
Zscaler for Workloads (EDU-240)

Hands-on Lab Guide



Copyright

This document is protected by the United States copyright laws, and is proprietary to Zscaler Inc. Copying, reproducing, integrating, translating, modifying, enhancing, recording by any information storage or retrieval system or any other use of this document, in whole or in part, by anyone other than the authorized employees, customers, users or partners (licensees) of Zscaler, Inc. without the prior written permission from Zscaler, Inc. is prohibited. ©2015-24 Zscaler, Inc. All rights reserved.

Trademark Statements

Zscaler™, Zscaler Internet Access™, Zscaler Private Access™, ZIA™ and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the property of their respective owners.

Zscaler for Workloads (EDU-240) Lab Guide

Feb. 2024, Rev. 1.0a

Contents

About the Zscaler for Workloads Hands-on Labs	4
Lab Setup.....	5
Accessing the Environment.....	6
Task 1: Connect to your pod	6
Pre-Lab: Provision AWS and Azure	9
Lab 1: Navigating the Cloud Connector Dashboard	11
Task 1: Navigate to the Cloud Connector Dashboard	11
Lab 2: Managing Location and Provisioning Templates	17
Task 1: Configure a Location Template	17
Task 2: Configure a Provisioning Template	19
Lab 3: Managing Traffic Forwarding Policy	23
Task 1: Verify Internet Connection.....	23
Task 2: Configure a Traffic Forwarding Rule.....	24
Lab 4: Using Analytics and Logging	30
Task 1: Review Insights Logs	30
Lab 5: Enforcing Minimum TLS Versions	33
Task 1: Configure SSL Inspection Policy	33
Task 2: Verify SSL Inspection Policy.....	37
Lab 6: Protecting Against Malicious Payloads, Phishing, and BotNet	42
Task 1: Test Zscaler Security Protections.....	42
Lab 7: Enforcing a Data Loss Prevention Policy.....	48
Task 1: Configure DLP Policy	48
Task 2: Verify DLP Policy.....	52
Lab 8: Controlling Access to Specific Resources on Websites.....	56
Task 1: Configure URL Filtering Rule.....	56
Task 2: Verify URL Filtering Rule	61
Lab 9: Integrating with Zscaler Private Access.....	65
Summary	85
Clean-up.....	86

About the Zscaler for Workloads Hands-on Labs

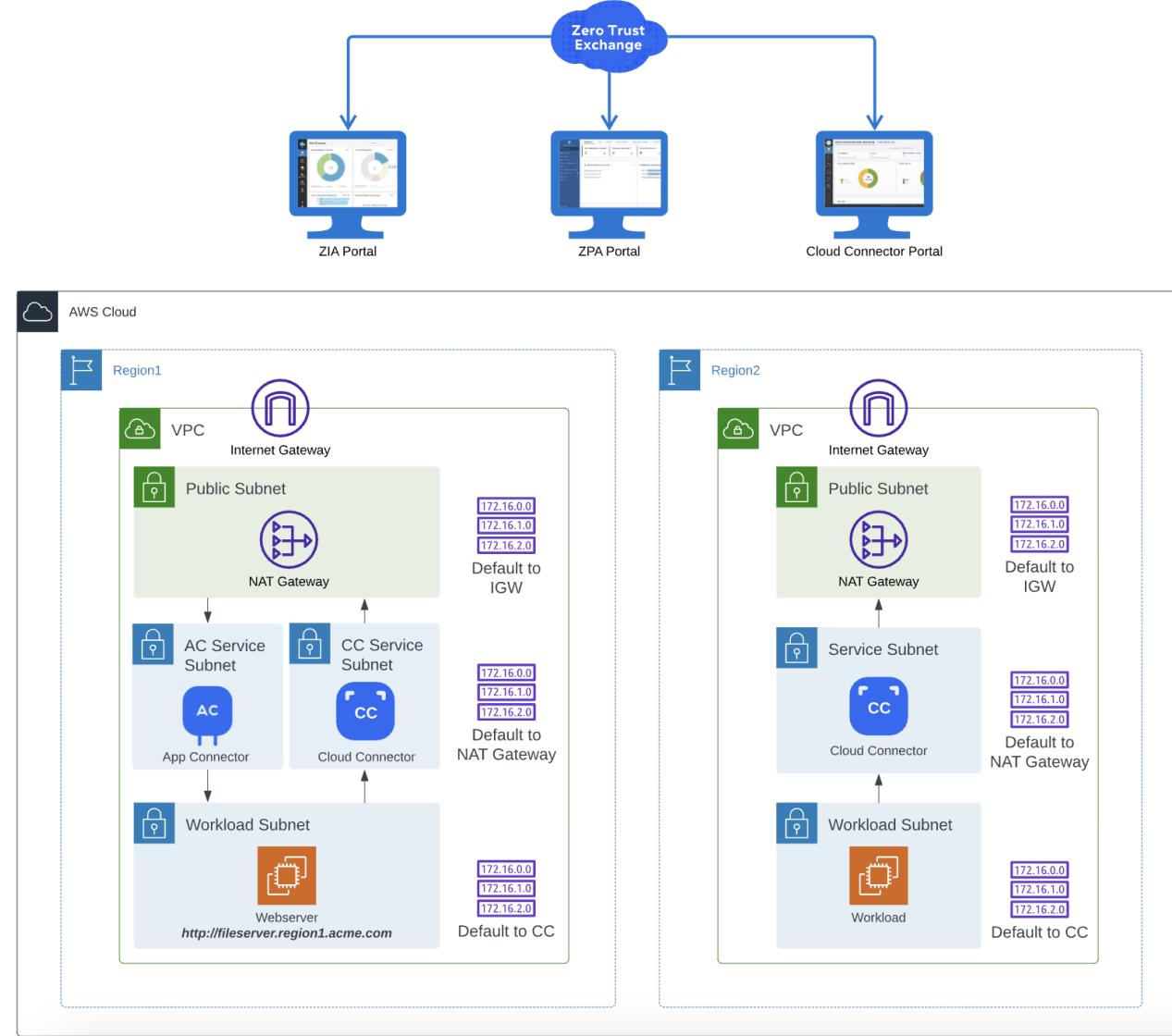
Keeping applications and cloud workloads secure is a growing concern across all industries. Zero trust architecture is an effective approach to workload security. Zscaler Workload Communications on Amazon Web Services (AWS) allows you to securely connect your applications anywhere by minimizing the attack surface, preventing lateral movement, and reducing the risk of bad actors gaining access to your data. Unlike legacy firewalls and security appliances, Zscaler Workload Communications directly connects any application to any destination and enforces least-privileged policies for zero trust security.

This lab covers three main areas:

- Cloud Connector Overview
- Protecting Workload Internet Access with ZIA
- Integrating with Zscaler Private Access

Lab Setup

This lab deploys resources in two AWS regions (Region1 and Region2 in the diagram).



Accessing the Environment

Your pod has been configured with a Bastion host to proxy communication between your machine and each of the lab components you wish to access without the need for a VPN or client. As part of the event, a **URL was displayed that you can use to secure a pod**. Simply browse to this URL, input your information and click the **RSVP** button.

Task 1: Connect to your pod

In this task, you will connect to your lab environment. To connect to your pod and log in, follow these steps:

1. Navigate to the **RSVP URL** displayed during your session.
2. Enter the information requested.
3. Click **RSVP!**.

E-mail*

First Name*

Last Name*

I agree to the [Terms of Service](#)*

RSVP!

Note: Once registered, the demo tool will place you directly into your pod's dashboard. You can access any of your pod's resources by simply clicking on the icons in the image map. Clicking each will open a new tab with access into that respective device, so ensure pop-up blockers are disabled.

Assessing the Environment



You can find the credentials for your pod at the bottom of your pod dashboard under the **Input Variables** dropdown. These will be used to login to the Cloud Connector and ZIA/ZPA portals, respectively:

 Documentation

 Input Variables (24)

Region1 Preference (aws_region1)

us-west-2



Region2 Preference (aws_region2)

us-east-2



Zscaler Cloud Name (cloudname)

zscalertwo.net



Pod Suffix (name_suffix)

2GKMEW



Pod Password (secret_password)

CloudConnector2023!



Pod Username (secret_username)

student@zenithlive1.net



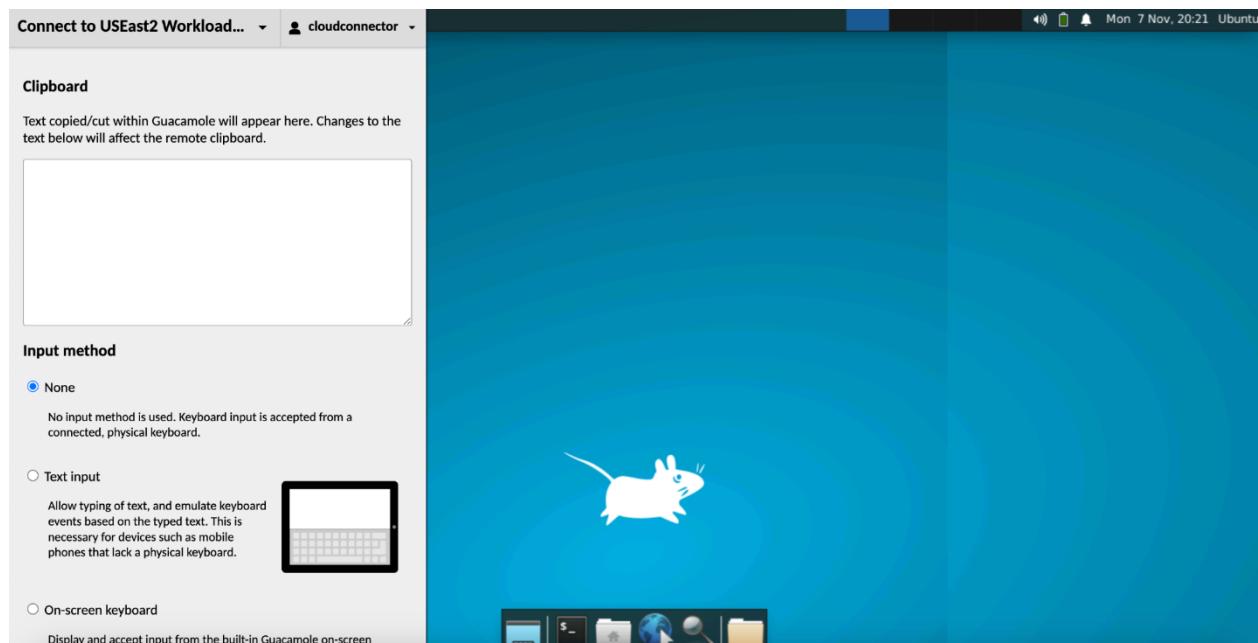
Assessing the Environment

For reference, the table below lists the credentials to all pods (replace 'XX' in the username with your pod's number):

	Username	Password
ZIA Portal	student@zenithliveXX.net	CloudConnector2023!
ZPA Portal	student@zenithliveXX.net	CloudConnector2023!
Cloud Connector Portal	student@zenithliveXX.net	CloudConnector2023!
Test Machines	cloudconnector	CloudConnector2022!

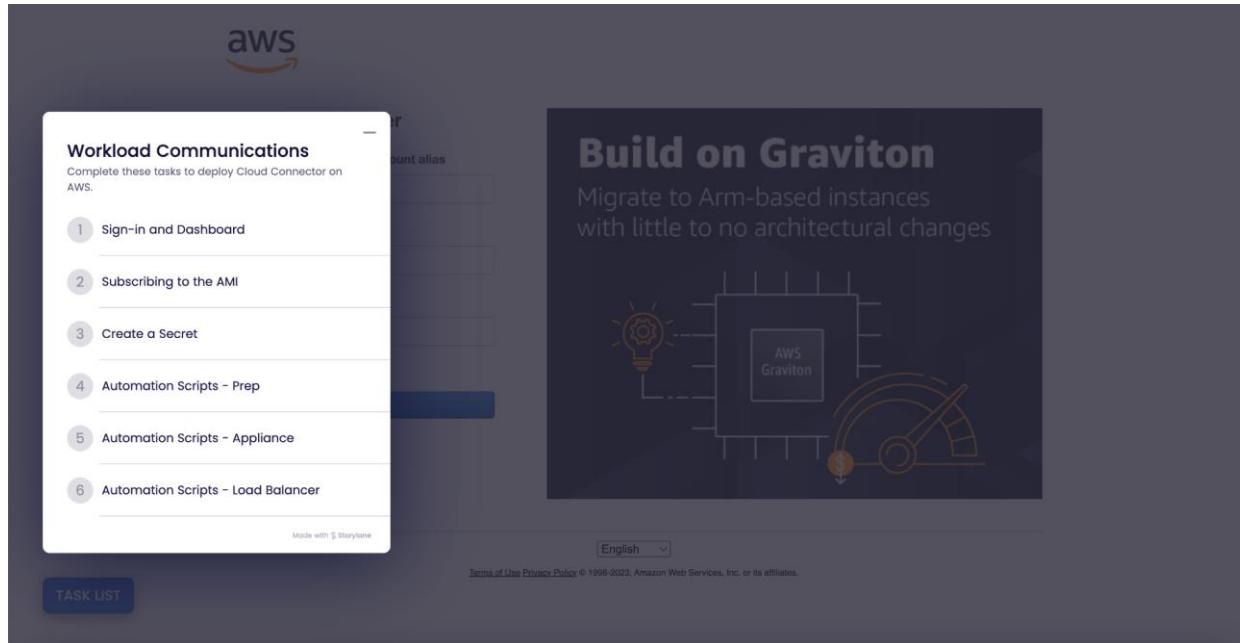
- To adjust settings within your current window, press **CTRL+ALT+SHIFT** (CTRL+OPTION+SHIFT on Mac).

Note: This option is useful for split-screening consoles, copying or pasting, and quickly navigating between connections.



Pre-Lab: Provision AWS and Azure

Your pod has been preconfigured with Cloud Connector appliances using an automation tool. Before we get started, let's review what this tool did to understand what was configured within the cloud provider. When you RSVP'd, a modal should have appeared on your screen with a click through demo of the AWS workflow:



This modal will walk you through the basic deployment of a Cloud Connector appliance inside of AWS. Take a moment to walk through this click-through demo. There are three main steps to consider when deploying the appliances within a public cloud:

1. Subscribing to the Cloud Connector AMI (or VHD, if Azure) in the Marketplace.
2. Creating a Secrets Manager object to store registration credentials (or Key Vault, if Azure) that the appliance will use to authenticate to the Zscaler service.
3. Running automation scripts to deploy the infrastructure (CloudFormation, Terraform, Marketplace ARM, etc.)

The demonstration in the modal used CloudFormation Templates to deploy the appliances. In this case, CloudFormation Templates assume a brownfield environment where basic infrastructure already exists: such as a VPC, Subnets, Route Tables, Internet Gateway, etc. Hence, the modal does not demonstrate the deployment of those resources.



For more information on provisioning and deploying Cloud Connector appliances, please refer to the reference documentation [here](#). We strongly recommend reviewing this workflow prior to proceeding so that you have a complete understanding of the remaining tasks.

Lab 1: Navigating the Cloud Connector Dashboard

Zscaler Cloud Connector is a virtual machine (VM) that simplifies traffic being forwarded to Zscaler services. It extends the capabilities of Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) to cloud-native workloads, which allows enterprises to secure cloud workload communications over any network.

Task 1: Navigate to the Cloud Connector Dashboard

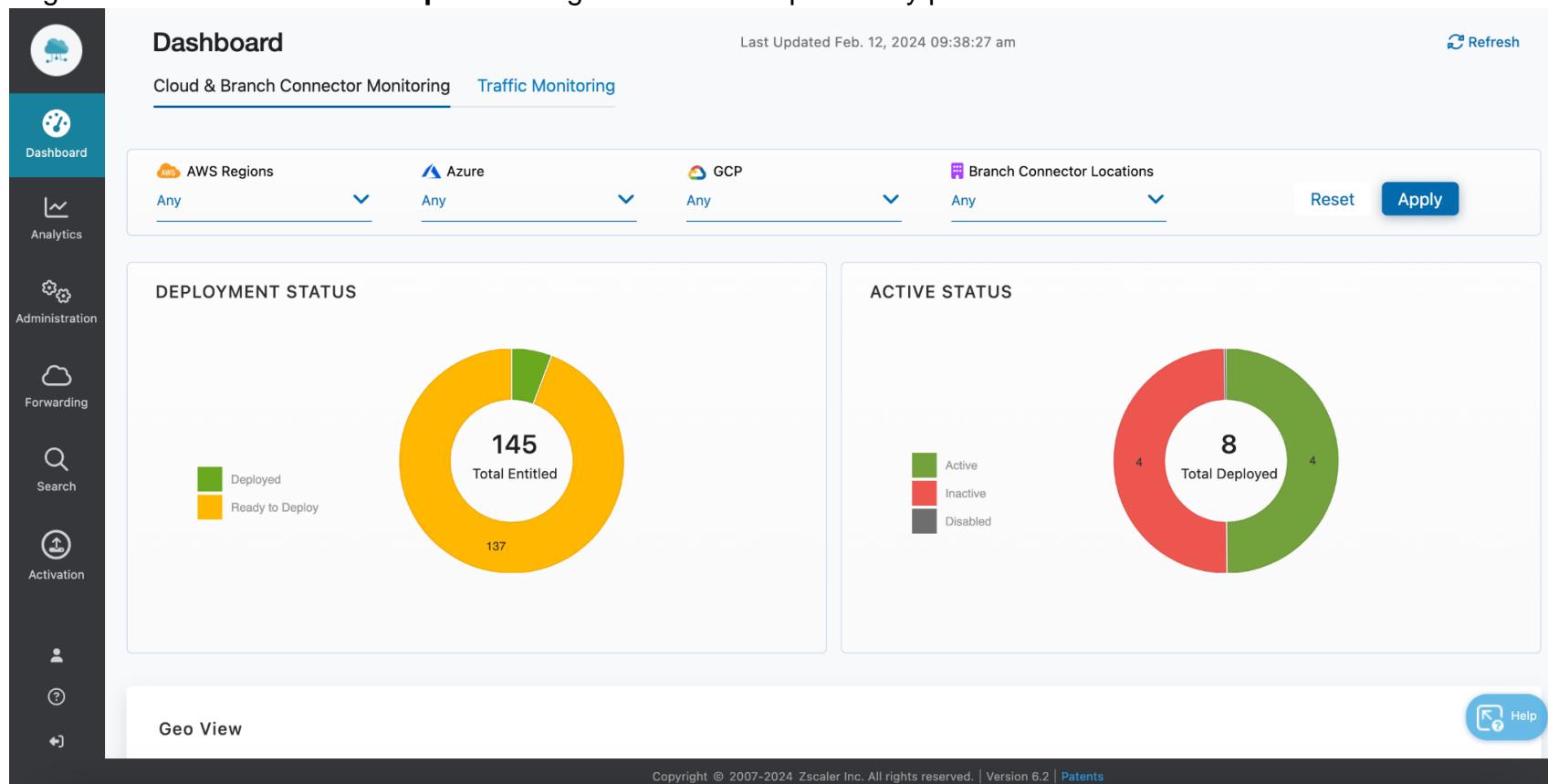
In this task, you will familiarize yourself with the Cloud Connector dashboard and its three main functions:

- Facilitating the onboarding, provisioning, and registration process of appliances within various Branch and Cloud environments.
- Providing a new logging perspective on traffic leaving or transiting the cloud. This can aid in troubleshooting as well as threat correlation.
- Providing a traffic steering mechanism to allow administrators to granularly control how traffic is forwarded through the appliance (ZIA, ZPA, or direct).

Lab1: Navigating the Cloud Connector Dashboard

Navigate to the Cloud Connector portal by clicking on the icon at the top of your pod's image map:

1. Log in to the **Cloud Connector portal** using the credentials previously provided.



The screenshot shows the Zscaler Cloud Connector Dashboard. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Administration, Forwarding, Search, Activation, and Help. The main dashboard has two primary sections: Deployment Status and Active Status.

Deployment Status: A donut chart titled "145 Total Entitled" with a breakdown of 137 Ready to Deploy and 8 Deployed. A legend indicates "Deployed" is green and "Ready to Deploy" is yellow.

Status	Count
Ready to Deploy	137
Deployed	8

Active Status: A donut chart titled "8 Total Deployed" with a breakdown of 4 Active, 4 Inactive, and 0 Disabled. A legend indicates "Active" is green, "Inactive" is red, and "Disabled" is grey.

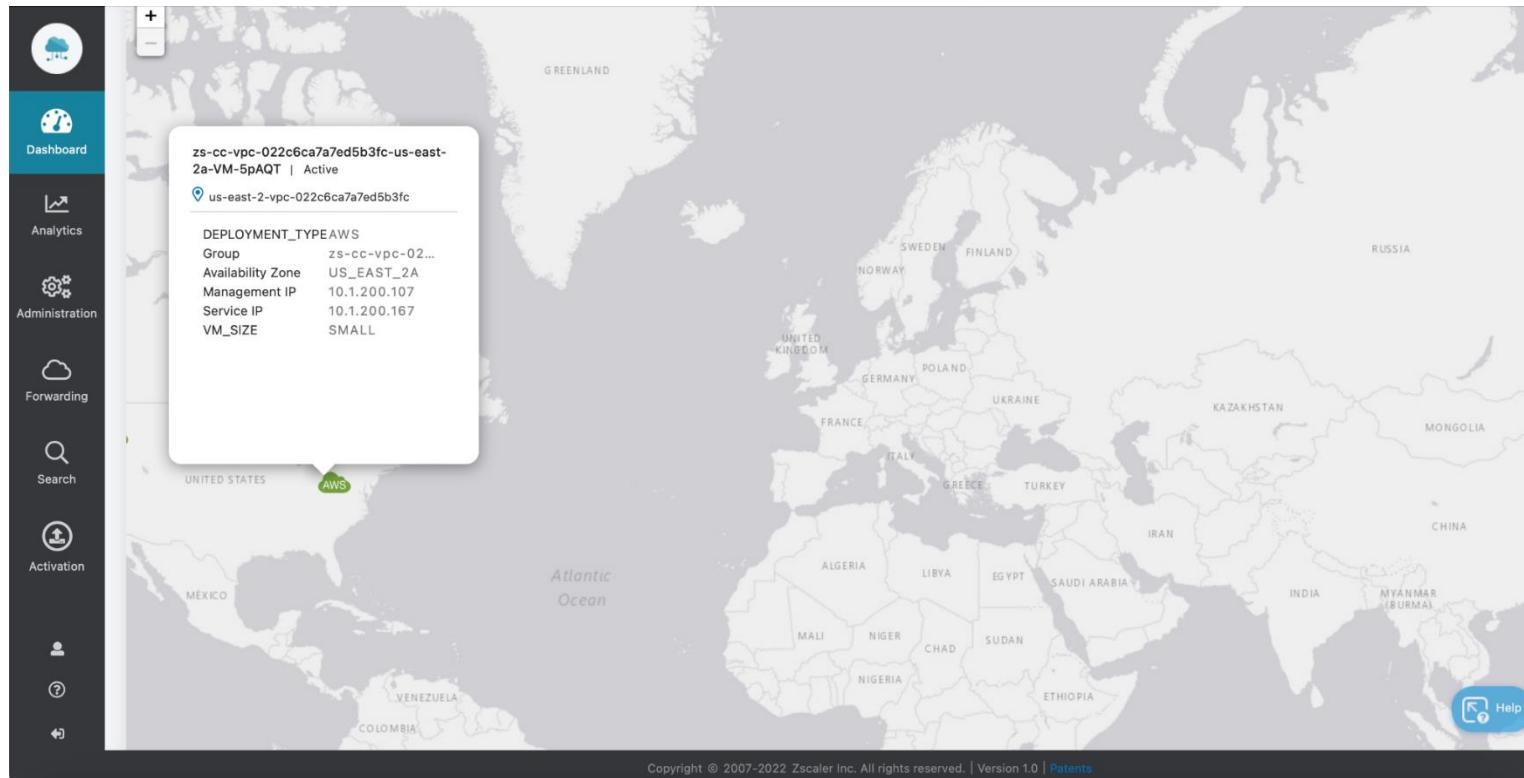
Status	Count
Active	4
Inactive	4
Disabled	0

At the bottom of the dashboard, there is a "Geo View" button and a "Help" button. The footer contains copyright information: "Copyright © 2007-2024 Zscaler Inc. All rights reserved. | Version 6.2 | Patents".

Lab1: Navigating the Cloud Connector Dashboard

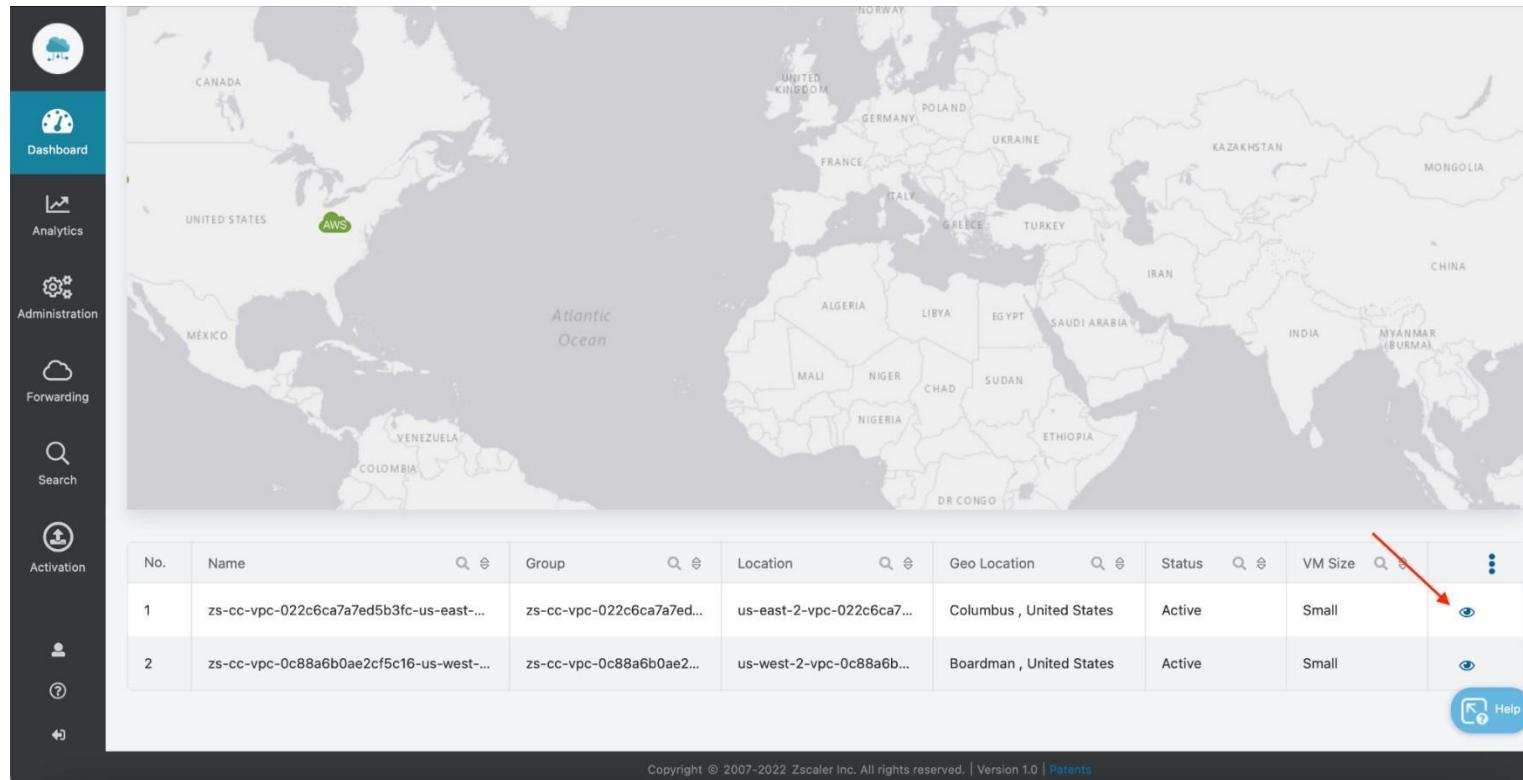
2. At the top of the dashboard, review the number of Cloud Connector appliances deployed and the number of active vs. inactive. Note that the inactive Cloud Connector appliances are normal. Your pod has been pre-configured with AWS Auto Scale functionality. The inactive appliances represent Warm Pool instances that will remain inactive until traffic demand increases. Your pod may have more inactive instances than depicted in the preceding graphic, though all pods should have at least four active instances (two in each region)
3. Scroll down to a geographical view of where each of the Cloud Connector appliances are deployed.
4. Click on the Cloud Connector icon on the map to view additional information about the appliance, including appliance size, health, status, VPC information.

Lab1: Navigating the Cloud Connector Dashboard



5. Scroll down further to see a listing of the Cloud Connector appliances.
6. Click on the view details icon (eyeball) to the right of one of your Cloud Connectors.

Lab1: Navigating the Cloud Connector Dashboard



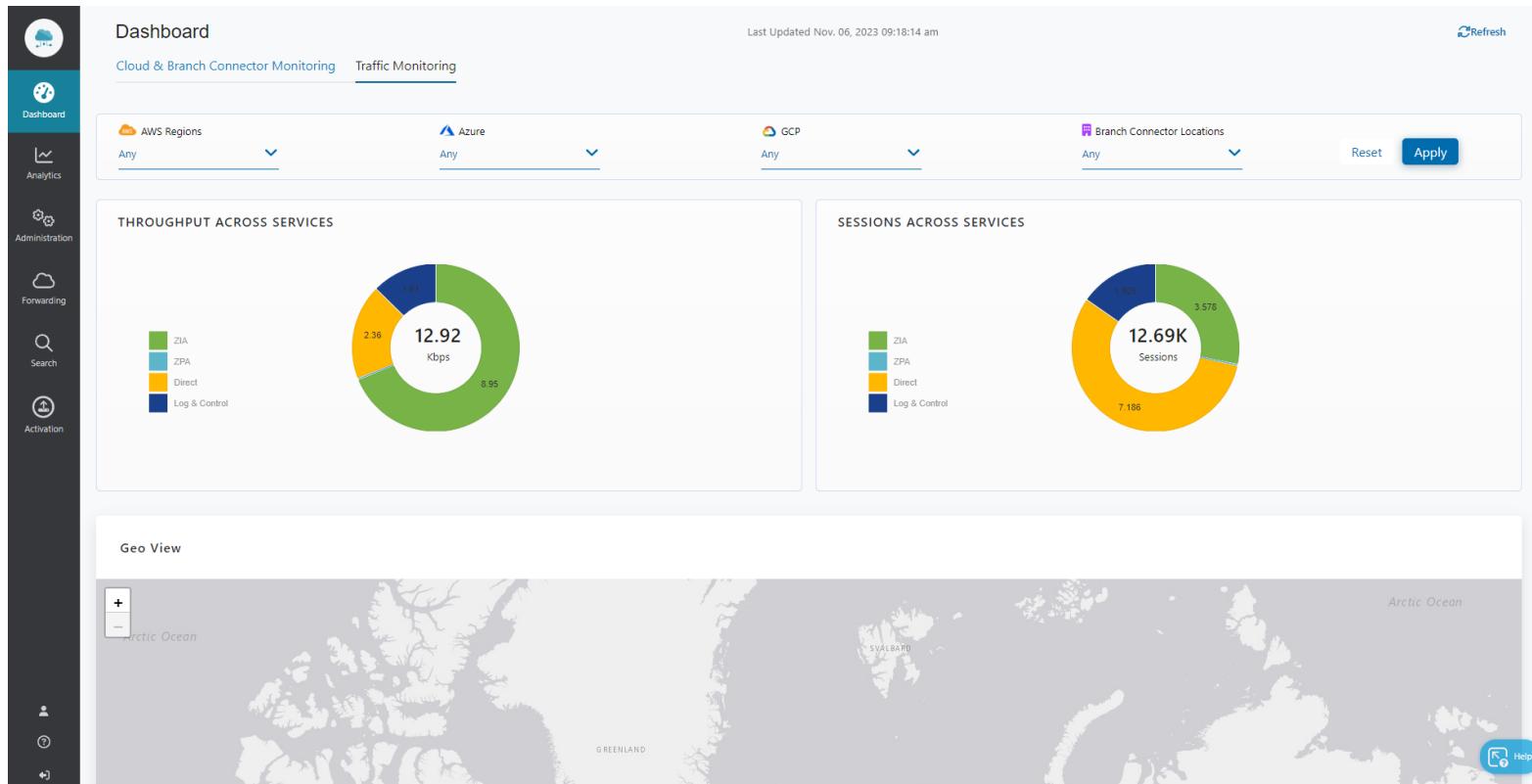
The screenshot shows the Zscaler Cloud Connector Dashboard. On the left is a vertical navigation bar with icons for Home, Dashboard, Analytics, Administration, Forwarding, Search, Activation, Help, and Logout. The main area features a world map with a green marker labeled 'AWS' over the United States. Below the map is a table listing two Cloud Connectors:

No.	Name	Group	Location	Geo Location	Status	VM Size	Actions
1	zs-cc-vpc-022c6ca7a7ed5b3fc-us-east-...	zs-cc-vpc-022c6ca7a7ed...	us-east-2-vpc-022c6ca7...	Columbus , United States	Active	Small	
2	zs-cc-vpc-0c88a6b0ae2cf5c16-us-west-...	zs-cc-vpc-0c88a6b0ae2...	us-west-2-vpc-0c88a6b...	Boise , United States	Active	Small	

A red arrow points to the eye icon in the Actions column of the first row. At the bottom right of the dashboard is a 'Help' button with a question mark icon.

