SecPath防火墙静态网段地址转换在L2TP VPN中的典型配置

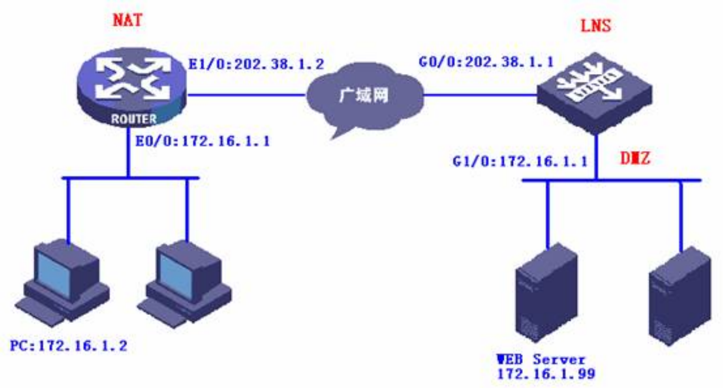
赵彪 2006-09-30 发表

SecPath防火墙静态网段地址转换在L2TP VPN中的典型配置

一、 组网需求：

私网相同的情况下，实现L2TP接入和访问。

二、 组网图



LNS：SecPath1000F，版本为Version 3.40, ESS 1604P01

三、 配置步骤

1. LNS的主要配置

使能L2TP

```
l2tp enable
```

在本地应用策略路由

```
ip local policy route-policy aaa
```

配置本端IKE名称

```
ike local-name zhongxin
```

定义防火墙包过滤规则

```
firewall packet-filter enable
firewall packet-filter default permit
```

配置网段地址静态转换

```
nat static inside ip 172.16.1.1 172.16.1.254 global ip 192.168.1.0 255.255.255.0
```

给L2TP用户分配地址池

```
domain system
 ip pool 1 10.0.0.2 10.0.0.10
```

配置L2TP帐号

```
local-user zhaobiao
 password simple 123
 service-type ppp
```

配置IKE参数

```
ike peer 1
 exchange-mode aggressive
 pre-shared-key 123
 id-type name
 remote-name fenzhi
 nat traversal
```

创建安全提议,采用默认参数

```
ipsec proposal 1
```

创建IPSEC模板，并引用IKE和安全提议

```
ipsec policy-template temp 1
 ike-peer 1
 proposal 1
```

创建IPSEC策略

```
ipsec policy pol1 1 isakmp template temp
```

定义策略路由的ACL

```
acl number 3000
```

```
 rule 0 permit udp source-port eq 1701
```

创建L2TP的虚接口

```
interface Virtual-Template1
 ppp authentication-mode chap
 ip address 10.0.0.1 255.255.255.0
 remote address pool 1
 nat outbound static
```

配置外网口

```
interface GigabitEthernet0/0
 ip address 202.38.1.1 255.255.255.0
 ipsec policy pol1
```

配置内网口

```
interface GigabitEthernet0/1
 ip address 10.2.0.1 255.255.255.0
```

配置DMZ区网口

```
interface GigabitEthernet1/0
 ip address 172.16.1.1 255.255.255.0
```

配置区域

```
firewall zone trust
 add interface GigabitEthernet0/1
 set priority 85
firewall zone untrust
 add interface GigabitEthernet0/0
 add interface Virtual-Template1
 set priority 5
firewall zone DMZ
 add interface GigabitEthernet1/0
 set priority 50
```

创建L2TP组

```
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 1
```

创建策略路由

```
route-policy aaa permit node 10
 if-match acl 3000
 apply output-interface GigabitEthernet0/0
```

配置默认路由

```
ip route-static 0.0.0.0 0.0.0.0 202.38.1.2
```

2.　NAT的主要配置

定义NAT转换的ACL

```
acl number 3000
 rule 0 permit ip source 172.16.1.0 0.0.0.255
```

配置内网口

```
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
```

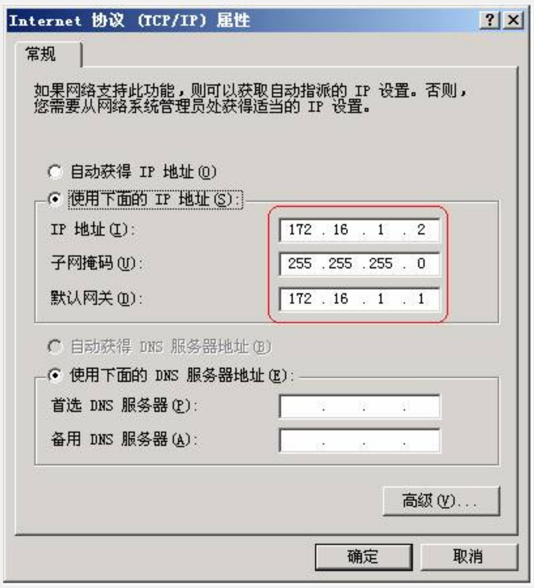
配置外网口

```
interface Ethernet1/0
 ip address 202.38.1.2 255.255.255.0
 nat outbound 3000
```

