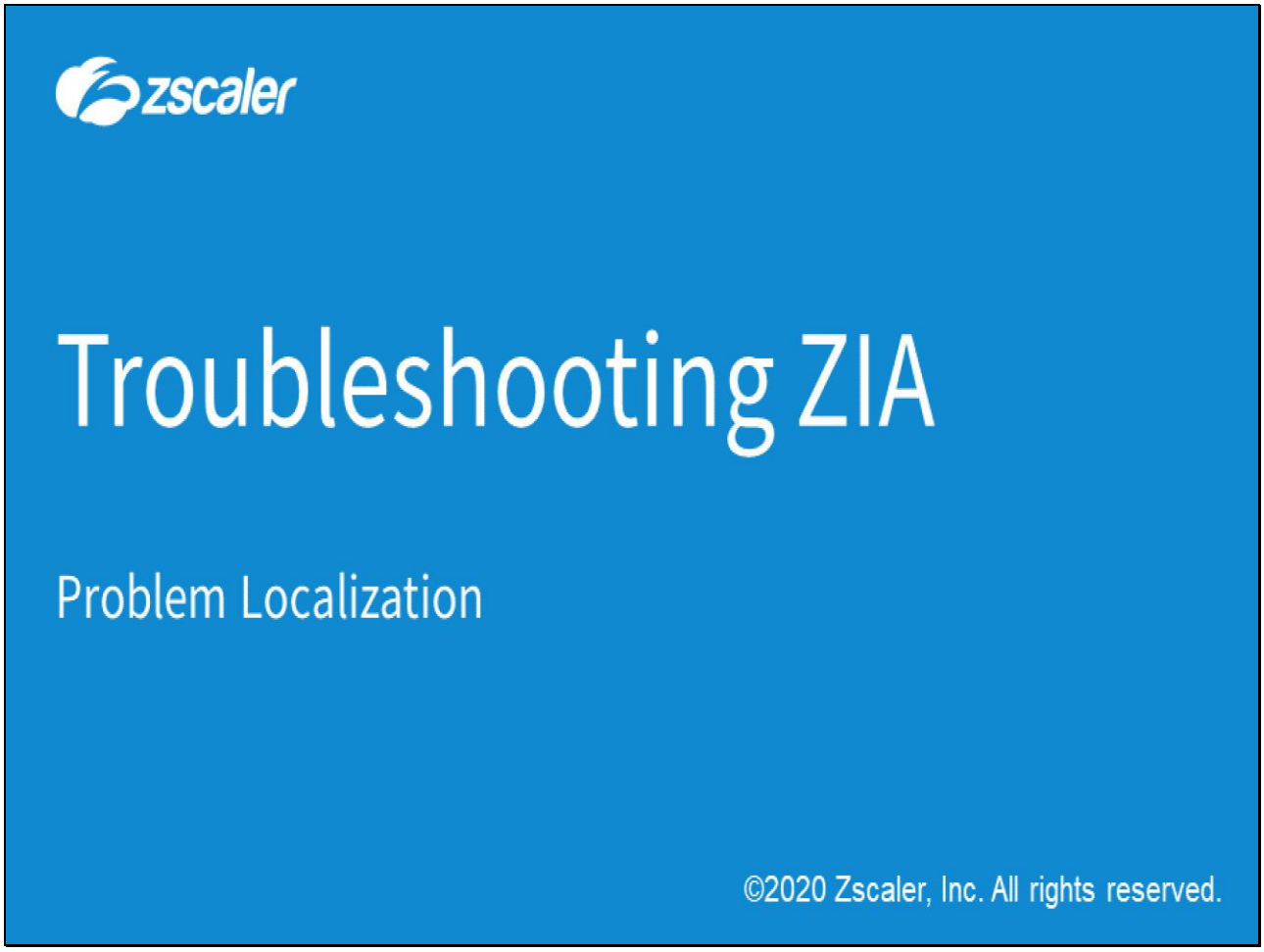
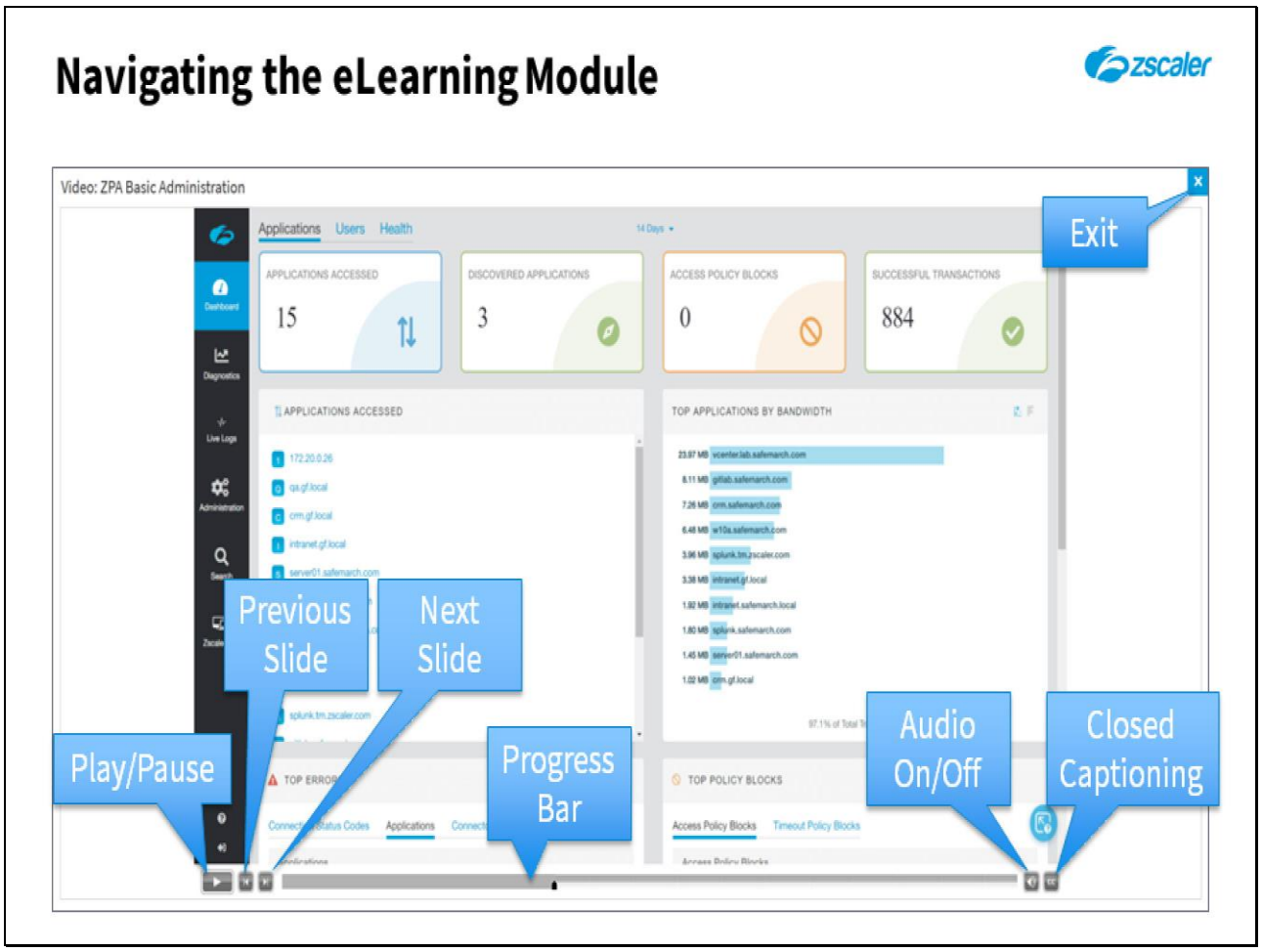
**Slide 1 - Troubleshooting ZIA**




**Slide notes**

Welcome to this training module on localizing problems when troubleshooting end user connectivity issues with Zscaler Internet Access.

**Slide 2 - Navigating the eLearning Module**

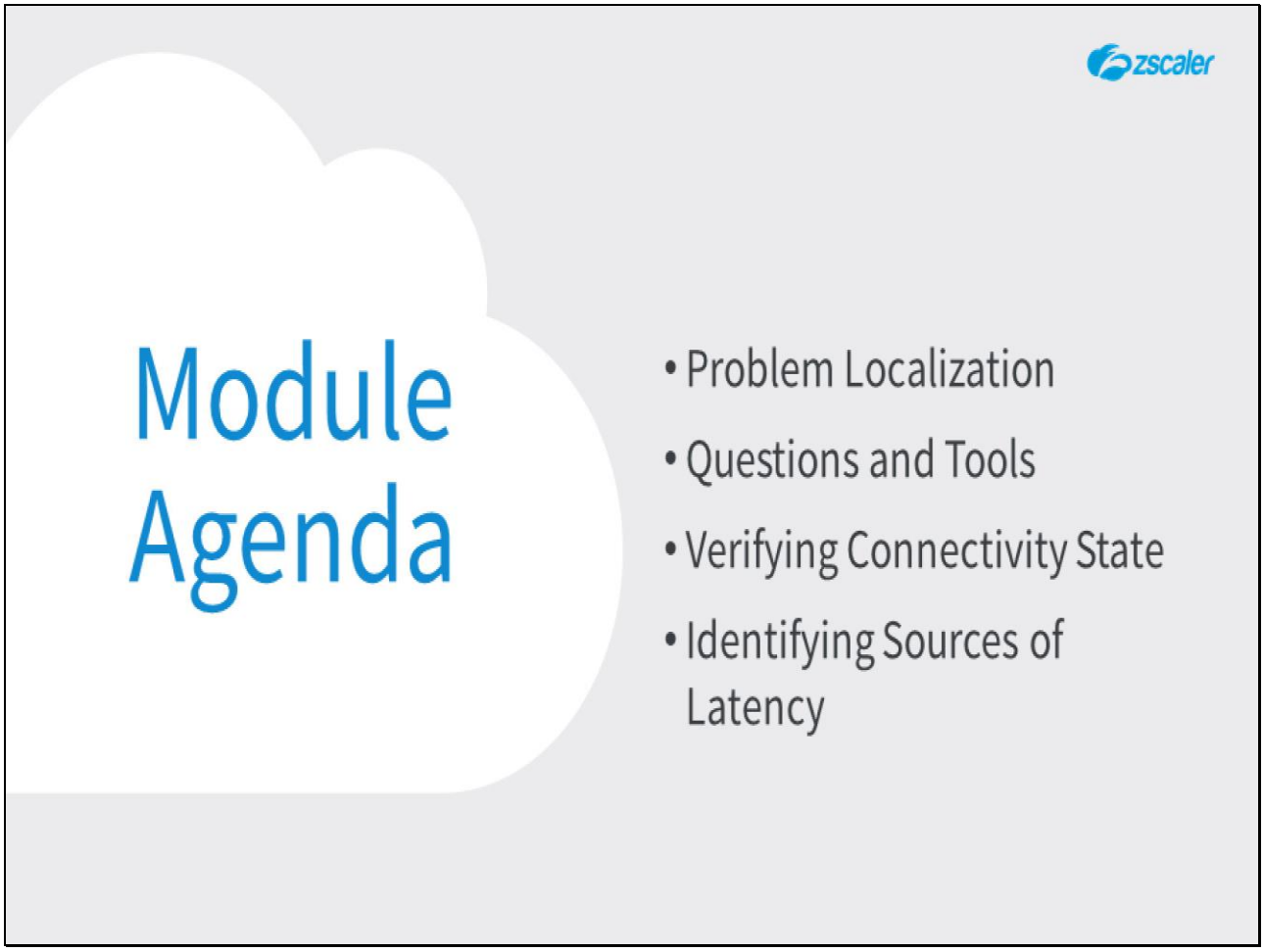



**Slide notes**

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**




**Slide notes**

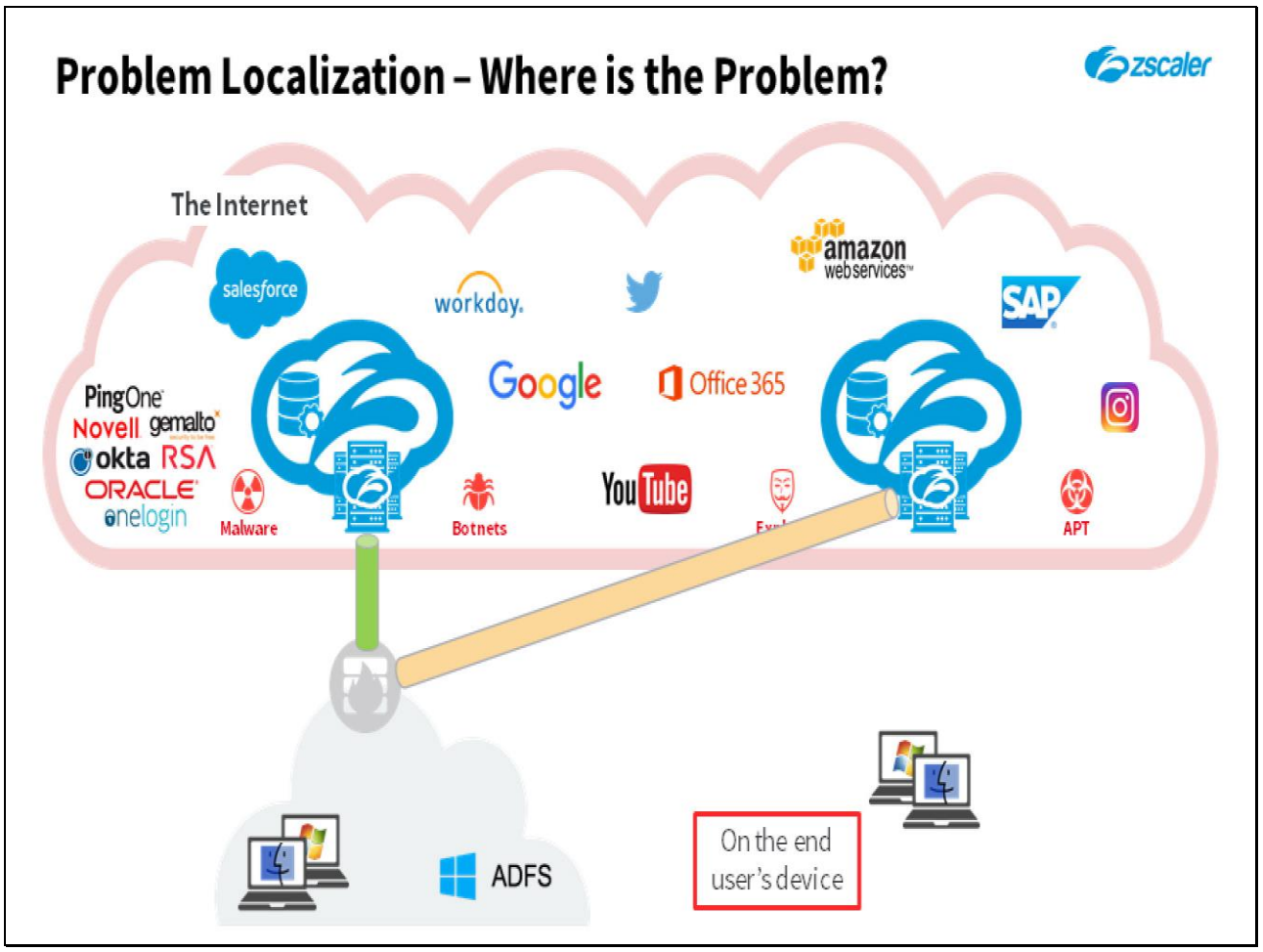
In this module, we will cover: The process of localizing a problem to identify the failure domain; the questions and tools that can help to narrow down the precise location of a problem; the Zscaler Proxy Test tool for verifying end user connection status; and the identification of the sources of latency on user connections.

**Slide 4 - Problem Localization**


**Slide notes**

In the first section, we will look at potential problem locations, and the process of narrowing down **exactly** where a problem is occurring.

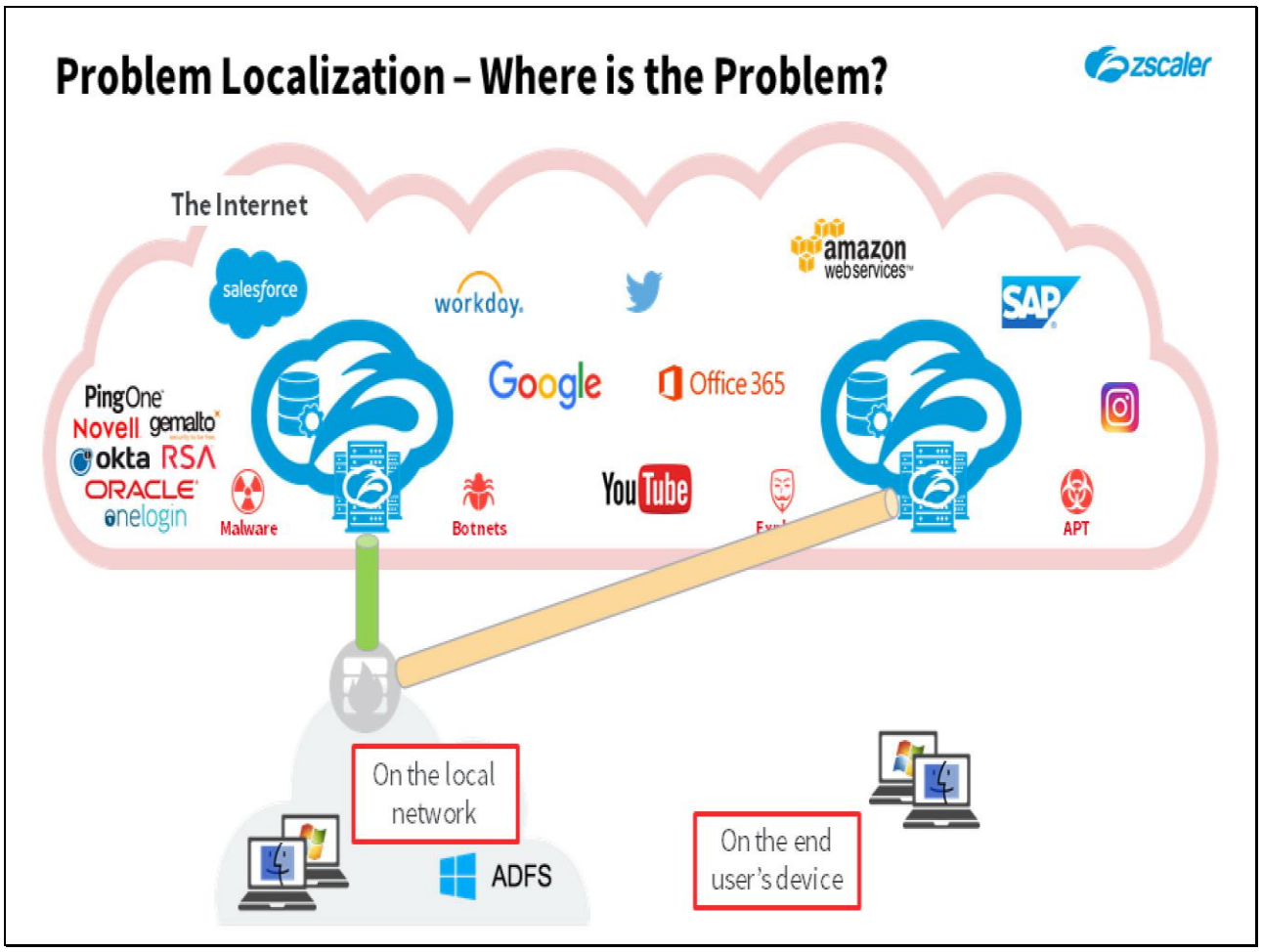
**Slide 5 - Problem Localization – Where is the Problem?**




**Slide notes**

With the Zscaler Internet Access solution, there are many places where a problem can potentially arise. There may be fundamental problems on the end user's client device, possibly operating system, or software agent- or client-related.

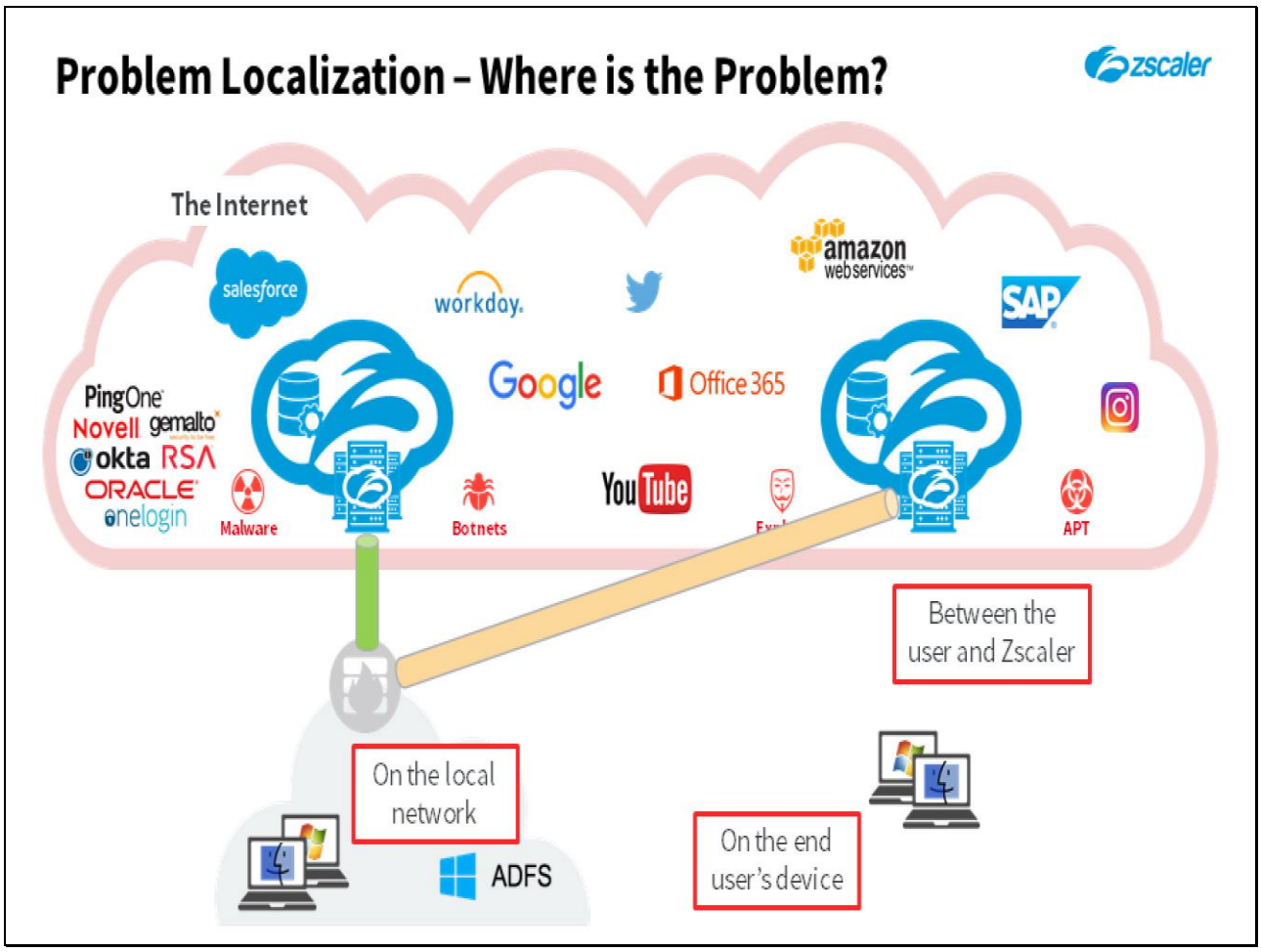
**Slide 6 - Problem Localization – Where is the Problem?**




**Slide notes**

The end user may have basic connectivity problems on the local network.

