


Slide 1 - Zscaler Policies



# Zscaler Fundamentals

## SSL Inspection

©2018 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on the SSL Inspection capabilities of the Zscaler platform.

## Slide 2 - Navigating the eLearning Module

## Navigating the eLearning Module

The screenshot shows the Zscaler Cloud Portal dashboard. At the top right is the Zscaler logo. Below it is a navigation bar with links: Dashboard, Analytics, Policy, and Administration. The main content area is titled 'Web Overview' and includes a 'Web Overview' dropdown menu. The dashboard displays several charts and tables: 'Cloud Application Classes' (a donut chart showing 301.3 MB and 100%), 'Top URL Categories' (a donut chart showing 16.8 K and 100%), 'Top Users' (a table listing users and their transaction counts), 'Streaming Media Applications' (a table listing applications and their transaction counts), and 'Top Advanced Threats' (a table listing threats and their transaction counts). Overlaid on the dashboard are several blue callout boxes with white text: 'Exit' (top right), 'Previous Slide' (left), 'Next Slide' (right), 'Play/Pause' (bottom left), 'Fast Forward' (bottom center-left), 'Progress Bar' (bottom center), 'Audio On/Off' (bottom center-right), and 'Closed Captioning' (bottom right).

**Slide notes**

Here is a quick guide to navigating this module. There are various controls for playback including play and pause, previous, next slide and fast forward. You can also mute the audio or enable Closed Captioning which will cause a transcript of the module to be displayed on the screen. Finally, you can click the ' X ' button at the top to exit.

## Slide 3 - Agenda

The slide features a light gray background with a large white cloud shape on the left side. The word "Agenda" is written in a large, blue, sans-serif font inside the cloud. To the right of the cloud, there is a bulleted list item. The Zscaler logo is located in the top right corner of the slide.

# Agenda

- SSL Inspection Overview

## Slide notes

In this module, we will provide an overview of the Zscaler SSL Inspection capabilities.


Slide 4 - SSL Inspection



Slide notes

The first topic we will cover is the ability for Zscaler to inspect SSL traffic forwarded to the proxy service.

## Slide 5 - Why Use SSL Inspection?



## Why Use SSL Inspection?

Pros
<ul style="list-style-type: none"><li>• Almost all popular sites use SSL (Google, Facebook, Youtube, Twitter, SFDC, SAP, Workday, etc.)<ul style="list-style-type: none"><li>○ &gt;80% of end user traffic is now SSL encrypted</li></ul></li></ul>


## Slide notes

One of the most important decisions you will need to make with your organization is whether to have the Zscaler service intercept and inspect SSL traffic. More and more sites are moving to SSL-only:

- Routine Google searches now use SSL;
- YouTube is SSL;
- Facebook, Twitter, and on and on.
- In addition, all of the enterprise services have only ever been SSL.

This means that easily 80% of the traffic your end users generate is SSL encrypted.

## Slide 6 - SSL Inspection – Mechanics



## Why Use SSL Inspection?


Pros
------

**Slide notes**

What this means is that if you do not enable SSL Inspection you will be blind to a massive amount of traffic entering and leaving your environment.

It is important to understand that, just because it is encrypted, that does NOT mean that it is safe! We find that ~50% of the advanced threats that we detect on customer environments, have entered the network on an SSL encrypted connection. This is because all of the popular services pull data from Content Delivery Networks (CDNs), which are a primary target for the bad actors.

## Slide 7 - Why Use SSL Inspection?



## Why Use SSL Inspection?


Pros
------

**Slide notes**

For this reason, we highly recommend enabling SSL Inspection, which allows us to scan the SSL connections just like an unencrypted connection.

Another major advantage of enabling the inspection of SSL traffic is that it gives us visibility into the users generating the traffic streams, which allow you to apply policies down to the user/group/department level; it also gives you visibility to the user level in the Zscaler logs, making them a much more powerful forensic analysis tool.

## Slide 8 - Why Use SSL Inspection?



## Why Use SSL Inspection?

Pros	Cons
<ul style="list-style-type: none"><li>• Almost all popular sites use SSL (Google, Facebook, Youtube, Twitter, SFDC, SAP, Workday, etc.)<ul style="list-style-type: none"><li>◦ &gt;80% of end user traffic is now SSL encrypted</li></ul></li><li>• More and more threats ride on SSL connections</li><li>• Enabling SSL Inspection allows:<ul style="list-style-type: none"><li>◦ The security scanning of SSL traffic</li><li>◦ The application of user-based and Web 2.0 policies</li><li>◦ User-based logging for SSL traffic (rather than just Location-based)</li></ul></li></ul>	<ul style="list-style-type: none"><li>• SSL Certificate management<ol style="list-style-type: none"><li>1. <b>Use default Zscaler certificate</b> Zscaler root CA certificate required on end user devices</li><li>2. <b>Use custom certificate</b> Management of the certificate through its lifetime required</li></ol></li></ul>


## Slide notes

People tend to have a couple of concerns when it comes to enabling SSL Inspection, the first being the need to manage the certificate environment. There are two ways to manage this:

1. You may simply use the default Zscaler certificate, although this requires you to distribute the Zscaler root CA certificate to all users, so they can trust the connection to Zscaler.
2. Alternatively, you can load a custom certificate to Zscaler signed by your own internal PKI, so your users can automatically trust the connection to Zscaler.



## Slide 9 - Why Use SSL Inspection?



## Why Use SSL Inspection?

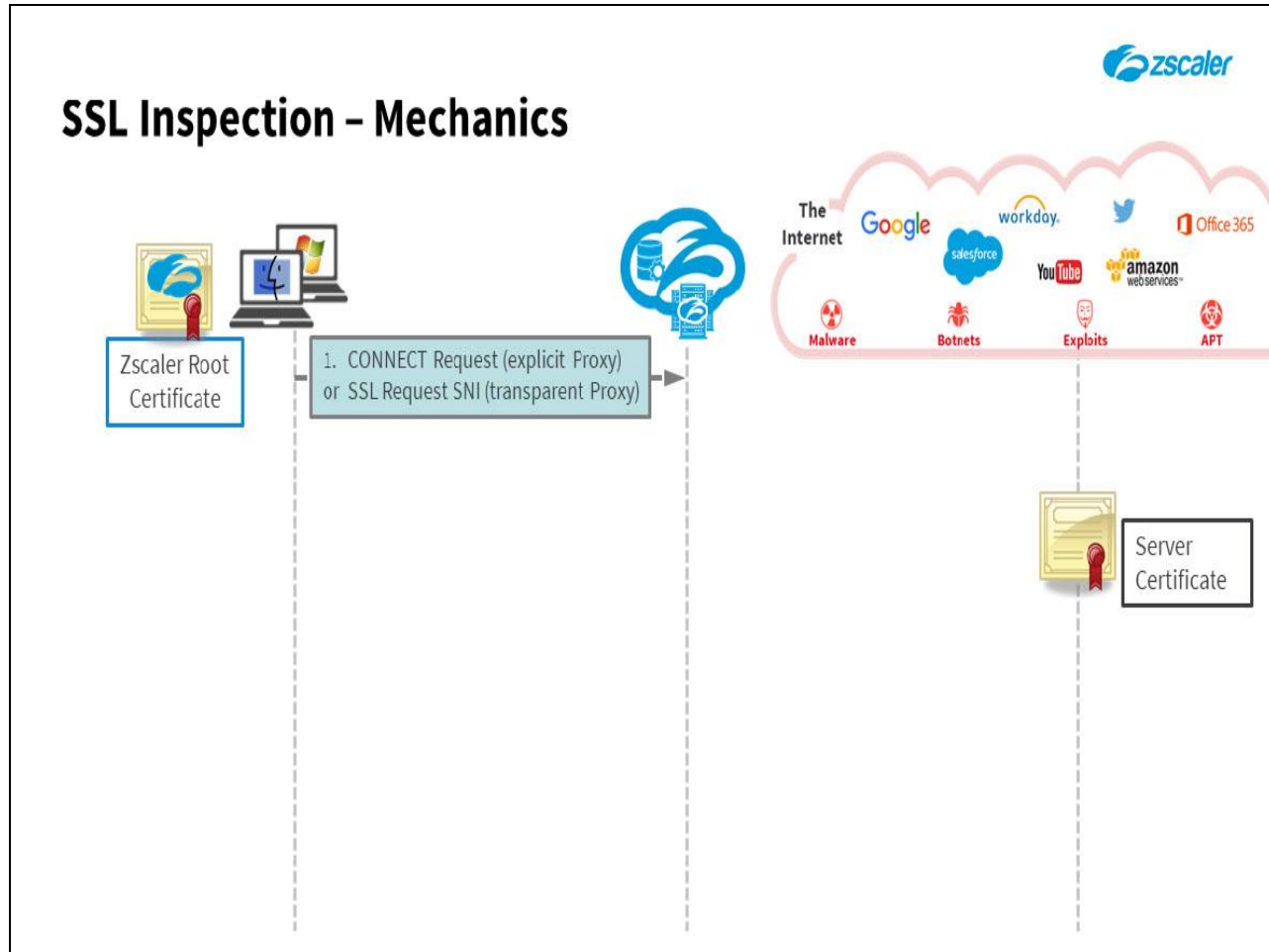
Pros	Cons
<ul style="list-style-type: none"><li>• Almost all popular sites use SSL (Google, Facebook, Youtube, Twitter, SFDC, SAP, Workday, etc.)<ul style="list-style-type: none"><li>○ &gt;80% of end user traffic is now SSL encrypted</li></ul></li><li>• More and more threats ride on SSL connections</li><li>• Enabling SSL Inspection allows:<ul style="list-style-type: none"><li>○ The security scanning of SSL traffic</li><li>○ The application of user-based and Web 2.0 policies</li><li>○ User-based logging for SSL traffic (rather than just Location-based)</li></ul></li></ul>	<ul style="list-style-type: none"><li>• SSL Certificate management<ol style="list-style-type: none"><li>1. <b>Use default Zscaler certificate</b> Zscaler root CA certificate required on end user devices</li><li>2. <b>Use custom certificate</b> Management of the certificate through its lifetime required</li></ol></li><li>• Some users may be concerned that their personal data is being scanned<ul style="list-style-type: none"><li>○ Add SSL Inspection exemptions as necessary</li><li>○ Connections to exempted URLs or URL Categories are established end-to-end</li><li>○ Zscaler cannot view data on connections to exempted destinations</li></ul></li></ul>

