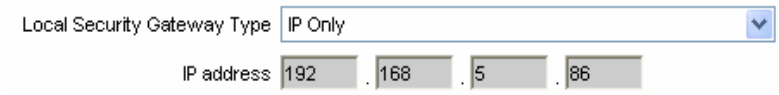
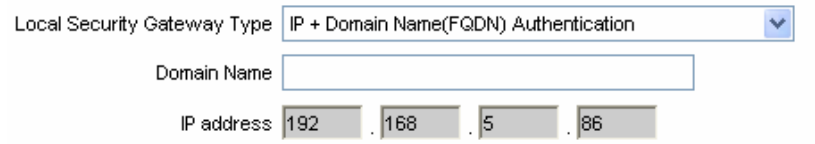
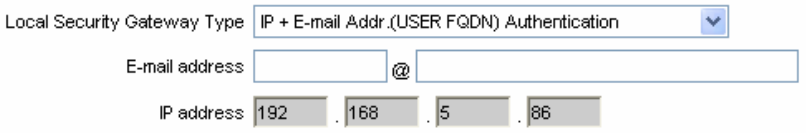
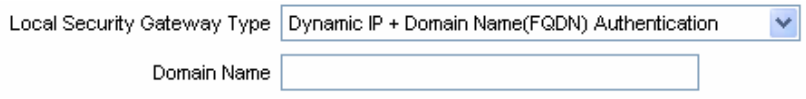
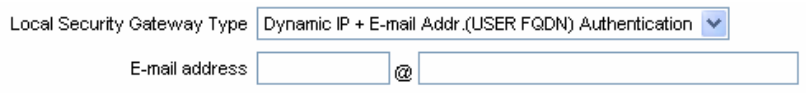
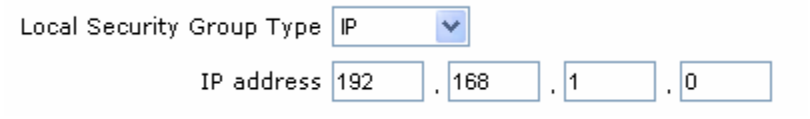
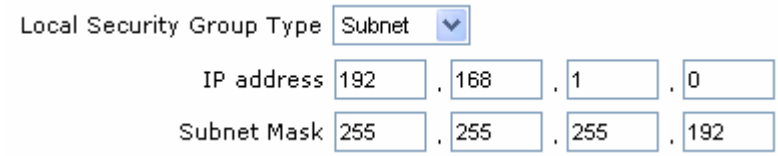
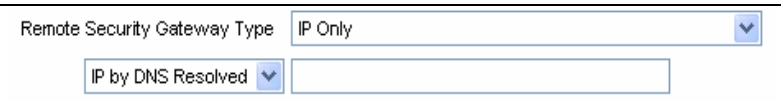
附文：传统 IPSec VPN 设置参数

隧道编号	当设定内建之 VPN 功能时，段选择要设定的 Tunnel 隧道编号。不同的服务器支持隧道数量不一。
隧道名称	设定此通道连接名称，如 XXX Office，若有一个以上的通道设定的话，务必将每一个通道名称都设为不同，以免混淆。 **Note：此通道名称若是需要连接其它 VPN 设备（非 VPN 网关）时，部分设备规定此通道名称须与主控端为相同名称并做验证，此通道才会顺利联机开启。**
启动:	勾选 Enable 选项，将此 VPN 信道开启。
Local Group Setup:	此项目的近端网关安全群组设定（ Local Security Gateway Type ）型态必须与连接远程的网关安全群组设定（ Remote Security Gateway Type）型态相同。
Local Security Gateway Type:	区域端群组设定，有五种操作方式项目选择，分别为: IP Only-只使用 IP 作为认证 IP + Domain Name（FQDN） Authentication，-IP+网域名称 IP + E-mail Addr. **（USER FQDN） Authentication，-IP+电子邮件** **Dynamic IP + Domain Name（FQDN） Authentication，-动态 IP 位置+网域名称** **Dynamic IP + E-mail Addr.（USER FQDN） Authentication.** 动态 IP 位置+电子邮件名称 此项目的近端网关安全群组设定（ Local Security Gateway Type ）型态必须与连接远程的远程连接远程的网关安全群组设定（ Remote Security Gateway Type）型态相同. **（1） IP Only: 若用户选择 IP Only 型态的话，只有固定填入此 IP 位置可以存取此信道，然后，VPN 网关的 WAN IP 位置将会自动填入此项目空格内，而不再需要进行额外设定.。**  **（2） IP + Domain Name（FQDN） Authentication:若选择 IP +网域名称型态，须输入所验证的网域名称以及 IP 位置，然后 VPN 网关的 WAN IP 位置将会自动填入此项目空格内，而不再需要进行额外设定。** FQDN 是指主机名称以及网域名称的结合，也必须存在于 Internet 上可以查询的到，如 vpn.server.com.此 IP 位置以及网域名称必须与

