一、开始

SSL VPN 以 SSL（Secure Sockets Layer，安全套接字层）为基础提供远程的安全连接服务。用户可通过互联网，使用内嵌 SSL 协议的浏览器与远端的 Web 服务器建立安全的连接，访问内部资源。企业或机构可通过 SSL VPN 来为移动用户或者外部客户提供访问内部资源的服务并保证安全性。SSL VPN 服务通过 SSL VPN 网关来提供。SSL VPN 网关位于远端接入用户和企业内部网络之间，负责在二者之间转发报文。管理员需要在 SSL VPN 网关上创建与企业网内服务器对应的资源。SSL VPN 网关与远端接入用户建立 SSL 连接，并对接入用户进行身份认证。远端接入用户的访问请求只有通过 SSL VPN 网关的安全检查和认证后，才会被 SSL VPN 网关转发到企业网络内部，从而实现对企业内部资源的保护。

SSLVPN 的接入方式包括 Web 接入、TCP 接入和 IP 接入。Web 接入方式是指用户使用浏览器，通过 HTTPS 协议访问 SSL VPN 网关提供的 Web 资源。用户登录后，Web 页面上会显示用户可访问的资源列表，用户可以选择需要访问的资源直接访问。TCP 接入方式是指用户对企业内部服务器开放端口的安全访问。通过 TCP 接入方式，用户可以访问任意基于 TCP 的服务，包括远程访问服务（如 Telnet）、桌面共享服务、电子邮件服务、Notes 服务以及其他使用固定端口的 TCP 服务。IP 接入方式用来实现远程主机与企业内部服务器网络层之间的安全通信，进而实现所有基于 IP 的远程主机与服务器的互通，如在远程主机上 ping 内网服务器。

本文以 V7 防火墙 D032 分支版本为例，介绍完成配置后 SSL VPN 不通问题的排查及解决方法，配置 SSL VPN 过程中问题排查的定位思路如下：首先判断是否能打开 SSL VPN 首页，如果首页打不开说明 SSL VPN 网关配置有问题，需检查网关配置和证书状态。其次查看登录用户是否有授权资源，没有授权资源的用户无法使用 SSL VPN 功能，然后再查看配置的 Web 资源、TCP 资源或者 IP 资源是否可以正常使用，如果资源无法使用，需要检查相关配置是否正确。

使用 NGFW 防火墙的 SSL VPN 功能需要购买授权，未安装 SSL VPN license 缺省支持使用 15 个并发用户，如果是测试环境足够使用，如果是现网环境下需注意授权用户数和授权时间。本文在测试环境的前提下进行，不涉及 license 问题，现网环境注意提前查看授权状态。

此外，排查 SSL VPN 不通问题之前应保证以下前提：

- 配置接口 IP 地址以及加入安全域，配置安全策略，确保外网与 SSL VPN 网关设备可达，SSL VPN 网关设备与内网主机可达。
- SSL VPN 网关设备与 PC 客户端、Web Server 之间路由可达。

二、流程图相关操作说明：

1、是否能打开 SSL VPN 首页

完成 SSL VPN 网关配置并在 SSL VPN 访问实例引用 SSL VPN 网关，使能 SSL VPN 网关功能和 SSL VPN 访问实例功能，然后在浏览器输入网关地址及端口号就能打开 SSL VPN 首页，如图 1 所示。如果打不开 SSL VPN 首页，说明 SSL VPN 网关配置有误，需要检查 sslvpn gateway 的相关配置。

图 1 SSL VPN 首页

2、检查网关配置

通过 Web 导航栏“网络>SSL VPN>网关”可以查看网关状态，检查网关的 IP 地址和端口号是否正确，网关工作状态是否为生效，如图 2 所示，网关状态正常。

