

知 Experience case of how to deal with the issue when WEB page of firewall is not accessible

Security 姜霖琛 2021-02-27 Published

Network Topology

none

#### Problem Description

The WEB page of firewall can not be reached from Internet.

## Process Analysis

The configuration of security zone is checked, and the management address can be pinged. The type of browsers is not related with this issue. Check the session on the firewall, it is found that there is no record of related HTTPS session.

```
#
interface GigabitEthernet1/0/3
port link-mode route
ip address x.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
```

Further checking the configuration, it is found that in the object policy, only the HTTPS service is permitted, which is equivalent to port 443, but the HTTPS port is modified to 2000 by customer, and 2000 is not permitted in object policy. Therefore, when the HTTPS access with port 2000 comes up, it will be discarded by the policy, resulting in the access failure.

## Solution

In case of such issues, check the device configuration first as follows:

1. Whether the interface is bound to VPN instance;
2. Is http / HTTPS access control list configured? Command: IP HTTPS ACL XXXX ;
3. Whether the interface imported to the security zone and whether the address can be pinged;
4. Whether the HTTPS port has been modified, whether the modified port has been permitted in the security policy, and whether the port mapping has been configured on the interface which is conflicted with the HTTPS port.

