

第 11 章

VPN和远端接入设置

12.1 介绍

VPN即虚拟专用网，是通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。通常，VPN是对企业内部网的扩展，通过它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

有两种类型的VPN连接：远端用户拨入VPN连接和LAN-to-LAN VPN连接。“远端用户拨入VPN”允许一个远端接入节点，一台NAT路由器或一台单一的用户电脑通过Internet建立VPN隧道到Vigor路由器，从而能够访问VPN路由器后面的网络资源。如图 1 所示。“LAN-to-LAN VPN连接”可将两个独立的局域网连接起来，为共享双方的网络资源提供了一种解决方案。譬如，总公司网络可以访问分支办公室的网络，反之亦然。如图 2 所示。

VPN and Remote Access Setup

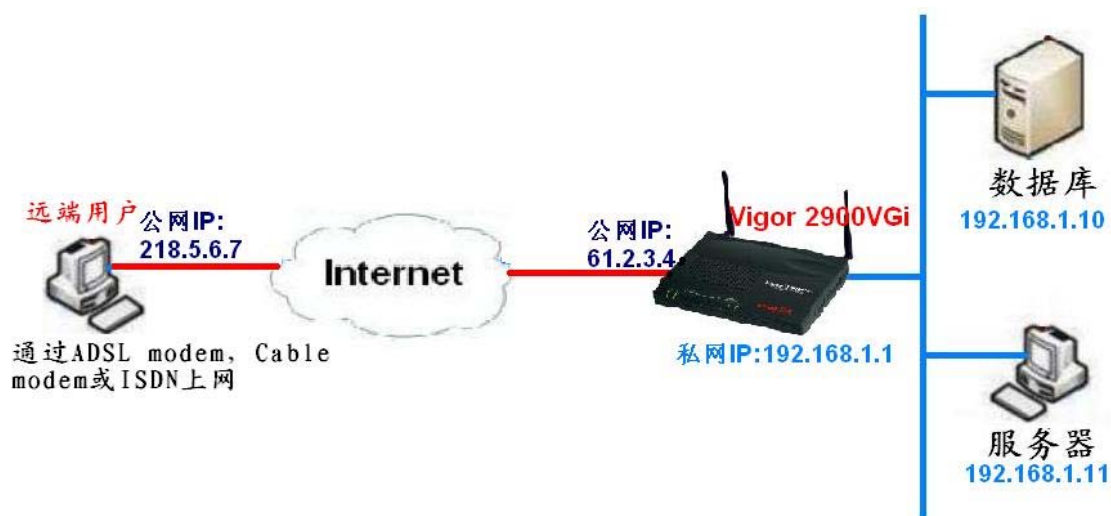


图 1. 远端用户拨入VPN连接

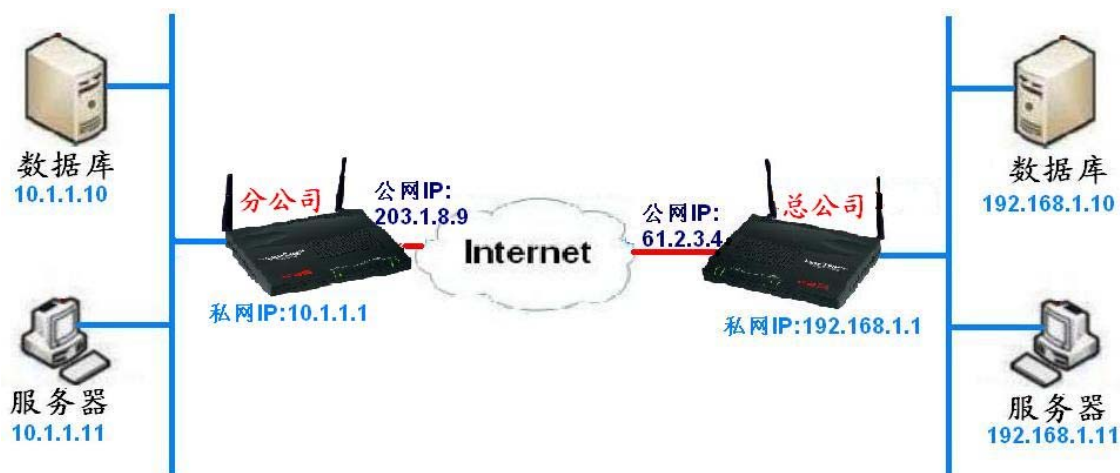


图 2. LAN-to-LAN VPN连接

Vigor路由器使用的VPN技术支持Internet工业标准，为用户提供了丰富的VPN解决方案。譬如Internet安全协议（Internet Protocol Security, IPSec），点到点隧道协议（Point to Point Tunneling Protocol, PPTP），第二层隧道协议（Layer Two Tunneling Protocol, L2TP）。

本章将介绍Vigor路由器的VPN工具的功能和设置。在Vigor路由器的主配置界面下，请使用以下链接访问“VPN与远程接入设定”页面。

高级设定 > VPN与远程接入



在“VPN与远程接入设定”页面里有五个主要的功能，如下图所示。你可以根据需要设置这些功能。



远端接入控制功能设定：该功能允许你启用或关闭特定的VPN服务（IPSec，PPTP，L2TP）。默认设置是所有VPN服务都已启用。如果你想要路由器提供VPN pass-through功能，必须在该页面关闭相应的VPN服务。譬如，如果你不想使用Vigor路由器本身提供的PPTP服务器，而是要在Vigor路由器后面连一台PPTP服务器（譬如Windows 2000 Server），你就必须将PPTP服务关闭。

VPN and Remote Access Setup

PPP一般设定：该页面的设置仅与PPP相关的VPN连接有关，包括PPTP，L2TP和L2TP over IPsec。你可以为这些PPP相关的VPN连接设置一些PPP协商阶段的参数，譬如PPP认证方式和分配给拨入VPN的IP范围。

VPN IKE / IPsec一般设定：该页面的设置仅与IPsec相关的VPN连接有关，包括IPsec和L2TP over IPsec。你可以为这些IPsec相关的VPN连接设置一个公用的预共享密钥（Pre-shared key）以及安全方法。这些设定用于远端拨入用户或拨入节点（LAN-to-LAN），通常他们都使用动态IP地址。

设置远端拨入用户设定档：该页面设置远端拨入用户的帐号。应用拓扑如图 1 所示。Vigor路由器支持四种类型的VPN拨入方式：PPTP，L2TP，IPsec和L2TP over IPsec。可使用Vigor提供的VPN工具或其它厂商提供的VPN工具（包括Windows内建的VPN工具）从单机建立VPN连接到Vigor路由器。

设置LAN-to-LAN设定档：该页面设置LAN-to-LAN VPN设定档。Vigor路由器支持四种类型的LAN-to-LAN VPN方式：PPTP，L2TP，IPsec和L2TP over IPsec。你可以同时建立总共 32 条VPN隧道，包括LAN-to-LAN VPN连接和远端拨入用户VPN连接。

12.2 远端接入控制功能设定

如下图所示，默认情况下所有VPN服务都已启用。



如果你不想使用Vigor路由器提供的VPN服务器，而是要在Vigor路由器后面连一台VPN服务器（如图 3 所示），你必须禁用相关的VPN服务（将该服务前面的勾去掉），并做相关的NAT设定，以便路由器能正确处理相关的数据包。具体设置如下：

PPTP：禁用PPTP服务，打开TCP 1723 到VPN服务器

L2TP：禁用L2TP服务，打开UDP 1701 到VPN服务器

IPSec：禁用IPSec服务，打开UDP 500 到VPN服务器

关于如何打开端口，请参考第 8 章“NAT设置”。

你也可以访问<http://www.draytek.com.cn> 并查看 技术支持 -> 常见问题 -> VPN问题 -> 如何设定VPN Pass-through



图 3. 在Vigor 2900V上设置VPN pass-through

12.3 PPP一般设定

该页面的设置仅与PPP相关的VPN连接有关，包括PPTP，L2TP和L2TP over IPsec。并且，该设定仅对远端拨入用户VPN或拨入的LAN-to-LAN VPN有效，若Vigor路由器拨出LAN-to-LAN VPN到远端VPN路由器，那么相关的PPP设定是在 **LAN-to-LAN设定档** 里设置的。下面介绍各选项含义：

高级设定 > PPP一般设定

PPP一般设定

PPP/MP协议	
拨入ppp验证	PAP或CHAP
拨入ppp加密 (MPPE)	可选MPPE
相互验证 (PAP)	<input type="radio"/> 是 <input checked="" type="radio"/> 否
用户名	
密码	

分配IP给拨入用户

起始IP地址: 192.168.1.200

OK

Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

PPP/MP协议

拨入PPP验证:

仅 PAP: 若选择该设置, 那么在VPN建立的PPP协商阶段, 将固定只使用PAP协议认证远端拨入用户或拨入的LAN-to-LAN连接。

PAP 或 CHAP: 若选择该设置, 那么在VPN建立的PPP协商阶段, Vigor路由器将接受远端拨入用户或拨入的LAN-to-LAN VPN使用以下任意一种验证协议: MS-CHAPv2, MS-CHAPv1, CHAP, PAP。并且Vigor路由器总是先提议对方使用MS-CHAPv2。

拨入PPP加密 (MPPE):

可选MPPE: 若选择该设置, 那么MPPE加密是可选的。如果远端拨入用户或拨入的LAN-to-LAN VPN不支持MPPE加密算法, 那么Vigor路由器将不加密VPN数据, 否则Vigor路由器将用相应的MPPE加密算法加密VPN数据。

要求 MPPE (40/128bits): 若选择该设置, 那么拨入端 (远端拨入用户或拨入的 LAN-to-LAN VPN) 必须使用 MPPE 加密算法, 或者 MPPE 40-bit, 或者 MPPE 128-bit。若拨入端同时提议这两个算法, Vigor 路由器将首选 MPPE 128-bit。

MPPE 最大值: 若选择该设置, 那么 Vigor 路由器将只接受拨入端 (远端拨入用户或拨入的 LAN-to-LAN VPN) 使用最大强度的 MPPE 加密算法 (MPPE 128-bit)。

相互验证(PAP): 有些路由器 (譬如Cisco) 支持相互验证 (Mutual Authentication) 功能, 建立VPN的时候需要两个方向上的验证, 可以提供更强的安全性。默认情况下该功能是关闭的。注意, 如果你启用了该功能, 就必须正确输入用于验证的用户名和密码。

用户名：为相互验证输入用户名。

密码：为相互验证输入密码。

分配IP给拨入用户

起始IP地址：该起始IP地址规定了一个IP范围，用于VPN建立的PPP协商阶段分配IP给拨入端（远端拨入用户或拨入的LAN-to-LAN VPN），它必须在本地私网范围里。譬如，如果本地私网范围是192.168.1.0/255.255.255.0，那么起始IP地址就必须是192.168.1.1～192.168.1.254中的一个。

12.4 VPN IPSec / IKE一般设定

该页面的设置仅与IPSec相关的VPN连接有关，包括IPSec和L2TP over IPSec。你可以为这些IPSec相关的VPN连接设置一个公用的预共享密钥（Pre-shared key）以及安全方法（Phase 2 协商阶段）。这些设定用于远端拨入用户或拨入的LAN-to-LAN VPN。通常他们都使用动态IP地址。

在后面的介绍里，你将发现在“**远端拨入用户设定档**”和“**LAN-to-LAN VPN设定档**”里，你都可以为相应的设定档单独配置IPSec拨入设定（包括预共享密钥和安全方法）。如果你没有为那些设定档专门配置拨入设定，它们将使用“**VPN IPSec/IKE一般设定**”里的设置。

高级设定 > VPN与远程接入 > VPN IKE / IPSec一般设定

VPN IKE / IPSec一般设定

远程拨入用户及动态IP客户的拨入设定(LAN to LAN)。

IKE认证方法

预共享密钥

重新键入预共享密钥

IPSec安全方法

☒ 中级 (AH)
会对数据进行认证，但不会加密。

高级 (ESP) ☒ DES ☒ 3DES ☒ AES
会对数据进行认证及加密。

Cancel OK

Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

IKE认证方法：目前Vigor 2900V仅支持预共享密钥(Pre-Shared Key)方式的隧道认证方式。不支持公钥证书(PKIs)方式。

预共享密钥：输入密钥。

重新键入预共享密钥：输入相同的密钥，确认输入正确。

IPSec安全方法：选择允许的IPSec安全方法。**注意：**该设定仅用于IPSec Phase 2 阶段的协商。


中级 (AH)：数据将被认证，但不会被加密。默认该选项被启用。

高级 (ESP)：数据将被认证和加密。这里我们支持DES，3DES和AES加密方式。默认所有选项都被启用。

12.5 为远端拨入用户设定帐号

在完成以上三个基本设定后，你可以在这里为远端拨入用户设置相应的设定档。Vigor 2900VG为远端拨入用户提供了 32 个接入帐号。此外，你也可以使用RADIUS服务器来扩充用户帐号的个数，因为Vigor 2900VG本身也支持RADIUS客户端功能。下图显示了“设置远端拨入用户设定档”的主界面。



(Set to Factory Default): 将鼠标移到右上栏箭头符号左边的图标，会出现一栏文字“Set to Factory Default”。点击该图标将清除所有的设定档。

用户: 这里显示的值是设定档里用户名栏里的设定。如果你在用户名栏里什么都没有输入，将显示默认的符号`???`。因为只有当VPN类型是PPTP, L2TP或L2TP over IPSec的时候才需要设定用户名栏，所以如果VPN类型是