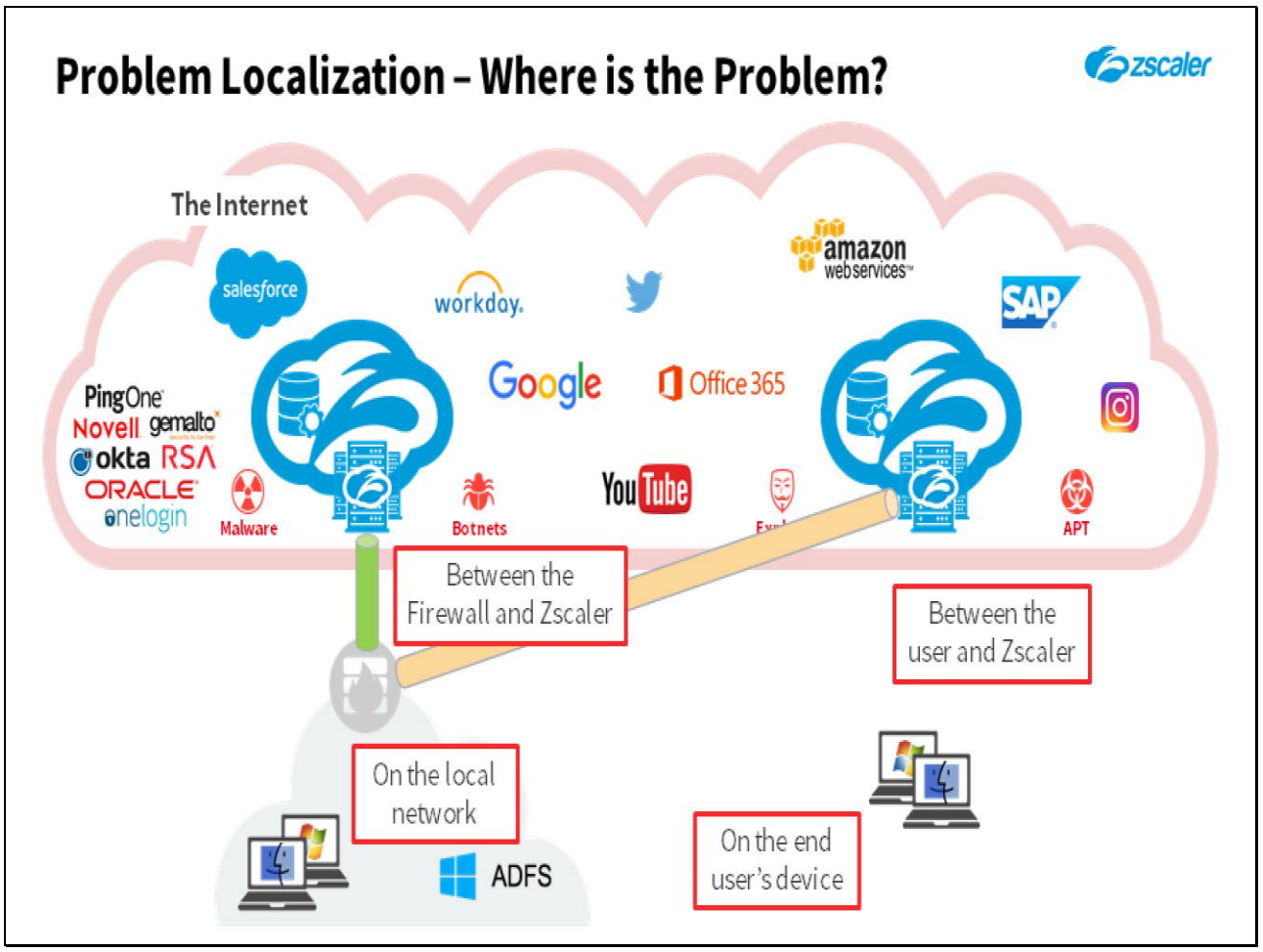
**Slide 7 - Problem Localization – Where is the Problem?**




**Slide notes**

For end users that connect directly to Zscaler using a PAC file configuration, or the Zscaler Client Connector, problems can occur between the end user's device and Zscaler.

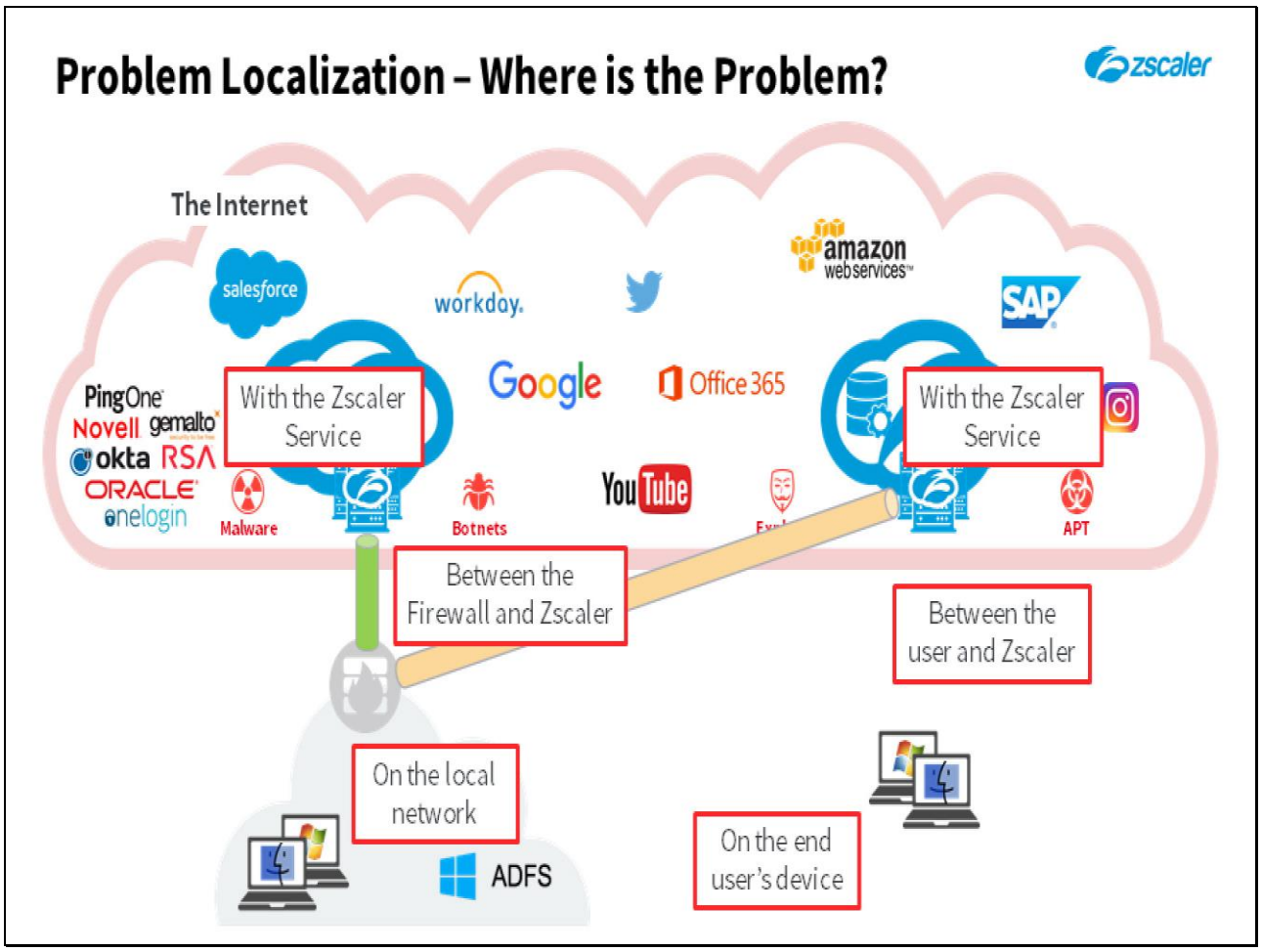
**Slide 8 - Problem Localization – Where is the Problem?**




**Slide notes**

For users who connect from a corporate location, problems can occur between the Customer Premise Equipment (CPE) and Zscaler, for example because of a firewall or router misconfiguration.

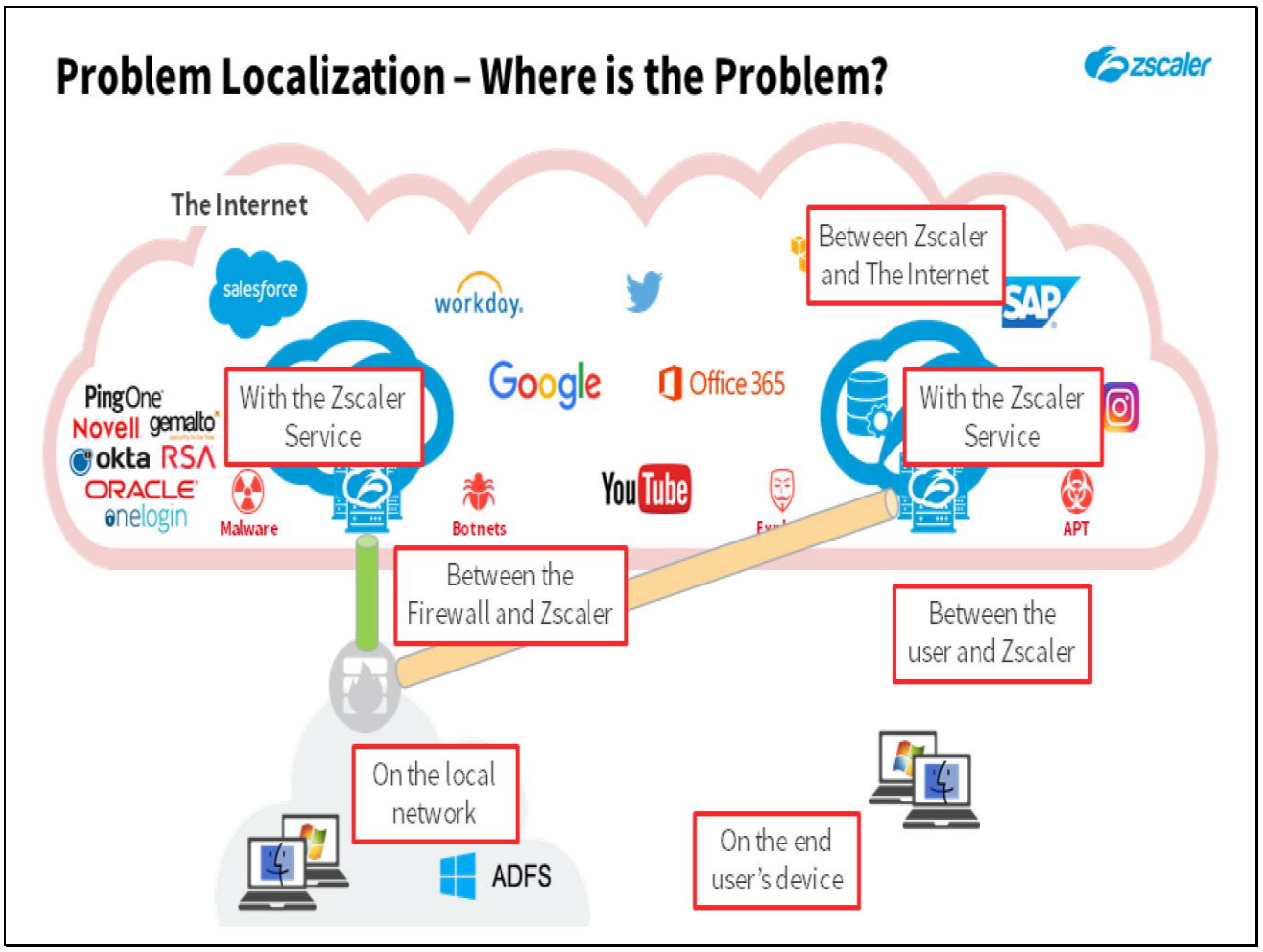
**Slide 9 - Problem Localization – Where is the Problem?**




**Slide notes**

There may be problems with the Zscaler service itself, either infrastructure issues, or misconfigurations of settings or policies.

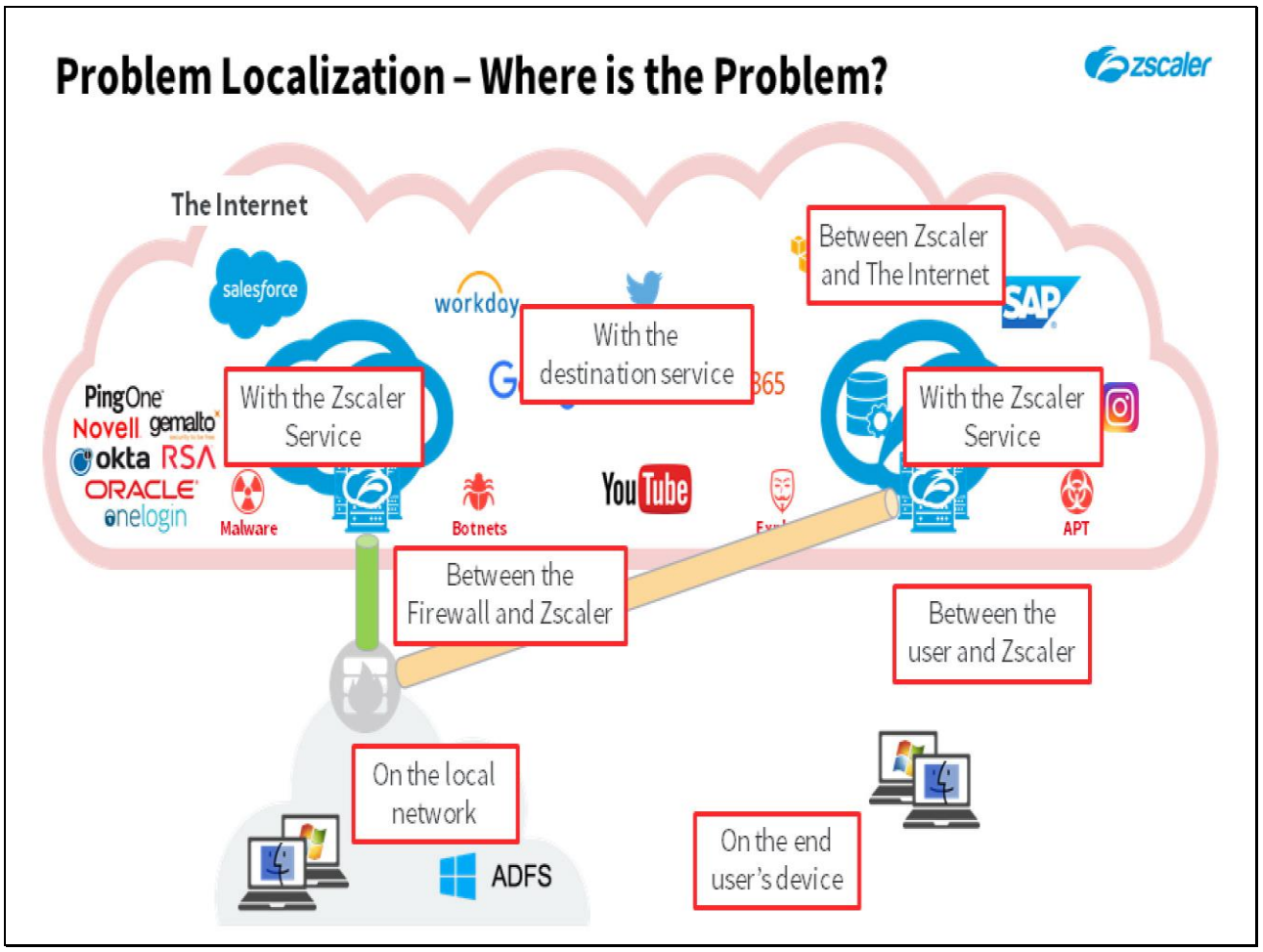
**Slide 10 - Problem Localization – Where is the Problem?**




**Slide notes**

As Zscaler acts as a proxy between the end users and the Internet, there may be problems between Zscaler and destinations on the Internet.

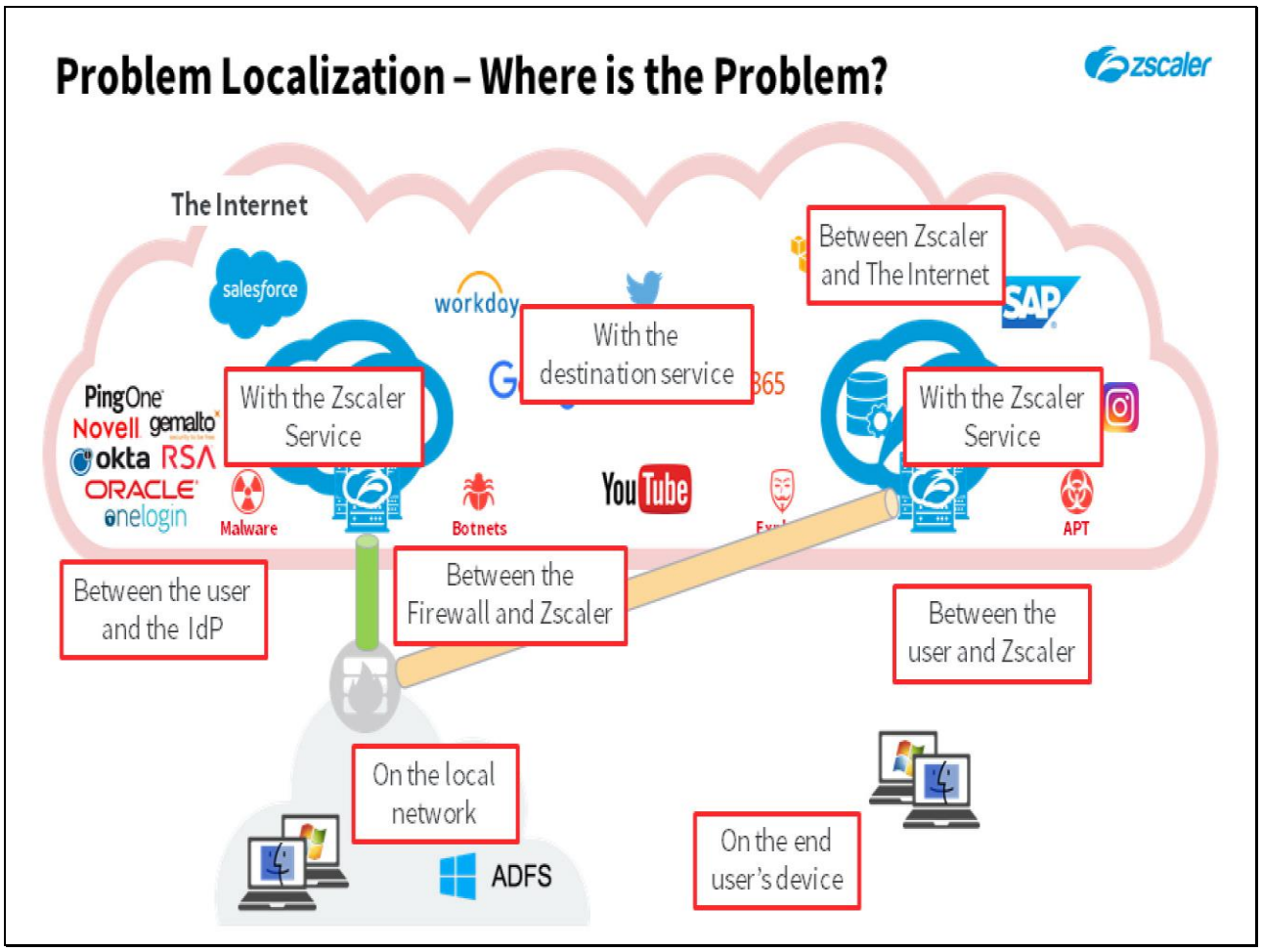
**Slide 11 - Problem Localization – Where is the Problem?**




**Slide notes**

The destination service may be experiencing an outage, or may be misconfigured for the users in question.

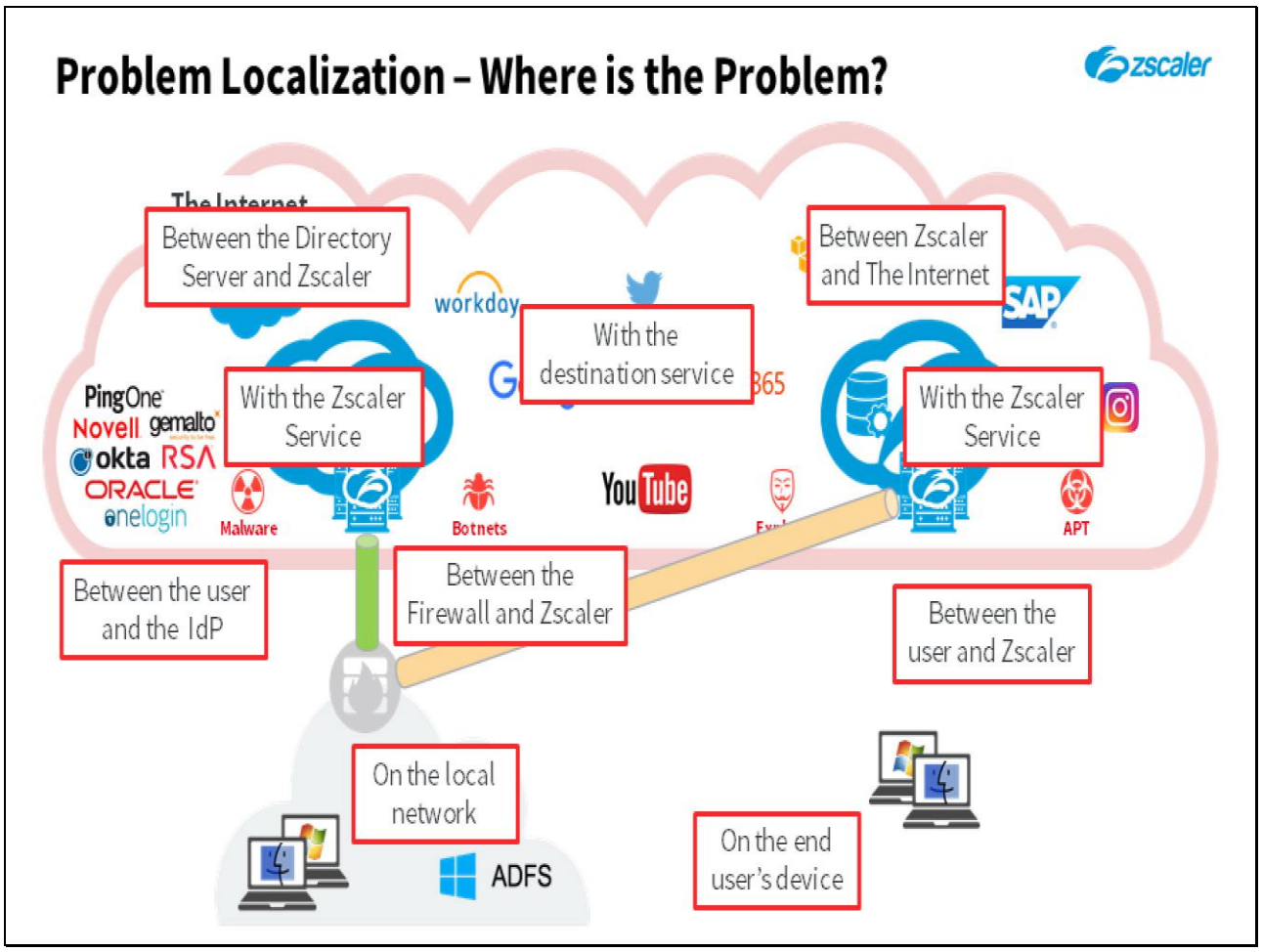
**Slide 12 - Problem Localization – Where is the Problem?**




**Slide notes**

If authentication is enabled for access to Zscaler, additional potential problem areas are introduced, such as the connection between the end user and the authentication service or IdP.

**Slide 13 - Problem Localization – Where is the Problem?**




**Slide notes**

Or there can be problems between the authentication service and Zscaler.

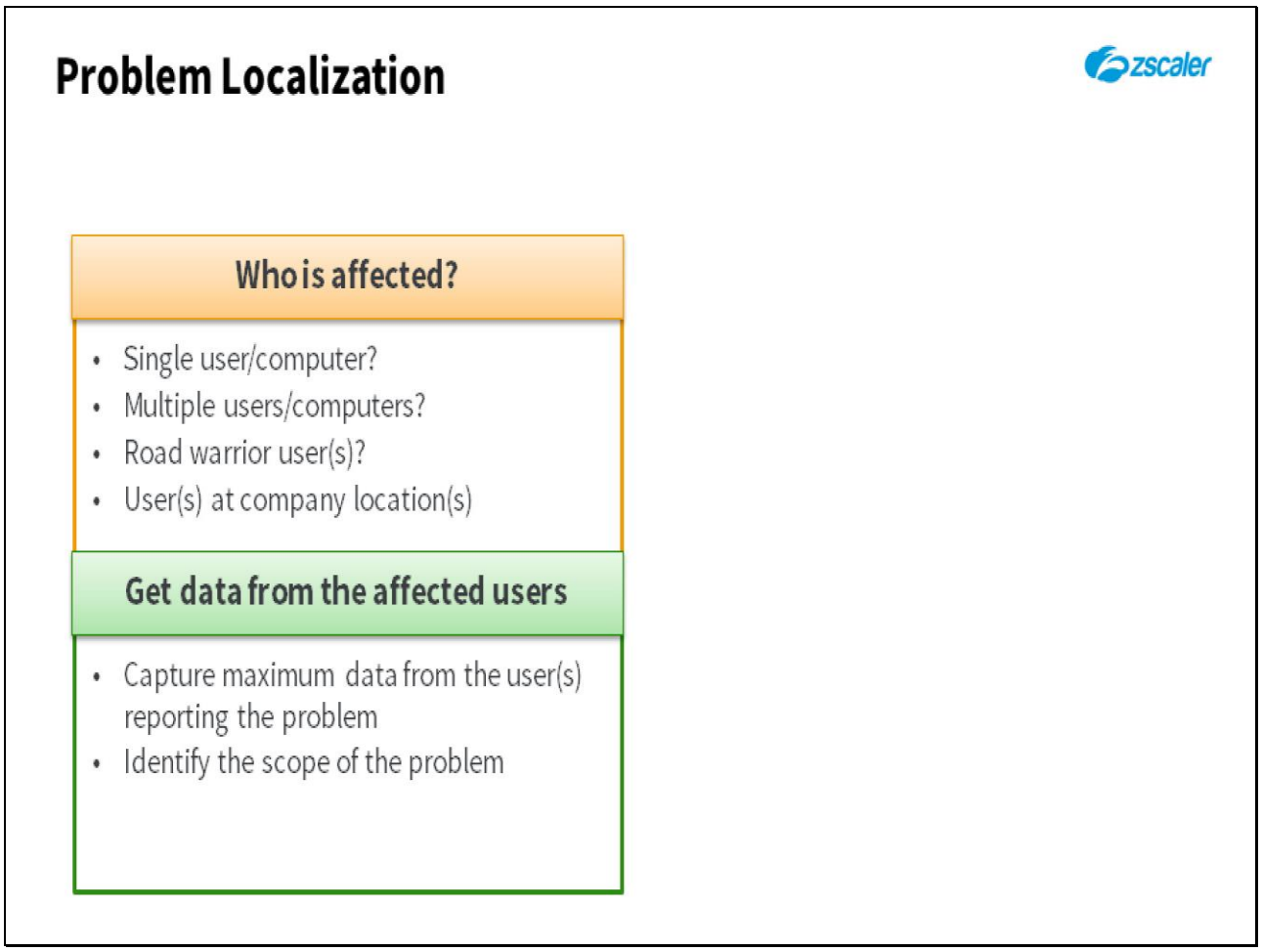
**Slide 14 - Problem Localization**


**Slide notes**

To narrow down the scope of the problem, and effectively identify the true location of the issue, you must identify precisely who is affected by it. Is it an issue for a single user, or a single client machine (or type of machine)?

