端的相关功能设定。

如何运用网络验证

建立虚拟私有网络验证 Virtual Private Network (VPN)，无须至【管制条例】设定，只需依照下列步骤，设定 VPN 名称、来源端网络地址、目的端网络地址与认证与加密模式，即可为联机两端建立安全保密的网络通讯。

VPN 专有名词解释

RSA 为非对称性密码系统，使用者拥有两把金钥，一个为秘密金钥，使用者须秘密收藏，为联机解密时用，另一个为公开金钥，将任何欲传送讯息者皆可自认证中心取得，并使用此金钥将讯息加密传送给接收者。

Preshared Key 当 VPN 双方进行联机时用来进行 IPSec 验证用的专用的 Key.

ISAKMP 「IP Security Association Key Management Protocol」(ISAKMP) 就是提供一种方法供两台计算机建立安全性关联 (SA)。SA(Security Association) 对两台计算机之间进行联机编码，指定使用哪些算法和什么样的金钥长度或实际加密金钥。事实上 SA 不止一个联机方式：从两台计算机 ISAKMP SA 作为起点，必须指定使用何种加密算法 (DES、triple DES、40 位 DES 或根本不用)、使用何种认证。

Aggressive mode 在 VPN 第一阶段的 IKE 开始联机时，会提供两种模式选择,其中的一种模式就是 Aggressive mode 会对资料交换的双方先进行认证，Aggressive mode 会提供三个讯息在双方之间进行传递来达到认证的需求，确保与自己交流资料是对方本人，而不是伪造的。

AH (Authentication Header) 提供 VPN 联机时的认证及选择性的认证检测。

ESP (Encapsulated Security Payload) 提供 VPN 联机时的认证及认证检测。并对传送中的资料提供了机密和保护。

DES 资料加密标准（Data Encryption Standard）是一种 NIST 标准安全加密金钥方法，使用的加密金钥为 56 位。
3DES 提供比 DES 更加安全的三重资料加密标准(Triple Data Encryption Standard,3DES) 安全加密金钥方法，使用的加密金钥为 168 位。

AES 为高阶加密模式其标准比 DES 的加密标准更加严谨，DES 加密金钥长度为 56 位，AES 加密金钥长度则高达 128 位、192 位、以及 256 位。

NULL 算法是一种快速又便利的联机模式来取代确保其机密性或负责身份验证而不进行加密的动作。NULL 算法不提供机密性也没有提供其它任何安全服务，仅仅是一条快速方便去替换在使用 ESP 加密时的选项。

SHA1 安全杂凑算法 (Secure Hash Algorithm，SHA) 是用于产生讯息摘要或杂凑的算法。原有的 SHA 算法已被改良式的 SHA1 算法取代。 可以计算出 160 位的演算。

MD5 杂凑算法一种单向字符串杂凑演算，其演算方式是将你给予任何长度字符串，使用 MD5 杂凑算法，可以计算出一个长度为 128 位的演算。

GRE 通用路由协议封装。GRE 只提供了资料包的封装，它没有防止网络侦听和攻击的加密功能。所以在实际环境中它常和 IPsec 一起使用，由 IPsec 为用户资料的加密，给用户提供更好的安全服务。

【IPSec 自动加密】窗口表格内图标与名词名称定义：

- 名称：定义虚拟私有网络（VPN）验证信道名称。此名称必须是唯一且不可重复。
- 网关 IP 地址：目的端网络接口地址。
- 目的端子网络：目的端子网络地址。
- 算法：显示目前 VPN 联机后的资料加密模式。
- 状态：连接或断线。
- 变更：变更服务表中各项设定值。点选【修改】，可修改自动加密之各项参数；点选【删除】，可删除该项设定；点选【联机】，激活与目的端联机；点选【断线】，关闭与目的端加密联机功能。 *（如图 9-1）*

图 9-1　IPSec 自动加密窗口表格

我们在此范例设定中，总共架设了 4 种 VPN 环境。

范例 1	使用两台负载平衡器机器 VPN 上设定联机方法。
范例 2	使用一台负载平衡器机器之 VPN 与 Windows 2000 VPN IPSec 的设定 VPN 联机方法。
范例 3	使用两台负载平衡器机器 VPN 上设定联机方法。 (联机使用 Aggressive mode 算法 3DES 加密.MD5 认证) (数据使用 IPSec 演算 3DES 加密.MD5 认证)
范例 4	使用两台负载平衡器机器 VPN 上设定联机方法。 (使用 ISAKMP 算法 3DES 加密.MD5 认证) (数据使用 IPSec 演算 3DES 加密.MD5 认证) (使用 GRE 封包封装)

范例 1：使用两台负载平衡器机器 VPN 上设定联机方法。

先前作业

甲公司　External IP 为 61.11.11.11
　　Internal IP　为 192.168.10.X
乙公司　External IP 为 211.22.22.22
　　Internal IP　为 192.168.20.X

本范例以两台负载平衡器机器作为平台操作。假设甲公司 192.168.10.100 要向乙公司 192.168.20.100 做【虚拟私有网络】联机并下载其分享档案。

甲公司 192.168.10.100 的预设网关为自己网域的 192.168.10.1，以下设定步骤：

步驟1.　进入甲公司负载平衡器预设地址 192.168.10.1，在左方的功能选项中，点选【**VPN**】功能，再点选【**IPSec 自动加密**】次功能选项。 *（如图9-2）* 并点选【**新增**】功能。

图 9-2　IPSec 自动加密窗口

步驟2. 于【**VPN 自动金钥管理信道**】窗体中，填写所使用的 VPN 联机名称 VPN_A，并点选来源地址为【内部网络】。并填入甲公司内部网络地址 192.168.10.0 及屏蔽 255.255.255.0。 ***（如图 9-3）***

图 9-3 VPN 自动金钥管理信道设定窗体

步驟3. 于【到目的地址】窗体中，选择远程网关-固定 IP，填写所要联机乙公司的远程 IP 地址，并填入乙公司内部网络地址 192.168.20.0 及屏蔽 255.255.255.0。 ***（如图 9-4）***

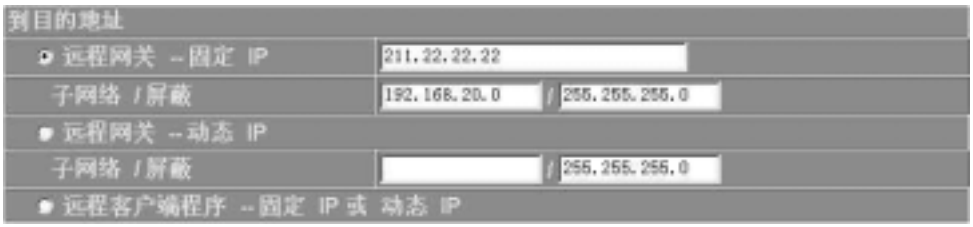


图 9-4 IPSec 到目的地址设定窗体

步驟4. 于【认证方法】窗体中，选择 Preshare，并填入联机时的加密金钥 (加密金钥最高可输入 100 位)。 ***（如图 9-5）***

图 9-5 IPSec 认证方法设定窗体

步驟5. 于【加密或认证】窗体中， 选择 ISAKMP 算法(请参阅名词解说)，双方开始进行联机沟通时，选择建立联机时所需加密的算法
请选择加密演算(3DES/DES/AES) 我们选择 3DES 及选择认证的算法(MD5/SHA1)我们选择 MD5 认证方式,另外需选择群组.(GROUP 1,2,5)双方需选择同一群组 我们选择 GROUP 1 来进行联机。 *(如图 9-6)*

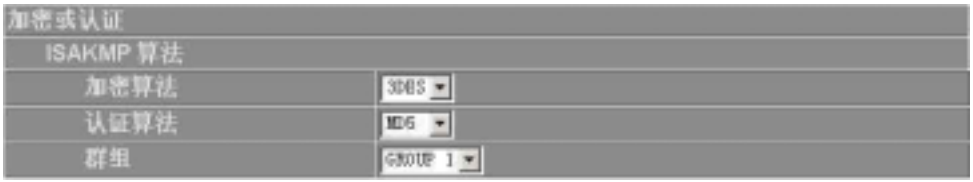


图 9-6 IPSec 加密或认证设定窗体

步驟6. 于【IPSec 算法】窗体中勾选资料加密+认证，可以选择资料加秘+认证或是仅选择认证方式来沟通:
加密算法可选择(3DES/DES/AES/NULL)我们选择 3DES 加密演算，认证算法可选择(MD5/SHA1)我们选择 MD5 认证演算方式，来确保数据传输时所使用的加密认证方式。 *(如图 9-7)*

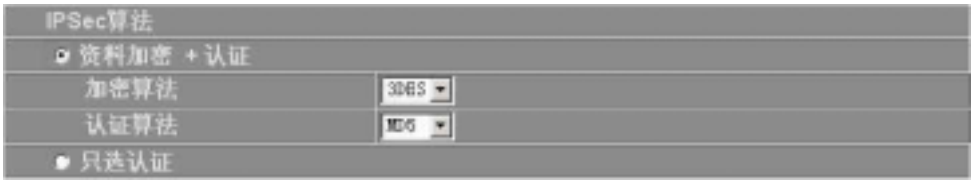


图 9-7 IPSec 算法设定窗体

步驟7. 勾选进阶加密，并填写加密金钥更新周期填入 28800 秒，并可输入乙公司可以保持联机的 IP 地址 192.168.20.100，使 VPN 能够持续联机保持不断线。 *(如图 9-8)*

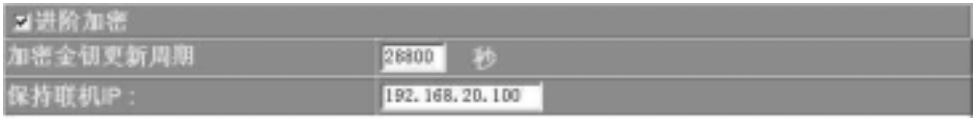


图 9-8 IPSec 进阶加密设定窗体

步驟8. 排程选择甲公司 VPN 可联机时间。 *（如图9-9）*

图 9-9 IPSec 自动排程设定窗体

步驟9. 点选【**确定**】，完成甲公司设定。 *（如图9-10）*

图 9-10 甲公司 IPSec VPN 完成设定

乙公司 192.168.20.100 的预设网关为自己网域的 192.168.20.1，以下设定步骤：

步驟1. 进入乙公司负载平衡器预设地址 192.168.20.1，在左方的功能选项中，点选【**VPN**】功能，再点选【**IPSec 自动加密**】次功能选项。并点选【**新增**】功能。 ***（如图 9-11）***

图 9-11 IPSec 自动加密窗口

步驟2. 于【**VPN 自动金钥管理信道**】窗体中，填写所使用的 VPN 联机名称 VPN_B，并点选来源地址为【内部网络】。并填入乙公司内部网络地址 192.168.20.0 及屏蔽 255.255.255.0。 ***（如图 9-12）***

图 9-12 VPN 自动金钥管理信道设定窗体

步驟3. 于【到目的地址】窗体中，选择远程网关-固定 IP，填写所要联机甲公司的远程 IP 地址，并填入甲公司内部网络地址 192.168.10.0 及屏蔽 255.255.255.0。 *（如图9-13）*

图 9-13 IPSec 到目的地址设定窗体

步驟4. 于【认证方法】窗体中，选择 Preshare，并填入联机时的加密金钥(加密金钥最高可输入 100 字符)。 *（如图9-14）*

图 9-14 IPSec 认证方法设定窗体

步驟5. 于【加密或认证】窗体中， 选择 ISAKMP 算法(请参阅名词解说)，双方开始进行联机沟通时,选择建立联机时所需加密的算法 请选择 3DES 加密演算，及选择认证的算法 MD5 认证方式,另外需选择群组.双方需选择同一群组 GROUP 1 进行联机。 *（如图9-15）*

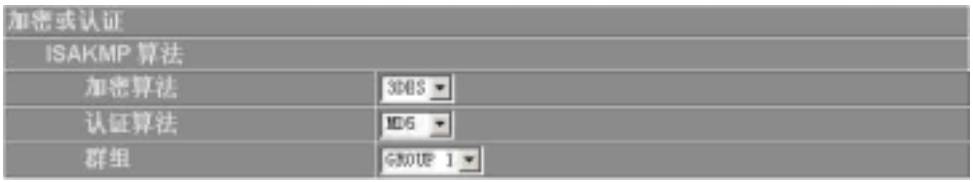


图 9-15 IPSec 加密或认证设定窗体

步驟6. 于【IPSec 算法】窗体中勾选资料加密+认证，可以选择资料加秘+认证或是仅选择认证方式来沟通:
加秘算法可选择(3DES/DES/AES/NULL)我们选择 3DES 加密演算，
认证算法可选择(MD5/SHA1)我们选择 MD5 认证演算方式，来确保数据传输时所使用的加密认证方式。 *（如图9-16）*

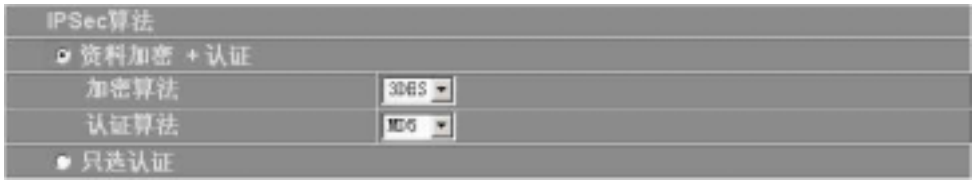


图 9-16 IPSec 算法设定窗体

步驟7. 勾选进阶加密，并填写加密金钥更新周期填入 28800 秒，并可输入甲公司可以保持联机的 IP 地址 192.168.10.100，使 VPN 能够持续联机保持不断线。 *（如图9-17）*

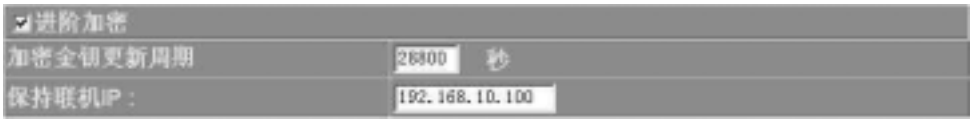


图 9-17 IPSec 进阶加密设定窗体

步驟8. 排程选择甲公司 VPN 可联机时间。 *（如图9-18）*

图 9-18 IPSec 自动排程设定窗体

步驟9. 点选**【确定】**，完成乙公司设定。 *（如图9-19）*

图 9-19 乙公司 IPSec VPN 完成设定

范例 2：使用一台负载平衡器机器之 VPN 与 Windows 2000 VPN IPSec 的设定 VPN 联机方法。

先前作业

甲公司　External IP 为 61.11.11.11
　　Internal IP　为 192.168.10.X
乙公司　External IP 为 211.22.22.22

本范例以一台负载平衡器机器及 Windows 2000 VPN-IPsec 作为平台操作。假设甲公司 192.168.10.100 要向乙公司 211.22.22.22 做【虚拟私有网络】联机并下载其分享档案。

甲公司 192.168.10.100 的预设网关为自己网域的 192.168.10.1，以下设定步骤：

步驟1.　进入甲公司负载平衡器预设地址 192.168.10.1，在左方的功能选项中，点选【**VPN**】功能，再点选【**IPSec 自动加密**】次功能选项。
并点选【**新增**】功能。 ***（如图 9-20）***

图 9-20　IPSec 自动加密窗口

于【**VPN 自动金钥管理信道**】窗体中，填写所使用的 VPN 联机名称 VPN_A，并点选来源地址为【内部网络】。并填入甲公司内部网络地址 192.168.10.0 及屏蔽 255.255.255.0。 ***（如图 9-21）***

图 9-21　VPN 自动金钥管理信道设定窗体

步驟3.　于【到目的地址】窗体中，选择远程客户端程序 – 固定 IP 或动态 IP。 ***（如图 9-22）***

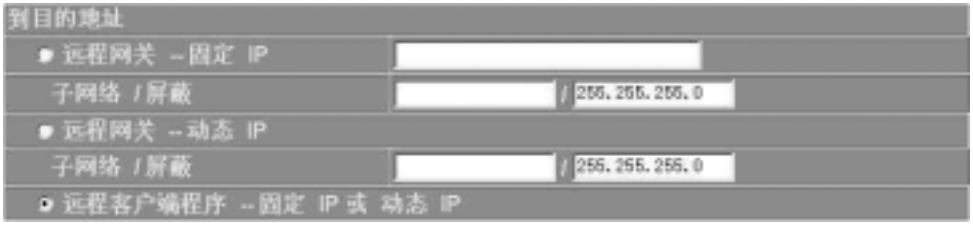


图 9-22　IPSec 到目的地址设定窗体

步驟4.　于【认证方法】窗体中，选择 Preshare，并填入联机时的加密金钥 (加密金钥最高可输入 100 位)。 ***（如图 9-23）***

图 9-23　IPSec 认证方法设定窗体

步驟5. 于【加密或认证】窗体中， 选择 ISAKMP 算法(请参阅名词解说)，双方开始进行联机沟通时，选择建立联机时所需加密的算法
请选择加密演算(3DES/DES/AES) 我们选择 3DES 及选择认证的算法(MD5/SHA1)我们选择 MD5 认证方式,另外需选择群组.(GROUP 1,2,5)双方需选择同一群组 我们选择 GROUP 2 来进行联机。 ***(如图 9-24)***

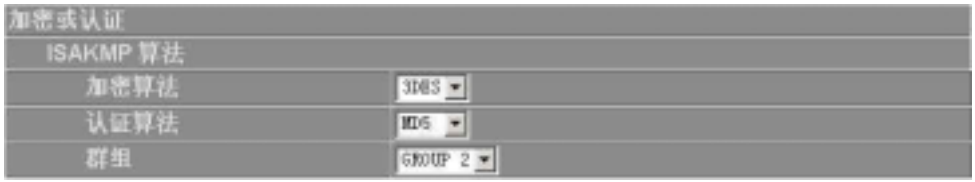


图 9-24 IPSec 加密或认证设定窗体

步驟6. 于【IPSec 算法】窗体中勾选资料加密+认证，可以选择资料加秘+认证或是仅选择认证方式来沟通:
加秘算法可选择(3DES/DES/AES/NULL)我们选择 3DES 加密演算，认证算法可选择(MD5/SHA1)我们选择 MD5 认证演算方式，来确保数据传输时所使用的加密认证方式。 ***(如图 9-25)***

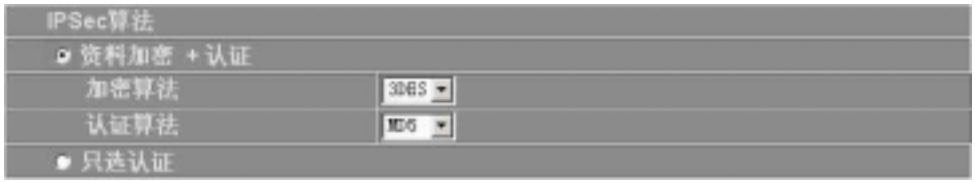


图 9-25 IPSec 算法设定窗体

步驟7. 勾选进阶加密，并填写加密金钥更新周期填入 28800 秒，并可输入乙公司可以保持联机的 IP 地址 211.22.22.22,使 VPN 能够持续联机保持不断线。 ***(如图 9-26)***

