Edition 2024

SL DPI

Solution description

slinkin.tech

Contents

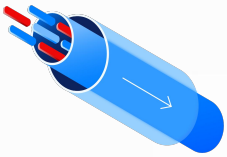
What is SL DPI?

SL DPI is a class of network software solutions that implements DPI* technology and has flexibile capabilities for integration into other software solutions.

***Deep Packet Inspection (DPI)** is a network traffic analysis technology that allows to extract their contents from packets, keep statistics on network flows and classify it, as well as filter and shape traffic.

When analyzing traffic, **SL DPI** can work not only on determining the list of protocols in the packet, but also on extracting all the fields of these protocols. This approach makes it possible to flexibly configure policies for shaping, blocking and/or logging, which allows you to cover a wide range of tasks in the field of network traffic analysis and management.
SL DPI is a multi-module, easily scalable solution, thanks to which it is distributed as 3 independent solutions:

SL DPI



#roadmap

SL Shaper

The most complete solution that implements all the basic functionality of DPI systems.

SL Sniffer

A network monitor that provides logging capability with flexible configuration of logged data. This solution includes only traffic monitoring and logging modules.

SL DC Engine

An integration solution that comes in the form of a software framework and provides the API for parsing the packet and obtaining protocol fields. In addition to packet dissection, DC Engine has the functionality to classify the Internet services and determine the properties of network flows. This product belongs to a class of DPI engine solutions.

DC Engine Packet dissection, service classification	**DC Engine** Packet dissection, service classification	**DC Engine** Packet dissection, service classification
Traffic Engine Traffic capture, shaping, network flows blocking	**Traffic Engine** Traffic capture	
DLog Network activity logging	**DLog** Network activity logging	
Packet Patcher Making changes to network packets/messages		
Policy Hub Description of regulating rules for network flows		

Functionality

SL DPI is a universal complex of network solutions, because its functional and technical features allow solving problems in the field of information security, system administration and telecommunications. The modular architecture of the product allows integration into third-party software solutions.
SL DPI has the following functionality:

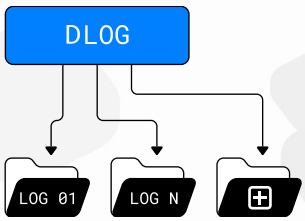
- Restricting access to prohibited resources
- Prevention of exploitation of new vulnerabilities, before the release of official fixes (HotFix)
- Maintaining logs of network activity that can be used in the investigation of incidents
- Accumulation of information on streams for use in Billing
- Load balancing in order to improve the quality of communication (traffic shaping)
- Putting users under control (saving all or selected information for certain users)
- Detection of network attacks (DDOS, Buffer Overflow, Scanning, etc.)
- Integration into IT solutions (IPS/IDS, SIEM, DLP, etc.)
- Data collection for AI systems

Technical advantages

> LOGGING SYSTEM

The logging module has a flexible configuration, which makes it possible to:

- Logging with the task of formatting and data for output
- Rotation of logs according to a schedule or file size
- Storing extracted field data to log journals for future analysis

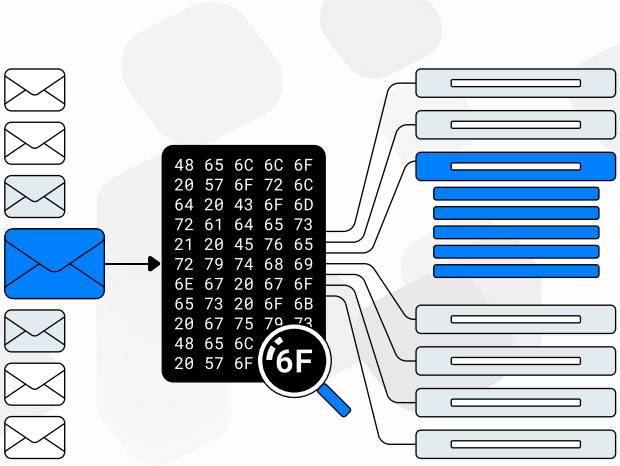


Included only in solutions: **SL Sniffer** and **SL Shaper**

> DETAILED PACKET ANALYSIS

The packet analysis module is implemented with a number of advantages, for example, such as:

- The module does not allocate additional memory for packet fields **(in-place dissection)** and allows you to access them directly
- Cross-platform solution (C++)
- Convenient API
- Extension mechanism allows users/developers to extend engine functionality with own code based on other engine features
- Each supported protocol has its own documentation page
- Network independent (supported protocols of the Internet, IoT, Industrial stack)

