Encryption, Privacy, & Data Protection: A Balancing Act

The Business, Privacy, and Security Mandates for Comprehensive SSL/TLS Inspection

zscaler™

Abstract

SSL/TLS public-key encryption is the industry standard for data protection and is used to secure web transactions for much of the internet. Its secure encryption protects privileged data in transit and provides trust and anonymity to users. But it also offers cover for bad actors who use SSL/TLS to exploit that trust and anonymity to cloak their activities.

Enterprise IT leaders must employ comprehensive SSL/TLS inspection methodologies to mitigate the risks hidden in encrypted traffic. This white paper examines the risk posed by encrypted threats; considers the business, privacy, and security implications of managing that risk; and presents constructive measures for balancing security needs with employee privacy rights. In the end, the best way for IT leadership to ensure the rights of the individual employee is to protect the organization from threats and attacks.

The internet used to be much simpler—an open playground for the technically-savvy elite…

Nowadays, it has become the place where much of complex modern business and normal life happens. With ubiquity comes new risk. By its very nature, an "internet for everyone" includes a haven for bad actors that are determined to take advantage of those of us using it to conduct business and go about our everyday lives.

Privileged data must be protected, especially when it is in transit. Encryption offers the most practical way to do that. Data encoded with industry-standard SSL/TLS encryption protocols cannot practically (read: affordably) be decoded by a bad actor who intercepts it. (See Figure 1 and refer to the "Transport Layer Security [TLS] and Secure Sockets Layer [SSL]" sidebar.) Encryption also helps establish trust and preserve anonymity. It's this combination of capabilities that makes SSL/TLS encryption ideal for protecting communication over the internet, from simple web-browsing to e-commerce purchasing.

In today's business environments, it's essential to protect enterprise resources *and* to preserve the privacy of the individual. SSL/TLS serves both of those seemingly opposite missions. But in the wrong hands, SSL/TLS technologies can be potently dangerous. What happens when bad actors use it to encrypt malware and hide their activities? How can the modern enterprise combat this threat?

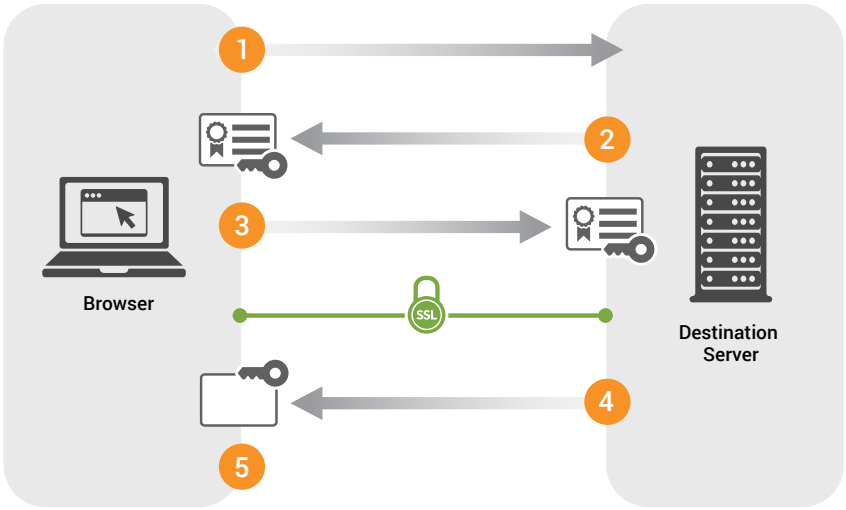
From open to secure: How SSL/TLS enables online protection

The internet has evolved. In the past, browsing—whether to Yahoo, Google, Microsoft, or your local university website—didn't require privacy or protection. Typing a URL in the browser address bar would take you directly to that site, with no cookies or detours introduced, and with little-to-no potentially exploitable data shared along the way. Nowadays, we commonly share both personal and private information and conduct business over the same network. We *live* on the internet. Even our browsing habits themselves have become valuable data. This change requires a more private and secure way of engaging with web services.

Enter encryption technology. Secure Sockets Layer (SSL) encryption (and its successor Transport Layer Security, or TLS) establishes *secure tunnels* between a browser and destination site using third party validated, "public-key" certificates. Those certificates, and the relationships they establish, create a set of interlinked *chains of trust*: "I trust you because someone I trust trusts you." When a company purchases such a certificate from a browser-recognized trust vendor (e.g., Verisign, Thawte), that company becomes a trusted member of that chain. When you browse to an SSL/TLS-protected site, your browser and the website exchange credentials (the certificate) and parameters so that the subsequent communication is encrypted.

