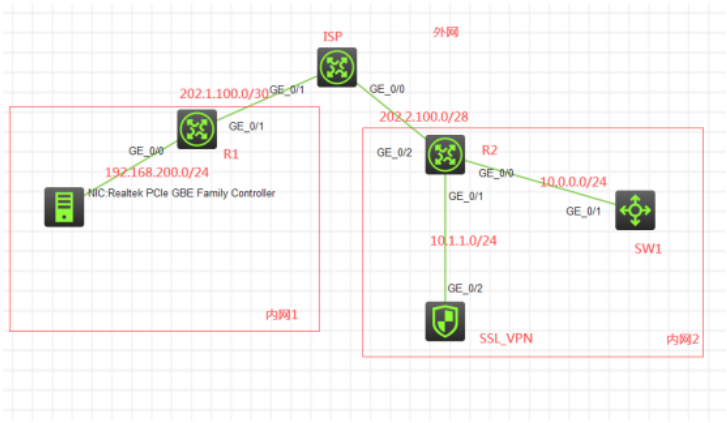
SSL VPN IP接入（缺省证书）双臂（旁路）典型组网配置案例

SSL VPN | 设备部署方式 | NAT | 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）双臂（旁路）典型组网。内网和外网均在网络拓扑图中有了明确的标识。R1和R2分别作为内网1和内网2的出口设备。本案例的SSL VPN网关使用F1060模拟器来实现，SSL VPN网关处在内网2内部的旁路，需要通过R2的NAT server映射发布到外网，内网1的终端通过inode客户端连接到SSL VPN映射出来的网关后，通过SSL VPN的IP分配，来访问内网2的WEB服务器。

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

配置思路：

1、按照网络拓扑图正确配置IP地址

2、R1配置NAT，并配置默认路由指向ISP

3、SW1开启WEB功能，并创建账户及赋予权限，配置默认路由指向R2

4、SSL_VPN配置默认路由指向R2

5、R2配置NAT，并将SSL_VPN发布到外网，配置默认路由指向ISP

6、SSL_VPN开启SSL VPN功能

配置关键点

1、第一阶段调试（基础网络配置）：

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 192.168.200.254 24
[R1-GigabitEthernet0/0]quit
[R1]acl basic 2000
[R1-acl-ipv4-basic-2000]rule 0 permit source any
[R1-acl-ipv4-basic-2000]quit
[R1]int gi 0/1
[R1-GigabitEthernet0/1]des <connect to ISP>
[R1-GigabitEthernet0/1]ip address 202.1.100.2 30
[R1-GigabitEthernet0/1]nat outbound 2000
[R1-GigabitEthernet0/1]quit
[R1]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1
```

ISP：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname ISP
[ISP]int gi 0/1
```

```
[ISP-GigabitEthernet0/1]des <connect to R1>
[ISP-GigabitEthernet0/1]ip address 202.1.100.1 30
[ISP-GigabitEthernet0/1]quit
[ISP]int gi 0/0
[ISP-GigabitEthernet0/0]des <connect to R2>
[ISP-GigabitEthernet0/0]ip address 202.2.100.1 30
[ISP-GigabitEthernet0/0]quit
[ISP]
```

