Zscaler Internet Access (ZIA) and Cisco SD-WAN Deployment Guide

March 2019

Version 2.0

Table of Contents

Terms and Acronyms

Acronym	Definition
DPD	Dead Peer Detection *(RFC 3706)*
GRE	Generic Routing Encapsulation *(RFC2890)*
IKE	Internet Key Exchange *(RFC2409)*
IPsec	Internet Protocol Security *(RFC2411)*
OAM	Operation, Administration, and Management
OMP	Overlay Management Protocol (Cisco SD-WAN)
PFS	Perfect Forward Secrecy
SSL	Secure Socket Layer *(RFC6101)*
TLS	Transport Layer Security *(RFC5246)*
vBond	Cisco SD-WAN orchestrator facilitates the initial bring-up authentication and authorization of the network elements.
SD-WAN Edge	Cisco SD-WAN Router Platform
vSmart	Cisco SD-WAN centralized control plane and policy engine
XFF	X-Forwarded-For *(RFC7239)*
ZAPP	Zscaler End-point Client Application
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

1 Document Overview

This Deployment Guide document will provide GUI examples for configuring Zscaler Internet Access (ZIA) and Cisco SD-WAN. 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 ZIA and with Cisco SD-WAN.

The Cisco SD-WAN portion of this document was authored by Cisco.

1.1 Document Audience

This document was designed for Network Engineers and Network Architects. For additional product and company resources, please refer to the Appendix section.

1.2 Software Revisions

This document was written using Zscaler Internet Access v5.6 and Cisco SD-WAN 18.3.0.

1.3 Request for Comments

We value the opinions and experiences of our readers. To offer feedback or corrections for this guide, please contact partner-doc-support@zscaler.com.

1.4 Document Prerequisites

Zscaler Internet Access (ZIA)

- A working instance of ZIA 5.6 (or newer)
- Administrator login credentials to ZIA

Using vManage (GUI)

- A working instance of Cisco SD-WAN vManage with administrator login credentials.

Using CLI:

- Must have IP or console access to the device.
- Must have the valid user credentials for the Cisco SD-WAN device (SD-WAN Edge Router)

1.5 Document Revision Control

Revision	Date	Change Log
1.0	August 2017	Initial document by Zscaler and Viptela
1.1	August 2017	Updated Viptela references to Cisco SD-WAN
1.2	September 2017	Minor edits
1.3	September 2018	Major update: ▪ Updated ZIA screen captures to ZIA 5.6 ▪ Added IPsec Section ▪ Other supporting edits
2.0	March 2019	Added GRE and IPsec template creation

1.6 Lab Topology and Configuration Overview

This document is based on the following lab topology. Our lab branch office has two Cisco SD-WAN Edge routers. Cisco SD-WAN Edge-1 will be used for establishing dual GRE tunnels to diverse Zscaler locations. Cisco SD-WAN Edge-2 will be used for establishing dual IPsec tunnels to diverse Zscaler locations.

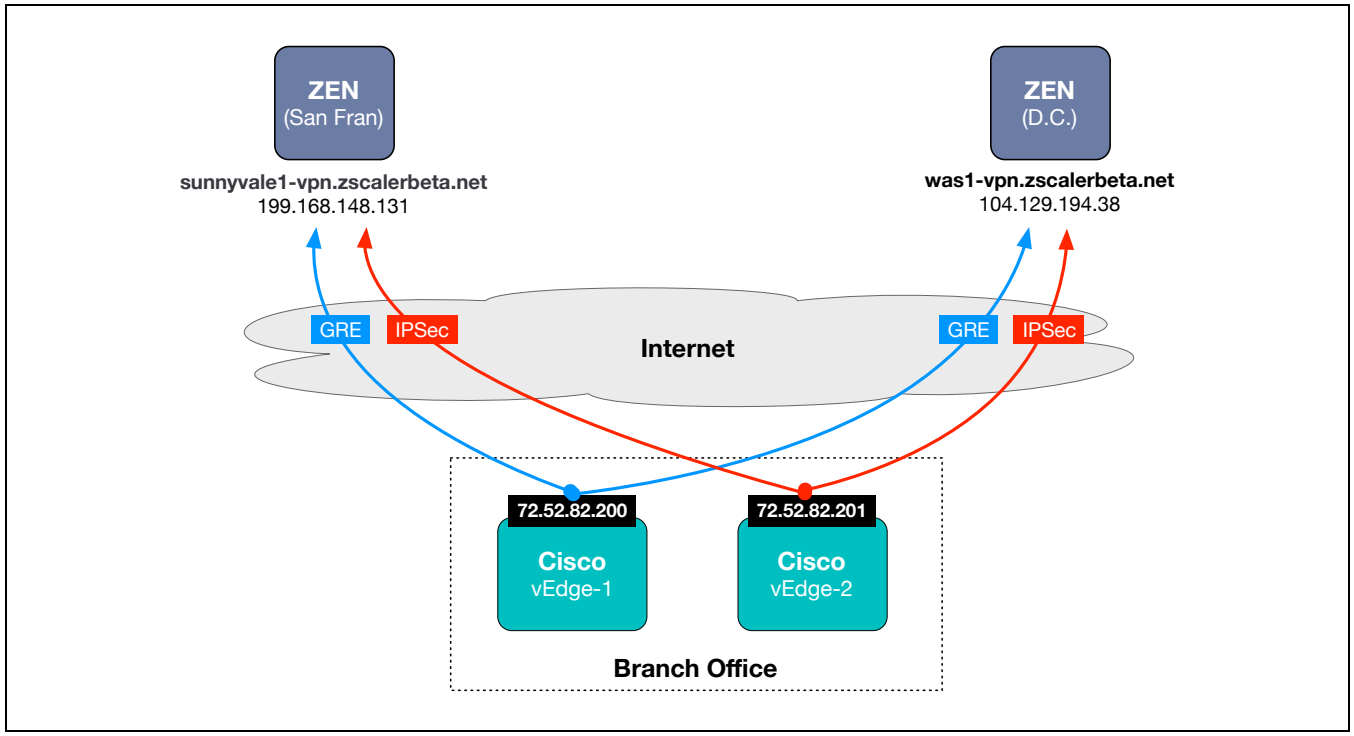


Figure 1: ZIA GRE Configuration Details

Note: This topology and proposed configuration is for demonstration purposes and is not necessarily what should be deployed by customers. The following IP addresses and IP subnets will be used for this section:

	Primary Tunnel	Secondary Tunnel
Tunnel Destination	199.168.148.131	104.129.194.38
Tunnel Source	72.52.82.200	72.52.82.200

Figure 2: ZIA GRE Configuration Details

If you intend to reference this section to configure a GRE tunnel to Zscaler, and you do not have your GRE Tunnel details, please open a support ticket. The instructions to open a Zscaler support ticket for GRE provisioning is in section 9, “Requesting Zscaler Support”.

2 Configuring Zscaler Internet Access (ZIA)

2.1 Logging into ZIA

Figure 3: Log into Zscaler

First, we will setup the Zscaler side of this service. The required steps for this section are:

- Log into Zscaler using your administrator account. If you are unable to log in using your administrator account, please contact support: https://help.zscaler.com/submit-ticket.

2.2 Configuring ZIA for GRE Tunnel

2.2.1 Navigate to Locations

After logging in, we need to add a location is one is not present for GRE access to ZIA. If you are uncertain if you already have a site configured, these steps will verify a location is present.

Navigation: Administration -> **Resources** -> and then click **Locations**.

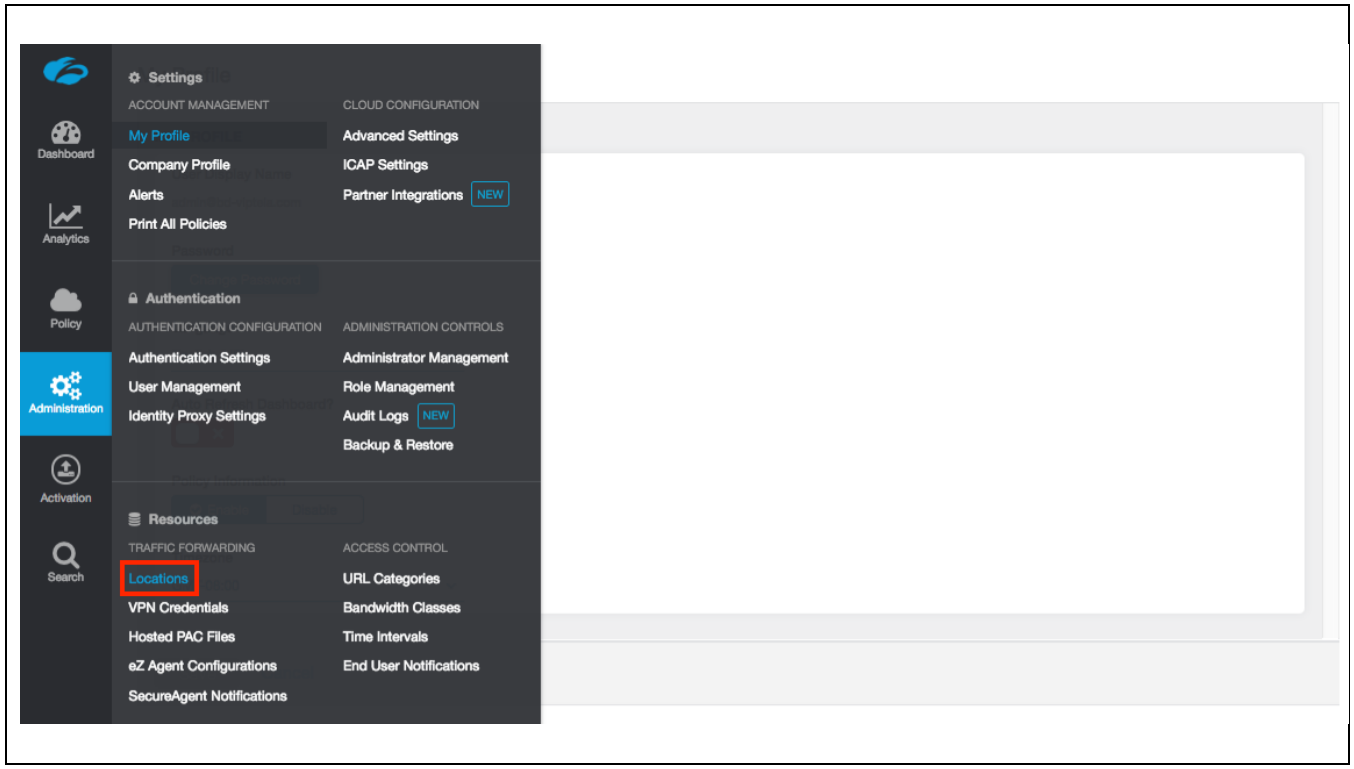


Figure 4: Navigate to Locations

2.2.2 Add a Location

In Figure 5, if you see "*No Matching Items Found*", your ZIA instance does not have any locations configured. To add a location, click "Add" that is identified in the red box in the upper left.

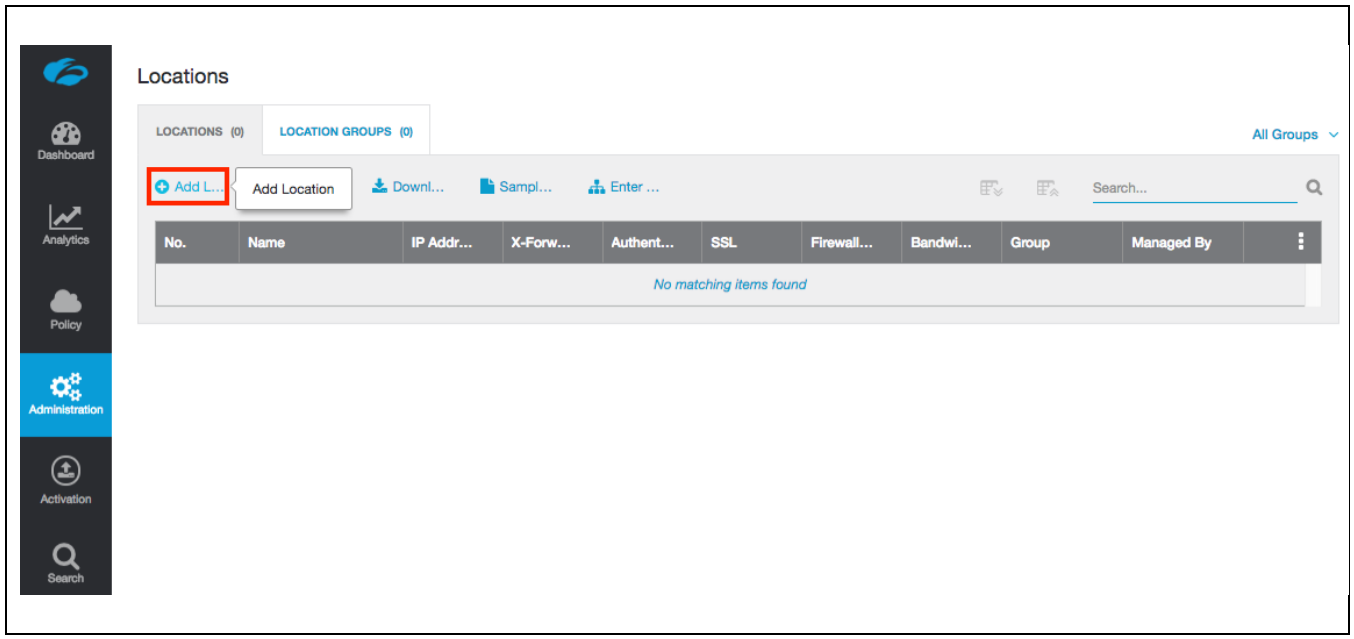


Figure 5: Add a Location

Note: It is common for ZIA users to have 1 location per physical location. The amount of locations can scale to the largest of Enterprise networks.

2.2.3 Enter Location Data

The data in the red box in Figure 6 must be entered.

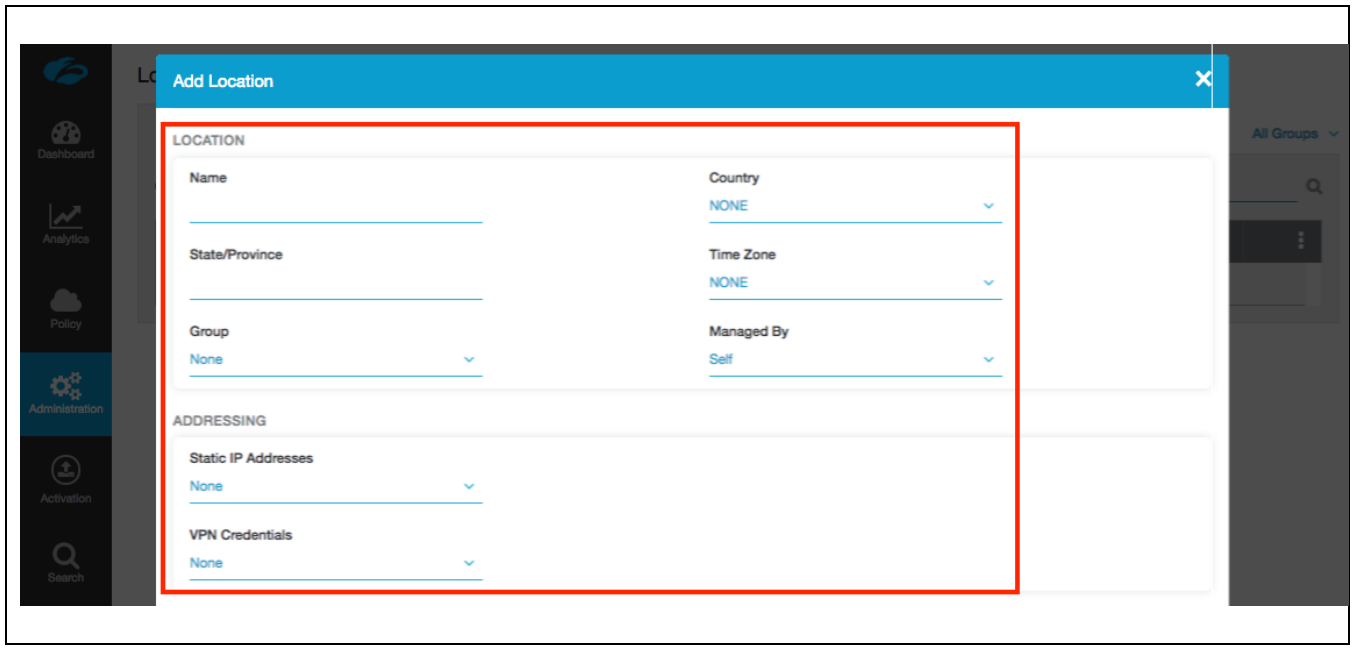


Figure 6: Enter Location Data

Note: If the "Public IP Address" does not show the IP address to your new location, please refer to section "Requesting Zscaler Support". A support ticket will need to be created to have the public IP address of your location present to associate to your new location. The next section will provide examples with a Public IP address defined prior.

2.2.4 Verify Location Information and Save

Now that you have entered your location information, you are ready to save your new location. Please click “Save” in Figure 7 the red box to continue.

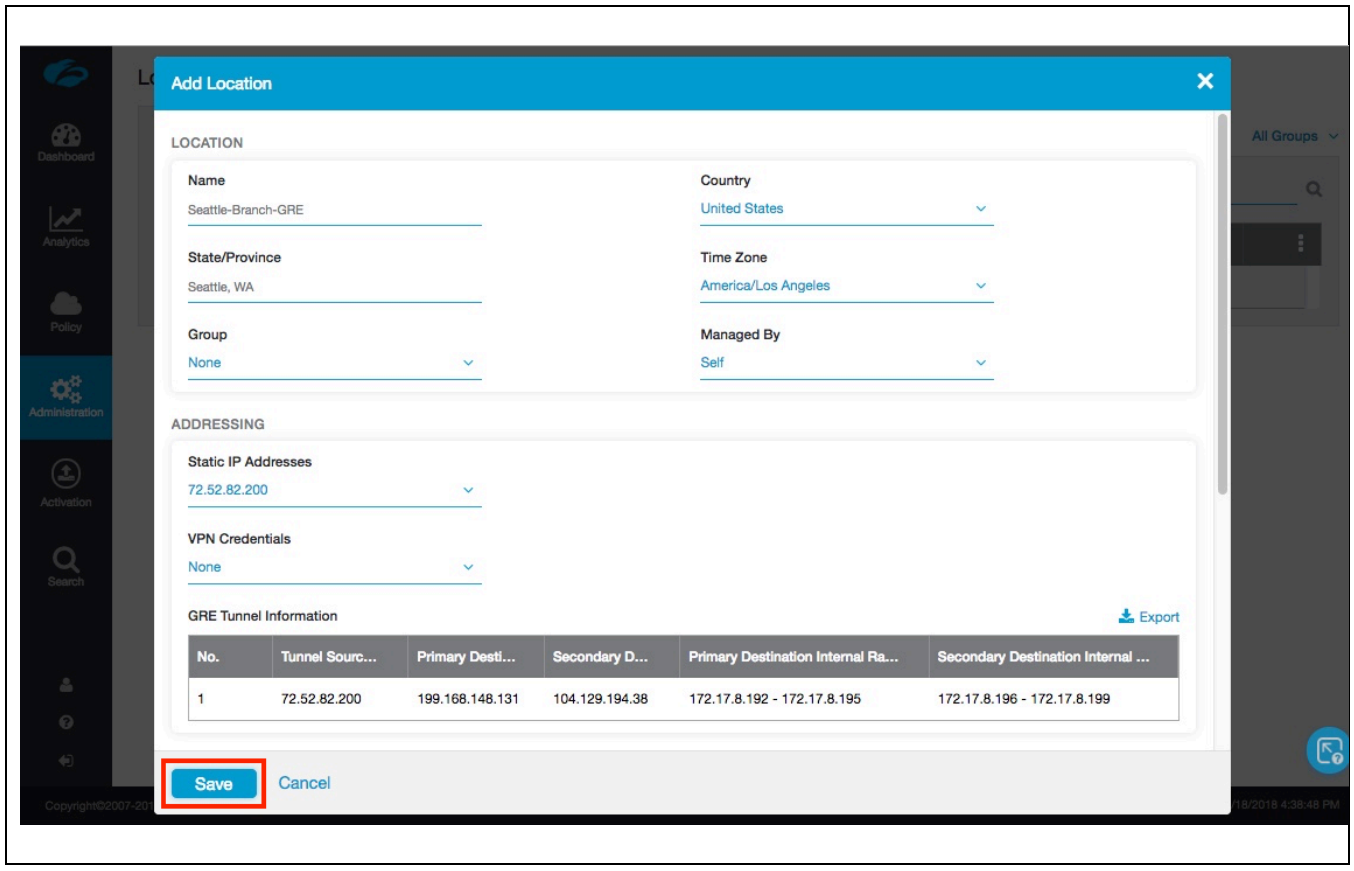


Figure 7: Verify Location Information and Save

2.2.5 Confirm Changes Have Been Submitted

Once you click “Save”, the screen will refresh and you should see “All Changes have been saved” on the top of the page. Below that, you should see the new location.

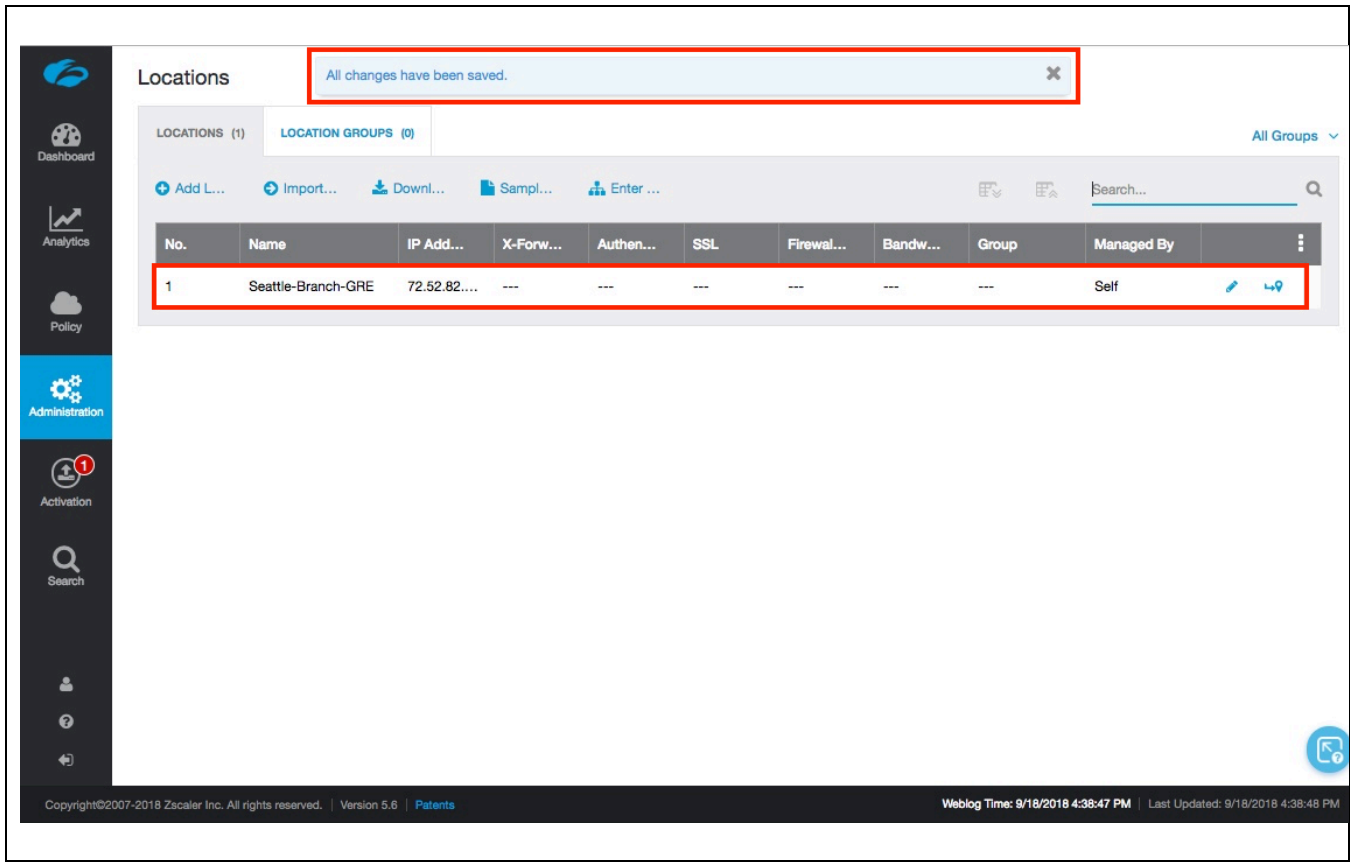


Figure 8: Confirm Changes Have Been Submitted

At this point, although we have saved our new location, it has only submitted the change for pending activation. If you wanted to make other changes throughout ZIA, you could. None of these changes would get applied until they are activated, which allows you to batch groups of changes as you require. Only upon activation do the changes get pushed to ZEN nodes.

2.3 Configuring ZIA for IPsec Tunnel

2.3.1 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. Please refer to Figure X: Navigate to VPN Credentials.

Navigation: Administration -> **Resources** -> and then click **VPN Credentials**.

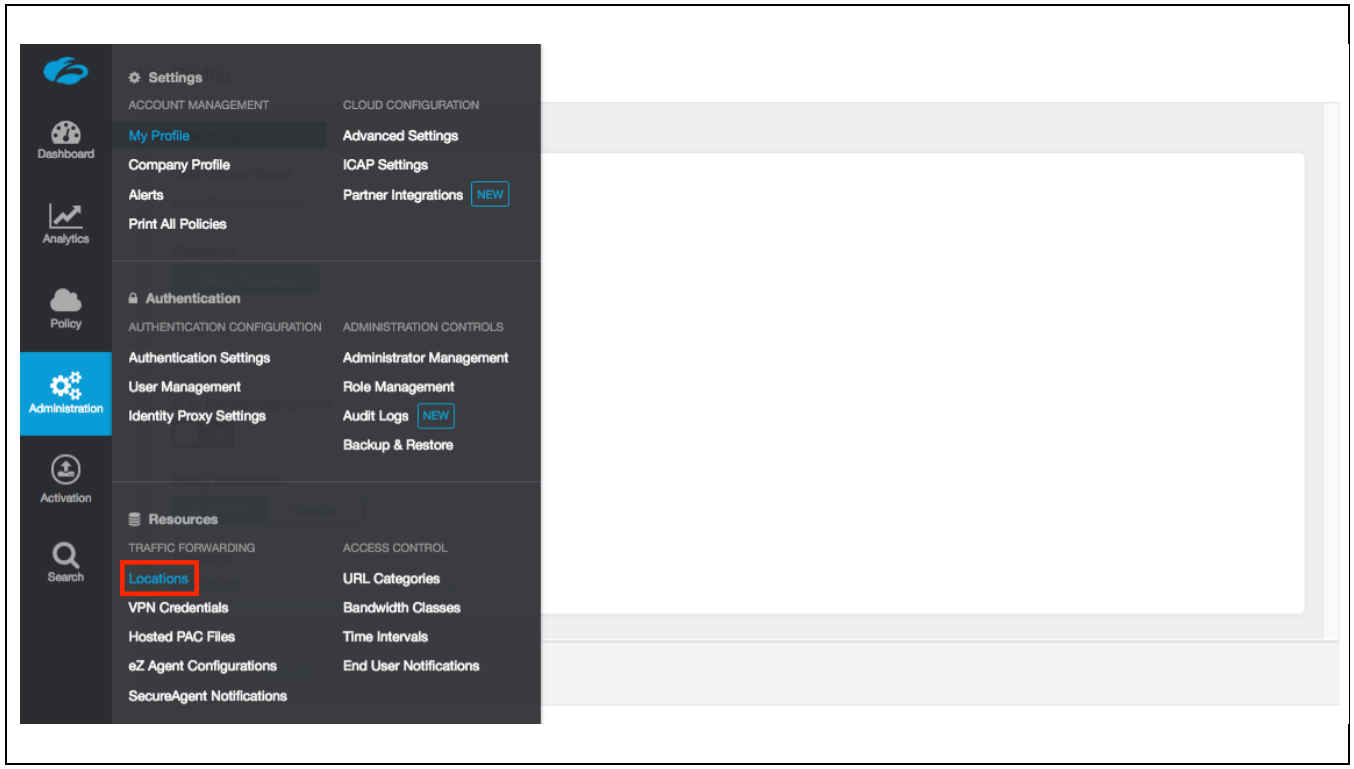


Figure 9: Navigate to VPN Credentials

2.3.2 Add a VPN Credential

In Figure 10, if you see "*No Matching Items Found*", your ZIA instance does not have any locations configured. To add a location, click "Add" that is identified in the red box in the upper left.

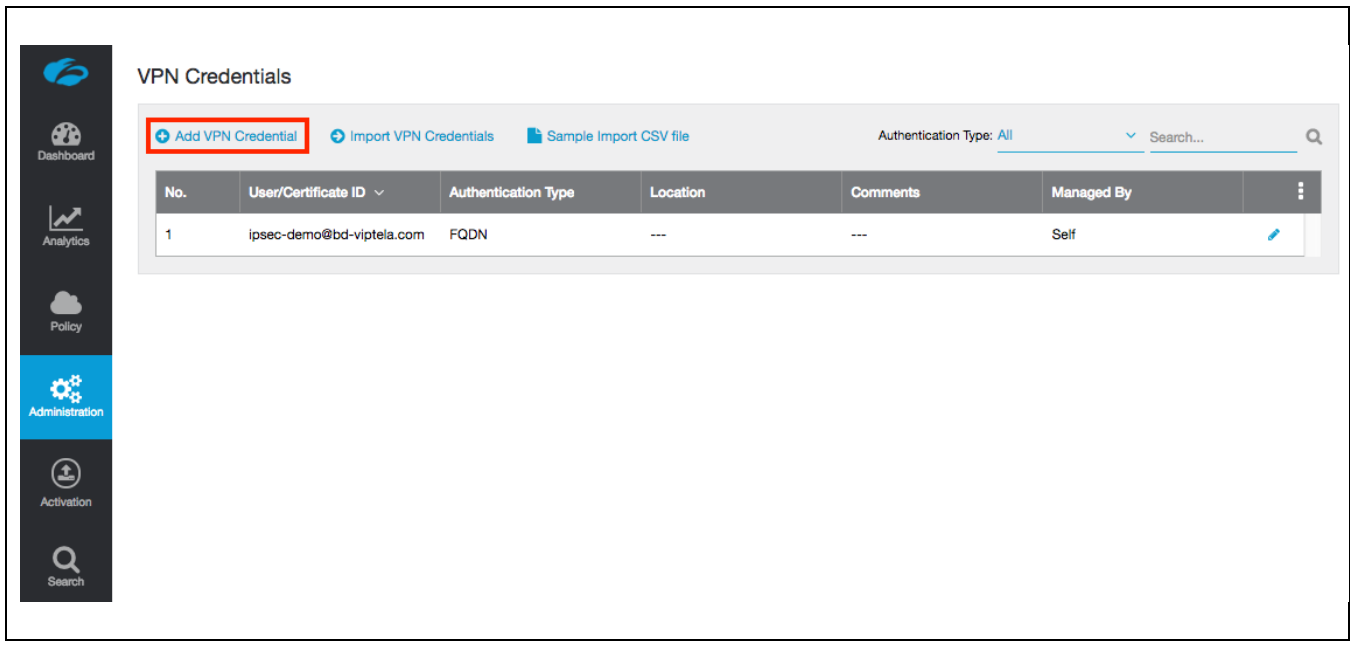


Figure 10: Adding a VPN Credential

It is common for ZIA users to have 1 location per physical location. The amount of locations can scale to the largest of Enterprise networks.

