L2TP over IPSEC 穿越NAT配置案例

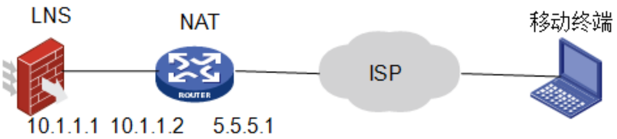
IPSec VPN　L2TP VPN　**程咪**　2019-10-30 发表

问题描述

L2TP over IPSEC 穿越NAT配置案例

解决方法

一、　　组网：



二、　　需求：

某公司总部采用UTM部署了L2TP VPN，采用IPSec对数据进行加密，该设备位于NAT设备后，员工使用iNode进行拨入，拨入后获得的地址范围是192.168.10.2—192.168.10.10。

三、　　配置：

LNS：

```
<H3C>dis cu
#
 version 5.20, Release 5142P03
#
 sysname H3C
#
 l2tp enable   //使能l2tp
#
 undo voice vlan mac-address 00e0-bb00-0000
#
 ike local-name lns   、、制定本端ike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 3005       //配置ipsec感兴趣流量
 rule 0 permit udp source-port eq 1701
#
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分配的地址池
#
pki domain default
```

```
 crl check disable
#
ike peer pc      、、配置ike对等体，使用野蛮模式，开启nat穿越
 exchange-mode aggressive
 pre-shared-key cipher admin
 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
#
user-group system
 group-attribute allow-guest
#
cwmp
 undo cwmp enable
#
l2tp-group 1    //配置l2tp group组
 undo tunnel authentication
 allow l2tp virtual-template 1
#
interface Virtual-Template1    //配置虚接口
 ppp authentication-mode chap
 remote address pool 1
 ip address 192.168.10.1 255.255.255.0
#
interface NULL0
#
interface GigabitEthernet0/0
 port link-mode route
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 ipsec policy pc        //在与nat互联借口上使能ipsec策略
#
interface GigabitEthernet0/2
 port link-mode route
#
interface GigabitEthernet0/3
 port link-mode route
#
interface GigabitEthernet0/4
 port link-mode route
#
vd Root id 1
#
zone name Management id 0
 priority 100
 import interface GigabitEthernet0/0
zone name Local id 1
```

```
 priority 100
zone name Trust id 2
 priority 85
 import interface GigabitEthernet0/1
 import interface GigabitEthernet0/2
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
#
```

NAT设备：

```
#
 version 5.20, Release 5142P02
#
session synchronization enable
#
 password-recovery enable
#
vlan 1
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
pki entity sun
  common-name U200-S
#
pki domain ca-server
  certificate request from ca
  certificate request entity sun
  crl check disable
#
pki domain default
  crl check disable
#
dhcp server ip-pool 1
 network 5.5.5.0 mask 255.255.255.0
 gateway-list 5.5.5.1
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher $c$3$hYJiDtWJEmaHNhFUEekJKVdFCEGvKs02
 authorization-attribute level 3
 service-type telnet
 service-type web
#
cwmp
 undo cwmp enable

#
interface GigabitEthernet0/0
 port link-mode route
#
interface GigabitEthernet0/1
 port link-mode route
#
interface GigabitEthernet0/2
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
#
```

```
interface GigabitEthernet0/3
 port link-mode route
 nat outbound     //公网借口使能nat，并映射udp 1701、500、4500
 nat server 1 protocol udp global current-interface 1701 inside 10.1.1.1 1701
 nat server 2 protocol udp global current-interface 500 inside 10.1.1.1 500
 nat server 3 protocol udp global current-interface 4500 inside 10.1.1.1 4500
 ip address 5.5.5.1 255.255.255.0
#
interface GigabitEthernet0/4
 port link-mode route
#
vd Root id 1
#
zone name Management id 0
 priority 100
 import interface GigabitEthernet0/0
zone name Local id 1
 priority 100
zone name Trust id 2
 priority 85
 import interface GigabitEthernet0/1
 import interface GigabitEthernet0/2
 import interface GigabitEthernet0/3
 import interface GigabitEthernet0/4
 import interface Vlan-interface1
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
```

