



NETGEAR VPN 产品

配置完全手册



NETGEAR 中国
2004 年 6 月



目 录

一 . NETGEAR VPN 防火墙产品介绍.....	4
1.1 常用的 VPN 技术	4
1.2 关于动态域名 (Dynamic Domain Name Service)	4
1.3 Netgear VPN 设备的应用	4
二 . Netgear VPN 设备配置指南.....	6
2.1 FVS318 to FVS318 (网关到网关 IKE Main 模式)	7
2.1.1 配置网关 A 静态的 VPN (MAIN 模式)	7
2.1.2 配置网关 B 静态的 VPN (MAIN 模式)	11
2.2 Remote to FVS318 (客户端到网关 IKE Main / Aggressive 模式)	15
2.2.1 用 Main 模式建立 Remote-to-LAN 的 VPN	16
2.2.2 用 Aggressive 模式建立 Remote-to-LAN 的 VPN	21
2.3 Remote to FQDN FVS318 (IKE Main 模式网关为动态 IP 地址)	28
2.3.1 配置 FVS318 的动态 VPN (Main 模式)	28
2.3.2 配置远程客户端动态的 VPN (Main 模式)	32
2.4 FVL328 to FVL328 (网关到网关 IKE Main 模式)	33
2.4.1 配置网关 A 固定 IP 地址的 VPN (MAIN 模式)	34
2.4.2 配置网关 B 固定 IP 的 VPN (Main 模式)	38
2.5 Remote to FVL328 (客户端到网关 Aggressive 模式)	44
2.5.1 配置 FVL328 的远程接入 VPN (Aggressive 模式)	44
2.5.2 配置远程客户端的静态 VPN (Aggressive 模式) 。	49
2.6 Remote to FQDN FVL328(IKE Aggress 模式网关为动态 IP)	54
2.6.1 配置 FVL328 的动态的 (Aggressive 模式) VPN。	54
2.6.2 配置远程客户端的动态的 VPN (Aggressive 模式)	57
2.7 FVS318 to FVL328 (网关到网关 IKE Main 模式)	58
2.7.1 配置 FVS318 的静态 VPN(MAIN 模式).....	58
2.7.2 配置 FVL328 固定 IP 的 VPN (Main 模式) 。	62
2.8 FQDN FVS318 to FVL328 (网关到网关 IKE Main/Aggressive 模式)	68
2.8.1 IKE Main 模式网关到网关的 VPN 配置	68
2.8.2 IKE Aggressive 模式网关到网关的 VPN 配置	74
三 . 常用 VPN 专业术语	77
3.1 IPsec 简介	77
3.2 Internet 密钥交换协议(IKE)	77
3.2.1 IKE 协商	77
3.2.2 IKE 协议	78
3.2.3 IKE 阶段 1 - IKE 安全协商	78
3.2.4 IKE 阶段 2 - IPsec 安全协商	78
3.2.4 IKE 参数	79
3.3 IKE 认证方法 (手工 , PSK , 证书)	82
3.3.1 手工密钥	82
3.3.2 Pre-Shared 密钥, PSK	82
3.3.3 证书	82



3.4 IPsec 协议(ESP/AH).....	83
3.4.1 认证头(Authentication Header).....	83
3.4.2 ESP (Encapsulating Security Payload)	83



一 . NETGEAR VPN 防火墙产品介绍

1.1 常用的 VPN 技术

VPN 技术是指在公共的网络平台如 Internet 上搭建隧道传输用户私有的数据，从而使得在不安全的互联网上安全地传输私有数据来实现用户的广域互联。这种技术的效果类似于传统的租用专线联网方式，但其费用远比采用专线方式联网要便宜。

目前常见的 VPN 隧道协议分三种：点到点隧道协议 PPTP，第二层隧道协议 L2TP，网络层隧道协议 IPSec。现在一般情况下的 VPN 设备都会支持 IPSec 协议，在绝大部分情况下都采用 IPSEC 协议来构建 VPN 网络。

常见的利用 VPN 技术的组网方式分三种：

- 远程访问（客户端到网关，Client to Gateway），一般用于个人远程用户、出差用户等对公司局域网集中资源的访问。
- Intranet VPN（网关到网关，Gateway to Gateway），一般用于企业不同分支机构局域网之间的互连。
- Extranet VPN（网关到网关，Gateway to Gateway），用于合作伙伴/客户局域网等与企业局域网之间的安全互连。

早期用于远程访问是 VPN 应用的主要类型，但随着宽带接入的快速发展，目前后两种 VPN 的应用已成为企业尤其是中小型企业利用 Internet 组建公司广域网的主流方式。

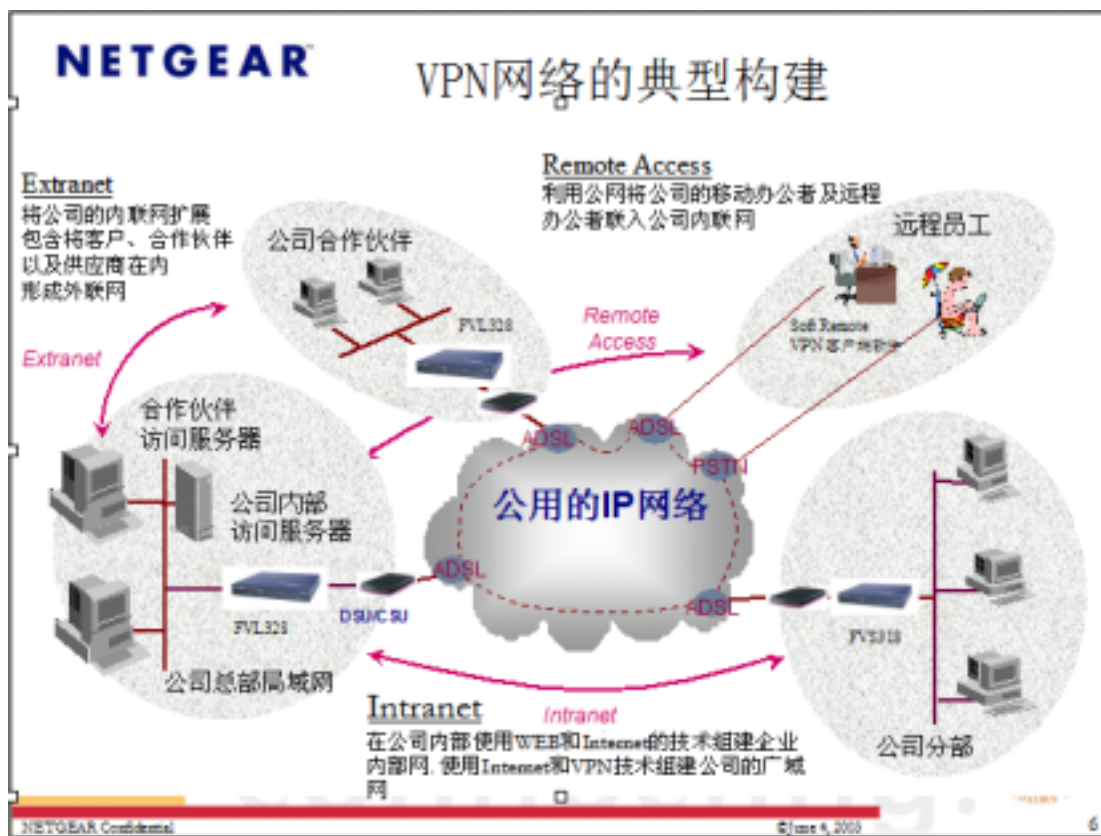
1.2 关于动态域名（Dynamic Domain Name Service）

根据 VPN 虚拟专用网的组网原理,当创建 VPN 网络时一般情况下要求隧道的至少一方具有固定的 IP 地址(有很多产品还要求双方都要求固定的 IP 地址)。由于申请固定 IP 地址的月租费远远高于动态 IP 地址的月租费，因此如果用户想采用宽带接入进行 VPN 组网的话如两端均申请动态 IP 地址的宽带接入方式将大大降低组网成本。

NETGEAR 公司创新地采用 FQDN 技术，并与国内大型的 DDNS 运营公司结盟。用户可免费从 NETGEAR 的合作伙伴处申请到 DDNS(动态域名解析服务)，在组建 VPN 网络时可支持网络的两端均为动态的 IP 地址，从而可低成本地组建 VPN 网络。NETGEAR 公司的 VPN 产品为用户组网带来巨大的好处，如只需申请普通的 ADSL 接入,就可方便便宜地组建 VPN 虚拟专用网,实现多分支机构的广域网互连和公司远程员工的远程访问了。

1.3 Netgear VPN 设备的应用

NETGEAR 公司高性能价格比的 VPN 产品组网示意图如下：



NETGEAR 公司为企业网络、中小型商用网络、SOHO 网络以及家庭网络提供完整的高性能 VPN 设备。

NETGEAR 全系列的 VPN 防火墙产品有：

型号	产品描述
FVL328	具 1 个 10/100M 广域网口，8 个 10/100M 局域网口、具 SPI 防火墙功能的 VPN 防火墙 (100 个 IPSEC VPN 隧道)
FVS328	具 1 个 10/100M 广域网口，8 个 10/100M 局域网口、具 SPI 防火墙功能的 VPN 防火墙 (50 个 IPSEC VPN 隧道)
FVS318	具 1 个 10M 广域网口，8 个 10/100M 局域网口、具防火墙功能的 VPN 防火墙 (8 个 IPSEC VPN 隧道)
FWG114P	具 1 个 10/100M 广域网口，4 个 10/100M 局域网口、802.11g 54Mbps 无线局域网接入点、防火墙功能的 VPN 防火墙 (2 个 IPSEC VPN 隧道)
FVM318	具 1 个 10/100M 广域网口，8 个 10/100M 局域网口、11M 无线局域网接入点、防火墙功能的 VPN 防火墙 (102 个 IPSEC VPN 隧道)
FWAG114	具 1 个 10/100M 广域网口，4 个 10/100M 局域网口、双频三模无线局域网接入点、防火墙功能的 VPN 防火墙 (2 个 IPSEC VPN 隧道)
VPN01L VPN05L	NETGEAR VPN 客户端软件 (单用户与五用户版)



在本配置文档当中各 VPN 设备所用到的软件版本是：

产品名称	软件版本
FVS318	Version 2.3
FVS328	Version 1.0 Release 09
FVL328	Version 2.0 Release 02
FWG114P	Version 2.0Release 10
FVM318	Version 1.1
FWAG114	Version 1.0.26 RC4
IPSec VPN Client Software	Netgear Prosafe vpn client 10.1.1(build 10)

所有产品的最新版本信息请及时查询 [Http://www.NETGEAR.com](http://www.NETGEAR.com) 网站。

由于 FVM318 的 VPN 配置界面与 FVS318 相同，FWAG114、FWG114P、FVS328 的 VPN 配置界面与 FVL328 相同，所以在本文档将以 FVS318 及 FVL328 两种产品作为代表，详细介绍建立 VPN 隧道的相关设置，其他各种产品的设置都可以此为蓝图。

二 . Netgear VPN 设备配置指南

本文档提供的 NETGEAR VPN 产品配置案例共有以下 8 种不同的情况，在这常见的 8 种情况的基础之上，只要稍一变通，就能配置出各种情形下的 VPN 配置来。并不是说在建网时一定要完全按照这 8 种不同情形，完全可以变通。

FVS318 to FVS318 (IKE Main)	双方静态 IP 地址
Remote to FVS318 (IKE Main / Aggressive)	网关方为静态 IP 地址
Remote to FQDN FVS318 (IKE Main)	网关方为动态 IP 地址
FVL328 to FVL328 (IKE Main)	双方静态 IP 地址
Remote to FVL328 (IKE Main / Aggressive)	网关方为静态 IP 地址
Remote to FVL328 (IKE Aggressive)	网关方为动态 IP 地址
FVS318 to FVL328 (IKE Main)	双方静态 IP 地址
FQDN FVS318 to FVL328 (IKE Main/Aggressive)	双方动态 IP 地址

我们只提供了基于 IPSec 协议的 IKE 模式下的 VPN 组网配置，其实所有这些设备也支持 IPSec 协议下的 Manual 模式，但由于其配置复杂而很少被使用，这里不作详细说明。

在下文的配置介绍中，将会出现一些 VPN 的专业表述，具体请参考最后一个章节的常用 VPN 专业术语或者登陆网站 www.vpnc.com 查询。



2.1 FVS318 to FVS318 (网关到网关 IKE Main 模式)

LAN-to-LAN (两边全静态 IP 的 VPN) 从 FVS318 to FVS318 (MAIN 模式)

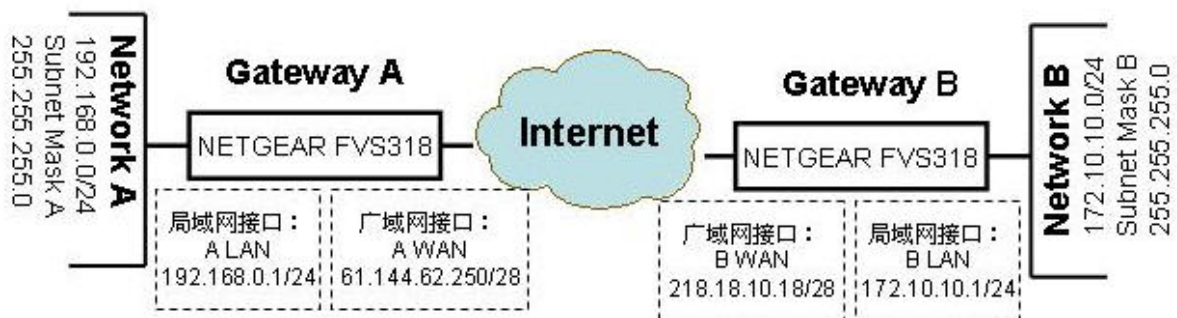
VPN 建立的模式：	LAN-TO-LAN (FVS318-TO-FVS318 的 MAIN 模式)
VPN 的类型	LAN-to-LAN 或是 Gateway-to-Gateway (Client-to-Gateway 另外讲)
VPN 的安全配置:	利用 IKE 进行密钥交换并采用共享密钥方式 (不是能过 CA 认证方式) 建立 IPSEC 通道。
产品型号和版本号:	
NETGEAR-网关 A	FVS318 用的版本号是 version 2.3
NETGEAR-网关 B	FVS318 用的版本号是 version 2.3
IP 地址的方式：	
NETGEAR-网关 A	由 ISP 提供的固定 IP 地址及网关和子网掩码。
NETGEAR-网关 B	由 ISP 提供的固定 IP 地址及网关和子网掩码。

表一 建立动态VPN 的LAN-TO-LAN的测试参数

这是静态 (MAIN 模式) 的 LAN-TO-LAN 的 VPN 例子配置的过程。有关于 VPN 的一些原理可去参考最后一个章节的常用 VPN 专业术语或者登陆网站 www.vpnc.com 查询。这一过程的配置是根据实际情况来进行的。

VPN 构建的方式: Gateway-to-Gateway 利用共享密钥方式。

以下是一个静态 (MAIN 模式) 的 LAN-TO-LAN 的 VPN, VPN 利用共享加密的认证方式。



图一：网络结构图

NETGEAR FVS318 Gateway A 的一端连接到局域网，内部 IP 为 192.168.0.1/24.。其广域网接口连接到互联网，并由 ISP 提供的固定 IP 地址及网关和子网掩码。

NETGEAR FVL328 Gateway B 的一端连接到局域网，内部 IP 为 192.168.0.1/24.。其广域网接口连接到互联网，并由 ISP 提供的固定 IP 地址及网关和子网掩码。如上图所示

2.1.1 配置网关 A 静态的 VPN (MAIN 模式)

首先登录到FVS318的管理界面：



1. 在IE地址栏上输入,FVS318的出厂值默认的IP地址：<http://192.168.0.1>。然后系统要要求你输入登陆的用户名和密码。用默认的用户名：**admin** 和 默认密码：**password**. 登陆到FVS318。我们假定已设定好LAN接口、广域网接口的IP地址和子网掩码以及网关、DNS服务器的IP地址。如下图：

图例二：NETGEAR FVS318 v2.3 VPN 设置。

2. 在工具栏左边点击 VPN Settings. 点击第一个VPN连接。(总共可以输入八个有效的VPN 连接)。按编辑的 Edit 按钮一下。这下面就是 VPN Settings – MAIN Mode 的设置。



NETGEAR FVS318 ProSafe VPN Firewall settings

VPN Settings - Main Mode

• Setup Wizard
• VPN Wizard

Setup

- Basic Settings
- VPN Settings

Security

- Security Logs
- Block Sites
- Block Service
- Add Service
- Schedule
- E-mail

Maintenance

- Router Status
- Attached Devices
- Set Password
- Settings Backup

Connection Name: to-GatewayB

Local IPSec Identifier: 0.0.0.0

Remote IPSec Identifier: 0.0.0.0

Tunnel can be accessed from: a subnet of local address

Local LAN start IP Address: 192.168.0.0

Local LAN finish IP Address: 0.0.0.0

Local LAN IP Subnetmask: 255.255.255.0

Tunnel can access: a subnet of remote address

Remote LAN start IP Address: 172.10.10.0

Remote LAN finish IP Address: 0.0.0.0

Remote LAN IP Subnetmask: 255.255.255.0

Remote WAN IP or FQDN: 218.18.10.18

图三：NETGEAR FVS318 v2.3 VPN Settings (第一部分) – MAIN Mode

- 在 **Connection Name** 框中，输入一个VPN通道名称。例如：我们设为：“to-Gateway B”。
- 在 NETGEAR FVS318 Gateway A 的 **Local IPSec Identifier** 中输入本地身份认证标识。这个表示必须和对端的 **Remote IPSec Identifier** 相对应。在这个例子中使用 0.0.0.0 作为 **local identifier**。
- 在 **Remote IPSec Identifier** 中输入远端身份认证表示，该标识必须和远端的 **Local IPSec Identifier** 的表示相一致。在这个例子中我们输入 0.0.0.0 作为 **the remote identifier**。
- 在 **Tunnel can be accessed from** 下拉菜单中选择 **a subnet from local address**。
- 在 **Local LAN start IP Address** 输入本地LAN所在网段 (例如：192.168.0.0)。
- 在 **Local LAN IP Subnetmask** 的对话框中输入子网掩码 (例如：255.255.255.0)。
- 从 **Tunnel can access** 的下拉菜单中选择 **a subnet from local address**。
- 在 **Remote LAN Start IP Address** 的对话框中输入对端 (GatewayB) 的内网的所在地址段 (例如：172.10.10.0) 在。
- 在 **Remote LAN IP Subnetmask** 的对话框中输入局域网的子网掩码 (例如：255.255.255.0) 在。
- 在 **Remote WAN IP or FQDN** 的对话框中输入对端FVS318 Gateway B的广域网接口的IP地址 (例如：218.18.10.18)。



Secure Association: Main Mode

Perfect Forward Secrecy: ☒ Enabled ☐ Disabled

Encryption Protocol: 3DES

PreShared Key: netgear2004

Key Life: 28800 Seconds

IKE Life Time: 86400 Seconds

☒ NETBIOS Enable

Apply Cancel

图 四：NETGEAR FVS318 v2.3 VPN 设置模式 – MAIN Mode

- 从 Secure Association 下拉框中, 选择Main Mode.
- 在 Perfect Forward Secrecy, 选择Enabled 按钮。 .
- 再从Encryption Protocol 下拉对话框, 选择3DES加密方式。 .
- 在PreShared Key 对话框中, 输入统一的子字符串共享密钥。在这个例子中我们输入”netgear2004”. 你必须在对端的设备上输入同样的共享密码。 .
- 在 Key Life 对话框, 输入28800 seconds.(出厂默认值)
- 在 IKE Life 对话框中, 输入86400 seconds(出厂默认值)。 .
- 如果你希望 NetBIOS数据流量从 VPN通道中运行, 在前方方框中选择 NETBIOS Enable , 行, 例如允许在Microsoft 系统中的网络邻居看到对方的计算机就必须选上。
- 点击Apply 按钮 这些所有配置都会存储到设备中. 然后就会返回到 VPN Settings 屏幕上。

NETGEAR FVS318 ProSafe VPN Firewall settings

VPN Settings

	#	Enable	Connection Name	Local IPSec ID	Remote IPSec ID
<input checked="" type="radio"/>	1	<input checked="" type="checkbox"/>	to-GatewayB	0.0.0.0	0.0.0.0
<input type="radio"/>	2	<input type="checkbox"/>	-	-	-
<input type="radio"/>	3	<input type="checkbox"/>	-	-	-
<input type="radio"/>	4	<input type="checkbox"/>	-	-	-
<input type="radio"/>	5	<input type="checkbox"/>	-	-	-
<input type="radio"/>	6	<input type="checkbox"/>	-	-	-
<input type="radio"/>	7	<input type="checkbox"/>	-	-	-
<input type="radio"/>	8	<input type="checkbox"/>	-	-	-

Edit Delete Cancel

图五：NETGEAR FVS318 v2.3 VPN 设置之后的VPN返回的状态介面。



3. 按返回 回到VPN Settings的界面,注意必须在您新建立的连接中选择 **Enable** 选项。.

2.1.2 配置网关 B 静态的 VPN (MAIN 模式)

首先登录到FVS318的管理界面：

1.在IE地址栏上输入,FVS318的出厂值默认的IP地址：<http://192.168.0.1>。然后系统要要求你输入登陆的用户名和密码。用默认的用户名：**admin** 和 默认密码：**password**. 登陆到FVS318。我们假定已设定好LAN接口、广域网接口的IP地址和子网掩码以及网关、DNS服务器的IP地址。如下图：

Basic Settings

Does your Internet connection require a login?

☒ No
☐ Yes

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

☐ Get dynamically from ISP
☒ Use static IP address

IP Address

IP Subnet Mask

Gateway IP Address

Domain Name Server (DNS) Address

☐ Get automatically from ISP
☒ Use these DNS servers

Primary DNS

Secondary DNS

图六：NETGEAR FVS318 v2.3 VPN 设置

2. 在工具栏左边点击 VPN Settings. 点击第一个VPN连接。(总共可以输入八个有效的VPN连接)。按编辑的 Edit 按钮一下。这下面就是 VPN Settings – MAIN Mode 的设置。



NETGEAR FVS318 ProSafe VPN Firewall settings

VPN Settings - Main Mode

• Setup Wizard
• VPN Wizard

Setup

- Basic Settings
- VPN Settings

Security

- Security Logs
- Block Sites
- Block Service
- Add Service
- Schedule
- E-mail

Maintenance

- Router Status
- Attached Devices
- Set Password
- Settings Backup

Connection Name: to-Gateway A

Local IPSec Identifier: 0.0.0.0

Remote IPSec Identifier: 0.0.0.0

Tunnel can be accessed from: a subnet of local address

Local LAN start IP Address: 172.10.10.0

Local LAN finish IP Address: 0.0.0.0

Local LAN IP Subnetmask: 255.255.255.0

Tunnel can access: a subnet of remote address

Remote LAN start IP Address: 192.168.0.0

Remote LAN finish IP Address: 0.0.0.0

Remote LAN IP Subnetmask: 255.255.255.0

Remote WAN IP or FQDN: 61.144.62.250

图七：NETGEAR FVS318 v2.3 VPN Settings (第一部分) – MAIN Mode

- 在 Connection Name 框中，输入一个VPN通道名称. 例如：我们设为：“to-Gateway A”。
- 在 NETGEAR FVS318 Gateway B 的 **Local IPSec Identifier** 中输入本地身份认证标识。这个表示必须和对端的 **Remote IPSec Identifier** 相对应。在这个例子中使用 0.0.0.0 作为 local identifier。
- 在 **Remote IPSec Identifier** 中输入远端身份认证表示，该标识必须和远端的 **Local IPSec Identifier** 的表示相一致。在这个例子中我们输入 0.0.0.0 作为 the remote identifier。
- 在 Tunnel can be accessed from 下拉菜单中选择 a subnet from local address。 .
- 在Local LAN start IP Address 输入本地LAN所在网段 (例如：172.10.10.0)。 .
- 在Local LAN IP Subnetmask 的对话框中输入子网掩码 (例如：255.255.255.0)。 .
- 从 Tunnel can access 的下拉菜单中选择 a subnet from local address。
- 在Remote LAN Start IP Address 的对话框中输入对端 (GatewayA) 的内网的所在地址段 (例如：192.168.0.0) 在。
- 在Remote LAN IP Subnetmask 的对话框中输入局域网的子网掩码(例如：255.255.255.0) 在。
- 在Remote WAN IP or FQDN 的对话框中输入对端FVS318 Gateway A的广域网接口的IP地址 (例如：61.144.62.250)。



Secure Association

Perfect Forward Secrecy ☒ Enabled ☐ Disabled

Encryption Protocol 3DES

PreShared Key netgear2004

Key Life 28800 Seconds

IKE Life Time 86400 Seconds

☒ NETBIOS Enable

Apply Cancel

图八：NETGEAR FVS318 V2.3 VPN 设置模式 – MAIN Mode

- 从 Secure Association 下拉框中, 选择Main Mode.
- 在 Perfect Forward Secrecy, 选择Enabled 按钮。 .
- 再从Encryption Protocol 下拉对话框, 选择3DES加密方式。 .
- 在PreShared Key 对话框中, 输入统一的子字符串共享密钥。在这个例子中我们输入”netgear2004”. 你必须在对端的设备上输入同样的共享密码。 .
- 在 Key Life 对话框, 输入28800 seconds.(出厂默认值)
- 在 IKE Life 对话框中, 输入86400 seconds(出厂默认值)。 .
- 如果你希望 NetBIOS数据流量从 VPN通道中运行, 在前方方框中选择 NETBIOS Enable , 行, 例如允许在Microsoft 系统中的网络邻居看到对方的计算机就必须选上。
- 点击Apply 按钮 这些所有配置都会存储到设备中. 然后就会返回到 VPN Settings 屏幕上。

NETGEAR FVS318 ProSafe VPN Firewall

settings

VPN Settings

	#	Enable	Connection Name	Local IPSec ID	Remote IPSec ID
<input checked="" type="radio"/>	1	<input checked="" type="checkbox"/>	to-Gateway A	0.0.0.0	0.0.0.0
<input type="radio"/>	2	-	-	-	-
<input type="radio"/>	3	-	-	-	-
<input type="radio"/>	4	-	-	-	-
<input type="radio"/>	5	-	-	-	-
<input type="radio"/>	6	-	-	-	-
<input type="radio"/>	7	-	-	-	-
<input type="radio"/>	8	-	-	-	-

Edit Delete Cancel

图九：NETGEAR FVS318 v2.3 VPN 设置之后的VPN返回的状态介面



3. 按返回 回到VPN Settings的界面,注意必须在您新建立的连接中选择 **Enable** 选 项。

当Gateway A和 Gateway B两 端的VPN创建好之后，在两端的任一端局域网上PING对方的局域网客户端。例如：ping 172.10.10.1 -t.或 Ping 192.168.0.1 -t 在半分钟左右会通，证明VPN通道已建立连接。



2.2 Remote to FVS318 (客户端到网关 IKE Main / Aggressive 模式)

从 Remote to FVS318 (MAIN 模式和 Aggressive 模式, 一边是静态 IP, 另一端是移动用户)的 VPN 建立。

VPN 建立的模式:	Remote-TO-LAN (Remote-TO-FVS318 的 MAIN 模式和 Aggressive 模式)
VPN 的类型	Client-to-Gateway(LAN-to-LAN 和 Gateway-to-Gateway)
VPN 的加密:	利用 IKE 进行密钥交换和共享密钥方式 (不是能过 CA 认证方式) 建立 IPSEC 通道。
产品型号和版本号:	
NETGEAR-网关 A	FVS318 用的版本号是 version 2.3
移动用户	通过拨号接入当地的 ISP.(如: Modem 拨号、ADSL、ISDN 等上网。
IP 地址的方式:	
NETGEAR-网关 A	由 ISP 提供的固定 IP 地址及网关和子网掩码。
移动用户	通过多种方式只要能上互联网 即 OK。

表一: 建立动态VPN的LAN-TO-LAN的测试参数

这是个 Remote-TO-LAN 的 VPN 配置例子的过程。有关于 VPN 的一些原理可去参考最后一个章节的常用 VPN 专业术语或者登陆网站 www.vpnc.com 查询。这一过程的配置是根据实际情况来进行的。

VPN 构建的方式: Remote-to-Gateway 利用共享密钥方式。

以下为一个静态 (MAIN 模式) 的 Remote-TO-LAN 的 VPN 建立例子, 使用共享加密和认证方式。



NETGEAR FVS318 Gateway A 的一端连接到局域网, 内部 IP 为 192.168.0.1/24.。其广域网接口连接到互联网, 并由 ISP 提供的固定 IP 地址及网关和子网掩码。移动用户即要连入当地的 ISP 能上网即可。(见上图)



2.2.1 用 Main 模式建立 Remot-to-LAN 的 VPN

2.2.1.1 配置 FVS318 静态的 VPN (MAIN 模式)

首先登录到FVS318的管理界面：

- 1.在IE地址栏上输入,FVS318的出厂值默认的IP地址：<http://192.168.0.1>。然后系统要要求你输入登陆的用户名和密码。用默认的用户名：**admin** 和 默认密码：**password**. 登陆到FVS318。我们假定已设定好LAN接口、广域网接口的IP地址和子网掩码以及网关、DNS服务器的IP地址。如下图：

NETGEAR FVS318 ProSafe VPN Firewall settings

Basic Settings

Does your Internet connection require a login?