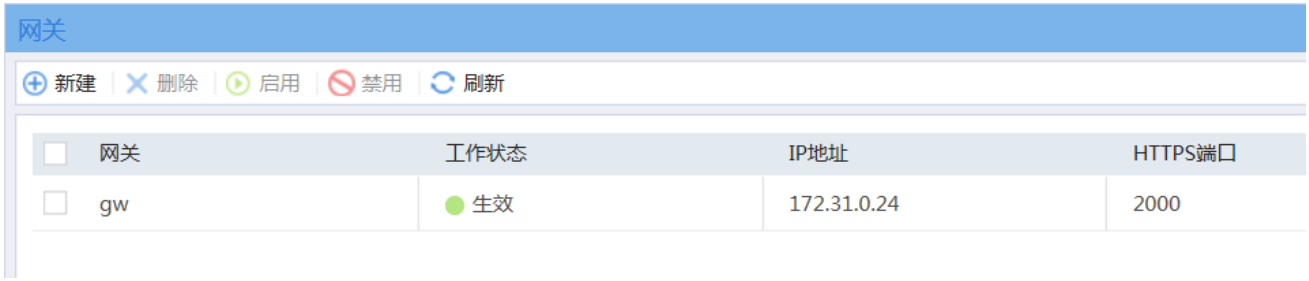

图 2 SSL VPN 网关

点击右侧<编辑>按钮，进入编辑网关窗口，查看 SSL VPN 服务器端策略。缺省情况下（即不引用的情况下），SSL VPN 网关引用设备自带的 SSL 服务器端策略。如果引用了自定义 SSL VPN 服务器端策略，查看网关状态正常，但无法打开 SSL VPN 首页，可以尝试取消 SSL

VPN 服务器端策略的引用，此时防火墙自动调用设备缺省服务器端策略。如果测试成功，则说明引用 SSL VPN 服务器端策略有问题，需要进一步排查。

图 3 检查网关配置

D032 分支鼓励使用 Web 界面操作，命令行同样也支持查看网关状态，通过 display sslvpn gateway 命令查看网关 Operation state 状态，当引用了服务器端策略会显示策略名称，如没有引用，则不显示任何 SSL server policy 参数。

命令：*display sslvpn gateway name XX*

例如：以下网关 gw 里，第一个是没有引用服务器端策略的状态显示，第二个是引用了服务器端策略 ssl 的状态显示。

```
<H3C>display sslvpn gateway name gw
Gateway name: gw
  Operation state: Up
  IP: 172.31.0.24  Port: 2000
  Front VPN instance: Not configured

<H3C>display sslvpn gateway name gw
Gateway name: gw
  Operation state: Up
  IP: 172.31.0.24  Port: 2000
  SSL server policy configured: ssl
  SSL server policy in use: ssl
  Front VPN instance: Not configured
```

3、检查服务器端策略

如果 SSL VPN 首页打不开，页面报如图 4 所示错误，可以判断为服务器端策略出错，更进一步说，很可能是证书出错。需要说明的是，如果在 SSL VPN 网关下引用自定义服务器端策略必须要导入证书，没有证书的话使用设备缺省服务器端策略（即不引用）。

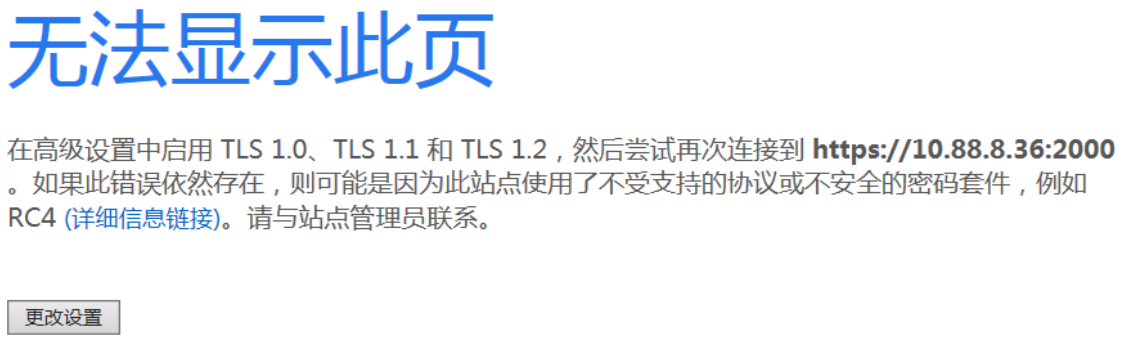

图 4 首页报错

一般情况下，使用离线证书正确的配置过程为，通过 Web 导航栏“对象>PKI>证书”进入证书配置页面，点击上方的<新建 PKI 域>，在弹框里填写域名称 ssl2，点击确定。然后点击上方的<导入证书>，选择对应的域名称 ssl2，依次导入 CA 证书和本地证书，其中本地证书一般设有证书口令，注意不要输入错误。

如果证书导入过程中出错，可以参考《H3C 安全设备 PKI 证书安装指导》文档解决。

图 5 新建 PKI 域

图 6 导入 CA 证书

图 7 导入本地证书

通过 Web 导航栏“对象>SSL>服务器端策略”进入配置页面，点击<新建>进入新建服务器端策略弹框，填写策略名称 ssl2，引用刚才创建的 PKI 域 ssl2，点击确定后完成。

