

# Vpn Hack 深入浅出

Kaka kaka at 0x557 dot org

--Begin==0x0a==0x0b==0x0c==0x0d==0x0e==0x0f==

--0x0a ==

前言

--0x0b==

安装所需软件，环境

--0x0c==

安装过程，配置

--0x0d==

连接 VPN，利用

--0x0e==

其它

--0x0f==

Q&A

--0x0a==

Only for Hack Hack

--0x0b==

安装所需软件

```
[root@papa vpn]# ls -la
total 1460
drwxr-xr-x  3 root  root    4096 Oct 12 17:24 .
drwxr-xr-x  3 root  root    4096 Oct 12 17:05 ..
-rw-r--r--  1 root  root   54872 Jun  7 09:26 dkms-1.12-1.noarch.rpm
-rw-r--r--  1 root  root   58837 Jul  2 10:35 kernel_ppp_mppe-0.0.4-2dkms.noarch.rpm
-rw-r--r--  1 root  root  279894 Jun  7 10:06 ppp-2.4.3-0.cvs_20040527.1.i386.rpm
-rw-r--r--  1 root  root   87966 Jun 23 19:08 pptpd-1.2.1-1.i386.rpm
```

软件运行环境

```
[root@papa vpn]# uname -a
```

```
Linux papa 2.4.20-8 #1 Thu Mar 13 17:54:28 EST 2003 i686 i686 i386 GNU/Linux
[root@papa vpn]# cat /etc/issue
Red Hat Linux release 9 (Shrike)
Kernel \r on an \m
```

## Windows 2k 自带。

控制面板-管理工具-路由和远程访问

%SystemRoot%\System32\rrasmgmt.msc /s

--0x0c--

--0x0c\_0a--

Linux 下 VPN 安装过程，配置

下载所需的软件包 [安装包随文章发放]

```
kernel_ppp_mppe-0.0.4-2dkms.noarch.rpm
ppp-2.4.3-0.cvs_20040527.1.i386.rpm
pptpd-1.2.1-1.i386.rpm
dkms-1.12-1.noarch.rpm
```

升级 ppp

```
[root@papa vpn]# rpm -Uvh ppp-2.4.3-0.cvs_20040527.1.i386.rpm
warning: ppp-2.4.3-0.cvs_20040527.1.i386.rpm: V3 DSA signature: NOKEY, key ID b56a8bac
Preparing... #####
[100%]
 1:ppp #####
[100%]
```

安装 pptp

```
[root@papa vpn]# rpm -ivh pptpd-1.2.1-1.i386.rpm
Preparing... #####
[100%]
 1:pptpd #####
[100%]
```

打 mmpe 补丁

```
[root@papa vpn]# rpm -ivh dkms-1.12-1.noarch.rpm
warning: dkms-1.12-1.noarch.rpm: V3 DSA signature: NOKEY, key ID 23b66a9d
Preparing... #####
```

```
[100%]
  1:dkms #####
[100%]
[root@papa vpn]# rpm -ivh kernel_ppp_mppe-0.0.4-2dkms.noarch.rpm
warning: kernel_ppp_mppe-0.0.4-2dkms.noarch.rpm: V3 DSA signature: NOKEY, key ID b56
Preparing... #####
[100%]
  1:kernel_ppp_mppe #####
[100%]

Creating symlink /var/dkms/kernel_ppp_mppe/0.0.4/source ->
        /usr/src/kernel_ppp_mppe-0.0.4
.....
- Installing to /lib/modules/2.4.20-8/kernel/drivers/net//
depmod.....
DKMS: Install Completed.
```

## 0x0c\_0b

### 配置

需要配置 3 个文件:

```
/etc/pptpd.conf
/etc/ppp/options.pptpd
/etc/ppp/chap-secrets
```

配置好的文件内容

//配置文件本来会有些记录日志的选项, 但是为了 Hack, 为了 long long time 使用, 我去掉了那些记录日志的选项, 有兴趣的想调试可以自己加上。默认安装的配置文件有日志记录功能。

/etc/pptpd.conf

```
[root@papa vpn]# grep ^[^#] /etc/pptpd.conf #除掉注释后的配置参数
option /etc/ppp/options.pptpd #options 文件的位置
speed 115200 #
localip 219.163.8.243 #本网段没有被使用的 ip 地址
remoteip 219.163.8.245-250 #本网段没有被使用的其它 ip 地址
```

