Making Everything Easier!™

Blue Coat Special Edition

Encrypted Traffic Management

FOR DUMMIES®

A Wiley Brand

Learn to:

- Uncover hidden threats within SSL-encrypted traffic
- Control SSL to maintain data security and user privacy
- Deploy high-performance SSL visibility appliances

Brought to you by

BLUE COAT®

Steve Piper, CISSP

About Blue Coat

Blue Coat empowers enterprises to safely and securely choose the best applications, services, devices, data sources, and content the world has to offer, so they can create, communicate, collaborate, innovate, execute, compete and win in their markets. Blue Coat has a long history of protecting organizations, their data, and their employees and is the trusted brand to 15,000 customers worldwide, including 78 percent of the Fortune Global 500. With a robust portfolio of intellectual property anchored by more than 200 patents and patents pending, the company continues to drive innovations that assure business continuity, agility, and governance.

Learn more at www.bluecoat.com.

Encrypted Traffic Management

FOR DUMMIES®
A Wiley Brand

Blue Coat Systems Special Edition

by Steve Piper, CISSP

FOR DUMMIES®
A Wiley Brand

***Encrypted Traffic Management* For Dummies®,**
***Blue Coat Systems Special* 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.

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.

ISBN 978-1-119- 04763-0 (pbk); ISBN 978-1-118- 04732-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

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

Development Editor: Kathy Simpson

Project Editor: Jennifer Bingham

Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Kimberley Schumacher

Project Coordinator: Melissa Cossell

Special help from Blue Coat Systems: Greg Mayfield, Mark Urban, Hugo Isaac, Joe Levy, David Wells

Table of Contents

Introduction

Combatting advanced cyberthreats grows more challenging every day. With up to a third of enterprise Internet traffic now being encrypted, cybercriminals are cloaking their attacks within Secure Sockets Layer (SSL) traffic, knowing very well that perimeter security devices are blind to their exploits.

But even if all of your network security devices could scrutinize SSL traffic, maintaining user privacy is the next concern. How can you inspect SSL traffic for threats while maintaining the privacy of employee online banking, healthcare, and shopping transactions?

Unfortunately, increased SSL usage causes new headaches for IT security. Monitoring and enforcing compliance with internal and external standards for acceptable use of SSL encryption is difficult at best. And implementation of weak encryption keys and subpar cipher suites often give organizations a false sense of security.

Isn't there anything you can do to equip your security devices to inspect SSL traffic while maintaining user privacy and enforcing SSL-usage standards? Fortunately, the answer is "Yes!" And the solution is simpler than you might expect.

About This Book

This book introduces you to a category of technology that you may have never heard of: encrypted traffic management. This technology uses dedicated, high-performance appliances that give your security devices an instant look at SSL-encrypted communications while maintaining user privacy and allowing you to control the way that SSL is used on your network.

If you're responsible for securing your employer's network from today's advanced cyberthreats, this is one book you can't afford to miss.

Foolish Assumptions

In preparing this book, I've assumed a few things about you, the reader:

- You work in the IT security or compliance field for a corporation, government agency, or services firm.
- You have foundational knowledge of computers and computer networking concepts.
- You're responsible for securing your employer's IT systems and data and/or for auditing and enforcing internal and external compliance policies.

Icons Used in This Book

This book uses the following icons to indicate special content.

REMEMBER

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

TIP

A Tip icon points out practical advice that can help you craft a better strategy, whether you're planning a purchase or setting up your software.

WARNING!

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

TECHNICAL STUFF

Maybe you're one of those highly detailed people who really needs to grasp all the nuts and bolts — even the most techie parts. If so, these tidbits are right up your alley.

Beyond the Book

Although this book is chock-full of useful information regarding encrypted traffic management solutions, there is only so much ground I can cover in 48 pages! If you'd like to learn more about the features and benefits of leading enterprise-class SSL visibility appliances, go to `www.bluecoat.com/products/ssl-visibility-appliance`.

Chapter 1

The Risks and Rewards of SSL Encryption

In This Chapter

- Getting grounded in SSL
- Recognizing the risks of SSL encryption
- Getting to know SSL visibility appliances

The use of *Secure Sockets Layer (SSL)* encryption to secure Internet communications is rising steadily. According to the information security research firm NSS Labs, SSL now secures 25 to 35 percent of Internet traffic.

Today, SSL is the de facto encryption standard for web, cloud, and mobile communications. Thousands of Internet applications use SSL by default, including Gmail, Microsoft SharePoint, Microsoft Exchange, Facebook, LinkedIn, Salesforce.com, Amazon Web Services (AWS), and Google Apps.

Although SSL is intended to secure Internet traffic, the "bad guys" often use it to conceal advanced and targeted cyberthreats, and to exfiltrate data. Unless your network security strategy allows for visibility and inspection of SSL traffic, your organization is clearly at risk — and perhaps your job is, too.

This chapter provides an in-depth look at the risks and rewards of SSL encryption. First, I describe how SSL works and recap the key benefits of encrypting Internet traffic. Then I explore several risks that many enterprises fail to guard against. I end the chapter by describing an innovative network security solution that mitigates these risks, minimizing your chances of being the next victim of a targeted attack or an *advanced persistent threat* (APT).

SSL Encryption 101

This section discusses some of the fundamentals of SSL encryption, including its derivative encryption standards.

Reviewing common Internet encryption standards

Two common standards are used for securing Internet communications: SSL and TLS. They both rely on the same underlying encryption technologies.

SSL

SSL is a cryptographic protocol developed by Netscape to encrypt Internet communications. Version 1 was never released publicly. Version 2, released in 1995, contained security flaws that led to version 3 — the latest, released in 1996.

SSL uses X.509 certificates and, hence, *asymmetric cryptography* to authenticate trusted hosts and exchange public and private keys. The result is a symmetric session key that's used to encrypt and decrypt data flowing between two trusted hosts. SSL achieves data confidentiality and message authentication. In the Open Systems Interconnection (OSI) model, SSL is initialized at Layer 5 (Session layer) and works at Layer 6 (Presentation layer).

TLS

Transport Layer Security (TLS) is widely considered to be the successor to SSL. Version 1 was defined in 1999 as an upgrade of SSL version 3. Versions 1.1 and 1.2 followed in 2006 and 2008, respectively. Version 1.2 is the latest version, although version 1.3 is currently in draft.

The differences between SSL and TLS are subtle and extremely technical. For the purposes of this book, it's easiest to think of them as being the same.

For the rest of this book, I refer only to SSL because of the wide use of the term, although all the concepts in this book apply equally to both Internet encryption standards. It is worth noting that most modern browsers and secure sites use TLS rather than SSL and may even prefer later versions of TLS.

Hypertext Transfer Protocol Secure (HTTPS) is the result of layering HTTP on top of the SSL protocol, thus securing HTTP communications by providing secure authentication and session confidentiality. Although many application and protocols leverage SSL for confidentiality, such as IMAP, POP3, LDAP, SQL connections, and many others, HTTPS is the most popular in its use for accessing sensitive applications or sending/receiving sensitive data, as in online banking.

Odds are that you use HTTPS nearly every day and don't even know it. When you connect to a website that uses HTTPS, such as PayPal, a little padlock icon appears to the left of the URL in your web browser (see Figure 1-1). If you see that padlock, your connection is secure.

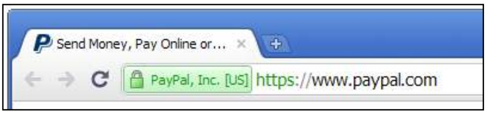


Figure 1-1: Sample HTTPS connection.

Seeing how SSL works

The following five steps describe how an SSL connection is established between a client and a server:

1. Client browser connects to an SSL-capable website and advertises which key exchange mechanisms and cipher suites it supports.
2. The web server sends an X.509 certificate containing the server's public key issued by a *certificate authority* (CA). The server also selects the key exchange mechanism to be used and the cipher suite.
3. Client authenticates the certificate against a list of known CAs. If the CA is unknown, the browser allows the user to accept the certificate at his or her own risk.
4. Client generates a random symmetric key and encrypts it, using the server's public key.
5. Client and server both possess the symmetric key and use it to encrypt communications.

Benefitting from SSL encryption

Here are some of the benefits that SSL encryption offers (not all of which are obvious):

- **Facilitated authentication:** When your endpoint device connects to a server, it's important to know that you're sharing sensitive information with the real intended server. When a server incorporates an SSL certificate from a legitimate CA, users can be confident that their sensitive data won't fall into the wrong hands.
- **Encrypted user sessions:** SSL encrypts sensitive information sent across the Internet so that only the intended recipient can understand it. SSL supports a large and growing set of ciphers and key sizes, helping it to stay one step ahead of hackers who would try to decrypt the coded information.
- **Protection against phishing:** Phishing and spearphishing emails often contain hyperlinks that lead unsuspecting users to convincing replicas of reputable websites. When they connect to fake websites and see "untrusted CA" messages, however, most users navigate away without entering any confidential information.
- **Improved customer trust:** Security-conscious consumers and business customers gain peace of mind from doing business over the Internet via SSL. Implementing SSL with certificates purchased from a reputable, publicly trusted CA improves customer trust, often leading to increased revenue and enhanced customer loyalty. Use of server certificates issued by CAs that aren't publicly trusted or that are self-signed may result in decreased website traffic.

