MSR V7平台路由器GRE over IPSEC对接典型配置

目录

1 配置需求或说明

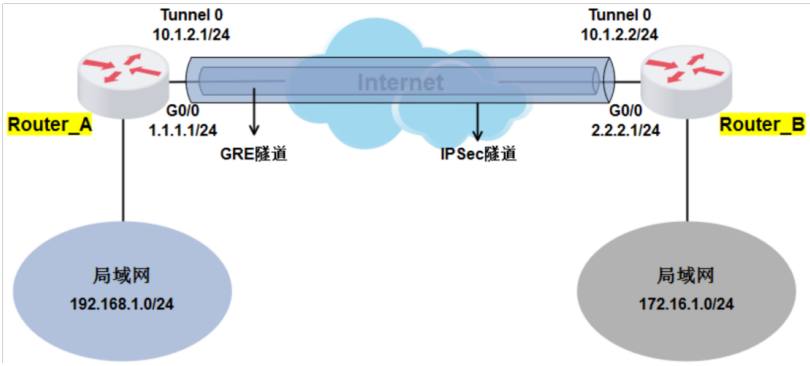
1.1 适用产品系列

本案例提到的MSR V7平台路由器是指Comware V7平台的MSR830-WiNet系列路由器，如MSR830-10BEI-WiNet 、MSR830-6EI-WiNet 、MSR830-5BEI-WiNet 、MSR830-6BHI-WiNet 、MSR830-10BHI-WiNet等

1.2 配置需求及实现的效果

RTA路由器外网口G0/0的地址为1.1.1.1（模拟运营商公网固定地址环境），RTB路由器外网口G0/0的地址为2.2.2.1（模拟运营商公网固定地址环境），两个路由器外网口地址之间路由可达可以互相ping通。要对RTA路由器所在的内网（192.168.1.0/24）与RTB路由器所在的内网（172.16.1.0/24），实现两端内网终端通过GRE over IPsec VPN 隧道进行互访。

2 组网图



3 配置步骤

3.1 配置路由器基本上网

#路由器基本上网配置省略， MSR V7路由器的上网具体设置步骤请参考“2.1.2 路由器外网使用固定IP地址上网配置方法”章节中“MSR830-WiNet系列路由器基本上网（静态IP）命令行配置（V7）”案例

3.2 设置A路由器

#配置GRE隧道，

```
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]interface Tunnel0 mode gre
[H3C-Tunnel0]ip address 10.1.2.1 24
[H3C-Tunnel0]source 1.1.1.1
[H3C-Tunnel0]destination 2.2.2.1
```

#配置一个访问控制列表3000，定义由子网1.1.1.0/24去子网

2.2.2.0/24的数据流，封装GRE数据流。

```
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000]rule permit ip source
1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
[H3C-acl-ipv4-adv-3000]quit
```

#配置公网口NAT要关联的ACl 3001，作用是把IPSec感兴趣流从NAT转换的数据流deny掉，防止IPSec数据流被NAT优先转换

```
[H3C]acl number 3001
[H3C-acl-adv-3001]rule 0 deny ip source 1.1.1.0
0.0.0.255 destination 2.2.2.0 0.0.0.255
[H3C-acl-adv-3001]rule 1 permit ip
[H3C-acl-adv-3001]quit
```

#创建一条IKE提议1，指定IKE提议使用的认证算法为MD5，加密算法为3des-cbc

```
[H3C]ike proposal 1
[H3C-ike-proposal-1]authentication-algorithm
md5
[H3C-ike-proposal-1]encryption-algorithm 3des-
cbc
[H3C-ike-proposal-1]quit
```

#创建并配置IKE keychain，名称为RTA。

```
[H3C]ike keychain RTA
```

#配置对端IP地址为2.2.2.1，使用的预共享密钥为明文123456

```
[H3C-ike-keychain-RTA]pre-shared-key address
2.2.2.1 255.255.255.0 key simple 123456
[H3C-ike-keychain-RTA]quit
```

#创建并配置IKE profile，名称为RTA，引用上面配置的keychain

RTA，配置本地地址为本端的公网接口地址1.1.1.1，对端地址为对端公网接口地址2.2.2.1，引用之前配置IKE提议1

```
[H3C]ike profile RTA
[H3C-ike-profile-RTA]keychain RTA
[H3C-ike-profile-RTA]local-identity address 1.1.1.1
[H3C-ike-profile-RTA]match remote identity address 2.2.2.1 255.255.255.0
[H3C-ike-profile-RTA]proposal 1
[H3C-ike-profile-RTA]quit
```

#配置IPsec安全提议1，ESP协议采用的加密算法为3des-cbc，认证算法为md5

```
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm md5
[H3C-ipsec-transform-set-1]quit
```

