Global Information Assurance Certification Paper

Network-Based Intrusion Prevention System Technology

Revolution or Evolution?

Name: Stephanie Hagopian

Certification: GIAC Security Essentials Certification (GSEC)
Version 1.4b, Option 1

Date Submitted: January 5, 2004

Network-Based Intrusion Prevention System Technology
Revolution or Evolution?

ABSTRACT

Intrusion Prevention System (IPS) technology is considered one of the newest and most promising technological advancements to network security. Intrusion prevention systems, devices that combine the filtering abilities of a firewall with the packet analysis capabilities of an intrusion detection system, have already caused a lot of debate in the IT community. Many IT professionals question whether intrusion prevention technology is the only defense mechanism needed on a network, or if it is simply a new component to "defense in-depth": something that should be used in conjunction with the firewall and intrusion detection technology that already exists.

In order to fully analyze this new technology, I first summarize the benefits and weaknesses of both network firewalls and network-based intrusion detection systems (NIDS), as they are both the predecessors to intrusion prevention systems, as well as the building blocks for the technology itself. After discussing these two network security tools, I then evaluate the advantages and disadvantages of intrusion prevention systems, how they can be incorporated into a network infrastructure, and if they are indeed a "silver bullet" to network security or just another layer of good network defense.

Up until very recently, IT professionals have considered effective network security to include two major technological components: firewalls and network intrusion detection systems. As singular entities, these two technologies are not sufficient to adequately defend a network. However, when combined, firewalls and intrusion detection systems, paired with responsible system administration of individual systems, create "defense in-depth," providing layers of security in order to neutralize the weaknesses inherent to the technologies themselves.

In the past two years, intrusion prevention technology has begun to be a presence in the network security community as a genuine form of network defense. Intrusion prevention technology has the unique capability of combining firewall technology with the packet analysis capabilities of intrusion detection systems. It is a direct answer to the question network security analysts have been asking for years: how do we, as responsible network security professionals, adequately perform system security despite the weaknesses of these two forms of network defense?

In order to fully understand this new technology, it is first essential to outline why firewalls and intrusion detection systems simply do not provide enough network security for an organization, and why IT professionals feel there is a need to provide a new alternative.

Part I. Firewalls and Intrusion Detection Systems: The two foundations of network security.

A. The Inception of the Firewall

With the inception of packet filtering abilities in the mid-80s, firewall technology emerged as a legitimate element of network security. By 1997, Cisco Systems created the first commercial firewall product based on a kernel proxy architecture.[1] The Cisco Centri Firewall was the culmination of five generations of firewall advancements. (Figure 1.1) A kernel proxy firewall had the ability to do "stateful inspection" of network packets at every layer of the network stack by having the proxies reside within the kernel and pass packets through on a per session basis via custom TCP/IP stacks. In this manner, each packet was inspected at every layer from the physical hardware to the application space and back again. (Figure 1.3) At the time, this was a revolutionary concept: to have a complete 7-layer communication exchange between two network objects in order to construct proxy-based stacks dynamically for each session. Compared to most firewalls, which only view traffic on a 4-layer model that excludes application-level inspection, the Centri Firewall marked a major improvement to the basic firewall architecture. This evolution in firewall technology provided intelligent filtering on an application level, while still being able to filter and process packet data quickly and efficiently.[2]

This new generation of firewall technology, like all the previous generations, was initially regarded with a "silver bullet" mentality, as it seemed to solve the age-old problem of combining a maximum-security benefit with outstanding network performance. However, security professionals began asking themselves whether this new firewall structure solved every network security issue that existed. How intelligent was the filtering? Could it protect a web server from something like the W32.Nimda worm, which exploits Internet Explorer through port 80/tcp by embedding itself within HTTP traffic? Many firewalls have to retain an open 2-way-communication with port 80/tcp and 443/tcp, so it can let all standard web traffic pass, which gives an exploit like the Nimda worm the ability to circumvent a firewall's basic defenses. [3] A firewall has the distinct disadvantage of not being

[1] *Evolution of the Firewall Industry.* Cisco Systems, Inc. (Sept. 28, 2002): pg. 2. <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm>.
[2] *Inside the Cisco Centri Firewall.* Cisco Systems, Inc. (Sept 28, 2002): pgs 17-19. <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch5.htm>.
[3] "Attack and Intrusion Prevention: A Practical Approach to Reducing Risk." *NetContinuum, Inc.* (2003): pg 3. <https://www.netcontinuum.com/products/whitePapers/pdf/NC_WhitePaper_AttackPrevention.pdf>.

able to “see” the bad traffic that lies within a packet that is assumed “good” because it is traveling via an accepted port. Even a kernel proxy firewall like the Cisco Centri Firewall, despite its advanced ability to detect the Nimda worm, still has limitations to the type and amount of files and scripts it can recognize.[4] Unfortunately, any exploit still can get through standard ports without raising a red flag for a firewall. At this juncture, there is no way the firewall can filter an exploit that comes through the standard pathways of traffic.