Surveying the Risks of SSL Encryption

Every benefit of SSL encryption, however, has an offsetting risk. If organizations fail to mitigate the risks described in this section, they may just find themselves in the headlines for all the wrong reasons.

Missed cyberthreats

REMEMBER

If there's one thing that I'd like for you to take away from reading this book, it's this: *Every single one of your network security devices is powerless to inspect SSL-encrypted traffic unless that traffic is decrypted before inspection.* With 25 to 35 percent of Internet traffic being encrypted, roughly a quarter to a third of the traffic entering your network at the perimeter may go uninspected for cyberthreats.

Following are examples of typical network security devices that play important roles in detecting cyberthreats and subsequent data loss:

- Intrusion detection and prevention systems (IDS/IPS)
- Next-generation firewalls (NGFWs)
- Secure web gateways (SWGs)
- Advanced threat protection/sandbox solutions
- Security analytics and forensics solutions
- Data loss prevention (DLP) solutions

TIP

Chapter 3 describes these solutions in detail and discusses the ramifications of failing to decrypt SSL traffic before inspection by each device.

WARNING!

Some of these devices only inspect *ingress* (inbound) traffic; others only inspect *egress* (outbound) traffic; still others inspect both kinds. If your solution doesn't allow you to inspect both ingress and egress SSL-encrypted traffic, you dramatically increase your organization's risk of being victimized by an APT attack (see the nearby sidebar "Exploiting SSL in APT attacks").

Reduced efficacy of DLP investment

In the fight against advanced threats, data loss prevention (DLP) technology is widely viewed as a last line of defense.

Sure, DLP commonly guards against accidental disclosures of confidential and/or proprietary data, but it's also an important tool in the fight against APTs and other advanced targeted attacks. DLP systems may be triggered upon unauthorized exfiltration of data.

Knowing that many organizations fail to decrypt both ingress and egress SSL traffic, cybercriminals establish SSL-encrypted channels specifically to exfiltrate stolen data when a targeted system has been compromised. Without inspecting SSL traffic, a company's DLP systems are far less effective at mitigating advanced threats.

Exploiting SSL in APT attacks

Advanced threat tactics have grown in sophistication in recent years. Today, cybercriminals commonly use SSL to hide their activities before, during, and after attacks:

- ***Before the attack,*** the cybercriminal usually constructs a highly targeted spearphishing email, often with an embedded hyperlink that redirects targeted victims to an SSL-enabled website. When a user reaches that website, his or her endpoint device may become compromised.
- ***During the attack,*** the compromised endpoint device receives instructions via the cybercriminal's *command and control* (*C&C*) server to scour the network in search of servers of interest. When a target server has been compromised, data is exfiltrated. Both of these activities commonly occur through SSL-encrypted channels.
- ***After the attack,*** the cybercriminal covers his tracks by uninstalling a remote-administration tool — sometimes called a remote-access Trojan, or RAT — that was installed during the initial exploitation. The command for uninstalling the RAT is, once again, delivered under cover of SSL.

Trying to uncover APT attacks without decrypting SSL traffic is like trying to find a needle in a haystack while wearing a blindfold. APT attacks are hard enough to detect when all traffic is available for inspection. Why make life even more difficult by ignoring your SSL traffic?

Inability to assess data breaches

Savvy IT security organizations rely on *network forensics* (also known as *security intelligence and analytics)* appliances to capture every bit and byte that traverses the network. These systems are particularly useful to incident responders, who must investigate the causes and effects of advanced threats.

Naturally, SSL traffic remains encrypted when it's captured by network forensics appliances and, in most cases, the captured encrypted traffic can't subsequently be decrypted. Thus, incident responders can't obtain all the forensic evidence they need to truly assess the effect of a successful attack and data breach.

Circumvented internal compliance policies

Some sophisticated IT security organizations have documented policies about the use of SSL encryption. One such policy may restrict access to SSL-equipped servers that don't have bona fide SSL certificates from reputable CAs. Or an organization may require all SSL communications to incorporate 128-bit or higher encryption keys, because traffic encrypted with 64-bit keys is much easier to decipher.

Unfortunately, most organizations aren't capable of monitoring compliance with such policies, much less enforcing them. This situation poses risks to organizations that unknowingly deploy systems with self-signed certificates and/or encrypt communications with weak encryption keys.

Introducing SSL Visibility Appliances

Fortunately, a simple solution can mitigate all the risks associated with SSL encryption. This solution is an SSL visibility appliance.

An *SSL visibility appliance* is a high-performance, purpose-built, appliance (see Figure 1-2) designed to decrypt SSL, pass unencrypted traffic to a series of network security devices for inspection, and then forward (safe) re-encrypted traffic to its intended destination. Think of it as a *transparent SSL proxy*.

Figure 1-2: Sample SSL visibility appliance from Blue Coat.

SSL visibility appliances don't decrypt traffic corresponding to virtual private network (VPN) connections because the VPN connection contains multiple sessions multiplexed together into one data stream. However, because VPN connections are typically initiated by trusted employees and contractors, inspecting VPN traffic for threats is generally less of a concern. If VPN traffic requires inspection, then this should be done on egress from the VPN termination device.

The primary objective of an SSL visibility appliance is to maintain an end-to-end encrypted session between the client and server while providing visibility into that session for security appliances. Leading solutions can decrypt multiple gigabits per second (Gbps) of SSL traffic while adding no perceptible latency. Because these appliances are merely forwarding decrypted traffic to other network security devices, they're compatible with all network security devices.

Chapter 2 explores key features of SSL visibility appliances.

Seeing how they work

SSL visibility appliances can be deployed in many ways to meet the SSL decryption, inspection, re-encryption, and management needs of any organization. This section provides a brief overview of how they're deployed to decrypt ingress SSL traffic for the benefit of both passive and active (inline) network security devices (see Figure 1-3).

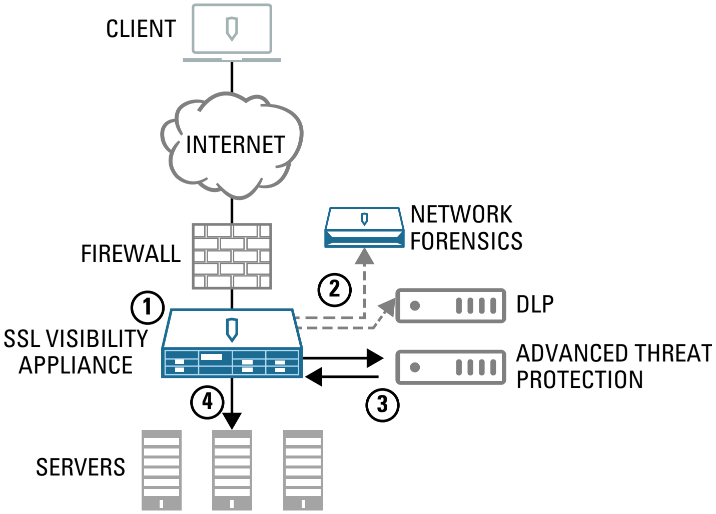


Figure 1-3: Sample SSL visibility appliance deployment.

TIP

SSL visibility appliances can be deployed inline to support both active and passive security devices. Or they can be deployed passively to support passive security devices (only). Chapter 5 explores these deployment options in great detail.

The flow of SSL traffic in Figure 1-3 follows a four-step process:

1. The SSL visibility appliance decrypts SSL traffic after it passes through the perimeter firewall.
2. Decrypted SSL traffic is copied to passive network security devices, such as network forensics and DLP appliances.
3. Decrypted SSL traffic is simultaneously forwarded to one or more network security devices, such as IPSs, NGFWs, malware analysis (*sandboxing*) appliances, and security analytics and forensics systems.
4. Traffic (free of cyberthreats) returned by the active network security device is forwarded to its final destination in its original SSL-encrypted state.

Securing SSL certificates

To decrypt SSL traffic midstream between the client and server, an SSL visibility appliance performs what some people call a controlled man-in-the-middle (MITM) attack. Instead of intercepting SSL sessions with malicious intent, this “attack” is done with the full authorization of IT security personnel.

To do its job, an SSL visibility appliance must be configured to store all server SSL certificates and private keys used. Maintaining so many certificates and keys in one place could pose a security risk if the SSL visibility appliance were to become compromised. That’s why leading SSL visibility appliance vendors go to great lengths to keep them secure:

- All SSL certificates and keys are stored on the SSL visibility appliance in an encrypted state.
- Only privileged users with proper administrative credentials can access SSL certificates and keys.
- Certificates and private keys are never exported from an SSL visibility appliance in plaintext.
- Their appliances adhere to regulatory compliance mandates, such as Federal Information Processing Standard (FIPS) 140-2, that ensures protection in U.S. federal government environments requiring the most stringent security.
- The use of an optional internal or external hardware security module (HSM) to protect certificates and keys against physical attack or compromise of the appliance.