/etc/ppp/options.pptpd

```
[[root@papa vpn]# grep ^[^#] /etc/ppp/options.pptpd
auth
name pptpd #服务器名称
require-mschap-v2
```

```
require-mppe-128
require-chap
proxyarp
lock
nobsdcomp
```

/etc/ppp/chap-secrets

```
[root@ papa vpn]# grep ^[^#] /etc/ppp/chap-secrets
#用户名[tab]服务器名对应 name [tab]secret 密码[tab]Ip addresses *代表从地址池自动分配
test pptpd fuckjp *
```

Pptpd 一些命令

```
[root@ papa vpn]# service pptpd
Usage: /etc/init.d/pptpd {start|stop|restart|restart-kill|status}
```

--0x0c\_0c--

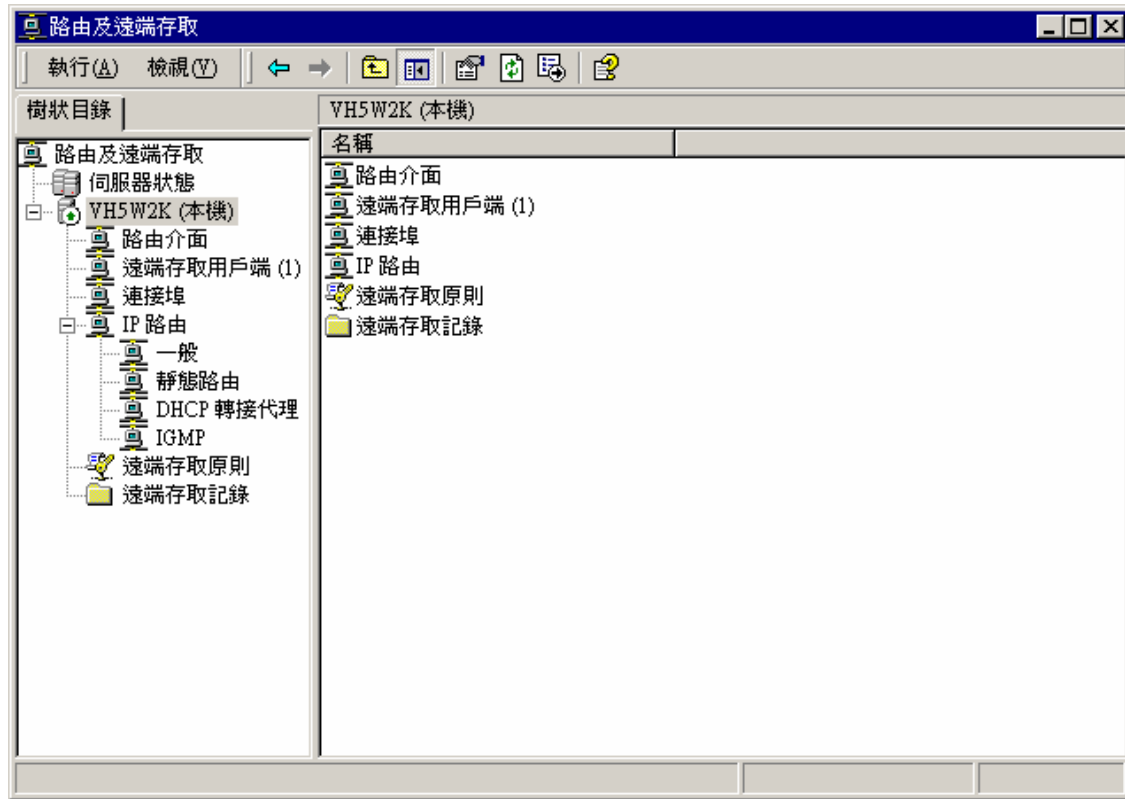
## Windows 下 Vpn 安装配置

Windows 下 Vpn 安装是利用系统自带的路由和远程访问来设置的。设置起来比较简单。

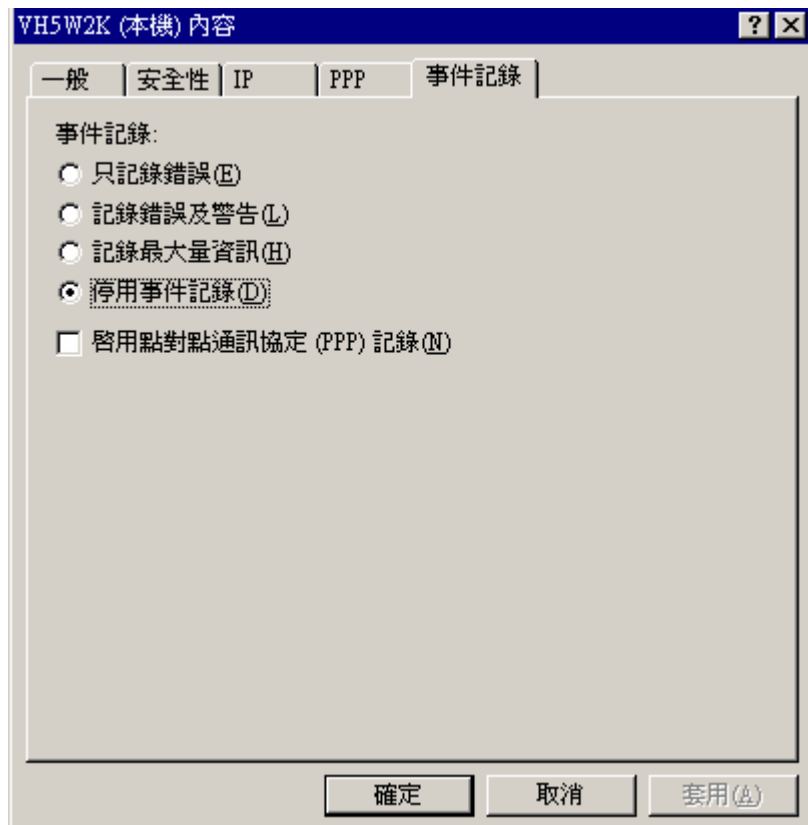
安装的时候默认安装就可以，在选择指派 ip 的时候要选择手工指派，认证选择 windows 认证。一路 next 就可以。

只说几个需要注意的地方：[配图说明]

