napatech

Case study: Hyperscale data center steps up security

ntop

Industry pain points

The ability to detect threats at any speed is a challenge. In a world of software-defined everything, with trillions of endpoints, massive amounts of data and networks operating at speeds of 40G and 100G, these challenges become even more complex. To make matters worse, there is a severe lack of commercial, affordable offerings capable of addressing industry needs. Many enterprises and cloud service providers are therefore driven to build their own security monitoring solutions. But how do you build an efficient solution that provides complete traffic visibility, even at 100G?

Client challenges

This was the challenge faced by a global hyperscale data center as they engaged ntop and Napatech to help develop a 100G line rate traffic monitoring solution focusing both on network performance measurement and security traffic analysis. Their current solution was based on Random Sampled NetFlow, which only provided them a fractional overview of who had been on their network and what action they had taken.

To reinforce their security posture, they needed to gain full traffic visibility. Losing even a single data packet could potentially expose their critical infrastructure and compromise the safety of assets and resources. What they needed was a solution that would guarantee lossless capture, even at 100G. To enhance efficiency, they also needed a 1:1 overview of the NetFlow statistics while only storing selected flows to disk. That way they could focus their further processing on any abnormal, suspicious activity, instead of committing resources to investigate each single data packet.

Solution

ntop and Napatech partnered to develop a compact high-speed solution that would both ensure complete packet capture while also providing the needed 1:1 NetFlow overview.

Challenge

A global hyperscale data center engaged ntop to help develop a 100G traffic monitoring solution. Their current solution only provided a fractional overview of their network traffic, so they needed to reinforce their security posture.

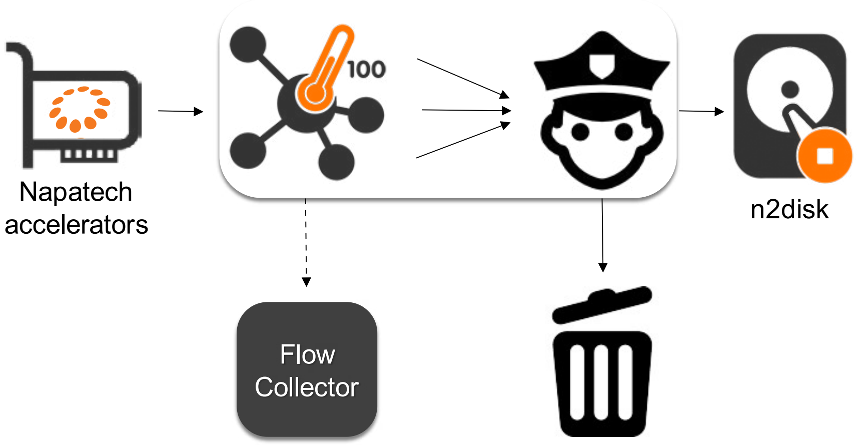
Solution

ntop partnered with Napatech to develop a compact 100G monitoring solution that would provide complete and efficient network visibility. The solution was powered by Napatech's FPGA SmartNICs, ensuring lossless capture and full compatibility even at 100G.

Benefits

The solution helped the data center to realize a drastically stronger network security with a minimum strain on resources.

The Cento 100G Capacity Solution



Napatech's FPGA-powered SmartNICs were integrated with the nProbe™ Cento software. This provided guaranteed lossless capture and enabled traffic analysis even at 100G. When captured, the data packets were classified by the Cento NetFlow probe and converted into flows. The n2disk™ network traffic recorder made it possible to write packets from suspicious flows to disk for extensive periods of time, enabling subsequent forensic investigation.

Key benefits

By combining the high-speed Cento software with Napatech SmartNICs, we successfully developed a 100G capacity solution that would both ensure zero packet loss while also providing a fully reliable 1:1 overview of the NetFlow. The combined power of this packet and flow-centric solution helped the data center to realize a drastically stronger network security with a minimum strain on resources.

nProbe™ Cento

nProbe™ Cento is a high-speed NetFlow probe able to keep up with 10/40/100G. Besides capturing ingress packets and computing flow data, it can be used to classify the traffic via DPI (Deep Packet Inspection) and perform optional actions on selected packets/flows when used as traffic forwarder in combination with other applications such as IPS/IDS, traffic recorders, etc.

Napatech

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.

Find out more at:
www.napatech.com

Find more case studies at:
www.napatech.com/resources/case-studies

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.

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