配置默认路由

```
ip route-static 0.0.0.0 0.0.0.0 202.38.1.1
```

3.　PC的主要配置



Internet 协议 (TCP/IP) 属性

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。

○ 自动获得 IP 地址(O)

● 使用下面的 IP 地址(S):

IP 地址(I): 172 . 16 . 1 . 2

子网掩码(U): 255 . 255 . 255 . 0

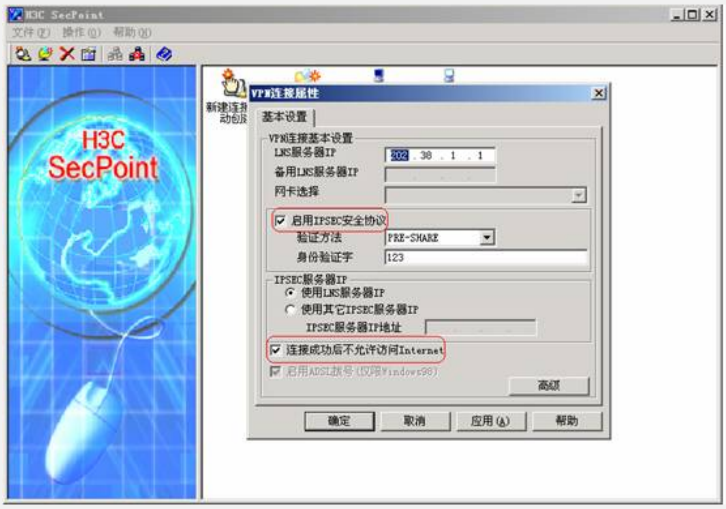
默认网关(D): 172 . 16 . 1 . 1

○ 自动获得 DNS 服务器地址(B)

● 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P): . . .

备用 DNS 服务器(A): . . .



VPN连接属性

基本设置

VPN连接基本设置

LNS服务器IP: 202 . 38 . 1 . 1

备用LNS服务器IP: . . .

网卡选择:

☑ 启用IPSEC安全协议

验证方法: PRE-SHARE

身份验证字: 123

IPSEC服务器IP

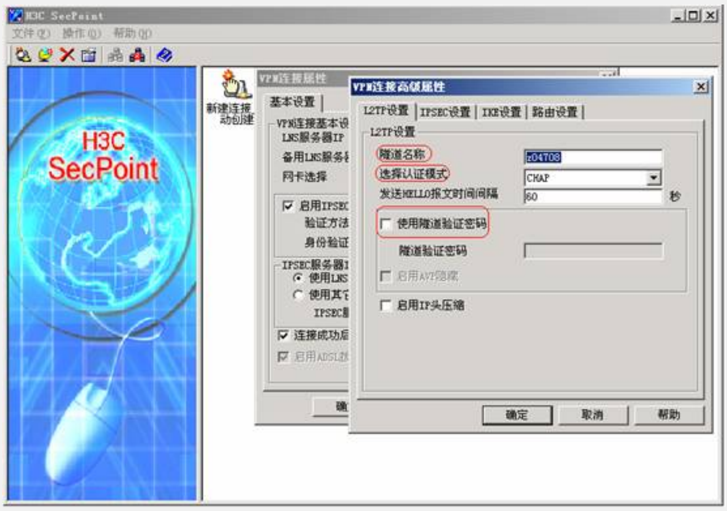
● 使用LNS服务器IP

○ 使用其它IPSEC服务器IP

IPSEC服务器IP地址: . . .

