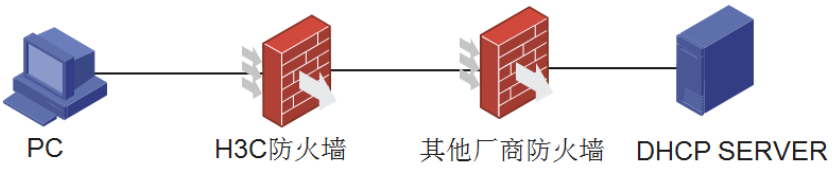
某局点F1030防火墙做DHCP中继终端无法获取地址处理经验案例

DHCP 俞璇 2019-03-19 发表

组网及说明



H3C防火墙为终端网关，并配置DHCP中继。

问题描述

H3C防火墙为终端网关，并配置DHCP中继，终端无法获取到IP地址。

过程分析

查看防火墙配置：

终端属于OA域，DHCP Server属于trust域。

```
#
interface Vlan-interface10
 ip address 29.128.0.1 255.255.255.0
 dhcp select relay
 dhcp relay server-address 10.5.32.110
 dhcp relay server-address 10.220.175.110
#
#
interface Route-Aggregation10
 ip address 29.2.0.68 255.255.255.248
#
#
security-zone name Trust
 import interface Vlan-interface10
#
#
security-zone name OA
 import interface GigabitEthernet1/0/22
 import interface GigabitEthernet1/0/23
 import interface Route-Aggregation10
#
```

现场策略全部放通，终端无法获取地址。查看会话：

```
<GuangMing-FW01>dis session table ipv4 destination-ip 10.5.32.110 verbose

Slot 1:

Initiator:

  Source      IP/port: 29.2.0.68/67

  Destination IP/port: 10.5.32.110/67

  DS-Lite tunnel peer: -

  VPN instance/VLAN ID/Inline ID: -/-/-

  Protocol: UDP(17)

  Inbound interface: InLoopBack0

  Source security zone: Local

Responder:
```

Source IP/port: 10.5.32.110/67

Destination IP/port: 29.2.0.68/67

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: UDP(17)

Inbound interface: Route-Aggregation10

Source security zone: OA

State: UDP_OPEN

Application: BOOTPS

Start time: 2019-01-17 22:36:23 TTL: 21s

Initiator->Responder: 4 packets 1312 bytes

Responder->Initiator: 0 packets 0 bytes

从会话看我司防火墙已经向服务器发送了请求，但是未收到回应，并且请求报文的源地址为我司防火墙上行接口的地址而不是DHCP中继的接口地址。由于现场工程师误解，中间其他厂商的防火墙策略未放通我司防火墙的上行口地址导致DHCP请求被阻断，无法到达DHCP Server。

解决方法

修改其他厂商防火墙配置，在策略中放通源地址为我司防火墙上行接口的地址，终端获取IP地址正常。