7. In this screen, review additional information about the Cloud Connector appliance, such as General and Management Information and Forwarding Information.
8. In the upper left portion of the screen, click the **Traffic Monitoring** tab.

Lab1: Navigating the Cloud Connector Dashboard



- Review statistics about the traffic that this appliance is processing.

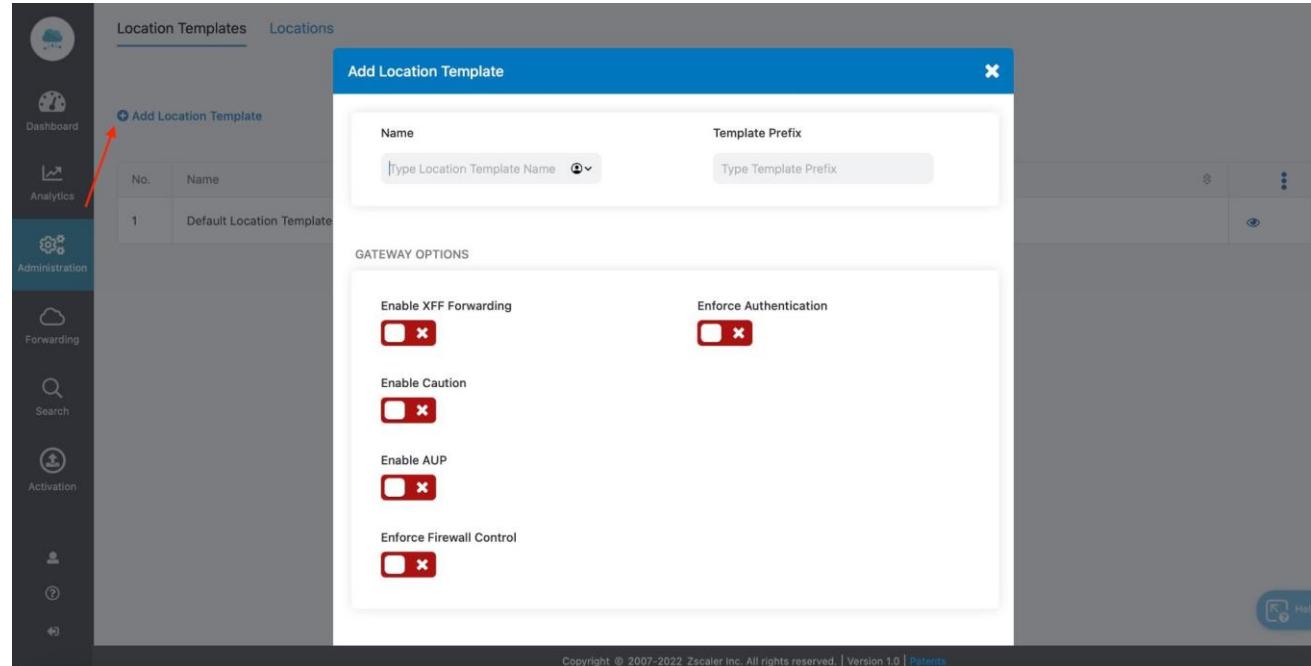
Lab 2: Managing Location and Provisioning Templates

Cloud Connector appliances use *Provisioning Templates* and *Location Templates* to bootstrap themselves when they register.

Task 1: Configure a Location Template

Zscaler Cloud Connector appliances automatically create Locations based on the Cloud Service Provider networks that they serve. Controlling which features are enabled or disabled for dynamically created Locations is the job of a Location Template. In this task, you will create a new Location Template.

1. In the Cloud Connector portal, select **Administration > Location Templates > Add Location Template**.

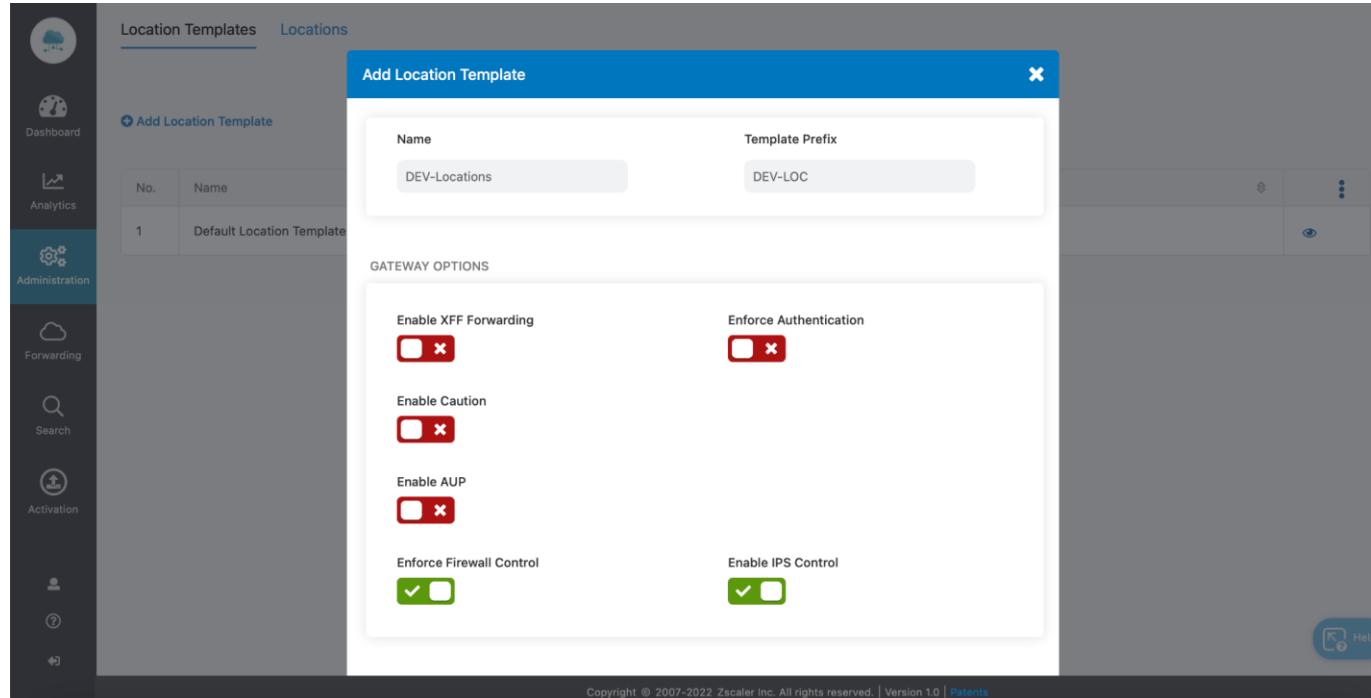


Lab 2: Managing Location and Provisioning Templates

2. To configure the template:

- Enter a **Name**.
- Optionally, enter a **Template Prefix**.

Note: The Template Prefix will be prepended to all Locations this template is attached to in order to help make a Location more easily identifiable.



- Select the options you wish to enable.
- Click **Save**.

Note: This template will not be used, so feel free to explore.

Task 2: Configure a Provisioning Template

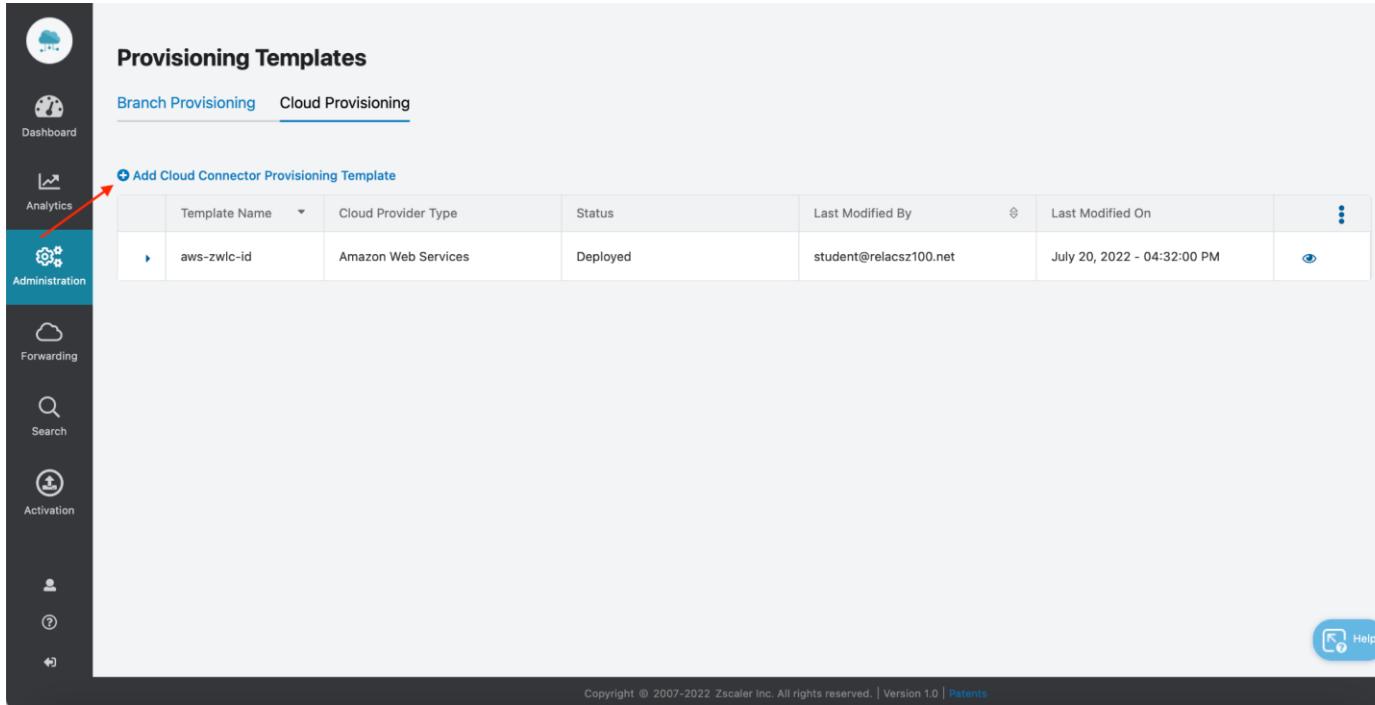
The glue that binds a cloud network to a Location Template and, hence, a Location and its configured attributes is a Provisioning Template.

1. In the Cloud Connector portal, select **Administration > Provisioning & Configuration**.
-

Note: An AWS template has already been configured for you. In fact, your currently registered Cloud Connectors used this template when registering.

2. Click **Add Cloud Connector Provisioning Template**.

Lab 2: Managing Location and Provisioning Templates



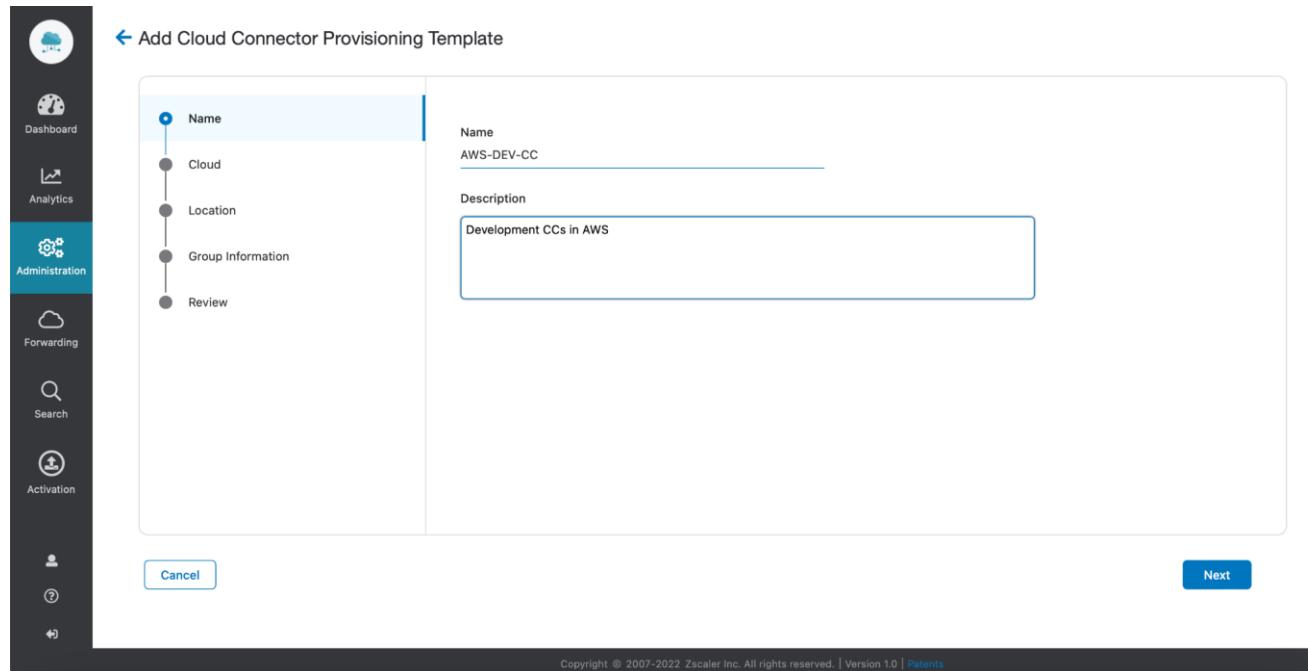
The screenshot shows the Zscaler Cloud Provisioning interface. On the left, a vertical sidebar lists various navigation options: Dashboard, Analytics (with a red arrow pointing to it), Administration (selected), Forwarding, Search, Activation, and Help. The main content area is titled "Provisioning Templates" and shows two tabs: "Branch Provisioning" and "Cloud Provisioning" (selected). Below the tabs is a table with the following data:

Template Name	Cloud Provider Type	Status	Last Modified By	Last Modified On	Actions
aws-zwlc-id	Amazon Web Services	Deployed	student@relacsz100.net	July 20, 2022 - 04:32:00 PM	

At the bottom of the page, there is a copyright notice: "Copyright © 2007-2022, Zscaler Inc. All rights reserved. | Version 1.0 | Patents".

3. To configure the template:
 - a. Enter a **Name**.
 - b. Enter a **Description**.

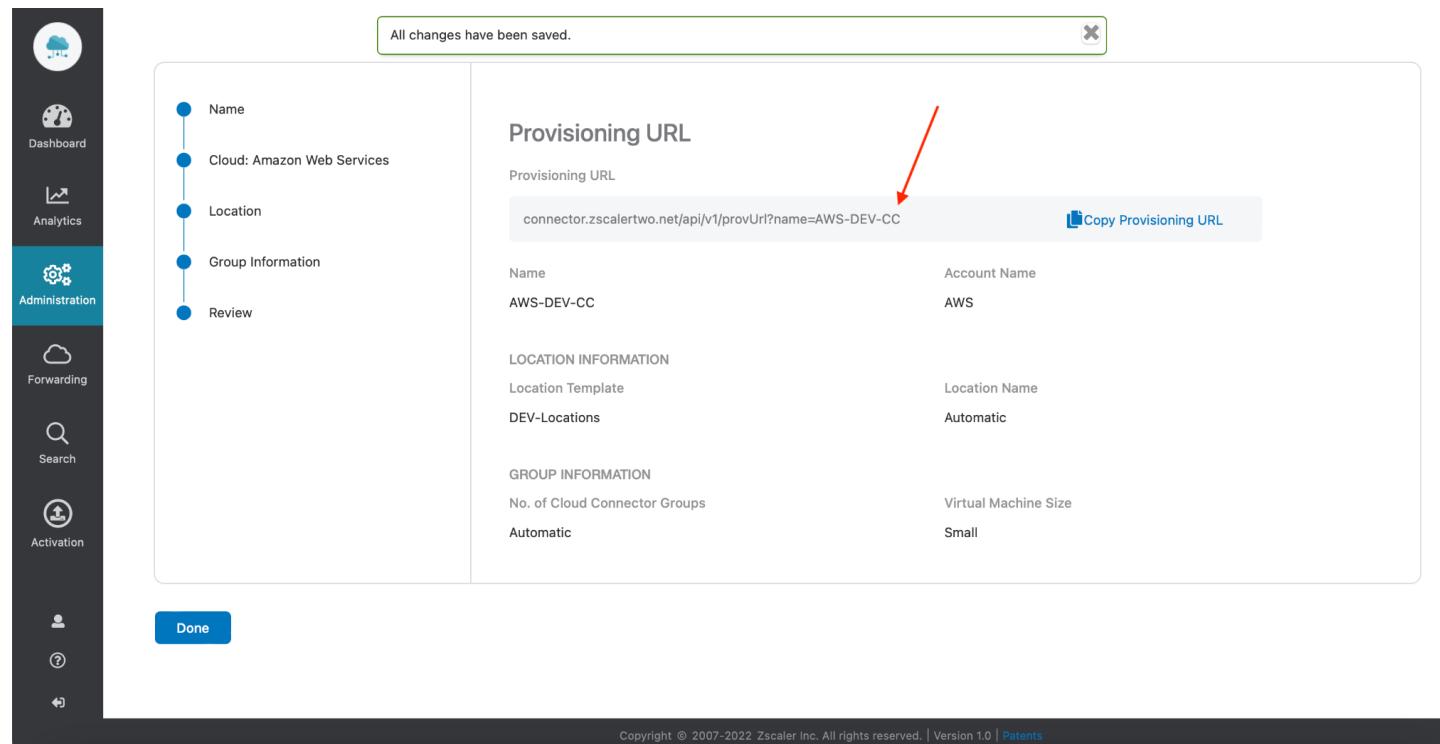
Lab 2: Managing Location and Provisioning Templates



The screenshot shows the 'Add Cloud Connector Provisioning Template' page. On the left, a vertical sidebar lists navigation options: Dashboard, Analytics, Administration (which is selected and highlighted in blue), Forwarding, Search, Activation, and a user icon. The main content area has a title 'Add Cloud Connector Provisioning Template' with a back arrow. It displays a vertical workflow with steps: Name (highlighted with a blue dot), Cloud, Location, Group Information, and Review. The 'Name' step is expanded, showing a text input field with 'AWS-DEV-CC' and a 'Description' text area with 'Development CCs in AWS'. At the bottom of the main panel are 'Cancel' and 'Next' buttons. A copyright notice at the very bottom of the screen reads 'Copyright © 2007-2022 Zscaler Inc. All rights reserved. | Version 1.0 | [Patents](#)'.

- c. Click **Next**.
- d. In the Location Template dropdown menu, select the **Location Template** you created in the previous steps.
- e. Click **Next**.
- f. Leave the VM size as **Small**, and click **Next**.
- g. Complete the workflow by clicking **Save**.
- h. In the screen that appears, note the **Provisioning URL**.

Lab 2: Managing Location and Provisioning Templates



The screenshot shows the Zscaler Cloud Connector configuration interface. On the left, there's a sidebar with various navigation options: Dashboard, Analytics, Administration (selected), Forwarding, Search, Activation, and User Management. The main panel displays a 'Provisioning URL' configuration screen. At the top, a message says 'All changes have been saved.' Below it, a list of steps is shown: Name, Cloud: Amazon Web Services, Location, Group Information, and Review. The 'Location' step is currently active. The 'Provisioning URL' section contains the URL 'connector.zscalertwo.net/api/v1/provUrl?name=AWS-DEV-CC'. To the right of the URL is a 'Copy Provisioning URL' button, which is highlighted by a red arrow. Below this, sections for 'LOCATION INFORMATION' (Location Template: DEV-Locations, Location Name: Automatic) and 'GROUP INFORMATION' (No. of Cloud Connector Groups: Automatic, Virtual Machine Size: Small) are displayed. At the bottom of the main panel is a 'Done' button.

Note: The Provisioning URL is used as part of the bootstrapping process of a Cloud Connector appliance. When the appliance boots, this URL tells the appliance how to “dial home” and inherit the correct Location settings.

- i. Click Done.

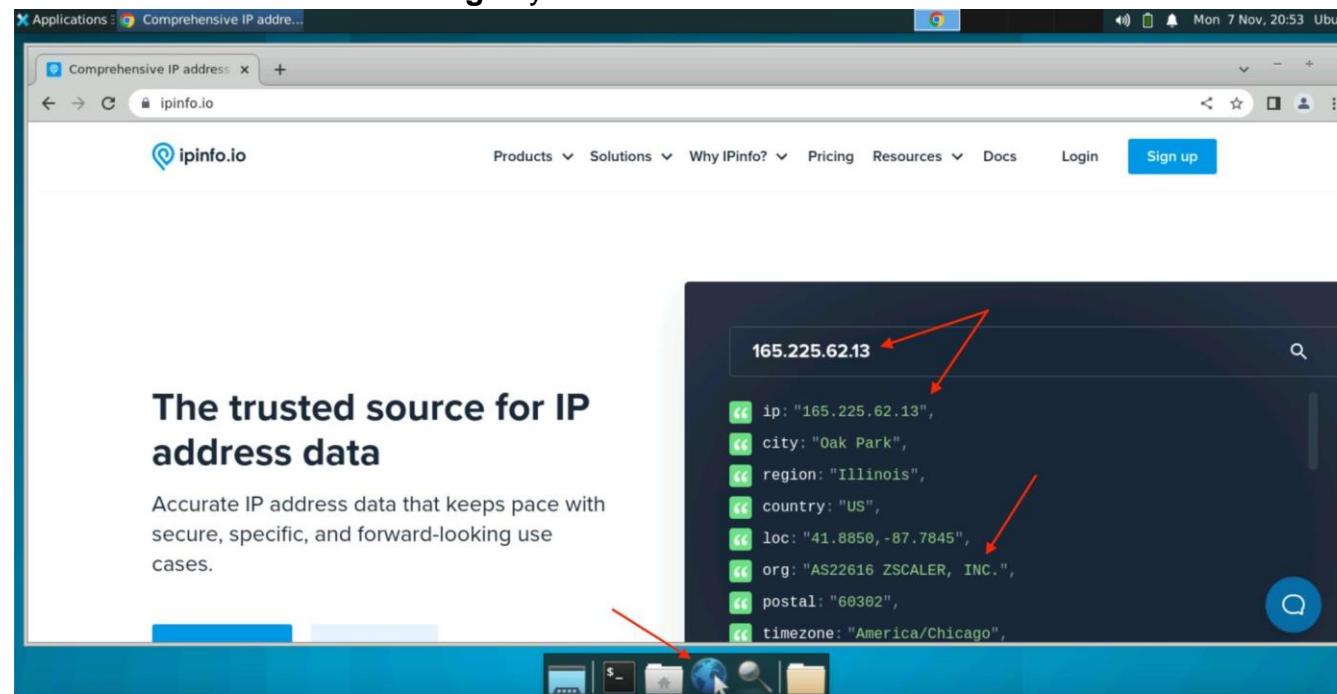
Lab 3: Managing Traffic Forwarding Policy

Throughout this lab, you'll have access to two separate test machines: Region1 Workload and Region2 Workload. Both of these machines send their traffic to the internet via their respective Cloud Connector and, hence, the Zscaler Zero Trust Exchange, which includes ZIA. In this section, we'll experiment with Traffic Forwarding Policy within the Cloud Connector portal. Traffic Forwarding Policies allow you to manipulate how traffic is processed within the Cloud Connector.

Task 1: Verify Internet Connection

In this task, you will check how one of your workloads' currently connects to the Internet.

1. From your pod dashboard, access your **Region1** Workload by clicking on it.
2. In the console of your machine, open a web browser and browse to <https://www.ipinfo.io>.
3. Note the **IP Address** and **Org** of your workload.



Note: This traffic reached the Internet via ZIA and used one of Zscaler's public IP addresses.

Task 2: Configure a Traffic Forwarding Rule

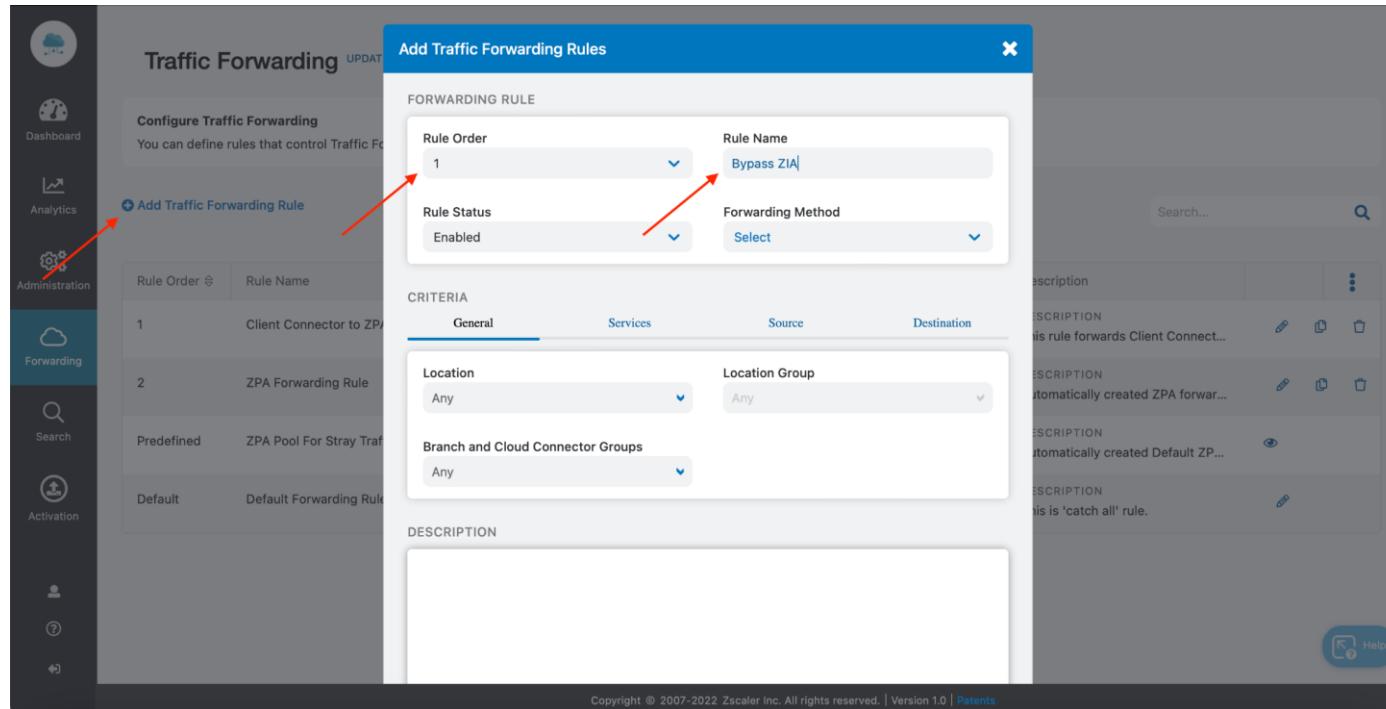
Let's assume that you'd like to prevent this traffic from using ZIA and, instead, go directly out to the Internet from AWS. In this task, you will configure a Traffic Forwarding Policy and then verify its impact on a workload's traffic.

1. In the Cloud Connector portal, select **Forwarding > Traffic Forwarding**.
-

Note: You will see a few default rules installed automatically when the Cloud Connector registered. These rules triggered when you sent traffic to <https://www.ipinfo.io> (specifically, the Default ZIA rule).

2. Click **Add Traffic Forwarding Rule**.
3. Configure the rule as follows:
 - a. Change the Rule Order to **1** to ensure your new rule is placed at the top.
 - b. Enter a **Name**.

Lab 3: Managing Traffic Forwarding Policy



The screenshot shows the Zscaler Traffic Forwarding Rules interface. On the left, there's a sidebar with various navigation options: Dashboard, Analytics, Administration, Forwarding (which is selected and highlighted in blue), Search, Activation, and Help. The main area is titled "Traffic Forwarding" and contains a table of existing rules:

Rule Order	Description
1	Client Connector to ZPA
2	ZPA Forwarding Rule
Predefined	ZPA Pool For Stray Traffic
Default	Default Forwarding Rule

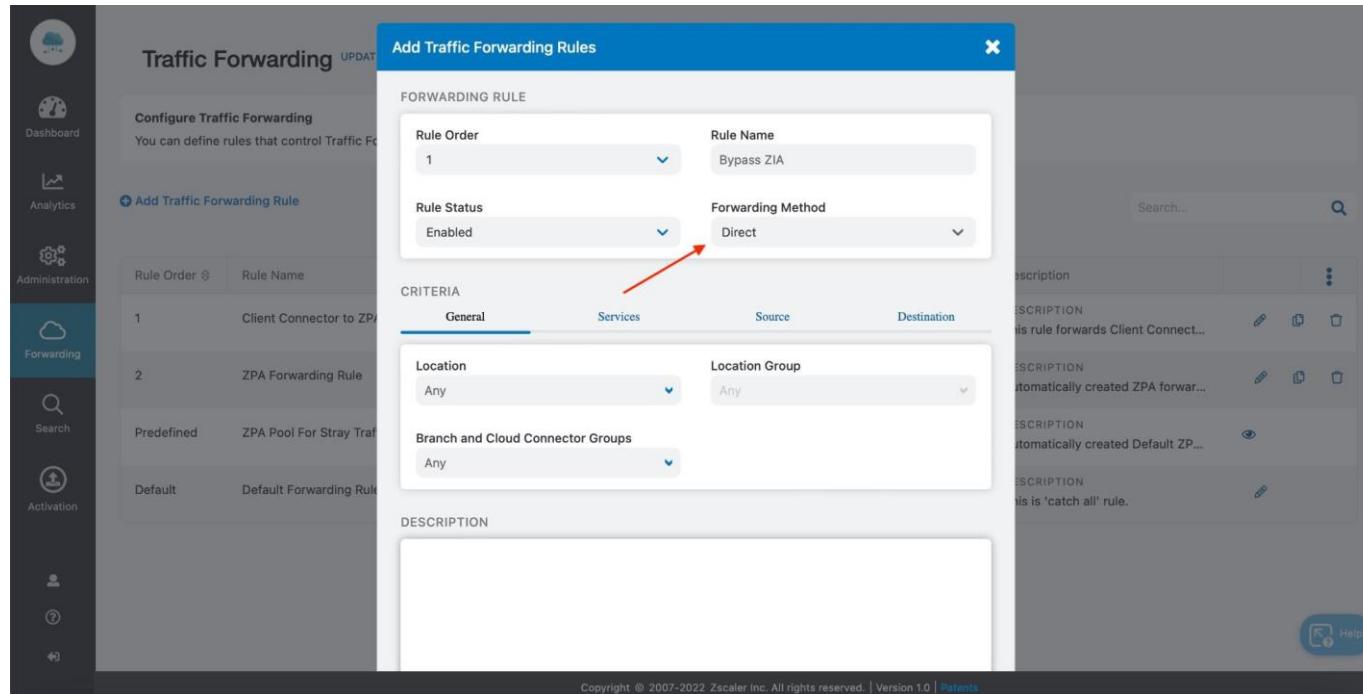
A modal window titled "Add Traffic Forwarding Rules" is open over the table. It has several input fields:

- "Rule Order": Set to 1.
- "Rule Name": "Bypass ZIA".
- "Rule Status": "Enabled".
- "Forwarding Method": A dropdown menu currently set to "Select".
- "CRITERIA" tab: Contains sections for "General", "Services", "Source", and "Destination". Under "General", there are dropdowns for "Location" (set to "Any") and "Location Group" (set to "Any").
- "DESCRIPTION" section: An empty text area.

Two red arrows point from the text instructions below to the "Rule Order" field and the "Forwarding Method" dropdown.

- c. In the Forwarding Method dropdown, choose the **Direct** option.

