ÖLÇSAN 50
to measure is to know
50 years in the industry

T-STRAINER

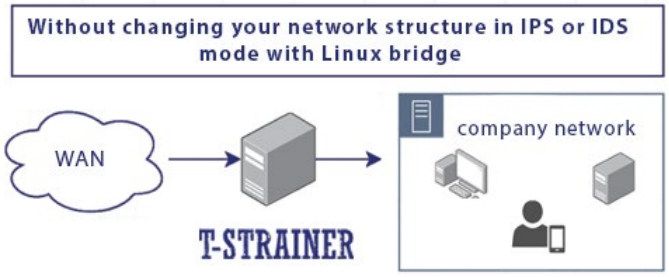
INTRUSION DETECTION and PREVENTION SYSTEM (IDPS)

T-STRAINER

IDS is the system name used to detect malicious activities or malicious connections in your network traffic. It is used as an abbreviation for Intrusion Detection Systems. The purpose of IDS security systems is to identify and log malicious activities. **IPS'**s are security systems used to detect and prevent malicious activities or malicious connections in your network traffic. It is used as an abbreviation of the words Intrusion Prevention Systems. The purpose of IPS systems is to intercept and prevent malicious connections or activities on network traffic.

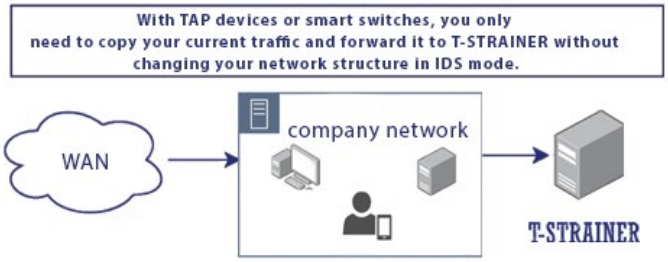
IDS is used for misuse detection and malicious activities checking. Malicious activities are identified by detecting anomalies that may occur in your network (known threats). Packets in network traffic are monitored and classified according to known rules. Unlike IDS, IPS's are placed in the direct communication path between source and destination, packets are actively analyzed and automated actions are performed to prevent intrusions.

Topology 1



In this mode **IDS and IPS** are working together. This topology should be used to prevent attacks. Requires downtime. However, T-STRAINER downtime periods for signature updates etc are **faster than any other competitor on the market.**

Topology 2



In this mode IDS is working stand-alone mode. With this configuration only detection will be available for threat hunting. Deployment within the network is easy. Does not require downtime

Advantages & Technical Strength

T-STRAINER protects you better, faster and cost effectively by consuming less resources.

- Supports **more protocols & metakey** information of these protocols. By using meta key information, it offers **wider and more comprehensive network security.**
- The user can go beyond the supported signature rules with the number of supported metakeys. Allows users to create **new custom rules.**
- Uses the standard **CIDSS* signature format**. Full translation of some signature types to other systems is impossible, but all signatures can be translated to CIDSS.
- Allows the **user to easily create new signatures** from the interface. The created signature rules are automatically converted to CIDSS format.
- Comes with an **ergonomic user interface.**

Detection and Prevention of Malicious Activities

FAST
Fully in-house developed system for high performance without latency.

EFFICIENT
We are able to add new protocols rapidly allowing users to react faster to attacks.

SECURE
Faster and deeper analysis performance than competitors. No effect on network speed while on duty.

EASIER TO USE
Fully in-house developed easy to manage IDS/IPS with user friendly interface.

NO OPEN SOURCE
Most of the commercial solutions are using their user interface with open source libraries. T-STRAINER is fully in-house developed.

