Intrusion Prevention Systems (IPS): Next Generation Firewalls

A Spire Research Report – March 2004

By Pete Lindstrom, Research Director

Spire Security, LLC
P.O. Box 152
Malvern, PA 19355
www.spiresecurity.com

Executive Summary

Much is being said about "intrusion prevention," but little is being done to acknowledge the potential impact of a solution on the network architecture. With so much attention being paid to the intrusion detection-like characteristics, the need for firewall capabilities is being ignored. In fact, the firewall is a more appropriate model for considerations around the deployment and use of a network intrusion prevention solution.

This white paper discusses the characteristics of both intrusion detection and firewall solutions that compose the evolving intrusion prevention solutions. It identifies the features that are useful and highlights the architectural requirements for any security device that intends to be inline on the network.

Finally, the paper discusses Top Layer's approach to intrusion prevention – a practical approach that evolves firewall capabilities into a deeper content inspection solution.

About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues and requirements. Spire provides clarity and practical security advice based on its "Four Disciplines of Security Management," an operational security model that encompasses identity management, trust management, threat management, and vulnerability management. Spire's objective is to help define and refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper is sponsored by Top Layer Networks. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.

Intrusion Prevention Systems: Next Generation Firewalls

Table of Contents

Introduction

Intrusion prevention is full of promise. The idea is that all attacks against any part of the protected environment will be deflected by intrusion prevention solutions because they are omnipotent; they can take any stream of network packets and make the determination of intent – whether it is an attack or legitimate use – then take appropriate action with complete perfection. The end result is a limited need for intrusion detection or monitoring solutions since everything that represents a threat is blocked. While an admirable goal, it is impossible in practice.

The pipe dream of complete protection, however, does not limit the potential of intrusion prevention - make no mistake, intrusion prevention solutions are a core requirement for any security architecture. **Fundamentally, intrusion prevention solutions are the replacement for firewalls and therefore must act more like a firewall to be successful.** This paper explains why.

Detection vs. Prevention

On the surface, intrusion detection and intrusion prevention solutions appear competitive. After all, they share a long list of similar functions, like packet inspection, stateful analysis, fragment reassembly, TCP segment reassembly, deep packet inspection, protocol validation, and signature matching. But these capabilities take a backseat to the starkly different purposes for which they are deployed. An IPS operates like a security guard at the gate of a private community, allowing and denying access based on credentials and some predefined ruleset, or policy. An IDS works like a patrol car within the community, monitoring activities and looking for abnormal situations. No matter how strong the security at the gate is, the patrols continue to operate in a system that provides its own checks and balances.

Intrusion Detection

The purpose of intrusion detection is to provide monitoring, auditing, forensics, and reporting of network activity. It operates on the packets that are allowed through an access control device. Because of reliability constraints, internal threats, and a healthy dose of skepticism, intrusion prevention must allow some "gray area" attacks through to protect against false positives. IDS solutions, on the other hand, are loaded with intelligence, using many different techniques to identify potential attacks, intrusions, exploits, and abuses. An IDS has the luxury of being out-of-band and can therefore perform its operations without affecting the computing & networking architectures.

The passive nature of IDS is what provides the strength to conduct intelligent analysis of the packet stream. That positions IDS well to identify:

- Known attacks via signatures and rules.
- Variations in traffic volume and direction using complex rules and statistical analysis.

- Communication traffic pattern variations using flow analysis.
- Anomalistic activity detection using baseline deviation analysis.
- Suspicious activity detection using heuristics, flow analysis, statistical techniques, and anomaly detection.

Some attacks are just plain hard to detect with any degree of certainty, and most can only be detected by methods that are non-deterministic in nature. That is, they are not suitable for a policy-driven blocking decision.

Intrusion Prevention

As mentioned earlier, intrusion prevention solutions are intended to provide protection for assets, resources, data, and networks. The primary expectation is that they will reduce the threat of attack by eliminating the harmful and/or malicious network traffic while continuing to allow legitimate activity to continue. The goal is a perfect system – no false positives that reduce end user productivity and no false negatives that create undue risk within the environment. Perhaps a more crucial role is the need to be reliable; to perform in the expected manner under any conditions. In order to accomplish this goal, IPS solutions must be deterministic in nature.

Deterministic capabilities imbue the confidence required for a "hard" decision. This means that intrusion prevention solutions are ideally positioned to deal with:

- Undesired applications and active Trojan horse attacks against private networks and applications, by using deterministic rules and access control lists.
- Attack packets like those from LAND and WinNuke by using high-speed packet filters.
- Protocol abuse and evasive actions – network protocol manipulations like Fragroute and TCP overlap exploits – by using intelligent reassembly.
- Denial of service (DOS/DDOS) attacks such as SYN and ICMP floods by using threshold-based filtering algorithms
- Application abuse and protocol manipulations – known and unknown attacks against HTTP, FTP, DNS, SMTP etc. – by using application protocol rules and signatures.
- Application overload or abuse attacks by using threshold-based resource consumption limits.

All of these attacks and the vulnerable state that allows them to happen are well-documented. In addition, the aberrations in communications protocols from network through application layer have no place in any sort of legitimate traffic, making the faults self-selective in a deterministic context.

