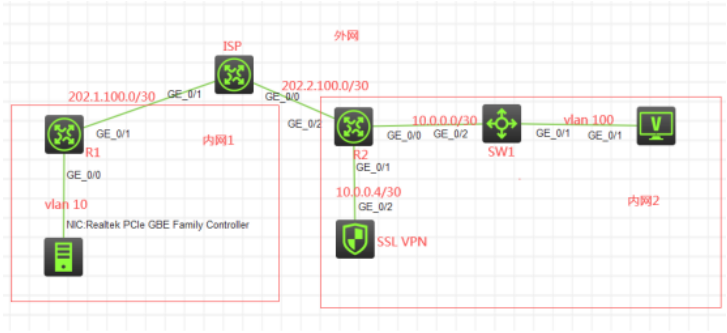
L2TP VPN典型组网配置案例4（L2TP VPN隧道建立后再SSL VPN认证）

SSL VPN　L2TP VPN　PPPoE　SSL VPN　NAT　H3C模拟器　**韦家宁**　2020-02-08 发表

组网及说明



组网说明：

本案例采用H3C HCL模拟器来模拟完成，模拟L2TP VPN隧道后并不能直接访问内网资源，而是再进行SSL VPN认证后才能访问。内网和外网在网络拓扑图中已经有了明确的标识，R1作为内网1的出口设备。R2作为内网2的出口设备，也作为本次L2TP VPN隧道的LNS端点。由于模拟器和本物理机的局限性，因此使用模拟器的F1060防火墙作为SSL VPN网关，本次SSL VPN的架构采用双臂（旁路）的模式，另外使用模拟器的S5820交换机开启WEB功能模拟成为一台WEB服务器。在完成L2TP VPN隧道的配置和建立前，内网1的终端无法到达内网2。在完成L2TP VPN隧道的建立及SSL VPN的配置后，内网1的终端方可通过SSL VPN网关来访问指定的资源。

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，并创建相应的账户和赋予相关的权限
3、R1配置NAT，并配置默认路由指向外网
4、R1配置PPPOE，用于内网1的终端接入
5、SW1配置默认路由指向R2
6、F1060作为SSL VPN网关，采用路由模式，配置默认路由指向R2，并放通相应策略
7、R2配置NAT，并配置默认路由指向外网，同时配置静态路由指向内网
8、R2配置为L2TP VPN LNS端
9、内网1的终端配置VPN拨号软件，作为L2TP VPN的LAC节点进行VPN的拨号
10、F1060开启SSL VPN功能，并发布相应资源
11、L2TP VPN隧道建立后，内网1的终端能够到达内网2，只能访问SSL VPN网关，并通过SSL VPN网关访问相应的资源

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]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
[R1]local-user weijianing class network
New local user added.
[R1-luser-network-weijianing]password simple weijianing
[R1-luser-network-weijianing]service-type ppp
[R1-luser-network-weijianing]quit
[R1]domain name system
[R1-isp-system]authentication ppp local
[R1-isp-system]quit
```

```
[R1]ip pool weijianing 192.168.10.2 192.168.10.254
[R1]ip pool weijianing gateway 192.168.10.1
[R1]int Virtual-Template 1
[R1-Virtual-Template1]ip address 192.168.10.1 255.255.255.0
[R1-Virtual-Template1]ppp authentication-mode pap domain system
[R1-Virtual-Template1]remote address pool weijianing
[R1-Virtual-Template1]quit
[R1]int gi 0/0
[R1-GigabitEthernet0/0]pppoe-server bind virtual-template 1
[R1-GigabitEthernet0/0]quit
```

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]vlan 100
[SW1-vlan100]quit
[SW1]int vlan 100
[SW1-Vlan-interface100]ip address 172.16.100.1 24
[SW1-Vlan-interface100]quit
[SW1]int gi 1/0/1
[SW1-GigabitEthernet1/0/1]port link-type access
[SW1-GigabitEthernet1/0/1]port access vlan 100
[SW1-GigabitEthernet1/0/1]quit
[SW1]int gi 1/0/2
[SW1-GigabitEthernet1/0/2]port link-mode route
[SW1-GigabitEthernet1/0/2]des <connect to R2>
[SW1-GigabitEthernet1/0/2]ip address 10.0.0.1 30
[SW1-GigabitEthernet1/0/2]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 10.0.0.5 30
[SSL_VPN-GigabitEthernet1/0/2]quit
[SSL_VPN]ip route-static 0.0.0.0 0.0.0.0 10.0.0.6
```

