某局点NGFW防火墙配置dhcp server无法下发地址

DHCP 孔凡安 2023-02-01 发表

组网及说明

防火墙（vlan-interface16）---PC

告警信息

无

告警信息

问题描述

新开局设备，防火墙作为DHCP服务器，终端无法获取到IP地址。

关键配置如下：

```
#
 dhcp enable
#
dhcp server ip-pool vlan16
 gateway-list 172.16.16.1
 network 172.16.16.0 mask 255.255.255.0
 dns-list 114.114.114.114
#
interface Vlan-interface16
 ip address 172.16.16.1 255.255.255.0
 dhcp server apply ip-pool vlan16
#
security-zone name Trust
 import interface GigabitEthernet1/0/17 vlan 16
#
security-policy ip
 rule 2 name any-local
  action pass
```

过程分析

1. 检查设备DHCP相关配置，查看是否遗漏，无问题。
2. 检查安全域与安全策略，接口已加入安全域，安全策略全部放通。
3. 进行debugging dhcp server的相关调试，没有回显。说明没有触发dhcp流程，怀疑是不是PC的dhcp discover没有到达防火墙。
4. 在接口抓包，发现收到PC的dhcp discover报文，防火墙未回应；此外通过debugging ip packet 也证实了防火墙已经收到来自PC的报文。

```
<H3C>*Jan 15 12:40:55:878 2023 H3C IPFW/7/IPFW_PACKET: -COntext=1;
Receiving, interface = Vlan-interface16
version = 4, headlen = 20, tos = 224
pktlen = 338, pktid = 26, offset = 0, ttl = 255, protocol = 17
checksum = 47521, s = 0.0.0.0, d = 255.255.255.255
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
VsysID = 1
prompt: Receiving IP packet from interface Vlan-interface16.
Payload: UDP
  source port = 68, destination port = 67
  checksum = 0xc3ba, length = 318.
```

5. 检查设备配置，发现存在一条全局NAT，可能与该问题有关，配置如下：

```
#
nat global-policy
 rule name nat
  source-zone Trust
  action snat easy-ip
  action dnat no-nat
#
```

尝试删除该配置后，PC能够正确获取地址。

解决方法

后续实验室复现，是因为dhcp discover报文的目的地址是广播地址走了NAT流程，但是广播地址无法做DNAT转换，会话创建失败。

解决方案：

全局NAT下配置action dnat no-nat 配置 destination-ip，新版本同样有这个限制。

示例：

```
[FW-nat-global-policy-rule-nat]action dnat no-nat

The destination address matching condition can not be null.

[FW-nat-global-policy-rule-nat]dis th

#
 rule name nat

  source-zone
Trust
  action snat easy-ip

#
```