**Slide notes**

Some users may also be concerned that their personal data is at risk if we are inspecting all traffic. It is important to understand that we never store any payload data, it is only ever processed in RAM for the security checks and policy rules to be applied, the only data we ever log is metadata about the connections.

However, if people are concerned about the privacy of their personal data, we support the configuration of exemptions to the SSL Inspection policy. These are destinations (URLs or URL categories) that we will not inspect, which means that the encryption is established end-to-end with the destination server. Typically, customers will add banking or healthcare sites to the exemption list.

## Slide 10 - SSL Inspection – Mechanics

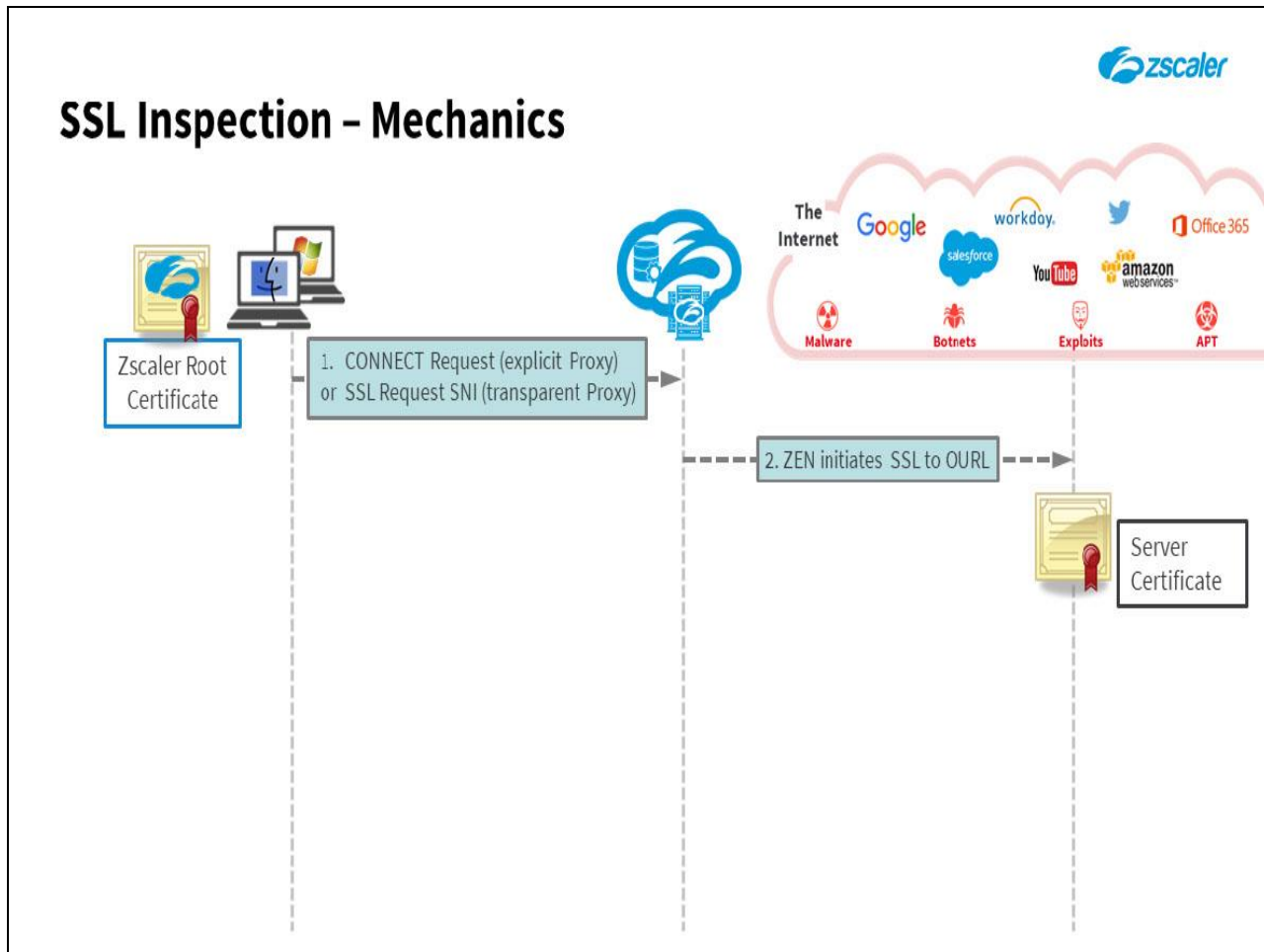


## Slide notes

The diagram here details what happens when you enable SSL Inspection.

1. The first step in the process is that a client will initiate an outbound SSL connection to a server. If the client knows that there is a Proxy (meaning there is an explicit Proxy definition) it makes an 'SSL CONNECT' request to the original URL (OURL), if it does not know there is a Proxy (the transparent Proxy case) then we must look at the request 'Server Name Indication' field (SNI) to identify the OURL. As traffic is being proxied by Zscaler, the outbound SSL request is terminated by the ZEN.

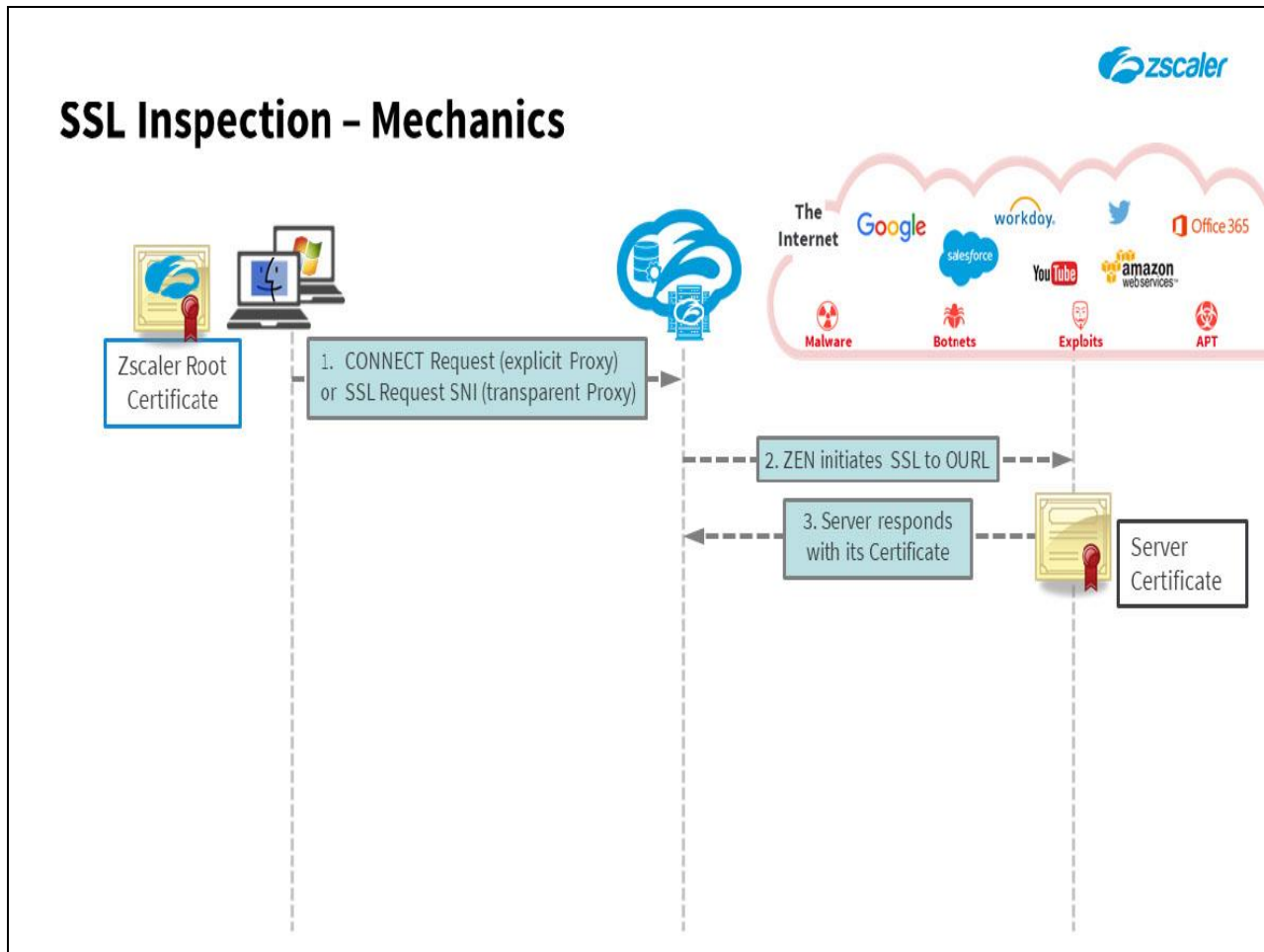
## Slide 11 - SSL Inspection – Mechanics



