’’A new approach to network security appliance development that promises lower overall cost, lower risk and faster time-to-market”
Intrusion prevention requires systems that can react quickly to potential threats and attacks. With over 7.1 million unique malware signatures currently detected, networks are constantly under attack. The attackers are no longer technically literate, anti-social teenagers with a point to prove, but highly organized criminal organizations who see cyber-crime as a lucrative new "business opportunity".

The ability to detect an attack in real time is therefore paramount. The combined forces of a network firewall followed by an effective, real-time network Intrusion Prevention System (IPS) working in concert with a comprehensive Security Information and Event Management (SIEM) system provides the bulwark of an effective network security solution to combat attacks and protect users and businesses alike.

As networks move to both 1 Gbps and 10 Gbps connectivity, the processing requirements demand higher performance network security systems or appliances. For example, at 1 Gbps, up to 3 million packets per second need to be processed. At 10 Gbps, that figure rises to 30 million packets per second or a packet every 33 nanoseconds. A nanosecond is 1 billionth of a second, so 33 nanoseconds is not a lot of time to receive a packet, check the authenticity of the packet, the content and the sender and then send the packet on its way.

To address these performance demands, network security appliance vendors have developed systems based on proprietary hardware that have the processing power and memory required to operate at these speeds.

This paper describes the next phase in development of network security appliances, namely the emergence of the universal network security appliance. In some senses this phase is a commoditization, and while this might be true in technical terms, the term does not do justice to the technical performance that is achieved and the future performance targets that can be reached. In other words, universal network security appliances can provide the same performance, but in a much more efficient and cost effective manner.

This next phase is a necessary step in the development of the network security appliance market to ensure affordable solutions that can maintain pace with bandwidth demands and the ingenuity of cyber-criminals.

**NETWORK SECURITY SYSTEM ARCHITECTURE**

Most people associate security with firewalls and antivirus scanners implemented in software and running on client PCs. But, the world of network security encompasses a range of solutions that are designed to stop threats and attacks before they ever reach clients.

Modern enterprises now maintain sophisticated data communication networks that can range from a single Local Area Network (LAN) for a small office to global communication networks linking hundreds of branch offices to multiple headquarters. These networks are not only used for data communication, but also form the basis for a range of other services, such as Voice over IP (VoIP) telephony, teleconferencing and a range of cloud computing services, such as remote access to hosted Customer Relationship Management (CRM) or Enterprise Resource Management (ERP) systems.

This diversity and flexibility underlines the value of communication networks, but also exposes weaknesses that can be exploited by would-be criminals. It is therefore important to meet these threats at the point of entry into the network to minimize their proliferation throughout the network.
A typical enterprise network for a data center, company headquarters or larger branch office location would resemble the diagram in Figure 1.

The enterprise network is based on a hierarchical architecture connecting multiple servers. Clients access servers via Ethernet access switches, which are connected by Ethernet distribution switches in a hierarchical structure. The distribution switch itself provides access to the outside world via an IP router, which has a redundant backup IP router to ensure access to the Internet at all times.

A typical network security architecture includes a firewall and some means of intrusion detection. The firewall typically sits between the gateway IP router and main Ethernet distribution switch. This ensures that only traffic that meets firewall rules is admitted into the network. Most firewalls operate with a “De-Militarized Zone” (DMZ) concept whereby external access can be provided to certain servers, such as a Virtual Private Network (VPN) server, a web server or other extranet server.

Firewalls traditionally provide coarse filtering of traffic based on port information. Next generation firewalls, on the other hand, include more intelligence so that higher layer application information can be used to detect attacks.

Firewalls are supplemented by Intrusion Detection Systems (IDS) or IPS, which ensure that coordinated attacks are thwarted. Some next generation firewalls now include some intrusion prevention functionality, which can be attractive for small to medium business applications. Nevertheless, the current practice is to supplement a firewall appliance with a stand-alone intrusion detection or prevention system. These provide the fine-granularity filtering of traffic examining each packet to detect key signatures and anomalies that can be used to identify a coordinated attack or threat (i.e. a Distributed Denial of Service (DDoS) attack).

An IDS monitors traffic sent from the firewall to the distribution switch to detect anomalies and known threats or attacks based on their distinctive pattern (often referred to as a “signature”). The IDS maintains a “white list” for approved
packet flows known to be authentic and a “black list” for packet flows known to be suspicious. If a suspicious signature is detected, the IDS typically notifies the network operator via an event.

As shown in Figure 2, the IDS is “out-of-line” (i.e. it is not in the main flow of traffic, but works on a copy of the traffic being sent and received). An IPS, on the other hand, is “in-line”. This is significant, as it allows the IPS to react immediately to a threat by blocking suspicious traffic. The security system is now no longer reactive, but proactive by blocking traffic, while waiting for the network operator to confirm. Because of this benefit, there is a trend towards replacement of IDS solutions with IPS solutions.