Maintaining user privacy

The primary job of an SSL visibility appliance is to decrypt, inspect, re-encrypt, and forward SSL traffic based on established policies, in support of a company’s business. From time to time, however, employees may use SSL for personal business, such as online banking. Anyone would deem decrypting SSL packets related to personal online banking transactions to be a complete invasion of privacy. Thus, leading SSL visibility appliance solutions enable administrators to easily configure policies to bypass SSL decryption and inspection for certain types of transactions, such as online banking, benefits enrollment, healthcare management, and payroll processing.

Chapter 2

Exploring SSL Visibility Appliances

In This Chapter

- Knowing what hardware features to look for
- Reviewing key software features

What makes for a good SSL visibility appliance, and how do you know whether a given appliance is right for your organization? This chapter helps answer those questions.

Selecting the Right Hardware

SSL visibility appliance models vary with regard to scalability, latency, connectivity, and availability. The following sections review the hardware factors that you need to consider when selecting an SSL visibility appliance.

Scalability

REMEMBER

Decrypting SSL-encrypted traffic is computationally expensive. In other words, decrypting SSL eats up enormous amounts of central processing unit (CPU) and memory resources. It's important to offload SSL decryption to a dedicated appliance to preserve the processing power of your existing network security devices. (I discuss this topic in more detail in Chapter 3.)

It's also important to select an SSL visibility appliance that can keep up with your SSL bandwidth consumption. You may have a 3 Gbps connection to the Internet, for example, but if only a third of your traffic is SSL-encrypted, a 1 Gbps SSL appliance may suit your needs, at least for today!

Modern SSL visibility appliances typically scale to support multigigabit SSL throughput while simultaneously processing tens of gigabits per second of unencrypted packets. Because most traffic that passes through the box is unencrypted, that traffic passes through the box with little effort and at low latency, in support of time-sensitive applications and services.

In high-transaction environments (those with thousands of concurrent connections), be sure to evaluate maximum concurrent SSL flow states and maximum SSL connections per second. High-end models usually can handle hundreds of thousands of concurrent SSL-inspected flows and over 10,000 new full-handshake SSL connections per second.

Latency

Latency is another important factor to consider in evaluating SSL visibility appliances, especially for transaction-based applications (such as stock trading) and for organizations that frequently use voice over IP (VoIP) or live video applications such as Skype. Too much latency can affect transaction logging and the performance of voice and/or video calls.

Connectivity

SSL visibility appliances usually offer media options to suit the connectivity needs of any organization. Common options include 10/100/1000 copper interfaces, 10/100/1000 fiber interfaces, and 10 Gbps fiber interfaces.

TIP

Leading SSL visibility appliance vendors provide solutions (see Figure 2-1) that enable customers to purchase media connections in the form of network modules (also known as *netmods*). Thus, customers can choose the netmods that meet their needs today and in the future.

Figure 2-1: Sample 1U SSL visibility appliance with modular interfaces.

Availability and resiliency

Some SSL visibility appliance vendors build resilient, high-availability (HA) features into their offerings. You should look for features such as these:

- Redundant power supplies
- Fail-to-wire/*fail-open* media
- Link-state monitoring

Reviewing Key Features

Selecting the right hardware is certainly important, but so is selecting an encrypted traffic management solution with the right feature set. This section provides insight into the key features of best-of-breed SSL visibility appliances.

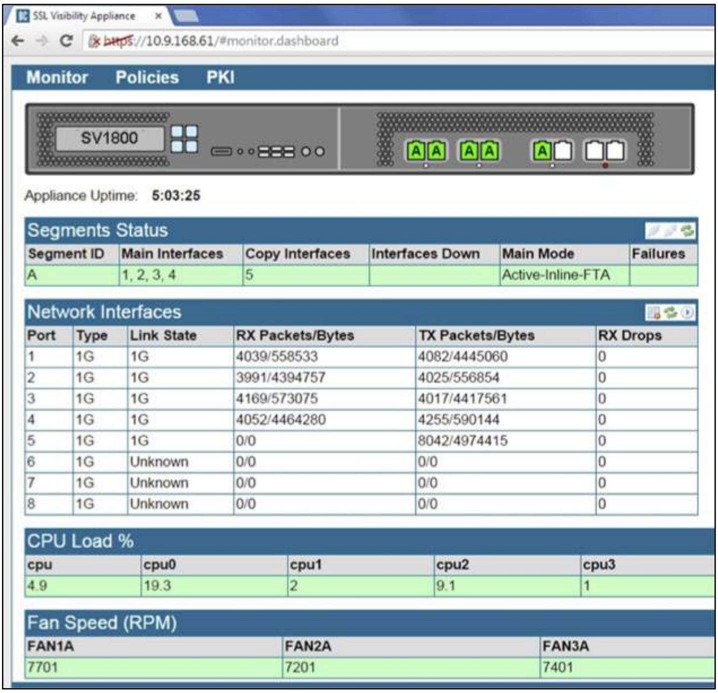
Comprehensive policy engine

The policy engine is the brain of every SSL visibility appliance, allowing administrators to configure granular policies that control SSL traffic throughout the enterprise. For example, SSL policy enforcement enables IT administrators to effectively balance data privacy and security by excluding the decryption and inspection of certain types of traffic, such as online banking and social networking.

Chapter 4 provides a few examples of SSL visibility appliance policies.

Intuitive web-based interface

First and foremost, your SSL visibility solution should feature an intuitive, easy-to-use interface. Better offerings incorporate a graphical depiction of the appliance (see Figure 2-2), making it simple to configure individual interfaces.



Appliance Uptime: 5:03:25

Segments Status

Segment ID	Main Interfaces	Copy Interfaces	Interfaces Down	Main Mode	Failures
A	1, 2, 3, 4	5		Active-Inline-FTA	

Network Interfaces

Port	Type	Link State	RX Packets/Bytes	TX Packets/Bytes	RX Drops
1	1G	1G	4039/558533	4082/4445060	0
2	1G	1G	3991/4394757	4025/556854	0
3	1G	1G	4169/573075	4017/4417561	0
4	1G	1G	4052/4464280	4255/590144	0
5	1G	1G	0/0	8042/4974415	0
6	1G	Unknown	0/0	0/0	0
7	1G	Unknown	0/0	0/0	0
8	1G	Unknown	0/0	0/0	0

CPU Load %

cpu	cpu0	cpu1	cpu2	cpu3
4.9	19.3	2	9.1	1

Fan Speed (RPM)

FAN1A	FAN2A	FAN3A
7701	7201	7401

Figure 2-2: Sample web-based interface for viewing appliance status.

Operational-based alerting

Logs can be configured to trigger alerts, which can be forwarded via email immediately or at designated intervals to SSL visibility appliance administrators. Examples of operational alerts include hard-disk space warnings and problems with system shutdowns.

TIP

Most SSL visibility appliances also support exporting alerts via syslog to SIEM (security information and event management) platforms, help-desk applications, or other systems monitored by IT support staff.

Traffic aggregation

Typical SSL visibility appliances are equipped with multiple sets of copper and/or fiber interfaces. In passive-TAP mode, these interfaces can aggregate traffic from multiple network TAPs (see Figure 2-3) for the benefit of one network security device, such as an IDS or security analytics and forensics appliance. Thus, one network security device can be used to effectively monitor traffic from multiple network TAPs, making it unnecessary to purchase a standalone aggregation TAP.

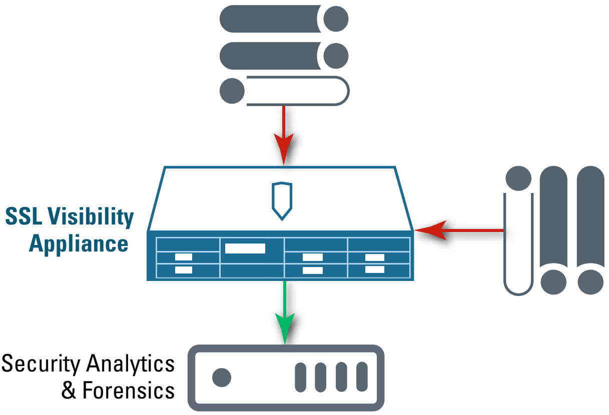


Figure 2-3: Traffic aggregation.

Traffic mirroring

Traffic mirroring (see Figure 2-4) is similar to traffic aggregation except that traffic from multiple segments isn't aggregated for the benefit of one security device. Instead, traffic from one network segment is copied (mirrored) for the benefit of multiple security devices.

TIP

Traffic mirroring saves you money by using a single SSL visibility appliance to decrypt SSL traffic from one network segment for the benefit of multiple security devices. You don't have to purchase an SSL visibility appliance for each network security device.

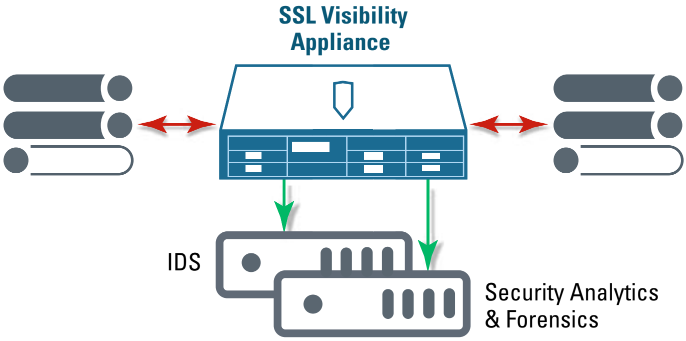


Figure 2-4: Traffic mirroring.