☒ No

☐ Yes

Account Name (If Required) FVS318

Internet IP Address

☐ Get dynamically from ISP

☒ Use static IP address

IP Address 61 144 62 250

IP Subnet Mask 255 255 255 248

Gateway IP Address 61 144 62 249

Domain Name Server (DNS) Address

☐ Get automatically from ISP

☒ Use these DNS servers

Primary DNS 202 96 128 68

Secondary DNS 202 96 128 110

Logout

图一：- NETGEAR FVS318 v2.3 VPN 设置。

2. 在工具栏左边点击 VPN Settings. 点击第一个VPN连接。(总共可以输入八个有效的VPN 连接)。按编辑的 Edit 按钮一下。这下面就是 VPN Settings – MAIN Mode 的设置。



NETGEAR FVS318 ProSafe VPN Firewall settings

VPN Settings - Main Mode

• Setup Wizard
• VPN Wizard

Setup

- Basic Settings
- VPN Settings

Security

- Security Logs
- Block Sites
- Block Service
- Add Service
- Schedule
- E-mail

Maintenance

- Router Status
- Attached Devices
- Set Password
- Settings Backup

Connection Name: Remote-to-318

Local IPSec Identifier: 0.0.0.0

Remote IPSec Identifier: 0.0.0.0

Tunnel can be accessed from: a subnet of local address

Local LAN start IP Address: 192.168.0.0

Local LAN finish IP Address: 0.0.0.0

Local LAN IP Subnetmask: 255.255.255.0

Tunnel can access: the remote WAN IP or FQDN

Remote LAN start IP Address: 0.0.0.0

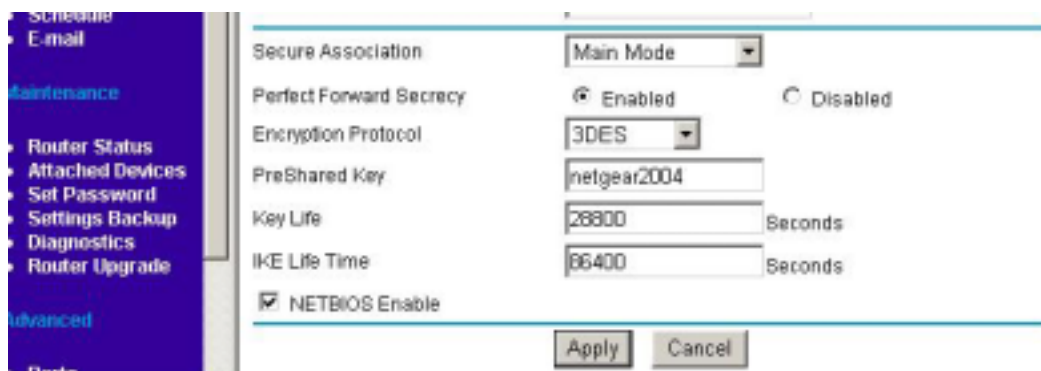
Remote LAN finish IP Address: 0.0.0.0

Remote LAN IP Subnetmask: 0.0.0.0

Remote WAN IP or FQDN: 0.0.0.0

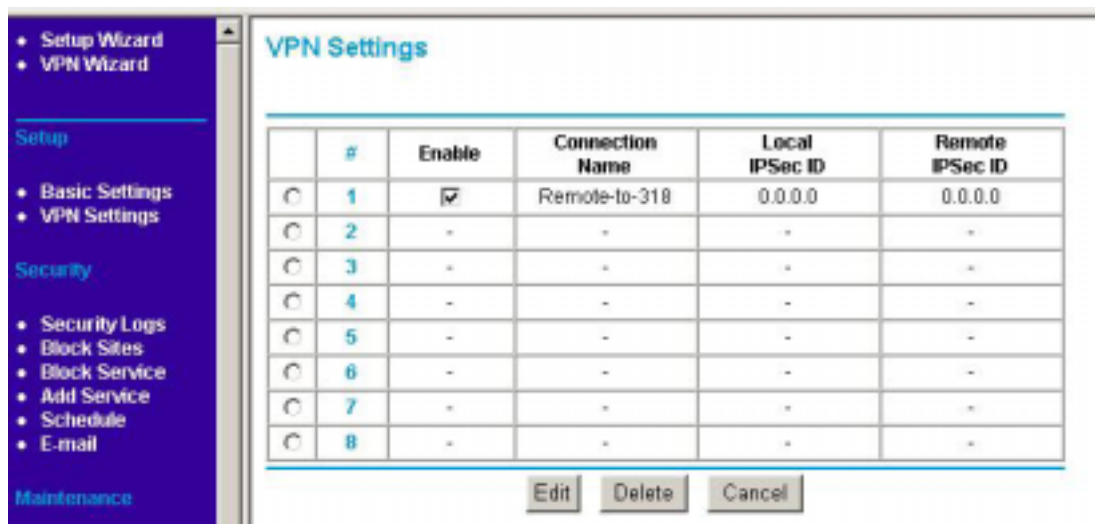
图三：NETGEAR FVS318 vA1.4 F VPN Settings (第一部分) – MAIN Mode

- 在 Connection Name 框中，输入一个VPN通道名称. 例如：我们设为：“Remote-to-318”。
- 在 NETGEAR FVS318 Gateway A 的 Local IPSec Identifier 中输入本地身份认证标识。这个表示必须和对端的 Remote IPSec Identifier 相对应。在这个例子中使用 0.0.0.0 作为 local identifier。
- 在 Remote IPSec Identifier 中输入远端身份认证表示，该标识必须和远端的 Local IPSec Identifier 的表示相一致。在这个例子中我们输入 0.0.0.0 作为 the remote identifier。
- 在 Tunnel can be accessed from 下拉菜单中选择 a subnet from local address。
- 在 Local LAN start IP Address 输入本地LAN所在网段 (例如：192.168.0.0)。
- 在 Local LAN IP Subnetmask 的对话框中输入子网掩码 (例如：255.255.255.0)。
- 从 Tunnel can access 的下拉菜单中选择 Remote WAN IP or FQDN。
- 在 Remote WAN IP or FQDN 的对话框中输入客户端广域网接口的IP地址 (因为客户端的IP地址不固定的所以输入0.0.0.0)。



图四：NETGEAR FVS318 v2.3 VPN 设置模式 – MAIN Mode

- 从 Secure Association 下拉框中, 选择Main Mode.
- 在 Perfect Forward Secrecy, 选择Enabled 按钮。 .
- 再从Encryption Protocol 下拉对话框, 选择3DES加密方式。 .
- 在PreShared Key 对话框中, 输入统一的子字符串共享密钥。在这个例子中我们输入”netgear2004”. 你必须在对端的设备上输入同样的共享密码。 .
- 在 Key Life 对话框, 输入28800 seconds.(出厂默认值)
- 在 IKE Life 对话框中, 输入86400 seconds(出厂默认值)。 .
- 如果你希望 NetBIOS数据流量从 VPN通道中运行, 在前方方框中选择 NETBIOS Enable , 行, 例如允许在Microsoft 系统中的网络邻居看到对方的计算机就必须选上。
- 点击Apply 按钮 这些所有配置都会存储到设备中. 然后就会返回到 VPN Settings 屏幕上。



图五：NETGEAR FVS318 v2.3 VPN 设置之后的VPN返回的状态介面。

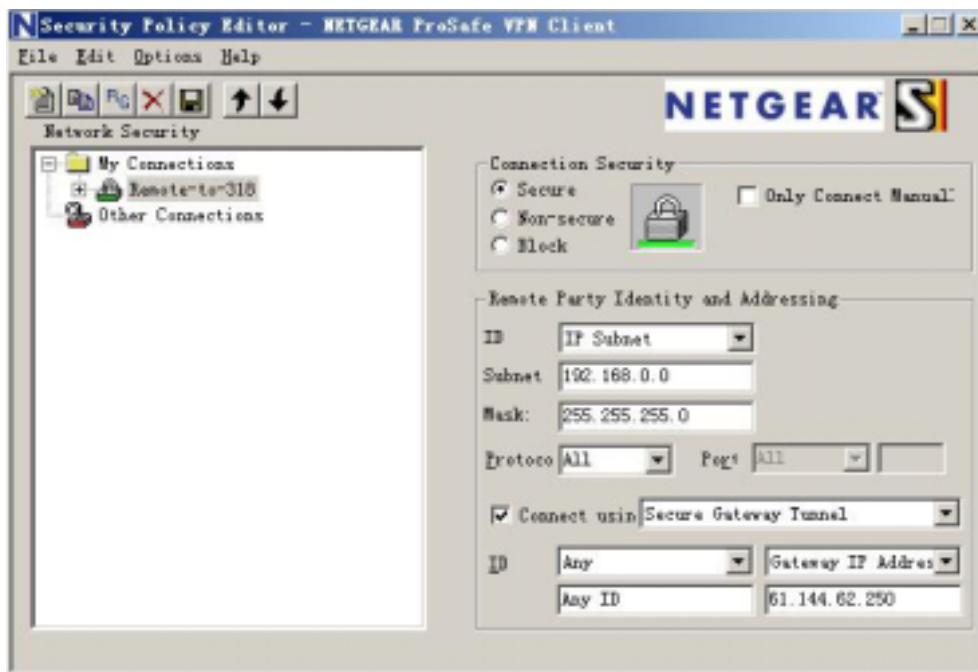
3. 按返回 回到VPN Settings的界面,注意必须在您新建立的连接中选择 Enable 选 项。 .



2.2.1.2 配置远程客户端的静态 VPN (Main 模式)

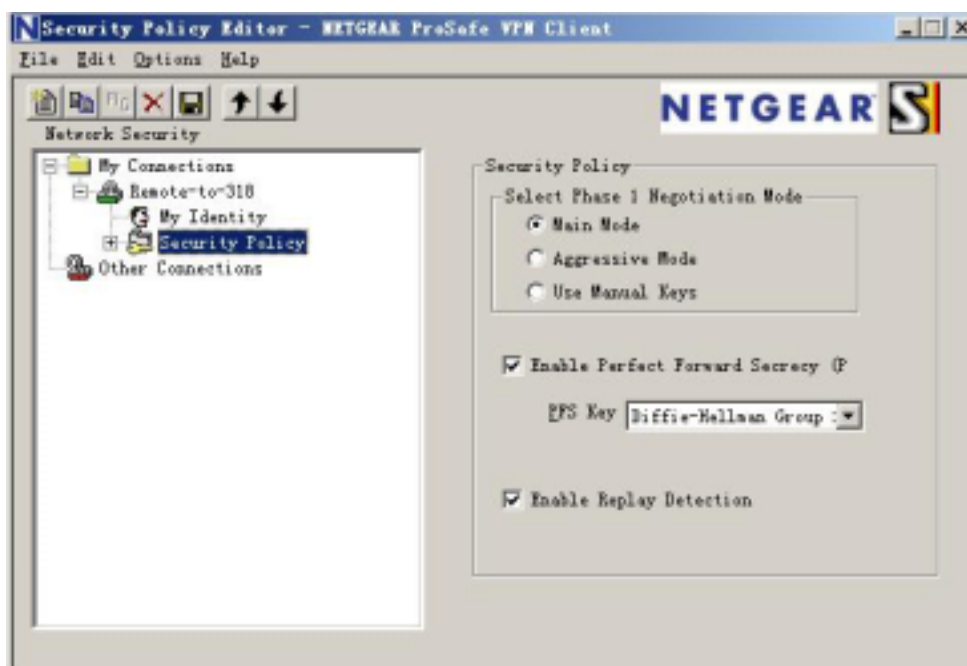
1. 首先在移动用户的电脑上装好Netgear Prosafe VPN Client v 10.1.1的客户端软件
2. 打开Netgear Prosafe VPN Client 的客户端软件的Security Policy Edit。

客户端的配置软件如下的介面：



图六：客户端配置界面

- 选择客户端的模式 (Main模式)。



图七：客户端配置界面

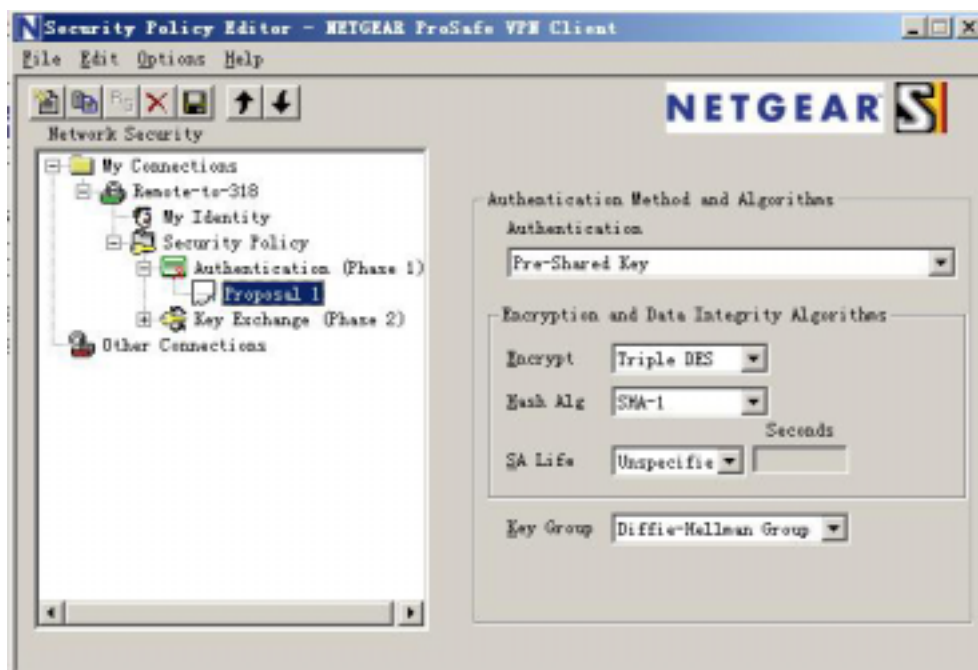


- 打开My Identity 对话框，编辑Pre-Shared-Key。输入与318对应的密码：“netgear2004”。如图：

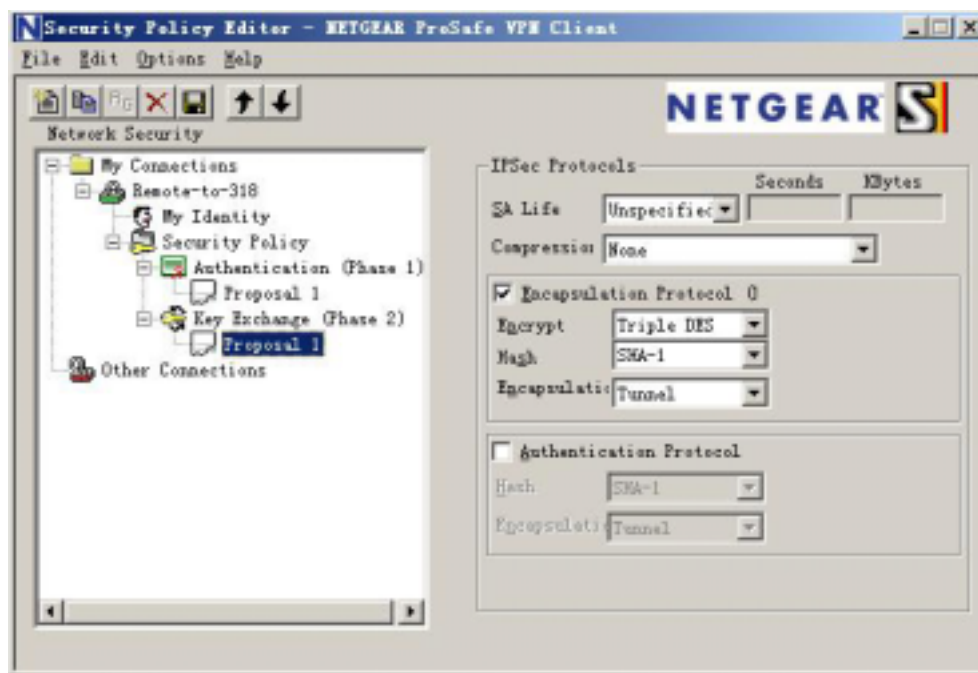


图八：客户端配置界面

- 分别建立VPN验证和加密两个步骤的规则：



图九：客户端配置界面



图十：客户端配置界面

- 设置好并及时保存配置。并在客户端一端ping 192.168.0.1 -t.半分钟左右会通。证明VPN通道已建通。

如果通道建立成功，能在Route Status 工具栏中打开Show VPN Status中可以看到VPN建立的两个步骤已经建通，如下图：

IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Inactive	remote-to-318	0.0.0.0	0.0.0.0/32		Idle	Drop
Inactive	remote-to-318_tmp5	61.144.128.30	61.144.128.30/32		Idle	Drop
Active	remote-to-318_tmp6	218.20.177.201	218.20.177.201/32	ESP(3DES-CBC SHA-1)	[P1:M-Estab] [P2:Q-Estab]	Drop

图十一：与客户端建立VPN的过程

2.2.2 用 Aggressive 模式建立 Remote-to-LAN 的 VPN

2.2.2.1 配置 FVS318 静态的 VPN (Aggressive 模式)

首先登录到FVS318的管理界面：

- 1.在IE地址栏上输入,FVS318的出厂值默认的IP地址：<http://192.168.0.1>。然后系统要要求你输入登陆的用户名和密码。用默认的用户名：**admin** 和 默认密码：**password**. 登



陆到FVS318。我们假定已设定好LAN接口、广域网接口的IP地址和子网掩码以及网关、DNS服务器的IP地址。如下图：

The screenshot shows the 'VPN Settings - Aggressive Mode' configuration page. The left sidebar has a 'Setup' section with 'VPN Wizard' selected, and a 'Maintenance' section with 'Router Status' selected. The main configuration area includes the following fields:

- Connection Name: Remote-to-318
- Local IPsec Identifier: fvs_local
- Remote IPsec Identifier: fvs_remote
- Tunnel can be accessed from: a subnet of local address (dropdown)
- Local LAN start IP Address: 192.168.0.0
- Local LAN finish IP Address: 0.0.0.0
- Local LAN IP Subnetmask: 255.255.255.0
- Tunnel can access: the remote WAN IP or FQDN (dropdown)
- Remote LAN start IP Address: 0.0.0.0
- Remote LAN finish IP Address: 0.0.0.0
- Remote LAN IP Subnetmask: 0.0.0.0
- Remote WAN IP or FQDN: 0.0.0.0

图十二：NETGEAR FVS318 v2.3 VPN 设置模式 –Aggressive Mode

- 在 **Connection Name** 框中，输入一个单一的名字作为VPN通道的名称。例如：我们设为：“Remote-to-318”。
- 在 NETGEAR FVS318 Gateway A 的**Local IPsec Identifier** 名对话框中输入本地的身份认证信息。这个名字必须在对端的**Remote IPsec Identifier**输入。在**Aggressive** 模式下，该信息必须为字符串。在这个例子中使用fvs_local作为 local identifier。
- 在 NETGEAR FVS318 Gateway A 的**Remote IPsec Identifier** 名对话框中输入客户端的身份认证信息。这个名字必须和客户端的**Remote IPsec Identifier**相一致。在这个例子中使用fvs_remote作为 Remote identifier。
- 从**Tunnel can be accessed from** 下拉菜单中选择 a subnet of local address：。
- 在**Local LAN start IP Address** 输入本地LAN的起始IP的FVS318 Gateway A的地址（例如：192.168.0.0）。。
- 在**Local LAN IP Subnetmask** 的对话框中输入子网掩码。（例如：255.255.255.0）。
- 从 **Tunnel can access** 的下拉菜单中选择 **The remote WAN IP or FQDN**。。
- 在**Remote WAN IP or FQDN** 的广域网接口中输入移动用户的广域网接口的IP地址，因为不知道对端的地址，所以输入0.0.0.0（例如：0.0.0.0）。



Secure Association: Aggressive Mode
Perfect Forward Secrecy: ☒ Enabled ☐ Disabled
Encryption Protocol: 3DES
Key Group: Diffie-Hellman Group1
PreShared Key: netgear2004
Key Life: 28800 Seconds
IKE Life Time: 86400 Seconds
☒ NETBIOS Enable
Apply Cancel

图十三：NETGEAR FVS318 v2.3 VPN 设置模式 –Aggressive Mode

- 在 Secure Association 下拉框中, 选择Aggressive Mode.
- 下一步是在 Perfect Forward Secrecy, 选择Enabled 按钮。.
- 再从Encryption Protocol 下拉对话框, 选择3DES加密方式。.
- 在Key Group下拉框中选取Diffie-Hellman Group1。
- 在PreShared Key 对话框中,输入统一的子字符串共享密钥, 在这个例子中我们输入”netgear2004”. 你必须在对端的设备上输入同样的共享密码。.
- 在 Key Life 对话框, 输入28800 seconds.(出厂默认值)
- 在 IKE Life 对话框中, 输入86400 seconds(出厂默认值)。
- 如果你希望 NetBIOS数据流量从 VPN通道中运行, 在前方方框中选择 NETBIOS Enable。
- 点击Apply 按钮 , 然后就会返回到 VPN Settings 屏幕。

NETGEAR FVS318 ProSafe VPN Firewall settings

VPN Settings

	#	Enable	Connection Name	Local IPSec ID	Remote IPSec ID
<input checked="" type="radio"/>	1	<input checked="" type="checkbox"/>	Remote-to-318	fvs_local	fvs_remote
<input type="radio"/>	2	<input type="checkbox"/>	-	-	-
<input type="radio"/>	3	<input type="checkbox"/>	-	-	-
<input type="radio"/>	4	<input type="checkbox"/>	-	-	-
<input type="radio"/>	5	<input type="checkbox"/>	-	-	-
<input type="radio"/>	6	<input type="checkbox"/>	-	-	-
<input type="radio"/>	7	<input type="checkbox"/>	-	-	-
<input type="radio"/>	8	<input type="checkbox"/>	-	-	-

Edit Delete Cancel

图十四：NETGEAR FVS318 vA1.4 VPN 设置之后的VPN返回的状态介面。

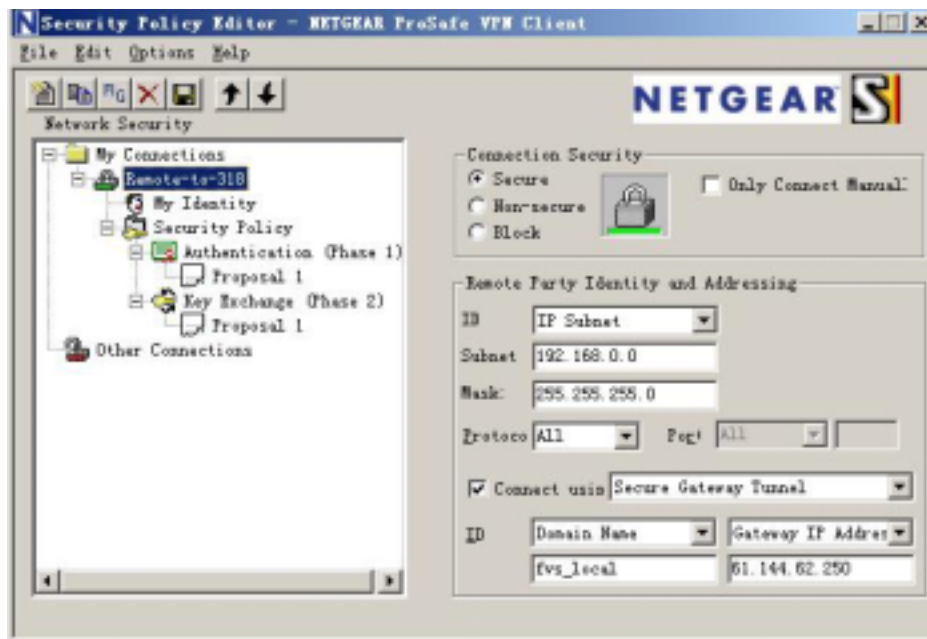


3. 按返回 回到VPN Settings的界面,注意必须在您新建立的连接中选择 **Enable** 选项。.