☑ 连接成功后不允许访问Internet

☑ 启用ADSL拨号(仅限Windows98)



VPN连接高级属性

L2TP设置 | IPSEC设置 | IKE设置 | 路由设置

L2TP设置

隧道名称: z04708

选择认证模式: CHAP

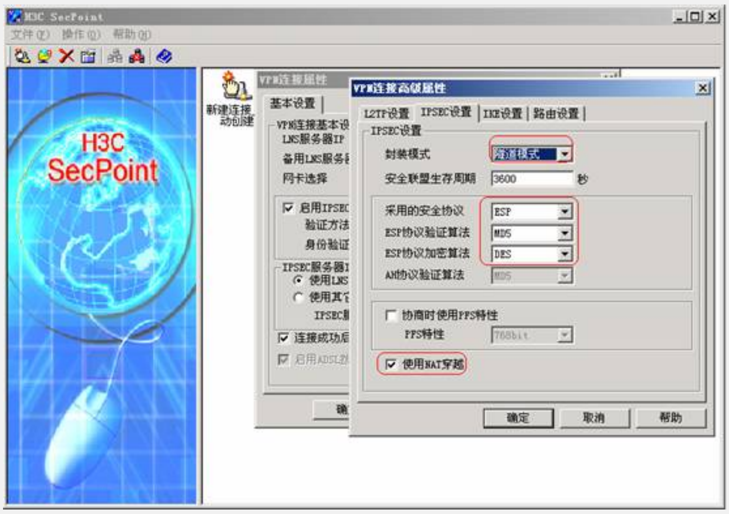
发送HELLO报文时间间隔: 60 秒

☐ 使用隧道验证密码

隧道验证密码:

☐ 启用AVP隐藏

☐ 启用IP头压缩



IPSEC设置

封装模式 隧道模式

安全联盟生存周期 3600 秒

采用的安全协议 ESP

ESP协议验证算法 MD5

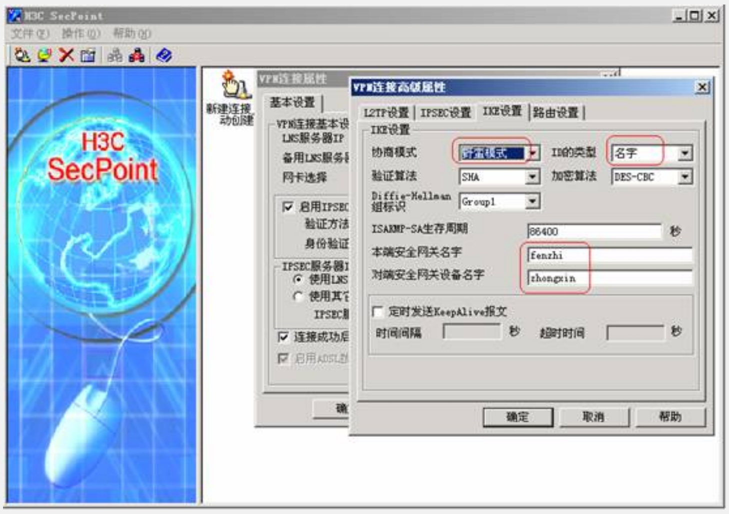
ESP协议加密算法 DES

AH协议验证算法 MD5

☐ 协商时使用PFS特性

PFS特性 768bit

☑ 使用NAT穿越



IKE设置

协商模式 野蛮模式 ID的类型 名字

验证算法 SHA 加密算法 DES-CBC

Diffie-Hellman组标识 Group1

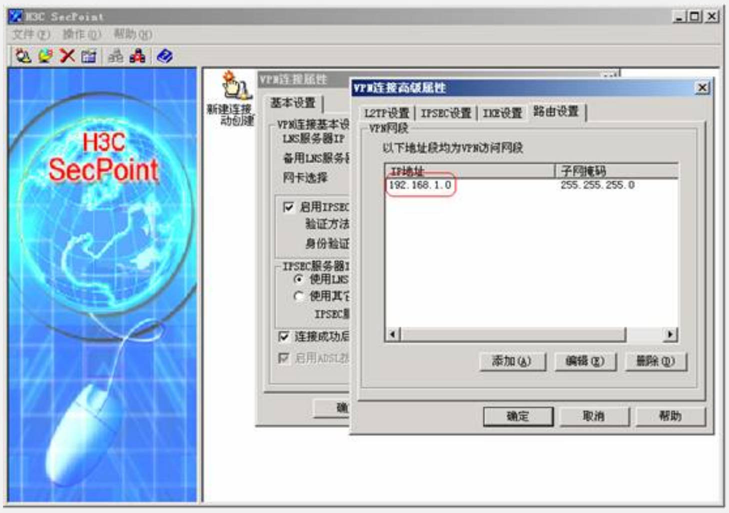
ISAKMP-SA生存周期 86400 秒

本端安全网关名字 fenzhi

对端安全网关设备名字 zhongxin

☐ 定时发送KeepAlive报文

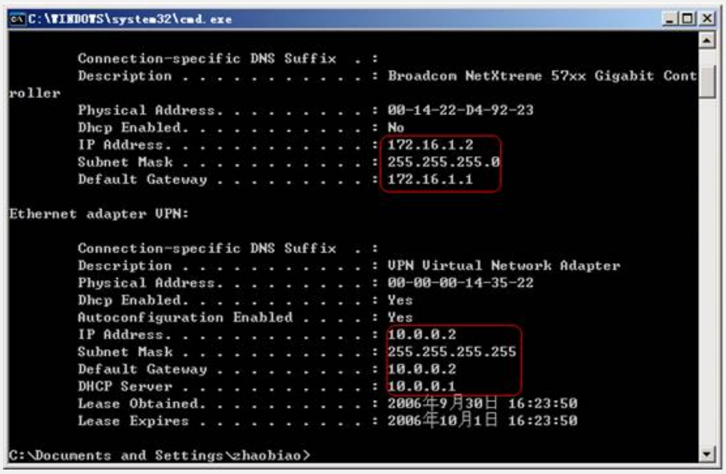
时间间隔 秒 超时时间 秒



VPN网段

以下地址段均为VPN访问网段

IP地址	子网掩码
192.168.1.0	255.255.255.0



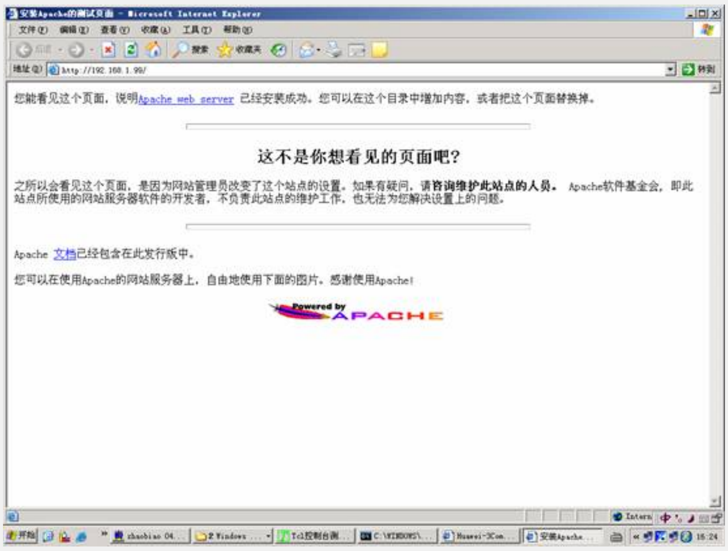
```
C:\WINDOWS\system32\cmd.exe

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Broadcom NetXtreme 57xx Gigabit Cont
roller
        Physical Address. . . . . . . . . : 00-14-22-D4-92-23
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 172.16.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.1.1

Ethernet adapter VPN:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VPN Virtual Network Adapter
        Physical Address. . . . . . . . . : 00-00-00-14-35-22
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.0.0.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 10.0.0.2
        DHCP Server . . . . . . . . . . . : 10.0.0.1
        Lease Obtained. . . . . . . . . . : 2006年9月30日 16:23:50
        Lease Expires . . . . . . . . . . : 2006年10月1日 16:23:50

C:\Documents and Settings\zhaobiao>
```



安装Apache的测试页面 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
搜索 收藏夹
地址(D) http://192.168.1.99/
转到

您能看见这个页面，说明Apache web server 已经安装成功。您可以在这个目录中增加内容，或者把这个页面替换掉。

这不是你想看见的页面吧?

之所以会看见这个页面，是因为网站管理员改变了这个站点的设置。如果有疑问，**请咨询维护此站点的人员。** Apache软件基金会，即此站点所使用的网站服务器软件的开发者，不负责此站点的维护工作，也无法为您解决设置上的问题。

Apache 文档已经包含在此发行版中。

您可以在使用Apache的网站服务器上，自由地使用下面的图片。感谢使用Apache!

四、 配置关键点

1. VRP3.4-R1210P01及以前版本的静态地址段转换的命令为nat static net-to-net；
2. SecPoint必须配置192.168.1.0/24的路由；
3. 由于做了net static net-to-net，访问对端私网地址不再是172.16.1.X/24，而是192.168.1.X/24，最后一位地址不变；
4. 策略路由必须应用在Local。