某局点SecPath F1000-AI-80(V7)安全策略不生效

域间策略/安全域 卢鹏 2天前 发表

问题描述

现场配置了到local阻断的安全策略，并且挪到了最前面，但是到local还是可以ssh通，可以ssh上和登陆web，怀疑安全策略不生效

过程分析

debug安全策略没有任何输出，查看现场配置，接口开启了manage命令

#

interface Ten-GigabitEthernet1/0/3

port link-mode route

ip address 1.5.1.28 255.255.255.248

manage http inbound

manage http outbound

manage https inbound

manage https outbound

manage ssh inbound

manage ssh outbound

#

1.1.9 manage

manage命令用来配置允许和其他设备交互的协议，指定协议的报文不受策略控制。

undo manage命令用来删除允许和其他设备交互的协议。

【命令】

manage { { **http** | **https** | **ping** | **ssh** | **telnet** } { **inbound** | **outbound** } | { **netconf-http** | **netconf-https** | **netconf-ssh** | **snmp** } **inbound** }

undo manage { { **http** | **https** | **ping** | **ssh** | **telnet** } { **inbound** | **outbound** } | { **netconf-http** | **netconf-https** | **netconf-ssh** | **snmp** } **inbound** }

【缺省情况】

仅允许和Management安全域接口相连的其他设备进行报文交互。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

http：表示HTTP协议。

https：表示HTTPS协议。

netconf-http：表示NETCONF over SOAP over HTTP协议。

netconf-https：表示NETCONF over SOAP over HTTPS协议。

netconf-ssh：表示NETCONF over SSH协议。

ping：表示Ping协议。

snmp：表示SNMP协议。

ssh：表示放行SSH协议报文。

telnet：表示放行Telnet协议报文。

inbound：放行访问设备的指定协议报文。

outbound：放行由设备主动发出的指定协议报文。

【使用指导】

当设备的某接口配置了允许通过指定协议和其他设备进行交互，则和该接口相连设备交互的指定协议报文将直接放行，不再被安全策略或带宽管理策略控制。

可以通过多次执行本命令，配置多个本机和其他设备交互的不受控协议。

解决方法

删除接口下manage命令后，安全策略匹配正常