TLS/SSL Inspection with Zscaler Internet Access™

Reference Architecture

Contents

About Zscaler Reference Architectures Guides

The Zscaler™ Reference Architecture series delivers best practices based on real-world deployments. The recommendations in this series were developed by Zscaler's transformation experts from across the company.

Each guide steers you through the architecture process and provides technical deep dives into specific platform functionality and integrations.

The Zscaler Reference Architecture series is designed to be modular. Each guide shows you how to configure a different aspect of the platform. You can use only the guides that you need to meet your specific policy goals.

Who is this guide for?

The Overview portion of this guide is suitable for all audiences. It provides a brief refresher on the platform features and integrations being covered. A summary of the design follows, along with a consolidated summary of recommendations.

The rest of the document is written with a technical reader in mind, covering detailed information on the recommendations and the architecture process. For configuration steps, we provide links to the appropriate Zscaler Help site articles or configuration steps on integration partner sites.

A note for Federal Cloud customers

This series assumes you are a Zscaler public cloud customer. If you are a Federal Cloud user, please check with your Zscaler account team on feature availability and configuration requirements.

Conventions used in this guide

The product name ZIA Service Edge is used as a reference to the following Zscaler products: ZIA Public Service Edge, ZIA Private Service Edge, and ZIA Virtual Service Edge. Any reference to ZIA Service Edge means that the features and functions being discussed are applicable to all three products. Similarly, ZPA Service Edge is used to represent ZPA Public Service Edge and ZPA Private Service Edge where the discussion applies to both products.

Notes call out important information that you need to complete your design and implementation.

Warnings indicate that a configuration could be risky. Read the warnings carefully and exercise caution before making your configuration changes.

Finding out more

You can find our guides on the **Zscaler website** (**https://www.zscaler.com/resources/reference-architectures**).

You can join our user and partner community and get answers to your questions in the **Zenith Community** (**https://community.zscaler.com**).

Terms and acronyms used in this guide

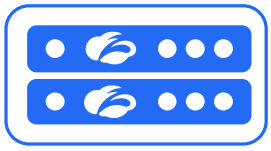
Acronym	Definition
ZIA	Zscaler Internet Access
ZPA	Zscaler Private Access
ZDX	Zscaler Digital Experience
ZTE	Zero Trust Exchange
AUP	Acceptable Use Policy
BYOD	Bring Your Own Device
CA	certificate authority
CSR	certificate signing request
DC	Data Center
DPA	Data Processor Agreement
FQDN	Fully Qualified Domain Name
GRE	Generic Routed Encapsulation
IPS	intrusion prevention system
IPSec	Internet Protocol Security
OCSP	Online Certificate Status Protocol
PII	personally identifiable information
QUIC	Quick UDP Internet Connections
SSL	Secure Socket Layer (superseded by TLS)
TLS	Transport Layer Security
URI	Uniform Resource Identifier

Icons used in this guide

The following icons are used in the diagrams contained in this guide.

Zscaler Zero Trust Exchange

ZIA or ZPA Service Edge



Public CA Certificate

Zscaler Issued Certificate

Public or Private Cloud

Internet

Generic Application or Workload

Laptop

Data Tunnel

Introduction

The use of encryption to protect internet traffic has grown significantly over the last decade. HTTPS used to be used only for transactions where the risks were deemed high enough to justify the investment in security. The use of Transport Layer Security (TLS), formerly Secure Socket Layer (SSL), is the primary mechanism used to protect client-to-server traffic. There are several factors that have contributed to this increase.

Campaigns such as HTTPS Everywhere (https://www.eff.org/https-everywhere) publicly championed the use of encryption for privacy and security. News coverage of attacks by individual threat actors and nation states who monitor internet traffic is now a regular occurrence. This is combined with the availability of free, short-lived certificates that make it simple for websites and applications to enable encryption. Together, these forces contribute steadily towards a 100% encrypted internet.

While encryption is a benefit to both the user and the business, it presents challenges to inspecting data traffic for malicious content and data leakage. Security appliances are typically expected to handle only a small fraction of their traffic capacity when decryption is enabled. For this reason, TLS/SSL inspection has been done for only sensitive URLs. Unfortunately, this means that advanced analysis tools such as malware protection, sandbox, and other features can't inspect that encrypted traffic.

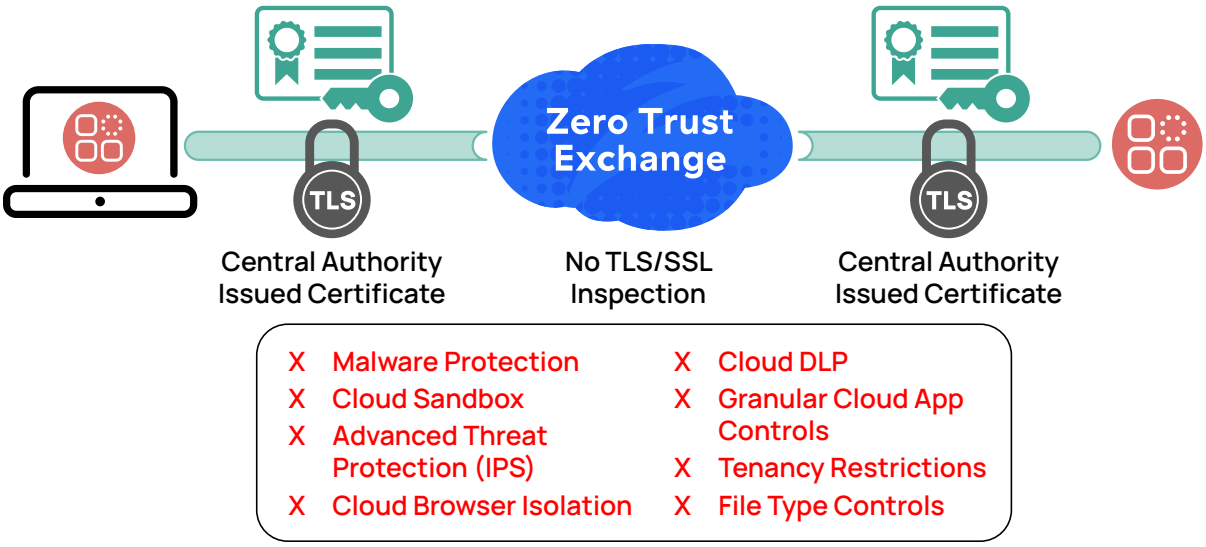


Figure 1. Without TLS/SSL inspection, many security functions are disabled

With Zscaler Internet Access (ZIA), inspection at scale is not a concern. The Zscaler Zero Trust Exchange™ (ZTE) is a platform built to handle full TLS/SSL inspection, based on an advanced proxy architecture. Zscaler recommends inspecting 100% of traffic to protect your users and your organization from threats hiding in encrypted channels.

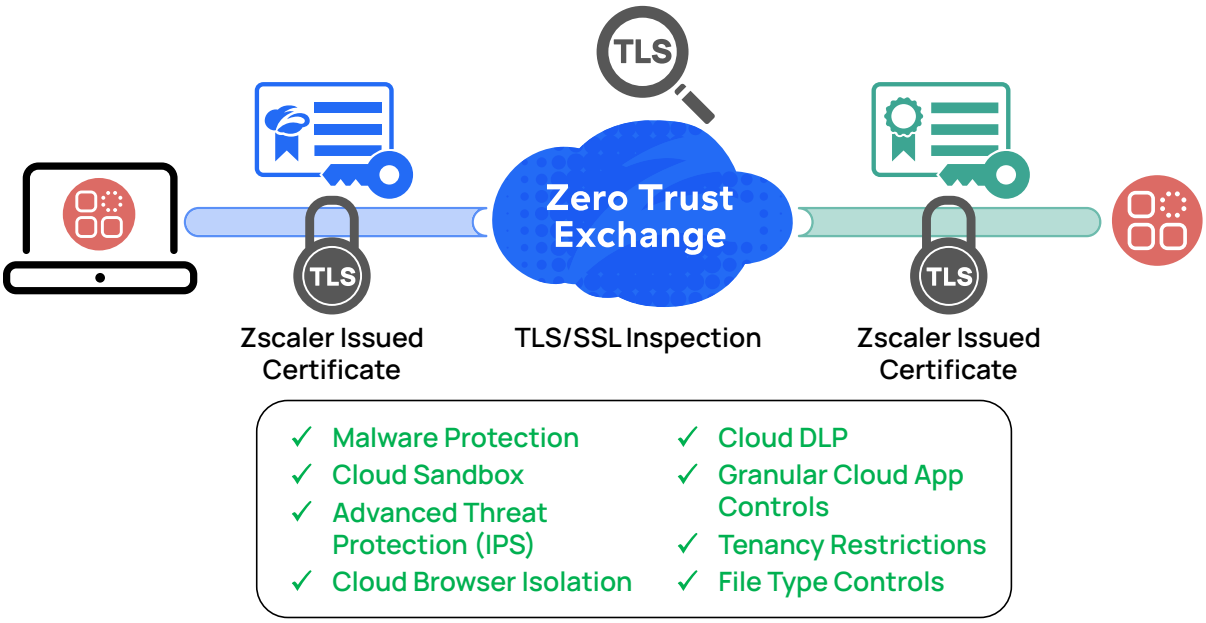


Figure 2. Zscaler TLS/SSL Inspection allows all your security subscriptions to be used on all traffic

By inspecting all traffic, you gain the benefits of the full ZTE platform. Without inspection, you are blind to many of the threats on the internet today. To realize the full value of your Zscaler subscription, you must decrypt and inspect TLS/SSL traffic. The following tools rely on decryption to perform their functions:

- In-line Malware Protection – Ransomware, antivirus, and spyware protection.
- Sandbox – Opening and checking files for embedded threats.
- Advanced Threat Protection (intrusion prevention system or IPS) – Monitor traffic flow watching for exploits.
- Browser Isolation – Remotely rendered web browsing.
- Data Loss Prevention – Prevent sensitive data from leaving the organization.
- Granular Cloud App Controls – Limits on actions, bandwidth, and time used.
- Tenancy Restrictions – No private accounts on services such as Microsoft 365™ (formerly Office 365).
- File Type Controls – Restrict the upload and download of various file types.

Inspecting all TLS/SSL traffic is critical to the safety and security of your users, organization, and assets. This level of visibility means that threats cannot hide by cloaking themselves in an encrypted data stream. You have visibility and control across the ZIA platform.

The product name ZIA Service Edge is used as a reference to the following Zscaler products: ZIA Public Service Edge, ZIA Private Service Edge, and ZIA Virtual Service Edge. Any reference to ZIA Service Edge means that the features and functions being discussed are applicable to all three products.

