

知 某局点过设备NAT转发异常

NAT 陈阳 1天前 发表

组网及说明

不涉及

问题描述

设备MSR3620在出口位置，做了NAT Server，将内网一台服务器映射到公网，服务器提供了WEB服务，在WEB上可以访问服务器上的虚拟机，虚拟机地址和服务器地址一样，但是端口不同

```
interface Ten-GigabitEthernet0/X
ip address X.X.X.X 255.255.255.252
nat outbound
nat server protocol tcp global current-interface A inside 192.168.1.D 443
nat server protocol tcp global current-interface B inside 192.168.1.D Y
nat server protocol tcp global current-interface C inside 192.168.1.D Z
```

在公网访问测试，能打开WEB界面，但是访问WEB上的虚拟机时无法连接。

过程分析

在内网通过WEB界面访问虚拟机正常，说明服务器是正常的，虚拟机也是正常的，在设备debug，看到访问过程是正常的：

```
<H3C>*Nov 18 19:07:26:139 2024 H3C IPFW/7/IPFW_PACKET:
```

```
Receiving, interface = Ten-GigabitEthernet0/X
```

```
version = 4, headlen = 20, tos = 4
```

```
pkthlen = 52, pktid = 35599, offset = 0, ttl = 112, protocol = 6
```

```
checksum = 34526, s = 221.12.4.143, d = X.X.X.X
```

```
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
```

```
VsysID = 1
```

```
prompt: Receiving IP packet from interface Ten-GigabitEthernet0/X.
```

```
Payload: TCP
```

```
source port = 62060, destination port = B
```

```
sequence num = 0xc0427819, acknowledgement num = 0x00000000, flags = 0x2
```

```
window size = 64240, checksum = 0x8881, header length = 32.
```

```
*Nov 18 19:07:26:139 2024 H3C NAT/7/COMMON:
```

```
PACKET: (Ten-GigabitEthernet0/20-in-config) Protocol: TCP
```

```
221.12.4.143:62060 - X.X.X.X:B(VPN: 0)(vsys: 1) ----->
```

```
221.12.4.143:62060 - 192.168.1.D: Y(VPN: 0)(vsys: 1)
```

```
*Nov 18 19:07:26:140 2024 H3C IPFW/7/IPFW_PACKET:
```

```
Sending, interface = Vlan-interface1
```

```
version = 4, headlen = 20, tos = 4
```

```
pkthlen = 52, pktid = 35599, offset = 0, ttl = 111, protocol = 6
```

```
checksum = 56483, s = 221.12.4.143, d = 192.168.1.D
```

```
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
```

```
VsysID = 1
```

```
prompt: Sending IP packet received from interface Ten-GigabitEthernet0/X at interface Vlan-interface
```

```
1.
```

```
Payload: TCP
```

```
source port = 62060, destination port = Y
```

```
sequence num = 0xc0427819, acknowledgement num = 0x00000000, flags = 0x2
```

```
window size = 64240, checksum = 0x9905, header length = 32.
```

```
*Nov 18 19:07:26:140 2024 H3C IPFW/7/IPFW_PACKET:
```

```
Receiving, interface = Vlan-interface1
```

```
version = 4, headlen = 20, tos = 0
```

```
pkthlen = 52, pktid = 0, offset = 0, ttl = 64, protocol = 6
```

```
checksum = 38583, s = 192.168.1.D, d = 221.12.4.143
```

```
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.  
VsysID = 1  
prompt: Receiving IP packet from interface Vlan-interface1.  
Payload: TCP  
source port = Y, destination port = 62060  
sequence num = 0xca824f67, acknowledgement num = 0xc042781a, flags = 0x12  
window size = 29200, checksum = 0x0738, header length = 32.
```

```
*Nov 18 19:07:26:140 2024 H3C NAT/7/COMMON:  
PACKET: (Ten-GigabitEthernet0/X-out-session) Protocol: TCP  
192.168.1.D: Y - 221.12.4.143:62060(VPN: 0)(vsys: 1) ----->  
X.X.X.X:B - 221.12.4.143:62060(VPN: 0)(vsys: 1)
```

```
*Nov 18 19:07:26:140 2024 H3C IPFW/7/IPFW_PACKET:  
Sending, interface = Ten-GigabitEthernet0/X  
version = 4, headlen = 20, tos = 0  
pktlen = 52, pktid = 0, offset = 0, ttl = 63, protocol = 6  
checksum = 17138, s = X.X.X.X, d = 221.12.4.143  
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.  
VsysID = 1  
prompt: Sending IP packet received from interface Vlan-interface1 at interface Ten-GigabitEthernet0/  
X.  
Payload: TCP  
source port = B, destination port = 62060  
sequence num = 0xca824f67, acknowledgement num = 0xc042781a, flags = 0x12  
window size = 29200, checksum = 0xf81b, header length = 32.
```

进一步在内网测试，发现通过软件登录时，使用了443端口，而非Y端口，所以怀疑通过WEB访问时，被重定向到了一个内网端口，从公网发起访问时，没有访问到真正的服务，为验证猜测，在接口下新增如下配置，转换时端口不变，新增配置后测试访问正常。

```
nat server protocol tcp global current-interface Y inside 192.168.1.D Y  
nat server protocol tcp global current-interface Z inside 192.168.1.D Z
```

解决方法

内网服务器WEB上访问虚机经过了一次端口跳转，且跳转的是内网真实端口，所以该端口也需要在公网进行映射。