CCNP Enterprise Certification

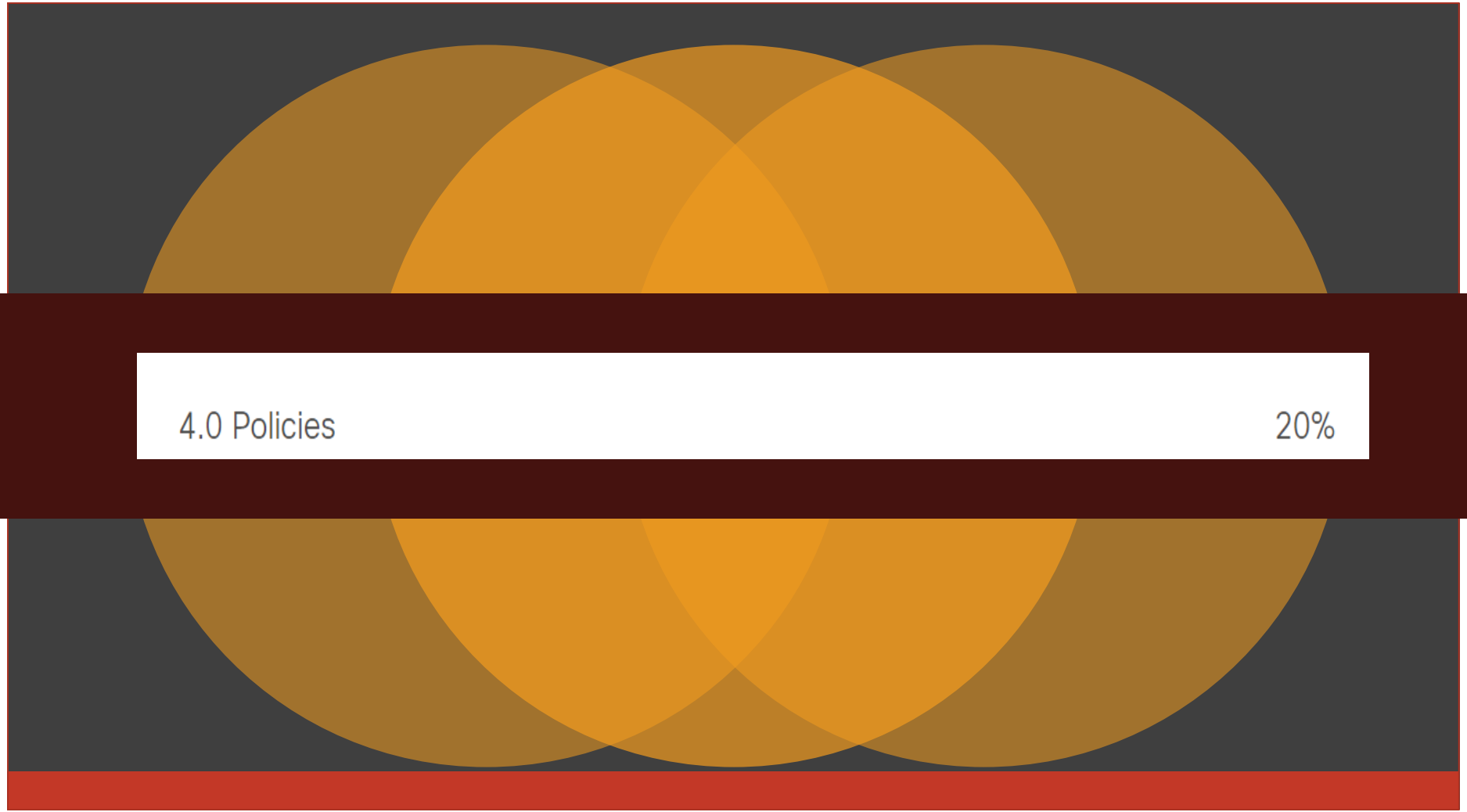
ENSDWI : 300-415

CCNP Enterprise Certification

ENSDWI : 300-415

CCNP Enterprise Certification

ENSDWI : 300-415


4.0 Policies
20%

4.0

- 4.1 Configure and verify control policies
- 4.2 Configure and verify data policies
- 4.3 Configure and verify end-to-end segmentation
- 4.3.a VPN segmentation
- 4.3.b Topologies
- 4.4 Configure and verify SD-WAN application-aware routing
- 4.5 Configure and verify direct Internet access

4.1 till 4.3b

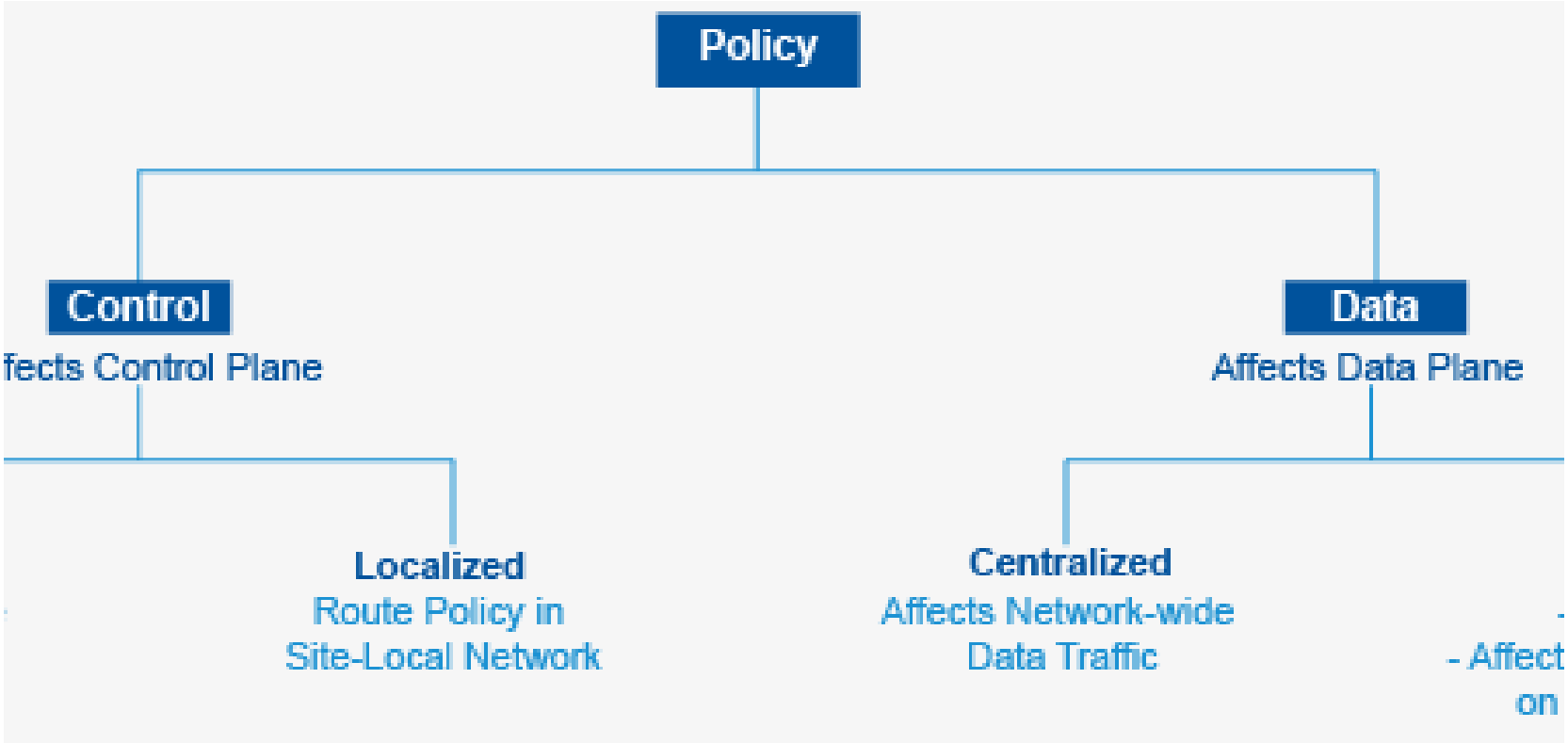
- 4.1 Configure and verify control policies
- 4.2 Configure and verify data policies
- 4.3 Configure and verify end-to-end segmentation
- 4.3.a VPN segmentation
- 4.3.b Topologies

4.4 Configure and verify SD-WAN application-aware routing

4.5 Configure and verify direct Internet access

Cisco SDWAN Viptela

Viptela Policy


Policy
Control
fects Control Plane
Data
Affects Data Plane
Localized
Route Policy in
Site-Local Network
Centralized
Affects Network-wide
Data Traffic
- Affect
on

Policy Overview

- Policy is used to influence the flow of data traffic among the vEdge routers in the overlay network. Policy comprises:
- ***Control or Routing policy***, which affects the flow of routing information in the network's control plane

- ***Data policy***, which affects the flow of data traffic in the network's data plane
- To implement enterprise-specific traffic control requirements, you create basic policies, and you deploy advanced features of the Viptela software that are activated by means of the policy configuration infrastructure.

- Just as the Viptela overlay network architecture clearly separates the control plane from the data plane and clearly separates control between centralized and localized functions, the Viptela policy software is cleanly separated: policies apply either to control plane or data plane traffic, and they are configured either centrally (on vSmart controllers) or locally (on vEdge routers).

vSmart Policy Architecture Components

The implementation of vSmart policy is done by configuring the entire policy on the vSmart controller. vSmart policy configuration is accomplished with three building blocks:

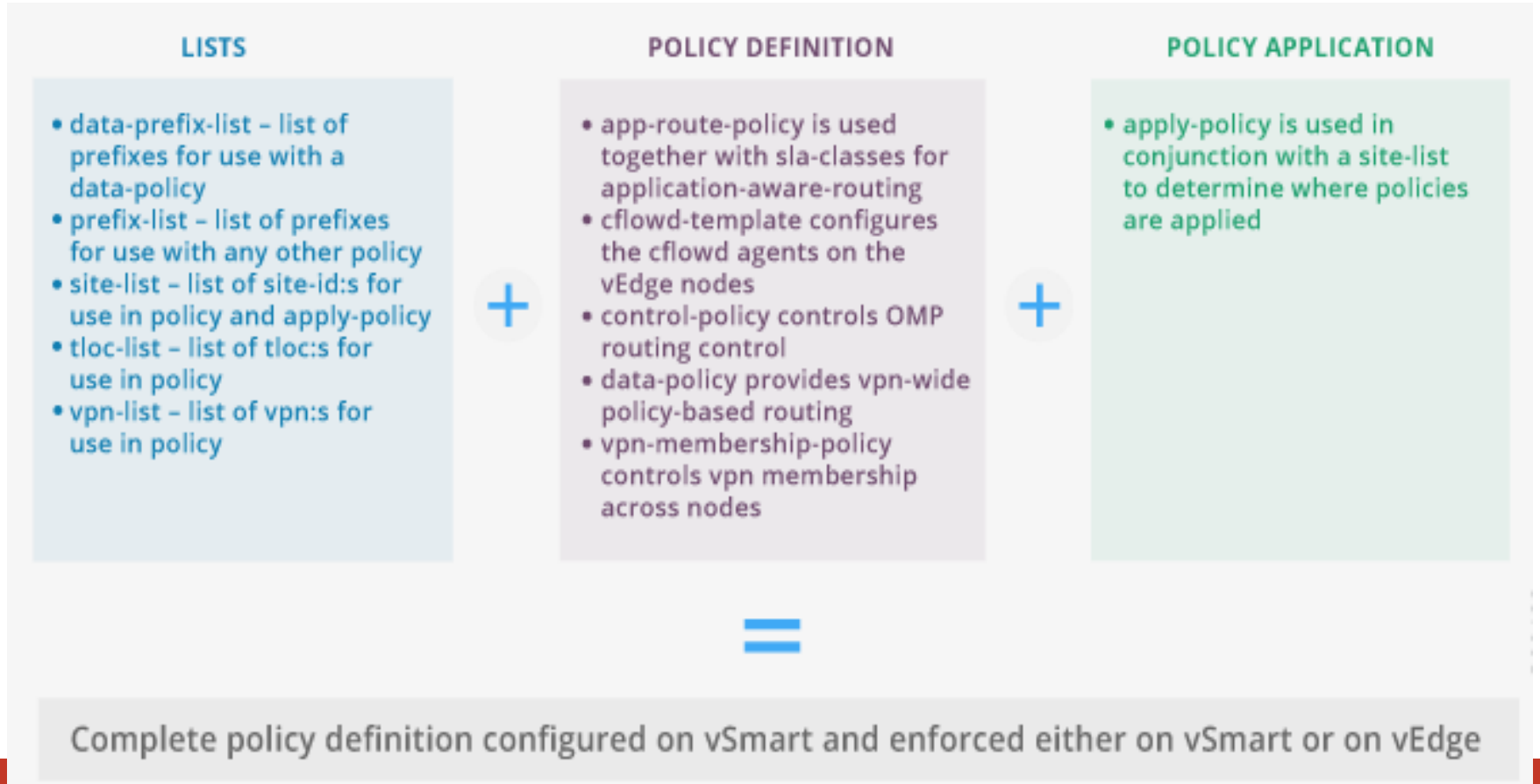
•***Lists*** define the targets of policy application or matching.

•***Policy*** *definition*, or *policies*, controls aspects of control and forwarding. There are different types of policy, including:

- app-route-policy (for application-aware routing)
- cflowd-template (for cflowd flow monitoring)
- control-policy (for routing and control plane information)
- data-policy (for data traffic)
- vpn-membership-policy (for limiting the scope of traffic to specific VPNs)

•***Policy application* controls** what a policy is applied towards. Policy application is site-oriented, and is defined by a specific list called a site-list.

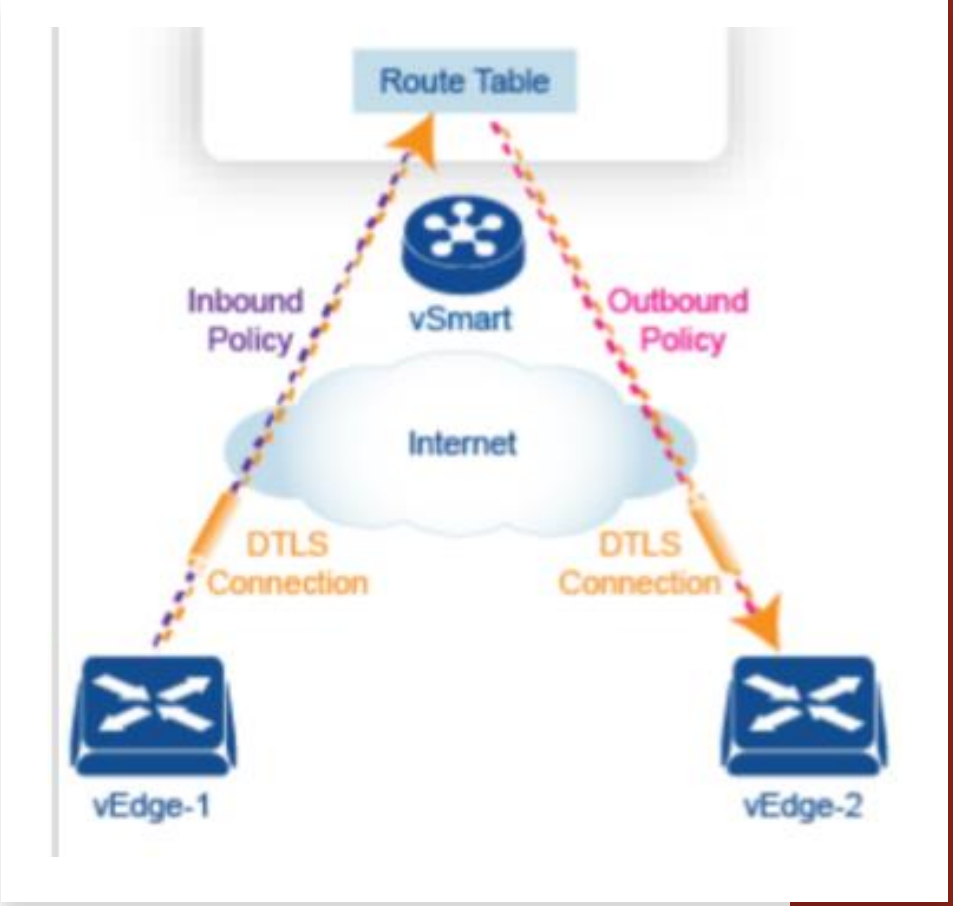
Assemble these three building blocks to vSmart policy



Centralized Control Policy: Inbound vs. Outbound

- In-bound Policy: determines which routes are installed in the local routing database of the vSmart controller

- Out-bound Policy: applied AFTER a route is retrieved from routing database, but BEFORE the vSmart controller advertises it



Configuring and Executing vSmart Policies

- All vSmart policies are configured on the vSmart controller, using a combination of policy definition and lists. All vSmart policies are also applied on the vSmart controller, with a combination of apply-policy and lists. However, where the actual vSmart policy executes depends on the type of policy, as shown in this figure:

vSmart

Action	App-route Policy	Cflowd Template	Control Policy	Data Policy	VPN Membership Policy
Configure	✓	✓	✓	✓	✓
Apply	✓	✓	✓	✓	✓
Execute			✓		✓

vEdge

Action	App-route Policy	Cflowd Template	Control Policy	Data Policy	VPN Membership Policy
Configure					
Apply					
Execute	✓	✓		✓	

vSmart Policy Components

data-prefix-list is used in data-policy to define prefix and upper layer ports, either individually or jointly, for traffic matching.
prefix-list is used in control-policy to define prefixes for matching RIB entries.
site-list is used in control-policy to match source sites, and in apply-policy to define sites for policy application.
tloc-list is used in control-policy to define TLOCs for matching RIB entries and to apply redefined TLOCs to vRoutes.
vpn-list is used in control-policy to define prefixes for matching RIB entries, and in data-policy and app-route-policy to define VPNs for policy application.

```
policy
 lists
  data-prefix-list app1
   ip-prefix 1.1.1.1/32 port 100
  !
  prefix-list pfx1
   ip-prefix 1.1.1.1/32
  !
  site-list site1
   site-id 100
  !
  tloc-list site1_tloc
   tloc 1.1.1.1 color mpls
  vpn-list vpn1
   vpn 1
  !
!
```

Policy Definition

policy-type—which can be **control-policy**, **data-policy**, or **vpn-menbership**
(as well as a few other keywords that we discuss later)—dictates the type of policy. Each type has a particular syntax and a particular set of match conditions and settable actions.
vpn-list is used by data-policy and app-route-policy to list the VPNs for which the policy is applicable.
sequence defines each sequential step of the policy by sequence number.
match decides what entity to match on in the specific policy sequence.
action determines the action that corresponds to the preceding match statement.
default-action is the action to take for any entity that is not matched in any sequence of the policy. By default, the action is set to reject.

```
policy
 policy-type name
 vpn-list vpn-list
  sequence number
   match
    <route | tloc | vpn | other>
   !
    action <accept | reject |drop>
     set attribute value
    !
   default-action <reject | accept>
  !
 !
!
```

Policy Application

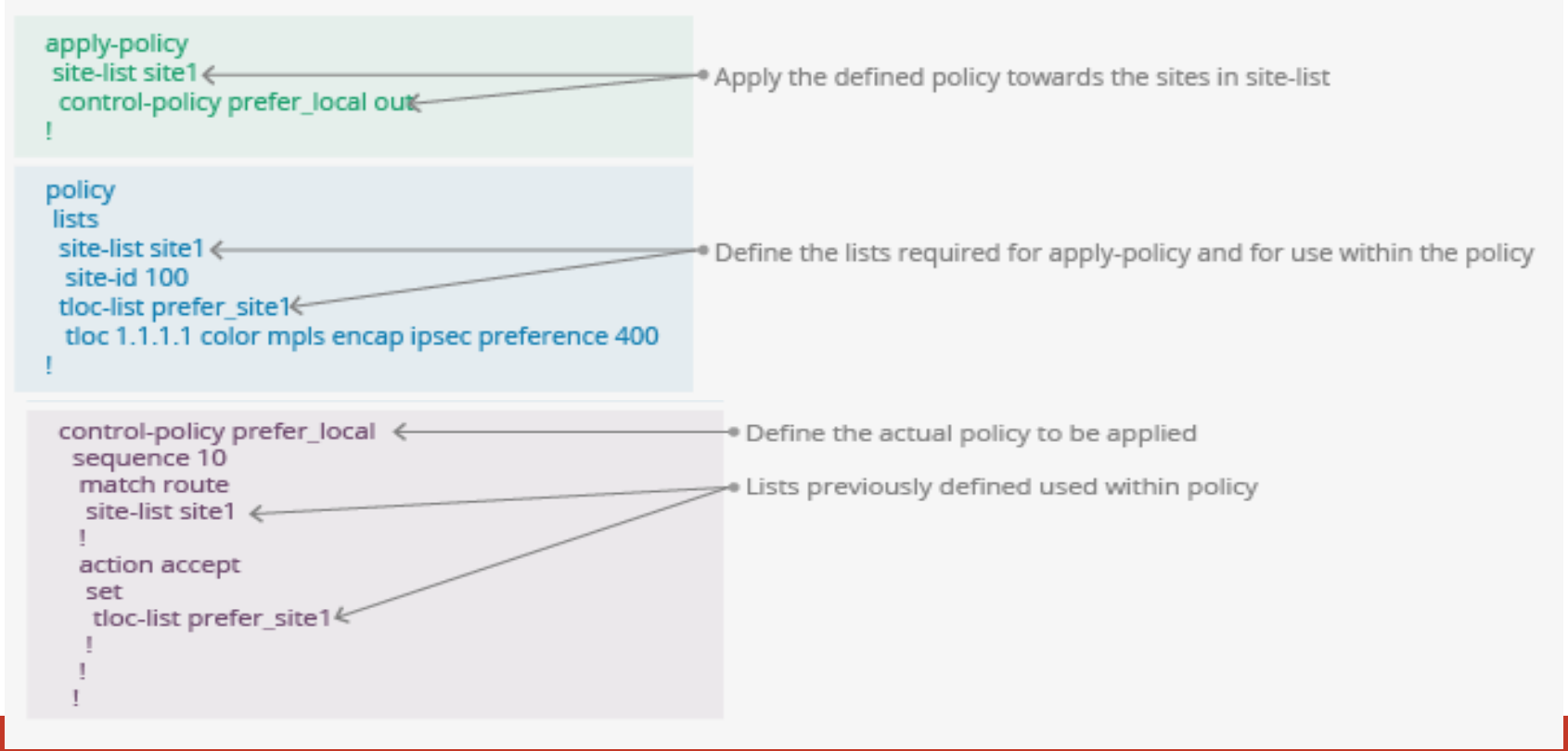
For a policy definition to take effect, you associate it with sites in the overlay network.

The following are the configuration components: **site-list** determines the sites to which a given policy is applies. The direction (in | out) applies only to control-policy.

The policy type—**control-policy**, **data-policy**, **vpn-membership**—and name refer to an already configured policy to be applied to the sites specified in the site-list for the section.

```
apply-policy
 site-list name
  control-policy name <in|out>
 !
 site-list name
  data-policy name
  vpn-membership name
policy
 policy-type name
 vpn-list vpn-list
  sequence number
   match
    <route | tloc | vpn | other>
   !
    action <accept | reject |drop>
     set attribute value
    !
   default-action <reject | accept>
  !
 !
!
```

Policy Example



Understanding vSmart Policy Processing and Application

Understanding how vSmart policy is processed and applied allows to proper design of policy and evaluation of how policy is being implemented across the overlay network. Policy is processed in this way:

•A policy definition consists of a numbered, ordered sequence of match–action pairings. Within each policy, the pairings are processed in sequential order, starting with the lowest number and incrementing.

•As soon as a match occurs, the matched entity is subject to the configured action of the sequence and is then no longer subject to continued processing.
•Any entity not matched in a sequence is subject to the default action for the policy. By default, this action is reject.

vSmart policy is applied on a per-site-list basis, so:

•When applying policy to a site-list, you can apply only one of each type of policy. For example, you can have one control-policy and one data-policy, or one control-policy in and one control-policy out. You cannot have two data policies or two outbound control policies.

•Because a site-list is a grouping of many sites, you should be careful about including a site in more than one site-list, and in general, we recommend that you not do this at all. You should take special care when a site-list includes a range of site identifiers, to ensure that there is no overlap. If the same site is part of two site-lists and the same type of policy is applied to both site-lists, the policy behavior will be unpredictable and possibly catastrophic.

Control-policy is unidirectional, being applied either inbound to the vSmart controller or outbound from it. When control-policy is needed in both directions, configure two control policies.

Data-policy is directional and can be applied either to traffic received from the service side of the vEdge router, traffic received from tunnel side, or both. VPN membership policy is always applied to traffic outbound from the vSmart controller.

