MSR 系列路由器 L2TP over IPsec 典型配置举例

目 录

1 简介

本文档介绍 L2TP over IPsec 的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

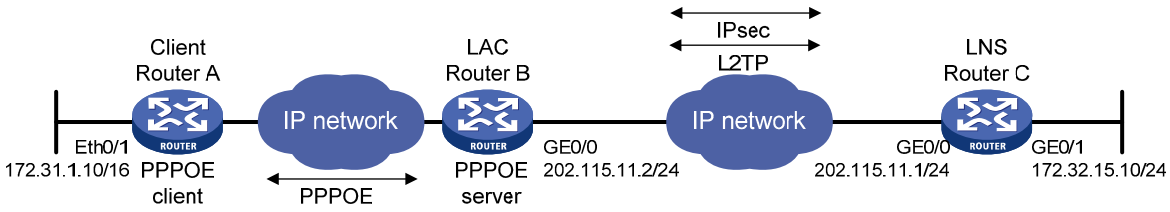
本文档假设您已了解 L2TP 和 IPsec 特性。

3 配置举例

3.1 组网需求

如 图 1 所示，L2TP Client使用PPPoE接入到LAC，LAC与LNS之间配置IPsec，加密L2TP数据流。Client的拨号接口配置出方向NAT，对内网访问外网的数据进行地址转换。LNS配置Radius方案，使用IMC服务器对PPP用户进行认证。

图1 L2TP over IPsec 配置组网图



3.2 使用版本

本举例是在 Release 2317 版本上进行配置和验证的。

3.3 配置步骤

3.3.1 Router A的配置

配置拨号访问规则。

```
<RouterA> system-view
[RouterA] dialer-rule 1 ip permit
```

配置拨号接口 Dialer0。

```
[RouterA] interface dialer 0
```

```
[RouterA-Dialer0] ppp chap user l2tp@l2tp
[RouterA-Dialer0] ppp chap password simple l2tp
[RouterA-Dialer0] ip address ppp-negotiate
[RouterA-Dialer0] dialer user PPPoE
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] dialer bundle 1
[RouterA-Dialer0] quit
```

配置 PPPoE Client。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] pppoe-client dial-bundle-number 1 idle-timeout 300
[RouterA-Ethernet0/0] quit
```

配置默认路由

```
[RouterA] ip route-static 0.0.0.0 0 Dialer0
```

配置 NAT 转换规则。

```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule 0 permit ip
[RouterA-acl-adv-3000] quit
```

在拨号接口下绑定出方向 NAT。

```
[RouterA] interface dialer 0
[RouterA-Dialer0] nat outbound 3000
[RouterA-Dialer0] quit
```

3.3.2 Router B的配置

使能 L2TP。

```
<RouterB> system-view
[RouterB] l2tp enable
```

创建 domain 和本地用户。

```
[RouterB] domain l2tp
[RouterB-isp-l2tp] quit
[RouterB] local-user l2tp
[RouterB-luser-l2tp] service-type ppp
[RouterB-luser-l2tp] quit
```

配置 l2tp-group。

```
[RouterB] l2tp-group 1
[RouterB-l2tp1] tunnel password simple msr_l2tp
[RouterB-l2tp1] tunnel name msr_lac
[RouterB-l2tp1] start l2tp ip 202.115.11.1 fullusername l2tp@l2tp
[RouterB-l2tp1] quit
```

创建 ACL3000,定义需要 IPsec 保护的数据流。

```
 [RouterB] acl number 3000
[RouterB-acl-adv-3000] rule 0 permit udp source 202.115.11.2 0 destination 202.115.11.1 0
destination-port eq 1701
[RouterB-acl-adv-3000] quit
```

配置 ike 对等体。

```
[RouterB] ike peer l2tp
[RouterB-ike-peer-l2tp] pre-shared-key l2tp
[RouterB-ike-peer-l2tp] remote-address 202.115.11.1
[RouterB-ike-peer-l2tp] quit
```

配置 IPsec proposal。

```
[RouterB] ipsec proposal l2tp
[RouterB-ipsec-proposal-l2tp] transform ah-esp
[RouterB-ipsec-proposal-l2tp] quit
```

配置 IPsec policy。

```
[RouterB] ipsec policy l2tp 1 isakmp
[RouterB-ipsec-policy-isakmp-l2tp-1] security acl 3000
[RouterB-ipsec-policy-isakmp-l2tp-1] ike-peer l2tp
[RouterB-ipsec-policy-isakmp-l2tp-1] proposal l2tp
[RouterB-ipsec-policy-isakmp-l2tp-1] quit
```

在接口 GigabitEthernet 0/0 下应用 IPsec 安全策略。

```
[RouterB] interface gigabitethernet 0/0
[RouterB-GigabitEthernet0/0] ip address 202.115.11.2 24
[RouterB-GigabitEthernet0/0] ipsec policy l2tp
[RouterB-GigabitEthernet0/0] quit
```

3.3.3 Router C的配置

配置接口 GigabitEthernet0/1 的 IP 地址。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 0/1
[RouterC-GigabitEthernet0/1] ip address 172.32.15.10 24
[RouterC-GigabitEthernet0/1] quit
```