+ *Custom threat intelligence from T-STRAINER is also very fast and supportive.*

** CIDSS: Common Intrusion Detection Signatures Standard*

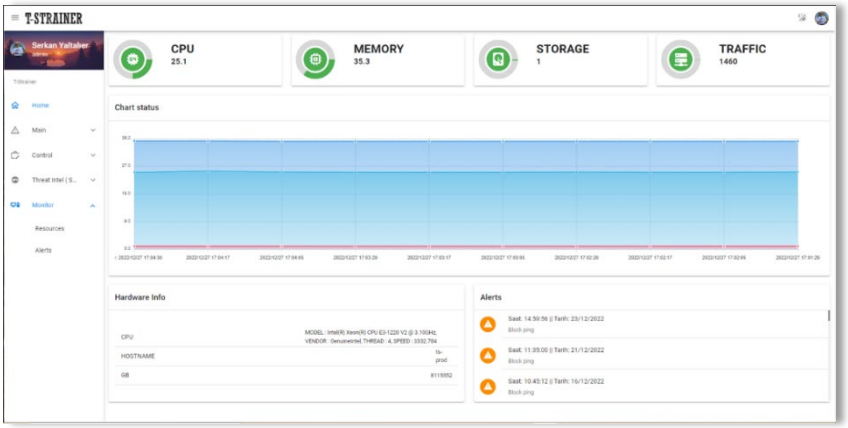
T- STRAINER Advanced Features

High Availability	→ Runs your entire protection infrastructure with redundancy.
SOC Integration	→ Multiple integration options for your SOC/NOC systems.
IP Reputation	→ Provides most up-to-date & false-positives excluded IP secure lists.
Optimized Speed	→ Designed to work with minimal latency on the busiest networks.
Current Signatures	→ Most up-to-date signatures from trusted sources for known threats.
Automatic Updates	→ Most up-to-date information & protection for network against attacks.
Metakey Based Rules signatures.	→ Provides metakey-based signature infrastructure for smarter
Multithread Operation	→ High performance & efficiency with multiple core usage.

- IPS protections include checks for well-known protocols such as HTTP, HTPPS, SMTP, DNS, POP, and IMAP…
- In order not to slow down the traffic and to prevent packet loss, accelerator cards/expensive processors and memories are used in both commercial and open source products. T-STRAINER does not…

T-STRAINER achieves high performance and efficiency by using multiple cores. The number of threads can be determined according to the hardware features. 120 Gbps live network traffic speed on 60 threads with 60.000 flow can be reached without any package loss.

T-STRAINER protects your network from malicious packets and enables a clean traffic flow to you firewall appliances.



WHY is T-STRAINER more advanced?

- Number of supported Network and Transport Layer Protocols for T-STRAINER are exceeding 75+
- Number of Supported Application Layer Protocols are 35+
- We provide enormous number 15.000+ Data Keywords (metakeys)
- Signature format as XML
- Performance: 4 threads with 15 flows 540 Mbps

Use Case

DDoS Protection - It makes the right decisions under load by separating normal traffic from malicious traffic against DDoS attacks.

Network Security - It makes accurate debugged decisions with advanced signatures and behavior analysis.

WEB Application Security - Nowadays, when web applications are on the rise, it monitors the security of these services in the best way and prevents attacks.

Database Security - Independent from the database system, it monitors the traffic in between and takes the right decisions with the right signatures.

Network Visibility - Increasingly complex networks and environments make it difficult to find specific traces. Therefore, you can reduce losses by increasing your network visibility.

Traffic Logging - You may need to review both the current and historical status of what's going on in your network. You can make these records with the signatures you specify.

Management Platform - With its easy-to use and simple interface, it provides a platform for the user to manage and monitor the product. There are different language options.

Quick and easy installation - You can easily setup in IDS or IPS mode without changing your existing network structure.

T-STRAINER is integrated with 3rd party applications like ELK. It can be also easily integrated with commercial and open source applications.

**Redundant: To prevent interruptions that may occur as a result of hardware failures by running more than one T-STRAINER on different devices.*
**Downtime: It is the time period when the running service or devices do not perform their functions. *Thread: T-STRAINER can be run more than once on the same device. In this way, more than one core in the process or is better utilized. *Flow: It is called traffic separation, which is created by looking at certain parameters. With this method, traffic is channeled.*