Control-policy remains on the vSmart controller and affects routes that the controller sends and receives.
Data-policy is sent to vEdge routers in the site-lite. The policy is sent in OMP updates, and it affects the data traffic that the routers send and receive.
When any node in the overlay network makes a routing decision, it uses any and all available routing information. In the overlay network, it is the vSmart controller that distributes routing information to the vEdge nodes.

vSmart policy Examples & Lab

All the policies we discuss here are vSmart policies, also called centralized policies, which are policies that are configured on the vSmart controller.

We discuss the following applications of the vSmart policy framework:

- **Application-aware routing policy** looks at the network and path characteristics of the data plane connections between vEdge routers, compares them to configured SLA parameters, and computes optimal paths for data traffic.

- **Control policy** uses OMP vRoute and TLOC information to enable services and engineer specialized routing applications.
- **Data policy**
- **VPN membership policy**

Advanced features **of Viptela policy**

Advanced features of Viptela policy software offer specialized policy-based network applications. Examples of these applications include the following:

- **Service chaining**, which redirects data traffic to shared devices in the network, such as firewall, intrusion detection and prevention (IDS), load balancer, and other devices, before the traffic is delivered to its destination. Service chaining obviates the need to have a separate device at each branch site.

- **Cflowd**, for monitoring traffic flow.

- **Converting a vEdge router into a NAT device**, to allow traffic destined for the Internet or other public network can exit directly from the vEdge router.

Application-Aware Routing Policies

Application-Aware Routing Policies

Application-aware routing is created in three portions of the configuration:
•Configure the **sla-class**, which defines the required **latency and loss** for the traffic that is to be affected by a given app-route-policy.

•Configure the **app-route-policy**, which specifies the traffic that is to belong to an sla-class. (This is done in a fashion similar to a data-policy.) The app-route-policy references a vpn-list to dictate which VPNs at the listed sites benefit from the policy.

•Apply the app-route-policy towards the desired overlay network sites.

```
apply-policy
 site-list site1
  app-route-policy app_route
 !
!
```

```
policy
 sla-class EF
  loss 2
  latency 100
!
app-route-policy app_route
 vpn-list app_vpn
  sequence 10
   match dscp 46
!
action
  sla-class EF
  !
 !
!
```

```
lists
  site-list site 100
    site-id 100
!
vpn-list app_vpn
  vpn 1
 !
!
```

sla-class defines the required performance metrics for the application.
Here, the sla-class is named EF. For the performance metrics, the maximum acceptable packet loss is 2 percent and the maximum acceptable packet latency is 100 milliseconds. If the latency is greater than 100 milliseconds or if the packet loss is greater than 2 percent, that tunnel is not considered as a valid data path.

vpn-list defines the VPNs where the policy is applied to at the target sites. You create the vpn-list in the lists section, and you apply it in the definition of the app-route-policy itself.
app-route-policy defines the actual application route policy. In the policy definition, you link the matched traffic (in the match portion of the policy) with the required sla-class, which is called in the action portion of the policy.

Cflowd Flow Data Collection

Cflowd monitors traffic flowing through vEdge routers in the overlay network and exports flow information to a collector, where it can be processed by an IPFIX analyzer.
Cflowd flow collection is enabled by means of a vSmart policy, specifically, by a vSmart data policy. The parameters for capturing and exporting flow data are defined in two sections of the policy:

- **A cflowd-template** configures the flow cache behavior and flow export. For the flow cache, the cflowd-template defines how often the sampled flows should be sent to a collection. For the flow export, the cflowd-template specifies the location of the flow collection.

- **A data-policy selects the** traffic subject to flow data collection. The data-policy can be configured to be very specific or as a general flow collection filter, depending on requirements.

```
apply-policy
 site-list site100
  data-policy cflowd_data all
  cflowd-template cflowd_temp
 !
!
```

```
policy
 data-policy cflowd_data
  vpn-list cflowd_vpn
   sequence 10
    match
     protocol 17
    !
    action accept
     cflowd
    !
   !
   default-action drop
  !
 !
```

data-policy (in the purple policy section of the configuration) defines the actual traffic subject to flow data collection. Here, data-policy cflowd_data matches all UDP traffic (protocol 17) and applies flow monitoring to it. The default-action is drop, so all non-UDP data traffic is dropped.

data-policy (in the green apply-policy section) applies data-policy cflowd_data to the vEdge routers at sites that are part of the site-list named site100. The **all** option applies the policy to data traffic entering and leaving the vEdge routers.

cflowd-template (in the brown policy section) creates a template to manage cache management and flow export settings. Here, we define the template called cflowd_temp that gives the location flow collector location (in VPN 100, at address 1.1.1.1 and port 4739) and exports flow information every 60 seconds for both active and inactive flows.

```
cflowd-template cflowd_temp
 flow-active-timeout   60
 flow-inactive-timeout 60
 collector vpn 100 address 1.1.1.1 port 4739 transport transport_udp
!
!
```

cflowd-template (in the green apply-policy section) applies the cflowd template to the vEdge routers in site-list site100. The cflowd-template and data-policy are applied at the same time

Control Policy Applications and Services

- vSmart **control policies** are put in place to **influence routing** in the overlay domain. Using OMP routing information, these policies can enable services and engineer specialized routing applications. Control policy is a powerful tool for any type of path management. Having it be centralized and managed on vSmart controllers greatly simplifies policy operations throughout the network.
- Types of vSmart control policies:

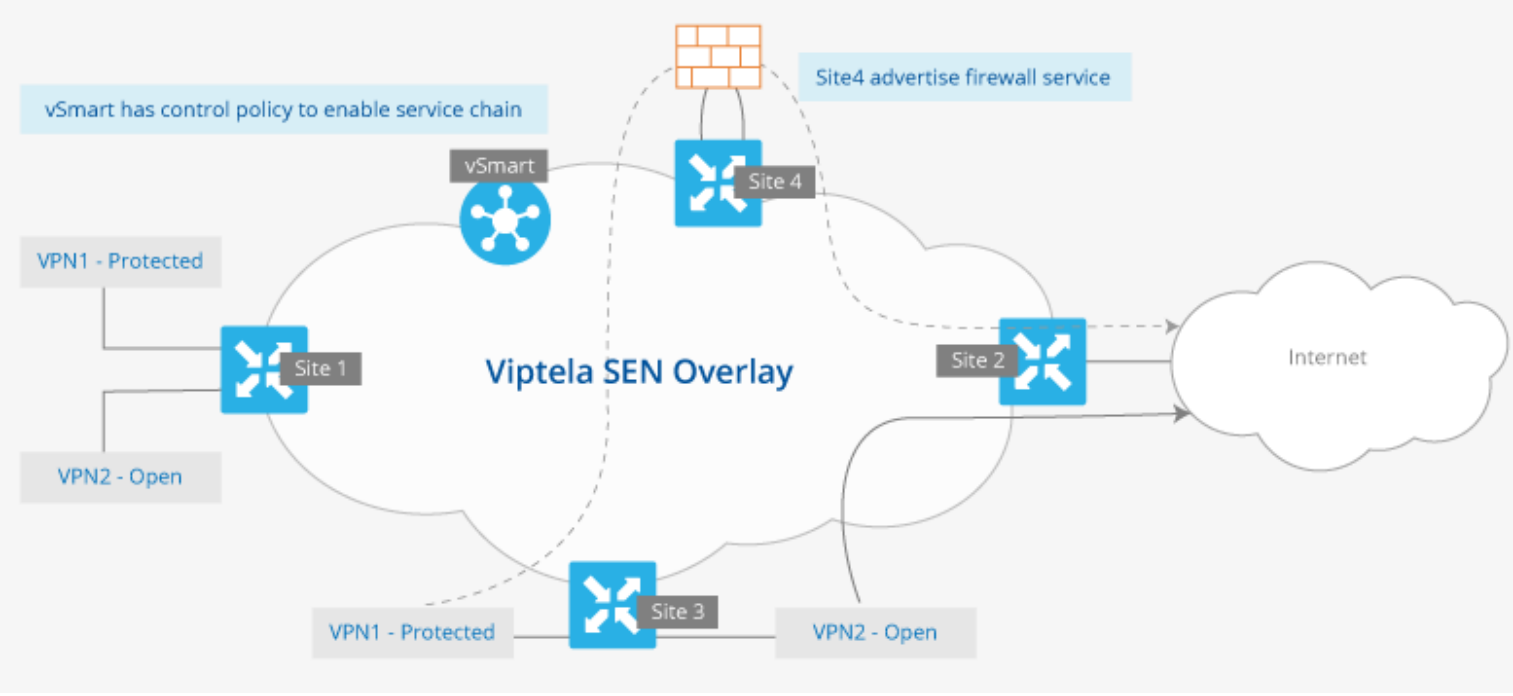
- Service chaining
- Traffic engineering
- Extranet VPNs
- Service and path affinity
- Arbitrary VPN topologies

Service Chaining with Control Policy

When security devices and resources are located at one site in the network and routers and hosts dispersed throughout the network need to access these resources, you can use vSmart policies to redirect data traffic to those resources before it is forwarded towards its final destination. In the Viptela policy framework, this process is called ***service chaining***, because an intermediate destination at which a service is located is being attached, or *chained*, to a route. These centralized security devices and resources are called ***services***.

vSmart policy that implement service chaining selectively directs traffic to standard services—firewalls, Intrusion Detection Systems (IDSs), and Identity Providers (IDPs)—or to custom services that you define.

Use case:


vSmart has control policy to enable service chain
Site4 advertise firewall service
vSmart
Site 4
VPN1 - Protected
Site 1
Viptela SEN Overlay
Site 2
Internet
VPN2 - Open
Site 3
VPN1 - Protected
VPN2 - Open

```
vpn 1
 service FW address 1.1.1.1
```

```
policy
 lists
  vpn-list closed_vpn
   vpn 1
  !
  site-list branch_sites
   site-id site1, site3
  !
  site-list site2
   site-id site2
 !
!
```

```
control-policy service-chain
  sequence 10
   match route
    origin bgp-external
    vpn-list closed_vpn
   !
   action accept
    set
     service FW
    !
   !
  !
  default-action accept
 !
!
```

The vSmart control policies have these components:

In **vpn-list**, the list called **closed_vpn** contains VPN 1, the protected VPN. We need this list for the match condition in control-policy **service-chain**. If we decide later that traffic from other VPNs needs firewall protection, we can simply add these VPNs to the closed_vpn VPN list.
In site-list, we create the lists used in the apply-policy commands.

The site-list branch_sites holds the two sites in VPN 1, and site-list site2 contains the site that connects to the Internet.

control-policy **service-chain** defines the target routes for which the firewall service is needed. These routes are external BGP prefixes in VPN 1. A default-action of accept means that nonmatching prefixes, such as those in other VPNs, pass through the policy unchanged.

```
control-policy service-chain-return
 sequence 10
  match route
   site-list branch_sites
  !
  action accept
   set
    service FW
   !
  !
 !
 default-action accept
!
!
```

```
apply-policy
 site-list branch_sites
  control-policy service-chain out
 !
 site-list site2
  control-policy service-chain-return out
 !
```

control-policy service-chain-return defines the target routes for the firewall service in the return path. These are the prefixes in Sites 1 and 3 that are in VPN 1.
Again, the default-action accept means that nonmatching prefixes pass through the policy unchanged.

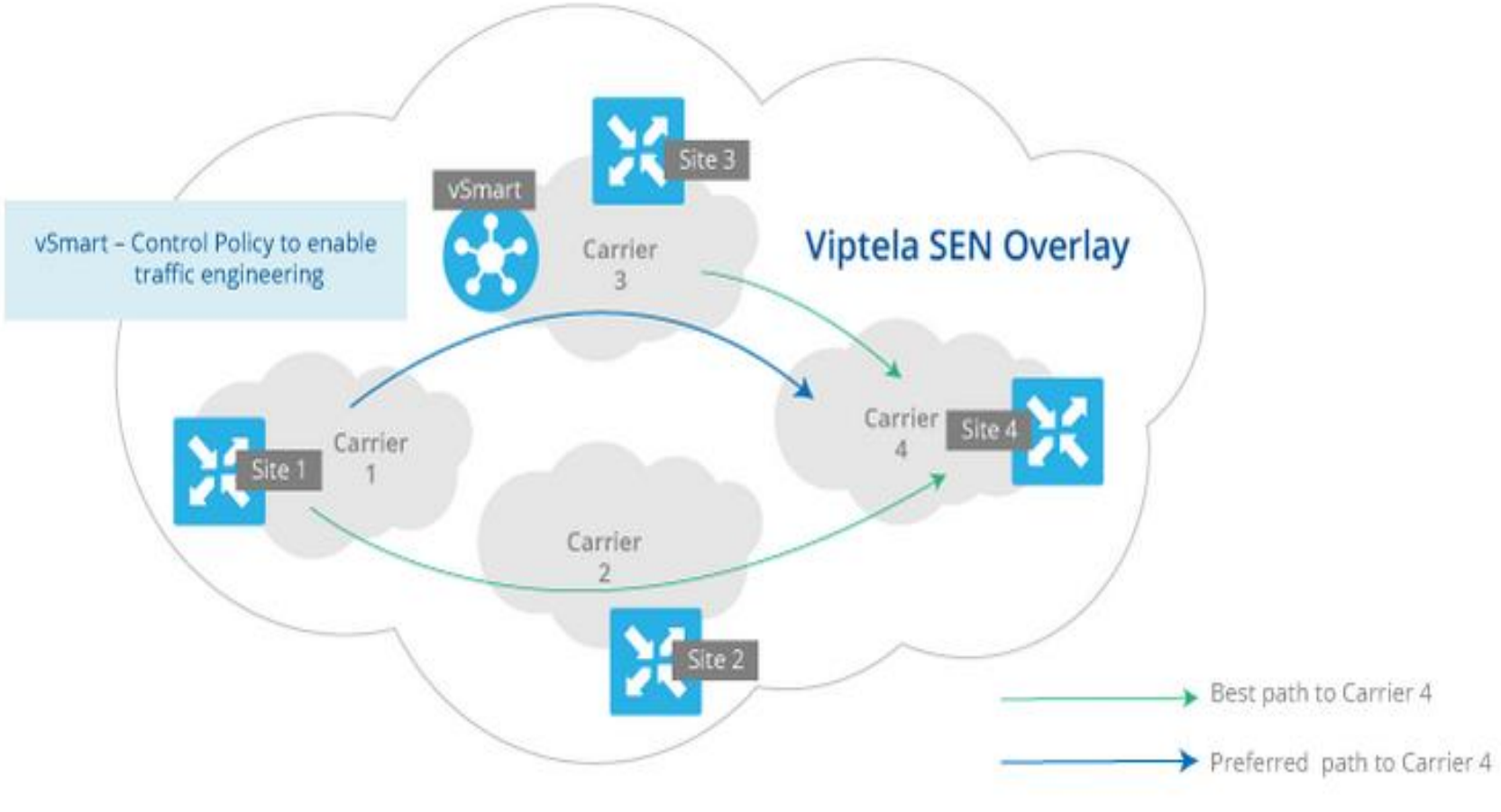
apply-policy site-list branch_sites applies the control-policy service-chain for the upstream firewall service to Sites 1 and 3. This control-policy has the following effect on outbound traffic towards the Internet:

- For traffic originating from VPN 1 at Sites 1 and 3, the next hop for outgoing BGP prefixes is changed to point to the location where the firewall service is hosted.
- The firewall receives the traffic from its directly connected vEdge router, processes it, and then follows its route table, which points back to the connected vEdge router. It is very likely that the firewall device simply has a default route and nothing more in its route table.

Traffic Engineering

- Traffic engineering is a mechanism for controlling traffic flow through links in the network, optimizing the path to suit the needs of the network. MPLS is one way to integrate traffic engineering into Layer 3 applications, such as routing IP traffic. In the Viptela network, you can use vSmart policy directly to traffic-engineer paths through the overlay network.

- In the example illustrated below, even though the best path from Carrier 1 to Carrier 4 is through Carrier 2, we instead want traffic to go via Carrier 3.


vSmart – Control Policy to enable traffic engineering
vSmart
Site 3
Carrier 3
Viptela SEN Overlay
Site 1
Carrier 1
Carrier 4
Site 4
Carrier 2
Site 2
Best path to Carrier 4
Preferred path to Carrier 4

Prefer Data Center DC1 and DC2 for Different Set of Branches for Regional Internet Exit

```
!
policy
 lists
  site-list Branch1
   site-id 300
  !
  site-list Branch2
   site-id 400
  !
  site-list DC1
   site-id 100
  !
  site-list DC2
   site-id 200
  !
 !
```

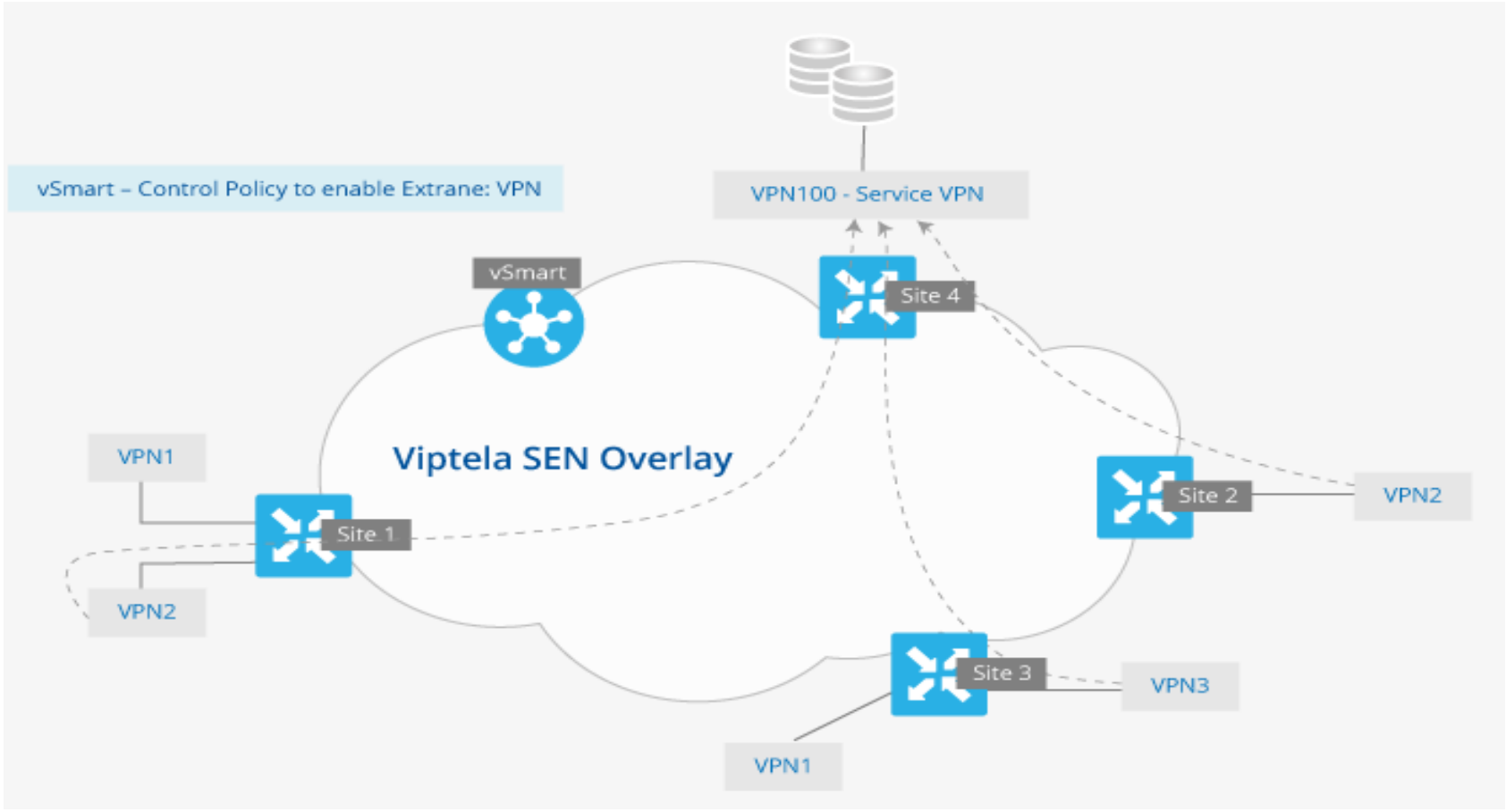
```
!
 control-policy PreferDC1
  sequence 1
   match route
    site-list DC1
   !
   action accept
    set
     preference 100
    !
   !
  !
  default-action accept
 !
```

```
!
 control-policy PreferDC2
  sequence 1
   match route
    site-list DC2
   !
   action accept
    set
     preference 100
    !
   !
  !
  default-action accept
 !
!
```

```
!
apply-policy
 site-list Branch1
  control-policy PreferDC1 out
 !
 site-list Branch2
  control-policy PreferDC2 out
 !
!
```

Extranet VPNs

- When services that reside in a VPN must be shared across users residing in multiple other VPNs (see illustration below), you can create a vSmart extranet VPN control policy.
- This policy advertises the prefixes in the service VPNs to the other (client) VPNs, and it advertises the client prefixes to the service VPN, so that the vEdge routers connected to these VPNs have reachability information for each other.


vSmart – Control Policy to enable Extrane: VPN
VPN100 - Service VPN
vSmart
Site 4
Viptela SEN Overlay
VPN1
Site 1
VPN2
Site 2
VPN2
Site 3
VPN3
VPN1

```
vpn 2
interface loopback2
 ip address 4.4.4.1/32
 no shutdown
 !
 interface loopback3
 ip address 4.5.4.1/24
 no shutdown
 !
 vpn 3
 interface loopback4
 ip address 5.5.5.1/32
 no shutdown
 !
 interface loopback5
 ip address 5.4.5.1/24
 no shutdown
 !
```

```
policy
lists
vpn-list client-vpn2
vpn 2
!
vpn-list service-vpn3
vpn 3
!
site-list DC
site-id 100
!
!
```

Extranet Policy Example

```
!
control-policy extranet
sequence 60
match route
vpn-list client-vpn2
!
action accept
export-to
vpn-list service-vpn3
sequence 70
match route
vpn-list service-vpn3
!
action accept
export-to
vpn-list client-vpn2
!
default-action accept
!
```

```
!
apply-policy
site-list DC
control-policy extranet in
!
```

Data Policy

- vSmart data policy is a powerful tool for any type of data plane–centered traffic management. Because it is centralized and managed on a vSmart controller data policy greatly simplifies policy operations. Data policies are used to enable a number of services, including:
- **Service chaining**
- **Cflowd traffic monitoring**
- **Traffic policing and counting**
- A data policy acts on an entire VPN and is not interface-specific.

- Some of the policy applications that can be enabled with control policies can also be enabled with data policies (and also with traditional routing policy). Enabling applications with data policies instead of control policies can be simpler to administer, because the policies apply only to a single node and they do not interact across the overlay network.

