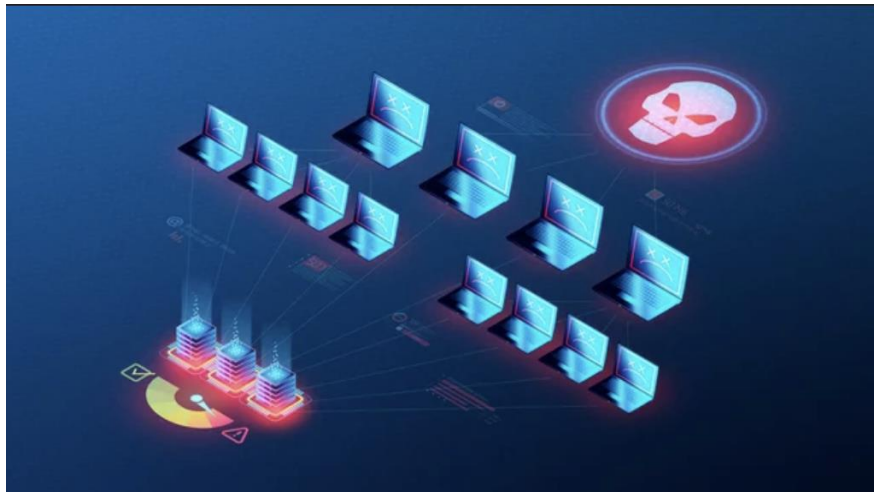
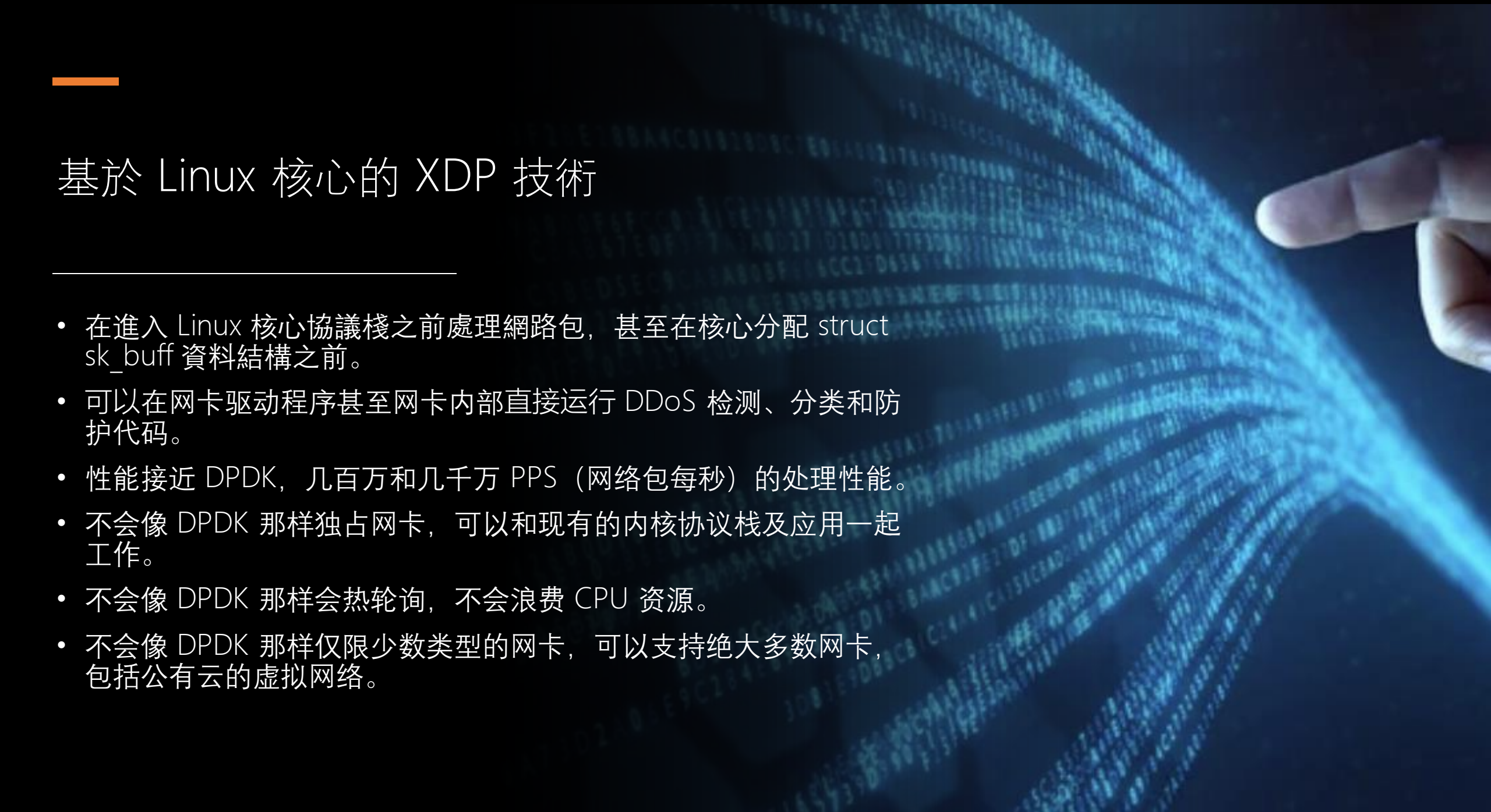
OpenResty DDoS 產品簡介