The End Result

The difference between IDS and IPS ends up being determinism. That is, IDS can (and should) use non-deterministic methods to divine any sort of threat, or potential threat, from existing and historical traffic. This includes performing statistical analysis of traffic volume, traffic patterns, and anomalous activities. It is not for the

faint of heart, nor should it be – it is for individuals who truly want to "know" what is happening on their networks.

IPS, on the other hand, must be deterministic – correct – in all of its decisions in order to perform its function of scrubbing traffic. An IPS device is not supposed to take chances or react with some technical version of "gut instinct." It is supposed to work all of the time, and make access control decisions on the network. Firewalls provided the first deterministic approach to access control on the network, providing basic IPS capability. IPS devices add next-generation capability to these firewalls – still operating inline and providing the type of deterministic comfort required of an inline device that is making access control decisions.

Architecture Matters

So far, the focus of this paper has been on intelligence and purpose. There is a more basic difference between IDS and IPS – architecture. To a large extent, the success of IDS has been possible because it was passive. Security professionals could deploy them without fear that it would break the network. Moving inline changes that.

Fundamentally, any network security device that is going to operate inline must be reliable. Reliability is driven by constant operations and suitability to task – it must perform the functions for which it is designed. Ultimately, an IPS solution must consistently block traffic that is malicious or inappropriate while allowing all appropriate traffic to pass by unfettered. This means that an IPS solution must have the following qualities:

- High availability – no security device has the luxury of crashing due to system overload, it must be built to withstand the toughest network environment.
- High performance – devices in the line of fire must be able to analyze every packet without any noticeable impact on traffic. Performance is driven by high throughput and low network latency.
- Manageability and scalability – ultimately, deploying devices throughout the network drives the need to effectively manage them without worrying about their ability to support the traffic on the wire.

These architectural requirements, when coupled with the deterministic techniques discussed earlier, highlight the true calling of an IPS solution: to be the next generation firewall. This tracks closely with the firewall's need for architectural strength while adding the more intelligent deterministic capabilities associated with deep packet inspection.

Deterministic Intrusion Prevention

The clarification of purpose for intrusion prevention provides the center of gravity necessary to piece together the fit in a security architecture. Deterministic characteristics focus on the behavior and attributes of packets and transactions and understand when activity is inappropriate or malicious. It does not require advanced knowledge of specific exploits because it works backwards from design models, like

protocol RFCs, reference implementations, and individual application environment characteristics to known ways to abuse these communications. Then, it sets bounds around what is allowed in a network environment based on this knowledge.

The benefits are clear:

- Proactive protection from the network security infrastructure.
- Operational efficiencies due to reduced need to react to event logs for protection.
- Increased coverage against packet attacks and zero-day attacks.

Deterministic intrusion prevention *is* the next generation firewall with deep packet inspection. It is not a silver bullet, but it will clearly become a staple at the perimeter and deeper in the network for "Defense in Depth."

Top Layer

The Top Layer IPS 5500 approaches intrusion prevention from a network architecture perspective. It builds on Top Layer's core competencies in network appliances to create a "deep packet inspection" intrusion prevention solution, with key features in four primary areas:

Architecture

The IPS 5500 contains several dedicated hardware processing units to handle the demands of deterministic IPS. For example, one ASIC-based network processor is dedicated to reassembling IP fragments and addressing common network evasion techniques. At layers 2-4, it adds an FPGA (field programmable gate array) with a built-in stateful inspection firewall to conduct all the core firewall capabilities. In addition, it uses a second FPGA subsystem to implement streaming stateful parsing and matching for deep packet inspection and detection of protocol anomalies and unknown attacks.

Protection

Top Layer provides protection "up the stack" and across the enterprise. It provides protection that ranges from basic stateful-inspection firewall capabilities to denial-of-service (DOS/DDOS) and protocol anomaly prevention. The IPS 5500 adds value deployed either on the perimeter or in front of critical assets.

Performance

The key to any inline security device is its ability to handle high-speed traffic without slowing it down (latency) or dropping packets. In third party tests, Top Layer has consistently demonstrated its strength in the performance arena.

Reliability

Top Layer's IPS 5500 was designed for reliability. It contains bypass ports for seamless network insertion and failsafe connectivity, redundant and hot-swappable

components for failover requirements and cluster configurations for high availability.

Spire Viewpoint

The buzz bandwagon is a crowded one in the security space. Intrusion prevention can mean many things to many different people. It is important to understand what type of intrusion prevention device is a good solution. While IDS is most often compared to IPS, firewalls are the closest relative, since architecture trumps intelligence (and rock beats scissors) every time.

While the architecture provides the strength of IPS, it also highlights a different kind of "strength" for IDS – it's passive nature. As long as there are packets on the network, there will be a need for intrusion detection. IDS is intended to monitor all traffic that is allowed into the network. It operates as a part of a system of checks and balances that ensure the proper operation of the network.

Ultimately, the decision to deploy IPS devices comes when a firewall is being upgraded or there is a desire for additional protection with defense in depth deployments. Because of this, IPS devices should operate like a firewall, complete with deterministic ruleset, and an architecture that will integrate with the rest of the network environment.

Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at www.spiresecurity.com.

This white paper is sponsored by Top Layer Networks. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.