Lab 3: Managing Traffic Forwarding Policy



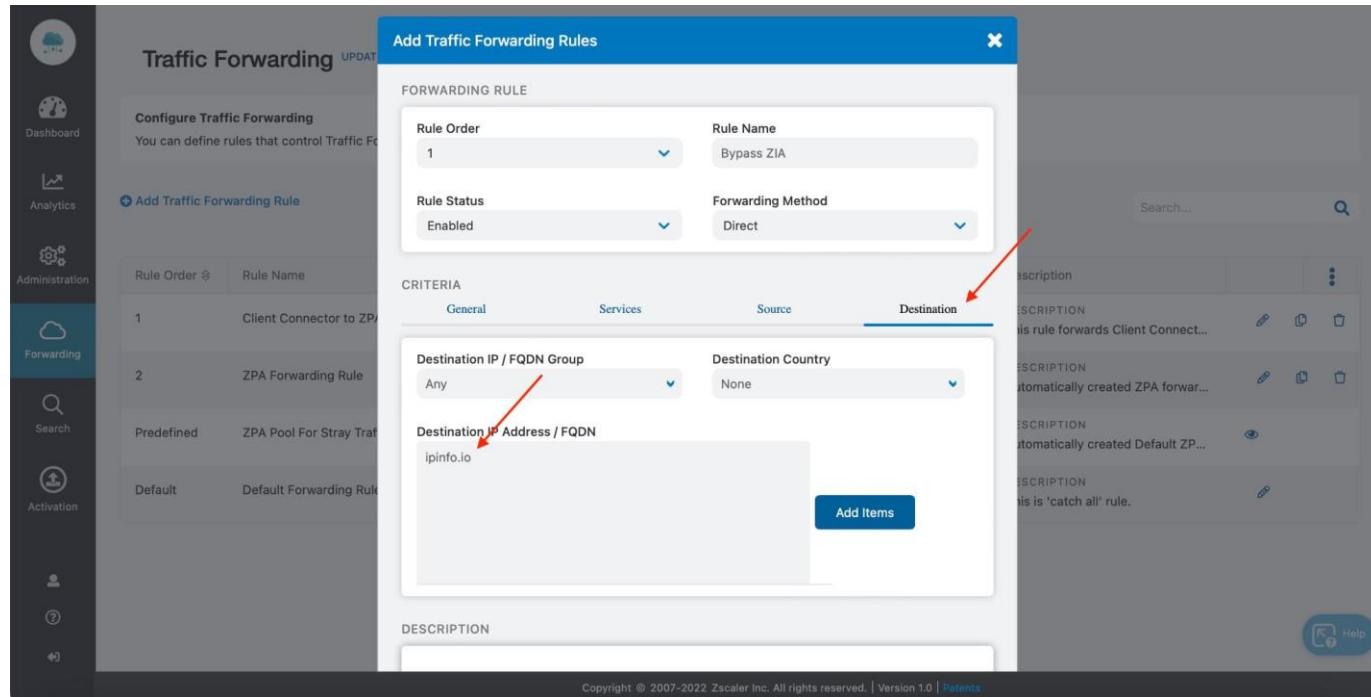
The screenshot shows the Zscaler UI for managing traffic forwarding rules. The main interface on the left lists existing rules: 'Client Connector to ZPA', 'ZPA Forwarding Rule', 'ZPA Pool For Stray Traf', and 'Default Forwarding Rule'. The central window is titled 'Add Traffic Forwarding Rules' and contains the following fields:

- FORWARDING RULE**
 - Rule Order:** 1
 - Rule Name:** Bypass ZIA
 - Rule Status:** Enabled (highlighted with a red arrow)
 - Forwarding Method:** Direct
- CRITERIA** tab (General selected)
 - Location:** Any
 - Location Group:** Any
 - Branch and Cloud Connector Groups:** Any
- DESCRIPTION** field (empty)

Note: In the Criteria section, you can select all of the options available for identifying which traffic will adhere to this rule.

- d. Click the **Destination** tab.
- e. In the Destination IP Address / FQDN field, enter **ipinfo.io**.

Lab 3: Managing Traffic Forwarding Policy




You may have noticed other Forwarding Methods when you created the Direct rule. The Zscaler Internet Access (ZIA) option, as implied, will allow traffic matching the criteria defined to be forwarded to the ZIA cloud for inspection.

By default, for ZIA customers, a rule will be automatically created for you to send all traffic to ZIA. The Zscaler Private Access (ZPA) option allows traffic that matches the criteria defined to be forwarded to the ZPA cloud. Cloud Connector automatically downloads ZPA Application Segments from your ZPA portal. Hence, any traffic it receives that is destined to these segments will be proxied, assuming it is permitted within the ZPA Access Policy and Client Forwarding Policy.

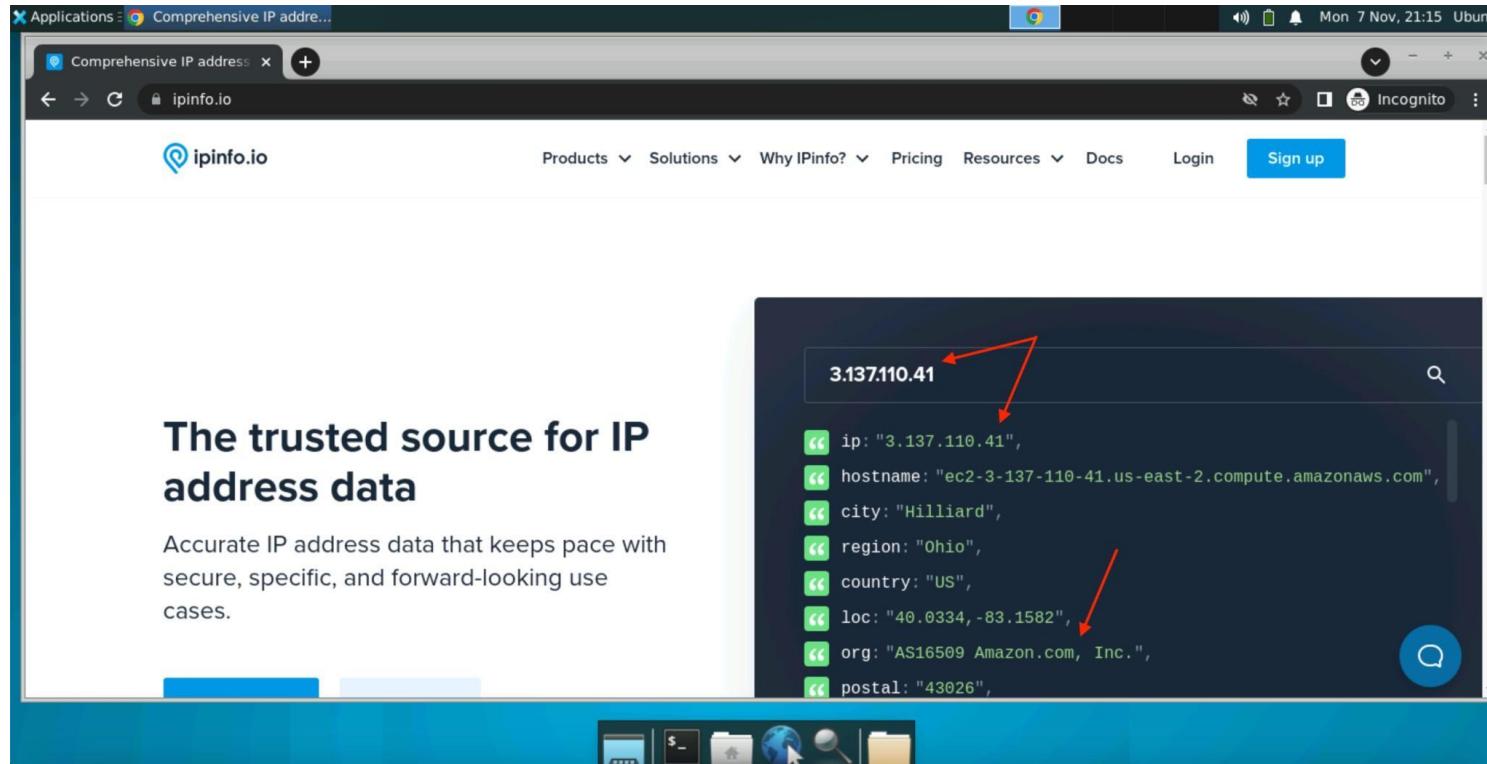
Similar to ZIA, for ZPA customers, a default rule will be added automatically to ensure ZPA-bound traffic is automatically forwarded to the ZPA Broker.

- Click **Save**, then **Activate** your changes.

Note: You may need to give the system 1-2 minutes for the change to take effect.

5. Return to your **Region1** Workload console and open a new browser window (we recommend that this be an Incognito window to avoid browser caching issues).
6. Navigate to <https://www.ipinfo.io> again and review the results.
7. Note the **IP Address** and **Org** of your workload.
8. Verify that this traffic now exits AWS directly as evidenced by the IP Address and Org. Feel free to experiment with additional Traffic Forwarding Rules.

Lab 3: Managing Traffic Forwarding Policy



The screenshot shows a web browser window with the URL ipinfo.io. The page displays the following JSON data for the IP address 3.137.110.41:

```
3.137.110.41
{
  "ip": "3.137.110.41",
  "hostname": "ec2-3-137-110-41.us-east-2.compute.amazonaws.com",
  "city": "Hilliard",
  "region": "Ohio",
  "country": "US",
  "loc": "40.0334,-83.1582",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "43026"
}
```

A red arrow points from the IP address "3.137.110.41" in the JSON output back to the input field on the left side of the page.



- You may have noticed other Forwarding Policy types in the Forwarding menu of the Cloud Connector portal.
- **Log and Control Policies** allow an administrator to identify control-plane traffic from specific cloud locations and redirect this traffic to a specified Zscaler Logging Gateway.
 - **DNS Policies** find their usefulness with regards to ZPA use cases, which we'll discuss in a future lab. Cloud Connector proxies ZPA traffic via synthetic IP Addressing hosted within the appliance. Administrators can use DNS Policies to allow, block, and forward DNS requests for ZPA-bound traffic. Furthermore, when forwarding to ZPA, DNS Policies also allow the administrator to specify the synthetic IP ranges used.

Whether using DNS Policies, Log and Control or Traffic Forwarding, each of the three options permits the administrator to define a range of match criteria. This lab focused only on Traffic Forwarding Policies, but the workflow remains roughly the same regardless of the policy chosen.

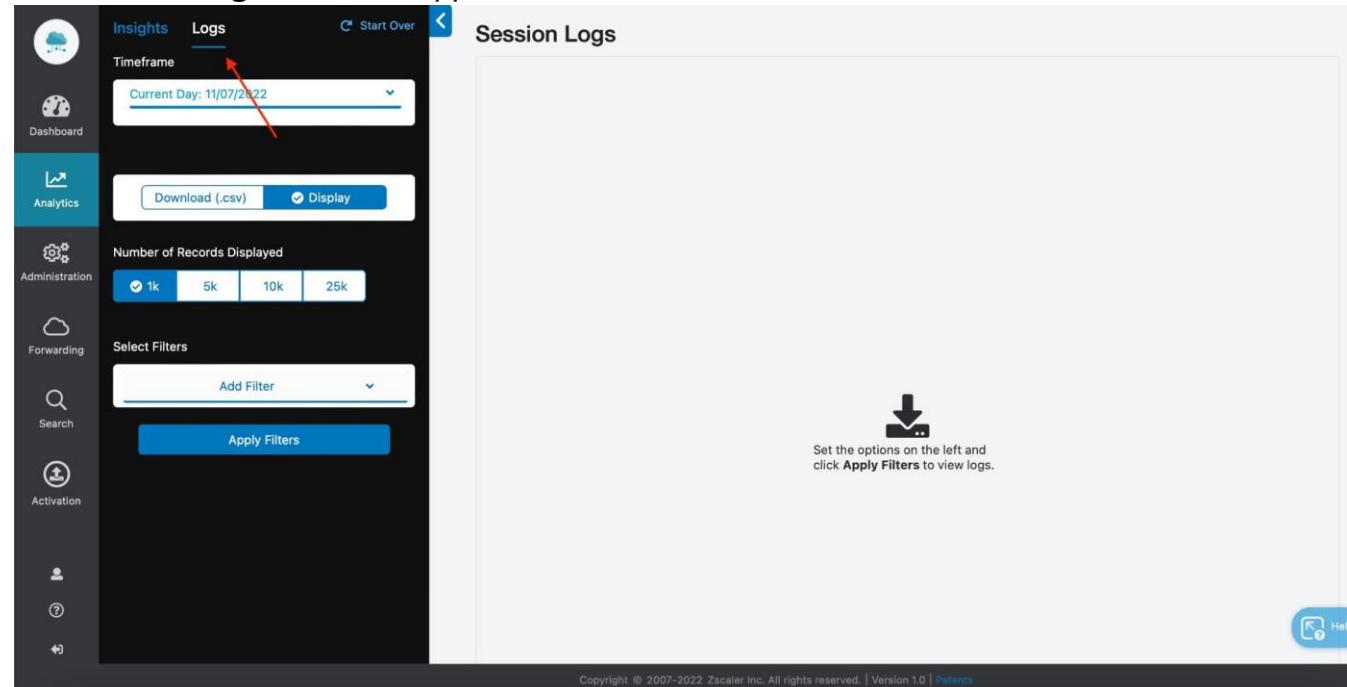
Lab 4: Using Analytics and Logging

Now that we've generated some traffic through our Cloud Connectors, let's review some of the logging that's available. Remember, Cloud Connector portal provides a new vantage point for logging of traffic before it reaches the Zero Trust Exchange. This allows you to ensure traffic not only reaches the appliance, but is routed to the correct Zscaler service.

Task 1: Review Insights Logs

In this task, you will access and filter logs to review details for each transaction processed by Zscaler

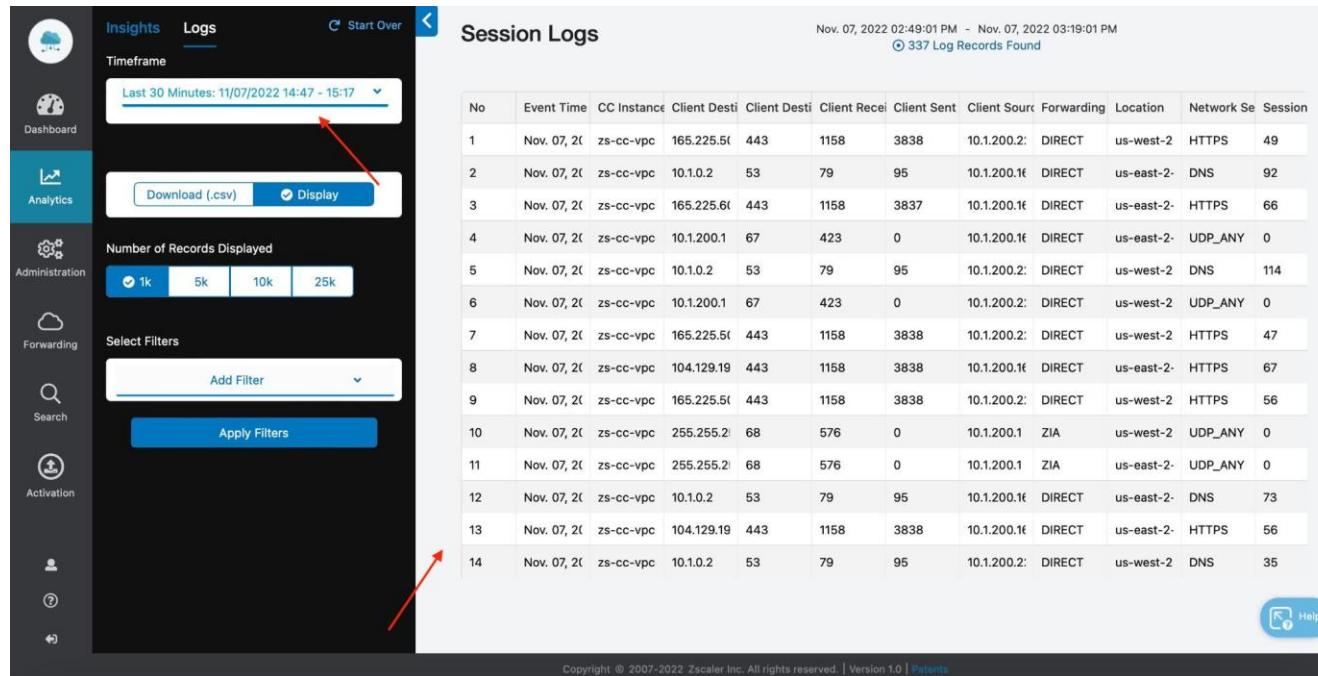
1. In the Cloud Connector portal, select **Analytics > Session Insights**.
2. Click the **Logs** tab in the upper left.



The screenshot shows the Zscaler Cloud Connector portal interface. The left sidebar has icons for Dashboard, Analytics (which is selected), Administration, Forwarding, Search, Activation, and Help. The main content area has a header with 'Insights' and 'Logs' tabs, where 'Logs' is underlined. Below the tabs are 'Timeframe' (set to 'Current Day: 11/07/2022'), 'Download (.csv)', and 'Display' buttons. There are also buttons for 'Number of Records Displayed' (1k, 5k, 10k, 25k) and 'Select Filters' (with 'Add Filter' and 'Apply Filters' buttons). To the right, a large area is labeled 'Session Logs' with a download icon and the text 'Set the options on the left and click Apply Filters to view logs.' At the bottom, there is a copyright notice: 'Copyright © 2007-2022 Zscaler Inc. All rights reserved. | Version 1.0 | Patents'.

3. Change the Timeframe to **Last 30 Minutes** and click **Apply Filters**.

Lab 4: Using Analytics and Logging



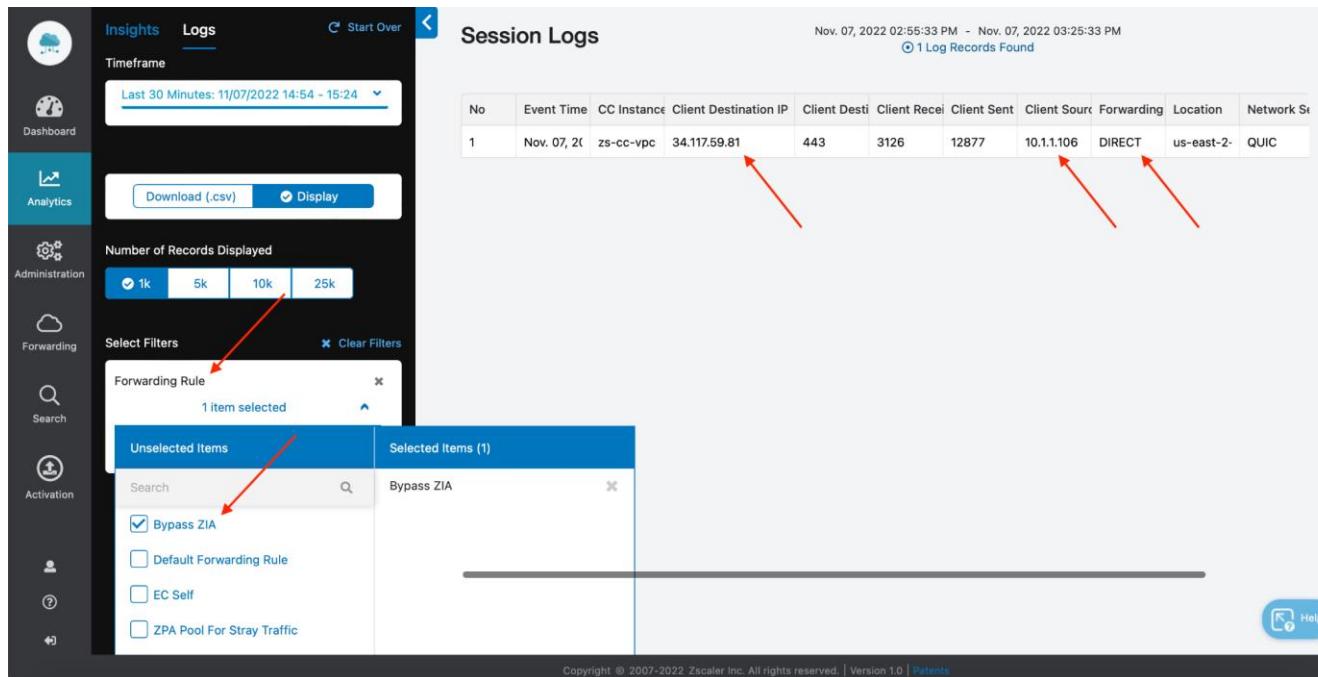
The screenshot shows the Zscaler Analytics and Logging interface. On the left, there's a sidebar with various navigation options: Insights, Dashboard, Analytics, Administration, Forwarding, Search, Activation, and User. The 'Logs' tab is selected. In the main area, the title 'Session Logs' is displayed along with the date range 'Nov. 07, 2022 02:49:01 PM - Nov. 07, 2022 03:19:01 PM' and '337 Log Records Found'. A red arrow points to the 'Timeframe' dropdown menu, which shows 'Last 30 Minutes: 11/07/2022 14:47 - 15:17'. Another red arrow points to the 'Select Filters' section, which includes an 'Add Filter' dropdown and an 'Apply Filters' button. The main content area is a table titled 'Session Logs' with 14 rows of log records. The columns include: No, Event Time, CC Instance, Client Desti, Client Desti, Client Recei, Client Sent, Client Sourc, Forwarding, Location, Network Se, and Session.

No	Event Time	CC Instance	Client Desti	Client Desti	Client Recei	Client Sent	Client Sourc	Forwarding	Location	Network Se	Session
1	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	165.225.56.443	443	1158	3838	10.1.200.2	DIRECT	us-west-2	HTTPS	49
2	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	10.1.0.2	53	79	95	10.1.200.1	DIRECT	us-east-2	DNS	92
3	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	165.225.64.443	443	1158	3837	10.1.200.1	DIRECT	us-east-2	HTTPS	66
4	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	10.1.200.1	67	423	0	10.1.200.1	DIRECT	us-east-2	UDP_ANY	0
5	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	10.1.0.2	53	79	95	10.1.200.2	DIRECT	us-west-2	DNS	114
6	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	10.1.200.1	67	423	0	10.1.200.2	DIRECT	us-west-2	UDP_ANY	0
7	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	165.225.56.443	443	1158	3838	10.1.200.2	DIRECT	us-west-2	HTTPS	47
8	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	104.129.19	443	1158	3838	10.1.200.1	DIRECT	us-east-2	HTTPS	67
9	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	165.225.56.443	443	1158	3838	10.1.200.2	DIRECT	us-west-2	HTTPS	56
10	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	255.255.2	68	576	0	10.1.200.1	ZIA	us-west-2	UDP_ANY	0
11	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	255.255.2	68	576	0	10.1.200.1	ZIA	us-east-2	UDP_ANY	0
12	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	10.1.0.2	53	79	95	10.1.200.1	DIRECT	us-east-2	DNS	73
13	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	104.129.19	443	1158	3838	10.1.200.1	DIRECT	us-east-2	HTTPS	56
14	Nov. 07, 2022 02:49:01 PM	zs-cc-vpc	10.1.0.2	53	79	95	10.1.200.2	DIRECT	us-west-2	DNS	35

4. Review the log details for a transaction, including the 5-tuple information on flows seen by the Cloud Connector as well as the disposition of the traffic (where it was sent).
5. Experiment with the available filtering options. For example, try to find the traffic to <https://www.ipinfo.io> you sent earlier.

Hint: Try filtering by Forwarding Rule.

Lab 4: Using Analytics and Logging



The screenshot shows the Zscaler Session Logs interface. On the left, a sidebar lists various navigation options: Insights (selected), Logs, Dashboard, Analytics, Administration, Forwarding, Search, Activation, and Help. The main area is titled "Session Logs" and displays a single log record from November 7, 2022, between 02:55:33 PM and 03:25:33 PM. The log details a DNS query from client IP 34.117.59.81 to port 443, received by port 3126, sent by port 12877, and originating from client source 10.1.1.106 via a DIRECT connection. The log also notes the location as us-east-2 and the network as QUIC. Below the log table, there are download and display buttons. A "Select Filters" section is open, showing a "Forwarding Rule" filter applied, with one item selected: "Bypass ZIA". Other unselected items include "Default Forwarding Rule", "EC Self", and "ZPA Pool For Stray Traffic". The sidebar also includes a "Number of Records Displayed" section with buttons for 1k, 5k, 10k, and 25k.

No	Event Time	CC Instance	Client Destination IP	Client Desti	Client Recei	Client Sent	Client Sourc	Forwarding	Location	Network S
1	Nov. 07, 2022 02:55:33 PM	zs-cc-vpc	34.117.59.81	443	3126	12877	10.1.1.106	DIRECT	us-east-2-	QUIC



DNS Insights provides visibility into DNS traffic that crosses the appliance. This is particularly useful in ZPA use cases in which the appliance is proxying traffic using synthetic IP addresses, but it also provides a bit of visibility into the domains being queried by cloud workloads that are outside the organization. You'll find information on the DNS request itself, the resolved IP, and the disposition of the traffic.

Tunnel Insights provides a glimpse into the data tunnels that are created from the appliance toward the Zero Trust Exchange. Here, you can view the source VPC or VNet the Cloud Connector sits within, its public IP, and the Zscaler IP address used to terminate the far end of the data tunnel.

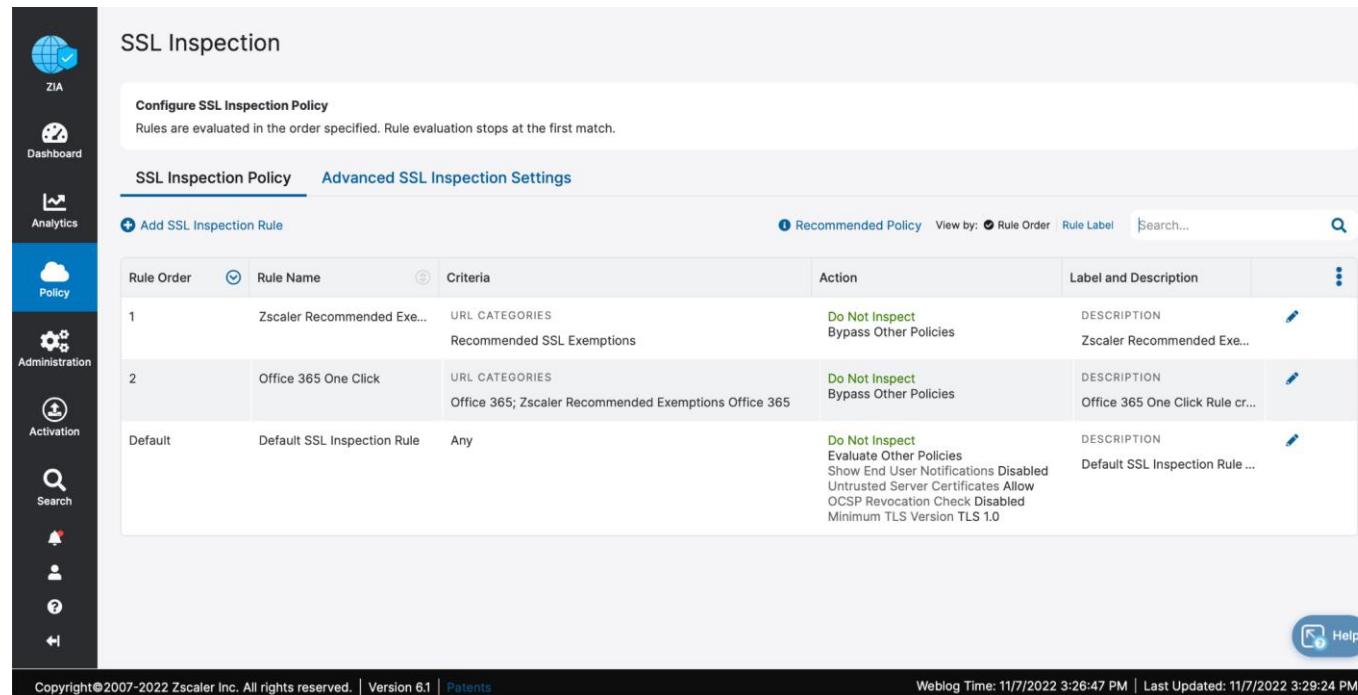
Lab 5: Enforcing Minimum TLS Versions

Now that we have traffic flowing through the Cloud Connector and into ZIA, let's create some security policy to keep our cloud workloads secure. With known vulnerabilities in earlier versions of TLS—namely TLS 1.0 and 1.1—these protocol versions should no longer be used.

Task 1: Configure SSL Inspection Policy

In this task, you will configure a ZIA SSL Inspection policy to enforce the minimum TLS version as 1.2.

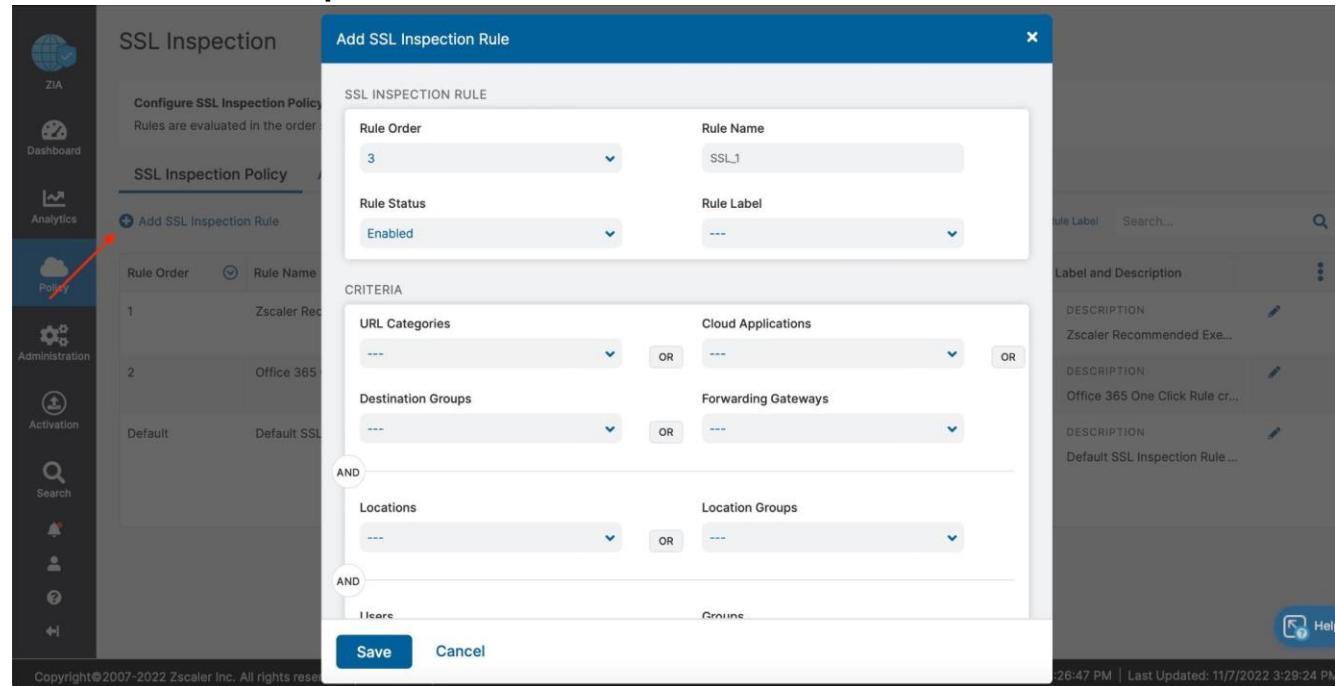
1. Navigate to the **ZIA Admin Portal URL** and log in using the credentials provided previously.
2. Select **Policy > ACCESS CONTROL > SSL Inspection**.



Rule Order	Rule Name	Criteria	Action	Label and Description	More Options
1	Zscaler Recommended Ex...	URL CATEGORIES Recommended SSL Exemptions	Do Not Inspect Bypass Other Policies	DESCRIPTION Zscaler Recommended Ex...	
2	Office 365 One Click	URL CATEGORIES Office 365; Zscaler Recommended Exemptions Office 365	Do Not Inspect Bypass Other Policies	DESCRIPTION Office 365 One Click Rule cr...	
Default	Default SSL Inspection Rule	Any	Do Not Inspect Evaluate Other Policies Show End User Notifications Disabled Untrusted Server Certificates Allow OCSP Revocation Check Disabled Minimum TLS Version TLS 1.0	DESCRIPTION Default SSL Inspection Rule ...	

Note: As you can see from the rules listed, the default behavior is to not inspect SSL traffic. However, you will now create a rule to change that.