2.3.3 Enter VPN Credential Data

In Figure 11, we will 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 will automatedly be added (which is to the right). Once both the FQDN and PSK are configured, click “Save” to continue.

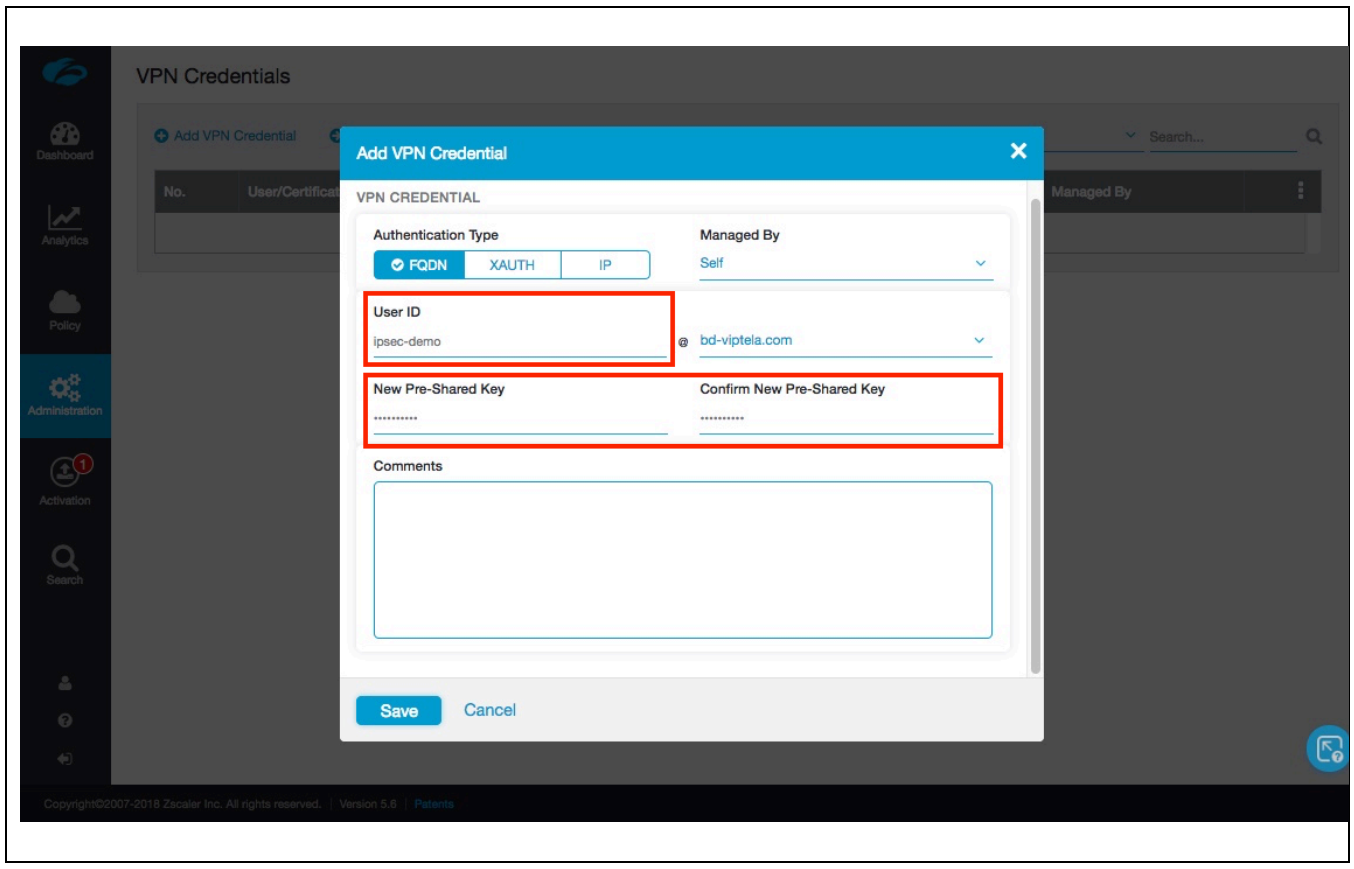


Figure 11: Enter VPN Credential Data

2.3.4 Verify Location Information and Save

In Figure 12, 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.

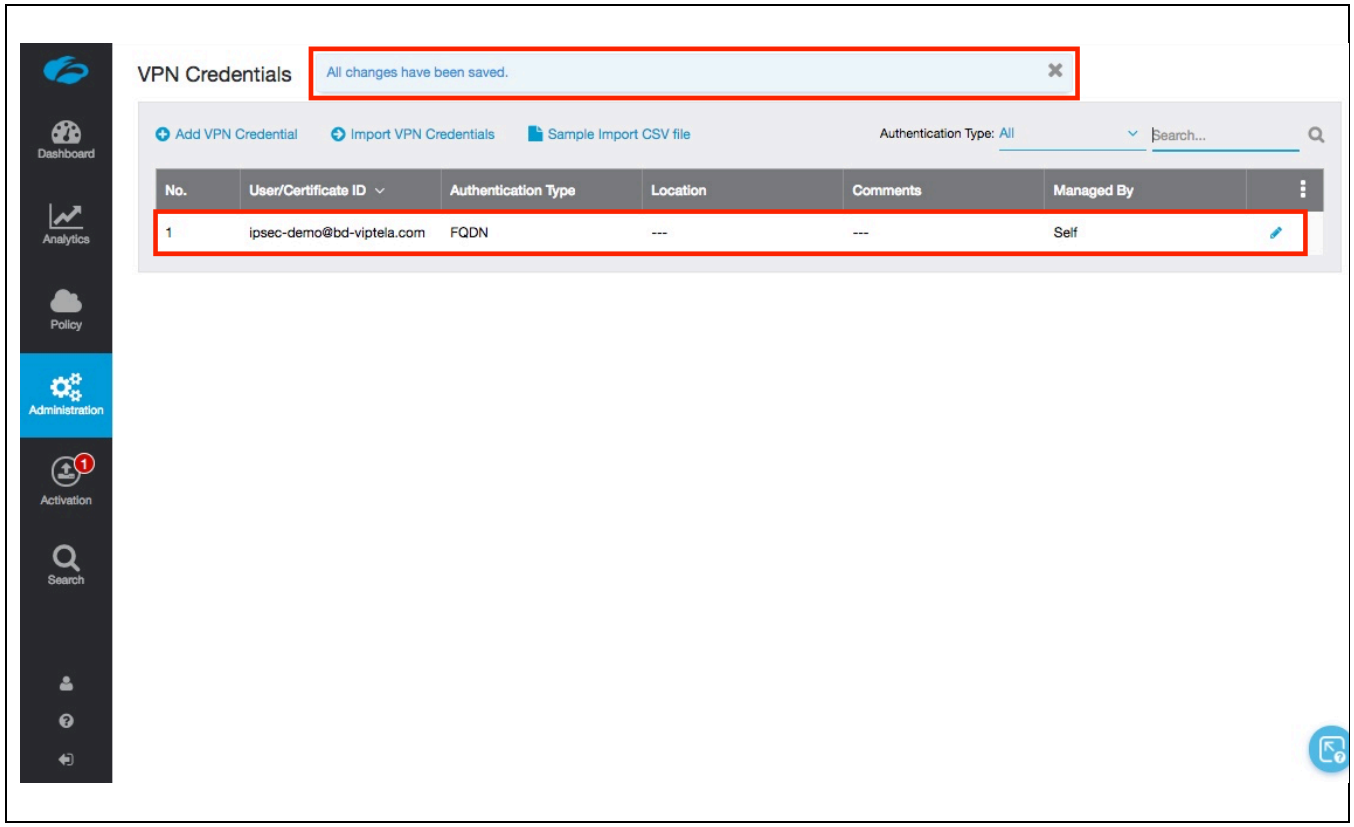


Figure 12: Verify Location Information and Save

2.3.5 Navigate to Locations

After logging in, we need to add a location is one is not present for GRE access to ZIA. If you are uncertain if you already have a site configured, these steps will verify a location is present.

Navigation: Administration -> **Resources** -> and then click **Locations**.

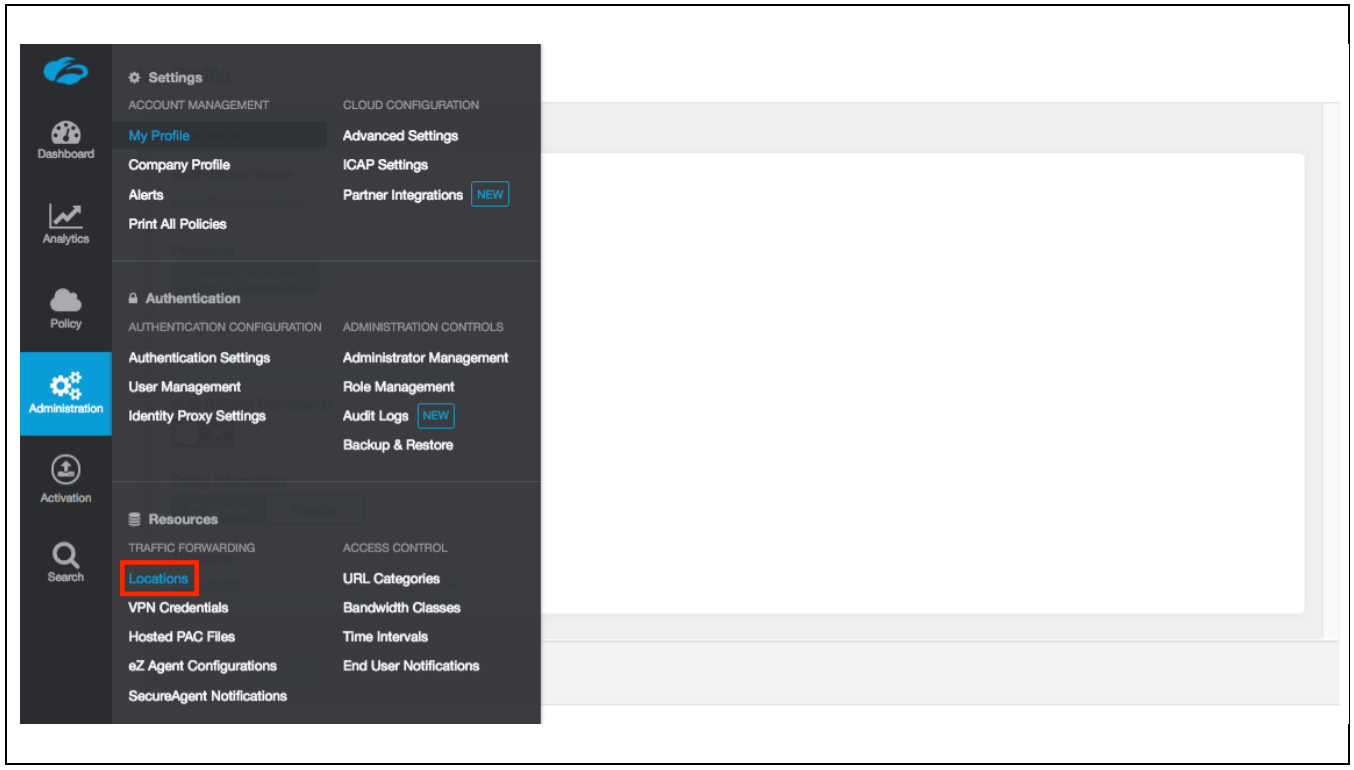


Figure 13: Navigate to Locations

2.3.6 Add a Location

In “Figure 5: ”, if you see “*No Matching Items Found*”, your ZIA instance does not have any locations configured. To add a location, click “Add” that is identified in the red box in the upper left.

Figure 14: Add a Location

It is common for ZIA users to have 1 location per physical location. The amount of locations can scale to the largest of Enterprise networks.

2.3.7 Enter Location Data

In Figure 15, you will need to fill in the fields within the red box. The name of the location will be 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. Lastly, under “VPN Credential”, select the VPN credential you configured in the prior steps. Once you select the drop down, the screen in the next section will appear.

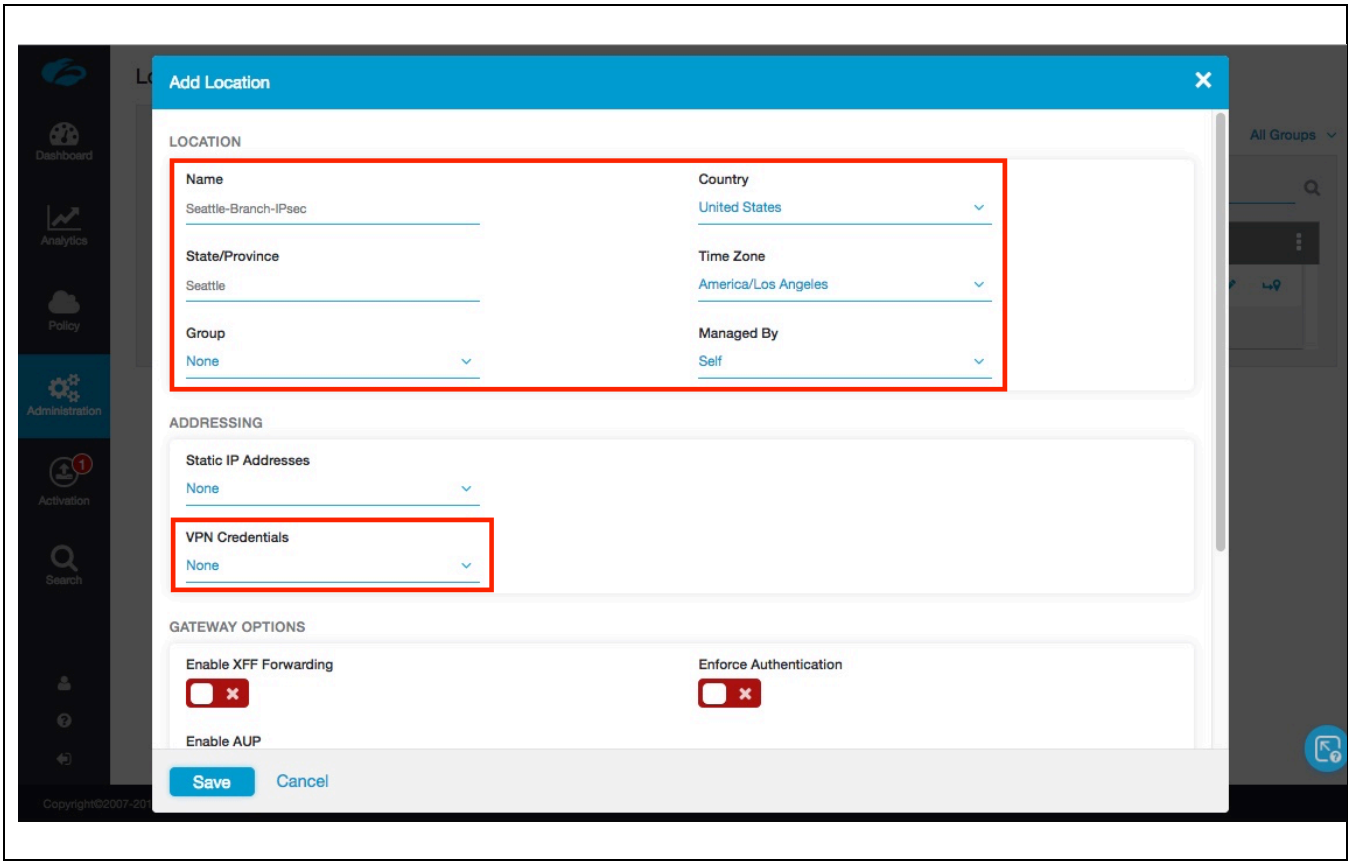


Figure 15: Enter Location Data

2.3.8 Add VPN Credential to Location and Save

In Figure 16, you should see the VPN Credential you configured in the prior section. Select it and click “Save” after. 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.

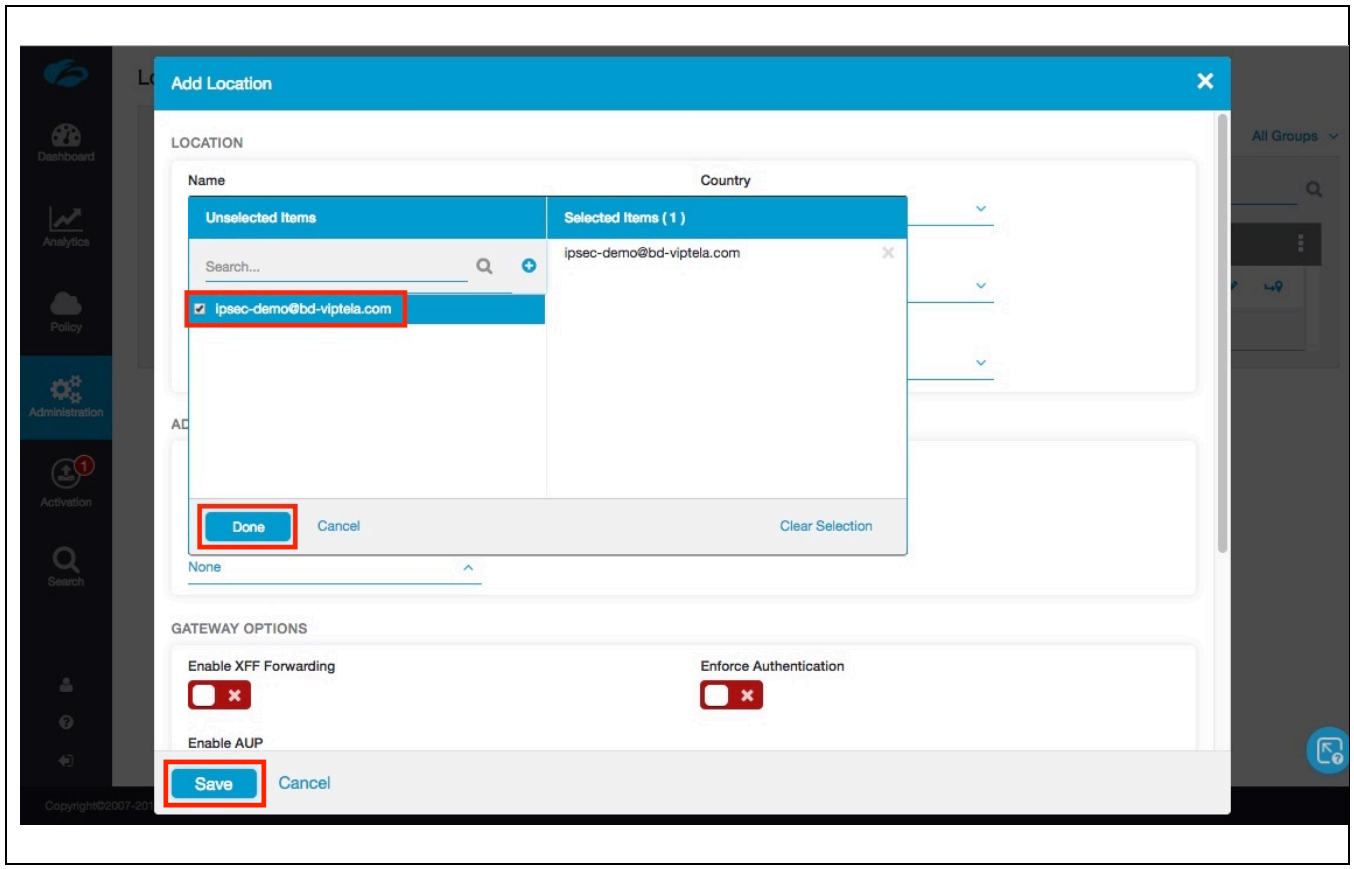


Figure 16: Add VPN Credential to Location and Save

2.3.9 Confirm Changes Have Been Saved

In Figure 17, 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.

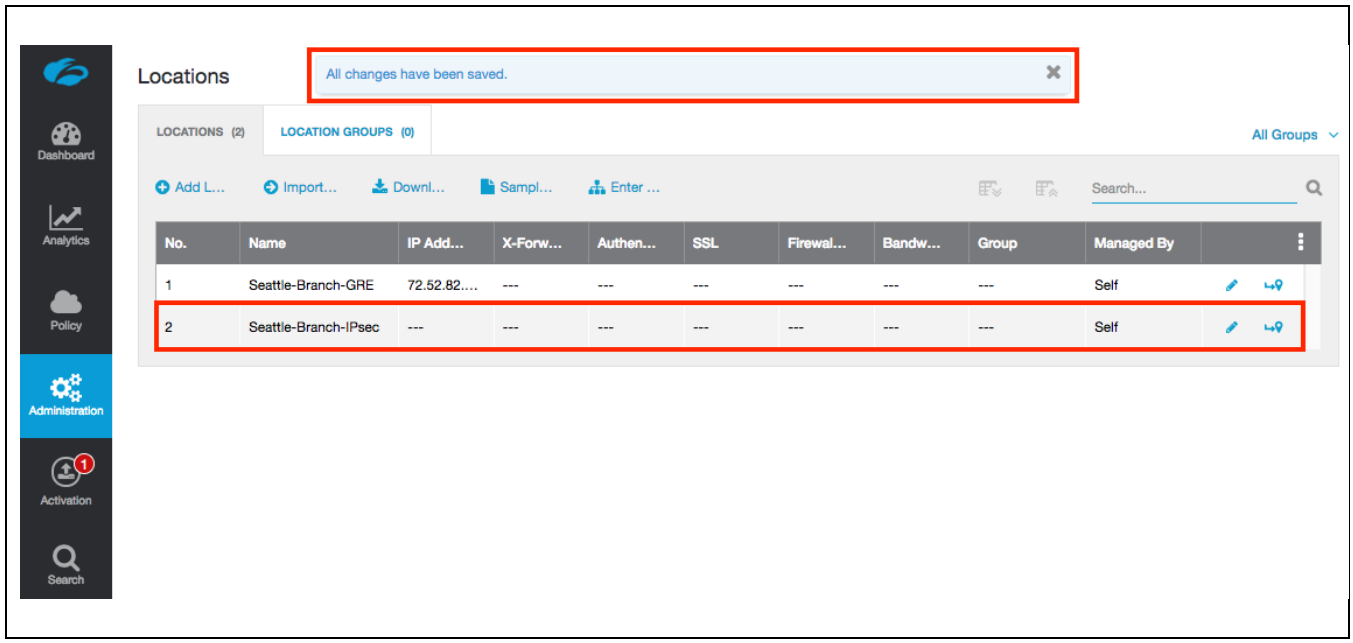


Figure 17: Confirm Changes Have Been Saved

2.4 Activate Pending Changes

2.4.1 Activate Changes

Anytime you make a change in ZIA, you will see a number over the image in the upper right corner.

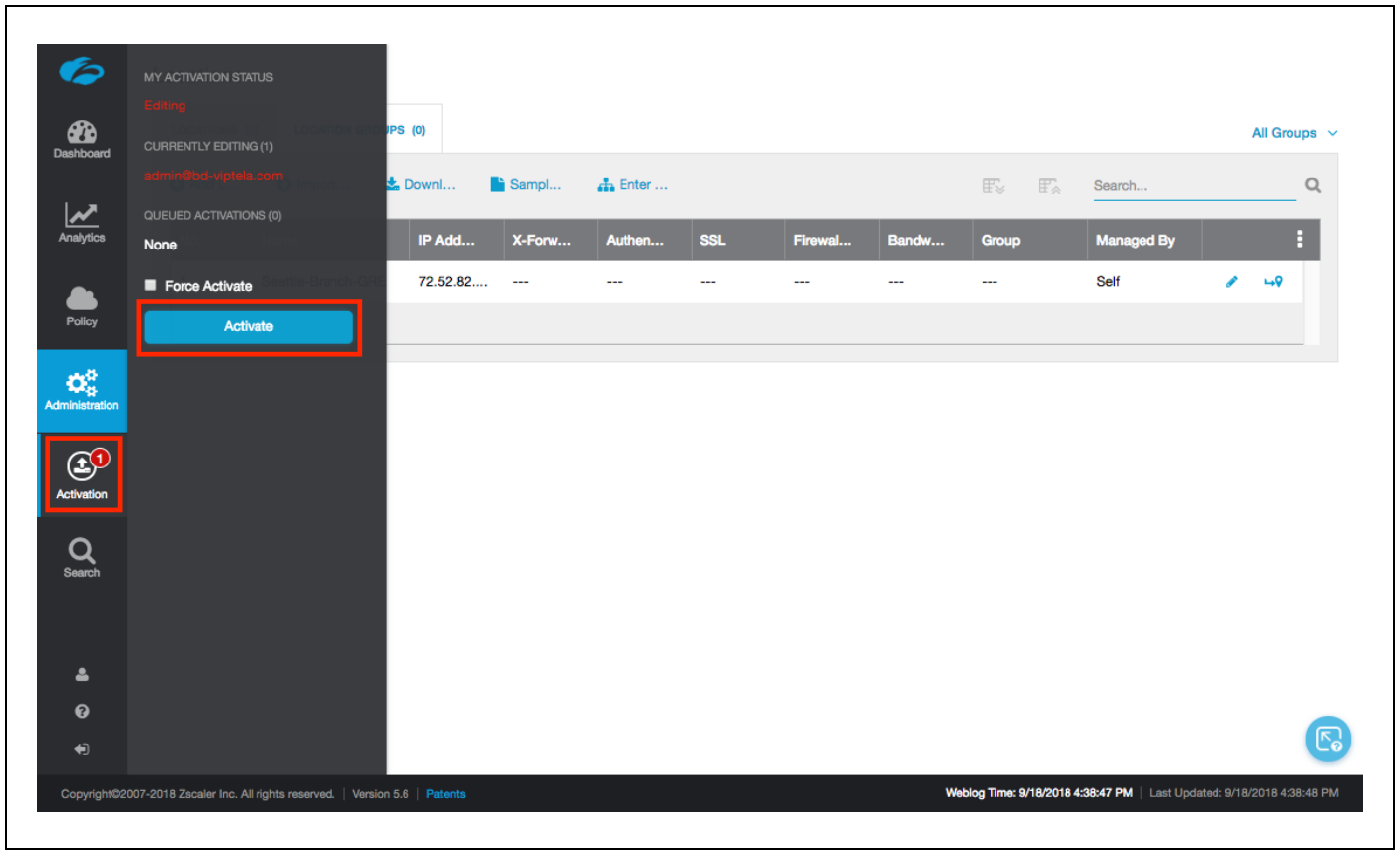


Figure 18: Activate Changes

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.

2.4.2 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.

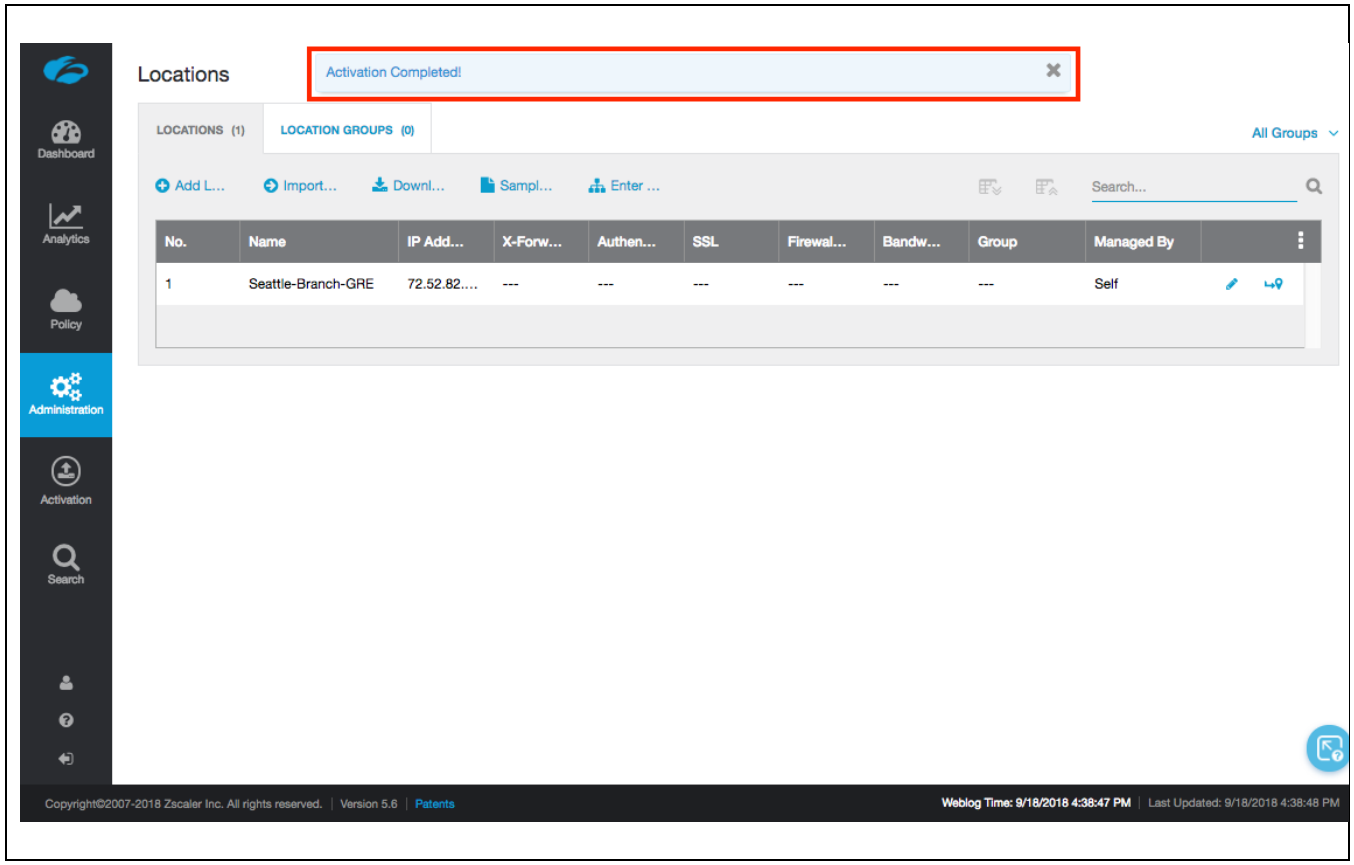


Figure 19: Activation Confirmation

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

3 Configuring Cisco SD-WAN

Cisco SD-WAN Edge routers may be configured through a direct serial connection or SSH. Often these methods are used to get a basic configuration onto a device to then lifecycle manage it using Cisco SD-WAN vManage.

The vManage NMS is a centralized network management system that provides a GUI interface to easily monitor, configure, and maintain all Cisco SD-WAN devices and links in the overlay network. The vManage NMS software runs on a virtual server in the cloud.

