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

February 2020

Version 3.1

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 provides configuration guidance for integrating Zscaler Internet Access (ZIA) and Cisco SD-WAN successfully. There are examples to show how to provision a new service with ZIA and Cisco SD-WAN using GRE or Ipsec tunnels. For Cisco SD-WAN, configurations that use feature templates through vManage and CLI are both shown. All examples in this guide presumes the reader has a basic comprehension of IP Networking.

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 Hardware Used

Both Cisco vEdge and IOS XE-SD-WAN routers were tested. For the vEdge router, both a vEdge 100b and ISR1100-4G were tested and for the IOS XE SD-WAN router, an ISR4331 was tested.

1.3 Software Revisions

This document was written using Zscaler Internet Access version 6.0 and Cisco SD-WAN version 19.2.099 vEdge and 16.12.1e IOS XE SD-WAN code. In addition, Cisco SD-WAN 19.3.0 vEdge and 16.12.1r IOS XE SD-WAN code were tested as well.

1.4 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.

1.5 Document Prerequisites

Zscaler Internet Access (ZIA)

- A working instance of ZIA 6.0 (or newer)
- Administrator login credentials to ZIA

Cisco SD-WAN

- This document assumes you have the Cisco SD-WAN controllers already built and operational, either through the Cisco cloud service or on-premise. You can use vManage to configure and manage the WAN Edge routers (recommended) or you can use CLI.
- It is also assumed that the WAN Edge devices are already connected to the controllers in the SD-WAN overlay, and a basic device template configuration from vManage has been deployed on them. See Appendix 7 for onboarding information, deploying base device template instructions, and CLI-equivalent configurations.

Using vManage (GUI)

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

Using CLI:

- Must have SSH or console access to the device.
- Must have the valid user credentials for the Cisco WAN Edge router.

1.6 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
3.0	January 2020	Updated for 19.2.099 and 19.3.0 code, added IOS XE SD-WAN router information, added design information, added L7 health checking, tested ISR1100-4G
3.1	February 2020	Incorporated review feedback

1.7 Cisco Design Overview

Enterprises can take advantage of secure local Internet breakout by using Cisco SD-WAN combined with Zscaler. Using Cisco SD-WAN, the network administrator can decide what traffic should be forwarded to Zscaler, using either GRE or IPsec tunnels (with NULL encryption).

The following example topology shows a Cisco SD-WAN network with two transports (MPLS and Internet) and the SD-WAN controllers reachable through the Internet cloud. Two branch sites are shown with a datacenter site. IPsec tunnels are built between each WAN Edge router at each site for corporate traffic. GRE or IPsec primary and secondary tunnels are built to Zscaler for direct Internet traffic.

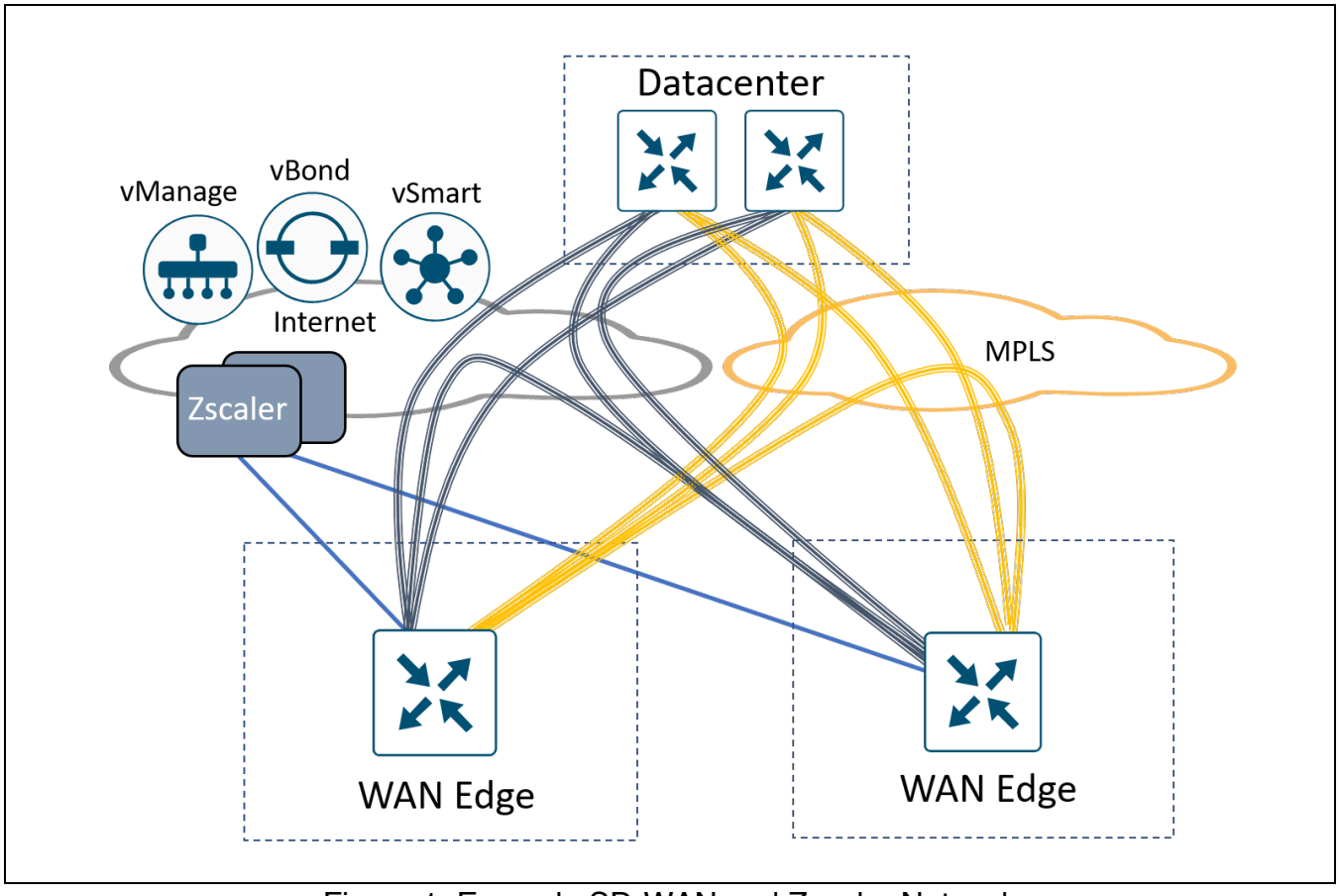


Figure 1: Example SD-WAN and Zscaler Network

1.7.1 GRE and IPsec Tunnels

Zscaler supports GRE and IPsec tunnels. For GRE, traffic is encapsulated in an IP packet using IP protocol type 47. Using GRE with Zscaler requires a static IP address.

IPsec, using IKE, does not require a static IP address, and instead relies on a FQDN for IKE ID versus an IP address. Unlike typical site-to-site deployments of IPsec which encrypt traffic, when using IPsec to Zscaler for Internet-destined traffic, NULL encryption is to be used. IKE uses UDP port 500, or in the case of NAT traversal, UDP 4500. Traffic is encapsulated in an ESP packet using IPv4 protocol 50 (and is non-encrypted in this case).

A GRE or IPSec tunnel is defined by a source IP address/interface and a destination IP address pair. Multiple tunnels can exist that reference the same source IP address, but each must have a unique destination IP address.

1.7.2 Tunnel Liveliness

1.7.2.1 **Keepalives**

GRE Tunnel Keepalives for GRE tunnels and Dead Peer Detection (DPD) for IPsec tunnels are ways for the local router to determine whether the remote end of the tunnel is reachable. In the case of GRE tunnels, a keepalive packet is sent and looped back to the sender from the remote end. The default timers are one keepalive sent every 10 seconds, and after 3 retries, the tunnel is declared down.

Note: If the router sits behind a NAT device, GRE tunnel keepalives are not passed, so keepalives must be disabled in this case. Keepalives are disabled by specifying 0 for the keepalive interval and 0 for the retry value.

In the case of IPsec tunnels, Dead Peer Detection is used, which can be either periodic or on-demand. Periodic works similarly to keepalives, where a packet is sent at every interval and the remote end sends an acknowledgement. The default timers are one DPD packet sent every 10 seconds, and after 3 retries, the tunnel is declared down. In the case of on-demand, packets are only sent when traffic is being sent but no traffic is being received.

Note: IKEv2 DPD timing changed for vEdge routers starting in 18.4.303 code. Instead of DPD being sent at every constant interval, the interval gets longer for each retransmitted DPD packet. The interval is calculated for retransmission attempt N using the formula [interval*1.8 ^(N-1)], so for an interval of 10 with a retry value of 3, the retransmission attempt is 10 seconds for the first retry packet, 18 seconds for the next retry packet, and 32.4 seconds for the third retry packet.

Note: vEdge routers currently support only periodic DPD. On-demand DPD is currently the default for IOS XE SD-WAN routers.

Note: Zscaler requests that GRE Keepalives and DPD packets are sent no more than one every 10 seconds.

1.7.2.2 **Layer 7 Health Checks**

GRE Keepalives and Dead Peer Detection can validate whether the network path is up between the tunnel source and destination, but they cannot verify whether a particular service or application is up and operational through the tunnel and ZEN node.

Layer 7 health checking allows you to monitor performance based on an HTTP request and response and allows you to failover to an alternate tunnel based on the results.

A tracker is defined globally which defines an HTTP URL. The endpoint in the URL must respond to an HTTP request and return a 200 OK response in order for the tracker to be in an UP state. The tracker is attached to a tunnel, where the software periodically sends HTTP requests over that tunnel. The HTTP requests are directed to the destination tunnel interface IP address, which is used as an HTTP proxy for the requests. DNS for the URL in the request is performed by the HTTP proxy endpoint. By default, requests are sent every 60 seconds but can be set to a minimum interval of 10 seconds. If there is no response, three requests are resent before the tunnel is declared down and the route is withdrawn to the tunnel. The tracker components also measure latency and compare it with the SLA threshold defined under the tracker configuration. If latency exceeds the configured SLA, the tunnel interface is also marked as down and the routes withdrawn to the tunnel.

Note: To health-check the application stack of the Zscaler node, Zscaler recommends not performing L7 health checks to commonly visited websites, but instead recommends using the following URL for the tracker, which is not publicly accessible, but only reachable through a Zscaler tunnel:

http://gateway.<zscaler_cloud>.net/vpntest

Note: Only vEdge routers support L7 health checks at this time, beginning in version 19.3.0. L7 health checking is also supported for transport-side tunnels only, not for service-side tunnels.

1.7.3 Transport-side vs Service-side Tunnels

Tunnels can be built either as transport-side or service-side tunnels. With transport-side tunnels, the tunnel resides entirely in VPN 0, and with service-side tunnels, the tunnel destination and/or source definitions are reachable from VPN 0, but the tunnel interface itself is configured in the service VPN.

Service-side tunnels allow you to define a different tunnel per VPN and allow you to keep your VPN traffic, such as guest and corporate traffic, separated into different tunnels. For transport-side tunnels, all VPN traffic can use the same tunnel, simplifying the configuration.

Note: For IOS XE SD-WAN routers, only service-side IPsec tunnels are supported at this time.

1.7.4 Traffic Redirection

Once the GRE or IPSec tunnel is built, there are two ways to redirect traffic to the tunnel:

- With a static route to rely on destination-based routing, which is typically a default route where all internet-bound traffic is sent.
- With a centralized data policy which allows you to customize the traffic sent to the Zscaler service.

1.7.4.1 **Static Route**

Transport-side Tunnels (applies to vEdge only at this time)

For transport-side tunnels, the source and destination and the GRE or IPsec tunnel interface itself resides in the transport VPN (VPN 0). To direct traffic from a service VPN, a route should be installed in the service VPN which points to the GRE or IPsec interface in VPN 0 as the next hop. In the vManage GUI, this route is described as a GRE Route or IPsec Route in the VPN feature template.

```
ip gre-route 0.0.0.0/0 vpn 0 interface gre1 gre2
ip ipsec-route 0.0.0.0/0 vpn 0 interface ipsec1 ipsec2
```

With these static routes, the GRE or IPsec tunnels are implemented as active/standby only. Only when the first interface is removed from the route table through GRE keepalive, DPD, or L7 health-check failures will the second interface become active.

Note: When using static routes specifying the interface as the next hop, GRE tunnel interfaces can be IP unnumbered, but IPsec tunnels do not come up and active unless an IP address is assigned to the tunnel interface.

Service-side Tunnels

There are multiple ways to set up service-side tunnels. One way is for the source and destination of the tunnel to reside in the transport VPN (VPN 0). The tunnel interface itself resides in the service VPN. To direct traffic from a service VPN, a route is installed in the service VPN and the next-hop IP address becomes the remote end of the tunnel. The next-hop address is already reachable from the service VPN, so nothing more needs to be configured.

```
vpn 1
interface ipsec1
ip address 11.1.1.1/30

interface ipsec2
ip address 11.1.2.1/30

ip route 0.0.0.0/0 11.1.1.2
ip route 0.0.0.0/0 11.1.2.2
```

In this configuration, the tunnels are active/active and traffic can load share between them based on a hash of the flow. You can tag one route with a higher admin distance so that it becomes a backup route instead of using equal cost paths to diverse Zscaler nodes. In this case, interface tunnels are required to be assigned an IP address in order to configure the service VPN IPv4 route needed.

Note: In vManage when defining a route in the service VPN, you cannot specify an interface (gre1, ipsec1) for a next-hop when the tunnel itself resides in the service VPN because this route next-hop is only valid when the tunnel itself resides in the transport VPN (VPN 0).

Note: Service-side tunnels, where the tunnel interface itself resides in the service VPN, but the source and destination of the tunnel resides in the transport VPN is supported only for IPsec tunnels for both vEdge and IOS XE SD-WAN routers.

Note: In IOS XE SD-WAN, commands get translated from vManage into IOS XE-compatible commands. In IOS XE SD-WAN, VPN 0 is the global table, the vrf keyword is used instead of vpn, and gre and ipsec tunnel interfaces get translated into a Tunnel10000x format when the configuration is pushed to the router.

1.7.4.2 **Policy**

Traffic can be directed to Zscaler using a centralized policy instead of using static routes. In order to direct data traffic to a tunnel using a centralized data policy, you first advertise the service in the service VPN, and you then create a centralized data policy on the vSmart controller to forward matching traffic to that service. This utilizes service chaining to advertise a service so that other WAN Edge routers can utilize the service even if they are not local. See for additional information:

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/System-Interface/systems-interfaces-book/configure-interfaces.html#id_113930

Note: The IOS XE SD-WAN router currently does not support service chaining. As a workaround, a data policy using matches and setting the next hop as the remote end of the tunnel can be configured instead.

1.7.5 Cisco SD-WAN Configuration Requirements

GRE

To set up a GRE tunnel, you need to minimally configure a source for the tunnel, which can be an IP address or source interface of the SD-WAN router, as well as a tunnel destination, which is the Zscaler node. For a transport-side tunnel, the source of the tunnel is typically the port connected to the Internet transport in VPN 0, which is reachable to the Zscaler node. This address needs to be a publicly-routable IP address or the SD-WAN router needs to sit behind a NAT device that can NAT the source IP address in order to get a response back from the Zscaler node. Note that because the Zscaler GRE tunnel configuration is a manual provisioning process at this time, this source IP address must be a static IP address and cannot be changed. DHCP can only be used if the router is guaranteed to receive the static IP address that's been provisioned in Zscaler – a random IP address cannot be obtained dynamically through DHCP. Once the tunnel is up, user traffic sent over it to Zscaler does not need to be subjected to NAT and can be sent sourced as private (RFC 1918) addresses.

The IPv4 address for the tunnel is optional for transport-side tunnels since you are using an interface as the next-hop in the route.

In the vManage GUI, you specify the name of the tunnel, which is gre[1..255], and this name can be referenced in the GRE route if needed.

GRE Keepalives are turned on by default with an interval value of 10 seconds and 3 retries. Note that if the router sits behind a NAT device, keepalives must be disabled, as they do not pass through the NAT device. To disable keepalives, set the **Interval** and **Retries** value to 0. To prevent fragmentation, set the **IP MTU** to 1476 bytes and the **TCP MSS** to 1436 bytes to account for the GRE packet overhead (24 bytes).

Note: GRE is supported only by the vEdge router at this time.

IPsec

To set up an IPsec tunnel, you need to configure a source for the tunnel, which can be an IP address or source interface of the SD-WAN router, as well as a tunnel destination, which is the Zscaler node. The tunnel destination can be an IP address or FQDN for a vEdge router and only an IP address at this time for the IOS XE SD-WAN router. For a transport-side tunnel, the source of the tunnel is typically the port connected to the Internet transport in VPN 0, which is reachable to the Zscaler node. This address needs to be a publicly-routable IP address or the SD-WAN router needs to sit behind a NAT device that can NAT the source IP address in order to get a response from the Zscaler node. Note that because the Zscaler IPsec tunnel configuration is a dynamic provisioning process, this source IP address can be a static IP address or it can be obtained dynamically through DHCP.

The IPv4 address for the tunnel is necessary for both vEdge and IOS XE SD-WAN routers. In the vManage GUI, you specify the name of the tunnel, which is ipsec[1..255], and this name can be referenced in the IPsec route if needed. Note that in IOS XE SD-WAN code, this tunnel name gets translated into a different label in the command line interface (CLI) (Tunnel100001, for example).

Dead Peer Detection is turned on by default with an interval value of 10 seconds and 3 retries. Encryption settings are a balance between security and performance. The following parameters indicate the preferred Zscaler settings:

Crypto Phase I

- IKEv2
- Encryption AES256 with integrity SHA2-256 or SHA1-128
- Diffe Hellman Group 2.
- Authentication = Pre-shared keys. Note that the pre-shared key MUST be at least 16 characters or more starting in vEdge software version 18.4 or higher.

Crypto Phase II

- Mode = Tunnel mode only
- Null encryption with integrity of SHA1-128 or MD5
- Perfect Forward Secrecy disabled.

- The IKE ID for local end point can be an IP address or FQDN, but the same value must be configured in the VPN authentication profile on the Zscaler admin portal.

- The IKE ID for remote end point should be the IP address of the Zscaler tunnel destination.

1.6.7 Cisco SD-WAN Considerations

vEdge (version 19.2.099 or 19.3.0)

- For the vEdge router, GRE service-side tunnels where the tunnel source and destination reside inside VPN 0 are not supported. GRE transport-side and IPsec transport-side and IPsec service-side tunnels are supported.

- Starting in version 18.4 and greater, IPsec tunnels now require pre-shared key lengths of 16 characters or greater. ISAKMP will not establish unless this condition is met.

- IPsec tunnel interfaces need to be IP numbered using IPv4 IP address space that does not need to be advertised outside of the router. If the tunnels do not have an IP address, the tunnels will not become operational and will not appear as valid next-hops in the routing table.

- L7 health checks are supported on vEdge transport-side tunnels (not on service-side tunnels), starting in the 19.3 version of code.

IOS XE SD-WAN (version 16.12.1e or 16.12.1r)

- For IOS XE SD-WAN routers, only service-side IPsec tunnels are supported at this time (GRE tunnels and transport-side IPsec tunnels are not supported).

- L7 health checking is not yet supported

- You cannot use FQDN to specify the destination of an IPsec tunnel, you must use an IP address.

- vManage does not push local and remote-id fields for IPsec tunnels until vManage version 19.2 and above.

- If you have more than one TLOC/transport and two tunnels with Zscaler, then static host routes to the tunnel destinations are required in addition to the default routes already defined. As an example, for the Internet transport where the Zscaler tunnels can be reached, the following routes in VPN 0 are defined:

```
ip route 0.0.0.0 0.0.0.0 207.47.45.81
ip route 104.129.194.39 255.255.255.255 207.47.45.81 (tunnel 1 destination host route)
ip route 199.168.148.132 255.255.255.255 207.47.45.81 (tunnel 2 destination host route)
```

- The tunnel interfaces need to be IP numbered using IPv4 link-local IP address space that does not need to be advertised outside of the router. If the tunnels do not have an IP address, they will not appear as valid next-hops in the routing table.

- In earlier versions of software, the IKE profiles used “email” for their local identity instead of “fqdn” as the command parser did not allow the “fqdn” option.

- In this revision of IOS XE software, an implicit ACL exception is not automatically configured to allow IPsec traffic. To allow this traffic, an ACL must be configured on the interface inbound to allow this traffic. You can match on ISAKMP (UDP port 500 or 4500 if NATed) as well as ESP protocol 50 so data plane traffic can be allowed through. Alternatively, you can just match the source IP address of the Zscaler tunnel.

- Disabling IKE Config Exchange is required due to Zscaler BUG-58687. By default, the IOS XE SD-WAN router enables the CFG_Request in the IKE_AUTH request, which results in the responder (Zscaler) pushing a random IP address in the IKE_AUTH reply. This causes traffic over the newly-established IPSec SAs to fail. In vManage version 19.2.1 (together with IOS XE SD-WAN IOS version 16.12.1r), the command is disabled automatically by vManage. Before the 19.2.1 version and in the 19.3.0 version of vManage, this command needs to be configured manually. Ensure the IOS XE SD-WAN router is in CLI mode and add the following configuration (you need to enable the command first, then disable it). This command does not survive between router reloads.

```
WAN_EdgeB(config)# crypto ikev2 profile if-ipsec1-ikev2-profile
WAN_EdgeB(config-ikev2-profile)# config-exchange request
WAN_EdgeB(config-ikev2-profile)# commit
Commit complete.
WAN_EdgeB(config-ikev2-profile)# no config-exchange request
WAN_EdgeB(config-ikev2-profile)# commit
Commit complete.
```

  You can try a `clear crypto session` command if the command is entered after IKE was negotiated.

1.7.5.1 What is covered in this guide

This guide demonstrates:

- Transport-side GRE and IPsec tunnels for the vEdge router
- Service-side IPsec tunnels for the IOS XE SD-WAN router (though supported by the vEdge router also)
- How to direct traffic to zScaler using a default route
- How to configure L7 Health Checks for the vEde router

This guide focuses on configurations built from vManage for both vEdge and IOS XE SDWAN routers. Go to Appendix 7 to build base configurations for both router types using vManage. After IPsec tunnels are built using vManage, workarounds for tunnel restrictions on IOS XE SD-WAN are shown. See Appendix 7 for CLI-based configurations.

1.8 Lab Topology and Configuration Overview

This document is based on the following lab topology. There are two branch offices each with a single WAN Edge router. Branch A contains a vEdge router (WAN Edge A) and Branch B contains an IOS XE SD-WAN router (WAN Edge B). WAN Edge A is used to establish dual GRE or IPsec tunnels to diverse Zscaler locations, while WAN Edge B is used to establish dual IPsec tunnels to the same diverse Zscaler locations. The Zscaler nodes are accessible over the Internet transports. In this document, transport-side tunnels are deployed on WAN Edge A, and service-side IPsec tunnels are deployed on WAN Edge B.

Note: IOS XE SD-WAN routers currently only support service-side IPsec tunnels.

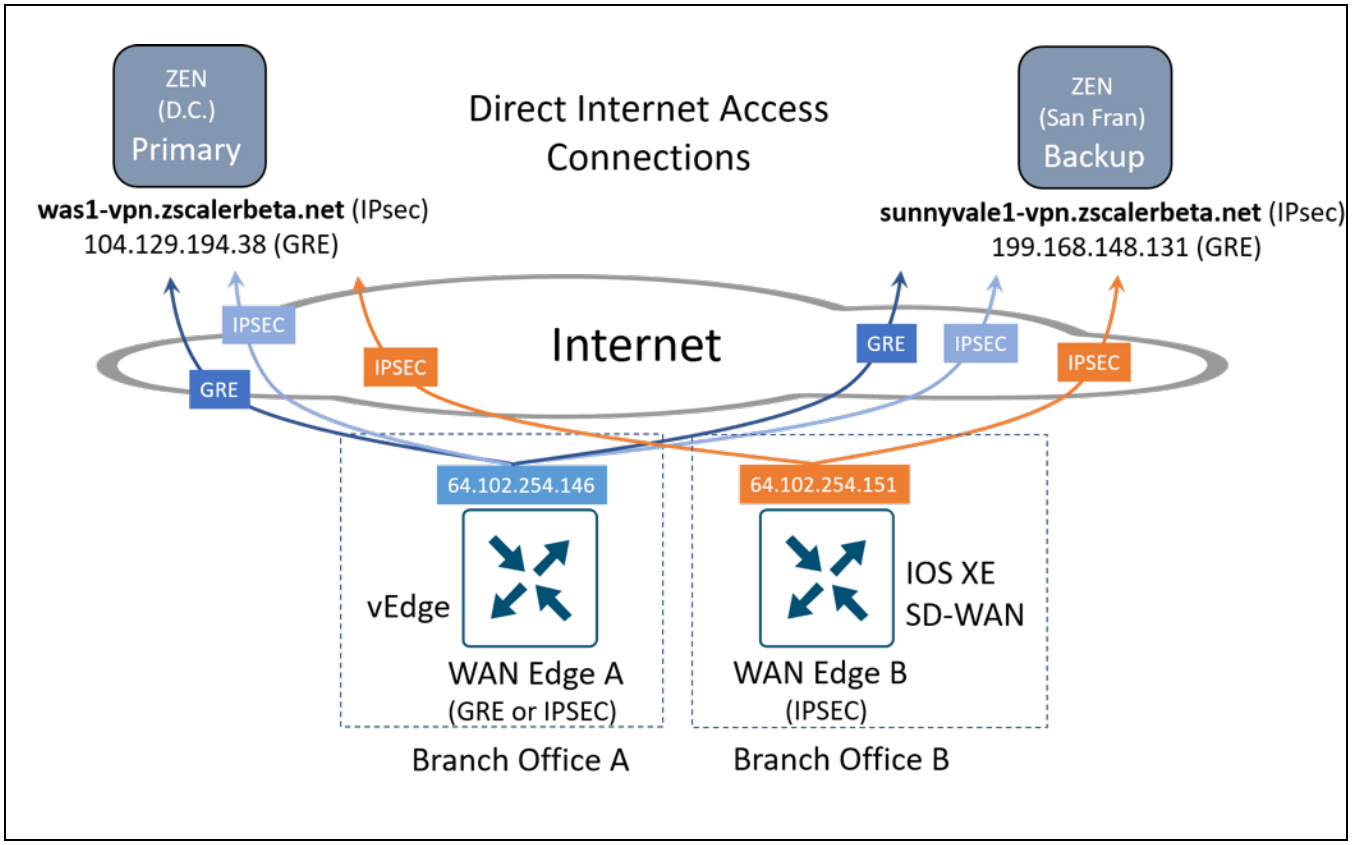


Figure 2: Lab Topology

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 are used:

WAN Edge A GRE	Tunnel Source	Tunnel Destination	Router Tunnel IP
Primary Tunnel	64.102.254.146	104.129.194.38	172.17.12.217/30
Secondary Tunnel	64.102.254.146	199.168.148.131	172.17.12.221/30
WAN Edge A IPsec	**Tunnel Source**	**Tunnel Destination**	**Router Tunnel IP**
Primary Tunnel	64.102.254.146	was1-vpn.zscalerbeta.net 104.129.194.39	11.1.1.1/30
Secondary Tunnel	64.102.254.146	sunnyvale1-vpn.zscalerbeta.net 199.168.148.132	11.1.2.1/30
WAN Edge B IPsec	**Tunnel Source**	**Tunnel Destination**	**Router Tunnel IP**
Primary Tunnel	64.102.254.151	was1-vpn.zscalerbeta.net 104.129.194.39	11.2.1.1/30
Secondary Tunnel	64.102.254.151	sunnyvale1-vpn.zscalerbeta.net 199.168148.132	11.2.2.1/30

Figure 3: ZIA Tunnel Configuration Details

Note: The GRE tunnel details are provisioned manually by Zscaler. The IPsec tunnel is dynamically provisioned and no manual provisioning is needed. The router IP addresses for IPsec tunnels are locally significant so any subnet can be used. As such, you are able to ping to the other side of the GRE tunnel, but with IPsec, you won't be able to.

2 Configuring Zscaler Internet Access (ZIA)

2.1 Overview

Location

When you provision a GRE tunnel or configure an IPsec tunnel, you must tie it to a "*Location*" in the Zscaler Admin Portal. *Locations* identify the various networks from which your organization sends its Internet traffic. It can be defined in many ways, but many ZIA users define a location as a branch office. The amount of locations can scale to the largest of Enterprise networks. Multiple GRE and IPsec tunnels can be part of one location.

GRE

A GRE tunnel requires a manual provisioning process, so a tunnel source static IP address which is publicly routable from your SD-WAN device is required and a support case must be opened to provision it. When it is provisioned, a primary and a secondary tunnel are both provisioned. You are provided with a destination IP address for both primary and secondary tunnels, and /30 IP addresses to allocate to the tunnel interfaces themselves if needed. Note that GRE tunnels can be configured as unnumbered. The source static IP address is also configured in the Zscaler Admin Portal so you can associate it with a location.

To complete the GRE tunnel configuration in Zscaler, in the Zscaler Admin Portal, you select or create a location and choose the source static IP address in order to link the GRE tunnel with the location.

IPsec

An IPsec tunnel does not require pre-provisioning. A dynamic IP address can be used as the source. Please look in the Appendix (Zscaler Resources) for the IPSec VIP IP addresses to each Zscaler datacenter, for each Zscaler cloud.

To complete the IPsec configuration in Zscaler, in the Zscaler Admin Portal, you must first configure the VPN credentials. On the VPN credentials page, you configure the authentication type of the IPsec tunnel as an FQDN (recommended) or an IP address. This defines the remote ID of the IPsec tunnel from the Zscaler perspective.

On the Cisco SD-WAN router, this translates to the local ID, so ensure the values match. If you use an IP address instead as the authentication type, the source IP address of the tunnel must exist in the Admin Portal, which can be done by opening a support case. On the VPN credentials page, you also configure the pre-shared key. This pre-shared key must also match on both sides of the tunnel. You then select or create a location and configure the VPN

Credentials (either an FQDN or IP address under the VPN Credentials drop-down box) in order to link the VPN credentials profile with the location.

Note: When you make configuration changes in the Zscaler Admin Portal, activation is required before the changes take place.

2.2 Logging into ZIA

Figure 4: Log into Zscaler

First, set up the Zscaler side of this service.

- 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.

2.3 Configuring ZIA for GRE Tunnel

2.3.1 Provision GRE Tunnel

GRE tunnels need to be provisioned manually. If you do not yet have your GRE Tunnel details, please open a support ticket. You will need to provide a publicly-routable source IP address. You are provided with a provisioned primary and secondary GRE tunnel. The instructions to open a Zscaler support ticket for GRE provisioning is in section 5, “Requesting Zscaler Support”

2.3.2 Navigate to Locations

After logging in, add a location if one is not present for GRE access to 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 **Locations**.

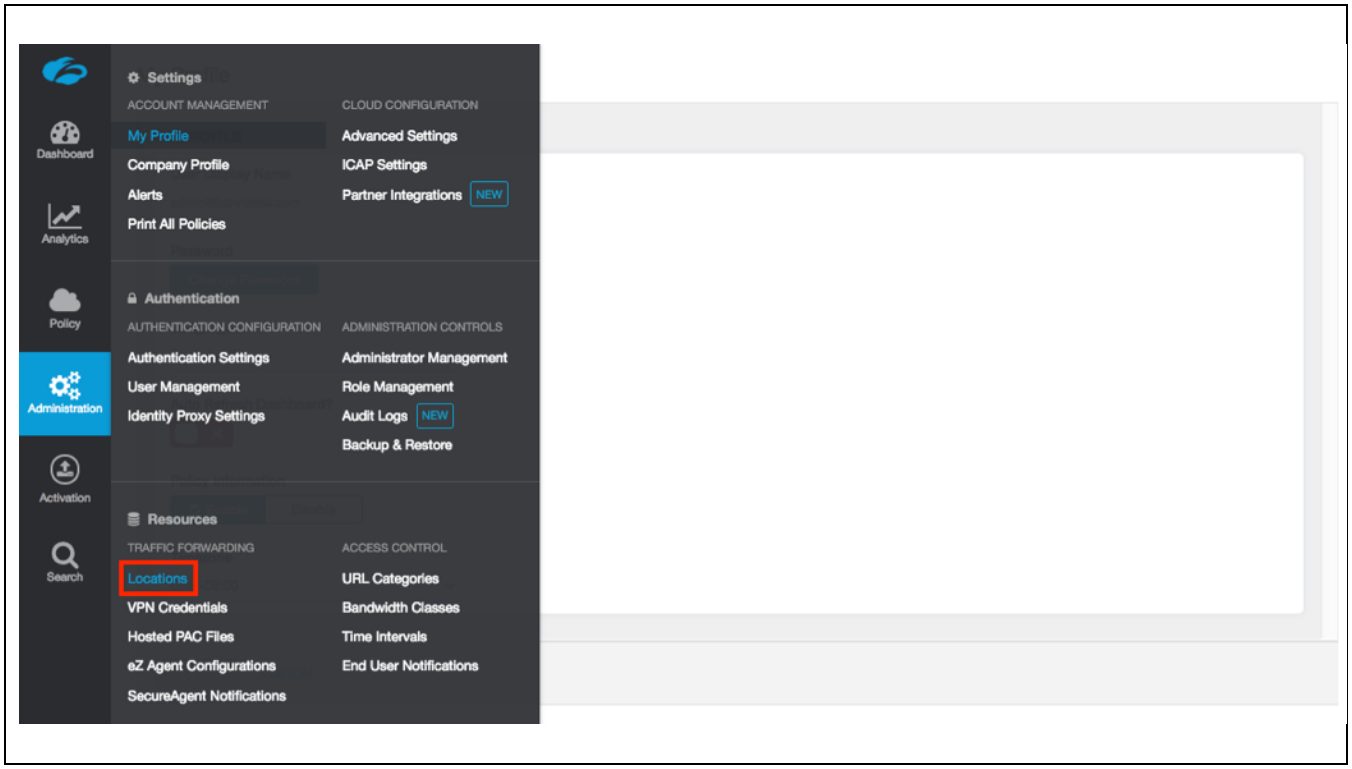


Figure 5: Navigate to Locations

2.3.3 Add a Location

In Figure 6, 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 any location that is listed.

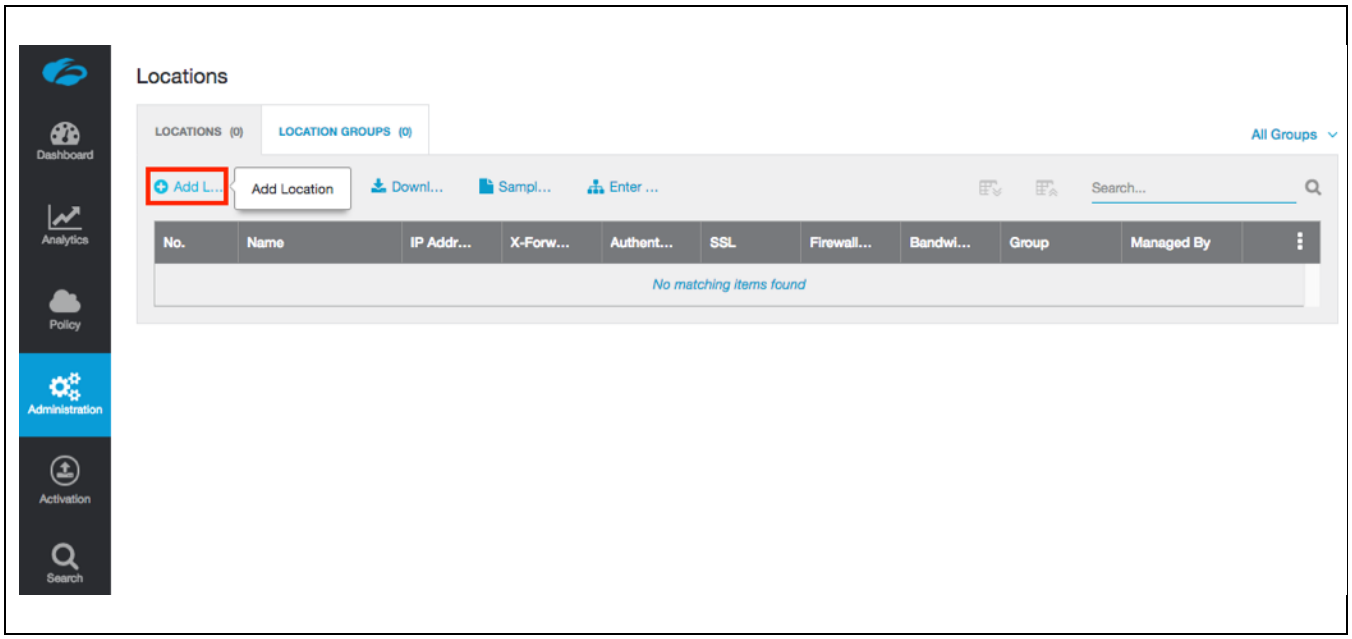


Figure 6: Add a Location

2.3.4 Enter Location Data

The data in the red box in Figure 7 must be entered. Fill in **Name, State/Province, Country, Time Zone**, and under **Addressing**, under **Static IP Addresses**, pick the source IP address of your GRE tunnel.

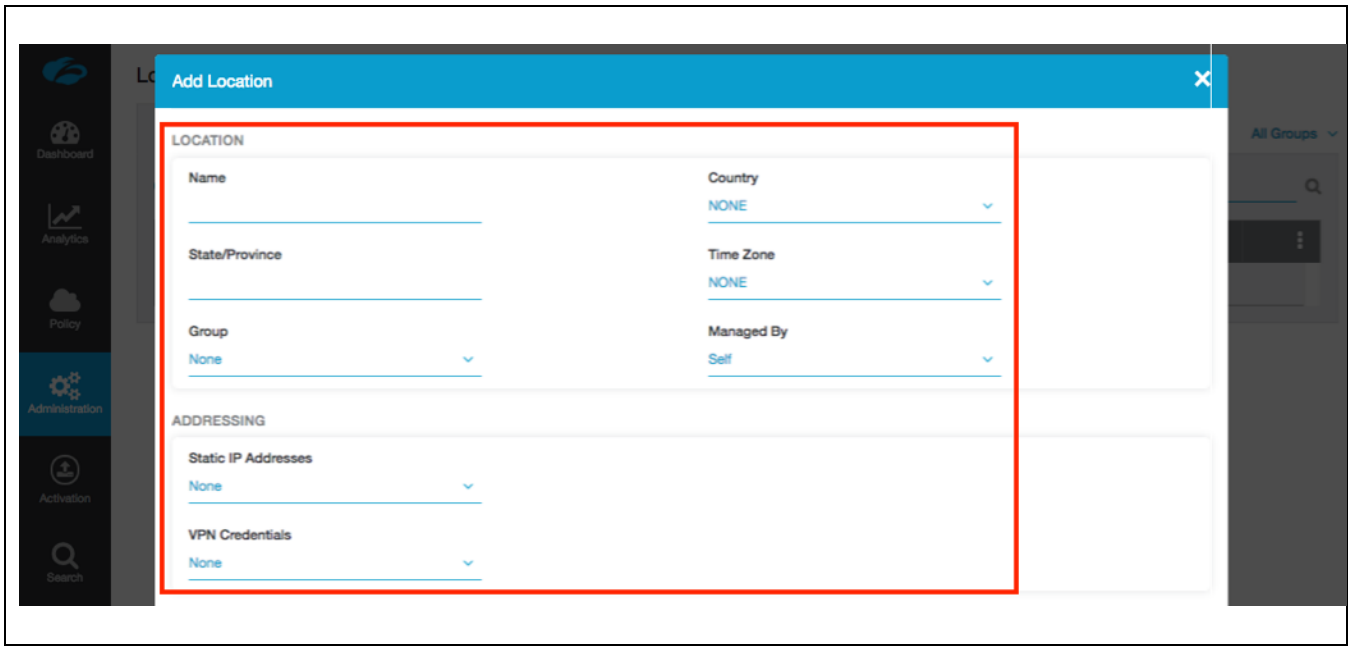


Figure 7: Enter Location Data

Note: If the **Static IP Addresses** drop-down box 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.

2.3.5 Verify Location Information and Save

Now that you have entered your location information, you are ready to save your new location. Please click **Save** to continue.

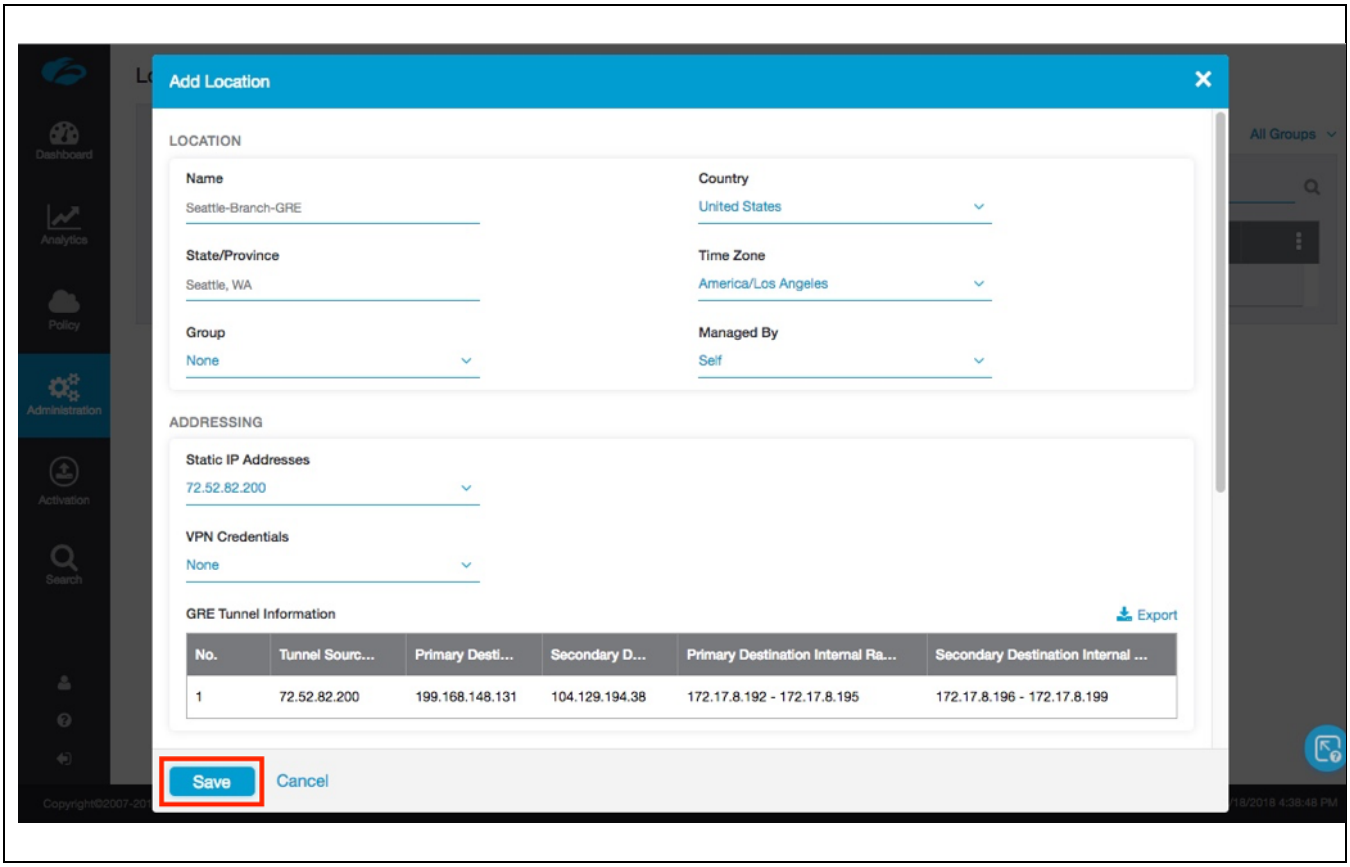


Figure 8: Verify Location Information and Save

2.3.6 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.

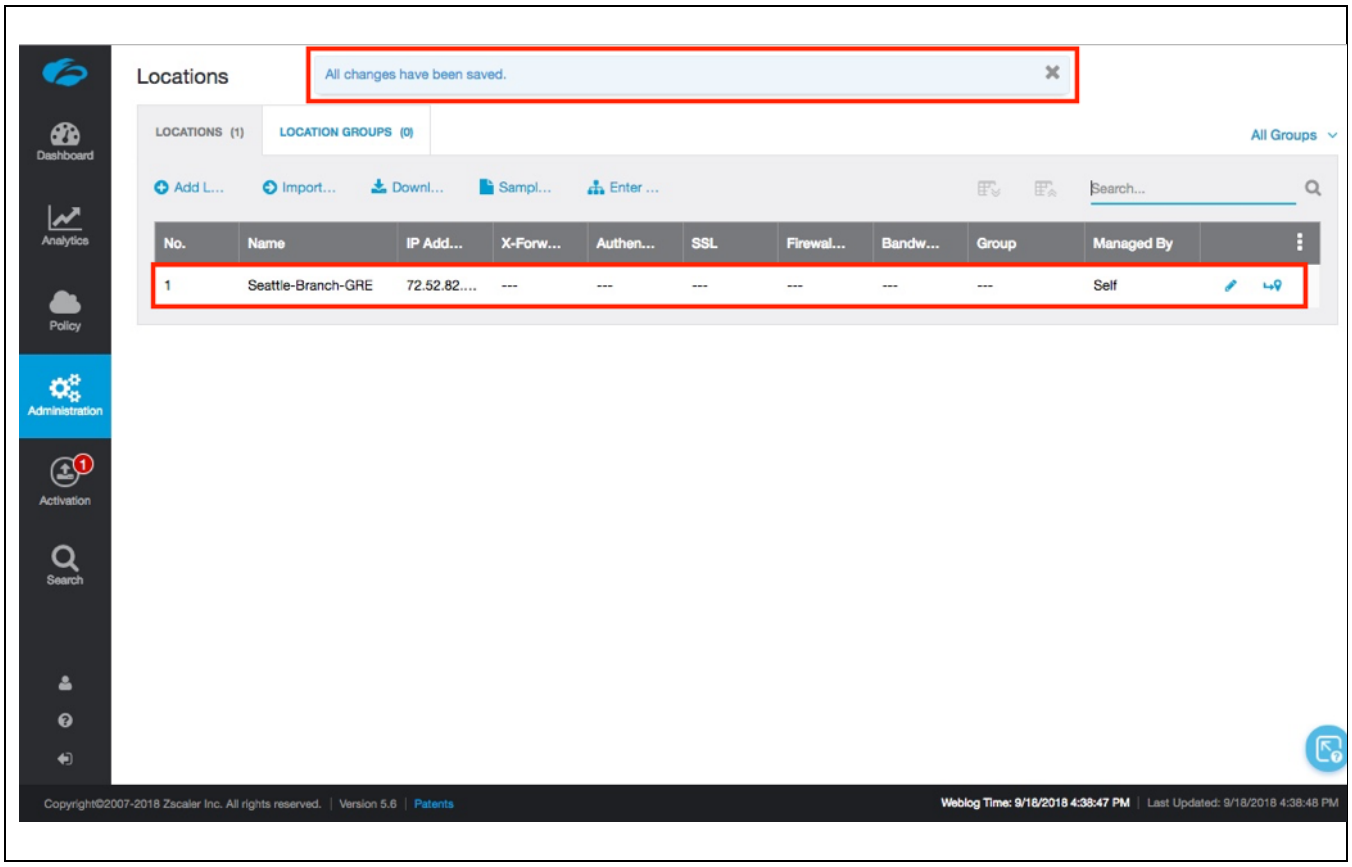


Figure 9: Confirm Changes Have Been Submitted

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.

2.3.7 Activate Changes

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

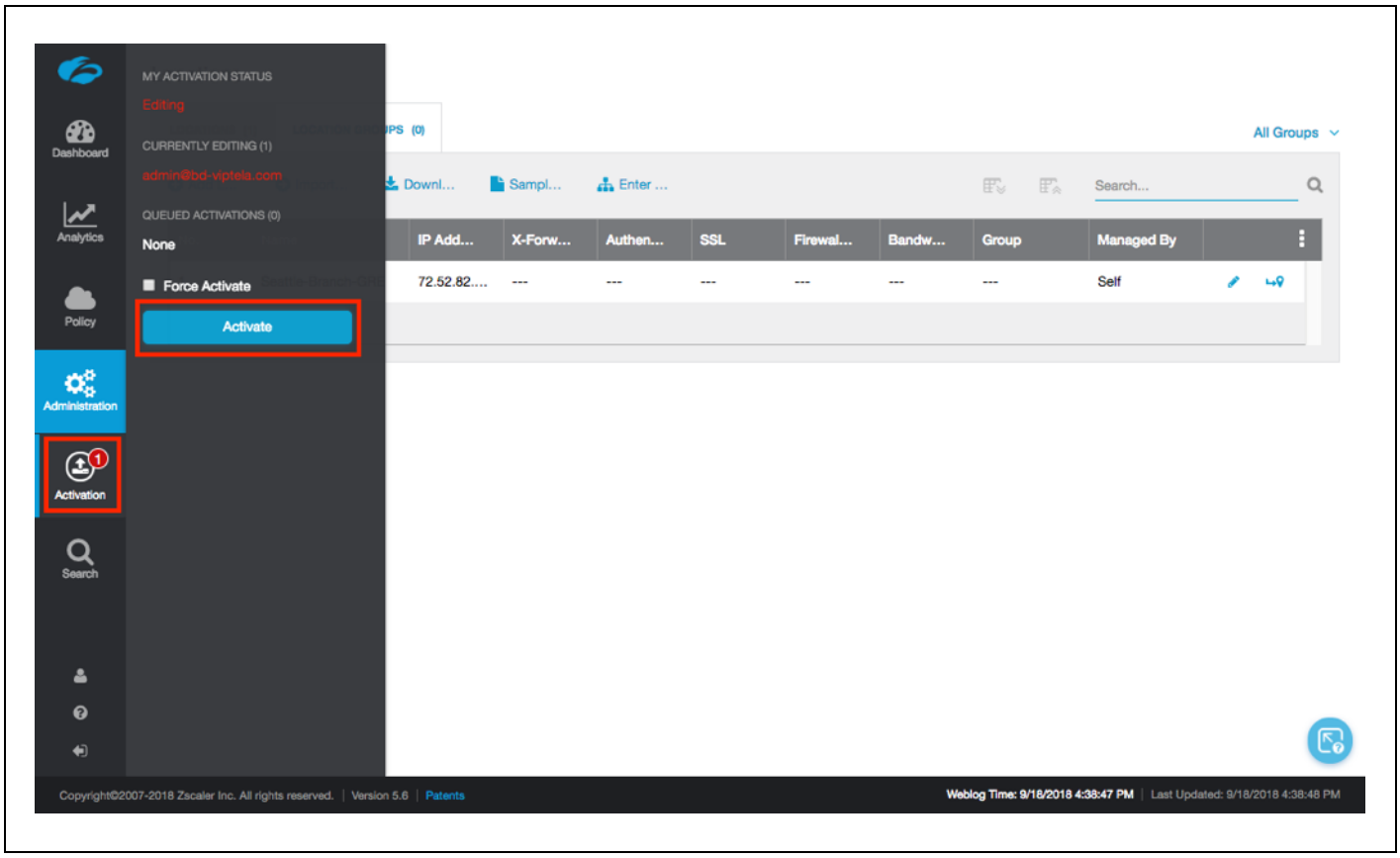


Figure 10: Activate Changes

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 Configuring ZIA for IPsec Tunnel

2.4.1 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**.

