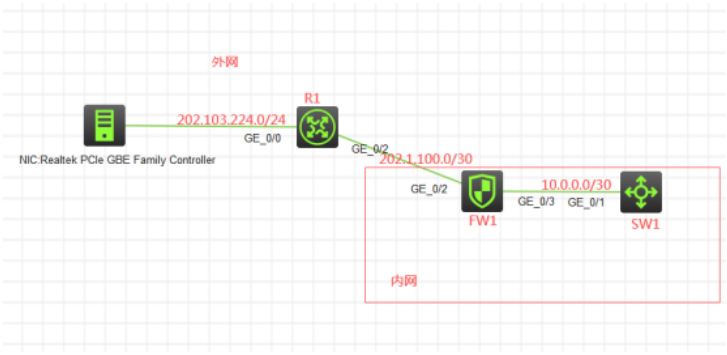
F1060 L2TP VPN 客户LAC模式典型组网配置案例

L2TP VPN H3C模拟器 韦家宁 2020-02-27 发表

组网及说明



组网说明：
本案例采用H3C HCL模拟器的F1060防火墙来实现L2TP VPN客户模式的典型组网。内网和外网在网络拓扑图中已有了明确的标识。FW1为内网的出口设备，提供NAT转换的服务。同时为了能让外网的移动办公终端能访问内网的SW1，需要启用L2TP VPN 客户LAC模式，FW1为LNS端点。

特别说明：
由于模拟器及物理机的局限性，因此采用HCL模拟器的S5820交换机开启WEB功能模拟成为WEB服务器

配置步骤

1、按照网络拓扑图正确配置IP地址
2、SW1开启WEB功能，并创建账户及赋予权限
3、FW1配置NAT，并配置默认路由指向R1
4、FW1开启L2TP VPN服务

配置关键点

SW1：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname SW1
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]port link-mode route
[SW1-GigabitEthernet1/0/1]des <connect to FW1>
[SW1-GigabitEthernet1/0/1]ip address 10.0.0.1 30
[SW1-GigabitEthernet1/0/1]quit
[SW1]ip route-static 0.0.0.0 0.0.0.0 10.0.0.2
[SW1]ip http enable
[SW1]ip https enable
[SW1]local-user admin
New local user added.
[SW1-luser-manage-admin]password simple admin
[SW1-luser-manage-admin]service-type http https
[SW1-luser-manage-admin]authorization-attribute user-role network-admin
[SW1-luser-manage-admin]quit
```

R1：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname R1
[R1]int gi 0/0
[R1-GigabitEthernet0/0]ip address 202.103.224.254 24
[R1-GigabitEthernet0/0]quit
[R1]int gi 0/2
```

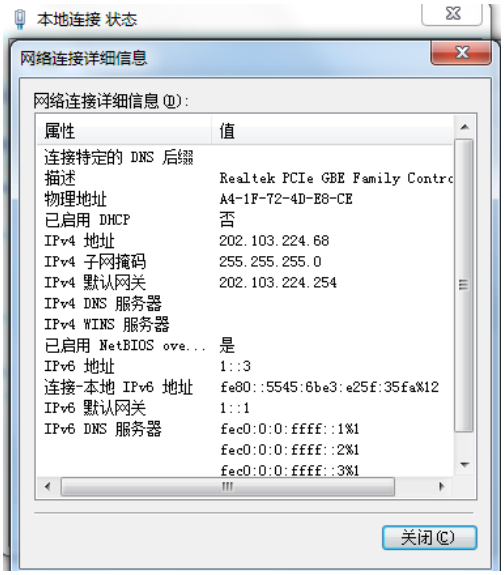
[R1-GigabitEthernet0/2]des <connect to FW1>
[R1-GigabitEthernet0/2]ip address 202.1.100.1 30
[R1-GigabitEthernet0/2]quit

