napa:tech;
RECONFIGURABLE COMPUTING

Symantec

CASE STUDY

Gigabit performance gain for Symantec DLP

Challenge
A major US medical firm acutely needed to prevent leakage of sensitive patient data. But as their outbound traffic had exceeded the scope of their standard server deployment, Symantec DLP could not perform to its full potential.

Solution
The medical firm approached Napatech to optimize their deployment. By simply adding Napatech FPGA SmartNIC software and hardware to their existing infrastructure, Napatech enhanced the firm's DLP and ensured optimal performance, even under ultra-highspeed conditions.

Benefits
With their infrastructure fueled by Napatech SmartNICs, the firm's Symantec DLP performance could be multiplied to handle as much as 4 x 900 Mbps. This was achieved at minimal cost and effort, compared to the alternative solution of integrating multiple servers and load balancers.

napa:tech;
RECONFIGURABLE COMPUTING

Industry pain points

Today, data loss prevention (DLP) is a core discipline in most security governance frameworks. Companies typically rely on intelligent security solutions, like Symantec DLP, which are highly efficient both in the combat against malicious data theft and in cases where employees unknowingly leak confidential data. Trouble is that there might be an upper limit to the data volume the given deployment can handle. So even though the DLP solution excels at its core expertise, it might still suffer from blind spots if the system is overloaded.

Client challenge

A major US medical firm was faced by this challenge as their egress traffic had exceeded the processing capacity of their DLP deployment. Operating in the strictly regulated pharmaceutical industry, the firm needed to safeguard a massive range of sensitive patient data, from insurance information to Social Security Numbers (SSN) and driver's license details.

The firm therefore needed to underpin their DLP solution with an extra layer of security, giving them full visibility of their outbound traffic. The firm was already deploying Network Monitor, the Symantec DLP module, which sits at egress and inspects all outbound, unencrypted network traffic via a mirrored/SPAN port.

A COTS server architecture with a standard Network Interface Card (NIC) had previously been enough to meet their needs. But as their outbound traffic now surpassed Symantec's maximum processing capacity of 300 Mbps for Windows and 650 Mbps for Red Hat, this solution no longer sufficed.

Server configuration	Operating system	Bandwidth (Mbps)
Native packet capture	Windows Server 2016	300
	Red Hat Linux 7.5	650

Source: Symantec Sizing Guidelines (cf. Table 2-5)

Solution

To solve the problem, the medical firm approached Napatech to optimize their deployment. By simply adding Napatech FPGA SmartNIC software and hardware to their existing infrastructure, the firm ensured that their DLP solution would perform at its best, even under ultra-highspeed traffic loads.

Industry-best buffering skills

Where a general-purpose NIC only includes a very limited packet buffer and loses packets as soon as the buffer is full, Napatech SmartNICs contain an extensive onboard buffer, which ensures guaranteed data delivery, even in circumstances where delivery to the DLP application is congested. The Ethernet frames are simply parked in server memory until the application is ready to accept them, ensuring that all the data is made available for analysis when needed.

The Napatech SmartNIC distributes the captured traffic to multiple DLP threads in hardware, resulting in a huge performance gain. With a general-purpose NIC, this packet distribution happens in software, which puts an additional processing load on the DLP.

Key benefits

Reusing their existing server infrastructure now fueled by Napatech SmartNICs, the medical firm's DLP performance could be multiplied to handle as much as 4 x 900 Mbps, with no packet drops.

Server configuration	Operating system	Bandwidth (Mbps)
Napatech SmartNICs	Windows Server 2016	900 x 4 capture interfaces
	Red Hat Linux 7.5	900 x 4 capture interfaces

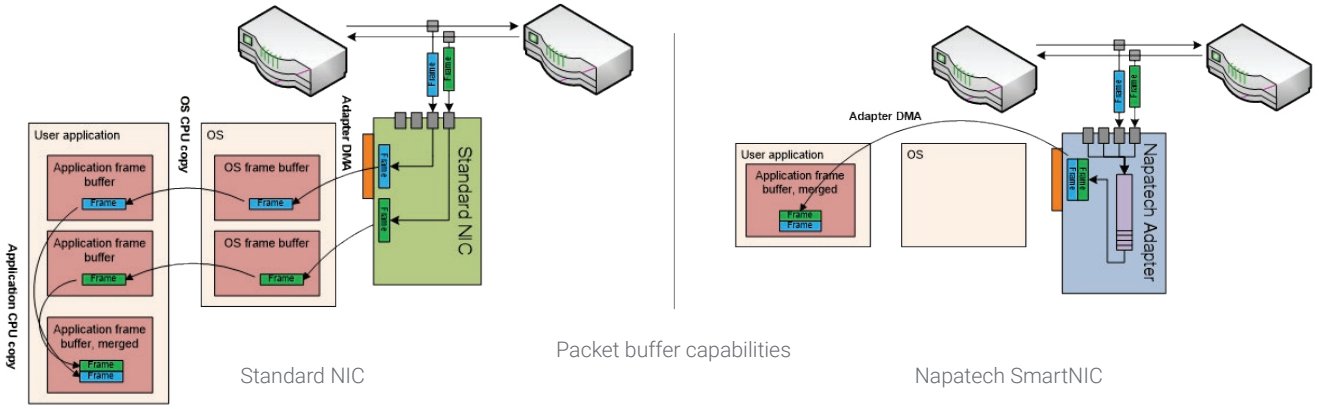
Source: Symantec Sizing Guidelines (cf. Table 2-5)

This was achieved at minimal cost and effort, compared to the alternative of integrating multiple servers and costly load balancers.

Customer value:

- Symantec DLP at 4 x 900 Mbps
- Ease of deployment
- Low upgrade expenditures
- Fast ROI

For more information, see www.napatech.com/solution-descriptions/symantec-dlp



Standard NIC

Packet buffer capabilities

Napatech SmartNIC

DN-1232