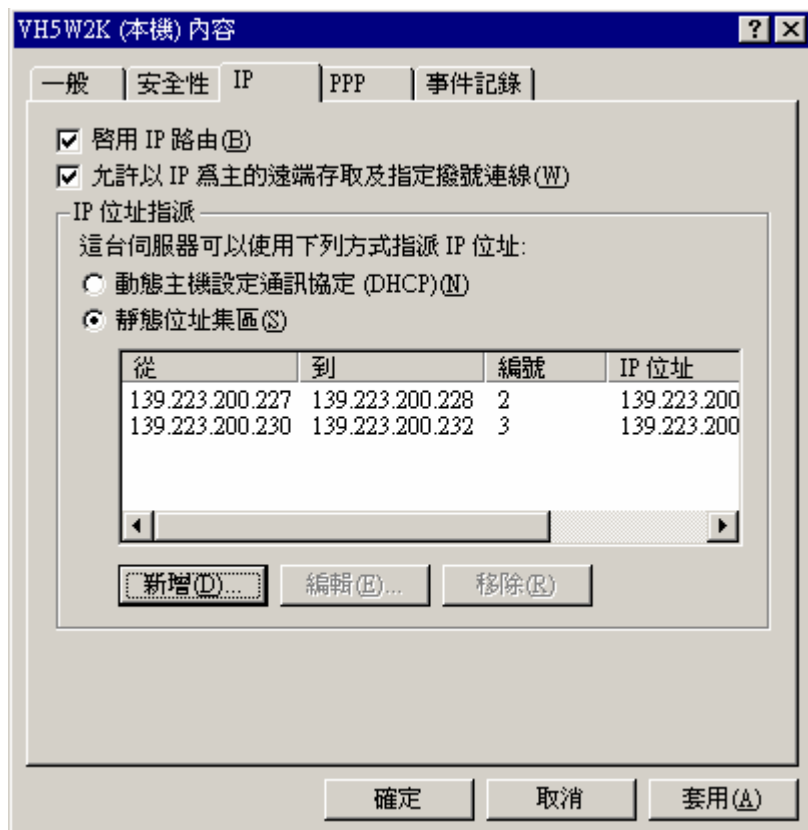
这个是正常启用 VPN 的截图：



远程存取用户端（1）代表有一个用户连接进来使用 VPN。  
禁用掉日志记录功能。SA love log; Hacker hate log。:D



有时候这个网段的 ip 不是都被使用的，但是却隔一个用一个，或者隔多个用一个，我们可以在 Hostname（本机），点击属性-IP 选项来添加。



--0x0d--

连接 VPN，利用

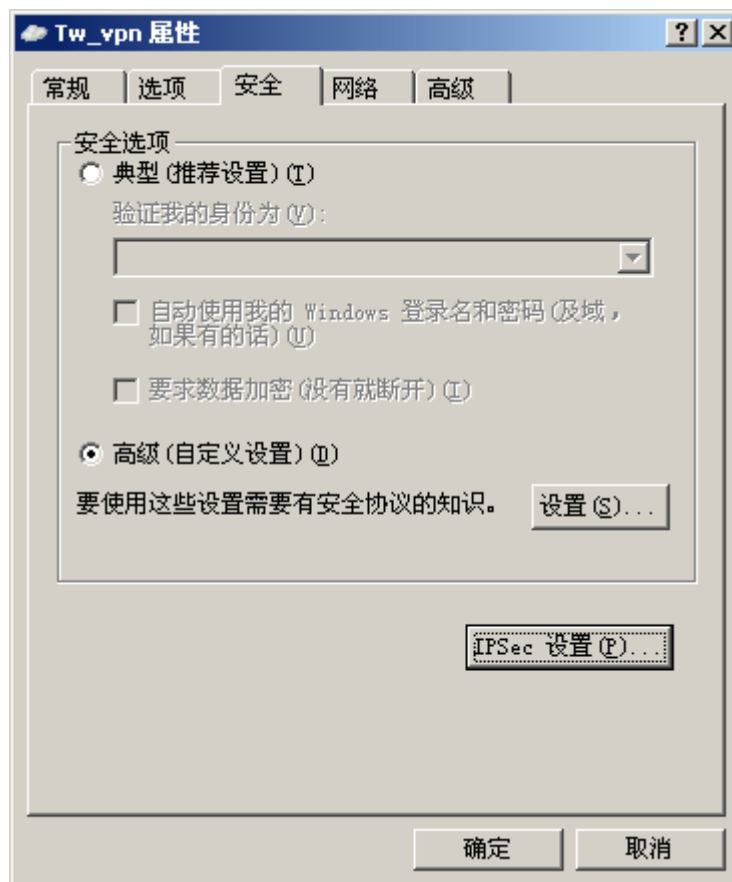
--0x0d\_0a--

Windows 下连接 VPN

网络邻居-属性-网络任务-创建一个新的网络连接  
连接到我的工作场所的网络-  
虚拟专用网络-  
公司名-随便填  
不拨初始连接-  
主机名或 IP 地址-填入 VPN 的 IP 地址  
NEXT-NEXT-DONE

