Zscaler Deployment Guide

April 2021

Version 3.5

Zscaler Business Development – Solutions Architecture Team

Table of Contents

Table of Figures

Terms and Acronyms

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DC	Data Center
DMPO	Dynamic Multipath Optimization
DPD	Dead Peer Detection *(RFC 3706)*
GRE	Generic Routing Encapsulation *(RFC2890)*
IKE	Internet Key Exchange *(RFC2409)*
IPsec	Internet Protocol Security *(RFC2411)*
PFS	Perfect Forward Secrecy
PSK	Pre-Share Key
SSL	Secure Socket Layer *(RFC6101)*
VCE	VMware SD-WAN Edge
VCG	VMware SD-WAN Gateway
VCO	VMware SD-WAN Orchestrator
XFF	X-Forwarded-For *(RFC7239)*
ZCC	Zscaler Client Connector
ZIA	Zscaler Internet Access (Zscaler)
ZEN	Zscaler Enforcement Node (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

About This Document

Zscaler Overview

Zscaler (Nasdaq: ZS), **Zscaler** enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. For more information on Zscaler, please visit www.zscaler.com or follow them on Twitter @zscaler.

VMware SD-WAN Overview

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit https://www.vmware.com/company.html.

Audience

This guide is written for Zscaler Administrators, IT Administrators, and IT Analysts responsible for deploying, monitoring and managing SaaS services in an Enterprise environment. For additional product and company resources, please refer to the Appendix section.

Document Authors

This document was authored by Solution Architects in the Zscaler Business Development / Technical Alliances team (aka "BD SA"). All solutions validated within this guide have been jointly reviewed by both vendors.

Software Revisions

This document was written using Zscaler Internet Access v6.1 and VMware SD-WAN Orchestrator 4.2.

Request for Comments

- **For Prospects / Customers:** We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact us at:
    - partner-doc-support@zscaler.com
- **For Zscaler Employees:** If you are trying to reach the team that validated and authored the integrations contained within this document, please contact us at:
    - z-bd-sa@zscaler.com

1 Zscaler and VMware SD-WAN

This guide will provide GUI examples for configuring Zscaler Internet Access and VMware SD-WAN Orchestrator. All examples in this guide presumes the reader has a basic comprehension of IP Networking. All examples in this guide will explain how to provision new service with Zscaler and with VMware SD-WAN. The prerequisites to use this guide are:

Zscaler Internet Access (ZIA)

- A working instance of ZIA (any cloud)
- Administrator login credentials

VMware SD-WAN Orchestrator

- Enterprise account access to VMware SD-WAN Orchestrator
- Administrator login credentials
- One or more VMware SD-WAN Edge appliances with “Online” status in VMware SD-WAN Orchestrator

2 Configuring Zscaler Internet Access (ZIA)

2.1 Configuring Zscaler Internet Access

In this section, we will configure the Zscaler side first before configuring VMware SD-WAN.

2.1.1 Logging into ZIA

Log into Zscaler using your administrator account, as show in *Figure 1*. If you are unable to log in using your administrator account, please contact support:

https://help.zscaler.com/submit-ticket.

Figure 2.1.1-A: Log into Zscaler

2.2 Configure ZIA for API Access

The first step we need to do to enable ZIA for API access is to create a SD-WAN "*Partner Key*". The *Partner Key* is simply an API key, which will be used as one form of authentication. The second form of authentication will be admin partner username and password, which will be explained further in this Deployment Guide. This admin credential set can only be used for API calls and will not work with the ZIA admin UI. Please follow the navigation below, which is also depicted in *Figure* 2.2-A.

Navigation: Administration → Cloud Configuration → Partner Integrations

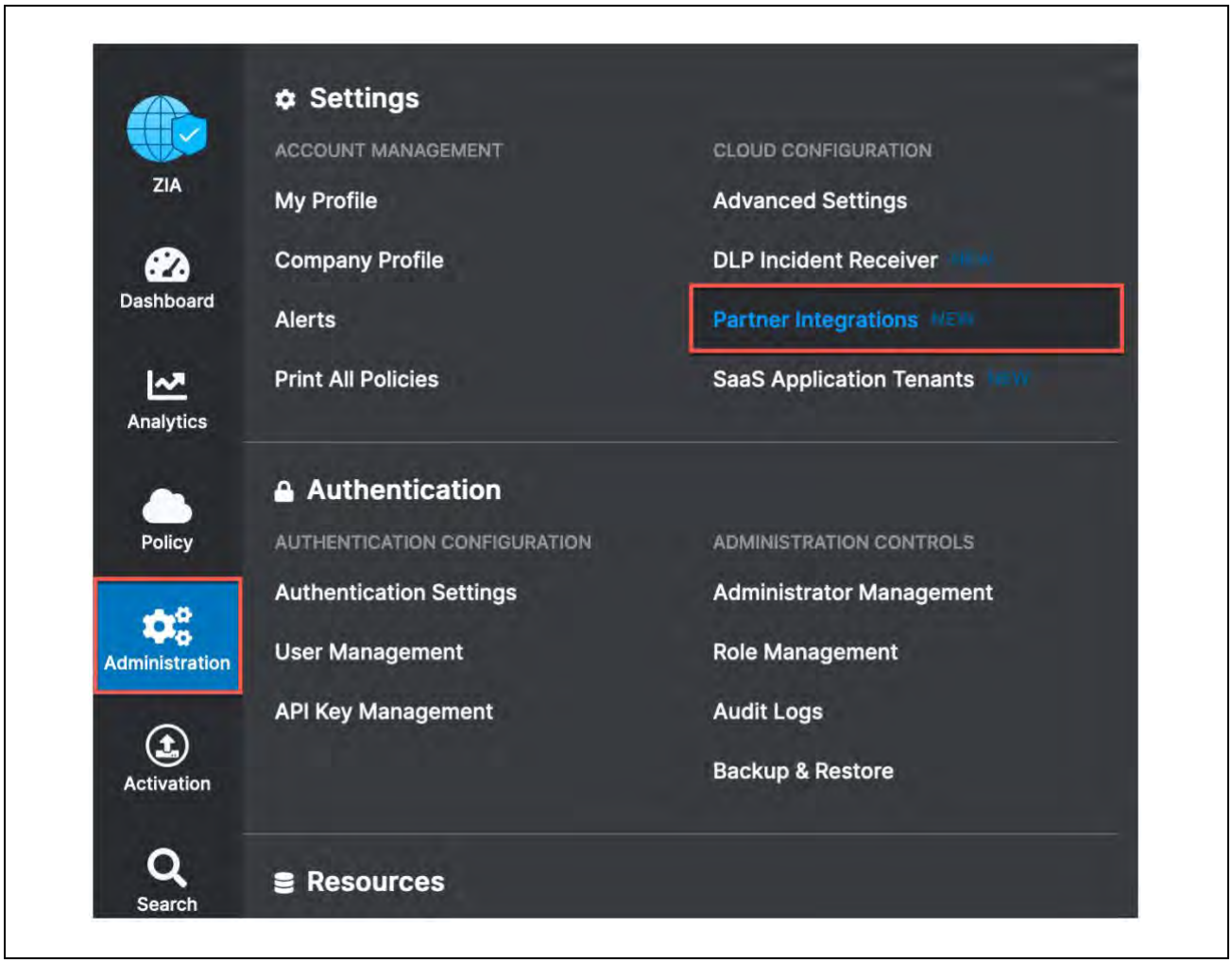

Figure 2.2-A: Configuring ZIA for API Access

2.2.1 Adding SD-WAN Partner Key

At the "*Partner Integration*" section of the ZIA Admin UI, please select "*SD-WAN*" and then "*Add Partner Key*", as shown in *Figure* 2.2.1-A.

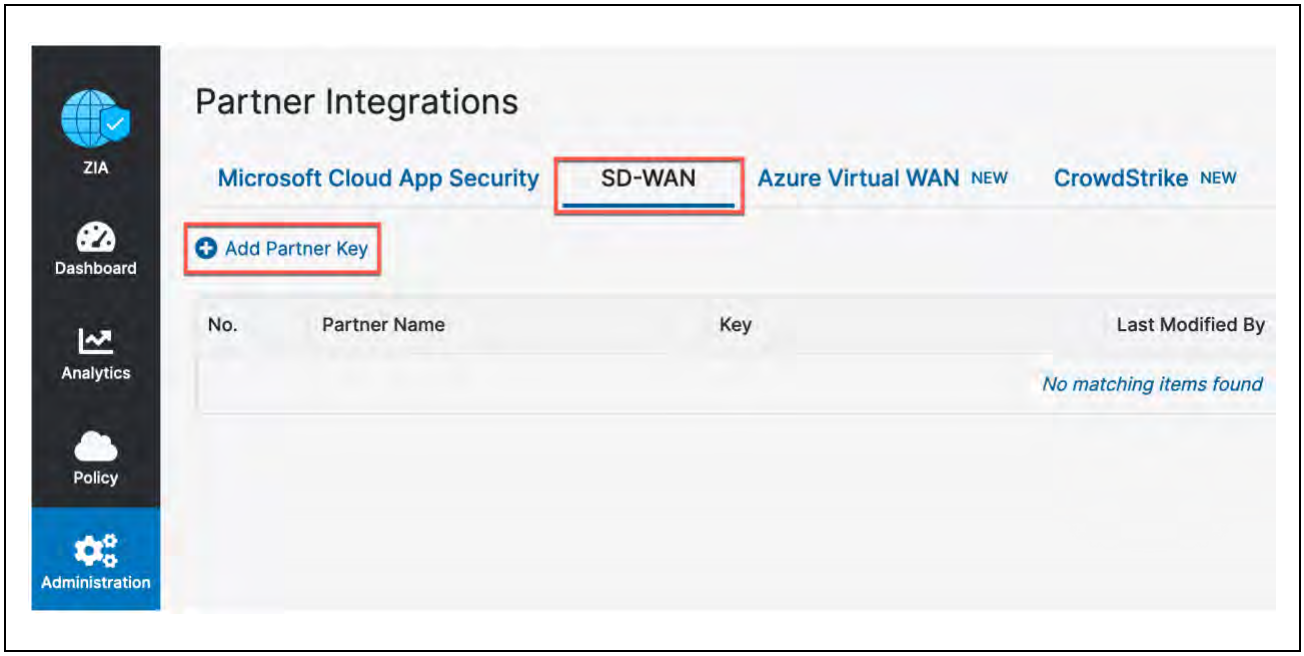

Figure 2.2.1-A: Add Partner Key

A window will appear, as shown in *Figure* 2.2.1-B. One the right side of the window, you can type in or select from the drop-down arrow on the right, which SD-WAN vendor you wish to create a *Partner Key* for. After typing or selection "*VMware Velocloud*", click on "*Generate*". After, you will return to the prior screen.

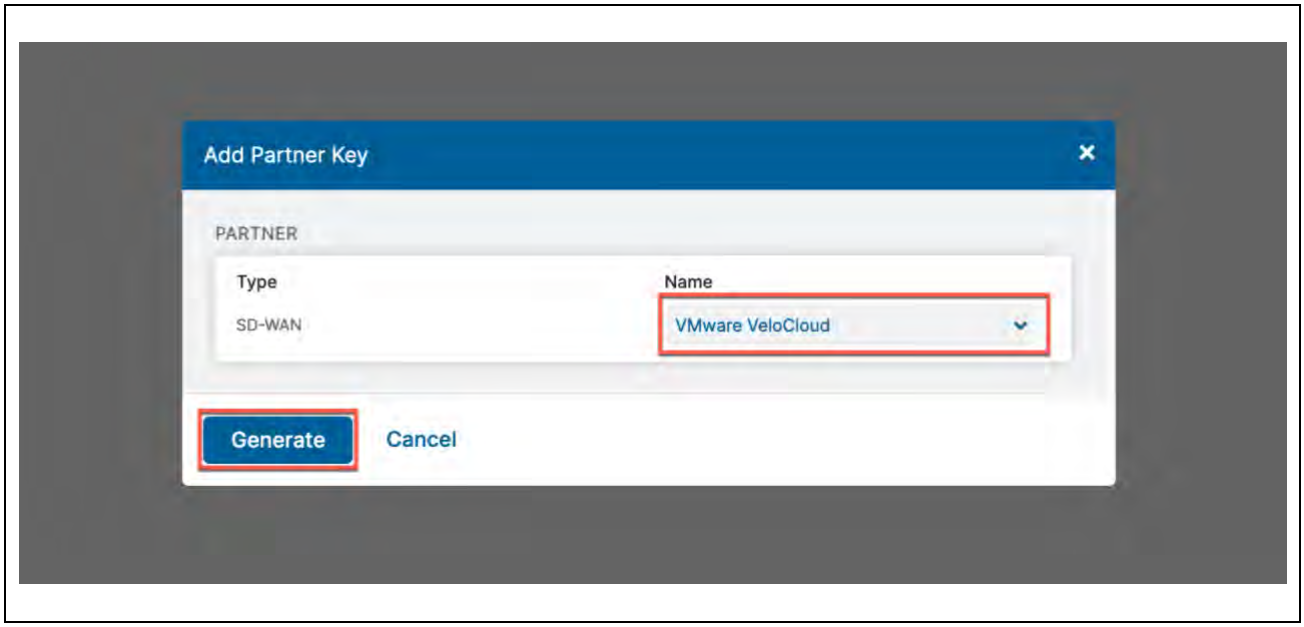

Figure 2.2.1-B: Add SD-WAN Partner Key

2.2.2 Verify SD-WAN Partner Key

Once you return to the screen shown in *Figure* 2.2.2-A, you should see the *Partner Key* you created for VMware SD-WAN. *Note: The Key will not be obfuscated as is in the figure.* The password has been hidden for the purpose of this document. You should also see a red circle, with a number, above the "Activation" icon. Although we have created a *Partner Key*, the configuration change is pending. Only after activation the change will this configuration become active.

Note: The "*Key*" value will be required in Step *3.1.2*. Make sure to copy it down as you will need to enter them in the VCO.

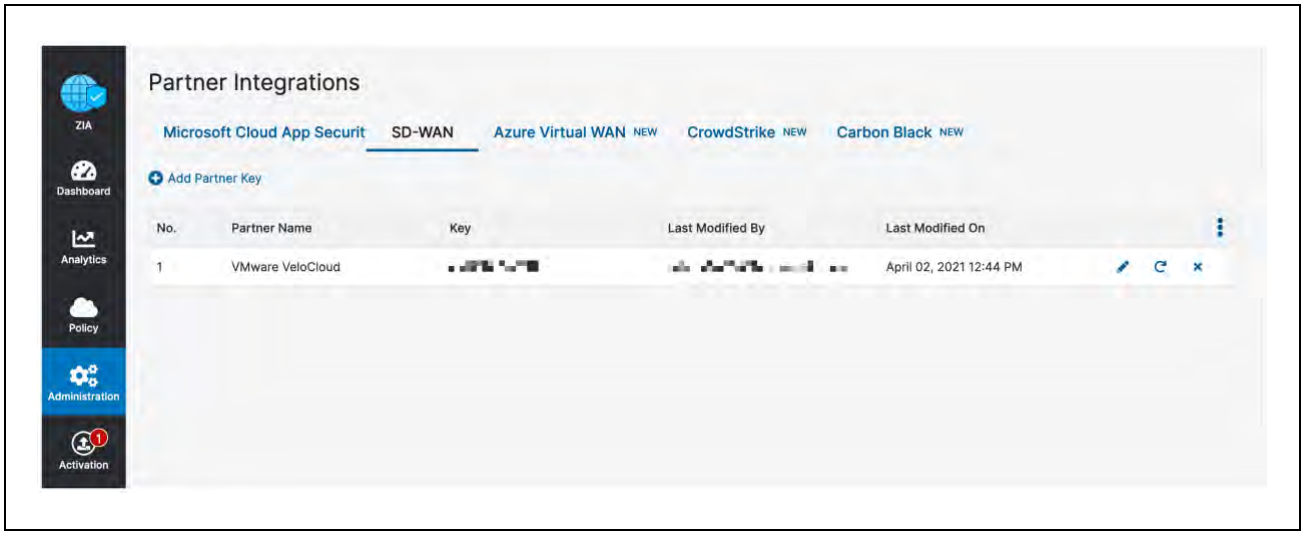

Figure 2.2.2-A: Verify SD-WAN Partner Key

Key obfuscated for security

At this point, you could active the change, but we suggest you batch changes. With this said, this Deployment Guide will tell you when you should active pending changes.

2.2.3 Adding a Partner Administrator Role

A Partner Admin role will need to be created so it can be assigned to the Administrator user that will be used to authenticate against the Zscaler ZIA Provisioning API.

Navigation: Administration → Authentication → Role Management

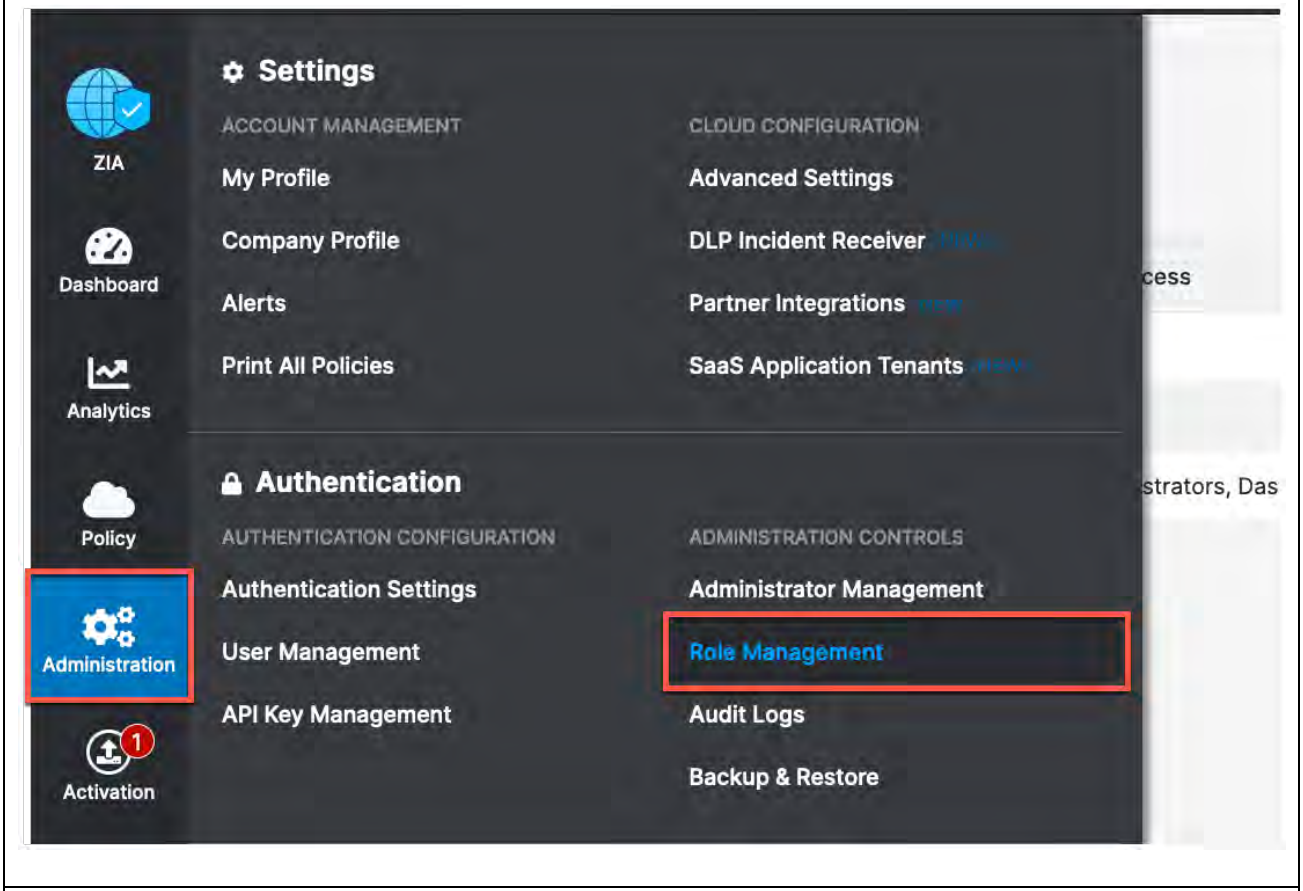

Figure 2.2.3-A: Adding Partner Administrator Role

2.2.4 Creating Partner Administrator Role

Clicking on the "*Add Partner Administrator Role*" option will bring up a window.

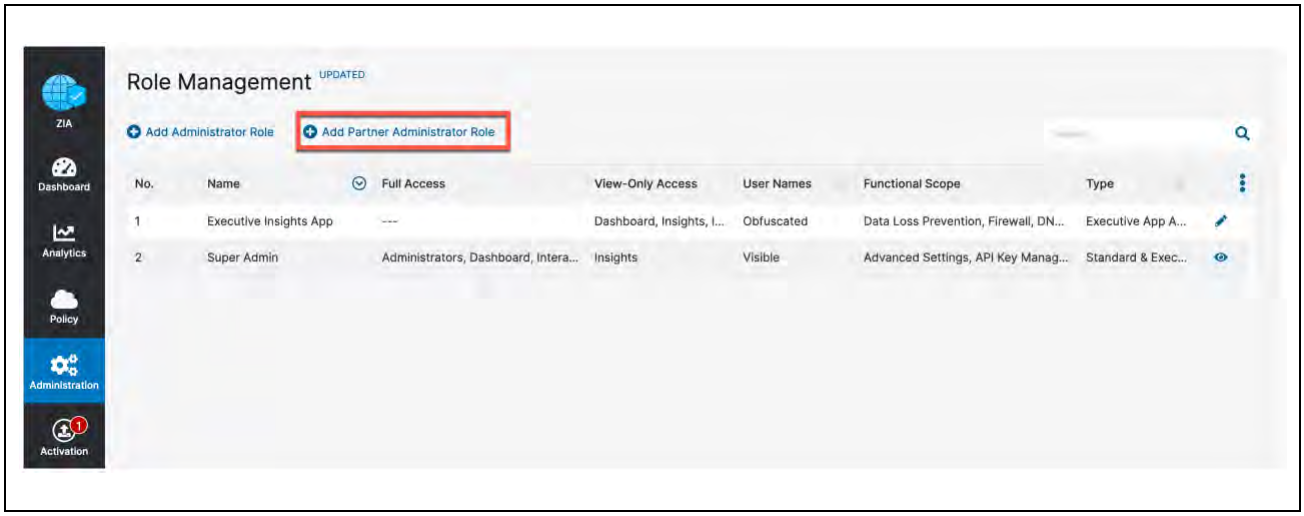

Figure 2.2.4-A: Add Partner Administrator Role

By creating a *Partner Administrator Role*, we can define the permission and access we wish to grant to a third-party partner, such as a SD-WAN partner. Once you name the *Partner Administrator Role*, change the Access Control to "Full", as shown in *Figure* 2.2.4-B The toggle "*Full*" allows partner admins to view and edit VPN credentials and Locations that VCO is managing via ZIA Provisioning API. This is necessary for the VCO to be able to create new VPN Credentials and Locations for branch locations. Once you have completed these steps, click "Save". After you will be returned to the prior screen.

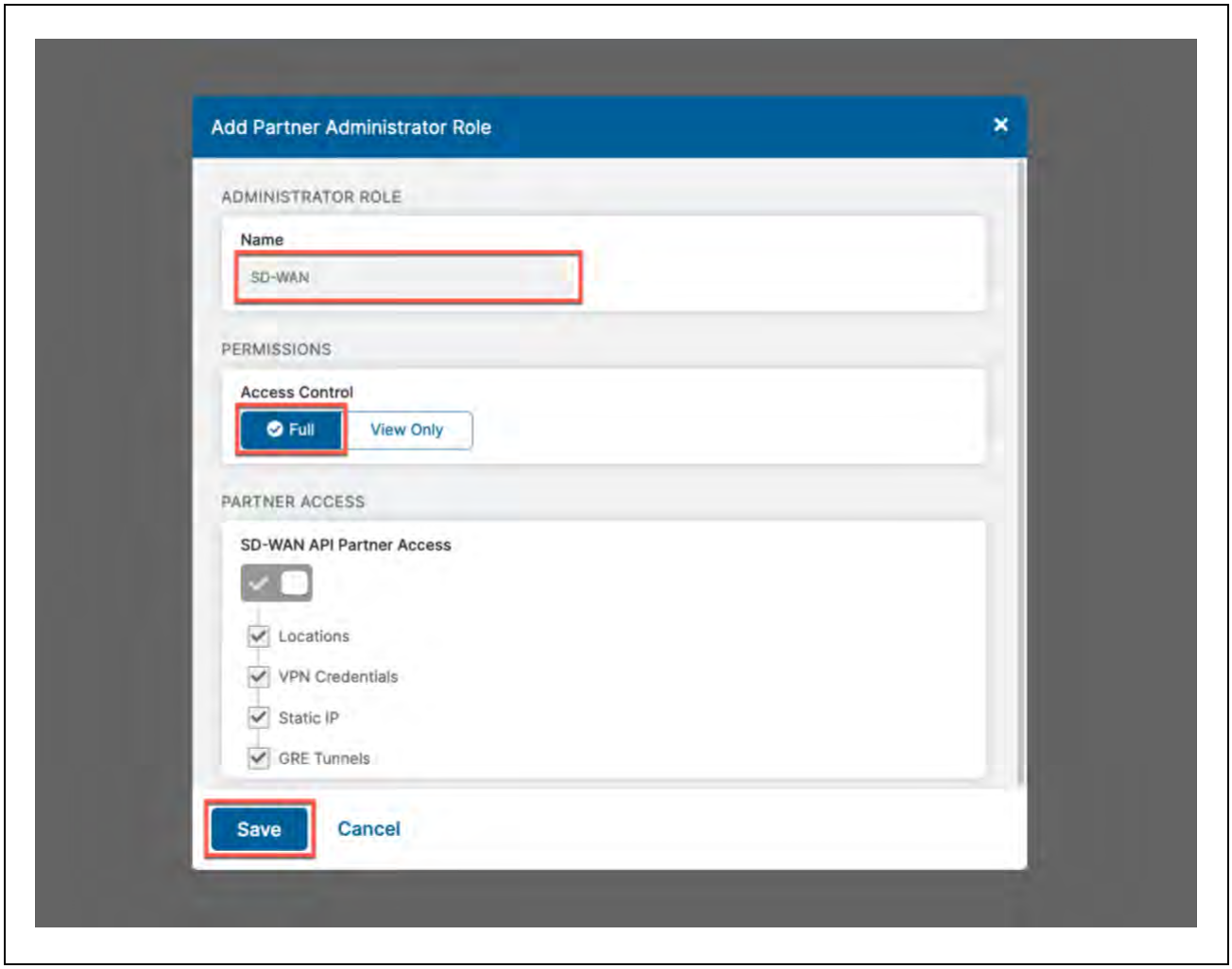

Figure 2.2.4-B: Creating Partner Administrator Role

2.2.5 Administrator Management

The last step required is creating a *Partner Administrator*. Please follow the navigation below, which is also depicted in *Figure* 2.2.5-A.

