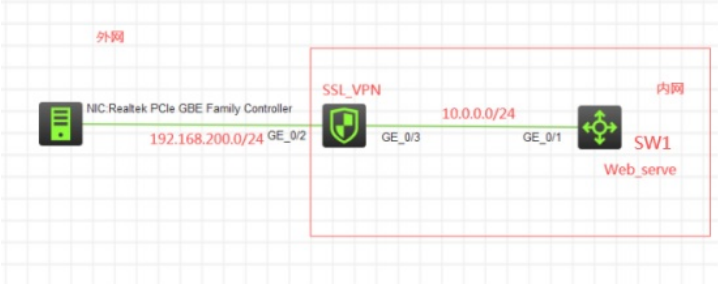
SSL VPN IP接入（缺省证书）单臂（直连）典型组网配置案例

SSL VPN　NAT　设备部署方式　H3C模拟器　韦家宁　2020-02-15 发表

组网及说明



组网说明：

本案例采用H3C HCL模拟器来模拟SSL VPN IP接入（缺省证书）单臂（直连）的组网。内网和外网均已在网络拓扑图中有了明确的说明。本案例使用F1060防火墙作为SSL_VPN网关，用于提供SSL VPN IP的接入，另外也是内网的出口设备。

特别说明：

1、由于模拟器的局限性，因此使用S5820交换机开启WEB功能模拟成为WEB服务器

2、需要自行在官网下载inode管理中心安装，并定制后生成inode客户端后再安装客户端

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，并创建账户赋予权限

3、SSL_VPN开启NAT地址转换功能，并配置默认路由指向外网

4、SSL_VPN配置SSL VPN功能

配置关键点

1、第一阶段调试（基础网络配置）

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 SSL_VPN>
[SW1-GigabitEthernet1/0/1]ip address 10.0.0.1 24
[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
```

SSL_VPN：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname SSL_VPN
[SSL_VPN]int gi 1/0/3
[SSL_VPN-GigabitEthernet1/0/3]des <connect to SW1>
[SSL_VPN-GigabitEthernet1/0/3]ip address 10.0.0.2 24
[SSL_VPN-GigabitEthernet1/0/3]quit
[SSL_VPN]acl basic 2000
[SSL_VPN-acl-ipv4-basic-2000]rule 0 permit source any
[SSL_VPN-acl-ipv4-basic-2000]quit
[SSL_VPN]int gi 1/0/2
[SSL_VPN-GigabitEthernet1/0/2]des <connect to WAN>
```

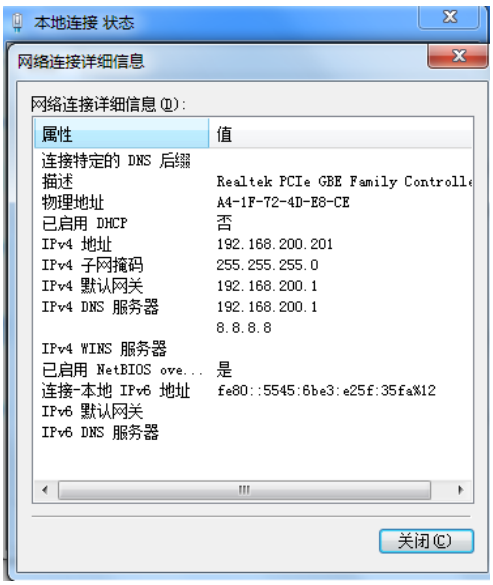
[SSL_VPN-GigabitEthernet1/0/2]ip address 192.168.200.200 24
[SSL_VPN-GigabitEthernet1/0/2]nat outbound 2000
[SSL_VPN-GigabitEthernet1/0/2]quit
[SSL_VPN]ip route-static 0.0.0.0 0.0.0.0 192.168.200.1

[SSL_VPN]security-zone name trust
[SSL_VPN-security-zone-Trust]import interface GigabitEthernet 1/0/3
[SSL_VPN-security-zone-Trust]quit