## Slide notes

2. The ZEN will initiate an SSL connection to the OURL...

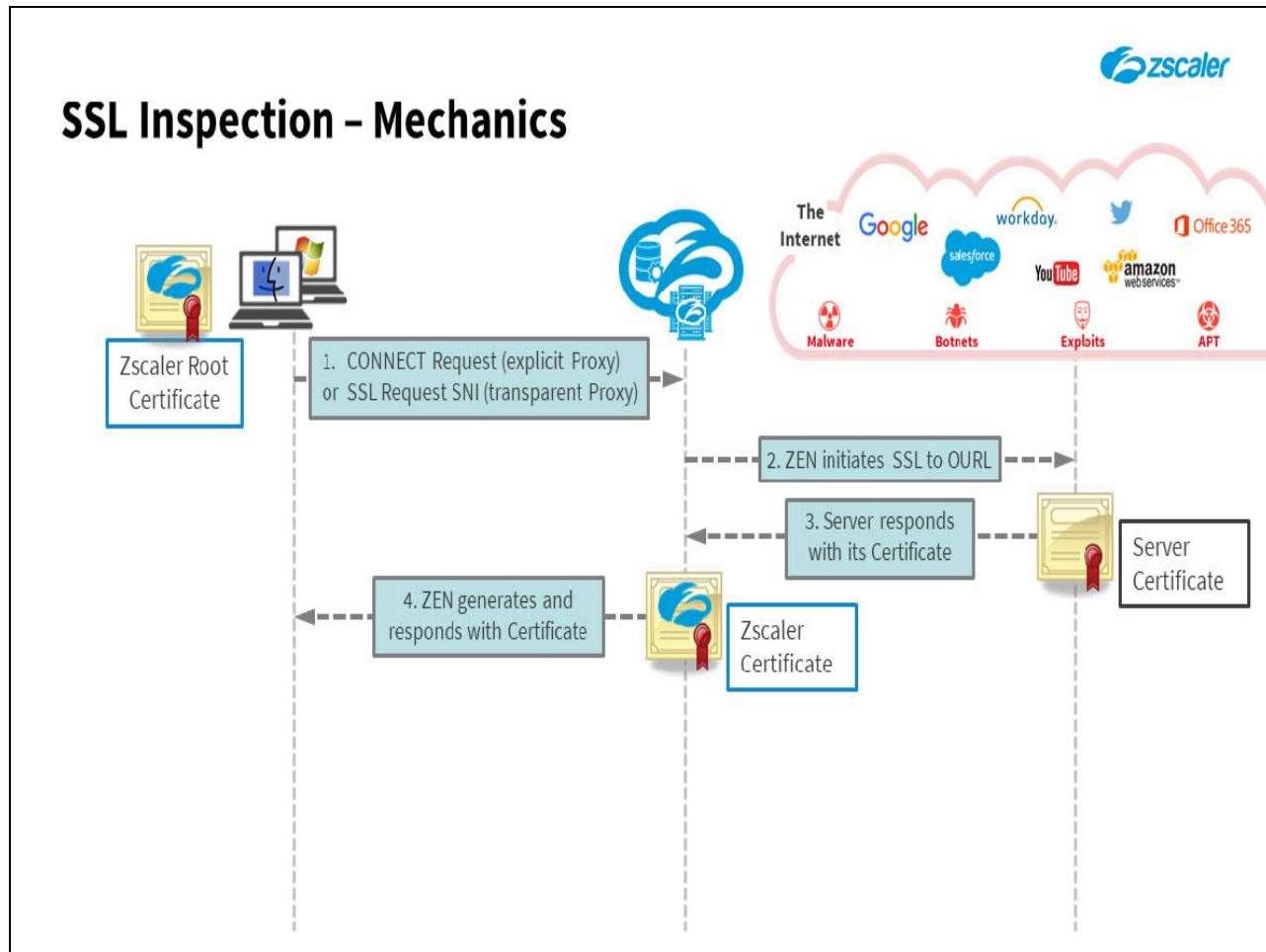
## Slide 12 - SSL Inspection – Mechanics



## Slide notes

3. And receives a response from the destination server that includes the server's certificate.

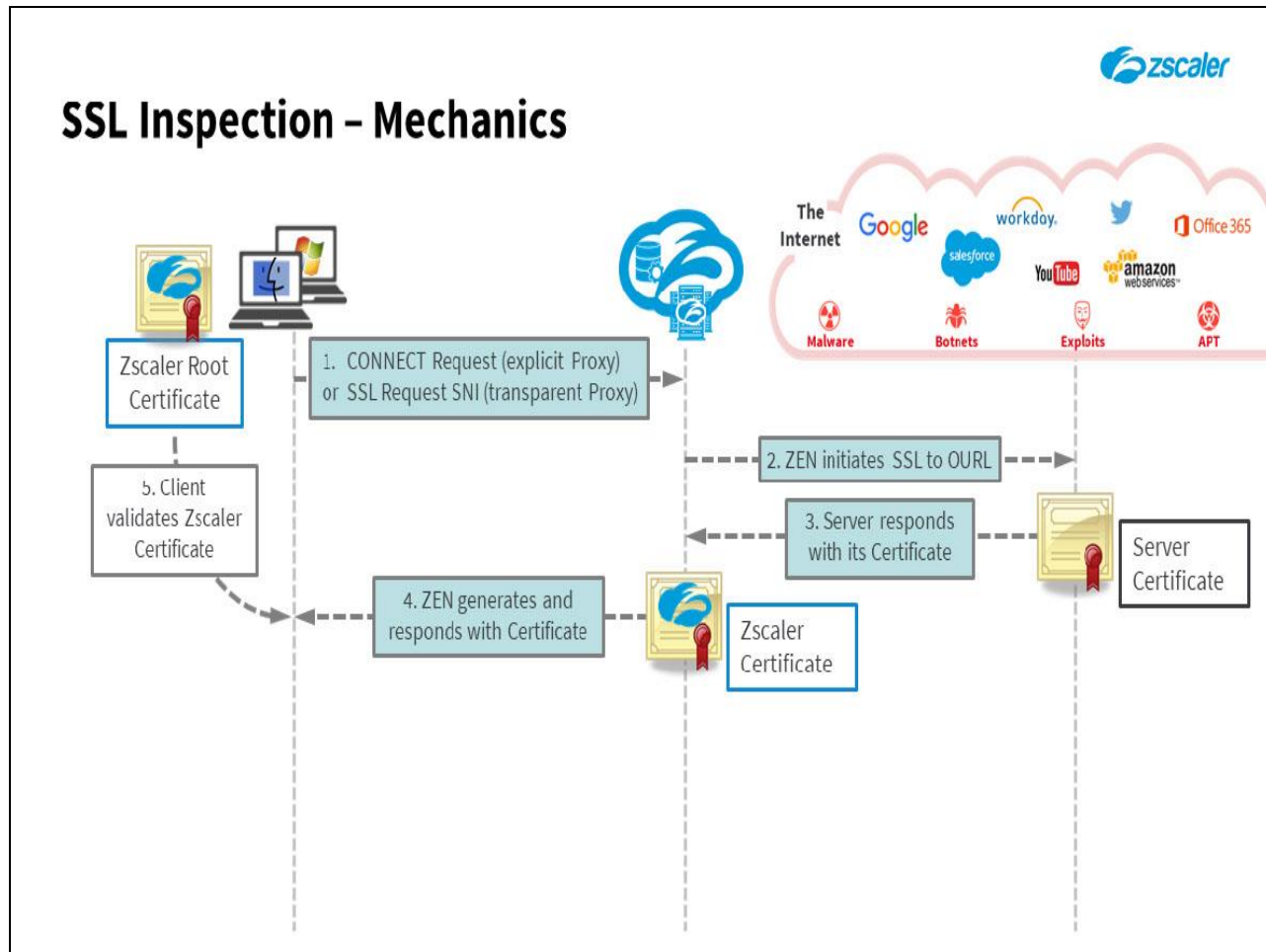
## Slide 13 - SSL Inspection – Mechanics



## Slide notes

4. The ZEN can now respond to the originating client with a certificate generated to replicate that of the destination server, however it is signed using a key managed by Zscaler. Either a Zscaler Intermediate CA key, or if you have loaded a custom certificate from your own CA to Zscaler, we will use the key from an Intermediate CA generated off of it.