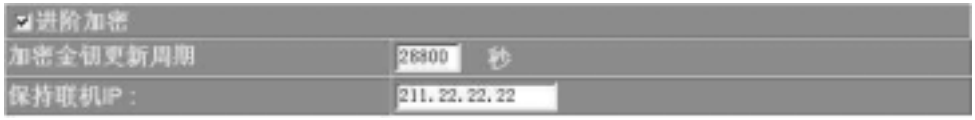


图 9-26 IPSec 进阶加密设定窗体

步驟8. 排程选择甲公司 VPN 可联机时间。 ***(如图 9-27)***

图 9-27 IPSec 自动排程设定窗体

步驟9. 点选【**确定**】，完成甲公司设定。 ***（如图9-28）***

图 9-28 甲公司 IPSec VPN 完成设定

乙公司的预设网关为自己的实体 IP（211.22.22.22），以下设定步骤：

步驟1.　进入 Windows 2000 点选【开始】，选择【运行】功能。 ***（如图 9-29）***

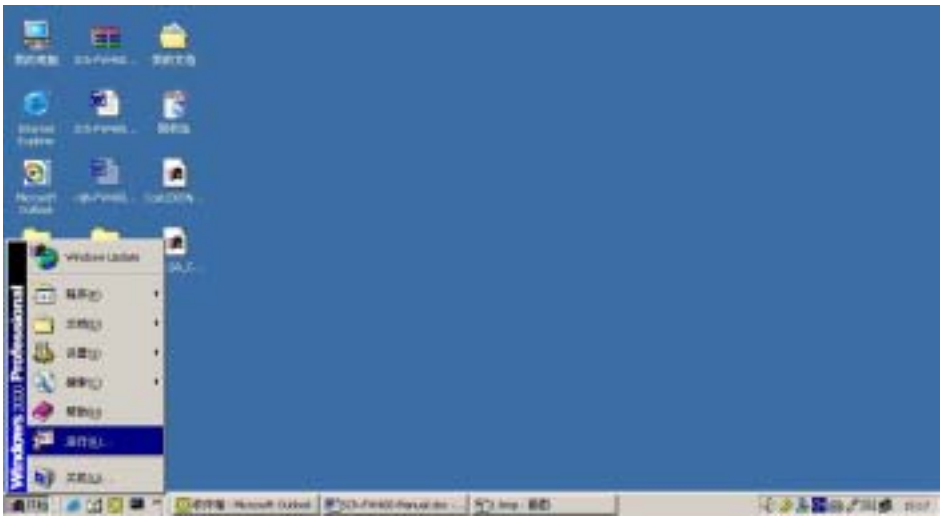


图 9-29　开始 Windows 2000 IPSec VPN 设定

步驟2.　在【运行】功能内。在开启的位置输入指令 MMC。 ***（如图 9-30）***

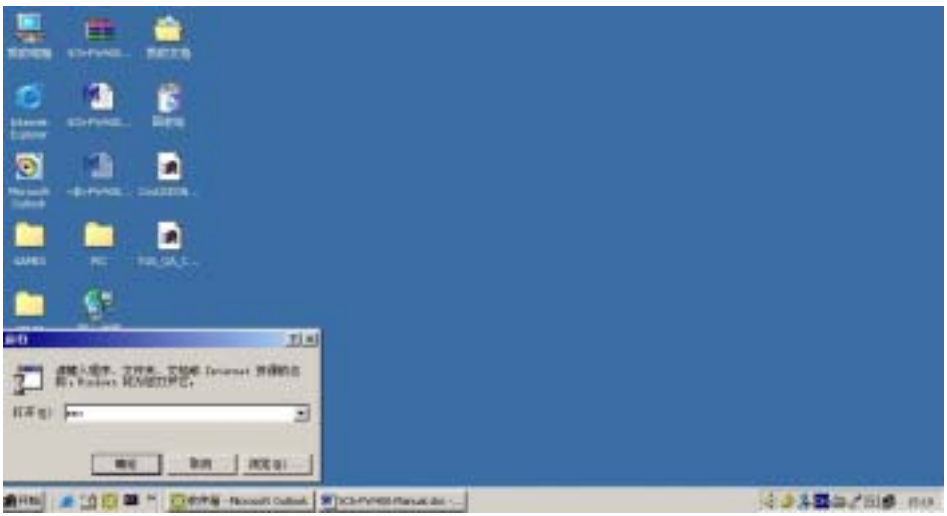


图 9-30　启动 Windows 2000 IPSec VPN 设定

步骤3. 进入控制台画面时，点选控制台(C)选项，并点选 **添加/删除管理单元。** ***（如图9-31）***

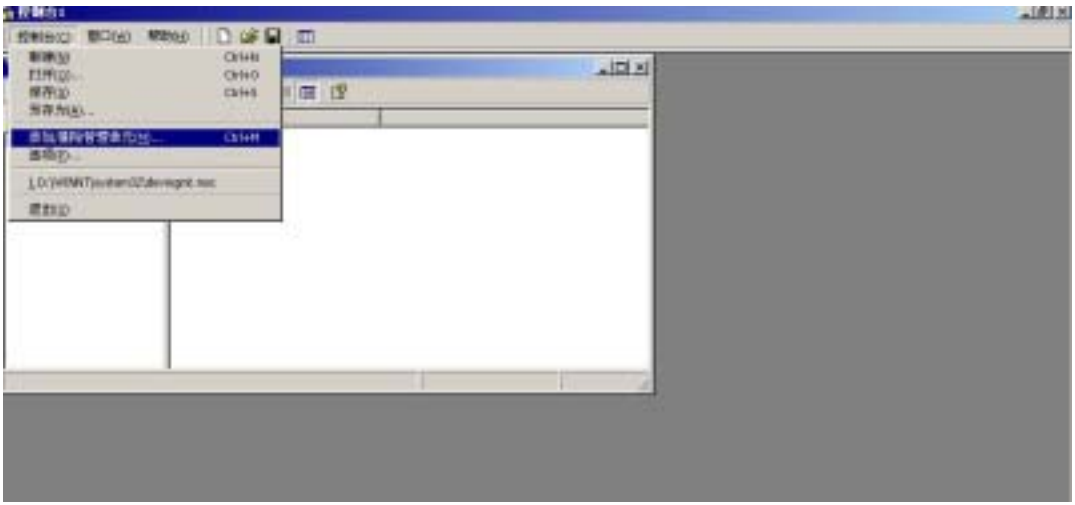


图 9-31 添加/删除管理单元

步骤4. 进入**添加/删除管理单元**画面中。点选**【添加】**，在**添加独立管理单元选择**画面中，**【添加】**IP 安全性原则管理。 ***（如图9-32）***

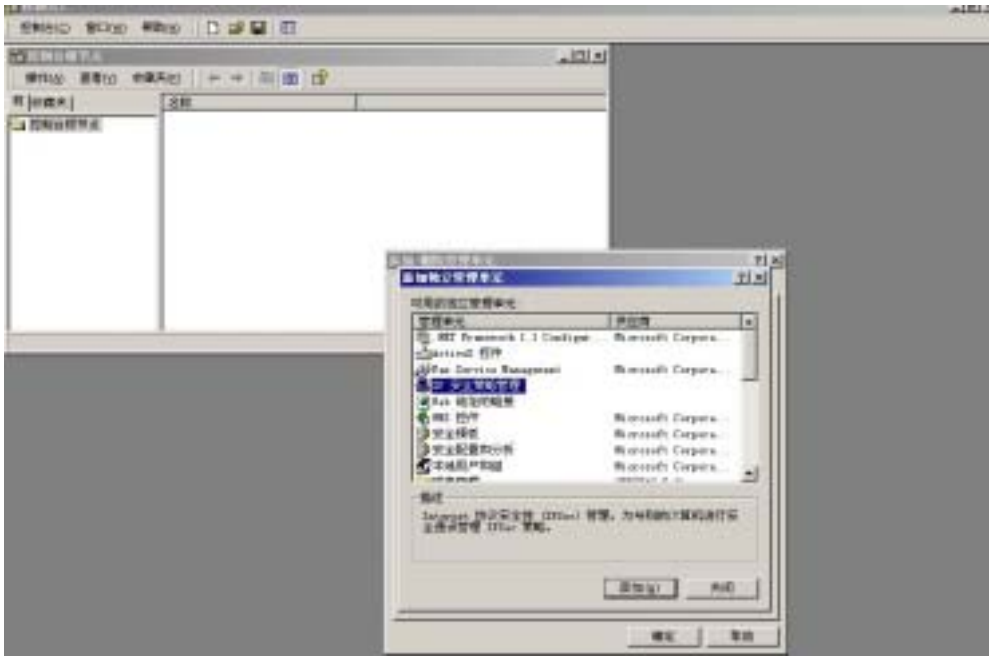


图 9-32 添加 IP 安全策略管理

步骤5． 选择本地计算机(L)，完成新增的动作。 *（如图9-33）*

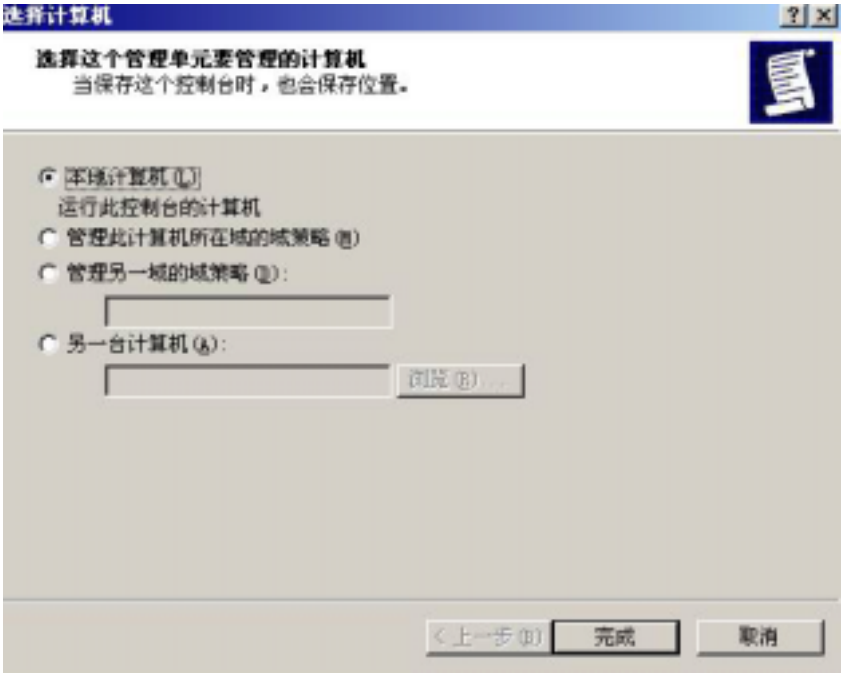


图 9-33 选择新增 IP 安全策略管理的类型

步骤6． 完成新增的动作。 *（如图9-34）*

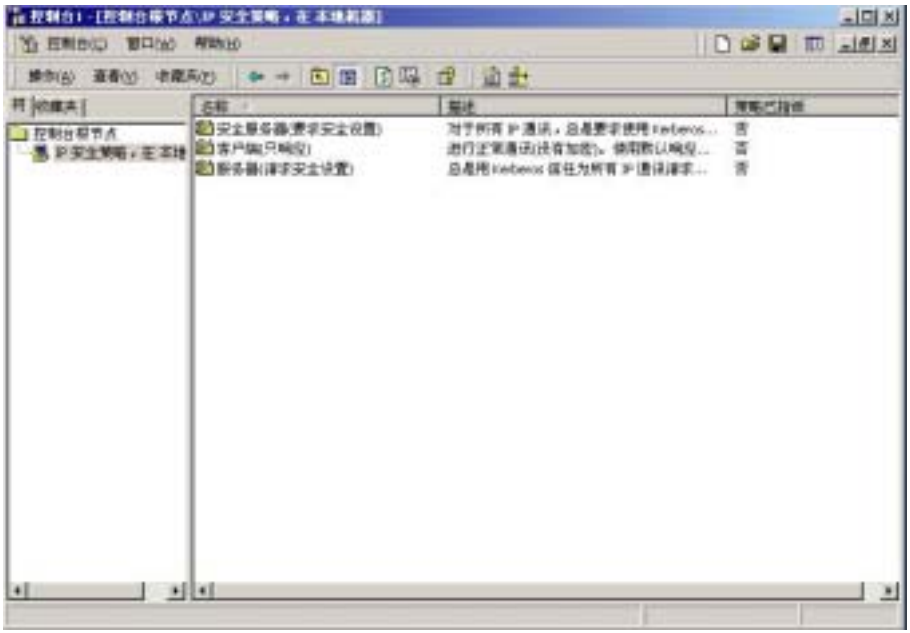


图 9-34 完成新增 IP 安全策略管理

步驟7. 在【本地计算机上的 IP 安全性原则】选项上按下鼠标右键，并选择创建 IP 安全策略(C)选项。 *（如图9-35）*

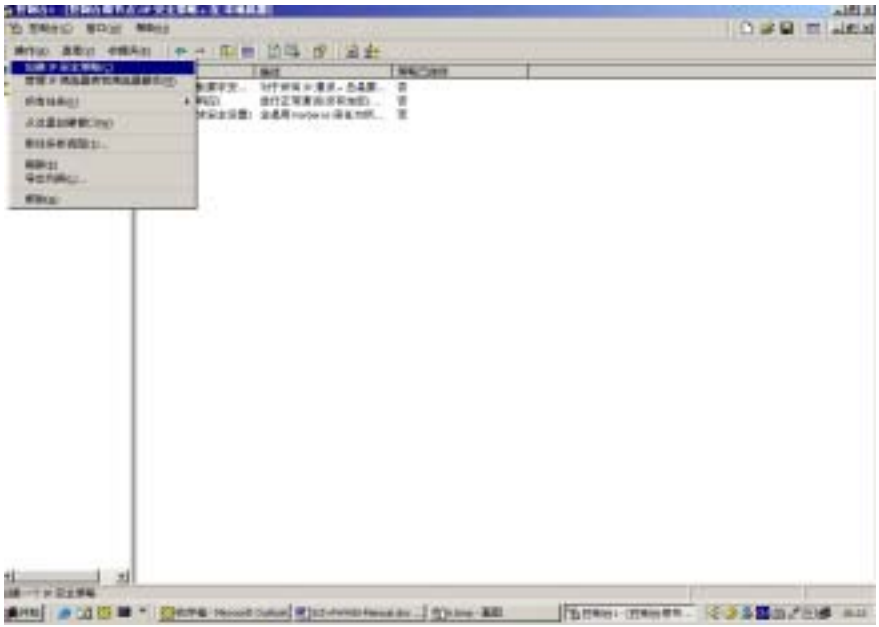


图 9-35 创建 IP 安全策略

步驟8. 点选【下一步】。 *（如图9-36）*

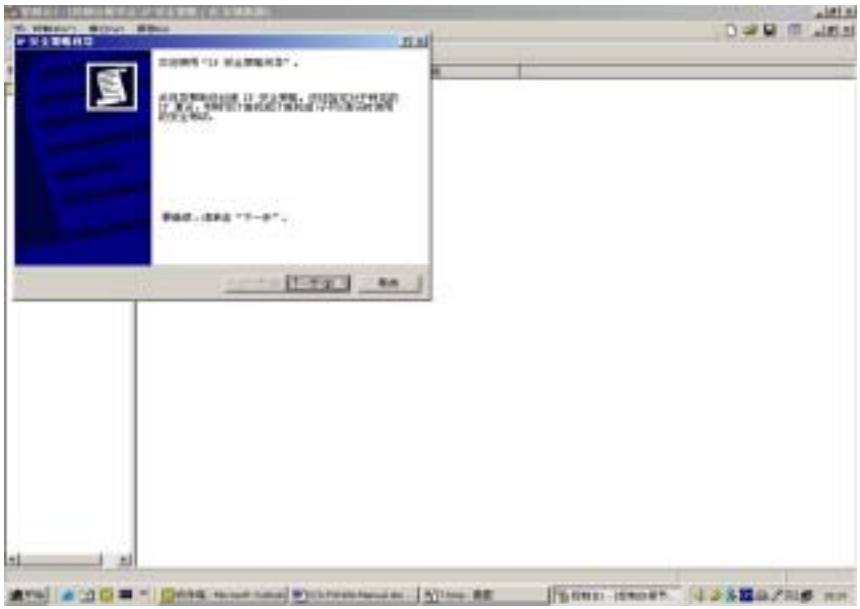


图 9-36 开启 IP 安全策略向导

步驟9. 填入 VPN 联机所使用的名称及描述，点选【下一步】。 *(如图9-37)*

图 9-37 设定 VPN 联机名称和描述

步驟10. 请取消使用启动预设的响应规则，点选【下一步】。 *(如图9-38)*

图 9-38 取消启动预设的响应规则

步驟11. 完成 IP 安全性原则，点选【**完成**】。并进入编辑内容。 *（如图9-39）*

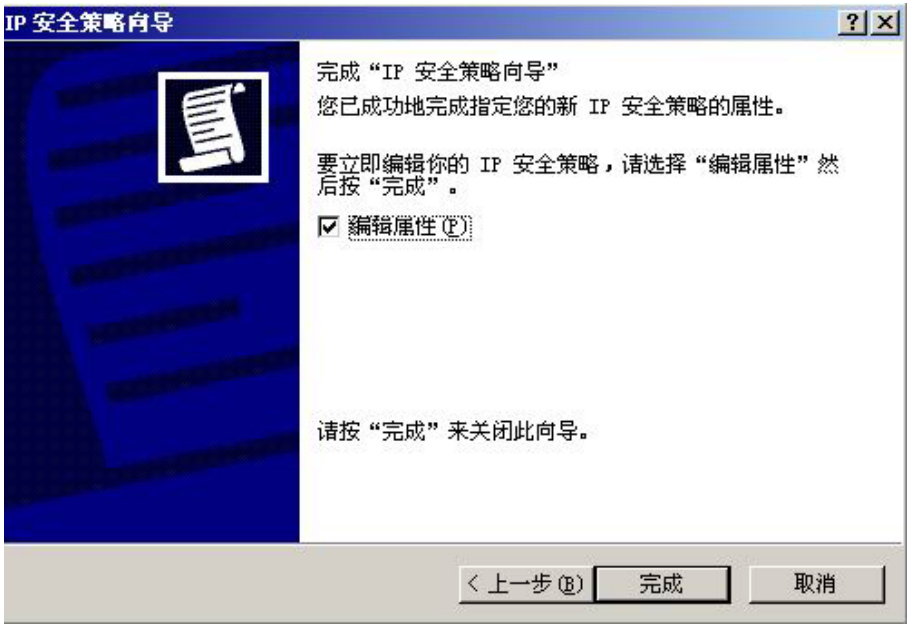


图 9-39　完成 IP 安全性原则精灵设定

步驟12. 进入 VPN_B 内容，请勿勾选使用“ 添加向导 ”，点选【**添加**】。进入编辑内容。 *（如图9-40）*

图 9-40　VPN_B 内容窗口

步骤13. 请在新增规则内容的画面中，点选【添加】。 *（如图9-41）*

图 9-41　添加 IP 筛选器列表

步骤14. 在 IP 筛选器列表的画面中，请勿勾选使用添加向导，更改名称为 VPN_B WAN TO LAN，并点选【添加】。 *（如图9-42）*

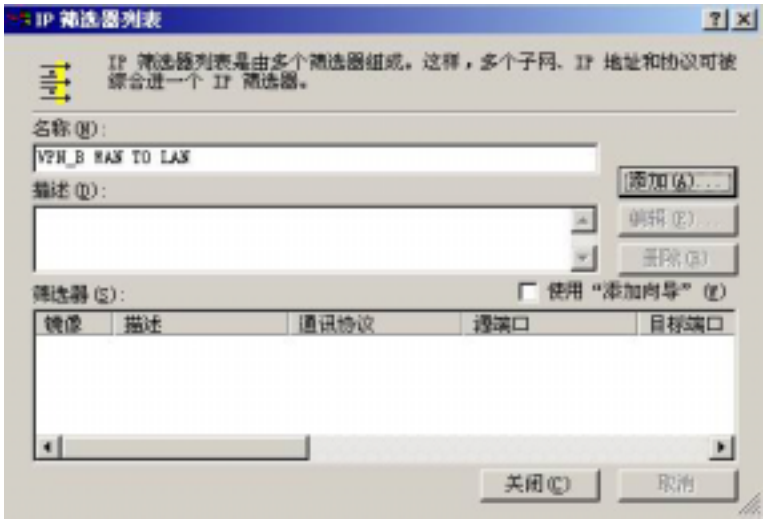


图 9-42　IP 筛选器列表窗口

步骤15. 进入筛选器内容，请将来源地址的下拉式选单中点选特定 IP 地址，并输入乙公司的外部网络 IP 211.22.22.22 子网掩码 255.255.255.255 请将目的地地址的下拉式选单中点选特定 IP 子网络，并输入甲公司的内部网络 192.168.10.0 子网掩码 255.255.255.0 请勿勾选已镜化处理，也对映完全相反的来源及目的地址的封包。 ***（如图9-43）***

