3 ADVANCED TECHNIQUES TO CLASSIFY ENCRYPTED TRAFFIC

The use of encryption is expanding, both to protect privacy – and hide malicious activity. Can service providers still effectively manage traffic flows, user experience and security? With DPI, YES!

3 Ways DPI Classifies Encrypted Traffic

Statistical Analysis

- Analyze combinations of packet spacing, size, frequency

Behavioral Analysis

- Match against characteristic protocol behaviors

DNS-Based Classification

- Correlate flows with DNS responses

Example #1

Classifying Traffic Encrypted with SSL/TLS

100% ACCURATE

Method

- Read (unencrypted) name of service in SSL/TLS certificate or in Server Name Indication (SNI)

Example #2

Classifying Encrypted P2P Traffic

100% of P2P sessions IDENTIFIED

Method

- The P2P initialization phase is often not encrypted: IP addresses of peers can be discovered and classified
- If P2P traffic is encrypted, Statistical Protocol Identification (SPID) is used to identify encrypted traffic

Example #3

Classifying Skype

90-95% ACCURATE

Method

- Search for known binary patterns in traffic flows
- This pattern is usually found in the first 2 or 3 packets

Qosmos, a division of Enea, is the market leader in IP traffic classification and network intelligence software. Our technology can classify all HTTPS-based traffic, Skype and 100+ P2P applications.