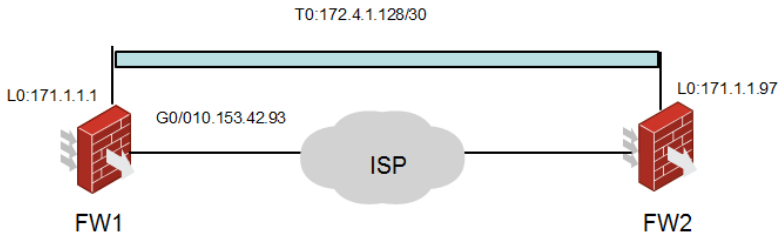
V7设备总部固定地址、分部动态获取地址GRE OVER IPsec典型配置案例

郑鑫 2015-10-23 发表

FW1和FWB先建立IPSec会话，在会话接口上建立GRE隧道，将g0/0所连网段的流量引入到GRE隧道上。通过GRE OVER IPsec，实现总部于分支流量既可以通信又能实现数据加密。



配置总部路由器

```
interface LoopBack0              //配置loopback地址，为gre的source地址
 ip address 171.1.1.1 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.153.42.93 255.255.255.0
 ipsec apply policy policy1                  //公网接口下启用ipsec策略
#

#
interface Tunnel93 mode gre                  //配置tunnel口，模式为gre
 ip address 174.1.2.129 255.255.255.252          //配置tunnel口的ip地址
 source 171.1.1.1                  //配置tunnel的源地址为本端的loopback地址
 destination 171.1.1.97            //配置tunnel的目的地址为对端的loopback地址
 keepalive 10 3                    //配置tunnel的keepalive
#
 ip route-static 0.0.0.0 0 10.153.42.1            //指向公网的默认路由
#

#
ipsec transform-set 1                  //配置ipsec  安全提议
 esp encryption-algorithm des-cbc     //配置ESP协议采用的认证算法des
 esp authentication-algorithm md5           //配置ESP协议采用的加密算法为md5
#
ipsec policy-template newvpn 1             //配置ipsec模版
 transform-set 1                   //关联ipsec安全提议
 local-address 10.153.42.93              //指定本端公网地址
 ike-profile newvpn                //关联ike  profile
#
ipsec policy policy1 102 isakmp template newvpn              //配置ipsec策略模版
#

 ike identity fqdn ct-center             //配置本端的fqdn
#

ike profile newvpn               //配置ike profile
 keychain 11              //关联ike  keychain
 exchange-mode aggressive          //配置为野蛮模式
 local-identity fqdn ct-center            //指定自己本端的fqdn
 match remote identity fqdn newvpn          //指定对端的fqdn
 match local address 10.153.42.93                //指定本端的公网地址
 proposal 1                        //关联ike  proposal
```

```
#
ike proposal 1              //配置ike  proposal
#
ike keychain 11               //配置ike预共享密钥
 pre-shared-key address 0.0.0.0 0.0.0.0 key simple  123
#
配置分部路由器

#
interface LoopBack0     //配置loopback地址，为gre的source地址
 ip address 171.1.1.97 255.255.255.255

#
interface GigabitEthernet2/0/0
 port link-mode route
 combo enable copper
 ip address  dhcp-alloc          //配置接口为自动获取地址
 ipsec apply policy policy1               //公网接口下启用ipsec策略
#
interface Tunnel1 mode gre        //配置tunnel口，模式为gre
 ip address 174.1.2.130 255.255.255.252          //配置tunnel口的ip地址
 source 171.1.1.97          //配置tunnel的源地址为本端的loopback地址
 destination 171.1.1.1           //配置tunnel的目的地址为对端的loopback地址
 keepalive 10 3                  //配置tunnel的keepalive
#
 ip route-static 0.0.0.0 0 10.153.42.1             //指向公网的默认路由
#
acl number 3000             //配置ipsec的安全acl，源目的地址分别为本端和对端的loopback地址
 rule 0 permit ip source 171.1.1.97 0 destination 171.1.1.1 0
#

ipsec transform-set 1               //配置ipsec  安全提议
 esp encryption-algorithm des-cbc            //配置ESP协议采用的认证算法des
 esp authentication-algorithm md5              //配置ESP协议采用的加密算法为md5
#
ipsec policy policy1 1 isakmp          //配置ipsec策略
 transform-set 1                        //关联ipsec安全提议
 security acl 3000                       //关联安全策略
 remote-address 10.153.42.93           //指定对端公网地址
 ike-profile ct-center                        //关联ike  profile
#
 ike identity fqdn newvpn                   //配置本端的fqdn
#
ike profile ct-center                       //配置ike profile
 keychain 1                                  //关联ike  keychain
 exchange-mode aggressive                      //配置为野蛮模式
 local-identity fqdn newvpn                    //指定自己本端的fqdn
 match remote identity address 10.153.42.93 255.255.255.255        //指定对端的公网地址
 match remote identity fqdn ct-center                //指定对端的fqdn
 proposal 1                //关联ike  proposal
#
ike proposal 1                //创建ike  proposal
#
ike keychain 1                //创建ikekeychain
 pre-shared-key address 10.153.42.93 255.255.255.255 key simple  123            //配置预共享密钥
#
验证tunnel口可以互通
分支ping总部的tunnel口地址可以正常ping通
<FW2> ping 174.1.2.129
Ping 174.1.2.129 (174.1.2.129): 56 data bytes, press CTRL_C to break
56 bytes from 174.1.2.129: icmp_seq=0 ttl=255 time=0.518 ms
56 bytes from 174.1.2.129: icmp_seq=1 ttl=255 time=0.374 ms
56 bytes from 174.1.2.129: icmp_seq=2 ttl=255 time=0.332 ms
56 bytes from 174.1.2.129: icmp_seq=3 ttl=255 time=0.331 ms
```

