大量分支GRE over IPSec接入的简易配置

温超军 2012-08-21 发表

大量分支GRE over IPSec接入的简易配置

一、 组网需求

客户的网络拓扑比较大，一个中心网点和N个分支网点，且每个分支网点都需要利用GRE OVER IPSec与中心网点建立VPN连接。

由于GRE隧道有一定的局限性，Tunnel接口过多，造成配置的复杂，而Tunnel接口的最大数目为4096个，那么，分支数目超过此数就无法继续建立GRE隧道，且还没有算上有些是备份的链路。采用P2MP将大大简化Tunnel接口的配置，且也解决了Tunnel接口数目不足带来的问题。

同样，设备的公网出接口数目是有限的，我们不可能在N个出接口上建立IPSec隧道。采用IPsec的模板配置，解决相应配置的问题。

二、 组网拓扑图

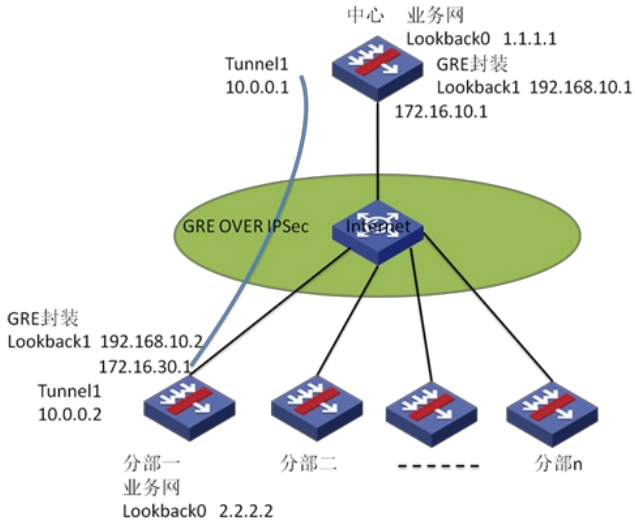
实验所用设备：

中心设备为SecBlade防火墙插卡；软件版本Feature 3171P11；公网出接口G0/3：172.16.10.1。

分部一设备为SecBlade防火墙插卡；软件版本Feature 3171P11；公网出接口G0/3：172.16.30.1。

分部二设备为SecPath V3防火墙；软件版本Release 1662P07；公网出接口G0/1：172.16.20.1。

因特网设备为S7503E-S交换机；软件版本Release 6616P01；实验中所用接口为G0/0/25：172.16.10.2，G0/0/27：172.16.30.2，G0/0/28:192.168.20.1。



三、 配置步骤

1) 基本配置

各个设备的接口和区域的配置。分部的IP地址本应该为动态获取，这里为了简化配置，直接改为静态了。

路由配置：

中心：ip route-static 0.0.0.0 0.0.0.0 172.16.10.2

//公网路由

ip route-static 2.2.2.2 255.255.255.255 10.0.0.2

//将业务数据流引向Tunnel接口，从而触发GRE封装

分部一：ip route-static 0.0.0.0 0.0.0.0 172.16.30.2

//公网路由

ip route-static 1.1.1.1 255.255.255.255 10.0.0.1

//将业务数据流引向Tunnel接口，从而触发GRE封装

分部二：ip route-static 0.0.0.0 0.0.0.0 172.16.20.2 preference 60

ip route-static 1.1.1.1 255.255.255.255 10.0.0.1 preference 60

2) GRE配置

中心设备：

interface Tunnel1

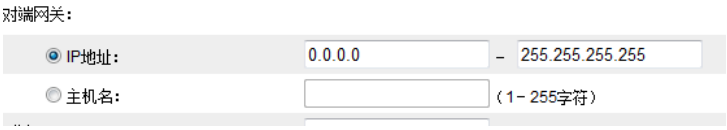
ip address 10.0.0.1 255.255.255.0

tunnel-protocol gre p2mp //这里默认采用GRE，改为P2MP

source 192.168.10.1　　//源封装地址为回环接口Lookback1的地址
gre p2mp branch-network-mask 255.255.255.0
　　//采用P2MP的封装模式，无表示对端的封装地址为多少，只能设置一个掩码表示范围
分部一设备：
interface Tunnel1
ip address 10.0.0.2 255.255.255.0
source 192.168.10.2
destination 192.168.10.1
//分部设备对中心设备来与是点到点的类型，直接封装相应的源地址和目标地址就行了
分部二：
interface Tunnel1
ip address 10.0.0.3 255.255.255.0
source 192.168.10.3
destination 192.168.10.1

