防火墙二层部署需要单独放通NS报文的安全策略

域间策略/安全域 **李瑞** 2022-08-25 发表

组网及说明

防火墙串联二层部署

告警信息

暂无告警

告警信息

问题描述

现场二层部署，开局放了全通策略，割接完毕后收紧策略，安全策略里限制了明细的源目地址

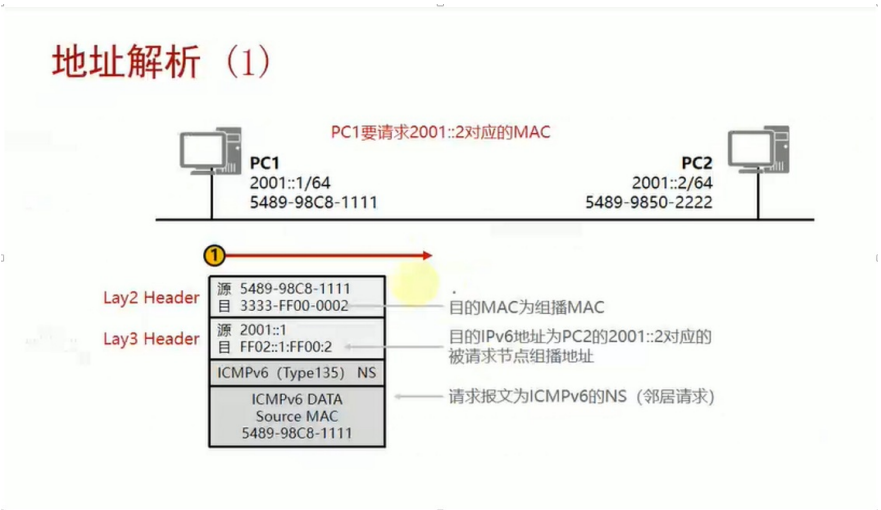
防火墙下行终端出现V6地址冲突，随后过墙V6业务全部不通，需要放全通的v6安全策略后才能恢复，后续重新收紧，业务依旧正常。

过程分析

全通策略开启日志记录，发现只有如下地址的icmp报文会命中

HZEDWFWm001CHS-F1090 FILTER/6/FILTER_ZONE_EXECUTION_ICMPV6: SrcZoneName(1025)=Untrust;DstZoneName(1035)=Trust;Type(1067)=ACL6;SecurityPolicy(1072)=test;RuleID(1078)=2;Protocol(1001)=IPv6-ICMP;SrcIPv6Addr(1036)=XXX:XXX::XXX;DstIPv6Addr(1037)=ff02::1:ff00:0;Icmpv6Type(1064)=OTHER(135);Icmpv6Code(1065)=0;MatchCount(1069)=89;Event(1048)=Deny;

目的地址是ff02::1:ff00:0 的icmpv6报文是V6的NS报文，NS报文具体构成如下：



解决方法

防火墙二层部署需要额外放通目的地址是ff02::1:ff00:0的icmpv6报文，这样NS报文才能正常透传

防火墙三层部署不需要单独放通，原因是三层默认放通了上本机的icmpv6报文