

Slide 1 - Troubleshooting ZPA



Troubleshooting ZPA

Problem Localization

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on localizing problems when troubleshooting end user ZPA connectivity issues.

Slide 2 - Navigating the eLearning Module

Navigating the eLearning Module

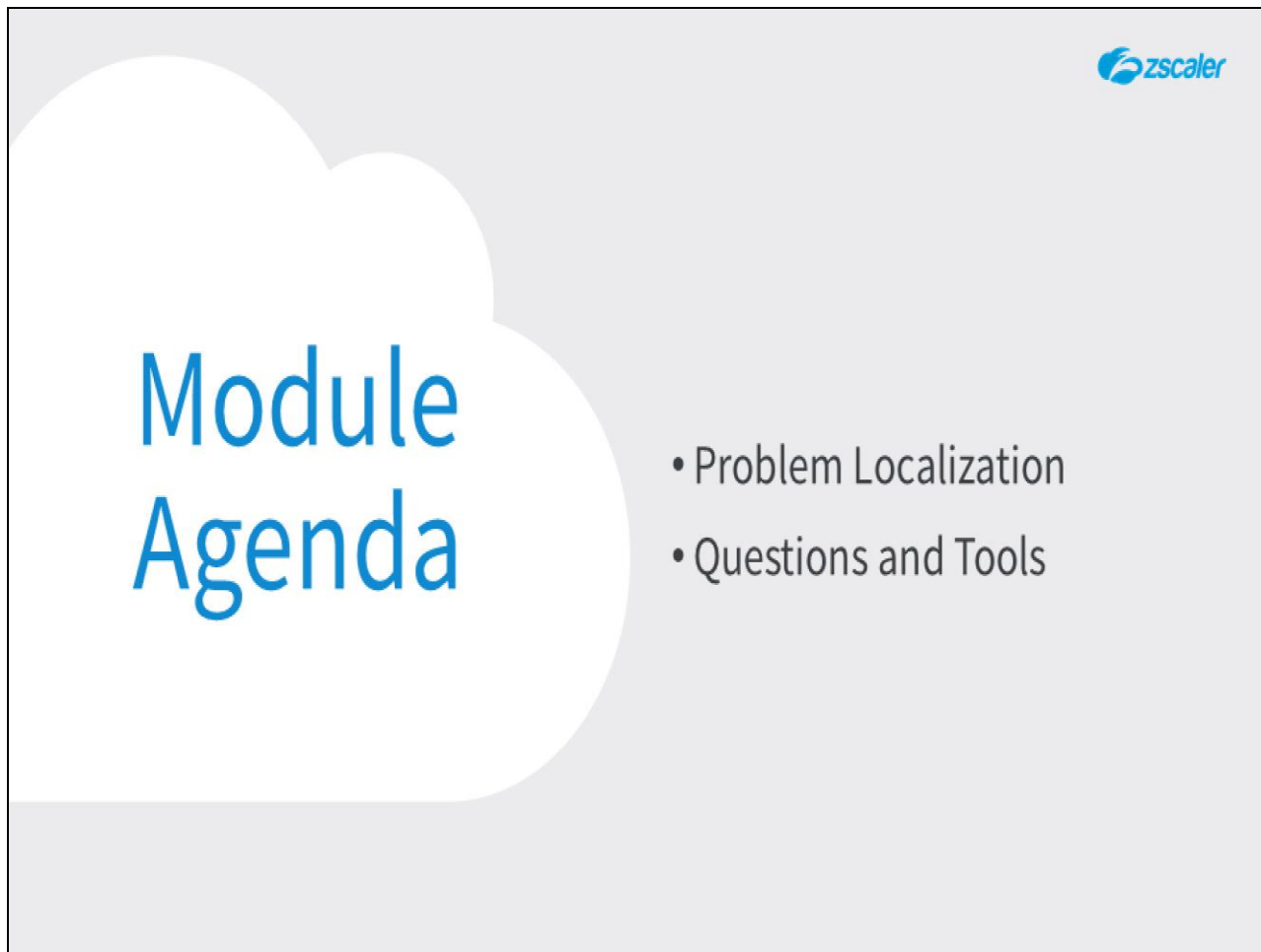
The screenshot displays the Zscaler ZPA Basic Administration dashboard. The dashboard includes a sidebar with navigation links: Dashboard, Diagnostics, Live Logs, Administration, and Search. The main content area shows four summary cards: Applications Accessed (15), Discovered Applications (3), Access Policy Blocks (0), and Successful Transactions (884). Below these are two tables: 'Applications Accessed' and 'Top Applications by Bandwidth'. The 'Applications Accessed' table lists applications like '172.20.0.26', 'qa.gl.local', 'crm.gl.local', 'intranet.gl.local', and 'server01.safemarch.com'. The 'Top Applications by Bandwidth' table lists applications like 'vcenter.lab.safemarch.com', 'glab.safemarch.com', 'crm.safemarch.com', 'w10a.safemarch.com', 'splunk.tn.zscaler.com', 'intranet.gl.local', 'intranet.safemarch.local', 'splunk.safemarch.com', 'server01.safemarch.com', and 'crm.gl.local'. At the bottom, there are sections for 'TOP ERROR', 'TOP POLICY BLOCKS', and 'Access Policy Blocks'. Navigation callouts are present: 'Exit' (top right), 'Previous Slide' (left), 'Next Slide' (right), 'Play/Pause' (bottom left), 'Progress Bar' (bottom center), 'Audio On/Off' (bottom 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**, 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

The slide features a light gray background with a large white cloud shape on the left. Inside the cloud, the words "Module Agenda" are written in a large, blue, sans-serif font. To the right of the cloud, there is a bulleted list with two items: "• Problem Localization" and "• Questions and Tools". In the top right corner of the slide, the Zscaler logo is displayed, consisting of a blue circular icon followed by the word "zscaler" in a blue, lowercase, sans-serif font.

Module Agenda

- Problem Localization
- Questions and Tools

Slide notes

In this module, we will cover: The process of localizing a problem to identify the failure domain; and the questions and tools that can help to narrow down the precise location of a problem.