2.2.1.2 配置远程客户端静态的 VPN (Aggressive 模式)

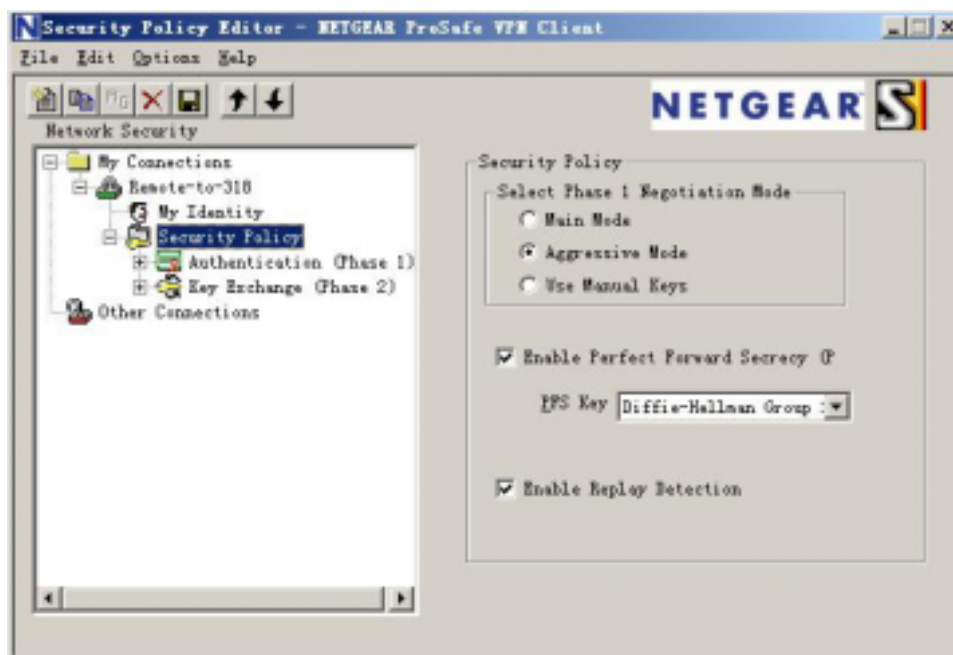
1. 首先在移动用户的电脑上装好Netgear Prosafe VPN Client v10.1.1的客户端软件
2. 打开Netgear Prosafe VPN Client v 10.1.1的客户端软件的Security Policy Edit。

- 客户端的配置软件如下的界面：



图十五：客户端配置界面

- 选择客户端的模式 (Aggressive Mode模式)。



图十六：客户端配置界面

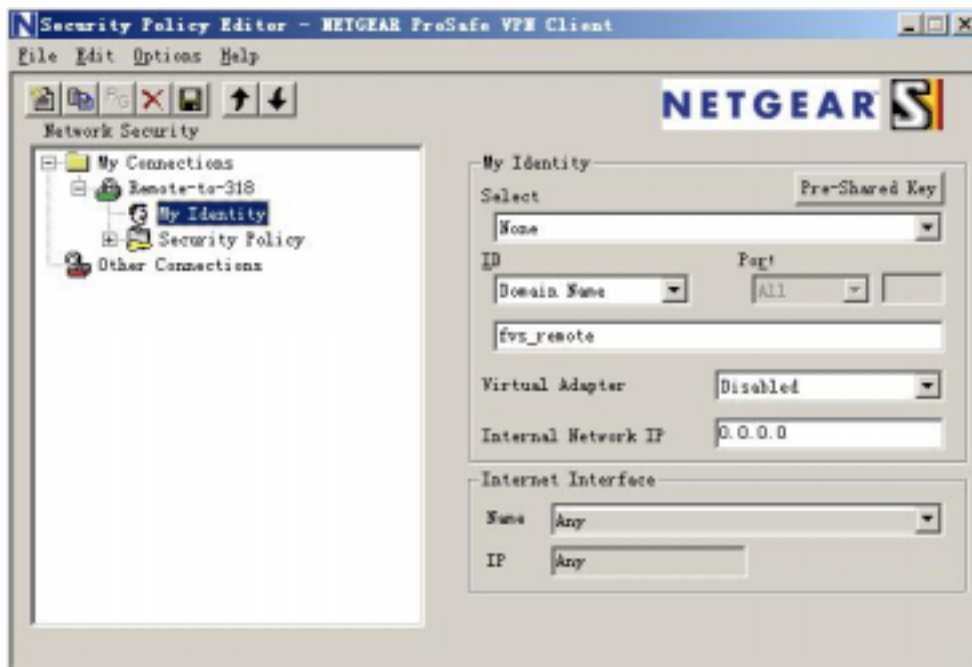


- 打开My Identity 对话框，编辑Pre-Shared-Key。输入与318对应的密码：“netgear2004”。如图：



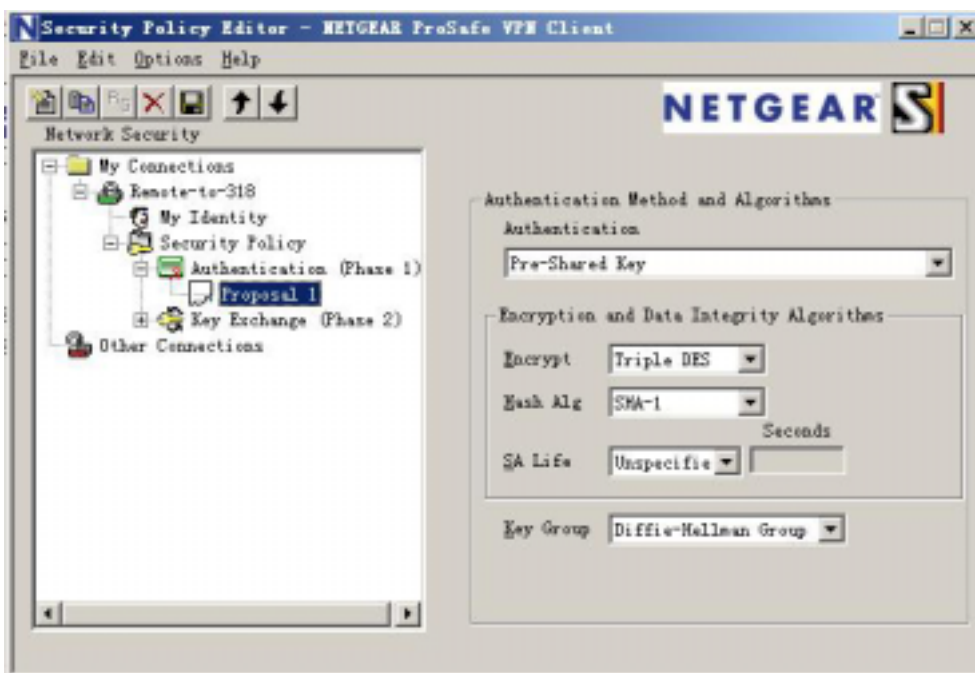
图十七：客户端配置界面

- 在My Identity 对话框里，填入My Identity 信息，这里填入的认证信息必须和Gateway A里所设置的Remote Identity信息相一致。

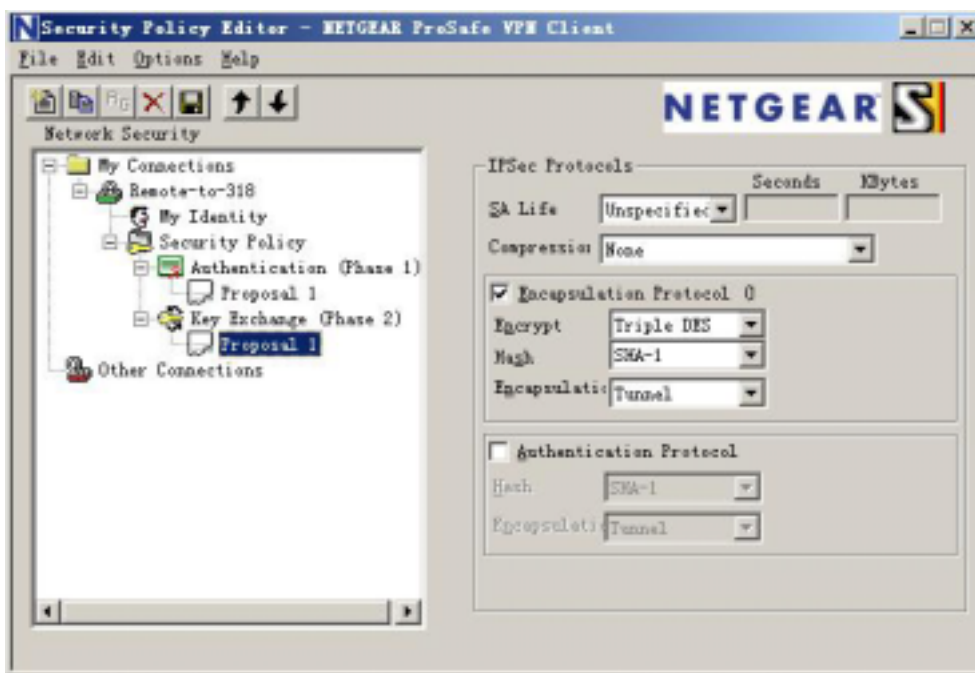


图十八：客户端配置界面

- 分别建立VPN认证和加密两个步骤的规则：



图十九：客户端配置界面



图二十：客户端配置界面

3. 设置好并及时保存配置。并在客户端一端ping 192.168.0.1 - t. 半分钟左右会通。证明VPN通道已建通。

如果通道建立成功，能在Route Status 工具栏中打开Show VPN Status中可以看到VPN的两个步已建通，如下图：



IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Inactive	remote-to-318	0.0.0.0	0.0.0.0/32		Idle	<input type="button" value="Drop"/>
Active	remote-to-318_tmp7	218.20.177.201	218.20.177.201/32	ESP(3DES-CBC SHA-1)	[P1:A-Estab.] [P2:Q-Estab.]	<input type="button" value="Drop"/>

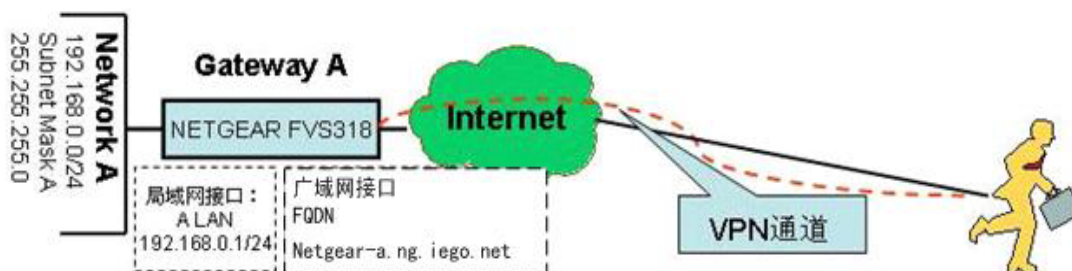
图二十一：VPN通道建立的过程



2.3 Remote to FQDN FVS318 (IKE Main 模式网关为动态 IP 地址)

当 VPN 服务器端为非固定 IP 地址的时候，必须在服务器端启用我们提供的免费动态域名服务，正如第一章所介绍。动态域名的作用是通过客户端软件和动态域名服务器的工作作用，使不断变化的 IP 地址总和固定的单一域名相对应。只有在中心设置了动态域名服务后，客户端软件就可以通过固定的动态域名解释到 VPN 服务器的真实 IP 地址。

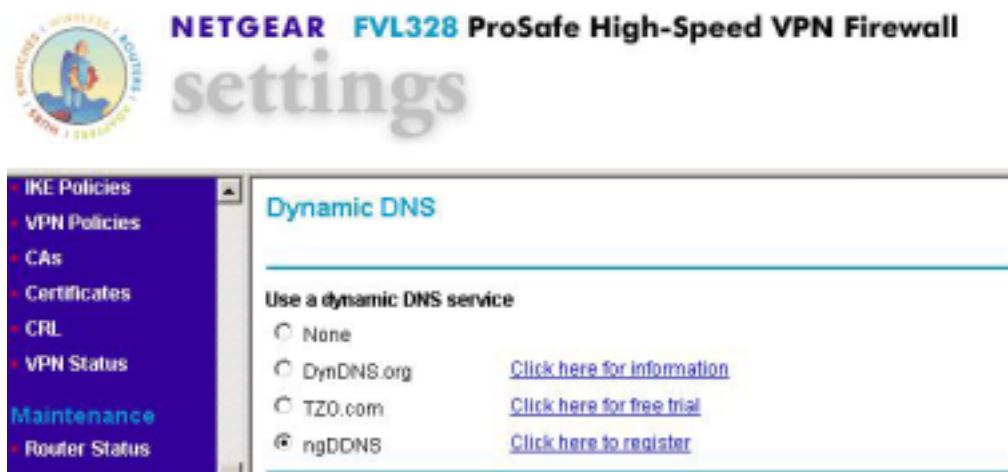
在此我们仍然以 2.2 章节里的环境为例子，所不同的是在 2.2 的例子中，中心 FVS318 采用的是固定的 IP 地址，而在我们现在的環境中，FVS318 采用的是动态拨号上网方式，并没有固定的 IP 地址，需要申请固定的动态域名。



2.3.1 配置 FVS318 的动态 VPN (Main 模式)

1. 申请动态域名：

在我们的网站里注册自己的动态域名：



图一：动态域名的申请

- 点击 ngDDNS 所在的连接，将引导我们进入动态域名服务的注册页面。



图二：动态域名的申请

- 点击注册，在用户名称一栏输入自己的用户名（注意：输入的用户名将作为动态域名的前缀，我们提供的动态域名格式为：用户名.ng.iego.net）。在用户密码里输入密码再确认重复输入一次，即完成对动态域名的注册。

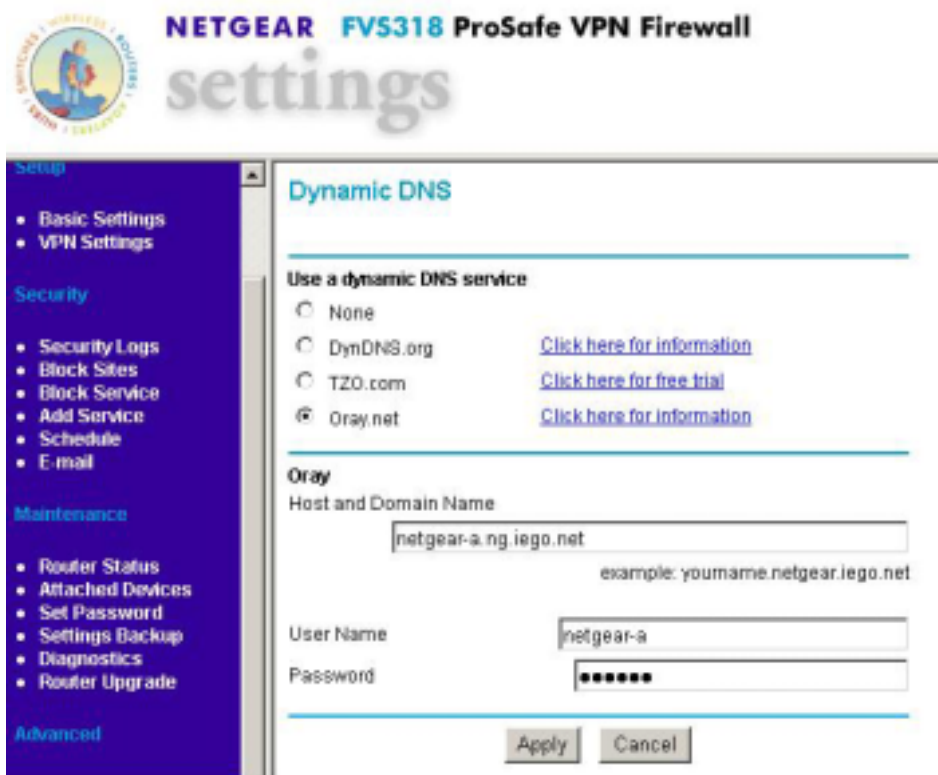


图三：动态域名的申请



2. 在 Gateway A (FVS318) 上启动动态域名服务：

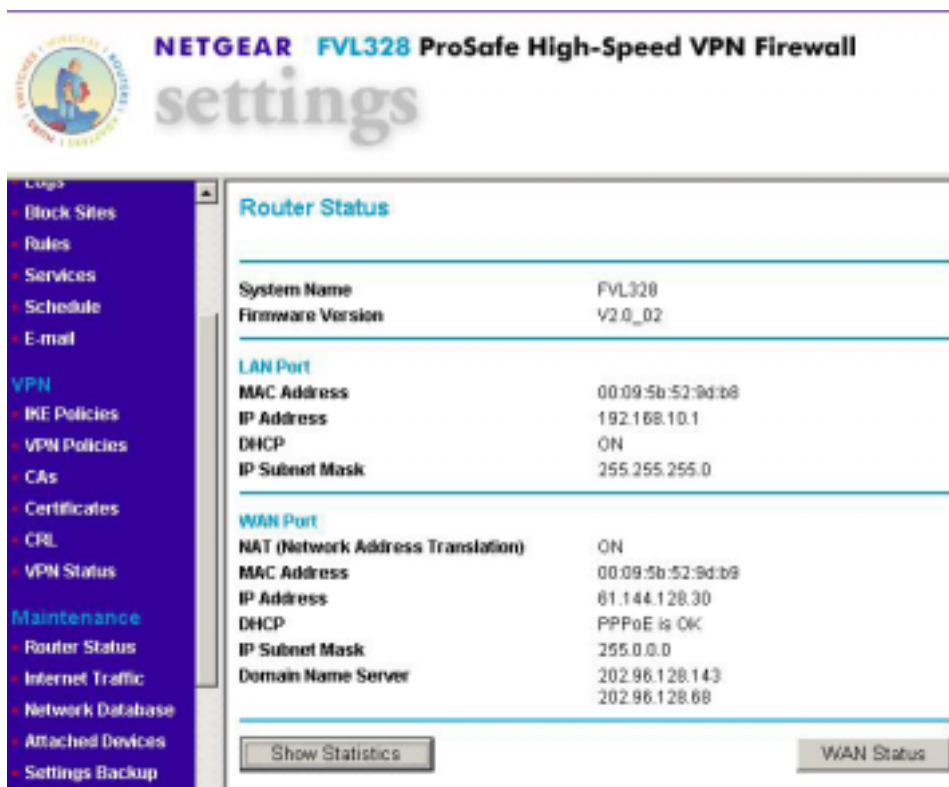
- 在 DDNS 选项里，先选中适当的服务提供商，在中国大陆我们应该选择 Oray.net（网域科技），然后在相应的信息栏目里填入相应的注册信息即可。如下图：在我们的例子里，我们为站点 A 申请了，名为 Netgear-a.ng.iego.net 的动态域名。



图四：动态域名的启用

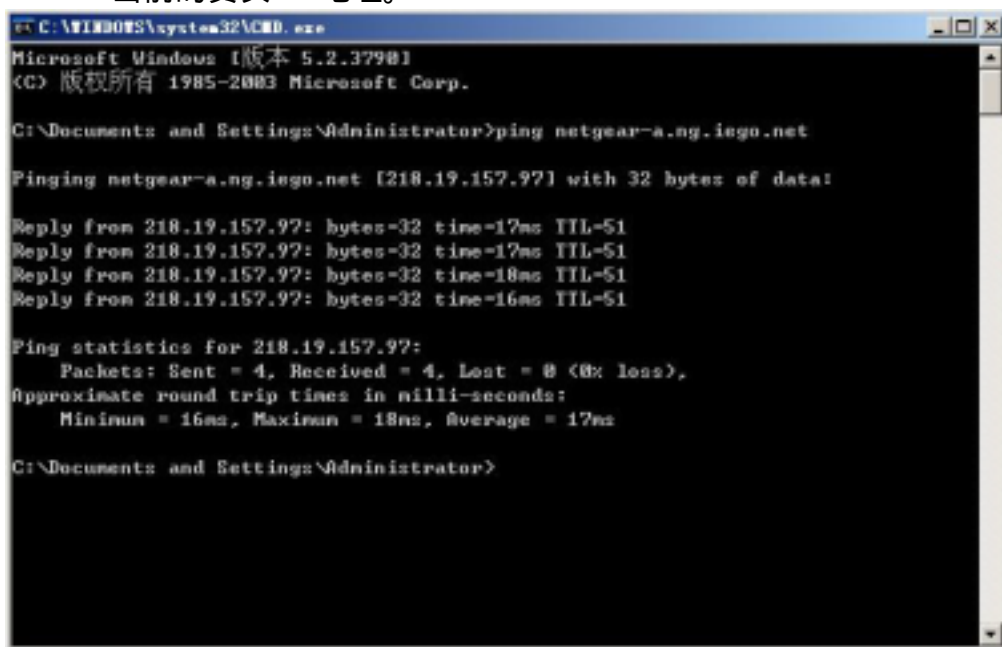
3. 验证动态域名的正确性能

- 查看当前的 IP 地址，如图在 Router Status 栏目里：



图五：动态域名的确认

- 用 PING 命令观察动态域名是否能够正确解释 IP 地址：
在 DOS 状态下面，用 ping netgear-a.ng.iego.net 观察解释出来的 IP 地址是否和 GATEWAY 当前的真实 IP 地址。



图六：动态域名的确认



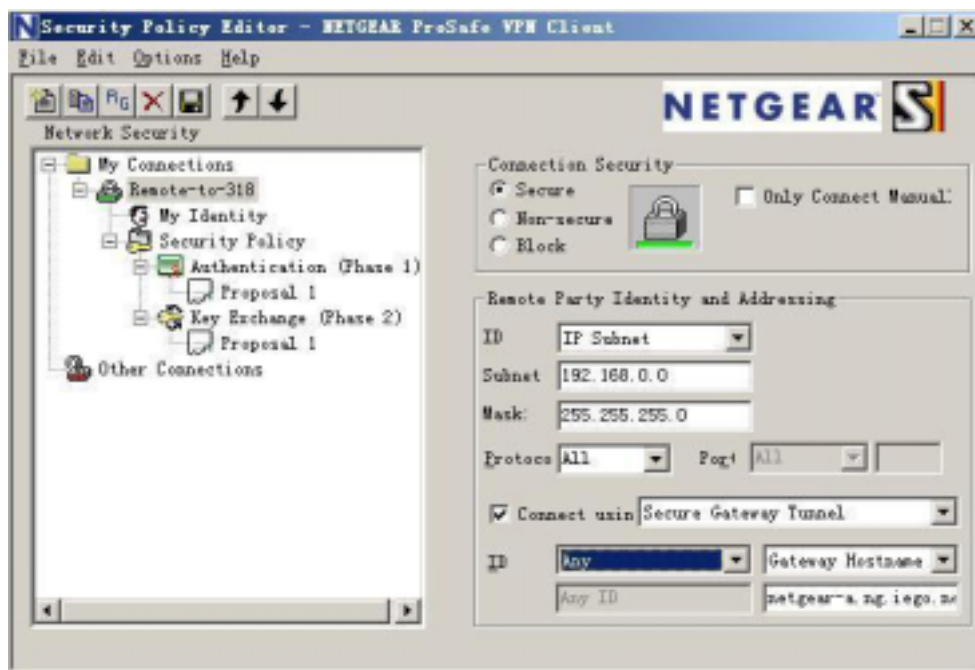
如上图，动态域名能够正确解释当前的 IP 地址，因此我们可以相信，动态域名已经建立了和 Gateway A 的关联。

4. 建立 VPN 策略

VPN 的配置策略可以参考 2.2 章节的介绍，是完全一样的，这里不再重复。

2.3.2 配置远程客户端动态的 VPN（Main 模式）

全部过程都可以参照章节 2.1 的介绍，只有一处不同，就是在 Remote Party Identity and Addressing 里面，将 ID 一项又原来的 IP Address 改为 Gateway Hostname 然后在输入对应的动态域名。如图所示：



图七：客户端软件的配置

设置好并及时保存配置。并在客户端一端ping 192.168.0.1 -t. 半分钟左右会通。证明VPN通道已建通。

如果通道建立成功，能在Route Status 工具栏中打开Show VPN Status中可以看到VPN的两个步骤已建通，如下图：

IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Inactive	remote-to-318	0.0.0.0	0.0.0.0/32		Idle	Drop
Active	remote-to-318_tmp7	218.20.177.201	218.20.177.201/32	ESP(3DES-CBC SHA-1)	[P1:A-Estab] [P2:Q-Estab]	Drop

图八：VPN通道建立的确



2.4 FVL328 to FVL328 (网关到网关 IKE Main 模式)

LAN-to-LAN 的 VPN (两边全固定 IP 的 VPN 的建立) 从 FVL328 to FVL328 (MAIN 模式)

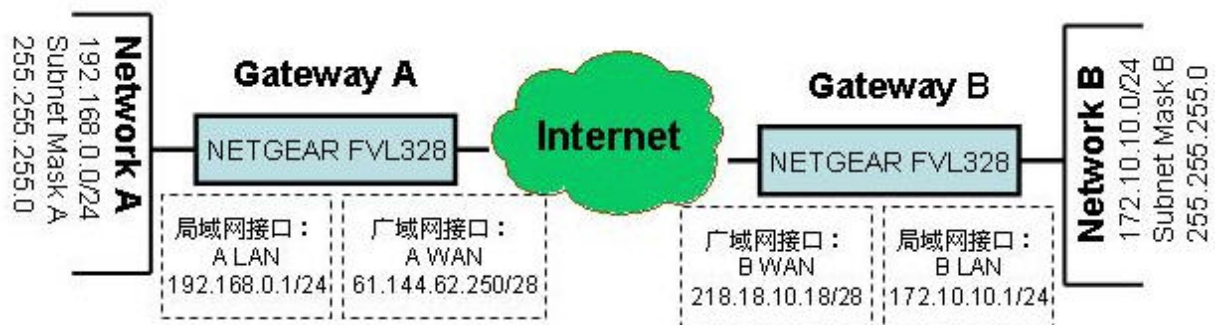
VPN 建立的模式 :	LAN-TO-LAN (FVL328-TO-FVL328 的 MAIN 模式)	
VPN 的类型	LAN-to-LAN 或是 Gateway-to-Gateway (Client-to-Gateway 另外讲)	
VPN 的加密:	利用 IKE 进行密钥交换和共享密钥方式 (而且可以通过 CA 认证方式) 建立 IPSEC 通道。	
产品型号和版本号:		
	NETGEAR-网关 A	FVL328 用的版本号是 Version 2.0 Release 02
	NETGEAR-网关 B	FVL328 用的版本号是 Version 2.0 Release 02
IP 地址的方式 :		
	NETGEAR-网关 A	由 ISP 提供的固定 IP 地址及网关和子网掩码。
	NETGEAR-网关 B	由 ISP 提供的固定 IP 地址及网关和子网掩码。

表一：建立动态VPN的LAN-TO-LAN的测试参数

这是个静态 (MAIN 模式) 的 LAN-TO-LAN 的 VPN 例子配置的过程。有关于 VPN 的一些原理可去参考最后一个章节的常用 VPN 专业术语或者登陆网站 www.vpnc.com 查询。这一过程的配置是根据实际情况来配置的。

VPN 构建的方式: Gateway-to-Gateway 利用共享密钥方式。

以下是一个静态 (MAIN 模式) 的 LAN-TO-LAN 的 VPN 的 gateway-to-gateway VPN , 利用共享加密和认证方式。



NETGEAR FVL328 Gateway A 的一端连接局域网一端的内部 IP 为 : LAN 192.168.0.0 /24。局域网接口的 IP 地址为 : 192.168.0.1/24, 和它连接的广域网接口是由 ISP 提供的固定 IP 地址及网关和子网掩码 , 在基础配置介面上输入信息。(见上图)

NETGEAR FVL328 的 Gateway B 的一端局域网的内部 IP 地址 IP 为 : LAN :172.10.10.0 /24。Gateway B 的广域网接口 (Internet) 配置由 ISP 提供的固定 IP 地址及网关和子网掩码。(见上图)。

这个 IKE 第一阶段的参数使用情况是:

- 主模式 (Main mode)
- 3DES的加密 (TripleDES)



- 算法是：MD5
- Key group 2 (1024 bits)
- pre-shared secret of "netgear2004"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

这个 IKE 第二阶段的参数使用是：

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- 选择所有的协议运行, 所有的端口, 使用 IPv4 子网掩码。从 172.10.10.0/24。

2.4.1 配置网关 A 固定 IP 地址的 VPN (MAIN 模式)

首先登录到 FVS318 的管理界面：

1. 在 IE 地址栏上输入, FVL328 的出厂值默认的 IP 地址：<http://192.168.0.1>。然后系统要要求你输入登陆的用户名和密码。用默认的用户名：**admin** 和 默认密码：**password**. 登陆到 FVL328。我们假定已设定好 LAN 接口、广域网接口的 IP 地址和子网掩码以及网关、DNS 服务器的 IP 地址。如下图：

图一：NETGEAR FVL328 v2.0 r02 VPN 设置。

2. 首先是配置 VPN 的 IKE Policies 策略了，链接到 VPN 工具栏上在图行设置的最左边 Settings 图示上。打开 IKE Policies 菜单，点击 Add，我们会见到新 IKE Policy 配置界面如下：