Service chaining

```
vpn 1
 service FW address 1.1.1.1
```

```
policy
 lists
  vpn-list closed_vpn
   vpn 1
  !
  site-list branch_sites
  site-id site1
  site-id site3
  !
 !
!
```

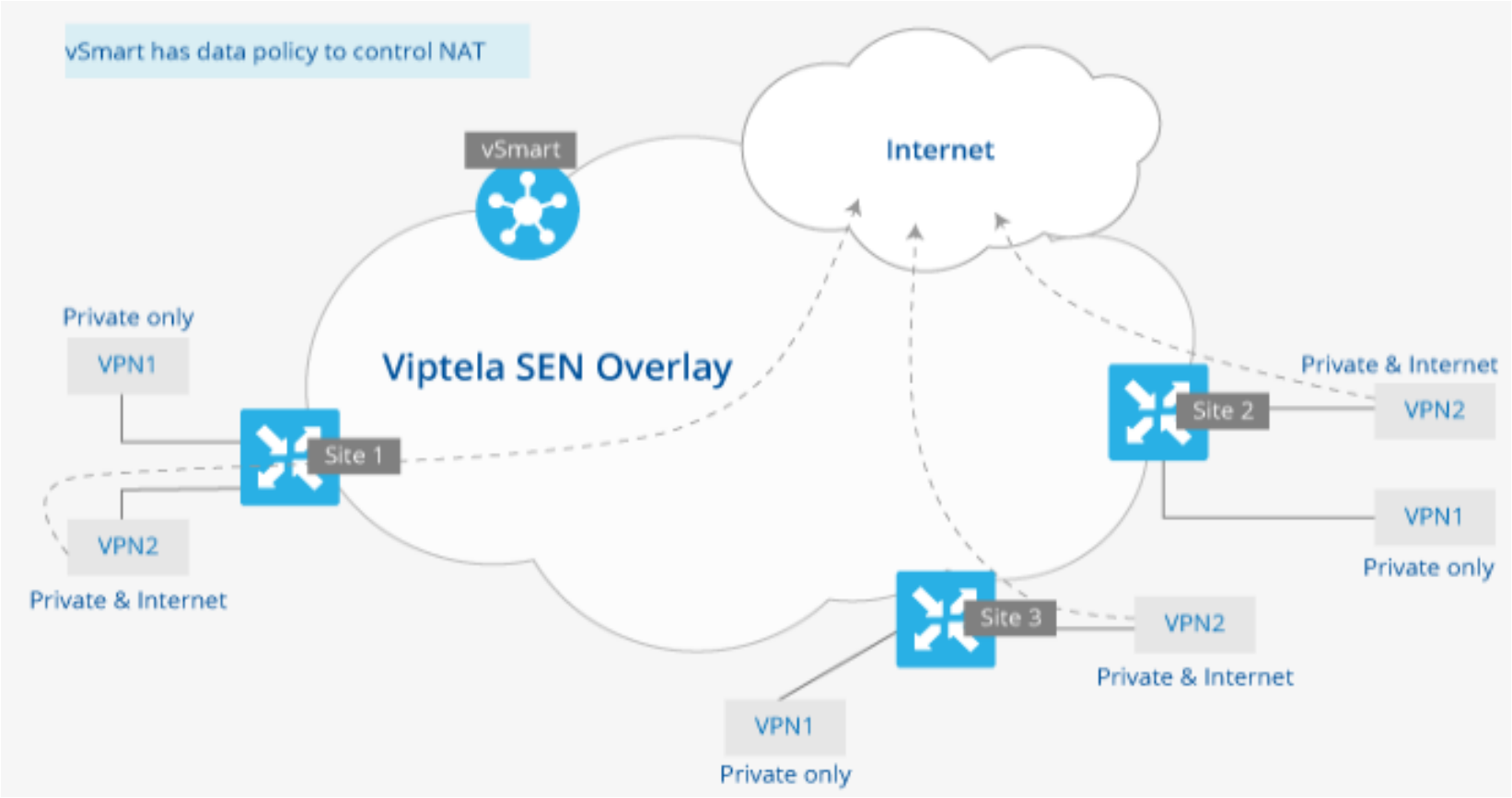
```
policy
 data-policy service-chain
  vpn-list closed_vpn
   sequence 10
    match
     dscp     10
    !
    action accept
     set
      service FW
     !
    !
   !
   default-action accept
  !
 !
```

```
apply-policy
 site-list branch_sites
  data-policy service-chain all
 !
!
```

Using a NAT for Local Internet Exit

- Rather than have a single exit point from the overlay network to the Internet, vSmart data-policy can provide local Internet exit from vEdge routers. You implement this using a data-policy that includes a NAT directive. The data-policy is configured on the vSmart controller, so local Internet exit is managed centrally.

- The figure below illustrates a topology that provides local Internet exit to departments that are part of VPN 2. The users in these departments are located at all three of the sites in the overlay network.


vSmart has data policy to control NAT
vSmart
Internet
Viptela SEN Overlay
Private only
VPN1
Site 1
VPN2
Private & Internet
Private & Internet
Site 2
VPN2
VPN1
Private only
Site 3
VPN2
Private & Internet
VPN1
Private only

Here are the configuration components that set up the NAT function on the vEdge routers so that traffic passing destined for the Internet can travel directly from the vEdge router to the Internet, without having to go to a centralized or other site before exiting to the Internet:

data-prefix-list identifies the source IP prefixes whose traffic is destined for the NAT, and hence for the Internet

vpn-list identifies the affected VPNs.

site-list groups together the three sites that participate in VPN 1.

data-policy in the **policy** section directs matching traffic towards the NAT, and hence towards the Internet.

data-policy in the **apply-policy** section is applied in the from-service direction to match incoming traffic from the service side to the vEdge router.

```
policy
 lists
  data-prefix-list internet_bound
   ip-prefix 1.1.1.0/24
   ip-prefix 2.2.2.0/24
  !
  vpn-list Internet_vpn
   vpn 2
  !
  site-list branch_sites
   site-id site1
   site-id site2
   site-id site3
  !
 !
!
```

```
policy
 data-policy internet_nat
  vpn-list Internet_vpn
   sequence 10
    match
     source-data-prefix-list internet_bound
    !
    action accept
     nat use-vpn 0
    !
   !
   default-action accept
  !
 !
```

```
apply-policy
 site-list branch_sites
  data-policy internet_nat from-service
 !
!
```

4.4 Configure and verify SD-WAN application-aware routing

4.5 Configure and verify direct Internet access

ABC of Cisco SDWAN Viptela App-aware Routing

Let us talk about Data Policies

- **Centralized data policy.** You configure this policy on the vSmart controller, and the policy is passed to the vEdge router. You define the configuration with the **policy data-policy configuration** command, and you apply it with the **apply-policy site-list data-policy** or **apply-policy site-list vpn-membership** command.

- **Localized data policy**, which is commonly called access lists. You configure access lists on the vEdge router with the **policy access-list** configuration command. You apply them, within a VPN, to an incoming interface with the **vpn interface access-list in** configuration command or to an outgoing interface with the **vpn interface access-list out** command.

Application-aware routing policy. Application-aware routing policy affects only traffic that is flowing from the service side (the local/LAN side) to the tunnel (WAN) side of the vEdge router.

You configure application-aware routing policy on the vSmart controller with the **policy app-route-policy** configuration command, and you apply it with the **apply-policy site-list app-route-policy** command.

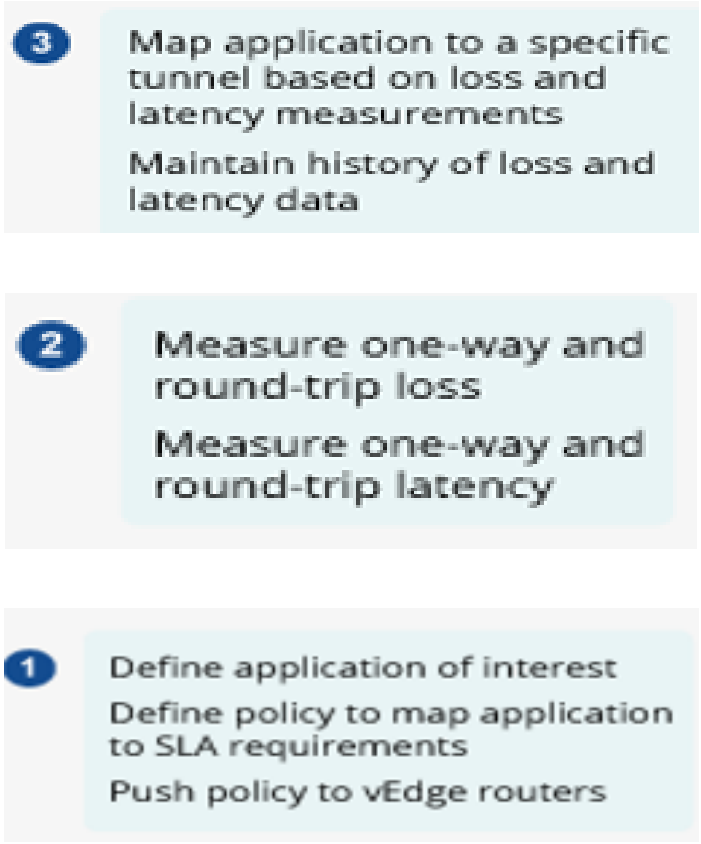
When you commit the configuration, the policy is passed to the appropriate vEdge routers. Then, matching data traffic on the vEdge routers is processed in accordance with the configured SLA conditions

Application-aware routing tracks network and path characteristics of the data plane tunnels between vEdge routers and uses the collected information to compute optimal paths for data traffic. These characteristics include packet loss, latency, and jitter, and the load, cost and bandwidth of a link

offers a number of advantages to an enterprise:

- In normal network operation, the path taken by application data traffic through the **network can be optimized**, by directing it to WAN links that support the required levels of packet loss, latency, and jitter defined in an application's SLA.

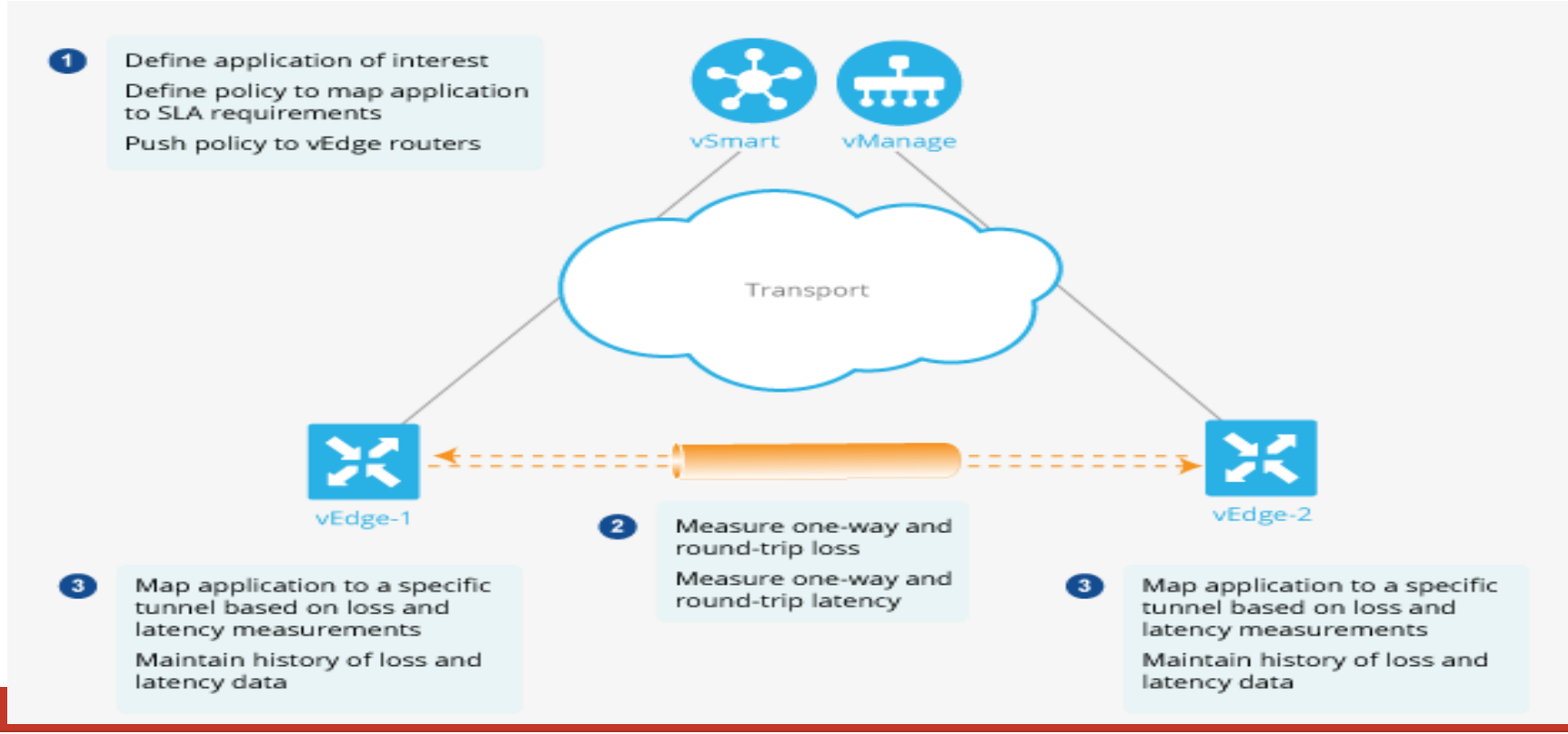
- In the face of network soft failures, **performance degradation can be minimized.**
- **Network costs can be reduced** because data traffic can be more efficiently load-balanced.
- **Application performance can be increased** without the need for WAN upgrades.



Components of Application-Aware Routing

- Each vEdge router supports up to four TLOCs, allowing a single vEdge router to connect to up to four different WAN networks.
- This capability allows path customization for application traffic that has different needs in terms of packet loss and latency.

The Viptela Application-Aware Routing solution consists of three elements:



Classification of Tunnels into SLA Classes

- **Measure Loss, Latency, and Jitter**
- When a data plane tunnel in the overlay network is established, a BFD session automatically starts on the tunnel. In the overlay network, each tunnel is identified with a color that identifies a specific link between a local TLOC and a remote TLOC.

- By default, the BFD Hello packet interval is 1 second. This interval is user-configurable (with the **bfd color interval** command). Note that the BFD Hello packet interval is configurable per tunnel.

Calculate Average Loss, Latency, and Jitter

- BFD periodically polls all the tunnels on the vEdge router to collect packet latency, loss, jitter, and other statistics for use by application-aware routing. At each poll interval, application-aware routing calculates the average loss, latency, and jitter for each tunnel, and then calculates or recalculates each tunnel's SLA. Each poll interval is also called a "**bucket**.“

- By default, the poll interval is 10 minutes. With the default BFD Hello packet interval at 1 second, this means that information from about 600 BFD Hello packets is used in one poll interval to calculate loss, latency, and jitter for the tunnel.
- The poll interval is user-configurable (with the **bfd app-route poll-interval** command). Note that the application-aware routing poll interval is configurable per vEdge router; that is, it applies to all tunnels originating on a router.

Classification of Tunnels into SLA Classes

- **Determine the SLA Classification**

- To determine the SLA classification of a tunnel, application-aware routing uses the loss, latency, and jitter information from the latest poll intervals. The number of poll intervals used is determined by a multiplier. By default, the multiplier is 6, so the information from all the poll intervals (specifically, from the last six poll intervals) is used to determine the classification.

- For the default poll interval of 10 minutes and the default multiplier of 6, the loss, latency, and jitter information collected over the last hour is considered when classifying the SLA of each tunnel.

These default values have to be chosen to provide damping of sorts, as a way to prevent frequent reclassification (flapping) of the tunnel.

The multiplier is user-configurable (with the **bfd app-route multiplier** command). Note that the application-aware routing multiplier is configurable per vEdge router; that is, it applies to all tunnels originating on a router.

Configure the Monitoring of Data Plane Tunnel Performance

- BFD sends Hello packets periodically to test the liveness of a data plane tunnel and to check for faults on the tunnel. These Hello packets provide a measurement of packet loss and packet latency on the tunnel. The vEdge router records the packet loss and latency statistics over a sliding window of time. BFD keeps track of the six most recent sliding windows of statistics, placing each set of statistics in a separate bucket.

Parameters	Default	Configuration Command	Range
BFD Hello packet interval	1 second	**bfd color** color **hello-interval** seconds	1 through 65535 seconds
Polling interval for application-aware routing	10 minutes (600,000 milliseconds)	**bfd app-route poll-interval** milliseconds	1 through 4,294,967 (2^{32} – 1) milliseconds
Multiplier for application-aware routing	6	**bfd app-route multiplier** number	1 through 6

Configure Application-Aware Routing Policy

An application-aware routing policy is a type of centralized data policy: you configure it on the vSmart controller, and the controller automatically pushes it to the affected vEdge routers.

When a data packet matches one of the match conditions, an SLA action is applied to the packet to determine the data plane tunnel to use to transmit the packet.

If a packet matches no parameters in any of the policy sequences, and if no default SLA class is configured, the packet is accepted and forwarded with no consideration of SLA. Because application-aware routing policy accepts nonmatching traffic by default, it is considered to be a positive policy.

Other types of policies in the Viptela software are negative policies, because by default they drop nonmatching traffic.

Create and apply an application-aware routing policy

Component	Description	Configuration Command
Lists	Groupings of related items that you reference in the match and action portions of the data policy configuration. For application-aware routing policy, you can group IP prefixes, sites, and VPNs.	**policy lists**
SLA class	Required performance metrics for the application.	**policy sla-class**
Application-aware routing policy instance	Container for an application-aware routing policy.	**policy app-route-policy**
Numbered sequences of match–action pairs	Sequences that establish the order in which the policy components are applied.	**policy app-route-policy vpn-list sequence**

Create and apply an application-aware routing policy

Component	Description	Configuration Command
Match parameters	Conditions that packets must match to be considered for an application-aware routing policy.	**policy app-route-policy vpn-list sequence match**
Actions	SLA class to apply to matching data packets.	**policy app-route-policy vpn-list sequence action**
Default action	Action to take if a data packet matches none of the application-aware routing policy conditions.	**policy app-route-policy vpn-list default-action**
Application of application-aware routing policy	Apply an application-aware routing policy to overlay network sites.	**apply-policy site-list app-route-policy**

```
    app-list list-name
      (app application-name | app-family application-family)
    prefix-list list-name
      ip-prefix prefix
    site-list list-name
      site-id site-id
    vpn-list list-name
      vpn-id vpn-id
 sla-class sla-class-name
   jitter milliseconds
   latency milliseconds
   loss percentage
 app-route-policy policy-name
   vpn-list list-name
     sequence number
       match
         match-parameters
       action
         count
         log
         sla-class sla-class-name [preferred-color color] [strict]
     default-action
       sla-class sla-class-name
apply-policy site-list list-name
```

Structural Components of Policy Configuration for Application-Aware Routing

Application-aware routing policy lists

List Type	Description	Command
Application list	List of one or more applications or application families running on the subnets connected to the vEdge router. Each **app-list** can contain either applications or application families, but you cannot mix the two. • **application-name** is the name of an application. The Viptela software supports about 2300 different applications. To list the supported applications, use the ? in the CLI. • **application-family** is one of the following: **antivirus, application-service, audio_video, authentication, behavioral, compression, database, encrypted, erp, file-server, file-transfer, forum, game, instant-messaging, mail, microsoft-office, middleware, network-management, network-service, peer-to-peer, printer, routing, security-service, standard, telephony, terminal, thin-client, tunneling, wap, web, and webmail.**	**app-list** list-name (**app** application-name | **app-family** application-family)
Data prefix list	List of one or more IP prefixes.	**data-prefix-list** list-name **ip-prefix** prefix/length

Application-aware routing policy lists

List Type	Description	Command
Site list	List of one or more site identifiers in the overlay network. You can specify a single site identifier (such as **site-id 1**) or a range of site identifiers (such as **site-id 1-10**).	**site-list** *list-name* **site-id** *site-id*
VPN list	List of one or more VPNs in the overlay network. You can specify a single VPN identifier (such as **vpn-id 1**) or a range of VPN identifiers (such as **vpn-id 1-10**).	**vpn-list** *list-name* **vpn** *vpn-id*

SLA Classes

Description	Command	Value or Range
Maximum acceptable packet jitter on the data plane tunnel	**jitter** milliseconds	1 through 1000 milliseconds
Maximum acceptable packet latency on the data plane tunnel.	**latency** milliseconds	1 through 1000 milliseconds
Maximum acceptable packet loss on the data plane tunnel.	**loss** percentage	0 through 100 percent

- The action taken in application-aware routing is applied based on what is called an SLA (a service-level agreement). An SLA class is defined by the maximum jitter, maximum latency, maximum packet loss, or a combination of these values, for the vEdge router's data plane tunnels. (Each tunnel is defined by a local TLOC–remote TLOC pair.) You configure SLA classes under the **policy sla-class** command hierarchy on vSmart controllers.

Description	Command	Value or Range
Match all packets	Omit **match** command	—
Applications or application families	**app-list** list-name	Name of an **app-list** list
Group of destination prefixes	**destination-data-prefix-list** list-name	Name of a **data-prefix-list** list
Individual destination prefix	**destination-ip** prefix/length	IP prefix and prefix length
Destination port number	**destination-port** number	0 through 65535. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

Match Parameters

- Application-aware routing policy can match IP prefixes and fields in the IP headers. You configure the match parameters with the **match** command under the **policy app-route-policy vpn-list sequence** command hierarchy on vSmart controllers. You can match these parameters:

Match Parameters

Description	Command	Value or Range
DSCP value	**dscp** number	0 through 63
Internet Protocol number	**protocol** number	0 through 255
Group of source prefixes	**source-data-prefix-list** list-name	Name of a **data-prefix-list** list
Individual source prefix	**source-ip** prefix/length	IP prefix and prefix length
Source port number	**source-port** number	0 through 65535; enter a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])

Action Parameters

DESCRIPTION	COMMAND	VALUE OR RANGE
Count matching data packets.	**action count**	—
Place a sampled set of packets that match the SLA class rule into the messages and vsyslog system logging (syslog) files.	**action log**	To display logging information, use the **show app log flow-all**, **show app log flows**, and **show log** commands on the vEdge router.
SLA class to match. All matching data traffic is directed to the tunnel whose performance matches the SLA parameters defined in the class.	**action sla-class** *sla-class-name*	SLA class name defined in **policy sla-class** command

- When data traffic matches the match parameters, the specified action is applied to it. For application-aware routing policy, the action is to apply SLA class. The SLA class defines the maximum packet latency or maximum packet loss, or both, that the application allows on the data plane tunnel used to transmit its data.

Description	Command	Value or Range
Data plane tunnel color to prefer when an SLA class match occurs. If no tunnel of the preferred color is available, traffic is forwarded using another tunnel that matches the SLA class. That is, color preference is a loose matching, not a strict matching.	**action sla-class** *sla-class-name* **preferred-color** *color*	SLA class name defined in **policy sla-class** command and one of the supported tunnel colors.
Strict matching of SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. Note that for policy configured with this option, data traffic that matches the match conditions is dropped until the application-aware routing path is established.	**action sla-class** *sla-class-name* **strict**	SLA class name defined in **policy sla-class** command

Action Parameters

- If more than one data plane tunnel satisfies an SLA class criteria, the vEdge router selects one of them by performing load-balancing across the equal paths.

Applying Application-Aware Routing Policy

- For an application-aware route policy to take effect, you apply it to a list of sites in the overlay network:
- vSmart(config)# **apply-policy** **site-list** *list-name*
- **app-route-policy** *policy-name*
- When you apply the policy, you do not specify a direction (either inbound or outbound). Application-aware routing policy **affects only the outbound traffic on the vEdge routers**.

- To view the policy configured on the vSmart controller,
- **show running-config Policy**
- To view the policy that the vSmart controller has pushed to the vEdge router, issue the **show policy from-vsmart** command on the router.
- To display flow information for the application-aware applications running on the vEdge router, issue the **show app dpi flows** command on the router.

Application-Aware Routing Policy Configuration Example

- !
- Some of the applications have already had SLAs defined and are pinned
- to the MPLS (interface ge0/0 on BR2-VEDGE1). Some applications have been pinned to the internet transport (interface ge0/1 on BR2-VEDGE1). The policy is applied to ALL sites, so the policy has impact on all the traffic received and sent by BR2-VEDGE1. More traffic is received than sent by the BR2-VEDGE1.

- Look at the traffic received by BR2-VEDGE1 on mpls interface (ge0/0) and internet interface (ge0/1). You would observe traffic received switch from mpls interface to internet interface after the latency impairment on MPLS transport.
- !

Application-Aware Routing Policy Configuration Example

```
policy
 sla-class WebSLA
  latency 100
 !
 sla-class voicevideo
  latency 50
 !
 app-route-policy _myvpns_AppRoutePolicy
  vpn-list myvpns
   sequence 1
    match
     app-list SIPApp
    !
    action
     log
     backup-sla-preferred-color biz-internet
     sla-class voicevideo preferred-color mpls
    !
```

```
sequence 11
   match
    app-list HTTPS
   !
   action
    log
    backup-sla-preferred-color biz-internet
    sla-class WebSLA preferred-color biz-internet
   !
  !
sequence 21
   action
    backup-sla-preferred-color biz-internet
    sla-class voicevideo preferred-color mpls
   !
 !
lists
 vpn-list myvpns
  vpn 10
 !
```

```
app-list HTTPS
  app-family web
  app-family webmail
 !
 app-list SIPApp
  app-family audio_video
 !
 site-list AllBranches
  site-id 300-400
 !
 site-list AllDC
  site-id 100-200
 !
!
apply-policy
 site-list AllBranches
  app-route-policy _myvpns_AppRoutePolicy
 !
 site-list AllDC
  app-route-policy _myvpns_AppRoutePolicy
 !
```

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

Terms and Acronyms

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

1 Document Overview

This Deployment Guide document will provide GUI examples for configuring Zscaler Internet Access (ZIA) and Cisco SD-WAN. All examples in this guide presumes the reader has a basic comprehension of IP Networking. All examples in this guide will explain how to provision new service with ZIA and with Cisco SD-WAN.