FW1：
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW1
[FW1]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]ip address 10.0.0.2 30
[FW1-GigabitEthernet1/0/3]des <connect to SW1>
[FW1-GigabitEthernet1/0/3]quit
[FW1]acl basic 2000
[FW1-acl-ipv4-basic-2000]rule 0 permit source any
[FW1-acl-ipv4-basic-2000]quit
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]des <connect to R1>
[FW1-GigabitEthernet1/0/2]ip address 202.1.100.2 30
[FW1-GigabitEthernet1/0/2]nat outbound 2000
[FW1-GigabitEthernet1/0/2]quit
[FW1]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1
[FW1]security-zone name trust
[FW1-security-zone-Trust]import interface GigabitEthernet 1/0/3
[FW1-security-zone-Trust]quit
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[FW1-security-zone-Untrust]quit
[FW1]acl basic 2001
[FW1-acl-ipv4-basic-2001]rule 0 permit source any
[FW1-acl-ipv4-basic-2001]quit
[FW1]
[FW1]zone-pair security source trust destination untrust
[FW1-zone-pair-security-Trust-Untrust]packet-filter 2001
[FW1-zone-pair-security-Trust-Untrust]quit
[FW1]
[FW1]zone-pair security source untrust destination trust
[FW1-zone-pair-security-Untrust-Trust]packet-filter 2001
[FW1-zone-pair-security-Untrust-Trust]quit
[FW1]
[FW1]zone-pair security source trust destination local
[FW1-zone-pair-security-Trust-Local]packet-filter 2001
[FW1-zone-pair-security-Trust-Local]quit
[FW1]
[FW1]zone-pair security source local destination trust
[FW1-zone-pair-security-Local-Trust]packet-filter 2001
[FW1-zone-pair-security-Local-Trust]quit
[FW1]
[FW1]zone-pair security source untrust destination local
[FW1-zone-pair-security-Untrust-Local]packet-filter 2001
[FW1-zone-pair-security-Untrust-Local]quit
[FW1]
[FW1]zone-pair security source local destination untrust
[FW1-zone-pair-security-Local-Untrust]packet-filter 2001
[FW1-zone-pair-security-Local-Untrust]quit

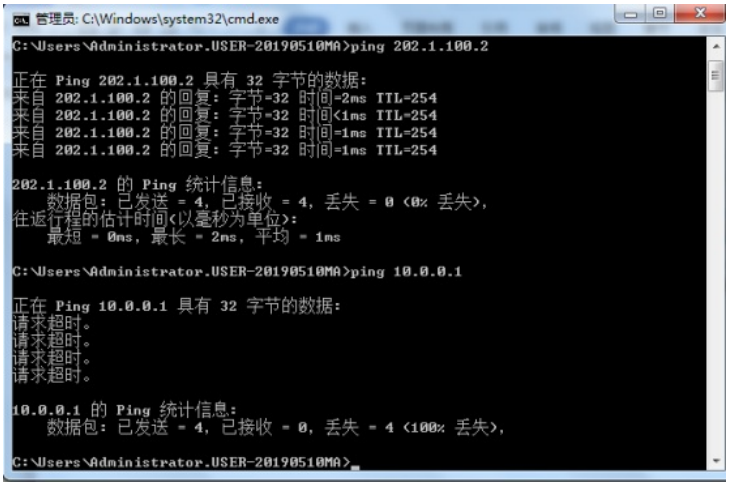
FW1 L2TP VPN LNS关键配置点：
[FW1]local-user weijianing class network
New local user added.
[FW1-luser-network-weijianing]password simple weijianing
[FW1-luser-network-weijianing]service-type ppp
[FW1-luser-network-weijianing]quit
[FW1]domain system
[FW1-isp-system]authentication ppp local
[FW1-isp-system]quit

[FW1]ip pool weijianing 172.16.1.2 172.16.1.254
[FW1]ip pool weijianing gateway 172.16.1.1
[FW1]int Virtual-Template 1
[FW1-Virtual-Template1]ip address 172.16.1.1 24
[FW1-Virtual-Template1]ppp authentication-mode chap domain system
[FW1-Virtual-Template1]remote address pool weijianing
[FW1-Virtual-Template1]quit
[FW1]security-zone name Untrust
[FW1-security-zone-Untrust]import interface Virtual-Template 1
[FW1-security-zone-Untrust]quit
[FW1]l2tp enable
[FW1]l2tp-group 1 mode lns
[FW1-l2tp1]undo tunnel authentication
[FW1-l2tp1]tunnel name LNS
[FW1-l2tp1]allow l2tp virtual-template 1
[FW1-l2tp1]quit