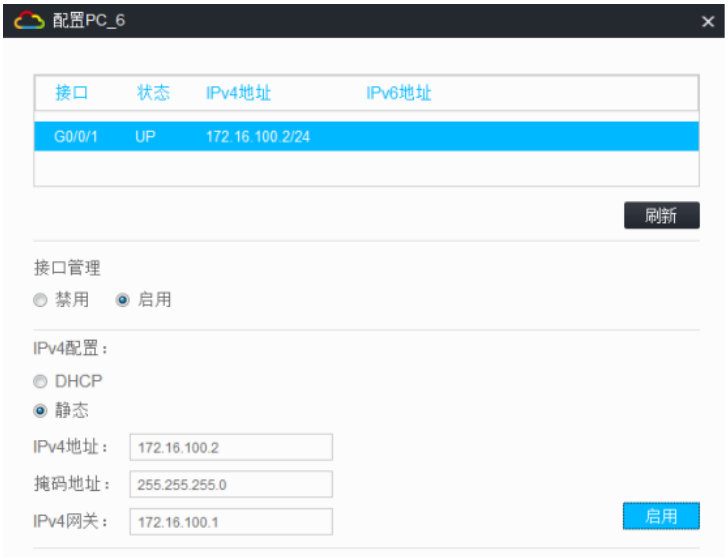
```
[SSL_VPN]security-zone name Untrust
[SSL_VPN-security-zone-Untrust]import interface GigabitEthernet 1/0/2
[SSL_VPN-security-zone-Untrust]quit

[SSL_VPN]acl basic 2000
[SSL_VPN-acl-ipv4-basic-2000]rule 0 permit source any
[SSL_VPN-acl-ipv4-basic-2000]quit
[SSL_VPN]
[SSL_VPN]zone-pair security source trust destination untrust
[SSL_VPN-zone-pair-security-Trust-Untrust]packet-filter 2000
[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 2000
[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 2000
[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 2000
[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 2000
[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 2000
[SSL_VPN-zone-pair-security-Local-Untrust]quit
[SSL_VPN]
```

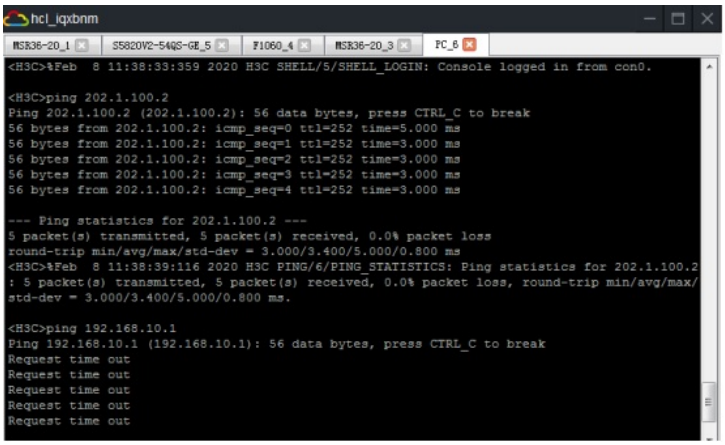
R2：

```
<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 30
[R2-GigabitEthernet0/0]quit
[R2]ip route-static 172.16.100.0 255.255.255.0 10.0.0.1
[R2]int gi 0/1
[R2-GigabitEthernet0/1]des <connect to SSL_VPN>
[R2-GigabitEthernet0/1]ip address 10.0.0.6 30
[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 30
[R2-GigabitEthernet0/2]nat outbound 2000
[R2-GigabitEthernet0/2]quit
[R2]ip route-static 0.0.0.0 0.0.0.0 202.2.100.1
```

