

## 两台mGuard如何通过Internet建立VPN连接

修订号: V1.0

作 者: CCAX / XGC

硬件:

序号	型号	HW/FW
1	FL MGuard RS4000 TX/TX VPN	01/7.4.0
2	FL MGuard RS2000 TX/TX VPN	01/7.5.0

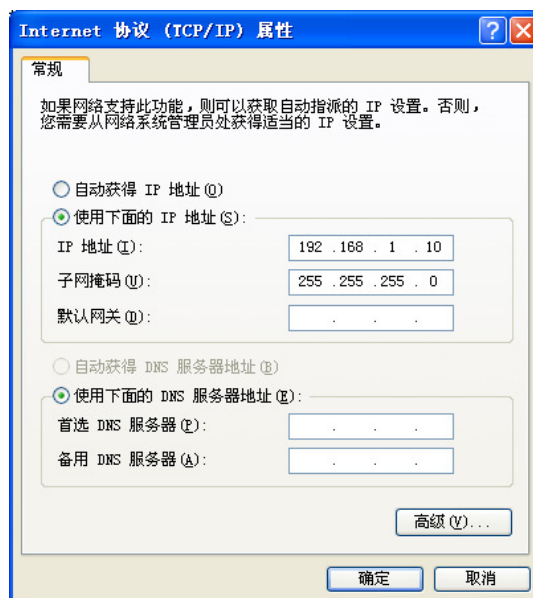
软件:

序号	名称	版本
1		
2		

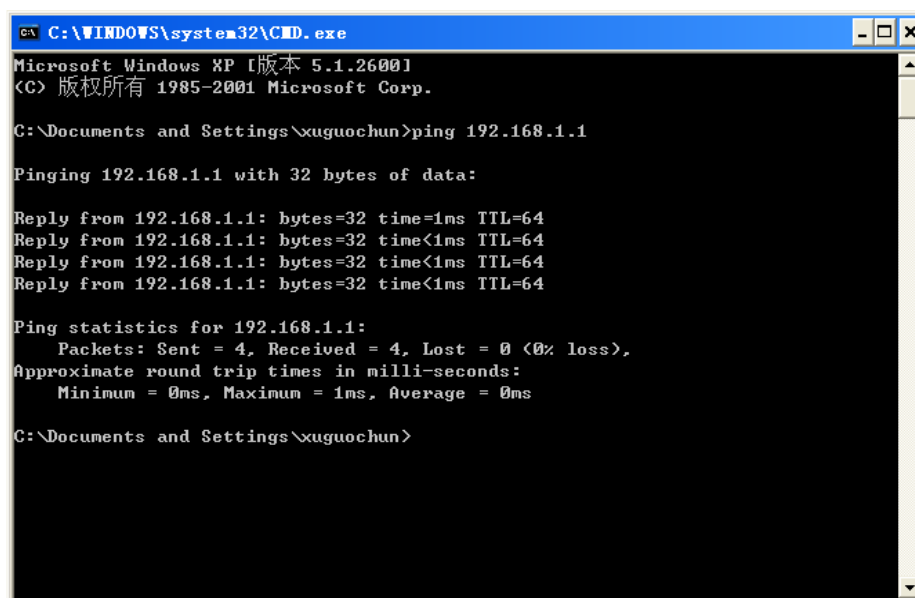


本文以两台mGuard，两台3G路由器为例，演示如何通过Internet建立VPN连接。假设mGuard2 (FL MGUARD RS4000 TX/TX VPN) 与一台3G路由器作为VPN连接的主叫方，mGuard1 (FL MGUARD RS2000 TX/TX VPN) 与另一台3G路由器 (使用电信的CDMA2000上网卡，可以获得临时性的公网IP地址) 作为VPN连接的等待方。

