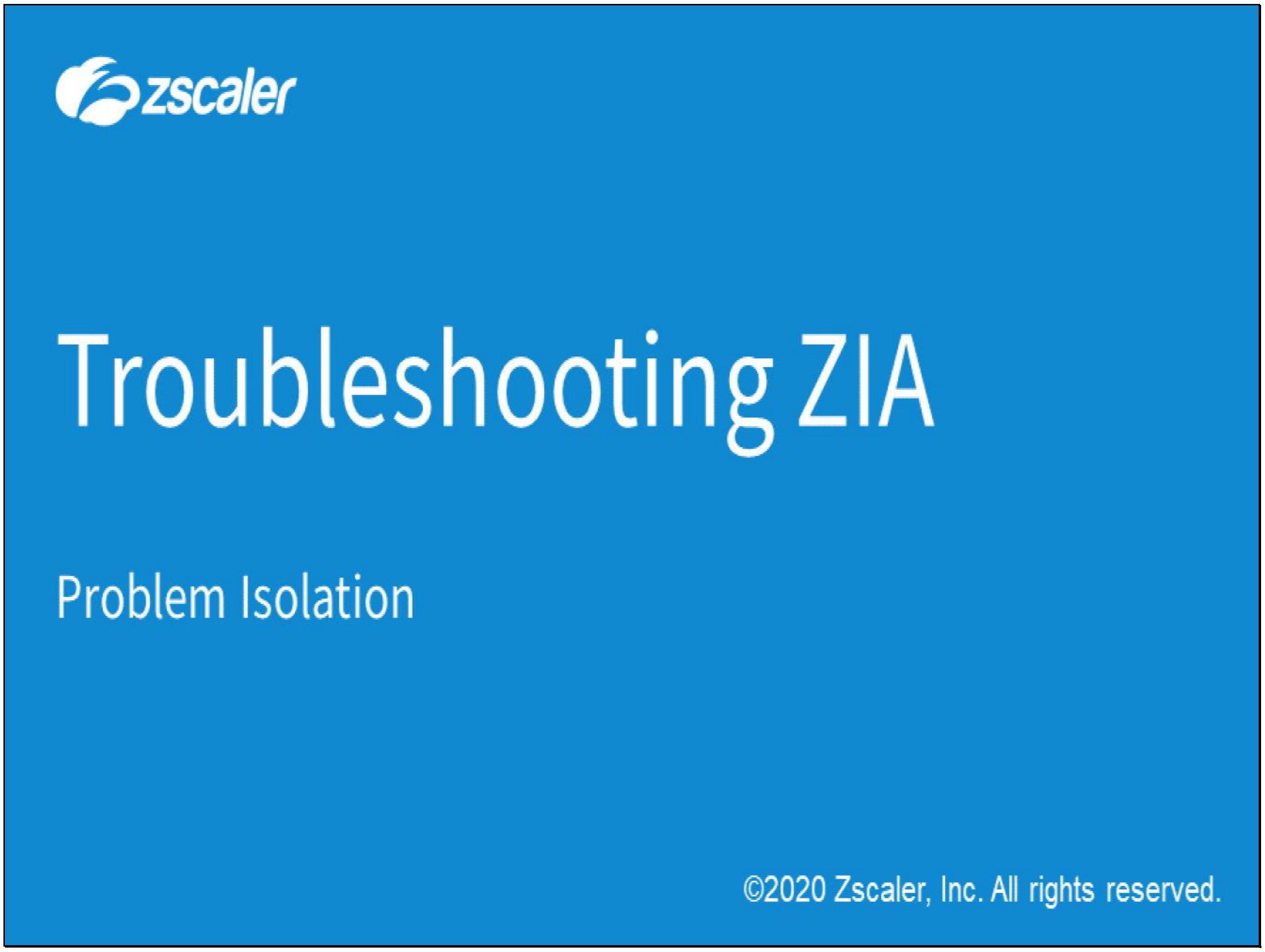
Slide 1 - Troubleshooting ZIA



Troubleshooting ZIA

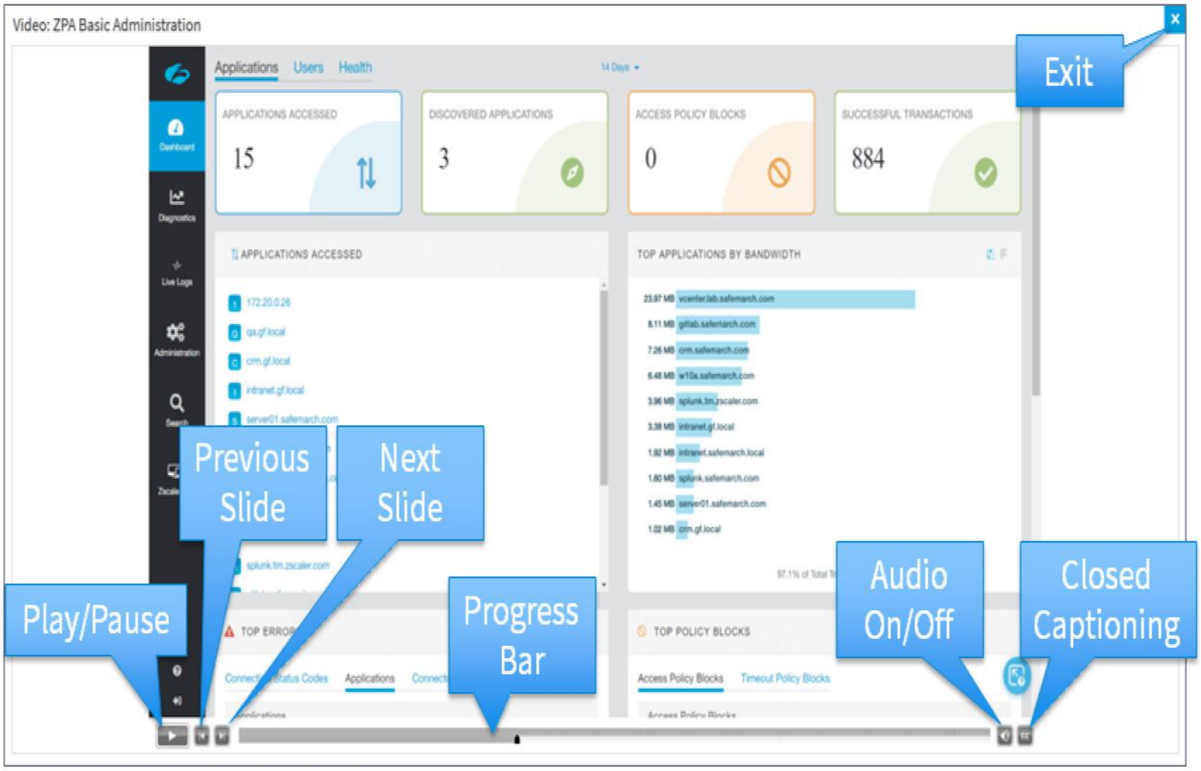
Problem Isolation

Slide notes

Welcome to this training module on isolating Zscaler Internet Access problems.

Slide 2 - Navigating the eLearning Module

Navigating the eLearning Module

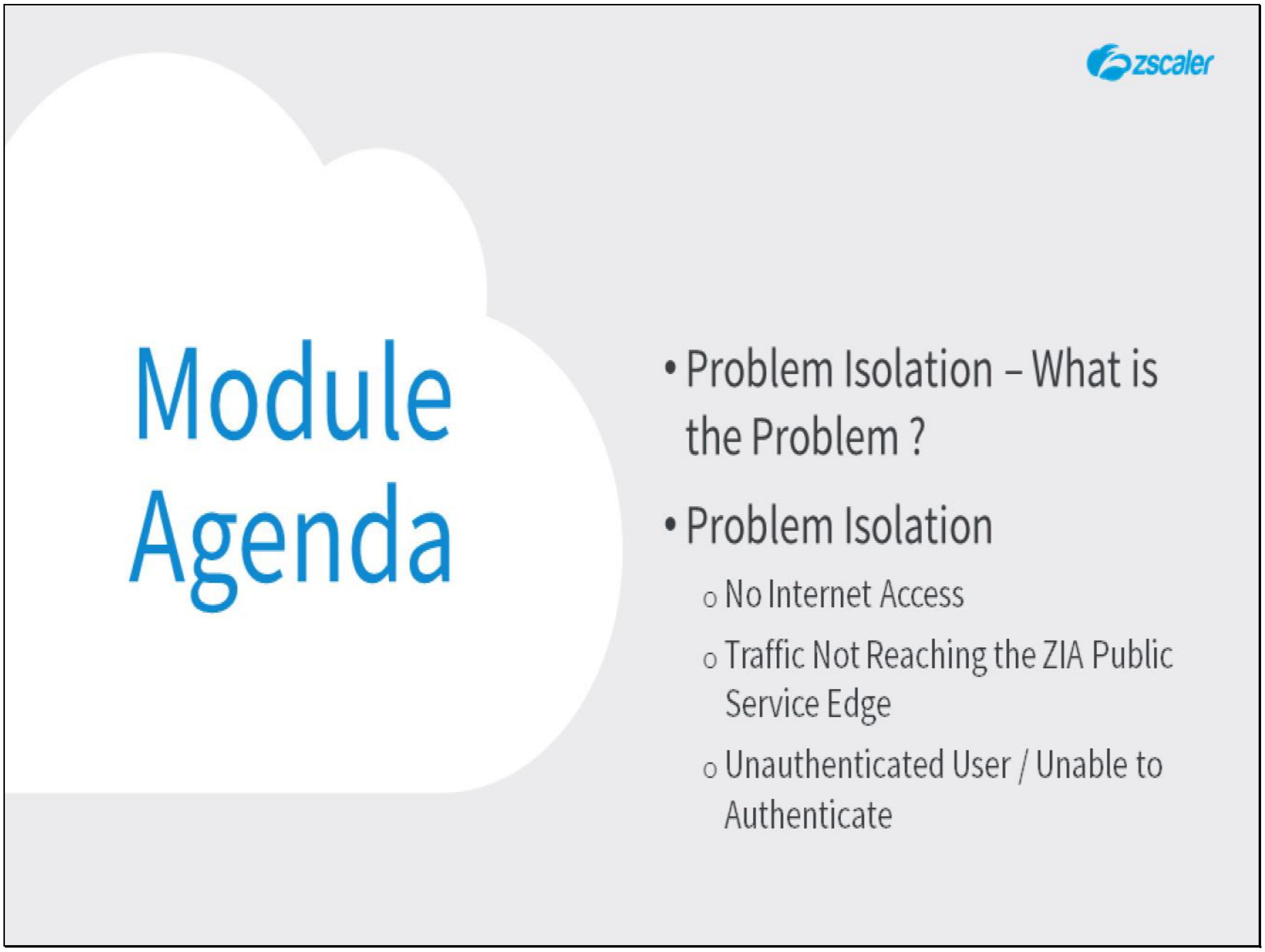


Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **play** and **pause**, **previous**, and **next** slide.