3.1 GRE or IPSec tunnel configuration on Cisco SD-WAN Edge router

3.1.1 Log into Cisco SD-WAN vManage

Open a web browser and enter the URL to your vManage instance. For best results, it is recommended to use Chrome browser

Figure 20: Cisco vManage Login

3.2 Configuring GRE Tunnel

Please define Cisco SD-WAN Edge router device template prior to configuring GRE tunnels. Refer to Appendix 7.1 for details about configuring device templates.

3.2.1 Add Feature Template

The GRE tunnel can be configured under vManage's ***Configuration > Templates > Feature Template > VPN Interface GRE*** and attached to the respective device template.

Once there, go to ***Configuration > Templates > Feature*** and click "Add Template" button as shown below.

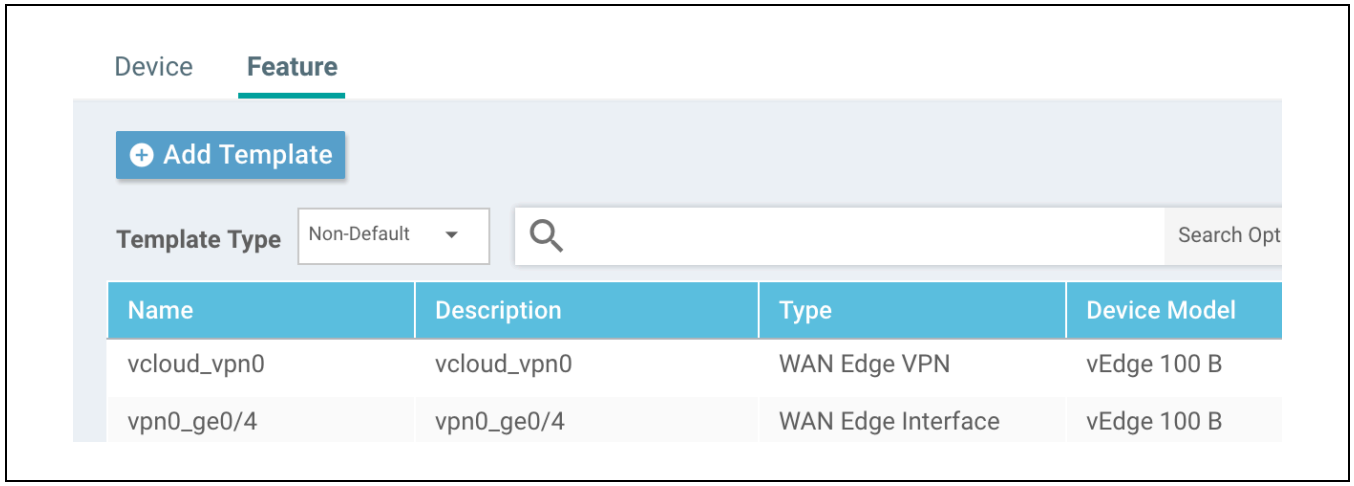


Figure 21: Add Feature Template

3.2.2 Add VPN Interface GRE Feature

Choose the device type on left pane and select “VPN Interface GRE” template under VPN-WAN section as shown below.

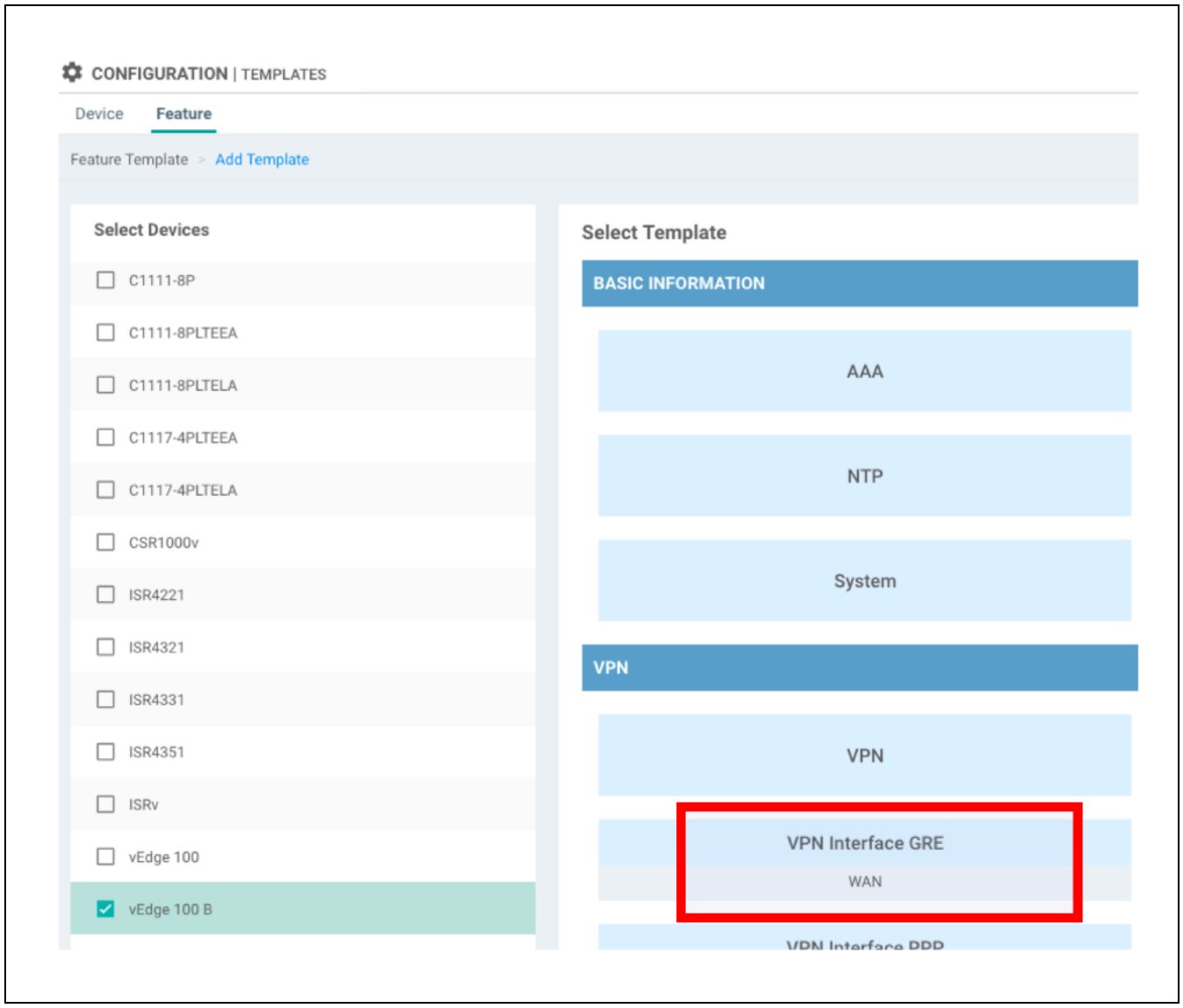


Figure 21: Add VPN Interface GRE Feature

3.2.3 Set GRE Source Interface

- Provide template name and description for the VPN Interface GRE feature template
- Under ***Basic Configuration > Shutdown***, change the attribute type to Global and select “No” radio button. This will unshut the GRE interface.
- Configure ***Interface Name*** as “gre1”. This is the name of the virtual GRE interface on the SD-WAN Edge router connecting to Zscaler.
- Configure the ***Tunnel Source Interface***. This is the physical VPN0 transport side interface connecting SD-WAN Edge router to the wide area network.

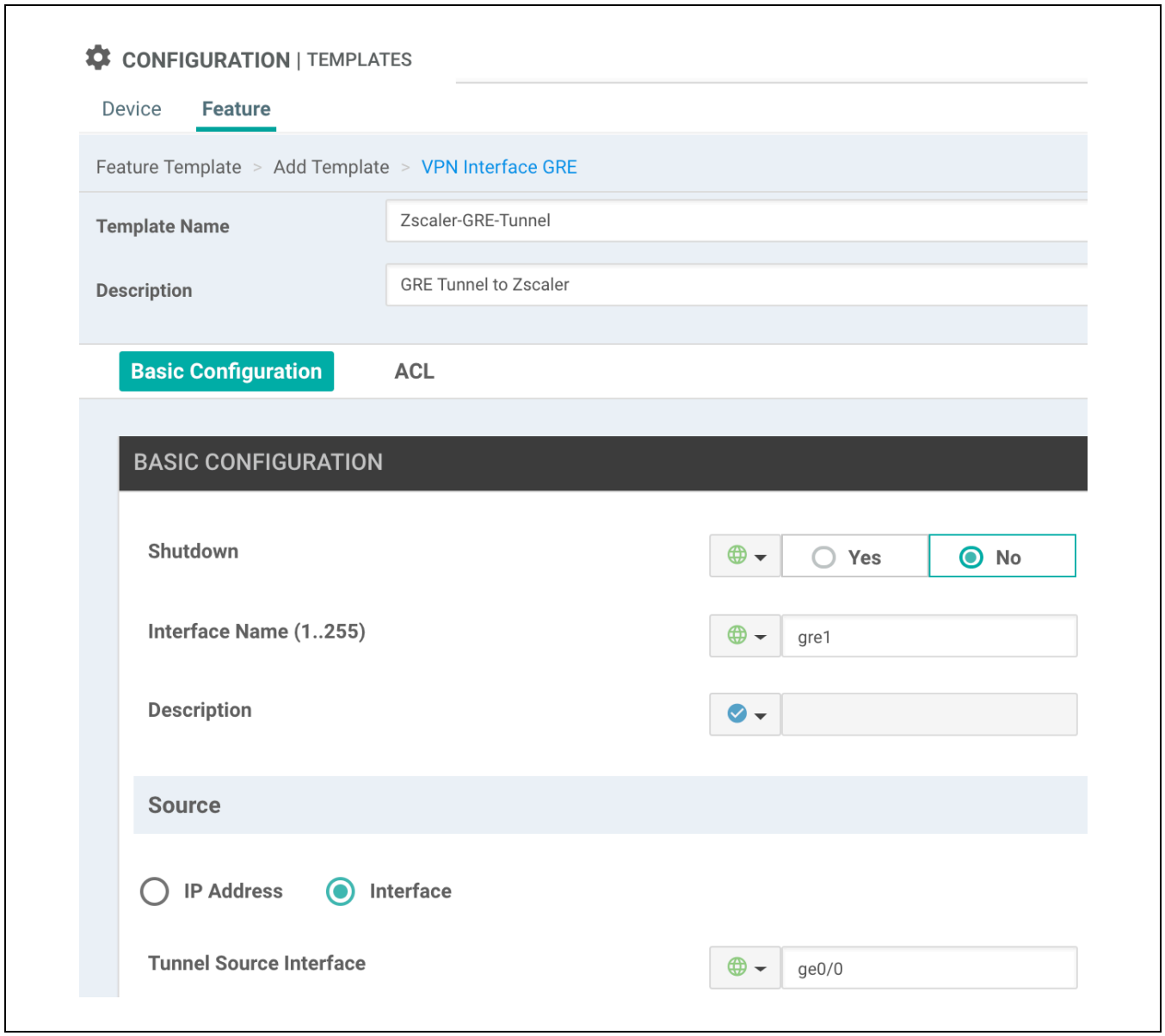


Figure 22: GRE Interface Source Settings

3.2.4 Set GRE Interface Destination

Provide GRE tunnels destination details

- Under ***GRE Destination IP Address*** specify IP address which will be the destination of the GRE tunnel. This is Zscaler ZEN IP address
- Change the ***IPv4 Address*** attribute type to Global and type in the GRE interface IP address. In this case we use "172.17.8.193/30". **Note:** This is for routing purpose and it accepts only /30 address.
- Change the ***IP MTU*** attribute type to Global and type in 1476
- Change the ***TCP MSS*** attribute type to Global and type in 1432

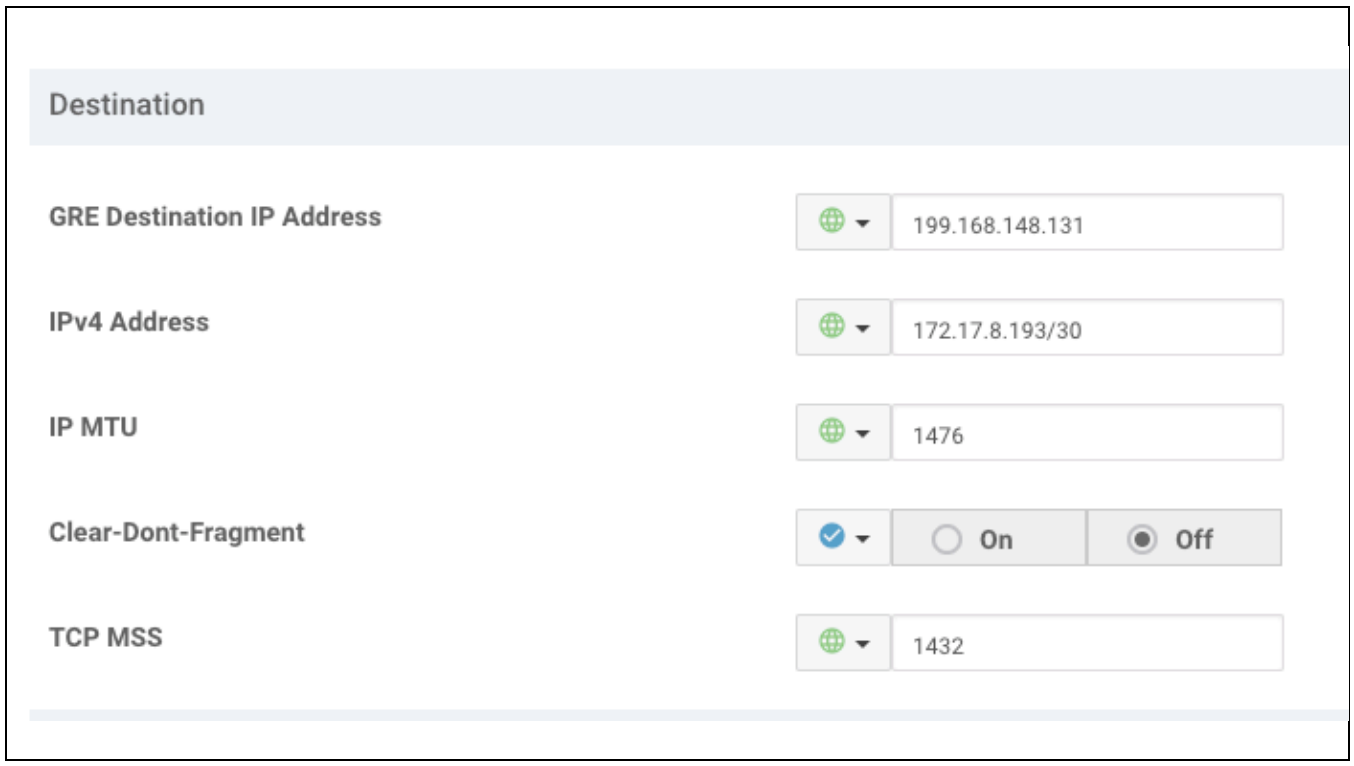


Figure 23: GRE Interface Destination Settings

3.2.5 Enable GRE Keepalives

GRE Keep Alive should be configured for an **Interval** of 10 and **Retries** of 3.

Note: If SD-WAN Edge router is placed behind device performing Network Address Translation, GRE keepalives need to be disabled to allow GRE tunnel to come up.
You can disable GRE Keep Alives by configuring the **Interval** to 0 and **Retries** to 0, as shown in Figure 22.

Figure 22: Disable GRE Keepalives

3.2.6 Add GRE Interface Feature Template

Add the GRE Interface feature template to the device template. Navigate to ***Configuration > Templates > Device*** and choose the device template for the SD-WAN Edge router connecting to Zscaler. In this example, we are going to use the device template called “Edge-A”, as shown below

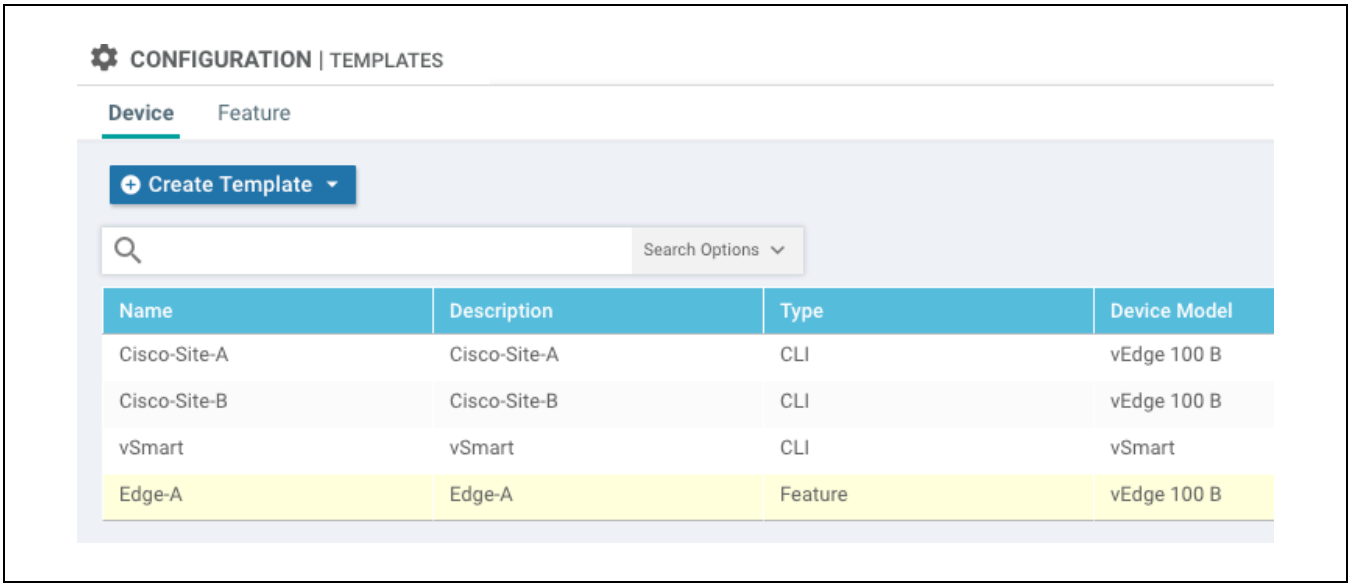


Figure 23: Device Templates List

3.2.7 Edit Device Template

Next, right-click on the three dots at right-side and choose “Edit “option from the drop-down menu, as shown in Figure 24.

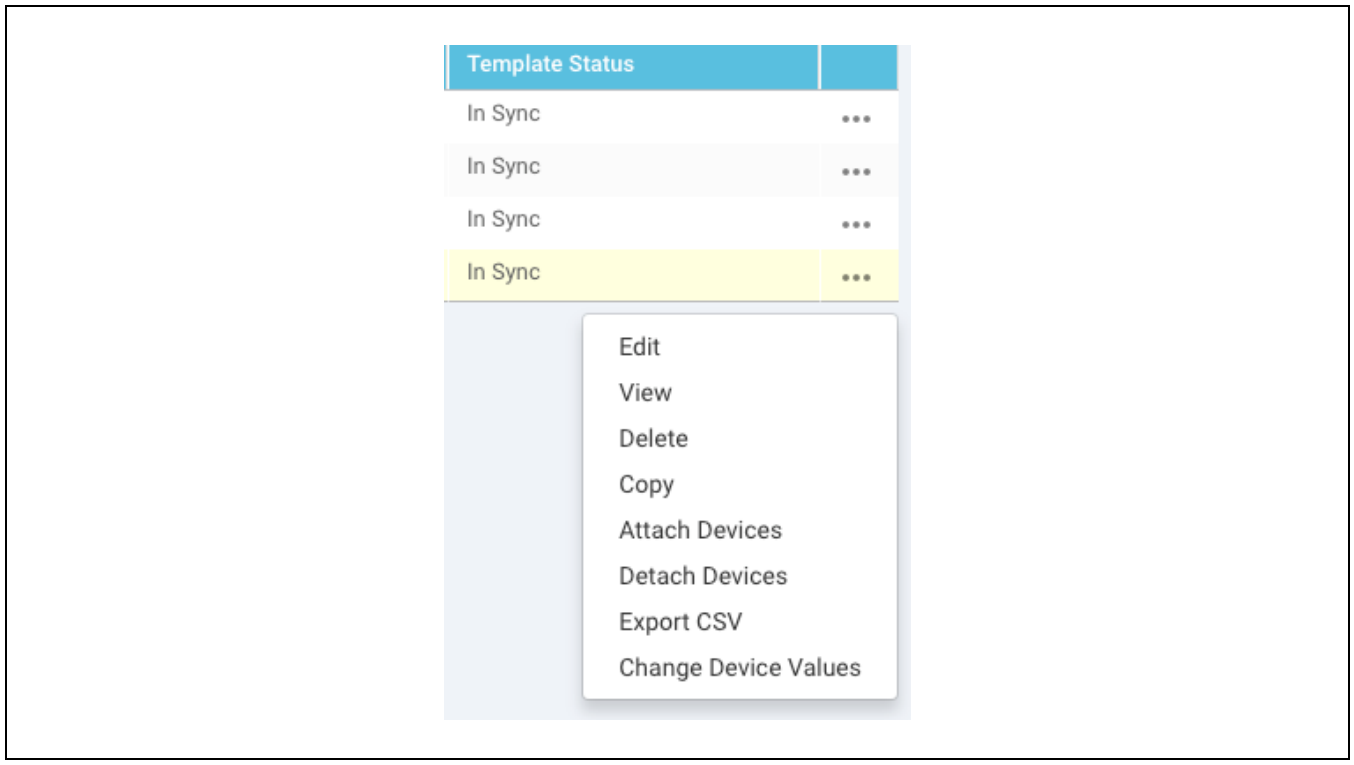


Figure 24: Edit Device Template

3.2.8 VPN-0 Template

Click on the (+) next to **VPN Interface GRE** under ***Transport and Management VPN*** section

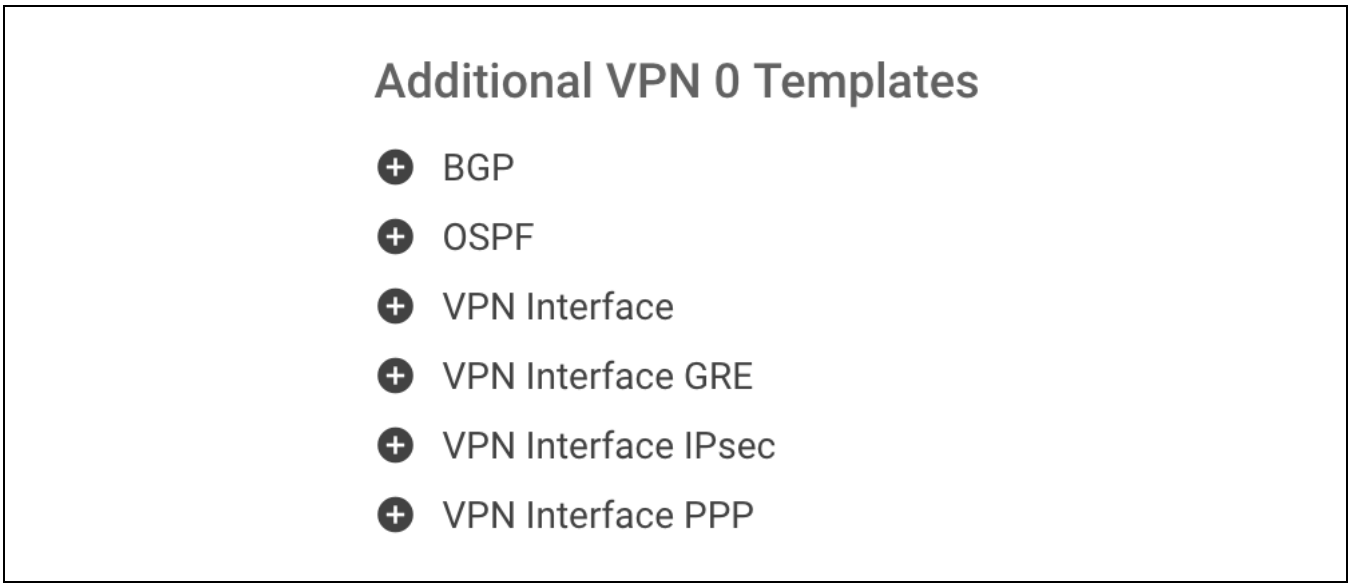


Figure 25: VPN0 Templates

3.2.9 Assign GRE Interface Feature to Device Template

VPN Interface GRE will be added to the device template. Click on the drop-down menu for the VPN Interface GRE and choose the VPN Interface GRE feature template you had created in the prior steps.

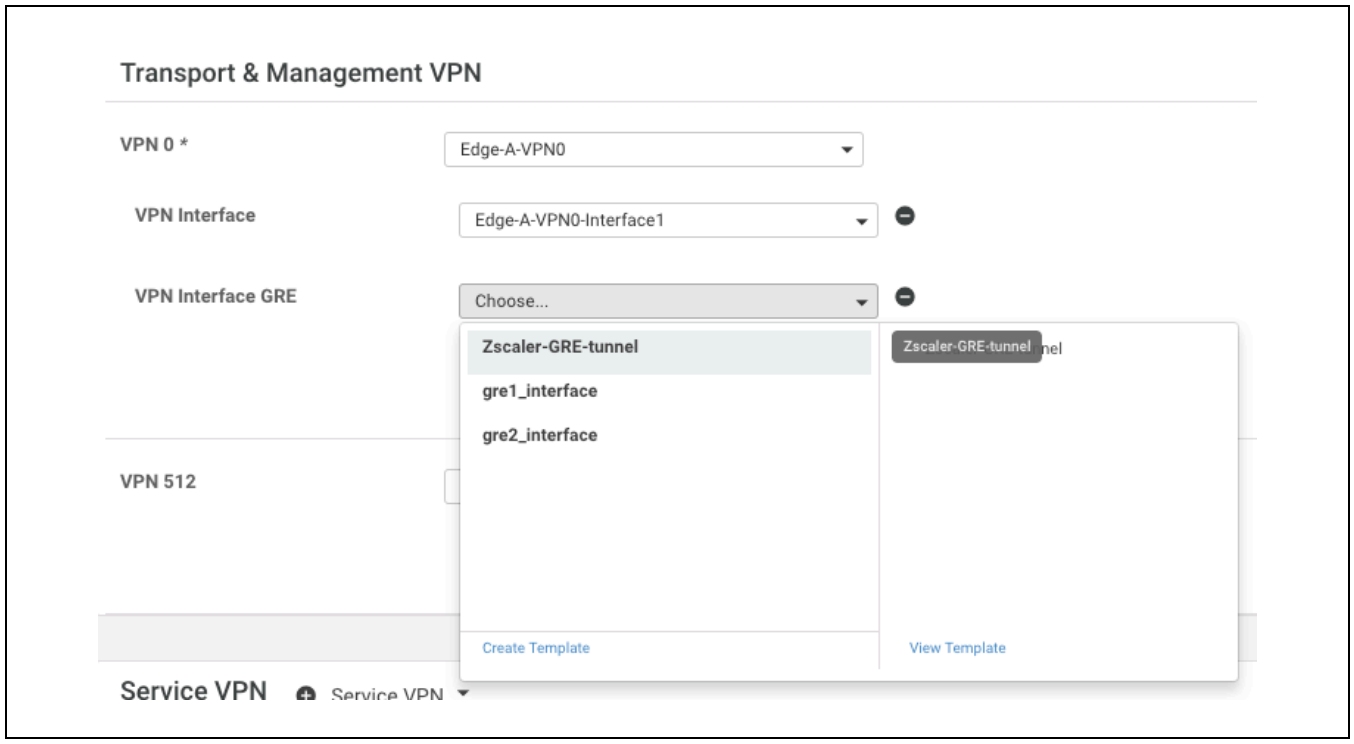


Figure 26: Assign GRE Interface Feature to Device Template

3.2.10 Verify Configuration Update

Click on Update button at the bottom of the page. If device template was previously attached to the SD-WAN Edge router, update performed in Figure 27 will result in device configuration push from vManage to the SD-WAN Edge router. Please make sure to complete the process and allow configuration change to take place.

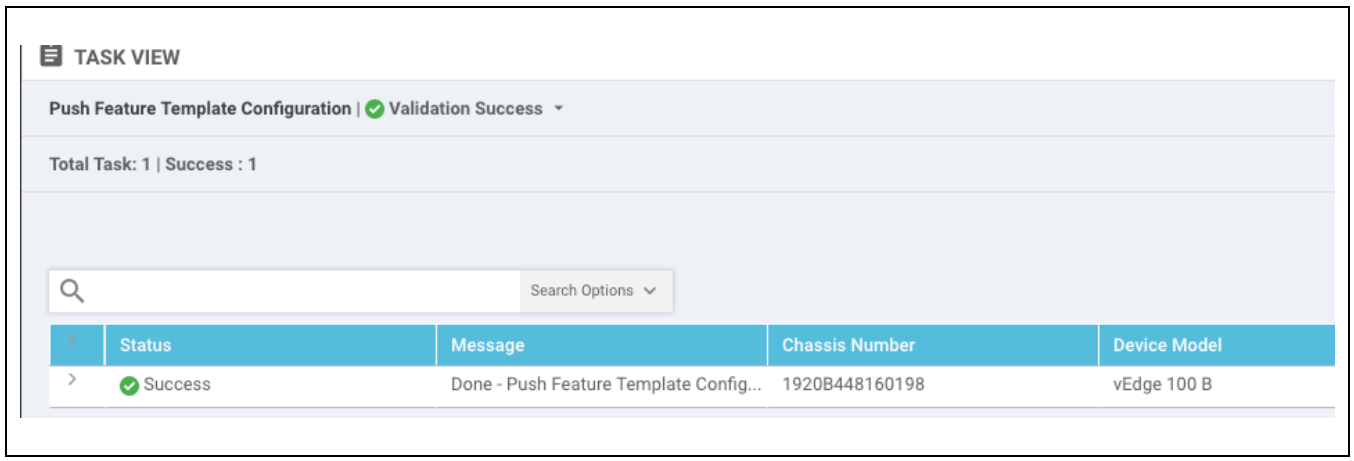
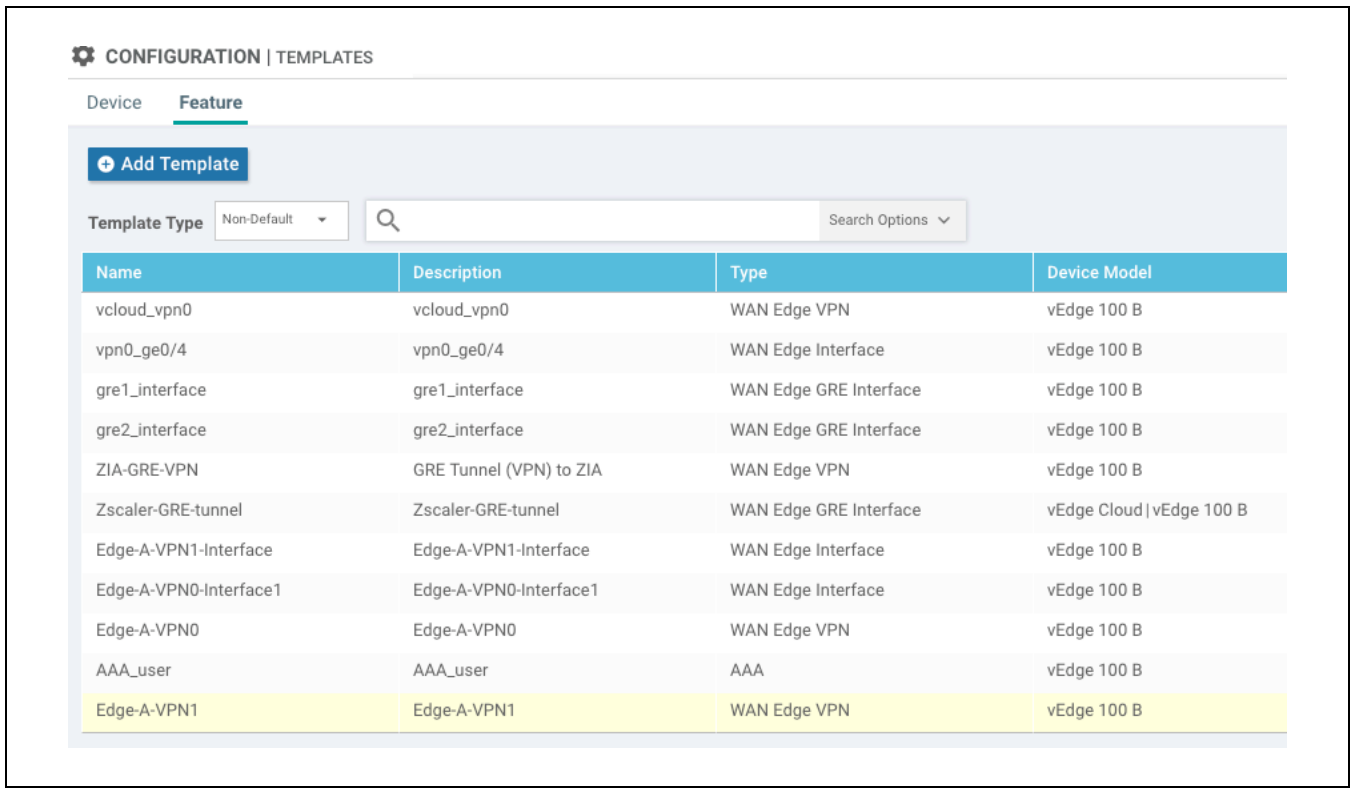


Figure 27: Successful Configuration Update

3.2.11 Feature Template

Add static GRE route under Service VPN (LAN) to direct user traffic to Zscaler through the GRE tunnel. Go to ***Configuration > Templates > Feature*** and choose the Service VPN template used for the SD-WAN Edge router connecting to Zscaler. In this example, we are using "Edge-A-VPN1" as Service VPN feature template.



