Making Everything Easier!™

Palo Alto Networks Edition

Network Security Management

FOR DUMMIES®

A Wiley Brand

Learn to:

- Consolidate firewalls and other security deployments
- Automate common security management processes
- Use actionable intelligence to respond to threats

Brought to you by

paloalto NETWORKS®

Lawrence C. Miller, CISSP

Palo Alto Networks

Palo Alto Networks is leading a new era in cybersecurity by securing thousands of enterprise, government, and service provider networks from cyber threats and protecting our digital way of life. The next-generation platform uses an innovative traffic classification engine that identifies network traffic by application, user, and content.

The Palo Alto Networks next-generation security platform is built on four main principles:

1. **Natively integrated** technologies that support open communication, orchestration, and visibility;
2. **Automation** of protection creation and reprogramming of the security posture across network, endpoint and cloud environments;
3. **Extensibility** that allows for protection of customers as they expand and market requirements change; and
4. **Threat intelligence sharing** to minimize the spread of attacks by providing protection based on comprehensive global threat data.

The next generation security platform offers superior protection against the sophistication of modern attacks, can reduce the total cost of ownership for organizations by simplifying their security infrastructure, and eliminates the need for multiple, stand-alone security appliances and software products.

Find out more at **www.paloaltonetworks.com**

Network Security Management

FOR

DUMMIES®

A Wiley Brand

Palo Alto Networks Edition

Network Security Management FOR DUMMIES®

A Wiley Brand

Palo Alto Networks Edition

by Lawrence C. Miller, CISSP

FOR DUMMIES®
A Wiley Brand

Network Security Management For Dummies®, Palo Alto Networks Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-1-119-28399-7 (pbk); ISBN 978-1-119-28400-0 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

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

Development Editor: Elizabeth Kuball

Copy Editor: Elizabeth Kuball

Acquisitions Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Kumar Chellappan

Table of Contents

Introduction

Albert Einstein is famously quoted as saying that "insanity is doing the same thing over and over again and expecting different results." Yet many organizations exhibit such insanity with a "rinse and repeat" approach to network security management that includes the following:

- Performing manual, error-prone processes that increase network and security complexity
- Deploying numerous and costly "one-off" network security products that don't integrate with the rest of the network security environment
- Restricting network visibility and creating information silos with security products that report independently on limited parts or aspects of network security

This approach is inefficient and ineffective and does nothing to improve the organization's overall network security. It increases management complexity, produces overwhelming amounts of threat information from numerous data streams, and slows the organization's ability to effectively respond to network security threats.

Today's enterprise security deployments require a network security management solution that provides the following:

- Centralized administration with automated and streamlined management and configuration processes
- Greater network visibility with comprehensive reporting across the entire network security environment
- Prioritization of critical threats to enable faster, more effective incident response

The benefits of effective network security management include greater efficiency, reduced complexity, and better overall security. In addition to the ability to configure and manage a network from a central location, a single security rule base can be accurately and consistently maintained and kept current much more easily than multiple, independently managed security product deployments.

About This Book

Network Security Management For Dummies consists of seven short chapters that explore the following:

- The constantly evolving threat landscape and the challenges it creates in network security management (Chapter 1)
- The complexity in today's network security environment (Chapter 2)
- The "operational gap" in network security (Chapter 3)
- Why network security management is necessary (Chapter 4)
- What you need in a network security management solution (Chapter 5)
- How to effectively manage network security data (Chapter 6)
- How to evaluate your network security management options and need (Chapter 7)

Finally, if you get lost in all the acronyms and technical terms used throughout the book, there's a glossary to help you out!

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I'll assume a few things nonetheless!

Mainly, I assume that you're an information security professional for an organization of some sort — perhaps a small or medium business, large enterprise, nonprofit, or military or government agency. As such, this book is written primarily for technical readers who know a little something about network security.

I also assume that you're looking for a network security management that will help you address the visibility and management challenges in your network environment.

If any of these assumptions describes you, then this book is for you. If none of these assumptions describes you, keep reading anyway. It's a great book and when you finish reading it, you'll know enough about network security management to be dangerous.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out information that you should commit to your nonvolatile memory, your gray matter, or your noggin' — along with anniversaries and birthdays!

TECHNICAL STUFF

You won't find a map of the human genome here, but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon!

TIP

Thank you for reading, hope you enjoy the book, please take care of your writers! Seriously, this icon points out helpful suggestions and useful nuggets of information.

WARNING!

This icon points out the stuff your mother warned you about. Okay, probably not. But you should take heed nonetheless — you might just save yourself some time and frustration!

Beyond the Book

There's only so much I can cover in 72 short pages, so if you find yourself at the end of this book, thinking, "Gosh, this was an amazing book — where can I learn more?" just go to `www.paloaltonetworks.com`.

Where to Go from Here

If you don't know where you're going, any chapter will get you there — but Chapter 1 is a good place to start! If you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is written to stand on its own, so feel free to start reading anywhere and skip around to your heart's content! Read this book in any order that suits you (though I don't recommend upside down or backward).

Chapter 1

Defining Network Security Management Challenges

In This Chapter

- Surveying the modern threat landscape
- Understanding how “defense in depth” has become “defense ad nauseam”
- Taking stock of network security responsibilities

Albert Einstein famously — okay, perhaps not as famous as his “insanity” quote (see the Introduction), but no less sage — said, “Everything should be made as simple as possible, but not simpler.” Yet network and security administrators today are besieged by a deluge of security data flowing relentlessly from multiple disparate sources. This situation has created a complex morass that is almost impossible to manage and inevitably weakens the organization’s overall security posture and threat response capability. All this complexity is the result of changes in the way we store, access, and share data among different security systems and functions.

In this chapter, you learn about the different network security challenges that growing organizations must address in order to maintain an effective security posture and threat response capability — that is, to make everything as simple as possible, but not simpler!

The Evolving Threat Landscape

Over the past decade, the application landscape has changed dramatically. Enterprise business applications, such as ERP and CRM, have been joined by a horde of social networking and personal productivity applications, such as LinkedIn and Box, that are often available as SaaS, web-based, or mobile apps. Employees are accessing corporate data remotely and through their mobile devices, and an increasing amount of data is stored in the public cloud.

This convergence of corporate infrastructures and personal technologies is being driven by several important trends:

- **Cloud computing:** The popularity of cloud computing service models in general, and SaaS application services in particular, continues to surge. A recent Gartner survey found that alternative consumption models, including SaaS, hosted license, on-premises subscriptions, and open source, accounted for more than half of new enterprise software implementations.
- **Consumerization:** The process of consumerization occurs as end-users increasingly find personal technology and applications that are more powerful or capable, more convenient, less expensive, quicker to install, and easier to use than corporate IT solutions.
- **BYOD:** Closely related to consumerization is BYOD, a policy trend in which organizations permit end-users to use their own personal devices, primarily smartphones and tablets, for work-related purposes.
- **BYOA:** Social networking and personal productivity apps on personal devices are increasingly being used for work-related purposes. As the boundary between work and their personal lives becomes less distinct, end-users are practically demanding that these same apps be available to them in their workplaces.
- **Mobile computing:** People's appetite for rapid, on-demand access to apps and data from anywhere, at any time, on any device is insatiable. There are more than 2.6 billion smartphone subscriptions worldwide and according to the June 2015 Ericsson Mobility Report, total mobile monthly data traffic (including audio, file sharing, social networking, software uploads and downloads, video, web browsing, and other sources) in the first quarter of 2015 was approximately 3,500 petabytes!

Clearing the air about cloud computing service and deployment models

The three cloud computing service models defined by NIST are

- **SaaS:** Customers are provided access to an application running on a cloud infrastructure. The application is accessible from various client devices and interfaces, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer may have access to limited user-specific application settings, and security of the customer's data is still the responsibility of the customer.
- **PaaS:** Customers can deploy supported applications onto the provider's cloud infrastructure, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over the deployed applications and limited configuration settings for the application-hosting environment. The company owns the deployed applications and data and is, therefore, responsible for the security of those applications and data.
- **IaaS:** Customers can provision processing, storage, networks, and other computing resources and deploy and run operating systems and applications, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over operating systems, storage, and deployed applications, as well as some networking components (for example, host firewalls). The company owns the deployed applications and data and is, therefore, responsible for the security of those applications and data.

NIST defines four cloud computing deployment models:

- **Public:** A cloud infrastructure that is open to use by the general public. It's owned, managed, and operated by a third party (or parties) and exists on the cloud provider's premises.
- **Community:** A cloud infrastructure that is used exclusively by a specific group of organizations.
- **Private:** A cloud infrastructure that is used exclusively by a single organization. It may be owned, managed, and operated by the organization or by a third party (or a combination of both), and may exist on or off premises.
- **Hybrid:** A cloud infrastructure that is composed of two or more of the aforementioned

(continued)

(continued)

deployment models, bound together by standardized or proprietary technology that enables data and application portability (for example, failover to a secondary data center for disaster recovery or content delivery networks across multiple clouds).

The rapid adoption of many popular SaaS, web-based, and mobile apps is often driven by end-users, not by IT. The ease with which these apps can be accessed and their familiarity to end-users point toward a continuation of the above trends, as well as a growing "shadow" IT culture in which individual end-users, cross-functional teams and ad-hoc workgroups, and entire departments, use both sanctioned ("allowed") and unsanctioned ("not allowed") apps in the enterprise. Examples of these apps include the following:

- Collaboration tools such as Google Docs and Microsoft Office 365
- Cloud storage services such as Box and Dropbox
- Web-based email such as Gmail, Outlook.com, and Yahoo! Mail
- Content management tools such as Microsoft SharePoint
- CRM portals such as Salesforce and SugarCRM
- Social networks such as Facebook and LinkedIn
- Web publishing tools such as YouTube
- Unified messaging tools such as Skype and Vidyo
- Posting tools such as Twitter

To appreciate how rapidly these apps, both sanctioned and unsanctioned, have proliferated the corporate network, consider that the Palo Alto Networks Spring 2015 Application Usage and Threat Report found that SaaS- and web-based app usage increased 46 percent (from 218 to 316 unique apps) between 2012 and 2015 in organizations participating in the research. Cloud-based storage and web-based email accounted for the overwhelming majority of these apps — 40.7 percent and 38 percent, respectively.