Firewalls were designed to serve as a sufficient border between an organization’s private network and the unregulated, outside world. They were never meant to adequately protect any large enterprise or multiple public servers within an organization.[5] Firewalls essentially serve as a part of defense but not as a whole, lacking the ability to protect specific devices from internal attacks or highly specialized outside attacks, especially attacks that deal with newly released exploits and vulnerabilities.

B. Network-based Intrusion Detection Technology (NIDS)

Intrusion Detection Systems are commonly thought of as the other major component to network security. For some corporations and public organizations, the breadth of users is so heterogeneous and in such a high volume, that *no* firewall could possibly be able to comply with the various demands of its network. For example, it would be very impractical for a large public University with over 65,000 machines to have a firewall at its border that could efficiently handle the amount of network traffic that ultimately results from such a high number of active users, nor could the device easily create an adequate permission/authentication set that would satisfy researchers, doctors, students, professors *and* staff: all people who need varying degrees of access to their data at various levels of integrity. For example, a doctor needs to worry about HIPAA compliance and might need to legitimately participate in a peer-2-peer exchange community for data and research purposes. A student, on the other hand, might be using a peer-2-peer application to download illegal mp3s and share them with other users. One rule set can’t possibly satisfy the needs of both doctor and student. Although this proves to be a definite disadvantage for a firewall, can simply examining the network with custom signatures, such as with an NIDS, help stave the onslaught of malicious exploits as efficiently as a firewall?

Ultimately, detection can never be as efficient as automatic filtering. There will always be a significant time lag between seeing a security problem and solving that problem when a human being is involved and not a machine. NIDS-based methodology is typically called a “reactive” solution, because there is always a

---

[4] *Inside the Cisco Centri Firewall.* Cisco Systems, Inc. (Sept 28, 2002): pg. 16. <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch5.htm>.

[5] Vu, Hung. “Armored Networks Intrusion Prevention Evolution.” *Armored Networks.com* (April 15, 2003): pg 1. <http://www.armorednetworks.com/intrusionprevention.htm>.

noticeable time interval between the intruder's actions, the NIDS reports and the human intervention from the system administrator.[6]

The other liability inherent to an Intrusion Detection System lies in its signature-based strategy. Signatures can't detect any "unknown" security exploits, which inevitably make an organization susceptible to loss from both an integrity-of-data standpoint, as well as a financial one.

However, some organizations simply have no alternative, and so individuals must look at NIDS logs daily, sorting out the prolific assortment of false positives that inevitably are part of the NIDS package and implementing other strategies to make up for an NIDS's deficiencies.

C. NIDS and Firewalls: The "Maginot Line" of In-Depth Defense:

When evaluating both forms of technology, an NIDS and a network firewall implementation both share a common bond and, consequently, a common weakness: they lack true in-depth inspection as stand-alone entities. Over the past five years, security professionals have begun to realize that system security *must* be regarded within the framework of an in-depth defense model. Every barricade is not 100% impenetrable. No matter how high you build the walls to your castle, eventually someone will be able to penetrate the barrier defenses. And, once that breach occurs, it's only a matter of time before your camp will be infiltrated completely by "the enemy".

This concept has been verified throughout history. Take, for example, the infamous French "Maginot line," built during WWI. "France spent 11 years, from 1927 to 1933, constructing a series of fortifications along its eastern frontier from Switzerland to Belgium and dubbed the accomplishment the "Maginot line." The Maginot line was believed by the French to be impregnable and a tribute to their military prowess." [7] France was defeated almost immediately, despite the fact that they had spent most of their time, energy, and resources building their Maginot line. The Germans ended up going around the "line" by invading through Belgium and took Paris with hardly a skirmish. The French had invested their energy into something that was ultimately useless for their needs.