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 R2>
[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
```

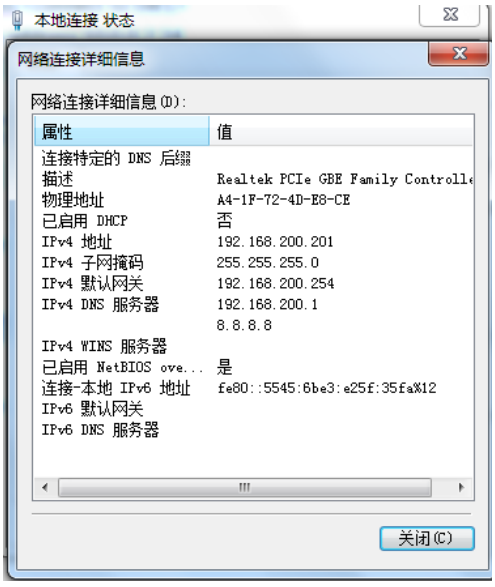
SSL_VPN：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname SSL_VPN
[SSL_VPN]int gi 1/0/2
[SSL_VPN-GigabitEthernet1/0/2]des <connect to R2>
[SSL_VPN-GigabitEthernet1/0/2]ip address 10.1.1.1 24
[SSL_VPN-GigabitEthernet1/0/2]quit
[SSL_VPN]ip route-static 0.0.0.0 0.0.0.0 10.1.1.2

[SSL_VPN]security-zone name Trust
[SSL_VPN-security-zone-Trust]import interface GigabitEthernet 1/0/2
[SSL_VPN-security-zone-Trust]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
```

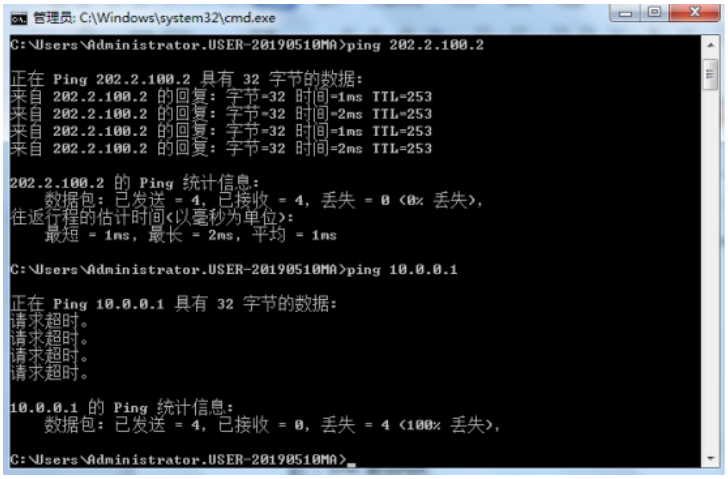
[SSL_VPN-zone-pair-security-Untrust-Local]quit
[SSL_VPN]
[SSL_VPN]zone-pair security source local destination untrust
[SSL_VPN-zone-pair-security-Local-Untrust]packet-filter 2001
[SSL_VPN-zone-pair-security-Local-Untrust]quit

R2：
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname R2
[R2]int gi 0/0
[R2-GigabitEthernet0/0]des <connect to SW1>
[R2-GigabitEthernet0/0]ip address 10.0.0.2 24
[R2-GigabitEthernet0/0]quit
[R2]int gi 0/1
[R2-GigabitEthernet0/1]des <connect to SSL_VPN>
[R2-GigabitEthernet0/1]ip address 10.1.1.2 24
[R2-GigabitEthernet0/1]quit
[R2]acl basic 2000
[R2-acl-ipv4-basic-2000]rule 0 permit source any
[R2-acl-ipv4-basic-2000]quit
[R2]int gi 0/2
[R2-GigabitEthernet0/2]des <connect to ISP>
[R2-GigabitEthernet0/2]ip address 202.2.100.2 28
[R2-GigabitEthernet0/2]nat outbound 2000
[R2-GigabitEthernet0/2]nat server global current-interface inside 10.1.1.1
[R2-GigabitEthernet0/2]quit
[R2]ip route-static 0.0.0.0 0.0.0.0 202.2.100.1
[R2]ip route-static 172.16.1.0 255.255.255.0 10.1.1.1

