某局点F1050 打不开部分网页处理经验案例

刘文峰 2018-03-27 发表

某局点采用我司F1050 防火墙作为出口设备，配置完之后，发现上网打开部分网页有问题，比如hao123，但是大部分网页都是正常的，把我司设备换下来，电脑直连外网线测试都是正常的，初步怀疑是出口的tcp mss 或者mtu 问题导致，指导客户在外网口修改tcp mss 1024，mtu改成1400 ，但是测试之后都不行，后续把mtu 改成1200、1000 测试都不行，升级到官网最新版本也不行。

关键配置：

```
interface GigabitEthernet1/0/1（外网出口）
 port link-mode route
 ip address 11.1.1.1 255.255.255.252
 tcp mss 1024
 nat outbound 2000
zone-pair security source Trust destination Untrust
 object-policy apply ip 1
 packet-filter 3500
ip route-static 0.0.0.0 0 11.1.1.2
 ip route-static 1.1.1.0 24 172.20.1.254
 ip route-static 1.1.1.1 32 172.20.1.254
 ip route-static 2.2.2.0 24 172.20.1.254
 ip route-static 10.0.0.0 8 172.20.1.254
 ip route-static 172.0.0.0 8 172.20.1.254
 ip route-static 173.0.0.0 8 172.20.1.254
 ip route-static 180.0.0.0 8 172.20.1.254
 ip route-static 192.0.0.0 8 172.20.1.254
```

故障时的会话：

```
Initiator:
  Source      IP/port: 172.16.50.181/5034
  Destination IP/port: 180.163.32.172/8080（hao123的公网地址）
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface50
  Source security zone: Trust
Responder:
  Source      IP/port: 180.163.32.172/8080
  Destination IP/port: 172.16.50.181/5034
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface1
  Source security zone: Trust
State: TCP_SYN_SENT
Application: GENERAL_TCP
Start time: 2018-03-12 16:41:41  TTL: 10s
Initiator->Responder:            3 packets        152 bytes
Responder->Initiator:            0 packets          0 bytes
```

查看会话发现回来的方向没有数据包，但是出接口是内网vlan-interface 1，说明访问外网的数据从内网出去，排查路由后发现，客户配置了180.0.0.0/8 指向内网，导致某些公网地址是180网段的，没有从外网出去，从内网出去了，导致访问不通。

1.如果内网有180段的服务器，建议配置32位掩码的明细路由指向内网。

2.或者修改内网服务器网段地址，不要跟公网网段冲突。

1. 规划内网网段的时候，建议不要采用公网地址段，防止后续配置路由出现问题。