Similarly, no matter how sophisticated a firewall becomes, it is still something that only provides a perimeter defense; a fact that became brutally obvious from the results of a 2002 study from CSI/FBI indicating that 85% of companies with firewalls and access control products still experienced an intrusion within the past year.[8] A firewall is an object that sits at the border of a network, which means,

---

[6] Vu, Hung. "Armored Networks Intrusion Prevention Evolution." *Armored Networks.com* (April 15, 2003): pg 2. <http://www.armorednetworks.com/intrusionprevention.htm>.

[7] Bleiz, Gwen. *The Maginot Line.* (November 10, 2003): <http://www.ifrance.com/letunnel/Maginot/history.html>.

[8] Vu, Hung. "Armored Networks Intrusion Prevention Evolution." *Armored*

inevitably, that with enough malignant traffic attempting to intrude, it will only be a matter of time before something gets through and propagates within a secure network. Thus, there is always a way to "step around" a network's Maginot line.

In response to this timeless problem, network professionals eventually adopted an in-depth defense model to protect a system's confidentiality, integrity and availability by incorporating multiple levels of defense. In order to accomplish a multi-tiered protection system, there is a need for both client-based and network-based applications to protect systems from both external *and* internal attacks. A network-based kernel proxy firewall, despite having intelligent filtering capabilities on an application level, still can't provide protection against internal attacks that spread within the network infrastructure. Nor does it have the ability to do "deep" packet inspection. Thus it is still just the outer ring of the defense strategy model. Similarly, an NIDS, despite having very packet-specific filtering rules that are highly customizable, will only show you what's coming in and going out of a network border and it will not actively defend a network against attack or abuse.

In theory, a security professional could set up an NIDS or firewall in every "zone" of a network (zone being each part of a network that has distinct or separate needs), thus having the ability to track (in the case of an NIDS) and block (in the case of a firewall) traffic internally. However, practical considerations, such as labor, time, and money, make this solution more infeasible. How many people are required to constantly monitor over fifty intrusion detection systems? How much money would be required to set up a large number of firewalls? Who would administer those firewalls or those intrusion detection systems? Most security professionals only look at a business's network as a whole: from "above". If you are not actively within each department, touching each machine as it becomes infected with the 'worm du jour', then how can you effectively administer an adequate defense system in each of those microcosms via an NIDS or firewall alone?

D. Is There A Silver Bullet?

When a security professional looks at all the options, the question must eventually arise, is there truly a "silver bullet" to network security? *Is* a fix-all for system security even possible, much less available on a commercial basis? Can network security ever be guaranteed with just one solution, or is in-depth defense a necessity?

Some people argue that the true solution to defense lies within intrusion prevention technology: a security solution that combines the custom packet inspection capabilities of an intrusion detection system with the proactive filtering methods of a firewall. In essence, intrusion prevention technology is like an "intelligent" firewall, having the capability to view packets up to an application level and block very specific traffic based on constantly updated signatures.

Networks.com (April 15, 2003): pg 1. <http://www.armorednetworks.com/intrusionprevention.htm>.

Intrusion Prevention Systems (IPS), on the surface, look like they provide the ultimate answer to the mutable problems of network security. The advantages far outweigh the disadvantages of the technology, but further explanation is needed to truly determine whether it's truly a silver bullet for the security community, or simply just another element of the in-depth strategy model.

Part II. Intrusion Prevention Technology

A. Adding an Army Behind the Barricade

An intrusion prevention system's capabilities represent a culmination of different technologies and provide a way to fill the gaps that firewalls and intrusion detection systems leave in their wake. Essentially, an IPS has the capability to prevent both external and internal attacks from machines running a large variety of applications and operating systems, encompassing a wide range of security needs.

An IPS inspects every layer of packet information that travels on the network except for the physical layer, rather than just the first 4 layers traditionally inspected by a firewall. A six-layer inspection method, commonly called "deep packet" inspection, allows an IPS to run signatures against packets up to an application level. The result is a highly accurate filtering device that, unlike an NIDS, has minimal false positives: a feature that is more suggestive of a firewall. This is an essential improvement over the false positives that usually dominate the content of most daily reports found in standard NIDS logs.