打开刚刚建立的 VPN 属性，修改几个地方。

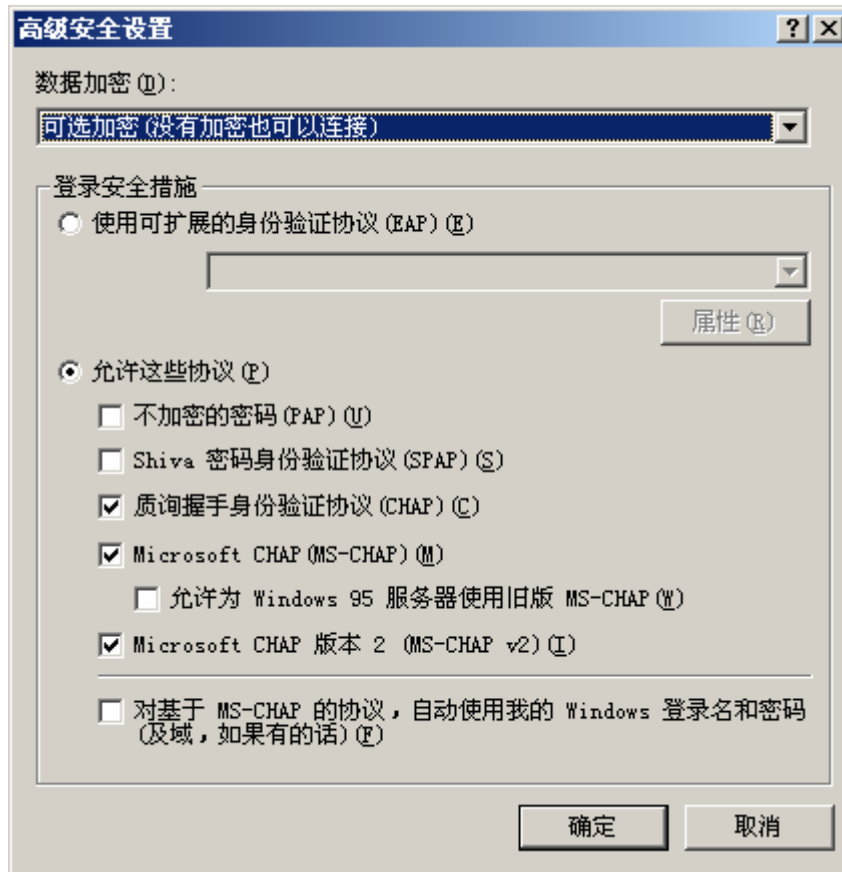
## 安全选项选择 – 高级（自定义设置）



## 高级 – 设置

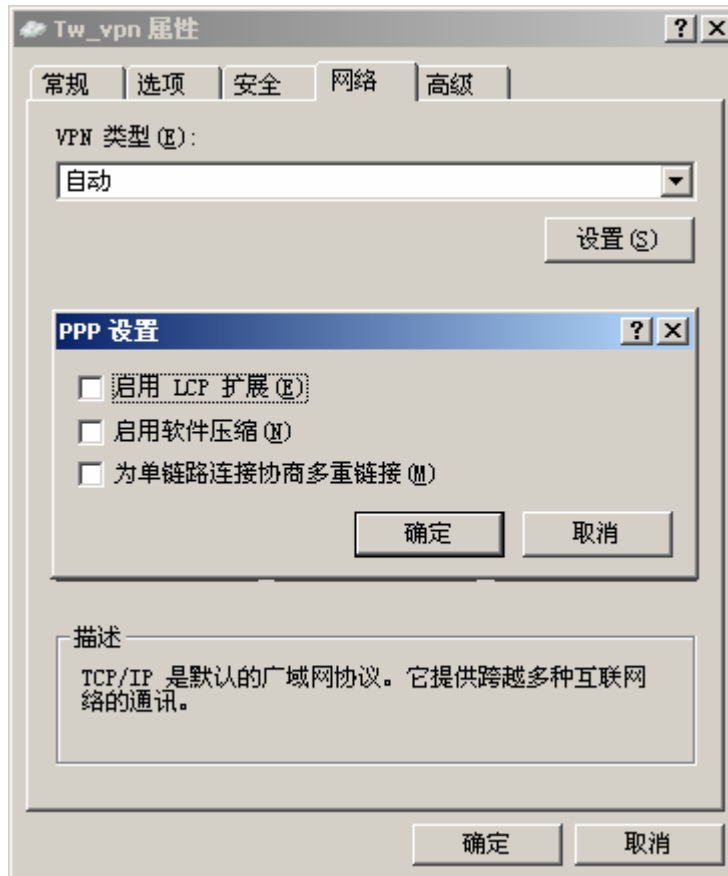
数据加密选择 可选加密(没有加密也可以连接)

选择 质询握手身份验证协议(CHAP)

