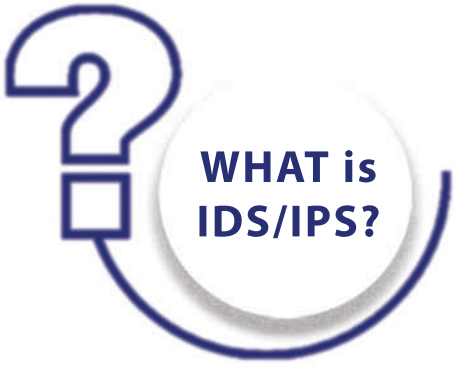
T-STRAINER

IDS/IPS SOLUTION

ÖLÇSAN

to measure is to know

T-STRAINER IDS/IPS



IDS is the system name used to **detect** malicious activities or malicious connections in your network traffic. It is used as an abbreviation for **I**ntrusion **D**etection **S**ystems. 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 **I**ntrusion **P**revention **S**ystems. The purpose of **IPS** systems is to intercept and prevent malicious connections or activities on network traffic.

HOW DOES IT WORK?

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.

ADVANTAGES & TECHNICAL STRENGHT

- ✓ 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.**

* CIDSS: Common Intrusion Detection Signatures Standard

OUR SKILLS

✓ **High Availability**
With T-STRAINER , you can run your entire protection infrastructure as redundant*. Thus, you can ensure that the network flow and security are always active with minimum downtime*.

✓ **SOC Integration**
You can easily integrate it into your SOC/NOC systems for security operations. You can take instant security actions with T-STRAINER API. We provide similar outputs (logs) with other commercial and open source products.

✓ **IP Reputation**
We provide the most up-to-date and false alarm-free secure IP lists powered by multiple sources.

✓ **Optimized for speed with minimal resources**
Architectural design to prevent packet loss/latency in complex corporate networks.
Compatible with 5G.
150mbps lossless speed achieved with 15 parallel streams.
Configuration: Single core performance with 8000 signatures installed.
System: Intel Xeon E3-1220 v2 (Geekbench score: 811)

✓ **Current Signatures**
It has the most up-to-date signatures against known threats from trusted sources.

✓ **Automatic Update**
It automatically receives the most up-to-date information against network-based attacks and protects your network.

✓ **Metakey Based Rules**
It has a metakey-based signature infrastructure so you can create smarter signatures.

✓ **Multithread Operation**
We can work using multiple cores for high performance and efficiency. The number of threads* can be determined according to the hardware features.
Lossless speed reached with 120 gbps live network traffic on 60 threads with 60.000 flow*.

* 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: TSTRAINER can be run more than once on the same device. In this way, more than one core in the processor is better utilized.
* Flow: It is called traffic separation, which is created by looking at certain parameters. With this method, traffic is channeled.

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.

✓ **It is easily integrated with other applications, works commercially and open source.**
It can be easily integrated with commercial and open source applications.

T-STRAINER IDS/IPS

COMPARISON CHART

FEATURES	T-STRAINER	COMPANY A	COMPANY B
Number of Supported Network and Transport Layer Protocols	75+	20	25
Number of Application Layer Protocols Supported	35+	20	32
Number of Data Keywords (Metakey)	15.000+	540	160
Signature Format	XML (CIDSS)Common Intrusion Detection Signatures Standard https://datatracker.ietf.org/doc/html/draft-wierzbicki-cidss-05	TXT	TXT
Modules Used	NFQueue, AFPacket, Pcap	NFQueue, AFPacket, Pcap	NFQueue, AFPacket
Operating Modes	IDS, IPS	IDS, IPS	IDS, IPS
Performance (4 thread, 15 flow)	540 Mbps	480 Mbps	440 Mbps

PS: OSI Model Layers; Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer (Session Layer), Presentation Layer (Presentation Layer), Application Layer (Application Layer)
Configuration: 4 thread processing performance with 8,000 signatures installed
System: Intel Xeon E3-1220v2 (Geekbench score: 811)
Flow: Independent traffic. The higher the number the harder it will be to handle traffic
Thread: Number of services performing parallel processing

Topology 1

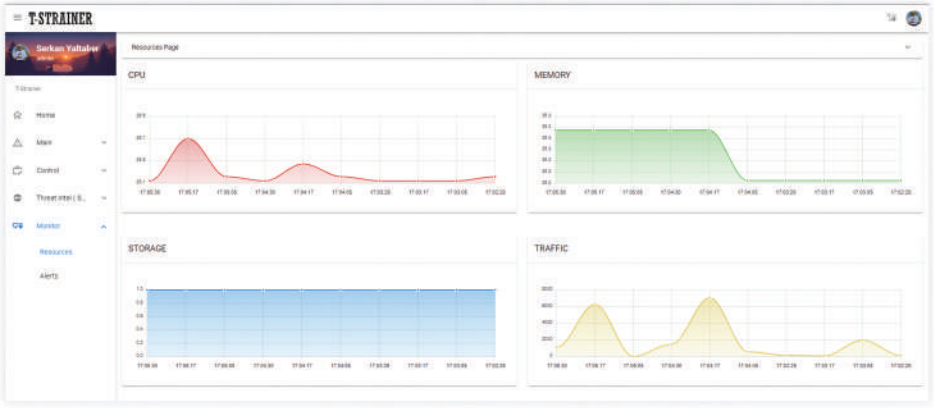
Without changing your network structure in IPS or IDS mode with Linux bridge

- ✓ 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

With TAP devices or smart switches, you only need to copy your current traffic and forward it to T-STRAINER without changing your network structure in IDS mode.

- ✓ 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



to measure is to know

messen ist wissen **ölçmek bilmektir** **mesurer c'est savoir**

meten is weten **medir es saber** Измерить, значит знать

kupima ni kujua **aunawa shine sani** **wiwọn jẹ mọ**

측정한다는 것은 안다는 것이다 **測定は知っている** **測量就是知道**

mengukur adalah mengetahui **misurare è conoscere** मापना जानना है

پیمائش جاننا ہے القیاس هو المعرفة اندازه گیری دانستن است

পরিমাপ হচ্ছে জানা

T-STRAINER_EN/2023.04

www.olcsan.com info@olcsan.com P: +90 (212) 216 50 80

ÖLÇSAN
to measure is to know