# L2TP over IPsec 私网用户同网段案例

IPSec VPN L2TP VPN 程咪 2019-10-30 发表

## 问题描述

L2TP over IPsec 私网用户同网段案例

## 解决方法

**一、 组网需求：**

客户client端网段与LNS内网同网段，现客户想要通过L2TP over IPsec实现访问内部的telnet资源。

**二、 组网图**


**三. 典型配置：**

**LNS侧配置：**

```
#
 version 5.20, Release 5142P03
#
 sysname H3C
#
 l2tp enable   //使能L2TP
#
 ike local-name lns   //配置本端IKE对等体名字
#
 interzone policy default by-priority
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
session synchronization enable
#
 password-recovery enable
#
acl number 3010
rule 5 permit ip
#
vlan 1
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 1 192.168.10.2 192.168.10.10   //配置L2TP地址池
#
pki domain default
  crl check disable
#
ike peer pc   //配置ike对等体
```

```
 exchange-mode aggressive
 pre-shared-key cipher simple
 id-type name
 remote-name pc
 nat traversal
#
ipsec transform-set 1    //配置ipsec安全提议
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm sha1
 esp encryption-algorithm des
#
ipsec policy-template temp1 1   //配置ipsec策略模板
 security acl 3005
 ike-peer pc
 transform-set 1
 sa duration traffic-based 1843200
 sa duration time-based 3600
#
ipsec policy pc 1 isakmp template temp1   //配置ipsec策略
#
acl number 3005   //配置本地策略路由，将匹配L2TP的报文，重定向到公网接口
 rule 0 permit udp source-port eq 1701
#
policy-based-route aaa permit node 5
if-match acl 3005
 apply output-interface GigabitEthernet0/2
#
ip local policy-based-route aaa
#
user-group system
 group-attribute allow-guest
#
local-user 3210   //配置L2TP用户
 password cipher 3210
 service-type ppp
#
cwmp
 undo cwmp enable
#
l2tp-group 1     //配置L2TP组
 undo tunnel authentication
 allow l2tp virtual-template 1
#
interface Virtual-Template1   //配置VT接口，将内网的telnet服务器映射到VT虚接口
 ppp authentication-mode chap
 remote address pool 1
 ip address 192.168.10.1 255.255.255.0
 nat server 1 protocol tcp global current-interface 2323 inside 192.168.202.55 telnet
#
interface NULL0
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/1
 port link-mode rout
 ip address 192.168.202.11 255.255.255.0  //与服务器互联
#
interface GigabitEthernet0/2
 port link-mode route
 nat outbound 3010
 ip address 11.1.1.1 255.255.255.0
```

```
 ipsec policy pc       //公网接口绑定ipsec策略
#
interface GigabitEthernet0/3
 port link-mode route
#
interface GigabitEthernet0/4
 port link-mode route
#
vd Root id 1
#
zone name Trust id 2   //测试方便起见，将所有接口加入trust安全域
 priority 85
 import interface GigabitEthernet0/1
 import interface GigabitEthernet0/2
 import interface Virtual-Template1
#
```

