AR系列路由器GRE Over IPSec的典型配置

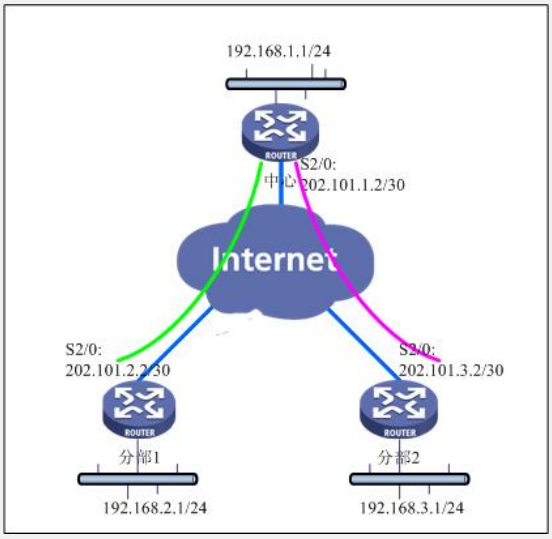
姚忆斌 2006-09-30 发表

AR系列路由器GRE Over IPSec的典型配置

【需求】

分部1和分部2通过野蛮IPSec的方式连接到中心，采用GRE-Over-IPSec的方式，在tunnel上运行OSPF协议来实现总部和分部之间的互通。

【组网图】



【配置脚本】

中心配置脚本

```
#
sysname Center
#
ike local-name center              /中心ike的local-name为：center/
#
router id 1.1.1.1
#
radius scheme system
#
domain system
#
ike peer branch1                   /配置到分部1的ike peer/
exchange-mode aggressive           /设置IPSec为野蛮方式/
pre-shared-key abc                 /预共享密钥为abc/
id-type name                       /选择名字作为ike协商过程中使用的ID/
remote-name branch1                /分部1的名字为branch1/
#
ike peer branch2                   /配置到分部2的ike peer/
exchange-mode aggressive
pre-shared-key abc
id-type name
remote-name branch2
#
ipsec proposal 1                   /定义ipsec proposal/
#
ipsec policy center 10 isakmp      /配置到分部1的ipsec policy/
security acl 3001                  /指定安全策略所引用的访问控制列表号/
ike-peer branch1                   /引用ike peer/
proposal 1                         /引用ipsec proposal/
#
ipsec policy center 20 isakmp      /到分部2的配置和分部1的配置类似/
security acl 3002
ike-peer branch2
proposal 1
#
acl number 3001                    /定义从中心到分部1的GRE数据流/
rule 0 permit gre source 202.101.1.2 0 destination 202.101.2.2 0
acl number 3002                    /定义从中心到分部2的GRE数据流/
rule 0 permit gre source 202.101.1.2 0 destination 202.101.3.2 0
#
interface Serial2/0
link-protocol ppp
ip address 202.101.1.2 255.255.255.252
ipsec policy center                /在公网出口上应用IPSec policy/
#
interface Tunnel0                  /配置中心和分部1之间的GRE tunnel/
ip address 10.0.0.1 255.255.255.252
source 202.101.1.2
destination 202.101.2.2
#
interface Tunnel1                  /配置中心和分部2之间的GRE tunnel/
ip address 10.0.0.5 255.255.255.252
source 202.101.1.2
destination 202.101.3.2
#
interface NULL0
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
#
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0  /中心的内网地址/
#
ospf 1
area 0.0.0.10                      /分部1属于area 10/
network 10.0.0.0 0.0.0.3
#
area 0.0.0.20                      /分部2属于area 20/
network 10.0.0.4 0.0.0.3
#
area 0.0.0.0                       /总部属于area 0/
network 1.1.1.1 0.0.0.0
network 192.168.1.0 0.0.0.255
#
ip route-static 0.0.0.0 0.0.0.0 202.101.1.1 preference 60
#
user-interface con 0
user-interface vty 0 4
#
return
```