With more than 40 percent of unknown malware threats and exploits still being delivered by email, and the inherent risk of data loss due to sensitive data (such as PHI and PII) potentially being uploaded to cloud-based storage and improperly shared, the risks associated with these apps cannot be ignored by enterprise security teams.

Unsure of how to manage these trends in their business processes and leverage the associated benefits, many organizations either implicitly allow these apps simply by ignoring their use in the workplace, or explicitly prohibit their use, but are then unable to effectively enforce such policies with traditional port-based firewalls and other add-on security technologies. Neither of these two approaches is ideal, and both incur lost productivity and inherent risks for the organization. Other adverse issues include the following:

- Creating a "shadow IT" subculture of backchannel or underground workflow processes that are critical to the businesses' operations, but are known only to a few users and fully dependent on personal mobile devices and SaaS-based, web-based, and mobile apps
- Introducing new risks to the entire networking and computing infrastructure, due to the presence of unknown and, therefore, unaddressed and unpatched vulnerabilities, as well as threats that target normal application and user behavior — whether a vulnerability exists in the application or not
- Being exposed to noncompliance penalties for organizations that are subject to regulatory requirements such as HIPAA, FINRA, and PCI DSS
- Having employees circumvent security controls with anonymizers and proxies (such as Tor and UltraSurf), encrypted tunnels (such as SSL/TLS), and remote access tools (such as Ammyy, LogMeIn, RDP, and TeamViewer), making it difficult, if not impossible, for security and risk managers to see the risks they're attempting to manage

WARNING!

The use of anonymizers and proxies on any network should be considered extremely risky and highly suspect.

REMEMBER

Remote access tools can be both good and bad. They're valuable productivity tools for IT administrators and support technicians, but also prone to exploit by attackers in order to control systems.

Ammyy

In recent years, the legitimate remote access application known as Ammyy has commonly been exploited by adversaries in vishing attacks. These attacks have been largely targeted at English-speaking countries and have been fairly successful in duping users into installing the remote access application and giving the adversary access to their systems.

The attack generally starts with a user receiving a phone call from a person purporting to be from Microsoft, Dell, or even their own organization's IT department. The adversary may then claim that the user's system has been discovered to be infected by some form of advanced malware and the user must now install a specific application (Ammyy) to remove it. The adversary then directs the user either to the official Ammyy website to download the server software or to another website that hosts the server software. The adversary asks the user for the code that the Ammyy software generates, giving the adversary complete access to the user's system. At this point, the adversary may claim the malware infection has been fixed or may begin to load actual malware onto the now remotely controlled system to hold the user at ransom or perform other nefarious activities. The industries with the most number of sessions captured for Ammyy usage were federal government, manufacturing, and energy.

The challenge is not only the growing diversity of the apps, but also the inability to clearly and consistently classify them as good or bad. Although many apps are clearly good (low risk, high reward) and others are clearly bad (high risk, low reward), most apps are somewhere in between — depending on how they're used, which can vary from one scenario to the next and from user to user or from session to session.

For example, using a cloud-based storage service, such as Dropbox, to share product documentation with a prospective customer would be "good" (medium risk, high reward), while using the same service to share details of an upcoming software release with a group of friends that includes employees of a competitor would be "not so good" (high risk, no reward).

Indeed, many organizations now use a variety of SaaS-based, web-based, and mobile apps to support a wide range of legitimate business functions, such as recruiting, research and development, marketing and sales, and customer support — and many are even inclined to allow the use of such apps, to some extent, as a way to provide an “employee friendly” work environment and improve morale. Many organizations are also seeing significant benefits from the use of these apps and technologies, including an increased ability to share ideas, more rapid access to knowledge experts, and a reduction in travel, operations, and communications costs.

New Threats Mean New Security Deployments

The modern threat landscape has led many organizations to adopt a reactive security strategy in which the response to each new threat is to purchase and deploy a new security solution. For example:

- Anti-DDoS is deployed to mitigate distributed denial-of-service attacks.
- Anti-malware is deployed to prevent malware infection.
- DLP solutions are deployed to prevent the accidental or intentional exposure of sensitive data such as PHI, PII, or credit card information.
- IDS and IPS are deployed to defend against vulnerabilities and exploits.
- Spam filters are deployed to counter email spam.
- URL filters are deployed to enforce Internet acceptable use policies and prevent web-based threats.

You have to protect all your users wherever they are, and all your data wherever it resides. This means all the security solutions listed earlier need to protect on premises, across endpoints, and in public and private cloud environments.

All these purpose-built network security deployments have created more complex network architectures, administrative nightmares, and an increased threat exposure for organizations.

The multitude of different security technologies, management consoles, and reporting mechanisms requires a “cutting-edge” depth of knowledge and skills about different security technologies and solutions that is practically impossible to maintain, and presents network and security teams with insurmountable volumes of disjointed data from many different sources. Many organizations then add even more security products, such as logging and monitoring or security information and event management (SIEM) tools, to make sense of all the data!

Network Security Management Responsibilities

Peter Parker's uncle famously said, "With great power comes great responsibility." The reality for today's network and security teams is that with ever greater responsibilities comes less power to see what's happening on the network and respond adequately to security threats and cyberattacks.

A day in the life of a network or security administrator might typically include the following:

- Setting up networks and device configurations
- Managing firewall and other security rules and policies
- Monitoring network traffic and threats on-premises, off-premises, and in the cloud for both company-approved (sanctioned) and not approved (unsanctioned) applications
- Correlating threats and responding to critical security events
- Logging all traffic and threats for research purposes, as well as for compliance reasons
- Providing actionable reports for management and executives, who need exactly the right information to make quick, informed decisions

Of course, I'm referring to a 2,802-hour day in the life of a network or security administrator on Venus! A day in *your* life is still just 24 hours. You either need to pack up your network and move to Venus (take lots of sunscreen) or explore network security management solutions that can help you take back control of network security in your organization back here on Earth!

Chapter 2

Recognizing the Complexity in Network Security Today

In This Chapter

- Controlling firewall sprawl
- Eliminating multiple-point security solutions
- Maintaining security policies and rule bases
- Monitoring volumes of security log data
- Losing visibility across your network
- Managing and controlling multiple administrators
- Deploying next-generation firewalls and network security management

In this chapter, you learn how complexity in the network has made the job of network security management so challenging.

Multiple Firewalls

In even the smallest networks, multiple firewalls have become commonplace because organizations understand the pivotal role that firewalls play in protecting their networks and attempt to eliminate single points of failure in their networks with high-availability deployments that provide redundancy.

As the organization grows, so, too, does its network. And the perimeter often expands beyond a traditional on-premises data center. As firewalls are added in multiple data centers, on different network segments, in the cloud, and on individual virtualized application workloads (known as *micro-segmentation*), the security management nightmare begins.

But the problem for network and security teams isn't necessarily the number of firewalls that are being deployed. In fact, many current and evolving security best practices advocate the deployment of even more firewalls throughout the network. Instead, the problem is the type of firewalls that are deployed.

Years ago, most firewalls did a pretty good job of controlling traffic in and out of corporate networks. That's because application traffic was generally well behaved. Email would typically flow through port 25, FTP was assigned to port 20, and web surfing was hanging, uhhh, port 80. Everybody played by the rules that "ports + protocols = applications" and the firewall had everything under control. Blocking a port meant blocking an application. Nice and simple.

Unfortunately, the Internet has never really been nice and simple — and that's truer today than ever before. Today, the Internet often accounts for 70 percent or more of the traffic on your corporate network. And it's not just port 80 web surfing. Typically, 20 percent to 30 percent of it is encrypted SSL traffic on port 443. Even worse, there is a plethora of new Internet applications that insist on making their own rules. They wrap themselves in other protocols, sneak through ports that don't belong to them, and bury themselves inside SSL tunnels. In short, they just don't play fair.

All these applications carry some inherent risk to your business. And they play host to clever new threats that can slip through your firewall undetected. Meanwhile, your firewall just sits there like nothing's wrong because it's still playing by rules that don't exist anymore!

Because they're deployed in-line at critical network junctions, firewalls see all traffic and, therefore, are the ideal resource to provide granular access control. The problem, however, is that most firewalls are "far-sighted" — they can see the general shape of things, but not the finer details of what's actually happening. This is because they operate by inferring the application-layer service that a given stream of traffic is associated with, based on the port number used in the packet's header, and they only look at the first packet in a session to determine the type of traffic being processed, typically to improve performance. They rely on a convention — not a requirement — that a given port corresponds to a given service (for example, TCP port 80 corresponds to HTTP).

As such, they're also incapable of distinguishing between different applications that use the same port/service.

The net result is that traditional, "port-based" firewalls have basically gone blind. Besides being unable to account for common evasion techniques such as port hopping, protocol tunneling, and the use of nonstandard ports, these firewalls simply lack the visibility and intelligence to discern which network traffic

- Corresponds to applications that serve a legitimate business purpose
- Corresponds to applications that can serve a legitimate business purpose but, in a given instance, are being used for unsanctioned activities
- Should be blocked because it includes malware or other types of threats, even though it corresponds to legitimate business activities

On top of everything else, their control model is typically too coarse-grained. Said firewalls can either block or allow traffic, but offer little variation in between to craft a more appropriate response for all the "gray" applications that enterprises would ultimately like to support — for example, by allowing certain functions or file transfers within an application but not others, allowing but also applying traffic-shaping policies, allowing but scanning for threats or confidential data, or allowing based on users, groups, or time of day.

Multiple-Point Solutions

Traditional port-based firewalls really don't provide value anymore — not in a world where network boundaries are disintegrating and Internet applications are exploding.

But you already know that, which is why you've been forced to make up for their glaring deficiencies with more specialized security deployments and point security solutions — IPSs, proxies, antivirus, anti-spyware, URL filtering, and more. Sure, these tools add some incremental value, but it's getting harder to justify their additional cost and complexity. A recent study by Enterprise Strategy Group (ESG) sponsored by Tufin, a security policy orchestration vendor, found that

55 percent of enterprises believe network security is more difficult today than two years ago because of additional devices on the network, more traffic, and increased use of technologies.

Without network security management, these additional security deployments add more noise to your security environment and actually make it more difficult for you to protect your network.

