

**The Profound Benefits  
of  
Network-Based Intrusion Prevention**



## Table of Contents

Table of Contents .....	2
The Power of Network-Based Intrusion Prevention .....	3
Network-Based Intrusion Prevention – A Primer .....	3
NBIPS – Bilateral Peer-to-Peer Protection .....	4
Network-Based Intrusion Prevention – Like Having 10,000 Fingers To Plug The Holes In The Dyke .....	5
Centralized Protection Of All Core IT Assets .....	5
Protecting Operating Systems (Desktop and Server) .....	6
Application Security .....	7
Web Services Security (Port 80 Applications).....	7
Infrastructure Protection.....	8
The Costs of Insecurity Become the Profits of Security.....	8
Basic Requirements for Network-Based Intrusion Prevention .....	8
Low Latency – A Must Have .....	8
Backbone Speeds and Large Session Counts .....	9
Intrinsic Reliability – Dependable Security .....	9
Absolute Precision .....	9
Conclusion.....	11

## The Power of Network-Based Intrusion Prevention

The advent of Network-Based Intrusion Prevention heralds a new era of effective and efficient information security for corporations, educational institutions and government agencies. In effect, Network-Based Intrusion Prevention Systems (NBIPS) transform networks from a vulnerable and weak IT element to a tremendously powerful weapon against cyber-terrorism. The network becomes a potent and forceful instrument of protection – continuously defending every resource attached to it. Desktops, servers, operating systems, applications and Web services are aggressively protected from both external and internal attacks by Network-Based Intrusion Prevention Systems.

As well, the cost of securing your information assets declines dramatically with the deployment of Network-Based Intrusion Prevention. These efficient systems continuously filter attacks as they attempt to traverse the network and as a result, no damage occurs and no clean-up is required. Security administration is reduced and system downtime as a result of attack is eliminated.

## Network-Based Intrusion Prevention – A Primer

An NBIPS installs in the network and is used to create physical security zones. (Figure 1)

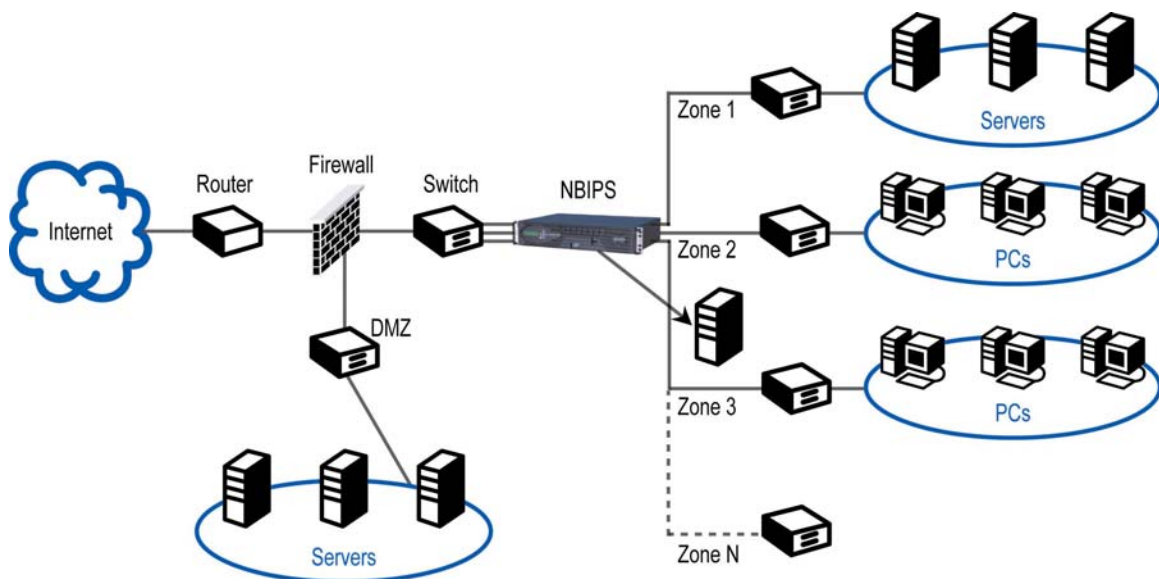


Figure 1 – Multi-Zone Network Security

In essence, the network becomes intelligent and is able to quickly and precisely discern good traffic from bad traffic. The Intrusion Prevention System becomes a

“jail” for hostile traffic such as Worms, Trojans, Viruses, Blended Attacks and Polymorphic Threats.