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

1. Document Audience

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

2. Software Revisions

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

3. Request for Comments

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

4. Document Prerequisites

Zscaler Internet Access (ZIA)

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

Using vManage (GUI)

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

Using CLI:

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

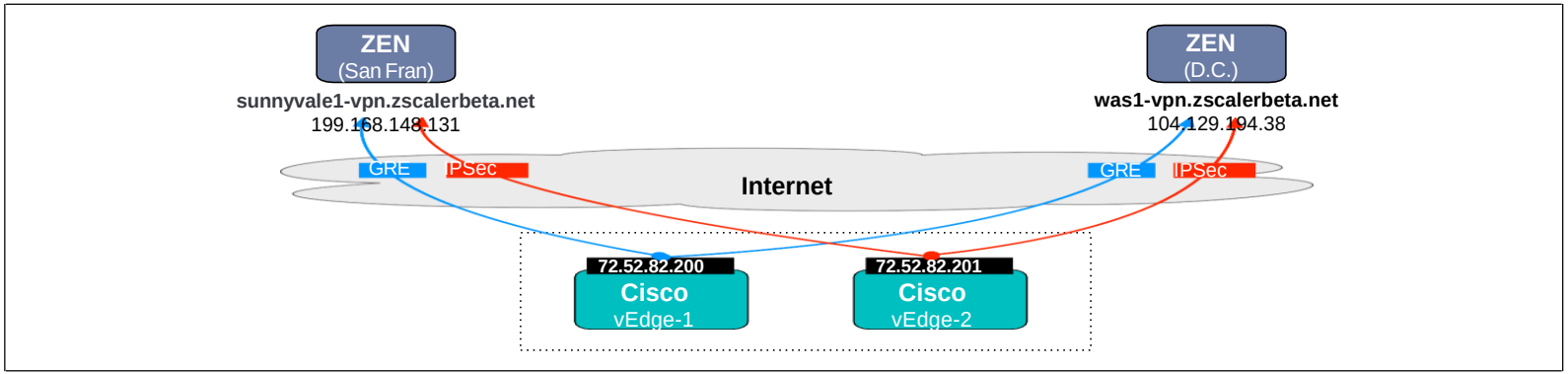
1.5 Document Revision Control

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

Lab Topology and Configuration Overview

1.6 Lab Topology and Configuration Overview

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



	Primary Tunnel	Secondary Tunnel
Tunnel Destination	199.168.148.131	104.129.194.38
Tunnel Source	72.52.82.200	72.52.82.201

Branch Office

Figure 1: ZIA GRE Configuration Details

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

Figure 2: ZIA GRE Configuration Details

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

2 Configuring Zscaler Internet Access (ZIA)

2.1 Logging into ZIA

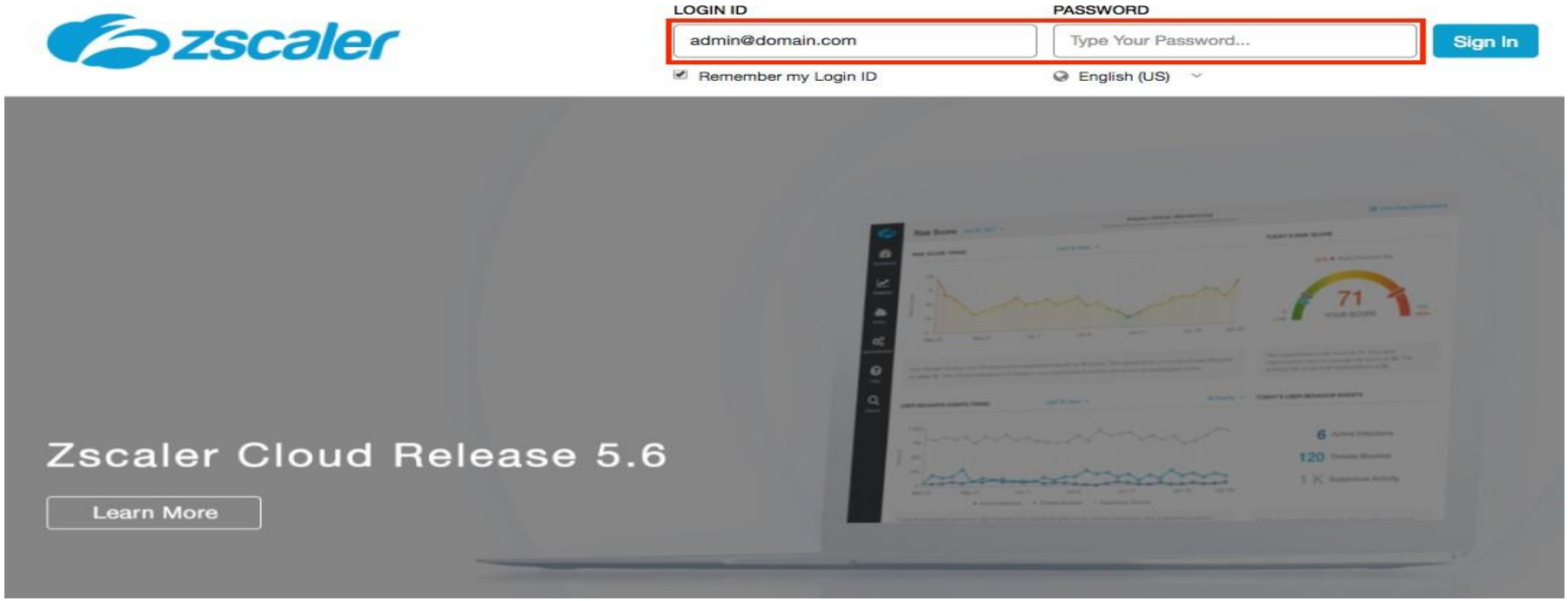


Figure 3: Log into Zscaler

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

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

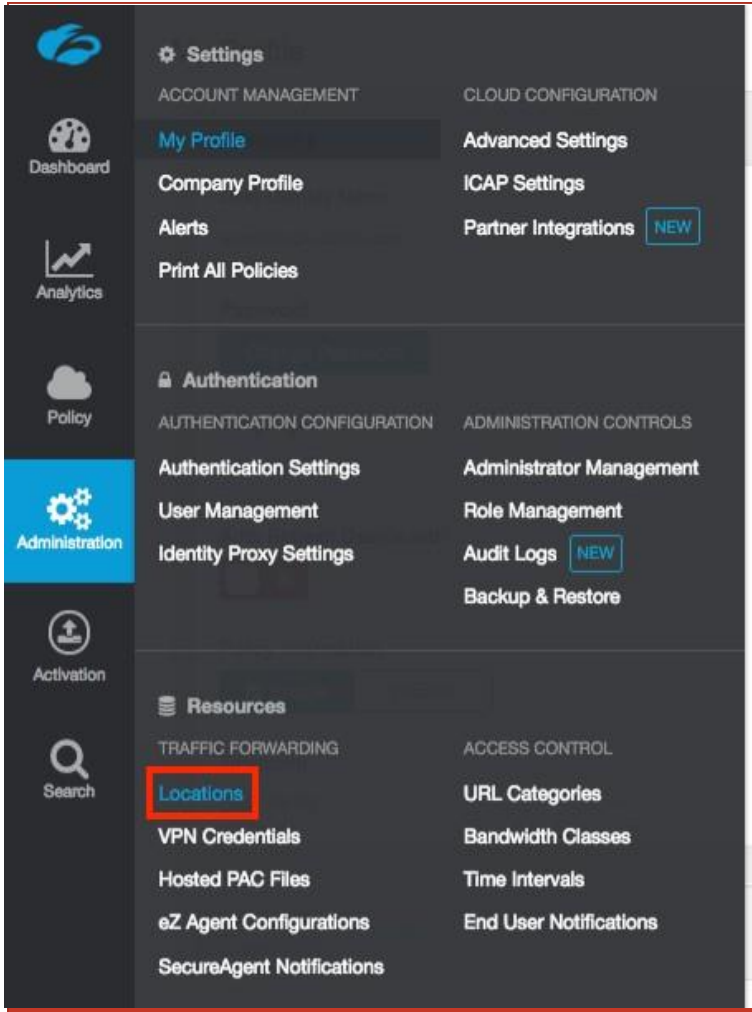
2.2 Configuring ZIA for GRE Tunnel

2.2.1 Navigate to Locations

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

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

Figure 4: Navigate to Locations


Dashboard
Analytics
Policy
Administration
Activation
Search
Settings
ACCOUNT MANAGEMENT
My Profile
Company Profile
Alerts
Print All Policies
CLOUD CONFIGURATION
Advanced Settings
ICAP Settings
Partner Integrations
NEW
Authentication
AUTHENTICATION CONFIGURATION
Authentication Settings
User Management
Identity Proxy Settings
ADMINISTRATION CONTROLS
Administrator Management
Role Management
Audit Logs
NEW
Backup & Restore
Resources
TRAFFIC FORWARDING
Locations
VPN Credentials
Hosted PAC Files
eZ Agent Configurations
SecureAgent Notifications
ACCESS CONTROL
URL Categories
Bandwidth Classes
Time Intervals
End User Notifications

2.2.2 Add a Location

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

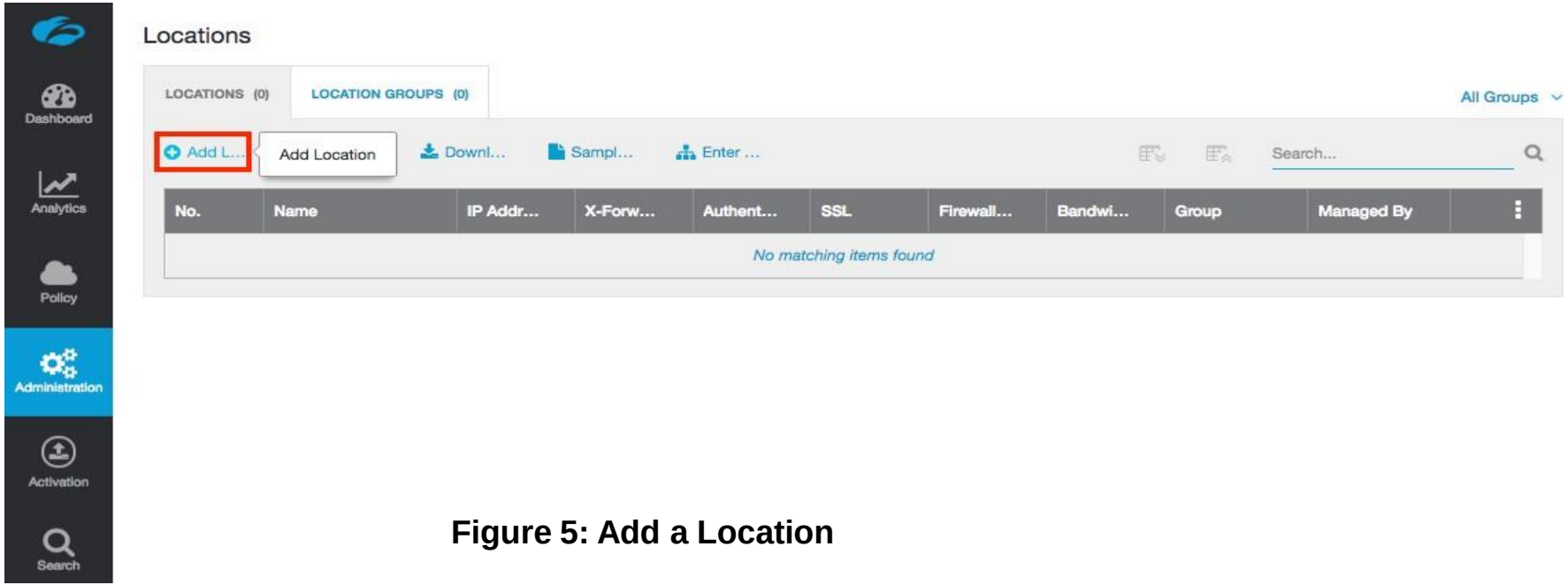


Figure 5: Add a Location

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

2.2.3 Enter Location Data

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

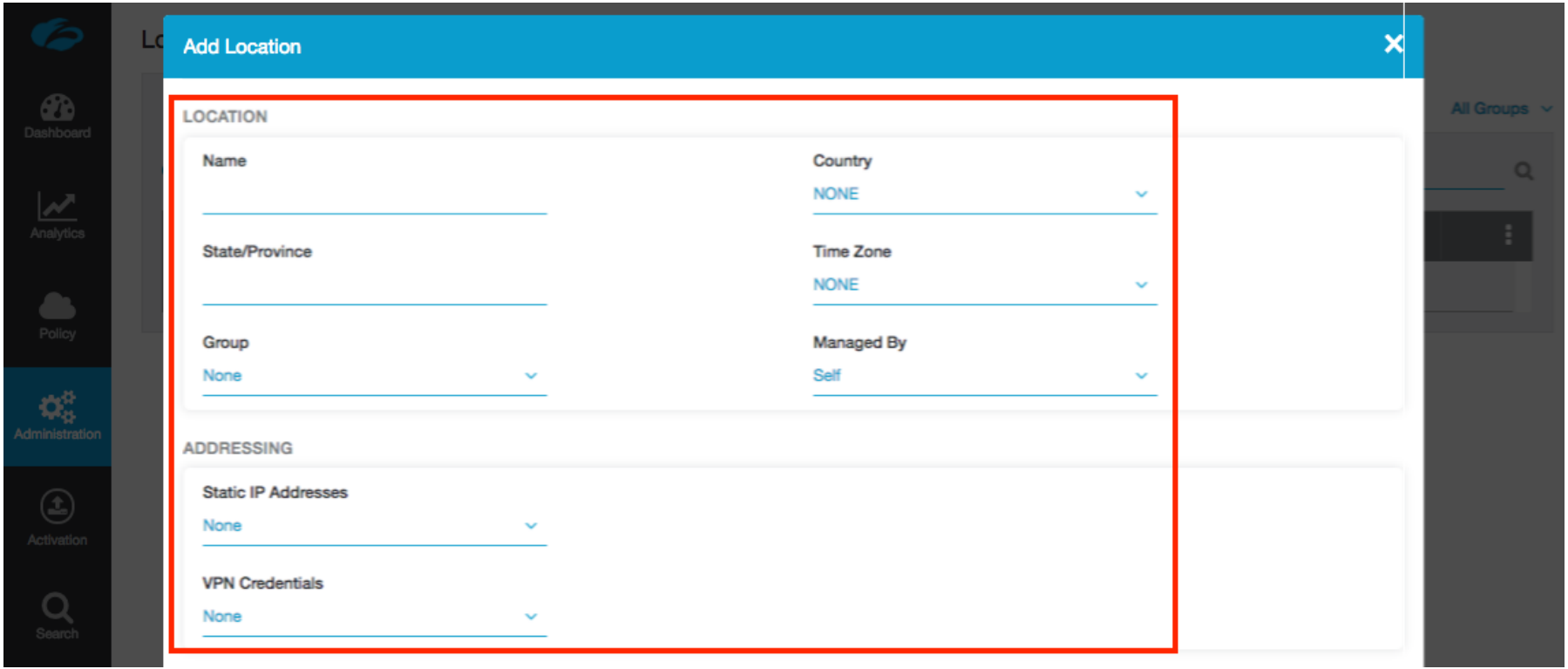


Figure 6: Enter Location Data

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

2.3 Configuring ZIA for IPsec Tunnel

2.3.1 Navigate to VPN Credentials

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

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

2.2.4 Verify Location Information and Save

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

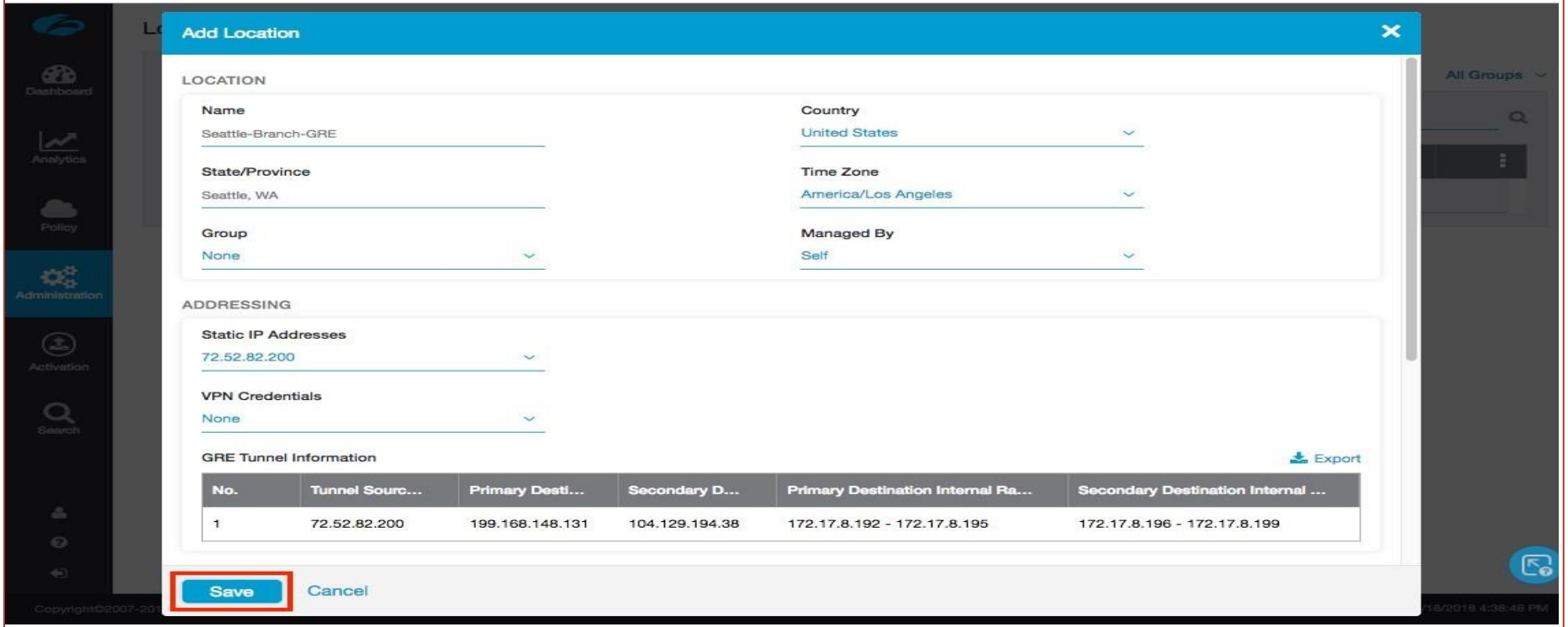


Figure 7: Verify Location Information and Save

2.2.5 Confirm Changes Have Been Submitted

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

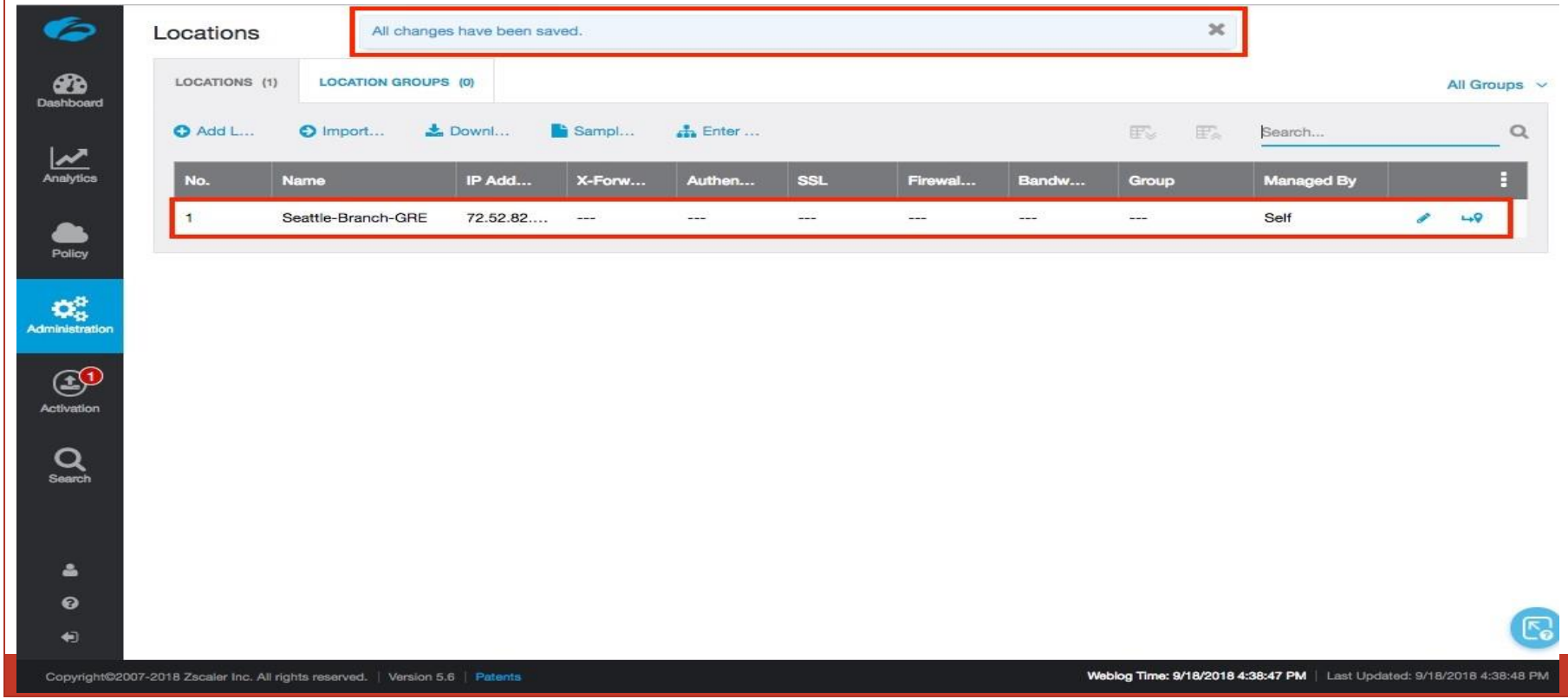


Figure 8: Confirm Changes Have Been Submitted

At this point, although we have saved our new location, it has only submitted the change for pending activation. If you wanted to make other changes throughout ZIA, you could.

None of these changes would get applied until they are activated, which allows you to batch groups of changes as you require. Only upon activation do the changes get pushed to ZEN nodes.

