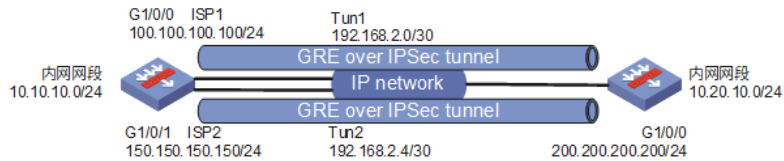


组网及说明



F1与F2建立两条IPsec隧道，一条主用，一条备用，当主用隧道出现故障时，流量切换到备用隧道。

配置步骤

1. Internet配置

```
interface GigabitEthernet0/0
ip address 100.100.100.1 255.255.255.0
#
interface GigabitEthernet0/1
ip address 150.150.150.1 255.255.255.0
#
interface GigabitEthernet0/2
ip address 200.200.200.1 255.255.255.0
```

2. F1配置

```
interface LoopBack0 # 配置作为建立GRE隧道源地址的环回口
ip address 192.168.1.1 255.255.255.255
#
interface LoopBack1 # 配置作为建立GRE隧道源地址的环回口
ip address 192.168.1.3 255.255.255.255
#
interface LoopBack10 # 配置作为内网地址的环回口
ip address 10.10.10.1 255.255.255.0
#
interface GigabitEthernet1/0/0 # 配置ISP1公网接口，调用IPSec策略
ip address 100.100.100.100 255.255.255.0
nat outbound name nat
ipsec apply policy ipsec-isp1
#
interface GigabitEthernet1/0/1 # 配置ISP2公网接口，调用IPSec策略
ip address 150.150.150.150 255.255.255.0
nat outbound name nat
ipsec apply policy ipsec-isp2
#
interface Tunnel1 mode gre # 配置GRE隧道1
ip address 192.168.2.1 255.255.255.252
source 192.168.1.1 # 源地址为lo 0地址
destination 192.168.1.2 # 目的地址为对端lo 0地址
keepalive 10 3 # 配置Keepalive检测GRE隧道是否正常通信
#
interface Tunnel2 mode gre # 配置GRE隧道2
ip address 192.168.2.5 255.255.255.252
source 192.168.1.3 # 源地址为lo 1地址
destination 192.168.1.4 # 目的地址为对端lo 1地址
keepalive 10 3
#
policy-based-route ipsec permit node 10 # 配置PBR，匹配主用公网出口和对端建立ipsec的流量走主用出口
if-match acl 3500
apply next-hop 100.100.100.1
#
policy-based-route ipsec permit node 20 # 配置PBR，匹配备用公网出口和对端建立ipsec的流量走备用出口
if-match acl 3501
```

```

apply next-hop 150.150.150.1
#
ip local policy-based-route ipsec # 本地调用策略路由, 如果不配置这个, 会导致备用出口的ipsec流量
根据路由表走主用出口, 从而导致ipsec协商失败。
#
security-zone name Trust # 将GRE隧道口与内网口加入Trust域
import interface LoopBack10
import interface Tunnel1
import interface Tunnel2
#
security-zone name Untrust # 将公网口加入Untrust域
import interface GigabitEthernet1/0/0
import interface GigabitEthernet1/0/1
#
zone-pair security source Local destination Trust # 放通Local到Trust, 用于业务网段互访, 由于实验
环境时环回口模拟内网网段, 因此是Local到Trust而不是Trust到Trust
packet-filter 2000
#
zone-pair security source Local destination Untrust # 放通Local到Untrust, 使GRE over IPSec隧道正
常建立
packet-filter 2000
#
zone-pair security source Trust destination Local # 放通Trust到Local, 用于业务网段互访, 由于实验
环境时环回口模拟内网网段, 因此是Trust到Local而不是Trust到Trust
packet-filter 2000
#
zone-pair security source Trust destination Trust # 放通Trust到Trust, 在真实的环境下配置实现业务
网段互访
packet-filter 2000
#
zone-pair security source Untrust destination Local # 放通Untrust到Local, 使GRE over IPSec隧道正
常建立
packet-filter 2000
#
ip route-static 0.0.0.0 0 100.100.100.1 # 公网主用路由
ip route-static 0.0.0.0 0 150.150.150.1 preference 65 # 公网备份路由
ip route-static 10.20.20.0 24 192.168.2.2 # 业务互访走主用隧道
ip route-static 10.20.20.0 24 192.168.2.6 preference 65 # 业务网段备份路由
ip route-static 192.168.1.2 32 100.100.100.1 # GRE over IPSec隧道1走ISP1
ip route-static 192.168.1.4 32 150.150.150.1 # GRE over IPSec隧道2走ISP2, 若没有此条路由, 会
因为接口地址与需协商的IPsec SA不一致导致无法正常协商IPsec SA
#
acl basic 2000 # 域间策略ACL
rule 0 permit
#
acl advance 3500 # PBR ACL1
rule 10 permit ip source 100.100.100.100 0 destination 200.200.200.200 0
#
acl advance 3501 # PBR ACL2
rule 10 permit ip source 150.150.150.150 0 destination 200.200.200.200 0
#
acl advanced name ipsec # IPSec ACL
rule 10 permit ip source 192.168.1.1 0 destination 192.168.1.2 0
rule 20 permit ip source 192.168.1.3 0 destination 192.168.1.4 0
#
acl advanced name nat # NAT ACL, 拒绝IPSec流量
rule 10 deny ip source 192.168.1.1 0 destination 192.168.1.2 0
rule 20 deny ip source 192.168.1.3 0 destination 192.168.1.4 0
rule 30 permit ip
#
ipsec transform-set 1 # 配置IPSec转换集
esp encryption-algorithm aes-cbc-256
esp authentication-algorithm sha1
#