WARNING!

More security appliances doesn't necessarily mean a more secure environment. In fact, the complexity and inconsistency associated with such an approach can be a detriment to your organization's security strategy. Clearly, such a strategy doesn't scale. More important, none of these additional products give you the visibility and control you need over the applications running on your network.

Bolt-on functionality is fundamentally flawed

Many purveyors of traditional firewalls have attempted to correct the far-sighted nature of their products by incorporating deep packet inspection (DPI) capabilities. On the surface, adding a measure of application-layer visibility and control in this manner appears to be a reasonable approach.

However, the boost in security effectiveness that can be achieved in most cases is only incremental because the additional capability is being "bolted on," and the foundation it's being bolted onto is weak to begin with. In other words, the new functionality is added on rather than integrated, and the port-based firewall, with its complete lack of application awareness, is still used for initial classification of all traffic.

Here are the problems and limitations this leads to:

- **Applications that shouldn't be on the network are allowed onto the network.**
- **Not everything that should be inspected necessarily gets inspected.** Because the firewall is unable to accurately classify application traffic, deciding which sessions to pass along to the DPI engine becomes a hit-or-miss proposition.

- **Security posture gets limited.** The bolted-on application classification ability often doesn't get shared with later enforcement capabilities (for example, file transfer). This makes it impossible for those enforcement options to be precisely applied "per application."
- **Policy management gets convoluted.** Rules on how to handle individual applications essentially get "nested" within the DPI portion of the product — which itself is engaged as part of a higher/outer-level access control policy.
- **Inadequate performance forces compromises to be made.** Inefficient use of system resources and CPU and memory-intensive application-layer functionality can put considerable strain on the underlying platform. To account for this situation, administrators can only implement advanced filtering capabilities selectively.

Firewall "helpers" don't help

Over the years, enterprises have also tried to compensate for their firewalls' deficiencies by implementing a range of supplementary point security solutions, often in the form of stand-alone appliances. IPSs, antivirus gateways, web filtering products, and application-specific solutions — such as a dedicated platform for instant messaging security — are just a handful of the more popular choices. Unfortunately, the outcome is disappointingly similar to that of the DPI approach, with an additional twist.

Not everything that should get inspected does because these firewall helpers can't see all the traffic, rely on the same port- and protocol-based classification scheme that has failed the legacy firewall, or only provide coverage for a limited set of applications. Policy management is an even greater problem given that access control rules and inspection requirements are spread among several consoles and involve multiple policy models. And performance is still an issue as well, at least in terms of having a relatively high aggregate latency.

Then comes the kicker: device sprawl. As one "solution" after another is added to the network, the device count, degree of complexity, and total cost of ownership all continue to rise. Capital costs for the products themselves and all the supporting infrastructure that is required are joined by a substantial collection of recurring operational expenditures, including support/maintenance contracts, content subscriptions, and facilities costs (power, cooling, and floor space) — not to mention an array of “soft” costs such as those pertaining to IT productivity, training, and vendor management. The result is an unwieldy, ineffective, and costly endeavor that simply isn’t sustainable.

The traditional IPS is a poor match for today’s threats

IPSs detect and block attacks focused on vulnerabilities that exist in systems and applications. Unlike IDSs, which focus only on alerting, IPSs are intended to be deployed in-line to actively block attacks as they’re detected.

One of the core capabilities of an IPS is the ability to decode protocols to more accurately apply signatures. This allows IPS signatures to be applied to very specific portions of traffic, thereby reducing the percentage of false positives that were often experienced with signature-only systems. It’s important to note that most IPS offerings will use port and protocol as the first pass of traffic classification, which, given the evasive characteristics of today’s applications, may lead to an erroneous identification of the application. And because IPS systems are focused mainly on attacks, they’re typically deployed in conjunction with a firewall as a separate appliance or as a combination firewall and IPS.

IPSs are designed to stop threats using a “find it and kill it” approach. They aren’t designed to control applications. But even for stopping threats, IPSs have their flaws.

Given the new application and threat landscape, organizations are also reexamining traditional IPSs. The major IPS vendors are struggling to differentiate across several basic elements of IPSs:

- **Server and data center protection:** There are only a handful of detection and prevention techniques, and most IPS products support them all. These techniques include protocol anomaly detection, stateful pattern matching, statistical anomaly detection, heuristic analysis, blocking of invalid or malformed packets, and IP defragmentation and TCP reassembly (for anti-evasion). Most IPS vendors also use vulnerability-facing signatures (as opposed to exploit-facing signatures) and turn off server-to-client protection to improve performance.

- **Research and support:** This comes down to how much actual research vendors are doing, and how quickly they can respond to help enterprises protect against new attacks and vulnerabilities. Much is made of the efforts of the research teams of IPS vendors, and while there certainly are differences, much of the research is outsourced to a few industry research stalwarts. The other aspect is critical, regardless of who does the research: Can the vendor deliver timely updates to protect customers from new and emerging threats?
- **Performance:** Organizations are clearly sensitized to IPS performance issues. The introduction of traffic/ application latency and bandwidth/performance are major concerns that cause enterprises to deploy "out-of-band" IPSs. Clearly, being able to keep up with enterprise expectations for throughput and latency is top of mind for many customers.

As defenses mature, however, attackers evolve. Given that IDSs and IPSs, like firewalls, are based on legacy techniques that are relatively well understood, new attacks are able to exploit well-known weak spots, including the following:

- **Application-borne threats:** Threat developers are using applications, both as targets and as transmission vectors. Applications provide fertile ground for both methods. Some application-borne threats (for example, many of the threats that move across social networks) are well understood; others are not. Regardless, attackers find it far easier to piggyback on applications and start their attack with the client.
- **Encrypted threat vectors:** The other important technique that threats employ is encryption. Security researchers have warned for years that encryption can be used by various threats, but encrypted attacks still need a conduit.

> Enter user-centric applications. Users are easily duped into clicking on encrypted links (too many users think that `https://` means "safe"), which can send encrypted threats sailing through enterprise defenses. This is increasingly simple on social networks, where the level of trust is extremely high. The other closely related vector is obfuscation via compression — traditional IPSs can't decompress and, thus, can't scan compressed content.

A common theme here is the level of control needed to prevent these newer threats — controlling applications and content, decrypting SSL/TLS, unzipping content to look for threats — all of which goes well beyond what IPSs traditionally do. A major limitation of IPSs, despite all the work to transition from IDSs, is that they remain a negative security model and are architected as such. Put more simply, IPSs rely on a "find it and kill it" model — which doesn't work very well for the types of control necessary to deal with many of these new threats that move over applications. Nor do IPSs lend themselves to an architecture and platform capable of decrypting and classifying all traffic.

A positive security model operates by expressly allowing all communications that are known to be benign, appropriate, or necessary, and excluding everything else. A negative security model operates by seeking to classify only undesirable communications and content, and employing countermeasures for those that are known to be bad.

A word on data leaks

Some of the biggest information-security news stories over the past few years involve the leaking of confidential or sensitive organizational data via applications (for example, U.S. government agencies and contractors, pharmaceuticals, and retailers). In most cases, the applications that the data leaked across were expressly forbidden — unfortunately, their policies couldn't be enforced with traditional firewalls and IPSs, or alerts (that required manual response) were lost in a sea of information. Given these high-profile security breaches, it's no wonder that organizations are starting to look for a better solution to help protect against such embarrassing incidents.

UTM only makes what is broken cheaper

Unified threat management (UTM) devices are another approach to modern security challenges that are nonetheless based on traditional techniques. UTM solutions were born as security vendors began bolting intrusion prevention and antivirus add-ons to their stateful firewalls in an effort to reduce the cost of deployment.

UTM products don't perform their functions any better than stand-alone devices. Instead, they provide convenience to the customer by integrating multiple functions into one device. Unfortunately, UTMs have a reputation for being inaccurate, being hard to manage, and performing poorly when services are enabled, relegating them to environments where the value of device consolidation outweighs the downside of lost functionality, manageability, or performance.

The primary advantage of the UTM solution is that it typically does a reasonable job of addressing the issues associated with device sprawl. Instead of having all the "helper" countermeasures deployed as separate devices, with UTM they all come in one physical package.

But so what? The result is really no different from the bolted-on approach and, therefore, exhibits the same deficiencies. Inadequate application classification and resulting blind spots in the inspections that are performed remain fundamental problems, while performance and policy management issues are compounded even further based on having to account for multiple additional countermeasures instead of just one.

Complex and Outdated Rule Bases

A major problem with deploying numerous port-based firewalls and different point security solutions is that they're practically impossible to manage and maintain. Inevitably, these security products don't integrate with other security products in your network — particularly when they're made by different vendors — and each has its own unique management interface.

Beyond the initial configuration of these security solutions, policies and rule bases must often be changed or updated to support the needs of the business. Manually updating policies and rule bases across even a handful of security devices can be challenging and error-prone — updating hundreds or even thousands of devices manually would take a mutant army of security administrators!

The net result of multiple security deployments that must be managed with manual processes is that network complexity increases, potentially harmful mistakes are made, productivity declines (try troubleshooting a newly deployed or updated application on your network in this environment), security policies and rule bases become outdated, and your overall security posture is compromised.

Juggling Multiple Administrators

Hand-in-hand with the nightmare of managing multiple firewalls and rule bases usually goes the complexity of managing multiple administrators, each with his or her own list of rule changes, reporting requirements, and visibility needs. How can you run one security network when you have independently managed firewalls managed by multiple administrators who make uncoordinated changes to the security and configuration settings of each firewall?

Waking Up to a Logging Nightmare!

Having multiple point solutions and firewall deployments leads to a convoluted logging nightmare. How can you possibly monitor and keep track of completely unrelated logs that come from multiple security solutions and are stored in different formats? The resulting data dump quickly turns into an unmanageable nightmare for a network or security administrator, where menacing threats can hide in the dark — well, in mountains of data.

Inability to View Information Centrally

The inability to view security information centrally goes hand-in-hand with deploying numerous port-based firewalls, different point security solutions, and multiple logging sources (as described in the preceding section). Again, because these solutions don't fully integrate with each other, it's impossible to get a complete picture of what's going on in your network. Without full visibility of the network, automated correlation of IOCs, and prioritization of threats, it's difficult to respond to threats in a timely and effective manner.