56 bytes from 174.1.2.129: icmp_seq=4 ttl=255 time=0.327 ms
分支查看ike sa和ipsec sa
通过dis ike sa可以看到分支与总部正常建立的ike
<FW2> dis ike sa
Connection-ID Remote Flag DOI
---
50 10.153.42.93 RD IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING

通过dis ipsec sa查看分支与总部已经正常建议ipsec sa
<FW2>dis ipsec sa

Interface: GigabitEthernet2/0/0

IPsec policy: policy1
Sequence number: 1
Mode: isakmp

Tunnel id: 0
Encapsulation mode: tunnel
Perfect forward secrecy:
Path MTU: 1443
Tunnel:
local address: 10.153.42.36
remote address: 10.153.42.93
Flow:
sour addr: 171.1.1.97/255.255.255.255 port: 0 protocol: ip
dest addr: 171.1.1.1/255.255.255.255 port: 0 protocol: ip

[Inbound ESP SAs]
SPI: 4270357317 (0xfe887b45)
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843197/3361
Max received sequence-number: 51
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: active

[Outbound ESP SAs]
SPI: 1957355160 (0x74aade98)
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843197/3361
Max sent sequence-number: 52
UDP encapsulation used for NAT traversal: N
Status: active
总部查看ike sa和ipsec sa
通过dis ike sa可以看到总部与分支正常建立的ike
<FW1>dis ike sa
Connection-ID Remote Flag DOI
---
5 10.153.42.36 RD IPsec
Flags:
RD--READY RL--REPLACED FD-FADING

通过dis ipsec sa查看总部与分支已经正常建议ipsec sa
<FW1>dis ipsec sa

Interface: GigabitEthernet0/0

```
-------------------------------

  -----------------------------
  IPsec policy: policy1
  Sequence number: 102
  Mode: Template
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Inside VPN:
    Path MTU: 1443
    Tunnel:
        local  address: 10.153.42.93
        remote address: 10.153.42.36
    Flow:
        sour addr: 171.1.1.1/255.255.255.255  port: 0  protocol: ip
        dest addr: 171.1.1.97/255.255.255.255  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 1957355160 (0x74aade98)
      Connection ID: 21474836482
      Transform set:  ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843198/3469
      Max received sequence-number: 31
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 4270357317 (0xfe887b45)
      Connection ID: 21474836483
      Transform set:  ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843198/3469
      Max sent sequence-number: 30
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

1、使用防火墙配置的时候，需要注意放通相应的域间策略，诸如 IPsec和L2TP等VPN业务都涉及到上送防火墙本地进行加解封装的操作，故一定要配置VPN流量所在域到Local域和相应反向的域间策略，确保VPN流量不被默认域间策略所拒绝。

2、两端的业务需要互通，需要使用静态路由或者是动态路由协议。且注意tunnel口中的source和destination地址如果与雨雾网段在同一个网段，则需要指两端互指32位明细路由到公网接口，或者是通过路由过滤，禁止两端通过tunnel学习到对端的loopback的路由，否则会引起tunnel不断up/down。

3、野蛮模式建立ipsec建议使用模版方式，否则会导致ipsec建立不成功。