MSR V7 系列路由器和 MSR V5 系列路由器野蛮式对接 L2TP over IPSEC 典型配置

一、 组网需求：

要求 MSR3020 和 MSR3620 之间路由可达，PCA 使用 MSR3620 上的 loopback 0 口代替，PCB 由 MSR3020 上的 loopback 0 口代替，并且有如下要求：

1、双方使用野蛮模式建立 IPsec 隧道；

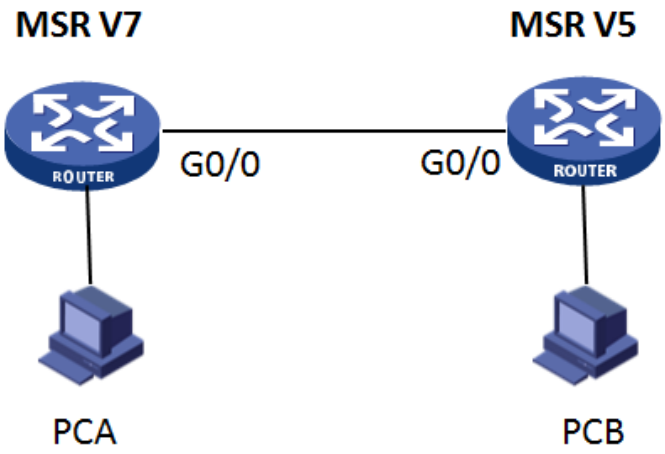
2、双方使用预共享密钥的方式建立 IPsec；

3、MSR3620 作为 LAC，MSR3020 作为 LNS

4、LAC 采用 LAC-auto-initiate 方式连接到 LNS。

5、双方采用 IPSec over L2TP 的方式。

二、 组网图：



三、 配置步骤：

MSR3620（V7 平台）配置：

#配置出接口地址：

[MSR3620] interface GigabitEthernet0/0

[MSR3620-GigabitEthernet0/0] ip address 10.0.0.1 255.255.255.0

#使用一个 Loopback 地址，用来模仿内部 PC：

```
[MSR3620] interface LoopBack0

[MSR3620-LoopBack0] ip address 192.168.1.1 255.255.255.255
```

配置 ACL 3000，定义要保护 L2TP 的数据流。

```
[MSR3620] acl number 3000

[MSR3620-acl-adv-3000] rule permit ip source 10.0.0.1 0 destination
10.0.0.2 0

[MSR3620-acl-adv-3000] quit
```

创建 IPsec 安全提议 tran1

```
[MSR3620] ipsec transform-set tran1

[MSR3620-ipsec-transform-set-tran1] encapsulation-mode tunnel

[MSR3620-ipsec-transform-set-tran1] protocol esp

[MSR3620-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc

[MSR3620-ipsec-transform-set-tran1] esp authentication-algorithm sha1

[MSR3620-ipsec-transform-set-tran1] quit
```

#配置 IKE 的钥匙链，对端地址 10.0.0.2，密钥为 123

```
[MSR3620] ike keychain keychain1

[MSR3620-ike-keychain-keychain1]pre-shared-key address 10.0.0.2
255.255.255.255 key simple 123
```

#配置标识本端身份的方式为 fqdn

```
[MSR3620]ike identity fqdn
```

#配置 IKE profile，定义使用野蛮模式，本端名字为 MSR3620，对端名字为 MSR3020

```
[MSR3620] ike profile profile1

[MSR3620-ike-profile-profile1] exchange-mode aggressive

[MSR3620-ike-profile-profile1] local-identity fqdn MSR3620

[MSR3620-ike-profile-profile1] match remote identity fqdn MSR3020

[MSR3620-ike-profile-profile1] keychain keychain1
```

#配置 IPSEC 策略 map1，调用了 IKE profile、IPSEC 提议、安全 ACL 以及指定对端地址

```
[MSR3620] ipsec policy map1 10 isakmp

[MSR3620-ipsec-policy-isakmp-map1-10] remote-address 10.0.0.2

[MSR3620-ipsec-policy-isakmp-map1-10] transform-set tran1

[MSR3620-ipsec-policy-isakmp-map1-10] security acl 3000

[MSR3620-ipsec-policy-isakmp-map1-10] ike-profile profile1

[MSR3620-ipsec-policy-isakmp-map1-10] quit
```

#物理接口下调用 IPSEC 策略

```
[MSR3620] interface GigabitEthernet0/0

[MSR3620-GigabitEthernet0/0] ipsec apply policy map1
```

#配置 L2TP,隧道名为 LAC，开启隧道认证，认证密码为 aabbcc

```
[MSR3620] l2tp enable

[MSR3620] l2tp-group 1 mode lac

[MSR3620-l2tp1] tunnel name LAC

[MSR3620-l2tp1] lns-ip 10.0.0.2

[MSR3620-l2tp1] tunnel authentication

[MSR3620-l2tp1] tunnel password simple aabbcc
```

```
[MSR3620-l2tp1] quit
```

#创建虚拟 PPP 接口 Virtual-PPP 1，配置 PPP 用户的用户名为 vpdnuser、密码为 Hello，并配置 PPP 验证方式为 PAP

```
[MSR3620] interface virtual-ppp 1
[MSR3620-Virtual-PPP1] ip address ppp-negotiate
[MSR3620-Virtual-PPP1] ppp pap local-user vpdnuser password simple Hello
[MSR3620-Virtual-PPP1] quit
```