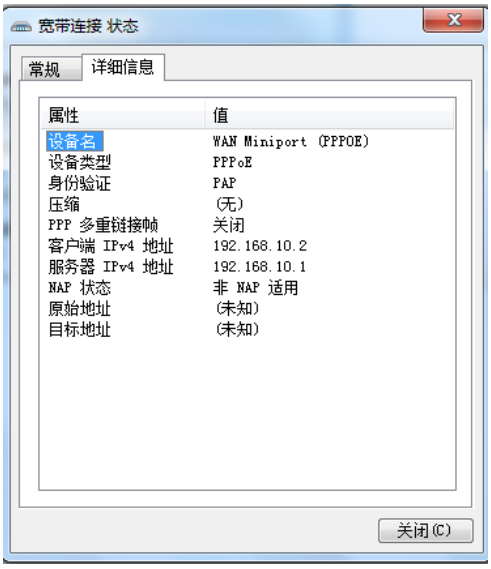
第一阶段测试：

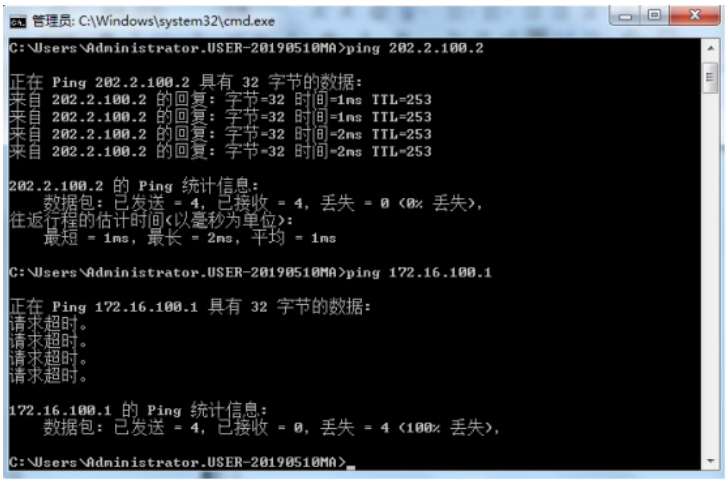
内网2终端填写IP地址，仅能ping通内网1的外网地址，PING不同内网1的私网地址，因为做了NAT地址转换：





内网1终端打开宽带连接，输入用户名、密码，点击“连接”。仅能PING通内网2的外网地址，PING不同内网2的私网地址：





2、第二阶段调试

SSL VPN关键配置点:

[SSL_VPN]acl advanced 3000

[SSL_VPN-acl-ipv4-adv-3000]rule 0 permit tcp source any destination any

[SSL_VPN-acl-ipv4-adv-3000]quit

[SSL_VPN]

[SSL_VPN]

[SSL_VPN]sslvpn gateway james

[SSL_VPN-sslvpn-gateway-james] ip address 10.0.0.5

[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 domain james

[SSL_VPN-sslvpn-context-james]url-list S5820

[SSL_VPN-sslvpn-context-james-url-list-S5820] heading web

[SSL_VPN-sslvpn-context-james-url-list-S5820]url S5820-https url-value https://10.0.0.1

[SSL_VPN-sslvpn-context-james-url-list-S5820]url S5820-http url-value http://10.0.0.1

[SSL_VPN-sslvpn-context-james-url-list-S5820]quit

[SSL_VPN-sslvpn-context-james] policy-group url

[SSL_VPN-sslvpn-context-james-policy-group-url]resources url-list S5820

[SSL_VPN-sslvpn-context-james-policy-group-url]filter web-access acl 3000

[SSL_VPN-sslvpn-context-james-policy-group-url]service enable

[SSL_VPN-sslvpn-context-james]quit

[SSL_VPN]

[SSL_VPN]

[SSL_VPN]local-user james class network

New local user added.