IPSec, 用户将显示为???.当然你也可以在IPSec连接的设定档里键入一个用户名来标识此设定档, 并区分其它设定档, 它不会影响IPSec的正常建立。

状态: 显示该设定档是否被启用了。符号v表示设定档已经启用, 符号x表示 设定档已经禁用。

索引值: 要进入某个用户帐号配置页面必须点击相应的索引值号码。

以下分别介绍PPTP, L2TP, L2TP over IPSec和IPSec所需要的典型设置。这里远端拨入用户使用Draytek公司提供的VPN工具: Smart VPN Client 3.2.1。它可以在下面的链接下载到:

http://www.draytek.com.cn/support/ProductdownloadShow.php?router_id=73

连接拓扑如下图所示。



图 4. 远端拨入VPN应用拓扑

12.5.1 PPTP

A. Vigor 2900VG的VPN设定

确保在“远端接入控制功能设定”里PPTP服务已经启用。

“PPP一般设定”里建议使用默认设置。

点击进入“设置远端拨入用户设定档”页面，如下图所示，其中红色框出的部分是必须设置的，蓝色框出的部分是可选设定。具体解释如下：

高级设定 > VPN与远程接入 > 设置接入远端用户设定档

索引值编号1

用户帐号与验证

☒ 启用此帐号

闲置超时: 0 秒

允许的接入类型

☒ ISDN

☒ PPTP

☒ IPSec隧道

☒ L2TP with IPSec Policy: 无

☐ 指定远端节点

远端用户Ip或端点 (Peer) IDSN号码: []

或端点 (Peer) ID: []

用户名: draytek

密码: *****

IPSec安全方法

☒ 中级 (AH)

☒ 高级 (ESP)

☒ DES ☒ 3DES ☒ AES

本地ID: [] (选择性)

回拨功能

☐ 检查以启动回拨功能

☐ 指定回拨号码

回拨号码: []

☒ 启动回拨定额控制

回拨定额: 30 分钟

OK

用户帐号与验证

启用此帐号：只有勾选此设定，该设定档才会被启用。默认是禁用的。

闲置超时：如果没有任何数据传输通过这条建立好的VPN隧道超过“闲置超时”规定的时间，路由器将断掉该连接。默认设置是 300 秒，也就是说如果有个远端用户使用该设定档建立了一条VPN连接，一旦超过

300 秒的时间没有任何数据通过该VPN隧道传输，VPN连接将被自动断开。如果你不想有此时间限制，请将该值设为 0 秒。

用户名：为该远端用户设置用户名。

密码：为该远端用户设置密码。

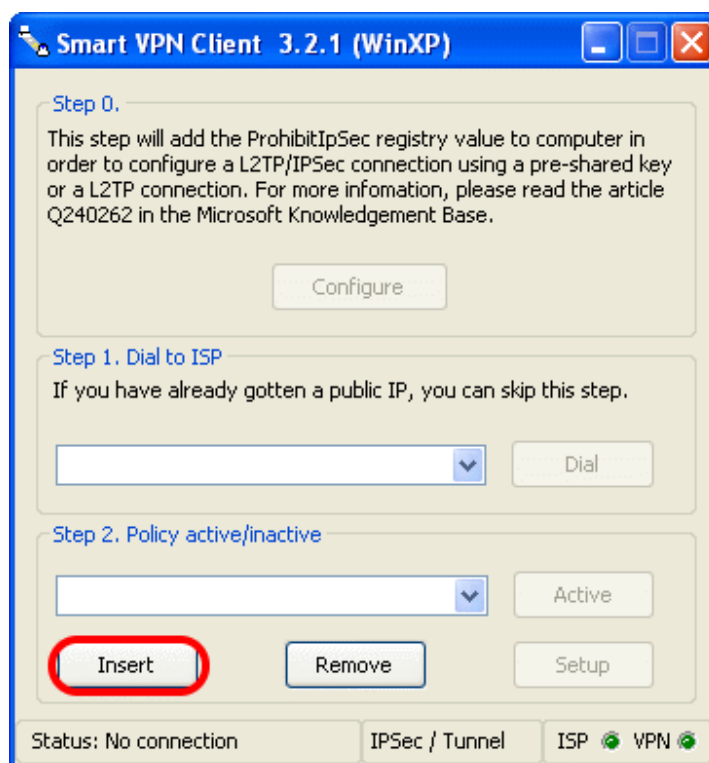
允许的拨入类型：确保PPTP被勾选。

指定远端节点：该选项是可选的。默认是禁用的，也就是说任何远端用户（特别是使用动态IP地址的用户）都可以使用此设定档的设置建立PPTP VPN到Vigor路由器。如果为了安全性需要限制特定的用户才能拨入VPN，你可以启用“指定远端节点”功能，并在“远端用户IP”栏里填入该特定用户的公网IP地址。这样，即使其他用户的PPTP设置都匹配此设定档，由于他们的公网IP地址不被允许拨入，他们也无法建立VPN连接。以图 4 为例，你可以在这里填入 218.5.6.7。

B. 远端用户的VPN设定（Smart VPN Client）

安装并打开Smart VPN Client 3.2.1，按“Insert”按钮新建一个设定档。此后，只要直接从上面的下拉菜单里选此帐号就能连接。

VPN and Remote Access Setup



在弹出窗口里完成以下设置：

Session Name: 为此策略输入任意一个名字。

VPN Server IP/Host Name: 输入VPN服务器的公网地址或动态域名。

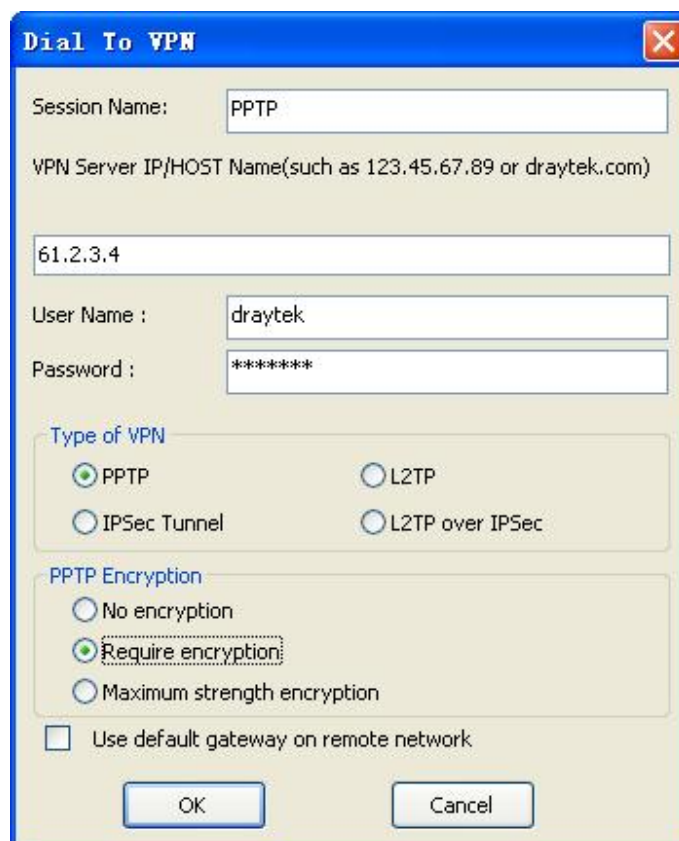
User Name/Password: 此帐号的用户名和密码，必须和Vigor路由器里的相关设定（用户帐号与验证栏里设置的用户名和密码）匹配。

Type of VPN: 选择VPN协议，这里选择PPTP。

PPTP Encryption: 为PPTP选择加密方式。No encryption（不加密），Require encryption（需要加密，但具体采用何种加密强度由服务器决定），Maximum strength encryption（强制采用MPPE 128bit）。

Use default gateway on remote network: 拨入VPN服务器后，使用VPN服务器的网关做为本机的默认网关。

设定完成后点OK。



The image shows a 'Dial To VPN' configuration window. It has a blue title bar with the text 'Dial To VPN' and a close button. The window contains several input fields and radio button options. The 'Session Name' field is set to 'PPTP'. The 'VPN Server IP/HOST Name' field is set to '61.2.3.4'. The 'User Name' field is set to 'draytek' and the 'Password' field is masked with '*****'. Under the 'Type of VPN' section, 'PPTP' is selected with a radio button. Other options include 'L2TP', 'IPSec Tunnel', and 'L2TP over IPSec'. Under the 'PPTP Encryption' section, 'Require encryption' is selected. At the bottom, there is a checkbox labeled 'Use default gateway on remote network' which is currently unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

Dial To VPN

Session Name: PPTP

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

61.2.3.4

User Name : draytek

Password : *****

Type of VPN

☒ PPTP ☐ L2TP

☐ IPSec Tunnel ☐ L2TP over IPSec

PPTP Encryption

☐ No encryption

☒ Require encryption

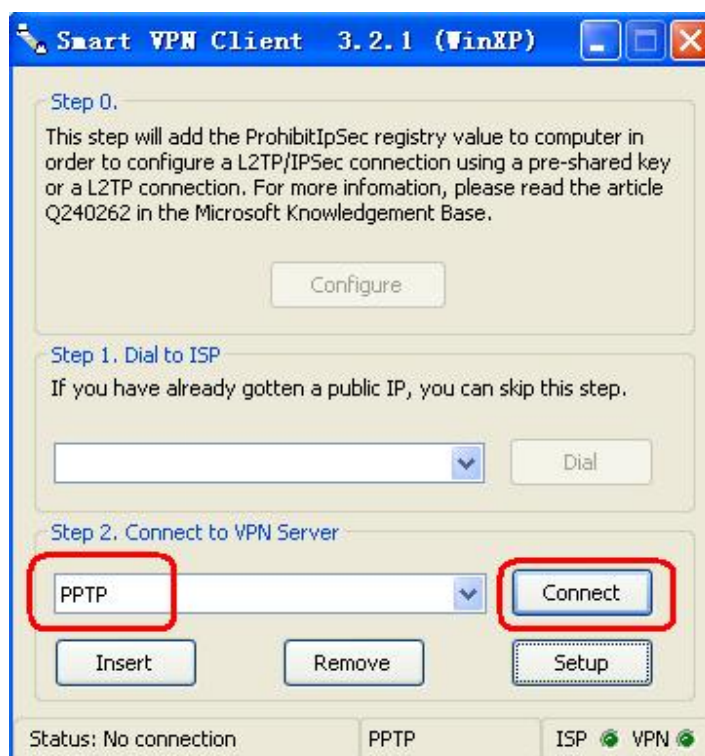
☐ Maximum strength encryption

☐ Use default gateway on remote network

OK Cancel

在下拉菜单里选择相应的策略，点Connect连接。

VPN and Remote Access Setup



12.5.2 L2TP

A. Vigor 2900VG的VPN设定

确保在“远端接入控制功能设定”里L2TP服务已经启用。

“PPP一般设定”里建议使用默认设置。

点击进入“设置远端拨入用户设定档”页面，如下图所示，其中红色框出的部分是必须设置的，蓝色框出的部分是可选设定。具体解释如下：

高级设定 > VPN与远程接入 > 设置拨入远端用户设定档

索引值编号 1

用户帐号与验证

☒ 启用此帐号

闲置超时: 0 秒

允许的拨入类型

☒ ISDN

☒ PPTP

☒ IPsec隧道

☒ L2TP with IPsec Policy 无

☐ 指定远端节点

远端用户IP或端点 (Peer) ISDN号码

或端点 (Peer) ID

用户名: draytek

密码: *****

IKE预设密钥

IPsec安全方法

☒ 中级 (AH)

高级 (ESP)

☒ DES ☒ 3DES ☒ AES

本地ID (选择性)

回拨功能

☐ 检查以启动回拨功能

☐ 指定回拨号码

回拨号码

☒ 启动回拨定额控制

回拨定额: 30 分钟

OK

用户帐号与验证

启用此帐号：只有勾选此设定，该设定档才会被启用。默认是禁用的。

闲置超时：如果没有任何数据传输通过这条建立好的VPN隧道超过“闲置超时”规定的时间，路由器将断掉该连接。默认设置是 300 秒，也就是说如果有个远端用户使用该设定档建立了一条VPN连接，一旦超过 300 秒的时间没有任何数据通过该VPN隧道传输，VPN连接将被自动断开。如果你不想有此时间限制，请将该值设为 0 秒。

用户名：为该远端用户设置用户名。

密码：为该远端用户设置密码。

允许的拨入类型：确保L2TP被勾选，并确保“with IPsec Policy”必须是无。

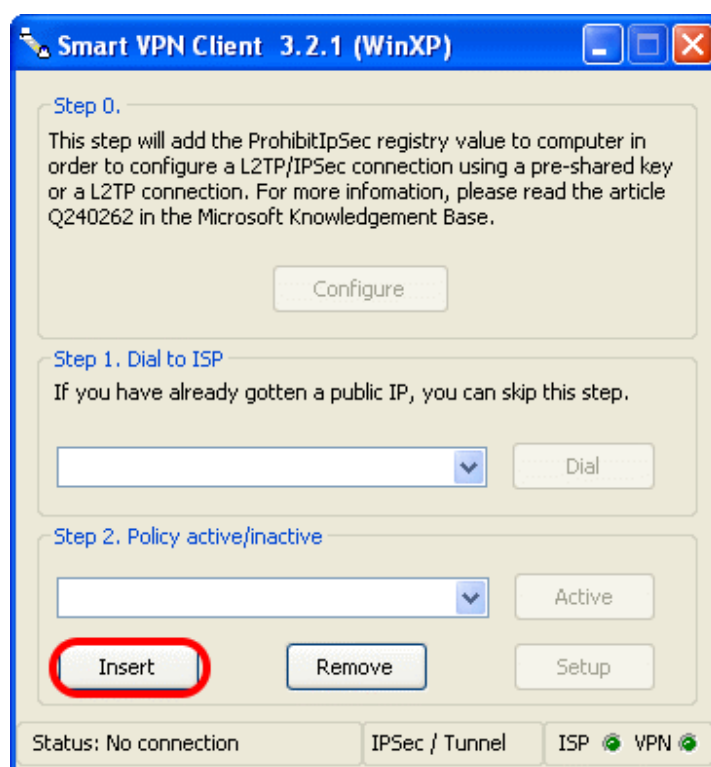
指定远端节点：该选项是可选的。默认是禁用的，也就是说任何远端用户（特

VPN and Remote Access Setup

别是使用动态IP地址的用户）都可以使用此设定档的设置建立L2TP VPN到Vigor路由器。如果为了安全性需要限制特定的用户才能拨入VPN，你可以启用“指定远端节点”功能，并在“远端用户IP”栏里填入该特定用户的公网IP地址。这样，即使其他用户的L2TP设置都匹配此设定档，由于他们的公网IP地址不被允许拨入，他们也无法建立VPN连接。以图4为例，你可以在这里填入218.5.6.7。