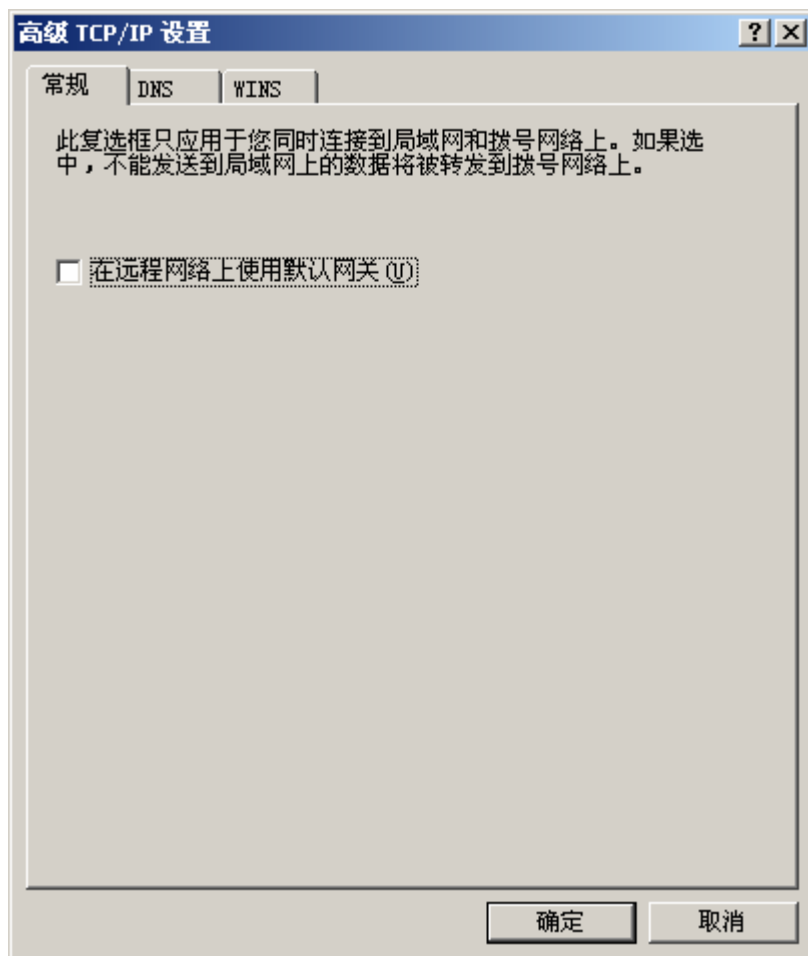


网络选项 - 设置

去掉 启用 LCP 扩展



Internet 协议(TCP/IP) – 属性 – 高级 – 常规  
去掉 在远程网络上使用默认网关。



VPN 连接配置完成。

--0x0d\_0b--

Linux 下连接 VPN [不会] 略 那位大虾补全??

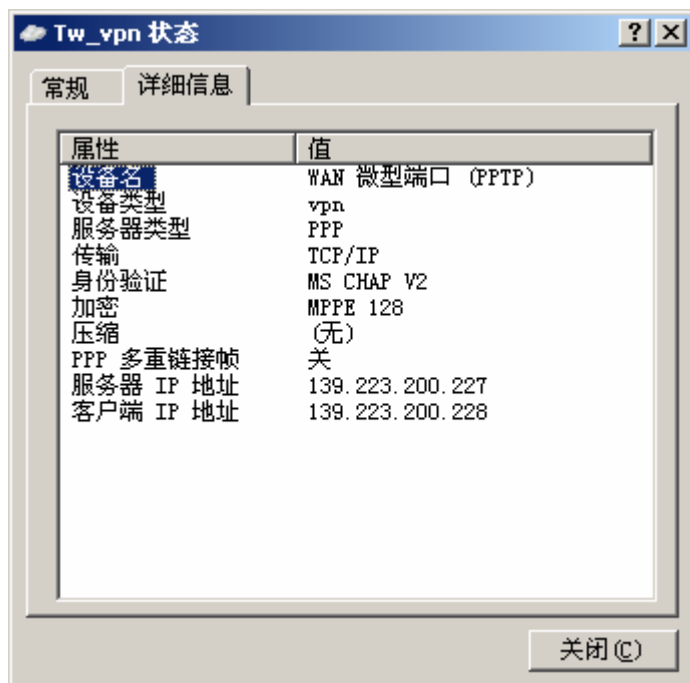
--0x0d\_0c--

利用

1. 可以直接获取在对方同网络段内的一个公网 ip，达到了掩藏自己的 log 的目的。甚至不用擦除在被黑机器上的痕迹。
2. 如果对方有内网，作 vpn 的这台机器是网关，那么我们可以通过拨 VPN 获得对方网络的一个内网地址，NEXT HACK。
3. 访问速度加快，某些时候访问国外的网络不快，但是某台机器访问国外却非常快，我们自己的机器到这台机器的速度也非常快，于是我们把这台机器作了一个 vpn，拨上 vpn 获得 ip，yeah，我们现在访问国外也快。
4. Other。

## Example

139.223.200.224 是我做好的 VPN



没有添加默认网关，现在访问除了 139.223.\*.\*是通过 VPN 访问的外，访问其他 ip 都是使用本机的真实 IP

```
C:\>netstat -r
```