Financial media conglomerate is bullish on SSL visibility solution

A privately held financial software, data, and media company headquartered in New York City — with more than 15,000 employees in 192 locations — recently sought a solution to improve the efficacy of its network security investments by decrypting SSL traffic prior to inspection. Having read about major data breaches affecting other media outlets in the city, the company's network security director decided that failing to inspect SSL traffic for threats and data loss is a financial risk he's simply unwilling to take.

Having already deployed web security appliances from Blue Coat (`www.bluecoat.com`), the company requested an evaluation unit of Blue Coat's SSL Visibility Appliance. Within hours, the company's network security personnel realized how quick and easy the SSL Visibility Appliance is to deploy. And within days, the company began observing security alerts related to threats embedded deep within its SSL traffic.

Today, the company has acquired and deployed multiple Blue Coat SSL Visibility Appliances at strategic locations along the company's network perimeter. Each appliance is deployed inline to decrypt SSL traffic prior to inspection by an antimalware device. Once inspected, traffic is re-encrypted before being forwarded to its final destination — allowing the company to maintain compliance with both internal IT policies and external compliance regulations.

Furthermore, the company leveraged Blue Coat's powerful policy engine to construct SSL policies prohibiting the decryption of private employee SSL sessions pertaining to online banking, healthcare correspondences, web-based email, and more.

Chapter 3

Achieving Visibility into SSL-Encrypted Traffic

In This Chapter

- Beefing up your existing security
- Making compliance with regulations easier

The first of two use cases for implementing an encrypted traffic management solution is decrypting SSL traffic for the benefit of existing security defenses. Even if one or more of your network security components can decrypt SSL, enabling onboard SSL decryption can be a recipe for disaster.

In this chapter, I discuss how SSL visibility can make specific network security technologies more effective. I also discuss how an encrypted traffic management solution can improve your compliance with industry and government mandates.

Strengthening Your Existing Security Defenses

Dozens of network security technologies can benefit from a dedicated encrypted traffic management solution. This section explores some of the most common ones.

Intrusion prevention system (IPS)

An IPS or IDS (intrusion detection system), if configured for passive inspection, is only as effective as the traffic it sees.

With so much of your network traffic being encrypted, failing to inspect SSL is a risk that your organization can't afford to take.

Following are a few examples of cyberthreats that may hide within your SSL traffic:

- Malware designed to exploit operating-system and application vulnerabilities
- Buffer overflows and SQL injection attacks
- Phishing and spearphishing attacks
- Spyware and botnets
- Application-layer denial-of-service (DoS) attacks

Next-generation firewall (NGFW)

Many enterprises are moving away from standalone firewall and IPS products in favor of NGFW solutions. These solutions add powerful application-control capabilities to reduce networks' attack surfaces while improving network performance and employee productivity. Unfortunately, applications that communicate to the outside world through SSL prevent an NGFW from monitoring and controlling them, creating unnecessary risk.

WARNING!

Although some NGFW vendors' products may be able to decrypt SSL traffic before inspection, you'll discover in the "The case for offloading SSL decryption" sidebar, however, this process may be overly complex and costly.

Secure web gateway (SWG)

SWG appliances have evolved over the past decade to become mission-critical components of enterprise perimeter defense. Key capabilities of modern, best-of-breed SWGs include the following:

- URL filtering
- Detection of malicious code
- Application control
- Data loss prevention

Most SWG appliances monitor both ingress and egress traffic. If you fail to decrypt outbound SSL traffic as well as inbound, you may miss the ability to enforce acceptable use and productivity policies or attempts by infected hosts to "phone home" to their command-and-control (C&C) servers in concert with an APT attack.

The case for offloading SSL decryption

Enabling SSL decryption on your IPS, NGFW, or other network security device may seem like a good idea. However, here are four compelling reasons doing so is a concern:

Enabling SSL decryption on an IPS, NGFW, or other device dramatically affects its throughput, reducing performance by as much as 80 percent. A 10 Gbps IPS, for example, may suddenly turn into a 2 Gbps IPS when SSL decryption is enabled, due to the considerable computing resources (CPU and memory) required.

A "decrypt once, feed many" solution allows you to easily feed multiple network security tools simultaneously, making the solution much more manageable than decrypting SSL traffic on individual security devices. Further, when you enable SSL decryption on your security devices, you're also installing dozens or perhaps hundreds of SSL certificates and keys. That's no problem if you have just one security device that needs to inspect traffic, but when you have multiple devices inspecting traffic in sequence (such as IPS, SWG, and DLP appliances), this process becomes an administrative burden.

Most network security devices that offer onboard decryption usually fail to re-encrypt good traffic before passing it on to its final destination. If you're required to encrypt credit-card information for PCI (Payment Card Industry) compliance or health records for HIPAA compliance, you're in a world of trouble if that data doesn't remain encrypted from end to end.

Because more and more protocols are SSL-encrypted today, it's critical for any encrypted traffic management solution to be *port agnostic* and to decrypt more than just HTTPS traffic on port 443. Having the ability to see and decrypt SSL traffic across protocols like FTP, SMTP, SPDY, XMPP, IMAP, and POP3 is a growing imperative and, unfortunately, a capability that onboard SSL decryption features commonly lack.

If a security vendor tries to sell you on its product's capability to inspect SSL traffic, be sure to consider the performance, flexibility, compliance, and coverage ramifications of doing so in your real-world environment.

Advanced threat protection

Companies are in the news every day for being victimized by APTs and other advanced targeted attacks. In reaction to this bad press, an increasing number of companies are adopting modern, forward-leaning advanced threat protection and defense technologies.

Specialized malware analysis appliances lead the charge for detecting advanced threats embedded within everyday computer files (such as Microsoft Office documents, Adobe PDFs, HTML, Flash, .ZIP files, and dozens of other file formats). These appliances are designed to evaluate suspicious files in the safety of a *sandbox* (virtual machine and emulation engine) to uncover custom malware and zero-day threats that traditional signature-based defenses miss.

Obviously, a malware analysis appliance can't evaluate files that it can't see. I think you get the picture.

Security analytics and forensics

Security analytics and forensics systems provide a treasure trove of network intelligence by capturing every packet, file, and flow that traverses your network. Analysts use these systems to detect threats that bypass existing defenses and for incident response. Achieving full network visibility by decrypting SSL traffic is critical to your incident-response efforts (see the sidebar "Right-sizing incident response").

Data loss prevention (DLP)

DLP technology is widely viewed as being a last line of defense against the loss or misappropriation of confidential data. Sometimes, sensitive data is accidentally shared with the wrong party; at other times, data is purposefully exfiltrated from the network after an APT attack.

Regardless of how data is lost, a DLP solution can guard against data leakage. But of course, like every other network security device, it's blind to SSL-encrypted traffic.

Right-sizing incident response

When (notice that I'm not saying *if)* your organization's network is compromised by an advanced threat, overresponding is almost as bad as underresponding. If you underrespond by failing to notify all parties affected by a data breach, those parties (most likely your customers) may continue to be victimized, and they'll certainly lose trust in your company when they find out about the breach.

Conversely, if you overrespond by unnecessarily contacting parties who may be affected by a breach, you may cause unnecessary panic. Your customers may request replacement credit cards as a preventive measure, for example, which will cause them great inconvenience and may prompt them to reevaluate their relationship with your company.

When you respond to a data breach, it's imperative to right-size your response by notifying only those parties who are known to be affected by the breach. If only 10 credit cards were stolen, for example, why panic 100,000 customers?

Complying with Industry and Government Regulations

Enterprises face a multitude of complex industry and government regulations on securing sensitive data. Every IT security professional is obliged to inspect SSL traffic for threats and data loss. Failing to do so, however, doesn't give you a free pass on meeting compliance mandates, such as:

- Payment Card Industry (PCI)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- North American Electric Reliability Corporation (NERC)

TIP

Although the preceding mandates are North American-focused, European and Asia-Pacific countries continue to drive data privacy regulations as well.

Maintaining PCI compliance

The PCI Security Standards Council mandates the use of threat-detection technologies such as IPS; it also mandates that cardholder information remain encrypted from end to end. These requirements may seem to be conflicting, but they're really not.

When an SSL visibility appliance decrypts SSL traffic, that plain-text traffic is visible only within a closed loop by those network security devices in the flow of traffic. Encrypted cardholder information, for example, passes through the firewall in a decrypted state; is evaluated by IPS, SWG, and DLP solutions in a decrypted state, and then is forwarded to its final destination in its re-encrypted form, courtesy of the SSL visibility appliance. Cardholder data is never sent across the network unencrypted.

Electric automobile manufacturer steers clear of SSL-embedded threats

Producing environmentally friendly automobiles in the face of status quo fossil fuel–based competition takes a tremendous amount of forward thinking. Fortunately, the decision to implement an encrypted traffic management solution was a no-brainer for this U.S.-based electric automobile manufacturer.

After making considerable investments in malware analysis and security analytics solutions, the company's CISO knew there was still a missing piece to the company's network security puzzle. The company was completely blind to potential threats and data loss embedded within its SSL communications.

