Making Everything Easier!™

Intrusion Prevention Systems FOR DUMMIES®

Learn to:

- **Understand common network threats**
- **Select the right intrusion prevention system for your company**
- **Figure out how an intrusion prevention system can fit into your organization's network**

Brought to you by

SOURCEfire®

Steve Piper, CISSP, SFCP

About Sourcefire

Sourcefire, Inc. (Nasdaq: FIRE), a world leader in intelligent cybersecurity solutions, is transforming the way Global 2000 organizations and government agencies manage and minimize network security risks. A Leader in Gartner's 2010 Network IPS Magic Quadrant and recognized by NSS Labs in 2009 and 2010 for offering best overall IPS detection, Sourcefire has received more than 60 awards and accolades. In 2011, Sourcefire was listed #15 on Forbes' annual list of America's top 25 fastest-growing technology companies — ranked highest among all IT security vendors in the United States.

For more information, visit www.sourcefire.com.

Sample Sourcefire Awards & Recognitions

Intrusion Prevention Systems FOR DUMMIES®

by Steve Piper, CISSP, SFCP

Wiley Publishing, Inc.

Intrusion Prevention Systems For Dummies®
Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774

www.wiley.com

Published by Wiley Publishing, Inc., Indianapolis, Indiana

ISBN: 978-1-118-00474-6

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact info@dummies.biz. For details on licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Development Editor: Peter Gregory

Project Editor: Jennifer Bingham

Editorial Manager: Rev Mengle

Business Development Representative: Sue Blessing

Custom Publishing Project Specialist: Michael Sullivan

Composition Services

Project Coordinator: Kristie Rees

Layout and Graphics: Carrie A. Cesavice, Samantha K. Cherolis, Melanee Habig

Proofreader: Debbye Butler

Special Help from Sourcefire: Steve Kane, Richard Park, Doug Hurd, Mike Guiterman, Kimberly Connor, Chris Chon, Marc Solomon

---

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Director, Acquisitions

Mary C. Corder, Editorial Director

Publishing and Editorial for Consumer Dummies

Diane Graves Steele, Vice President and Publisher, Consumer Dummies

Composition Services

Debbie Stailey, Director of Composition Services

Business Development

Lisa Coleman, Director, New Market and Brand Development

Table of Contents

Introduction

With this book, you get the "must have" knowledge that you need to understand how intrusion prevention systems (IPS) and emerging Next-Generation IPS (NGIPS) solutions improve the security in an organization's networks. I help you understand why they're needed and how to determine which features are most important for your organization. I also show you how to lower the total cost of ownership of an intrusion prevention system, so that it will pay for itself.

How This Book Is Organized

This book is organized so that you don't have to read it cover-to-cover, front to back. You can skip around and read just the chapters that are of interest.

- In **Chapter 1, Understanding IPS,** I explain how intrusion prevention systems work, and the ways they detect network-based attacks. I compare passive versus inline systems, and explain how they differ from firewalls.
- **Chapter 2, IPS Attack Coverage,** explains the various types of threats that IPSs are designed to detect and deflect. I explain some of the nastier threats such as zero-day and advanced persistent threats.
- In **Chapter 3, Modern IPS Features,** I explain many of the features and functions found in Next-Generation IPSs, including dashboards, reporting, management, forensics, and user identification. I also discuss nifty features such as SSL inspection, network behavior analysis, and data loss prevention.
- **Chapter 4, IPS, Virtualization, and Cloud Computing,** includes in-depth discussions of virtualization and cloud computing technologies, and the role that IPSs play to protect these new types of environments.

- In **Chapter 5, IPS and Regulatory Compliance,** I explain standards and regulations such as PCI, HIPAA, GLBA, SAS70, and FISMA, and explain how IPSs help an organization be compliant.
- **Chapter 6, Selecting the Right IPS,** is all about helping you get your IPS shopping list organized so that you can be sure to get the IPS that is right for your organization.
- In **Chapter 7, Ten Ways to Lower TCO,** I explain ten proven ways to improve your investment in an IPS.

Icons Used in This Book

This book uses the following icons to indicate special content.

You won't want to forget the information in these paragraphs.

These paragraphs provide practical advice that will help you craft a better strategy, whether you're setting up your software or planning to purchase.

Look out! When you see this icon, it's time to pay attention — you'll find important cautionary information you won't want to miss.

Chapter 1

Understanding IPS

In This Chapter

- Understanding today's intrusion prevention systems
- Comparing and contrasting IPSs and firewalls
- Looking at passive versus inline systems
- Exploring detection techniques
- Understanding how IPS fits into the big picture

Intrusion prevention systems (IPSs) are a critical part of an organization's overall network and systems protection strategy and a critical part of a *defense-in-depth* architecture. Without them, you're fighting the bad guys with one arm tied behind your back.

In this chapter, I look at the function of intrusion prevention systems and how they fit into an organization's network.

Defining Intrusion Prevention Systems

Intrusion prevention systems, or IPSs, are devices or programs that are used to detect signs of intrusions into networks or systems and take action. That action consists of generating alarms and/or actively blocking intrusions.

IPSs usually take the form of purpose-built hardware devices, software agents that run on servers, or software programs that run within virtualized environments.

Understanding the difference between IPSs and firewalls

Firewalls and IPSs are both essential tools for protecting an enterprise from intrusions. Both are needed, primarily because they're each designed to look at different things:

- A firewall is designed to block all network traffic except that which is explicitly allowed.
- An intrusion prevention system is designed to permit everything except that which is explicitly disallowed.
- A firewall is designed to permit (or block) network packets based on their source, destination, and port number, regardless of the contents of each packet's *payload* (the contents of the message).
- An intrusion prevention system is designed to permit (or block) network packets based on the packet's payload.

Maybe an analogy will help here. Imagine a business building that has a lobby with a security guard, who permits personnel to enter based on who they are. The guard permits the mail carrier and the package courier to bring letters and packages into the building, but the guard doesn't examine the contents of the letters or packages. In the mailroom, a mail clerk opens all the letters and packages and examines them.

In this analogy, the guard is a firewall, permitting personnel to come and go, but doesn't examine what they're bringing in or taking out. The mailroom clerk is an IPS, because the clerk is examining the contents of each letter and package.

In the 1990s, virtually all network-based attacks could be blocked with the combination of firewalls and anti-virus software. That isn't the case today: Most new attacks are targeted directly at web applications. These attacks are impossible to defend with firewalls and anti-virus software alone. Without an IPS, attacks have a significantly greater chance to succeed.

Passive Detection versus Inline Prevention

The two modes of operation used by intrusion detection and prevention systems are *passive detection* and *inline prevention*. These modes are described in Table 1-1.

Table 1-1 Comparison of Passive IDS and Inline IPS

Passive Detection	*Inline Prevention*
Connected to a "tap" or switch span port	Directly inline
Receives a "copy" of traffic	Traffic actually flows through system
Creates alerts	Creates alerts
Can't block attacks	Can block attacks
Detection errors can result in false alarms	Detection errors can result in service disruption
Device malfunctions will cause a cessation of alarms	Device malfunctions can result in service disruption

Not your father's IDS

IDSs in the early 1990s were notorious for generating hordes of false positives. Network engineers would have to spend hours upon hours to "tune out" the false positives. This was a laborious, manual task that gave early IDSs a bad reputation. This was mostly the case because early IDSs lacked intelligence and an easy way to root out false positives. Today's IPSs are far superior in both respects, to the point that false positives are now an anomaly and no longer a major headache.

Although IPSs can operate in a pure passive detection mode, you should understand that there are no longer any strictly passive intrusion detection systems (IDSs) offered today; instead, today's systems are IPSs that can be run in either passive detection (alerting) mode or in inline prevention (blocking) mode, or both.

Network versus Host IPS

Intrusion prevention systems come in two basic flavors: network-based and host-based. The differences and similarities between these types are described here.

Network-based IPS

Network-based intrusion prevention systems typically take the form of a rack-mounted appliance or system that is attached to a data network. The network is configured to send a copy of all the traffic in the network through the IPS so that the IPS may examine it to identify possible intrusions.

IPS alphabet soup

There are four main types of IPSs, each with its own FLA (four-letter acronym). They are:

- **HIDS (host-based intrusion detection system).** This is an intrusion detection system that is installed on a host and is designed to detect attacks against the host system.
- **HIPS (host-based intrusion prevention system).** This is an intrusion prevention system that is installed on a host and is designed to block attacks against the host system.
- **NIDS (network-based intrusion detection system).** This is an IDSs monitoring a network to detect attacks.
- **NIPS (network-based intrusion prevention system).** You guessed it — this is an IPS monitoring a network to block attacks.

Common Detection Methodologies

Intrusion prevention systems use different methods to detect security incidents. The makers of IPSs have learned that no one method is effective for detecting and stopping most kinds of incidents; instead, they have settled on a number of well-known ways to accomplish this.

Rule-based detection

IPSs can detect incidents by comparing observations against a list of previously defined incidents and known vulnerabilities. This type of detection is quite effective at detecting both known and unknown threats. Some examples of rules (also known as *signatures*) are:

- Attacks targeting vulnerabilities in operating systems and applications
- Botnets used to perform targeted Denial of Service (DoS) attacks or steal personally identifiable information (PII)
- Unusually large ping packets, which may be an indication of a ping of death attack

Because new types of attacks against information systems are continually being developed, IPSs need to regularly update their rules. Rules are developed by the makers of IPSs, and in some cases a "community" of rule writers, and are distributed to running IPSs via the Internet.

Savvy intruders know how signature-based detection works, and in response they have developed a number of ways of evading detection, usually by introducing subtle variants in their attacks. For this reason, leading IPS makers usually publish vulnerability-based rules (instead of exploit-based signatures) to detect all possible variants of an attack. They may also offer anomaly-based detection techniques, discussed in the next section.

If you're familiar with the basic workings of anti-virus software, particularly in regard to its use of signatures and signature-based detection, then you'll have little trouble understanding how an IPS works. In this regard, they are quite similar. But unlike anti-virus solutions, leading IPS vendors rely on vulnerability-based rules (rather than exploit-based signatures) to detect any possible exploit variation targeting an operating system- or application-level vulnerability, thus affording users with the ultimate protection against zero-day threats.