3) IPSec配置
在本实验中，分部的IP都不是固定的，都为动态获取所得，所以，IKE的协商方式这里采用野蛮模式
中心设备：
ike local-name fw1　//IKE本端名字（千万不能忘记）

ike peer 10
exchange-mode aggressive
pre-shared-key cipher c3$/3EvhWhcCcw0SYCWzLohIg2r1bGeCVY=
id-type name
remote-name fw2
remote-address fw2 dynamic
//此处可以不做配置，如果不做配置默认为所有IP地址，如图所示：



ipsec proposal 10
//安全提议采用默认的配置即可，也可以自行更改，默认为：

IKE安全提议号	认证方法	认证算法	加密算法	DH组	SA生存周期（秒）
10	Preshared Key	SHA1	DES-CBC	Group1	86400
default	Preshared Key	SHA1	DES-CBC	Group1	86400

ipsec policy-template zb1 10
ike-peer 10
proposal 10
//总部的类型为点到多点，所以这里采用模板的方法，这样无法配置ACL进行数据流匹配
ipsec policy cnc 10 isakmp template zb1
//模板的应用方式
interface GigabitEthernet0/3
port link-mode route
ip address 172.16.10.1 255.255.255.0
ipsec policy cnc

分部一：
acl number 3000
rule 0 permit ip source 192.168.10.2 0 destination 192.168.10.1 0
ike local-name fw2 //配置本端名字
ike peer 10
exchange-mode aggressive
pre-shared-key cipher c3$UaPgUwWG/SiXbHB6XVbtbAVmEBQk1AE=
id-type name
remote-name fw1
remote-address 172.16.10.1
#
ipsec proposal 10//采用默认，这里也可以不做配置
#
ipsec policy fb 10 isakmp
security acl 3000

```
 ike-peer 10
 proposal 10
//分部为点到点模式，不用配置模板，此里的acl可以用于中心设备的反向匹配
```

分部二：

```
ike peer 10
 exchange-mode aggressive
 pre-shared-key cipher KqbfKcrPdHA=
 id-type name
 remote-name fw1
 remote-address 172.16.10.1
#
ipsec proposal 10
#
ipsec policy fb 10 isakmp
 security acl 3000
 ike-peer 10
 proposal 10
#
acl number 3000
 rule 0 permit ip source 192.168.10.3 0 destination 192.168.10.1 0
```

4) 连通性测试

只能由分部触发建立，中心侧无法触发。

分部一：

```
[H3C]ping -a 2.2.2.2 1.1.1.1
  PING 1.1.1.1: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 1.1.1.1 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[H3C]
```

分部二：

```
<Quidway>ping -a 3.3.3.3 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=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 1.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
<Quidway>
```

中心设备情况：

```
<H3C>display ike sa
    total phase-1 SAs:  2
    connection-id  peer           flag       phase   doi      status
  -----------------------------------------------------------------------
      1            172.16.30.1     RD         1     IPSEC    --
      3            172.16.20.1     RD         1     IPSEC    --
      2            172.16.30.1     RD         2     IPSEC    --
      4            172.16.20.1     RD         2     IPSEC    --
```

```
  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
<H3C>
分部一与分部二都已经成功建立隧道
查看IPSec SA隧道
<H3C>display ipsec sa
===============================
Interface: GigabitEthernet0/3
    path MTU: 1500
===============================

  ----------------------------
  IPsec policy name: "zb"
  sequence number: 10
  mode: template
  ----------------------------
    connection id: 1
    encapsulation mode: tunnel
    perfect forward secrecy:
    tunnel:
        local  address: 172.16.10.1
        remote address: 172.16.30.1  //这个是分部一
    flow:
        sour addr: 192.168.10.1/255.255.255.255  port: 0  protocol: IP
dest addr: 192.168.10.2/255.255.255.255  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 3758878501 (0xe00bef25)
//这个与分部一的出方向的SA相同
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843196/1246
      max received sequence-number: 34
      anti-replay check enable: Y
      anti-replay window size: 32
      udp encapsulation used for nat traversal: N
      status: --

    [outbound ESP SAs]
      spi: 2870550202 (0xab191eba)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843196/1246
      max received sequence-number: 35
      udp encapsulation used for nat traversal: N
      status: --

  ----------------------------
  IPsec policy name: "zb"
  sequence number: 10
  mode: template
  ----------------------------
    connection id: 2
    encapsulation mode: tunnel
    perfect forward secrecy:
    tunnel:
        local  address: 172.16.10.1
        remote address: 172.16.20.1  //这个是分部二
    flow:
        sour addr: 192.168.10.1/255.255.255.255  port: 0  protocol: IP
dest addr: 192.168.10.3/255.255.255.255  port: 0  protocol: IP

    [inbound ESP SAs]
```

```
    spi: 3651661767 (0xd9a7efc7)
    proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1843197/1559
    max received sequence-number: 19
    anti-replay check enable: Y
    anti-replay window size: 32
    udp encapsulation used for nat traversal: N
    status: --

  [outbound ESP SAs]
    spi: 460917123 (0x1b790983)
    proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1843197/1559
    max received sequence-number: 20
    udp encapsulation used for nat traversal: N
    status: --
<H3C>
```

