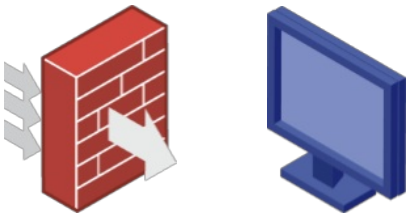
某局点SecPath F100-A-G5(V7) ping大包不通

ASPF ACL 二层转发 **刘文粟** 2022-04-28 发表

组网及说明



问题描述

PC通过access口和FW互联

小包通大包不通

过程分析

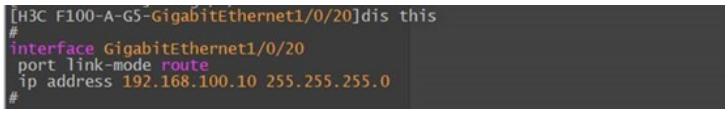
收集debug查看是检测到攻击丢掉的。

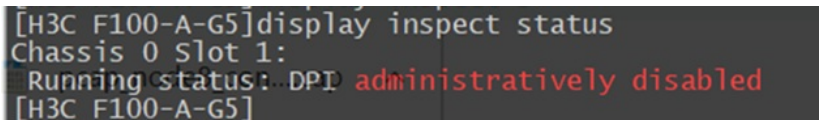
*Apr 12 11:29:51:365 2022 H3C F100-A-G5 IPFW/7/IPFW_INFO:
MBUF was intercepted! Phase Num is 1(pre routing), **Service ID is 11(atk),** Bitmap is 100000000000
00, return 1(0:continue, **1:dropped,** 2:consumed, 3:enqueued, 4:relay)! Interface is Vlan-
interface100,
s= 192. .x.x. 250, d= 192 .x.x. .10, protocol= 1, pktid = 23110
VsysID = 1.

把攻击防范关了能正常ping通了，也没有出现丢包

于是修改接口在route接口模式下，数据包大小过50000会出现不通，在bridge下反而不丢包
CPU的使用率是正常的

rule 21 name 防火墙管理
 description 允许访问防火9090和22
 action pass
 counting enable
 destination-zone Local
 service 防火墙管理端口
 service-port icmp





==========

 ==========display cpu-usage history slot 1 ==========

100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%| #

5%|##

---

10 20 30 40 50 60 (minutes)

cpu usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)

解决方法

设备接口调整100M速率

另外出现一个很奇怪的现象，收集debug的瞬间ping测试正常。

debugging ip packet acl 之前是不通的，开了后就立马通了

*Apr 12 14:26:00:169 2022 H3C F100-A-G5 IPFW/7/IPFW_PACKET:
Receiving, interface = GigabitEthernet1/0/20
version = 4, headlen = 20, tos = 0
pktlen = 1500, pktid = 65099, offset = 20720, ttl = 64, protocol = 1
checksum = 840, s = 192.x.x.20, d = 192.x.x.10
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
VsysID = 1
prompt: Receiving IP packet from interface GigabitEthernet1/0/20.
Payload: ICMP
IP packet fragment(1480 bytes).

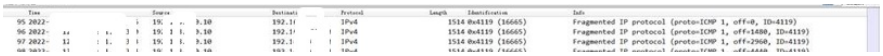
*Apr 12 14:26:00:169 2022 H3C F100-A-G5 IPFW/7/IPFW_INFO:
MBUF was intercepted! Phase Num is 0(pre all), Service ID is 7(app proxy), Bitmap is 100000000000
000, return 0(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is GigabitEthernet1/
0/20,
s= 192.x.x.20, d= 192. x.x. 10, protocol= 1, pktid = 65099
VsysID = 1.

*Apr 12 14:26:00:169 2022 H3C F100-A-G5 IPFW/7/IPFW_INFO:
MBUF was intercepted! Phase Num is 1(pre routing), Service ID is 11(atk), Bitmap is 1000000000000
0, return 0(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is
GigabitEthernet1/0/20,
s= 192.x.x.20, d= 192.x.x.10, protocol= 1, pktid = 65099
VsysID = 1.

*Apr 12 14:26:00:169 2022 H3C F100-A-G5 IPFW/7/IPFW_PACKET:
Delivering, interface = GigabitEthernet1/0/20
version = 4, headlen = 20, tos = 0
pktlen = 1500, pktid = 65099, offset = 20720, ttl = 64, protocol = 1
checksum = 840, s = 192.x.x.20, d = 192.x.x.10
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
VsysID = 1
prompt: Forwarding IP packet to upper layer.
Payload: ICMP
IP packet fragment(1480 bytes).

开启Undo attack-defense malformed-packet defend enable
开启ip virtual-reassembly enable
开启以上命令后，全都超时了

通过抓包看异常时间防火墙的reply报文发出了41个分片报文，但是电脑上抓包只收到了38-40个分片报文，是这个原因导致的；



No.	Time	Source	Destination	Protocol	Length	Identification	Info
95	2022-	1 19. . ..	).10	192.1! IPv4	1514	0x4119 (16665)	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4119)
96	2022-	.. : 1.. 3)	19. 1).	).10	192.1! .. ! IPv4	1514	0x4119 (16665)	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=4119)
97	2022-	12 : 1. 3 (| 19. 1).	).10	192.1 (! IPv4	1514	0x4119 (16665)	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=4119)