第 3 章　广域网协议及传输安全

广域网俗称 WAN(Wide Area Network),是覆盖较大地理范围的数据通信网络,WAN 可能会覆盖一座城市、一个国家/地区或者是全球,一般情况广域网使用 ISP(Internet Service Provider)提供的传输设施传输数据。而在广域网上传输数据,如何保证其安全性能是至关重要的,虚拟专网 VPN(Virtual Private Network)就是利用公用网络来架设专用网络的技术,从而保证数据传输的安全。

3.1　PPP 协议

PPP 协议是提供在点到点链路上承载网络层数据包的一种链路层协议。PPP 定义了一整套的协议,包括链路控制协议(LCP)、网络层控制协议(NCP)和验证协议(PAP 和 CHAP)。由于 PPP 易于扩充、支持同异步且能够提供用户验证,因而获得了较广泛的应用。有关于 PPP 的协议规范详见 RFC 1661。

3.1.1　PAP 认证配置

【配置命令解析】

```
Ruijie(config-if)#encapsulation ppp
配置接口封装 PPP 协议
```

1. 被认证方

```
Ruijie(config-if)#ppp pap sent-username username password [0|7] password
指定 PPP PAP 认证的用户名和密码,被认证方配置
```

2. 主认证方

```
Ruijie(config-if)#ppp authentication pap
主认证方启用 PAP 认证
Ruijie(config)#username username password [0|7] password
创建用户数据库账号密码
```

3.1.2　CHAP 认证配置

【配置命令解析】

```
Ruijie(config-if)#encapsulation ppp
配置接口封装 PPP 协议
```

1. 被认证方

```
Ruijie(config-if)#ppp chap hostname hostname
指定 PPP CHAP 认证的主机名，如果不配置用户名，被认证方发送自己的主机名作为 PPP 的用户名
Ruijie(config-if)#ppp chap password [0|7] password
指定 PPP CHAP 认证的密码
Ruijie(config)#username username password [0|7] password
在知道认证方使用的用户名和密码前提下，可以创建用户数据库记录而不配置认证密码
```

2. 主认证方

```
Ruijie(config-if)#ppp authentication chap
主认证方启用 CHAP 认证
Ruijie(config)#username username password [0|7] password
创建用户数据库账号密码
```

3.1.3　PPP 多链路捆绑配置

【配置命令解析】

```
Ruijie(config)#interface multilink group-number
创建逻辑接口 multilink
Ruijie(config)#interface serial interface-number
进入串行接口配置模式
Ruijie(config-if)#encapsulation ppp
封装 PPP 协议
Ruijie(config-if)#ppp multilink
设置 multilink 协商模式
Ruijie(config-if)#ppp multilink group group-number
设定多链路组的组号
```