Name	Description	Type	Device Model
vcloud_vpn0	vcloud_vpn0	WAN Edge VPN	vEdge 100 B
vpn0_ge0/4	vpn0_ge0/4	WAN Edge Interface	vEdge 100 B
gre1_interface	gre1_interface	WAN Edge GRE Interface	vEdge 100 B
gre2_interface	gre2_interface	WAN Edge GRE Interface	vEdge 100 B
ZIA-GRE-VPN	GRE Tunnel (VPN) to ZIA	WAN Edge VPN	vEdge 100 B
Zscaler-GRE-tunnel	Zscaler-GRE-tunnel	WAN Edge GRE Interface	vEdge Cloud | vEdge 100 B
Edge-A-VPN1-Interface	Edge-A-VPN1-Interface	WAN Edge Interface	vEdge 100 B
Edge-A-VPN0-Interface1	Edge-A-VPN0-Interface1	WAN Edge Interface	vEdge 100 B
Edge-A-VPN0	Edge-A-VPN0	WAN Edge VPN	vEdge 100 B
AAA_user	AAA_user	AAA	vEdge 100 B
Edge-A-VPN1	Edge-A-VPN1	WAN Edge VPN	vEdge 100 B

Figure 28: Feature Templates List

3.2.12 Add New GRE Route

Right-click on the three dots shown at the right corner of the selected Service VPN template and click Edit. Navigate to "**GRE Route**" section and click-on "**New GRE Route**" button.

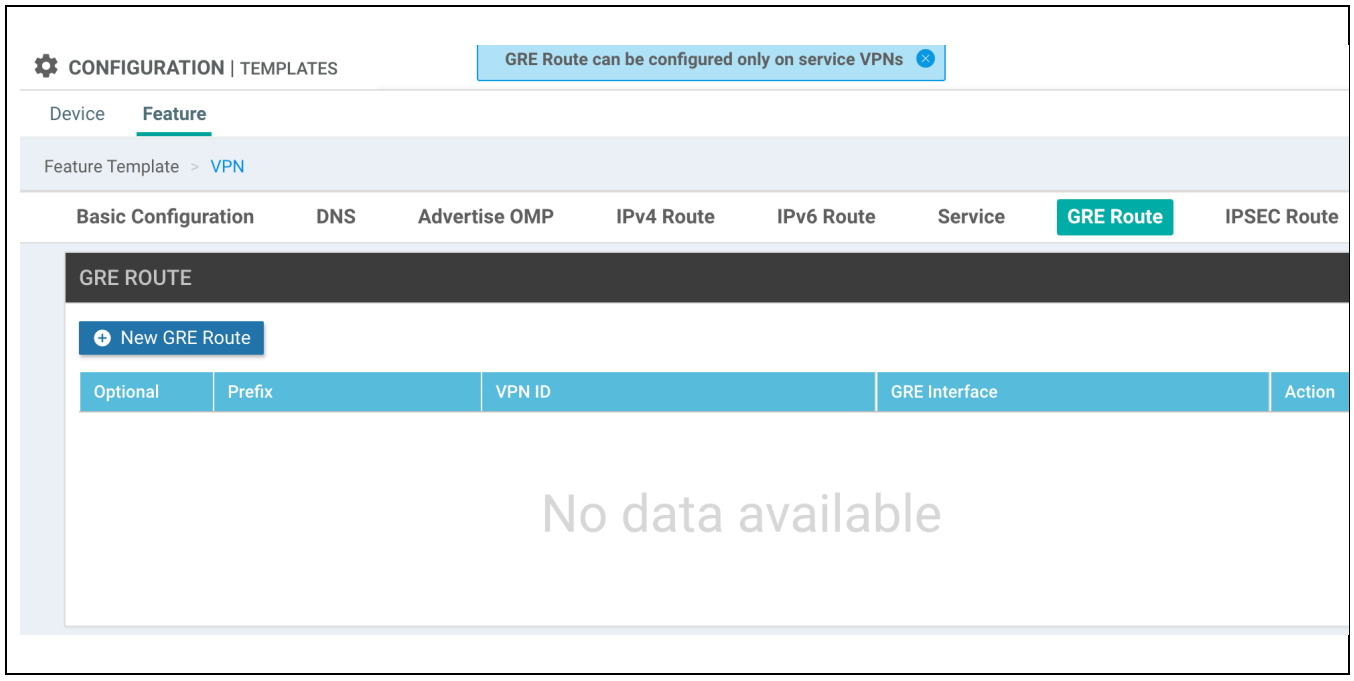


Figure 29: Add a New GRE route

3.2.13 Configure Routing towards GRE Tunnel

Configure the ***Prefix*** as 0.0.0.0/0 if you want to route all user traffic in a given service side VPN to Zscaler. Under ***GRE Interface***, change the attribute type to Global and type “gre1, gre2”. This selects gre1 as the primary tunnel to egress towards Zscaler and gre2 as the backup tunnel.

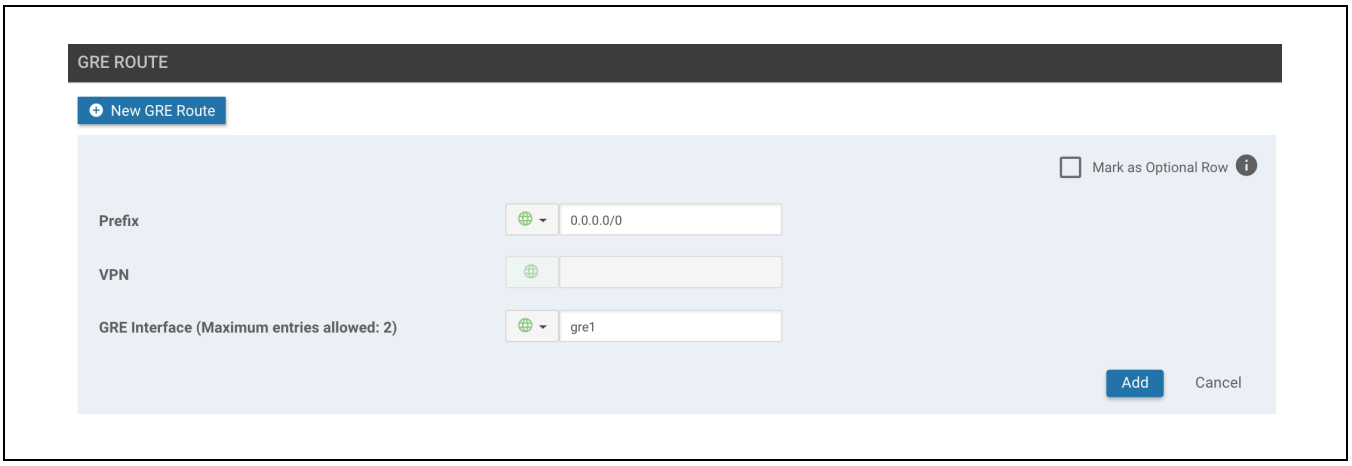


Figure 30: Provide destination prefix and GRE tunnel interface name

3.2.14 Verify GRE Route is Added

Click “Add” button to add IPSec route to the service side feature template

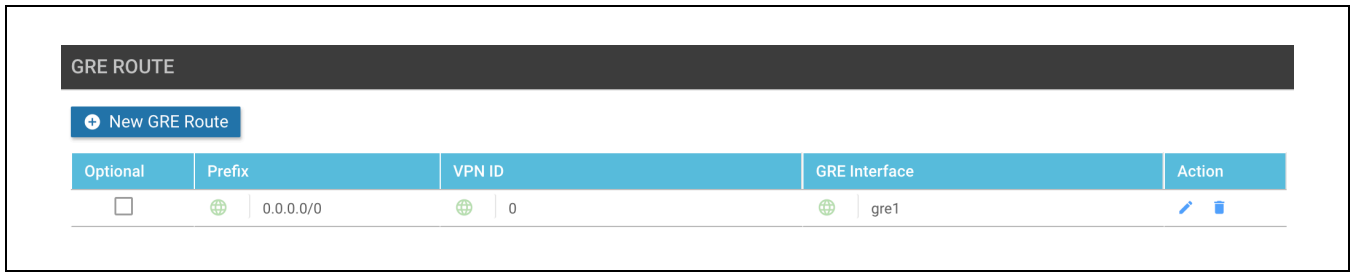


Figure 31: Check the added GRE route

Next, click on “Update” button at the bottom of the page. This will result in configuration push from vManage to the SD-WAN Edge router. Please make sure to complete the process and allow configuration change to take place.

3.2.15 Verify Configuration Update

Once completed, you should see “Success”, as shown in Figure 32.

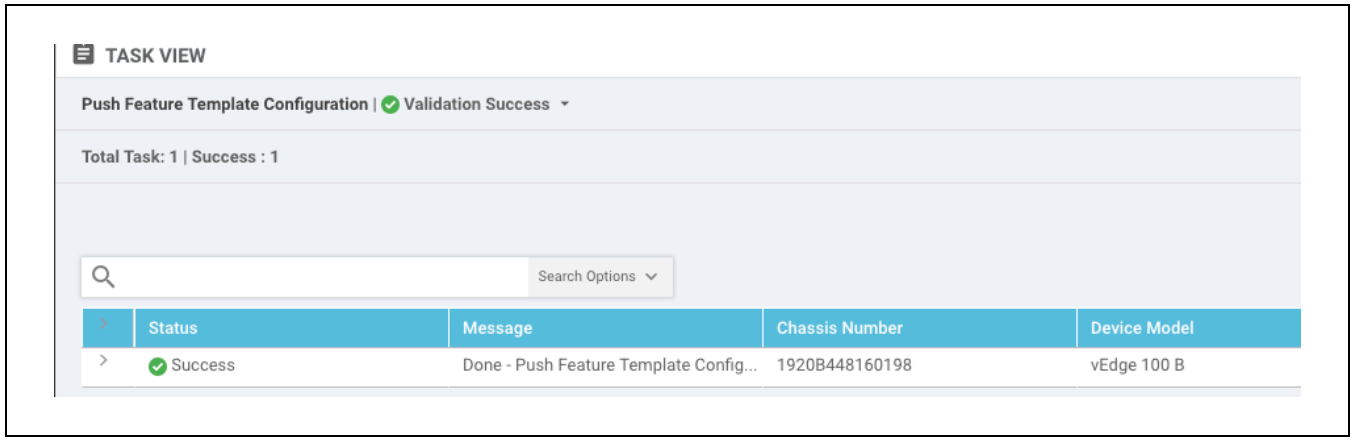


Figure 32: Successful Configuration Update

3.3 Configuring IPsec Tunnel

Note: Please define Cisco SD-WAN Edge router device template prior to configuring IPSec tunnels. Refer to Appendix 7.1 for details about configuring device templates.

3.3.1 View Feature Template List

The IKE based IPSec tunnel can be configured under vManage's ***Configuration > Templates > Feature Template > VPN Interface IPSec*** and attached to the respective device template.

Go to ***Configuration > Templates > Feature*** and click "Add Template" button as shown below.

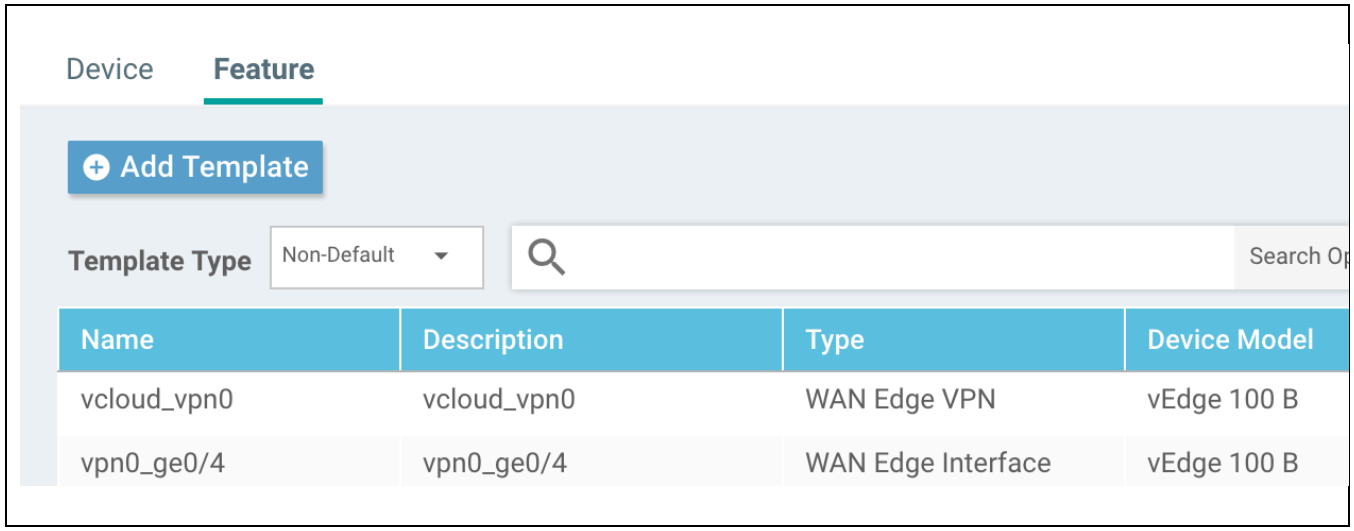


Figure 33: Feature Templates List

3.3.2 Select IPsec Tunnel to Zscaler

Choose the device type on left pane and select “VPN Interface IPSec WAN” template under VPN section as shown below.

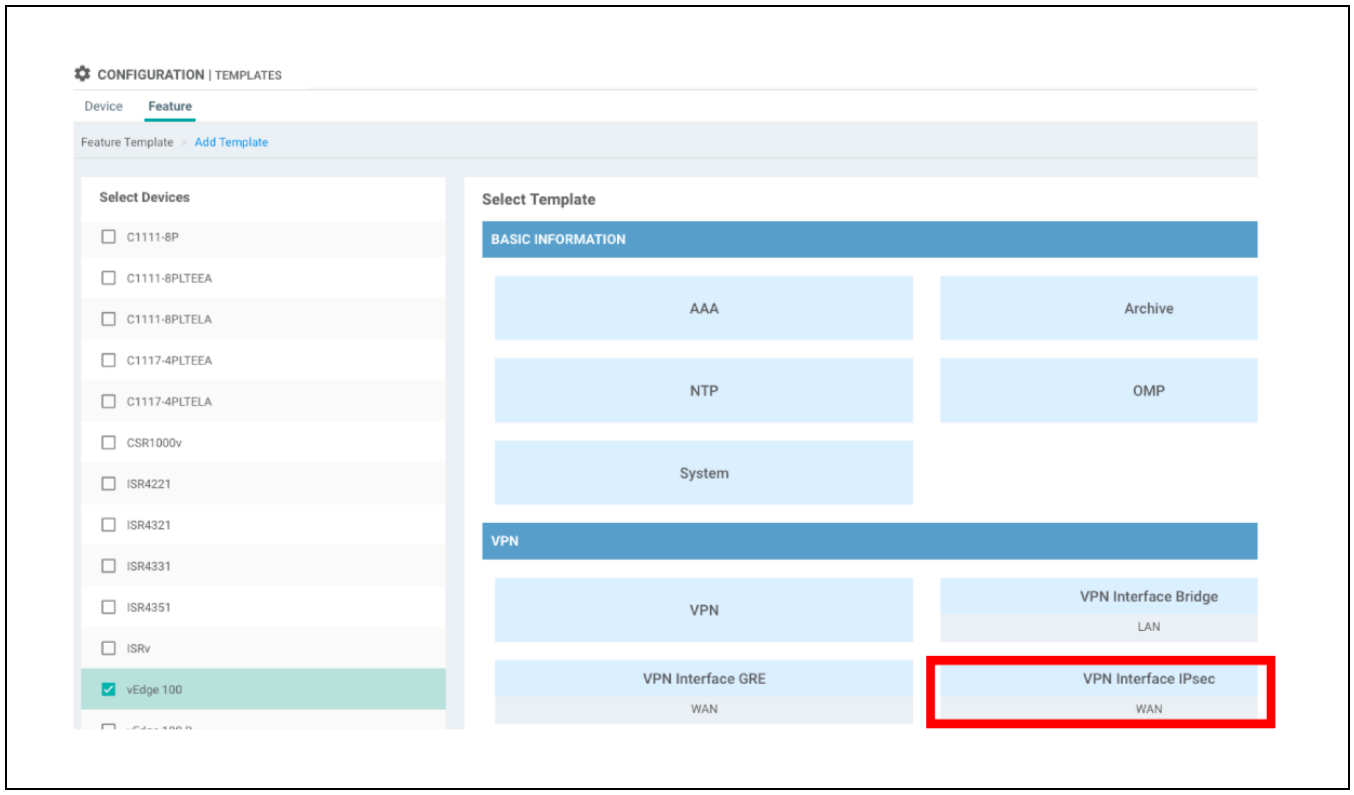


Figure 34: Select “VPN Interface IPSec” for IPSec tunnel to Zscaler

3.3.3 Configure IPsec Tunnel Source and Destination

- Provide template name and description for the VPN Interface IPSec feature template
- Under ***Basic Configuration > Shutdown***, change the attribute type to Global and select “No” radio button. This will unshut the IPSec interface.
- Configure ***Interface Name*** as “ipsec1”. This is the name of the virtual IPSec interface on the SD-WAN Edge router connecting to Zscaler ZEN.
- Change the ***IPv4 Address*** attribute type to Global and type in the IPSec tunnel interface IP address. In this case we use “10.100.200.1/30”. **Note**: This is for routing purpose and it accepts only /30 address.
- Configure the ***IPSec Source Interface*** as “ge0/0”. This is the physical VPN0 transport side interface connecting SD-WAN Edge router to the wide area network. Refer to Section 3.1 for more details.
- Configure ***IPSec Destination IP Address***. This is Zscaler ZEN IP address where IPSec tunnel is terminated.

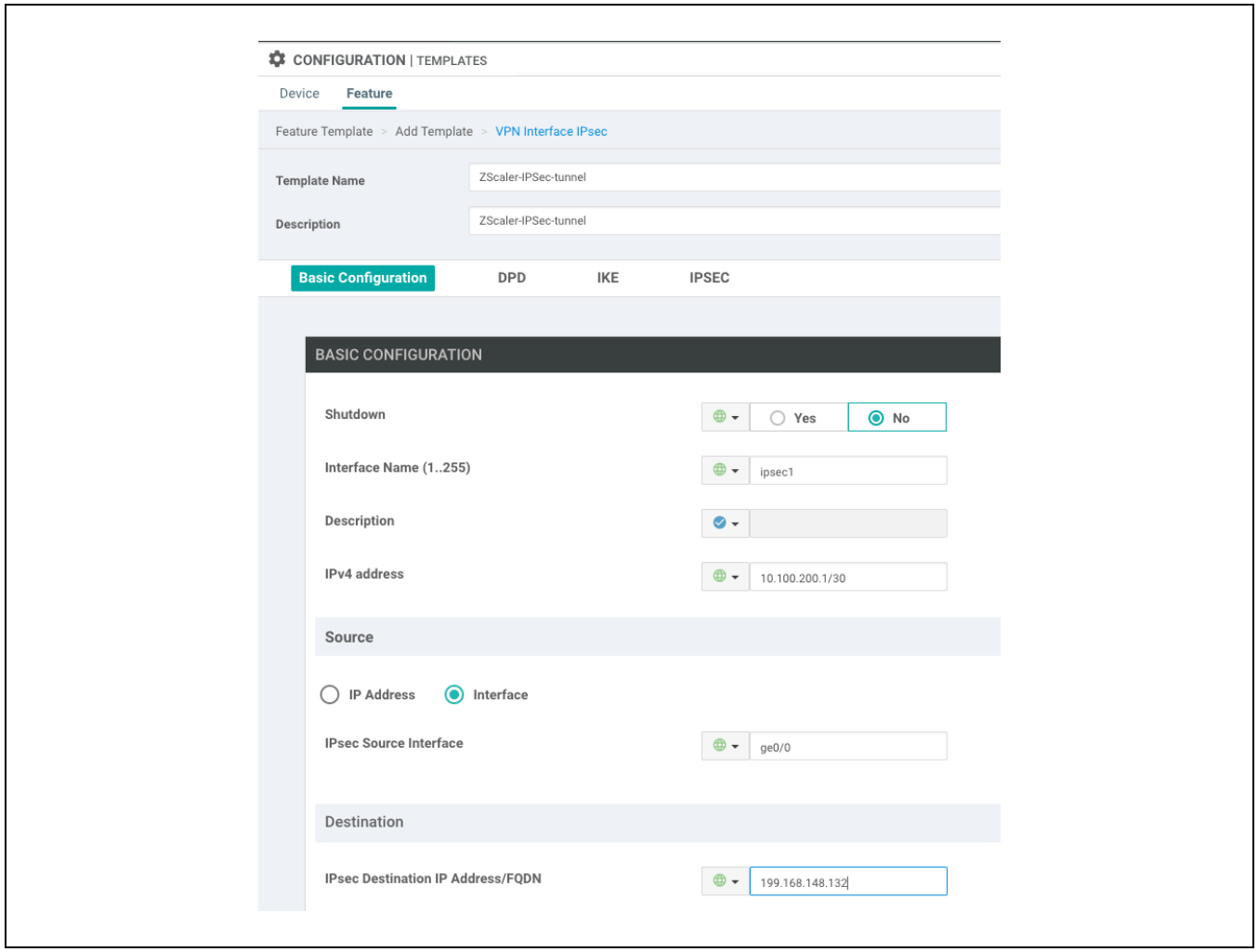


Figure 35: Configure IPSec Source & Destination

3.3.4 Configure Dead Peer Detection

Configure the Dead Peer Detection values. You can keep the defaults.

3.3.5 Configure IKE Parameters

Configure IKE parameters:

- Under ***IKE Version***, change the attribute type to Global and type “2”
- Under ***IKE Diffie-Hellman Group***, change the attribute type to Global and choose “2 1024-bit modulus”
- Under ***Preshared Key***, change the attribute type to Global and type the preshared key value. Preshared key value must match between SD-WAN Edge router and ZScaler ZEN for IPSec tunnel to successfully come up.
- Under ***IKE ID for Local Endpoint***, change the attribute type to Global and type the local ID value. Local ID value configured on SD-WAN Edge router must match Remote ID value configured on ZScaler ZEN for IPSec tunnel to successfully come up.
- Under ***IKE ID for Remote Endpoint***, change the attribute type to Global and type the remote ID value. Remote ID value configured on SD-WAN Edge router must match Local ID value configured on ZScaler ZEN for IPSec tunnel to successfully come up.

Note: Refer to Section 2.3.3 for configuring preshared key, local ID and remote ID in ZScaler portal

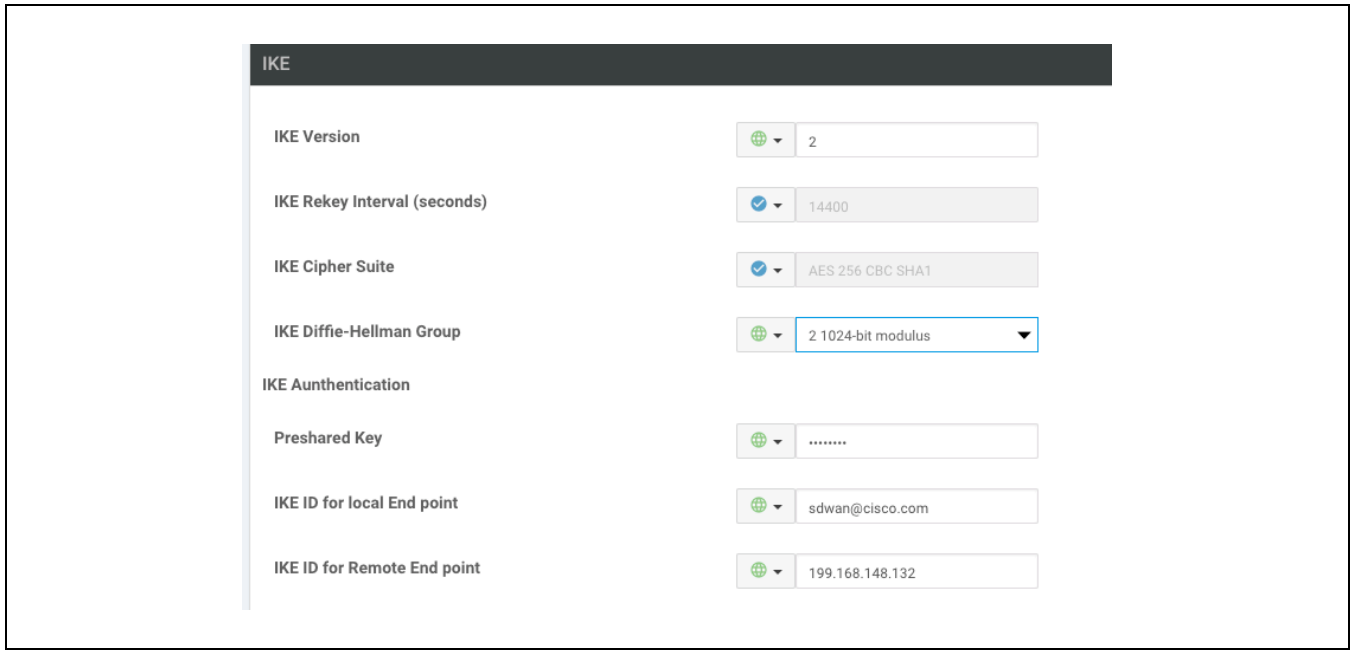


Figure 36: Configure IKE parameters

3.3.6 Configure IPsec Cipher-suite

Configure IPSec parameters:

- Under ***IPsec Cipher Suite***, change the attribute type to Global and choose “Null SHA1”
- Under ***Perfect Forwarding Secrecy***, change the attribute type to Global and choose “Group-2 1024-bit modulus”

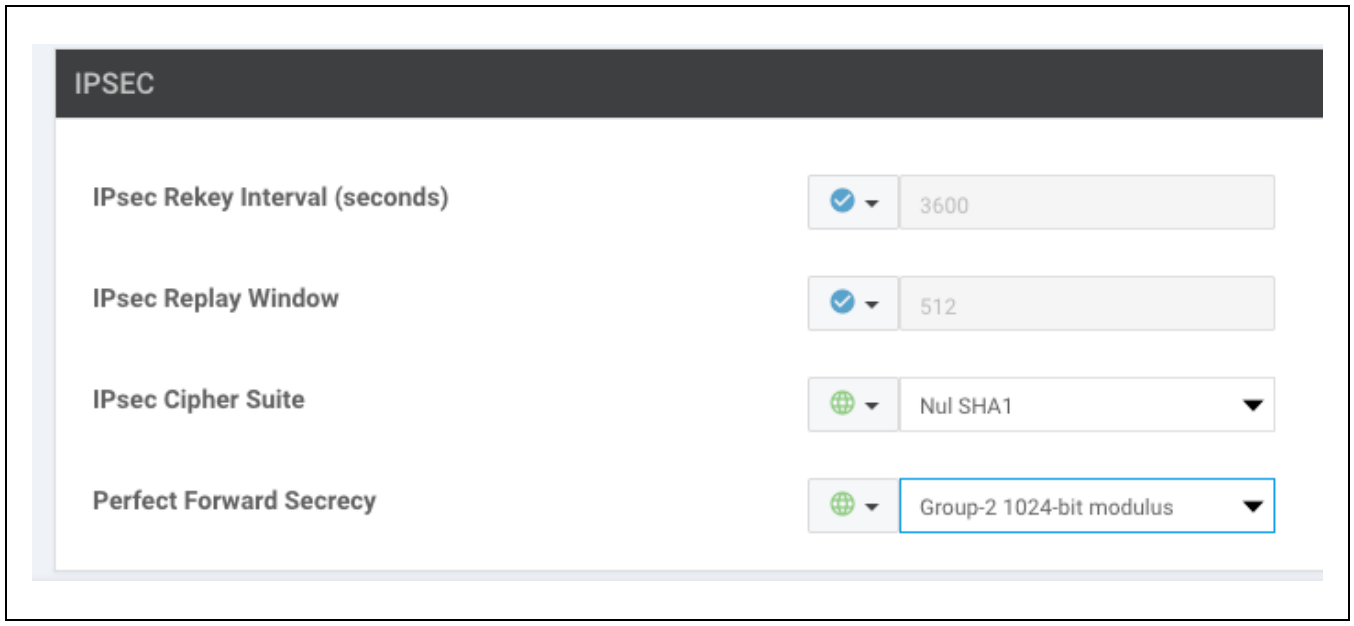


Figure 37: Configure IPSec Cipher-suite

3.3.7 View Device Template List

Click on Save button to save the VPN IPSec interface template. Once completed, add the VPN IPSec interface template under device template. Navigate to ***Configuration > Templates > Device*** and choose the device template for the SD-WAN Edge router connecting to ZScaler. In this example we are using the device template called “Edge-A”, as shown below

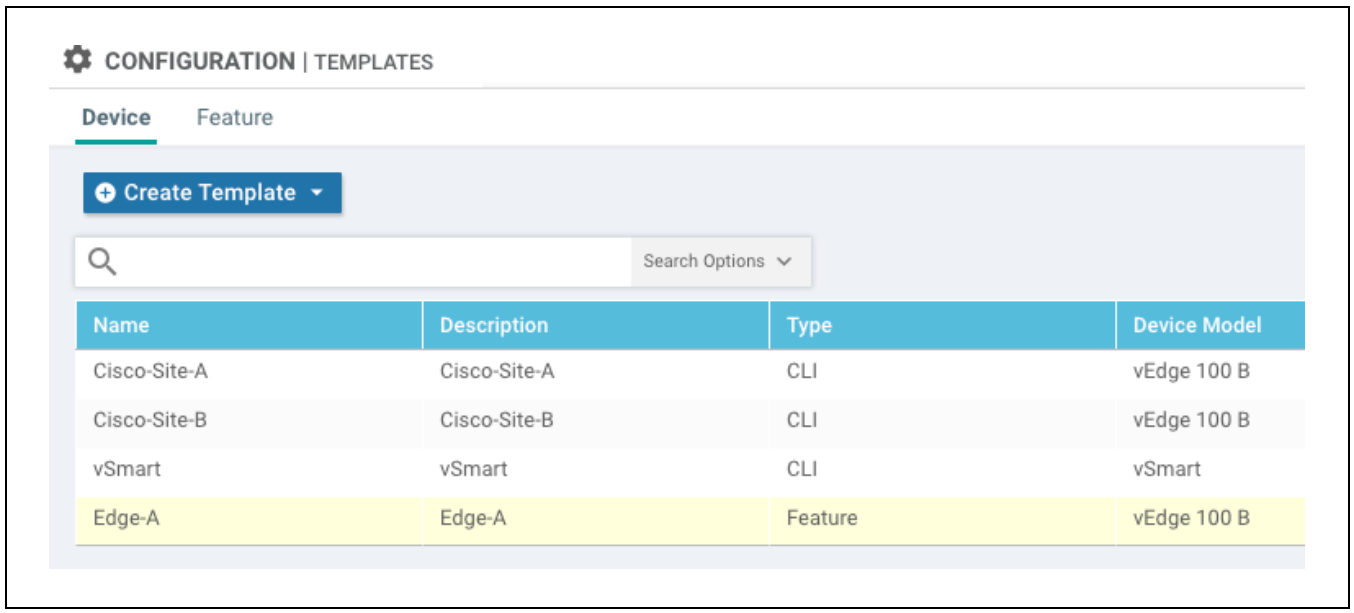


Figure 38: Device Templates List

3.3.8 Edit the Device Template

Right-click on the three dots at right-side and choose Edit option from the drop-down menu.