Are multiple users or machines affected? Does the problem only affect road warriors? Is it only a problem for users connecting from fixed locations? …or does it affect all users regardless of connectivity?

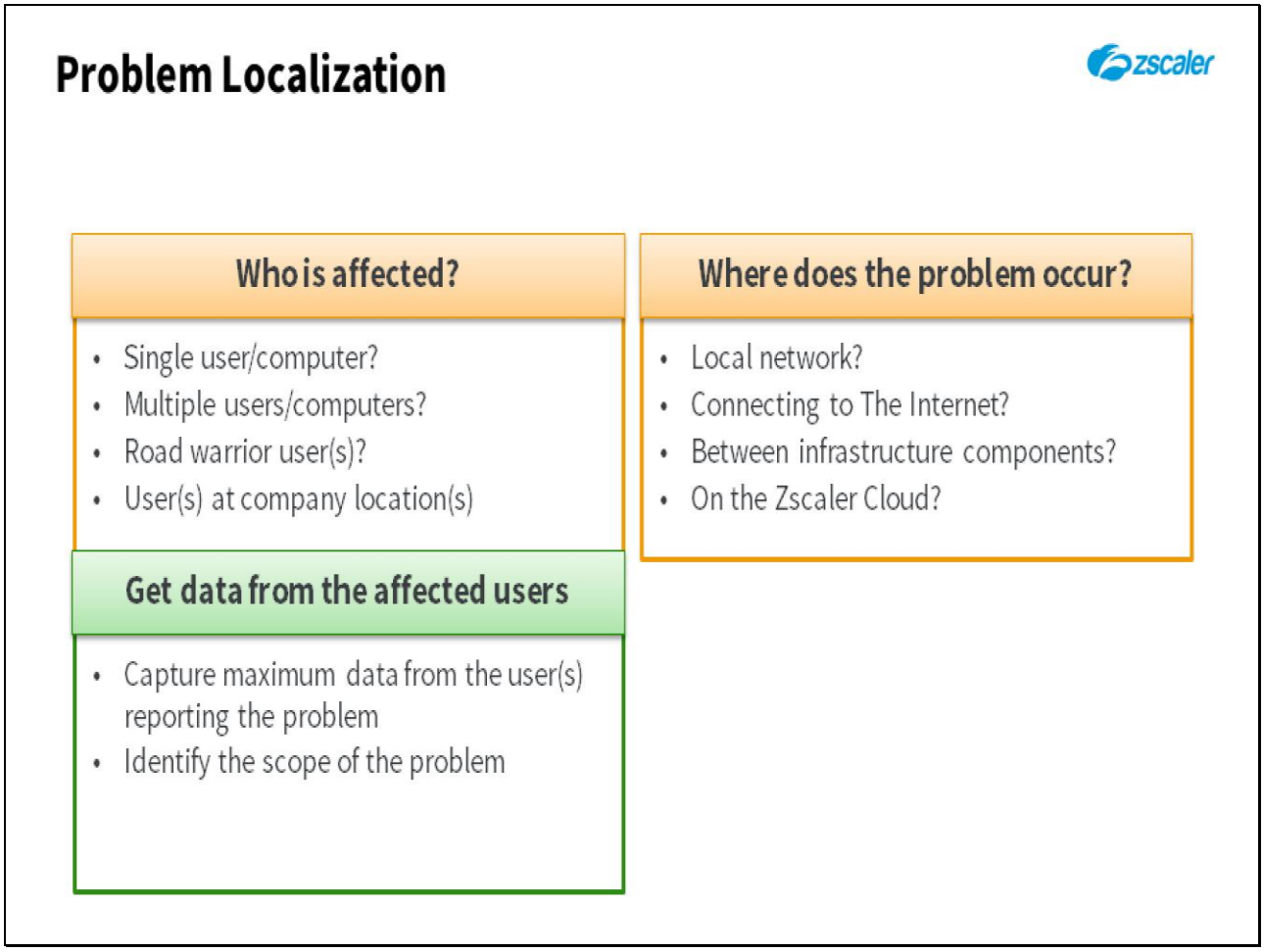
**Slide 15 - Problem Localization**




**Slide notes**

The best way to identify the scope of the issue is to capture the maximum data from the affected end users. This may require you to access their client devices remotely to see the issue with your own eyes, and to capture data directly.

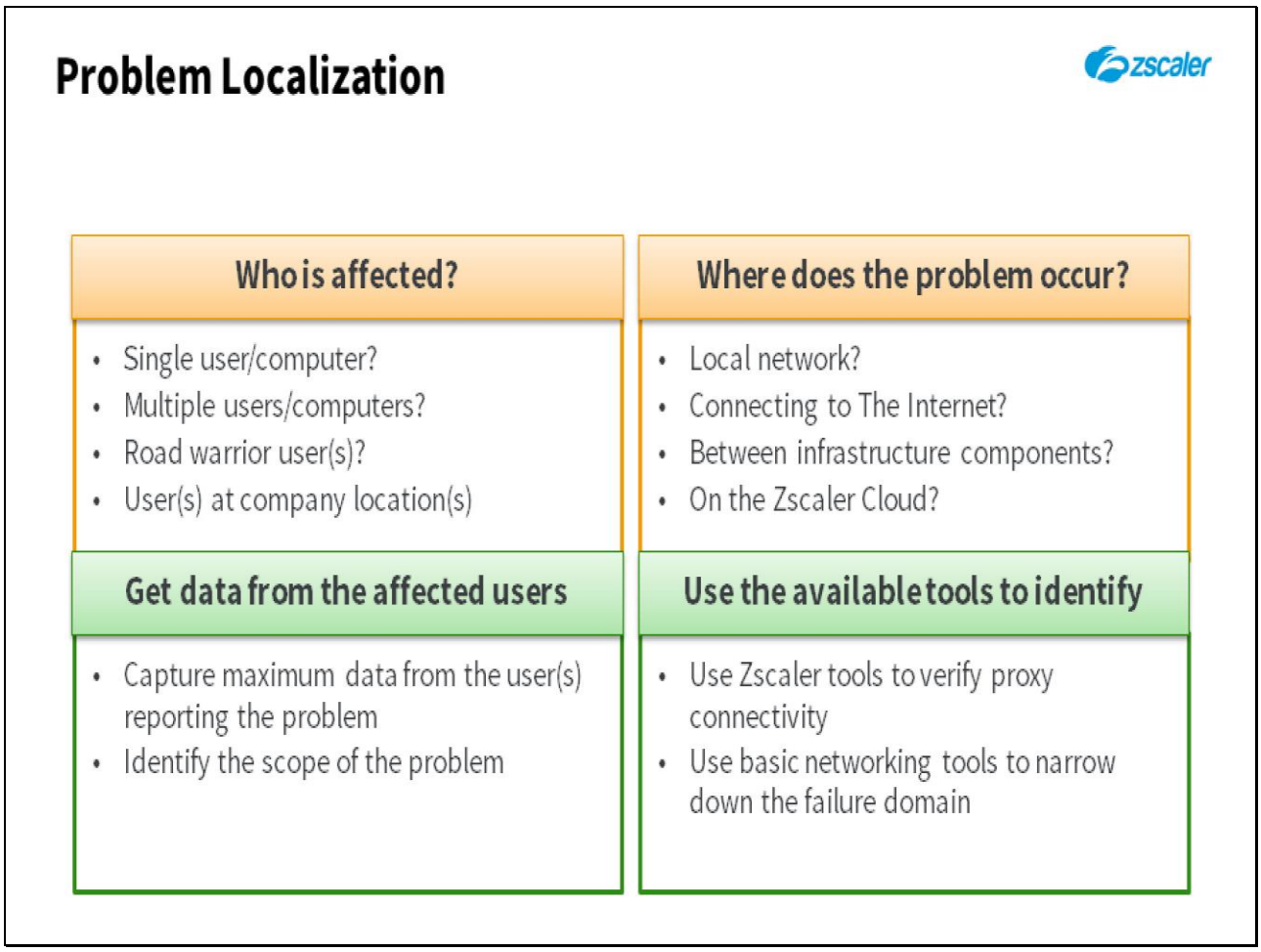
**Slide 16 - Problem Localization**




**Slide notes**

Having figured out who is affected by the problem, you then need to start homing in on the precise location of the problem. Is it a local issue? Is it an uplink problem to the Internet? Are there infrastructure components implicated? Or is it an issue with the Zscaler service?

**Slide 17 - Problem Localization**




**Slide notes**

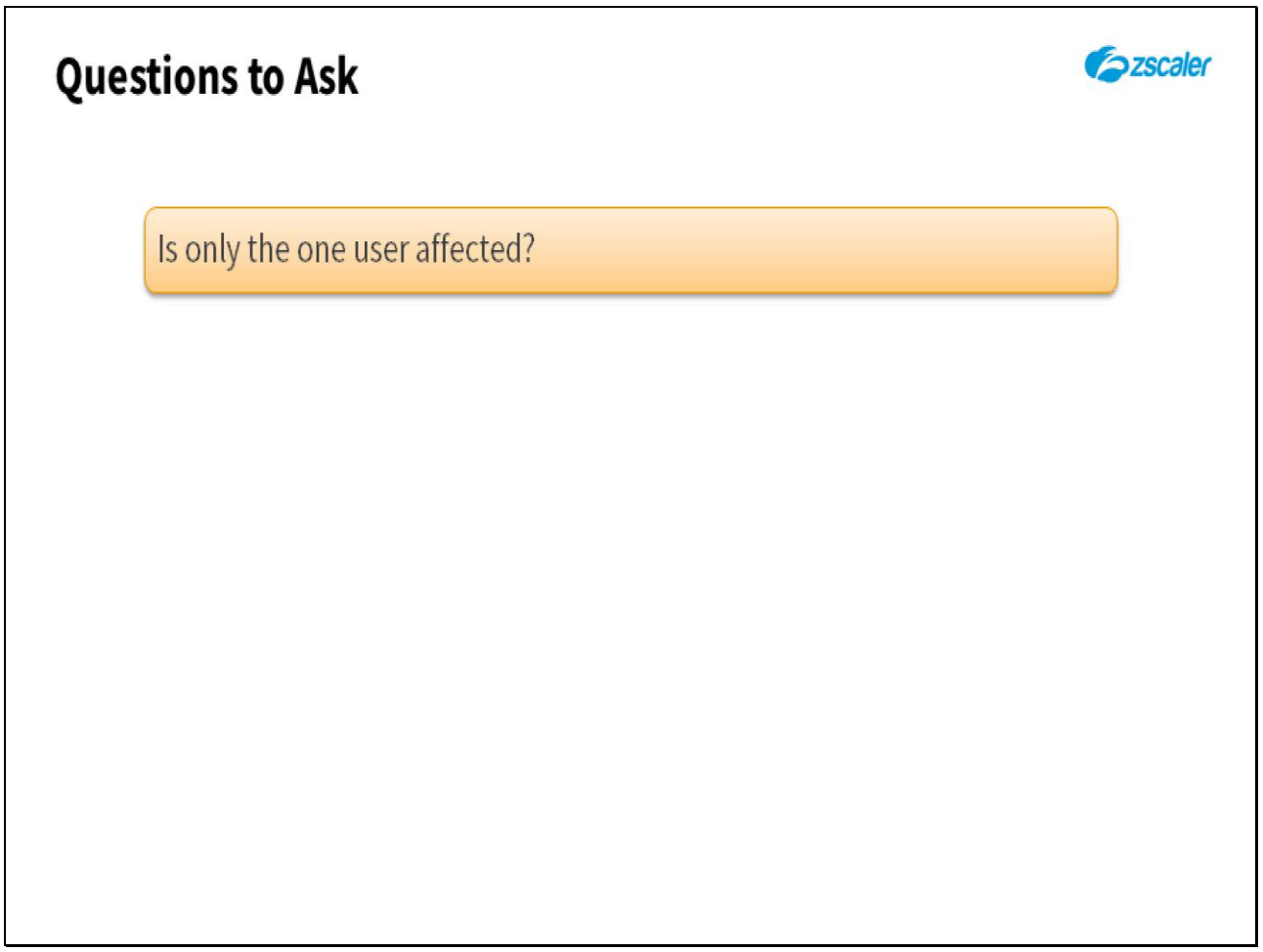
Here you will need to use the available tools, and a process of trial and error to identify the failure domain. This may require you to access client devices remotely to capture data from the Proxy Test tool, the Zscaler performance test page, the Zscaler Analyzer, or basic network troubleshooting tools such as **ping** and **traceroute**.

**Slide 18 - Questions and Tools**


**Slide notes**

In the next section, we will look at some of the questions to ask, and the tools to use to effectively narrow down the failure domain.

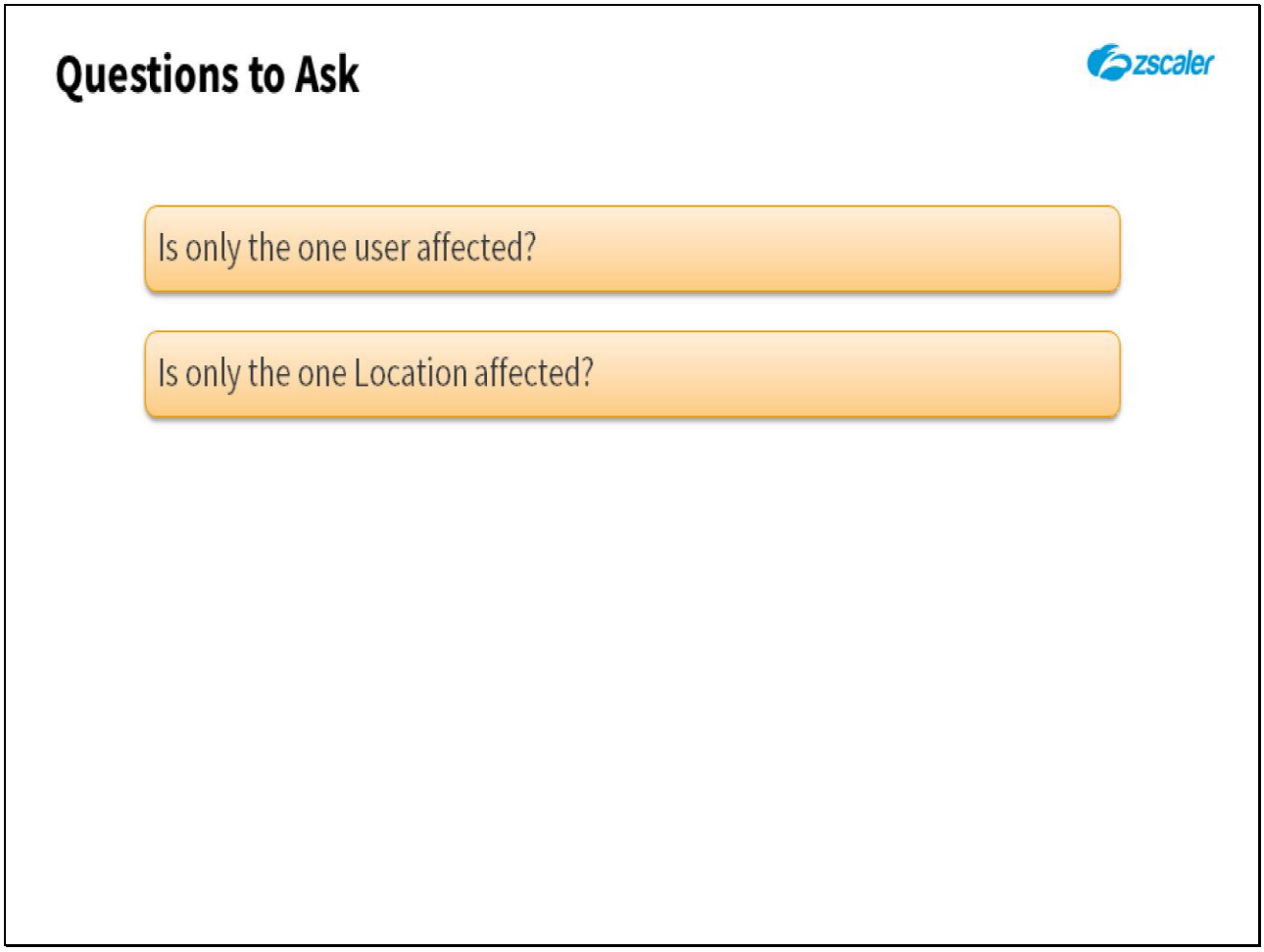
**Slide 19 - Questions to Ask**




**Slide notes**

Some questions to ask an end user calling in to report a problem, include: Whether they are the only one affected by the problem, …or do they know of others with the same issue?

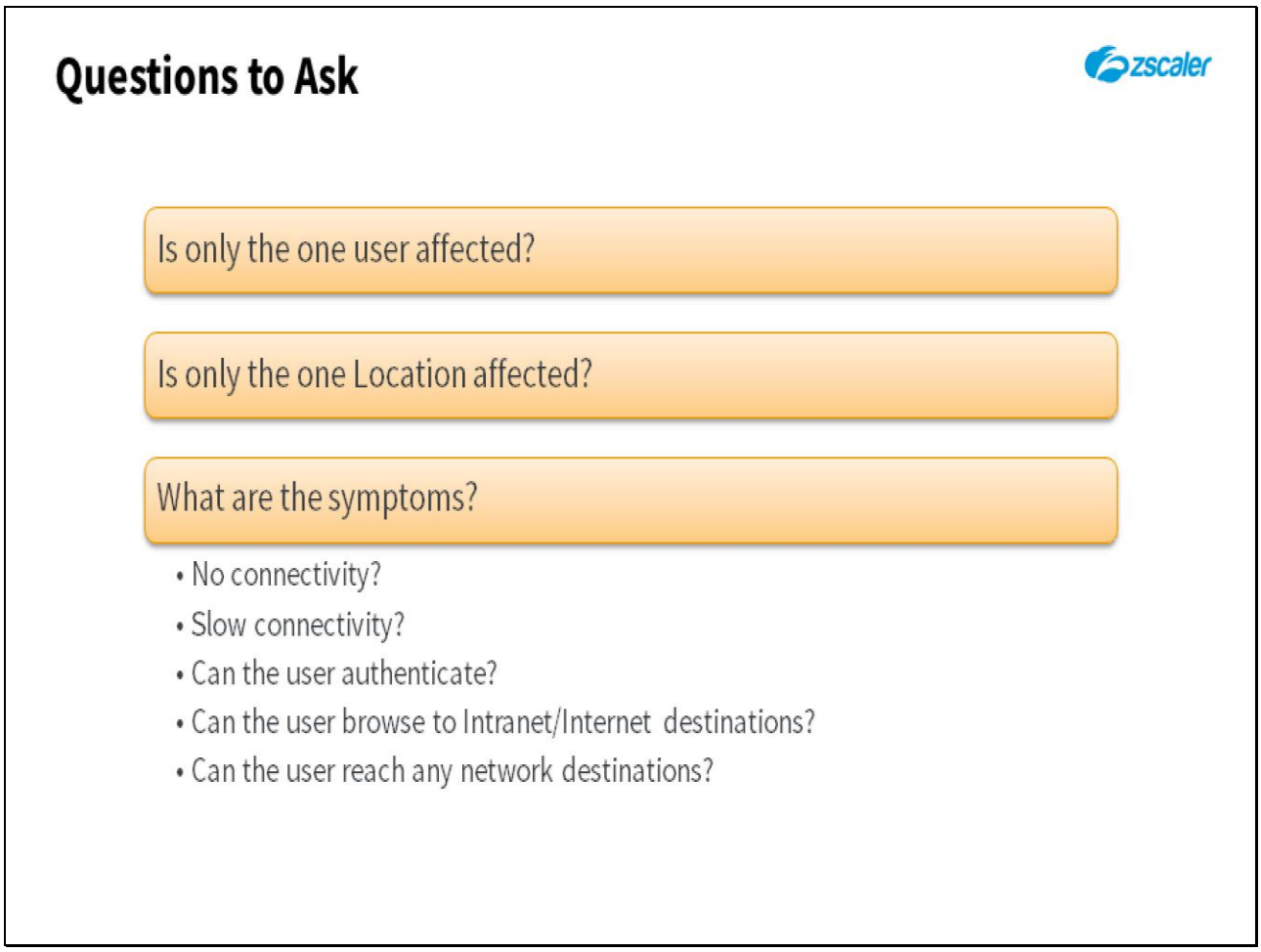
**Slide 20 - Questions to Ask**




**Slide notes**

Does the problem only happen at the one location? Or is it an issue from several, or even all locations?

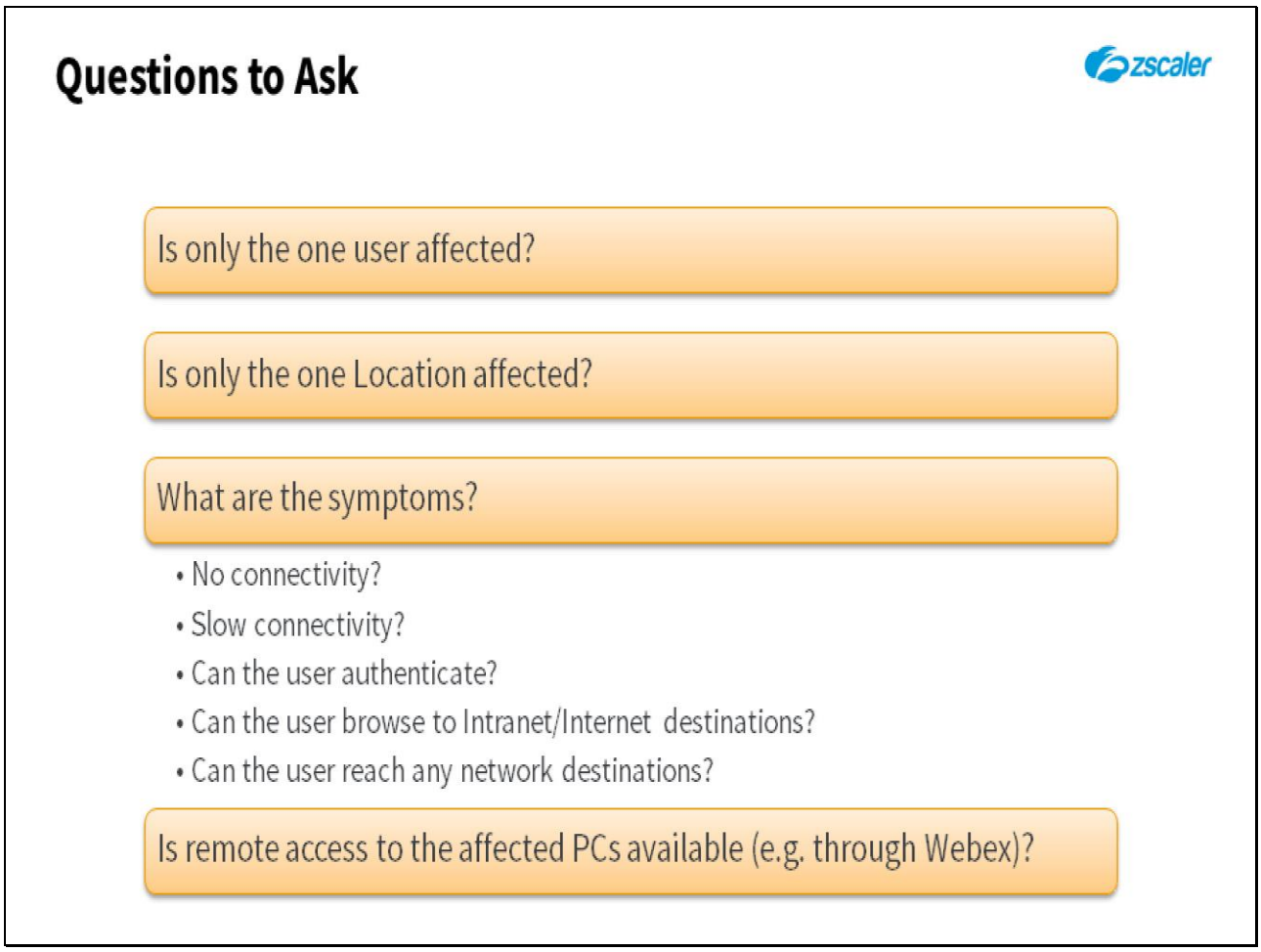
**Slide 21 - Questions to Ask**




**Slide notes**

What exactly are the symptoms? No connectivity at all? Slow connectivity, or response from some, or all Websites? Is the user able to authenticate (if authentication is required)? Can the user browse to Intranet or Internet destinations? Can the user reach any network destinations at all?