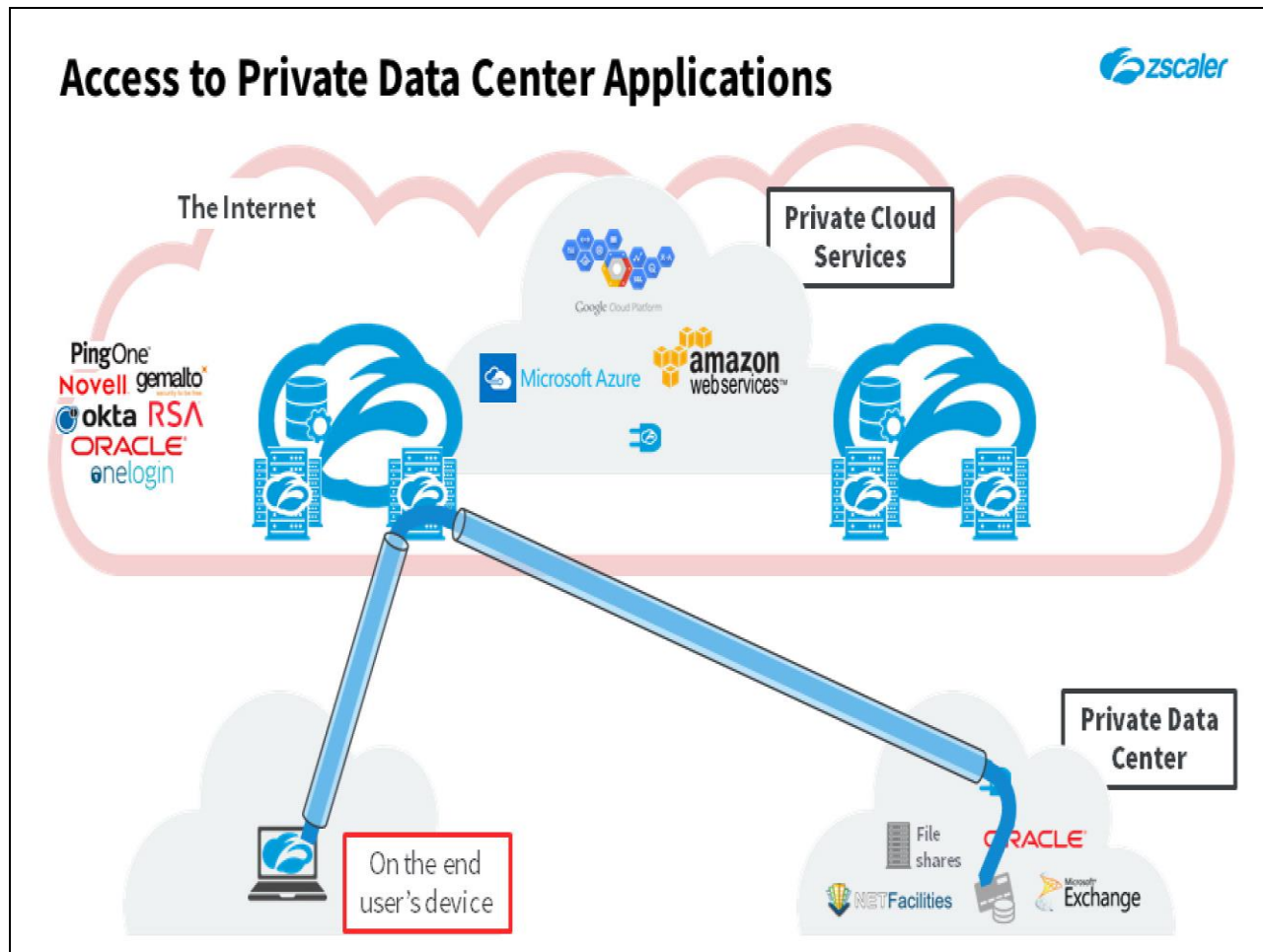
Slide 4 - Problem Localization



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.

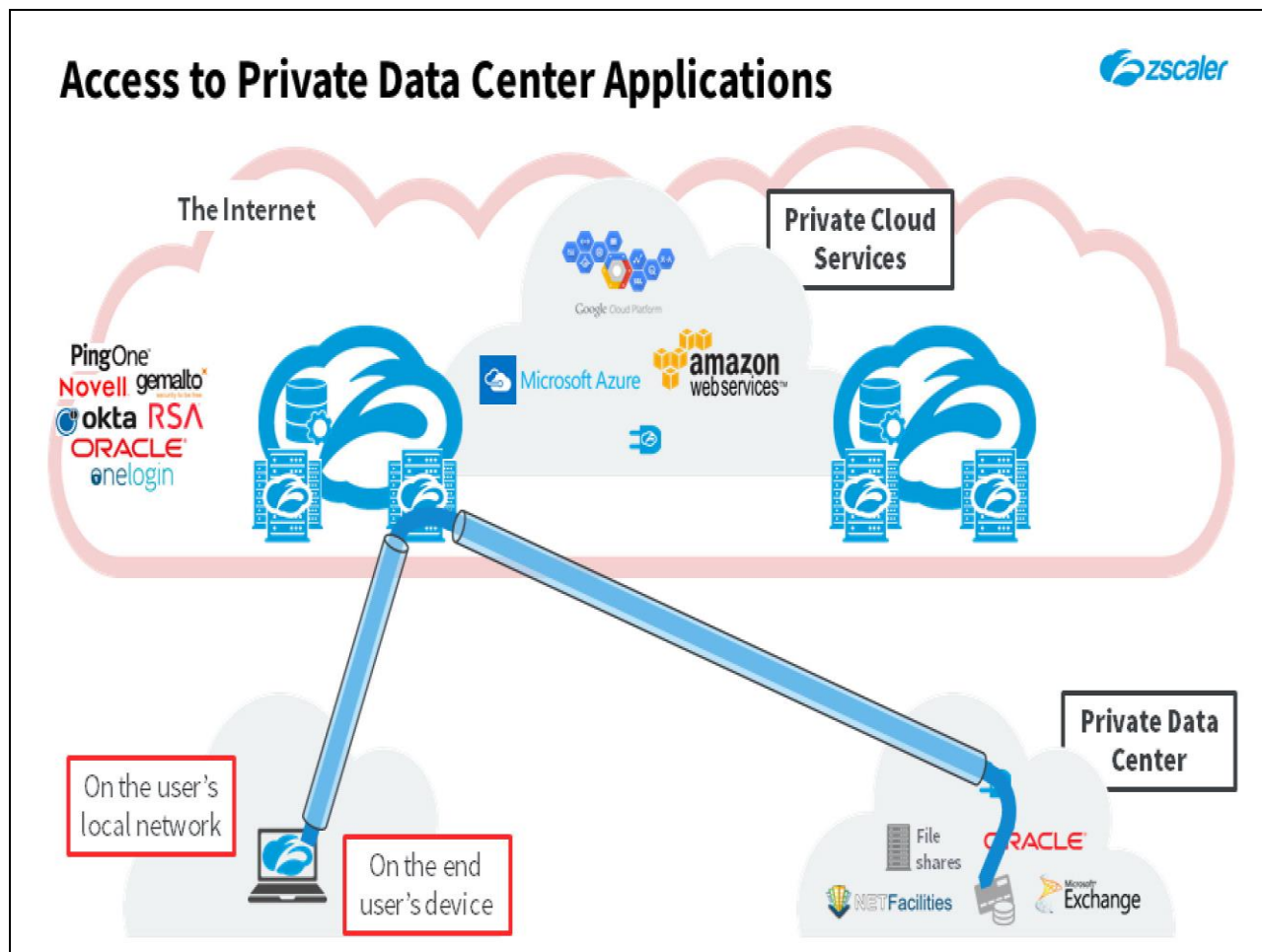
Slide 5 - Access to Private Data Center Applications



Slide notes

With the Zscaler Private 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 related, or with the Zscaler Client Connector.

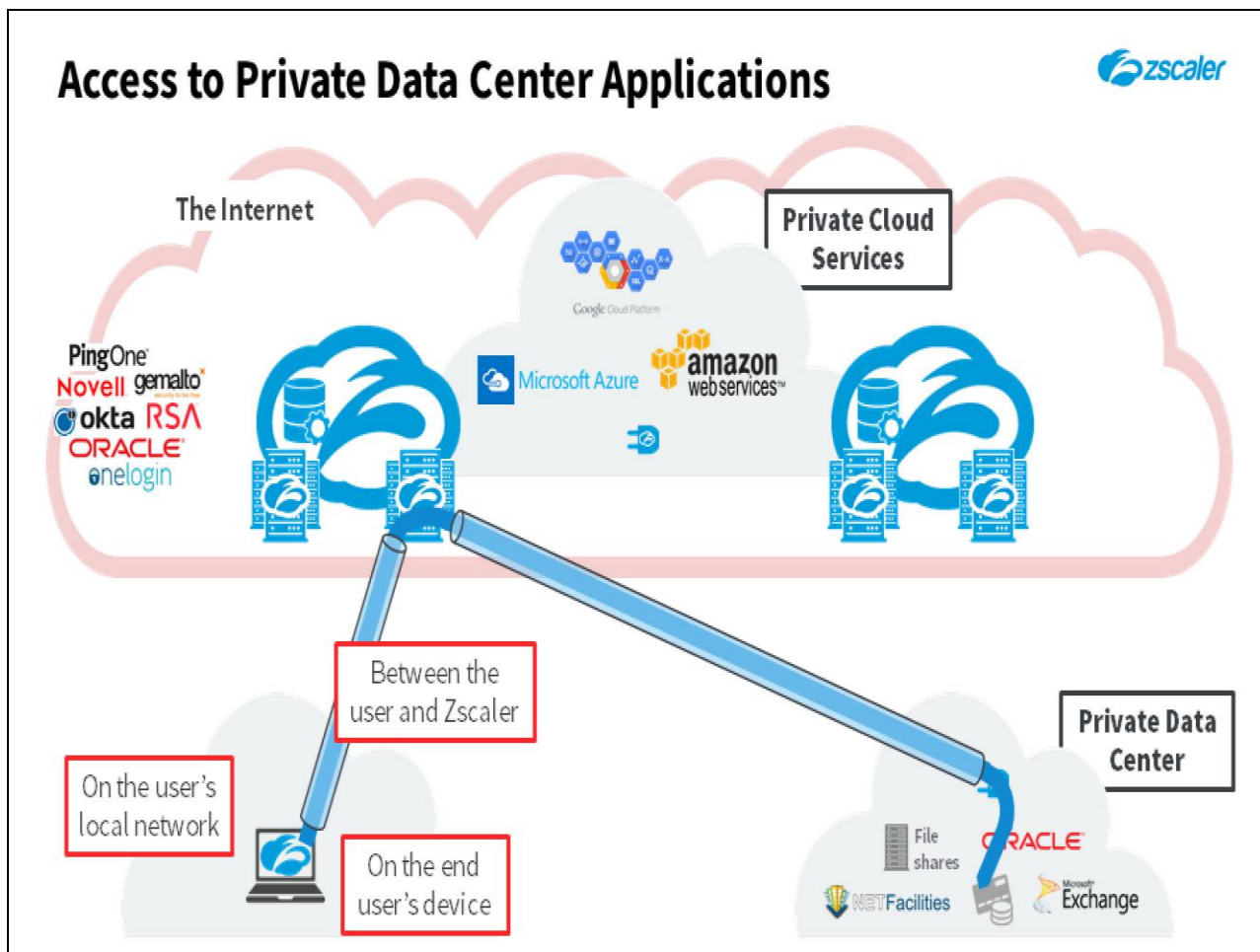
Slide 6 - Access to Private Data Center Applications