Deploying Next-Generation Firewalls

To restore the firewall as the cornerstone of enterprise network security, next-generation firewalls "fix the problem at its core." Starting with a blank slate, next-generation firewalls classify traffic by the application's identity in order to enable visibility and control of all types of applications — including web applications, SaaS, and legacy — running on organizational networks.

The essential functional requirements for an effective next-generation firewall include the ability to

- ✓ Identify applications regardless of port, protocol, evasive techniques, or SSL encryption before doing anything else
- ✓ Provide visibility of and granular, policy-based control over applications, including individual application functions
- ✓ Accurately identify users and subsequently use identity information as an attribute for policy control
- ✓ Provide real-time protection against a wide array of threats, including those operating at the application layer
- ✓ Integrate, not just combine, traditional firewall and network intrusion prevention capabilities
- ✓ Support in-line deployments with negligible performance degradation

The key to next-generation firewalls is the ability to do everything traditional port-based firewalls and many point security solutions do with the advanced capabilities that combine innovative identification technologies, high performance, and additional foundational features to yield an enterprise-class solution. Reducing the number of different firewalls and other security deployments in the network is an important first step toward effective network security management.

Chapter 3

Closing the Operational Gap

In This Chapter

- Springing into action after an alert is received
- Knowing what you know and what you don't know
- Streamlining security management processes

New products regularly come to market, purporting to provide better security and solve the latest security challenges. But for the most part, these solutions don't solve the complexity created by multiple, independent point products deployed in your network. Nor do they fully integrate with your existing security solutions in an automated way. This increased complexity and lack of integration and automation, along with the enormous amounts of largely uncorrelated data these products generate — which are impossible to fully sift through and hamper response times — results in operational gaps between where most organizations are with their network security and where they need to be. In this chapter, you examine these operational gaps more closely.

The Gap Between Security Alert and Action

The first operational gap exists between the time when a security alert is received and the time when action is taken. Network and security teams are inundated with data, but the data deluge doesn't help if they can't easily discern which alerts are inconsequential and which alerts are critical. Several cyberattacks against high-profile organizations in various industries over the past few years demonstrate the significance of this operational gap. Although each of these organizations had the tools they needed to detect the attack and take prompt action in each of their respective cases, the breach information was buried in mountains of other data. Thus, the gap between security alert and action was typically at least two weeks and, in some cases, as long as four to five months or more.

The 2015 Verizon Data Breach Investigations Report (DBIR) found that attackers were able to compromise an organization within days or less in approximately 90 percent of breaches, and in a matter of minutes 60 percent of the time. The DBIR also finds that the gap between compromise and discovery is widening (see Figure 3-1).

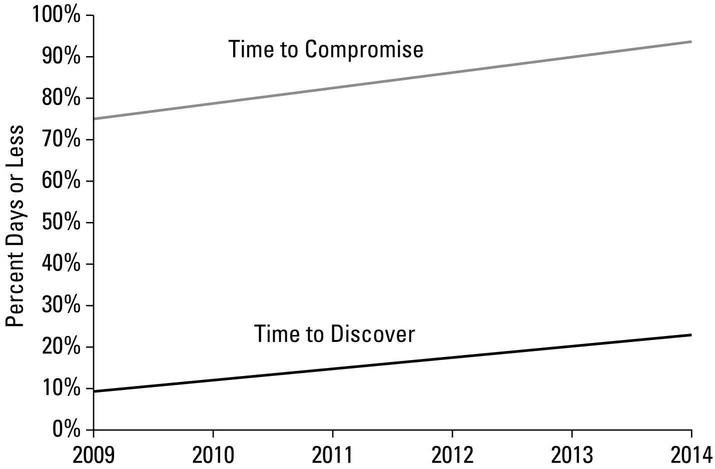

Figure 3-1: Two roads (time to compromise and time to discover) diverged, and I — I took the one less well managed.

According to a recent Ernst & Young study, 33 percent of all companies are not even aware of how long it takes their organization to organize a response to a threat. Is your organization among that 33 percent?

The Gap Between the Known and the Unknown

A second gap exists between what is known and unknown, or in the words of former U.S. Defense Secretary Donald Rumsfeld, "As we know, there are known knowns; there are things we know we know. We also know that there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns — the ones we don't know we don't know."

As the threat landscape grows increasingly complex, we are facing a growing number of unknown threats, and many security teams are struggling to keep pace. Discovering these threats quickly is crucial, but once discovered, security professionals also need to be able to quickly differentiate between critical and noncritical threats. Attacks are increasing in number and evasiveness, requiring more detailed detection and analysis that can keep up with the rapid threat innovation of cybercriminals and provide the tools needed for quick protection and easy mitigation.

To reduce the gap between known and unknown threats, many organizations deploy multiple, single-use sandboxing devices at every ingress, egress, and network point of presence. Again, these types of security deployments add complexity to the network architecture, and rely on highly skilled security teams with all the time in the world to analyze the mountains of data that are collected. The effectiveness of the sandboxing approach is limited by several additional factors, including the following:

- Only traffic that is seen on your network can be analyzed, as opposed to global traffic analysis that can be shared to provide a more proactive response capability before a new threat "in the wild" reaches your network.
- Threat analysis must be performed by a single organization's security team (or a security vendor, if engaged) with limited time and resources.
- No inherent threat prevention capability exists, so security protection (such as IPS signatures and firewall rules) must be manually created and deployed on the fly.

The 2015 Verizon DBIR found that 75 percent of all attacks spread from victim zero to victim one within 24 hours. (Talk about the zombie apocalypse!) This is largely due to the slow detection rate of unknown threats.

A cloud-based threat intelligence and prevention platform that provides complete visibility into unknown exploits and malware threats within all traffic across thousands of applications, including web traffic, email protocols (such as SMTP, IMAP, and POP), and FTP, regardless of ports or encryption (SSL), and integrates natively with your next-generation firewalls is a key security component to quickly identify and automatically stop advanced cyberattacks.

The Gap Between the Idea of Security and Implementation

Finally, there is a gap between the idea of security and the implementation of security to prevent breaches. Enterprise networks are growing fast and becoming more complex, while users are becoming more technologically savvy — and dangerous — and cybercriminals are becoming more sophisticated — and dangerous.

Many organizations have lots of outdated security policies, and maintain legacy security products, in a hapless effort to enforce those policies in the face of today's network security challenges, as well as trends — such as BYOD/BYOA and mobile computing (see Chapter 1) — that are fast becoming the new realities of our modern age.

The complexity of provisioning and managing new network security solutions has simply has become too overwhelming for many enterprise network and security teams. According to AlgoSec, 64 percent of all organizations are consumed with complex security policies that reduce the effectiveness of operations. Streamlining the security management process is a top priority in closing this gap.

Here are the keys to streamlining the security management process:

- **Reducing management complexity** by reducing the number of independently managed firewalls; consolidating security rule bases into a single, centralized rule base; coordinating the efforts of a team of administrators who are committing changes to configurations and rule bases; and matching network configurations to your organizational structure
- **Surfacing actionable important data** with central visibility of all network traffic, automated threat correlation, visual display of critical data, simple drill-down response capabilities, and actionable reporting
- **Implementing enterprise-class management** with the right capabilities, performance, hardware, and software for your growing and evolving network

The key to closing the operational gap is reducing response time (the gap between security alert and action), fast discovery of the unknown (the gap between the known and the unknown), and streamlined management (the gap between the idea of security and implementation).

Chapter 4

Why Network Security Management Is Essential

In This Chapter

- Understanding the challenge of managing multiple independent firewalls
- Avoiding error-prone, manual repetitive tasks, manual repetitive tasks
- Seeing the forest — and the trees

Managing enterprise firewalls is an important network security management function. But as an organization's network changes and becomes increasingly complex, efficient and effective network security management has become a growing challenge.

This chapter explores the challenges of network security management and explains why you need a network security management solution to help you maintain your organization's information security posture.

Too Many Firewalls, Not Enough Time

The traditional analogy likening a network perimeter to the walls of a medieval castle and a firewall to a drawbridge controlling access to the castle has evolved.

Today, even the smallest of networks typically have two drawbridges, uh, firewalls to provide fault tolerance should one of the firewalls fail.

Different departments or lines of business may be segmented on the network, minimally requiring different firewall rules and possibly more firewalls — add a drawbridge to the separate halls of the castle.

Larger networks may span multiple, geographically dispersed public, private, and hybrid data centers requiring still more firewalls — add drawbridges throughout the realm and in the clouds (to keep the dragons out, of course)!

Finally, advanced security concepts such as micro-segmentation in virtualized data centers require firewalls on individual workloads — put a drawbridge on every stone in the castle!

And, of course, whether it's 2 or 2,000 firewalls, somehow the king only sees fit to hire a handful of knights in shining armor to manage all those firewalls! Unfortunately, with so many firewalls to manage, you don't have time to properly maintain those firewalls, investigate policy violations, or create a more effective security strategy — let alone shine your armor!

Attempting to effectively and efficiently manage multiple, independent firewalls, rule bases, and security policies is an unwieldy task that puts organizations at risk. In addition to needless complexity, potential technical and security issues include the following:

- Unnecessary or outdated rules that allow vulnerable ports, services, and applications
- Overly permissive rules (for example, ANY-ANY or ALLOW ALL rules) that are hastily configured to deploy a new application, because of insufficient time to properly research, test, and narrowly define the appropriate permissions
- Conflicting rules that cause poor performance, prevent applications from working correctly, and/or create vulnerabilities
- Undocumented or unknown rules leading to application or network downtime (when they're removed) and audit discrepancies

- Poor performance caused by rule bases that are not optimally configured (for example, the most commonly matched rules are near the bottom of the policy, but rules are processed by the firewall from the top down)
- Unused or improperly configured VPN tunnels that cause lost productivity for remote workers and IT staff

To Err Is Human, But Cybercriminals Aren't Divine

As enterprise networks become increasingly complex and independently managed firewall rule bases continue to grow in number and size, human error becomes a greater factor to consider in network security management, as the following data suggests:

- According to *Firewall Configuration Errors Revisited,* by Avishai Wool, Tel Aviv University research found that among the most complex firewalls, at least 20 errors were detected in 75 percent of the configurations.
- The same Tel Aviv University research found that 80 percent of firewalls examined in breach investigations are misconfigured and aren't properly blocking traffic.
- Infonetics Research found that 25 percent of all network outages are caused by human error.
- Gartner has predicted that through 2018, more than 95 percent of firewall breaches will be caused by firewall misconfigurations.