NETGEAR FVL328 ProSafe High-Speed VPN Firewall

settings

IKE Policy Configuration

General

Policy Name: to-GatewayA

Direction/Type: Both Directions

Exchange Mode: Main Mode

Local

Local Identity Type: WAN IP Address

Local Identity Data: 219.137.214.219

Remote

Remote Identity Type: Remote WAN IP

Remote Identity Data: 51.144.62.250

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

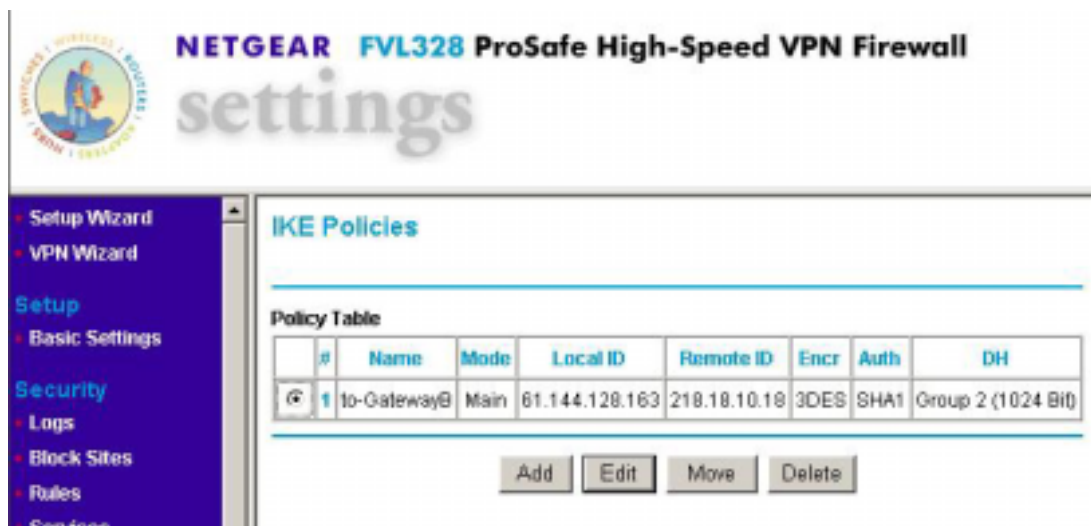
Authentication Method: ☒ Pre-shared Key

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

SA Life Time: 28800 (secs)

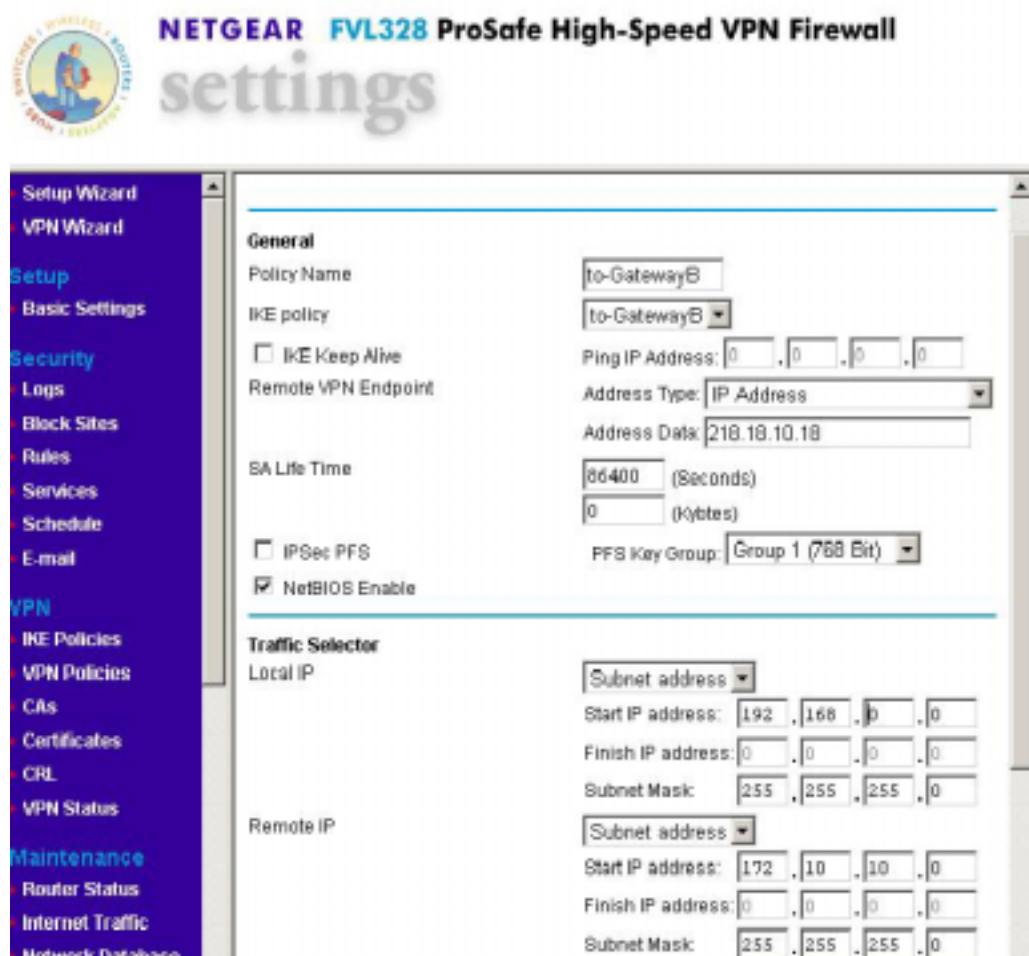
图二: NETGEAR FVL328 v2.0 R02 VPN Settings

- 在 **Policy Name** 字段中输入策略的属性名字. 这个名称不一定要与对端的 VPN 产品取名一样. 它的用途主要上用来帮助管理 IKE 策略的. 在这个例子中我们使用”to-Gateway A”来作为策略名称. 在 **Policy Name** 对话框中输入 to-GatewayB。
- 从这 **Direction/Type** 下拉对话框中, 选取 **Both Directions**。
- 从 **Exchange Mode** 模式的下拉菜单中, 选择 **Main Mode**。
- 从 **Local Identity Type** 下拉对话框中, 选择 **WAN IP Address**(在 **Local Identity Data** 对话框输入设备会自动找到广域网口的 IP 作为一个标识符)。
- 从 **Remote Identity Type** 下拉对话框中, 选择 **Remote WAN IP** (在 **Remote Identity Data** 对话框中会自动找到远端设备的广域网接口的 IP 地址作为一个标识符)。
- 从加密的算法 **Encryption Algorithm** 下拉框中, 选择 **3DES**。
- 从认证算法的 **Authentication Algorithm** 下拉对话框中, 选择 **MD5**。
- 再把认证方法 **Authentication Method** 按钮选上, 点击 **Pre-shared Key**。
- 在 **Pre-Shared Key field** 对话框中, 输入”Netgear2004”. 你必须确保两端网关设备的加密钥匙的一致性 (包括字母的大小写)。
- 再从 **Diffie-Hellman (DH) Group** 下拉对话框中, 选择 **Group 2 (1024 Bit)**。
- 在 **SA Life Time field** 对话框中, 输入 28800。
- 点击 **Apply** 按钮. 这就返回到 **IKE Policies** 的主菜单上。



图三：NETGEAR FVL328 v2.0 R02 VPN 设置之后的VPN返回的状态介面

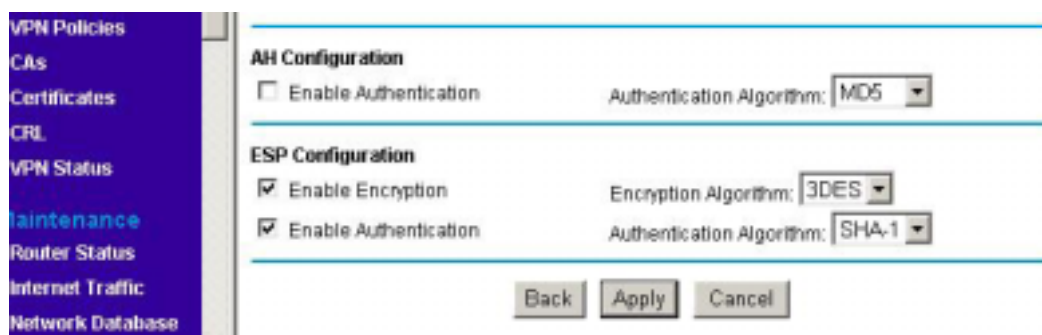
3. 在 VPN Policies 点击链接就可打开在 VPN 分类栏中，在左边的 Settings 图示管理界面中。我们来设置 VPN Policies 主界面的配置。点击 Add Auto Policy 的按钮。（如果是手动去配置 VPN 则是选择 Add Manual Policy）。然后我们就可看到新的配置界面 VPN – Auto Policy。



图四：NETGEAR FVL328 v2.0 R02 VPN Policy配置界面



- 输入一个统一的策略名。这个名称不一定要与远端的VPN设备取的名称相同。在这个例子中我们使用 "to-GatewayB" 来作为策略名。
- 在Policy Name字段对话框 中输入 "to-Gateway B" 。
- 再从 IKE policy下拉对话框中,选取我们定义好的IKE Policy。这里是"to-GatewayB作为IKE Policy。
- IKE Keep Alive可以使IKE始终保持在连接状态,默认不配置的。这样有利于增加VPN隧道的安全性。
- 再从 Remote VPN Endpoint Address Type 下拉对话框中,选取"IP Address"。
- 在 Address Date 对话框中输入Remote VPN Endpoint Address Date作为远端 Gateway A (218.18.10.18作为例子)。
- 在SA Life Time (Seconds) 对话框中输入默认86400。
- 在SA Life Time (Kbytes)对话框中输入默认为 0。
- 在 IPsec PFS 对话复选框中选上。。
- 从 PFS Key Group 下拉对话框中选取Group 1 (768 Bit)。
- 再从Traffic Selector Local IP 下拉框中选取 Subnet address作为配置。。
- 在 Start IP Address 填上本地LAN IP地址段作为网关B的可访问范围 (本例子中是：192.168.0.0)。。
- 在 Subnet Mask对话框中填上网关B的子网掩码(在本例中是：255.255.255.0)。
- 再从Traffic Selector Remote IP下拉对话框中选取 Subnet address.一项。
- 在这 Start IP Address字段上输入远端LAN IP地址作为网关A的可访问范围 (在本例中是：172.10.10.0)。
- 在Subnet Mask 字段上填上LAN 网关A的子网掩码 (在本例中是：255.255.255.0)。。

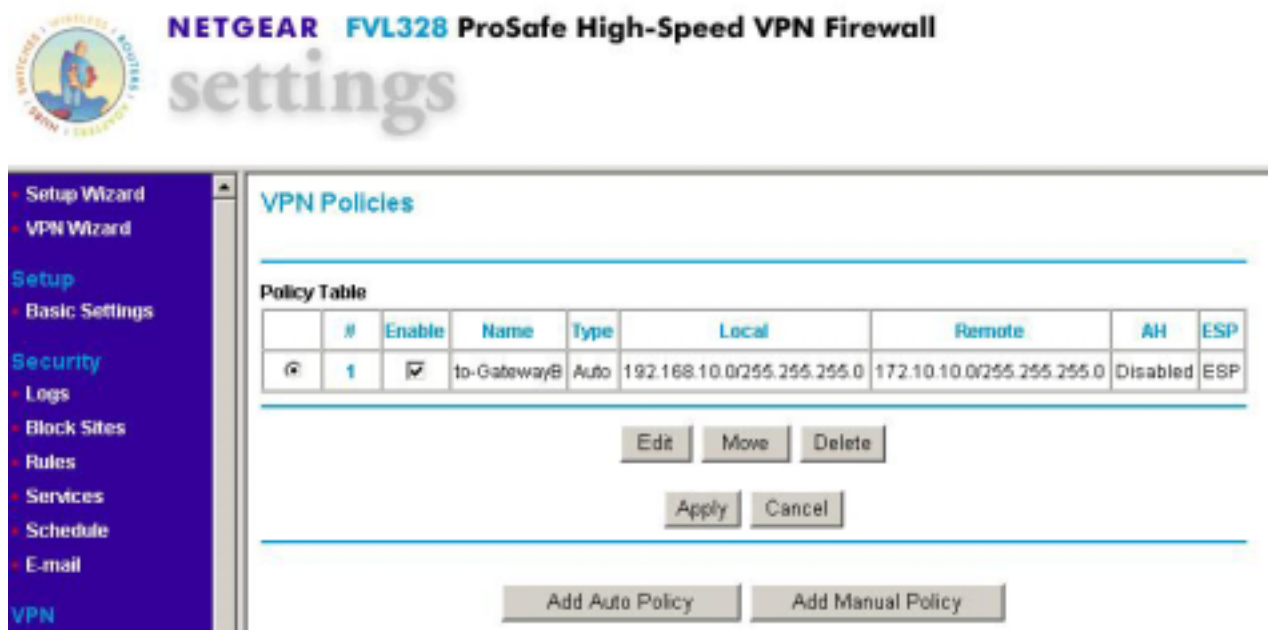


图五：NETGEAR FVL328 v2.0 R02 VPN Policy配置界面

- 必须选上Enable Encryption在 ESP Configuration Enable Encryption 的对话框。。
- 再从 ESP Configuration Encryption Algorithm 下拉对话框中选取3DES。
- 必须选上Enable Authentication 在 ESP Configuration Enable Authentication 的对话框中。
- 再从 ESP Configuration Authentication Algorithm 下拉对话框中选取SHA-1。。
- 可选上NETBIOS Enable的功能在NETBIOS Enable 复选框上。



- 点击Apply按钮。你会返回到 VPN Policies 主菜单的功能页面上。



图六：NETGEAR FVL328 v2.0 r02 VPN 策略菜单(Post Configuration)

4. 当返回到 VPN Policies的界面上, 要确保 Enable

2.4.2 配置网关 B 固定 IP 的 VPN (Main 模式)

首先登录到FVS318的管理界面：

1. 在IE地址栏上输入,FVL328的出厂值默认的IP地址：<http://192.168.0.1>。然后系统要要求你输入登陆的用户名和密码。用默认的用户名：**admin** 和 默认密码：**password**. 登陆FVL328。我们假定已设定好LAN接口、广域网接口的IP地址和子网掩码以及网关、DNS服务器的IP地址。如下图：



NETGEAR FVL328 ProSafe High-Speed VPN Firewall settings

VPN

- IKE Policies
- VPN Policies
- CAs
- Certificates
- CRL
- VPN Status

Maintenance

- Router Status
- Attached Devices
- Settings Backup
- Set Password
- Diagnostics
- Router Upgrade

Advanced

- Dynamic DNS
- LAN IP Setup
- Remote Management
- Static Routes

Basic Settings

Does Your Internet Connection Require A Login?

☒ No

☐ Yes

Account Name (If Required)

☒ Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

Domain Name Server (DNS) Address

☐ Get Automatically From ISP

☒ Use These DNS Servers

Primary DNS

Secondary DNS

Router's MAC Address

☒ Use Default Address

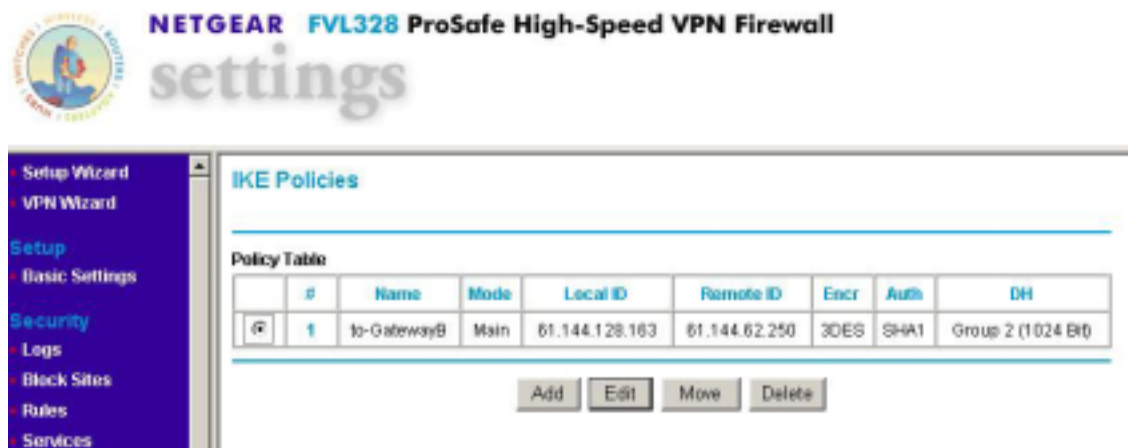
图七：NETGEAR FVL328 v2.0 r02 VPN 设置。

2. 首先是配置VPN的 IKE Policies策略了，链接到 VPN 工具栏里的IKE Policies 菜单. 点击 Add. 我们会见到新 IKE Policy配置界面如下：



图八：NETGEAR FVL328 v2.0 r02IKE Policy 配置

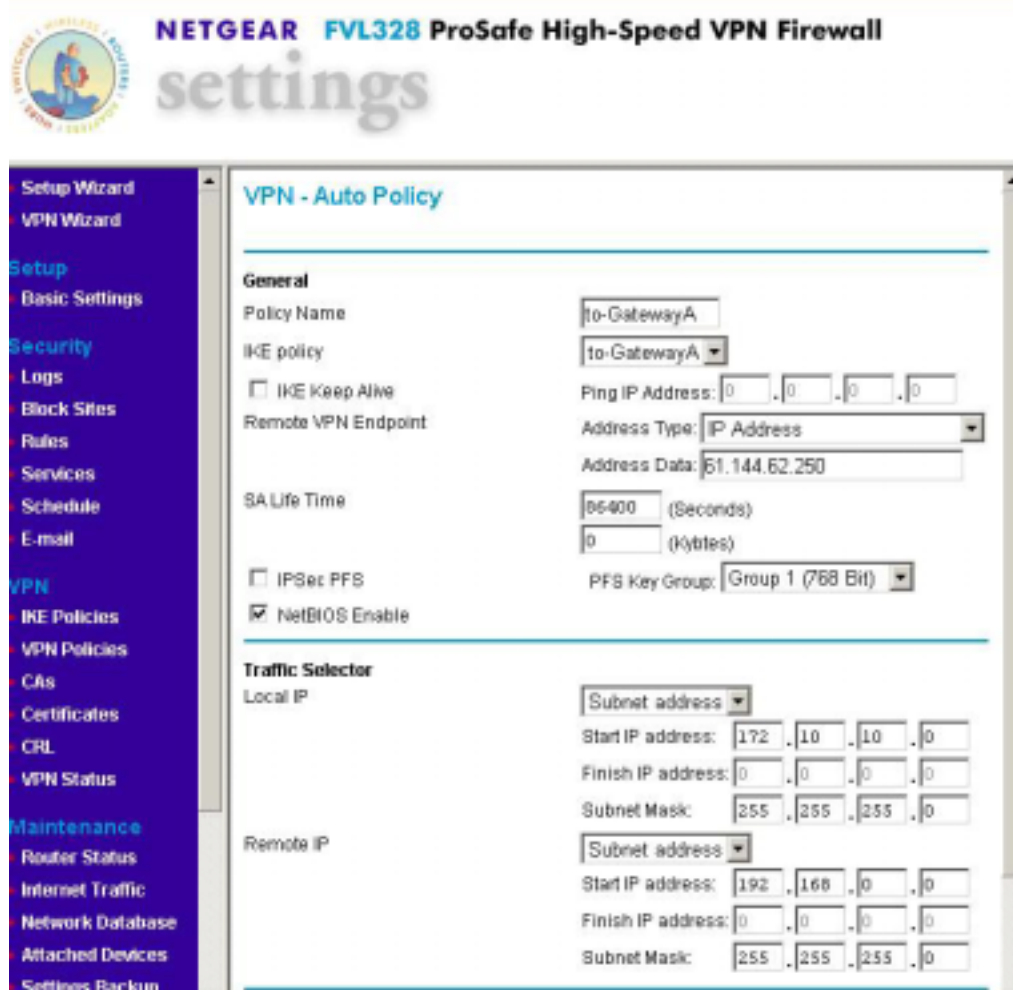
- 在 **Policy Name** 字段中输入策略的属性名字. 这个名称不一定要与对端的 VPN 产品取名一样. 它的用途主要上用来帮助管理 IKE 策略的. 在这个例子中我们使用“to-GatewayA”来作为策略名称. 在 **Policy Name** 对话框中输入 to-GatewayA.
- 从这 **Direction/Type** 下拉对话框中，选取 **Both Directions**.
- 从 **Exchange Mode** 模式的下拉菜单中，选择 **Main Mode**.
- 从 **Local Identity Type** 下拉对话框中，选择 **WAN IP Address** (在 **Local Identity Data** 对话框输入设备会自动找到广域网口的 IP 作为一个标识符)。
- 从 **Remote Identity Type** 下拉对话框中，选择 **Remote WAN IP** (在 **Remote Identity Data** 对话框中会自动找到远端设备的广域网接口的 IP 地址作为一个标识符)。
- 从加密的算法 **Encryption Algorithm** 下拉框中，选择 **3DES**.
- 从认证算法的 **Authentication Algorithm** 下拉对话框中，选择 **SHA-1**.
- 再把认证方法 **Authentication Method** 按钮选上，点击 **Pre-shared Key**.
- 在 **Pre-Shared Key field** 对话框中，输入 “Netgear2004”. 你必须确保两端网关设备加密钥匙是一至的（包括字母的大小写）。
- 再从 **Diffie-Hellman (DH) Group** 下拉对话框中，选择 **Group 2 (1024 Bit)**。
- 在 **SA Life Time field** 对话框中，输入 **28800**。
- 点击 **Apply** 按钮. 这就返回到 **IKE Policies** 的主菜单。



图九：NETGEAR FVL328 v2.0 r02 IKE Policies 配置返回的菜单

这是 FVL328 IKE Policy 显示的就是 IKE Policies 主菜单介面。

3. 在 VPN 分类栏在点击 VPN Policies 链接可打开配置界面。点击 Add Auto Policy 的按钮。（如果是手动去配置 VPN 则是选择 Add Manual Policy）。然后我们就可看到新的配置界面 VPN - Auto Policy。



图十：NETGEAR FVL328 VPN v2.0 r02 – 自动策略配置。



- 输入一个统一的策略名来。这个名称不一定要与远端的VPN设备取的名称相同。在这个例子中我们使用 "to-GatewayA" 来作为策略名。在Policy Name字段对话框 中输入 "to-GatewayA"。
- 再从 IKE policy下拉对话框中,选取我们定义好的IKE Policy：这里是 "to-GatewayA" 作为IKE Policy。
- 再从 Remote VPN Endpoint Address Type 下拉对话框中，选取"Ip Address"。
- 在 Address Date 对话框中输入Remote VPN Endpoint Address Date作为远端 Gateway A (61.144.62.250作为例子)。
- 默认在SA Life Time (Seconds) 对话框中输入86400。
- 默认在SA Life Time (Kbytes) 对话框中输入 0。
- 在 IPSec PFS 对话复选框中选上。
- 从 PFS Key Group 下拉对话框中选取Group 1 (768 Bit)。
- 再从Traffic Selector Local IP 下拉框中选取 Subnet address作为配置。
- 在 Start IP Address 填上，输入本地LAN IP地址作为网关B可以访问的地址范围 (本例子中是：172.10.10.0)。
- 在 Subnet Mask对话框中填上输入网关B的子网掩码(在本例中是：255.255.255.0)。
- 再从Traffic Selector Remote IP下拉对话框中选取 Subnet address.一项。
- 在这 Start IP Address字段上，输入远端LAN IP地址作为网关A可访问IP地址范围 (在本例中是：192.168.0.0)。
- 在这Subnet Mask 字段上输入LAN 网关A的子网掩码 (在本例中是：255.255.255.0)。

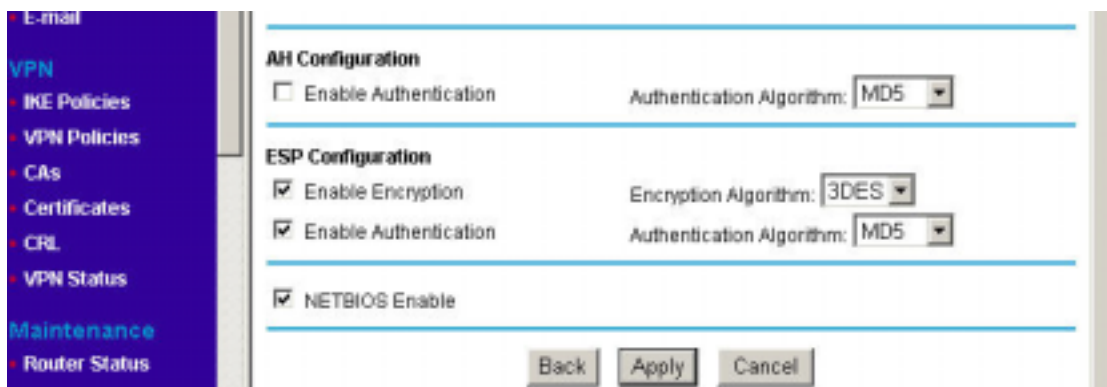
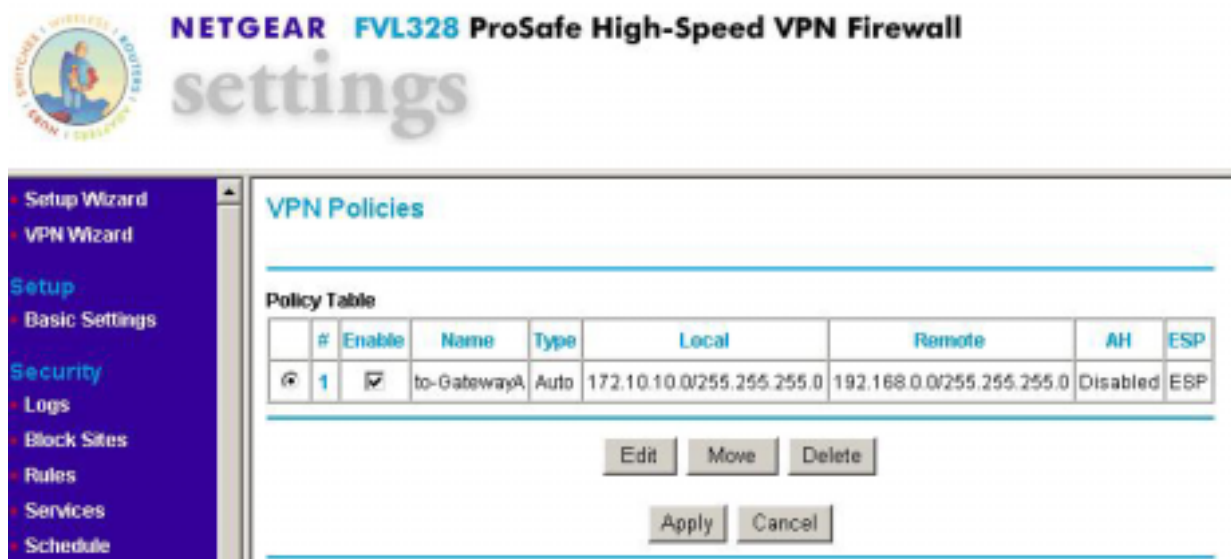


图 十一: NETGEAR FVL328 VPN v2.0 r02 –自动策略

- 再从 AH Configuration Authentication Algorithm 下拉框中,选 上SHA-1, 在方框中不能选上。
- 必须选上Enable Encryption在 ESP Configuration Enable Encryption 的对话框。
- 再从 ESP Configuration Encryption Algorithm 下拉对话框中选取3DES。
- 必须在 ESP Configuration Enable Authentication 的对话框中选上Enable Authentication。
- 再从 ESP Configuration Authentication Algorithm 下拉对话框中选取MD5。
- 可选上NETBIOS Enable的功能在NETBIOS Enable 复选框上。