B. 远端用户的VPN设定（Smart VPN Client）

安装并打开Smart VPN Client 3.2.1，按“Insert”按钮新建一个设定档。此后，只要直接从上面的下拉菜单里选此帐号就能连接。



在弹出窗口里完成以下设置：

Session Name: 为此策略输入任意一个名字。

VPN Server IP/Host Name: 输入VPN服务器的公网地址或动态域名。

User Name/Password: 此帐号的用户名和密码，必须和Vigor路由器里的
相关设定（用户帐号与验证栏里设置的用户名和密码）匹配。

Type of VPN: 选择VPN协议，这里选择L2TP。

Use default gateway on remote network: 拨入VPN服务器后，使用
VPN服务器的网关做为本机的默认网关。

设定完成后点OK。

Dial To VPN

Session Name: L2TP

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

61.2.3.4

User Name : draytek

Password : *****

Type of VPN

☐ PPTP ☒ L2TP

☐ IPSec Tunnel ☐ L2TP over IPSec

PPTP Encryption

☒ No encryption

☐ Require encryption

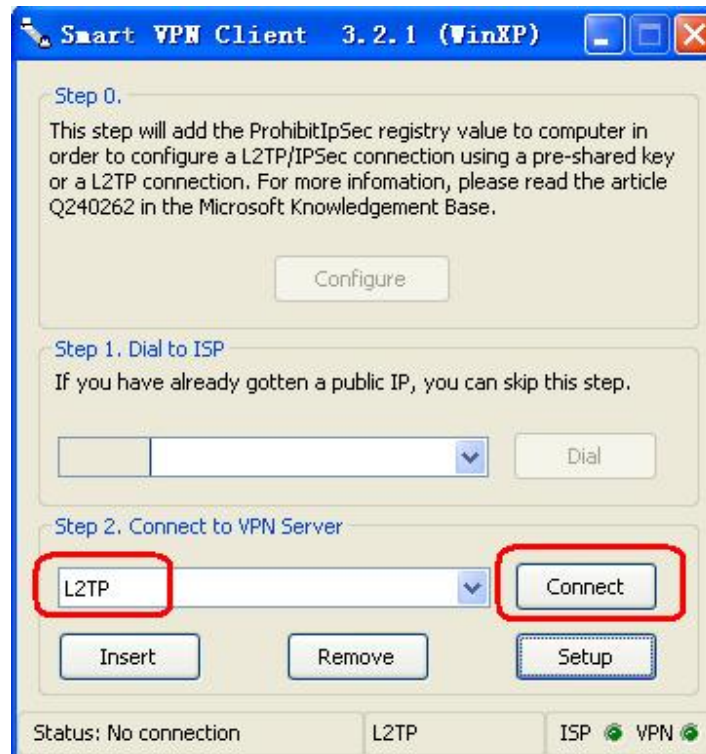
☐ Maximum strength encryption

☐ Use default gateway on remote network

OK Cancel

VPN and Remote Access Setup

在下拉菜单里选择相应的策略，点Connect连接。



12.5.3 IPSec (Main Mode)

A. Vigor 2900VG的VPN设定

确保在“远端接入控制功能设定”里IPSec服务已经启用。

在“VPN IPSec / IKE一般设定”里，必须正确输入两次预共享密钥。IPSec安全方法设置的是IPSec Phase 2 的协商参数，建议使用默认设置。

高级设定 > VPN与远程接入 > VPN IKE / IPSec一般设定

VPN IKE / IPSec一般设定

远程拨入用户及动态IP客户的拨入设定(LAN to LAN)。

IKE认证方法

预共享密钥

重新键入预共享密钥

IPSec安全方法

☒ 中级 (AH)
会对数据进行认证, 但不会加密。

高级 (ESP) ☒ DES ☒ 3DES ☒ AES
会对数据进行认证及加密。

Cancel OK

点击进入“设置远端拨入用户设定档”页面，如下图所示，其中红色框出的部分是必须设置的，蓝色框出的部分是可选设定。具体解释如下：

VPN and Remote Access Setup

高级设定 > VPN与远程接入 > 设置拨入远端用户设定档

索引值编号 1

用户帐号与验证 <input checked="" type="checkbox"/> 启用此帐号 闲置超时: 0 秒	用户名: ??? 密码: IKE预设密钥 IPSec安全方法 <input checked="" type="checkbox"/> 中级 (AH) 高级 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 本地ID: (选择性)
允许的拨入类型 <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec隧道 <input checked="" type="checkbox"/> L2TP with IPSec Policy 无 <input type="checkbox"/> 指定远端节点 远端用户IP或端点 (Peer) ISDN号码: 或端点 (Peer) ID:	回拨功能 <input type="checkbox"/> 检查以启动回拨功能 <input type="checkbox"/> 指定回拨号码 回拨号码: <input checked="" type="checkbox"/> 启动回拨定额控制 回拨定额: 30 分钟

OK

用户帐号与验证

启用此帐号：只有勾选此设定，该设定档才会被启用。默认是禁用的。

闲置超时：如果没有任何数据传输通过这条建立好的VPN隧道超过“闲置超时”规定的时间，路由器将断掉该连接。默认设置是 300 秒，也就是说如果有个远端用户使用该设定档建立了一条VPN连接，一旦超过 300 秒的时间没有任何数据通过该VPN隧道传输，VPN连接将被自动断开。如果你不想有此时间限制，请将该值设为 0 秒。

用户名：这项设置不会对IPSec连接建立产生任何影响，主要是为了使用一个特定的名称来区别其它设定档，而不是使用默认的符号???

允许的拨入类型：确保IPSec被勾选。

指定远端节点：该选项是可选的。默认是禁用的，也就是说任何远端用户（特

别是使用动态IP地址的用户）都可以使用此设定档的设置建立IPSec VPN到Vigor路由器，此时该设定档使用的**预共享密钥**和**IPSec安全方法**在“VPN IPSec / IKE一般设定”里设定。如果为了安全性需要限制特定的用户才能拨入VPN，你可以启用“指定远端节点”功能，并在“远端用户IP”栏里填入该特定用户的公网IP地址。这样，即使其他用户的IPSec设置都匹配此设定档，由于他们的公网IP地址不被允许拨入，他们也无法建立VPN连接。以图 4 为例，你可以在这里填入 218.5.6.7。

IKE预设密钥与IPSec安全方法：一旦启用了“指定远端节点”功能，就必须为此设定档单独配置**预共享密钥**和**IPSec安全方法**。这里的设定与“VPN IPSec / IKE一般设定”里的设置在功能上是一样的，只不过它被限定只能用于指定的用户。

注意：不要“设置端点（peer）ID”和“本地ID”。

B. 远端用户的VPN设定（Smart VPN Client）

安装并打开Smart VPN Client 3.2.1，按“Insert”按钮新建一个设定档。此后，只要直接从上面的下拉菜单里选此帐号就能连接。

VPN and Remote Access Setup



在弹出窗口里完成以下设置：

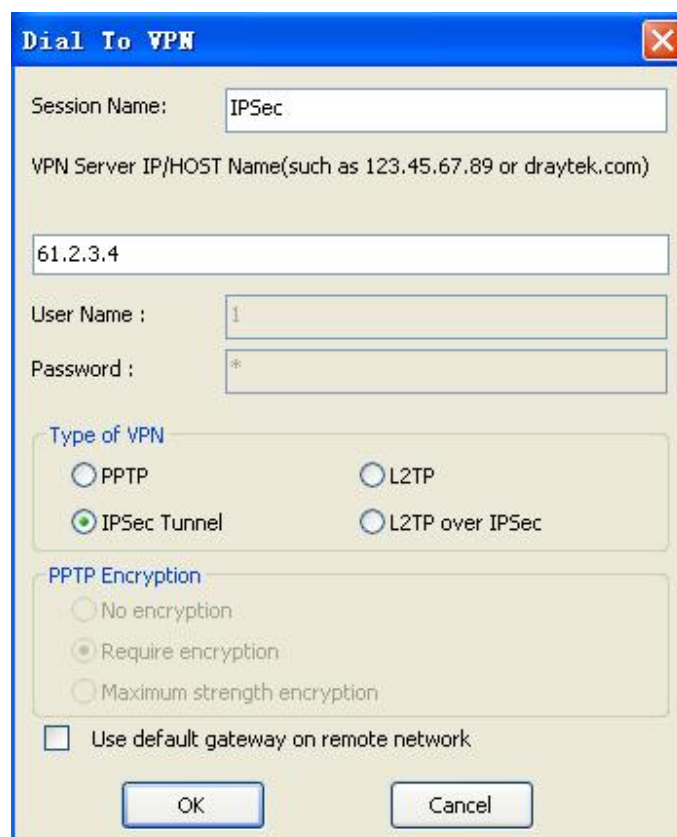
Session Name: 为此策略输入任意一个名字。

VPN Server IP/Host Name: 输入VPN服务器的公网地址或动态域名。

Type of VPN: 选择VPN协议，这里选择IPSec。

Use default gateway on remote network: 拨入VPN服务器后，使用VPN服务器的网关做为本机的默认网关。

设定完成后点OK。



The image shows a 'Dial To VPN' configuration window. It has a blue title bar with the text 'Dial To VPN' and a red close button. The window contains several input fields and radio button groups. The 'Session Name' field is set to 'IPSec'. The 'VPN Server IP/HOST Name' field is set to '61.2.3.4'. The 'User Name' field is set to '1' and the 'Password' field is masked with asterisks. Under the 'Type of VPN' section, 'IPSec Tunnel' is selected with a radio button. Under the 'PPTP Encryption' section, 'Require encryption' is selected. At the bottom, there is a checkbox for 'Use default gateway on remote network' which is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

Dial To VPN

Session Name: IPSec

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

61.2.3.4

User Name : 1

Password : *

Type of VPN

☐ PPTP ☐ L2TP

☒ IPSec Tunnel ☐ L2TP over IPSec

PPTP Encryption

☐ No encryption

☒ Require encryption

☐ Maximum strength encryption

☐ Use default gateway on remote network

OK Cancel

在弹出窗口里完成以下设置：

My IP: 如果你的电脑有多块网卡，选择用于连接VPN服务器的网卡的IP地址。（以图 4 为例，选择 218.5.6.7）

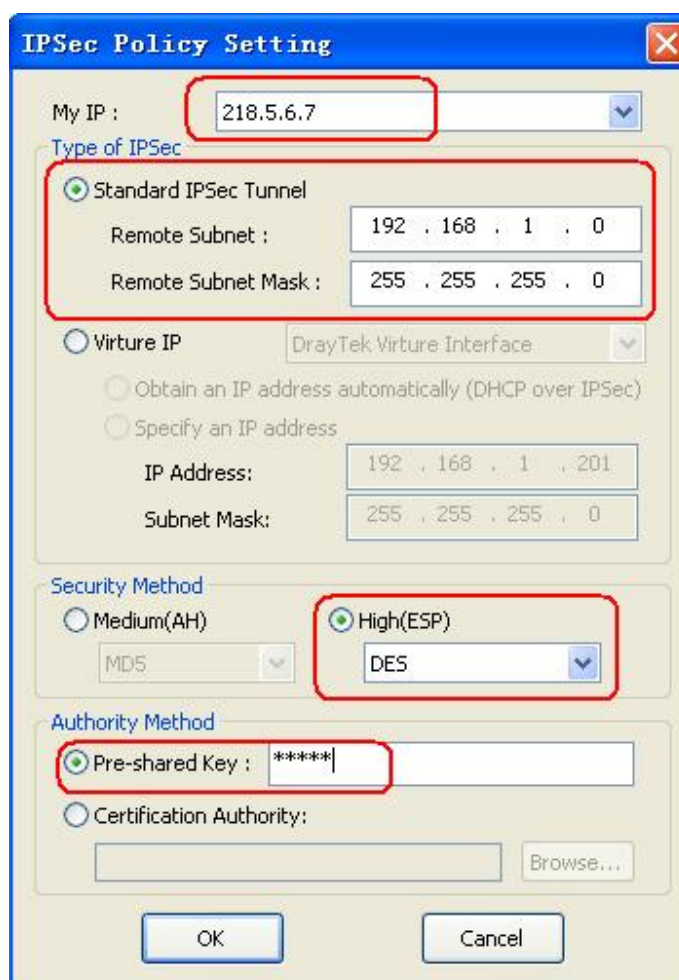
Type of IPSec: Standard IPSec Tunnel: 默认设置。在Remote Subnet和Remote Subnet Mask里分别填入VPN服务器的内部网段和子网掩码。（以图 4 为例，这里填入 192.168.1.0/255.255.255.0）

Virtual IP: 有些VPN服务器支持DHCP over IPSec技术，可以为IPSec拨入用户分配一个内部网段的IP地址。若无特殊应用需求，请不要选此方式。

VPN and Remote Access Setup

Security Method: 根据VPN服务器的设定选择AH或ESP。注意，如果VPN客户端在NAT后面，不能选择AH。

Authority Method: 根据VPN服务器的设定选择隧道认证协议。有预共享密钥（Pre-shared Key）和公钥证书两种方式。（以图 4 为例，选择Pre-shared Key。输入的密钥必须和VPN服务器里的预共享密钥设定相同。）



The image shows a screenshot of the 'IPSec Policy Setting' dialog box. The 'My IP' field is set to '218.5.6.7'. Under 'Type of IPSec', 'Standard IPSec Tunnel' is selected, with 'Remote Subnet' set to '192 . 168 . 1 . 0' and 'Remote Subnet Mask' set to '255 . 255 . 255 . 0'. Under 'Security Method', 'High(ESP)' is selected, and the encryption algorithm is set to 'DES'. Under 'Authority Method', 'Pre-shared Key' is selected, and the key is masked with '*****'. The 'OK' and 'Cancel' buttons are at the bottom.