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 - Module Agenda



zscaler

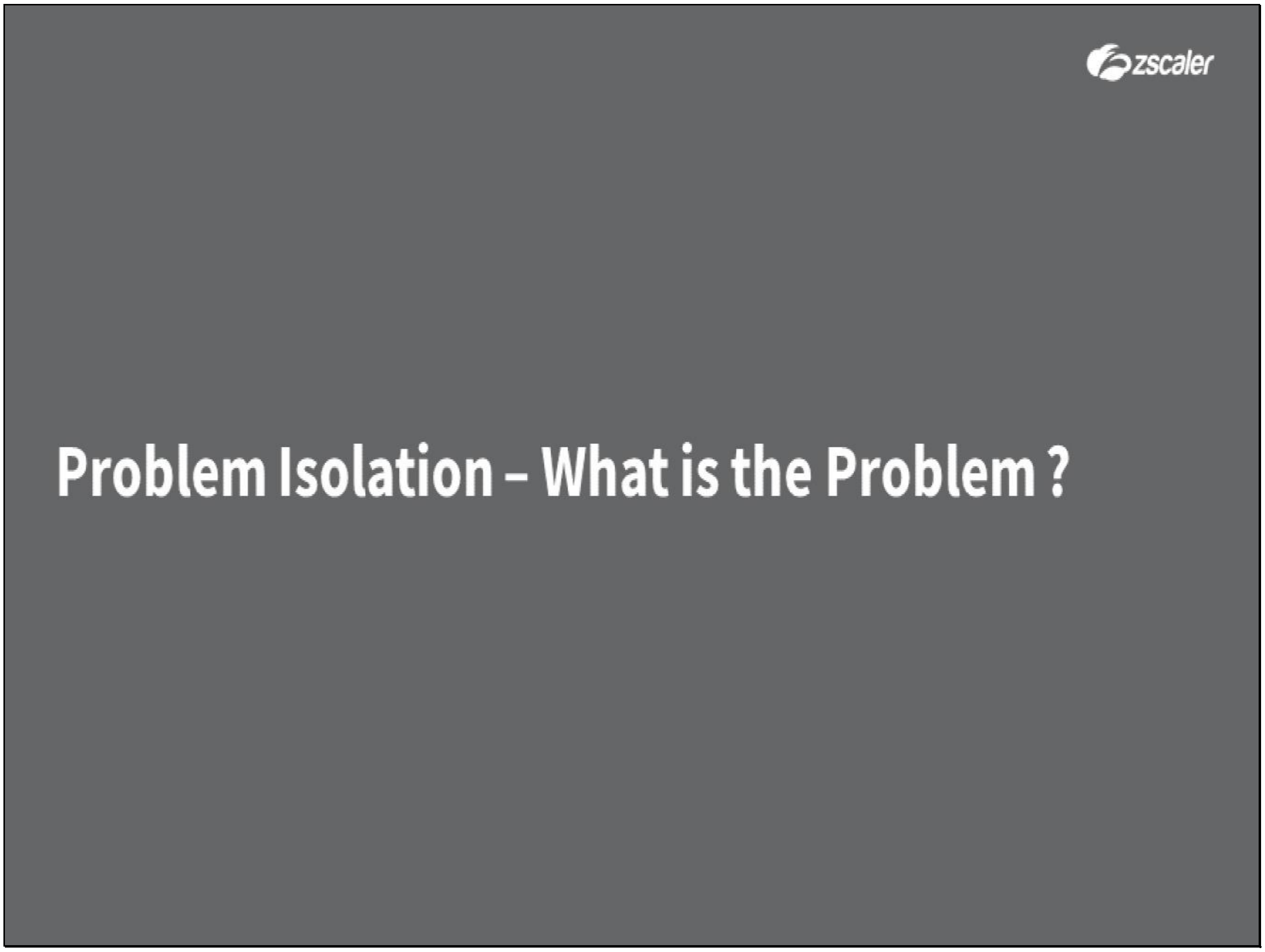
Module Agenda

- Problem Isolation – What is the Problem ?
- Problem Isolation
  - No Internet Access
  - Traffic Not Reaching the ZIA Public Service Edge
  - Unauthenticated User / Unable to Authenticate

Slide notes

In this module, we will look at the following topics: Problem isolation in general, to identify precisely what the problem is; and problem isolation in three situations: No Internet access at all; traffic not reaching the ZIA Public Service Edge; and users not being able to authenticate.

Slide 4 - Problem Isolation – What is the Problem ?

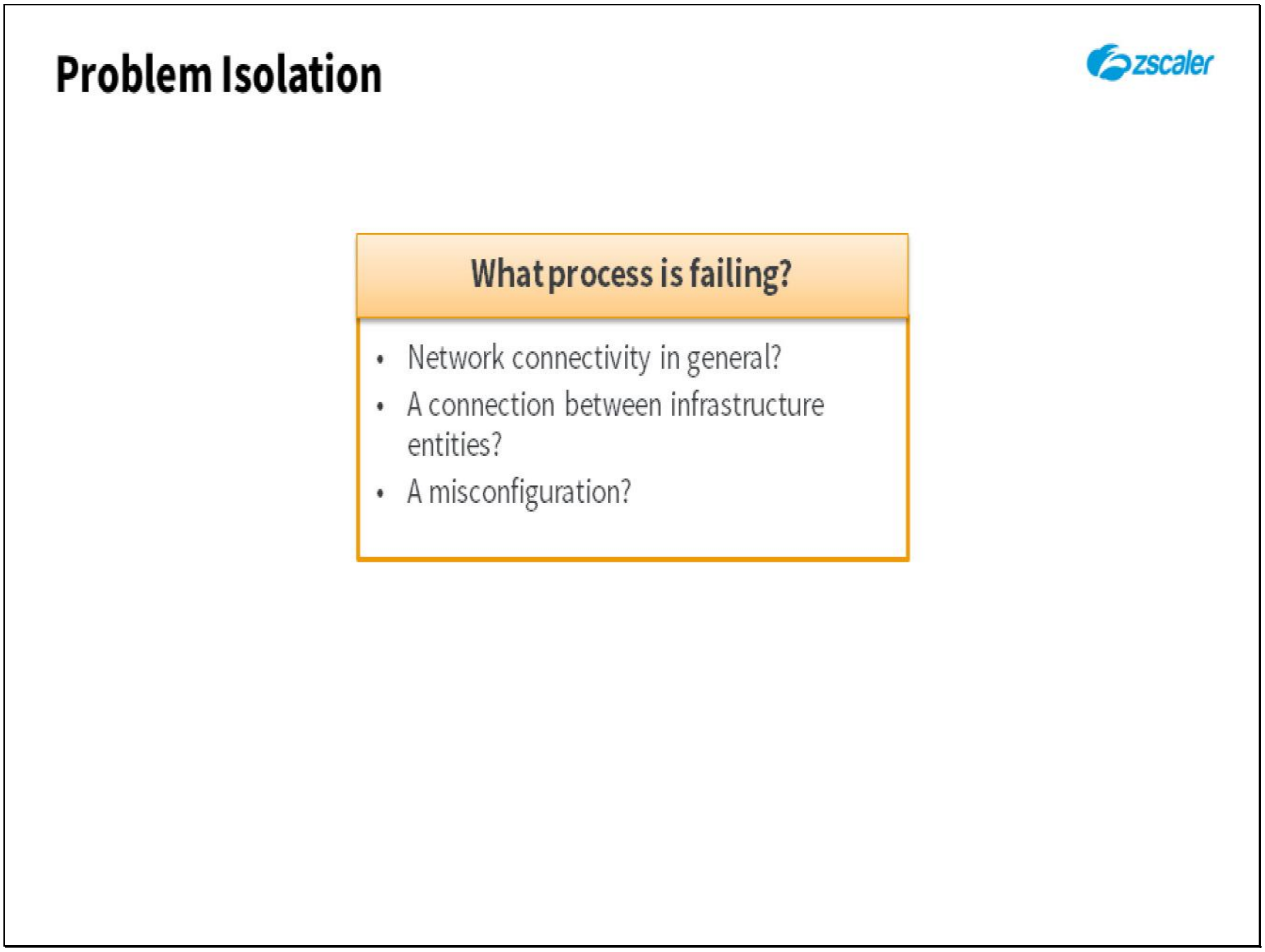


Problem Isolation – What is the Problem ?

Slide notes

In the first section, we will look at the concept of problem isolation in general, to identify precisely what the problem is.

Slide 5 - Problem Isolation



Problem Isolation

What process is failing?

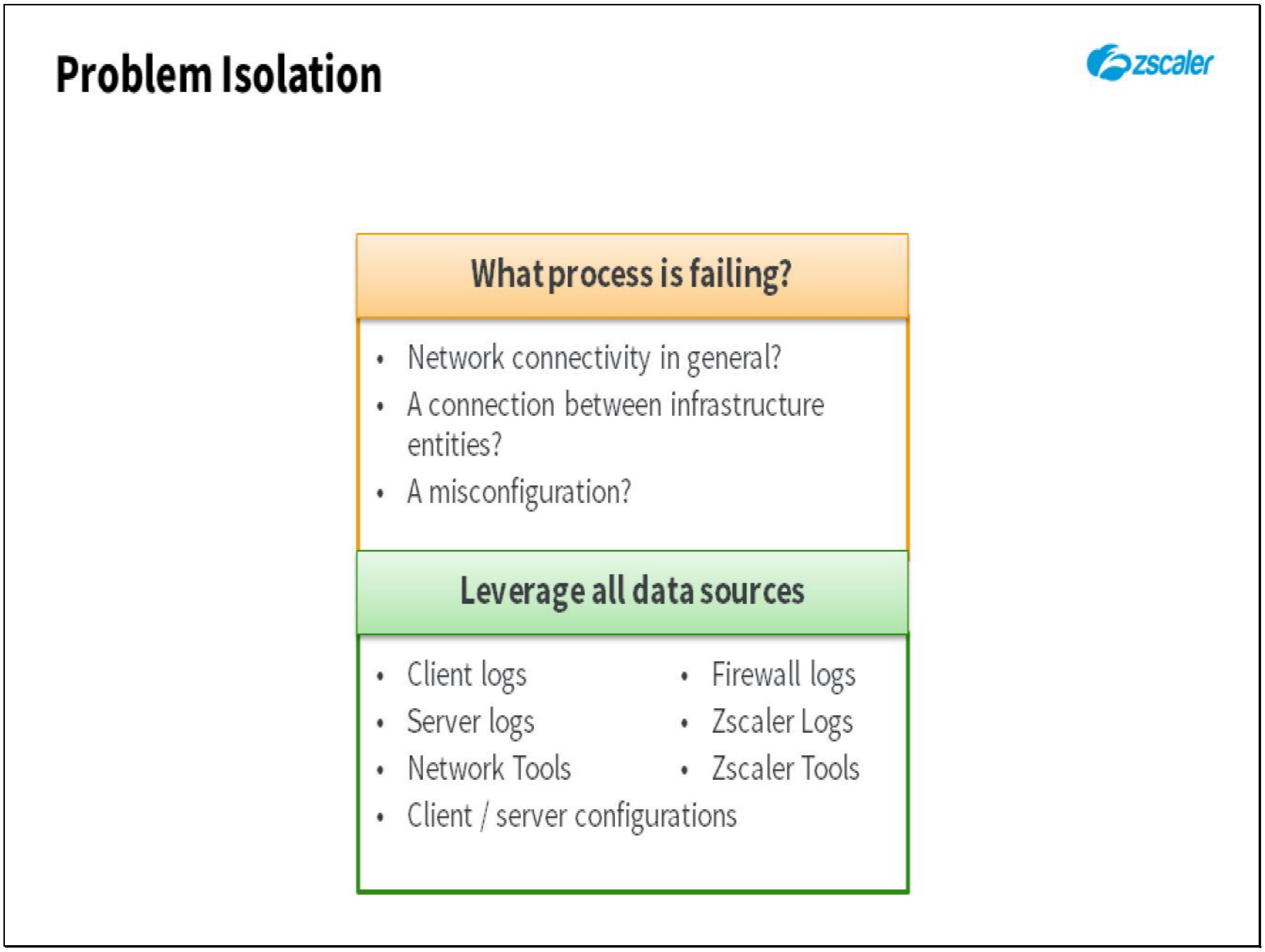
- Network connectivity in general?
- A connection between infrastructure entities?
- A misconfiguration?

Slide notes

Hopefully by this point you have localized the problem, so you know more or less where it is occurring, now we need to identify what logical process is failing.

Is there some general network connectivity issue? Is there a problem between infrastructure entities, for example between the Identity Provider and Service Provider in a SAML implementation? Or is there a misconfiguration somewhere, within the infrastructure, or on the Zscaler Cloud?

Slide 6 - Problem Isolation



Problem Isolation

zscaler

What process is failing?

- Network connectivity in general?
- A connection between infrastructure entities?
- A misconfiguration?