## IPv4 Route Table

## Interface List

```
0x1 ..... MS TCP Loopback interface
0x10003 ...***** ..... Dual-band Wi-Fi Wireless Mini PCI Adapter
0x10004 ...***** ..... Intel(R) PRO/1000 MT Mobile Connection
0x40005 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
```

## Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
139.223.0.0	255.255.0.0	139.223.200.228	139.223.200.228	1
139.223.200.224	255.255.255.255	192.168.1.1	192.168.1.2	20
139.223.200.228	255.255.255.255	127.0.0.1	127.0.0.1	50
139.223.255.255	255.255.255.255	139.223.200.228	139.223.200.228	50

如果要通过 VPN 访问 218.1.71.119 需要添加一个路由

```
Example
route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
      destination^      ^mask      ^gateway      metric^      ^
                          Interface^
Route add 218.1.71.119 mask 255.255.255.225 139.223.200.228 if 0x40005
```

现在我们访问 218.1.71.119 走的路由都是从 139.223.200.228 开始。  
Ssh 到 218.1.71.119 机器上查看

```
[kaka@core kaka]$ ifconfig | grep 218 && w
      inet addr:218.1.71.119 Bcast:218.1.71.127 Mask:255.255.255.224
20:23:37 up 146 days, 9:42, 2 users, load average: 0.02, 0.03, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
kaka      pts/0    222.64.226.117 7:56pm 14:46  0.03s  0.03s  -bash
kaka      pts/1    139.223.200.228 8:21pm  0.00s  0.05s  0.01s  w
```

在本机 tracert 218.1.71.119 结果

```
C:\>tracert 218.1.71.119 -d

Tracing route to 218.1.71.119 over a maximum of 30 hops

  1  414 ms  415 ms  414 ms  139.223.200.227
  2  415 ms  408 ms  409 ms  139.223.200.193
  3  400 ms  403 ms  402 ms  10.6.1.2
  4  411 ms  401 ms  399 ms  203.160.226.229
  5  387 ms  389 ms  381 ms  203.160.227.241
  6  404 ms  408 ms  404 ms  203.160.225.206
  7  670 ms  684 ms  692 ms  202.97.33.157
  8  717 ms  718 ms  714 ms  202.97.35.45
  9  714 ms  717 ms  701 ms  202.101.63.241
 10  708 ms  715 ms  720 ms  202.109.0.145
 11  727 ms  728 ms  737 ms  202.109.0.166
 12  739 ms  754 ms  764 ms  218.1.1.237
 13  763 ms  760 ms  756 ms  218.1.1.206
 14  761 ms  761 ms  766 ms  218.1.71.204
 15  750 ms  742 ms  739 ms  218.1.71.119

Trace complete.
```

呵呵，速度慢点，我现在是 TW 佬了，这只是演示:D。

--0x0e--

其它

### Example

想对 218.0.0.0 使用 VPN 进行访问，需要添加路由如下

```
Route add 218.0.0.0 mask 255.0.0.0 139.223.200.228 if 0x40005
```

想对 218.1.0.0 使用 VPN 进行访问，需要添加路由如下

```
Route add 218.1.0.0 mask 255.255.0.0 139.223.200.228 if 0x40005
```

等等，总结说，想对那些 ip 使用 VPN 进行访问，就在本机添加一条对应的路由。

### [注意]

在进行路由添加的时候，一般变化的是要访问的 ip 地址或者地址段，mask 掩码地址，以及 interface 网络接口。

添加路由格式

对于直接获得公网 IP 的路由添加格式

Route add [需要经过 VPN 访问的 IP 或 IP 段] mask [IP 或者 IP 段对应的网络掩码] 拨上 VPN 后获得的 IP 地址 if 网络接口[WAN (PPP/SLIP) Interface]

对于获得内网 IP 地址，如果想利用 VPN 访问其他 IP 或 IP 段的路由添加格式

Route add [需要经过 VPN 访问的 IP 或 IP 段] mask [IP 或者 IP 段对应的网络掩码] 做 VPN 机器的 IP 地址 if 网络接口[WAN (PPP/SLIP) Interface]

### Example

```
Route add 218.1.71.119 mask 255.255.255.255 219.163.8.244 if 0x*****
```

--0x0f--

Q&A

.....