## Slide 14 - SSL Inspection – Mechanics

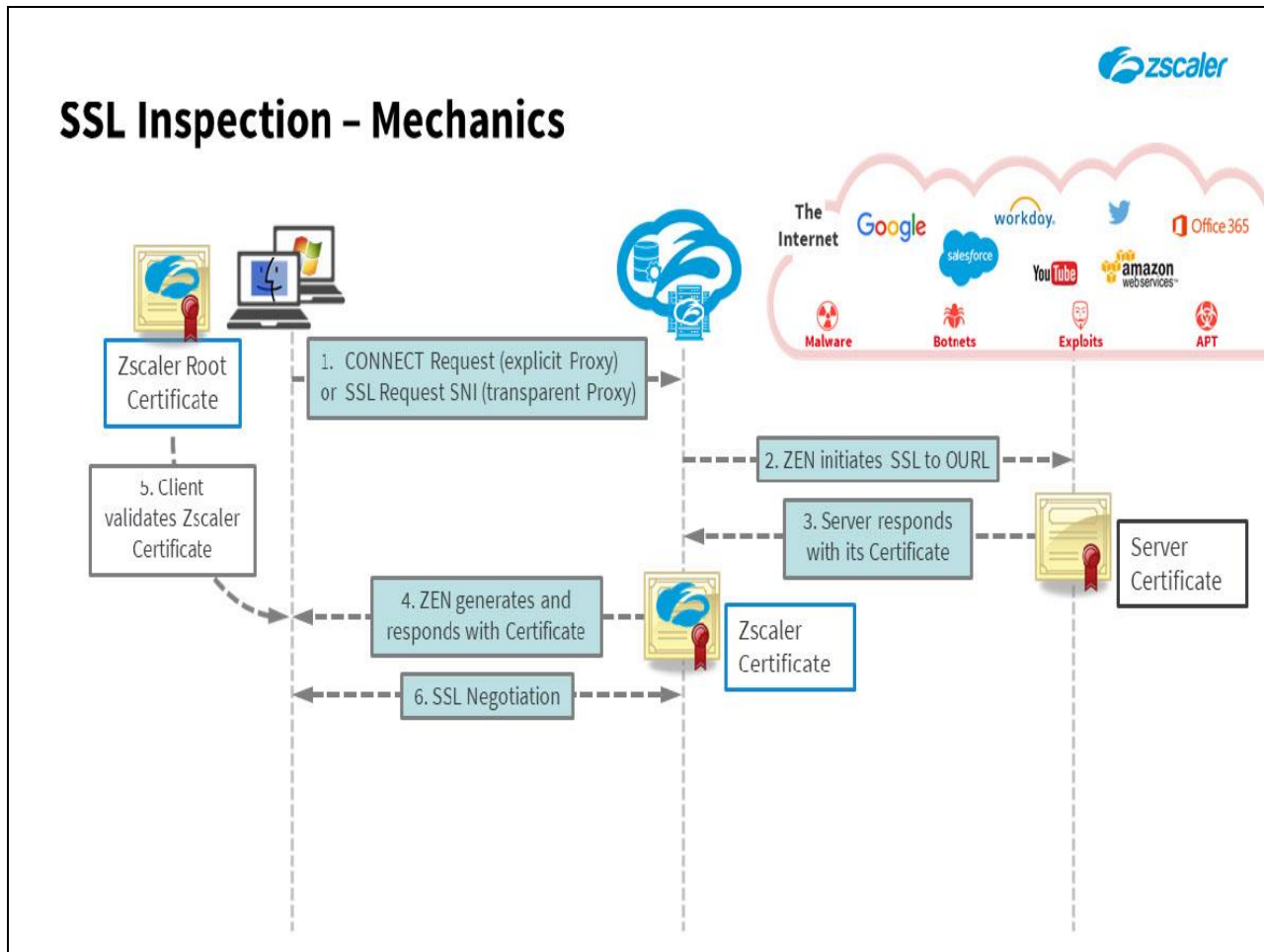


## Slide notes

- The client device should be in possession of the Zscaler root certificate, so that it can use the public key from it to validate the certificate received on this new connection. Otherwise the user will see certificate warning messages and manual intervention will be required to establish the connection.

If you have loaded a custom certificate to Zscaler, the client device should anyway already have the root certificate from your own CA.

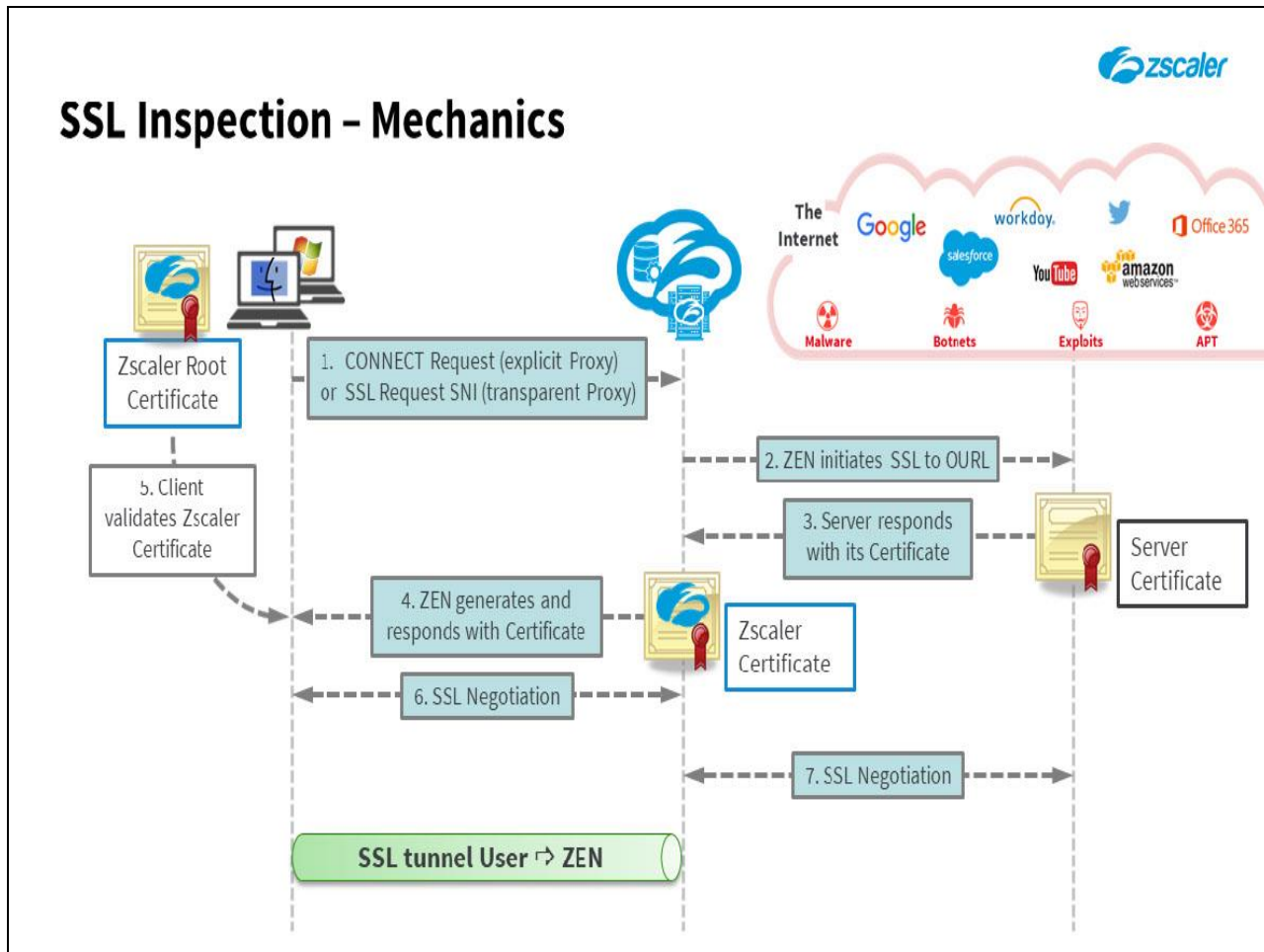
## Slide 15 - SSL Inspection – Mechanics