- 点击Apply按钮。你会返回到 VPN Policies 主菜单的功能页面上。

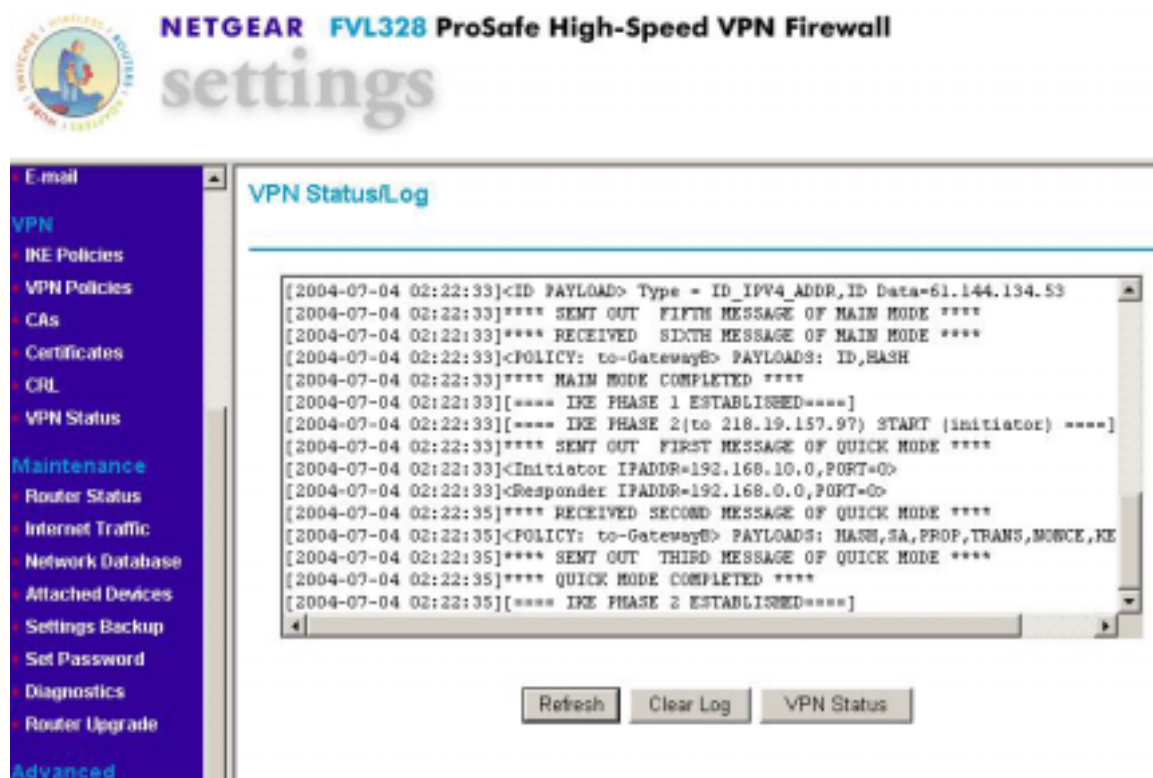


图十二：NETGEAR FVL328 v2.0 r02 VPN 策略菜单(Post Configuration)

4. 当返回到 VPN Policies的介面上，要确保 Enable 对话框要选上，

当Gateway A和 Gateway B两端的VPN创建好之后，在两端的任一端局域网上PING对方的局域网客户端。例如：ping 172.10.10.1 -t. 或 ping 192.168.0.1 -t半分钟左右会通，证明VPN通道已建通。

半分钟之后可以可以看到FVL328的VPN已经连通的状态。见下图：



图十三：NETGEAR FVL328 v2.0 r02 VPN 建立的确定



2.5 Remote to FVL328 (客户端到网关 Aggressive 模式)

一边是固定 IP 另一端是拨号移动用户的建立)的 VPN 从 Remote to FVL328 (我们只建议 Remote 到 Gateway 采用 Aggressive 模式建立 VPN)

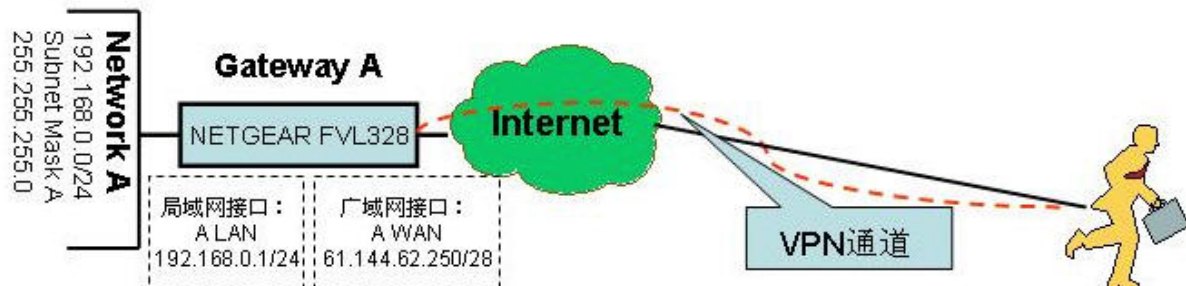
VPN 建立的模式：	Remote-TO-LAN (Remote-TO-FVL328 的 MAIN 模式和 Aggressive 模式)	
动态 VPN 的类型	Client-to-Gateway(LAN-to-LAN 和 Gateway-to-Gateway)另有讲	
建立动态 VPN 的加密:	利用 IKE 进行密钥交换和共享密钥方式 (不是能过 CA 认证方式) 建立 IPSEC 通道	
产品型号和版本号：		
NETGEAR-网关 A	FVL328 用的版 本号是 version 2.0 Release 02	
移动用户	Netgear Prosafe vpn client 版本是 version 10.1.1	
IP 地址的方式：		
NETGEAR-网关 A	由 ISP 提供的固定 IP 地址及网关和子网掩码	
移动用户	通过多种方式只要能上互联网即 OK	

表一：建立动态VPN的LAN-TO-LAN的测试参数

这个 Remote-to-LAN 的 VPN 例子配置的过程。有关于 VPN 的一些原理可去参考最后一个章节的常用 VPN 专业术语或者登陆网站 www.vpnc.com 查询。这里给出例子的配置是根据实际情况进行的。

VPN 构建的方式: Remote-to-Gateway 利用共享密钥方式。

以下的一个静态 (Aggressive 模式) 的 Remote-TO-LAN 的 VPN , 利用共享加密和认证方式建立 VPN 通道。



NETGEAR FVL328 Gateway A 连接局域网一端的内部 IP 为：LAN 192.168.0.0/24. 局域网接口的 IP 地址为：192.168.0.1/24, 广域网的 IP 地址由 ISP 自动分配。移动用户即要连入当地的 ISP 能上网即可。具体网络结构如上图。

2.5.1 配置 FVL328 的远程接入 VPN (Aggressive 模式)

首先登录到FVS318的管理界面：

1. 在IE地址栏上输入,FVL328的出厂值默认的IP地址：<http://192.168.0.1>。然后系统要要求你输入登陆的用户名和密码。用默认的用户名：**admin** 和 默认密码：**password**. 登陆到FVL328。我们假定已设定好LAN接口、广域网接口的IP地址和子网掩码以及网关、DNS服务器的IP地址。如下图：

**NETGEAR FVL328 ProSafe High-Speed VPN Firewall****settings**

图一:NETGEAR FVL328 v2.0 r02 VPN 设置。

2. 首先是配置 VPN 的 IKE Policies 策略了 , 链接到 VPN 工具栏, 打开里面的的 IKE Policies 菜单. 点击 Add . 我们会见到新 IKE Policy 配置介面如下 : .



NETGEAR FVL328 ProSafe High-Speed VPN Firewall settings

IKE Policy Configuration

General

Policy Name: Remote-328

Direction/Type: Remote Access

Exchange Mode: Aggressive Mode

Local

Local Identity Type: Fully Qualified Domain Name

Local Identity Data: fv1_local

Remote

Remote Identity Type: Fully Qualified Domain Name

Remote Identity Data: fv1_remote

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ☒ Pre-shared Key

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

SA Life Time: 28800 (secs)

Buttons: Back, Apply, Cancel

图二 :NETGEAR FVL328 v2.0 r02 IKE Policy 配置

- 在Policy Name 字段中输入策略的属性名字. 这个名称不一定要与对端的VPN产品取名一样 它的用途主要上用来帮助管理IKE策略的。在这个例子中我们使用 ” Remote-328 ” 来作为策略名称。在 Policy Name对话框中输入”Remote-328”
- 从这 Direction/Type 下拉对话框中，选取 Remote Access。
- 从Exchange Mode 模式的下拉菜单中，选择Aggressive Mode。
- 从 Local Identity Type下拉对话框中，选择 Fully Qualified Domain Name(在Local Identity Data 对话框输入与FVL328对应的fv1_local作为一个标识符。)
- 从Remote Identity Type 下拉对话框中, 选择Fully Qualified Domain Name (在Remote Identity Data 对话框中输入与FVL328对应的fv1_remote作为一个标识符。)
- 从加密的算法 Encryption Algorithm 下拉框中, 选择3DES。
- 从认证算法的 Authentication Algorithm 下拉对话框中, 选择SHA-1。再把认证方法 Authentication Method 按钮选上, 点击 Pre-shared Key。



- 在 **Pre-Shared Key field**对话框中, 输入 " Netgear2004 " . 你必须确保两端网关设备有加密 KEY是一至的 (包括字母的大小写) 。再从 **Diffie-Hellman (DH) Group** 下拉对话框中, 选择 **Group 2 (1024 Bit)**。
- 在 **SA Life Time field**对话框中, 输入180。
- 点击 **Apply** 按钮. 这就返回到**IKE Policies** 的主菜单上。

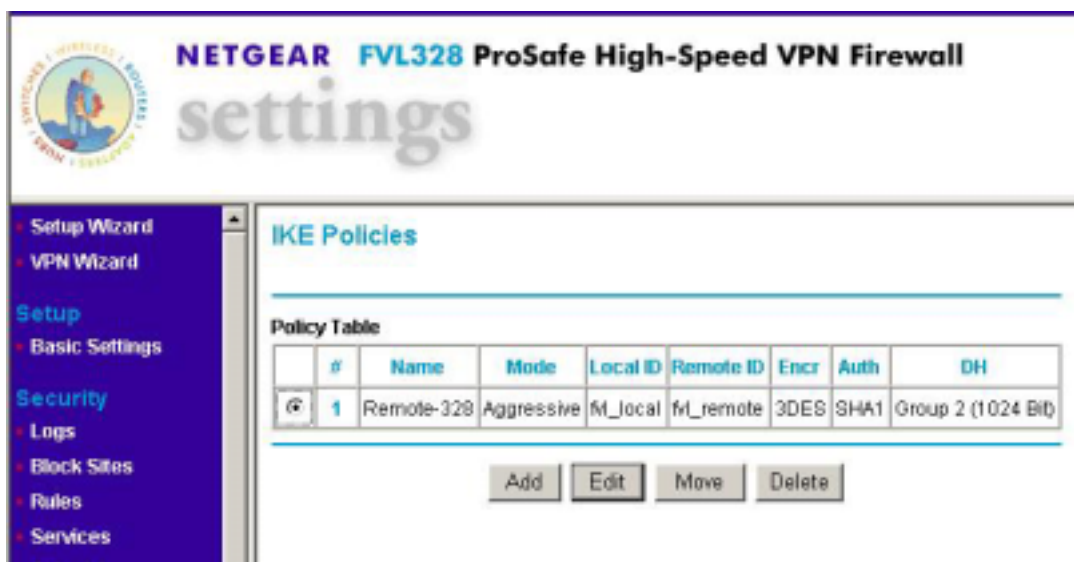


图 三 : NETGEAR FVL328 v2.0 r02 IKE Policies 配置返回的菜单

3. 在左边的 Settings图示管理界面中, 打开VPN分类栏中链接就可点击VPN Policies , 我们来设置 VPN Policies 主界面的配置。 点击 **Add Auto Policy**的按钮. (如果是手动去配置VPN则是选择**Add Manual Policy** , 一般过程比较复杂 , 这里不作推荐) . 然后我们就可看到新的配置界面**VPN – Auto Policy** .

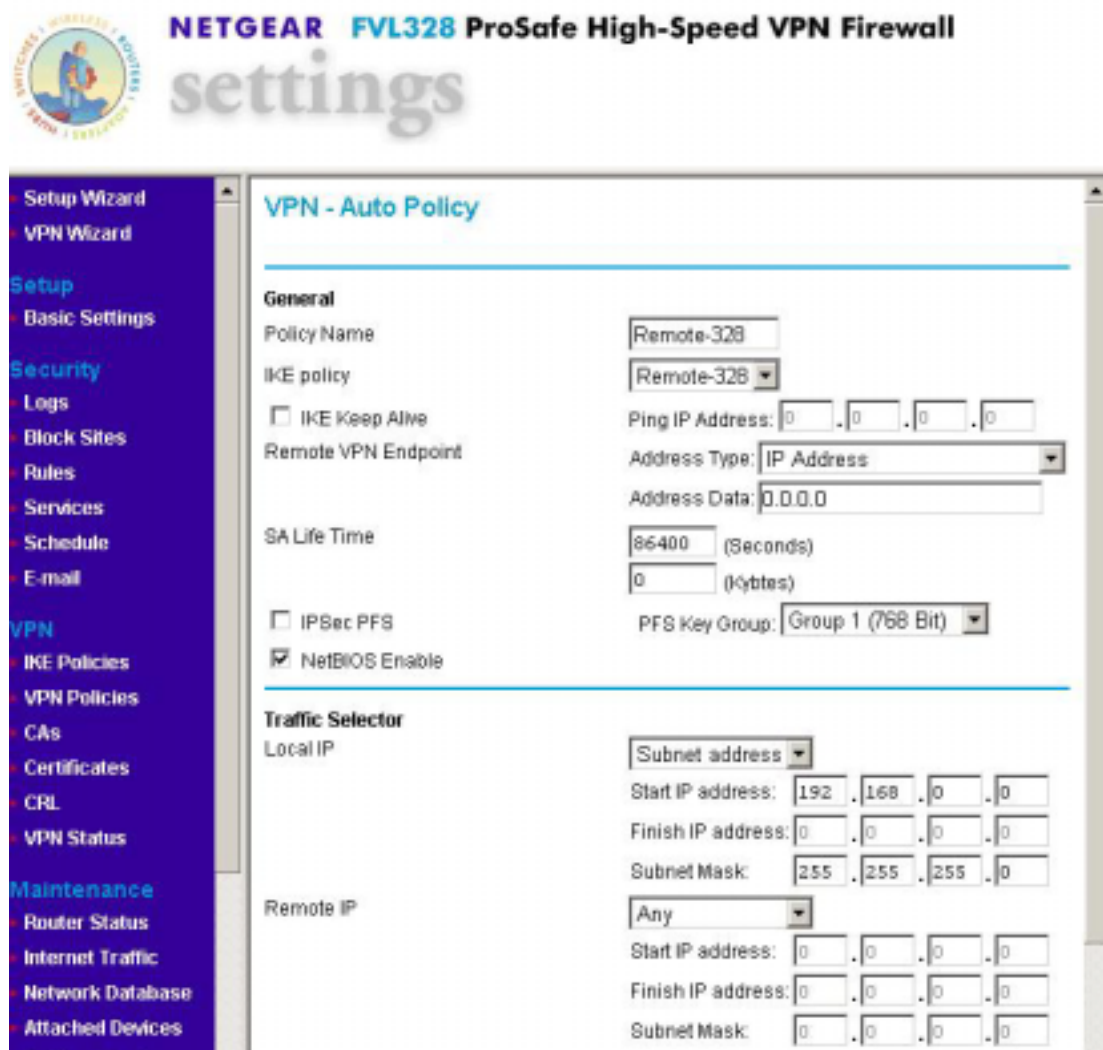
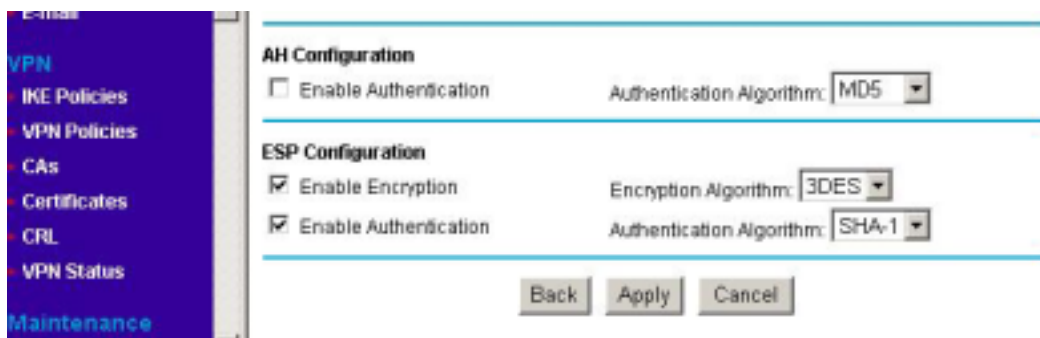


图 四：NETGEAR FVL328 VPN v2.0 r-2- 自动策略配置。

- 输入一个统一的策略名。这个名称不一定要与远端的VPN设备取的名称相同。在这个例子中我们使用 “Remote-328” 来作为策略名。在Policy Name字段对话框 中输入 “Remote-328”。
- 再从 IKE policy下拉对话框中, 选取我们先定义好的IKE Policy– 这里是”Remote-328”作为IKE Policy.
- 再从 Remote VPN Endpoint Address Type 下拉对话框中，选 取”Ip Address”。
- 在Remote VPN Endpoint Address Date中输入0.0.0.0作为远端 Gateway B的Ip Address。
- 默认在SA Life Time (Seconds) 对话框中输入86400。
- 默认在SA Life Time (Kbytes) 对话框中为输入0。
- 在 IPSec PFS 对话框复选框中选中。
- 从 PFS Key Group 下拉对话框中选取Group2(1024Bit).
- 再从Traffic Selector Local IP 下拉框中选取 Subnet address作为配置。
- 输入本地LAN IP地址作为网关B的范围在 Start IP Address 填上。(本例子中是：192.168.0.0)

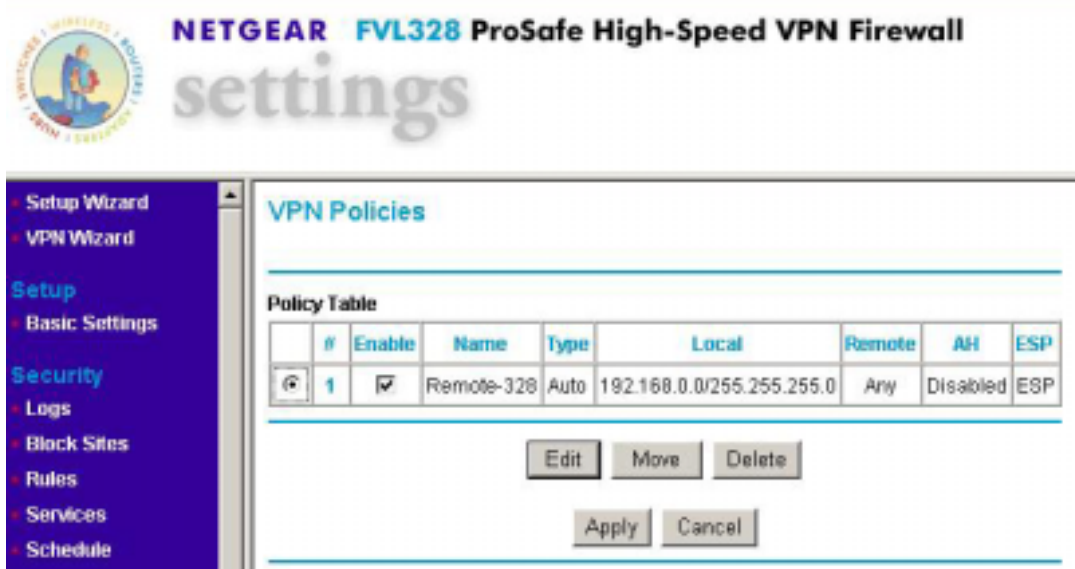


- 输入网关B的子网掩码(在本例中是：255.255.255.0) 在 Subnet Mask对话框中填上。
- 再从Traffic Selector Remote IP下拉对话框中选取 ANY一项。



图五：NETGEAR FVL328 VPN v2.0 r02-自动策略

- 再从 AH Configuration Authentication Algorithm 下拉框中, 选上 MD5. , 在方框中不能选上。
- 必须选上Enable Encryption在 ESP Configuration Enable Encryption 的对话框。 .
- 再从 ESP Configuration Encryption Algorithm 下拉对话框中选取3DES.
- 必须选上Enable Authentication 在 ESP Configuration Enable Authentication 的对话框中。
- 再从 ESP Configuration Authentication Algorithm 下拉对话框中选取SHA-1。 .
- 可选上NETBIOS Enable的功能在NETBIOS Enable 复选框上。
- 点击Apply按钮。你会返回到 VPN Policies 主菜单的功能页面上。



图六：NETGEAR FVL328 v2.0 r02 VPN 策略菜单(Post Configuration)

4. 当返回到 VPN Policies的介面上, 要确保 Enable 对话框要选上。

2.5.2 配置远程客户端的静态 VPN (Aggressive 模式)。

1. 首先在移动用户的电脑上装好Netgear Prosafe VPN Client v 10.1.1的客户端软件。



2. 打开Netgear Prosafe VPN Client v 10.1.1的客户端软件的Security Policy Edit。

- 客户端的配置软件如下：

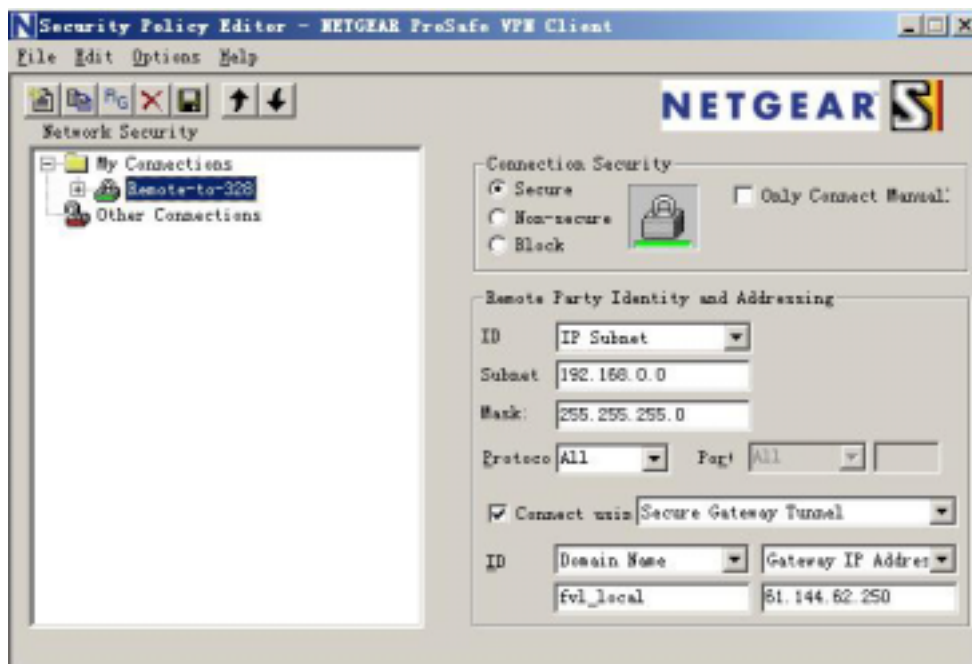


图 六：客户端软件的配置

- 选择客户端的模式（Aggressive Mode模式）。

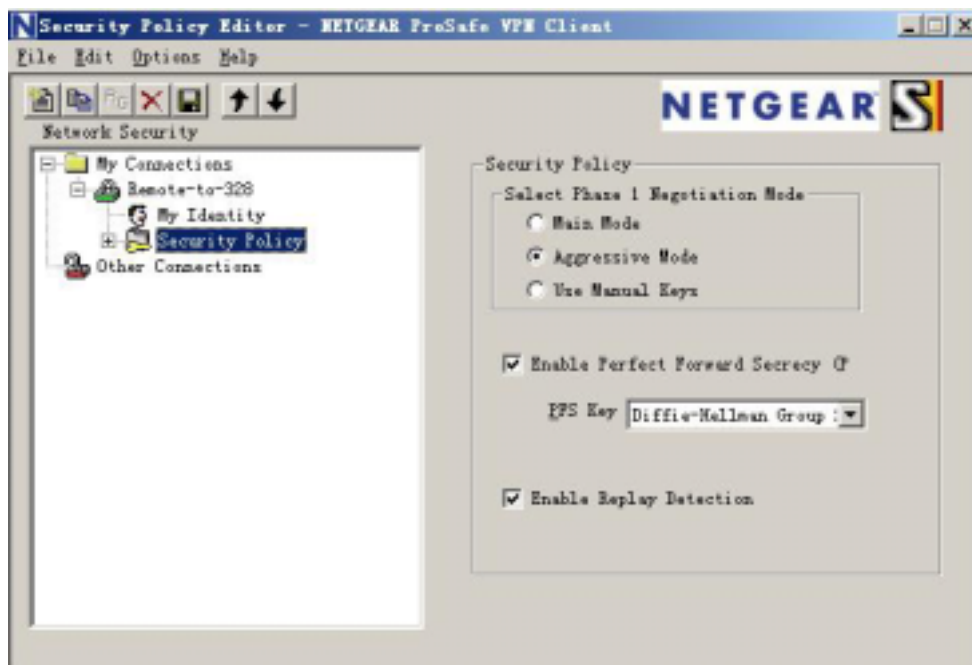


图 七：客户端软件的配置



- 打开My Identity 对话框，编辑Pre-Shared-Key。输入与318对应的密码：“netgear2004”。如图：



图 八：客户端软件的配置

- 在My Identity 对话框里，填入My Identity 信息，这里填入的认证信息必须和Gateway A里所设置的Remote Identity信息相一致。