New to TLS/SSL Inspection?

- If you are new to TLS/SSL Inspection, or just want a quick refresher, read this short introduction at What is SSL Inspection (https://www.zscaler.com/resources/security-terms-glossary/what-is-ssl-inspection).
- To explain TLS/SSL Inspection at the executive level of your organization, leverage our whitepaper Encryption, Privacy, & Data Protection: A Balancing Act (https://www.zscaler.com/resources/white-papers/encryption-privacy-data-protection.pdf).
- For a current view of the threats facing organizations, read our ThreatLabZ whitepaper The State of Encrypted Attacks, 2021 (https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks).
- For a gentle introduction to cryptography, certificates, and public key encryption, we recommend the book *Cryptography Decrypted 1st Edition* by H. Mel & Doris Baker.

Solution Overview

Inspecting TLS/SSL at scale is moving from organizational wish list to business requirement. Effectively defending your organization requires inspection of encrypted traffic. In this chapter, we'll see how threats to your organization move behind encrypted channels along with almost all other data traffic. We'll look at what interception does at the ZIA Service Edge. Then we'll layout the roadmap for the rest of this guide.

Threats in encrypted traffic

Internet encryption levels continue to rise year after year. There are many contributing factors, including increased awareness by the public of threats, disruptive attacks by threat actors including nation states, and the advent of free, short-lived certificates. In 2021, Zscaler continued to see growth in encrypted traffic across our platform. Our transaction reporting, along with that of Google and Firefox, often reveals encryption internet wide at 90+%.

Alongside this growth and democratization of encryption is an increasing number of threats. Attackers know the limitations of hardware solutions to decrypt TLS/SSL and use those limitations to hide their malicious payloads. For the first nine months of 2021, Zscaler blocked 20.7 billion threats over encrypted channels, with the primary threat being malware. This was a 314% increase over the same time in 2020.

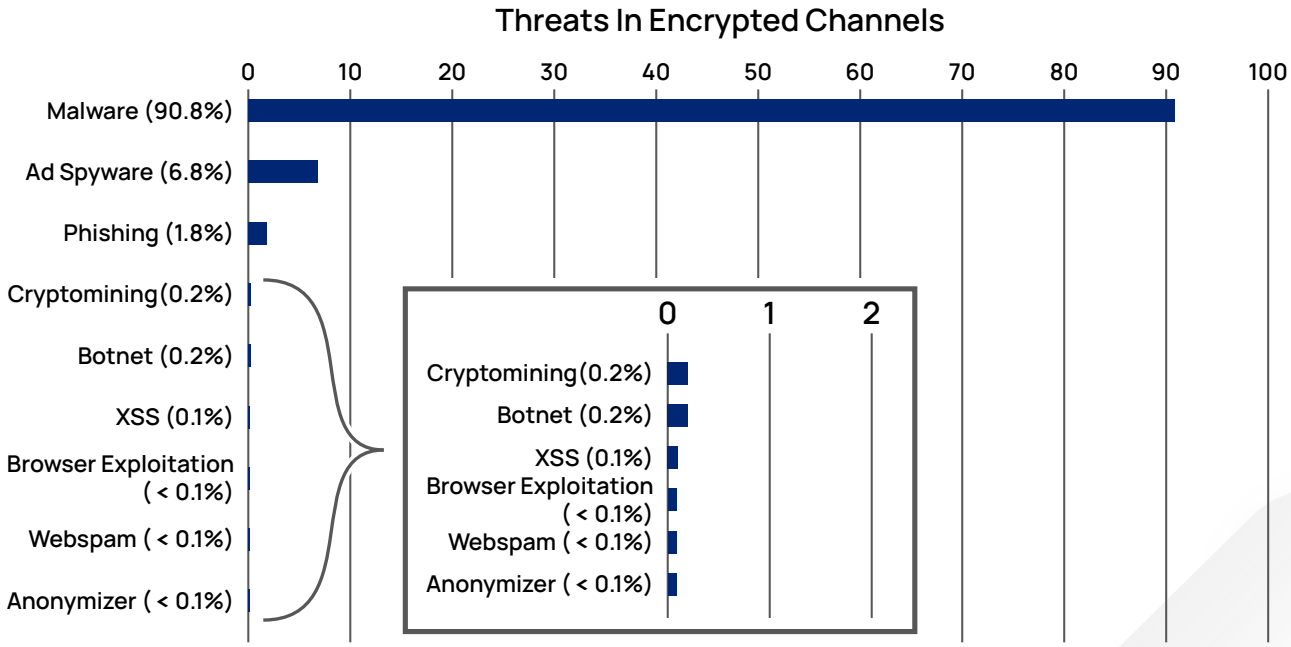


Figure 3. A view of threats hiding in encrypted channels

Threat actors know that most organizations do not have the capacity to scan most of their encrypted traffic, much less all of it. Threat actors also realize that user agents trust the freely available certificates from organizations such as Let's Encrypt (https://letsencrypt.org/). Many of these certificates require little to no user validation. Certificates offer a sense of legitimacy because users often know to look for the certificate lock symbol in their browser. However, the same users often do not know how to dissect the URL or read a certificate to check its legitimacy. Certificates are not an indicator that the site or its contents are safe.

There is also a widespread belief that if you aren't that important, the attackers will find a more interesting target. The truth is that these threats target every industry at every scale.

Serious threats are launched by sophisticated threat actors and nation states with specific targets. The Solar Winds supply chain attacks that hit the tech industry in 2020 is a prime example. These attacks look to gather information or disable systems, install their software, and remain undetected for some time despite reports of spurious traffic from the affected products. These kinds of attacks are highly targeted with a specific goal in mind, such as disruption of gas supplies or industrial espionage.

Attacks can also be indiscriminate and opportunistic in nature. The attacker might not even know how the attack really works. They are often looking for unpatched systems with off-the-shelf or rented tool sets. These attacks by unsophisticated users are often launched in the hopes of earning a payout from the victim, rather than any moral or political goals.

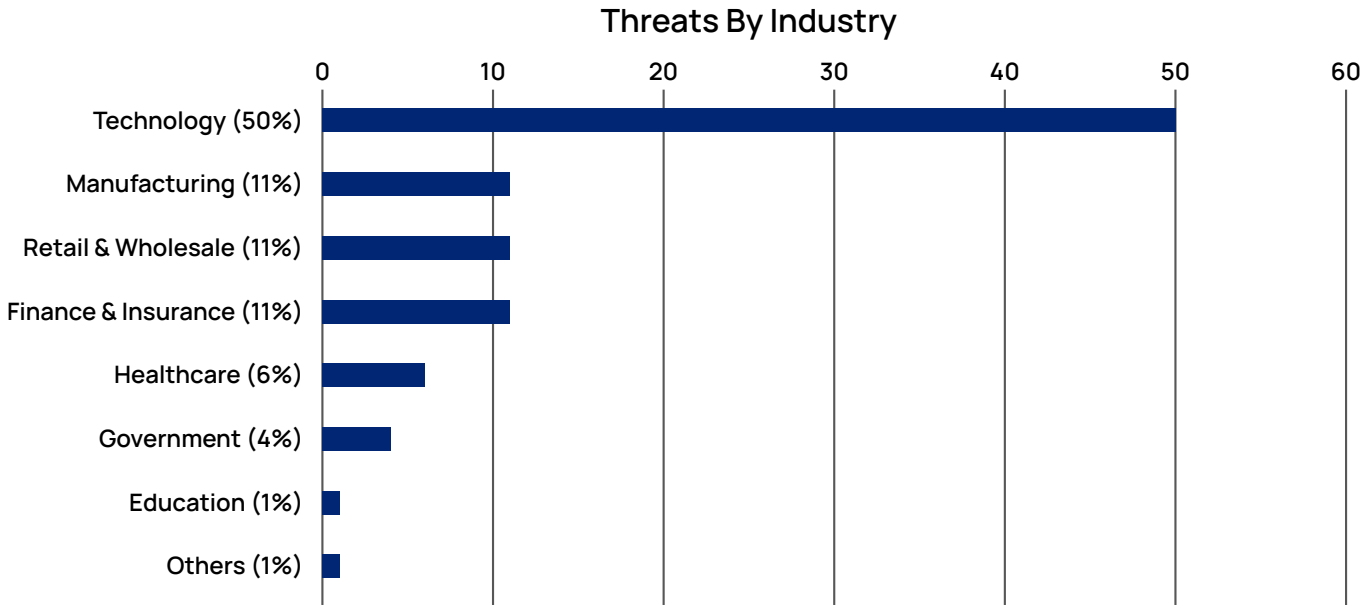


Figure 4. Threats by industry as reported in Zscaler's whitepaper The State of Encrypted Attacks 2021

No matter who you are or what business your organization is in, you could be the target of an attack. Therefore, it is critical that you know what's coming in and what's going out of your organization. Without this visibility, you are missing many of the threats launched against your organization. Compare the data for a connection without TLS/SSL inspection on the left, and with inspection on the right in the following image.

