WASABI Networks

Network Traffic Analysis (NTA) Software Engine

Protect and optimize your valuable network infrastructure with the worlds most scalable, flexible and powerful solution for professionals to effectively manage and secure any network.

Designed to zoom in on the right data, fast and efficiently, and thereby minimizing the time from discovery of a problem in or on the network, to devising a solution.

Record and leverage your network data to improve security and performance.

- 100% Line Rate recording - packet capture and storage
- Full visibility in all network traffic – always on
- Scalable performance to 100G+ on commodity hardware
- Dynamic real-time protocol decoding
- Filter out unnecessary information
- Ultra-fast search & retrieval
- Simultaneous write/search/retrieve operation
- Work as a team to resolve issues
- 100% Line Rate transmit
- API & Protocol Definition capabilities

Capture

Decode

Filter

Store

Search

Analyze

Cooperate

Extract

Extend

Transmit

Improve What Matters in Your Network

Cybersecurity

Cybercrime to the most common risk facing all modern companies today. Period. And the amount of investments going into preventing being hacked is growing each day.

Prevent and Protect

No firewall/IPS is impenetrable, and when it detects an attack it become vital to know exactly how the attack impacts your infrastructure, and the best way to do this is to record all activity on the network. The WN NTA Engine is designed to be always on, so when your security equipment raises an alarm, the activity that caused it is already recorded on disk. With the WN NTA Engine API it is possible to automatically lock down the traces of the attack and thereby providing the security team with the best conditions for mitigating the attack.

Incident Response

Most incident responders rely on analyzing logs and flow information, which are sufficient for analyzing the most common cyber attacks. However, as attacks becomes increasingly more sophisticated in avoiding detection, sample-based incident information falls short. A full-packet based recording of all traffic, which is provided by the WN NTA Engine, is a far more potent tool in the hands of the skilled responder.

Network Forensics

After the immediate cleaning up after a cyber attack, it is vital for the organization's capability to withstand similar attacks in the future that the root cause of the attack is established. Enter the Network Forensics experts. The ground work behind the attack may have been laid months before the discovery of the attack, so months worth of archived data must be provided as input. The WN NTA Engine provides exactly this, but more importantly, it also provides ultra-fast search capabilities to zoom in on exactly the information that the investigator is looking for.

Security Hardening

When you have been breached, and you have found the cause, and you believe you have mitigated the problem, how can you be sure that everything is now OK? Well, with the WN NTA Engine you have a recording of the entire attack scenario, and you can then replay that scenario again and again (and at different speeds) against your infrastructure to see if your defenses holds up.

Threat Hunting

Even in "peace time", the war against cyber attacks needs to be fought. With a perfect record of all network traffic, security professionals can identify anomalies and other traces that can indicate lateral movement in the network by attackers that are lurking around in the preparation of an attack. In cooperation with the global community of cybersecurity experts, you can match your observations with databases of attack patterns and spot attacks before they materialize.

Network Operations

Whatever you do: Keep your network services up and running! Maintaining continuous operations is crucial, and the users are becoming ever more impatient with the time it takes to mitigate issues. With a WN NTA Engine you can cut to the chase in the event of a network performance problem.

Network Visibility 24/7

Networks are running in real time and most companies probably have lots of network monitoring equipment already to tell them how the network is performing, both from a network perspective and from an application perspective. Yet users often experience issues that are not explained by looking at a dashboard or traversing log files. The WN NTA Engine provides a 100% copy of your network traffic and therefore provides a complete account of what happened in the infrastructure.

GDPR compliance

With the introduction of the GDPR data protection legislation, the leak of data – however benign or well-intended the reason is behind the leak – needs to be analyzed, reported to the affected users, and reported to the authorities. Without complete insight into the network communications, GDPR compliance becomes difficult.

Help the Help Desk

Users calling in with a problem want immediate action to be taken to resolve their issues. If the issue is anything but the most trivial problems (often related to the user's own machine or handling thereof) the Help Desk often need to "look into the issue". With a WN NTA Engine, will be able to provide a more meaningful response, and perhaps even solve more complex issues instantly so the user can verify this on the spot. Happy user, happy help desk, case closed.

WASABI Networks

Leverage Your Network Traffic

Always on, always learning

The WN NTA Engine is designed to operate continuously 24/7 to make sure all network traffic is being captured and analyzed. Especially in Cybersecurity, it is important you don't miss any bit of data.

A new level of interaction

Similar systems often rely on data being exported to Wireshark, in order to view the actual data. The WN NTA Engine also allows viewing and analyzing data live on the system, while being captured. Speed is of essence in modern networks operations.

A new level of teamwork

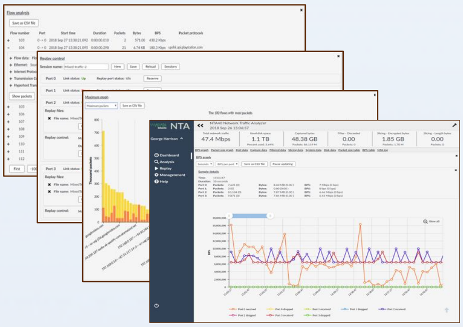
Finding the root cause of a breach or hunting for APTs often requires different areas of expertise. The WN NTA Engine allows teams of experts to build and share network searches for fast and effective resolution of the issues.