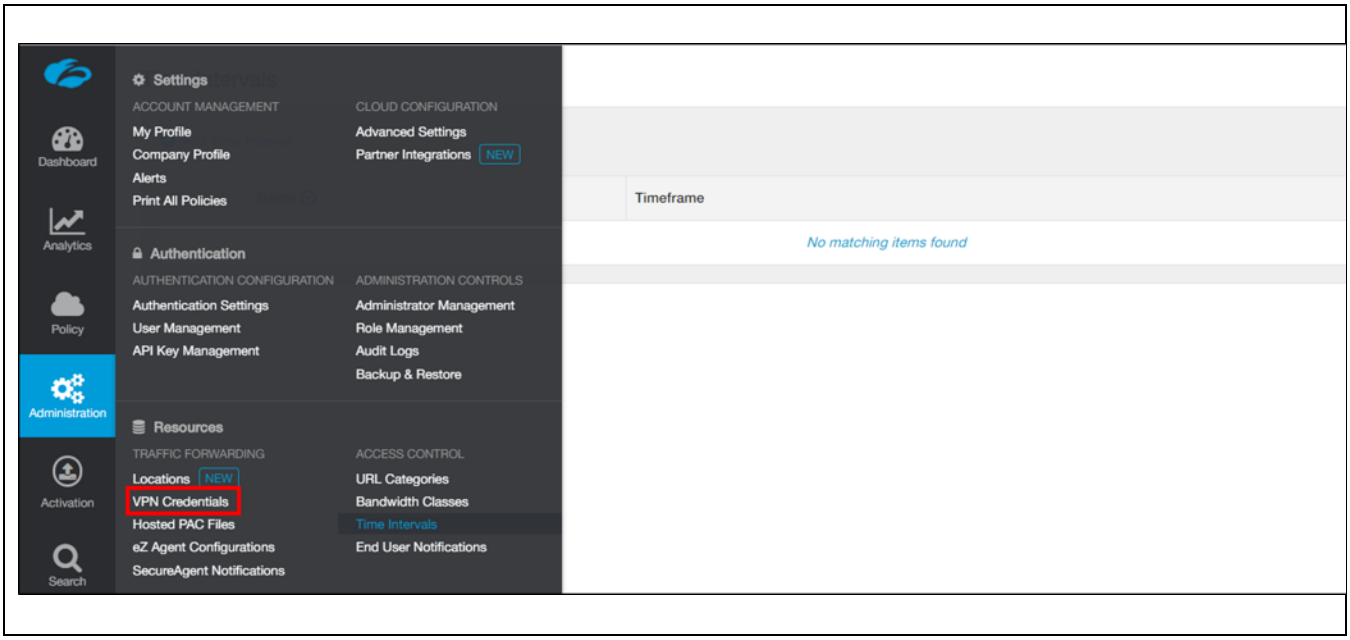


Figure 11: Navigate to VPN Credentials

2.4.2 Add a VPN Credential

In Figure 12, 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 12: Adding a VPN Credential

2.4.3 Enter VPN Credential Data

In Figure 13, 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.

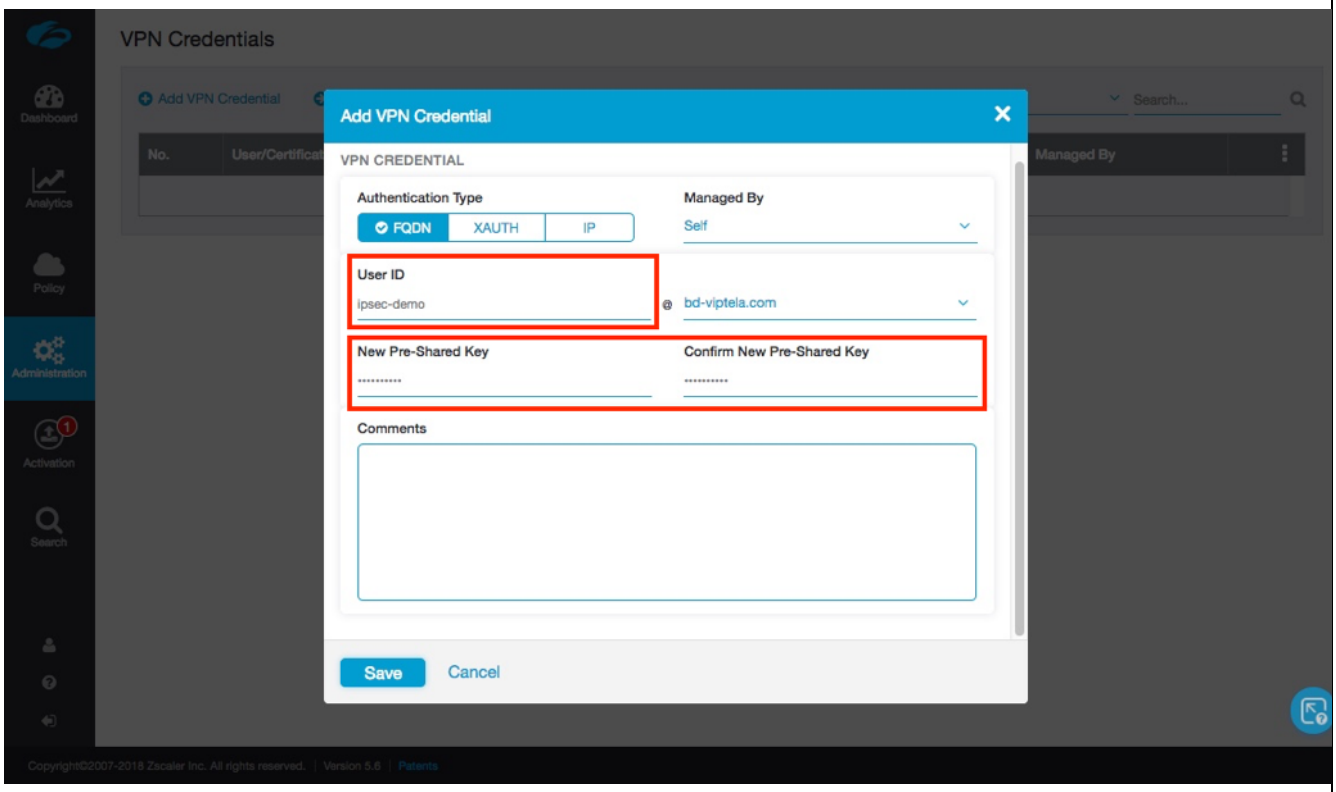


Figure 13: Enter VPN Credential Data

2.4.4 Verify VPN Credential

In Figure 14, 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.

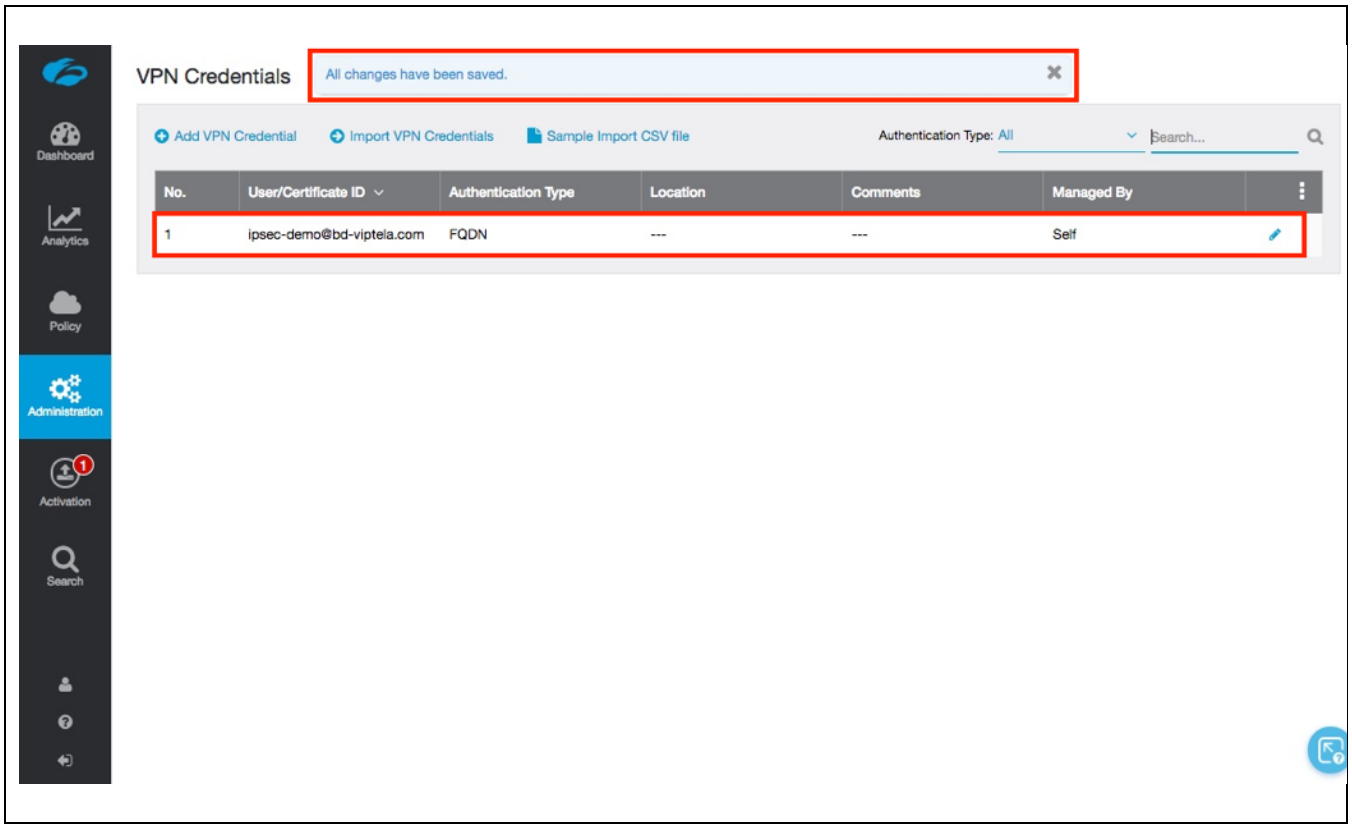


Figure 14: Verify Location Information and Save

2.4.5 Navigate to Locations

After the VPN credential has been added, it needs to be linked to a location. Add a location if one is not present for IPSec access to 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 **Locations**.

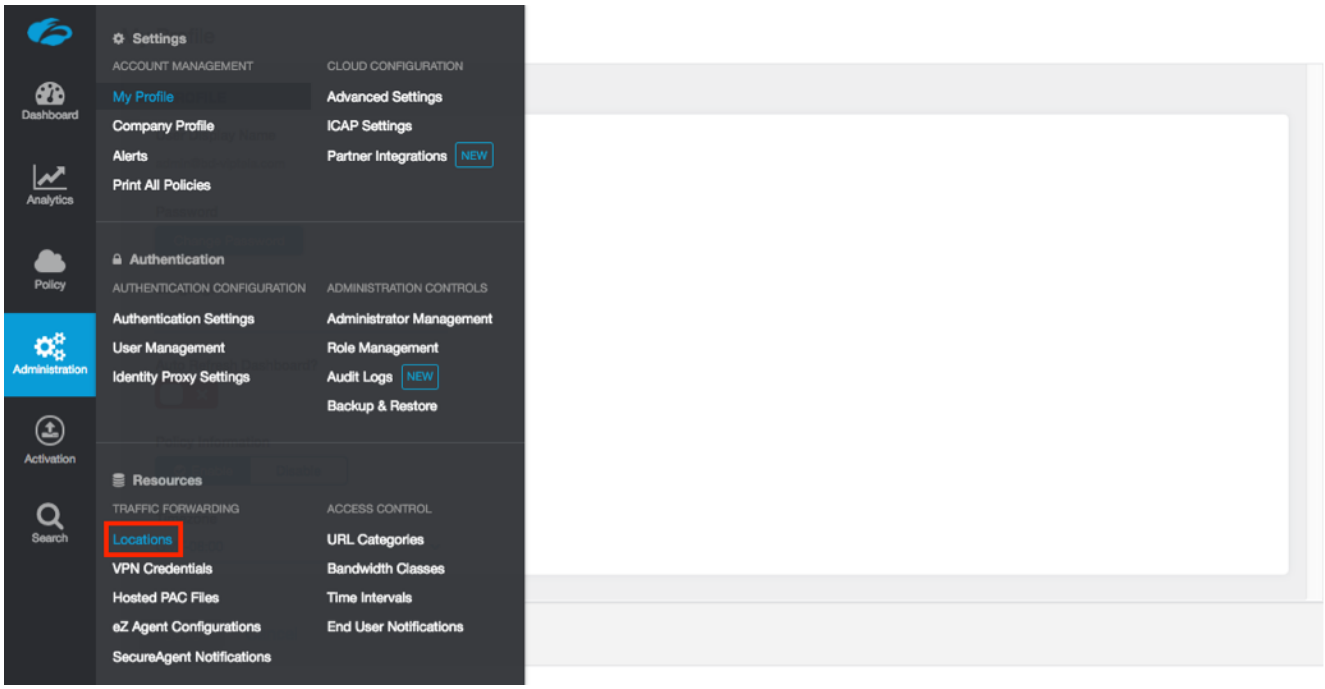


Figure 15: Navigate to Locations

2.4.6 Add a Location

In Figure 16,, 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 16: Add a Location

2.4.7 Enter Location Data

In Figure 17, 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. Lastly, under **VPN Credentials**, select the VPN credential you configured in the prior steps. Once you select the drop down, the screen in the next section will appear.

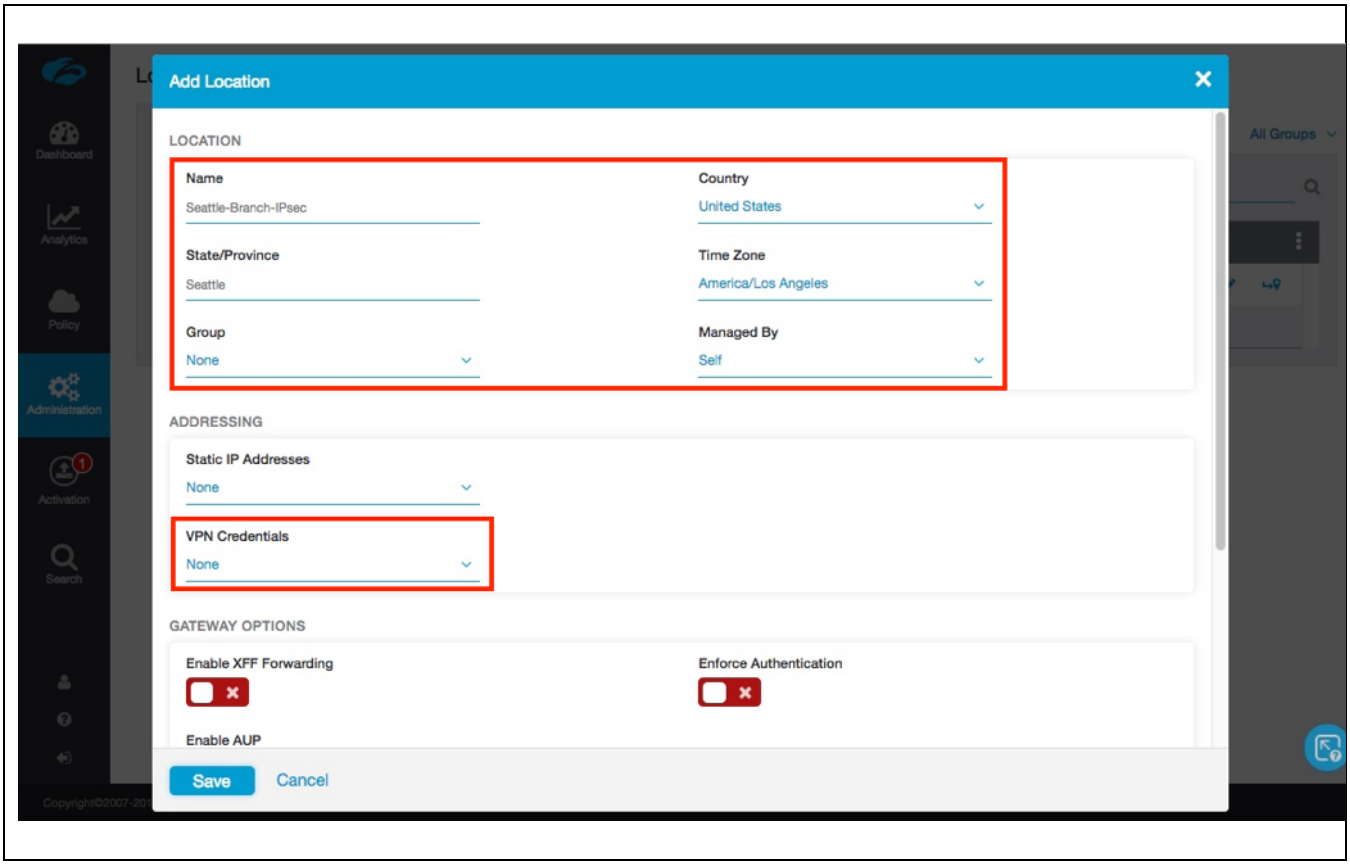


Figure 17: Enter Location Data

2.4.8 Add VPN Credential to Location and Save

In Figure 18, you should see the VPN Credential you configured in the prior section. Select it and click **Save**. 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.

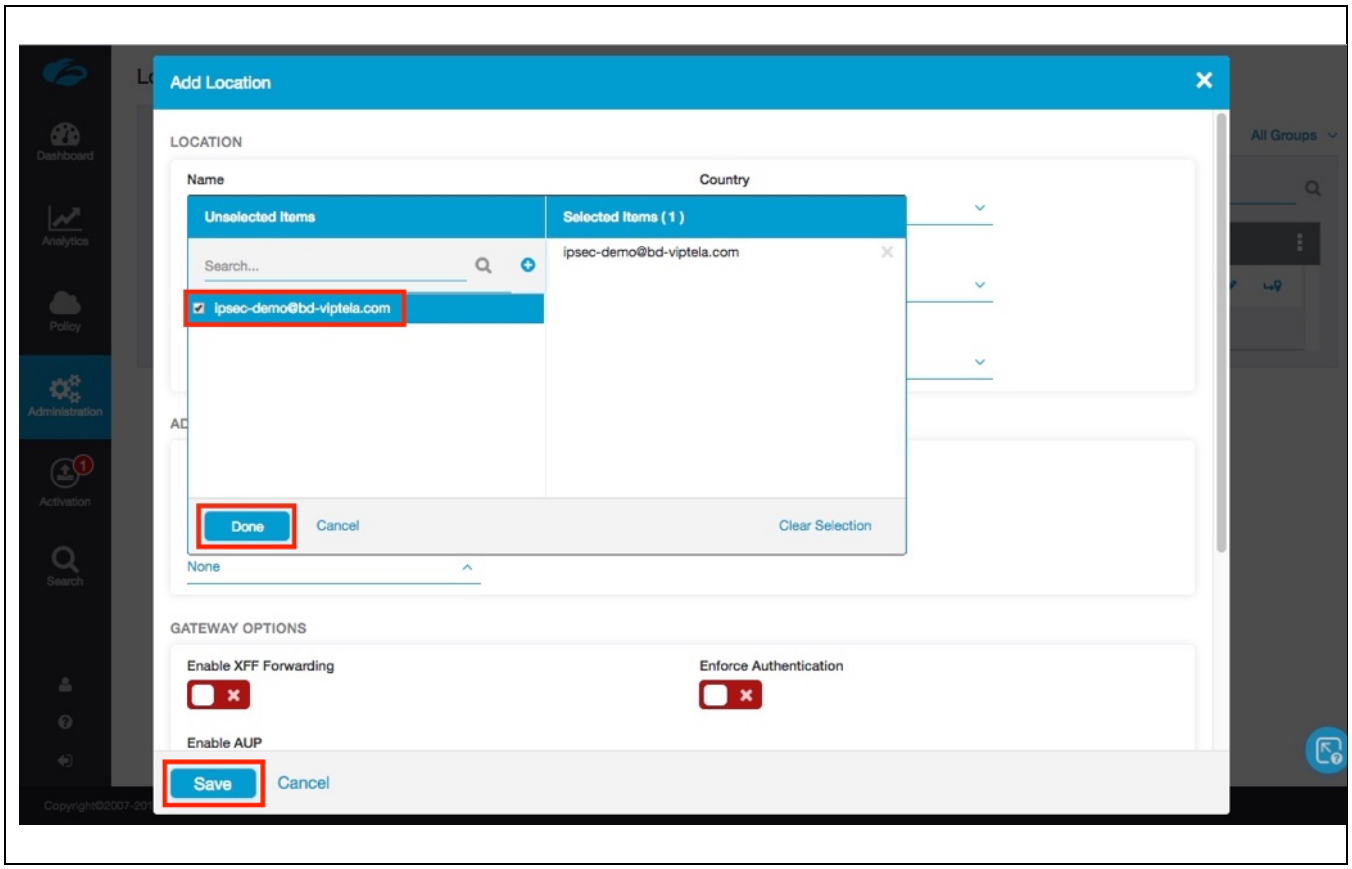


Figure 18: Add VPN Credential to Location and Save

2.4.9 Confirm Changes Have Been Saved

In Figure 19, 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.

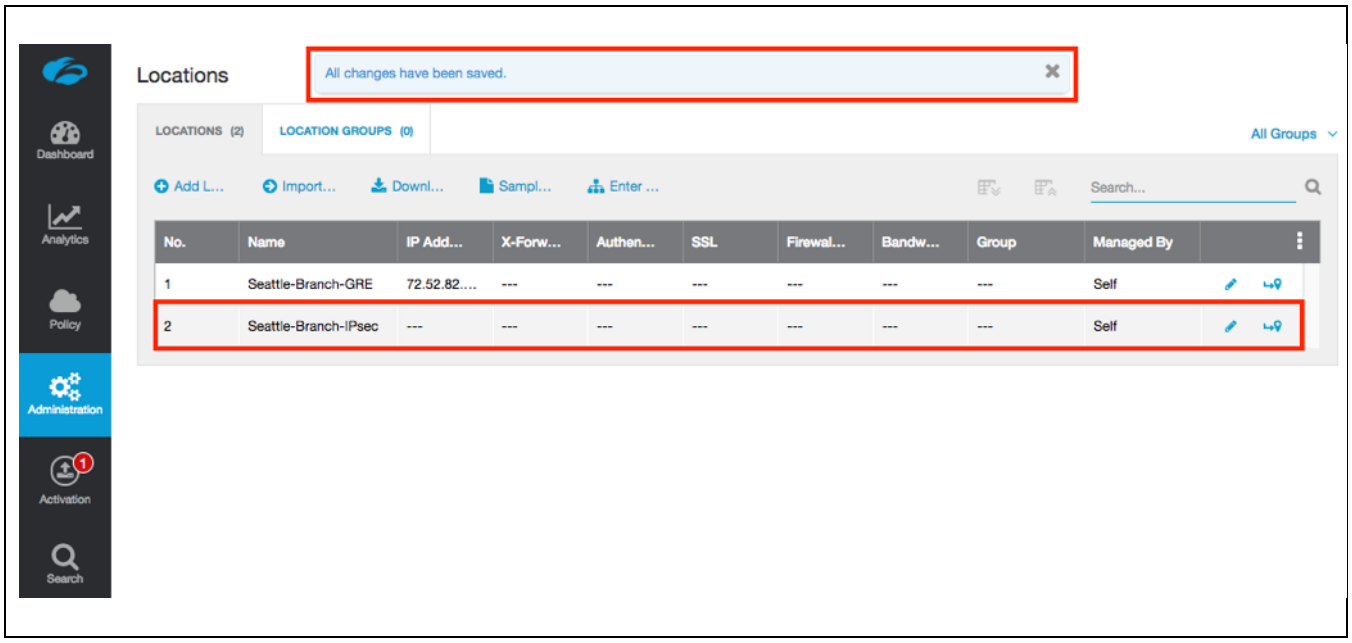


Figure 19: Confirm Changes Have Been Saved

2.5 Activate Pending Changes

2.5.1 Activate Changes

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

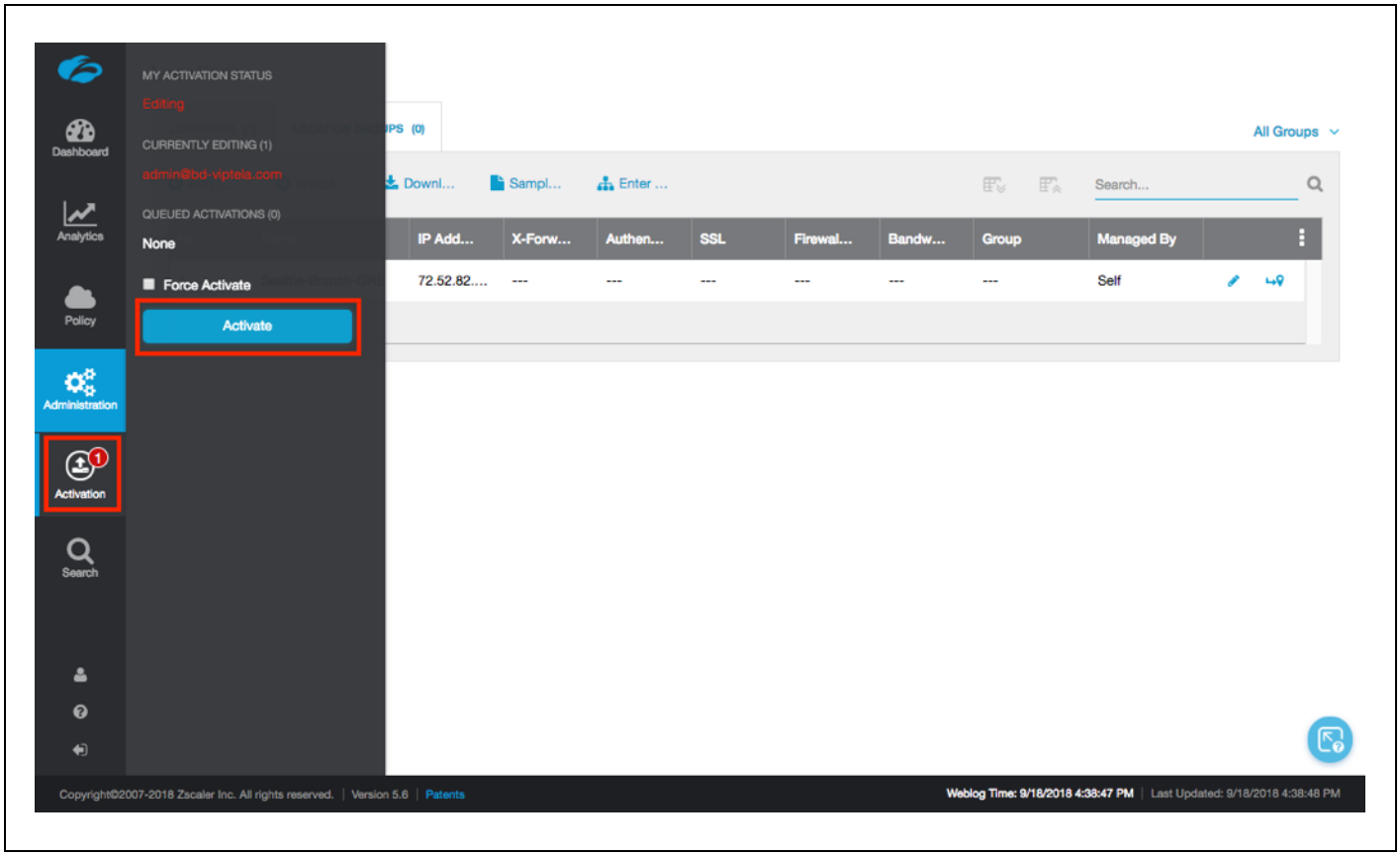


Figure 20: Activate Changes

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.

2.5.2 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.

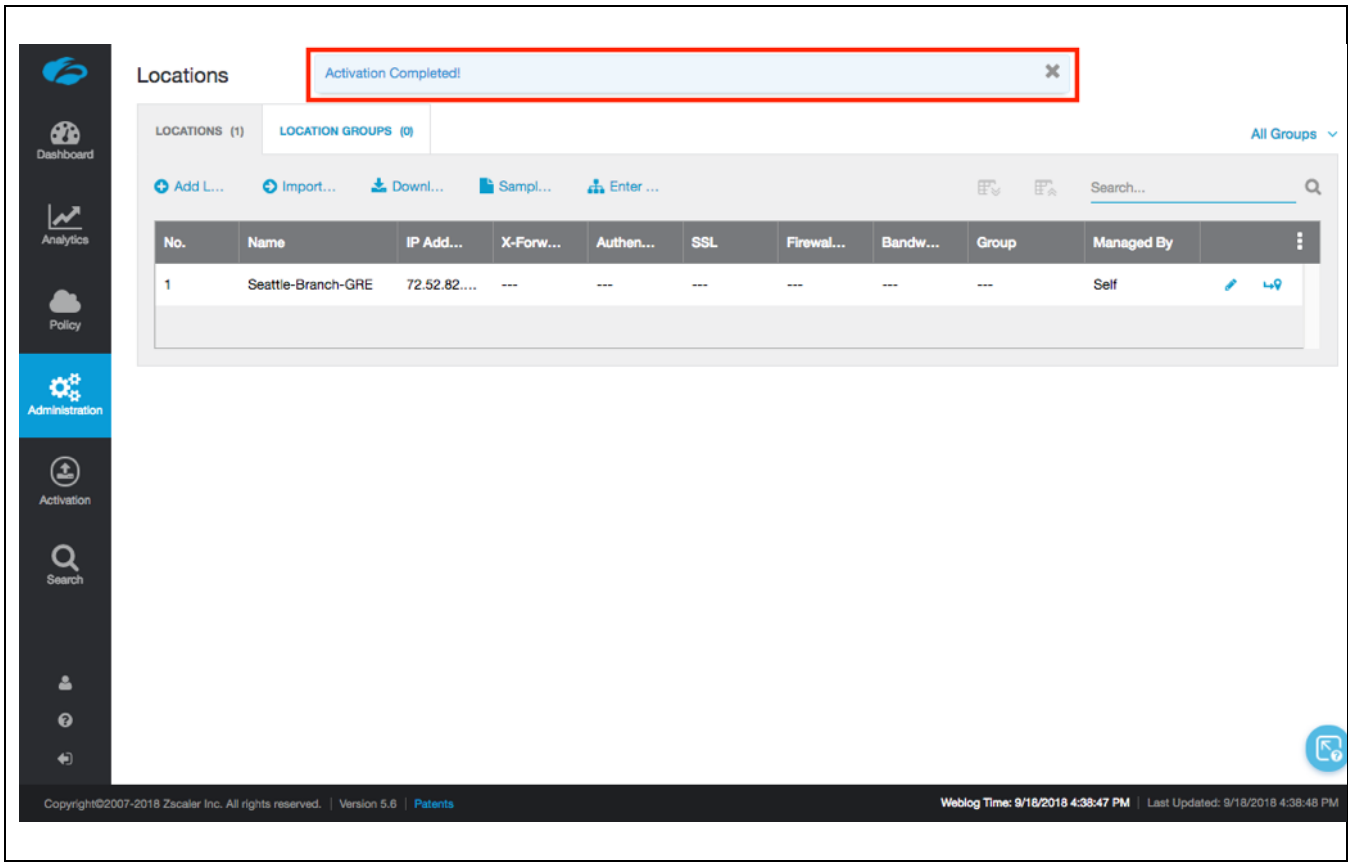


Figure 21: Activation Confirmation

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 the device in order to bring them into the SD-WAN network overlay, where they are managed 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 SD-WAN overlay network. The vManage NMS software runs on a virtual server in the cloud or on-premise.

3.1 Log into Cisco SD-WAN vManage

Open a web browser and enter the URL for your vManage instance (*https://<vManage IP address>:8443*). Enter the username and password. For best results, it is recommended to use a Chrome or Firefox browser.

Note: Before moving forward, ensure the WAN Edge router has a device template deployed from vManage with, at minimum, basic connectivity to the Internet. Refer to Appendix 7.3 for onboarding the SD-WAN device and Appendix 7.5 for step-by-step instructions on deploying an SD-WAN device template for basic connectivity.

3.2 Configure GRE Tunnel (transport-side tunnel)

This section applies to the vEdge router. In this section, a primary and secondary GRE tunnel feature template is attached to the current WAN Edge device template in the transport VPN. A GRE default route is then added in the service VPN to point default route traffic to the Zscaler node.

Note: This section assumes you have a device template already deployed with basic Internet connectivity as a minimum. Please refer to Appendix 7 for details on configuring device templates.

3.2.1 Feature and Device Template Modifications

The following feature and device template modifications are added to the base configurations. Variables are used in multiple places so the template has the flexibility to be applied to multiple devices. See section 3.2.2 for step-by-step details for configuring.

VPN Interface GRE feature template (Primary Tunnel)

Devices: All vEdge routers **Template**: **VPN/VPN Interface GRE**
Template Name: *vEdge-Zscaler-GRE-Tunnel1* **Description**: *vEdge GRE Tunnel 1 to Zscaler*

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Global	gre1
Basic Configuration/Source	Source	Radio button	Interface
	Tunnel Source Interface	Device Specific	GRE_tunnel1_source_interface
Basic Configuration/Destination	GRE Destination IP Address	Device Specific	GRE_tunnel1_destination
	IPv4 Address	Device Specific	GRE_tunnel1_ipv4_address
	IP MTU	Global	1476
	TCP MSS	Global	1436

VPN Interface GRE feature template (Secondary Tunnel)

Devices: All vEdge routers **Template**: **VPN/VPN Interface GRE**
Template Name: *vEdge-Zscaler-GRE-Tunnel2* **Description**: *vEdge GRE Tunnel 2 to Zscaler*

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Global	gre2
Basic Configuration/Source	Source	Radio button	Interface
	Tunnel Source Interface	Device Specific	GRE_tunnel2_source_interface
Basic Configuration/Destination	GRE Destination IP Address	Device Specific	GRE_tunnel2_destination
	IPv4 Address	Device Specific	GRE_tunnel2_ipv4_address
	IP MTU	Global	1476
	TCP MSS	Global	1436

Note: GRE Keepalives are on by default with an interval of 10 seconds and 3 retries. If the device sits behind a NAT device, turn GRE Keepalives off by setting the interval and retries to 0.

Device Template:

Template type	Template sub-type	Template name
Basic Information	AAA	WAN_Edge_AAA_Template
VPN0	VPN	WAN_Edge_VPN0
	VPN Interface	WAN_Edge_VPN0_INET
	VPN Interface	WAN_Edge_VPN0_MPLS
	VPN Interface GRE	**vEdge-Zscaler-GRE-Tunnel1**
	VPN Interface GRE	**vEdge-Zscaler-GRE-Tunnel2**
VPN 512	VPN Interface	WAN_Edge_VPN512_Template
VPN1	VPN	WAN_Edge_VPN1
	VPN Interface	WAN_Edge_VPN1_LAN_INT

Branch VPN 1 feature template

Devices: All except vManage, vSmart **Template**: **VPN/VPN**
Template Name: *WAN_Edge_VPN1* **Description**: *VPN 1 Template for the WAN Edge branch routers*

Branch VPN 1 feature template

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	1
	Name	Global	LAN
GRE Route	**Prefix (optional)**	**Device Specific**	**vpn_gre_route_prefix**
	VPN	**Global**	**0**
	GRE Interface	**Global**	**gre1,gre2**

Note: If you delete this GRE tunnel configuration from a router, first unconfigure the GRE route in the service VPN before removing the GRE tunnels from the device template. The route references the tunnel name, which is defined in the GRE Interface feature templates and you won't be able to successfully remove the GRE Interfaces from the device template until the GRE route reference is removed.

3.2.2 Add Feature Template for the Primary GRE Tunnel

In the vManage GUI, go to **Configuration>Templates** and under the **Feature** tab, click the **Add Template** button.

Figure 22: Add Feature Template

3.2.3 Select VPN Interface GRE Feature Template

Choose the device type on left pane under **Select Devices** (all vEdge routers as examples) and select **VPN Interface GRE** template under VPN-WAN section as shown below.

Note: Do not select any IOS XE SD-WAN routers under **Select Devices** since there is no current support for GRE at this time.

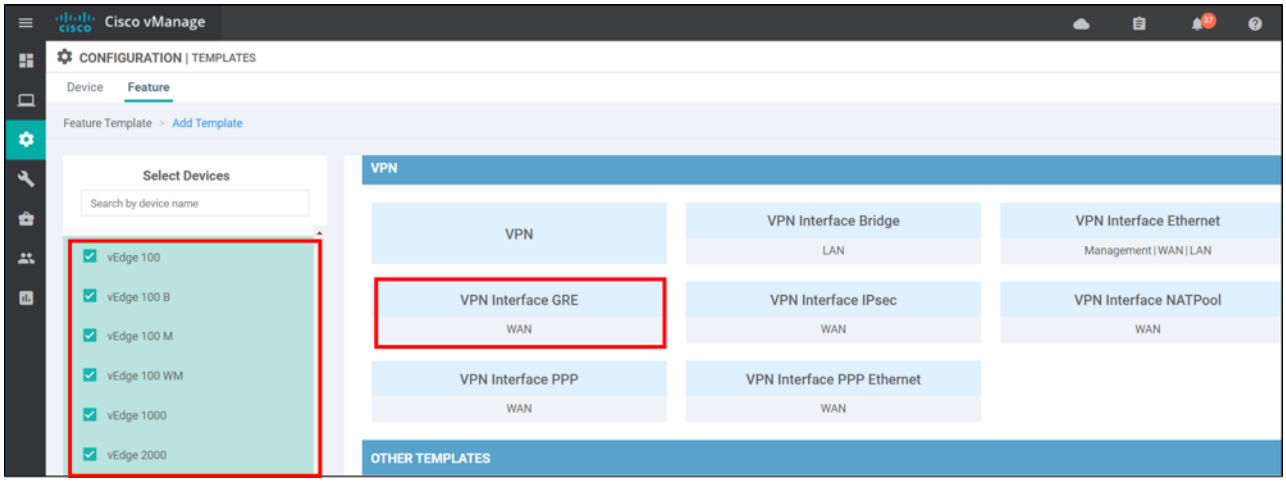


Figure 23: Add VPN Interface GRE Feature

3.2.4 Set GRE Basic Configuration and Source Interface

- Provide a Template Name (*vEdge-Zscaler-GRE-Tunnel1*) and Description (*vEdge GRE Tunnel 1 to Zscaler*) for the VPN Interface GRE feature template.
- Under **Basic Configuration,** and next to **Shutdown**, choose **Global** from the drop-down list and click the **No** radio button. This will unshut the GRE interface.
- Next to **Interface Name**, type *gre1*. This is the name of the virtual GRE interface on the SD-WAN Edge router connecting to Zscaler.
- Under the **Source** section, click the **Interface** radio button. Next to **Tunnel Source Interface**, select **Device Specific** from the drop-down box and type in a variable (*GRE_tunnel1_source_interface*). This is the physical VPN 0 transport side interface connecting the SD-WAN Edge router to the Internet for reachability to the Zscaler nodes. Note that the IP address connecting to this transport is the source IP address of the GRE tunnel that was provisioned by Zscaler. Since this template can apply to multiple devices, a variable is used to define it.

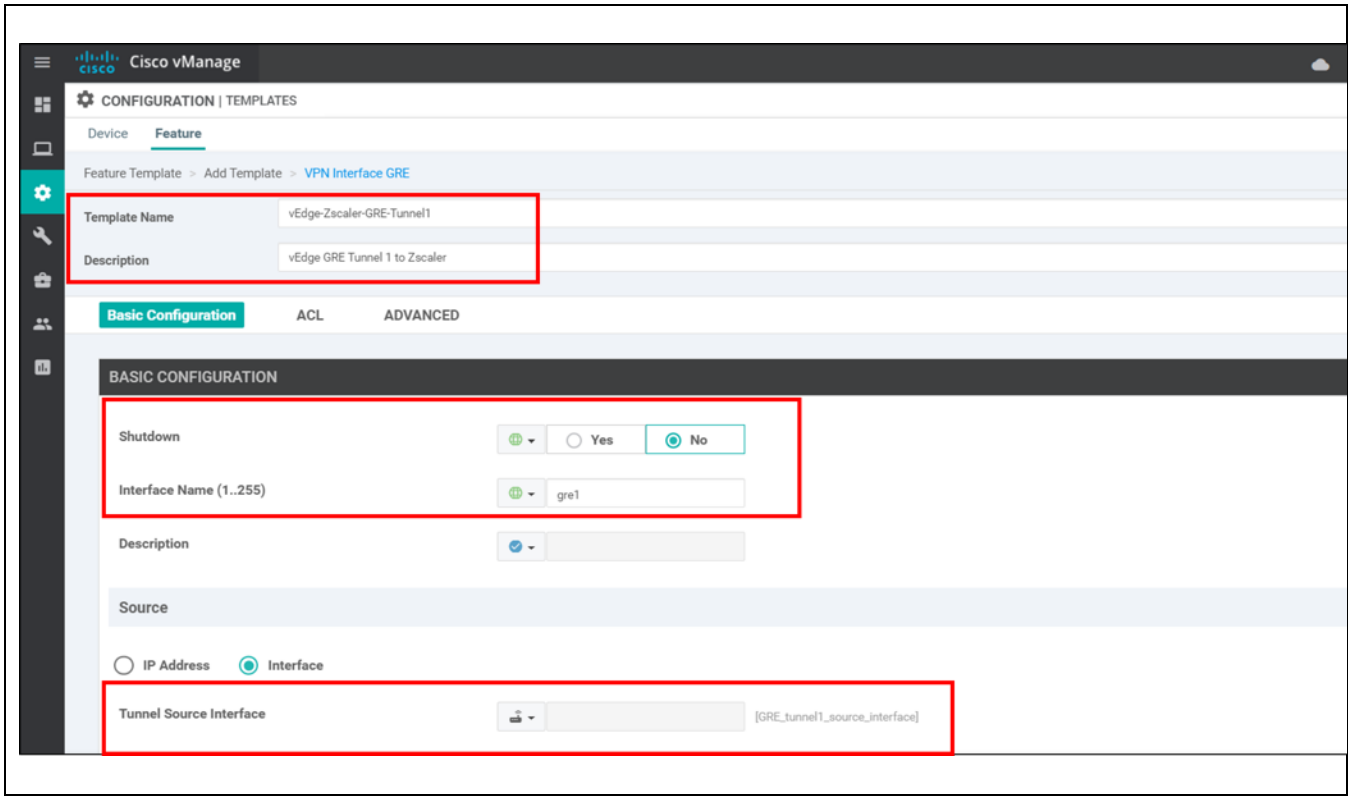


Figure 24: GRE Basic Configuration and Source Settings

3.2.5 Set GRE Interface Destination

- Under the **Destination** section, next to **GRE Destination IP Address**, select **Device Specific** from the drop-down box and type a variable (*GRE_tunnel1_destination*). This is the destination of the primary GRE tunnel.
- Next to **IPv4 Address**, select **Device Specific** from the drop-down box and type a variable (*GRE_tunnel1_ipv4_address*). This is the IP address that is assigned to the tunnel itself. Note that this is for routing purposes and it accepts only /30 addresses.
- Next to **IP MTU**, select **Global** from the drop-down box and type *1476*.
- Next to **TCP MSS**, select **Global** from the drop-down box and type 1436.

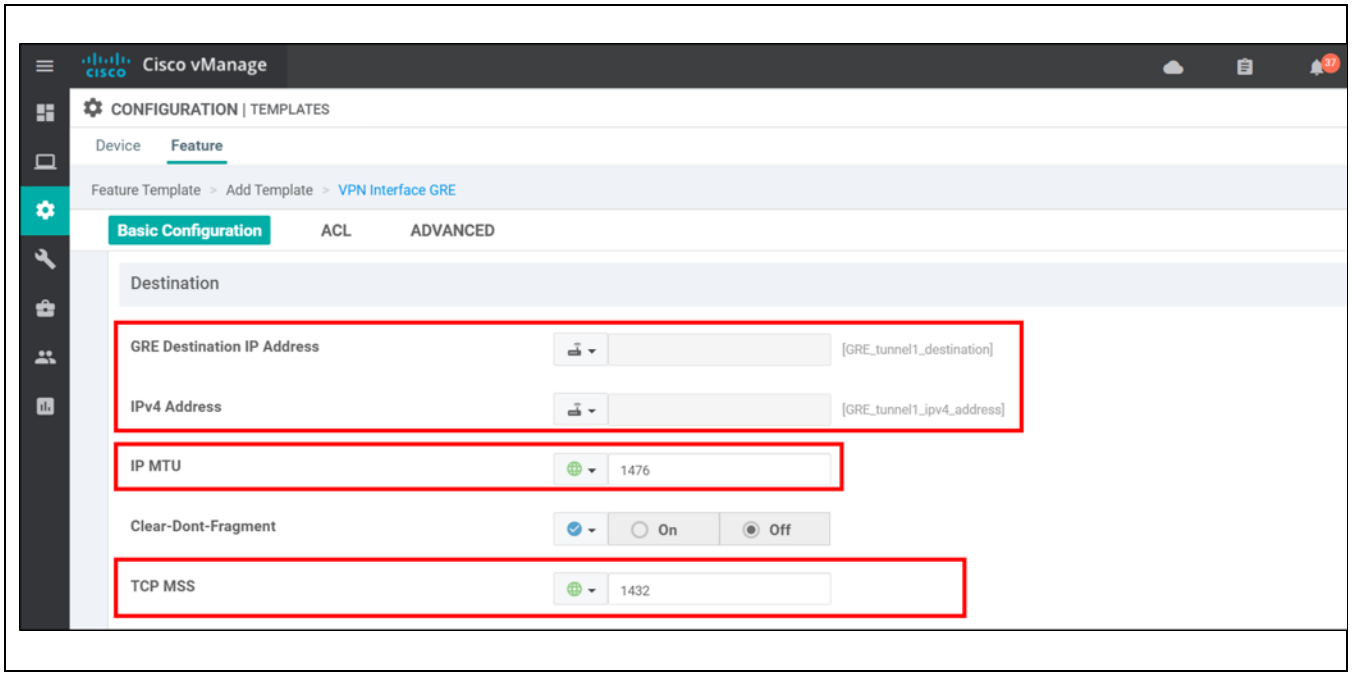


Figure 25: GRE Interface Destination Settings

3.2.6 Enable GRE Keepalives

GRE Keepalives detect the liveliness of the tunnel and should be configured for an **Interval** of 10 and **Retries** of 3, which is the default.

Note: If the SD-WAN Edge router is placed behind a device performing Network Address Translation (NAT), GRE keepalives need to be disabled in order to allow the GRE tunnel to come up. You can disable GRE Keepalives by configuring the **Interval** to 0 and **Retries** to 0, as shown in the figure below.

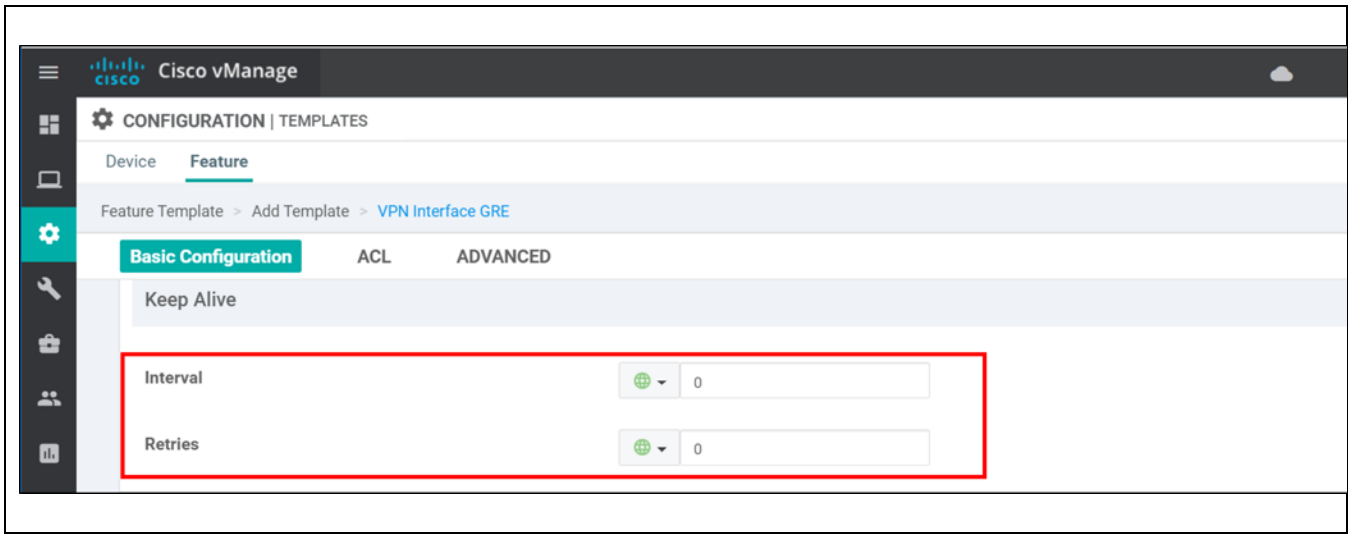


Figure 26: Disable GRE Keepalives

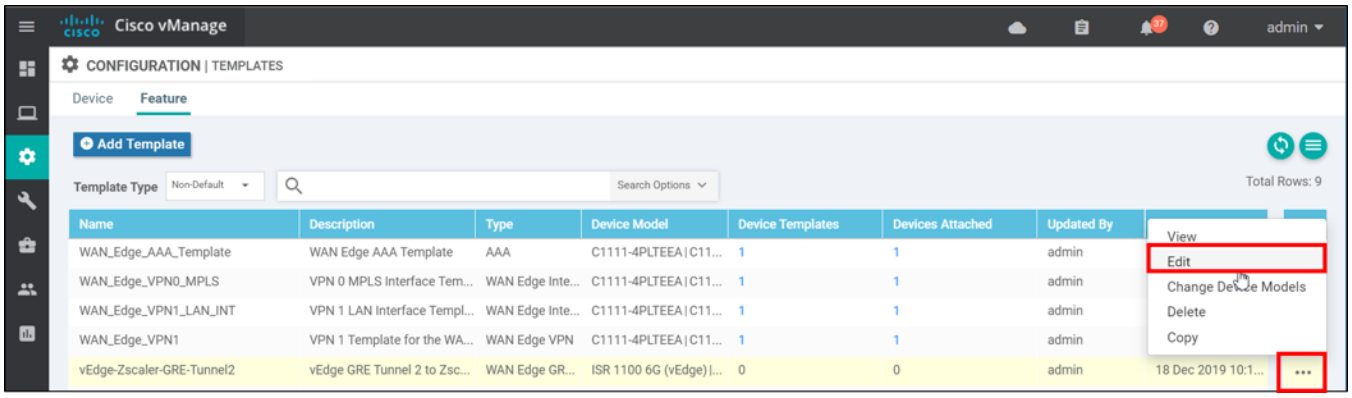
Click **Save** to save the feature template.

3.2.7 Create Feature Template for the Secondary GRE Tunnel

Copy the primary GRE Tunnel feature template and modify parameters and variables for the secondary GRE tunnel.

To the right of the newly-created feature template, *vEdge-Zscaler-GRE-Tunnel1*, click **…** and select **Copy** from the drop-down box. Type in a **Template Name** (*vEdge-Zscaler-GRE-Tunnel2*) and **Description** (*vEdge GRE Tunnel 2 to Zscaler*) and click **Copy**.