1. 首先演示主叫方的配置，将本机IP地址改为与mGuard2的LAN口默认IP地址（192.168.1.1）同网段，如192.168.1.10。

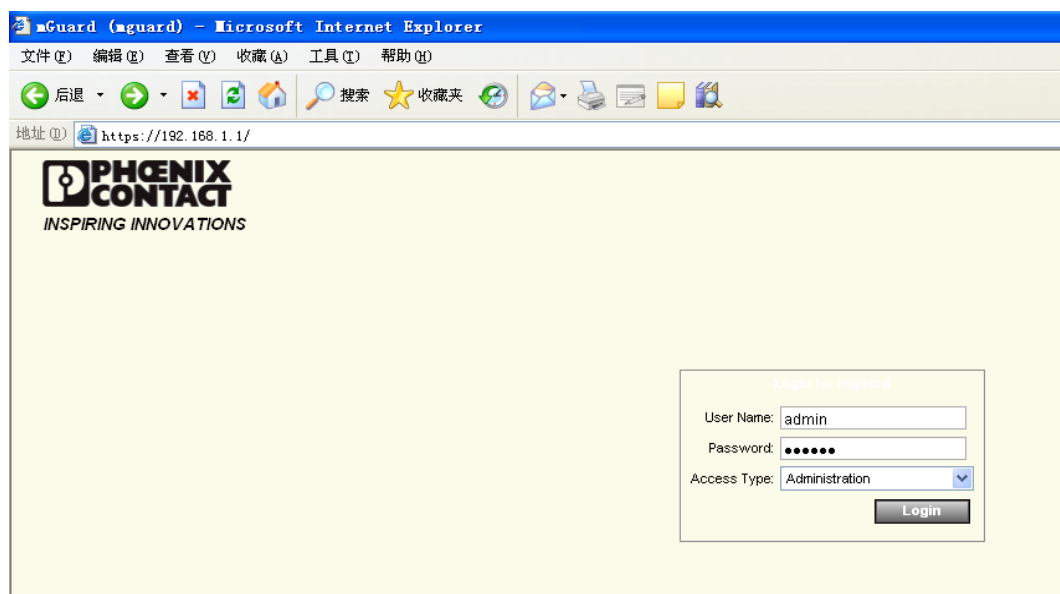


2. 测试是否可以 Ping 通 mGuard2 的 LAN 口。

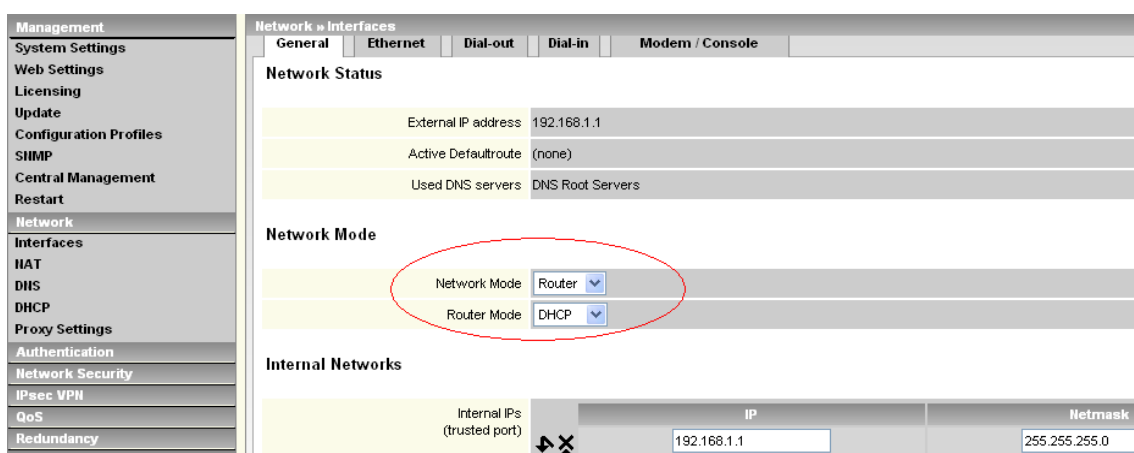


3. 在IE浏览器通过mGuard2的LAN口默认IP地址访问mGuard2的配置界面，键入<https://192.168.1.1>，默认用户名：admin，密码：mGuard。