NBIPS are made possible through the deft blending of high-speed Application Specific Integrated Circuits (ASICs) and newly available Network Processors. Network Processors are very different from microprocessors in that they are specifically designed to process a high-speed flow of network traffic by executing tens of thousands of instructions and comparisons in parallel. A microprocessor, such as the Pentium<sup>®</sup>, was designed as a general-purpose processor for graphics and spreadsheets and only executes one instruction at a time.

Network-Based Intrusion Prevention Systems are an extension of today’s Firewall technologies. To some extent, you can think of an NBIPS as a Seven-Layer Firewall. Today’s Firewalls inspect only the first four layers of any packet of information flow. NBIPS inspect all 7 Layers, making it impossible to hide anything in the last four layers of a packet (Figure 2).

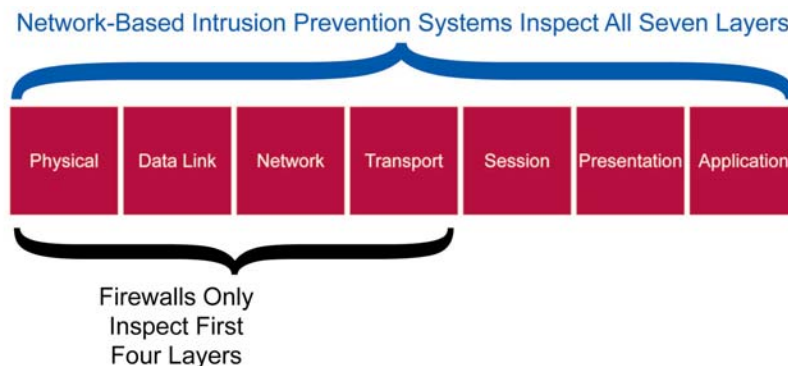


Figure 2 – Seven-Layer OSI Information Model

## NBIPS – Bilateral Peer-to-Peer Protection

Peer-to-peer applications like Limewire, Grokster, Morpheus, Kazaa, represent a tremendous threat to all organizations. These file-sharing programs have proliferated and are being used by employees, students and competitors to steal sensitive information and to share copyrighted materials. A well-designed NBIPS should protect from the illegitimate use of these tools. A NBIPS should be able to:

- Protect your bandwidth by rate limiting or blocking illegitimate use of file sharing applications.
- Limit your exposure to copyright infringement suits and royalties (from your employees or students breaking copyright laws)
- Protect your intellectual property from file sharing theft

Content providers are aggressively seeking damages from corporations and educational institutions that are not taking steps to eliminate unauthorized sharing of copyrighted materials like songs and movies. A NBIPS with anti-piracy capabilities will protect your organization from potentially massive legal judgments.

## Network-Based Intrusion Prevention – Like Having 10,000 Fingers To Plug The Holes In The Dyke

Network-Based Intrusion Prevention Systems can be used to protect any element that is connected to the network. Operating systems, application servers, Web servers, Web applications, wireless networks and even routers and switches can be protected through NBIPS deployment. (Figure 3)