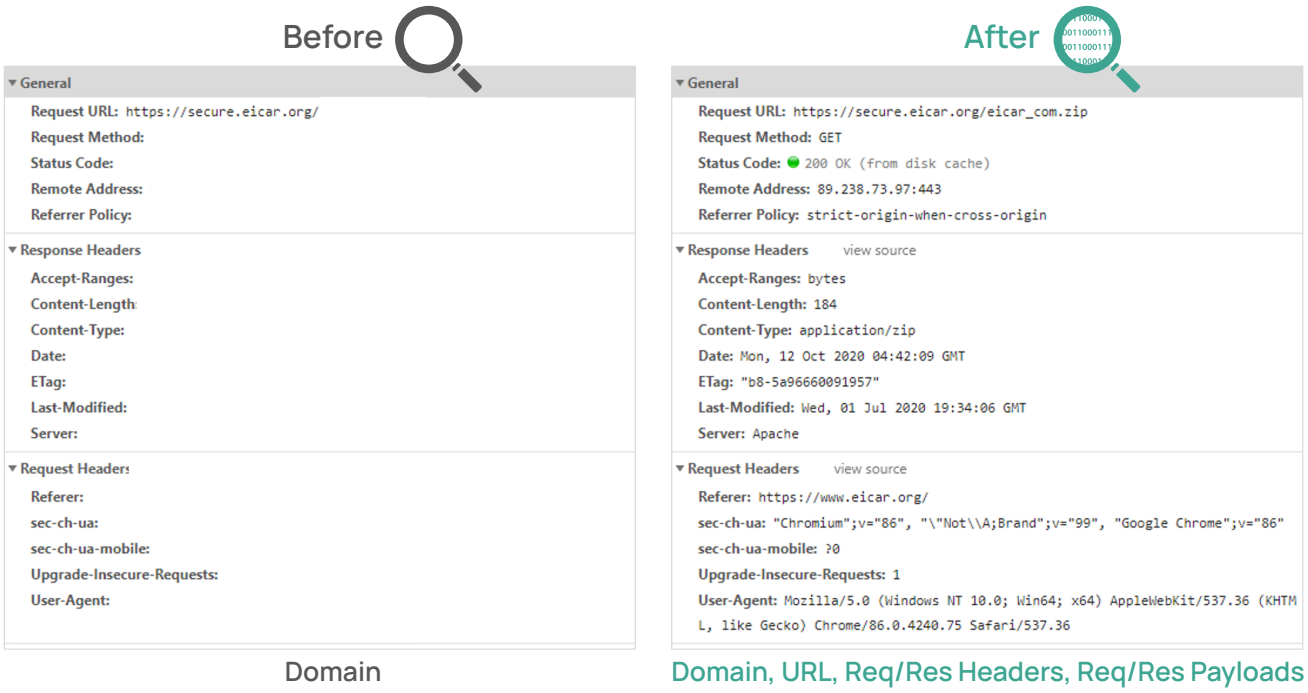


Figure 5. The difference in visibility before and after TSL/SSL inspection

Without TLS/SSL inspection, most of what occurs inside a transaction is hidden. This is critical data that can mean the difference between an attack succeeding or failing.

How TLS/SSL inspection functions

Encrypting traffic using TLS/SSL involves the use of certificates containing public keys and corresponding private keys held by the server. This system allows users to communicate with remote servers without first having to share keys. Typically, the authentication process occurs directly between your client machine and the application you are trying to access.

Key to your understanding of this workflow is that Public-key Cryptography uses two keys. The first, a public key, is shared freely and embedded within a certificate. The second, the private key, is kept private by the server or user. The two types of keys together are used to encrypt and decrypt data. The method is designed so that data encrypted with one key can only be decrypted with the other key.

If someone sends you a letter encrypted with your public key, only your private key can decrypt it. However if you encrypt something with your private key, anyone with your public key can decrypt it. Let's look at an example of how a TLS tunnel is established without Zscaler inspection.

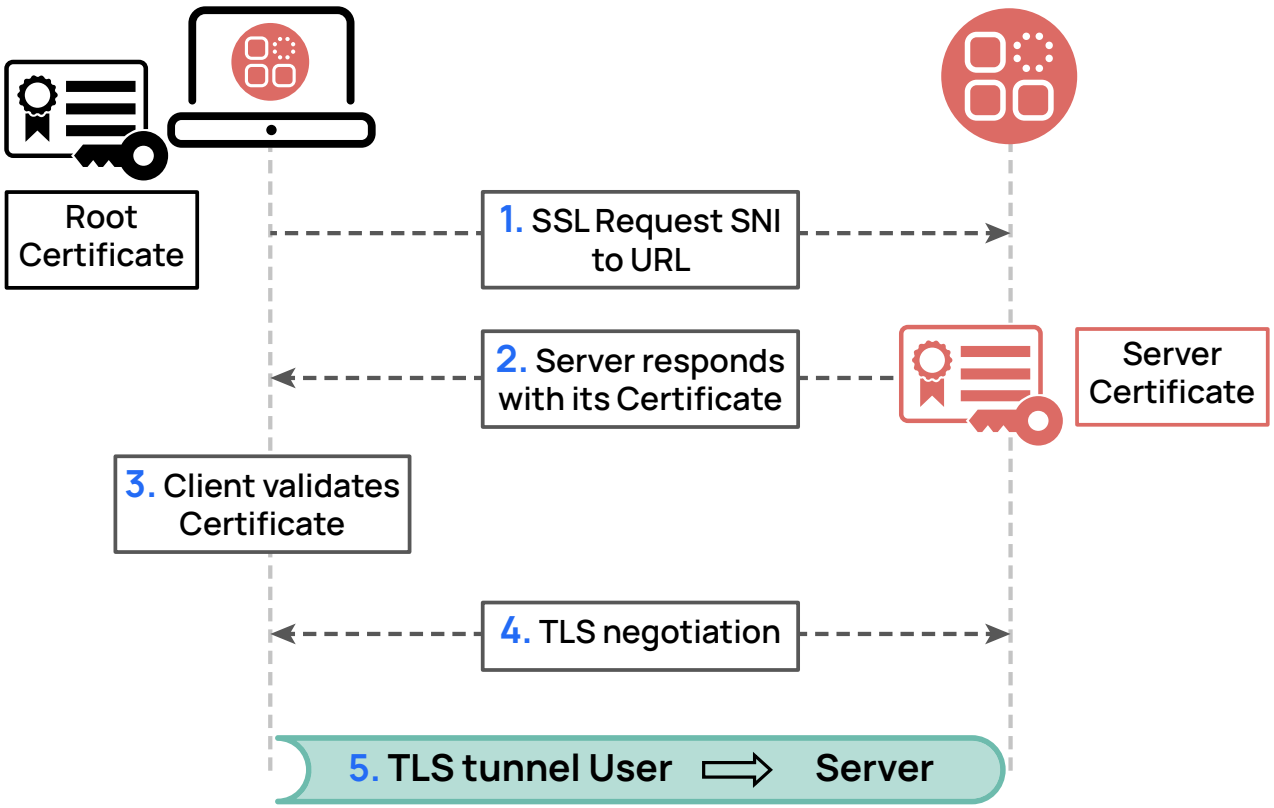


Figure 6. TLS tunnel setup

1. The user opens a browser and requests a URL using HTTPS to the server.
2. The server responds with its public certificate containing its public key. The CA issuing the certificate creates a hash of the certificate data, which it then encrypts with its private key. The system also sends across keying information for tunnel setup.
3. The user's machine checks that the server or app name matches the name on the certificate, and that the certificate has not expired. The user's machine decrypts this hash using the CA's public key, which is preloaded in the device's local certificate store, and then creates its own hash of the certificate and compares the two values. Trusted root CA certificates are preloaded by the operating and browser vendors, so there is no need to manually install these certificates. The comparison of the provided and locally generated hash values verify that:
    a. The CA has issued the certificate because its public key decrypts the hash value.
    b. The certificate has not changed since it was issued because its hash value matches the hash on the certificate after decryption.
4. If the certificate is valid, the machine responds with its own keying information, this time encrypted using the server's public key. Only the server with its private key can decrypt that file. If the certificate is not valid, the connection is dropped.
5. Using the previously established keys combined within the message exchange, TLS negotiation occurs, and the tunnel is formed between client and server.

This connection is what occurs when we are shopping or banking online. The connection is secured via encryption, and we are protected against inspection. It requires no key exchanges beforehand, and the user does not need a certificate to verify and interact with the server. An observer might be able to see that we are sending traffic, and its high-level destination, but all other content is hidden within the encrypted channel.

Certificates and keys are our trust mechanisms. The keys must be generated securely and managed carefully to avoid breaches. We trust the certificate authority (CA) who issued the certificate to the server by signing the server's public key with the CA's private key. Our machine has the public key for the CA already, either at the machine, browser, or application level because the public key is pre-installed by OS and application developers.

When ZIA Service Edge intercepts traffic for inspection with ZIA, we must continue the trust between the public and private keys. This is achieved by installing a trusted certificate for Zscaler's CA on client machines. The Zscaler certificate allows the clients to trust the Zscaler CA for these transactions. Let's look at the same transaction, but this time with the ZIA Service Edge inspecting the TLS/SSL connection.

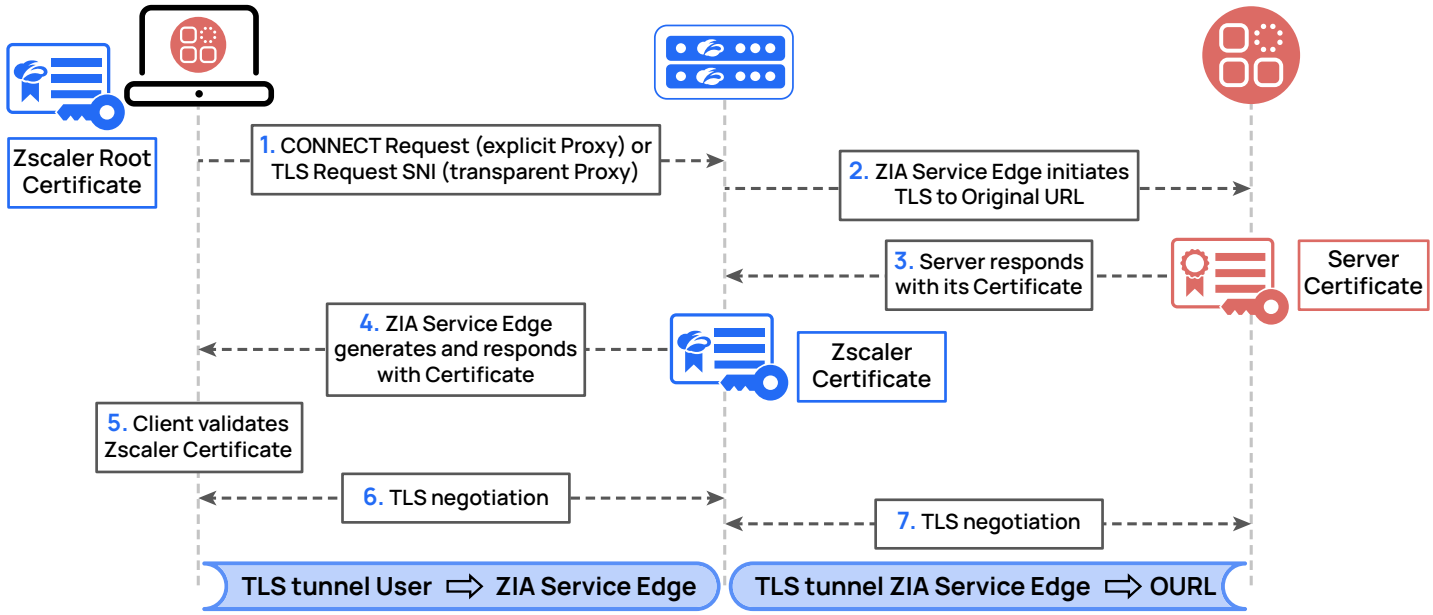


Figure 7. How TLS/SSL inspection differs from a standard TLS connection setup

1. The user sends a connection request. The request is sent to the nearest ZIA Service Edge, or transparently if all traffic is automatically proxied to ZIA by an edge router.
2. The ZIA Service Edge receives the request and opens its own connection to the original server on behalf of the user.
3. The server responds with its public certificate and an encrypted key that can be decrypted with the public certificate.
4. The ZIA Service Edge validates the server's certificate. This is the same set of checks that the client machine did above for valid date, hash decryption, and validation. If the certificate is found to be valid, the ZIA Service Edge generates a certificate to represent that server to the client and sends this new certificate back to the user's machine. This new certificate is signed by the Zscaler intermediate CA.
5. The user's machine validates the certificate using the Zscaler root certificate because Zscaler issued the certificate. The machine responds with an encryption key, encrypted using the Zscaler's public key.
6. The user's machine negotiates the setup of a TLS tunnel with the ZIA Service Edge.
7. Separately, the ZIA Service Edge negotiates the setup of a TLS tunnel with the original server.