Anomaly-based detection

IPSs can detect incidents by comparing traffic patterns that the IPS considers "normal" with new traffic patterns, and deciding whether new traffic patterns fall within acceptable patterns or not. A distinct advantage of anomaly-based detection is the capability to detect incidents that may not be triggered by a standard IPS rule or signature.

Stateful protocol analysis

IPSs can detect incidents by observing individual network connections, for instance, and making alerting or blocking decisions based on what's considered normal for various types of activities.

For example, an IPS may learn the sequence of events when the user of a web application logs in, and after logging in issues commands to the application to perform work. The IPS may consider a user issuing commands without logging in to be an event that should be blocked, because this may be a sign of an intruder who is attempting to perform unauthorized transactions.

False Positives

In the context of intrusion prevention, a *false positive* is an IPS declaring good traffic as bad, resulting in either a false alarm (if the IPS is in passive detection mode) or service disruption (if the IPS is in inline prevention mode). A false positive is usually caused by an ineffective IPS rule or signature.

A false positive should not be confused with a "real" attack that is ineffective against the operating system or application it is targeting. For example, if Conficker attacks a Linux host, and an intrusion event is triggered, it is technically not a "false positive" but more of a "not applicable" since Conficker only affects Windows operating systems. I go into this in more detail in Chapter 3.

First-generation IDSs were legendary for creating massive quantities of alerts, overwhelming administrators who spent hours trying to tune out the noise. Learning from those painful times, IPS vendors have made their systems much better through intelligent learn modes, easier administration, and highly tuned rule sets.

False Negatives

The opposite problem is that of a *false negative,* where an IPS fails to recognize an intrusion or other security event. This can occur if the IPS doesn't have up-to-date rules, or if the IPS vendor hasn't released a rule for a new type of attack or vulnerability.

When an IPS is placed in inline blocking mode, false negatives are generally far more damaging to an organization than a false positive. A false negative permits bad traffic to enter the network, potentially leading to compromised systems and possibly stolen or lost data. A false positive blocks good traffic from entering the network, potentially leading to lost business or productivity.

Vulnerability-Based Rules versus Exploit-Based Signatures

One of the main problems with a signature-based (for example, exploit-based) approach is the inability to detect zero-day attacks.

Although some zero-day attacks are exploiting a new vulnerability, many target vulnerabilities that are already known.

Given this, it makes more sense for an IPS to have its rules based on actual vulnerabilities rather than signatures based on known attacks.

Let me explain with another analogy. Consider a padlock that may have a design weakness that makes it vulnerable to picking. It would be better for an IPS to be familiar with the lock's vulnerability, so that it will be able to detect any kind of an attack upon it. However, if the IPS were instead configured to detect only known lock-picking methods (attacks), then any new methods for picking the lock would go undetected.

Open versus Closed Architectures

Open and closed architectures refer to the way that IPS providers design their products and control the publication of those designs. In an *open* architecture, important parts of a product's design will be openly published, permitting not only inspection but also integration with other companies' products.

Closed architectures, on the other hand, aren't open for inspection. This makes it difficult or impossible for security administrators to validate the architecture of the IPS, to inspect its rules and create custom rules, and to integrate with common third-party platforms (for example, SIEMs, vulnerability management systems, network forensics, and so on).

Selecting an IPS with an open architecture offers numerous advantages, including increased levels of security, greater flexibility for defending proprietary systems, and superior integration and intelligence-sharing with existing IT infrastructure.

With more than 300,000 registered users, open source Snort is a popular choice for intrusion detection and prevention, boasting a huge quality assurance (QA) team of both commercial and open source users. A Snort-based IPS features an open architecture, making it easy to inspect the quality of IPS rules and create custom rules for proprietary systems. More than 100 vendors have incorporated Snort into their network security devices.

Understanding IPS Components and Network Architectures

To understand how an IPS protects an enterprise, it helps to look at the components of an enterprise-class IPS. Figure 1-1 shows a typical organization's Internet-network boundary along with IPS components.

IPS sensor

An IPS sensor is typically a purpose-built hardware appliance that is connected to the network. The sensor may be connected in one of three ways:

- **Inline.** Here, the IPS is placed inline behind a firewall, router, or switch so that all network traffic actually flows through it. This configuration supports both IPS (blocking) and IDS (alerting) modes.
- **Network tap.** A tap is a hardware device that provides a way to access the data flowing across a network. A *bypass tap* is typically used for inline IPS configurations for IPS devices that lack a fail-open capability or for organizations that may wish to disconnect their inline IPS from the network regularly for maintenance or reconfiguration. A *regeneration tap* is used for passive IDS configurations typically when the span ports on monitored switch devices are already consumed.
- **Switch span port.** This is a port on a network switch where a copy of all traffic that flows through the switch can be monitored. This supports a passive IDS configuration.

Interface sets on an inline IPS should be configurable to *fail open,* meaning that all network traffic should continue to flow through the IPS sensor in the event of a hardware or software failure in the IPS. This ensures high availability of the network.

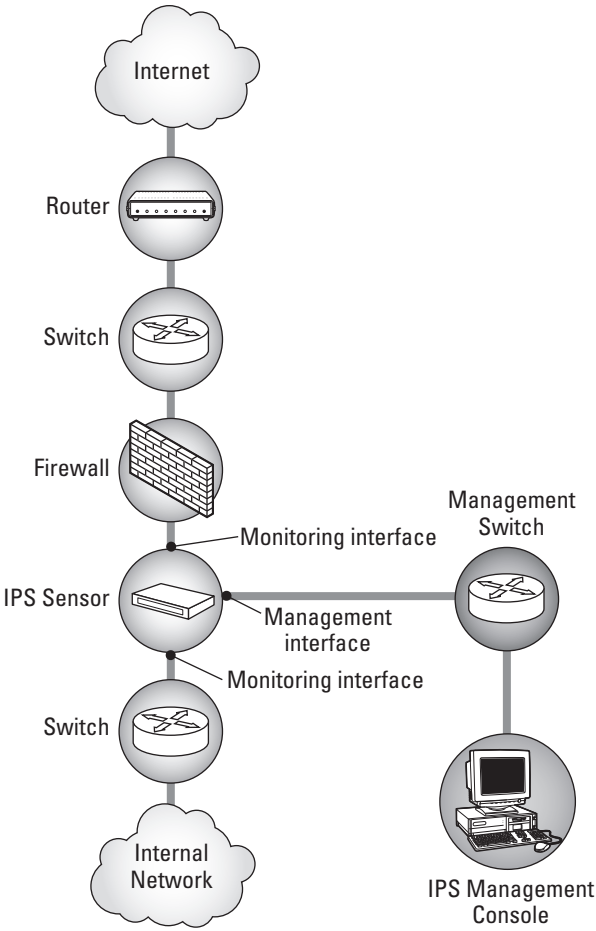

Figure 1-1: IPS components in an enterprise network.

Enterprises will typically have many IPS sensors, each located in a different part of the network. Some of the common places where an IPS sensor might be placed are:

- **Perimeter or DMZ.** Here, the IPS sensor is detecting traffic flowing from the Internet to public-facing web servers (and other hosts) placed in the Demilitarized Zone (DMZ) or hosts located near the perimeter behind the firewall.

Often, an IPS placed at the perimeter or DMZ will operate in inline IPS blocking mode to fend off potential attacks.

- **Core or data center network.** More organizations are extending protection of their perimeter IPS by installing IPS sensors (typically placed in passive IDS mode) in the core or data center. This provides an additional layer of defense and helps to detect attacks hand-carried into the office on mobile computing devices.
- **Extranets.** Larger organizations with extranet connections to partner or supplier networks may place an inline IPS device in front of associated routers to both defend against potential incoming attacks and to ensure that local malware doesn't spread to partner networks.
- **Wireless access points.** Contractors and guests commonly connect to the network through wireless access points. As these devices are typically uncontrolled by IT, many organizations place IPS sensors behind wireless access points to monitor for potential unwanted traffic.
- **Virtualization platforms.** Although virtualization provides significant cost-saving benefits, it also introduces new risks and uncertainties. A physical IPS placed in front of a virtualization network, or a virtual IPS installed on each virtualization host, can help defend against hidden attacks originating from within or targeting virtual machines.
- **Critical network segments.** These may be networks containing critical systems (such as servers containing financial or medical data, for instance), where intrusions would be especially serious.

The Payment Card Industry Data Security Standard (PCI DSS) mandates the use of IPS technology on networks that process credit card transactions. Learn more about the role of an IPS for PCI DSS compliance in Chapter 5.

IPS sensors placed at the perimeter and strategic points inside the network serve as the organization's eyes and ears for defending against today's most sophisticated threats.

IPS management console

The IPS management console provides centralized command and control over all IPS sensors. Typical features of an IPS management console include:

- Security event aggregation
- Centralized detection policy management
- Downloading, importing, and applying IPS rule updates
- User interfaces for viewing and filtering security events
- Reports, alerts, and dashboards
- Health monitoring, to monitor health and performance of IPS sensors and the IPS management console itself

More modern IPS management consoles provide additional functionality beyond legacy IPS platforms, including:

- Network forensics (for example, view full packet payload)
- Event correlation and impact assessment
- User identification and tracking
- Application monitoring
- Flow (for example, NetFlow, proprietary flow) storage and analysis
- Advanced detection policy management (for example, policy layering)
- APIs to enable streaming of events to external platforms, remediation to network infrastructure devices, and importing of external network and vulnerability intelligence
- Granular administrative access permissions
- "Manager of managers" hierarchy, enabling one IPS management console to manage multiple subordinate IPS management consoles

The IPS management console is typically offered on dedicated hardware appliances, but may sometimes be offered as Windows-based software (requiring server-class hardware) or as a VMware, Xen, or other virtual machine.

Chapter 2

IPS Attack Coverage

In This Chapter

- Understanding common network threats
- Determining what constitutes a zero-day attack
- Coming to terms with advanced persistent threats

Intrusion prevention systems (IPSs) are designed to block many different types of attacks. It is easier to understand IPSs if you better understand the types of things they're designed to detect and prevent.