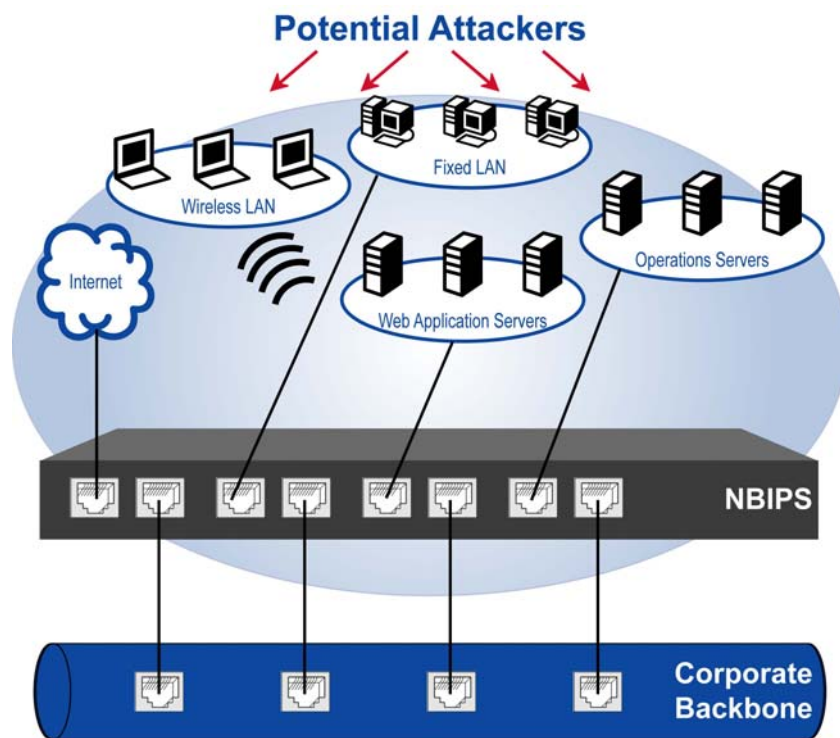


Figure 3 – NBIPS Deployment

## Centralized Protection Of All Core IT Assets

Network-Based Intrusion Prevention Systems significantly reduce the time and expense associated with securing a multi-vendor environment. The average enterprise has five different operating systems deployed and has at least nine mission critical applications running at any given time. Each operating system and application vendor has its own unique security vulnerabilities and

weaknesses, leaving a typical organization with hundreds of vulnerabilities at any given time. How do you manage so many vulnerabilities with so many vendors? Either you ignore the situation or you spend hundreds of thousands of dollars every year trying to keep up with patches. Or, you could leverage Network-Based Intrusion Prevention to centrally protect this myriad of operating systems, hosts, and applications. Case in point:

**A major university deployed Network-Based Intrusion Prevention to protect over 5,000 Windows XP hosts. On August 14, 2002, it was reported that a vulnerability in the Microsoft Help and Support Center HCP VRI handler could allow a remote attacker to delete files on another user's computer. Faced with weeks of exposure and an estimated 220 man-hours to patch all of the XP hosts and a total cost of \$24,000, the University instead asked their NBIPS vendor to provide a new attack filter for the exploits against the Windows XP Help vulnerability. Delivered 18 hours later, the University was now fully protected. Total cost \$1,100. Total cost savings of \$22,900 from a single incident.**

## Protecting Operating Systems (Desktop and Server)

Operating systems like Windows, Linux and Unix are all vulnerable to attack. A network that has been augmented with NBIPS will filter attacks before they can infect and infiltrate your computing systems. Attacks like Code Red (single attack vector), Nimda (multiple attack vectors), and Sapphire (single UDP packet) are stopped cold in the network.



## Application Security

Mission critical applications like financial systems and collaboration systems are all vulnerable to attack. Outlook and Exchange, Notes, Instant Messaging, Oracle database, MS SQL and IBM DB2 are all examples of applications that get protected by a well designed NBIPS. Examples of exploits that are extinguished through an NBIPS armed network include:



Resolution Service Buffer Overflow



Malformed MIME Header DoS



eManager Buffer Overflow



Log On “%%%" DoS

## Web Services Security (Port 80 Applications)

Web servers (such as IIS and Apache) and Web-based applications (such as Websphere, .Net, Oracle 9i, BEA) are especially vulnerable to attack. These applications typically include complex mechanisms for parsing and handling arbitrary user input, providing many opportunities for programming errors. Examples of exploits that are extinguished through an NBIPS armed network:

Front Page Server Extensions  
Sun Cobalt RaQ4 Server  
IIS Web Server  
Apache Web Server  
Allaire ColdFusion

Visual Studio Buffer Overflows  
Remote Compromise via CGI Errors  
Chunked Transfer Encoding Heap Overflow  
OpenSSL Slapper Worm  
Sample Script Vulnerabilities



## Infrastructure Protection

Core networking infrastructure like the DNS and even Cisco routers can be brought to their knees by a savvy attacker. Infrastructure attacks such as the malformed SNMP DoS triggered by PROTOS (Cisco) and the BIND TSIG buffer overflow used by the Lion worm (DNS) are knocked down by NBIPS equipped LANs.



## The Costs of Insecurity Become the Profits of Security

A network augmented with Intrusion Prevention infrastructure becomes a hardened shield for everything connected to it – internal and external. Network crashes, server crashes, and stolen information all accrue to impact the corporate bottom line.