An Intrusion Prevention device is based off of Network Processor technology[9] rather than a traditional microprocessor, so that the device can sit almost invisibly within a network. Network processors process thousands of instructions simultaneously in order to handle a much larger amount of traffic than a microprocessor, which can only process one task at a time. In fact, most Intrusion Prevention Systems attain minimal to unnoticeable latency sitting in-line on a network as they can analyze traffic at up to multi-gigabit speeds. Tipping Point's Unity One systems, for example, have 215 microseconds of average latency.[10] This means that the device lets the network operate at about 100MB/sec. [figure 1.2]. All intrusion prevention systems also use "stateful inspection" to keep latency low. By using stateful inspection, the devices only have to analyze the parts of a session that match an attack signature. Most organizations demand this type of functionality, especially for any device that actually must sit in-line to a network that must perform at high speeds for many users.

---

[9] "The Profound Benefits of Network-Based Intrusion Prevention." *Tipping Point Technologies* (2003): pg 4.

[10] "The Profound Benefits of Network-Based Intrusion Prevention." *Tipping Point Technologies* (2003): pg 9.

Another benefit of intrusion prevention technology lies in its ability to acutely filter peer-to-peer traffic.[11] With the advent of peer-to-peer applications that direct traffic through port 80/tcp, it has become impossible to filter the traffic with a firewall, because the traffic stems from a port that is also used by legitimate traffic. An intrusion prevention system, however, has the unique capability to filter the specific peer-to-peer packets that come through the system. With the increasing digital copyright concerns that pervade the marketplace, this is an essential asset to avoiding the legal complications, potential financial loss, and the potential exposure of critical data that threatens any organization. Additionally, the filter can eradicate the bandwidth "hogging" that most peer-to-peer applications cause on a network.

Intrusion Prevention technology also provides a very large hidden cost benefit to an organization implementing it. A white paper distributed by Tipping Point Technologies cites the following example:[12]

"A major University deployed Network-Based Intrusion Prevention to protect over 5000 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."

Organizations can justify using an NIDS, despite its comparatively high cost, because the cost-benefit analysis is so high.

Additionally, many forms of IPS technology ensure "intrinsic high-availability," a feature that ensures the device will become transparent within the network if it should ever fail, by falling back to layer two switching mode. Many IPS devices also have redundant hot-swappable power supplies to ensure even greater reliability.

As a result of all the benefits of IPS technology, organizations can create something more than just a barricade between itself and the rest of the Internet. Intrusion Prevention Systems essentially create "security zones" within a private network. The theory is that a compromise of a system can only go "so far" within a network before being prevented by an IPS that is strategically set between network segments.

---

[11] "The Profound Benefits of Network-Based Intrusion Prevention." *Tipping Point Technologies* (2003): pg 4.

[12] "The Profound Benefits of Network-Based Intrusion Prevention." *Tipping Point Technologies* (2003): pg 6.

A perfect example of this arose within my own network security office at the University of North Carolina at Chapel Hill. I was testing one of Tipping Point's UnityOne systems, placing it between one of the larger departments and the rest of the campus community. Coincidentally, the demo unit was placed in-line to the network just days before the Blaster worm hit computers worldwide. The University was affected like every other large organization at the time, except in the department that was protected by the Tipping Point Intrusion Prevention System. The "security zone" that was established by the device kept that department at a zero infection rate, while the rest of the campus all experienced various degrees of infection, including the ones protected by a firewall. The evidence clearly suggested that the cost benefit of the device could be enormous, given the right circumstances: circumstances that are becoming the norm, as exploits seem to only increase with time.

B. The downside of IPS technology.

Initially, intrusion prevention seemed to be the ultimate solution, but, as the product has become more prolific in the marketplace, studies and evaluations have slowly revealed the weaknesses behind the technology.

The biggest flaw intrinsic to Intrusion Prevention lies in its reliability on frequent updates to the signatures that must be applied to the operating systems. Although this weakness cannot be circumvented, due to the fact that exploits and vulnerabilities are constantly emerging, it does create a necessity to actively manage the device. The distribution company must regularly and reliably create signatures as soon as vulnerabilities are discovered, and administrators must apply those updates as soon as they receive them, or create custom signatures as soon as they see vulnerabilities or exploits appear on their networks. Like most anti-virus software, there is a two-fold responsibility model put into place. If Symantec, for example, didn't recognize a new worm on day zero of infection, then administrators of the anti-virus software are prevented from doing anything proactive to their environment to stop the proliferation of the worm in their network. Administrators rely on the ability of the company to give them frequent access to the information they need to stay one step ahead of the next exploit.

