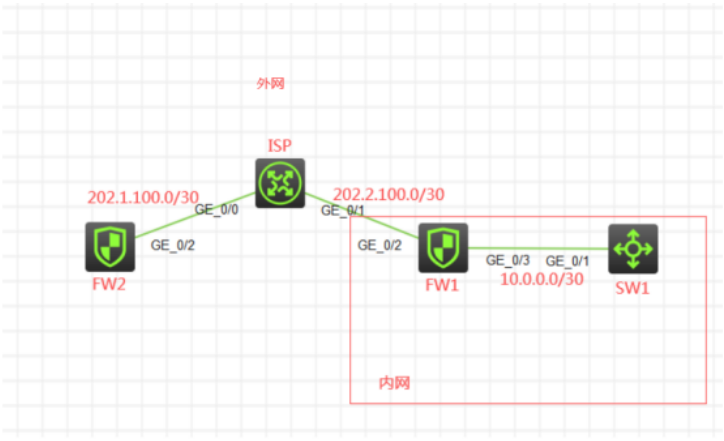
F1060 L2TP VPN 独立LAC典型组网配置案例

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防火墙来模拟L2TP VPN独立LAC模式的典型组网。内网和外网在网络拓扑图中已经有了明确的标识。FW1为内网的出口设备，提供地址转换的服务。FW2为分支的节点设备。要求FW2能与FW1建立L2TP VPN隧道，使得FW2能与内网的SW1互通。FW1为L2TP VPN LNS端点，FW2为L2TP VPN LAC端点。

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，并创建相应账户及赋予权限
3、FW2配置NAT，并配置默认路由指向ISP
4、FW1配置NAT，并配置默认路由指向ISP
5、FW2配置为L2TP VPN LAC端点
6、FW1配置为L2TP VPN LNS端点

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
```

ISP:

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]des <connect to FW2>
[ISP-GigabitEthernet0/0]ip address 202.1.100.1 30
```

```
[ISP-GigabitEthernet0/0]quit
[ISP]int gi 0/1
[ISP-GigabitEthernet0/1]des <connect to FW1>
[ISP-GigabitEthernet0/1]ip address 202.2.100.1 30
[ISP-GigabitEthernet0/1]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 ISP>
[FW1-GigabitEthernet1/0/2]ip address 202.2.100.2 30
[FW1-GigabitEthernet1/0/2]nat outbound 2000
[FW1-GigabitEthernet1/0/2]quit
[FW1]ip route-static 0.0.0.0 0.0.0.0 202.2.100.1
[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]tunnel authentication
[FW1-l2tp1]tunnel name LNS
[FW1-l2tp1]allow l2tp virtual-template 1 remote LAC
[FW1-l2tp1]tunnel password simple weijianing
[FW1-l2tp1]quit
```

FW2：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname FW2
[FW2]acl basic 2000
[FW2-acl-ipv4-basic-2000]rule 0 permit source any
[FW2-acl-ipv4-basic-2000]quit
[FW2]int gi 1/0/2
[FW2-GigabitEthernet1/0/2]des <connect to ISP>
[FW2-GigabitEthernet1/0/2]ip address 202.1.100.2 30
[FW2-GigabitEthernet1/0/2]nat outbound 2000
[FW2-GigabitEthernet1/0/2]quit
[FW2]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1
[FW2]security-zone name Untrust
[FW2-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[FW2-security-zone-Untrust]quit
[FW2]acl basic 2001
[FW2-acl-ipv4-basic-2001]rule 0 permit source any
[FW2-acl-ipv4-basic-2001]quit
[FW2]
[FW2]zone-pair security source trust destination untrust
[FW2-zone-pair-security-Trust-Untrust]packet-filter 2001
[FW2-zone-pair-security-Trust-Untrust]quit
[FW2]
[FW2]zone-pair security source untrust destination trust
[FW2-zone-pair-security-Untrust-Trust]packet-filter 2001
[FW2-zone-pair-security-Untrust-Trust]quit
[FW2]
[FW2]zone-pair security source trust destination local
[FW2-zone-pair-security-Trust-Local]packet-filter 2001
[FW2-zone-pair-security-Trust-Local]quit
[FW2]
[FW2]zone-pair security source local destination trust
[FW2-zone-pair-security-Local-Trust]packet-filter 2001
[FW2-zone-pair-security-Local-Trust]quit
[FW2]
[FW2]zone-pair security source untrust destination local
[FW2-zone-pair-security-Untrust-Local]packet-filter 2001
[FW2-zone-pair-security-Untrust-Local]quit
[FW2]
[FW2]zone-pair security source local destination untrust
[FW2-zone-pair-security-Local-Untrust]packet-filter 2001
[FW2-zone-pair-security-Local-Untrust]quit
```

FW2 L2TP VPN LAC端点配置关键点：

[FW2]local-user weijianing class network
New local user added.
[FW2-luser-network-weijianing]password simple weijianing
[FW2-luser-network-weijianing]service-type ppp
[FW2-luser-network-weijianing]quit
[FW2]l2tp enable
[FW2]l2tp-group 1 mode lac
[FW2-l2tp1]tunnel name LAC
[FW2-l2tp1]tunnel authentication
[FW2-l2tp1]tunnel password simple weijianing
[FW2-l2tp1]user fullusername weijianing
[FW2-l2tp1]source 202.1.100.2
[FW2-l2tp1]lns-ip 202.2.100.2
[FW2-l2tp1]quit
[FW2]int Virtual-PPP 1
[FW2-Virtual-PPP1]ip address ppp-negotiate
[FW2-Virtual-PPP1]ppp chap user weijianing
[FW2-Virtual-PPP1]ppp chap password simple weijianing
[FW2-Virtual-PPP1]l2tp-auto-client l2tp-group 1
[FW2-Virtual-PPP1]quit
[FW2]ip route-static 172.16.1.0 255.255.255.0 Virtual-PPP 1
[FW2]ip route-static 10.0.0.0 255.255.255.0 Virtual-PPP 1
[FW2]security-zone name Untrust
[FW2-security-zone-Untrust]import interface Virtual-PPP 1
[FW2-security-zone-Untrust]quit

测试：
查看FW1的L2TP显示信息：

