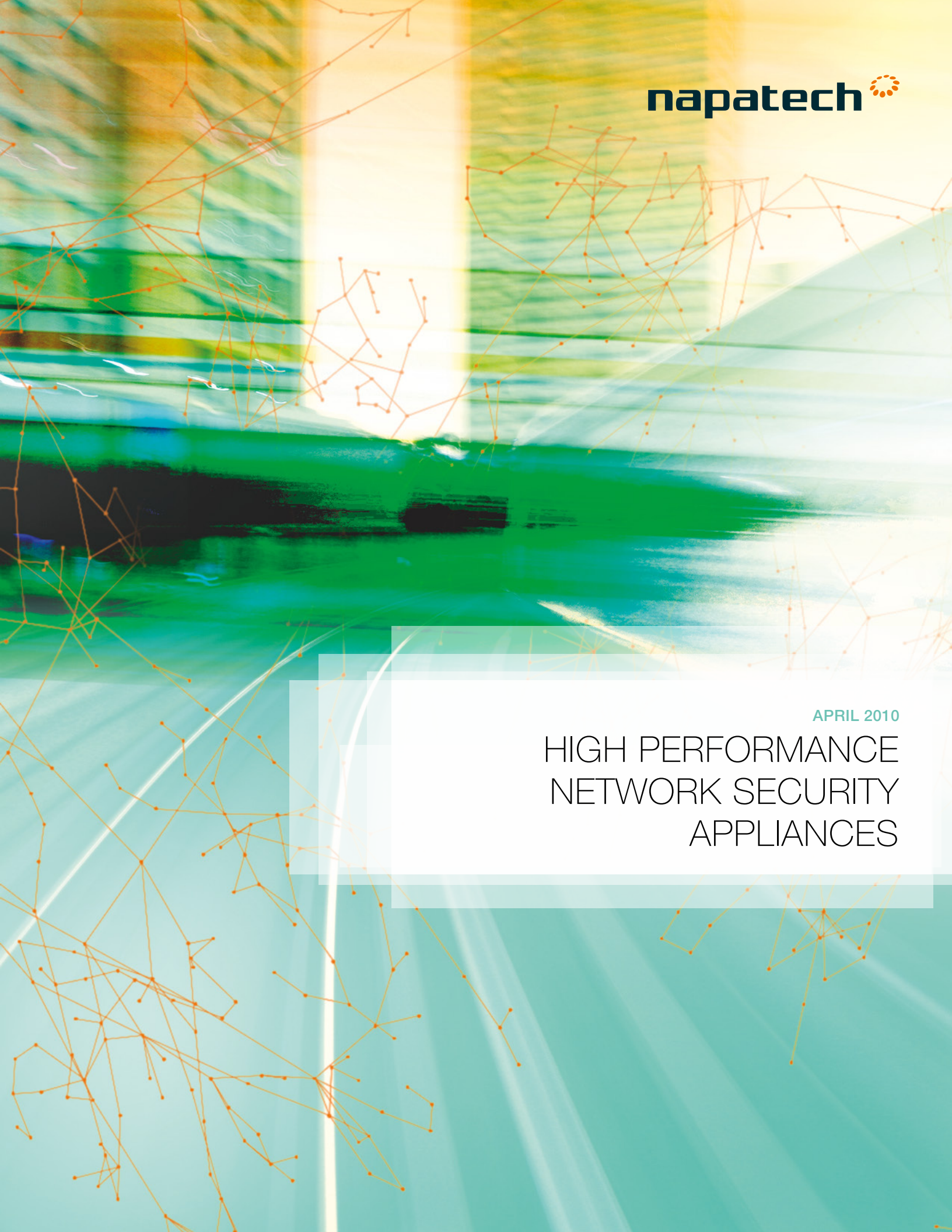


APRIL 2010

HIGH PERFORMANCE NETWORK SECURITY APPLIANCES

HIGH PERFORMANCE NETWORK SECURITY APPLIANCES

Network security appliances are an essential part of any enterprise's network security strategy. Firewalls, Intrusion Detection and Prevention Systems (IDS/IPS) and Security Information and Event Management (SIEM) systems ensure that threats are stopped before they reach clients and otherwise wreak havoc on enterprise networks.

Demands on network security appliances are increasing as we move to even faster Ethernet and IP networks, such as 10 Gbps networks. More and more services are moving to IP, which is driving the need for more bandwidth, but also increases the pressure on network security appliances to keep up. Real-time services, such as VoIP, IP video streaming, teleconferencing and many cloud computing services cannot tolerate packet loss or latency. At 10 Gbps, making sure that network security appliances will not impact these services is critical.