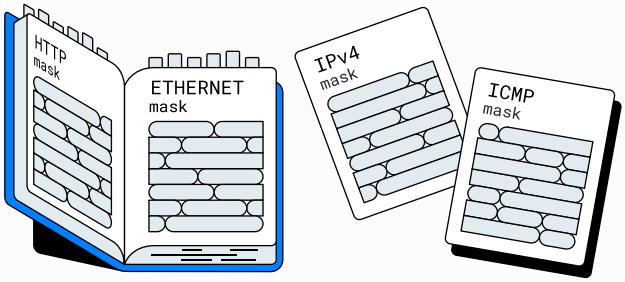


> PROTOCOLS

Our solution supports many network protocols, a list of which can be found on the page:

The protocol dictionary contains general information about each of them, and is also supported by the name of the RFC document according to which the protocol is supported. In addition, a table of supported fields is presented for each protocol, each of which has its own characteristics, such as identifier, name, type, size, mask, purpose.

When processing network traffic, the **SL DC Engine API** is used to dissect packets and gain access to protocol fields. This data can be used for logging and configuring restrictive policies. Third-party applications can use the result of the dissection to expand the functionality of their own applications, for example, using heuristic algorithms on the resulting data set or implementing complex logic to detect malicious activity on the network.



> INTEGRATION

The use of network traffic analysis technology is extremely popular for solutions such as **SEIM, IPS/IDS, DLP**. In addition to information security tasks, **DPI** is also used by Internet service providers and mobile operators to solve traffic classification problems, collect statistics, block prohibited resources and apply restrictions to subscribers.

SL DC Engine is an integration solution with a user-friendly API. This allows developers to focus more on the logic and functionality of their product and spend less time implementing network traffic processing functions. **SL DC Engine** supports internal and external flow table mode.

> TRAFFIC FILTERING

Restricting access to prohibited resources and setting regulatory policies for network users are among the most common tasks in the field of network administration, network security analysis and prevention of network attacks. **SL Shaper** is a solution that helps:

- Comply with the requirements of regulators to restrict access to Internet resources
- Register and analyze suspicious activity on the network in time
- Set limits for users on the speed and volume of transmitted information.

DPI technology helps to achieve maximum results when solving such tasks, providing the possibility of flexible configuration when setting filtering policies, as well as providing high performance when processing network traffic.

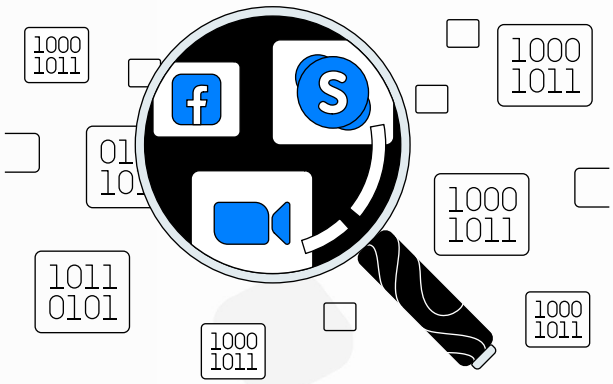
Included only in the **SL Shaper** solution

> CLASSIFICATION OF NETWORK SERVICES AND INTERNET SERVICES

The most important properties of network flows are:

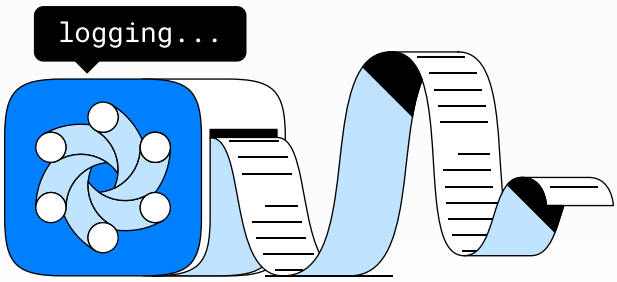
- Service definition
- Determining the nature of traffic (for example, audio/video traffic, file transfer, encryption, etc.)
- Determination of traffic properties (for example, gaming traffic, social networks, etc.)

DC Engine uses tagging mechanism for classification methods which helps to identify the service to which the network flow belongs. For example, Internet services, facebook, viber, youtube, etc. or network services such as ssh, telnet, dns, etc. Determining the properties of a flow is a complex technical task, since the underlying classification methods are mainly based on statistical indicators that may change in the process of updating/evolution of services. The tagging mechanism provides flexible functionality to mark network flows by any signature and behavior fingerprints which can be used not only for service determination but also for determining evil traffic, data leaks or just for marking flows for any other purposes (e.g. tethering, content type, etc.).



