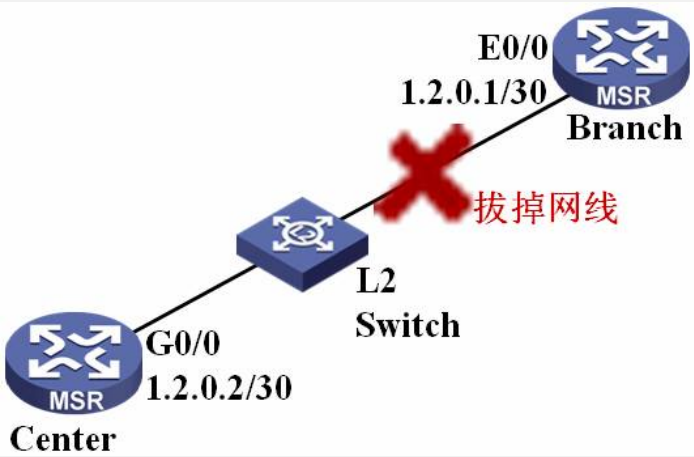
MSR系列路由器IKE DPD功能的配置

丘子隽 2007-01-18 发表

MSR系列路由器
IKE DPD功能的配置

关键字：MSR;IPSec;IKE;DPD;调试

一、**组网需求**：
Center和Branch建立IPSec连接，Center和Branch都配置DPD，并在Center上进行验证
设备清单：MSR系列路由器2台
二、组网图：



三、配置步骤：
适用设备和版本：MSR系列、Version 5.20, Beta 1202后所有版本。

Center配置

```
#
//配置DPD组，采用默认配置10秒空闲计时，5秒应答等候超时
ike dpd dpdgroup
#
//IKE Peer配置
ike peer Branch
 pre-shared-key h3c
 remote-address 1.2.0.1
 //指定dpd组
 dpd dpdgroup
#
//IPSec提议配置
ipsec proposal def
#
//IPSec策略配置
ipsec policy branch 1 isakmp
 security acl 3000
 ike-peer branch
 proposal def
#
//ACL配置
acl number 3000
 rule 0 permit ip source 1.2.0.2 0 destination 1.2.0.1 0
#
//对接接口
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 1.2.0.2 255.255.255.252
 //绑定IPSec策略
 ipsec policy branch
#
```

Branch配置

```
#
//配置DPD组，采用默认配置10秒空闲计时，5秒应答等候超时
ike dpd dpdgroup
#
//IKE Peer配置
ike peer center
 pre-shared-key h3c
 remote-address 1.2.0.2
 //指定dpd组
 dpd dpdgroup
#
//IPSec提议配置
ipsec proposal def
#
//IPSec策略配置
ipsec policy center 1 isakmp
 security acl 3000
 ike-peer center
 proposal def
#
//ACL配置
acl number 3000
 rule 0 permit ip source 1.2.0.1 0 destination 1.2.0.2 0
#
//对接接口
interface Ethernet0/0
 port link-mode route
 combo enable copper
 ip address 1.2.0.1 255.255.255.252
 //绑定IPSec策略
 ipsec policy center
#
```

