防火墙web登录问题（详细版）

WEB管理 彭钦 2024-03-21 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

现场登录某账号发现登录几次登录不上，刚开始显示登录失败，随后显示用户已被锁定，请稍后再试。再试几次登录就提示 登录失败，请检查网络是否连通，或者HTTPS服务是否启动，然后直接web界面也刷不出来。

过程分析

（1）该账户下配置了password-control，连续三次登录失败，则会被锁3min，可通过display password-control blacklist查看到。

```
local-user xxxxxxx class manage
 service-type ssh terminal https
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
 password-control aging 90
 password-control login-attempt 3 exceed lock-time 3

RBM_P[M9010_1]display password-control blacklist
 Per-user blacklist limit: 32.
 Blacklist items matched: 2.
 Username          IP address        Login failures   Lock flag
 admin             10.30.xx.xx       2                unlock
 xxxxxxx           10.30.xx.xx       3                lock
```

（2）开启了Login用户攻击防范功能，若原先已经测试了三次都密码错误，再测试两次则会被这个拉入动态黑名单。

```
 attack-defense login enable
```

attack-defense login max-attempt 5
attack-defense login reauthentication-delay 60

开启了Login用户攻击防范功能，Login用户登录失败后重新进行认证的等待时长为60s，Login用户登录失败的最大次数为5（Login用户登录失败后默认阻断时长为60分钟，Login用户登录失败5次后，若用户的IP地址被加入黑名单，则设备将会丢弃来自该IP地址的报文，使得该用户不能在指定的阻断时长内进行登录操作）。

下图一个是password-control黑名单，一个是动态黑名单：

```
RBM_P<M9010_1>display password-control blacklist
 Per-user blacklist limit: 32.
 Blacklist items matched: 1.
 Username                    IP address          Login failures   Lock flag
                             10.30.              5                lock
RBM_P<M9010_1>
RBM_P<M9010_1>
RBM_P<M9010_1>dis b
RBM_P<M9010_1>dis beacon
RBM_P<M9010_1>dis bfd
RBM_P<M9010_1>dis bl
RBM_P<M9010_1>dis bla
RBM_P<M9010_1>dis blacklist ip
CPU 0 on slot 4:
IP address      VPN instance   DS-Lite tunnel peer  Type    TTL(sec) Dropped
10.30.          management     --                   Dynamic 3558     45
CPU 0 on slot 5:
IP address      VPN instance   DS-Lite tunnel peer  Type    TTL(sec) Dropped
10.30.          management     --                   Dynamic 3558     0
CPU 1 on slot 6:
IP address      VPN instance   DS-Lite tunnel peer  Type    TTL(sec) Dropped
10.30.          management     --                   Dynamic 3558     0
```

RBM_P[M9010_1]%Mar 20 23:30:20:667 2024 M9010_1 PWDCTL/6/PWDCTL_ADD_BLACKLIST: xxxx was added to the blacklist for wrong password input.
RBM_P[M9010_1]%Mar 20 23:30:35:518 2024 M9010_1 PWDCTL/6/PWDCTL_ADD_BLACKLIST: xxxx was added to the blacklist for wrong password input.
%Mar 20 23:30:40:523 2024 M9010_1 PWDCTL/3/LOCKBLACKLIST: User xxxx was locked in 3 minutes for achieve maximum login attempts.
%Mar 20 23:33:00:219 2024 M9010_1 PWDCTL/3/USERINLOCKING: User xxxx is locking for maximum times failure loged in.

可通过debugging local-server all看是什么原因导致输入密码后失败

*Mar 20 23:36:33:920 2024 M9010_1 LOCALSER/7/EVENT:
Received authentication request message.
*Mar 20 23:36:33:921 2024 M9010_1 LOCALSER/7/EVENT:
Authentication failed, user password is wrong.

解决方法

连接console
reset password-control blacklist user-name xxxx ////清除password-control黑名单
reset blacklist ip x.x.x.x /////清除动态黑名单
或者调整password-control和attack-defense login的配置