The consequence of this is that two pieces of equipment are now placed “in-line” in the path of traffic. It is vital that these appliances do not affect traffic by introducing too much delay or latency in the traffic path or taking down the connection should something happen to the network security appliance. It is equally important that these appliances provide high performance to ensure that traffic is not delayed or even dropped while waiting for “approval”.

Many enterprises are augmenting their network security solutions with SIEM systems. SIEMs have the ability to assimilate information from a number of sources to establish a profile for the network under normal working conditions. By monitoring input from firewalls, IDS, IPS and other security systems and by simultaneously monitoring network traffic and performance, it is possible to detect traffic anomalies. For example, this could be certain users showing more activity than normal, certain servers being accessed more than normal, etc. In this regard, a SIEM can be considered an “umbrella” solution encompassing both network security and network activity monitoring.

Most SIEM systems are software-only solutions running on dedicated servers. They use Cisco netflow (or Juniper jflow or other similar information) to gather network performance
data. This data is usually accessible through a so-called “SPAN port” on the router or switch. However, while netflow data can be quite informative, it is not always completely reliable as the router or switch needs to provide this information, while also routing or switching traffic. Routers and switches can become loaded to the point where they cannot provide this information, or at least not provide it reliably.

Therefore, some SIEM systems use network probes or “taps” to capture packets directly from critical links and provide the network data to the SIEM, as shown in the diagram below.

The advantage of this approach is that the information from probes can be guaranteed to be real-time, where no packet information is lost. In other words, it provides the most comprehensive and up-to-date information on what is happening in the network and can be relied upon. This, of course, assumes that the network probe has been built properly using intelligent network adapters. These adapters provide full throughput, do not drop packets and do not place a load on processing resources.

If a separate network performance management system is available, its data could also be used as input to the SIEM, though this would depend on the integration possibilities between these two systems.

The next section will describe in detail how high performance IDS, IPS and SIEM network probes can be built using commercial off-the-shelf PC servers and accelerators using a universal network appliance approach.

BUILDING NETWORK SECURITY APPLIANCES

In Napatech’s white paper “A Guide to Building Universal Network Appliances”, a network appliance is defined as having the following generic characteristics:

- It is a stand-alone device dedicated to a particular application
- It can either sit “out-of-line” (i.e. capturing or “sniffing” packets) or “in-line” (i.e. as part of the link both receiving and transmitting data) depending on the needs of the application
• It requires fast, high-speed data input/output with full throughput for all packets no matter the packet size
• It requires sufficient processing power to process all received packet data in real time, especially at high line-rates
• It requires efficient memory structures to ensure that there are minimal delays in accessing data

Using this platform, a number of applications can be defined in software to provide the application-specific functionality required. For network security appliances, the application-specific functionality could be firewall, IDS or IPS functionality. It could also be a network probe providing captured packet data to a SIEM system.

Today, most network security appliances are based on a proprietary hardware platform, which is customized to provide high performance. However, a universal network appliance is a generic hardware platform based on commercial off-the-shelf products that not only provide the same (or sometimes better performance), but have the potential to do so at a much lower total cost for the network appliance vendor.

The key components of the universal network appliance are:
• Standard PC servers with underlying server CPU processing and memory architecture
• Intelligent network adapters
• Customer proprietary application software defining the specific functions of the network appliance
• High-speed storage solution for capture-to-disk that will allow intelligent indexing for fast retrieval of captured data

Standard PC servers can be obtained from Dell, HP, Intel, IBM or Cisco at relatively low prices. However, a standard server Network Interface Card (NIC), which is normally used for communication, is not suitable for network analysis and network security. The main reason is that server NICs are not designed to handle all the traffic available on a link or port; only traffic with the right MAC address. When server NICs are used for monitoring networks, such as in network security applications, they quickly become overloaded, consuming precious processing resources and indiscriminately drop packets.

In Figure 4, the maximum theoretical throughput that can be achieved is shown. The figures supporting this graphic are shown in Table 1.

![Figure 4](image)

**TABLE 1**

Max theoretical throughput for 10 Gbps Ethernet at different frame sizes with zero packet loss

<table>
<thead>
<tr>
<th>Frame size</th>
<th>64</th>
<th>128</th>
<th>256</th>
<th>512</th>
<th>1,024</th>
<th>1,518</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gbps</td>
<td>7.6</td>
<td>8.6</td>
<td>9.3</td>
<td>9.6</td>
<td>9.8</td>
<td>9.9</td>
</tr>
</tbody>
</table>

As can be seen, intelligent network adapters such as Napatech accelerators for network management and security applications are capable of performing at maximum throughput. Typical Server NIC adapters struggle at lower Ethernet frame sizes. This is because the number of frames increases dramatically, which can be viewed in Figure 5.

