napatech

SOLUTION DESCRIPTION

# NTOP - NAPATECH

## 1-100G SECURITY ANALYSIS PLATFORM

ntop

This is a description of the joint solution from ntop and Napatech, enabling enterprises to build efficient and accurate systems to track, trace, monitor and alert traffic traversing the network, even at 100G. The solution offers the combined power of a flow-centric and packet-centric solution in a single standard server, providing a powerful and cost-effective basis for advanced multi-dimensional security solutions.

### POTENTIAL USERS

The solution is aimed at enterprises, cloud and data centers, Internet providers and government. It is the perfect fit for companies already doing flow-based threat detection but wanting full visibility into all network flows at speeds up to 100G, complemented with application protocol and network telemetry information.

### WHAT IT SOLVES

Today, NetFlow statistics is typically sample based – especially when speeds increase beyond 10G. Sampling only provides a glimpse of the potential threats on the network – and as such poses a potential liability. nProbe™ Cento solves this through zero packet loss and 1:1 NetFlow generation.

Based on DPI (Deep Packet Inspection) the solution also enables packets/flows to be redistributed to specific applications such as Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS), traffic recorders, etc. If one of the clients slows down and thereby causes back-pressure, nProbe™ Cento will throttle the traffic to that client ensuring that the 1:1 NetFlow is still maintained.

### HOW IT WORKS

nProbe™ Cento provides packet broker like functionalities, but as it is a lightweight software-based packet broker it can run inside the same server as its clients/subscribers.

At the basis of all use cases lies the need to capture packets traversing one or more network interfaces. Relevant use cases range from quick network flow export to more sophisticated integrations with traffic recorders and IDS/IPS. The great flexibility of nProbe™ Cento effectively provides solutions to:

1. Quickly convert network packets into flows that can be stored, analyzed or exported to custom or third-party software. For example, flows can be sent to ntopng or other NetFlow-compliant flow collectors to carry on network-intelligence tasks such as historical investigations of congestions or intrusions.

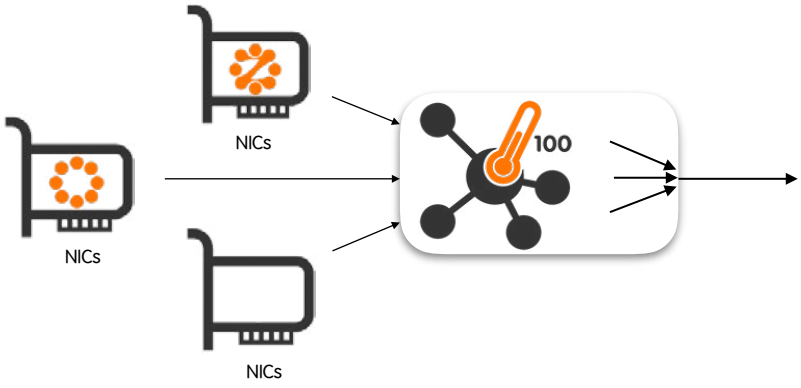
2. Forward network packets to a traffic recorder for full packet payload analysis with a substantial control on the forwarding policies. This makes it possible to exclude e.g. encrypted traffic with the aim of alleviating the load on the recorder.

3. Seamlessly integrate IDS or IPS by delivering network traffic on multiple output queues. Balancing the traffic on multiple queues has the benefit that several IDS/IPS processes/instances can work in parallel on meaningful subsets of traffic.

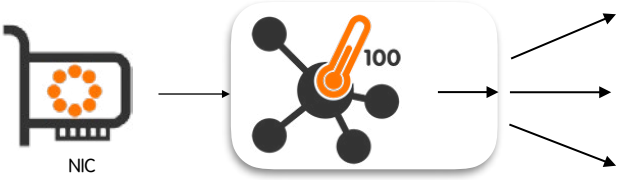
## EGRESS QUEUES

nProbe™ Cento implements traffic forwarding functionalities that enable:

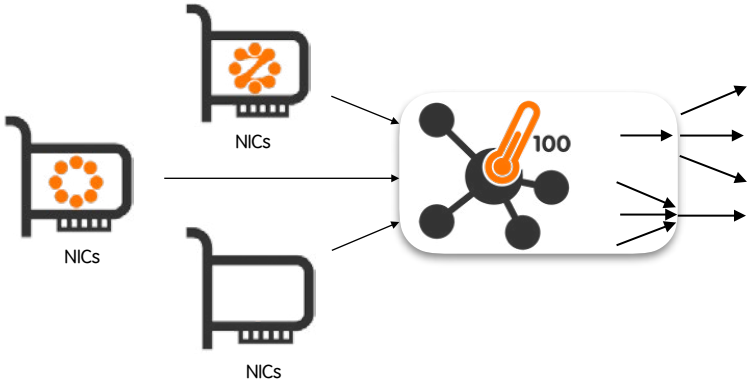
- Packet capture from multiple input interfaces and forwarding to a single, aggregated egress queue



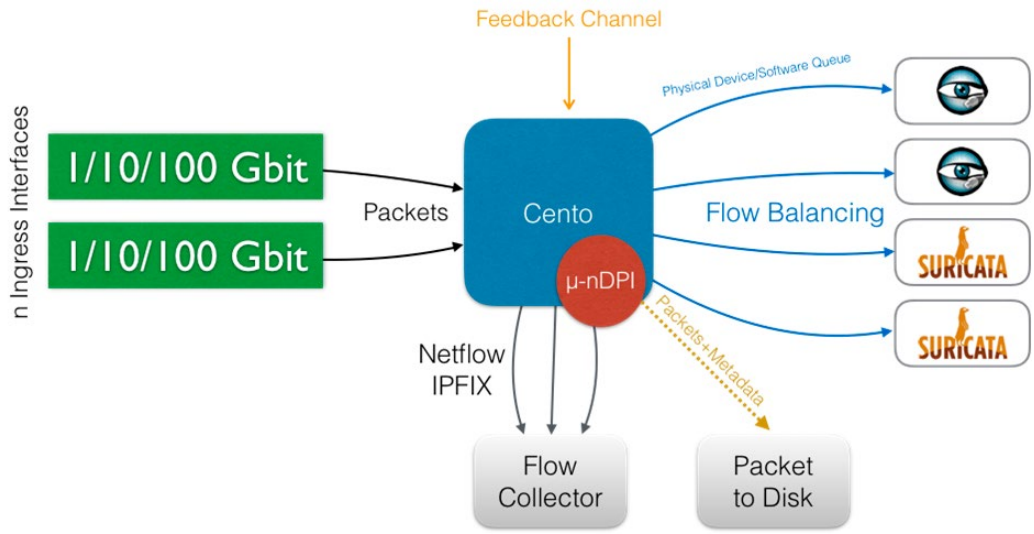

- Packet capture from an input interface and forwarding to multiple, balanced egress queues




- Packet capture from one or more input interfaces and simultaneous forwarding to multiple balanced queues and to a single aggregated queue