In addition, administrators must operate on a relatively intensive learning curve at the onset of using an IPS. A fairly significant amount of time and resources must be dedicated initially to learn what constitutes malicious traffic within your own network. Signatures must be judged individually for their effect on the network and administrators must determine whether they wish to use a signature to block that traffic, notify them of the traffic, or even ignore the traffic. This can be a long and arduous process, depending on the variability of the network involved. For networks that span various hardware and software types, a lot of work must be done determining why an alert is generated and how it will affect traffic before a decision can be made about handling the traffic in a specific manner.

Within my own security experiences with the Tipping Point UnityOne systems, I noticed that the units did an excellent job of blocking what matched the attack signatures, but they did experience an initial problem with the mail servers. The IPS sitting in-line with the mail server recognized the SMTP server's SYN requests as a match to an attack signature, and it blocked all the SYN ACKs as a result. As the SMTP server wasn't getting acknowledgments, the SYN requests remained half-open, resulting in a SYN-flood denial-of-service attack.

The negative impact of this event was not very large or long-term. The SMTP server had noticeably slower delivery time for a while, but the problem was resolved quickly, once it was recognized that the IPS was the root of the problem. However, the event did make my group much more cognizant of how the IPS was going to function within my work environment, and how cautious my coworkers and I were going to have to be when implementing this new technology on a broader scale within the University network.

My group's experiences with Intrusion Prevention Technology echoes a lot of the same thing seen through beta testing and comparison testing in the overall marketplace. According to a comparison review conducted by Security Pipeline Magazine on network intrusion prevention systems, the main problem they encountered was not with the effectiveness of the signatures, but with the "odd false positives that cropped up when we installed the products on our live network."[13]

For example, during their experiments with McAfee's IntruShield 4000, Security Pipeline magazine had problems with it recognizing the STARTTLS command that appeared because they use SSL to authenticate to their mail server instead of SMTP.[14] The STARTTLS command, when ignored, made the IPS block the traffic because it looked like malicious binary data instead of traditional SMTP commands. To repair this problem, Security Pipeline created a rule to detect the STARTTLS command. Just as in my scenario, although the workaround was very easy to implement, the problem lay in figuring out why the error was occurring in the first place. Once the point of failure was isolated, the fix was almost immediate.[15]

Like any new technology, there are some inconsistencies and unforeseen problems that appear only upon widespread use of the product. For Tipping Point Technologies, my University has been instrumental in helping them understand

---

[13] Fratto, Mike. "Comparison Review: Network Intrusion Prevention Systems." *Network Computing's Security Pipeline* (September 4, 2003): pg. 3 <http://www.securitypipeline.com/story/showArticle.jhtml?articleID=15000841>.

[14] Fratto, Mike. "Comparison Review: Network Intrusion Prevention Systems." *Network Computing's Security Pipeline* (September 4, 2003): pg. 4 <http://www.securitypipeline.com/story/showArticle.jhtml?articleID=15000841>.

[15] Fratto, Mike. "Comparison Review: Network Intrusion Prevention Systems." *Network Computing's Security Pipeline* (September 4, 2003): pg. 4 <http://www.securitypipeline.com/story/showArticle.jhtml?articleID=15000841>.

the limits and capabilities of their product. Every time they come out with an upgrade or enhancement to their custom operating system or their actual hardware, my team and I cautiously apply it to different segments of the network to see how it's going to react with the environment. The vast majority of the time, the outcome of these upgrades does not adversely affect the network. However, even after using the technology for over six months, my coworkers and I still encounter some unpredictable problems and setbacks. To Tipping Point's credit, their technicians will always immediately evaluate how their product must be altered or upgraded to eliminate future points of error. Tipping Point's due diligence and immediate response time to our problems allows those issues to remain one-time incidents, rather than habitual ones.

This type of setup creates a very productive environment of dual exchange between the vendor and the client. My coworkers and I constantly provide feedback to them and, in return, they provide my group with constant improvements, upgrades, and suggestions. Although it can be frustrating to be a part of something so new and unpredictable, my group feels that we are pivotal in the development of a new technology and perhaps a new trend in network security. As such, I feel it is my responsibility as a network security analyst to participate and play in such a role, learning and adapting to something that could become a major element in network security.