Leverage all data sources

- Client logs
- Server logs
- Network Tools
- Client / server configurations
- Firewall logs
- Zscaler Logs
- Zscaler Tools

Slide notes

Once you have a good idea **where** a problem is occurring, you can make use of all the related sources of data to help you finally diagnose **what** the problem actually is. Logs can be a particularly helpful source of information, logs from software on the client device, the server the client is attempting to connect to, logs from some intermediate device or infrastructure component, such as; router or Firewall, authentication server or IdP, and of course there are the Zscaler logs.

You should make use of all the tools available to you, whether general networking tools, or those provided by Zscaler. Plus, you should start to review the configuration settings of the implicated components.

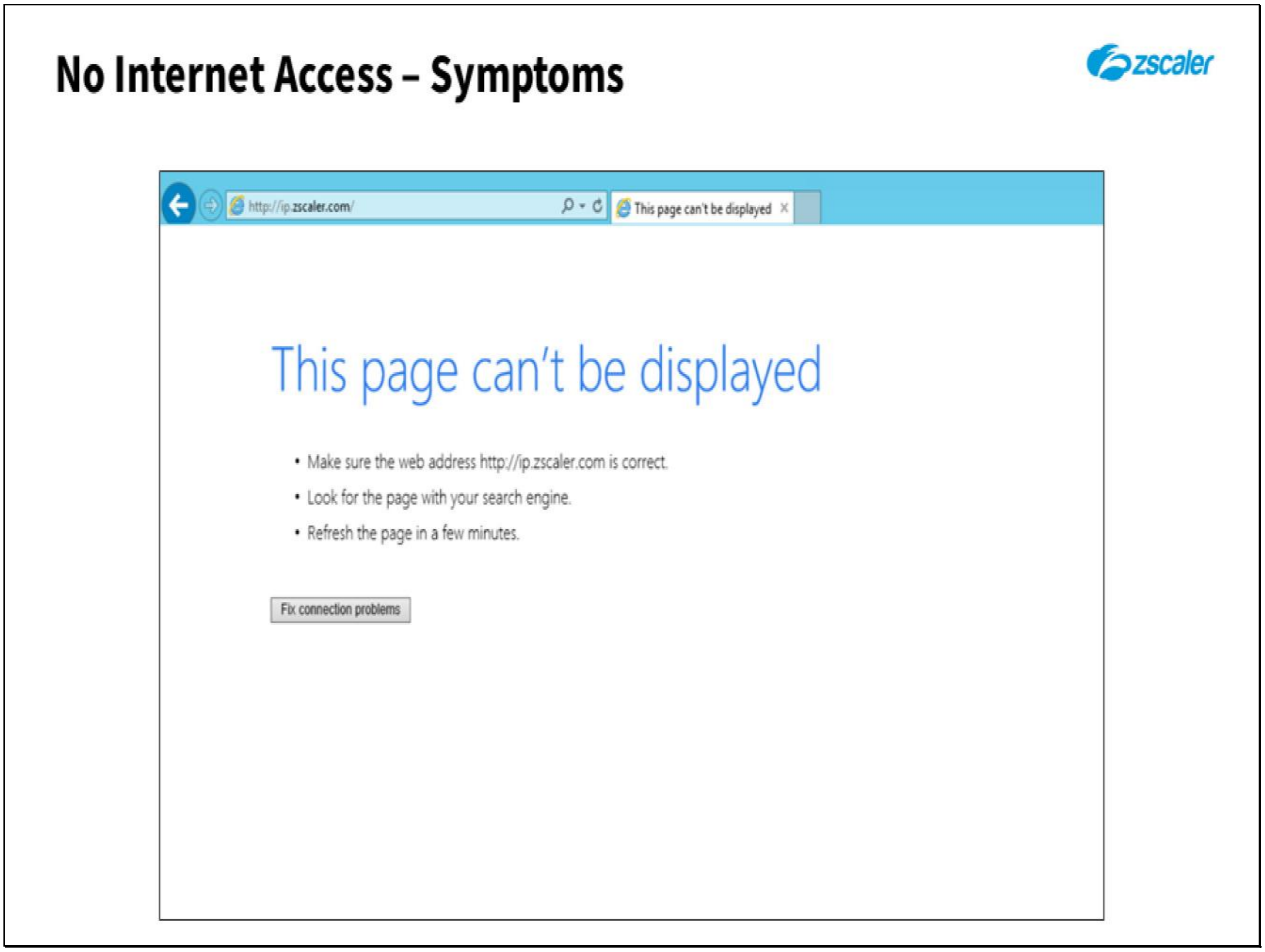
Slide 7 - No Internet Access

No Internet Access

Slide notes

In the next section, we will look at symptoms and possible causes for when a user has no Internet connectivity at all.

Slide 8 - No Internet Access – Symptoms



No Internet Access – Symptoms

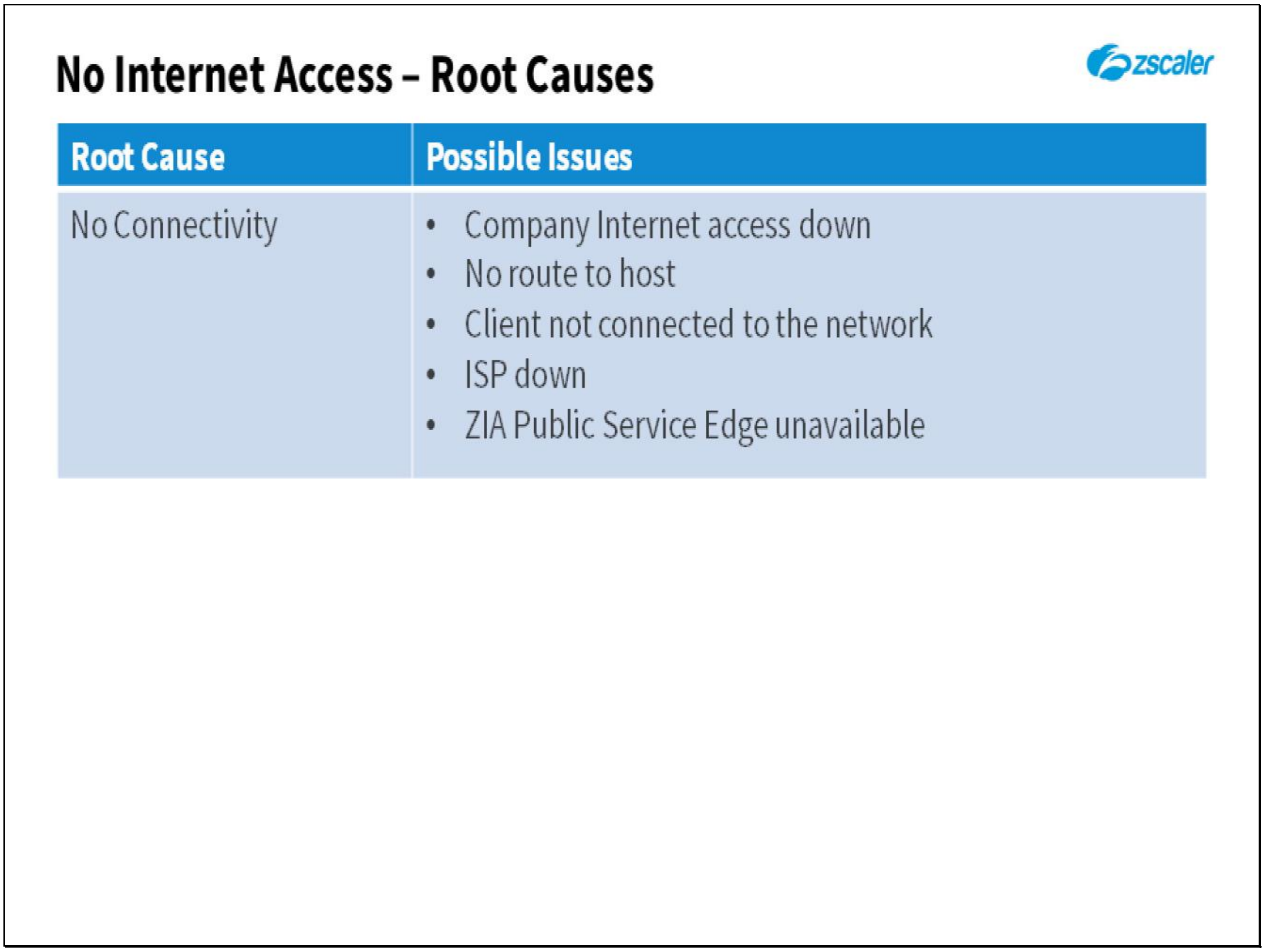
This page can’t be displayed

- Make sure the web address http://ip.zscaler.com is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Slide notes

The primary symptom an end user will experience is that they cannot reach any destination on the Internet.

Slide 9 - No Internet Access – Root Causes



No Internet Access – Root Causes

Root Cause	Possible Issues
No Connectivity	• Company Internet access down • No route to host • Client not connected to the network • ISP down • ZIA Public Service Edge unavailable

Slide notes

There are four main root causes for an inability to access the Internet, and you should start by checking the potential issues listed here to ensure that the client is connected to the network:

You can perform several tests; for instance, on a Windows machine you can:

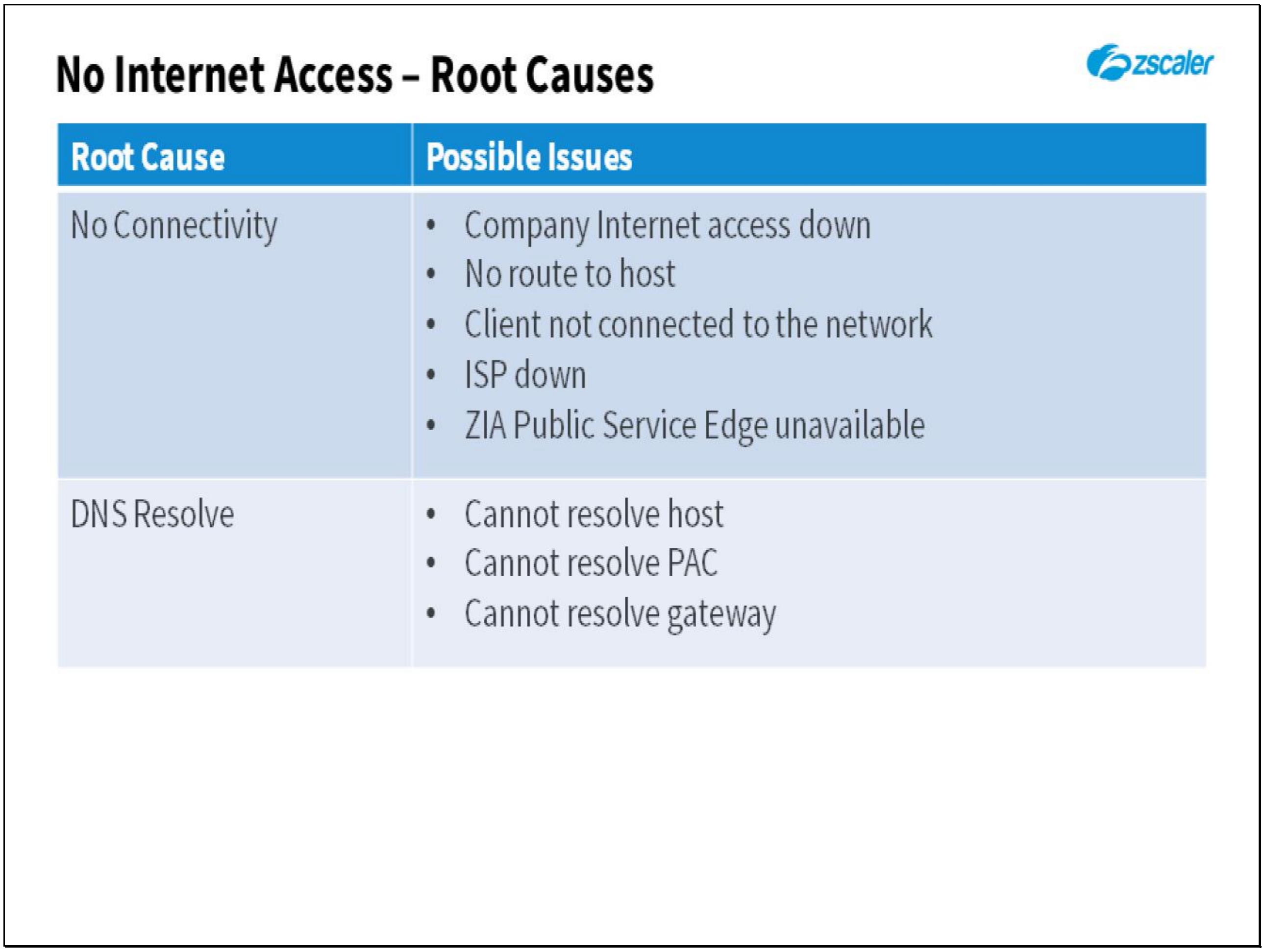
- Run the **ipconfig** command and verify that the client has an IP address.
- Run the **ping** command to the default gateway of the client.