分部一的IPSec SA

```
<H3C>display ipsec sa
==============================
Interface: GigabitEthernet0/3
  path MTU: 1500
==============================

 ----------------------------
 IPsec policy name: "fb"
 sequence number: 10
 mode: isakmp
 ----------------------------
   connection id: 1
   encapsulation mode: tunnel
   perfect forward secrecy:
   tunnel:
      local  address: 172.16.30.1
      remote address: 172.16.10.1 //与总部方向建立SA
   flow:
      sour addr: 192.168.10.2/255.255.255.255  port: 0  protocol: IP
      dest addr: 192.168.10.1/255.255.255.255  port: 0  protocol: IP

   [inbound ESP SAs]
    spi: 2870550202 (0xab191eba)
//对比总部的第一个出方向的SA，这两个值相同
    proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1843196/738
    max received sequence-number: 34
    anti-replay check enable: Y
    anti-replay window size: 32
    udp encapsulation used for nat traversal: N
    status: --

   [outbound ESP SAs]
    spi: 3758878501 (0xe00bef25)
    proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1843196/738
    max received sequence-number: 35
    udp encapsulation used for nat traversal: N
    status: --
<H3C>
```

分部二IPSec SA

```
<Quidway>display ipsec sa
================================
Interface: GigabitEthernet0/1
    path MTU: 1500
================================

  ----------------------------
  IPsec policy name: "fb"
  sequence number: 10
  mode: isakmp
  ----------------------------
    Created by: "Host"
    connection id: 4
    encapsulation mode: tunnel
    perfect forward secrecy: None
    tunnel:
        local  address: 172.16.20.1
        remote address: 172.16.10.1 //与总部方向建立SA
    flow:    (38 times matched)
        sour addr: 192.168.10.3/255.255.255.255  port: 0  protocol: IP
        dest addr: 192.168.10.1/255.255.255.255  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 460917123 (0x1b790983)
        //与总部第二个出方向的SA值相同
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa key duration (bytes/sec): 1887436800/3600
      sa remaining key duration (bytes/sec): 1887434748/938
      max received sequence-number: 19
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 3651661767 (0xd9a7efc7)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa key duration (bytes/sec): 1887436800/3600
      sa remaining key duration (bytes/sec): 1887434748/938
      max sent sequence-number: 20
      udp encapsulation used for nat traversal: N
<Quidway>
```

使用模板的IPSec配置，原理与直接使用策略的配置相同，相比之下，使用模板的配置主要是为总部设备简化了配置，并且大大的减少了所需要的公网出接口，但是采用模板的配置也有一个缺点，就是数据的通道只能由分部进行触发了。

中心设备：

在web界面上查看GRE的隧道情况

GRE隧道情况：

GRE隧道的老化时间为默认为5秒，这里我改为20秒，方便查看。

默认的Tunnel接口封装为GRE的点对点模式，这样，如果要建立N个隧道，那么将需要N个Tunnel接口，配置也将复杂化，采用P2MP的模式，需要的Tunnel接口减少到了一个配置量也大大的减少了，和IPSec的模板形式一样，采用P2MP的模式，总部设备将无法触发隧道的建立，采用P2MP，相应的数据封装和GRE一样。

分部设备：

略！

四、 配置关键点

1、 中心设备采用P2MP的方式建立GRE隧道，分部设备也采用P2MP方式，将无法建立GRE隧道，所以分部必须采用点到点的方式。

2、 中心设备的IPSec由于要与N个分部建立隧道连接，所以采用模板的配置，如果分部也采用模板，那么将无法建立IPSec连接，所以分部一定要配置策略。