## Slide notes

6. The client and ZEN then establish an SSL connection...

## Slide 16 - SSL Inspection – Mechanics

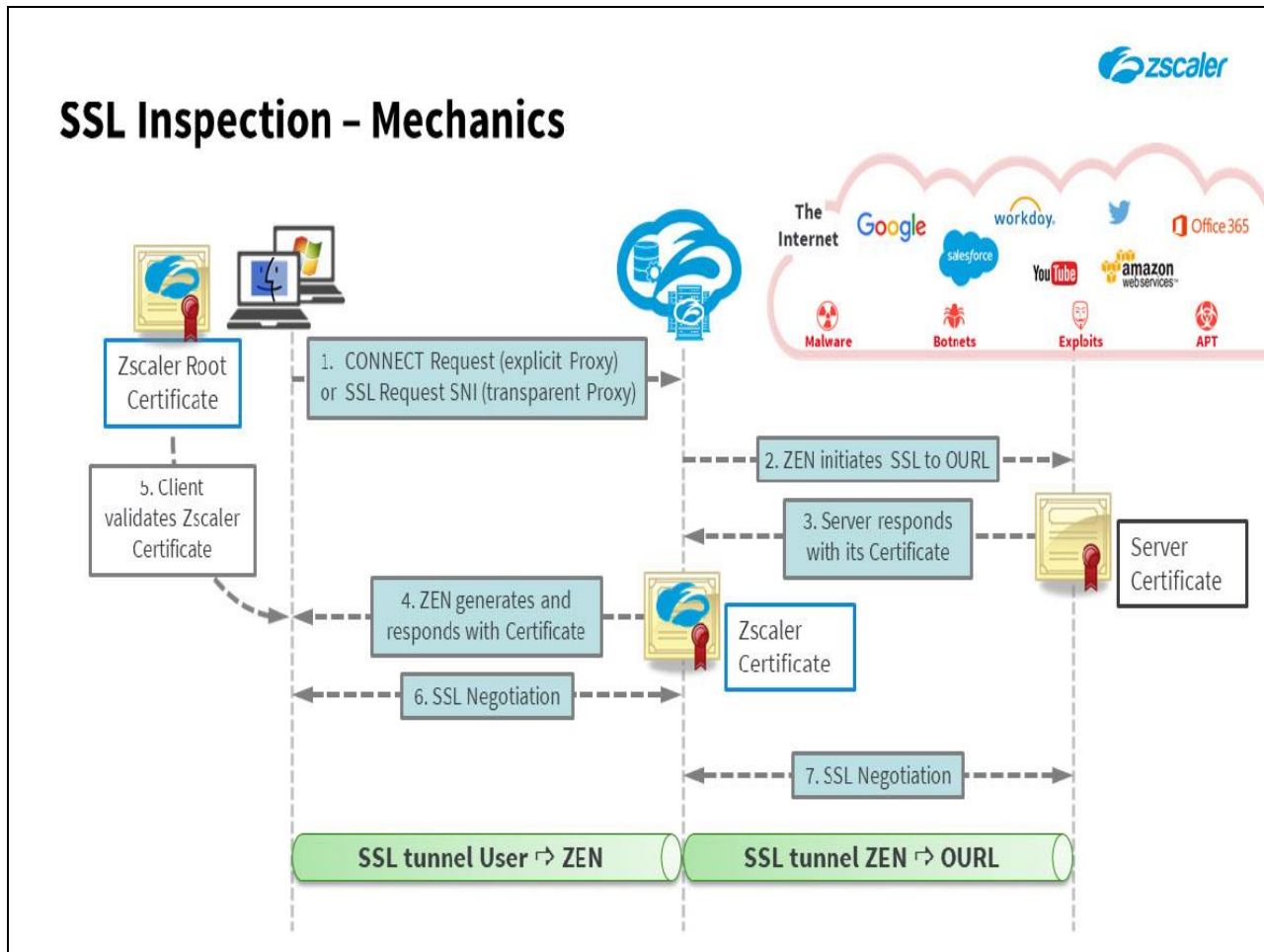


## Slide notes

7. And the ZEN establishes a connection to the server on the OURL.



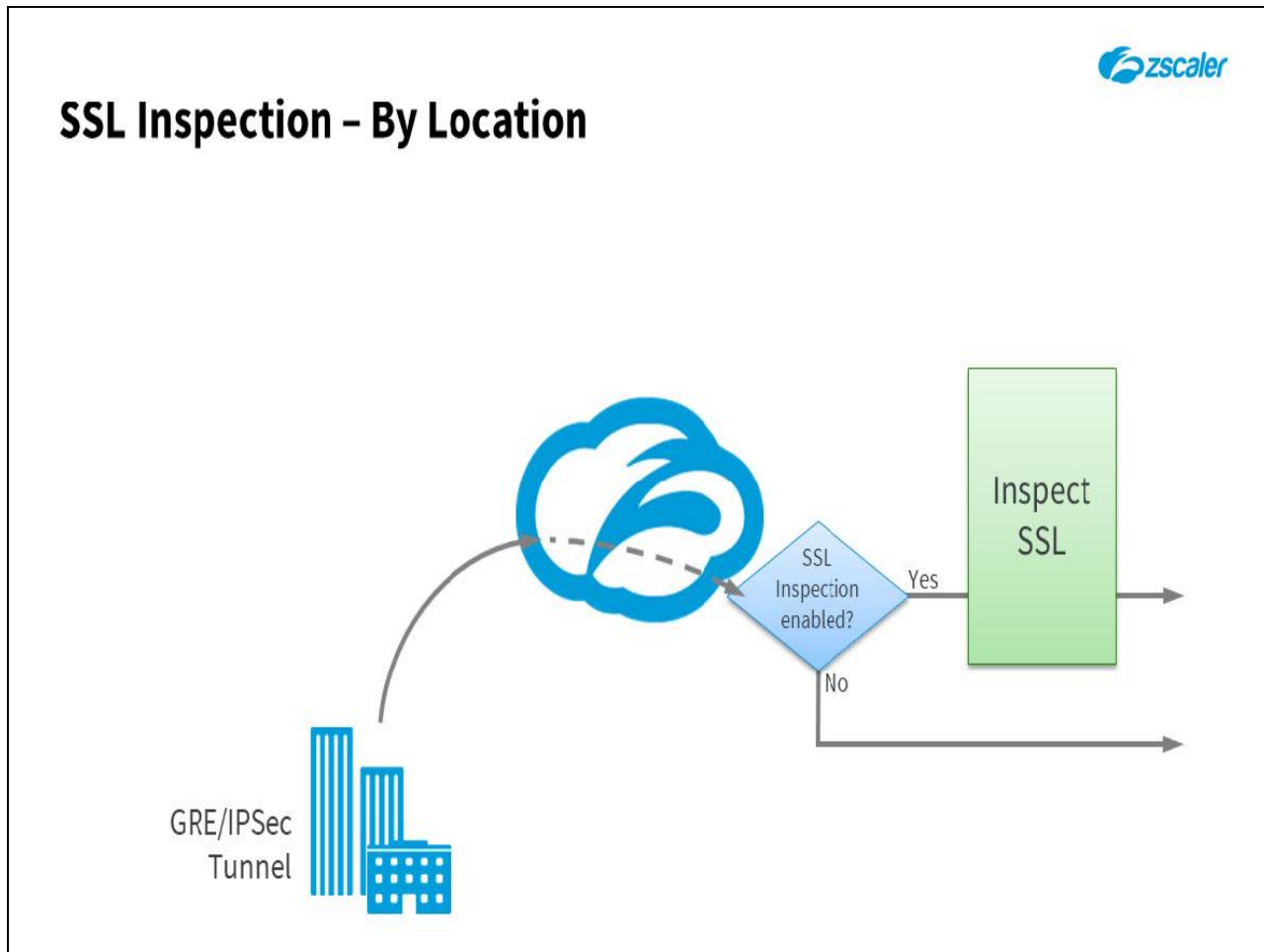
## Slide 17 - SSL Inspection – Mechanics



## Slide notes

In this way, the ZEN is in a position to inspect the traffic and apply policy as it flows in between tunnels.

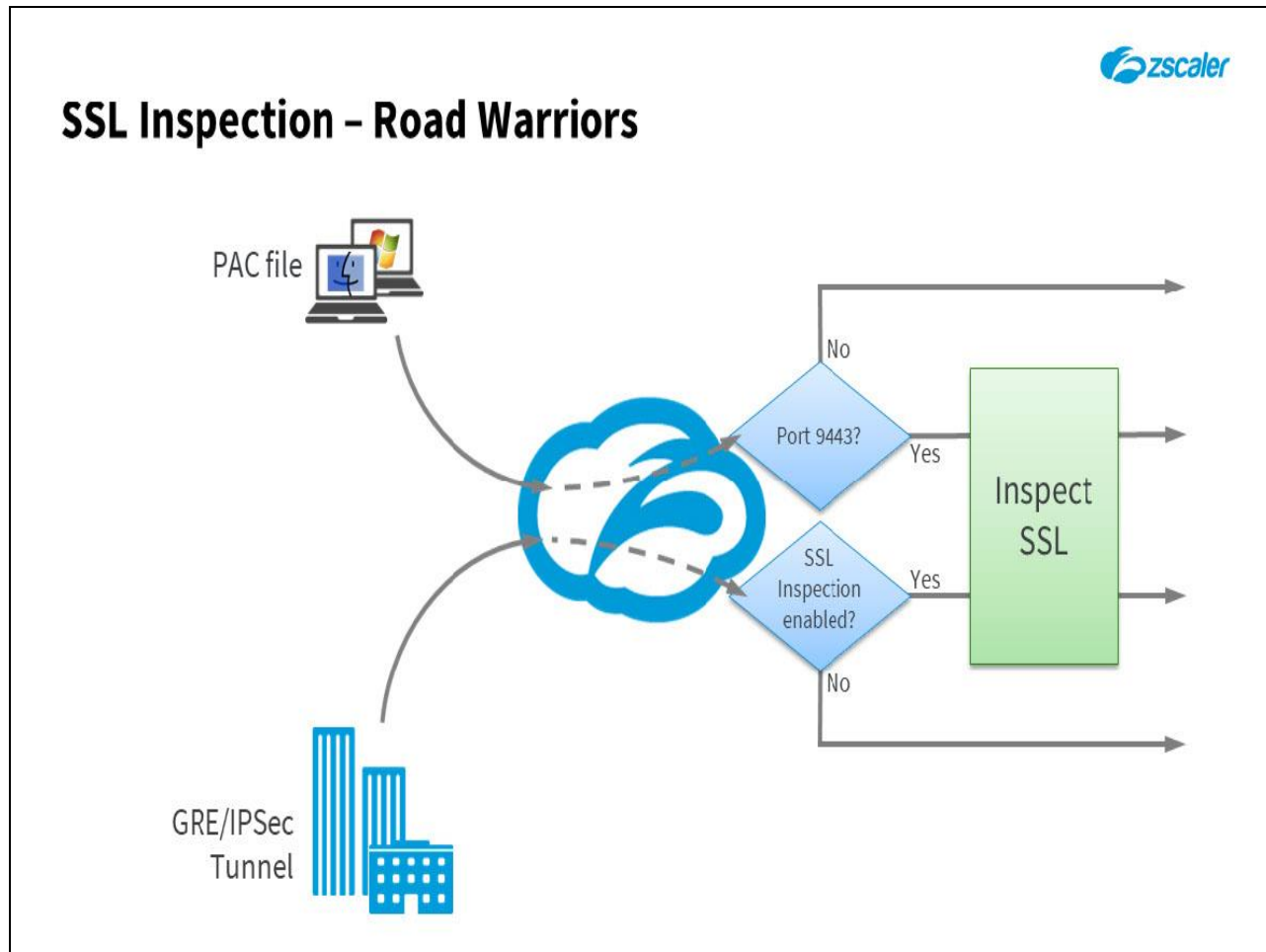
## Slide 18 - SSL Inspection – By Location