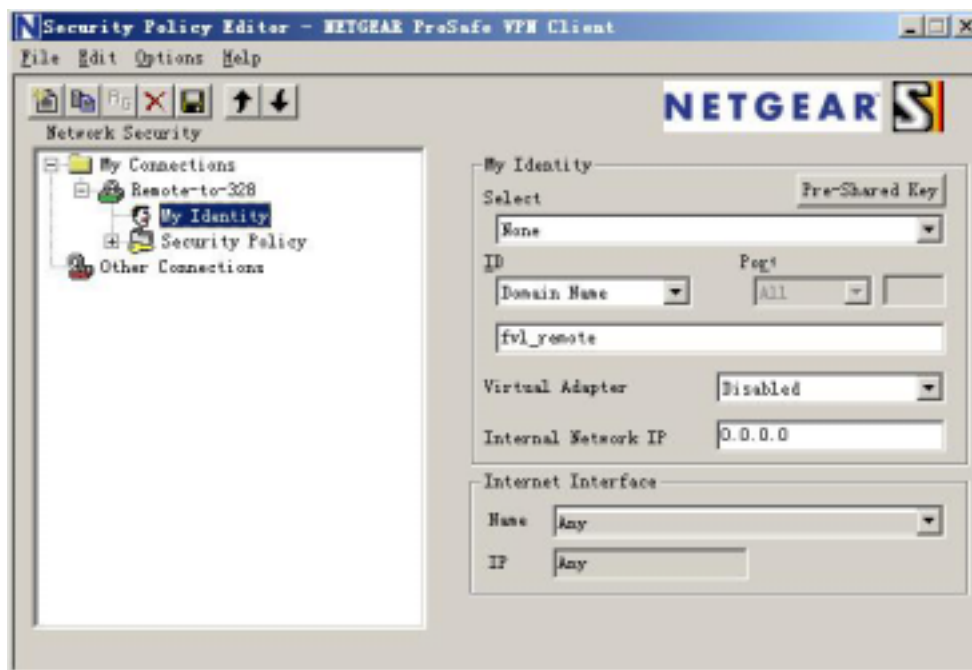
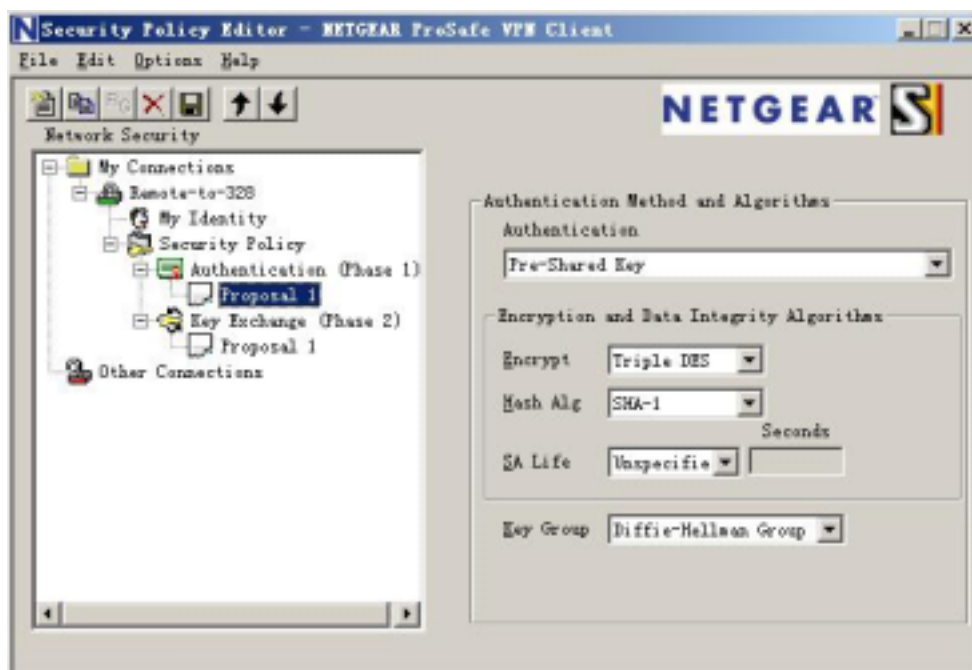


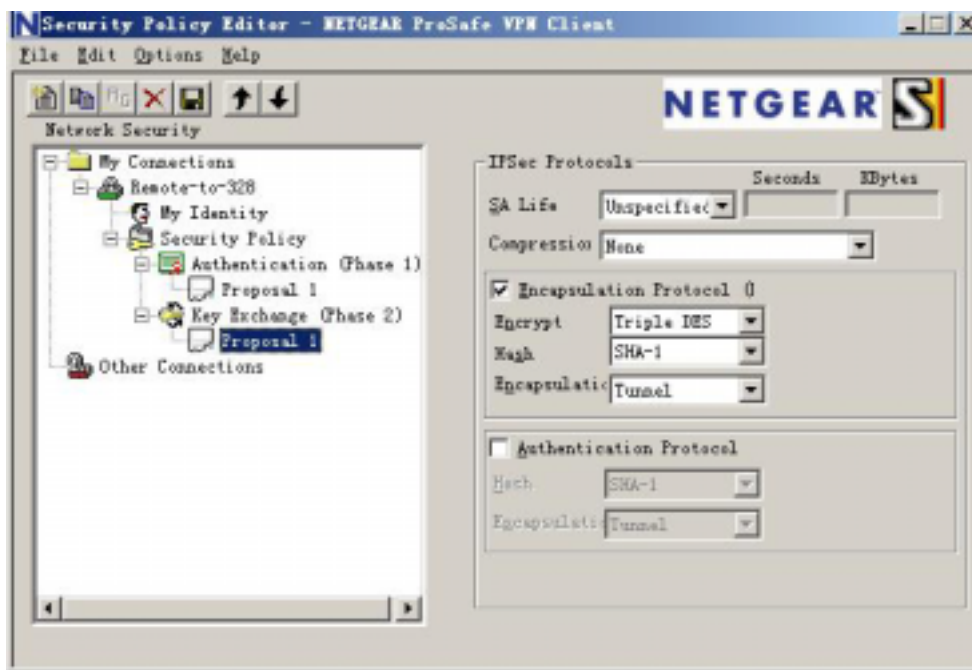
图 八：客户端软件的配置



- 分别建立 VPN 证和加密的两个步骤规则：



图九：客户端软件的配置



图十：客户端软件的配置

3. 设置好并及时保存配置。并在客户端一端 ping 192.168.0.1 -t.半分钟左右会通。证明 VPN 通道已建通。



如果通道建立成功，能在VPN 工具栏中打开VPN Status中可以看到VPN的两个步已建通，如下图：

IPSec Connection Status

#	Policy Name	Endpoint	Tx (KBytes)	State	Action
1	Remote-328-1	218.20.176.129	260072	Phase 1: M-ESTABLISHED / Phase 2: ESTABLISHED	Drop

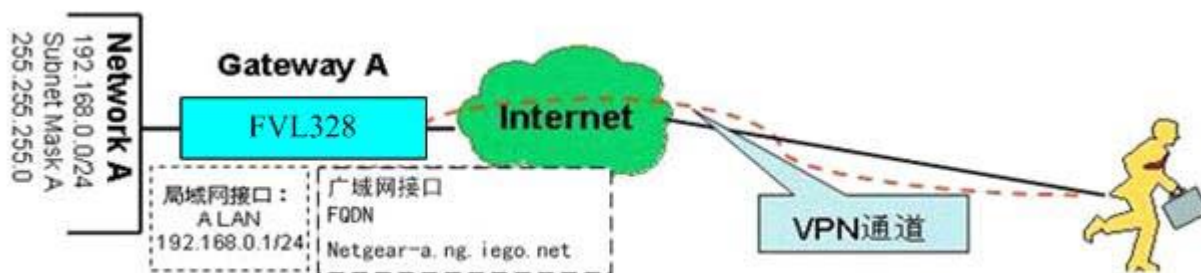
图 十一：客户端软件的配置



2.6 Remote to FQDN FVL328(IKE Aggress 模式网关为动态 IP)

有关动态域名的描述请参考上面的章节 2.3 的介绍。

在此我们仍然以 2.5 章节里的环境为例子，所不同的是在 2.5 的例子中中心 FVL328 采用的是固定的 IP 地址，而在我们当前的环境中，FVL328 采用的是动态拨号上网方式，并没有固定的 IP 地址，需要申请固定的动态域名。

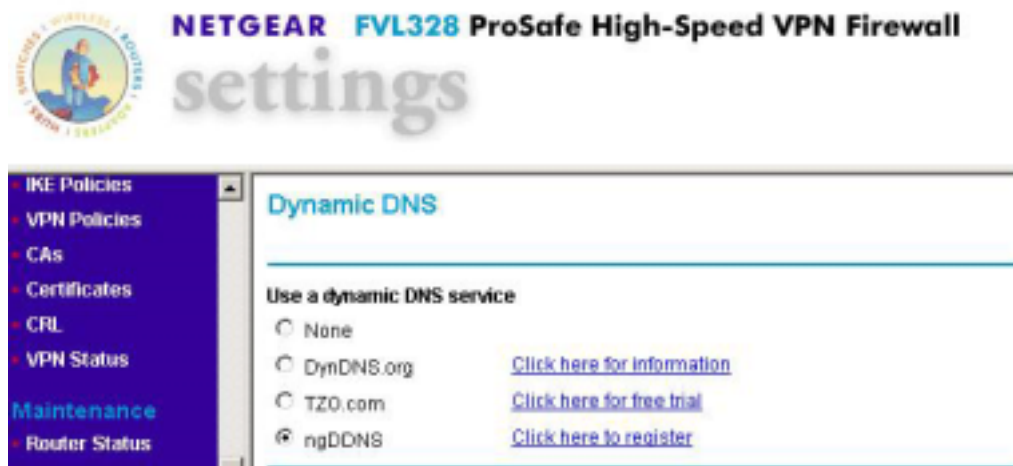


具体设置方法如下：

2.6.1 配置 FVL328 的动态的（Aggressive 模式）VPN。

1. 申请动态域名：

在我们的网站里注册自己的动态域名：



图一：动态域名的申请

- 点击 ngDDNS 所在的连接，将引导我们进入动态域名服务的注册页面。



图二：动态域名的申请

- 点击注册，在用户名称一栏输入自己的用户名（注意：输入的用户名将作为动态域名的前缀，我们提供的动态域名格式为：用户名.ng.iego.net）。在用户密码里输入密码再确认重复输入一次，即完成对动态域名的注册。



图三：动态域名的申请



2. 在 Gateway A (FVS318) 上启动动态域名服务：

- 在 DDNS 选项里，先选中适当的服务提供商，在中国大陆我们应该选择 Oray.net（网域科技），然后在相应的信息栏目里填入相应的注册信息即可。如下图：在我们的例子里，我们为站点 A 申请了，名为 Netgear-a.ng.iego.net 的动态域名。

NETGEAR FVL328 ProSafe High-Speed VPN Firewall settings

Dynamic DNS

Use a dynamic DNS service

☐ None

☐ DynDNS.org [Click here for information](#)

☐ TZO.com [Click here for free trial](#)

☒ ngDDNS [Click here to register](#)

ngDDNS

Host and Domain Name: netgear-a.ng.iego.net
example: youname.ng.iego.net

Account Name: netgear-a

Password: *****

Apply Cancel Show Status

图 四：动态域名的启用

3. 验证动态域名的正确性能

- 在 Dynamic Dns 里面，点击 Show Status 按钮。以下是成功登陆的信息。

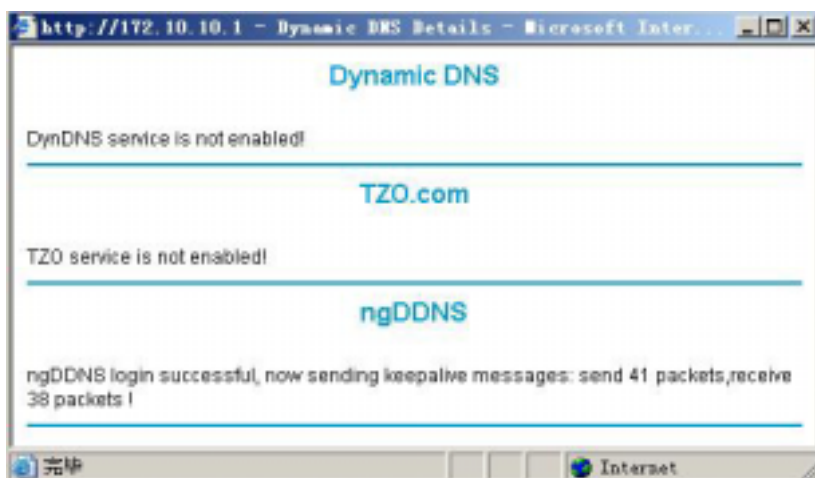


图 五：动态域名解释的确定



4. 建立 VPN 策略

VPN 的配置策略可以参考 2.5 章节的介绍，是完全一样的，这里不再重复。

2.6.2 配置远程客户端的动态的 VPN（Aggressive 模式）

全部过程都可以参照章节 2.5 的介绍，只有一处不同，就是在 Remote Party Identity and Addressing 里面，将 ID 一项由原来的 IP Address 改为 Gateway Hostname。然后再输入对应的动态域名。如图所示：

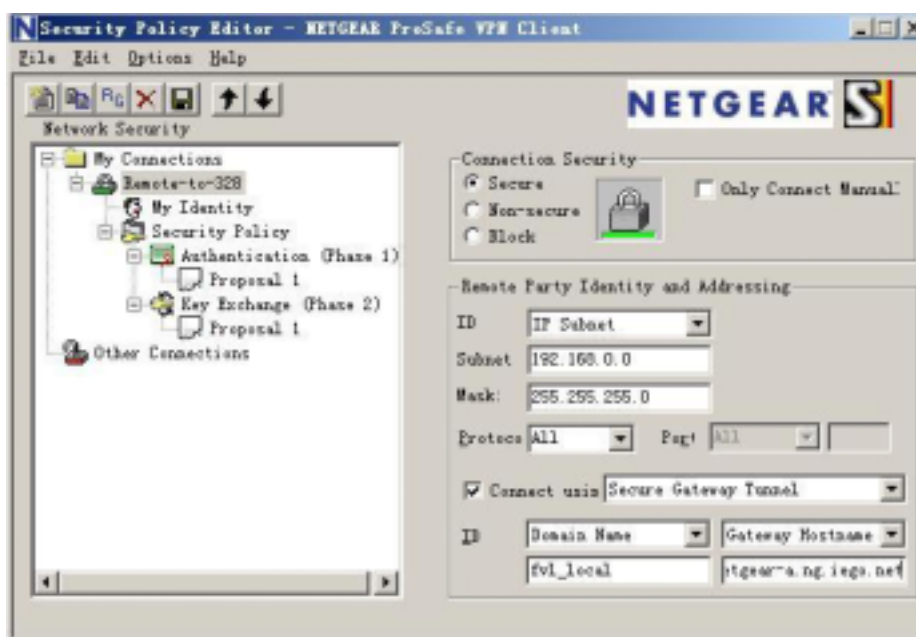


图 五：客户端软件的配置

设置好并及时保存配置。并在客户端一端 ping 192.168.0.1 -t. 半分钟左右会通。证明 VPN 通道已建通。

如果通道建立成功，能在 Route Status 工具栏中打开 Show VPN Status 中可以看到 VPN 的两个步骤已建通，如下图：

IPSec Connection Status					
#	Policy Name	Endpoint	Tx (KBytes)	State	Action
1	Remote-328-1	218.20.176.129	260072	Phase 1: M-ESTABLISHED / Phase 2: ESTABLISHED	Drop

图 六：VPN 通道建立的确定



2.7 FVS318 to FVL328 (网关到网关 IKE Main 模式)

从 FVS318 to FVL328 建立 LAN-to-LAN 的 VPN (两边全固定 IP , MAIN 模式)

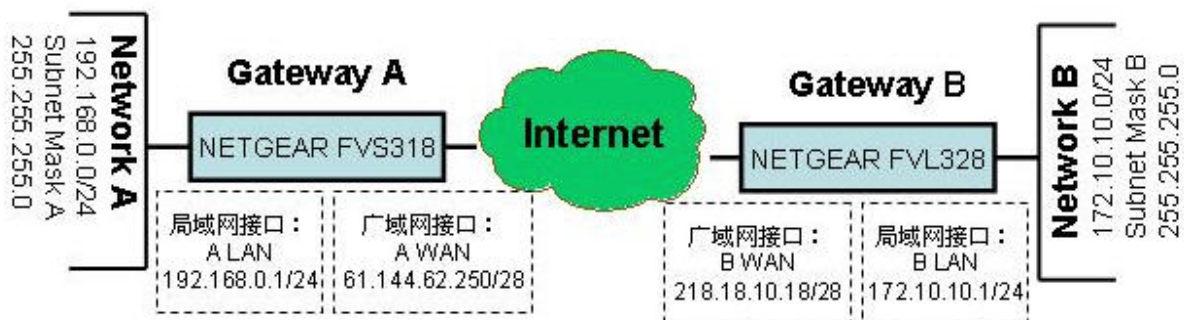
VPN 建立的模式 :	LAN-TO-LAN (FVS318-TO-FVS318 的 MAIN 模式)
VPN 的类型	LAN-to-LAN 或是 Gateway-to-Gateway (Client-to-Gateway 另有讲)
建立动态 VPN 的加密:	利用 IKE 进行密钥交换和共享密钥方式 (不能通过 CA 认证方式) 建立 IPSec 通道。
产品型号和版本号:	
NETGEAR-网关 A	FVS318 用的版本号是 version 2.3
NETGEAR-网关 B	FVL328 用的版本号是 version 2.0 Release 02
IP 地址的方式 :	
NETGEAR-网关 A	由 ISP 提供的固定 IP 地址及网关和子网掩码。
NETGEAR-网关 B	由 ISP 提供的固定 IP 地址及网关和子网掩码。

表一:建立动态VPN的LAN-TO-LAN的测试参数

这个静态 (MAIN 模式) 的 LAN-TO-LAN 的 VPN 例子配置的过程。有关于 VPN 的一些原理可去参考最后一个章节的常用 VPN 专业术语或者登陆网站 www.vpnc.com 查询。这一过程的配置是根据实际情况来配置的。

VPN 构建的方式: Gateway-to-Gateway 利用共享密钥方式。

以下是一个静态 (MAIN 模式) 的 LAN-TO-LAN 的 VPN 例子 : gateway-to-gateway 的连接方式 ; 共享加密和认证方式。



NETGEAR FVS318 Gateway A 的一端连接局域网 , 内部 IP 为 : LAN 192.168.0.0/24. 局域网接口的 IP 地址为 : 192.168.0.1/24, 广域网接口是由 ISP 提供的固定 IP 地址及网关和子网掩码的连接 , 在基础配置介面上输入信息. (见上图)

NETGEAR FVL328 的 Gateway B 的一端局域网的内部 IP 地址 IP 为 : LAN :172.10.10. /24. Gateway B 的 广域网接口 (Internet) 配置由 ISP 提供的固定 IP 地址及网关和子网掩码. (见上图)

2.7.1 配置 FVS318 的静态 VPN(MAIN 模式)

首先登录到FVS318的管理界面 :

1. 在IE地址栏上输入,FVS318的出厂值默认的IP地址 : <http://192.168.0.1> 。然后系统要要求你输入登陆的用户名和密码。用默认的用户名 : admin 和 默认密码 : password. 登



陆到FVS318。我们假定已设定好LAN接口、广域网接口的IP地址和子网掩码以及网关、DNS服务器的IP地址。如下图：

NETGEAR FVS318 ProSafe VPN Firewall settings

Basic Settings

Does your Internet connection require a login?

☒ No
☐ Yes

Account Name (If Required)

Internet IP Address

☐ Get dynamically from ISP
☒ Use static IP address

IP Address
IP Subnet Mask
Gateway IP Address

Domain Name Server (DNS) Address

☐ Get automatically from ISP
☒ Use these DNS servers

Primary DNS
Secondary DNS

Left Sidebar:

- Basic Settings
- VPN Settings
- Security
 - Security Logs
 - Block Sites
 - Block Service
 - Add Service
 - Schedule
 - E-mail
- Maintenance
 - Router Status
 - Attached Devices
 - Set Password
 - Settings Backup
 - Diagnostics
 - Router Upgrade
- Advanced
 - Ports
 - Dynamic DNS
 - LAN IP Setup
 - Static Routes
 - Remote Management
- Logout

图一: NETGEAR FVS318 v2.3 VPN 设置。

2.在工具栏左边点击 VPN Settings. 点击第一个VPN连接。(总共可以输入八个有效的VPN连接)。按编辑的 Edit 按钮一下。这下面就是 VPN Settings – MAIN Mode 的设置。



NETGEAR FVS318 ProSafe VPN Firewall settings

VPN Settings - Main Mode

• Setup Wizard
• VPN Wizard

Setup

- Basic Settings
- VPN Settings

Security

- Security Logs
- Block Sites
- Block Service
- Add Service
- Schedule
- E-mail

Maintenance

- Router Status
- Attached Devices
- Set Password
- Settings Backup

Connection Name: to-GatewayB

Local IPSec Identifier: 0.0.0.0

Remote IPSec Identifier: 0.0.0.0

Tunnel can be accessed from: a subnet of local address

Local LAN start IP Address: 192.168.0.0

Local LAN finish IP Address: 0.0.0.0

Local LAN IP Subnetmask: 255.255.255.0

Tunnel can access: a subnet of remote address

Remote LAN start IP Address: 172.10.10.0

Remote LAN finish IP Address: 0.0.0.0

Remote LAN IP Subnetmask: 255.255.255.0

Remote WAN IP or FQDN: 218.18.10.18

图二：NETGEAR FVS318 v2.3 VPN Settings – MAIN Mode

- 在 **Connection Name** 框中，输入一个VPN通道名称。例如：我们设为：“to-Gateway B”。
- 在 NETGEAR FVS318 Gateway A 的 **Local IPSec Identifier** 中输入本地身份认证标识。这个表示必须和对端的 **Remote IPSec Identifier** 相对应。在这个例子中使用 0.0.0.0 作为 local identifier。
- 在 **Remote IPSec Identifier** 中输入远端身份认证表示，该标识必须和远端的 **Local IPSec Identifier** 的表示相一致。在这个例子中我们输入 0.0.0.0 作为 the remote identifier。
- 在 **Tunnel can be accessed from** 下拉菜单中选择 a subnet from local address。
- 在 **Local LAN start IP Address** 输入本地LAN所在网段（例如：192.168.0.0）。
- 在 **Local LAN IP Subnetmask** 的对话框中输入子网掩码（例如：255.255.255.0）。
- 从 **Tunnel can access** 的下拉菜单中选择 a subnet from local address。
- 在 **Remote LAN Start IP Address** 的对话框中输入对端（GatewayB）的内网的所在地址段（例如：172.10.10.0）在。
- 在 **Remote LAN IP Subnetmask** 的对话框中输入局域网的子网掩码（例如：255.255.255.0）在。
- 在 **Remote WAN IP or FQDN** 的对话框中输入对端FVS318 Gateway B的广域网接口的IP地址（例如：218.18.10.18）。



Secure Association: Main Mode

Perfect Forward Secrecy: ☒ Enabled ☐ Disabled

Encryption Protocol: 3DES

PreShared Key: netgear2004

Key Life: 28800 Seconds

IKE Life Time: 86400 Seconds

☒ NETBIOS Enable

Apply Cancel

图三：NETGEAR FVS318 v2.3 VPN 设置模式 – MAIN Mode

- 从 Secure Association 下拉框中, 选择Main Mode.
- 在 Perfect Forward Secrecy, 选择Enabled 按钮。 .
- 再从Encryption Protocol 下拉对话框, 选择3DES加密方式。 .
- 在PreShared Key 对话框中, 输入统一的子字符串共享密钥。在这个例子中我们输入“netgear2004”. 你必须在对端的设备上输入同样的共享密码。 .
- 在 Key Life 对话框, 输入28800 seconds.(出厂默认值)
- 在 IKE Life 对话框中, 输入86400 seconds(出厂默认值)。 .
- 如果你希望 NetBIOS数据流量从 VPN通道中运行, 在前方方框中选择 NETBIOS Enable , 行, 例如允许在Microsoft 系统中的网络邻居看到对方的计算机就必须选上。
- 点击Apply 按钮 这些所有配置都会存储到设备中. 然后就会返回到 VPN Settings 屏幕上。

NETGEAR FVS318 ProSafe VPN Firewall settings

VPN Settings

	#	Enable	Connection Name	Local IPSec ID	Remote IPSec ID
<input checked="" type="radio"/>	1	<input checked="" type="checkbox"/>	to-GatewayB	0.0.0.0	0.0.0.0
<input type="radio"/>	2	-	-	-	-
<input type="radio"/>	3	-	-	-	-
<input type="radio"/>	4	-	-	-	-
<input type="radio"/>	5	-	-	-	-
<input type="radio"/>	6	-	-	-	-
<input type="radio"/>	7	-	-	-	-
<input type="radio"/>	8	-	-	-	-

Edit Delete Cancel

图四：NETGEAR FVS318 v2.3 VPN 设置之后的VPN返回的状态介面。



3. 按返回 回到VPN Settings的界面,注意必须在您新建立的连接中选择 **Enable** 选项。.