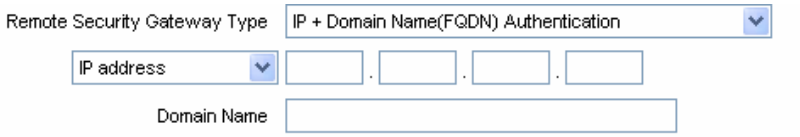
	远程的 VPN 安全网关器设定型态相同才可以正确连接。  **（3） IP + E-mail Addr。(USER FQDN) Authentication: 若选择 IP 位置加上电子邮件型态的，只有固定填入此 IP 位置以及电子邮件位置可以存取此信道，然后 VPN 网关的 WAN IP 位置将会自动填入此项目空格内，而不再需要进行额外设定。**  **（4） Dynamic IP + Domain Name（FQDN） Authentication: 若是使用动态 IP 位置连接 VPN 网关，就可以选择动态 IP 位置加上主机名称以及网域名称的结合。** 若使用动态 IP 位置连接 VPN 网关,就可以选择此型态连接 VPN，当远程的 VPN 网关要求与 VPN 网关作为 VPN 联机时，VPN 网关将会开始验证并反应此 VPN 通道联机；如选择此型态连接 VPN，就只须输入网域名称即可  **（5） Dynamic IP + E-mail Addr.（USER FQDN） Authentication: 若 是使用动态 IP 位置连接 VPN 网关， 就可以选择此型态连接 VPN，使用者不必输入 IP 位置，当远程的 VPN 网关要求与 VPN 网关作为 VPN 联机时， VPN 网关将会开始验证并反应此 VPN 通道联机。若可以选择此型态连接 VPN，就需要输入电子邮件认证到 E-Mail 位置空格字段中** 
Local Security Group Type	此为设定本地区域端的 VPN 联机安全群组设定，以下有几个关于本地区域端设定的项目，须选择并设置适当参数: IP Address **此项目为允许此 VPN 通道联机后，只有输入此 IP 位置的本地端计算机可以联机。**

	 以上的设定参考为:当此 VPN 通道联机后，于 192.168.1.0~255 的此网段的 IP 位置范围的计算机可以联机。 Subnet 此项目为允许此 VPN 通道联机后，每一台于此网段的本地端计算机都可以联机。  以上的设定参考为:当此 VPN 通道联机后，只有 192.168.1.0，子网掩码为 255.255.255.192 的此网段计算机可以与远程 VPN 联机
Remote Group Setup:远程安全群组设定:此项目的远程网关安全群组设定（ Remote Security Gateway Type)型态必须与连接远程的近端网关安全群组设定（ Local Security Gateway Type）型态相同. Remote Security Gateway Type:	远程安全群组设定，有五种操作方式项目选择，分别为: IP Only-只使用 IP 作为认证 IP + Domain Name（FQDN） Authentication，-IP+网域名称 IP + E-mail Addr.（USER FQDN） Authentication，-IP+电子邮件 Dynamic IP + Domain Name（FQDN） Authentication，-动态 IP 位置+网域名称 Dynamic IP + E-mail Addr.（USER FQDN） Authentication. 动态 IP 位置+电子邮件名称 此项目的远程网关安全群组设定（ RemoteLocal Security Gateway Type）型态必须与连接远程的近端的网关安全群组设定（ Local Remote Security Gateway Type）型态相同。 **（1） IP Only: 若选择 IP Only 型态的，只有固定填入此 IP 位置可以存取此信道，然后 VPN 网关的 WAN IP 位置将会自动填入此项目空格内，而不再需要进行额外设定。**  若是使用者不知道远程客户的 IP address，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP address。并且在设定完成后在 Summary 的远程网关下面显示出相对应的 IP address。

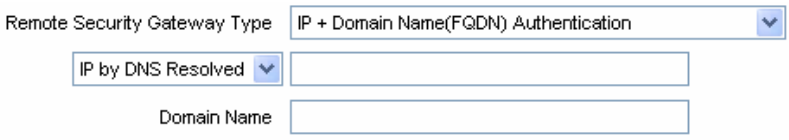


（2） IP + Domain Name（FQDN） Authentication:若选择 IP +网域名称型态的，需输入使用者所验证的网域名称以及 IP 位置，输入 IP 位置以及所验证的网域名称，然后 VPN 网关的 WAN IP 位置将会自动填入此项目空格内，而不再需要在进行额外设定。