Slide notes

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

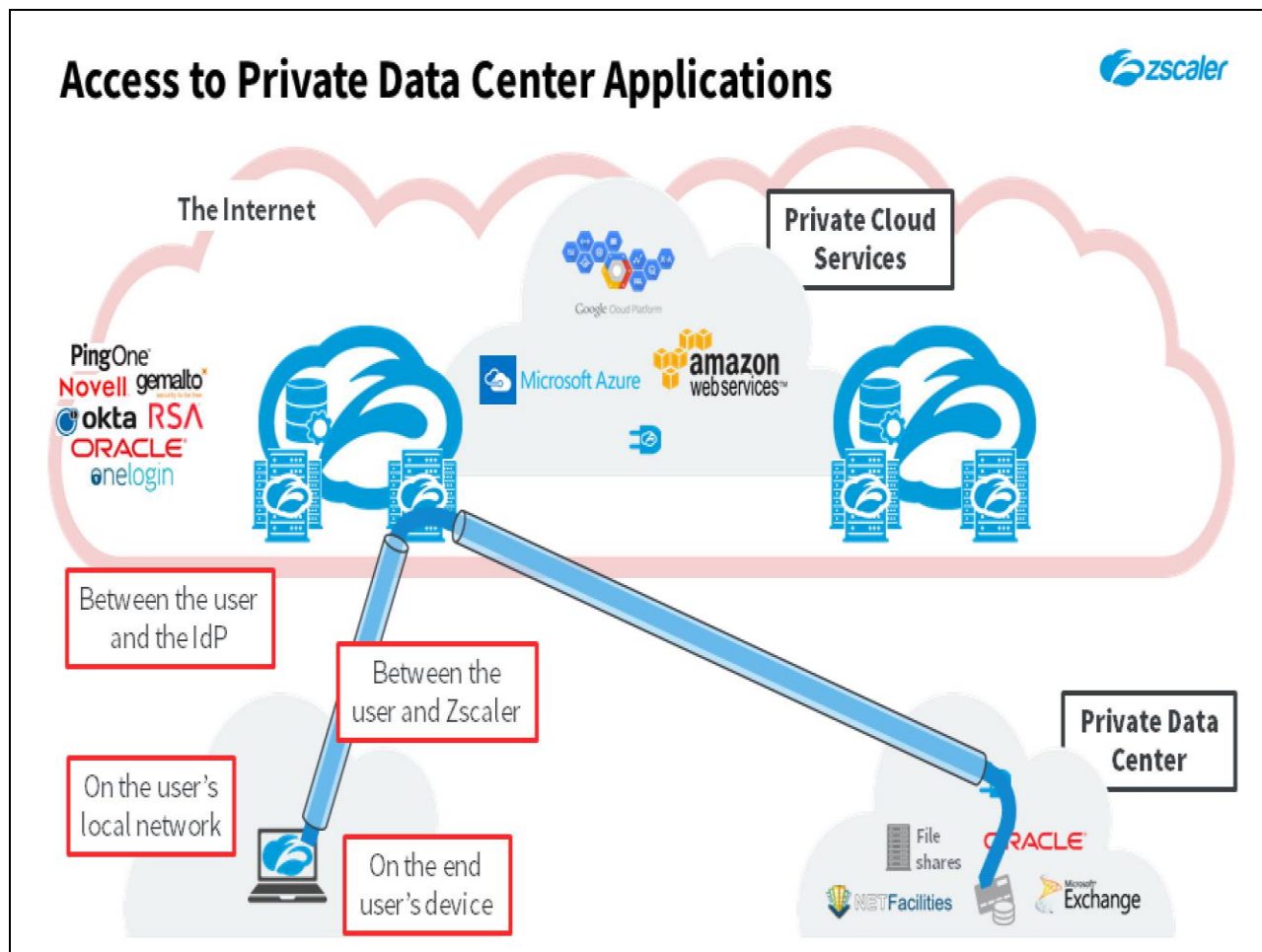
Slide 7 - Access to Private Data Center Applications



Slide notes

There may be problems between the end user's device and Zscaler.

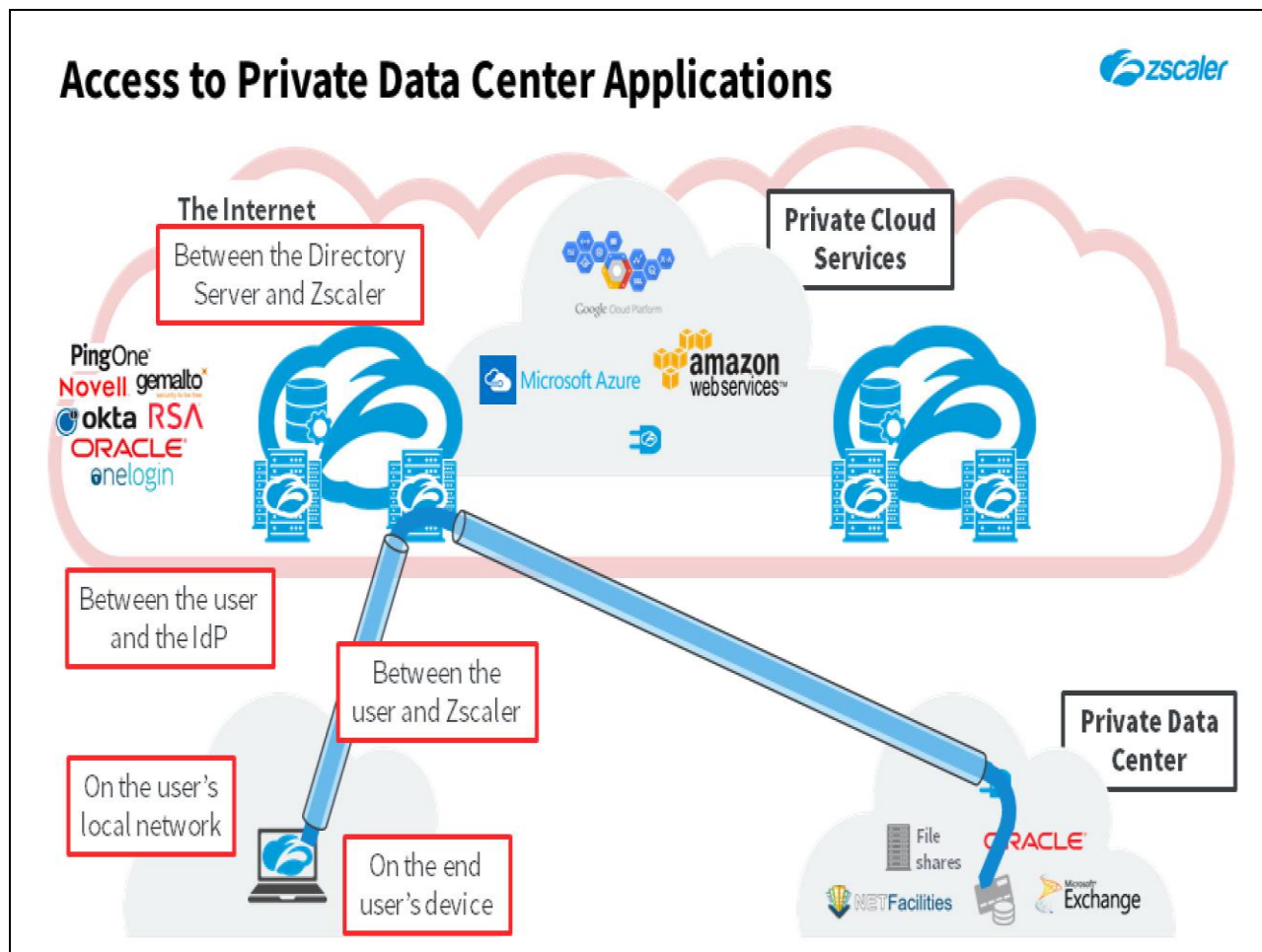
Slide 8 - Access to Private Data Center Applications



Slide notes

There may be problems on the connection between the end user and the authentication service or IdP.