For example, at two times 10 Gbps (two ports on a 10GbE in-line device) up to 30 million packets per second need to be captured, analyzed in real time and, in the case of in-line appliances, re-transmitted if there are no issues. That's a packet every 33ns! Needless to say, this is a significant challenge and throughput (how many packets or bits can be processed by the network security appliances at a time) is a key benchmark.

According to Frost & Sullivan, there is a strong correlation between throughput and the price of a network security appliance. This is shown in Figure 1.

In other words, the more you can process, the more value your network security appliance provides. As the data infers, not all network security appliances can provide full throughput.

The challenge can be broken down into two key elements:

- Getting data in and out of the appliance as efficiently as possible
- Harnessing as much processing power as possible to process data

Systems exist that can meet these demands, but they are often based on proprietary hardware designs and can be expensive to develop and maintain. There is another way, which can provide the same performance (or even better) with lower development cost, maintenance, risk and time-to-market.

The answer is to adopt a universal network appliance approach. A universal network appliance uses commerical off-the-shelf products to provide a generic network appliance platform that can be applied to a number of applications, including the network security applications listed above.

FIGURE 1
Price per throughput comparison for IDS/IPS
Total IDS/IPS Market: Network IDS/IPS Appliance Average of Throughput per Price Band (World), 2006. Note: All figures are rounded: the base year is 2006. Source: Frost & Sullivan.

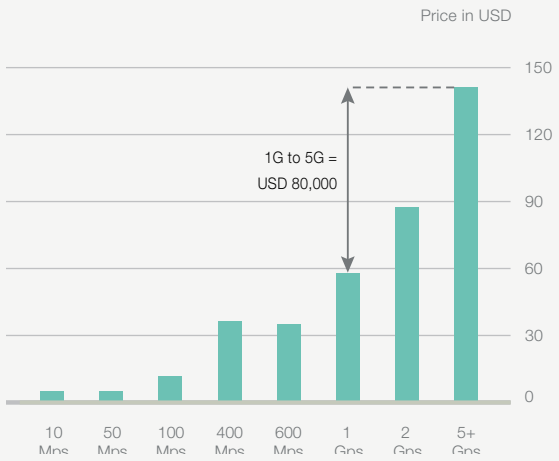


FIGURE 2
Zero loss throughput for different frame sizes (in bytes)
10 Gbps throughput performance of server NIC and Napatech accelerator

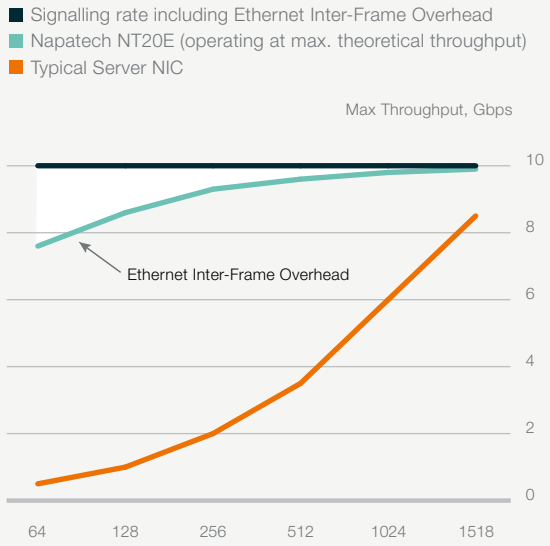
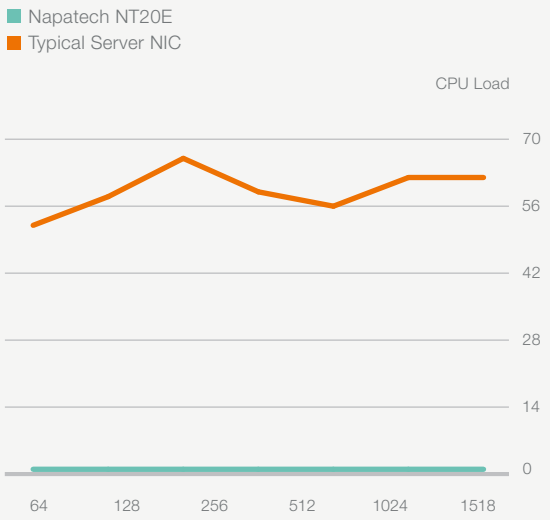


FIGURE 3
CPU load at max throughput for different frame sizes (in bytes)
CPU load for transferring data to the application



The key components are:
- A standard PC server based on the latest generation of processing chips
- An accelerator for network monitoring and security applications that provides fast and efficient data input/output

Dell, HP, Intel, IBM and Cisco and others provide very powerful standard servers today often based on AMD or Intel chipsets (e.g. Intel's Nehalem multi-CPU core chip architecture). These servers, which can be obtained for a few thousand dollars, provide unprecedented processing power and efficient memory architectures. In addition, investment in these servers and chip architectures is driven by a much larger market ensuring continuous innovation and lower prices relative to performance.