在下拉菜单里选择相应的策略，点Active。



此时可观察左下角的连接状态。若状态显示为**Connected**，按钮变为**Inactive**。

VPN and Remote Access Setup



Ping Vigor的LAN IP来初始化连接。你会看到最初的回应是Negotiating IP Security。

```
D:\Documents and Settings\Administrator>ping 192.168.1.1 -t

Pinging 192.168.1.1 with 32 bytes of data:

Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
```

12.5.4 IPSec (Aggressive Mode)

A. Vigor 2900VG的VPN设定

确保在“远端接入控制功能设定”里IPSec服务已经启用。

点击进入“设置远端拨入用户设定档”页面，如下图所示，其中红色框出的部分是必须设置的，蓝色框出的部分是可选设定。具体解释如下：

用户帐号与验证

启用此帐号：只有勾选此设定，该设定档才会被启用。默认是禁用的。

闲置超时：如果没有任何数据传输通过这条建立好的VPN隧道超过“闲置超时”规定的时间，路由器将断掉该连接。默认设置是 300 秒，也就是说如果有个远端用户使用该设定档建立了一条VPN连接，一旦超过 300 秒的时间没有任何数据通过该VPN隧道传输，VPN连接将被自动

VPN and Remote Access Setup

断开。如果你不想有此时间限制，请将该值设为 0 秒。

用户名：这项设置不会对IPSec连接建立产生任何影响，主要是为了使用一个特定的名称来区别其它设定档，而不是使用默认的符号???

允许的拨入类型：确保IPSec被勾选。

指定远端节点：必须启用此功能，并在**端点（Peer）ID**栏里设置一个ID。ID的格式可以是Email地址或域名，不一定要实际存在的Email地址或域名。这个ID在远端用户的VPN客户端软件里也要输入，不同的VPN客户端软件对这个ID有不同的命名。这个ID是必须设置的，VPN建立的时候，客户端将发送此ID给VPN服务器进行认证。

IKE预设密钥与IPSec安全方法：一旦启用了“指定远端节点”功能，就必须为此设定档单独配置**预共享密钥**和**IPSec安全方法**。这里的设定与“VPN IPSec / IKE一般设定”里的设置在功能上是一样的，只不过它被限定只能用于指定的用户。

本地ID：这个ID是可选的，不一定要设置。如果VPN客户端支持认证VPN服务器的功能，可以设置此ID。VPN建立的时候，VPN服务器将发送此ID给客户端进行认证。ID的格式可以是Email地址或域名，不一定要实际存在的Email地址或域名。

B. 远端用户的VPN设定（TheGreenBow）

目前Smart VPN Client还不支持Aggressive mode，我们用TheGreenBow为例。

安装并打开TheGreenBow，鼠标右键点击Configuration新建一个Phase 1。

Name: 任意输入一个标识名。

Interface: 选择正确的网卡的IP地址。如果你使用动态IP地址（譬如ADSL拨号上网），可以选择星号（*）。

Remote Gateway: 填入VPN服务器的公网IP地址或域名。

Preshared Key: 输入预共享密钥。必须和VPN服务器里的设定相同。

IKE: 配置Phase 1 阶段协商的参数。这部分在Vigor路由器里没有提供配置界面。Vigor将接受以下参数的组合：

Encryption: DES / 3DES
Authentication: MD5 / SHA
Key Group: DH768(Group 1) / DH1024(Group 2)

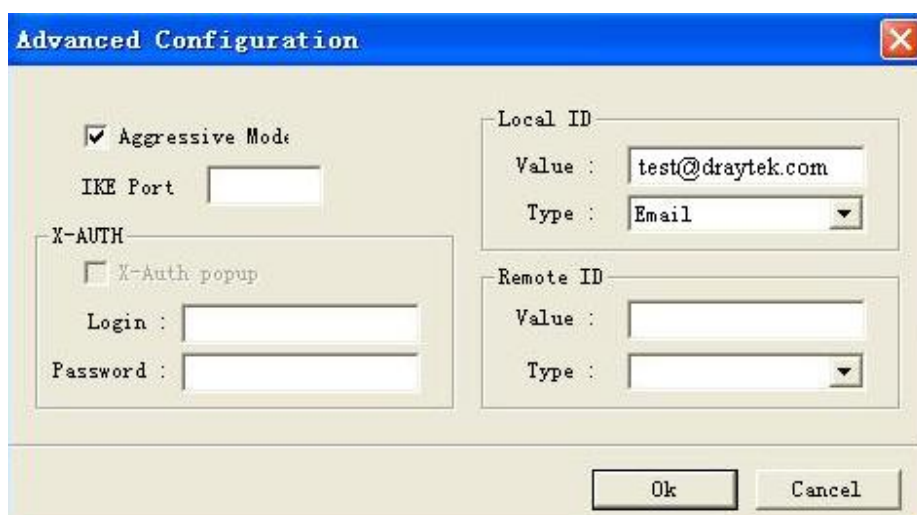
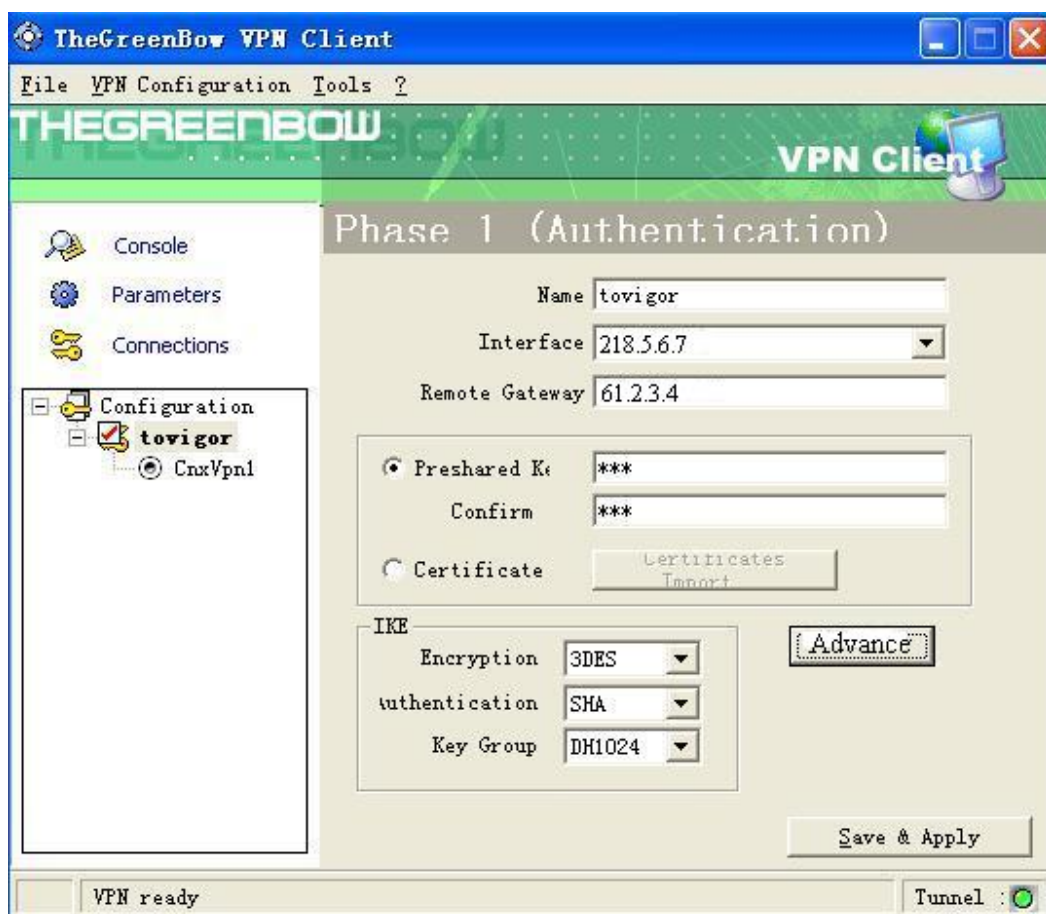
点击**Advance**按钮，在弹出窗口里继续完成以下设置：

Aggressive Mode: 勾选此选项，启用Aggressive mode。

Local ID: 这个ID的Value对应Vigor的端点（Peer）ID。Type可选择DNS或Email。

Remote ID: 这个ID的Value对应Vigor的本地ID，是可选的。Type可选择DNS或Email。

VPN and Remote Access Setup



设置完毕后点OK，再点Save & Apply。在左面的窗口里鼠标右击Phase 1 新建

一个Phase 2。

Name: 输入任意一个名称用于标识。

VPN Client address: 这里你可以输入任意一个IP地址，即使 0.0.0.0 也可以。

Address type, Remote LAN address, Subnet Mask: 选择 Subnet address并输入VPN服务器的内部网络和子网掩码。

ESP & PFS: 该设定对应Vigor的IPSec安全方法，但是IPSec安全方法只提供设置加密方式（Encryption）。Vigor将接受以下参数的组合：

Encryption: DES / 3DES / AES-128

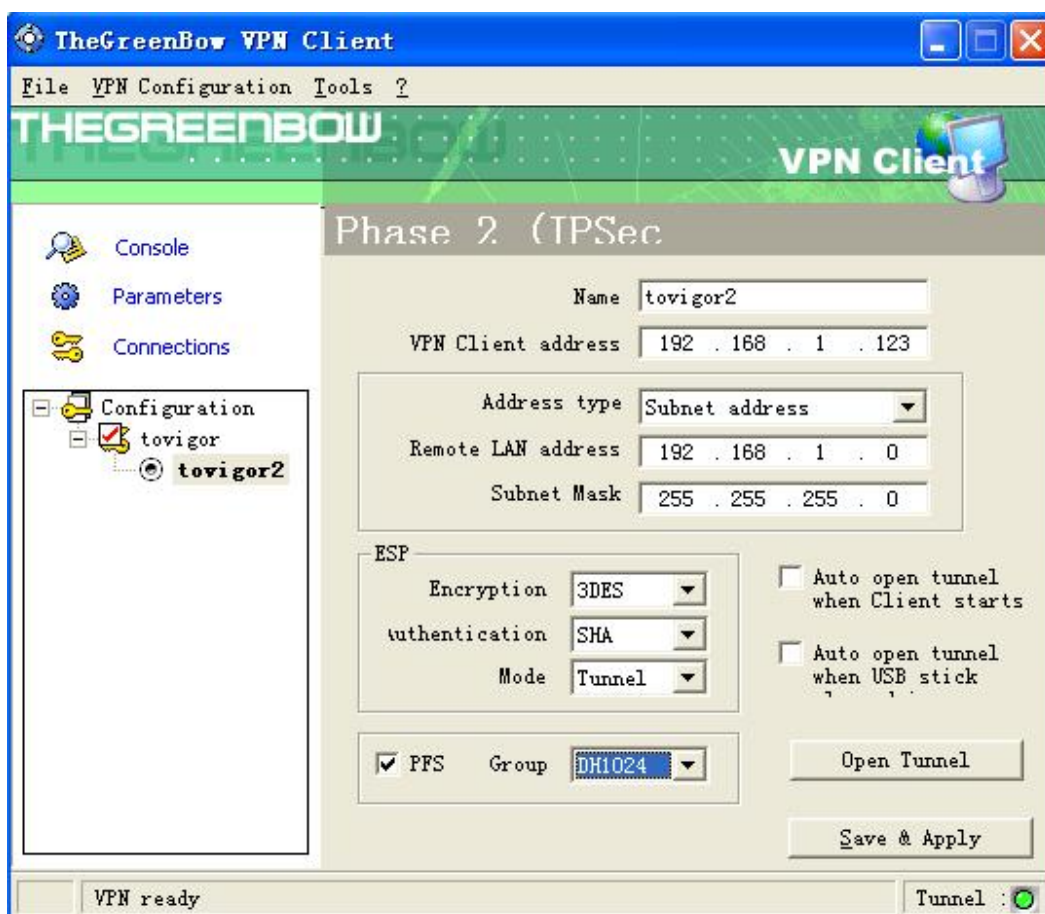
Authentication: MD5 / SHA

Mode: Tunnel

PFS Group: DH768(Group 1) / DH1024(Group 2)