[SSL_VPN-luser-network-james]password simple james

[SSL_VPN-luser-network-james]service-type sslvpn
[SSL_VPN-luser-network-james]authorization-attribute user-role network-operator
[SSL_VPN-luser-network-james]authorization-attribute sslvpn-policy-group url
[SSL_VPN-luser-network-james]quit
[SSL_VPN]

R2 L2TP LNS关键配置点：

[R2]local-user james class network
New local user added.
[R2-luser-network-james]password simple james
[R2-luser-network-james]service-type ppp
[R2-luser-network-james]quit

[R2]ip pool james 172.16.10.2 172.16.10.254
[R2]ip pool james gateway 172.16.10.1

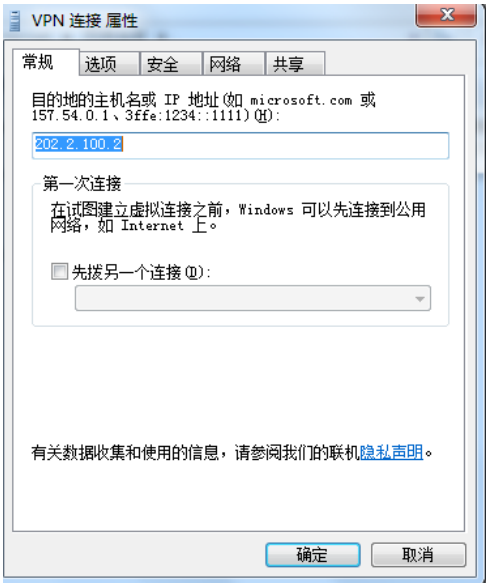
[R2]domain name system
[R2-isp-system]authentication ppp local
[R2-isp-system]quit

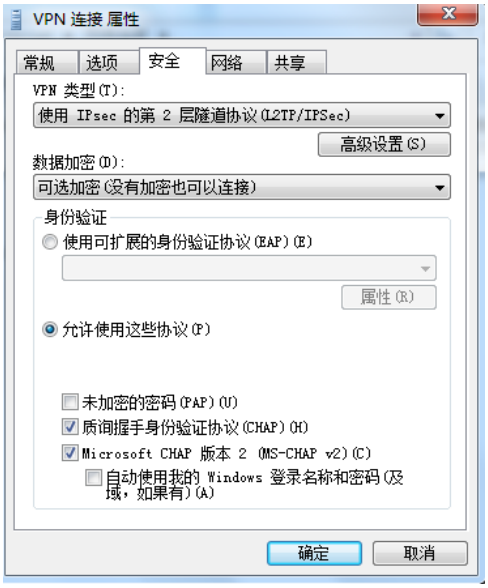
[R2]int Virtual-Template 1
[R2-Virtual-Template1]ip address 172.16.10.1 255.255.255.0
[R2-Virtual-Template1]ppp authentication-mode chap domain system
[R2-Virtual-Template1]remote address pool james
[R2-Virtual-Template1]quit

[R2]l2tp enable

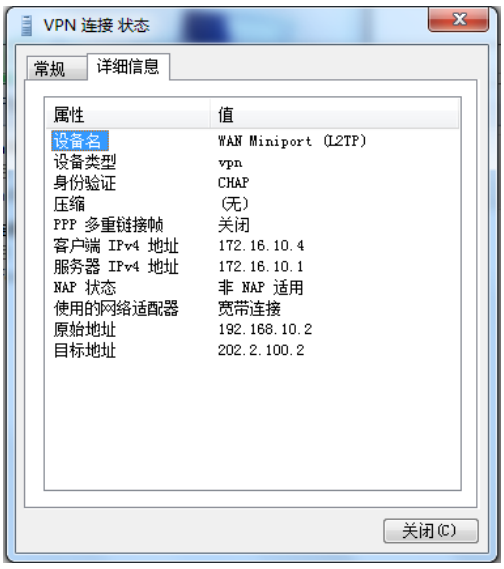
[R2]l2tp-group 1 mode lns
[R2-l2tp1]undo tunnel authentication
[R2-l2tp1]tunnel name LNS
[R2-l2tp1]allow l2tp virtual-template 1
[R2-l2tp1]quit