图 8 新建服务器端策略

上述操作顺利完成后就可以在 SSL VPN 网关下引用服务器端策略 ssl2。如果配置没有问题主页仍然报错，可以通过命令可以查看证书状态。

命令：*pki validate-certificate domain domain-name ca*

pki validate-certificate domain domain-name local

例如：通过命令查看，可以确认 PKI 域 ssl2 的 CA 证书和 Local 证书存在且状态正常。只有 CA 证书和 Local 证书的 Verify result 都是 OK 的情况下，才判断为证书合法，否则一律判断证书无效。证书无效时，Verify result 这里会显示原因，常见的有证书过期等，建议更换证书再做测试。

```
[H3C]pki validate-certificate domain ssl2 ca
Verifying certificates......
        Serial Number:
            25:7c:e0:13:d9:cd:cf:a3:42:c8:ea:d1:05:98:61:90
        Issuer:
            CN=TS-SECURITY-CA
        Subject:
            CN=TS-SECURITY-CA
Verify result: OK

[H3C]pki validate-certificate domain ssl2 local
Verifying certificates......
        Serial Number:
            61:84:54:2a:00:04:00:00:00:1d
        Issuer:
            CN=TS-SECURITY-CA
        Subject:
            C=CN
            ST=zhejiang
            L=hangzhou
            O=H3C Hangzhou
            OU=ts-security
            CN=H3C_local
            emailAddress=cert_local12652@h3c.com
Verify result: OK
```

4、用户是否有资源授权

如果没有配置缺省资源组，又没有资源授权的用户是无法访问任何资源的。如图 9 所示，通过浏览器方式，登录 SSL VPN 用户（h3c），Web 资源和 TCP 资源为空，说明没有授权相应资源。IP 接入需要使用 inode 客户端登录，如果没有任何可用资源，inode 客户端也无法拨入，如图 10 所示。

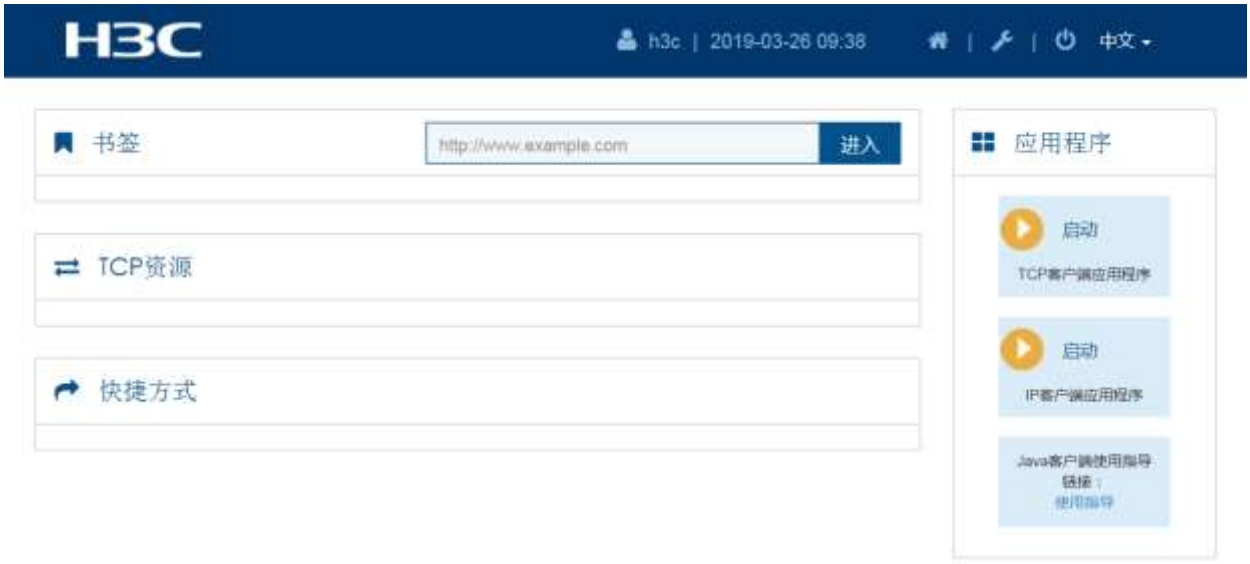

图 9 登录用户

图 10 没有授权资源无法拨入 inode

5、授权用户资源组

以本地 SSL VPN 用户的用户名/密码认证为例，通过 Web 导航栏“对象>用户管理>本地用户”创建本地用户，可用服务里选择 SSL VPN 类型。在下拉窗口的授权属性里，关联相应