**Slide 22 - Questions to Ask**

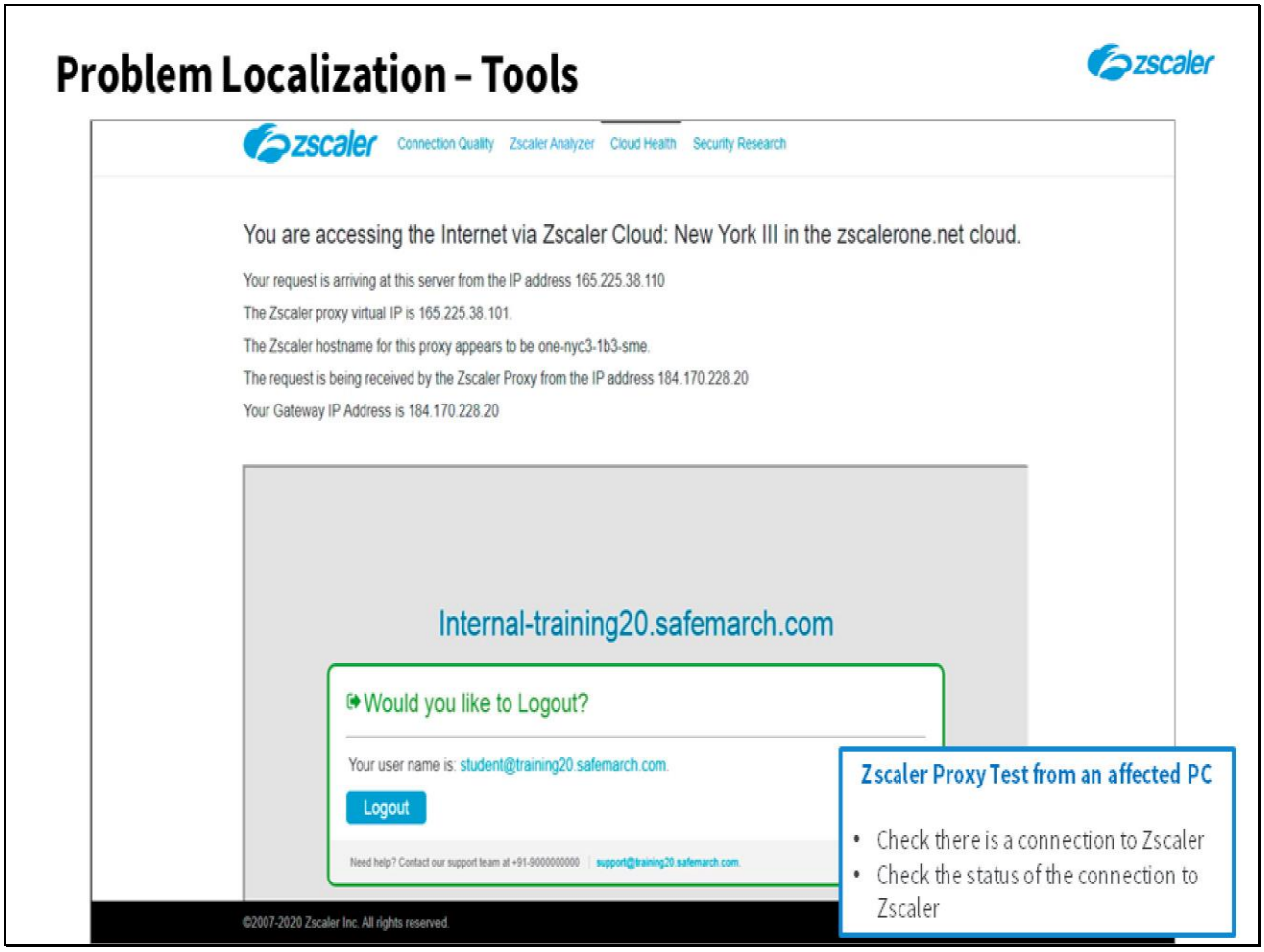



**Slide notes**

There is nothing that beats actually seeing the problem for yourself, so if at all possible arrange to get onto an affected device, either physically, or using some remote collaboration tool such as Webex.

Ideally you should be able to take over control of the machine, to run tests, and possibly to install software, such as the Zscaler Analyzer tool.

**Slide 23 - Problem Localization – Tools**

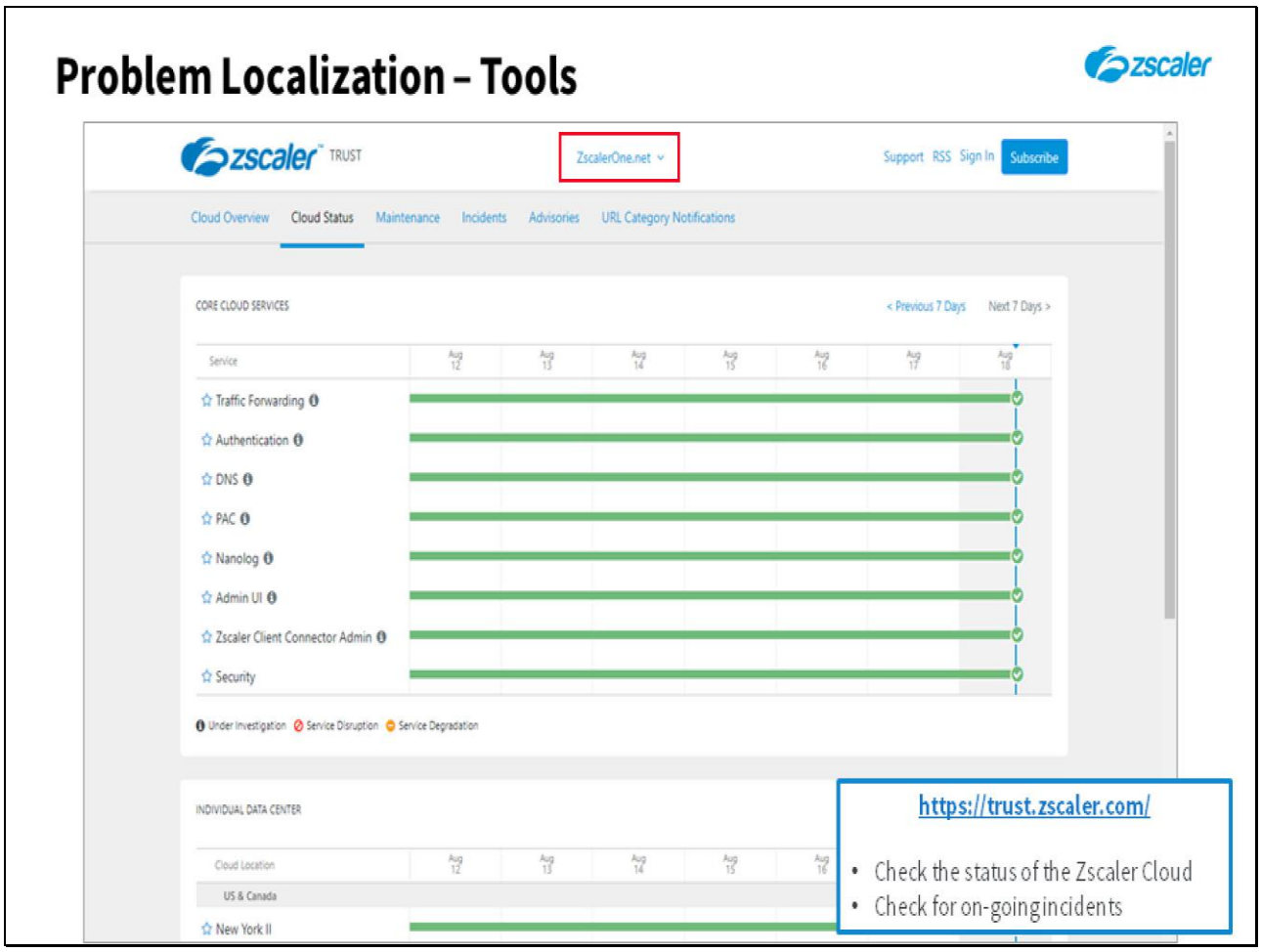



**Slide notes**

Tools that you should use (or ask the end user to use) as soon as possible after a problem is reported, include the Zscaler Proxy Test Website from the affected device. There are four main scenarios that you will see (which we will discuss in more detail in just a minute):

- Scenario 1: The user is connecting through Zscaler and is authenticated.
- Scenario 2: The user is connecting through Zscaler but is not authenticated.
- Scenario 3: The user is not connecting through Zscaler.
- Scenario 4: The user has no Internet connection at all.

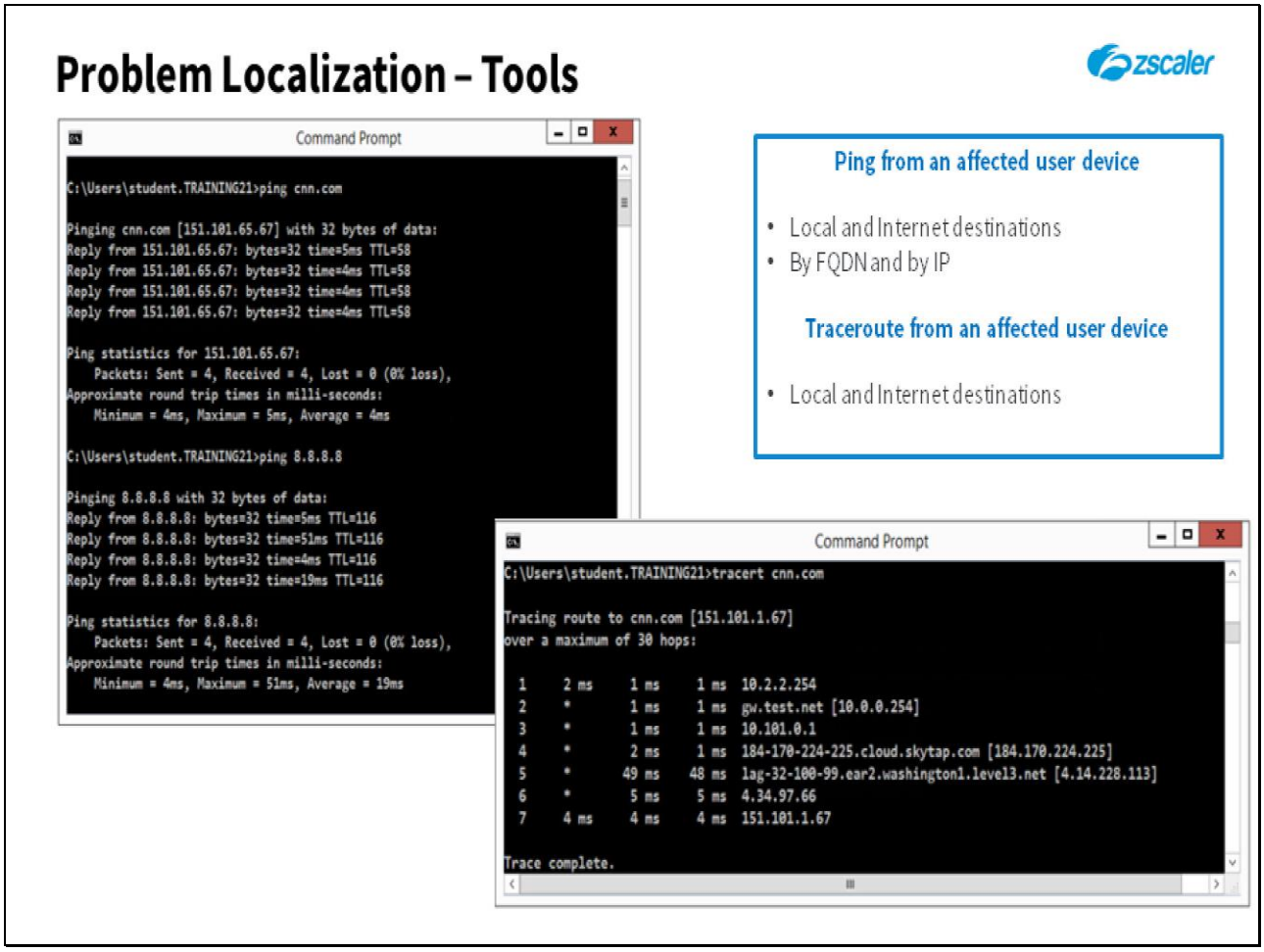
**Slide 24 - Problem Localization – Tools**




**Slide notes**

One of your first checks when an end user calls in with a problem should be the Zscaler Trust site for the Cloud in question, to check for known outages or known issues.

**Slide 25 - Problem Localization – Tools**




**Slide notes**

Do not neglect basic network connectivity tools such as a **ping** from an affected user device. Test for responses from Intranet and Internet destinations, and using FQDNs and IP addresses (to verify that DNS is resolving OK).

Another basic network troubleshooting tool is to do a **traceroute** from an affected user device. Once again, run the test against both Intranet, and Internet destinations.

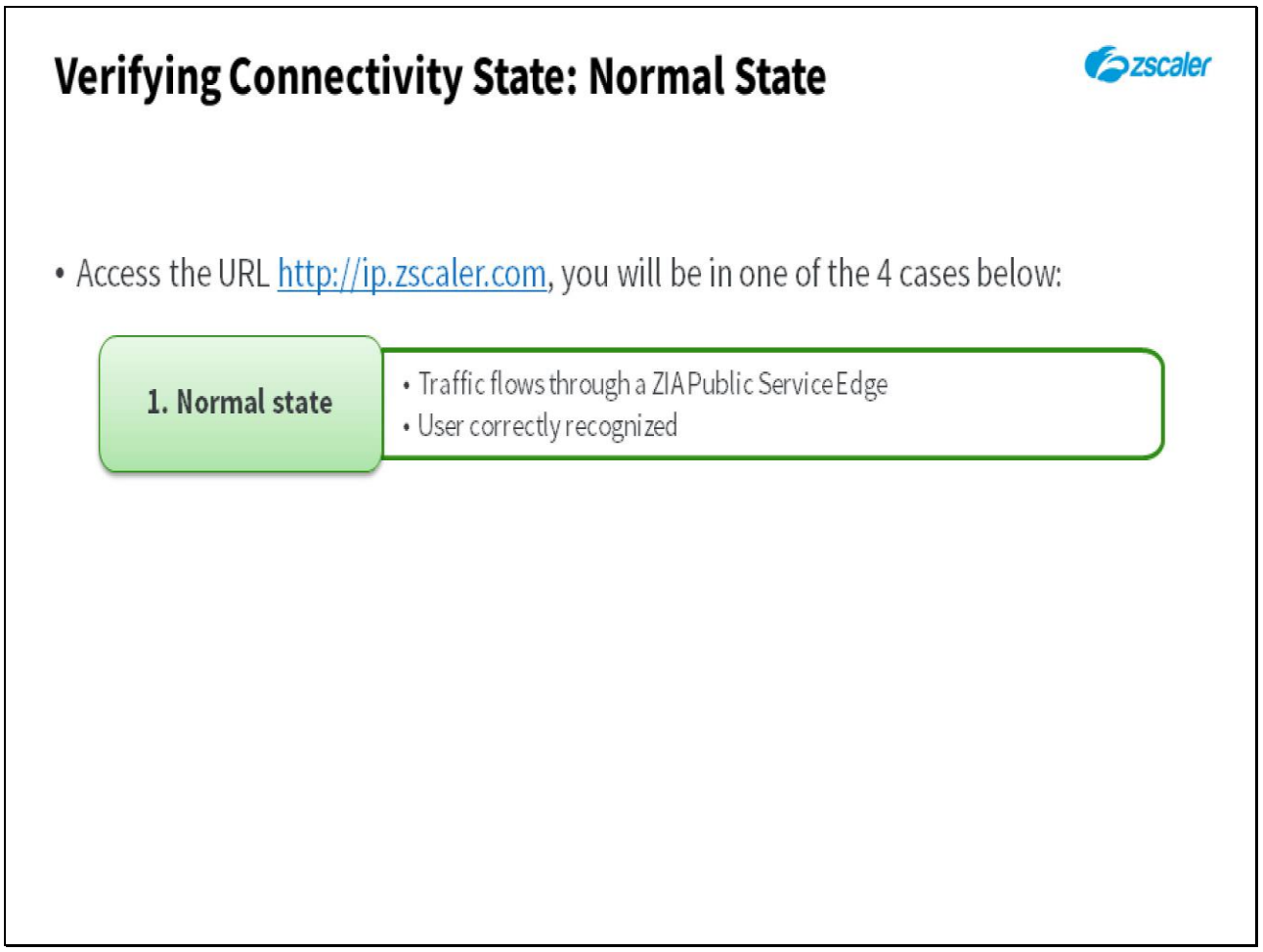
Another basic network troubleshooting tool is to do a ‘traceroute’ from an affected user device. Once again, run the test against both Intranet, and Internet destinations.

**Slide 26 - Verifying Connectivity State**


**Slide notes**

In the next section, we will look at using the Zscaler Proxy Test Website for verifying a user's connectivity state.

**Slide 27 - Verifying Connectivity State: Normal State**

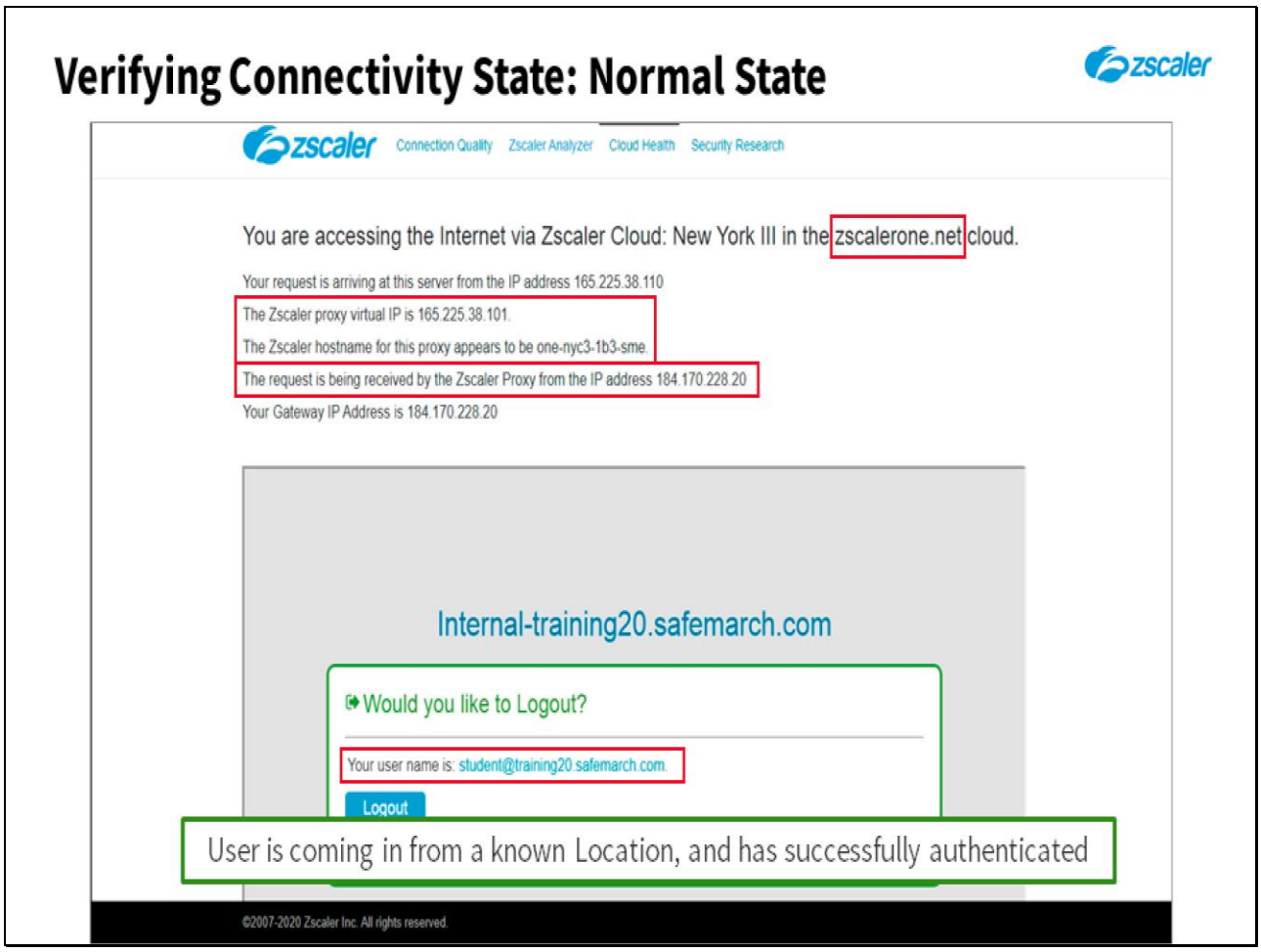



**Slide notes**

The first step in troubleshooting connectivity issues is to try and reach the URL **http://ip.zscaler.com**, where you will see one of these four results:

1. Everything is in a completely normal state, which means your traffic reaches the ZIA Public Service Edge and users are being authenticated. The ZIA Public Service Edge recognizes the authentication cookies that are stored by the Browsers.

**Slide 28 - Verifying Connectivity State: Normal State**




**Slide notes**

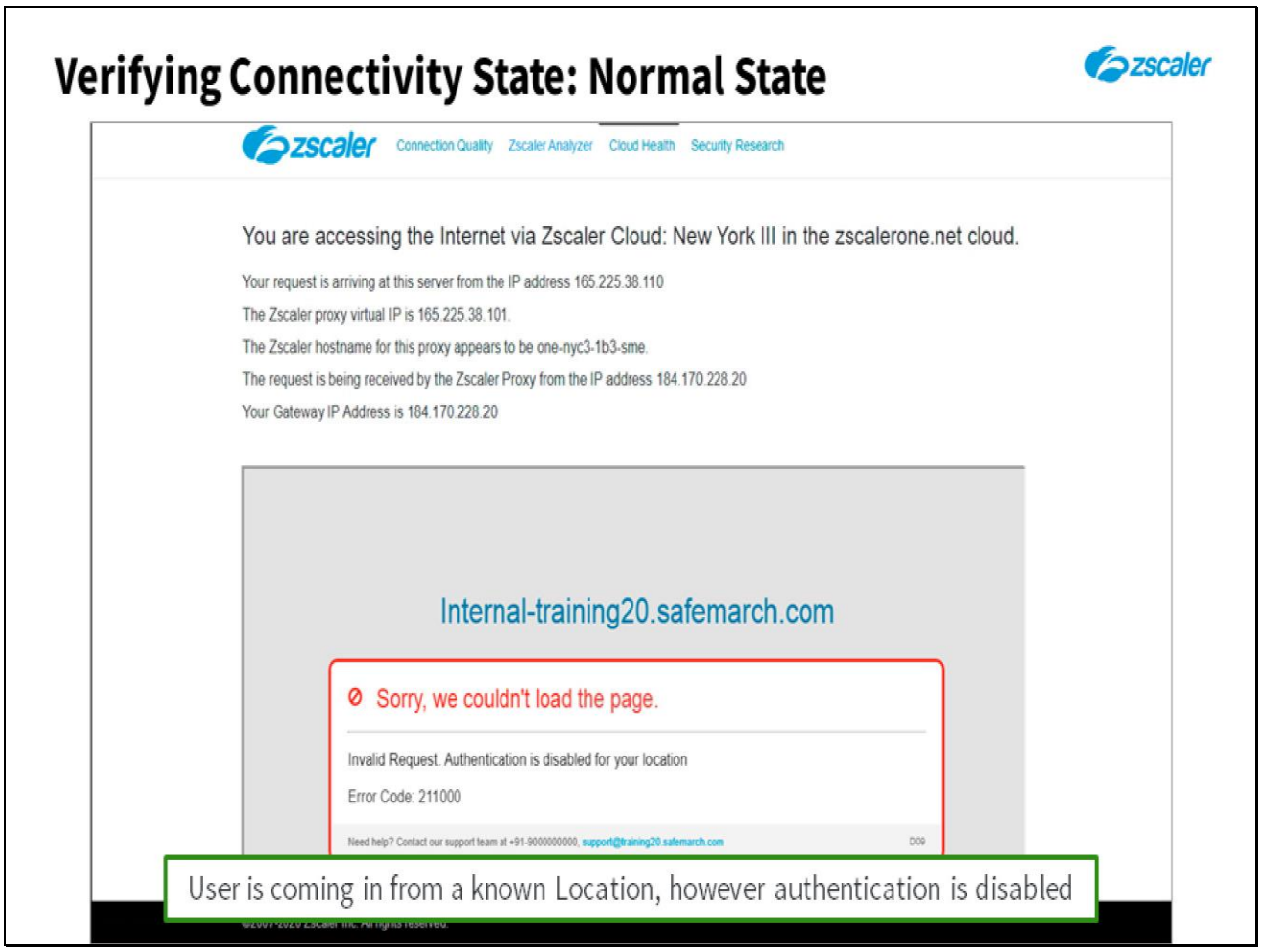
This slide shows you what happens when everything is working as expected, you are accessing the Internet through a ZIA Public Service Edge and the system correctly detects your username. In this example:

The traffic flows through the ZIA Public Service Edge with IP address 165.225.38.110, and hostname one-nyc3-1b3-sme. Note that this ZIA Public Service Edge is part of the Zscalerone cloud.

In this example, your IP address is 184.170.228.20 and your username is student@training20.safemarch.com

The information outlined here should be readily available anytime you need to contact Zscaler technical support, as these parameters are required by Zscaler technical support so they can effectively troubleshoot customer issues.

