# 1.文档说明

## 1.1作者

作者, 版本

|  |  |  |
| --- | --- | --- |
| 项目 | 版本说明 | 作者 |
| DDoS | V0.1 | 高鹏举 |

## 1.2阅读前提

了解DDoS攻击及防护原理

了解Openresty的基本运行原理

了解Lua预言

## 1.3文档说明

本文档描述基于openresty的七层DDoS防护的策略管理部分，涉及策略的范围、策略组织结构、和策略下发和生效的过程。

# 2需求分析

策略的配置是针对域名对象的配置。全局的情况下，默认是访问该域名内的任意URL。

防护级别：

关闭->低->中->高

根据防护级别，选用具体的CC防护算法:

低 -> 基于URL参数的302跳转

中 -> 基于JS的302跳转

高 -> 基于图片验证的302跳转

触发防护阈值：对客户不可见，需要程序自己来学习。

二种：1、针对某URL的访问超过阈值；

2、某源IP的URL访问超过阈值；

针对上面二种情况，分别防护针对某URL对象，或防护某源IP的流量

连接控制

限制指定源IP的连接速率 --限制指定源IP的TCP连接速率

限制指定源IP的请求速率 --限制指定源IP的http请求速率

限制对该域名的访问速率 --不限制源，仅限制对该域名的访问速率

限制对指定URL的访问速率 --不限制源，仅限制对指定URL的访问速率

限制指定源IP的URL请求速率 --限制指定源IP对指定URL的请求速率

限制任意确定源IP访问确定URL的请求速率 --限制任意的某个源访问某个URL的速率，相当于针对每一个(源IP->URL)对做速率的限制

黑白名单设置：

IP黑名单（支持访问特定域名的设置）

IP白名单（支持访问特定域名的设置）

URL白名单（支持特定源IP的设置）

HTTPS防护

开->关

限制指定源IP的连接速率 --限制指定源IP的tcp连接

限制指定源IP访问指定目的IP的连接速率　–限制指定源对指定目的IP的连接速率

# 3技术方案

3.1策略管理的进程示图

该进程示图主要描述策略管理在系统内部的进程交互情况。包括设备外部配置数据的来源接口，设备内部各进程对配置数据的处理过程。

1. ZK数据：设备集成ZKserver和外部的EM设备对接。保证配置数据的下发和同步。
2. 管理进程：
3. 配置管理进程，主要是与ZKserver交互，读取配置信息。Watch配置的修改，当配置有变更时，转换配置到配置文件，并触发引擎加载。
4. 监听CLI的命令，支持设备本地的策略配置。该配置只修改本地的配置文件，使本地设备生效。不上传到ZKserver。
5. 防护引擎：基于openresty的防护进程。主要读取配置文件，按配置来进行相应的七层防护功能。



3.2进程交互图

该交互图主要描述各进程在对配置部分的读取和加载的过程。主要明确策略管理过程业务的需求，然后再确定具体的实现技术和方案。



主要过程如下：

1. 设备刚启动，策略管理进程和引擎都运行起来。
2. 引擎加载上次配置的数据或默认的配置文件
3. 设备端ZKserver和EM进行数据同步
4. 配置管理进程把ZK内部的配置转换成引擎识别的配置文件
5. 配置管理进程向引擎发送加载全部配置信号，进行加载。
6. 运行过程中，有策略变更。则策略管理进程通知引擎，进行加载。如果加载该策略失败，则保持原来的策略。并记录日志。
7. 加载成功则继续运行。

3.3． ZK数据格式

ZK的配置数据组织结构如下：

/sys节点下面保存系统配置的数据，log\_level:日志的级别，log\_timeout:日志输出的周期。

/policy下放策略配置的信息，其下每个子节点以防护的域名字为节点名字，节点的内容为该域名的所有配置项。为了减少watch的数量，把一个域名的配置项放到一个节点内。节点内部项的修改，都会导致该域名的配置被重新加载。由于黑名单和白名单数量比较大，单独拆出来，放到/policy\_data节点下面。也是对应相应的域名为子节点，下面分开放黑名单和白名单。在修改配置时，要保证policy\_data下的数据被修改时，也要同时写policy相应的节点来触发配置更新。

每个域名节点内是具体的配置项，具体如下：

/policy/domain节点内容：

1. 分二部分：防护级别和限速
2. 防护级别 protect\_level：

level：关、低、中、高

threshold\_url：访问某URL的速率门限值，超过后触发防护

threshold\_srcip:某源IP访问速率门限值，超过后触发防护

1. 限速 qos：

https:是否开启https的防护

srcip:限速的源IP

url:限速的访问的url

each\_srcip:是否对每IP实施策略，开启时，不能配置具体的srcip

each\_url: 是否对每url实施策略，开启时，不能配置具体的url

白名单 trust\_list：

节点位置：/policy\_data/trust\_list/domain/listnode

srcip: 信任的源IP

url:信任的url

1. 黑名单 block\_list：

节点位置：/policy\_data/block\_list/domain/listnode

srcip:黑名单源IP

url: 黑名单url



# 4风险点

## 4.1待确认

## 4.2风险点