的 SSL VPN 策略组，如图 12 所示。

图 11 创建 SSL VPN 用户

图 12 SSL VPN 用户管理策略组

如果使用用户组给 SSL VPN 用户分类，每个用户组的用户使用相同的资源，可以在用户组的授权属性中关联 SSL VPN 策略组，并将用户加入对应授权用户组。

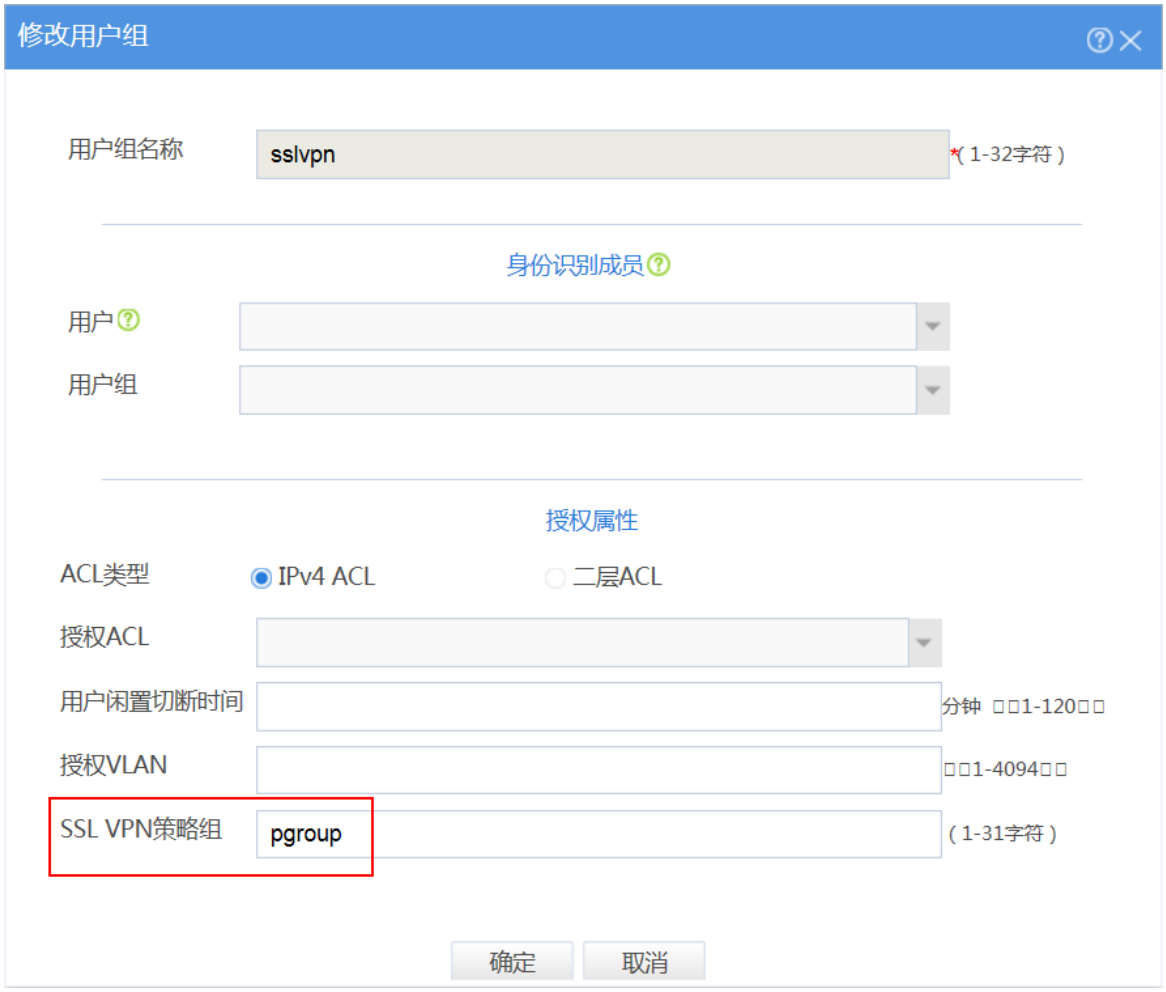

图 13 用户组关联 SSL VPN 策略组

6、是否能访问 Web 资源

Web 接入方式中，所有数据的显示和操作都是通过 Web 页面进行的。登录 SSL VPN 首页输入用户名/密码，单击<登录>按钮，可以成功登录 SSL VPN 网关。网关首页的“书签”栏显示 h3c 用户可以访问的 Web 资源 ACG，如图 14 所示。

