某局点添加两台防火墙设备后网络不通

会话 王周华 2019-06-03 发表

组网及说明

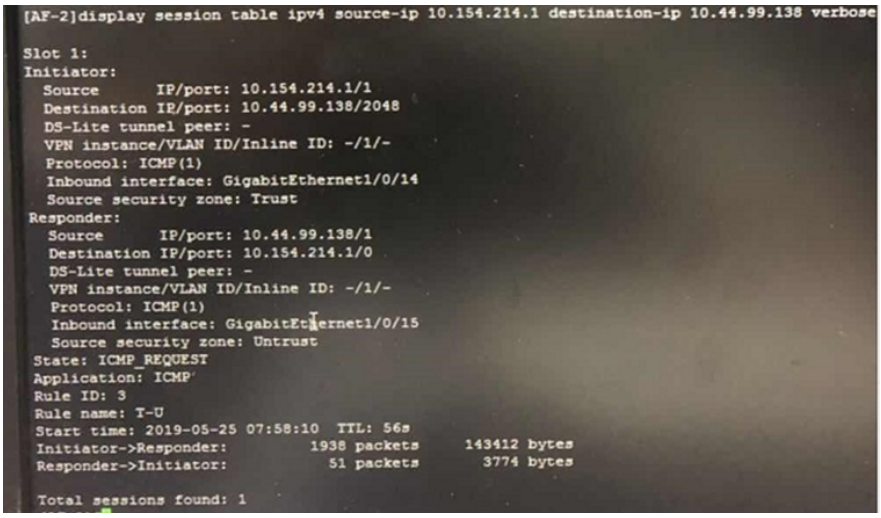
现场两台防火墙设备透明部署在出口，处于独立运行状态。防火墙型号是F1000-AK175，版本是version 7.1.064, Release 9333P17。

问题描述

反馈只部署一台防火墙时网络正常，两台同时部署时网络不通，无法访问外网的某一服务器 。

过程分析

首先确认现场的流量转发路径和安全策略是否放通，现场反馈流量是从一台防火墙转发的，查看安全策略的配置没有发现问题，让现场反馈测试流量的会话信息，可以看到发包的数量大于回包的数量，那么有可能是流量转发出去后丢失了。



让现场反馈两台防火墙的debug ip packet和debug aspf packet的信息进一步确认，发现 另一防火墙上有10.44.99.138回包被拒绝的记录，那么回包的流量部分是通过另一防火墙进行转发时被拒绝了。被拒绝的原因是无效的状态。

*May 25 17:02:10:828 2019 AF-1 ASPF/7/PACKET: -COntext=1; The first packet was dropped by ASPF for **invalid status**. Src-ZOne=Untrust, Dst-ZOne=Trust;If-In=GigabitEthernet1/0/15(16), If-Out=GigabitEthernet1/0/14(15), VLAN-In=1, VLAN-Out=1; Packet Info:Src-IP=10.44.99.138, Dst-IP=10.154.214.1, VPN-Instance=none, Src-Port=1, Dst-Port=0. Protocol=ICMP(1).

解决方法

让现场开启会话宽松session state-machine mode loose放通回包的流量后问题解决。