Case study: Lancope accelerates security performance by a factor 4

Industry pain points

In the age of reconfigurable computing, with data amounts constantly snowballing, security infrastructures are challenged to keep pace. Safeguarding networks against sophisticated attacks is a continuous cat-and-mouse game where the only rule is that there are no rules.

Many security solutions are created around assumptions on how attacks are structured in strictly-defined, deterministic approaches. Companies rely on firewall port-based analysis, antivirus, malware detection and IDS/ IPS pattern-based analysis to protect against attacks, but these approaches can only prevent known threats.

The ever-ingenious hacker is constantly looking for new ways to circumvent these static defenses with Advanced Persistent Threats (APTs), insider threats and multi-faceted attacks that use a combination of DDoS, malware and zero-day attacks to breach defenses. So how can these threats be detected and prevented in real-time?

Client challenge

Lancope has long been an advocate for a more holistic approach to network security that not only relies on static defenses, such as firewalls, anti-virus and IDS/IPS, but also makes active use of the vast amount of real-time information available from other devices and the network itself to get a real-time view.

By collecting and analyzing data flows in the network, Lancope detects abnormal behavior not picked up by signature-based defenses, enabling improved detection of a wide range of threats, as well as enhanced incident response and network forensics. The Lancope Stealthwatch FlowSensor plays a key role in this process by using a combination of Deep Packet Inspection (DPI) and behavioral analysis to identify applications and protocols across the network.

With increasing data traffic, speeds and complexity, however, Lancope needed to increase performance of the Stealthwatch FlowSensors. The challenge was to ensure that the proposed solution could be optimized

Challenge

To keep up with the growing variety, velocity and volume of data, Lancope needed to increase performance of their Stealthwatch FlowSensor. The challenge for Lancope was ensuring that the solution could be optimized using a standard Dell OEM server platform.

Solution

A pre-integrated solution from Napatech and Rohde & Schwarz Cybersecurity was chosen for application acceleration and DPI.

Benefits

With this solution, Lancope successfully accelerated performance of Stealthwatch FlowSensors by a factor of 4, providing increased real-time insight into the network traffic. The pre-integrated solution ensured a seamless and fast time-to-market.

using a Dell OEM standard server platform. Dell OEM and Lancope therefore selected a pre-integrated solution from Napatech and Rohde & Schwarz Cybersecurity for application acceleration and Deep Packet Inspection (DPI).

Solution

Napatech's FPGA-based SmartNICs enable appliance developers to stay one step ahead of the networks they need to manage and secure. With guaranteed delivery of network data for analysis, Napatech SmartNICs ensure that all the relevant data for effective analysis is provided in real-time, even at speeds beyond 100G.

Designed for open and standard servers, Napatech SmartNICs make optimal use of server CPU and memory architectures providing substantial acceleration for analysis applications including offload of critical data handling tasks.

R&S®PACE 2

The protocol and application classification engine R&S®PACE 2 from Rohde & Schwarz Cybersecurity performs dedicated deep packet inspection (DPI). It enables network equipment and security vendors to easily integrate recognition of layer 7 protocols and applications. The tool is ideal for identifying protocols and applications that use advanced obfuscation and encryption techniques to avoid detection.

R&S®PACE 2 is optimized for fast performance, efficient memory usage and classification reliability. It supports thousands of network protocols and applications, and frequent signature updates ensure ongoing reliable detection. Based on performance tests on real traffic data, it can accurately identify over 95% of network traffic, even at high speeds.

Benefits

By integrating Napatech SmartNICs and R&S®PACE 2, Lancope successfully accelerated the performance of Stealthwatch FlowSensors by a factor of 4, providing greater real-time insight into what is happening in the network. As Napatech SmartNICs are pre-integrated with R&S®PACE 2, Lancope and Dell OEM could quickly design and verify their new solution without the risk of incompatibility and resulting delays, ensuring faster time-to-market.

Added benefits

- Rohde & Schwarz Cybersecurity provides continuous updates to ensure that the latest protocols and applications continue to be detected.
- Napatech's reconfigurable SmartNIC hardware and software is continually updated and new solutions can be seamlessly integrated.

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

DN-0867 Rev. 5

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