MSR使用IPsec虚拟隧道接口建立IPsec安全隧道典型配置

IPsec 马文斌 2013-07-25 发表

一、 组网需求：
要求RTA和RTB之间路由可达，PCA使用RTA上的loopback 0口代替，PCB由RTB上的loopback 0口代替，并且有如下要求：
1、分支RTA和总部RTB之间所有的数据流都需要使用IPsec加密，并且要求IPsec自动建立，不要人工触发。
2、分支的接口IP地址不固定情况下。
3、当企业分支的私网IP地址段调整时，不需要改变企业总部网关的IPsec配置。
其中RTA模拟总部、RTB模拟分支
二、 组网图：

图1 组网图
三、 配置步骤：
总部RTA配置：

```
#
 ike local-name rta  //配置本地ike-name为rta
#
ike peer rtb  //配置ike peer
 exchange-mode aggressive  //由于对端地址不固定，故使用野蛮模式
 pre-shared-key cipher $c$3$uDGtFFtWMQH6VTGbBg3tVMZg5uAk0w==
 id-type name
 remote-name rtb  //对端名称，一定要配对
 local-name rta   //本端名称，必须配置，否则IKE第一阶段协商不通过
#
ipsec proposal 1
#
ipsec profile rtb  //配置名字为rtb的安全框架，用于保护RTA和RTB之间的流
 ike-peer rtb
 proposal 1
#
interface Serial5/0
 link-protocol ppp
ip address 2.2.1.1 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 1.1.5.1 255.255.255.0
#
interface Tunnel0
 ip address 10.1.1.1 255.255.255.0
 tunnel-protocol ipsec ipv4  //更改tunnel接口的封装模式为IPsec over IPv4方式，默认为GRE方式
 source GigabitEthernet0/1  //源地址为G0/1接口，由于对端为自动获取地址，所以不需要指定目的，特别说明一下，此处两端使用串口也是一样的。
 ipsec profile rtb  //绑定安全框架
#
//将流量引入到tunnel口上
ip route-static 0.0.0.0 0 255.255.255.255 Tunnel0
#
Return
```

分支RTB配置：

```
ike local-name rtb
#
ike peer rta
 exchange-mode aggressive
 pre-shared-key cipher $c$3$t8+iPH8IHJrgmbrxnH3DI0jh6nbSTw==
 id-type name
```

```
 remote-name rta
 local-name rtb
#
ipsec proposal 1
#
ipsec profile rtb
 ike-peer rtb
 proposal 1
interface Serial5/0
 link-protocol ppp
ip address 2.2.1.2 255.255.255.0
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet0/1
 port link-mode route
ip address 1.1.5.2 255.255.255.0
#
interface Tunnel0
 ip address 10.1.1.2 255.255.255.0
 tunnel-protocol ipsec ipv4
 source GigabitEthernet0/1
 destination 1.1.5.1
 ipsec profile rtb
#
ip route-static 0.0.0.0 0 Tunnel0
#
Return
```

配置结果检验：

以上配置完成之后，当RTA的接口G0/1完成自动拨号后，RTA会自动发起与Router B之间的IKE协商。当IKE协商完成之后，RTA和RTB上的IPsec虚拟隧道接口链路状态都将up，即可以满足上述组网需求，对总部和分支的数据流进行安全保护。

IKE协商通过后会有如下提示：

```
%Sep 10 19:46:22:595 2012 D IFNET/3/LINK_UPDOWN: Tunnel0 link status is UP.
%Sep 10 19:46:22:596 2012 D IFNET/5/LINEPROTO_UPDOWN: Line protocol on the interface Tunn
el0 is UP.
```

此时查看IKE和IPsec的信息：

```
dis ike sa
   total phase-1 SAs:  1
   connection-id  peer           flag       phase   doi
  --------------------------------------------------------------------
    301          1.1.5.1        RD|ST        1     IPSEC
    302          1.1.5.1        RD|ST        2     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
dis ipsec sa
================================
Interface: Tunnel0
   path MTU: 1443
================================

  -----------------------------
  IPsec policy name: "rtb"
  sequence number: 1
  mode: tunnel
  -----------------------------
    connection id: 8
    encapsulation mode: tunnel
    perfect forward secrecy:
    tunnel:
        local  address: 1.1.5.2
        remote address: 1.1.5.1
    flow:
```

```
    sour addr: 0.0.0.0/0.0.0.0  port: 0  protocol: IP
    dest addr: 0.0.0.0/0.0.0.0  port: 0  protocol: IP

  [inbound ESP SAs]
    spi: 2403848327 (0x8f47d087)
    proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1843200/3574
    max received sequence-number: 1
    anti-replay check enable: Y
    anti-replay window size: 32
    udp encapsulation used for nat traversal: N

  [outbound ESP SAs]
    spi: 3623996886 (0xd801cdd6)
    proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1843200/3574
    max received sequence-number: 1
    udp encapsulation used for nat traversal: N
```

ping测试：

```
[RTB]ping -a 4.4.4.4 3.3.3.3
  PING 3.3.3.3: 56  data bytes, press CTRL_C to break
    Reply from 3.3.3.3: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 3.3.3.3: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 3.3.3.3: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 3.3.3.3: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 3.3.3.3: bytes=56 Sequence=5 ttl=255 time=1 ms
```

四、 配置关键点：

1、ike peer下的local-name一定要配置，否则会导致IKE协商不通过

2、Tunnel口下的隧道封装要改为ipsec over ipv4，默认情况下为gre封装