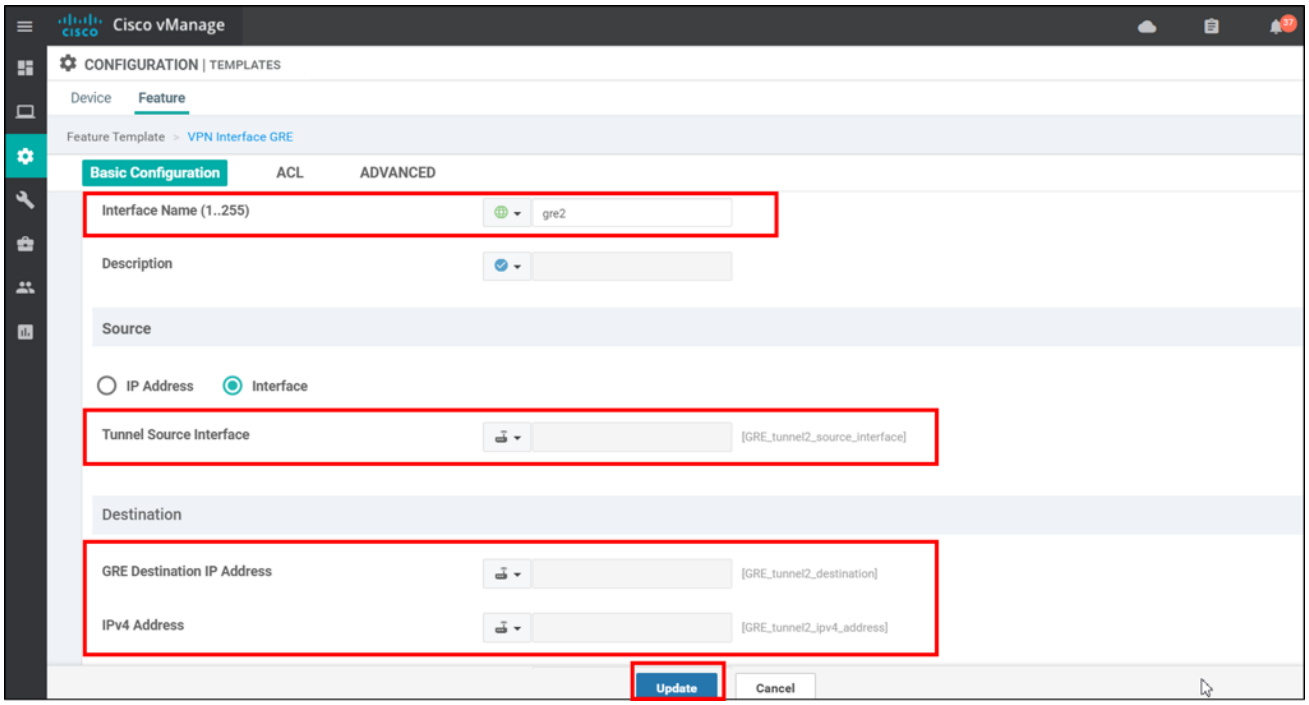
To the right of the newly-copied feature template, click **…** and select **Edit** from the drop-down box.



Make the following modifications:

Interface Name = *gre2*
Tunnel Source Interface = *GRE_tunnel2_source_interface*
GRE Destination IP Address = *GRE_tunnel2_destination*
IPv4 Address = *GRE_tunnel2_ipv4_address*

Click **Update** to save the feature template.



3.2.8 Add GRE Interface Feature Template to Device Template

Next, the GRE Interface feature templates are added to the device template. Navigate to **Configuration>Templates** and under the **Device** tab, identify the device template for the SD-WAN Edge router connecting to Zscaler (WAN_Edge_Remote_A). To the far right of the template, click **…** and select **Edit** from the drop-down box.

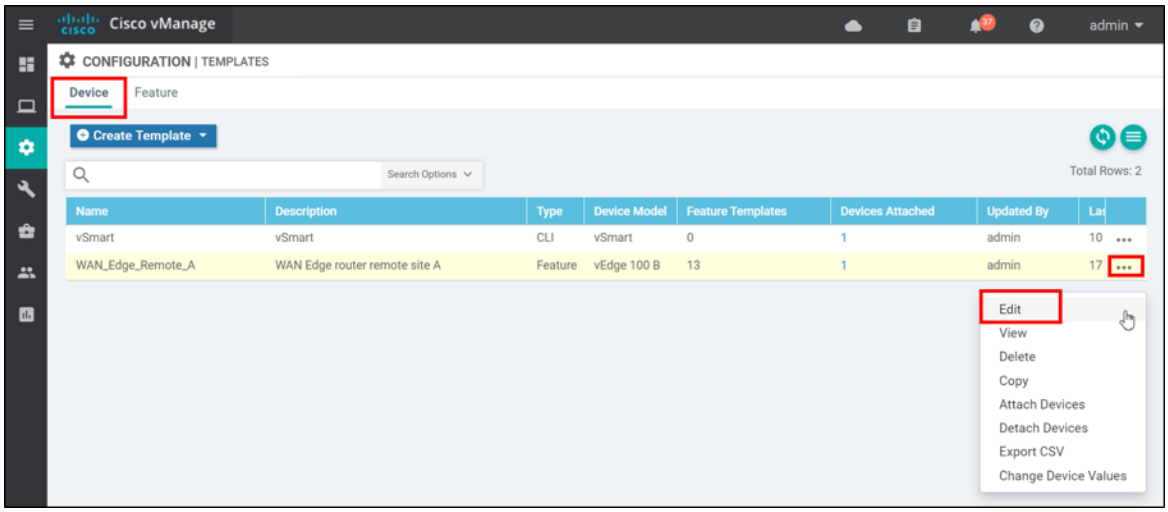


Figure 27: Device Templates List

3.2.9 VPN 0 Template

Under **Transport & Management VPN** in the **VPN 0** section, Click **(+) VPN Interface GRE** on the right side two times to add both the primary and secondary GRE tunnels.

Next to one **VPN Interface GRE** entry, choose the *vEdge-Zscaler-GRE-Tunnel1* feature template from the drop-down box, and next to the other **VPN Interface GRE** entry, choose the *vEdge-Zscaler-GRE-Tunnel2* feature template.

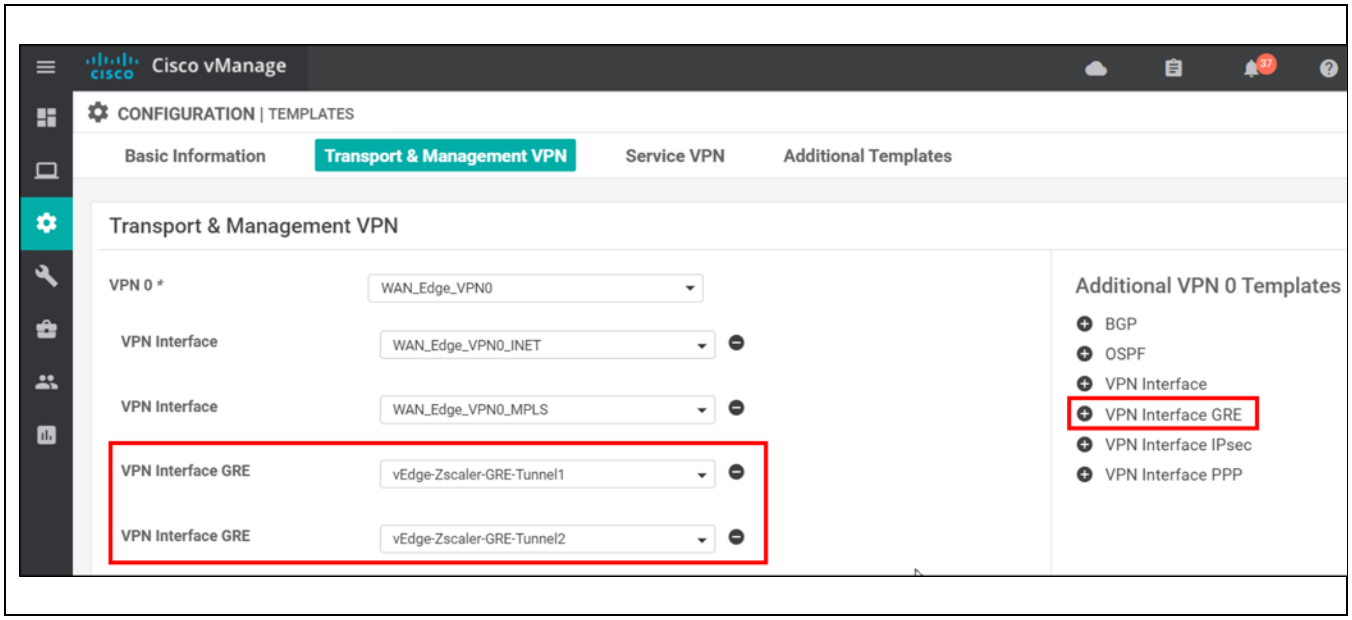


Figure 28: VPN0 Templates

3.2.10 Configuration Update

Click on the **Update** button at the bottom of the page to save the device template changes. If the device template was previously attached to an SD-WAN Edge router, a configuration update is performed and the updated device configuration pushed from vManage to the SD-WAN Edge router.

Because variables were created in the newly-added feature templates, the variables need to be defined before the configuration update can take place. To the right of the SD-WAN device attached to the device template, click **…** and select **Edit Device Template** from the drop-down box.

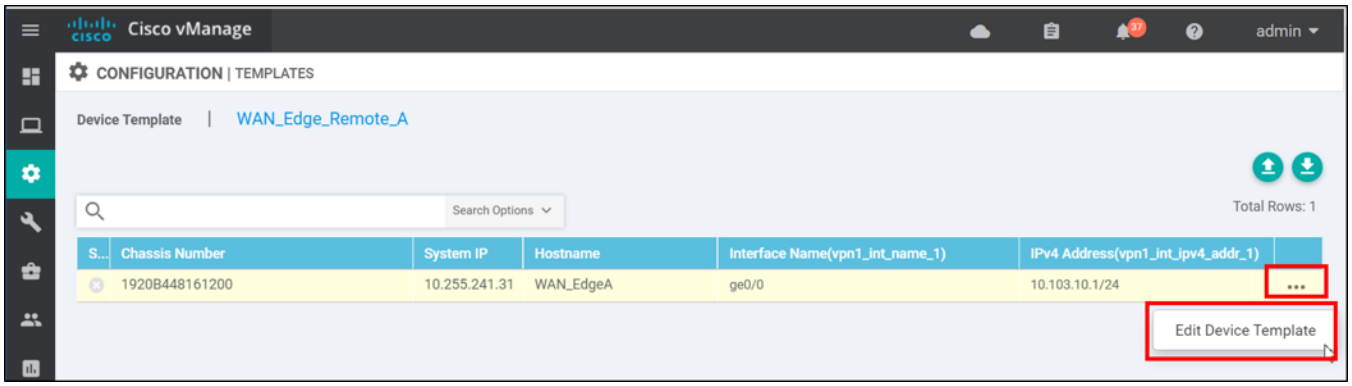


Figure 29: Configuration Update

The pop-up window prompts you to enter in the variable values.

Note that the Zscaler GRE provisioning information for the primary tunnel is:

Primary Destination: 104.129.194.38
Internal Router IP: 172.17.12.217/30
Internal ZEN IP: 172.17.12.218/30

The GRE_tunnel1_source_interface is ge0/4. The *GRE_tunnel1_destination* variable is the Primary Destination. The *tunnel1_ipv4_address* variable is the Internal Router IP, which is the IP address that is assigned on the tunnel. The Internal ZEN IP is the IP address configured on the Zscaler side of the tunnel.

Click **Update**.

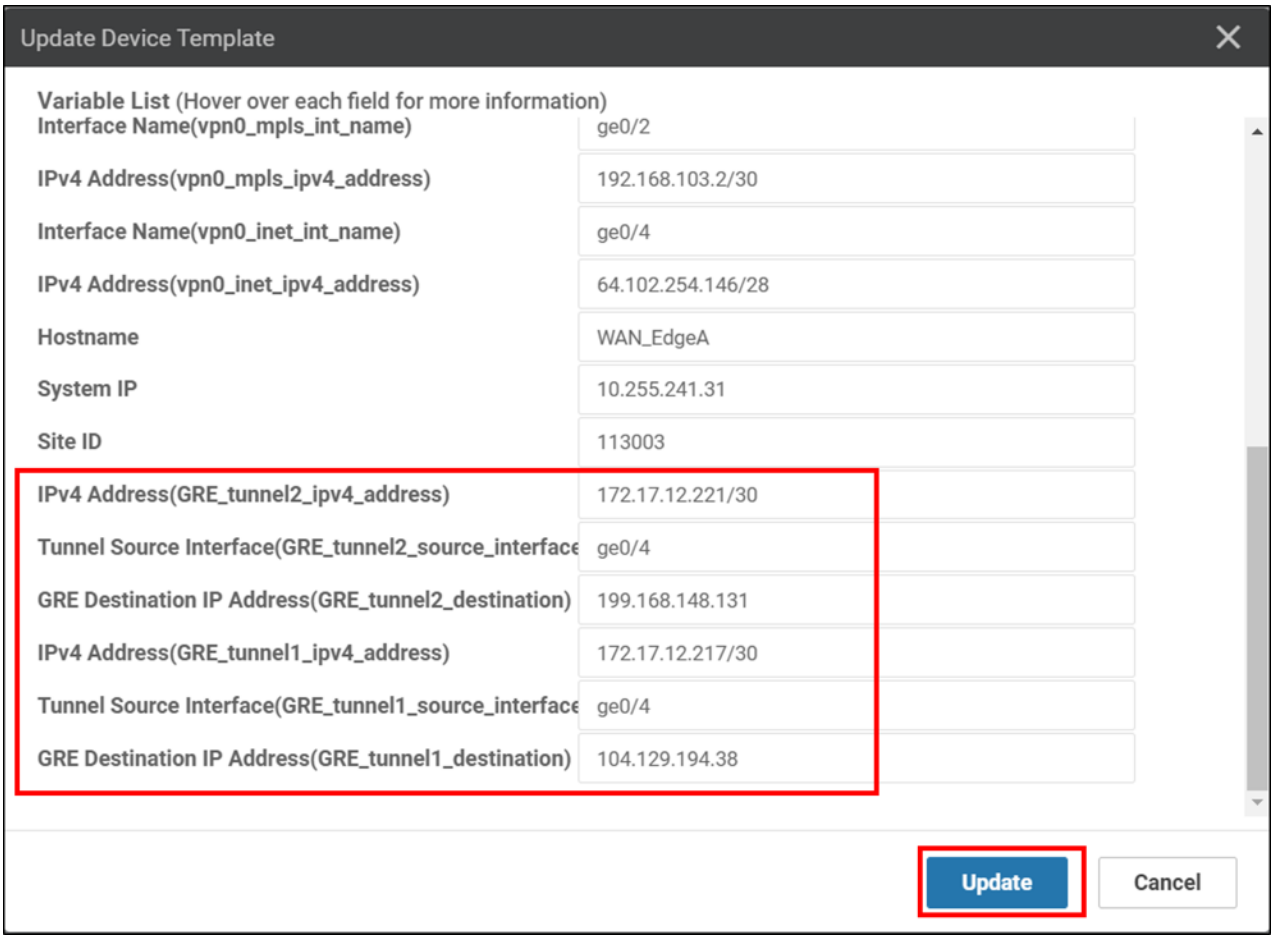


Figure 30: Fill in Values

Click **Next**. Click **Configure Devices**.
The updated configuration is pushed to the SD-WAN router. The router returns with a **Success** status.

3.2.11 Add GRE Route

The GRE tunnels have been added to VPN 0, so now a static GRE route is needed on the service-side VPN to direct user traffic to Zscaler through the GRE tunnel.

In vManage go to **Configuration>Templates** and under the **Feature** tab, find the service VPN template (*WAN_Edge_VPN1* in this example). To the far right of the desired template, click **…** and select **Edit** from the drop-down box.

Navigate to the **GRE Route** section of the feature template. Click **New GRE Route**. Note that the VPN 1 VPN template is shared with other routers and this configuration is applied to all devices using this feature template. You can create a separate VPN 1 feature template for routers utilizing GRE tunnels, or you can make this route optional, and only apply the route to specific devices. When you define variables before a configuration is pushed to the router, you can leave this optional variable blank and the route is not applied to the device.

- Next to **Prefix**, select **Device Specific** from the drop-down box and type the variable, *vpn1_gre_route_prefix*.
- To make the route optional, click the checkbox next to **Mark as Optional Row**. If you do this before the **Prefix** variable is set, the Prefix field is locked and you cannot change the name of the variable.
- The VPN where the tunnel is located defaults to 0 and you cannot change it.
- Next to **GRE Interface**, select **Global** from the drop-down box and type *gre1, gre2*. These are the two GRE tunnels created in the above steps. *gre1* becomes primary and *gre2* becomes secondary. Only when *gre1* goes down does *gre2* become active.

Click **Add** to add the route into the feature template and then click **Update** to save the feature template.

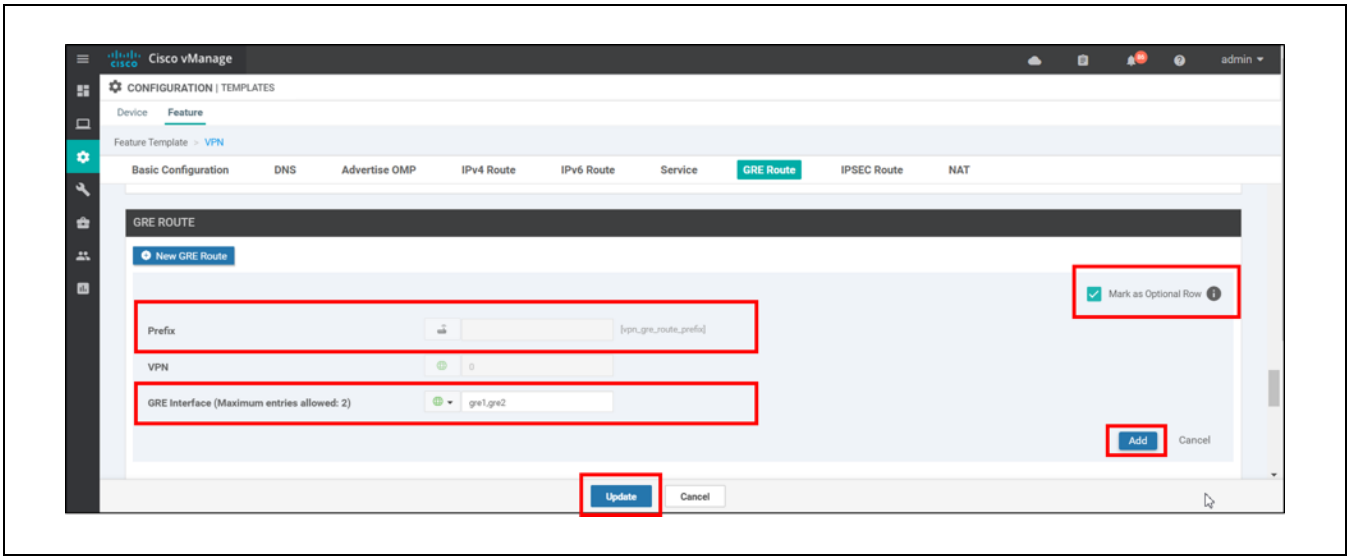


Figure 31: Add GRE Route

3.2.12 Configuration Update

Once the feature template is updated, the routers attached to the template are displayed. All required variables for all devices associated with the feature template need to be filled in before the configuration update can be completed.

Figure 32: View Devices for Configuration Update

Since the GRE route was marked optional, the WAN Edge Remote A (vEdge) is the only device that needs the GRE route prefix variable defined.

Select **WAN_Edge_Remote_A** and to the far right of the device, click **…** and select **Edit Device Template** from the drop-down list.

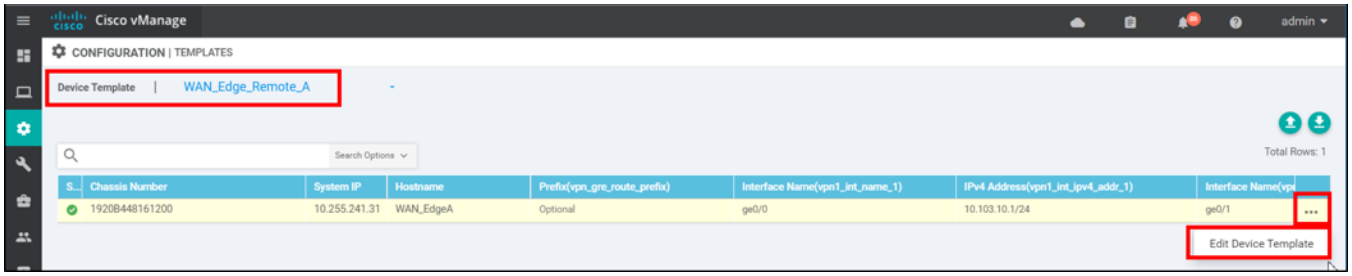


Figure 33: Edit Configuration Values

Next to **Prefix(vpn_gre_route_prefix)**, type *0.0.0.0/0* and click **Update**.

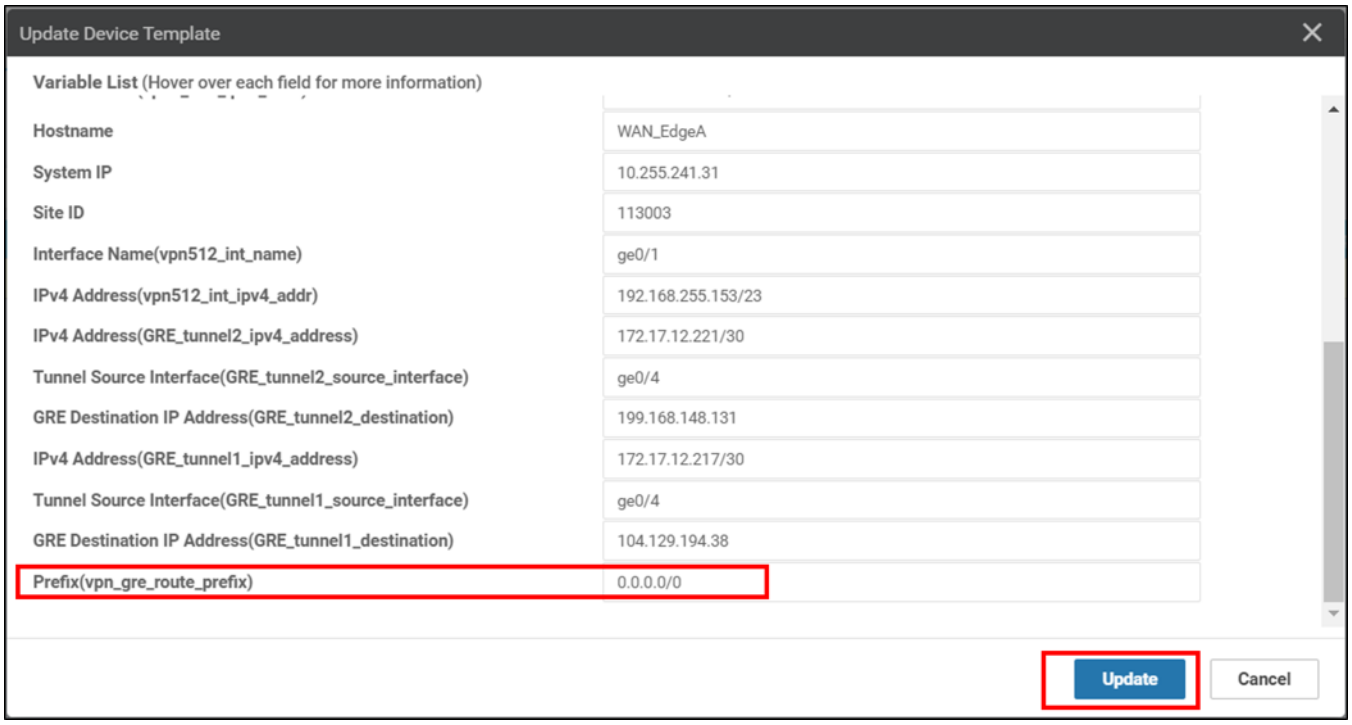


Figure 34: Fill in Variable Values

Click **Next**, then **Configure Devices**. A pop-up window asked to you confirm changes. Confirm changes and click **OK**.

The modified configuration is pushed to the WAN Edge router and when complete, vManage returns with a **Success** status.

Note: If you delete this GRE tunnel configuration from a router, first unconfigure the GRE route prefix in the service VPN before removing the GRE tunnels from the device templates. To unconfigure the GRE route prefix, click **…** to the right of the device template and select **Change Device Values**. The route references the tunnel name, which is defined in the GRE Interface feature templates and you won't be able to successfully remove the GRE Interfaces from the device template until the GRE route reference is removed.

3.2.13 Verify Tunnel Operation

In vManage, go to **Monitor>Network** and click the device of interest (*WAN_EdgeA*). On the left-hand side, click **Interface**. View the status and traffic statistics for the tunnel interfaces.

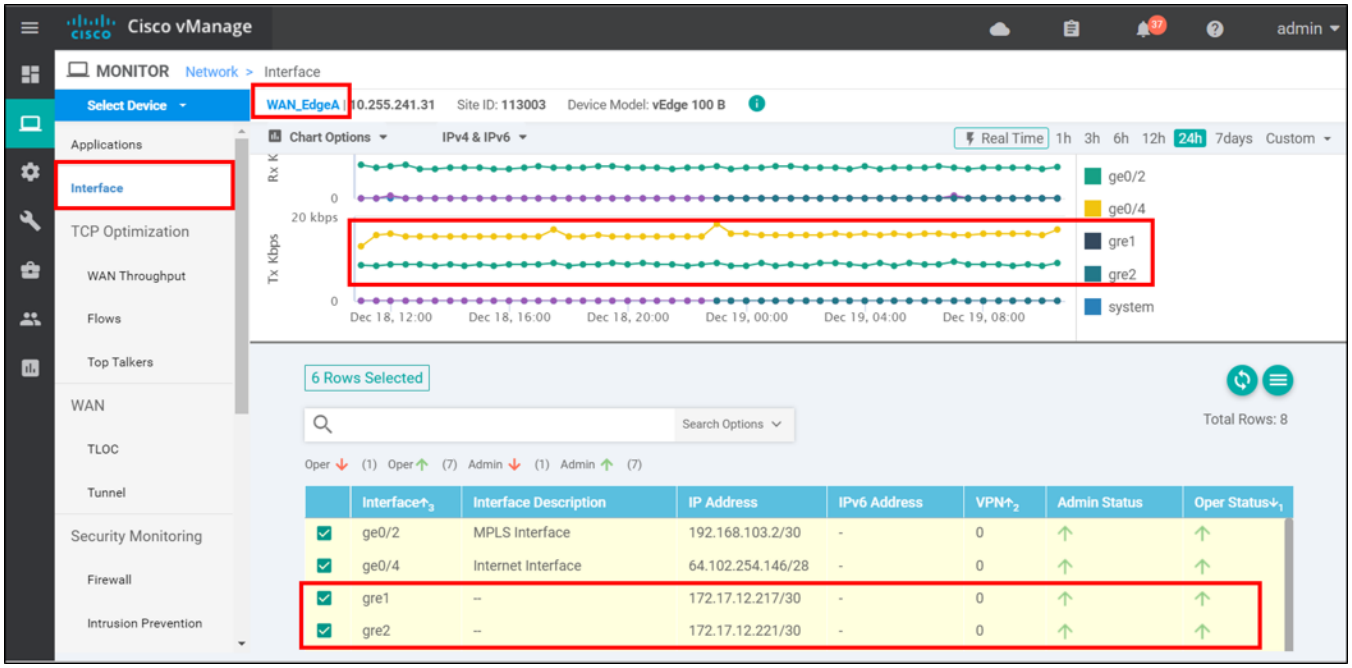


Figure 35: Check Tunnel Status

To view the primary GRE route, on the left-hand side, click **Real Time**, then in the **Device Options** box, select **IP Routes**. A pop-up window asks you to choose filters to display data faster. Click **Do Not Filter**.

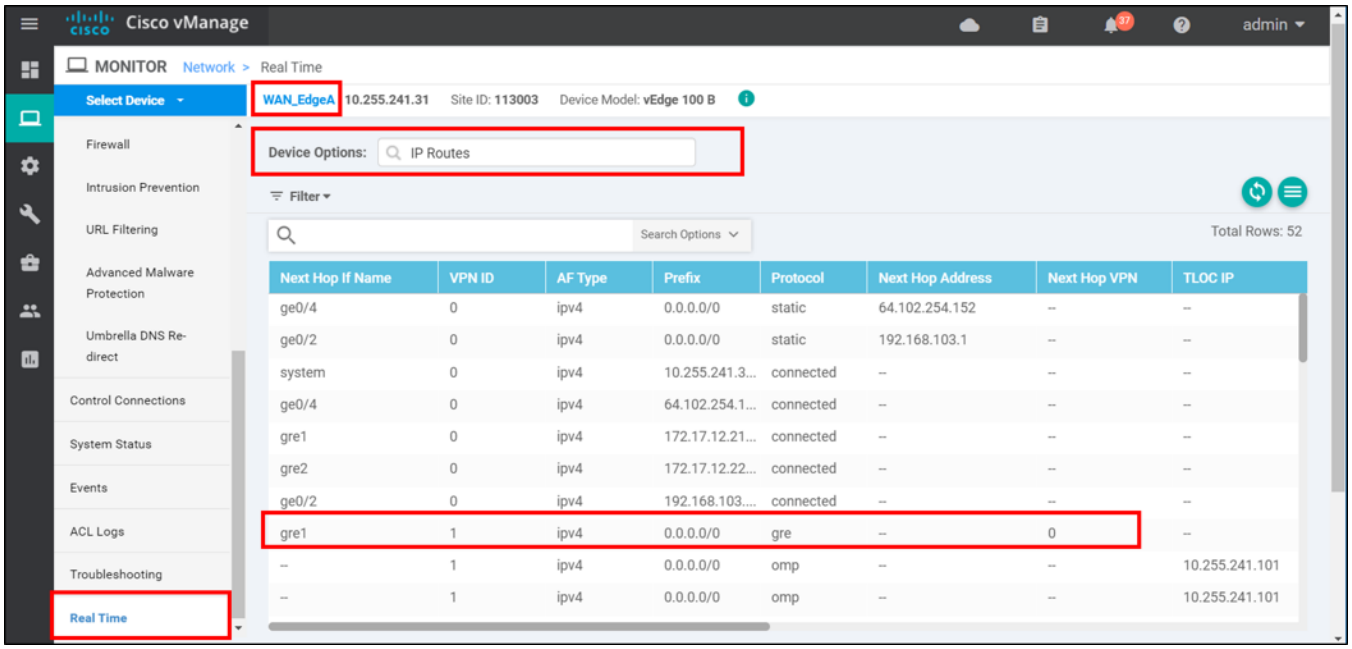


Figure 36: View GRE Route

3.3 Configuring IPsec Tunnel (Transport-side and Service-side)

Transport-side
This section applies to the vEdge router. In this section, a primary and secondary IPsec tunnel feature template is attached to the current WAN Edge device template in the transport VPN. An IPsec default route is then added in the service VPN to point default route traffic to the Zscaler node. This is similar to the GRE transport-side tunnel configuration. The vEdge router, attached to the WAN_Edge_Remote_A device template, is configured with a transport-side tunnel in this section.

Service-side
This section applies to both the vEdge and IOS XE SD-WAN router. In this section, a primary and secondary IPsec tunnel is sourced in the transport VPN, but the IPsec tunnel feature template is configured in the service VPN (service-side). IPv4 routes are then installed in the service VPN using the Zscaler tunnel remote end as the next hop for the routes. The IOS XE SD-WAN router, attached to the WAN_Edge_Remote_B device template, is configured with a service-side tunnel in this section.

Note: This section assumes you have a device template already deployed with basic Internet connectivity as a minimum. Please refer to Appendix 7 for details on configuring device templates.

3.3.1 Feature and Device Template Modifications

The following feature and device template modifications are added to the base configurations. Variables are used in multiple places so the template has the flexibility to be applied to multiple devices. See section 3.3.2 for step-by-step details for configuring.

VPN Interface IPsec feature template (Primary Tunnel)

Devices: All vEdge routers **Template**: **VPN/VPN Interface IPSEC**
Template Name: *Zscaler-IPsec-Tunnel1* **Description**: *IPsec Tunnel 1 to Zscaler*

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Global	ipsec1
	IPv4 address	Device Specific	IPsec_tunnel1_ipv4_address
Basic Configuration/Source	Source	Radio button	Interface
	Tunnel Source Interface	Device Specific	IPsec_tunnel1_source_interface

Basic Configuration/Destination	GRE Destination IP Address	Device Specific	IPsec_tunnel1_destination
IKE	IKE Version	Global	2
	IKE Diffie-Hellman Group	Global	2 1024-bit modulus
IKE Authentication	Preshared Key	Device Specific	IPsec_tunnel1_pre_shared_secret
	IKE ID for local End point	Device Specific	IPsec_tunnel1_ike_local_id
	IKE ID for Remote End point	Device Specific	IPsec_tunnel1_ike_remote-id
IPSEC	IPsec Cipher Suite	Global	Null SHA1
	Perfect Forward Secrecy	Global	None

VPN Interface IPsec feature template (SecondaryTunnel)

Devices: All vEdge routers **Template**: **VPN/VPN Interface IPSEC**
Template Name: *Zscaler-IPsec-Tunnel2* **Description**: *IPsec Tunnel 2 to Zscaler*

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Global	ipsec2
	IPv4 address	Device Specific	IPsec_tunnel2_ipv4_address
Basic Configuration/Source	Source	Radio button	Interface
	Tunnel Source Interface	Device Specific	IPsec_tunnel2_source_interface
Basic Configuration/Destination	GRE Destination IP Address	Device Specific	IPsec_tunnel2_destination
IKE	IKE Version	Global	2
	IKE Diffie-Hellman Group	Global	2 1024-bit modulus
IKE Authentication	Preshared Key	Device Specific	IPsec_tunnel2_pre_shared_secret
	IKE ID for local End point	Device Specific	IPsec_tunnel2_ike_local_id
	IKE ID for Remote End point	Device Specific	IPsec_tunnel2_ike_remote-id
IPSEC	IPsec Cipher Suite	Global	Null SHA1

	Perfect Forward Secrecy	Global	None

Note: DPD is on by default with an interval of 10 seconds and 3 retries.

Device Template (transport-side, WAN_Edge_Remote_A (vEdge)):

Template type	Template sub-type	Template name
Basic Information	AAA	WAN_Edge_AAA_Template
VPN0	VPN	WAN_Edge_VPN0
	VPN Interface	WAN_Edge_VPN0_INET
	VPN Interface	WAN_Edge_VPN0_MPLS
	VPN Interface IPSEC	**Zscaler-IPsec-Tunnel1**
	VPN Interface IPSEC	**Zscaler-IPsec-Tunnel2**
VPN 512	VPN Interface	WAN_Edge_VPN512_Template
VPN1	VPN	WAN_Edge_VPN1
	VPN Interface	WAN_Edge_VPN1_LAN_INT

Device Template (service-side, WAN_Edge_Remote_B (IOS XE SD-WAN)):

Template type	Template sub-type	Template name
Basic Information	AAA	WAN_Edge_AAA_Template
VPN0	VPN	WAN_Edge_VPN0
	VPN Interface	WAN_Edge_VPN0_INET
	VPN Interface	WAN_Edge_VPN0_MPLS
VPN 512	VPN Interface	WAN_Edge_VPN512_Template
VPN1	VPN	WAN_Edge_VPN1
	VPN Interface	WAN_Edge_VPN1_LAN_INT
	VPN Interface IPSEC	**Zscaler-IPsec-Tunnel1**
	VPN Interface IPSEC	**Zscaler-IPsec-Tunnel2**

Branch VPN 1 feature template (needed for transport-side tunnel)

Devices: All except vManage, vSmart **Template**: **VPN/VPN**
Template Name: *WAN_Edge_VPN1* **Description**: *VPN 1 Template for the WAN Edge branch routers*

Branch VPN 1 feature template

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	1
	Name	Global	LAN
IPSEC Route	**Prefix (optional)**	**Device Specific**	**vpn1_ipsec_route_prefix**
	VPN	**Global**	**0**
	IPSEC Interface	**Global**	**ipsec1,ipsec2**

Note: If you delete this IPsec tunnel configuration from a router, first unconfigure the IPsec route in the service VPN if it exists before removing the IPsec tunnels from the device template. The route references the tunnel name, which is defined in the IPsec Interface feature templates and you won't be able to successfully remove the IPsec Interfaces from the device template until the IPsec route reference is removed.

Branch VPN 1 feature template (needed for service-side tunnel)

Devices: All except vManage, vSmart **Template**: **VPN/VPN**
Template Name: *WAN_Edge_VPN1* **Description**: *VPN 1 Template for the WAN Edge branch routers*

Branch VPN 1 feature template

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	1
	Name	Global	LAN
IPv4 Route	**Prefix (optional)**	**Device Specific**	**vpn1_ipv4_prefix_to_zscaler**
	Gateway	**Radio Button**	**Next Hop**
	Next Hop (optional)	**Device Specific**	**vpn1_next_hop_zscaler_remote_end1**
	Next Hop (optional)	**Device Specific**	**vpn1_next_hop_zscaler_remote_end2**

3.3.2 Add Feature Template for the Primary IPsec Tunnel

In the vManage GUI, go to **Configuration>Templates** and under the **Feature** tab, click the **Add Template** button.

Figure 37: Add Feature Template

3.3.3 Select VPN Interface IPsec Feature Template

Choose the device type on left pane under **Select Devices** (In this example, all platforms except vManage and vSmart are chosen) and select **VPN Interface IPsec** template under the VPN section as shown below.

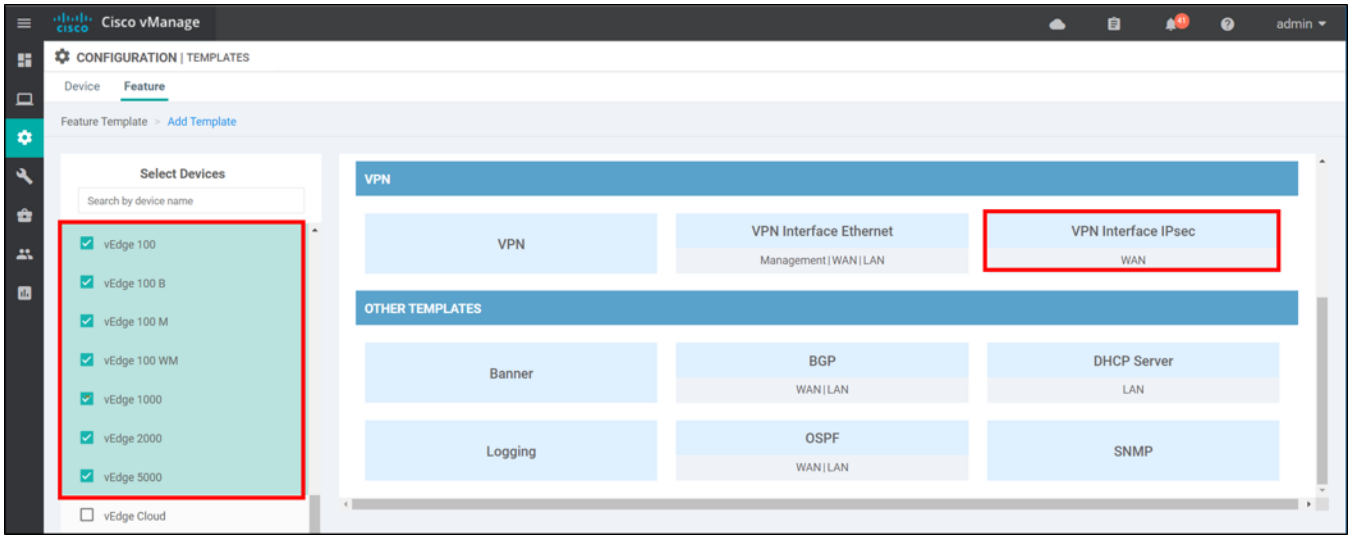


Figure 38: Add VPN Interface IPsec Feature

3.3.4 Set IPsec Basic Configuration and Source and Destination Interface

- Provide a Template Name (*Zscaler-IPsec-Tunnel1*) and Description (*IPsec Tunnel 1 to Zscaler*) for the VPN Interface IPsec feature template.
- Under **Basic Configuration,** and next to **Shutdown**, choose **Global** from the drop-down list and click the **No** radio button. This will unshut the IPsec interface.
- Next to **Interface Name**, type *ipsec1*. This is the name of the primary virtual IPsec interface on the SD-WAN Edge router connecting to Zscaler.
- Next to IPv4 address, select **Device Specific** from the drop-down box and type a variable (*IPsec_tunnel1_ipv4_address*). This is the IP address that is assigned to the tunnel itself. Note that this is for routing purposes and it accepts only /30 addresses.
- Under the **Source** section, click the **Interface** radio button. Next to **IPsec Source Interface**, select **Device Specific** from the drop-down box and type in a variable (*IPsec_tunnel1_source_interface*). This is the physical VPN 0 transport side interface connecting the SD-WAN Edge router to the Internet for reachability to the Zscaler nodes. Note that the IP address connecting to this transport is the source IP address of the IPsec tunnel that is used to connect to Zscaler. Since this template can apply to multiple devices, a variable is used to define it.

- Under the **Destination** section, next to **IPsec Destination IP Address/FQDN**, select **Device Specific** from the drop-down box and type a variable (*IPsec_tunnel1_destination*). This is the destination of the primary IPsec tunnel and can either be an IP address or a Fully-Qualified Domain Name (FQDN).
- Dead-Peer detection detects the liveliness of the tunnel and should be configured for an **Interval** of 10 and **Retries** of 3, which is the default.

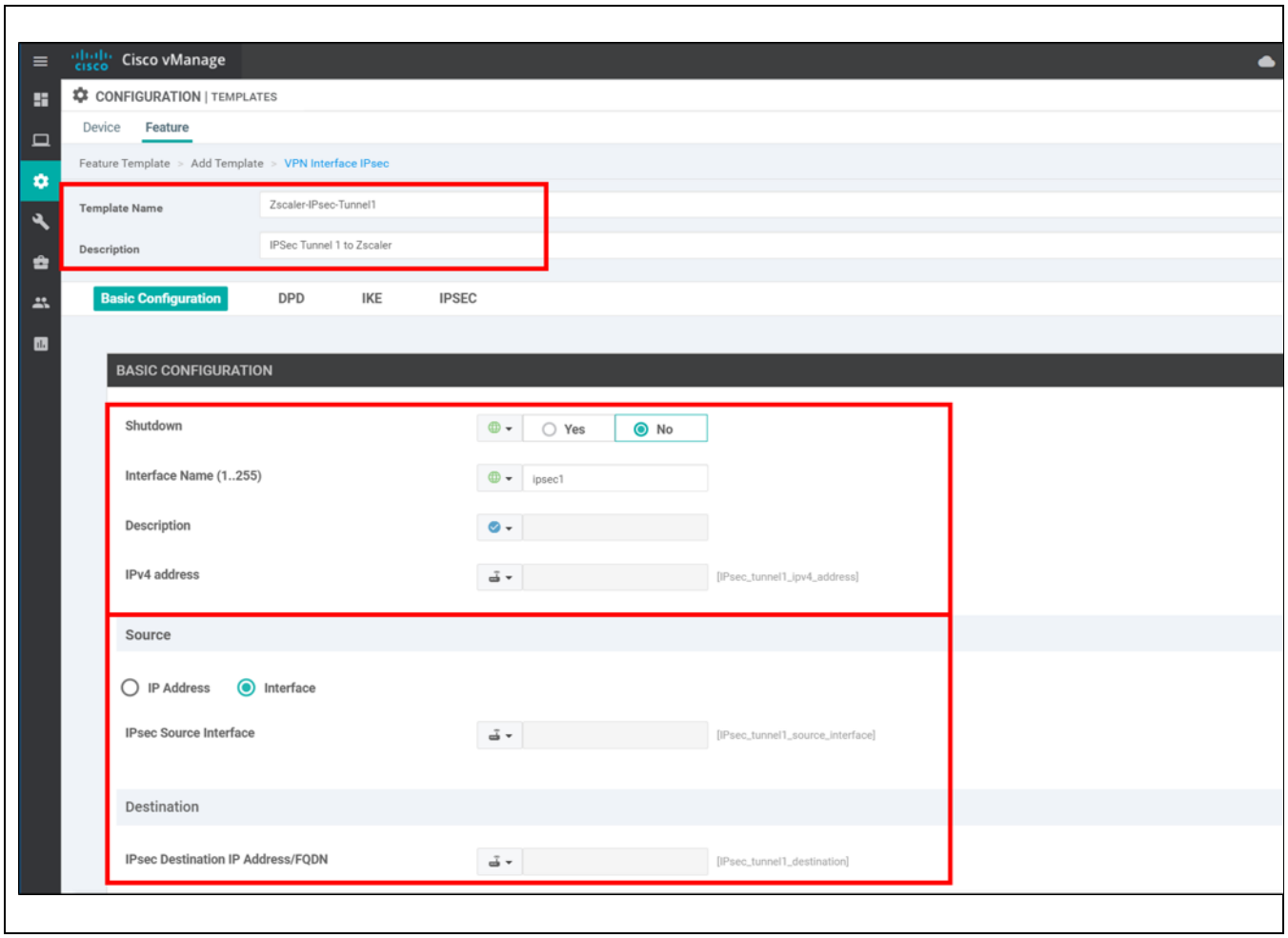


Figure 39: IPsec Basic Configuration and Source and Destination Settings

3.3.5 Configure IKE Parameters

The following parameters are configured under the IKE section.

- Next to ***IKE Version***, choose **Global** from the drop-down box and type *2*.
- Next to ***IKE Diffie-Hellman Group***, choose **Global** form the drop-down box and choose *2 1024-bit modulus*.
- Next to ***Preshared Key***, choose **Device Specific** from the drop-down box and type a variable (*IPsec_tunnel1_pre_shared_secret*). The preshared key value configured here must match the preshared key configured in the Zscaler Admin Portal for the IPsec tunnel to successfully come up. Note that starting in 18.4 vEdge code, this key needs to be 16 characters or more. This parameter can also be a **Global** parameter if devices using the feature template use the same preshared keys.
- Next to ***IKE ID for Local Endpoint***, choose **Device Specific** from the drop-down box and type the variable (*IPsec_tunnel1_ike_local_id*) for the local ID value, which can be an IPv4 address, a domain name, or email address. The local ID value configured here must match the **Authentication Type** (**FQDN** or **IP**) value configured in the Zscaler Admin Portal in order for the IPsec tunnel to successfully come up.
- Next to ***IKE ID for Remote Endpoint***, choose **Device Specific** from the drop-down box and type the variable (*IPsec_tunnel1_ike_remote_id*) for the remote ID value. The remote ID value is the tunnel destination IP address or FQDN.

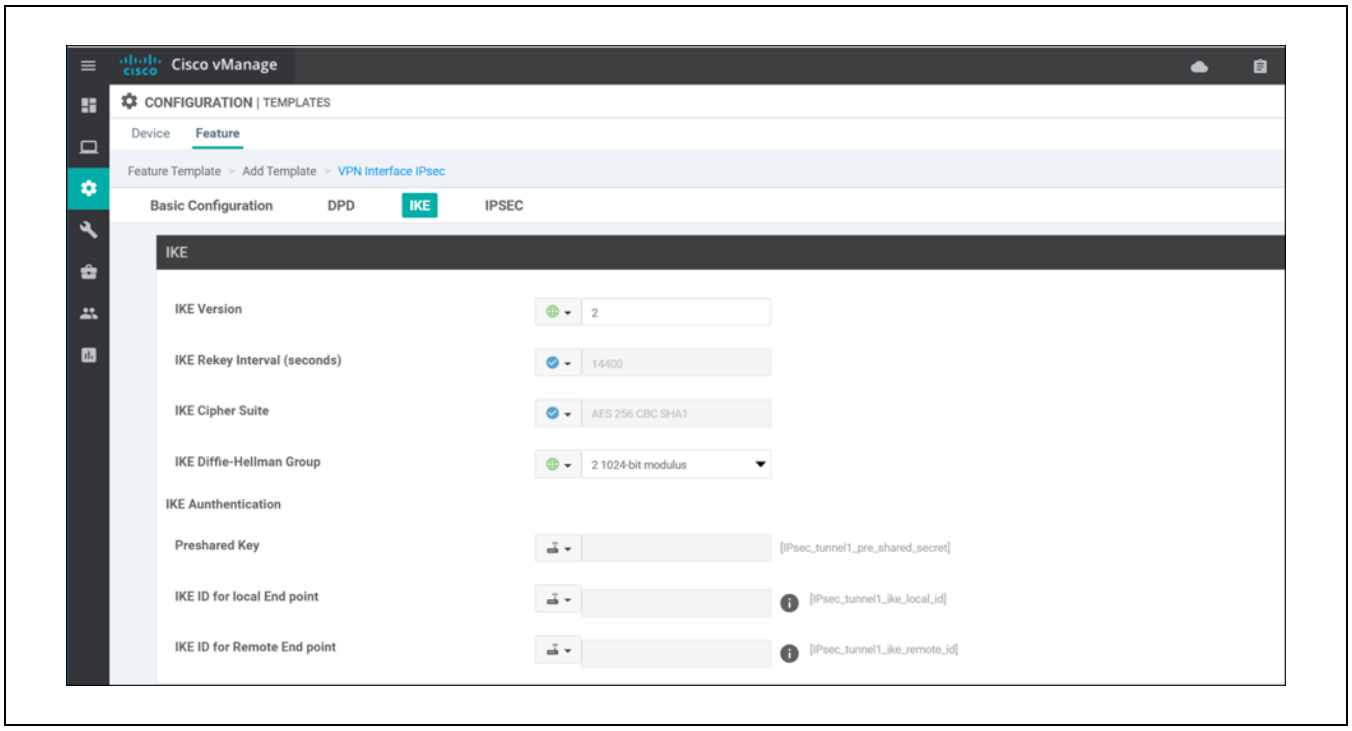


Figure 40: Configure IKE parameters

3.3.6 Configure IPsec Cipher-suite

Configure the IPsec parameters under the **IPSEC** section.

- Next to ***IPsec Cipher Suite***, choose **Global** from the drop-down box and choose *Null SHA1*.
- Next to ***Perfect Forwarding Secrecy***, choose Global from the drop-down box and choose *none.*

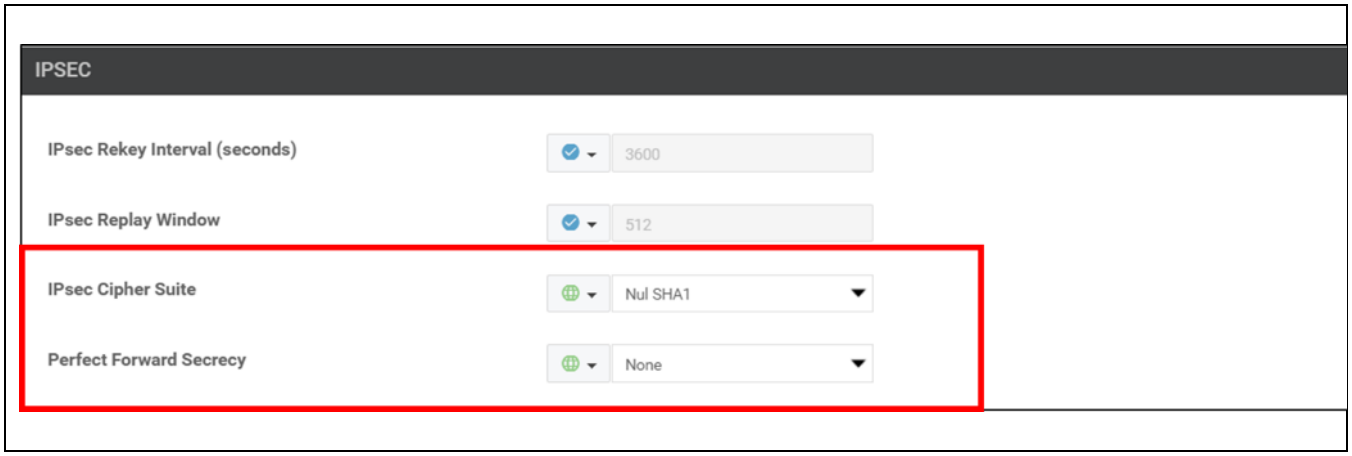


Figure 41: Configure IPsec Cipher-suite

Click **Save** to save the feature template.

3.3.7 Create Feature Template for the Secondary IPsec Tunnel

Copy the primary IPsec Tunnel feature template and modify parameters and variables for the secondary IPsec tunnel.

To the right of the newly-created feature template, *Zscaler-IPsec-Tunnel1*, click **…** and select **Copy** from the drop-down box. Type in a **Template Name** (*Zscaler-IPsec-Tunnel2*) and **Description** (*IPsec Tunnel 2 to Zscaler*) and click **Copy**.

To the right of the newly-copied feature template, click **…** and select **Edit** from the drop-down box.

