# AR28/AR46系列路由器DVPN穿越NAT的典型配置

岳斌 2006-09-13 发表

**AR28/AR46系列路由器DVPN穿越NAT的典型配置**

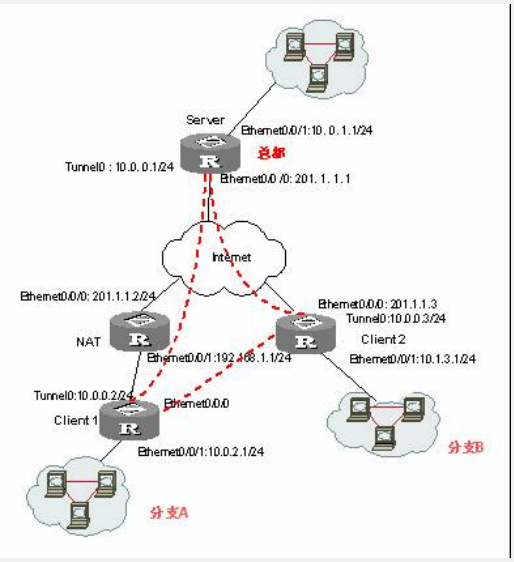
**【需求】**

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。具体配置要求如下：

？ 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，使用算法套件6，即加密算法为3des、验证算法为MD5，使用dh-gropp2算法进行密钥协商。

**【组网图】**




**【配置脚本】**

| **Server的配置教本** |
| --- |
| **# 使能DVPN功能。**<br><Server> system-view<br>[Server] dvpn service enable<br>**# 配置Ethernet0/0/0接口。**<br>[Server] interface Ethernet0/0/0<br>[Server-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0<br>[Server-Ethernet0/0/0] quit<br>**# 创建DVPN策略，并配置IPSec的算法套件为5**<br>[Server] dvpn policy 1<br>[Server -dvpn-policy-1] data algorithm-suite 5<br>**# 配置Ethernet0/0/1接口。**<br>[Server] interface Ethernet0/0/1<br>[Server-Ethernet0/0/1] ip address 10.0.1.1 255.255.255.0<br>[Server-Ethernet0/0/1] quit<br>**# 配置Tunnel0接口。**<br>[Server] interface tunnel 0<br>[Server-Tunnel0] tunnel-protocol udp dvpn<br>[Server-Tunnel0] dvpn interface-type server<br>[Server-Tunnel0] ip address 10.0.0.1 255.255.255.0<br>[Server-Tunnel0] source Ethernet0/0/0<br>[Server-Tunnel0] dvpn dvpn-id 1<br>[Server-Tunnel0] dvpn policy 1<br>[Server-Tunnel0] quit<br>**# 配置路由信息。**<br>[Server] ip route-static 10.0.2.0 255.255.255.0 10.0.0.2<br>[Server] ip route-static 10.1.3.0 255.255.255.0 10.0.0.3 |
| **NAT设备的配置脚本** |

**# 配置Ethernet0/0/0接口。**
[Nat] interface Ethernet0/0/0
[Nat-Ethernet0/0/0] ip address 201.1.1.2 255.255.255.0
[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

**Client1的配置脚本**

**# 使能DVPN功能**
<Client1> system-view
[Client1] dvpn service enable
**# 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。**
[Client1] dvpn class testserver
[Client1-dvpn-class-testserver] public-ip 201.1.1.1
[Client1-dvpn-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 10.1.3.0 255.255.255.0 10.0.0.3

**Client2的配置脚本**

**# 使能DVPN功能**
<Client2> system-view
[Client2] dvpn service enable
**# 配置Ethernet0/0/0接口。**
[Client2] interface Ethernet0/0/0
[Client2-Ethernet0/0/0] ip address 201.1.1.3 255.255.255.0
[Client2-Ethernet0/0/0] quit
**# 配置Ethernet0/0/1接口。**
[Client2] interface Ethernet0/0/1
[Client2-Ethernet0/0/1] ip address 10.1.3.1 255.255.255.0
[Client2-Ethernet0/0/1] quit
**# 配置dvpn-class。**
[Client2] dvpn class testserver
[Client2-dvpn-class-testserver] public-ip 201.1.1.1
[Client2-dvpn-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 server
[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

**【提示】**

Server、Client1和Client2之间建立Session后，所有传输的数据在缺省情况下都使用IPSec加密，并使用算法套件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。