You should verify that the ISP is reachable, to do this you can:

- Run the **ping** command to an external IP address (for example the Google DNS site 8.8.8.8 responds to pings)
- Run the **traceroute** command to an external IP address.

You should also verify that the ZIA Public Service Edge you are trying to reach is actually available. To do this visit the URL **https://trust.zscaler.com**, which shows the real-time status of the Zscaler cloud.

Slide 10 - No Internet Access – Root Causes



No Internet Access – Root Causes

Root Cause	Possible Issues
No Connectivity	• Company Internet access down • No route to host • Client not connected to the network • ISP down • ZIA Public Service Edge unavailable
DNS Resolve	• Cannot resolve host • Cannot resolve PAC • Cannot resolve gateway

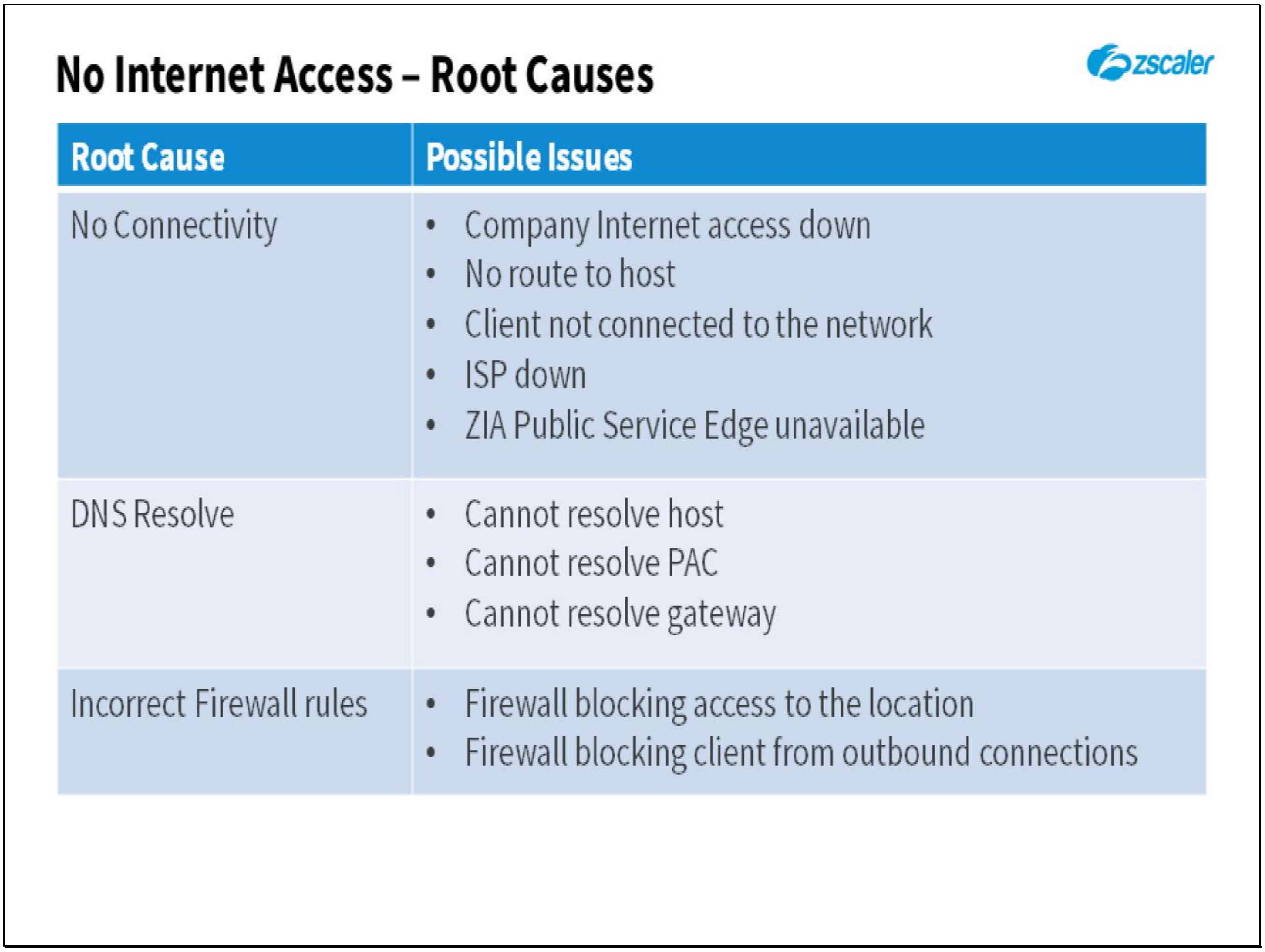
Slide notes

Next, ensure that DNS is resolving the required hosts correctly. There are three key hosts that need to be resolved, depending on whether the client is using explicit proxy settings or not:

- For a client device with explicit proxy settings (meaning a PAC file is applied to it), the following need to be resolved:
- The server on which the PAC file is stored.
- The ZIA Public Service Edge.

For the transparent proxy scenario, where the user is connecting through a tunnel at a fixed location, the host in the URL that the client is attempting to access must be resolvable.

Slide 11 - No Internet Access – Root Causes



No Internet Access – Root Causes

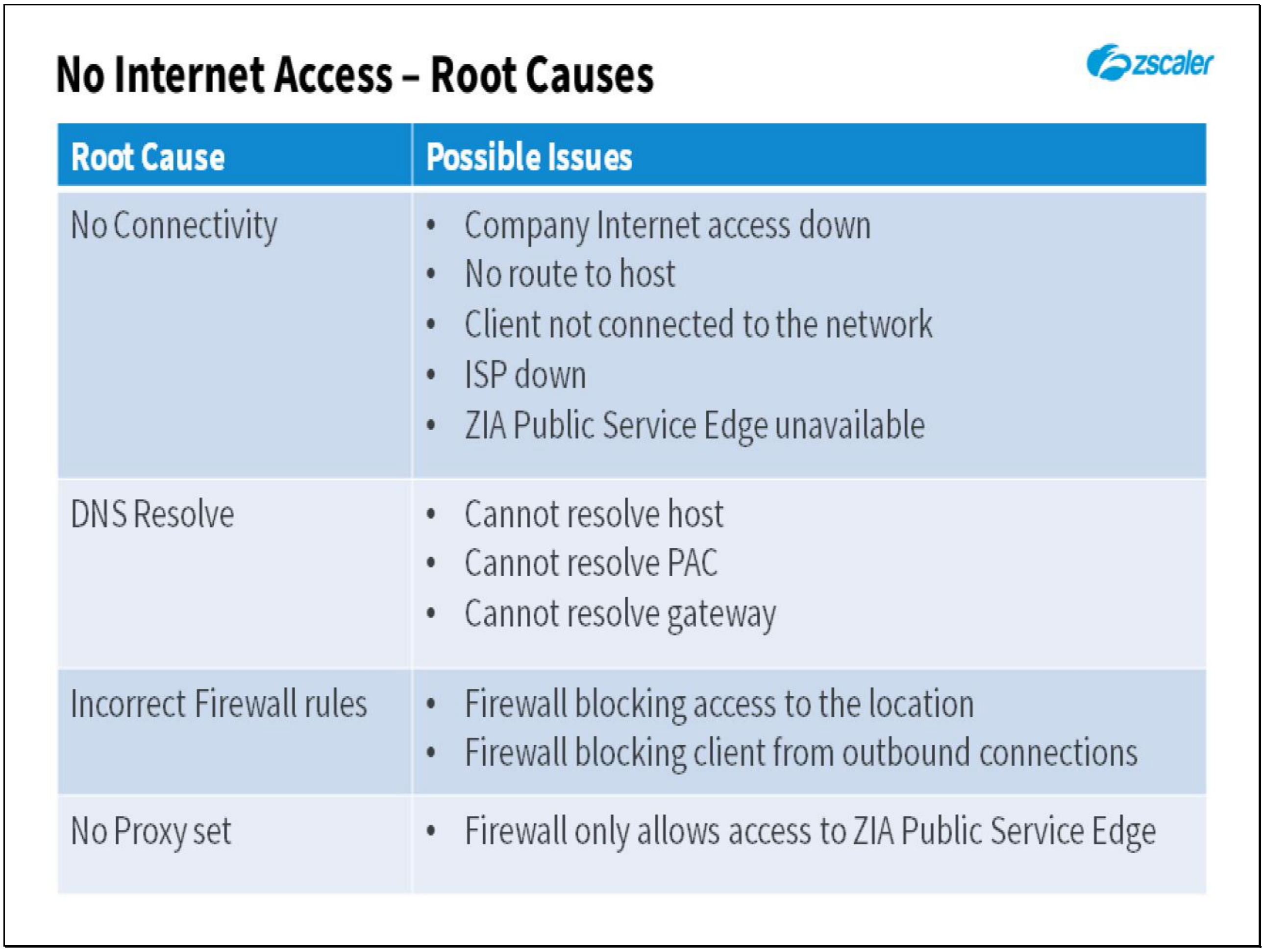
Root Cause	Possible Issues
No Connectivity	• Company Internet access down • No route to host • Client not connected to the network • ISP down • ZIA Public Service Edge unavailable
DNS Resolve	• Cannot resolve host • Cannot resolve PAC • Cannot resolve gateway
Incorrect Firewall rules	• Firewall blocking access to the location • Firewall blocking client from outbound connections

Slide notes

The last two root causes both relate to the firewall configuration. It is possible that the customer’s firewall is either:

- Blocking access to the location the user is trying to access (either URL or ZIA Public Service Edge).
- Or, blocking the client from any and all outbound connections.

Slide 12 - No Internet Access – Root Causes



No Internet Access – Root Causes

Root Cause	Possible Issues
No Connectivity	• Company Internet access down • No route to host • Client not connected to the network • ISP down • ZIA Public Service Edge unavailable
DNS Resolve	• Cannot resolve host • Cannot resolve PAC • Cannot resolve gateway
Incorrect Firewall rules	• Firewall blocking access to the location • Firewall blocking client from outbound connections
No Proxy set	• Firewall only allows access to ZIA Public Service Edge

Slide notes

This second item closely relates to the root cause ‘No proxy set’. In many companies, end users cannot access the Internet directly, they must go through a pre-defined proxy.

For instance, the proxy may block all access to the Internet unless the user connects to a ZIA Public Service Edge. If the Browser is not configured with a Proxy or a PAC file, the user will be unable to connect to any Internet resource.