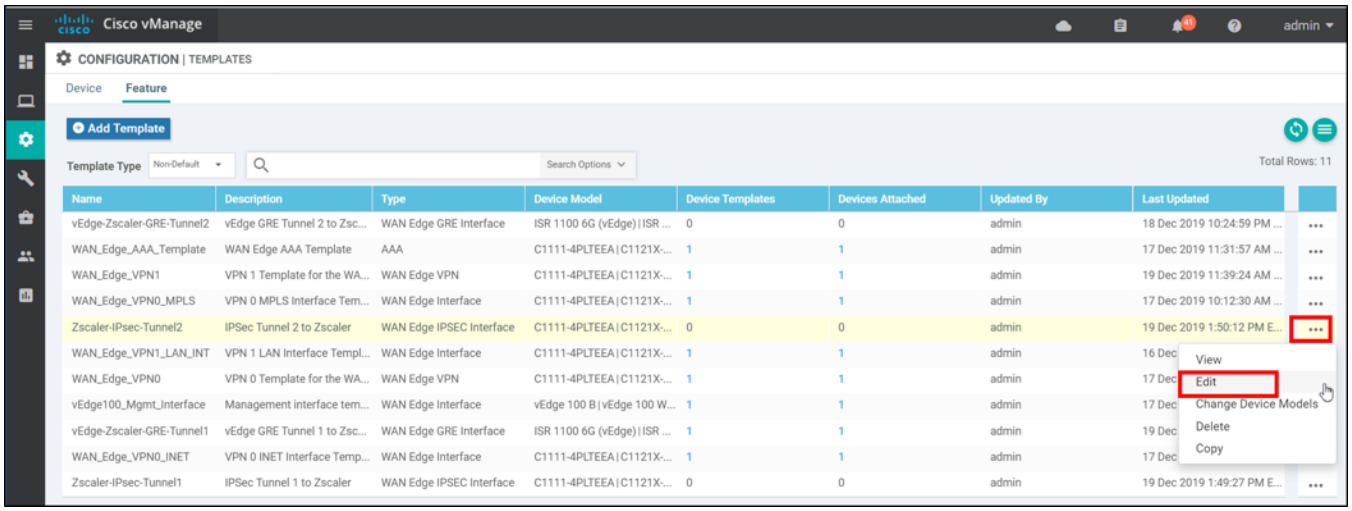


Figure 42: Edit Newly-copied Feature Template

Make the following modifications:

Interface Name = *ipsec2*
IPv4 address = IPsec_tunnel2_ipv4_address
IPsec Source Interface = *IPsec_tunnel2_source_interface*
IPsec Destination IP Address/FQDN = *IPsec_tunnel2_destination*
Preshared Key = *IPsec_tunnel2_pre_shared_secret*
IKE ID for Local End point = *IPsec_tunnel2_ike_local_id*
IKE ID for Remote End point = *IPsec_tunnel2_ike_remote_id*

Click **Update** to save the feature template.

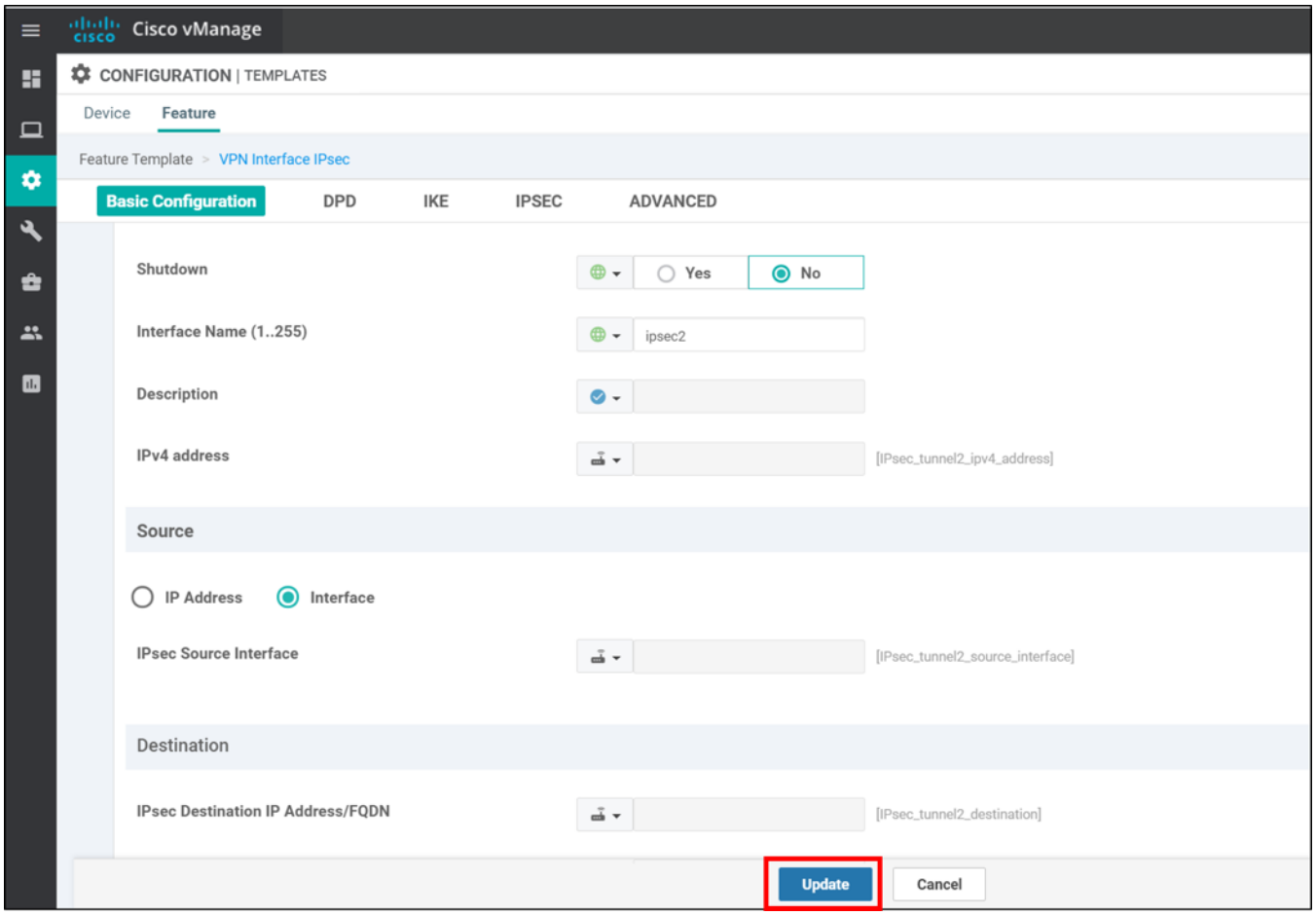


Figure 43: Modify New Feature Template

3.3.8 Add IPsec Interface Feature Template to Device Template

Next, the IPsec Interface feature templates are added to the device template. Navigate to **Configuration>Templates** and under the **Device** tab, identify the device template for the SD-WAN Edge router connecting to Zscaler (*WAN_Edge_Remote_A or WAN_Edge_Remote_B*). To the far right of the template, click **…** and select **Edit** from the drop-down box.

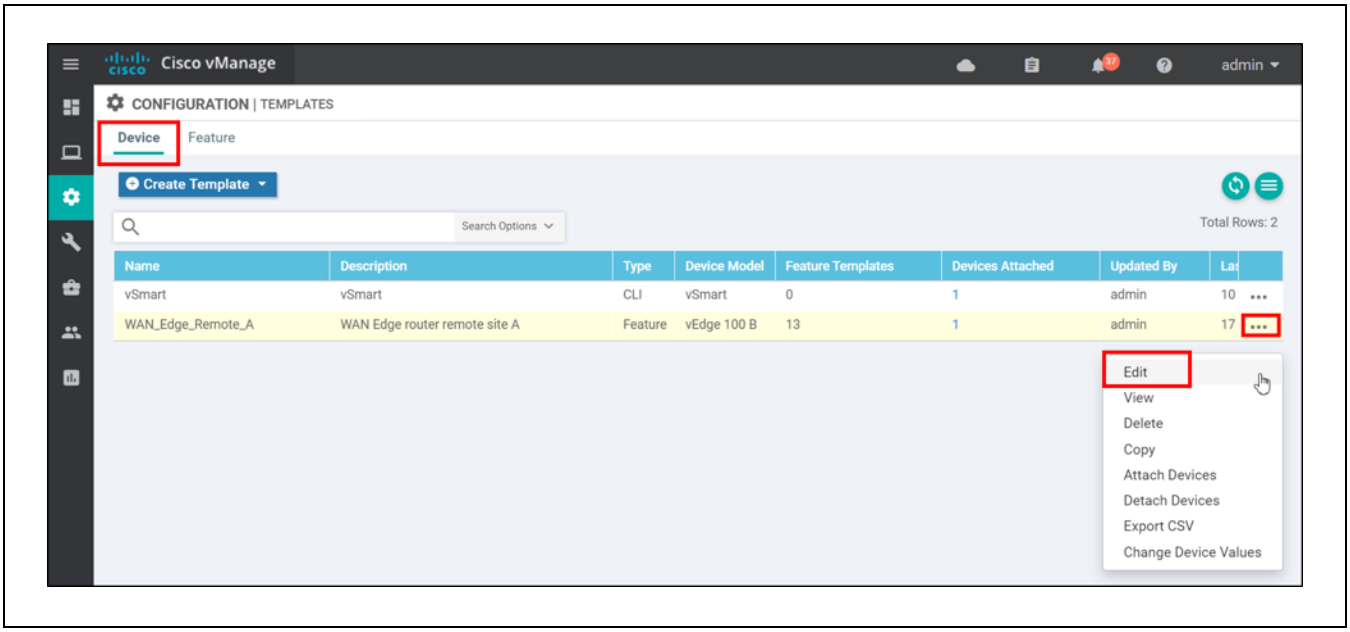


Figure 44: Device Templates List

3.3.9 VPN 0 or VPN 1 Template

For transport-side tunnels, add the IPsec tunnels under VPN 0 and for service-side tunnels, add the IPsec tunnels under VPN 1.

In the WAN_Edge_Remote_A (vEdge) device template, in the **VPN 0** section, click **(+) VPN Interface IPsec** on the right side two times to add both the primary and secondary IPsec tunnels.

In the WAN_Edge_Remote_B (IOS XE SD-WAN) device template, in the **Service VPN** section, click **(+) VPN Interface IPsec** on the right side two times to add both the primary and secondary IPsec tunnels.

Next to one **VPN Interface IPsec** entry, choose the *Zscaler-IPsec-Tunnel1* feature template from the drop-down box, and next to the other **VPN Interface IPsec** entry, choose the Zscaler-*IPsec-Tunnel2* feature template.

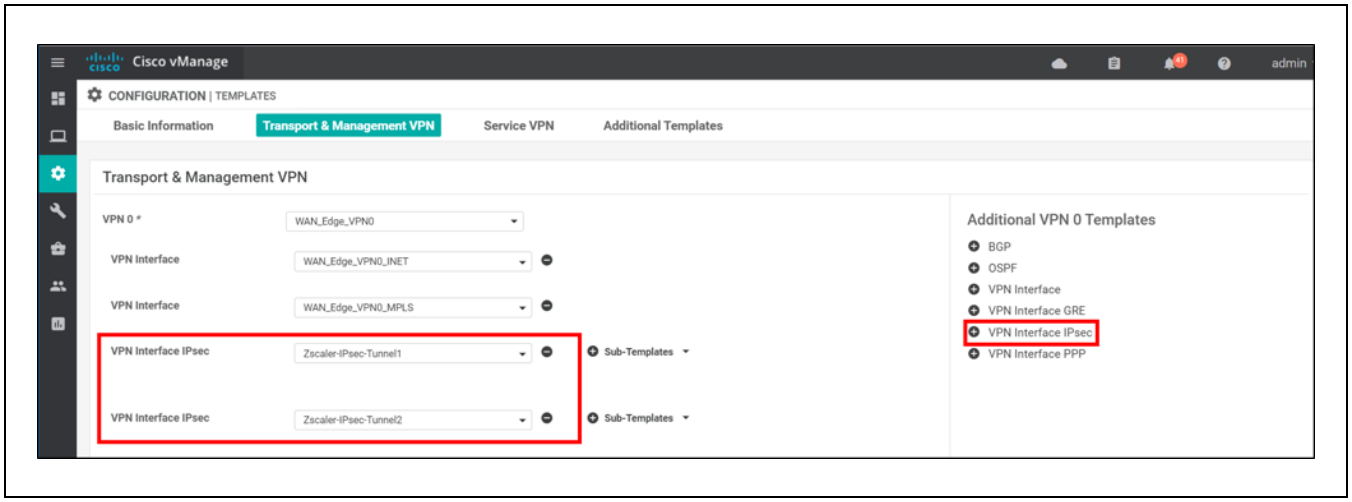


Figure 45: VPN0 Templates

3.3.10 Configuration Update

Click on the **Update** button at the bottom of the page to save the device template changes. If the device template was previously attached to an SD-WAN Edge router, a configuration update is performed and the updated device configuration pushed from vManage to the SD-WAN Edge router.

Because variables were created in the newly-added feature templates, the variables need to be defined before the configuration update can take place. To the right of the SD-WAN device attached to the device template, click **…** and select **Edit Device Template** from the drop-down box.

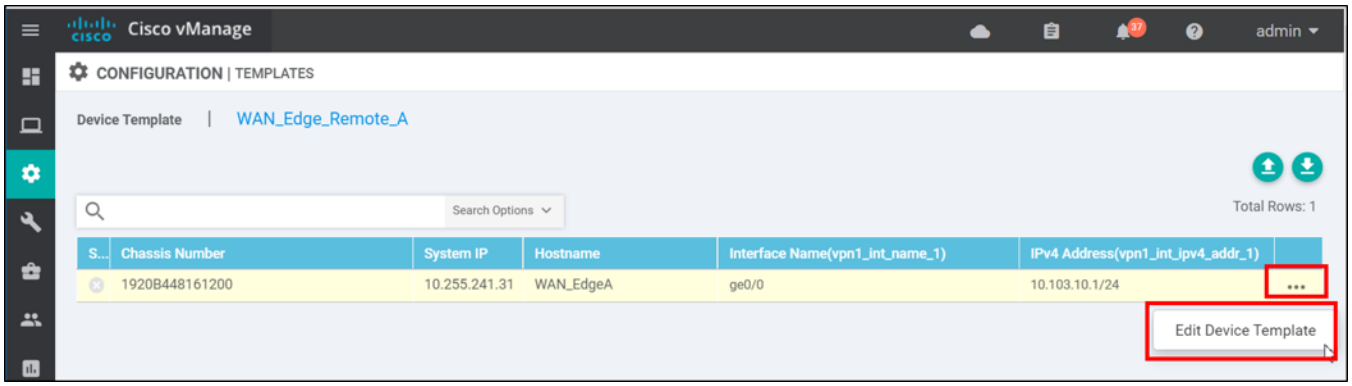


Figure 46: Configuration Update

The pop-up window prompts you to enter in the variable values. Fill in the values:

WAN_Edge_Remote_A (transport-side tunnel, vEdge router):

Primary IPsec Tunnel:
IPsec Destination IP Address/FQDN (IPsec_tunnel1_destination) = *was1-vpn.zscalerbeta.net*
IPv4 address (IPsec_tunnel1_ipv4_address) = *11.1.1.1/30*
Preshared Key (IPsec_tunnel1_pre_shared_secret) = *Cisco12345678901*
IKE ID for Local End point (IPsec_tunnel1_ike_local_id) = user@cisco.com
IKE ID for Remote End point (IPsec_tunnel1_ike_remote_id) = *104.129.194.39*

Secondary IPsec Tunnel:
IPsec Destination IP Address/FQDN (IPsec_tunnel1_destination)= *sunnyvale1-vpn.zscalerbeta.net*
IPsec Source Interface (IPsec_tunnel1_source_interface) = *ge0/4*
IPv4 address (IPsec_tunnel1_ipv4_address) = *11.1.2.1/30*
Preshared Key (IPsec_tunnel1_pre_shared_secret) = *Cisco12345678901*
IKE ID for Local End point (IPsec_tunnel1_ike_local_id) = user@cisco.com
IKE ID for Remote End point (IPsec_tunnel1_ike_remote_id) = *199.168.148.132*

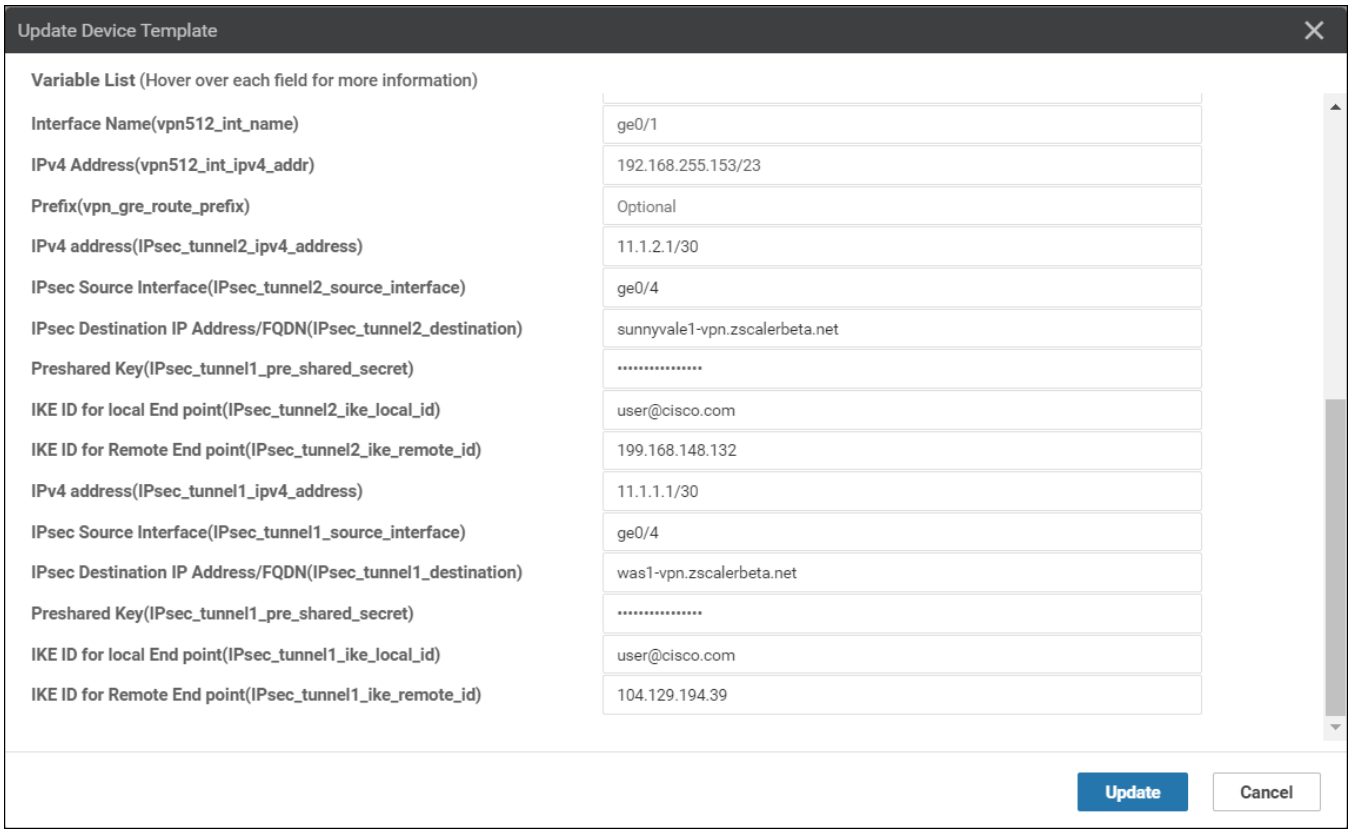


Figure 47: WAN_Edge_Remote_A Configuration Update

WAN_Edge_Remote_B (service-side tunnel, IOS XE SD-WAN router):

Primary IPsec Tunnel:
IPsec Destination IP Address/FQDN (IPsec_tunnel1_destination) = *104.129.194.39*
IPv4 address (IPsec_tunnel1_ipv4_address) = *12.1.1.1/30*
Preshared Key (IPsec_tunnel1_pre_shared_secret) = *Cisco12345678901*
IKE ID for Local End point (IPsec_tunnel1_ike_local_id) = user@cisco.com
IKE ID for Remote End point (IPsec_tunnel1_ike_remote_id) = *104.129.194.39*

Secondary IPsec Tunnel:
IPsec Destination IP Address/FQDN (IPsec_tunnel1_destination)= *199.168.148.132*
IPsec Source Interface (IPsec_tunnel1_source_interface) = *ge0/4*
IPv4 address (IPsec_tunnel1_ipv4_address) = *12.1.2.1/30*
Preshared Key (IPsec_tunnel1_pre_shared_secret) = *Cisco12345678901*
IKE ID for Local End point (IPsec_tunnel1_ike_local_id) = user@cisco.com
IKE ID for Remote End point (IPsec_tunnel1_ike_remote_id) = *199.168.148.132*

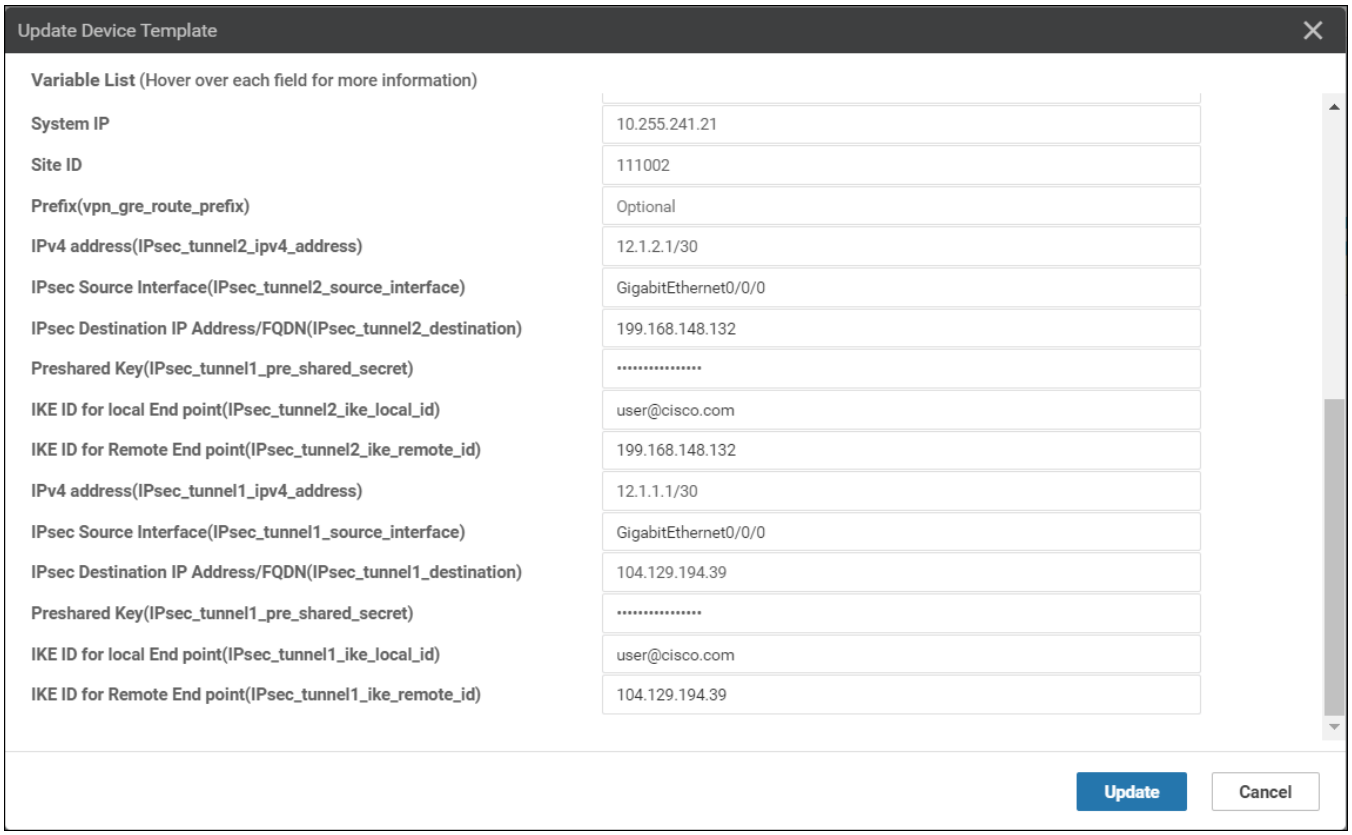


Figure 48: WAN_Edge_Remote_B Configuration Update

Click **Update**.

Click **Next**. Click **Configure Devices**.
The updated configuration is pushed to the SD-WAN router. The router returns with a **Success** status.

3.3.11 Add Service Routes

The IPsec tunnels have been added to VPN 0 (transport-side) or VPN 1 (service-side), so now statics routes are needed on the service-side VPN to direct user traffic to Zscaler through the IPsec tunnel.

For transport-side tunnels, IPsec routes are added to the service side in the vEdge device template. These routes point to a list of ipsec tunnel interfaces as their next-hops.
The first ipsec tunnel defined is primary and the second one listed is the backup interface which is used when the first one goes down.

For service-side tunnels, IPv4 routes are added to the service side in the IOS XE SD-WAN device template. These routes point to the remote side of the tunnels as their next hops. By default, the routes are both installed into the routing table and used in an active/active fashion

– traffic is hashed to one link or the other. To set up one tunnel as backup, configure a higher admin distance on the route referencing the backup tunnels as the next-hop.

In vManage go to **Configuration>Templates** and under the **Feature** tab, find the service VPN template (*WAN_Edge_VPN1* in this example). To the far right of the desired template, click **…** and select **Edit** from the drop-down box.

Routes for transport-side tunnels

Navigate to the **IPSEC Route** section of the feature template. Click **New IPSEC Route**. Note that the VPN 1 VPN template is shared with other routers and this configuration is applied to all devices using this feature template. You can create a separate VPN 1 feature template for routers utilizing the different types of tunnels, or you can make this route optional, and only apply the route to specific devices. When you define variables before a configuration is pushed to the router, you can leave this optional variable blank and the route is not applied to the device.

- Next to **Prefix**, select **Device Specific** from the drop-down box and type the variable, *vpn1_ipsec_route_prefix*.
- To make the route optional, click the checkbox next to **Mark as Optional Row**. If you do this before the **Prefix** variable is set, the **Prefix** field is locked and you cannot change the name of the variable.
- The VPN where the tunnel is located defaults to 0 and you cannot change it.
- Next to **IPSEC Interface**, select **Global** from the drop-down box and type *ipsec1,ipsec2*. These are the two IPsec tunnels created in the above steps. *ipsec1* becomes primary and *ipsec2* becomes secondary. Only when *ipsec1* goes down does *ipsec2* become active.

Click **Add** to add the route into the feature template.

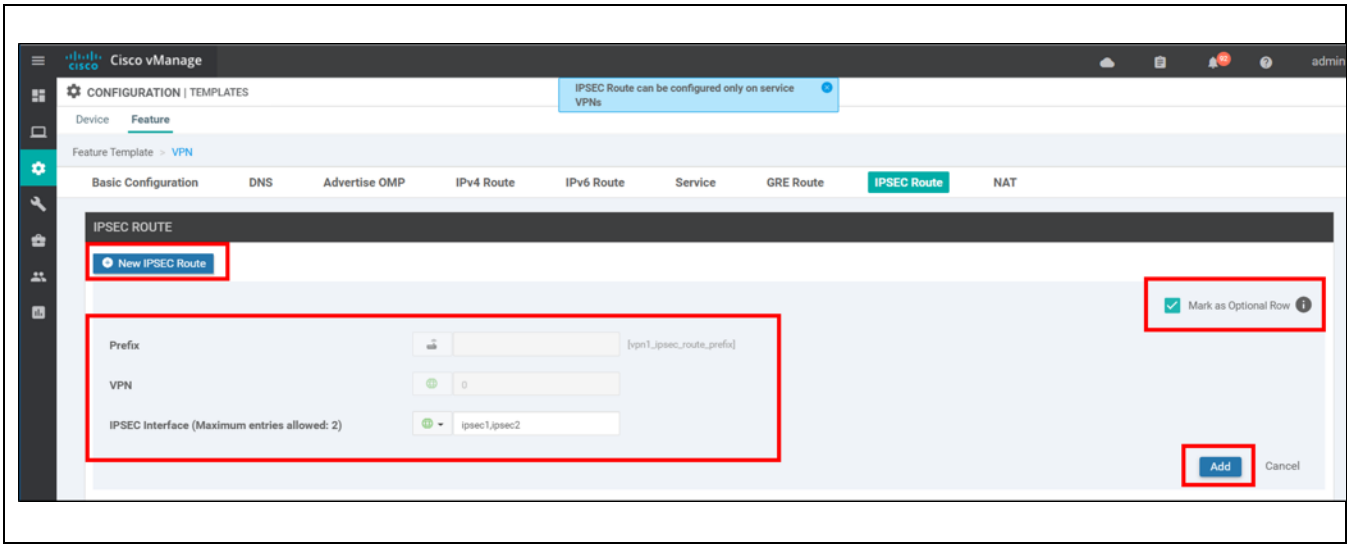


Figure 49: Add IPsec Route

Routes for service-side tunnels

Navigate to the **IPv4 Route** section of the feature template. Click **New IPv4 Route**. Note that the VPN 1 VPN template is shared with other routers and this configuration is applied to all devices using this feature template. You can create a separate VPN 1 feature template for routers utilizing the different types of tunnels, or you can make this route optional, and only apply the route to specific devices. When you define variables before a configuration is pushed to the router, you can leave this optional variable blank and the route is not applied to the device.

- Next to **Prefix**, select **Device Specific** from the drop-down box and type the variable, *vpn1_ipv4_prefix_to_zscaler*.
- To make the route optional, click the checkbox next to **Mark as Optional Row**. If you do this before the **Prefix** variable is set, the **Prefix** field is locked and you cannot change the name of the variable.
- Next to **Gateway**, keep **Next Hop** selected.
- Click **Add Next Hop**.

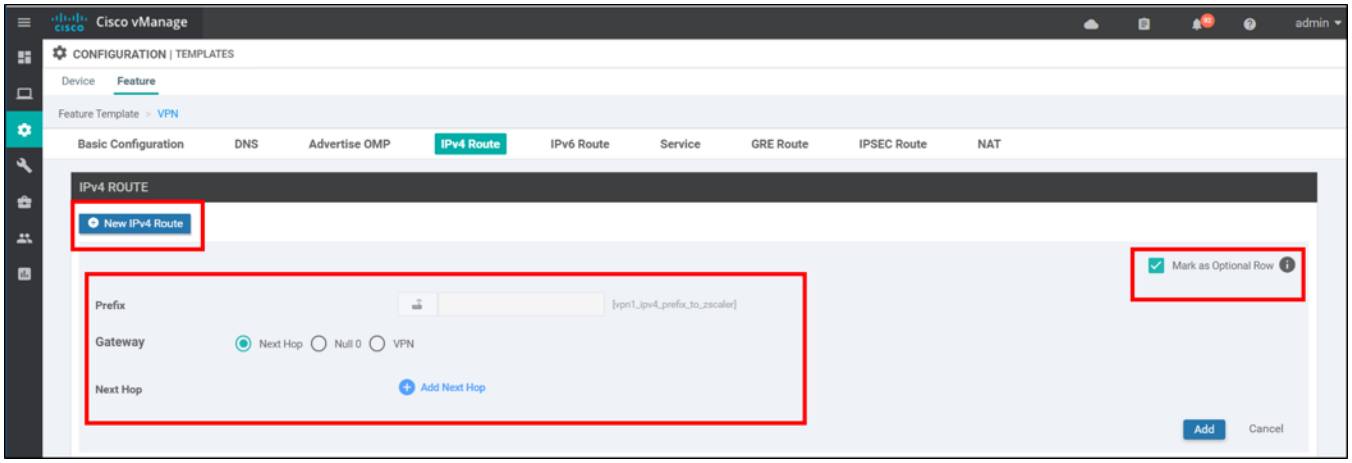


Figure 50: Add IPv4 Route

- In the pop-up window, click **Add Next Hop**.
- Under **Address**, select **Device Specific** from the drop-down box and type the variable, *vpn1_next_hop_zscaler_remote_end1*
- Click **Add Next Hop** to fill in the next hop over the secondary tunnel and select **Device Specific** from the drop-down box and type the variable, *vpn1_next_hop_zscaler_remote_end2*
- Modify any (admin) distance values if needed.
- Click **Add** to complete the next-hop configuration for the prefix.

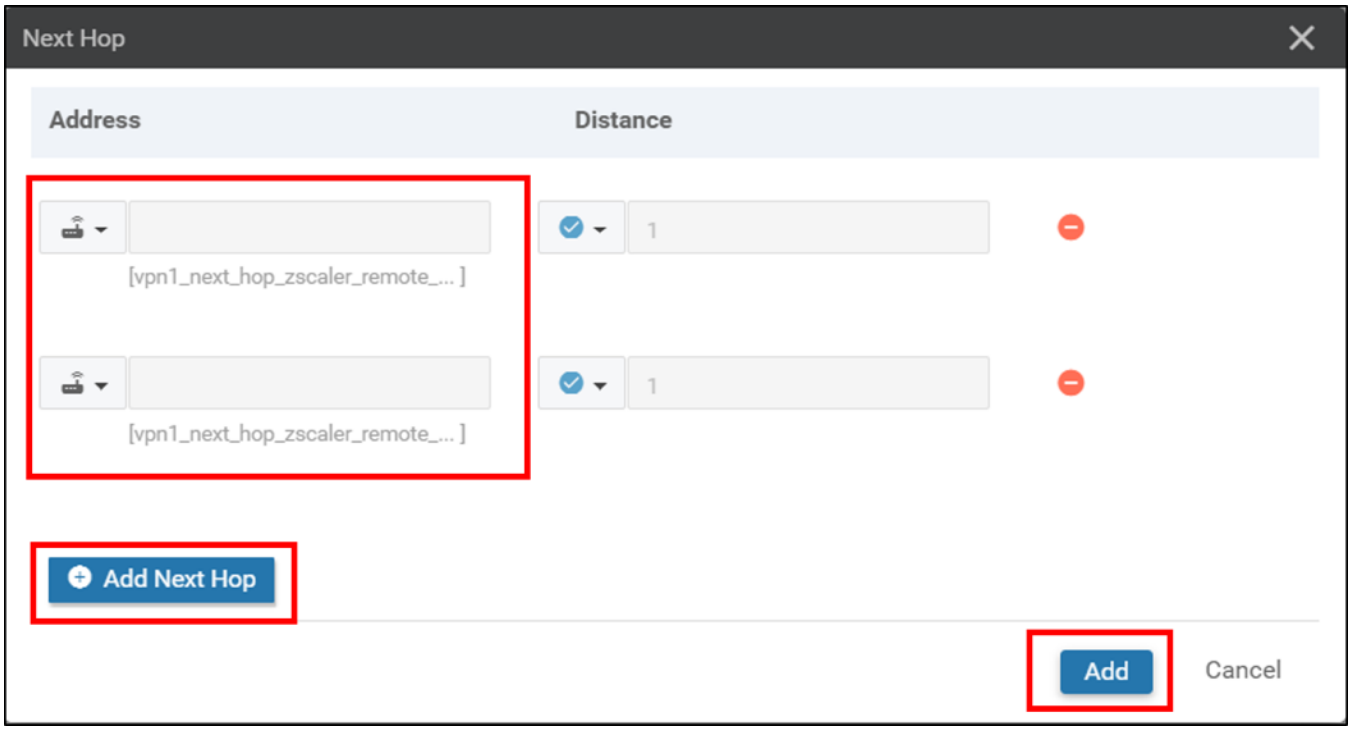


Figure 51: Configure Next-Hop Information for IPv4 Route

Click **Add** to add the route into the feature template and then click **Update** to save the feature template.

Note: Remember to click **Add** to add the route into the feature template before you click **Update**, or the route is not saved.

3.3.12 Configuration Update

If the device template was previously attached to an SD-WAN Edge router, a configuration update is performed and the updated device configuration pushed from vManage to the SD-WAN Edge router.

Because variables were created in the newly-modified feature templates, the variables need to be defined before the configuration update can take place. In the top left corner, ensure that **WAN_Edge_Remote_A** device template is selected. To the right of the device template, click **…** and select **Edit Device Template** from the drop-down box.

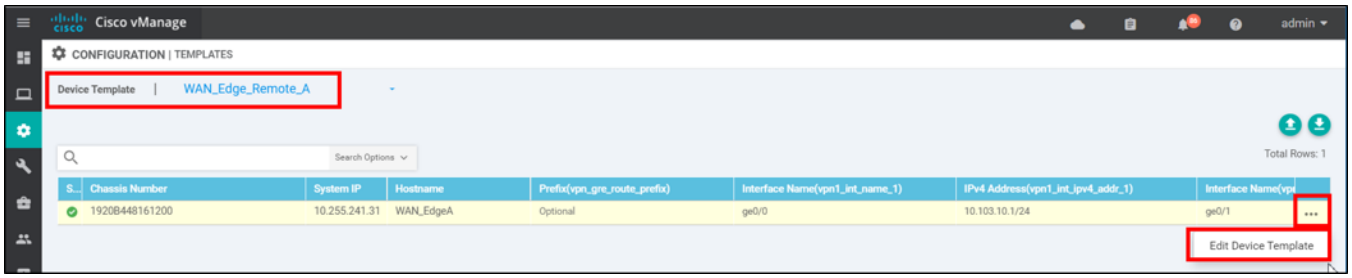


Figure 52: Configuration Update

The pop-up window allows you to enter in the newly-added variable values. All are optional. Fill in the following value for WAN_Edge_Remote_A (transport-side tunnel, vEdge router):

Prefix(vpn1_ipsec_route_prefix) = *0.0.0.0/0*

This variable adds a default route to the service VPN, pointing to ipsec1,ipsec2 as the next hops.

Click **Update**.

Figure 53: Configuration Update

Finish defining variables for the attached templates. In the top left corner, ensure that **WAN_Edge_Remote_B** device template is selected. To the right of the device template, click **…** and select **Edit Device Template** from the drop-down box.

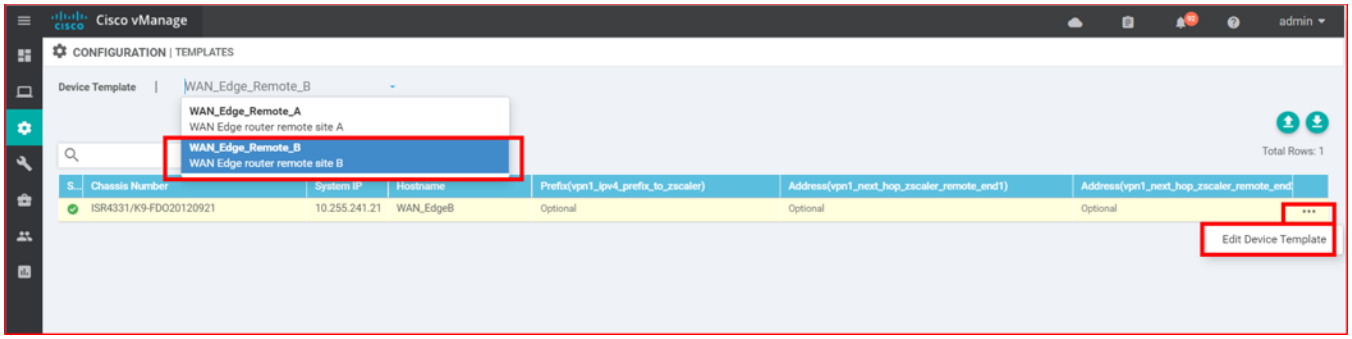


Figure 54: Configuration Update

The pop-up window allows you to enter in the newly-added variable values. All are optional. Fill in the following value for WAN_Edge_Remote_B (service-side tunnel, IOS XE SD-WAN router):

Prefix(vpn1_ipv4_prefix_to_zscaler) = *0.0.0.0/0*
Address(vpn1_next_hop_zscaler_remote_end1) = *12.1.1.2*
Address(vpn1_next_hop_zscaler_remote_end2) = *12.1.2.2*

This variable adds 2 default routes to the service vpn, pointing to 12.1.1.2 and 12.1.2.2 as the next hops.

Click **Update**.

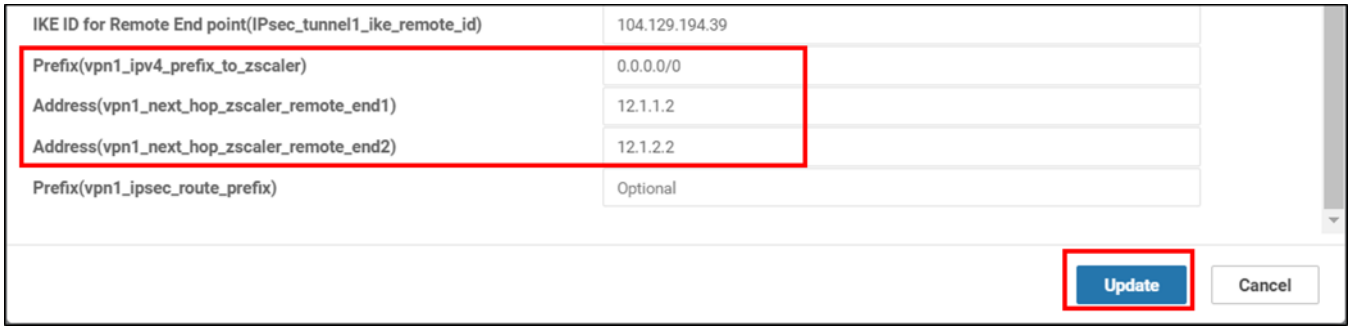


Figure 55: Configuration Update

Click **Next**. Click **Configure Devices**. In the pop-up window, confirm the configuration changes and click **OK**. The updated configuration is pushed to the SD-WAN router. The router returns with a **Success** status.

3.3.13 IOS XE SD-WAN IPsec Tunnel Workarounds

At this point, the IOS XE SD-WAN IPsec tunnels are configured, but not fully operational. There are a few workarounds that need to be implemented to allow the tunnels to work fully.

The following workarounds should be implemented:

1) Host routes should be added for the tunnel destinations in VPN 0.
2) Disable IKE Config Exchange – vManage version 19.2.1 pushes this configuration, but in this version of code, it needs to be configured manually via CLI.
3) An ACL should be implemented to explicitly allow IPsec traffic.

Do switch to CLI mode, go to the vManage GUI and go to **Configuration>Devices**. Click **Change Mode** and select **CLI mode** from the drop-down box.

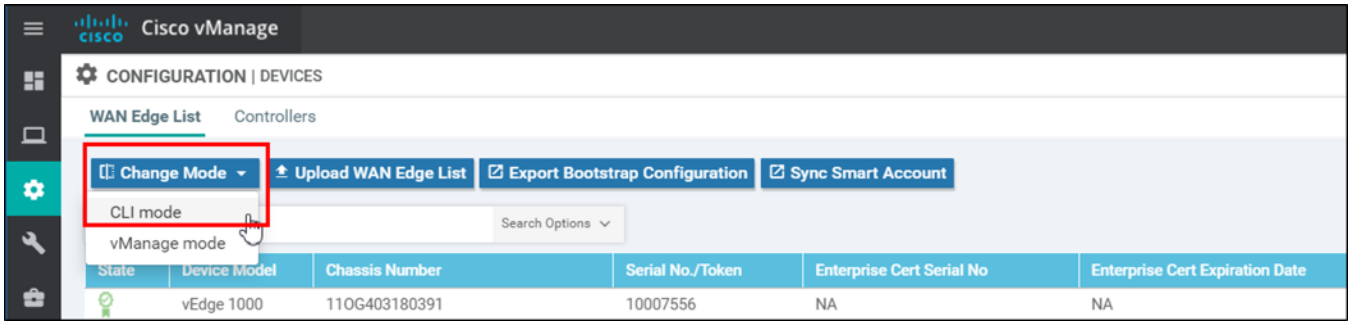


Figure 56: Change Mode

Select the device (**WAN_EdgeB**) on the left-hand side, move it to the right-hand side, and click **Update to CLI Mode**.

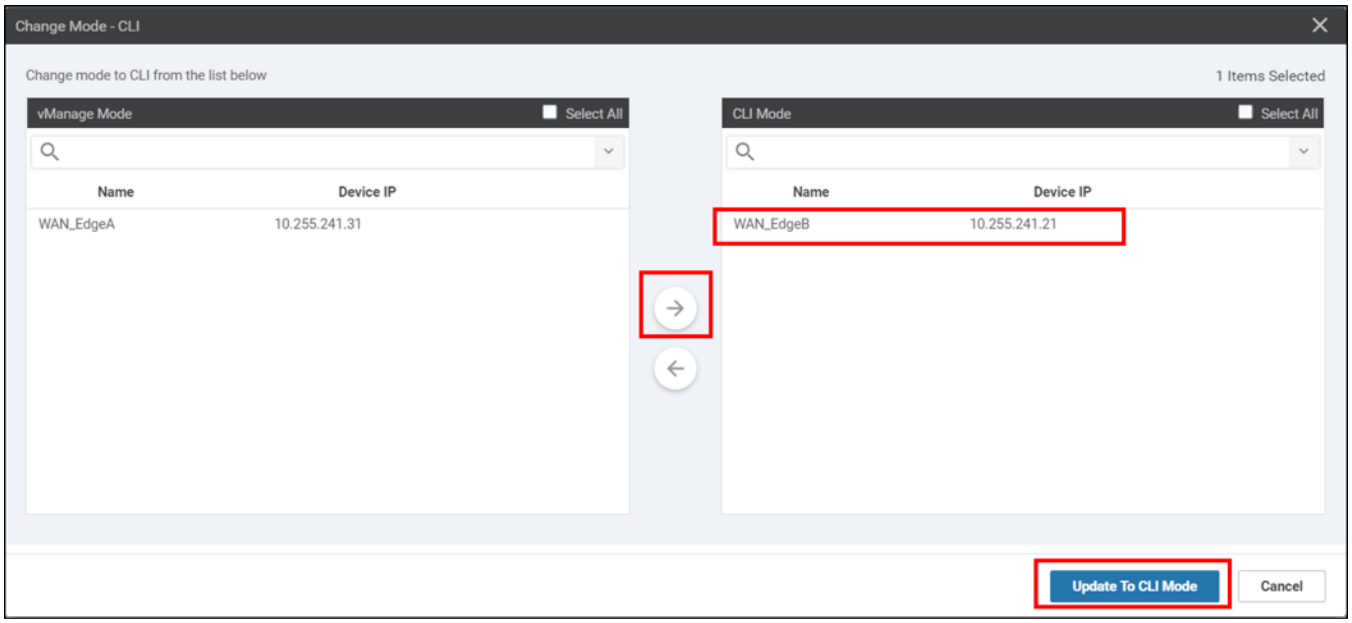


Figure 57: Change Mode

The router returns back with success.

Console or SSH to WAN_EdgeB, and configure the following:

1) Host routes in VPN 0 for the tunnel destinations:

```
config-t

ip route 104.129.194.39 255.255.255.255 64.102.254.152
ip route 199.168.148.132 255.255.255.255 64.102.254.152
commit
```

Disable IKE Config exchange (note this not survive reboots).

```
crypto ikev2 profile if-ipsec1-ikev2-profile
config-exchange request
commit
no config-exchange request
commit

crypto ikev2 profile if-ipsec2-ikev2-profile
config-exchange request
commit
no config-exchange request
commit
```

2) Add ACL to allow IPsec traffic. This example lets in traffic from the IPsec tunnel endpoints.

```
policy
 access-list PERMIT-ZSCALER-ZENS
  sequence 1
   match
    source-ip 199.168.148.132/32
   !
   action accept
   !
  !
   exit
  exit
  sequence 2
   match
    source-ip 104.129.194.39/32
  !
   action accept
   !
  !
  default-action accept
!
sdwan
interface GigabitEthernet0/0/0
access-list PERMIT-ZSCALER-ZENS in
commit
```

Note: You can try a `clear crypto session` command if IKE Config Exchange was disabled after IKE was negotiated.

3.3.14 Verify Tunnel Operation

In vManage, go to **Monitor>Network** and click the device of interest (*WAN_EdgeA or WAN_EdgeB*). On the left-hand side, click **Interface**. View the status and traffic statistics for the tunnel interfaces.

Note: In IOS XE SD-WAN code, the tunnel interfaces ipsec1 and ipsec2 translate into Tunnel10000x nomenclature.

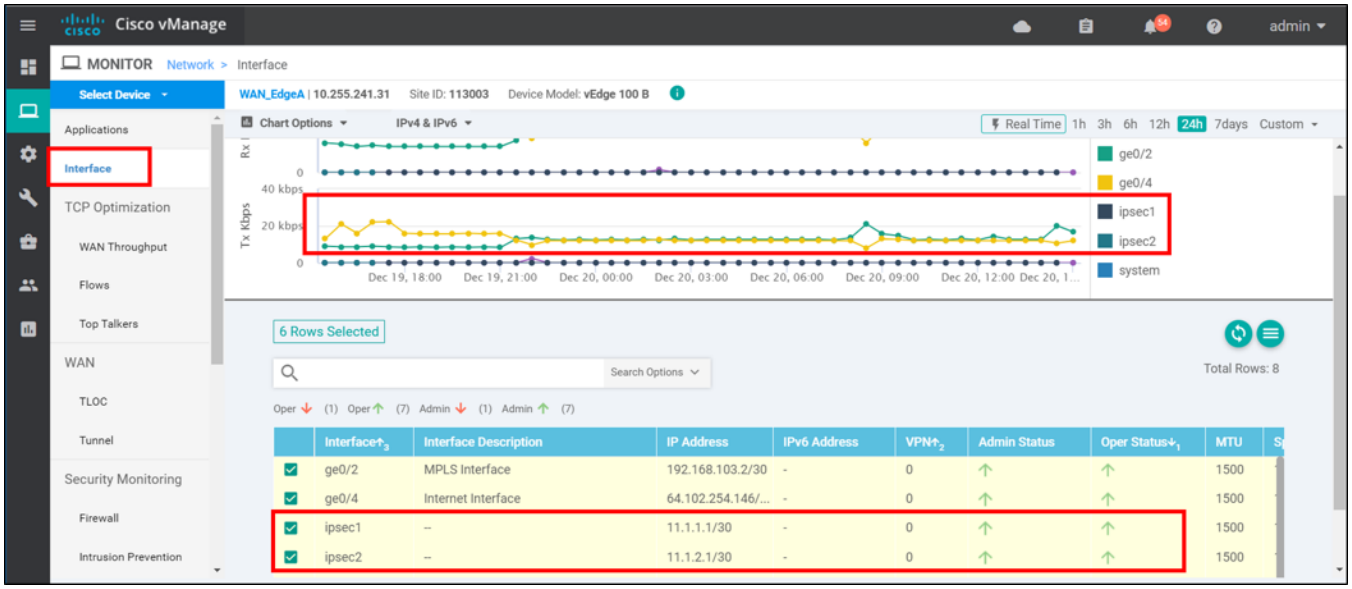


Figure 58: Check Tunnel Status

To view the primary IPsec route, on the left-hand side, click **Real Time**, then in the **Device Options** box, select **IP Routes**. A pop-up window asks you to choose filters to display data faster. Click **Do Not Filter**.