That communication, even if it were to be captured, is unintelligible to anyone but the browser and website server. SSL and TLS protocols have been providing this encryption capability for several decades.

How SSL/TLS works in a browser-server connection



1. A user opens a browser and sends an HTTPS request.
2. The destination server returns an encrypted public key coupled with SSL/TLS certificate.
3. The browser client validates the certificate, creates and sends an encrypted key back to the destination server. (If the server certificate is not validated, communication ends.)
4. The destination server decrypts the received key, and delivers encrypted content (and key) to the client.
5. Client decrypts content.

Figure 1. How SSL/TLS works in a browser-to-destination server connection.

SSL/TLS provides three important features for web-browsing:

Privacy

Data contained within the secure tunnel cannot be seen or shared with another party.

Trust

There is validation that the browser is indeed speaking to the intended server/website.

Anonymity

The user's browsing behaviors are hidden to any parties in between the user and the server.

Transport Layer Security (TLS) and Secure Sockets Layer (SSL)[1] are network protocols intended to create a secure tunnel between two devices using cryptography. This provides secure communications over an otherwise public computer network. SSL and TLS protect data via cryptographic methods that use both public and private keys for encryption and decryption, and rely on certificates to authenticate communicating parties.

1 https://en.wikipedia.org/wiki/Transport_Layer_Security

Anonymity shields information about the browser and person behind it, but not the browser and server IP addresses. This gap has been addressed through the advent of anonymizing proxies[2] and anonymity networks like TOR.[3]

Encryption risk #1: Bad actors exploit trust

SSL/TLS encryption offers the reassurance of privacy: No one in between your browser and your destination knows what you're looking at, or what data is being shared. But recall the chain of trust—bad actors seek to exploit trust (See Figure 1), and have made SSL/TLS' inherent trust even more important than the tunnel's privacy and anonymity capabilities.