分部1配置脚本

```
#
sysname Branch1
#
ike local-name branch1              /分部1的ike的local-name为：branch1/
#
radius scheme system
#
domain system
#
ike peer center                     /配置到中心的ike peer/
exchange-mode aggressive            /设置IPSec为野蛮方式/
pre-shared-key abc                  /预共享密钥为abc/
id-type name                        /选择名字作为ike协商过程中使用的ID/
remote-name center                  /对端的名字为center/
remote-address 202.101.1.2          /对端的地址为202.101.1.2（中心的公网地址）/
#
ipsec proposal 1                    /定义ipsec proposal/
#
ipsec policy branch1 10 isakmp      /配置到中心的ipsec policy/
security acl 3001                   /指定安全策略所引用的访问控制列表号/
ike-peer center                     /引用ike peer/
proposal 1                          /引用ipsec proposal/
#
acl number 3001                     /定义从分部1到中心的GRE数据流/
rule 0 permit gre source 202.101.2.2 0 destination 202.101.1.2 0
#
interface Serial2/0
link-protocol ppp
ip address 202.101.2.2 255.255.255.252
ipsec policy branch1                /在公网出口上应用IPSec policy/
#
interface Tunnel0                   /配置分部1和中心之间的GRE tunnel/
ip address 10.0.0.2 255.255.255.252
source 202.101.2.2
destination 202.101.1.2
#
interface NULL0
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
interface Ethernet0/0               /配置分部1的内网地址/
ip address 192.168.2.1 255.255.255.0
#
ospf 1
area 0.0.0.10                       /分部1属于area 10/
network 2.2.2.2 0.0.0.0
network 10.0.0.0 0.0.0.3
network 192.168.2.0 0.0.0.255
#
ip route-static 0.0.0.0 0.0.0.0 202.101.2.1 preference 60
#
user-interface con 0
user-interface vty 0 4
#
return
```

分部2配置脚本

```
#
sysname Branch2
#
ike local-name branch1          /分部2的ike的local-name为：branch2/
#
radius scheme system
#
domain system
#
ike peer center                 /配置到中心的ike peer/
exchange-mode aggressive        /设置IPSec为野蛮方式/
pre-shared-key abc              /预共享密钥为abc/
id-type name                    /选择名字作为ike协商过程中使用的ID/
remote-name center              /对端的名字为center/
remote-address 202.101.1.2    /对端的地址为202.101.1.2(中心的公网地址)/
#
ipsec proposal 1                /定义ipsec proposal/
#
ipsec policy branch1 10 isakmp /配置到中心的ipsec policy/
security acl 3001               /指定安全策略所引用的访问控制列表号/
ike-peer center                 /引用ike peer/
proposal 1                      /引用ipsec proposal/
#
acl number 3001                 /定义从分部2到中心的GRE数据流/
rule 0 permit gre source 202.101.3.2 0 destination 202.101.1.2 0
#
interface Serial2/0
link-protocol ppp
ip address 202.101.3.2 255.255.255.252
ipsec policy branch2            /在公网出口上应用IPSec policy/
#
interface Tunnel0               /配置分部1和中心之间的GRE tunnel/
ip address 10.0.0.6 255.255.255.252
source 202.101.3.2
destination 202.101.1.2
#
interface NULL0
#
interface LoopBack0
ip address 3.3.3.3 255.255.255.255
#
interface Ethernet0/0           /配置分部1的内网地址/
ip address 192.168.3.1 255.255.255.0
#
ospf 1
area 0.0.0.20                   /分部2属于area 20/
network 3.3.3.3 0.0.0.0
network 10.0.0.4 0.0.0.3
network 192.168.3.0 0.0.0.255
#
ip route-static 0.0.0.0 0.0.0.0 202.101.3.1 preference 60
#
user-interface con 0
user-interface vty 0 4
#
return
```

