Using nDPI for Monitoring and Security

Introduction :

Network administrators must continuously monitor the network to ensure optimal performance and security. This involves several key tasks: limiting bandwidth to prevent congestion, blocking malicious traffic and communication to safeguard the network, prioritizing traffic protocols to ensure critical services receive adequate resources, and decrypting traffic for deeper inspection. Achieving these objectives requires comprehensive traffic fingerprinting, which involves detecting protocols and analyzing their behaviors, preventing specific flows, implementing measures that respect content privacy, and identifying malware.

DPI

Deep Packet Inspection (DPI) comes into play as a critical technique that inspects packet payloads, while respecting the analysis of packet headers. DPI ensures the privacy and confidentiality of the inspected data by applying encryption techniques.

nDPI

nDPI goes further by analyzing encrypted traffic to detect hidden issues and previously undetected payloads. It extracts metadata from protocol headers and employs algorithms to detect threats. Additionally, nDPI identifies communications with potential risks, enhancing the overall security posture of the network.

Protocols functioning in nDPI

A protocol is characterized by two primary components:
- Major: Determines the transport protocol.
- Minor: Specifies the application protocol.

nDPI includes string-based protocol detection techniques, which involve:
- Analyzing DNS query names.
- Inspecting header fields.

- Identifying server names.

Traffic classification lifecycle

based on the traffic type dissectores are applied sequentially starting with ones that will most likely match the flow . Each flow will keep a track for non-matching dissectors in order to skip them in the future . Meanwhile the analysis lasts until a match is found or after too many attempts .

Packet processing performance

nDPI's packet processing performance is efficient because it helps analyze high-speed packets without adversely affecting network performance. This is achieved by effectively utilizing hardware resources to maintain accuracy.

Behavior and fingerprinting

nDPI goes beyond mere application recognition to provide comprehensive network analysis:

- **Traffic Classification:** Determines the type of connection.
- **Malware Recognition:** Identifies malware based on packet type and size.
- **Content Enforcement:** Measures the distribution of bytes to enforce content policies, considering byte entropy for more detailed analysis.

nDPI Flow Risks

nDPI assesses flow risks by analyzing various aspects of network traffic to identify potential threats and vulnerabilities.as an example Identifying the improper use of protocols that could lead to security breaches or data leaks.

Encrypted Traffic Analysis

Evaluating encrypted traffic to uncover hidden threats and ensure that encryption is not being used to mask malicious activities.Encrypted traffic analysis in nDPI involves two main components: behavior and fingerprinting.
By combining behavioral analysis and fingerprinting, nDPI can effectively analyze encrypted traffic, detect hidden threats, and ensure network security without compromising data privacy.

Detecting malwares

Clear Text Traffic:

- Signature-Based Detection:Utilizes known malware signatures and patterns within packet payloads to identify malicious content.
- Behavior Analysis:Employs heuristic rules to detect anomalies and suspicious behaviors indicative of malware.

Encrypted Traffic:

- Fingerprinting:
- Entropy Analysis: Measures the randomness (entropy) of encrypted payloads to detect obfuscated or encrypted malware traffic.

Bytes Entropy:

Used to assess the randomness of byte distribution within packet payloads, aiding in identifying encrypted or obfuscated traffic.

NB : The larger the entropy, the greater the uncertainty and randomness in the data. High entropy values often suggest encryption or compression, while lower values may indicate clear text or uncompressed data.

Malware analysis : trickbot

TrickBot is a sophisticated and modular malware strain primarily known for its capabilities as a banking trojan, but it has evolved into a more versatile threat with various functionalities.