某据点无法访问防火墙web页面的经验案例

WEB管理 姜霁琛 2020-08-20 发表

组网及说明

无

问题描述

现场从外网无法访问防火墙的https web管理页面

过程分析

检查现场配置，安全域已放通，且管理地址可以ping通，更换多个浏览器依旧，在防火墙上查看会话，发现并没有相关https会话的记录

```
#
 interface GigabitEthernet1/0/3
 port link-mode route
 ip address 183.24.70.130 255.255.255.248
#
object-policy ip untrust_to_local
 rule 1000 pass service ping
 rule 2000 pass service ssh
 rule 3000 pass service https
 rule 4000 pass service http
#
zone-pair security source Untrust destination Local
 object-policy apply ip untrust_to_local
#
security-zone name Untrust
 import interface GigabitEthernet1/0/3
#
 ip https port 2000
 ip https enable
```

进一步检查配置，发现在对象策略中，只放通了https服务，相当于只放通了443端口，而没有放通修改后的https端口2000，所以当端口为2000的https访问上来的时候会被策略丢弃，导致访问失败

解决方法

遇到此类问题，首先检查设备配置

1.接口是否绑定vpn实例

2.是否配置了http/https访问限制ip https acl xxxx

3.接口是否加入安全域，地址能否ping通

4.是否修改了https端口，安全策略中是否放通了修改后的端口，是否接口上配置了和https端口冲突的端口映射