INODE客户端配置截图：

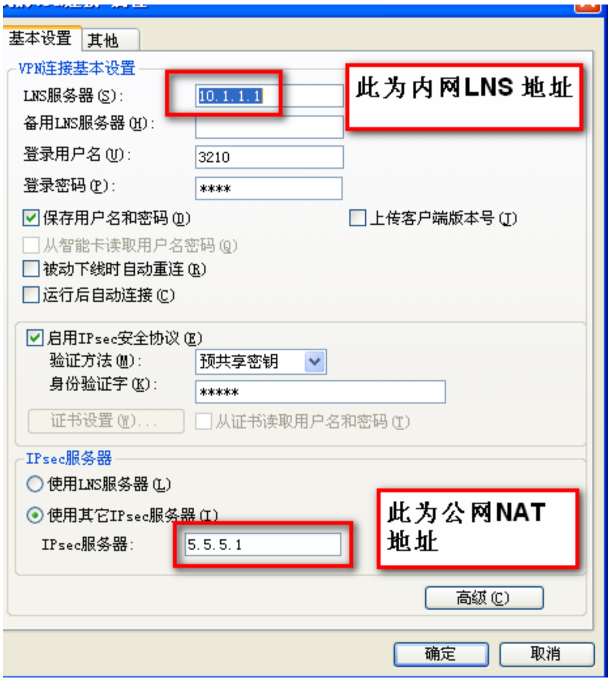
1、基本配置

此处LNS服务器地址对应LNS外网口地址：

```
interface GigabitEthernet0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
```

IPsec服务器地址对应NAT设备公网口地址：

```
interface GigabitEthernet0/3
 port link-mode route
ip address 5.5.5.1 255.255.255.0
```



基本设置 其他

VPN连接基本设置

LNS服务器(S): 10.1.1.1

此为内网LNS 地址

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(T)

□ 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(I)

IPsec服务器

○ 使用LNS服务器(L)

● 使用其它IPsec服务器(I)

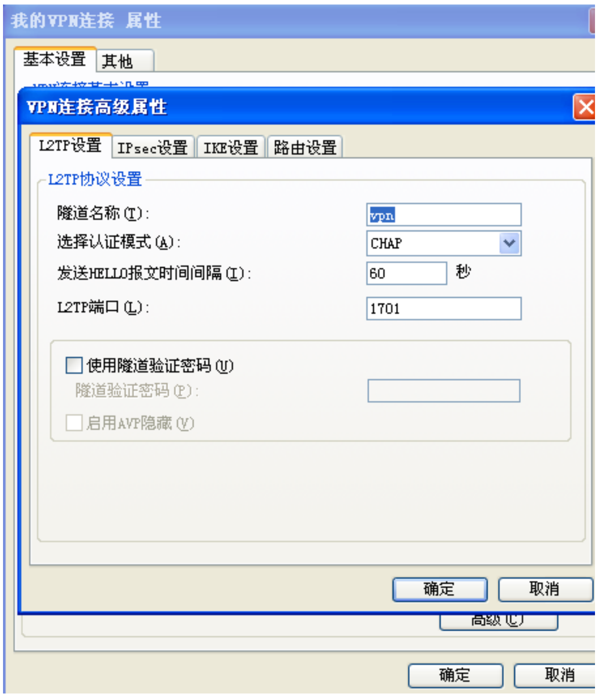
IPsec服务器: 5.5.5.1

此为公网NAT 地址

高级(C)

确定 取消

2、l2tp配置



我的VPN连接 属性

基本设置 其他

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(V)

确定 取消

高级(C)