3. Click Add SSL Inspection Rule.

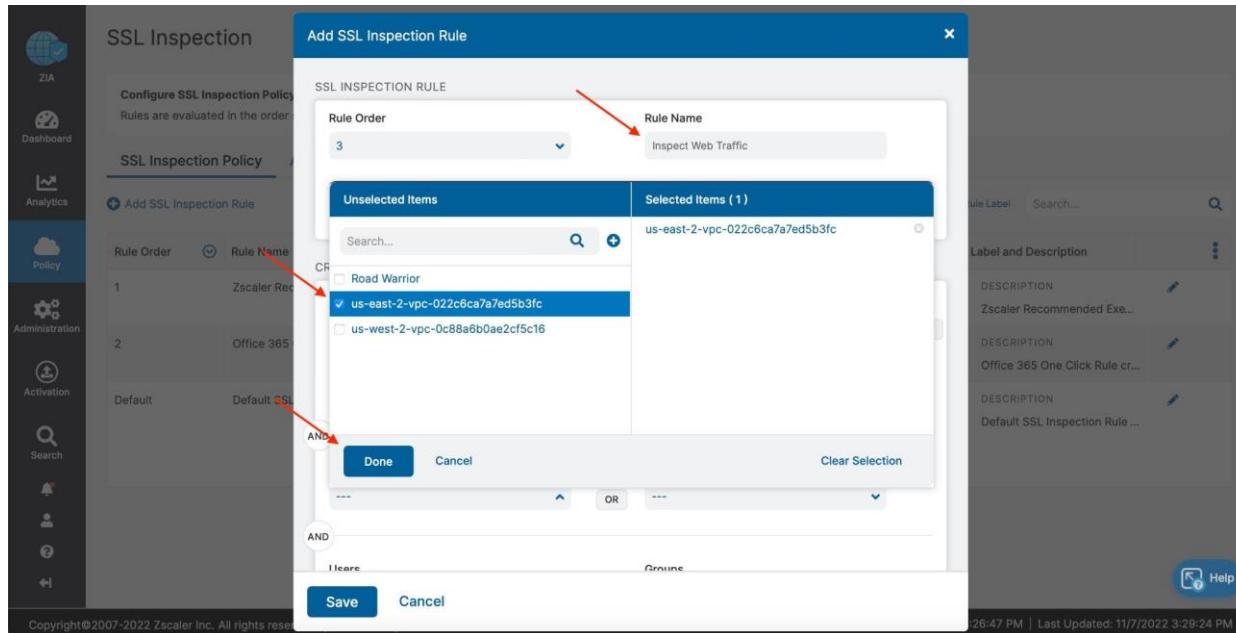


The screenshot shows the Zscaler UI for managing SSL Inspection Rules. On the left, there's a sidebar with various icons: ZIA, Dashboard, Analytics (highlighted with a red arrow), Policy, Administration, Activation, Search, and Notifications. The main area is titled 'SSL Inspection' and shows an 'SSL Inspection Policy'. A sub-menu 'SSL Inspection Policy' is open, displaying a table with two rows: '1 Zscaler Recommended' and '2 Office 365'. Below this is a large 'Add SSL Inspection Rule' dialog box. The dialog has sections for 'Rule Order' (set to 3), 'Rule Name' (SSL_1), 'Rule Status' (Enabled), and 'Rule Label' (set to '...'). The 'CRITERIA' section contains four AND clauses: 'URL Categories OR Cloud Applications', 'Destination Groups OR Forwarding Gateways', 'Locations OR Location Groups', and 'Users OR Groups'. At the bottom of the dialog are 'Save' and 'Cancel' buttons. To the right of the dialog, a sidebar lists existing rules with their descriptions: 'Zscaler Recommended Execution Rule...', 'Office 365 One Click Rule cr...', and 'Default SSL Inspection Rule ...'. The status bar at the bottom right shows '26:47 PM | Last Updated: 11/7/2022 3:29:24 PM'.

4. Configure the rule as follows:

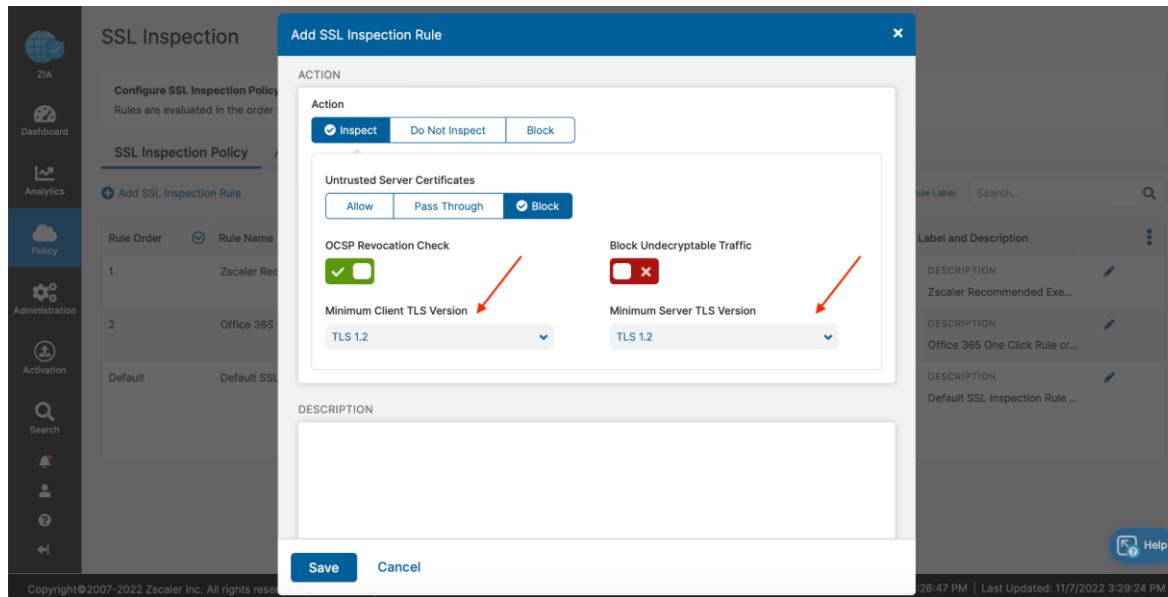
- Enter a **Name**.
- Under the Criteria section, click on **Locations** and select your **Region1** and **Region2** Locations.

Note: The Locations listed take on the naming convention of **Region + VPC ID**. Selecting only Region1 would ensure that this policy only applies to your Region1 workload. Likewise, you also have the option of selecting multiple Locations, or not selecting a Location at all. In this case, this policy would be applied to multiple, or all Locations, respectively.



- Click Done.
- Scroll down to the Action section and, under **Minimum Client TLS Version** and **Minimum Server TLS Version**, select **TLS 1.2**.

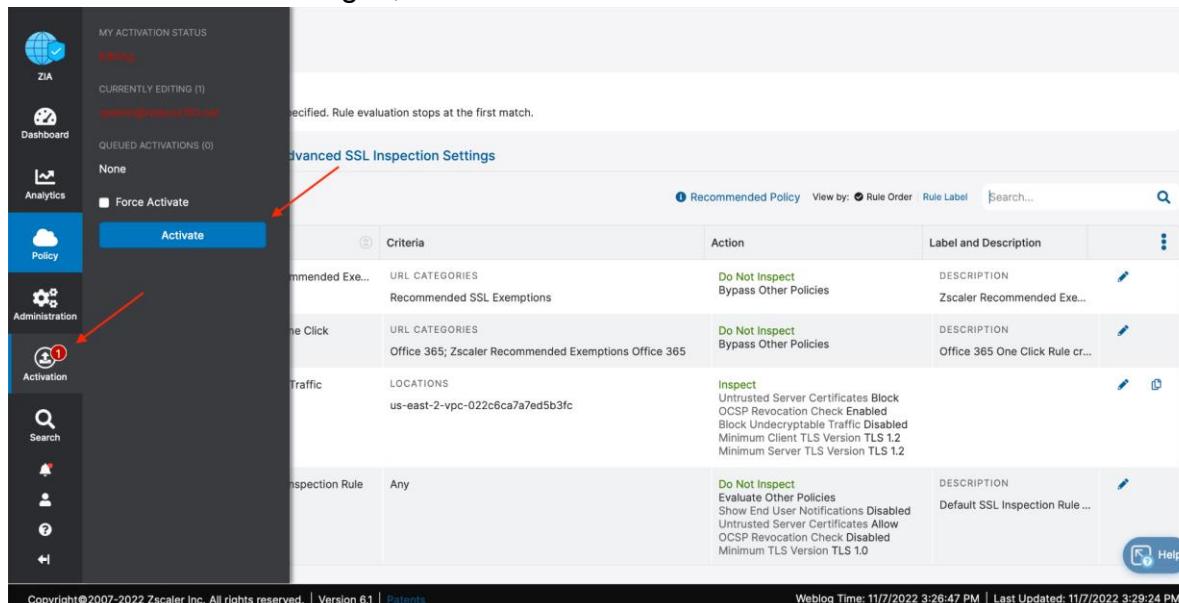
Lab 5: Enforcing Minimum TLS Versions



The screenshot shows the Zscaler SSL Inspection Rule configuration interface. The 'Add SSL Inspection Rule' dialog is open, displaying various settings. A red arrow points to the 'Minimum Client TLS Version' dropdown, which is set to 'TLS 1.2'. Another red arrow points to the 'Minimum Server TLS Version' dropdown, which is also set to 'TLS 1.2'. The background shows a list of existing SSL inspection policies.

5. Click **Save**.

6. To activate the changes, mouse over the **Activation** menu and click **Activate**.



The screenshot shows the Zscaler Activation interface. The 'Activation' menu is highlighted with a red arrow. The 'Activate' button is highlighted with a red arrow. The main pane shows 'Advanced SSL Inspection Settings' with a table of rules. One rule is highlighted with a red arrow, showing 'Criteria' (URL CATEGORIES: Recommended SSL Exemptions), 'Action' (Do Not Inspect, Bypass Other Policies), and 'Label and Description' (Zscaler Recommended Exec...).

Task 2: Verify SSL Inspection Policy

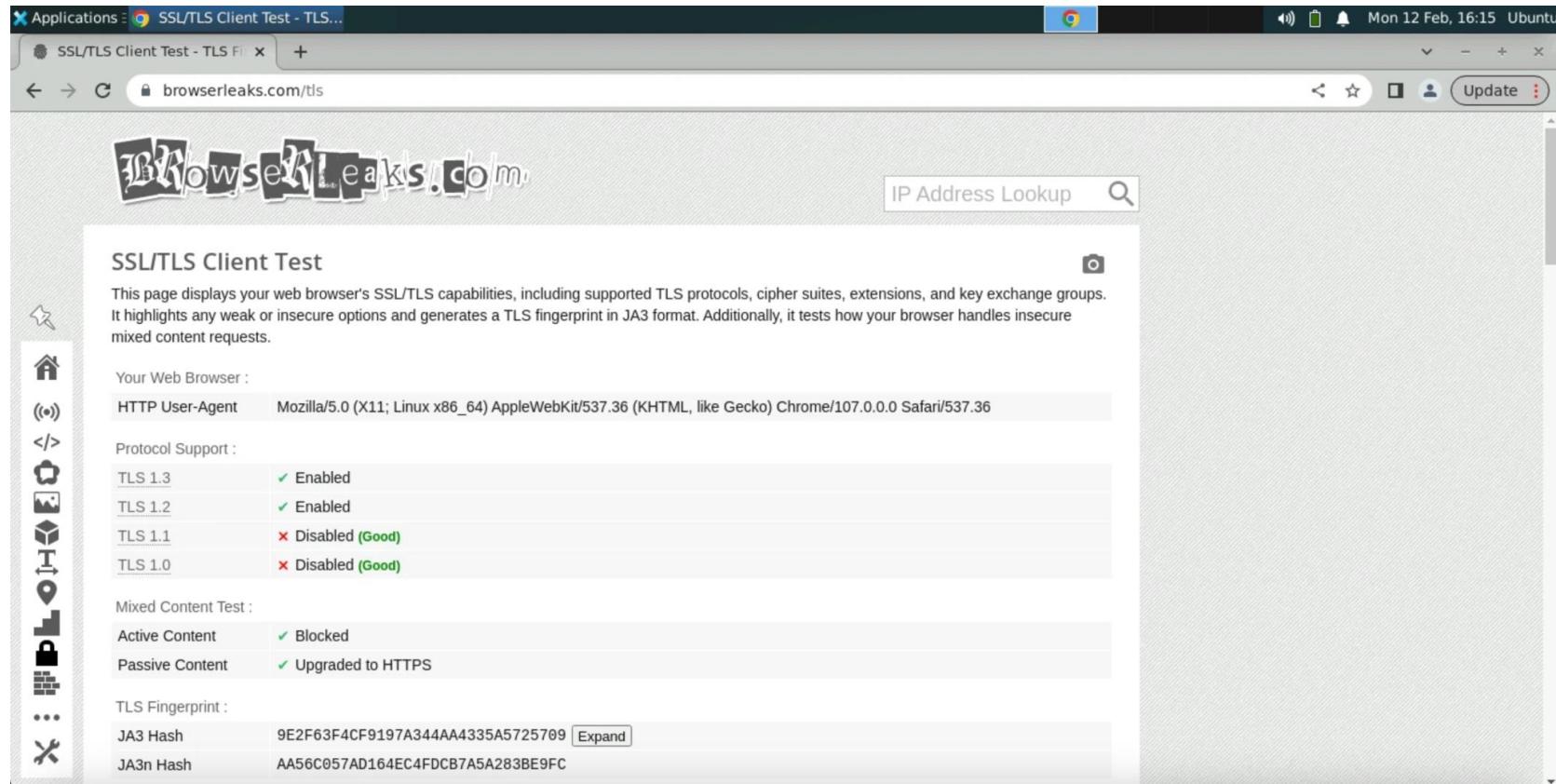
In this task, you will verify that the configured SSL Inspection Policy has the desired effect.

1. Return to the **Region1** Workload, open a web browser and navigate to <https://browserleaks.com/ssl>.
-

Note: The site will automatically begin to test the TLS versions enabled and accessible on your browser.

2. On the page that appears, note the Protocol Support section of the page. Clicking on the links for TLS 1.2 and TLS 1.3 will open a new page that negotiates TLS 1.2 or TLS 1.3, respectively.

Lab 5: Enforcing Minimum TLS Versions



SSL/TLS Client Test

This page displays your web browser's SSL/TLS capabilities, including supported TLS protocols, cipher suites, extensions, and key exchange groups. It highlights any weak or insecure options and generates a TLS fingerprint in JA3 format. Additionally, it tests how your browser handles insecure mixed content requests.

Your Web Browser :

HTTP User-Agent Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36

Protocol Support :

TLS 1.3	Enabled
TLS 1.2	Enabled
TLS 1.1	Disabled (Good)
TLS 1.0	Disabled (Good)

Mixed Content Test :

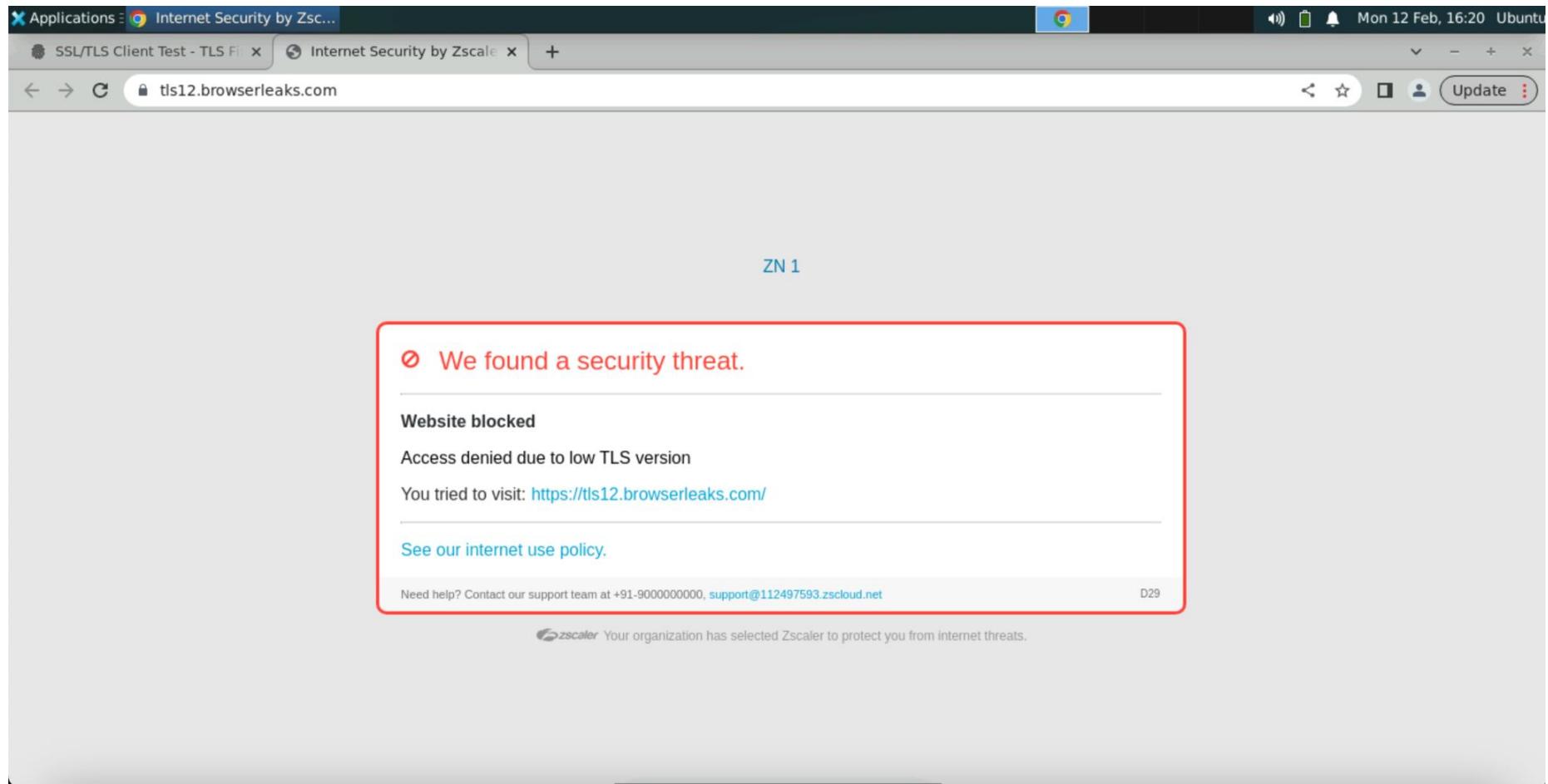
Active Content	Blocked
Passive Content	Upgraded to HTTPS

TLS Fingerprint :

JA3 Hash	9E2F63F4CF9197A344AA4335A5725709	Expand
JA3n Hash	AA56C057AD164EC4FDCB7A5A283BE9FC	

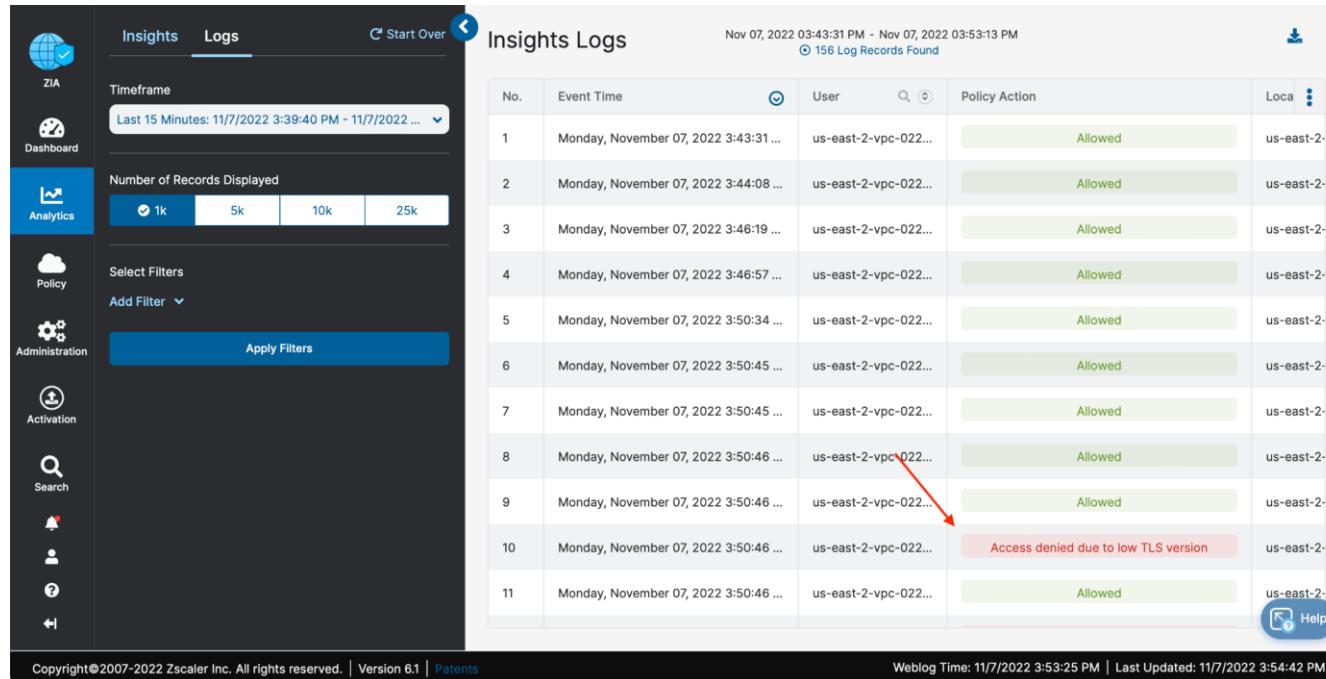
3. Return to the ZIA Admin portal and select **Policy > ACCESS CONTROL > SSL Inspection**.
4. Click the “pencil” icon next to your SSL policy to edit it.
5. Scroll to the Action section and, under **Minimum Client TLS Version** and **Minimum Server TLS Version**, select **TLS 1.3**.
6. Click **Save**.
7. Activate the changes.
8. Return to the **Region1** Workload, and refresh the web browser .
9. You should notice that clicking on the TLS v1.2 (or below) links now result in a **blocked page**. This is because the Zero Trust Exchange is enforcing TLS 1.3 in the environment.

Lab 5: Enforcing Minimum TLS Versions



10. To verify this behavior, return to the ZIA Admin portal and select **Analytics > Web Insights**.
11. Select the **Logs** tab (upper left).
12. Narrow the Timeframe to **Last 15 Minutes** and click **Apply Filters**.

Lab 5: Enforcing Minimum TLS Versions



The screenshot shows the Zscaler Insights Logs interface. The left sidebar includes links for ZIA, Dashboard, Analytics, Policy, Administration, Activation, Search, and Help. The main area has tabs for 'Insights' and 'Logs', with 'Logs' selected. It displays a table of log records from Nov 07, 2022, 03:43:31 PM to Nov 07, 2022, 03:53:13 PM, with 156 log records found. The table columns are No., Event Time, User, Policy Action, Location, and a more options menu. Log entry 10 is highlighted with a red arrow and a callout box stating 'Access denied due to low TLS version'.

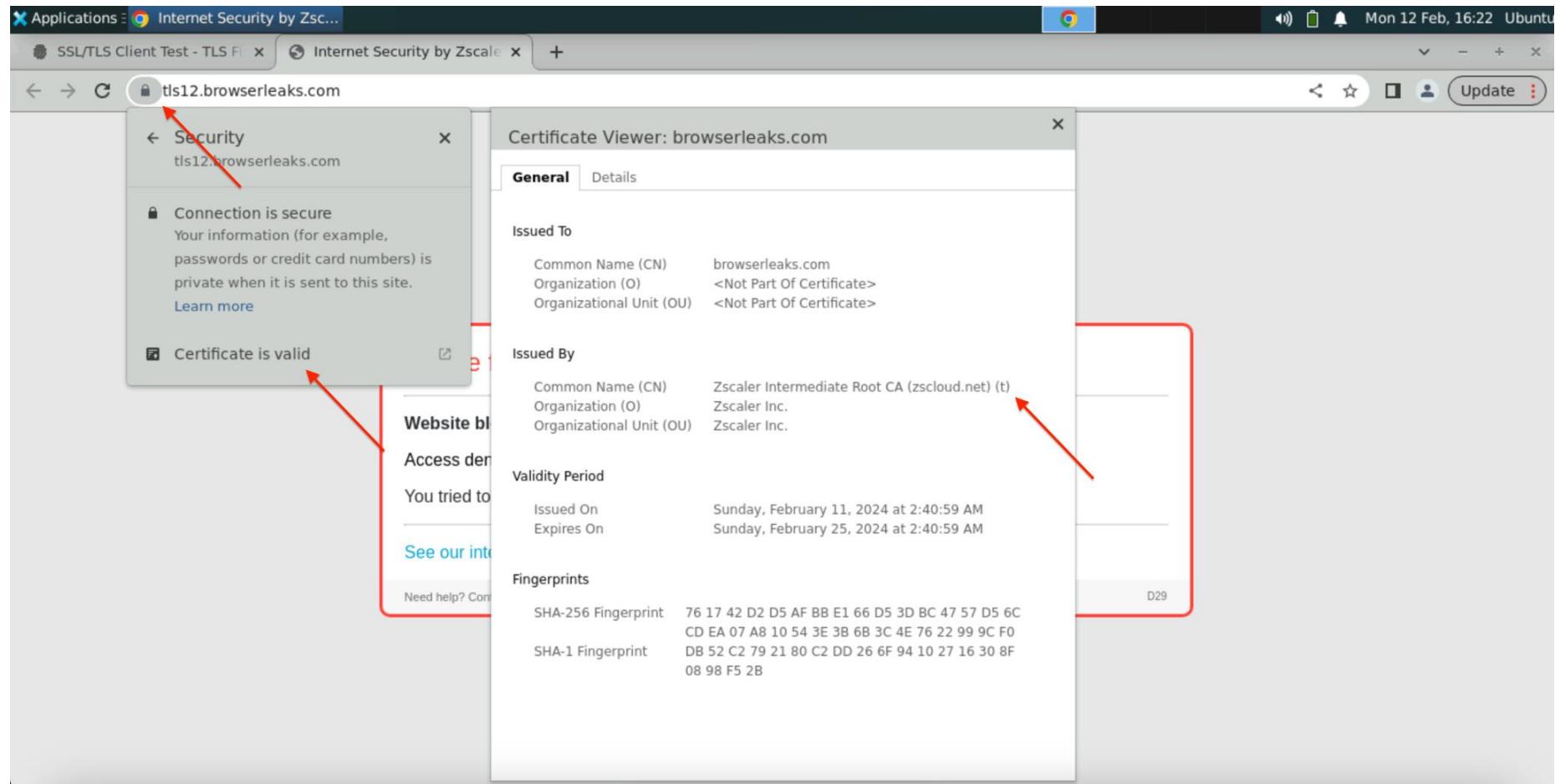
No.	Event Time	User	Policy Action	Loca
1	Monday, November 07, 2022 3:43:31 ...	us-east-2-vpc-022...	Allowed	us-east-2-
2	Monday, November 07, 2022 3:44:08 ...	us-east-2-vpc-022...	Allowed	us-east-2-
3	Monday, November 07, 2022 3:46:19 ...	us-east-2-vpc-022...	Allowed	us-east-2-
4	Monday, November 07, 2022 3:46:57 ...	us-east-2-vpc-022...	Allowed	us-east-2-
5	Monday, November 07, 2022 3:50:34 ...	us-east-2-vpc-022...	Allowed	us-east-2-
6	Monday, November 07, 2022 3:50:45 ...	us-east-2-vpc-022...	Allowed	us-east-2-
7	Monday, November 07, 2022 3:50:45 ...	us-east-2-vpc-022...	Allowed	us-east-2-
8	Monday, November 07, 2022 3:50:46 ...	us-east-2-vpc-022...	Allowed	us-east-2-
9	Monday, November 07, 2022 3:50:46 ...	us-east-2-vpc-022...	Allowed	us-east-2-
10	Monday, November 07, 2022 3:50:46 ...	us-east-2-vpc-022...	Access denied due to low TLS version	us-east-2-
11	Monday, November 07, 2022 3:50:46 ...	us-east-2-vpc-022...	Allowed	us-east-2-

13. Review the log entries and focus on the policy block due to TLS version.

Note: Zscaler proxies SSL connections by inserting itself into the HTTPS exchange. The Cloud Connector appliance does not inspect this traffic.

14. Return to the **Region1** Workload, and in the web browser click the “lock” icon in the upper left (next to the address bar).
 15. Click the **Connection is secure** link, followed by **Certificate is valid**.
 16. Verify that the certificate presented to the workload is actually that of Zscaler, rather than that of the requested website:

Lab 5: Enforcing Minimum TLS Versions



The Zscaler Zero Trust Exchange terminated the connection between your workload and itself, then created a new connection out to the requested website. This allows ZIA to perform man-in-the-middle inspection of encrypted traffic.

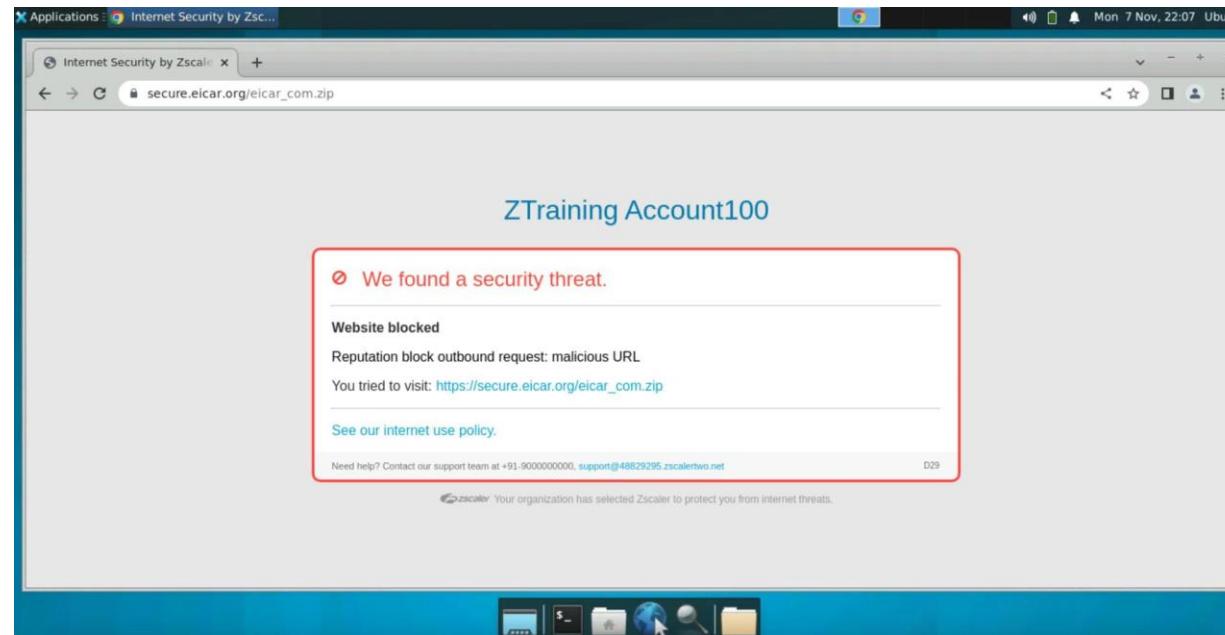
Lab 6: Protecting Against Malicious Payloads, Phishing, and BotNet

So far, you've explored SSL Decryption and enforced minimum TLS versions. Let's now look at what protection Zscaler offers out of the box. Apart from viruses, Zscaler can also detect other threats such as phishing sites and BotNets.

Task 1: Test Zscaler Security Protections

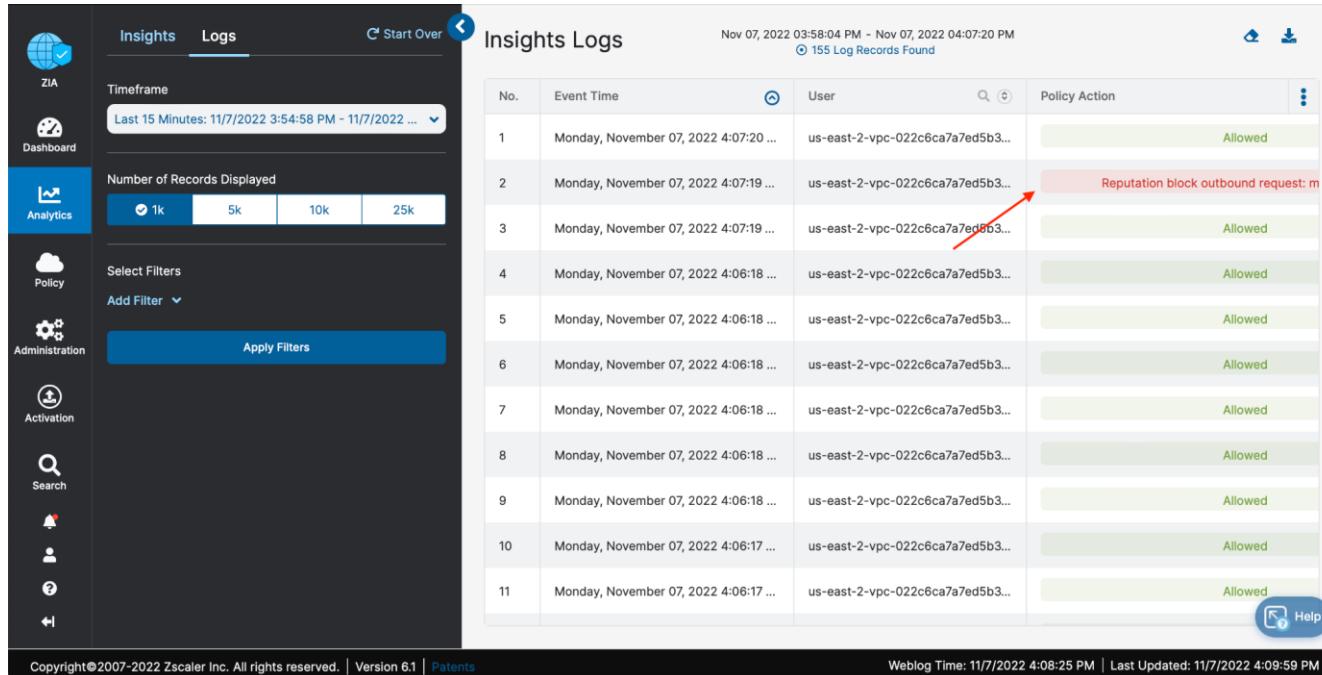
In this task, you will use a well-known test file from EICAR (European Institute for Computer Anti-Virus Research) to trigger ZIA security protections.