**Slide 29 - Verifying Connectivity State: Normal State**

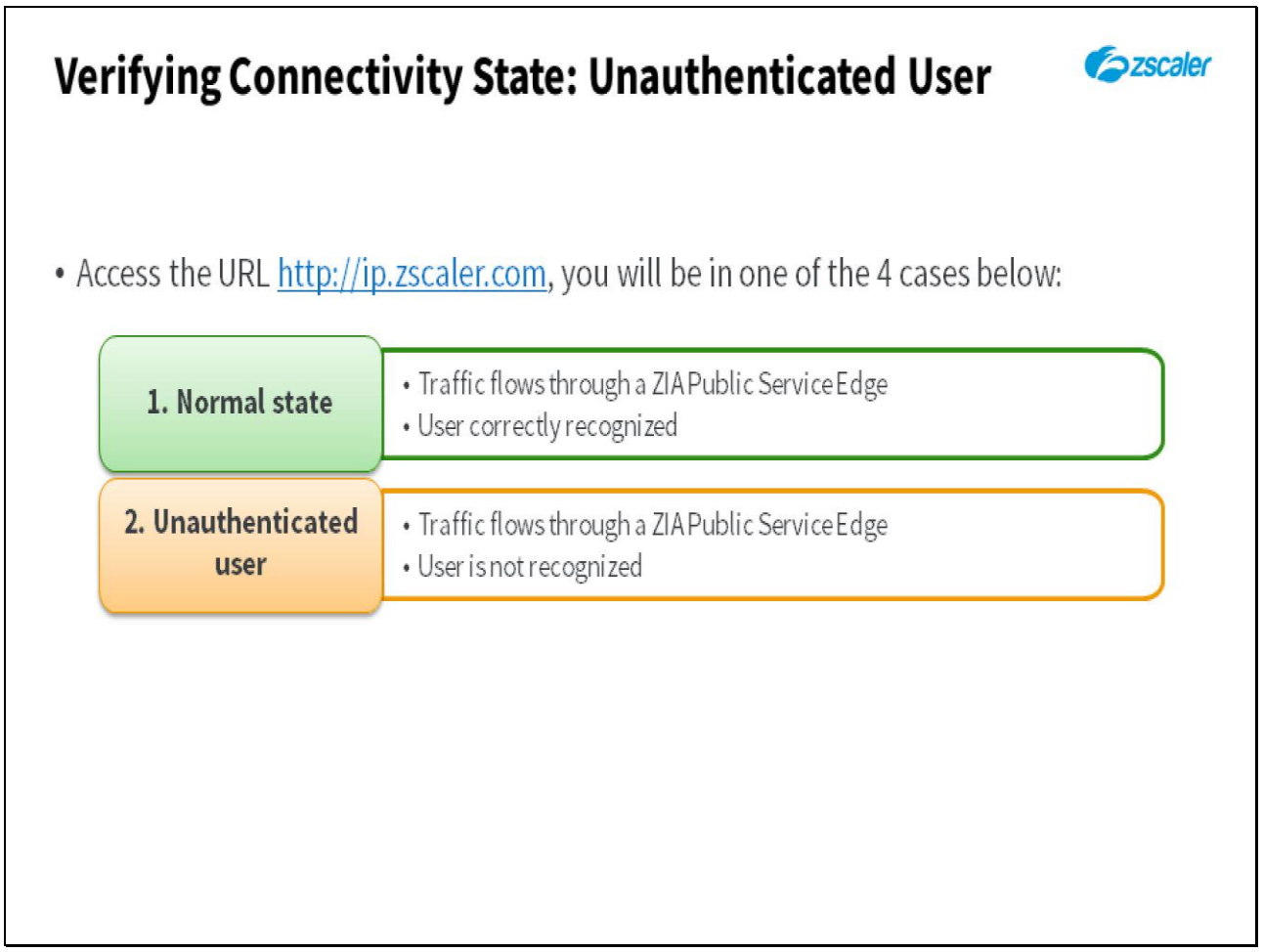



**Slide notes**

If you are accessing the Internet through a ZIA Public Service Edge, but your system is not being authenticated, the service displays a message similar to the one shown on this slide.

There are several causes for this, however, they are relatively simple to troubleshoot. In this case, the 'error' message says, **Authentication is disabled for your location**, …which indicates that authentication is not required. So this is the 'Normal' state for users from locations that do not require authentication.

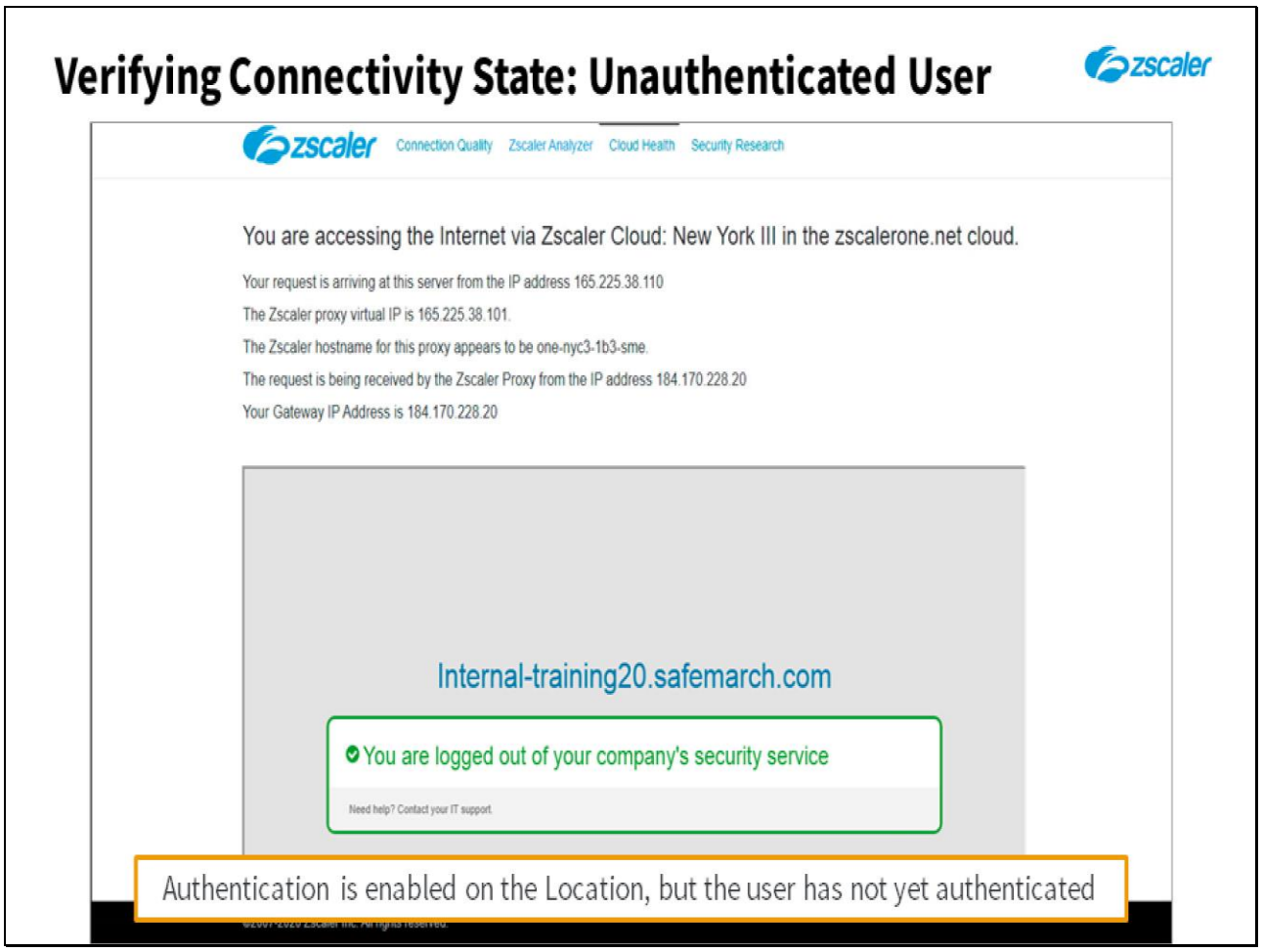
**Slide 30 - Verifying Connectivity State: Unauthenticated User**




**Slide notes**

In Case 2, your traffic reaches the ZIA Public Service Edge, but the user is not recognized. This means that the Browser does not have valid authentication cookies stored, either because authentication has failed, or authentication is not required.

**Slide 31 - Verifying Connectivity State: Unauthenticated User**

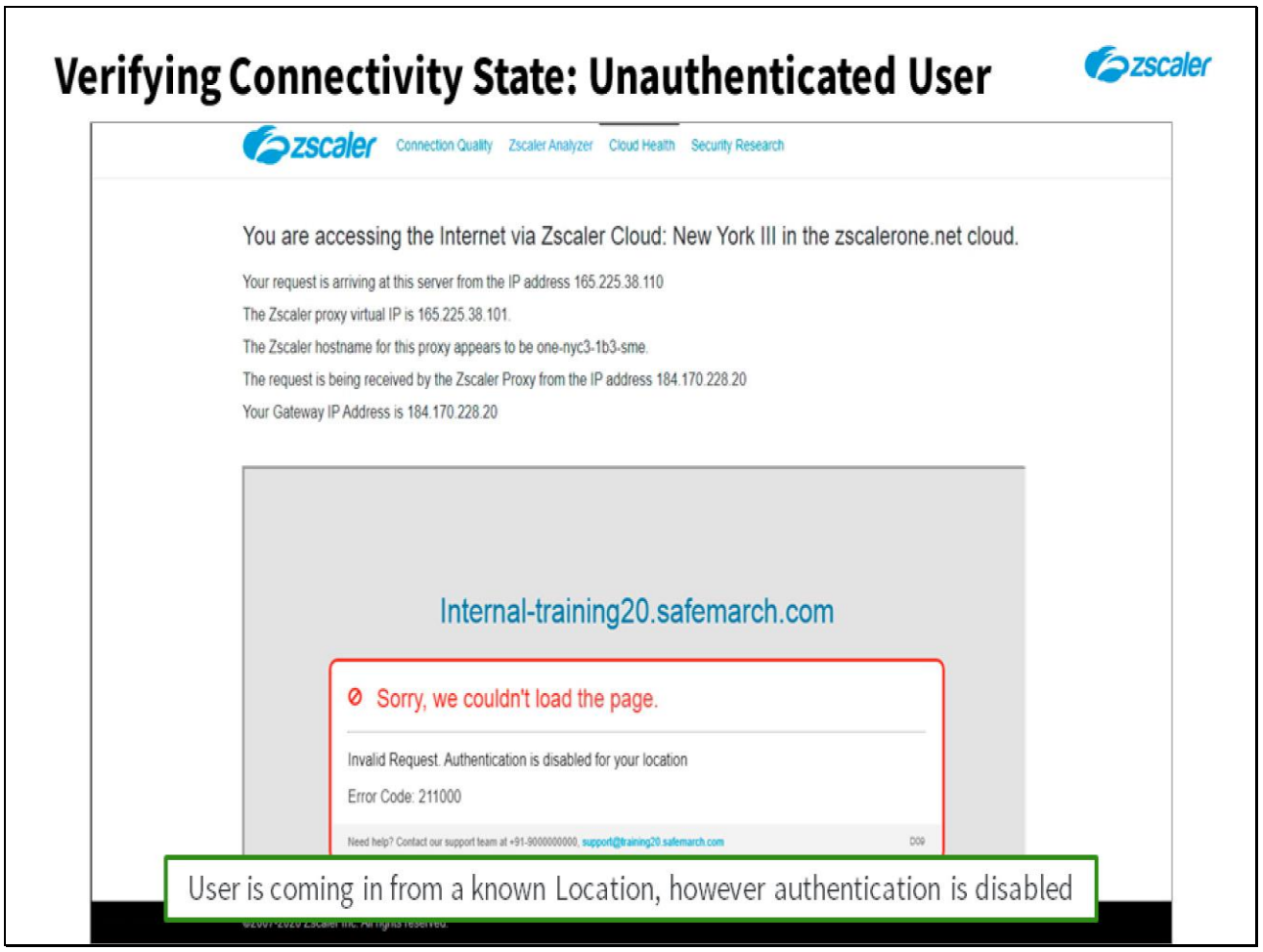



**Slide notes**

If you are accessing the Internet through a ZIA Public Service Edge, but your system is not being authenticated, the service displays a message similar to the one shown on this slide. There are several causes for this; however, they are relatively simple to troubleshoot.

It may be that the user simply has not logged in, that their password has expired, or that their account has somehow been disabled.

**Slide 32 - Verifying Connectivity State: Unauthenticated User**

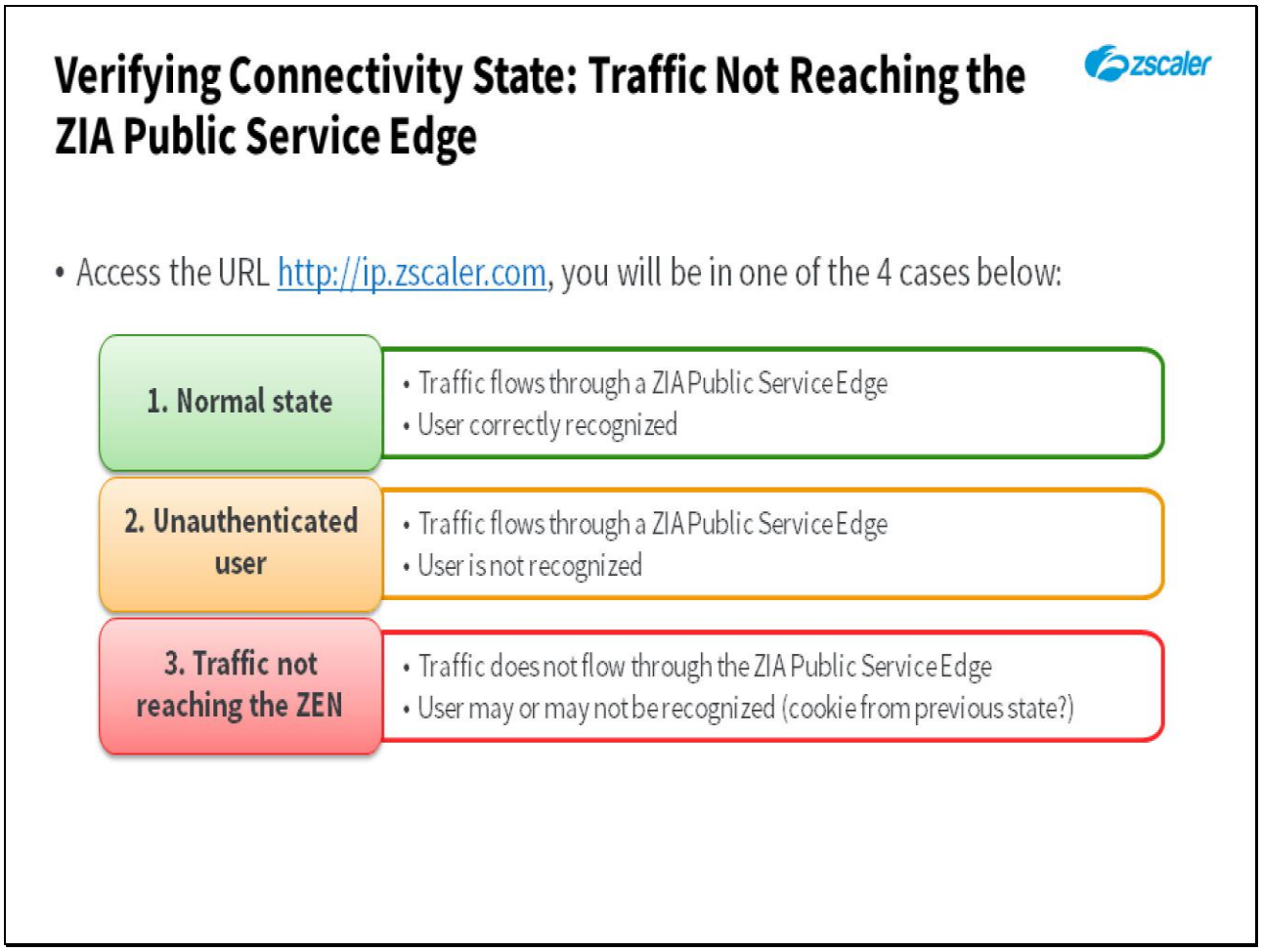



**Slide notes**

Or, as we saw earlier, it could simply be that authentication is not required for the user's location.

**Slide 33 - Verifying Connectivity State: Traffic Not Reaching the**

**ZIA Public Service Edge**

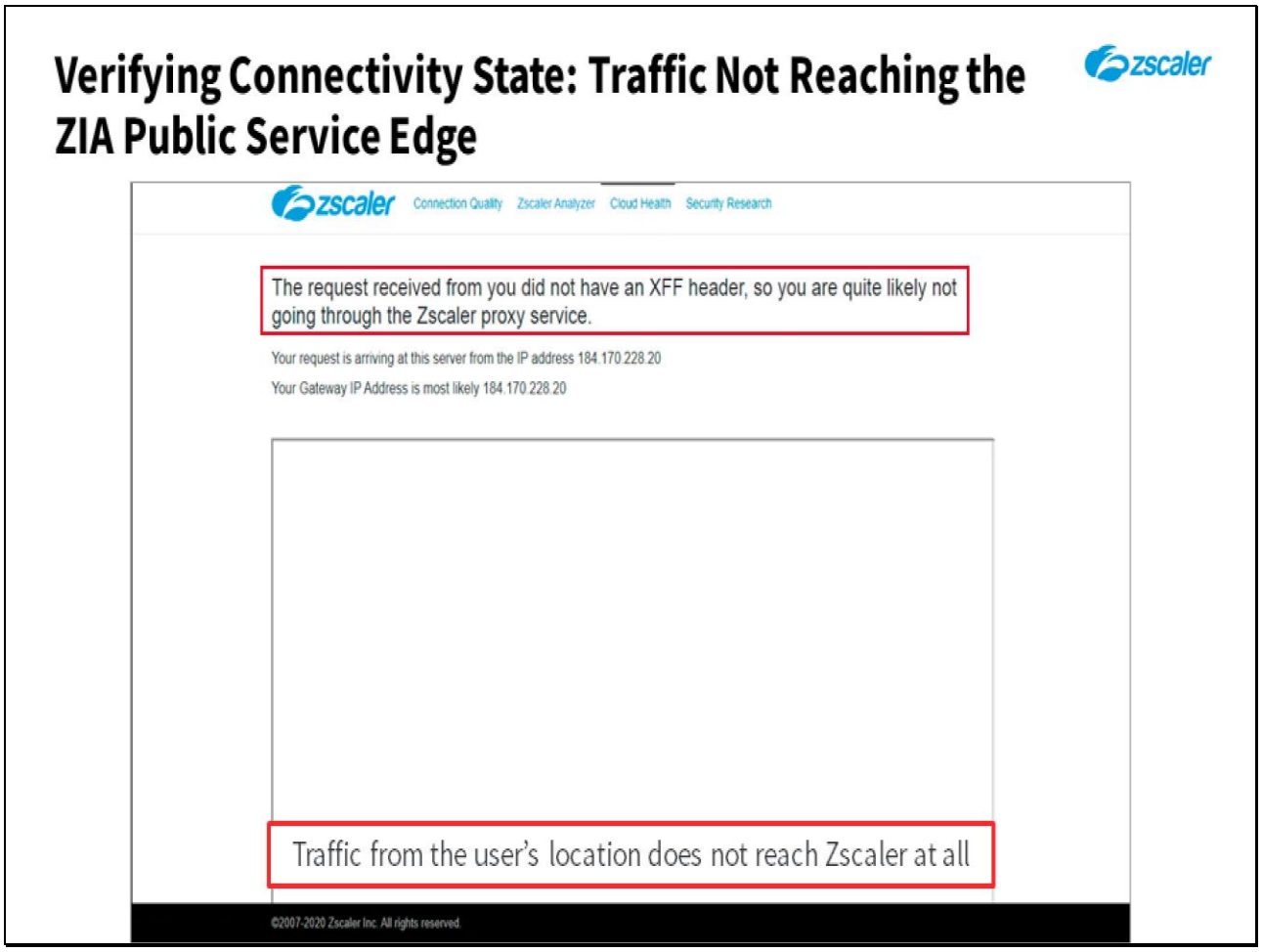



**Slide notes**

In Case 3, your traffic does not reach the ZIA Public Service Edge. Although the end user may still be identified because the Browser has stored cookies from a previous session in which the user was successfully authenticated.

**Slide 34 - Verifying Connectivity State: Traffic Not Reaching the**

**ZIA Public Service Edge**



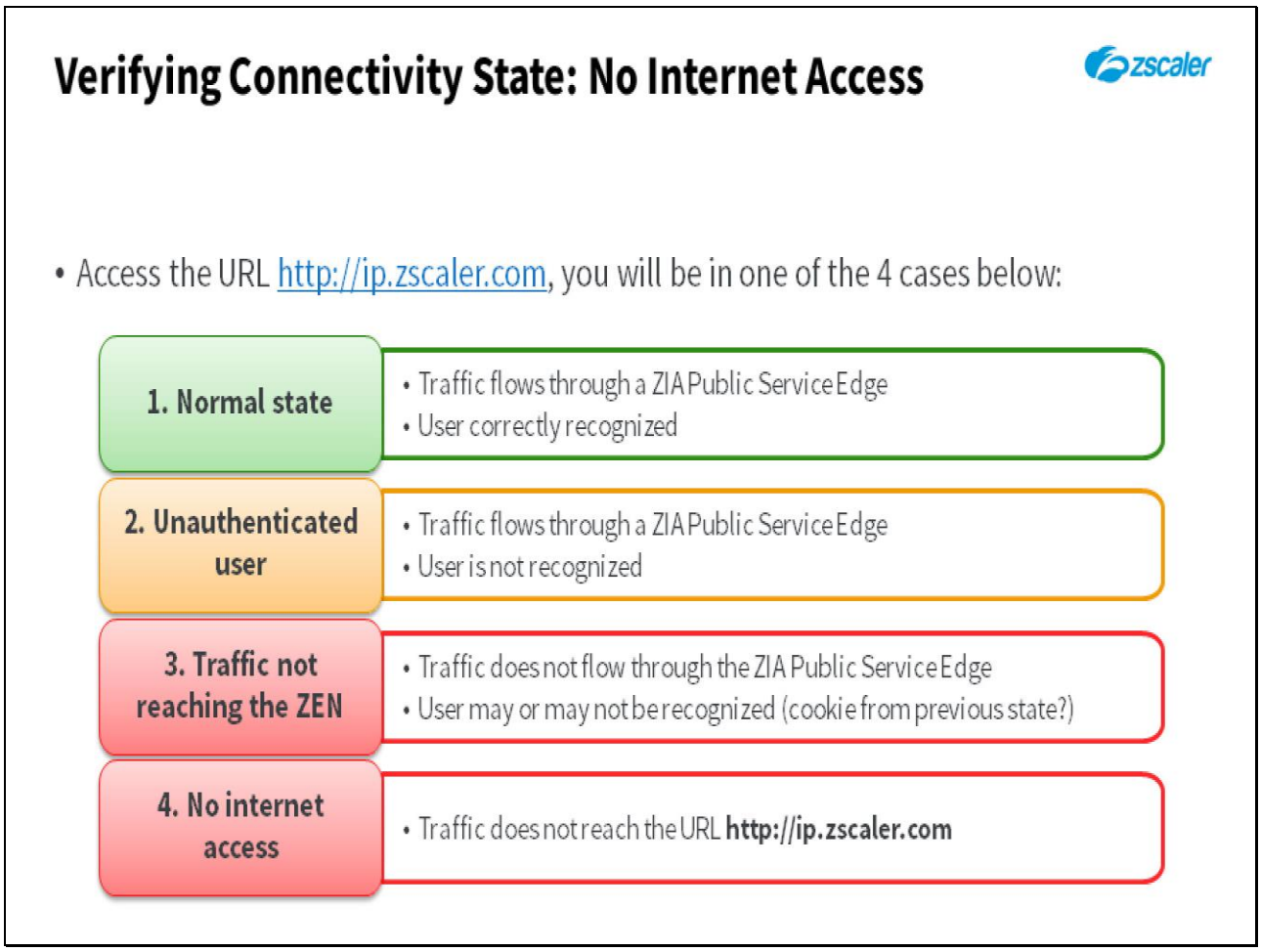

**Slide notes**

There are two subcases for this scenario:

1. In the first case, your traffic does not reach a ZIA Public Service Edge and the system cannot detect your identity, as shown in this slide.

2. In the second case, your traffic does not reach the ZIA Public Service Edge, however, the system can detect your identity. This simply means that your Browser recently reached a ZIA Public Service Edge and was correctly authenticated, the authentication cookies are still valid and stored in the Browser.

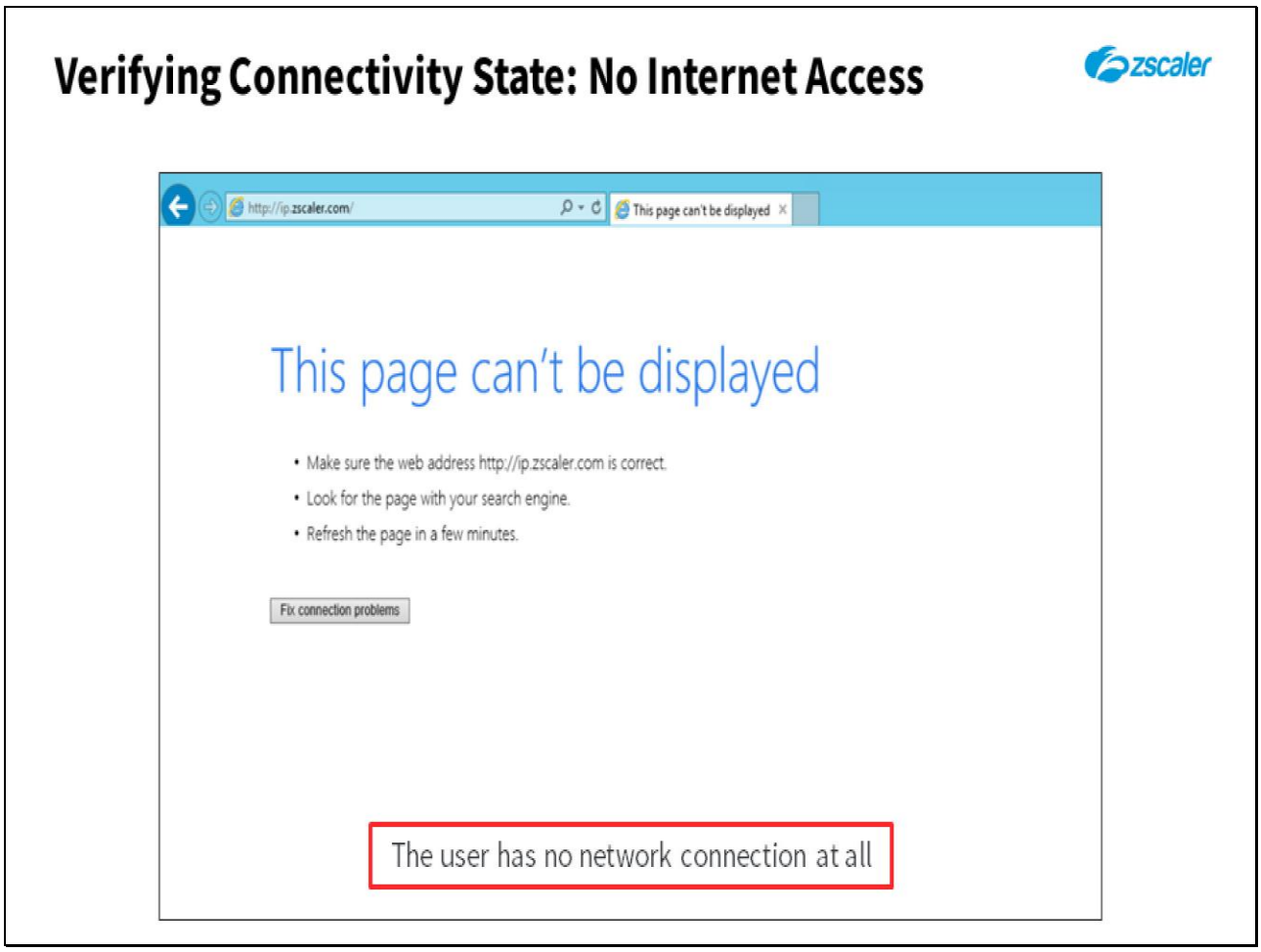
**Slide 35 - Verifying Connectivity State: No Internet Access**




**Slide notes**

In the final case, you have no Internet access at all and you're unable to reach **ip.zscaler.com** or any other site that you are testing.