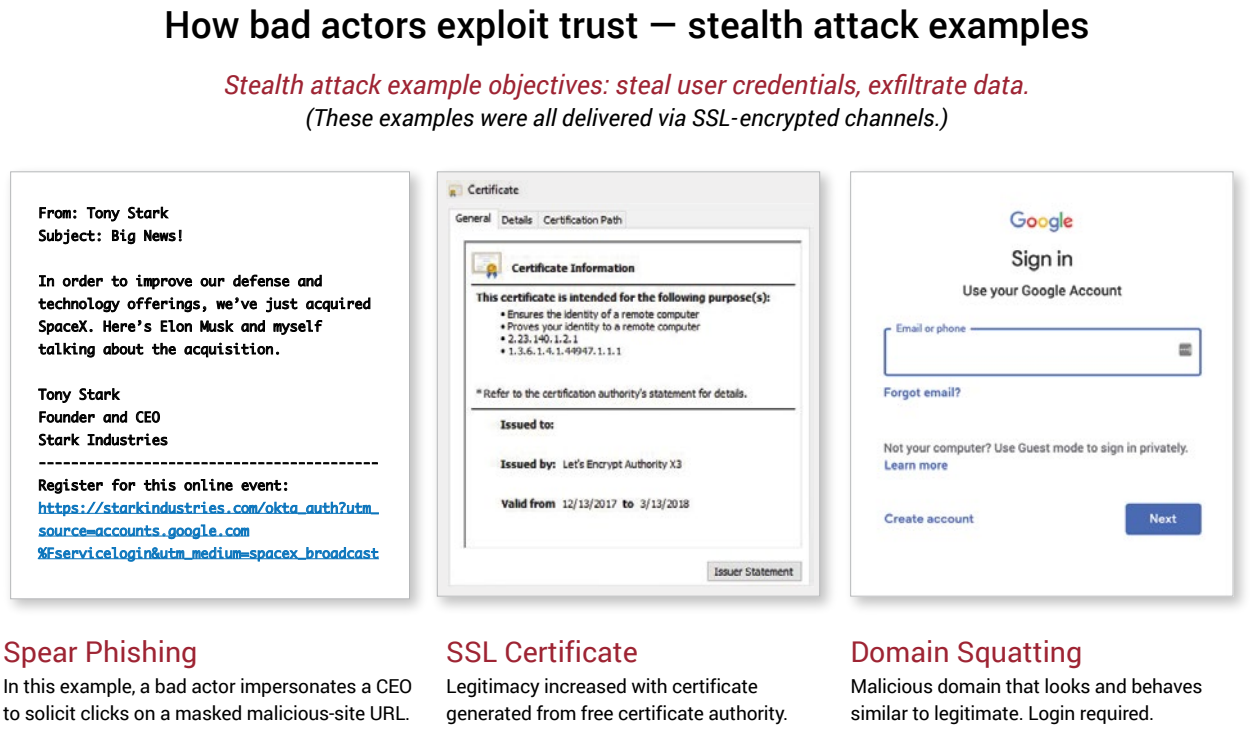


Figure 2. Examples of how bad actors exploit trust via SSL/TLS-encrypted delivery.

For instance, a simple internet search may not merit encryption, but Google does it anyway. Though the data may not be sensitive, the *certainty* of knowing that it is Google serving the page provides that essential element of trust. That same encryption chain of trust provides that validation. Like most modern websites, Google now serves all of its pages via SSL/TLS with "HTTPS" URLs. The age of open-text browsing "in the

2 https://en.wikipedia.org/wiki/Anonymizer

3 https://en.wikipedia.org/wiki/Tor_(anonymity_network)

clear" is ending. (Here at Zscaler, we're in a unique position to be able to observe internet traffic trends, and more than 83% of data traffic flowing through Zscaler is now encrypted via SSL/TLS.[4])

The secure tunnel model is, by design, secure. But it's still exploitable, particularly when it comes to user trust. Any organization (and even an individual) can purchase an SSL/TLS certificate. That organization can use that certificate to co-opt or mimic legitimate internet destinations (or even components of a legitimate web page), effectively compromising a site with a legitimate certificate. In this way, bad actors deceive the human behind the computer, and gain access to valuable user data that they can then decode, *even if it is encrypted in transit*. The bad actors are posing as a trustworthy entity. Since the traffic is encrypted, their data collection is undetected, and they bypass enterprise controls or tools put in place to stop them.

Encryption risk #2: Bad actors hide malware

The rise of phishing, spoofing, and ransomware attacks has eroded trust in the internet: How do I know I'm looking at a legitimate site? How do I know something on the site (ad, article, element) isn't compromised? How do I know this apparently legitimate site doesn't harbor encrypted malware?

Bad actors often compromise (or impersonate) third-party providers like Content Delivery Networks (CDNs) that feed content to legitimate sites, thereby serving up malware on a legitimate site that for all intents and purposes is otherwise HTTPS-"secured."

The bad actors use SSL/TLS encryption to hide their work, and the threat they present is getting progressively worse. This is not a new threat. Bad actors have always had the opportunity to hide malware within secure code. It's the economics that have changed. In the past few years, *free* SSL/TLS certificates have become readily available, greatly reducing the cost (and effort) of encrypting destructive malware.

Here at Zscaler, we've seen the volume of threats borne in encrypted tunnels grow exponentially over the last few years. More than 54% of detected advanced threats are now delivered over SSL/TLS-encrypted channels.[5] More worryingly, in 2018 phishing attacks encrypted with SSL/TLS were up 300%.[6]

Bad actors use the same SSL/TLS protocols to encrypt the source of their malware (for example, a "drive-by," purpose-built encrypted site housing the malware), and the malware's outbound communications. That encryption presents the illusion of "trustable" data, giving the bad actors a free pass to infiltrate enterprises, access assets, and obscure data exfiltration.

---

4 https://www.zscaler.com/threatlabz/encrypted-traffic-dashboard

5 https://www.zscaler.com/resources/solution-briefs/add-advanced-threat-protection-to-close-your-security-gaps.pdf

6 https://www.zscaler.com/blogs/research/february-2018-zscaler-ssl-threat-report

Encryption risk #3: Bad actors mask data exfiltration

If an outside bad actor manages to infiltrate a corporate network with the intent of stealing digital assets, that bad actor faces the challenge of getting data outside the enterprise's security perimeter. An inside bad actor is presented with the same issue: How to get proprietary information outside the organization?

Bad actors hide malware within inbound encrypted data. In some cases, that malware detonates inside an organization, infecting internal systems, then contacts external command-and-control (C&C) servers to exfiltrate valuable corporate data outside the organization.