DC Engine provides a user-friendly API for working with classification capabilities, which helps:

- Update classification rules without changing the program code
- Add new services
- Easily transfer services and rules between releases/network nodes/applications
- All the above functionality is available via tagging mechanism configuration

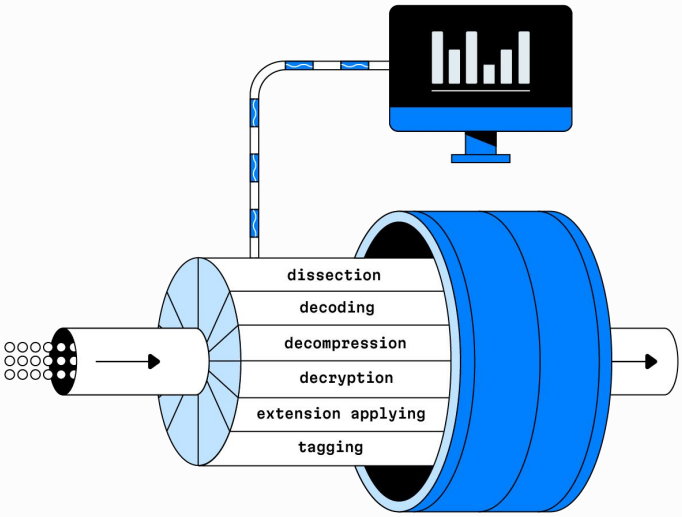


DC Engine keeps an internal event log available to the user, which helps to better understand the logic of the module, analyze the behavior, and understand on the basis of which characteristics the classification was made. This functionality significantly speeds up the process of mastering working with the module, and also helps to quickly identify problems, thereby reducing the time to fix them. The package includes detailed documentation on the supported protocols and their fields, built-in extensions (e.g. dns-cache) and **CLI** tool.

> FLEXIBILITY

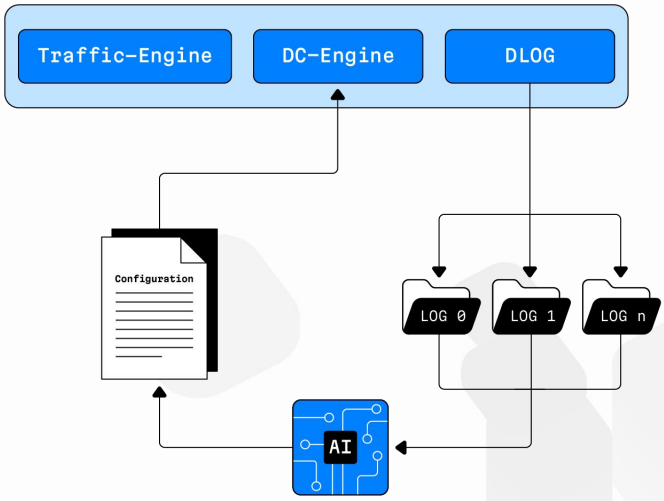
All **SL DPI** solutions are based on **DC Engine** and each of them are quite configurable. Configuration opportunities of engine and other solutions allow to set:

- Set thread count
- Set network interface settings
- Configure output journal format, log levels, log/journal rotation policies, log flush interval
- Configure packet assembling features such as fragment/segment count, max length, etc.
- Create tagging rules via human-readable language to classify network flows
- Create own code extensions to extend base engine functionality