OpenResty Inc. 公司出品

2023.4

基於 Linux 核心的 XDP 技術



- 在進入 Linux 核心協議棧之前處理網路包，甚至在核心分配 struct sk_buff 資料結構之前。
- 可以在网卡驱动程序甚至网卡内部直接运行 DDoS 检测、分类和防护代码。
- 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。

基於 OpenResty Inc. 公司的 eBPF+ 技術

- 可以和較老的內核一起工作（如 Red Hat 4.18 內核）並同時享受很多最新的內核特性。
- eBPF 程式擁有真正的圖靈完全的靈活度，並同時保有安全性（通過我們私有的編譯期和運行期沙箱）。
- 複雜 eBPF 程式的載入速度有了數量級的提升，開源實現會耗費大量的 CPU 時間載入程式，且很可能會阻塞很久並超時。
- 程式編譯和運行總是發生在不同的機器上，確保生產系統上無需安裝編譯器工具鏈、內核頭檔等很多無關依賴。

已支援或即將支援的 DDoS 攻擊檢測與防護

- 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……

內建的 DDoS 檢測與防護

- 自動過濾非法功能變數名稱的 DNS 或 SSL/TLS 包。
- 自適應地針對來源IP位址、IP位址段、地理位置區域進行包限速或遮罩。
- 通過在線增量式機器學習模型自動學習正常流量包，並自動識別出異常流量包並採取限速或遮罩動作。

即將支援pcap filter語言規則

- 用戶可以使用流行的pcap filter語法自定義 DDoS 檢測規則。
- 主控系統會自動編譯規則為防護程序，進行高效地篩選和過濾。
- 未來會考慮支援更強大的Wireshark規則語言。

```
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
```

即將支援 p0f 網路包指紋模式定義

- 自動將 p0f 包指紋模式編譯成 DDoS 平台的識別和防護條件

```
*:128:0:*:16384,0:mss,nop,nop,sok:df,id+:0
*:128:0:*:65535,0:mss,nop,nop,sok:df,id+:0
```

即將支援 Perl 相容正則表達式過濾

- 使用者使用自定義正則表示式描述複雜的包匹配和過濾條件。
- 使用 OpenResty Regex 優化編證器編譯成高效的 eBPF 程式。
- 自動合併多條正則模式為一個狀態機，最小化掃描次數。
- 在正則模式集一定時，在演算法上保證O（n） 的時間複雜度（相對於掃描的數據包的數據量）和O（1） 的空間複雜度（與數據包的數量和大小無關）
- 可選的內核級別 SIMD 向量化指令優化（同時支援 Intel AVX 指令集和 Aarch64/ARM64 NEON 指令集）。

DDoS 攻擊和防護細節的實時監控能力

- 當前的攻擊流量和過慮後流量的 PPS 和頻寬佔用
- 當前自動或手動檢測到的攻擊類型
- 當前 DDoS 限速和遮罩的即時細節統計
- 基於採樣的正常流量通過率自動檢查

佈署方式

- 可作為 OpenResty Edge 的外掛程式佈署。
- 由 OpenResty Edge Admin 對眾多邊緣節點的 DDoS 防護進行集中式管理。
- 無須和Edge Node閘道伺服器佈署在同一台伺服器上（也支援佈署在一起）。
- 由特殊的最小化過的Edge Node服務進程來自動管理（也支持複用同一台機器上現有的Edge Node服務進程來管理）。

聯繫我們

- 歡迎發送電子郵件到 info@openresty.com 問詢
- 歡迎訪問我們的官方網站 openresty.com.cn