Complex security deployments are difficult to configure and manage, creating numerous opportunities for cybercriminals to exploit human errors in enterprise networks. In addition to being time-consuming and costly, manual and repetitive security configuration and management tasks introduce additional risks to the organization due to human errors in critical network security deployments.

If a Tree Falls and No One Is Around, Your Data Will Get Stolen

Sophisticated threats are too often hidden in mountains of security data and can go undiscovered for extended periods of time, increasing your risk profile and exposure to breaches and data loss.

As a result of this deluge of data, many network and security administrators can't see the forest for the trees. But if a tree falls and no one is around, cybercriminals will steal your organization's sensitive and valuable data, and CNN or *The Wall Street Journal* will make a sound and millions will hear it!

Most security deployments focus on threat identification and remediation, and generate an enormous amount of threat data without correlating information. As a result, critical threats are often buried in the noise, and network and security teams are overloaded with the task of finding the critical threats among the hundreds of thousands or possibly millions of less critical or insignificant events and alerts — the proverbial needle in the haystack.

The problem isn't a lack of data — it's a lack of actionable intelligence. Network and security teams have all the raw data they need, but they don't have enough resources — time, money, knowledge, and caffeine — to sift through and analyze the data.

The right network security management solution provides actionable intelligence in a coherent, visual, and interactive format that enables a rapid, effective response to new and emerging threats.

REMEMBER

Network breaches and vulnerabilities don't go undiscovered due to a lack of data. Enterprise network and security teams are overwhelmed by raw data that lacks correlation and central visibility and is, therefore, not actionable.

Chapter 5

Knowing What to Look for in a Network Security Management Solution

In This Chapter

- Consolidating security deployments and rule bases
- Simplifying and automating network security operations
- Keeping network security devices organized
- Correlating indicators of compromise and making data actionable

The centralized features in a network security management platform can minimize the administrative efforts and operational costs associated with your security deployments in multiple locations — whether internal or global.

In this chapter, you learn how a network security management platform empowers you with consolidated, simplified policy creation and management, solving the complexity of security deployments with intuitive and enterprise-class functionality, efficient rule bases, and actionable threat visibility and intelligence.

Streamlined Policy Management

Complexity is a reality in today's network security environment. With numerous, independently managed security deployments — such as firewalls, IPSs, URL filtering, endpoint protection, and more — network and security administrators frequently end up with an unmanageable amount of devices, interfaces, security rule bases, configuration elements, and raw data on their networks. With multiple-point security solutions come multiple, frequently outdated, inconsistent, and improperly configured security policies and rules, which expose your organization to increased risk.

Consolidating multiple security deployments is an important first step toward eliminating a network security management nightmare. For example, you may be able to combine several security technologies into a single solution such as a next-generation firewall that offers IPSs, URL filtering, sandboxing, and more.

The next step is to centralize and streamline policy management with a network security management platform. Even in relatively small networks — with perhaps as few as three firewalls — security policies can easily be improperly configured or maintained, and quickly become dangerously outdated and inconsistent.

A network security management platform can help you streamline policy management in your organization with features such as a

- **Single security rule base** that enables you to manage one set of security policies for all your URL filtering, threat prevention, and content filtering deployments
- **Policy browser** that allows you to quickly create policies that include application-, user-, and traffic-specific threat prevention (such as IPSs, antivirus, anti-spyware, and so forth), eliminating the duplicate data entry common in other security product offerings
- **Tag browser** that allows you to "tag" rules with common names (for example, "DMZ," "perimeter," or "data center"), so you can easily search and manage those rules as needed

Simplified Operations

Common network security operations include setting up networks and device configurations, managing security policies and firewall rules, monitoring network traffic for real-time threats, and analyzing and correlating threat data to effect an appropriate and prompt response, when necessary (see Chapter 1).

Without a network security management platform, every firewall and security deployment on your network must be manually configured and individually managed, because each has its own policies and rule bases.

A network security management platform can simplify your security operations, saving you valuable time and reducing costly mistakes that put your organization at greater risk, by providing the necessary capabilities to automate and optimize many common network security configuration and management processes. Powerful tools to look for in a network security management platform include the following:

- **Template stacks** that let you create and reuse templates during device and network configuration, reducing manual tasks (see Figure 5-1)

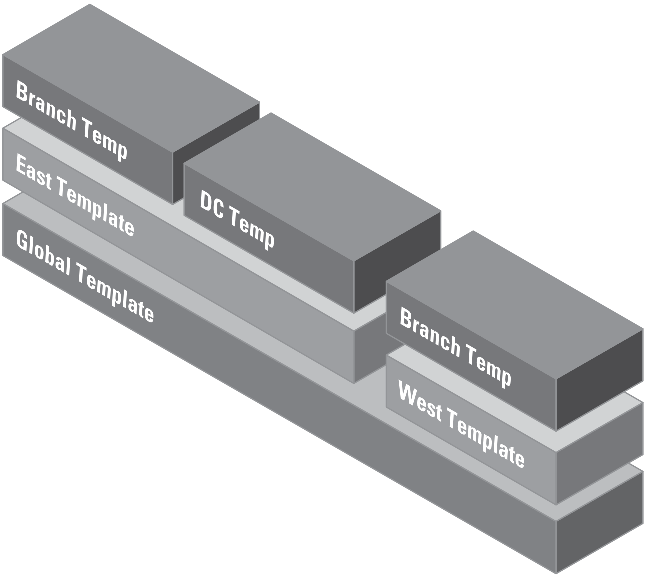

Figure 5-1: Template stacks let you create and reuse standard configurations throughout your network.

- **Global search capabilities** that enable you to search an entire configuration for a particular string, such as an IP address, object name, policy name, threat ID, or application name, helping you avoid the duplication of rules and configuration elements
- **Firewall configuration imports** that allow you to import existing or preproduction firewalls into your network configuration with the click of a button
- **Commit queuing,** which allows you to apply configuration and rule-base changes done by multiple administrators in an orderly fashion, without conflict, and without wasting anyone's time by having to try to recommit every 15 minutes

Intuitive Network and Device Management

A key requirement of a good network security management solution is that it must be simple to understand and use! A familiar user interface (UI) that is very similar or identical to your existing firewall UIs is a great starting point. This will ease the transition from individually managed devices to a centralized network security management solution for your network and security administrators.

The UI should be visual, interactive, customizable, and automated (see Chapter 6). Important capabilities include the following:

- **Device group hierarchies** allow you to create nested device groups in a tree hierarchy, with lower-level groups inheriting the settings of higher-level groups. This enables you to organize devices based on function and location, without redundant configuration (see Figure 5-2).
- **Management access segmentation** lets you associate access domains with administrator roles to enforce information separation among the functional or regional areas of your organization. Role-based administration is used to delegate feature-level administrative access

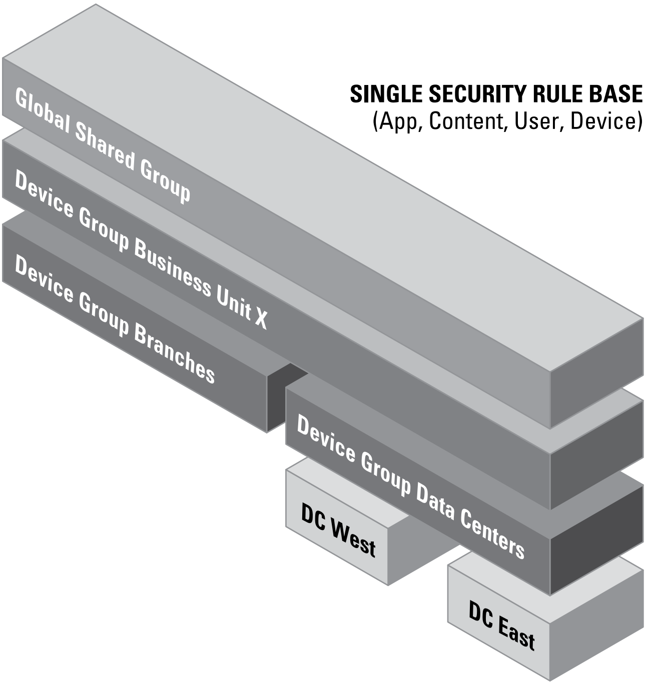
SINGLE SECURITY RULE BASE
(App, Content, User, Device)
Global Shared Group
Device Group Business Unit X
Device Group Branches
Device Group Data Centers
DC West
DC East

Figure 5-2: Device group hierarchies allow you to mirror your configuration to your organizational structure.

to firewalls and the network security management platform, including availability of data (enabled, read-only, or disabled and hidden from view) to different members of your staff. Specific individuals can be given appropriate access to the tasks that are pertinent to their job, including access to the dashboard and reporting to give administrators more focus and context, while making other access either hidden or read-only (see Figure 5-3).

- **Flexible deployment options** allow you to support on-premises deployments, as well as public, private, and hybrid cloud environments that scale easily from as few as two or three to several thousand security deployments as your organization grows.

