TOP 10 CHECKLIST FOR SOURCING DPI SOFTWARE

- High detection rate
- Performance and efficiency
- Accuracy
- Identification of encrypted apps
- Ease of integration
- Metadata extraction
- Frequency of updates
- Global application visibility
- Flexibility
- In-house engineers and developers

High detection rate
Reliable DPI software should be able to detect over 95% of traffic in networks, including the latest and newest protocols and applications along with frequent version updates. A high detection rate can only be achieved through maintaining a DPI software library on a regular basis. Before selecting a partner, in-house engineers will typically carry out performance tests based on real traffic data to determine application detection rates.

Performance and efficiency
DPI software is designed to inspect packets at high wire speeds, where the throughput and required resources are critical factors. It is crucial to keep the amount of resources that integrated DPI and application classification technology requires at a low level. The fewer cores (on a multi-core processor) and the less on-board memory a DPI engine needs, the better. Multi-threading provides almost linear scalability on multi-core systems. In addition, highly optimized flow tracking is required for handling millions of concurrent subscribers.

Accuracy
It is critical for certain use cases, such as policy control and charging, that applications are identified correctly to avoid false positives. In addition, traffic management and policy control require a very low false negative rate, i.e. a low classification rate of applications. Advanced DPI techniques can reliably detect network protocols, even if they use advanced obfuscation and encryption techniques. Applications can also be grouped into service types, e.g. video, P2P, VoIP, IM, making it easier to analyze and enable intelligent traffic decisions rather than individual protocols.

Identification of encrypted apps
It has become harder to identify applications with every fourth protocol and every fourth application now being encrypted, e.g. Skype, WhatsApp, BitTorrent, Facebook, Twitter, Dropbox, Gmail, Office 365 or Instagram. In addition, some protocols, e.g. Skype and other P2P apps, can adapt to circumvent firewalls and DPI detection when, for example, traffic for a specific protocol is limited or blocked. Advanced DPI uses a variety of detection techniques, including finite state machine, byte pattern matching and behavioral analysis to accurately identify applications.

Ease of integration

This is a key selection criteria since DPI software needs to be integrated into a vendor's existing hardware or software environment (e.g. into any Windows and Unix environment, such as Linux, BSD, Mac OS, Solaris etc.), including both C and Java APIs. In addition, it's important that thorough documentation is provided, including fully documented APIs and code samples. Usually, DPI software is sold as an SDK, with integration requiring just a couple of API calls. In addition, some providers offer network traffic test tools which double-check the validity of an integration and provide a deeper understanding for use cases.

Metadata extraction

DPI software offers the option to extract metadata on protocols and applications for both plain and encrypted IP communication to enable several use cases in the network security domain and performance monitoring. This includes:

- Service classification such as audio, video or chat for OTT applications, including WhatsApp, Skype, LINE, Telegram, WeChat and many more
- Performance KPIs as important fundamentals for various QoS/QoE measurements
- Protocol dissectors for deep understanding and validation of encrypted communication, including QUIC and HTTPS

Frequency of updates

The evolution of network traffic means that protocols and signatures are constantly changing and an application identification system must keep up. Good DPI software is achieved by having a team of experts who study application protocols and analyze their patterns and behaviors. Signature updates should be issued on a frequent basis to ensure a high level of accurate application identification. Even small changes to protocols and applications can lead to problems with classification, and since details for most application changes are not publicly announced, this requires constant attention. As a result of ongoing performance and reliability testing, regular improvements can be made to the software to ensure that all applications are detected.

Global application visibility

A key factor in choosing to source DPI is that the software is often deployed globally and regularly enhanced with the newest applications based on continuous feedback from multiple customers and regions. This results in a much better detection rate than an in-house DPI. This is especially important considering the level of performance, accuracy and reliability that a network supporting millions of subscribers would require.

Flexibility

Network infrastructure vendors and operators want to ensure that they choose a DPI partner who offers flexibility in terms of adding new applications or protocols and also in terms of being able to gain direct access to engineers, influencing roadmap for new features etc. This flexibility also allows to add custom-defined protocols to extend the detection. This enables customers to adapt the solution to individual use cases and reporting needs by offering the flexibility to add unique applications to the existing signature database. This also means that protocol and application detection can be customized within days as new business demands arise.

In-house engineers and developers

Last but not least, it is worth double-checking that the DPI software company you are considering actually develops their own software in-house rather than sub-contracting it to another software house. This ensures a high level of quality assurance and a tighter connection between the developers, the product management, the sales and support teams. This also means that your technical engineering staff can speak directly to engineers and developers who work on the DPI software. This is a real nice-to-have for technical teams who work on integrating DPI software into their solutions.

ipoque GmbH
A Rohde&Schwarz Company
Augustusplatz 9, 04109 Leipzig, Germany
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 3607.2349.32 | Version 03.00 | Juni 2020
Top 10 checklist for sourcing DPI software
Data without tolerance limits is not binding | Subject to change

36072349 32

3607.2349.32 03.00 PDP 1 de