```

```

ipsec policy ipsec-isp1 10 isakmp # 配置ISP1的IPSec策略
transform-set 1
security acl name ipsec # 匹配GRE隧道流
local-address 100.100.100.100
remote-address 200.200.200.200 # policy必须配置remote-address, 若采用policy-template则不是必
选
ike-profile isp1
#
ipsec policy ipsec-isp2 10 isakmp # 配置ISP2的IPSec策略
transform-set 1
security acl name ipsec # 匹配GRE隧道流
local-address 150.150.150.150
remote-address 200.200.200.200
ike-profile isp2
#
ike profile isp1 # 配置ISP1的IKE策略集
keychain 1
local-identity address 100.100.100.100
match remote identity address 200.200.200.200 255.255.255.255
proposal 1
#
ike profile isp2 # 配置ISP2的IKE策略集
keychain 1
local-identity address 150.150.150.150
match remote identity address 200.200.200.200 255.255.255.255
proposal 1
#
ike proposal 1 # 配置IKE proposal
encryption-algorithm aes-cbc-256
dh group2
#
ike keychain 1 # 配置IKE密钥
pre-shared-key address 200.200.200.200 255.255.255.255 key simple ipsec

```

### 3. F2配置

```

interface LoopBack0 # 配置作为建立GRE隧道源地址的环回口
ip address 192.168.1.2 255.255.255.255
#
interface LoopBack1 # 配置作为建立GRE隧道源地址的环回口
ip address 192.168.1.4 255.255.255.255
#
interface LoopBack10 # 配置作为内网地址的环回口
ip address 10.20.10.1 255.255.255.0
#
interface GigabitEthernet1/0/0 # 配置公网接口, 调用IPSec策略
ip address 200.200.200.200 255.255.255.0
nat outbound name nat
ipsec apply policy ipsec
#
interface Tunnel1 mode gre # 配置GRE隧道1
ip address 192.168.2.2 255.255.255.252
source 192.168.1.2
destination 192.168.1.1
keepalive 10 3
#
interface Tunnel2 mode gre # 配置GRE隧道2
ip address 192.168.2.6 255.255.255.252
source 192.168.1.4
destination 192.168.1.3
keepalive 10 3
#
security-zone name Trust # 将GRE隧道口与内网口加入Trust域
import interface LoopBack10
import interface Tunnel1
import interface Tunnel2

