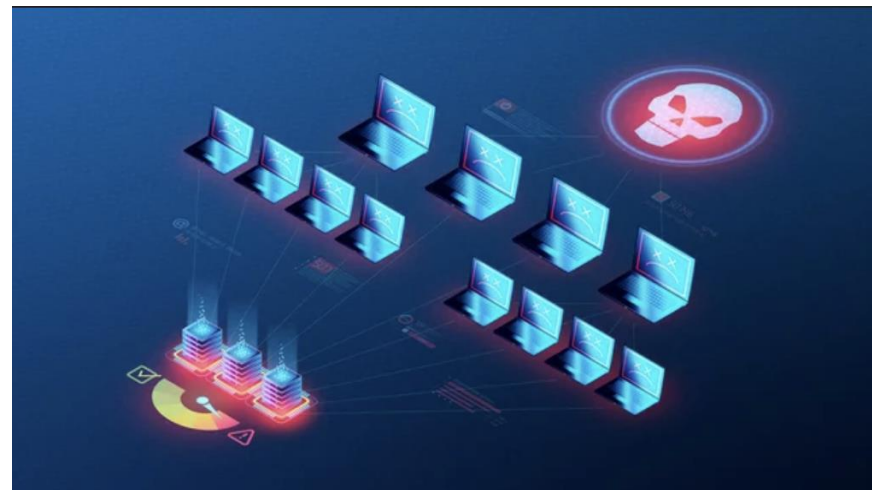


OpenResty DDoS 产品介绍

OpenResty Inc. 公司出品
2023.4




A hand is pointing towards the right side of the frame. The background is a dark blue gradient with a glowing, wavy pattern of light blue lines that resemble a digital data stream or network traffic. The lines are composed of small, faint characters and symbols, creating a sense of motion and depth. The overall aesthetic is futuristic and technical.

基于 Linux 内核的 XDP 技术

- 在进入 Linux 内核协议栈之前处理网络包，甚至在内核分配 `struct sk_buff` 数据结构之前。
- 可以在网卡驱动程序甚至网卡内部直接运行 DDoS 检测、分类和保护代码。
- 性能接近 DPDK，几百万和几千万 PPS（网络包每秒）的处理性能。
- 不会像 DPDK 那样独占网卡，可以和现有的内核协议栈及应用一起工作。
- 不会像 DPDK 那样会热轮询，不会浪费 CPU 资源。
- 不会像 DPDK 那样仅限少数类型的网卡，可以支持绝大多数网卡，包括公有云的虚拟网络。



基于 OpenResty Inc. 公司的 eBPF+ 技术

- 可以和较老的内核一起工作（如 Red Hat 4.18 内核）并同时享受很多最新的内核特性。
 - eBPF 程序拥有真正的图灵完全的灵活度，并同时保有安全性（通过我们私有的编译期和运行期沙箱）。
 - 复杂 eBPF 程序的加载速度有了数量级的提升，开源实现会耗费大量的 CPU 时间加载程序，且很可能会阻塞很久并超时。
 - 程序编译和运行总是发生在不同的机器上，确保生产系统上无需安装编译器工具链、内核头文件等很多无关依赖。
- 

已支持或即将支持的 DDoS 攻击检测与防护

- DNS water torture attacks
- DNS reflection attacks
- SYN flood attacks
- ACK flood attacks
- Slowloris attacks
- TLS/SSL exhaustion attacks
- ICMP/NTP/Memcache flood attacks
- 以及更多.....



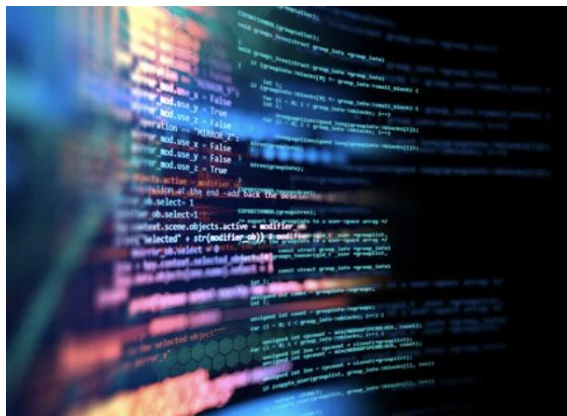
内建的 DDoS 检测与防护

- 自动过滤非法域名的 DNS 或 SSL/TLS 包。
- 自适应地针对来源 IP 地址、IP 地址段、地理位置区域进行包限速或屏蔽。
- 通过在线增量式机器学习模型自动学习正常流量包，并自动识别出异常流量包并采取限速或屏蔽动作。



即将支持 pcap filter 语言规则

- 用户可以使用流行的 pcap filter 语法自定义 DDoS 检测规则。
- 主控系统会自动编译规则为防护程序，进行高效地筛选和过滤。
- 未来会考虑支持更强大的 Wireshark 规则语言。



```
tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) -  
((tcp[12]&0xf0)>>2)) != 0)
```

```
tcp[tcpflags] & (tcp-syn|tcp-fin) != 0 and not  
src and dst net localnet
```

即将支持 p0f 网络包指纹模式定义

- 自动将 p0f 包指纹模式编译成 DDoS 平台的识别和防护条件

```
*:128:0:*:16384,0:mss,nop,nop,sok:df,id+:0
```

```
*:128:0:*:65535,0:mss,nop,nop,sok:df,id+:0
```



RegeX

即将支持 Perl 兼容 正则表达式过滤

- 用户使用自定义正则表达式描述复杂的包匹配和过滤条件。
- 使用 OpenResty Regex 优化编译器编译成高效的 eBPF 程序。
- 自动合并多条正则模式为一个状态机，最小化扫描次数。
- 在正则模式集一定时，在算法上保证 $O(n)$ 的时间复杂度（相对于扫描的数据包的数据量）和 $O(1)$ 的空间复杂度（与数据包的数量和大小无关）
- 可选的内核级别 SIMD 向量化指令优化（同时支持 Intel AVX 指令集和 Aarch64/ARM64 NEON 指令集）。



DDoS 攻击和防护细节的实时监控能力

- 当前的攻击流量和过滤后流量的 PPS 和带宽占用
- 当前自动或手动检测到的攻击类型
- 当前 DDoS 限速和屏蔽的实时细节统计
- 基于采样的正常流量通过率自动检查

部署方式

- 可作为 OpenResty Edge 的插件部署。
- 由 OpenResty Edge Admin 对众多边缘节点的 DDoS 防护进行集中式管理。
- 无须和 Edge Node 网关服务器部署在同一台服务器上（也支持部署在一起）。
- 由特殊的最小化过的 Edge Node 服务进程来自动管理（也支持复用同一台机器上现有的 Edge Node 服务进程来管理）。



联系我们

- 欢迎发送电子邮件到 info@openresty.com 询问
- 欢迎访问我们的官方网站 openresty.com.cn