完成设定后点 Save & Apply。然后点 Open Tunnel 按钮建立连接，或用 Ping 来触发连接。

VPN and Remote Access Setup

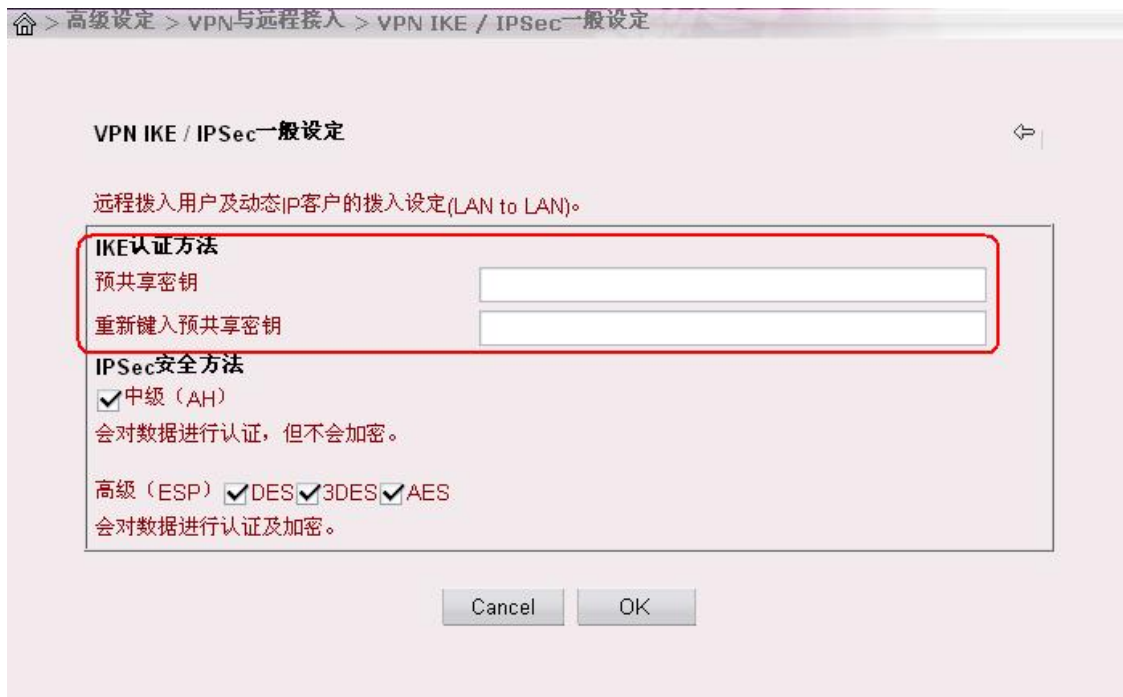


12.5.5 L2TP over IPSec

A. Vigor 2900VG的VPN设定

确保在“远端接入控制功能设定”里L2TP和IPSec服务已经启用。

在“VPN IPSec / IKE一般设定”里，必须正确输入两次预共享密钥。IPSec安全方法设置的是IPSec Phase 2 的协商参数，建议使用默认设置。



点击进入“设置远端拨入用户设定档”页面，如下图所示，其中红色框出的部分是必须设置的，蓝色框出的部分是可选设定。具体解释如下：

VPN and Remote Access Setup

高级设定 > VPN与远程接入 > 设置拨入远端用户设定档

索引值编号 1

用户帐号与验证

☒ 启用此帐号

闲置超时: 0 秒

允许的拨入类型

☒ ISDN
☒ PPTP
☒ IPsec隧道
☒ L2TP with IPsec Policy 最好能使用

☐ 指定远端节点
远端用户IP或端点 (Peer) ISDN号码:
或端点 (Peer) ID:

用户名: draytek
密码: *****

IKE预设密钥:

IPsec安全方法

☒ 中级 (AH)
高级 (ESP)
☒ DES ☒ 3DES ☒ AES

本地ID: (选择性)

回拨功能

☐ 检查以启动回拨功能
☐ 指定回拨号码
回拨号码:
☒ 启动回拨定额控制
回拨定额: 30 分钟

OK

用户帐号与验证

启用此帐号：只有勾选此设定，该设定档才会被启用。默认是禁用的。

闲置超时：如果没有任何数据传输通过这条建立好的VPN隧道超过“闲置超时”规定的时间，路由器将断掉该连接。默认设置是 300 秒，也就是说如果有个远端用户使用该设定档建立了一条VPN连接，一旦超过 300 秒的时间没有任何数据通过该VPN隧道传输，VPN连接将被自动断开。如果你不想有此时间限制，请将该值设为 0 秒。

用户名：为L2TP连接设置用户名。

密码：为L2TP连接设置密码。

允许的拨入类型：确保L2TP with IPsec Policy被勾选，在下拉菜单里选择“最好能使用”或“一定要有”。

指定远端节点：该选项是可选的。默认是禁用的，也就是说任何远端用户（特别是使用动态IP地址的用户）都可以使用此设定档的设置建立IPSec VPN到Vigor路由器，此时该设定档使用的**预共享密钥**和**IPSec安全方法**在“VPN IPSec / IKE一般设定”里设定。如果为了安全性需要限制特定的用户才能拨入VPN，你可以启用“指定远端节点”功能，并在“远端用户IP”栏里填入该特定用户的公网IP地址。这样，即使其他用户的IPSec设置都匹配此设定档，由于他们的公网IP地址不被允许拨入，他们也无法建立VPN连接。以图 4 为例，你可以在这里填入 218.5.6.7。

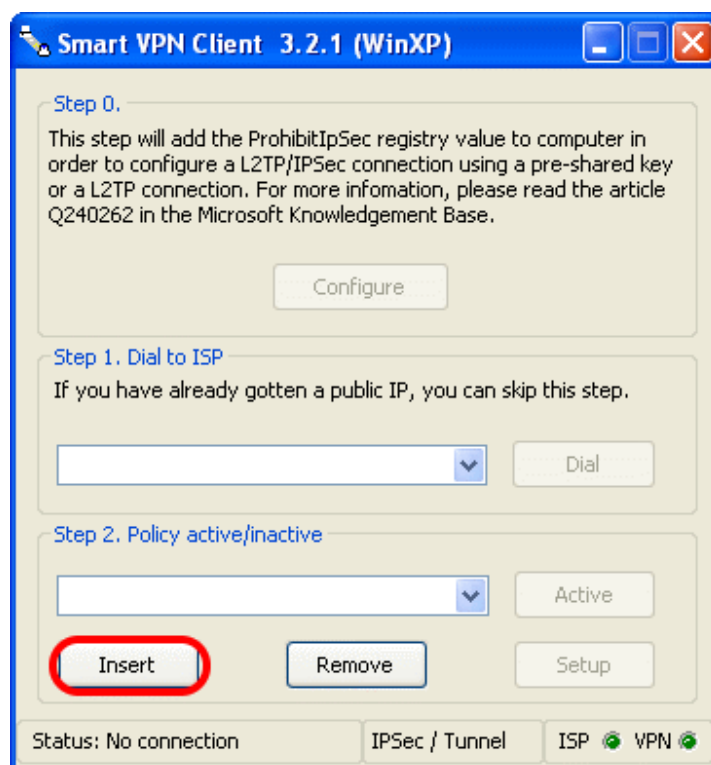
IKE预设密钥与IPSec安全方法：一旦启用了“指定远端节点”功能，就必须为此设定档单独配置**预共享密钥**和**IPSec安全方法**。这里的设定与“VPN IPSec / IKE一般设定”里的设置在功能上是一样的，只不过它被限定只能用于指定的用户。

注意：不要“设置端点（peer）ID”和“本地ID”。

B. 远端用户的VPN设定（Smart VPN Client）

安装并打开Smart VPN Client 3.2.1，按“Insert”按钮新建一个设定档。此后，只要直接从上面的下拉菜单里选此帐号就能连接。

VPN and Remote Access Setup



在弹出窗口里完成以下设置：

Session Name: 为此策略输入任意一个名字。

VPN Server IP/Host Name: 输入VPN服务器的公网地址或动态域名。

User Name/Password: 此帐号的用户名和密码，需和VPN服务器里的相关设定匹配。

Type of VPN: 选择VPN协议，这里选择L2TP over IPSec。

Use default gateway on remote network: 拨入VPN服务器后，使用VPN服务器的网关做为本机的默认网关。

设定完成后点OK。



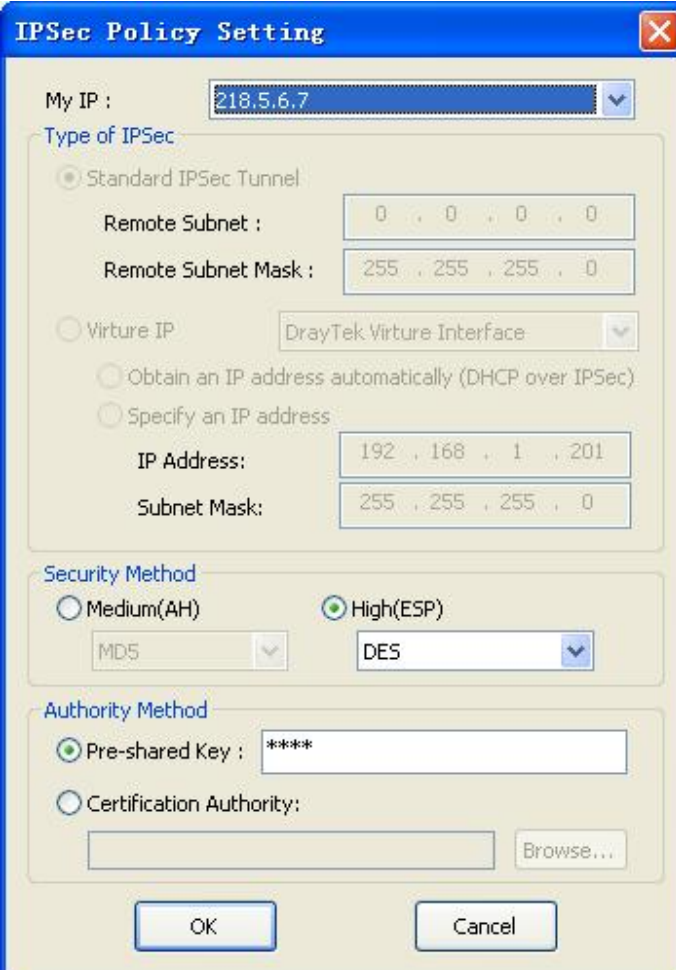
在弹出窗口里完成以下设置：

My IP: 如果你的电脑有多块网卡，选择用于连接VPN服务器的网卡的IP地址。(以图 4 为例，选择 218.5.6.7)

Security Method: 根据VPN服务器的设定选择ESP。注意，不能选择AH。

Authority Method: 选择预共享密钥（Pre-shared Key），输入的密钥必须和VPN服务器里的预共享密钥设定相同。

VPN and Remote Access Setup



The image shows a Windows-style dialog box titled "IPSec Policy Setting". It has a blue title bar with a close button (X) in the top right corner. The dialog is divided into several sections:

- My IP :** A text box containing "218.5.6.7" with a dropdown arrow on the right.
- Type of IPSec :** A section with three radio buttons:
 - ☒ **Standard IPSec Tunnel**: Below this are two text boxes: "Remote Subnet :" with "0 . 0 . 0 . 0" and "Remote Subnet Mask :" with "255 . 255 . 255 . 0".
 - ☐ **Virture IP**: Below this is a dropdown menu showing "DrayTek Virture Interface".
 - ☐ **Obtain an IP address automatically (DHCP over IPSec)**
 - ☐ **Specify an IP address**: Below this are two text boxes: "IP Address:" with "192 . 168 . 1 . 201" and "Subnet Mask:" with "255 . 255 . 255 . 0".
- Security Method**: A section with two radio buttons:
 - ☐ **Medium(AH)**: Below it is a dropdown menu showing "MD5".
 - ☒ **High(ESP)**: Below it is a dropdown menu showing "DES".
- Authority Method**: A section with two radio buttons:
 - ☒ **Pre-shared Key :** Followed by a text box containing "*****".
 - ☐ **Certification Authority:** Followed by a text box and a "Browse..." button.


At the bottom of the dialog are two buttons: "OK" and "Cancel".

设定往后点OK并尝试连接。

12.6 设置LAN-to-LAN设定档

下面将介绍如何在两台VPN路由器之间建立一条VPN隧道，从而将两个局域网连接起来。点击进入“设置LAN-to-LAN设定档”页面，总共可以创建 32 个设定档。



(Set to Factory Default): 将鼠标移到右上栏箭头符号左边的图标，会出现一栏文字“Set to Factory Default”。点击该图标将清除所有的设定档。

名称: 这里显示设定档里**设定档名称**栏里的设定。如果你在该栏里什么都没有输入，将显示默认的符号**???**。

状态: 显示该设定档是否被启用了。符号**v**表示设定档已经启用，符号**x**表示 设定档已经禁用。

索引值: 要进入某个用户帐号配置页面必须点击相应的索引值号码。

每个LAN-to-LAN设定档包含四个部分：一般设定，拨出设定，拨入设定和TCP/IP网络设定。以下将分别介绍这四个部分的设定，最后介绍如何在两台Vigor路由器之间建PPTP，L2TP，L2TP over IPSec和IPSec VPN。

◆ 一般设定

1. 一般设定

设定档名称: ???