图 9-43　筛选器属性窗口

步驟16. 完成设定，并关闭 IP 筛选器列表。 *（如图9-44）*

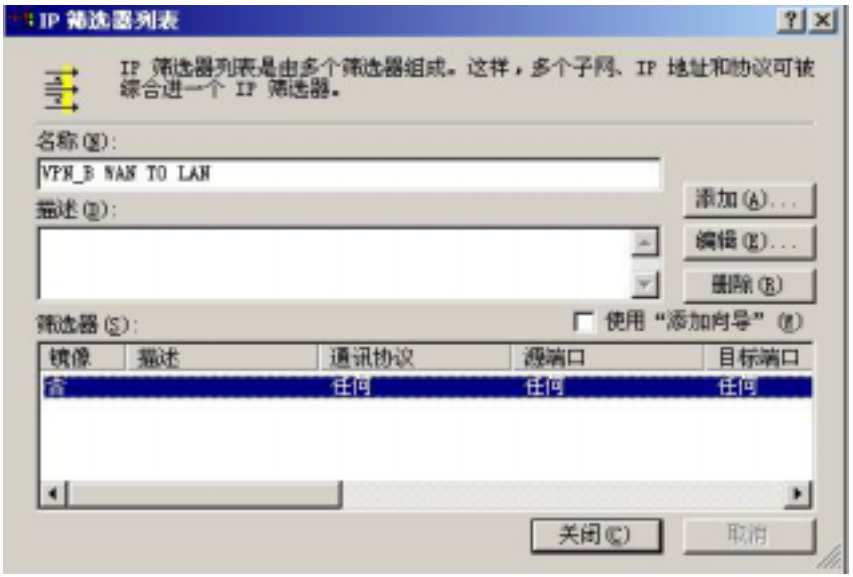


图 9-44　完成 IP 筛选器设定

步驟17. 点选最上面筛选器动作选项，并在筛选器动作中，选择要求安全设置，并点选编辑进入编辑。 *（如图9-45）*

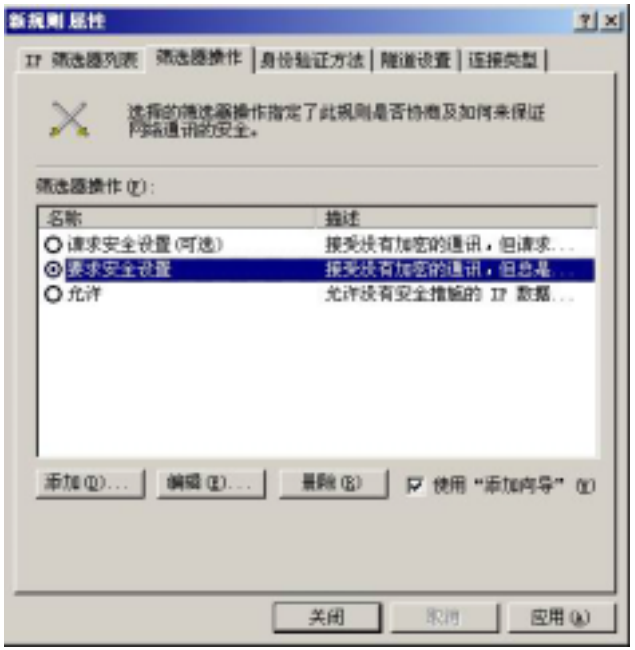


图 9-45　筛选器动作设定

步骤18. 进入要求安全设置内容，勾选会话密钥完全向前保密。 *（如图9-46）*

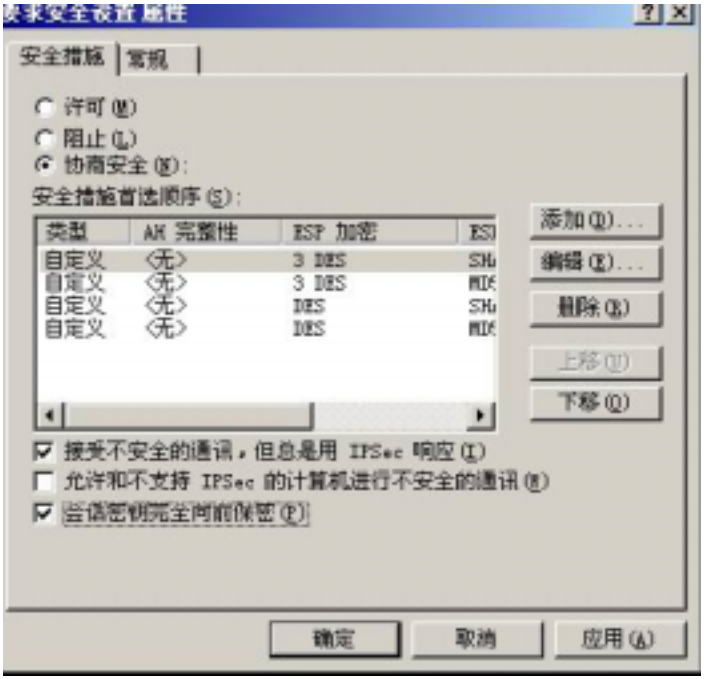


图 9-46　选取会话密钥完全向前保密

步骤19. 请在 自定义 / 无 / 3DES / MD5 上，点选编辑。 *（如图9-47）*

图 9-47　编辑安全性方法

步骤20. 点选自定义(专业用户)，并点选【**设置**】。 ***（如图9-48）***

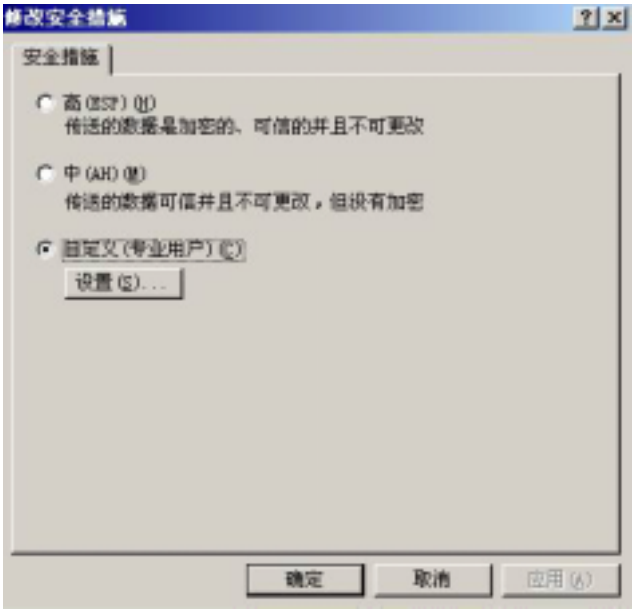


图 9-48　修改安全措施

步骤21. 请勾取数据完整性和加密(ESP) 选择 MD5 和 3DES 并勾选生成新密钥间隔，和输入 28800 秒。然后按 3 次【**确定**】回到规则内容。 ***（如图9-49）***

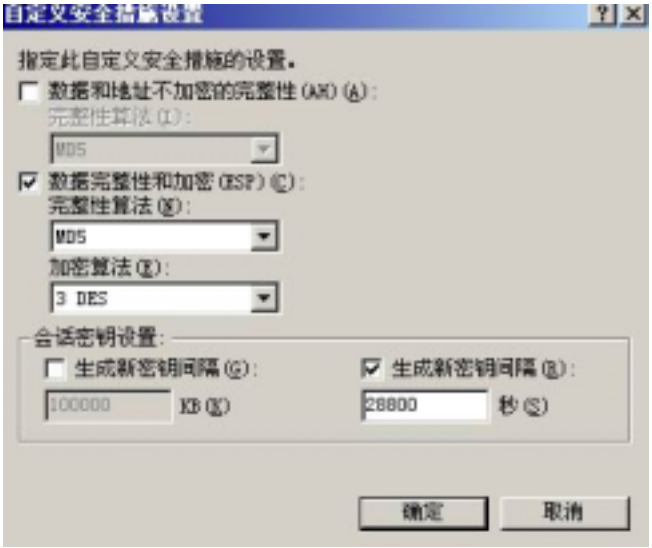


图 9-49　设定自定义安全措施设置

步骤22. 点选最上面连接类型选项，并在点选为 **所有网络连接**。 *（如图9-50）*

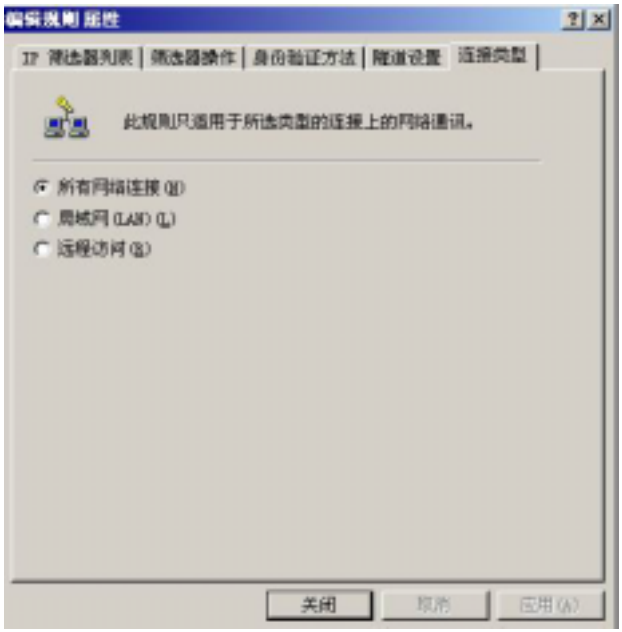


图 9-50　连接类型设定

步骤23. 点选最上面隧道设定选项，点选由这个 IP 地址来指定隧道的结束点。并输入甲公司 WAN 的 IP 地址 61.11.11.11。 *（如图9-51）*

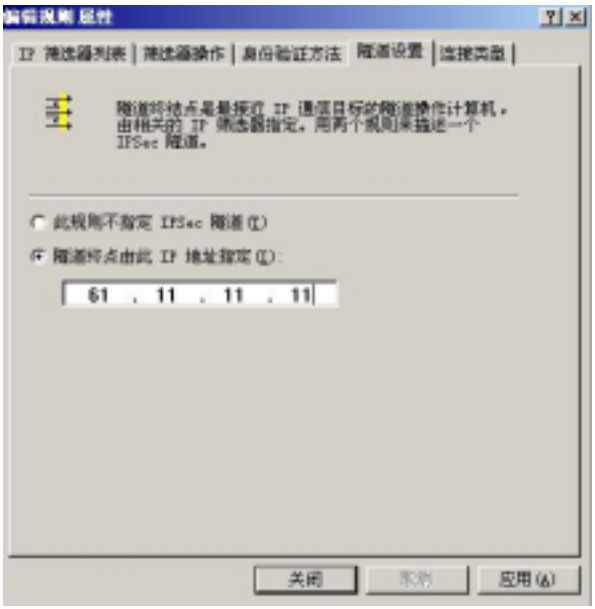


图 9-51　隧道设定窗口

步驟24. 点选最上面身份验证方法选项，并点选编辑进入编辑。 *（如图9-52）*

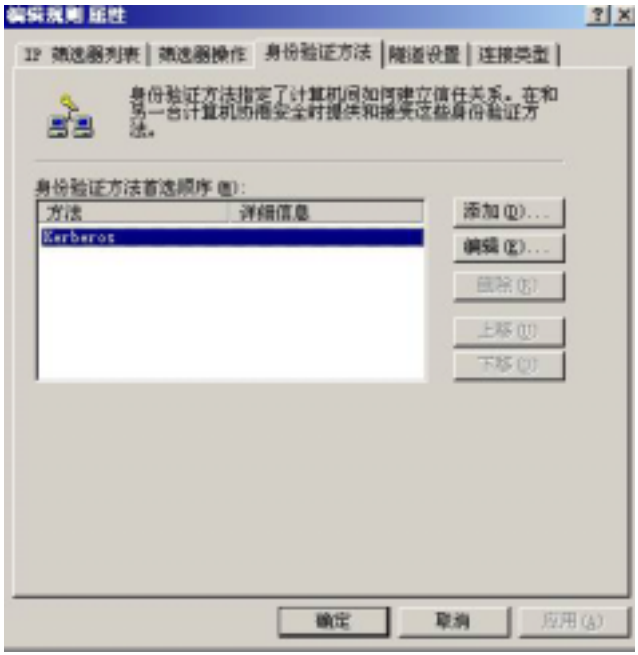


图 9-52　验证方法设定窗口

步驟25. 点选使用此字符串用来保护密钥交换选项，并输入双方所要联机的密钥 123456789。 *（如图9-53）*

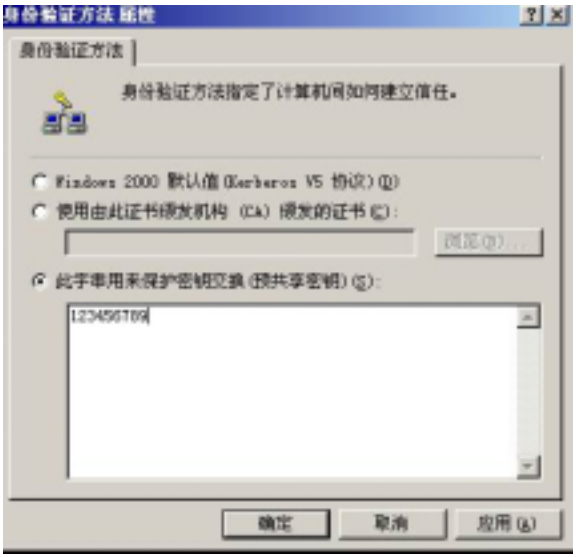


图 9-53　设定 VPN 联机密钥

步驟26. 完成设定，并关闭设定窗口。 *（如图9-54）*

图 9-54　完成验证方法设定

步驟27. 完成 VPN_B WAN TO LAN 规则所有设定。 *（如图9-55）*

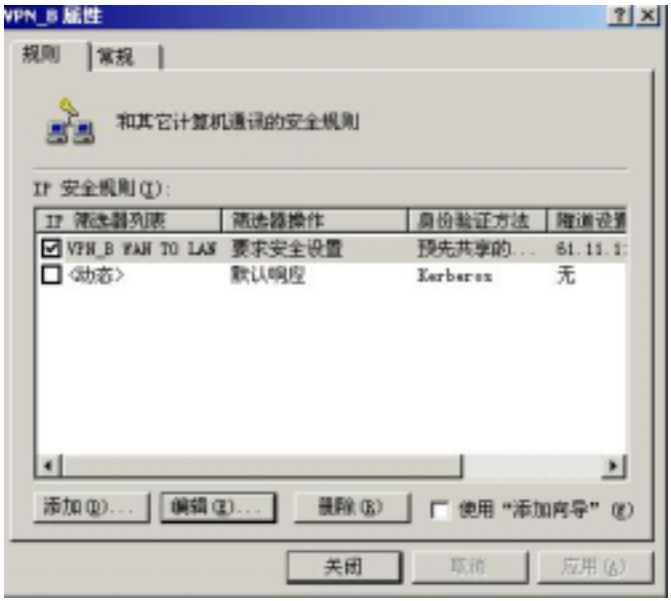


图 9-55　完成 VPN_B WAN TO LAN 规则设定

步驟28. 请再次进入 VPN_B 内容，请勿勾选使用添加向导，点选【**添加**】。再添加第二条 IP 安全性规则，进入编辑内容。 ***（如图 9-56）***

