DVPN NAT穿越典型配置组网

赵彪　2006-09-14 发表

DVPN穿越Nat典型配置组网

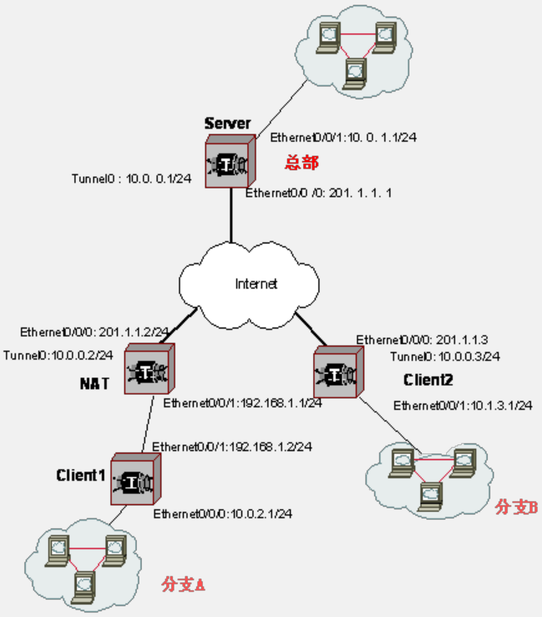
一、 组网需求

如下图所示，总部和两个分支机构分支A和分支B分别建立DVPN连接，其中分支A的私有网络需要通过NAT转换与总部私有网络连接，需要实现DVPN的NAT穿越。

? 　在注册和会话过程中需要使用缺省的算法套件1，即加密算法为des、验证算法为MD5，使用dh-gropp1算法进行密钥协商。

? 　数据传输采用IPSec进行加密保护，也使用缺省的算法套件1，即加密算法为des、验证算法为MD5，使用dh-gropp1算法进行密钥协商。

二、 组网图


Server
Ethernet0/0/1:10. 0. 1.1/24
总部
Tunnel0 : 10.0. 0.1/24
Ethernet0/0 /0: 201. 1. 1. 1
Internet
Ethernet0/0/0: 201.1.1.2/24
Tunnel0:10.0.0.2/24
NAT
Ethernet0/0/1:192.168.1.1/24
Ethernet0/0/0: 201.1.1.3
Tunnel0: 10.0.0.3/24
Client2
Ethernet0/0/1:10.1.3.1/24
Ethernet0/0/1:192.168.1.2/24
Client1
Ethernet0/0/0:10.0.2.1/24
分支B
分支A

三、 配置步骤

1. 配置Server

配置Ethernet0/0/0接口

```
[Server] interface Ethernet0/0/0
[Server-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
[Server-Ethernet0/0/0] quit
```

配置Ethernet0/0/1接口

```
[Server] interface Ethernet0/0/1
[Server-Ethernet0/0/1] ip address 10.0.1.1 255.255.255.0
[Server-Ethernet0/0/1] quit
```

配置Tunnel0接口

```
[Server] interface tunnel 0
[Server-Tunnel0] tunnel-protocol udp dvpn
[Server-Tunnel0] dvpn interface-type server
[Server-Tunnel0] ip address 10.0.0.1 255.255.255.0
[Server-Tunnel0] source Ethernet0/0/0
[Server-Tunnel0] dvpn dvpn-id 1
[Server-Tunnel0] quit
```

配置路由信息

```
[Server] ip route-static 10.0.2.0 255.255.255.0 10.0.0.2
[Server] ip route-static 10.0.3.0 255.255.255.0 10.0.0.3
```

2. 配置NAT设备

配置Ethernet0/0/0接口

```
[Nat] interface Ethernet0/0/0
[Nat-Ethernet0/0/0] ip address 201.1.2.1 255.255.255.0
```

```
[Nat-Ethernet0/0/0] nat outbound 3000
[Nat-Ethernet0/0/0] quit
配置Ethernet0/0/1接口
[Nat] interface Ethernet0/0/1
[Nat-Ethernet0/0/1] ip address 192.168.1.1 255.255.255.0
[Nat-Ethernet0/0/1] dhcp select interface
[Nat-Ethernet0/0/1] quit
配置ACL
[Nat] acl number 3000
[Nat-Acl-Adv-3000] rule permit ip
```

3. 配置分支A

```
配置Ethernet0/0/0接口通过dhcp获取地址。
[Client1] interface Ethernet0/0/0
[Client1-Ethernet0/0/0] ip address dhcp-alloc
[Client1-Ethernet0/0/0] quit
配置Ethernet0/0/1接口
[Client1] interface Ethernet0/0/1
[Client1-Ethernet0/0/1] ip address 10.0.2.1 255.255.255.0
[Client1-Ethernet0/0/1] quit
配置dvpn-class
[Client2] dvpn class testserver
[Client1-class-testserver] public-ip 201.1.1.1
[Client1-class-testserver] quit
配置Tunnel0接口属性
[Client1] interface tunnel 0
[Client1-Tunnel0] ip address 10.0.0.2 255.255.255.0
[Client1-Tunnel0] tunnel-protocol udp dvpn
[Client1-Tunnel0] source Ethernet0/0/0
[Client1-Tunnel0] dvpn interface-type client
[Client1-Tunnel0] dvpn server testserver
[Client1-Tunnel0] dvpn vpn-id 1
[Client1-Tunnel0] quit
配置静态路由
[Client1] ip route-static 10.0.1.0 255.255.255.0 10.0.0.1
[Client1] ip route-static 10.0.3.0 255.255.255.0 10.0.0.3
```

4. 配置分支B

```
配置Ethernet0/0/0接口
[Client2] interface Ethernet0/0/0
[Client2-Ethernet0/0/0] ip address 201.1.3.1 255.255.255.0
[Client2-Ethernet0/0/0] quit
配置Ethernet0/0/1接口
[Client2] interface Ethernet0/0/1
[Client2-Ethernet0/0/1] ip address 10.0.3.1 255.255.255.0
[Client2-Ethernet0/0/1] quit
配置dvpn-class
[Client2] dvpn class testserver
[Client2-class-testserver] public-ip 201.1.1.1
[Client2-class-testserver] quit
配置Tunnel0接口属性
[Client2] interface tunnel 0
[Client2-Tunnel0] ip address 10.0.0.3 255.255.255.0
[Client2-Tunnel0] tunnel-protocol udp dvpn
[Client2-Tunnel0] source Ethernet0/0/0
[Client2-Tunnel0] dvpn interface-type client
[Client2-Tunnel0] dvpn server testserver
[Client2-Tunnel0] dvpn vpn-id 1
[Client2-Tunnel0] quit
配置静态路由
[Client2] ip route-static 10.0.1.0 255.255.255.0 10.0.0.1
[Client2] ip route-static 10.0.2.0 255.255.255.0 10.0.0.2
```

四、 配置关键点

> 1、只有支持DVPN二期的设备才具有加密功能；
> 2、NAT后面的分支不能和其它分支之间单独建立隧道(Session)；
> 3、SecPath安全网关产品VRP3.4 E1604以前的版本都是DVPN一期，不支持加密功能。