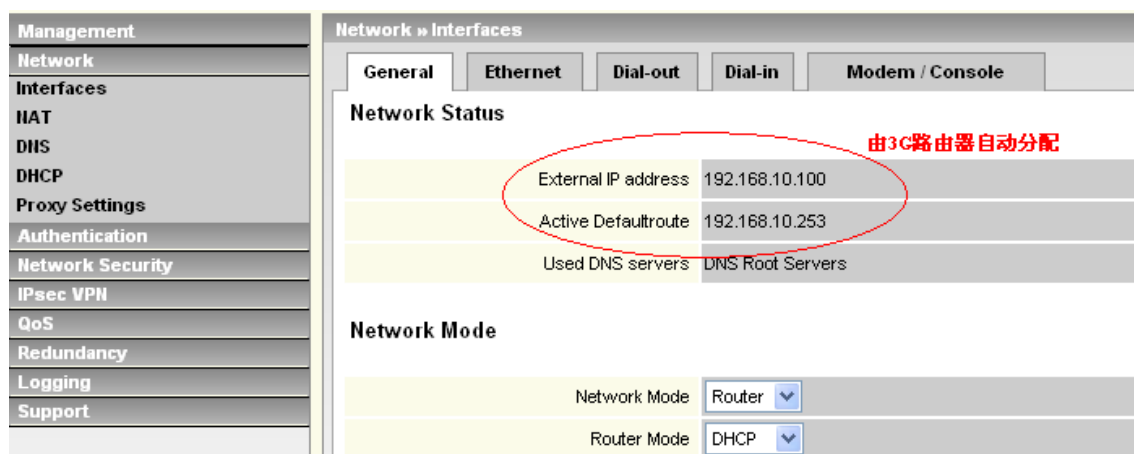




4. 进入 Network >> Interfaces, 将 Network Mode 更改为 Router, 选择相应的 Router Mode: Static/DHCP/PPPoE/PPTP, 本例中选择 DHCP 模式 (需根据实际应用选择相应模式)。



5. Apply 设置生效后如下图

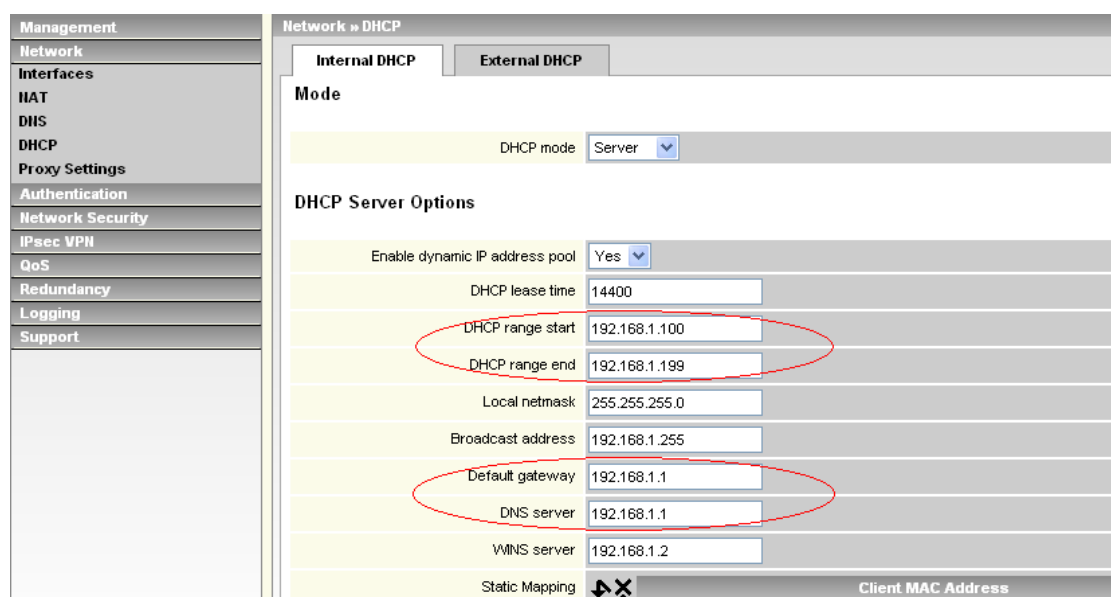


6. 接于 mGuard2 的 LAN 口后的设备 IP 地址分配分为 DHCP 模式和非 DHCP 模式。



## 6.1. DHCP 模式

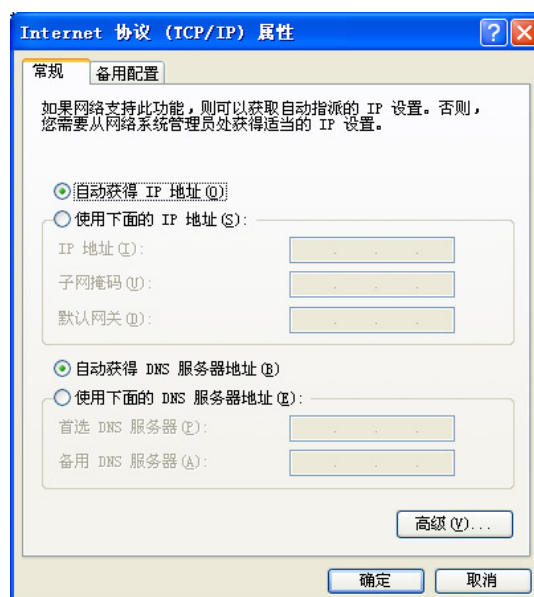
### 6.1.1. Network >> DHCP，DHCP 模式选择 Server。