Encryption can mask malicious (and even the occasional accidental) data leakage. Without outbound SSL/TLS inspection, how can an IT lead determine if confidential data is remaining private? SSL/TLS inspection must address both inbound (keep the bad actors out) and outbound (keep private information inside) data traffic. In the outbound example, SSL inspection is critical to preventing data loss and identifying and remediating zero-day attack data-exfiltration vulnerabilities.[7]

Balancing access and security in a new age of privacy

The evolution of internet connectivity heralds a new age of privacy—from clear-text to encrypted data transmission, from implicit to explicit trust. That's reflected not just in consumer demand for private data management, but in regulatory guidelines defining a user's right to privacy, such as Europe's General Data Protection Regulation (GDPR)[8], Canada's Personal Information Protection and Electronic Documents Act[9], and several existing (California, Maine, Nevada) and proposed (Hawaii, Illinois, Massachusetts, Mississippi, New Mexico, New York, Rhode Island, Texas, and Washington) U.S. state privacy laws.

Not all browsing or internet traffic is equal. In most cases, privacy leans to the individual. A casual user in a democratic state is likely to browse privately, whereas a web user in an authoritarian-governed location may use an anonymity network like Tor to shield communications from censor visibility to communicate with family abroad. In each case, the data is the user's own, and few—with the possible exception of that authoritarian government—would argue against preserving each user's right to privacy. Both users assume risk of data loss or interception, a risk which is limited to their own homes and devices.

It's a different story within an enterprise, or with government-provided internet access. Most would agree that corporate users should enjoy a right to some level of privacy on the internet—there's little reason a user's shopping habits, holiday destination choices, hobbies, or browsing destinations should become visible to

7 https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

8 https://eugdpr.org/

9 https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

fellow employees. The various laws governing privacy in many cases support that end. SSL/TLS has enabled that privacy, and even browsing anonymity, for years.

However, that expected privacy comes with cost and risk: Can we continue to enjoy that privacy if bad actors can exploit that privilege for their own gain? In an enterprise context, the risk is no longer just to the individual employee, but to the entire organization. Within the context of encryption technology capabilities, modern enterprise IT leaders must weigh the risk of incoming threats against the promise of privacy—a delicate balancing act between the rights of the individual employee and the requirement of the enterprise to protect itself.

In an organization, the view of a right to absolute privacy is less clear. Any enterprise that uses the internet—and, let's face it, that's every enterprise—has a responsibility to its employees, shareholders, and customers to protect itself and adhere to legal and regulatory guidelines. IT leaders employ technical and procedural controls to prevent and detect attacks and risky behavior. To reduce risk and protect the "house," those controls must be applied to all internal, inbound, and outbound data traffic.

The regulatory environment can add complexity to corporate data management. Some European jurisdictions require corporations to protect employees' personal data to ensure the privacy and, in some cases the anonymity, of personal web-browsing. For example, the German Telekommunikationsgesetz[10] ("Telecommunications Act," or TKG) is generally considered to apply to corporations providing employees with access to the internet for their personal use. The TKG specifically requires users be subject to "telecommunications secrecy." It also mandates that an organization adequately protect the service from damage and/or interception, AND protect the users' browsing data appropriately. TKG-compliant companies must balance user "telecommunications secrecy" against asset protection.

According to a recent Google Transparency Report,[11] up to 93% of Chrome browser traffic is encrypted. With bad actors presenting advanced threats via encrypted channels to evade enterprise security controls, how can a company protect both itself and its data, yet maintain employee privacy rights in compliance with data protection regulations?

Opening the tunnel—SSL/TLS decryption and inspection

In an enterprise, a malware attack is limited not only to an individual. Once an attacker has gained access to an employee's machine, that attacker can typically move elsewhere ("east/west[12]") within that employee's realm, and infect other systems and computers inside the corporate network.

10 https://germanlawarchive.iuscomp.org/?p=692

11 https://transparencyreport.google.com/https/overview?hl=en

12 https://searchnetworking.techtarget.com/definition/east-west-traffic

Cybersecurity controls can easily inspect open-text communication coming in or going out of an organization, but SSL/TLS encryption of inbound or outbound data complicates inspection. Can the presumed privacy of a secure tunnel be preserved if encrypted threats present such a danger to both the individual user *and* the larger enterprise?

The answer is YES. Combatting the risk of destructive encrypted threats starts with SSL/TLS data inspection. A company has an institutional and legal obligation to protect its assets, and that includes protecting its employees' communications.

To inspect SSL/TLS data, the organization must effectively divert that communication chain of trust, interrupting it with one tunnel between browser and inspection device, and then a subsequent tunnel between inspection device and destination.