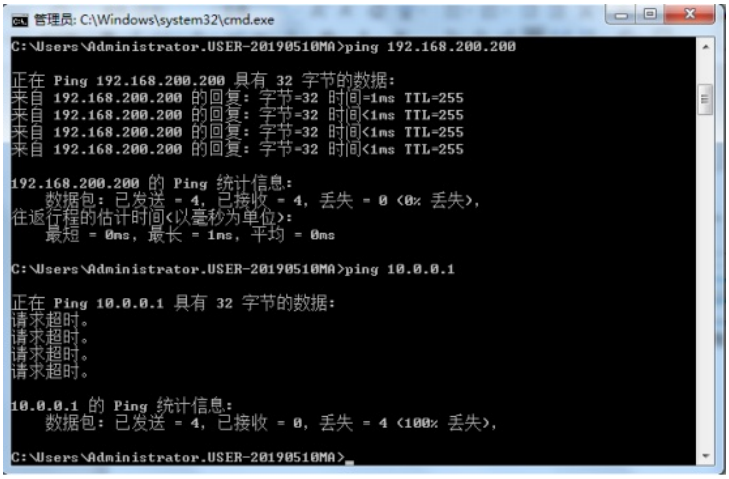
[SSL_VPN]security-zone name Untrust
[SSL_VPN-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[SSL_VPN-security-zone-Untrust]quit

[SSL_VPN]acl basic 2001
[SSL_VPN-acl-ipv4-basic-2001]rule 0 permit source any
[SSL_VPN-acl-ipv4-basic-2001]quit
[SSL_VPN]
[SSL_VPN]zone-pair security source trust destination untrust
[SSL_VPN-zone-pair-security-Trust-Untrust]packet-filter 2001
[SSL_VPN-zone-pair-security-Trust-Untrust]quit
[SSL_VPN]
[SSL_VPN]zone-pair security source untrust destination trust
[SSL_VPN-zone-pair-security-Untrust-Trust]packet-filter 2001
[SSL_VPN-zone-pair-security-Untrust-Trust]quit
[SSL_VPN]
[SSL_VPN]zone-pair security source trust destination local
[SSL_VPN-zone-pair-security-Trust-Local]packet-filter 2001
[SSL_VPN-zone-pair-security-Trust-Local]quit
[SSL_VPN]
[SSL_VPN]zone-pair security source local destination trust
[SSL_VPN-zone-pair-security-Local-Trust]packet-filter 2001
[SSL_VPN-zone-pair-security-Local-Trust]quit
[SSL_VPN]
[SSL_VPN]zone-pair security source untrust destination local
[SSL_VPN-zone-pair-security-Untrust-Local]packet-filter 2001
[SSL_VPN-zone-pair-security-Untrust-Local]quit
[SSL_VPN]
[SSL_VPN]zone-pair security source local destination untrust
[SSL_VPN-zone-pair-security-Local-Untrust]packet-filter 2001
[SSL_VPN-zone-pair-security-Local-Untrust]quit
[SSL_VPN]

第一阶段测试：
外网终端填写IP地址



外网终端能PING通SSL_VPN的外网地址，PING不到私网地址



2、第二阶段调试（SSL VPN配置）：
SSL VPN IP接入配置关键点：
SSL_VPN：

[SSL_VPN]acl advanced 3000
[SSL_VPN-acl-ipv4-adv-3000]rule 0 permit ip source any
[SSL_VPN-acl-ipv4-adv-3000]quit

[SSL_VPN]sslvpn ip address-pool weijianing 172.16.1.2 172.16.1.254

[SSL_VPN]int SSLVPN-AC 1
[SSL_VPN-SSLVPN-AC1]ip address 172.16.1.1 24
[SSL_VPN-SSLVPN-AC1]quit

[SSL_VPN]sslvpn gateway james
[SSL_VPN-sslvpn-gateway-james]ip address 192.168.200.200
[SSL_VPN-sslvpn-gateway-james]service enable
[SSL_VPN-sslvpn-gateway-james]quit