第二阶段测试
内网1终端打开VPN链接，设置相关参数：





输入用户名、密码，点击“链接”：



查看L2TP隧道及会话信息：

```
[R2]dis l2tp session
LocalSID    RemoteSID    LocalTID    State
28886       1            16344       Established
[R2]
```

```
[R2]dis l2tp tunnel
LocalTID RemoteTID State        Sessions RemoteAddress   RemotePort RemoteName
16344    6         Established  1        202.1.100.2     1064       wgw2195.h3c
                                                                     .huawei-3co
                                                                     m.com

[R2]
```

3、第三阶段调试

在R2配置策略路由，让L2TP VPN拨号过来的用户必须先登录SSL VPN后，才可以在SSL VPN网关内访问资源

R2配置关键点：

[R2]acl basic 2001

[R2-acl-ipv4-basic-2001]rule 0 permit source 172.16.10.0 0.0.0.255

[R2-acl-ipv4-basic-2001]quit

[R2]policy-based-route james permit node 1

[R2-pbr-james-1]if-match acl 2001

[R2-pbr-james-1]apply next-hop 10.0.0.5

[R2-pbr-james-1]quit

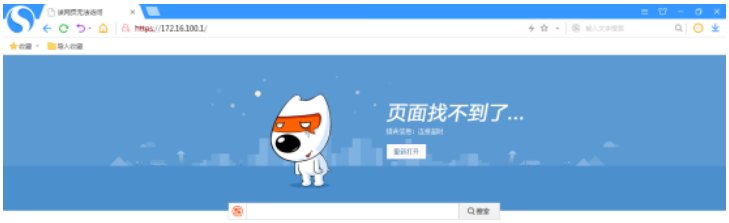
[R2]int Virtual-Template 1