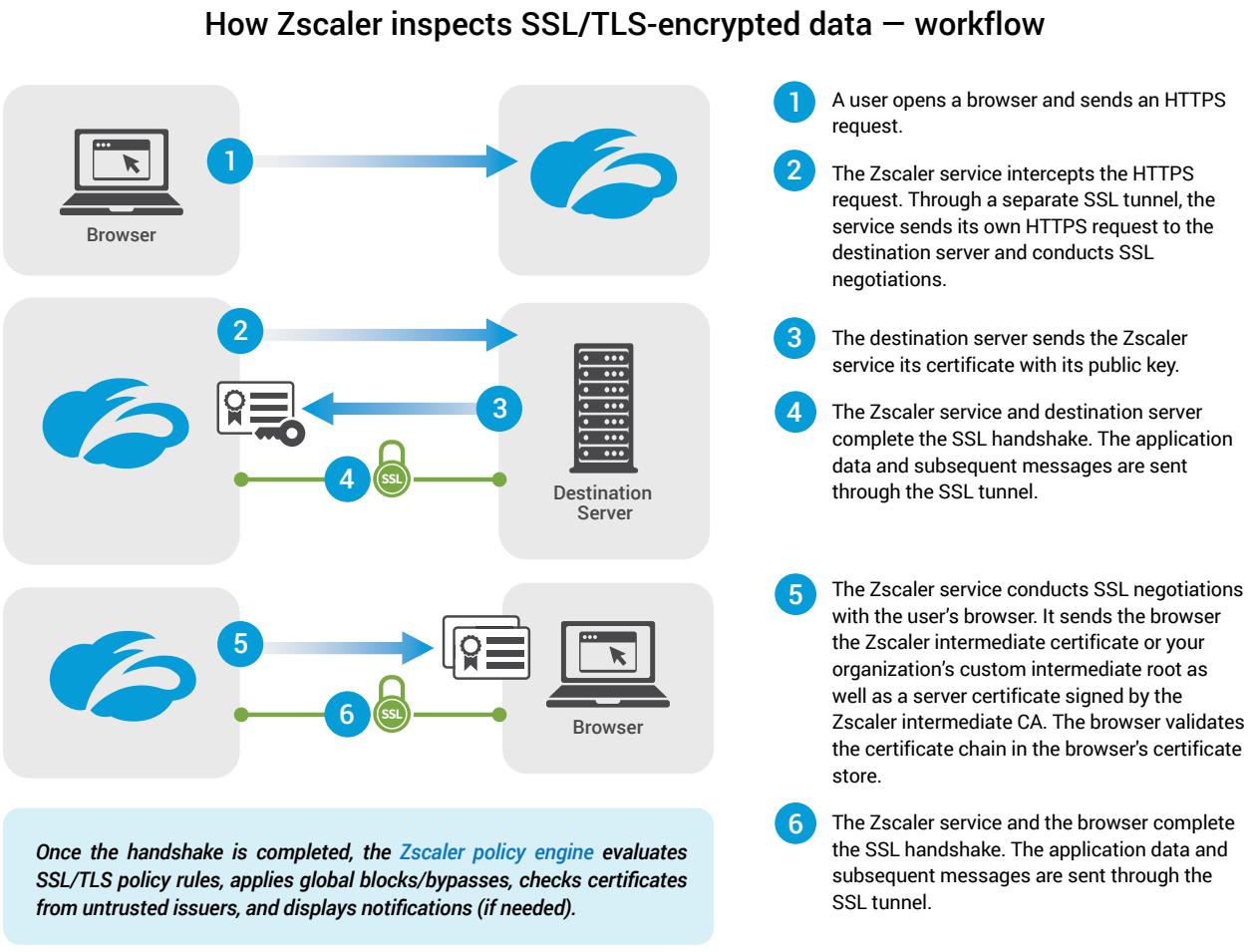


Figure 3. Workflow for how Zscaler inspects SSL/TLS-encrypted data.[13]

13 https://help.zscaler.com/zia/about-ssl-inspection

In this example, inspection does not break the trust relationship between individual and source. The employee places trust in the organization that provides the browsing device, rather than in the data source. The inspecting device will "see" the destination and the data contents.