Center上进行验证

```
//通过Ping触发建立IPSec会话
[center]ping 1.2.0.1
  PING 1.2.0.1: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 1.2.0.1: bytes=56 Sequence=2 ttl=255 time=6 ms
    Reply from 1.2.0.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=4 ttl=255 time=4 ms
    Reply from 1.2.0.1: bytes=56 Sequence=5 ttl=255 time=3 ms

  --- 1.2.0.1 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 2/3/6 ms
//察看IKE SA
[center]dis ike sa
    total phase-1 SAs:  1
    connection-id  peer          flag       phase   doi
  --------------------------------------------------------------
       3         1.2.0.1        RD|ST      2     IPSEC
       2         1.2.0.1        RD|ST      1     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO—TIMEOUT
//察看IPSec SA
[center]dis ipsec sa
==============================
Interface: GigabitEthernet0/0
    path MTU: 1500
==============================

  ----------------------------
  IPsec policy name: "branch"
  sequence number: 1
  mode: isakmp
  ----------------------------
    connection id: 3
    encapsulation mode: tunnel
    perfect forward secrecy: None
    tunnel:
       local  address: 1.2.0.2
       remote address: 1.2.0.1
    flow:    (5 times matched)
       sour addr: 1.2.0.2/255.255.255.255  port: 0  protocol: IP
       dest addr: 1.2.0.1/255.255.255.255  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 114800532 (0x6d7b794)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887436464/3591

[center]q
<center>dis deb
<center>deb ike dpd ?
  <cr>
```

```
//打开Debug IKE DPD的开关
<center>deb ike dpd
<center>t d
% Current terminal debugging is on

<center>t m
% Current terminal monitor is on

<center>dis th
#
Return
//连续发出100个包
<center>ping -c 100 1.2.0.1
  PING 1.2.0.1: 56  data bytes, press CTRL_C to break
//发包前会发出DPD请求
*Jan 18 15:42:17:76 2007 center IKE/7/DEBUG:branch REQUEST(send dpd request): send a message (seqno:847857594)
//收到了对方发回的DPD应答
*Jan 18 15:42:17:79 2007 center IKE/7/DEBUG:branch REQUEST(recv dpd response): received a message (seqno:847857594)
    Reply from 1.2.0.1: bytes=56 Sequence=1 ttl=255 time=5 ms
    Reply from 1.2.0.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=4 ttl=255 time=3 ms
    Reply from 1.2.0.1: bytes=56 Sequence=5 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=6 ttl=255 time=3 ms
    Reply from 1.2.0.1: bytes=56 Sequence=7 ttl=255 time=3 ms
    Reply from 1.2.0.1: bytes=56 Sequence=8 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=9 ttl=255 time=3 ms
    Reply from 1.2.0.1: bytes=56 Sequence=10 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=11 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=12 ttl=255 time=4 ms
    Reply from 1.2.0.1: bytes=56 Sequence=13 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=14 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=15 ttl=255 time=3 ms
    Reply from 1.2.0.1: bytes=56 Sequence=16 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=17 ttl=255 time=3 ms
    Reply from 1.2.0.1: bytes=56 Sequence=18 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=19 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=20 ttl=255 time=3 ms
    Reply from 1.2.0.1: bytes=56 Sequence=21 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=22 ttl=255 time=3 ms
Reply from 1.2.0.1: bytes=56 Sequence=23 ttl=255 time=2 ms
//此时Branch端拔掉网线
    Request time out
    Request time out
    Request time out
    Request time out
Request time out
//在等候一段时间后发送第一个DPD请求
*Jan 18 15:42:33:23 2007 center IKE/7/DEBUG:branch REQUEST(send dpd request): send a message (seqno:847857595)
    Request time out
Request time out
//发送第一个DPD请求后，等待5秒后超时
*Jan 18 15:42:38:62 2007 center IKE/7/DEBUG:branch REQUEST: wait for response timeout
//发送第二个DPD请求
*Jan 18 15:42:38:62 2007 center IKE/7/DEBUG:branch REQUEST(send dpd request): send a message (seqno:847857595)
    Request time out
Request time out
//第二个请求等候超时
*Jan 18 15:42:43:101 2007 center IKE/7/DEBUG:branch REQUEST: wait for response timeout
//发送第三个DPD请求
*Jan 18 15:42:43:101 2007 center IKE/7/DEBUG:branch REQUEST(send dpd request): send a message (seqno:847857595)
    Request time out
Request time out
//第三个请求等候超时
*Jan 18 15:42:48:140 2007 center IKE/7/DEBUG:branch REQUEST: wait for response timeout
//DPD三次请求超时后删除所有SA
*Jan 18 15:42:48:140 2007 center IKE/7/DEBUG:branch REQUEST: there are three fail and all SAs associated were deleted
    Request time out
    Request time out
    Request time out
    Request time out

  --- 1.2.0.1 ping statistics ---
    38 packet(s) transmitted
    23 packet(s) received
    39.47% packet loss
    round-trip min/avg/max = 2/2/5 ms
//此时可以看到SA已经不能建立
<center>dis ike sa
    total phase-1 SAs:  0
```

```
  connection-id  peer           flag       phase   doi
 ------------------------------------------------------------
      4        <unnamed>      NONE         1     IPSEC

 flag meaning
 RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
<center>
//等待一段时间再次察看SA，不存在任何SA
<center>dis ike sa
   total phase-1 SAs:  0
   connection-id  peer           flag       phase   doi
 ------------------------------------------------------------
//此时Branch插上网线，再ping触发SA建立
<center>ping 1.2.0.1
  PING 1.2.0.1: 56  data bytes, press CTRL_C to break
//显示IKE协商中的Vender ID信息，此时表明IKE重协商
*Jan 18 15:44:57:287 2007 center IKE/7/DEBUG:send VID: afcad713 68a1f1c9
6b8696fc 77570100 (DPD)
*Jan 18 15:44:57:487 2007 center IKE/7/DEBUG:vendor[0] :
*Jan 18 15:44:57:487 2007 center IKE/7/DEBUG:afcad713 68a1f1c9 6b8696fc 7
7570100
*Jan 18 15:44:57:488 2007 center IKE/7/DEBUG:recv_VID: afcad713 68a1f1c9
6b8696fc 77570100 (DPD)
Request time out
//发送DPD请求
*Jan 18 15:44:59:430 2007 center IKE/7/DEBUG:branch REQUEST(send dpd r
equest): send a message (seqno:847857595)
//收到DPD应答
*Jan 18 15:44:59:432 2007 center IKE/7/DEBUG:branch REQUEST(recv dpd re
sponse): received a message (seqno:847857595)
    Reply from 1.2.0.1: bytes=56 Sequence=2 ttl=255 time=5 ms
    Reply from 1.2.0.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 1.2.0.1: bytes=56 Sequence=4 ttl=255 time=3 ms
    Reply from 1.2.0.1: bytes=56 Sequence=5 ttl=255 time=3 ms

  --- 1.2.0.1 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 2/3/5 ms
//察看IKE SA
<center>dis ike sa
   total phase-1 SAs:  1
   connection-id  peer           flag       phase   doi
 ------------------------------------------------------------
      7        1.2.0.1        RD|ST        2     IPSEC
      6        1.2.0.1        RD|ST        1     IPSEC

 flag meaning
 RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
<center>
```

四、**配置关键点**:

1) DPD实验不要采用2台设备直连方式，在这种方式下把网线，链路层Down，不会有路由，所以用于触发IPSec的包不会发送到接口，因而也不能触发任何IPSec模块。

2) DPD并不是自始至终地周期性发送，而是通过空闲定时器机制，在每**接收**到一个IPSec加密的包后就重置这个包对应IKE SA的空闲定时器，如果空闲定时器计时开始到计时结束过程都没有**接收**到该SA对应的加密包，那么下一次有IP包要被这个SA加密**发送或接收到加密包**之前就需要使用DPD来检测对方是否存活。

3) DPD检测主要靠超时计时器，超时计时器用于判断是否再次发起请求，一般来说连续发出3次请求（请求->超时->请求->超时->请求->超时）都没有收到任何DPD应答就应该删除SA，后续如需继续发送加密数据包就需要重新协商SA，如果此时收到加密数据包表明是原来SA的会通知对端重新协商SA。