```

```
#
security-zone name Untrust # 将公网口加入Untrust域
import interface GigabitEthernet1/0/0
#
zone-pair security source Local destination Trust # 放通Local到Trust
packet-filter 2000
#
zone-pair security source Local destination Untrust # 放通Local到Untrust
packet-filter 2000
#
zone-pair security source Trust destination Local # 放通Trust到Local
packet-filter 2000
#
zone-pair security source Trust destination Trust # 放通Trust到Trust
packet-filter 2000
#
zone-pair security source Untrust destination Local # 放通Untrust到Local
packet-filter 2000
#
ip route-static 0.0.0.0 0 200.200.200.1 # 默认路由
ip route-static 10.20.10.0 24 192.168.2.1 # 业务互访走主用隧道
ip route-static 10.20.10.0 24 192.168.2.5 preference 65 # 业务网段备份路由
#
acl basic 2000 # 域间策略ACL
rule 0 permit
#
acl advanced name ipsec_to_isp1 # 前往ISP1的IPSec ACL
rule 10 permit ip source 192.168.1.2 0 destination 192.168.1.1 0
#
acl advanced name ipsec_to_isp2 # 前往ISP2的IPSec ACL
rule 10 permit ip source 192.168.1.4 0 destination 192.168.1.3 0
#
acl advanced name nat # NAT ACL
rule 10 deny ip source 192.168.1.2 0 destination 192.168.1.1 0
rule 20 deny ip source 192.168.1.4 0 destination 192.168.1.3 0
rule 30 permit ip
#
ipsec transform-set 1 # 配置IPSec转换集
esp encryption-algorithm aes-cbc-256
esp authentication-algorithm sha1
#
ipsec policy ipsec 10 isakmp # 配置前往ISP1的IPSec策略
transform-set 1
security acl name ipsec_to_isp1
local-address 200.200.200.200
remote-address 100.100.100.100
ike-profile to_isp1
#
ipsec policy ipsec 20 isakmp # 配置前往ISP2的IPSec策略
transform-set 1
security acl name ipsec_to_isp2
local-address 200.200.200.200
remote-address 150.150.150.150
ike-profile to_isp2
#
ike profile to_isp1 # 配置前往ISP1的IKE策略集
keychain to_isp1
local-identity address 200.200.200.200
match remote identity address 100.100.100.100 255.255.255.255
proposal 1
#
ike profile to_isp2 # 配置前往ISP2的IKE策略集
keychain to_isp2
local-identity address 200.200.200.200
```

```
match remote identity address 150.150.150.150 255.255.255.255
proposal 1
#
ike proposal 1 # 配置IKE proposal
encryption-algorithm aes-cbc-256
dh group2
#
ike keychain to_isp1 # 配置前往ISP1的IKE密钥
pre-shared-key address 100.100.100.100 255.255.255.255 key simple ipsec
#
ike keychain to_isp2 # 配置前往ISP2的IKE密钥
pre-shared-key address 150.150.150.150 255.255.255.255 key simple ipsec
```

#### 配置关键点

1. IPsec本身没有虚接口，无法实现主备切换，因此采用GRE over IPsec方式利用GRE的Tunnel接口实现主备切换。
2. NAT的优先级比IPsec高，因此必须在NAT的感兴趣流中拒绝掉IPsec的数据流，否则数据流会优先被NAT转换，然后会导致无法匹配IPsec感兴趣流。
3. F1是双出口，F2是单出口，因此F1必须要配置本地策略路由，确保主接口去对端协商IPsec的流量和备接口协商IPsec的流量分别走各自出口，否则会导致备接口协商IPsec的流量根据路由表走主接口，从而无法协商IPsec SA。