So the question remains: *Can an organization perform this essential protective function while still respecting the other two features of encryption, anonymity and privacy?* Done correctly, absolutely. The threat posed by encrypted malware makes SSL/TLS inspection a cybersecurity control mandate for the modern enterprise, and organizations must balance their security needs with their employees' privacy rights. An organization that does not inspect SSL/TLS traffic exposes itself to unnecessary risks, including lost PII, stolen intellectual property, industrial espionage, or even ransomware infections. (The percentage of organizations inspecting encrypted data has grown: Among Zscaler enterprise customers—nearly half of which are based in Europe—72% inspect SSL/TLS traffic.)

In an enterprise, individual anonymity online can be preserved...to an extent

When evaluating SSL/TLS inspection models, we must first look at anonymity. In some organizations, the provision of internet access is a right granted and governed by employee contract, established and controlled by policy in the same way that employee workplace behavior is governed by policy.

The enforcement of this policy requires monitoring. An SSL/TLS tunnel exposes its source and destination already to anything, and anyone, between browser and server. Logging these transactions is essential for behavioral analysis and incident detection. Log reviews can help ensure policy adherence and contribute to continuous improvement of policy efficacy. (Retrospective log analysis is even often used in criminal investigations.)

With an SSL/TLS inspection protocol in place in the workplace, employees should not expect complete anonymity when browsing online as internet access is a privilege given by the organization to its employees and governed by each employees' contract of employment. To protect corporate assets, the organization may choose to track a user's destination URLs, browsing behavior, and device access. An organization's corporate policy establishes guardrails for that internet use, as well as repercussions for violating such policy.

To be clear, SSL/TLS inspection does not mean an end to individual anonymity online. Enterprises can balance employee privacy demands with up-to-date cybersecurity measures. Comprehensive data-monitoring is required for effective SSL/TLS inspection, but access to the data that results from that inspection can be limited. Employees can remain anonymous throughout log analysis, even during investigations and

adjudication (e.g., review and response to potential policy violations) until the need to engage arises. This anonymizing is typically referred to as log-indexing or obfuscation.

At times, IT leaders will need to inspect and analyze logs in full. For instance, a cybersecurity lead would regularly review logs to identify malware callbacks via SSL/TLS tunnel. When one is found, IT security must trigger a machine cleanup workflow, engaging with the employee to clear malware from the specific infected device (or even reformat or destroy it). This process can be implemented to support a "four eyes[14]" approach, with both a security administrator and a workers' representative (for instance, an employee association leader, or perhaps outside counsel) reviewing console logs at the same time.

When logs identify an infection, an individual corporate user cannot remain anonymous, and must be "de-obfuscated" to reveal identity so IT security can remediate the threat before it impacts the broader organization.

Data exfiltration—the unwanted "leaking" of data out of an organization—represents another situation that can require de-obfuscation. Typically, a log review process can determine that previous, un-filtered SSL/TLS traffic may actually be destined for a criminal or unapproved destination website. In this case, law enforcement may need to be engaged, and data de-obfuscated to support an investigation.

Employees should expect browsing to be anonymous to enterprise peers, management, and even corporate security teams...until a risk or threat to the organizations triggers the need to remove that anonymity. In the above situations, it is essential that the organization has a *documented need* to de-obfuscate through an Acceptable Use Policy (AUP) that would oftentimes be incorporated into the employee's employment agreement. Internet use via corporate devices or networks should be granted only when this has been agreed to by the employee (typically at the start of employment).

Securing the data: SSL/TLS decryption in a GDPR-governed environment

At face value, "opening" the SSL/TLS encrypted-communication tunnel for data inspection and policy enforcement seemingly makes the data no longer private. This is a common concern raised by corporate legal departments and privacy advocates. Some point to the GDPR as a basis for arguing that the GDPR prohibits an organization from decrypting and inspecting SSL/TLS encrypted personal data. In our opinion, this is incorrect.

14 https://whatis.techtarget.com/definition/four-eyes-principle

Even normal, unencrypted sessions will require the exact same obligations be applied to every party (ISP, network provider, caching proxy) between the browser and server. GDPR guidelines *still* require each party to treat the personal data with the same level of sensitivity. Encryption does not change the obligations placed on a data controller, or even a processor. Reducing the erroneous argument even further, the personal data is being processed by the employee's corporate-supplied device in an unencrypted fashion, *even when using an encrypted tunnel.* There can be no absolute provision of privacy within that corporate context.

SSL/TLS inspection is used to enforce policy and identify potential threats hidden in encrypted data traffic. To identify threats, an inspecting device decrypts the data, reviews it against a set of "known-bad" signatures, and inspects the data stream to determine threat risk such as malware coming in or company data inappropriately going out. If the data presents no threat, it is repackaged and sent on its way. Performed in this fashion, SSL/TLS inspection does not abridge employee privacy. Data is not shared with anyone, nor is it used in such a way that infringes on a data subject's rights. The SSL/TLS inspection process protects organizational assets from threat of attack, without impinging on individual privacy rights.