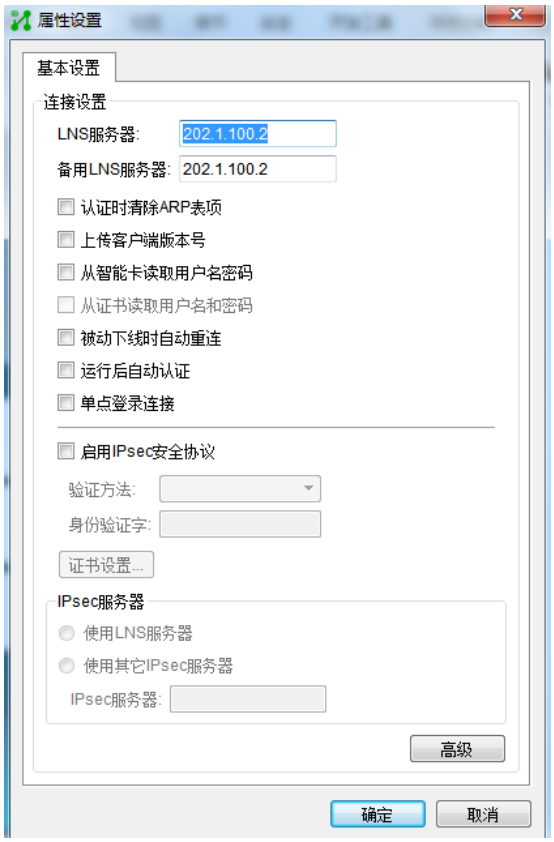
测试：
物理机填写IP地址：



物理机能PING通FW1的外网地址，PING不通私网地址：

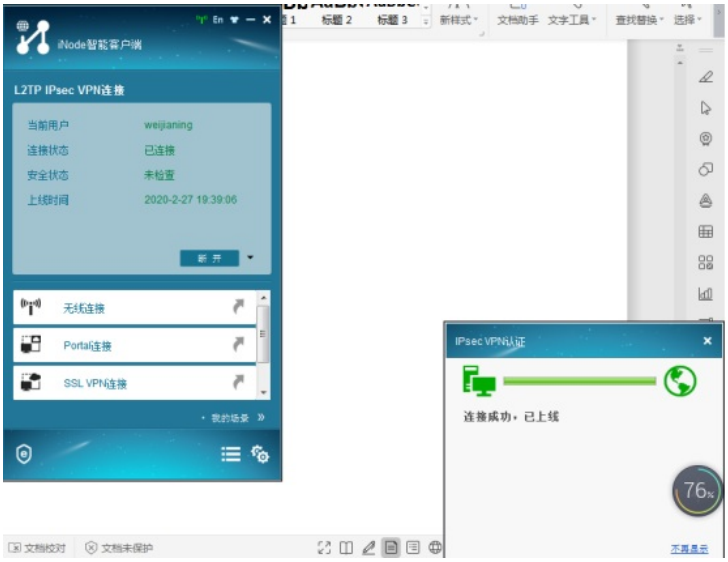


打开iNode智能客户端，点击连接右边的小三角，设置LNS服务器的IP地址：

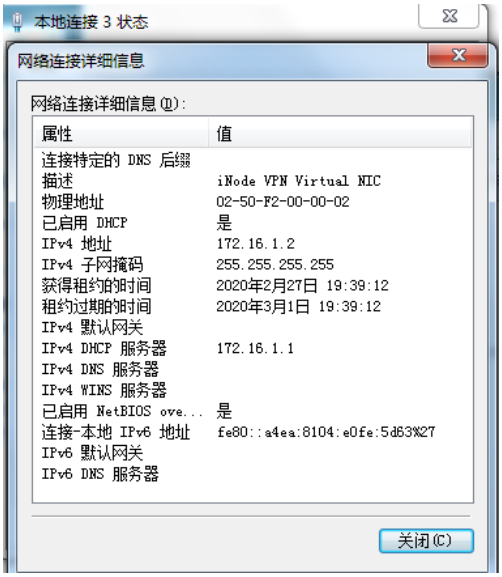


输入用户名、密码，点击连接：

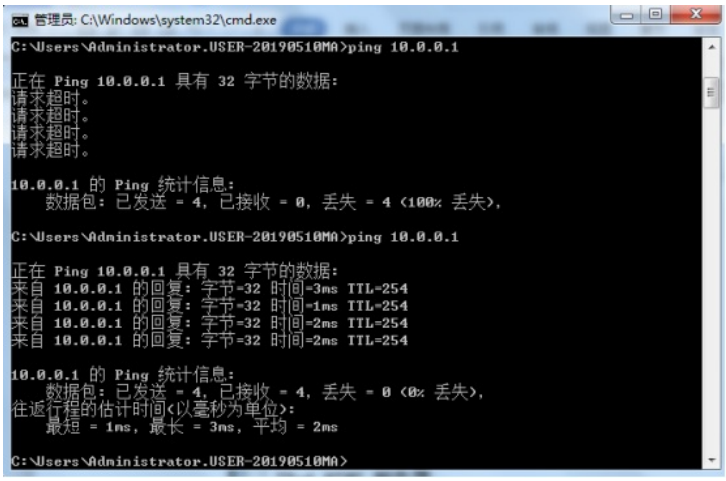
连接成功：



查看获取到的IP地址：



此时物理机已经可以PING通FW1的私网地址：



同时也可以打开SW1的WEB服务：

查看FW1的L2TP显示信息：

```
[FW1]dis l2tp session
LocalSID    RemoteSID    LocalTID    State
10400       11632        17372       Established
[FW1]
```

```
[FW1]dis l2tp tunnel
LocalTID RemoteTID State       Sessions RemoteAddress   RemotePort RemoteName
17372    1         Established 1        202.103.224.68  61796      h3c
[FW1]
```

查看已分配的IP：

```
[FW1]dis ip pool weijianing
Group name: default
  Pool name           Start IP address    End IP address      Free   In use
  weijianing          172.16.1.2          172.16.1.254        252    1
In use IP addresses:
  IP address          Interface
  172.16.1.2          VA0
[FW1]
```

至此，F1060 L2TP VPN 客户LAC模式典型组网配置案例已完成！