The screenshot shows the 'Network >> DHCP' configuration window. The 'Internal DHCP' tab is selected. The 'Mode' is set to 'Server'. Under 'DHCP Server Options', the following settings are visible:

Option	Value
Enable dynamic IP address pool	Yes
DHCP lease time	14400
DHCP range start	192.168.1.100
DHCP range end	192.168.1.199
Local netmask	255.255.255.0
Broadcast address	192.168.1.255
Default gateway	192.168.1.1
DNS server	192.168.1.1
WINS server	192.168.1.2
Static Mapping	Client MAC Address

### 6.1.2. 将本机 IP 地址及 DNS 服务器地址改为自动获得。

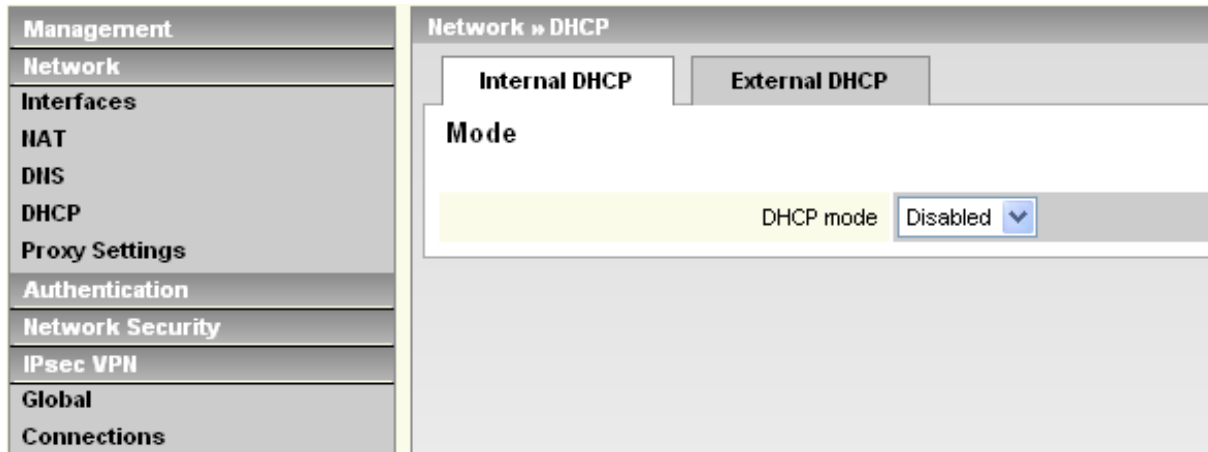


The screenshot shows the 'Internet Protocol (TCP/IP) Properties' dialog box. The '常规' (General) tab is selected. The '备用配置' (Alternate Configuration) section is expanded. The '自动获得 IP 地址 (A)' (Obtain an IP address automatically) radio button is selected. The '自动获得 DNS 服务器地址 (S)' (Obtain DNS server address automatically) radio button is also selected. The '高级 (A)...' (Advanced...) button is visible at the bottom right.