One of the company's existing network security vendors recommended Blue Coat's (`www.bluecoat.com`) SSL Visibility Appliance. It's "decrypt once and feed many" approach enabled its malware analysis and security analytics appliances to gain instant visibility while also affording the company newfound capabilities for enforcing internal SSL compliance policies.

Unlike some of this company's competitors, this CISO feels confident he can steer his company away from information security breach headlines.

Chapter 4

Maintaining SSL Policy Control

In This Chapter

- ▶ Balancing threat protection and user privacy
- ▶ Checking websites' SSL certificates
- ▶ Enforcing baseline encryption

The second of two encrypted traffic management use cases relates to establishing and enforcing policies that stipulate how SSL is used within an organization. These policies help strengthen the network's security posture by enforcing SSL best practices while ensuring that user privacy is maintained when SSL traffic is inspected for threats.

TIP

As you discover in Chapter 6, not all SSL visibility appliances are built the same way. Some rudimentary offerings only recognize HTTPS or web traffic, some only decrypt certain types of SSL traffic; these solutions are limited and can't maintain user privacy or enforce healthy SSL use standards.

Establishing SSL Policy Controls

IT can implement three types of SSL use policies through an SSL visibility appliance:

- ✓ User privacy safeguards
- ✓ SSL certificate validation
- ✓ Enforcement of minimum encryption standards

I explore all three types in the following sections.

Maintaining user privacy

The primary purpose of an SSL visibility appliance is to decrypt, inspect, and manage SSL traffic so that network security devices can uncover hidden cyberthreats. But if you decrypt and inspect all SSL traffic flowing in and out of your perimeter, you run the risk of disgruntling your users as well as potentially violating regulatory, industry, or other jurisdictional compliance mandates.

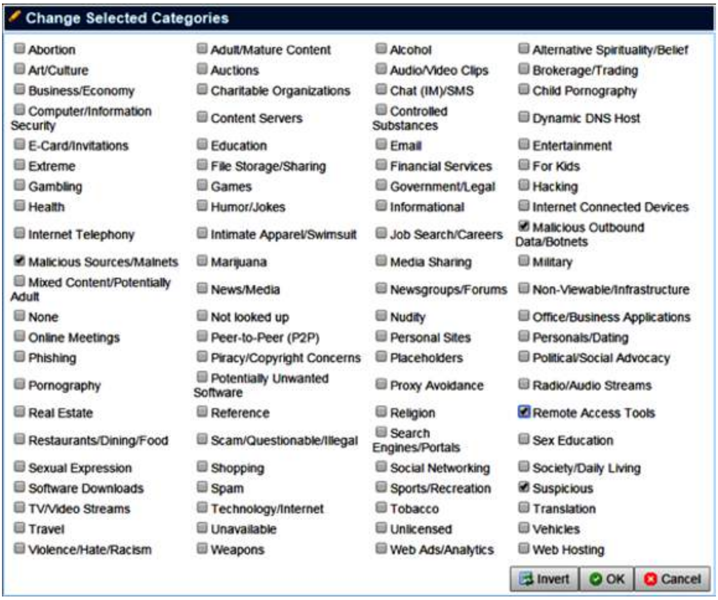
Although corporate networks are established to serve the needs of the business, virtually every company's employees also use its network for personal purposes such as the following:

- Online banking
- Brokerage/trading transactions
- Web-based email
- Internet telephony
- Shopping
- Social networking
- Education
- Healthcare provider communications

Although your organization could conceivably be vulnerable to a cyberthreat during an online banking transaction, the risk is very low, and the added protection of decrypting employees' private communications just isn't worth the fallout of upsetting those employees.

Wise administrators establish cut-through policies that detect SSL communications with reputable consumer websites. When approved SSL traffic is detected, that traffic bypasses the decryption process, and the organization saves valuable computing resources by not having to decrypt low-risk traffic.

Better SSL visibility vendors make it easy to establish and implement *whitelist* (allow) and *blacklist* (reject) policies by providing a host categorization list (see Figure 4-1), with dozens of categories of websites linking to thousands of URLs. These lists are reviewed and dynamically updated via a global,



Change Selected Categories

□ Abortion	□ Adult/Mature Content	□ Alcohol	□ Alternative Spirituality/Belief
□ Art/Culture	□ Auctions	□ Audio/Video Clips	□ Brokerage/Trading
□ Business/Economy	□ Charitable Organizations	□ Chat (IM)/SMS	□ Child Pornography
□ Computer/Information Security	□ Content Servers	□ Controlled Substances	□ Dynamic DNS Host
□ E-Card/Invitations	□ Education	□ Email	□ Entertainment
□ Extreme	□ File Storage/Sharing	□ Financial Services	□ For Kids
□ Gambling	□ Games	□ Government/Legal	□ Hacking
□ Health	□ Humor/Jokes	□ Informational	□ Internet Connected Devices
□ Internet Telephony	□ Intimate Apparel/Swimsuit	□ Job Search/Careers	☑ Malicious Outbound Data/Botnets
☑ Malicious Sources/Malnets	□ Marijuana	□ Media Sharing	□ Military
□ Mixed Content/Potentially Adult	□ News/Media	□ Newsgroups/Forums	□ Non-Viewable/Infrastructure
□ None	□ Not looked up	□ Nudity	□ Office/Business Applications
□ Online Meetings	□ Peer-to-Peer (P2P)	□ Personal Sites	□ Personals/Dating
□ Phishing	□ Piracy/Copyright Concerns	□ Placeholders	□ Political/Social Advocacy
□ Pornography	□ Potentially Unwanted Software	□ Proxy Avoidance	□ Radio/Audio Streams
□ Real Estate	□ Reference	□ Religion	☑ Remote Access Tools
□ Restaurants/Dining/Food	□ Scam/Questionable/Illegal	□ Search Engines/Portals	□ Sex Education
□ Sexual Expression	□ Shopping	□ Social Networking	□ Society/Daily Living
□ Software Downloads	□ Spam	□ Sports/Recreation	☑ Suspicious
□ TV/Video Streams	□ Technology/Internet	□ Tobacco	□ Translation
□ Travel	□ Unavailable	□ Unlicensed	□ Vehicles
□ Violence/Hate/Racism	□ Weapons	□ Web Ads/Analytics	□ Web Hosting

Figure 4-1: Sample host categorization list.

cloud-based collaborative database to provide administrators with proactive threat protection and policy enforcement.

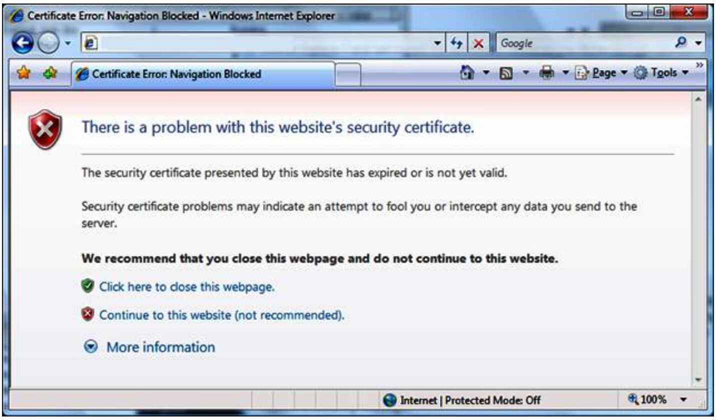
Validating SSL certificates

Virtually every company or government agency that conducts business over the Internet purchases SSL certificates from a reputable certificate authority (CA), such as Entrust, Thawte, Trustwave, and Verisign. Each CA validates the request by obtaining key information from the requester, including:

- *Certificate signing request (CSR)* (text generated by the requester's web server containing the public key)
- Correct contact information in domain name's WHOIS record associated with requester's website
- Business/organization validation documents (for high-assurance/extended validation certificates)

WARNING!

Some organizations create *self-signed certificates*, as they don't want to go to the trouble and expense of purchasing a certificate from a CA. Connecting to a website with a self-signed


Certificate Error: Navigation Blocked - Windows Internet Explorer
Google
Certificate Error: Navigation Blocked
Page
Tools
Internet | Protected Mode: Off
100%

There is a problem with this website's security certificate.

The security certificate presented by this website has expired or is not yet valid.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Figure 4-2: Warning displayed upon detection of self-signed SSL certificate.

certificate doesn't necessarily mean that the website is illegitimate, but it certainly poses a risk. That's why modern web browsers warn users (see Figure 4-2) before connecting to websites with self-signed certificates.

Fortunately, SSL visibility appliances can mitigate risks by decrypting SSL communications with websites that use self-signed certificates to allow inspection or by blocking such communications altogether (depending on the risk appetite of the IT organization).

Enforcing minimum encryption standards

SSL certificates are available in various key lengths (for example, 40-, 128-, 256-, and 2,048-bit) and incorporate multiple cipher suites (for example, AES, 3DES). The longer the encryption key, and the stronger the cipher suite, the harder it is for hackers to crack the system through a brute-force attack (trying each possible key in turn).

With SSL visibility appliances, administrators can configure policies that block SSL traffic that doesn't adhere to the company's policies regarding minimum key length and approved cipher suites.