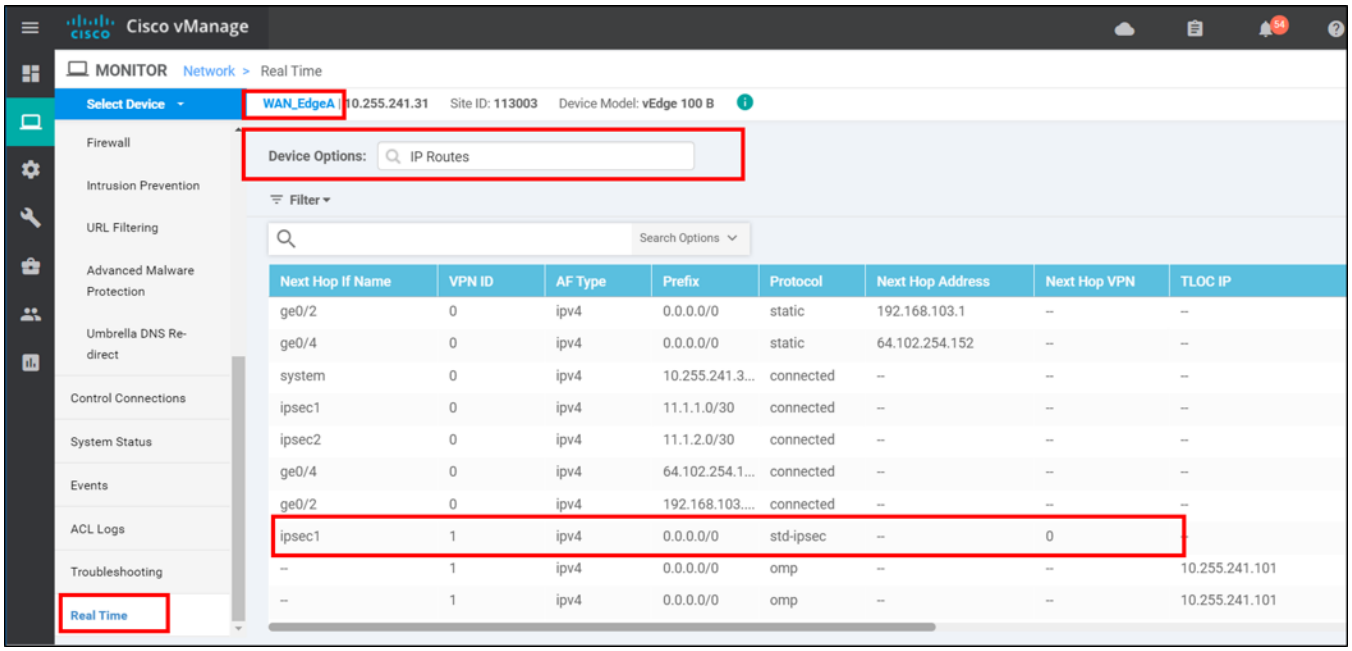


Figure 59: View IPsec Route

3.4 Configuring Layer 7 Health Checks

This section applies to the vEdge router. In this section, a vEdge router with an IPsec transport-side tunnel is assumed, so the ipsec1 tunnel is the primary tunnel and the ipsec2 tunnel is the backup tunnel. An L7 health check, or tracker, is configured for the primary tunnel. The tracker is configured for an interval of 10 seconds, which is interval at which tracker probes are sent. The multiplier is kept to the default of 3, which is how many retries until the tunnel is reported as down.The threshold value, which is the maximum round trip time a tracker probe can have, is left at the default of 300 msec. If the tracker fails or exceeds the SLA threshold, the route to the primary tunnel is removed from the table and the route for the backup tunnel is inserted into the routing table.

To configure layer 7 health checks, the tracker names and destinations are defined in the system template, and then any tracker name can be referenced in the interface IPsec or GRE tunnel template.

3.4.1 Feature and Device Template Modifications

The following feature and device template modifications are added to the base configurations and existing IPSEC tunnel template. See section 3.4.2 for step-by-step details for configuring.

System feature template

Devices: All vEdge routers **Template**: **Basic Information/System**
Template Name: *vEdge_System_Tracker* **Description**: *System Template with Zscaler Trackers*

Section	Parameter	Type	Variable/value
Tracker	Name	Global	l7_zscaler_health_check1
	Interval	Global	10
	API url of endpoint	Global	http://gateway.zscalerbeta.net/vpntest

VPN Interface IPsec feature template

Devices: All vEdge routers **Template**: **VPN/VPN Interface IPSEC**
Template Name: *Zscaler-IPsec_Tunnel1-with-Tracker* **Description**: *IPsec Tunnel 1 to Zscaler with Tracker*

Section	Parameter	Type	Variable/value
Advanced	Tracker	Global	l7_zscaler_health_check1

Device Template (transport-side, WAN_Edge_Remote_A (vEdge)):

Template type	Template sub-type	Template name
Basic Information	**System**	**vEdge_System_Tracker_Template**
	AAA	WAN_Edge_AAA_Template
VPN0	VPN	WAN_Edge_VPN0
	VPN Interface	WAN_Edge_VPN0_INET
	VPN Interface	WAN_Edge_VPN0_MPLS
	VPN Interface IPSEC	**Zscaler-IPsec-Tunnel1-with-Tracker**
	VPN Interface IPSEC	Zscaler-IPsec-Tunnel2
VPN 512	VPN Interface	WAN_Edge_VPN512_Template
VPN1	VPN	WAN_Edge_VPN1
	VPN Interface	WAN_Edge_VPN1_LAN_INT

3.4.2 Add System Template with Tracker

In this section, the default System template is copied and a new System template is created with a tracker configured.

Go to **Configuration>Templates**, and click the **Feature** tab. Next to **Template Type**, select **Default** from the drop-down box and type *vEdge_System* in the search box and press return. To the right of *Factory_Default_vEdge_System_Template*, click **…** and select **Copy** from the drop-down box.

Configure a **Template Name** (*vEdge_System_Tracker*) and **Description** (*System template with Zscaler Trackers*). Click **Copy**.

Next to **Template Type**, select **Non-Default**. Next to the newly-copied template, click **…** to the far right and select **Edit** from the drop-down box.

Under the **Tracker** section, click **New Tracker**. Type a **Name** for the tracker (*I7_zscaler_health_check1*). Next to **Interval**, select **Global** and type *10*. Next to **Endpoint Type**, select the **URL** radio button. Next to **API url of endpoint**, type a URL destination (http://gateway.<zscalercloud>.net/vpntest). Click **Add**.

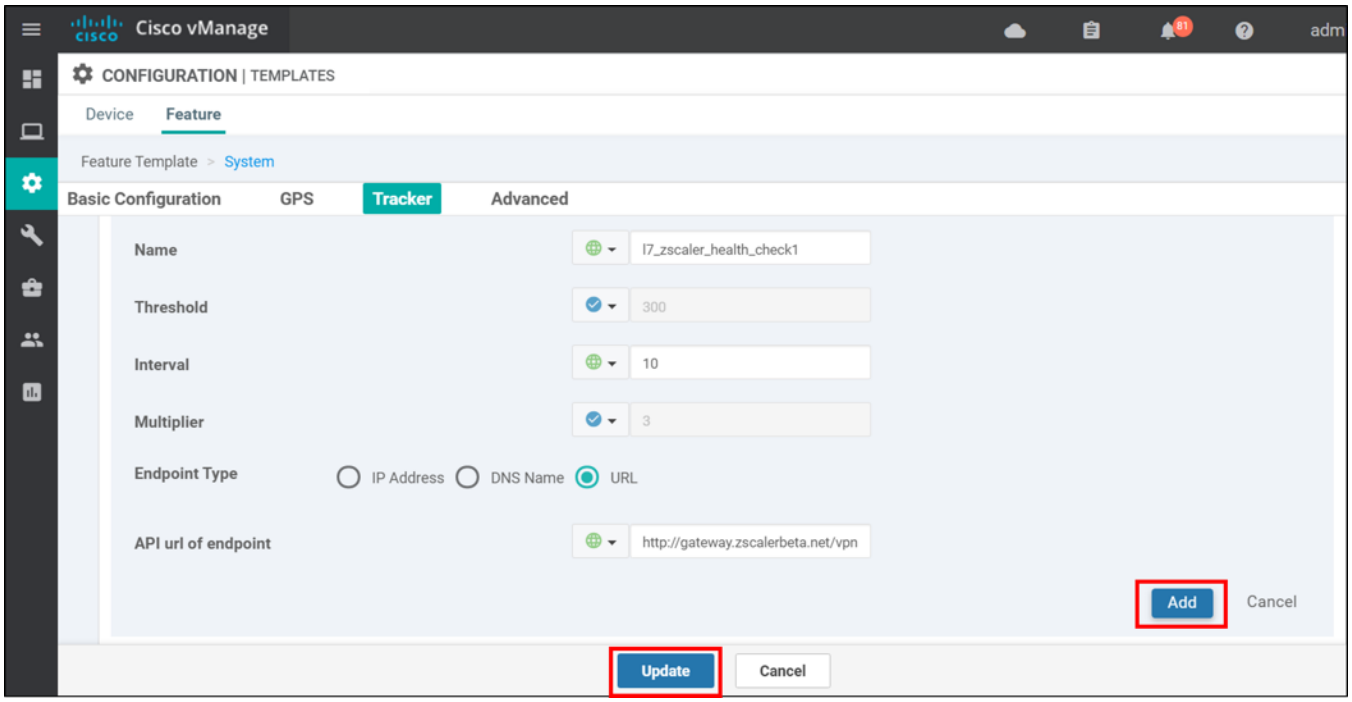


Figure 60: Configure Tracker in System Template

Repeat the previous steps to add any additional trackers. Click **Update** to complete the configuration.

3.4.3 Add IPSEC Tunnel Interface with a Tracker

The tracker defined in the system configuration can be applied to the tunnels in the IPSec and GRE tunnel templates and are non-optional configurations, so tunnel interface templates can be copied and applied only to devices using the tracker.

Note: You cannot apply the tracker to the interface without the tracker defined in the system template.

In the vManage GUI, under **Configuration>Templates>Features**, copy the *Zscaler-IPsec-Tunnel1* configuration by clicking **…** to the right of the template and selecting **Copy.** Enter a new **Name** (*Zscaler-IPsec-Tunnel1-with-Tracker*) and **Description** (*IPsec Tunnel 1 to Zscaler with Tracker*).

Edit the newly-copied template. Under the **Advanced** section, next to **Tracker**, select **Global** from the drop-down list and type the tracker defined in the System template (*I7_zscaler_health_check1* in this case). Click **Update** to save the Tunnel Interface template.

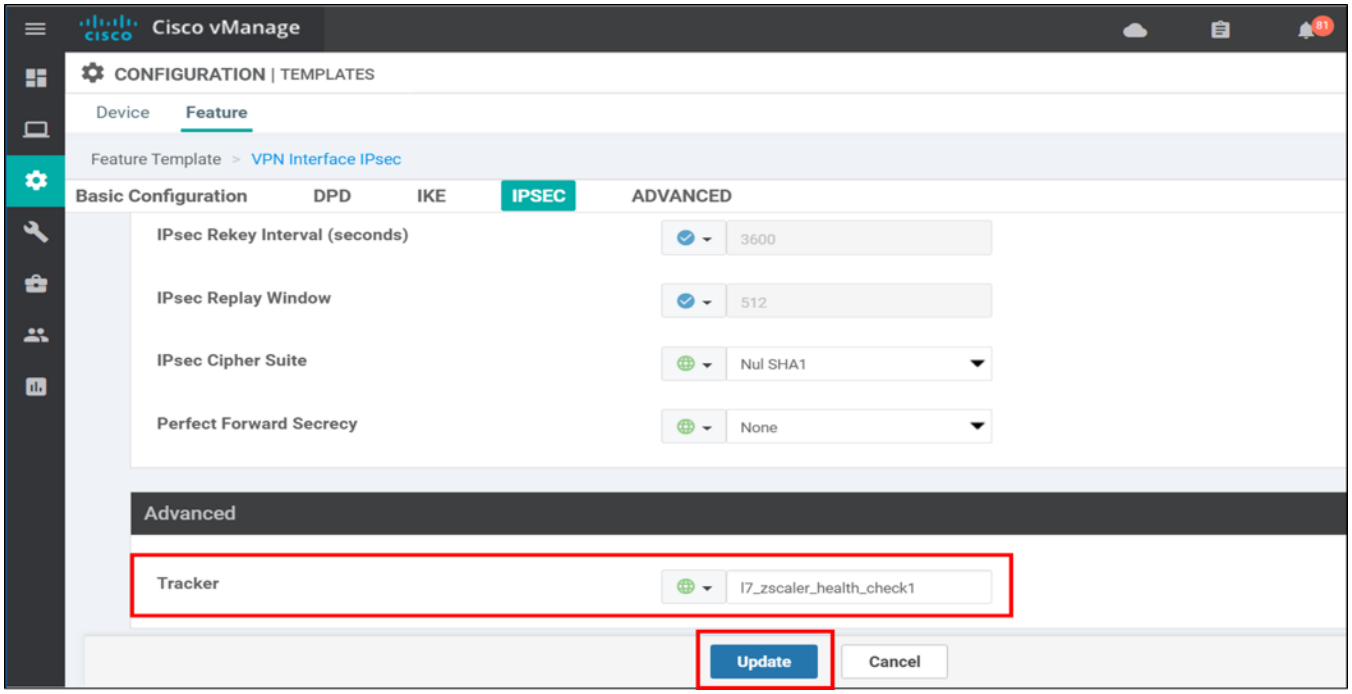


Figure 61: Configure Tracker in Tunnel Interface Template

Repeat creating new tunnel templates if needed.

3.4.4 Add New Feature Templates to the Device Templates

Now, add the new tracker configuration templates to the device template. Go to **Configuration>Templates** and ensure you are on the **Device** tab. To the right of the desired device template, click **…** and select **Edit** from the drop-down box.

Next to **System**, choose the System template with the tracker configuration (*vEdge_System_Tracker*) and next to the tunnel interface, select the new tunnel interface template with the tracker defined (*Zscaler-IPsec_Tunnel1-with-Tracker*). Add any additional ones if you are using. Click **Update** to save the device template configuration.

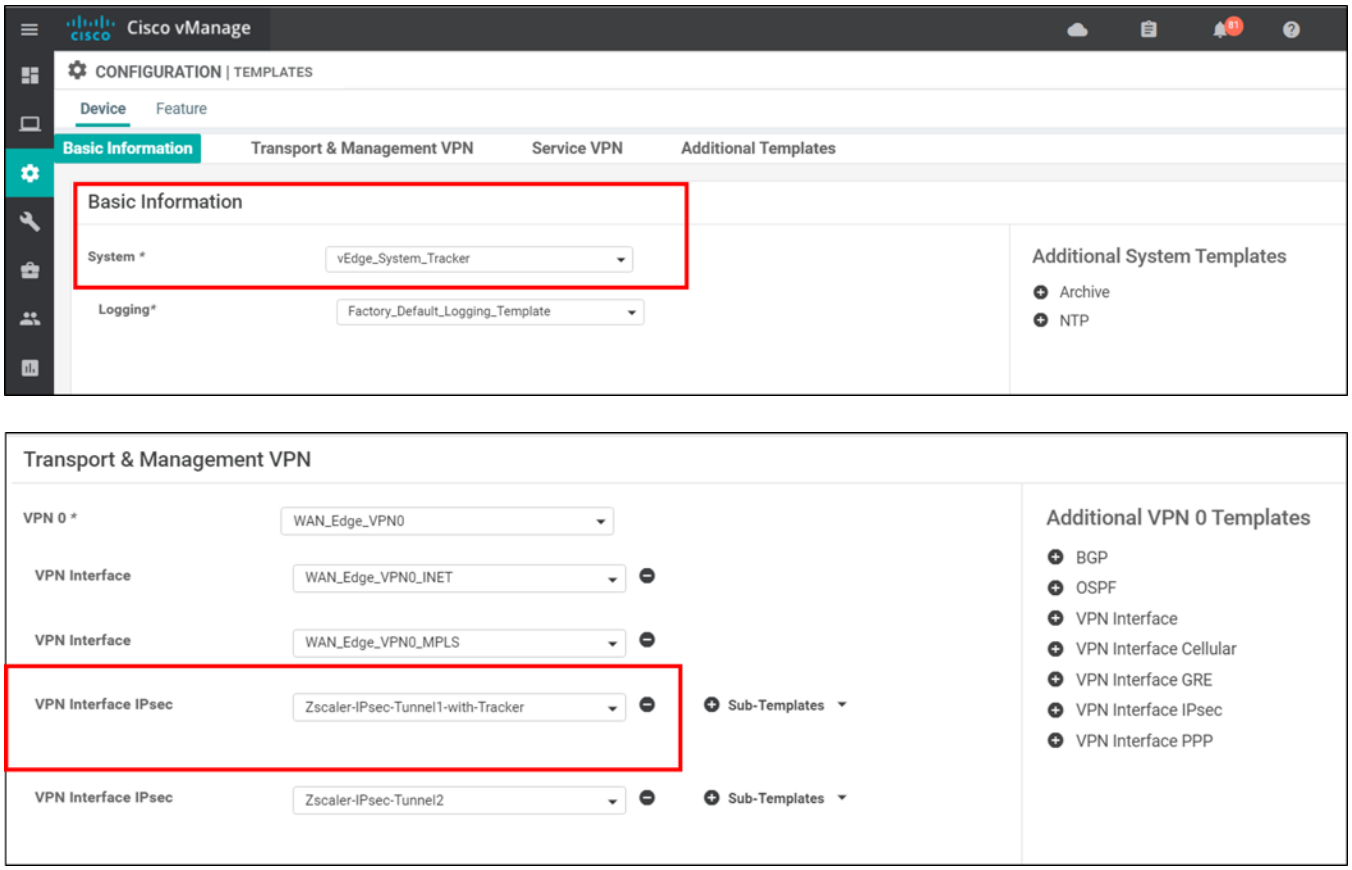


Figure 62: Configure Device Template

No variables need to be defined, so click **Next**, then **Configure Devices** and vManage should return back with success.

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 63: Non-working Example

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

Figure 64: Working Example

5 Requesting Zscaler Support

5.1 Gather Support Information

Zscaler support is required to provision new locations for GRE. 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**.

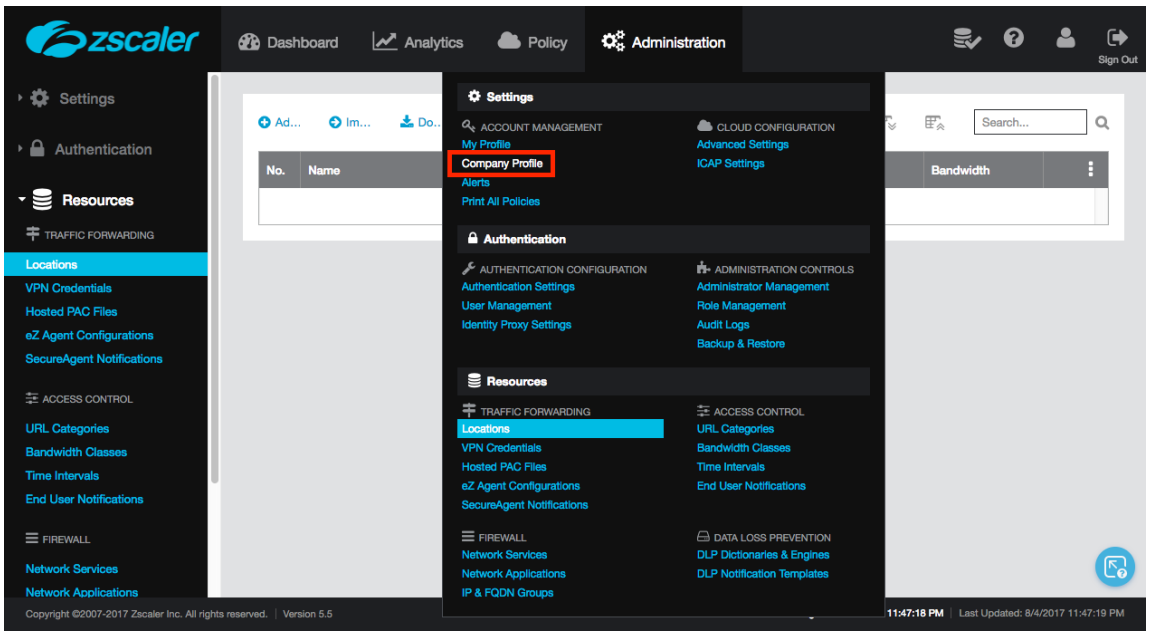


Figure 65: Obtaining Company ID

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.

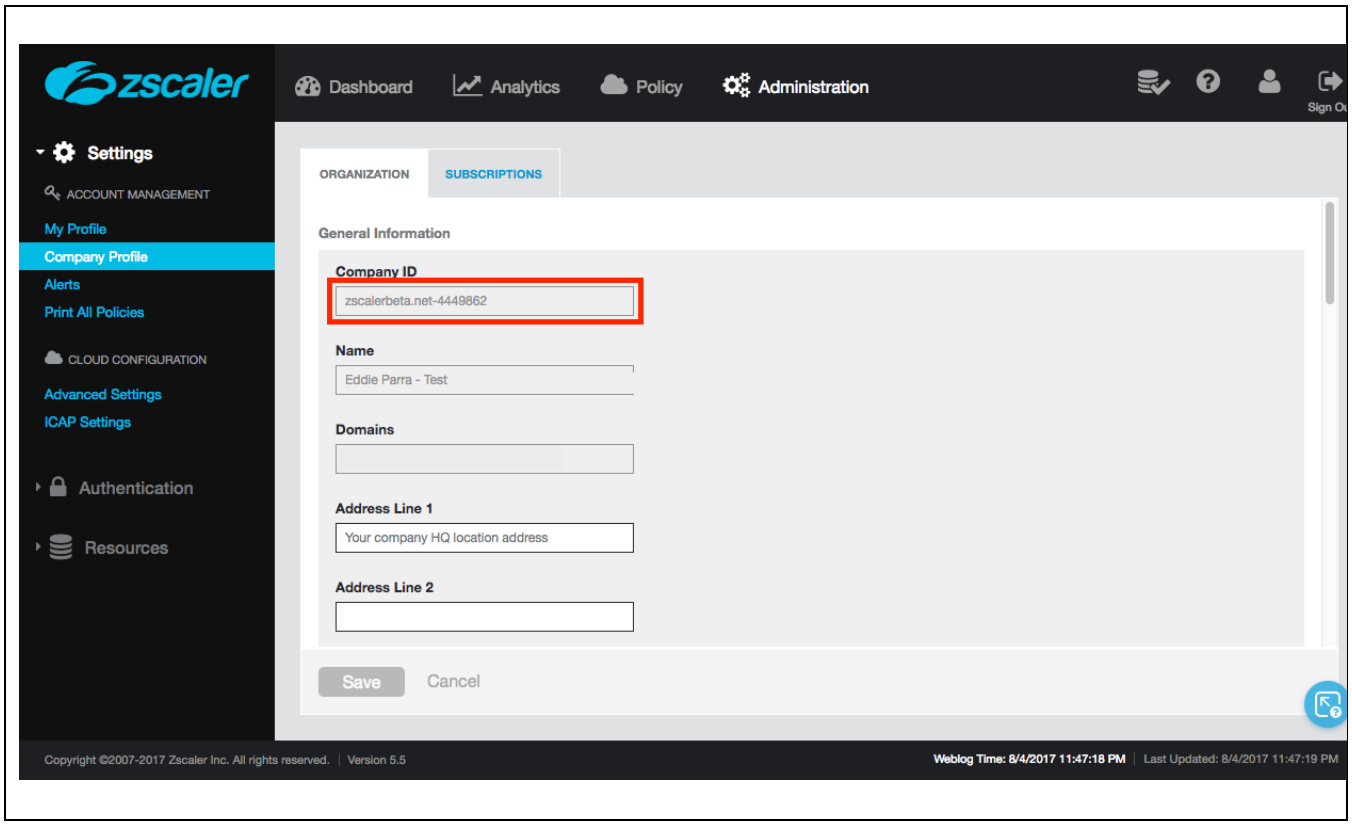


Figure 66: Save Company ID

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**.

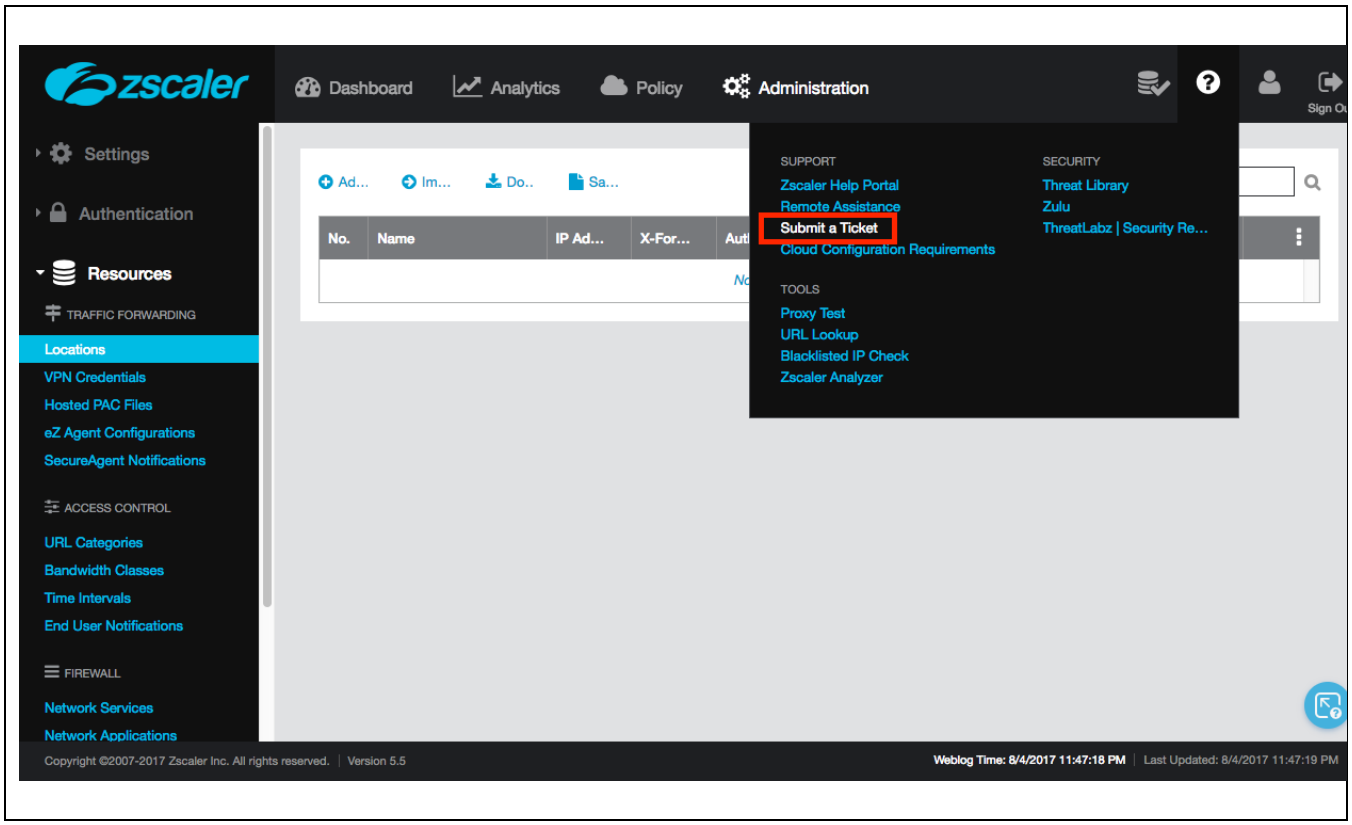


Figure 67: Enter Support Section

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.

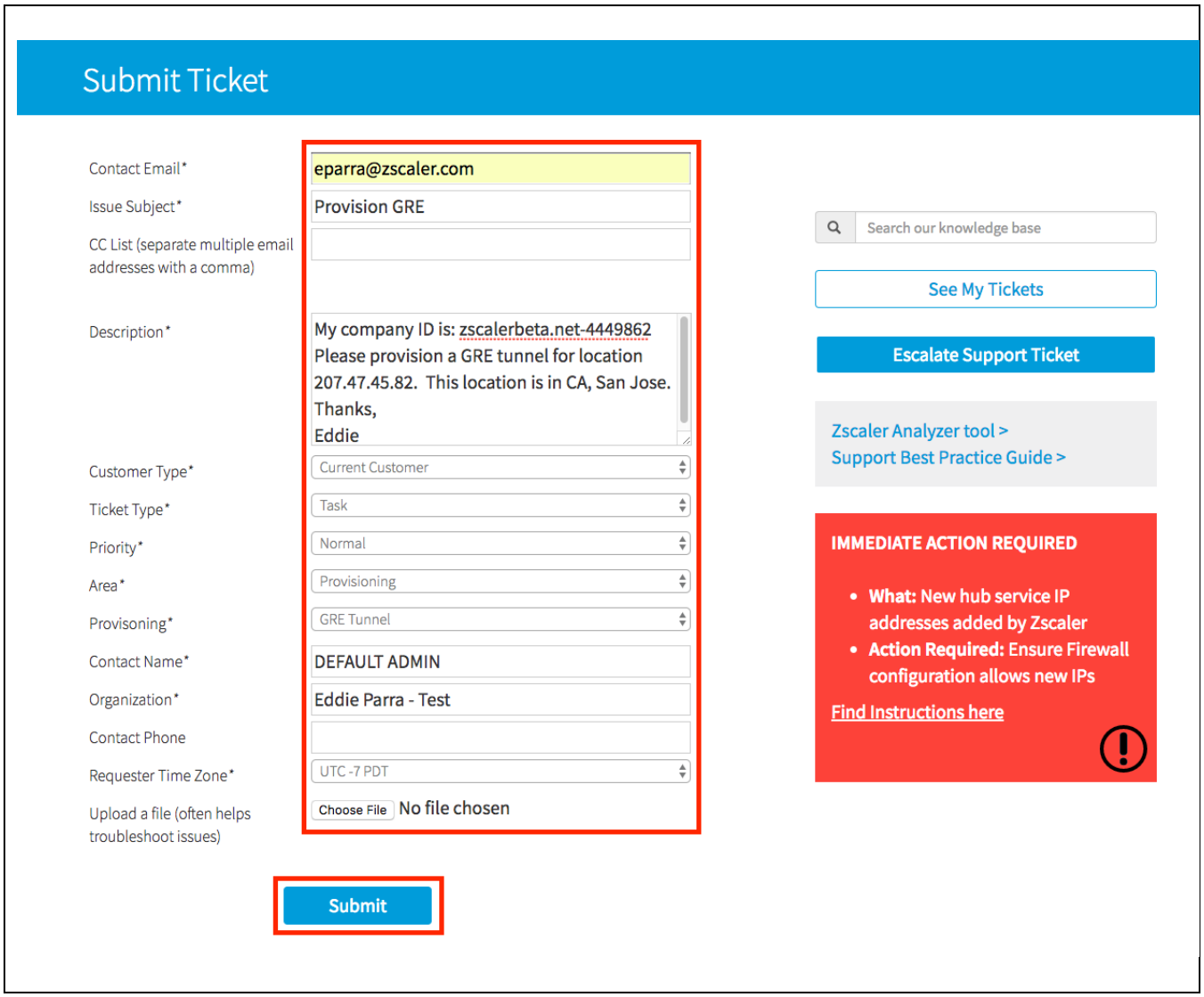


Figure 68: Creating a Support Ticket

5.1.5 Reviewing Provisioning Email

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

The request has been processed and the GRE tunnel has been configured. The details are given below:

```
------------------------------------------------------------------------
Tunnel Source IP:    64.102.254.146
Internal Range:  172.17.12.216-172.17.12.223

Primary Destination:    104.129.194.38
Internal Router IP:    172.17.12.217/30
Internal ZEN IP:    172.17.12.218/30

Secondary Destination:    199.168.148.131
Internal Router IP:    172.17.12.221/30
Internal ZEN IP:    172.17.12.222/30
------------------------------------------------------------------------
```

Figure 69: 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/

ZIA Datacenters (by cloud)
https://ips.zscaler.net/cenr/
https://ips.zscalerbeta.net/cenr/
https://ips.zscalerone.net/cenr/
https://ips.zscalertwo.net/cenr/
https://ips.zscalerthree.net/cenr/

7 Appendix B: Cisco SD-WAN Resources

7.1 Cisco SD-WAN References

For an overview on the Cisco SD-WAN solution, see the Cisco SD-WAN Design Guide at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf

For additional information on deploying a Cisco SD-WAN network from end to end, see the Cisco SD-WAN End-to-End Deployment Guide at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/SD-WAN-End-to-End-Deployment-Guide.pdf

For all Cisco EN Validated Design and Deployment guides, go to http://cs.co/en-cvds.

For the Cisco SD-WAN Communities resource page and discussion board, see http://cs.co/sdwan-resources.

For additional Cisco SD-WAN resources, including training opportunities and opening support cases, go to https://www.cisco.com/sd-wan

7.2 Base Feature Templates and Configuration Values Used

The following section shows the non-default device and feature template configurations used and referenced in this guide. The GRE and IPsec configurations that are shown in the main sections of the guide are built on top of these base configurations. See section 7.3 for information on SD-WAN device onboarding and section 7.4 for step-by-step instructions on configuring and applying the base device and feature templates. These base configuration feature templates can be applied to vEdge or IOS XE SD-WAN routers.

AAA feature template

Devices: All except vManage and vSmart
Template Name: *WAN_Edge_AAA_Template*
Template: **Basic Information/AAA**
Description: WAN Edge *AAA Template*

AAA feature template settings

Section	Parameter	Type	Variable/value
Local/New User	Name/Password/User Groups	Global	netadmin/netadmin/netadmin

Branch VPN 0 feature template

Devices: All except vManage, vSmart
Template Name: *WAN_Edge_VPN0*

Template: **VPN/VPN**
Description: *VPN 0 Template for the WAN Edge branch routers*

Branch VPN 0 feature template

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	0
	Name	Global	Transport VPN
DNS	Primary DNS Address	Global	64.100.100.125
	Secondary DNS Address	Global	64.100.100.126
IPv4 Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio button	Next Hop
	Next Hop	Device Specific	vpn0_next_hop_ip_addr_inet
	Next Hop	Device Specific	vpn0_next_hop_ip_addr_mpls

Branch Internet interface feature template

Devices: All except vManage, vSmart
Template Name: *WAN_Edge_VPN0_INET*

Template: **VPN/VPN Interface Ethernet**
Description: *VPN 0 INET Int Template for WAN Edge branch rtrs*

Branch VPN0 Internet interface static IP feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn0_inet_int_name
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn0_inet_ipv4_addr
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet
Allow Service	NTP	Global	On

Branch MPLS interface feature template

Devices: All except vManage, vSmart
Template Name: *WAN_Edge_VPN0_MPLS*

Template: **VPN/VPN Interface Ethernet**
Description: *VPN 0 MPLS Int Template for WAN Edge branch rtrs*

Branch VPN0 MPLS interface static IP feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn0_mpls_int_name
IPv4 Configuration	IPv4 Address	Radio button	Static

	IPv4 Address	Device Specific	vpn0_mpls_ipv4_addr
Tunnel	Tunnel Interface	Global	On
	Color	Global	mpls
	Restrict	Global	On
Allow Service	NTP	Global	On

Branch VPN 512 interface feature template

Devices: All except vManage, vSmart **Template**: **VPN/VPN Interface Ethernet**
Template Name: *WAN_Edge_VPN512_MGT_INT* **Description**: *VPN 512 Mgt Int Template for WAN Edge*

Branch VPN 512 interface static IP feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_int_name
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn512_int_ipv4_addr

Branch VPN 1 feature template

Devices: All except vManage, vSmart **Template**: **VPN/VPN**
Template Name: *WAN_Edge_VPN1* **Description**: *VPN 1 Template for the WAN Edge branch routers*

Branch VPN 1 feature template

Section	Parameter	Type	Variable/value
Basic Configuration	VPN	Global	1
	Name	Global	LAN

Branch VPN 1 interface feature template

Devices: All except vManage,vSmart **Template**: **VPN/VPN Interface Ethernet**
Template Name: *WAN_Edge_VPN1_LAN_INT* **Description**: *VPN 1 LAN Int Template for WAN Edge branch rtrs*

Branch VPN0 Internet interface static IP feature template

Section	Parameter	Type	Variable/value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn1_int_name_1
IPv4 Configuration	IPv4 Address	Radio button	Static
	IPv4 Address	Device Specific	vpn1_int_ipv4_addr_1

Device Template

Device Model: vEdge 100 B or **ISR1100 4G (vEdge)**
Template Name: *WAN_Edge_Remote_A*
Description: WAN Edge router remote site A

and

Device Model: ISR4331
Template Name: *WAN_Edge_Remote_B*
Description: WAN Edge router remote site B

Note: For IOS XE SD-WAN routers, choose either AAA or AAA-Cisco templates and choose None for the one not in use.

Template type	Template sub-type	Template name
Basic Information	AAA	WAN_Edge_AAA_Template
VPN0	VPN	WAN_Edge_VPN0
	VPN Interface	WAN_Edge_VPN0_INET
	VPN Interface	WAN_Edge_VPN0_MPLS
VPN 512	VPN Interface	WAN_Edge_VPN512_Template
VPN1	VPN	WAN_Edge_VPN1
	VPN Interface	WAN_Edge_VPN1_LAN_INT

Device Variable Values:

WAN Edge A device template variable values

Variable	Value
Hostname	WAN_EdgeA
System IP	10.255.241.31
Site ID	113003
Interface Name(vpn1_int_name_1)	ge0/0
IPv4 Address(vpn1_int_ipv4_addr_1)	10.103.10.1/24
Interface Name(vpn0_inet_int_name)	ge0/4
IPv4 Address(vpn0_inet_ipv4_address)	64.102.254.146/28
Address(vpn0_next_hop_ip_addr_inet)	64.102.254.152
Interface Name(vpn0_mpls_int_name)	ge0/2
IPv4 Address(vpn0_mpls_ipv4_addr)	192.168.103.2/30

Address(vpn0_next_hop_ip_addr_mpls)	192.168.103.1
Interface Nam(vpn512_int_name)	ge0/1
IPv4 Address(vpn512_int_ipv4_addr)	192.168.255.153/23

WAN Edge B device template variable values

Variable	Value
Hostname	WAN_EdgeB
System IP	10.255.241.21
Site ID	111002
Interface Name(vpn1_int_name_1)	GigabitEthernet0/0/1
IPv4 Address(vpn1_int_ipv4_addr_1)	10.102.10.1/24
Interface Name(vpn0_inet_int_name)	GigabitEthernet0/0/0
IPv4 Address(vpn0_inet_ipv4_address)	64.102.254.151/28
Address(vpn0_next_hop_ip_addr_inet)	64.102.254.152
Interface Name(vpn0_mpls_int_name)	GigabitEthernet0/0/2
IPv4 Address(vpn0_mpls_ipv4_addr)	192.168.102.2/30
Address(vpn0_next_hop_ip_addr_mpls)	192.168.102.1
Interface Nam(vpn512_int_name)	GigabitEthernet0
IPv4 Address(vpn512_int_ipv4_addr)	192.168.255.134/23

7.3 Onboarding the WAN Edge Devices

Before configuration templates can be built for a WAN Edge router, it must first be onboarded onto the SD-WAN overlay network, establishing control connections with the Cisco SD-WAN controllers. There are multiple ways to onboard the WAN Edge router onto the SD-WAN overlay network. One option is the manual method, where you console to the router and minimally configure the router to reach and establish control connections with the Cisco SD-WAN controllers. The following minimal configurations were used on each router in this guide to onboard them and establish control connections with the controllers.

Note: The clock on the router should be synced with the rest of the network. If the clock is not accurate, be certain to set it or configure NTP.

Note: For vEdge, starting in version 19.1 and higher code, due to security reasons, default settings for the admin user cannot be kept and you are forced to either change the admin password or create a new admin user (depending on the version). For IOS XE SD-WAN, a new admin user and password is required starting in 16.10.2, 16.10.3, 16.11.1 and 16.12 and higher. To avoid issues, it is highly recommended to add a new admin user and password before upgrading to these code versions if possible. The new admin user is added to the below configuration during onboarding.

WAN Edge A (vEdge router):

```
config t
system
 host-name               WAN_EdgeA
 system-ip               10.255.241.31
 site-id                 113003
 organization-name       "ENB-Solutions - 21615"
 vbond vbond3-21615.cisco.net
 aaa
  user netadmin
   password (REMOVED)
   group netadmin
 vpn 0
 dns 64.100.100.125 primary
 interface ge0/4
 ip address 64.102.254.146/28
 !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
  !
  no shutdown
 !
 ip route 0.0.0.0/0 64.102.254.152
!
commit
```

Verify the control connections are up (output is abbreviated):

```
WAN_EdgeA# show control connections
                                                    PEER                 PEER
PEER    PEER PEER            SITE DOMAIN PEER       PRIV  PEER           PUB
TYPE    PROT SYSTEM IP       ID   PRIVATE IP        PORT  PUBLIC IP      PORT  LOCAL COLOR STATE
-------------------------------------------------------------------------------------------------
vsmart  dtls 10.255.255.77   1    64.100.100.77     12446 64.100.100.77  12446 biz-internet  up
vbond   dtls 0.0.0.0         0    64.100.100.75     12346 64.100.100.75  12346 biz-internet  up
vmanage dtls 10.255.255.71   1    64.100.100.71     12646 64.100.100.71  12646 biz-internet  up
```

WAN Edge B (IOS XE SD-WAN router):

Note: In XE SD-WAN IOS, VPN 0 is represented by the global table and VPN 512 is represented by vrf Mgmt-intf. Also to configure via CLI, the command is **config-transaction**, or **config-t**. When entering the command, pause before pasting in the additional configuration.

```
config-t
hostname WAN_EdgeB
username netadmin privilege 15 password (REMOVED)
ip domain lookup
ip name-server 64.100.100.125
ip route 0.0.0.0 0.0.0.0 64.102.254.152
interface GigabitEthernet 0/0/0
ip address 64.102.254.151 255.255.255.240
no shutdown
system
system-ip 10.255.241.21
site-id 111002
organization-name "ENB-Solutions - 21615"
vbond vbond3-21615.cisco.net
interface Tunnel 0
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
color biz-internet
encapsulation ipsec
commit
```

Verify the control connections are up (output is abbreviated):

```
WAN_EdgeB#show sdwan control connections
                                                                                  PEER
PEER    PEER PEER           PEER                 PRIV  PEER            PUB
TYPE    PROT SYSTEM IP      ID   PRIVATE IP      PORT  PUBLIC IP       PORT  LOCAL COLOR  STATE
-------------------------------------------------------------------------------------------------
vsmart  dtls 10.255.255.77   1   64.100.100.77   12346 64.100.100.77   12346 biz-internet  up
vbond   dtls 0.0.0.0         0   64.100.100.75   12346 64.100.100.75   12346 biz-internet  up
vmanage dtls 10.255.255.71   1   64.100.100.71   12746 64.100.100.71   12746 biz-internet  up
```

For additional options and more information on onboarding WAN Edge routers onto the SDWAN overlay network, see the Cisco SD-WAN WAN Edge Onboarding Deployment Guide at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sd-wan-wan-edge-onboarding-deploy-guide-2019dec.pdf

7.4 Upgrade Software on WAN Edge router

Via vManage

After onboarding, software upgrades can optionally be performed from vManage. On the vManage GUI, you can upload images to **Maintenance>Software Repository** and then go to **Maintenance>Software Upgrade** to upgrade/install, then activate images.

Via CLI (vEdge Routers)

Alternatively, upgrades can be performed via CLI if needed. For vEdge routers, first download the image:

```
WAN_EdgeA# request download vpn 512
ftp://admin:c1sco123@192.168.254.51/viptela-19.2.099-x86_64.tar.gz
```

Install the image:

```
WAN_EdgeA# request software install viptela-19.2.099-x86_64.tar.gz
```

Verify the image installed:

```
WAN_EdgeA# show software

VERSION   ACTIVE  DEFAULT  PREVIOUS  CONFIRMED
-------------------------------------------
18.4.1    false   false    true      -
18.4.302  true    true     false     user
19.2.099  false   false    false     user
```

Activate the image:

```
WAN_EdgeA# request software activate 19.2.099
```

Once confirmed, the router boots, and you can then make the new image the default:

```
WAN_EdgeA# request software set-default 19.2.099
```

Via CLI (IOS XE SD-WAN Routers)

For IOS XE SD-WAN routers, first download the image:,

```
WAN_EdgeB#copy ftp://admin:c1sco123@192.168.254.51/isr4300-
ucmk9.16.12.1e.SPA.bin bootflash: vrf Mgmt-intf
```

Install the image:

```
request platform software sdwan software install bootflash:isr4300-
ucmk9.16.12.1e.SPA.bin
```

Verify the image installed:

```
WAN_EdgeB#show sdwan software
VERSION         ACTIVE  DEFAULT  PREVIOUS  CONFIRMED
```

```
-----------------------------------------------------
16.10.3b.0.0    false   true     true      user
16.11.1a.0.382  false   false    false     auto
16.12.1b.0.4    true    false    false     auto
16.12.1e.0.66   false   false    false     user
```

Activate the image:

```
WAN_EdgeB#request platform software sdwan software activate
16.12.1e.0.66
```

The router then boots, and you can make the new image the default.

```
WAN_EdgeB#request platform software sdwan software set-default
16.12.1e.0.66
```

7.5 Create a Device Template

The following section demonstrates how to configure the WAN Edge router through feature-based device templates from the vManage GUI. In this workflow, feature templates are created first, followed by the device template which references the feature templates configured. From the vManage GUI, the device template is attached to a Cisco WAN device, which causes the resulting network configuration to be pushed down to the device to completely configure it so it can be fully managed by the vManage.

A minimal configuration is demonstrated of a WAN Edge configured with two transports (Internet and MPLS), using default feature templates where possible. It is assumed that the Cisco WAN Edge device has already established control connections to the vManage and vSmart controllers.

For more information on deploying feature and device templates, see the Cisco SD-WAN end-to-end deployment guide at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/SD-WAN-End-to-End-Deployment-Guide.pdf. For more generic device-template creation information, see the product documentation at https://sdwan-docs.cisco.com/Product_Documentation/vManage_How-Tos/Configuration/Create_a_Device_Configuration_Template

In the following sections, the VPN 0, VPN 0 Interface, VPN 1, and VPN 1 interface templates are created and added to a new device template. The out-of-band management VPN 512 and its interface are also configured as well as a AAA feature template in order to create a new admin user. Default feature templates are used otherwise. The device template is attached and deployed to the WAN Edge router. VPN 0 is the transport, or WAN-facing VPN and VPN 1 is a user-defined service VPN, or LAN-facing VPN.

Note that three different configuration parameter types for each feature setting can be configured in the templates, **Global**, **Device Specific**, and **Default**. The **Global** parameter type allows you to assign a specific value that is applied to all devices the feature template is attached to. The **Device Specific** type asks you to define a variable, which allows you to use a feature template on a wide variety of different devices but gives you the flexibility to tailor values to each device when device templates are attached and deployed. **Default** parameters are what's configured by default (it could be a specific value or no feature configuration at all as examples).

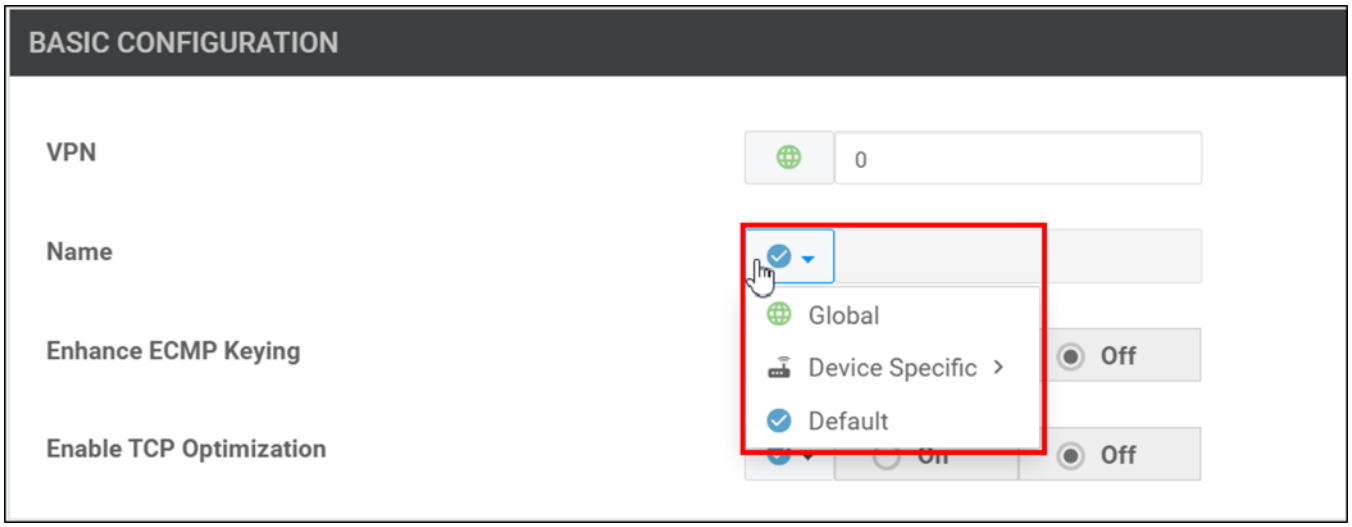


Figure 70: Configuration Parameter Types

7.5.1 Log into vManage

Go to *http://<*IP *address of vManage server>:8443* and type in the username and password. Click the **Log In** button.

Figure 71: Log into vManage

7.5.2 Create VPN 0 Feature Template

In the vManage GUI, go to **Configuration>Templates** and click the **Feature** tab. Click the **Add Template** button.

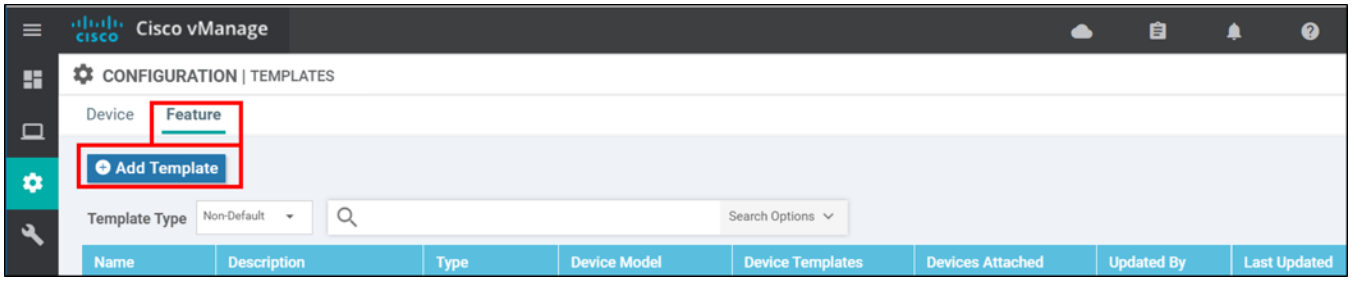


Figure 72: Create a Feature Template

7.5.2.1 Select Devices and Template

On the left-hand side of the GUI under **Select Devices**, select which devices this feature template can apply to. In this example, all platforms except vManage and vSmart are chosen.

On the right-hand side under **Select Template**, click the **VPN** box under **VPN**.