Navigation: Administration → Administration Controls → and then click **Administrator Management**

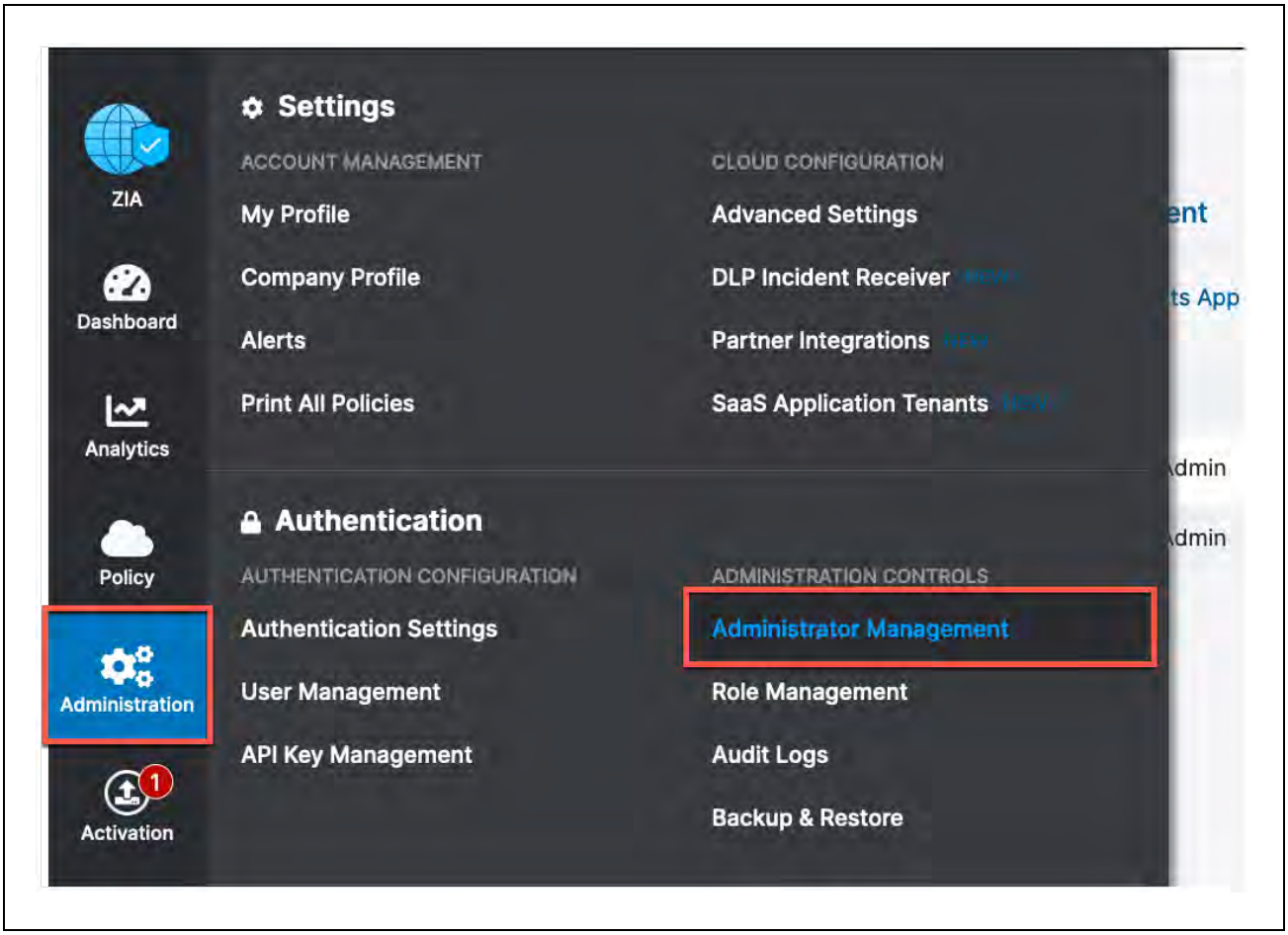

Figure 2.2.5-A: Administrator Management

2.2.6 Add Partner Administrator

Once you arrive to the "*Administrator Management*" page, please select "*Add Partner Administrator*", as show in *Figure* 2.2.6-A. A user input screen will appear, which is shown in the next section.

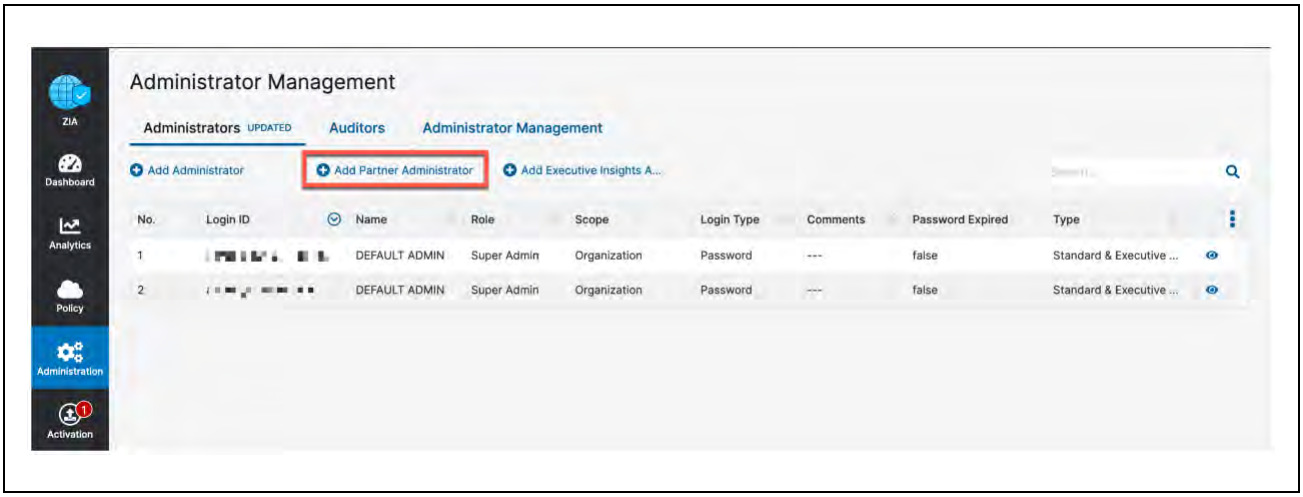

Figure 2.2.6-A:Admin Partner Administrator

Login ID's obfuscated for security

2.2.7 Creating Partner Administrator

Once the "*Add Partner Administrator*" input box appears, fill in the fields with red boxes around then, as shown in *Figure* 2.2.7-A. Once this is completed, click "*Save*".

Note: Save these settings as you will need to enter them in VCO.

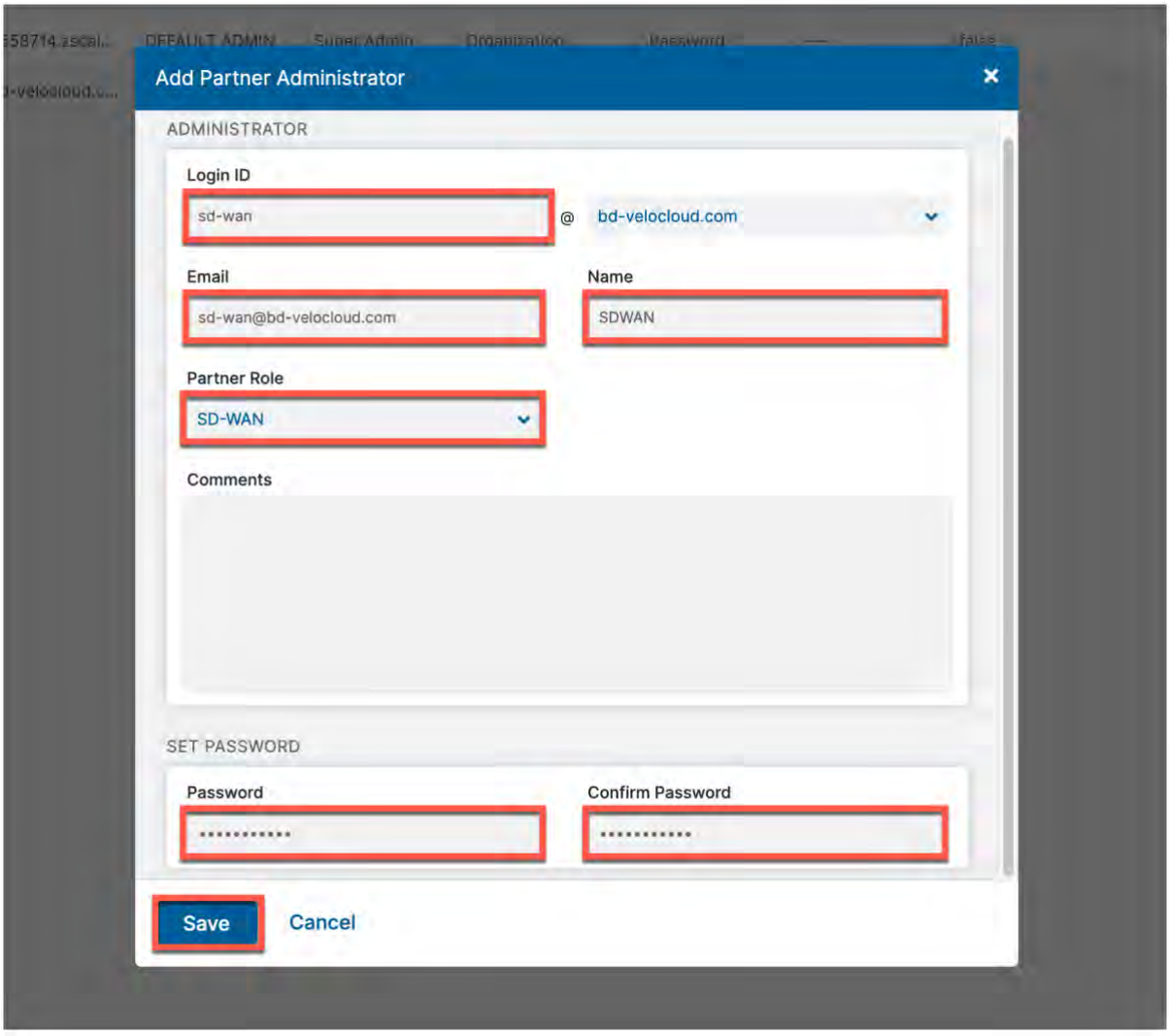

Figure 2.2.7-A: Creating Partner Administrator

2.2.8 Active Pending Changes

Finally, we have reached our last step in the Zscaler ZIA Admin UI. You can now navigate to "*Activation*" and activate the pending configurations, as shown in *Figure* 2.2.8-A.

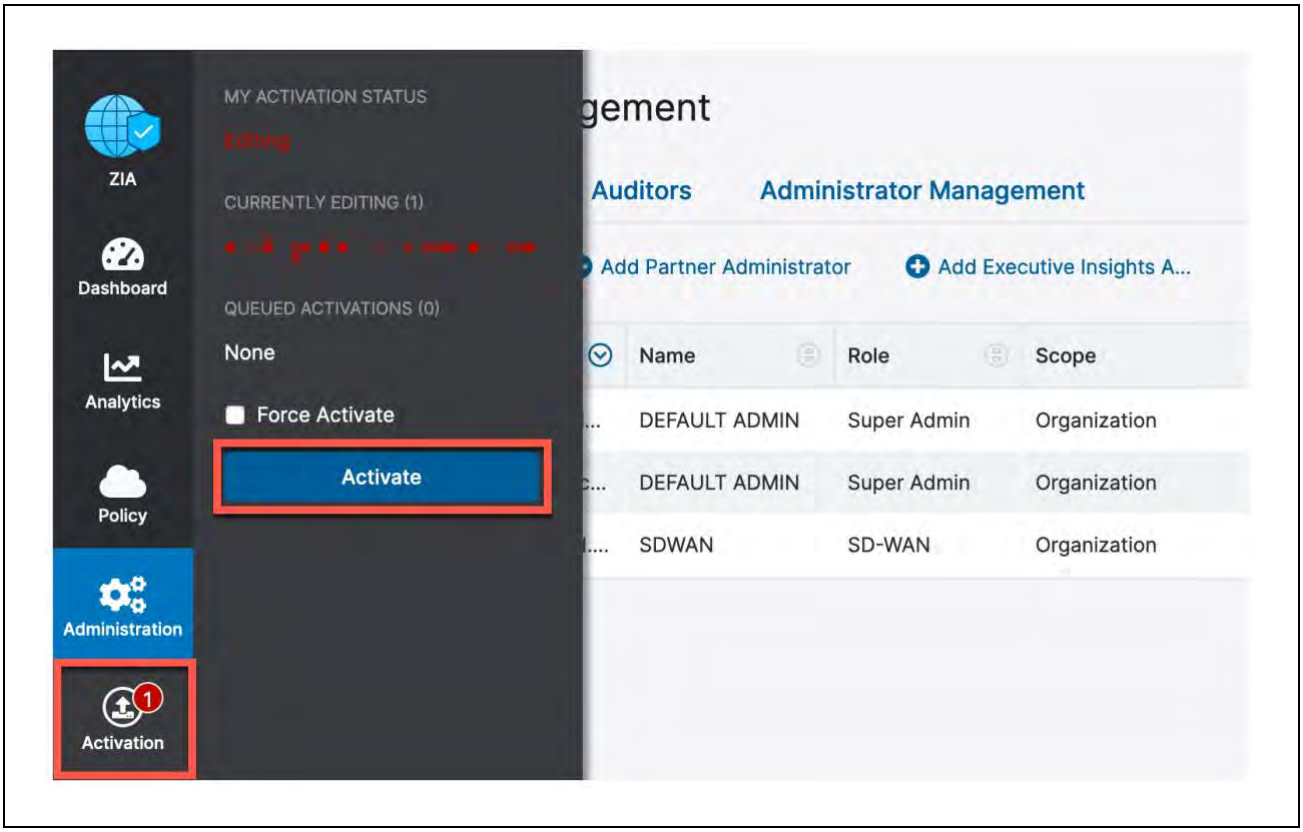

Figure 2.2.8-A: Activate Pending Changes

Login ID obfuscated for security

2.2.9 Verify Activation

After activating pending changes, you should be returned to the prior page, and "*Activation Complete*" should appear in the top of the window, as shown in *Figure* 2.2.9-A.

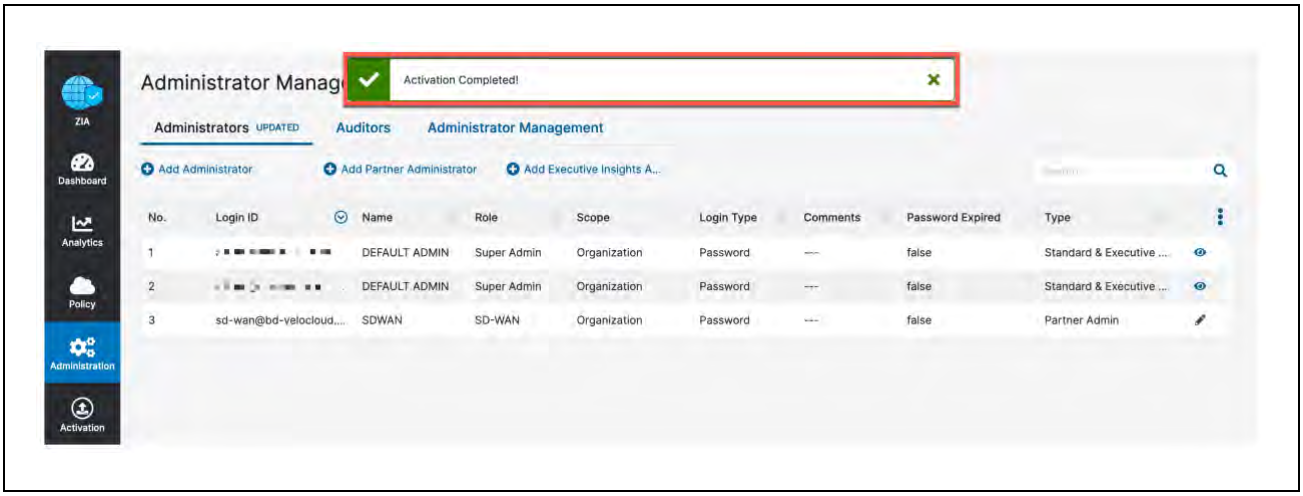

Figure 2.2.9-A: Verify Activation

Login ID's Obfuscated for security

3 Configuring VMware SD-WAN

This section will cover 3 deployment models:

1) Configuring Automated IPsec Tunnels from VMware SD-WAN Edge (VCE)
2) Configuring GRE Tunnel to ZIA from VMware SD-WAN Edge (VCE)
3) Configuring IPsec Tunnel from VMware SD-WAN Gateway (VCG)

The configuration is up to date as of VMware SD-WAN Release 4.2.0.

3.1.1 Configuring Automated IPsec Tunnel from VCE

First, we need to create a Clous Security Service Site entry for Zscaler.
Navigation: Configure → Network Services → Cloud Security Service → New.

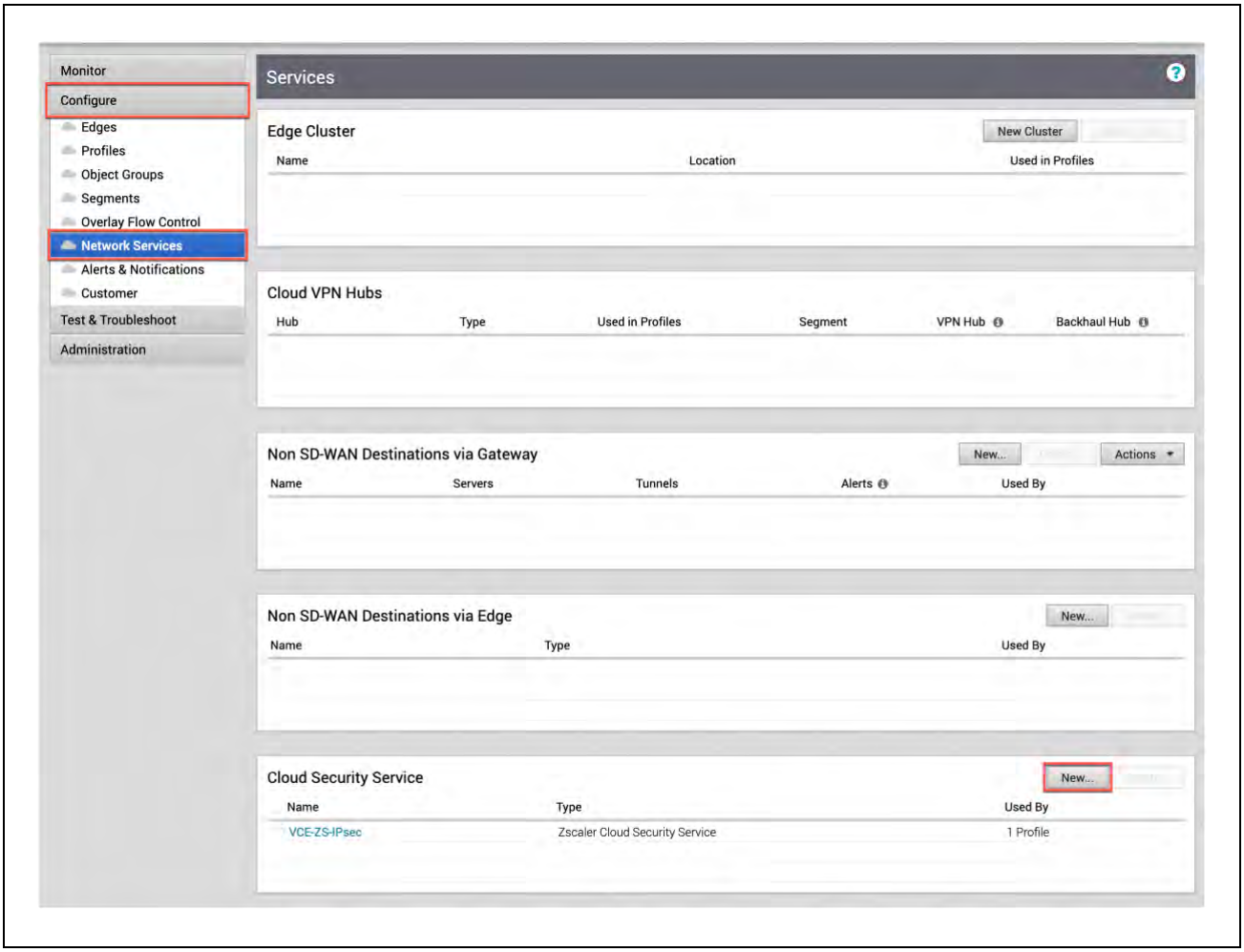

Figure 3.1.1-A: Configuring new Cloud Security Service

3.1.2 New Cloud Security Provider for Automated Deployment

After selecting “New”, a pop-up should appear, as shown below. You need to configure:

Figure 3.1.2-A: New Cloud Security Provider

1) **Service Type:** Zscaler Cloud Security Service
2) **Automated Cloud Service:** Enable
3) **Zscaler Cloud:** Type in the name of the Zscaler cloud you are provisioned in.
4) **Partner Admin Username:** Type in the *Partner Admin Username* you provisioned.
5) **Partner Admin Password:** Type in the *Partner Admin Password* you provisioned.
6) **Partner Key:** Type in the *Partner Key* you provisioned. Gotten from Step 2.2.2
7) **Domain:** Type in the domain name your ZIA instance is provisioned wit (typically your company domain). This can be found by going to the **Administration → Company Profile** selection in the Zscaler Admin portal.

Once you have completed filling in these fields, click the “Validate Credentials” Button.

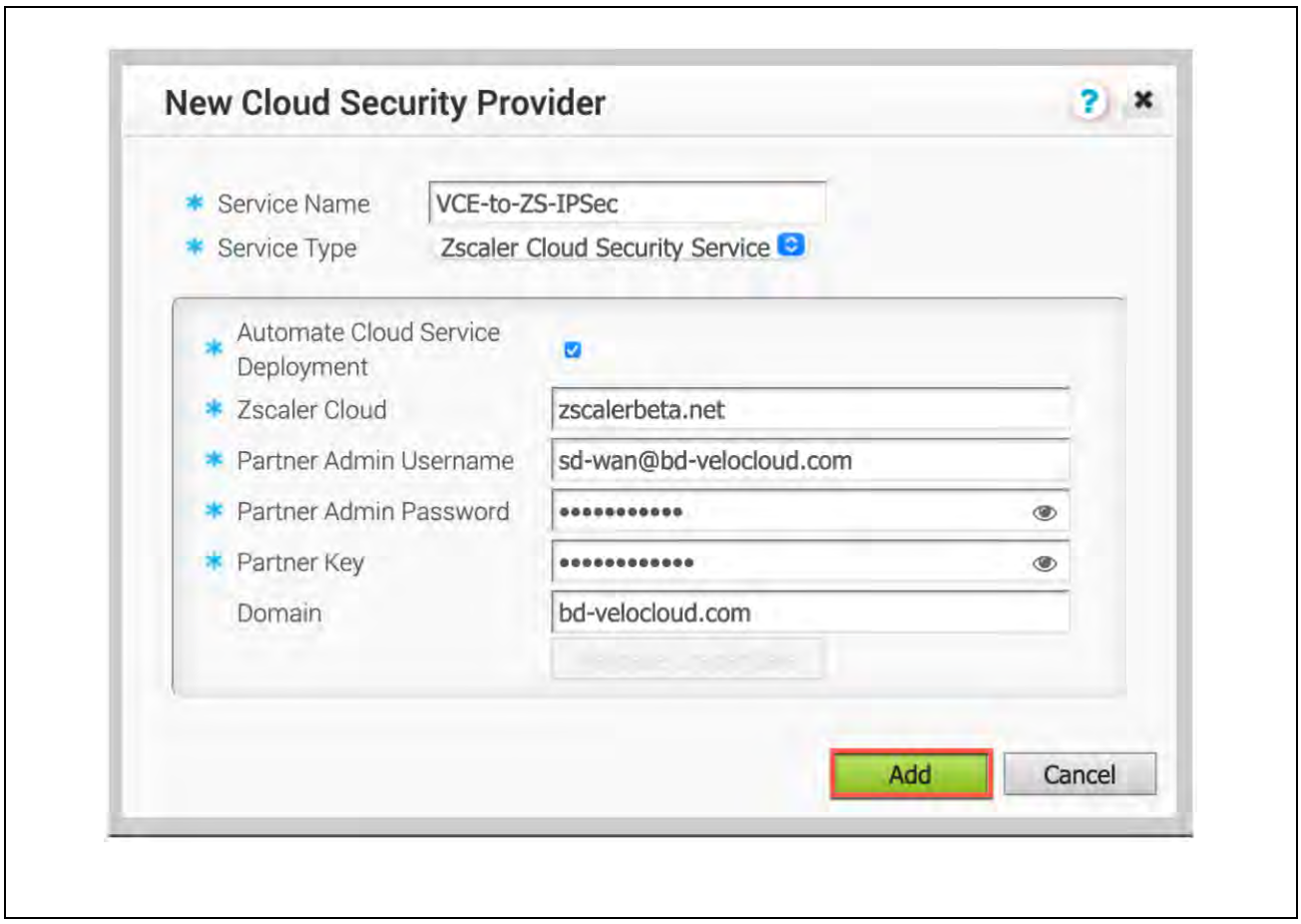

Figure 3.1.2-B: Save Cloud Service Provider Configuration

If all the information is correct, then the “Add” button will turn a brighter green and you will be able to click add to save the Network Service

Figure 3.1.2-C: Check for Cloud Security Provider Errors

If you have any errors in the date inputted from *Figure* 3.1.2-B, you will see a red warning icon (*Figure* 3.1.2-C) next to the "Validate Credentials" button and the "Add" button will remain dimmed and unclickable. You will need to verify and correct that the information entered is accurate.

3.1.3 Profile for Cloud Security Service

In this section, navigate to **Configure → Profiles**. Once you select the profile you wish to use, select "Device". You need to configure:

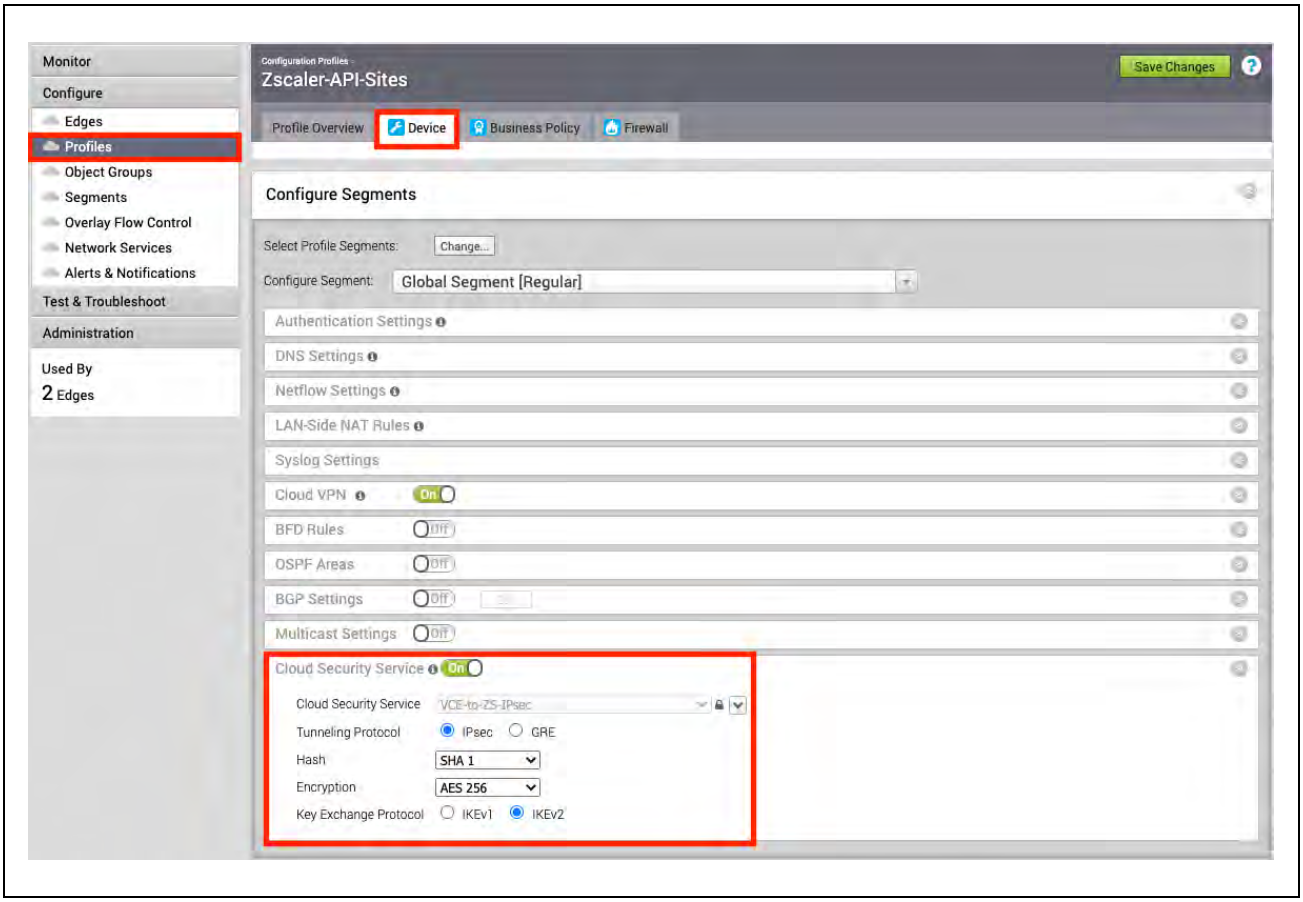

Figure 3.1.3-A: Profile for Cloud Security Service

1) **Cloud Security Service:** Select it "On"
2) **Cloud Security Service:** Select the Cloud Security Service you configured in the prior section
3) **Tunneling Protocol:** IPsec
4) **Hash:** Select SHA1 or SHA256
5) **Encryption:** Select None, AES-128 or AES-256 per your requirements
6) **Key Exchange Protocol:** IKEv2

Once you have completed these fields, select "Save Changes" in the upper right of your screen. This will cause the VCO to make outbound API calls to Zscaler and automatically configure all the Edge's using the Profile.