使能 L2TP。

```
[RouterC] l2tp enable
```

配置虚模板 Virtual-Template 的相关信息。

```
[RouterC] interface virtual-template0
[RouterC-virtual-template0] ip address 10.1.1.1 255.255.255.0
[RouterC-virtual-template0] ppp authentication-mode chap
[RouterC-virtual-template0] remote address pool 1
[RouterC-virtual-template0] quit
```

配置 l2tp-group。

```
[RouterC] l2tp-group 1
[RouterC-l2tp1] allow l2tp virtual-template 0 remote msr_lac domain l2tp
[RouterC-l2tp1] tunnel password simple msr_l2tp
[RouterC-l2tp1] tunnel name msr_lns
[RouterC-l2tp1] quit
```

配置 radius 方案。

```
[RouterC] radius scheme l2tp
[RouterC-radius-l2tp] primary authentication 172.32.0.16
[RouterC-radius-l2tp] primary accounting 172.32.0.16
[RouterC-radius-l2tp] key authentication msr
```

```
[RouterC-radius-l2tp] key accounting msr
[RouterC-radius-l2tp] quit
```
配置域。
```
[RouterC] domain l2tp
[RouterC-isp-l2tp] authentication ppp radius-scheme l2tp
[RouterC-isp-l2tp] authorization ppp radius-scheme l2tp
[RouterC-isp-l2tp] accounting ppp radius-scheme l2tp
[RouterC-isp-l2tp] ip pool 1 10.1.1.2 10.1.1.100
[RouterC-isp-l2tp] quit
```
创建 ACL3000,定义需要 IPsec 保护的数据流。
```
[RouterC] acl number 3000
[RouterC-acl-adv-3000] rule 0 permit udp source 202.115.11.1 0 source-port eq 1701
destination 202.115.11.2 0
[RouterC-acl-adv-3000] quit
```
配置 ike 对等体。
```
[RouterC] ike peer l2tp
[RouterC-ike-peer-l2tp] pre-shared-key l2tp
[RouterC-ike-peer-l2tp] remote-address 202.115.11.2
[RouterC-ike-peer-l2tp] quit
```
配置 IPsec proposal。
```
[RouterC] ipsec proposal l2tp
[RouterC-ipsec-proposal-l2tp] transform ah-esp
[RouterC-ipsec-proposal-l2tp] quit
```
配置 IPsec policy。
```
[RouterC] ipsec policy l2tp 1 isakmp
[RouterC-ipsec-policy-isakmp-l2tp-1] security acl 3000
[RouterC-ipsec-policy-isakmp-l2tp-1] ike-peer l2tp
[RouterC-ipsec-policy-isakmp-l2tp-1] proposal l2tp
[RouterC] quit
```
在接口 GigabitEthernet0/0 下应用 IPsec 安全策略。
```
[RouterC] interface gigabitethernet 0/0
[RouterC-GigabitEthernet0/0] ip address 202.115.11.2 24
[RouterC-GigabitEthernet0/0] ipsec policy l2tp
[RouterC-GigabitEthernet0/0] quit
```

3.4 验证配置

(1) 流量触发 PPPoE 拨号：

发送 172.31.0.0 到 172.32.0.0 网段的数据流，在 Router A 上触发 PPPoE 拨号，dialer 接口 UP，LNS 为其分配 10.1.1.0 网段地址。

```
[RouterA]
%Sep 23 20:02:47:78 2013 RouterAIFNET/4/UPDOWN:
 Line protocol on the interface Dialer0:0 is UP
%Sep 23 20:02:47:132 2013 RouterAIFNET/4/UPDOWN:
 Protocol PPP IPCP on the interface Dialer0:0 is UP
```

```
[RouterA]display interface dialer 0
Dialer0 current state: UP
Line protocol current state: UP (spoofing)
Description: Dialer0 Interface
The Maximum Transmit Unit is 1492, Hold timer is 10(sec)
Internet Address is negotiated, 10.1.1.5/32
Link layer protocol is PPP
LCP initial
Physical is Dialer, baudrate: 64000 bps
Output queue : (Urgent queuing : Length)  50
Output queue : (Protocol queuing : Length)  500
Output queue : (FIFO queuing : Length)  75
  Last clearing of counters:  Never
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  20 bytes/sec 0 packets/sec
    5 packets input, 280 bytes, 0 drops
    197 packets output, 9442 bytes, 0 drops
Bound to : Dialer0:0
Dialer0:0 current state: UP
Line protocol current state: UP
Link layer protocol is PPP
LCP opened, IPCP opened, OSICP opened
Physical is PPPOE, baudrate: 64000 bps
    Last 300 seconds input:  1 bytes/sec 0 packets/sec
    Last 300 seconds output:  22 bytes/sec 0 packets/sec
    45 packets input, 495 bytes, 0 drops
    230 packets output, 9411 bytes, 0 drops
```