If this were a book about law enforcement, this chapter would be about different types of criminals and the crimes they commit. Understanding the types of attacks you're trying to prevent helps you gain perspective on the strategic role of a network IPS.

In this chapter, I look at the types of attacks that intrusion prevention systems are designed to prevent.

Worms, Trojans, and Buffer Overflows

This section is kind of a grab bag of attack types.

Worms

A *worm* is a program that is designed to self-propagate from one computer to the next. Typical worms are designed to discover nearby computers with specific features, particularly

features with specific flaws that permit the worm to successfully attack the next computer and install itself there. Then the worm begins to scan for other nearby potential victims, and the cycle repeats itself until the worm can find no new victim computers to invade.

The primary characteristics of worms are:

- Self propagation; they travel automatically with no human intervention required.
- Exploits a vulnerability to install itself.
- Scans the network for additional potential victims.

Worms cause harm in three different ways:

- **Network traffic.** Worms have a tendency to flood networks with their probes for new victims, and for the traffic caused by their propagation.
- **System resources.** Worms consume resources on the victim system through their propagation operations. Worms can even consume resources on adequately protected systems if a worm's attack is persistent.
- **Harmful payload.** Individual worms may be programmed to do more than just scoot around on the Internet. In addition, they may be designed to hunt for specific data on infected systems, implant other malware, or intentionally harm data.

Trojan horses

A *Trojan horse* is another type of malware. Like a worm, a Trojan is designed to propagate itself from system to system. But unlike a worm, a Trojan requires human intervention to keep it moving.

A Trojan horse is so-named because it is disguised as something benign. For example, a Trojan may be embedded inside a computer program purported to be a game, screen saver, or other program. But once activated, a Trojan will do whatever harmful things that it was designed to do.

When activated, a Trojan may scan nearby networks for neighboring systems that are potential victims. Or, the Trojan may scan the user's system to look for valuable data, or install other malware that it is carrying.

Buffer overflows

A *buffer overflow* is a specific type of attack against a system, where the attack is designed to confuse the system into executing the attacker's instructions.

A buffer overflow attack works like this. An attacking program establishes a communications session with a specific component on the target system, and sends a specially crafted message to the target system. The message deliberately sends too much data into the target system's input buffer. In a program that is vulnerable to a buffer overflow attack, the excess data will overwrite program instructions in the vulnerable program, and eventually the program will execute those instructions (thinking that it is executing its original instructions). Those new instructions usually contain code to open the target system and permit a partial or complete takeover of the target system.

Sound complicated? You bet it is!

A buffer overflow attack isn't easy to develop. It takes detailed knowledge of the target system's internal architecture (both software and hardware), as well as detailed knowledge of the program or service being attacked. That said, hackers who develop buffer overflow exploits often build a "kit" that makes it easy for others to exploit the same vulnerability.

Worms, Trojans, viruses, and other types of malware often use buffer overflows as a way of gaining a foothold in a new victim system.

Buffer overflows account for a significant portion of the attacks against systems on the Internet.

Spyware, Phishing, and Botnets

Here is another grab bag of attacks on systems and people.

Spyware

Spyware is a term ascribed to a wide range of techniques used to covertly obtain information from computers. Spyware most often takes on the form of computer code that is installed on a user's computer without his or her knowledge or consent, gathers specific information, and sends that information to a central source. Spyware may also alter the behavior of the victim's computer.

The activities performed by spyware include:

- Tracking sites visited with a browser
- Recording keystrokes and mouse clicks
- Changing browser settings (for instance, changing home page, default search engine, and so on)

Unlike other types of malware such as viruses and Trojans, spyware doesn't usually contain code for making copies of itself onto other computers.

Phishing

A pun on the word *fishing,* a *phishing attack* is an attack on computer users in an attempt to con them into performing an action that is intended to cause them harm. That harm may take the form of financial fraud or the installation of malware or spyware on their computer, for instance.

A typical phishing scam works like this:

- **The bait.** The scammer sends out large quantities of genuine-looking e-mail messages to intended victims in an effort to entice them to open an attachment or click a URL.
- **The hook.** Although most people ignore or don't receive (because of anti-spam) the message, a few believe it is legitimate, or they're just curious. They open the attachment or click on the link.

- **The harm.** The attachment installs malware or spyware on the victim's computer, which may steal information, install a key logger, or perform some other harmful action. If the user clicks a URL, the website may trick the user into believing she is logging into a legitimate website (such as online banking). If she types in her user ID and password, the scam artist will use these credentials to log in later and steal money from the victim. Also, the website may attempt to infect the user's computer with malware. The victim's computer may also be made a part of a botnet, which is discussed later in this section.

Phishing scams account for a significant portion of computer security incidents and malware infections by preying on a user's gullibility.

Botnets

A *botnet* is a collection of victim computers that have been commandeered into a *bot army,* a powerful computing resource awaiting instructions from its owner. Creators of botnets are typically financially motivated.

Here is how a botnet works. An individual or group will write a small software program — a bot — that will enable the computer it's running on to be remotely controlled. This bot will be packaged into a worm, malware program, or loaded on a malicious website, at which time a campaign of some sort (say, a phishing scam) will ensue to get the bot installed on as many computers as possible.

The owner of these bots, usually known as a *bot herder,* has a centralized "command and control" program that can be used to control all the computers that are running his bots. This control program can then be used to perform work on behalf of the bot herder, such as:

- **Spam.** A bot army can be used to send millions of spam messages — which themselves may contain malware intended to grow the bot army.
- **Denial of service attacks.** The bot army can be used to remotely attack a computer or network of the bot herder's choosing. Denial of service attacks are discussed later in this chapter.

Botnets range in size from hundreds to millions of computers. According to the BBC, as many as a quarter of all personal computers may be members of one or more botnets.

SYN Floods and Denial of Service (DoS) Attacks

The next grab bag of attacks includes two common network-based attacks.

SYN floods

A *SYN flood* is an attack on a target system, specifically an attack in a key design attribute of the TCP/IP networking protocol.

In a SYN flood, the attacker sends thousands of SYN packets to a target system. A *SYN packet* is ordinarily a message sent from another computer that wants to establish a network connection with the target. Upon receiving the SYN, the target system will reply with a SYN/ACK, at which point the conversation will begin.

An important fact to note is that the target computer will allocate resources (mainly, memory) in anticipation of the new connection. But in a SYN flood, the attacker sends thousands of SYNs and ignores all the SYN/ACKs. The purpose of this is to flood the target system until it is incapable of communicating on any legitimate channels.

A SYN flood is a special type of a denial of service attack. These attacks are discussed in the next section.

Denial of service

A *denial of service (DoS) attack* is an attack on a target system where the objective of the attack is to partially or completely incapacitate the target system. The purpose of a DoS attack is to render the target system unusable for legitimate purposes.

Encryption and other detection evasion

In the malware economy, the developers of malware consider their products successful if they're able to evade detection. Early attempts at this involved the release of several "variants" that were constructed differently from one another. However, this has proven ineffective in comparison to encryption.

Encryption is a popular way of hiding from signature-based detection systems. This is particularly effective when each computer's copy of malware is encrypted with a different decryption key, making every copy of the malware unique. This can make detection by signature-based systems very difficult. Anomaly-based systems should have no trouble with encrypted malware, because the basic attack pattern is likely unchanged.

The reason that an attacker would carry out a DoS attack could include revenge, jealousy, ideology, or economics.

Committing a DoS attack is akin to blocking the entrances to a business so that its customers are unable to patronize it.

There are two basic types of DoS attacks:

- **Flooding.** The most common form of DoS attack is one where the attacker sends such a high volume of messages to a target system that it either malfunctions or is otherwise unavailable for legitimate purposes.
- **Malfunction.** The other common form of DoS attack is one where a specially crafted message is sent to the target system; the message causes the target system to malfunction or crash.

Another type of DoS attack is known as the Distributed Denial of Service (DDoS) attack. In a DDoS attack, the attacker causes many different systems to flood a target system simultaneously. Such an attack can be nearly impossible to block if there are hundreds or thousands of different sources.

Botnets are often used to commit DDoS attacks.

Zero-Day Attacks

A *zero-day attack* is a brand new attack on a previously unknown vulnerability, or a new type of an attack on an existing vulnerability.

The term *zero day* comes from the number of days of warning between the time when the vulnerability is announced and when it is exploited. In other words, these are vulnerabilities for which no patches are available.

Zero-day attacks are significant because signature-based (exploit-based) IPS devices are generally defenseless against them. However, IPSs that also use anomaly-based detection and leverage vulnerability-based rules (as opposed to exploit-based signatures) can protect effectively against zero-day attacks.

Advanced Persistent Threats (APT)

There is presently more hype and misinformation about advanced persistent threats (APTs) than practically everything else in this book combined. In truth, there is no silver bullet or single security device for defending against APTs. But a network IPS is a strategic component of a defense-in-depth strategy that can help you get ahead in the game.

What is APT

To understand what APT is and what it is not, start with a short definition and then delve into the details.

An advanced persistent threat is information warfare, conducted by sophisticated adversaries who are determined to control information systems and gather intelligence on persons, organizations, and governments.

Does this definition scare you? Good! It should, because the actors who are responsible for these threats are financially motivated, patient professionals with research and development resources at their disposal. They're not looking for instant gratification, but instead are willing to go "low and slow" to patiently, systematically infiltrate the systems used by individuals and organizations.

So enough about the actors. What about the actual threats?

Advanced persistent threats are malicious, and they certainly fall into the class of malware. However, for highly sophisticated threats, you won't find signatures of this malware in anti-virus products or intrusion detection systems, because these threats are custom made for their specific targets.

Advanced persistent threats do consist of attacks that are detectable. However, these attacks may be subtle and take place over a very long period of time. Traditional defenses such as anti-virus, IPS, and firewalls may not see anything at all. The actors behind an advanced persistent threat don't want to set off any alarms.

IPS's role in APT

Resisting advanced persistent threats requires advanced detection systems. An IPS with an effective vulnerability-centric detection system is helpful. APT actors often try to target vulnerabilities in operating systems and applications, but often do so with custom-built tools instead of "off the shelf" malware. An IPS that knows how to spot novel, zero-day attacks against known vulnerabilities will help.