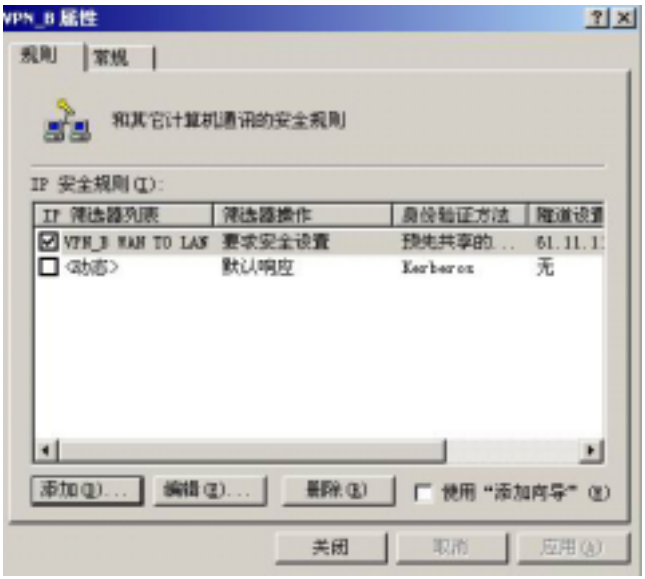


图 9-56　VPN_B 内容窗口

步驟29. 请在新增规则内容的画面中，点选【**添加**】。 ***（如图 9-57）***

图 9-57　新增规则内容窗口

步骤30.　请在 IP 筛选器列表的画面中，请勿勾选使用添加向导，输入名称为 VPN_B LAN TO WAN，并点选【**添加**】。 *（如图9-58）*

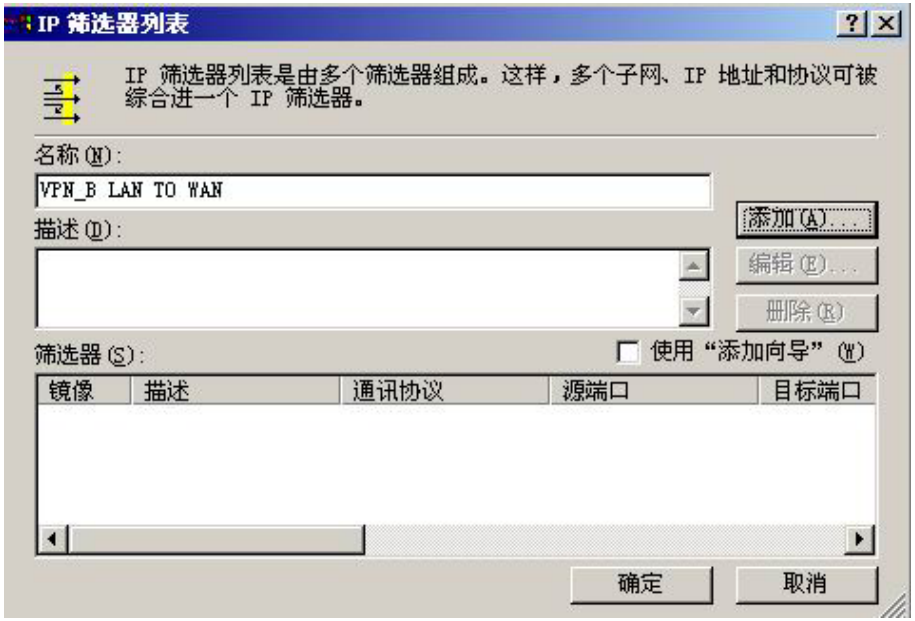


图 9-58　IP 筛选列表窗口

步骤31. 进入筛选器属性，请将来源地址的下拉式选单中点选特定 IP 子网络，并输入甲公司的内部网络 192.168.10.0 子网掩码 255.255.255.0 请将目的地地址的下拉式选单中点选特定 IP 地址，并输入乙公司的外部网络 IP 211.22.22.22 子网掩码 255.255.255.255 请勿勾选镜像，也对映完全相反的来源及目的地址的封包。 *（如图9-59）*

图 9-59　筛选器内容窗口

步驟32. 完成设定，并关闭 IP 筛选器列表。 *（如图9-60）*

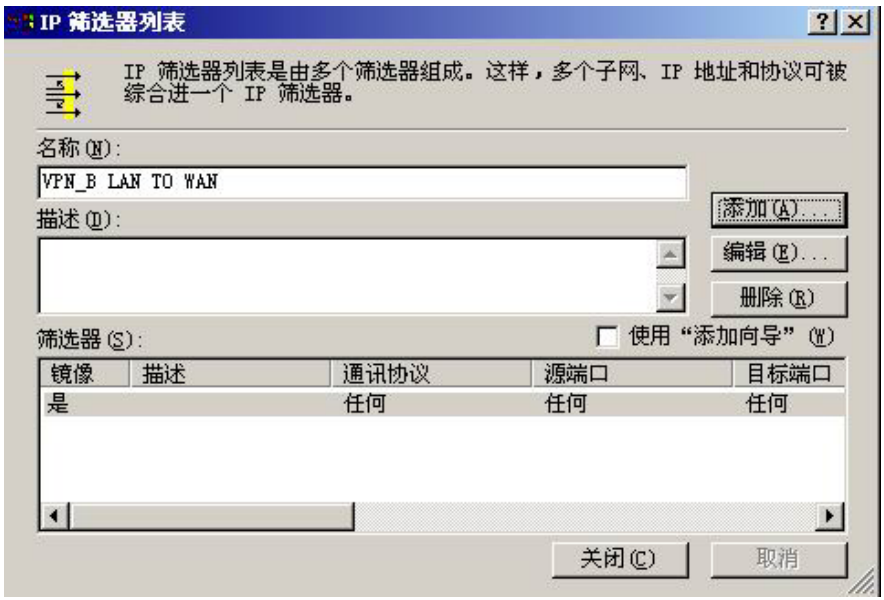


图 9-60　完成 IP 筛选器列表设定

步驟33. 点选最上面筛选器动作选项，并在筛选器动作中，选择需要安全性，并点选编辑进入编辑。 *（如图9-61）*

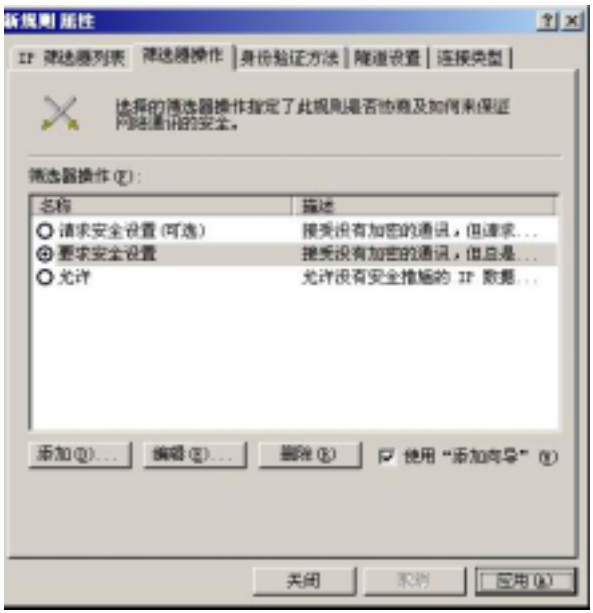


图 9-61　筛选器动作窗口

步驟34. 进入要求安全设置属性，勾选会话密钥完全向前保密。 *(如图9-62)*

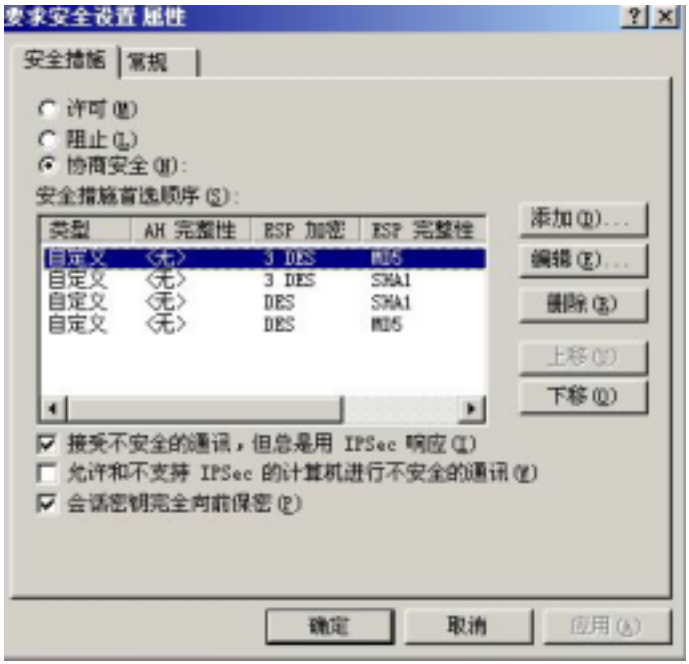


图 9-62　选择会话密钥完全向前保密

步驟35. 请在 自定义 / 无 / 3DES / MD5 上，点选编辑。 *(如图9-63)*

图 9-63　设定安全性方法

步驟36. 点选自定义(专业用户)，并点选【**设置**】。 *（如图9-64）*

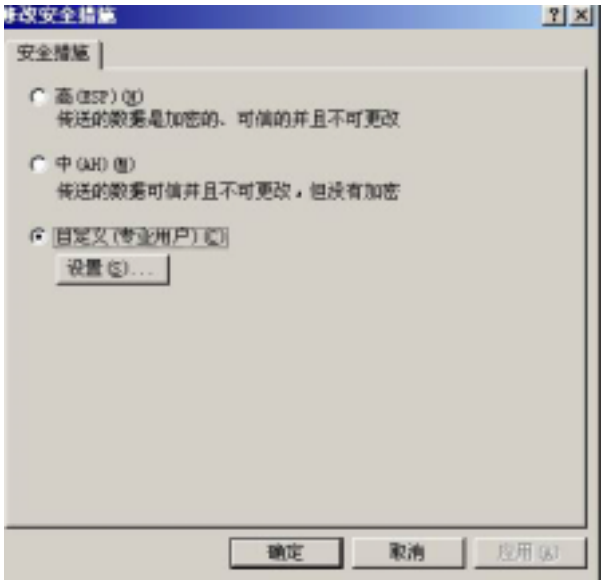


图 9-64　自定义安全措施

步驟37. 请勾取数据完整性和加密(ESP) 选择 MD5 和 3DES 并勾选生成新密钥间隔，和输入 28800 秒。然后按 3 次【**确定**】回到规则内容。 *（如图9-65）*

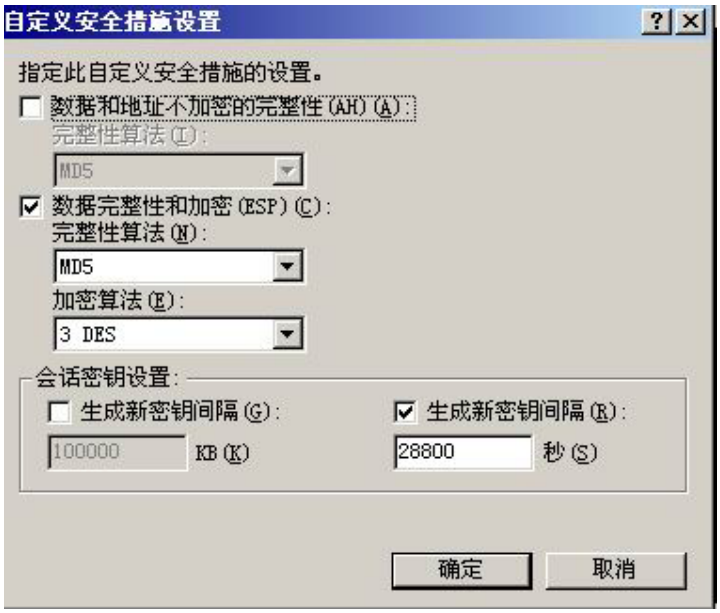


图 9-65　完成自定义安全性措施设置

步骤38. 点选最上面连接类型选项，并在点选为 **所有网络连接**。 *（如图9-66）*

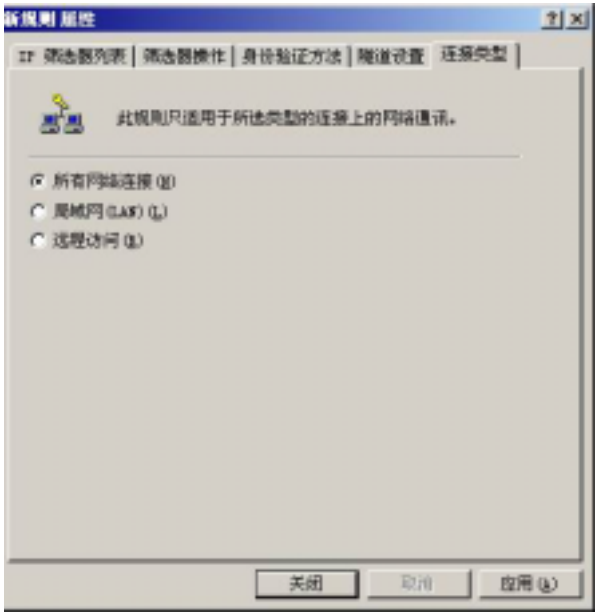


图 9-66　设定连接类型

步骤39. 点选最上面隧道设置选项，点选由这个 IP 地址来指定隧道的结束点。并输入乙公司 WAN 的 IP 地址 211.22.22.22。 *（如图9-67）*