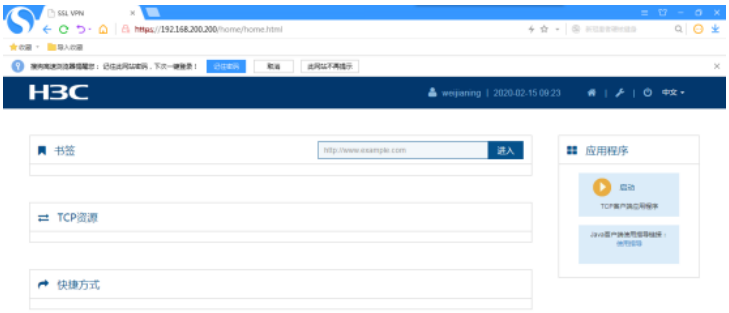
[SSL_VPN]sslvpn context james
[SSL_VPN-sslvpn-context-james]gateway james
[SSL_VPN-sslvpn-context-james]ip-tunnel address-pool weijianing mask 24
[SSL_VPN-sslvpn-context-james]ip-tunnel interface SSLVPN-AC 1
[SSL_VPN-sslvpn-context-james]ip-route-list james
[SSL_VPN-sslvpn-context-james-route-list-james]include 10.0.0.0 24
[SSL_VPN-sslvpn-context-james-route-list-james]quit
[SSL_VPN-sslvpn-context-james]policy-group ip
[SSL_VPN-sslvpn-context-james-policy-group-ip]filter ip-tunnel acl 3000
[SSL_VPN-sslvpn-context-james-policy-group-ip]ip-tunnel access-route ip-route-list james
[SSL_VPN-sslvpn-context-james-policy-group-ip]quit
[SSL_VPN-sslvpn-context-james]service enable
[SSL_VPN-sslvpn-context-james]quit

[SSL_VPN]local-user weijianing class network
New local user added.
[SSL_VPN-luser-network-weijianing]password simple weijianing
[SSL_VPN-luser-network-weijianing]service-type sslvpn
[SSL_VPN-luser-network-weijianing]authorization-attribute sslvpn-policy-group ip
[SSL_VPN-luser-network-weijianing]quit

[SSL_VPN]security-zone name Untrust
[SSL_VPN-security-zone-Untrust]import interface SSLVPN-AC 1
[SSL_VPN-security-zone-Untrust]quit

第二阶段测试：
外网终端打开浏览器，输入网址：https://192.168.200.200

输入用户名、密码，点击“登陆”：



打开inode客户端：

输入网关、用户名、密码，点击“连接”：

SSL VPN建立连接成功

此时外网终端可以PING通内网WEB服务器

```
C:\Users\Administrator.USER-20190510MA>ping 10.0.0.1

正在 Ping 10.0.0.1 具有 32 字节的数据:
来自 10.0.0.1 的回复: 字节=32 时间=10ms TTL=254
来自 10.0.0.1 的回复: 字节=32 时间=2ms TTL=254
来自 10.0.0.1 的回复: 字节=32 时间=3ms TTL=254
来自 10.0.0.1 的回复: 字节=32 时间=2ms TTL=254

10.0.0.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 10ms, 平均 = 4ms

C:\Users\Administrator.USER-20190510MA>
```

同时也可以打开WEB服务器网页：

SSL VPN信息显示：

```
[SSL_VPN]dis sslvpn gateway
Gateway name: james
  Operation state: Up
  IP: 192.168.200.200  Port: 443
  Front VPN instance: Not configured

[SSL_VPN]
```

```
[SSL_VPN]dis sslvpn context
Context name: james
  Operation state: Up
  AAA domain: Not specified
  Certificate authentication: Disabled
  Password authentication: Enabled
  Authentication use: All
  Dynamic password: Disabled
  Code verification: Disabled
  Default policy group: Not configured
  Associated SSL VPN gateway: james
  Maximum users allowed: 1048575
  VPN instance: Not configured
  Idle timeout: 30 min

[SSL_VPN]
```

```
[SSL_VPN]dis sslvpn session
Total users: 2

SSL VPN context: james
Users: 2
Username        Connections  Idle time   Created       User IP
weijianing      0            0/00:07:03  0/00:07:04    192.168.200.201
weijianing      1            0/00:00:14  0/00:06:07    192.168.200.201
[SSL_VPN]
```

```
[SSL_VPN]dis sslvpn ip-tunnel statistics
Context                       : james
User                          : weijianing
Session ID                    : 2
User IPv4 address             : 192.168.200.201
Received requests             : 679
Sent requests                 : 637
Dropped requests              : 42
Received replies              : 821
Sent replies                  : 821
Dropped replies               : 0
Received keepalives           : 13
Sent keepalive replies        : 13
Received configuration updates: 0
Sent configuration updates    : 0

[SSL_VPN]
```

至此，SSL VPN IP接入（缺省证书）单臂（直连）的典型组网配置案例已完成！