Slide 13 - Traffic Not Reaching the ZIA Public Service Edge

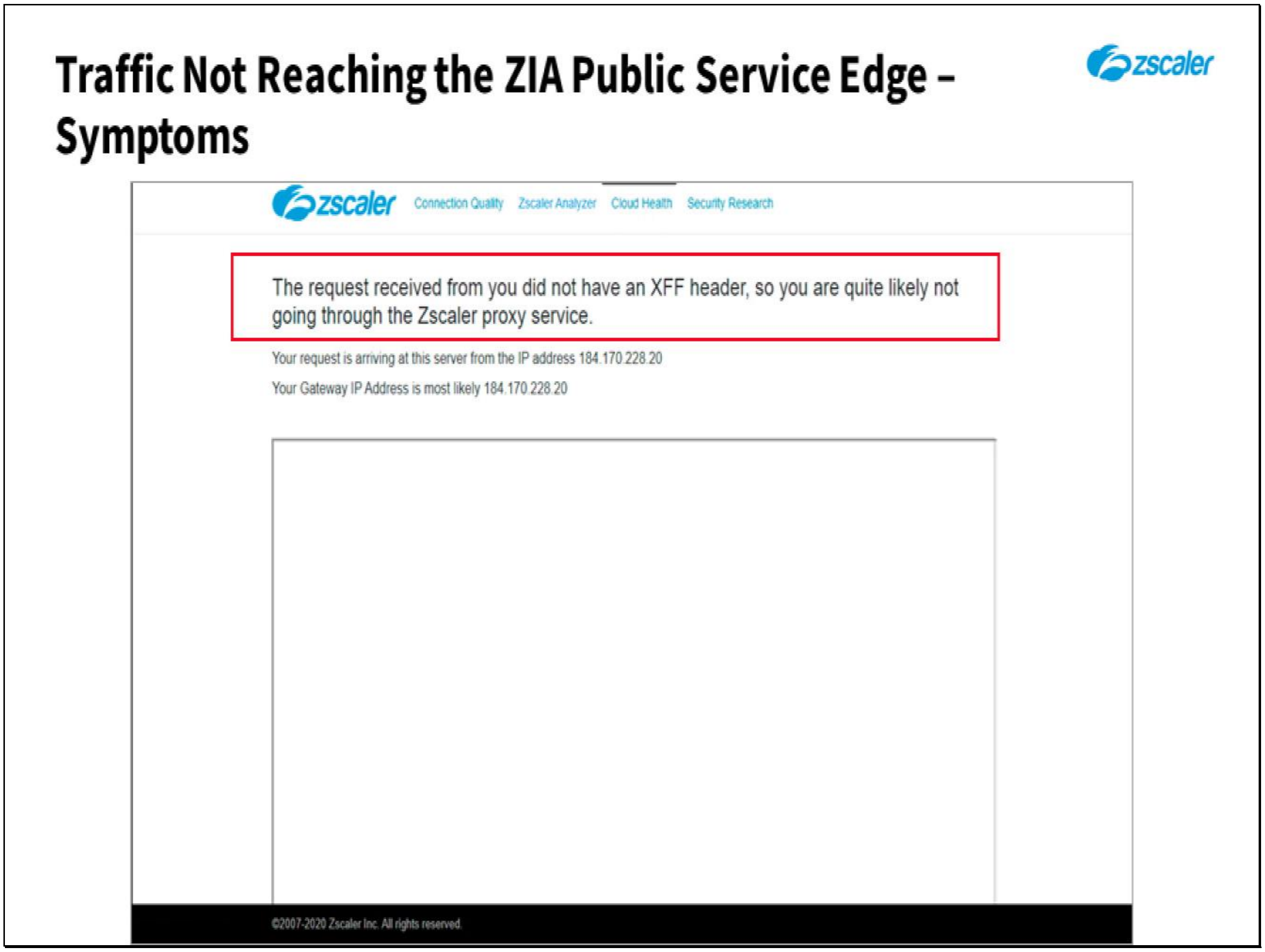
Traffic Not Reaching the ZIA Public Service Edge

Slide notes

In the next section, we will look at symptoms and possible causes for when traffic from the user does not reach the ZIA Public Service Edge.

Slide 14 - Traffic Not Reaching the ZIA Public Service Edge –

Symptoms



Traffic Not Reaching the ZIA Public Service Edge – Symptoms

The request received from you did not have an XFF header, so you are quite likely not going through the Zscaler proxy service.

Your request is arriving at this server from the IP address 184.170.228.20

Your Gateway IP Address is most likely 184.170.228.20

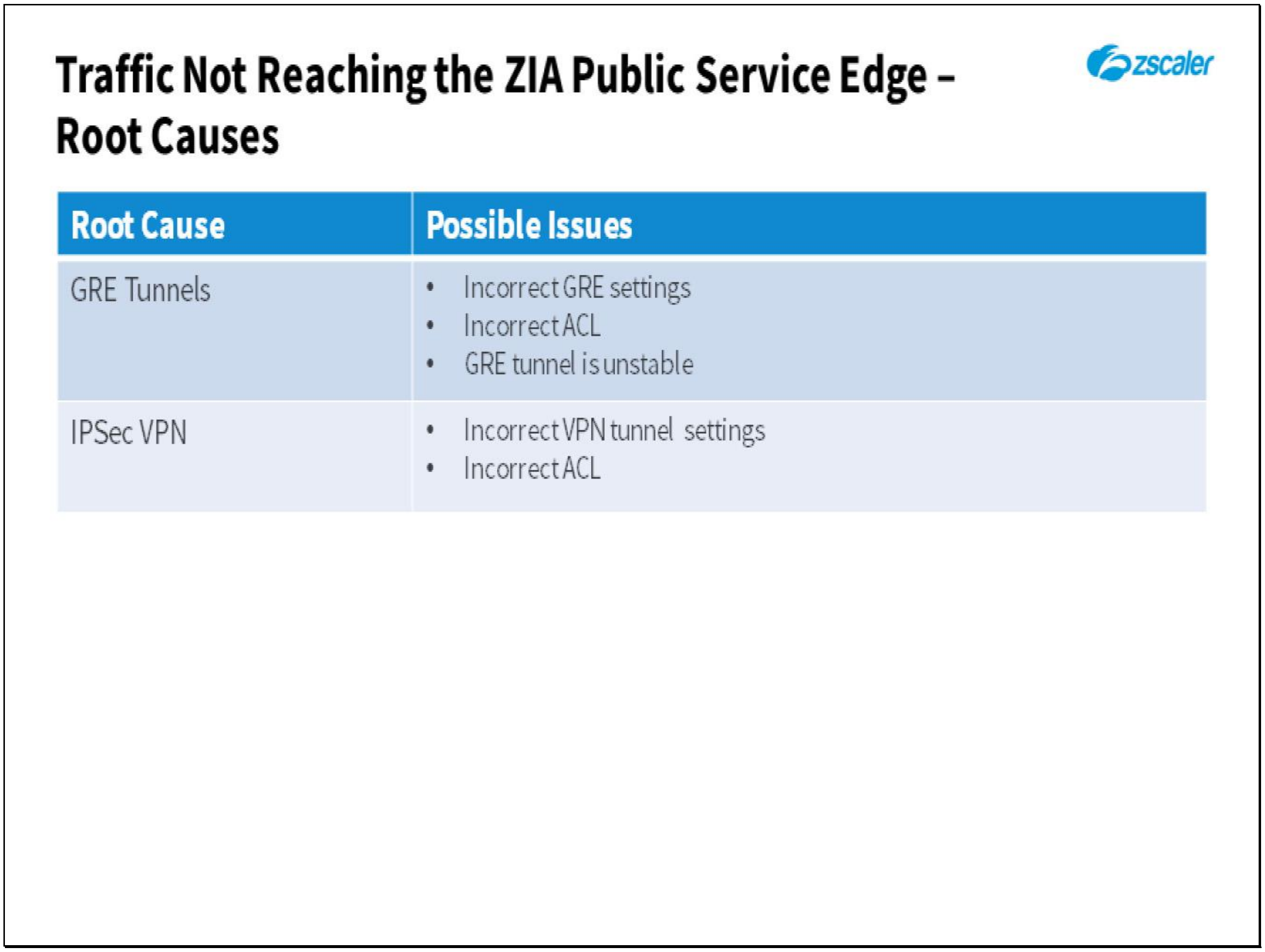
©2007-2020 Zscaler Inc. All rights reserved.

Slide notes

An obvious symptom for your traffic not reaching a ZIA Public Service Edge is that the Zscaler proxy test page looks similar to the screenshot shown here.

Slide 15 - Traffic Not Reaching the ZIA Public Service Edge –

Root Causes



Traffic Not Reaching the ZIA Public Service Edge – Root Causes

Root Cause	Possible Issues
GRE Tunnels	• Incorrect GRE settings • Incorrect ACL • GRE tunnel is unstable
IPSec VPN	• Incorrect VPN tunnel settings • Incorrect ACL

Slide notes

As there are five main ways in which traffic can be sent from the user devices to the ZIA Public Service Edge, there are also at least five potential main root causes. The first two are related to situations where tunnels are used from your locations:

First, The GRE tunnel is not operating as expected. Malfunctions in the GRE tunnel may be attributed to three main causes:

The GRE parameters may not be correct - Verify all settings, both on the local router and on the Zscaler Admin portal.

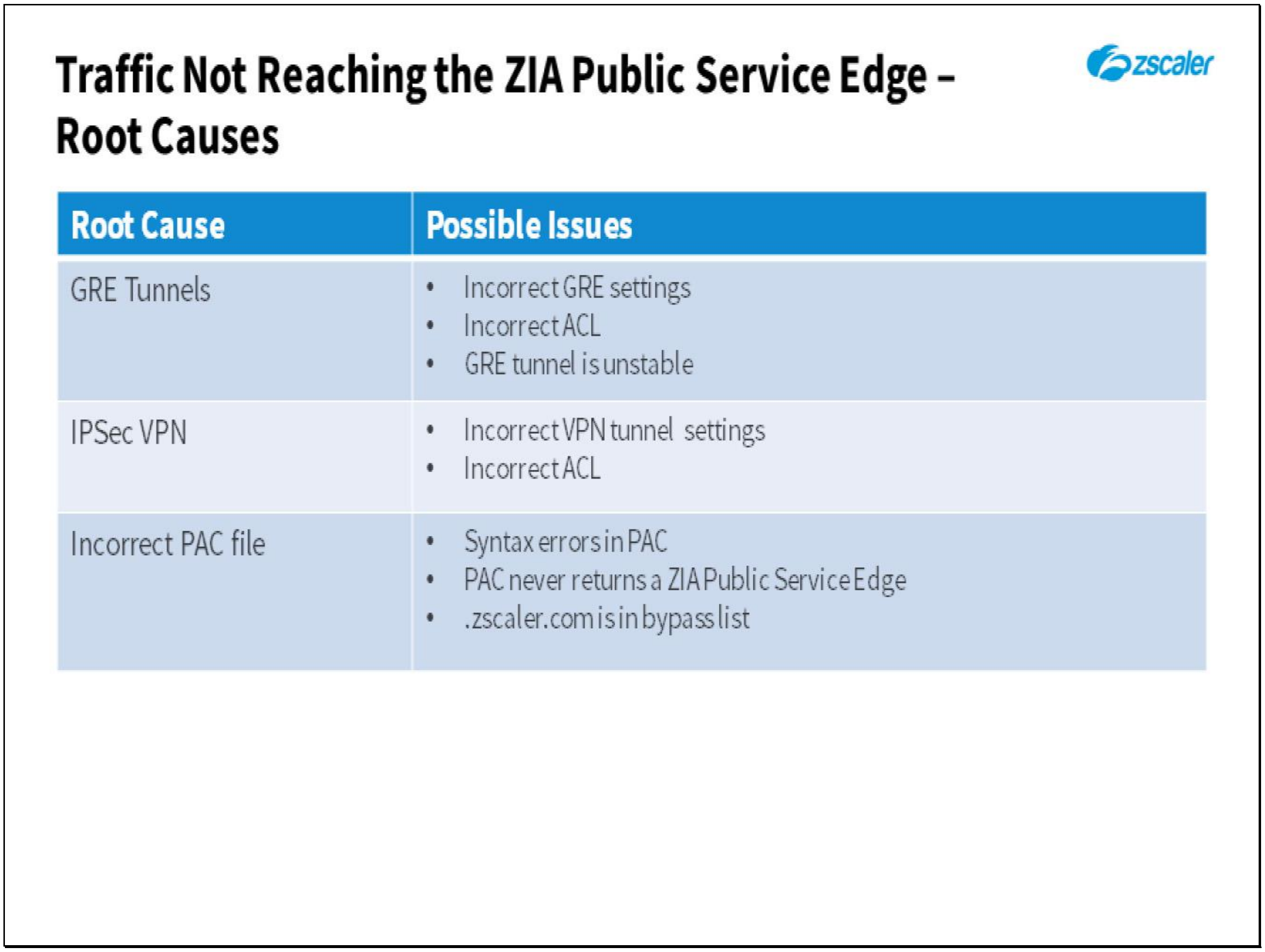
The ACLs that direct traffic through the GRE tunnel may not be operating as expected - You need to verify the configuration and ensure that the traffic to ip.zscaler.com is not bypassing the GRE tunnel.