Zscaler offers comprehensive SSL/TLS inspection capabilities to protect customer data traffic and provide "perfect forward secrecy" (PFS).[15] Zscaler never stores data to disk: Once data inspection is complete, data flow continues unimpeded, with no record of the source data preserved beyond the log of the transaction itself. In addition to protecting data in transit, Zscaler safeguards all SSL/TLS keys during inspection. (Refer to Figures 3 and 4 for how Zscaler inspects SSL/TLS-encrypted data. Read more about how Zscaler secures all data and all encryption keys here.[16])

15 https://www.zscaler.com/blogs/corporate/tls-13-busting-myths-and-debunking-fear-uncertainty-doubt

16 https://help.zscaler.com/zia/safeguarding-ssl-keys-and-data-collected-during-ssl-inspection

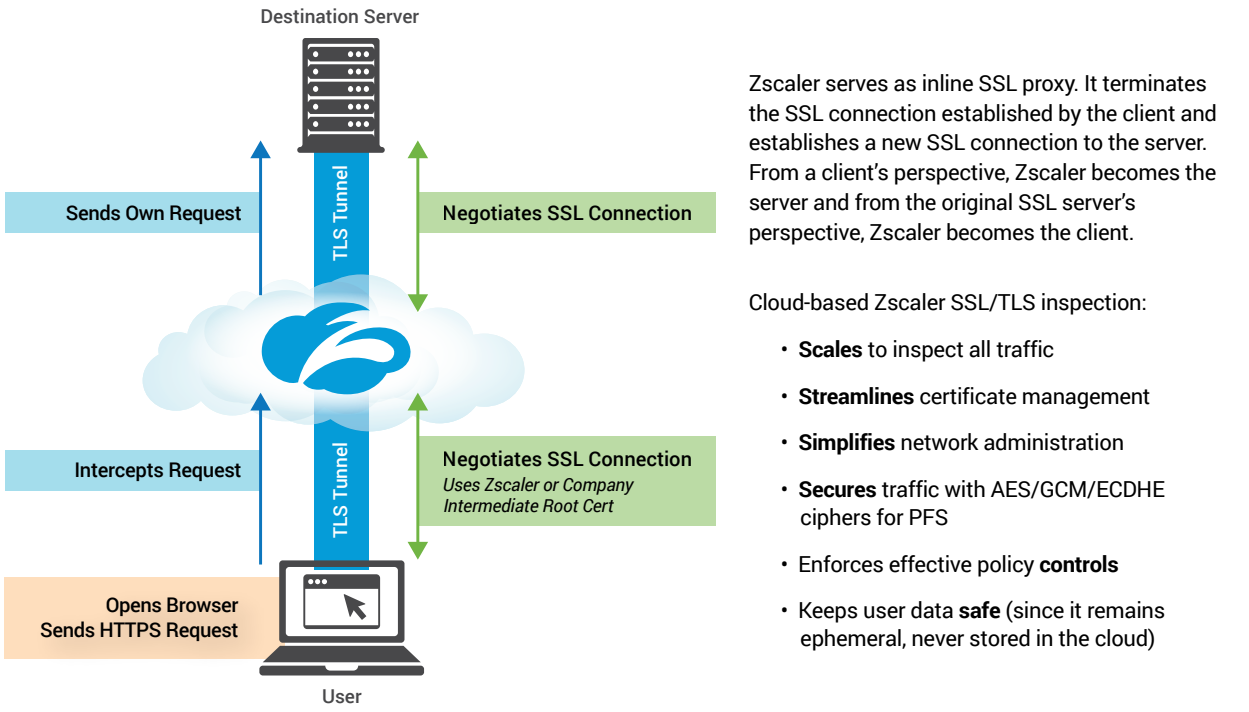


Figure 4. Inline proxy model for how Zscaler inspects SSL/TLS-encrypted data.[17]

It's helpful to look at the right to privacy as an outcome, and to review the way the outcome is achieved, rather than to disambiguate the individual steps that seemingly impact that outcome. Inspection of the traffic, and the binary result of block or not block, is not the same as accessing, monitoring, or storing the encrypted data.

