某局点F10X0防火墙sslvpn拨入用户访问外网不通故障案例

SSL VPN 单畅 2022-09-30 发表

问题描述

防火墙25口接政务网，做ospf和VPN实例，内网用户通过NAT出去访问政务网资源；
24口接互联网，做ssl vpn拨号，通过iNode客户端获取172.168.0.x的地址；
电脑通过iNode拨号后，无法访问政务网的地址。

过程分析

接口配置如下：

```
#
interface GigabitEthernet1/0/24
 port link-mode route
 description T-联通互联网专线
 ip address 123.13.176.208 255.255.255.0
 gateway 123.13.176.1
#
interface GigabitEthernet1/0/25
 port link-mode route
#
interface GigabitEthernet1/0/25.10
 ip address 172.16.201.202 255.255.255.252
 ospf network-type p2p
 vlan-type dot1q vid 10
#
interface GigabitEthernet1/0/25.2001
 ip binding vpn-instance KF_GongXiang_2001
 ip address 100.79.38.146 255.255.255.252
 ospf network-type p2p
 nat outbound 3001 address-group 1 vpn-instance KF_GongXiang_2001
 vlan-type dot1q vid 2001
#
#
sslvpn context SSLVPNSL
 gateway SSLVPNWG
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool SSLVPN地址池 mask 255.255.224.0
 ip-tunnel dns-server primary 202.102.224.68
 ip-tunnel dns-server secondary 114.114.114.114
 ip-route-list 1
  include 0.0.0.0 0.0.0.0
  include 10.46.0.0 255.255.0.0
  include 59.0.0.0 255.0.0.0
 policy-group SSLVPN资源组
  filter ip-tunnel acl 3999
  ip-tunnel access-route ip-route-list 1
  ip-tunnel address-pool SSLVPN 地址池  mask 255.255.224.0
 default-policy-group SSLVPN资源组
 force-logout max-onlines enable
 service enable
#
 ip route-static vpn-instance KF_GongXiang_2001 0.0.0.0 0 100.79.38.145
 #
ospf 2 vpn-instance KF_GongXiang_2001
 import-route direct route-policy YeWu
 import-route static
 area 0.0.0.0
  network 59.227.246.144 0.0.0.7
#
  network 100.79.38.144 0.0.0.3
#
```

查看配置有VPN路由配置，sslvpn ip-route-list 引入了全零路由。

但是外网接口绑定了vpn实例，sslvpn进来后由于AC口没有绑定VPN实例，所以进入了全局，需要增加配置ip route-static 0.0.0.0 0 vpn-instance KF_GongXiang 100.79.38.145，即destination口绑定了VPN实例KF_GongXiang

解决方法

增加配置ip route-static 0.0.0.0 0 vpn-instance KF_GongXiang 100.79.38.145解决