As shown, typical Server NICs cannot handle more than 979k frames per second, while the demand at 10 Gbps is to capture and analyze up to 14.8 million frames per second.
One of the reasons why Server NICs struggle is that these adapters transfer data frame-by-frame. This operation is performed by the NIC driver and operating system and uses a large percentage of CPU processing resources, as shown in Figure 6.

Napatech accelerators use an entirely different approach. They transfer data directly to the network application bypassing the driver and operating system. This means that almost no CPU processing resources are used. By using an accelerator (such as the Napatech NT20E used in the measurements), both throughput and CPU load are improved dramatically.

MEETING PERFORMANCE OBJECTIVES AND ACCELERATING APPLICATIONS

Accelerators also have the ability to improve performance by making efficient use of available CPU resources. In Napatech’s white paper “A Guide to Building Universal Network Appliances”, it was shown that the Nehalem architecture is based on multiple CPU processors or cores with Symmetrical Multi-Threading (called hyper-threads by Intel). Napatech accelerators are designed to make optimal use of multiple CPUs.

Napatech accelerators are capable of decoding frames and packets and using this information to define flows. The flows are based on protocol information indicating the source and destination, the application used to send the frame or IP packet and, if applicable, an identifier for the tunnel being supported by the frame.

These flows can then be directed intelligently to up to 32 CPU cores. This can be on a balanced basis, where each CPU is equally loaded or where specific type of flows (for example tunnel traffic flows or HTTP flows) are directed to specific CPUs. In this way, a number of flows can be processed in parallel by the same application running on multiple CPUs or several applications can be run simultaneously each working on their own flow types.

The key to network security appliance acceleration lies in the combined effect of higher throughput, lower CPU load and intelligent flow distribution that accelerators provide.
PERFORMANCE REQUIREMENTS FOR NETWORK SECURITY APPLIANCES

For network security appliances, performance is still key, especially throughput. According to Frost & Sullivan, there is a direct relationship between throughput performance and the price users are willing to pay for a network security appliance (see Figure 7).

This is a trend that can also be seen for other network security appliances. There is therefore a clear need for better throughput performance despite the fact that most network security appliances are based on proprietary hardware. There are two reasons for this apparent paradox:

- Much of the throughput bottleneck is due to application-level processing and lack of sufficient processing power and/or memory
- Data input/output is based on the same technology as standard network interface cards, which are not capable of providing full throughput

But, as we have seen in Figure 4 and Figure 6, both throughput and CPU load can be improved dramatically by using a Napatech accelerator. Therefore, by adopting a universal network appliance approach, it will be possible to:

- Address the application-level processing bottleneck by ensuring that data input/output handling is fully off-loaded
- Remove the data input/output bottleneck

With next to zero CPU load, almost all of CPU processing power is now available to the network security application rather than 30% to 40% as seen above. This accelerates performance and enables the development of a high throughput network security appliance.

Napatech accelerators also provide the ability to intelligently identify and distribute flows to up to 32 CPU cores, which allows parallel processing and better throughput.

The investment in a universal network appliance approach can be justified by the performance gains that can be achieved and the willingness of customers to pay for this performance. As Figure 7 clearly shows, an improvement of throughput performance from 1 Gbps to 5 Gbps can result in up to $80,000 more revenue per port.

FIGURE 7
Price per throughput comparison for IDS/IPS
Total IDS/IPS Market: Network IDS/IPS Appliance Average Throughput per Price Band (World), 2006. Note: All figures are rounded: the base year is 2006. Source: Frost & Sullivan.

FIGURE 8
Relative performance of server NIC versus Napatech accelerator

Napatech NT20E
Server NIC
The stage is now set for a new approach to network security appliance development that promises lower overall cost, lower risk and faster time-to-market with new high performance products.

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

UNIVERSAL NETWORK SECURITY APPLIANCE A REALITY
Based on the above, it should be clear that the combination of a standard server and accelerators provides a powerful platform capable of supporting 10 Gbps network security applications. Studies by Napatech have shown that a 2 to 3 times improvement in performance compared to server NICs is achievable and have been confirmed by customers, as shown in Figure 8.

For example, Napatech has helped IPS vendors to achieve 9 Gbps throughput performance on their network security applications using a universal network appliance approach. With new server generations this performance will probably improve even further.

Developers of network security appliances based on proprietary hardware designs can justifiably point to the shortcomings of a standard PC server using a typical server NIC with regard to performance. However, with the latest servers and intelligent network adapters from companies like Napatech, a product development strategy based on standard servers can provide the performance required to meet network security appliance needs, even at speeds of 10 Gbps.