The ZIA Service Edge is now in the middle of the connection. It is decrypting the traffic, running ZIA's inspection engines against the traffic, and re-encrypting the traffic between the user's device and the server. ZIA inspects your traffic and enforces policy as if encryption weren't in use.

Certificates in the preceding example are using Zscaler-generated certificates. ZIA can also act as a subordinate to your existing infrastructure if you prefer to use your own certificates. We'll cover more on certificates and certificate authorities in Phase 2: Enroll a Root Certificate Authority (CA) later in this guide.

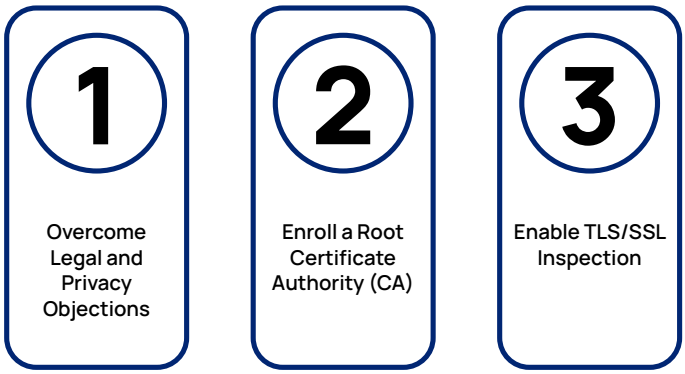
Zscaler invests heavily in testing and securing our own platform. Access to all infrastructure components including the Zscaler Central Authority and ZIA Service Edge platforms is highly restricted and controlled. All systems are monitored 24 hours a day. Zscaler is committed to keeping customer data secure from attacks, both virtual and physical.

When we handle your encryption keys, we take additional precautions to ensure that the keys are stored and deleted in a secure manner. Keys are never written to disk at the ZIA Service Edge and are overwritten before being deleted.

You can read more about Zscaler's security certifications at Compliance (https://www.zscaler.com/platform/privacy-and-compliance).

The TLS/SSL inspection journey

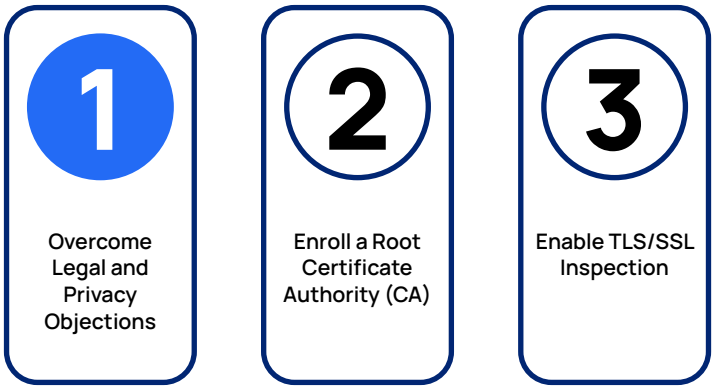
Inspecting TLS/SSL significantly changes your user's perception of data privacy within the organization. Even if you already perform some limited inspection, full inspection happens in stages. Inspecting encrypted traffic requires some additional education for your organization.



1. **Phase 1: Overcome Legal and Privacy Objections** – In this section, we discuss why inspecting TLS/SSL is critical to keeping your users and organization safe. Your users must understand that inspection is about protection and not about spying on their activities. At the end, you should have an Acceptable Use Policy (AUP) that everyone agrees on.
2. **Phase 2: Enroll a Root Certificate Authority (CA)** – For inspection to work, your users must trust the Zscaler certificate. Decide if you are going to use a Zscaler certificate or make Zscaler an extension of your certificate authority.
3. **Phase 3: Enable TLS/SSL Inspection** – Start by deploying TLS/SSL inspection with a limited group to refine your policy and notifications. Continue to expand to all users and all traffic per your rollout plan. Analyze and remediate tools with poor encryption support.

As we work through this guide, we will discuss each stage in the framework in more detail. We encourage you to proceed to the next chapter on legal and privacy considerations. Everyone in your organization should understand the requirements and responsibilities of inspection.

Phase 1: Overcome Legal and Privacy Objections



Both news headlines and statistics around data breaches reflect the need to inspect encrypted traffic. The threats are inside encrypted payloads, and the tools to detect those threats need visibility to that payload to do their jobs. You must inspect encrypted traffic to protect your users and your organization.

Ironically, the success of security awareness campaigns, stories of identity theft, and a user's sense of their own privacy can complicate the rollout. This is especially true in countries with strong regulations around an employee's right to privacy while in the workplace.

The tension between inspecting data and data privacy can be alleviated through clear, consistent communication. Your IT staff, CISO, CIO, legal team, and workers' council all have a role to play. Everyone in the organization needs to be trained on what inspection is and what it is not. Your organization must negotiate an Acceptable Use Policy (AUP) that details who can access data and data obfuscation for admins and provides a clear process for exceptions and technical issues.

In this section, we'll focus on specific actions to help your users understand the balance of inspection and privacy.

Zscaler Data Processor Agreement (DPA) and data privacy

Your discussions about TLS/SSL inspection center around access to your organizational data and personally identifiable information (PII). With the advent of GDPR in the European Union and other similar legislation around the world, many users are now more well versed in data processing protections. Zscaler acts as a data processor for your organization.

In support of data privacy, Zscaler offers a series of documents and websites to help you better understand what data we are collecting and how it is used.

When you subscribe to ZIA, you enter into a Data Processor Agreement (DPA). This agreement describes what data Zscaler has access to and how it is handled.

- The Zscaler Data Processing Agreement (https://www.zscaler.com/resources/legal/zscaler-data-processing-agreement.pdf)

Zscaler publishes its privacy policy online for anyone to access. This policy details what information Zscaler has access to as a normal part of providing the service to you.

- The Zscaler Privacy Policy (https://www.zscaler.com/privacy-compliance/privacy-policy)

Zscaler is compliant with many regulatory privacy requirements. Our privacy and compliance pages contain links to specific regulatory information.

- For more information about privacy, see Compliance (https://www.zscaler.com/industries/privacy-and-compliance)

Develop an Acceptable Use Policy

Before any formal communications begin, you must develop a policy and privacy framework based on updates to both your current AUP and data privacy policies. When reviewing proposed policy updates, make sure to call out policy differences, such as previous hardware limitations versus desired policy outcome.

You can view the Zscaler product Acceptable Use Policy (https://www.zscaler.com/legal/acceptable-use-policy). This agreement constitutes acceptable use of our service. You will develop a similar framework for your organization, tailored to your specific needs.

Having a clearly defined policy framework and privacy control for discussion is a must when communicating policy and privacy changes to your users. The framework also serves as a starting point for discussion with workers' councils and unions. Involve multiple groups in development of the policy, such as:

- Legal department
- Privacy and compliance
- CIO and/or CISO
- Workers' council or union

The outcome of these discussions is an updated policy document that enables full TLS/SSL inspection. When developing your acceptable use policy, you should strive for 100% of traffic to be inspected. Zscaler strongly recommends that you take position as a starting point. Make exceptions only when required by regulation, vendor recommendation, or contractual agreement.

Zscaler recommends that the goal for TLS/SSL inspection is 100% of traffic inspected.

ZIA supports an AUP notification that allows you to log when a user accepts the policy. You can also set the frequency from none to per session, depending on your regulatory and governance needs. Consult with your legal team on the frequency and triggers for displaying the AUP acceptance notification. You can read more about displaying the AUP acceptance and logging for users at Configuring the Acceptable Use Policy (https://help.zscaler.com/zia/configuring-acceptable-use-policy).

Explaining inspection to your users

When you set out to inspect TLS/SSL, you must clearly explain what your intentions are to everyone in your organization. Looking into a user's encrypted traffic comes with many questions and concerns. Your users will want to know what you are looking for, how their data is protected, and how inspection aligns with workers' protections.

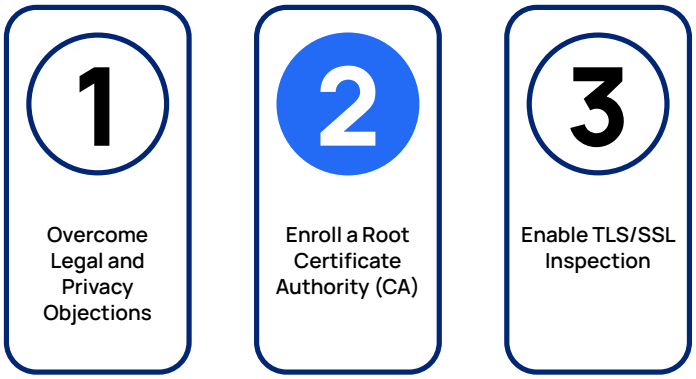
When first implementing the policy and privacy change, it is recommended to hold training sessions for your users. You likely have security awareness training in your organization, and policy and privacy should be viewed as an extension of that. Zscaler has developed two whitepapers you can use as the basis of your training to share with your users.

The first whitepaper is focused on business risk and makes the case for TLS/SSL inspection: Encryption, Privacy, & Data Protection: A Balancing Act (https://www.zscaler.com/resources/white-papers/encryption-privacy-data-protection.pdf).

The second whitepaper was developed by Zscaler's in-house security research team ThreatLabZ. This paper reviews security threat trends for the first nine months of 2021: The State of Encrypted Attacks, 2021 (https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks).

These resources help your users understand the risks of not inspecting traffic. Helping your users get comfortable with their traffic being scanned for their own protection is critical to a smooth transition. In the next chapter, we'll look at certificates and certificate authorities.