(2) L2TP tunnel 和 L2TP session 建立：

LAC 和 LNS 上可以看到 L2TP tunnel 和 L2TP session 的建立情况。

```
<RouterB> display l2tp tunnel
 Total tunnel = 1

 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         202.115.11.1     1701   1        msr_lns
< RouterB>display l2tp session
 Total session = 1

 LocalSID  RemoteSID  LocalTID
  790       30851      1

[RouterC]display l2tp tunnel
 Total tunnel = 1

 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         202.115.11.2     1701   1        msr_lac
[RouterC]display l2tp session
 Total session = 1
```

```
 LocalSID  RemoteSID  LocalTID
  30851     790        1
```

(3) IKE SA 建立：

LAC 和 LNS 上可以看到 IKE SA 的建立情况。

```
<RouterB> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ------------------------------------------------------------
        5          202.115.11.1    RD|ST         2     IPSEC
        4          202.115.11.1    RD|ST         1     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO—TIMEOUT

[RouterC] display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ------------------------------------------------------------
        5          202.115.11.2    RD            2     IPSEC
        4          202.115.11.2    RD            1     IPSEC

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

(4) LNS 上的直联路由：

LNS 上可以看到与 Router A 的直联路由。

```
[RouterC] display ip routing-table
Routing Tables: Public
         Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

10.1.1.0/24         Direct 0    0            10.1.1.1        VT0
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.1.1.5/32         Direct 0    0            10.1.1.5        VT0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
172.32.0.0/16       Direct 0    0            172.32.15.10    GE0/0
172.32.15.10/32     Direct 0    0            127.0.0.1       InLoop0
202.115.11.0/24     Direct 0    0            202.115.11.1    GE0/1
202.115.11.1/32     Direct 0    0            127.0.0.1       InLoop0
202.115.22.0/24     OSPF   10   2            202.115.11.2    GE0/1
```

(5) 私网网段互访：

172.31.0.0 网段主机可以访问 172.32.0.0 网段资源。

3.5 配置文件

- Router A：

```
#
acl number 3000
 rule 0 permit ip
#
interface Dialer0
 nat outbound 3000
 link-protocol ppp
 ppp chap user l2tp@l2tp
 ppp chap password simple l2tp
 ip address ppp-negotiate
 dialer user PPPoE
 dialer-group 1
 dialer bundle 1
#
interface Ethernet0/0
 port link-mode route
 PPPoE-client dial-bundle-number 1 idle-timeout 300
#
 ip route-static 0.0.0.0 0.0.0.0 Dialer0
#
```

- Router B：

```
#
l2tp enable
#
domain l2tp
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
ike peer l2tp
 pre-shared-key l2tp
 remote-address 202.115.11.1
#
ipsec proposal l2tp
 transform ah-esp
 undo esp authentication-algorithm
#
ipsec policy l2tp 1 isakmp
 security acl 3000
 ike-peer l2tp
 proposal l2tp
#
local-user l2tp
```

```
 service-type ppp
#
acl number 3000
 rule 0 permit udp source 202.115.11.2 0 destination 202.115.11.1 0 destination-port eq 1701
#
l2tp-group 1
 tunnel password simple msr_l2tp
 tunnel name msr_lac
 start l2tp ip 202.115.11.1 fullusername l2tp@l2tp
interface GigabitEthernet0/0
 port link-mode route
 ip address 202.115.11.2 255.255.255.0
 IPsec policy l2tp
```

- Router C：

```
#
 l2tp enable
#
radius scheme l2tp
 primary authentication 172.32.0.16
 primary accounting 172.32.0.16
 key authentication msr
 key accounting msr
#
domain l2tp
 authentication ppp radius-scheme l2tp
 authorization ppp radius-scheme l2tp
 accounting ppp radius-scheme l2tp
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 1 10.1.1.2 10.1.1.100
 accounting optional
#
ike peer l2tp
 pre-shared-key l2tp
 remote-address 202.115.11.2
#
ipsec proposal l2tp
 transform ah-esp
 undo esp authentication-algorithm
#
ipsec policy l2tp 1 isakmp
 security acl 3000
 ike-peer l2tp
 proposal l2tp
#
acl number 3000
```

```
 rule 0 permit udp source 202.115.11.1 0 source-port eq 1701 destination 202.115.11.2 0
#
l2tp-group 1
 allow l2tp virtual-template 0 remote msr_lac domain l2tp
 tunnel password simple msr_l2tp
 tunnel name msr_lns
#
interface Virtual-Template0
 ppp authentication-mode chap
 remote address pool 1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 202.115.11.1 255.255.255.0
 IPsec policy l2tp
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 172.32.15.10 255.255.0.0
#
```

4 相关资料

- H3C MSR 系列路由器 命令参考(V5)-R2311
- H3C MSR 系列路由器 配置指导(V5)-R2311