**Slide 36 - Verifying Connectivity State: No Internet Access**




**Slide notes**

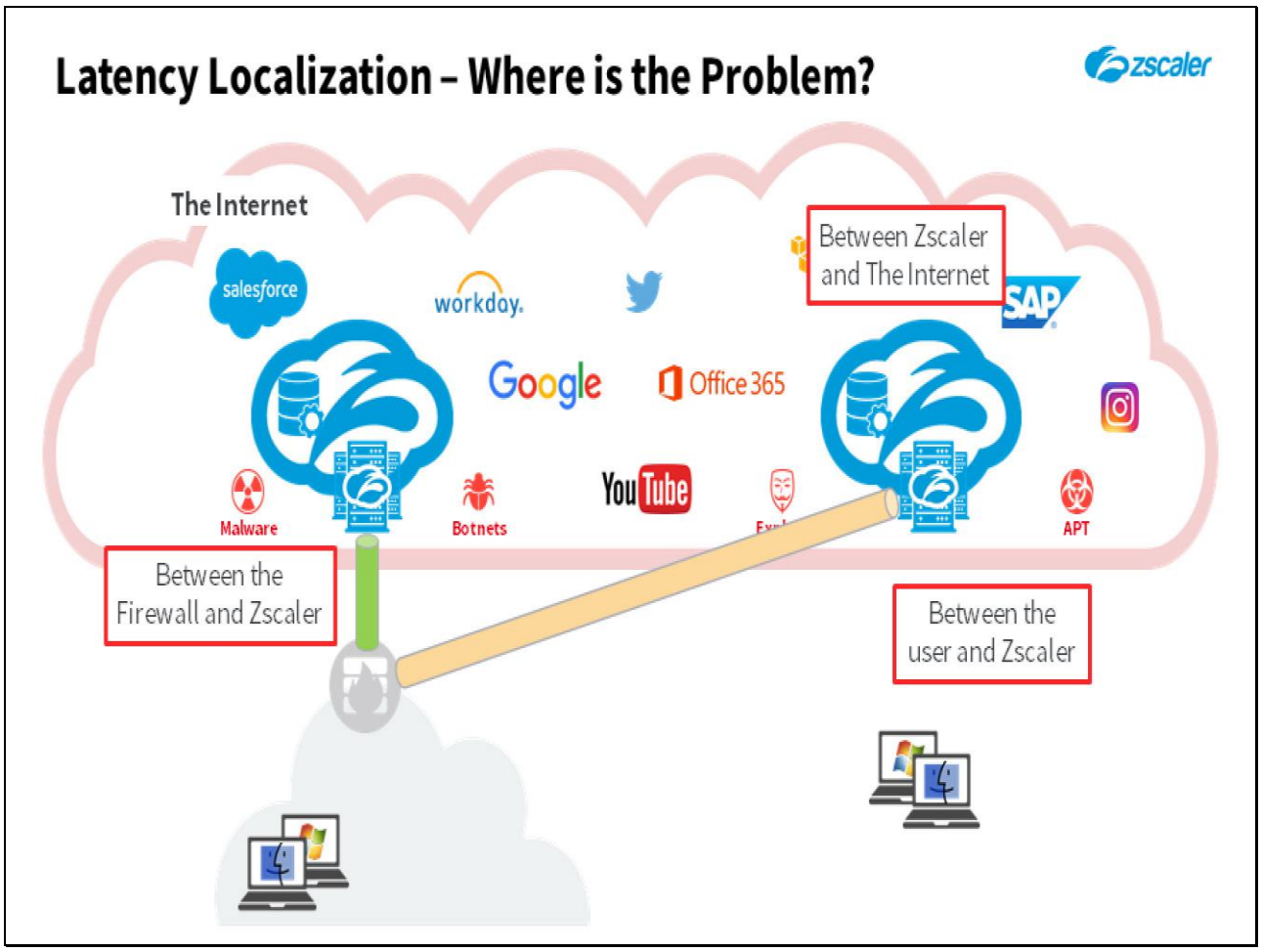
There are several causes for this issue, some causes (and the most likely ones) are not related to Zscaler at all.

**Slide 37 - Identifying Sources of Latency**


**Slide notes**

In the final section, we will look at using the Zscaler Proxy Test Website for verifying a user's connectivity state.

**Slide 38 - Latency Localization – Where is the Problem?**

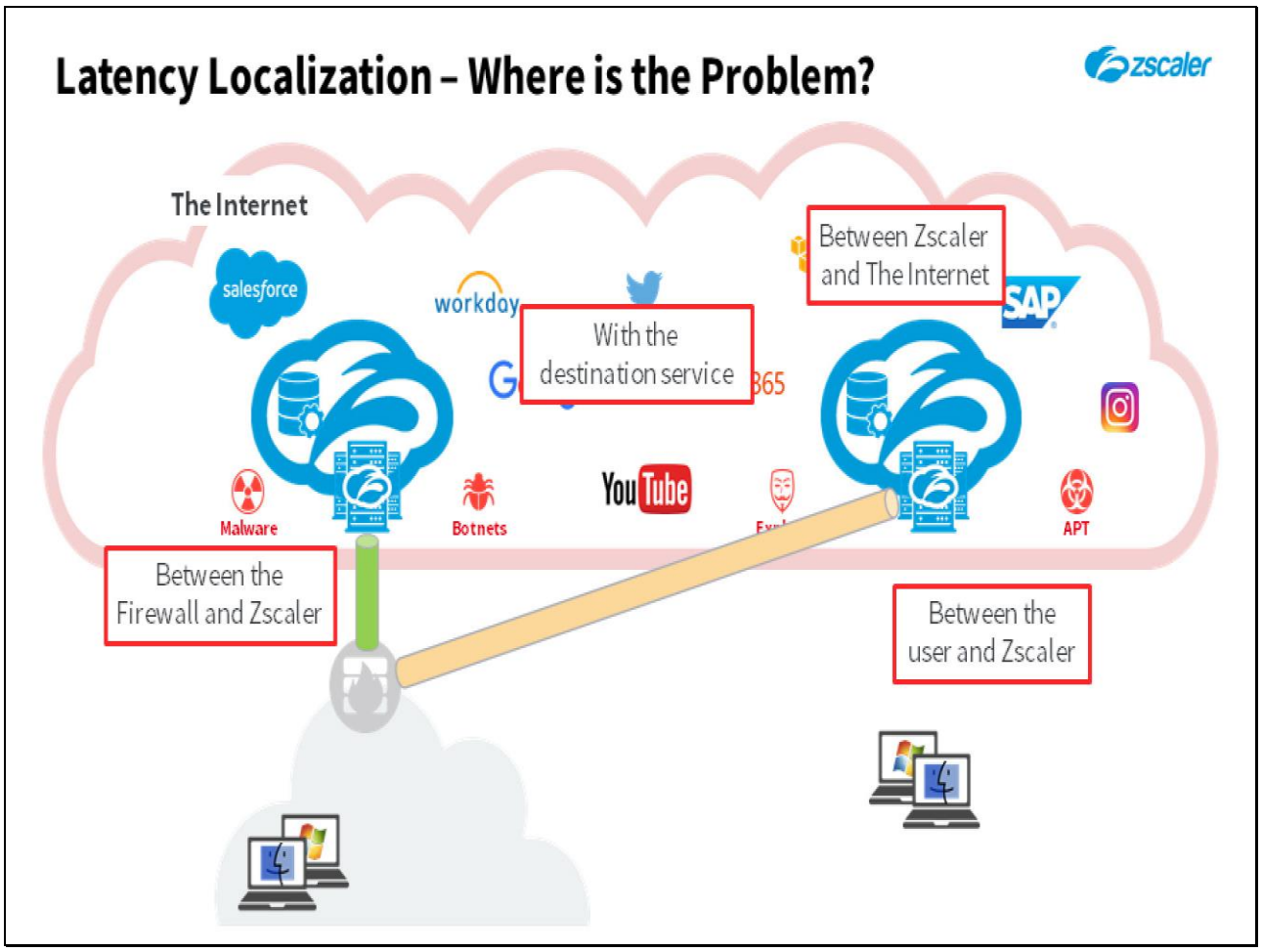



**Slide notes**

As with all other reported problems, latency can occur on any of the connections between the end user and the destination service or site.

Remember that user traffic processed by Zscaler must transit the Internet twice, reaching Zscaler in the first place, then between Zscaler and the final destination.

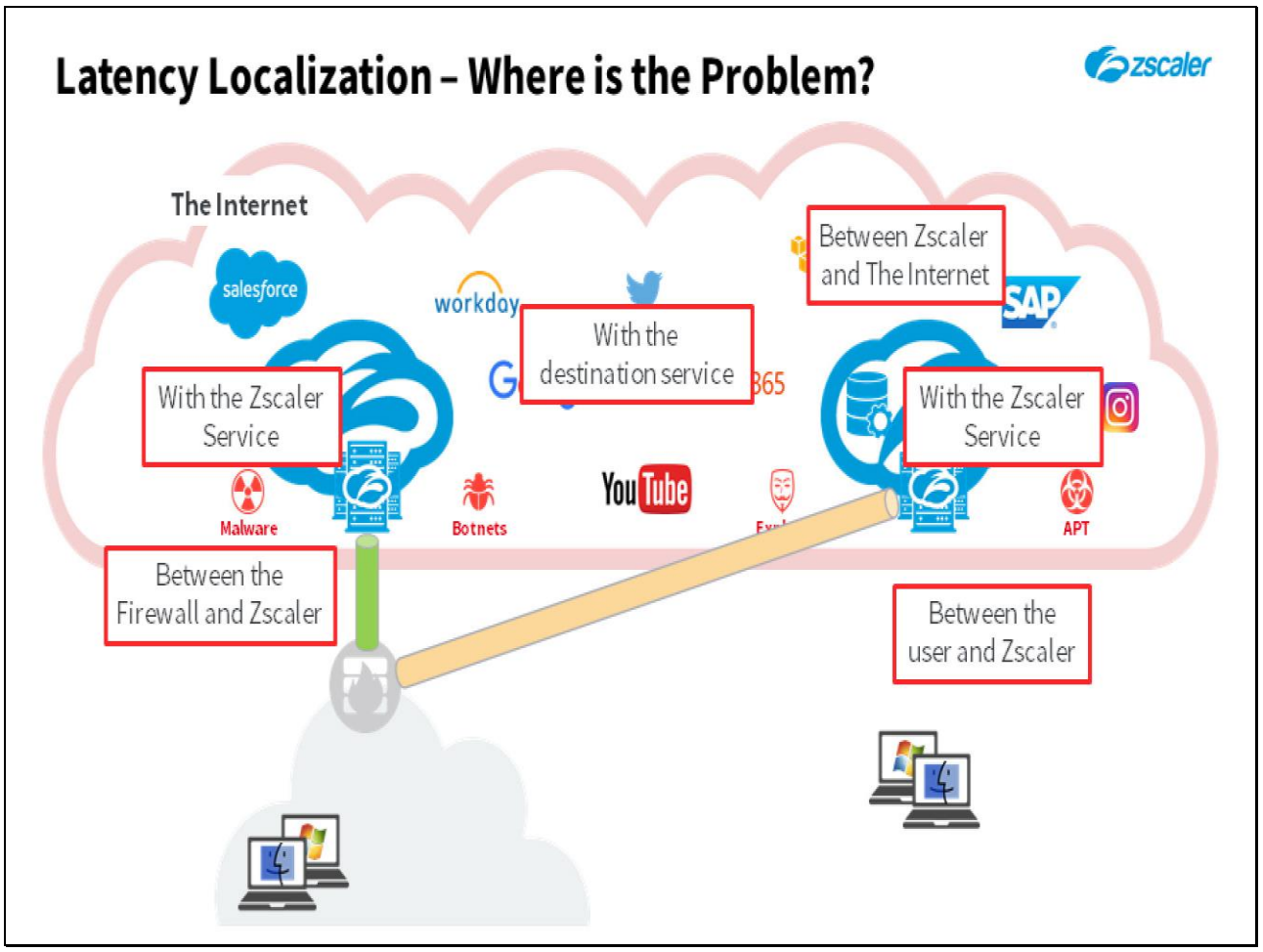
**Slide 39 - Latency Localization – Where is the Problem?**




**Slide notes**

Also bear in mind that the destination service or site may have performance issues that will add to the latency experienced by the end user.

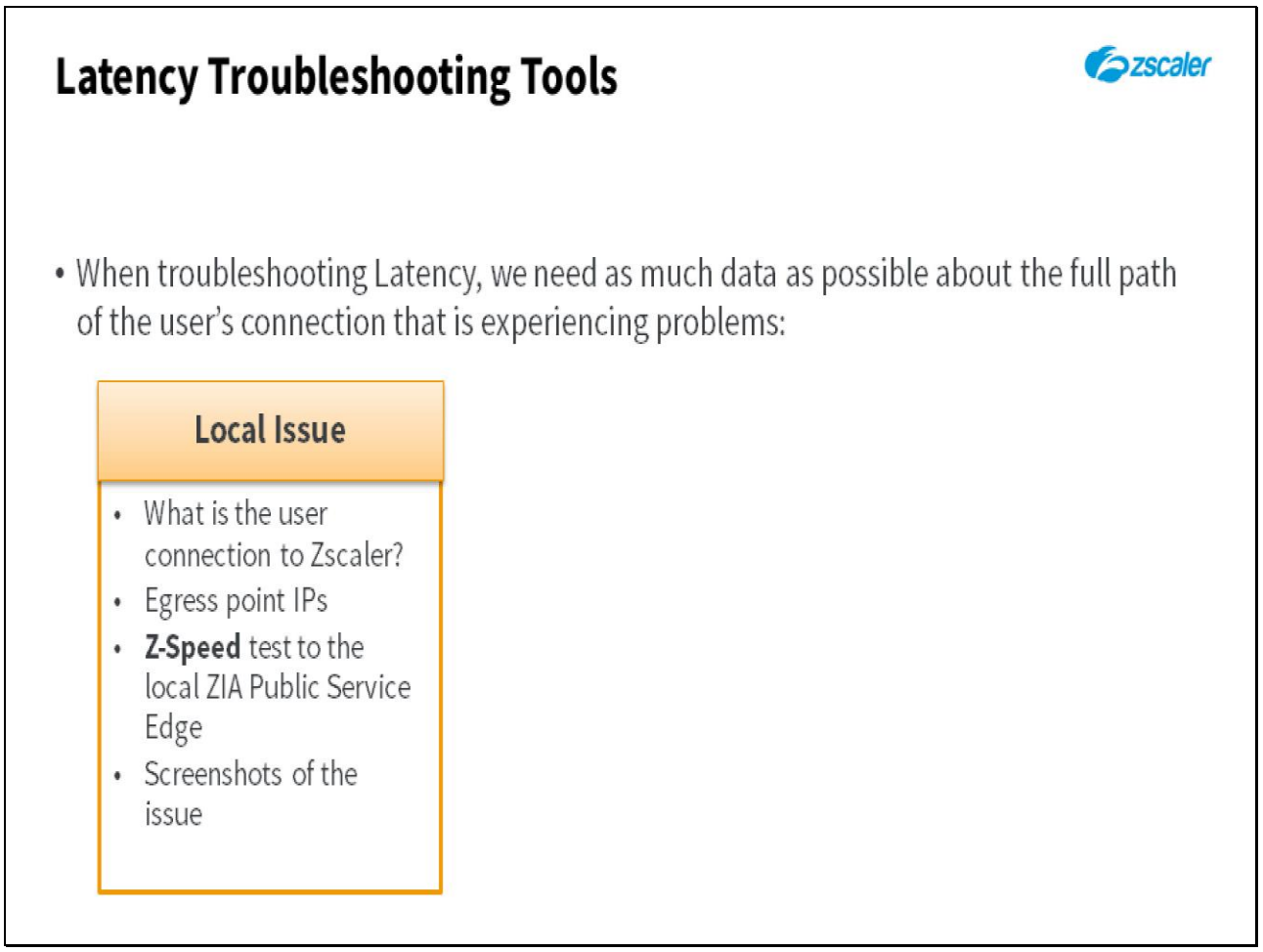
**Slide 40 - Latency Localization – Where is the Problem?**




**Slide notes**

There may under exceptional circumstances be latency issues within the Zscaler Cloud. However, this would be due to error conditions that should be identified and fixed very quickly.

**Slide 41 - Latency Troubleshooting Tools**

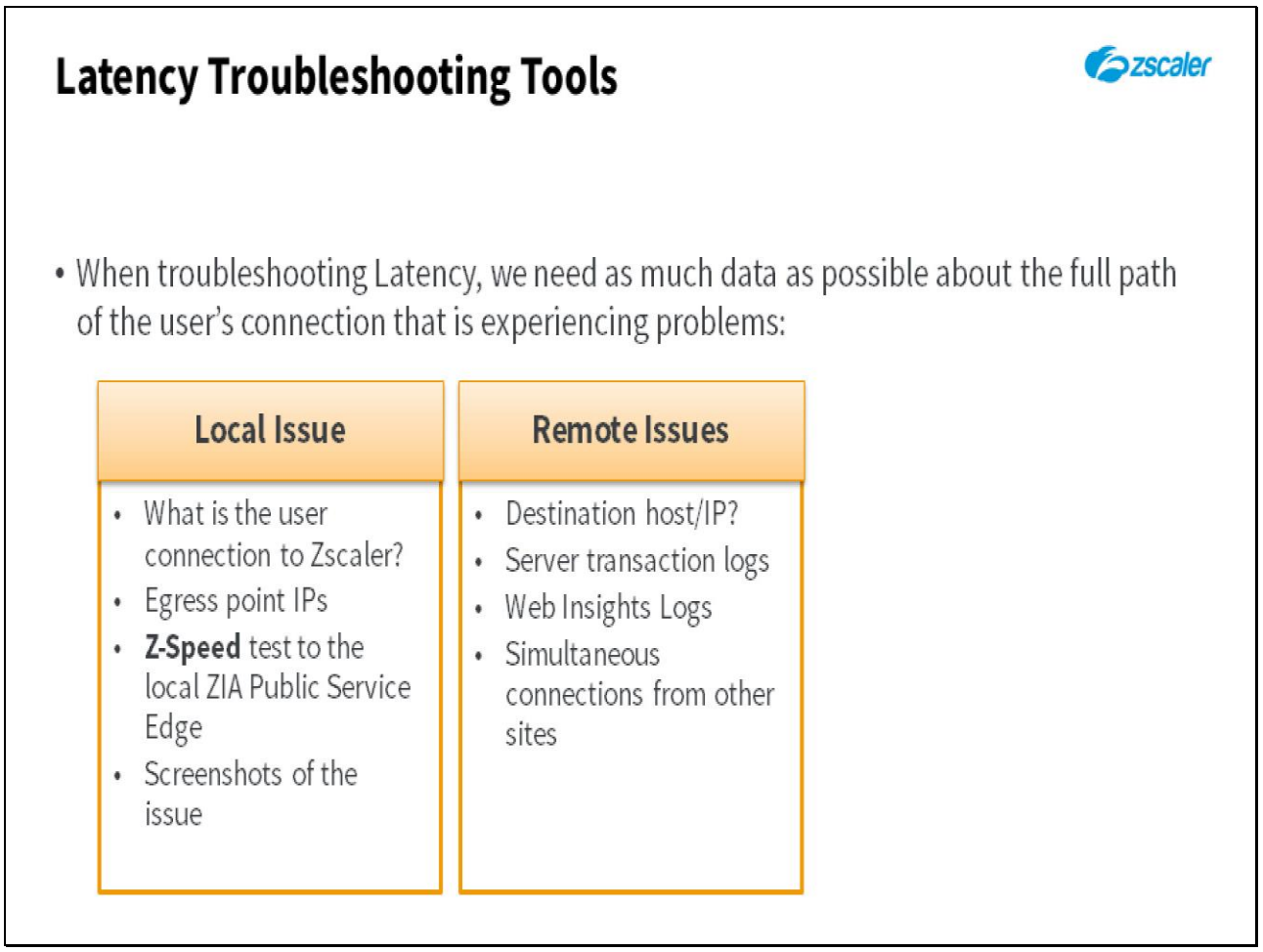



**Slide notes**

To troubleshoot potential problems with the user's local connection through Zscaler, there are a number of items that need to be checked. We will need to know what the user's connection to Zscaler is, and how is it performing.

So we will need: The output from ip.zscaler.com; the IP addresses of the user's egress point (router or firewall); the results of the connection speed test to the ZIA Public Service Edge the user connects to; and any relevant screenshots of the issue that may assist us in troubleshooting.

**Slide 42 - Latency Troubleshooting Tools**

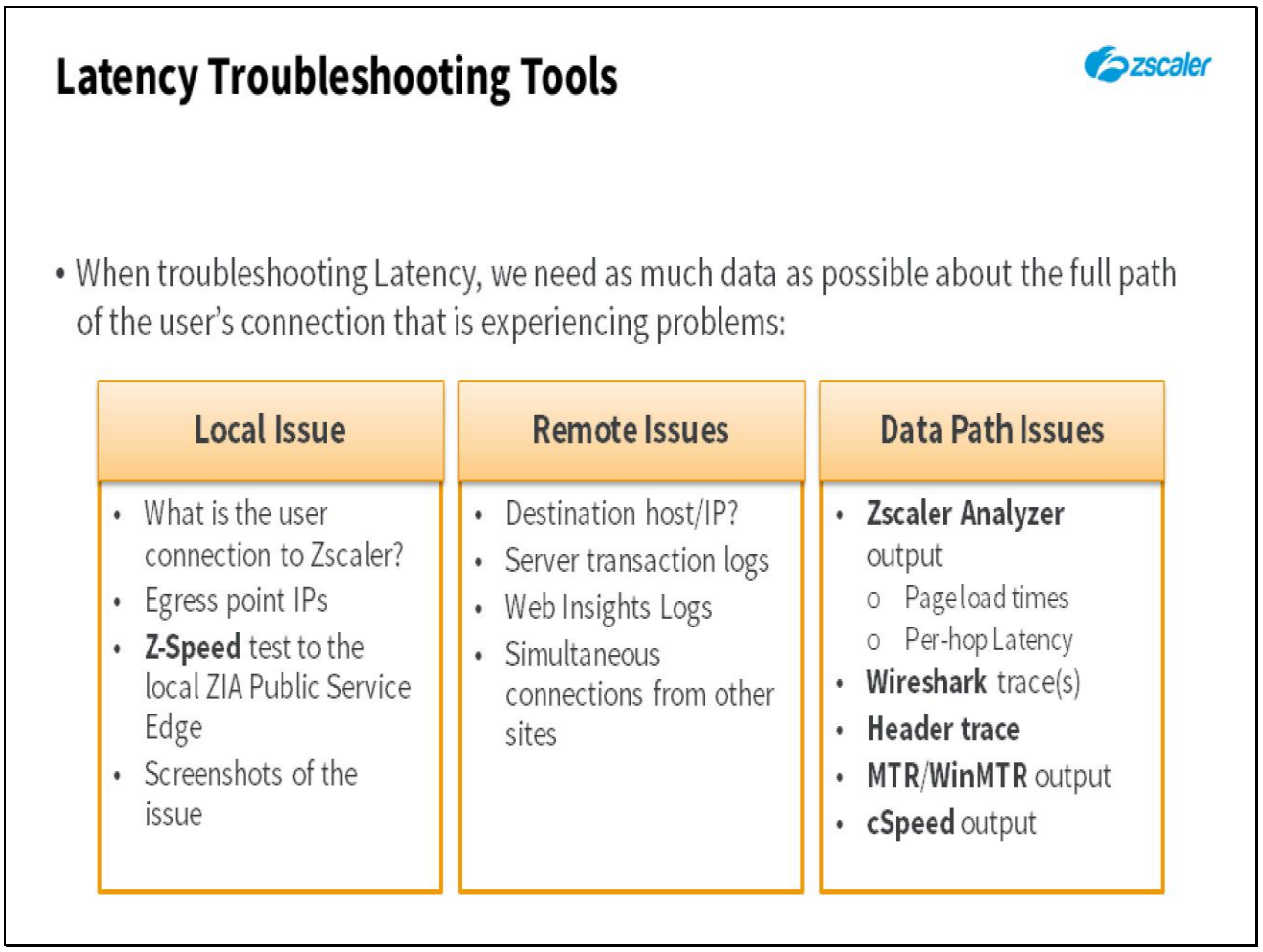



**Slide notes**

We will also require as much information as possible on the other end of the connection, the service or site that the user is connecting to, such as where is it physically located, and how is it currently performing?

