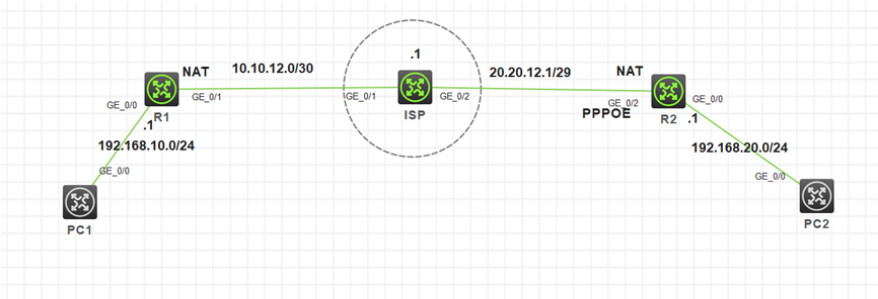
一端地址不固定如何实现GRE并使用IPSEC保护

GRE VPN IPSec VPN 吴秀涛 2022-10-11 发表

组网及说明



问题描述

需求：

R1有固定IP，R2是拨号上网，需要实现R1和R2建立OSPF实现内网的多网段互通且跑组播业务

配置思路：

使用IPSEC野蛮模式将R1和R2的环回口打通，通过环回口建立GRE隧道实现

过程分析

主要配置：

R1：

```
#
acl advanced name IPSEC12
 rule 2 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
#
acl advanced name NAT
 rule 2 deny ip source 1.1.1.1 0 destination 2.2.2.2 0
 rule 5 permit ip
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 10.10.12.2 255.255.255.252
 nat outbound name NAT
 ipsec apply policy 1
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ip route-static 0.0.0.0 0 GigabitEthernet0/1 10.10.12.1
#
ipsec transform-set 12
 esp encryption-algorithm 3des-cbc aes-cbc-128
 esp authentication-algorithm md5
#
ipsec policy-template 1 1
 transform-set 12
 security acl name IPSEC12
 local-address 10.10.12.2
 ike-profile 12
#
ipsec policy 1 1 isakmp template 1
#
 ike identity fqdn R1
#
ike profile 12
 keychain 12
 exchange-mode aggressive
 local-identity fqdn R1
 match remote identity fqdn R2
 match local address GigabitEthernet0/1
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike keychain 12
 match local address 10.10.12.2
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$15l1sJQZilIbSRI0rxoELx9QAjJiCw==
#
interface Tunnel1 mode gre
 ip address 192.168.12.1 255.255.255.0
 ospf 1 area 0.0.0.0
 source 1.1.1.1
 destination 2.2.2.2
#
```

R2：

#
acl advanced name IPSEC21
 rule 1 permit ip source 192.168.20.0 0.0.0.255 destination
192.168 .10.0 0.0.0.255
 rule 2 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
#
acl advanced name NAT
 rule 1 deny ip source 192.168.20.0 0.0.0.255 destination
192.168 .10.0 0.0.0.255
 rule 2 deny ip source 2.2.2.2 0 destination 1.1.1.1 0
 rule 5 permit ip
#
ipsec transform-set 21
 esp encryption-algorithm 3des-cbc aes-cbc-128
 esp authentication-algorithm md5
#
ipsec policy 2 1 isakmp
 transform-set 21
 security acl name IPSEC21
 remote-address 10.10.12.2
 ike-profile 21
#
 ike identity fqdn R2
#
ike profile 21
 keychain 21
 exchange-mode aggressive
 local-identity fqdn R2
 match remote identity address 10.10.12.2 255.255.255.252
 match local address Dialer1
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike keychain 21
 match local address 20.20.12.2
 pre-shared-key address 10.10.12.2 255.255.255.252 key cipher
c 3$B0MzOjTZ40lSqvNRs9ff7QW0s/UBCA=
=
#
interface Tunnel1 mode gre
 ip address 192.168.12.2 255.255.255.0
 ospf 1 area 0.0.0.0
 source 2.2.2.2
 destination 1.1.1.1
#

解决方法

1921正常的GRE over ipsec组网是两端有公网IP，GRE的底层地址使用两端公网的IP，IPSEC兴趣流是两端公网IP，数据转发流程：

组网：

PC1（192.168.1.1）——R1（11.11.11.11）——ISP——（22.22.22.22）R2——PC2（192.168.2.1）

PC1访问PC2的将数据包发给R1，R1查路由表发现目的IP（192.168.2.1）需要从GRE接口出去，数据到达GRE接口进行GRE封装，将数据包的源IP改成11.11.11.11，目的IP改成22.22.22.22，此时设备再查路由表发现想要去目的IP 22.22.22.22需要将数据包送到物理接口，物理接口调用了IPSEC查询是否匹配IPSEC兴趣流，如果匹配进行IPSEC封装，在GRE的基础上再封装一层IPSEC，源IP：11.11.11.1 1，目的IP：22.22.22.22。数据包到达R2后首先进行IPSEC解封装，再把GRE解封装把真实的私网IP数据包恢复发给PC2。

2、如果一端是拨号，一端固定IP去实现GRE Over IPSEC，因为GRE的配置无法配置域名相关所以无法用DDNS，考虑到GRE的源目IP可以是私网，例如常用环回口，那么首先使用IPSEC的野蛮模式打通环回口，然后GRE的源目IP使用环回口去建立。

组网：

PC1（192.168.1.1）——R1（11.11.11.11）——ISP——（pppoe）R2——PC2（192.168.2.1）

通过IPSEC野蛮模式将R1/2的环回口打通，即2.2.2.2和1.1.1.1可以互通，再设置R1 GRE源目分别是1.1.1.1、2.2.2.2，R2 GRE源目IP分别是2.2.2.2、1.1.1.1。PC1和PC2通信和普通的GRE Over IPSEC流程一样，先查路由表送到GRE口进行GRE封装，GRE封装完后源目IP变成环回口，查表去往目的IP需要送到物理接口再匹配IPSEC，所以公网也是ESP加密数据。

3、无论是哪一种，都和GRE的一个特性有关，无需destination IP可达逻辑接口才会UP，只要本端有去往des ip的路由（明细或者默认都可以）那么tunnel接口会UP，那么只需将私网互访的路由引到tunnel接口，那么私网互访的数据先发到tunnel口进行GRE封装再送到物理接口进行IPSEC封装再发往公网。