Phase 2: Enroll a Root Certificate Authority (CA)



Certificates play a critical role in securing web applications by confirming the validity of the applications. The certificate is trusted by a user's device because of a chain of trust links that show the server certificate's relationship to a trusted certificate authority. The information contained in the certificate allows for the setup of secure connections with TLS/SSL using public-key encryption.

In this chapter, we'll discuss how certificates and key handling happen within the ZIA platform. You'll decide between using Zscaler's Certificate Authority (CA), or your own existing CA with Zscaler as an intermediary CA. We will also discuss uploading the root CA certificate and trust chain, as well as rotating certificates.

Using your existing CA is an additional subscription with Zscaler.

Understanding certificate trust chains

Certificates are mechanisms for distributing a server's public key. A certificate contains fields relating to its validity. Key fields include the organization name, DNS server names, certificate start and end dates, and most importantly the server's public key string. The issuer of the certificate signs the certificate using its private key, and the client decrypts the signature using the CA's public key.

In nearly all cases, the root CA does not sign the end certificate directly. Instead, the root CA signs the certificate of an intermediary CA that is authorized to issue certificates on the root's behalf. The intermediary allows the root CA to be highly secured and even taken offline, because the intermediary handles the day-to-day work of issuing certificates. More than one layer of intermediate CAs can exist, with one intermediate CA signing the certificate of a second-level intermediate CA. The final intermediate CA issues the certificates to the server at the end of the certificate chain.

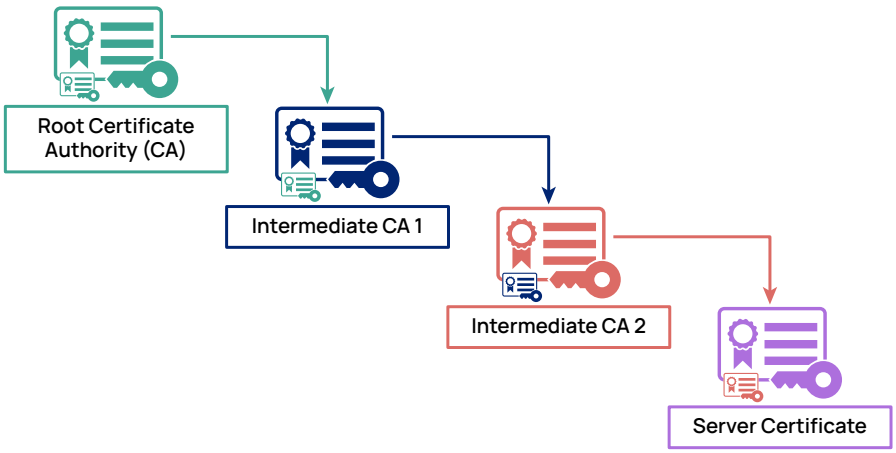


Figure 8. Certificate chain of trust relies on tracing signatures to a trusted root CA

At each level of the chain, the certificate in use is signed by the next higher-level CA. The client machine can validate a certificate by following the chain to the root CA. Using the root CA certificate, the client machine can then authenticate the signing of the intermediate CA's certificate. The authentication continues down the chain until the final server certificate is checked. If all signatures are in place, the certificate can be trusted as having been issued by a trusted CA.

In ZIA, the Central Authority is a private Certificate Authority, acting as both root and intermediary CA for the ZIA platform, or as an intermediary to your private Certificate Authority. The Central Authority authorizes the ZIA Service Edges to act as intermediary CAs, issuing certificates to end users for their requested destinations.

Certificate use in ZIA

Certificates are used in a different manner in a TLS/SSL inspection scenario. In normal operation, a certificate is issued to a server to enable encryption and prevent interception. The server certificate is issued by a CA that the user's device, application, or browser trusts. The root CA certificates for many common, trusted public CAs come preloaded.

Generally preventing interception is what we want. Having a third party be able to impersonate a legitimate service with a valid certificate allows the impersonator to see into the transactions. When a legitimate TLS/SSL inspection occurs, impersonating all the destinations a user wants to visit is exactly what happens. The ZIA proxy must sit in the traffic flow and must present itself as the legitimate service the user is attempting to reach.

To do this, the ZIA Service Edge acts as a short-lived intermediate CA. As a user requests a connection, the ZIA Service Edge issues certificates on demand for the application. From the browser's point of view, the ZIA Service Edge certificate is valid for the destination. This is because the user or administrator imported the ZIA Service Edge trust chain into the device's certificate store. Let's look at which certificates go where in the system.

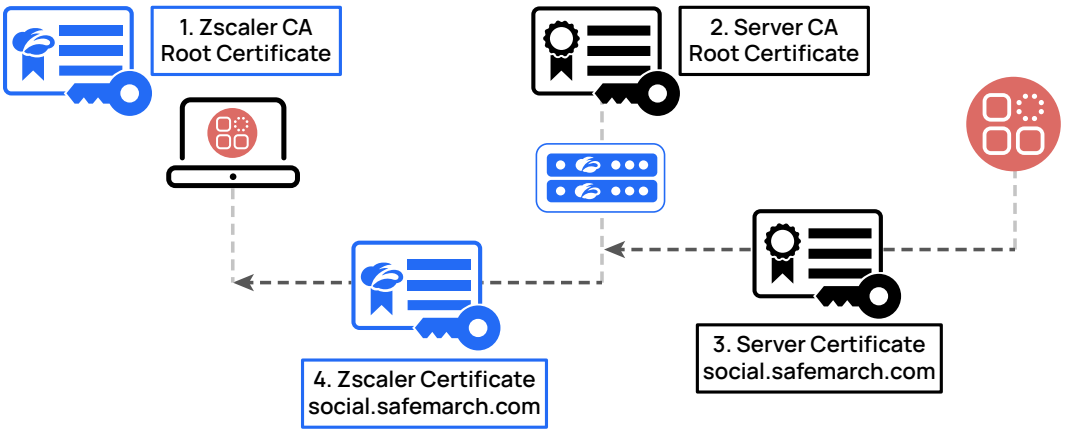


Figure 9. The ZIA Service Edge acts as an intermediate CA issuing certificates on demand for web traffic

In our earlier discussion, we went over how TLS/SSL encryption is setup. Now we'll look at the certificates that are used directly.

1. The client machine is installed with the root certificate that is used to validate all ZIA Service Edge generated certificates.
2. The ZIA Service Edge also has root CAs for common certificate providers pre-installed. Much like your client machine and browsers, Zscaler ensures the ZIA Service Edge is updated with major certificate providers' root certificates.
3. When a request is made to a server such as *social.safemarch.com*, the server responds with its server certificate. This server is signed by the root CA that issued the certificate.
4. The ZIA Service Edge validates the certificate, then generates a short-lived wildcard certificate for that service.

This chain of trust actions allows the client machine to receive a valid certificate to build a tunnel to the ZIA Service Edge. As far as the client is concerned, the ZIA Service Edge is the service the client was originally trying to reach.

Key generation

When you generate a new certificate signing request (CSR) in the Zscaler Central Authority, the system generates both private and public keys with a key strength of 2048 bits. The key is then immediately encrypted using AES and stored within the Zscaler Central Authority database. This SQL database also stores your other policy rules and is only accessible by admins with authorized credentials for your organization.

Key storage and lifetimes

ZIA issues certificates on behalf of other services and handles keys in a secure fashion, both while in use and when it's time for the keys to be removed. The Zscaler Central Authority does not send keys to all ZIA Service Edges, but instead only to those servicing your users. The ZIA Service Edge keeps the key only in RAM. The key is never written to disk. Let's look at an example and review key management.

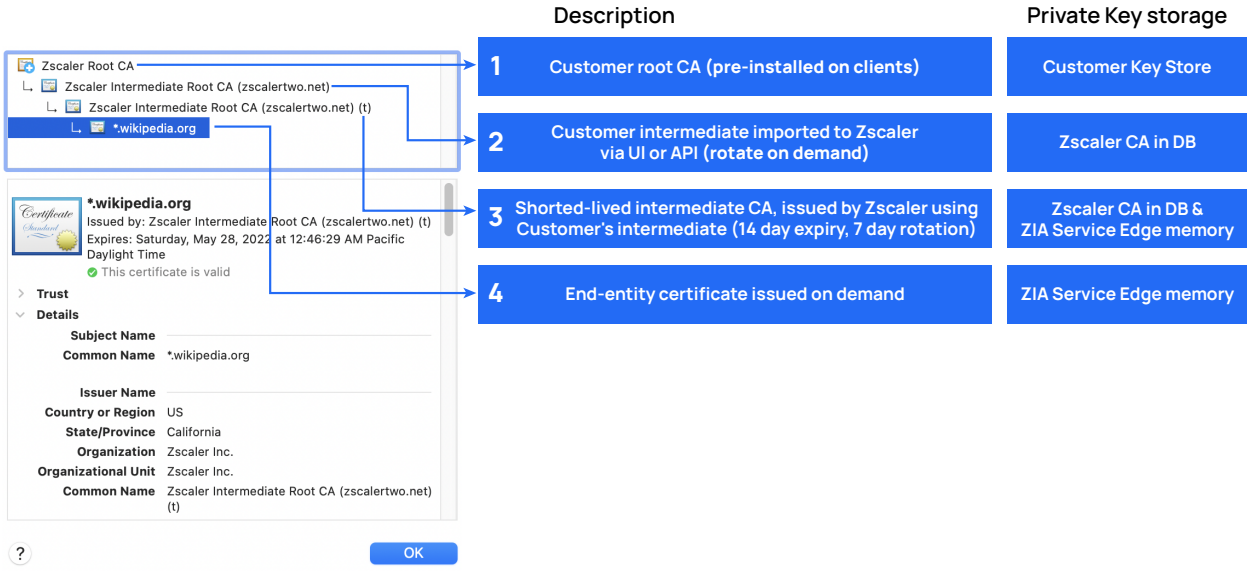


Figure 10. Certificate chain of trust breakdown

In this image, we see that the client attempted to reach Wikipedia. The client received a wildcard certificate for Wikipedia issued by the ZIA Service Edge. Because the client machine has the Zscaler Root CA installed, the client accepts the wildcard certificate as being valid. There are four components to the certificate we'll look at next.