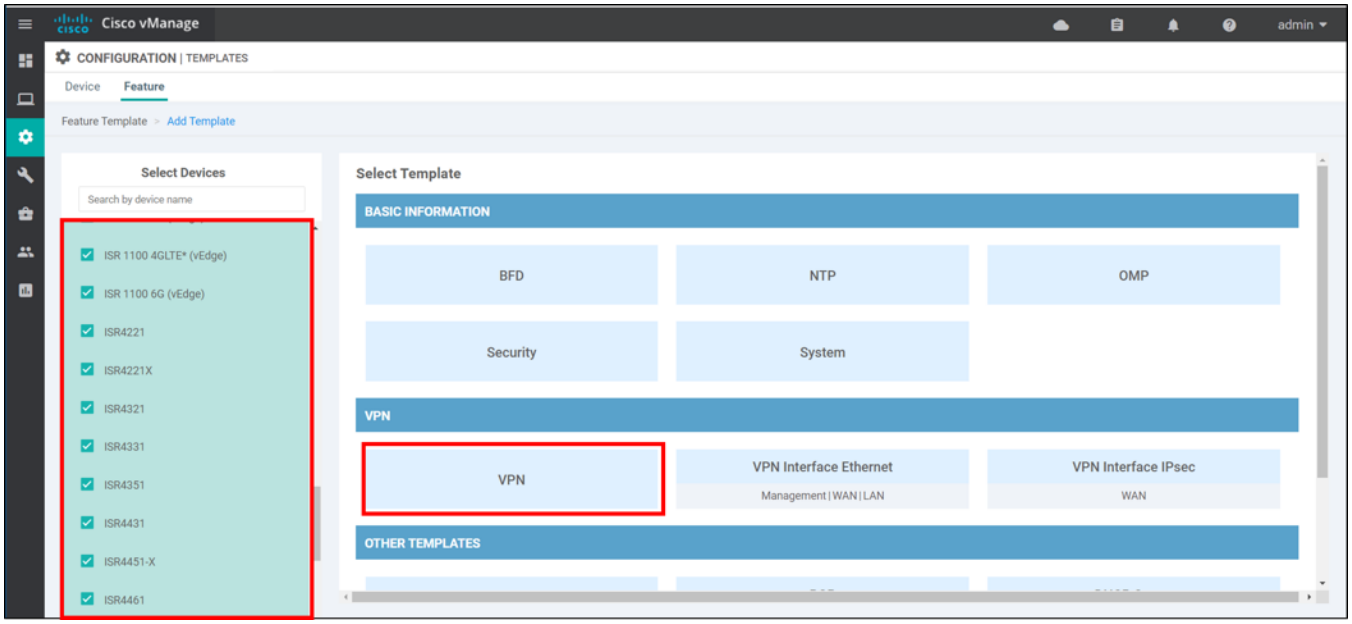


Figure 73: Select Devices and Template Type

7.5.2.2 Name and Describe the Template

Type a **Template Name** (*WAN_Edge_VPN0*) and **Description** (*VPN 0 Template for the WAN Edge branch routers*) for the VPN 0 template.

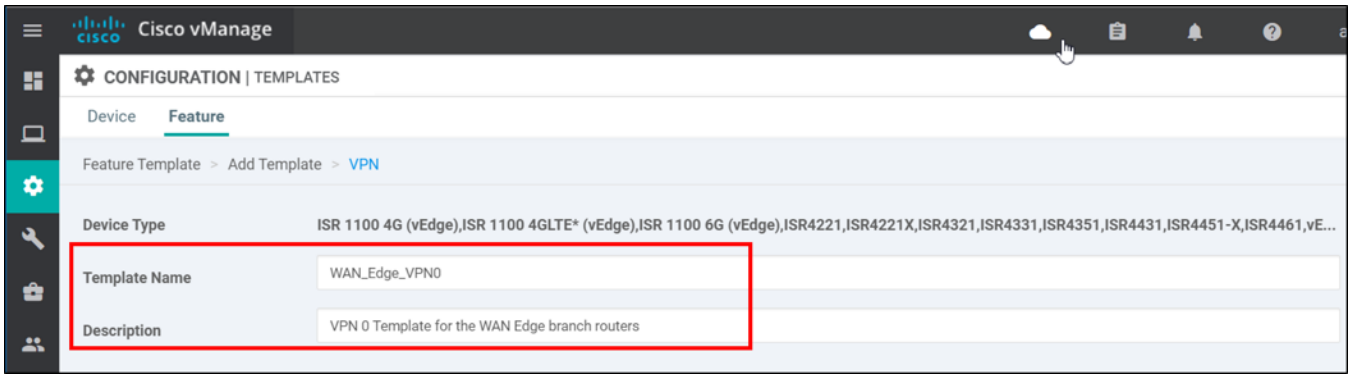


Figure 74: Enter VPN0 Template Name and Description

7.5.2.3 Configure Basic Configuration in VPN 0

Note the **VPN** ID already defaults to **0**. Next to **Name** which is just a description, select **Global** from the drop-down box and type *Transport VPN*.

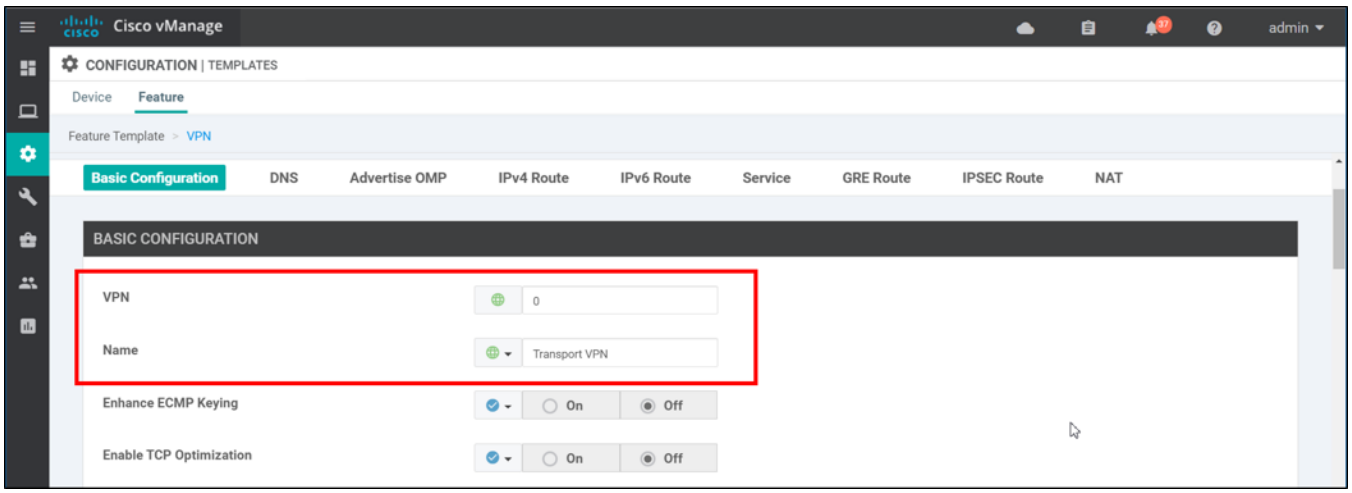


Figure 75: Enter VPN0 Basic Configuration

7.5.2.4 Configure the DNS Server in VPN 0

This DNS server is a server reachable through VPN 0, located on one of the WAN transports. It could be used to resolve the vBond hostname, as an example.

Under the **DNS** section next to **Primary DNS Address (IPv4)**, select **Global** from the drop-down box, and type the DNS server IP address (64.100.100.125 in this example).

A second line appears. If there is a secondary DNS address to configure, next to **Secondary DNS Address (IPv4)**, select **Global** from the drop-down box and type the DNS server IP address (64.100.100.126 in this example).

Note: Alternatively, you can use static host name/IP address mappings instead of a DNS server definition. To configure, click the **New Host Mapping** button and configure **Hostname** and IP address or a **List of IP** addresses, then click **Add**.

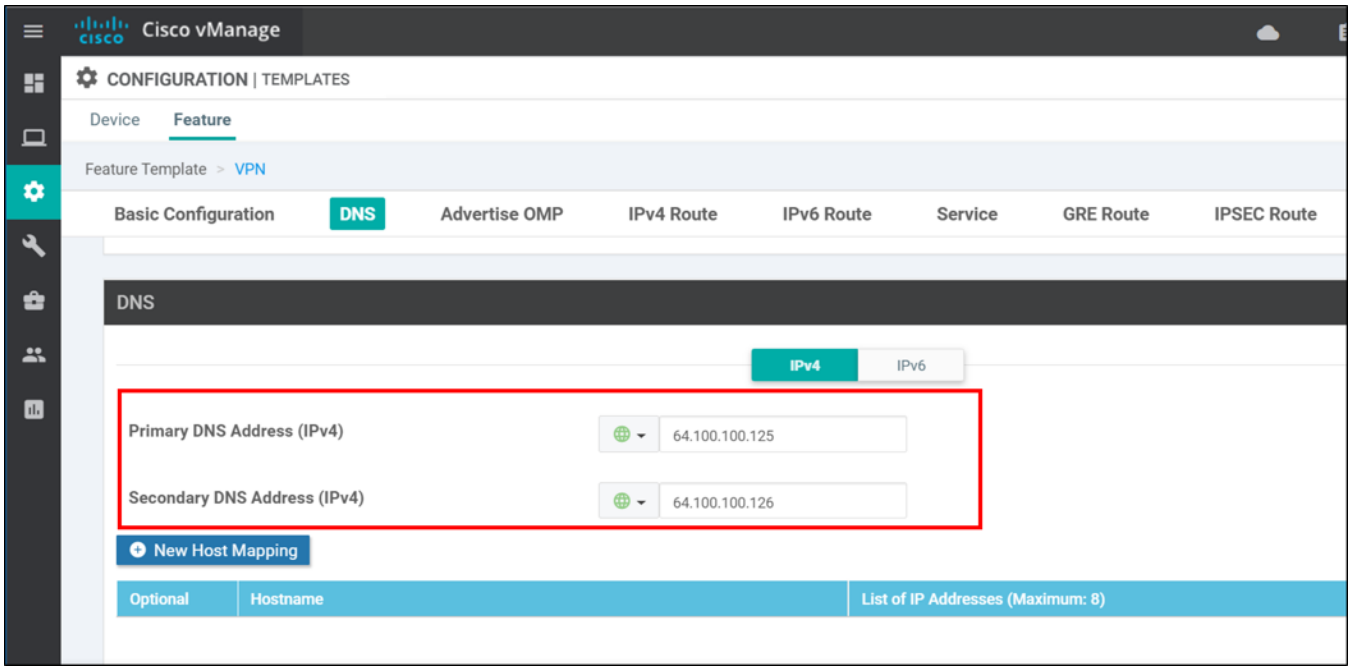


Figure 76: Enter Primary and Secondary DNS server IP addresses

7.5.2.5 Add IPv4 Default Route and Next-Hop

A default route and next-hop gateways for both WAN transports are defined in VPN 0. The default route is used to build SD-WAN tunnels to other sites for data traffic and to build control connections to the controllers for control traffic as well.

Next to Prefix, type **0.0.0.0/0** in the text box and click **Add Next Hop**.

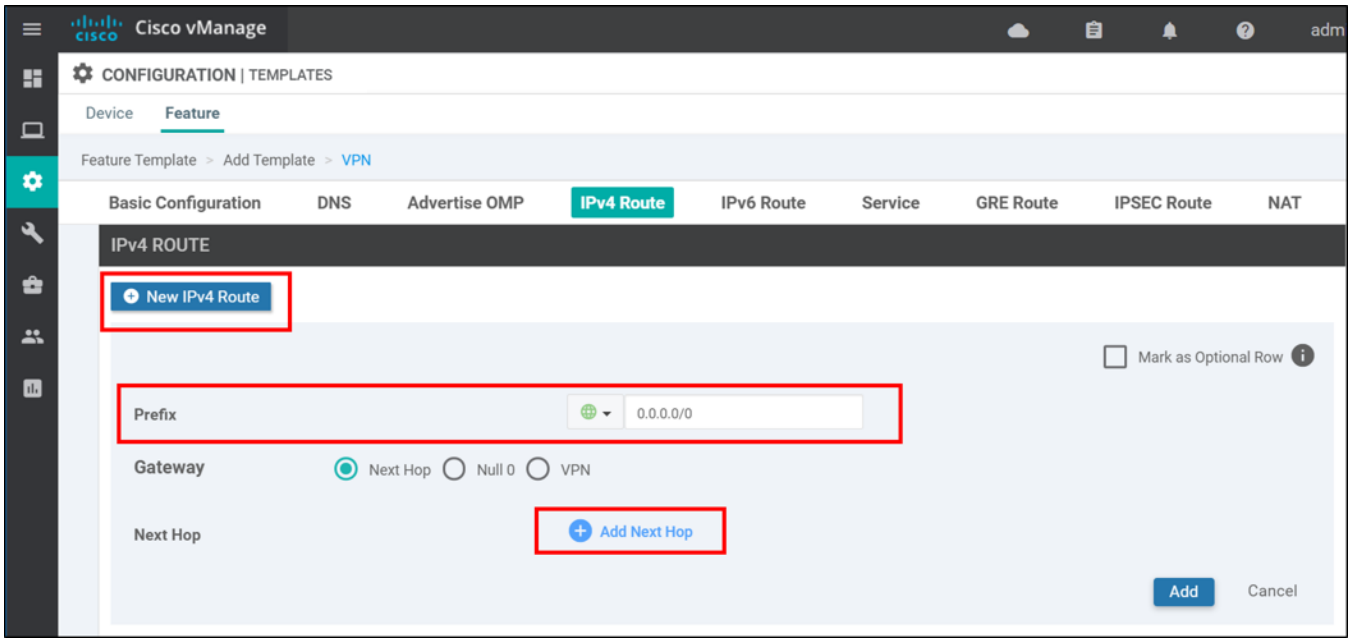


Figure 77: Add Default route

In the pop-up window, click **Add Next Hop**.

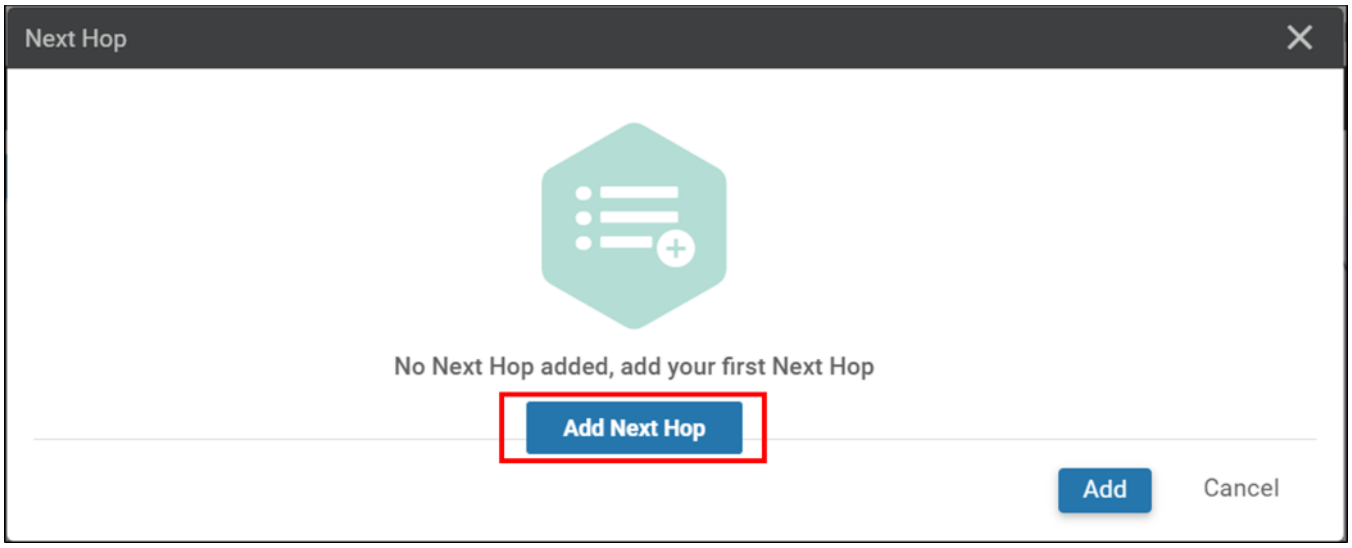


Figure 78: Add Default route

To apply this template to multiple remote site routers, the next-hop values are configured as variables. Under **Address**, select **Device Specific** from the drop-down box and type in a variable name (*vpn0_next_hop_ip_addr_inet* in this example). The variable should be

descriptive because the values are defined when the device template is attached to the WAN Edge device.

Add a second next hop for the MPLS transport by clicking the **Add Next Hop** button. For this next hop, select **Device Specific** from the drop-down box and type in a variable name (*vpn0_next_hop_ip_addr_mpls* in this example). Click **Add**.

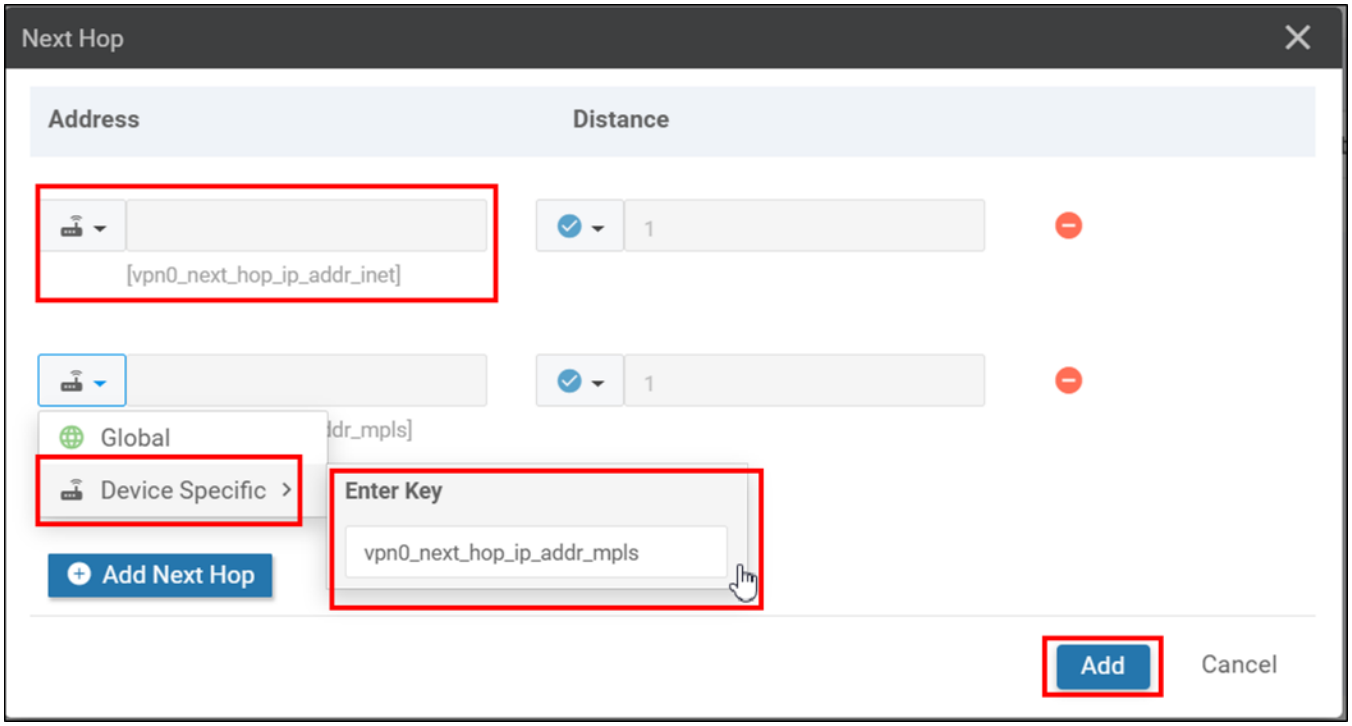


Figure 79: Add Next-hop IP Address

You are taken back to the main feature template page. Now that **2 Next Hop**s is added to the 0.0.0.0/0 prefix, click **Add** to add the route into the feature template.

Note: You must click **Add** or the route and its next-hop information will not be saved.

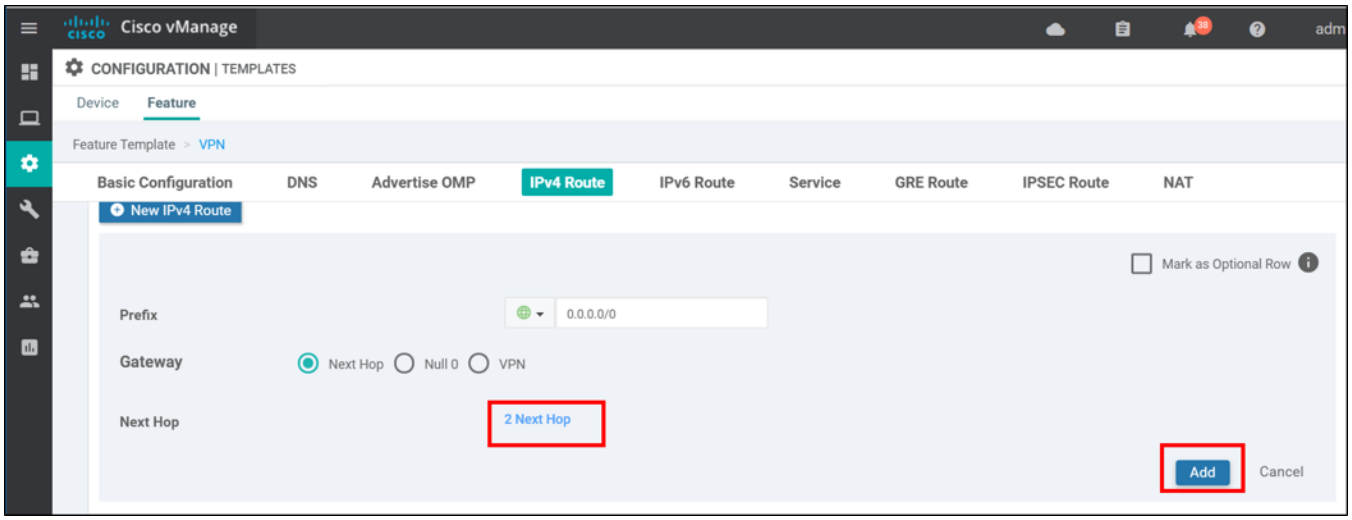


Figure 80: Add Default route and Next-hop Information to template

Verify the newly-added route.

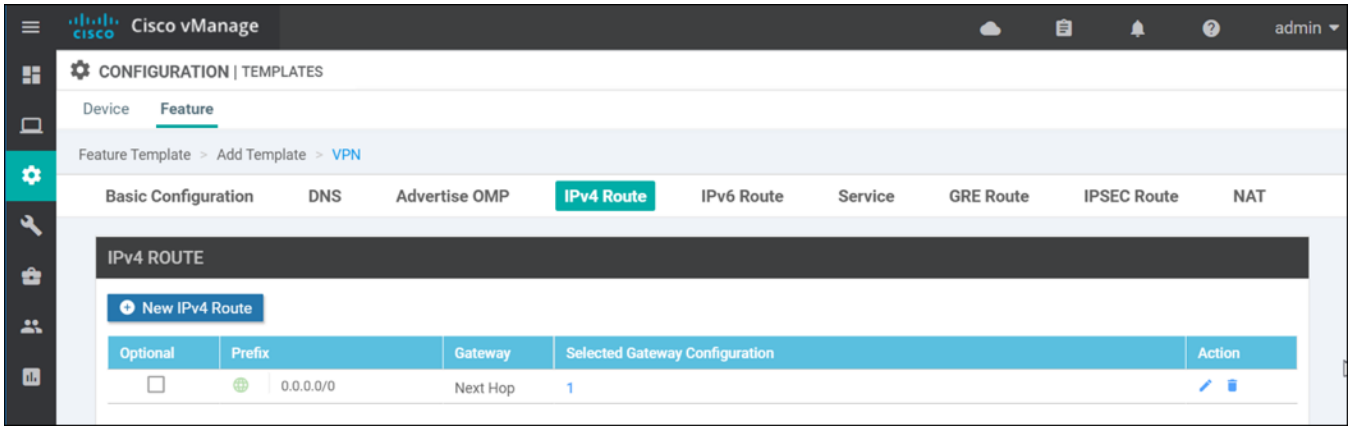


Figure 81: Verify newly-added route

7.5.2.6 Save the VPN 0 Feature Template

From the main feature template page, click **Save**.

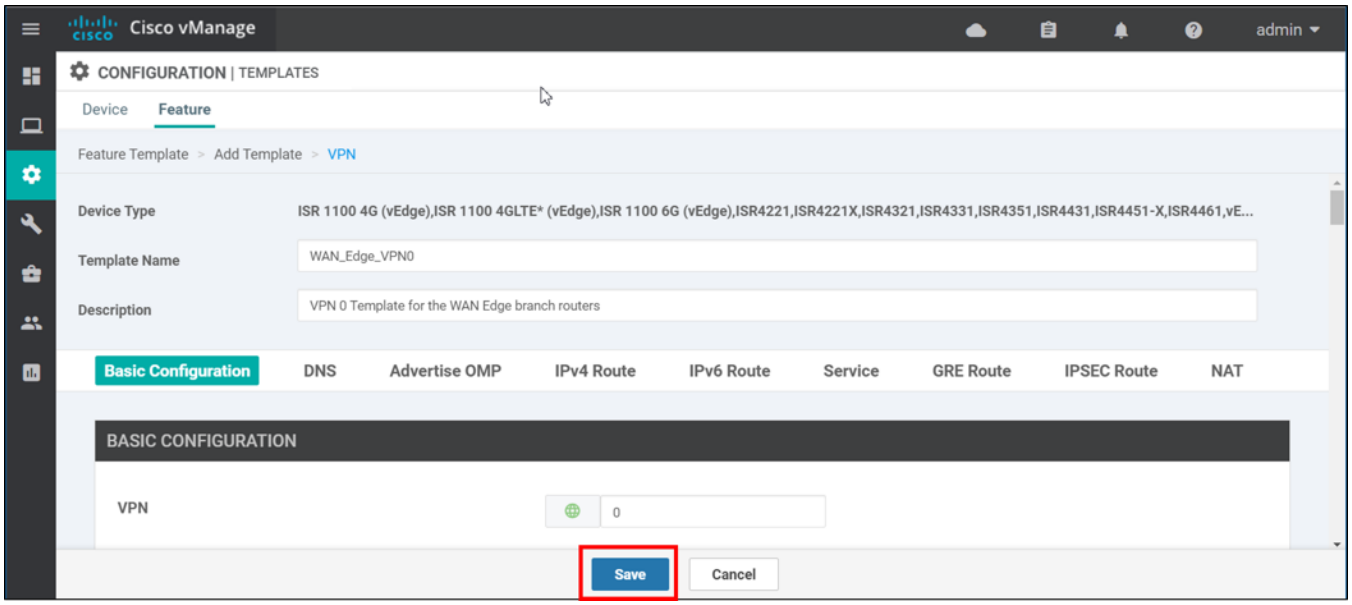


Figure 82: Save the VPN 0 feature template

The new feature template now appears in the list of available feature templates in the vManage GUI under the **Configuration>Templates>Feature** tab.

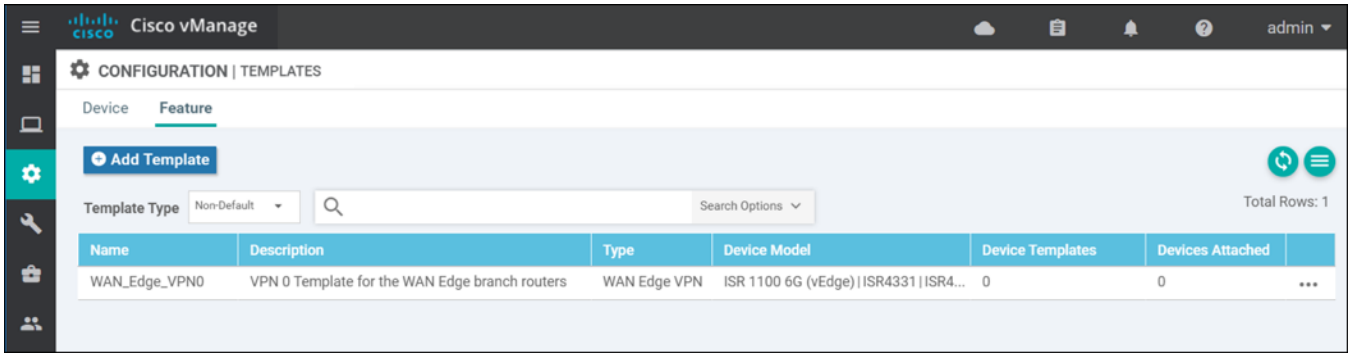


Figure 83: Available Feature Templates

7.5.3 Create the VPN 0 Internet Interface Templates

Now that the VPN 0 template has been created, the VPN 0 Interface templates must be created to define the configuration parameters of each WAN transport interface connecting to the Service Provider (Internet and MPLS). The Internet interface is configured first.

In the vManage GUI, go to **Configuration>Templates** and click the **Feature** tab. Click the **Add Template** button.

7.5.3.1 **Select Devices and Template**

On the left-hand side of the GUI under **Select Devices**, select which devices this feature template can apply to. In this example, all platforms except vManage and vSmart are chosen.

On the right-hand side under **Select Template**, click the **VPN Interface Ethernet** box under **VPN**.

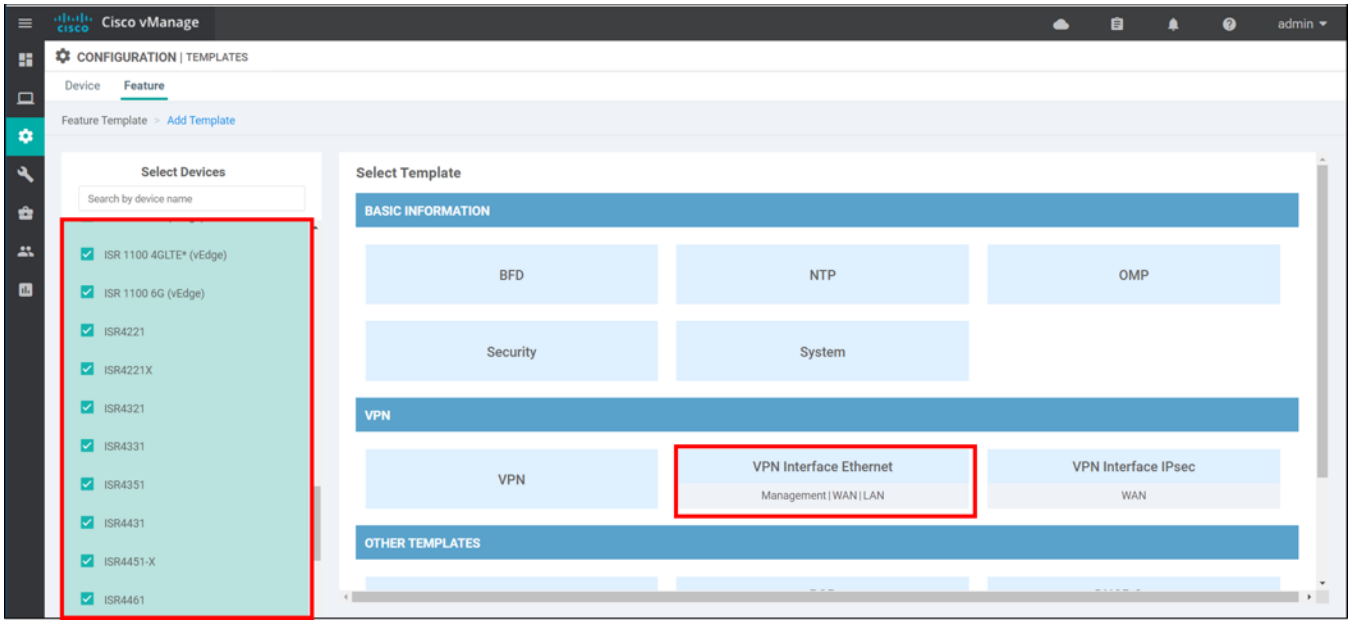


Figure 84: Select Devices and Template Type

7.5.3.2 Name and Describe the Template

Type a **Template Name** (*WAN_Edge_VPN0_INET*) and **Description** (*VPN 0 INET Interface Template for the WAN Edge branch routers*) for the VPN 0 Interface template.

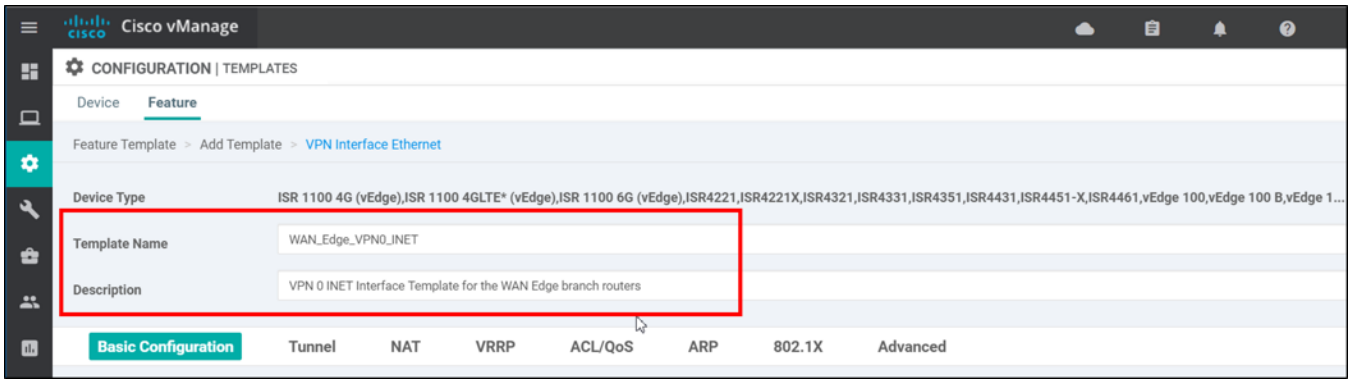


Figure 85: Enter VPN0 Interface Template Name and Description

7.5.3.3 Configure Basic Configuration for VPN 0 Interface

In this section, the interface is set to *No Shutdown* and a variable is defined for the Interface name specification. A variable is used so the same feature template can be referenced across multiple platforms, where the interface numbering may vary from one platform to another.

Under the **Basic Configuration** section, next to **Shutdown**, select **Global** from the drop-down box, and select the **No** radio button.
Next to **Interface Name**, select **Device Specific** from the drop-down box and configure a variable name in the text box (*vpn0_inet_int_name* in this example).

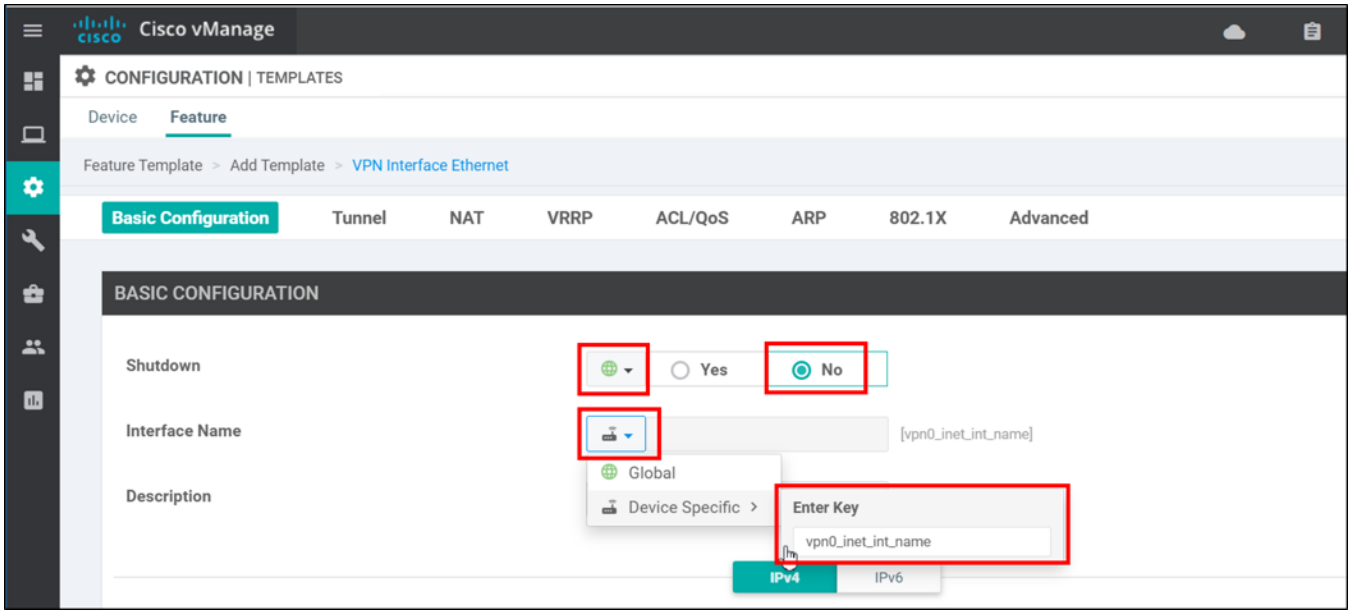


Figure 86: Enter VPN0 Interface Basic Configuration

7.5.3.4 **Configure IPv4 IP address for VPN 0 Interface**

Under **Basic Configuration** then under **IPv4**, ensure the **Static** radio button is selected, although dynamic IP allocation is also an option in the case of IPsec tunnels Next to **IPv4 Address**, select **Device Specific** from the drop-down box and configure a variable name in the text box (*vpn0_inet_ipv4_addr* in this example).

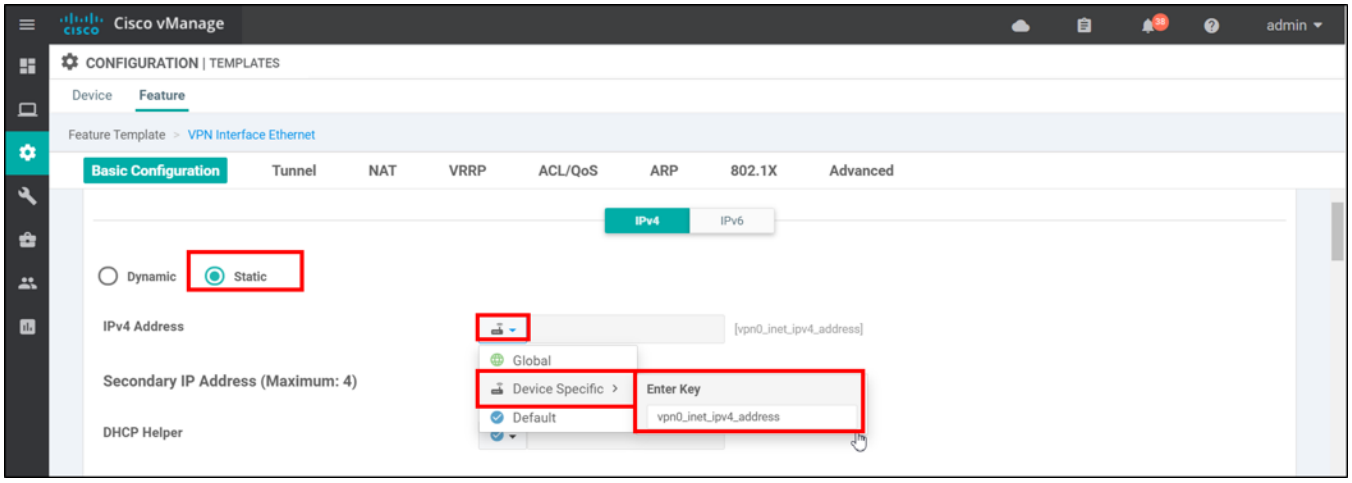


Figure 87: Configure VPN 0 Interface IP Address

7.5.3.5 Configure Tunnel Interface for VPN 0 Interface

An IPsec tunnel is configured in order for the router to be able to join the Cisco SD-WAN overlay.

Under the **TUNNEL** section next to **Tunnel Interface**, choose **Global** from the drop-down box and click the **On** radio button. Once the tunnel is enabled, tunnel parameters can be configured. IPsec is the default encapsulation.

Next to **Color**, configure the transport label for this interface. In this example, all of the devices use the *biz-internet* public color, but a variable could also be defined for this parameter. Select **Global** from the drop-down box and select **biz-internet** from the drop-down box.

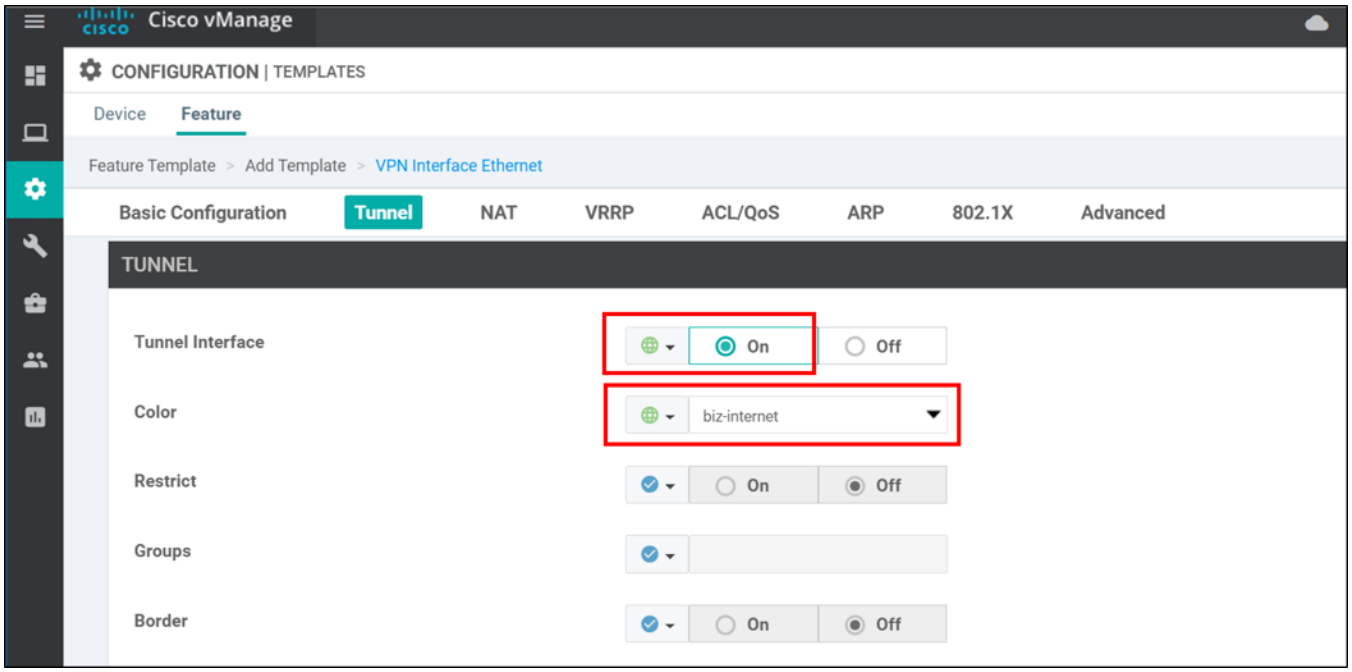


Figure 88: Configure VPN 0 Interface Tunnel Parameters

7.5.3.6 Configure Tunnel Interface for VPN 0 Interface

Once the tunnel is enabled, IPsec traffic is allowed through the interface, but most native protocols are restricted from passing through the interface. By default, DHCP, DNS, ICMP, and HTTPS is allowed. In this example, NTP is enabled.

Under the **TUNNEL>Allow Service** section, next to **NTP**, select **Global** from the drop-down box and click the **On** radio button.

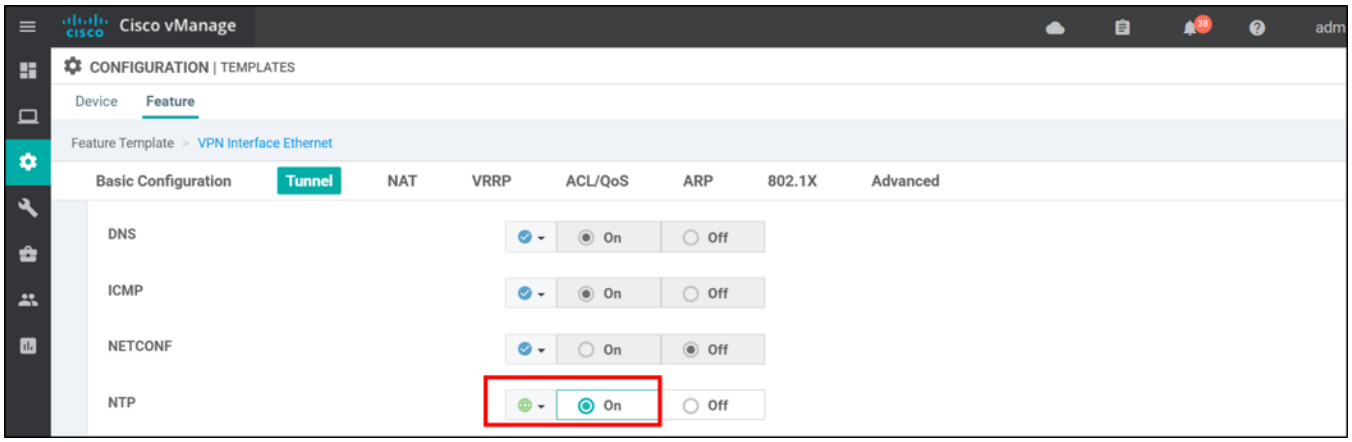


Figure 89: Configure VPN 0 Interface Tunnel Allowed Protocols

7.5.3.7 Save the VPN 0 Interface Feature Template

At the bottom of the page, click **Save.**

The new feature template now appears in the list of available feature templates in the vManage GUI under **Configuration>Templates>Feature** tab.

7.5.4 Create the VPN 0 MPLS Interface Templates

To the far right of the newly-created interface template (**WAN_Edge_VPN0_INET**), click **…** and select **Copy** from the drop-down box.

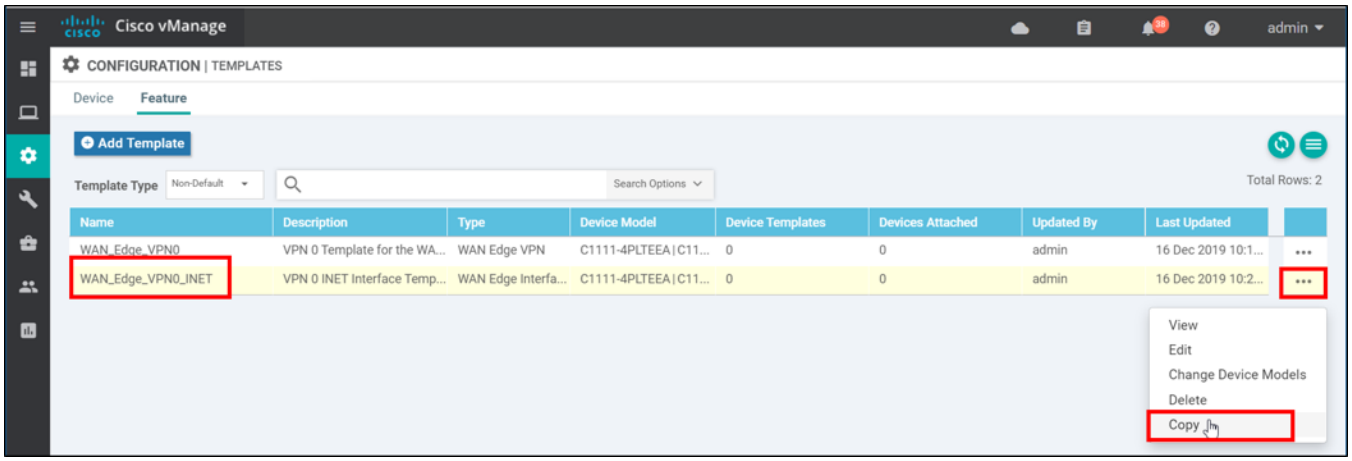


Figure 90: Copy the VPN 0 Internet Interface feature template

7.5.4.1 Name and Describe the Template

Type a **Template Name** (*WAN Edge_VPN0_MPLS*) and **Description** (*VPN 0 MPLS Interface Template for the WAN Edge branch routers*) for the VPN 0 Interface template. Click **Copy**.

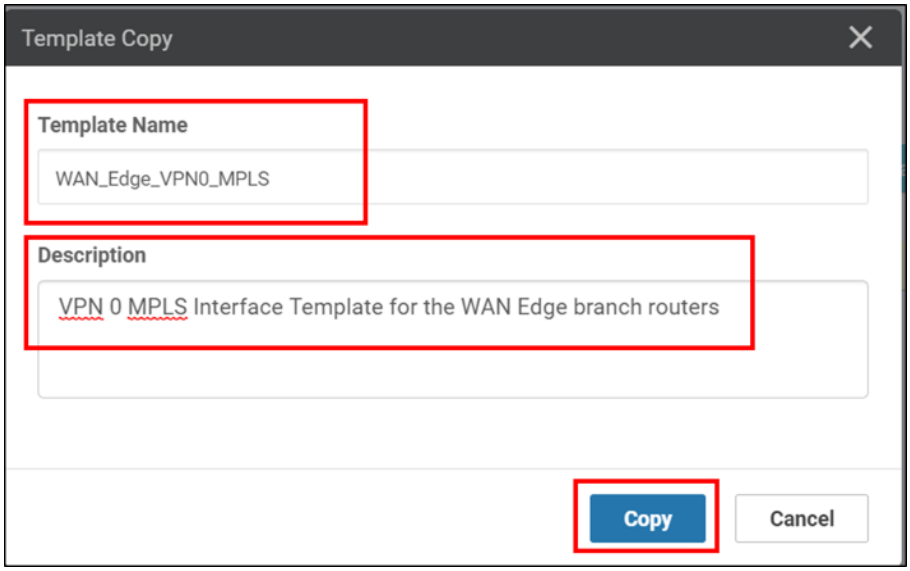


Figure 91: Name and Describe the MPLS Interface feature template

7.5.4.2 Edit the VPN 0 MPLS Interface Feature Template

To the right of the newly-copied template (**WAN_Edge_VPN0_MPLS**), click **…** and select **Edit** from the drop-down box.

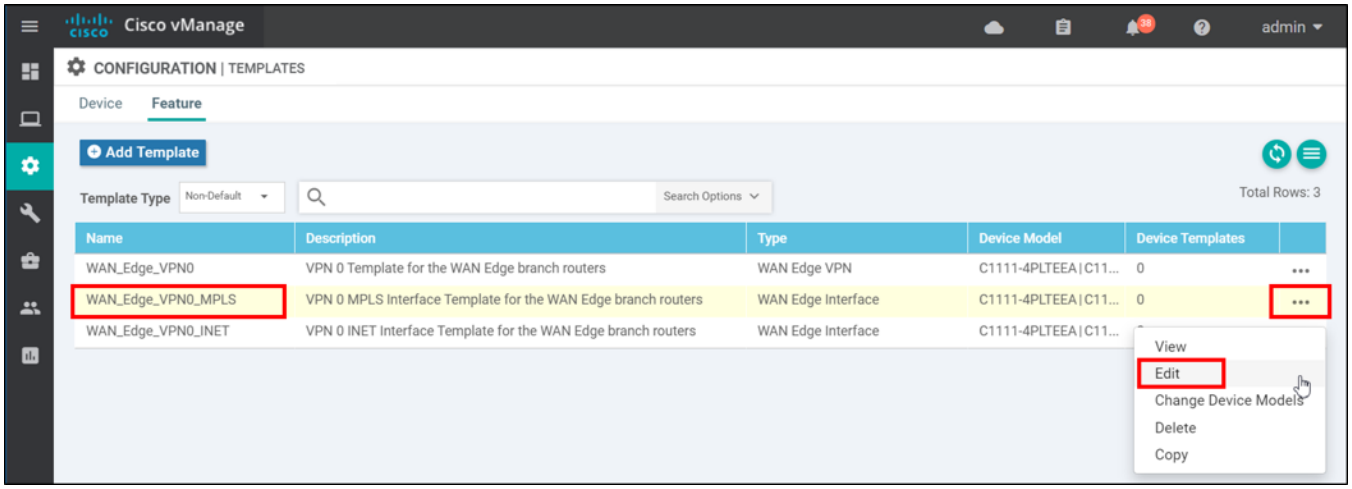


Figure 92: Edit the MPLS Interface feature template

7.5.4.3 **Configure VPN 0 MPLS Interface Feature Template**

Modify the configuration for the MPLS interface.

Next to **Interface Name**, change the variable to *vpn0_mpls_int_name*. Next to **IPv4 Address**, change the variable to *vpn0_mpls_ipv4_address*.