Or the GRE tunnel may be unstable - Troubleshooting this issue requires an escalation to Zscaler support.

If IPSec tunnels are in use, they may also not be operating as expected, for similar reasons to the GRE case.

Slide 16 - Traffic Not Reaching the ZIA Public Service Edge –

Root Causes



Traffic Not Reaching the ZIA Public Service Edge – Root Causes

Root Cause	Possible Issues
GRE Tunnels	• Incorrect GRE settings • Incorrect ACL • GRE tunnel is unstable
IPSec VPN	• Incorrect VPN tunnel settings • Incorrect ACL
Incorrect PAC file	• Syntax errors in PAC • PAC never returns a ZIA Public Service Edge • .zscaler.com is in bypass list

Slide notes

Next, the PAC file may be configured incorrectly.

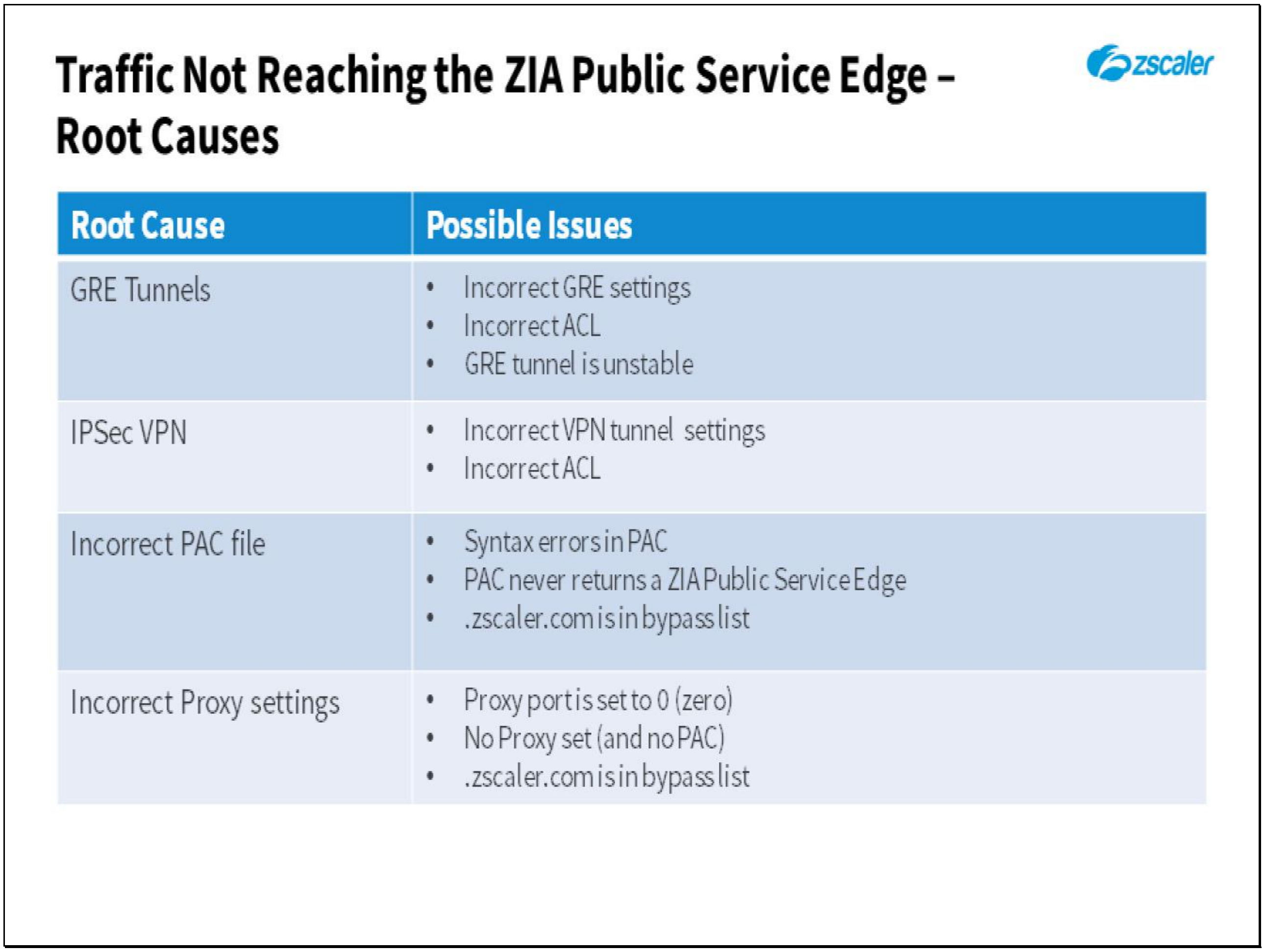
There may be a syntax error in the PAC file - You can use the Zscaler Admin portal to verify the PAC file syntax.

The test URL ip.zscaler.com may for some reason be in an exception list.

Or the PAC file may have some statements that cause all traffic to bypass the proxy, thus matching the RETURN ‘DIRECT’ clause in the script.

Slide 17 - Traffic Not Reaching the ZIA Public Service Edge –

Root Causes



Traffic Not Reaching the ZIA Public Service Edge – Root Causes

Root Cause	Possible Issues
GRE Tunnels	• Incorrect GRE settings • Incorrect ACL • GRE tunnel is unstable
IPSec VPN	• Incorrect VPN tunnel settings • Incorrect ACL
Incorrect PAC file	• Syntax errors in PAC • PAC never returns a ZIA Public Service Edge • .zscaler.com is in bypass list
Incorrect Proxy settings	• Proxy port is set to 0 (zero) • No Proxy set (and no PAC) • .zscaler.com is in bypass list

Slide notes

The proxy settings may be incorrect in the Browser.

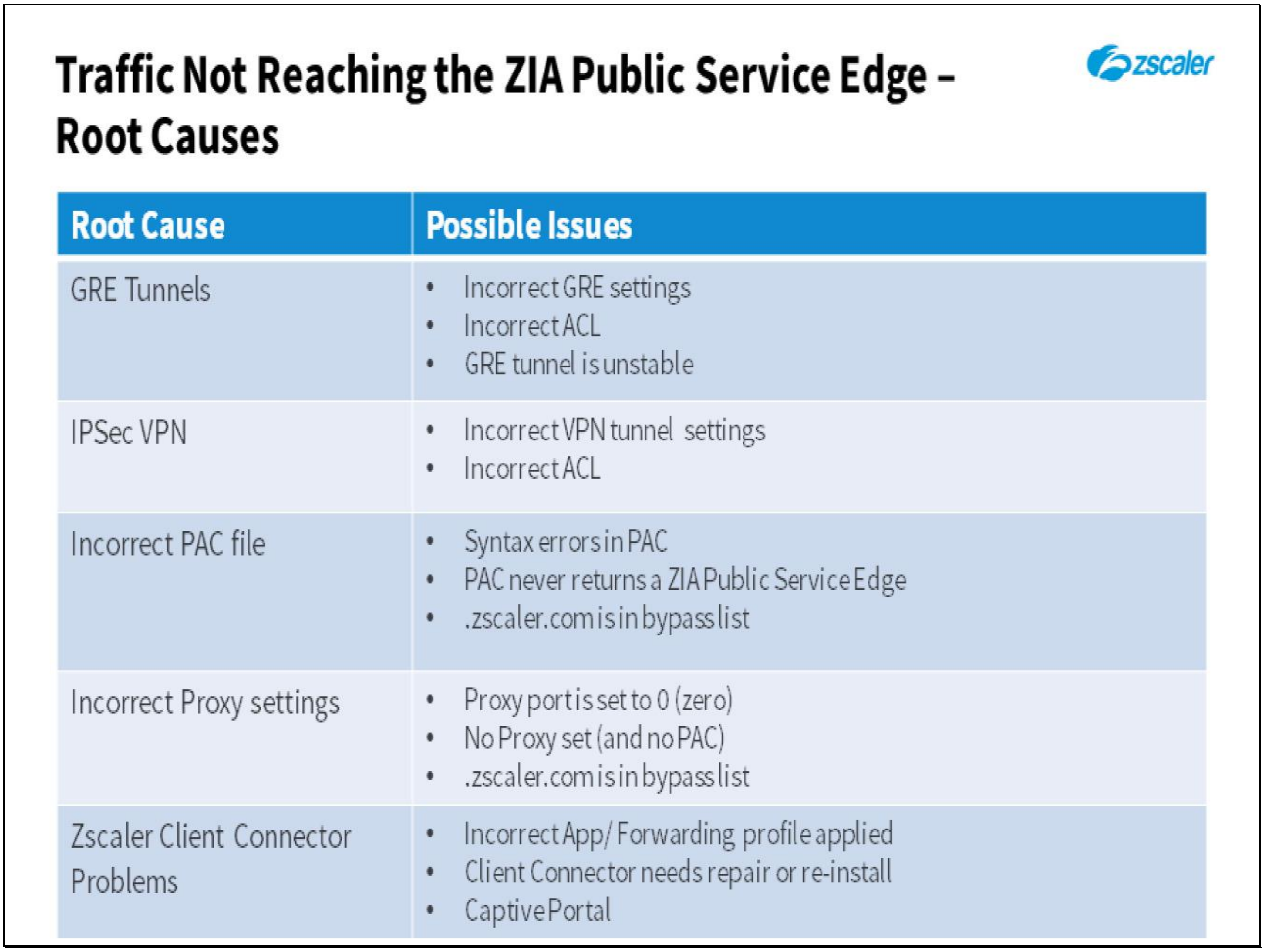
The proxy port on the proxy URL may be incorrect.

There may be no PAC file configuration at all, so no proxy is defined on the system.

Or once again, the Zscaler domain may for some reason be in an exception list.

Slide 18 - Traffic Not Reaching the ZIA Public Service Edge –

Root Causes



Traffic Not Reaching the ZIA Public Service Edge – Root Causes

Root Cause	Possible Issues
GRE Tunnels	• Incorrect GRE settings • Incorrect ACL • GRE tunnel is unstable
IPSec VPN	• Incorrect VPN tunnel settings • Incorrect ACL
Incorrect PAC file	• Syntax errors in PAC • PAC never returns a ZIA Public Service Edge • .zscaler.com is in bypass list
Incorrect Proxy settings	• Proxy port is set to 0 (zero) • No Proxy set (and no PAC) • .zscaler.com is in bypass list
Zscaler Client Connector Problems	• Incorrect App/ Forwarding profile applied • Client Connector needs repair or re-install • Captive Portal

Slide notes

Finally, if the Zscaler Client Connector is being used, there can be a number of issues that cause connectivity to fail:

- The incorrect Forwarding or App profile is being applied to the user.
- The Client Connector may need updating, repair, or complete re-installation.
- The end user may be on a network with a captive portal, and has not yet logged in through the portal.