Another effective tool to combat APTs is network behavior analysis (NBA). NBA, which is incorporated into better IPSs, helps to detect changes in the composition of network traffic, which may be a sign that spies have infiltrated the network.

Network versus host-based detection

Arguably, APTs most often target systems that store, transmit, or process data. So it would make sense that a host-based detection and prevention would be best, right? Well, not really.

The problem with host-based detection is that the attacker, once he has been able to compromise a system, will be able to notice the presence of HIDS or HIPS on the system. This is akin to a burglar who spots a video surveillance camera after he has broken into a home or office. Not that the NIDS, NIPS, or video camera will necessarily scare off the intruder, but it may force the intruder to change his tactics in order to make his actions less noticeable.

In order to detect attacks on systems, network-based IDSs and IPSs offer a key advantage over host-based solutions. The main reason for this is that the intruder will not be able to observe any of the detection/prevention capabilities. Done right, NIDS and NIPS are virtually undetectable. This gives the organization an advantage, because intruders, who can't know (for certain) that they're being watched, may be a little more lax in their tactics, and as a result they may be a little easier to detect.

Other advantages to network-based IPSs are:

- Network-based IPSs/IDSs don't consume system resources
- Passive implementations of IPSs/IDSs don't interrupt network traffic flow

Although I hope that I have convinced you that network-based IDSs/IPSs is the way to go, I don't want you to throw out the baby with the bathwater. Some systems-based security tools should still be used, and may detect APTs. These tools include:

- **Anti-virus and anti-spyware.** You need this anyway to stop the cheap stuff, and these may also slow down APT attacks.
- **Firewalls.** Packet filtering at the system level may still be a good idea, particularly if outbound connections are also limited to those services that are truly required.

- **File integrity monitoring (FIM).** Another good idea for detecting unauthorized changes to operating system and application files. FIM also helps to detect other types of threats, including systems engineers who make changes to systems without going through proper procedures, such as change management.

These other security controls comprise a *defense-in-depth* strategy necessary to combat APT.

APTs, while more difficult to detect than ordinary malware, can often be detected, provided the organization is willing to invest in the tools required to repel them.

Chapter 3

Modern IPS Features

In This Chapter

- Understanding Next-Generation IPS
- Automating key IPS functions
- Removing network blind spots with SSL inspection
- Integrating third-party products into an IPS

Intrusion Prevention Systems have come a long way since the introduction of open source Snort in 1998. Although a "typical" IPS contains everything you need to bring the box online and start blocking attacks, a new breed of IPS technology has raised the bar in terms of what organizations should expect from their IPS investment.

In this chapter, I contrast the key features of a typical IPS against those of a Next-Generation IPS (NGIPS), with emphasis on capabilities related to security, automation, and total cost of ownership (TCO). I also discuss strategies for SSL (Secure Sockets Layer) inspection and integration with existing IT security products and infrastructure.

Typical IPS versus Next-Generation IPS

Figure 3-1 compares the key attributes of a typical IPS and a Next-Generation IPS.

In the remainder of this chapter, I describe common features found in virtually all IPS devices, but then delve deeper into the sophisticated capabilities found in today's Next-Generation IPS solutions.

Key IPS Attributes	Typical IPS	Next-Gen IPS
Inline IPS & Passive IDS Modes	✓	✓
Default Detection Policy	✓	✓
Reports, Alerts & Dashboards	✓	✓
Custom Rules		✓
Vulnerability-Based Protection		✓
Automated Impact Assessment		✓
Automated Tuning		✓
User Identity Tracking		✓
Application Monitoring		✓
Network Behavior Analysis		✓
Virtual IPS & Management Console		✓

Figure 3-1: Features of typical versus Next-Generation IPS.

Common functions

Virtually all of today's IPS devices share the following common functions:

- **Inline IPS and passive IDS modes.** However, when an IPS device is placed inline, be sure it supports fail-open ports. Some IPS providers offer fail-open ports on only a portion of their models.
- **Default detection policy.** Every IPS vendor should provide a detection policy comprised of the most common IPS rules to help get you started. But an organization should never just rely on a default policy because it never adapts to your dynamically changing network environment. Don't let IPS vendors fool you about this. "Tuning" is required to select the IPS rules that are most relevant for your organization. In IPS, one size does *not* fit all.
- **Reports, alerts, and dashboards.** Most IPS providers offer a selection of reports, alerts, and dashboards usually present in the management console. Reporting

should be flexible, alerts should be offered through e-mail, syslog, and SNMP, and dashboards should be customizable based on the user's role in the organization. The managers who paid for IPS want to see their reports and dashboards, to know that the IPS is really working and providing business value.

Advanced protection

Most of today's IPS devices are *black boxes* that offer little visibility into the protection being offered. However, a Next-Generation IPS — especially one based on an open architecture — is different:

- **Visibility.** Vendors with IPS offerings based on closed architectures require you to "trust" that they have the best protection for your needs, as you have no visibility into how the detection engine works or whether their rules (or signatures) are designed to defend vulnerabilities or simply detect known threats. In contrast, a NGIPS features an open architecture with full visibility into the detection engine and rules, yielding higher quality products, increased effectiveness, and peace of mind.
- **Custom rules.** Most typical IPS vendors will tell you that you can create custom rules, but few provide the means to do it effectively. It's best to select an IPS vendor that makes it easy to create custom IPS rules through training and an easy-to-use wizard interface.
- **Vulnerability-based protection.** Most IPS providers offer exploit-based signatures that detect a single variant of malware. A Next-Generation IPS puts in the extra effort to construct IPS rules to detect *any possible variant* of an exploit that targets an operating system or application vulnerability. This approach provides the best security and offers the greatest zero-day protection. It's better to be able to detect any possible exploit of a faulty lock than it is to have to detect every possible skeleton key.

The general trend in IT products is the capability to see inside the product to view and manage detailed configuration and operation. Make sure you select an IPS that gives you the capability to view and manage detection rules.

Lower TCO through IPS automation

Whether you work for a small, medium, or large organization, there never seem to be enough IT security resources to go around. IT security must work smarter — not harder — to defend today's dynamic network. A Next-Generation IPS makes it easier to do more with less:

- **Automated impact assessment.** It's not uncommon for an IPS device to generate hundreds of security events on a daily basis. When you take into account that a traditional enterprise may have a dozen IPS devices or more, sifting through thousands of security events each day is virtually impossible and can effectively render an IPS useless, because it will be ignored. A Next-Generation IPS, on the other hand, correlates threats against endpoint intelligence to reduce the quantity of "actionable" security events by 95 percent or more.
- **Automated tuning.** Every network is different. Customize your IPS detection policy with rules that are relevant for your organization. If the detection policy is too small, the IPS will offer inadequate protection. And if it's too big, it can overburden the IPS, causing decreased network throughput and increased latency. A Next-Generation IPS can passively profile your network and automatically recommend rules to enable and disable at a user-defined interval (for instance, weekly or monthly).
- **User identity tracking.** What good is an IP address for an end-user device related to a security or compliance event if you don't know who is being attacked or who is violating a company IT policy? Instead of sifting through DHCP and Active Directory logs to manually cross-reference users with IP addresses, a Next-Generation IPS can place usernames and user identity at your fingertips. The time it takes to tie a user to a security event can be shrunk from one hour to under a second.

Reducing TCO through IPS automation

According to a SANS Institute white paper entitled "Calculating TCO on Intrusion Prevention Technology," a multi-national credit reporting organization with approximately 20,000 nodes and 7,500 employees saved more than $230,000 per year in annual TCO reductions through automated impact assessment, automated tuning, and user identification. By leveraging a Next-Generation IPS solution, organizations can recover their initial IPS investments in a matter of months by automating key IPS administrative tasks.

Protection beyond a typical IPS

Today's Next-Generation IPS offers network security capabilities beyond just intrusion detection and prevention:

- **Application monitoring.** Most enterprises have documented acceptable use policies (AUPs) depicting operating systems and applications approved and/or restricted from use, but few organizations have the means to monitor and enforce them. A Next-Generation IPS helps IT to "reduce the surface area of attack" by alerting IT to the unauthorized user of operating systems, applications, and devices.
- **Network Behavior Analysis.** Not all attacks come through the perimeter. Many are hand-carried on mobile computing devices right through the front door, thus bypassing a perimeter IPS. Network Behavior Analysis (NBA) technologies baseline "normal" network traffic (using NetFlow or proprietary flow technology) and detect anomalies, such as the spread of malware.
- **Virtual IPS & management console.** A typical appliance-based IPS can't inspect traffic between one virtual machine (VM) and another on a VMware or Xen server. A Next-Generation IPS provider solves this challenge by offering virtual IPS sensors and management consoles to protect virtualization environments from within and to defend cloud computing infrastructures.

SSL inspection

Every network security device is blind to SSL-encrypted traffic, including a network IPS. This is because an SSL session is encrypted end-to-end, and the IPS in between sees only encrypted data. As the use of SSL grows within an organization — oftentimes comprising one-quarter to one-third of traffic — the potential of an SSL-encrypted attack rises.

To mitigate this risk, a Next-Generation IPS should be complemented by a dedicated SSL inspection appliance — whether from the same vendor or another third party. The SSL inspection device should decrypt SSL traffic, pass it to the IPS for inspection, and then re-encrypt the (clean) traffic before placing it back onto the wire — all with minimal added latency. When placed inline, the SSL inspection appliance should also feature fail-open ports.

Beware of IPS providers that only offer on-board SSL decryption. Enabling SSL decryption on an IPS can adversely affect the performance (for example, throughput) of the box by up to 80 percent. In most instances, organizations will want to offload the SSL decryption process to a stand-alone appliance, which not only decrypts traffic for the IPS, but all network security devices placed behind it. But regardless of whether SSL is decrypted by the IPS or a stand-alone appliance, ensure the SSL decryption capability also re-encrypts the original (clean) traffic before placing it back onto the wire to maintain confidentiality of the data and to maintain compliance with PCI or other regulatory standards.