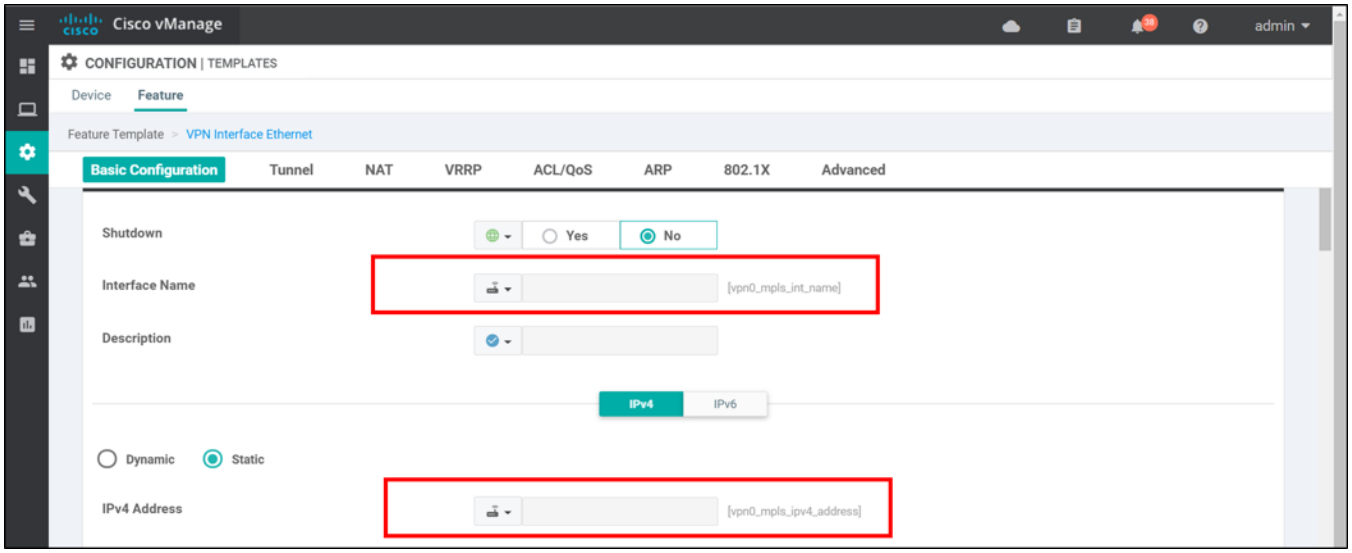


Figure 93: Configure MPLS Interface Name and IPv4 Address

Under **TUNNEL** next to **Color**, select *mpls* from the drop-down box. Next to **Restrict**, select **Global** from the drop-down box and select the **On** radio button. The restrict option prevents tunnels forming with other colors. Click **Update** to complete the feature template.

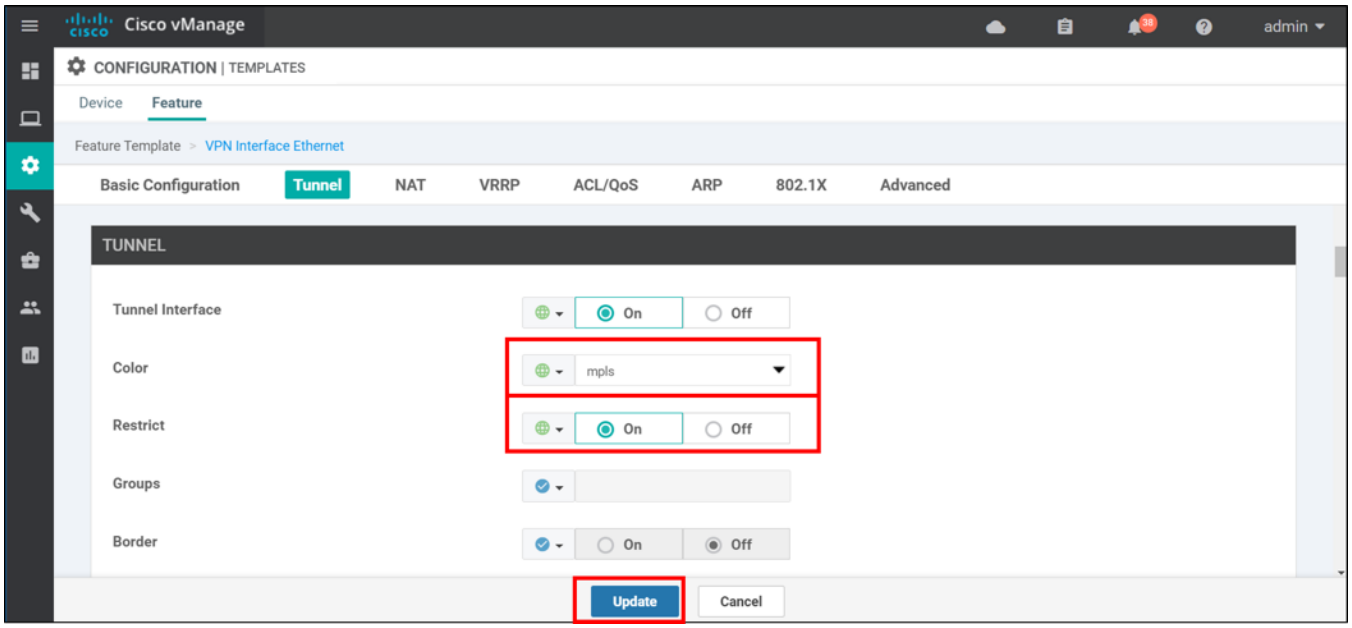


Figure 94: Configure MPLS Color and Restrict Option

The new feature template now appears in the list of available feature templates in the vManage GUI under **Configuration>Templates>Feature** tab.

7.5.5 Create VPN 1 Feature Template

In this section, the service VPN, or LAN-side VPN is configured.

In the vManage GUI, go to **Configuration>Templates** and click the **Feature** tab. Click the **Add Template** button.

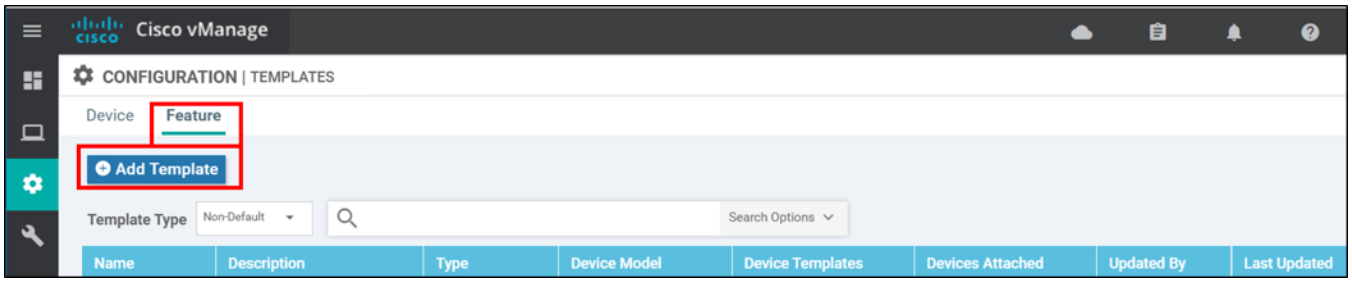


Figure 95: Create a Feature Template

7.5.5.1 Select Devices and Template

On the left-hand side of the GUI under **Select Devices**, select which devices this feature template can apply to. In this example, all platforms except vManage and vSmart are chosen.

On the right-hand side under **Select Template**, click the **VPN** box under **VPN**.

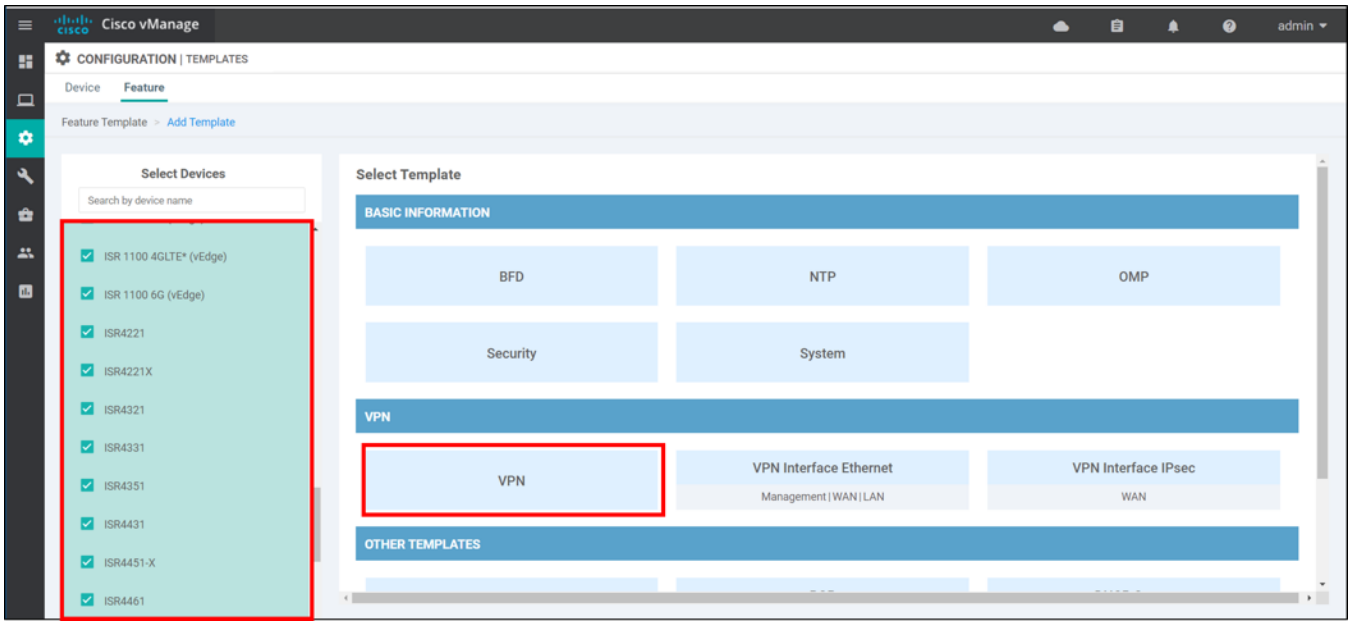


Figure 96: Select Devices and Template Type

7.5.5.2 Configure Basic Settings for VPN 1 Template

Type a **Template Name** (*WAN_Edge_VPN1*) and **Description** (*VPN 1 Template for the WAN Edge branch routers*) for the VPN 0 template. Note that the VPN parameter defaults to a global value **0**, so change the value to **1**. Next to **Name**, which is just a description, select **Global** from the drop-down box, and type *LAN*.

Optionally, configure a DNS server that is reachable from the service VPN if needed by the WAN Edge router.

In this example, a simple site is assumed, and static and connected routes are automatically redistributed in the OMP protocol across the SD-WAN overlay network, so no additional parameters are configured. These settings are found in the default OMP template that is part of the **Basic Information** section of the device template.

At the bottom of the GUI, click **Save**.

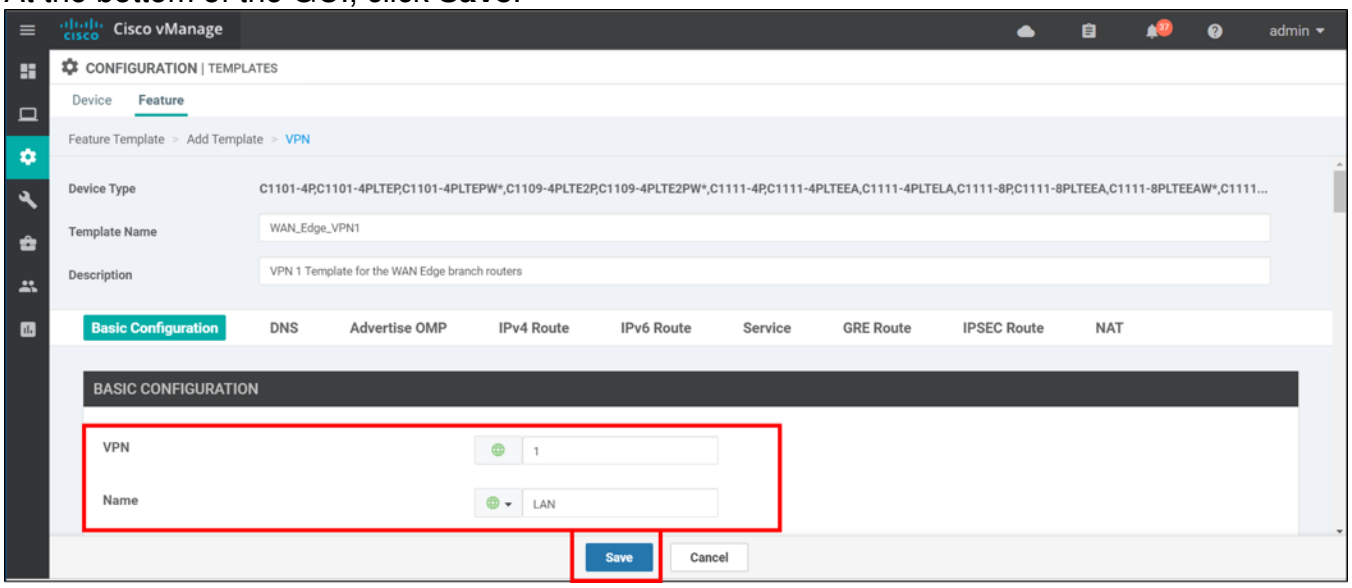


Figure 97: Enter VPN1 Basic Settings

The new feature template now appears in the list of available feature templates in the vManage GUI under **Configuration>Templates>Feature** tab.

7.5.6 Create the VPN 1 Interface Template

Now that the VPN 1 template has been created, a VPN 1 Interface template must be created to define the configuration parameters of the LAN interface connecting to the rest of the branch site.

In the vManage GUI, go to **Configuration>Templates** and click the **Feature** tab. Click the **Add Template** button.

7.5.6.1 **Select Devices and Template**

On the left-hand side of the GUI under **Select Devices**, select which devices this feature template can apply to. In this example, all platforms are chosen except vManage and vSmart.

On the right-hand side under **Select Template**, click the **VPN Interface Ethernet** box under **VPN**.

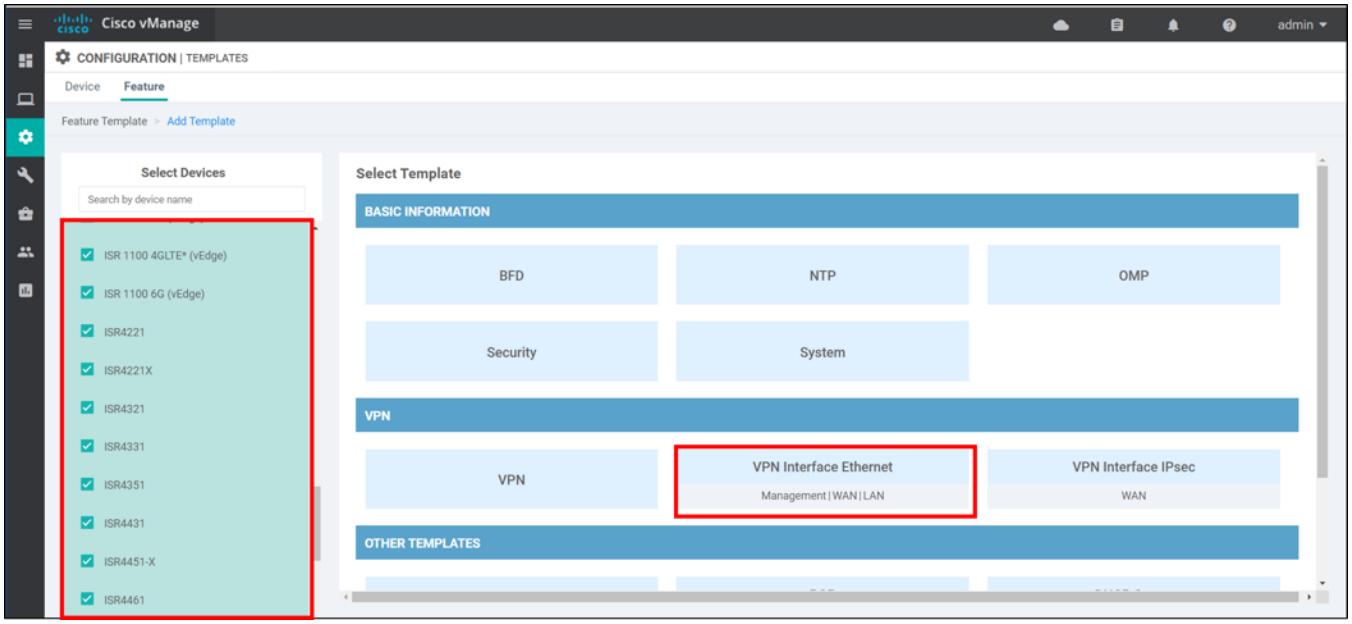


Figure 98: Select Devices and Template Type

7.5.6.2 Name and Describe the Template

Type a **Template Name** (*WAN_Edge_VPN1_LAN_INT*) and **Description** (*VPN 1 LAN Interface Template for the WAN Edge branch routers*) for the VPN 1 Interface template.

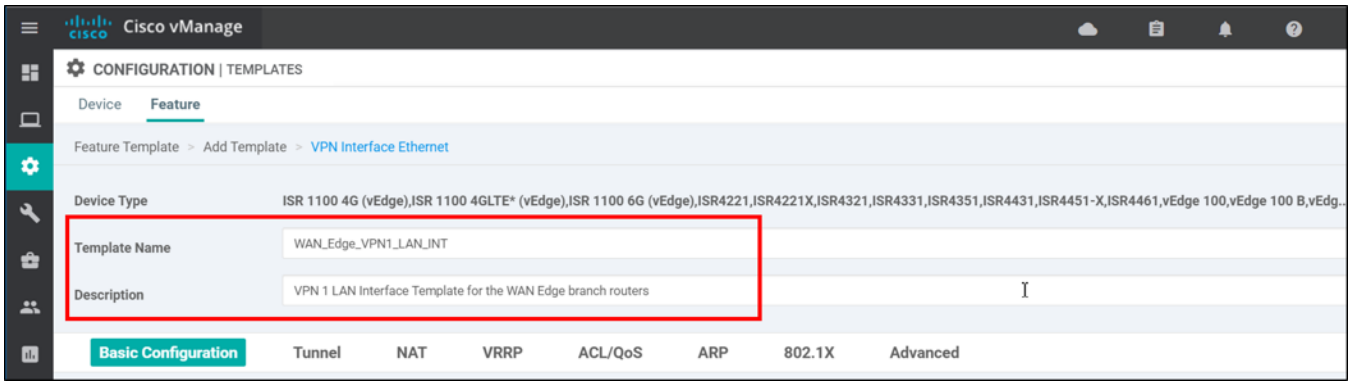


Figure 99: Enter VPN1 Interface Template Name and Description

7.5.6.3 Configure Basic Configuration for VPN 1 Interface

In this section, the interface is set to “No Shutdown” and a variable is defined for the Interface name and IP address.

Under the **Basic Configuration** section, next to **Shutdown**, select **Global** from the drop-down box, and select the **No** radio button.

Next to **Interface Name**, select **Device Specific** from the drop-down box and configure a variable name in the text box (*vpn1_int_name_1* in this example).

Under the **IPv4** section, ensure the static radio button is selected. Next to **IPv4 Address**, select **Device Specific** from the drop-down box and configure a variable name in the text box (*vpn1_int_ipv4_addr*_1 in this example).

At the bottom of the GUI, click **Save**.

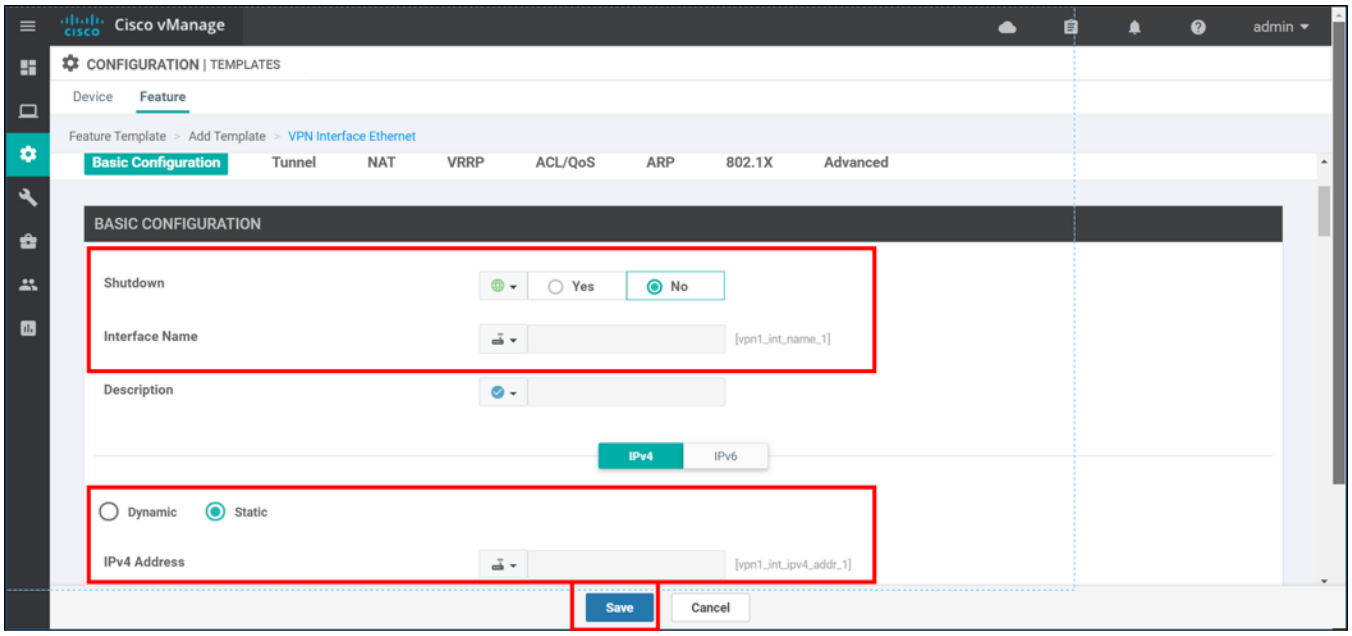


Figure 100: Enter VPN1 Interface Basic Configuration

The new feature template now appears in the list of available feature templates in the vManage GUI under **Configuration>Templates>Feature** tab.

7.5.7 Create the VPN 512 Interface Template

The default VPN 512 interface template for the vEdge 100 uses ge0/0 as the **Interface Name** and 192.168.1.1/24 as the **IPv4 Address**. Create a new interface template to modify these values if needed. Using a variable for the interface allows the template to be applied to multiple device types.

Note that the VPN 512 default template does not contain any configured routes. If a default route or other static routes need to be configured for the out-of-band management network, create a VPN 512 template in addition to the VPN 512 interface template.

In the vManage GUI, go to the **Configuration>Templates>Feature** tab. Click the **Add Template** button.

On the left-hand side of the GUI under **Select Devices**, select which devices this feature template can apply to. In this example, all platforms are chosen except vManage and vSmart.

On the right-hand side under **Select Template**, click the **VPN Interface Ethernet** box under **VPN**.

7.5.7.1 **Name and Describe the Template**

Type a **Template Name** (*WAN_Edge_VPN512_MGT_INT*) and **Description** (*VPN 512 Mgt Interface Template for the WAN Edge branch routers*) for the VPN 512 Interface template.

7.5.7.2 **Configure Basic Configuration for VPN 512 Interface**

In this section, the interface is set to “No Shutdown” and a variable is defined for the Interface name and IP address.

Under the **Basic Configuration** section, next to **Shutdown**, select **Global** from the drop-down box, and select the **No** radio button.

Next to **Interface Name**, select **Device Specific** from the drop-down box and configure a variable name in the text box (*vpn512_int_name* n this example).

Under the **IPv4** section, ensure the static radio button is selected. Next to **IPv4 Address**, select **Device Specific** from the drop-down box and configure a variable name in the text box (*vpn512_int_ipv4_addr* in this example).

At the bottom of the GUI, click **Save**.

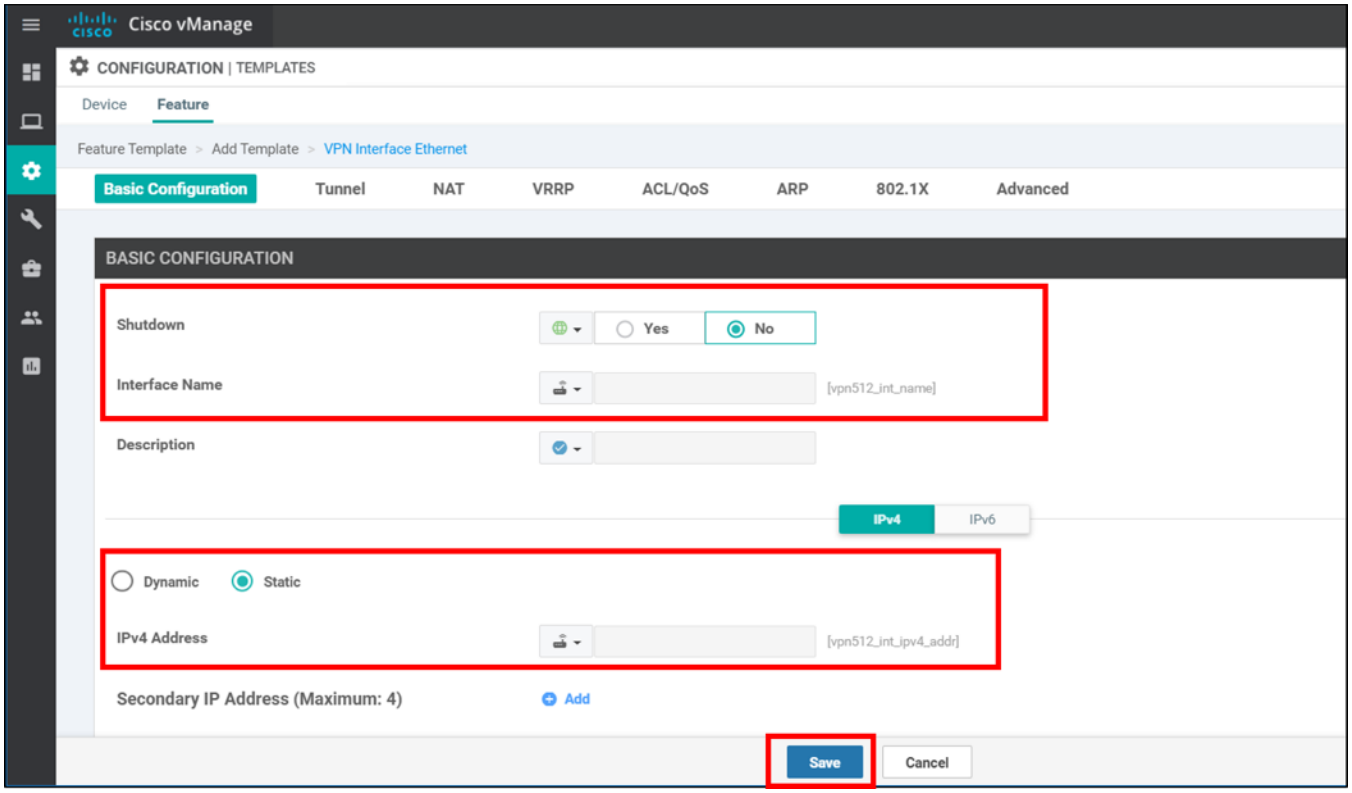


Figure 101: Enter VPN512 Interface Basic Configuration

The new feature template now appears in the list of available feature templates in the vManage GUI under **Configuration>Templates>Feature** tab.

7.5.8 Create the AAA Template

A new admin user should be created based on the new security software changes.

At the **Configuration>Templates>Feature** tab, next to **Template Type**, choose **Default** from the drop-down box. Type **AAA** in the search box and hit return.

To the right of the **Factory_Default_AAA_template**, click **…** and select **Copy** from the drop-down box.

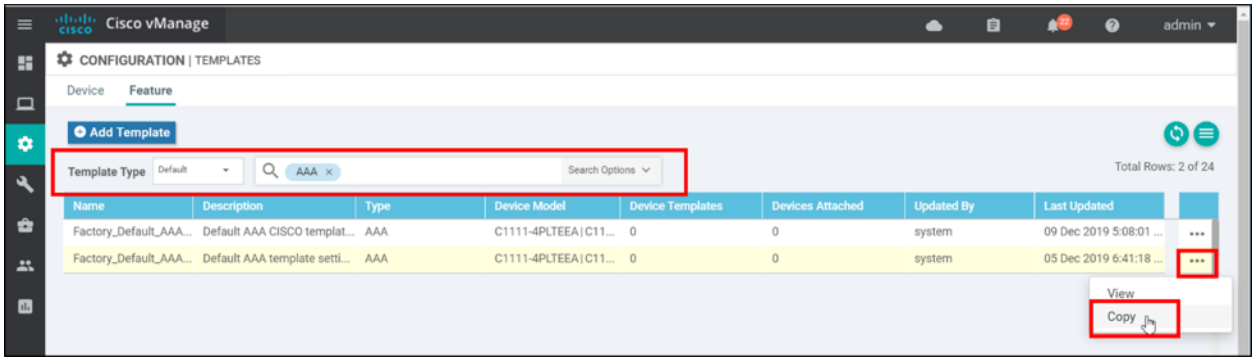


Figure 102: Create the AAA Interface Template

Modify the **Template Name** (*WAN_Edge_AAA_Template*) and **Description** (*WAN Edge AAA Template*). Click **Copy**.

7.5.8.1 **Edit the AAA Template**

Next to **Template Type**, select **Non-Default** from the drop-down box, and to the far right of the newly-copied template, **WAN_Edge_AAA_Template**, click **…** and select **Edit** from the drop-down box.

Under the **Local** section, click the **New User** button. Next to **Name**, enter the new username (*netadmin* for example). Next to **Password**, enter a password (*netadmin*, for example). Next to **User Groups**, select *netadmin* from the drop-down list. Click **Add** to add the new user, then click **Update** to save the template.

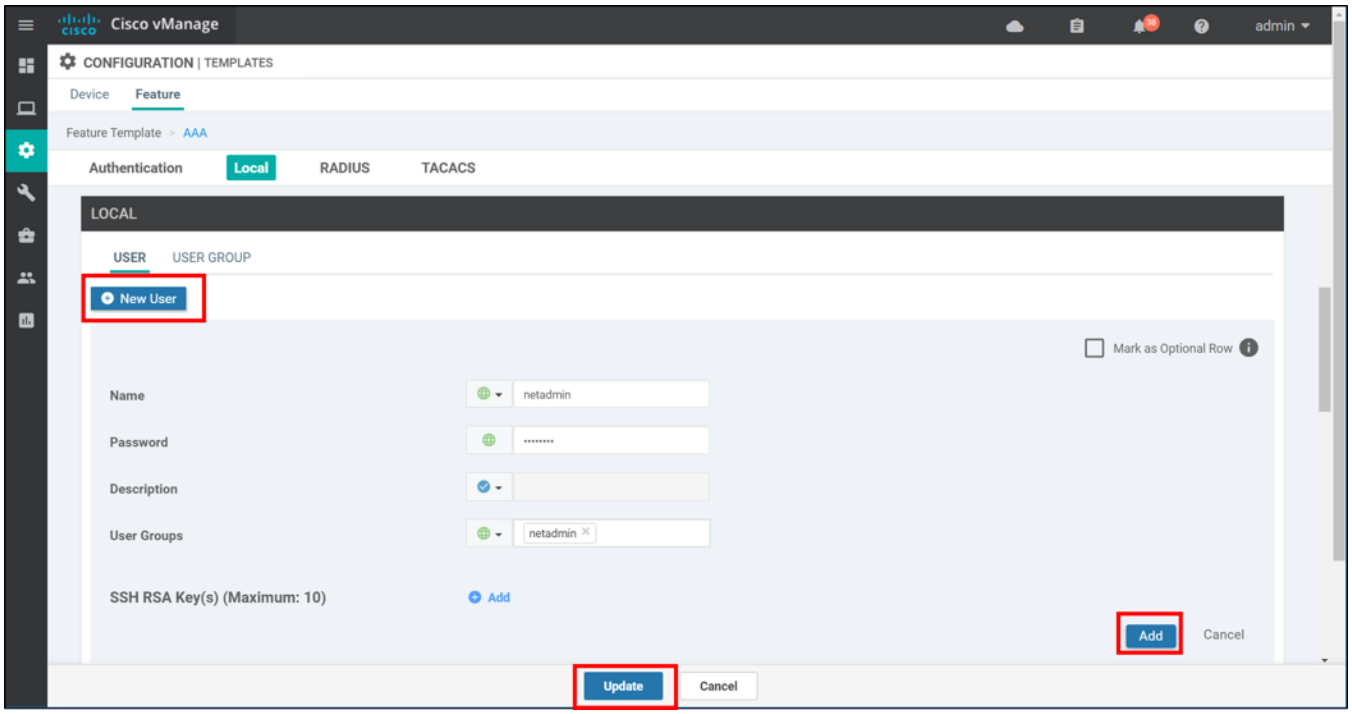


Figure 103: Edit the AAA Interface Template

7.5.9 Create Device Template (vEdge Router)

Create a device template for the WAN Edge router that uses the feature templates just created.

On the vManage GUI, go to **Configuration>Templates**, then click the **Device** tab, and click the **Create Template** button and select **From Feature Template** from the drop-down list.

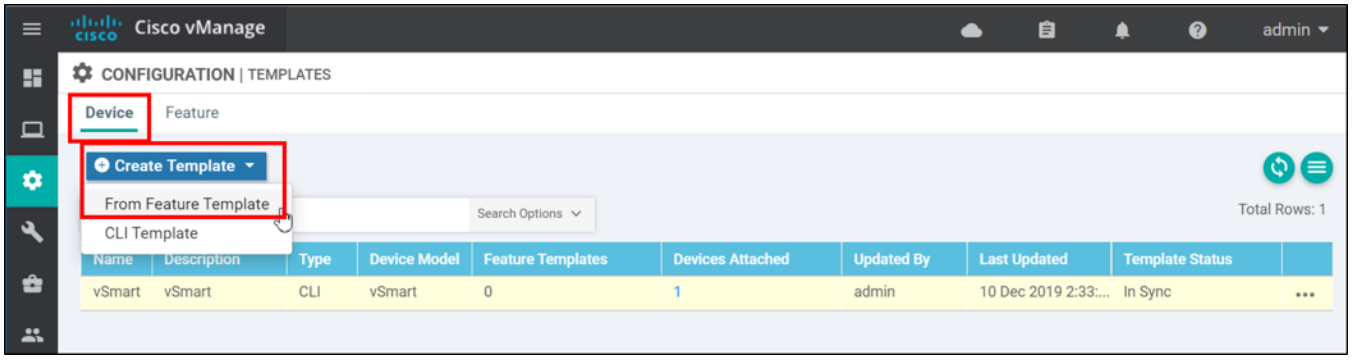


Figure 104: Create Device Template

7.5.9.1 **Choose Device Model and Name the Device Template**

Next to **Device Model**, select from the drop-down box the device model the device template applies to. In this example, a **vEdge 100 B** model is selected.

Provide a **Template Name** (WAN_Edge_Remote_A) and a **Description** (*WAN Edge router remote site A*).

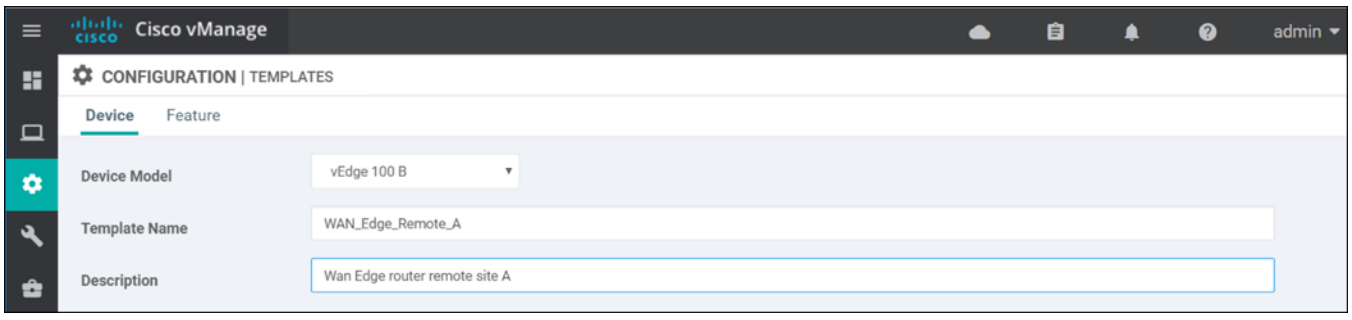


Figure 105: Configure Device Template Model, Name, and Description

7.5.9.2 **Choose Basic Information Feature Templates**

Under the **Basic Information** section, next to **AAA**, select the **WAN_Edge_AAA_Template** and keep the other default feature templates for this example.

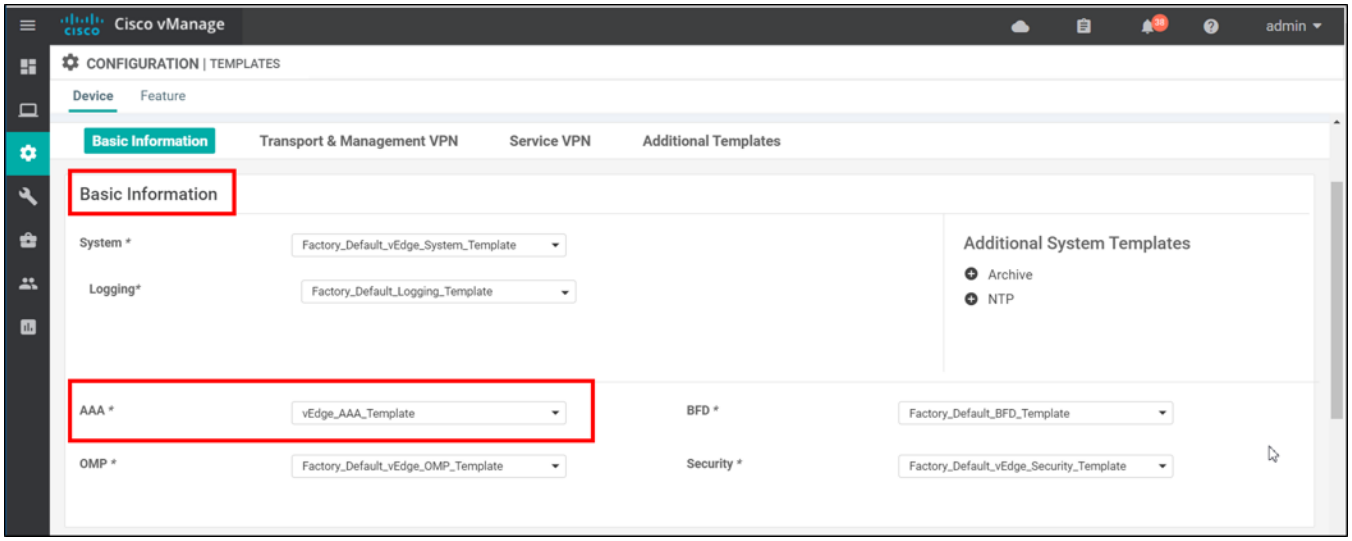


Figure 106: Device Template Basic Information Feature Template

7.5.9.3 Choose Transport & Management VPN Feature Templates

Next to **VPN 0**, select the newly-created VPN 0 feature template created in the previous sections (**WAN_Edge_VPN0**).

Next to **VPN Interface** under **VPN 0**, select the VPN 0 Interface feature template **WAN_Edge_VPN0_INET** from the drop-down box. Create another transport interface by clicking **VPN Interface** on the right-hand side, then select the VPN0 Interface feature template **WAN_Edge_VPN0_MPLS** from the drop-down box.

Under **VPN 512** and next to **VPN Interface**, select **WAN_Edge_VPN512_MGT_INT** from the drop-down box.

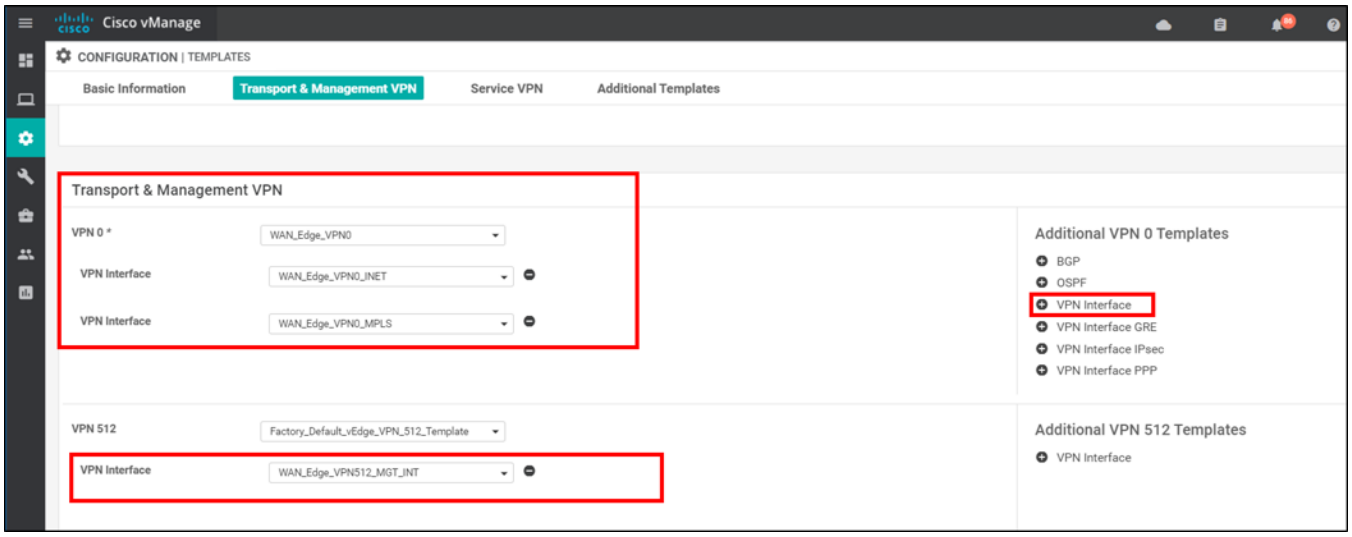


Figure 107: Device Template Transport & Management Feature Template

7.5.9.4 Choose Service VPN Feature Templates

Under the Service VPN section, click the **+ Service VPN** text to add a service VPN to the device template.

Next to **VPN**, select the newly-created VPN 1 feature template from the previous sections (**WAN_Edge_VPN1**).

To add the VPN 1 Interface template, click **+ VPN Interface** on the right-hand side, then next to **VPN Interface**, select the newly-created VPN 1 Interface feature template from the previous sections (**WAN_Edge_VPN1_LAN_INT**).

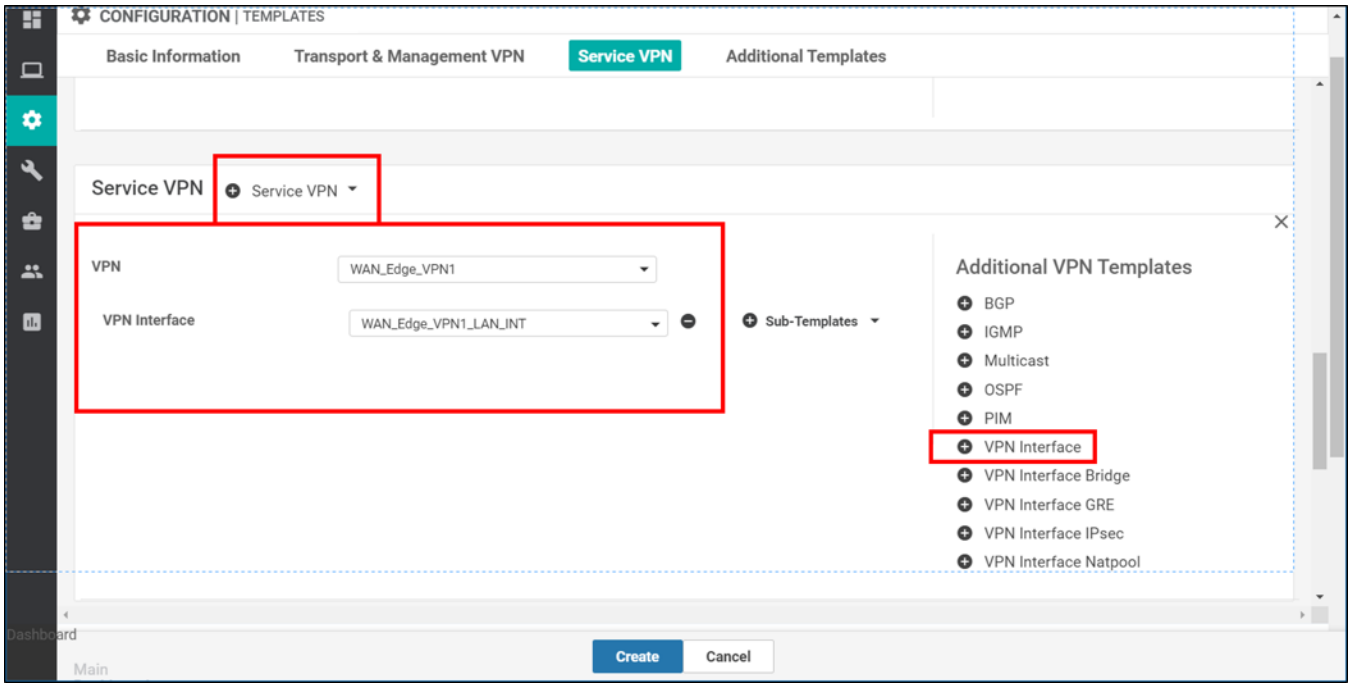


Figure 108: Device Template Service VPN Feature Templates

7.5.9.5 Save the Device Template

At the bottom of the GUI Screen, click **Create**.

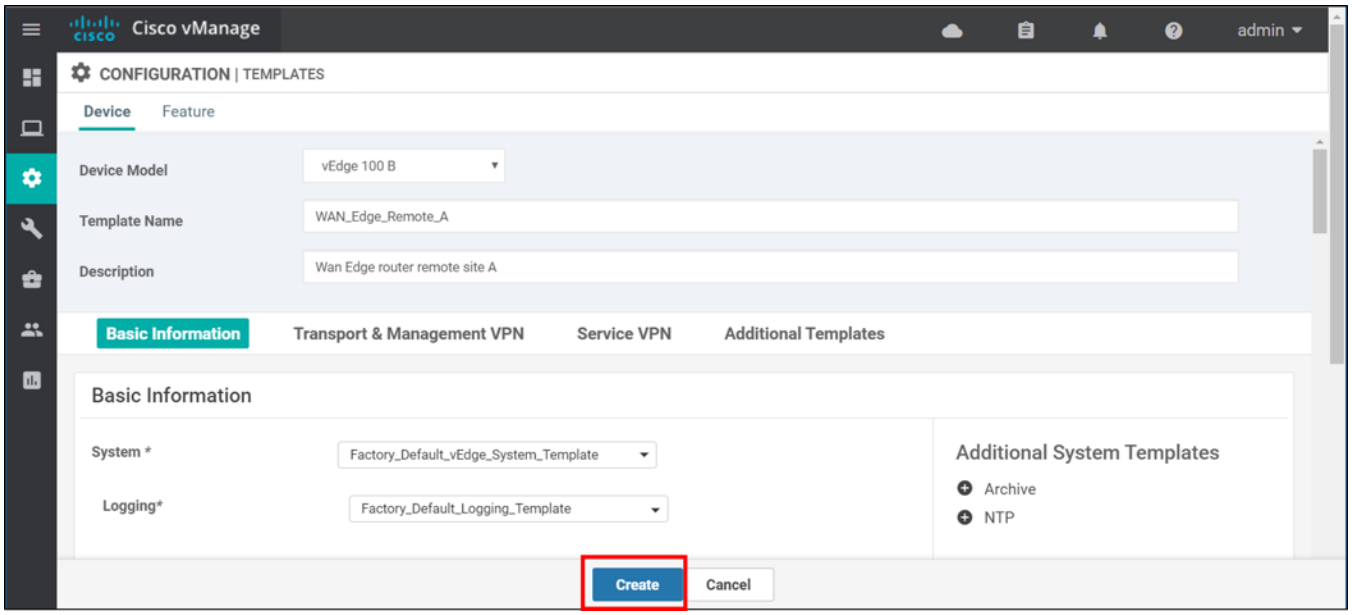


Figure 109: Save the Device Template

The new device template now appears in the list of available device templates in the vManage GUI under **Configuration>Templates>Device** tab.

7.5.10 Create Device Template (IOS XE SD-WAN Router)

Repeat the above steps to create a device template for the IOS XE SD-WAN router.

On the vManage GUI, go to **Configuration>Templates**, then click the **Device** tab, and click the **Create Template** button and select **From Feature Template** from the drop-down list.

7.5.10.1 Choose Device Model and Name the Device Template

Next to **Device Model**, select from the drop-down box the device model the device template applies to. In this example, an **ISR4331** model is selected.

Provide a **Template Name** (WAN_Edge_Remote_B) and a **Description** (*WAN Edge router remote site B*).

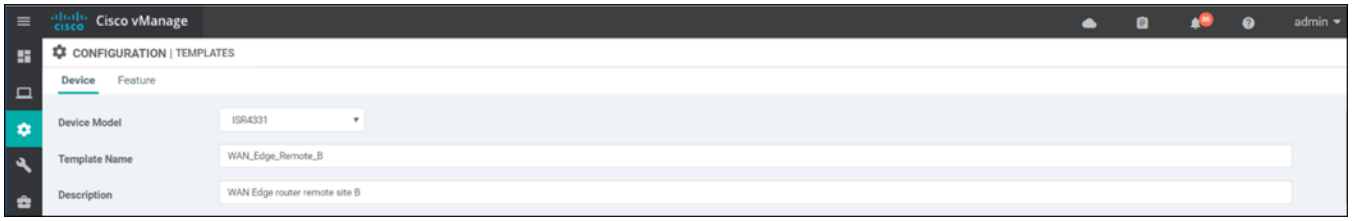


Figure 110: Configure Device Template Model, Name, and Description

7.5.10.2 Choose Basic Information Feature Templates

Under the **Basic Information** section, next to **AAA**, select the **WAN_Edge_AAA_Template**. Next to **AAA-CISCO**, choose **None**, and keep the other default feature templates for this example. Only one AAA template can be used at any one time. When **None** is selected from the drop-down box, it shows up as **Choose…** in the device template.

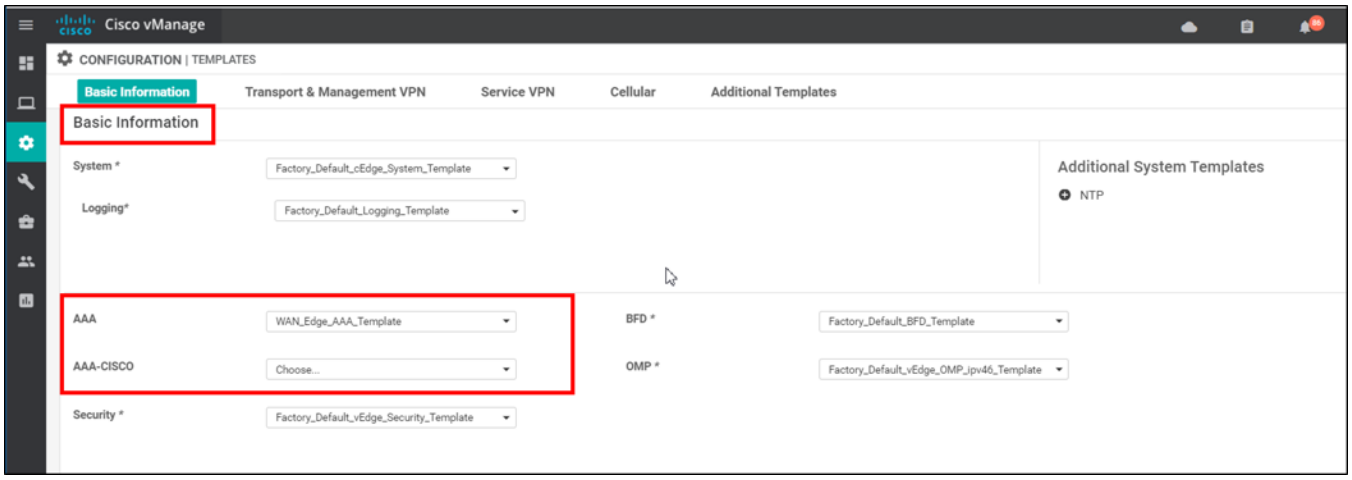


Figure 111: Device Template Basic Information Feature Template

7.5.10.3 Choose Transport & Management VPN Feature Templates

Next to **VPN 0**, select the newly-created VPN 0 feature template created in the previous sections (**WAN_Edge_VPN0**).