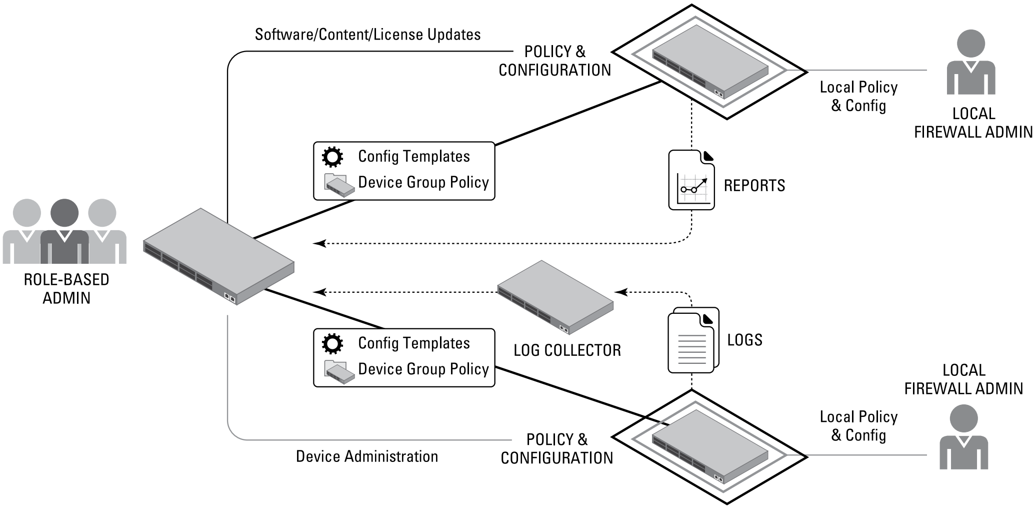

Figure 5-3: Role-based administration enables granular permissions for local visibility and control, as appropriate.

Network-wide Visibility, Logging, and Reporting

The current state of threat intelligence is a perpetual cycle of adding more and more detection-focused data, inundating security teams with logs and alerts and clogging an organization's ability to quickly respond to the most critical attacks. We're entering a new era where identifying unique, targeted attacks requires prioritizing threat intelligence and making it actionable, instead of simply adding more of it.

Another benefit of deploying network security management is the ability to see into all parts of the network (including on-premises and off-premises infrastructure, endpoints, and public and private cloud environments, among others) from one central location. Most network security management solutions offer this capability, but with major differences in the way the data is displayed to the administrator. It's not really about data visibility — it's about making the data actionable, interactive, and valuable to the user.

A good network security management solution prioritizes security data, displays critical data in a visual and intuitive interface, and facilitates fast, effective responses to any threat encountered on the network. It automatically correlates IOCs based on logs across your entire network, no matter how hidden, and highlights compromised hosts for fast resolution.

Network security management on the high seas with MSC Cruises

Customer profile

Every year, MSC Cruises (www.msccruisesusa.com) takes more than 1.5 million travelers on cruises to beautiful holiday spots around the world. In the complex and demanding cruise sector, the company must take advantage of every potential market differentiator. This includes providing reliable, fast, and secure Internet access to guests onboard its ships.

Challenges

When carrying guests to exotic locations, MSC Cruises wants nothing

(continued)

(continued)

less than smooth sailing. Its goal for the performance of its network is the same. Bandwidth availability issues hindered high-quality service to MSC Cruises' travelers and occasionally impacted communications.

MSC Cruises also recognized the need to upgrade network security and keep traffic free from harm. "It's really important to secure end-to-end network communications from ships to headquarters and offices," says Salvatore Russo, IT Fleet Supervisor, MSC Cruises Technical Department. "We wanted layer 7 security, the visibility to see malware, application ID, and to define policies to control users, content, and applications. At the time, we also didn't have the tools to see into the network to gather information and take steps to make ourselves safer."

MSC Cruises strives for the highest levels of service and security at all times. It felt that its previous infrastructure could no longer deliver what the company needed. "We had proxy servers, and all the IT infrastructure was managed manually," says Russo. "It was cumbersome and resource hungry to manage everything. When we signed a new SLA for bandwidth service with our provider, the time was right to look for a new IT environment that offered more throughput, bandwidth optimization capabilities, and better security and efficiencies."

Solution

MSC Cruises began looking at security solutions. "Performance, comprehensive capabilities, throughput, bandwidth control, price, and the cost of deployment were key factors," says Russo.

MSC Cruises purchased 24 Palo Alto Networks next-generation firewalls, which were deployed in high-availability configurations on its cruise ships. Two additional next-generation firewalls were installed at the firm's data center. "The firewalls are connected to the Internet through a couple of multi-beam satellite networks," says Russo. "The network provides broadband Internet access for passengers and crew, VoIP, and backs up our core information systems."

MSC Cruises deployed Panorama to provide centralized management and logging capabilities in order to easily manage all its security platforms from one location and interface, and quickly deploy uniform policies to all devices.

The enterprise security platform from Palo Alto Networks enabled MSC Cruises to achieve all its objectives related to bandwidth optimization, security, IT management, and connectivity for guests and crew. "Thanks to Palo Alto Networks, we control traffic flow and optimize bandwidth for crew and guests to meet their needs very effectively," says Russo. MSC Cruises now enjoys security at layer 7 and newfound visibility into its network. "We can see applications, users, malware — everything," says Russo.

"The visibility, and Panorama's collection of all data logs from all devices in one central location, lets us see and monitor everything happening on the network. We have full control of all devices, traffic, bandwidth, and access — at sea and onshore."

Palo Alto Networks solutions are also helping to reduce IT administration headaches for MSC Cruises. "Everything is easy to use and saves time. With just one click on Panorama, we can update all our devices wherever they are," says Russo.

Chapter 6

Managing Security with Actionable Intelligence

In This Chapter

- Knowing what to look for in a network security management dashboard
- Keeping track of security data with logging and monitoring

"Action is the real measure of intelligence."

Though Napoleon Hill wrote these words in the context of personal improvement, they are no less germane to cybersecurity. Intelligent collection, organization, mining, prioritization, and display of network and threat data enables fast, informed, and effective action to prevent cyberattacks from succeeding against an enterprise network.

In this chapter, you learn how a centralized network security management solution can provide deep visibility and actionable intelligence across your entire network.

The Power to Act at Your Fingertips

Having actionable, well-organized information about network traffic and threats at your fingertips is more crucial today than ever before. IT and security organizations are inundated with unmanageable and uncorrelated amounts of threat and vulnerability data from multiple, independent security deployments, making it practically impossible to find critical threats that are too often buried in mountains of raw data.

Frequently, it's not a lack of data that leads to a data breach, but a lack of appropriately prioritized, actionable information. IT and security teams have to manage too many data sources and don't have the time or the resources to pinpoint threats in the network. They're simply too overwhelmed to find the needle in the haystack and, as a result, can't quickly identify threats and prioritize responses appropriately.

A centralized network security management solution can provide comprehensive visibility into network activity, application usage, users, and threats. In order for a centralized network security management solution to provide actionable intelligence, it must have an intuitive dashboard that is

- **Visual:** A visual interface is critical because the overwhelming amounts of data in today's cybersecurity space are just too confusing. Being able to provide visuals that make the navigation and control of information easier are crucial to deliver a valuable and actionable interface for network and security administrators.
- **Customizable:** Every network and security administrator has different needs. Thus, the user interface in a network security management solution must be easily customizable for individual administrators, for example, with predesigned widgets that can be selected from a drop-down list to customize existing tabs on the dashboard.

  Another powerful capability to look for in a network security management solution is the ability to create new custom tabs, for example, to monitor certain employee activity, troubleshoot new application deployments, remediate security events, or track application usage.
- **Interactive:** When you're searching for answers, you need them fast. This is where an interactive dashboard can help tremendously, enabling you to find answers fast by drilling into greater details from any part of the user interface.
- **Automated:** Automation is critical in today's security environment. Automation eliminates duplication of work, cuts back on manual research, and reduces human error and oversight.

An automated correlation engine is an analytics tool that can verify compromised hosts in your network and cut back on manual data mining requirements within your organization. It scrutinizes isolated events automatically across multiple logs, queries the data for specific patterns, and correlates network events to identify compromised hosts. Correlation objects trigger correlation events when they match on traffic patterns and network artifacts that indicate a compromised host on your network.

Spotlighting network security management at OSRAM

Customer profile

From basic light bulbs to specialized light-emitting diodes (LEDs), OSRAM (`www.osram.com`) has been the world's foremost maker of lighting products for more than a century. As the company has grown, so, too, has its number of offices and locations worldwide, and the network that connects them.

Challenges

As it evolved, OSRAM's network became extremely complex and highly decentralized, efficiencies declined and IT struggled to maintain the level of security and responsiveness that the business required.

OSRAM's decentralized network was cumbersome to maintain, costly, and made it difficult for IT to respond quickly to the needs of the business. "Our network was highly decentralized with different rules for access at [remote branch] sites," says Steffen Siguda, Corporate InfoSec Officer and Data Protection Officer for OSRAM.

With thousands of users distributed across numerous sites worldwide, fulfilling business requests was time-consuming and inefficient. "We use a lot of customized applications and get lots of requests for tweaks to policies to accommodate production," says Siguda. "It took half a day of work to accommodate changes because we had to do global configuration changes manually for 78 proxy servers. At one point, we had over 1,000 lines of configuration in our previous firewall solution."

The lack of visibility across the entire network was also a significant challenge and detracted from security. "We had no global view or monitoring of security," says Siguda. "If something went wrong in India, China, or Brazil, it was impossible to search the log of every proxy server to identify the problem. We couldn't get a consolidated view to address

(continued)

(continued)

a threat or infection. We needed visibility and a global view of devices to improve security and make uniform changes, and better protect our intellectual property (IP) and business."

Solution

Siguda and his team spent just two hours setting up their first Palo Alto Networks next-generation firewall. "We let it run for two weeks, and it gave us a great overview of our apps, systems, and users," says Islam Masoud, Security Operations Manager for OSRAM. "Plus, our 1,000 lines of configurations instantly went down to just 75 rules."

Within weeks, OSRAM replaced the legacy firewalls at its main data center. Next, OSRAM swapped out its three main firewalls, and then replaced all 78 of its proxy servers with 56 Palo Alto Networks next-generation firewalls.

OSRAM added Panorama from Palo Alto Networks to efficiently and centrally manage all its firewalls and policies. Panorama, running as a VMware virtual machine, provides centralized management and logging capabilities for OSRAM to easily manage all its security platforms from one location and interface, and quickly deploy uniform polices to all devices.

The deployment of the Palo Alto Networks solution was seamless. "We took out the box, set up an IP, hit a button, clicked, and told the person at each local site around the world to remove the cables and proxy servers. No local tweaks were required because the configuration is done globally, and distributed through Panorama. We just clicked and synchronized everything," says Siguda.

Results

IT at OSRAM is now far more responsive. "It used to take half a day to accommodate changes," says Masoud. "Now, users can request access to things on their own and get an instant, automatic reply based on our rules, instead of [our] having to look at each one and decide.