3.1.4 Monitor Provisioning Status

Navigate to **Monitor** → **Events** and you should see the events showing the VCO configuring the automatic IPsec Tunnels for each Edge.

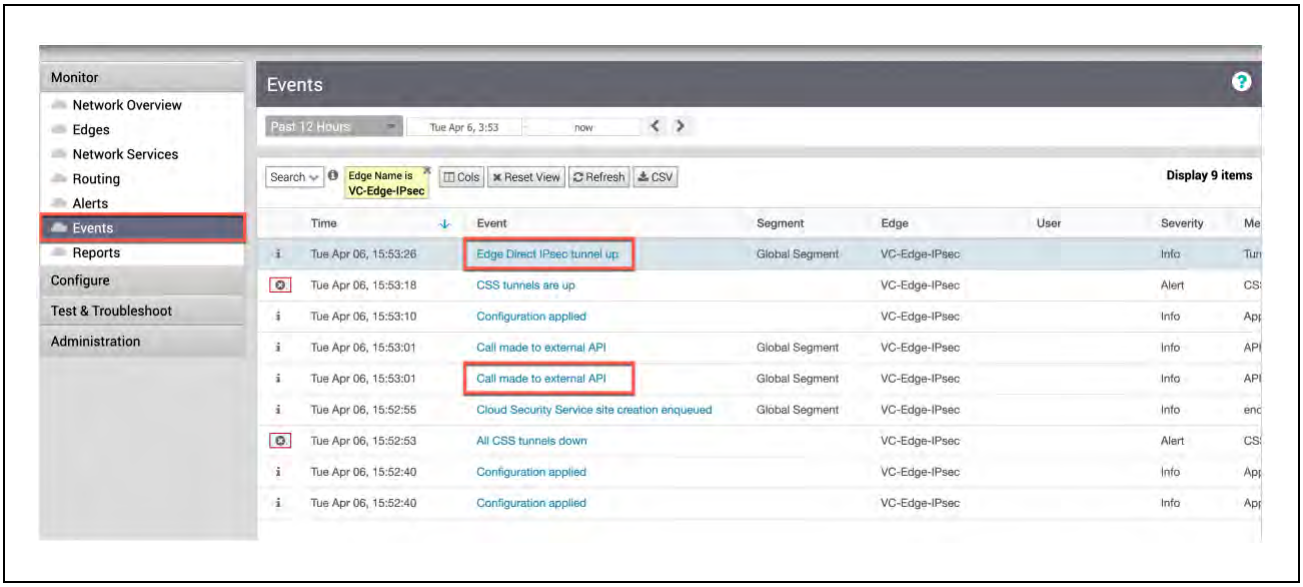

Figure 3.1.4-A: API Automation Events

3.1.5 Automated IPsec Tunnel for Edge

After several seconds to a few minutes, the IPsec Tunnels from the Edges using the configured Profile should automatically establish IPsec Tunnels from its public WAN interfaces. For any parameter changes needed at specific sites, you may navigate to **Configure → Edges → and select the VCE you want to configure** and check the **Enable Edge Override** option to change the IPsec parameter.

If there are no changes from the Profile and the API call succeeded for the Edge, you should see the **Credentials** automatically populated. The automated IPsec tunnel configuration is complete, and you may configure Business Policies to forward user traffic to Zscaler.

Figure 3.1.5-A: Automated IPsec Tunnel from VCE

3.1.6 Verify Tunnels are Up (Active)

To verify the state of the Automated IPsec tunnel, navigate to **Monitor → Edges**. You may have to wait 30 seconds, but you should see the primary IPsec tunnel establish. The standby tunnel will remain grey until it becomes active, which should only occur if the primary IPsec tunnel fails.

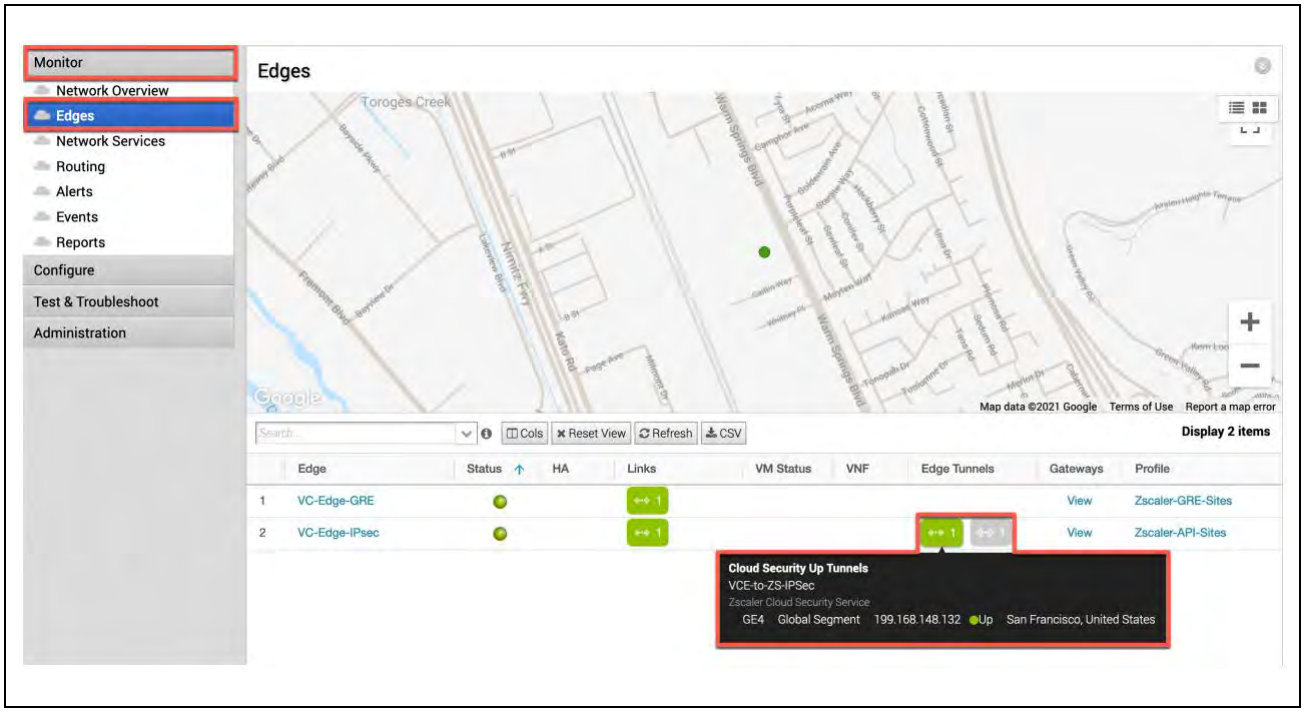

Figure 3.1.6-A: Monitor Edge Tunnels

3.2 Configure GRE Tunnel from VCE to ZIA

It is recommended that you perform the steps required in ZIA admin before performing the configuration in the VCO:

- Locate the primary and secondary ZIA DC VPN endpoints from config.zscaler.com.
- Add the Static IP for the GRE tunnel source, refer to section: *Add a Static IP Configuration*.
- Link the Static IP to a GRE Tunnel configuration, refer to section: *Add a GRE Tunnel Configuration*.
- Create a Location and assign the GRE tunnel to that location so the traffic will get the proper policy, refer to section: *Appendix C: ZIA - Configuring a Location for Manual Tunnels*.

3.2.1 New Cloud Security Provider for GRE

First, we need to create a Cloud Security Service entry for Zscaler. Navigate to **Configure → Network Services → Cloud Security Service → New**.

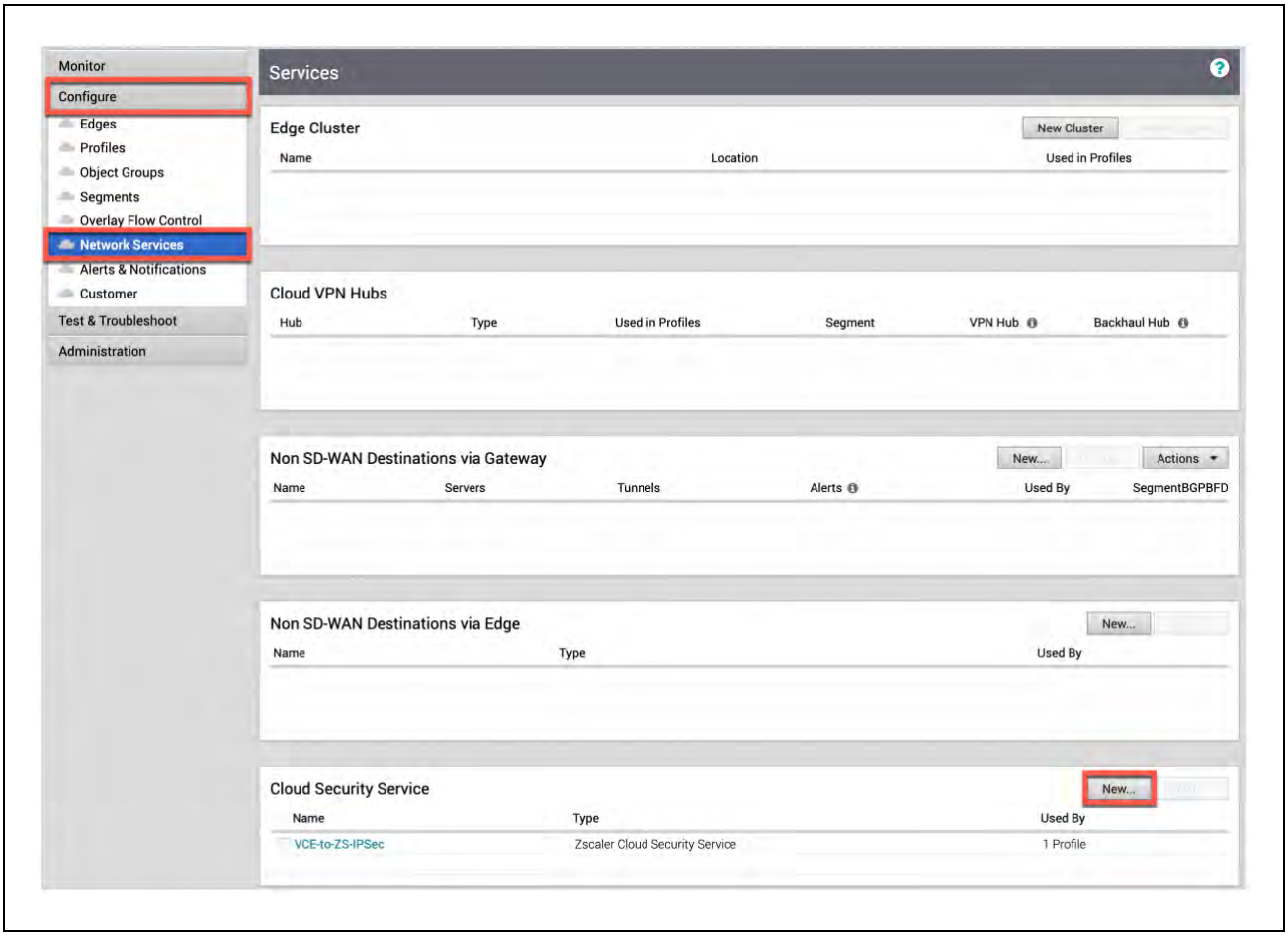

Figure 3.2.1-A: Configuring new Cloud Security Service for GRE tunnels

After selecting “New”, a pop-up should appear, as shown below. You need to configure:

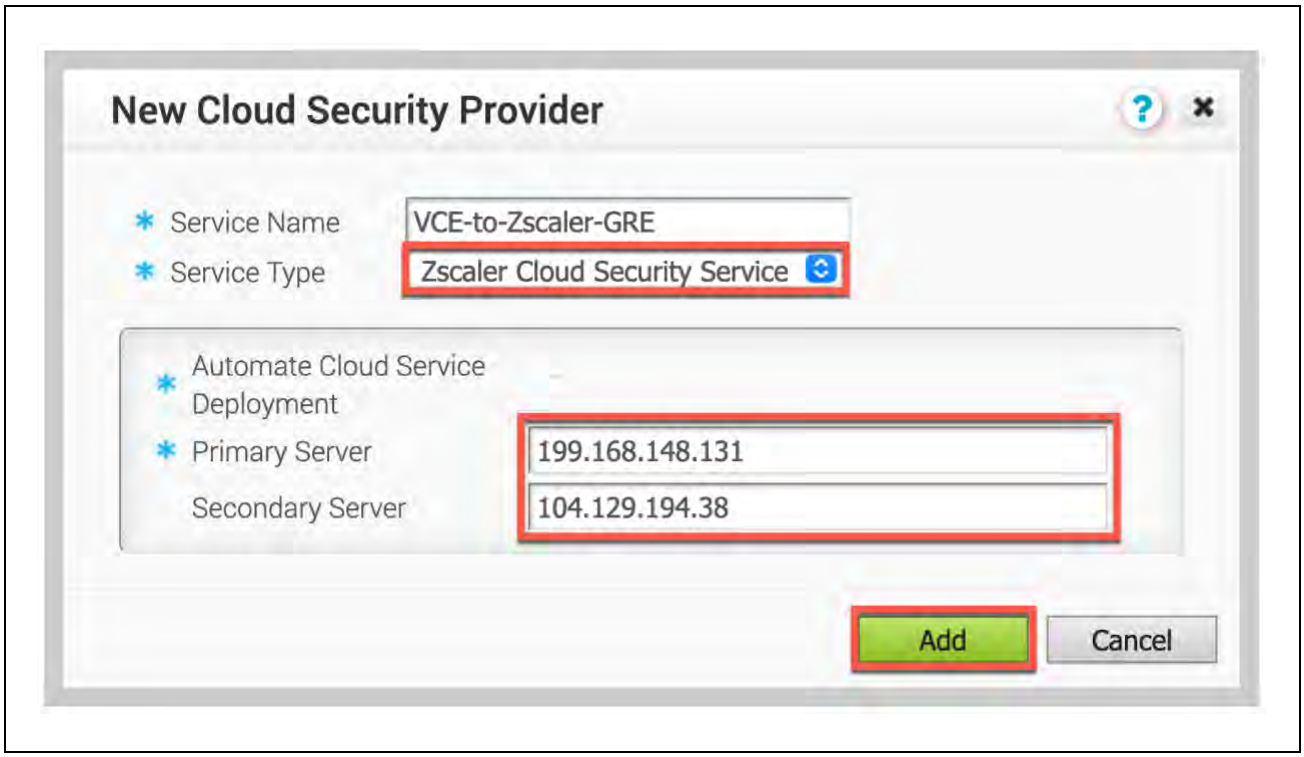

Figure 3.2.1-B: New Cloud Security Provider for GRE

1) **Service Type:** Zscaler Cloud Security Service

2) **Primary and Secondary Server:** Obtain the GRE VIP IP from the Zscaler IP Pages (look at Appendix). You should use the IP Pages for the Zscaler cloud you are provisioned in (e.g., ZS3).

Once you have completed filling in these fields, select “Add” to continue.

3.2.2 Profile for Cloud Security Service

In this section, navigate to **Configure → Profiles**. Once you select the profile you wish to use, select "**Device**". You need to configure:

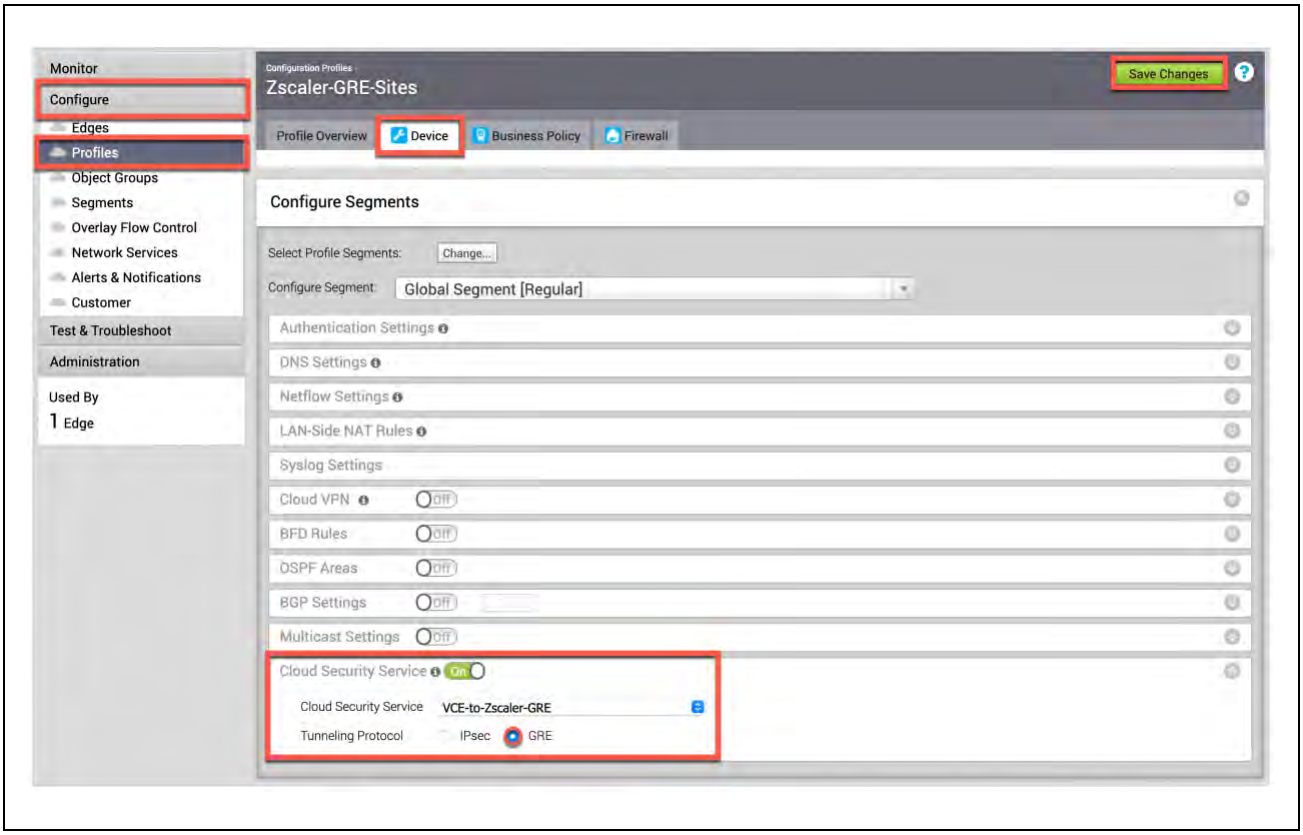

Figure 3.2.2-A: Profile for Cloud Security Service

1) **Cloud Security Service:** Toggle it "On"

2) **Cloud Security Service:** Select the Cloud Security Service you configured in the prior section

3) **Tunneling Protocol:** Select GRE

Once you have completed these fields, select "Save Changes" in the upper right of your screen.

3.2.3 Edge Device configuration for GRE

Next you need to navigate to **Configure → Edges** -> and select the VCE you want to configure the GRE tunnel on. Next select "**Device**" and then scroll down to configure:

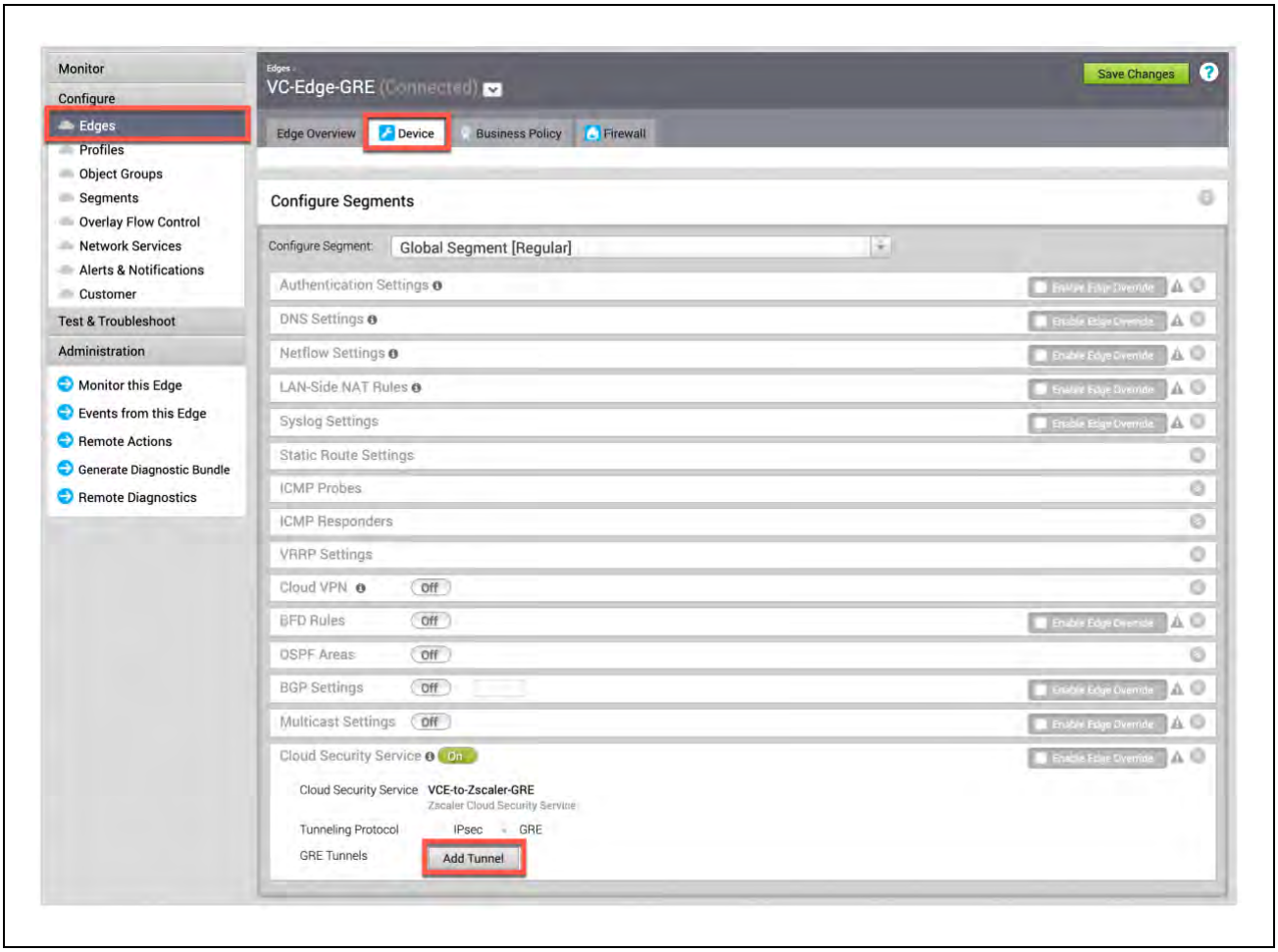

Figure 3.2.3-A: GRE Tunnel for Edge (VCE)

The Cloud Security Service section is already inherited from the previous profile configuration step. Click the "Add Tunnel" button next to the **GRE Tunnels:** selection.

3.2.4 GRE Tunnel Details from Zscaler

After selecting “Add Tunnel”, a pop-up should appear, as shown below. You want to configure:

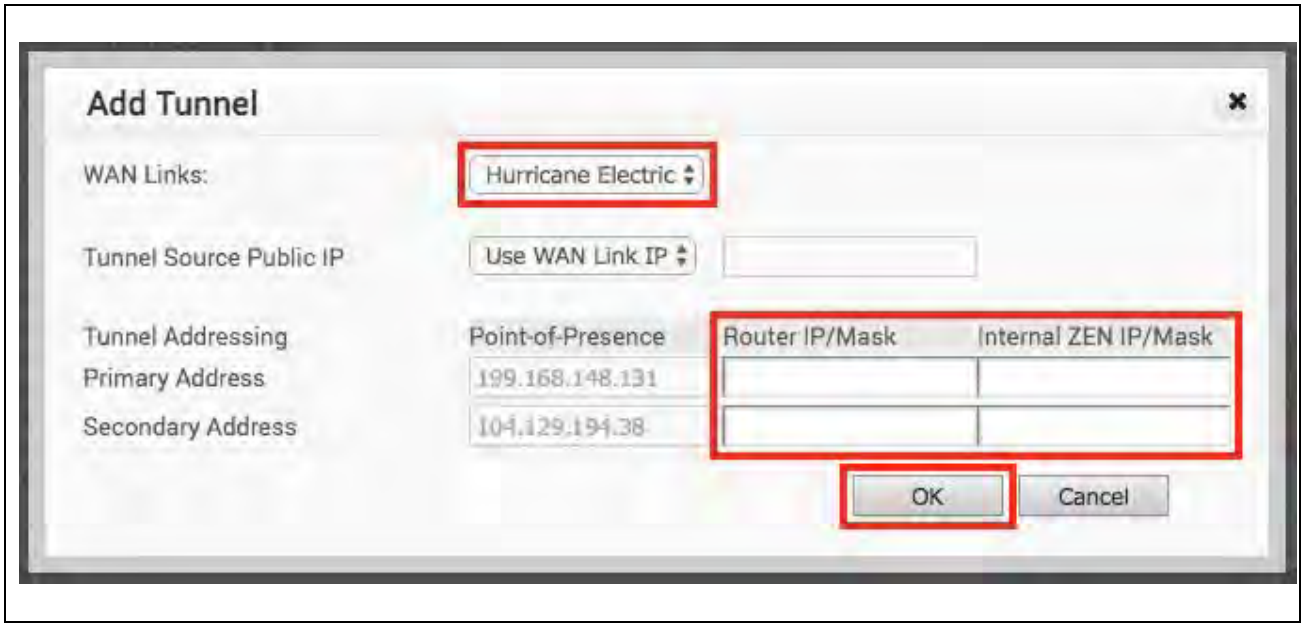

Figure 3.2.4-A: Input GRE Tunnel Details

1) **WAN Link:** Select the WAN interface the GRE tunnel should source from (in our example, our lab WAN link is called “Hurricane Electric”.

2) **Tunnel Addressing:** The Router IP/Mask and Internal ZEN IP/Mask is provided by Zscaler. If you have not already opened a support ticket with Zscaler to have a GRE Tunnel provisioned, please see Appendix XXXX: Configuring Static IP’s and GRE Tunnels

As part of the GRE Tunnel configuration, you will need to assign the Static IP for the Tunnel Source to a Location. See Appendix XXX: Configuring a Location for Manual Tunnels Once you have completed these fields, select “*OK*” to continue.

3.2.5 Verify GRE Tunnel Configuration

Once you return to the **Cloud Security Service** section, you should see the WAN interface name below (e.g., Hurricane Electric, which is the name of the WAN interface for the lab this guide was authored).

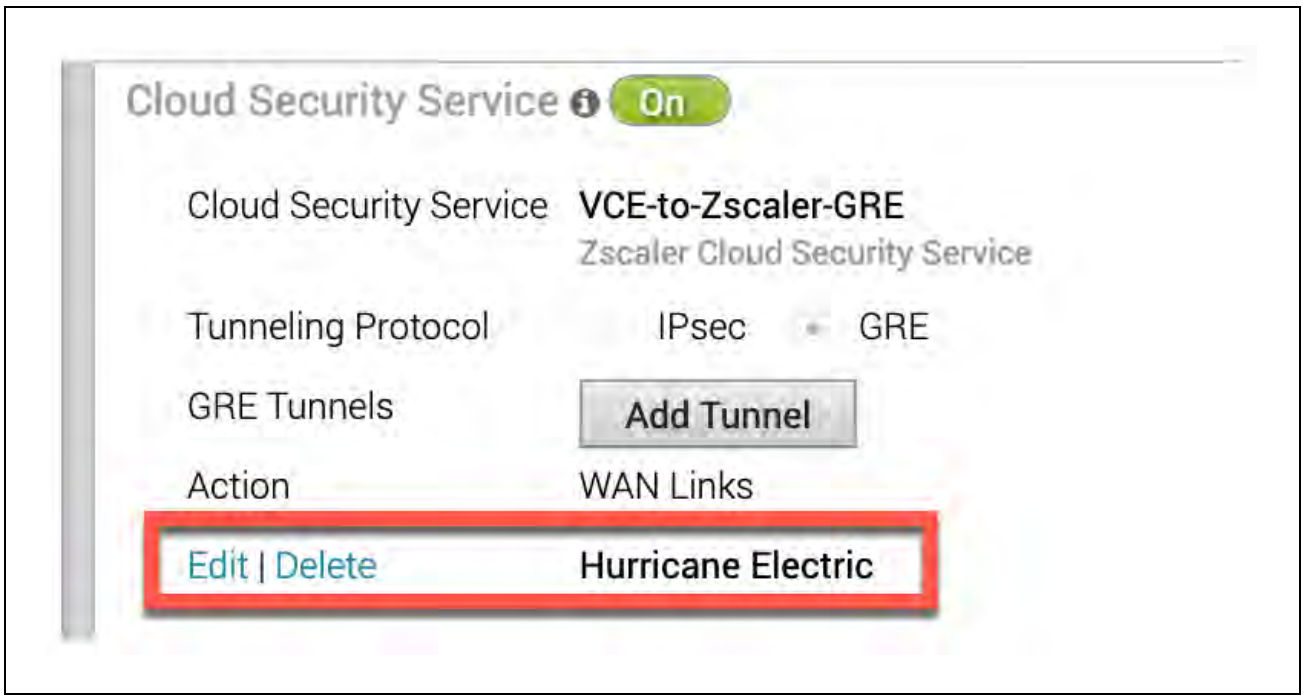

Figure 3.2.5-A: Verify GRE Tunnel Configuration

3.2.6 Verify Tunnels are Up (Active)

To verify the state of the GRE tunnel, navigate to **Monitor → Edges**. You may have to wait 30 seconds, but you should see the primary GRE tunnel establish. The standby tunnel will remain grey until it becomes active, which should only occur if the primary GRE tunnel fails.

