某局点M9000 sslvpn登录1分钟掉线，提示“安全认证失败”

SSL VPN　孔凡安　2024-04-07 发表

组网及说明

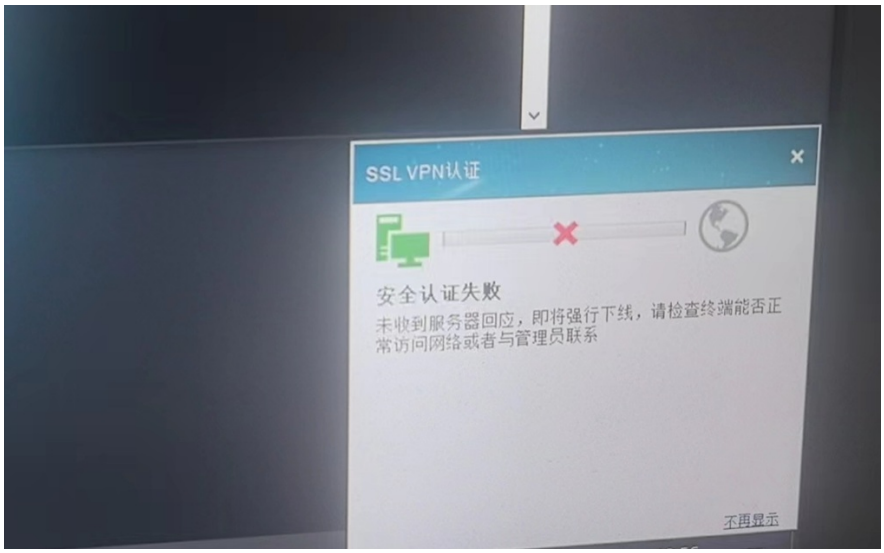
不涉及

告警信息

不涉及

问题描述

客户端登录sslvpn之后，过1分钟之后自动下线，下线原因显示：



过程分析

从下线报错来看，设备下线原因为为与认证服务器超时导致。

和现场了解到故障时ping sslvpn-ac口不通，因此针对拨号地址到sslvpn-ac接口地址写acl进行debug分析，debug内容如下：

1. 收集现网的拓扑结构，需要明确网络中设备具体的接口和IP地址以及不通时的源地址（X.X.X.X）和目的地址（Y.Y.Y.Y），ping测试。

2. 确定防火墙的入接口和出接口以及对接的安全域和安全策略规则号。

3. 开启会话统计功能：session statistics enable。并查看故障时的会话状态信息 display session table ipv4 source-ip X.X.X.X destination-ip Y.Y.Y.Y verbose （一定要带上verbose！）

4. 创建一个空ACL 3XXX，写上两条明细rule，分别对应来回流量的源目地址，如下：

[FW]acl advanced 3XXX

[FW-acl-ipv4-adv-3010]rule 0 permit ip source X.X.X.X 0 destination Y.Y.Y.Y 0

[FW-acl-ipv4-adv-3010]rule 5 permit ip source Y.Y.Y.Y 0 destination X.X.X.X 0

另外如果有NAT，假设（X.X.X.X） NAT后的地址为（A.A.A.A 会话中可以看到NAT后的地址），则需要再写上两条rule，分别对应NAT后的来回流量的源目地址，如下：

[FW]acl advanced 3XXX

[FW-acl-ipv4-adv-3010]rule 0 permit ip source X.X.X.X 0 destination Y.Y.Y.Y 0

[FW-acl-ipv4-adv-3010]rule 5 permit ip source Y.Y.Y.Y 0 destination X.X.X.X 0

[FW-acl-ipv4-adv-3010]rule 10 permit ip source A.A.A.A 0 destination Y.Y.Y.Y 0

[FW-acl-ipv4-adv-3010]rule 15 permit ip source Y.Y.Y.Y 0 destination A.A.A.A 0

5. 以安全策略security-policy为例，分别进行以下debug调试：

<FW>debugging ip packet acl 3XXX　　# 查看报文具体从哪个接口，哪个slot上来和发出的情况

<FW>debugging ip info acl 3XXX　　# 如果有丢包则会打印信息丢包的具体模块，如果没有丢包则不打印

<FW>debugging aspf packet acl 3XXX　# 如果报文状态不合法，则会显示被aspf丢弃，需检查流量来回是否一致

<FW>debugging security-policy packet ip acl 3XXX　　# 如果是对象策略则用object-policy，如果是包过滤则用packet-filter

<FW>debugging nat packet acl 3XXX　　#查看nat会话情况

如果没有会话，但是debug有报文上来，还需要收集：
<FW>debugging session session-table event acl 3XXX # 可以查看会话被删除的具体情况

6. web界面抓包使用ACL 3XXX限制，不指定接口，参数请设置最大。
如果抓包的文件过大导致分成多个文件，请用wireshark中的mergecap工具进行报文的合并。
具体可参考：
https://blog.csdn.net/qq_20480611/article/details/50774686

7. 如果是直连互ping不通，需要检查有没有对应的arp信息，如果没有arp，还得debugging arp packet acl 3XXX 查看防火墙有无arp请求发出，确定arp请求已经发出，需检查对端设备原因。

【注】如果防火墙的策略没有问题，一般会有以下情况导致报文过防火墙不通：
1，防火墙冗余口对接聚合口，回包从冗余口非激活接口上来被丢弃。
2，上送到防火墙的报文携带的VLAN标签不对称，导致报文被丢弃。
3，双主场景下，NAT配置在物理口上，流量跨框时报文会被丢弃。

来自 <http://10.88.8.36:8195/pages/viewpage.action?pageId=3834117>

<FW>debugging ip packet acl 3XXX # 查看报文具体从哪个接口，哪个slot上来和发出的情况
<FW>debugging ip info acl 3XXX # 如果有丢包则会打印信息丢包的具体模块，如果没有丢包则不打印
<FW>debugging aspf packet acl 3XXX # 如果报文状态不合法，则会显示被aspf丢弃，需检查流量来回是否一致
<FW>debugging security-policy packet ip acl 3XXX # 如果是对象策略则用object-policy，如果是包过滤则用packet-filter
如果没有会话，但是debug有报文上来，还需要收集：
<FW>debugging session session-table event acl 3XXX # 可以查看会话被删除的具体情况
<FW>debugging nat packet acl 3XXX #查看nat回话情况

解决方法

通过debug信息发现，报文被安全策略丢弃。找到对应的策略发现现场针对sslvpn地址池地址配置了策略阻断。
现场联动IMC有配置EAD检测，终端到IMC不通会强制客户端下线。
解决方案：放通sslvpn地址池地址到IMC的流量，使得终端EAD检测通过，避免强制客户端下线。