"The app awareness of Palo Alto Networks allows us to shrink our rule sets considerably, and gives us information we can read and use. Previously, we couldn't make anything out of our logs. Now it's so easy: We just click, look, and understand. It's like going from zero to 100 kilometers per hour in seconds," says Masoud.

The granular network visibility of Palo Alto Networks firewalls, and their extensive reporting capabilities, have also elevated OSRAM's security posture. "Our previous proxy servers had poor visibility, so it took forever to find the source of a botnet or some other infection," says Masoud. "Now, we can identify and monitor stuff globally at all our sites that we just couldn't see before . . . all in one quick view."

"Palo Alto Networks has reduced the noise in our logs by 95 percent. It's removed the fog so we can clearly see what's really going on in our network," says Siguda.

Panorama is also shedding light into traffic and network activity, and enhancing security. "We can view global traffic and activities and change and issue rules right away," says Masoud. "If there's a malware attempt, in one click I can address the target IP and distribute the security solution to everyone all over the world. This wasn't easy in the past with a decentralized network; by the time we got to the malware it would be all over the place. With Panorama, we can apply rules and fixes to every device in seconds."

"Before we were blind to some things, but now we've raised overall security without expending more resources," says Siguda. "I tell my peers in IT that Palo Alto Networks is 'simplicity within complexity.'"

Logging and Reporting

Logging is a critical component in any security network. Being able to log all network activity in a way that is logical, organized, and easily segmented makes logging very valuable.

In addition, logs can be kept for individual firewalls, entire networks of firewalls, or any subset of a network. For large networks, dedicated log collectors can be deployed to increase the log storage capacity and simplify network design.

Reporting has to be user friendly, intuitive, and easy to share. Network administrators have to be able to create custom reports for network and cloud applications based on their needs, and schedule, download, and share them with ease.

The number of SaaS applications is growing tremendously, so clear visibility into sanctioned and unsanctioned applications is critical to provide effective security. A good network security management solution provides full insight into what types of SaaS applications employees are using, as well as where data is being used.

With today's distributed environments, it becomes increasingly important to have central visibility into all network and threat activity. Being able to see traffic across an entire network of firewalls from one central location provides convenience, time savings, and efficiency. It also provides added security because data from several firewalls can be correlated to detect indicators of compromise and confirm compromised hosts in the network.

Chapter 7

Ten Important Criteria for Evaluating Network Security Management Solutions

Here are ten capabilities and features to look for in a network security management solution:

- **Centralized management with customized and localized control of individual firewalls and dynamic updates:** The ability to efficiently manage all your firewalls with a master rule base is of paramount importance. Likewise, the ability to rapidly deploy dynamic security updates to stay ahead of the ever-changing threat landscape is critical. Finally, the flexibility to accommodate regional or local security policy requirements or exceptions is also an important capability to look for in a network security management solution.
- **Streamlined enterprise class management in complex environments:** Organizing firewalls based on function and location into hierarchical device groups, with lower-level groups inheriting the settings of higher-level groups, greatly simplifies network security management.
- **Automated configuration processes:** The ability to create, reuse, and stack templates enables efficient network and device configuration across the enterprise, eliminating many redundant and manual configuration tasks and greatly reducing the risk of human error. In addition, the ability to commit changes to any configuration in series (commit queuing) without conflicts is crucial for a smooth management process.

- **Consolidation of network security functions in a single rule base:** The ability to secure your network with a single security rule base for all firewall, threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking, and data filtering security functions helps to eliminate manual duplication of effort, ensure all security policies are up to date, and reduce threat exposure.
- **Deployment flexibility and scaling:** Look for a network security management solution with flexible deployment options in a variety of physical and virtual form factors, capable of easily scaling to support a few to hundreds of physical and virtual firewalls deployed in geographically dispersed data centers in public, private, and hybrid cloud environments.
- **Full enterprise visibility:** The ability to see into all parts of the network from one central location is an important capability, as are customizable dashboards, easy drill-down access to security information, and providing the right level of visibility into network traffic and threats for local administrators.
- **Actionable reporting:** Most network security management solutions provide reporting capabilities, but with major differences in the way the data is displayed. It's not only about data visibility — it's about making the data actionable, interactive, and valuable to the user with prioritized data that visually displays critical events and facilitates fast responses to threats. The ability to report on company sanctioned and unsanctioned SaaS application usage is quickly becoming crucial in today's business environment.
- **Automated correlation of IOCs:** How much time are you spending on manual data mining and analysis looking for the proverbial the "needle in a haystack"? A good network security management solution can automatically correlate IOCs — no matter how well hidden — across your entire firewall infrastructure and identify compromised hosts for fast resolution.
- **Familiar, intuitive, and full-featured user interface (UI):** To make the transition from individually managed devices to a centralized network security management solution as smooth as possible, look for a UI that is very similar or identical to the UI of your existing individual firewalls. Administrators should also be able to perform all their firewall management functions from the network

security management solution, instead of having to go back and forth to individual firewall UIs to perform "one-off" configuration tasks.

- **Role-based administration:** Role-based administration is used to delegate feature-level administrative access, including availability of data (for example, enabled, read-only, or disabled and hidden from view) to different members of your team. Specific individuals can be given appropriate access to the tasks that are pertinent to their job while making other access either hidden or read-only.

TIP

A general rule of thumb is to deploy a network security management solution if you already manage or are planning to deploy three or more firewalls in your network.

Should you move to network security management?

Answer the following questions, add up your points, then turn the page upside down to see your results (not really, the results are at the end of the questionnaire!).

1. **How many firewalls do you currently have deployed?**

   a. None (0 points)

   b. 1 to 2 (1 point)

   c. 3 to 5 (5 points)

   d. 5 to 25 (10 points)

   e. More than 25 (15 points)

2. **How many additional firewalls do you plan to deploy in the next two years?**

   a. None (0 points)

   b. Up to 2 (2 points)

   c. 3 to 5 (10 points)

   d. 6 or more (15 points)

(continued)

(continued)

3. **How are your firewalls configured?**

   a. I only have one firewall. (0 points)

   b. They are all identically configured. (2 points)

   c. There are slight variations in their configurations. (3 points)

   d. They're snowflakes — every firewall is unique. (5 points)

4. **How do you feel about the time spent configuring/managing your firewalls?**

   a. It's not very time-consuming. (0 points)

   b. It's time consuming, but I don't have anything better to do. (2 points)

   c. I'm wasting a lot of time. (5 points)

   d. It keeps several admins busy — call it job security. (15 points)

5. **How much manual involvement and duplication of work do you have in network and device configurations?**

   a. I'm in control and everything is fine, keep moving, nothing to see here. (0 points)

   b There is some duplication and duplication, but I manage to manage. (5 points)

   c. There are many errors, but Oscar Wilde wrote "Experience is the name everyone gives to their mistakes" so I'm getting a lot of experience. (10 points)

   d. It's completely out of control — don't tell my boss! (15 points)

6. **Which one of these statements rings true regarding your security rule base?**

   a. My rule bases is current and secure. (1 point)

   b. Most security rules should probably be pretty correct (fingers crossed). (3 points)

   c. I'm frequently correcting errors (that other admins make). (10 points)

   d. There are more holes than Swiss cheese in a shooting gallery. (15 points)

7. **Do you have central threat and traffic visibility across your network?**

   a. Visibility is overrated — let's go flying! (0 points)

   b. It requires multiple UIs, but it makes me look busy and really smart. (5 points)

   c. I'm overwhelmed — I need eyes in the back of my head. (15 points)

Results

Tally up your points and see where you come out:

- **0 to 15 points:** You're a Zen master! And you're managing fine without a network security management solution, but it's worth considering an investment in a network security management solution as your organization grows. It could save you time and effort configuring and managing your firewalls in the future.
- **16 to 30 points:** You might need to explore your options. Either you're already at the point where a network security management solution will pay for itself, or you'll be there shortly. Now is the time to make the leap into network security management.
- **31 to 60 points:** You're a glutton for punishment. You'd be pleasantly surprised by the amount of time you'd save and how much more efficient you'd be with a network security management solution. You'd love the benefits of a network security management solution.
- **61 to 90 points:** Wow! You should pick up the phone today and meet with your security vendor to talk about getting a network security management solution — or make an appointment with your cardiologist.

Glossary

adware: Pop-up advertising programs that are commonly installed with freeware or shareware.

Ammyy: A remote access application that has been commonly exploited by attackers in *vishing* (voice phishing) attacks.

anti-AV software: Malware that disables any legitimately installed antivirus software on a compromised endpoint, thereby preventing automatic detection and removal of malware that is subsequently installed by the attacker. Many anti-AV programs work by infecting the master boot record (MBR) of a target endpoint.

Application Usage and Threat Report (AUTR): Security research prepared by the Palo Alto Networks threat intelligence team, Unit 42. It examines global trends across the threat landscape and application usage. The report is available for free download at `www.paloaltonetworks.com`.

AUTR: *See* Application Usage and Threat Report.

backdoor: Malware that enables an attacker to bypass normal authentication procedures in order to gain access to a compromised system. It's often installed as a failover, in case other malware is detected and removed from the system.

bootkit: A kernel-mode variant of a rootkit, commonly used to attack computers that are protected by full-disk encryption.

bot: An individual endpoint that has been infected with malware.

botnet: A network of bots working together and controlled by an attacker through command-and-control (CnC) servers.

Box: A cloud-based file sharing and content management service.

bring your own application (BYOA): A popular trend related to BYOD (albeit, less well known) and consumerization in which employees are permitted to use personal applications in the workplace for work-related and personal business.

bring your own device (BYOD): A popular trend in which employees are permitted to use their personal mobile devices, such as smartphones and tablets, in the workplace for work-related and personal business.

BYOA: *See* bring your own application.

BYOD: *See* bring your own device.

community cloud: A cloud computing deployment model that consists of a cloud infrastructure that is used exclusively by a specific group of organizations.

consumerization: A process that occurs as users increasingly find personal technology and applications that are more powerful or capable, more convenient, less expensive, quicker to install, and easier to use than corporate IT solutions.