3.1.4　PPP 综合案例解析

【案例拓扑】

案例拓扑如图 3-1 所示。

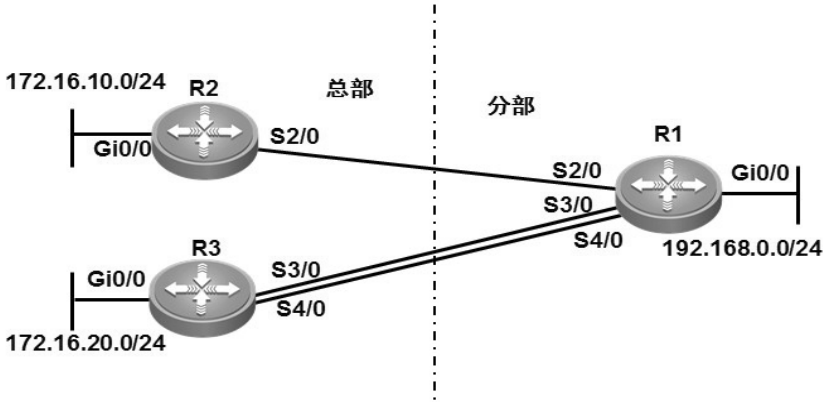

图 3-1 案例拓扑

设备参数如表 3-1 所示。

表 3-1 设备参数表

设备	设备接口	IP 地址	子网掩码	说明
R2	Gi0/0	172.16.10.254	255.255.255.0	
	S2/0	10.1.2.1	255.255.255.252	
R3	Gi0/0	172.16.20.254	255.255.255.0	
	S3/0	10.1.3.1	255.255.255.252	捆绑组 1 成员口
	S4/0	10.1.3.1	255.255.255.252	捆绑组 1 成员口
R1	Gi0/0	192.168.0.254	255.255.255.0	
	S2/0	10.1.2.2	255.255.255.252	
	S3/0	10.1.3.2	255.255.255.252	捆绑组 1 成员口
	S4/0	10.1.3.2	255.255.255.252	捆绑组 1 成员口

【任务需求】

某小型公司本部和分部通过广域网线路连接，其中 R1～R2 间所租用的链路带宽为 2M，R1～R3 间租用的 2 条链路带宽均为 2M。具体要求如下：

(1)使用 CHAP 协议；

(2)双向认证，用户名＋验证口令方式；

(3)用户名为 ruijie，密码为 123456；

(4)R1 与 R3 间使用 PPP 链路捆绑，捆绑组号为 1。

【任务实施】

1. PPP 与多链路捆绑配置

(1)R1 的 PPP

```
R1(config)# interface multilink 1
//创建多链路捆绑组，组号为 1
```

```
R1(config-if-multilink 1)# ip address 10.1.3.2 255.255.255.252
//捆绑组配置 IP 地址,不需要给物理接口配置 IP 地址
R1(config-if-multilink 1)# exit
R1(config)# interface range serial 2/0 , 3/0 , 4/0
R1(config-if-range)# bandwidth 2000
//配置链路接口带宽
R1(config-if-range)# encapsulation ppp
//接口启用 PPP 协议封装
R1(config)# interface serial 3/0
R1(config-if-Serial 3/0)# ppp multilink
R1(config-if-Serial 3/0)# ppp multilink group 1
//物理链路加入捆绑组 1 号
R1(config-if-Serial 3/0)# exit
R1(config)# interface serial 4/0
R1(config-if-Serial 4/0)# ppp multilink
R1(config-if-Serial 4/0)# ppp multilink group 1
```

(2)R2 的 PPP

```
R2(config)# interface serial 2/0
R2(config-if-Serial 2/0)# bandwidth 2000
R2(config-if-Serial 2/0)# encapsulation ppp
```

(3)R3 的 PPP

```
R3(config)# interface multilink 1
R3(config-if-multilink 1)# ip address 10.1.3.1 255.255.255.252
R3(config-if-multilink 1)# exit
R3(config)# interface range serial 3/0, 4/0
R3(config-if-range)# bandwidth 2000
R3(config-if-range)# encapsulation ppp
R3(config-if-range)# exit
R3(config)# interface serial 3/0
R3(config-if-Serial 3/0)# ppp multilink
R3(config-if-Serial 3/0)# ppp multilink group 1
R3(config)# interface serial 4/0
R3(config-if-Serial 4/0)# ppp multilink
R3(config-if-Serial 4/0)# ppp multilink group 1
```

2. PPP 认证配置

(1)R1 的认证

```
R1(config)# username ruijie password 0 123456
//配置本地数据库认证用的账号与密码
R1(config)# interface serial 2/0
R1(config-if-Serial 2/0)# ppp authentication chap
```

```
//启用 CHAP 认证,此接口为主认证端
R1(config-if-Serial 2/0)#ppp chap hostname ruijie
//配置 CHAP 认证发送的用户名
R1(config-if-Serial 2/0)#ppp chap password 123456
//配置 CHAP 认证发送的密码
R1(config)#interface serial 3/0
R1(config-if-Serial 3/0)#ppp authentication chap
R1(config-if-Serial 3/0)#ppp chap hostname ruijie
R1(config-if-Serial 3/0)#ppp chap password 123456
R1(config)#interface serial 4/0
R1(config-if-Serial 4/0)#ppp authentication chap
R1(config-if-Serial 4/0)#ppp chap hostname ruijie
R1(config-if-Serial 4/0)#ppp chap password 123456
```

