SecPath防火墙使用环回口建立GRE over IPSec的典型配置

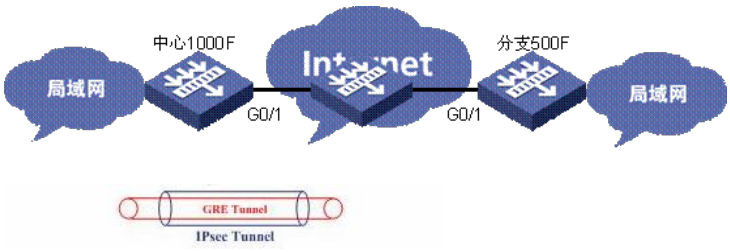
万欣 2009-05-15 发表

SecPath防火墙使用环回口GRE over IPSec的典型配置

一、 组网需求：

中心设备和分支设备之间通过GRE over IPSec（野蛮模式）建立VPN隧道，但由于分支出口地址经常变化，因此采用环回口地址来建立GRE隧道。从而保证两局域网之间能够互访。

二、 组网图



三、 配置步骤

1．中心：SecPath1000F的主要配置：

```
#
 sysname zhongxin
#
 ike local-name zhongxin   //配置IPSec的野蛮模式
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
ike dpd 1
#
ike peer test
 exchange-mode aggressive
 pre-shared-key h3c
 id-type name
 remote-name fenzhi
 local-address 202.103.1.1
 nat traversal
 dpd 1
#
ipsec proposal 1
#
ipsec policy-template 1 10
 ike-peer test
 proposal 1
#
ipsec policy test 1 isakmp template 1    //中心设备采用模板方式
#
interface GigabitEthernet0/0
 loopback
 ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 ip address 202.103.1.1 255.255.255.0
 ipsec policy test
#
interface Tunnel0            //创建Tunnel接口，采用环回口封装
 ip address 1.1.1.1 255.255.255.0
 source 7.7.7.7
 destination 6.6.6.6
#
```

```
interface LoopBack100
 ip address 7.7.7.7 255.255.255.0
#
 firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet0/1
 add interface Tunnel0
 set priority 85
#
ospf 1                    //路由配置
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 202.103.1.2 preference 60
```

2．分支：SecPath500F的主要配置：

```
#
sysname fenzhi
#
ike local-name zhongxin      //配置IPSec的野蛮模式
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
acl number 3000          //配置感兴趣的流量
 rule 0 permit ip source 6.6.6.0 0.0.0.255 destination 7.7.7.0 0.0.0.255
#
 ike dpd 1
#
ike peer test
 exchange-mode aggressive
 pre-shared-key simple h3c
 id-type name
 remote-name zhongxin
 remote-address 202.103.1.1
 nat traversal
 dpd 1
#
ipsec proposal 1
#
ipsec policy 1 10 isakmp
 security acl 3000
 ike-peer test
 proposal 1
#
interface LoopBack100
 ip address 6.6.6.6 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 loopback
 ip address 200.1.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 202.103.2.1 255.255.255.0
 ipsec policy 1
#
interface Tunnel0        //创建Tunnel接口，采用环回口封装
 ip address 1.1.1.2 255.255.255.0
 source 6.6.6.6
 destination 7.7.7.7
```

```
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet0/1
 add interface Tunnel0
 set priority 85
#
ospf 1                  //路由配置
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 200.1.1.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 202.103.2.2
#
```

3．验证结果：

1.网络连通性：

```
  [fenzhi]ping -a 1.1.1.2 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms

   [fenzhi]ping -a 200.1.1.1 100.1.1.1
  PING 100.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 100.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 100.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
```

2．VPN的建立：

```
  [fenzhi]dis ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  --------------------------------------------------------------
       102         202.103.1.1     RD|ST        1     IPSEC
       103         202.103.1.1     RD|ST        2     IPSEC

[fenzhi]dis ipsec sa
================================
Interface: GigabitEthernet0/1
    path MTU: 1500
================================

  ------------------------------
  IPsec policy name: "1"
  sequence number: 10
  mode: isakmp
  ------------------------------
    connection id: 17
    encapsulation mode: tunnel
    perfect forward secrecy: None
    tunnel:
        local  address: 202.103.2.1
        remote address: 202.103.1.1
    Flow :
        sour addr: 6.6.6.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 7.7.7.0/255.255.255.0  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 2436129503 (0x913462df)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887427352/3169
      max received sequence-number: 91
      anti-replay check enable: Y
      anti-replay window size: 32
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
```

spi: 4167546169 (0xf867b539)
proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
sa remaining key duration (bytes/sec): 1887427152/3169
max sent sequence-number: 94
udp encapsulation used for nat traversal: N

四、 配置关键点

请参看注释。