Slide 19 - Unauthenticated User / Unable to Authenticate

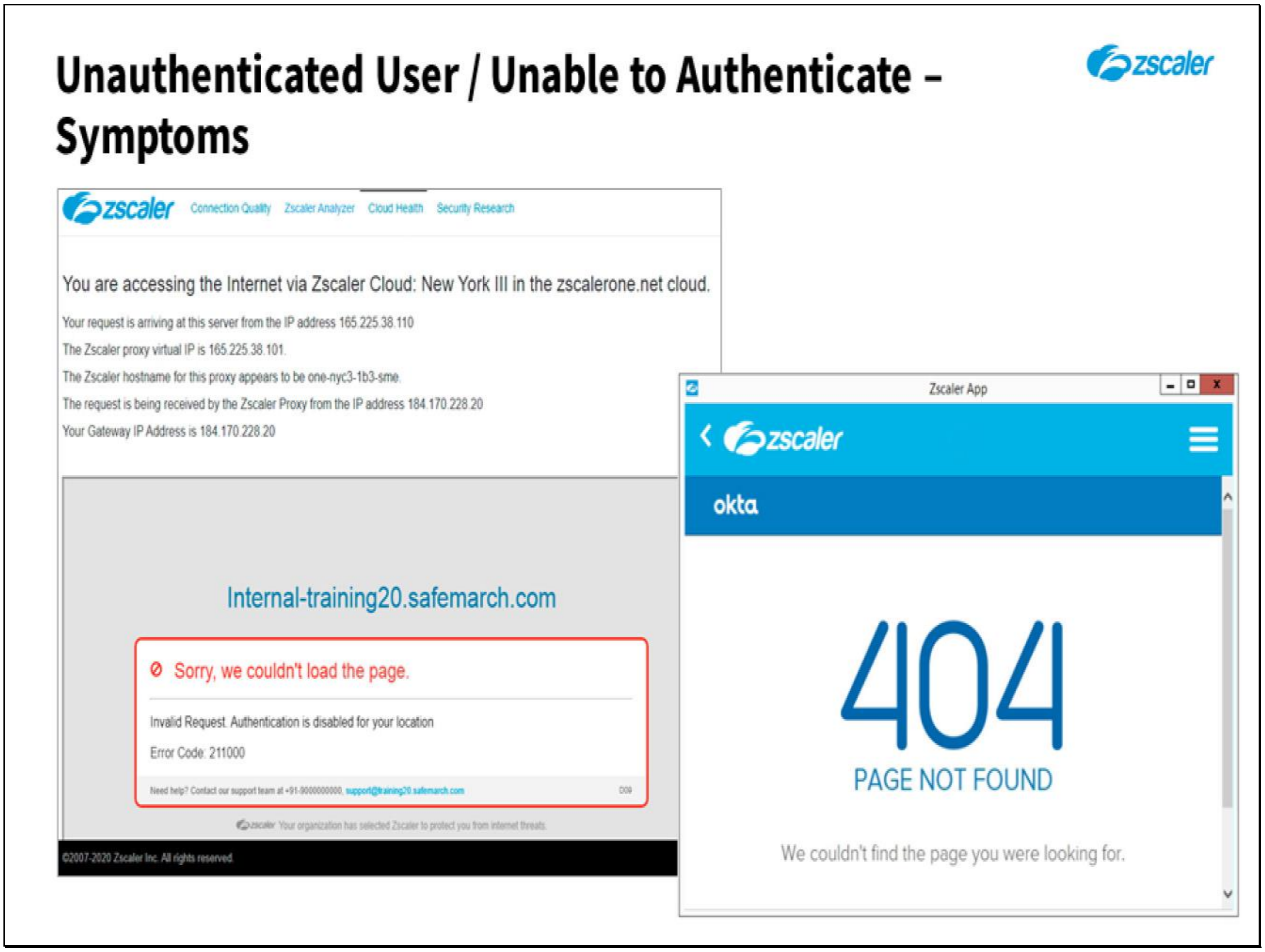
Unauthenticated User / Unable to Authenticate

Slide notes

In the final section, we will look at symptoms and possible causes for when a user is unable to authenticate.

Slide 20 - Unauthenticated User / Unable to Authenticate –

Symptoms



Unauthenticated User / Unable to Authenticate – Symptoms

You are accessing the Internet via Zscaler Cloud: New York III in the zscalerone.net cloud.

Your request is arriving at this server from the IP address 165.225.38.110

The Zscaler proxy virtual IP is 165.225.38.101.

The Zscaler hostname for this proxy appears to be one-nyc3-1b3-sme.

The request is being received by the Zscaler Proxy from the IP address 184.170.228.20

Your Gateway IP Address is 184.170.228.20

Internal-training20.safemarch.com

Sorry, we couldn't load the page.

Invalid Request. Authentication is disabled for your location

Error Code: 211000

Need help? Contact our support team at +91-9000000000, support@training20.safemarch.com D09

Your organization has selected Zscaler to protect you from internet threats.

©2007-2020 Zscaler Inc. All rights reserved.

404

PAGE NOT FOUND

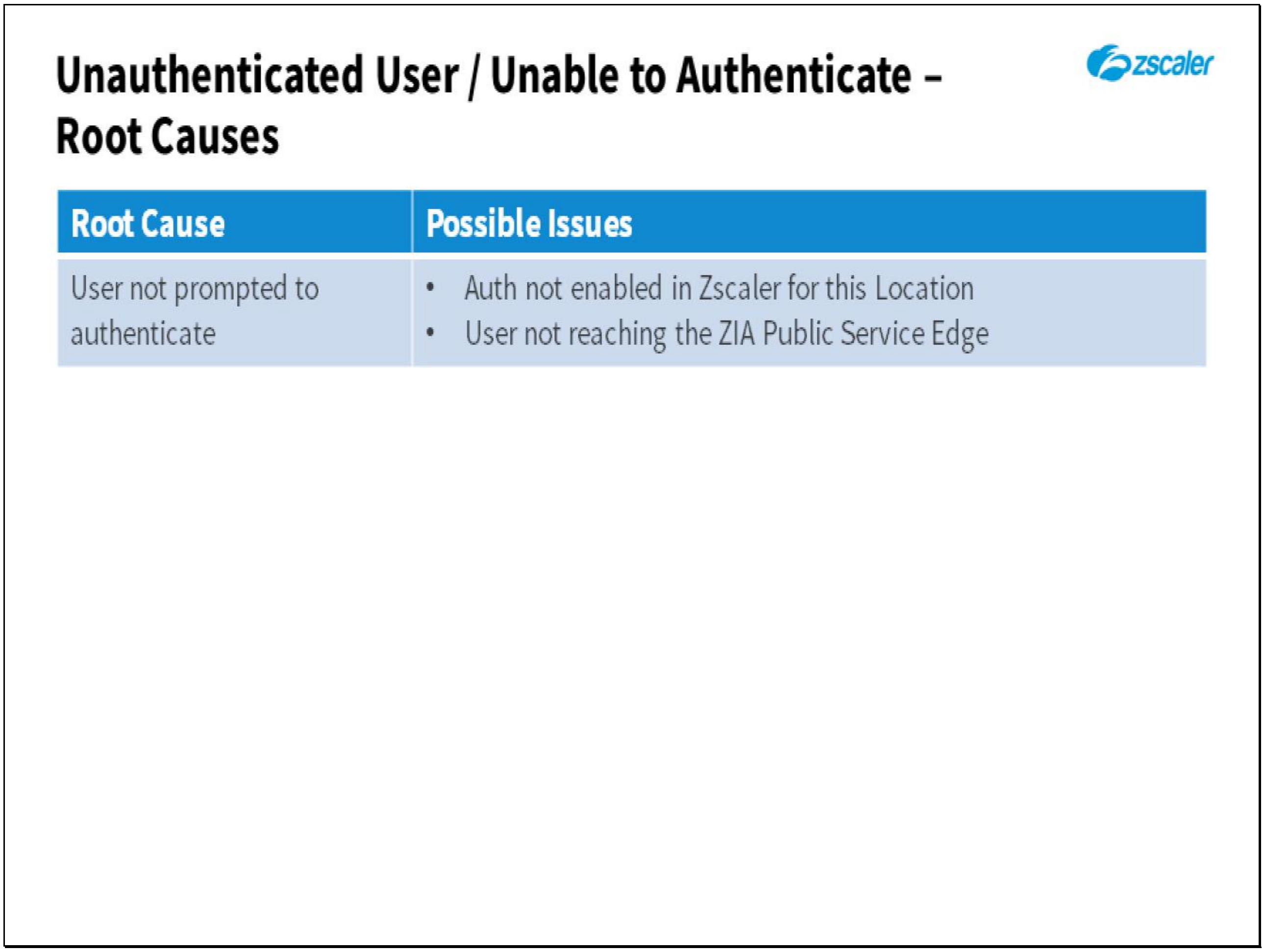
We couldn't find the page you were looking for.

Slide notes

Some symptoms for authentication issues are shown here. For example, If a user sees a ‘404’ page while authenticating, this indicates that the IdP login page cannot be reached.

Slide 21 - Unauthenticated User / Unable to Authenticate –

Root Causes



Unauthenticated User / Unable to Authenticate – Root Causes

Root Cause	Possible Issues
User not prompted to authenticate	• Auth not enabled in Zscaler for this Location • User not reaching the ZIA Public Service Edge

Slide notes

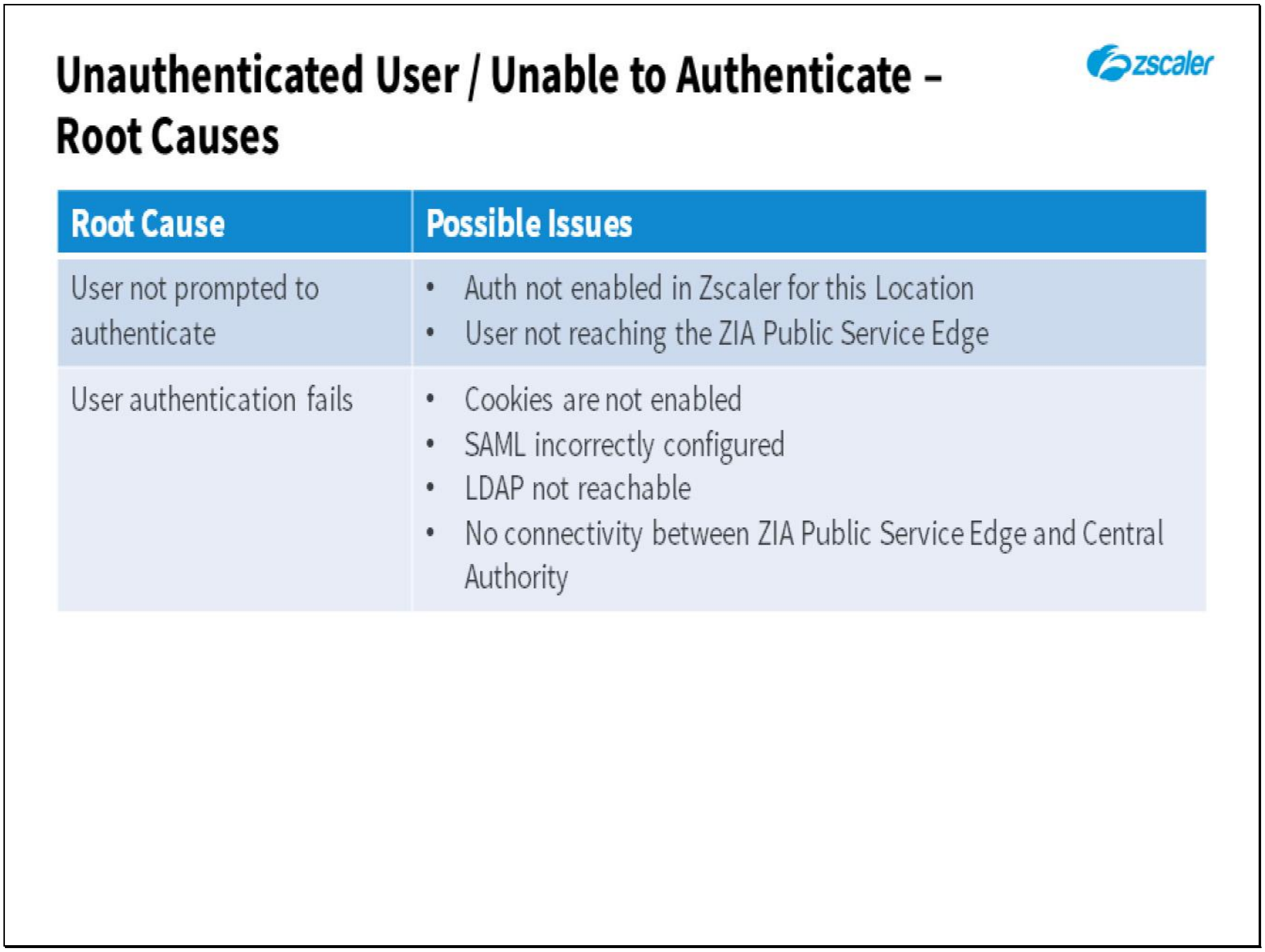
Let’s take a look at the possible causes for a user failing to authenticate. This may presume that the user was actually prompted for authentication. But let’s also look at situations where the user was not prompted to login, there can be two primary reasons for this:

First, the specified location does not have authentication enabled. Besides the ability to granularly control authentication by location, Zscaler maintains a list of authentication exemption sites, which is not controlled by the users. If you are accessing the Internet from a location with authentication off, or if you are accessing a site in the exemption list, you will obviously not be prompted to authenticate.