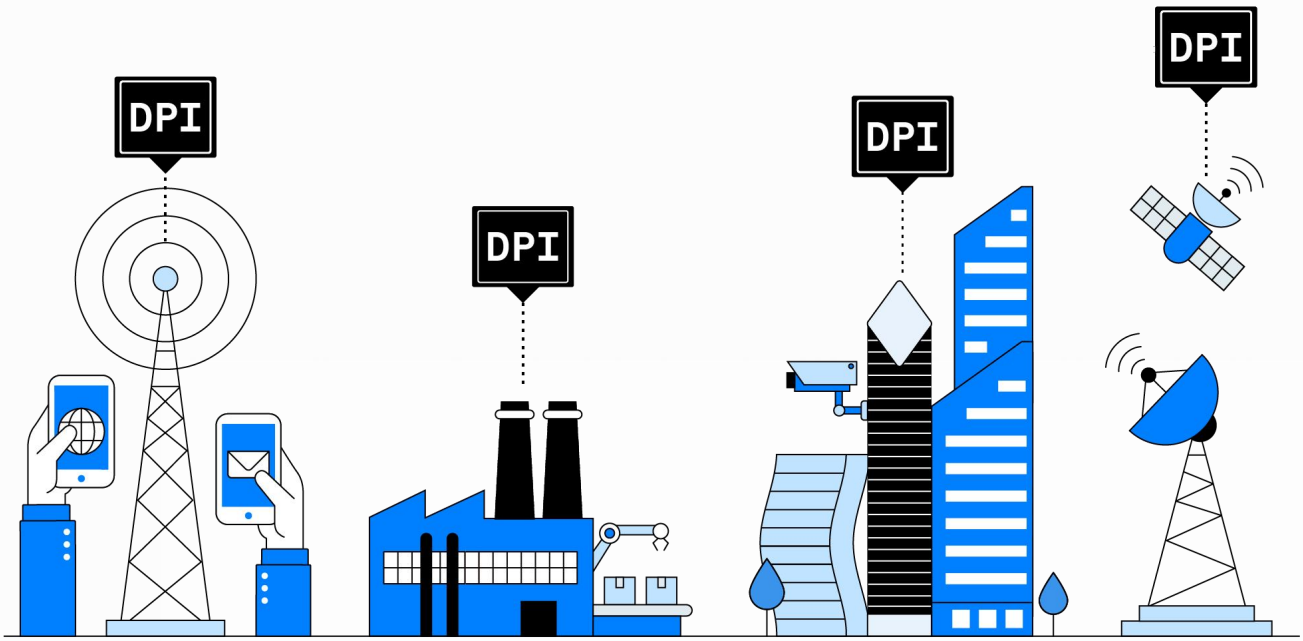
> SELF-SUFFICIENT SYSTEM

SL DPI includes products can be used together to achieve the best results in traffic classification. **SL Sniffer** and **SL Shaper** include **DLog** module which logs information obtained from **DC Engine** module (including extracted information by user extensions). Log journals can be used by AI systems or cybersecurity analysts to derive new traffic patterns which subsequently can be used for **DC Engine** configuring without code changing.



> NETWORK INDEPENDENT

DPI plays a significant role in any kind of network – the Internet, IoT, Industrial, satellite, etc. That's because network monitoring is an important part of providing reliable and safe infrastructure. Network engineers and developers must have the opportunity to control the network for debugging and configuring purposes, and information security engineers for detecting/preventing malicious activity. **DC Engine** is implemented as cross-platform and network-independent solution to be able to support protocols of any complexity level.



About the company

"Slinkin Technologies" is an IT company whose main specialization is software development in the field of computer networks. We develop flexible solutions that can be used in the field of analysis, balancing, modification of network traffic.

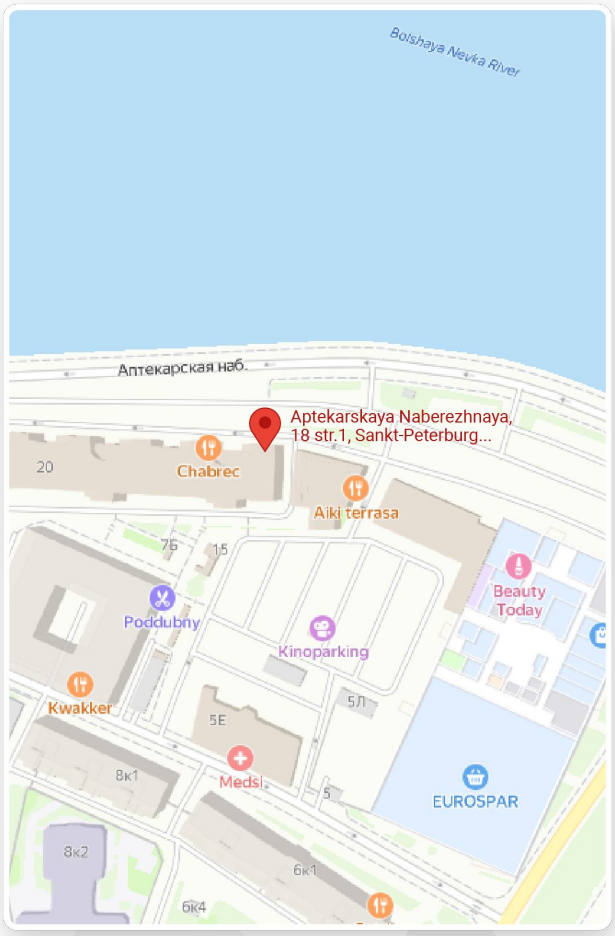
Despite the fact that our products function away from the eyes of most people, we try to make them as pleasant and convenient to use as possible.

> CONTACTS

Saint Petersburg

slinkin.tech

info@slinkin.tech



slinkin.tech