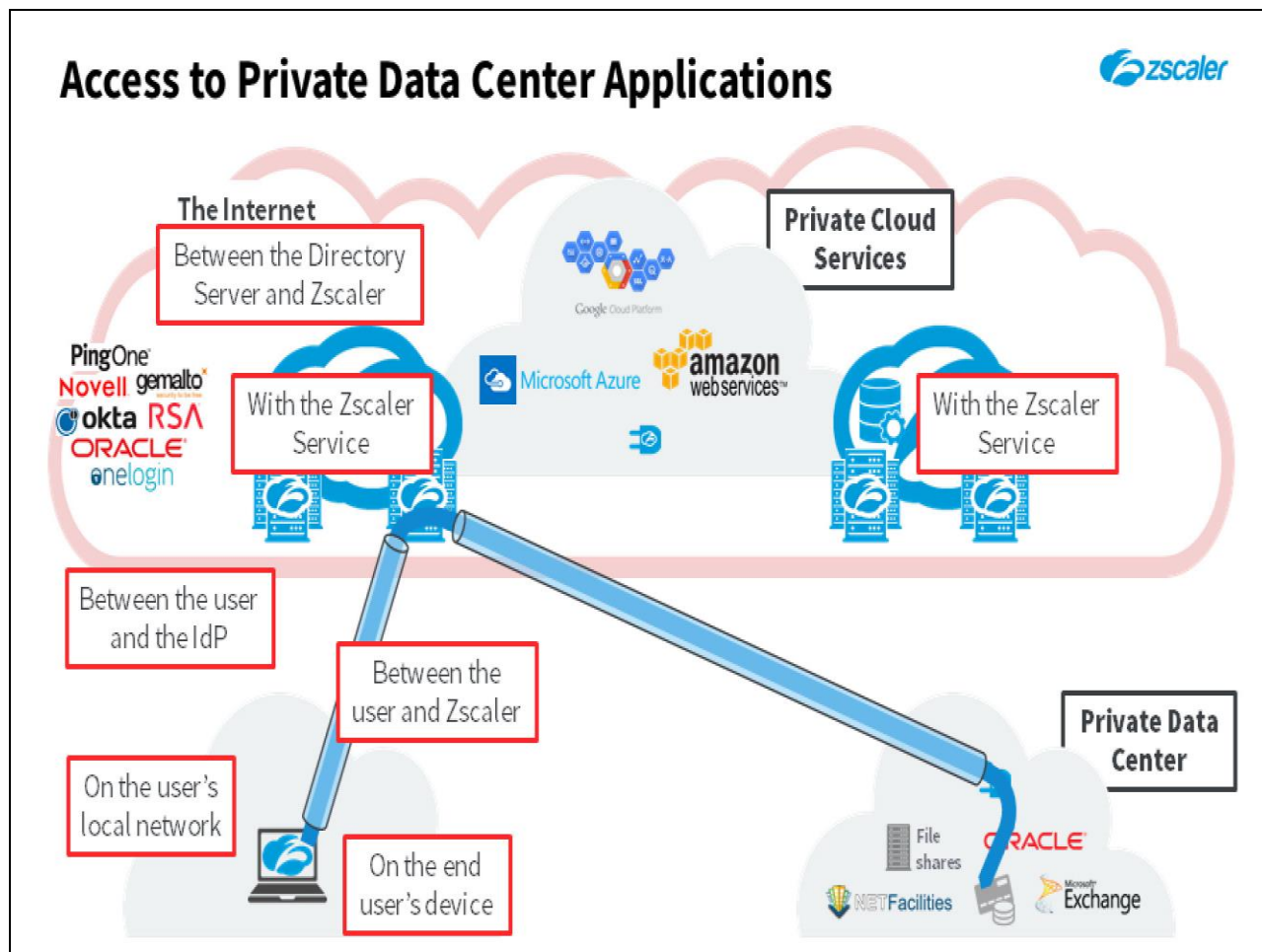
Slide 9 - Access to Private Data Center Applications



Slide notes

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

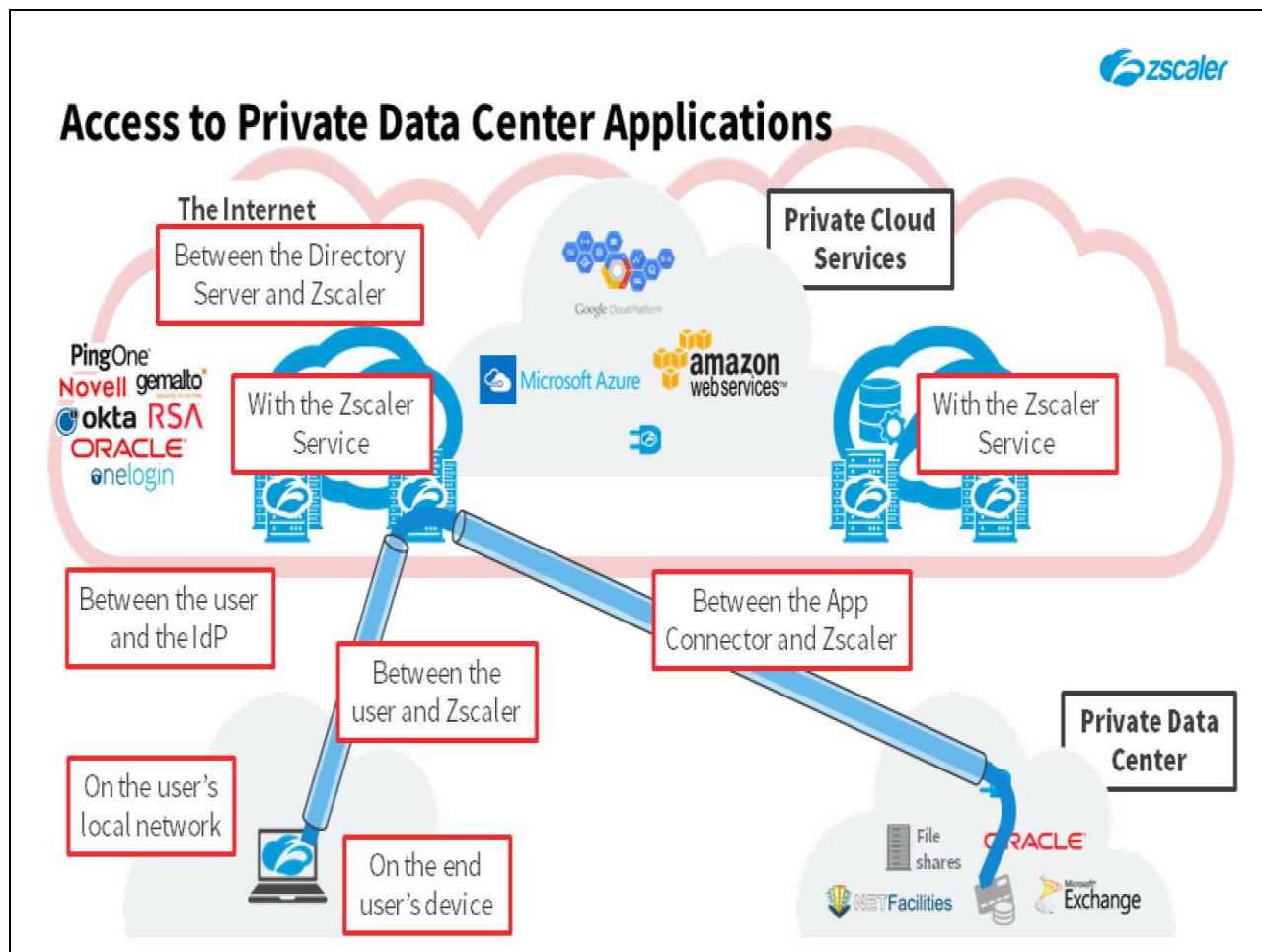
Slide 10 - Access to Private Data Center Applications