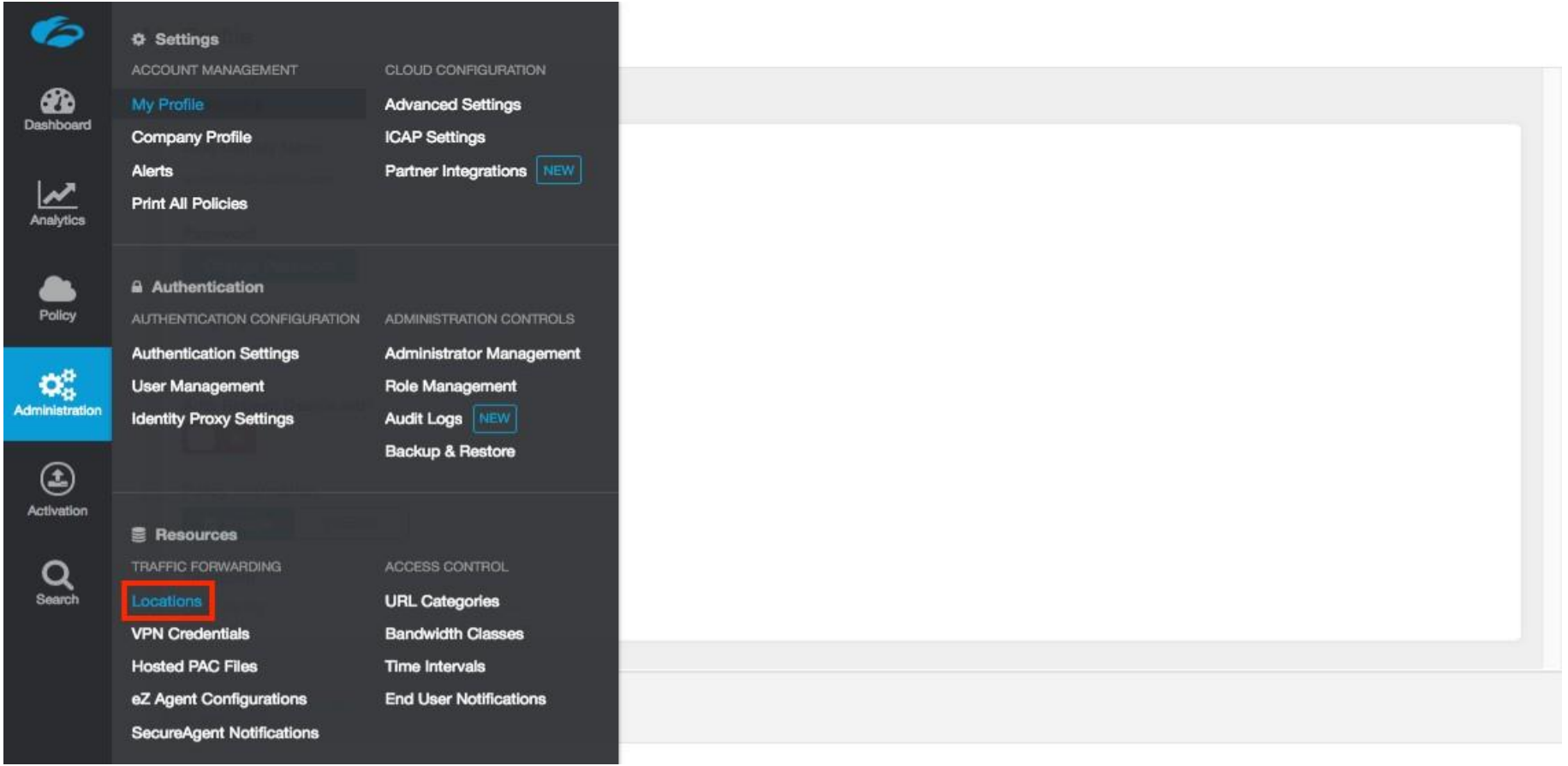


Figure 9: Navigate to VPN Credentials

2.3.2 Add a VPN Credential

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

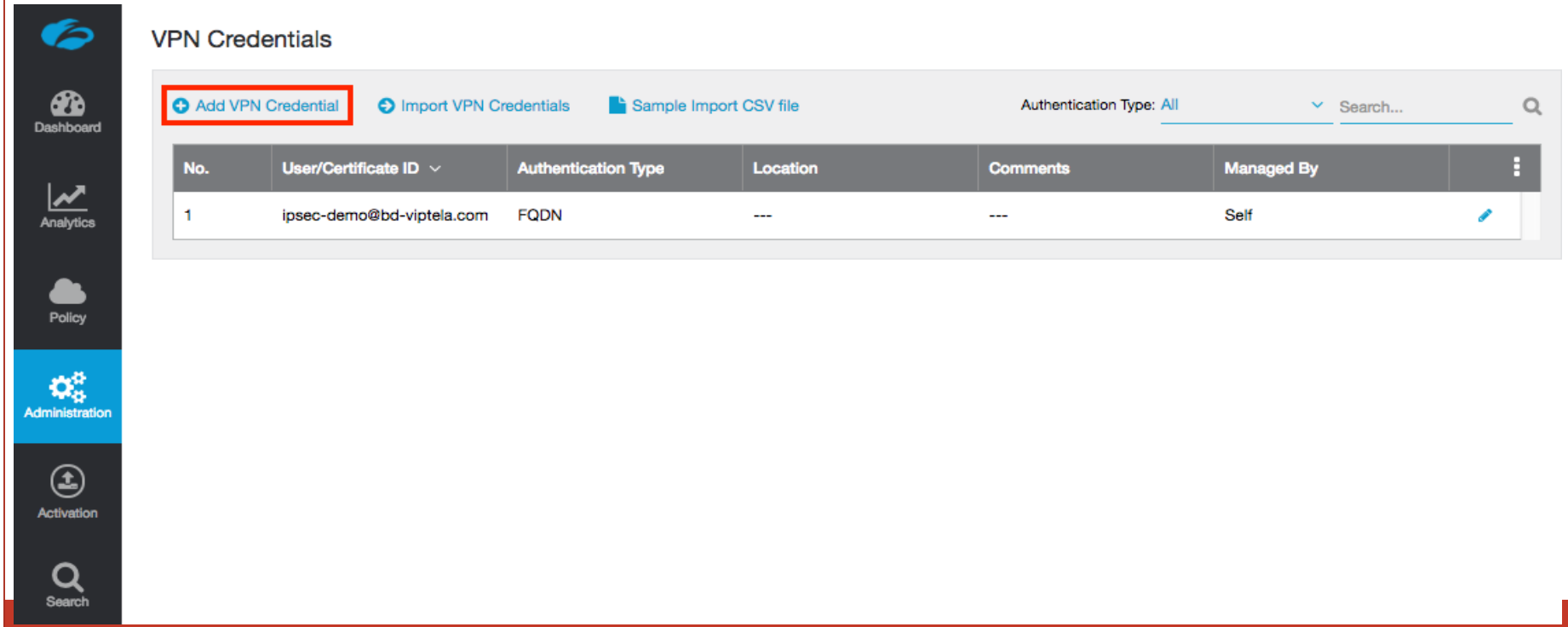


Figure 10: Adding a VPN Credential

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

2.3.3 Enter VPN Credential Data

In Figure 11, we will configure the FQDN and Pre-Shared Key (PSK) for IKE. For the FQDN, you only need to configure the username portion of the FQDN as the domain name will automatedly be added (which is to the right). Once both the FQDN and PSK are configured, click “Save” to continue.

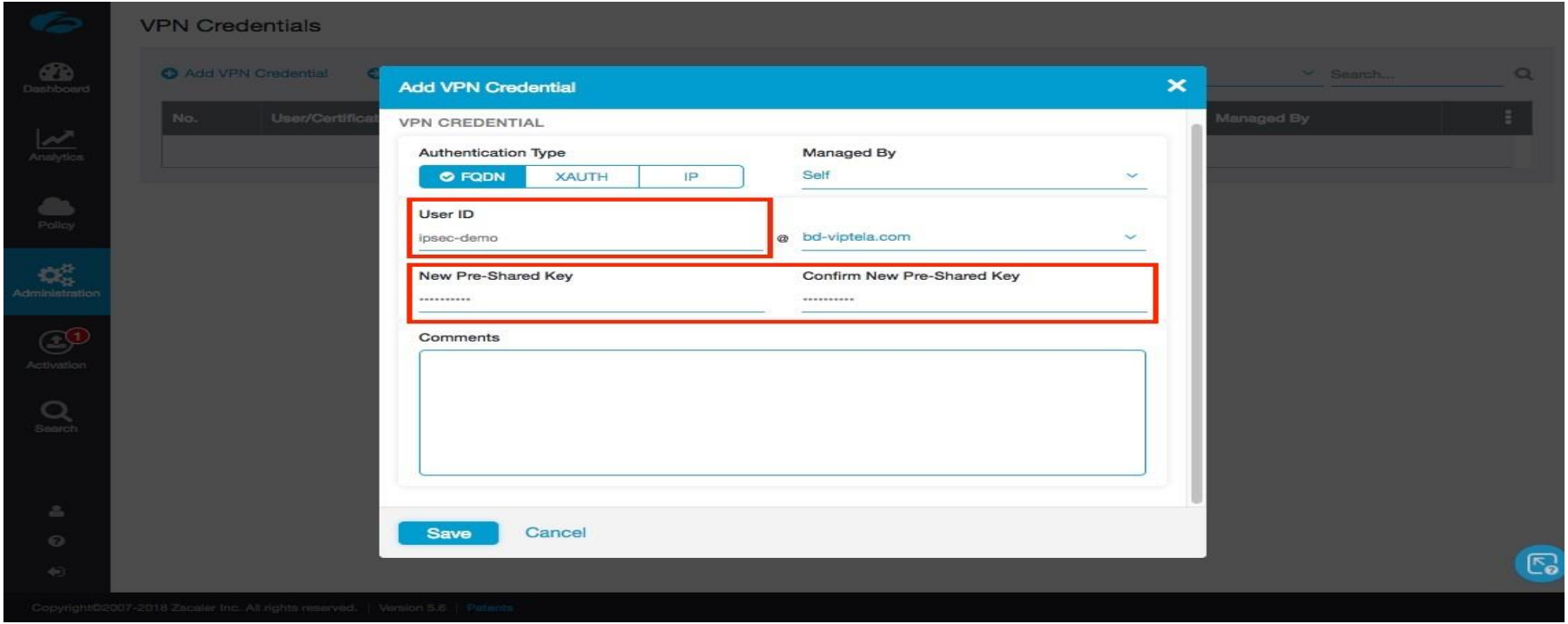


Figure 11: Enter VPN Credential Data

2.3.4 Verify Location Information and Save

In Figure 12, after saving the VPN Credential, you see “All changes have been saved” in the top center of your screen. If you look below this, you should see the VPN Credential you created.

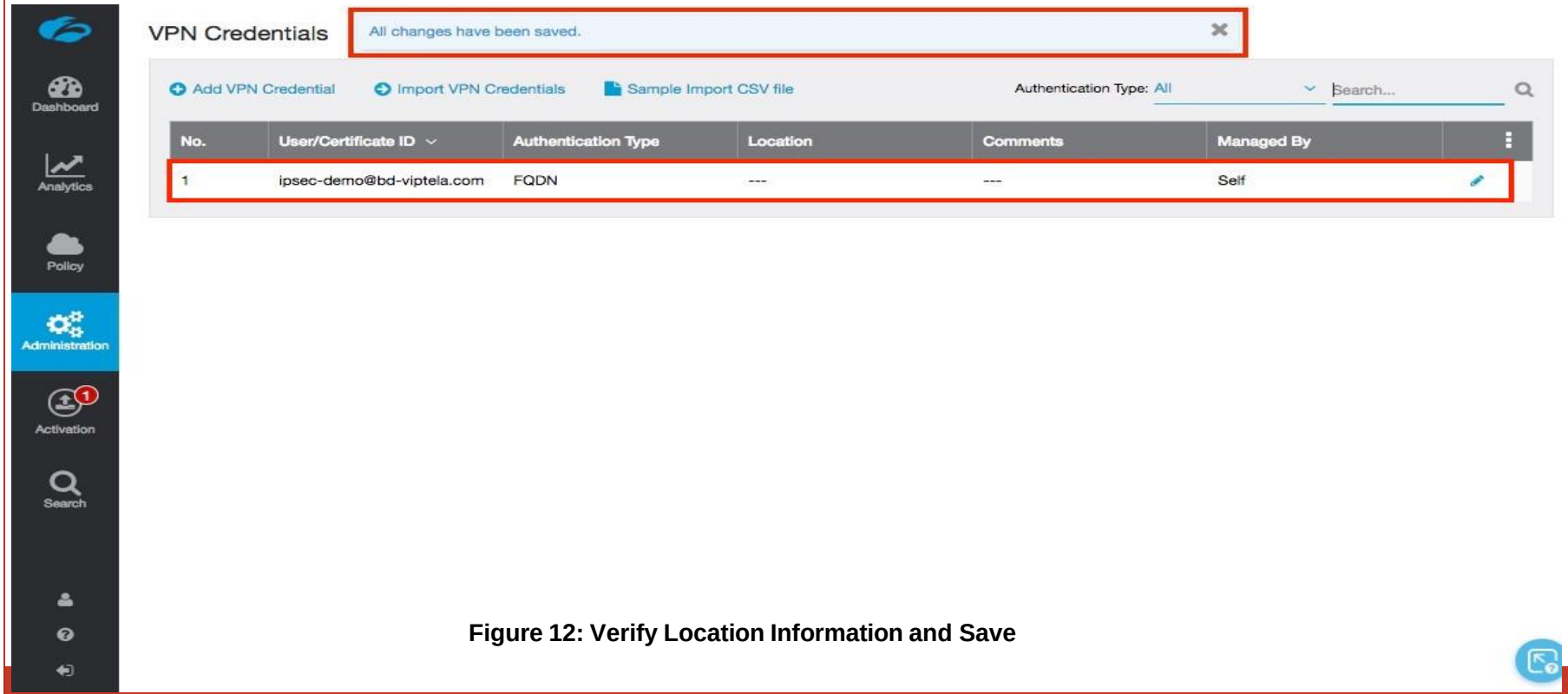


Figure 12: Verify Location Information and Save

2.3.5 Navigate to Locations

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

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

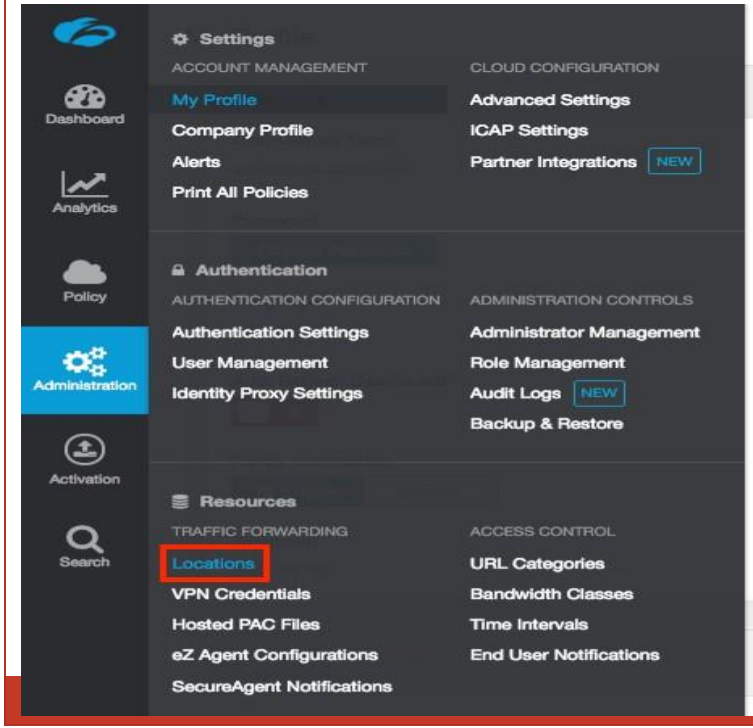


Figure 13: Navigate to Locations

2.3.6 Add a Location

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

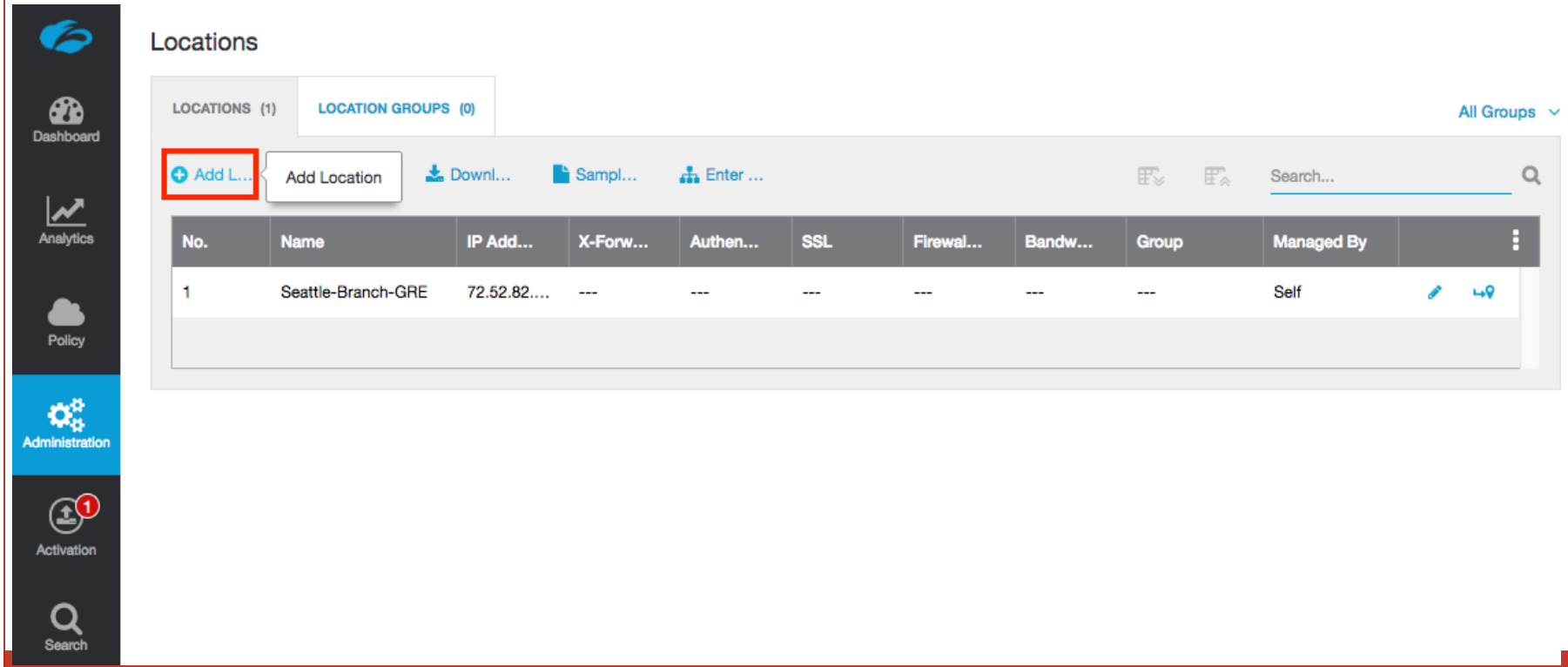


Figure 14: Add a Location

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

2.3.7 Enter Location Data

In Figure 15, you will need to fill in the fields within the red box. The name of the location will be used as a policy object within ZIA.
The “Managed By” field you can leave alone as “Self” is used for administration through the web interface. Lastly, under “VPN Credential”, select the VPN credential you configured in the prior steps. Once you select the drop down, the screen in the next section will appear.

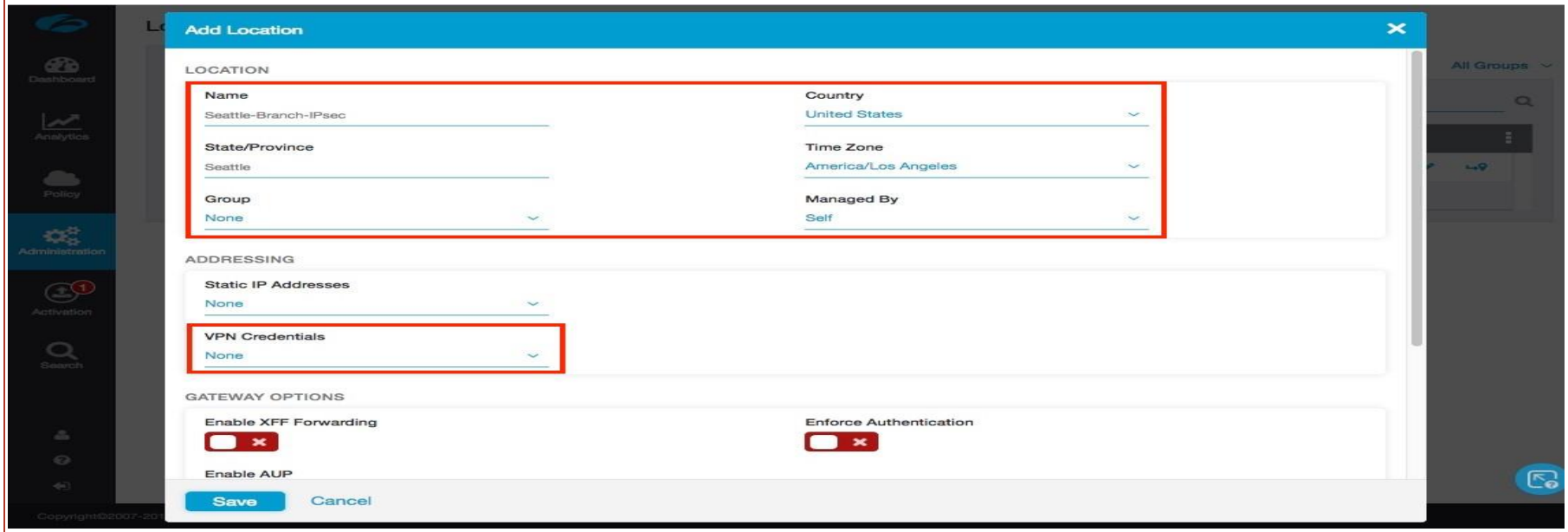


Figure 15: Enter Location Data

2.3.8 Add VPN Credential to Location and Save

In Figure 16, you should see the VPN Credential you configured in the prior section. Select it and click “Save” after. From there, once you save the Location itself, this will couple the VPN Credential to this Location. When you have competed the fields, select “Save” to continue.

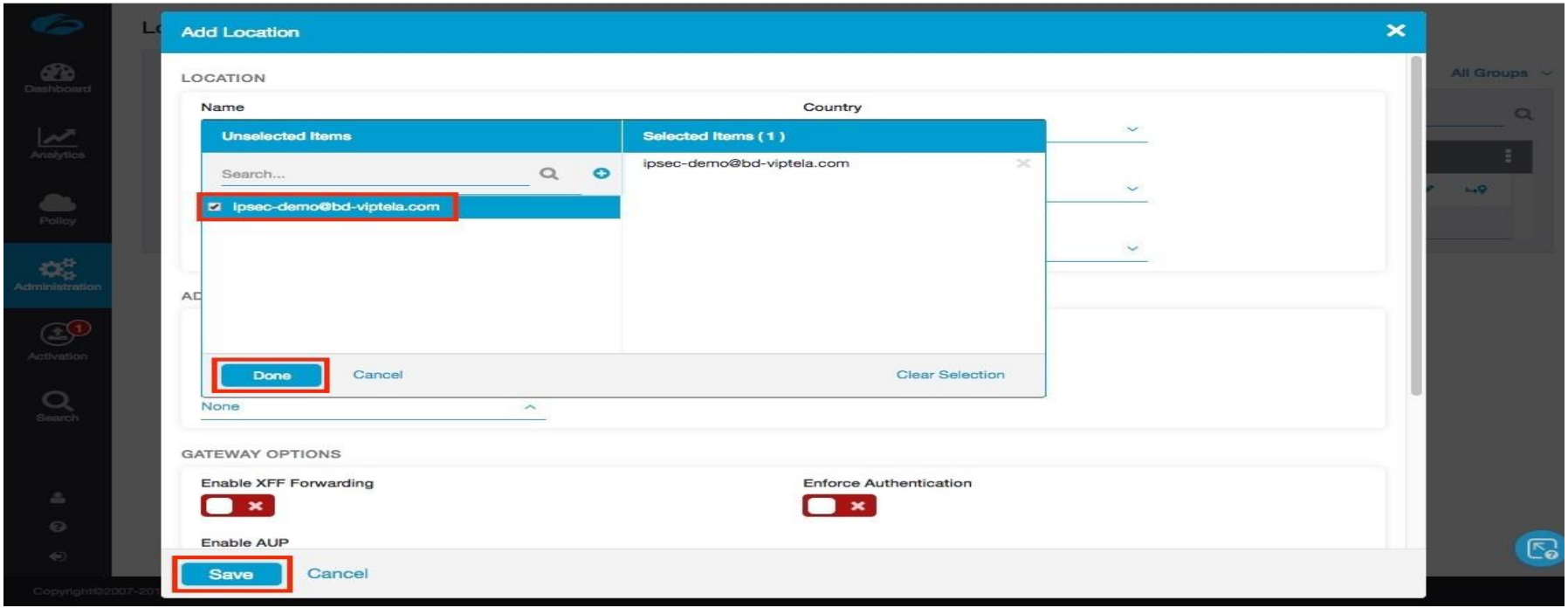


Figure 16: Add VPN Credential to Location and Save

2.3.9 Confirm Changes Have Been Saved

In Figure 17, after saving the Location, you see “All changes have been saved” in the top center of your screen. If you look below this, you should see the Location you created.