(2)R2 的认证

```
R2(config)#username ruijie password 0 123456
R2(config)#interface serial 2/0
R2(config-if-Serial 2/0)#ppp authentication chap
R2(config-if-Serial 2/0)#ppp chap hostname ruijie
R2(config-if-Serial 2/0)#ppp chap password 123456
```

(3)R3 的认证

```
R3(config)#username ruijie password 0 123456
R3(config)#interface serial 3/0
R3(config-if-Serial 3/0)#ppp authentication chap
R3(config-if-Serial 3/0)#ppp chap hostname ruijie
R3(config-if-Serial 3/0)#ppp chap password 123456
R3(config)#interface serial 4/0
R3(config-if-Serial 4/0)#ppp authentication chap
R3(config-if-Serial 4/0)#ppp chap hostname ruijie
R3(config-if-Serial 4/0)#ppp chap password 123456
```

3. 实验调试

(1)查看接口信息

```
R1#show ip interface brief
Interface                IP-Address(Pri)      IP-Address(Sec)   Status   Protocol
multilink 1              10.1.3.2/30          no address        up       up
Serial 2/0               10.1.2.2/30          no address        up       up
Serial 3/0               no address           no address        up       down
Serial 4/0               no address           no address        up       down
GigabitEthernet 0/0      192.168.0.254/24     no address        up       up
GigabitEthernet 0/1      no address           no address        down     down
```

由于 3 与 4 号串行接口进行了捆绑，所以实际的物理接口信息 Protocols 为 down。

```
R1#show interfaces multilink 1
Index(dec):38 (hex):26
multilink 1 is UP, line protocol is UP
//链路状态为 UP
Hardware is  multilink
Interface address is: 10.1.3.2/30
  MTU 1500 bytes, BW 4000 Kbit
  Encapsulation protocol is PPP, loopback not set
//协议封装为 PPP
  Keepalive interval is 10 sec ,retries 10.
  Carrier delay is 0 sec
  Rxload is 1/255, Txload is 1/255
  LCP Open, Multilink Open
  Open: ipcp
  Queueing strategy: FIFO
    Output queue 0/40, 0 drops;
    Input queue 0/75, 0 drops
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 44 bits/sec, 0 packets/sec
    10 packets input, 1020 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    20 packets output, 1180 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 5 interface resets
```

(2)查看 PPP 验证过程

```
R2(config)#interface serial 2/0
R2(config-if-Serial 2/0)#no ppp authentication
//为了方便观察调试信息，改成单向认证
R1#debug ppp authentication
//开启 PPP 认证调试信息
R1(config)#interface serial 2/0
R1(config-if-Serial 2/0)#shutdown
R1(config-if-Serial 2/0)#no shutdown
//重新打开接口观察认证过程
* Sep  1 11:41:54: %7: PPP: ppp_clear_author(), protocol = LCP
* Sep  1 11:41:54: %LINK-3-UPDOWN: Interface Serial 2/0, changed state to up.
* Sep  1 11:41:57: %7: PPP: Serial 2/0 Using CHAP hostname ruijie.
//使用 ruijie 作为 CHAP 认证的用户名
* Sep  1 11:41:57: %7: PPP: Serial 2/0 [O] CHAP CHALLENGE id 13 len 23
```

```
//从 R1 发送 ID 为 13 的质询
*Sep  1 11:41:57: %7: PPP: Serial 2/0 [I] CHAP RESPONSE id 13 len 23
*Sep  1 11:41:57: %7: PPP: Serial 2/0 CHAP response id=13 ,received from ruijie
//从 R2 收到 ID 为 13 的响应
*Sep  1 11:41:57: %7: PPP: Serial 2/0 [O] MSG:"Authentication success"
*Sep  1 11:41:57: %7: PPP: Serial 2/0 [O] CHAP SUCCESS id 13 len 22
//从 R1 发送 ID 为 13 的认证成功信息
*Sep  1 11:41:57: %7: :PPP: Serial 2/0 authentication OK, begin networkphase!
*Sep  1 11:41:57: %7: PPP: ppp_clear_author(), protocol = IPCP
*Sep  1 11:41:57: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial 2/0, changed
state to up.
```