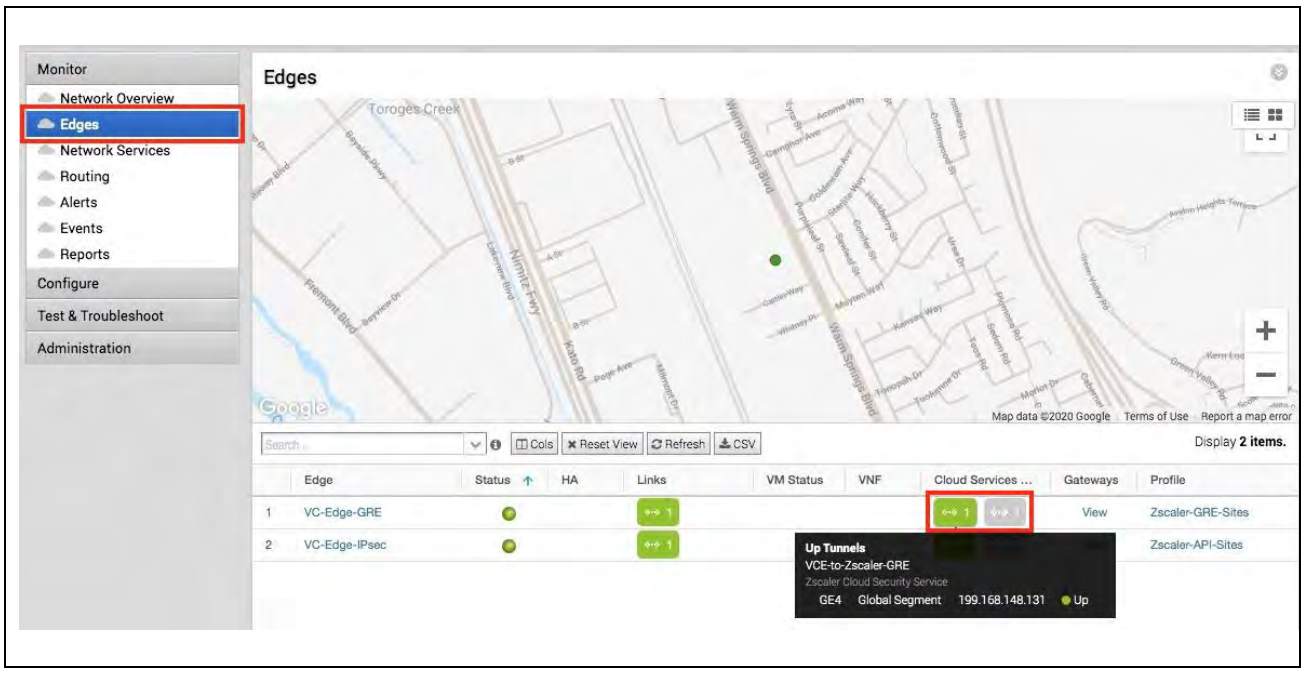

Figure 3.2.6-A: Monitor Edge GRE Tunnel State

3.3 Configuring IPsec Tunnel from VCG

It is recommended that you perform the steps required in ZIA admin before performing the configuration in the VCO:

- Locate the primary and secondary ZIA DC VPN endpoints from config.zscaler.com deriving the IP address from the DNS hostname. If you are not familiar with how to get the IP from a DNS name, please refer to section: *Appendix F: Deriving the Zscaler IPSEC VPN VIP*.
- Create the FQDN and PSK for the IPsec Tunnels, refer to section: *Appendix B: Adding VPN Credentials for manual tunnel creation*.
- Create a Location and assign the VPN Credentials to that location so the traffic will get the proper policy, refer to section: *Appendix C: ZIA - Configuring a Location for Manual Tunnels*.

3.3.1 New Non-SD-WAN Destination

First, we need to create a Non-SD-WAN Destination entry for Zscaler. Navigate to **Configure → Network Services → Non-SD-WAN Destinations via Gateway → New**.

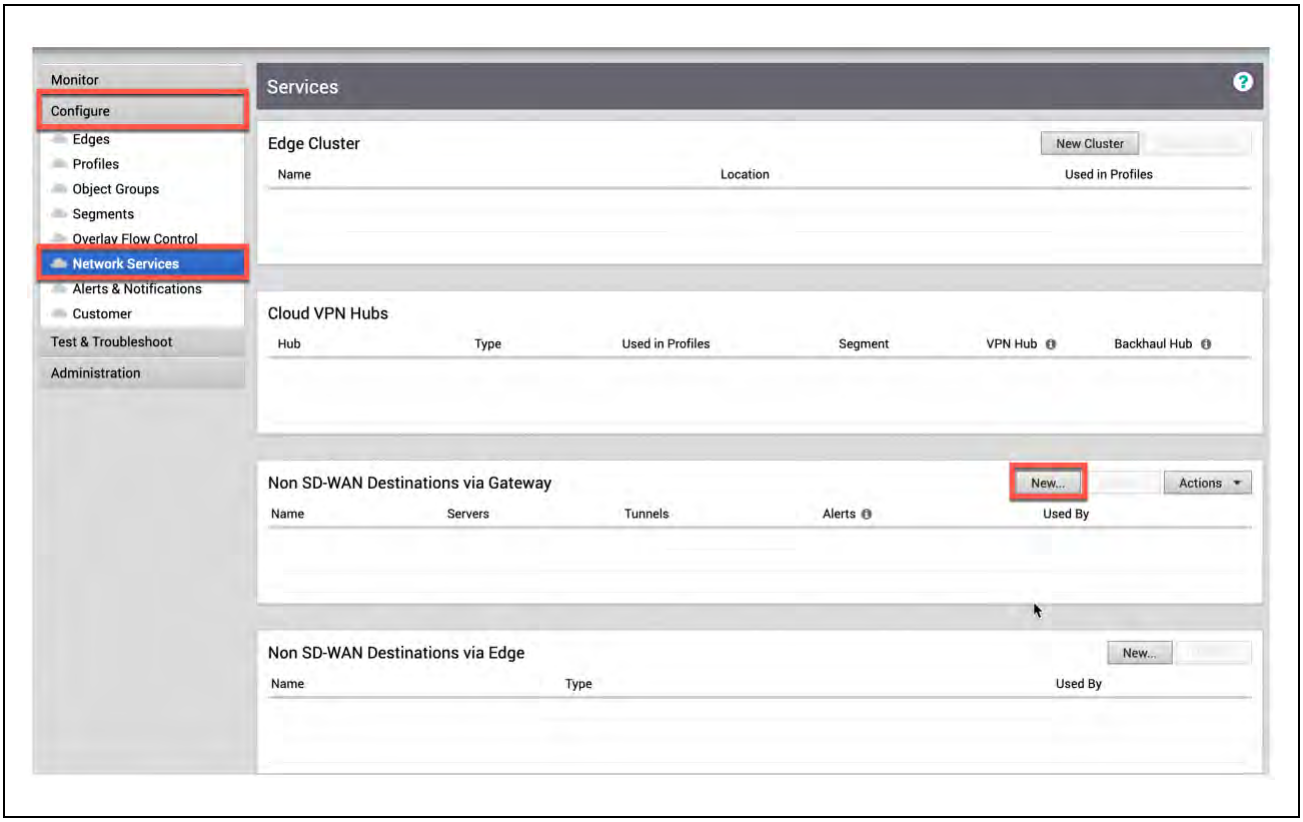

Figure 3.3.1-A: Create New Non-SD-WAN Destination via Gateway

3.3.2 Create Non-SD-WAN Destination Site

After selecting “New”, a pop-up should appear, as shown below. You need to configure:

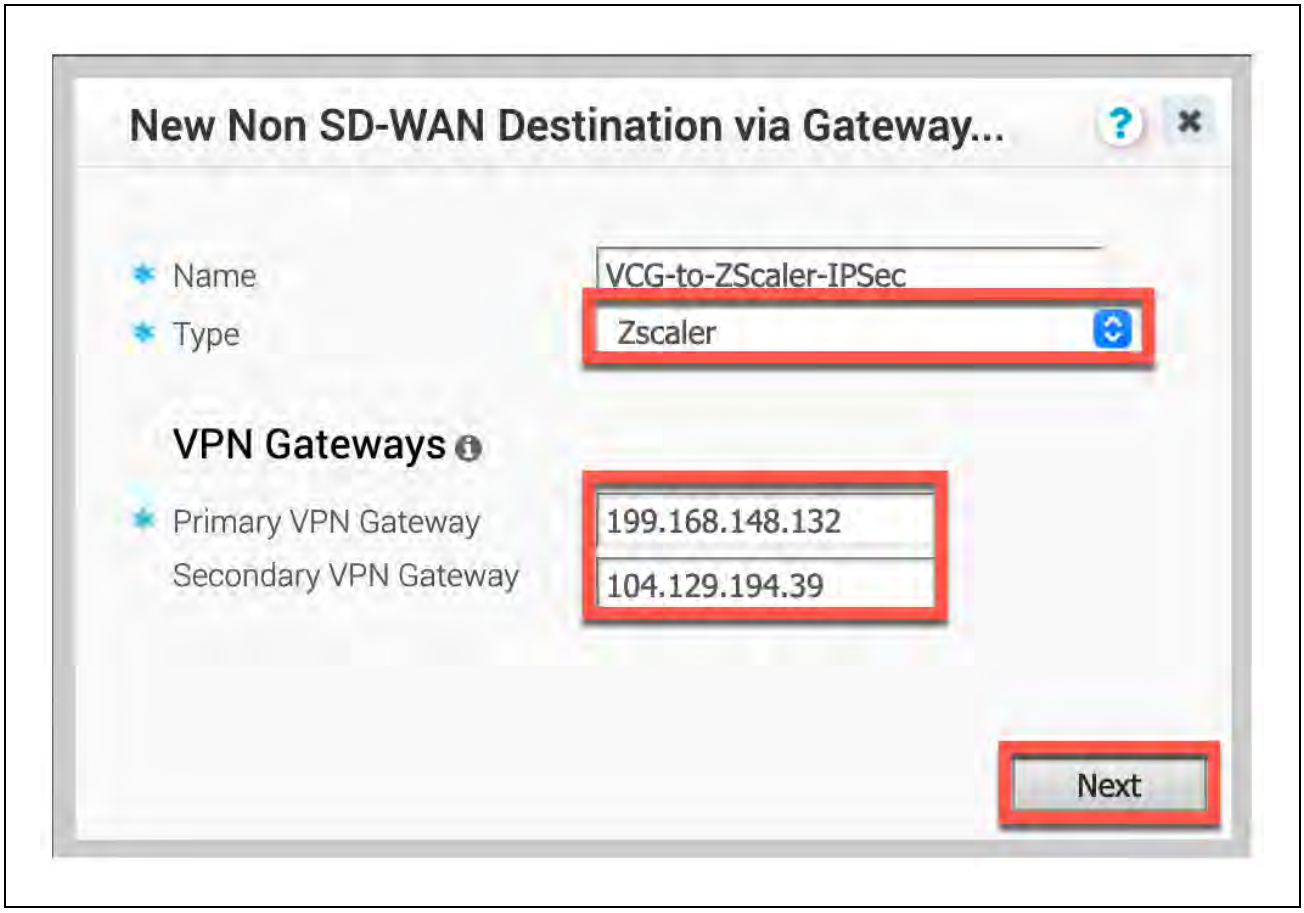

Figure 3.3.2-A: Create New Non-SD-WAN Destination via Gateway

1) **Type:** Select “Zscaler”
2) **Primary and Secondary VPN Gateway:** Obtain the IPsec VIP IP from the Zscaler IP Pages (look at Appendix). You should use the IP Pages for the Zscaler cloud you are provisioned in (e.g., ZS3).

Once you have completed filling in these fields, select “Next” to continue.

3.3.3 Advanced Settings for Non SD-WAN Site

Next select “Advanced” at the lower-left bottom. The window should expand with additional configuration options, as show below in *Figure 28*. You need to configure:

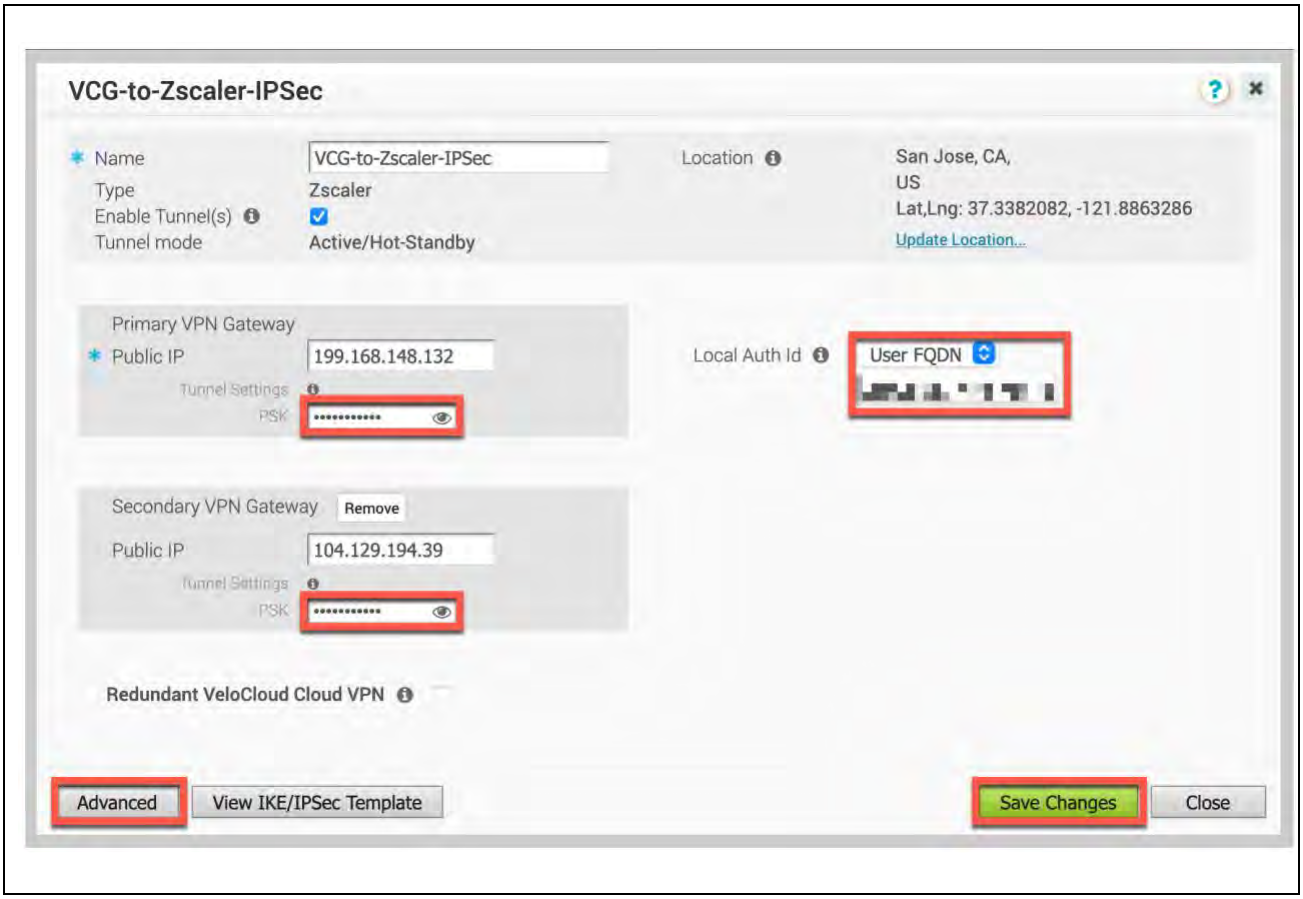

Figure 3.3.3-A: Advanced Settings for Non-SD-WAN Destination via Gateway

1) **Local Auth Id:** User FQDN. Below, paste in your ZIA VPN Credential FQDN.

2) **Primary and Secondary VPN Gateway – PSK**: Paste in your ZIA VPN Credential PSK.

Once you have completed these fields, select “Save Changes” in the lower right.

3.3.4 Enable Cloud VPN

Next you need to navigate to **Configure → Profiles → and select the Profile** you want to enable. Next select "Device" and then scroll down to configure:

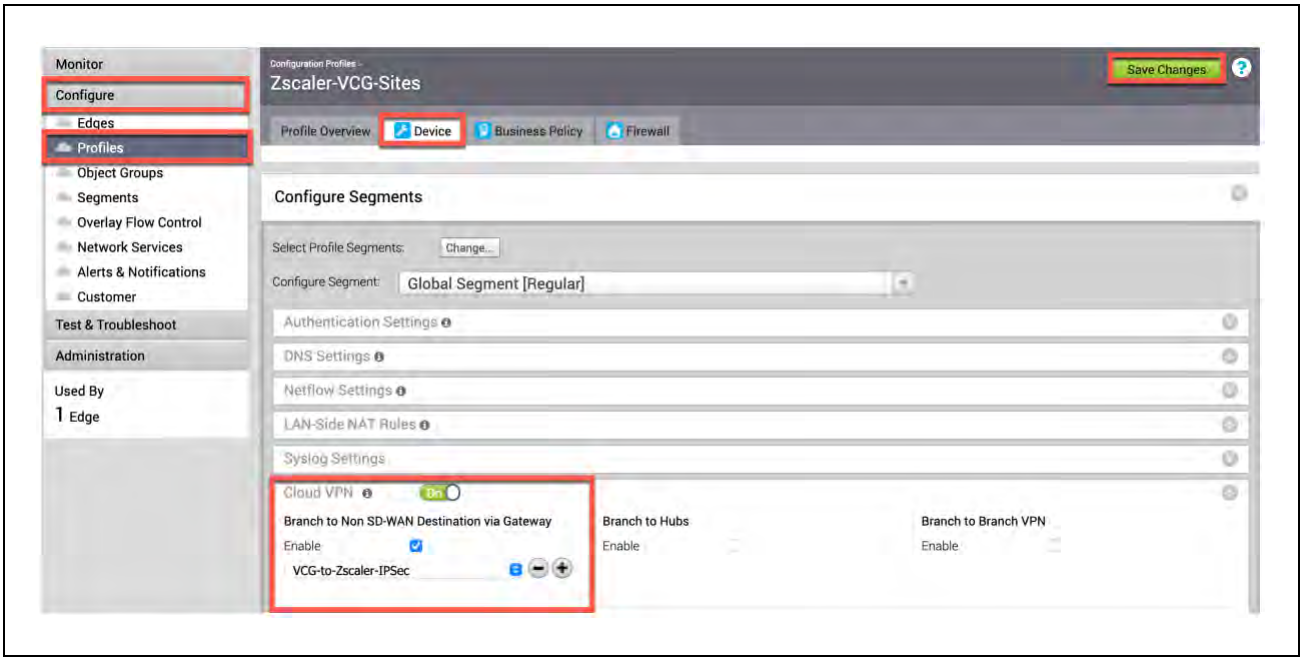

Figure 3.3.4-A: Enabling Zscaler Connectivity from VCG on VMware SD-WAN VCO

1) **Cloud VPN:** Select it "On".

2) **Enable:** Select the Non-SD-WAN Site in the drop down.

3.3.5 Verify Tunnels are Up (Active)

To verify the state of the IPsec tunnel from VCG, navigate to **Monitor → Network Services**. You may have to wait 30 seconds, but you should see the primary and secondary IPsec tunnels establish. The redundant tunnels, if configured will remain grey until they become active, which should only occur if the primary and secondary IPsec tunnels fail.

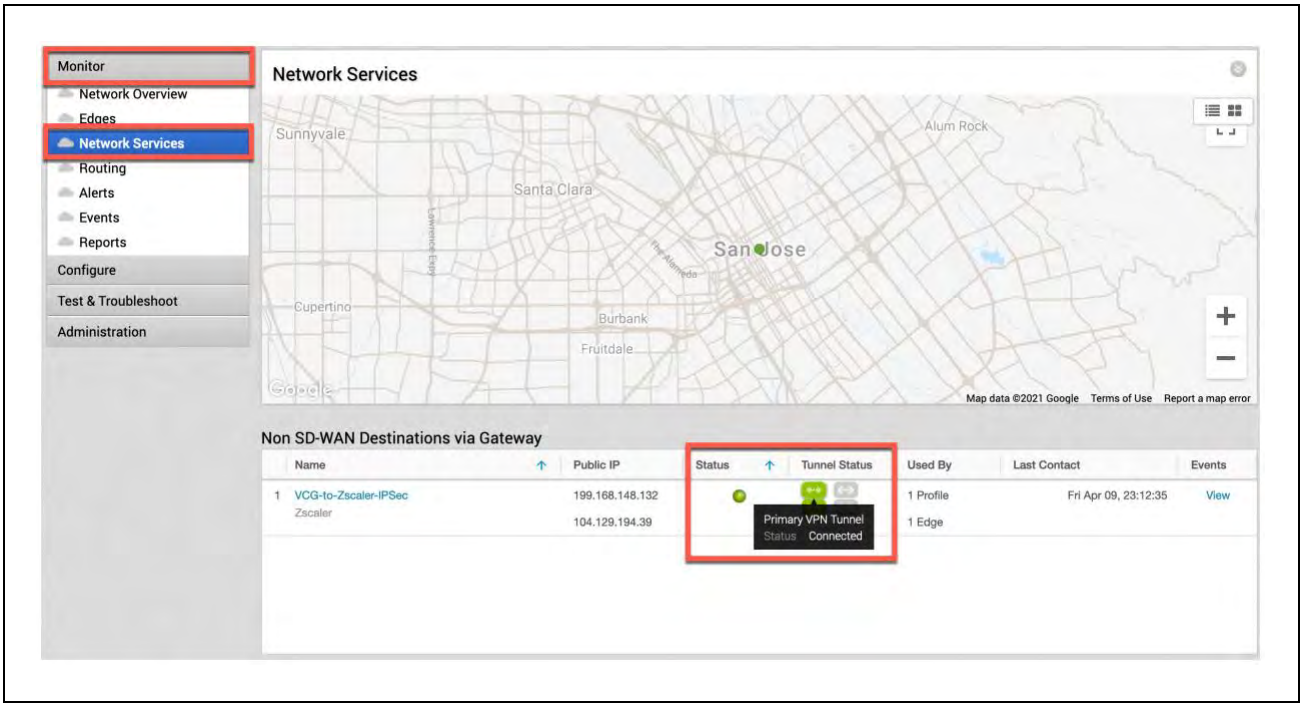

Figure 3.3.5-A: Monitor Network Services Tunnel State from VCG

3.4 Configuring Business Policy for ZIA

In this section we will create a Business Policy to send all Internet destined traffic to Zscaler. Navigate to **Configure** → **Profiles** → and select your **Profile**. Next, select "Business Policy", and then select "New Rule".

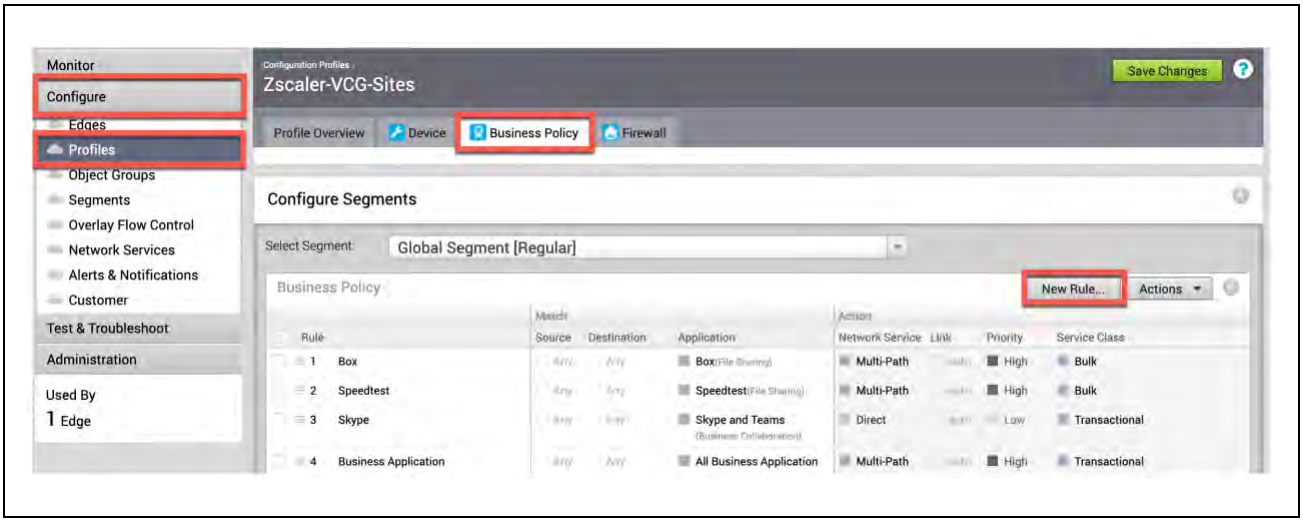

Figure 3.3.5-A: Configuring Business Policy for ZIA

3.4.1 Configure Rule for VCE

After selecting “New”, a pop-up should appear, as shown below. You need to configure:

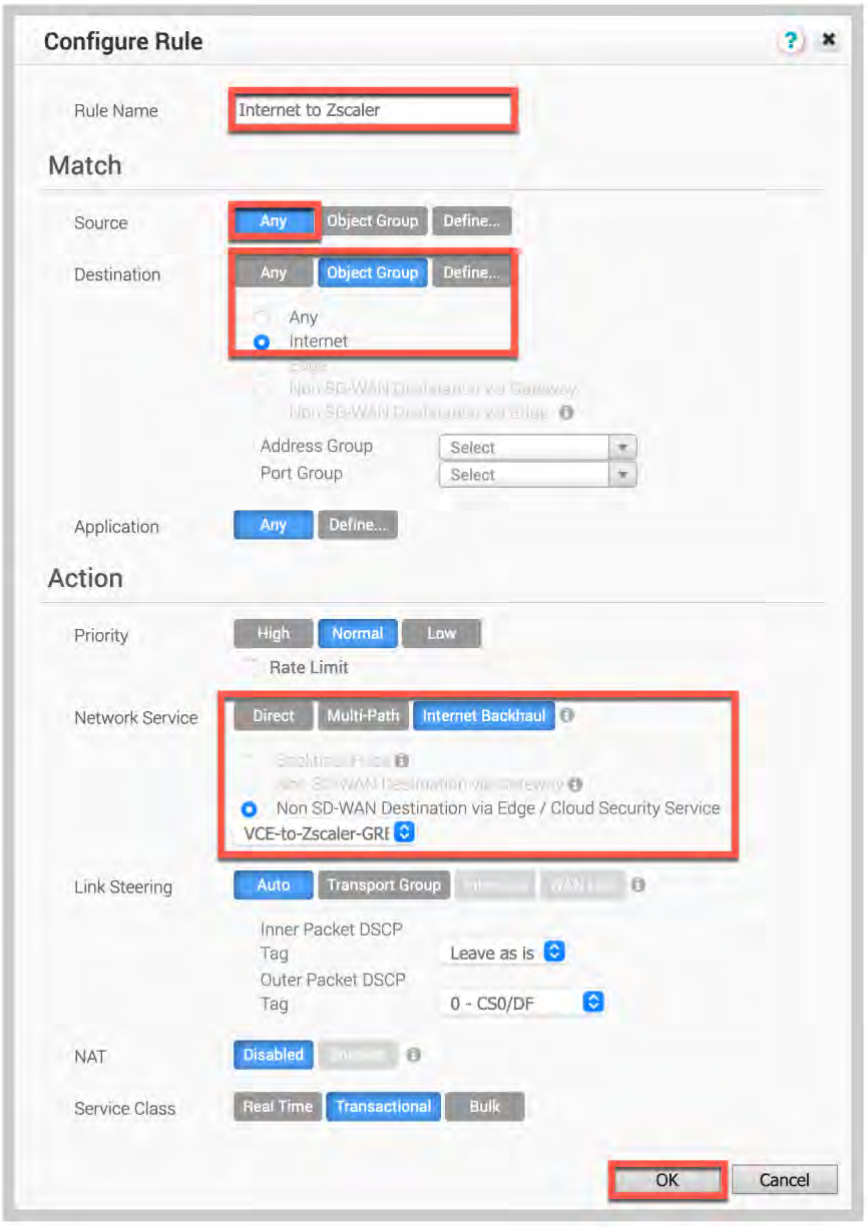

Figure 3.4.1-A: Configure Rule for Edges Using Direct Tunnel from VCE

3.4.2 Configure Rule for VCG

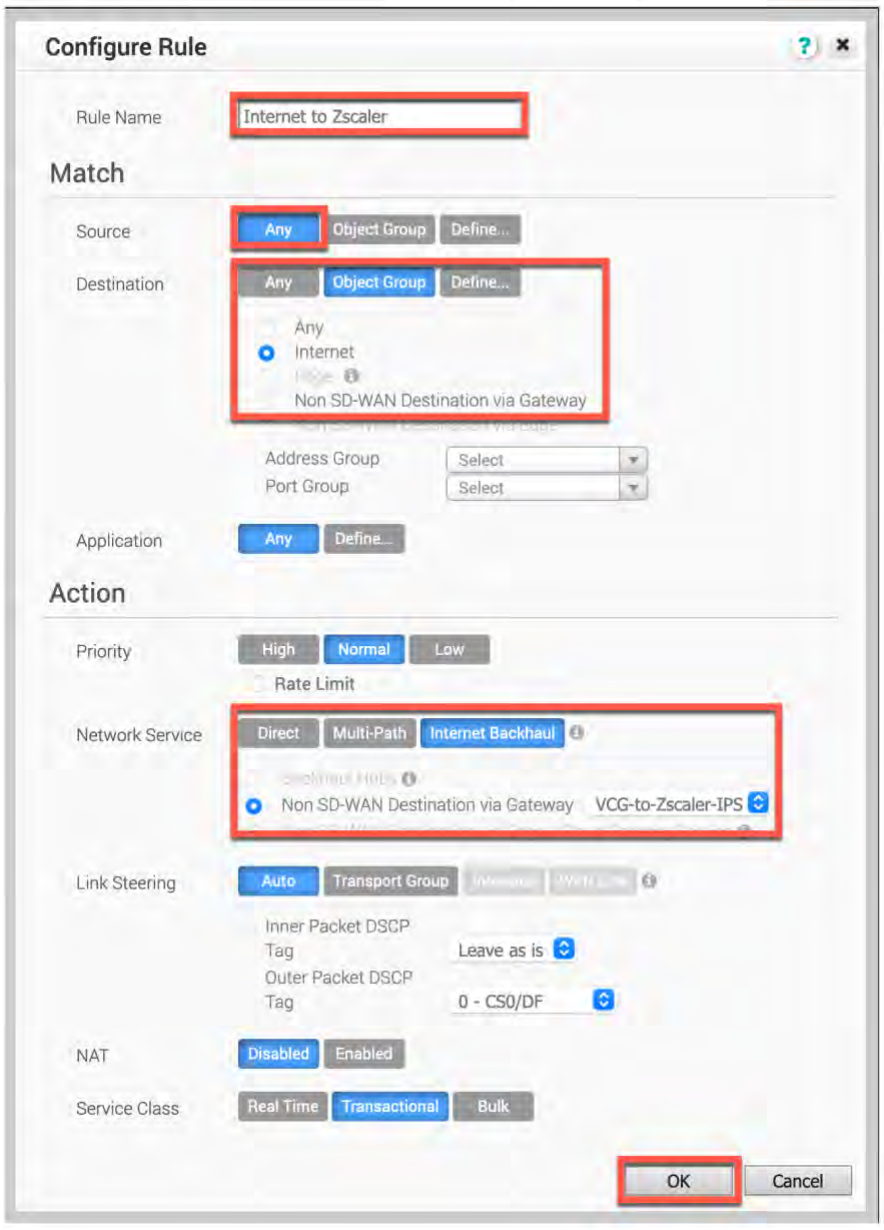

Figure 3.4.2-A: Configure Rule for Edges Using Tunnels from VCG

4 Appendix A: ZIA - Configuring Static IP's and GRE Tunnels

The ZIA Admin UI supports provisioning Static IPs for GRE Tunnels

Navigation: Administration → Resources → Static IPs & GRE Tunnels:

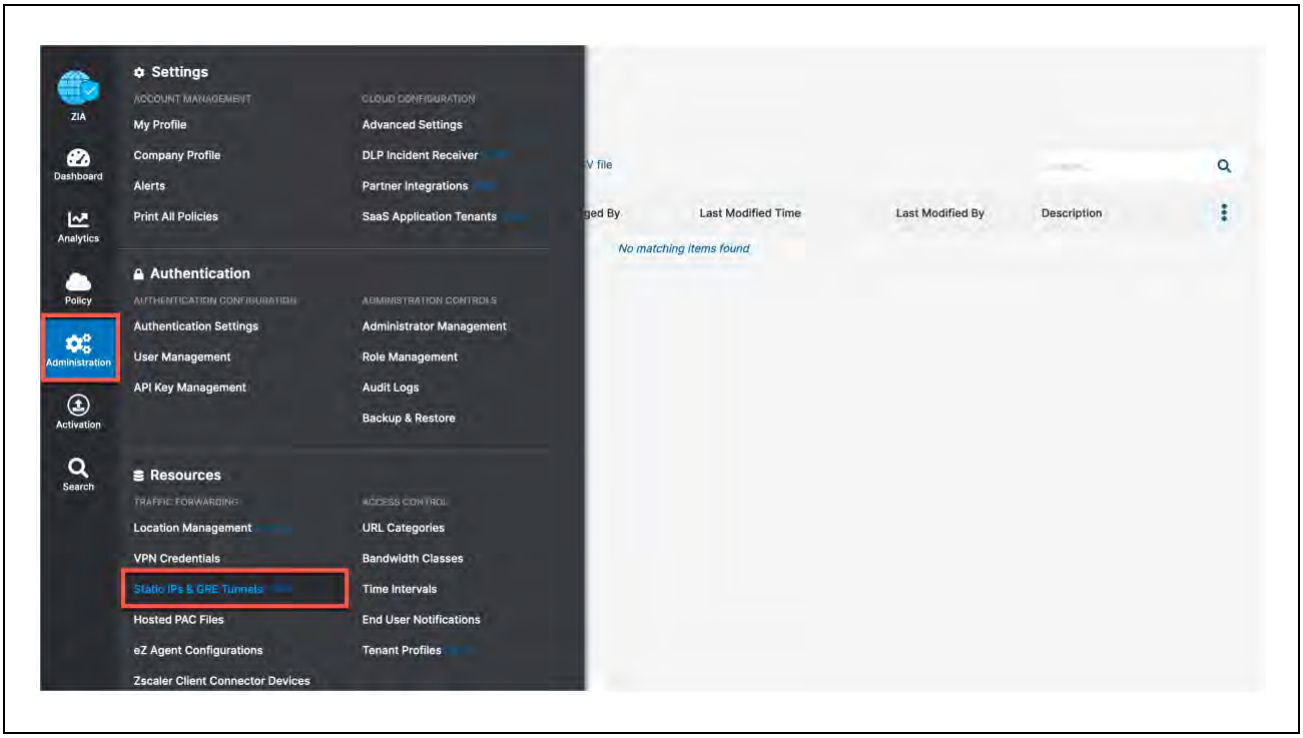

Figure 4-A:Navigate to Static IPs & GRE Tunnel configuration screen

4.1 Add a Static IP Configuration

Click on the “Add Static IP” selection from the page:

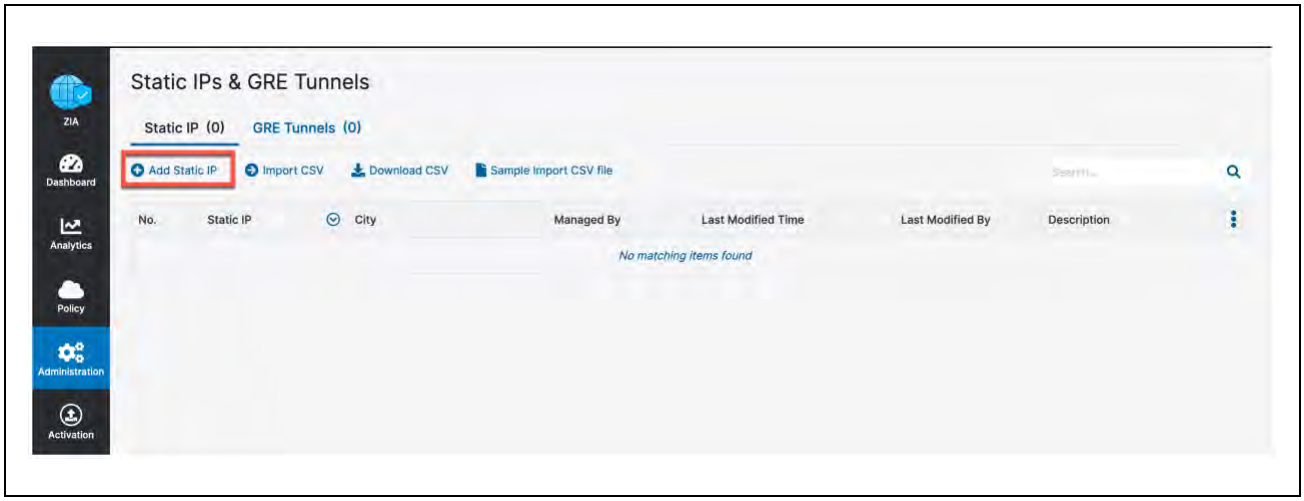

Figure 4.1-A: Adding a Static IP

4.1.1 Enter the Static IP

In the window the appears:

- Enter the public static IP that will initiate the tunnel connection
- Add a Description if desired

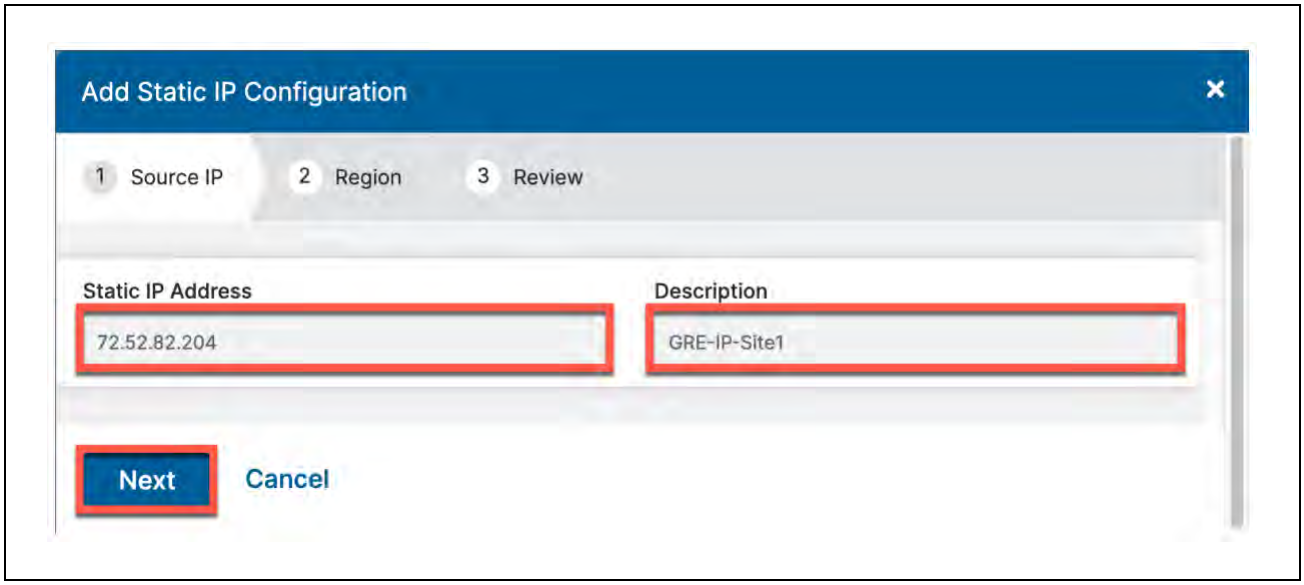

Figure 4.1.1-A: Entering the Static IP

Click "*Next*" to continue.

4.1.2 Verify Geospatial data

Next, verify the Geospatial location lookup is correct for the IP address entered. If not click the "*Manual*" button and enter the correct location. Then click "*Next*":

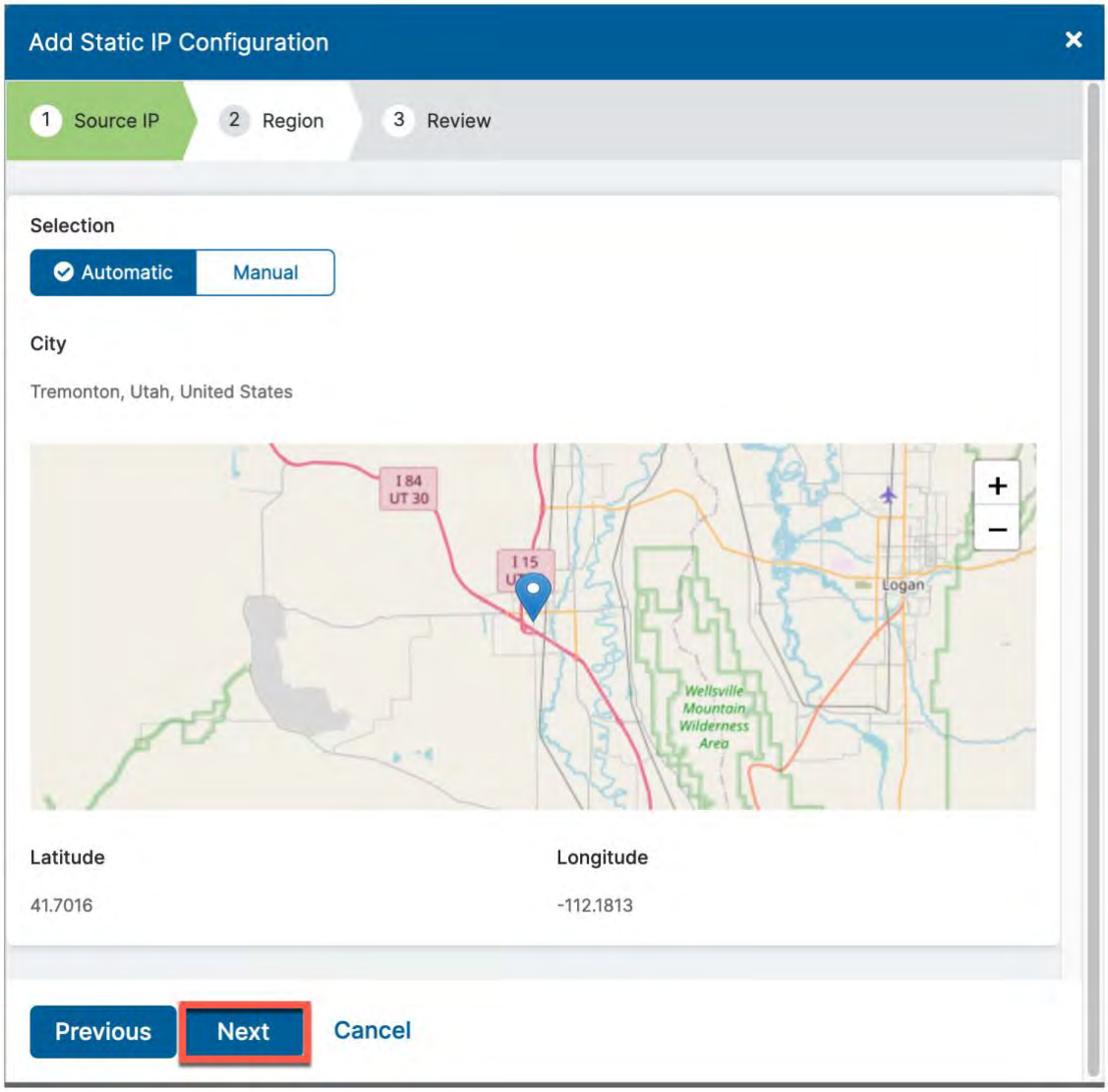

Figure 4.1.2-A: Verifying Geospatial information

This information will be used by the Central Authority to choose the best Data Centers for tunnel termination.

4.1.3 Review Information and Save

Review the information entered for the static IP and click "*Save*".

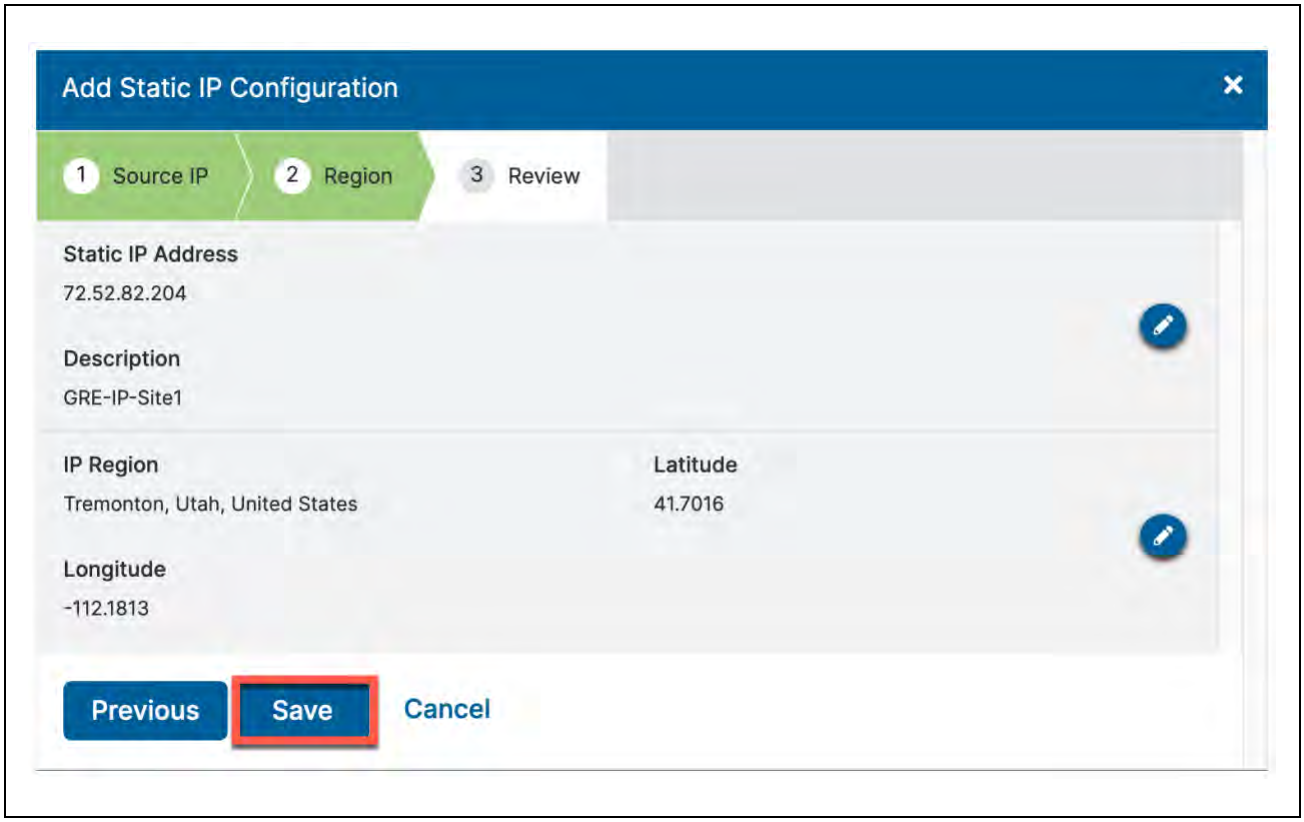

Figure 4.1.3-A:Review and save the Static IP

4.1.4 Validate Static IP Configuration is Saved

After completing the Static IP provisioning wizard and clicking save, you should see a message appear “All changes have been saved.” And the Static IP added to the list.

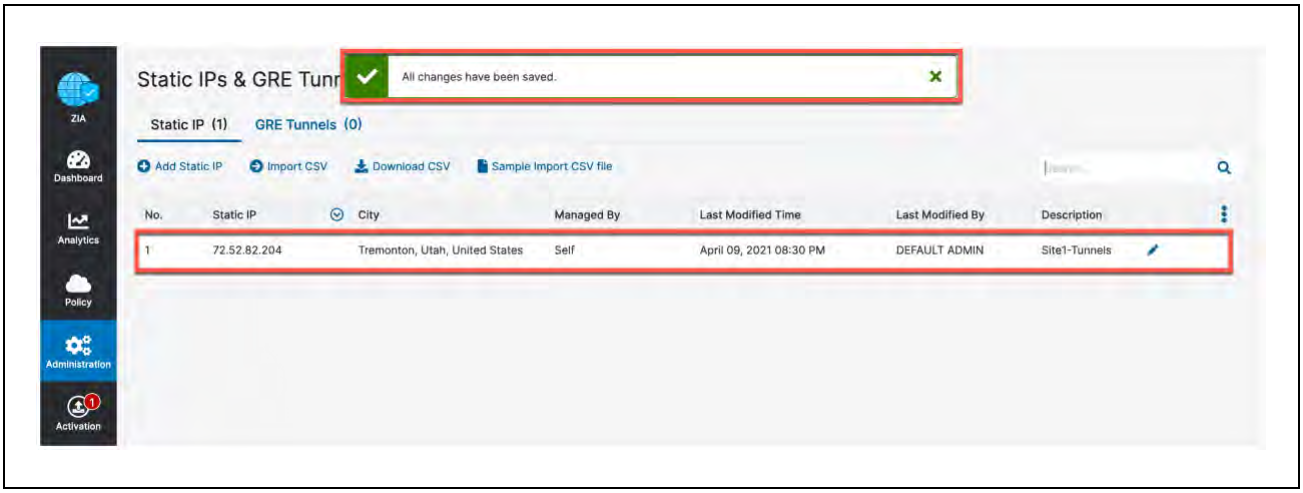

Figure 4.1.4-A:Validate the Static IP was saved

Next go onto step *4.2* to assign the IP to a GRE tunnel.

4.2 Add a GRE Tunnel Configuration

With the Static IP that has been added from section *4.1* we need to configure the GRE Tunnel information, click on "*GRE Tunnels*" and then on "*Add GRE Tunnel*" from the screen:

Figure 4.2-A: Navigate to the GRE Tunnel Configuration screen

4.2.1 Assign the Source IP to the Tunnel

In the window that appears, choose the static IP address that will be the source of GRE tunnel and enter a Description if desired:

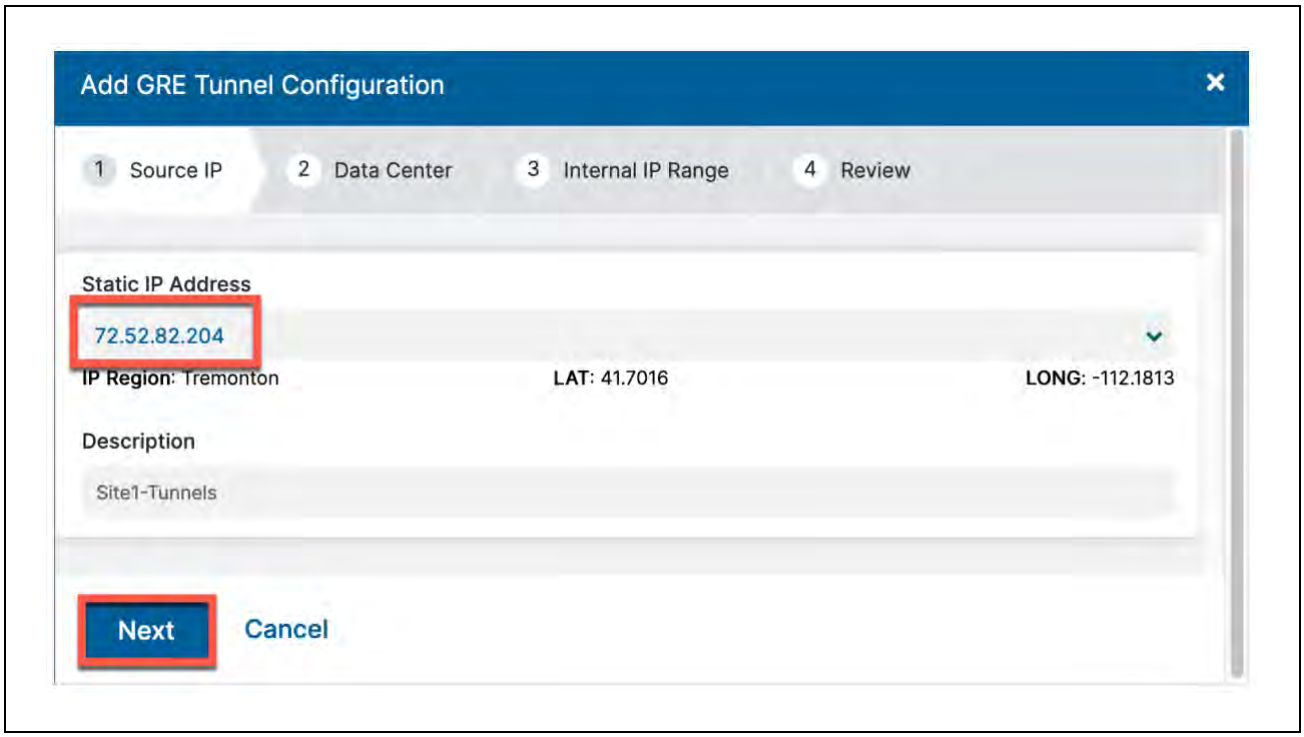

Figure 4.2.1-A:Choose the GRE tunnel source IP

Then click "*Next*".

4.2.2 Choose Data Centers for Tunnel Termination

Now, assuming the Geospatial information from adding the Static IP was correct the closest Data Center VIP and Next Closet Data Center VIP will be chosen. If you want to change these to different VIP's or DC's, choose them from the Dropdown.