#创建IPsec安全策略，名称为RTA，序列号为1，设置对端地址为对端公网地址2.2.2.1，引用之前创建的ACL3000，引用之前创建的IKE profile RTA，引用之前的IPSec安全提议1

```
[H3C]ipsec policy RTA 1 isakmp
[H3C-ipsec-policy-isakmp-RTA-1]remote-address
```

```
2.2.2.1
[H3C-ipsec-policy-isakmp-RTA-1]security        acl
3000
[H3C-ipsec-policy-isakmp-RTA-1]transform-set
1
[H3C-ipsec-policy-isakmp-RTA-1]ike-profile RTA
[H3C-ipsec-policy-isakmp-RTA-1]quit
```

#设置外网口做NAT转换的时候关联ACL 3001 （如果之前已经在外网口配置了 nat outbound，需要先undo掉），并将IPSec安全策略RTA应用在外网接口

```
[H3C]interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0]undo nat outbound
[H3C-GigabitEthernet0/0]nat outbound 3001
[H3C-GigabitEthernet0/0]ipsec apply policy RTA
[H3C-GigabitEthernet0/0]quit
```

#配置到对端内网的路由

```
[H3C]ip route-static 172.16.1.0 24 Tunnel 0
```

#保存配置

```
[H3C]save force
```

3.3 设置B路由器

#配置GRE隧道，

```
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]interface Tunnel0 mode gre
[H3C-Tunnel0]ip address 10.1.2.2 24
[H3C-Tunnel0]source 2.2.2.1
[H3C-Tunnel0]destination 1.1.1.1
```

#配置一个访问控制列表3000，定义由子网1.1.1.0/24去子网2.2.2.0/24的数据流，封装GRE数据流。

```
[H3C]acl advanced 3000
[H3C-acl-ipv4-adv-3000]rule permit ip source 2.2.2.0 0.0.0.255 destination 1.1.1.0 0.0.0.255
[H3C-acl-ipv4-adv-3000]quit
```

#配置公网口NAT要关联的ACl 3001，作用是把IPSec感兴趣流从NAT转换的数据流deny掉，防止IPSec数据流被NAT优先转换

```
[H3C]acl number 3001
[H3C-acl-adv-3001]rule 0 deny ip source 2.2.2.0 0.0.0.255 destination 1.1.1.0 0.0.0.255
[H3C-acl-adv-3001]rule 1 permit ip
[H3C-acl-adv-3001]quit
```

#创建一条IKE提议1，指定IKE提议使用的认证算法为MD5，加密算法

为3des-cbc

```
[H3C]ike proposal 1
[H3C-ike-proposal-1]authentication-algorithm
md5
[H3C-ike-proposal-1]encryption-algorithm    3des-
cbc
[H3C-ike-proposal-1]quit
```

#创建并配置IKE keychain，名称为RTA。

```
[H3C]ike keychain RTA
```

#配置对端IP地址为1.1.1.1，使用的预共享密钥为明文123456

```
[H3C-ike-keychain-RTA]pre-shared-key      address
1.1.1.1 255.255.255.0 key simple 123456
[H3C-ike-keychain-RTA]quit
```

#创建并配置IKE profile，名称为RTA，引用上面配置的keychain RTA，配置本地地址为本端的公网接口地址2.2.2.1，对端地址为对端公网接口地址1.1.1.1，引用之前配置IKE提议1

```
[H3C]ike profile RTA
[H3C-ike-profile-RTA]keychain RTA
[H3C-ike-profile-RTA]local-identity       address
2.2.2.1
[H3C-ike-profile-RTA]match    remote    identity
address 1.1.1.1 255.255.255.0
[H3C-ike-profile-RTA]proposal 1
```

```
[H3C-ike-profile-RTA]quit
```

#配置IPsec安全提议1，ESP协议采用的加密算法为3des-cbc，认证算法为md5

```
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm md5
[H3C-ipsec-transform-set-1]quit
```

#创建IPsec安全策略，名称为RTA，序列号为1，设置对端地址为对端公网地址1.1.1.1，引用之前创建的ACL3000，引用之前创建的IKE profile RTA，引用之前的IPSec安全提议1

```
[H3C]ipsec policy RTA 1 isakmp
[H3C-ipsec-policy-isakmp-RTA-1]remote-address 1.1.1.1
[H3C-ipsec-policy-isakmp-RTA-1]security acl 3000
[H3C-ipsec-policy-isakmp-RTA-1]transform-set 1
[H3C-ipsec-policy-isakmp-RTA-1]ike-profile RTA
[H3C-ipsec-policy-isakmp-RTA-1]quit
```

#设置外网口做NAT转换的时候关联ACL 3001 （如果之前已经在外网口配置了 nat outbound，需要先undo掉），并将IPSec安全策略RTA

应用在外网接口

```
[H3C]interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0]undo nat outbound
[H3C-GigabitEthernet0/0]nat outbound 3001
[H3C-GigabitEthernet0/0]ipsec apply policy RTA
[H3C-GigabitEthernet0/0]quit
```

#配置到对端内网的路由

```
[H3C]ip route-static 192.168.1.0 24 Tunnel 0
```

#保存配置

```
[H3C]save force
```

3.4 验证配置结果

#在RTA路由器上带源ping RTB路由器内网网关地址