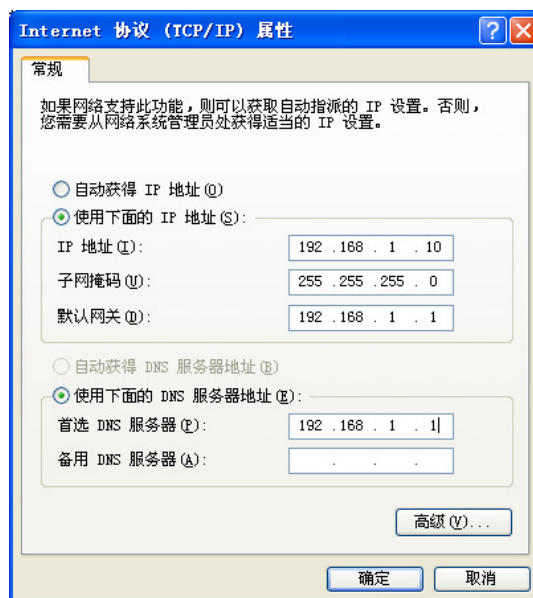
## 6.2. 非 DHCP 模式

### 6.2.1. Network >> DHCP，DHCP 模式选择 Disabled。

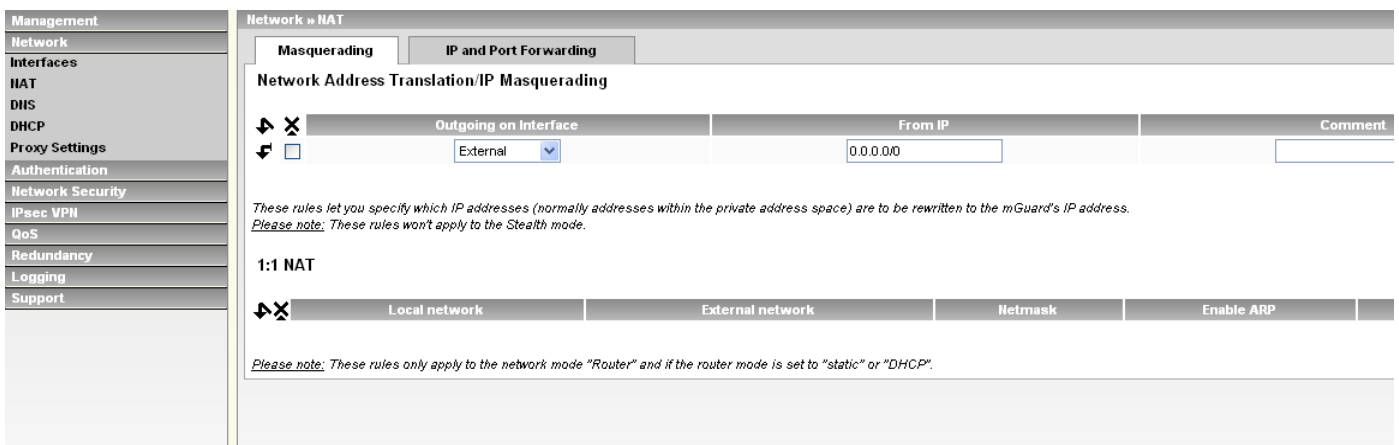




- 6.2.2. 保证本机 IP 地址与 mGuard2 的 LAN 口默认 IP 地址（192.168.1.1）同网段，默认网关及 DNS 服务器地址使用 mGuard2 的 LAN 口默认 IP 地址。



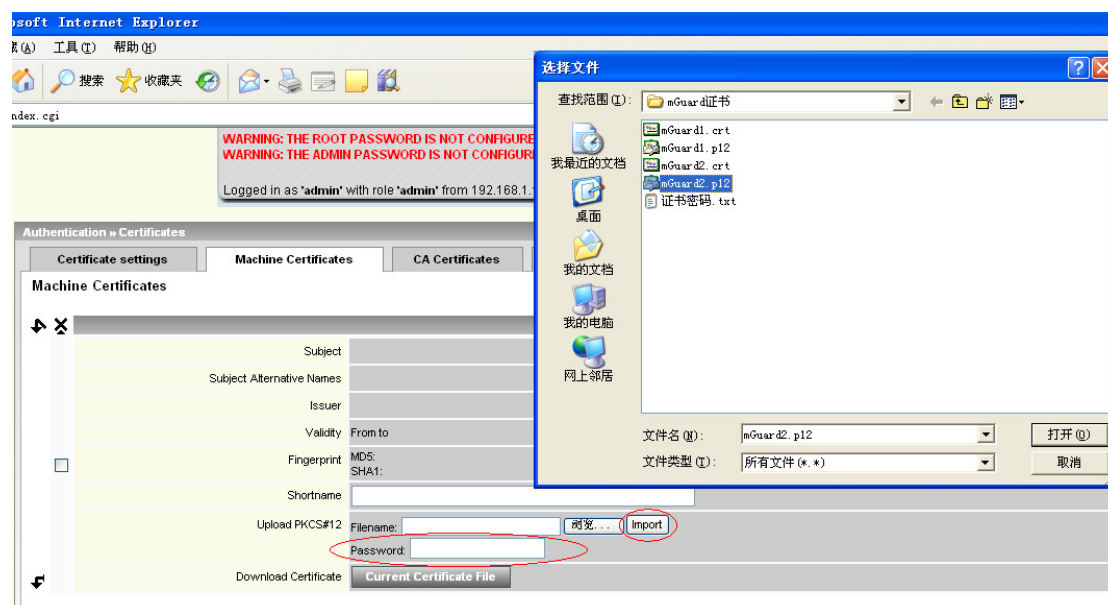
7. 进入 Network >> NAT，设置 Network Address Translation/IP Masquerading。缺省设置为 External/0.0.0.0/0，即允许所有内网设备访问外网。