单击链接“ACG”，即可访问内网资源 ACG，如果访问不了，或者没有 Web 资源，建议检查 Web 接入配置。

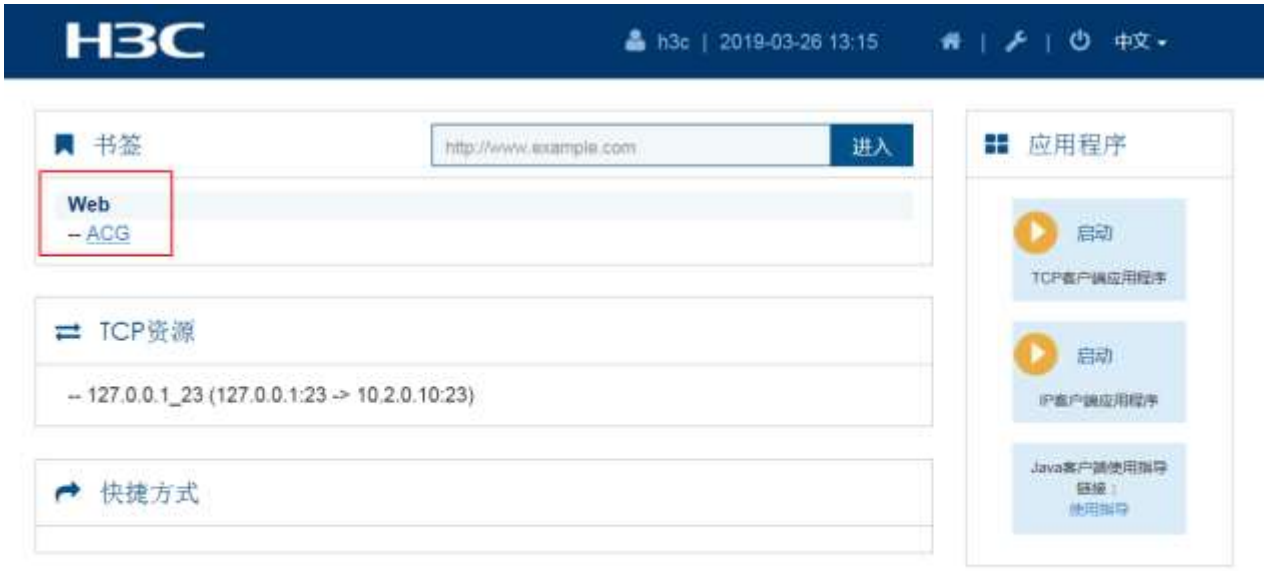

图 14 访问 Web 资源

7、检查 Web 接入配置

Web 接入方式下，管理员需要在 SSL VPN 网关上创建 URL 列表，URL 表项为企业网内部服务器的 IP 地址（或域名）。通过 Web 导航栏“网络>SSL VPN>访问实例”新建实例或者编辑已有实例，查看 Web 业务配置，如图 15 所示，新建 URL 表项 ACG，并在 URL 列表 Web 里引用表项 ACG。