There is also a huge cost involved that can be considered a detriment when evaluating intrusion prevention technology as a whole. Network-based intrusion detection software, if it is not obtained from an open source, is still usually an efficient, inexpensive way for an organization on a limited budget to keep up a secure network. Firewalls have various price tags, but the range of price options makes the technology relatively affordable for most organizations. However, intrusion prevention systems come with a very high cost. Many small to mid-size companies cannot afford a device that costs over $50,000 per unit. It would be hard to justify the high price tag that comes with it, especially when most organizations have already invested a lot of time and money into other forms of network security. Essentially, an organization must choose either hiring a full-time employee to increase the productivity of an organization, or buying a machine to decrease the man hours necessary for production. In addition, most organizations would have to buy three or four of these devices to effectively segregate their network into manageable security zones. For many companies, that sort of budget is infeasible.

Part III. Conclusions

Intrusion prevention technology is best summed up by the words of Greg Shipley, a security consultant working for Chicago-based company, Neohapsis:

"Although there's nothing wrong with a tactical solution that adds a layer to your defenses, let's call a spade, a spade: This isn't revolutionary technology: it's evolutionary, and its mutation is far from over."[16]

After reviewing both the positive and negative aspects of intrusion prevention technology, the best conclusion that can be made avoids either extreme. Although intrusion prevention systems are not the only element necessary for network security, they are also not just a dead-end security solution. The idea of intrusion prevention began with the inception of the firewall and these new systems are merely another improvement over firewall technology. They are "intelligent" firewalls, in that their inspection capabilities are stronger, more sophisticated, more effective, and easier to implement. However, despite their advancements, these systems are not foolproof and should not be the sole technology used within an in-depth defense model.

As always, the best practice for security professionals is to use caution when implementing this new technology and to, above all, rely on the hardening of the workstations and servers, as well as user education before relying on a technology to filter the traffic that might hit these devices. Like firewalls, intrusion prevention systems will only serve as a wall of defense. Although this wall is higher and stronger, it can still be penetrated. Intrusion prevention systems create security zones within an organization, but exploits can still proliferate extensively within a zone if an infection occurs internally. This being the case, a server lying within that zone must still be fully updated, patched and hardened for the worst attack scenario.

According to the Gartner report made on Intrusion Prevention technology, their conclusion echoes a similar note of caution:

"Through 2006, enterprises should deploy a combination of both intrusion prevention and intrusion detection to meet security best practices," as the technology is still new and the margin of error is still high enough that there should not be an implicit trust in the technology. [17]

Retaining a high level of auditing functionality within a corporation will allow that organization to see what the IPS is truly doing and will limit how much that organization must rely on a singular technology to keep their network secure. Keeping intrusion detection in place is still very necessary, as IPS technology is still very new and relatively untested in a mixture of environments. At my University, my team still has an NIDS in place, mirroring all the traffic coming in at the border, despite the fact that my team members and I have placed intrusion prevention systems in front of various zones of the network. The NIDS is still pivotal in detecting malicious traffic that the IPS isn't blocking, because of its modest filtering settings. Once this device sits in-line with the network for a

---

[16] Shipley, Greg. "Security Watch: Don't Get Bitten by NIPS Hype." *Network Computing* (June 13, 2003): pg 1. <http://www.nwc.com/1411/1411colshipley.html>.

[17] Pescatore, John. "Enterprise Security Moves Towards Intrusion Prevention." *CSO Analyst Reports* (September 25, 2003): pg. 5. <http://www.csoonline.com/analyst/report1771.html>.

longer amount of time, my team and I will begin to gain confidence in the device and we will be able to increase the filtering to its full potential. As long as the IPS needs fine-tuning, however, my team and I feel that an NIDS must be set up in the background to audit all the traffic that won't be automatically blocked by the IPS units.

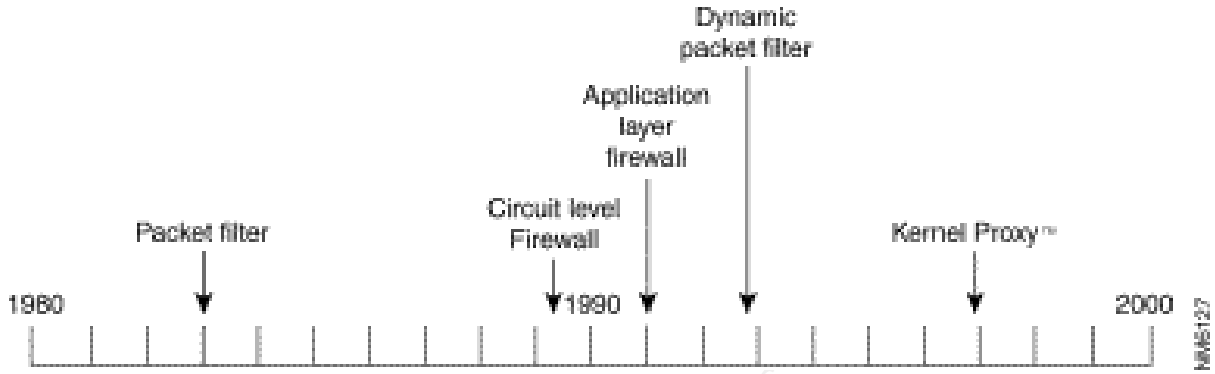
Tim McCormick, vice president of marketing at Internet Security Systems Inc. in Atlanta advocates the same theory:

"We built a $240 million business by inventing the IDS. But the underlying message about convergence is right on. You need all the components. It's not whether IDS is better than a firewall. You need them all."[18]

Intrusion Prevention, then, is not a silver bullet, but a technology that will aid the entire network security community in developing an overall defense strategy. It is an element to a whole, which will, it can be assured, continue to develop over time and evolve into something used by security professionals everywhere.

[18] Fisher, Dennis. "IDS: What Lies Ahead?" *eWeek: Enterprise News and Reviews* (June 11, 2003): pg. 2. <http://www.eweek.com/article2/0,4149,1124829,00.asp>.

FIGURE 1.1 Time Line of Firewall Architectures



Source: *Evolution of the Firewall Industry.* Cisco Systems, Inc. 28 Sept. 2002 <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm>.

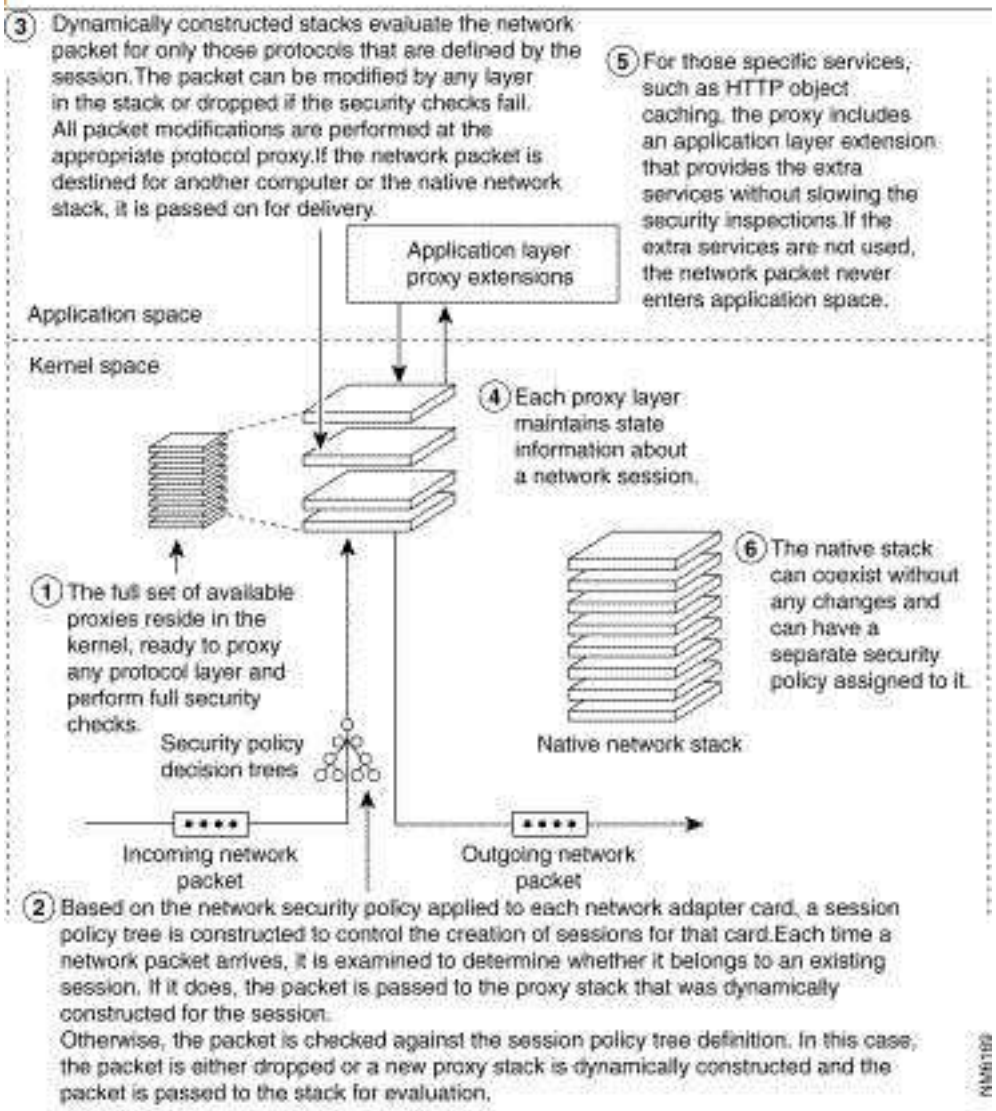
Figure 1.2

How Latency Affects Data Speeds

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.

Source:
"The Profound Benefits of Network-Based Intrusion Prevention." Tipping Point Technologies (2003): pg 9.

Figure 1.3: Kernel Proxy Firewall Architecture



Source:

Evolution of the Firewall Industry. Cisco Systems, Inc. 28 Sept. 2002 <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm>.

List of References

1. Bleiz, Gwen. *The Maginot Line. (*November 10, 2003): <http://www.ifrance.com/letunnel/Maginot/history.html>.

2. Fisher, Dennis. "IDS: What Lies Ahead?" *eWeek: Enterprise News and Reviews* (June 11, 2003): 2 pgs. <http://www.eweek.com/article2/0,4149,1124829,00.asp>.

3. Fratto, Mike. "Comparison Review: Network Intrusion Prevention Systems." *Network Computing's Security Pipeline* (September 4, 2003): 8 pgs. <http://www.securitypipeline.com/story/showArticle.jhtml?articleID=15000841>.

4. Fratto, Mike. "Network-Based Intrusion-Prevention System (NIPS)." *Network Computing (*June 2, 2003): 12 pgs. <http://www.nwc.com/1417/1417p1.html>.