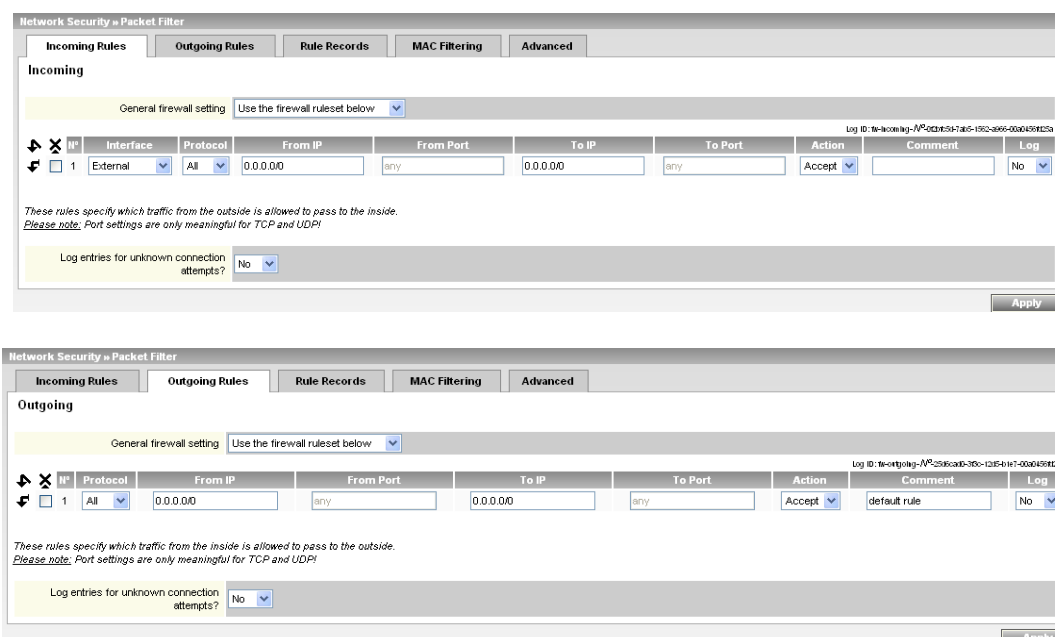
8. 导入 mGuard2 的 Machine Certificate，进入 Authentication >> Certificates，选择 mGuard 的



Machine Certificate (mGuard2 自身的.p12 文件)，输入证书的密码后点 import 导入（证书的制作可参考相关文档）。

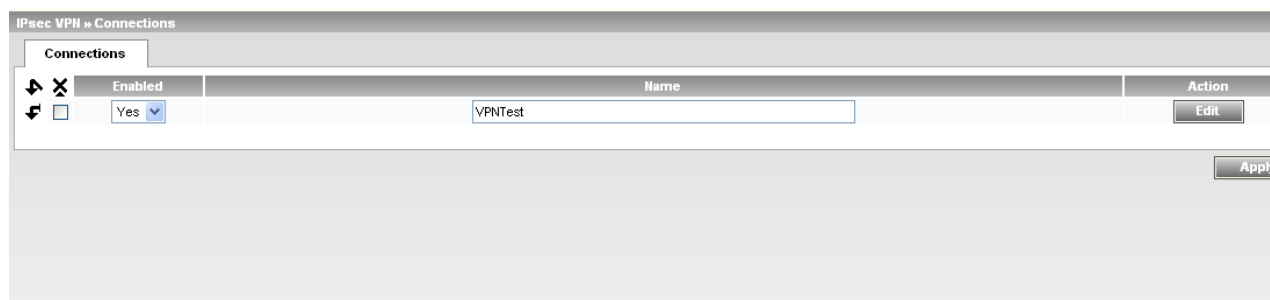


9. 进入 Network Security >> Packet Filter，在 Incoming rules 和 Outgoing rules 下，设置 Protocol 为 “All”，From IP 为 “0.0.0.0/0”，To IP 为 “0.0.0.0/0”，Action 为 “Accept”。