2.7.2 配置 FVL328 固定 IP 的 VPN (Main 模式)。

首先登录到FVS318的管理界面：

- 1.在IE地址栏上输入,FVL328的出厂值默认的IP地址：<http://192.168.0.1>。然后系统要要求你输入登陆的用户名和密码。用默认的用户名：**admin** 和 默认密码：**password**. 登陆FVL328。我们假定已设定好LAN接口、广域网接口的IP地址和子网掩码以及网关、DNS服务器的IP地址。如下图：

The screenshot shows the 'settings' page for the NETGEAR FVL328 ProSafe High-Speed VPN Firewall. The left sidebar contains a navigation menu with categories: VPN (IKE Policies, VPN Policies, CAs, Certificates, CRL, VPN Status), Maintenance (Router Status, Attached Devices, Settings Backup, Set Password, Diagnostics, Router Upgrade), and Advanced (Dynamic DNS, LAN IP Setup, Remote Management, Static Routes). The main content area is titled 'Basic Settings' and includes the following sections:

- Does Your Internet Connection Require A Login?**
 - ☒ No
 - ☐ Yes
- Account Name (If Required)**
 - ☒ Use Static IP Address
 - Account Name: FVL328
- IP Address**
 - 218 . 18 . 10 . 18
- IP Subnet Mask**
 - 255 . 255 . 255 . 248
- Gateway IP Address**
 - 218 . 18 . 1 . 100
- Domain Name Server (DNS) Address**
 - ☐ Get Automatically From ISP
 - ☒ Use These DNS Servers
 - Primary DNS**: 202 . 104 . 32 . 253
 - Secondary DNS**: 202 . 96 . 120 . 60
- Router's MAC Address**
 - ☒ Use Default Address

图五：NETGEAR FVL328 v2.0 r02 VPN 设置。

2. 首先是配置VPN的 IKE Policies策略了，链接到 VPN 工具栏里的IKE Policies 菜单。点击 Add。我们会见到新 IKE Policy配置界面如下：



The screenshot shows the 'IKE Policy Configuration' window. On the left is a navigation tree with categories: Setup (Setup Wizard, VPN Wizard), Security (Logs, Block Sites, Rules, Services, Schedule, E-mail), VPN (IKE Policies, VPN Policies, CAs, Certificates, CRL, VPN Status), and Maintenance (Router Status, Internet Traffic, Network Database). The main area is titled 'IKE Policy Configuration' and contains the following fields:

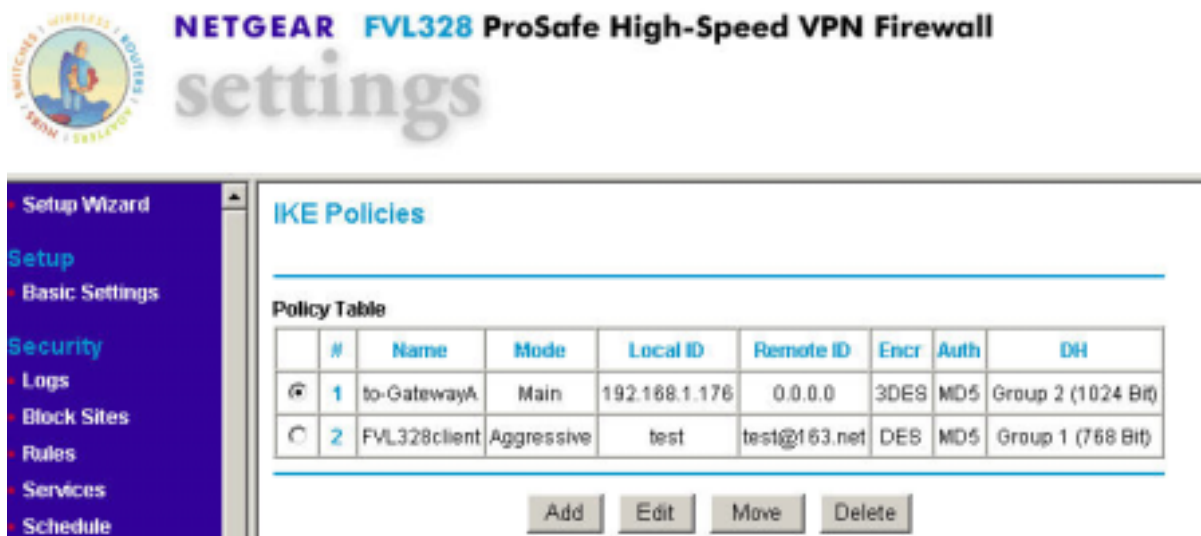
- General**
 - Policy Name: to-GatewayA
 - Direction/Type: Both Directions
 - Exchange Mode: Main Mode
- Local**
 - Local Identity Type: WAN IP Address
 - Local Identity Data: 61.144.128.163
- Remote**
 - Remote Identity Type: Remote WAN IP
 - Remote Identity Data: 216.18.10.16
- IKE SA Parameters**
 - Encryption Algorithm: 3DES
 - Authentication Algorithm: SHA-1
 - Authentication Method: ☒ Pre-shared Key
 - Diffie-Hellman (DH) Group: Group 2 (1024 Bit)
 - SA Life Time: 28800 (secs)

图六：NETGEAR FVL328 v2.0 r02IKE Policy 配置

- 在 **Policy Name** 字段中输入策略的属性名字。这个名称不一定要与对端的 VPN 产品取名一样.它的用途主要上用来帮助管理 IKE 策略的。在这个例子中我们使用”to-GatewayA”来作为策略名称。在 **Policy Name** 对话框中输入 to-GatewayA。
- 从这 **Direction/Type** 下拉对话框中，选取 **Both Directions**。
- 从**Exchange Mode** 模式的下拉菜单中，选择**Main Mode**。
- 从 **Local Identity Type** 下拉对话框中，选择 **WAN IP Address**(在**Local Identity Data** 对话框输入设备会自动找到广域网口的IP作为一个标识符)。
- 从**Remote Identity Type** 下拉对话框中, 选择 **Remote WAN IP** (在**Remote Identity Data** 对话框中会自动找到远端设备的广域网接口的IP地址作为一个标识符)。
- 从加密的算法 **Encryption Algorithm** 下拉框中, 选择**3DES**。
- 从认证算法的 **Authentication Algorithm** 下拉对话框中, 选择 **SHA-1**。
- 再把认证方法 **Authentication Method** 按钮选上, 点击 **Pre-shared Key**。
- 在 **Pre-Shared Key field**对话框中, 输入”Netgear2004”。你必须确保两端网关设备加密钥匙是一至的（包括字母的大小写）。
- 再从 **Diffie-Hellman (DH) Group** 下拉对话框中, 选择 **Group 2 (1024 Bit)**。
- 在 **SA Life Time field**对话框中, 输入28800。



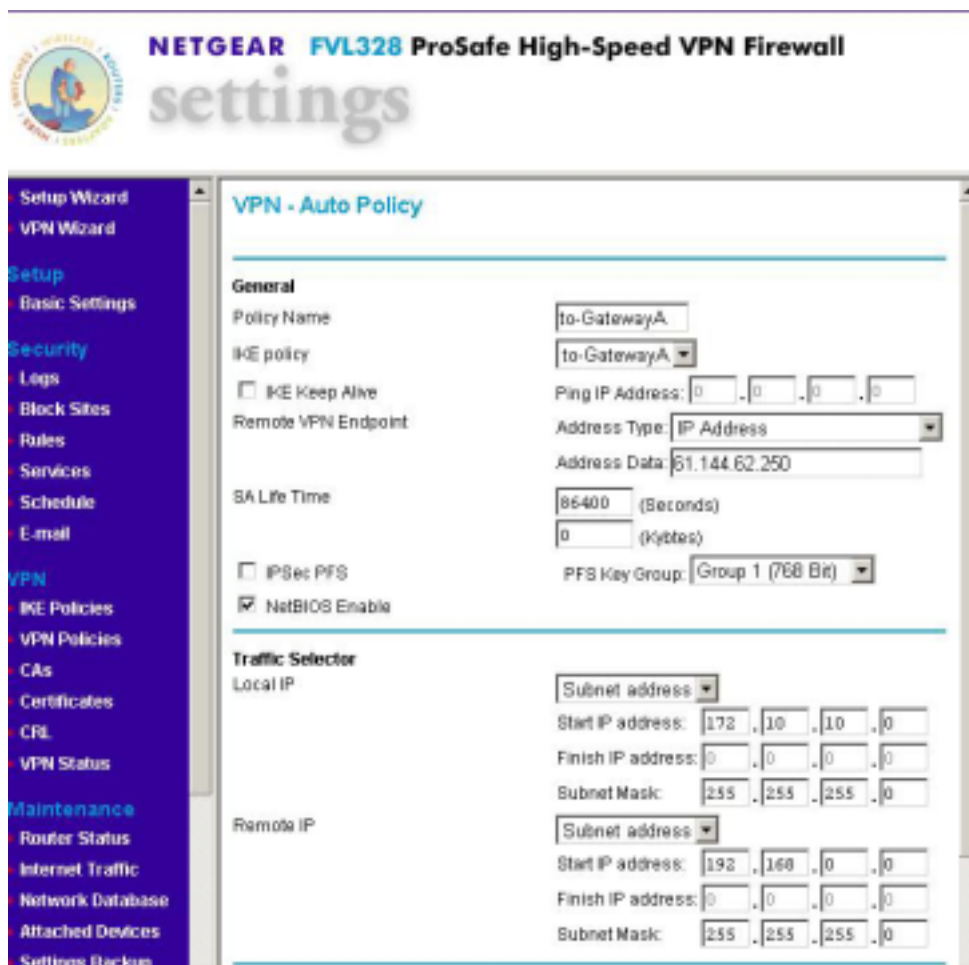
- 点击 **Apply** 按钮. 这就返回到IKE Policies 的主菜单。



图七：NETGEAR FVL328 v1.4 IKE Policies 配置返回的菜单

这 FVL328 IKE Policy 显示就是IKE Policies 主菜单介面。

3. 在 VPN Policies 点击链接就可打开在 VPN 分类栏中，在左边的 Settings图示管理介面中。我们来设置 VPN Policies 主介面的配置。 点击 Add Auto Policy的按钮.（如果是手动去配置VPN则是选择Add Manual Policy）。然后我们就可看到新的配置介面 **VPN – Auto Policy**.

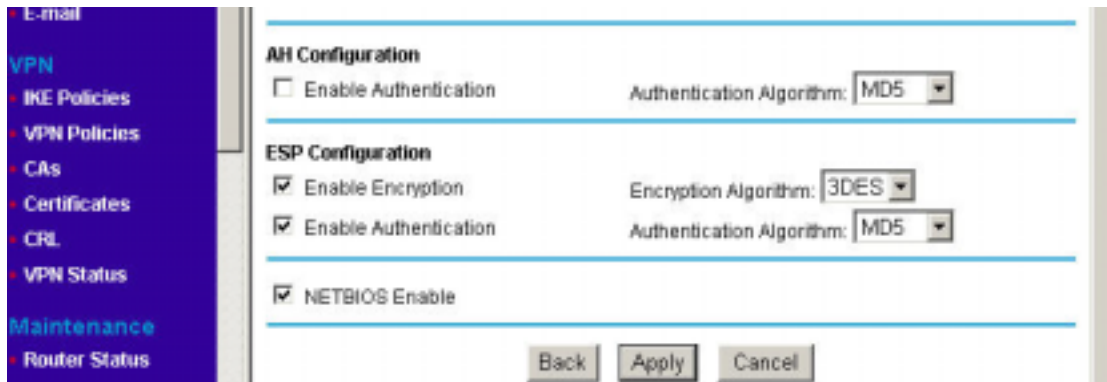


图八：NETGEAR FVL328 VPN v2.0 r02 自动策略配置。

- 输入一个统一的策略名来。这个名称不一定要与远端的VPN设备取的名称相同。在这个例子中我们使用 "to GatewayA" 来作为策略名。在Policy Name字段对话框中输入 "to-GatewayA"。
- 再从 IKE policy下拉对话框中, 选取我们先定义好的IKE Policy- 这里是"to-GatewayA作为IKE Policy。
- 再从 Remote VPN Endpoint Address Type 下拉对话框中, 选取"IP Address"。
- 在 Address Date 对话框中输入Remote VPN Endpoint Address Date作为远端 Gateway A (61.144.62.250作为例子)
- 默认在SA Life Time (Seconds) 对话框中输入86400。
- 默认在SA Life Time (Kbytes) 对话框中输入 0。
- 在 IPSec PFS 对话框复选框中选上。
- 从 PFS Key Group 下拉对话框中选取Group 1 (768 Bit)。
- 再从Traffic Selector Local IP 下拉框中选取 Subnet address作为配置。
- 在 Start IP Address 填上, 输入本地LAN IP地址作为网关B可以访问的地址范围 (本例子中是 : 172.10.10.0)
- 在 Subnet Mask对话框中填上输入网关B的子网掩码(在本例中是 : 255.255.255.0)。



- 再从Traffic Selector Remote IP下拉对话框中选取 Subnet address.一项。
- 在这 Start IP Address字段上，输入远端LAN IP地址作为网关A可访问IP地址范围 (在本例中是：192.168.0.0) 要
- 在这Subnet Mask 字段上输入LAN 网关A的子网掩码 (在本例中是：255.255.255.0)。

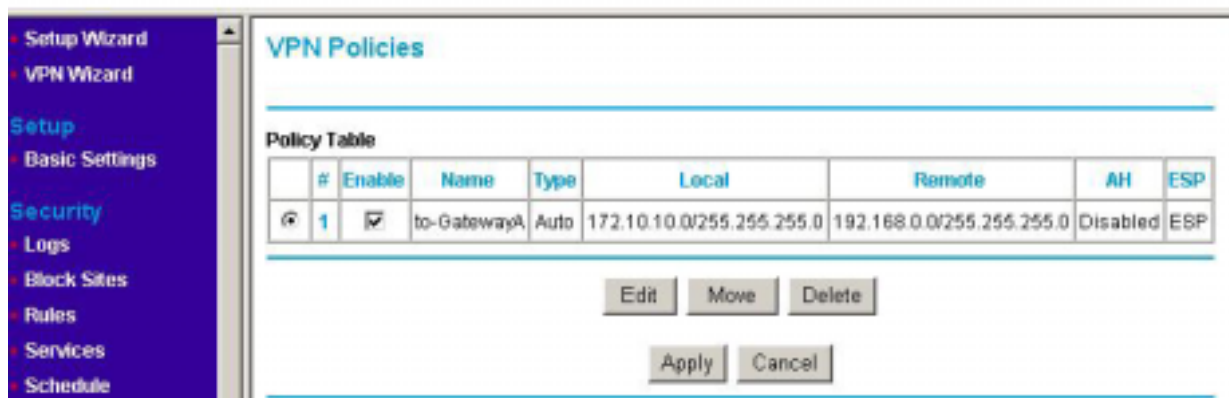


图九：NETGEAR FVL328 VPN v2.0 r02 –自动策

- 再从 AH Configuration Authentication Algorithm 下拉框中, 选上 MD5.，在方框中不能选上。
- 必须选上Enable Encryption在 ESP Configuration Enable Encryption 的对话框。.
- 再从 ESP Configuration Encryption Algorithm 下拉对话框中选取3DES.
- 必须在 ESP Configuration Enable Authentication 的对话框中选上Enable Authentication。
- 再从 ESP Configuration Authentication Algorithm 下拉对话框中选取MD5。.
- 可选上NETBIOS Enable的功能在NETBIOS Enable 复选框上。
- 点击Apply按钮。你会返回到 VPN Policies 主菜单的功能页面上。



NETGEAR FVL328 ProSafe High-Speed VPN Firewall settings



图十：NETGEAR FVL328 v2.0 r02 VPN 策略菜单(Post Configuration)

4. 当返回到 VPN Policies的界面上，要确保 Enable 对话框要选上，



成 当Gateway A和 Gateway B两 端的VPN创建好之后，在两端的任一端局域网上PING对方的局域网客户端。例如：ping 172.10.10.1 -t. 或 ping 192.168.0.1 -t半分钟左右会通，证明VPN通道已建通。

半分钟之后可以可以看到FVL328的VPN已经连通的状态。见下图：

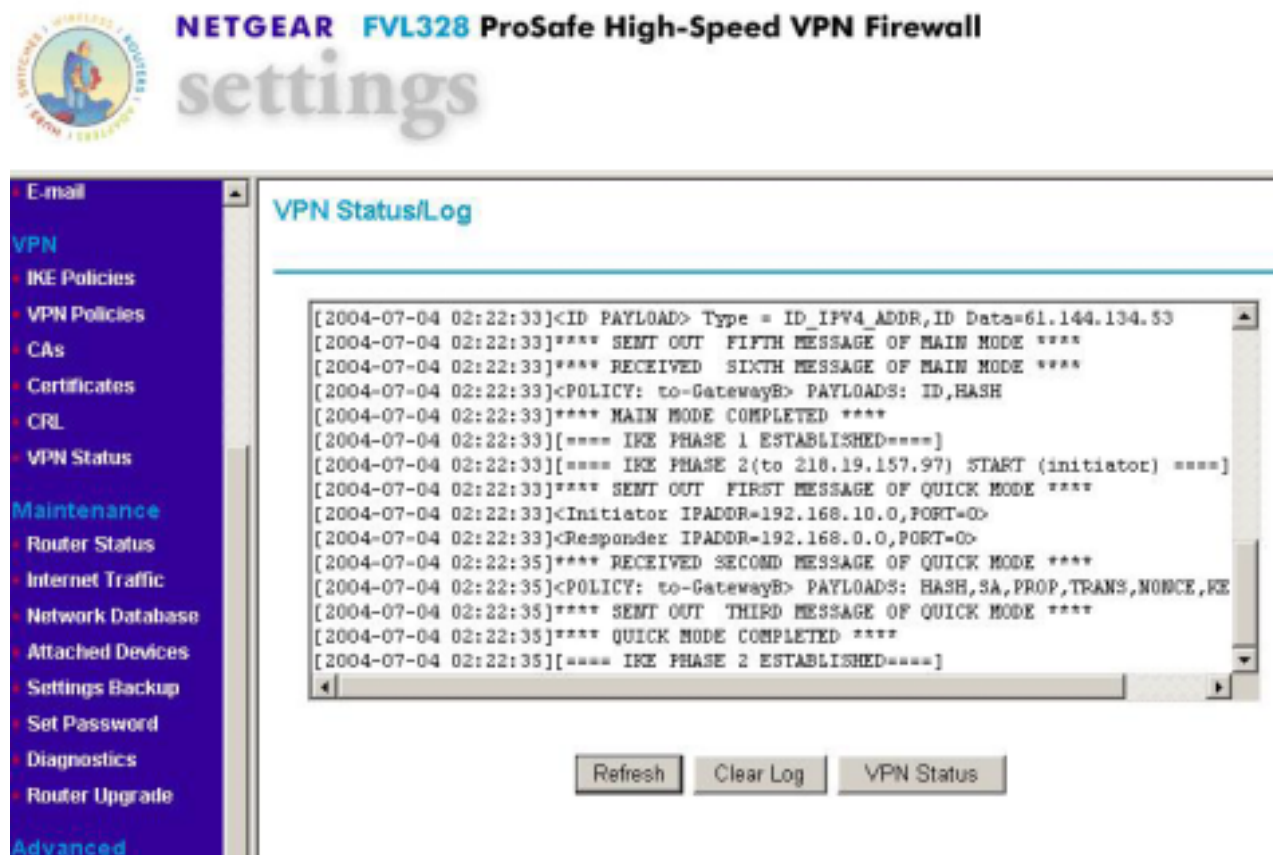


图 十一：NETGEAR FVL328 v2.0 r02 VPN 日志记录



2.8 FQDN FVS318 to FVL328 (网关到网关 IKE Main/Aggressive 模式)

LAN-to-LAN VPN (两边全动态 IP 的 VPN 的建立) 从 FVS318 to FVL328 (Main/Aggressive Mode) 模式。

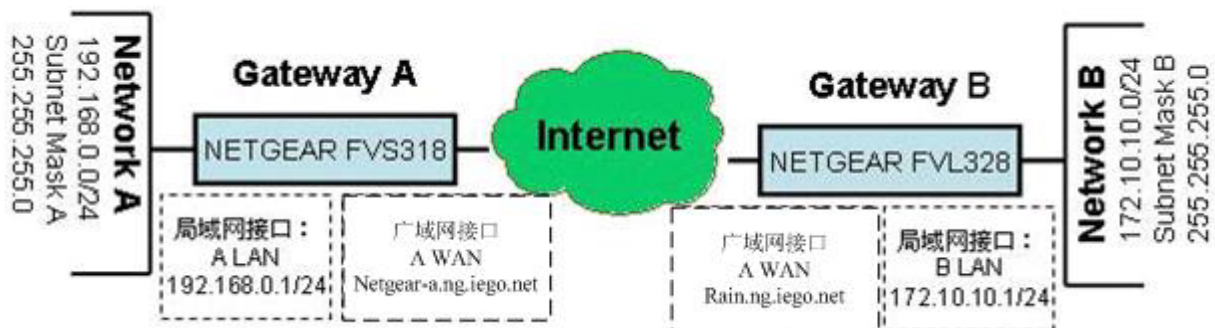
VPN 建立的模式：	LAN-TO-LAN (MAIN 模式)	
动态 VPN 的类型	LAN-to-LAN 或是 Gateway-to-Gateway (Client-to-Gateway 另有讲)	
建立动态 VPN 的加密:	利用 IKE 进行密钥交换和共享密钥方式 (不是能过 CA 认证方式) 建立 IPSEC 通道。	
产品型号和版本号:		
	NETGEAR-网关 A	FVS318 用的版本号是 version 2.3
	NETGEAR-网关 B	FVL328 用的版本号是 version 2.0 Release02
IP 地址的方式：		
	NETGEAR-网关 A	通过 ADSL 动态拨号获取 IP 地址。
	NETGEAR-网关 B	通过 ADSL 动态拨号获取 IP 地址

表一:建立动态VPN的LAN-TO-LAN的测试参数

这个动态 LAN-TO-LAN 的 VPN 例子配置的过程。有关于 VPN 的一些原理可去参考最后一个章节的常用 VPN 专业术语或者登陆网站 www.vpnc.com 查询。这一过程的配置是根据实际情况来配置的。

VPN 构建的方式: Gateway-to-Gateway 利用共享密钥方式。

以下的一个动态 VPN 的 gateway-to-gateway VPN 就上利用共享加密和认证方式。



NETGEAR FVS318 的一端连接局域网一端的内部 IP 为: LAN 192.168.0.0/24. 局域网接口的 IP 地址为: 192.168.0.1, 广域网接口通过 ADSL 线路动态拨号上网, 其申请的动态域名为: netgear-a.ng.iego.net.

NETGEAR FVL328 的一端连接局域网一端的内部 IP 为: LAN 172.10.10.0/24. 局域网接口的 IP 地址为: 172.10.10.1, 广域网接口通过 ADSL 线路动态拨号上网, 其申请的动态域名为: rain.ng.iego.net.

2.8.1 IKE Main 模式网关到网关的 VPN 配置

2.8.1.1 配置 FVS318 的动态 VPN

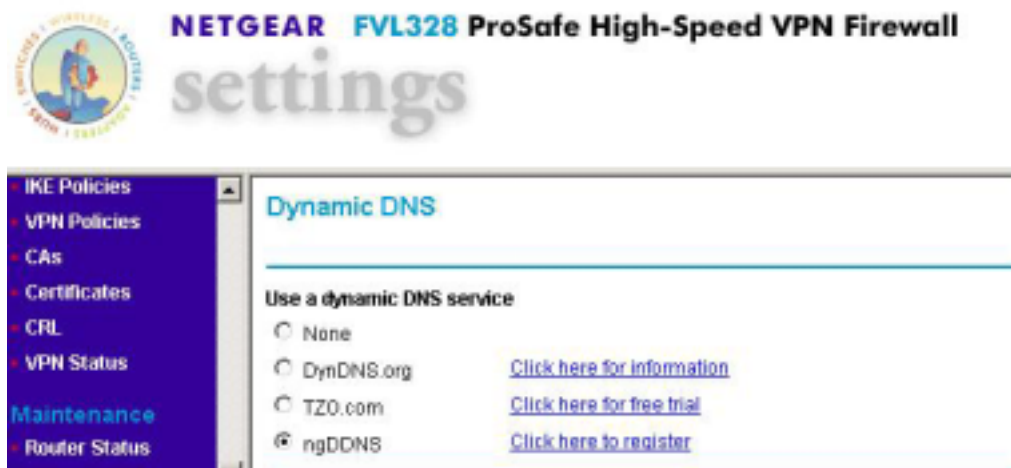
在这个例子中首先登录到 FVS318 的管理界面配置好 ADSL 拨号上网的如用户名, 密码等参数, 让路由器可以连上互联网。关于 IKE MAIN 模式的网关到网关的 VPN 配置, 在前面



的2.7 FVS318toFVL328 (网关到网关 IKE Main模式) 章节已经具体介绍过了, 我们在配置FVS318和FVL328的时候本参考该章节的配置进行。不同的地方是在2.7章节里的例子在两个防火墙节点使用的是静态的IP地址, 而在本章节中则使用了单一的动态域名取代了随时变动的IP地址。在本章将针对上一个章节的例子, 对在配置过程中不一致的地方进行详细介绍。

1. FVS318动态域名的申请

在我们的网站里注册自己的动态域名：



- 点击 ngDDNS 所在的连接, 将引导我们进入动态域名服务的注册页面。



- 点击注册, 在用户名称一栏输入自己的用户名 (注意: 输入的用户名将作为动态域名的前缀, 我们提供的动态域名格式为: 用户名.ng.iego.net)。在用户密码里输入密码再确认重复输入一次, 即完成对动态域名的注册。

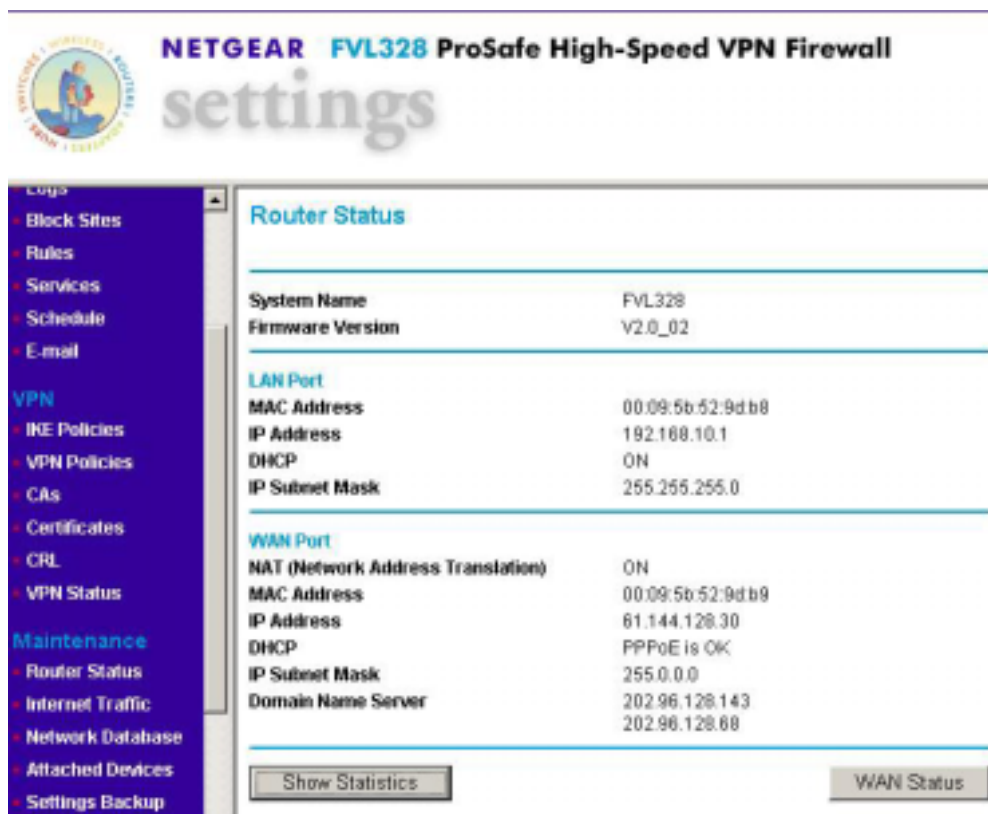


2. FVS318 动态域名的启用

- 在 DDNS 选项里，先选中适当的服务提供商，在中国大陆我们应该选择 Oray.net（网域科技），然后在相应的信息栏目里填入相应的注册信息即可。如下图：在我们的例子里，我们为站点 A 申请了，名为 Netgear-a.ng.iego.net 的动态域名。