完成 Web 业务配置后，还需要在资源组 pgroup 里引用 Web 资源，如图 16 所示：

图 15 Web 业务

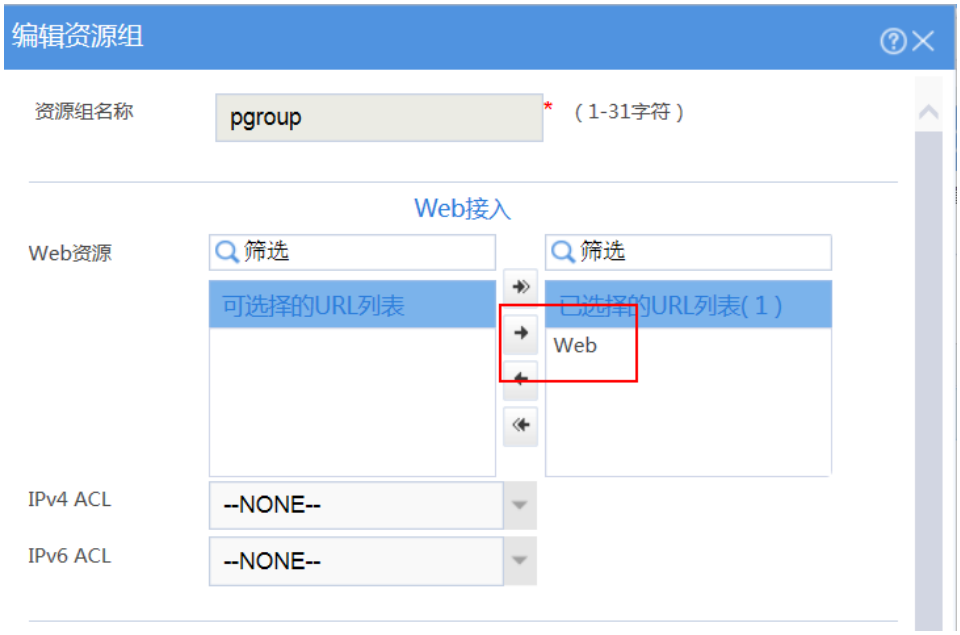

图 16 Web 资源加入资源组

命令行也可以检查 Web 业务相关配置，配置思路跟 Web 没有区别。

命令：*display current-configuration configuration sslvpn-context*

例如：配置完成 URL 列表 Web，在资源组 pgroup 下引用。

```
<H3C>display current-configuration configuration sslvpn-context
#
sslvpn context ctl
 gateway gw
 ip-tunnel interface SSLVPN-AC10
 ip-tunnel address-pool pool mask 255.255.255.0
 web-access ip-client auto-activate
 port-forward-item 127.0.0.1_23
  local-port 23 local-name 127.0.0.1 remote-server 10.2.0.10 remote-port 23
 port-forward pl
  resources port-forward-item 127.0.0.1_23
 ip-route-list rtlist
  include 10.2.0.0 255.255.255.0
 url-item ACG
  url http://10.2.0.10/
 url-list Web
  resources url-item ACG
 policy-group pgroup
  resources port-forward pl
  resources url-list Web
 log user-login enable
 log resource-access enable filtering
 session-connections 0
 max-onlines 1048500
 service enable
#
return
```

如果确认 Web 接入配置无误，仍然无法成功跳转资源，可以考虑采用 IP 接入。

8、是否能访问 TCP 资源

用户利用 TCP 接入方式访问内网服务器时,需要在 SSL VPN 客户端(用户使用的终端设备）上安装专用的 TCP 接入客户端软件，由该软件实现使用 SSL 连接传送应用层数据。此外，SSL VPN 用户的电脑需要安装 Java Runtime Environment version7（JRE7）及其以上版本。

登录 SSL VPN 首页输入用户名/密码，单击<登录>按钮，可以成功登录 SSL VPN 网关。在网页的应用程序栏中选择“启动 TCP 客户端应用程序”，如图 17 所示。单击<启动>按钮，下载 TCP 接入客户端软件并运行。