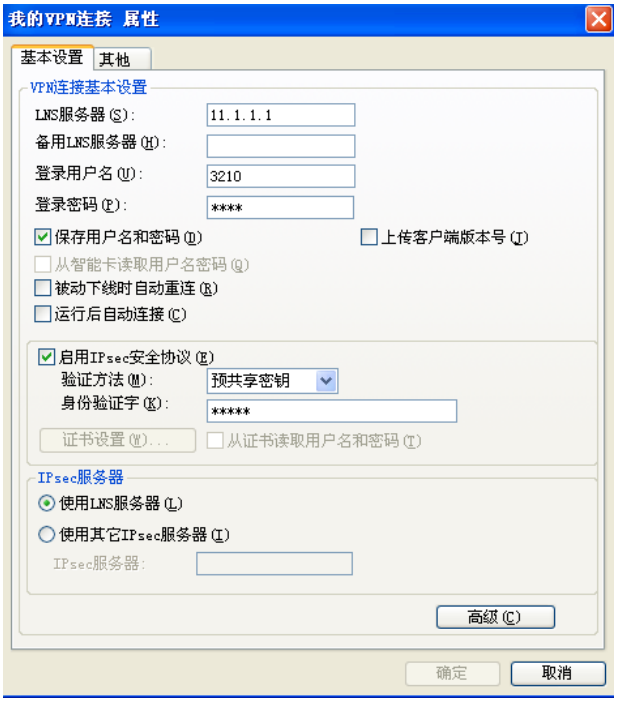
**TELNET服务器配置：**

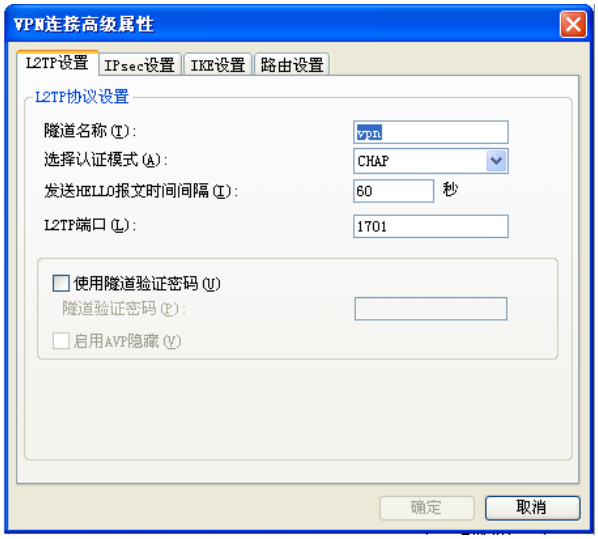
```
#
 telnet server enable
#
local-user admin
 password cipher .]@USE=B,53Q=^Q`MAF4<1!!
 authorization-attribute level 3
 service-type telnet
#
interface GigabitEthernet0/2
 port link-mode route
ip address 192.168.202.55 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.202.11
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
#
```

**Client网卡信息：**

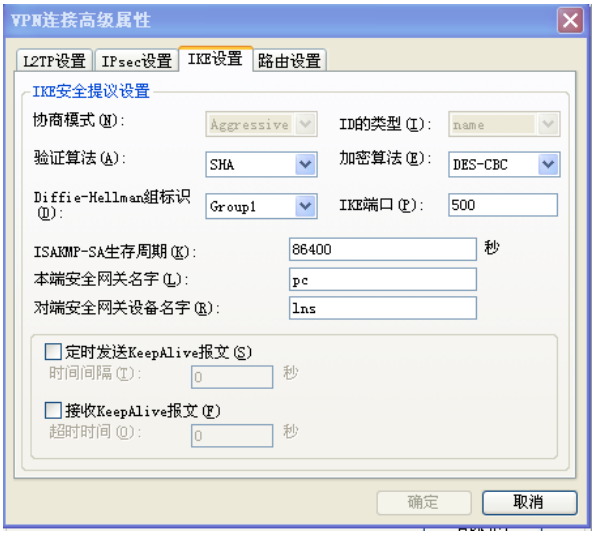
```
Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . : localdomain
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter

        Physical Address. . . . . . . . . : 00-0C-29-CE-54-90
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.202.128
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.202.2
        DHCP Server . . . . . . . . . . . : 192.168.202.254
        DNS Servers . . . . . . . . . . . : 192.168.202.2
        Primary WINS Server . . . . . . . : 192.168.202.2
        Lease Obtained. . . . . . . . . . : 2015年5月21日 19:59:20
        Lease Expires . . . . . . . . . . : 2015年5月21日 20:29:20
```

**Client配置：**


我的VPN连接 属性
基本设置
其他
VPN连接基本设置
LNS服务器(S):
11.1.1.1
备用LNS服务器(H):
登录用户名(U):
3210
登录密码(P):
****
保存用户名和密码(D)
上传客户端版本号(I)
从智能卡读取用户名密码(Q)
被动下线时自动重连(R)
运行后自动连接(C)
启用IPsec安全协议(E)
验证方法(M):
预共享密钥
身份验证字(K):
*****
证书设置(W)...
从证书读取用户名和密码(T)
IPsec服务器
使用LNS服务器(L)
使用其它IPsec服务器(I)
IPsec服务器:
高级(C)
确定
取消


