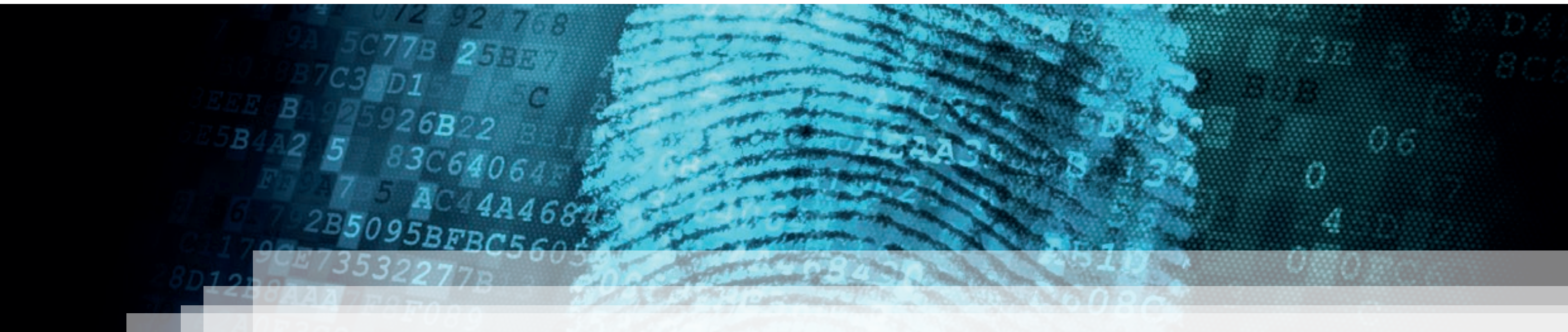

Case study: Leveraging open source PCAP software for robust and cost effective security solutions

Challenge: Providing cost-effective enterprise-grade network security
The benefits of open source cannot be ignored. Businesses can develop applications leveraging the collective knowledge of the open source community while reducing time-to-deployment. Developers can create innovative solutions tailored to a business' immediate and long term needs, no longer relying on any particular commercial solution.

An excellent example of this is in the area of Network Security, where all enterprises are challenged to defend their networks against security threats, especially those that have yet to be identified. Unlike companies offering proprietary security solutions, the open source community presents many advantages that the area of network security can leverage. The "community" itself is organized to ensure that the code can be examined by anyone, and, when necessary, address security concerns as they are encountered, unlike with proprietary software. Open source software can therefore, merely by the nature of how it is developed, be faster and more thorough in addressing security vulnerabilities.

Another advantage of open source software is the ability to customize code to the enterprises' specific and immediate security needs. Consider that more enterprises are embracing the practice of building out their IT networks using commercial off-the-shelf (COTS) components. Not only are these networks developed to meet their unique business requirements, but building out these networks can also prove to be more cost-effective with open source software.

Solution: Napatech's Network Acceleration Cards (NACs)
One crucial element in any security solution is the ability to capture and monitor traffic in real time to provide visibility and insight into attempts to breach networked systems. Napatech provides the ideal support for this capability with its Network Acceleration Card (NAC). Combined with open source network security software and standard servers, an enterprise can deploy and tailor its own solution while benefiting from Napatech's high-performance packet capture technology that, at one point, was only available for large commercial solution providers.

Challenge
Anyone that need to secure their IT infrastructure have industry-standard PCAP applications such as Suricata, Bro, and Wireshark at their disposal. The problem is the scale and bandwidth at which enterprises operate today.

Solution
Integrating PCAP applications with the NAC allows businesses to ensure proper security measures under all network conditions.

Benefits
Not only does the NAC enable a deeper understanding of both existing and potential vulnerabilities, but the ability to provide zero packet loss also enables the complete visibility which is vital to identify potential security breaches. The NAC supports numerous industry standard PCAP applications and can be easily used by the open source community.

DN-1045 Rev. 1

Key benefits

The NAC enables the customer to capture a perfect copy of all packets traversing a network, without any loss of information. Not only does the NAC enable a deeper understanding of both existing and potential vulnerabilities, but the ability to provide zero packet loss also enables the complete visibility which is vital to identify potential security breaches. Building Napatech into a custom security solution is also easy since it is designed in a compact form factor that integrates well with standard servers. Napatech has also ensured that the NAC can be easily used by the open source community, as the card supports numerous industry standard PCAP applications.

Case

Ensuring security; key to success in a web-scale social network

Large social network companies must maintain Web-scale IT infrastructures that continuously deliver services to attract and retain users: the larger its user base, the larger is the potential for growing revenue. Rather than rely on traditional hardware and software companies to supply the components for the underlying network infrastructure, some companies have opted to build these components using COTS hardware and open source software.

Because social networks hold the personal information of millions of users worldwide, their IT staff recognize security to be a constant and ongoing concern. Users expect a social network to be “always on”, and the social network provider cannot afford to allow any issue preventing user access. More importantly, these networks must protect themselves from anyone hacking into users’ accounts. If they cannot protect their users against a security attack, having that information leaked or stolen (e.g. passwords, credit card information) will discourage use of the social network, ultimately leading to a decline in network expansion and revenue generation.

A security solution that monitors traffic at Web-scale without disrupting service delivery is of utmost importance. Using Napatech’s NAC is ideal given both the variety and amount of traffic the underlying infrastructure supports. With the NAC enabling complete packet capture, a social network can monitor and examine all traffic, enabling IT to identify every possible security vulnerability within the social network infrastructure.

Other key NAC features that enable the social network to detect security breaches under all possible network conditions:

- Distribution of the network processing load via its multicore architecture, maximizing the number of packets processed at any given moment;
- Large packet buffers allow the application to process massive amounts of network traffic in real time, enabling zero packet loss;
- The merging of multiple ports into one time-ordered packet stream (with hardware timestamps), allowing precise analysis of all vulnerable network traffic;
- Proven hardware reliability to ensure maximum uptime for network monitoring activities in high-speed networks.

Anyone that need to secure their IT infrastructure have industry-standard PCAP applications such as Suricata, Bro, and Wireshark at their disposal. The problem is the scale and bandwidth at which social network providers operate today. Integrating these applications with the NAC allows social networks to ensure proper security measures under all network conditions, ideally eliminating any future breach or hack.

Conclusion

Building out an enterprise-grade security solution for corporate IT networks using COTS components is achievable regardless of the size of the network infrastructure and the amount of traffic generated. Some social networks today have embraced a DIY approach to deploy a security solution for their Web-scale infrastructures. They have recognized that complete packet capture is the only viable approach in monitoring security continuously. Using Napatech’s NAC provides the ideal foundation for enabling such security monitoring on any given network.

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

Napatech Korea
Seoul, South Korea
Tel. +82 2 6001 3545

ntapacsales@napatech.com
www.napatech.com