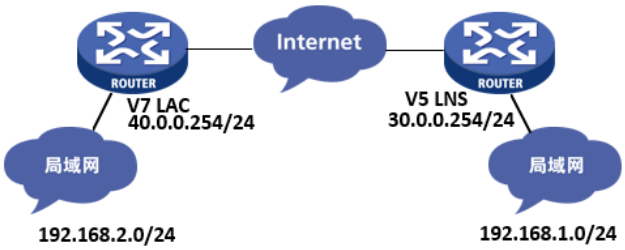
IPSEC OVER L2TP(V7LAC,V5LNS)典型配置

钟俊涛 2017-11-04 发表

客户需要通过IPSEC OVER L2TP实现对LAC和LNS之间的数据进行加密



MSRV7设备作为LAC和MSRV5的LNS设备建立L2TP。IPSEC保护的数据流为LAC的192.168.2.0/24和LNS 192.168.1.0/24。LAC和LNS都是手动配置L2TP隧道地址，LAC为10.0.0.2，LNS为10.0.0.1。LAC的公网IP为40.0.0.254，LNS的公网IP为30.0.0.254。

MSRV7(LAC)

1 配置L2TP

```
#
 l2tp enable            //开启L2TP
#
l2tp-group 1 mode lac
 lns-ip 30.0.0.254       //配置LNS的IP地址
 undo tunnel authentication   //关闭隧道认证
#
interface Virtual-PPP1
 ppp chap password cipher $c$3$jC1BLtrp78KwIF6CLV5VpjySyQ24tw==
 ppp chap user ppp
 ip address 10.0.0.2 255.255.255.0   //配置隧道口地址为10.0.0.2
 l2tp-auto-client l2tp-group 1        //触发LAC自动建立隧道
#
 ip route-static 192.168.1.0 24 Virtual-PPP1   //配置去往对端的路由
```

2 配置IPSEC

```
#
ike keychain 1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$E4P89BOZeRoKjfxLAXY78zxyOEb40A==
  //配置预共享密钥
#
ike profile 1       //配置IKE profile
 keychain 1       //调用keychain
 exchange-mode aggressive    //配置野蛮模式
 local-identity fqdn zongbu      //配置本端的fqdn为总部
 match remote identity fqdn fenzhi   //配置对端的fqdn为分支
#
ipsec transform-set 1     //配置IPSEC 安全提议
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
acl advanced 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255  //创建ACL匹配IPSEC的数据流
#
ipsec policy a 10 isakmp    //创建IPSEC策略
 transform-set 1
 security acl 3000
 remote-address 10.0.0.1   //指定对端地址，为l2tp隧道地址
 ike-profile 1
#
interface Virtual-PPP1
```

ipsec apply policy a //**virtual-ppp接口调用IPSEC策略**

MSRV5（LNS）

1　配置L2TP

#

l2tp enable //**开启L2TP**

#

interface Virtual-Template1 //**创建VT接口**

ppp authentication-mode chap

ip address 10.0.0.1 255.255.255.0 //**配置隧道地址为10.0.0.1**

#

l2tp-group 1 //**创建L2TP组1**

undo tunnel authentication //**关闭隧道认证**

allow l2tp virtual-template 1

#

local-user ppp //**创建LAC的认证的PPP账户**

password cipher c3$LATxqwpC5lJ3WPt8nCmiJVpV/eOpjw==

service-type ppp

#

ip route-static 192.168.2.0 255.255.255.0 10.0.0.2 //**配置去往LAC内网的路由**

2 配置IPSEC

#

ike peer 1 //**配置IKE对等体**

exchange-mode aggressive //**配置模式为野蛮模式**

pre-shared-key cipher c3$DWPZCGSWERWpN/fbqXSS+l83qQ9/gg==

id-type name //**指定ID类型为name类型**

remote-name zongbu //**指定对端名称为zongbu**

remote-address 10.0.0.2 //**指定对端地址为L2TP隧道地址10.0.0.2**

local-name fenzhi //**配置本端名称fenzhi**

#

ipsec transform-set 1 //**创建IPSEC安全提议**

esp authentication-algorithm md5

esp encryption-algorithm 3des

#

acl number 3000

rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 //**创建ACL匹配IP SEC数据流**

#

ipsec policy a 10 isakmp //**配置IPSEC安全策略**

security acl 3000

ike-peer 1

transform-set 1

#

interface Virtual-Template1

ipsec policy a //**在VT接口引用策略**

流量触发后可以建立成功。

<H3C>dis ipsec sa

Interface: Virtual-PPP1

IPsec policy: a

Sequence number: 10

Mode: ISAKMP

Tunnel id: 0

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1444

```
  Tunnel:
     local  address: 10.0.0.2
     remote address: 10.0.0.1
  Flow:
     sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip
     dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 2790206877 (0xa64f2d9d)
    Connection ID: 21474836481
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3428
    Max received sequence-number: 4
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 4121513637 (0xf5a94ea5)
    Connection ID: 12884901888
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3428
    Max sent sequence-number: 4
    UDP encapsulation used for NAT traversal: N
    Status: Active

<H3C>display l2tp session
LocalSID    RemoteSID    LocalTID    State
58094       12555        31353       Established
```

1.两边的IPSEC指定的对端地址都是L2TP的隧道地址。

2.配置同样适用于PPPOE拨号和IP地址不固定的LAC