【验证】

1、中心上的ike sa 状态：

```
disp ike sa
   connection-id  peer            flag       phase   doi
 ------------------------------------------------------------------
       4        202.101.3.2     RD          1     IPSEC
       5        202.101.3.2     RD          2     IPSEC
       2        202.101.2.2     RD          1     IPSEC
       3        202.101.2.2     RD          2     IPSEC

 flag meaning
 RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO—TIMEOUT
```

2、中心上的IPSec sa状态：

```
disp ipsec sa
================================
Interface: Serial2/0/0
   path MTU: 1500
================================

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

```
  IPsec policy name: "center"
  sequence number: 10
  mode: isakmp
  ----------------------------
    connection id: 3
    encapsulation mode: tunnel
    perfect forward secrecy: None
    tunnel:
        local  address: 202.101.1.2
        remote address: 202.101.2.2
    flow:    (72 times matched)
        sour addr: 202.101.1.2/255.255.255.255  port: 0  protocol: GRE
        dest addr: 202.101.2.2/255.255.255.255  port: 0  protocol: GRE

    [inbound ESP SAs]
      spi: 1168206412 (0x45a16a4c)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887434028/3365
      max received sequence-number: 33
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 2150942891 (0x8034c8ab)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887433260/3365
      max sent sequence-number: 36
      udp encapsulation used for nat traversal: N

  ----------------------------
  IPsec policy name: "center"
  sequence number: 20
  mode: isakmp
  ----------------------------
    connection id: 4
    encapsulation mode: tunnel
    perfect forward secrecy: None
    tunnel:
        local  address: 202.101.1.2
        remote address: 202.101.3.2
    flow:    (73 times matched)
        sour addr: 202.101.1.2/255.255.255.255  port: 0  protocol: GRE
        dest addr: 202.101.3.2/255.255.255.255  port: 0  protocol: GRE

    [inbound ESP SAs]
      spi: 2624895419 (0x9c74b9bb)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887433796/3385
      max received sequence-number: 35
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 1281853764 (0x4c678944)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887432856/3385
      max sent sequence-number: 39
      udp encapsulation used for nat traversal: N

3、中心路由表
disp ip rout
 Routing Table: public net
Destination/Mask   Protocol Pre  Cost        Nexthop         Interface
0.0.0.0/0          STATIC   60   0           202.101.1.1     Serial2/0/0
1.1.1.1/32         DIRECT   0    0           127.0.0.1       InLoopBack0
2.2.2.2/32         OSPF     10   1563        10.0.0.2        Tunnel0
```

```
3.3.3.3/32        OSPF     10   1563        10.0.0.6        Tunnel1
10.0.0.0/30       DIRECT   0    0           10.0.0.1        Tunnel0
10.0.0.1/32       DIRECT   0    0           127.0.0.1       InLoopBack0
10.0.0.4/30       DIRECT   0    0           10.0.0.5        Tunnel1
10.0.0.5/32       DIRECT   0    0           127.0.0.1       InLoopBack0
127.0.0.0/8       DIRECT   0    0           127.0.0.1       InLoopBack0
127.0.0.1/32      DIRECT   0    0           127.0.0.1       InLoopBack0
192.168.1.0/24    DIRECT   0    0           192.168.1.1     LoopBack10
192.168.1.1/32    DIRECT   0    0           127.0.0.1       InLoopBack0
192.168.2.0/24    OSPF     10   1563        10.0.0.2        Tunnel0
192.168.3.0/24    OSPF     10   1563        10.0.0.6        Tunnel1
202.101.1.0/30    DIRECT   0    0           202.101.1.2     Serial2/0/0
202.101.1.1/32    DIRECT   0    0           202.101.1.1     Serial2/0/0
202.101.1.2/32    DIRECT   0    0           127.0.0.1       InLoopBack0
```

4、分部1的ike sa状态：