Chapter 5

Deploying SSL Visibility Appliances

In This Chapter

- Identifying deployment options
- Seeing how deployment types function
- Making deployments successful

There are three options for deploying an SSL visibility appliance:

- Inline deployment with active security devices
- Inline deployment with passive security devices
- Passive TAP deployment with passive security devices

In this chapter, I explore all three deployment options and show you how to select the best one for your environment. I also provide a few tips that you'll find useful when the time comes to install and configure your SSL visibility appliance.

Exploring Deployment Options

To make an informed choice among the three SSL visibility appliance deployment options, it's important to know the differences between inline and passive TAP deployments, as well as the differences between active and passive security devices:

- **Inline versus passive TAP deployments:** When an SSL visibility appliance is deployed *inline,* client/server traffic flows bidirectionally through the appliance.

  When the appliance is deployed in *passive TAP* mode, client/server traffic flows only into it. In both cases, decrypted traffic is emitted through one or more interfaces from the appliance to other security devices.

  Inline deployment is required for both decrypting outbound SSL traffic and supporting active security devices.

- **Active versus passive devices:** When a security device is in *active* mode (which means that it's also inline), the device is capable of blocking bad or noncompliant traffic. Examples of inline devices include intrusion prevention systems (IPSs), next-generation firewalls (NGFWs), secure web gateways (SWGs), data loss prevention (DLP), and antimalware or sandboxing solutions; see Chapter 3 for details.

  When a security device is deployed in *passive* mode, it's capable only of triggering alerts when it sees bad or noncompliant traffic. Examples of passive devices include intrusion detection systems (IDSs) and security analytics/network forensics devices.

All the network diagrams in this chapter depict a single active or passive security device. However, most SSL visibility appliances support multiple network modules (netmods) and, thus, can support multiple inline and/or passive devices simultaneously.

Having access to multiple interfaces within the same SSL visibility appliance provides many advantages. First, multiple interface sets (pairs) enable one SSL visibility appliance to decrypt SSL traffic for the benefit of security devices on multiple network segments. Second, multiple interfaces can be used to support a combination of active and passive security devices on the same network segment. The more interfaces your appliance offers, the more choices you have for deployment.

Option 1: Inline deployment with active security devices

For an active security device, such as an IPS, to block threats, it must be placed inline (refer to the preceding section). Therefore, the SSL visibility appliance must be placed inline, too.

Figure 5-1 depicts traffic flowing into and out of both the active security device and the SSL visibility appliance. Note that all four monitoring interfaces on one of the appliance's netmods are in use.

When you select an SSL visibility appliance for an inline deployment, be sure its monitoring interfaces are capable of *failing open* or *fail-to-wire mode* (mechanically bridging the network connection) in the unlikely event that the appliance loses power or its software malfunctions. Otherwise, if the appliance fails, it may disrupt your entire network.

Option 2: Inline deployment with passive security devices

Passive network security devices, such as IDS or network forensics devices, can connect to an SSL visibility appliance whether that appliance is configured for inline or passive deployment.

In Figure 5-2, the passive security device uses one monitoring interface instead of two, because traffic is flowing unidirectionally from the SSL visibility appliance to the security device.

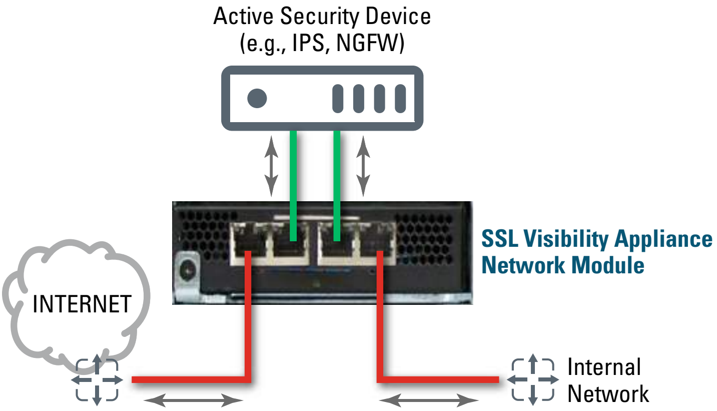


Figure 5-1: Inline deployment supporting an active security device.

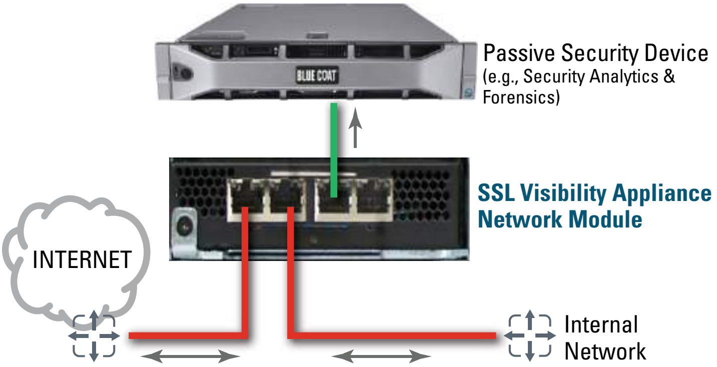

Passive Security Device
(e.g., Security Analytics & Forensics)
BLUE COAT
SSL Visibility Appliance Network Module
INTERNET
Internal Network

Figure 5-2: Inline deployment supporting a passive security device.

Option 3: Passive TAP deployment with passive security devices

When an SSL visibility appliance is serving traffic only to passive security devices, you have little need to deploy the appliance inline. But the appliance has to plug into *something* to receive a copy of bidirectional perimeter traffic.

In the previous two deployment options, the appliance simply plugs into the network at the perimeter — typically, just beyond the gateway or firewall. However, a passive TAP deployment requires a standalone network TAP (see Figure 5-3). Although the TAP is deployed as an inline device, it copies the traffic that it sees and forwards that traffic to the SSL visibility appliance in its entirety. Then the SSL visibility appliance decrypts the SSL packets and forwards all nonencrypted traffic to the passive security devices that it's configured to serve.

In practice, passive TAP deployments are rare and can only support the inspection of inbound SSL sessions bound for enterprise servers. Two important caveats exist with passive TAP deployments:

- SSL sessions must use RSA for key exchange — not DHE or ECDHE, for example
- The SSL visibility appliance must have a copy of the servers' certificates and private keys

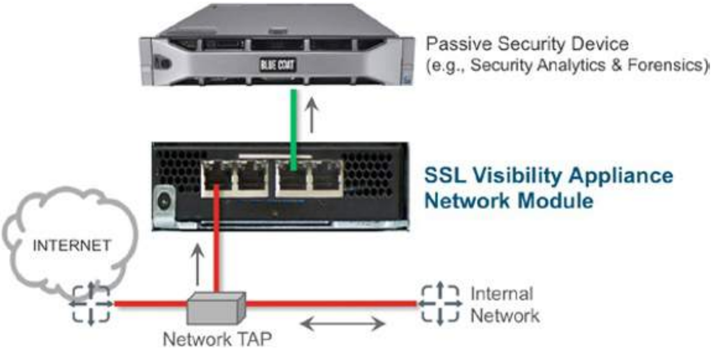


Figure 5-3: Passive deployment supporting a passive security device.

Ensuring Successful Deployment

Over the years, SSL visibility appliance vendors and their consultants (including channel partner consultants) have developed several deployment best practices. This section describes four of them.

Future-proof your investment

Most vendors offer multiple models of SSL visibility appliances with a range of throughput and monitoring interfaces (copper or fiber). Although a current model may accommodate your immediate needs, it's usually wise to plan ahead by purchasing the next-higher model. That way, you can future-proof your investment.

In other words, if your network throughput is likely to increase in the next few years, or if you may need to add more copper or fiber monitoring interfaces to support additional security devices, spend a few extra dollars now. Replacing an outdated box a few years down the line will be costly.

TIP

The average useful life of an SSL visibility appliance is three to five years. I recommend multiplying your current bandwidth requirement by 1.5 to ensure that you're covered when your bandwidth increases in the years ahead.

Leverage traffic aggregation and mirroring to save money

Most enterprise-class SSL visibility appliances offer at least eight copper and/or fiber monitoring interfaces, and some boxes support up to 28. Smart IT personnel know how to get the most out of these interfaces by aggregating multiple network connections or feeding multiple network security devices from the same traffic stream. (I discuss aggregation and mirroring in Chapter 2.)

This process saves organizations considerable money, as one SSL visibility appliance can serve multiple network segments and multiple inline or passive network security devices.

Bypass decryption of verified employee communications

If you acquire a full-featured encrypted traffic management solution, you should have no reason to decrypt sensitive or personal employee communications with legitimate consumer websites, such as those used for online banking and shopping. (See Chapter 4 for more about protecting user privacy.)

REMEMBER

Bypassing decryption of sensitive employee communications keeps users satisfied and also reduces the computational burden on SSL visibility appliances by reducing their workload.

Monitor outbound traffic too

So much emphasis is placed on advanced cyberthreats embedded in encrypted SSL communications that folks sometimes forget that hosts — especially laptops and mobile devices — may become infected when they're used outside the office. As a result, some threats are literally carried through the front door of the office.

It's important to decrypt both ingress and egress perimeter traffic so that your network security devices can detect malicious outbound communications, such as malware phoning a cybercriminal's command-and-control (C&C) server or data being exfiltrated after a security breach.