Slide notes

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

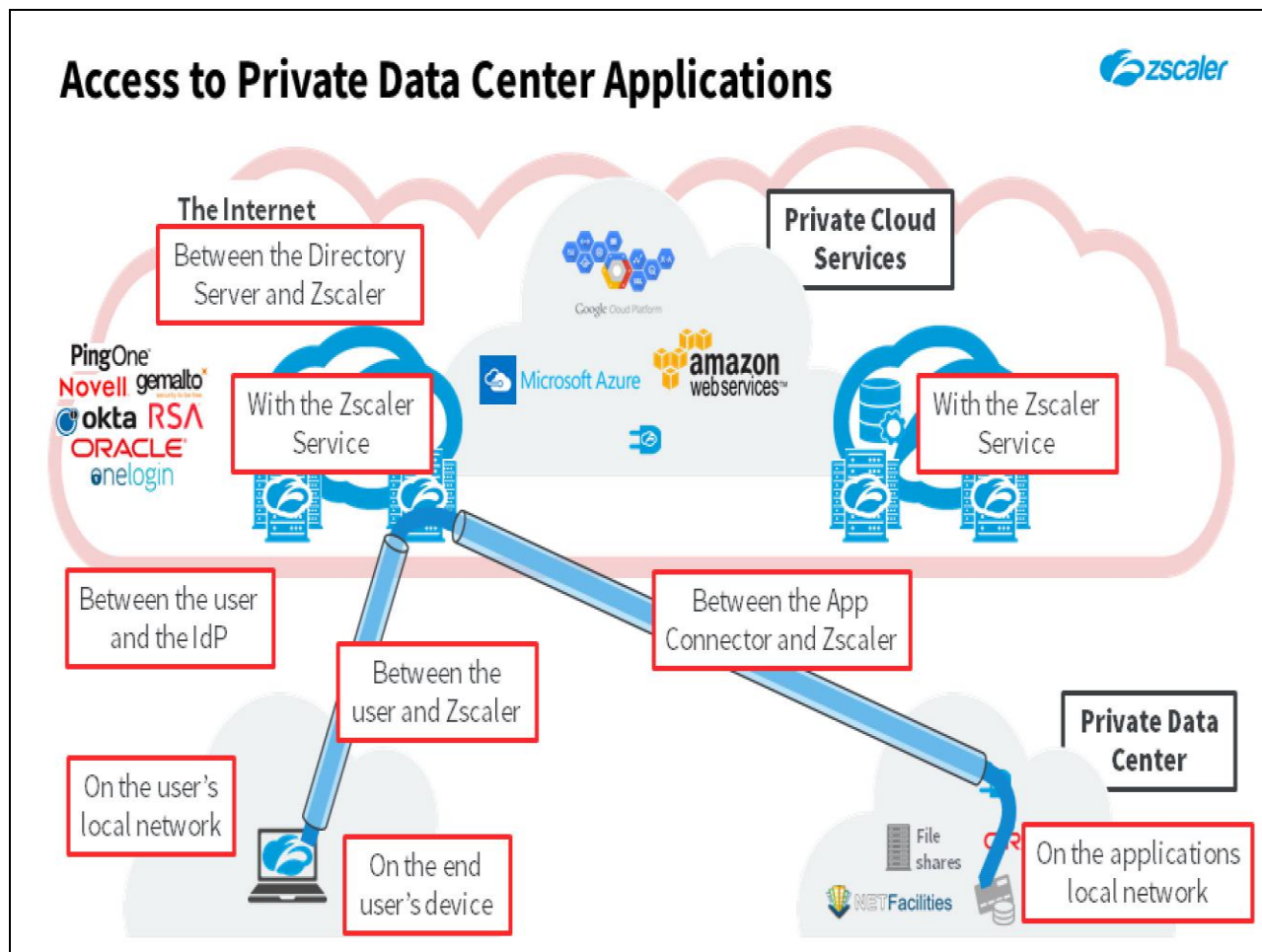
Slide 11 - Access to Private Data Center Applications



Slide notes

Problems can arise between the App Connectors and the ZPA infrastructure.

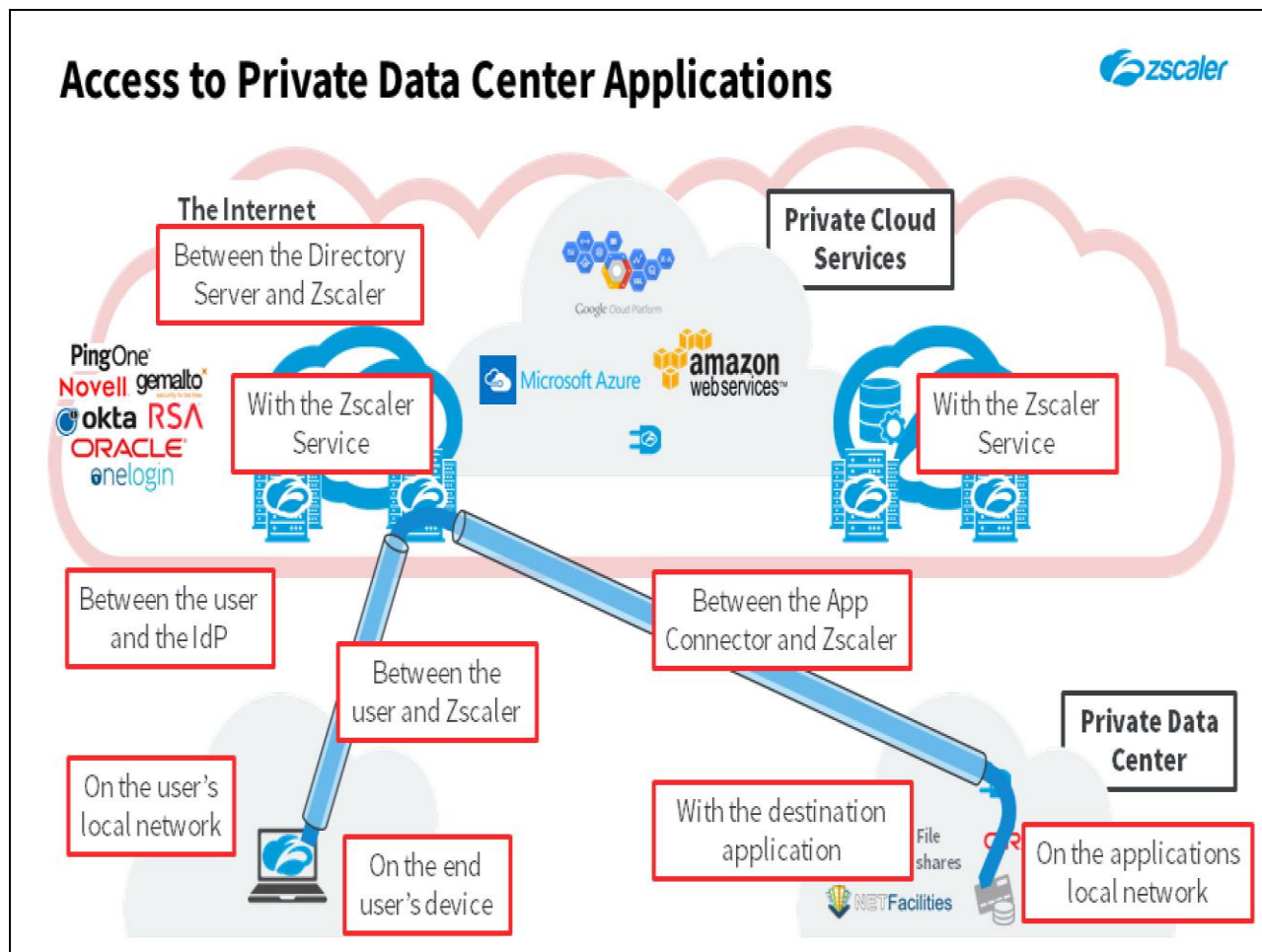
Slide 12 - Access to Private Data Center Applications



Slide notes

There can be problems on the destination network, between the App Connector and the target application.