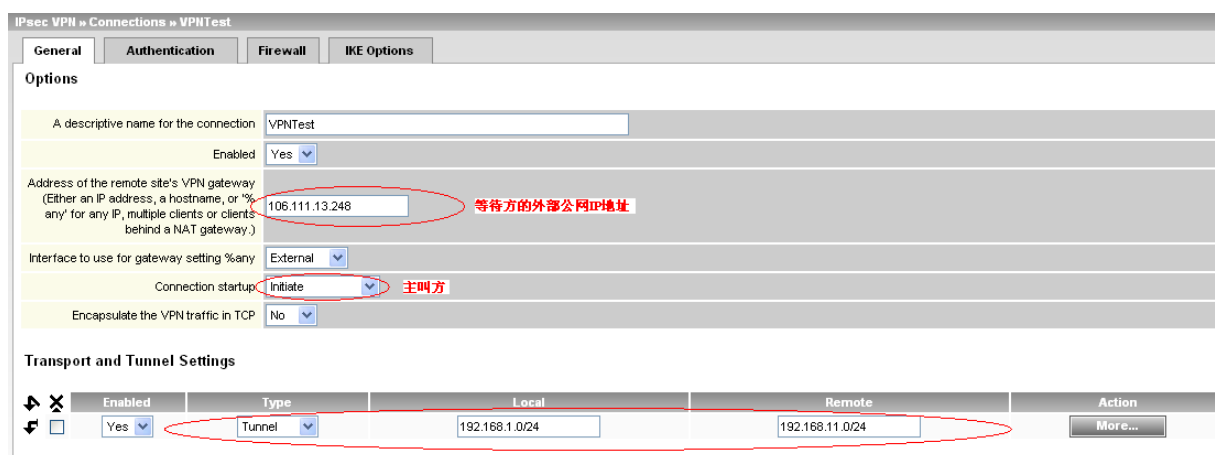


10. 进入 IPsec VPN >> Connections，创建一个 VPN 连接，定义 Name，点击 Edit 进入相应设置页面。



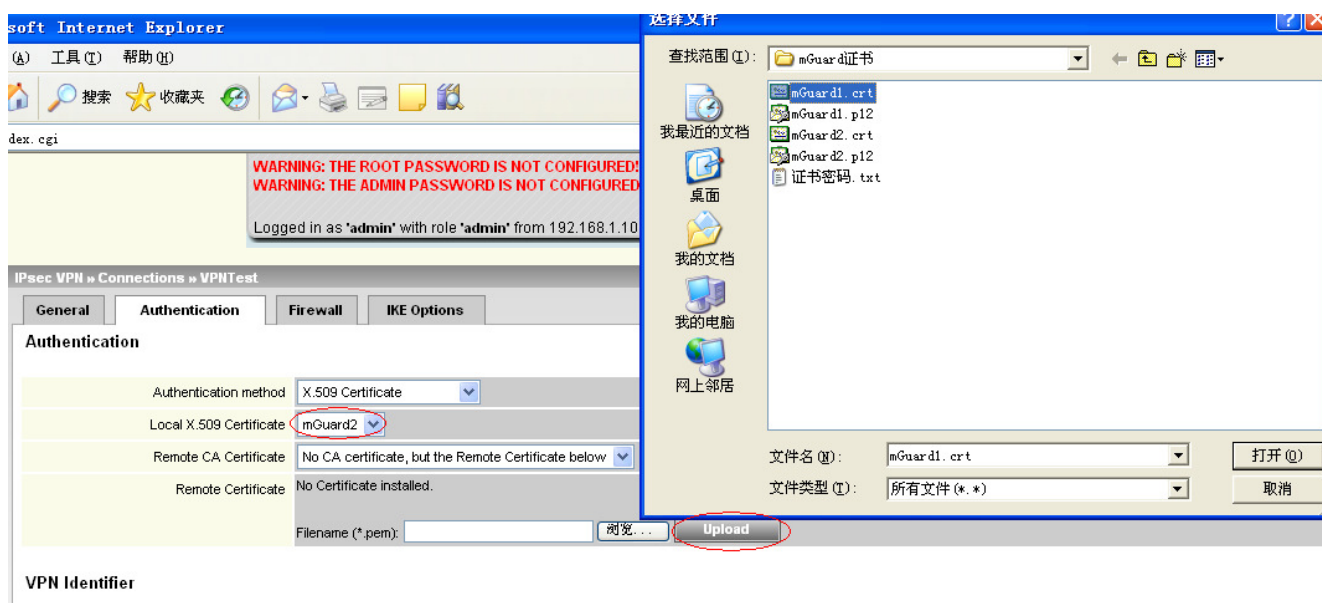


本例中，mGuard2 作为 192.168.1 网段(mGuard2 的 LAN 口及其后设备的网段)与 192.168.11 网段(mGuard1 的 LAN 口及其后设备的网段)之间 VPN 通道的终端。当数据发送就绪时，由此终端建立通道。