1. From the **Region1** Workload, browse to <https://www.eicar.org/download-anti-malware-testfile>.
2. On the right side of the page, click one of the test files to download (eicar.com, eicar.com.txt, eicar_com.zip, etc.).
3. Verify that Zscaler Internet Access automatically blocks this download attempt.



Note: This is because the file contained malicious code. Even malicious files hidden inside compressed archives (ZIP) can be blocked.

4. Return to the ZIA Admin portal and select **Analytics > Web Insights**.
5. Select the **Logs** tab (upper left).
6. View the log entry for the file you just attempted to download.

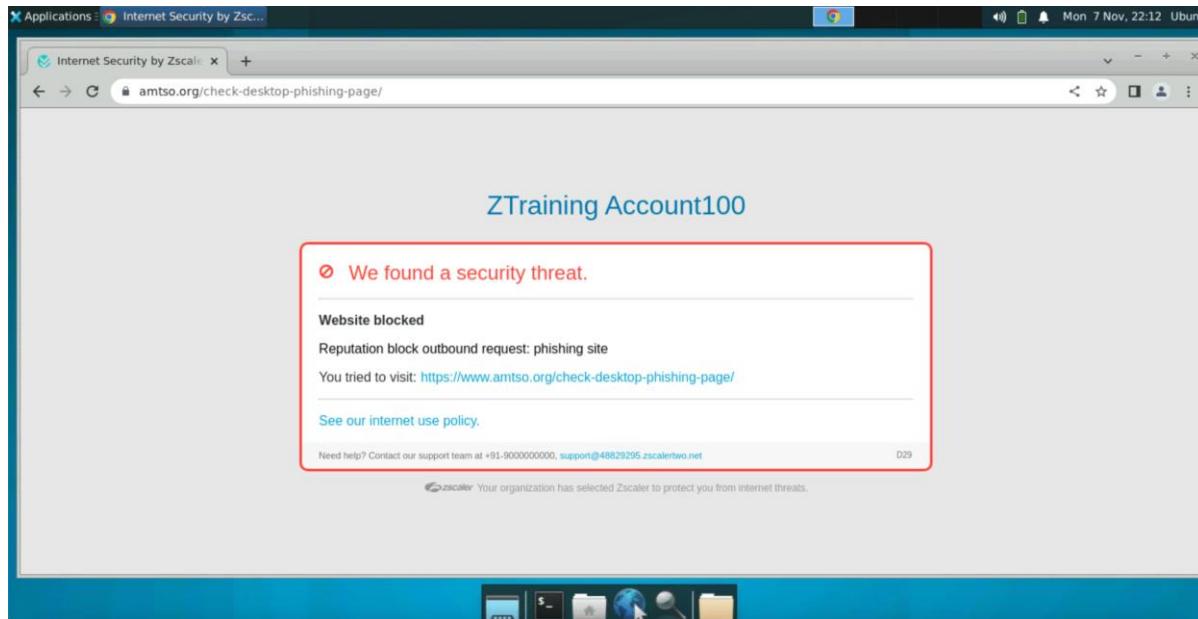


No.	Event Time	User	Policy Action
1	Monday, November 07, 2022 4:07:20 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed
2	Monday, November 07, 2022 4:07:19 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Reputation block outbound request: m
3	Monday, November 07, 2022 4:07:19 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed
4	Monday, November 07, 2022 4:06:18 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed
5	Monday, November 07, 2022 4:06:18 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed
6	Monday, November 07, 2022 4:06:18 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed
7	Monday, November 07, 2022 4:06:18 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed
8	Monday, November 07, 2022 4:06:18 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed
9	Monday, November 07, 2022 4:06:18 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed
10	Monday, November 07, 2022 4:06:17 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed
11	Monday, November 07, 2022 4:06:17 ...	us-east-2-vpc-022c6ca7a7ed5b3...	Allowed

Note: Be patient, it may take 2-3 minutes for logging to catch up.

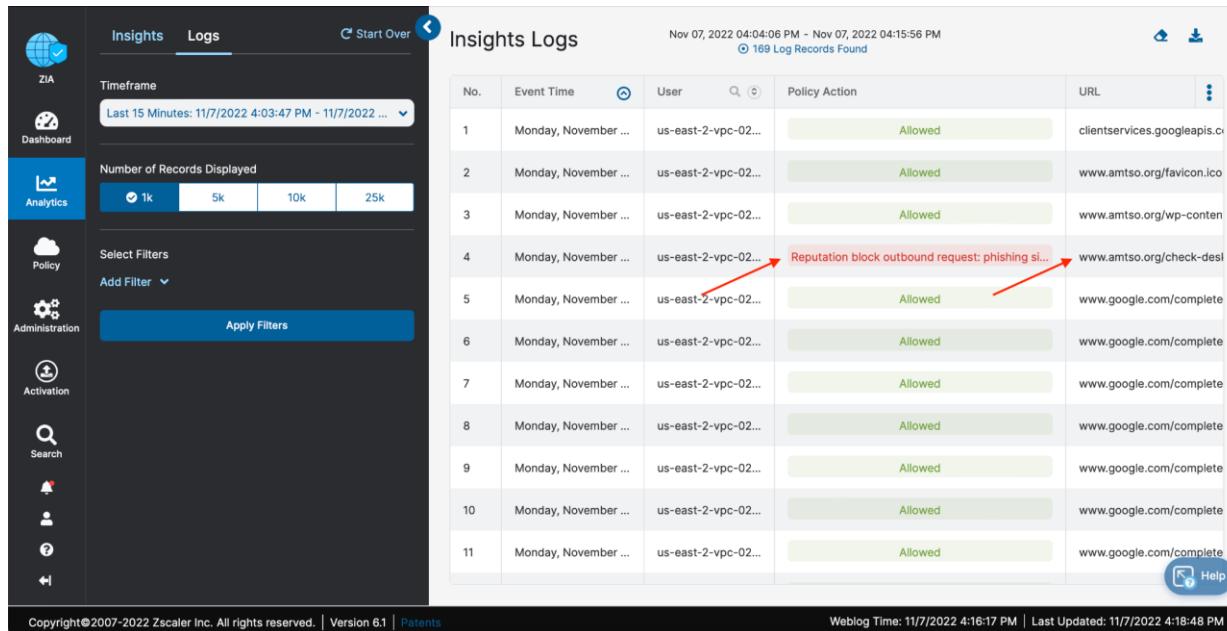
Lab 6: Protecting Against Malicious Payloads, Phishing, and BotNet

7. From your **Region1** Workload, navigate to <https://www.amtso.org/check-desktop-phishing-page>.



8. Verify that the threat was blocked since this is a known phishing site.
9. As before, on the ZIA Admin Portal **Analytics** (Log tab) page, review the log entry for the site you just attempted to visit.

Lab 6: Protecting Against Malicious Payloads, Phishing, and BotNet



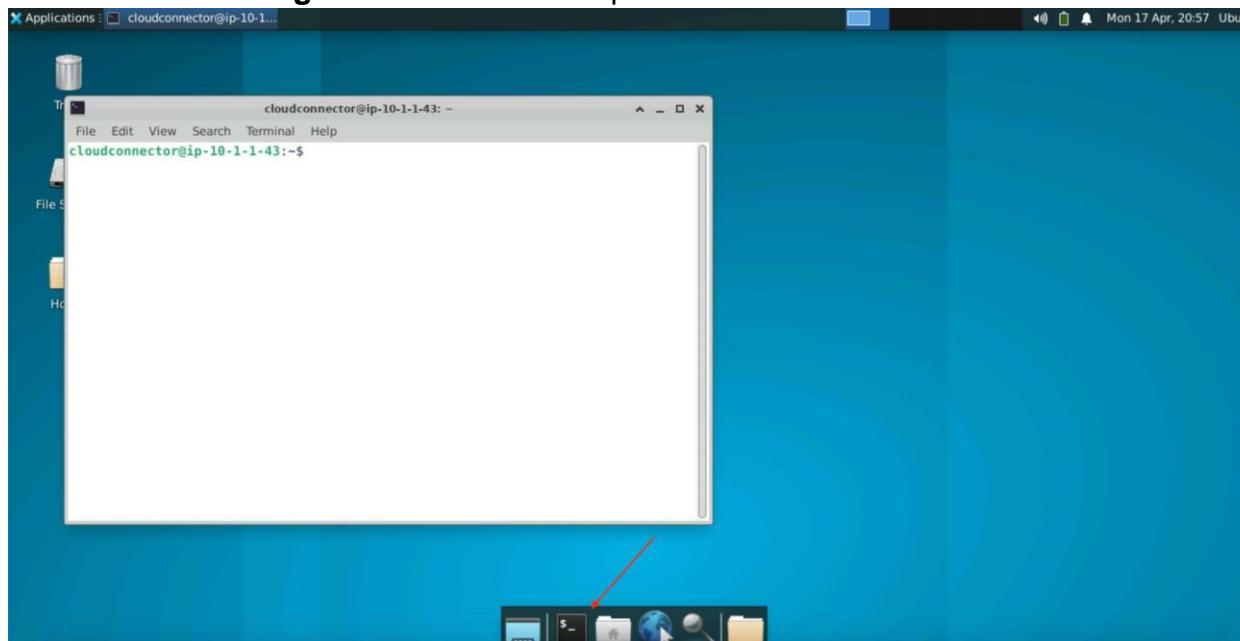
The screenshot shows the Zscaler Cloud UI interface. On the left is a sidebar with various navigation options: ZIA, Dashboard, Analytics, Policy, Administration, Activation, Search, Notifications, and Help. The main area is titled "Insights Logs" and displays a table of log records from November 7, 2022, between 04:04:06 PM and 04:15:56 PM. There are 169 log records found. The columns are No., Event Time, User, Policy Action, and URL. Log entry number 4 is highlighted with a red arrow pointing to the URL column, which shows "www.amtso.org/check-desl". The URL is partially truncated as "Reputation block outbound request: phishing si...".

No.	Event Time	User	Policy Action	URL
1	Monday, November ...	us-east-2-vpc-02...	Allowed	clientservices.googleapis.c...
2	Monday, November ...	us-east-2-vpc-02...	Allowed	www.amtso.org/favicon.ico
3	Monday, November ...	us-east-2-vpc-02...	Allowed	www.amtso.org/wp-conten...
4	Monday, November ...	us-east-2-vpc-02...	Blocked	Reputation block outbound request: phishing si...
5	Monday, November ...	us-east-2-vpc-02...	Allowed	www.google.com/complete
6	Monday, November ...	us-east-2-vpc-02...	Allowed	www.google.com/complete
7	Monday, November ...	us-east-2-vpc-02...	Allowed	www.google.com/complete
8	Monday, November ...	us-east-2-vpc-02...	Allowed	www.google.com/complete
9	Monday, November ...	us-east-2-vpc-02...	Allowed	www.google.com/complete
10	Monday, November ...	us-east-2-vpc-02...	Allowed	www.google.com/complete
11	Monday, November ...	us-east-2-vpc-02...	Allowed	www.google.com/complete

Copyright©2007-2022 Zscaler Inc. All rights reserved. | Version 6.1 | Patents

Weblog Time: 11/7/2022 4:16:17 PM | Last Updated: 11/7/2022 4:18:48 PM

10. Return to the Region1 Workload and open a terminal.



Lab 6: Protecting Against Malicious Payloads, Phishing, and BotNet

11. At the Command Line, enter the following command: **curl -A “BlackSun” www.google.com.**

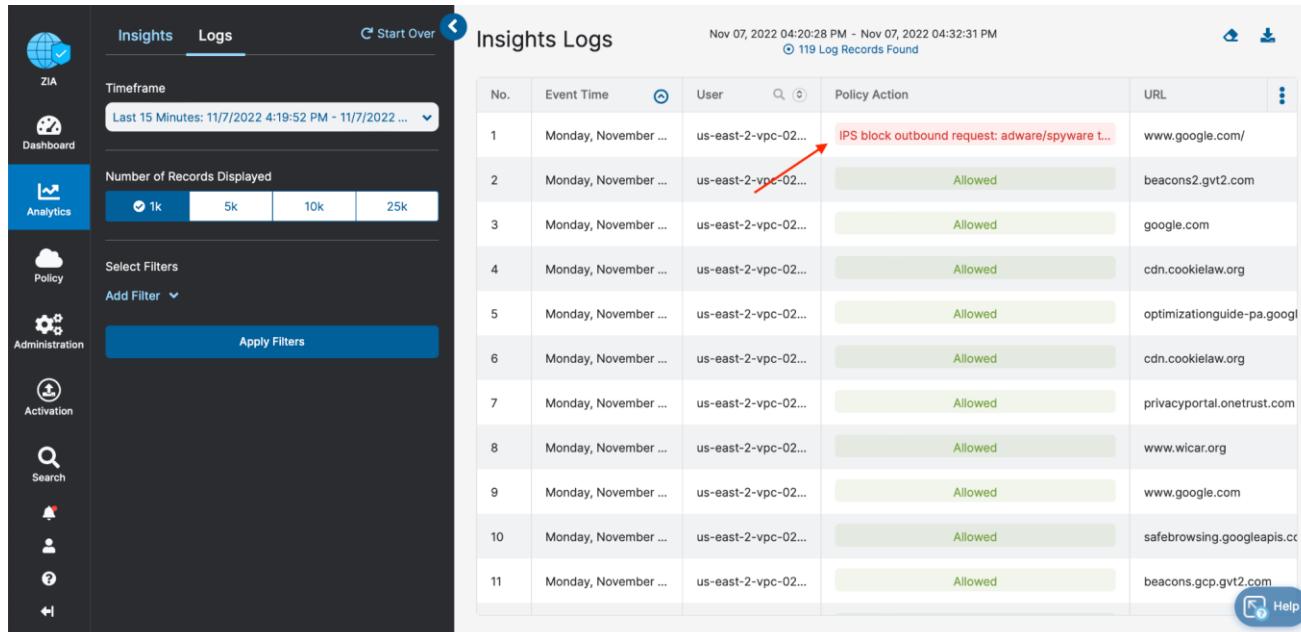
Note: This is a test that spoofs the BlackSun browser agent and will trigger an IPS response from most firewalls.

12. Verify this threat too is blocked by ZIA IPS automatically.

```
<!--locale en_US-->
<table id="en_US" width="100%" border="0" cellspacing="0" cellpadding="0">
<tbody><tr><td class="eu_h">
<i class="a_i"></i>
We found a security threat.
</td></tr>
<tr><td class="hr"><hr></td></tr>
<tr><td class="eu_co">
<b>Website blocked</b>
</td></tr>
<tr><td class="eu_co_rsn">
IPS block outbound request: adware/spyware traffic
</td></tr>
<tr><td class="eu_co">
You tried to visit:<div class="eu_l"><a href="http://www.google.com/">http://www.google.com/</a></div>
</td></tr>
<td class="hr"><hr></td>
</tr>
<tr><td class="eu_co_ln">
<a href="http://48829295.zscalertwo.net/policy.html">
See our internet use policy.
</a>
</td></tr>
<tr><td class="eu_co_fo">
Need help? Contact our support team at +91-9000000000, <a href="mailto:support@48829295.zscalertwo.net">support@48829295.zscalertwo.net</a>
</td></tr>
<tr><td class="eu_co_st_red">
<span class="s_img"></span>
Your organization has selected Zscaler to protect you from internet threats.
</td></tr>
</tbody></table>
<!--/locale en_US-->
</td></tr>
</tbody></table>
</div>
</div>
</body></html>
<!-- 0 0 64 0 1667860352 4 http://www.google.com/ -->cloudconnector@ip-10-1-1-106:~$ █
```

13. On the ZIA Admin Portal Analytics (Log tab) page, review the log entry for this IPS Block.

Lab 6: Protecting Against Malicious Payloads, Phishing, and BotNet



The screenshot shows the Zscaler Insights Logs interface. On the left is a sidebar with various navigation options: ZIA, Dashboard, Analytics, Policy, Administration, Activation, Search, Notifications, and Help. The main area is titled 'Insights Logs' and shows a table of log records from November 7, 2022. The table has columns for No., Event Time, User, Policy Action, and URL. The first record in the table is highlighted with a red background and the text 'IPS block outbound request: adware/spyware t...' is visible. A red arrow points to this row. The table contains 11 rows of data.

No.	Event Time	User	Policy Action	URL
1	Monday, November ...	us-east-2-vpc-02...	IPS block outbound request: adware/spyware t...	www.google.com/
2	Monday, November ...	us-east-2-vpc-02...	Allowed	beacons2.gvt2.com
3	Monday, November ...	us-east-2-vpc-02...	Allowed	google.com
4	Monday, November ...	us-east-2-vpc-02...	Allowed	cdn.cookielaw.org
5	Monday, November ...	us-east-2-vpc-02...	Allowed	optimizationguide-pa.googl
6	Monday, November ...	us-east-2-vpc-02...	Allowed	cdn.cookielaw.org
7	Monday, November ...	us-east-2-vpc-02...	Allowed	privacyportal.onetrust.com
8	Monday, November ...	us-east-2-vpc-02...	Allowed	www.wicar.org
9	Monday, November ...	us-east-2-vpc-02...	Allowed	www.google.com
10	Monday, November ...	us-east-2-vpc-02...	Allowed	safebrowsing.googleapis.cc
11	Monday, November ...	us-east-2-vpc-02...	Allowed	beacons.gcp.gvt2.com

Copyright©2007-2022 Zscaler Inc. All rights reserved. | Version 6.1 | Patents

Weblog Time: 11/7/2022 4:34:08 PM | Last Updated: 11/7/2022 4:34:53 PM



Though these are simple tests, the above exercises help demonstrate what Zscaler can do straight out of the box without requiring additional configuration. Aside from enabling SSL decryption, Zscaler automatically identifies and blocks threats without requiring administrators to build a complex policy first.

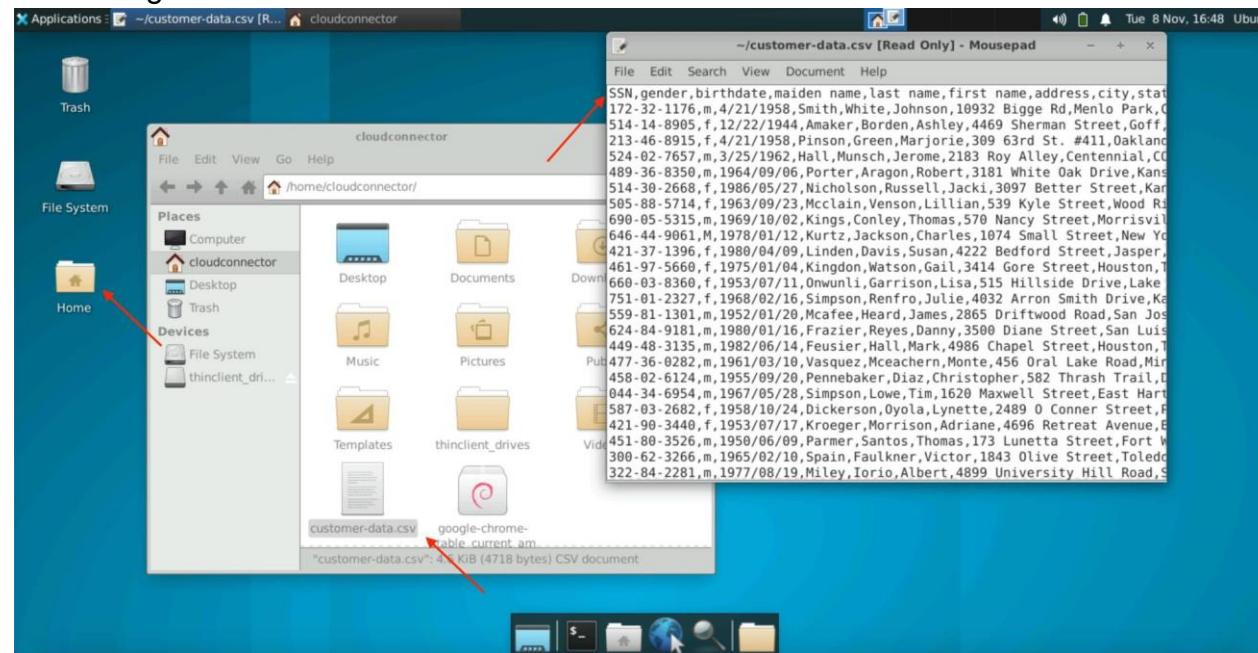
Lab 7: Enforcing a Data Loss Prevention Policy

We've demonstrated how Zscaler protects your workload from external threats such as viruses, phishing sites, and BotNets. However, what if the bad actor originates from within your organization, or perhaps a workload has been compromised? In this lab, we demonstrate how Zscaler prevents data exfiltration.

Task 1: Configure DLP Policy

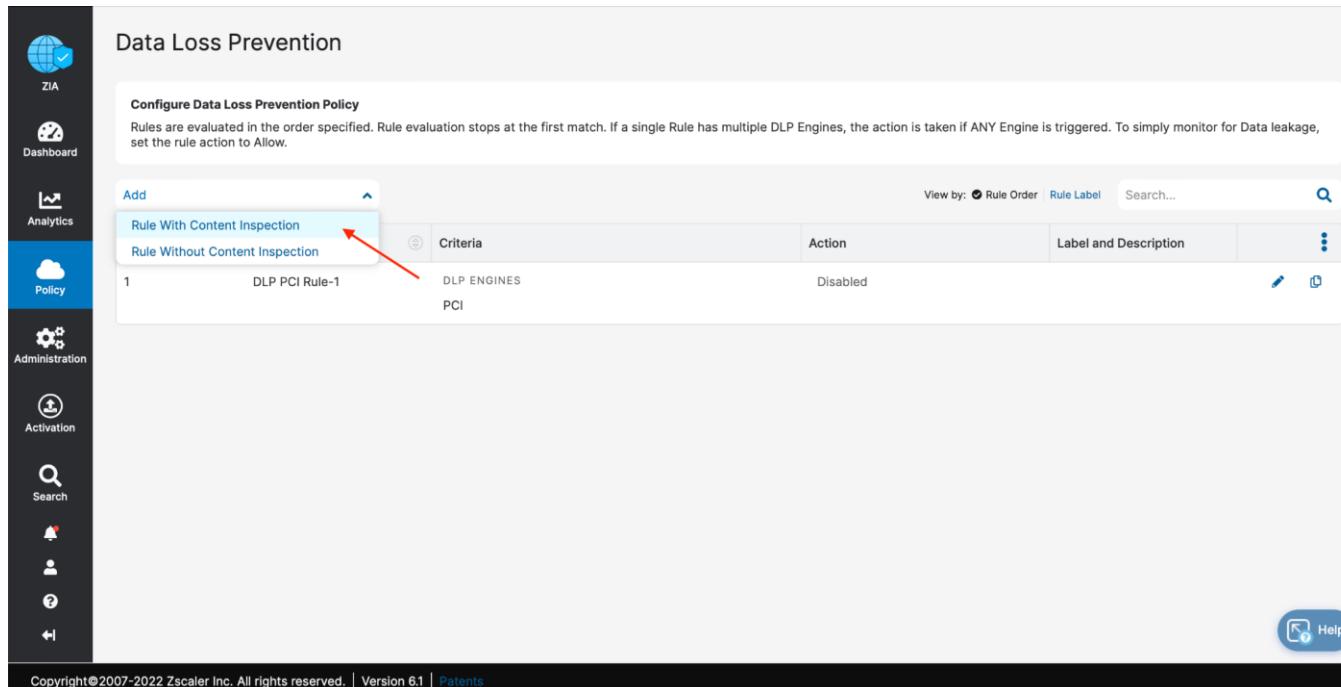
In this task, you will configure a DLP Policy to block the exfiltration of Personal Identifiable Information (PII).

- From the **Region1** Workload, take a look at the **customer-data.csv** file located in the **Home** folder on the Desktop by double-clicking it.



Note: Ensure you review the CSV file and not the TXT file. This file contains fake Personal Identifiable Information (PII). Let's assume a disgruntled employee tries to exfiltrate this data.

2. In the ZIA Admin portal, select **Policy > DATA LOSS PREVENTION > Data Loss Prevention**.
3. Click the **Add** button and select **Rule With Content Inspection**.

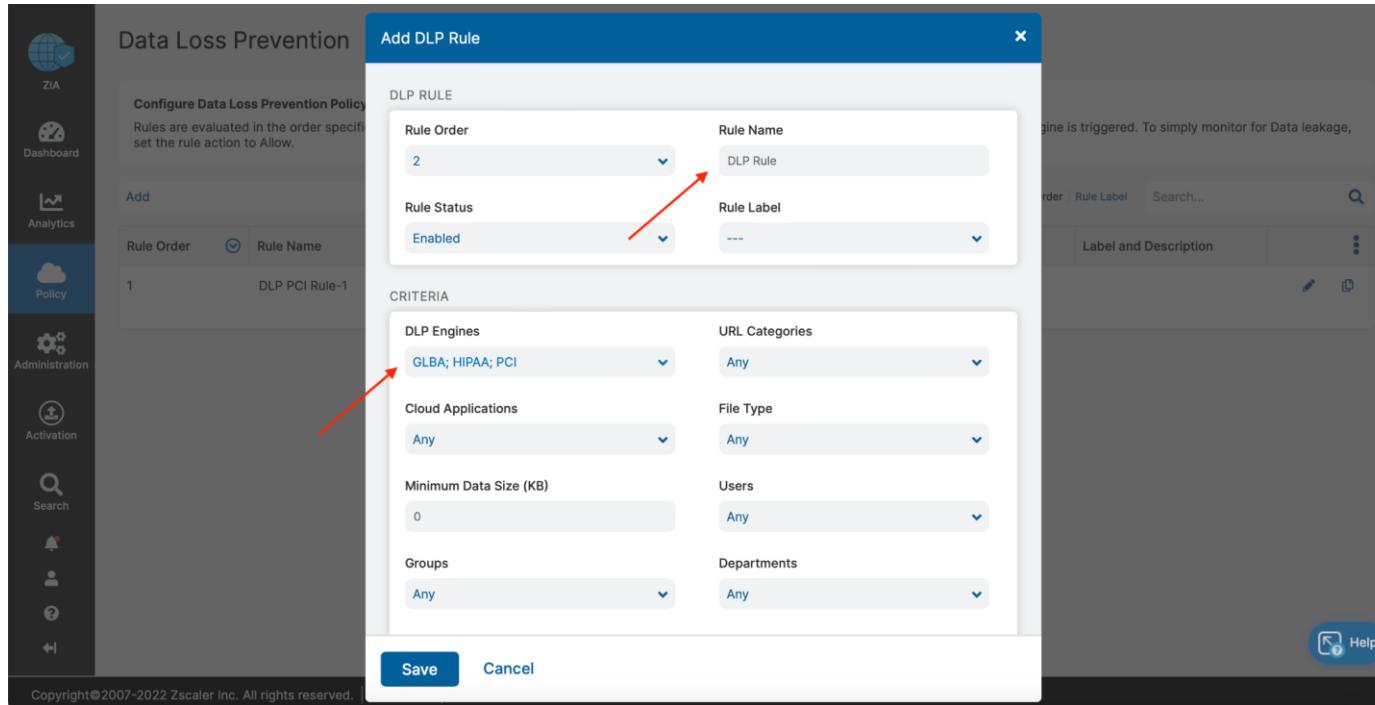


The screenshot shows the Zscaler Admin Portal interface. On the left, there is a vertical sidebar with icons for ZIA, Dashboard, Analytics, Policy (which is selected), Administration, Activation, Search, and Help. The main content area is titled "Data Loss Prevention" and contains a sub-section titled "Configure Data Loss Prevention Policy". It includes a note about rule evaluation and a table for managing rules. The table has columns for "Criteria", "Action", and "Label and Description". There is one row visible: "DLP PCI Rule-1" under Criteria, "Disabled" under Action, and "DLP ENGINES PCI" under Label and Description. At the top of the table, there is an "Add" button with a dropdown menu open, showing "Rule With Content Inspection" and "Rule Without Content Inspection". A red arrow points to the "Rule With Content Inspection" option. The bottom of the screen shows a copyright notice: "Copyright © 2007-2022 Zscaler Inc. All rights reserved. | Version 6.1 | Patents".

4. Configure the rule as follows:
 - a. Enter a **Name**.

Lab 7: Enforcing a Data Loss Prevention Policy

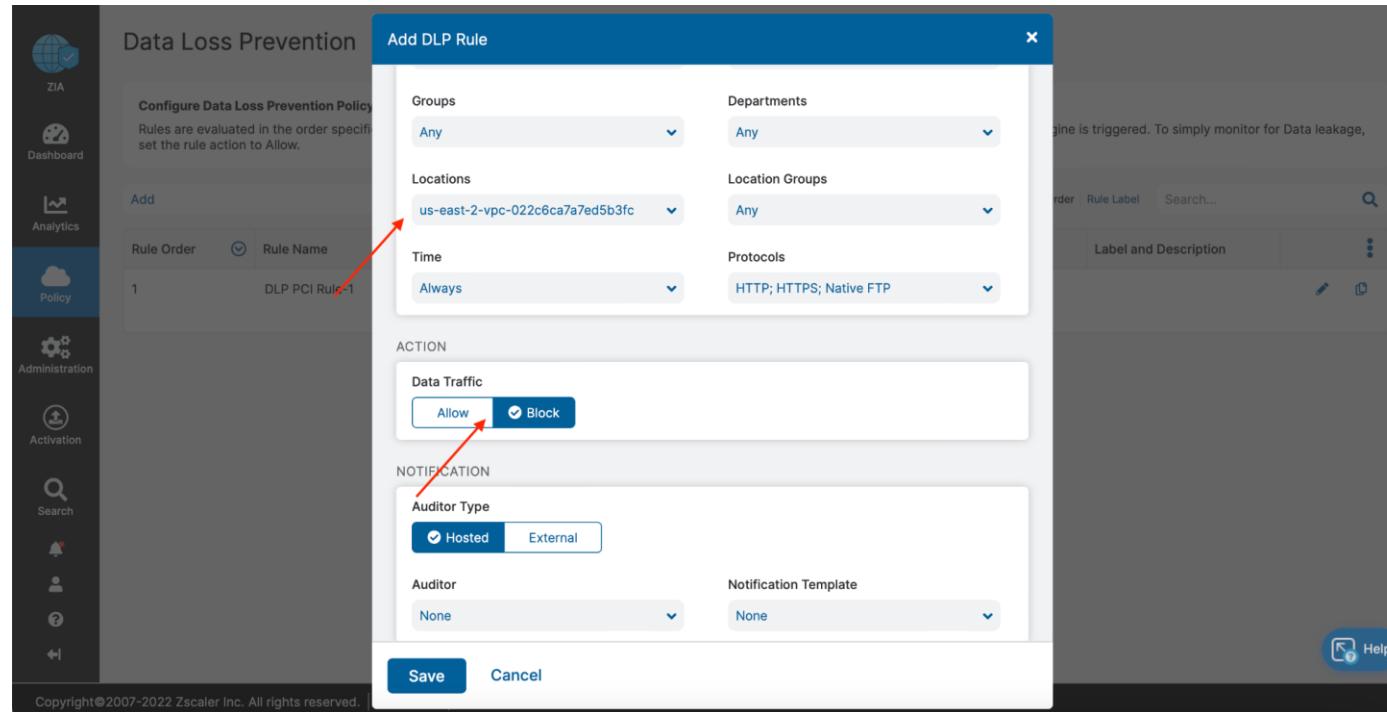
- b. Under the Criteria section, click **DLP Engines** and select **GLBA, HIPAA, and PCI**. Click **Done**.



The screenshot shows the Zscaler DLP rule configuration interface. The main window displays a list of existing DLP rules, with one rule named "DLP PCI Rule-1" visible. A modal dialog titled "Add DLP Rule" is open, allowing the creation of a new rule. The "DLP RULE" section includes fields for "Rule Order" (set to 2), "Rule Name" (set to "DLP Rule"), "Rule Status" (set to "Enabled"), and "Rule Label" (set to "---"). The "CRITERIA" section contains several dropdown menus: "DLP Engines" is set to "GLBA; HIPAA; PCI" (with a red arrow pointing to it); "Cloud Applications" is set to "Any"; "Minimum Data Size (KB)" is set to "0"; "Groups" is set to "Any"; "URL Categories" is set to "Any"; "File Type" is set to "Any"; "Users" is set to "Any"; and "Departments" is set to "Any". At the bottom of the dialog are "Save" and "Cancel" buttons.

- c. Under the Criteria section, click **Locations** and select your **Cloud Connector Locations** from the dropdown menu.
 d. Click **Done**.
 e. Under the Action section, select **Block**.