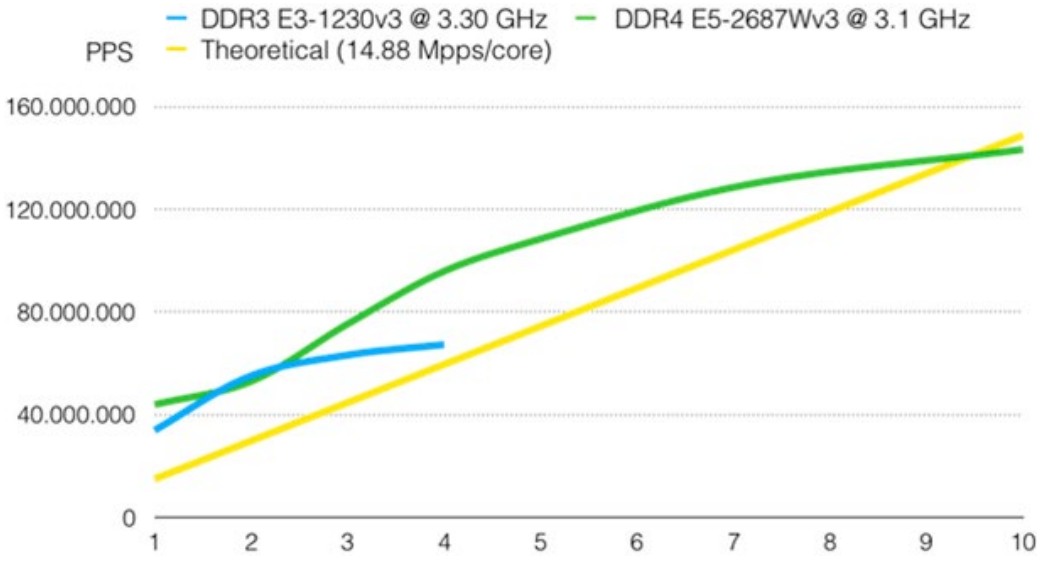
## ARCHITECTURE




## PERFORMANCE

nProbe™ Cento is designed to keep up with 1-100G speeds on commodity hardware. It leverages the latest innovations, such as timestamping, hardware packet filtering and the ability to distribute the traffic to multiple cores.

On adequate hardware, Cento can process 10G per physical core, and scale almost linearly in the number of cores (if there is enough memory bandwidth available).




The above figure shows the result of a performance test with a 100G FPGA-based Napatech SmartNIC configured with 26 streams. The total processed rate (sustained) was 132 Mpps with 70-byte packets and zero drops.

The configuration used for the test:

- nProbe™ Cento (native PF_RING support)
- CentoOS 6.x x64
- PF_RING 6.3.X
- 2 x CPU Intel E5 v3
- Napatech 100G SmartNIC
- 500K rotating IP addresses
- Generation of 25 million flows/minute
- No flow storage on DB or disk, just forwarding (in NFv9 format) to a collector

## THE NAPATECH DIFFERENCE

Napatech SmartNICs are uniquely suited for this solution. They capture data from networks at high speed and high volume using patented packet capture technology, enabling real-time insight into network traffic. With a portfolio that scales from 1 to 200G, they provide more efficient data delivery through such features as zero packet loss and nanosecond time precision.

Napatech SmartNICs ensure that identified flows are distributed in an optimal way to the available CPU cores. With flow distribution to multiple CPU cores, the throughput performance of the analysis application can be increased linearly with the number of cores, up to 128.

## NPROBE™ CENTO FEATURES

- NetFlow v5/v9/IPFIX support
- Flow export to JSON, Text, Kafka, Syslog, ntopng
- IPv4 and IPv6 support
- Native PF_RING and PF_RING ZC support for high-speed packet processing
- Scalable, multithreaded design, ingress traffic can be load balanced across multiple streams
- Layer-7 application visibility
- Flow-based Load Balancing to IDS/IPS (Snort, Bro, Suricata)
- Traffic filtering based on protocols to reduce the load on the IDS
- Feedback channel for traffic filtering/shunting from an IPS
- Traffic filtering and slicing for saving storage space removing irrelevant data

## COMPANY PROFILE

Napatech helps companies to reimagine their business, by bringing hyper-scale computing benefits to IT organizations of every size. We enhance open and standard virtualized servers to boost innovation and release valuable computing resources that improve services and increase revenue.

Our Reconfigurable Computing Platform™ is based on a broad set of FPGA software for leading IT compute, network and security applications that are supported on a wide array of FPGA hardware designs.


**EUROPE, MIDDLE EAST AND AFRICA**
Napatech A/S
Copenhagen, Denmark

Tel. +45 4596 1500
Info@napatech.com
www.napatech.com

**NORTH AMERICA**
Napatech Inc.
Boston, Massachusetts
Los Altos, California
Washington D.C.
USA

Tel. +1 888 318 8288
Info@napatech.com
www.napatech.com

**APAC**
Napatech China/South Asia
Taipei City, Taiwan
Tel. +886 2 28164533 Ext. 319

Napatech Japan K.K.
Tokyo, Japan
Tel. +81 3 5326 3374

ntapacsales@napatech.com
www.napatech.com


DN-1098 Rev. 2