V7 10506X交换机防暴力破解配置

AAA 攻击检测与防范 **薛佳宇** 2023-06-07 发表

组网及说明

现场设备经常可以看到日志中有提示某ip地址使用不同的、设备上不存在的用户名登陆失败的日志，希望后续再有此类情况时，将对应ip地址加入黑名单。

配置步骤

```
#
attack-defense login enable                    //开启Login用户攻击防范功能
attack-defense login max-attempt 5             /配置Login用户登录失败的最大次数为5次
attack-defense login block-timeout 100         //配置Login用户登录失败后阻断时长为100分钟，即拉黑的时长
blacklist global enable                        //开启全局黑名单过滤功能
#
```

配置完成后模拟用不存在的用户反复登陆：

```
Login: 1
Password:
E65004: User does not exist.
AAA authentication failed.
Login: 2
Password:
E65013: Password is NULL.
AAA authentication failed.
Login:
```

随后我测试的电脑就无法登陆设备了，直接显示访问目的ip超时，后续用其他电脑登陆上去发现我的ip被加入了黑名单

```
<HZB7-R5-S10506X>dis blacklist ip
IP address      VPN instance   DS-Lite tunnel peer  Type    TTL(sec)
10.40.100.191   management     --                   Dynamic 23
<HZB7-R5-S10506X>
```

配置关键点

配置手册链接：https://www.h3c.com/cn/d_202208/1663407_30005_0.htm#_Toc110522438

可参考：配置Login用户攻击防范功能

Login用户攻击防范功能处于开启状态时，如果用户登录设备连续失败的次数达到指定次数，则此用户IP地址将被加入黑名单，在全局黑名单功能开启的情况下，来自该IP地址的用户报文将被阻断指定的时长。

通过Login攻击防范功能与全局黑名单功能相配合，可以有效防范Login用户DoS攻击。