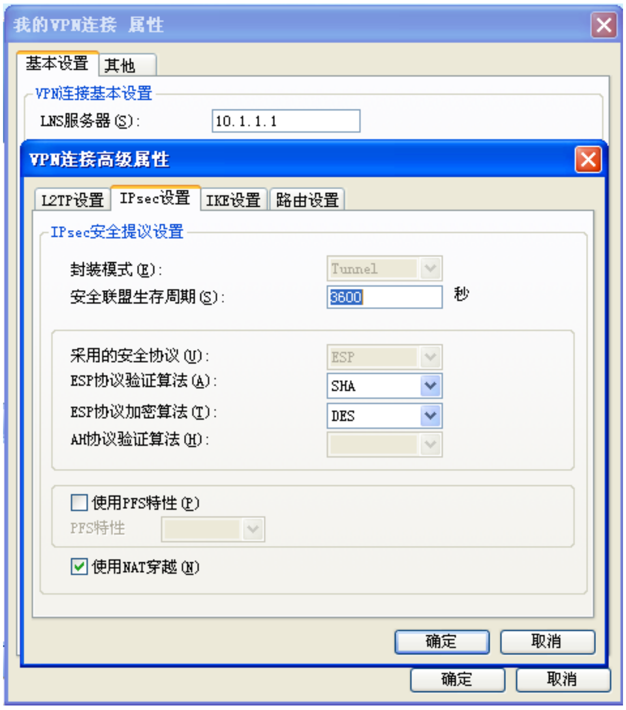
确定 取消

3、IPsec配置:

此处对应LNS设备:

```
<H3C>dis ipsec tran 1

 IPsec transform-set name: 1
   encapsulation mode: tunnel
   ESN : disable
   ESN scheme: NO
   transform: esp-new
   ESP protocol:
     Integrity: sha1-hmac-96
     Encryption: des
```



VPN连接基本设置

LNS服务器(S): 10.1.1.1

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(P)

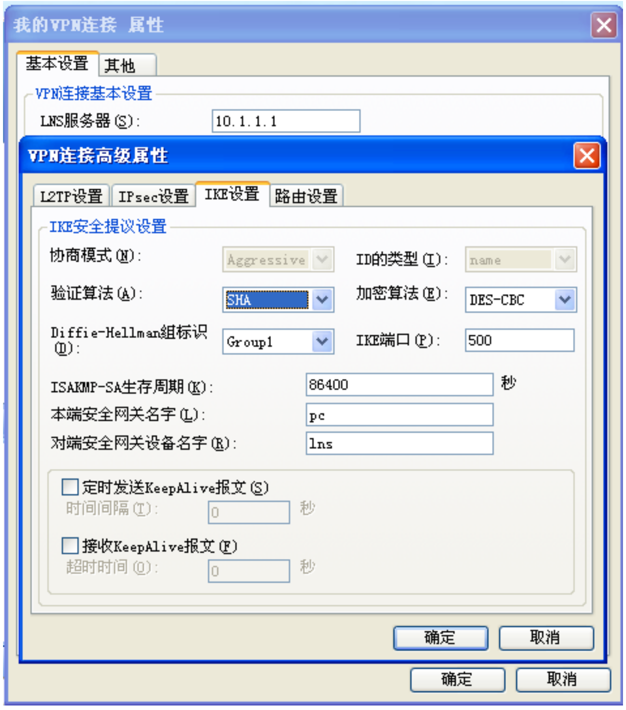
PFS特性

☑ 使用NAT穿越(N)

4、IKE配置：

此处对应LNS：

```
<H3C>dis ike proposal
 priority authentication authentication encryption Diffie-Hellman duration
 method      algorithm   algorithm     group       (seconds)
---------------------------------------------------------------------------
default  PRE_SHARED     SHA        DES_CBC       MODP_768       86400
```