Slide 13 - Access to Private Data Center Applications




Slide notes

Or, the target application may be experiencing an outage, or may be misconfigured for the users in question.

Slide 14 - Problem Localization

Problem Localization



Who is affected?

- Single user/computer?
- Multiple users/computers?
- Road warrior user(s)?
- User(s) at company location(s)


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

Problem Localization



Who is affected?

- Single user/computer?
- Multiple users/computers?
- Road warrior user(s)?
- User(s) at company location(s)

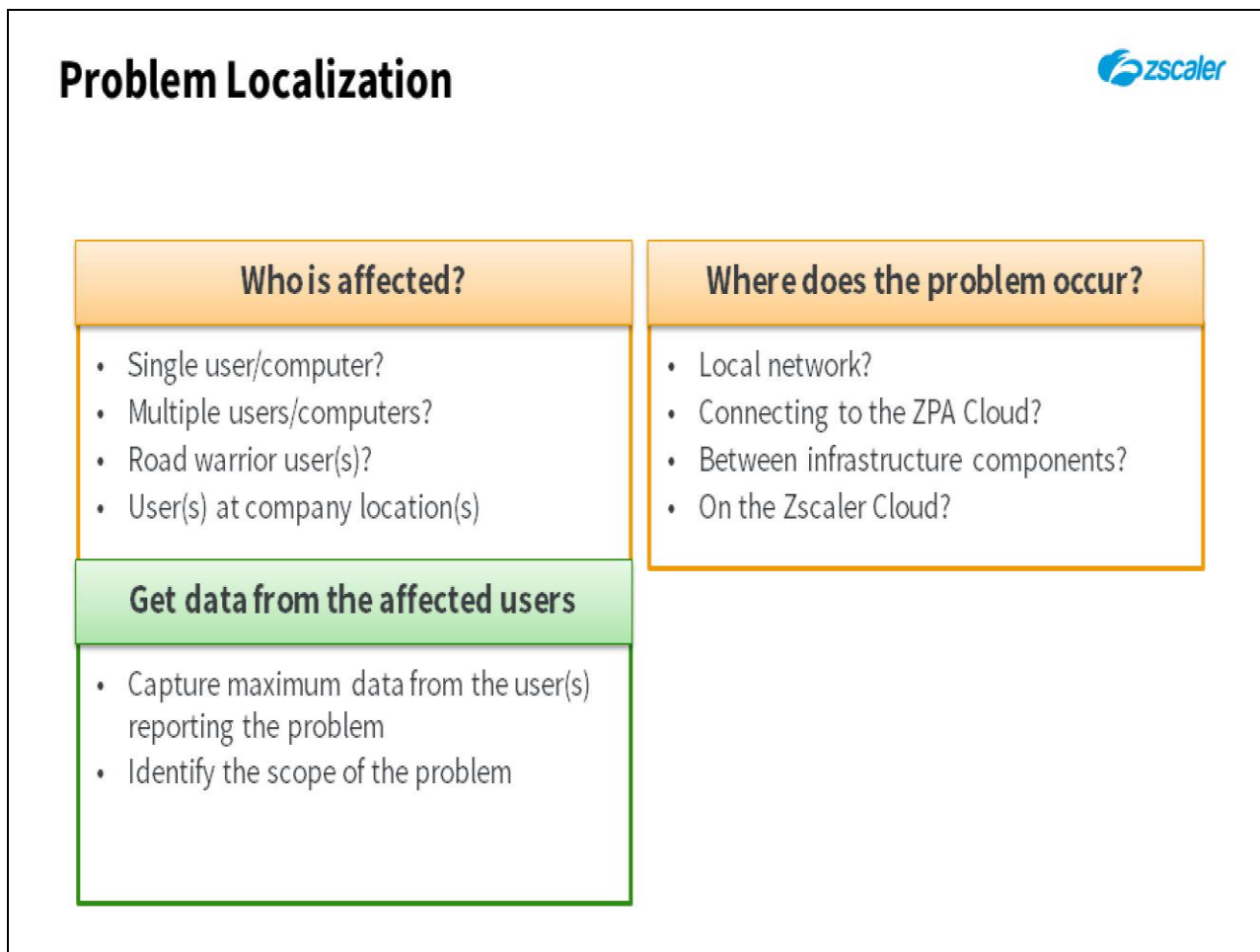
Get data from the affected users

- Capture maximum data from the user(s) reporting the problem
- Identify the scope of the problem

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 ZPA Cloud? Are there infrastructure components implicated (such as the SAML IdP)? Or is it an issue with the Zscaler service?

Slide 17 - Problem Localization

Problem Localization	
	
Who is affected?	Where does the problem occur?
<ul style="list-style-type: none">• Single user/computer?• Multiple users/computers?• Road warrior user(s)?• User(s) at company location(s)	<ul style="list-style-type: none">• Local network?• Connecting to the ZPA Cloud?• Between infrastructure components?• On the Zscaler Cloud?
Get data from the affected users	Use the available tools to identify
<ul style="list-style-type: none">• Capture maximum data from the user(s) reporting the problem• Identify the scope of the problem	<ul style="list-style-type: none">• Use Zscaler tools to verify user, application, and App Connector status• Use basic networking tools to narrow down the failure domain

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 the ZPA admin portal to view data from the **Dashboards**, or the **Diagnostics** page.

You may also need to use basic network troubleshooting tools such as **ping** and **tracert**, either on the user's network, or that of the target application, to narrow down the failure domain.

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

Questions to Ask




Is only the one user affected?

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

Questions to Ask



Is only the one user affected?


Is only the one Location affected?

Slide notes

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

Slide 21 - Questions to Ask

Questions to Ask



Is only the one user affected?

Is only the one Location affected?

What are the symptoms?


- No access to any application? No access to specific applications?
- Slow application access?
- Can the user authenticate?
- Can the user browse to Intranet/Internet destinations?
- Can the user reach any network destinations?

Slide notes

What exactly are the symptoms? No access to any application at all? Access only to some of the applications? Slow connectivity, or response from some, or all applications? Is the user able to authenticate? Can the user browse to Intranet or Internet destinations? Can the user reach any network destination at all?

Slide 22 - Questions to Ask

Questions to Ask



Is only the one user affected?

Is only the one Location affected?

What are the symptoms?

- No access to any application? No access to specific applications?
- Slow application access?
- Can the user authenticate?
- Can the user browse to Intranet/Internet destinations?
- Can the user reach any network destinations?

Is remote access to the affected PCs available (e.g. through Webex)?

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 install software, such as the Zscaler Analyzer tool.

Slide 23 - Problem Localization – Tools

Problem Localization – Tools

The screenshot shows the Zscaler Trust interface. At the top, there's a navigation bar with 'Zscaler TRUST' logo, a 'Zscaler Private Access' dropdown menu (highlighted with a red box), and links for 'Support', 'RSS', 'Sign In', and 'Subscribe'. Below the navigation bar, there's a 'Cloud Status' tab selected. The main content area shows a table of 'CORE CLOUD SERVICES' with columns for dates from Aug 4 to Aug 10. Each service row has a green checkmark in the Aug 10 column, indicating operational status. A legend at the bottom left explains the status icons: 'Under Investigation' (blue circle with exclamation mark), 'Service Disruption' (red circle with exclamation mark), and 'Service Degradation' (orange circle with exclamation mark). A blue box on the right contains the URL <https://trust.private.zscaler.com/> and two bullet points: 'Check ZPA Cloud status' and 'Check for on-going incidents'.