☐ 启用此设定档

拨叫方向: ☒ 两者均有 ☐ 拨出 ☐ 拨入

☐ 一直连线

闲置超时: 300 秒

☐ 启用PING以维持连线

指定IP地址:

设定档名称：为该设定档设定一个名字，便于区分其它设定档。

启用此设定档：要启用此设定档必须勾选此选项。

拨叫方向：选择该设定档建立VPN的方向。**两者均有：**该设定档的“拨出设定”部分和“拨入设定”部分均被启用，Vigor路由器即能主动拨VPN连接到远端VPN路由器，又能接受远端VPN路由器拨入的VPN连接。**拨出：**仅“拨出设定”部分被启用，使用此设定档Vigor路由器只能主动拨VPN到远端VPN路由器，不能做为VPN服务器接受拨入的VPN连接。**拨入：**仅“拨入设定”部分被启用，使用此设定档Vigor路由器只能接受远端VPN路由器拨入的VPN，不能主动拨出VPN连接。

一直连线：启用该功能后，只要VPN连接还未建立，Vigor路由器就会以固定的时间间隔不断尝试连接，直到VPN连接建立。连接建立后，会保持该连接一直在线，除非连接被手动断开或由于线路问题导致断线。并且一旦VPN连接断开，Vigor路由器就又开始不断尝试连接。该选项仅对“拨出”方向的VPN有效，所以启用该功能后，**拨叫方向**会被自动设定为**拨出**。另外，该功能被启用后，**闲置超时**会被自动设为-1，并且变成不可设置。

闲置超时： 如果没有任何数据传输通过这条建立好的VPN隧道超过“闲置超时”规定的时间，路由器将断掉该连接。默认设置是 300 秒，如果你不想有此时间限制，请将该值设为 0 秒。

启用PING以维持连线： 启用该功能并在**指定IP地址**栏里输入远端VPN网络里的一个可以ping通的IP地址。当该IP地址ping不通的时候，Vigor路由器即认为该VPN隧道已经无效，便会将该连接断开。该功能是专门为IPSec设计的，而对PPTP，L2TP和L2TP over IPSec是无效的。因为PPTP，L2TP和L2TP over IPSec这类基于PPP的VPN连接会使用相关的PPP机制来实时侦测VPN连接的状态，而IPSec只能在重新交换密钥的时候发现对端是否存在，由于重建密钥的时间间隔一般都是一个小时以上，IPSec无法实时侦测VPN连接的状态。使用该功能就能帮助IPSec快速发现并断开有问题的VPN连接。

指定IP地址： 指定远端VPN内网里一个可以ping通的IP地址，通常指定远端VPN路由器的内网网关。

VPN and Remote Access Setup

◆ 拨出设定

2. 拨出设定

我拨出的服务器类型

☒ ISDN
☐ PPTP
☐ IPSec隧道
☐ L2TP with IPsec Policy 无

服务器IP或域名。
(例如draytek.com或123.45.67.89)

连接类型: 64k bps

用户名: ???

密码:

PPP验证: PAP/CHAP

VJ压缩: ☒ 开启 ☐ 关闭

IKE预设共享密钥:

IPSec安全方法

☒ 中级 (AH)
☐ 高级 (ESP) DES无验证

高级

计划任务 (1-15)

回拨功能 (CBCP)

☐ 要求远端回拨
☐ 提供ISDN号码给远端

拨出的服务器类型： 确定拨出的VPN类型。共有三种类型可选：**PPTP**，**IPSec隧道** 和**L2TP with IPsec Policy**。在L2TP with IPsec Policy的下拉菜单里也有三个选项：**无**，**最好使用**，**一定要有**。选择**无**的时候，VPN类型是L2TP；选择**一定要有**的时候，VPN类型是L2TP over IPsec；选择**最好使用**的时候，VPN类型可以是L2TP，也可以是L2TP over IPsec，优先选择L2TP over IPsec。

服务器IP或域名： 填入远端VPN路由器的公网IP地址或域名。

注意： 以上两处设定是通用设定，在设置**PPTP**，**L2TP**，**L2TP over IPsec**和**IPsec**的时候都必须设置。

计划任务 (1-15)： 这个是可选设定。可以为该VPN设定档设置自动拨号计划，指定在一周的某天的某个时间自动连接，并在另一天另一个时间自动断

开。具体的设置请参考第七章“拨号计划任务设定”。

以下四处设定用于PPP相关的VPN连接，包括PPTP，L2TP和L2TP over IPSec。纯IPSec连接不需要设置这些参数。

用户名：该用户名必须匹配远端VPN路由器上的相关设定。

密码：该密码必须匹配远端VPN路由器上的相关设定。

PPP验证：仅 PAP：若选择该设置，那么在VPN建立的PPP协商阶段，将只支持使用PAP协议进行认证。

PAP/CHAP：若选择该设置，那么Vigor路由器支持以下任意一种验证协议：MS-CHAPv2，MS-CHAPv1，CHAP，PAP。具体使用哪一种由VPN服务器决定。推荐选择此设定。

VJ压缩：它用于TCP/IP协议头的压缩，可以稍微节省一点带宽。建议使用默认设定：开启。

以下三处设定用于L2TP over IPSec和IPSec连接。

IKE预设共享密钥：按此按钮并在弹出窗口里输入预共享密钥（Pre-Shared Key），它必须匹配远端VPN服务器里的相关设定。

IPSec安全方法：选择允许的IPSec安全方法。**注意：**该设定仅用于IPSec Phase 2阶段的协商。

中级 (AH)：数据将被认证，但不会被加密。默认该选项被启用。

高级 (ESP)：数据将被认证和加密。下拉菜单里有 6 个选项：**DES无验证 / DES有验证 / 3DES无验证 / 3DES有验证 / AES无验证 / AES有验证**。无验证指的是不使用MD5 或SHA1 认证算法。当选择“有验证”

VPN and Remote Access Setup

的时候，Vigor将发送两个提议，按先后顺序是SHA1，MD5。譬如，若你选择了 3DES有验证，Vigor将先后发送 3DES+SHA1 和 3DES+MD5 到远端VPN服务器。

高级： 按此按钮，在弹出窗口里可以进行IKE高级设定。



IKE阶段 1 模式： 可以选择主模式（Main mode）或积极模式（Aggressive mode）。该设定必须匹配VPN服务器的设定。*注意：如果选择了积极模式，必须配置本地ID，否则不要配置本地ID。*

IKE阶段 1 提议方法： 在阶段 1（Phase 1），Vigor支持的加密算法是**DES**和**3DES**；支持的认证算法是**MD5** 和**SHA1**；支持的DH组是**Group 1**（768-bit）和**Group 2**（1024-bit）。这些参数的组合总共有 8 组，在下拉菜单里你可以单独选择一组，它必须与VPN服务器的相关设定匹配。此外Vigor 还提供了一个包含了 4 组提议的选项（DES_MD5_G1 / DES_SHA1_G1 / 3DES_MD5_G1 / 3DES_MD5_G2），在VPN建立过程中，Vigor将发送这四个提议给VPN服务器，这四个提议中，第一个匹配VPN服务器设定的组将被VPN服务器采用。当你不确定VPN服务器的配置

的时候，可以选择该选项。

IKE阶段 1 密钥有效时间：设定Phase 1 阶段的密钥存活时间，时间一到，IKE 将协商一个新的密钥。单位是秒，有效值是 900 秒到 86400 秒，默认值是 28800 秒。

IKE阶段 2 密钥有效时间：设定Phase 2 阶段的密钥存活时间，时间一到，IKE 将协商一个新的密钥。单位是秒，有效值是 600 秒到 86400 秒，默认值是 3600 秒。

Perfect Forward Secret：启用该功能将在Phase 2 引入一个新的DH密钥交换，从而提供了更强的安全性。通常不需要PFS，因为危及加密或认证密钥安全性的可能性很小，而且启用PFS也会影响IPSec的速度。如果VPN服务器要求使用PFS，请点选启用。

本地ID：只有在IKE阶段 1 模式是积极模式（Aggressive mode）的时候才需要设定本地ID。它的格式可以是Email地址，域名或字符串。该ID必须匹配VPN服务器里的相关设定，如果远端VPN服务器是Vigor路由器，对应的值是“拨入设定”里的端点（Peer）ID。

◆ 拨入设定

VPN and Remote Access Setup

3. 拨入设定

允许的拨入类型 <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec隧道 <input checked="" type="checkbox"/> L2TP with IPsec Policy 无 <input type="checkbox"/> 指定远端VPN网关 端点 (Peer) VPN服务器IP 或端点 (Peer) ID	用户名 密码 VPN压缩 <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭 IKE预设共享密钥 IPsec安全方法 <input checked="" type="checkbox"/> 中级 (AH) 高级 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 回拨功能 (CBCP) <input type="checkbox"/> 启用回拨功能 <input type="checkbox"/> 使用以下号码回拨 回拨号码 回拨定额 分钟
--	--

允许的拨入类型： 确定允许拨入的VPN类型。共有三种类型可选：**PPTP**，**IPsec 隧道** 和 **L2TP with IPsec Policy**。在L2TP with IPsec Policy的下拉菜单里也有三个选项：**无**，**最好使用**，**一定要有**。选择**无**的时候，VPN类型是L2TP；选择**一定要有**的时候，VPN类型是L2TP over IPsec；选择**最好使用**的时候，VPN类型可以是L2TP，也可以是L2TP over IPsec，优先选择L2TP over IPsec。

指定远端VPN网关： 如果拨入的VPN类型是PPTP，L2TP或IPsec主模式(Main mode)，那么该选项是可选的。如果拨入的VPN类型是IPsec积极模式(Aggressive mode)，那么该选项是必须选择的。该功能默认是禁用的，也就是说任何远端用户（特别是使用动态IP地址的用户）都可以使用此设定档的设置建立VPN到Vigor路由器。如果为了安全性需要限制特定的用户才能拨入VPN，你可以启用“指定远端节点”功能，并在“端点 (Peer) VPN服务器IP”栏里填入该特定VPN服务器的公网IP地址。这样，即使其他用户的设置都匹配此设定档，由于他们的公网IP地址不被允许拨入，他们也无法建立VPN连接。如果拨入的VPN类型是IPsec积极模式，必须启用此功能，并在**端点 (Peer) ID**栏里设置一个ID（不需要设置“端点 (Peer)”

VPN服务器IP”)。ID的格式可以是Email地址，域名或字符串。这个ID在远端VPN路由器里也要输入，如果远端VPN路由器也是Vigor，对应的值是“拨出设定”里的**本地ID**。

以下三处设定用于PPP相关的VPN连接，包括PPTP，L2TP和L2TP over IPSec。纯IPSec连接不需要设置这些参数。

用户名：该用户名必须匹配远端VPN路由器上的相关设定。

密码：该密码必须匹配远端VPN路由器上的相关设定。

VJ压缩：它用于TCP/IP协议头的压缩，可以稍微节省一点带宽。建议使用默认设定：开启。

注意：PPP验证方式在“PPP一般设定”里设置，请参考 12.3 节的内容。

以下两处设定用于IPSec和L2TP over IPSec连接。

IKE预设密钥与IPSec安全方法：一旦启用了“指定远端节点”功能，就必须为此设定档单独配置**预共享密钥**和**IPSec安全方法**。这里的设定与“VPN IPSec / IKE一般设定”里的设置在功能上是一样的，只不过它被限定只能用于指定的用户。

回拨功能（CBCP）：用于ISDN LAN-to-LAN，这里不做介绍。

◆ TCP/IP网络设定

4. TCP/IP网络设定

我的WAN IP	0.0.0.0	RIP方向	TX/RX两者均有
远端网关IP	0.0.0.0	RIP版本	版本: 2
远端网络IP	0.0.0.0	在NAT操作中, 将远端子网络视为	私网IP
远端网络掩码	255.255.255.0		
更多			
<input type="checkbox"/> 变更默认路由到此VPN隧道			

以下设定仅用于PPP相关的VPN连接, 包括PPTP, L2TP, L2TP over IPSec。如果是纯IPSec VPN, 请保留此处的默认设定。

我的WAN IP & 远端网关IP: PPP协商阶段完成安全参数的协商后, 会立即开始IPCP协商阶段, 作用是为PPP链路两端的PPP接口协商IP地址。从本地路由器的角度看, **我的WAN IP**对应PPP链路的本地PPP接口, **远端网关IP**对应PPP链路的远端PPP接口。

注意: 这两个IP是虚拟IP, 用于VPN隧道, 并不是实际的公网IP地址或本地网关。如果你不熟悉IPCP协议, 请使用默认的设定: **0.0.0.0**, 在协商IPCP的时候将使用远端VPN路由器分配的IP地址。

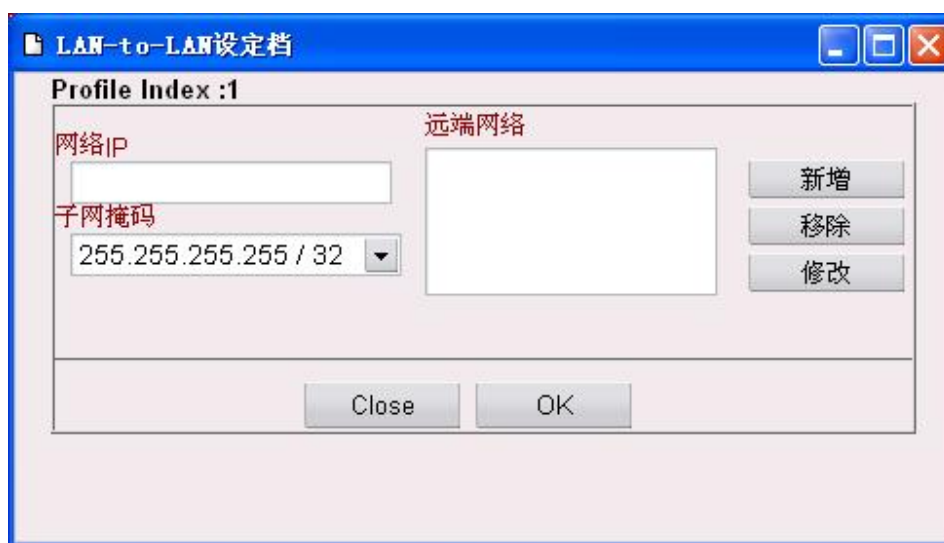
以下设定用于所有类型的VPN。

远端网络IP: 指定远端VPN子网。注意, 这里必须输入一个网络IP, 而不是一个具体的IP地址。譬如远端VPN子网是一个C类网, 内网机器的IP是192.168.100.x (x: 1~254), 那么你应该在这里输入 192.168.100.0。

