防火墙ssl vpn拨号正常但访问内网失败

SSL VPN　吴昊A　2020-01-11 发表

组网及说明

不涉及

问题描述

SSL VPN通过iNode拨号成功，但是内网不通。

关键配置:

```
#
sslvpn ip address-pool sslvpnpool 10.150.0.10 10.150.0.200
#
sslvpn gateway gw
 ip address 140.206.62.12 port 4430
 service enable
#
sslvpn context ctxip
 gateway gw domain domainip
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool sslvpnpool mask 255.255.255.0
 ip-route-list rtlist
  include 6.6.6.0 255.255.255.0
  include 7.7.7.0 255.255.255.0
  include 8.8.8.0 255.255.255.0
  include 10.6.0.0 255.255.0.0
  include 10.7.0.0 255.255.0.0
  include 10.9.0.0 255.255.0.0
  include 10.10.0.0 255.255.255.0
  include 10.10.1.0 255.255.255.0
  include 10.150.0.0 255.255.255.0
  include 172.29.0.0 255.255.0.0
 policy-group resourcegr
  filter ip-tunnel acl 3939
  ip-tunnel access-route ip-route-list rtlist
 policy-group resourcegrp
  filter ip-tunnel acl 3939
  ip-tunnel access-route ip-route-list rtlist
 service enable
#
```

测试1：我通过电脑拨上SSL VPN后，获取到10.150.0.11地址，ping 10.9.240.215（内网服务器）不通，ping 10.10.1.138（FW自身跨网段地址）可以通，且路由下发没问题。

测试2：防火墙上ping –a 10.150.0.1（SSL-AC口） 10.9.240.215（内网服务器）可以通

```
<WT2-MDFT-FW-M>ping -a 10.150.0.13 10.9.240.215
Ping 10.9.240.215 (10.9.240.215) from 10.150.0.13: 56 data bytes, press CTRL_C to break
56 bytes from 10.9.240.215: icmp_seq=0 ttl=62 time=1.828 ms
56 bytes from 10.9.240.215: icmp_seq=1 ttl=62 time=1.483 ms
56 bytes from 10.9.240.215: icmp_seq=2 ttl=62 time=1.596 ms
56 bytes from 10.9.240.215: icmp_seq=3 ttl=62 time=1.504 ms
56 bytes from 10.9.240.215: icmp_seq=4 ttl=62 time=1.426 ms
```

测试3：流统测试，发现交换机侧收发包没问题，IPS侧只能看到outbound方向的包，防火墙侧只能看到发包，看不到回包

```
<WT2-MDFT-FW-M>dis qos po interface FortyGigE 1/0/3
Interface: FortyGigE1/0/3
  Direction: Inbound
  Policy: test2
   Classifier: test2
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
```

If-match acl 3992
Behavior: test2
Filter enable: Permit

Interface: FortyGigE1/0/3
Direction: Outbound
Policy: test1
Classifier: test1
Matched : 16 (Packets) 1248 (Bytes)
5-minute statistics:
Forwarded: 0/8 (pps/bps)
Dropped : 0/0 (pps/bps)
Operator: AND
Rule(s) :
If-match acl 3991
Behavior: test1
Filter enable: Permit

测试4：debug ip+aspf packet只能看到以下信息：

*Jan 2 17:25:09:645 2020 WT2-MDFT-FW-M IPFW/7/IPFW_PACKET: -COntext=1;
Receiving, interface = SSLVPN-AC1
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 61590, offset = 0, ttl = 64, protocol = 1
checksum = 34176, s = 10.150.0.10, d = 10.9.240.1
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface SSLVPN-AC1.
Payload: ICMP
type = 8, code = 0, checksum = 0x48e4.

*Jan 2 17:25:09:645 2020 WT2-MDFT-FW-M IPFW/7/IPFW_PACKET: -COntext=1;
Sending, interface = Vlan-interface934
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 61590, offset = 0, ttl = 63, protocol = 1
checksum = 34432, s = 10.150.0.10, d = 10.9.240.1
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Sending IP packet received from interface SSLVPN-AC1 at interface Vlan-interface934.
Payload: ICMP
type = 8, code = 0, checksum = 0x48e4.

过程分析

经定位，现场vpn拨入后，访问内部服务器的流量（比如10.9.240.1）命中了策略路由，直接被扔了出去，导致访问不通，修改策略路由测试正常。

```
#
interface Vlan-interface934
ip address 10.10.1.130 255.255.255.248
ospf authentication-mode simple cipher $c$3$W9KS5XOEeX0ZCkPVw8eEcqw83/0lLus2DA==
ospf bfd enable
ip policy-based-route user
bfd min-transmit-interval 500
bfd min-receive-interval 500
bfd detect-multiplier 7
#

#
policy-based-route user permit node 50
if-match acl 3013
apply next-hop 140.206.62.9 track 1
#
#
acl advanced 3013
description T2-Free-1
 rule 1 permit ip source 10.9.96.0 0.0.15.255
rule 2 permit ip source 10.9.112.0 0.0.15.255
rule 3 permit ip source 10.9.176.0 0.0.15.255
```

rule 4 permit ip source 172.29.240.0 0.0.15.255
rule 5 permit ip source 10.9.240.0 0.0.3.255
rule 6 permit ip source 10.150.0.0 0.0.0.255
#

解决方法

修改策略路由后测试正常

附件下载： 四代板配置.txt