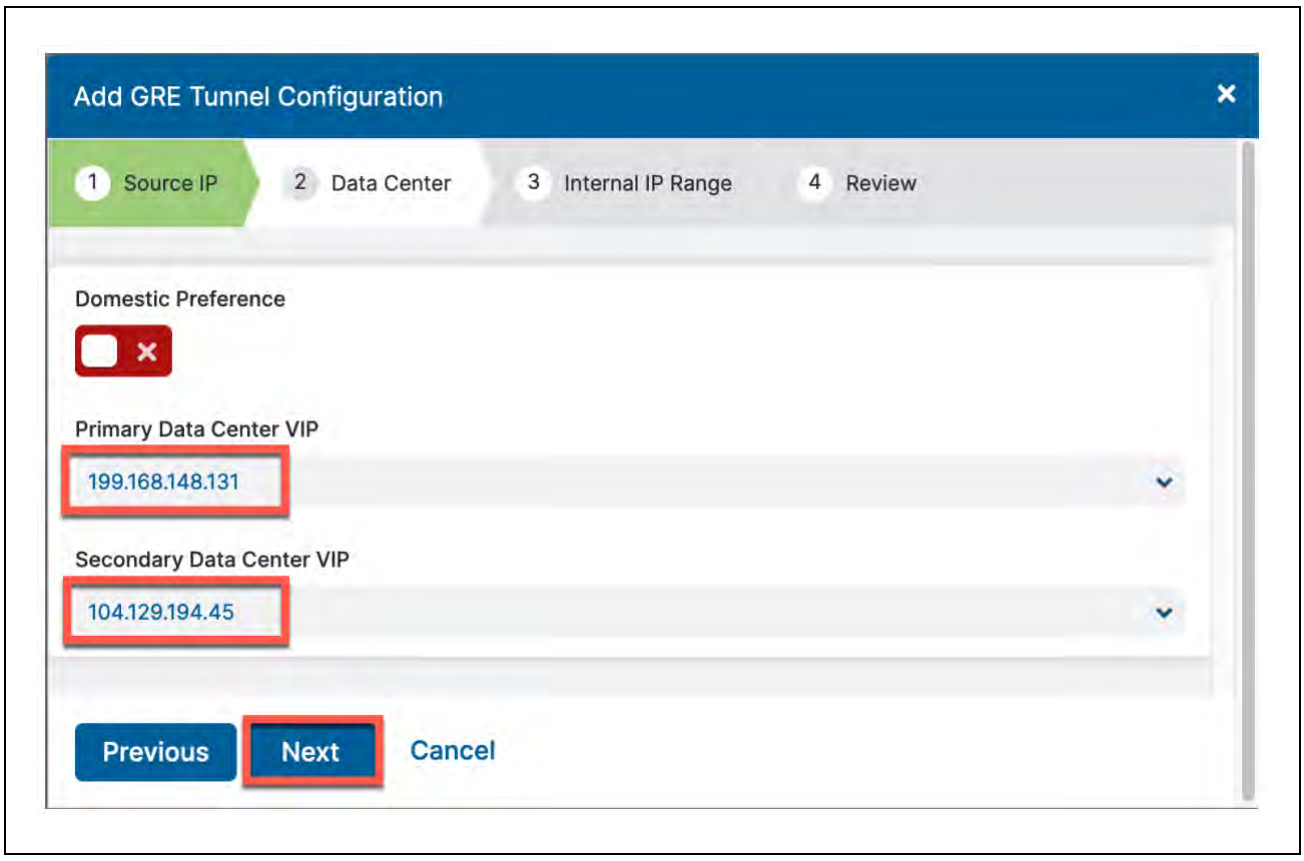

Figure 4.2.2-A:Choose the Data Centers for tunnel termination

Then click "*Next*".

4.2.3 Select GRE Tunnel Internal IP Subnet

Choose an IP subnet (/29) that will be assigned as the Source and Destination for the GRE Tunnel. This is a locally specific range and there is no fear of choosing a subnet that is already in use.

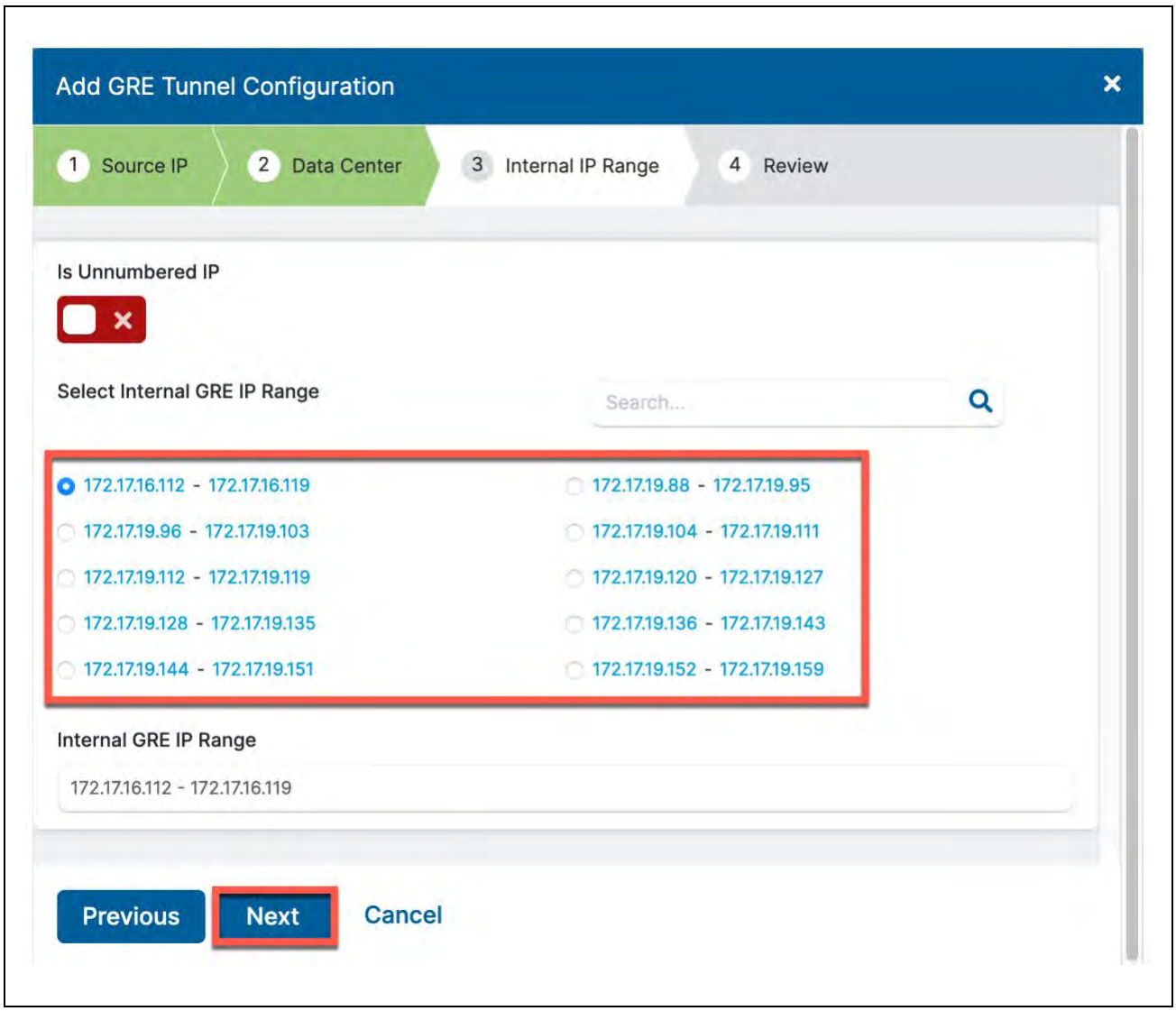

Figure 4.2.3-A: Select the Internal GRE IP Range

Click "*Next*" to review and save.

4.2.4 Save Tunnel Configuration

Review the configuration and click "*Save*"

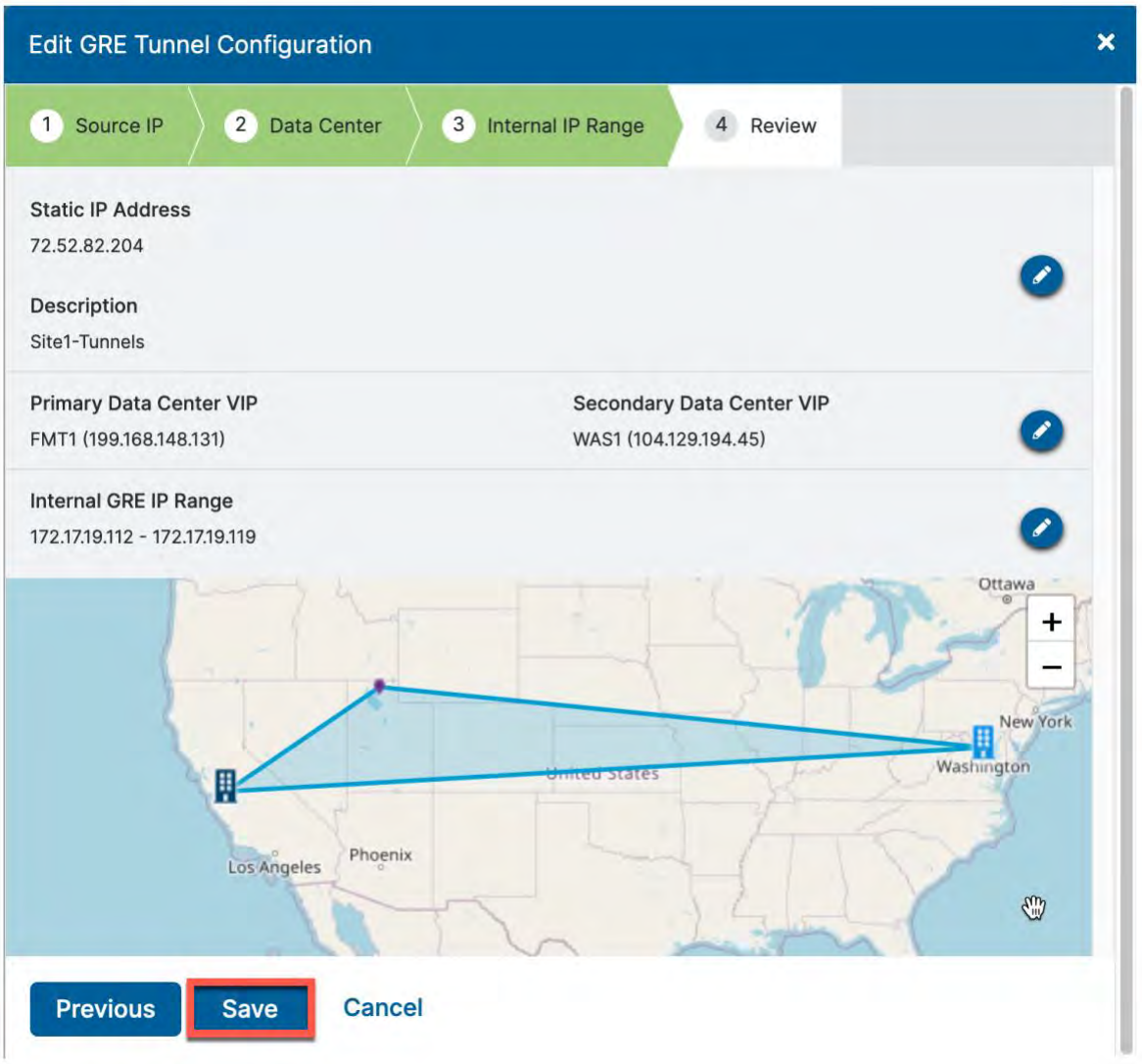

Figure 4.2.4-A:Review and save the tunnel setup

Take note of the "Internal GRE IP Range" that was chosen.
You will need to enter the IPs from it into the VCO GRE Tunnel configuration in Step *3.2.4*.

4.3 Activate all Configuration Changes

Finally, we need to activate the saved configuration changes:

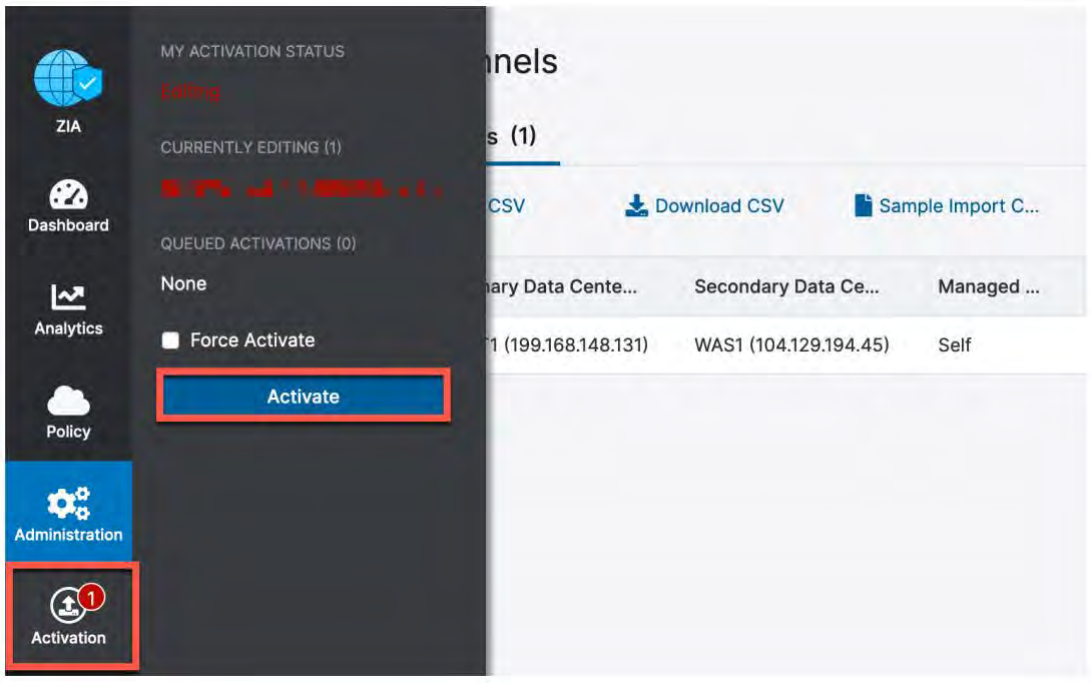

Figure 4.3-A:Activate the GRE Tunnel configuration

Login ID obfuscated for security

You can now navigate to "*Activation*" and activate the pending configurations, as shown above.

The “Activation Completed!” pop-up will appear to indicate your changes are now live.

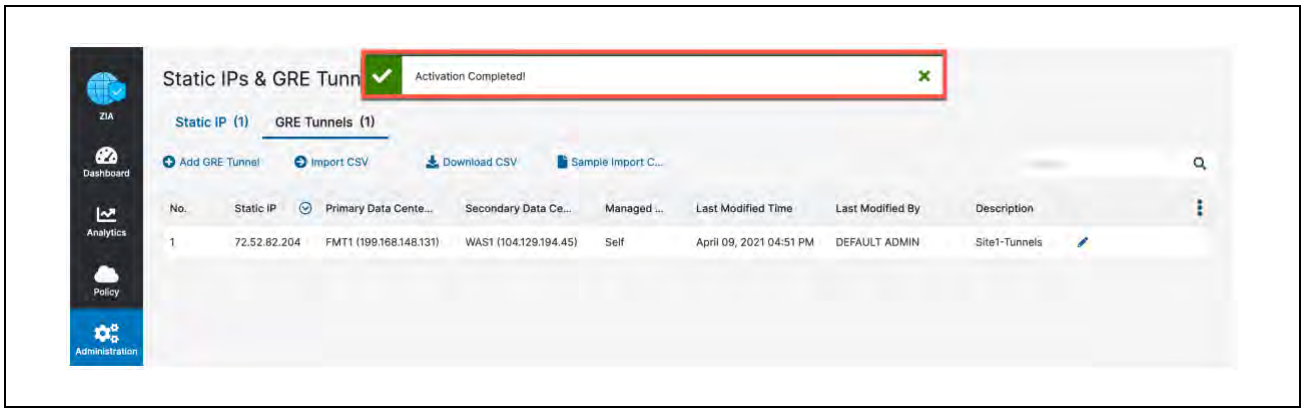

Figure 4.3-B: Verify the GRE Tunnel configuration was Activated

5 Appendix B: Adding VPN Credentials for manual tunnel creation

5.1 Navigate to VPN Credentials

The first step in configuring an IPsec tunnel is to create a VPN Credential in ZIA. In the VPN Credential section, we will create a FQDN and Pre-Shared Key (PSK) for our IPsec session.

Navigation: Administration → **Resources** → and then click **VPN Credentials**.

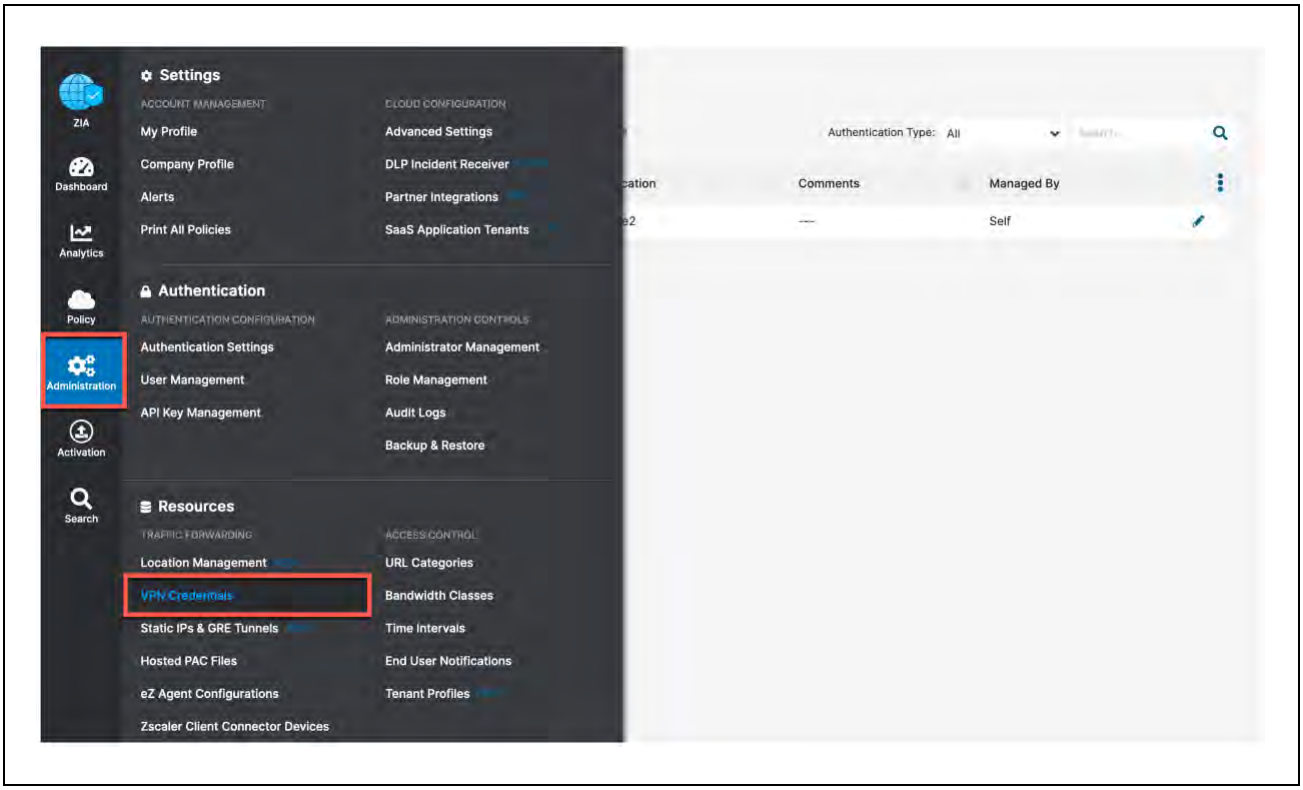

Figure 5.1-A: Navigate to VPN Credentials

5.2 Add a VPN Credential

In Figure 57, if you see "*No Matching Items Found*", your ZIA instance does not have any VPN credentials configured. To add a VPN Credential, click **Add VPN Credential** that is identified in the red box in the upper left.

Figure 5.2-A: Adding a VPN Credential

5.3 Enter VPN Credential Data

In Figure 58, configure the FQDN and Pre-Shared Key (PSK) for IKE. For the FQDN, you only need to configure the username portion of the FQDN as the domain name is automatically added to the right. Once both the FQDN and PSK are configured, click **Save** to continue.

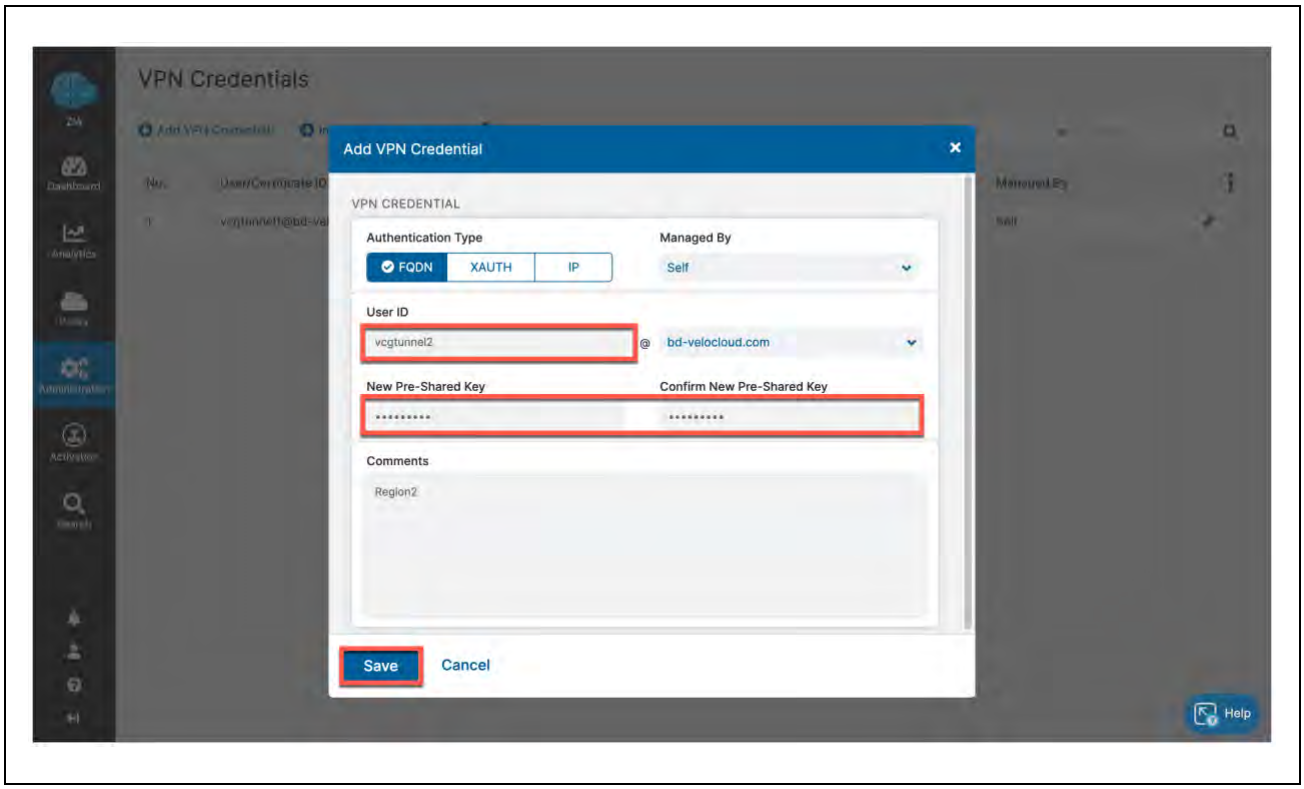

Figure 5.3-A: Enter VPN Credential Data

5.4 Verify VPN Credential

In Figure 59, after saving the VPN Credential, you see “All changes have been saved” in the top center of your screen. If you look below this, you should see the VPN Credential you created.

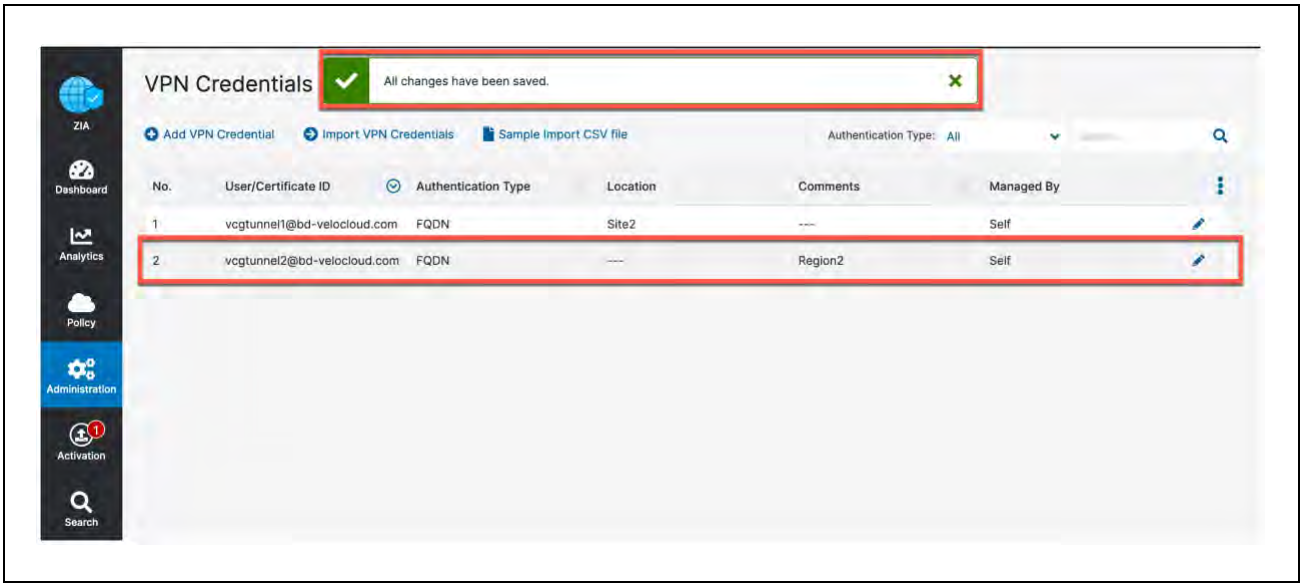

Figure 5.4-A: Verify Location Information and Save

5.5 Activate Pending Changes

Now we need to save the changes. You can now navigate to "*Activation*" and activate the pending configurations, as shown in *Figure* 5.5-A.

Figure 5.5-A: Activate Pending Changes

Login ID obfuscated for security

5.6 Verify Activation

After activating pending changes, you should be returned to the prior page, and "*Activation Complete*" should appear in the top of the window, as shown in Figure 5.6-A.

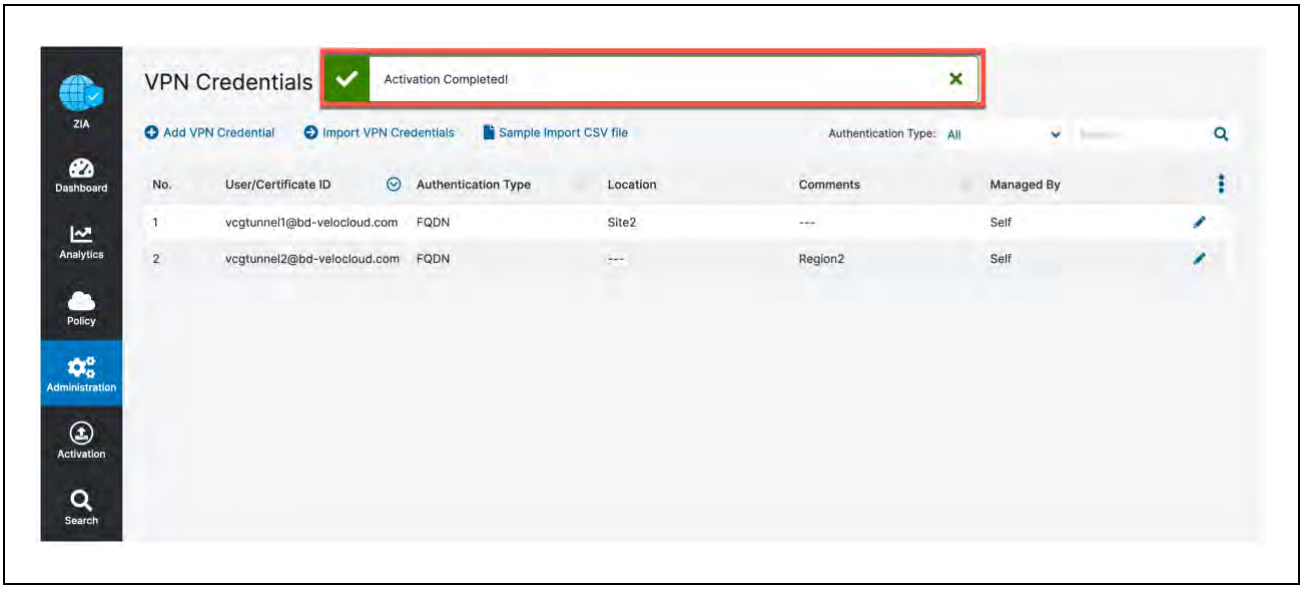

Figure 5.6-A: Verify Activation

6 Appendix C: ZIA - Configuring a Location for Manual Tunnels

Add a location if one is not present for the tunnel to access ZIA. If you are uncertain if you already have a site configured, these steps will verify if a location is present.

Navigation: Administration → Resources -> and then click **Location Management**.

