SR6600路由器IPSec VPN多分支NAT模板穿越功能的配置

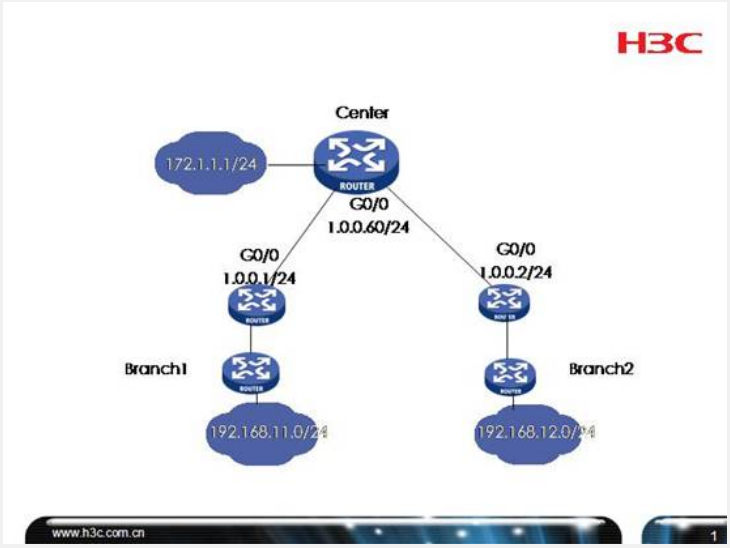
管祥杰 2008-12-11 发表

SR6600路由器
GRE Over IPSec配合OSPF穿越NAT多分支互通

关键词：SR66;IPSec;IKE;野蛮模式;模板;VPN;多分支互通;NAT;穿越;OSPF;GRE

一、组网需求:
总部对多个分支提供IPSec VPN接入，分支出口存在NAT设备，因此总部与分支之间配置成野蛮模式和NAT穿越，总部路由器不配置ACL，而使用安全模板，总部和分支之间通过内网Loopback建立GRE隧道，分支通过建立ACL使分支Loopback和总部Loopback之间的GRE通过IPSec互通，建立好GRE隧道后，在隧道上运行OSPF，使各内部路由互通，分支之间的流量通过总部转发，需要注意的是**Loopback口不能添加到OSPF中**
设备清单：SR6600路由器5台

二、组网图:



三、配置步骤:

Center的配置

```
#
 //本地IKE名字
 ike local-name center
#
//配置到分支1的IKE Peer
ike peer branch1
 //配置成野蛮模式
 exchange-mode aggressive
 //配置预共享密钥
 pre-shared-key h3c-sr66-branch1
 //使用名字作为身份标识
 id-type name
 //配置对端名字
 remote-name branch1
 //配置NAT穿越
 nat traversal
#
//配置到分支1的IKE Peer
ike peer branch2
 //配置成野蛮模式
 exchange-mode aggressive
 //配置预共享密钥
 pre-shared-key h3c-sr66-branch2
 //使用名字作为身份标识
 id-type name
 //配置对端名字
 remote-name branch2
 //配置NAT穿越
 nat traversal
#
//配置默认安全提议
ipsec proposal default
#
//配置分支1的安全模板，序号1
ipsec policy-template branch1 1
 //指定IKE Peer
 ike-peer branch1
 //指定安全提议
 proposal default
#
//配置分支2的安全模板，序号1
ipsec policy-template branch2 1
 //指定IKE Peer
 ike-peer branch2
 //指定安全提议
 proposal default
#
//根据安全模板branch1创建安全策略branch序号1
ipsec policy branch 1 isakmp template branch1
#
//根据安全模板branch2创建安全策略branch序号2
ipsec policy branch 2 isakmp template branch2
#
//总部外网接口G0/0
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 //外网接口地址
 ip address 1.0.0.60 255.255.255.0
 //绑定安全策略
 ipsec policy branch
#
interface GigabitEthernet0/1
 port link-mode route
 //总部内网接口地址
 ip address 172.0.0.1 255.255.255.0
#
 //11.0.0.0/8网段为分支1转换后的出口地址网段，1.0.0.1为分支1的NAT设备
 ip route-static 11.0.0.0 255.0.0.0 1.0.0.1
 //12.0.0.0/8网段为分支2转换后的出口地址网段，1.0.0.2为分支2的NAT设备
 ip route-static 12.0.0.0 255.0.0.0 1.0.0.2
 //192.168.1.0/24网段为分支1内网网段，1.0.0.1为分支1的NAT设备
 ip route-static 192.168.1.0 255.255.255.0 1.0.0.1
 //192.168.2.0/24网段为分支2内网网段，1.0.0.2为分支2的NAT设备
 ip route-static 192.168.2.0 255.255.255.0 1.0.0.2
#
```