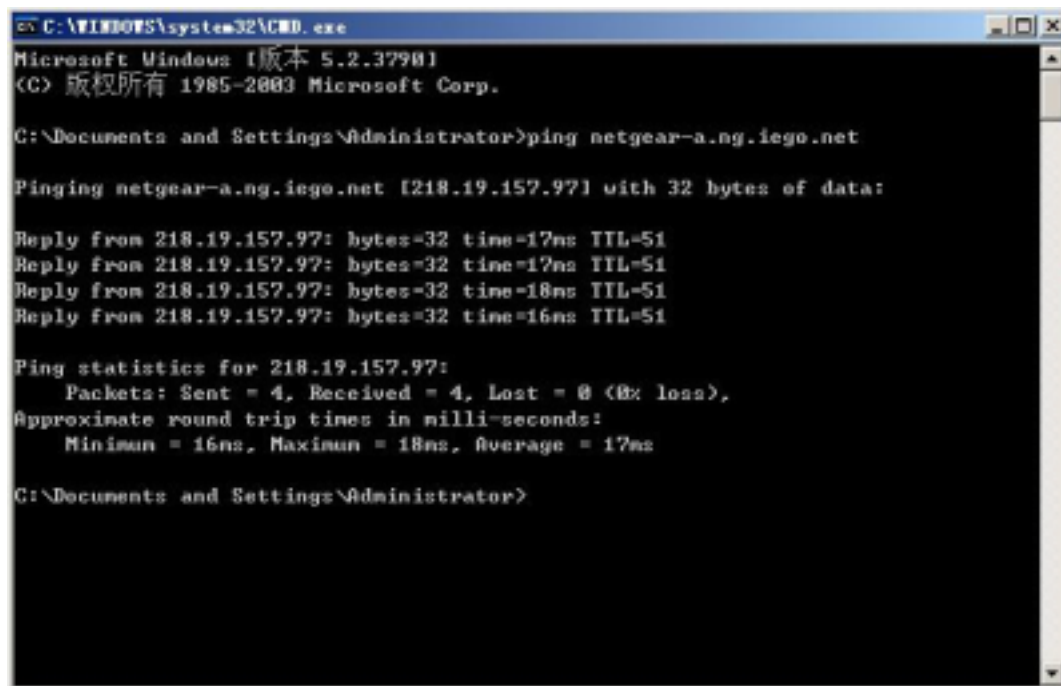
3. 验证动态域名的正确性能

- 查看当前的 IP 地址，如图在 Router Status 栏目里：



■ 用 PING 命令观察动态域名是否能够正确解释 IP 地址

在 DOS 状态下面，用 ping netgear-a.ng.iego.net 观察解释出来的 IP 地址是否和 GATEWAY 当前的真实 IP 地址相一致。

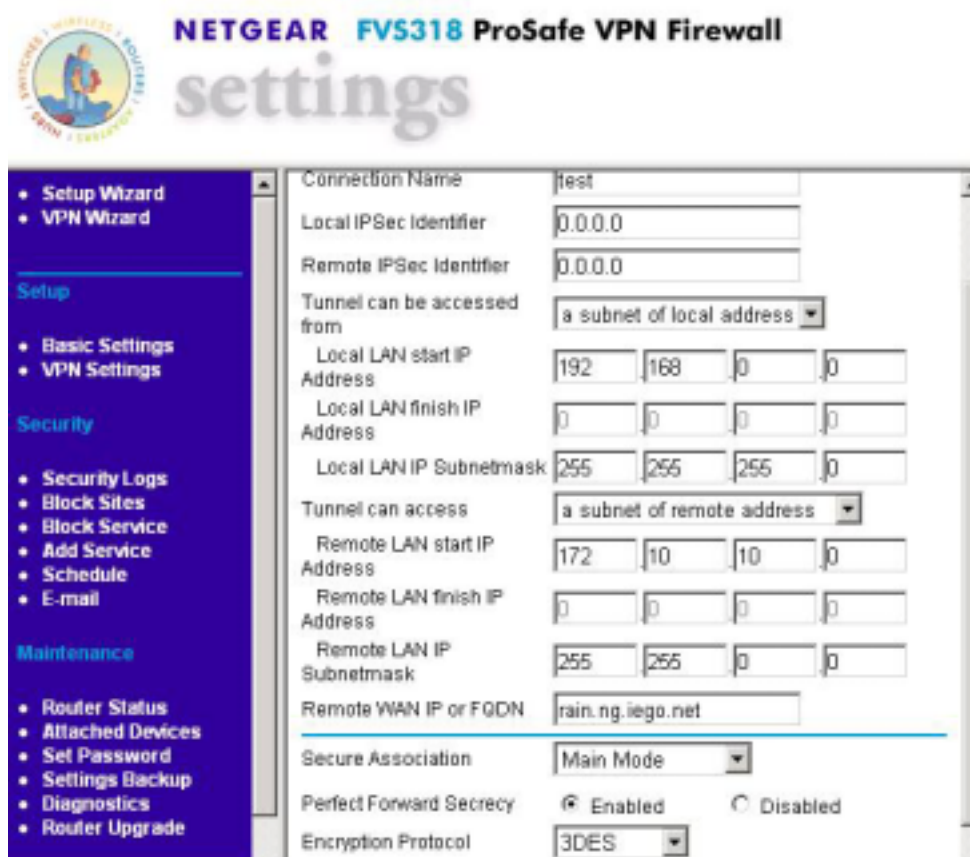




如上图，动态域名能够正确解释当前的 IP 地址，因此我们可以相信，动态域名已成功建立了和 Gateway A 的关联。

4. 建立隧道和动态域名的关联

在FVS318里面的配置，如下图



只需在 Remote WAN IP or FQDN 栏目里将原来固定的 IP 地址改成相应的动态域名就可以了。其他配置不变。

2.9.1.2 配置 FVL328 的动态 VPN

1. 申请动态域名

方法和 FVS318 一致。

2. 在 Gateway A (FVS318) 上启动动态域名服务：

- 在 DDNS 选项里，先选中适当的服务提供商，在中国大陆我们应该选择 Oray.net（网域科技），然后在相应的信息栏目里填入相应的注册信息即可。如下图：在我们的例子里，我们为站点 A 申请了，名为 Netgear-a.ng.iego.net 的动态域名。



NETGEAR FVL328 ProSafe High-Speed VPN Firewall settings

Dynamic DNS

Use a dynamic DNS service

☐ None

☐ DynDNS.org [Click here for information](#)

☐ TZO.com [Click here for free trial](#)

☒ ngDDNS [Click here to register](#)

ngDDNS

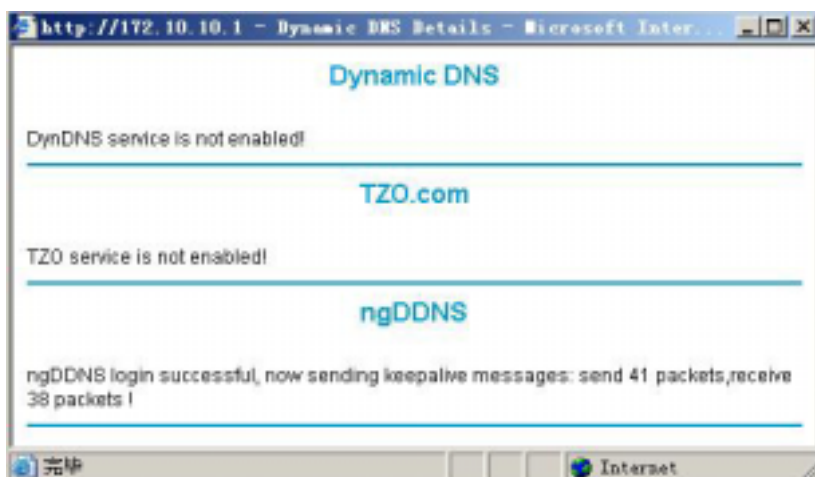
Host and Domain Name
example: youname.ng.iego.net

Account Name

Password

3. 验证动态域名的正确性能

- 在 Dynamic Dns 里面，点击 Show Status 按钮。以下是成功登陆的信息。



4. 动态域名和 VPN 隧道的关联

配置如下图，在对应的 To-GatewayA 的 VPN Policy 里面：



NETGEAR FVS328 Prostate High-Speed VPN Firewall

settings

The screenshot shows the 'VPN - Auto Policy' configuration page. On the left is a navigation menu with options: Setup Wizard, VPN Wizard, Setup, Basic Settings, Security, Logs, Block Sites, Rules, Services, Schedule, E-mail, VPN, IKE Policies, VPN Policies, CAs, Certificates, and CPU. The main content area is titled 'VPN - Auto Policy' and contains two sections: 'General' and 'Traffic Selector'. In the 'General' section, 'Policy Name' is 'To-GatewayA', 'IKE policy' is 'To-GatewayA', 'IKE Keep Alive' is unchecked, 'Remote VPN Endpoint' is 'netgear-a.ng.iego.net' (with 'Address Type' set to 'Fully Qualified Domain Name'), 'SA Life Time' is '86400 (Seconds)', 'PFS Key Group' is 'Group 1 (768 Bit)', 'IPSec PFS' is unchecked, and 'NetBIOS Enable' is checked. In the 'Traffic Selector' section, 'Local IP' is 'Subnet address' and 'Start IP address' is '172.10.10.0'.

VPN - Auto Policy	
General	
Policy Name	To-GatewayA
IKE policy	To-GatewayA
<input type="checkbox"/> IKE Keep Alive	Ping IP Address: 0.0.0.0
Remote VPN Endpoint	Address Type: Fully Qualified Domain Name
	Address Data: netgear-a.ng.iego.net
SA Life Time	86400 (Seconds)
	0 (Kbytes)
<input type="checkbox"/> IPSec PFS	PFS Key Group: Group 1 (768 Bit)
<input checked="" type="checkbox"/> NetBIOS Enable	
Traffic Selector	
Local IP	Subnet address
	Start IP address: 172.10.10.0

配置和 2.7 章节里面的相同，只需要在 Remote VPN Endpoint 里面将原来的固定 IP 地址改成相应的动态域名即可。

2.8.2 IKE Aggressive 模式网关到网关的 VPN 配置

实验环境如本章节的表一和图一所描述。本节介绍如何使用 Aggressive 模式建立 FVS318 和 FVS328 的 VPN 隧道。

2.8.2.1 FVS318 的配置

1. VPN Setting 配置

如下图：



NETGEAR FVS318 ProSafe VPN Firewall settings

• Setup Wizard
• VPN Wizard

Setup

- Basic Settings
- VPN Settings

Security

- Security Logs
- Block Sites
- Block Service
- Add Service
- Schedule
- E-mail

Maintenance

- Router Status
- Attached Devices
- Set Password
- Settings Backup
- Diagnostics
- Router Upgrade

Advanced

- Ports
- Dynamic DNS
- LAN IP Setup
- Static Routes
- Remote Management

Logout

Connection Name: to-GatewayB
Local IPSec Identifier: netgear-a.ng.iego.net
Remote IPSec Identifier: rain.ng.iego.net
Tunnel can be accessed from: a subnet of local address
Local LAN start IP Address: 192.168.0.0
Local LAN finish IP Address: 0.0.0.0
Local LAN IP Subnetmask: 255.255.255.0
Tunnel can access: a subnet of remote address
Remote LAN start IP Address: 172.10.10.0
Remote LAN finish IP Address: 0.0.0.0
Remote LAN IP Subnetmask: 255.255.0.0
Remote WAN IP or FQDN: rain.ng.iego.net
Secure Association: Aggressive Mode
Perfect Forward Secrecy: ☒ Enabled ☐ Disabled
Encryption Protocol: 3DES
Key Group: Diffie-Hellman Group1
PreShared Key: netgear2004
Key Life: 28800 Seconds
IKE Life Time: 86400 Seconds
☒ NETBIOS Enable
Apply Cancel


如图所示，使用 Aggressive 模式以后，需要把本来为 IP 地址的本地和远端身份标识改成相应的动态域名或者主机名，电子邮件地址等。（本例子则修改成相对应的动态名域）。

2.8.2.2 FVL328 的配置

1.IKE Policy 配置

如下图：



 **NETGEAR FVL328 ProSafe High-Speed VPN Firewall**
settings

IKE Policy Configuration

Setup Wizard
VPN Wizard

Setup
Basic Settings

Security
Logs
Block Sites
Rules
Services
Schedule
E-mail

VPN
IKE Policies
VPN Policies
CAs
Certificates
CRL
VPN Status

Maintenance
Router Status
Internet Traffic
Network Database
Attached Devices
Settings Backup
Set Password

General
Policy Name: To-GatewayA
Direction/Type: Both Directions
Exchange Mode: Aggressive Mode

Local
Local Identity Type: Fully Qualified Domain Name
Local Identity Data: rain.ng.iego.net

Remote
Remote Identity Type: Fully Qualified Domain Name
Remote Identity Data: netgear-a.ng.iego.net

IKE SA Parameters
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: ☒ Pre-shared Key
Diffie-Hellman (DH) Group: Group 1 (768 Bit)
SA Life Time: 28800 (secs)

Back Apply Cancel

如图所示，使用 Aggressive 模式以后，需要把本来为 IP 地址的本地和远端身份标识改成相应的动态域名或者主机名，电子邮件地址等。（本例子则修改成相对应的动态名域）。

2. VPN Policy 配置

VPN 的配置则和 Main 模式的相一致，请参考章节 [2.9.1.2 配置 FVL328 的动态 VPN](#)。



三．常用 VPN 专业术语

3.1 IPsec 简介

IPSec，因特网协议安全，是由 IETF（Internet Engineering Task Force）定义的一套在网络层提供 IP 安全性的协议。

基于 Ipsec 的 VPN，如阿姆斯特 VPN，由两部分组成：

- Internet 密钥交换协议(IKE)
- IPsec 协议(AH/ESP/二者都有)

第一部分，IKE 是初始协商阶段，两个 VPN 端点在这个阶段协商使用哪种方法为下面的 IP 数据流提供安全。而且，通过定义一套安全联盟（SA），IKE 用于管理连接；SA 面向每个连接的。SA 是单向的，因此每个 Ipsec 连接至少有 2 个 SA。在 IKE（因特网密钥交换）部分对此有更详细的描述。

另一部分是 IKE 协商后，用加密和认证方法实际传输的 IP 数据。有几种方法，如 IPsec 协议 ESP，AH 或两者结合在一起都可以做到这一点。IPsec 协议（ESP/AH）部分对此进行了解释。

建立 VPN 事件的流程可做如下简要描述：

- IKE 协商如何保护 IKE
- IKE 协商如何保护 Ipsec
- Ipsec 在 VPN 中传输数据

后面的部分将具体描述每一个步骤。

3.2 Internet 密钥交换协议(IKE)

这部分描述 IKE，因特网密钥交换协议，及其使用的参数。

加密和认证数据比较直接，唯一需要的是加密和认证算法，及其使用的密钥。因特网密钥交换协议（IKE），用作分配这些对话用密钥的一种方法，而且在 VPN 端点间，规定了如何保护数据的方法。

IKE 主要有三项任务：

- 为端点间的认证提供方法
- 建立新的 IPsec 连接（创建一对 SA）
- 管理现有连接

IKE 跟踪连接的方法是给每个连接分配一组安全联盟（SA）。SA 描述与特殊连接相关的所有参数，包括使用的 Ipsec 协议(ESP/AH/二者兼有)，加密/解密和认证/确认传输数据使用的对话密钥。SA 本身是单向的，每个连接需要一个以上的 SA。大多数情况下，只使用 ESP 或 AH，每个连接要创建 2 个 SA，一个描述入站数据流，另一个描述出站数据流。同时使用 ESP 和 AH 的情况中就要创建 4 个 SA。

3.2.1 IKE 协商

协商对话参数过程中包含许多阶段和模式。下面对其进行具体描述。



事件流程如下描述：

IKE 阶段 1

- 协商应该如何保护 IKE

IKE 阶段 2

- 协商应该如何保护 Ipsec
- 源自阶段 1 的密钥交换生成一些新的加密信息，以提供 VPN 数据流加密和认证中使用的对话密钥。

IKE 和 Ipsec 连接都有使用期限的限制，使用时间（秒）和数据大小（KB）来描述。使用期限用于防止连接建立的时间过长，从密码学的角度看，这是有必要的。IPSec 的使用期限一般要比 IKE 的使用期限短。这样通过进行阶段 2 协商时，对 Ipsec 连接再次加密。不必进行另外的阶段 1 协商直至到 IKE 使用期限。

3.2.2 IKE 协议

IKE 提议是如何保护数据的建议。发起 IPsec 连接的 VPN 网关，作为发起者会发出提议列表，提议表建议了不同的护连接的方法。

协商连接可以是通过 VPN 来保护数据流的 Ipsec 连接，或是 IKE 连接，保护 IKE 协商本身。

响应的 VPN 网关，在接收到此提议表后，就会根据自己的安全策略选择最适合的提议，并根据已选择的提议做出响应。

如果没有找到可接受的提议，就会做出没有可接受提议的响应，并可能提供原因。提议包括需要的全部参数，如加密和认证数据使用的算法，以及 [IKE 参数](#) 中描述的其他参数。

3.2.3 IKE 阶段 1 - IKE 安全协商

一个 IKE 协商可分两个阶段。第一阶段（阶段 1），通过确认远端网关是否具有匹配的 Pre-Shared 密钥，来进行 2 个 VPN 网关或 VPN 客户端的相互认证。

可是，因为我们不希望以明文方式公布太多的协商信息，所以我们还是要保护其余的 IKE 协商信息。可以用前面描述的方法做到这一点，即通过发起者向响应者发送提议列表来完成。一旦这个工作完成，响应者选择并接受其中的一个提议后，将尝试着认证 VPN 的另一端，以确保它就是要认可的一端，并校验远端网关正是所期望的。

通过 Pre-Shared 密钥、证书或公开密钥加密能够完成认证。Pre-Shared 密钥是目前最常见的认证方法。阿姆瑞特防火墙 VPN 模式支持 Pre-Shared 密钥和证书两种方式。

3.2.4 IKE 阶段 2 - IPsec 安全协商

另一个协商是在阶段 2 进行的，详细说明了 Ipsec 的连接参数。

在阶段 2，我们将从阶段 1 的 Diffie-Hellman 密钥交换中摘取新的密钥信息，并将其作为保护 VPN 数据流的会话密钥。

如果使用 PFS（完善的转发机密），每个阶段 2 协商中，会进行新的 Diffie-Hellman 交换。虽然这种操作比较慢，但可确保密钥不依赖于以前用过的任何密钥，不从同样的初始密钥材料中摘取密钥。这就保证了在不太安全的事件中，危及了某些密钥安全时，而不衍生出并发的密钥。

一旦完成阶段 2 协商，就会建立 VPN 连接，以备使用。



3.2.4 IKE 参数

在协商过程中要使用许多参数。

下面对建立 VPN 连接需要的配置参数加以小结。我们强烈建议了解这些参数的作用后，再试着配置 VPN 端点，因为两个端点能够同意所有这些参数是非常重要的。当安装 2 个阿姆瑞特防火墙作为 VPN 端点时，就可以减少在两个相同对话框中进行对比的过程。可是，使用不同供应商的设备时，就不是很容易了。

下面是对涉及 IKE 协商的参数小结，后面是对这些参数的具体描述。

端点身份 (Endpoint identification)	本地和远端网络/主机 (Local and Remote networks/hosts)
通道/传输模式 (Tunnel/transport mode)	远端网关 (Remote gateway)
主/挑战模式 (Main/aggressive mode)	IPsec 协议(ESP/AH/二者兼有) (IPsec protocol (ESP/AH/both))
IKE 加密 (IKE encryption)	IKE 认证 (IKE authentication)
IKE DH 组 (IKE DH group)	IKE 使用期限 (IKE lifetime)
PFS 打开/关闭/身份 (PFS on/off/identities)	IPsec DH 组 (IPsec DH group)
Ipsec 加密 (IPsec encryption)	Ipsec 认证 (IPsec authentication)
Ipsec 使用期限 (IPsec lifetime)	

- **端点身份 (Endpoint Identification)**

这是表示 VPN 网关身份的一组数据。确切地说，它取决于使用的认证方法。使用 Pre-Shared 密钥时，它可以是一组 16 进制串或某种其他数据，用于识别 VPN 网关。为了使 VPN 网关可以通过相互的认证，远端网关必须拥有相同的 Pre-Shared 密钥。

用 Pre-Shared 密钥的认证是基于 Diffie-Hellman 算法。

- **本地和远端网络/主机 (Local and Remote Networks/Hosts)**

子网或主机间的 IP 数据流是受到 VPN 的保护的。

在 LAN 到 LAN 连接里，这里表示各自 LAN 的网络地址。

如果使用漫游客户，远端网络可以设为 0.0.0.0/0，这意味着漫游客户可从任何地方接入本网络。

- **通道/传输模式 (Tunnel/Transport mode)**

Ipsec 可以使用 2 种模式：通道或传输模式

通道模式表明数据流经过通道到达远端网关，远端网关将对数据进行解密/认证，把数据从通道中提取出来，并发往最终目的地。这样，偷听者只能看到加密数据流从 VPN 的一



端发往另一端。在传输模式里，数据流无法通过通道传输，因此不适用于 VPN 通道。它可以用于保证 VPN 客户端到安全网关连接的安全，如 Ipsec 保护的远程配置。

大多数配置中都设置为“通道”。

- **远端网关 (Remote Gateway)**

远端网关就是远端安全网关，它负责进行解密/认证，并把数据发往目的地。也可以把该字段设成“none”（无），迫使阿姆瑞特 VPN 把远端地址看作远端网关。这种做法在漫游访问方式里尤其有用，因为事先不知道远端 VPN 客户的 IP 地址。把它设置为 none，只要认证正确，IP 地址符合上面讨论的远端网络地址，就允许来自任何 IP 地址的任何人打开 VPN 连接。

传输模式不适用远程网关。

- **主/挑战模式 (Main/Aggressive Mode)**

IKE 协商有 2 种操作模式：主模式和挑战模式。

二者的不同之处在于，挑战模式可以用更少的包发送更多信息，这样做的优点是快速建立连接，而代价是以清晰的方式发送安全网关的身份。

使用挑战模式时，有的配置参数如 Diffie-Hellman 和 PFS 不能进行协商，因此两端拥有兼容的配置是至关重要的。

- **IPsec 协议 (IPsec Protocols)**

Ipsec 协议描述了如何处理数据的方法。其中可以选择的 2 种协议是 AH（认证头，Authentication Header）和 ESP（封装安全有效载荷，Encapsulating Security Payload）。ESP 具有加密，认证或二者兼有的功能。但是，我们不建议仅使用加密功能，因为它会大大降低安全性。

关于 ESP 更多信息，请参看 [ESP \(Encapsulating Security Payload\)](#)。

AH 只有认证作用。与 ESP 的认证之间的不同之处仅仅在于，AH 可以认证部分外发的 IP 头，如源和目的地址，保证包确实来自 IP 包声明的来源。

关于 AH 更多信息，请参看[认证头\(Authentication Header\)](#)。

- **IKE 加密 (IKE Encryption)**

这里指定 IKE 协商使用的加密算法，如算法种类和使用的密钥长度。

阿姆瑞特 VPN 支持的算法是：

- AES
- Blowfish
- Twofish
- Cast128
- 3DES
- DES

DES 只在与其它老的 VPN 设备共同操作时使用。应尽可能地避免使用 DES，因为 DES 是一种老算法，我们认为其不是很安全。

- **IKE 认证 (IKE Authentication)**

这里指定 IKE 协商使用的认证算法。

阿姆瑞特 VPN 支持的算法是：

- SHA1
- MD5



- **IKE DH (Diffie-Hellman) 组**

这里指定 IKE 交换密钥时使用的 Diffie-Hellman 组。

阿姆瑞特 VPN 支持的 Diffie-Hellman 组有：

- DH group 1 (768-bit)
- DH group 2 (1024-bit)
- DH group 5 (1536-bit)

密钥交换的安全性随着 DH 组的扩大而增加，但交换的时间也增加了。

- **IKE 使用期限 (IKE Lifetime)**

IKE 连接的使用期限。

使用期限以时间（秒）和数据量（KB）计算。超过其中任何一个期限时，就会进行新的阶段 1 交换。如果上一个 IKE 连接中没有发送数据，就不建立新连接，直到有人希望再次使用 VPN 连接。

- **PFS**

当 PFS 无效时，IKE 协商阶段 1 的密钥交换过程中会创建一个初始密钥材料。在 IKE 协商阶段 2 中，从初始密钥材料提取加密和认证密钥。使用 PFS（完善转发机密）时，总能够根据重读的密钥创建全新材料。如果有一个密钥符合，就不会用该信息衍生其他密钥。

PFS 的使用有 2 种方式：第一种是密钥 PFS，可在每个阶段 2 协商中交换新密钥。另一种是身份 PFS，在此可以保护身份，方法是每完成一个阶段 2 的协商就删除阶段 1 的 SA，保证使用相同的密钥对一个阶段 2 的协商进行加密。

通常不需要 PFS，因为危及加密或认证密钥安全性的可能性微乎其微。

- **IPsec DH 组**

这是与 IKE 十分相似的 Diffie-Hellman 组。但是，Diffie-Hellman 组仅用于 PFS。

- **IPsec 加密**

这里的加密算法用于保护数据流的传输。

使用 AH 或使用不加密的 ESP 时，就不需要 IPsec 加密。

阿姆瑞特 VPN 支持的算法有：

- AES
- Blowfish
- Twofish
- Cast128
- 3DES
- DES

- **IPsec 认证 (IPsec Authentication)**

这里的认证算法用于保护数据流的传输。

使用不经认证的 ESP（尽管建议不使用未经认证的 ESP）时不使用 IPsec 认证。

阿姆瑞特 VPN 支持的算法有：

- SHA1
- MD5



● IPsec 使用期限 (IPsec Lifetime)

VPN 连接的使用期限，用时间（秒）和数据量（千字节）表示。只要超出其中任何一个值，就要重新创建用于加密和认证的密钥。如果最后一个密钥期没有使用 VPN 连接，那么就会终止连接并在需要连接时从头开始重新打开连接。

3.3 IKE 认证方法（手工，PSK，证书）

3.3.1 手工密钥

配置 VPN 最简单的办法是使用称为手工密钥的方法。使用这种方法时根本不需要使用 IKE，在 VPN 通道两端直接配置加密和认证密钥以及其他参数。

优点：

因为该密钥很直接，所以共同操作性很大。目前大多数共同操作问题都出在 IKE 上。手册密钥完全避开 IKE，只设置自己的 IPsec SA。

缺点：

这种方法陈旧，是 IKE 产生之前使用的方法，缺少 IKE 具有的所有功能。因此此法有诸多限制，如总要使用相同的加密/认证密钥，无防止重放攻击服务，非常死板，不够灵活。也无法保证远端主机和网关的真实性。

这种连接也易受某些重放攻击的攻击，这意味着访问加密数据流的恶意实体能够记录一些包，并把包储存下来并在以后发到目的地址。目的 VPN 端点无法辨别此包是不是重放的包。用 IKE 就可避免这种攻击。

3.3.2 Pre-Shared 密钥, PSK

Pre-Shared 密钥是 VPN 端点间共享一个密钥的方法，是由 IKE 提供的服务，所以具有 IKE 的所有优点，比手工密钥灵活许多。

优点：

Pre-Shared 密钥具有比手工密钥多得多的优点。包括端点认证，PSK 是真正进行端点认证的。还包括 IKE 的所有优点。相反，在使用固定加密密钥时，一个新的对话密钥在使用后，有一定的时间周期限制。

缺点：

使用 Pre-Shared 密钥时需要考虑的一件事是密钥的分配。如何把 Pre-Shared 密钥分配给远端 VPN 客户和网关呢？这个问题很重要，因为 PSK 系统的安全性是基于 PSK 的机密性的。如果在某些情况下危及到 PSK 的安全性时，就需要改动配置，使用新的 PSK。

3.3.3 证书

每个 VPN 网关都有自己的证书，和一或多个可信任根证书。

此认证基于几种理论：

每个端点都有私有密钥，在证书里有与该私有密钥相对应的公有密钥，而且任何人无法访问私有密钥。

证书已经过远端网关信任人员的签署。

优点：



增加了灵活性。例如许多 VPN 客户端在没有配置相同 pre-shared 密钥时也能够得到管理，使用 pre-shared 密钥和漫游客户端时经常是这种情况。相反，如果某客户端不安全时，就可以轻松地取消该客户端证书。无需对每个客户进行重新配置。

缺点：

增加了复杂性。基于证书的认证可作为庞大的公有密钥体系结构的一部分，使 VPN 客户端和网关可依赖于第三方。换言之，要配置更多内容，也可能会出现更多错误。

3.4 IPsec 协议(ESP/AH)

Ipssec 协议是用来保护通过 VPN 传输数据流的。使用的协议及其密钥是由 IKE 协商的。

与 Ipssec 相关的协议有 2 种：AH 和 ESP。下面对它们进行详细说明。

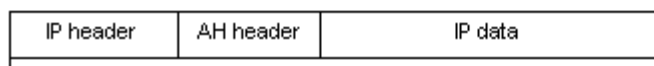
3.4.1 认证头(Authentication Header)

AH 是一种认证数据流的协议。它运用加密学复述功能，根据 IP 包的数据生成一个 MAC。此 MAC 随包发送，允许网关确认原始 IP 包的整体性，确保数据在通过因特网的途中不受损坏。

Original IP packet

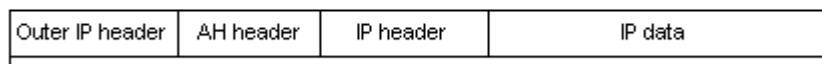


AH in transport mode



Authenticated

AH in tunnel mode



Authenticated

除 IP 包数据外，AH 也认证部分 IP 头。

AH 协议把 AH 头插在原始 IP 头之后，在通道模式里，AH 头是插在外部 IP 头之后的，但在原始内部 IP 头之前。

3.4.2 ESP (Encapsulating Security Payload)

ESP 用于 IP 包的加密和认证。还可只用于加密或认证。



Original IP packet



ESP in transport mode



ESP in tunnel mode



ESP 头插在原始 IP 头之后，在通道模式里，ESP 头是插在外部 IP 头之后的，但在原始内部 IP 头之前。

ESP 头之后的所有数据是经过加密/认证的。与 AH 不同的是 ESP 也对 IP 包加密。认证阶段也不同，ESP 只认证 ESP 头之后的数据，因此不保护外部 IP 头。



封底