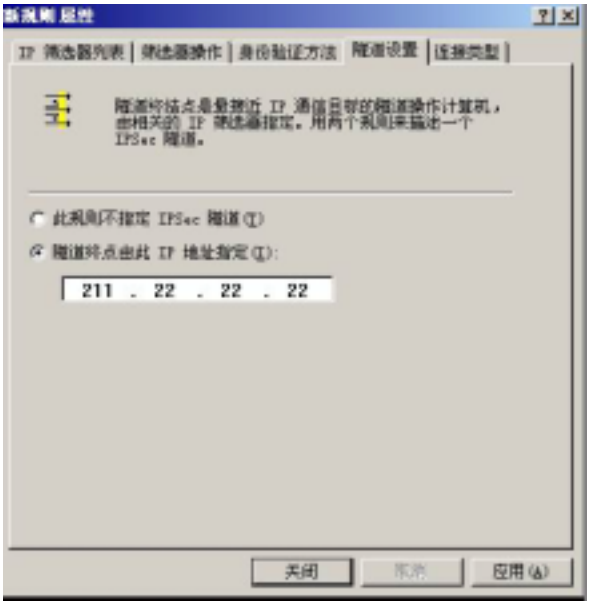


图 9-67　隧道设置窗口

步驟40. 点选最上面身份验证方法选项，并点选编辑进入编辑。 *(如图9-68)*

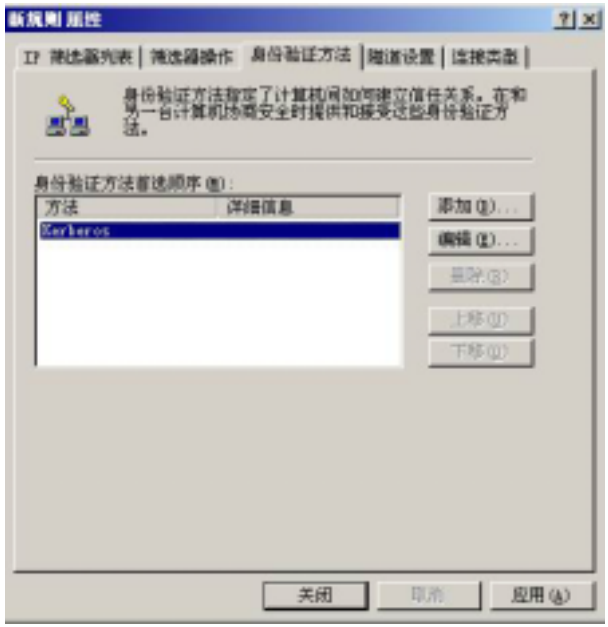


图 9-68　验证方法窗口

步驟41. 点选使用此字符串用来保护密钥间的交换选项，并输入双方所要联机的密钥 123456789。 *(如图9-69)*

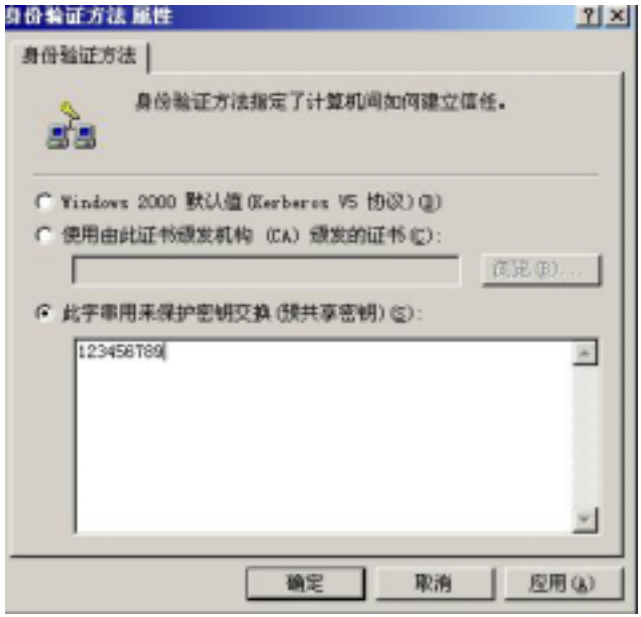


图 9-69　设定 VPN 联机密钥

步驟42. 应用设定，并关闭设定窗口。 *（如图9-70）*

图 9-70　完成验证方法设定

步驟43. 完成 VPN_B LAN TO WAN 规则所有设定。 *（如图9-71）*

图 9-71　完成 VPN_B LAN TO WAN 规则设定

步驟44. 请在 VPN_B 内容上方，选择常规，并选择高级设定。 *（如图9-72）*

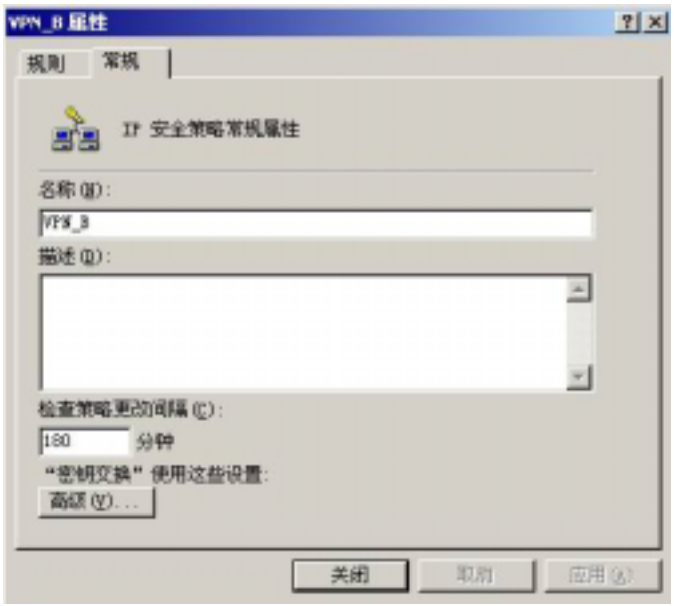


图 9-72　VPN_B 内容之一般内容窗口

步驟45. 请勾选主密钥完全向前保密后，并进入方法设定。 *（如图9-73）*

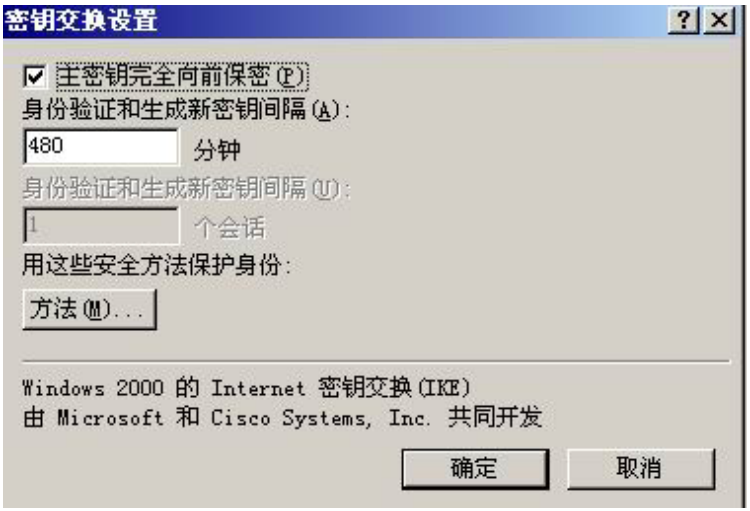


图 9-73　密钥交换设定窗口

步驟46. 请选择将 IKE / 3DES / MD5 / 中(2)移至最上方。 *(如图9-74)*

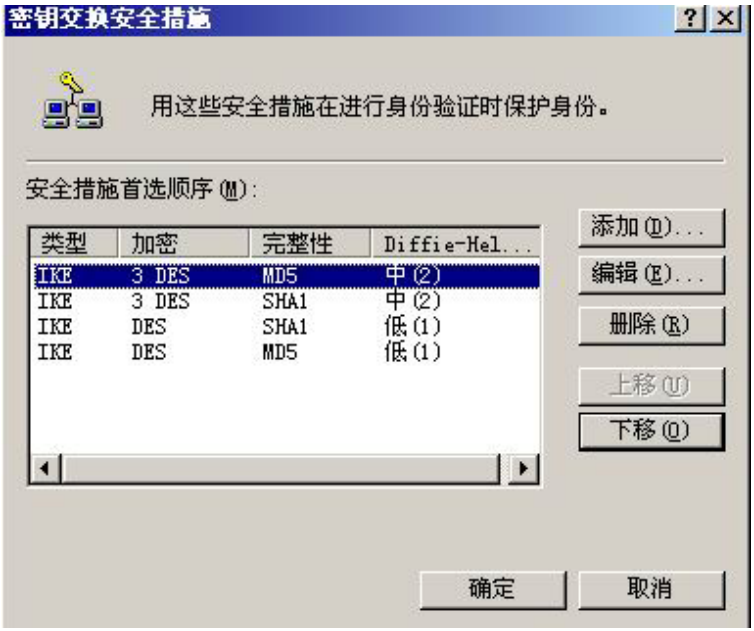


图 9-74 调整安全性方法顺序

步驟47. 完成乙公司 Windows 2000 VPN 所有设定。 *(如图9-75)*

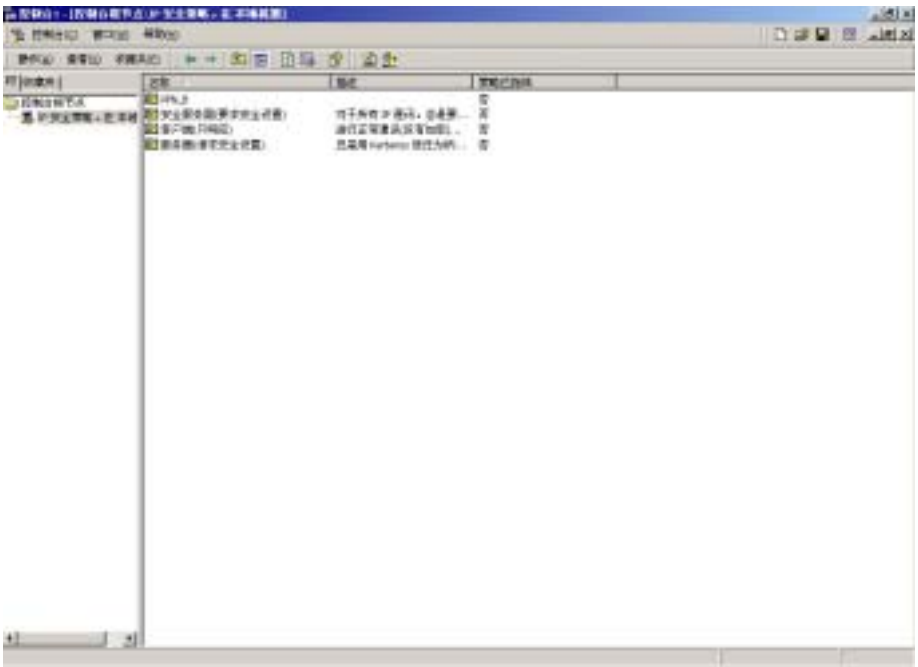


图 9-75 完成 Windows 2000 IPSec VPN 设定

步骤48. 请在 VPN_B 上点选鼠标右键，选择将 VPN_B 指派启动。 *（如图9-76）*

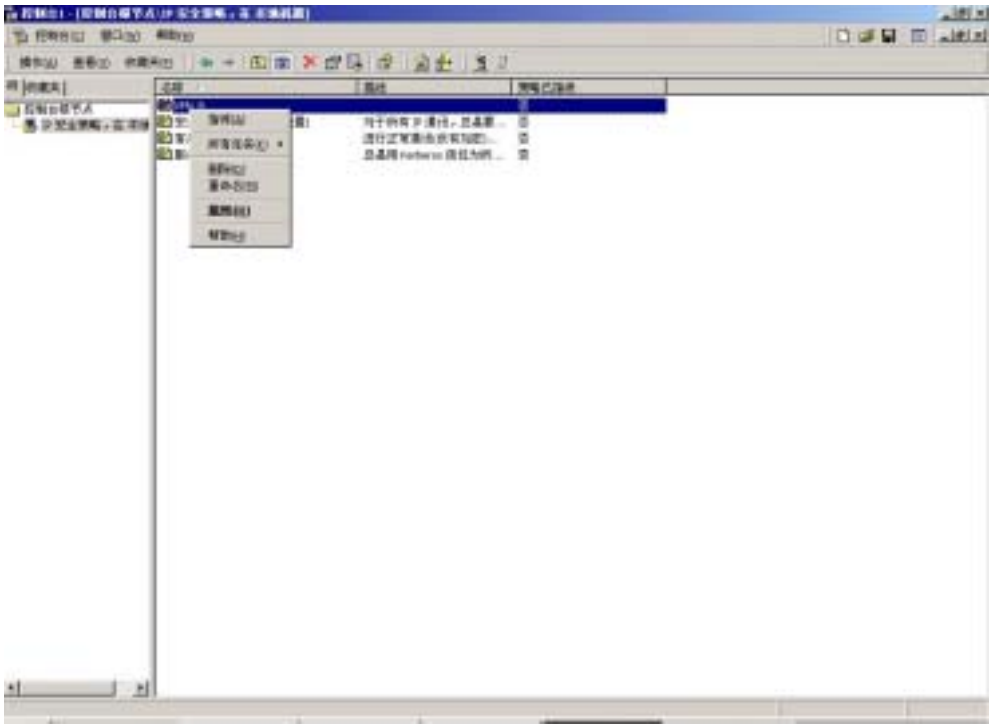


图 9-76　启动 VPN_B 安全性规则

步骤49. 我们需要重新启动 IPsec 服务，请由开始选单，选择设置选项，选择进入控制面版。 *（如图9-77）*

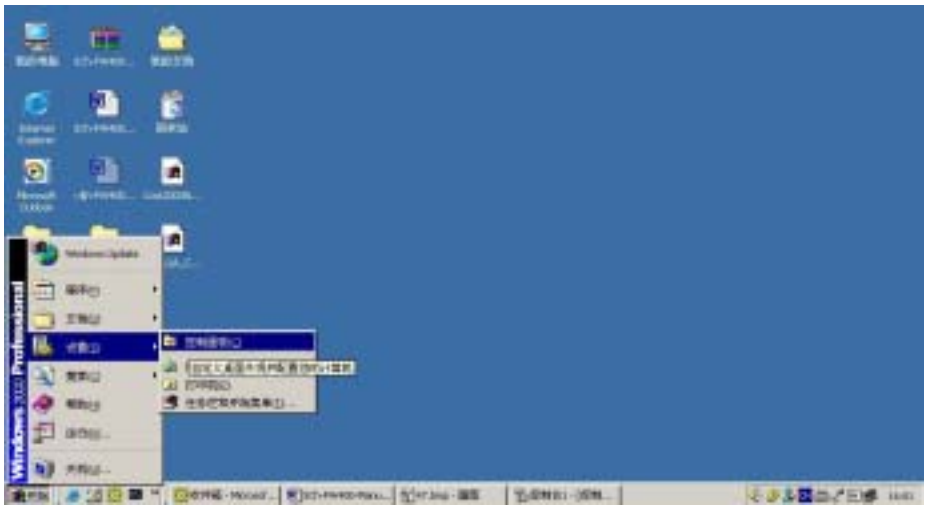


图 9-77　进入控制面版

步骤50. 进入控制面版后，请选择进入管理工具。 *（如图9-78）*

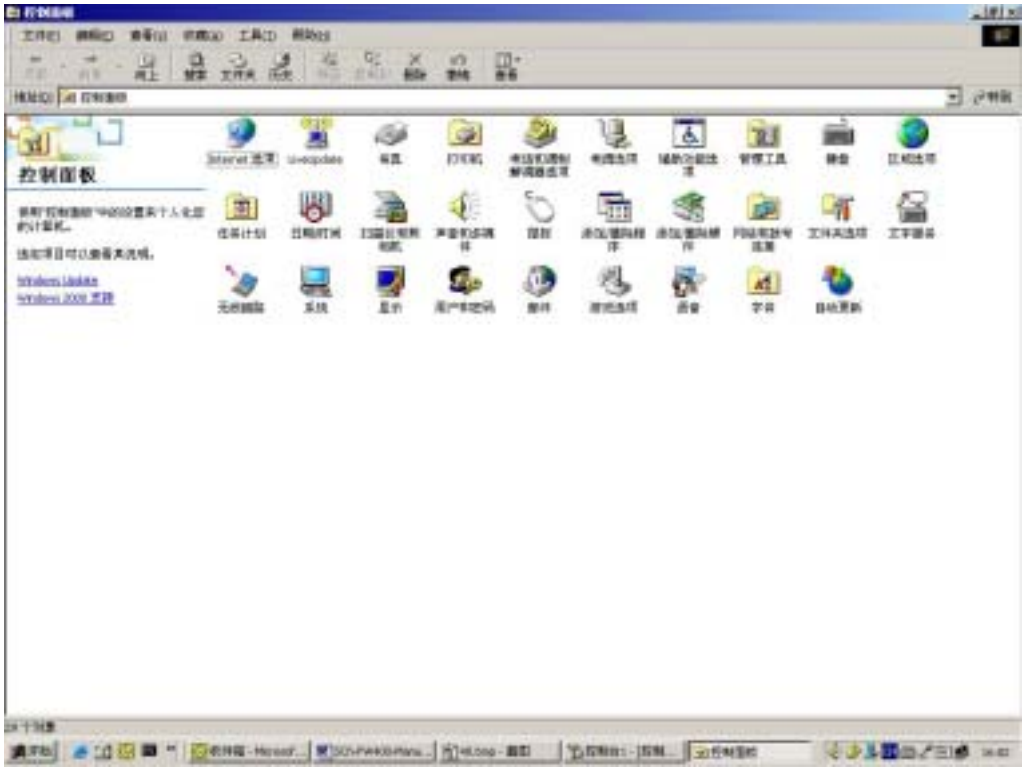


图 9-78　进入管理工具

步驟51. 进入管理工具后，请选择服务选项。 *（如图9-79）*

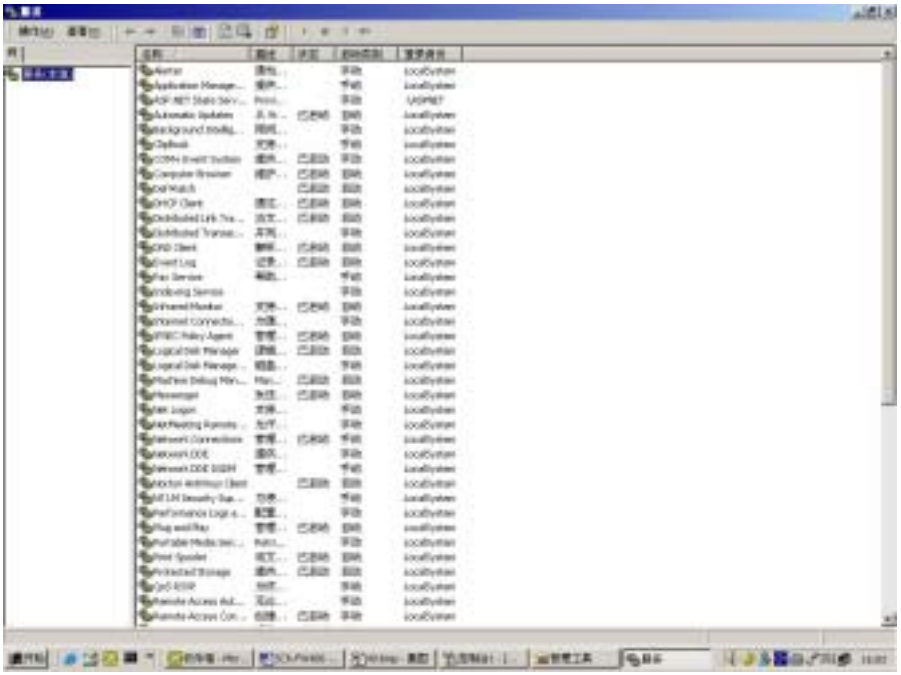


图 9-79　进入服务选项

步驟52. 进入服务后，请选择 IPsec Policy Agent 重新启动。 *（如图9-80）*

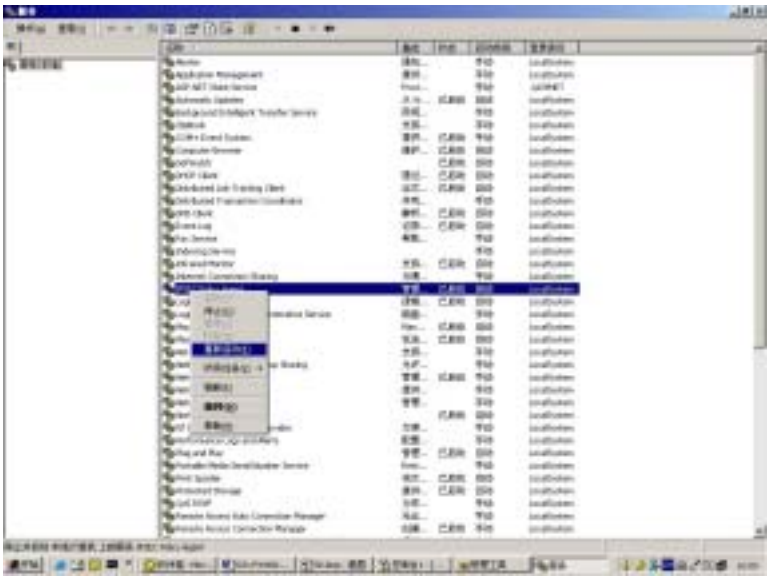


图 9-80　重新启动 IPSec Policy Agent

步驟53. 完成所有设定。

范例 3：使用两台 Firewall 机器 VPN 上设定联机方法。

(联机使用 Aggressive mode 算法)

先前作业

甲公司 External IP 为 61.11.11.11
Internal IP 为 192.168.10.X
乙公司 External IP 为 211.22.22.22
Internal IP 为 192.168.20.X

本范例以两台 FIREWALL 机器作为平台操作。假设甲公司 192.168.10.100 要向乙公司 192.168.20.100 做【虚拟私有网络】联机并下载其分享档案。(联机使用 Aggressive mode 算法)

甲公司 192.168.10.100 的预设网关为自己网域的 192.168.10.1，以下设定步骤：

步驟1. 进入甲公司负载平衡器预设地址 192.168.10.1，在左方的功能选项中，点选【VPN】功能，再点选**【IPSec 自动加密】**次功能选项。并点选**【新增】**功能。 ***（如图 9-81）***

图 9-81 IPSec 自动加密窗口

步驟2. 于【**VPN 自动金钥管理信道**】窗体中，填写所使用的 VPN 联机名称 VPN_A，并点选来源地址为【内部网络】。使用接口地址，选择 WAN1，并填入甲公司内部网络地址 192.168.10.0 及屏蔽 255.255.255.0。 ***（如图 9-82）***

图 9-82　VPN 自动金钥管理信道设定窗体

步驟3. 于【到目的地址】窗体中，填写所要联机乙公司的远程 IP 地址，并填入乙公司内部网络地址 192.168.20.0 及屏蔽 255.255.255.0。 ***（如图 9-83）***

图 9-83　IPSec 到目的地址设定窗体

步驟4. 于【认证方法】窗体中，选择 Preshare，并填入联机时的加密金钥 (加密金钥最高可输入 100 位)。 ***（如图 9-84）***

图 9-84　IPSec 认证方法设定窗体

步驟5. 于【加密或认证】窗体中， 勾选 Aggressive mode 算法(请参阅名词解说)，双方开始进行联机沟通时，Aggressive mode 建立联机时会自动选择所需加密的算法 3DES 加密演算，MD5 认证方式，选择群组 GROUP2 进行联机。

本地 / 远程 ID 可选择不输入。

本地 / 远程 ID 如要输入的话双方

需输入不相同的 IP 地址，例如 11.11.11.11 ,22.22.22.22。

如要输入数字或字母来提供验证前端需加@，例如 @123A ; @Abcd1。 ***（如图9-85）***

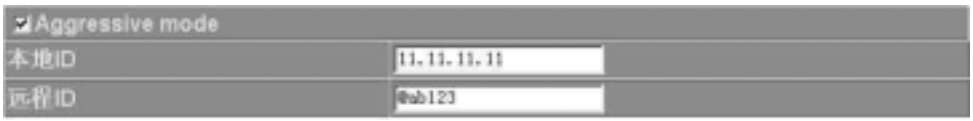


图 9-85 IPSec Aggressive mode 设定窗体

步驟5. 于【IPSec 算法】窗体中勾选资料加密+认证，可以选择资料加秘+认证或是仅选择认证方式来沟通:

加密算法可选择(3DES/DES/AES/NULL)我们选择 3DES 加密演算，

认证算法可选择(MD5/SHA1)我们选择 MD5 认证演算方式，来确保数据传输时所使用的加密认证方式。 ***（如图9-86）***

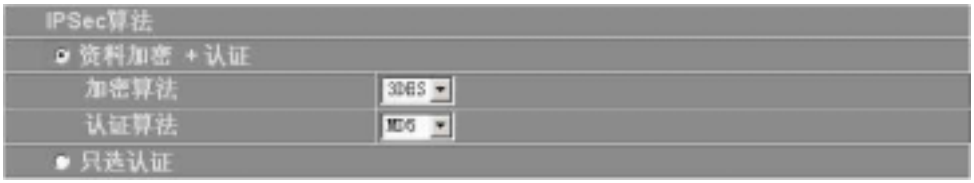


图 9-86 IPSec 算法设定窗体

步驟6. 勾选进阶加密，并填写加密金钥更新周期填入 28800 秒，并可输入乙公司可以保持联机的 IP 地址 192.168.20.100，使 VPN 能够持续联机保持不断线。 ***（如图9-87）***