以上输出显示 CHAP 的认证过程是 3 次握手。

3.2 IPsec VPN

IPSec 为两个 IPSec 对等体，例如两台设备，提供安全通道。由您定义哪些是需要保护的敏感数据流，并将由安全通道进行传送，并且通过指定这些通道的参数来定义用于保护这些敏感包的参数，当 IPSec 看到这样的一个敏感包时，它将建立起相应的安全通道，通过这条安全通道将这个数据报传送到远端对等体。

3.2.1 IPsec VPN 配置

IPsec 的配置任务主要分为几个部分：定义感兴趣的数据流、配置 IKE 协商或者手工指定、定义变换集合、配置加密映射集合、接口应用。其中感兴趣的数据流是通过访问控制列表来定义的，命令的解析请见第 7 章。

【配置命令解析】

1. 配置 IKE

```
Ruijie(config)#crypto isakmp enable
打开 IKE 功能
Ruijie(config)#crypto isakmp policy Priority
标识要创建的策略，每条策略由优先级唯一标识
Ruijie(config-isakmp)#encryption des | 3des | aes-128 | aes-192 | aes-256 | sm1
 指定加密算法
Ruijie(config-isakmp)#hash {sha | md5}
指定 HASH 算法
Ruijie(config-isakmp)#authentication {pre-share | rsa-sig | digital-email }
指定验证算法，预共享秘钥是常用的方法
Ruijie(config-isakmp)#group {1 | 2 | 5}
指定 Diffie-Hellman 组标识
Ruijie(config-isakmp)#lifetime seconds
指定 IKE 安全联盟的生命周期
```

2. 定义变换集合

Ruijie(config)# **crypto ipsec transform-set** *transform-set-name transform1* [*transform2* [*transform3*]]

transform 参数是系统所支持的算法，算法可以进行一定规则的组合

Ruijie(cfg-crypto-trans)# **mode** {**tunnel** | **transport**}

默认情况下是隧道模式，隧道模式会把原来整个 IP 报文封装，隐藏其源目的 IP 地址

3. 配置加密映射集合

Ruijie(config)# **crypto map** *map-name seq-num* **ipsec-manual**

手工方式创建安全联盟

Ruijie(config)# **crypto map** *map-name seq-num* **ipsec-isakmp**

使用 IKE 来建立安全联盟的加密映射条目

Ruijie(config-crypto-map)# **match address** *access-list-id*

为加密映射列表指定一个访问列表。这个访问列表决定了哪些通信应该受到 IPSec 的保护，哪些通信不应该受到此加密映射条目中定义的 IPSec 安全性的保护

Ruijie(config-crypto-map)# **set peer** {*hostname* | *ip-address*} [*trustpoint1* [*trustpoint2*]]

指定远端 IPSec 对等体，受到 IPSec 保护的通信将被发往这个对等体，可以设定多个 peer

Ruijie(config-crypto-map)# **set transform-set** *transform-set-name1*

指定使用哪个定义的变换集合

Ruijie(config-crypto-map)# **reverse-route** [**remote-peer** *ip-address*]

