某局点SecPath F1000-AK115(V7)无法打开某个网页的经验案例

会话 丁佳欣 2021-10-13 发表

组网及说明

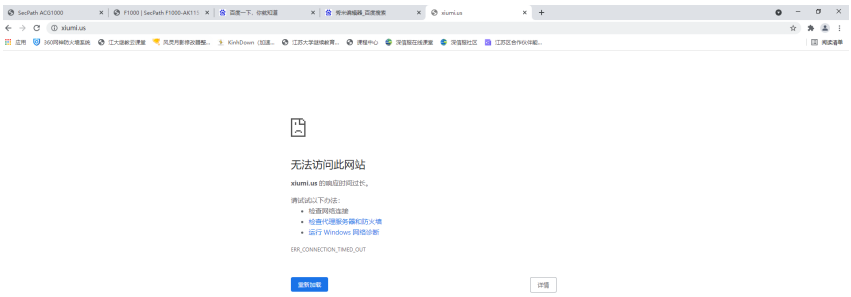
null

问题描述

现场反馈经过该防火墙无法打开某个网站，其他网站均能正常打开，且跳过设备则正常。

过程分析

1、 终端无法打开该网页，ping域名可以解析出地址



2、 根据终端ping域名解析出的公网地址，我们进一步收集会话和debug信息确认

<F1000>display session table ipv4 source-ip 182.xx.x.202（测试终端地址） destination-ip 182.254.143.92 verbose

Slot 1:

Initiator:

Source IP/port: 182.xx.x.202/2336

Destination IP/port: 182.254.143.92/443

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: TCP(6)

Inbound interface: Route-Aggregation1 //入接口是内网口聚合口1

Source security zone: Trust

Responder:

Source IP/port: 182.254.143.92/443

Destination IP/port: 182.xx.x.202/2336

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: TCP(6)

Inbound interface: Route-Aggregation1 //出接口也是内网口聚合口1

Source security zone: Trust

State: TCP_SYN_SENT

Application: HTTPS

Rule ID: 3001

Rule name: 1

Start time: 2021-10-13 14:38:47 TTL: 10s

Initiator->Responder: 320 packets 16640 bytes

Responder->Initiator: 0 packets 0 bytes

3、Debug信息也进一步确认访问该网站的流量从防火墙内网口收到后又从内网口转发出去了

<F1000>*Oct 13 14:38:46:895 2021 F1000 IPFW/7/IPFW_PACKET:

Receiving, interface = Route-Aggregation1

version = 4, headlen = 20, tos = 0

pktlen = 52, pktid = 49526, offset = 0, ttl = 127, protocol = 6

checksum = 15652, s = 182.xx.x.202, d = 182.254.143.92

channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.

prompt: Receiving IP packet from interface Route-Aggregation1.

//从聚合1口收到访问的流量

Payload: TCP
source port = 10512, destination port = 443
sequence num = 0xc9a07894, acknowledgement num = 0x00000000, flags = 0x2
window size = 64240, checksum = 0x09f6, header length = 32.

*Oct 13 14:38:46:895 2021 F1000 IPFW/7/IPFW_PACKET:
Sending, interface = Route-Aggregation1
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 49526, offset = 0, ttl = 126, protocol = 6
checksum = 15908, s = 182.xx.x.202, d = 182.254.143.92
channelID = 0, vpn-instanceIn = 0, vpn-instanceOut = 0.
prompt: Sending IP packet received from interface Route-Aggregation1 at interface Route-Aggregation1.
//从聚合1口将收到的访问流量又转发出去了
Payload: TCP
source port = 10512, destination port = 443
sequence num = 0xc9a07894, acknowledgement num = 0x00000000, flags = 0x2
window size = 64240, checksum = 0x09f6, header length = 32.

4、 进一步检查配置我们发现现场配置的内网路由存在问题
ip route-static 182.0.0.0 8 192.168.xx.x
ip route-static 183.0.0.0 8 192.168.xx.x
刚好现场访问的该网站解析地址为182.254.143.92，匹配到配置的去往内网的路由，从而流量从内网口收到后无法正常转发至外网。修改明细路由避免冲突后问题解决。

解决方法

建议现场修改路由配置，配置明细路由，避免和访问外网的流量有所冲突。