However, the key to unlocking this potential is an efficient data input/output mechanism that will ensure that:
- All received packets can be captured, analyzed and re-transmitted in real time
- No packets are lost
- No processing power is used by the server in handling data input/output
- An efficient transfer mechanism is in place that makes optimal use of multiple CPUs

Network Interface Cards (NIC), which are normally used by standard servers for data input/output, struggle to meet these requirements. This is because these server NICs are normally used for communicating between two peers and not for examining all packets. It should be noted that the basic design principles that NICs are based upon are also the basis for many data input/output designs in existing proprietary network security appliances, which also suffer from some of the same issues.

What is required is a NIC that is designed for network monitoring and analysis, yet is compatible with standard servers. Accelerators for network management and security applications, such as Napatech's, provide such a solution. To understand the difference, take a look at the performance graphs in Figure 2 and Figure 3.

As can be seen in the graph, the Ethernet inter-frame overhead of the Inter-Frame Gap (IFG) and preamble naturally reduces the effective amount of data that can be processed in real time. This effect increases as the Ethernet frame size gets smaller. Napatech accelerators can operate at the theoretical maximum effective throughput when taking inter-frame overhead into account, while standard server

NICs struggle to provide even a fraction of this throughput. The simple reason is that these adapters cannot handle the up to 15 million packets (or 30 million in duplex operation) that need to be processed on the port.

At the same time, the normal operation of NICs relies on the server CPU and operating system to assist in transferring data from the adapter to the application. At 10 Gbps, this can lead to up to 70% of a single CPU just being used for transferring data.

Napatech accelerators process all data on the accelerator itself and use an efficient Direct Memory Access (DMA) process to move data directly into the memory of the application without involving the operating system or consuming CPU resources. This ensures that maximum CPU processing power is provided to the application.

Finally, Napatech accelerators provide the intelligence to decode the packet information received and use this information to define flows. Flows indicate data that is related based on source/destination, protocol type, tunnel identifier, etc. The user can then direct these flows to up to 32 different CPUs. This allows specific flows to be processed according to their needs by individual applications running in parallel increasing the efficiency and throughput of the system many-fold.

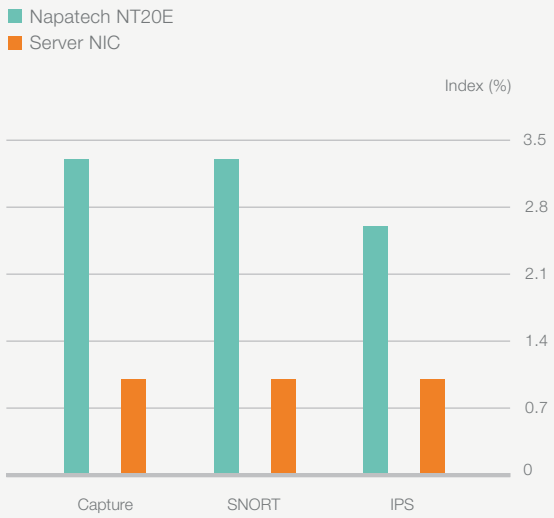
The net result of these real-time network analysis features are that a significant performance improvement can be achieved. As shown in Figure 4, an accelerator can provide a 2-3 times performance improvement for network security appliance applications.

For example, Napatech has helped IPS vendors to provide over 9 Gbps throughput performance using a single Napatech accelerator combined with the latest generation standard server, which is significant when compared to Frost & Sullivan's price analysis in Figure 1. More throughput means more value for customers and better price positioning for IPS vendors.

The combination of a standard server and accelerator thus provides a powerful platform for developing a high-performance network security appliance:

- at a much lower cost (as no proprietary hardware needs to be developed)
- at a much lower risk (the platform is off-the-shelf, tested and verified in the field)
- faster (as development can be focused on application development and not hardware)

FIGURE 4
Relative performance of server NIC versus Napatech accelerator



COMPANY PROFILE

Napatech is the world leader in accelerating network management and security applications. As data volume and complexity grow, the performance of these applications needs to stay ahead of the speed of networks in order to do their jobs. We make this possible, for even the most demanding financial, telecom, corporate and government networks.

Now and in the future, we enable our customers' applications to run faster than the networks they need to manage and protect.

Napatech. FASTER THAN THE FUTURE


The combination of
a standard server and accelerator
provides a powerful platform for
developing a high-performance
network security appliance

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

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

NORTH AMERICA
Napatech Inc.
Boston, Massachusetts
Mountain View, California
Washington D.C.

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

SOUTH AMERICA
Napatech
São Paulo, Brazil

Tel. +55 11 2127 0782
ntsouthamericasales@napatech.com
www.napatech.com

APAC
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