The other case is where user’s traffic does not reach the ZIA Public Service Edge and therefore the user cannot be authenticated. This issue should follow the troubleshooting process for ‘No Connectivity’.

Slide 22 - Unauthenticated User / Unable to Authenticate –

Root Causes



Unauthenticated User / Unable to Authenticate – Root Causes

Root Cause	Possible Issues
User not prompted to authenticate	• Auth not enabled in Zscaler for this Location • User not reaching the ZIA Public Service Edge
User authentication fails	• Cookies are not enabled • SAML incorrectly configured • LDAP not reachable • No connectivity between ZIA Public Service Edge and Central Authority

Slide notes

Now, let’s discuss the case where authentication actually fails, a user is prompted for their credentials, however, authentication is unsuccessful.

This is most likely due to cookies. If the User Agent has cookies disabled, you will not be able to complete the authentication process. Please note that when you are in ‘private’ or ‘incognito’ mode, your Browser accepts cookies, but it does not store the cookies once you close the anonymous session.

Other less likely causes may be:

- SAML is not configured correctly - Configuring SAML has several steps and complexities, you need to properly test your SAML configuration before rolling it out to all users.

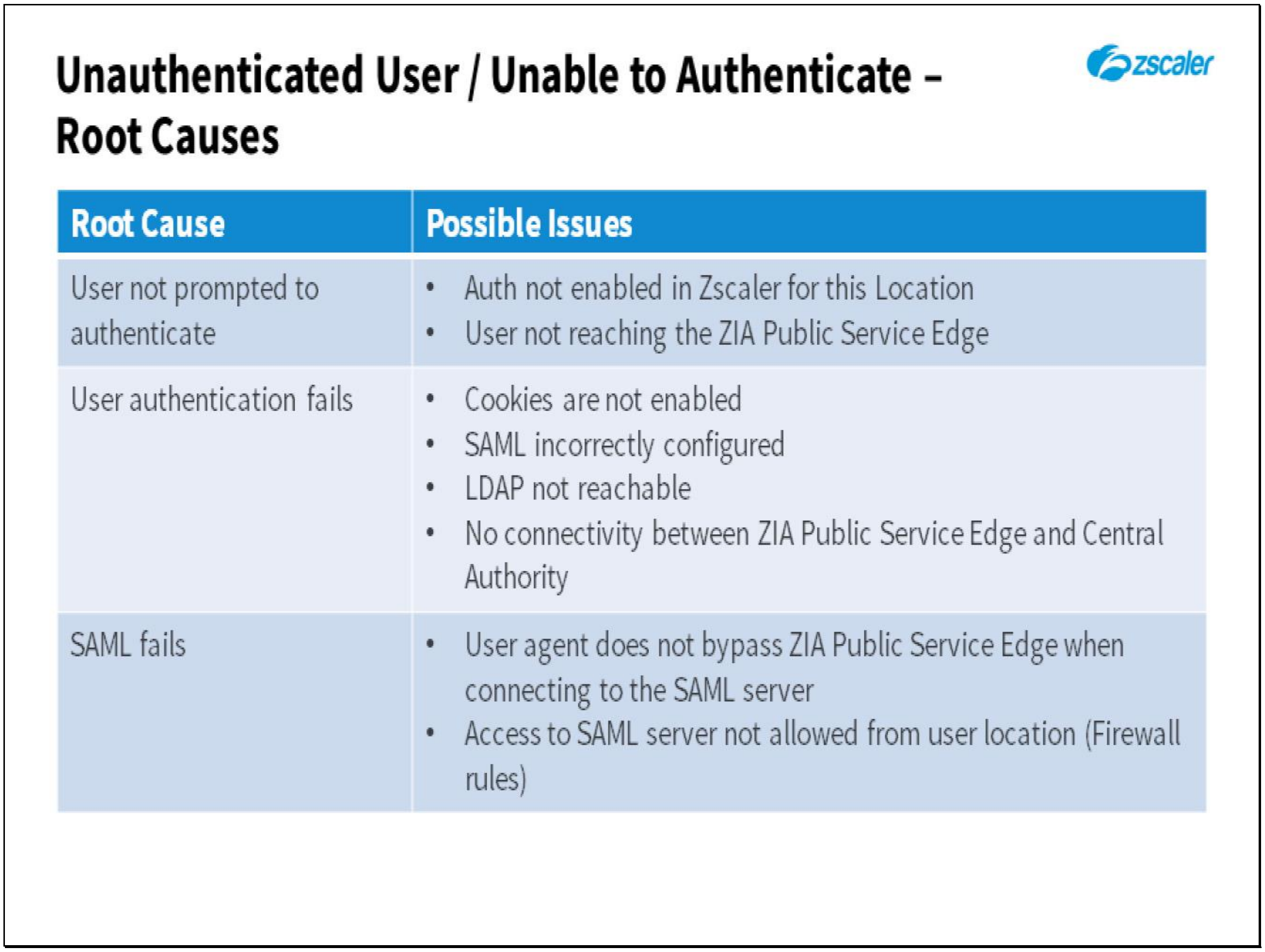
- The LDAP / AD server cannot be reached - Firewall changes may temporarily or permanently impede the Zscaler-to-LDAP connection.

- The ZIA Public Service Edge has temporarily lost connectivity to the Central Authority, and either the user has never connected and authenticated to that ZIA Public Service Edge or the password was changed since the last time the user was authenticated on that ZIA Public Service Edge.

- Finally, the user may be simply typing an incorrect (or non-existent) username, the password may be incorrect or have expired, or the account may be disabled.

Slide 23 - Unauthenticated User / Unable to Authenticate –

Root Causes



Unauthenticated User / Unable to Authenticate – Root Causes

Root Cause	Possible Issues
User not prompted to authenticate	• Auth not enabled in Zscaler for this Location • User not reaching the ZIA Public Service Edge
User authentication fails	• Cookies are not enabled • SAML incorrectly configured • LDAP not reachable • No connectivity between ZIA Public Service Edge and Central Authority
SAML fails	• User agent does not bypass ZIA Public Service Edge when connecting to the SAML server • Access to SAML server not allowed from user location (Firewall rules)

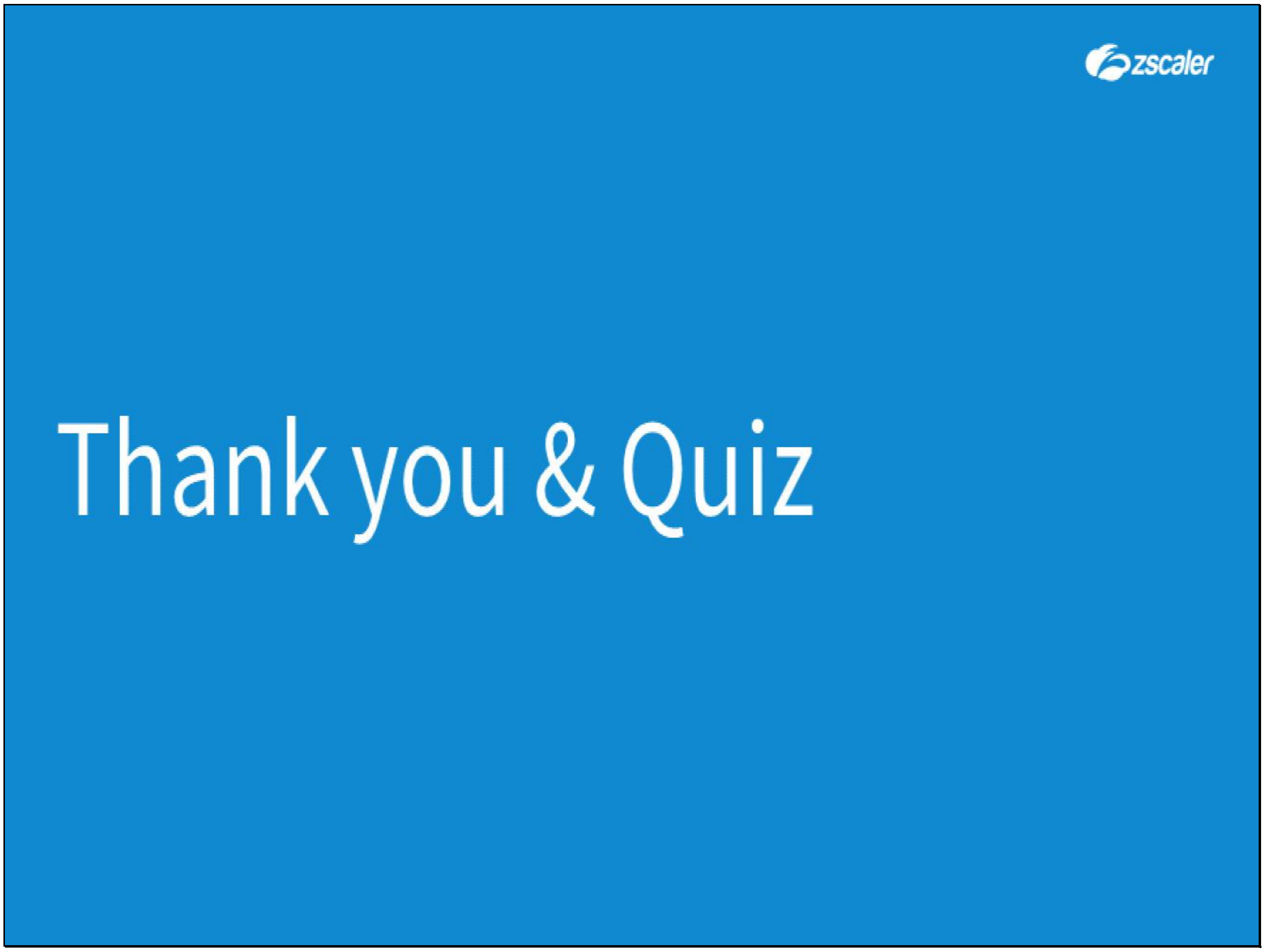
Slide notes

Finally, for a SAML configuration, you need to verify that:

The user agent bypasses the ZIA Public Service Edge when connecting to the SAML server - Ensure that the PAC file is configured accordingly.

Whether access to the SAML server is being denied by the firewall or some other security systems.

Slide 24 - Thank you & Quiz



zscaler

Thank you & Quiz

Slide notes

Thank you for following this training module on isolating Zscaler Internet Access problems. We hope this module has been useful to you and thank you for your time.

What follows is a short 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.