```
[FW1]dis l2tp session
LocalSID    RemoteSID    LocalTID    State
46659       42567        32730       Established
[FW1]
```

```
[FW1]dis l2tp tunnel
LocalTID RemoteTID State       Sessions RemoteAddress   RemotePort RemoteName
32730    17555     Established 1        202.1.100.2     1701       LAC
[FW1]
```

查看FW1已分配出去的IP地址：

```
[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]
```

查看FW2的L2TP显示信息：

```
[FW2]dis l2tp session
LocalSID    RemoteSID    LocalTID    State
42567       46659        17555       Established
```

```
[FW2]dis l2tp tunnel
LocalTID RemoteTID State       Sessions RemoteAddress   RemotePort RemoteName
17555    32730     Established 1        202.2.100.2     1701       LNS
[FW2]
```

查看FW2获取到的IP地址：

```
[FW2]dis int brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
GE1/0/0              DOWN DOWN     --
GE1/0/1              DOWN DOWN     192.168.0.1
GE1/0/2              UP   UP       202.1.100.2     <connect to ISP>
GE1/0/3              DOWN DOWN     --
GE1/0/4              DOWN DOWN     --
GE1/0/5              DOWN DOWN     --
GE1/0/6              DOWN DOWN     --
GE1/0/7              DOWN DOWN     --
GE1/0/8              DOWN DOWN     --
GE1/0/9              DOWN DOWN     --
GE1/0/10             DOWN DOWN     --
GE1/0/11             DOWN DOWN     --
GE1/0/12             DOWN DOWN     --
GE1/0/13             DOWN DOWN     --
GE1/0/14             DOWN DOWN     --
GE1/0/15             DOWN DOWN     --
GE1/0/16             DOWN DOWN     --
GE1/0/17             DOWN DOWN     --
GE1/0/18             DOWN DOWN     --
GE1/0/19             DOWN DOWN     --
GE1/0/20             DOWN DOWN     --
GE1/0/21             DOWN DOWN     --
GE1/0/22             DOWN DOWN     --
GE1/0/23             DOWN DOWN     --
InLoop0              UP   UP(s)    --
NULL0                UP   UP(s)    --
REG0                 UP   --       --
VPPP1                UP   UP       172.16.1.2

[FW2]
```

在FW2使用获取到的IP地址可以PING通SW1：

```
[FW2]ping -a 172.16.1.2 10.0.0.1
Ping 10.0.0.1 (10.0.0.1) from 172.16.1.2: 56 data bytes, press CTRL_C to break
56 bytes from 10.0.0.1: icmp_seq=0 ttl=254 time=3.000 ms
56 bytes from 10.0.0.1: icmp_seq=1 ttl=254 time=1.000 ms
56 bytes from 10.0.0.1: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 10.0.0.1: icmp_seq=3 ttl=254 time=2.000 ms
56 bytes from 10.0.0.1: icmp_seq=4 ttl=254 time=3.000 ms

--- Ping statistics for 10.0.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.000/3.000/0.894 ms
[FW2]%Feb 27 20:55:28:424 2020 FW2 PING/6/PING_STATISTICS: -Context=1; Ping statistics for 10.0.0.1:
round-trip min/avg/max/std-dev = 1.000/2.000/3.000/0.894 ms.
```

至此，F1060 L2TP VPN独立LAC典型组网配置案例已完成！