Chapter 6

Ten Buying Criteria for SSL Visibility Appliances

In This Chapter

▶ Knowing what to look for, and what to avoid, when evaluating encrypted traffic management solutions

▶ Reviewing top-ten buying criteria for SSL visibility appliances

The first five chapters of this book cover SSL visibility appliances in detail. This chapter tells you what to look for — and also what to avoid — when shopping for an encrypted traffic management solution.

WARNING!

Following are a few encrypted traffic management offerings that you should avoid like the plague:

- SSL decryption features built into your existing security devices. Enabling onboard SSL decryption can dramatically decrease the product's performance, and it doesn't decrypt SSL for adjacent (passive) security devices.
- SSL visibility appliances that can't scale to meet your organization's increasing bandwidth needs.
- Appliances that fail to re-encrypt SSL traffic after inspection. You can't meet PCI compliance, for example, if you transmit decrypted cardholder information across your network.
- Appliances that require third-party TAPs to be deployed in inline mode.

With that out of the way, the rest of the chapter focuses on attributes to look for when evaluating encrypted traffic management solutions.

User Privacy Protection

At the top of the list of criteria for SSL decryption is an appliance that knows which SSL traffic *not* to decrypt based on policies. A good SSL visibility appliance makes it easy to bypass decryption of user-initiated SSL sessions to legitimate websites through the use of an integrated and easy-to-use policy and enforcement engine that can categorize and filter SSL traffic based on host sites. That way, private connections to consumer sites (such as banking, brokerage, healthcare, and retail sites) stay private and aren't decrypted.

TIP

Better SSL visibility appliance vendors provide host categorization lists of SSL-enabled websites. Select a vendor that updates its lists frequently as new websites appear.

Compatibility with Existing Network Devices

An SSL visibility appliance is often described as a "bump in the wire," meaning that SSL traffic passes through the appliance with minimal latency, decrypting SSL traffic as it goes, and then passes decrypted traffic onto network security devices for further analysis. The administrator of the SSL visibility appliance doesn't have to reconfigure any of her network security devices because those devices have no way of knowing that the traffic was encrypted in the first place.

Comprehensive Policy Support

Although the primary use for any encrypted traffic management solution is to decrypt, inspect, manage, and re-encrypt SSL traffic, it's also important to control the way that SSL is accessed within an organization. Here are a few examples of user-defined policies:

- Maintaining user privacy (see "User Privacy Protection" earlier in this chapter)
- Validating SSL certificates

- Enforcing the use of approved cipher suites
- Enforcing minimum encryption strength requirements

Such policies help an organization increase security, reduce risk, and maintain user and data privacy.

TIP

For details on encrypted traffic management policies, refer to Chapter 4.

Support for Active and Passive Security Devices

A good SSL visibility appliance can support both active (inline) and passive security devices, separately or concurrently. Such appliances must have ample copper and/or fiber monitoring interfaces. Better SSL visibility appliances afford customers flexibility to add network modules to support new security devices and/or traffic from additional network segments.

REMEMBER

Only SSL visibility appliances that are deployed inline can serve decrypted traffic to active security devices. If the appliance is deployed passively (that is, traffic is copied to the appliance via a network TAP), it can serve traffic only to passive security devices.

TIP

Chapter 5 covers deployment options for SSL visibility appliances.

Line-Rate Network Performance

SSL visibility appliances feature specially designed hardware that decrypts SSL traffic — while passing through all other traffic — at line-rate speed.

Latency (refer to Chapter 2) is an especially important consideration for any organization that actively uses Voice over IP (VoIP) or videoconferencing technology — which these days is pretty much every enterprise. Significant latency degradations could affect the quality of voice and video communications. Identifying non-SSL traffic and ensuring it suffers minimal delay is an important feature to look out for.

Capability to Aggregate and Mirror Port Traffic

Traffic aggregation — a feature available with passive TAP deployments (refer to Chapter 5) — saves your organization money because you need only one SSL visibility appliance to decrypt SSL traffic from multiple network segments. Traffic mirroring also saves you money because one SSL visibility appliance can send decrypted and encrypted traffic to more than one network security device simultaneously.

If you select an appliance that doesn't offer both of these capabilities, you may need to purchase additional appliances as your needs grow — which can prove quite costly.

Support for Multigigabit Environments

Although your encrypted traffic management solution must meet your current throughput needs, you should consider one that can also support your SSL decryption needs as your network grows, Some vendors offer SSL visibility appliances that are capable of processing up to 1 Gbps of traffic, which may satisfy your current requirements, but you may be out of luck down the line if your needs change.

For more on future-proofing your environment, refer to Chapter 5.

Support for Multiple Protocols and Cipher Suites

When you evaluate an encrypted traffic management product, be sure to verify that it supports the protocols and cipher suites that you currently use for your network, as well as those that you plan to use. Just assuming that your chosen solution will support all protocols and encryption standards can prove costly. As the SSL/TLS standards continue to evolve, the management and support of these standards must also be supported in a timely manner within your SSL appliance.

The best SSL visibility appliances support SSL processing of both IPv4 and IPv6 flows, and can also handle common forms of LAN encapsulation, such as VLANs.

Following are common protocols supported by SSL visibility appliances:

- HTTPS
- SPDY
- POP3
- IMAP
- SMTP
- FTP

Protocols that typically aren't associated with SSL can pass through (or cut through) the box but aren't sent to the SSL processing engine. Examples include:

- Cisco ISL
- MPLS
- GRE
- IP-in-IP
- UDP
- ICMP
- ARP
- SOCKS
- DTLS
- IPsec

Finally, modern SSL visibility appliances support a variety of cipher suites and key exchange mechanisms. Examples include:

- Cipher suites: 3DES, AES, Camellia, ChaCha20, and RSA
- Key exchange mechanisms: DHE, ECDH, ECDSA, and RSA

Support of cipher suites and key exchange mechanisms may vary, depending on whether your SSL visibility appliance is configured for inline or passive operation. Check each product's documentation carefully.

Support for High-Availability Deployments

Although every IT professional considers his or her network to be mission-critical, some organizations that face incredibly high costs for downtime configure their networks — including security devices — for high availability (HA). As a result, they have two of everything, including firewalls, IPSs, SWGs, and business application servers.

TIP

Many enterprises invest millions in disaster-recovery sites. That way, if a natural or human-caused disaster destroys the primary data center, users are automatically redirected to a secondary data center on standby. If you work for such an organization, you should consider purchasing a redundant SSL visibility appliance for your disaster-recovery site.

Figure 6-1 shows a typical HA design. On the left, a primary SSL visibility appliance decrypts traffic for the primary network security devices. On the right, a secondary appliance decrypts traffic for the backup network infrastructure.

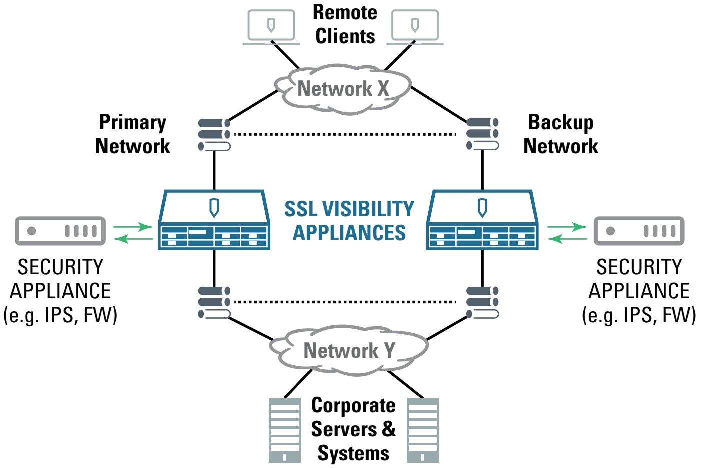

Remote Clients
Network X
Primary Network
Backup Network
SSL VISIBILITY APPLIANCES
SECURITY APPLIANCE (e.g. IPS, FW)
SECURITY APPLIANCE (e.g. IPS, FW)
Network Y
Corporate Servers & Systems

Figure 6-1: Sample high-availability design.

It's important to note that when a failover occurs, the SSL sessions that are being inspected will all fail and have to be reestablished as the SSL flow state can't be synchronized between two SSL visibility appliances.

Designing an HA deployment isn't easy. Each SSL visibility appliance works differently to support both active/active and active/passive HA environments (refer to Chapter 5). If your perimeter network infrastructure incorporates an HA design, have a detailed conversation with your encrypted traffic management vendor to ensure that its product is compatible with that design before you sign on the dotted line.

If you select an appliance that doesn't support high availability deployments, then you may need to replace that appliance in the future as your needs grow.

Superior Customer Support

Many enterprises overlook this criterion when they shop for IT solutions. In addition to focusing on the performance, manageability, scalability, reliability, and functionality of every product, be sure to assess the service provided by each vendor's customer-support organization.

Assessing tech support before you acquire a product from a vendor can be challenging, but here are a few methods that can provide valuable insights:

- Request an on-site evaluation of the SSL visibility appliance.
- Connect to the prospective vendor's website. Does the site have a support section with self-help resources such as a knowledge base, support videos, and customer forums?
- Call the customer-support telephone number to ask all the questions about the product you can think of — even if you already know the answers. Evaluate how long it takes to reach a human representative, as well as how knowledgeable and helpful that representative is.
- Submit a question via email or a web form. Once again, gauge how long it takes a representative to respond and how effective he was in answering your question.