图 17 启动 TCP 客户端应用程序

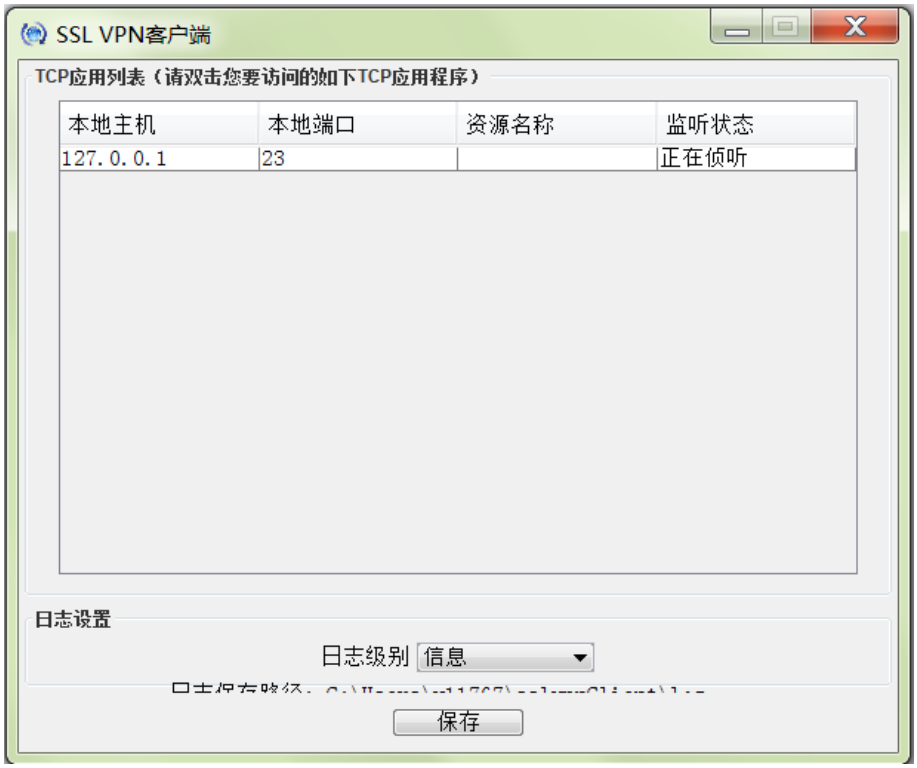

图 18 TCP 接入客户端

此时正常情况下，用户在 PC 上执行 telnet 127.0.0.1 23，可以远程连接到 Server。如果无法连接，需要检查 TCP 接入的配置。

如果 TCP 客户端无法正常启动，可以参考《Comware V7 SSLVPN IP 廋客户端接入方式使用

指导》。

9、检查 TCP 接入配置

TCP 接入方式下，管理员需要在 SSL VPN 网关上创建端口转发规则，将企业网内部服务器的 IP 地址（或域名）和端口号映射为 SSL VPN 客户端的本地 IP 地址（或主机名）和本地端口号。

通过 Web 导航栏“网络>SSL VPN>访问实例”新建实例或者编辑已有实例，查看 TCP 业务配置，如图 19 所示，创建端口转发表项 p1,添加端口转发实例，将 10.2.0.10 提供的 Telnet 服务映射到本地地址 127.0.0.1、本地端口 23。

完成 TCP 业务配置后，还需要在资源组 pgroup 里引用 TCP 资源，如图 20 所示。

图 19 TCP 业务

图 20 TCP 资源加入资源组

命令行也可以检查 TCP 业务相关配置，配置思路跟 Web 没有区别。

命令：*display current-configuration configuration sslvpn-context*

例如：配置完成端口转发表项 pl，在资源组 pgroup 下引用。

```
<H3C>display current-configuration configuration sslvpn-context
#
sslvpn context ctl
 gateway gw
 ip-tunnel interface SSLVPN-AC10
 ip-tunnel address-pool pool mask 255.255.255.0
 web-access ip-client auto-activate
 port-forward-item 127.0.0.1_23
  local-port 23 local-name 127.0.0.1 remote-server 10.2.0.10 remote-port 23
 port-forward pl
  resources port-forward-item 127.0.0.1_23
 ip-route-list rtlist
  include 10.2.0.0 255.255.255.0
 url-item ACG
  url http://10.2.0.10/
 url-list Web
  resources url-item ACG
 policy-group pgroup
  resources port-forward pl
  resources url-list Web
 log user-login enable
 log resource-access enable filtering
 session-connections 0
 max-onlines 1048500
 service enable
#
return
```

10、是否能访问 IP 资源

用户通过 IP 接入方式访问内网服务器前，需要安装专用的 IP 接入客户端软件，该客户端软件会在 SSL VPN 客户端上安装一个虚拟网卡。用户在客户端上安装 IP 接入客户端软件后，启动该软件并登录。SSL VPN 网关对其进行认证和授权。认证、授权通过后，SSL VPN 网关为客户端的虚拟网卡分配 IP 地址，并将授权用户访问的 IP 接入资源（即路由表项）发送给客户端。客户端为虚拟网卡设置 IP 地址，并添加路由表项，路由的出接口为虚拟网卡，用户即可访问内网资源。

登录 SSL VPN 首页输入用户名/密码，单击<登录>按钮，可以成功登录 SSL VPN 网关。在网页的应用程序栏中选择“启动 IP 客户端应用程序”，如图 21 所示。单击<启动>按钮，下载 IP 接入客户端软件 Svpnclient 并安装，安装完成后，启动 iNode 客户端，输入如图 22 所示的参数。