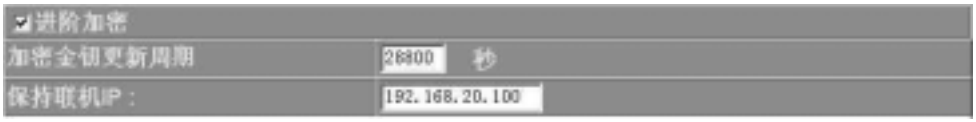


图 9-87 IPSec 进阶加密设定窗体

步驟7.　排程选择甲公司 VPN 可联机时间。 *（如图 9-88）*

图 9-88　IPSec 自动排程设定窗体

步驟8.　点选**【确定】**，完成甲公司设定。 *（如图 9-89）*

图 9-89　甲公司 IPSec VPN 完成设定

乙公司 192.168.20.100 的预设网关为自己网域的 192.168.20.1，以下设定步骤：

步骤1. 进入乙公司负载平衡器预设地址 192.168.20.1，在左方的功能选项中，点选【VPN】功能，再点选【**IPSec 自动加密**】次功能选项。并点选【**新增**】功能。 *（如图 9-90）*

图 9-90 IPSec 自动加密窗口

步骤2. 于【**VPN 自动金钥管理信道**】窗体中，填写所使用的 VPN 联机名称 VPN_B，并点选来源地址为【内部网络】。使用接口地址，选择 WAN1，并填入乙公司内部网络地址 192.168.20.0 及屏蔽 255.255.255.0。 *（如图 9-91）*

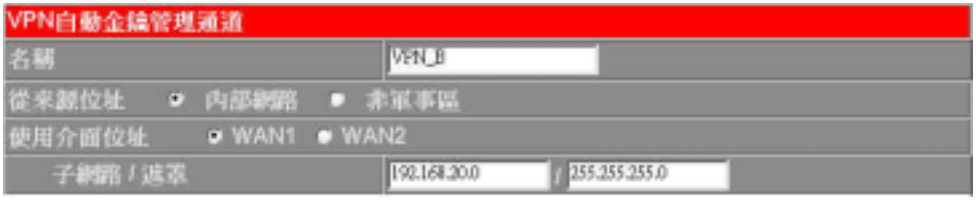


图 9-91 VPN 自动金钥管理信道设定窗体

步驟3. 于【到目的地址】窗体中，填写所要联机甲公司的远程 IP 地址，并填入甲公司内部网络地址 192.168.10.0 及屏蔽 255.255.255.0。 ***（如图9-92）***

图 9-92 IPSec 到目的地址设定窗体

步驟4. 于【认证方法】窗体中，选择 Preshare，并填入联机时的加密金钥(加密金钥最高可输入 100 位)。 ***（如图 9-93）***

图 9-93 IPSec 认证方法设定窗体

步驟5. 于【加密或认证】窗体中， 勾选 Aggressive mode 算法(请参阅名词解说)，双方开始进行联机沟通时，Aggressive mode 建立联机时会自动选择所需加密的算法 3DES 加密演算，MD5 认证方式，选择群组 GROUP2 进行联机。

本地 / 远程 ID 可选择不输入。

本地 / 远程 ID 如要输入的话双方

需输入不相同的 IP 地址，例如 11.11.11.11 ,22.22.22.22。

可输入数字或字母来提供验证前端需加@，例如 @123A ; @Abcd1。***（如图9-94）***

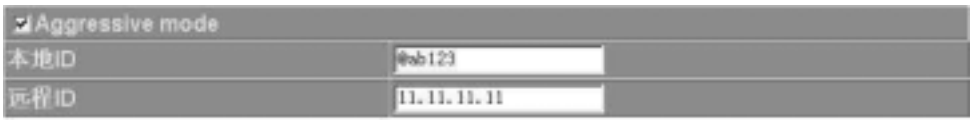


图 9-94 IPSec Aggressive mode 设定窗体

步驟6. 于【IPSec 算法】窗体中勾选资料加密+认证，可以选择资料加秘+认证或是仅选择认证方式来沟通:
加秘算法可选择(3DES/DES/AES/NULL)我们选择 3DES 加密演算，
认证算法可选择(MD5/SHA1)我们选择 MD5 认证演算方式，来确保数据传输时所使用的加密认证方式。 *（如图 9-95）*

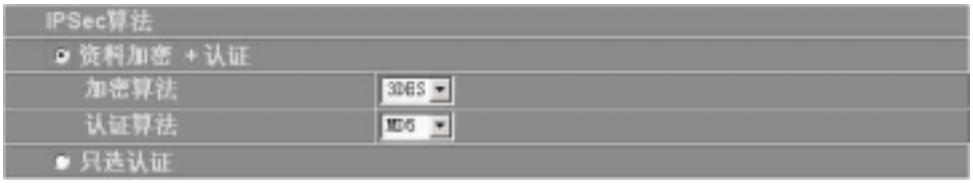


图 9-95 IPSec 算法设定窗体

步驟7. 勾选进阶加密，并填写加密金钥更新周期填入 28800 秒，并可输入甲公司可以保持联机的 IP 地址 192.168.10.100，使 VPN 能够持续联机保持不断线。 *（如图 9-96）*

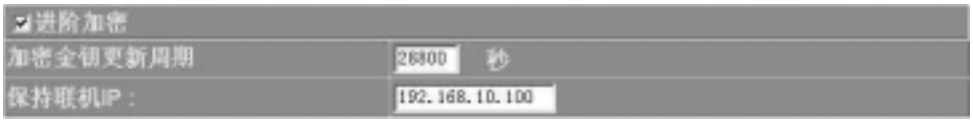


图 9-96 IPSec 进阶加密设定窗体

步驟8. 选择乙公司 VPN 排程可联机时间。 *（如图 9-97）*

图 9-97 IPSec 自动排程设定窗体

步驟9. 点选**【确定】**，完成乙公司设定。 *（如图 9-98）*

图 9-98 乙公司 IPSec VPN 完成设定

范例 4 :使用两台 Firewall 机器 VPN 上设定联机方法。

(联机使用 GRE/IPSec 封包封装算法)

先前作业

甲公司 External IP 为 61.11.11.11
Internal IP 为 192.168.10.X
乙公司 External IP 为 211.22.22.22
Internal IP 为 192.168.20.X

本范例以两台 FIREWALL 机器作为平台操作。假设甲公司 192.168.10.100 要向乙公司 192.168.20.100 做【虚拟私有网络】联机并下载其分享档案。(联机使用 **GRE/IPSec 封包封装**算法)

甲公司 192.168.10.100 的预设网关为自己网域的 192.168.10.1，以下设定步骤：

步驟1. 进入甲公司负载平衡器预设地址 192.168.10.1，在左方的功能选项中，点选【VPN】功能，再点选【**IPSec 自动加密**】次功能选项。并点选【**新增**】功能。 ***(如图 9-99)***

图 9-99 IPSec 自动加密窗口

步驟2. 于【**VPN 自动金钥管理信道**】窗体中，填写所使用的 VPN 联机名称 VPN_A，并点选来源地址为【内部网络】。使用接口地址，选择 WAN1，并填入甲公司内部网络地址 192.168.10.0 及屏蔽 255.255.255.0。 ***（如图 9-100）***

图 9-100　VPN 自动金钥管理信道设定窗体

步驟3. 于【到目的地址】窗体中，填写所要联机乙公司的远程 IP 地址，并填入乙公司内部网络地址 192.168.20.0 及屏蔽 255.255.255.0。 ***（如图 9-101）***

图 9-101　IPSec 到目的地址设定窗体

步驟4. 于【认证方法】窗体中，选择 Preshare，并填入联机时的加密金钥 (加密金钥最高可输入 100 位)。 ***（如图 9-102）***

图 9-102　IPSec 认证方法设定窗体

步驟5. 于【加密或认证】窗体中， 选择 ISAKMP 算法(请参阅名词解说)，双方开始进行联机沟通时，选择建立联机时所需加密的算法
请选择加密演算(3DES/DES/AES) 我们选择 3DES 及选择认证的算法(MD5/SHA1)我们选择 MD5 认证方式,另外需选择群组.(GROUP 1,2,5)双方需选择同一群组 我们选择 GROUP 1 来进行联机。 ***(如图 9-103)***

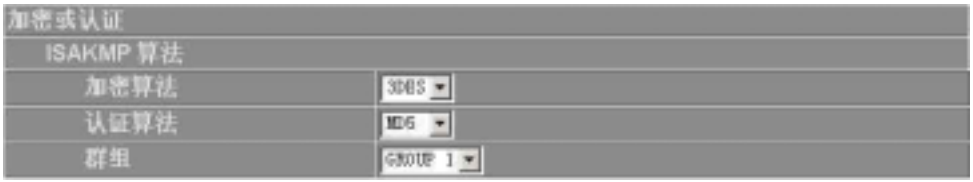


图 9-103 IPSec 加密或认证设定窗体

步驟6. 勾选 GRE/IPSec，并输入 GRE 来源端 IP 192.168.50.1
GRE 远程 IP 192.168.50.2 [此来源端 IP 和远程 IP 需为同一区段(C Class)，需自行设定]。 ***(如图 9-104)***

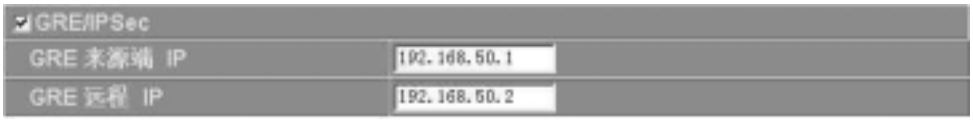


图 9-104 GRE/IPSec 设定窗体

步驟7. 于【IPSec 算法】窗体中勾选资料加密+认证，可以选择资料加秘+认证或是仅选择认证方式来沟通:
加秘算法可选择(3DES/DES/AES/NULL)我们选择 3DES 加密演算，认证算法可选择(MD5/SHA1)我们选择 MD5 认证演算方式，来确保数据传输时所使用的加密认证方式。 ***(如图 9-105)***

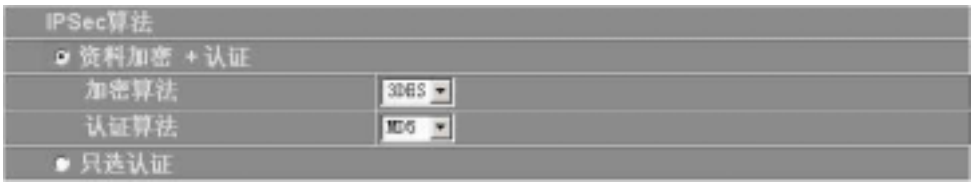


图 9-105 IPSec 算法设定窗体

步驟8. 勾选进阶加密，并填写加密金钥更新周期填入 28800 秒，并可输入乙公司可以保持联机的 IP 地址 192.168.20.100，使 VPN 能够持续联机保持不断线。 *（如图 9-106）*

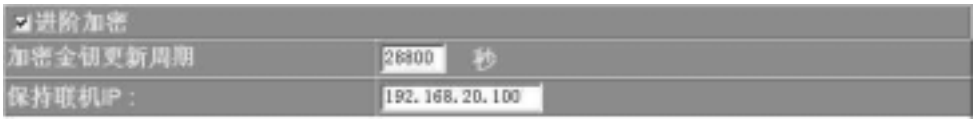


图 9-106 IPSec 进阶加密设定窗体

步驟9. 排程选择甲公司 VPN 可联机时间。 *（如图 9-107）*

图 9-107 IPSec 自动排程设定窗体

步驟10. 点选【**确定**】，完成甲公司设定。 *（如图 9-108）*

图 9-108 甲公司 IPSec VPN 完成设定

乙公司 192.168.20.100 的预设网关为自己网域的 192.168.20.1，以下设定步骤：

步骤1. 进入乙公司负载平衡器预设地址 192.168.20.1，在左方的功能选项中，点选【VPN】功能，再点选**【IPSec 自动加密】**次功能选项。并点选**【新增】**功能。 ***（如图 9-109）***

图 9-109 IPSec 自动加密窗口

步骤2. 于**【VPN 自动金钥管理信道】**窗体中，填写所使用的 VPN 联机名称 VPN_B，并点选来源地址为【内部网络】。使用接口地址，选择 WAN1，并填入乙公司内部网络地址 192.168.20.0 及屏蔽 255.255.255.0。 ***（如图 9-110）***

图 9-110 VPN 自动金钥管理信道设定窗体

步驟3. 于【到目的地址】窗体中，填写所要联机甲公司的远程 IP 地址，并填入甲公司内部网络地址 192.168.10.0 及屏蔽 255.255.255.0。 *（如图 9-111）*

图 9-111 IPSec 到目的地址设定窗体

步驟4. 于【认证方法】窗体中，选择 Preshare，并填入联机时的加密金钥(加密金钥最高可输入 100 位)。 *（如图 9-112）*

图 9-112 IPSec 认证方法设定窗体

步驟5. 于【加密或认证】窗体中， 选择 ISAKMP 算法(请参阅名词解说)，双方开始进行联机沟通时，选择建立联机时所需加密的算法
请选择加密演算(3DES/DES/AES) 我们选择 3DES 及选择认证的算法(MD5/SHA1)我们选择 MD5 认证方式,另外需选择群组.(GROUP 1,2,5)
双方需选择同一群组 我们选择 GROUP 1 来进行联机。 *（如图 9-113）*

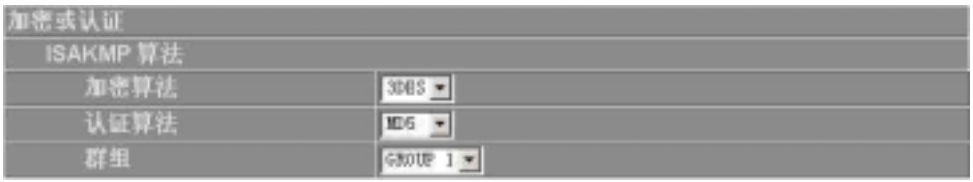


图 9-113 IPSec 加密或认证设定窗体

步驟6. 勾选 GRE/IPSec，并输入 GRE 来源端 IP 192.168.50.2
GRE 远程 IP 192.168.50.1 [此来源端 IP 和远程 IP 需为同一区段(C Class)，需自行设定]。 *（如图 9-114）*

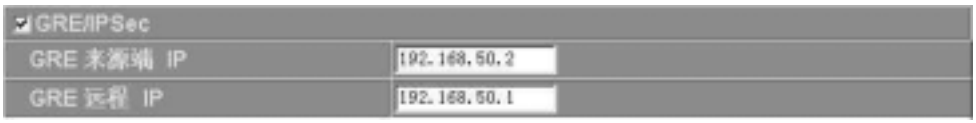


图 9-114 GRE/IPSec 设定窗体

步驟7. 于【IPSec 算法】窗体中勾选资料加密+认证，可以选择资料加秘+认证或是仅选择认证方式来沟通:
加秘算法可选择(3DES/DES/AES/NULL)我们选择 3DES 加密演算，认证算法可选择(MD5/SHA1)我们选择 MD5 认证演算方式，来确保数据传输时所使用的加密认证方式。 *(如图 9-115)*

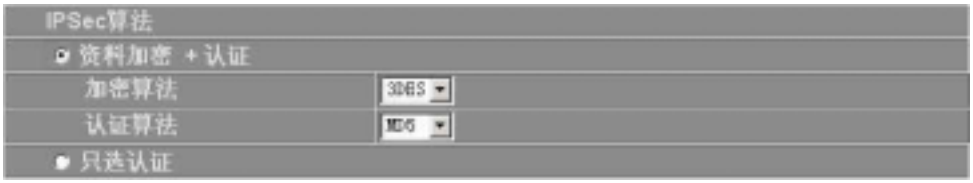


图 9-115 IPSec 算法设定窗体

步驟8. 勾选进阶加密，并填写加密金钥更新周期填入 28800 秒，并可输入甲公司可以保持联机的 IP 地址 192.168.10.100，使 VPN 能够持续联机保持不断线。 *(如图 9-116)*

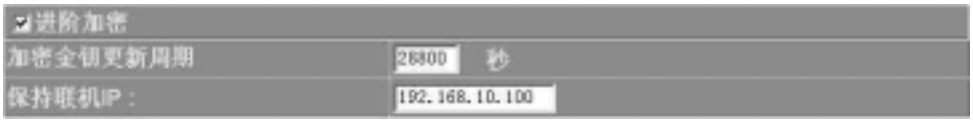


图 9-116 IPSec 进阶加密设定窗体

步驟9. 选择乙公司 VPN 排程可联机时间。 *(如图 9-117)*

图 9-117 IPSec 自动排程设定窗体

步驟10. 点选【确定】，完成乙公司设定。 *(如图 9-118)*

图 9-118 乙公司 IPSec VPN 完成设定

PPTP 服务器设定

步驟1. 在左方的功能选项中，点选【VPN】功能，再点选【PPTP 服务器】次功能选项。*（如9-119）*

图 9-119 PPTP 服务器设定

- PPTP 服务器：可设定激活或关闭
- 客户端 IP 范围 **192.94.49.1-254**：可设定 PPTP 客户端连入分配的网络地址范围。
- 使用者名称：PPTP 客户端连入时所使用的名称。
- 客户端 IP 地址：PPTP 客户端连入 PPTP 服务器时，所使用的客户端网络地址。
- 联机历时：显示目前 PPTP 客户端与 PPTP 服务器联机时间。
- 联机状况：显示目前 PPTP 客户端与 PPTP 服务器联机状况。
- 设定：变更各项设定值。点选【修改】，可修改 PPTP 服务器之各项参数；点选【删除】，可删除该项设定。

修改 PPTP 服务器设定

步骤1. 在【客户端 IP 范围】右方，点选【修改】按钮。

步骤2. 在【修改服务器设定】窗口中，键入下列参数 *(如图 9-120)*：

图 9-120 修改 PPTP 服务器设定

- 关闭 PPTP：可点选关闭 PPTP 服务器。
- 激活 PPTP：可点选激活 PPTP 服务器。
  1.加密认证设定为 开启 / 关闭。
  2.客户端 IP 范围：可输入 PPTP 客户端连入 PPTP 服务器所分配的 IP 网络地址范围。
- 闲置时间：可设定超过闲置时间范围将自动断线。
- 自动排程：可选择是否加入时间排程。