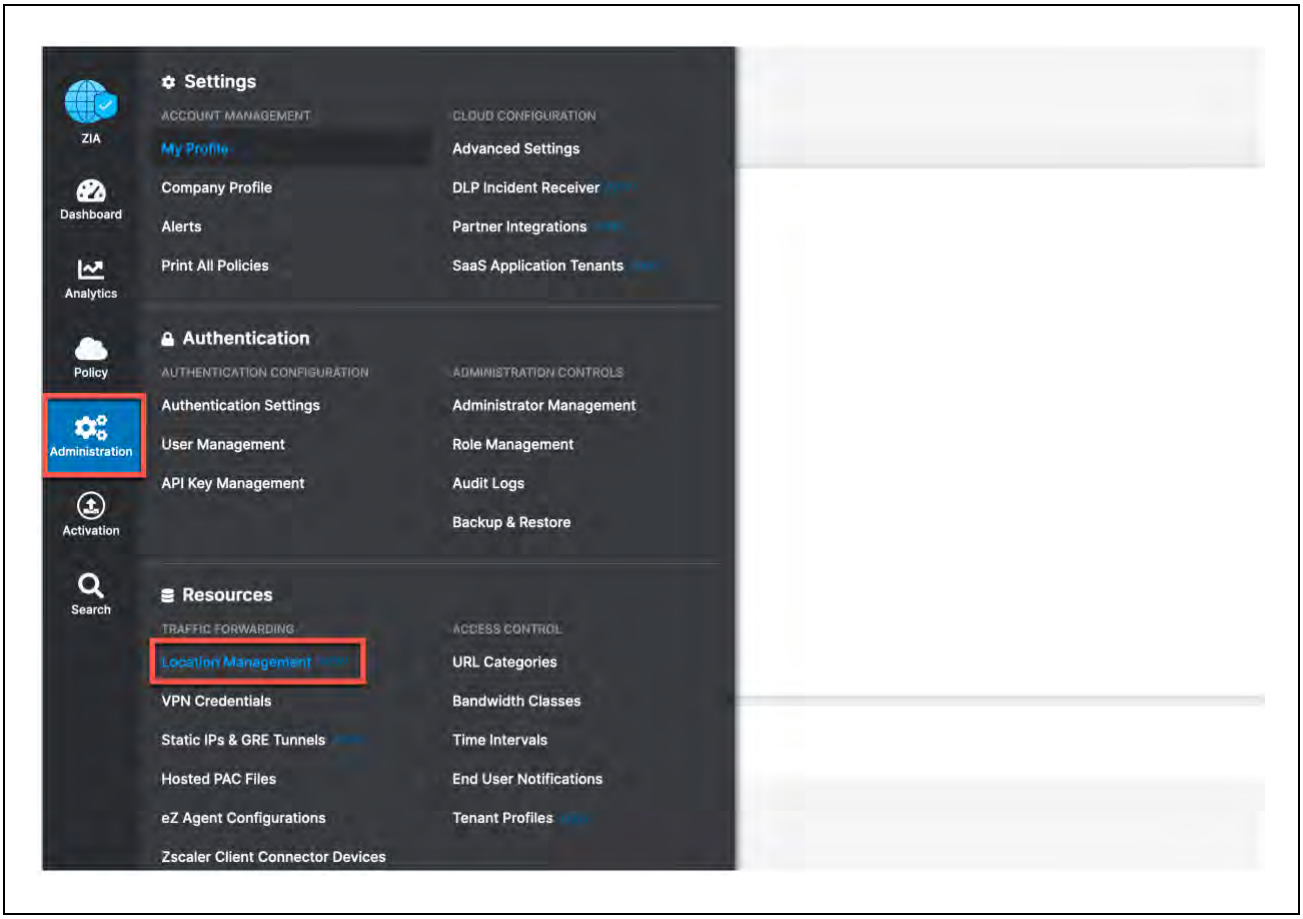

Figure 6-A: Navigate to Locations

6.1 Add a Location

In *Figure* 6-A, if you see "*No Matching Items Found*", your ZIA instance does not have any locations configured. To add a location, click Add Location that is identified in the red box in the upper left. You can also edit any existing locations by clicking the Edit symbol to the far right of the listed location

Figure 6-A: Add a Location

6.2 Enter Location Data

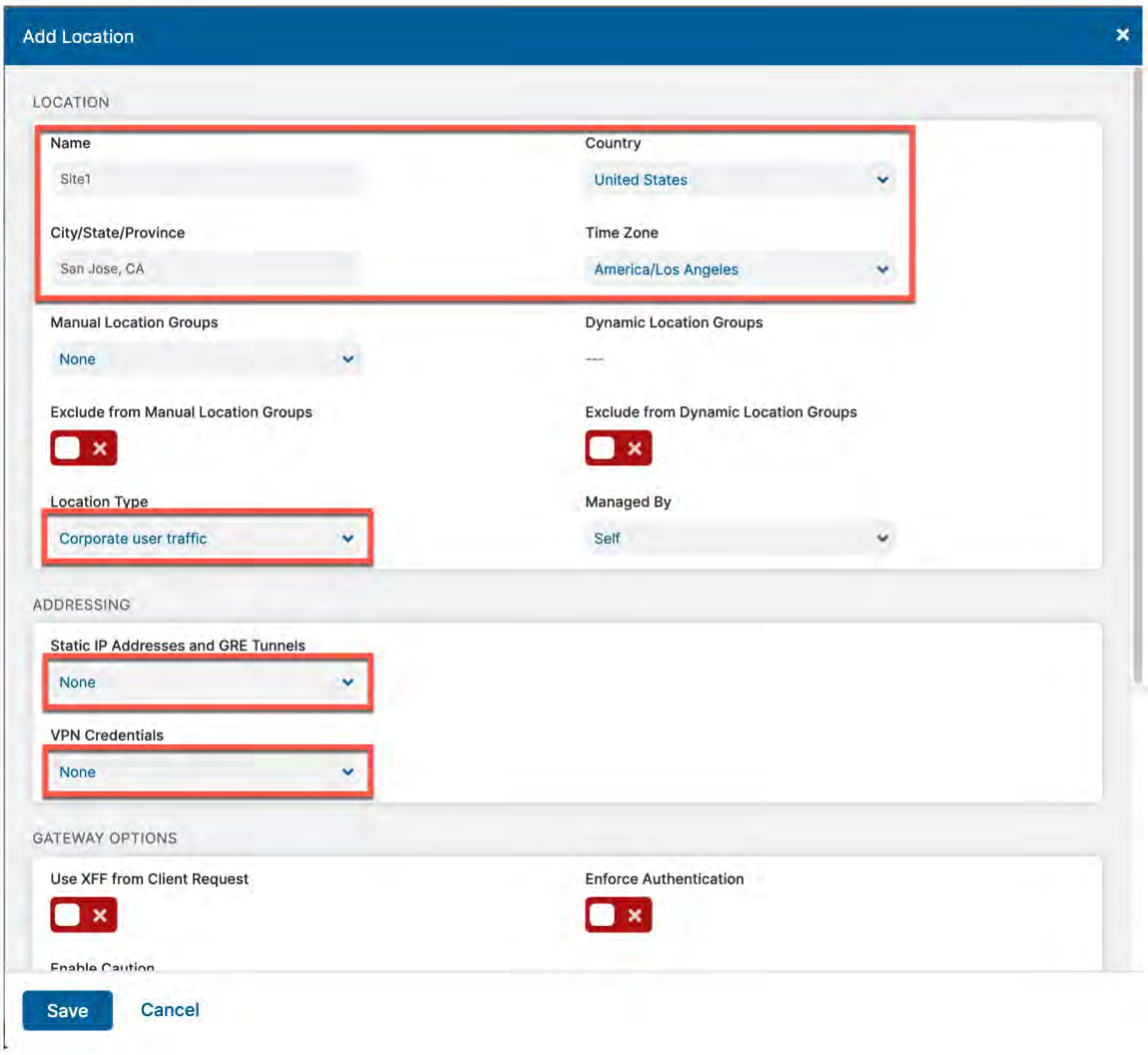

Figure 6.2-A: Enter Location Data

In *Figure* 6.2-A, fill in the fields within the red boxes. The name of the location is used as a policy object within ZIA. The **Managed By** field you can leave alone as "Self" is used for administration through the web interface. You need to choose a **Location Type** for the location as well. Choose the appropriate Location Group, typically it is "*Corporate user traffic*". See here for more information: https://help.zscaler.com/zia/about-location-groups

You must enter either **Static IP Address(es)** or **VPN Credentials** to ensure the traffic incoming from the tunnels is mapped to the proper tenant policy. Add either the Static IP address for GRE tunnels or VPN Credentials if a manually created IPsec tunnel based on your needs as shown in the next two steps.

6.2.1 Add Static IP Location

In *Figure* 6.2.1-A, you will see the Static IP you configured in section *4.1* and linked to a GRE tunnel in section *4.2*. Choose it and click "**Done**". This will then link the Static IP and Traffic arriving on the GRE tunnel assigned to it to this Location. When finished click the "**Save"** button to continue.

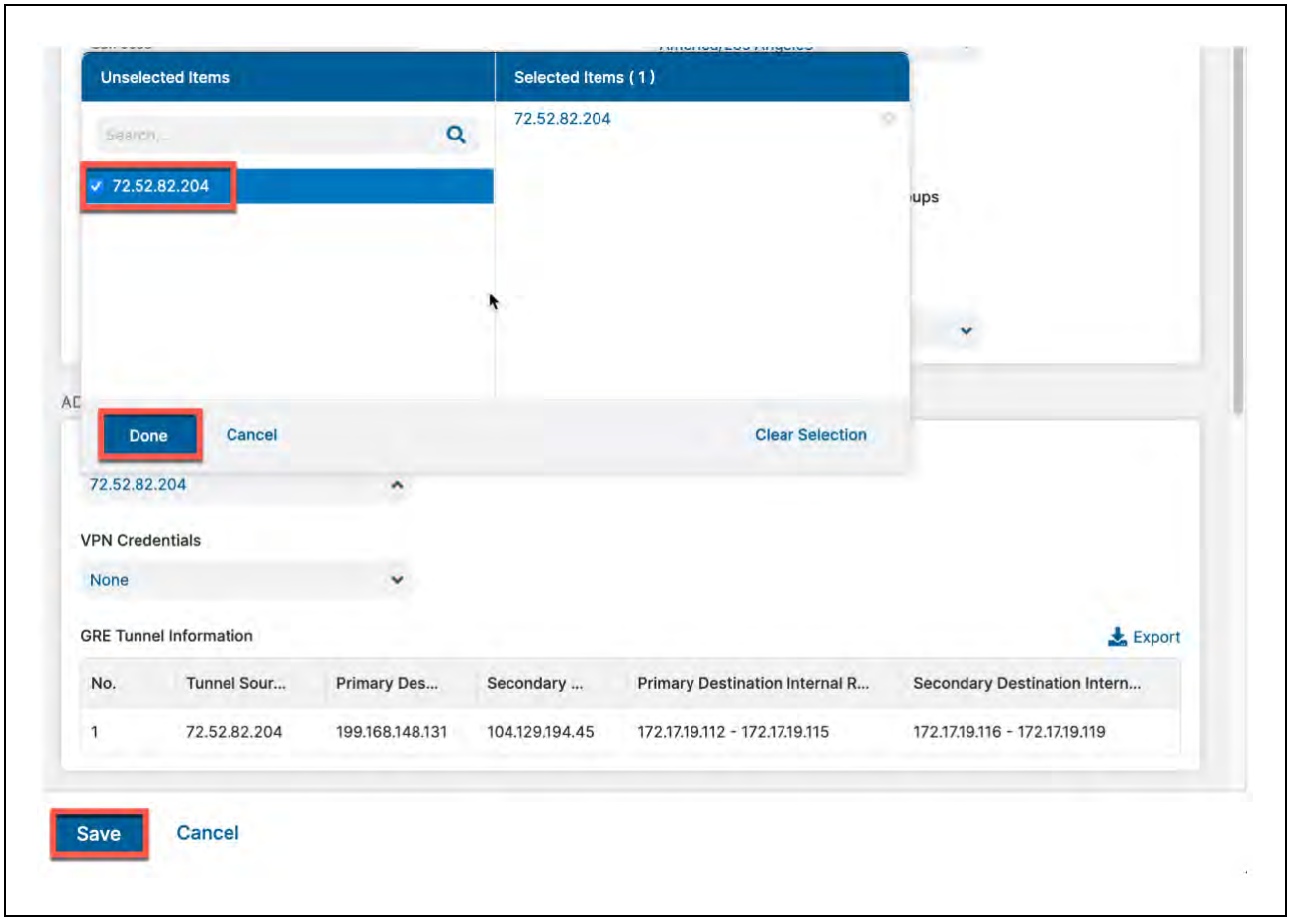

Figure 6.2.1-A: Select the Static IP that will be linked to the Location

6.2.2 Adding a VPN Credential to a Location

In *Figure* 6.2.2-A, you should see the VPN Credential you configured in the section *5*. Select it and click "**Done**". from there, once you save the Location itself, this will couple the VPN Credential to this Location. When you have competed the fields, select "**Save**" to continue.

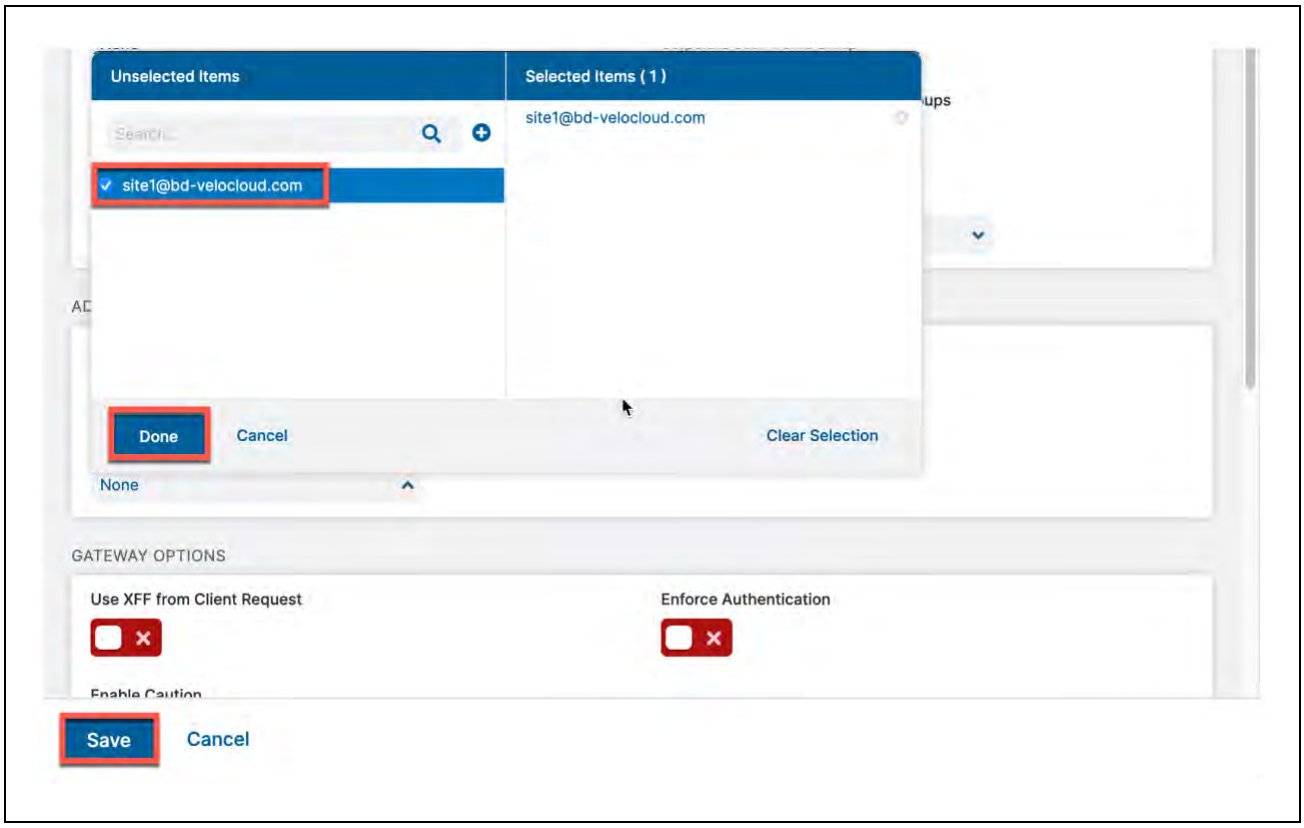

Figure 6.2.2-A: Add VPN Credential to Location and Save

6.3 Confirm Changes Have Been Saved

In *Figure* 6.3-A, after saving the Location, you see “All changes have been saved” in the top center of your screen. If you look below this, you should see the Location you created.

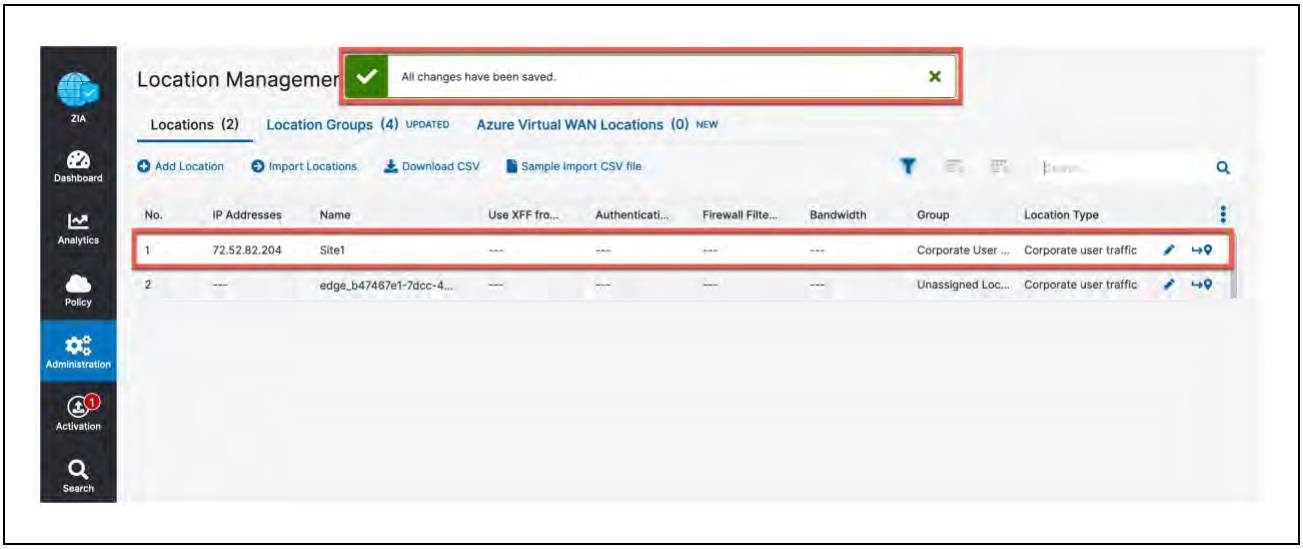

Figure 6.3-A: Confirm Changes Have Been Saved

6.4 Activate Pending Changes

Anytime you make a change in ZIA, you will see a number over the **Activation** image on the left-hand side menu.

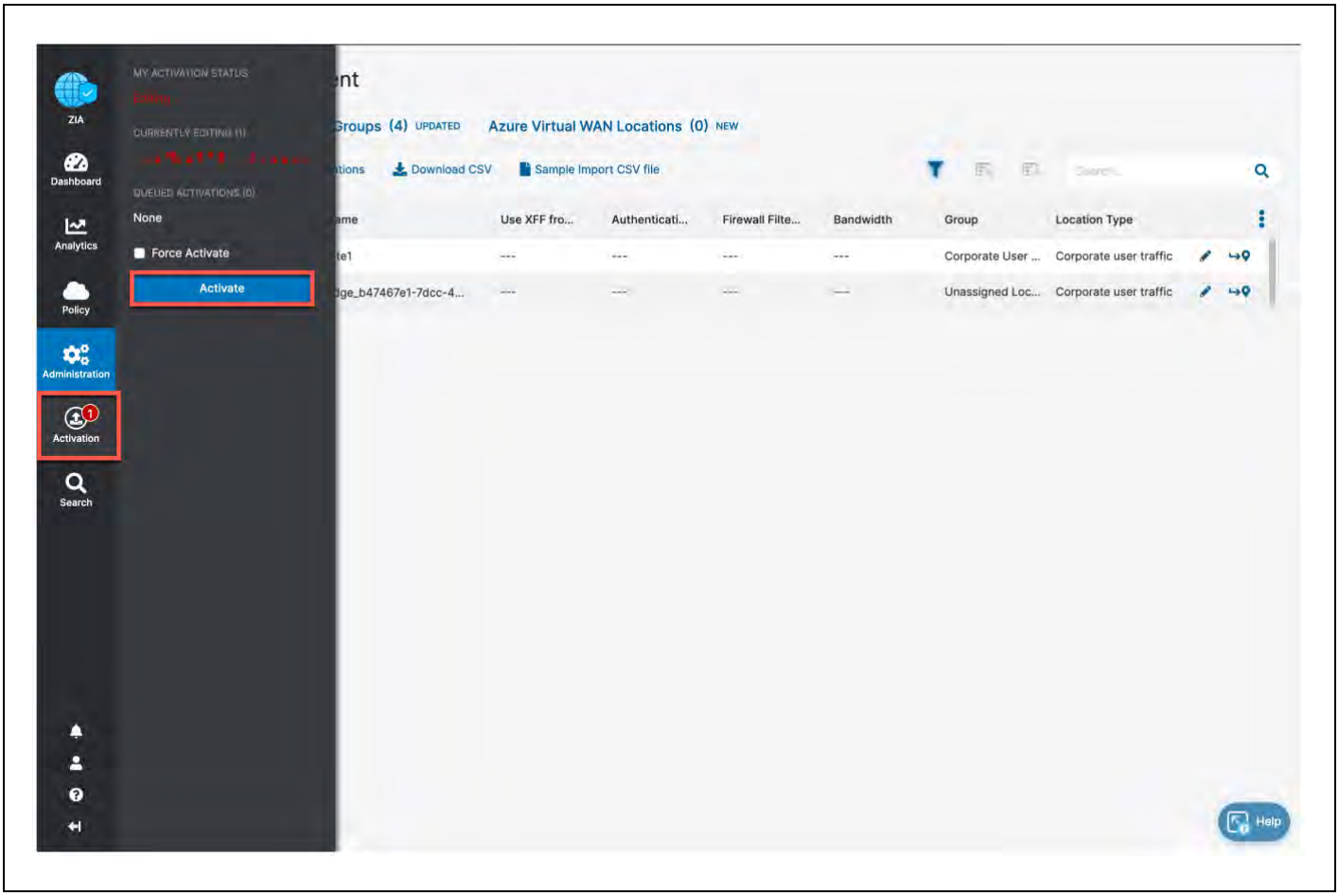

Figure 6.4-A: Activate Changes

Login ID obfuscated for security

This lets you know that you have changes pending in queue for activation. When you are ready to activate all changes in queue, click the blue **Activate** button.

6.5 Activation Confirmation

After activating all pending changes, you should see “Activation Completed” in the red box. At this point, all queued changes have been pushed into production. These changes should take effect within seconds.

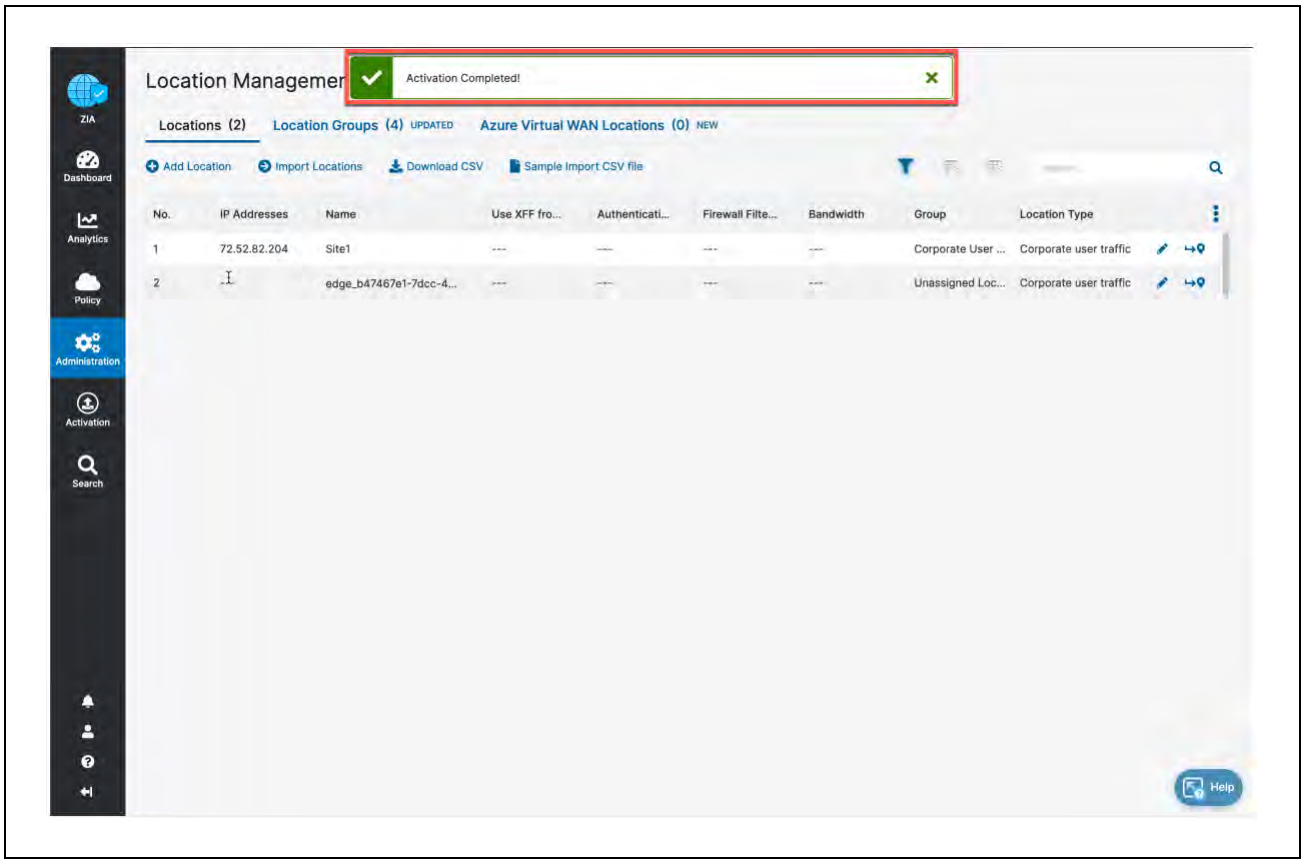

Figure 6.5-A: Activation Confirmation

This this point, you have a location, with a public IP associated to the location, and are ready to start configuring the VMware SD-WAN side.

7 Appendix D: Verifying ZIA Configuration

7.1 Request Verification Page

The URL https://ip.zscaler.com can be used to validate if you are transiting ZIA. In *Figure 90* and 91 below, you will see examples of what the page output should display if you are or are not transiting ZIA.

Note: the IP information presented in both figures should not match and instead should be your client IP address when attempting this page view.

Figure 7.1-A: Non-working Example

If you are transiting ZIA, you should see the following:

Figure 7.1-B: Working Example

8 Appendix E: Checking tunnel status in ZIA Admin

If you want to check the current status of tunnels to ZIA from your sites, ZIA provides the ability to see the traffic volume sent / received from your SD-WAN appliances and logging to see the current state of the tunnels via logging.

Navigation: Analytics → **Insights** → and then click **Tunnel Insights**.