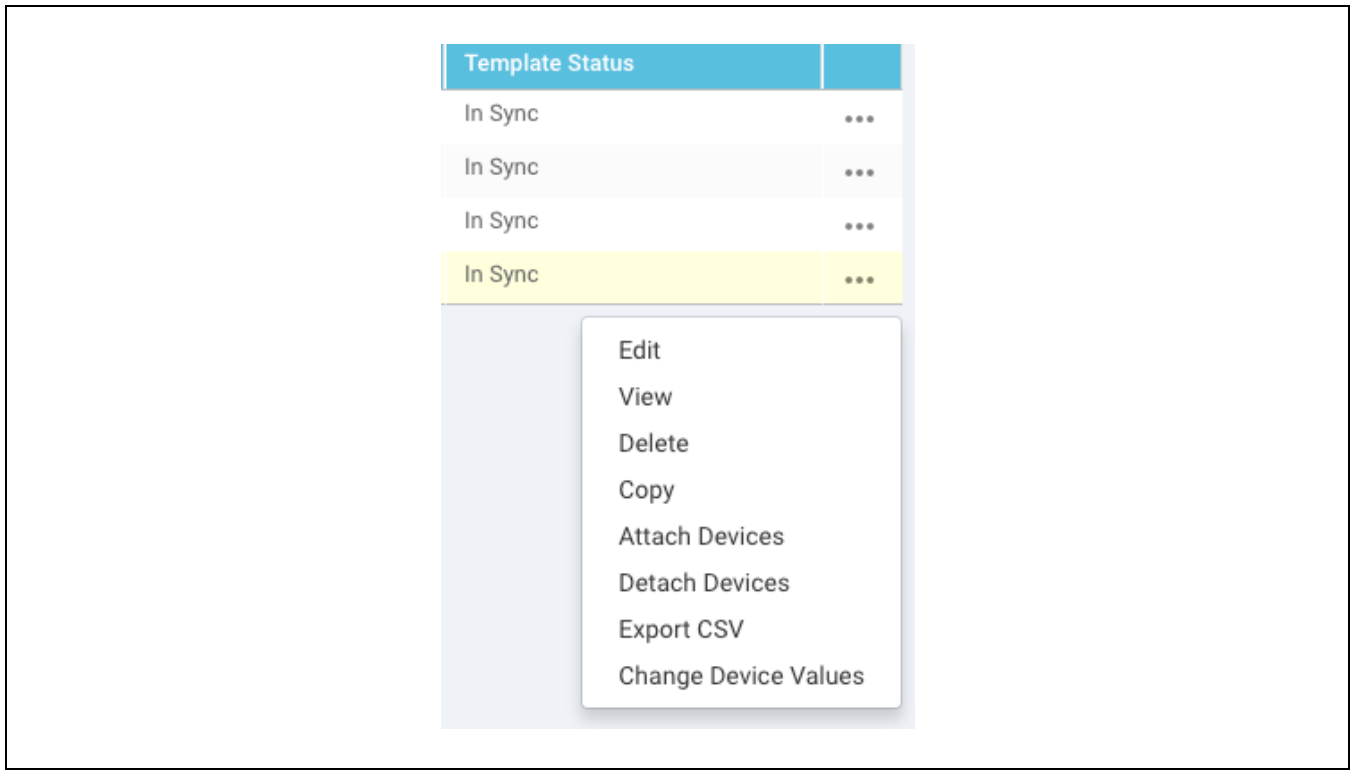


Figure 39: Edit the device template

3.3.9 Add VPN Interface IPsec

Once the device template is opened in Edit mode, Click on the (+) next to VPN Interface IPsec under ***Transport and Management VPN*** section

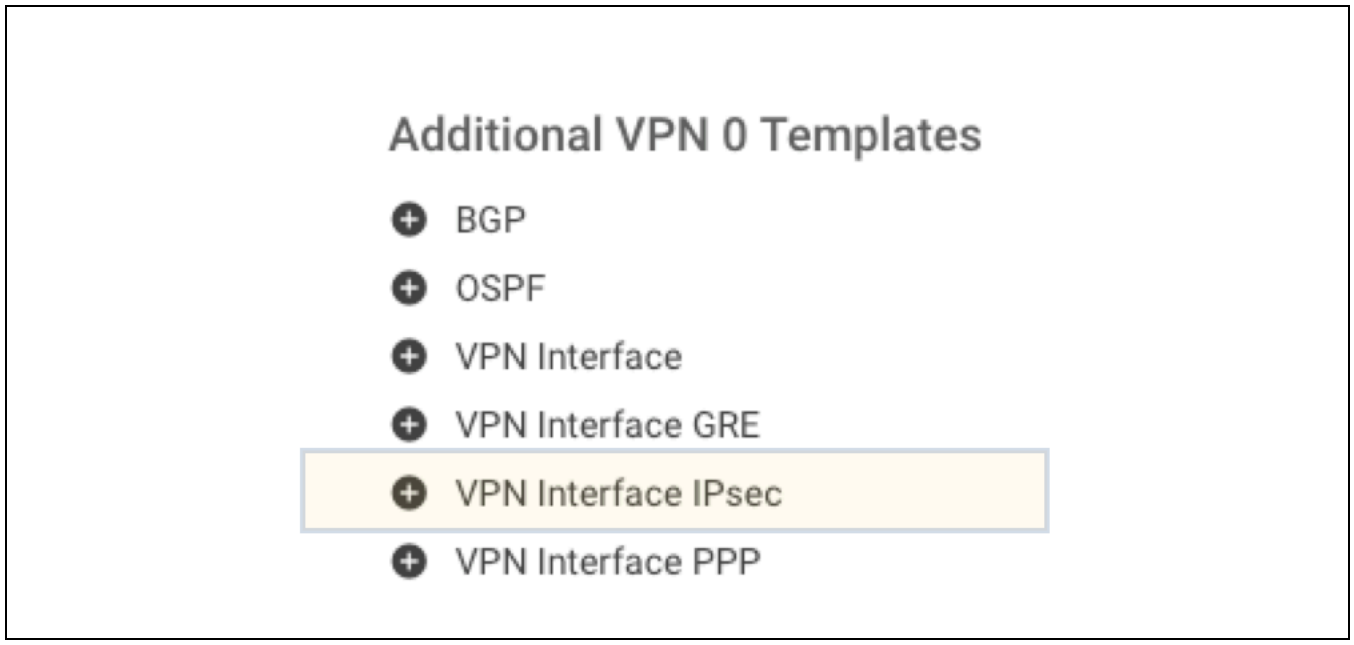


Figure 40: Add VPN Interface IPSec

3.3.10 Select IPsec Template

VPN Interface IPSec will be added to the device template. Click on the drop-down menu for the VPN Interface IPSec and choose the VPN Interface IPSec feature template you had created in the prior steps.

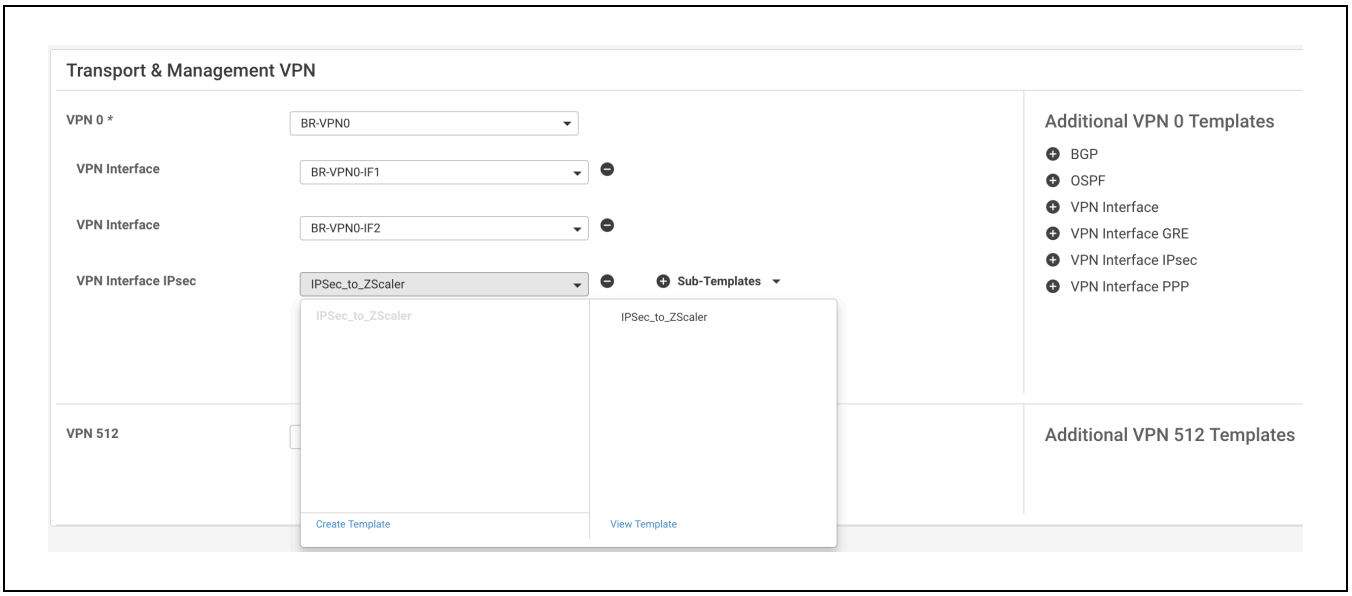


Figure 41: Select the IPSec template

3.3.11 Update and Verify Configuration Update

Click on Update button at the bottom of the page. Note: If device template was previously attached to the SD-WAN Edge router, update performed in prior steps will result in device configuration push from vManage to the SD-WAN Edge router. Please make sure to complete the process and allow configuration change to take place.

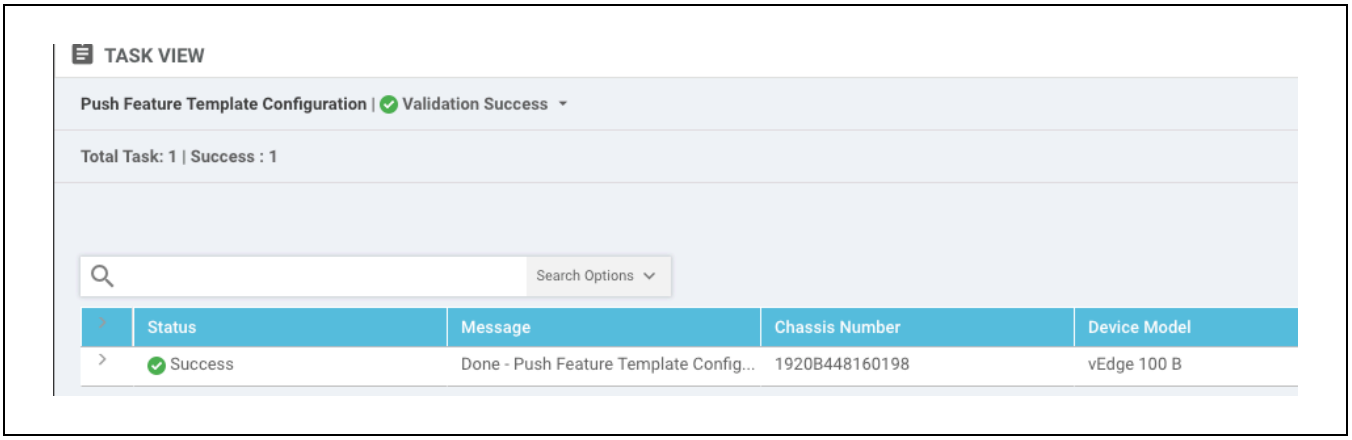


Figure 42: Successful configuration update

3.3.12 Add Static Route

Add static IPSec route under Service VPN (LAN) to direct user traffic to Zscaler through the IPSec tunnel. Go to ***Configuration > Templates > Feature*** and choose the Service VPN template used for the SD-WAN Edge router connecting to Zscaler. In this example, we are using “Edge-A-VPN1” as Service VPN feature template.

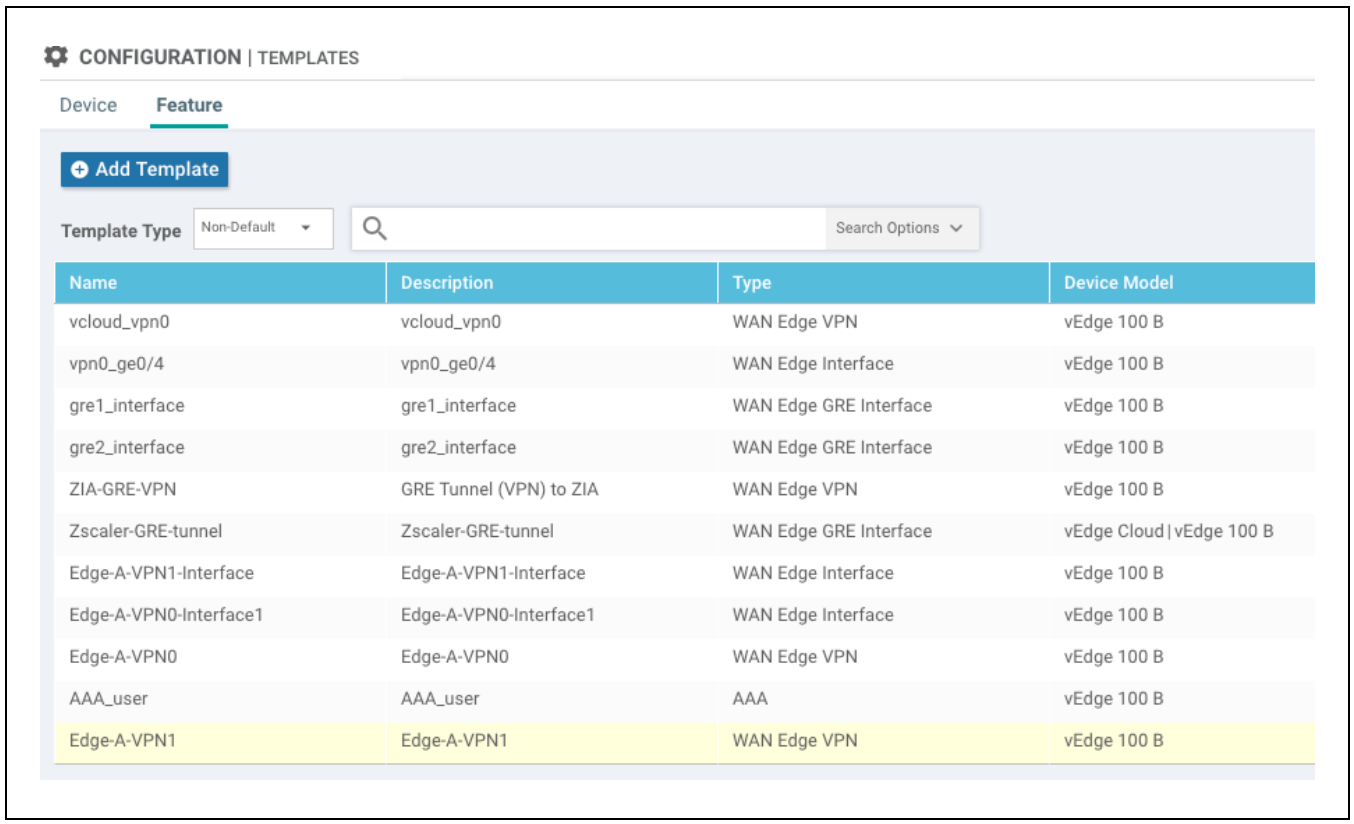


Figure 43: Feature Templates List

3.3.13 Add New IPsec Route

Right-click on the three dots shown at the right corner of the selected Service VPN template and click Edit. Navigate to “IPSec Route” section and click-on “New IPSec Route” button

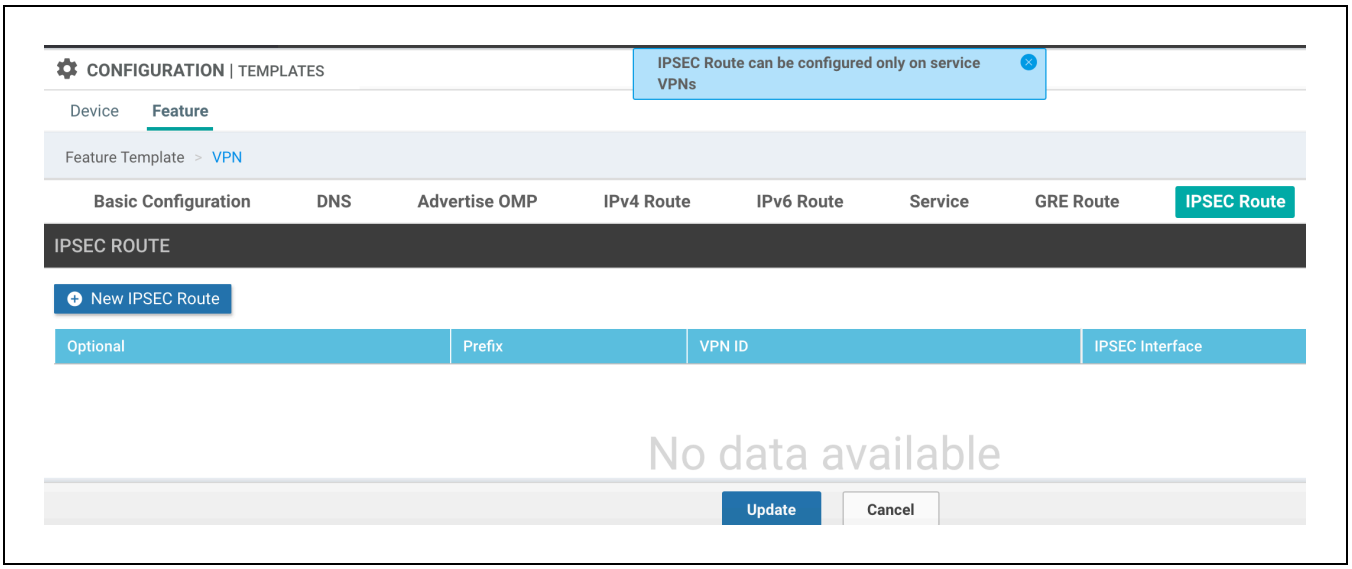


Figure 44: Add New IPSec route

3.3.14 Configure Destination Prefix

Configure the ***Prefix*** as 0.0.0.0/0 if you want to route all user traffic in a given service side VPN to Zscaler. Under ***IPSec Interface***, change the attribute type to Global and type "ipsec1, ipsec2". This selects ipsec1 as the primary tunnel to egress towards Zscaler and ipsec2 as the backup tunnel.

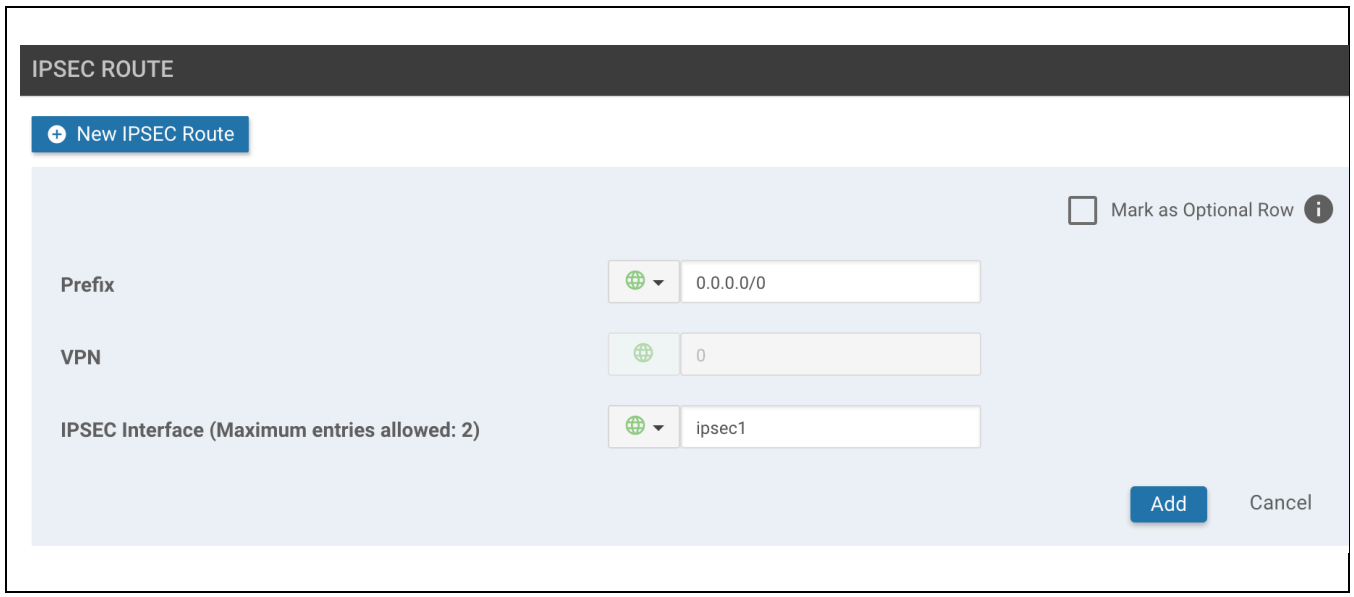


Figure 45: Provide destination prefix and IPSec tunnel interface name

Click "Add" button to add IPSec route to the service side feature template

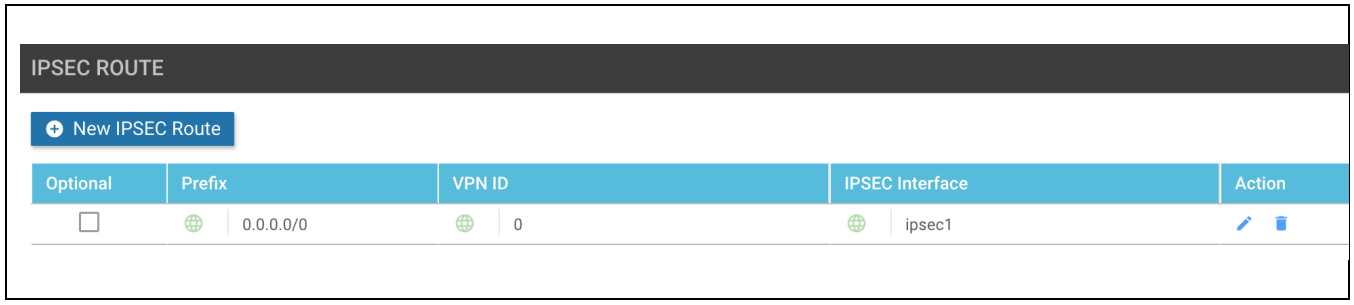


Figure 46: Check the added IPSec route

3.3.15 Push Configuration to SD-WAN Edge Router

Finally, click on “Update” button at the bottom of the page. This will result in configuration push from vManage to the SD-WAN Edge router. Please make sure to complete the process and allow configuration change to take place.

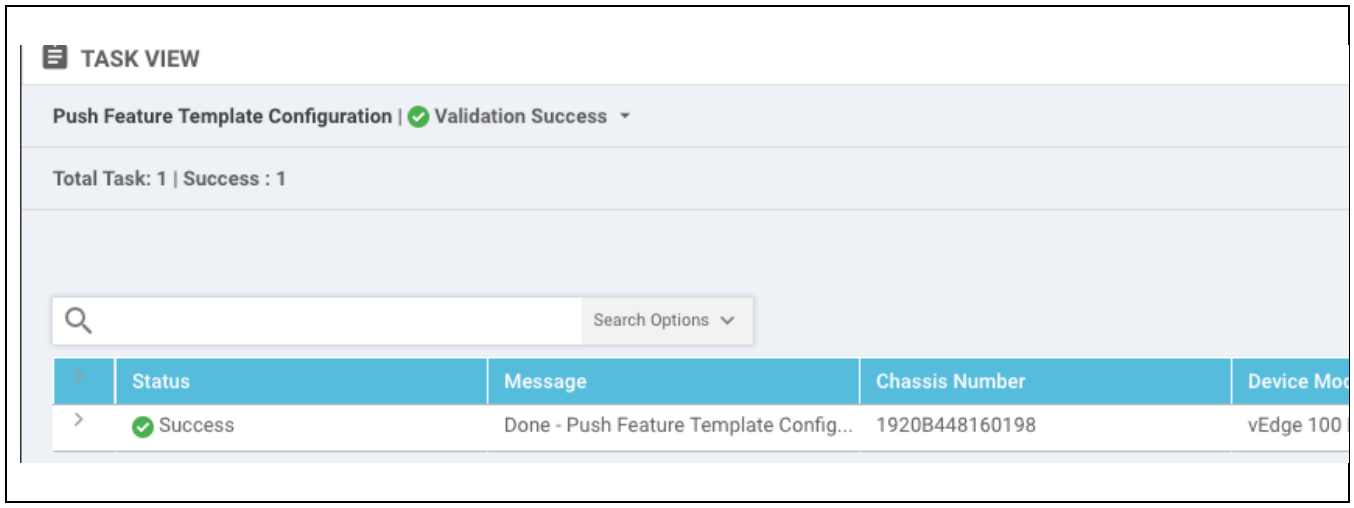


Figure 47: Successful configuration update

4 Verifying Service Configuration

4.1 Request Verification Page

The URL https://ip.zscaler.com can be used to validate if you are transiting ZIA. This is what you will see if you are not transiting ZIA.

Figure 48: Non-working Example

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

Figure 49: Working Example

5 Requesting Zscaler Support

5.1 Gather Support Information

Zscaler support is required to provision new locations for GRE or IPsec service. Zscaler support is also available to help troubleshoot configuration and service issues, and is available 24/7 hours a day, all year.

5.1.1 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**.

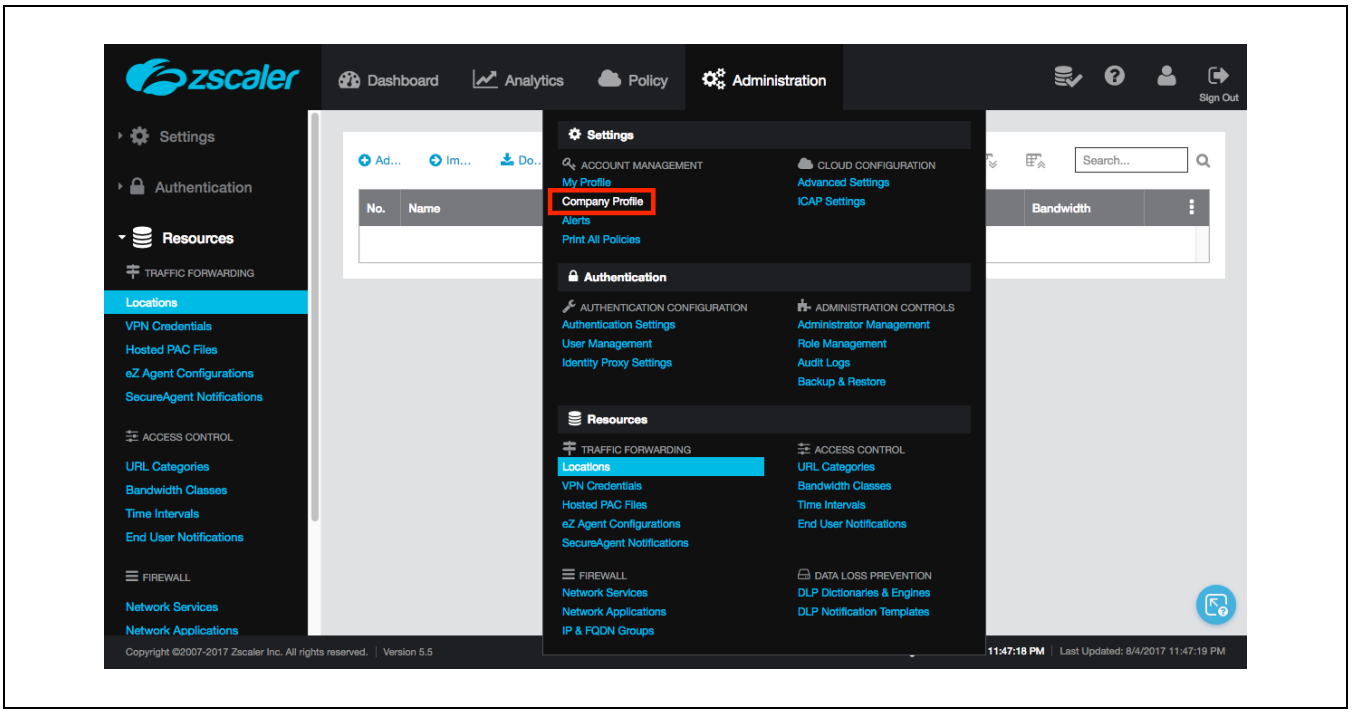


Figure 50: Obtaining Company ID

5.1.2 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.