1. **Root CA** – The root CA is the ultimate signing authority for the certificate chain. The root CA can be your own infrastructure or Zscaler's CA.
    a. This certificate's private keys are contained in your private key store if you use your own infrastructure.
    b. If you use Zscaler's CA, the keys are stored in the CA database. If you are using your own infrastructure, you enroll Zscaler as an intermediate CA.
2. **Intermediate CA certificate** – This next level down certificate does the work of issuing short-lived intermediate CA certificates to the ZIA Service Edge nodes.
    a. If you are using your own key store, you issue to Zscaler an intermediary certificate. The intermediary certificate can be rotated on demand and makes the ZIA Service Edge an intermediate CA for your infrastructure.
    b. If you are using Zscaler's CA, your certificate is issued by Zscaler. This certificate's private keys are stored in the Zscaler CA database.
3. **ZIA Service Edge Intermediate CA** – The Zscaler CA issues the ZIA Service a short-lived intermediary certificate. This certificate is used for issuing certificates for services, and is used for only 7 days and valid for only 14 days. This certificate's private keys are stored in two locations: in the Zscaler CA database and in the ZIA Service Edge memory.

The reason for this two-location storage is that the ZIA Service Edge does not write to disk. If the ZIA Service Edge is rebooted for any reason, the certificates keys are erased from memory and must be retrieved again from the Zscaler CA when the reboot completes.

4. **End-entity certificate** – This is the certificate that the client machine receives from the ZIA Service Edge. This certificate is created on demand, with its private keys existing only in the ZIA Service Edge memory. If the ZIA Service Edge is rebooted for any reason, the certificates it had previously issued become invalid. If the client reconnects with an old certificate, then the ZIA Service Edge issues a new certificate at that time.

Description	Custom Certificate	Zscaler Certificate	Use and Validity
Root CA	Your private database associated with your CA	The Zscaler Central Authority database	Used until validity is expired
Zscaler Central Authority Intermediate CA	Zscaler CA database	Zscaler CA database	Used until validity is expired or rotated
ZIA Service Edge CA	Zscaler CA database and ZIA Service Edge memory	Zscaler CA database and ZIA Service Edge memory	Used for 7 days, valid for 14 days
Application certificate delivered to the user	ZIA Service Edge memory	ZIA Service Edge memory	Used for 1 day, valid for 1 day

Table 1. The table above shows a summary of private key management within ZIA

Deleting keys from ZIA

When a key becomes invalid or is rotated out, the key must be removed from memory in a secure manner. Zscaler takes precautions that are beyond simply unlinking the file.

When a ZIA Service Edge needs to inspect your organizations TLS/SSL traffic, it requests the key for your organization as it needs it. The key is only resident in a special portion of memory and is never written to disk. The system software prevents a command line user from viewing or "dumping" this portion of memory for inspection.

A key is removed from memory when:

- It has not been used for a short period of time.
- The key has been rotated by an admin or the service.
- A software error occurs resulting in a core dump and reboot.

The key is first zeroed out and then removed from both RAM and packet buffers. It is removed before a core dump is written out to disk.

On the Zscaler CA, the keys are removed when a certificate is rotated out. The existing keys are removed from both the active database and the database backups to ensure that they are not recoverable.

Choosing a CA infrastructure

Zscaler provides two options for root CA certificates: using your own certificate authority or leveraging Zscaler's CA. From a functional standpoint, the two options are equivalent, but there are differences in the deployment of the root CA. The option you choose depends on your current infrastructure.

If you already have your own CA infrastructure in place, you may prefer to use your own certificates. Your client machines are already preloaded with your root CA certificate, and they can begin to use the ZIA service immediately without additional certificate installations in the client certificate store.

Zscaler recommends uploading your trust chain file to the Zscaler Central Authority when using your own private CA. This optional step helps your client machines validate the server certificate because the certificate chain is sent along with the certificate to the user's device. Zscaler accepts the .pem format with a Base64 encoding for a certificate chain file.

If you don't have a robust CA practice in place already, or don't want to make Zscaler an intermediate CA to your organization, Zscaler's CA is the best choice. Zscaler CA is a private CA. You will need to install Zscaler's root CA in your machines' certificate stores to deploy the Zscaler root CA certificate.

Device management platforms are ideal for installation of the new certificate. You can also host the certificate on your intranet and allow your users to install the certificate themselves, especially in Bring Your Own Device (BYOD) instances where the device might not be under management but is allowed to access services. Also note that some applications use certificate pinning as a form of security and can break connections. See the section on Certificate pinning later in this guide.

Some applications are hosting their own certificate trust store and might also need to be updated. You can read information on Adding Custom Certificate to an Application Specific Trusted Store (https://help.zscaler.com/zia/adding-custom-certificate-application-specific-trusted-store).

Zscaler recommends using your CA to issue the intermediary certificate if you already have a solution in place. You can find more information on both deployment methods at Choosing the CA Certificate for SSL Inspection (https://help.zscaler.com/zia/choosing-ca-certificate-ssl-inspection).

Certificate rotation and APIs

If you are using your own CA certificate, you should rotate the intermediary certificate after some time. A rotation of certificates occurs normally when the certificate's end of validity date is approaching, or when you suspect the certificate has been compromised and you proactively implement a change. When you upload a new certificate, the new certificate replaces the existing certificate for all new requests.

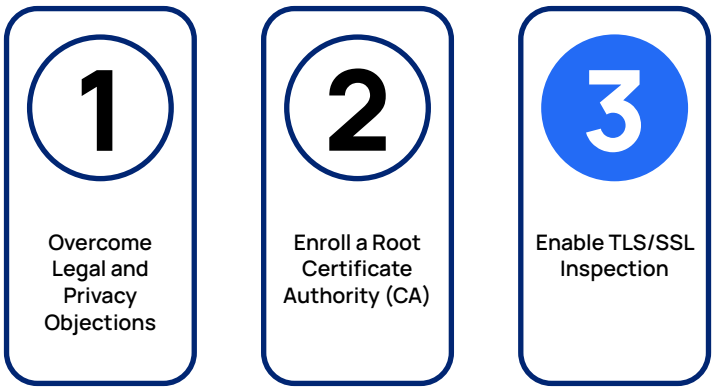
ZIA supports changing the intermediary certificate at any time. The change can be done manually via the admin interface or via APIs. Zscaler recommends that when you change your intermediary certification, you also upload its new certificate chain to speed up client adoption. Certificates can be rotated at any time.

Manually rotating the certificate occurs in the same way the original upload occurs, via the Zscaler Central Authority interface. You can read instructions on rotating the certificate at Configuring a Custom Intermediate Root Certificate (https://help.zscaler.com/zia/choosing-ca-certificate-ssl-inspection#Custom-Intermediate-Root-Certificate).

If you prefer to rotate your certificates programmatically, Zscaler supports API calls for certificate management actions. Using the API, you can automate the certificate rotation with your CA. Automated rotation is especially useful if your organizational policy requires that you use short-lived intermediary certificates. You can learn more about supported API calls by viewing:

- TLS/SSL inspection API use cases at SSL Inspection Settings Use Cases (https://help.zscaler.com/zia/ssl-inspection-settings-use-cases).
- The API developer reference guide for TLS/SSL inspection at SSL Inspection Settings (https://help.zscaler.com/zia/ssl-inspection-settings).

Phase 3: Enable TLS/SSL Inspection



Deploying TLS/SSL inspection is best rolled out in a controlled manner. Select a pilot group to enable first. This first group allows you to see where policy needs adjustment, and where notifications can be improved. As your policy becomes more refined, you can continue to expand your inspection to more groups and locations.

When you set out to develop your inspection policy, the instinct of many organizations is to attempt to re-create their existing configurations from their legacy appliance infrastructure. While it might be possible on some level, Zscaler does not recommend this approach. Security infrastructure grows and evolves over the lifetime of the organization. This growth and evolution often results in configurations with legacy workarounds that are not required when you integrate with Zscaler.

Zscaler recommends using your existing policy as a guide rather than a roadmap. Check your previous decisions and assumptions, and make sure they are still required. In this section, we help you plan out your deployment, policy, and notifications. We also identify applications with weak security that need upgrading, and handle application pinning and non-standard deployment scenarios.

TLS/SSL inspection prework

As you roll out inspection, you want to ensure that your organization continues to operate without interruption while you layer in this additional security. Zscaler recommends starting your inspection rollout with a limited group of users and policies, and then expanding as your policy becomes more robust. This method allows you to learn as you deploy with minimal disruption.

Block Google QUIC protocol

Google Quick UDP Internet Connections (QUIC) protocol is an attempt by Google to speed up internet connectivity on its browsers and devices. This is accomplished by skipping TCP handshake and using UDP instead. However, Zscaler's TLS/SSL inspection relies on TCP session information to operate, so Zscaler recommends blocking Google QUIC.

When blocked, the browser or device will fall back to using TCP connections like normal. Zscaler's firewall and Zscaler Client Connector both support blocking QUIC connections. You can also block this protocol using conventional branch office firewalls if needed.

You can find more information on blocking Google QUIC at Managing the QUIC Protocol (https://help.zscaler.com/zia/managing-quic-protocol).

Set up AUP acceptance and end-user notifications

To get started, collect the policy and messaging that you developed earlier in this guide. At this stage, you should have the following notification and messaging approved and ready for configuration:

- An approved Acceptable Use Policy (AUP) – This is the document users agree to when they connect for the first time, and as often as required by your legal team. You should configure this policy before you begin testing, ensuring all users have accepted the AUP. You can learn more information about AUP configuration and acceptance at Configuring the Acceptable Use Policy (https://help.zscaler.com/zia/configuring-acceptable-use-policy).
- Documented website for AUP and escalations – It is inevitable that your users will attempt to access a resource that is blocked by inspection. These blocked attempts trigger an escalation by the user if they feel that the resource is legitimate. It is a best practice to document your escalation procedures on your organization's intranet page. Your procedure should include your AUP, and what block and caution notifications mean. It should also include the procedure by which a user can have the destination reviewed by your IT and policy staff to ensure correct categorization. Link to this procedure document in your Block and Caution notification.
- Block notification – This message is displayed when the system blocks access to a resource, either because of a policy that you have set, or because of a bad certificate presented to the ZIA Service Edge. This notification can include a default message, or you can customize the message to include specific text. Zscaler recommends linking to your AUP and escalations site. Finally, your message can contain limited HTML styling to allow you more customization options. You can learn more about configuring a block notification at Configuring Block Notifications (https://help.zscaler.com/zia/configuring-block-notifications).
- Caution notification – Much like the block notification, the caution notification is triggered by user action. The action can be an attempt to reach a site that has questionable value to the organization. An example of problematic websites can include streaming media sites with user-generated content, or just a viral video. In this case, the caution notification is appropriate, and the user can make the choice to proceed or abandon their browsing. Zscaler recommends linking to your AUP on caution notifications, providing more detail on the policy You can learn more about configuring caution notifications at Configuring the Caution Notification (https://help.zscaler.com/zia/configuring-caution-notification).
- Initial policy controls roadmap – It's likely that your organization already has classes of sites, web applications, or special deployments that you want to gain control over. These can include things you wish to outrightly ban, such as gambling or adult content. It can be things you'd like more control over, such as who can access social media and when. These policy decisions will be implemented in the next steps.