To evaluate this, we will need: The destination host name or IP address of the server; if available, the server transaction logs at the time of the reported problem; extracts from the Zscaler Web Insights logs from the Admin Portal; Plus it is extremely useful to know what the situation is when accessing the destination from other locations.

**Slide 43 - Latency Troubleshooting Tools**

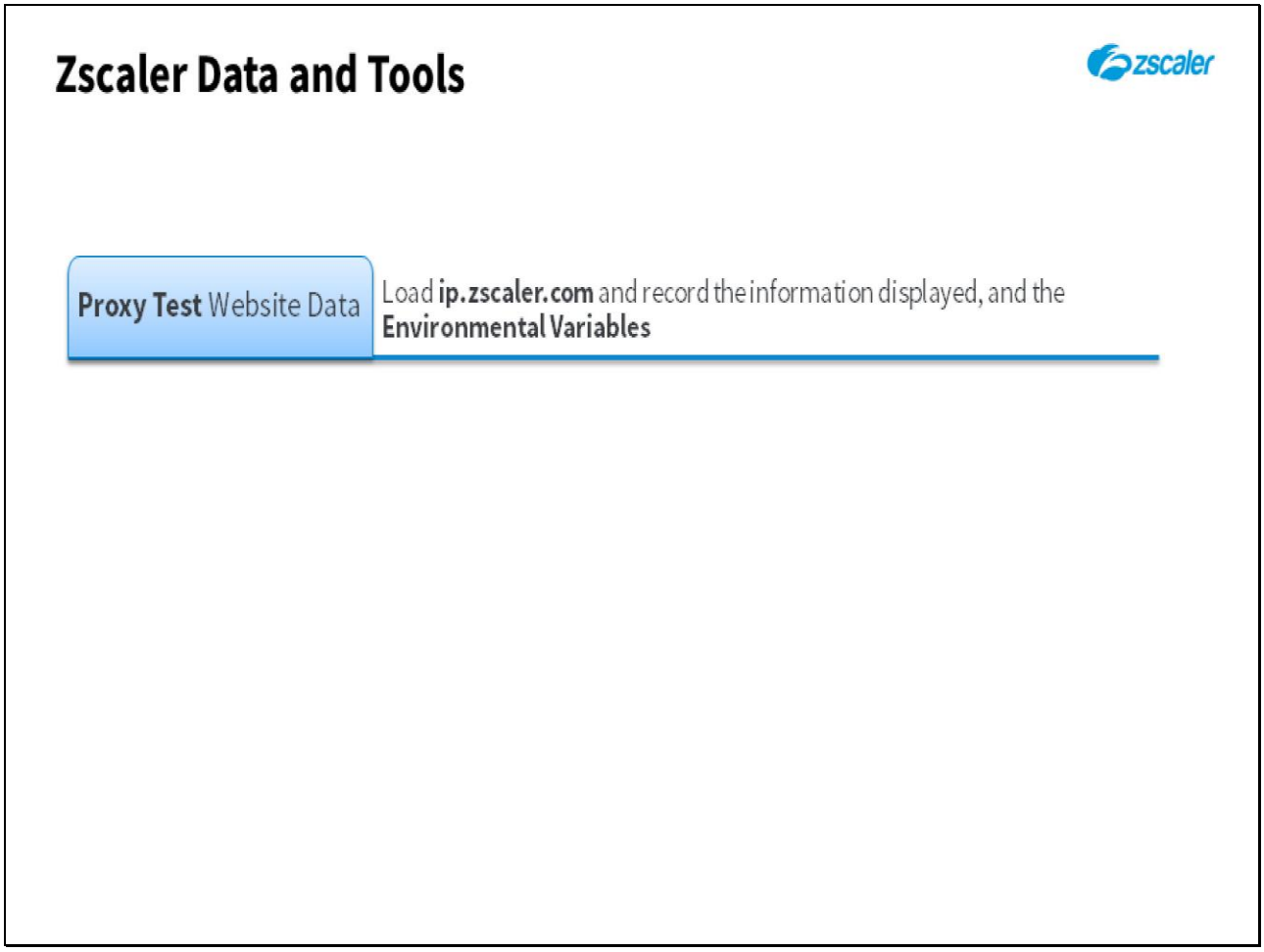



**Slide notes**

We will also need real-time data, at the time that the problem is occurring, from across the path of the data.

For example: The output from the Zscaler Analyzer tool (at intervals if necessary), specifically the Page load times, and per-hop latency recorded; a Wireshark trace on the data path; Header traces from the affected Browser; the output from MTR/WinMTR while the problem is apparent; also the output from the Chrome cSpeed plugin, if it is available.

**Slide 44 - Zscaler Data and Tools**



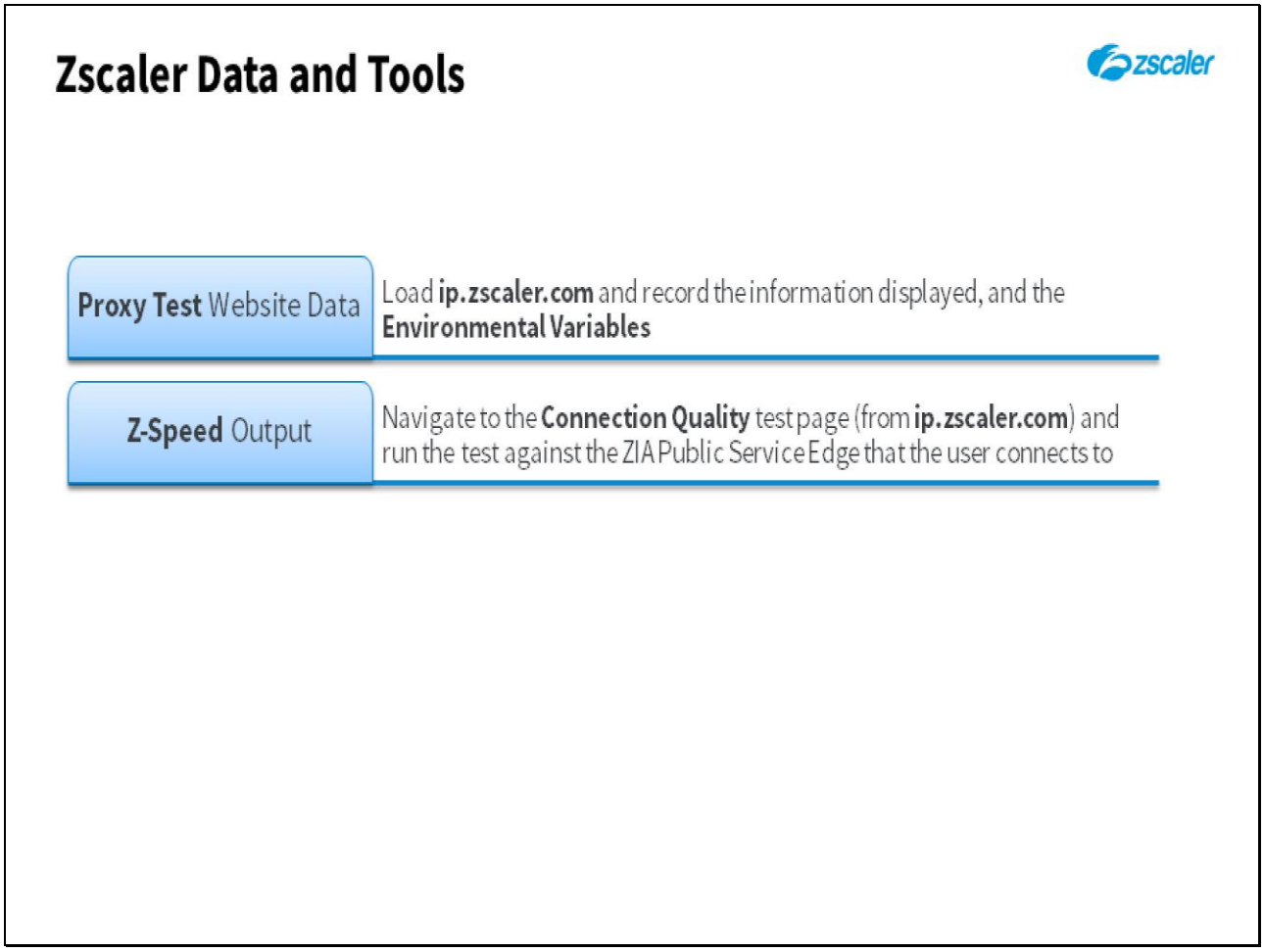

**Slide notes**

Some of the data required is static, and can simply be added to the Zscaler Ticket when it is raised, such as: the egress IP address; the destination host name or IP address; the physical locations of the user, and the server they are trying to connect to.

Other data is dynamic and may be subject to change, and you will need to use the appropriate tools to capture this data in real-time, as the problem is occurring.

Data from the Zscaler tools that we require, includes: The output from the Proxy Test Webpage at 'ip.zscaler.com'. Simply load that page from an affected device and record the content (you can copy/paste the text to a .txt file). Expand the 'Environmental Variables' section, and record that data as well.

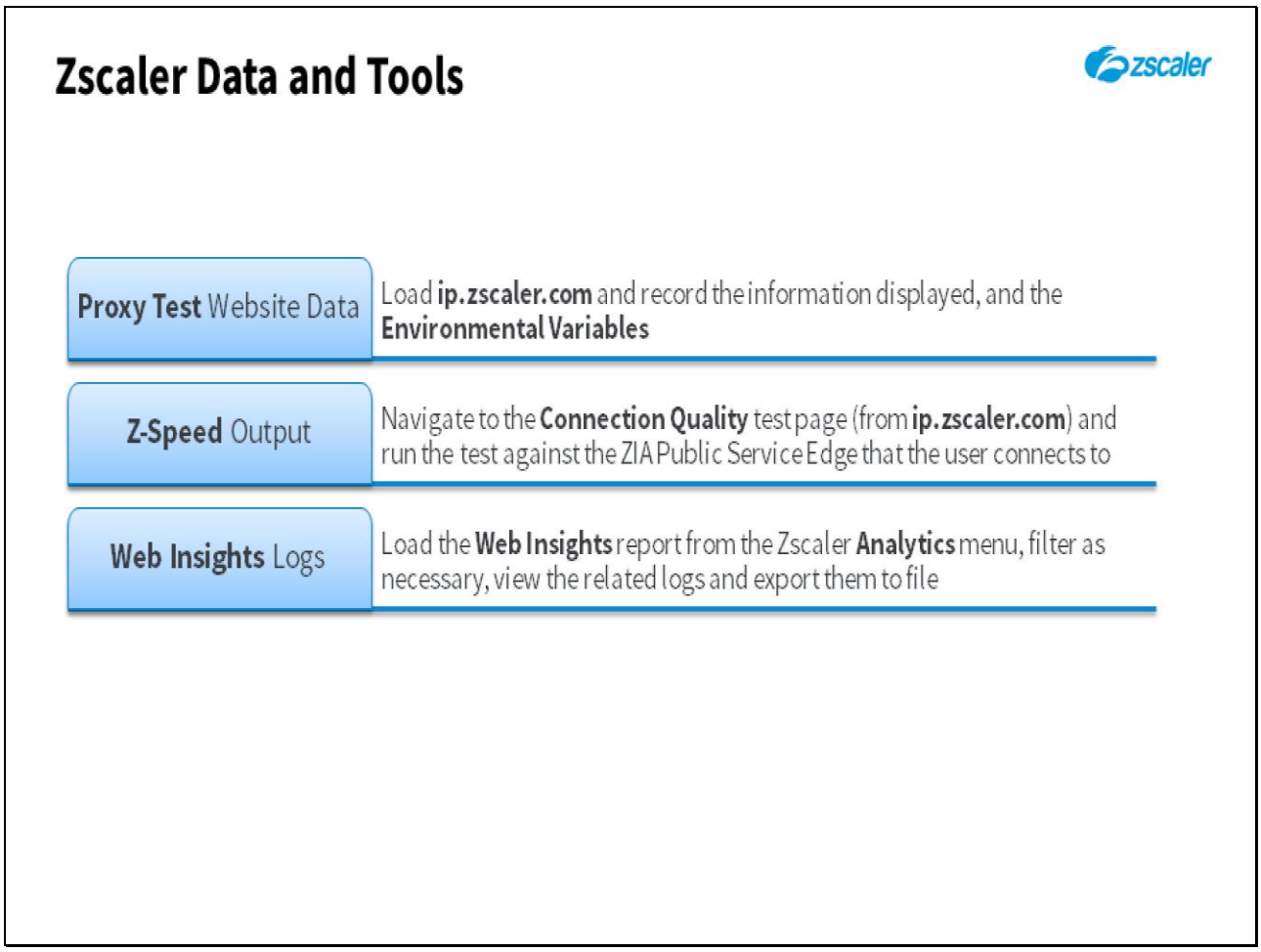
**Slide 45 - Zscaler Data and Tools**




**Slide notes**

You need to test and record the connection quality to the ZIA Public Service Edge the user is connecting through, at the time the problem is apparent. Do this by navigating to the 'Connection Quality' Web page from 'ip.zscaler.com', and running the test. The output can be saved to file for uploading to the Ticket, or for emailing to Zscaler Support.

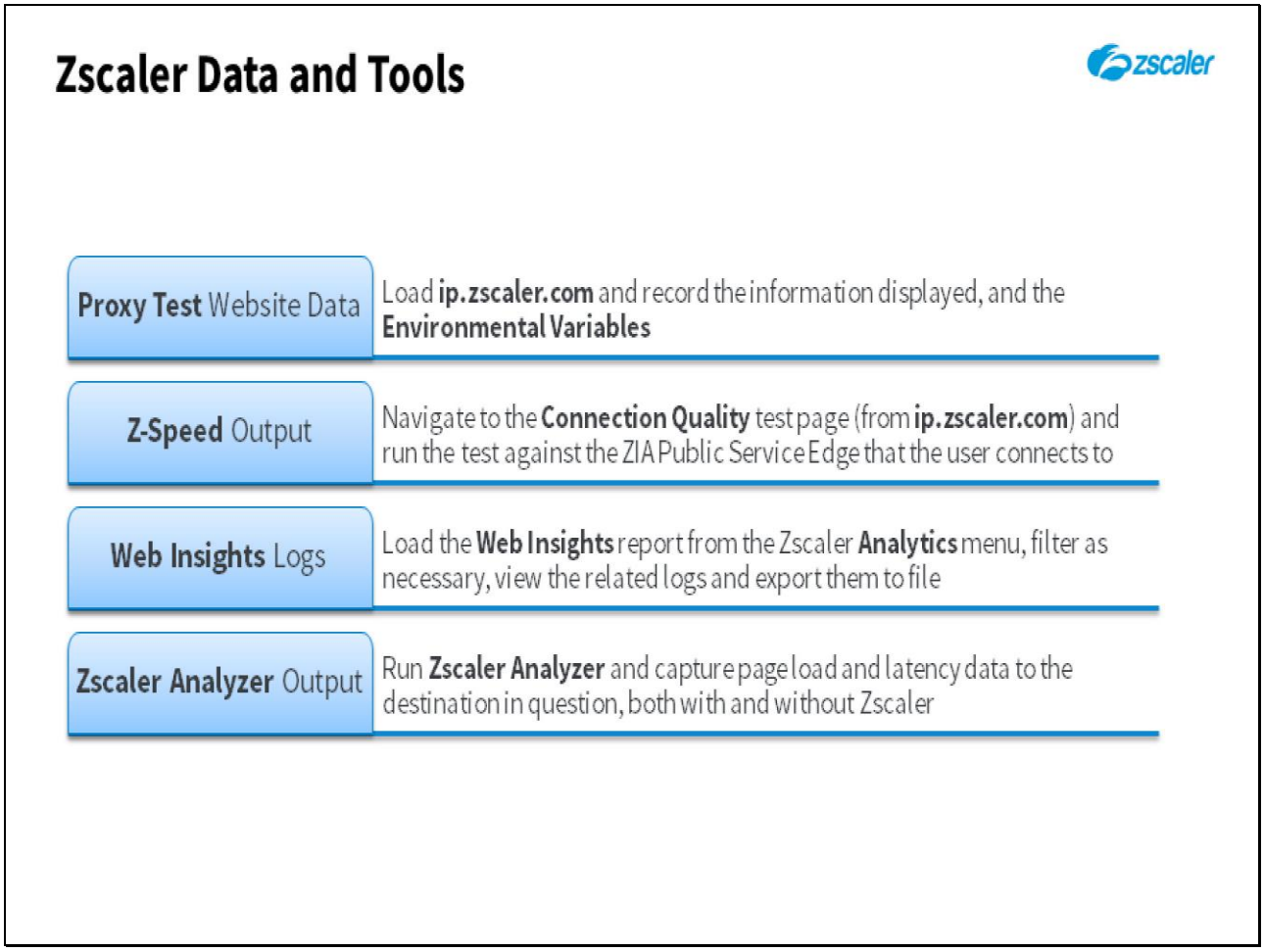
**Slide 46 - Zscaler Data and Tools**




**Slide notes**

It may be useful to correlate the logs from the Zscaler Web Insights report, for the times that the problem is apparent. To do this, load the 'Web Insights' report from the Zscaler **Analytics** menu, add an appropriate set of filters, then click on the chart and select the **View Logs** option. Once the logs are displayed, you have the option to save them to file for upload to the Zscaler Ticket, or to email to Support.

**Slide 47 - Zscaler Data and Tools**

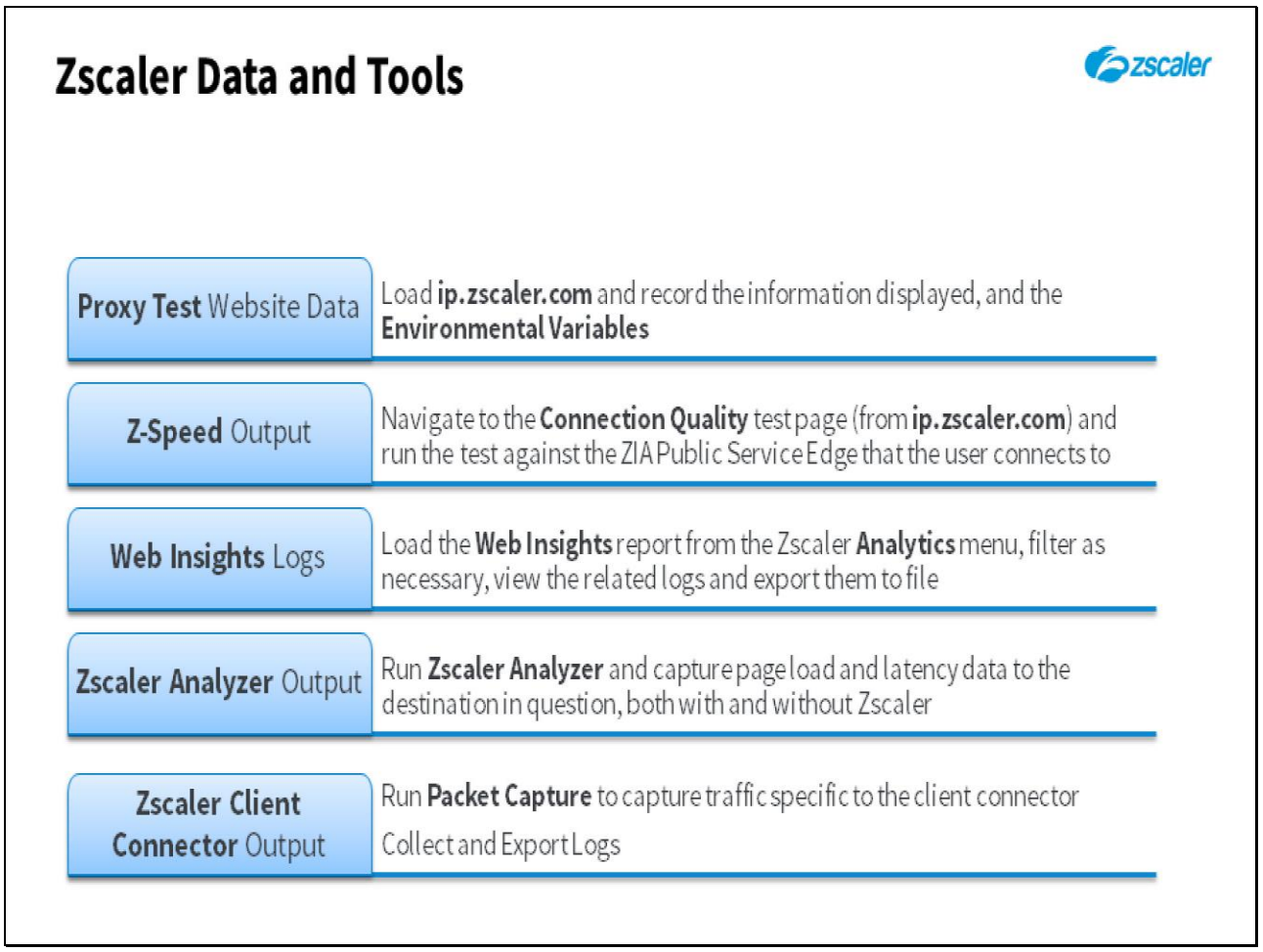



**Slide notes**

The Zscaler Analyzer is a tool that you must download and install on an affected end user device, it is available through the 'ip.zscaler.com' page. Download the appropriate version and install it, then run a test using the tool targeted at the specific destination server or service that is showing the problem, both when connecting through Zscaler, and when going direct. Output from the tool can be saved to file for upload onto the Zscaler Ticket, or to email to Support, you can even set the tool to run automatically at intervals.

Note that this tool does require some familiarity in order to get the best results, the detailed use of this tool is beyond the scope of this module.

**Slide 48 - Zscaler Data and Tools**

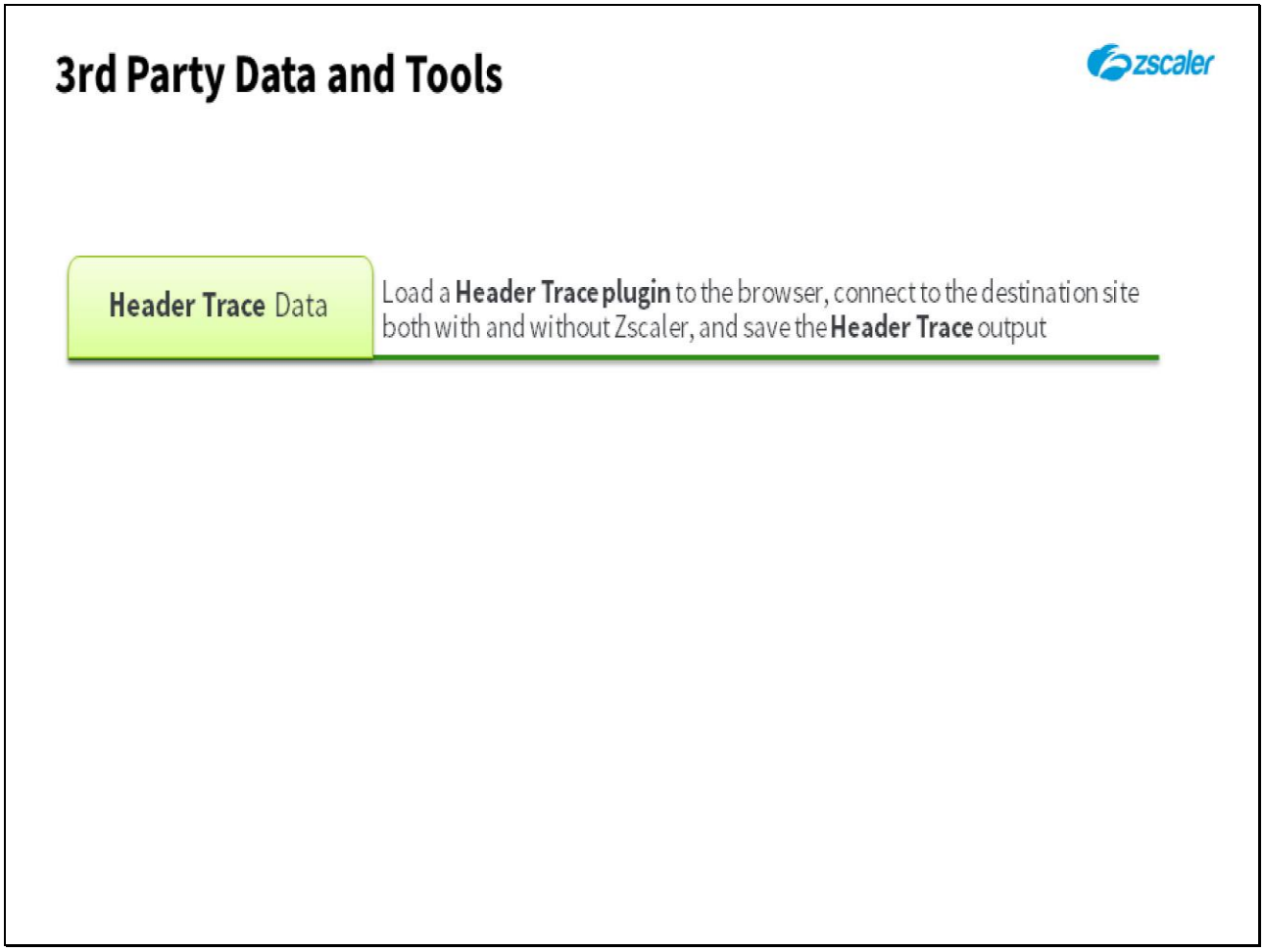



**Slide notes**

Is enabled in the Zscaler Client Connector portal, you can use the **Start Packet Capture** option to capture traffic specific to the client connector. This option is available under the Client Connector's **More** tab.

