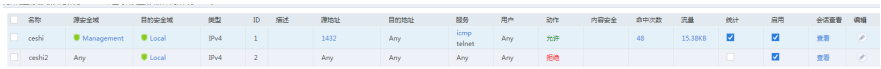
防火墙控制management域到local域，实现源地址限制

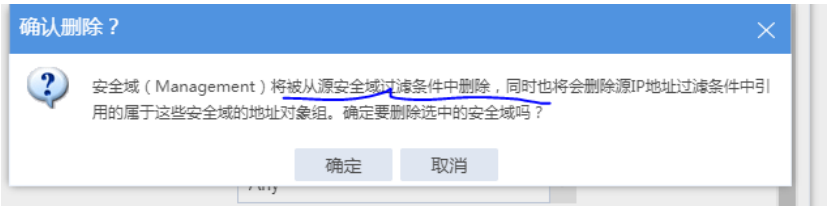
WEB管理 域间策略/安全域 王燕 2021-01-28 发表

问题描述

因为设备默认management域到local域属于全放通的状态，所以在实现允许某些ip进行访问时，需要后面再加一条拒绝策略；



但按照上面配置其实也是不成功的，因为在any安全域时候会提示下面的信息：（就any不包含management域）



解决方法

需要按照下面方式配置：

object-group ip address 1432

0 network host address 192.168.14.32 //允许访问的源地址

security-policy ip

rule 1 name ceshi

action pass

counting enable

source-zone Management

destination-zone local

source-ip 1432 //这是允许访问local的

service icmp

service telnet

rule 2 name ceshi2

source-zone Management //注明这里是重点，需要些明细的，不能写成any,否则就会匹配默认放通；

destination-zone Local