Network-based intrusion prevention may be the most powerful technology in the world when it comes to protecting against compromised desktops and servers, dishonest employees and industrial espionage. In the end, the payback of network-based intrusion prevention is almost immediate and in the long run it may be the difference between survival and failure.

## Basic Requirements for Network-Based Intrusion Prevention

First and foremost, NBIPS must be a highly reliable part of the network infrastructure. This means that they must be good network citizens, with very high intrinsic reliability and line-speed performance to insure no adverse effects on the network. As well, NBIPS must be absolutely precise, never confusing good traffic with bad traffic.

## Low Latency – A Must Have

NBIPS are designed from the ground up with an architecture that contemplates the requirements of a network element - much like a switch or router design. **This means that any NBIPS, to be viable, must have average latencies of less than 3 ms. regardless of frame size, traffic mix, line rate or number of attack filters/signature installed.** Otherwise, the NBIPS can dramatically reduce network performance and in some cases cause the network to crash.

Data, voice and video on a converged network all require low latency. For example, Vendor I claims to run 2 gigabits per second just like vendor T. However, traffic latency on Vendor I is about 3 seconds while traffic latency of vendor T is 50 microseconds. In essence, Vendor I is really only running an effective data rate of 22 kilobits per second making it non-viable as a network-based intrusion prevention system. Table I delineates effective data rates as a function of latency.

NBIPS Average Latency	Effective Data Range
10 microseconds	1 Gigabit
100 microseconds	100 Megabit/Sec.
1 millisecond	1 Megabit/Sec.
10 milliseconds	100 Kilobits/Sec.
100 milliseconds	10 Kilobits/Sec.
1 second	1 Kilobit/Sec.

## Backbone Speeds and Large Session Counts

**NBIPS must be scaleable to multi-gigabit speeds** in order to protect the backbone from internal threats. Most attacks today come from inside the enterprise where hundreds of thousands of simultaneous network sessions are occurring at any given time with thousands of new sessions being established every second. **At a minimum, NBIPS must support 500,000 simultaneous sessions and 10,000 new sessions per second to be deployable.**

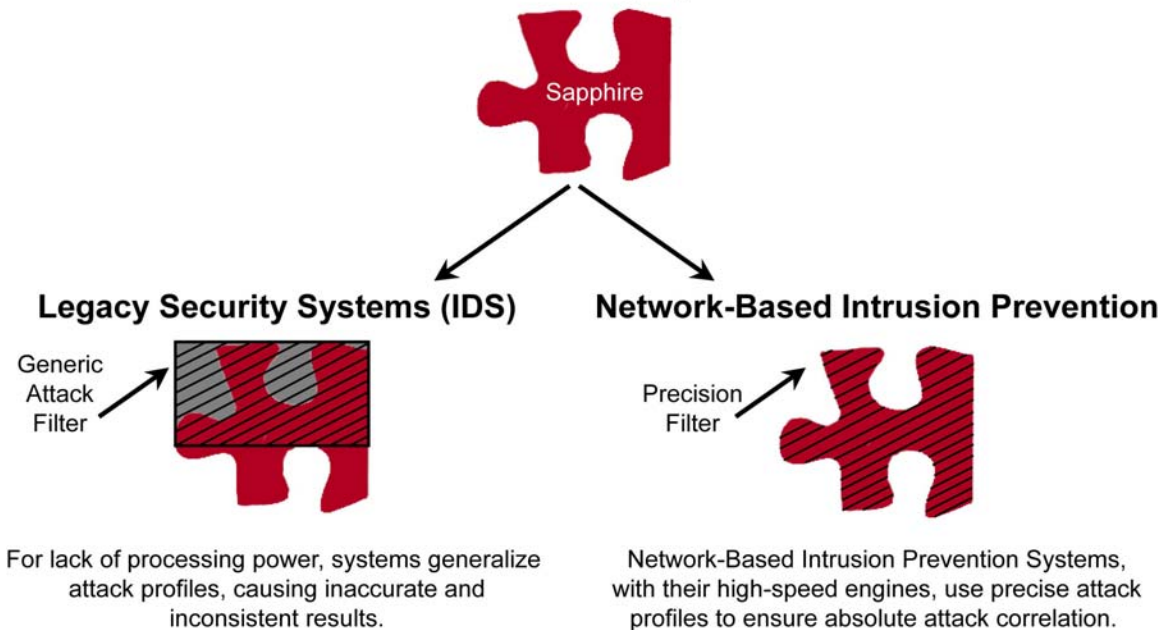
## Intrinsic Reliability – Dependable Security