## Slide notes

SSL Inspection is enabled by location, and when creating a location, you will need to enable SSL Scanning for it.

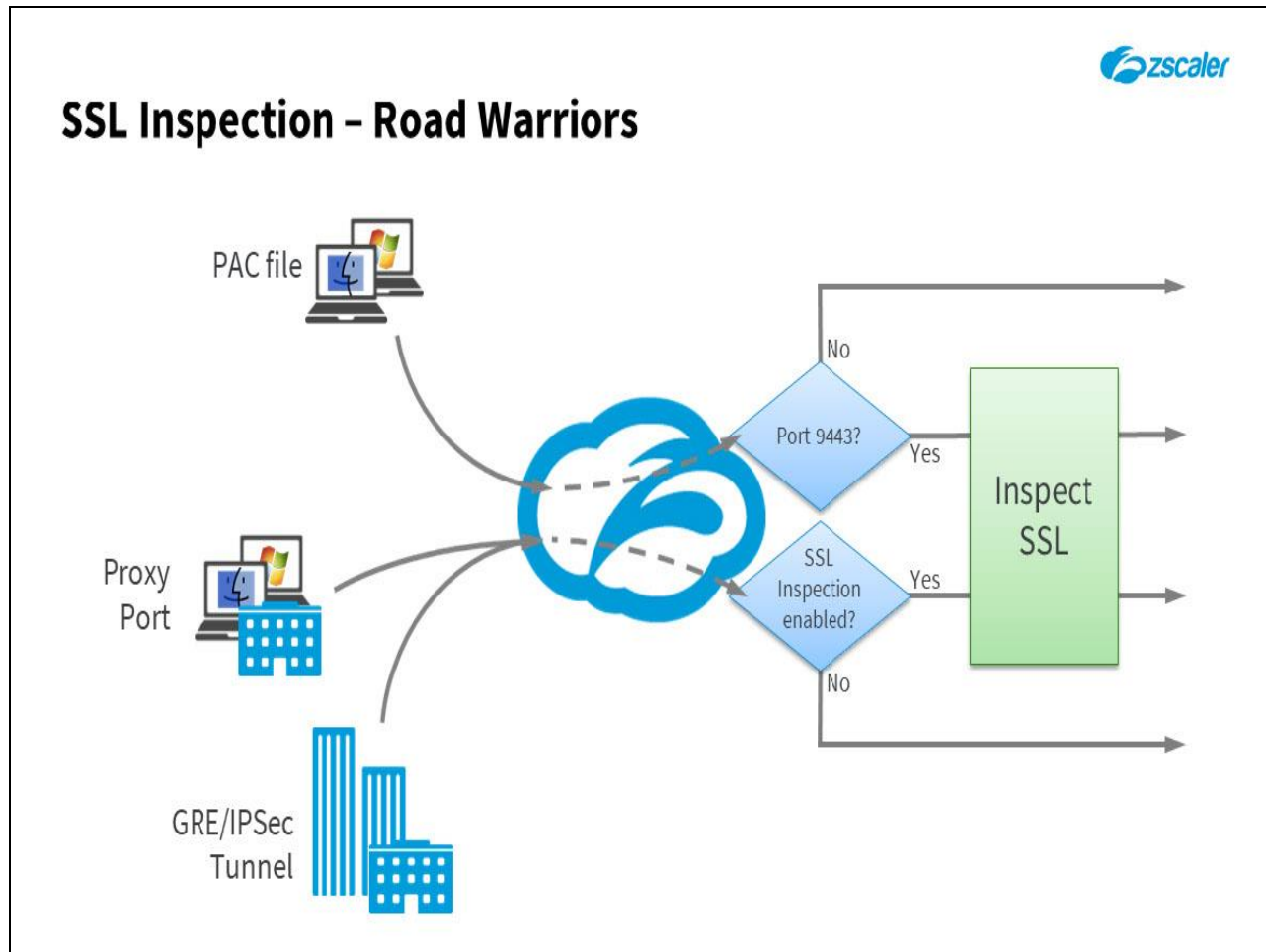
## Slide 19 - SSL Inspection – By Location

**Slide notes**

There are some extra steps we need to think about when we are dealing with Road Warriors, or users from an unknown location. The challenge is that when a user makes an SSL request from an unknown location, like a coffee shop, we have no way to identify the user.

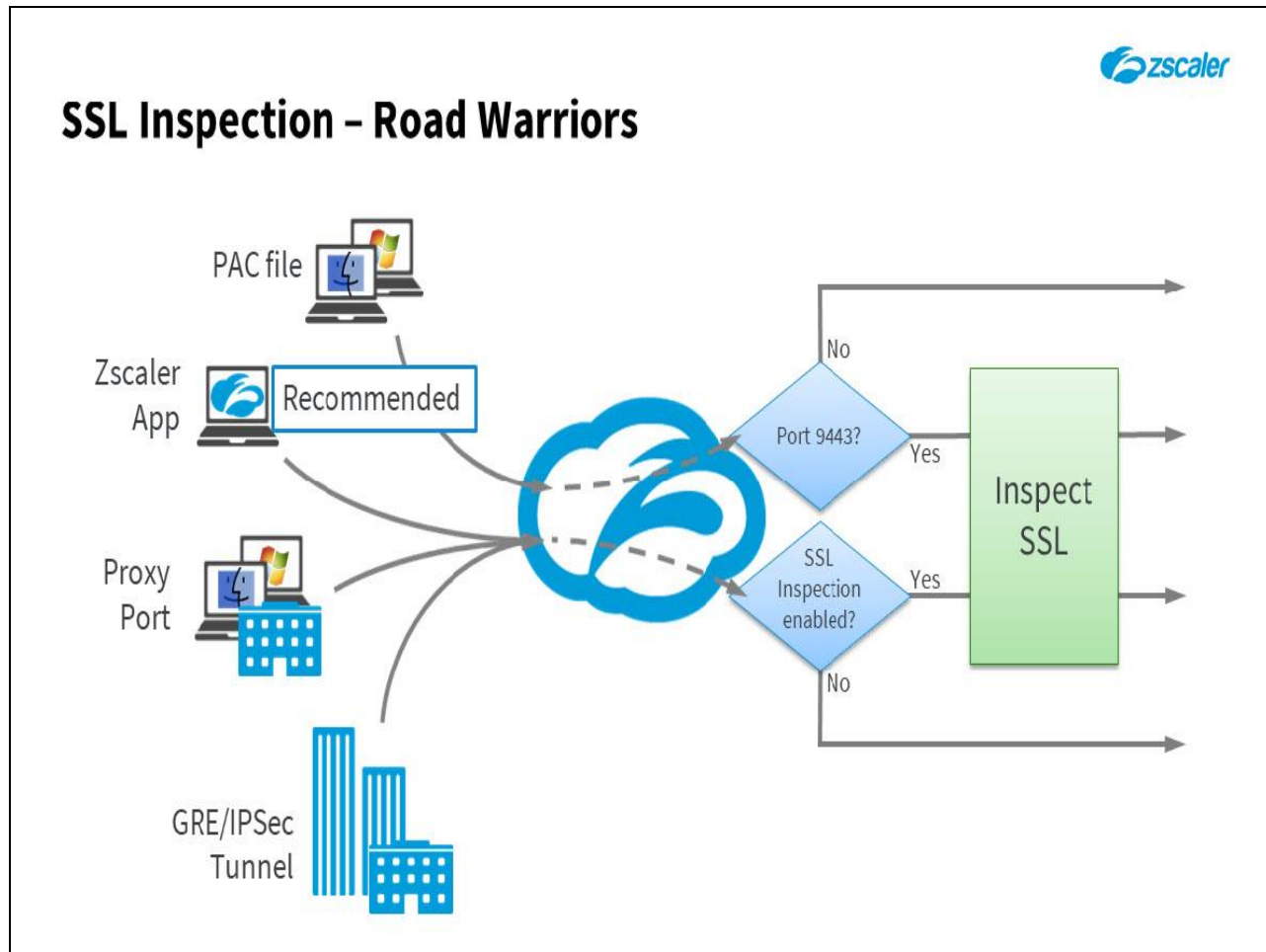
There are three ways to handle this for road warriors, and the first of these is to have the user connect to Zscaler using TCP port 9443, as all SSL requests on TCP 9443 will be inspected. This does mean however, that you cannot apply any SSL Inspection exemptions for categories such as banking or healthcare.