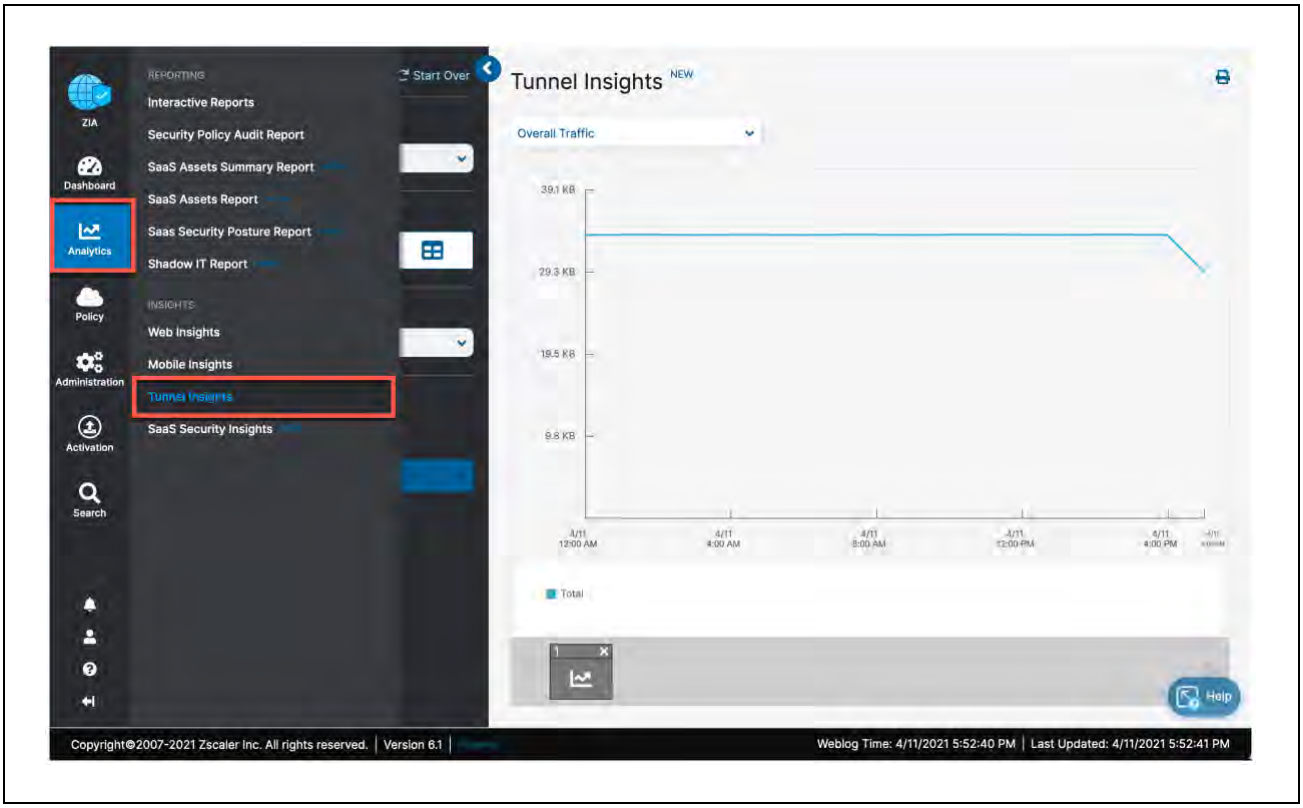

Figure 8-A: Navigate to Tunnel Insights

8.1 Tunnel Data Visualization

In the Insights screen you have the ability to visualize and filter data in various ways. Configure the Timeframe, Chart type, and Metrics you wish to view.
Additionally, you can filter the type of data shown in the chart, by clicking the "*filter*" carrot to expose a dropdown menu to select from.

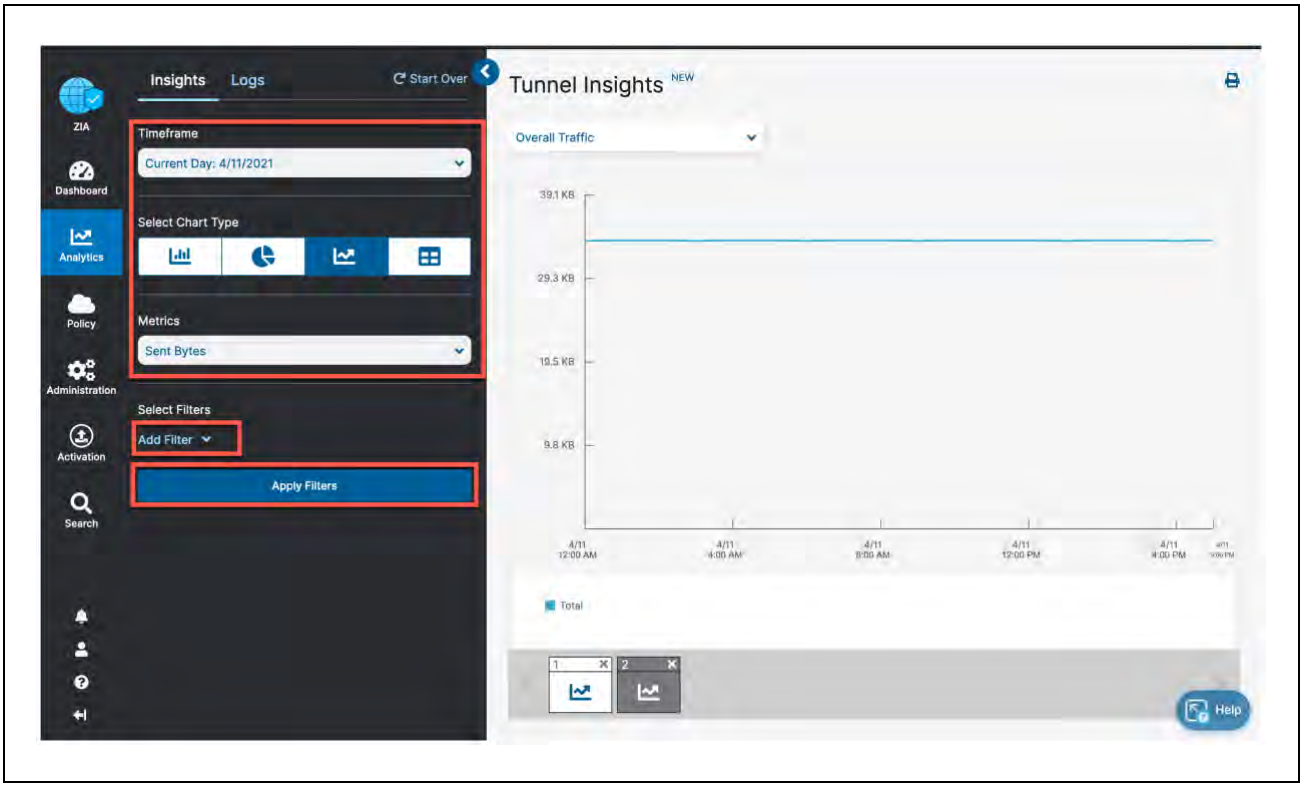

Figure 8.1-A: ZIA Tunnel Insight Charts

For further information please refer to ZIA Tunnel Insights help:
https://help.zscaler.com/zia/tunnel-data-types-and-filters

8.2 Tunnel Logging

To assist in troubleshooting you can also view the state of all tunnels for your tenant from the ZIA Admin UI. Click on the "*Logs*" button:

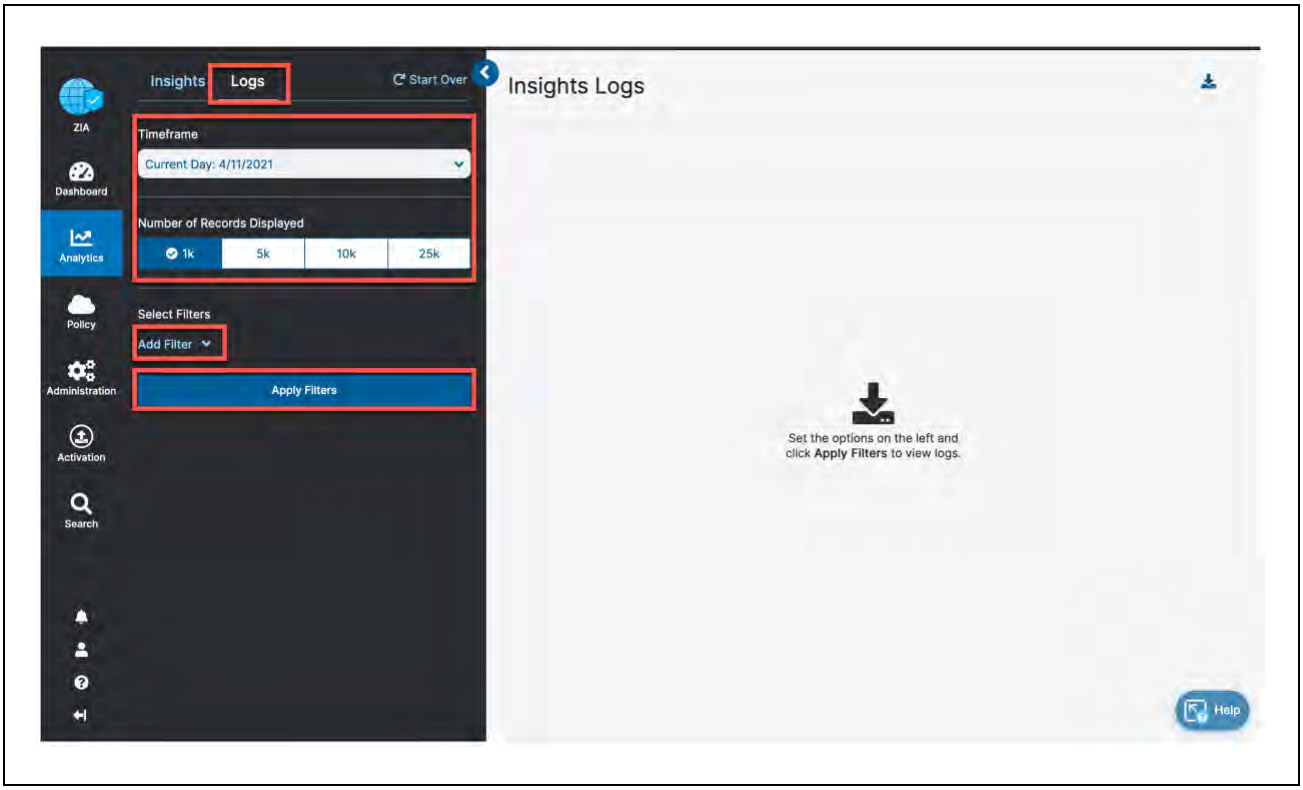

Figure 8.2-A: Viewing ZIA tunnel logs

From this screen you can then filter and change the timeframe for the tunnels and sites you would like to investigate. Please see the ZIA Tunnel Insights Logs: Columns help for details on the options: https://help.zscaler.com/zia/tunnel-insights-logs-columns

9 Appendix F: Deriving the Zscaler IPSEC VPN VIP

All Zscaler public IP endpoints can be found at https://config.zscaler.com/. It is preferred to use DNS hostnames as the destination for Tunnels and Proxies into the ZIA service. If the service or device that is the source of the traffic doesn't support DNS names, as is the case for AWS Customer Gateways you will need to derive the IP address from the DNS hostname of the endpoint.

When you go to the above URL, make sure you select the correct Zscaler *Cloud* that your tenant is provisioned into, ensure that *Cloud Enforcement Node Ranges* is selected from the navigation frame and then choose the closest DC locations *VPN Host Name* to your AWS region.

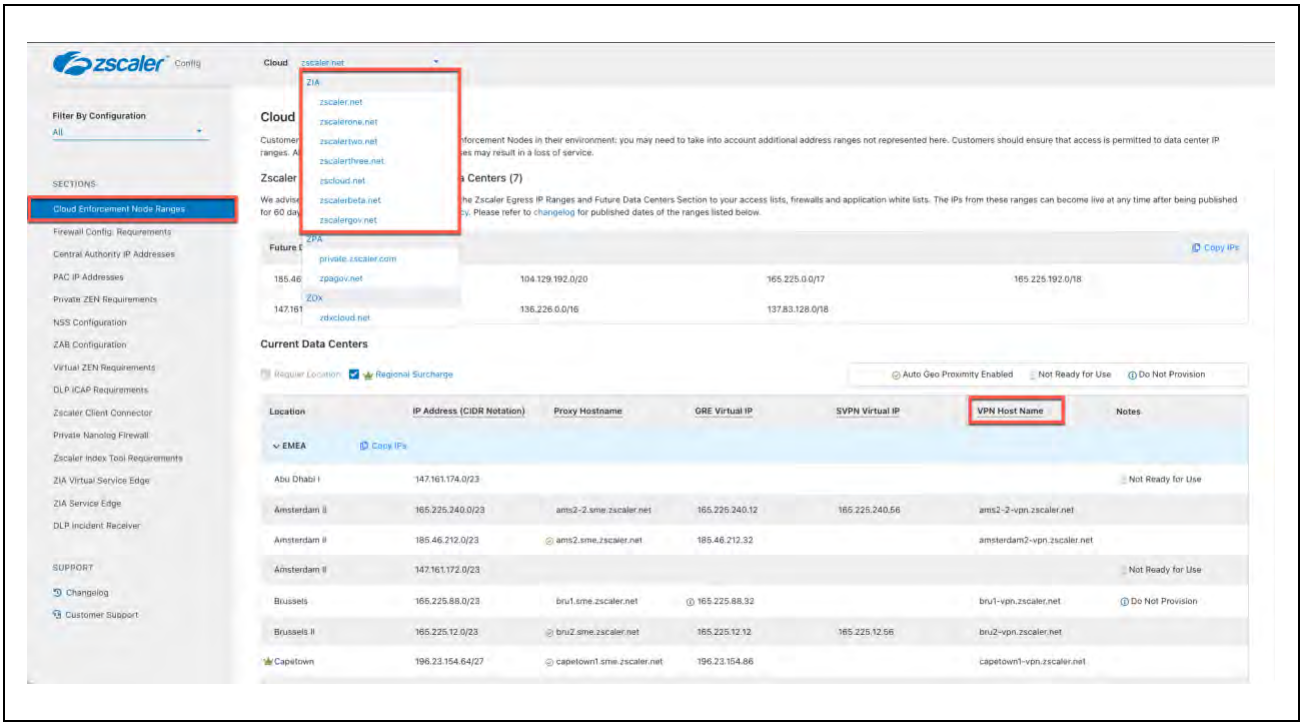

Figure 9-A: Zscaler Public IP reference

Then use either **nslookup** or **dig** to get the IP address from the DNS hostname, example:

```
➜  ~ dig ams2-2-vpn.zscaler.net

; <<>> DiG 9.10.6 <<>> ams2-2-vpn.zscaler.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38701
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;ams2-2-vpn.zscaler.net.            IN    A

;; ANSWER SECTION:
ams2-2-vpn.zscaler.net. 1800  IN    A     165.225.240.18

;; Query time: 50 msec
;; SERVER: 192.168.83.35#53(192.168.83.35)
;; WHEN: Thu Mar 25 22:32:28 PDT 2021
;; MSG SIZE  rcvd: 67
```

Figure 9-B: IP address lookup

10 Appendix G: Requesting Zscaler Support

10.1 Gather Support Information

Zscaler support is sometimes required for the provisioning of certain services. Zscaler support is also available to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round.

10.1.1 Obtain Company ID

First, let's grab our Company ID, which is how Zscaler uniquely identifies a given customer. The navigation is: **Administration** → **Settings** → and then click **Company profile**.

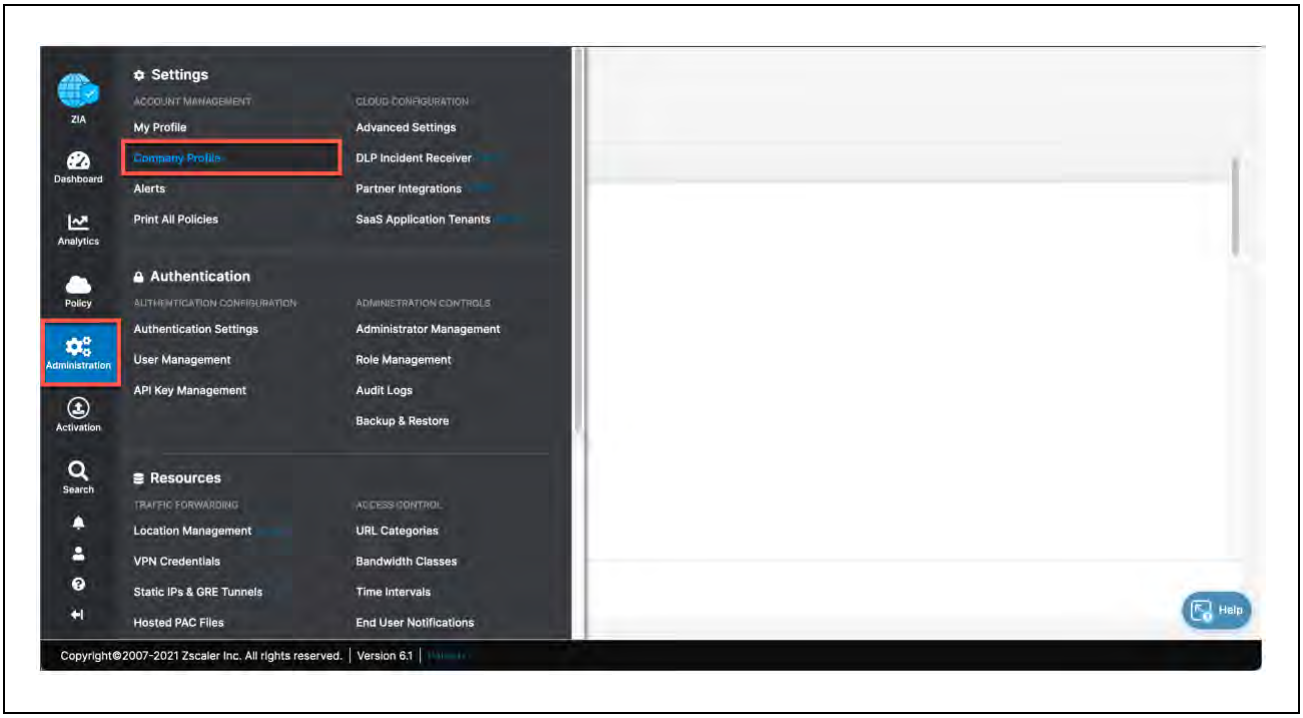

Figure 10.1-A: Obtaining Company ID

10.1.2 Save Company ID

Your company ID can be found in the red box below. Please copy this ID somewhere convenient as we will need it in subsequent screens.

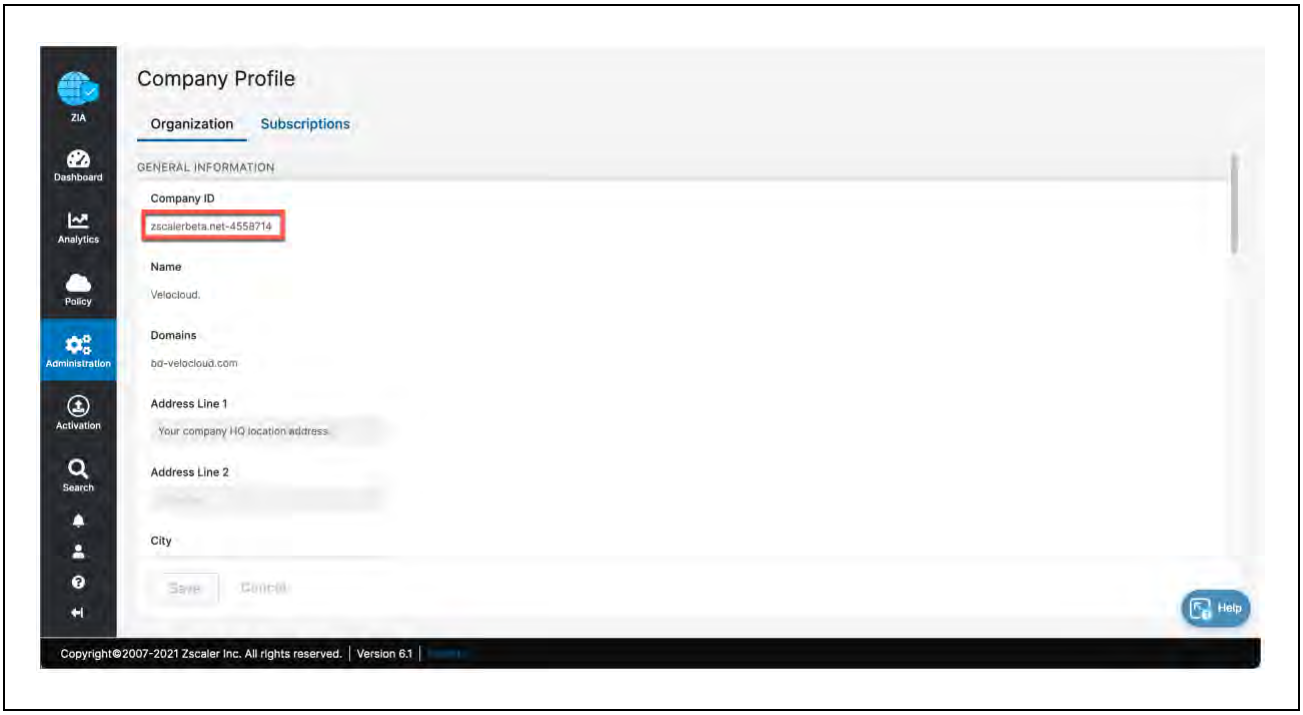

Figure 10.1.2-A: Save Company ID

10.1.3 Open Support Ticket

Now that we have our company ID, we are ready to open a support ticket. The navigation is: **"?"** → **Support** → and then click **Submit a Ticket**. You can also go directly to the ***Submit Ticket*** page by visiting https://help.zscaler.com/submit-ticket.

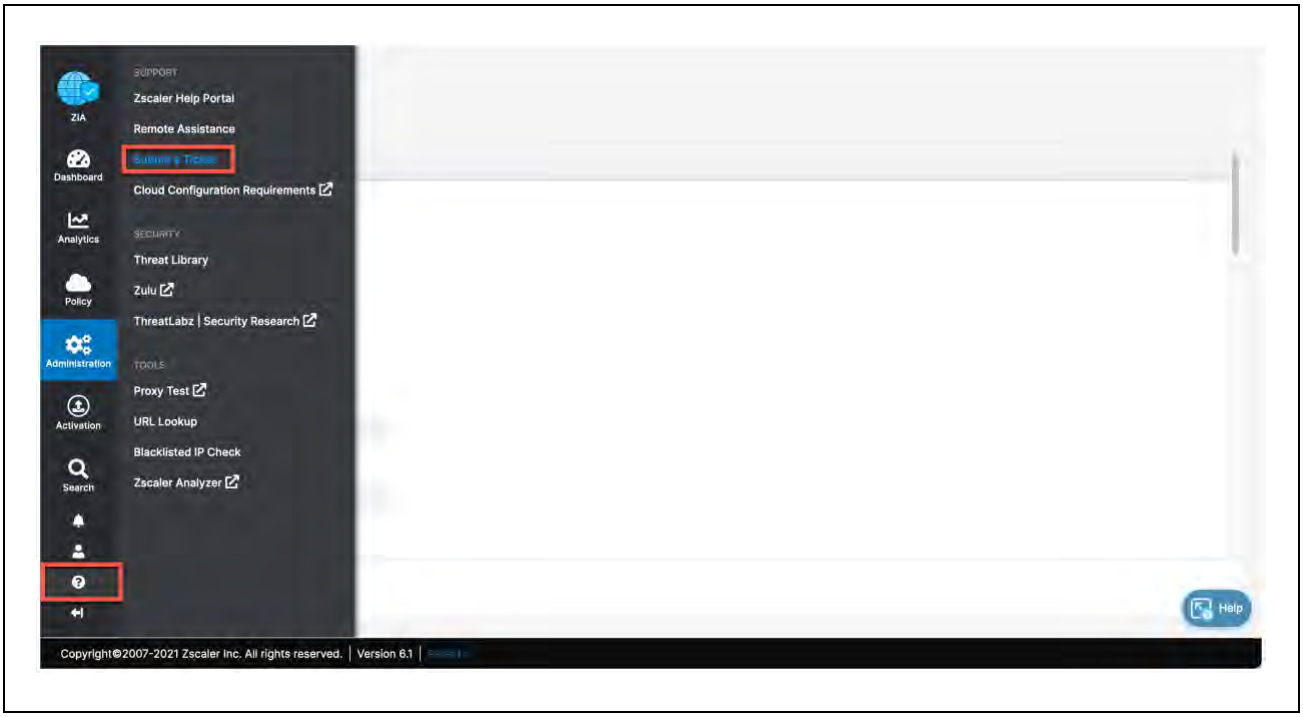

Figure 10.1.3-A: Enter Support Section

10.2 Adding Domain (Example)

Figure 10.2-A shows an example of how a support ticket is generally made. Each support ticket will ask targeted questions as a Ticket Type is defined. In this example below, we are requesting a domain be added to our ZIA instance.

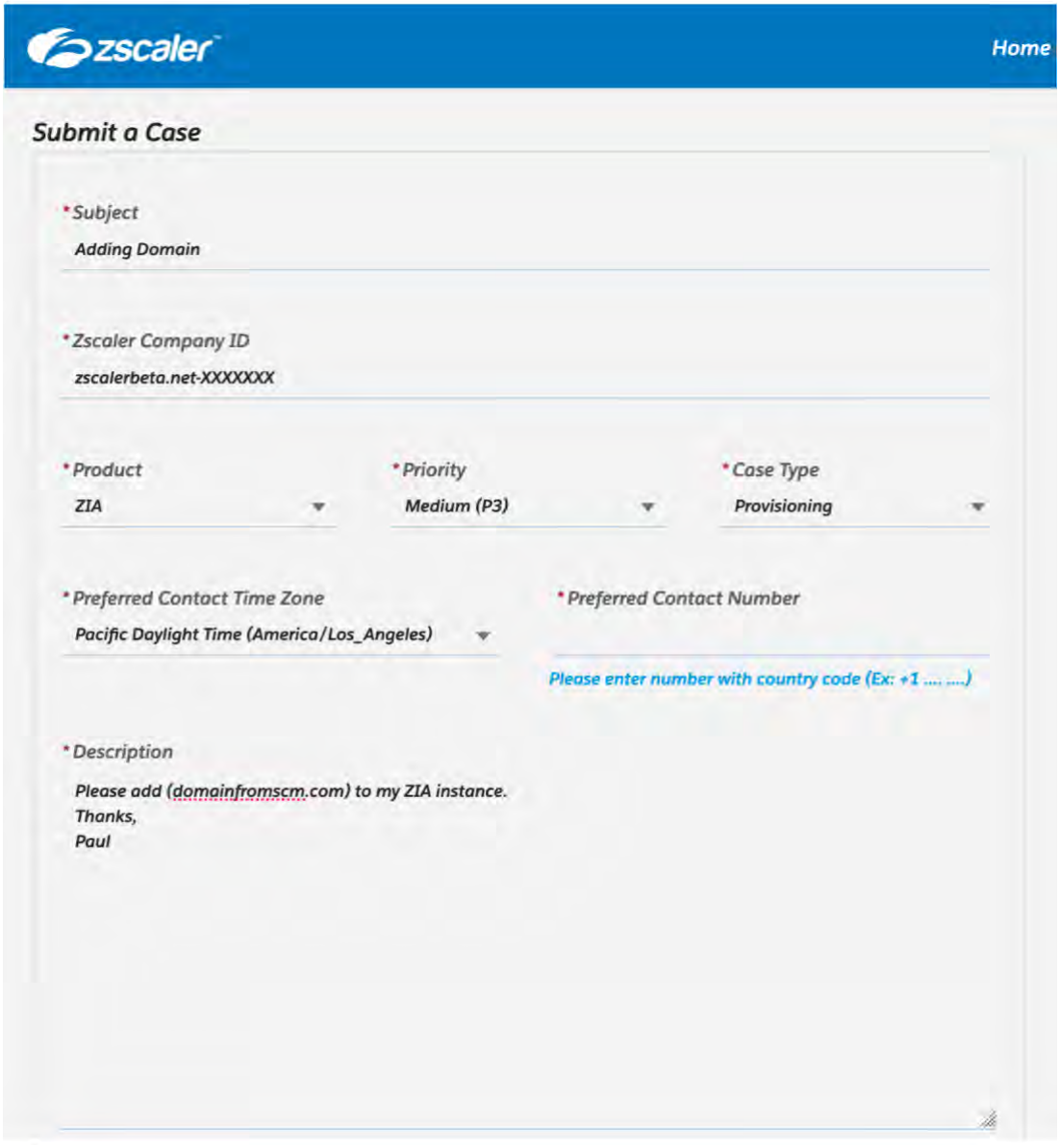

Figure 10.2-A: Adding Domain Example

11 Appendix H: Zscaler Resources

Zscaler Knowledge Base:
https://support.zscaler.com/hc/en-us/?filter=documentation

Zscaler Tools:
https://www.zscaler.com/tools

Zscaler Training and Certification:
https://www.zscaler.com/resources/training-certification-overview

Zscaler Submit a Ticket:
https://help.zscaler.com/submit-ticket

ZIA Test Page
http://ip.zscaler.com/

11.1 Zscaler IP Page

https://config.zscaler.com/

12 Appendix I: VMware SD-WAN Resources

VMware SD-WAN
https://sdwan.vmware.com/

VMware SD-WAN Support
https://sdwan.vmware.com/customers/support

VMware SD-WAN Knowledgebase
https://kb.vmware.com/s/