Lab 7: Enforcing a Data Loss Prevention Policy



The screenshot shows the Zscaler Data Loss Prevention (DLP) rule configuration interface. The 'Add DLP Rule' dialog is open, displaying various configuration options:

- Groups:** Any
- Departments:** Any
- Locations:** us-east-2-vpc-022c6ca7a7ed5b3fc
- Location Groups:** Any
- Time:** Always
- Protocols:** HTTP; HTTPS; Native FTP
- ACTION:** Data Traffic (Allow selected)
- NOTIFICATION:** Auditor Type (Hosted selected)

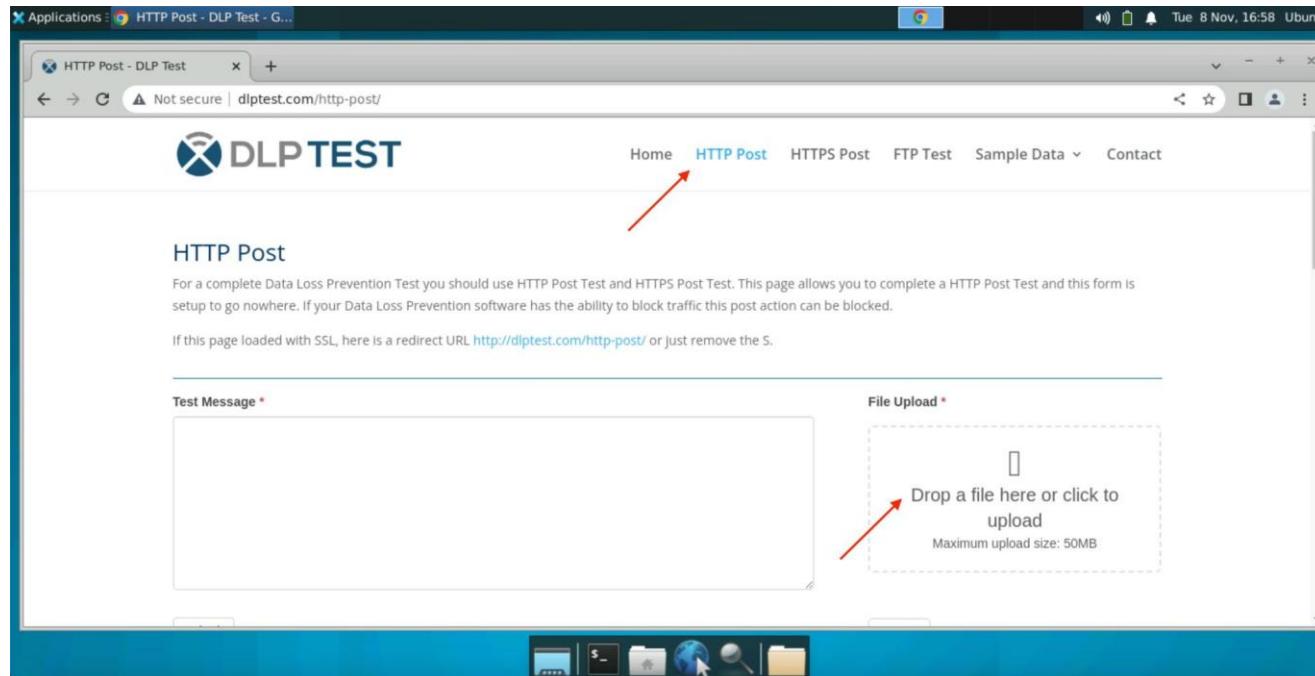
At the bottom of the dialog are 'Save' and 'Cancel' buttons. A red arrow points to the 'Allow' button in the ACTION section.

5. Click **Save**.
6. Activate the changes.

Task 2: Verify DLP Policy

In this task, you will verify that the configured DLP Policy has the desired effect.

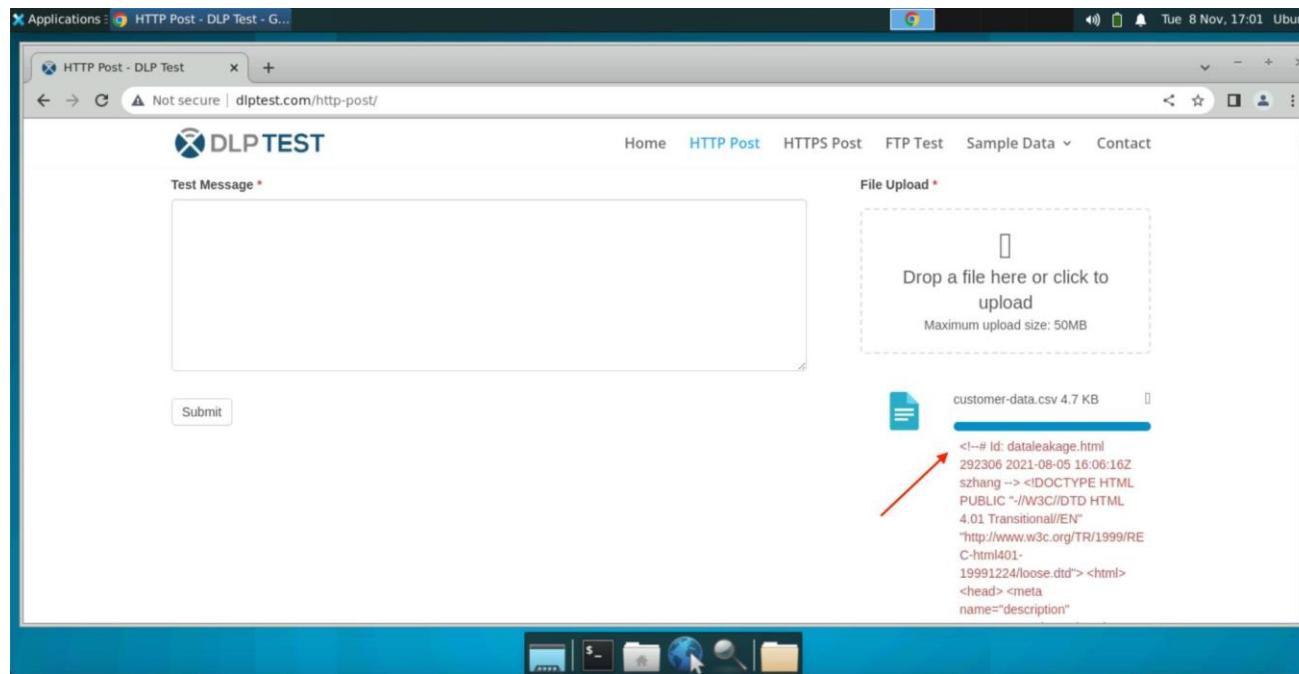
1. Return to the **Region1** Workload, open a web browser and navigate to <https://www.dlptest.com>.
2. Click on the **HTTP or HTTPS Post** option at the top of the website.



Note: If you wish to test an HTTPS upload, ensure your SSL Inspection policy is activated from the previous lab.

Lab 7: Enforcing a Data Loss Prevention Policy

3. Click the button to upload a file on the right and select the **customer-data.csv** file you reviewed earlier.
4. Click **Upload**.



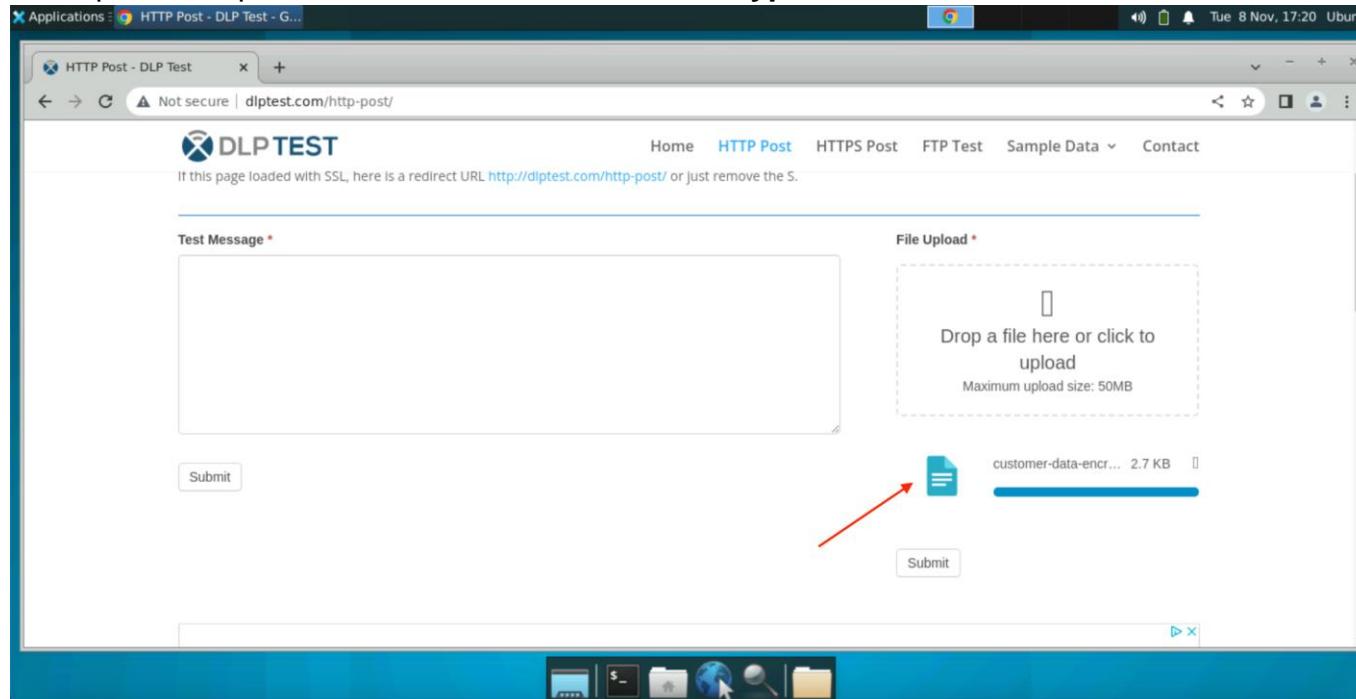
The screenshot shows a web browser window titled "HTTP Post - DLP Test - G...". The address bar says "Not secure | dlptest.com/http-post/". The page header includes "DLP TEST" and navigation links for Home, HTTP Post, HTTPS Post, FTP Test, Sample Data, and Contact. The main content area has two sections: "Test Message *" (empty) and "File Upload *". The "File Upload" section contains a dashed box with the text "Drop a file here or click to upload" and "Maximum upload size: 50MB". Below this, a file preview for "customer-data.csv 4.7 KB" is shown, displaying its contents. A red arrow points to the file preview area, highlighting the HTML code that was detected as a data leak.

```
<!--# id: dataleakage.html
292306 2021-08-05 16:06:16Z
szhang --><!DOCTYPE HTML
PUBLIC "-//W3C//DTD HTML
4.01 Transitional//EN"
"http://www.w3c.org/TR/1999/REC-HTML401-
19991224/loose.dtd"> <html>
<head> <meta
name="description"
```

5. Verify that the file is immediately blocked from being uploaded.

Note: What if, however, the attacker encrypts the data prior to uploading? To simulate this, we've already encrypted the customer-data.csv file using GNU Privacy Guard (GPG). This file is the encrypted version of the file you just attempted to upload.

Lab 7: Enforcing a Data Loss Prevention Policy

6. Repeat the upload test with **customer-data-encrypted.txt**.

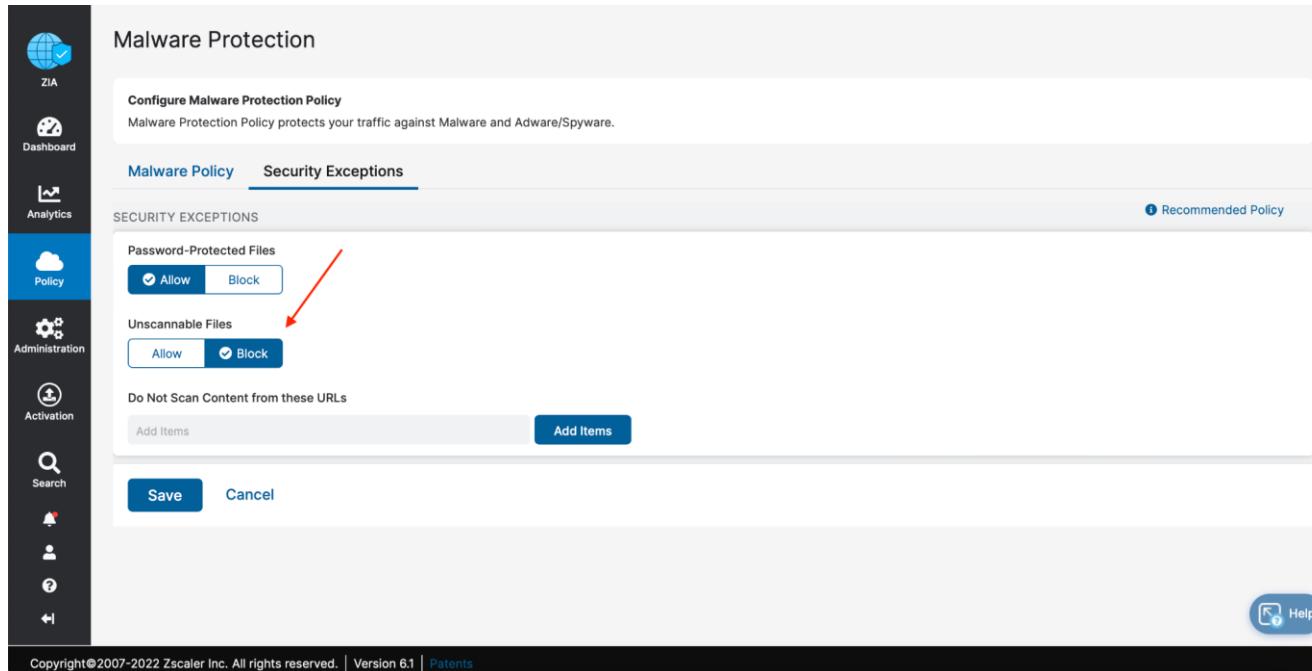
The screenshot shows a web browser window with the URL <http://dipitest.com/http-post/>. The page title is "HTTP Post - DLP Test". The main content area has two sections: "Test Message" and "File Upload". The "File Upload" section contains a dashed box with the instruction "Drop a file here or click to upload" and "Maximum upload size: 50MB". Below this, a file named "customer-data-encrypted.txt" is shown with a size of "2.7 KB". A red arrow points from the text "It worked!" below to the "Submit" button at the bottom of the upload area.



It worked! Now what? How can we block this traffic? To block this traffic, let's configure ZIA to deny file uploads for unscannable files.

7. Return to the ZIA Admin portal and select **Policy > SECURITY > Malware Protection**.
8. Click the **Security Exceptions** tab.
9. For **Unscannable Files**, choose the **Block** option.

Lab 7: Enforcing a Data Loss Prevention Policy



The screenshot shows the Zscaler Malware Protection Policy configuration interface. The left sidebar includes icons for ZIA, Dashboard, Analytics, Policy, Administration, Activation, Search, and Help. The main panel title is "Malware Protection" with a sub-section "Configure Malware Protection Policy". A note states: "Malware Protection Policy protects your traffic against Malware and Adware/Spyware." Below this are two tabs: "Malware Policy" (selected) and "Security Exceptions". The "Security Exceptions" tab contains sections for "Password-Protected Files" (with "Allow" and "Block" buttons, where "Block" is highlighted with a red arrow) and "Unscannable Files" (with "Allow" and "Block" buttons, where "Block" is also highlighted). There is also a section for "Do Not Scan Content from these URLs" with "Add Items" and "Save" buttons. A "Help" icon is located at the bottom right.

10. Click **Save**.
11. Activate the changes.
12. Return to the **Region1** Workload and try to upload the **customer-data-encrypted.txt** file again.
13. Verify that this time, the file failed to upload.

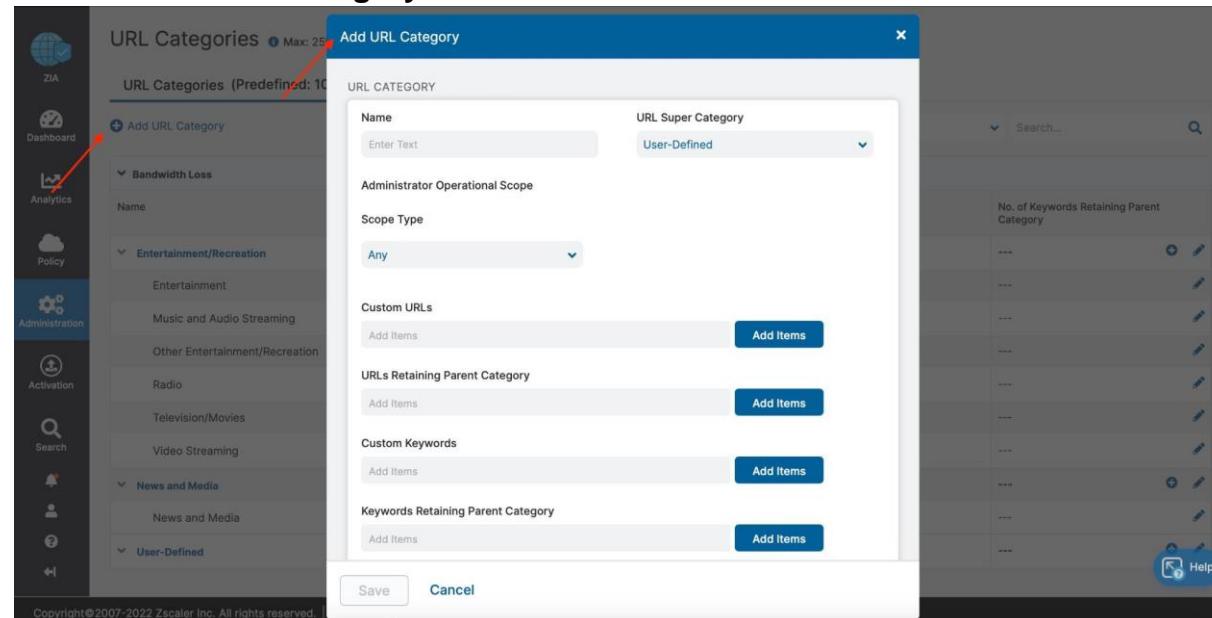
Lab 8: Controlling Access to Specific Resources on Websites

A company's security policy may dictate access is only granted for approved portions of a website. For example, Github contains numerous code repositories (repositories), but it may not be ideal to allow unfettered access to all repositories. In this lab, you'll configure the system to allow access to two official Github repositories – namely github.com/aws and github.com/aws-samples.

Task 1: Configure URL Filtering Rule

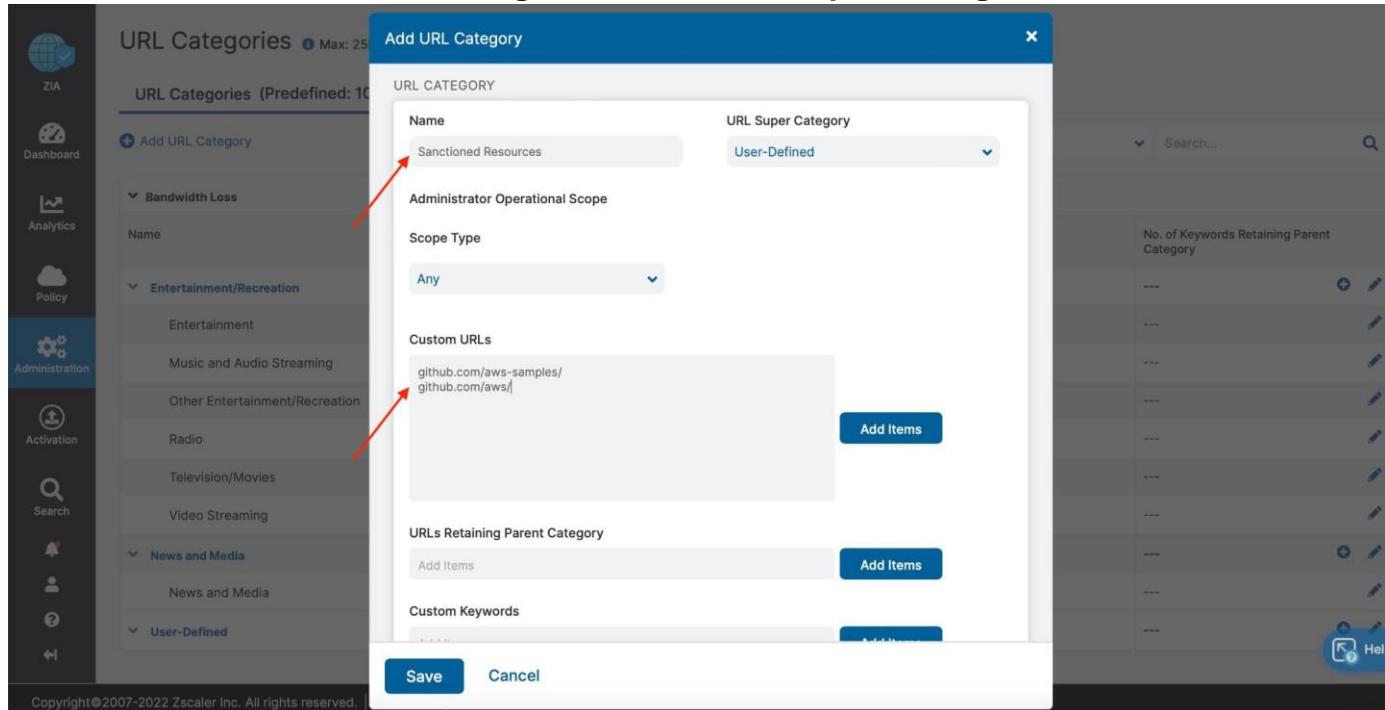
In this task, you will configure custom URL categories which will then be used in URL Filtering Rules to control access to sanctioned/unsanctioned Github repositories.

1. In the ZIA Admin portal, select **Administration > ACCESS CONTROL > URL Categories**.
2. Click **Add URL Category**.



Lab 8: Controlling Access to Specified Resources on Websites

3. Configure the category as follows:
 - a. For **Name**, enter **Sanctioned Resources**.
 - b. Under **Custom URLs**, enter **github.com/aws-samples/** and **github.com/aws/**.

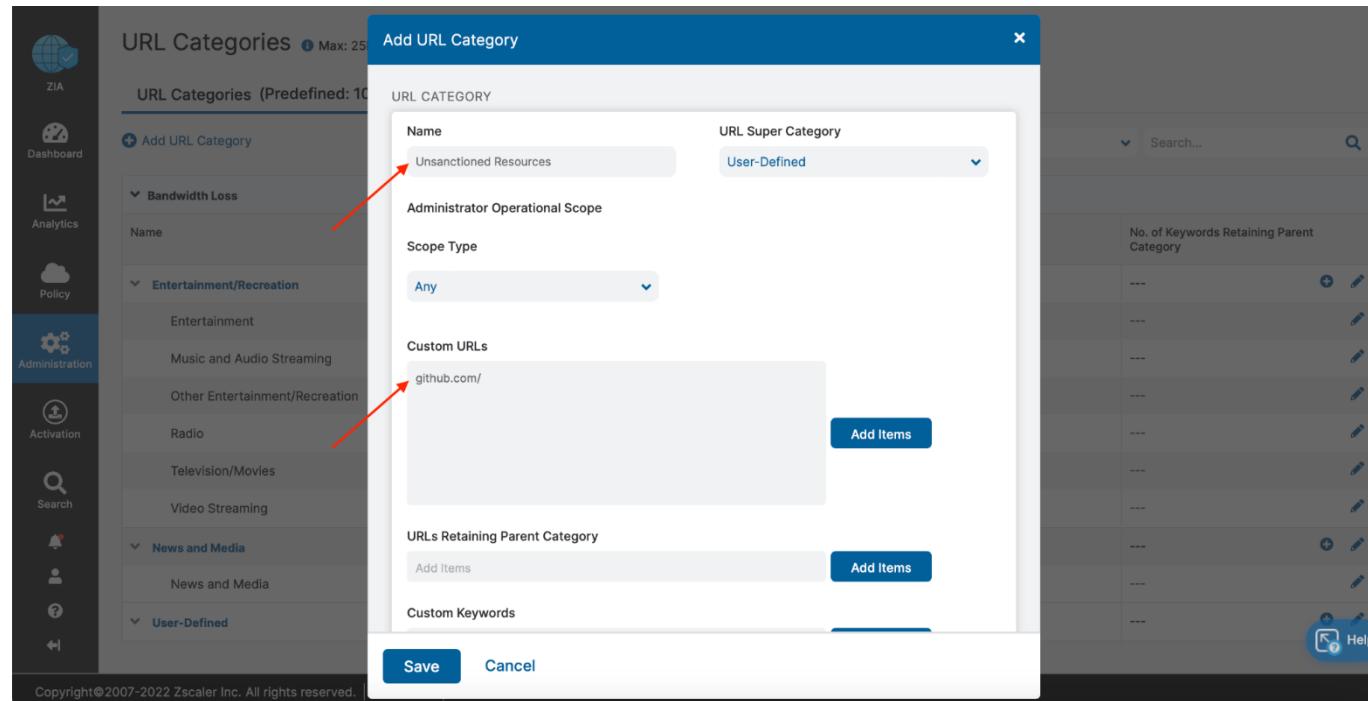


The screenshot shows the Zscaler UI with the 'URL Categories' page open. A modal window titled 'Add URL Category' is displayed. In the 'Name' field, 'Sanctioned Resources' is entered. In the 'Custom URLs' section, two entries are present: 'github.com/aws-samples/' and 'github.com/aws/'. The 'Scope Type' dropdown is set to 'Any'. The 'URL Super Category' dropdown is set to 'User-Defined'. At the bottom of the modal, there are 'Save' and 'Cancel' buttons.

Note: Make sure to include the trailing “/”.

4. Click **Save**.
5. Click **Add URL Category** again.
6. Configure the category as follows:
 - a. For **Name**, enter **Unsanctioned Resources**.
 - b. Under **Custom URLs**, enter **github.com/**.

Lab 8: Controlling Access to Specified Resources on Websites



The screenshot shows the Zscaler interface with the 'URL Categories' page open. A modal window titled 'Add URL Category' is displayed. In the 'Name' field, 'Unsanctioned Resources' is entered. In the 'Custom URLs' section, 'github.com/' is listed. The 'Scope Type' is set to 'Any'. The 'URL Super Category' is 'User-Defined'. At the bottom, there are 'Save' and 'Cancel' buttons.

Note: Make sure to include the trailing “/”.

7. Click **Add Items**.
8. Click **Save**.
9. Activate the changes.

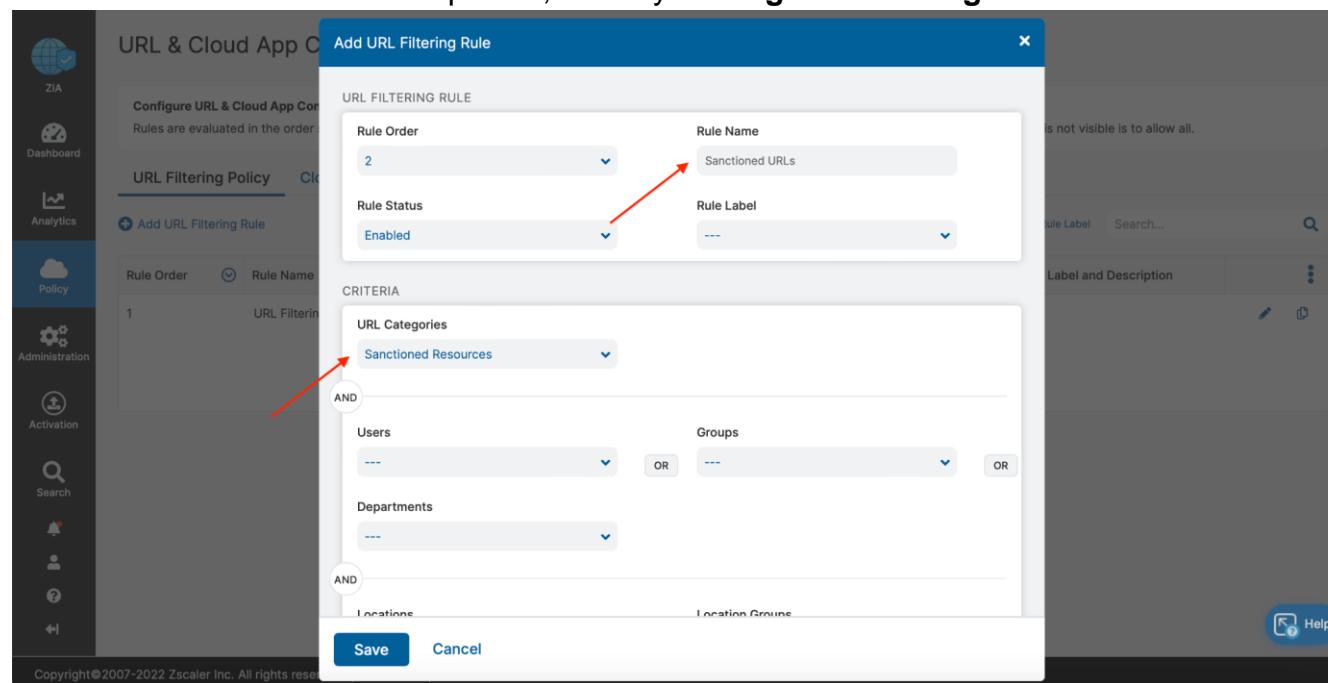
Note: After defining the two URL categories, it's necessary to add URL Filtering rules that leverage the two categories.

10. Select Policy > ACCESS CONTROL > URL & Cloud App Control.

11. To create a rule that allows access to sanctioned resources, click Add URL Filtering Rule.

12. Configure the rule as follows:

- For Name, enter **Sanctioned Resources**.
- In the Criteria section, under **URL Categories**, select **Sanctioned Resources**.
- From the Locations dropdown, select your **Region1** and **Region2** Locations.

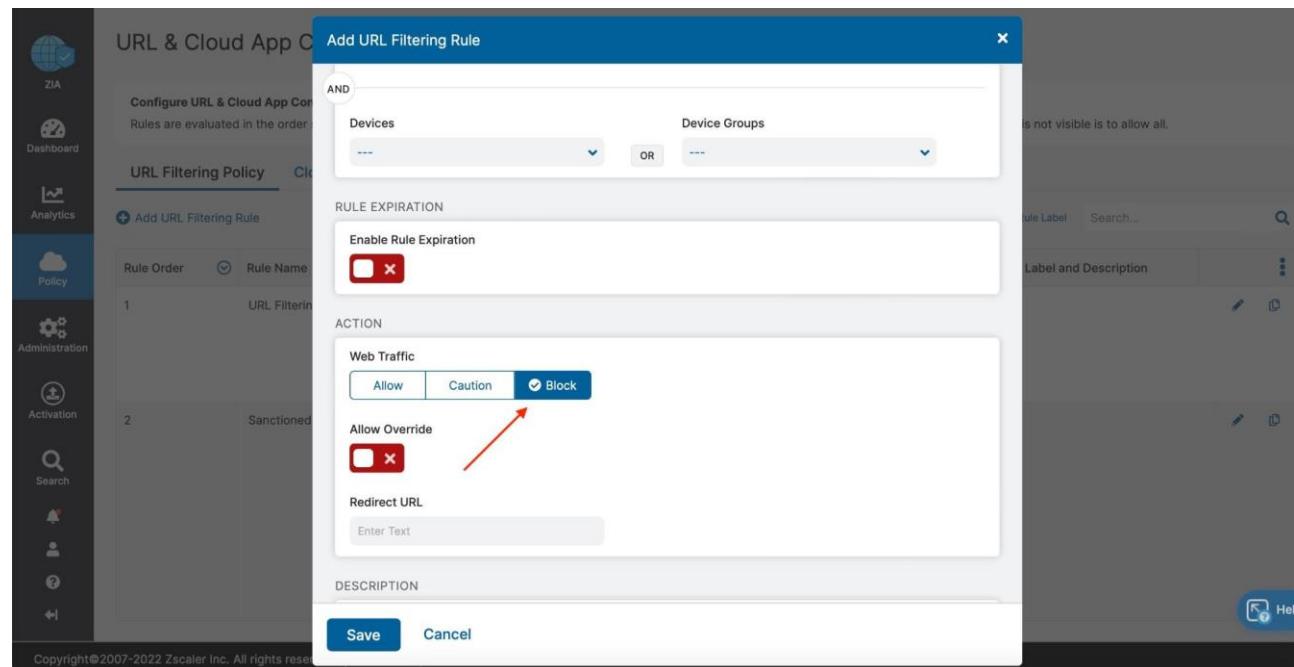


Lab 8: Controlling Access to Specified Resources on Websites

13. Click **Save**.
14. Activate the changes.

Note: Similarly, add a new URL Filtering rule for unsanctioned resources that uses the Unsanctioned Resources URL Category and the same Location.