You can also change the mode in which Zscaler Client Connector generates logs and export the logs.

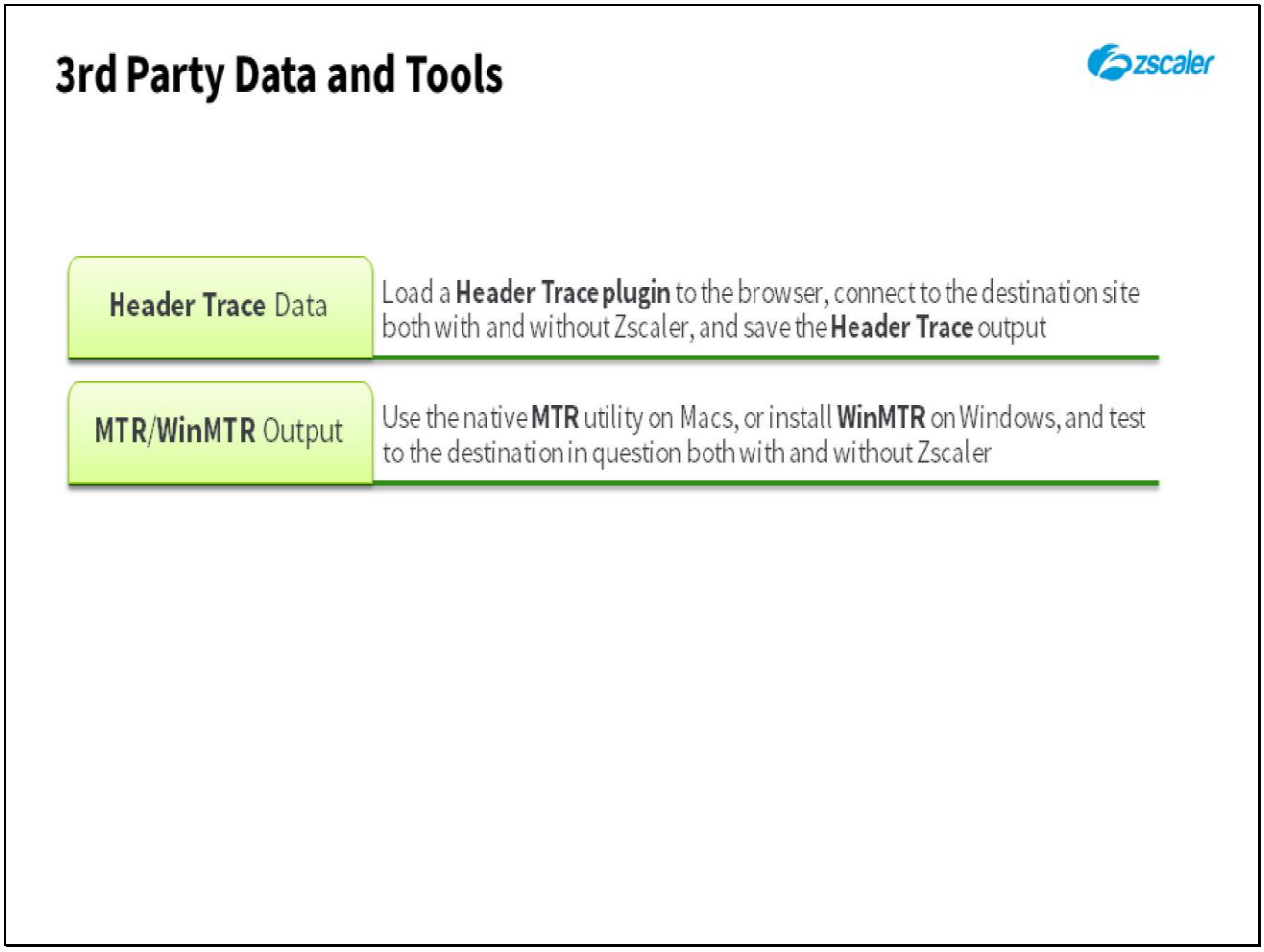
**Slide 49 - 3rd Party Data and Tools**




**Slide notes**

Real-time performance data can also be captured by 3rd party tools, to assist in troubleshooting latency issues, for example: A ‘Header Trace’ plug-in can be installed to the Browser on an affected device, and traces captured when accessing the problematic destination, both when connecting through Zscaler, and when going direct. Data from these plug-ins can be saved to file for upload to the Zscaler Ticket, or to email to Support.

**Slide 50 - 3rd Party Data and Tools**

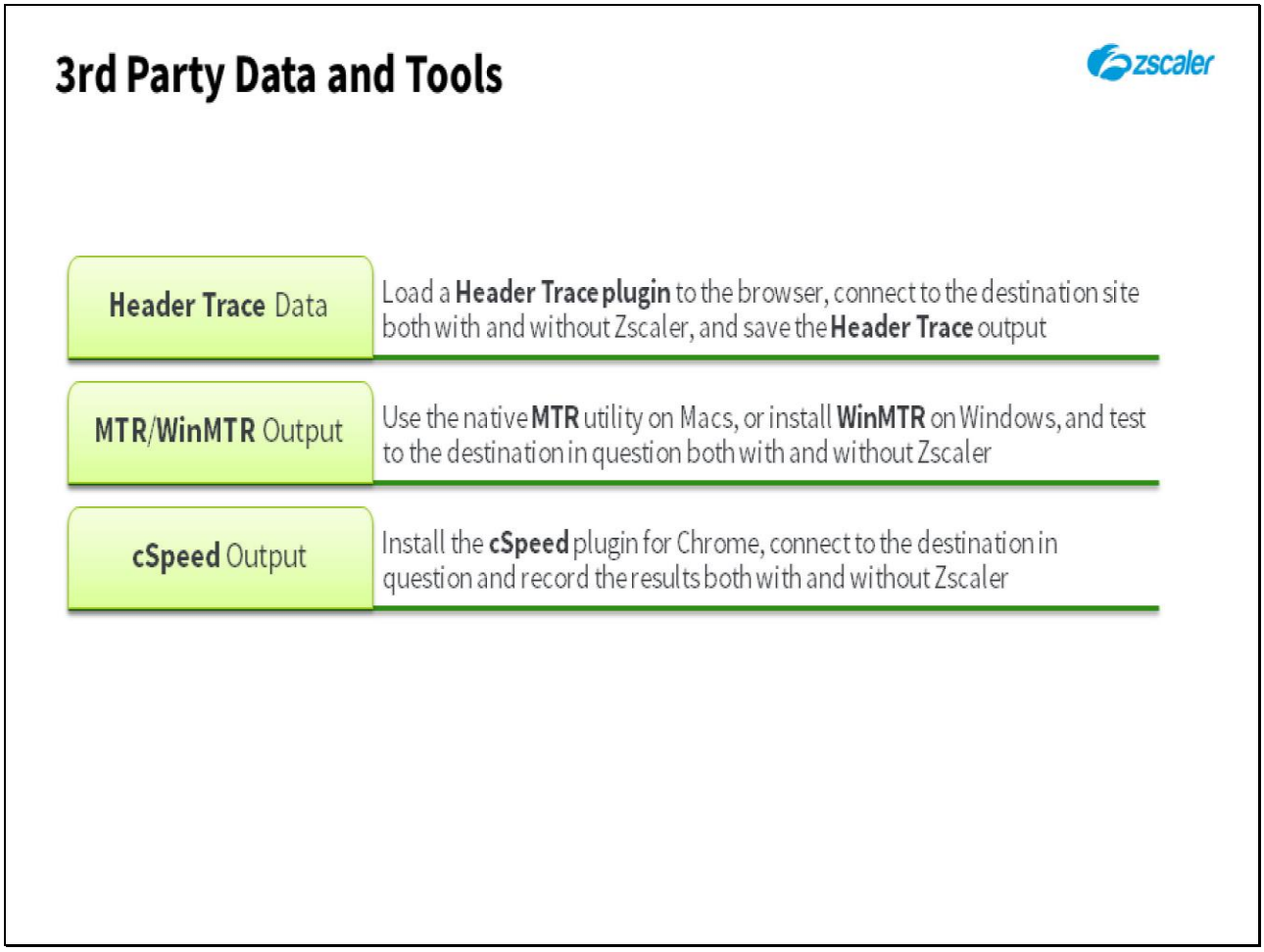



**Slide notes**

A native command line utility on Macs is a tool called **MTR**, which provides a combination of 'ping' and 'traceroute' output. There is a 3rd party Windows equivalent known as **WinMTR**, that can be downloaded and installed on an affected Windows device.

Run the tool when the problem is apparent, both with and without Zscaler, and save the data to file for uploading to the Ticket, or emailing to Support.

**Slide 51 - 3rd Party Data and Tools**

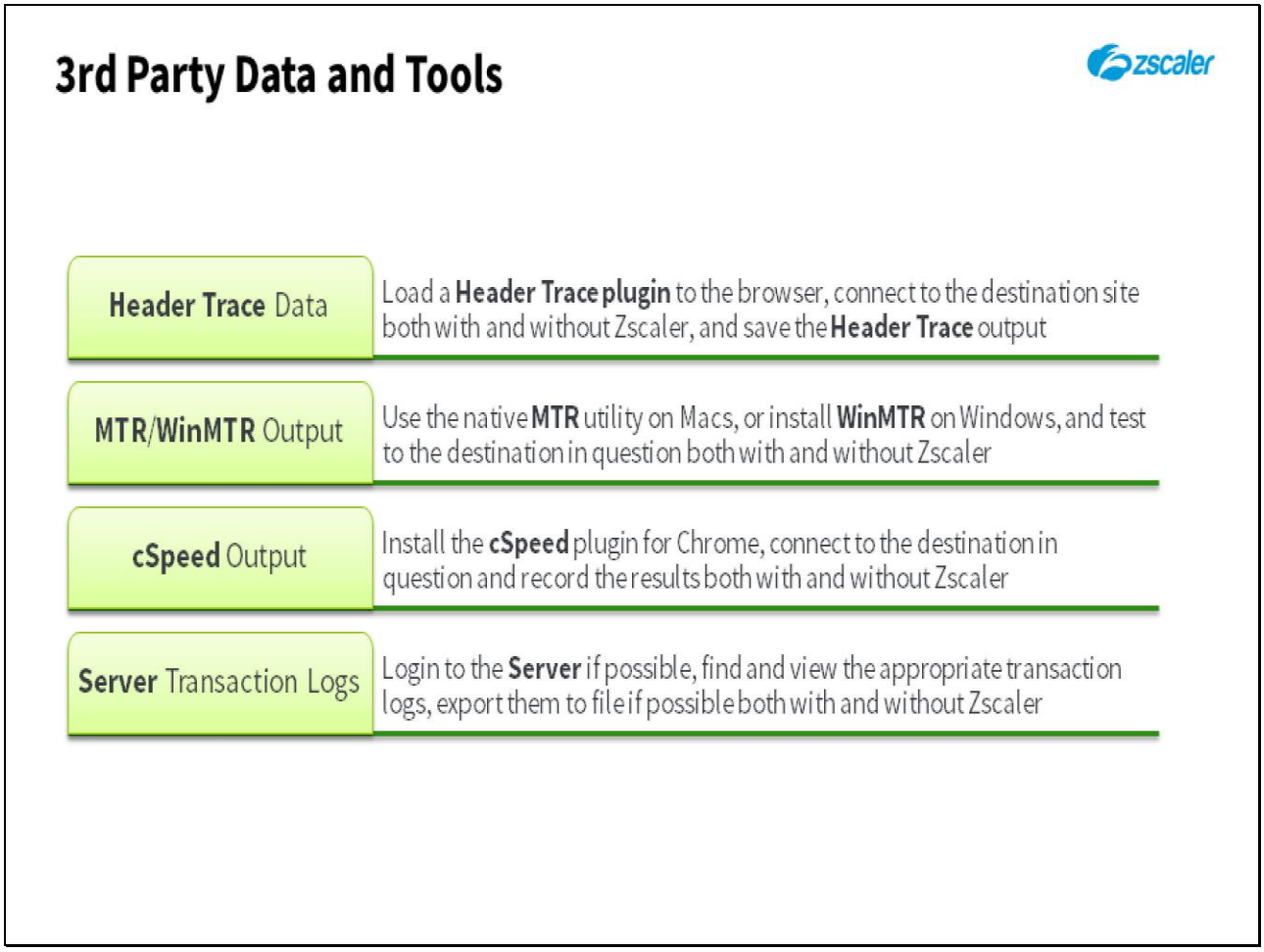



**Slide notes**

**cSpeed** is a plugin for the Chrome Browser that can provide useful insights to a potential latency issue.

If Chrome is available, download and install the plug-in, then use it while connecting to the problematic site, both with, and without Zscaler, and record the results. Save the data to file and make it available to Zscaler Support.

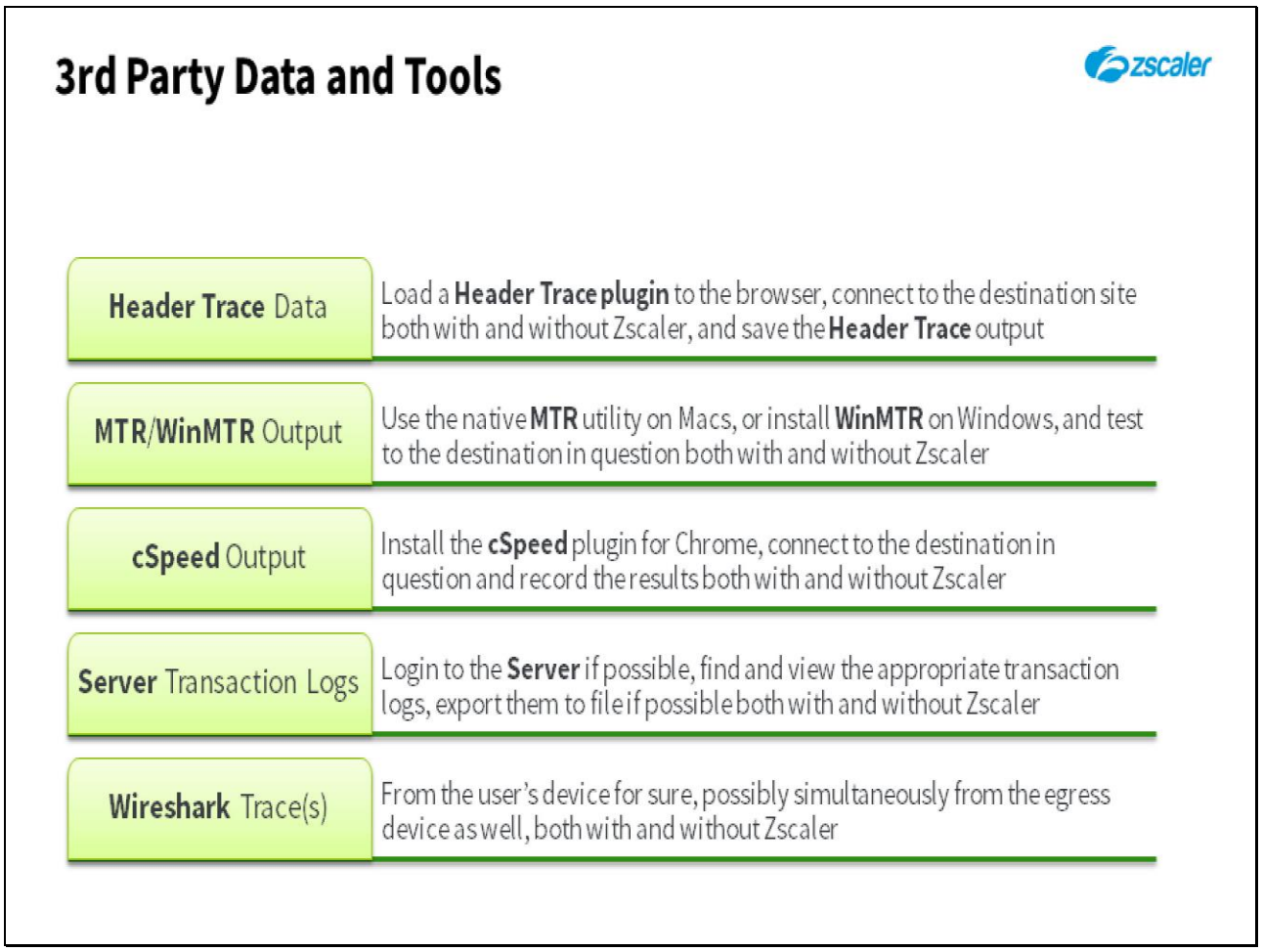
**Slide 52 - 3rd Party Data and Tools**




**Slide notes**

If you have access to the destination server, and can view, or better yet, download transaction logs from it, this will provide extremely useful data for Zscaler Support. If this is possible, save the logs while the problem is apparent, both when connecting through Zscaler, and going direct. Save the logs and make them available to Zscaler Support.

**Slide 53 - 3rd Party Data and Tools**

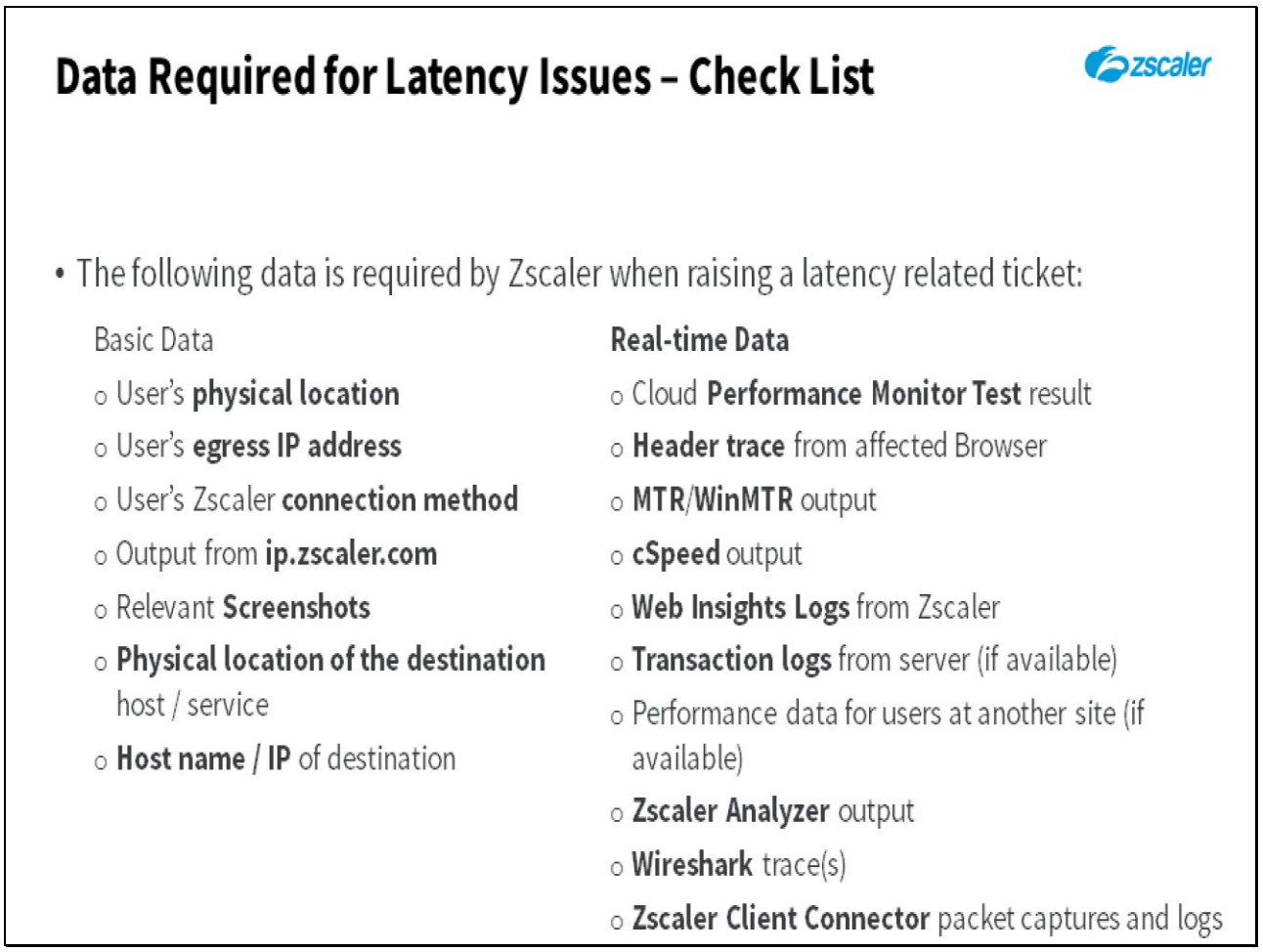



**Slide notes**

Taking a 'Wireshark' trace (or equivalent Protocol Analyzer tool), should be a last resort, as this kind of tool can be very complicated and time consuming to deploy. You may need to take traces in multiple locations simultaneously, to allow us to correlate the output with traces we take internally at the same time.

It may be sufficient to take a trace on an affected device while the problem is present, both going through Zscaler, and going direct. We may request that you trace simultaneously on the affected device, and at the egress gateway device, to allow us to better troubleshoot the problem. Of course, you will need to save the traces to file for upload or email to Zscaler Support.

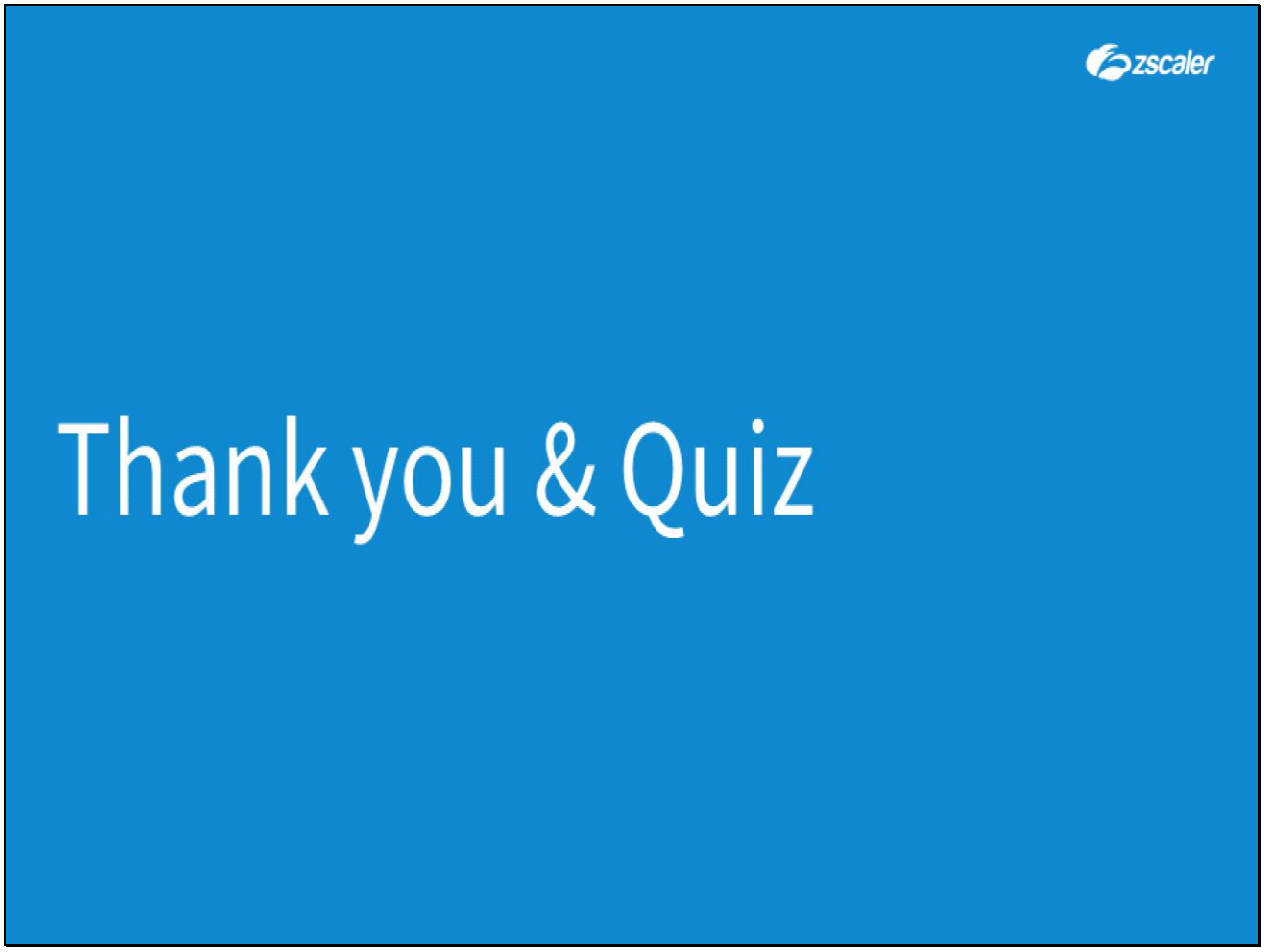
**Slide 54 - Data Required for Latency Issues – Check List**




**Slide notes**

Finally, here is a check list of the data items that we will require from you, when raising a latency-related support ticket.

**Slide 55 - Thank you & Quiz**




**Slide notes**

Thank you for following this training module on localizing problems with Zscaler Internet Access. 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.