“Service ID is 11(atk), ... return 1” ---NGFW防火墙NAT不通案例分享

域间策略/安全域 **孔凡安** 2023-09-07 发表

组网及说明

不涉及，防火墙出接口做SNAT，对应配置如下：

```
#
interface Route-Aggregation51.501
 ip address 111.X.X.X 255.255.255.224
 ip last-hop hold
 nat outbound 2100 counting
```

告警信息

不涉及

问题描述

现场反馈内网客户端连接云平台连不上，防火墙出接口配置了easy-ip

```
#
interface Route-Aggregation51.501
 ip address 111.X.X.X 255.255.255.224
 ip last-hop hold
 nat outbound 2100 counting
```

过程分析

对于此类访问不通的问题，常用的思路如下：

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：
    i. [FW]acl advanced 3XXX
    ii. [FW-acl-ipv4-adv-3010]rule 0 permit ip source X.X.X.X 0 destination Y.Y.Y.Y 0
    iii. [FW-acl-ipv4-adv-3010]rule 5 permit ip source Y.Y.Y.Y 0 destination X.X.X.X 0
    iv. 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：
    v. [FW]acl advanced 3XXX
    vi. [FW-acl-ipv4-adv-3010]rule 0 permit ip source X.X.X.X 0 destination Y.Y.Y.Y 0
    vii. [FW-acl-ipv4-adv-3010]rule 5 permit ip source Y.Y.Y.Y 0 destination X.X.X.X 0
    viii. [FW-acl-ipv4-adv-3010]rule 10 permit ip source A.A.A.A 0 destination Y.Y.Y.Y 0
    ix. [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：
    i. <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
    ii. <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
    iii. <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
    iv. <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
    v. <FW>debugging nat packet acl 3XXX #查看nat会话情况
    vi. 如果没有会话，但是debug有报文上来，还需要收集：
    vii. <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。
    i. 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。
    ii. 具体可参考：
    iii. https://blog.csdn.net/qq_20480611/article/details/50774686

通过debug可以看出，回包被ATK模块丢弃。

> *Sep 2 11:52:15:186 2023 ChuKou-FW1 IPFW/7/IPFW_INFO: -COntext=1-Slot=2; MBUF was intercepted! Phase Num is 1(pre routing), Service ID is 11(atk), Bitmap is 10404000000000, return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is Route-Aggregation51.501, s= 60.209.95.131, d= 111.57.232.226, protocol= 6, pktid = 0 VsysID = 1.

于是检查设备配置，发现现场配置了扫描攻击防范：

```
#
attack-defense policy saomiaofanghu
 scan detect level user-defined port-scan-threshold 1000 ip-sweep-threshold 1000 action logging block-source timeout 10080
#
```

对应解释：

解决方法：

攻击防范策略取消或者调整阈值，以及取消动态黑名单。

scan detect命令用来配置并启指定级别的扫描攻击防范。

undo scan detect命令用来关闭指定级别的扫描攻击防范。

【命令】

scan detect level { { high | low | medium } | user-defined { port-scan-threshold threshold-value | ip-sweep-threshold threshold-value } * [period period-value] } action { { block-source [timeout minutes] | drop } | logging } *

undo scan detect

【缺省情况】

扫描攻击防范处于关闭状态。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

mdc-admin

vsys-admin

【参数】

level：指定攻击防范的检测级别。

high：表示高防范级别，该级别能检测出大部分的扫描攻击，但对活跃主机误报率较高，即将可提供服务的主机的报文错误判断为攻击报文的概率比较高。该级别的扫描攻击检测周期为10秒，针对端口扫描的防范阈值为5000 packets，针对地址扫描的防范阈值为5000 packets。

low：表示低防范级别，该级别提供基本的扫描攻击检测，有很低的误报率，但对于一些扫描攻击类型不能检出。该级别的扫描攻击检测周期为10秒，针对端口扫描的防范阈值为100000 packets，针对地址扫描的防范阈值为100000 packets。

medium：表示中防范级别，该级别有适中的攻击检出率与误报率，通常能够检测出Filtered Scan等攻击。该级别的扫描攻击检测周期为10秒，针对端口扫描的防范阈值为40000 packets，针对地址扫描的防范阈值为40000 packets。

user-defined：表示用户自定义防范规则，用户可根据网络实际情况和需求指定端口扫描、地址扫描的防范阈值和检测周期。

port-scan-threshold threshold-value：指定端口扫描攻击防范的触发阈值。其中，threshold-value为源IP地址每个检测周期内发送的目的端口不同的报文数目，取值范围为1～1000000000。

ip-sweep-threshold threshold-value：指定地址扫描攻击防范的触发阈值。其中，threshold-value为源IP地址每个检测周期内发往不同目的IP地址的报文数目，取值范围为1～1000000000。

period period-value：表示检测周期，period-value的取值范围为1～1000000000，单位为秒，缺省值为10。

action：设置对扫描攻击的处理行为。

block-source：表示阻断并丢弃来自该IP地址的后续报文。具体实现是，当设备检测到攻击发生后，会自动将发起攻击的源IP地址添加到IP黑名单动态表项中，当接口或安全域上的黑名单过滤功能处于开启状态时，来自该IP地址的报文将被丢弃。

timeout minutes：动态添加的黑名单表项的老化时间。其中，minutes表示老化时间，取值范围为1～10080，单位为分钟，缺省值为10。

drop：表示丢弃攻击报文，即设备检测到攻击发生后，由该攻击者发送的报文都将被丢弃。

logging：表示输出告警日志，即设备检测到攻击发生时，生成记录告警信息，生成的告警信息将被发送到日志系统。

根据解释可以得到结论，攻击防范设定的阈值太小，导致云平台回包命中攻击防范策略被阻断。

于是告知现场取消该策略测试，结果客户端测试还是无法连接成功。

这就很奇怪了，于是继续debug，发现报错还是一样。那么这就很尴尬了，攻击防范功能已经取消那就只剩下一种可能了。可能服务器地址被加了黑明单，通过查看果然被加了动态黑名单。