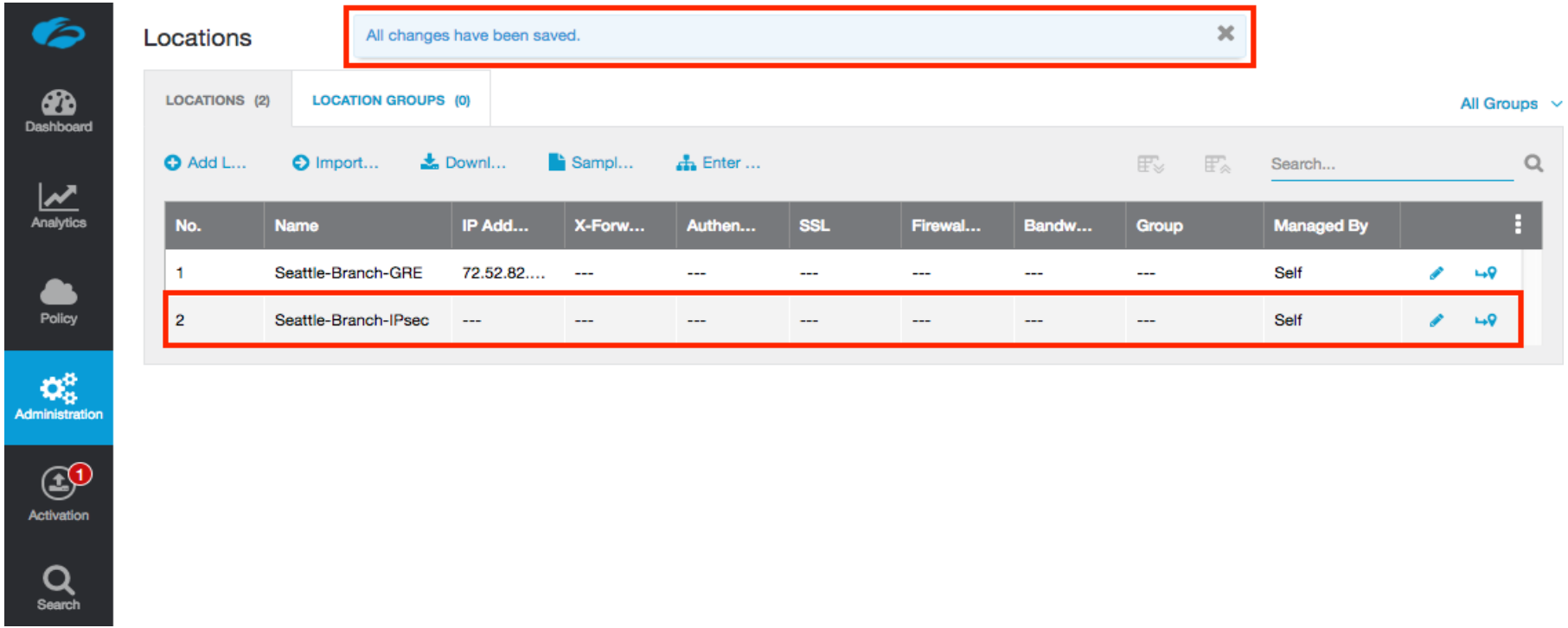


Figure 17: Confirm Changes Have Been Saved

2.4 Activate Pending Changes

2.4.1 Activate Changes

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

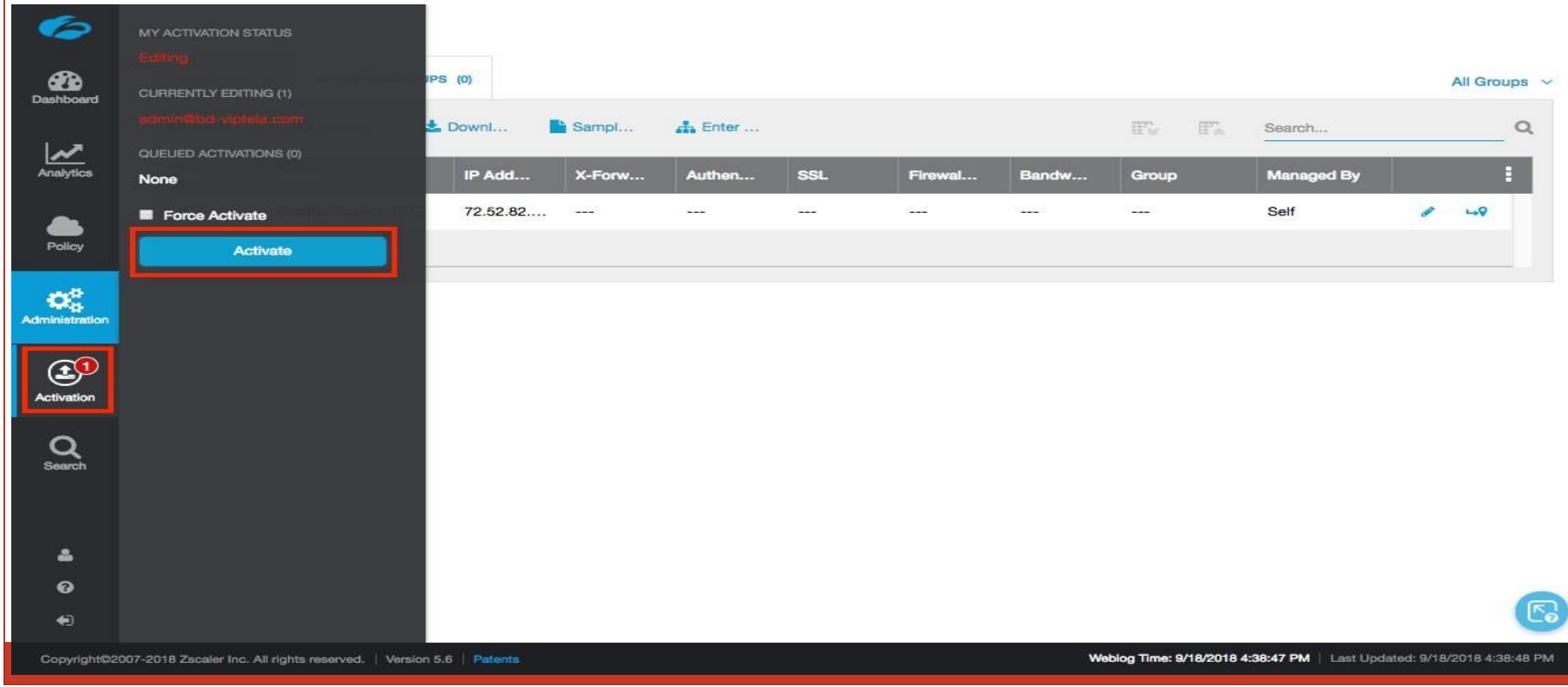


Figure 18: Activate Changes

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

2.4.2 Activation Confirmation

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

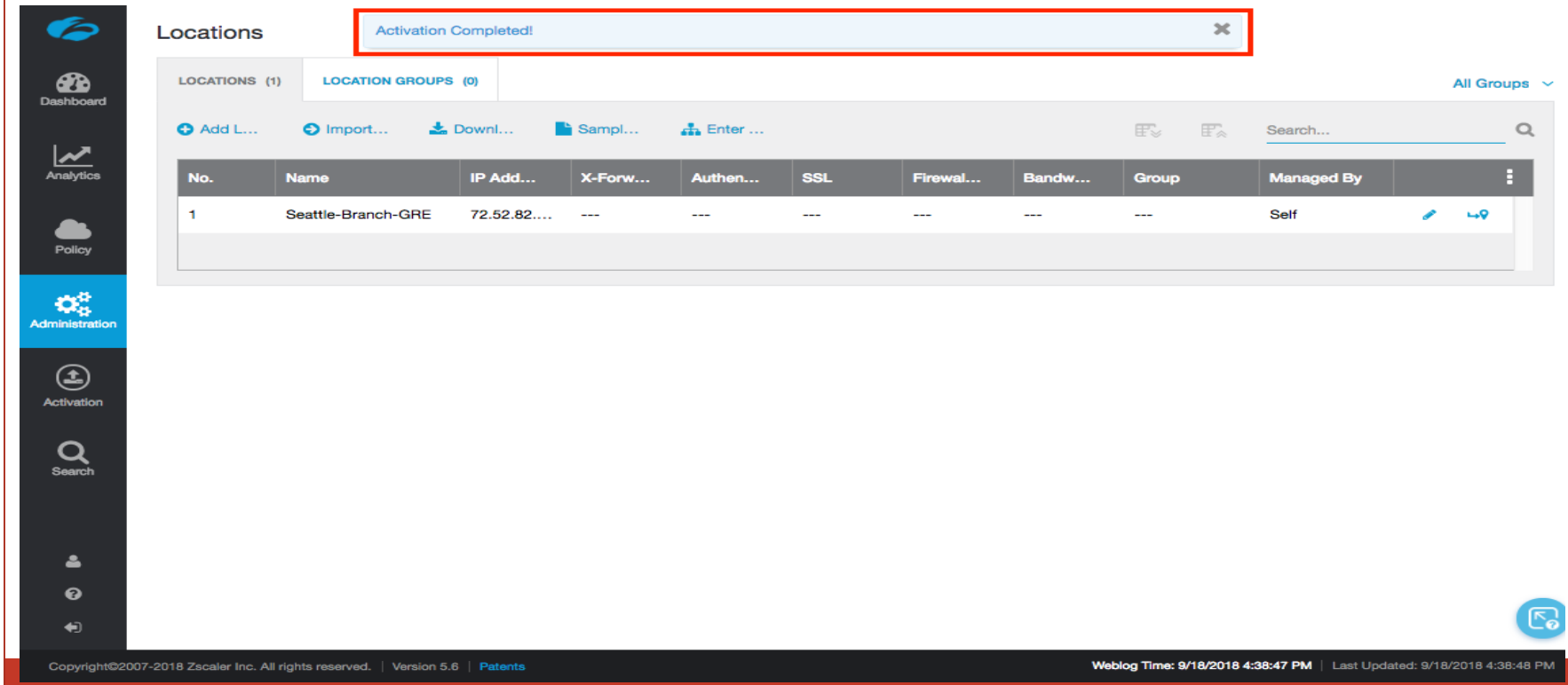


Figure 19: Activation Confirmation

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

Configuring Cisco SD-WAN

3 Configuring Cisco SD-WAN

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

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

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

3.1.1 Log into Cisco SD-WAN vManage

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

Figure 20: Cisco vManage Login

3.2 Configuring GRE Tunnel

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

3.2.1 Add Feature Template

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

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

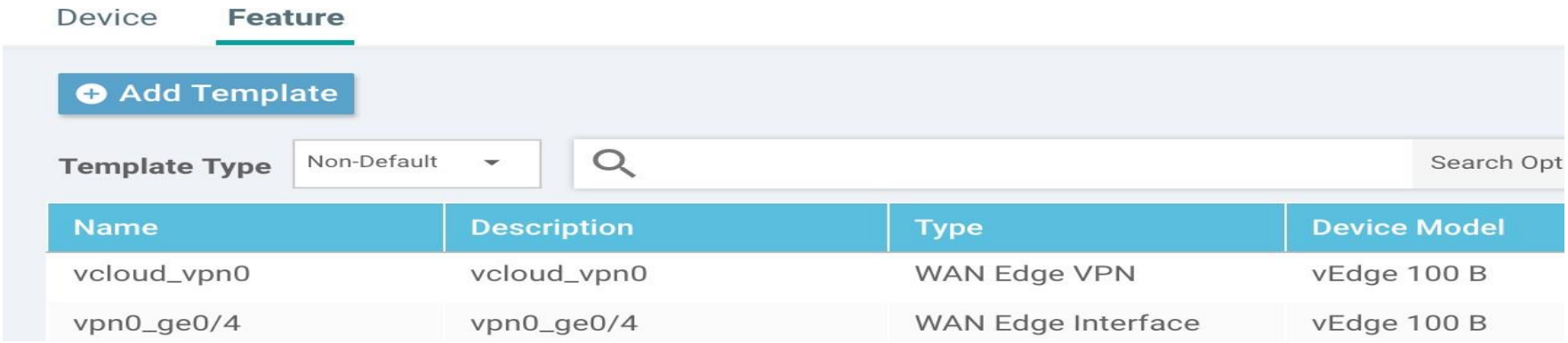


Figure 21: Add Feature Template

3.2.2 Add VPN Interface GRE Feature

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

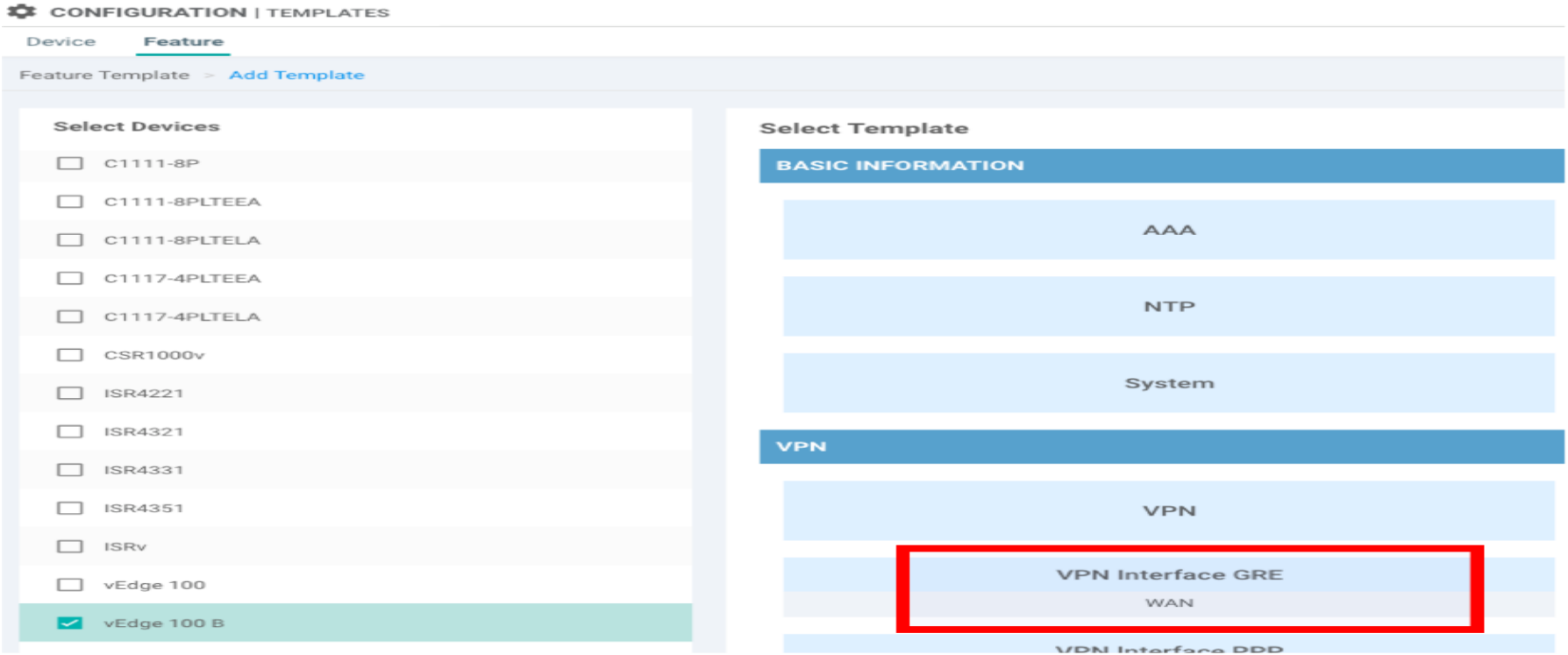


Figure 21: Add VPN Interface GRE Feature

3. *Set GRE Source Interface*

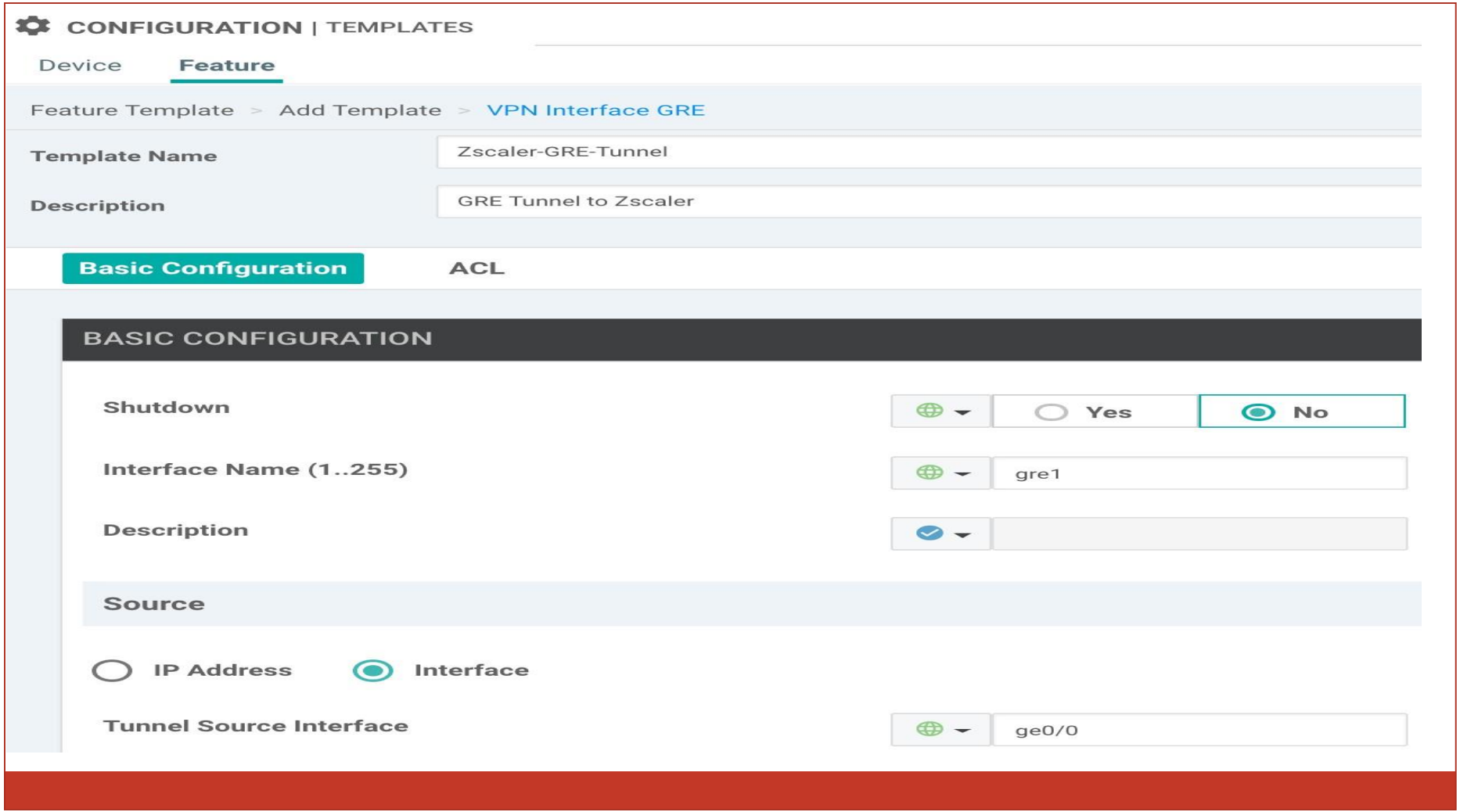
- Provide template name and description for the VPN Interface GRE feature template

- Under ***Basic Configuration > Shutdown***, change the attribute type to Global and select “No” radio button. This will unshut the GRE interface.

- Configure ***Interface Name*** as “gre1”. This is the name of the virtual GRE interface on the SD-WAN Edge router connecting to Zscaler.

- Configure the ***Tunnel Source Interface***. This is the physical VPN0 transport side interface connecting SD-WAN Edge router to the wide area network.

Figure 22: GRE Interface Source Settings


CONFIGURATION | TEMPLATES
Device
Feature
Feature Template > Add Template > VPN Interface GRE
Template Name
Zscaler-GRE-Tunnel
Description
GRE Tunnel to Zscaler
Basic Configuration
ACL
BASIC CONFIGURATION
Shutdown
Yes
No
Interface Name (1..255)
gre1
Description
Source
IP Address
Interface
Tunnel Source Interface
ge0/0

4. Set GRE Interface Destination

Provide GRE tunnels destination details

- Under ***GRE Destination IP Address*** specify IP address which will be the destination of the GRE tunnel. This is Zscaler ZEN IP address

- Change the ***IPv4 Address*** attribute type to Global and type in the GRE interface IP address. In this case we use “172.17.8.193/30”. **Note:** This is for routing purpose and it accepts only /30 address.