[R2-Virtual-Template1]ip policy-based-route james

[R2-Virtual-Template1]quit

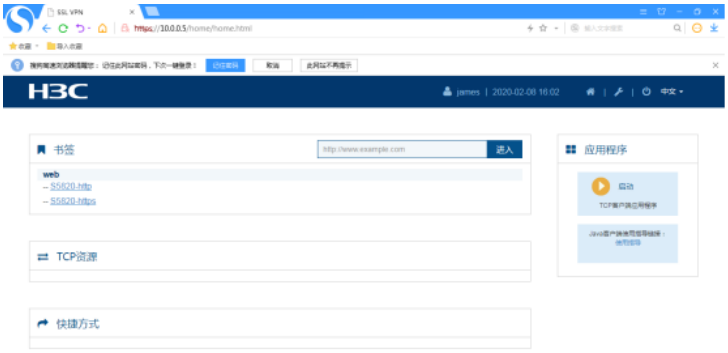
最终测试：

内网1终端无法直接登录SW1的WEB服务

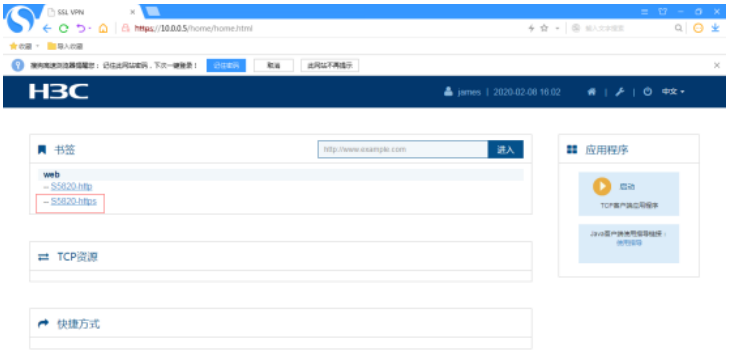


输入SSL VPN网关的登陆地址：https://10.0.0.5

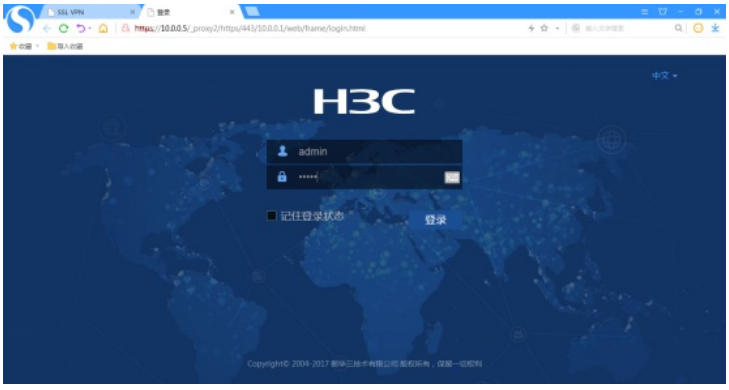
点击“james”后，输入用户名、密码，点击“登陆”：

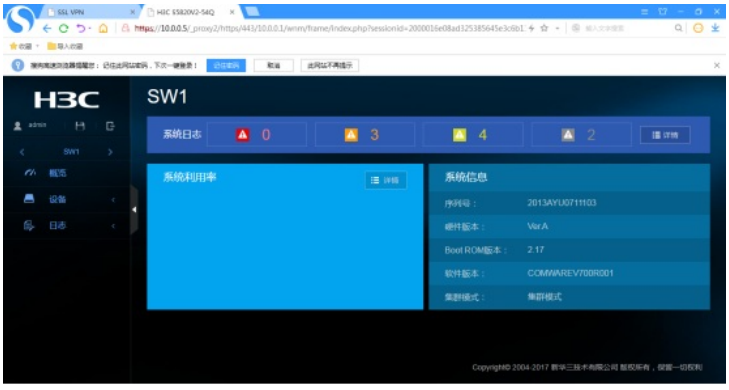


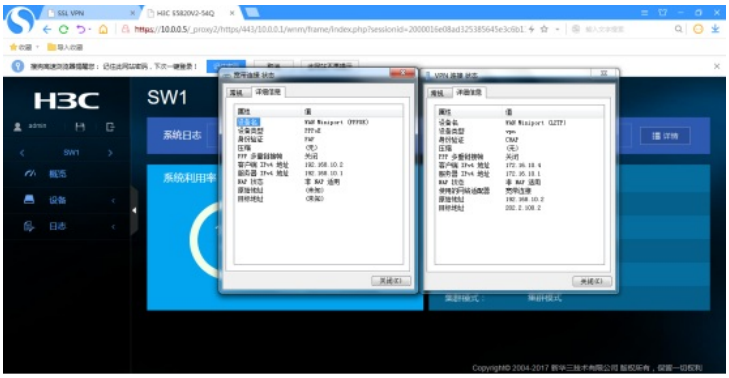
测试访问资源，点击“s5820-https”:



输入用户名、密码，点击“登陆”:







查看SSL VPN的信息：

```
[SSL_VPN]dis sslvpn session
Total users: 1

SSL VPN context: james
Users: 1
Username        Connections  Idle time   Created       User IP
james           0            0/00:05:29  0/00:06:58    172.16.10.4
[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
    Domain name: james
  Maximum users allowed: 1048575
  VPN instance: Not configured
  Idle timeout: 30 min

[SSL_VPN]
```

根据测试结果，内网1的终端通过PPPOE拨号后，再进行L2TP VPN的拨号，到达LNS后再通过SSL VPN的方式访问到内网的WEB服务资源。

至此，L2TP VPN典型组网配置案例4已完成！