第一阶段测试：
内网1终端填写IP地址：



内网1终端能PING通内网2的外网地址，PING不通内网2的私网地址：



2、第二阶段调试（SSL VPN配置）：

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

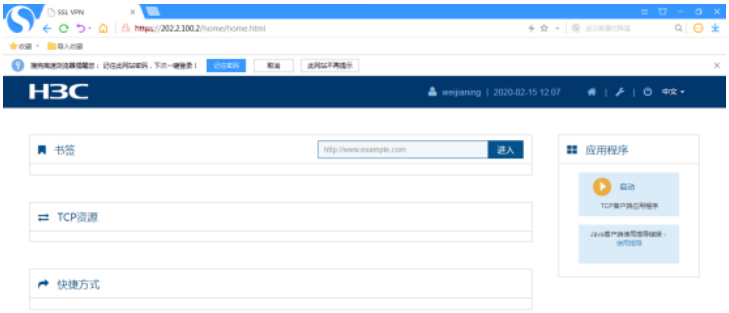
[SSL_VPN]sslvpn gateway james
[SSL_VPN-sslvpn-gateway-james]ip address 10.1.1.1
[SSL_VPN-sslvpn-gateway-james]service enable
[SSL_VPN-sslvpn-gateway-james]quit

[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]ip
[SSL_VPN-sslvpn-context-james-policy-group-ip]ip-tunnel access-route ip-route-list james
[SSL_VPN-sslvpn-context-james-policy-group-ip]filter ip-tunnel acl 3000
[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

第二阶段测试：
打开浏览器，输入网址：https://202.2.100.2

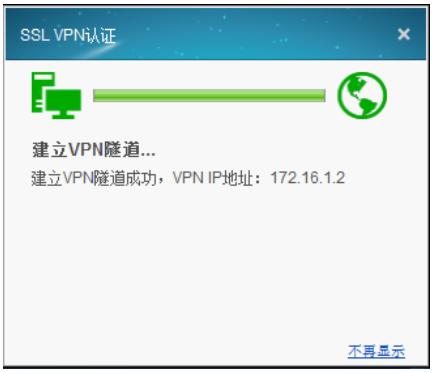
输入用户名、密码，点击登录：



打开inode智能客户端：

输入网关、用户名、密码，点击“链接”：

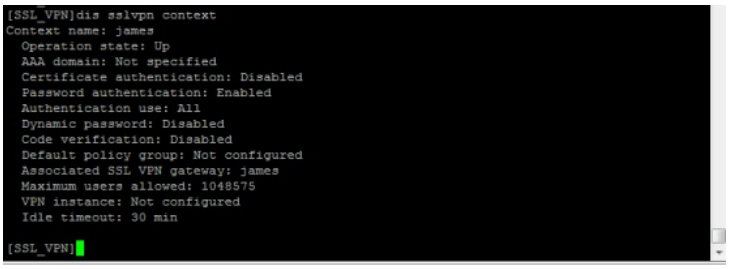
隧道建立成功：



此时内网1的终端可以PING通内网2的WEB服务器：

同时也可以打开WEB服务器的网页：

查看SSL VPN的显示信息：



```
[SSL_VPN]dis sslvpn session verbose
User              : weijianing
Context           : james
Policy group      : ip
Idle timeout      : 30 min
Created at        : 12:07:12 UTC Sat 02/15/2020
Lastest           : 12:07:13 UTC Sat 02/15/2020
User IPv4 address : 202.1.100.2
Session ID        : 1
Web browser/OS    : Chrome

User              : weijianing
Context           : james
Policy group      : ip
Idle timeout      : 30 min
Created at        : 12:09:14 UTC Sat 02/15/2020
Lastest           : 12:10:48 UTC Sat 02/15/2020
User IPv4 address : 202.1.100.2
Alloced IP        : 172.16.1.2
Session ID        : 3
Web browser/OS    : Windows

[SSL_VPN]
```

```
[SSL_VPN]dis sslvpn ip-tunnel statistics
Context                        : james
User                           : weijianing
Session ID                     : 3
User IPv4 address              : 202.1.100.2
Received requests              : 645
Sent requests                  : 608
Dropped requests               : 37
Received replies               : 859
Sent replies                   : 814
Dropped replies                : 45
Received keepalives            : 4
Sent keepalive replies         : 4
Received configuration updates: 0
Sent configuration updates     : 0

[SSL_VPN]
```

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