步骤2. 点选【确定】执行修改；或点选【取消】取消修改。

新增 PPTP 服务器

步骤1. 在【PPTP 服务器】窗口中，点选下方【新增】按钮。

步骤2. 在【新增 PPTP 服务器】窗口中，键入下列参数

- 使用者名称：定义 PPTP 客户端名称。此名称必须是唯一且不可重复。
- 密码：定义 PPTP 客户端密码。
- 远程客户端：

  1.可勾选 只对单一计算机作联机

  2.可勾选 对整个网域中的计算机作联机

  IP 地址：输入 PPTP 客户端整个网域 IP 地址

  子网掩码：输入 PPTP 客户端子网掩码
- 客户端的 IP 地址：

  1.使用配给的 IP 范围：勾选 PPTP 客户端连入时自动分配网络地址。

  2.使用特定 IP 地址：勾选 PPTP 客户端连入时使用键入的网络地址。

步骤3. 点选【确定】执行新增；或点选【取消】取消新增。*（如图 9-121）*

图 9-121 新增 PPTP 服务器

修改 PPTP 服务器

步驟1. 在【PPTP 服务器】窗口中，找到欲变更设定的 PPTP 服务器名称，对应至右方【设定】栏，点选【修改】。

步驟2. 在【修改 PPTP 服务器】窗口中，键入下列参数。

步驟3. 点选【确定】执行修改；或点选【取消】取消修改。*（如图 9-122）*

图 9-122 修改 PPTP 服务器

删除 PPTP 服务器

步驟1. 删除：在【PPTP 服务器】窗口表格中，找到欲删除设定的 PPTP 服务器名称，对应至右方【设定】栏，点选【删除】。

步驟2. 在【删除 PPTP 服务器】确定对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。*（如图 9-123）*

图 9-123 删除 PPTP 服务器图

PPTP 客户端

步驟1. 在左方的功能选项中，点选【VPN】功能，再点选【PPTP 客户端】次功能选项。*（如图 9-124）*

图 9-124 PPTP 客户端

- 使用者名称：PPTP 客户端连入 PPTP 服务器时所使用的名称。
- 服务器地址：PPTP 客户端连入的 PPTP 服务器网络地址。
- 联机历时：显示目前 PPTP 客户端与 PPTP 服务器联机时间。
- 联机状况：显示目前 PPTP 客户端与 PPTP 服务器联机状况。
- 设定：变更服务表中各项设定值。点选【联机】可使 PPTP 客户端与 PPTP 服务器端进行联机，点选【断线】会中断 PPTP 客户端与 PPTP 服务器端的联机，点选【修改】，可修改 PPTP 服务器之各项参数；点选【删除】，可删除该项设定。

新增 PPTP 客户端

步驟1. 在【PPTP 客户端】窗口中，点选下方【新增】按钮。

步驟2. 在【新增 PPTP 客户端】窗口中，键入下列参数

- 使用者名称：定义 PPTP 客户端名称。此名称必须是唯一且不可重复。
- 密码：定义 PPTP 客户端密码。
- 服务器地址：请键入欲联机 PPTP 服务器外部网络地址。
- 远程服务器：

  1.可勾选 只对单一计算机作联机。

  2.可勾选 对整个网域中的计算机作联机。

  IP 地址：输入 PPTP 服务器端整个网域 IP 地址。

  子网掩码：输入 PPTP 服务器子网掩码。
- 当封包传送时自动联机：可点选封包传送时自动与 PPTP 服务器联机。
- 闲置时间：可设定超过闲置时间范围将自动断线。
- 自动排程：可选择是否加入时间排程。

步驟3. 点选【确定】执行新增；或点选【取消】取消新增。*（如图 9-125）*

图 9-125 新增 PPTP 客户端

修改 PPTP 客户端

步驟1. 在【PPTP 客户端】窗口中，找到欲变更设定的 PPTP 客户端名称，对应至右方【设定】栏，点选【修改】。

步驟2. 在【修改 PPTP 客户端】窗口中，键入所修改的参数。

步驟3. 点选【确定】执行修改；或点选【取消】取消修改。*（如图 9-126）*

图 9-126 修改 PPTP 客户端

删除 PPTP 客户端

步驟1. 删除：在【PPTP 客户端】窗口表格中，找到欲删除设定的 PPTP 客户端名称，对应至右方【设定】栏，点选【删除】。

步驟2. 在【删除 PPTP 客户端】确定对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。*(如图9-127)*

图 9-127 删除 PPTP 客户端

第十章

监 控 记 录

监控记录为所有符合【管制条例】的联机记录，分为流量监控与事件监控两种，流量监控的参数是在制订管制条例时同时设定，流量监控详细记录每条管制条例资料封包联机内容，包含此封包的联机起始时间、封包来源地址、目的地址、服务项目及处置方式。事件监控则记录负载平衡器系统组态参数值(System Configurations)更改内容，包含更改者、更改时间、修改的参数，从什么 IP 地址登入…等。

本负载平衡器提供之「流量监控」与「事件监控」功能，为针对系统管理员所指定的「来源地址」与「目的地址」进行「服务项目」及「处置方式」的记录，让系统管理员掌握负载平衡器系统状况。同时，本负载平衡器亦提供系统管理员将各种记录下载备份。

（一）【流量监控】系统管理员可在流量监控记录里，查询目前进出负载平衡器各个联机状态，包括：联机起始时间、来源地址、目的地址与处置方式等。并每隔一段时间，将流量监控记录储存备份，再删除线上记录，让线上维持最新记录。
（二）【事件监控】当负载平衡器侦测到系统发生某些事件时，系统管理员可经由此事件监控功能，了解事件发生的时间详细说明，并将其下载备份。
（三）【联机纪录】：系统管理员可以利用此功能,了解目前对联机状态作纪录。
（四）【监控备份】：系统管理员可利用此功能，设定系统自动发出 E-mail 提醒管理员流量监控与事件监控的记录，也可利用远程记录实时接收负载平衡器的监控备份。

如何运用监控记录

系统管理员可利用监控记录，监控网络的使用情形，以作为网络管理的依据。

流量监控功能

步驟1. 在左方的功能选项中，点选【监控记录】功能，再点选【流量监控】次功能选项。*（如图10-1）*

图 10-1 流量监控功能

步驟2. 流量监控窗口名词名称定义：

- 下拉选单：点选下拉选单所显示的联机时间，以检视于该联机时间之流量状态。点选【下一页】，检视其它联机时间之流量状态。点选【上一页】，回到原流量监控画面。
- 时间：此监控记录发生的联机起始时间（月/日/时/分/秒）。
- 来源地址：来源端使用者的 IP 地址。（点选每一条纪录的此字段，可做 ”来源地址” 的过滤）
- 目的地址：目的端的 IP 地址。（点选每一条纪录的此字段，可做 ”目的地址” 的过滤）
- 协议：服务项目名称
- 端口号：服务项目服务端口。
- 处置方式：「」表示允许通过，「」表示禁止通过。

下载流量监控记录

步骤1. 在【流量监控】窗口中，点选屏幕下方【下载监控记录】功能按钮。

步骤2. 在【档案下载】对话框，将该流量监控记录储存至指定的硬盘目录位置 *（如图10-2）*

图 10-2 下载流量监控记录

清除流量监控记录

步骤1. 在【流量监控】窗口中，点选屏幕下方【清除监控记录】功能按钮。

步骤2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。*(如图10-3)*

图 10-3 清除流量监控记录

事件监控功能

步驟1. 在左方的功能选项中，点选【监控记录】功能，再点选【事件监控】次功能选项。*(如图 10-4)*

图 10-4 事件监控功能

步驟2. 事件监控窗口名词名称定义：

- 时间：此联机发生的起始时间。
- 事件：此联机发生时间的事件说明。

下载事件监控记录

步骤1. 在【事件监控】窗口中，点选屏幕下方【下载监控记录】功能按钮。

步骤2. 在【档案下载】对话框，将该事件监控记录储存至指定的硬盘目录位置 *（如图10-5）*

图 10-5 下载事件监控记录

清除事件监控记录

步骤1. 在【事件监控】窗口中，点选屏幕下方【清除监控记录】功能按钮。

步骤2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。*(如图10-6)*

图 10-6 清除事件监控记录

联机纪录功能

系统管理员可以利用此功能,了解目前对外部联机的状态作成纪录。*(如图10-7)*

图 10-7 联机纪录功能

联机纪录窗口名词名称定义：

- 时间：此联机发生的起始时间。
- 联机纪录：此联机发生时间的事件说明。

下载联机记录

步骤1. 在【联机纪录】窗口中，点选屏幕下方【下载监控纪录】功能按钮。

步骤2. 在【档案下载】对话框，将该联机纪录储存至指定的硬盘目录位置。*（如图10-8）*

图 10-8 下载联机记录

清除联机记录

步驟1. 在【联机纪录】窗口中，点选屏幕下方【清除监控记录】功能按钮。

步驟2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。*(如图10-9)*

图 10-9 清除联机记录

监控备份功能

步驟1. 在左方的功能选项中，点选【监控记录】功能，再点选【监控备份】次功能选项。*（如图 10-10）*

图 10-10 监控备份

步驟2. 【监控备份】窗口名词名称定义：

- 电子邮寄监控记录：当监控记录档案到达 300Kbytes 时，负载平衡器将会以电子邮件方式发出流量监控与事件监控记录通知系统管理员。
  ※请注意：激活此功能必须先于系统管理的系统设定填入 E-mail。
- 远程记录：设定此功能，系统会将流量监控与事件监控记录同步传送至此设定的 IP 地址的主机计算机。（该主机必须为提供 Syslog 功能的服务器）

欲重新起始联机监控记录，在【联机记录】工作窗口中。点选下方方【清除纪录】功能按钮，联机监控功能即由设定时实时激活。

激活电子邮件与远程监控记录

步驟1. 开启电子邮寄监控记录功能：请先于选单【系统管理】的【系统设定】中的【E-mail 设定】，勾选【开启电子邮件警讯通知】并键入欲接收监控记录之电子邮件地址，点选【确定】后再于【监控记录】的【监控备份】勾选【激活电子邮寄监控记录】，最后点选屏幕右下方【确定】按钮。

步驟2. 激活远程记录：勾选【激活远程记录】，并于下方【远程记录主机 IP】空栏中，键入提供接收记录监控的主机 IP 地址与 Port number 后，点选屏幕右下方【确定】按钮。*(如图 10-11)*

图 10-11 激活电子邮寄监控&远程记录

取消电子邮件与远程监控记录

步驟1. 取消电子邮寄监控记录：取消勾选【激活电子邮寄监控记录】功能，点选屏幕右下方【确定】按钮。

步驟2. 取消远程记录：取消勾选【激活远程记录】功能，并点选屏幕右下方【确定】按钮。*（如图 10-12）*

图 10-12 取消电子邮寄监控&远程记录

第十一章

警 示 记 录

警示记录分为「流量警示」与「事件警示」两种。

（一）【流量警示】：在制订管制条例时须先设定流量警示值，系统每隔一段时间会检查经过管制条例的资料量是否超过警示值，如果超过警示值，系统会将其记录在流量警示档案。

（二）【事件警示】：当负载平衡器侦测出网络正受到骇客恶意攻击时，系统会将攻击资料写入事件警示档，并发出 E-mail 通知管理员采取警急措施。

如何运用警示记录

系统管理员可利用「警示记录」功能，查询进出负载平衡器「来源地址」、「目的地址」、「网络服务」以及网络繁忙状况。每隔一段时间，系统主管理员可将「流量警示记录」与「事件警示记录」储存备份，再删除线上记录，让线上维持最新网络状态记录。

流量警示功能

步驟1. 在左方的功能选项中，点选【警示记录】功能，再点选【流量警示】次功能选项。*（如图 11-1）*

图 11-1 流量警示功能

步驟2. 流量警示窗口，表格内数值显现目前系统联机的状态。

- 时间：连结起始至结束的时间（起始时间 月/日/时/秒 至 结束 时/秒）。
- 来源地址：来源端网络地址。
- 目的地址：目的端网络地址。
- 服务名称：服务项目名称。
- 网络流量：网络流量（Kbytes/Sec）。

下载流量警示记录

步骤1. 在【流量警示】窗口中，点选屏幕下方【下载监控记录】功能按钮。

步骤2. 在【档案下载】对话框，将该流量警示记录储存至指定的硬盘目录位置 *（如图 11-2）*

图 11-2 下载流量警示记录

清除流量警示记录

步骤1. 在【流量警示】窗口中，点选屏幕下方【清除记录】功能按钮。

步骤2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。*（如图11-3）*

图 11-3 清除流量警示记录

事件警示功能

步驟1. 在左方的功能选项中，点选【警示记录】功能，再点选【事件警示】次功能选项。*(如图 11-4)*

图 11-4 事件警示记录功能

步驟2. 在【事件警示】窗口中，表格内数值显现目前系统联机状态

- 下拉选单：可点选下拉选单所显示的事件警示发生时间，以检视于该联机时间警示说明。点选【下一页】，检视其它联机时间之事件警示。点选【上一页】，回到原事件警示画面。
- 时间：事件发生的联机时间（月/日/时/秒）。
- 事件：事件说明。

下载事件警示记录

步骤1. 在【事件警示】窗口中，点选屏幕下方【下载监控记录】功能按钮。

步骤2. 在【档案下载】对话框，将该事件警示记录储存至指定的硬盘目录位置 *（如图 11-5）*

图 11-5 下载事件警示记录

清除事件警示记录

步骤1. 在【事件警示】窗口中，点选屏幕下方【清除记录】功能按钮。

步骤2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。*（如图11-6）*

图 11-6 清除事件警示记录

第十二章

流 量 统 计

「**外部网络流量**」即为所有符合【外部网络】的 上传/下载 封包及上传/下载 流量记录的统计资料。

「**管制条例流量**」即为所有符合【管制条例】的封包记录的统计资料。

系统管理员可运用流量统计功能，查询负载平衡器针对【管制条例】内之「来源网络」、「目的网络」、「网络服务」与管制动作等各联机进出负载平衡器的「封包」、「传输量」流量统计，以提供系统管理员监控网络系统流量状况，查看网络繁忙状况。

如何运用流量统计

系统管理员须先至【接口地址】功能设定中，激活并设定所要统计流量的【外部网络接口】，以经由「流量统计」功能得知目前网络的使用状况，作为网络管理的依据。

外部网络流量功能

在左方菜单点选【流量统计】，再点选下方【外部网络流量】次功能选项。

即为所有符合【外部网络】的 下载/上传 封包及 下载/上传 流量记录的统计资料。*（如图 12-1）*

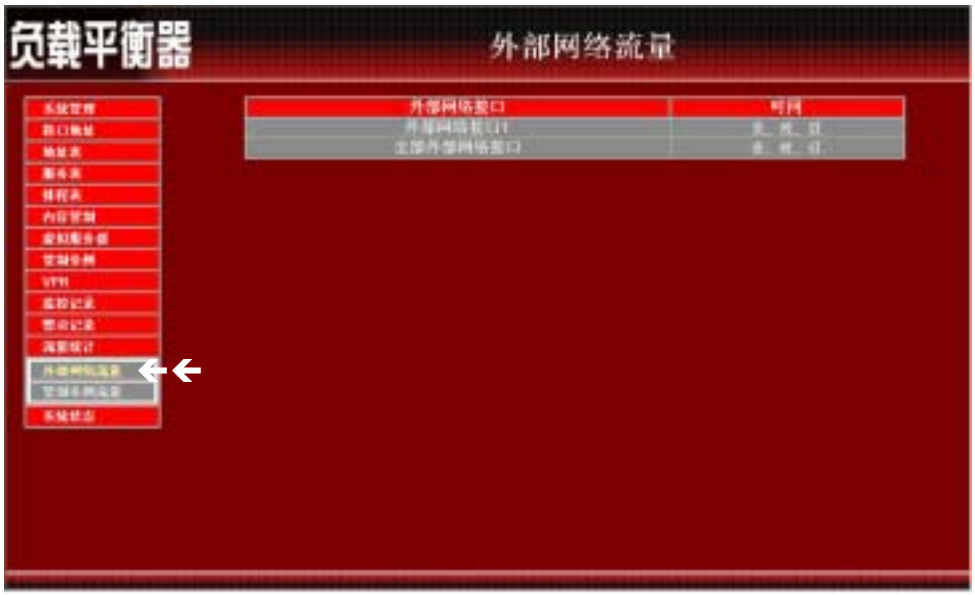


图 12-1 外部网络流量功能

显现目前系统外部网络接口 1/2 或所有外部网络接口 流量统计图。

- 时间：检视分别以分、时、日为时间单位的流量统计。

若欲使用【流量统计】，系统管理员须先至【接口地址】功能设定中，激活并设定所要统计流量的【外部网络接口】。

检视外部网络流量

步驟1. 在【流量统计】窗口中，找到欲检视的外部网络接口名称，对应至右方【时间】栏：点选【分】，可检视以每分钟（min）为单位的流量统计图表；点选【时】，可检视以每小时(hour)为单位的流量统计图表；点选【日】，可检视以日（day）为单位的流量统计图表。

步驟2. 流量统计图表 ***（如图 12-2）***

- 纵坐标：网络流量（Kbytes/Sec）。
- 横坐标：时间（时/分）。
- 实时流量：显示目前实时的 下载/上传 流量(Kbytes/秒)。

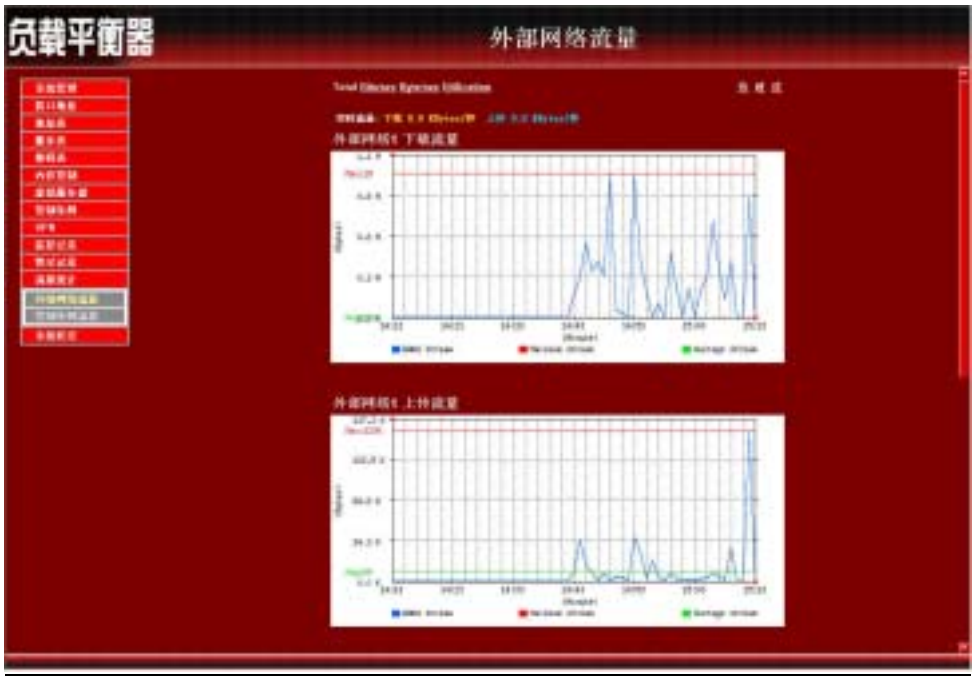


图 12-2 检视外部网络流量

管制条例流量功能

在左方菜单点选【流量统计】，再点选下方【管制条例流量】次功能选项。

本功能即为符合【管制条例】内设定的封包记录所产生该管制条例的统计资料 *(如图12-3)*

图 12-3 管制条例流量功能

管制条例流量统计窗口，表格内数值显现目前系统联机流量。

- 来源/目的 地址：来源/目的 端网络地址。
- 服务名称：服务项目名称。
- 管制动作：来源端网络地址、目的端网络地址进出负载平衡器资料封包的准许与拒绝动作。
- 时间：检视分别以分、时、日为时间单位的流量统计。