Third-party integration

A best-of-breed security device should integrate with other devices on your network to share intelligence, coordinate responses, and lower total cost of ownership. The following are common examples of how a Next-Generation IPS can integrate with popular third-party systems:

- **Security Information and Event Managers (SIEMs).** Stream security, compliance, and health events to your SIEM of choice (for example, Arcsight, Q1 Labs) for centralized security monitoring.
- **Vulnerability Management (VM) platforms.** Import vulnerability intelligence from popular VM platforms (for example, Qualys, Rapid7) for security event impact assessment and greater network visibility.
- **Network infrastructure devices.** Remediate to routers, switches, and NAC devices from leading network infrastructure providers (for example, Cisco, Juniper, Check Point) to quarantine hosts related to security and compliance events.
- **Network forensics.** Launch packet-level forensics queries directly from the IPS management console to leading network forensics devices (for example, NetWitness, Solera), saving both time and effort.

After you integrate your IPS into your SEIM and other platforms, you'll be humming right along at a level of security your organization has not experienced before.

Chapter 4

IPS, Virtualization, and Cloud Computing

In This Chapter

- Considering the benefits and risks of virtualization
- Securing virtualization
- Virtualizing security
- Securing the cloud

Virtualization and cloud computing are revolutionizing information technology by facilitating a more efficient use of computing resources.

Virtualization is the technology that enables many separately running operating system instances to occupy a single computer. Each *virtual machine (VM)* instance runs as though it were occupying its own dedicated server. This can enable an organization to more easily deploy and manage servers.

Cloud computing is the term encompassing many technologies that enable an organization to enjoy a dynamically expanding and contracting computing environment. Organizations can build their own clouds, or buy services offered by external cloud computing providers.

In this chapter, I discuss virtualization and cloud computing, and the relationship that each has with intrusion prevention systems.

Benefits and Risks of Virtualization

Virtualization is the technology that permits an organization to run many separate instances of operating systems on a single server. This permits an organization to greatly enhance the efficiency of its server hardware, by grouping many separately running operating systems onto a single server. Figure 4-1 illustrates virtualization.

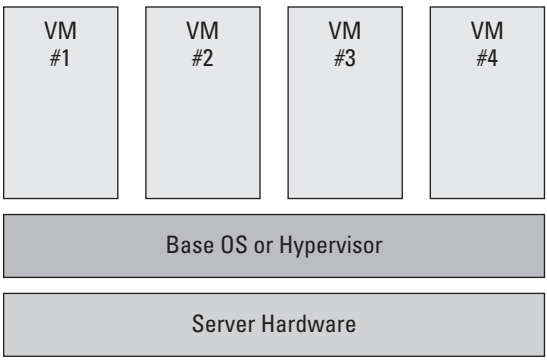

Figure 4-1: Virtual servers.

Before virtualization, an organization whose environment required six servers had to purchase six separate hardware servers. With virtualization, the organization can purchase one server and install six virtual machines on that server.

The primary benefit of virtualization is that an organization can implement new virtual machines at will and with very little effort.

The primary risk of virtualization is that an organization can implement new virtual machines at will and with very little effort.

Yes, you read that right: The main benefit is also the main risk. What I'm saying here is that, without proper safeguards, virtualization can introduce risks that can negate the benefits.

The benefits of virtualization include:

- **Agility.** Virtualization allows an organization to respond more quickly to changing needs in its technical environment.
- **Rapid deployment.** With virtualization technology, you can build and deploy a new server in just a few minutes. No more running down to the local computer store for a server and loading an OS.
- **Improved system availability.** Virtualization enables an organization to implement servers that are more consistent with each other. Consistency breeds higher availability, because there are fewer differences between systems, which means systems engineers are less likely to make mistakes that cause unexpected downtime.
- **Energy savings.** Running many virtual servers on just a few physical servers means there are a lot fewer physical servers consuming energy.
- **Space savings.** The amount of space that servers consume is expensive, especially in commercial data centers that literally charge for rack space by the inch.

With these benefits, what's not to love? However, there are also risks related to virtualization, and it's important to understand these risks, so that you won't make the same mistakes that others have made.

- **VM sprawl.** Because virtualization makes it so incredibly easy to deploy a new server, it can sometimes be tempting for an engineer to deploy a server and bypass the management processes that usually accompany the deployment of a new server. The result can be many unauthorized servers that are doing who-knows-what. VMs created outside of management processes may be unmanaged and invite malware infection. For more on the topic, see the section "Controlling VM sprawl," later in the chapter.
- **Vulnerabilities.** One of the neat features of virtualization is the capability to *roll back* to an earlier *snapshot,* which is a fancy way of reverting to an earlier version of the virtual server. Doing so, however, can also result in the

removal of critical security patches that can leave servers vulnerable to attack or malfunction.

- **Lack of separation of duties.** In the physical server world, there is more management and team coordination required to deploy a new server: Someone has to approve the hardware purchase, and network engineers provide support by enabling the connection of a new server to the network. With virtualization, none of this coordination is necessary. A single individual can deploy a server without telling anyone.
- **Blind spots.** In the physical world, it is easier to observe the logical architecture and data flow in an environment, and control security with firewalls and IDSs where needed. With virtualization, however, servers that were once separated by firewalls or IPSs may end up on the same physical server, resulting in the loss of those network controls.

These risks may sound pretty scary — so is virtualization worth it? You bet it is. And IT management, aware of the cost savings realized with virtualization, will insist on it. So it's best to hang on and make your virtual systems secure.

Some IPS providers offer virtual versions that can be incorporated into virtual environments, providing greater visibility and control of VM-to-VM traffic.

There are two approaches to virtualization and security. One is the process of securing virtualization, and the other is virtualizing security. Both are discussed in the next section.

Securing Virtualization

Like any information technology, virtualization needs to be secured. In other words, virtualization needs to be configured and managed in a way that will result in the virtualization environment being free of vulnerabilities that could lead to compromised systems.

There are three main areas where virtualization needs security controls: with the people, processes, and the virtualization technology itself.

Virtualization: People security

What I'm getting at here is the fact that all personnel who design, implement, manage, or operate virtualized environments can do so only when they have the knowledge required to do it properly. Not only do personnel need to understand virtualization technology, but they also need to be familiar with the organization's policies and procedures regarding virtualization.

You can have all the right virtualization technology in place, but if personnel don't understand how to use it (or are unwilling to understand), your virtual environment will not be secure.

Virtualization processes

Like personnel, a virtualized environment will not be very secure unless the right business processes are in place. Some of the processes that I feel are important include:

- **Change management.** Changes to virtual machines, as well as changes to virtualization configuration, should be done under the control of a formal change management process. Just *how formal* this process should be is dependent on the organization's needs. However, under no circumstances should changes be made without *at least* informing all affected parties!
- **Technical standards.** Configuration settings for virtualization, as well as the virtual machines themselves, should be written down. This is not a one-time exercise, but a process of establishing standards and then sticking to them. Sure, things need to change — in that case, you use Change Management to manage change.
- **Audit.** Virtualization settings and virtual machines need to be examined from time to time, to ensure that they're being deployed and operated properly, and that no unauthorized activity is going on.

Securing virtualization technology

Virtualized environments need to be properly designed and configured, so that they will be free of vulnerabilities that may expose them to threats. Virtual environments should be designed and configured according to the following principles:

- **Least-privilege administration.** Each staff member who administers virtualization should have his or her own user ID, and each person should have only the privileges required.
- **Logging.** Administrative activities within the virtualized environment should be logged. This helps to identify who is performing what administrative functions. A documented history of administrative activities makes troubleshooting a lot easier.
- **Disable unneeded components.** Just as disabling unused ports and components on a server is good for security, this same principle applies to virtualization.
- **Backup.** Certainly it should be obvious that all virtual machines in a virtualized environment should be backed up. But what may be less obvious is the need to back up virtualization configurations themselves if they're not contained in an OS being backed up.
- **Placement of IPS sensors.** Just as the placement of IPS sensors is critical in a traditional environment, it's also critical in a virtualized environment. This may necessitate both hardware IPSs as well as virtual IPSs that are installed within virtualized environments. This will help to protect VM-to-VM traffic even within individual hardware platforms.
- **Configuration standards.** Virtualization and virtual machines need to be configured according to a set of documented standards. There are two main benefits to standards. First, when properly circulated, reviewed, and approved, standards should represent a collective agreement on how systems should be configured. Second, standards (when enforced) help systems be more consistent with each other.

Controlling VM sprawl

VM sprawl is a result of the practice of deploying virtual machines without obtaining approval. Because engineers can unilaterally deploy VMs without obtaining approval, some enterprises are liable to experience uncontrolled growth of VMs and the chaos that results. Here I discuss some neat ways that IPSs can be used to control it.

Better IPSs can help to control VM sprawl by detecting a VM by its virtual network card's MAC address. An IPS can be configured to generate an alert whenever it sees a new VM on the network. This can help management to keep an eye on new VMs, so it is important that these alerts not be sent to the individuals who create VMs but to other personnel, in order to prevent engineers from creating VMs on the sly.

Organizations that are zealous about controlling VMs can use their IPSs to prevent new, unauthorized VMs from being able to communicate on the network. This is one important way that segregation of duties can be retained in a virtualized environment.

Virtualizing Security

Virtualization creates several new opportunities, including the capability to implement more than just operating systems in virtual environments. Besides OSs, you can also deploy network switches, firewalls, and IPSs as virtual machines, thus leveraging the cost-saving benefits that virtualization brings.

At first blush, it may appear that cost savings is the only motivator for virtualizing security devices. Sure, virtual versions of security devices may (or may not) cost less than their physical counterparts, but sometimes using a virtualized security device is the right thing to do.

For example, imagine that an Internet-facing application is deployed in a virtualized environment. The application consists of a web server, an application server, and a database server. Regulation requires IPS protecting the web server

and a firewall protecting the database server. All these components can be incorporated into a single physical platform, with the necessary detective and preventive controls in place to protect all these virtual components with as much confidence as though they were physically separate. Configured correctly, these components are every bit as secure as if they were air-gapped.

Virtual IPS solutions can also be deployed to small remote offices (equipped with virtualization hosts) to monitor both physical and virtual hosts for threats, without incurring the expense of physical IPS devices and the human costs to deploy them. Virtual IPS VMs can be *dragged and dropped* to protect virtually (no pun intended) any corner of the network with a few clicks of a mouse, saving both time and money.