Branch1配置

```
#
 //分支1本地的IKE名字
 ike local-name branch1
#
//配置到总部的IKE Peer
ike peer center
 //使用野蛮模式
 exchange-mode aggressive
 //配置预共享密钥，与总部配置一致
 pre-shared-key h3c-sr66-branch1
 //使用名字作为身份标识
 id-type name
 //配置对端名字
 remote-name center
 //指定对端IP地址，因为总部路由器出接口地址不变
 remote-address 1.0.0.60
 //配置NAT穿越
 nat traversal
#
//默认的安全提议
ipsec proposal default
#
//到总部的安全策略，序号1
ipsec policy center 1 isakmp
 //指定ACL
 security acl 3000
 //指定IKE Peer
 ike-peer center
 //指定安全提议
 proposal default
#
//配置流量的ACL
acl number 3000
 //此规则匹配从分支1内网到总部内网的流量
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 172.0.0.0 0.255.255.255
#
//分支1的外网出接口
interface GigabitEthernet0/0
 port link-mode route
 //出接口地址
 ip address 10.0.1.2 255.255.255.0
 //绑定安全策略
 ipsec policy center
#
interface GigabitEthernet0/1
 port link-mode route
 //分支1内网接口地址
 ip address 192.168.1.1 255.255.255.0
#
 //配置默认路由，下一跳指向NAT设备
 ip route-static 0.0.0.0 0.0.0.0 10.0.1.1
#
```

Branch2配置

```
#
 //分支2本地的IKE名字
 ike local-name branch2
#
//配置到总部的IKE Peer
ike peer center
 //使用野蛮模式
 exchange-mode aggressive
 //配置预共享密钥，与总部配置一致
 pre-shared-key h3c-sr66-branch2
 //使用名字作为身份标识
 id-type name
 //配置对端名字
 remote-name center
 //指定对端IP地址，因为总部路由器出接口地址不变
 remote-address 1.0.0.60
 //配置NAT穿越
 nat traversal
#
//默认的安全提议
ipsec proposal default
#
//到总部的安全策略，序号1
ipsec policy center 1 isakmp
 //指定ACL
 security acl 3000
 //指定IKE Peer
 ike-peer center
 //指定安全提议
 proposal default
#
//配置流量的ACL
acl number 3000
 //此规则匹配从分支2内网到总部内网的流量
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 172.0.0.0 0.255.255.255
#
//分支2的外网出接口
interface GigabitEthernet0/0
 port link-mode route
 //出接口地址
 ip address 10.0.2.2 255.255.255.0
 //绑定安全策略
 ipsec policy center
#
interface GigabitEthernet0/1
 port link-mode route
 //分支2内网接口地址
 ip address 192.168.2.1 255.255.255.0
#
 //配置默认路由，下一跳指向NAT设备
 ip route-static 0.0.0.0 0.0.0.0 10.0.2.1
#
```

分支1 nat设备配置

```
#
 //配置NAT地址池
 nat address-group 0 11.0.0.1 11.0.0.10
#
//配置需要被NAT处理的地址
acl number 2000
 rule 0 permit source 10.0.1.0 0.0.0.255
#
//NAT设备外网接口
interface GigabitEthernet0/0
 port link-mode route
 //配置动态NAT
 nat outbound 2000 address-group 0
 //接口地址
 ip address 1.0.0.1 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 //连接分支1路由器的接口地址
 ip address 10.0.1.1 255.255.255.0
#
```

分支2 nat设备配置

```
#
 //配置NAT地址池
 nat address-group 0 12.0.0.1 12.0.0.10
#
//配置需要被NAT处理的地址
acl number 2000
 rule 0 permit source 10.0.2.0 0.0.0.255
#
//NAT设备外网接口
interface GigabitEthernet0/0
 port link-mode route
 //配置动态NAT
 nat outbound 2000 address-group 0
 //接口地址
 ip address 1.0.0.2 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 //连接分支2路由器的接口地址
 ip address 10.0.2.1 255.255.255.0
#
```

四、配置关键点:

1) IKE要配置成野蛮模式，可以参考IPSec穿越NAT设备的典型配置案例；

2) 总部可以不用配置ACL，配置安全模板动态生成ACL；

3) 分支需要必须配置路由，保证可以访问总部的外网接口；

4) 分支需要配置ACL，使特定流量匹配安全策略；

5) 总部配置的访问分支内网的路由用于触发进入外网出口，无具体意义。