图 21 启动 IP 客户端应用程序

图 22 iNode 客户端

单击<连接>按钮，成功登录 SSL VPN 客户端，如下图所示：

图 23 成功登录 SSL VPN 网关

用户 IP 接入成功后，可以在 PC 上打印网卡地址信息和路由表信息。

命令：*ipconfig /all*

route print

例如：如下图所示，用户获取到网关分配的地址 192.168.10.2，与网关 AC 口同网段，并自动获取到内网资源的路由表项 10.2.0.0/24。

```
C:\Users\Administrator>ipconfig

Windows IP 配置


以太网适配器 本地连接 2:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::1cd:9de8:69a:3e6b%18
   IPv4 地址 . . . . . : 192.168.10.2
   子网掩码 . . . . . : 255.255.255.0
   默认网关. . . . . :

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . :
   IPv4 地址 . . . . . : 172.31.0.61
   子网掩码 . . . . . : 255.255.252.0
   默认网关. . . . . : 172.31.0.1
```

图 24 用户获取到网关分配地址

图 25 用户获取到网关下发的内网路由表项

11、检查 IP 接入配置

IP 接入方式下，管理员在 SSL VPN 网关上创建 SSL VPN AC 接口，并配置下发给 SSL VPN 客户端的路由表项。通过 Web 导航栏“网络>SSL VPN>IP 接入接口”查看 AC 口配置，如图 26 所示。需要注意 AC 口需要加入安全域，并且要放通 AC 口所在安全域到内网安全域的安全策略，如果客户端要 ping 通 AC 口还需放通 AC 口所在安全域到本地的安全策略。

图 26 配置 AC 口

通过 Web 导航栏“网络>SSL VPN>客户端地址池”查看 SSL VPN 客户端地址池，一般情况下客户端地址池与 AC 口同网段，但注意不要包含 AC 口地址。

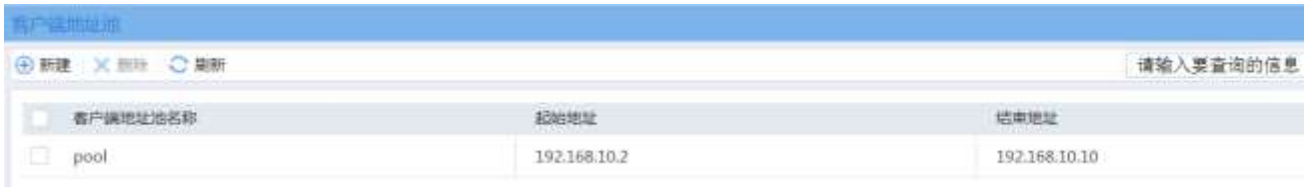

图 27 配置客户端地址池

通过 Web 导航栏“网络>SSL VPN>访问实例”新建实例或者编辑已有实例，查看 IP 业务配置，如图 28 所示，引用的 SSL VPN AC 接口 10 和 SSL VPN 客户端地址池 pool。然后下拉配置窗口，查看 IP 接入资源，即路由表项是否配置正确。

图 28 IP 业务

图 29 IP 接入资源

完成 IP 业务配置后，还需要在资源组 pgroup 里引用 IP 资源，如图 30 所示，引用路由列表 rtlist 和 SSL VPN 客户端地址池 pool，并同时配置对 IP 接入进行 ACL 过滤。其中 ACL 过滤的是 inode 客户端获取的地址池地址，一般配置为全允许。

图 30 IP 资源加入资源组

命令行也可以检查 IP 业务相关配置，配置思路跟 Web 没有区别。

命令：display current-configuration configuration sslvpn-context

例如：配置 AC 口 10、客户端地址池 pool 以及端口路由表项 rtlist，并在资源组 pgroup 下引用。

```
<H3C>display current-configuration configuration sslvpn-context
#
sslvpn context ctl
 gateway gw
 ip-tunnel interface SSLVPN-AC10
 ip-tunnel address-pool pool mask 255.255.255.0
 web-access ip-client auto-activate
 port-forward-item 127.0.0.1_23
  local-port 23 local-name 127.0.0.1 remote-server 10.2.0.10 remote-port 23
 port-forward pl
  resources port-forward-item 127.0.0.1_23
 ip-route-list rtlist
  include 10.2.0.0 255.255.255.0
 url-item ACG
  url http://10.2.0.10/
 url-list Web
  resources url-item ACG
 policy-group pgroup
  resources port-forward pl
  filter ip-tunnel acl 3000
  ip-tunnel access-route ip-route-list rtlist
  ip-tunnel address-pool pool mask 255.255.255.0
  resources url-list Web
 log user-login enable
 log resource-access enable filtering
 session-connections 0
 max-onlines 1048500
 service enable
#
return
```