Additionally, NBIPS must be intrinsically reliable. It cannot crash under any circumstances, including the most severe and aggressive attacks. If any element fails within an NBIPS -, processors, hardware, software, ASICs, etc., the network must continue to run. **The NBIPS must be able to automatically fall back to Layer 2 (transparent switch) in the case of internal failure.**

## Absolute Precision

Legacy network-based IDS systems, for lack of sufficient processing power, incorporate very general and broad signature technology (Figure 3) that often cannot discern between mission critical traffic and hostile attacks. Thus the well documented problems with false alerts. A true NBIPS, however, will have the processing power to be absolutely certain whether traffic is good or bad. **Therefore, a true NBIPS is designed much like a firewall and never blocks or drops good traffic.**

## The Attack Fingerprint



## Absolute Precision is an Absolute Requirement

In Summary, in order for any product to be deployed as a Network-Based Intrusion Prevention System it must first meet the basics of networking. These requirements must be met simultaneously in order for an NBIPS to be a reliable and transparent network element. For instance, some vendors will claim gigabit speeds but have latencies in excess of 1 second. (See Sidebar – Beware! A Sheep In Wolves Clothing!) The must haves are:

- **Low Latency** - less than 3ms. regardless of frame size, traffic mix, line rate, or attack filter count.
- **Multi-Gigabit Speeds** –To support backbone traffic and protect against internal attack.
- **Large Session Counts** – 500,000 to 1,000,000 simultaneous sessions. 10,000 new sessions per second.
- **Intrinsic High-Availability** – Must automatically become a transparent switch should any internal element fail.
- **Absolute Precision** – Can never block or drop good traffic.

## Beware! A Sheep In Wolves Clothing!

Many vendors have jumped on the Network-Based Intrusion Prevention bandwagon. Are they security wolves with strong network performance? Or are they really security sheep dressed as wolves? Here's what you need to ask your NBIPS vendor before you make a decision:

### **\*What is the latency through the NBIPS at various packet sizes?**

Your vendor should be able to provide latencies of just a few milliseconds maximum at any packet size or security posture. Some NBIPS vendors claim to have multi-gigabit speeds but have latencies on the order of several seconds. Put this type of NBIPS in your network and your gigabit Ethernet starts to run like a 1200-baud modem.

### **\*Does it ever filter or block good traffic?**

This is a measure of security precision. Many NBIPS use very general logic to discern an attack. This "fuzzy logic" results in the blocking of good traffic. As well, some NBIPS vendors, because they lack processing power, will "drop" out of sequence TCP/IP packets. Unfortunately, it is not uncommon for good traffic to be out of sequence. This type of out-of-sequence handling will degrade network performance.

### **\*Does the IPS really filter attacks or does it attempt TCP resets and Firewall shunts?**

Many IDS vendors claim Intrusion Prevention capabilities through mechanisms called TCP resets and Firewall shunts. These mechanisms are only effective in about one out of a 1,000 attacks. This is because by the time an IDS reprograms a Firewall or resets a TCP flow, the attack has already infected the network.

### **\*What happens if there is an internal NBIPS failure? Will it cause the network to crash?**

Make sure your vendor supports Intrinsic High-Availability. This means that (if you so choose) the NBIPS will fall back to a Layer 2 switching mode to ensure network availability.

### **\*How is the NBIPS kept current against emerging vulnerabilities and attacks?**

Waiting weeks for new attack filters is untenable. Vendor inoculation response time must be measured in hours, not weeks.

## Conclusion

Network-Based Intrusion Prevention Systems portend an immediate future where chaos, anxiety, cost and sweat are replaced with certainty, productivity and profitability. The nature of these systems creates a security posture never before seen and harmonizes the management of all security initiatives. We believe it is incumbent on all organizations, private and public, to deploy NBIPS for the following reasons:

- NBIPS will improve corporate productivity and profitability
- NBIPS will protect sensitive information from being stolen
- NBIPS will protect key infrastructure from imminent global cyber-attacks thus preserving standards of living and ways of life.
- NBIPS will limit copyright infringement liability

**The paybacks on Network-Based Intrusion prevention are immediate and significant.**