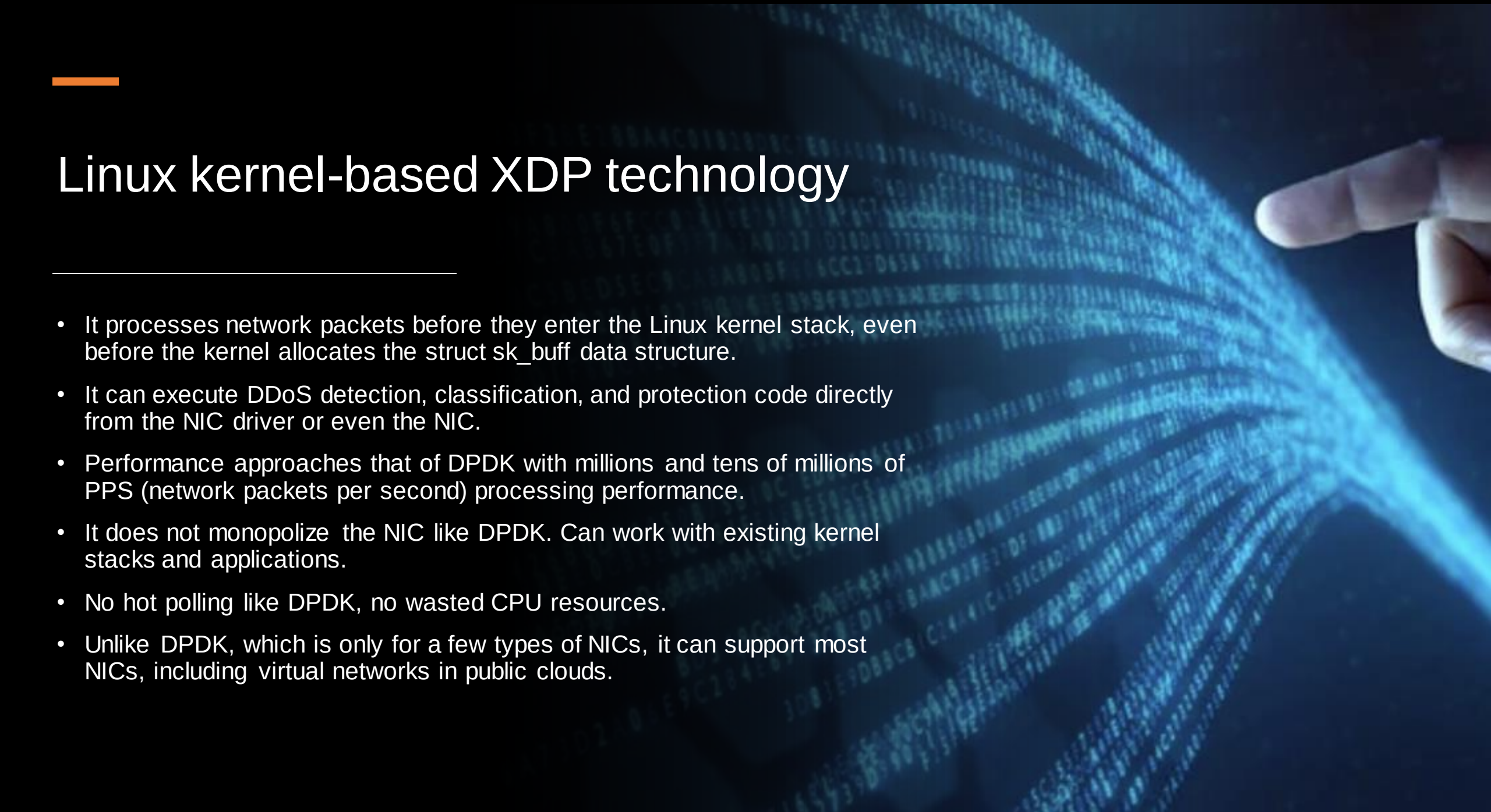
# Introduction to OpenResty DDoS

Produced by OpenResty Inc.

2023.4

# Linux kernel-based XDP technology



- It processes network packets before they enter the Linux kernel stack, even before the kernel allocates the struct sk_buff data structure.
- It can execute DDoS detection, classification, and protection code directly from the NIC driver or even the NIC.
- Performance approaches that of DPDK with millions and tens of millions of PPS (network packets per second) processing performance.
- It does not monopolize the NIC like DPDK. Can work with existing kernel stacks and applications.
- No hot polling like DPDK, no wasted CPU resources.
- Unlike DPDK, which is only for a few types of NICs, it can support most NICs, including virtual networks in public clouds.

# eBPF+ technology based on OpenResty Inc.

- Can work with older kernels (such as the Red Hat 4.18 kernel) and benefit from many features of the latest kernel.
- eBPF programs have the full Turing-complete flexibility while maintaining security (through our private compile-time and run-time sandboxes).
- The speed of loading complex eBPF programs has improved greatly. Open-source implementations take a lot of CPU time to load programs and are likely to crash for a long time and cause timeouts.
- Programs are always compiled and run on different machines, which ensures that many extraneous dependencies, such as compiler toolchains, kernel headers, etc., do not need to be installed on production systems.

# DDoS attack detection and protection supported or to be supported

- DNS water torture attacks
- DNS reflection attacks
- SYN flood attacks
- ACK flood attacks
- Slowloris attacks
- TLS/SSL exhaustion attacks
- ICMP/NTP/Memcache flood attacks
- And more…

# Built-in DDoS detection and protection

- Automatically filters DNS or SSL/TLS packets from illegal domains.
- Adaptively rate limits or blocks packets targeted to source IP addresses, IP address segments, and geographic regions.
- Learns normal traffic packets through online incremental machine learning models and automatically identifies abnormal traffic packets and takes action to limit or block them automatically.

# Support for pcap filter language rules is coming soon

- Users can customize DDoS detection rules using the popular pcap filter syntax.
- The main control system automatically compiles the rules into a protection program for efficient screening and filtering.
- Support for more powerful Wireshark rule languages will be considered in the future.

```
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
```

# Support for p0f network fingerprint pattern definitions is coming soon

Compiles p0f packet fingerprinting patterns into DDoS platform identification and protection conditions automatically

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


# Support for Perl-compatible regular expression filtering is coming soon

- Users use custom regular expressions to describe complex package matching and filtering conditions.
- Compile into efficient eBPF programs using the optimized OpenResty Regex compiler.
- Merge multiple regular patterns into one state machine automatically, minimizing the number of scans.
- Ensures O(n) time complexity (relative to the amount of data in the scanned packets) and O(1) space complexity (independent of the number and size of packets) in the algorithm when the set of regular patterns is certain.
- Optional kernel-level SIMD vectorized instruction optimization (supports both the Intel AVX instruction set and the Aarch64/ARM64 NEON instruction set).

# Real-time monitoring capabilities for the details of DDoS attacks and protection

- PPS and bandwidth usage of current attack traffic and filtered traffic.
- The type of attack currently detected automatically or manually.
- Real-time statistics detail the current DDoS rate limiting and blocking.
- Automatic testing based on samples of normal traffic performance.

# Deployment options

- Can be deployed as an OpenResty Edge plug-in.
- Centralized management of DDoS protection for many edge nodes by OpenResty Edge Admin.
- Does not have to be deployed on the same server as the Edge Node gateway server (CAN be deployed on the same server).
- Automatically managed by special minimized Edge Node service processes (also supports reusing existing Edge Node service processes on the same machine for management).

# Contact us

- Feel free to send an email to info@openresty.com
- Please visit our official website openresty.com