Service	Aug 4	Aug 5	Aug 6	Aug 7	Aug 8	Aug 9	Aug 10
Traffic Forwarding ⓘ							✓
Authentication ⓘ							✓
DNS ⓘ							✓
Zscaler Client Connector Admin ⓘ							✓
App Routing							✓
Client Enrollment							✓
Config Distribution							✓
Dashboard							✓
Diagnostics							✓
Downloads							✓
Health							✓
Security							✓

Under Investigation ⓘ Service Disruption ⓘ Service Degradation ⓘ

<https://trust.private.zscaler.com/>


- Check ZPA Cloud status
- Check for on-going incidents

Slide notes

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

Slide 24 - Problem Localization – Tools

Problem Localization – Tools



```
Command Prompt
Reply from 151.101.1.67: bytes=32 time=3ms TTL=59

Ping statistics for 151.101.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Users\student>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:
  0  <1 ms <1 ms <1 ms 192.168.1.254
  1  <1 ms <1 ms <1 ms 10.101.0.1
  2  <1 ms <1 ms <1 ms 184-170-224-225.cloud.skytap.com [184.170.224.225]
  3  <1 ms <1 ms <1 ms 184-170-224-225.cloud.skytap.com [184.170.224.225]
  4  2 ms 2 ms 2 ms lag-32-180-99.eas2.washington1.level3.net [4.14.228.113]
  5  * * * Request timed out.
  6  3 ms 3 ms 3 ms google-level3-60g.washingtondc.level3.net [4.68.71.186]
  7  4 ms 3 ms 3 ms 100.170.246.65
  8  4 ms 3 ms 3 ms 216.239.49.169
  9  3 ms 4 ms 3 ms dns.google [8.8.8.8]

Trace complete.

C:\Users\student>ping intranet.patrainig8.safemarch.com

Pinging intranet.patrainig8.safemarch.com [100.64.1.1] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.64.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping from user device and Connector

- Local and Internet hosts, ZPA infrastructure
- By FQDN and by IP
- Private applications should resolve, but not respond

Traceroute from user device and Connector

- Local and Internet hosts, ZPA infrastructure