## 11. VPN 设置 — 伙伴证书的认证

进入 IPsec VPN >> Connections >> VPNTTest，在 Local X.509 Certificate 下选择之前导入的 Machine Certificate，上传 Remote Certificate (mGuard1 的.crt 文件)。



这样 mGuard2 的设置完毕。

## 12. 等待方即 mGuard1 端 3G 路由器的配置如下：



中国电信  智能模式 已连接

  
 首页

  
 网络设置

  
 无线设置

  
 防火墙

  
 系统管理

### 局域网设置

您可以启用/停止以及设置所有的网络功能。

#### 局域网设置

IP 地址	<input type="text" value="192.168.169.1"/>
子网掩码	<input type="text" value="255.255.255.0"/>
MAC 地址	9C:41:7C:0F:18:15
DHCP 类型	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">服务器 ▼</div>
起始 IP 地址	<input type="text" value="192.168.169.2"/>
结束 IP 地址	<input type="text" value="192.168.169.254"/>

确定

取消

启用端口转发：

#### 单个端口转发

设置	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">启用 ▼</div>
IP地址	<input type="text" value="192.168.169.2"/>
外网端口	<input type="text" value="4500"/>
内网端口	<input type="text" value="4500"/>
协议	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">UDP ▼</div>
注解	<input type="text"/>

最大支持规则数目为30

确定

重设

#### 当前单个端口服务器

编号	IP地址	外网端口	内网端口	协议	注解
1 <input type="checkbox"/>	192.168.169.2	500	500	UDP	
2 <input type="checkbox"/>	192.168.169.2	4500	4500	UDP	

选择删除

重设

13. mGuard1 的 Network >> Interfaces 中的设置：



Network > Interfaces

General Ethernet Dial-out Dial-in Modem / Console

Network Status

External IP address	192.168.169.2	由3C路由器自动分配
Active Default route	192.168.169.1	
Used DNS servers	192.168.169.1	

Network Mode

Network Mode Router

Router Mode DHCP

Internal Networks

Internal IPs (trusted port)	IP	Netmask	Use VLAN	VLAN ID
	192.168.11.1	255.255.255.0		1

Additional Internal Routes

Network	Gateway

14. mGuard1 的 IPsec VPN >> Connections >> VPNtest 中的设置:

IPsec VPN >> Connections >> VPNtest

General Authentication Firewall IKE Options

Options

A descriptive name for the connection VPNtest

Enabled Yes

Address of the remote site's VPN gateway (Either an IP address, a hostname, or '%any' for any IP, multiple clients or clients behind a NAT gateway.) %any

Interface to use for gateway setting %any External 0.0.0.0

Connection startup Wait

Encapsulate the VPN traffic in TCP No

Transport and Tunnel Settings

Enabled	Type	Local	Remote
Yes	Tunnel	192.168.11.0/24	192.168.1.0/24

15. mGuard1 NAT 设置, Packet Filter 设置等均与 mGuard2 相同, mGuard1 的证书导入方法与 mGuard2 相同。

16. 查看 mGuard 的 VPN 连接状态

进入 IPsec VPN >> IPsec Status, 点 Update 刷新, 该页提供了有关连接状态和当前正在使用的密钥有效周期等信息。下图为 mGuard2 的 IPsec Status 信息。

IPsec VPN >> IPsec Status

Connection Name	Gateway	Connection	ISAKMP State	IPsec State
VPNtest (MAH1599494887_1)	192.168.10.100	106.111.13.248	STATE_MAIN_I4 (ISAKMP SA established)	STATE_QUICK_I2 (sent GI2, IPsec SA established)
	192.168.1.0/24	192.168.11.0/24	Algorithm: 3DES_CBC_192-MD5-MODP1536	Algorithm: 3DES_0-HMAC_MD5
	C=CN, ST=Jiangsu, L=Nanjing, O=Phoenix Contact, OU=RBUC, CN=mGuard2	C=CN, ST=Jiangsu, L=Nanjing, O=Phoenix Contact, OU=RBUC, CN=mGuard1	Lifetime: 2777s	Lifetime: 27700s
	Local	Remote		

Update