APPLICATION AWARENESS

FIRST PACKET CLASSIFICATION: EXECUTE NETWORK POLICIES INSTANTLY

Maximize performance for networking and cybersecurity

Speed up traffic filtering with first packet classification technology from ipoque. Detect applications and services in real-time from the very first packet, and execute network policies fast and without latency.

Background

The rise of latency-sensitive applications, such as video streaming and VoIP, and the overall growth in traffic volumes, require accelerated traffic detection. It enables networking and cybersecurity solution providers to speed up traffic steering and policy execution, and streamline these to the type of traffic. It also helps vendors balance network costs against application SLAs and user QoE requirements.

Challenges

Most traffic filtering tools require at least 3 - 5 packets to accurately identify the underlying applications and services. This detection lag often leads to partial or delayed processing. It also creates decision inconsistencies at the flow level, disrupts the order of packets, and in some cases, causes packet loss. These shortfalls eventually impact application performance through added latencies and buffering, and impair threat detection speeds. They also leave networking and cybersecurity solution providers resorting to overly complex tools or multi-vendor implementations, both of which increase processing redundancies and inefficiencies.

The solution

First packet classification (FPC) addresses these challenges by identifying a flow from the very first packet received, instead of waiting for additional packets, co-flows or the entire flow. This way, policies can be executed from the first packet itself, ensuring immediate processing and flow-wide consistency, and as a result, better service experience. ipoque, a Rohde&Schwarz company and an industry leader in network analytics solutions, offers FPC as part of its OEM deep packet inspection (DPI) engine, R&S®PACE 2. The engine classifies thousands of protocols, applications and services, and extracts metadata.

FPC is delivered via FPC-IP, DNS cacher engine (DECA) and Service cacher engine (SECA):

- **FPC-IP:** Uses commercially available IP lists to classify services and selected enterprise applications, such as Microsoft 365, Outlook, SharePoint and Teams. It not only runs on TCP-SYN packets but also on the first packet of any mid-stream flow. Can be seamlessly updated with DPI insights from subsequent packets or co-flows.
- **FPC-DECA:** Delivers FPC by leveraging DNS information from non-encrypted DNS connections. Used to classify flows for a basic level of application awareness, without the need for a full DPI solution. Caters for simplified, lightweight filtering.
- **FPC-SECA:** Leverages information that is cached from ipoque's DPI engine and brings FPC-readiness for traffic detection methods without built-in FPC. Appropriate for traffic with no caching or proxies involved. Retains existing traffic detection methods while stepping up flow detection speeds.

These techniques come with weekly-updated traffic intelligence ensuring vendors stay ahead of the latest traffic trends.