Next to **VPN Interface** under **VPN 0**, select the VPN 0 Interface feature template **WAN_Edge_VPN0_INET** from the drop-down box. Create another transport interface by clicking **VPN Interface** on the right-hand side, then select the VPN0 Interface feature template **WAN_Edge_VPN0_MPLS** from the drop-down box.

Under **Additional VPN 512 Templates, click +VPN Interface.** Next to **VPN Interface** under **VPN 512**, select **WAN_Edge_VPN512_MGT_INT** from the drop-down box.

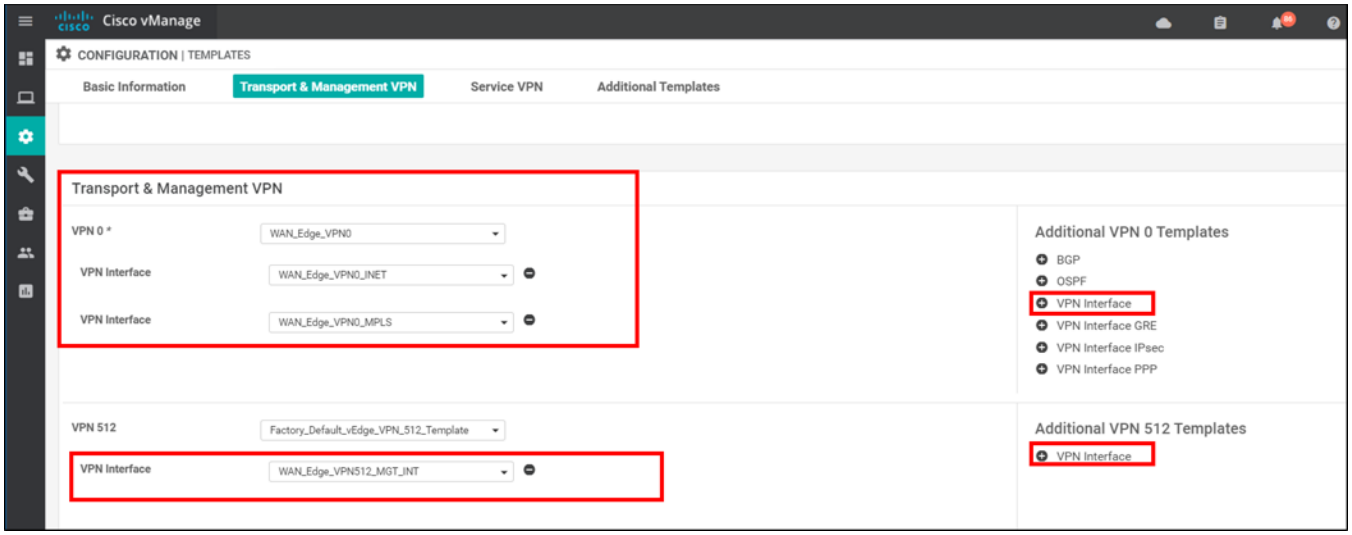


Figure 112: Device Template Transport & Management Feature Template

7.5.10.4 Choose Service VPN Feature Templates

Under the Service VPN section, click the **+ Service VPN** text to add a service VPN to the device template.

Next to **VPN**, select the newly-created VPN 1 feature template from the previous sections (**WAN_Edge_VPN1**).

To add the VPN 1 Interface template, click **+ VPN Interface** on the right-hand side, then next to **VPN Interface**, select the newly-created VPN 1 Interface feature template from the previous sections (**WAN_Edge_VPN1_LAN_INT**).

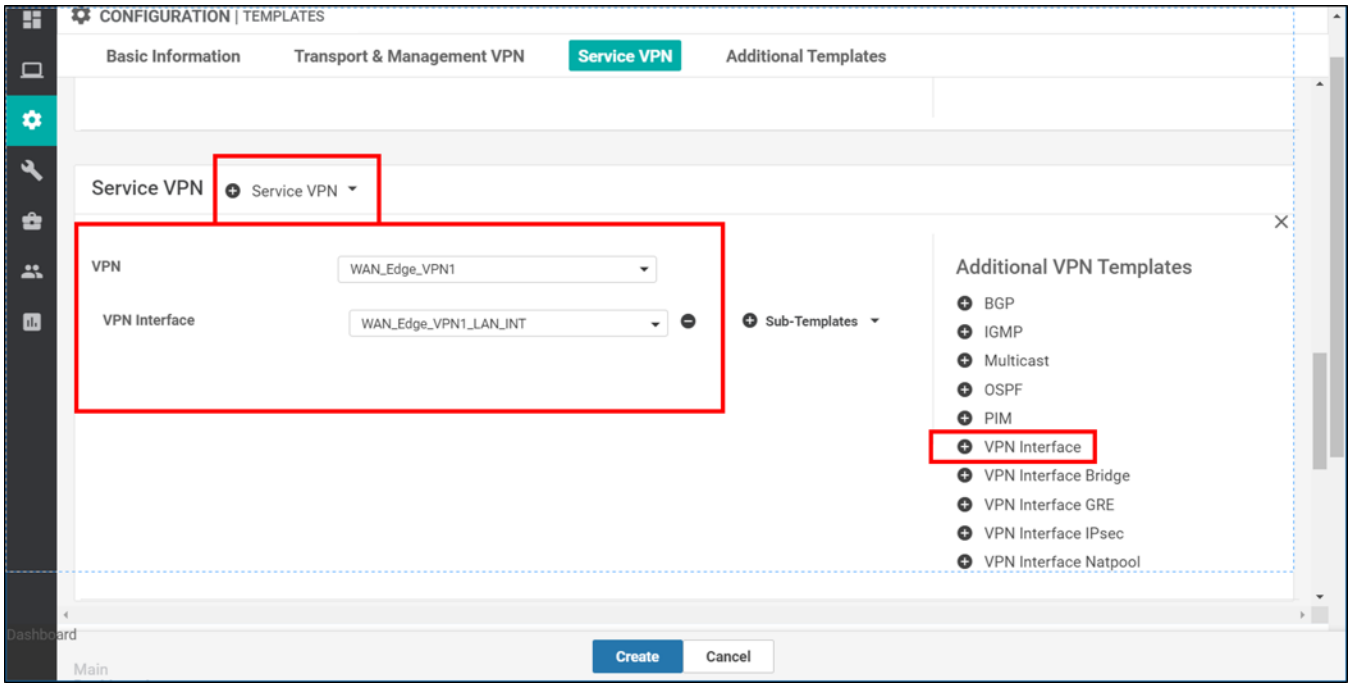


Figure 113: Device Template Service VPN Feature Templates

7.5.10.5 Save the Device Template

At the bottom of the GUI Screen, click **Create**.

The new device template now appears in the list of available device templates in the vManage GUI under **Configuration>Templates>Device** tab.

7.5.11 Attach Device to Device Template (vEdge Router)

Now that the device template is created, the configuration it generates can be applied to the SD-WAN router.

In the vManage GUI, go to **Configuration>Templates>Device**. To the right of the newly-created device template (**WAN_Edge_Remote_A**) click **…** and select **Attach Devices** from the drop-down list.

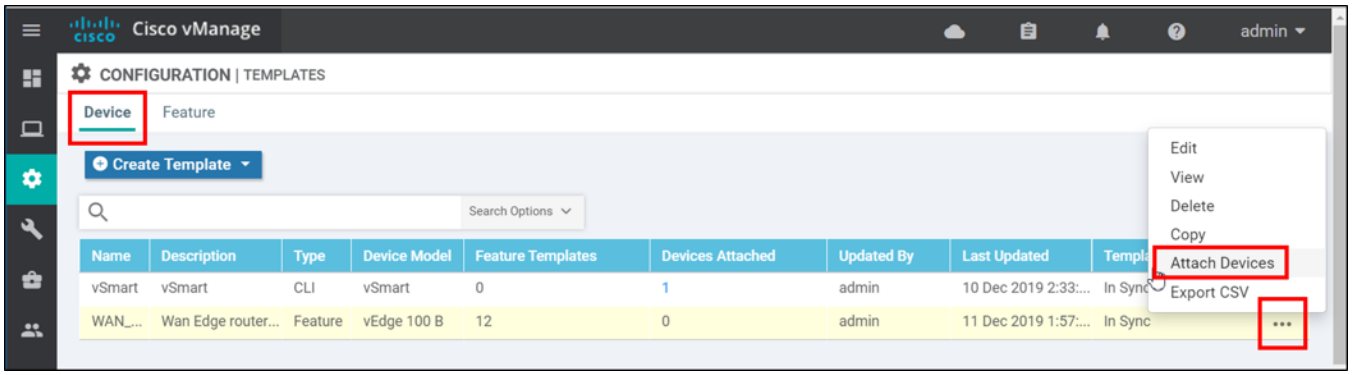


Figure 114: Attach Device to Device Template

7.5.11.1 Choose Devices to Attach to Device Template

A window is displayed that lists the available devices that can be attached to the device template based on platform type defined when the device template was created.

Choose the device from the left box (**WAN_EdgeA** in this example) and move it to the right box (more than one device can be selected). Click the **Attach** button.

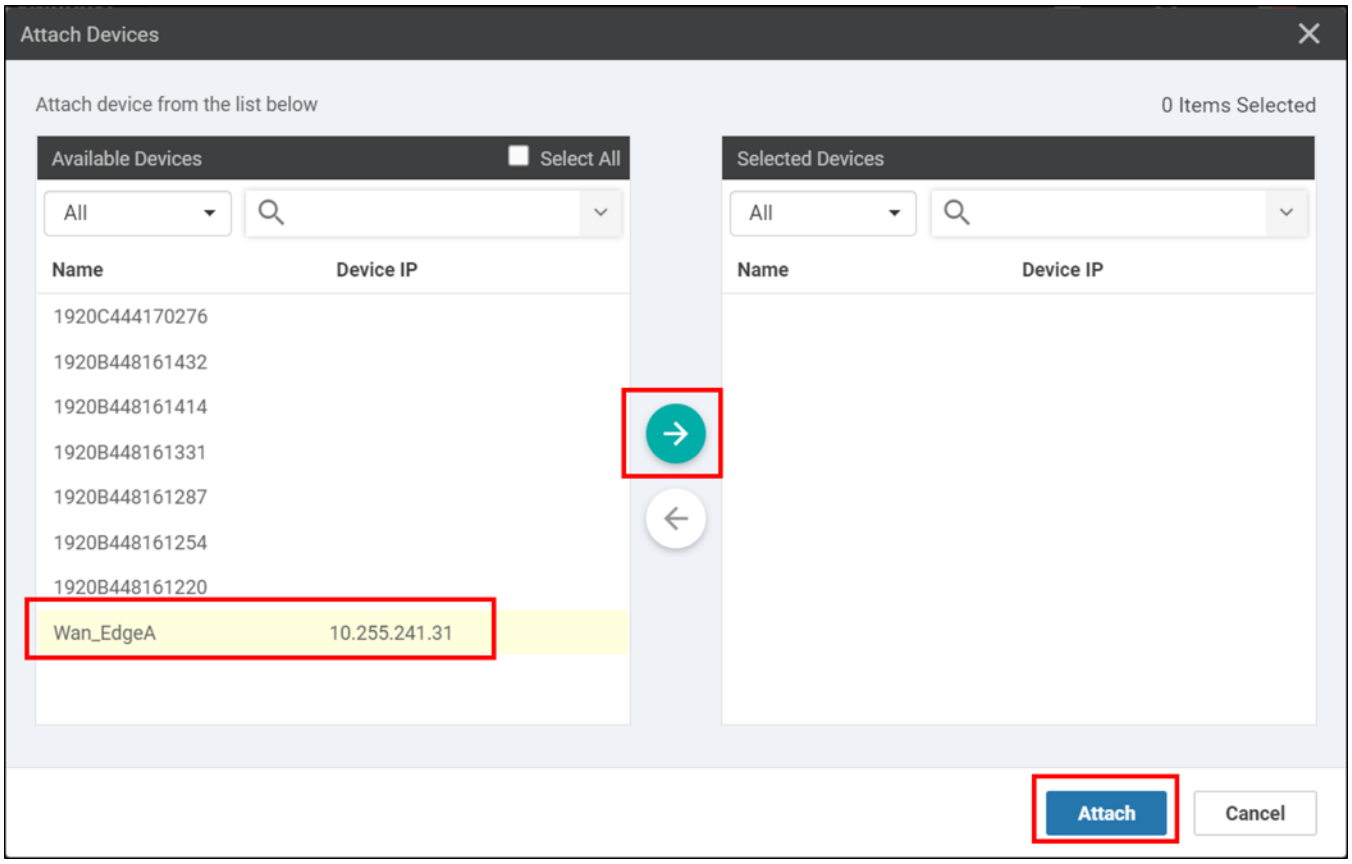


Figure 115: Choose the devices to be attached to device template

7.5.11.2 Edit Device Template

Before attaching the device, any variables that are defined in the feature templates that are attached to the device template need to be defined before the configuration can be created and pushed to the WAN Edge device. Variables associated with each device have to be defined or the configurations cannot be pushed to the WAN Edge devices. To define the variables, go to the right of each WAN Edge device being attached, click **…** and select **Edit Device Template**.

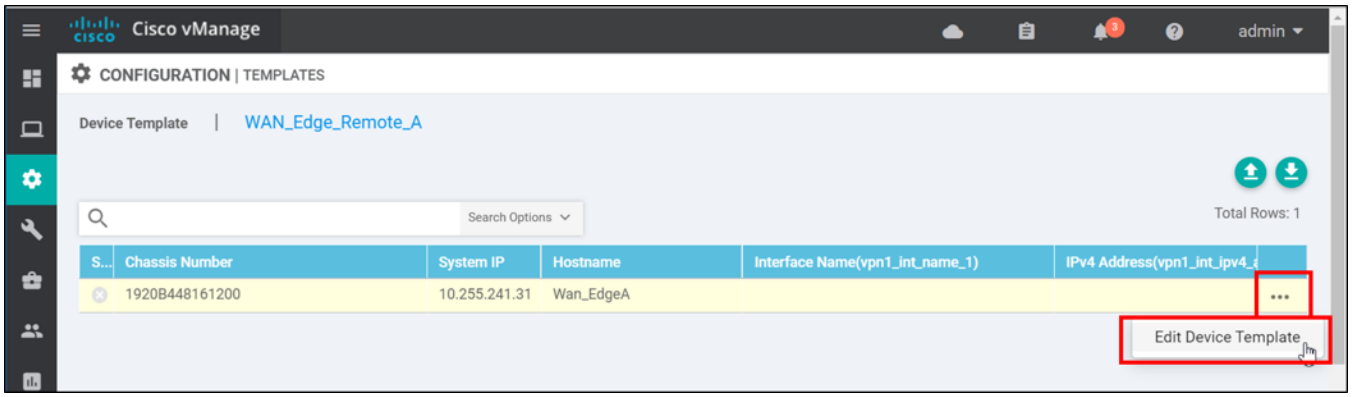


Figure 116: Edit the Device Template

7.5.11.3 Populate Device Template Values

In the **Update Device Template** window, fill in the values for the various variables. To get the system IP address and site ID that the device is originally configured with, you can issue a **show run system** on the device console or an SSH session. When defining IP addresses on an interface, be certain to include the mask bits. Alternatively, you can load values through a .csv file.

Fill in all values and click **Update**. Note that the configuration variables may be listed in a different order.

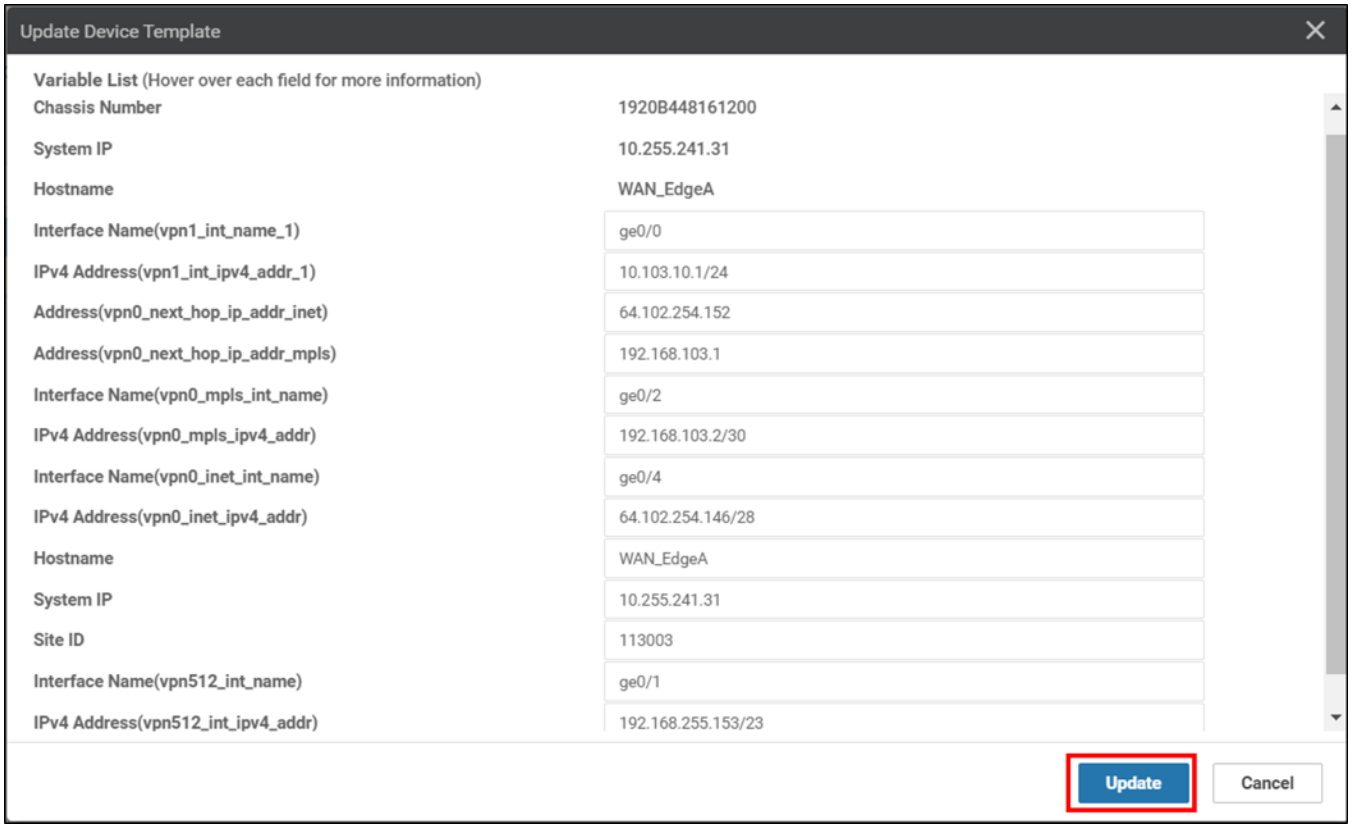


Figure 117: Populate Device Template Values

Note: It is recommended that once values are defined, click the download button before continuing. This saves the entered values in a .csv file, where they can be modified and uploaded again if need be, saving time in the future. You may need to rename the .csv file.

Click the **Next** button.

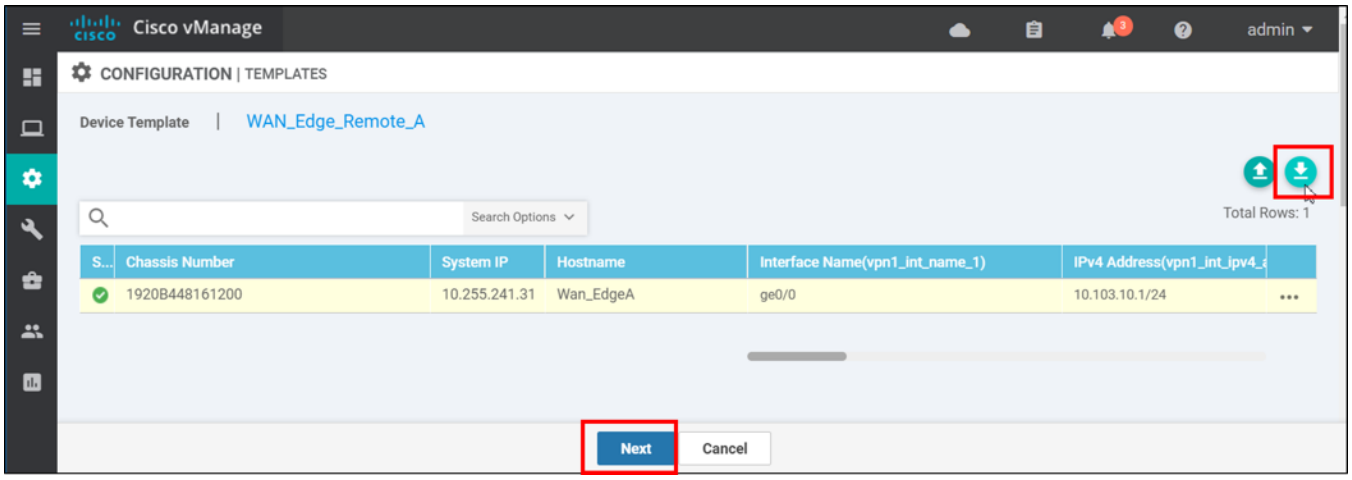


Figure 118: Download Variable Values into a spreadsheet

7.5.11.4 Configuration Preview

A configuration preview page is displayed. You can click devices on the left side of the GUI and view the resulting configuration that will be pushed to the device, as well as viewing the difference between the new and old configurations. Click **Configure Devices**.

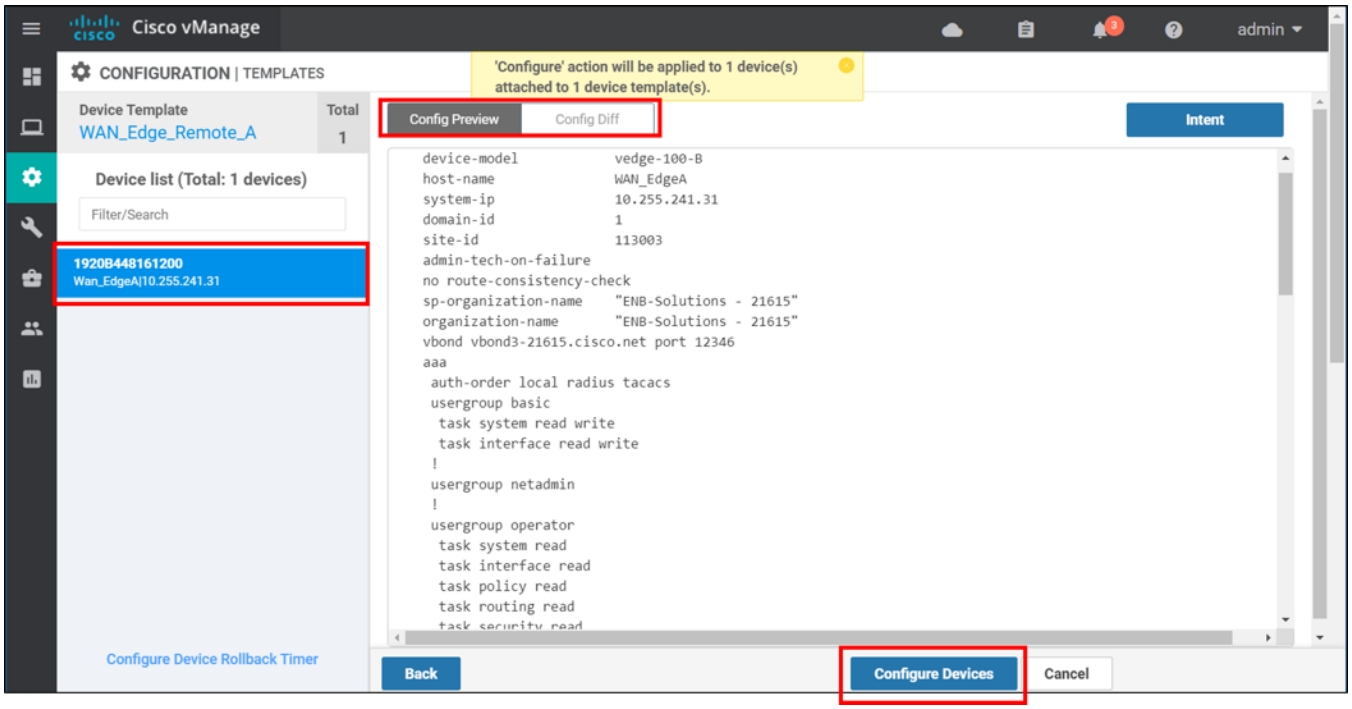


Figure 119: Configuration Preview

7.5.11.5 Verify Template Push

When the configuration is pushed completely to the SD-WAN device, the vManage indicates a **Success** message.

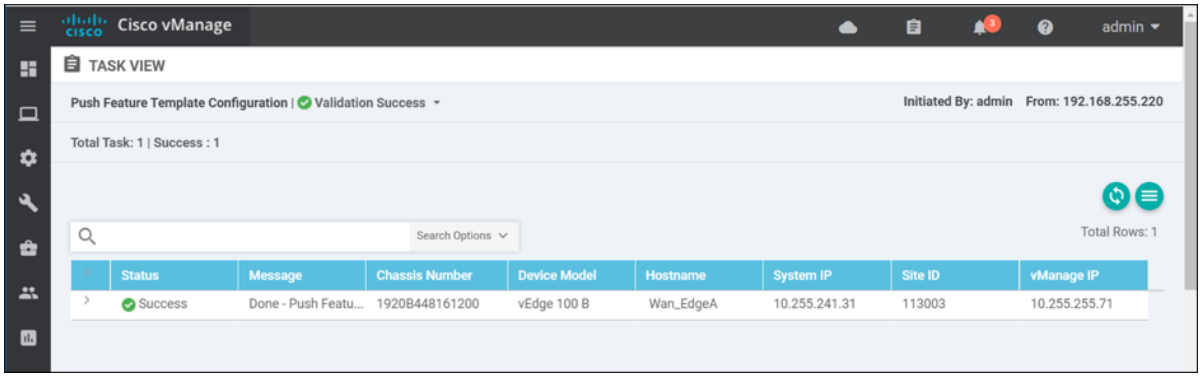


Figure 120: Successful Template Push

7.5.12 Attach Device to Device Template (IOS XE SD-WAN Router)

Now that the device template is created, the configuration it generates can be applied to the SD-WAN router. The steps are the same as the vEdge router.

In the vManage GUI, go to **Configuration>Templates>Device**. To the right of the newly-created device template (**WAN_Edge_Remote_B**) click **…** and select **Attach Devices** from the drop-down list.

7.5.12.1 Choose Devices to Attach to Device Template

A window is displayed that lists the available devices that can be attached to the device template based on platform type defined when the device template was created.

Choose the device from the left box (**WAN_EdgeB** in this example) and move it to the right box (more than one device can be selected). Click the **Attach** button.

7.5.12.2 Edit Device Template

Before attaching the device, any variables that are defined in the feature templates that are attached to the device template need to be defined before the configuration can be created and pushed to the WAN Edge device. Variables associated with each device have to be defined or the configurations cannot be pushed to the WAN Edge devices. To define the variables, go to the right of each WAN Edge device being attached, click **…** and select **Edit Device Template**.

7.5.12.3 Populate Device Template Values

In the **Update Device Template** window, fill in the values for the various variables. To get the system IP address and site ID that the device is originally configured with, you can issue a **show sdwan run system** on the device console or an SSH session. When defining IP addresses on an interface, be certain to include the mask bits. Interface names should be expanded out. Alternatively, you can load values through a .csv file.

Fill in all values and click **Update**. Note that the configuration variables may be listed in a different order.

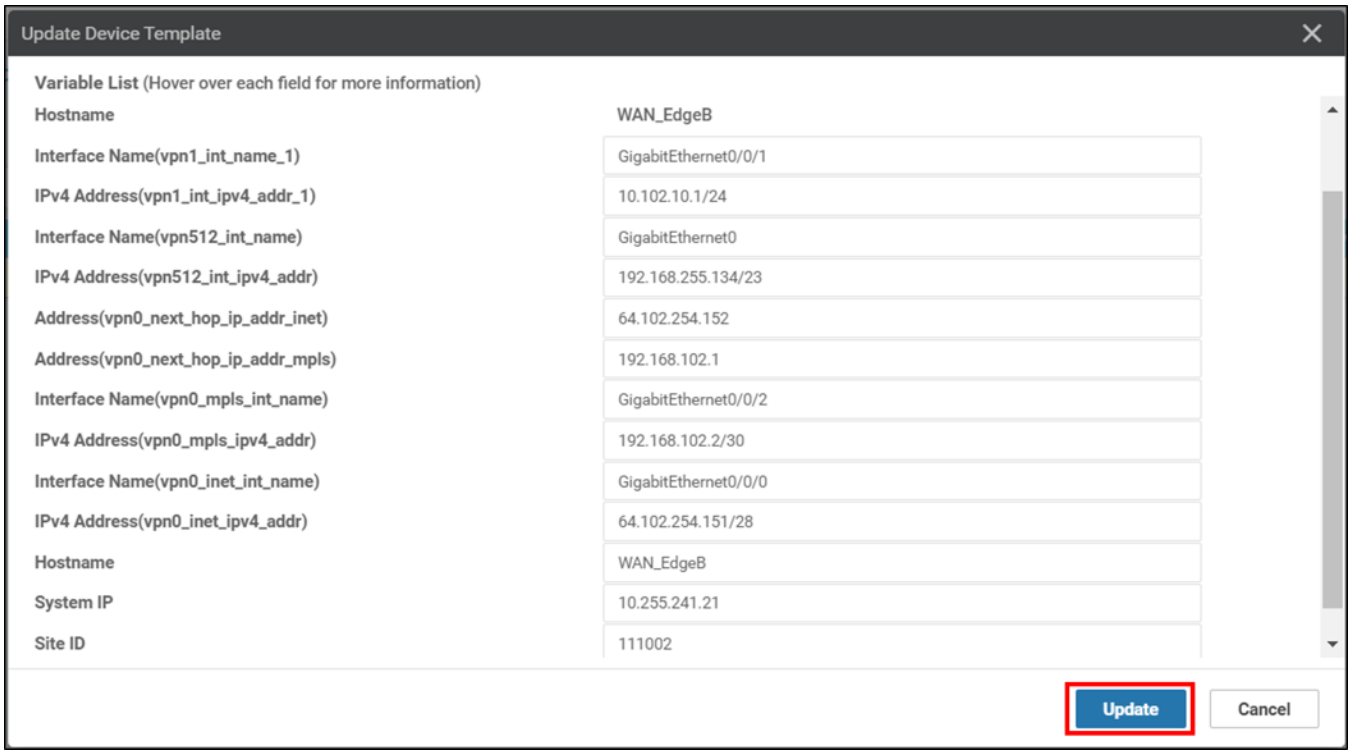


Figure 121: Populate Device Template Values

Note: It is recommended that once values are defined, click the download button before continuing. This saves the entered values in a .csv file, where they can be modified and uploaded again if need be, saving time in the future. You may need to rename the .csv file.

Click the **Next** button.

7.5.12.4 Configuration Preview

A configuration preview page is displayed. You can click devices on the left side of the GUI and view the resulting configuration that will be pushed to the device, as well as viewing the difference between the new and old configurations. Click **Configure Devices**.

7.5.12.5 Verify Template Push

When the configuration is pushed completely to the SD-WAN device, the vManage indicates a **Success** message.

7.5.13 Verify Control Connections

Verify that control connections are up over both transports. vManage is accessed over one transport, and vSmart controllers are accessed over both transports.

Under the vManage Main Dashboard, click the arrow in the WAN Edge status box at the top of the GUI.

Figure 122: Check WAN Edge Status

To the right of the WAN Edge router, click **…** and select **Real Time** from the drop-down box.

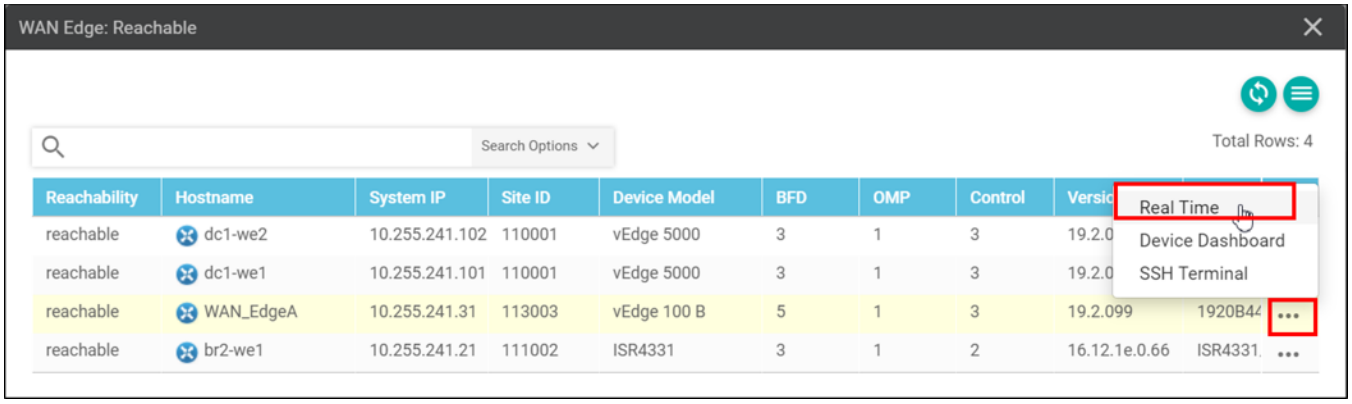


Figure 123: Select Real Time Status

To the left, scroll down and click **Control Connections**.

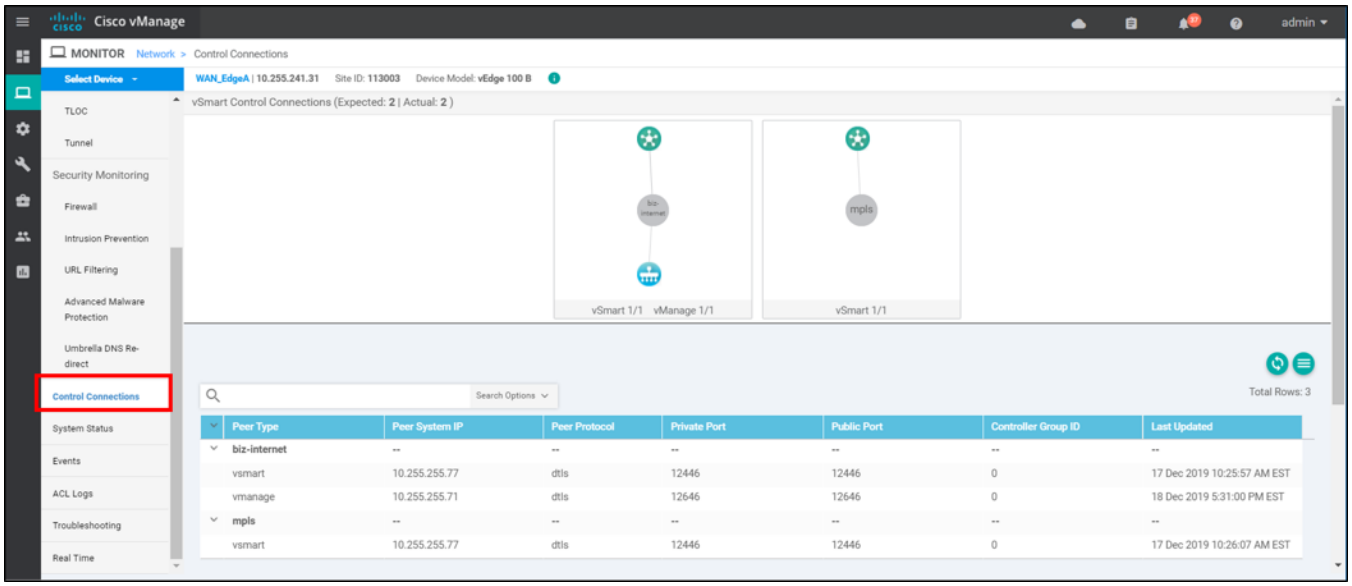


Figure 124: Verify Control Connections

7.6 vEdge CLI Configuration

This section demonstrates the CLI configuration needed to interoperate with Zscaler. These are equivalent to the feature and device templates developed earlier. Note that the recommended way to configure Cisco SD-WAN devices is through feature and device templates from vManage.

7.6.1 Configure Base Connectivity

The following is a basic connectivity configuration for the vEdge. It includes one other transport (mpls), which is not essential to the connectivity to the Zscaler. Some default configurations have been removed:

```
system
 host-name               WAN_EdgeA
 system-ip               10.255.241.31
 site-id                 113003
 organization-name       "ENB-Solutions - 21615"
 vbond vbond3-21615.cisco.net
 aaa
  !
  user netadmin
   password (REMOVED)
   group    netadmin
  !
!
vpn 0
 name "Transport VPN"
 dns 64.100.100.125 primary
 dns 64.100.100.126 secondary
 interface ge0/2
  ip address 192.168.103.2/30
  tunnel-interface
   encapsulation ipsec
   color mpls restrict
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 interface ge0/4
  ip address 64.102.254.146/28
  !
```

```
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 ip route 0.0.0.0/0 64.102.254.152
 ip route 0.0.0.0/0 192.168.103.1
!
vpn 1
 name LAN
 interface ge0/0
  ip address 10.103.10.1/24
  no shutdown
 !
!
vpn 512
 name "Transport VPN"
 interface ge0/1
  ip address 192.168.255.153/23
  no shutdown
 !
!
```

7.6.2 Add GRE Tunnels with a GRE route

The following configuration adds two GRE tunnels, one primary and one secondary to the transport VPN. A GRE route is added to direct traffic from the service VPN (VPN 1) to the Zscaler over the GRE tunnels. Tunnels operate as primary/backup.

```
config t
vpn 0
interface gre1
  ip address 172.17.12.217/30
  tunnel-source-interface ge0/4
  tunnel-destination      104.129.194.38
  mtu                     1476
  tcp-mss-adjust          1432
  no shutdown
 !
 interface gre2
  ip address 172.17.12.221/30
  tunnel-source-interface ge0/4
  tunnel-destination      199.168.148.131
  mtu                     1476
  tcp-mss-adjust          1432
  no shutdown

vpn 1
 ip gre-route 0.0.0.0/0 vpn 0 interface gre1 gre2
commit
```

Tunnel and Route Status:

```
WAN_EdgeA# sh int gre1
interface vpn 0 interface gre1 af-type ipv4
 ip-address        172.17.12.217/30
 if-admin-status   Up
 if-oper-status    Up
 if-tracker-status NA
 encap-type        null
 port-type         service
 mtu               1476
 hwaddr            40:66:fe:92:00:00
 speed-mbps        1000
 duplex            full
 tcp-mss-adjust    1392
 uptime            0:00:01:39
 rx-packets        2
 tx-packets        2
WAN_EdgeA# sh int gre2
interface vpn 0 interface gre2 af-type ipv4
 ip-address        172.17.12.221/30
 if-admin-status   Up
 if-oper-status    Up
 if-tracker-status NA
```

```
 encap-type         null
 port-type          service
 mtu                1476
 hwaddr             40:66:fe:92:00:00
 speed-mbps         1000
 duplex             full
 tcp-mss-adjust     1392
 uptime             0:00:01:41
 rx-packets         0
 tx-packets         0


WAN_EdgeA# show ip route vpn 1
                              NEXTHOP    NEXTHOP
VPN     PREFIX       PROTOCOL  IF NAME    VPN     TLOC IP          COLOR         ENCAP
-------------------------------------------------------------------------------------
1       0.0.0.0/0     gre       gre1      0       -                -              -
1       0.0.0.0/0     omp        -        -       10.255.241.101   mpls          ipsec
1       0.0.0.0/0     omp        -        -       10.255.241.101   biz-internet  ipsec
```

7.6.3 Add IPsec Tunnels with an IPsec route

The following configuration adds two IPsec tunnels to the base configuration, one primary and one secondary to the transport VPN. An IPsec route is added to direct traffic from the service VPN (VPN 1) to the Zscaler over the IPsec tunnels. Tunnels operate as primary/backup.

```
config t
vpn 0
interface ipsec1
  ip address 11.1.1.1/30
  tunnel-source-interface ge0/4
  tunnel-destination      was1-vpn.zscalerbeta.net
  ike
   version      2
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        2
   authentication-type
    pre-shared-key
     pre-shared-secret Cisco12345678901
     local-id          user@cisco.com
     remote-id         104.129.194.39
    !
   !
  !
  ipsec
   rekey                    3600
   replay-window            512
   cipher-suite             null-sha1
   perfect-forward-secrecy none
  !
  no shutdown
 !
 interface ipsec2
```

```
  ip address 11.1.2.1/30
  tunnel-source-interface ge0/4
  tunnel-destination      sunnyvale1-vpn.zscalerbeta.net
  ike
   version      2
   rekey        14400
   cipher-suite aes256-cbc-sha1
   group        2
   authentication-type
    pre-shared-key
     pre-shared-secret Cisco12345678901
     local-id          user@cisco.com
     remote-id         199.168.148.132
    !
   !
  !
  ipsec
   rekey                   3600
   replay-window           512
   cipher-suite            null-sha1
   perfect-forward-secrecy none
  !
  no shutdown
!
vpn 1
 ip ipsec-route 0.0.0.0/0 vpn 0 interface ipsec1 ipsec2
commit
```

Tunnel and Route Status:

```
WAN_EdgeA# sh int ipsec1
interface vpn 0 interface ipsec1 af-type ipv4
 ip-address        11.1.1.1/30
 if-admin-status   Up
 if-oper-status    Up
 if-tracker-status NA
 encap-type        vlan
 port-type         service
 mtu               1500
 hwaddr            72:41:c5:97:08:d3
 speed-mbps        1000
 duplex            full
 tcp-mss-adjust    1416
 uptime            0:00:05:18
 rx-packets        426
 tx-packets        278
WAN_EdgeA# sh int ipsec2
interface vpn 0 interface ipsec2 af-type ipv4
 ip-address        11.1.2.1/30
 if-admin-status   Up
 if-oper-status    Up
 if-tracker-status NA
 encap-type        vlan
 port-type         service
 mtu               1500
 hwaddr            72:41:c5:97:08:d3
```

```
 speed-mbps         1000
 duplex             full
 tcp-mss-adjust     1416
 uptime             0:00:05:20
 rx-packets         138
 tx-packets         9

WAN_EdgeA# show ipsec ike sessions

     IF                                  SOURCE                    DEST
VPN  NAME    VERSION  SOURCE IP         PORT    DEST IP           PORT          STATE
-------------------------------------------------------------------------------------
0    ipsec1  2        64.102.254.146    4500    104.129.194.39    4500 IKE_UP_IPSEC_UP
0    ipsec2  2        64.102.254.146    4500    199.168.148.132   4500 IKE_UP_IPSEC_UP

WAN_EdgeA# show ip route vpn 1
                              NEXTHOP    NEXTHOP
VPN    PREFIX    PROTOCOL     IF NAME    VPN     TLOC IP          COLOR        ENCAP
-----------------------------------------------------------------------------------
1      0.0.0.0/0  std-ipsec   ipsec1      0       -                -            -
1      0.0.0.0/0  omp         -          -       10.255.241.101   mpls         ipsec
1      0.0.0.0/0  omp         -          -       10.255.241.101   biz-internet ipsec
```

7.6.4 Add Layer 7 Health Check

The following adds a Layer 7 Health Check to the primary tunnel. This assumes you have GRE or IPSEC tunnels already configured. This example uses IPSEC tunnels.

```
system
 tracker l7_zscaler_health_check1
  endpoint-api-url http://gateway.zscalerbeta.net/vpntest
  interval 10

vpn 0
interface ipsec1
tracker l7_zscaler_health_check1
```

Status

```
WAN_EdgeA# show interface ipsec1

                                  IF      IF      IF
                AF                ADMIN   OPER    TRACKER  ENCAP  PORT
VPN  INTERFACE  TYPE  IP ADDRESS   STATUS  STATUS  STATUS   TYPE   TYPE     MTU
-------------------------------------------------------------------------------
0    ipsec1     ipv4  11.1.1.1/30  Up      Up      Up       vlan   service  1500
```

7.7 IOS XE SD-WAN CLI Configuration

The following is a basic connectivity configuration for the IOS XE SD-WAN router. It includes one other transport (mpls), which is not essential to the connectivity to the Zscaler. Some default configurations have been removed:

```
system
 system-ip             10.255.241.21
 site-id               111002
 organization-name     "ENB-Solutions - 21615"
 vbond vbond3-21615.cisco.net port 12346
!
hostname WAN_EdgeB
username admin privilege 15 password (REMOVED)
username netadmin privilege 15 password (REMOVED)
vrf definition 1
 description LAN
 rd          1:1
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 description Transport VPN
 rd          1:512
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
ip name-server 64.100.100.125 64.100.100.126
ip route 0.0.0.0 0.0.0.0 64.102.254.152 1
ip route 0.0.0.0 0.0.0.0 192.168.102.1 1
!
interface GigabitEthernet0
 no shutdown
 vrf forwarding Mgmt-intf
 ip address 192.168.255.134 255.255.254.0
exit
interface GigabitEthernet0/0/0
 no shutdown
 ip address 64.102.254.151 255.255.255.240
exit
interface GigabitEthernet0/0/1
 no shutdown
 vrf forwarding 1
 ip address 10.102.10.1 255.255.255.0
exit
```

```
interface GigabitEthernet0/0/2
 no shutdown
 ip address 192.168.102.2 255.255.255.252
exit
interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/0
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit
interface Tunnel2
 no shutdown
 ip unnumbered GigabitEthernet0/0/2
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/2
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/2
 tunnel mode sdwan
exit
clock timezone UTC 0 0
!
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec weight 1
   color biz-internet
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service ospf
   no allow-service stun
   no allow-service snmp
  exit
 exit
 interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec weight 1
   color mpls restrict
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   allow-service ntp
   no allow-service ospf
   no allow-service stun
```

```
   no allow-service snmp
  exit
 exit
```

7.7.1 Add Service-side IPsec Tunnels with an IPsec route

The following configuration adds two IPsec tunnels to the base configuration, one primary and one secondary to the service VPN. An IPsec route is added to direct traffic from the service VPN (VPN 1) to the Zscaler over the IPsec tunnels.

```
interface Tunnel100001
 no shutdown
 vrf forwarding 1
 ip address 12.1.1.1 255.255.255.252
 tunnel source      GigabitEthernet0/0/0
 tunnel destination 104.129.194.39
 tunnel mode ipsec ipv4
 tunnel path-mtu-discovery
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
exit
interface Tunnel100002
 no shutdown
 vrf forwarding 1
 ip address 12.1.2.1 255.255.255.252
 tunnel source      GigabitEthernet0/0/0
 tunnel destination 199.168.148.132
 tunnel mode ipsec ipv4
 tunnel path-mtu-discovery
 tunnel protection ipsec profile if-ipsec2-ipsec-profile
exit
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 104.129.194.39
  pre-shared-key Cisco12345678901
 !
!
crypto ikev2 keyring if-ipsec2-ikev2-keyring
 peer if-ipsec2-ikev2-keyring-peer
  address 199.168.148.132
  pre-shared-key Cisco12345678901
 !
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 profile if-ipsec1-ikev2-profile
 authentication local pre-share
 authentication remote pre-share
 dpd 10 3 on-demand
 identity local email user@cisco.com
 keyring local if-ipsec1-ikev2-keyring
 lifetime 86400
 match identity remote address 104.129.194.39
!
crypto ikev2 profile if-ipsec2-ikev2-profile
```

```
 authentication local pre-share
 authentication remote pre-share
 dpd 10 3 on-demand
 identity local email user@cisco.com
 keyring local if-ipsec2-ikev2-keyring
 lifetime 86400
 match identity remote address 199.168.148.132
!
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 group 14 15 16 2
 integrity sha1 sha256 sha384 sha512
!
crypto ipsec transform-set if-ipsec1-ikev2-transform esp-null esp-sha-hmac
 mode tunnel
!
crypto ipsec transform-set if-ipsec2-ikev2-transform esp-null esp-sha-hmac
 mode tunnel
!
crypto ipsec profile if-ipsec1-ipsec-profile
 set ikev2-profile if-ipsec1-ikev2-profile
 set transform-set if-ipsec1-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!
crypto ipsec profile if-ipsec2-ipsec-profile
 set ikev2-profile if-ipsec2-ikev2-profile
 set transform-set if-ipsec2-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!

ip route vrf 1 0.0.0.0 0.0.0.0 12.1.1.2 1
ip route vrf 1 0.0.0.0 0.0.0.0 12.1.2.2 1
```

7.7.2 Add IOS XE SD-WAN Workarounds

At this point, the IOS XE SD-WAN IPsec tunnels are configured, but not fully operational. There are a few workarounds in this code version that need to be implemented to allow the tunnels to work fully.

The following workarounds should be implemented:

1) Host routes should be added for the tunnel destinations in VPN 0.
2) Disable IKE Config Exchange – vManage version 19.2.1 pushes this configuration, but in this version of code, it needs to be configured manually via CLI.
3) An ACL should be implemented to explicitly allow IPsec traffic.

Configure the following:

```
config-t

ip route 104.129.194.39 255.255.255.255 64.102.254.152
ip route 199.168.148.132 255.255.255.255 64.102.254.152
commit

crypto ikev2 profile if-ipsec1-ikev2-profile
config-exchange request
commit
no config-exchange request
commit

crypto ikev2 profile if-ipsec2-ikev2-profile
config-exchange request
commit
no config-exchange request
commit

policy
 access-list PERMIT-ZSCALER-ZENS
  sequence 1
   match
    source-ip 199.168.148.132/32
   !
   action accept
   !
  !
   exit
  exit
  sequence 2
   match
    source-ip 104.129.194.39/32
  !
   action accept
  !
 !
 default-action accept
!
sdwan
interface GigabitEthernet0/0/0
access-list PERMIT-ZSCALER-ZENS in
commit
```

Note: You can try a `clear crypto session` command if IKE Config Exchange was disabled after IKE was negotiated.

Tunnel Status:

```
WAN_EdgeB#show int tun100001
Tunnel100001 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 12.1.1.1/30
  MTU 9958 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
```

```
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 64.102.254.151 (GigabitEthernet0/0/0), destination 104.129.194.39
   Tunnel Subblocks:
      src-track:
         Tunnel100001 source tracking subblock associated with GigabitEthernet0/0/0
          Set of tunnels with source GigabitEthernet0/0/0, 3 members (includes
iterators), on interface <OK>
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Path MTU Discovery, ager 10 mins, min MTU 92
  Tunnel transport MTU 1458 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "if-ipsec1-ipsec-profile")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 04:51:31
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     14 packets input, 5163 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     15 packets output, 1372 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
WAN_EdgeB#show int tun100002
Tunnel100002 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 12.1.2.1/30
  MTU 9958 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 64.102.254.151 (GigabitEthernet0/0/0), destination 199.168.148.132
   Tunnel Subblocks:
      src-track:
         Tunnel100002 source tracking subblock associated with GigabitEthernet0/0/0
          Set of tunnels with source GigabitEthernet0/0/0, 3 members (includes
iterators), on interface <OK>
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Path MTU Discovery, ager 10 mins, min MTU 92
  Tunnel transport MTU 1458 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "if-ipsec2-ipsec-profile")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 04:51:34
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   18 packets input, 6114 bytes, 0 no buffer
   Received 0 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   30 packets output, 5315 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 unknown protocol drops
   0 output buffer failures, 0 output buffers swapped out
```

In addition, you can use show crypto ikev2 session and show crypto ipsec sa to troubleshoot tunnel issues.