15. Click **Add URL Filtering Rule** again.
16. Configure the rule as follows:
 - a. For **Name**, enter **Unsanctioned Resources**.
 - b. In the Criteria section, under **URL Categories**, select **Unsanctioned Resources**.
 - c. From the **Locations** dropdown, select your **USEast2** Location.
 - d. In the Action section, select **Block**.



Lab 8: Controlling Access to Specified Resources on Websites

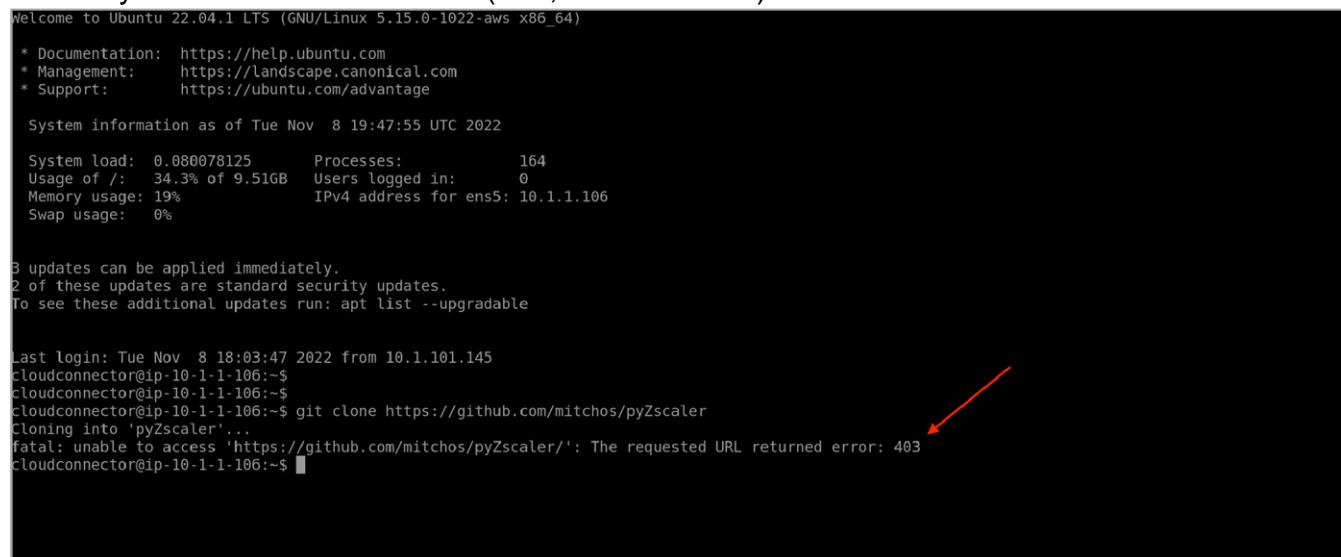
17. Click **Save**.
18. Activate the changes.

Note: SSL Inspection is required since GitHub will redirect HTTP requests to HTTPS. Ensure your SSL Inspection policy is enabled.

Task 2: Verify URL Filtering Rule

In this task, you will verify that the configured URL Filtering Rules have the desired effect.

1. Return to the **Region1** Workload connection and open a terminal.
2. At the Command Line, enter **git clone https://github.com/mitchos/pyZscaler**.
3. Verify that Git returns an error (403, Unauthorized).



```
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1022-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue Nov  8 19:47:55 UTC 2022

System load:  0.080078125   Processes:          164
Usage of /:   34.3% of 9.51GB  Users logged in:     0
Memory usage: 19%            IPv4 address for ens5: 10.1.1.106
Swap usage:   0%

3 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

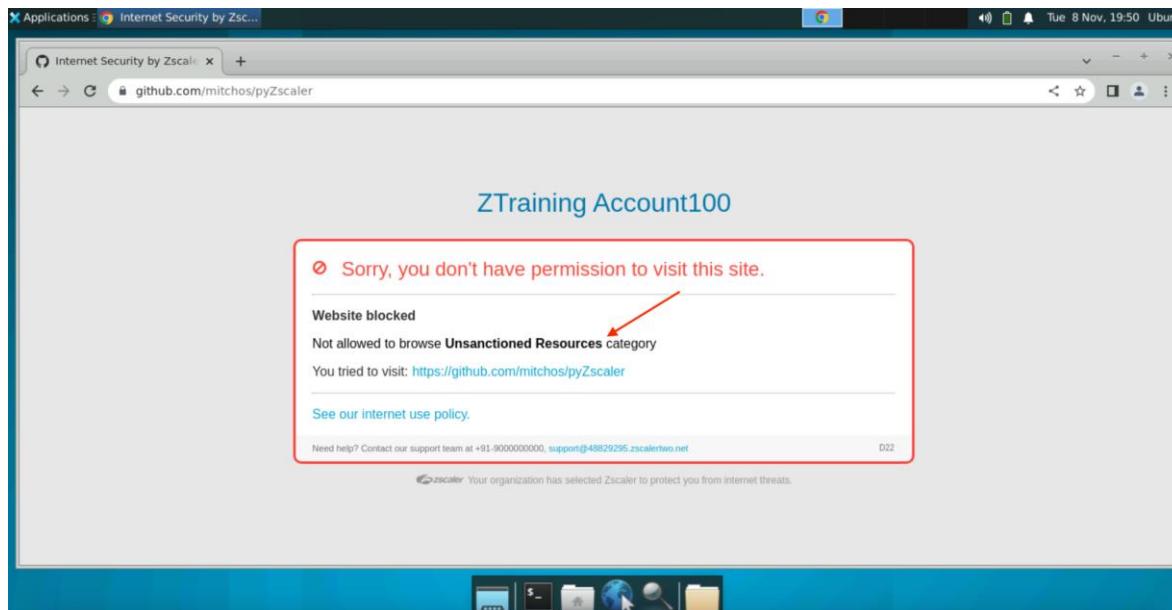
Last login: Tue Nov  8 18:03:47 2022 from 10.1.101.145
cloudconnector@ip-10-1-1-106:~$ 
cloudconnector@ip-10-1-1-106:~$ git clone https://github.com/mitchos/pyZscaler
Cloning into 'pyZscaler'...
fatal: unable to access 'https://github.com/mitchos/pyZscaler/': The requested URL returned error: 403
cloudconnector@ip-10-1-1-106:~$ 
```

Note: You can also use `curl -v github.com/mitchos/pyZscaler` to simulate a web browser when accessing this URL for additional information.

```
<table id="en_US" width="100%" border="0" cellspacing="0" cellpadding="0">
<tbody><tr><td class="eu_h">
<i class="a_1"></i>
Sorry, you don't have permission to visit this site.
</td></tr>
<tr><td class="hr"><hr></td></tr>
<tr><td class="eu_co">
<b>Website blocked</b>
</td></tr>
<tr><td class="eu_co rsn">
Not allowed to browse <B>Unsanctioned Resources</B> category
</td></tr>
<tr><td class="eu_co">
You tried to visit:<div class="eu_l"><a href="http://github.com/mitchos/pyZscaler">http://github.com/mitchos/pyZscaler</a></div>
</td></tr><tr>
<td class="hr"><hr></td>
</tr>
<tr><td class="eu_co ln">
<a href="http://48829295.zscalertwo.net/policy.html">
See our internet use policy.
</a>
</td></tr>
<tr><td class="eu_co fo">
Need help? Contact our support team at +91-9000000000, <a href="mailto:support@48829295.zscalertwo.net">support@48829295.zscalertwo.net</a>
</td></tr>
<tr><td class="eu_co st">
<span class="s_img"></span>
Your organization has selected Zscaler to protect you from internet threats.
</td></tr>
</tbody></table>
<!!--/locale en_US-->
</tbody></table>
</div>
</div>
</body></html>
* Connection #0 to host github.com left intact
<!!-- 647778 1 2 0 1667929800 192 http://github.com/mitchos/pyZscaler -->clouddconnector@ip-10-1-1-106:~$ █
```

4. Alternatively, you can also go to this website via Chrome to verify the behavior as well.

Lab 8: Controlling Access to Specified Resources on Websites



5. To clone the aws-cdk-examples and aws-cli repositories, enter **git clone https://github.com/aws-samples/aws-cdk-examples** and **git clone https://github.com/aws/aws-cli**.
6. Verify that the cloning of any repositories under aws-samples and aws was successful.

Lab 8: Controlling Access to Specified Resources on Websites

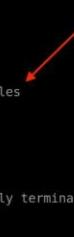
```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

System information as of Tue Nov  8 19:51:45 UTC 2022

System load: 0.0      Processes:          167
Usage of /: 34.3% of 9.51GB  Users logged in:    0
Memory usage: 19%           IPv4 address for ens5: 10.1.1.106
Swap usage:  0%

3 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Tue Nov  8 19:47:56 2022 from 10.1.101.145
cloudconnector@ip-10-1-1-106:~$ 
cloudconnector@ip-10-1-1-106:~$ git clone https://github.com/aws-samples/aws-cdk-examples
Cloning into 'aws-cdk-examples'...
remote: Enumerating objects: 5778, done.
remote: Counting objects: 100% (1004/1004), done.
remote: Compressing objects: 100% (223/223), done.
remote: Total 5778 (delta 821), reused 819 (delta 773), pack-reused 4774
Receiving objects: 100% (5778/5778), 55.77 MiB | 27.91 MiB/s, done.
error: RPC failed: curl 56 GnuTLS recv error (-110): The TLS connection was non-properly terminated.
Resolving deltas: 100% (3039/3039), done.
cloudconnector@ip-10-1-1-106:~$ git clone https://github.com/aws/aws-cli
Cloning into 'aws-cli'...
remote: Enumerating objects: 106143, done.
remote: Counting objects: 100% (656/656), done.
remote: Compressing objects: 100% (331/331), done.
remote: Total 106143 (delta 359), reused 567 (delta 286), pack-reused 105487
Receiving objects: 100% (106143/106143), 109.72 MiB | 19.94 MiB/s, done.
error: RPC failed: curl 56 GnuTLS recv error (-110): The TLS connection was non-properly terminated.
Resolving deltas: 100% (70442/70442), done.
cloudconnector@ip-10-1-1-106:~$ 
```



Note: It's also possible to restrict the cloning of a specific repository by specifying the name of the repo in the policy.

Lab 9: Integrating with Zscaler Private Access

During mergers and acquisitions, the acquiring company and the acquired company often need access to each other's applications - such as databases, web servers or financial tools. The traditional approach to achieve this goal is to connect the networks together. But this approach has two major drawbacks:

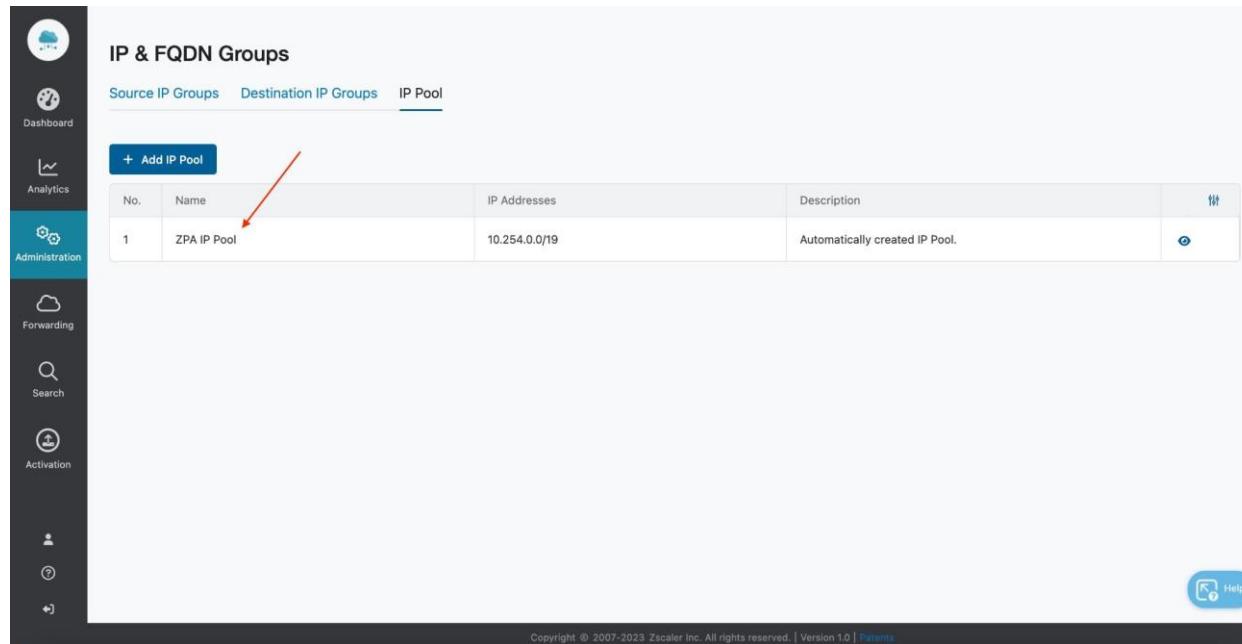
1. There is a high likelihood that the IP Address space may overlap. In which case, additional technologies, such as Network Address Translation, must be used to overcome this.
2. The security standard between the two companies differs, meaning they do not trust each other and therefore must go through an extensive vetting process.

It is not uncommon for this IT integration process to take 12 months or more to complete. This often introduces friction between IT and the business because, during this time, the business is not able to access key infrastructure of the acquired company. This module demonstrates how easy it is to overcome the two challenges mentioned above using Cloud Connector and Zscaler Private Access.

Note: *Cloud Connectors integrate with ZPA to allow workloads to seamlessly connect to other resources within your organization, or an acquired organization. To proxy this traffic, workload DNS queries are intercepted by the Cloud Connector. The Cloud Connector then responds to the DNS request on behalf of the “real” DNS server using a Synthetic IP. This forces the cloud workload to send traffic for the intended destination towards the Synthetic IP hosted on the Cloud Connector. On the receiving end of this transmission, the destination workload receives the traffic from the remote App Connector IP Address, rather than the “real” IP Address of the source workload.*

1. From the Cloud Connector portal, navigate to the **Administration** menu, followed by **IP & FQDN Groups**.
2. Click the **IP Pools** tab.

Lab 9: Integrating with Zscaler Private Access



The screenshot shows the ZPA Admin portal's IP & FQDN Groups section. On the left, a sidebar lists various navigation options: Dashboard, Analytics, Administration (which is selected), Forwarding, Search, Activation, and Help. The main content area is titled 'IP & FQDN Groups' and has tabs for 'Source IP Groups', 'Destination IP Groups', and 'IP Pool'. The 'IP Pool' tab is active. A table displays an IP pool entry:

No.	Name	IP Addresses	Description	Action
1	ZPA IP Pool	10.254.0.0/19	Automatically created IP Pool.	

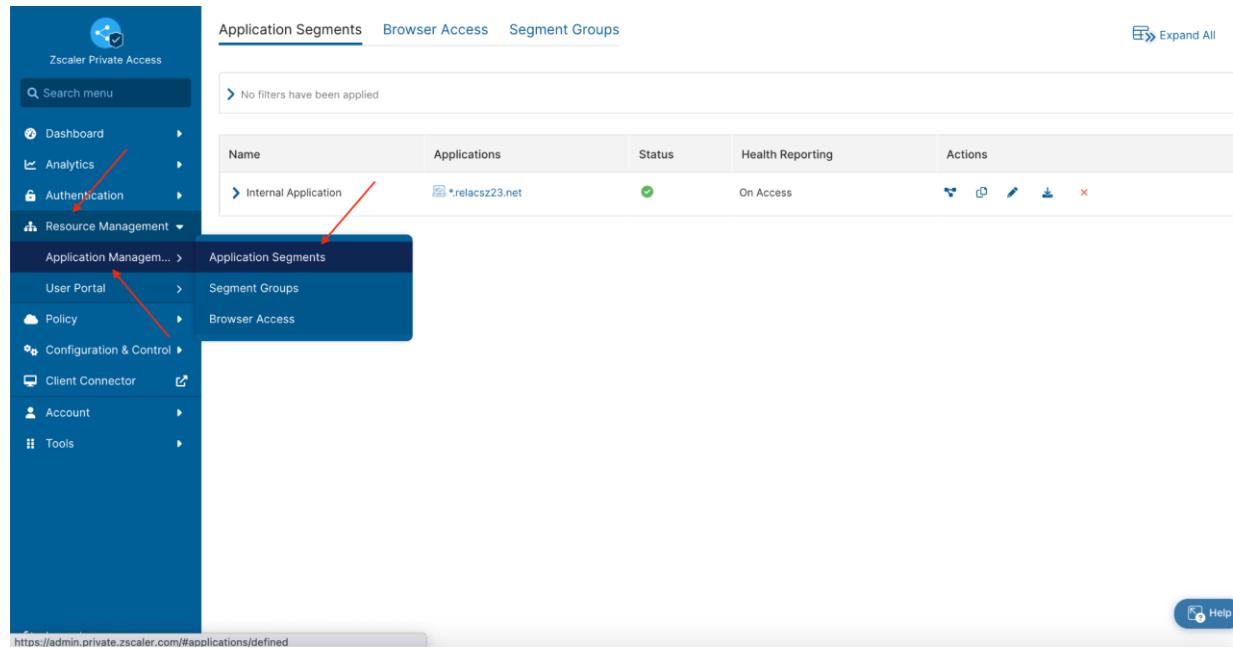
At the bottom of the page, there is a copyright notice: 'Copyright © 2007-2023 Zscaler Inc. All rights reserved. | Version 1.0 | [Help](#)'.

Here, we can see the Synthetic IP Pool that Cloud Connector appliances will use to proxy ZPA-bound traffic. Let's create some ZPA Application Segments so we can see this in action.

Note: The focus of this hands-on lab is on Cloud Connector. Hence, App Connectors and their deployment will not be covered and are already operational in your lab. Likewise, an in-depth discussion around Access Policy, Client Forwarding Policy or ZPA architecture in general is not covered.

3. Navigate to the ZPA Admin portal and login with your pod's credentials.
4. In the Resource Management menu, hover over the **Application Management** menu item, then select **Application Segments**.

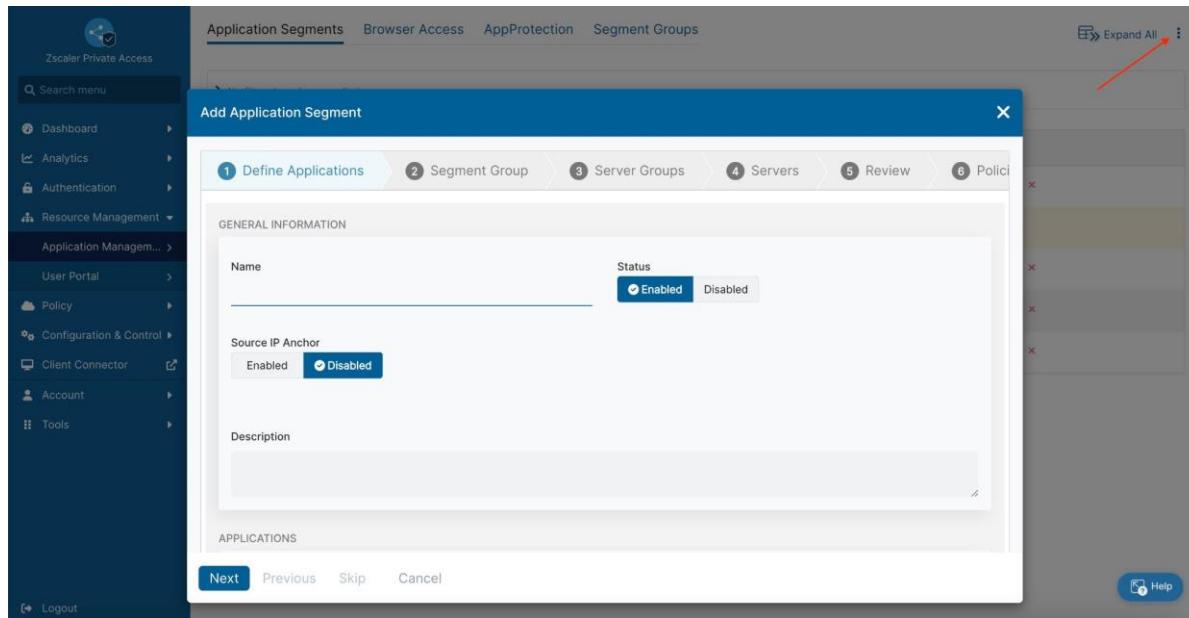
Lab 9: Integrating with Zscaler Private Access



The screenshot shows the Zscaler Private Access interface. The left sidebar has a search bar and a navigation menu with items like Dashboard, Analytics, Authentication (highlighted with a red arrow), Resource Management, Application Management (highlighted with a red arrow and a blue box), User Portal, Policy, Configuration & Control, Client Connector, Account, and Tools. The main content area is titled 'Application Segments' and shows a table with one row: Internal Application, *relacsz23.net, On Access. There are 'Actions' icons for each row. At the bottom right of the content area is a 'Help' button.

5. Click the **three dots** in the upper right corner of the screen and choose **Add Application Segment**.

Lab 9: Integrating with Zscaler Private Access



The screenshot shows the Zscaler Private Access web interface. On the left is a dark sidebar with various navigation options like Dashboard, Analytics, Authentication, Resource Management, Policy, Configuration & Control, Client Connector, Account, and Tools. The main area has tabs for Application Segments, Browser Access, AppProtection, and Segment Groups. A modal window titled 'Add Application Segment' is open. It has a progress bar at the top with steps 1 through 6. Step 1 is 'Define Applications'. The main section is 'GENERAL INFORMATION' with fields for 'Name' (a text input), 'Status' (radio buttons for Enabled or Disabled, with Enabled selected), and 'Source IP Anchor' (radio buttons for Enabled or Disabled, with Disabled selected). Below this is a 'Description' text area. At the bottom of the modal are buttons for 'Next', 'Previous', 'Skip', and 'Cancel', along with a 'Help' link. In the top right corner of the modal, there is a red arrow pointing to a small 'Expand All' button.

6. Provide a **name** for the Application Segment. In our case, we're going to test with a simple web-based file server, so we'll name our application **Region1-WebServer**.

Lab 9: Integrating with Zscaler Private Access

Add Application Segment

X

1 Define Applications 2 Segment Group 3 Server Groups 4 Servers 5 Review 6 Policies

GENERAL INFORMATION

Name: Region1-WebServer

Status: Enabled Disabled

Source IP Anchor: Enabled Disabled

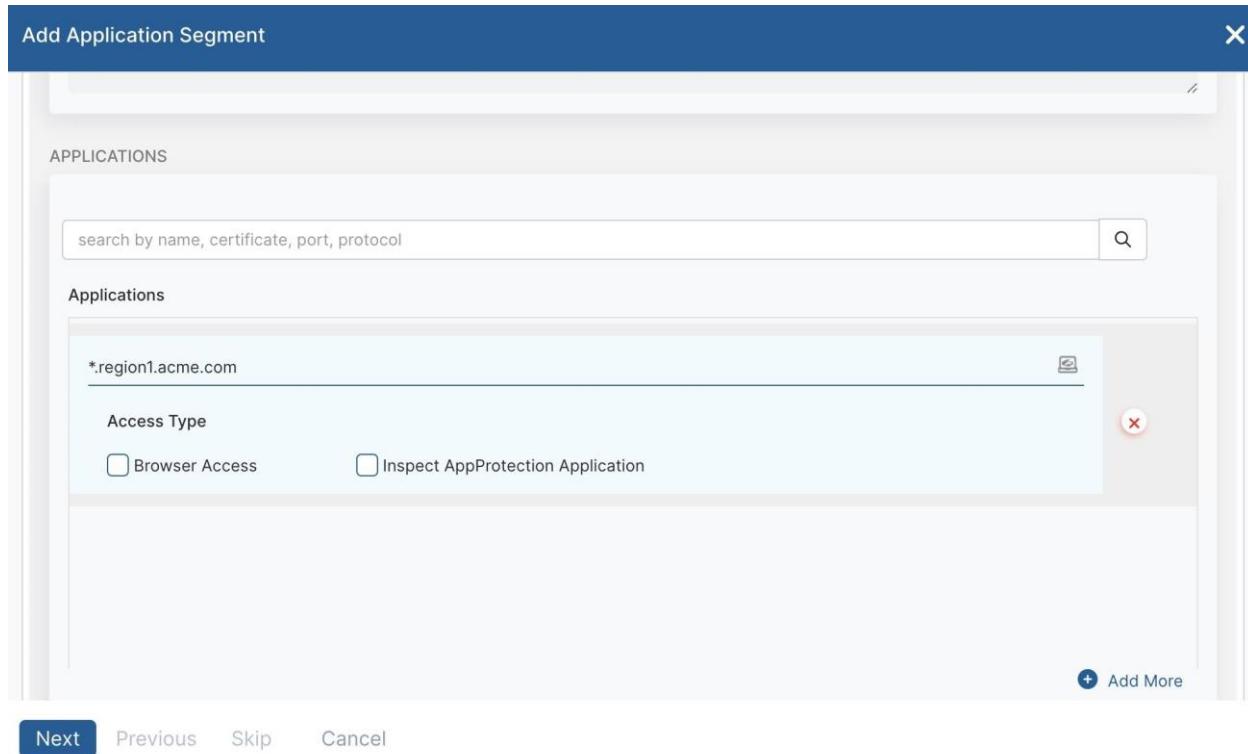
Description:

APPLICATIONS

Next Previous Skip Cancel

7. Enter the **domain** that you wish to proxy under the Applications section. Here, we'll use ***.region1.acme.com**.

Lab 9: Integrating with Zscaler Private Access



Add Application Segment X

APPLICATIONS

search by name, certificate, port, protocol Q

Applications

*.region1.acme.com ✖

Access Type

Browser Access Inspect AppProtection Application

+ Add More

Next Previous Skip Cancel

8. In the **TCP Port Ranges** section enter port **80**, as shown below, to define our web traffic.

Lab 9: Integrating with Zscaler Private Access

Add Application Segment

Select Enabled Disabled

TCP Port Ranges

From... 80 To... 80 [+ Add More](#)

UDP Port Ranges

From... To... [+ Add More](#)

ADDITIONAL CONFIGURATION

Double Encryption Enabled Disabled

Bypass Use Client Forwarding Policy

ICMP Access

[Next](#) [Previous](#) [Skip](#) [Cancel](#)

9. Click the **Next** button to proceed to the next step.

Segment Groups allow administrators to bundle multiple Application Segments together for easier policy definition. Rather than permitting or denying access to individual Application Segments, a policy can permit or deny access to a Segment Group, which contains multiple Application Segments. In our case, we'll create a new Segment Group called Region1-Apps.

10. Click the **Add Segment Group** tab and input your Segment Group name **Region1-Apps**.

Lab 9: Integrating with Zscaler Private Access

Add Application Segment

1 Define Applications 2 Segment Group 3 Server Groups 4 Servers 5 Review 6 Policies

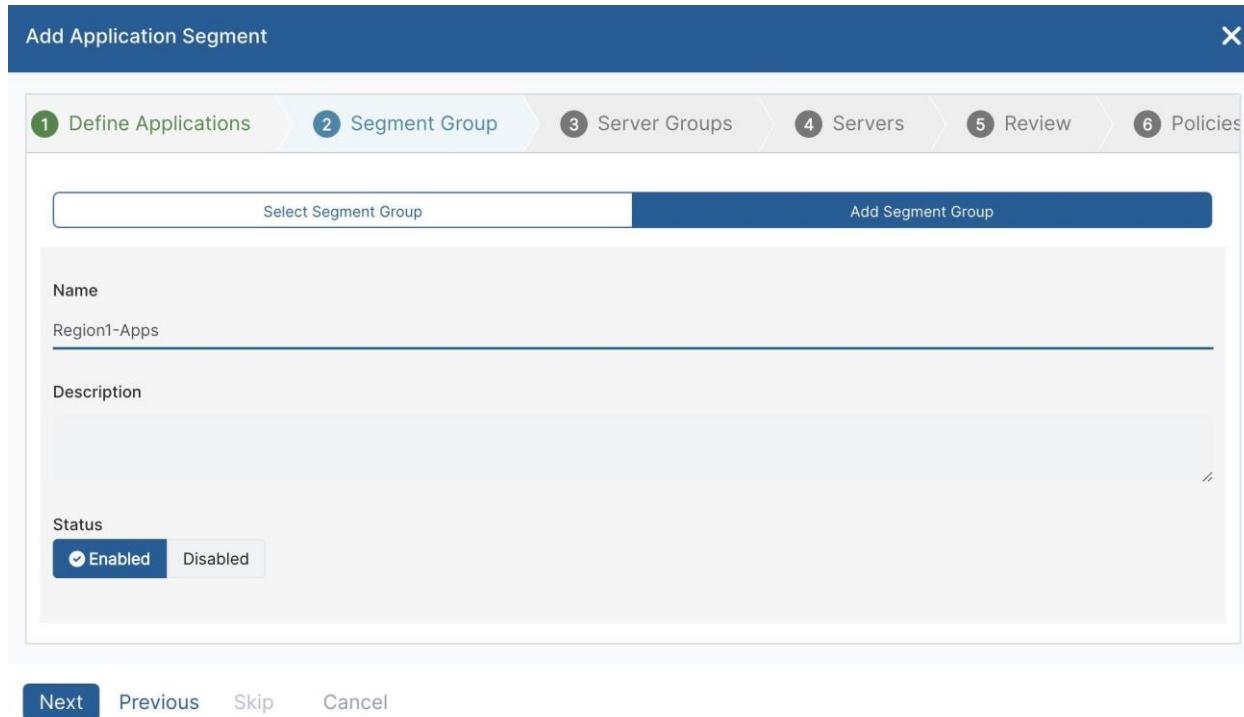
Select Segment Group Add Segment Group

Name
Region1-Apps

Description

Status
 Enabled Disabled

Next Previous Skip Cancel



11. Click the **Next** button to proceed.

Server Groups allow an administrator to define which App Connectors, or groups of App Connectors can reach a specific application. Here, we'll create a new Server Group that specifies our deployed App Connector.

12. Click the **Add Server Group** button, enter the **name** of your Server Group, then select your **App Connector** in the dropdown menu at the bottom.

Lab 9: Integrating with Zscaler Private Access

Add Application Segment

This is a recommended configuration. You can however skip this for Client To Client applications.

Select Server Group Add Server Group

Name: Region1-AppConnectors

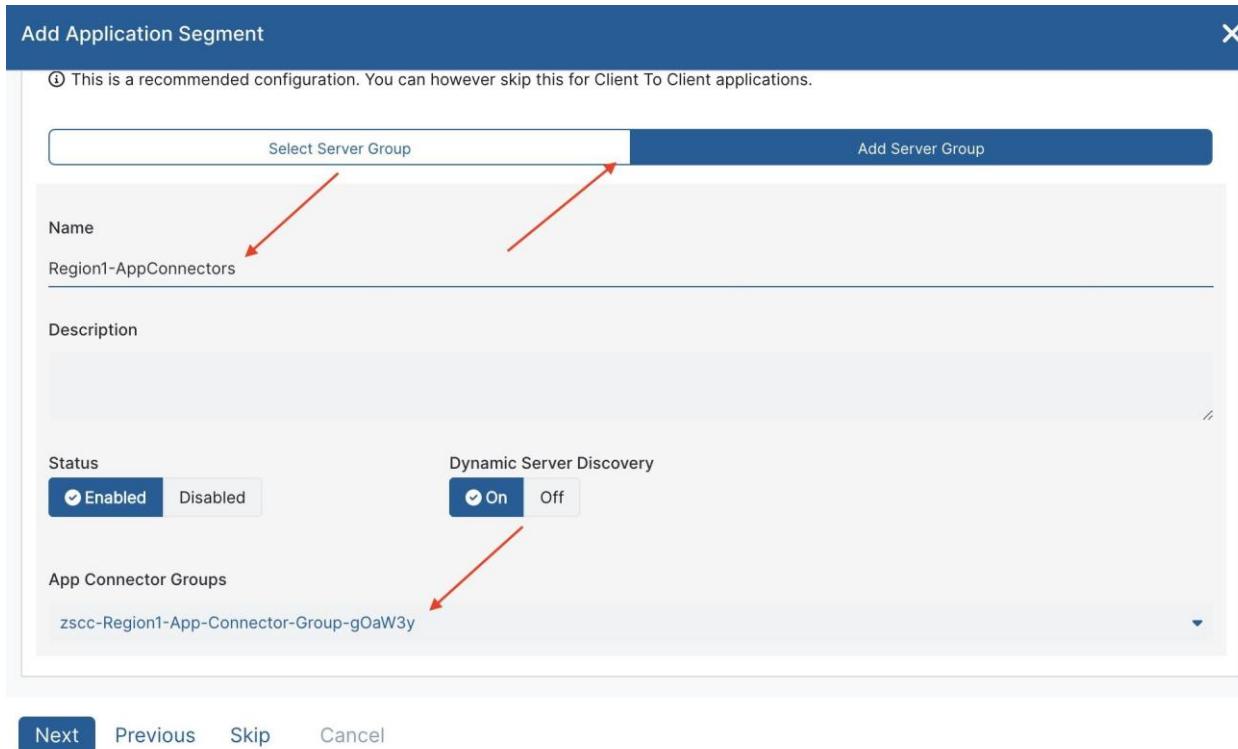
Description:

Status: Enabled Disabled

Dynamic Server Discovery: On Off

App Connector Groups:
zsc - Region1 - App - Connector - Group - gOaW3y

Next Previous Skip Cancel



13. Click the **Next** button to proceed, then **Save** your new Application Segment. The workflow should then prompt you to edit the Access Policy to allow traffic.