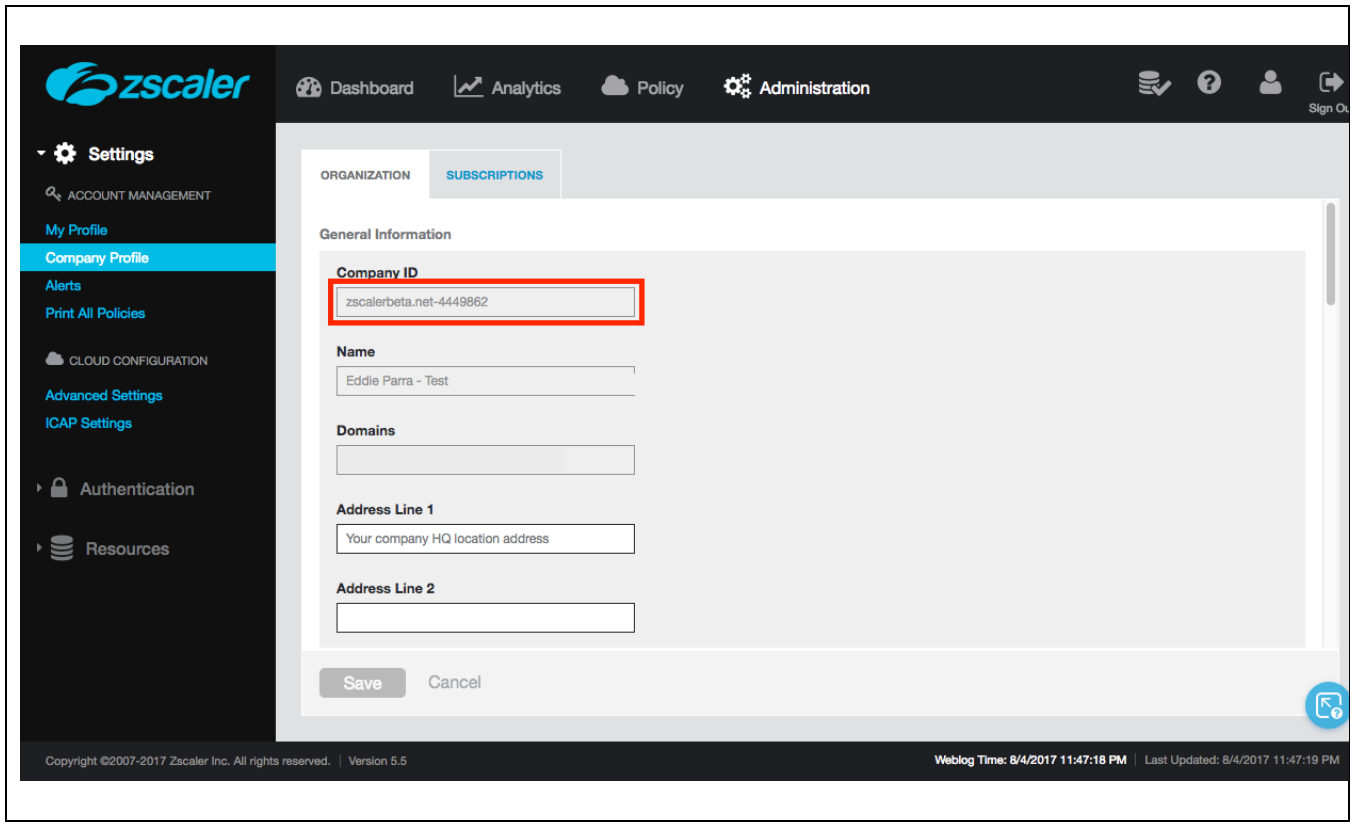


Figure 51: Save Company ID

5.1.3 Enter Support Section

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**.

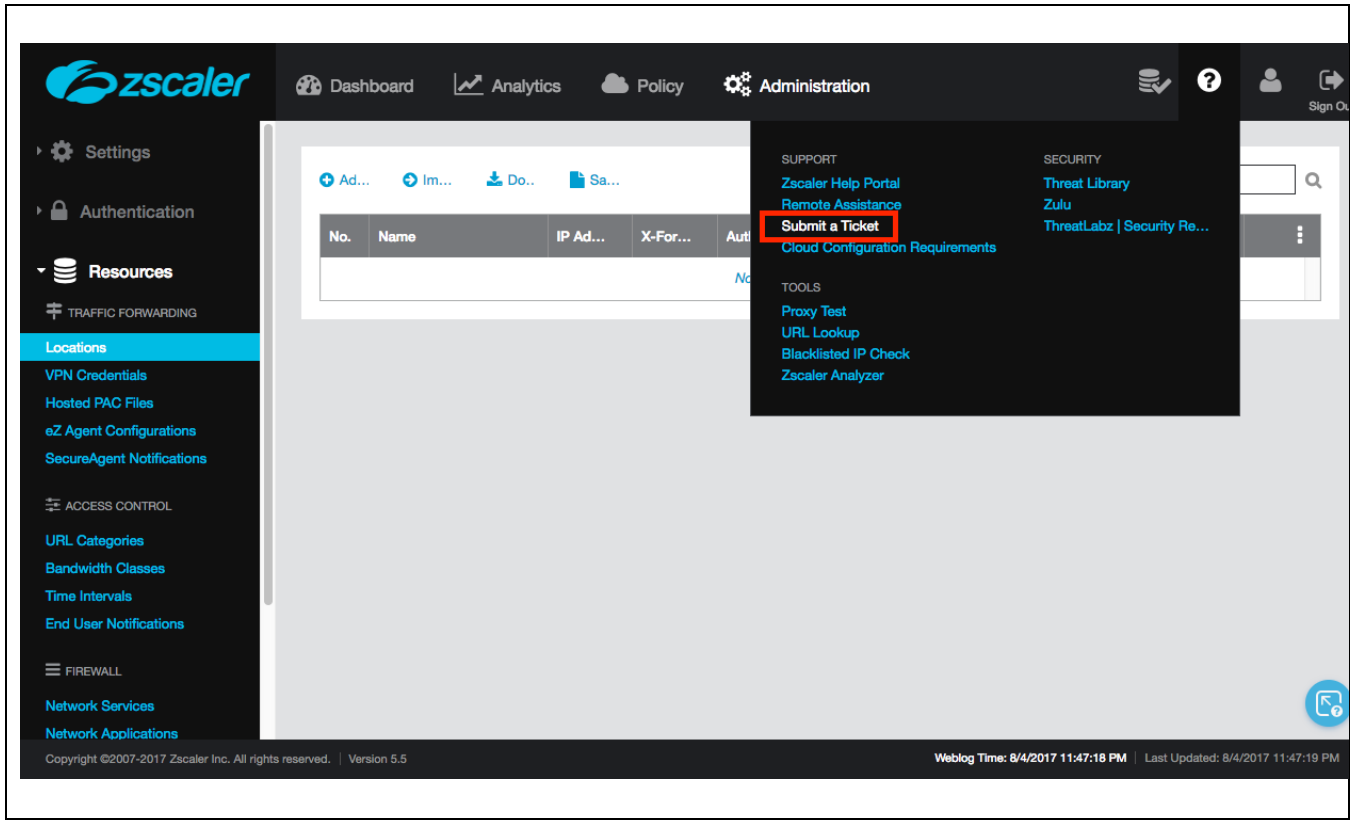


Figure 52: Enter Support Section

5.1.4 Create and Submit Support Request (GRE Provisioning)

It the example below, shows 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 GRE service be provisioned with our public IP information.

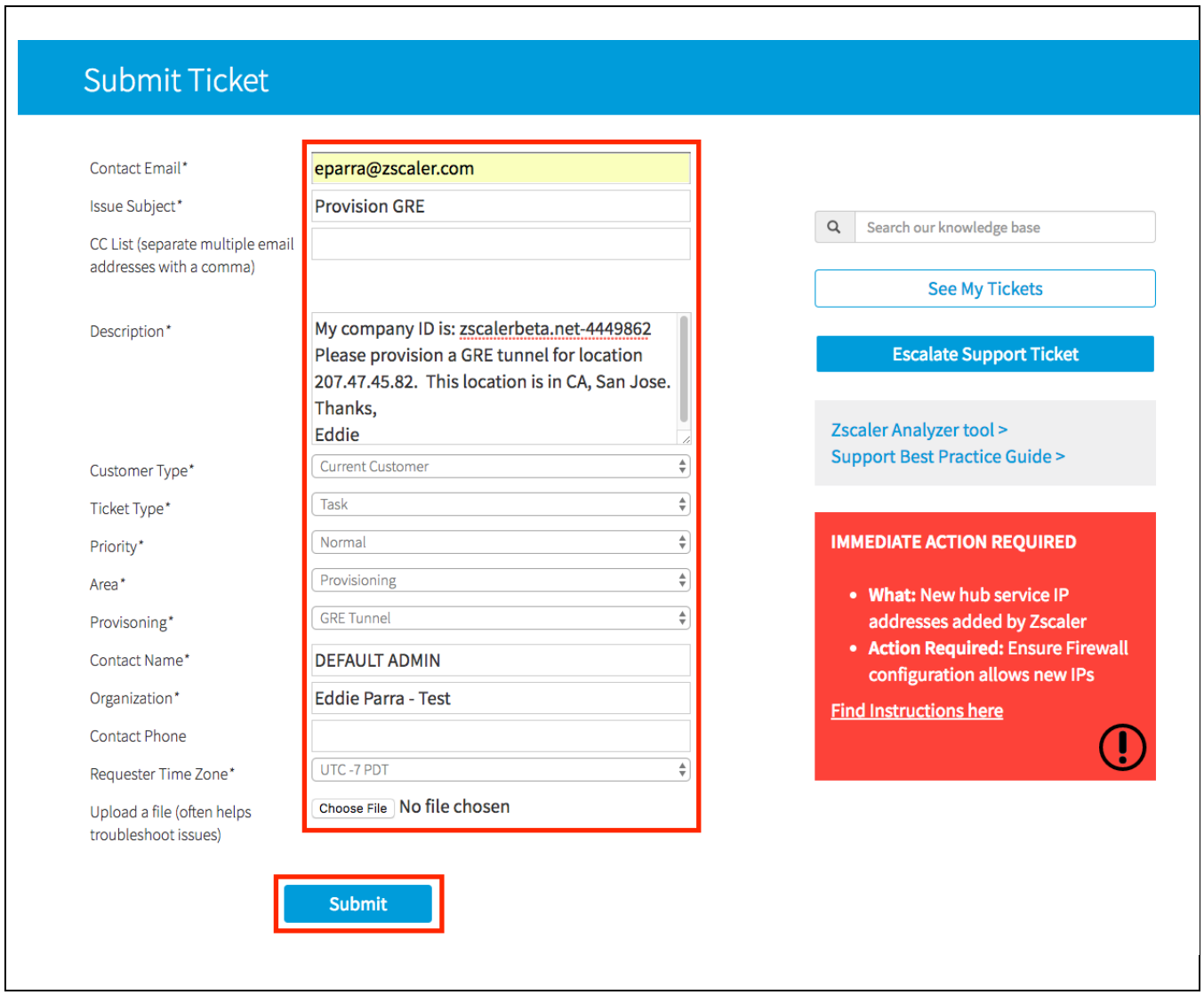
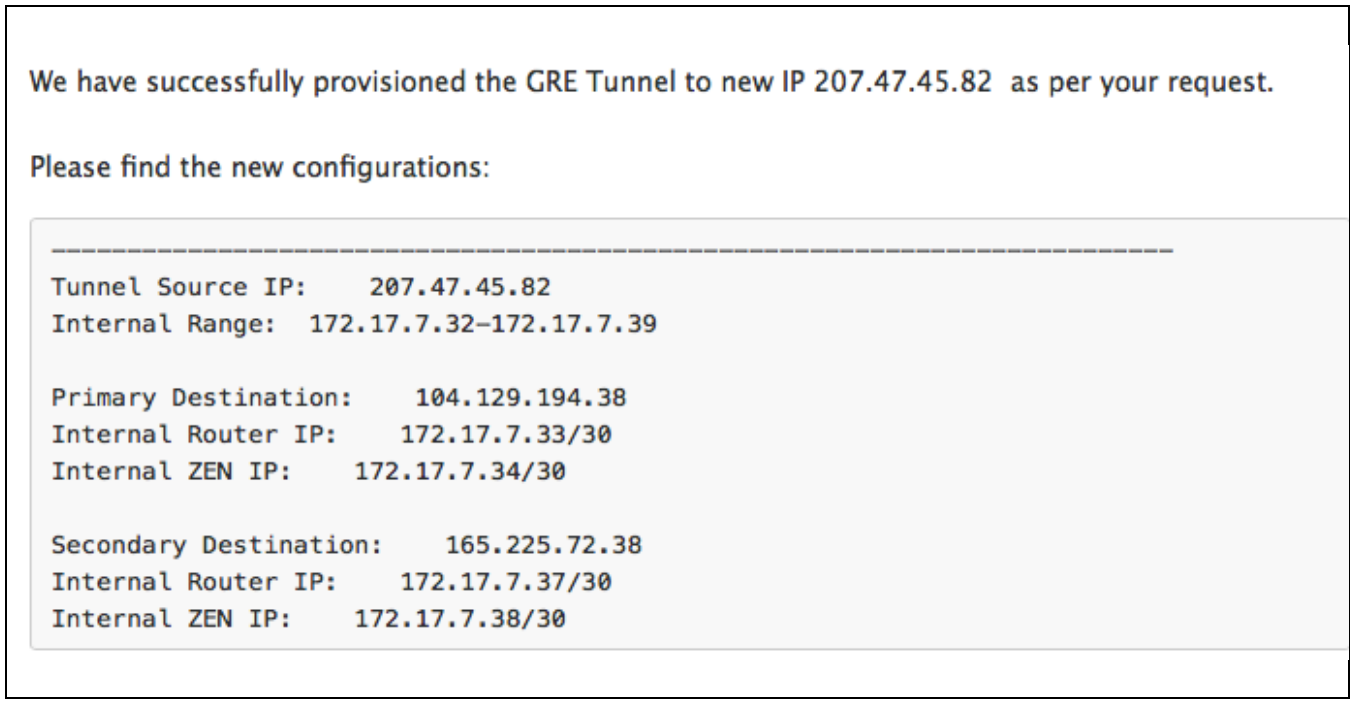


Figure 1: Creating a Support Ticket

5.1.5 Reviewing Provisioning Email

Once the ticket is processed by support for GRE service provisioning, you should see an emai shortly with your GRE IP information. An example email is below:



We have successfully provisioned the GRE Tunnel to new IP 207.47.45.82 as per your request.

Please find the new configurations:

```
------------------------------------------------------------------------
Tunnel Source IP:    207.47.45.82
Internal Range:  172.17.7.32-172.17.7.39

Primary Destination:    104.129.194.38
Internal Router IP:    172.17.7.33/30
Internal ZEN IP:    172.17.7.34/30

Secondary Destination:    165.225.72.38
Internal Router IP:    172.17.7.37/30
Internal ZEN IP:    172.17.7.38/30
```

Figure 54: Provisioning Email

6 Appendix A: Zscaler Resources

Zscaler: Getting Started
https://help.zscaler.com/zia/getting-started

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/

7 Appendix B: Cisco SD-WAN Resources

7.1 Create a Device Template

The device template is basic for any Cisco SD-WAN Edge device to get on-board and managed by Cisco vManage (the SD-WAN management tool).

- In this example, we are going to create the device-template first and attach it to the Edge router
- Following that we will create GRE and IPSec templates and attach it to the device template individually
- You can also refer to below link for Generic device-template creation

https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.2/Configuration/Templates#Create_a_Device_Template

7.1.1 Create Device Template

Choose "**From Feature Template**" under ***Configuration > Device > Create Template***

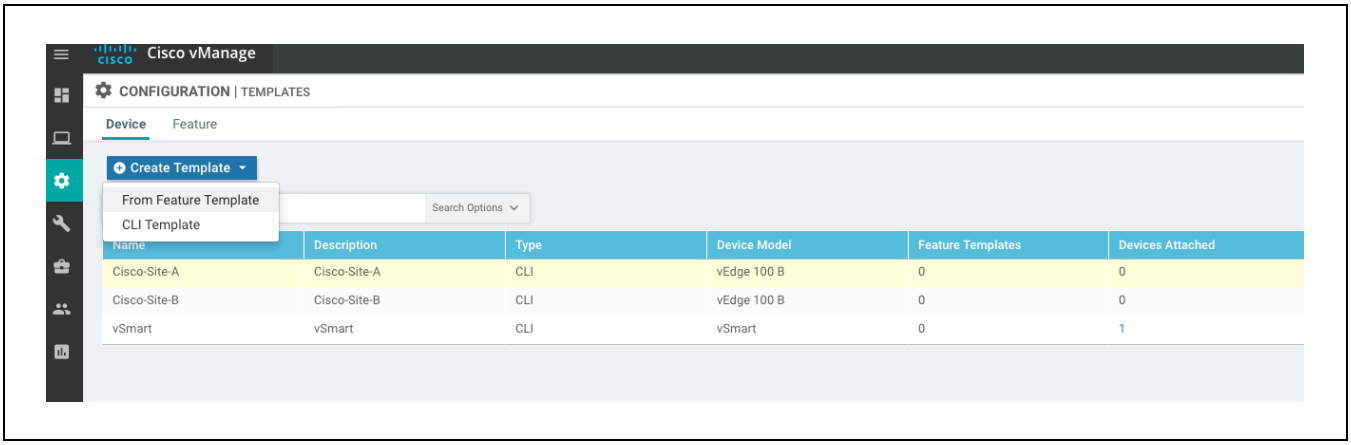


Figure 54: Create device template

7.1.2 Choose Device Template

Choose the device type under device-template

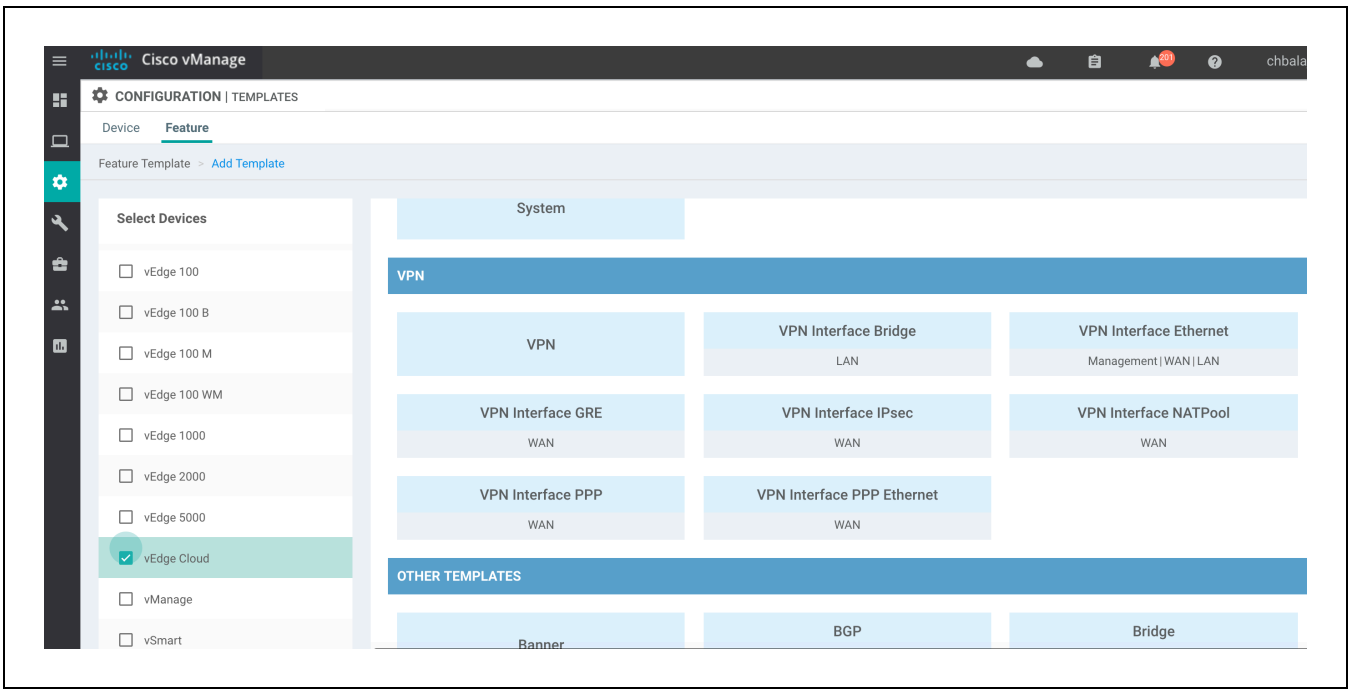


Figure 55: Choose the device type

7.1.3 Name Device Template

Provide name and description for the device-template

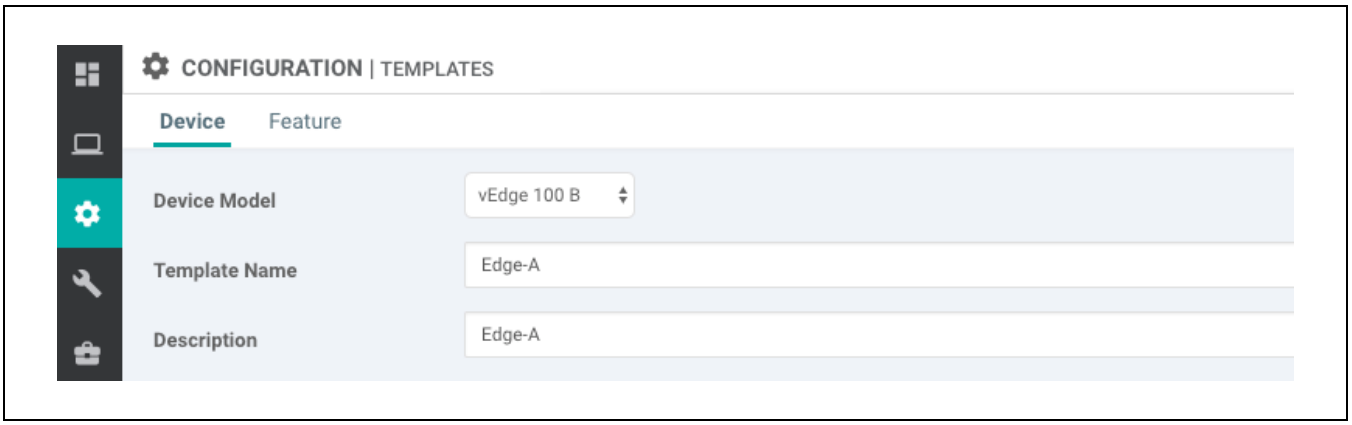


Figure 55: Enter the name for device template

Note: In this example: the default configs are used for features include AAA, BFD, Security and logging. So, we won't configure those parameters explicitly.

7.1.4 Create VPN-0 Template

Configure VPN-0 (Transport VPN) for the chosen device. From the drop-down menu under VPN0, choose “create-template”.

NOTE: Create Template will take you to the VPN0-Template page as shown in Figure 57.

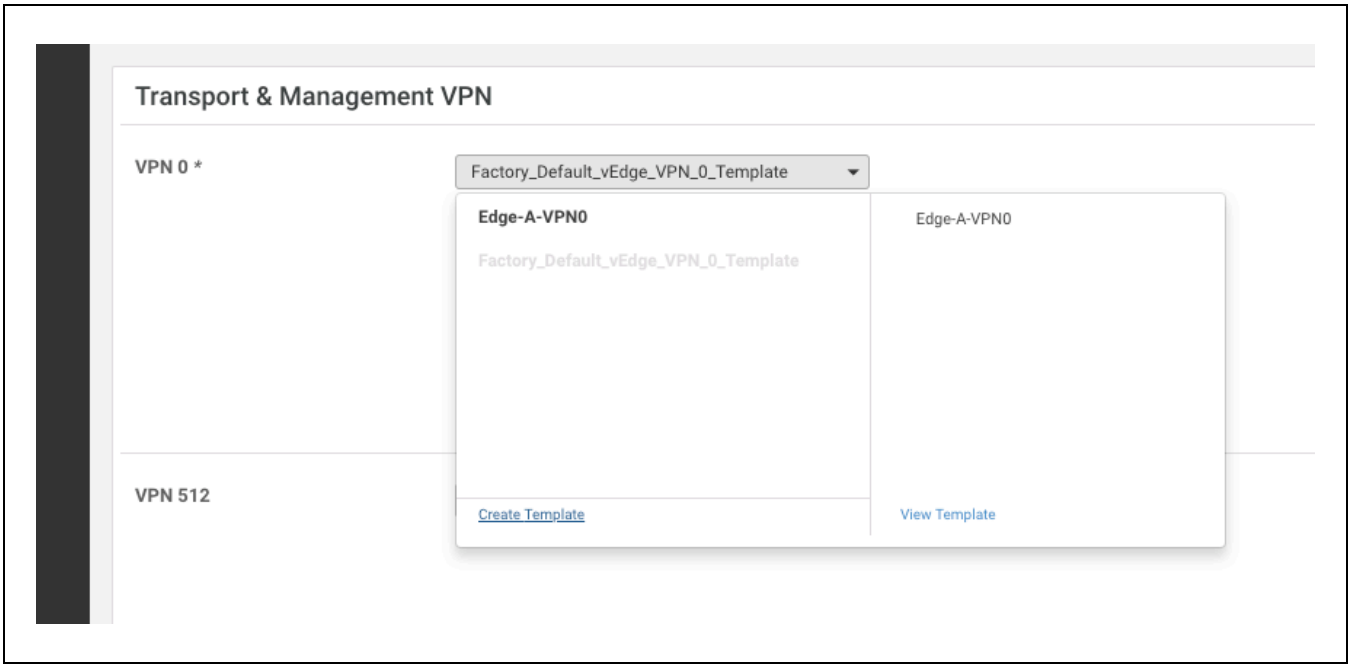


Figure 56: Create Template for VPN0

7.1.5 Configure VPN-0 Template Name

Under VPN0 template: Provide name and description for VPN-0 template

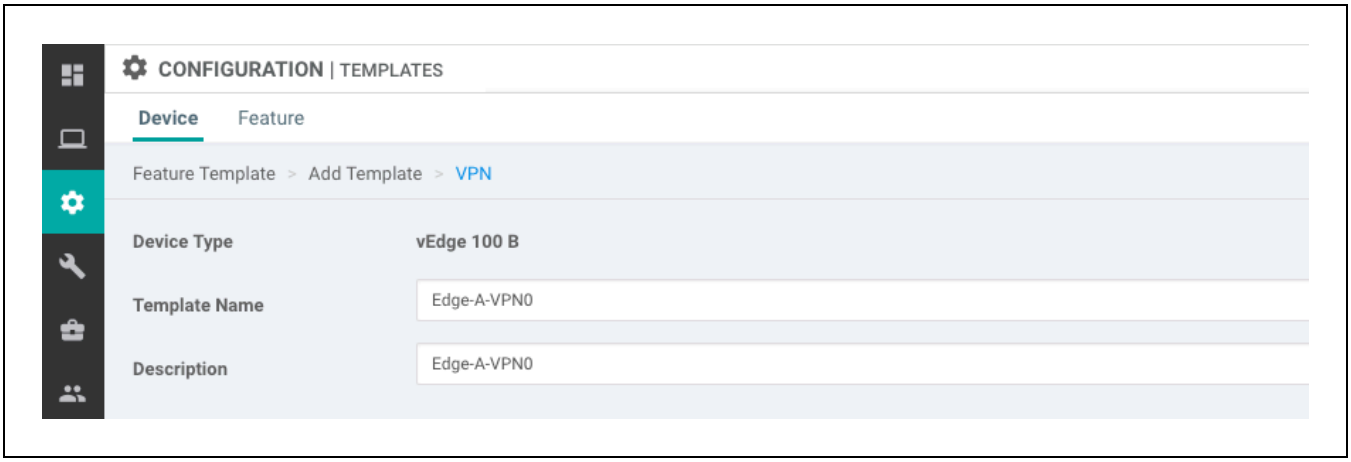


Figure 57: Enter the name for VPN0 template

Configure VPN-0 Template

Under VPN0 template: Configure VPN-ID as “0” and configure the DNS Server address as shown below