 # 配置私网路由，访问公司总部的报文将通过 L2TP 隧道转发。

```
[MSR3620] ip route-static 192.168.2.1 24 virtual-ppp 1
```

 # 触发 LAC 发起 L2TP 隧道建立请求。

```
[MSR3620] interface virtual-ppp 1
[MSR3620-Virtual-PPP1] l2tp-auto-client l2tp-group 1
```

MSR3020（V5 平台）配置：

#配置出接口地址：

```
[MSR3020] interface GigabitEthernet0/0
[MSR3020-GigabitEthernet0/0] ip address 10.0.0.2 255.255.255.0
```

#创建 loopback 0 口，模拟内网的终端设备 192.168.2.1

```
[MSR3020] interface LoopBack0
[MSR3020-LoopBack0] ip address 192.168.2.1 255.255.255.255
```

#配置 ike peer

```
[MSR3020]ike peer MSR3620
```

[MSR3020-ike-peer-msr3620]pre-shared-key simple 123

[MSR3020-ike-peer-msr3620]remote-name MSR3620

[MSR3020-ike-peer-msr3620]local-name MSR3020

[MSR3020-ike-peer-msr3620]exchange-mode aggressive

 # 创建 IPsec 安全提议 tran1

[MSR30]ipsec transform-set tran1

[MSR3020-ipsec-transform-set-tran1]esp authentication-algorithm sha1

[MSR3020-ipsec-transform-set-tran1]esp encryption-algorithm des

#配置 IPSEC 策略模版

[MSR3020]ipsec policy-template temp1 10

[MSR3020-ipsec-policy-template-temp1-10]ike-peer MSR3620

[MSR3020-ipsec-policy-template-temp1-10]transform-set tran1

#配置 IPSEC 策略，调用策略模版

[MSR3020]ipsec policy map1 10 isakmp template temp1

#物理接口下调用 IPSEC 策略

[MSR3020] interface GigabitEthernet0/0

[MSR3020-GigabitEthernet0/0] ipsec policy map1

 # 创建本地用户，配置用户名、密码及服务类型。

[MSR3020] local-user vpdnuser

[MSR3020-luser-vpdnuser] password simple Hello

[MSR3020-luser-vpdnuser] service-type ppp

[MSR3020-luser-vpdnuser] quit

 # 配置虚拟模板接口 Virtual-Template1 的相关信息。

```
[MSR3020] interface virtual-template 1

[MSR3020-virtual-template1] ip address 100.0.0.1 255.255.255.0

[MSR3020-virtual-template1] remote address pool 1

[MSR3020-virtual-template1] ppp authentication-mode pap

[MSR3020-virtual-template1] quit
```

 # 对 VPN 用户采用本地验证。

```
[MSR3020] domain system

[MSR3020-isp-system] authentication ppp local

[MSR3020-isp-system] ip pool 1 100.0.0.2 100.0.0.100

[MSR3020-isp-system] quit
```

#配置 L2TP,隧道名为 LAC，开启隧道认证，认证密码为 aabbcc

```
[MSR3020] l2tp enable

[MSR3020] l2tp-group 1

[MSR3020-l2tp1] tunnel name LNS

[MSR3020-l2tp1] allow l2tp virtual-template 1 remote LAC

[MSR3020-l2tp1] tunnel authentication

[MSR3020-l2tp1] tunnel password simple aabbcc

[MSR3020-l2tp1] quit
```

 # 配置私网路由，访问 VPN 用户的报文将通过 L2TP 隧道转发。

```
[MSR3020] ip route-static 192.168.1.1 24 virtual-template 1
```

配置结果：

触发建立 IPSec 之后，在 MSR3620 上使用 display ike sa 和 display ipsec sa，可以看到如下：

```
<MSR3620>display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    21              10.0.0.2              RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
<MSR36>display ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------


  -----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: isakmp
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
```

```
Perfect forward secrecy:

Path MTU: 1443

Tunnel:

    local  address: 10.0.0.1

    remote address: 10.0.0.2

Flow:

sour addr: 10.0.0.1/255.255.255.255  port: 0  protocol: ip

dest addr: 10.0.0.2/255.255.255.255  port: 0  protocol: ip


[Inbound ESP SAs]

  SPI: 798983257 (0x2f9f8459)

  Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1

  SA duration (kilobytes/sec): 1843200/3600

  SA remaining duration (kilobytes/sec): 1843092/2983

  Max received sequence-number: 263

  Anti-replay check enable: Y

  Anti-replay window size: 64

  UDP encapsulation used for NAT traversal: N

  Status: active


[Outbound ESP SAs]

  SPI: 3016720000 (0xb3cf7e80)
```

Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843092/2983

Max sent sequence-number: 254

UDP encapsulation used for NAT traversal: N

Status: active

触发建立 L2TP 之后，在 MSR3620 上使用 display l2tp tuunel 和 display l2tp session，可以看到如下

<MSR36>display l2tp tunnel

LocalTID RemoteTID State Sessions RemoteAddress RemotePort RemoteName

41386 1 Established 1 10.0.0.2 1701 MSR30

<MSR36>display l2tp session

LocalSID RemoteSID LocalTID State

1350 16363 41386 Established

四、 配置关键点：

1、本配置是 L2TP OVER IPSEC，因此 IPSEC 感兴趣流 acl 要匹配 L2TP 封装后的数据包的地址。

2、V7 侧 ike profile 下须要配置 match remote 命令，否则会导致 DPD 探测异常；

3、V7 侧非 IPSec 模板方式，IPSec 策略下须配置 remote address 命令，否则会导致无法触发 IPSec 触发。

4、在 L2TP OVER IPSEC 中，IPSec 应用在物理口上。