14. Click the **Edit Policy** button.

Lab 9: Integrating with Zscaler Private Access

Add Application Segment X

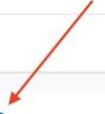
1 Define Applications 2 Segment Group 3 Server Groups 4 Review 5 Policies

POLICY

Rule Order	Name	Rule Action
1	Allow Internal Application Group	<input checked="" type="checkbox"/> Allow Access

Displaying 1-1 of 1

Edit Policy Skip Cancel



15. Click the **Add Rule** link in the top right corner of the page.

16. In the **Add Access Policy** workflow, give your Access Policy a **name** (such as Region1-Access).

Lab 9: Integrating with Zscaler Private Access

Add Access Policy X

Name
Region1-Access

Description

ACTION

Rule Action Allow Access Block Access

App Connector Selection Method
All App Connector groups for the application

Message to User

CRITERIA

 + Add Criteria

Save Cancel

- 17.In the **Criteria** section, click the button to **Add Criteria**, then choose **Cloud Connector Groups**.
- 18.In the dropdown that appears, choose your **Cloud Connector** appliances.

Lab 9: Integrating with Zscaler Private Access

Add Access Policy

X

Region1-Access

Description

ACTION

Rule Action

Allow Access Block Access

App Connector Selection Method

All App Connector groups for the application ▾

Message to User

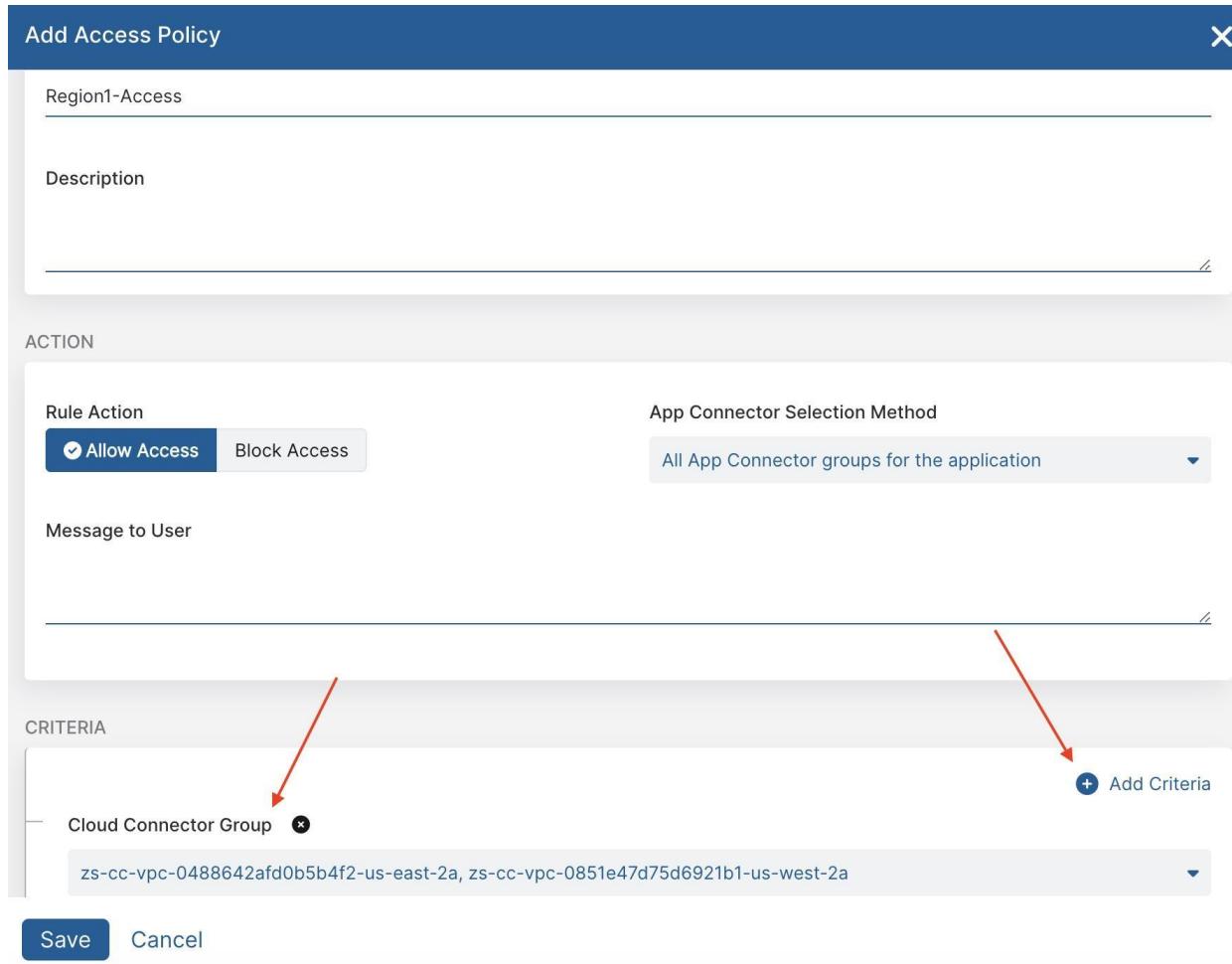
CRITERIA

Cloud Connector Group ×

zs-cc-vpc-0488642af0b5b4f2-us-east-2a, zs-cc-vpc-0851e47d75d6921b1-us-west-2a ▾

+ Add Criteria

Save Cancel



19. Click the **Add Criteria** button again, this time adding an Application. Choose your **Application Segment**.

Lab 9: Integrating with Zscaler Private Access

Add Access Policy X

Message to User

CRITERIA

Application Segments ✖ Add Criteria

Region1-WebServer

OR

Segment Groups

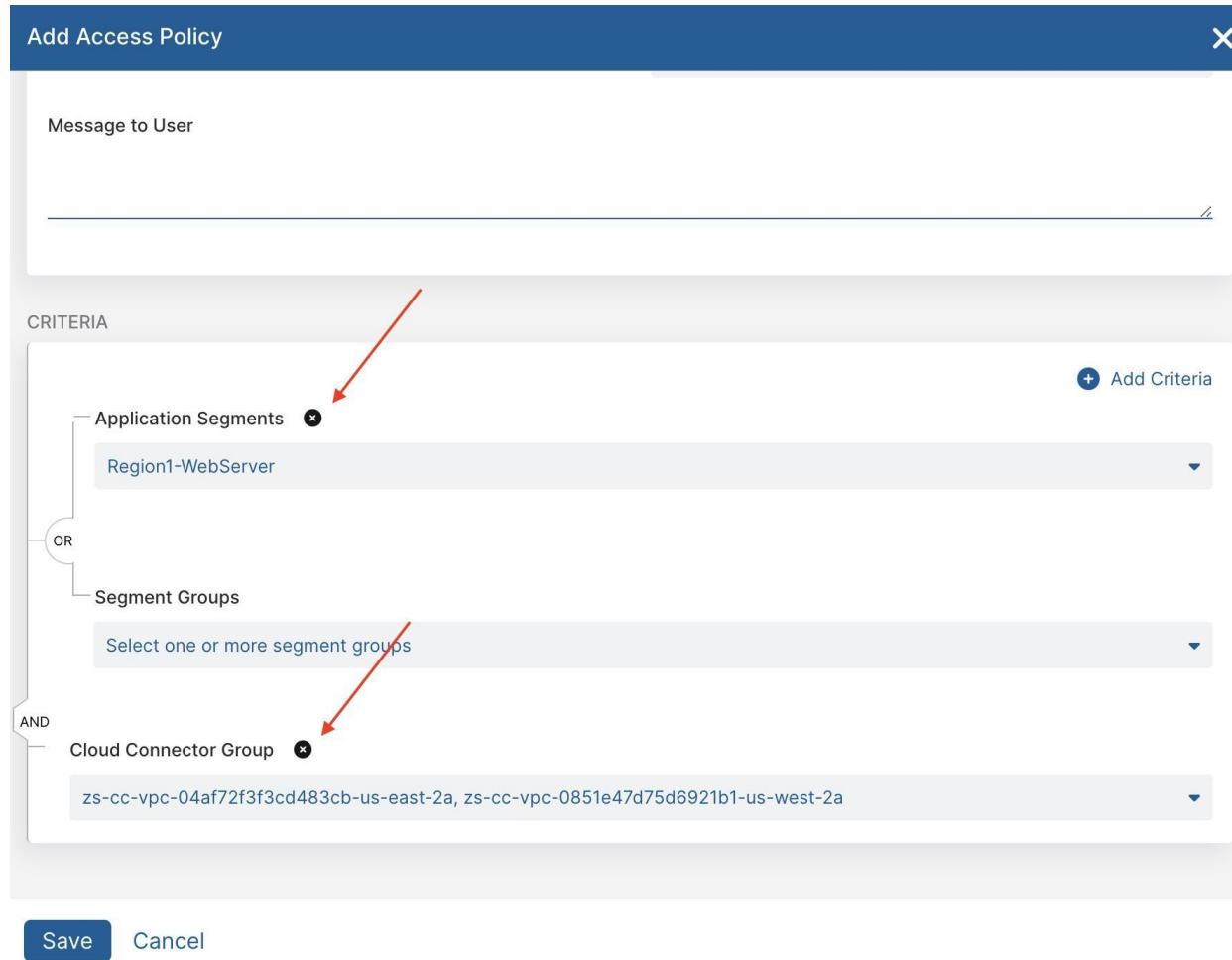
Select one or more segment groups

AND

Cloud Connector Group ✖

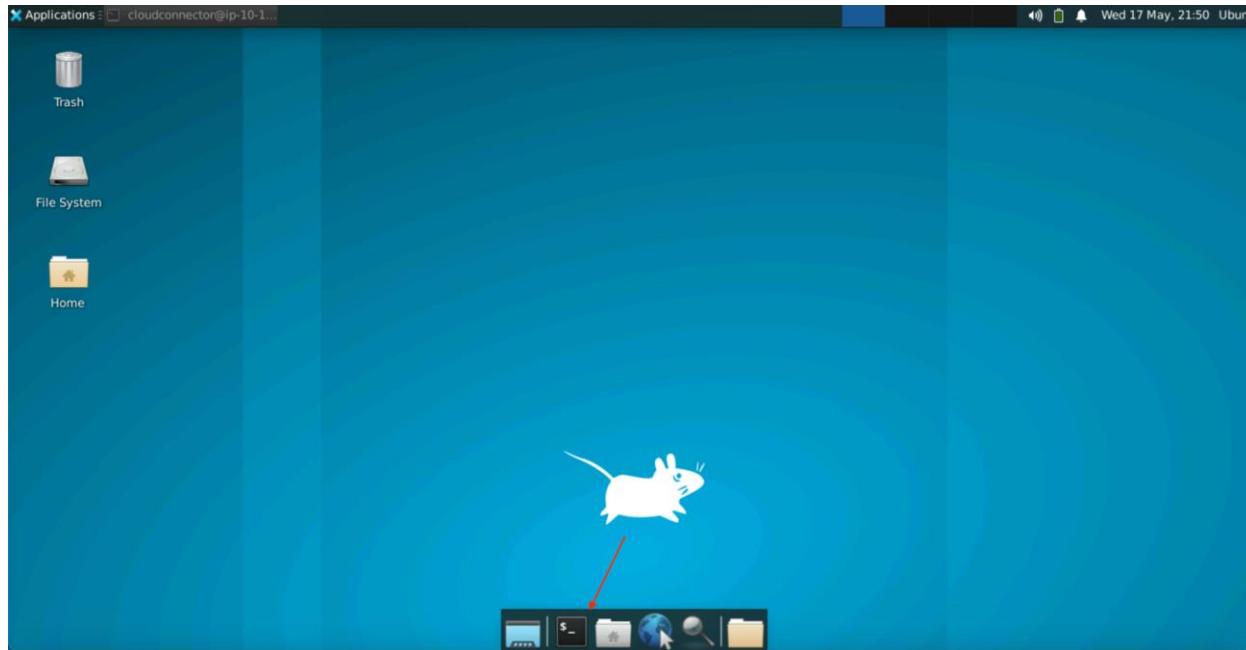
zs-cc-vpc-04af72f3f3cd483cb-us-east-2a, zs-cc-vpc-0851e47d75d6921b1-us-west-2a

Save Cancel



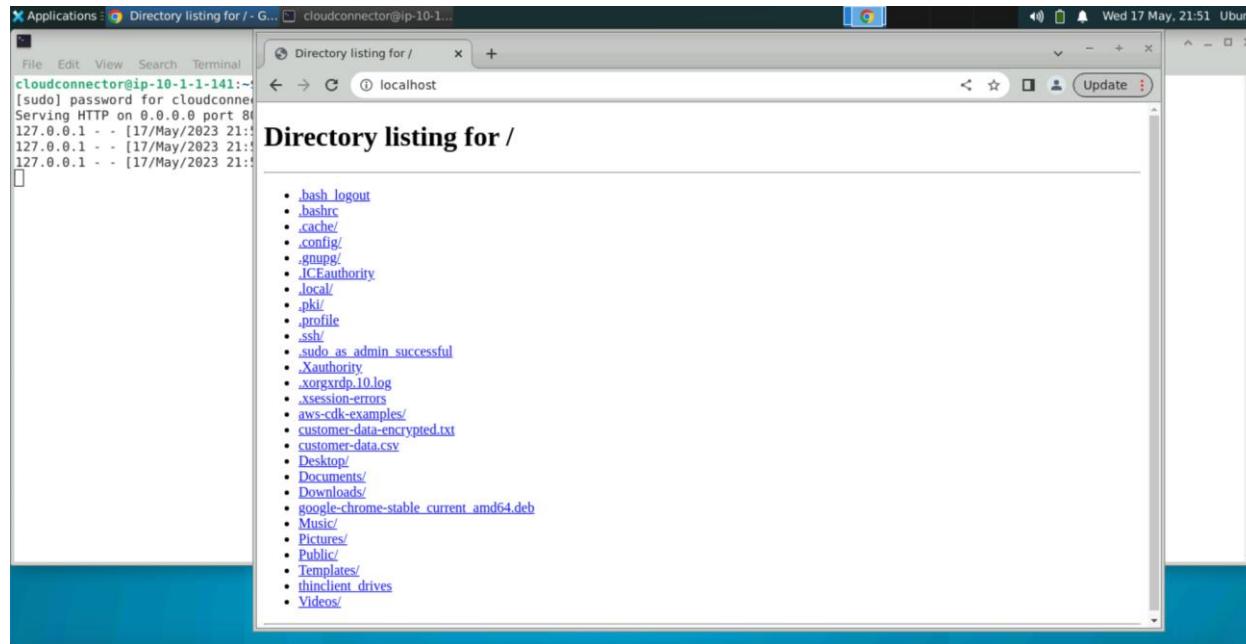
20. Next, it's time to test. Navigate to your **Region1** workload and open a Terminal.

Lab 9: Integrating with Zscaler Private Access



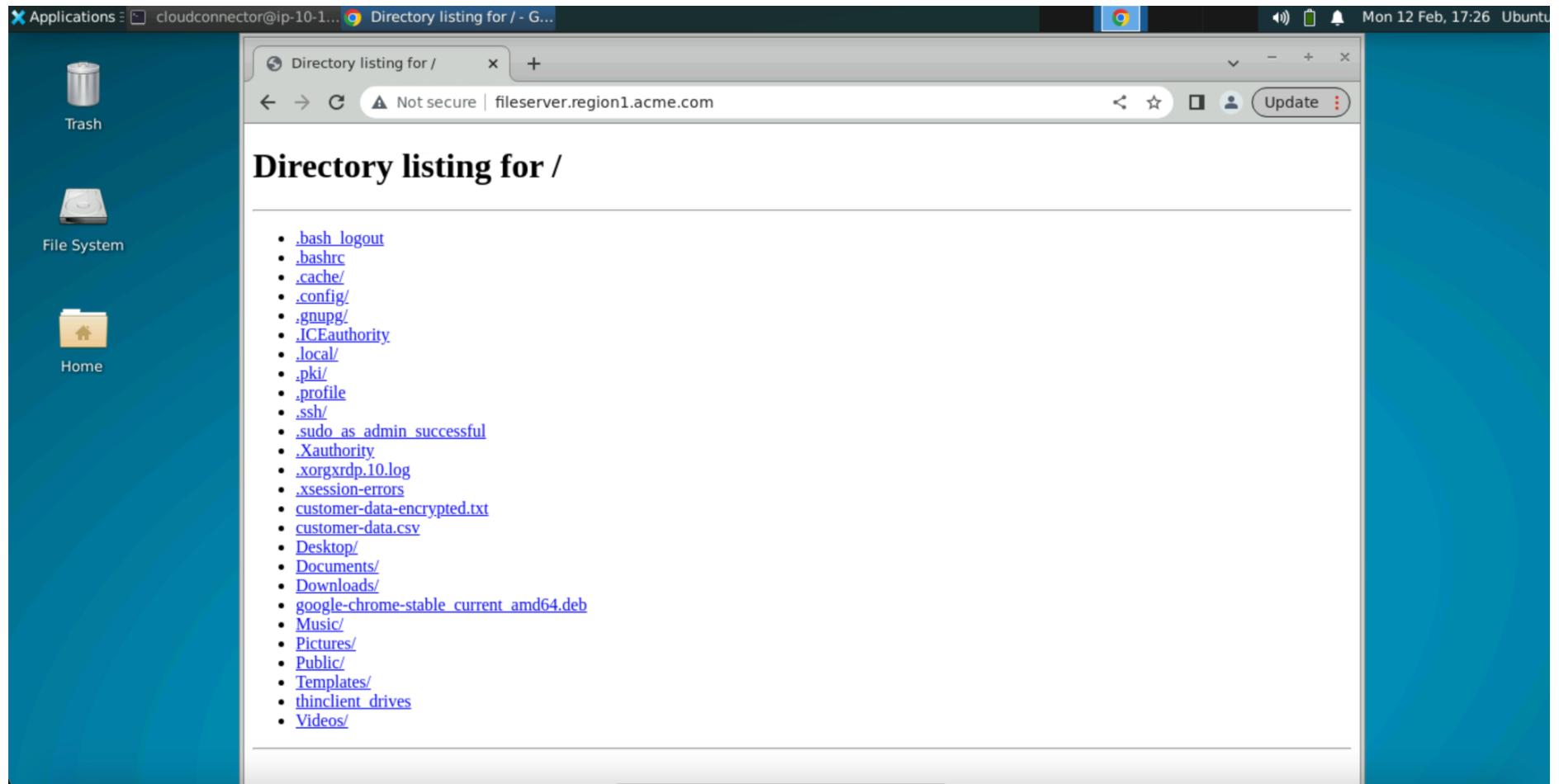
21. We'll use a simple Python-based web server for this test. Enter the command **sudo python3 -m http.server 80**. You may be prompted for a password. If so, enter your workload's sudo password: **CloudConnector2022!**.
22. Once started, the server should provide access to the user's Home directory. You can test this by opening a web browser and browsing to **http://localhost**. This should display the contents of the Home directory.

Lab 9: Integrating with Zscaler Private Access



23. Navigate to your **Region2** workload.

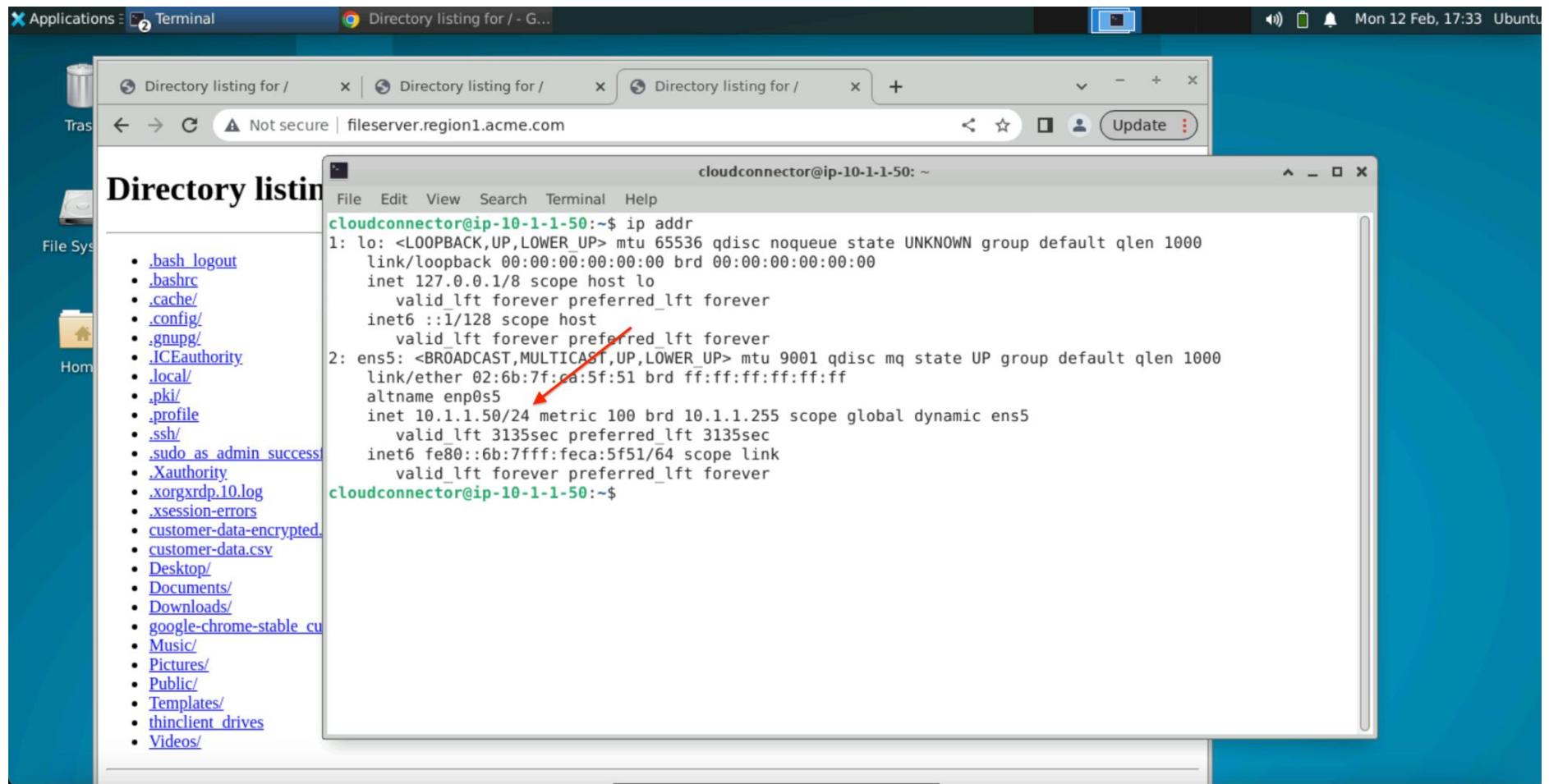
24. Open a web browser and enter <http://fileserver.region1.acme.com>. This should display the Region1 workload's Home directory.



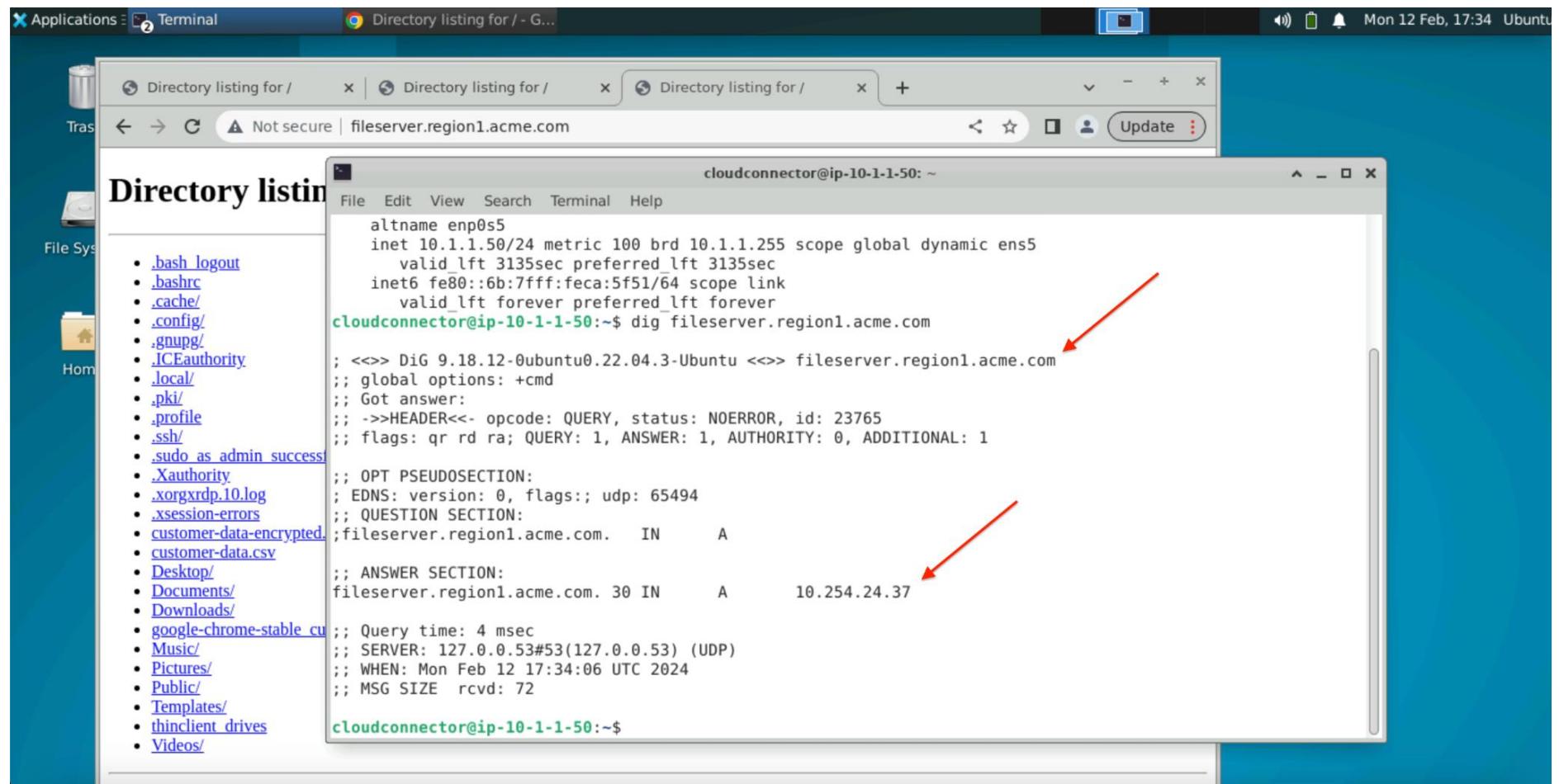
Congratulations! You've connected two workloads together over Zscaler Private Access!

Lab 9: Integrating with Zscaler Private Access

25.What's interesting here, however, is how this traffic was proxied. Open a terminal on your **Region2** host, then enter the command **ip addr**. Note the IP Address of the Region2 machine.



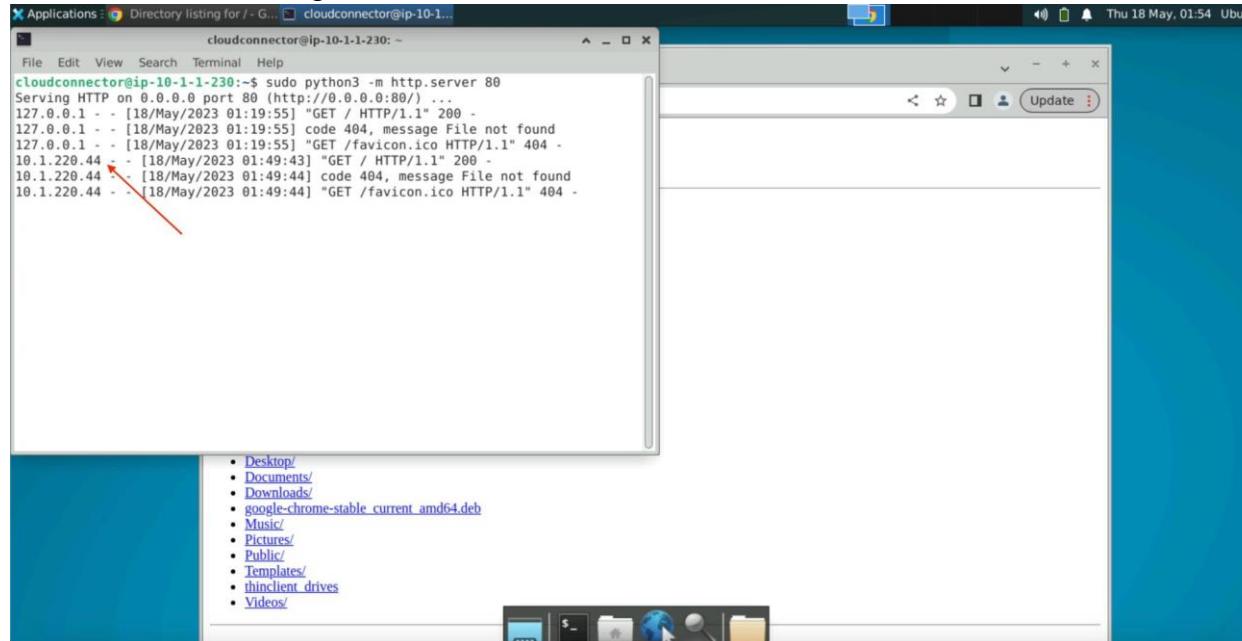
26.Similarly, enter the command **dig fileserver .region1.acme.com** from the terminal. Notice the IP Address that DNS returned for the remote web server.



Note: The IP Address returned should be within the Synthetic IP Pool we viewed in the Cloud Connector portal at the beginning of this module.

Lab 9: Integrating with Zscaler Private Access

27. Now, navigate to your **Region1** workload. Review the activity in the web server terminal that was logged when the Region2 host accessed this machine over ZPA. Notice the IP Address the web server saw is that of the App Connector - not the “real” IP Address of the Region2 workload!



28. Furthermore, open a new Terminal on the **Region1** workload.

29. Enter the command **ip addr**.

Note: If you recall, the IP Address that was returned in the dig command on the Region2 host was a different address. This means that the Region2 host is communicating with an IP Address that is not the “real” address of the destination web server! And likewise, the Region1 host was responding to an IP Address that was not the “real” source of the traffic. And, further, both workloads exist on the same subnet in two different Regions, meaning that ZPA handled the IP Address overlap for us!



As you can see, this entire communication was brokered through Synthetic IP Addressing via Cloud Connector and App Connector. These two regions were never directly connected, nor did “real” IP Address ranges ever exchange. This can make multi-cloud connectivity a breeze - especially when overlapping IP ranges are in place, such as with Mergers and Acquisitions or Divestitures!

Summary

Connecting workloads to the Internet across different networks is difficult. What makes this even more difficult is the traditional approach used by organizations to solve this challenge - such as technologies like VPNs and firewalls. While the outcome of connecting these workloads is achieved, the cost to achieve these goals is significant:

- Risk of lateral threats and internet-based attacks by over-extending the trusted network across the internet using VPN and WAN technologies
- Complexity increases because of complicated route filtering, multiple network hops, and fragmented policy management.
- Poor visibility across application connectivity paths and increased network blind spots.
- Increased costs due to overprovisioning network services and the use of virtual appliances such as firewalls, IPS, routers, and other point products in cloud environments.
- Limited scale and performance from the increase in network and security services used in cloud environments.

As a result, there is a need for a better approach to secure app-to-app and app-to-internet communications within multi-cloud environments. Zscaler Cloud Connector is a cloud-native zero trust access service that provides fast and secure app-to-app, app-to-internet connectivity across multi-cloud environments. With integrated, automated connectivity and security, it reduces complexity and cost and provides a faster, smarter, and more secure alternative to legacy network solutions.

Clean-up

Thank you for participating in the Zscaler for Workloads Hands-on Workshop! To help make the hands-on pods available for future users, please complete the following steps prior to logging out completely from your pod. This will ensure clean-up scripts can fully reset the environment prior to the next session:

1. Remove your ZPA Access Policy from the **Policy > Access Policy** page.
2. Remove your ZPA Segment Group from the **Resource Management > Application Management > Segment Group** page.
3. Remove your ZPA Application Segment from the **Resource Management > Application Management > Application Segments** page.
4. Remove your ZPA Server Group from the **Configuration & Control > Private Infrastructure > Server Groups** page.