F5030-D特征库服务器连接失败

特征库升级 吴欣 2024-08-19 发表

问题描述

现场防火墙为irf组网，使用管理口以及管理口VRF作为服务器在线升级源接口出现连接测试失败。

过程分析

查看配置如下：

#

failover group 1

bind chassis 1 slot 2 primary

bind chassis 2 slot 2 secondary

#

#

session synchronization enable

session synchronization dns http

#

查看设备版本说明书：

5 新增特性—特征库在线升级支持配置特征库服务器所属的VPN 实例

支持使用vpn实例。

#

inspect signature auto-update vpn-instance MGMT

inspect signature auto-update source ip interface M-GigabitEthernet1/0/0/0

#

测试时发现，可以正常进行dns解析：

测试连通性：

interface M-GigabitEthernet1/0/0/0

description To:MTRHZ5-OPM.AS-S3100-B12

ip binding vpn-instance MGMT

ip address 1.1.1.1 255.255.255.0

#

带源ip以及vpn实例可以通信。

安全域：

security-policy ip

rule 103 name any-any

action pass

disable

logging enable

counting enable

不选择接口，使用公网实例即可正常通信，

环境中有另一台防火墙可以正常使用，且解析出的ip地址一致。

尝试抓包，

抓包无法选择管理口，acl转包的话也无法捕获到报文。

查看会话：

Responder:

Source IP/port: 221.12.31.26/80

Destination IP/port: 1.1.1.1/55421

DS-Lite tunnel peer: -

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

Protocol: TCP(6)

Inbound interface: M-GigabitEthernet1/0/0/0

Source security zone: Management

State: TCP_CLOSE

Application: HTTP

链接测试的中间：

MTRHZ5-PRD.FW-F5030D-1&2]dis tcp

1.1.1.1:55420 221.12.31.26:80 ESTABLISHED 1 2 0x000000000000007d

页面提示失败后改tcp连接消失

解决方法

现场连接的为备用主控的管理口，到本机的流量需要上到IRF主主控上处理，分布式设备，必须上到一个板卡上处理才行，到本机的流量除了icmp的板卡都可以处理，其余大部分协议都是要IRF主主控进行处理。

使用主用主控的管理口后连通性正常