

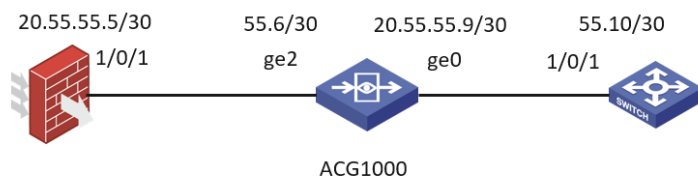
知 防火墙与交换机ping测试不通

ACG1000

zhlliao_VSolv

2022-05-25 发表

组网及说明



问题描述

现场故障现象是：在防火墙上ping ACG1000能通，ping交换机地址不通，交换机pingACG能通，交换机ping防火墙也不通，因此现场怀疑ACG导致ping测试不通

过程分析

1, 首先查看防火墙配置是否将接口加入安全域, 并放通安全策略

2, 检查路由配置

防火墙上配置路由如下

```
IP route-static 20.55.0.0 16 20.55.55.6
```

ACG上配置路由如下

```
IP route-static 20.55.0.0 16 20.55.55.10
```

```
IP route-static 0.0.0.0 0 20.55.55.5
```

交换机配置路由如下:

```
IP route-static 0.0.0.0 16 20.55.55.9
```

3, 检查安全域和安全策略没问题后, 检查ACG对报文是否丢弃:

查看debug结果, ACG对报文防火墙发过来的报文进行了转发, 但是没有收到交换机的回包, 初步排除ACG的原因导致ping不通

```
core 0 recv prot 1 packet 20.55.55.5 -> 20.55.55.10 , length 84
```

```
match rcache, send to interface ge0
```

```
core 0 recv prot 1 packet 20.55.55.5 -> 20.55.55.10 , length 84
```

```
Lookup route for ip packet, 20.55.55.5 -> 20.55.55.10 len 84 from interface ge2
```

```
lookup policy
```

```
match policy id 1, action permit
```

```
waf_hook: Waf hook process enter.
```

```
waf_hook: Waf hook process return accept.
```

```
match rcache, send to interface ge0
```

然后在交换机上debug看报文是否被丢弃

```
Debug ip packet acl 3000
```

```
Debug ip info acl 3000
```

```
Debug ip icmp acl 3000
```

其中acl 3000匹配来回流量

```
rule 1 permit ip source 10.55.55.5 0 destination 10.55.55.10 0
```

```
rule 2 permit ip source 10.55.55.10 0 destination 10.55.55.5 0
```

debug结果如下, 设备上有收发icmp, 因此怀疑设备回包并没有发到ACG上

```
*May 5 15:33:54:718 2022 BGWZ_hexin_7003X SOCKET/7/ICMP:
```

```
ICMP Input:
```

```
ICMP Packet: src = 11.57.50.5, dst = 11.57.50.10
```

```
type = 8, code = 0 (echo)
```

```
*May 5 15:33:54:718 2022 BGWZ_hexin_7003X SOCKET/7/ICMP:
```

```
ICMP Output:
```

```
ICMP Packet: src = 11.57.50.10, dst = 11.57.50.5
```

```
type = 0, code = 0 (echo-reply)
```

4, 检查交换机上路由, 发现配置了一条明细路由下一跳为另一台交换机设备, 导致报文没有发到ACG, 故障原因找到

解决方法

交换机上将此明细路由的下一跳配置为ACG