```
(admin@zpa-connector ~)$ ping intranet.patrainig8.safemarch.com
PING intranet.patrainig8.safemarch.com (10.0.0.9) 56(84) bytes of data:
64 bytes from HOST-1.patrainig8.safemarch.com (10.0.0.9): icmp_seq=1 ttl=128 time=0.168 ms
64 bytes from HOST-1.patrainig8.safemarch.com (10.0.0.9): icmp_seq=2 ttl=128 time=0.208 ms
64 bytes from HOST-1.patrainig8.safemarch.com (10.0.0.9): icmp_seq=3 ttl=128 time=0.269 ms
64 bytes from HOST-1.patrainig8.safemarch.com (10.0.0.9): icmp_seq=4 ttl=128 time=0.261 ms
64 bytes from HOST-1.patrainig8.safemarch.com (10.0.0.9): icmp_seq=5 ttl=128 time=0.258 ms
^C
--- intranet.patrainig8.safemarch.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.168/0.247/0.288/0.042 ms
(admin@zpa-connector ~)$
```

Slide notes

Do not neglect basic network connectivity tools such as a **ping**, both from the client device, and from the relevant App Connector. Test for responses from Intranet and Internet destinations, and from ZPA public network components. Also test using IP addresses and FQDNs (to verify that DNS is resolving OK).

Note that private applications accessible only by ZPA should resolve to a **100.64.0.0/16** IP address on the client device, but they will not respond to any pings.

Another basic network troubleshooting tool is to do a **tracert** from the user's device, and from the appropriate App Connector. Once again, run the test against Intranet and Internet destinations, including key ZPA public infrastructure components.

If CLI access to the App Connector is not available, do these tests from a host device adjacent to it on the same subnet.

Slide 25 - Problem Localization – Tools

Problem Localization – Tools

The screenshot displays the Zscaler ZPA Admin Portal interface, divided into two main sections: Applications and Users. The Applications dashboard (top) shows metrics for Applications Accessed (17), Discovered Applications (11), Access Policy Blocks (14, highlighted with a red box), and Successful Transactions (158). Below these are lists for Applications Accessed and Top Applications by Bandwidth. The Users dashboard (bottom) shows metrics for Recent Users (3), Current Connected Users (4), Top Policy Blocks (4, highlighted with a red box), and Users Blocked by Policies (4, highlighted with a red box). Below these are lists for Recent Users, Current Connected Users, Top Users by Applications, Top Users by Bandwidth, and Top Policies by Blocked Users. A sidebar on the left contains navigation links for Dashboard, Diagnostics, Live Logs, Administration, Search, and Zscaler App. A Zscaler logo is in the top right corner.

ZPA Apps/Users Dashboards

- Look for **Access Errors**, **Policy Blocks**, or **Users Blocked by Policies**

Slide notes

There are several ZPA-specific tools for troubleshooting available from the ZPA admin portal.

Check both the **Applications** and **Users** Dashboards looking for error messages relating to the user, or application(s) in question. Drill down as necessary to investigate the nature of any errors reported, or to view recent diagnostic activity.

Slide 26 - Problem Localization – Tools

Problem Localization – Tools

The screenshot displays the Zscaler ZPA Health Dashboard. The top navigation bar includes 'Applications', 'Users', 'Health', and 'Connectors'. The 'Applications' section shows a list of applications with status indicators (green for healthy, red for unhealthy). The 'Connectors' section shows a list of connectors. A detailed view of the 'San Jose Connector 4' is shown, displaying a network diagram with various endpoints and their connections to the connector. The endpoints include IP addresses and domain names, such as 172.20.0.26, 172.20.0.15, 172.20.0.12, 172.20.0.13, 172.20.0.35, 172.20.0.2, 172.20.0.14, and 172.20.0.15. The connections are color-coded: green for healthy and red for unhealthy.

ZPA Health Dashboard


- Check the health of Applications, Servers, and Connectors

Slide notes

At the ZPA admin portal, check the **Health** Dashboard to understand the status of the various infrastructure components; Applications, Servers, and Connectors. Drill down as necessary to investigate the nature of any errors reported, or to view recent diagnostic activity.

Slide 27 - Problem Localization – Tools

Problem Localization – Tools



Applications

Users

Health

Connectors

30 Mins

Requires recent connector version. Results may not be accurate if running an older connector version.

CPU UTILIZATION

Connector Name	Connector Group Name	Connector Location	Value	Actions
Orbiter-1	Orbiter	New York, US	1 %	
Azure-LSS-1	Connectors-LSS	New York, US	1 %	
Azure-LSS-2	Connectors-LSS	New York, US	1 %	
AzureApp-1	AzureApps	New York, US	1 %	

MEMORY UTILIZATION

Connector Name	Connector Group Name	Connector Location	Value	Actions
Orbiter-1	Orbiter	New York, US	17 %	
Azure-LSS-1	Connectors-LSS	New York, US	10 %	

BYTES (RECEIVED AND TRANSMITTED)

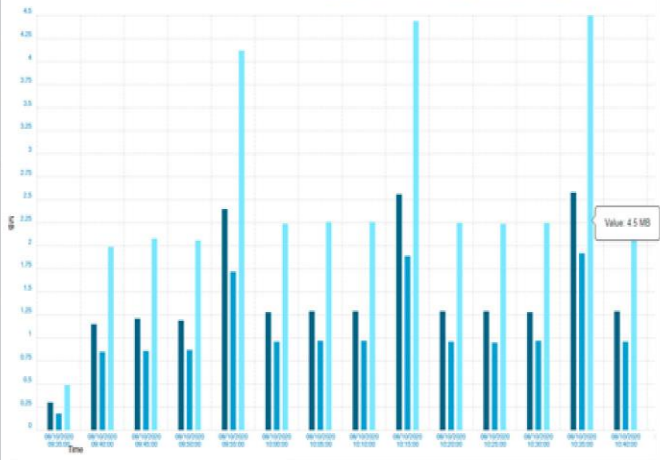
Connector Name	Connector Group Name	Connector Location	Value	Actions
Azure-LSS-2	Connectors-LSS	New York, US	2.22 MB	
Azure-LSS-1	Connectors-LSS	New York, US	1.68 MB	

Health of Connector: Azure-LSS-2

Bytes (Received and Transmitted)

Bytes (Received) Bytes (Transmitted) Bytes (Received and Transmitted)

Requires recent connector version. Results may not be accurate if running an older connector version.



Value 4.5 MB

ZPA Health Dashboard:
Connectors Details


- Check connector utilization

Slide notes

The **Connectors** dashboard includes a number of widgets that display detailed health information about all App connectors in an organization, including CPU and memory utilization, Bytes received and transmitted, Mtnet count and health charts.

Slide 28 - Problem Localization – Tools

Problem Localization – Tools



Log Type Connector Status

Jul 27, 2020 11:32:54 EDT - Aug 10, 2020 11:32:54 EDT

TOTAL

90

ERRORS

0

SUCCESSFUL

90

▼ [Connector Name Equals OnPrem-1] AND [Connector Connection Type Equals Control Connection]

CONNECTOR NAME: Equals CONNECTOR CONNECTION TYPE: Equals

X OnPrem-1 X Control Connection

Apply Clear All Add Filters

Session	Auth Log Timestamp	Authentication Time
Authenticated	Aug 10th, 11:30:15.292 EDT	Aug 10th, 09:30:15.504 EDT
Authenticated	Aug 10th, 11:36:15.292 EDT	Aug 10th, 09:30:15.504 EDT
Authenticated	Aug 10th, 11:32:15.292 EDT	Aug 10th, 09:30:15.504 EDT
Authenticated	Aug 10th, 11:18:15.292 EDT	Aug 10th, 09:30:15.504 EDT
Authenticated	Aug 10th, 11:14:15.292 EDT	Aug 10th, 09:30:15.504 EDT

ZPA Diagnostics

- Browse or search for events for the Applications, Servers, and Connectors affected

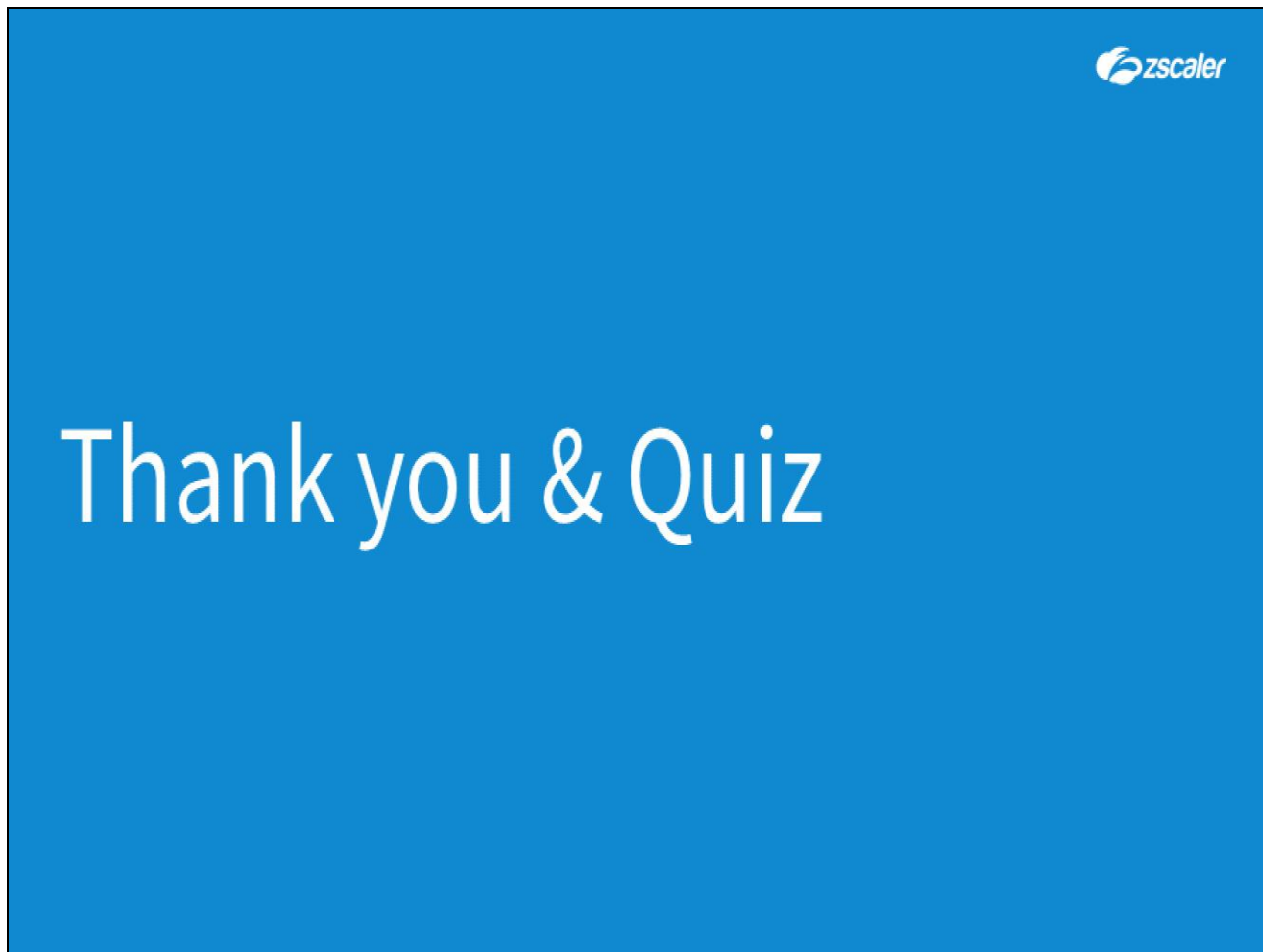
Connection	UTC	Policy	User	Service Edge	Connector	Application
Aug 10th, 11:04:14.4...	✓	Policy is not configured for access	hvac@patrainngl.safemarch.com	US-VA-9408	Unavailable	hvac.patrainngl.s... 80 TCP
Aug 10th, 11:04:14.3...	✓	Policy is not configured for access	hvac@patrainngl.safemarch.com	US-VA-9408	Unavailable	hvac.patrainngl.s... 80 TCP
Aug 10th, 11:04:01.8...	✓	Policy is not configured for access	hvac@patrainngl.safemarch.com	US-VA-9408	Unavailable	hvac.patrainngl.s... 80 TCP
START TIME: Aug 10th, 10:30:28.1...	✓	Block HMAC	student@patrainngl.safemarch.com	US-OH-9408	No connector can reach this app...	APPLICATION PORT & PROTOCOL: hvac.patrainngl.s... 80 TCP
END TIME: Aug 10th, 10:30:28.1...	✓	Deny	194.170.224.174	LOCATION: Cleveland, US	IP PORT & PROTOCOL: Unavailable TCP	APPLICATION SEGMENT: HVAC
STATUS CODE: Application policy blo...	✓	POLICY ID: 144123242213278029	LOCATION: Sterling, US	POLICY PROCESSING: 0 ms	LOCATION: Unavailable	SERIES IP PORT & PROTOCOL: Unavailable 80 TCP
INTERNAL STATUS CODE: BPK_M_T_SETUP_FAIL...	✓		CLIENT TYPE: Web Browser	RM FROM CLIENT: 0 B	CONNECTOR ID: Unavailable	APPLICATION ID: 144123242213278029
STATUS: Closed Connecto...	✓		USER MESSAGE	TX TO CONNECTOR: 0 B	CONNECTOR SETUP TIME: 0 ms	SERIES ID: Unavailable
DURATION: 0ms	✓			RM FROM CONNECTOR: 0 B	CONNECTOR GROUP NAME: Unavailable	DOUBLE ENCRYPTION: Disabled
TOTAL BYTES: 0 B	✓			TX TO CLIENT: 0 B	CONNECTOR GROUP ID: Unavailable	
CONNECTION ID: rlvRPhKX06A204...	✓					
CONNECTION STATUS LOG	✓					
Aug 10th, 10:30:27.9...	✓	Block HMAC	student@patrainngl.safemarch.com	US-OH-9408	No connector can reach this app...	hvac.patrainngl.s... 80 TCP
Aug 10th, 10:30:27.9...	✓	Block HMAC	student@patrainngl.safemarch.com	US-OH-9408	No connector can reach this app...	hvac.patrainngl.s... 80 TCP

Slide notes

The ZPA admin portal also contains a **Diagnostics** page, where you can filter and search log messages by the **User**, **Application**, and **Connector** in question.

This is a powerful interface for researching and investigating problems with the ZPA environment, and includes both real-time, and historic views of the log messages.

Slide 29 - Thank you & Quiz



Slide notes

Thank you for following this training module on localizing 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.