配置反向路由注入，在不允许配置明细静态路由的情况下可以由方向路由注入方式加入到路由表中

4. 接口应用加密图

Ruijie(config-if)# **crypto map** *map-name*

将加密映射集合应用于接口

3.2.2　VPN 案例解析

【案例拓扑】

案例拓扑如图 3-2 所示，各接口信息如表 3-2 所示。

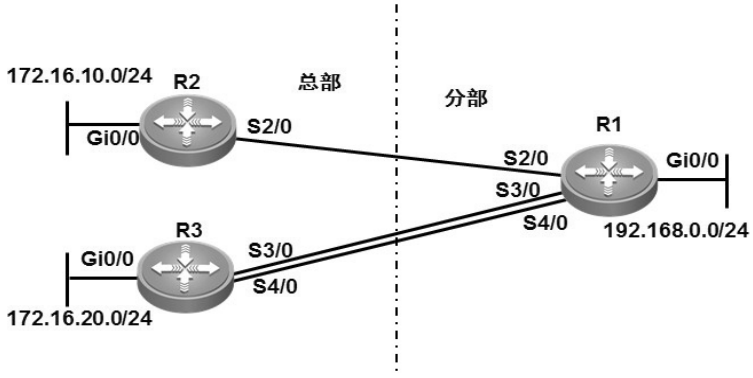

图 3-2　VPN 案例拓扑

设备参数如表 3-2 所示。

表 3-2 设备参数表

设备	设备接口	IP 地址	子网掩码	说明
R2	Gi0/0	172.16.10.254	255.255.255.0	
	S2/0	10.1.2.1	255.255.255.252	
R3	Gi0/0	172.16.20.254	255.255.255.0	
	S3/0	10.1.3.1	255.255.255.252	捆绑组 1 成员口
	S4/0	10.1.3.1	255.255.255.252	捆绑组 1 成员口
R1	Gi0/0	192.168.0.254	255.255.255.0	
	S2/0	10.1.2.2	255.255.255.252	
	S3/0	10.1.3.2	255.255.255.252	捆绑组 1 成员口
	S4/0	10.1.3.2	255.255.255.252	捆绑组 1 成员口

【任务需求】

总分机构之间使用 IPSec 对数据流进行加密，要求使用静态隧道模式，安全协议采用 ESP 协议，加密算法采用 3des，认证算法采用 md5，以 IKE 方式建立 IPsec SA。

在 R1 上所配置的参数要求如下：

(1)ACL 编号为 103；

(2)预共享秘钥为明文 ruijie；

(3)IPSEC 加密转换集为 Myset；

(4)R1、R2 间 IPSEC 加密图为 To_R2；

(5)R1、R3 间 IPSEC 加密图为 To_R3；

(6)启用 DPD 探测周期为 10 秒，使用周期探测模式。

在 R2 和 R3 上所配置的参数要求如下：

(1)ACL 编号为 103；

(2)预共享秘钥为明文 ruijie；

(3)IPSEC 加密转换集为 Myset；

(4)IPSEC 加密图为 Mymap。

【任务实施】

1. 路由部署

```
R1(config)# ip route 172.16.10.0 255.255.255.0 10.1.2.1
R1(config)# ip route 172.16.20.0 255.255.255.0 10.1.3.1
R2(config)# ip route 192.168.0.0 255.255.255.0 10.1.2.2
R3(config)# ip route 192.168.0.0 255.255.255.0 10.1.3.2
```

2. VPN 数据流定义

```
R1(config)#ip access-list extended 103
R1(config-ext-nacl)#10 permit ip 192.168.0.0 0.0.0.255 172.16.10.0 0.0.0.255
R1(config-ext-nacl)#20 permit ip 192.168.0.0 0.0.0.255 172.16.20.0 0.0.0.255
R2(config)#ip access-list extended 103
R2(config-ext-nacl)#10 permit ip 172.16.10.0 0.0.0.255 192.168.0.0 0.0.0.255
R3(config)#ip access-list extended 103
R3(config-ext-nacl)#10 permit ip 172.16.20.0 0.0.0.255 192.168.0.0 0.0.0.255
```

3. 配置 IKE

(1)R1 的 IKE

```
R1(config)#crypto isakmp enable
//启用 isakmp
R1(config)#crypto isakmp policy 10
//定义 isakmp 策略 10
R1(isakmp-policy)#authentication pre-share
//预共享秘钥模式
R1(isakmp-policy)#encryption 3des
//加密算法为 3des
R1(isakmp-policy)#hash md5
//认证算法为 md5
R1(isakmp-policy)#exit
R1(config)#crypto isakmp keepalive 10 periodic
//启动 isakmp 的 DPD 探测,并配置探测时间为 10s,模式为周期探测
R1(config)#crypto isakmp key 0 ruijie address 0.0.0.0 0.0.0.0
//配置 isakmp 秘钥与对端设备 IP,因对端有多台设备,匹配所有网段
```