Securing the Cloud

Cloud computing is all the rage these days. Whether they're providing cloud services or consuming them, enterprises are flocking to cloud environments faster than prospectors flocked to the Klondike in the 1896 Alaska gold rush.

In order to preserve the context of intrusion prevention systems, stay with the fairly general definition of *cloud computing* as the use of computers and networks as a general-purpose, on-demand, and dynamically scalable computing environment that hosts applications and other computer-based services.

Organizations that wish to move their applications "into the cloud" generally desire to outsource an application's infrastructure (computers and network devices), with the expectation that computing resources will expand and contract based on demand. Growing and managing a dynamic computing infrastructure is expensive and time consuming, and outsourcing this frees the organization to focus on its core competencies.

One of my favorite sayings is, "You can't outsource accountability." This means that, even if you hire an outside organization to perform work, you're still responsible for the outcome. In the context of cloud computing, an organization that outsources its infrastructure (and, possibly, applications and

other services) to the cloud needs to make sure that its systems and data are protected from security threats.

Cloud computing doesn't always mean "run by others." An organization can have its own private cloud.

The controls used to protect cloud-borne applications and data from threats are discussed in the remainder of this chapter. These controls are necessary, whether an organization is building and running its own cloud, or using the services from a cloud services provider.

Firewalls

These access control devices are used to control the communications flowing to and from networks and specific endpoints by blocking unauthorized access as well as many types of intrusion attempts.

Intrusion prevention systems (IPSs)

These systems watch for signs of malfunction, intrusion, and some types of malware attacks. IPSs detect and block the attacks that other controls (such as firewalls) are incapable of.

Strict access controls

A well-designed access controls program is necessary to effectively secure a network, a system, or a cloud environment. Some of the characteristics of an effective access control system include:

- Formal access request process
- Least privilege access
- No shared accounts
- Access logging
- Strong password quality standards
- Periodic access reviews

Logging

Significant events at every layer of the cloud infrastructure need to be logged. Preferably, logging will be centralized for ease of management and the capability to correlate individual separate events and be able to see them as incidents.

Precise time synchronization is a key ingredient for accurate logging. Computers' time-of-day clocks are notoriously inaccurate; use NTP to synchronize all computer and network device clocks to well-known standard time sources.

Change management

Change management is the formal process where all changes in an environment are formally requested, reviewed, scheduled, performed, and documented.

The heart of an effective change management process is a *period change review meeting,* where stakeholders discuss upcoming proposed changes. This helps ensure that changes will have the desired effect, be coordinated with the right parties, and help to reduce unscheduled downtime.

Configuration management

Developing good standards and using tools to ensure consistent configuration helps to make systems more resistant to intrusion and misuse. Configuration management tools can help to automate the settings on each virtual machine, enabling even instantaneous configuration changes across all systems in a virtualized environment.

Chapter 5

IPS and Regulatory Compliance

In This Chapter

- Understanding how IPS is needed for PCI, HIPAA, and other regulations
- Knowing how COBIT supports Sarbanes Oxley, Basel II, and SSAE16
- Seeing why IPS supports most security-related regulations and standards

Security is no longer just a good idea: It's the law.

When organizations put their information and their business processes online and made them available over the Internet, there were scores of large-scale security breaches and thousands of smaller incidents. This resulted in a backlash of laws and regulations designed to force organizations to take at least basic safeguards to protect information stored online.

Regulations and standards regarding information security are still young but beginning to mature. Many consistent themes are emerging that allow an organization to figure out how to be compliant to different laws and regulations.

This chapter discusses the heavyweights of laws and regulations, and how IPSs can help.

Security or compliance?

As various laws and regulations on data security emerged, conflicted with one another, and matured, often there was a question of whether an organization was secure or compliant. What does this mean?

Some of today's laws and standards on data security are very exacting in their demands. They require specific processes and technologies, regardless of the actual risk associated with those processes and technologies. And some of these same laws ignore other measures that organizations need to take.

Organizations that are focusing on compliance often take their eyes off the need for security. One can't be sacrificed for the other. Although compliance is important, security is even more important. Organizations can't rely merely on compliance to be secure, although many do just that.

Organizations still need to perform a periodic risk assessment in order to determine where the risks are. Controls mandated by laws and regulations will take care of many — but not all — of those risks. Organizations need to put additional controls in place to manage risks not covered by regulations.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS, commonly known as just PCI) is a highly detailed and comprehensive standard that is required for every merchant, retailer, and service provider that stores, processes, or transmits credit card data for any purpose. PCI compliance is required by all the major credit card companies, including MasterCard, Visa, American Express, Discover, and JCB.

The credit card brands, working through card issuers and banks, require every organization that handles credit card data to be compliant to the PCI standard. Merchants that process more than six million transactions per year, and service providers that process more than 600,000 transactions per year, are also required to undergo an external audit every year to ensure their compliance. Merchants and service providers are also required to undergo quarterly external security scans.

Several specific PCI standards require the use of IPSs, specifically:

- **1.1 - Configuration standards and acceptable ports/services for business use.** Organizations are required to develop configuration standards for all information systems and devices. These standards must contain a list of ports and services on these systems that are required for those systems to properly run.
- **2.2 - Development and enforcement of configuration policy.** An IPS can be configured to generate alarms or block traffic that violates these standards. Better IPS solutions offer compliance rules and whitelists, enabling customers to monitor and continuously enforce acceptable use policies (AUPs) for use of operating systems, applications, ports, protocols, and services.
- **6.2 - Identify and remediate vulnerabilities.** Organizations are required to have a formal vulnerability management program to proactively identify and remediate vulnerabilities in all layers of infrastructure. Better IPS solutions incorporate passive network intelligence collection to complement active scanning technologies to better defend the network against emerging zero-day threats.
- **11.2 - Quarterly vulnerability scans.** Organizations are required to undergo scans that are carried out by PCI-approved scanning vendors. Leading IPSs augment this by delivering this information to organizations' security specialists in real time. This helps an organization to discover and remediate vulnerabilities prior to the official quarterly scans.
- **12.5.2 - Monitor and analyze events.** Organizations are required to monitor systems for security events. An IPS can perform this monitoring.
- **12.9 - Incident response.** PCI requires organizations to have an organized incident response program and test it at least once per year. An IPS can provide automated alerting and response, as well as provide alerts to personnel who can perform manual analysis and remediation.

Every organization that is required to comply with PCI must have an IPS — there is no way to interpret this requirement in any other way.

PCI, the effective non-law

PCI DSS is a standard that was developed by the consortium of credit card brands. Despite the fact that PCI isn't a law, card brands have been able to effectively enforce compliance to PCI.

The credit card brands enforce PCI through fines, as well as the threat to block the organization's capability to process credit card transactions.

U.S. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA (pronounced *HIP-uh*) is a U.S. federal regulation that, among other things, requires that each organization that stores electronic health records (known as PHI, or protected health information) develop a set of controls to ensure the protection of that information. HIPAA is about security as well as privacy, requiring organizations to restrict access to PHI and also to handle it properly. HIPAA applies to all types of medical practices (hospitals, clinics, and doctors' offices) as well as insurance companies and other organizations that store or process patient medical records.

HIPAA requires organizations to enact several controls, some of which are easier to implement with an IPS. These are:

- **164.306 - General requirements.** Organizations are required to protect PHI against reasonably anticipated risks and threats. These threats include, of course, intrusion, which is detected and blocked by an IPS.
- **164.308 - Administrative safeguards.** Organizations are required to enact policies and procedures to prevent, detect, correct, and contain security violations. An IPS is perfectly suited to protect an organization against network-borne security violations, intrusions, and incidents.

- **164.312 - Technical safeguards.** Organizations are required to implement controls to detect and prevent security threats. An IPS is a part of the total solution for blocking network-based threats, from the Internet as well as from within the organization.
- **164.316 - Documentation requirements.** Organizations are required to implement reasonably appropriate policies and procedures to comply with standards and implementation specifications.

It would be hard to imagine a HIPAA-compliant organization that lacked an intrusion prevention system.

U.S. Federal Information Security Management Act (FISMA)

All agencies of the U.S. government, as well as service providers that process information for the U.S. government, are required to comply with the Federal Information Security Management Act (FISMA). FISMA (pronounced *FIZZ-muh*) requires all agencies to develop, document, and implement agency-wide information security programs. The publication NIST 800-53 ("Recommended Security Controls for Federal Information Systems") describes the control framework for all efforts to comply with FISMA.

Intrusion prevention systems help organizations to comply with several parts of FISMA, including:

- **CA-7 - Continuous Monitoring.** Agencies are required to continuously monitor their networks for security events and intrusion attempts. It's difficult to imagine anything but an IPS for this job.
- **RA-5 - Incident Monitoring.** An IPS helps security response teams to focus on critical events and incidents.
- **RA-3 - Risk Assessment.** Output data from an IPS helps a security team to complete its risk assessment by learning what security events are occurring on an agency's network.

- **RA-5 - Vulnerability Scanning.** Passive monitoring data from a leading IPS solution supplements results from active scans with tools such as Nessus.
- **SI-3 - Intrusion Detection Tools and Techniques.** With detection and automatic remediation, a leading IPS can exceed the NIST 800-53 requirements for intrusion detection tools.
- **CM-1 - Configuration Management Policies and Procedures.** Agencies are required to document their configuration management policies and procedures, including actions to take when an IPS detects intrusions.
- **CM-4 - Monitoring Configuration Changes.** Better IPS solutions can detect changes in a system's baseline configuration through passive observation.

An IPS is one of the necessary ingredients for any government system in scope for FISMA.

U.S. Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley act — also known as Sarbox or SOX — was passed by Congress in 2002 in response to a number of significant accounting scandals in the U.S. The goal of SOX is to ensure the accuracy of financial statements for all U.S. public companies.

SOX requires that organizations have a system of internal business and technology controls that ensure no possibility of tampering with organizations' financial systems.

Unlike other standards and regulations such as PCI, HIPAA, and FISMA, SOX doesn't include a standard set of controls. Many organizations have enacted the Control Objectives for Information and related Technology (COBIT) framework of controls to be compliant with SOX.

