技术介绍 攻击检测与防范

功能简介

攻击检测与防范是一个重要的网络安全功能，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相应的防御措施。

攻击检测与防范功能可针对单包攻击、泛洪攻击和扫描攻击等多类网络攻击进行有效防御。

单包攻击也称畸形报文攻击，攻击者向目标系统发送不符合协议标准的IP报文，造成目标系统出错、崩溃。

攻击者短时间内向目标系统发送大量虚假请求，导致目标系统疲于应付无用信息，从而无法提供正常服务。

攻击者运用扫描工具进行地址或端口扫描，探测目标系统的网络拓扑和开放服务端口，为进一步侵入目标系统做准备。

技术优势

以攻击防范策略形式聚合各类配置参数，方便用户进行配置和管理。

配置简便

智能阈值学习

可根据实际网络流量自适应调节攻击防范阈值，提升攻击检测精度。

支持各类攻击防范数据统计，供用户实时了解攻击防范状况。

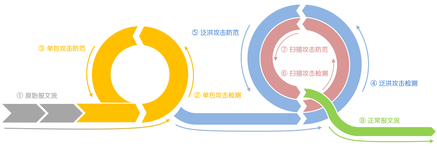
统计结果展示

防范多种攻击

可对各类常见单包攻击、泛洪攻击以及扫描攻击进行有效防范。

运行流程

攻击检测与防范由“检测”和“防范”两步骤组成。单包攻击、泛洪攻击和扫描攻击防护分别有各自的“检测”与“防范”步骤，各步骤在设备上的处理顺序如下图所示：



实现机制

单包攻击检测

单包攻击报文往往具有固定的报文格式，设备将接收到的报文与相关特征进行匹配，可有效识别单包攻击。

单包攻击防范

设备可对单包攻击报文执行丢弃操作，并支持上报单包攻击日志。

- 丢弃单包攻击报文
- 上报单包攻击日志

设备支持对如下单包攻击进行检测与防范：

ICMP redirect、ICMP unreachable、ICMP type、ICMPv6 type、Land、Large ICMP、Large ICMPv6、IP option、IP option abnormal、Fragment、Impossible、Tiny fragment、Smurf、TCP Flag、Traceroute、Winnuke、UDP Bomb、UDP Snork、UDP Fraggle、Teardrop、Ping of death、IPv6 ext-header等。

泛洪攻击检测

设备检测到来自或发往某IP的报文速率达到触发阈值，即认为存在泛洪攻击。此后，当设备监测到来自或发往该IP的报文速率低于恢复阈值，即认为攻击结束。

泛洪攻击防范

设备可对泛洪攻击报文执行丢弃或攻击源验证操作，并支持上报泛洪攻击日志。

提示：

攻击源验证是一套主动防护机制，通过“连接一接战一响应”协议使设备能够主动向报文源地址发起验证，判断其是否为虚假源，设备将丢弃来自虚假源的报文。

- 丢弃泛洪攻击报文
- 泛洪攻击源验证
- 上报泛洪攻击日志

设备支持对如下泛洪攻击进行检测与防范：

SYN flood攻击、ACK flood攻击、SYN-ACK flood攻击、FIN flood攻击、RST flood攻击、UDP flood攻击、ICMP flood攻击、ICMPv6 flood攻击、DNS flood攻击、DNS reply flood攻击、HTTP flood攻击、SIP flood攻击。

扫描攻击检测

设备通过监测网络用户向目标系统发起连接的速率来检测其探测行为。如果设备监测到某IP发起连接的目的IP或目的端口变化频率超过阈值，则判定该IP正在发起扫描攻击。

扫描攻击防范

设备可对扫描攻击报文执行丢弃或阻断报文源操作，并支持上报扫描攻击日志。

提示：

阻断报文源意味着在一定时间内，丢弃来自报文源IP地址的后续报文。

- 丢弃扫描攻击报文
- 阻断扫描攻击报文源
- 上报扫描攻击日志

设备支持对如下扫描攻击进行检测与防范：

IP Sweep攻击、Port Scan攻击。

典型应用

保护设备本身

在本机应用攻击防范策略，对目的为设备本身的各类网络攻击进行有效防范。

保护下游服务器

在设备接口或安全域上应用攻击防范策略，保护下游服务器、主机免受各类网络攻击侵害。