(2)R2 的 IKE

```
R2(config)#crypto isakmp enable
R2(config)#crypto isakmp policy 10
R2(isakmp-policy)#authentication pre-share
R2(isakmp-policy)#encryption 3des
R2(isakmp-policy)#hash md5
R2(isakmp-policy)#exit
R2(config)#crypto isakmp key 0 ruijie address 10.1.2.2
```

(3)R3 的 IKE

```
R3(config)#crypto isakmp enable
R3(config)#crypto isakmp policy 10
R3(isakmp-policy)#authentication pre-share
R3(isakmp-policy)#encryption 3des
R3(isakmp-policy)#hash md5
R3(isakmp-policy)#exit
R3(config)#crypto isakmp key 0 ruijie address 10.1.3.2
```

4. 定义变换集合

```
R1(config)#crypto ipsec transform-set Myset esp-3des esp-md5-hmac
R2(config)#crypto ipsec transform-set Myset esp-3des esp-md5-hmac
R3(config)#crypto ipsec transform-set Myset esp-3des esp-md5-hmac
```

5. 定义加密图与应用

(1)R1 的加密图与应用

```
R1(config)#crypto map To_R2 10 ipsec-isakmp
//创建名为 To_R2 的加密图,序号为 10,类型为 ipsec-isakmp
R1(config-crypto-map)#set peer 10.1.2.1
//配置对端 IP 地址
R1(config-crypto-map)#set transform-set Myset
//使用传输模式集 Myset
R1(config-crypto-map)#match address 103
//设置感兴趣的数据流
R1(config-crypto-map)#exit
R1(config)#interface serial 2/0
R1(config-if-Serial 2/0)#crypto map To_R2
//在设备对应出接口应用相应 map 映射
R1(config)#crypto map To_R3 10 ipsec-isakmp
R1(config-crypto-map)#set peer 10.1.3.1
R1(config-crypto-map)#set transform-set Myset
R1(config-crypto-map)#match address 103
R1(config-crypto-map)#exit
R1(config)#interface multilink 1
R1(config-if-multilink 1)#crypto map To_R3
```

(2)R2 的加密图与应用

```
R2(config)#crypto map Mymap 10 ipsec-isakmp
R2(config-crypto-map)#set peer 10.1.2.2
R2(config-crypto-map)#set transform-set Myset
R2(config-crypto-map)#match address 103
R2(config-crypto-map)#exit
R2(config)#interface serial 2/0
R2(config-if-Serial 2/0)#crypto map Mymap
```

(3)R3 的加密图与应用

```
R3(config)#crypto map Mymap 10 ipsec-isakmp
R3(config-crypto-map)#set peer 10.1.3.2
R3(config-crypto-map)#set transform-set Myset
R3(config-crypto-map)#match address 103
R3(config-crypto-map)#exit
R3(config)#interface multilink 1
R3(config-if-multilink 1)#crypto map Mymap
```

6. 实验调试

(1)显示 isakmp 策略

```
R1#show crypto isakmp policy
Protection suite of priority 10
   encryption algorithm:    Three key triple DES.
//加密算法 3des
   hash algorithm:          Message Digest 5
//HASH 算法 md5
   authentication method:   Pre-Shared Key
//预共享秘钥
   Diffie-Hellman group:    #1 (768 bit)
   lifetime:                86400 seconds
Default protection suite
   encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
   hash algorithm:          Secure Hash Standard
   authentication method:   Rsa-Sig
   Diffie-Hellman group:    #1 (768 bit)
   lifetime:                86400 seconds
//生存时间,即重认证时间
```

(2)显示 ipsec 传输模式集

```
R1#show crypto ipsec transform-set
transform set Myset: { esp-md5-hmac,esp-3des,}
//传输模式集 Myset
        will negotiate = {Tunnel,}
```