Results

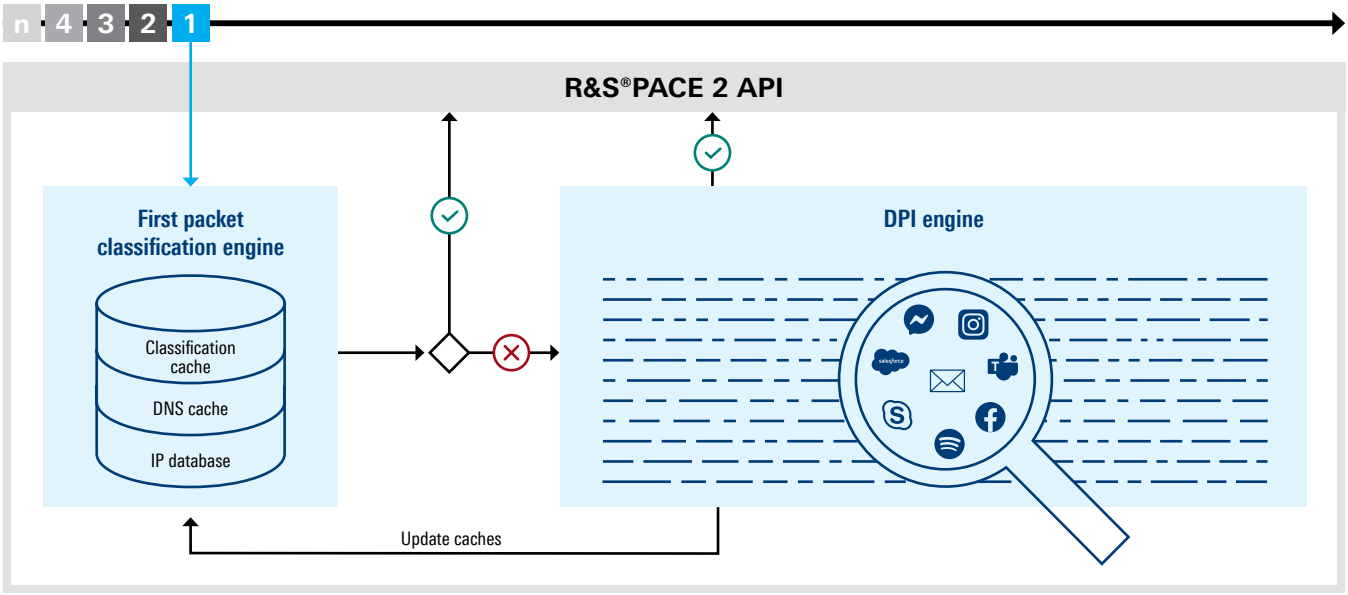
Due to FPC, networking and cybersecurity vendors can execute traffic rules from the first packet of a flow, with high perfomance and low resource cost. At the very least, FPC supports traffic policies mapped to high-level identifiers, such as CDNs. With subsequent analysis using advanced DPI, these vendors can qualify the initial results while digging deeper into service level attributes (e.g. audio, chat). Encrypted traffic intelligence by ipoque additionally enables vendors to extend this to encrypted, obfuscated and anonymized flows. Where standard DPI cannot be applied, FPCs provides basic-level traffic visibility.

Use cases

Networking and cybersecurity solutions such as SD-WAN, network packet brokers (NPBs), SASE and SSE benefit significantly from FPC. Here are some examples:

- **FPC for SD-WAN**
  SD-WAN introduces smart, traffic-aware routing for branch offices and work-from-anywhere employees: There, enterprise applications (e.g. proprietary ERP) are delivered via dedicated MPLS links while cloud / SaaS traffic (e.g. Teams or Sharepoint) is offloaded to the Internet instead of being backhauled to the data center. FPC plays an important role in SD-WAN edge filtering by identifying a flow upon commencement. This enables routing policies to be invoked from the first packet itself. With bandwidth allocated intelligently from the start, network costs and efficiencies are greatly improved. FPC also ensures low-latency transmission, for example, across a remote surgery app used by a hospital, with packets routed instantaneously and consistently.
- **FPC for networking and cybersecurity providers**
  NPBs aggregate traffic flows from routers, switches and TAPs. The flows are filtered, load balanced and distributed intelligently using application-based policies. FPC-IP powers NPBs with fast initial classification, upon which these policies are executed. These actions can be fine-tuned with more detailed classification from R&S®PACE 2, for example, an online meeting application can be classified further into an audio or video service. Using FPC-IP, an NPB can maintain traffic latency during processing, and avoid traffic buffering and bottlenecks, despite heavy traffic volumes and complex forwarding rules.

By deploying R&S®PACE 2 for real-time traffic intelligence, vendors will have immediate access to FPC and its benefits. FPC from ipoque is also available via its VPP-based DPI engine, R&S®vPACE.



ipoque GmbH
A Rohde&Schwarz Company
Augustusplatz 9, 04109 Leipzig
Info: +49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 3672.9609.32 | Version 01.00 | March 2024
First packet classification: Execute Network Policies instantly
Data without tolerance limits is not binding | Subject to change

3672960932

3672.9609.32 01.00 PDP 1 en