VPN连接基本设置

LNS服务器(S): 10.1.1.1

IKE安全提议设置

协商模式(N): Aggressive

ID的类型(I): name

验证算法(A): SHA

加密算法(E): DES-CBC

Diffie-Hellman组标识(D): Group1

IKE端口(P): 500

ISAKMP-SA生存周期(K): 86400 秒

本端安全网关名字(L): pc

对端安全网关设备名字(R): lns

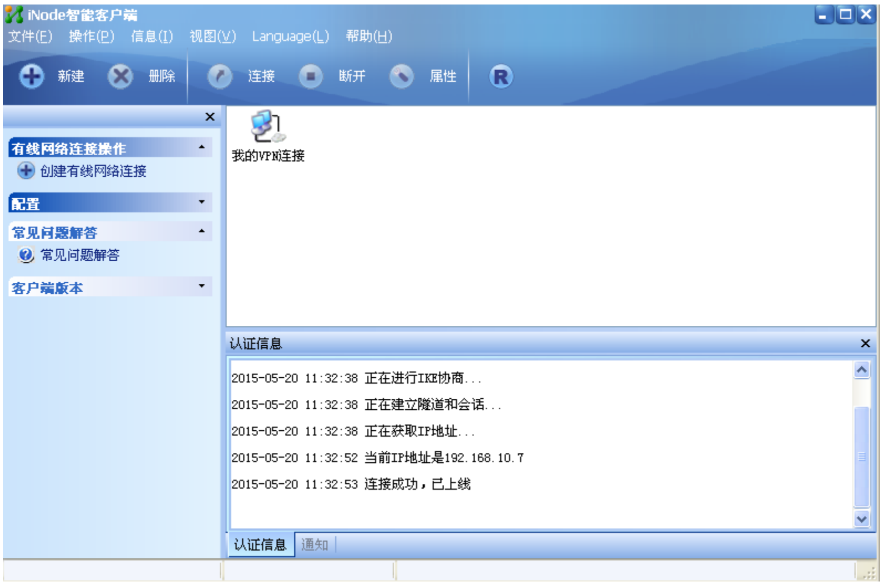
□ 定时发送KeepAlive报文(S)

时间间隔(T): 0 秒

□ 接收KeepAlive报文(F)

超时时间(O): 0 秒

四、 验证：



```
2015-05-20 11:32:38 正在进行IKE协商...
2015-05-20 11:32:38 正在建立隧道和会话...
2015-05-20 11:32:38 正在获取IP地址...
2015-05-20 11:32:52 当前IP地址是192.168.10.7
2015-05-20 11:32:53 连接成功，已上线
```

```
<H3C>dis ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi
  ----------------------------------------------------------------------
     18           5.5.5.2              RD          1       IPSEC
     19           5.5.5.2              RD          2       IPSEC
<H3C>dis ipsec sa
===============================
Interface: GigabitEthernet0/1
    path MTU: 1500
===============================


  -----------------------------
  IPsec policy name: "temp1"
  sequence number: 1
  acl version: ACL4
  mode: template
  -----------------------------
    connection id: 9
    encapsulation mode: tunnel
    perfect forward secrecy:
    tunnel:
        local  address: 10.1.1.1
        remote address: 5.5.5.2
    flow:
        sour addr: 10.1.1.1/255.255.255.255  port: 1701  protocol: UDP
        dest addr: 192.168.202.128/255.255.255.255  port: 0  protocol: UDP

    [inbound ESP SAs]
      spi: 1618176710 (0x60736ac6)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-SHA1
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843197/3448
      max sequence number received: 33
      anti-replay check enable: Y
      anti-replay window size: 32
      udp encapsulation used for nat traversal: Y

    [outbound ESP SAs]
      spi: 1926060403 (0x72cd5973)
      proposal: ESP-ENCRYPT-DES ESP-AUTH-SHA1
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843198/3448
      max sequence number sent: 32
      udp encapsulation used for nat traversal: Y

<H3C>dis l2tp tunnel
 Total tunnel = 1

 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         192.168.202.128  1039   1        vpn
```