(3)显示加密图

```
R1#show crypto map

Crypto Map:"To_R2" 10 ipsec-isakmp, (Complete)
//加密图名称
        Extended IP access list 103
//VPN 加密流量 ACL
        Security association lifetime: 4608000 kilobytes/3600 seconds(id=3)
        PFS (Y/N): N
        Transform sets = { Myset,  }
//使用的传输模式集
        Interfaces using crypto map To_R2:
                Serial 2/0
//加密图使用的接口
Crypto Map:"To_R3" 10 ipsec-isakmp, (Complete)
```

```
        Extended IP access list 103
        Security association lifetime: 4608000 kilobytes/3600 seconds(id=5)
        PFS (Y/N): N
        Transform sets = { Myset,  }

        Interfaces using crypto map To_R3:
                multilink 1
```

(4)显示 ipsec 会话情况

```
R1#show crypto ipsec sa

Interface: multilink 1
        Crypto map tag:To_R3
        local ipv4 addr 10.1.3.2
        media mtu 1500

        ==========================================
        sub_map type:static, seqno:10, id=2
        local  ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))
        remote  ident (addr/mask/prot/port): (172.16.10.0/0.0.0.255/0/0))
        PERMIT
        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
        #send errors 0, #recv errors 0

        No sa is created now.

        ==========================================
        sub_map type:static, seqno:10, id=3
        local  ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))
        remote  ident (addr/mask/prot/port): (172.16.20.0/0.0.0.255/0/0))
        PERMIT
        #pkts encaps: 23, #pkts encrypt: 23, #pkts digest 23
        #pkts decaps: 23, #pkts decrypt: 23, #pkts verify 23
        #send errors 0, #recv errors 0
//以上是该接口的加解密数据包流量统计情况
        Inbound esp sas:
//入方向的 ESP 安全会话
              spi:0xc01ba5e (201439838)
//区别会话的编号
               transform: esp-3des esp-md5-hmac
```

```
//传输模式集情况
                in use settings={Tunnel Encaps,}
//隧道模式
                crypto map To_R3 10
                sa timing: remaining key lifetime (k/sec): (4606994/3016)
//剩余的生存时间
                IV size: 8 bytes
                Replay detection support:Y

        Outbound esp sas:
//出方向的 ESP 安全会话
               spi:0x4d8cf2ed (1301082861)
                transform: esp-3des esp-md5-hmac
                in use settings={Tunnel Encaps,}
                crypto map To_R3 10
                sa timing: remaining key lifetime (k/sec): (4606994/3016)
                IV size: 8 bytes
                Replay detection support:Y
Interface: Serial 2/0
        Crypto map tag:To_R2
        local ipv4 addr 10.1.2.2
        media mtu 1500
        ============================================
        sub_map type:static, seqno:10, id=0
        local   ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))
        remote  ident (addr/mask/prot/port): (172.16.10.0/0.0.0.255/0/0))
        PERMIT
        #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 11
        #pkts decaps: 11, #pkts decrypt: 11, #pkts verify 11
        #send errors 0, #recv errors 0

        Inbound esp sas:
              spi:0x30b30c62 (817040482)
               transform: esp-3des esp-md5-hmac
               in use settings={Tunnel Encaps,}
               crypto map To_R2 10
               sa timing: remaining key lifetime (k/sec): (4606997/2909)
               IV size: 8 bytes
               Replay detection support:Y

        Outbound esp sas:
```

```
      spi:0x151fb54c (354399564)
       transform: esp-3des esp-md5-hmac
       in use settings={Tunnel Encaps.}
       crypto map To_R2 10
       sa timing: remaining key lifetime (k/sec): (4606997/2909)
       IV size: 8 bytes
       Replay detection support:Y
==========================================
sub_map type:static, seqno:10, id=1
local   ident (addr/mask/prot/port): (192.168.0.0/0.0.0.255/0/0))
remote  ident (addr/mask/prot/port): (172.16.20.0/0.0.0.255/0/0))
PERMIT
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#send errors 0, #recv errors 0

No sa is created now.
```