MSR系列路由器中心设备处于NAT网关后面时分支与中心建立Ipsec隧道功能的基础配置

陈安【技术大咖】 2007-03-21 发表

MSR系列路由器中心设备处于NAT网关后面时分支与中心建立Ipsec隧道功能的基础配置

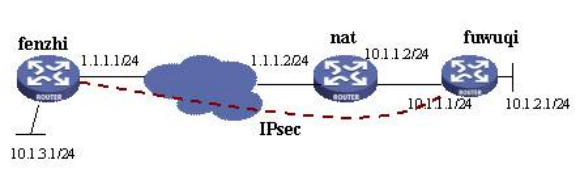
关键字：MSR;NAT;IPSEC;穿越

一、组网需求：

中心设备位于NAT网关后面，分支设备直接挂在公网。分支要与中心设备建立Ipsec连接。

设备清单：MSR系列路由器3台

二、组网图：



三、配置步骤：

适用设备和版本：MSR系列、Version 5.20, Beta 1105后所有版本。

fenzhi配置

```
<fenzhi>dis cu
#
 sysname fenzhi
#
 ike local-name fenzhi   //定义本端IKE 的名字
#
ike proposal 1
#
ike peer zhongxin
 exchange-mode aggressive  //采用野蛮模式
 pre-shared-key 123
 id-type name
 remote-name zhongxin
 remote-address 1.1.1.2   //远端地址为nat设备的公网出口地址
 nat traversal        //使能nat穿越
#
ipsec proposal 1
#
ipsec policy zhongxin 1 isakmp
 security acl 3000
 ike-peer zhongxin
 proposal 1
#
acl number 3000    //定义要进行加密的数据
 rule 0 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 1 deny ip
#
interface Ethernet2/0
 ip address 1.1.1.1 255.255.255.0
 ipsec policy zhongxin  //在接口里应用Ipsec policy
#
interface LoopBack0
 ip address 10.1.3.1 255.255.255.255
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2 preference 60  //定义静态路由
#
```

NAT 配置

```
#
 sysname NAT
#
acl number 3000   //定义进行NAT转换的私网网段
 rule 0 permit ip source 10.1.1.0 0.0.0.255
 rule 1 deny ip
#
interface Ethernet0/0
 ip address 1.1.1.2 255.255.255.0
 //使能NAT
 nat outbound 3000
 //开启nat server的功能
 nat server protocol udp global 1.1.1.2 500 inside 10.1.1.1 500
#
interface Ethernet0/1
 ip address 10.1.1.2 255.255.255.0
#
```

zhongxin 配置

```
#
 sysname zhongxin
#
 ike local-name zhongxin    //定义本端IKE 的名字
#
ike proposal 1
#
ike peer fenzhi
 exchange-mode aggressive  //采用野蛮模式
 pre-shared-key 123
 id-type name
 remote-name fenzhi
 remote-address 1.1.1.1   //远端地址为分支设备公网出口地址
 nat traversal            //使能nat穿越
#
ipsec proposal fenzhi
#
ipsec policy fenzhi 1 isakmp
 security acl 3000
 ike-peer fenzhi
 proposal fenzhi
#
acl number 3000    //定义要进行加密的数据
 rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
 rule 1 deny ip
#
interface Ethernet1/0
 ip address 10.1.1.1 255.255.255.0
 ipsec policy fenzhi  //在接口里应用Ipsec policy
#
interface LoopBack0
 ip address 10.1.2.1 255.255.255.255
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.2 preference 60
#
```

四、配置关键点:

1) 分支设备的IKE peer远端地址为NAT设备的公网出口地址;

2) NAT设备上要启用nat server功能，打开UDP 500端口;

3) 两个NAT设备的公网口地址要固定。