目 录

1 攻击检测及防范

1.1 攻击检测及防范简介

攻击检测及防范是一个重要的网络安全特性，它通过分析经过设备的报文的内容和行为，判断报文是否具有攻击特征，并根据配置对具有攻击特征的报文执行一定的防范措施，例如丢弃报文。

设备仅支持 TCP 分片攻击防范和 Login 用户字典序攻击防范功能。

1.1.1 TCP分片攻击

设备的包过滤功能一般是通过判断 TCP 首个分片中的五元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议号）信息来决定后续 TCP 分片是否允许通过。RFC 1858 对 TCP 分片报文进行了规定，认为 TCP 分片报文中，首片报文中 TCP 报文长度小于 20 字节，或后续分片报文中分片偏移量等于 8 字节的报文为 TCP 分片攻击报文。这类报文可以成功绕过上述包过滤功能，对设备造成攻击。

为防范这类攻击，可以在设备上配置 TCP 分片攻击防范功能，对 TCP 分片攻击报文进行丢弃。

1.1.2 Login用户字典序攻击

字典序攻击是指攻击者通过收集用户密码可能包含的字符，使用各种密码组合逐一尝试登录设备，以达到猜测合法用户密码的目的。

为防范这类攻击，可以在设备上配置 Login 用户延时认证功能，在用户认证失败之后，延时期间不接受此用户的登录请求。

1.2 配置TCP分片攻击防范

设备上开启 TCP 分片攻击防范功能后，能够对收到的 TCP 分片报文的长度以及分片偏移量进行合法性检测，并丢弃非法的 TCP 分片报文。

表1-1 配置 TCP 分片攻击防范

操作	命令	说明
进入系统视图	**system-view**	-
开启TCP分片攻击防范功能	**attack-defense tcp fragment enable**	缺省情况下，TCP分片攻击防范功能处于开启状态

1.3 配置Login用户延时认证功能

Login 用户登录失败后，若设备上配置了重新进行认证的等待时长，则系统将会延迟一定的时长之后再允许用户进行认证，可以有效地避免设备受到 Login 用户字典序攻击。

表1-2 配置 Login 用户失败延时认证功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置Login用户登录失败后重新进行认证的等待时长	**attack-defense login reauthentication-delay** *seconds*	缺省情况下，Login用户登录失败后重新进行认证不需要等待