fw用全局策略nat 转换源地址和目的端口，不转换目的地址 异常//黑洞路由

NAT 小王 2024-08-27 发表

组网及说明

1.1.1.1源---------1/0/27fw-1/0/25---------目的2.2.2.2
源访问目的
fw三层部署

告警信息

不涉及

问题描述

nat global-policy
rule name test
service 8080
 source-zone DMZ
 source-ip host 1.1.1.1
 destination-ip host 2.2.2.2
 action snat address-group name test
 action dnat ip-address 2.2.2.2 local-port 80

过程分析

源nat没转，就被丢弃了
目的端口转换成功后，被黑洞路由丢弃
* SESSION/7/TABLE: -COntext=1;
Tuple5(EVENT):1.1.1.1/2133-->2.2.2.2/15900(TCP(6))
Session entry was created.
*Aug 28 01:00:12:309 2024 NAT/7/COMMON: -COntext=1;
PACKET: (Ten-GigabitEthernet1/0/27-in-config) Protocol: TCP
 1.1.1.1: 2133 - 172.21.70.7:8080(VPN: 0)(vsys: 1) ------>
 1.1.1.1: 2133 - 172.21.70.7:80(VPN: 0)(vsys: 1)
*Aug 28 01:00:12:309 2024 F047-5G-001 IPFW/7/IPFW_INFO: -COntext=1;

*Aug 28 01:00:12:309 2024 test-name IPFW/7/IPFW_PACKET: -COntext=1;
Discarding, interface = Ten-GigabitEthernet1/0/27
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 24356, offset = 0, ttl = 120, protocol = 6
checksum = 27615, s = 1.1.1.1, d = 2.2.2.2
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
VsysID = 1
prompt: FIB BLACKHOLE.
Payload: TCP
 source port = 2133, destination port = 80
 sequence num = 0xe5ce5657, acknowledgement num = 0x00000xian000, flags = 0x2
 window size = 8192, checksum = 0xbbce, header length = 32.

display ip routing-table+2.2.2.2 发现设备自动下发了到nat server 的公网地址的黑洞路由
2.2.2.2/32 Direct 2 0 0.0.0.0 NULL0
设备配置nat server global地址，会智能的下发一个防环的黑洞路由，导致我们直接按照组网图中的配置方法会导致流量命中黑洞被丢弃
nat server只做目的端口转换，不做地址转换 - 知了社区 (h3c.com)
华三F5000防火墙做nat时，源地址转换后的公网地址与防火墙接口地址不在同一个子网时，不指黑洞路由，为啥会产生环路？ - 知了社区 (h3c.com)
某局点 F5000使能NAT后日志报地址冲突的经验案例 - 知了社区 (h3c.com)

解决方法

下发黑洞路由是为了防止环路
正常的转换顺序是目的nat 路由 源nat
现在目的nat的动作只转换了端口，目的地址不变，转换后并不变目的地址匹配了下发的黑洞路由，导致丢包
是正常的机制问题导致的，目的ip和端口一起转后正常