A shared resource

The ability to have full visibility into all your network traffic is a valuable resource that should be shared internally among the people responsible for the well-being of the company's infrastructure: Security experts in the SoC/SaC, compliance officers responsible for preventing GDPR violations, Help Desk staff, IT professionals in the NoC, etc. All these tasks can be performed simultaneously through the WN NTA Engine on the same data, in real time, and without accessing (disturbing) the active elements in the infrastructure.

Easy and configurable UI

As the WN NTA Engine can be used for many tasks and in many contexts, there are no right or wrong user interface: Configure it to your needs!



Not all data are created equal

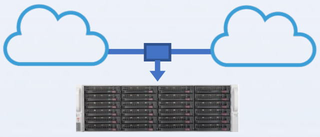
Disk real estate is always at a premium, and with the WN NTA Engine you can select, suppress or prioritize exactly the data you need to optimize the retention time window for your tasks.

Extend, Expand, Export

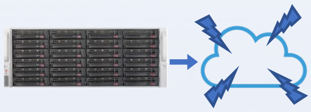
No system can do all things to man, so the WN NTA Engine can be easily extended with custom-built protocol decoders, dynamically expand storage to multiple Petabytes, and ultimately export PCAPs to other systems for further analysis.

Deployment Modes

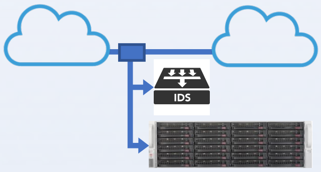
24/7 Continuous SLA Monitoring



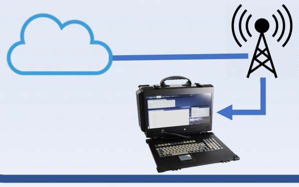
Infrastructure Load Testing



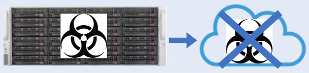
IDS triggered network search



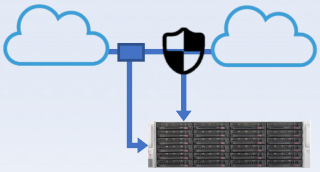
In-the-field trouble-shooting



Security Hardening



FW/IPS triggered network search



WASABI Networks

Specifications and Features

Capture

- Scalable capture rates up to 100G+ in a single server
- 1G/10G/40G/100G connectivity using state-of-the-art FPGA capture cards
- Any number of ports and port speeds can be combined for maximum peak capture speed
- 100% full packet capture and zero packet loss
- Nano-second packet time stamping
- Choose any commodity server suited to achieve the desired sustained packet processing and storage rate (see hardware datasheet)

Decode

- Real-time decoding of protocols for filtering and fast search
- Encapsulations: VLAN, MPLS, GRE
- L3: 38 protocols, e.g. IPv4, IPv6, LLC, ARP, FCoE
- L4: 46 protocols, e.g. TCP, UDP, GTPv1+2, STP, SCTP, DNS
- L5-L7: 21 protocols, e.g. HTTP/HTTPS, DHCP, SCCP, SIP

Filter

- Up to 16 filters can be defined and applied to narrow the scope of captured traffic
- Combine MAC address, IP address, encapsulation, protocol, port, and time window filter arguments – up to 16 combinations per filter
- Support for include and exclude type filtering
- Conditional slicing options for encrypted traffic and streaming media
- Supports grouping of filters in different retention tiers

Store

- Scalable storage up to 6.5 PB
- Maximum storage in a single (4U) server: 432 TB
- Choose any commodity server suited to achieve the desired sustained packet processing and storage rate (see hardware datasheet)
- Configurable data-overwrite behavior based on storage tiers (defined in capture filters)
- Extend storage size on-the-fly without system reconfiguration

Search

- Define search filters for fast selection of stored traffic
- For each user profile, up to 32 search filters (each with up to 16 parameters) can be defined to narrow the scope of traffic for analysis and extraction
- Combine e.g. IP address, encapsulation, protocol, port, GSM MAP messages and time window filter arguments

Analyze

- Customizable dashboard for top-level traffic overview
- Graphs for bps, packet size, etc.
- Statistics for each capture port
- Statistics for traffic type, filter, sliced and discarded traffic
- Real-time packet browsing, selection and drill-down
- Real-time full packet content display
- Real-time flow statistics and flow analysis

Cooperate

- Multi-user, multi access design
- Support for up to 32 user profiles
- Role-based access control
- User groups facilitating sharing of analysis results
- Up to 8 simultaneous users performing real-time search and analysis

Extract

- Export to PCAP format
- Export PCAP files in up to 1GB file size

Extend

- Custom protocol decoding can be defined
- Support for search acceleration based on custom protocols
- REST API for 3rd party integration

Transmit

- Replay stored traffic 100% as it was captured
- Modify transmit rates up to maximum port speed
- 1G/10G/40G/100G connectivity using state-of-the-art FPGA capture cards
- Scalable transmit rates up to 100G+ in a single server
- Any number of ports and port speeds can be combined for maximum peak transmit speed
- Choose any commodity server suited to achieve the desired sustained transmit rate (see hardware datasheet)

LEARN MORE

For more information please checkout our website www.wasabiNetworks.com or send us an email at sales@wasabiNetworks.com

ABOUT WASABI NETWORKS

Wasabi Networks helps companies around the world keeping their network infrastructure safe and sound, by making Network Analysis, Network Test and Network Security solutions with high performance, that are affordable and easy to use