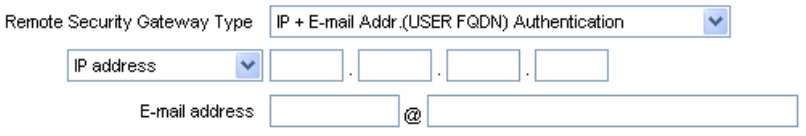
FQDN 是指主机名称以及网域名称的结合，使用者可以输入一个符合 FQDN 的网域名称即可。也必须存在于 Internet 上可以查询的到，如 vpn.server.com.此 IP 位置以及网域名称必须与远程的 VPN 安全网关器设定型态相同才可以正确连接。



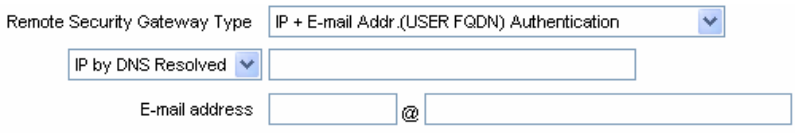
若是使用者不知道远程的 IP address，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP address。此网域名称必须存在 Internet 上可以查询的到。并且在设定完成后在 Summary 的远程网关下面自动显示出相对应的 IP address。

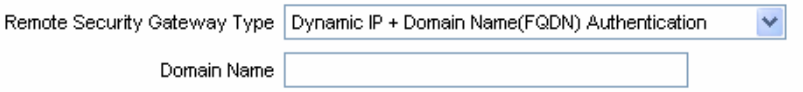
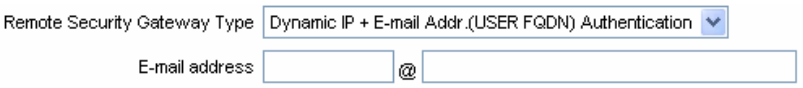
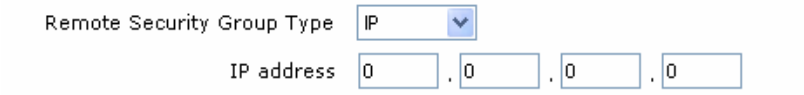
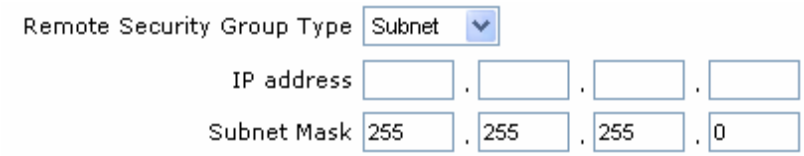


（3） IP + E-mail Addr.（USER FQDN） Authentication: 若选择 IP 位置加上电子邮件型态的，只有固定填入此 IP 位置以及电子邮件位置可以存取此信道，然后 VPN 网关的 WAN IP 位置将会自动填入此项目空格内，而不再需要进行额外设定。



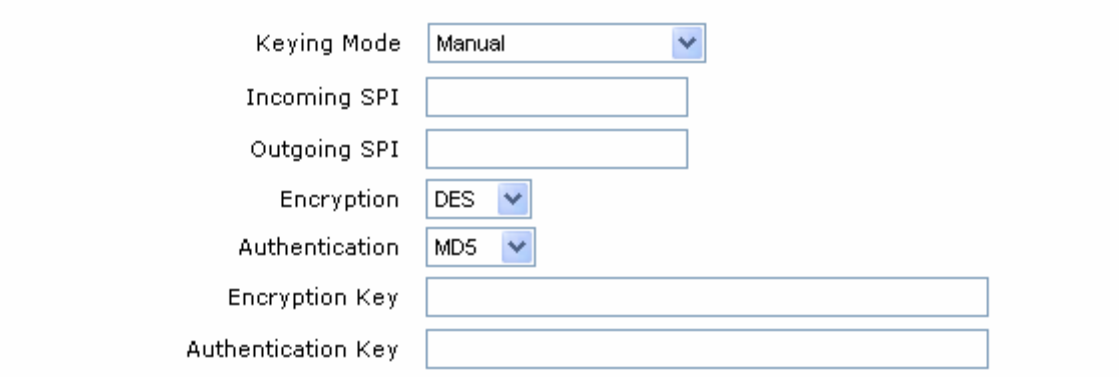
若是使用者不知道远程客户的 IP address，则可以通过网域名称转换 DNS Resolve 来将 DNS 转成 IP address。并且在设定完成后在 Summary 的远程网关下面显示出相对应的 IP address。

