某局点 S7606 包过滤异常

packet-filter 秦恬 2022-10-09 发表

组网及说明

服务器群---S7600----上传设备---VPN网关---VPN用户。

告警信息

不涉及

问题描述

服务器在vlan101内，IP地址为10.192.1.0/24，网关地址为10.192.1.1，使用vlan1000连接上行，走三层路由，vpn访问内网用户会转换源地址为10.188.186.24。现在再vlan101内配置inbound方向的packet-filter后，10.188.186.24地址能与服务器群主机互通，但是不能ping通10.192.1.1。ping不通网关地址的时候再76上debug ip packet 无任何信息，

过程分析

查看vlan101 inbound方向的packet-filter如下：

acl number 3000

rule 507 permit ip source 10.192.1.105 0 destination 11.222.0.117 0

rule 508 permit ip source 10.192.1.105 0 destination 11.222.0.240 0

rule 509 permit ip source 10.192.1.105 0 destination 11.222.0.12 0

rule 510 permit ip source 10.192.1.105 0 destination 11.222.0.13 0

rule 512 permit ip source 10.192.1.105 0 destination 11.222.2.200 0

rule 513 permit ip source 10.192.1.105 0 destination 11.222.2.201 0

rule 514 permit ip source 10.192.1.0 0.0.0.255 destination 10.188.186.24 0 logging

发现rule514刚好命中不通流量，被deny掉了，但是设备和10.188.186.24的交互是通过vlan1000。包过滤下发在vlan 101，按理说也不会被匹配上，不确定是不是报文从vlan 101进来了。进一步取消packet-filter查看报文交互时携带的van tag，

*Jun 28 15:52:11:487 2022 ZTF-IC-H3C-S7606 IPFW/7/IPFW_PACKET: -MDC=1-Chassis=2-Slot=2;

Delivering, interface = Vlan-interface101, version = 4, headlen = 20, tos = 0,

pktlen = 60, pktid = 3230, offset = 0, ttl = 57, protocol = 1,

checksum = 42126, s = 10.188.186.24, d = 10.192.1.1

prompt: IP packet is delivering up.

*Jun 28 15:52:11:487 2022 ZTF-IC-H3C-S7606 IPFW/7/IPFW_PACKET: -MDC=1-Chassis=2-Slot=2;

Sending, interface = Vlan-interface1000, version = 4, headlen = 20, tos = 0,

pktlen = 60, pktid = 38480, offset = 0, ttl = 255, protocol = 1,

checksum = 21723, s = 10.192.1.1, d = 10.188.186.24

prompt: Sending the packet from local at Vlan-interface1000.

现网icmp报文是从vlan 101进来，从vlan1000出去 入报文被vlan 101上下发的包过滤deny掉了，属正常现象。

解决方法

建议现场修改包过滤