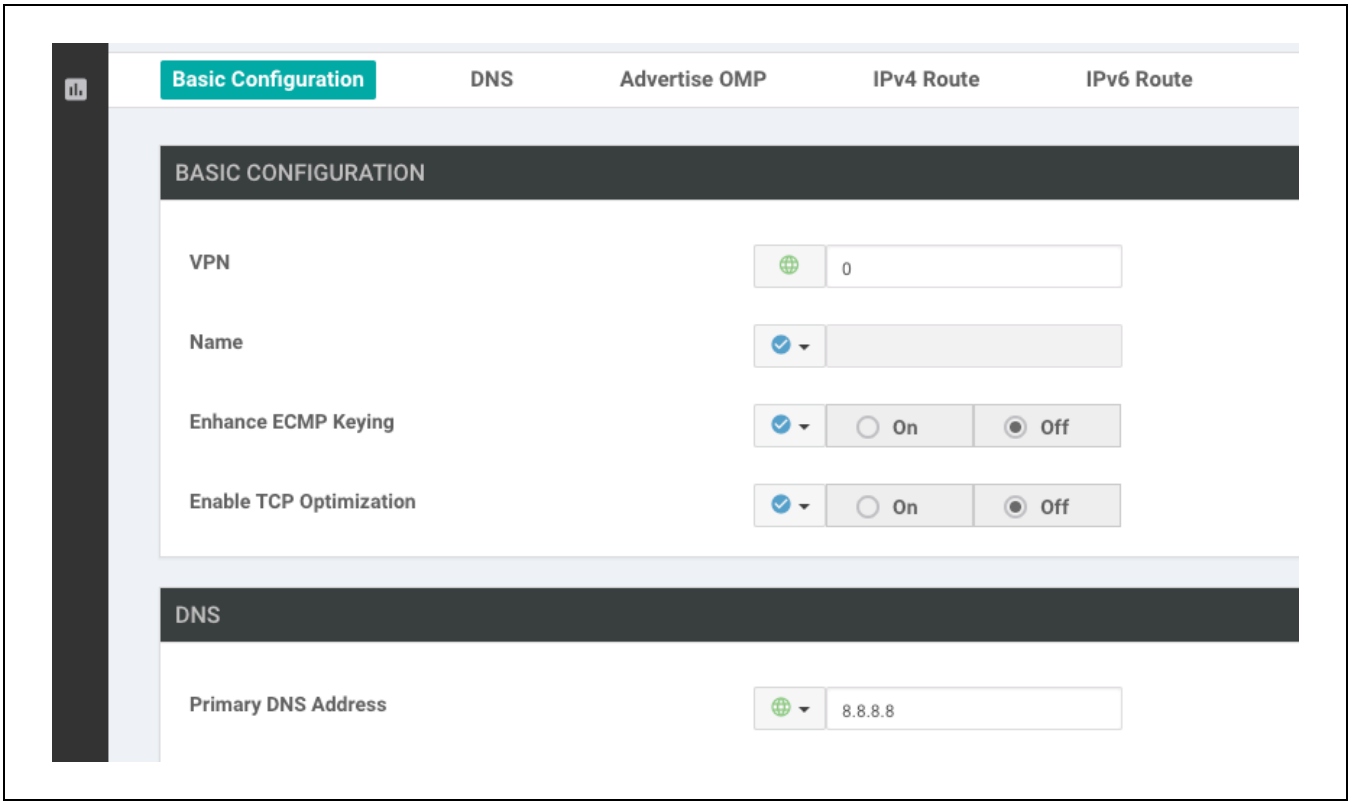


Figure 58: Basic configuration of VPN0 template

7.1.6 Add IPv4 Route

Under VPN0 template: Configure IPv4 default route as shown below

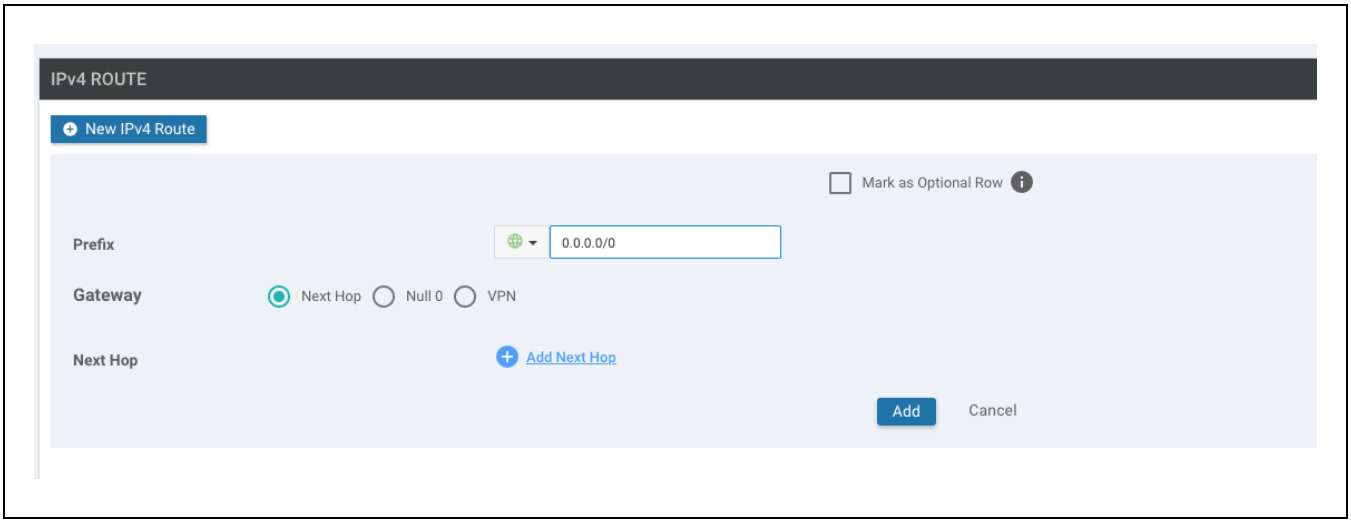


Figure 59: Add IPv4 route

7.1.7 Configure IPv4 Route Next-Hop

Under VPN0 template: Add next-hop for the default route which just got added

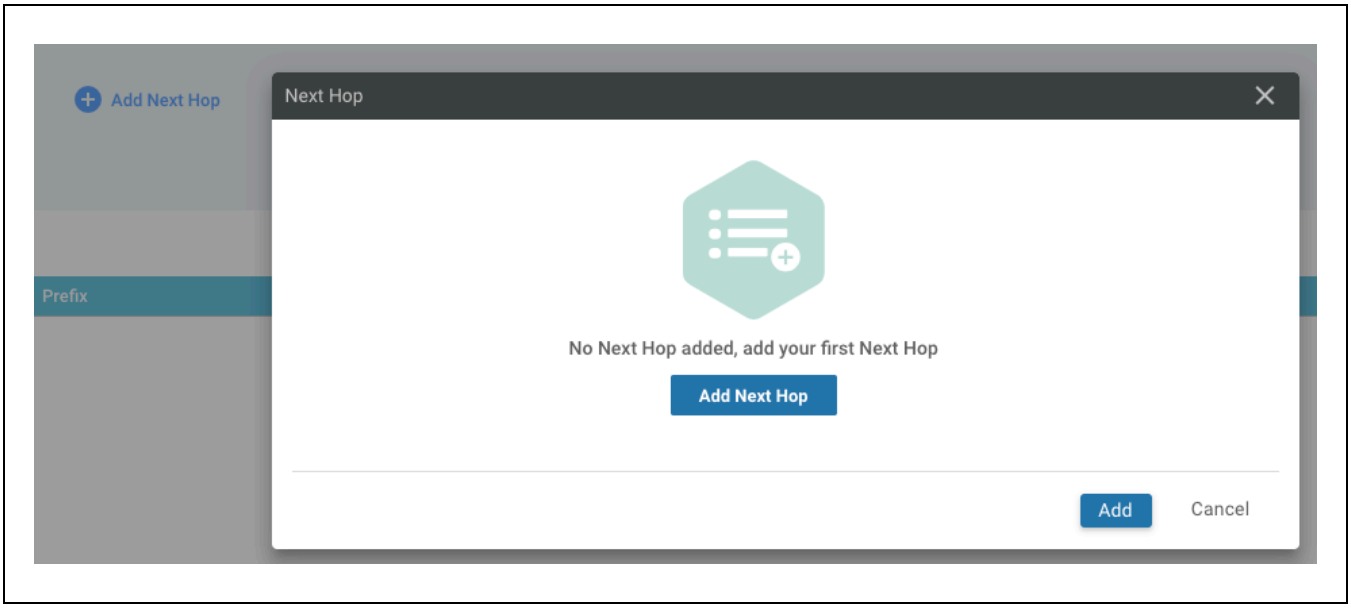


Figure 60: Add Next hop

7.1.8 Set Next-Hop Address

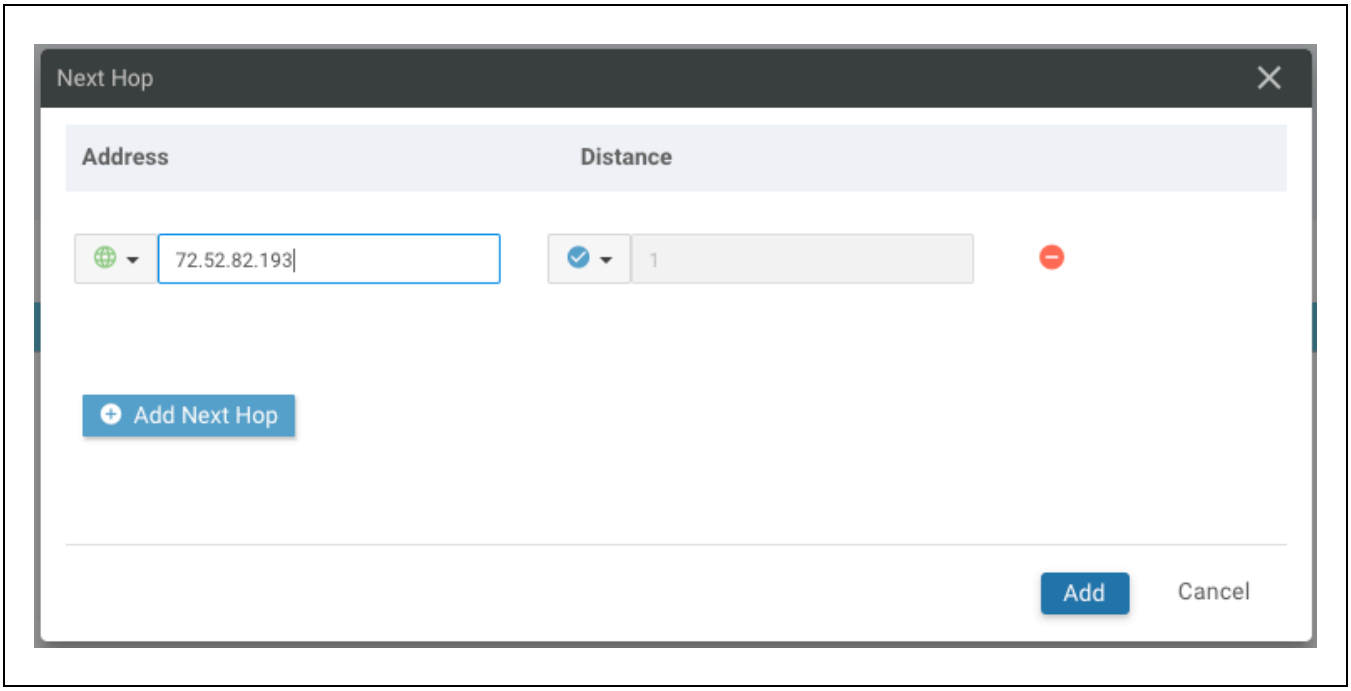


Figure 61: Add Next-hop address

Note: The added default IPv4 route will be shown under VPN-0 Template as below

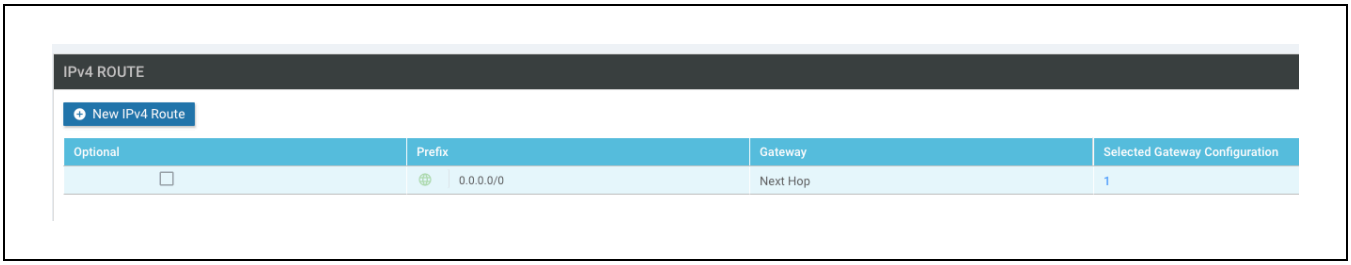


Figure 62: Check the added route

7.1.9 Save VPN-0 Template

Save the VPN0 template. NOTE: After saving the VPN-0 template, it will take you back to the Original Device Template page. Now add Interface under VPN-0 of the device template as shown below. Add VPN Interface from “Additional VPN0 Templates” on the right pane

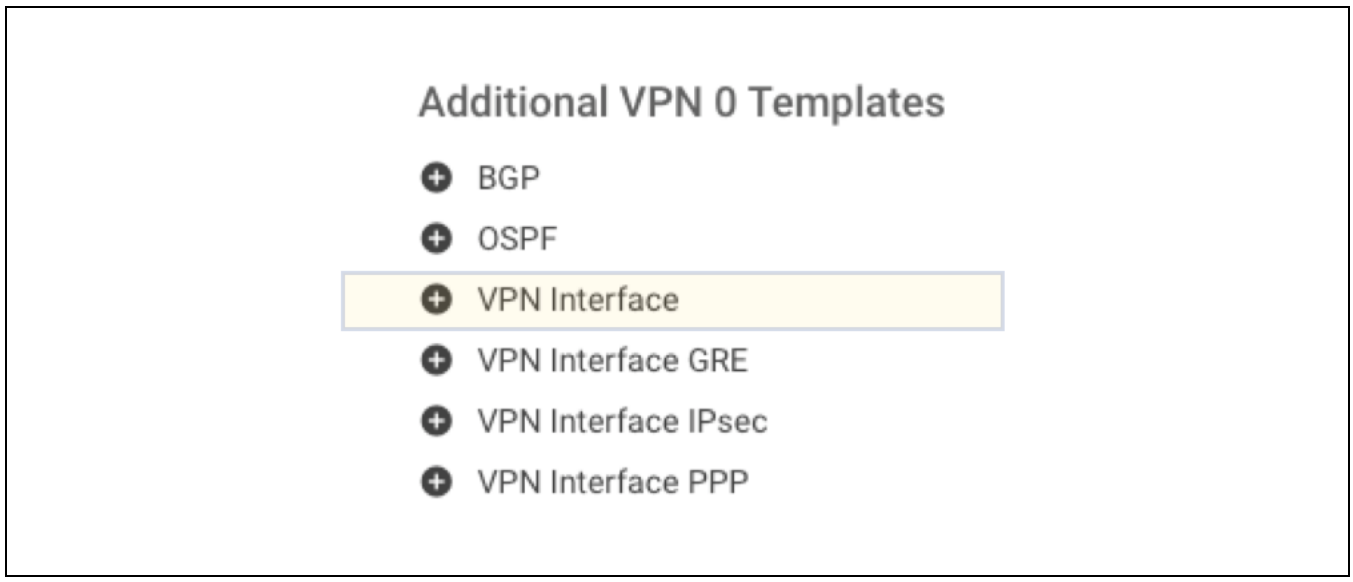


Figure 63: Add VPN Interface

Once VPN Interface got added, choose the create-template from VPN Interface drop-down list

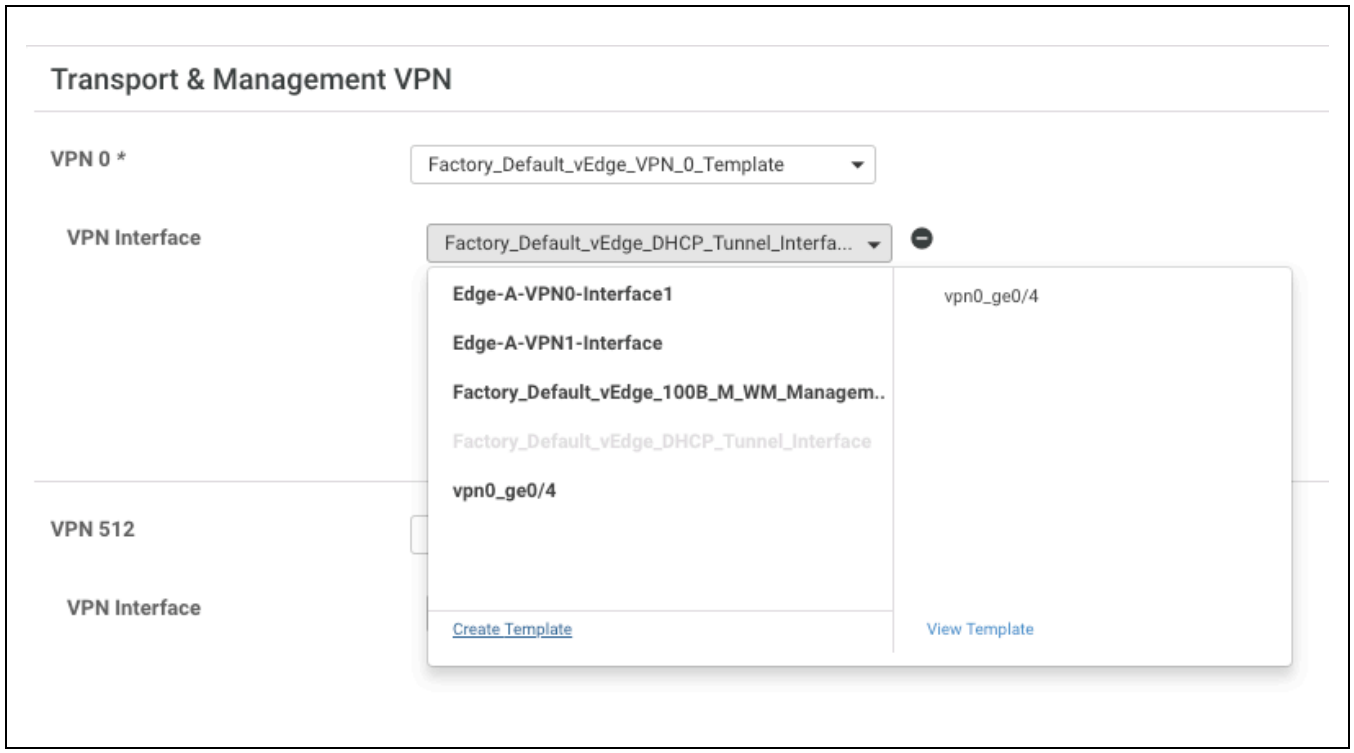


Figure 64: Create Template for a new VPN0 interface

Create Template will take you to the VPN0-Interface-Template page as shown in Figure 65.

7.1.10 Add Name and Description to Template

Under VPN Interface template, provide name and description for the template

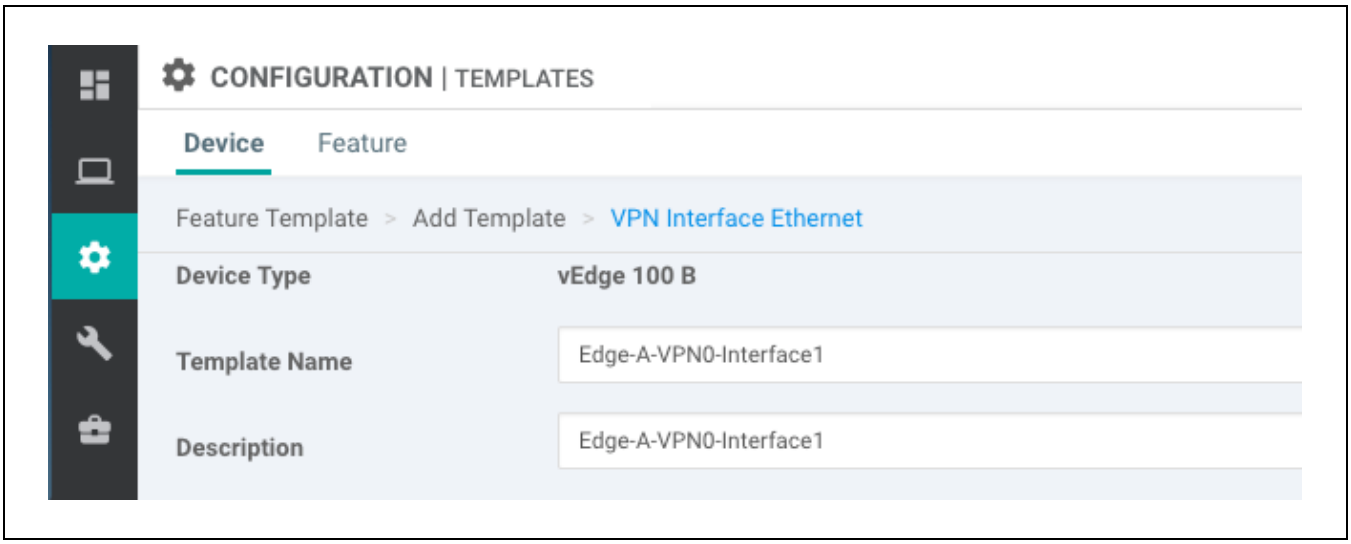


Figure 65: Provide name and description for VPN Interface template

7.1.11 Enter Basic Configuration for VPN-0 Interface

Configure the Interface Name under Basic Configuration and change the interface status to “No Shutdown” globally as shown below.

Figure 66: Enter basic configuration for VPN0 Interface

7.1.12 Set IPv4 Address

Configure the IPv4 address for the interface. If DHCP is preferred, then choose the IPv4 configuration option as “Dynamic” .

Figure 67: Choose the IP address type and add value

7.1.13 Enable SD-WAN Overlay

Change the tunnel-interface to **ON** under TUNNEL. **Note:** The color of the tunnel can be default, if there is going to be only one WAN transport interface. Otherwise, it is recommended to choose the color for the tunnel based on Public (or) Private WAN transport. In this example, we are using default color.

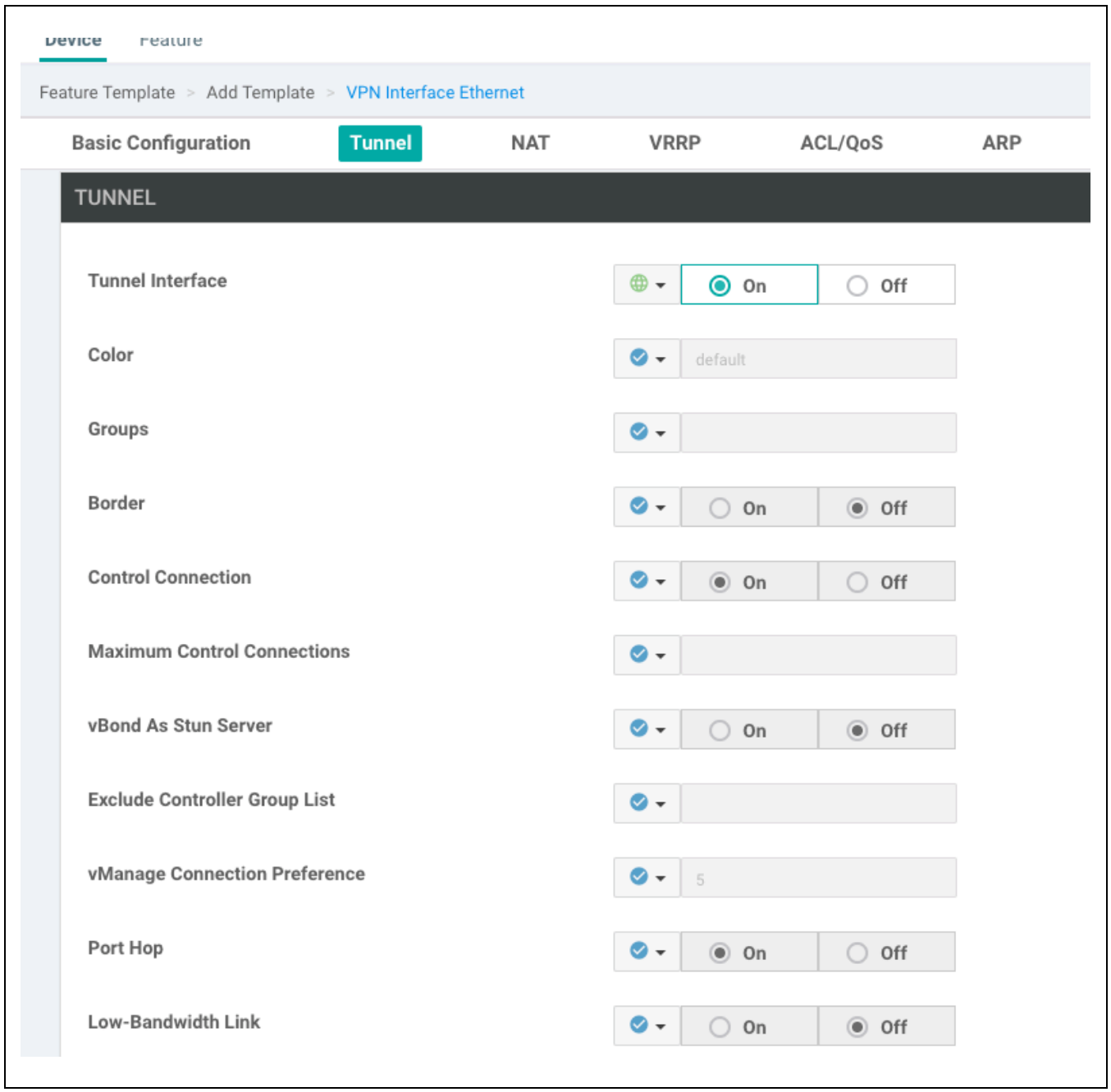


Figure 68: Enable SDWAN Overlay tunnel

7.1.14 Enable SSH of VPN-0

Under Allow Service of same TUNNEL configs, choose the services which needs to be allowed via that WAN Interface. In this example, I have allowed SSH Service via the WAN interface,

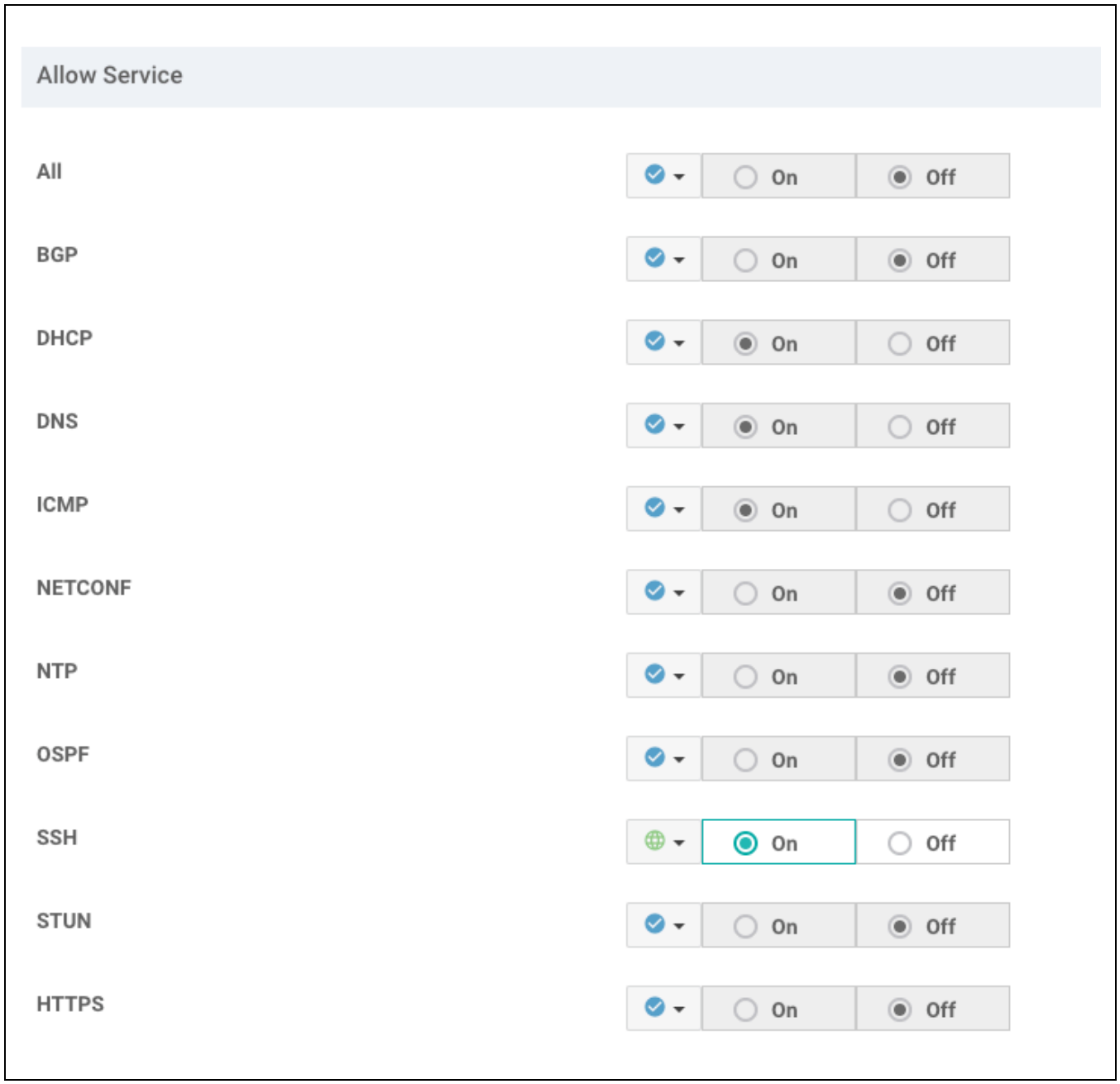


Figure 69: Enable SSH service on VPN0 Interface

7.1.15 Add Service VPN

Now, Save the whole “VPN Interface Ethernet” template by using “SAVE” button at the bottom of the page. This will take you back to the original device template page.

Now Add the Service VPN under Device-template as shown below. In this example, we are just going to add one Service VPN.

Figure 70: Add Service VPN

7.1.16 Verify Service Template

Once the service VPN got added, it will be shown in the device-template as below

Figure 71: Service Template

7.1.17 Set Basic Service VPN Configuration

- Provide name and description for the Service VPN template
- Assign the Service VPN-ID under basic configuration. In this example we are using VPN-ID as “1”
- Configure primary DNS Server if any.

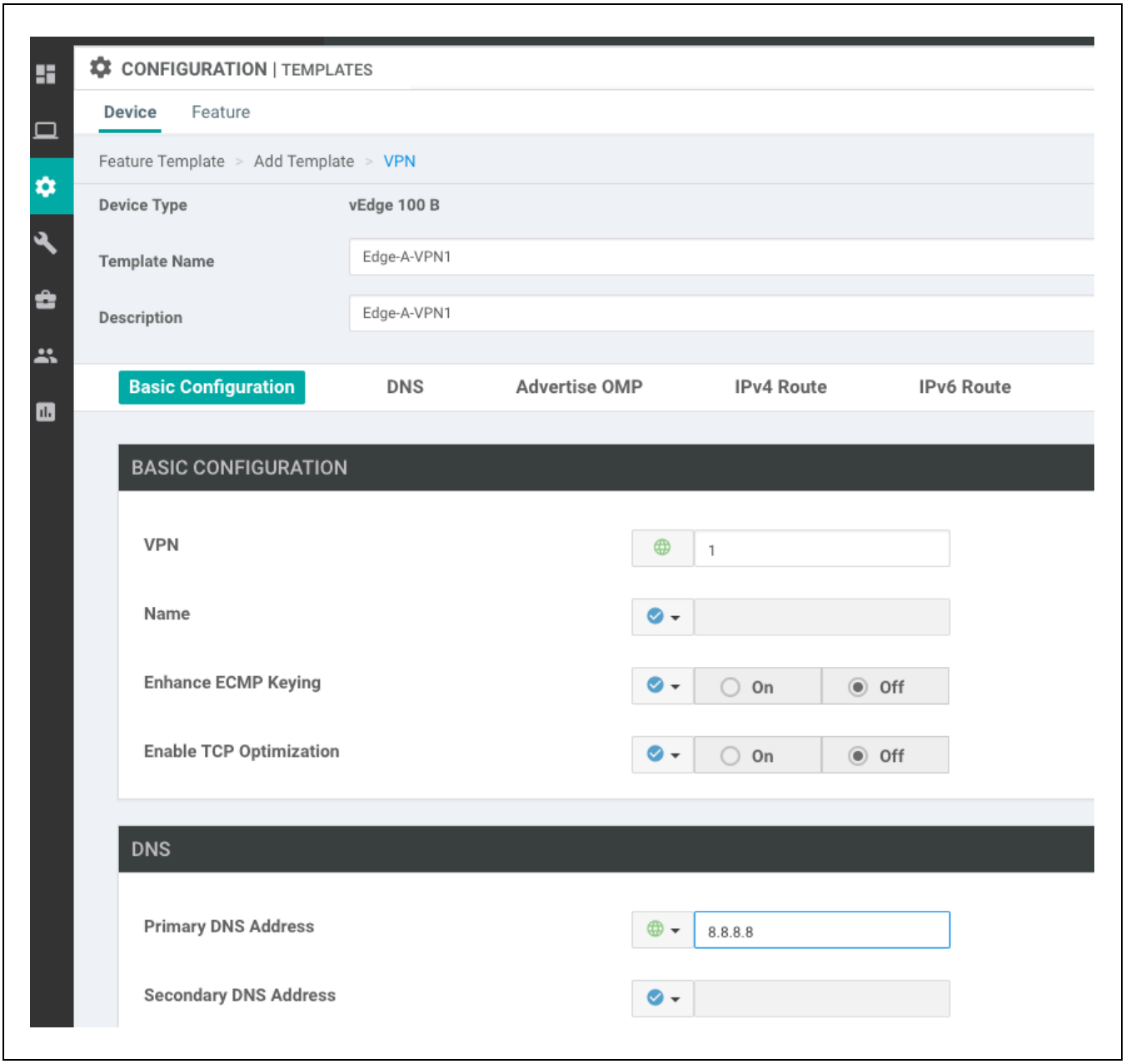


Figure 72: Enter basic configuration for Service VPN

7.1.18 Add VPN Interface Under Service VPN

Keep the other options under Service VPN template as default and do save. This will take you back to the original device template page. Next, add a VPN Interface under the Service VPN section as shown below.