An IPS part is an essential of every U.S. public company's infrastructure, in order to be compliant with several COBIT controls, including:

- **DS5.10 - Appropriate controls are in place to prevent unauthorized access via public networks.** An IPS is a key component to prevent unauthorized access of an organization's systems from the Internet.
- **DS5.5 - Monitoring and logging of security activity.** An IPS continuously monitors network-based security activity.
- **DS5.3, 5.4, 5.10 - System infrastructure is properly configured to prevent unauthorized access.** Intruders aren't welcome! An IPS helps to prevent unauthorized access by blocking unwelcome access attempts.
- **DS9.2 - Authorized software only on IT assets.** An IPS can help to detect the presence of unauthorized software on IT systems through the detection of new types of network traffic.

Whether an organization adopts COBIT or another set of controls for SOX compliance, certainly these controls will include those listed here. An IPS is a key component for achieving compliance with these controls.

U.S. Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act, usually known as GLBA, is a U.S. law passed by Congress to require financial services firms to protect sensitive information about their depositors and clients from theft and abuse. GLBA applies to all banks, investment firms, brokerages, and insurance companies doing business in the U.S.

GLBA requires every financial services organization to comply with three major rules: Financial Privacy Rule, having primarily to do with the privacy and handling of sensitive information; the Safeguards Rule, which requires firms to have a written data security plan that describes how they will protect their clients' information; and Pretexting Protection, which requires that firms train their employees to recognize and deflect attempts at *pretexting* — a social engineering attempt to obtain client information.

GLBA is enforced by the FDIC (Federal Deposit Insurance Corporation), FRB (Federal Reserve Board), and the National Credit Union Association (NCUA). The Federal Financial Institutions Examination Council (FFIEC) provides guidance for GLBA audits. IPSs are required to meet the following FFIEC examination guidelines:

- **Information Security Assessment — gathering data on assets and threats to those assets.** Better IPS solutions can enumerate a network using passive sensing technology. Each asset's operating system can be mapped against a database of vulnerabilities to aid impact assessment for associated intrusion events.
- **Security Strategy that includes prevention, detection, and response.** Management is required to establish a formal strategy for protecting client information that includes an IPS that aids in the detection and response to security incidents.
- **Monitor network access for policy violations and anomalous behavior.** An IPS will naturally be a major component in network monitoring.
- **IDS/IPS monitoring of incoming and outgoing traffic.** Can this be any more obvious?
- **Hardening — documented minimum system requirements and disallowing of noncompliant activity.** An IPS contributes to this by detecting exceptions to hardening standards, primarily through the detection of disallowed components and programs.
- **Security monitoring: policy violations, anomalous activity, and security events.** An IPS is the key component in any security monitoring strategy.

It's no surprise that IPSs play a key role in compliance to GLBA by preventing many kinds of security incidents and problems.

Basel II

Basel II is the second of the Basel Accords, an international standards committee on banking laws and regulations. The purpose of Basel II is sound capital management for banks and other depositor institutions.

Like Sarbanes-Oxley, Basel II doesn't prescribe specific controls, but many organizations that are required to comply with Basel II adopt the Control Objectives for Information and related Technology (COBIT) framework of controls.

See the earlier section on Sarbanes-Oxley for information on how IPS supports compliance to COBIT controls.

SSAE16 and SAS70

U.S. publicly traded companies that outsource any of their financial services to other organizations have a potential problem: Their external auditors who are measuring companies' compliance to Sarbanes-Oxley aren't able to directly audit the activities performed by the outsourcer.

Those auditors could require that they audit the service provider, but that would add considerable cost to each audit. And, the service provider would have a lot of auditors snooping around for their customers. A service provider with a lot of customers wouldn't be able to tolerate this many audits of its operations.

The answer: The outsourcing service provider undertakes an SSAE16 (formerly known as SAS70) audit. The audit report can be sent to its customers' auditors, who can then complete their audit on their U.S. public companies' financial operations.

Like Sarbanes-Oxley itself, there is no prescribed set of SSAE16 controls. Instead, most adopt COBIT controls to manage their services. The service provider's SSAE16 auditors can then audit the service provider's COBIT controls and then write an audit opinion that can be sent back to its U.S. public company customers.

Take a look at the Sarbanes-Oxley section earlier in this chapter for a discussion on how IPSs support compliance with COBIT.

Chapter 6

Selecting the Right IPS

In This Chapter

- Developing IPS selection criteria
- Understanding the unique requirements needed from enterprise and SMB organizations
- Unraveling industry specific requirements
- Exploring independent test labs

So here you are in the selection criteria section. You're probably thinking about getting an IPS for your organization now, or at least thinking about thinking about it. Or maybe you want to see what criteria other organizations use when they're ready to buy.

Regardless, it is important to develop objective criteria for any IT system, and then compare various products against your criteria. This may sound tedious, but would you rather buy based on emotion? Well, it may feel good at the moment, but later on you might not be happy with what you purchased at the time.

Common IPS Selection Criteria

In this chapter, I discuss selection criteria, starting with general requirements in this section, and moving to specialized requirements by company size and industry sector later on.

Here are the primary characteristics that organizations need to consider when shopping for an IPS:

- **Detection.** How an IPS detects unwanted traffic. This can be signature-based, anomaly-based, or both. Consider both false positives as well as false negatives. Is the rule base visible so that you can examine them or add more?
- **Scalability.** Rather than just consider what is needed today, what modes of change, growth, or future regulations or standards may require additional sensors, additional bandwidth, new technologies (such as virtualization), or different types of sensors (physical versus virtual)?
- **Performance.** Make a purchasing decision with the long-term in mind. If any type of growth is anticipated, then you should select a security platform that will grow with you without having to replace hardware sooner than you're ready to.
- **Compliance.** Understand how your IPS investment may satisfy any relevant governmental and/or industry compliance regulations that affect your organization. In the case of PCI DSS, for example, some IPS solutions may satisfy more requirements than others.
- **Vision.** You will need to consider whether you want to purchase an IPS from a market leader, or from a company that just does what everyone else does. As for me, choose a leader who is consistently respected for vision and execution, knowing that provider will develop new kinds of detection and prevention long before the followers will even think of it.
- **Viability.** I prefer to buy a product from a company that will be in business for the long haul. There may be some advantages from buying some products from a startup or a garage outfit, but for something as strategic as IPS, I would rather buy from a company that I know will be in business in five or ten years. Several years after purchase, I still want someone to answer the phone when I call.
- **Manageability.** There's nothing worse than a product that is difficult to operate and figure out. Most organizations will want a fully configurable IPS with deep levels of configurability — even if they don't plan on tinkering with the details too often.

- **Support.** Everyone gets stumped now and then, and every product is going to be prone to hardware or software trouble, no matter how good its quality program is. You want a company that stands behind its product and is ready to offer whatever kind of help you need.
- **Cost.** Don't be afraid to understand and specify your spending limits.

In the rest of this section, I discuss requirements that are specific to large (enterprise) organizations, smaller organizations, and government.

Small-to-medium-business (SMB) buying requirements

Hats off to small and medium sized businesses (those with fewer than 500 employees) that recognize their need for IPS and wade into the fray!

To the requirements listed earlier in this chapter, add one more that SMB customers are looking for: ease of management. They don't have deep staffs to take training courses and spend man-weeks planning their IPS implementation. In the SMB world, the IT guy (or gal) who has 12 other jobs besides security just wants to open the box and have the IPS running in a couple of hours. This means: easy setup and easy-to-understand configuration without having to take a week-long class on managing the device. They just want to set it and forget it!

Enterprise buying requirements

Enterprises are typically those organizations with, say, 500 or more employees. They generally have many business locations, often in more than one country. Usually they have larger IT organizations with network engineers, system engineers, security engineers, IT operations, and other individuals and departments — in other words, a lot of people who get involved in things like IPS because it potentially affects many people in the organization.

Two types of IPS users

Regarding how they approach security, there are generally two types of IPS users. First, there are "lean forward" users that truly care about security, are somewhat paranoid, but they use their fear as a tool to gain more knowledge and meet security problems head on.

Then there are "lean back" users that are either in senior-level positions or simply don't have time to spend monitoring and tuning the IPS. Some "lean back" users are driven by regulatory compliance and simply want to "check the IPS box" to satisfy compliance.

It's not only important to gauge the organization's goals for IPS usage, but also understand the types of users that will interact with the platform.

In addition to the general requirements discussed earlier in this chapter, enterprises are generally also interested in some of these requirements:

- **Management.** Rather than just a single administrative user for their IPS, enterprises need an IPS that can support many users and different roles.
- **Forensics.** Enterprises need their IPSs to be able to provide forensics-quality information to support security events related to sophisticated threats or those that may find their way into the criminal justice system as evidence.
- **Fault tolerance.** Enterprises build high-availability, fault-tolerant infrastructures to support high-demand applications. These organizations need IPSs that can match the *five-nines* availability environments they support, meaning there is practically zero minutes of unscheduled downtime per calendar year.
- **High throughput.** Moore's Law has proven that processing speed is doubling every two years. Thus, you will continue to see network speeds grow. IPS vendors, in particular, should have a broad range of products to support the smallest to the very largest network needs.
- **Low TCO.** Although enterprises have larger operating budgets than smaller organizations, they also have greater

demands for securing the network. Thus, enterprises must select an IPS that helps them to work smarter — not harder — by automating key functions, such as impact assessment, user identification, and IPS tuning.

Government buying requirements

Governments, especially the U.S. federal government, are tough customers, primarily because they know what they want and they communicate this through a comprehensive set of requirements. In addition to the general requirements at the beginning of this chapter, plus the requirements wanted by enterprises, governments often ask for these additional requirements:

- **Custom rules.** Some government organizations are required to "throw out" IPS rules provided by the manufacturer in favor of creating custom rules for proprietary systems. Selecting an IPS with an open architecture and easy-to-use rule creation wizard is optimal for such organizations.
- **IPv6 compliant.** U.S. federal government regulations require all IT systems to be IPv6 compatible. In the case of an IPS, it must be capable of detecting and blocking IPv6 attacks and be managed on an IPv6 network.
- **Federal Information Security Management Act (FISMA) compliance.** This is a complete end-to-end security framework required of all federal information systems and supporting environments. FISMA requires federal agencies (and their service providers) to establish and carry out a security plan, maintain IT asset inventories, categorize information and information systems according to risk level, enact security controls, perform risk assessments, perform continuous monitoring, and undergo periodic certification and accreditation. An IPS is an essential tool for achieving FISMA compliance.
- **NIST compliance.** Government customers will frequently cite various NIST (National Institute of Standards and Technology, the U.S. government's IT standards setting organization) standards as part of their IPS selection criteria, especially NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems."