## Slide 20 - SSL Inspection – By Location

**Slide notes**

The second option is to purchase a dedicated TCP proxy port from Zscaler and set your Browsers to use it when connecting to Zscaler. That port will show up in your Locations list like any other Location and since that port is tied to your company and location we can apply the rules that you specify.


## Slide 21 - SSL Inspection – By Location

**Slide notes**

The third, and recommended option is to install and use the Zscaler App on the client machines of your road warrior users. In the SSL Inspection policy, you have the options to enable or disable SSL Inspection for Zscaler App users on a per-platform basis, for; 'Windows', MacOS', 'iOS', and 'Android'.

Note that for mobile apps certificate pinning is quite prevalent, which can require the configuration of many SSL Inspection exemptions. The alternative is to simply disable SSL Inspection on iOS or Android, although this does leave your organization vulnerable to any malware delivered on an SSL connection.

## Slide 22 - SSL Inspection Policy when NOT Inspecting SSL Traffic



## SSL Inspection Policy when NOT Inspecting SSL Traffic


**SSL Inspection Disabled**

- You may need to configure SSL Inspection Policy even when not inspecting SSL!

**Slide notes**

If you choose not to inspect SSL traffic at all, or if there are individual locations that you do not want to inspect, you may still need to configure the SSL Inspection Policy. For example, there may be URLs or URL categories that you want to block access to, even if the user tries to use SSL.

## Slide 23 - SSL Inspection Policy when NOT Inspecting SSL Traffic



## SSL Inspection Policy when NOT Inspecting SSL Traffic

### SSL Inspection Disabled

- You may need to configure SSL Inspection Policy even when not inspecting SSL!

### Global HTTPS Block


- Configure the **IF SSL INSPECTION IS DISABLED, BLOCK HTTPS TO THESE SITES** settings
- Option to **Show Notifications for Blocked Traffic**

## Slide notes

You will need add a Global HTTPS Block configuration by adding the URL categories, and/or specific URLs to be blocked in the 'IF SSL INSPECTION IS DISABLED, BLOCK HTTPS TO THESE SITES' section of the 'SSL Inspection' Policy. There is also an option to enable notifications to the end users that their SSL connections are being blocked.

If the location is known (or there is a dedicated proxy port), the user has authenticated, and the surrogate IP feature is enabled, then the 'URL and Cloud App Control Policy' can be applied as normal.

## Slide 24 - SSL Inspection Policy when NOT Inspecting SSL Traffic



## SSL Inspection Policy when NOT Inspecting SSL Traffic

### SSL Inspection Disabled

- You may need to configure SSL Inspection Policy even when not inspecting SSL!

### Global HTTPS Block

- Configure the **IF SSL INSPECTION IS DISABLED, BLOCK HTTPS TO THESE SITES** settings
- Option to **Show Notifications for Blocked Traffic**


**Note:** in order to for end users to view the block notifications page, they will need the Zscaler (or custom) root certificate installed

## Slide notes

Note that in order to for end users to view the block notifications page, they will need the Zscaler (or the custom) root certificate installed (otherwise they will see a blank page).



## Slide 25 - SSL Inspection Policy when NOT Inspecting SSL Traffic




## SSL Inspection Policy when NOT Inspecting SSL Traffic

- SSL Inspection Disabled**
  - You may need to configure SSL Inspection Policy even when not inspecting SSL!
- Global HTTPS Block**
  - Configure the **IF SSL INSPECTION IS DISABLED, BLOCK HTTPS TO THESE SITES** settings
  - Option to **Show Notifications for Blocked Traffic**
- No Policy Applied**
  - Roaming PAC File users with no Dedicated Proxy Port

**Slide notes**

The one exception is for PAC File roaming users with no Dedicated Proxy Port. For these users no Global HTTPS Block can be applied, nor can the 'URL & Cloud App Control Policy'. If roaming users connect using the Zscaler App, then a Global HTTPS Block can be applied.

## Slide 26 - Custom Certificate Management



## Custom Certificate Management

1.
  - Generate a CSR  
(Policy > Web > SSL Inspection page)


**Slide notes**

If you do not want to distribute the Zscaler root certificate to all your user's client devices, an option is to subscribe to the Custom Certificate option and configure a custom intermediate root certificate for SSL inspection. When you do this, Zscaler does not use its own certificate for the incoming SSL connections, instead, it uses the custom intermediate root certificate signed by your own CA. This way you can use a trusted CA that is already known and trusted by your end user's machines.

The process to generate, load and use a custom SSL certificate for your Zscaler service is as follows:

1. Firstly, generate a Certificate Signing Request (CSR) from the 'Policy > Web > SSL Inspection' page.

## Slide 27 - Custom Certificate Management



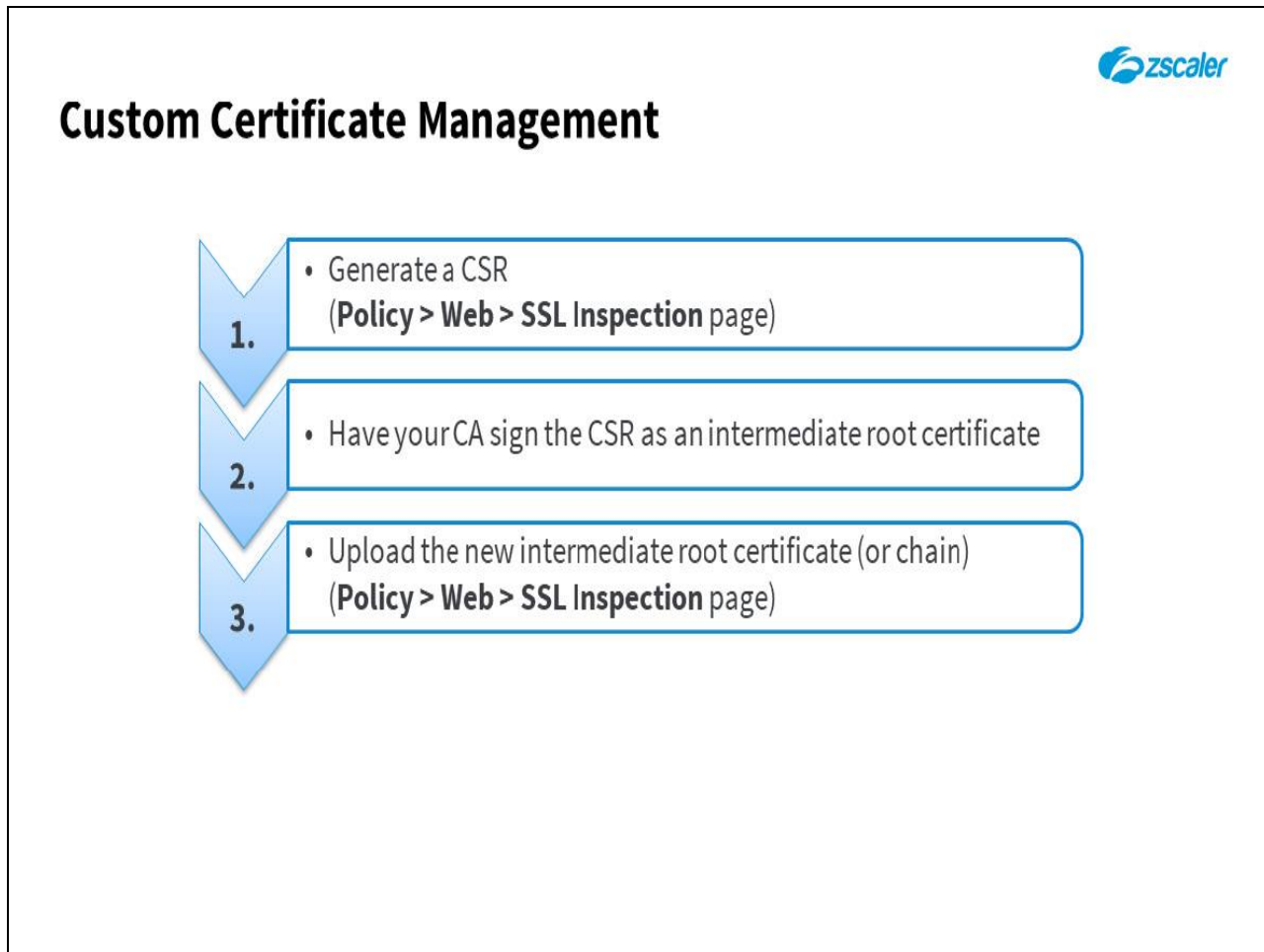
## Custom Certificate Management

1.
  - Generate a CSR  
(**Policy > Web > SSL Inspection** page)
2.
  - Have your CA sign the CSR as an intermediate root certificate

## Slide notes

2. Secondly - having downloaded the CSR from the Zscaler admin portal, send it to your internal CA for signing. Ensure that the CSR is signed as a Subordinate Certification Authority or Intermediate Certification Authority.