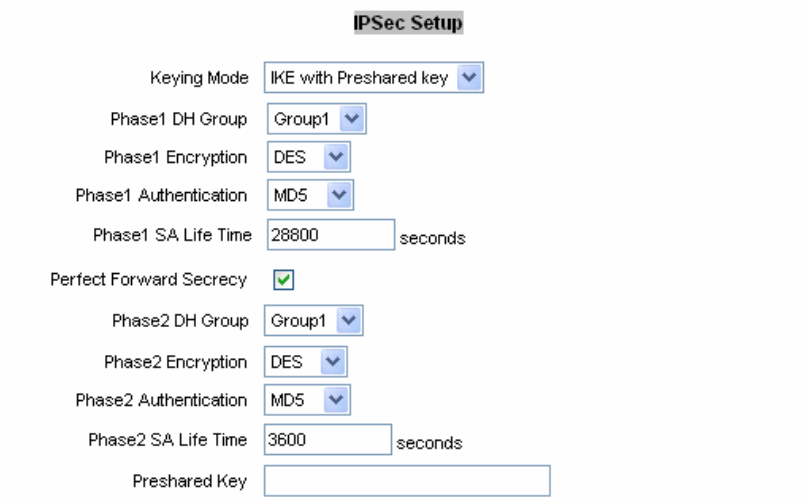


	（4） Dynamic IP + Domain Name（FQDN） Authentication: 若使用动态 IP 位置连接 VPN 网关，就可以选择动态 IP 位置加上主机名称以及网域名称的结合  （5） Dynamic IP + E-mail Addr. **（USER FQDN） Authentication: 若是使用动态 IP 位置连接 VPN 网关，则可以选择此型态连接 VPN，当远程的 VPN 网关要求与 VPN 网关作为 VPN 联机时， VPN 网关 将会开始验证并反应此 VPN 通道联机。输入电子邮件认证到 E-Mail 位置空格字段中** 
Remote Security Group Type:	此为设定本地区域端的 VPN 联机安全群组设定，以下是几个关于本地区域端设定的项目，须进行选择并设置适当参数: （1）IP Address 此项目为允许此 VPN 通道联机后，只有输入此 IP 位置的本地端计算机可以联机。  以上的设定参考为：当此 VPN 通道联机后，于 192.168.1.0~255 的此网段的 IP 位置范围的计算机可以联机。 （2）Subnet 此项目为允许此 VPN 通道联机后，每一台于此网段的本地端计算机都可以联机。  以上的设定参考为:当此 VPN 通道联机后，只有 192.168.1.0，子网掩码为 255.255.255.192 的此网段计算机可以与远程 VPN 联机

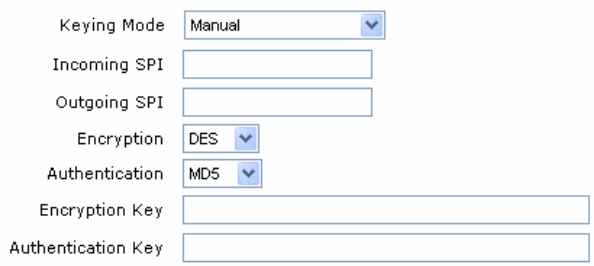
IPSec Setup

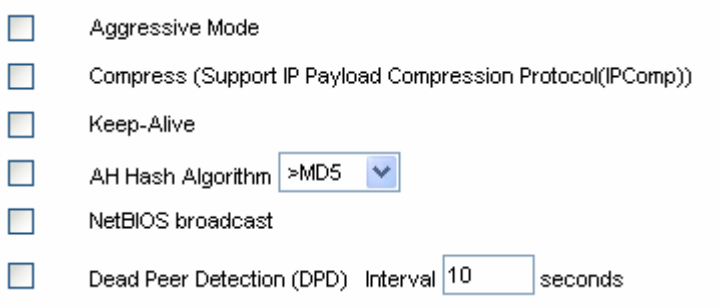
若是有任何加密机制存在，此两个 VPN 通道的加密机制必须要相同才可以将此通道连接，并于传输资料中加上标准的 IPSec 密钥，于此称为加密密钥 “key " 。 VPN 网关提供了以下二种加密管理方式 Key Management，分别为手动（Manual ） 以及 IKE 自动加密方式- IKE with Preshared Key （automatic），如下图所示：