远端网络掩码: 指定远端VPN子网的掩码。

更多: 按此按钮将弹出一个窗口, 如下图所示。在这个窗口里你可以添加静态路由。在**网络IP**栏里输入要访问的网络IP, 在下拉菜单里选择相应的子网

掩码，然后点击“新增”按钮。注意，在这里添加的静态路由必须是能通过远端VPN子网可路由访问的（请先确认你可以从远端VPN子网访问那些添加的网络）。另外，如果你连接的VPN是IPSec，并且远端VPN路由器是其它厂商的路由器，最好不要使用这个功能，因为它是专门针对Vigor和Vigor建VPN而设计的，我们不保证其它厂商的路由器能配合此功能。



RIP方向：除了在“更多”里添加静态路由，你也可以通过VPN隧道使用RIP协议传送路由信息。**TX/RX两者均有**是指即发送RIP路由信息，又接收RIP路由信息；**仅RX**是指仅接收RIP路由信息；**仅TX**是指仅发送RIP路由信息；**停用**是指禁止通过VPN隧道传送RIP路由信息。

RIP版本：选择RIP协议的版本。为获得最大的兼容性，请使用版本 2。

在NAT操作中，将远端子网络视为：默认设置是**私网IP**，绝大多数应用都应该选这个默认设置。如果没有特殊的目的，请不要选择**公众网IP**。这里的**公众网IP**是一个逻辑概念，并不是真正的公众网。当两个路由器建立了一条VPN，两边的网络便能通过VPN隧道互相访问，如果你希望只有一个方向能访问，另一个方向不能访问，可以选择**公众网IP**。譬如，你在router A

里选择公众网IP，router B里选择私网IP，那么VPN建好后，router A的网络可以访问router B的网络，而router B的网络不能访问router A的网络。此时router A的网络被当作NAT LAN，而router B的网络被当作公众网。**注意：请慎用此功能。**

变更默认路由到此VPN隧道：当VPN连接建立好后，将使用远端VPN路由器的网关做为本地的默认网关。也就是说，所有访问Internet的数据包都先通过VPN隧道路由到远端VPN路由器，再通过远端VPN路由器被发送到Internet。该设定仅对“拨出”方向的VPN有用，所以一旦你启用了这个功能，一般设定栏里面的“拨叫方向”将被自动设定为“拨出”。**注意：**一旦该VPN连接建立好后，就无法建立其它任何VPN连接了。

12.7 LAN-to-LAN VPN连接举例

下面我们将用两台 2900VG为例，介绍如何建立PPTP，L2TP，IPSec（主模式），IPSec（积极模式）和L2TP over IPSec。所有例子都尽可能使用默认设定，用户能体会到在两台Vigor之间建立VPN是非常方便的。连接拓扑如下图所示。假设VPN是从分公司拨出到总公司。

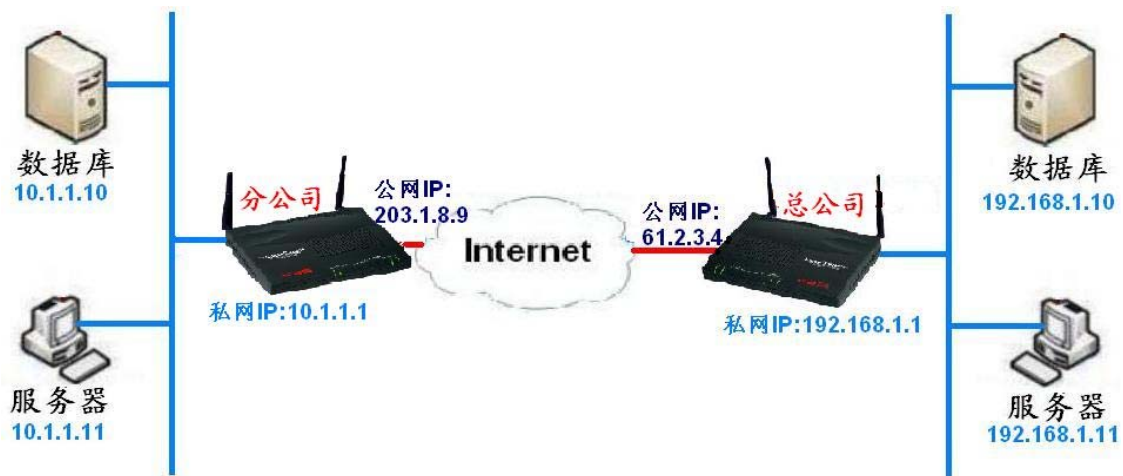


图 5. LAN-to-LAN VPN应用拓扑

12.7.1 PPTP

分公司VPN设定如下:

在默认设定的基础上, 所有需要更改的设定都用红框圈出。

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档索引: 1

1. 一般设定

设定档名称 <input checked="" type="checkbox"/> 启用此设定档 client	拨叫方向 <input checked="" type="checkbox"/> 一直连线 闲置超时: 1 秒 <input type="checkbox"/> 启用PING以维持连线 指定IP地址:	<input type="radio"/> 两者均有 <input checked="" type="radio"/> 拨出 <input type="radio"/> 拨入
---	--	---

2. 拨出设定

我拨出的服务器类型 <input type="radio"/> ISDN <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec隧道 <input type="radio"/> L2TP with IPsec Policy 无	连接类型: 64k bps 用户名: draytek 密码: ***** PPP验证: PAP/CHAP VJ压缩: <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭 IKE预设共享密钥: IPsec安全方法 <input checked="" type="radio"/> 中级 (AH) <input type="radio"/> 高级 (ESP) DES无验证 高级 计划任务 (1-15): 回拨功能 (CBCP) <input type="checkbox"/> 要求远端回拨 <input type="checkbox"/> 提供ISDN号码给远端
--	---

3. 拨入设定

允许的拨入类型 <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec隧道 <input checked="" type="checkbox"/> L2TP with IPsec Policy 无 <input type="checkbox"/> 指定远端VPN网关 端点 (Peer) VPN服务器IP: 或端点 (Peer) ID:	用户名: ??? 密码: VJ压缩: <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭 IKE预设共享密钥: IPsec安全方法 <input checked="" type="checkbox"/> 中级 (AH) 高级 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 回拨功能 (CBCP) <input type="checkbox"/> 启用回拨功能 <input type="checkbox"/> 使用以下号码回拨 回拨号码: 回拨定额: 0 分钟
--	---

4. TCP/IP网络设定

我的WAN IP: 0.0.0.0 远端网关IP: 0.0.0.0 远端网络IP: 192.168.1.0 远端网络掩码: 255.255.255.0 更多	RIP方向: TX/RX两者均有 RIP版本: 版本 2 在NAT操作中, 将远端子网络视为: 私网IP <input type="checkbox"/> 变更默认路由到此VPN隧道
--	--

OK

总公司VPN设定如下：

在默认设定的基础上，所有需要更改的设定都用红框圈出。

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档案索引: 1

1. 一般设定

设定档案名称 <input checked="" type="checkbox"/> 启用此设定档 server	拨叫方向 <input type="checkbox"/> 两者均有 <input type="checkbox"/> 拨出 <input checked="" type="radio"/> 拨入 <input type="checkbox"/> 一直连线 闲置超时 0 秒 <input type="checkbox"/> 启用PING以维持连线 指定IP地址
--	--

2. 拨出设定

我拨出的服务器类型

☒ ISDN
☐ PPTP
☐ IPsec隧道
☐ L2TP with IPsec Policy 无

服务器IP或域名。
(例如draytek.com或123.45.67.89)

连接类型 64k bps
用户名 ???
密码
ppp验证 PAP/CHAP
VJ压缩 ☒ 开启 ☐ 关闭

IKE预设共享密钥

IPsec安全方法

☒ 中级 (AH)
☐ 高级 (ESP) DES无验证

高级

计划任务 (1-15)

回拨功能 (CBCP)

☐ 要求远端回拨
☐ 提供ISDN号码给远端

3. 拨入设定

允许的拨入类型

☒ ISDN
☒ PPTP
☒ IPsec隧道
☒ L2TP with IPsec Policy 无

☐ 指定远端VPN网关
端点 (Peer) VPN服务器IP
或端点 (Peer) ID

用户名 draytek
密码 *****
VJ压缩 ☒ 开启 ☐ 关闭

IKE预设共享密钥

IPsec安全方法

☒ 中级 (AH)
高级 (ESP)
☒ DES ☒ 3DES ☒ AES

回拨功能 (CBCP)

☐ 启用回拨功能
☐ 使用以下号码回拨
回拨号码
回拨定额 0 分钟

4. TCP/IP网络设定

我的WAN IP 0.0.0.0 远端网关IP 0.0.0.0 远端网络IP 10.1.1.0 远端网络掩码 255.255.255.0 更多	RIP方向 TX/RX两者均有 RIP版本 版本. 2 在NAT操作中, 将远端子网络视为 私网IP <input type="checkbox"/> 变更默认路由到此VPN隧道
---	--

OK

12.7.2 L2TP

分公司VPN设定如下：

在默认设定的基础上，所有需要更改的设定都用红框圈出。

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档索引: 1

1. 一般设定

设定档名称:

☒ 启用此设定档

拨叫方向: ☐ 两者均有 ☒ 拨出 ☐ 拨入

☒ 一直连线

闲置超时: 秒

☐ 启用PING以维持连线

指定IP地址:

2. 拨出设定

我拨出的服务器类型

☐ ISDN

☐ PPTP

☐ IPsec隧道

☒ L2TP with IPsec Policy:

服务器IP或域名。
(例如 draytek.com 或 123.45.67.89)

连接类型:

用户名:

密码:

PPP验证:

VJ压缩: ☒ 开启 ☐ 关闭

IKE预设共享密钥:

IPsec安全方法

☒ 中级 (AH)

☐ 高级 (ESP):

高级:

计划任务 (1-15): , , ,

回拨功能 (CBCP)

☐ 要求远端回拨

☐ 提供ISDN号码给远端

3. 拨入设定

允许的拨入类型

☒ ISDN

☒ PPTP

☒ IPsec隧道

☒ L2TP with IPsec Policy:

☐ 指定远端VPN网关

端点 (Peer) VPN服务器IP:

或端点 (Peer) ID:

用户名:

密码:

VJ压缩: ☒ 开启 ☐ 关闭

IKE预设共享密钥:

IPsec安全方法

☒ 中级 (AH)

高级 (ESP): ☒ DES ☒ 3DES ☒ AES

回拨功能 (CBCP)

☐ 启用回拨功能

☐ 使用以下号码回拨

回拨号码:

回拨定额: 分钟

4. TCP/IP网络设定

我的WAN IP:

远端网关IP:

远端网络IP:

远端网络掩码:

RIP方向:

RIP版本:

在NAT操作中, 将远端子网络视为:

☐ 变更默认路由到此VPN隧道

总公司VPN设定如下：

在默认设定的基础上，所有需要更改的设定都用红框圈出。

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档案索引: 1

1. 一般设定

设定档名称 <input checked="" type="checkbox"/> 启用此设定档 server	拨叫方向 <input type="checkbox"/> 一直连线 <input type="checkbox"/> 两者均有 <input type="checkbox"/> 拨出 <input checked="" type="radio"/> 拨入 闲置超时 0 秒 <input type="checkbox"/> 启用PING以维持连线 指定IP地址
---	---

2. 拨出设定

我拨出的服务器类型

☒ ISDN
☐ PPTP
☐ IPsec隧道
☐ L2TP with IPsec Policy 无

服务器IP或域名。
(例如draytek.com或123.45.67.89)

连接类型 64k bps
用户名 ???
密码
PPP验证 PAP/CHAP
VJ压缩 ☒ 开启 ☐ 关闭

IKE预设共享密钥

IPsec安全方法

☒ 中级 (AH)
☐ 高级 (ESP) DES无验证

高级

计划任务 (1-15)

回拨功能 (CBCP)

☐ 要求远端回拨
☐ 提供ISDN号码给远端

3. 拨入设定

允许的拨入类型

☒ ISDN
☒ PPTP
☒ IPsec隧道
☒ L2TP with IPsec Policy 无

☐ 指定远端VPN网关
端点 (Peer) VPN服务器IP
或端点 (Peer) ID

用户名 draytek
密码 *****
VJ压缩 ☒ 开启 ☐ 关闭

IKE预设共享密钥

IPsec安全方法

☒ 中级 (AH)
高级 (ESP)
☒ DES ☒ 3DES ☒ AES

回拨功能 (CBCP)

☐ 启用回拨功能
☐ 使用以下号码回拨
回拨号码
回拨定额 0 分钟

4. TCP/IP网络设定

我的WAN IP 0.0.0.0 远端网关IP 0.0.0.0 远端网络IP 10.1.1.0 远端网络掩码 255.255.255.0 更多	RIP方向 TX/RX两者均有 RIP版本 版本. 2 在NAT操作中, 将远端子网络视为 私网IP <input type="checkbox"/> 变更默认路由到此VPN隧道
---	--

OK

12.7.3 IPSec（主模式）

分公司VPN设定如下：

在默认设定的基础上，所有需要更改的设定都用红框圈出。

按**IKE预设共享密钥**按钮，在弹出窗口里输入两次密钥：**draytek**。

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档案索引: 1

1. 一般设定

设定档案名称 <input checked="" type="checkbox"/> 启用此设定档 client	拨叫方向 <input checked="" type="checkbox"/> 一直连线 闲置超时 1 秒 <input checked="" type="checkbox"/> 启用PING以维持连线 指定IP地址 192.168.1.1
--	---