Note: This Service VPN interface is the one which connects to the SD-WAN router's LAN network.

- Add VPN Interface from "Additional VPN0 Templates" on the right pane

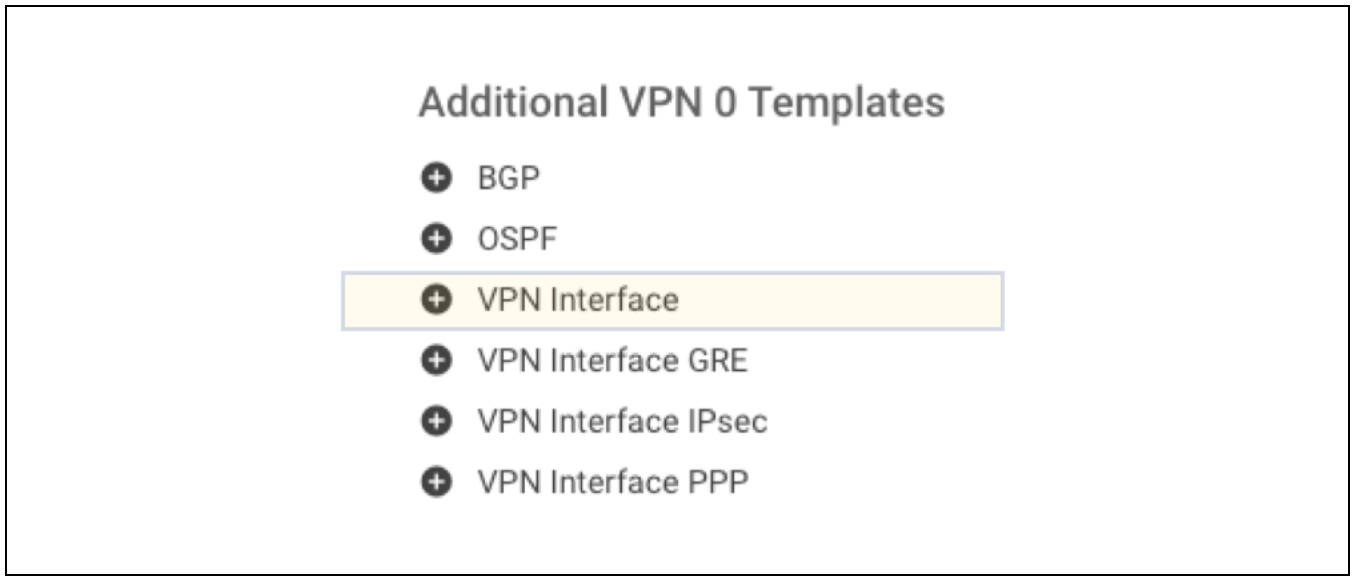


Figure 73: Add VPN Interface under Service VPN

7.1.19 Create Template Under Service VPN Interface

Once VPN Interface got added, choose the create-template from VPN Interface drop-down list.

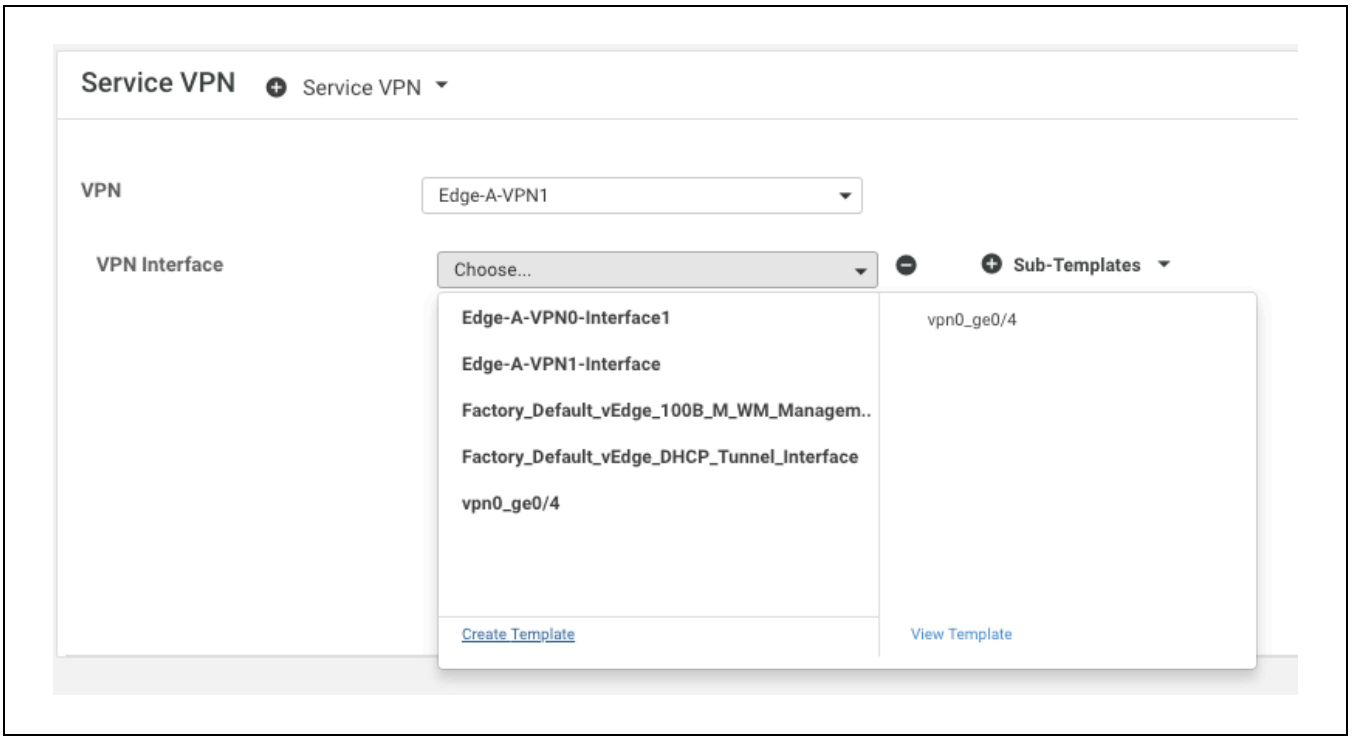


Figure 74: Create Template under Service VPN Interface

Note: Create Template will take you to the VPN0-Interface-Template page as shown in Figure 75.

7.1.20 Basic Configuration of Service VPN Interface

Under VPN Interface template:

- Provide name for the Service VPN – Interface template
- Change the interface status to “No shutdown” under basic configuration
- Configure the Service VPN interface name. In this example we use “ge0/1”
- Choose the IPv4 configuration as Static and configure IP address

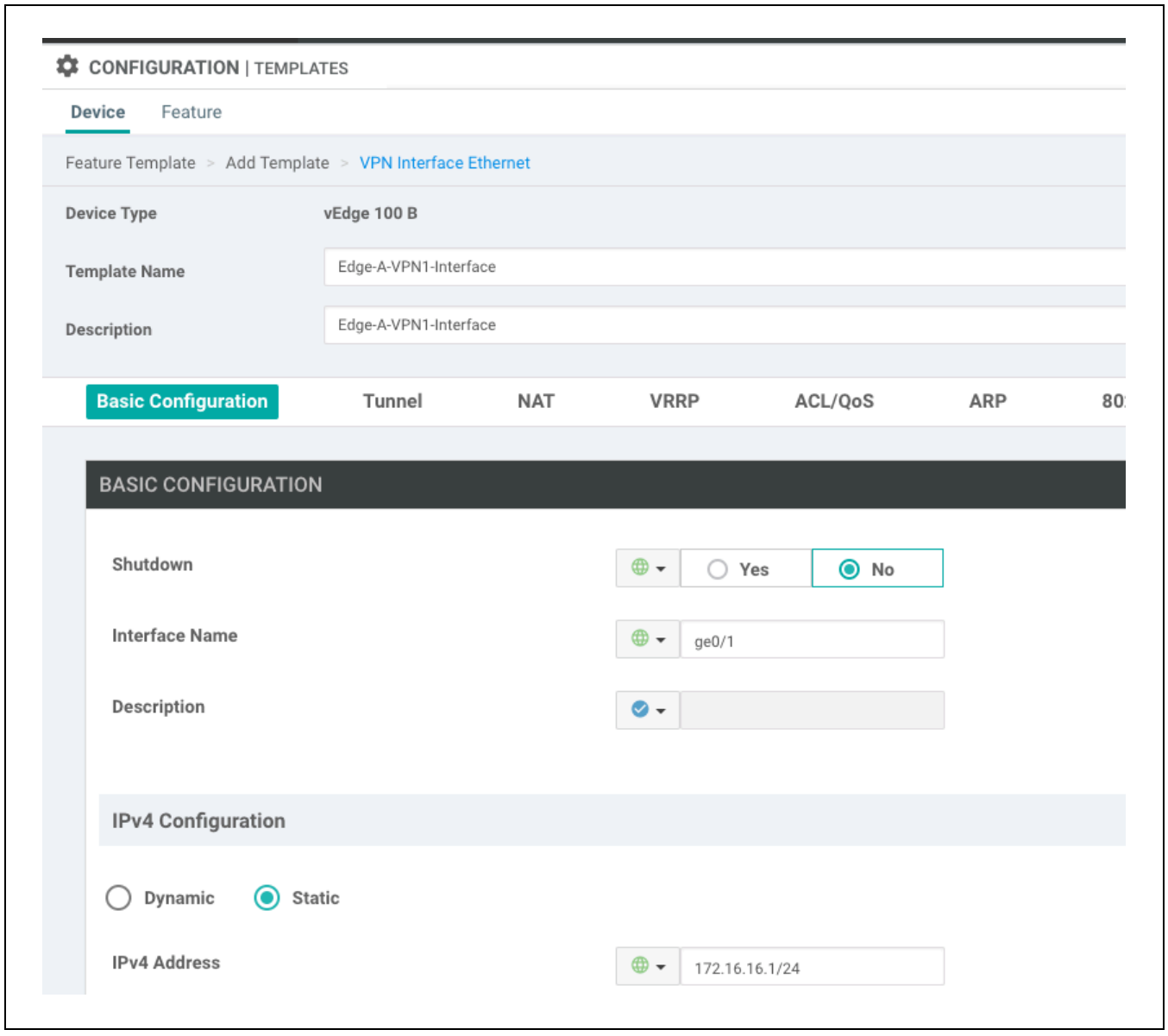


Figure 75: Basic configuration of Service VPN Interface

7.1.21 Device Template List

Keep rest of the settings as default and save the template. NOTE: This will take you back to the original device template.

Now, it's time to save the Device template. Go-to bottom of the page and complete the device template creation by clicking "CREATE" button. Once the device-template" is created, it will be shown as below.

Note: The device-template got created now. However it is yet to be attached/applied to a device (Cisco SD-WAN Edge router)

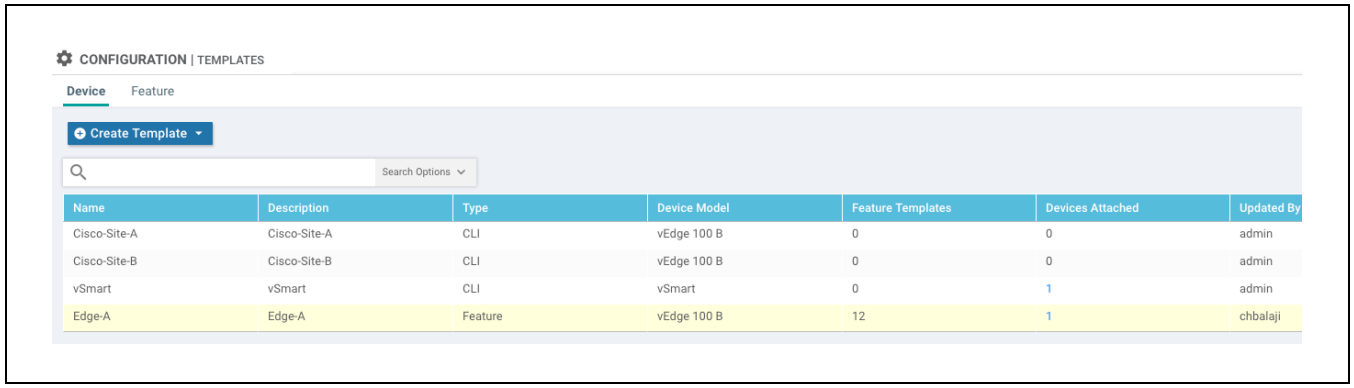


Figure 76: Device Template List

7.1.22 Attach Device to Device Template

To attach the device – template to a device (Cisco SD-WAN Edge router), choose the device-template name as shown in Figure 77 and do right click on the three dots at the right end as shown below

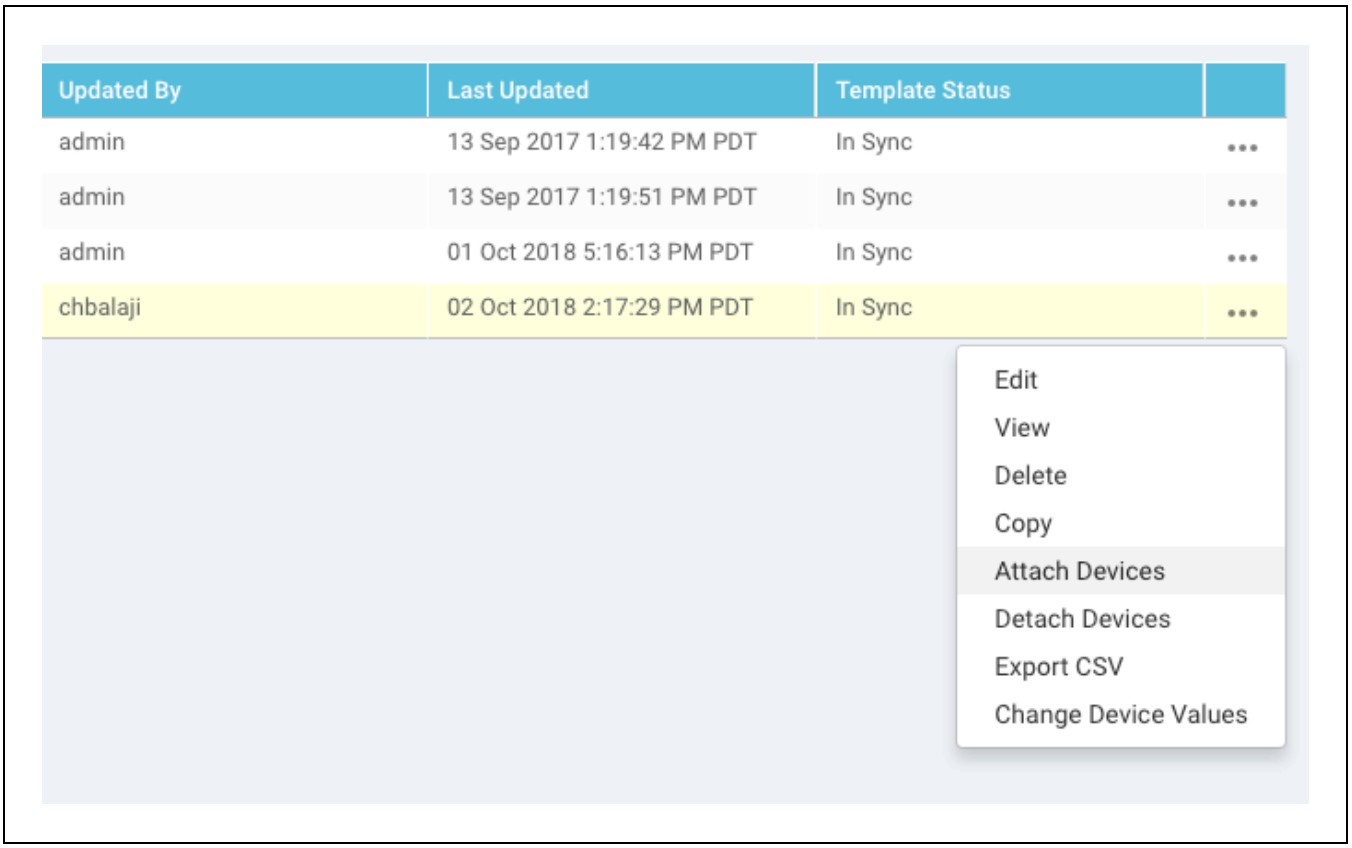


Figure 77: Attach devices to the device template

7.1.23 Chose Devices to Attach to Device Template

This will display a page with list of available devices for attaching the device template (based on the platform type we have chosen while creating the device template) as shown below.

- Choose the device from left box and move it to the right box (One or more devices can be selected and attached with same device template)
- Click “Attach” button

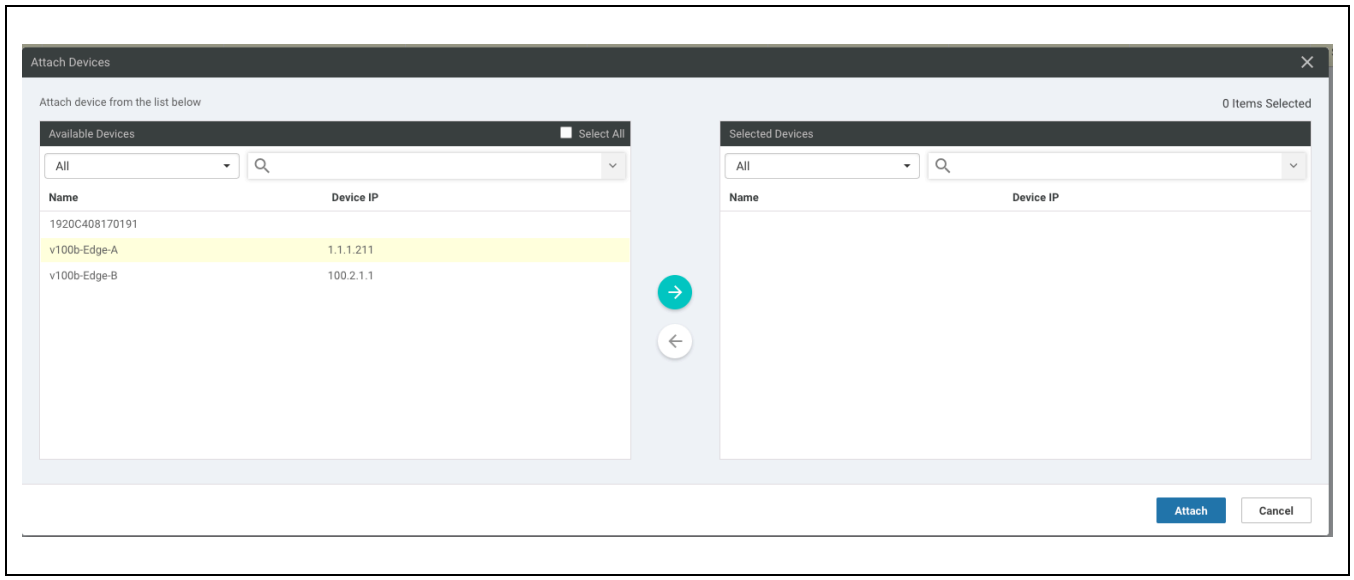


Figure 78: Choose the devices to be attached to device-template

Note: In this example, we are choosing “v100b-Edge-A” device to be attached with device-template

7.1.24 Edit Device Template

After attaching, it will navigate to the page as shown below where we need to fill the device system parameters as shown below. Next, click on the three dots at the right pane of the selected device and choose “Edit Device Template” as shown below.

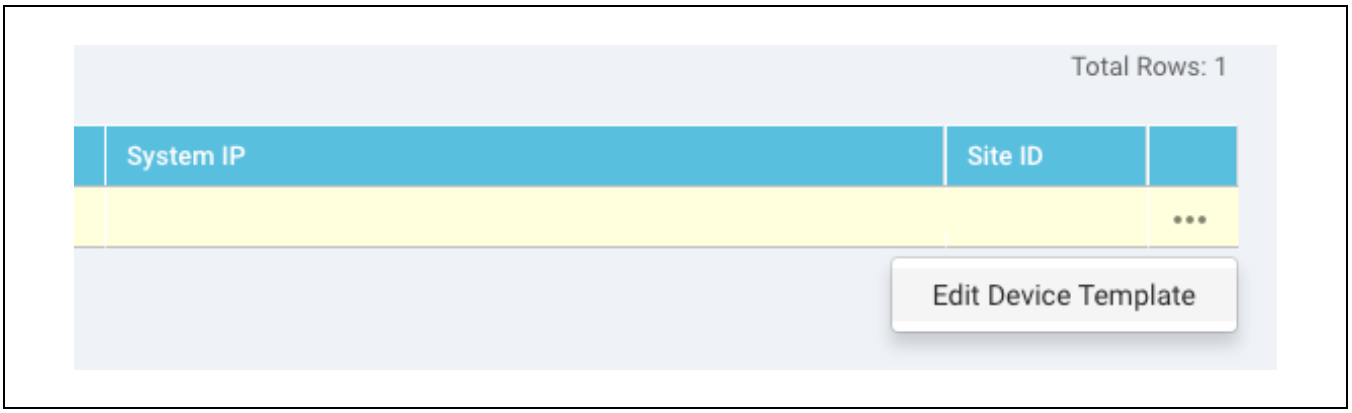


Figure 79: Click Edit device template

7.1.25 Populate Device Template Values

- Now, add the System IP, Hostname and Site-ID fields with appropriate values ("show run sys" on the device will get you these values)
- Once values are filled-in, do click the "Update/Save" button.

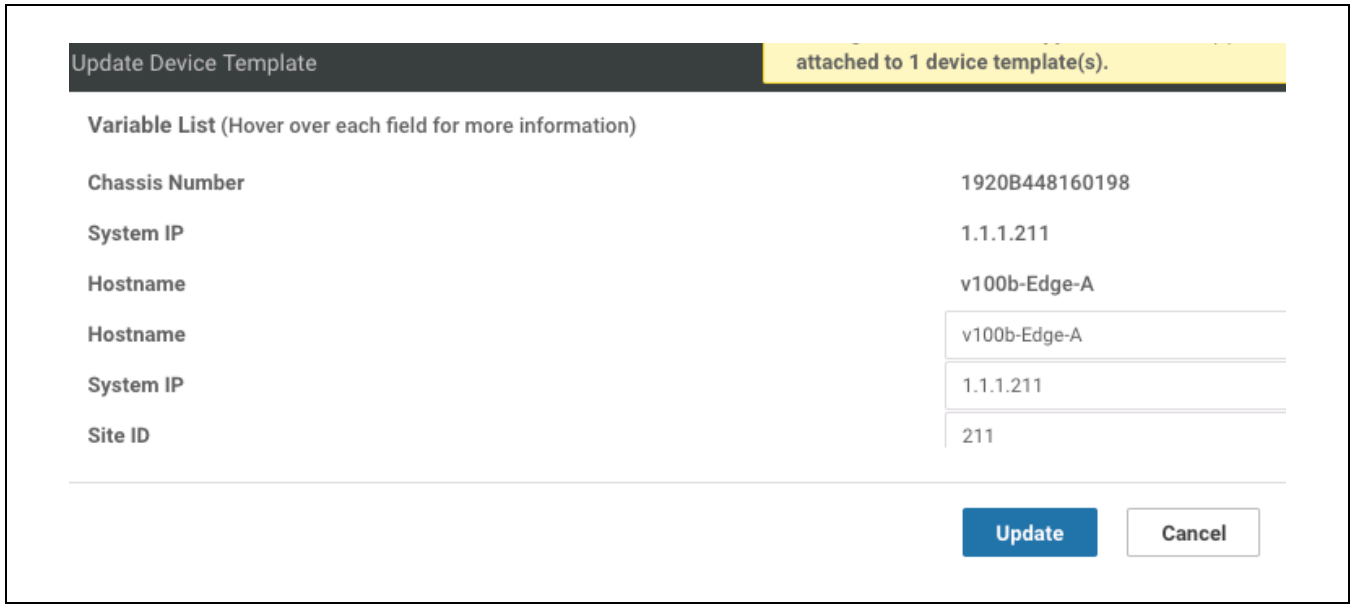


Figure 80: Enter the Device Template Values

7.1.26 Configuration Preview

Click on next button. This will take you to the config-preview page as shown below

- The config will be displayed by clicking the device listed on the left pane of the device
- The config diff w.r.to device's current running config can also be seen by choosing "Config diff" option
- Finally proceed further by clicking "Configure devices" button.

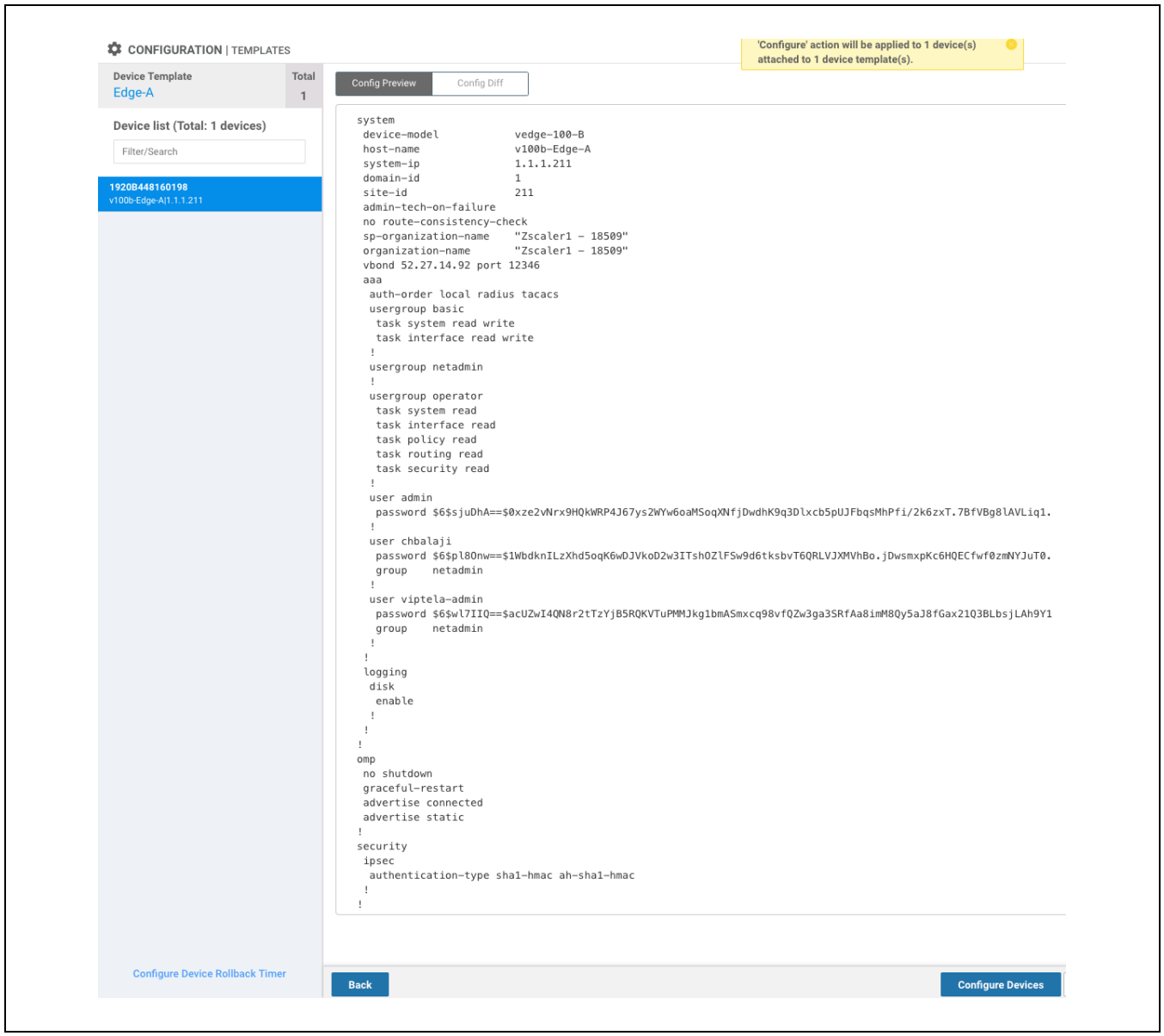


Figure 81: Config Preview

7.1.27 Verify Template Push

After the device-template got attached to the device successfully, the below message will be shown

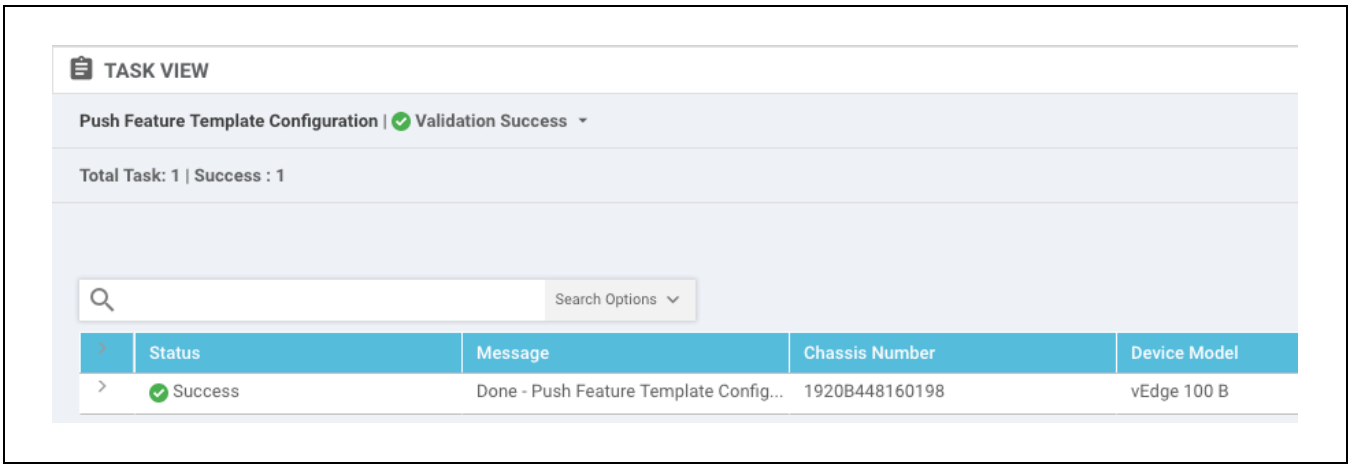


Figure 82: Successful Template Push