## Slide 28 - Custom Certificate Management




## Slide notes

3. Thirdly - upload the new intermediate root certificate issued by your internal CA to Zscaler, on the 'Policy > Web > SSL Inspection' page.

Optionally, you can upload the certificate chain that includes any other intermediate certificates that complete the chain to the intermediate root certificate you will upload. Having uploaded the certificate chain to Zscaler, Zscaler will send the intermediate root certificate along with this key chain and the signed server certificate to your users' machines when they initiate an SSL connection.

## Slide 29 - Custom Certificate Management




## Custom Certificate Management

1. • Generate a CSR  
(**Policy > Web > SSL Inspection** page)
2. • Have your CA sign the CSR as an intermediate root certificate
3. • Upload the new intermediate root certificate (or chain)  
(**Policy > Web > SSL Inspection** page)
4. • Enable the use of the intermediate root certificate  
(**Policy > Web > SSL Inspection** page)

## Slide notes

4. And finally - after you've uploaded the intermediate root certificate, turn on the 'Use Custom Certificate' option on the 'Policy > Web > SSL Inspection' page, to enable the Zscaler service to begin using your certificate for SSL inspection. Although, note that this only becomes visible after the successful upload of your custom certificate.

## Slide 30 - SSL Inspection – Pitfalls



## SSL Inspection – Pitfalls

Sites/Applications that use SSL Inspection Protection


- For example using 'Certificate Pinning'
- Client will only accept a specific certificate, or one from a specific certificate authority
- These sites must be added to the **Do Not Inspect Sessions to these URL Categories** list, on the **Policy > Web > SSL Inspection** page

**Slide notes**

There are some potential pitfalls to be aware of when enabling SSL inspection; the first of these is that some Websites or Web applications take steps to protect against SSL interception, even if they have been authorized. For example, the use of 'Certificate Pinning', where a client application will only accept a specific certificate, or one issued by a specific certificate authority, prevents Zscaler from inspecting SSL traffic.

Sites that use such SSL inspection protection mechanisms must be added to the 'Do Not Inspect Sessions to these Hosts' list on the SSL Inspection policy page.

## Slide 31 - SSL Inspection – Pitfalls




## SSL Inspection – Pitfalls

- Sites/Applications that use SSL Inspection Protection**
  - For example using 'Certificate Pinning'
  - Client will only accept a specific certificate, or one from a specific certificate authority
  - These sites must be added to the **Do Not Inspect Sessions to these URL Categories** list, on the **Policy > Web > SSL Inspection** page
- Application Unable to Use Zscaler Root Certificate**
  - Some client applications are unable to find, or use the Zscaler root certificate to validate the connection to a ZEN
  - Certificate warnings will always be displayed
  - The destination servers can be added to the **Do Not Inspect Sessions to these URL Categories** list

## Slide notes

There may be applications on the client devices (usually mobile devices) that are unable to find, or just don't look for the Zscaler root certificate, even when it is correctly installed. As a result, the user of the device will be prompted with certificate warnings when it connects to Zscaler. Once again, the resolution to this is to add problematic destinations to the 'Do Not Inspect Sessions to these Hosts' list in the SSL Inspection policy configuration.

## Slide 32 - SSL Inspection – Pitfalls



## SSL Inspection – Pitfalls

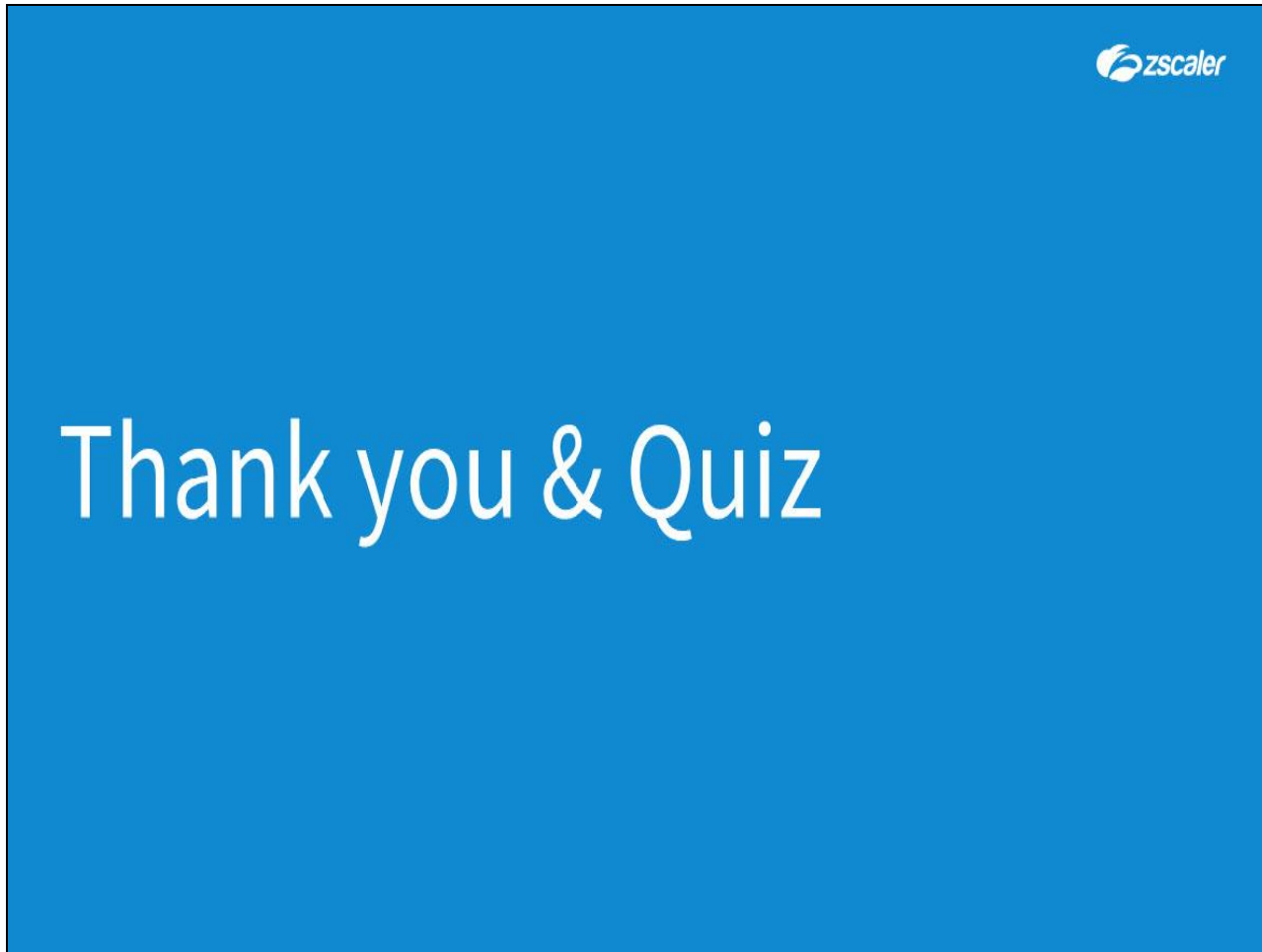
- Sites/Applications that use SSL Inspection Protection**
  - For example using 'Certificate Pinning'
  - Client will only accept a specific certificate, or one from a specific certificate authority
  - These sites must be added to the **Do Not Inspect Sessions to these URL Categories** list, on the **Policy > Web > SSL Inspection** page
- Application Unable to Use Zscaler Root Certificate**
  - Some client applications are unable to find, or use the Zscaler root certificate to validate the connection to a ZEN
  - Certificate warnings will always be displayed
  - The destination servers can be added to the **Do Not Inspect Sessions to these URL Categories** list
- OURL Server Certificate is Untrusted**
  - For example if a self-signed certificate is installed
  - Specify whether to **Allow**, **Pass Through**, or **Block** on the **Policy > Web > SSL Inspection** page

## Slide notes

There can also be issues if the certificate on the destination server is not trusted, for example if a self-signed certificate is installed. Here you have the option whether to simply 'Allow', or 'Block' access to such untrusted servers, or whether to pass through the certificate warnings to the end users, so that they are alerted to the problem. The behavior for untrusted sites is configured on the SSL Inspection policy page.



## Slide 33 - Thank you &amp; Quiz



## Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

Click the 'X' at top right to close this interface, then launch the quiz to test your knowledge of the material presented during this module. You may retake the quiz as many times as necessary in order to pass.