When you have these notification and messaging items in place and configured, you are ready to develop your policy and begin applying it to users. In the next section, you will focus on your pilot users, who will be the first to go through inspection as you work out your initial policy. You use the pilot group to test and become comfortable with the policy before you roll it out to your entire organization.

Selecting your pilot group

The first users you onboard, the pilot group, need to understand that they may experience some issues and disruption. Select a group of users that can handle the interruption. You don't want to include users that are at a critical time of year in either their product development or regulatory calendars. While changes to policy can be rapidly rolled back, you want to avoid that scenario. Select a minimally vulnerable group and ensure that you have that group's full cooperation before starting the pilot program.

The pilot team ideally will not be your IT or development staff, because IT and development users often try to work around issues before reporting them. Additionally, their work often entails operating in an environment that does not match that of the average user. See Developer environments for more information on deploying development teams.

The pilot group should consist of a diverse set of average users in an office location, business unit, or small region. The more job functions this group performs, the more applications will be tested and the more notifications you'll receive. You will also want feedback on your notification copy to see if it's clearly conveying what you mean, and the escalation process for resolving issues.

Ensure that your pilot group knows how the escalation process works. Ideally, have a representative of your security or IT team offer a presentation about inspection and escalation, and perhaps be available for real-time communication should an issue arise. Make sure that you have someone in place to make real-time changes or implement a quick rollback of policy. Zscaler makes it simple to roll back policy quickly, and direct communication with your security team is vital for the successful support of the pilot.

The pilot group must be identified by the policy engine so that the appropriate rules can be applied. There are several options here for you to select from depending on your needs, including user and location options.

When you start your policy selections, you will likely go back and expand the policy to apply to more users. You may rewrite the policy as you learn more about your users and application needs. When you are building out policies for long-term use:

- If you have a policy that applies to many of your users no matter where they are, focus on the user selection criteria.
- If the policy is only relevant based on location, such as required by a government mandate, choose the location selection criteria. You might also have criteria that apply only when users are in a particular location.

The following criteria use the logic 'AND' between the categories. This means that if you specify a user group AND a location, both must match for the policy to be applied. Not all criteria must be used. If you do not specify a criteria option, then the option is ignored.

After your pilot group is onboard and operational, you can start to roll out inspection to the rest of your organization. You should plan for this rollout to move quickly, region by region, until all your users are being inspected.

Select by User

User-specific policies are focused on users or groups of users.

- Users – The user policy allows you to select up to 4 specific users for your policy. You can also specify two user aliases: General Users (all authenticated users) or Special Users (all unauthenticated users). Zscaler does not recommend starting with these alias options for your rollout because the options are too constrained (user) or too broad (all authenticated users). The General Users selector will likely be used later when you need to broadly apply inspection rules to the entire organization, such as a Microsoft 365 policy.
- Groups – Users can be placed in groups, and the inspection policy allows up to 8 groups to be specified in the rule set. This is a very useful construct for rollout, and each user can be a member of up to 128 groups, which can be increased with a ticket to Zscaler Support. You can learn more about group use and editing at **About Groups** (**https://help.zscaler.com/zia/about-groups**).
- Departments – Departments group users together into a policy target. They are more restricted than groups because users can belong to only one department at a time. Department groups are also used in reporting. Consider using departments when you plan to inspect a larger group of people that work in the same grouping. You likely already have departments, job functions, or business units in your organization that align with a department model. You might also choose to use departments to group users, such as developers, who require more specific policies due to the nature of their work. You can learn more about departments at **About Departments** (**https://help.zscaler.com/zia/about-departments**).

Select by Location

In the context of ZIA, a location is a distinct work location that is configured to forward all traffic using Generic Routed Encapsulation (GRE), Internet Protocol Security (IPSec) connections, or dedicated proxy ports from known locations. Adding an entire work site as a location can be useful to get a larger number of applications inspected. If you enable a location as a part of your pilot testing, be sure that your staff is ready to handle issues from users using multiple applications.

- Location – A location is configured in the Zscaler cloud to identify your organization. It includes your static IP address, bandwidth available, etc. When you specify a location in an inspection policy, all traffic from that location is subject to the policy. This is a useful way to onboard all users at a site without having to worry about groups or departments. Each policy can contain up to 8 locations. You can learn more about locations at About Locations (https://help.zscaler.com/zia/about-locations).
- Location Groups – You can logically group individual locations into a location group. This can be useful when you are applying the same policy to all users in a particular region or country. You can configure up to 32 location groups per policy. You can learn more about location groups at **About Location Groups** (**https://help.zscaler.com/zia/about-location-groups**).

Using URL categories in policy development

Using the category level controls, you can Allow, Block, or Caution (Pass Through) users as appropriate per your AUP. This policy can handle most of your internet sites and applications. ZIA supports a hierarchical set of categories to allow you granular control. The hierarchy from more general to more specific is:

- **Application Classes** – 6 classes of application: Bandwidth Loss, Business Use, General Surfing, Legal Liability, Productivity Loss, and Privacy Risk.
- **Super-Categories** – More specific categories within an Application Class. For example, the Application Class Bandwidth Loss has Super-Category: Entertainment/Recreation.
- **Categories** – More specific categories within a Super-Category. For example, Super-Category: Entertainment/Recreation has Category Music and Audio Streaming.

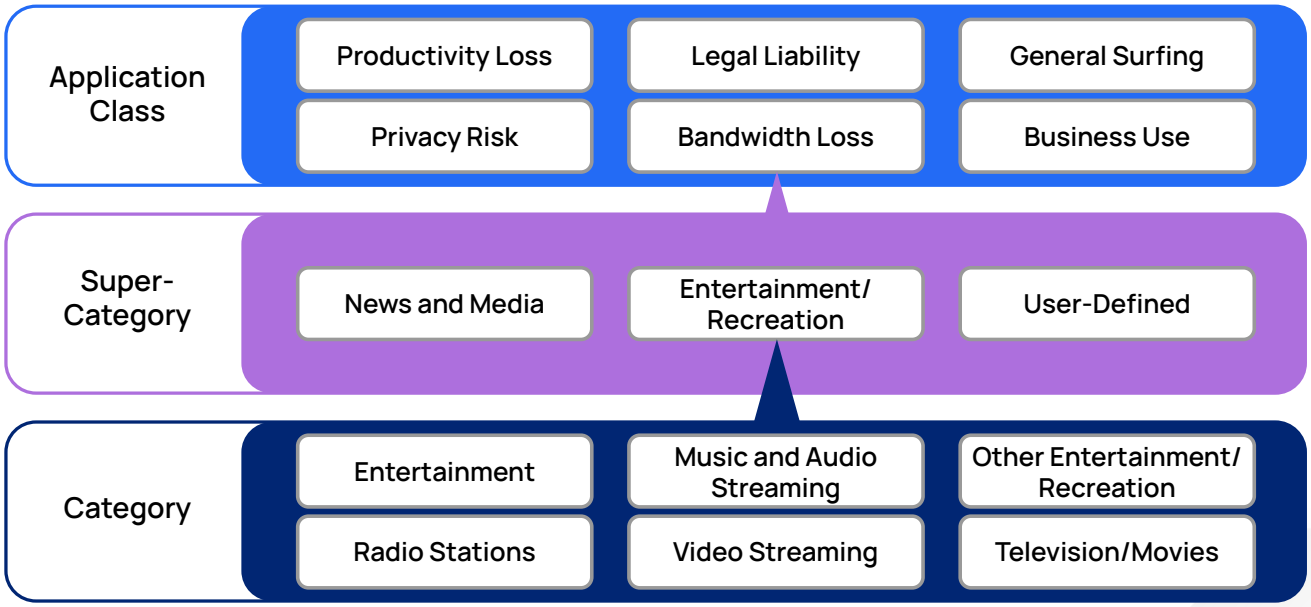


Figure 2. Example of URL Category hierarchy

You specify a rule match at one of these levels. Each rule is evaluated top to bottom until there is a match. This means you can exempt a Super-Category or Category while still blocking an Application Class. Let's look at an example rule order. The following organization has a policy that enables users to:

- Listen to a stream from a radio station.
- Check the news or other media site.
- Not access any other category that would lead to bandwidth loss.

With such a policy, users can still take advantage of URL Categories to Allow or Block sites. The rule set would look like:

Rule Order	URL Category	Action
1	Radio Stations	Allow
2	News and Media	Allow
3	Bandwidth Loss	Block

In this case, if a user wanted to listen to an online radio station or check the news, they are allowed. However, other sites in the bandwidth category are restricted. This rule ordering enables you to very quickly allow or block large sections of internet destinations.

You can find the definitions of Zscaler's URL categories at About URL Categories (https://help.zscaler.com/zia/about-url-categories).

If you need to understand the classification a URL falls under, you can use Zscaler's Site Review tool located at Site Review (https://sitereview.zscaler.com/). You must be logged into Zscaler to use this tool.

Custom categories

While Zscaler's URL categorizations are robust, you may want to modify existing categories or create your own categories and destinations. Your organization might require that URLs be categorized differently, based on your business policy, or you might want to have another category option for inspection.

Modifying the pre-existing categories to better suit your policy is possible with a few caveats. You cannot modify, add, or delete the top-level URL classes. At the next level, Super Categories, you cannot add or delete, but you can move URLs to other classes. By moving Super Category URLs amongst classes, you can allow URLs that might otherwise be blocked, without needing to specify additional rules. Using this ability, you can reorganize the Business Use class so that it contains all the Super Categories related to your business and applications, allowing you to specify one allow rule for your applications.

The narrowest/most specific category consists of two types: predefined categories and custom categories. Each of these category types can be modified to add URLs or keyword matches. Keyword matches allow you more flexibility in your matching. You can specify terms that you want to match in the entire Uniform Resource Identifier (URI) string, including the URL and any other identifier in the string, such as query strings and paths.

