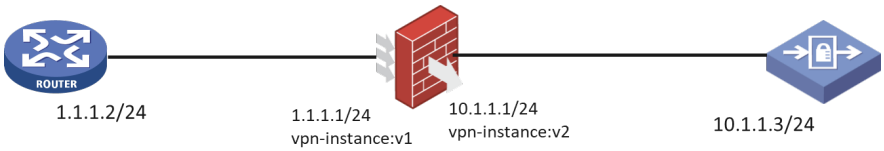
某局点跨VPN实例NAT server访问不生效分析

NAT 孔凡安 2022-04-01 发表

组网及说明



如图所示,防火墙做了vpn隔离,入接口为v1,出接口为V2.

问题描述

为方便理解，模型简化。

需求:

针对Router1.1.1.2访问1.1.1.11的流量，防火墙上配置DNAT转换

1.1.1.2:10969 - 1.1.1.11: 2048(VPN: 1) ------> 1.1.1.2:10969 - 10.1.1.3: 2048(VPN: 2)

现场需要对访问global地址的源做限制,所以采用了带有acl类型的nat server的配置方案:

```
#
acl advanced 3000
 rule 0 permit ip vpn-instance v1 source 1.1.1.2 0 destination 1.1.1.11 0
#
 nat server global 3000 inside 10.1.1.3 vpn-instance v2 rule ServerRule_1
```

结果发现访问侧无法学到global地址(1.1.1.11/24)的ARP

过程分析

关键配置:

```
#
ip vpn-instance v1
#
ip vpn-instance v2
#
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip binding vpn-instance v1
 ip address 1.1.1.1 255.255.255.0
 nat server global 3000 inside 10.1.1.3 vpn-instance v2 rule ServerRule_1
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip binding vpn-instance v2
 ip address 10.1.1.1 255.255.255.0
#
 ip route-static vpn-instance v2 1.1.1.0 24 vpn-instance v1 1.1.1.2
#
acl advanced 3000
 rule 0 permit ip vpn-instance v1 source 1.1.1.2 0 destination 1.1.1.11 0
#
security-policy ip
 rule 0 name any
 action pass vrf v2
```

分析:

1.测试采用nat server global 1.1.1.11 vpn-instance v1 inside 10.1 .1.3 vpn-instance v2的方法,发现可以正常学到1.1.1.11的ARP.

防火墙发送:*Apr 1 20:20:31:677 2022 H3C ARP/7/ARP_SEND: -COntext=1; Sent an ARP message, operation: 2, sender MAC: 0a28-9bd2-0105, sender IP: 1.1.1.11, target MAC: 0a28-b11c-0205, target IP: 1.1.1.2

发起方接收:*Apr 1 20:20:34:371 2022 H3C ARP/7/ARP_RCV: Received an ARP message, operation: 2, sender MAC: 0a28-9bd2-0105, sender IP: 1.1.1.11, target MAC: 0a28-b11c-0205, target IP: 1.1.1.2

但是这种方案不符合客户需求

2.采用案例中的方案,防火墙Global地址(1.1.1.11)不会回应发起方的ARP,只显示收到,导致访问侧不知道1.1.1.11的mac.

*Apr 1 20:24:55:082 2022 H3C ARP/7/ARP_RCV: -COntext=1; Received an ARP message, operation: 1, sender MAC: 0a28-b11c-0205, sender IP: 1.1.1.2, target MAC: 0000-0000-0000, target IP: 1.1.1.11

配置sub地址后,防火墙发送免费ARP.

*Apr 1 20:26:06:804 2022 H3C ARP/7/ARP_SEND: -COntext=1; Sent an ARP message, operation: 1, sender MAC: 0a28-9bd2-0105, sender IP: 1.1.1.11, target MAC: 0000-0000-0000, target IP: 1.1.1.11

此时,发起方可以学到防火墙的ARP.

解决方法

1. 在防火墙接口下配置sub地址

```
#
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip binding vpn-instance v1
 ip address 1.1.1.1 255.255.255.0
 ip address 1.1.1.11 255.255.255.0 sub
 nat server global 3000 inside 10.1.1.3 vpn-instance v2 rule ServerRule_1
```

2.访问侧写一条路由指到防火墙上