VPN连接高级属性
L2TP设置
IPsec设置
IKE设置
路由设置
L2TP协议设置
隧道名称(T):
vpn
选择认证模式(A):
CHAP
发送HELLO报文时间间隔(I):
60
秒
L2TP端口(L):
1701
使用隧道验证密码(U)
隧道验证密码(P):
启用AVP隐藏(Y)
确定
取消


VPN连接高级属性
L2TP设置
IPsec设置
IKE设置
路由设置
IPsec安全提议设置
封装模式(E):
Tunnel
安全联盟生存周期(S):
3600
秒
采用的安全协议(U):
ESP
ESP协议验证算法(A):
SHA
ESP协议加密算法(T):
DES
AH协议验证算法(H):
使用PFS特性(F)
PFS特性
使用NAT穿越(N)
确定
取消




**四、测试结果：**

1、不增加本地策略路由，INode无法正常拨号，此时，可以看到LNS侧ipsec正常建立：


```
[H3C]dis ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi
  ----------------------------------------------------------------
       5           11.1.1.10               RD          1       IPSEC
       6           11.1.1.10               RD          2       IPSEC

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

2、增加本地策略路由后，可以正常拨号，但是业务无法正常互通：

```
[H3C]ip local policy-based-route aaa
[H3C]dis ip policy-based-route
 policy Name             interface
 aaa                     local
[H3C]dis policy-based-route aaa
 Policy based routing configuration information:
 policy-based-route : aaa
    Node 5 permit :
       if-match acl 3005
       apply output-interface GigabitEthernet0/2
```


```
Ethernet adapter 本地连接 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : iNode VPN Virtual NIC
        Physical Address. . . . . . . . . : 02-50-F2-00-00-02
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.10.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 192.168.10.3
        DHCP Server . . . . . . . . . . . : 192.168.10.1
        Lease Obtained. . . . . . . . . . : 2015年5月21日 20:19:50
        Lease Expires . . . . . . . . . . : 2015年5月24日 20:19:50

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . : localdomain
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter

        Physical Address. . . . . . . . . : 00-0C-29-CE-54-90
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.202.128
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.202.2
        DHCP Server . . . . . . . . . . . : 192.168.202.254
        DNS Servers . . . . . . . . . . . : 192.168.202.2
        Primary WINS Server . . . . . . . : 192.168.202.2
        Lease Obtained. . . . . . . . . . : 2015年5月21日 20:14:20
        Lease Expires . . . . . . . . . . : 2015年5月21日 20:44:20
```

```
C:\Documents and Settings\Administrator>telnet 192.168.202.55
正在连接到192.168.202.55...不能打开到主机的连接， 在端口 23: 连接失败

C:\Documents and Settings\Administrator>ping 192.168.202.55

Pinging 192.168.202.55 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.202.55:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>
```

3、为解决Client访问服务器，可以再VT虚接口上增加相应服务的映射。

```
C:\Documents and Settings\Administrator>telnet 192.168.202.55
正在连接到192.168.202.55...不能打开到主机的连接， 在端口 23: 连接失败

C:\Documents and Settings\Administrator>ping 192.168.202.55

Pinging 192.168.202.55 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.202.55:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>
```

```
C:\Documents and Settings\Administrator>telnet 192.168.10.1 2323
```

```
******************************************************************************
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


Login authentication


Username:admin
Password:
<H3C>dis ip int brief
*down: administratively down
(s): spoofing
Interface                  Physical Protocol IP Address      Description
GigabitEthernet0/0         down     down     192.168.0.1     GigabitEt...
GigabitEthernet0/1         down     down     180.168.118.78  GigabitEt...
GigabitEthernet0/2         up       up       192.168.202.55  GigabitEt...
GigabitEthernet0/3         down     down     unassigned      GigabitEt...
GigabitEthernet0/4         down     down     unassigned      GigabitEt...
Virtual-Template0          up       up(s)    192.168.20.1    Virtual-T...
<H3C>
```