

# SSL VPN 同实例多网关配置举例

SSL VPN 李菁 2021-12-21 发表

## 组网及说明



客户现场要求使用域名方式登录SSL VPN，但是部分终端的拨号客户端不支持域名方式登录（如安卓手机的inode），现场其他客户端都是已经使用域名方式的了，不方便修改，现在需要访问同样的资源，支持域名方式和IP地址方式同时使用。

## 配置步骤

可以在同一个context中调用多个gateway实现。

关键配置：

```
#  
dns proxy enable  
ip host vpn.cn 1.1.1.2  
#  
interface GigabitEthernet1/0/1  
port link-mode route  
ip address 1.1.1.2 255.255.255.0  
#  
interface SSLVPN-AC1  
ip address 10.1.1.100 255.255.255.0  
#  
security-zone name Local  
#  
security-zone name Trust  
import interface GigabitEthernet1/0/2  
#  
security-zone name DMZ  
#  
security-zone name Untrust  
import interface GigabitEthernet1/0/1  
#  
security-zone name Management  
#  
security-zone name ssl  
import interface SSLVPN-AC1  
#  
acl advanced 3000  
rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 20.2.2.0 0.0.0.255  
#  
local-user ss1vpnuser class network  
password cipher $c$3$DkJv03wvhmBuVZg0z/LMNlcFhAgi2p+Y6w==  
service-type sslvpn  
authorization-attribute user-role network-operator  
authorization-attribute sslvpn-policy-group resourcegrp  
#  
sslvpn ip address-pool sslvpnpool 10.1.1.1 10.1.1.10  
#  
sslvpn gateway gw  
ip address 1.1.1.2 port 4430  
service enable  
#  
sslvpn gateway test  
ip address 1.1.1.2 port 4433  
service enable  
#  
sslvpn context ctxip  
gateway gw virtual-host vpn.cn  
gateway test domain domainip  
ip-tunnel interface SSLVPN-AC1  
ip-tunnel address-pool sslvpnpool mask 255.255.255.0  
ip-route-list rtlist  
include 20.2.2.0 255.255.255.0  
policy-group resourcegrp  
filter ip-tunnel acl 3000  
ip-tunnel access-route ip-route-list rtlist  
service enable
```

```
#  
security-policy ip  
rule 0 name untrst-local  
    配置关键点  
        action pass  
1destination-zone trust以调用多个gateway;  
2rule如果在 gateway 中配置了 gateway gw virtual-host xxxxx, 则只能通过域名方式登录该SSLVPN网关  
, as http请求头部需要时域名格式  
source-zone ssl  
destination-zone trust
```