2. 拨出设定

我拨出的服务器类型 <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec隧道 <input type="radio"/> L2TP with IPsec Policy 无	连接类型 64k bps 用户名 ??? 密码 PPP验证 PAP/CHAP VJ压缩 <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭 IKE预设共享密钥 IPsec安全方法 <input type="radio"/> 中级 (AH) <input checked="" type="radio"/> 高级 (ESP) DES无验证 高级 计划任务 (1-15) 回拨功能 (CBCP) <input type="checkbox"/> 要求远端回拨 <input type="checkbox"/> 提供ISDN号码给远端
--	---

服务器IP或域名。
(例如 draytek.com 或 123.45.67.89)
61.2.3.4

3. 拨入设定

允许的拨入类型 <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec隧道 <input checked="" type="checkbox"/> L2TP with IPsec Policy 无 <input type="checkbox"/> 指定远端VPN网关 端点 (Peer) VPN服务器IP 或端点 (Peer) ID	用户名 ??? 密码 VJ压缩 <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭 IKE预设共享密钥 IPsec安全方法 <input checked="" type="checkbox"/> 中级 (AH) 高级 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 回拨功能 (CBCP) <input type="checkbox"/> 启用回拨功能 <input type="checkbox"/> 使用以下号码回拨 回拨号码 回拨定额 0 分钟
--	---

4. TCP/IP网络设定

我的WAN IP 0.0.0.0 远端网关IP 0.0.0.0 远端网络IP 192.168.1.0 远端网络掩码 255.255.255.0 更多	RIP方向 TX/RX两者均有 RIP版本 版本 2 在NAT操作中, 将远端子网络视为 私有IP <input type="checkbox"/> 变更默认路由到此VPN隧道
--	---

OK

Vigor2900 series

总公司VPN设定如下：

在默认设定的基础上，所有需要更改的设定都用红框圈出。

按**IKE预设共享密钥**按钮，在弹出窗口里输入两次密钥：draytek。

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档案索引: 1

1. 一般设定

设定档名称 <input checked="" type="checkbox"/> 启用此设定档 server	拨叫方向 <input type="checkbox"/> 一直连线 <input type="checkbox"/> 两者均有 <input checked="" type="radio"/> 拨出 <input checked="" type="radio"/> 拨入 闲置超时 0 秒 <input type="checkbox"/> 启用PING以维持连线 指定IP地址
---	---

2. 拨出设定

我拨出的服务器类型

☒ ISDN
☐ PPTP
☐ IPsec隧道
☐ L2TP with IPsec Policy 无

服务器IP或域名。
(例如draytek.com或123.45.67.89)

连接类型: 64k bps
用户名: ???
密码:
PPP验证: PAP/CHAP
VJ压缩: ☒ 开启 ☐ 关闭

IKE预设共享密钥:

IPsec安全方法

☒ 中级 (AH)
☐ 高级 (ESP) DES无验证

高级

计划任务 (1-15)

回拨功能 (CBCP)

☐ 要求远端回拨
☐ 提供ISDN号码给远端

3. 拨入设定

允许的拨入类型

☒ ISDN
☒ PPTP
☒ IPsec隧道
☒ L2TP with IPsec Policy 无

☒ 指定远端VPN网关
端点 (Peer) VPN服务器IP
203.1.8.9
或端点 (Peer) ID

用户名: ???
密码:
VJ压缩: ☒ 开启 ☐ 关闭

IKE预设共享密钥: *****

IPsec安全方法

☒ 中级 (AH)
高级 (ESP)
☒ DES ☒ 3DES ☒ AES

回拨功能 (CBCP)

☐ 启用回拨功能
☐ 使用以下号码回拨
回拨号码:
回拨定额: 0 分钟

4. TCP/IP网络设定

我的WAN IP: 0.0.0.0 远端网关IP: 0.0.0.0 远端网络IP: 10.1.1.0 远端网络掩码: 255.255.255.0 更多	RIP方向: TX/RX两者均有 RIP版本: 版本 2 在NAT操作中, 将远端子网络视为: 私网IP <input type="checkbox"/> 变更默认路由到此VPN隧道
---	--

OK

12.7.4 IPSec（积极模式）

分公司VPN设定如下：

在默认设定的基础上，所有需要更改的设定都用红框圈出。

按**IKE预设共享密钥**按钮，在弹出窗口里输入两次密钥：draytek。

按**高级**按钮，在弹出窗口里完成以下设定。

IKE高级设定

IKE阶段1模式 ☐ 主模式 ☒ 积极模式

IKE阶段1提议方法 DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_SHA1_G1

IKE阶段1密钥有效时间 28800 (900~86400)

IKE阶段2密钥有效时间 3600 (600~86400)

Perfect Forward Secret ☒ 停用 ☐ 启用

本地ID test@a.com

Cancel OK

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档索引: 1

1. 一般设定

设定档名称 <input checked="" type="checkbox"/> 启用此设定档 client	拨叫方向 <input checked="" type="checkbox"/> 一直连线 闲置超时 1 秒 <input checked="" type="checkbox"/> 启用PING以维持连线 指定IP地址 192.168.1.1	<input type="radio"/> 两者均有 <input checked="" type="radio"/> 拨出 <input type="radio"/> 拨入
---	---	---

2. 拨出设定

我拨出的服务器类型 <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec隧道 <input type="radio"/> L2TP with IPsec Policy 无	连接类型 64k bps 用户名 ??? 密码 PPP验证 PAP/CHAP VJ压缩 <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭 IKE预设共享密钥 ***** IPsec安全方法 <input type="radio"/> 中级 (AH) <input checked="" type="radio"/> 高级 (ESP) DES无验证 高级 计划任务 (1-15) <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> 回拨功能 (CBCP) <input type="checkbox"/> 要求远端回拨 <input type="checkbox"/> 提供ISDN号码给远端
--	--

3. 拨入设定

允许的拨入类型 <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec隧道 <input checked="" type="checkbox"/> L2TP with IPsec Policy 无 <input type="checkbox"/> 指定远端VPN网关 端点 (Peer) VPN服务器IP 或端点 (Peer) ID	用户名 ??? 密码 VJ压缩 <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭 IKE预设共享密钥 IPsec安全方法 <input checked="" type="checkbox"/> 中级 (AH) 高级 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 回拨功能 (CBCP) <input type="checkbox"/> 启用回拨功能 <input type="checkbox"/> 使用以下号码回拨 回拨号码 回拨定额 0 分钟
--	--

4. TCP/IP网络设定

我的WAN IP 0.0.0.0 远端网关IP 0.0.0.0 远端网络IP 192.168.1.0 远端网络掩码 255.255.255.0 更多	RIP方向 TX/RX两者均有 RIP版本 版本 2 在NAT操作中, 将远端子网络视为 私网IP <input type="checkbox"/> 变更默认路由到此VPN隧道
--	--

OK

Vigor2900 series

总公司VPN设定如下：

在默认设定的基础上，所有需要更改的设定都用红框圈出。

按**IKE预设共享密钥**按钮，在弹出窗口里输入两次密钥：draytek。

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档案索引: 1

1. 一般设定

设定档名称 <input checked="" type="checkbox"/> 启用此设定档 server	拨叫方向 <input type="checkbox"/> 一直连线 <input type="checkbox"/> 两者均有 <input type="checkbox"/> 拨出 <input checked="" type="radio"/> 拨入 闲置超时 0 秒 <input type="checkbox"/> 启用PING以维持连线 指定IP地址
---	--

2. 拨出设定

我拨出的服务器类型

☒ ISDN
☐ PPTP
☐ IPsec隧道
☐ L2TP with IPsec Policy 无

服务器IP或域名。
(例如draytek.com或123.45.67.89)

连接类型 64k bps
用户名 ???
密码
PPP验证 PAP/CHAP
VJ压缩 ☒ 开启 ☐ 关闭

IKE预设共享密钥

IPsec安全方法
☒ 中级 (AH)
☐ 高级 (ESP) DES无验证

高级

计划任务 (1-15)

回拨功能 (CBCP)
☐ 要求远端回拨
☐ 提供ISDN号码给远端

3. 拨入设定

允许的拨入类型

☒ ISDN
☒ PPTP
☒ IPsec隧道
☒ L2TP with IPsec Policy 无

☒ 指定远端VPN网关
端点 (Peer) VPN服务器IP
或端点 (Peer) ID test@a.com

用户名 ???
密码
VJ压缩 ☒ 开启 ☐ 关闭

IKE预设共享密钥

IPsec安全方法
☒ 中级 (AH)
高级 (ESP)
☒ DES ☒ 3DES ☒ AES

回拨功能 (CBCP)
☐ 启用回拨功能
☐ 使用以下号码回拨
回拨号码
回拨定额 0 分钟

4. TCP/IP网络设定

我的WAN IP 0.0.0.0 远端网关IP 0.0.0.0 远端网络IP 10.1.1.0 远端网络掩码 255.255.255.0 更多	RIP方向 TX/RX两者均有 RIP版本 版本 2 在NAT操作中, 将远端子网络视为 私网IP <input type="checkbox"/> 变更默认路由到此VPN隧道
---	---

OK

12.7.5 L2TP over IPSec

分公司VPN设定如下：

在默认设定的基础上，所有需要更改的设定都用红框圈出。

按**IKE预设共享密钥**按钮，在弹出窗口里输入两次密钥：**draytek**。

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档案索引: 1

1. 一般设定

设定档案名称 <input checked="" type="checkbox"/> 启用此设定档 client	拨叫方向 <input checked="" type="checkbox"/> 一直连线 闲置超时: 1 秒 <input checked="" type="checkbox"/> 启用PING以维持连线 指定IP地址: 192.168.1.1	<input type="radio"/> 两者均有 <input checked="" type="radio"/> 拨出 <input type="radio"/> 拨入
--	---	---

2. 拨出设定

我拨出的服务器类型 <input type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPsec隧道 <input checked="" type="radio"/> L2TP with IPsec Policy 一定要有 服务器IP或域名。 (例如draytek.com或123.45.67.89) 61.2.3.4	连接类型: 64k bps 用户名: draytek 密码: ***** PPP验证: PAP/CHAP VJ压缩: <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭 IKE预设共享密钥: IPsec安全方法 <input type="radio"/> 中级 (AH) <input checked="" type="radio"/> 高级 (ESP) DES无验证 高级 计划任务 (1-15) 回拨功能 (CBCP) <input type="checkbox"/> 要求远端回拨 <input type="checkbox"/> 提供ISDN号码给远端
--	---

3. 拨入设定

允许的拨入类型 <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec隧道 <input checked="" type="checkbox"/> L2TP with IPsec Policy 无 <input type="checkbox"/> 指定远端VPN网关 端点 (Peer) VPN服务器IP 或端点 (Peer) ID	用户名: ??? 密码: VJ压缩: <input checked="" type="radio"/> 开启 <input type="radio"/> 关闭 IKE预设共享密钥: IPsec安全方法 <input checked="" type="checkbox"/> 中级 (AH) 高级 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 回拨功能 (CBCP) <input type="checkbox"/> 启用回拨功能 <input type="checkbox"/> 使用以下号码回拨 回拨号码: 回拨定额: 0 分钟
--	---

4. TCP/IP网络设定

我的WAN IP: 0.0.0.0 远端网关IP: 0.0.0.0 远端网络IP: 192.168.1.0 远端网络掩码: 255.255.255.0 更多	RIP方向: TX/RX两者均有 RIP版本: 版本 2 在NAT操作中, 将远端子网络视为: 私网IP <input type="checkbox"/> 变更默认路由到此VPN隧道
--	--

OK

总公司VPN设定如下：

在默认设定的基础上，所有需要更改的设定都用红框圈出。

按**IKE预设共享密钥**按钮，在弹出窗口里输入两次密钥：draytek。

VPN and Remote Access Setup

高级设定 > LAN-to-LAN 设定

设定档案索引: 1

1. 一般设定

设定档名称 <input checked="" type="checkbox"/> 启用此设定档 server	拨叫方向 <input type="checkbox"/> 一直连线 <input type="checkbox"/> 两者均有 <input type="checkbox"/> 拨出 <input checked="" type="radio"/> 拨入 闲置超时 0 秒 <input type="checkbox"/> 启用PING以维持连线 指定IP地址
---	---

2. 拨出设定

我拨出的服务器类型

☒ ISDN
☐ PPTP
☐ IPsec隧道
☐ L2TP with IPsec Policy 无

服务器IP或域名。
(例如draytek.com或123.45.67.89)

连接类型: 64k bps

用户名: ???

密码:

PPP验证: PAP/CHAP

VJ压缩: ☒ 开启 ☐ 关闭

IKE预设共享密钥:

IPsec安全方法

☒ 中级 (AH)
☐ 高级 (ESP) DES无验证

高级

计划任务 (1-15)

回拨功能 (CBCP)

☐ 要求远端回拨
☐ 提供ISDN号码给远端

3. 拨入设定

允许的拨入类型

☒ ISDN
☒ PPTP
☒ IPsec隧道
☒ L2TP with IPsec Policy 一定要有

☒ 指定远端VPN网关
端点 (Peer) VPN服务器IP
203.1.8.9
或端点 (Peer) ID

用户名: draytek

密码: *****

VJ压缩: ☒ 开启 ☐ 关闭

IKE预设共享密钥:

IPsec安全方法

☒ 中级 (AH)
高级 (ESP)
☒ DES ☒ 3DES ☒ AES

回拨功能 (CBCP)

☐ 启用回拨功能
☐ 使用以下号码回拨
回拨号码
回拨定额: 0 分钟

4. TCP/IP网络设定

我的WAN IP: 0.0.0.0	RIP方向: TX/RX两者均有
远端网关IP: 0.0.0.0	RIP版本: 版本, 2
远端网络IP: 10.1.1.0	在NAT操作中, 将远端子网络视为: 私网IP
远端网络掩码: 255.255.255.0	<input type="checkbox"/> 变更默认路由到此VPN隧道

更多

OK