Comprehensive SSL/TLS inspection strengthens an enterprise's GDPR and overall privacy compliance because it helps protect the privacy of the organization, the organization's employees, and the organization's assets. Without SSL/TLS inspection, the risk of exposing internal personal data/PII is higher, placing the organization at great risk of non-compliance.

17 https://help.zscaler.com/zia/about-ssl-inspection

Data-protection regulations support privacy *and* security

Data-privacy regulations—particularly European legislation like the GDPR,[18] the UK's Network and Information Systems Regulation 2018 (NIS)[19], and TKG[20]—were put in place to ensure organizations protect personal data while also preserving free and fair access to the internet. These regulations balance the rights of individuals with the requirements that corporate entities implement security measures to protect systems and data. For example, the TKG regulations require organizations to apply "protective technical precautions[21]" to prevent data loss and fend off external attack. The NIS explicitly states that an organization must have appropriate security measures in place to ensure that systems (and the data within them) cannot be compromised. And Article 5 of the GDPR[22] states that those organizations must process data

> *...in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.*

Moreover, GDPR Article 32 (Security of Processing) imposes an affirmative obligation on organizations to implement security measures for the processing of personal data that "ensure a level of security appropriate to the risk." SSL/TLS inspections are highly "appropriate," given the magnitude of the security risks they are aimed at mitigating.

Threats lurk in encrypted traffic. Without inspection, there's no way an enterprise can distinguish between "good" and "bad" SSL/TLS-encrypted data. No enterprise can fulfill both the privacy and security mandates of the TKG, NIS, and GDPR—let alone protect its employees and corporate interests—without comprehensive inspection of encrypted data traffic.

Takeaways: How to implement SSL/TLS inspection in your enterprise

The security and data-protection justifications for SSL/TLS inspection in the enterprise are sound and beyond reproach. IT leaders must employ SSL/TLS inspection to protect their organization's data, employees, and assets—Failure to do so can lead to irreparable harm, and even constitute dereliction of duty.

---

18 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-gdpr/

19 http://www.legislation.gov.uk/uksi/2018/506/contents

20 https://germanlawarchive.iuscomp.org/?p=692

21 https://germanlawarchive.iuscomp.org/?p=692#87

22 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1807-1-1

IT leaders that want to introduce SSL/TLS inspection into their organization must take into account several important considerations:

1. **Inform employees.**
   - Ensure that a valid AUP is in place and that its policies are enforced at the proxy/content filter.
   - Ensure that the AUP is explicitly agreed to by all employees, usually via their employment agreement.
   - Ensure employees are made aware of what constitutes personal data and how long it is preserved by the organization.
   - Ensure employees are notified exactly what data is being inspected so that they can make informed decisions about what they do when using corporate resources.
   - Obtain the agreement and support from workers' councils and/or unions, demonstrating that SSL/TLS inspection is actually also for the benefit of employees.
   - Socialize what is being done, and how it is being done.

2. **Choose a lawful basis for processing data under the GDPR.** The regulation is not the enemy here—if an enterprise is subject to the NIS or similar, the lawful basis is "legal obligation." And as noted earlier, an enterprise has a "legitimate interest" in protecting the organization and its assets.

3. **Obtain legal and privacy advice from in-house team or outside experts, but be prepared to argue points.** For instance, some lawyers and privacy professionals may not fully understand the services being provided by vendors, or have the technical perspective to judge whether security measures are appropriate to the risk.

4. **Ensure processes and controls are effective and appropriate.**
   - Obfuscate or otherwise hide data from regular users; ensure it is available only on a "need-to-know" basis.
   - Ensure that there is rigor and a documented process to review personal data.
   - Review and enforce this workflow on a regular basis.
   - Keep data for the designated time period, and delete it afterwards.
   - Keep the data safe while the enterprise has it.

SSL/TLS inspection: the right way to ensure regulatory compliance

SSL/TLS inspection represents the "appropriate security measures" to protect the privacy of the enterprise, the enterprise's employees, and the enterprise's assets. SSL/TLS inspection shields organizations from threat of attack while also balancing individual privacy rights, and in that way, strengthens those organizations' regulatory compliance.

Encrypted threats are tangible, destructive, virulent, and growing (exponentially) in volume. Enterprise IT leaders who choose not to decrypt traffic put both their users' privacy and their enterprise's assets at risk, while also risking non-compliance with various data protection regulations. In this modern age, IT leaders must employ SSL/TLS inspection to combat security risks to the enterprise and preserve the privacy of their employees and users.

About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.