

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

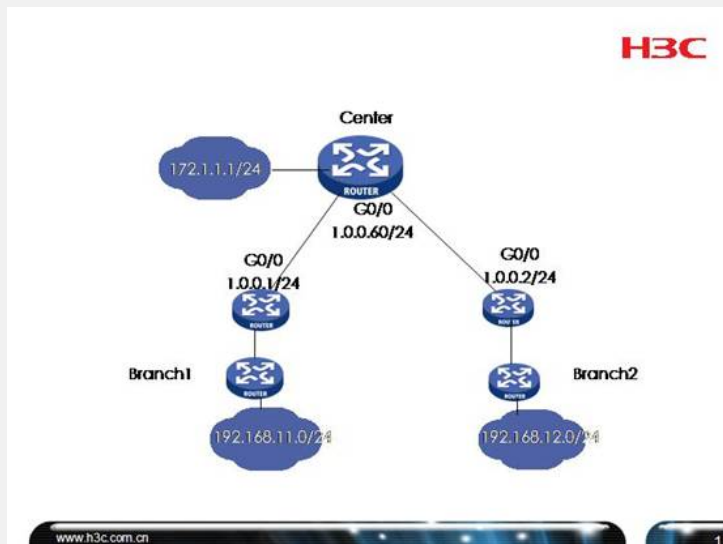
关键词：SR66;IPSec;IKE;野蛮模式;模板;VPN;多分支互通;NAT;穿越;OSPF;GRE

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  
#  
//OSPF的Router ID  
router id 172.0.0.1  
#  
//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2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
#
//用于建立GRE连接和OSPF Router ID的Loopback接口
interface LoopBack0
ip address 172.0.0.1 255.255.255.255
#
//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 172.1.1.1 255.255.255.0
#
//连接分支1的GRE隧道
interface Tunnel0
ip address 192.168.0.1 255.255.255.252
//指定源为Loopback0
source LoopBack0
//指定目的为分支1的Loopback0地址
destination 192.168.1.1
#
//连接分支2的GRE隧道
interface Tunnel1
ip address 192.168.0.5 255.255.255.252
//指定源为Loopback0
source LoopBack0
//指定目的为分支2的Loopback0地址
destination 192.168.2.1
#
ospf 1
area 0.0.0.0
//使能连接分支1的GRE隧道
network 192.168.0.4 0.0.0.3
//使能总部内网
network 172.1.1.0 0.0.0.255
//使能连接分支2的GRE隧道
network 192.168.0.0 0.0.0.3
#
//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
//192.168.1.1为分支1内Loopback，1.0.0.1为分支1的NAT设备
ip route-static 192.168.1.1 255.255.255.255 1.0.0.1
//192.168.2.1为分支2内Loopback，1.0.0.2为分支2的NAT设备
ip route-static 192.168.2.1 255.255.255.255 1.0.0.2
#

```

Branch1配置

```

#
//分支1本地的IKE名字
ike local-name branch1
#
//OSPF的Router ID
router id 192.168.1.1
#
//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 Loopback到总部Loopback的GRE流量
rule 0 permit gre source 192.168.1.1 0 destination 172.0.0.1 0
#
//用于创建于总部连接的GRE源和OSPF的Router ID的Loopback接口
interface LoopBack0
ip address 192.168.1.1 255.255.255.255
#
//分支1的外网出口
interface GigabitEthernet0/0
port link-mode route
//出口地址
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 192.168.11.1 255.255.255.0
#
//连接总部的GRE隧道
interface Tunnel0
ip address 192.168.0.2 255.255.255.252
//隧道源指定为Loopback0
source LoopBack0
//目的指定为总部的Loopback0
destination 172.0.0.1
#
ospf 1
area 0.0.0.0
//使能分支1内网
network 192.168.11.0 0.0.0.255
//使能GRE隧道
network 192.168.0.0 0.0.0.3
#
//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
#
//OSPF的Router ID
router id 192.168.2.1
#
//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 Loopback到总部Loopback的GRE流量
rule 0 permit gre source 192.168.2.1 0 destination 172.0.0.1 0
#
//用于创建GRE隧道源地址和OSPF Router ID的Loopback接口
interface LoopBack0
ip address 192.168.2.1 255.255.255.255
#
//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 192.168.12.1 255.255.255.0
#
//连接总部的GRE隧道
interface Tunnel0
ip address 192.168.0.6 255.255.255.252
//指定Loopback0为源地址
source LoopBack0
//目的地址为总部的Loopback0
destination 172.0.0.1
#
ospf 1
area 0.0.0.0
//使能GRE隧道
network 192.168.0.4 0.0.0.3
//使能分支2内网
network 192.168.12.0 0.0.0.255
#
//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) 大部分配置参考IPSec VPN多分支NAT穿越模板方式功能的配置；
- 2) 分支的ACL可以配置成精确的GRE流量；
- 3) 建立GRE隧道的地址必须是内网地址；
- 4) 不能将建立GRE隧道连接的Loopback接口加入到OSPF，否则连接会失效。