CRM: *See* customer relationship management.

customer relationship management (CRM): Software used to manage and analyze customer interactions and data throughout the customer life cycle.

data loss prevention (DLP): A security tool that is used to detect and prevent certain data, defined by policy, from being copied or sent outside of an organization. For example, a DLP solution might disable USB drives on user endpoints and block (or encrypt) certain data that matches a pattern (such as a credit card or Social Security number) from being sent via email.

DDoS: *See* distributed denial-of-service.

demilitarized zone (DMZ): A physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger, untrusted network, such as the Internet.

distributed denial-of-service (DDoS): A type of attack in which numerous compromised systems, often numbering hundreds of thousands or millions, are used to flood a single system or network with traffic, causing the target to crash or otherwise be rendered unusable.

DLP: *See* data loss prevention.

DMZ: *See* demilitarized zone.

Dropbox: A cloud-based file hosting service that offers cloud storage, file synchronization, personal cloud, and client software.

enterprise resource planning (ERP): Business process management software that uses a system of integrated applications to manage a business and automate various back office functions such as finance, human resources, and inventory control.

ERP: *See* enterprise resource planning.

Exploit: Software or code that takes advantage of a vulnerability in an operating system or application, and causes unintended behavior in the operating system or application, such as privilege escalation, remote control, or a denial-of-service.

Facebook: A free social networking website and application that enables members to create profiles, upload and share content, communicate with other members, and play games, among other things.

File Transfer Protocol (FTP): A standard network protocol used to transfer computer files from one host to another over TCP ports 20 and 21.

Financial Industry Regulatory Authority (FINRA): An independent not-for-profit organization responsible for ensuring that the U.S. securities industry operates fairly and honestly.

FINRA: *See* Financial Industry Regulatory Authority.

FTP: *See* File Transfer Protocol.

Gmail: A free web-based email service provided by Google.

Google Docs: An online word processor created by Google.

Health Insurance Portability and Accountability Act (HIPAA): U.S. legislation passed in 1996 that, among other things, protects the confidentiality and privacy of PHI.

HIPAA: *See* Health Insurance Portability and Accountability Act.

hybrid cloud: A cloud computing deployment model that is composed of public, private, and/or hybrid cloud infrastructures.

IaaS: *See* Infrastructure as a Service.

IDS: *See* intrusion detection system.

IMAP: *See* Internet Message Access Protocol.

indicator of compromise (IOC): An artifact, such as a malware signature, suspicious URL, or command-and-control (CnC) traffic, that provides strong evidence of a cyberattack.

Infrastructure as a Service (IaaS): A category of cloud computing services in which the customer manages operating systems, applications, compute, storage, and networking, but the underlying physical cloud infrastructure is maintained by the service provider.

Internet Message Access Protocol (IMAP): A standard client–server protocol for accessing email. IMAP version 4 is the current version and uses TCP port 143 by default.

intrusion detection system (IDS): A hardware or software application that detects and logs suspected network or host intrusions.

intrusion prevention system (IPS): A hardware or software application that both detects and blocks suspected network or host intrusions.

IOC: *See* indicator of compromise.

IPS: *See* intrusion prevention system.

LinkedIn: A business-oriented social networking service.

logic bomb: A program, or portion thereof, designed to perform some malicious function when a predetermined circumstance occurs.

LogMeIn: A SaaS- and cloud-based remote connectivity service for collaboration, IT management, and customer engagement.

malware: Malicious software or code that typically damages or disables, takes control of, or steals information from a computer system. Malware broadly includes adware, anti-AV software, backdoors, bootkits, bots and botnets, logic bombs, RATs, rootkits, spyware, Trojan horses, viruses, and worms.

master boot record (MBR): A special type of boot sector at the very beginning of partitioned computer hard drives that contains information about how partitions and files systems are organized on the storage media.

MBR: *See* master boot record.

Microsoft Office 365: A SaaS-based offering of Microsoft Office applications, including Word, Excel, PowerPoint, OneNote, Lync web conferencing, and Exchange Online, among others.

Microsoft SharePoint: A browser-based collaboration and document management platform.

National Institute of Standards and Technology (NIST): The U.S. federal agency that is responsible for working with industry to develop and apply technology, measurements, and standards.

NIST: *See* National Institute of Standards and Technology.

Outlook.com: A free web-based email service (formerly known as Hotmail) provided by Microsoft.

PaaS: *See* Platform as a Service.

Platform as a Service (PaaS): A category of cloud computing services in which the customer is provided access to a platform for deploying applications and can manage limited configuration settings, but the operating system, compute, storage, networking, and underlying physical cloud infrastructure are maintained by the service provider.

Payment Card Industry Data Security Standard (PCI DSS): A proprietary information security standard mandated for organizations that handle American Express, Discover, JCB, MasterCard, or Visa payment cards.

PCI DSS: *See* Payment Card Industry Data Security Standard.

personally identifiable information (PII): Any personal data that can potentially be used to identify a specific individual, such as full name, home address, date of birth, birthplace, Social Security number, passport number, driver's license number, and telephone number, among others, as well as email address and IP address (in some cases).

petabyte: A measure of memory or storage capacity equivalent to 1,024 terabytes (TB) or a million gigabytes.

PHI: *See* protected health information (PHI).

PII: *See* personally identifiable information.

point-of-sale (POS): A retail system typically composed of a computer, monitor, barcode scanner, credit/debit card reader, cash drawer, and receipt printer.

POP: *See* Post Office Protocol.

POS: *See* point-of-sale.

Post Office Protocol (POP): A standard client–server protocol for receiving email. POP version 3 is the current version; it uses TCP port 110 by default.

private cloud: A cloud computing deployment model that consists of a cloud infrastructure that is used exclusively by a single organization.

protected health information (PHI): Any information about health status, healthcare, or healthcare payments that can be associated with a specific, identifiable individual.

public cloud: A cloud computing deployment model that consists of a cloud infrastructure that is open to use by the general public.

RAT: *See* remote access Trojan.

RDP: *See* Remote Desktop Protocol.

remote access Trojan (RAT): A malware program that includes a backdoor to provide administrative control of a target computer.

Remote Desktop Protocol (RDP): A proprietary Microsoft protocol that provides remote access to a computer. RDP uses TCP port 3389 and UDP port 3389 by default.

rootkit: Malware that provides privileged (root-level) access to a computer.

SaaS: *See* Software as a Service.

Salesforce: A cloud-based CRM.

Secure Sockets Layer/Transport Layer Security (SSL/TLS): A transport layer protocol that provides session-based encryption and authentication for secure communication between clients and servers on the Internet.

service-level agreement (SLA): A contract between a service provider and its customers (internal or external) that formally defines the service that is being provided and specific service requirements such as performance, problem management, responsiveness, and availability. The SLA also typically includes penalties for noncompliance, such as credits or refunds.

Simple Mail Transfer Protocol (SMTP): A standard protocol for transmitting email. SMTP uses TCP port 25 by default.

Skype: An application that allows users to make phone calls over the Internet. Additional features include instant messaging, file transfer, and videoconferencing.

SLA: *See* service-level agreement.

SMTP: *See* Simple Mail Transfer Protocol.

Software as a Service (SaaS): A category of cloud computing services in which the customer is provided access to a hosted application that is maintained by the service provider.

spyware: Software that gathers information about a person or organization without his or her knowledge or consent.

SSL/TLS: *See* Secure Sockets Layer/Transport Layer Security.

SugarCRM: An open-source, cloud-based CRM.

TCP: *See* Transmission Control Protocol.

TeamViewer: TeamViewer provides remote control of PCs over the Internet, allowing a user to instantly take control over a computer anywhere on the Internet (even through firewalls).

Tor: A system that enables users to communicate anonymously over the Internet.

Transmission Control Protocol (TCP): A connection-oriented protocol responsible for establishing a connection between two hosts and guaranteeing the delivery of data and packets in the correct order.

Trojan horse: A program that purports to perform a given function, but which actually performs some other (usually malicious) function.

Twitter: An online social network service that enables users to send and read short messages known as tweets.

UDP: *See* User Datagram Protocol.

UltraSurf: UltraSurf implements a proxy with complete transparency and a high level of encryption that enables users to browse any website freely. It is used heavily in countries with Internet censorship.

Uniform Resource Locator (URL): Commonly known as a web address. The unique identifier for any resource connected to the web.

URL: *See* Uniform Resource Locator.

User Datagram Protocol (UDP): A connectionless-oriented protocol often used for time-sensitive, low-latency communications that don't require guaranteed delivery.

Vidyo: A videoconferencing software platform.

virtual private network (VPN): An encrypted tunnel that extends a private network over a public network (such as the Internet).

virus: A set of computer instructions whose purpose is to embed itself within another computer program in order to replicate itself.

vishing (voice phishing): A social engineering technique in which the attacker calls the intended victim and attempts to trick him or her into revealing private information.

voice phishing: *See* vishing.

Voice over Internet Protocol (VoIP): Technology that enables voice communications over IP.

VoIP: *See* Voice over Internet Protocol.

VPN: *See* virtual private network.

vulnerability: A bug or flaw in software that creates a security risk that may be exploited by an attacker.

worm: Malware that usually has the capability to replicate itself from computer to computer without the need for human interaction.

Yahoo! Mail: A free web-based email service provided by Yahoo!.

YouTube: A video sharing website.

Take back control and regain visibility on your network!

Myriad security deployments, disparate user interfaces, and complex and outdated policies make effective network security a real challenge today. Network security management enables streamlined policy creation and management, centralized firewall configuration and administration, and actionable insights into threats across your network.

- ***Control firewall and device sprawl* — deploy next-generation firewalls and network security management to reduce management complexity on your network**
- ***Close operational gaps* — between alert and action, known and unknown threats, and the idea of security and implementation**
- ***Streamline policy management* — eliminate multiple, independently managed rule bases with a single, consolidated rule base**
- ***Find the needle in the haystack* — use network security management to make sense of the mountains of network traffic and threat data**

Open the book and find:

- **How to streamline policy management**
- **How to automate repetitive configuration tasks**
- **How to reduce response times**
- **How to discover unknown threats in your network**
- **What you need in a network security management solution**

Go to Dummies.com®
for more!

Lawrence C. Miller has worked in information security in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 75 other *For Dummies* books on numerous technology and security topics.

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-119-28399-7
Book not for resale