Contact customer support both by phone and email, and submit at least two inquiries each time (four total) so that one novice support representative doesn't unfairly skew your perceptions.

The next step is yours

My hope is that after reading this book, you have a newfound appreciation for the importance of decrypting SSL to mitigate hidden cyberthreats and managing SSL to improve your organization's security posture and maintain user privacy. The next step is yours.

I encourage you to seek a reputable SSL visibility appliance vendor with offerings that support all your network security devices — not just its own. If you refer to the buying criteria in this chapter and the guidance provided throughout this book, you'll be well on your way.

Glossary

advanced persistent threat (APT): A sophisticated, targeted cyberattack that employs advanced stealth techniques to remain undetected for extended periods.

asymmetric cryptography: Class of cryptographic algorithms that requires two separate keys: a secret (or private) key and a public key. The parts of this key pair are linked mathematically.

certificate authority (CA): An entity that issues digital certificates for use in authenticating with SSL and TLS servers. The digital certificate verifies the ownership of a public key by the named subject of the certificate. See also *Secure Sockets Layer (SSL)* and *Transport Layer Security (TLS).*

certificate signing request (CSR): In public key infrastructure (PKI) systems, a CSR is a message sent from an applicant to a trusted certificate authority (CA) in order to apply for a digital identity certificate. See also *certificate authority (CA).*

command-and-control (C&C) server: A computer operated by an attacker to control distributed malware via the Internet. The attacker's purpose is to use the C&C server to send commands to compromised computers.

fail-open: A network appliance feature that, upon power loss or software failure, mechanically bridges a pair of monitoring interfaces to allow traffic to pass from one interface to the other without inspection.

Hypertext Transfer Protocol Secure (HTTPS): The result of layering HTTP on top of the SSL/TLS protocol, thus adding security to standard HTTP communications. See also *Secure Sockets Layer (SSL)* and *Transport Layer Security (TLS).*

phishing: Attempting to acquire personal information (such as usernames, passwords, and credit-card details) by masquerading as a trustworthy entity.

remote-administration tool (RAT): A program that allows a remote operator to control a system as though he or she had physical access to it. RATs are commonly used in APT attacks. Also called a remote-access Trojan. See also *advanced persistent threat (APT).*

sandbox: A virtual machine within security software that detonates suspected malware safely.

Secure Sockets Layer (SSL): Cryptographic protocols designed to provide communication security over the Internet by using X.509 certificates and asymmetric cryptography. See *X.509 certificate.*

self-signed certificate: A no-cost X.509 certificate signed by the same entity whose identity it carries. See *X.509 certificate.*

session key: A symmetric key used for encrypting all messages in a communication session.

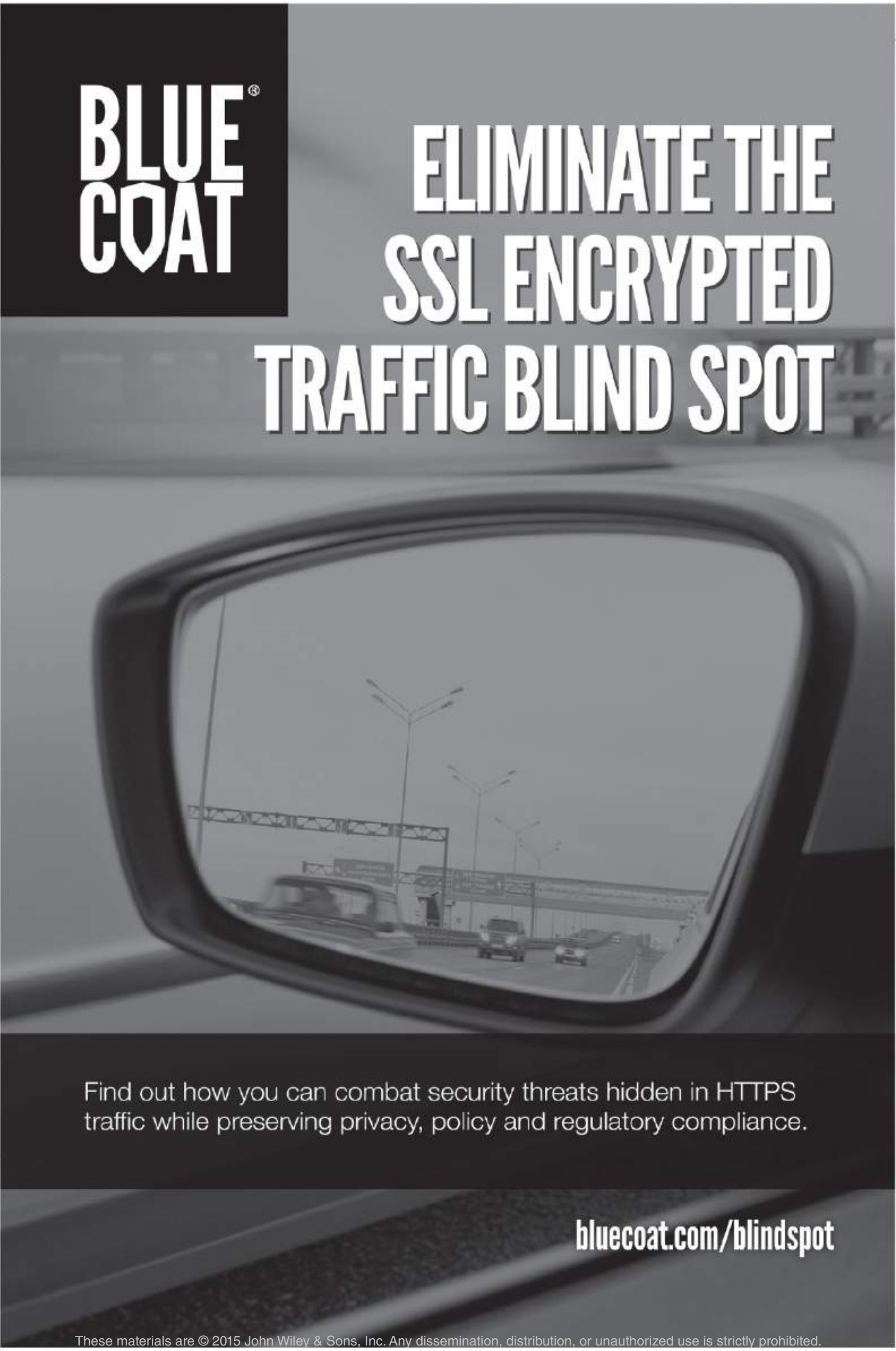
spearphishing: A highly customized phishing attempt on a specific organization or person. See also *phishing.*

SSL visibility appliance: A high-performance appliance designed to decrypt SSL communications for the benefit of perimeter security devices while allowing users to control SSL use to increase security and maintain user privacy.

transparent SSL proxy: A network device or application that intercepts SSL communications at the network layer for the purposes of decrypting and re-encrypting packets without requiring any special client configuration.

Transport Layer Security (TLS): The successor protocol to SSL. The latest TLS version, 1.2, is generally viewed as being more secure than the latest SSL version, 3. The two encryption standards are so similar, however, that the terms *TLS* and *SSL* are used interchangeably. See also *Secure Sockets Layer (SSL).*

X.509 certificate: A digital certificate that binds a public key to the name of its owner. X.509 certificates are used to both verify a person or entity's identity and to encrypt data so only that person or entity can read it.


BLUE COAT®
ELIMINATE THE
SSL ENCRYPTED
TRAFFIC BLIND SPOT
Find out how you can combat security threats hidden in HTTPS traffic while preserving privacy, policy and regulatory compliance.
bluecoat.com/blindspot

Expose APTs and other advanced threats cloaked within your SSL traffic!

Combatting advanced threats is a never-ending battle. With up to a third of your Internet traffic encrypted, savvy cybercriminals now cloak their attacks inside your SSL traffic. And your perimeter defenses are helpless to defeat them. Fortunately, high-performance encrypted traffic management solutions can help.

- ***Uncover hidden cyberthreats* — discover how purpose-built SSL visibility appliances can strengthen your existing perimeter defenses**
- ***Control your SSL traffic* — learn how to increase security, reduce risk, and maintain user privacy through SSL policy control**
- ***Weigh your deployment options* — explore three deployment options to support your active and passive network security devices**
- ***Know what to look for* — review important buying criteria to ensure your investment meets your needs today and tomorrow**

Open the book and find:

- **A primer on SSL and TLS encryption**
- **Features and benefits of SSL visibility appliances**
- **Methods for uncovering hidden cyberthreats**
- **Strategies for maintaining SSL policy control**
- **Tips for selecting and deploying your solution**
- **A handy glossary of terms**

Steve Piper is a high-tech veteran with over 20 years of experience. An award-winning writer and consultant, Steve has authored more than a dozen books on IT security, networking, and Big Data. He holds a CISSP security certification from ISC2 and Bachelor of Science and MBA degrees from George Mason University. Follow Steve on Twitter at @StevePiper or learn more at www.stevepiper.com.

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-119-04736-0
Not for resale