For example, to block gambling sites in your policy, block the Legal Liability > Gambling Super Category > Gambling category. This rule structure blocks known sites affiliated with gambling. To stop all gambling-related traffic of any kind, you can further modify the category by adding the keyword 'gambling' to the category. This catches the string 'gambling' even if it only appears in the URI as a query string or path. Searching for 'gambling' in Google results in the following URI, and triggers a match where gambling appears in bold:

```
https://www.google.com/search?q=gambling&source=hp&ei=gAywYdq6KMOf0PEP9OGZwAc&iflsig=
ALs-wAMAAAAAYbAakIIjcKxqKWjRLuD-syZqK6IfZ8Hj&ved=0ahUKEwja-pjWiNP0AhXDDzQIHfRwBngQ4-
dUDCAg&uact=5&oq=gambling&gs_lcp=Cgd...
```


If modifying the category is not sufficient for the policy, you can create your own custom category. Custom categories are based on URLs and keywords that you choose. You can specify up to:

- 64 custom categories
- 25,000 URLs across all policies (can be increased via subscription)
- 256 keywords per category
- 2,048 keywords across all categories

To learn more about Zscaler limits, visit **Ranges & Limitations** (**https://help.zscaler.com/zia/ranges-limitations**).

Using Cloud App in policy development

Cloud App provides granular control over popular websites and applications. Supported applications allow you to specify controls for those tools, or a category of tools. For most applications, you can Allow or Block either at the category level or the application level, in a similar manner to the URL category feature.

Cloud applications provide additional controls. Because these applications are understood by the ZIA Service Edge at a deeper level, you can specify a daily quota by bandwidth or time. When users reach the limit on number of attempts to browse back to an application or site, they receive a notification that they have reached their daily quota.

Five Cloud App categories are granted control down to the specific action level. In addition to being able to block an entire application, you can restrict actions specific to the site. You can include reading but not allow posting to social media, include reading web pages but not allow sending to web pages, etc.

Zscaler recommends using Cloud App categories and applications when you want to allow users access beyond Allow or Block, as provided by the URL categories.

The Cloud App categories are:

- Collaboration & Online Meetings
- Consumer
- DNS Over HTTPS Services
- Finance
- Health Care
- Hosting Providers
- Human Resources
- IT Services
- Legal
- Productivity & CRM Tools
- Sales & Marketing
- System & Development

The five categories that provide extra controls and quotas are:

- File Sharing
- Instant Messaging
- Social Networking
- Streaming Media
- Web mail

You can learn more about configuration Cloud App control policies at **About Cloud App Control** (**https://help.zscaler.com/zia/about-cloud-app-control**).

Using Destination Groups in policy development

Destination groups allow you to configure specific traffic destinations. You can leverage destination groups in rule sets in the same way as URL categories. This feature allows you to specify single objects, or ranges and wildcard entries. In addition, you can include country restrictions and specify URL Categories.

The types of selectors available are:

- IP Address – You can specify an individual address, a subnet, or an address range.
- Fully Qualified Domain Name (FQDN) – Use this when you're specifying a group of resources or a resource with an IP address that is likely to change.
- Wildcard Domain – You can add an FQDN as a wildcard by prefixing the domain with a single dot ('.') character. Do not specify an asterisk as a wildcard character.
- Other – You can select this option if you don't want to associate IP addresses, FQDNs, or domains with the destination group.

Do not specify wildcard domains with a leading asterisk (*), use a dot (.) instead. For example, to create a wildcard domain for safemarch.com, use .safemarch.com

After you select the type, you can specify a list of countries. The list affects only the specified services that also match that country. You can specify 'Any' to include all countries.

Finally, you can add URL categories to your policy set to combine multiple selectors in your rule sets.

Developer environments

Development teams often represent a challenge to organization security models. Developers often need direct internet access to their customer-facing applications, especially if they are still using **Certificate pinning**. Developers needs to ensure that their applications are functioning as expected, certificates are correct, etc. Development environments might also have local development resources that include custom DNS and mail servers.

Work with your development teams to understand their workflow. Development teams are ideal candidates for department designation and destination groups. You can exempt their workloads from inspection where necessary, allowing for development and testing. However, you should make it clear that this is a risk to the organization. You should have a plan in place to limit devices in a developer test lab from the rest of the organization.

Work to create a set of URLs that support their development. If you allow your developer teams to deploy resources, consider using wildcard certificates to bypass specified sites not only from inspection but from any bandwidth constraints as well.

For all other traffic, your developers should have the same policies as others in the organization. Order the development-specific rules higher in the list than the general employee rules to ensure that the rules for general users don't interfere with permissions for developers.

Understanding traffic that can't be inspected

In rare cases applications might not function as expected or at all when being inspected. This means that the traffic cannot be inspected to be judged as safe. The most common reasons for decryption failures and inability to inspect are:

- Bad or expired certificate for the site or application.
- Certificate pinning by an application, or more rarely by a web site (see **Certificate pinning** later in this section).
- Traffic that uses a protocol that is not understood by the ZIA Service Edge, and therefore cannot be decrypted.

Zscaler recommends in almost all cases that you drop traffic that cannot be inspected. If the traffic is legitimately needed by the organization, require that the user file a help ticket to request access. In the next sections, we'll explain our recommendation, and describe how you can bypass traffic.

Expired or incorrect certificates

When a certificate is bad or expired, allowing users to proceed and access the application risks the user visiting a malicious site. Legitimate sites, barring unforeseen issues, keep their certificates up to date. While not being able to access a site or application can be an inconvenience to users, their safety and that of the organization should be prioritized.

An untrusted certificate is one where the certificate and server details do not match. Causes of trust failure can include:

- A private certificate from an unknown issuer.
- The certificate has expired.
- The name on the server and certificate do not match.
- The certificate chain of trust validation fails.
- The signature does not match the certificate.

All components of a certificate must be correct and match the server information. When there is a failure, you can choose to Allow, Caution, or Block the connection. Zscaler recommends that you block access until the certificate issue is addressed on the server side.

Zscaler also supports Online Certificate Status Protocol (OCSP) revocation checks. When enabled, the ZIA Service Edge checks the revocation status of the certificate. This check is made even if the certificate is correct in all other aspects. If the certificate is revoked by the issuing CA, the ZIA Service Edge treats the certificate as an untrusted certificate. The same action you choose for failed trust certificates apply to an OCSP failure.

Zscaler recommends that you drop all traffic that is associated with bad certificates and enable OCSP for all inspection rules.

Certificate pinning

Certificate pinning is a method for applications (and previously web servers) to force a client to use a particular certificate and reject all other certificates. Certificate pinning was intended to ensure that clients connected to only legitimate servers. However, two issues arise from the use of certificate pinning:

1. Proxies (like Zscaler) break because the client does not accept the proxy-issued certificate. This is a non-starter for security-minded organizations, and those sites saw traffic drop.
2. If the vendors' certificate infrastructure needs to be updated, any client holding a server's older certificate is unable to connect because the browser or application will not accept the new certificate until the old certificate expires, preventing those customers on that machine from connecting. Typical certificate pinning expiration dates were set to expire after 1 year.

The industry has moved to deprecate the certificate pinning practice due to the loss of access when certificate issues appear. Application vendors, as with public CAs, are moving to shorter lifetimes for their intermediate CAs. Those developers who persist with certificate pinning are raising their cost of certificate maintenance and taking the risk of users being unable to connect to their service.

If you encounter certificate pins, you can either replace the application or bypass the traffic. Bypass the traffic only if the application in question is of such high value to the organization that it's worth the risks associated with not inspecting. Otherwise, deny the traffic. Also, encourage your vendors to avoid certificate pinning.

For another look at certificate pinning and what certificate authorities are doing to discourage its use, see **What is certificate pinning** (**https://www.digicert.com/blog/certificate-pinning-what-is-certificate-pinning**).

Handling un-decryptable traffic

The ZIA Service Edge is capable of decrypting most publicly documented encryption methods. You should be cautious of any traffic that is unable to be decrypted. It could simply be that at this time Zscaler is not able to decrypt a particular protocol. It could also be that the protocol has been broken and is no longer considered secure and should not be in use. You can find a list of supported protocols at **Supported Cipher Suites in SSL Inspection** (**https://help.zscaler.com/zia/zscaler-ssl-tls-support**).

The site could also be using a custom encryption protocol. This is most often associated with nation state actors who are using custom encryption due to communications being classified. Those protocols are considered state secrets and are not available to Zscaler to build into the ZIA Service Edge. It is rare to see custom encryption schemes if you are not a government employee or contractor, and this traffic should be blocked in most cases. If you are using one of these protocols in your organization, you will need to bypass that traffic.

Bypassing inspection

You can choose to bypass inspection on traffic in specific circumstances. Choose to bypass traffic only after consulting your legal counsel for the impacted region. In general, bypasses are applicable only for specific functions such as:

- Banking and finance destinations.
- Healthcare destinations.
- Business functions that require the use of unencryptable traffic.
- Business functions that require the use of certificate pinned sites or applications.
- Applications such as certain parts of Microsoft 365 that have issues when inspected.

Zscaler strongly recommends that you inspect all traffic and put in place a bypass only in extreme circumstances.

Microsoft 365 and Office 365 One Click

Guidance on inspecting Microsoft 365 has been changing in recent years. Microsoft originally strongly recommended bypassing inspection for all Office 365 services. In response, Zscaler built an Office 365 One Click configuration. This bypassed Office traffic and allowed transparent proxy to their cloud.

Microsoft has since started to relax this stance. Zscaler has introduced Microsoft 365 configuration. Similar to the Office 365 switch, the new Microsoft 365 One Click configuration is synchronized to the Microsoft IP mapping API. This means as Microsoft publishes additional ranges, the Zscaler service is automatically updated. It also allows for inspection, allowing you to restrict access to Microsoft 365 to your organization's tenant.

To learn more about configuring Microsoft 365 One Click options, see **About Microsoft One Click Options** (**https://help.zscaler.com/zia/about-microsoft-one-click-options**).

TLS version enforcement

ZIA supports many protocols and ciphers when inspecting TLS/SSL. As you use inspection, the ZIA platform reports on which protocols and ciphers are in use by your clients and infrastructure. To learn more about protocols and ciphers that are currently supported by ZIA, see **Supported Cipher Suites in SSL Inspection** (**https://help.zscaler.com/zia/zscaler-ssl-tls-support**).

Zscaler recommends initially allowing all supported protocols and ciphers to minimize disruption for users. During this time, you can discover what is in use on your network, and which services or platforms still use legacy encryption. Using the provided dashboards, you can discover which applications use legacy security and move to strengthen your requirements for connections.

The ZIA Admin Portal supports a display of the versions of TLS and SSL used in your organization. Using this information, you can upgrade or disable services that are still tied to legacy encryption suites. Zscaler recommends that you block all TLS versions earlier than 1.2, including any legacy SSL services.

