防火墙ssl vpn拨入后访问不了内网

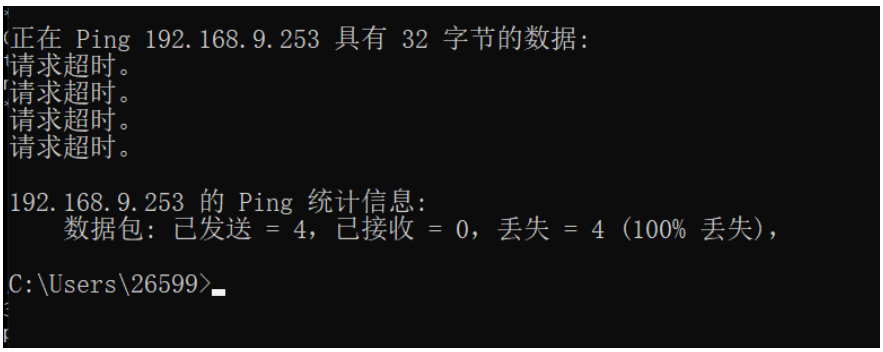
SSL VPN　李发展1　2023-01-31 发表

组网及说明

不涉及

问题描述

防火墙F1000-ak作为sslvpn网关 ip接入方式，拨号已经成功，但是访问不了内网业务资源。



过程分析

1.排查ac口是否加入了安全域中，安全策略是否放通.

排查无问题。

```
#
security-zone name Trust
 import interface GigabitEthernet1/0/0
 import interface GigabitEthernet1/0/17
#
security-zone name DMZ
 import interface GigabitEthernet1/0/15
#
security-zone name Untrust
 import interface Dialer0
 import interface GigabitEthernet1/0/2
 import interface GigabitEthernet1/0/3
 import interface SSLVPN-AC0
#
```

```
#
security-policy ip
 rule 1 name TtoU
  action pass
  profile 1_IPv4
  source-zone Trust
```

2.排查防火墙AC口到内网业务地址，和内网地址到ac口是否可通信。

可通信无问题。

```
[H3C]ping -a 172.16.10.1 192.168.9.253
Ping 192.168.9.253 (192.168.9.253) from 172.16.10.1: 56 data bytes, press CTRL+C to break
56 bytes from 192.168.9.253: icmp_seq=0 ttl=253 time=3.492 ms
56 bytes from 192.168.9.253: icmp_seq=1 ttl=253 time=0.519 ms
56 bytes from 192.168.9.253: icmp_seq=2 ttl=253 time=0.551 ms
56 bytes from 192.168.9.253: icmp_seq=3 ttl=253 time=0.584 ms
56 bytes from 192.168.9.253: icmp_seq=4 ttl=253 time=3.517 ms

--- Ping statistics for 192.168.9.253 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.519/1.733/3.517/1.447 ms
```

#配置中配置路由列表无问题

sslvpn context ss

gateway ssl

ip-tunnel interface SSLVPN-AC0

ip-tunnel address-pool sslpool mask 255.255.255.0

ip-tunnel dns-server primary 192.168.9.210

ip-tunnel dns-server secondary 223.5.5.5

ip-route-list 1

include 192.168.9.0 255.255.255.0

3.外网终端也可以获取到了sslvpn地址池内的地址

无问题

```
==========================================================================
动路由:
络目标          网络掩码          网关        接口    跃点数
        0.0.0.0         0.0.0.0      192.168.1.1    192.168.1.195     35
      127.0.0.0       255.0.0.0         在链路上         127.0.0.1    331
      127.0.0.1 255.255.255.255         在链路上         127.0.0.1    331
127.255.255.255 255.255.255.255         在链路上         127.0.0.1    331
    172.16.[redacted]   255.255.255.0         在链路上       172.16.[redacted]    257
    172.16.[redacted] 255.255.255.255         在链路上       172.16.[redacted]    257
  172.16.10.255 255.255.255.255         在链路上        172.16.10.2    257
```

4.查看内网接口配置应用有策略路由

内网口

```
#
interface GigabitEthernet1/0/17
 port link-mode route
 combo enable fiber
 ip address 10.0.0.1 255.255.255.252
 manage https inbound
 manage ping inbound
 manage ssh inbound
 ip policy-based-route yidong
#
```

解决方法

最后排查是由于：内网口是否有策略路由等将回程报文错误的转发到其他接口，导致报文丢弃。

优化方法：

发现配置策略路由有3个node节点

```
#
policy-based-route yidong permit node 950
 if-match acl 3997
#
policy-based-route yidong permit node 1000
 if-match acl 2999
 apply next-hop 39.152.24.1 direct
#
policy-based-route yidong permit node 1050
 if-match acl 2998
```

第一个node节点匹配了acl 3997，发现3997中匹配有一个内网地址。

由于pbr的策略是由上往下依次匹配，因此在acl 3997中再添加一条rule规则匹配内网9.253后问解决、

```
#
acl advanced 3000
 rule 0 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.9.0 0.0.0.255
 rule 5 permit ip source 192.168.9.0 0.0.0.255 destination 172.16.10.0 0.0.0.255
 rule 10 permit icmp
#
acl advanced 3997
 rule 0 permit ip destination 10.10.0.0 0.0.0.255
#
acl advanced 3998
 rule 0 permit ip destination 192.168.9.218 0
 rule 10 permit ip destination 192.168.9.210 0
#
acl advanced 3999
 rule 0 permit ip destination 192.168.9.216 0.0.0.7
 rule 5 permit ip destination 192.168.9.223 0
 rule 10 permit ip destination 192.168.9.224 0
 rule 15 permit ip destination 192.168.9.225 0
 rule 20 permit ip destination 192.168.9.226 0
#
```