若欲使用【管制条例流量】，系统管理员须先至【管制条例】功能设定中，在指定的网络地址，激活【流量统计】功能。

检视管制条例流量

步骤1. 在【管制条例流量】窗口中，找到欲检视的网络区域名称，对应至右方【时间】栏：点选【分】，可检视以每分钟（min）为单位的流量统计图表；点选【时】，可检视以每小时(hour)为单位的流量统计图表；点选【日】，可检视以日（day）为单位的流量统计图表。

步骤2. 流量统计图表 ***（如图 12-4）***

- 纵坐标：网络流量（Kbytes/Sec）。
- 横坐标：时间（时/分）。
- 实时流量：显示目前实时的 下载/上传 流量(Kbytes/秒)。

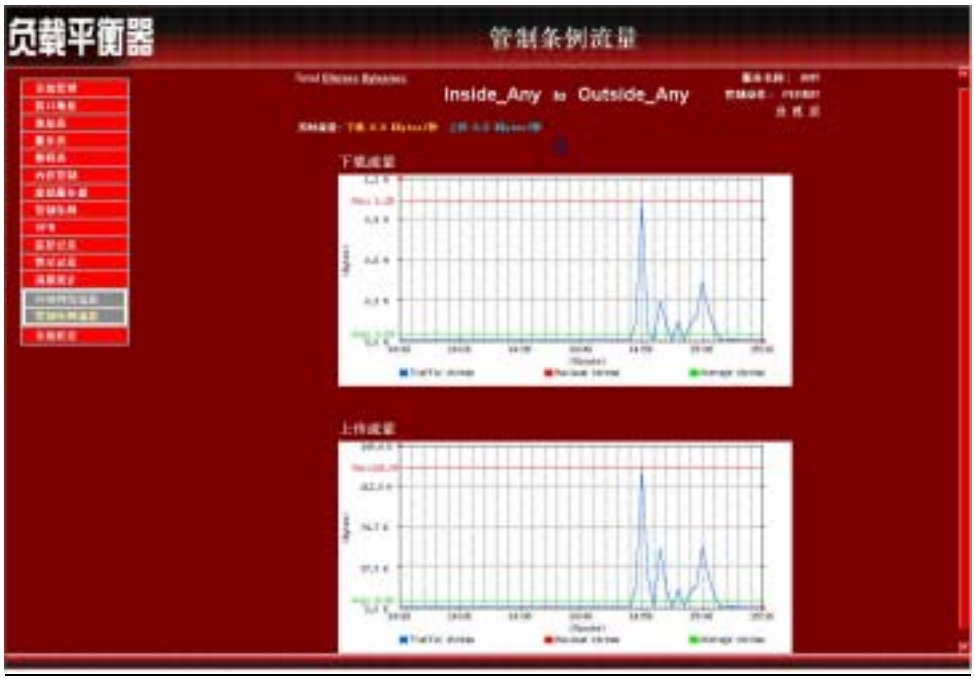


图 12-4 检视管制条例流量

第十三章

系 统 状 态

使用者可随时由系统状态中，得知目前网络联机，如局域网络与外部网络的 IP 地址、子网掩码、预设网关、DNS 服务器联机 IP 地址等各项信息。

（一）【接口地址】：目前网络服务器所设的接口地址信息。

（二）【ARP 表】：将 MAC 网卡地址转译为 IP 地址。

（三）【DHCP 用户表】：记录 DHCP 用户 IP 地址与 MAC 地址及其租约时间等信息。

接口状态功能

步驟1. 在左方的功能选项中，点选【系统状态】功能，再点选【接口状态】次功能选项。*（如图 13-1）*

图 13-1 接口状态功能

步驟2. 【接口状态】窗口内，显现目前系统联机之接口地址。

- 系统开机历时：负载平衡器开机历时时间。
- 系统模式：NAT / ADSL 拨接/固接 专线使用者或缆线调制解调器使用者
- 联机状态：显示联机或是断线
- 最大下载 / 上传频宽：显示目前外部网络所使用的最大 下载 / 上传 频宽。
- 流量下载分配比例：依照内部使用者对外部网络下载流量所占的分配比例(Byte)。
- 流量上传分配比例：依照内部使用者对外部网络上传流量所占的分配比例(Byte)。
- PPPoE 联机时间：显示 PPPoE 联机时间。

- MAC 地址：网络卡识别号码。
- IP 地址/子网掩码: 内/外部网络 IP 地址/内部网络子网掩码。
- 预设网关：显示外部通讯闸的地址。
- DNS 服务器 1：键入 ISP 所配发的 DNS 1 服务器地址。
- DNS 服务器 2：键入 ISP 所配发的 DNS 2 服务器地址。
- 接收封包数, 错误封包数：显示接收封包数,显示接收错误封包数。
- 传送封包数, 错误封包数：显示传送封包数,显示传送错误封包数。
- Ping, WebUI：

  显示 Ping 到负载平衡器外部网络接口地址功能使用状态,

  显示 WebUI 外部网络接口地址联机至负载平衡器功能使用状态,

ARP 表

步驟1. 在左方的功能选项中，点选【系统状态】功能，再点选【ARP 表】次功能选项。*（如图 13-2）*

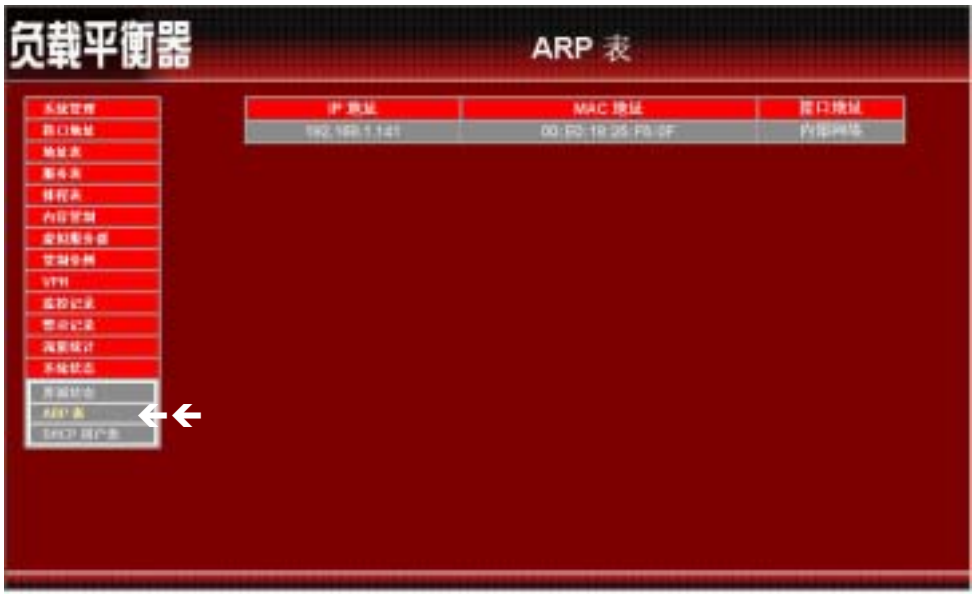


图 13-2 ARP 表

步驟2. 【ARP 表】工作窗口内表格名词定义：

- IP 地址 ： 内部网络 IP 地址。
- MAC 地址：网络卡识别号码。
- 接口地址：内/外部网络 IP 地址所属之接口地址。

DHCP 用户表

步驟1. 在左方的功能选项中，点选【系统状态】功能，再点选【DHCP 用户表】次功能选项。*（如图 13-3）*

图 13-3 DHCP 用户表

步驟2. 【DHCP 用户表】工作窗口内表格名词定义：

- IP 地址：动态 IP 地址。
- MAC 地址：连接动态 IP 地址的 MAC 地址。
- 租用时间：动态地址租用的(起始时间 / 结束时间)（年/月/日/时/分/秒）。

操 作 范 例

操作范例 1

以【管制条例】的制订流程为范例，让内部网络的所有 IP 地址都可以联机到网际网络。

步驟1. 在左方的功能选项中，点选【管制条例】功能，再点选【内部至外部】次功能选项。

步驟2. 在【内部至外部】窗口中，点选【新增】功能按钮。

步驟3. 在出现的【新增管制条例】窗口中，键入相关参数 *（如图 ex1-1）*

步驟4. 点选屏幕下方【确定】按钮，新增指定的内部网络。

图 ex1-1 新增内部至外部管制条例

操作范例 2

本范例让公司内部的 IP 地址只能连到 61.11.11.11 的网站的操作说明，制订流程为【地址表】至【管制条例】。

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【外部网络】次功能选项。

步驟2. 点选【新增】外部网络地址功能按钮。

步驟3. 在新窗口中，键入新外部网络各项参数值。 *（如图 ex2-1）*

步驟4. 点选屏幕下方【确定】按钮，新增指定外部网络。

图 ex2-1 新增外部网络地址

步驟5. 在左方的功能选项中，点选【管制条例】功能，再点选【内部至外部】次功能选项。

步驟6. 在【内部至外部】窗口中，点选【新增】功能按钮。

步驟7. 在出现的【新增管制条例】窗口中，键入相关参数*（如图ex2-2）*。

步驟8. 点选屏幕下方【确定】按钮，新增指定的内部网络。

图 ex2-2 新增内部至外部管制条例

步驟9. 开放所有的服务项目（ＡＮＹ），设定及完成。*（如图ex2-3）*

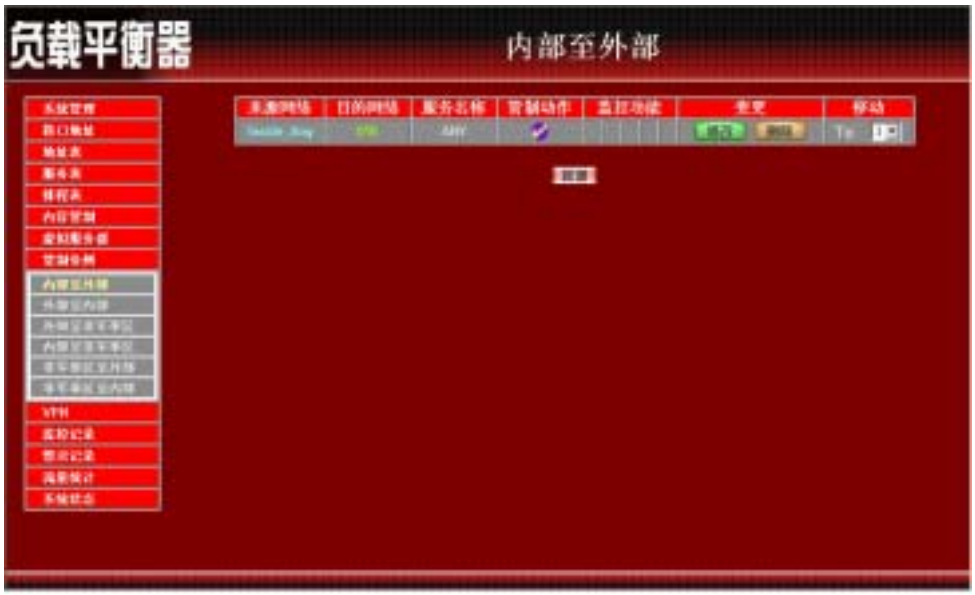


图 ex2-3 完成内部至外部管制条例

操作范例 3

本范例将以使用【ＩＰ对映】来制订【外部至内部】网络，达到将服务器架在公司内部(Internal 区)，现在要使外界的使用者，透过 IP 对应来使用服务器的功能。其制订流程为由【虚拟服务器】至【管制条例】。

步驟1. 在左方的功能选项中，点选【虚拟服务器】功能，再点选【IP 对映】次功能选项。

步驟2. 在 IP 对映窗口中，点选【新增】功能按钮。

步驟3. 在出现的新增 IP 对映窗口中，键入相关参数 ***(如图 ex3-1)***

步驟4. 点选屏幕下方【确定】按钮，新增指定的 IP 对映。

图 ex3-1　新增 IP 对映

步驟5. 出现以下画面，表示完成 IP 对映的设定。*(如图 ex3-2)*

图 ex3-2 新增 IP 对映

步驟6. 在左方的功能选项中，点选【管制条例】功能，再点选【外部至内部】次功能选项。 *(如图 ex3-3)*

步驟7. 在【外部至内部】窗口中，点选【新增】功能按钮。

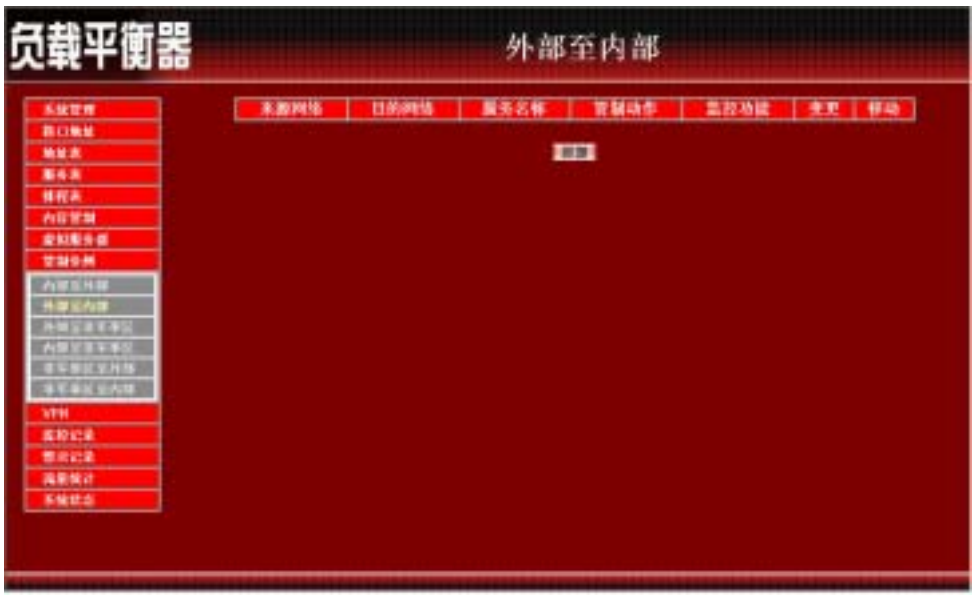


图 ex3-3 管制条例的外部至内部窗口

步驟8. 在出现的【新增管制条例】窗口中，键入相关参数后，点选【确定】执行新增群组。 *（如图 ex3-4）*

图 ex3-4 新增管制条例

步驟9. 开放所有的服务项目（ＡＮＹ），设定及完成。*（如图 ex3-5）*

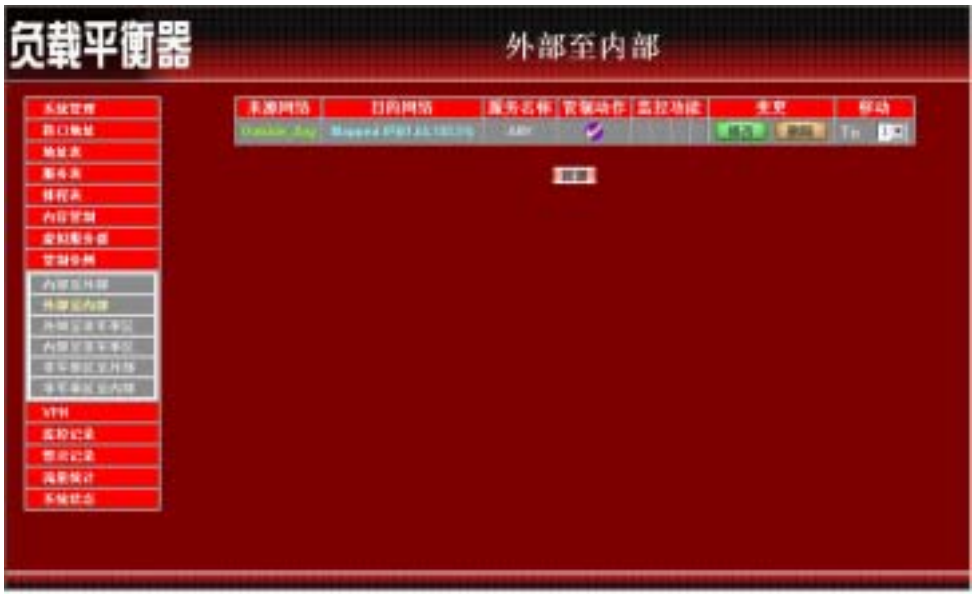


图 ex3-5 开放所有服务项目

操作范例 4

本范例将公司的服务器放在【非军事区网络】，开放给非军事区和外部所有ＩＰ地址使用，来制订【管制条例】。其制订流程为由【虚拟服务器】至【管制条例】。

步驟1. 在左方的功能选项中，点选【虚拟服务器】功能，再点选【虚拟服务器 1】次功能选项。进入【虚拟服务器 1】工作窗口。*(如图 ex4-1)*

步驟2. 点选屏幕上方的【选择】控制按钮。

图 ex4-1 进入虚拟服务器窗口

步驟3. 在【新增虚拟服务器 IP】窗口中，选择虚拟服务器 IP 地址后，点选下方【确定】按钮。*(如图ex4-2)*

图 ex4-2 新增虚拟服务器

步驟4. 新增虚拟服务器 IP 后，再接着点选屏幕下方的【新增】控制按钮。*(如图ex4-3)*

图 ex4-3 新增虚拟服务器服务设定

步驟5． 依照服务器所提供的服务项目，设定好各项参数后，按【确定】。*（如图 ex4-4）*

图 ex4-4　设定虚拟服务器

步驟6． 出现下列画面，即表示【虚拟服务器 1】部分设定完成。*（如图 ex4-5）*

图 ex4-5　完成虚拟服务器设定

步驟7.　再到【管制条例】里的【外部至内部】工作窗口。*（如图 ex4-7）*

步驟8.　点选屏幕下方的【新增】控制按钮。

图 ex4-7　进入管制条例之外部至非军事区窗口

步驟9.　在【新增管制条例】设定各项参数，完成后按【确定】。*（如图 ex4-8）*

图 ex4-8　新增管制条例

步驟10. 开放所有的服务项目（ＡＮＹ），设定及完成。*（如图 ex4-9）*

图 ex3-5　开放所有服务项目