```
disp ike sa
   connection-id  peer            flag       phase   doi
  --------------------------------------------------------------
       2         202.101.1.2     RD|ST        1     IPSEC
       3         202.101.1.2     RD|ST        2     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO—TIMEOUT
```

5、分部1的ipsec sa状态：

```
disp ipsec sa
================================
Interface: Serial2/0/0
   path MTU: 1500
================================

  ------------------------------
  IPsec policy name: "branch1"
  sequence number: 10
  mode: isakmp
  ------------------------------
    connection id: 3
    encapsulation mode: tunnel
    perfect forward secrecy: None
    tunnel:
       local  address: 202.101.2.2
       remote address: 202.101.1.2
    flow:    (82 times matched)
       sour addr: 202.101.2.2/255.255.255.255  port: 0  protocol: GRE
       dest addr: 202.101.1.2/255.255.255.255  port: 0  protocol: GRE

    [inbound ESP SAs]
      spi: 2150942891 (0x8034c8ab)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887433256/3293
      max received sequence-number: 42
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 1168206412 (0x45a16a4c)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887432880/3293
      max sent sequence-number: 41
      udp encapsulation used for nat traversal: N
```

6、分部1的路由表：

```
disp ip rout
 Routing Table: public net
```

```
Destination/Mask    Protocol Pre  Cost        Nexthop         Interface
0.0.0.0/0           STATIC   60   0           202.101.2.1     Serial2/0/0
1.1.1.1/32          OSPF     10   1563        10.0.0.1        Tunnel0
2.2.2.2/32          DIRECT   0    0           127.0.0.1       InLoopBack0
3.3.3.3/32          OSPF     10   3125        10.0.0.1        Tunnel0
10.0.0.0/30         DIRECT   0    0           10.0.0.2        Tunnel0
10.0.0.2/32         DIRECT   0    0           127.0.0.1       InLoopBack0
10.0.0.4/30         OSPF     10   3124        10.0.0.1        Tunnel0
127.0.0.0/8         DIRECT   0    0           127.0.0.1       InLoopBack0
127.0.0.1/32        DIRECT   0    0           127.0.0.1       InLoopBack0
192.168.1.0/24      OSPF     10   1563        10.0.0.1        Tunnel0
192.168.2.0/24      DIRECT   0    0           192.168.2.1     LoopBack10
192.168.2.1/32      DIRECT   0    0           127.0.0.1       InLoopBack0
192.168.3.0/24      OSPF     10   3125        10.0.0.1        Tunnel0
202.101.2.0/30      DIRECT   0    0           202.101.2.2     Serial2/0/0
202.101.2.1/32      DIRECT   0    0           202.101.2.1     Serial2/0/0
202.101.2.2/32      DIRECT   0    0           127.0.0.1       InLoopBack0
```

【提示】

1、IPSec -Over-GRE和GRE-Over-IPSec方式配置上的区别为：

	GRE-Over-IPSec	**IPSec-Over-GRE**
ACL定义	GRE数据流	内网数据流
Ike peer中指定的remote-address	对方公网地址	对方GRE tunnel地址
应用端口	公网出口	GRE tunnel上

2、各个分部和总部之间通过OSPF路由来实现互访，如果没有运行OSPF则必需在分部和总部配置静态路由。

【Center配置】

```
ip route-static 192.168.2.0 255.255.255.0 Tunnel 0 preference 60
/访问分部1内网的数据从tunnel 0走/
 ip route-static 192.168.3.0 255.255.255.0 Tunnel 1 preference 60
 /访问分部2内网的数据从tunnel 1走/
```

【分部1配置】

```
 ip route-static 192.168.1.0 255.255.255.0 Tunnel 0 preference 60
/访问中心内网的数据从tunnel 0走/
```

【分部2配置】

```
 ip route-static 192.168.1.0 255.255.255.0 Tunnel 0 preference 60
 /访问中心内网的数据从tunnel 0走/
```