5. Ohlhorst, Frank J. "Network Associates Detects Intrusions." *CRN.com* (Oct 3, 2003): 13 pars. <http://crn.channelsupersearch.com/news/crn/44861.asp>.

6. Pescatore, John. "Enterprise Security Moves Towards Intrusion Prevention." *CSO Analyst Reports* (September 25, 2003): <http://www.csoonline.com/analyst/report1771.html>.

7. Shipley, Greg. "Security Watch: Don't Get Bitten by NIPS Hype." *Network Computing* (June 13, 2003): 4 pgs. <http://www.nwc.com/1411/1411colshipley.html>.

8. Vu, Hung. "Armored Networks Intrusion Prevention Evolution." *Armored Networks.com* (April 15, 2003): <http://www.armorednetworks.com/intrusionprevention.htm>.

9. "Attack and Intrusion Prevention: A Practical Approach to Reducing Risk." *NetContinuum, Inc.* (2003): 13 pgs. <https://www.netcontinuum.com/products/whitePapers/pdf/NC_WhitePaper_AttackPrevention.pdf>.

10. *Evolution of the Firewall Industry.* Cisco Systems, Inc. 28 Sept. 2002 <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm>.

11. *Inside the Cisco Centri Firewall.* Cisco Systems, Inc. 28 Sept. 2002 <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch5.htm>.

12. *Overview of the Cisco Centri Firewall Product.* Cisco Systems, Inc. 28 Sept. 2002 <http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch1.htm>.

13. *Network Associates McAfee IntruShield Wins Industry's First Comparative Network Intrusion Prevention System Test.* Network Associates Inc. 4 September 2003 <http://www.networkassociates.com/us/about/press/sniffer_technologies/2003/20030904_083302.htm>.

14. "Network Intrusion Prevention" *WebDesk.com: Web News and Product Reviews (*September 23, 2003): 7 pars. <http://www.webdesk.com/network-intrusion-prevention/>.

15. "The Fundamentals of Intrusion Prevention System Testing*." Tipping Point Technologies* (2003): 1-10.

16. "The Profound Benefits of Network-Based Intrusion Prevention." *Tipping Point Technologies* (2003): 1-11.

17. "Tipping Point Technologies, Inc. UnityOne Intrusion Prevention Appliances, Performance Evaluation." *The Tolly Group* (Feb 2003): 1-8.

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event