Key Management:	此选项设定为当设定此 VPN 通道使用何种加密方式以及验证方式后，就必须设定一组交换密码，并注意，此参数必须与远程的交换密码参数相同;设定的方式有自动 Auto （IKE）或是手动 Manual.设定二种:于设定时选择其中一种设定方式即可!  **IKE with Preshared Key （automatic）:通过 IKE 产生共享的金钥来加密与验证远程的使用者。**若将 PFS（Perfect Forward Secrecy）启动后，会再第二阶段的 IKE 协调过程产生的第二把共同金钥做进一步加密与验证。当 PFS 启动后，通过 brute force

	来撷取金钥的黑客（hacker）无法在此短时间内，进一步得到第二把金钥。 Phase1/Phase2 DH Group: 于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5. Phase1/Phase2 Encryption: 此加密选项设定为设定此 VPN 通道使用何种加密方式，并须注意设置此参数必须与远程的加密参数相同: DES: 64-位加密方式 3DES:.128-位加密方式. Phase1/Phase2 Authentication: 此验证选项设定为设定此 VPN 通道使用何种验证方式，并须注意设置此参数必须与远程的验证方式参数相同: “MD5 " / “SHA " . Group: 于此选项可以选择采用 Diffie-Hellman 群组方式: Group1 或是 Group2/Group5.. Phase1 SA Lifetime 设定为此交换密码的有效时间，系统默认值为 28800 秒（8 小时），于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全. Phase2 SA Lifetime 设定为此交换密码的有效时间，系统默认值为 3600 秒（1 小时），于此有效时间内的 VPN 联机，系统会自动的将于有效时间后，自动的生成其它的交换密码以确保安全

	Preshared Key:于 Auto （IKE)， 选项中，使用者必须输入一组交换密码于 “Pre-shared Key " 的字段元中，在此的范例设定为 test，可以输入数字或是文字的交换密码，系统将会自动的将输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制：此数字或是文字的交换密码最高可输入 23 个文字组合。 Manual-手动方式  若选择手动方式 Manual 的话，此项可提供自订加密密钥，而此密钥不需经过任何交握（ negotiation）. Manual 为手动方式设定交换密码，于此分成加密密码“Encryption KEY”以及验证密码“Authentication KEY”二种，可以输入数字或是文字的交换密码，系统将会自动的将所输入的数字或是文字的交换密码自动转成 VPN 信道连接时的交换密码与验证机制：此数字或是文字的交换密码最高可输入 23 个文字组合。 另外还需要设定“Inbound SPI " 的交换字符串以及“Outbound SPI " 交换字符串，此字符串必须与远程 VPN 设备连接时相同;于此的 Inbound SPI 设定参数，使用者必须在远程的 VPN 设备的 Outbound SPI 设定相同字符串，而于本地端的 Outbound SPI 设定字符串，也必须与在远程的 VPN 设备的 Inbound SPI 设定

	相同字符串!
Advanced(进阶作业方式)-只供给使用自动交换密钥方式使用（IKE Preshareed Key Only） **Advanced settings are only for IKE with Preshared Key mode of IPSec.**	**Advance Mode:（进阶作业方式）**  在 VPN 网关 的进阶设定项目中，分别有主要模式 **Main Mode** 以及 进阶模式 **Aggressive Mode**，Main mode 是 VPN 网关的预设 VPN 作业模式而且与大多数的其它 VPN 设备使用连接方式为相同；另外 Aggressive mode 大多为远程的设备采用，如使用动态 IP 连接时，正是为了加强其安全控管的机制。 Compress: **若选择此项目勾选，则连接的 VPN 通道中 VPN 网关 支持 IP 表头型态的压缩（IP Payload compression Protocol）。** Keep-Alive： **若选择此项目勾选，则连接的 VPN 通道中会持续保持此条 VPN 连接不会中断，此使用多为分公司远程节点对总部的连接使用，或是无固定 IP 位置的远程使用.** AH Hash Algorithm: AH （Authentication Header） 验证表头封包格式，可选择 MD5/DSHA-1 NetBIOS Broadcast: **若选择此项目勾选，则连接的 VPN 通道中会让 NetBIOS 广播封包通过，**有助于微软的系统网络芳邻等连接容易，但是相对的占

	用此 VPN 通道的流量就会加大! Dead Peer Detection（DPD）: 若选择此项目勾选，则连接的 VPN 通道中会定期的传送 HELLO/ACK 信息封包来侦测是否 VPN 通道的两端仍有联机存在. 当有一端断线则 VPN 网关会自动断线，然后再建立新联机.使用 者可以选择每一次 DPD 信息封包传递的时间，默认值为 10 秒.