- **Evaluation Assurance Level (EAL).** Government customers may require that an IPS be tested and certified to a specific EAL standard. EAL testing is extremely expensive, so any vendor that claims EAL compliance is noteworthy for any government or non-government customer.

Industry-Specific Considerations

Organizations in some industries will impose additional requirements on IPS vendors, generally as a "pass through" where organizations are asserting requirements on the suppliers that are imposed upon them.

Public utilities

Power, water, natural gas, and other public utilities rely on Supervisory Control and Data Acquisition (SCADA), Process Control Network (PCN), and Smart Grid technology for remote control and monitoring of utility equipment. These systems are almost always IP-based and frequently utilize the public Internet for transmission.

An IPS helps to secure SCADA, PCN, and Smart Grid systems by detecting and blocking intrusions that could include terrorist attacks. Leading IPS solutions may offer special SCADA, PCN, and/or Smart Grid rule sets and may also incorporate passive network intelligence collection for correlating threats without actively scanning the network.

Healthcare

Healthcare providers and other industry organizations subject to HIPAA requirements need to incorporate IPSs into their network infrastructure as part of their technical safeguards. These organizations' requirements will often resemble those required for most enterprises, as discussed earlier in this chapter.

Financial

Banks, credit unions, brokerages, and insurance companies are required to protect sensitive customer information from

theft and abuse. These organizations will often impose enterprise level requirements, including enterprise scalability and management.

FISMA and Basel II are the primary regulations requiring financial institutions to protect their systems and networks.

Telecommunications

Common carriers, including telecommunications providers and Internet service providers, have the world's most extensive networks over which the world's Internet and private communications take place. Most of these organizations are under market or regulatory pressure to provide *five-nines* availability. Such organizations will require the most robust IPS platforms, including support for high-throughput environments, fault-tolerant hardware, and fail-open interfaces.

Hardware Considerations

Organizations shopping for IPSs need to understand what hardware features are important for them. Hardware centric requirements will generally fall into these categories:

- **Inline IPS or passive IDS.** An organization needs to decide whether it is looking for an inline IPS, which will block unwanted traffic, or a passive IDS, which will only report on (but not block) unwanted traffic. Although there are no purely passive IDS products available, this requirement speaks more to the functional requirement and purpose of the IPS — primarily whether it is intended to be an active (blocking) or passive (reporting only) device.
- **Purpose-built appliances.** Organizations may wish to specify whether they're looking for IPS software that they would install on their own servers, generic appliances, or a purpose-built appliance with IPS features built into the hardware. If you consider an IPS vendor with purpose-built appliances, ensure that this doesn't hinder the extensibility of the solution by verifying the availability of Virtual IPS offerings for VMware, Xen, or other virtualization platforms.

Some IPS appliances rely on ASICs (application-specific integrated circuits) to accelerate certain network processing functions. Although ASICs make it easier for the vendor to achieve higher throughputs, it usually makes it more difficult for them to port their software to VMware, Xen, and other virtual platforms. Even if you don't have a budgeted virtualization security project today, you will tomorrow. Be sure to select an IPS partner that offers both physical and virtual appliances so you don't eventually end up with two sets of IPS solutions.

- **Hardened operating system.** Organizations' requirements may be as detailed as specifying the desired operating system that supports the IPS software. Most of today's IPS products incorporate a hardened Linux OS in their appliances.
- **Fault tolerance.** Organizations may specify various fault tolerance features including redundant power supplies, disk drives, fans, and fail-open interfaces.
- **Fail open.** Organizations doing their homework will want an IPS appliance that fails open, meaning, in the event of a catastrophic hardware failure, network traffic will continue to flow through the IPS appliance uninterrupted. This feature requires special hardware not found in general purpose appliances.

Third-Party Testing

There are two independent test laboratories in particular that actively test IPS products — ICSA Labs and NSS Labs. These companies evaluate leading IPS devices for accuracy, reliability, and performance. Organizations that are serious about the desired quality of their IPS systems should consider only products that have been independently evaluated by a reputable third-party testing organization.

Test reports on leading IPS products may be purchased from ICSA Labs and NSS Labs directly or can often be obtained at no charge from the IPS vendors themselves.

Chapter 7

Ten Ways to Lower TCO

In This Chapter

- Recapping the benefits of a Next-Generation IPS
- Describing ten ways to lower IPS total cost of ownership (TCO)

When assessing the cost of a network IPS, it's not only important to assess the acquisition costs and annual maintenance fees, but also the cost to deploy and maintain the IPS — which often represents the bulk of total cost of ownership (TCO) over a three- to five-year period.

A Next-Generation IPS leverages real-time network, application, behavior, and user awareness to automate key IPS functions. These awareness capabilities provide you with unparalleled visibility, minimizing your reliance on other IT teams and empowering you to automate key IPS functions that a more traditional IPS simply can't.

By leveraging this newfound awareness, a Next-Generation IPS offers numerous advantages over a traditional IPS, including:

- Stronger network protection
- Superior performance, scalability, and availability
- Simpler deployment and ongoing maintenance
- Lower total cost of ownership

Total cost of ownership (TCO) includes all costs associated with acquiring, deploying, maintaining, and operating a system — in this case, a network IPS. Through powerful

automation and advanced feature sets, a next-generation IPS can lower TCO significantly — in many cases recovering the cost of IPS acquisition through drastic reductions in operating expenses.

The following are ten ways to lower TCO through the acquisition of a Next-Generation IPS:

- **Reduce the noise through impact assessment.** By correlating threats against real-time endpoint intelligence, a Next-Generation IPS can reduce the quantity of actionable security events by 95 percent or more. For example, why investigate a Conficker event that can only harm Windows hosts when it is targeting a Linux host?
- **Take the guesswork out through automated IPS tuning.** A Next-Generation IPS knows what's running on your network and can recommend IPS rules to enable and disable, resulting in increased protection, optimized IPS sensor performance, and recovery of up to a day's worth of effort each month.
- **Link users to security and compliance events.** What good is it to know that 192.168.4.12 is under attack if you don't know whom to contact? A Next-Generation IPS instantly provides usernames and contact information for users associated with security and compliance events, negating the need to manually sift through Active Directory, LDAP, and DHCP logs. Done the old-fashioned way, the attack might be over before you even know where to start looking!
- **Leverage one platform for physical and virtual IPS.** Don't buy physical IPS products from one vendor and virtual IPS products from another. Insist on one unified platform from a single vendor, negating the need for duplicative reports, alerts, dashboards, and technical support departments.
- **Customize IPS rules for proprietary applications and systems.** Don't spend money on a web application firewall (WAF) or other network security products to do the job of a Next-Generation IPS. Leverage custom rules to protect proprietary web applications and other systems.

- **Remove network blind spots through SSL inspection.** Improve your security posture by decrypting SSL traffic prior to IPS inspection. Ensure that original (clean) SSL traffic is re-encrypted before being placed back onto the wire to maintain data confidentiality and regulatory (for example, PCI) compliance.
- **Reduce the surface area of attack through compliance rules and whitelists.** Today's Next-Generation IPS can help you model and enforce your organization's acceptable use policies (AUPs). Leverage compliance rules and whitelists to help reduce your network's surface area of attack.
- **Detect threats from the inside that your IPS may miss.** A perimeter IPS will miss every exploit that is hand-carried through the office front door on mobile computing devices. Increase your defense-in-depth posture by implementing Network Behavior Analysis (NBA) to baseline normal network traffic and detect anomalies.
- **Improve security by controlling VM sprawl.** Be alerted when new VMware, Xen, or other virtual machines (VMs) pop up on the network without knowledge or approval of the IT security team. Audit new VMs for compliance with internal security policies. This will help you to be in control of your VM infrastructure.
- **Integrate your IPS into your existing IT security infrastructure.** Leverage existing investments in SIEM, vulnerability management, network forensics, network access control (NAC), and other infrastructure components to share intelligence, automate remediation, and accelerate incident response.

Sourcefire would like to thank its sponsors

Find out why intrusion prevention systems are needed and which features are most important for your organization

Intrusion prevention systems are a critical part of an organization's overall network and systems protection strategy. Without them, you're fighting the bad guys with one arm tied behind your back. This book gives you the need-to-know information that can help you understand how these solutions improve the security in an organization's networks.

- ***How intrusion prevention systems work* — *and the ways they detect network-based attacks***
- ***What types of threats that IPSs are designed to detect and deflect* — *including some of the nastier threats such as zero-day and advanced persistent threats***
- ***Which features and functions are found in Next-Generation IPSs* — *including impact assessment, application monitoring, automated IPS tuning, and user identification***
- ***How cloud and virtualization fit in* — *and the role that IPSs play to protect these new types of environments***
- ***Look at IPS and standards and regulations* — *such as PCI, HIPAA, GLBA, SAS70, and FISMA***
- ***Select the right IPS* — *get your IPS shopping list organized so that you get the IPS that is right for your organization***

Open the book and find:

- **What constitutes a zero-day attack**
- **A look at the benefits and risks of virtualization**
- **A list of ways to lower the total cost of ownership**
- **Information on complying with regulations**
- **The difference between passive and inline systems**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

Steve Piper, CISSP, SFCP, is Sr. Director of Product Marketing with Sourcefire and an 18-year high-tech veteran. Prior to Sourcefire, Steve held senior-level positions with Citrix and NetIQ and has achieved technical certifications from ISC², Microsoft, Novell, Sourcefire, and more. Steve holds BS and MBA degrees from George Mason University.

For Dummies®
A Branded Imprint of
WILEY

978-1-118-00474-6
Not for resale