- Change the ***IP MTU*** attribute type to Global and type in 1476

- Change the ***TCP MSS*** attribute type to Global and type in 1432

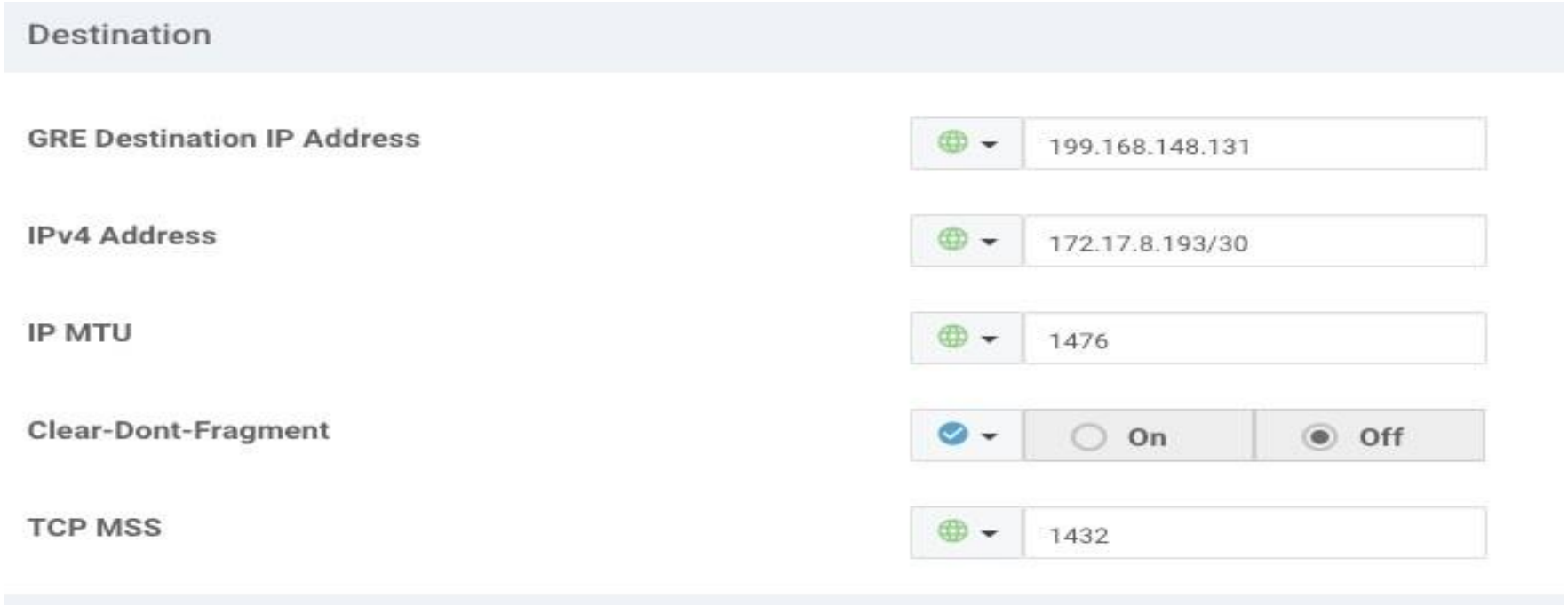


Figure 23: GRE Interface Destination Settings

3.2.5 Enable GRE Keepalives

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

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

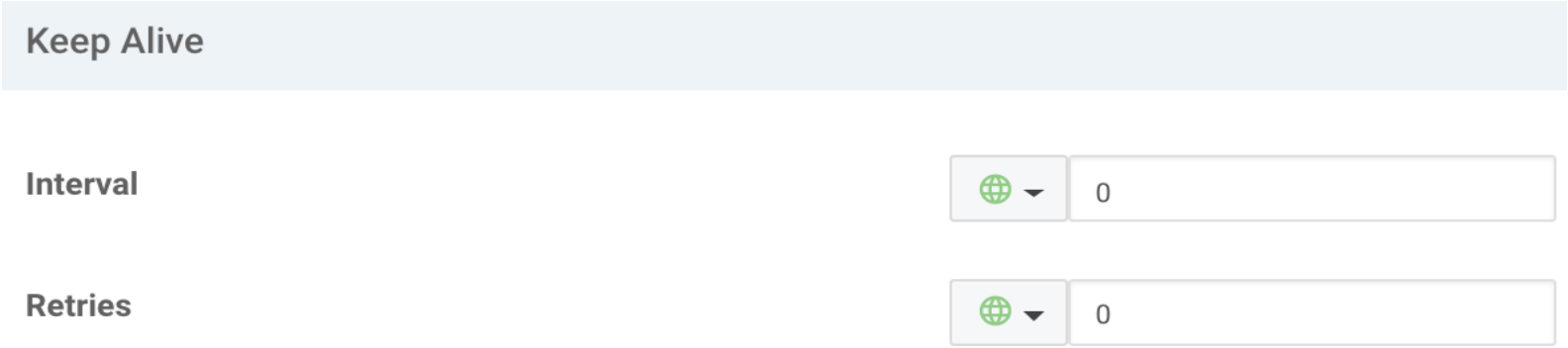


Figure 22: Disable GRE Keepalives

3.2.6 Add GRE Interface Feature Template

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

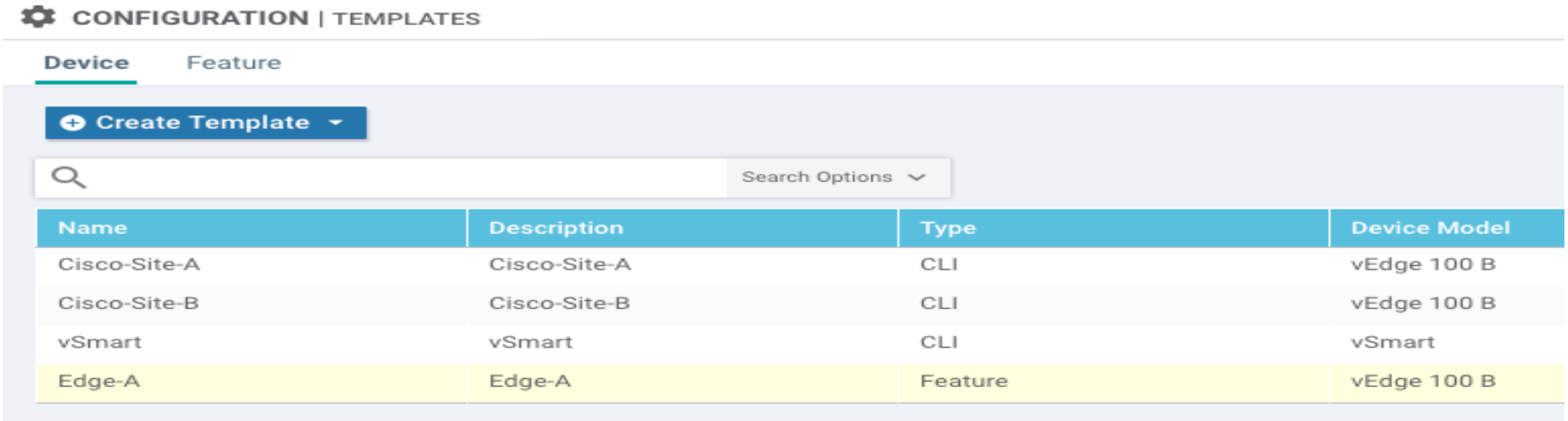


Figure 23: Device Templates List

3.2.7 Edit Device Template

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

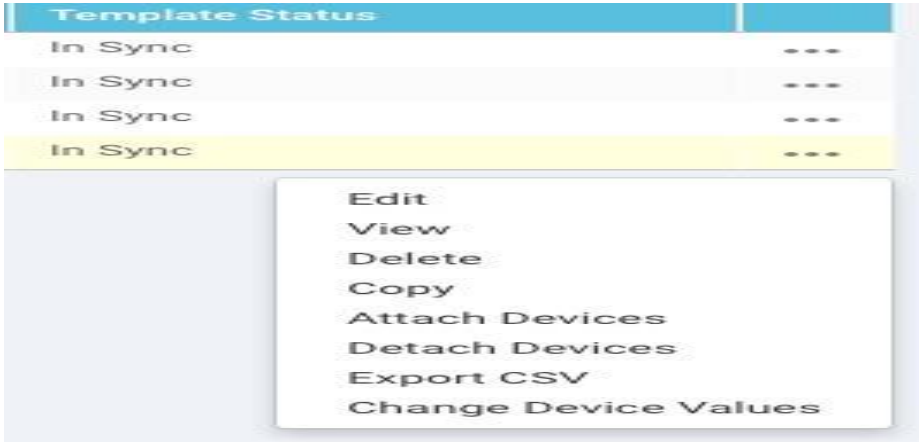


Figure 24: Edit Device Template

3.2.8 VPN-0 Template

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

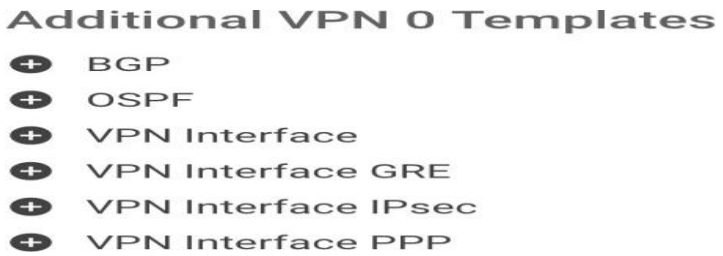


Figure 25: VPN0 Templates

3.2.9 Assign GRE Interface Feature to Device Template

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

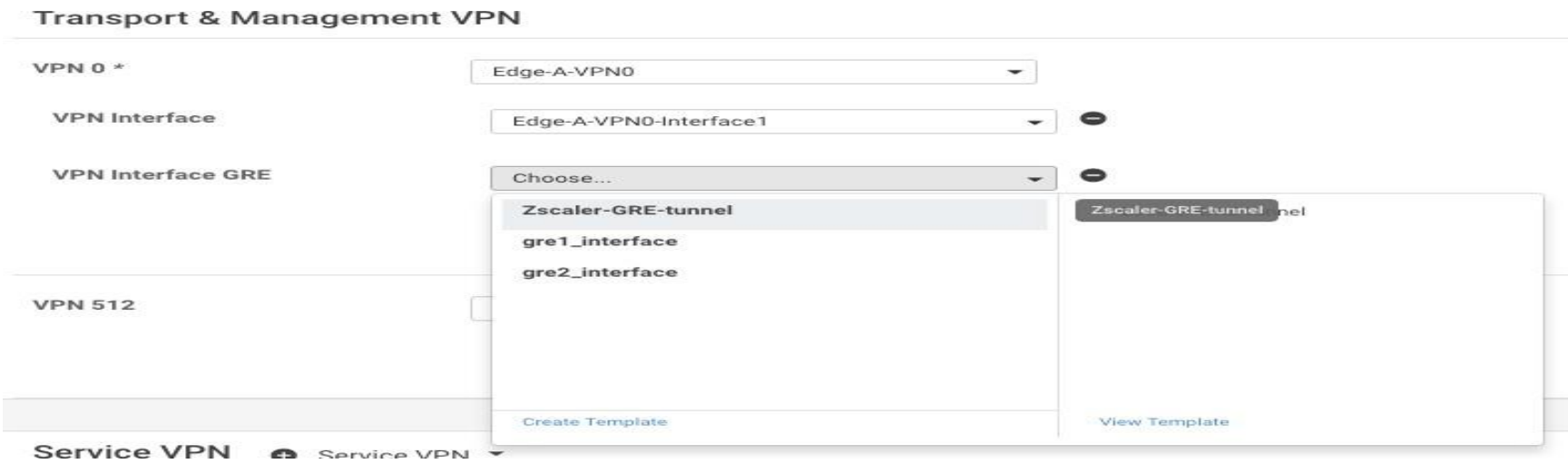


Figure 26: Assign GRE Interface Feature to Device Template

3.2.10 Verify Configuration Update

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

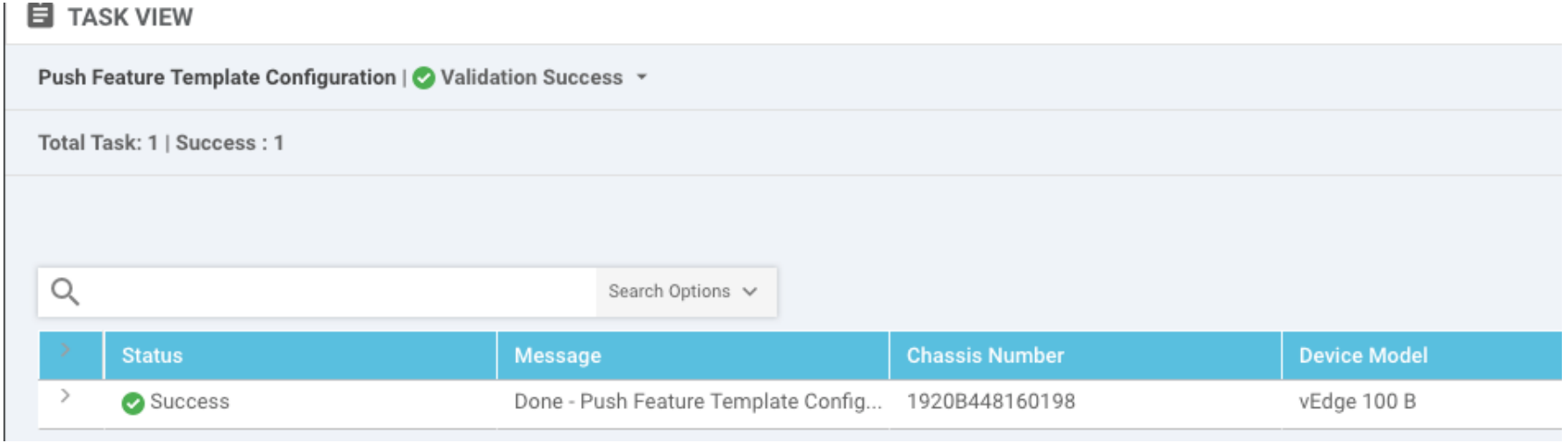
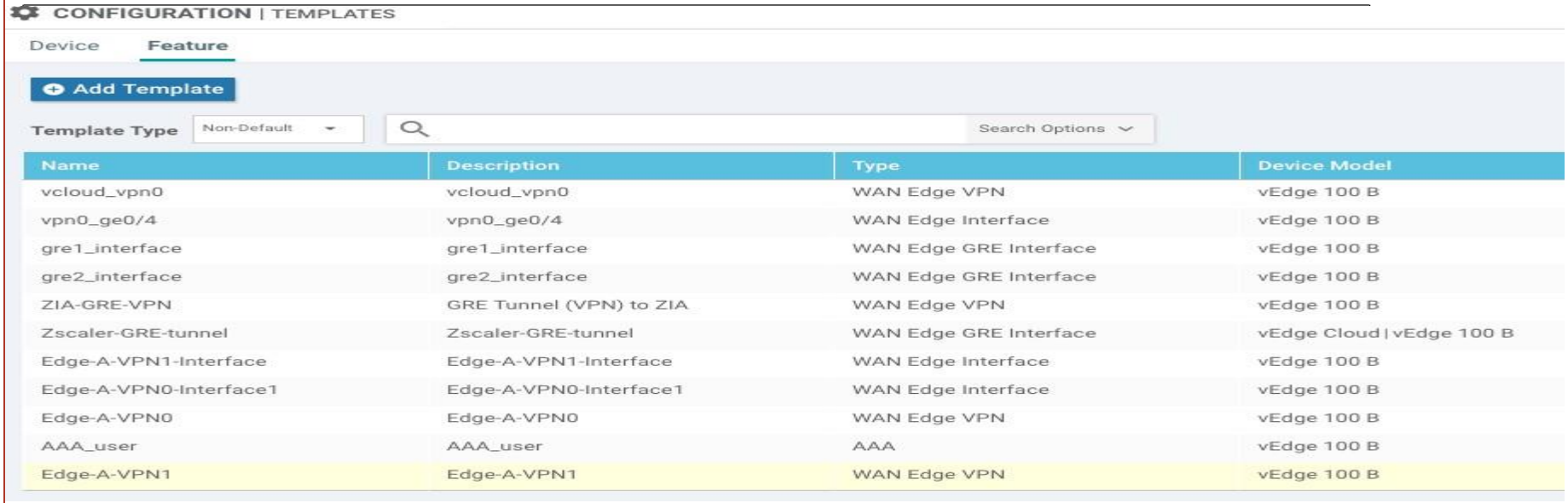


Figure 27: Successful Configuration Update

3.2.11 Feature Template

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



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

Figure 28: Feature Templates List

3.2.12 Add New GRE Route

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

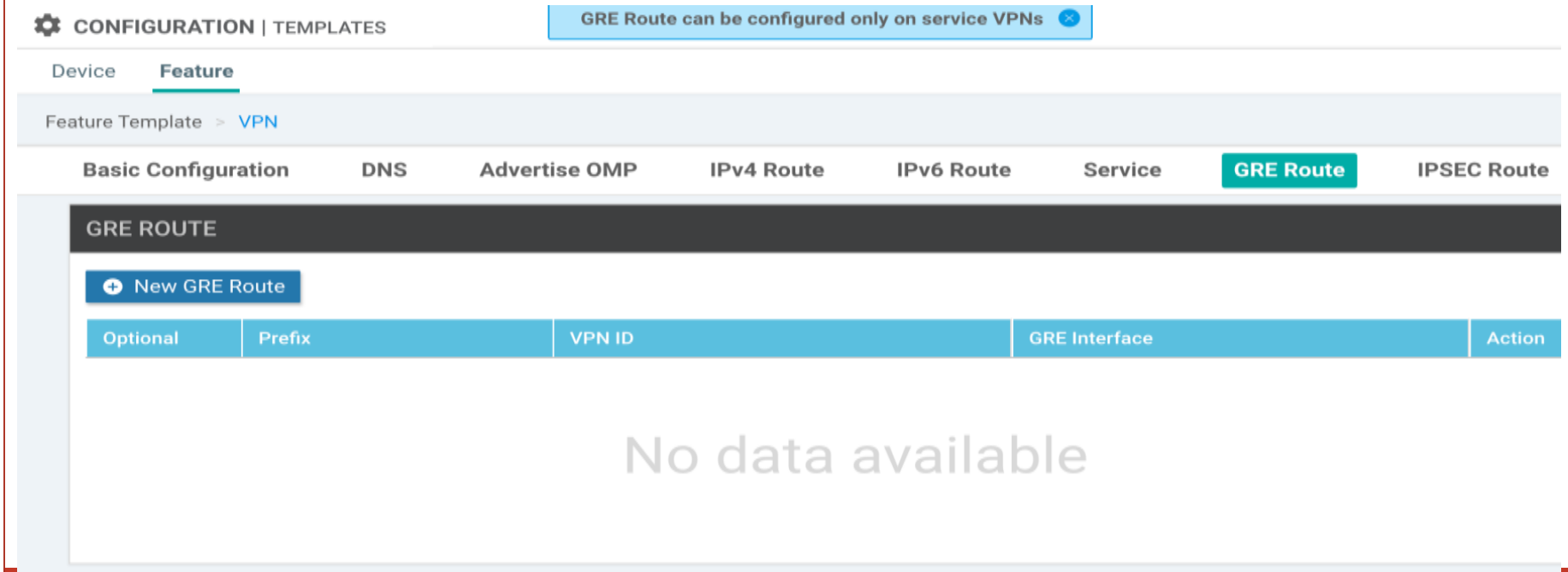


Figure 29: Add a New GRE route

3.2.13 Configure Routing towards GRE Tunnel

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

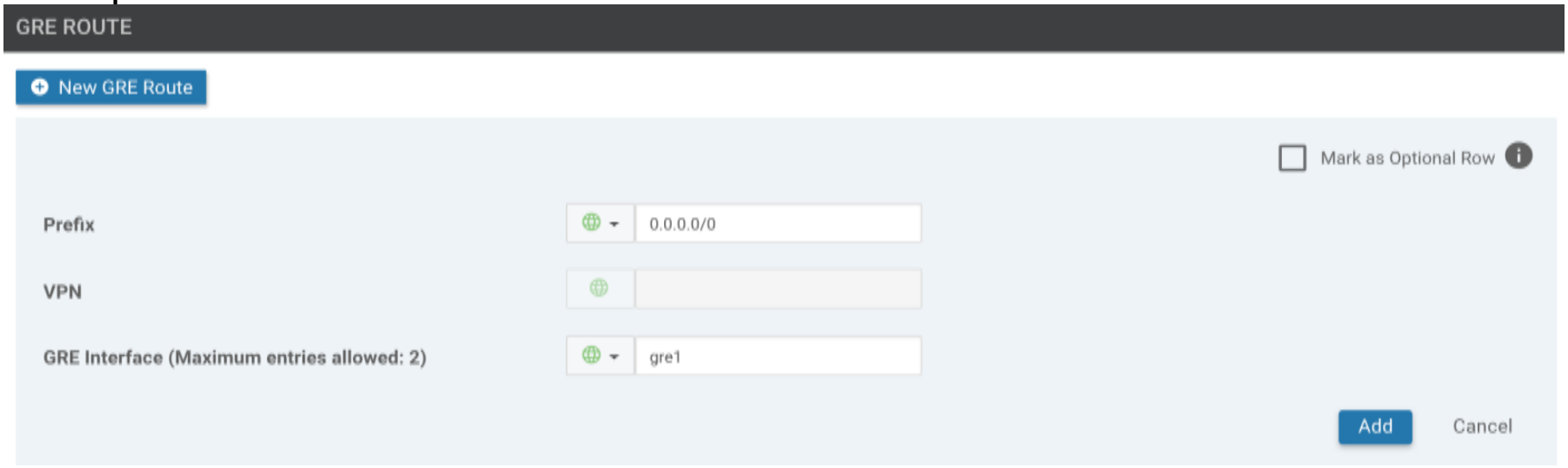


Figure 30: Provide destination prefix and GRE tunnel interface name

3.2.14 Verify GRE Route is Added

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

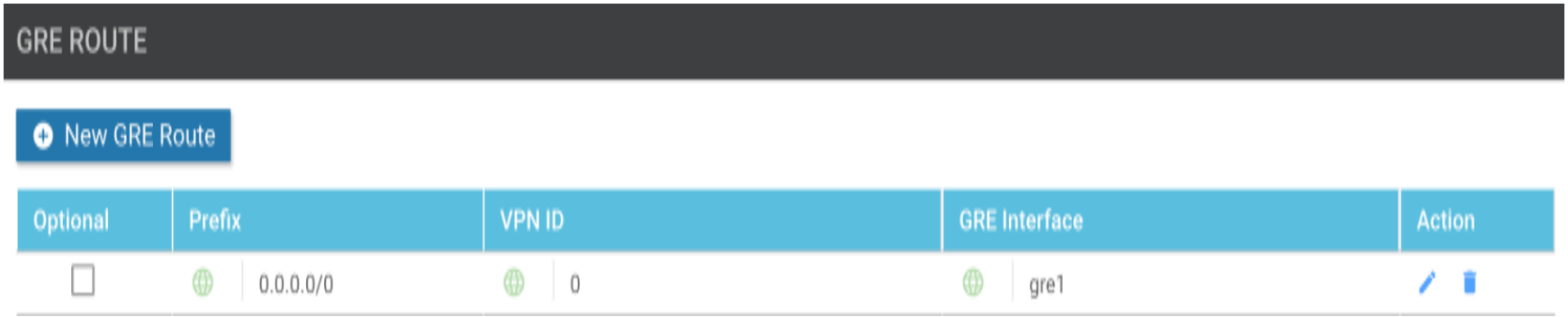


Figure 31: Check the added GRE route

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

3.2.15 Verify Configuration Update

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

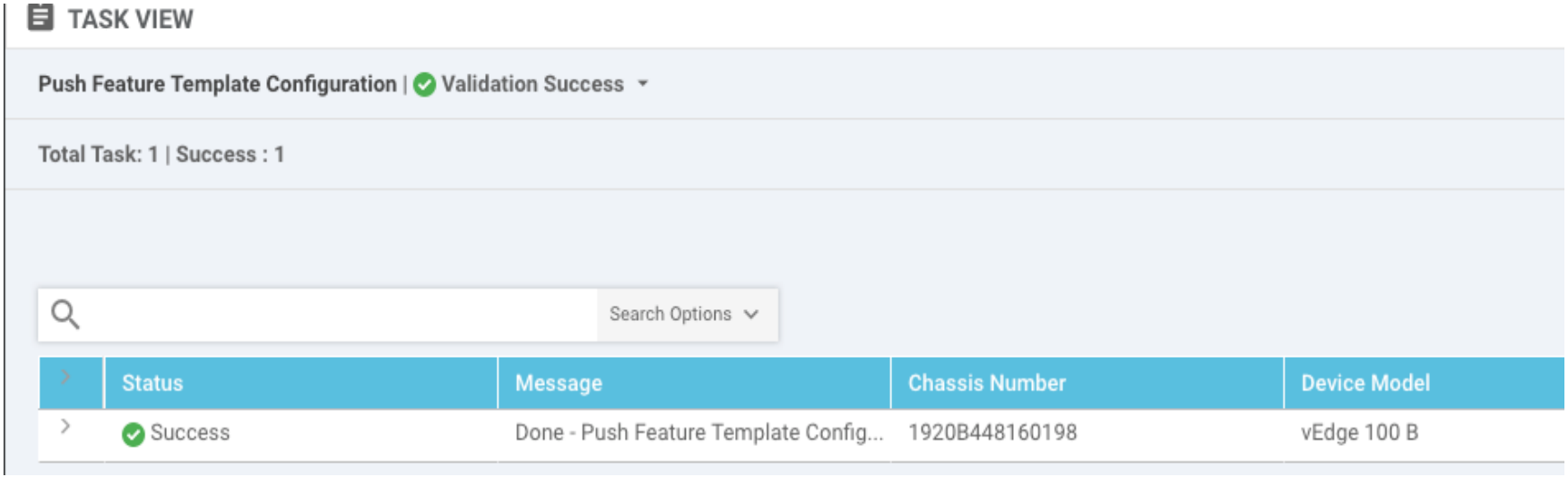


Figure 32: Successful Configuration Update

Configuring IPsec Tunnel

3.3 Configuring IPsec Tunnel

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

3.3.1 View Feature Template List

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

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

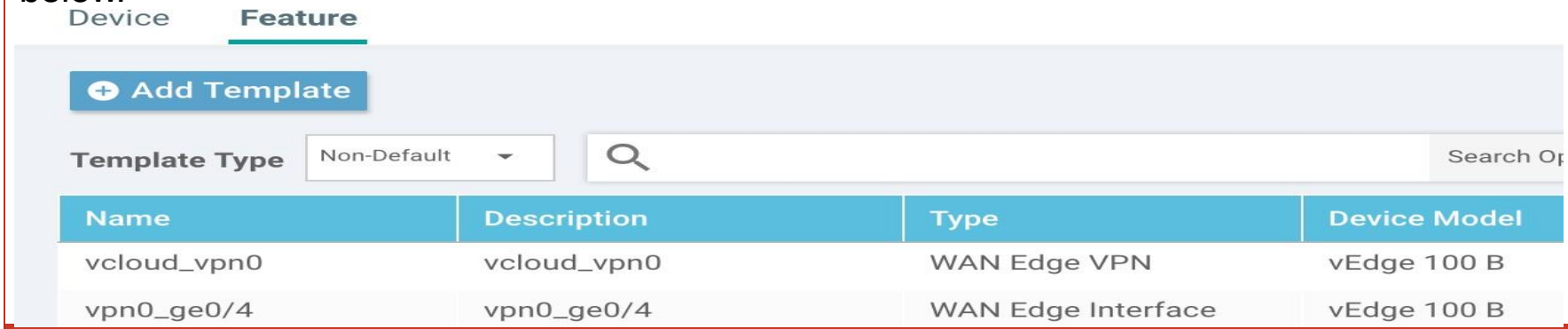


Figure 33: Feature Templates List

3.3.2 Select IPsec Tunnel to Zscaler

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

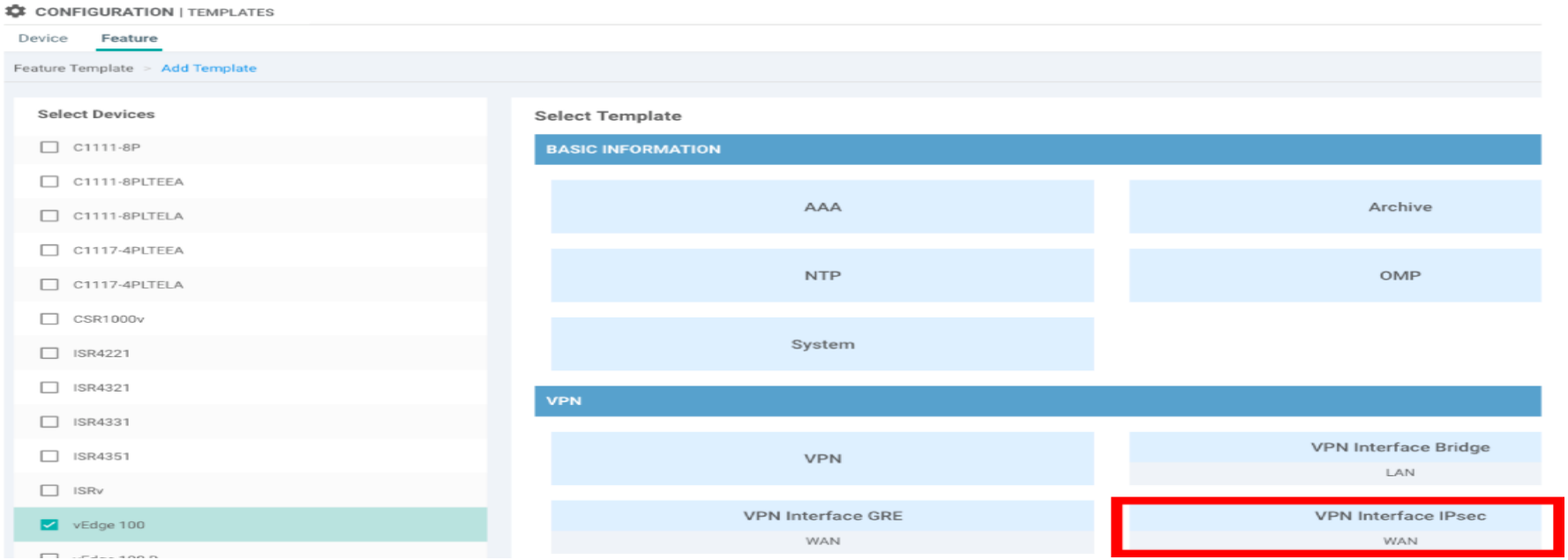


Figure 34: Select “VPN Interface IPSec” for IPSec tunnel to Zscaler

3. Configure IPsec Tunnel Source and Destination

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

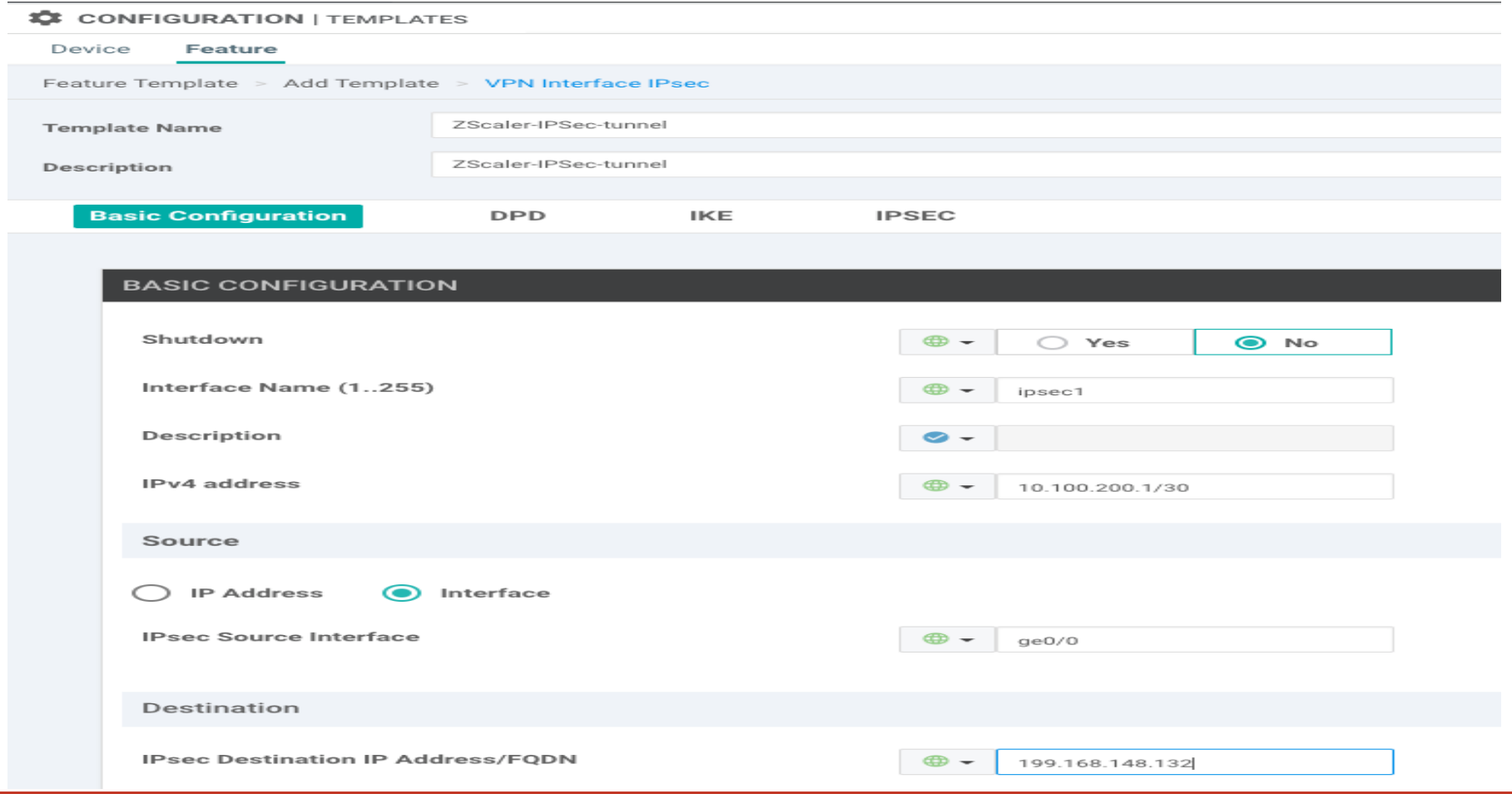


Figure 35: Configure IPSec Source & Destination

4. Configure Dead Peer Detection

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

5. Configure IKE Parameters

Configure IKE parameters:

- Under ***IKE Version***, change the attribute type to Global and type “2”
- Under ***IKE Diffie-Hellman Group***, change the attribute type to Global and choose “2 1024-bit modulus”

- Under ***Preshared Key***, change the attribute type to Global and type the preshared key value. Preshared key value must match between SD-WAN Edge router and ZScaler ZEN for IPSec tunnel to successfully come up.

- Under ***IKE ID for Local Endpoint***, change the attribute type to Global and type the local ID value. Local ID value configured on SD-WAN Edge router must match Remote ID value configured on ZScaler ZEN for IPSec tunnel to successfully come up.

- Under ***IKE ID for Remote Endpoint***, change the attribute type to Global and type the remote ID value. Remote ID value configured on SD-WAN Edge router must match Local ID value configured on ZScaler ZEN for IPSec tunnel to successfully come up.

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

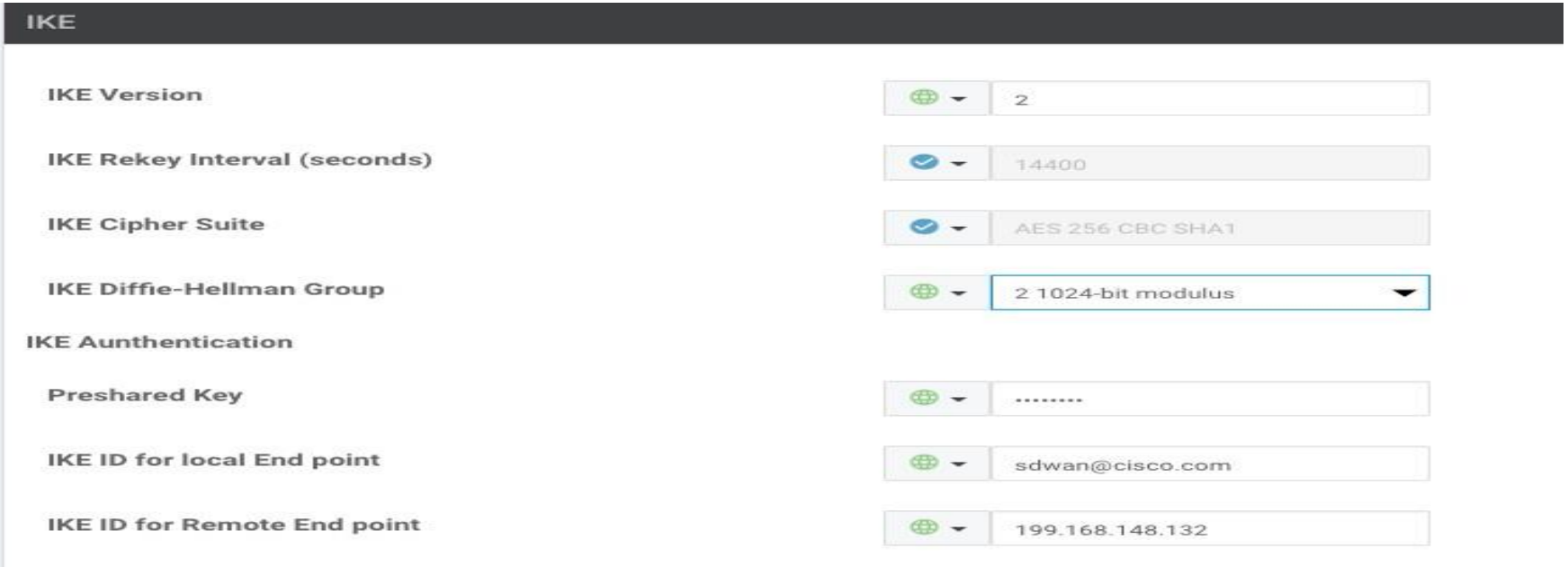


Figure 36: Configure IKE parameters

6. *Configure IPsec Cipher-suite*

Configure IPSec parameters:

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

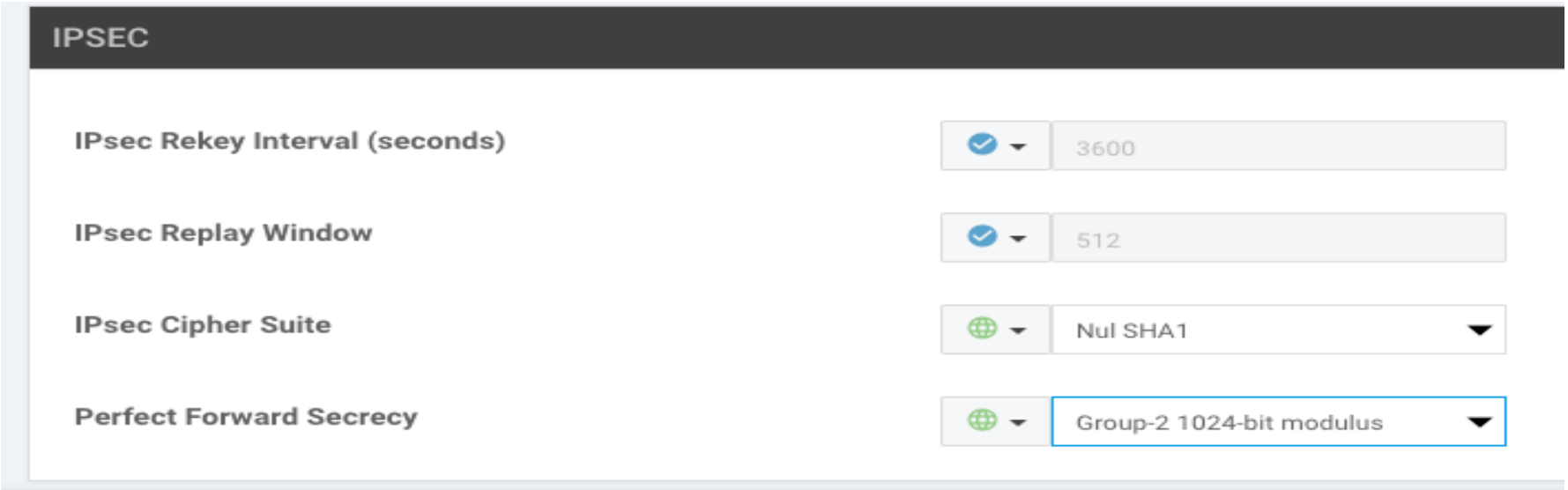


Figure 37: Configure IPSec Cipher-suite

3.3.7 View Device Template List

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

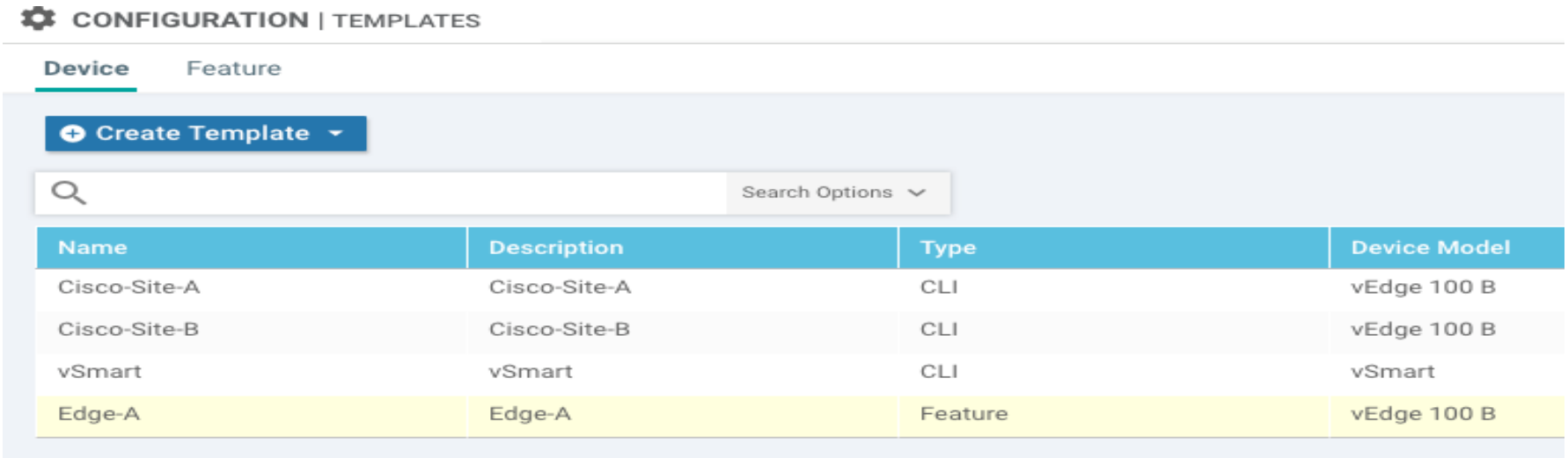


Figure 38: Device Templates List

3.3.8 Edit the Device Template

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

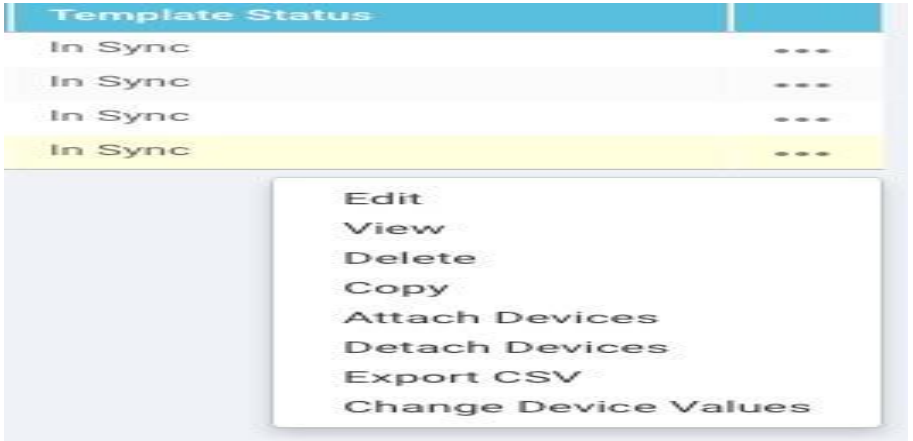


Figure 39: Edit the device template

3.3.9 Add VPN Interface IPsec

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

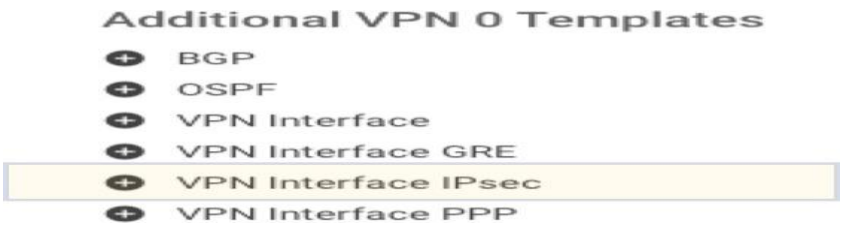


Figure 40: Add VPN Interface IPSec

3.3.10 Select IPsec Template

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

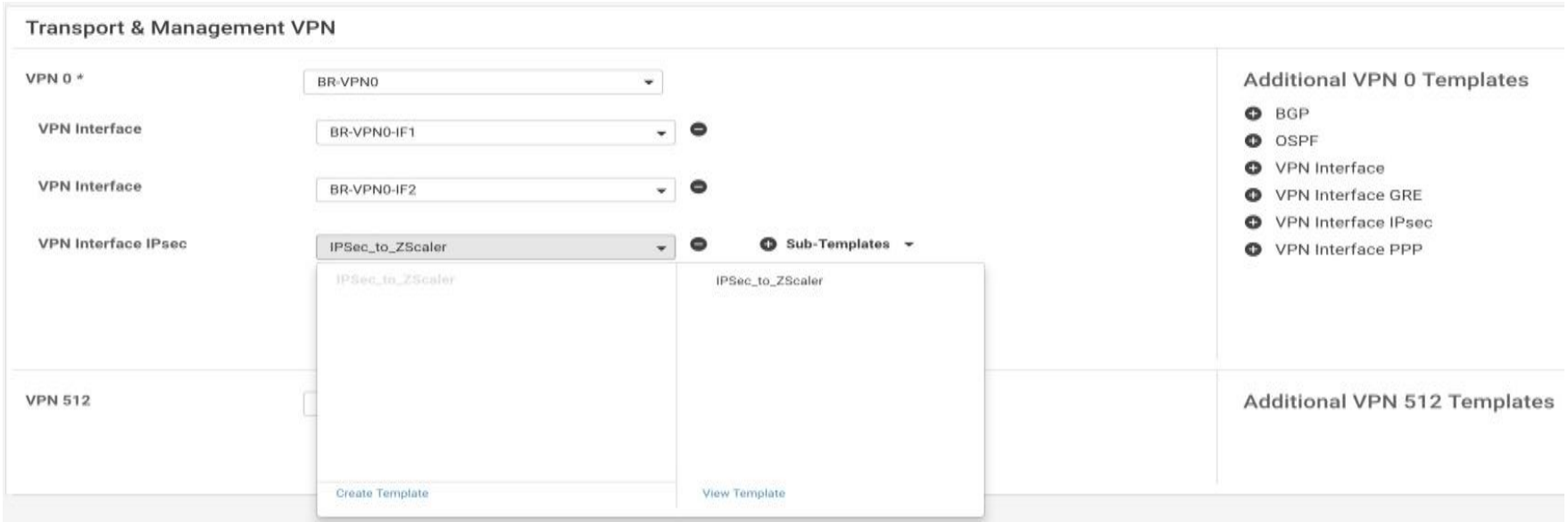


Figure 41: Select the IPSec template

3.3.11 Update and Verify Configuration Update

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

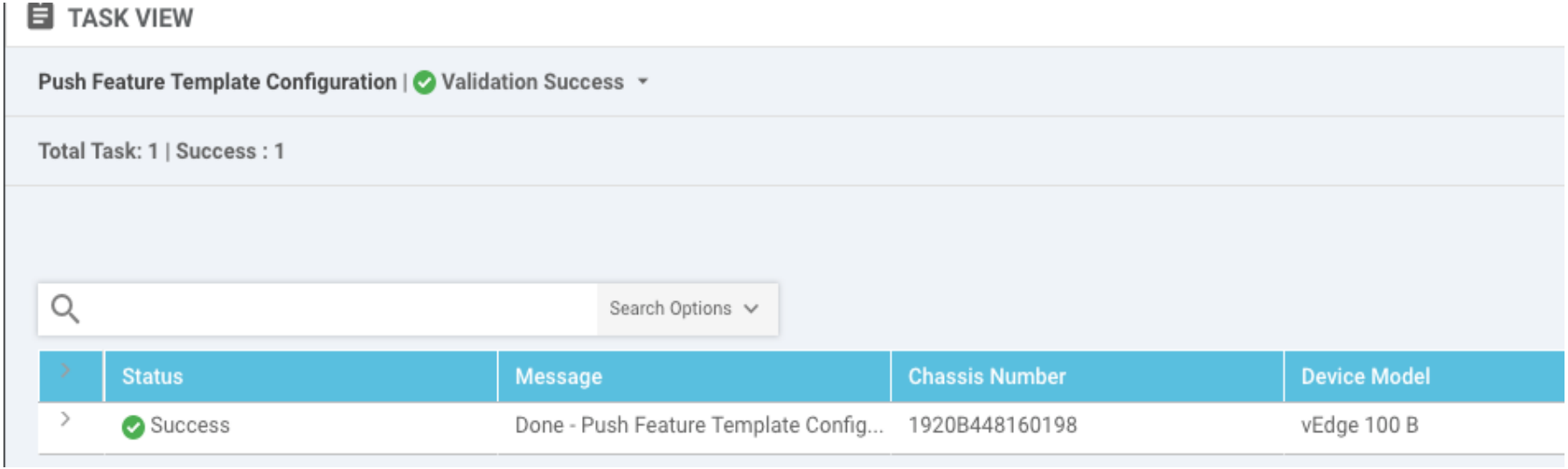
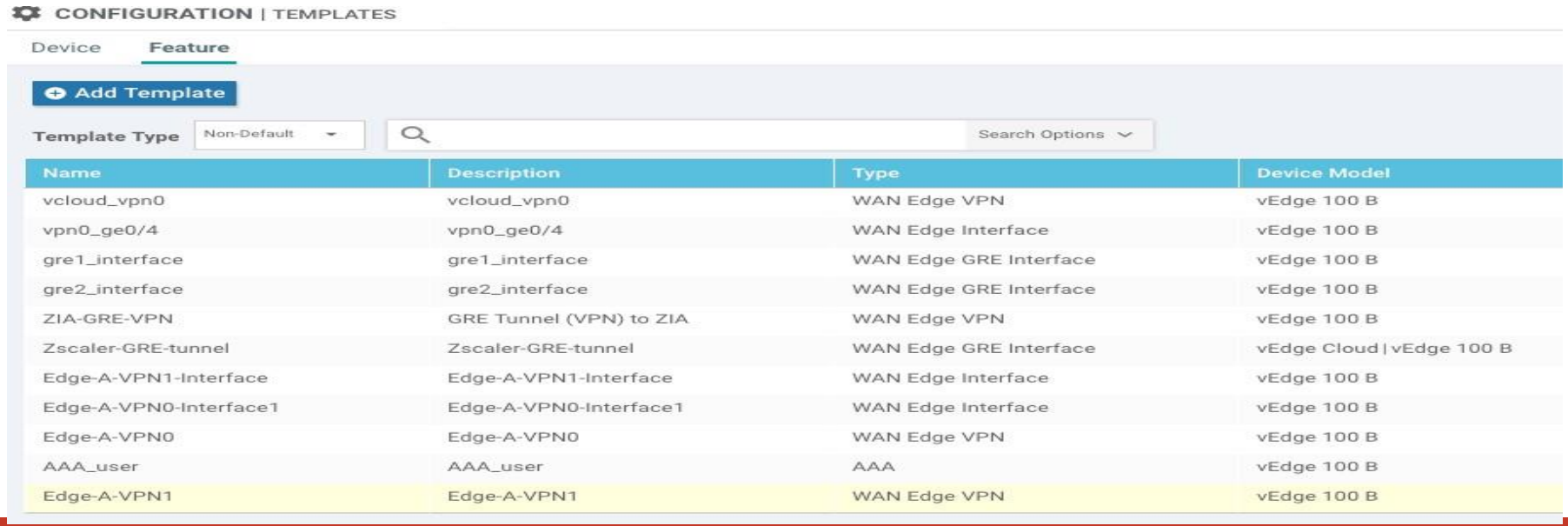


Figure 42: Successful configuration update

3.3.12 *Add Static Route*

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



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

Figure 43: Feature Templates List

3.3.13 *Add New IPsec Route*

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

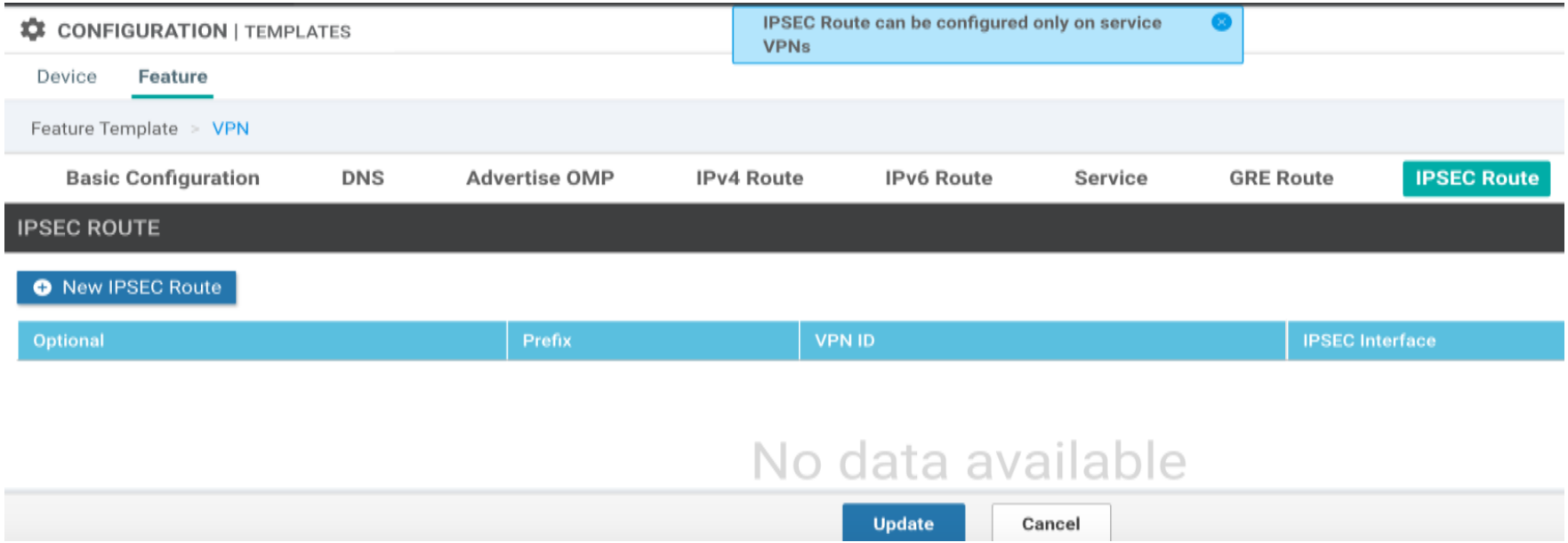


Figure 44: Add New IPSec route

3.3.14 Configure Destination Prefix

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

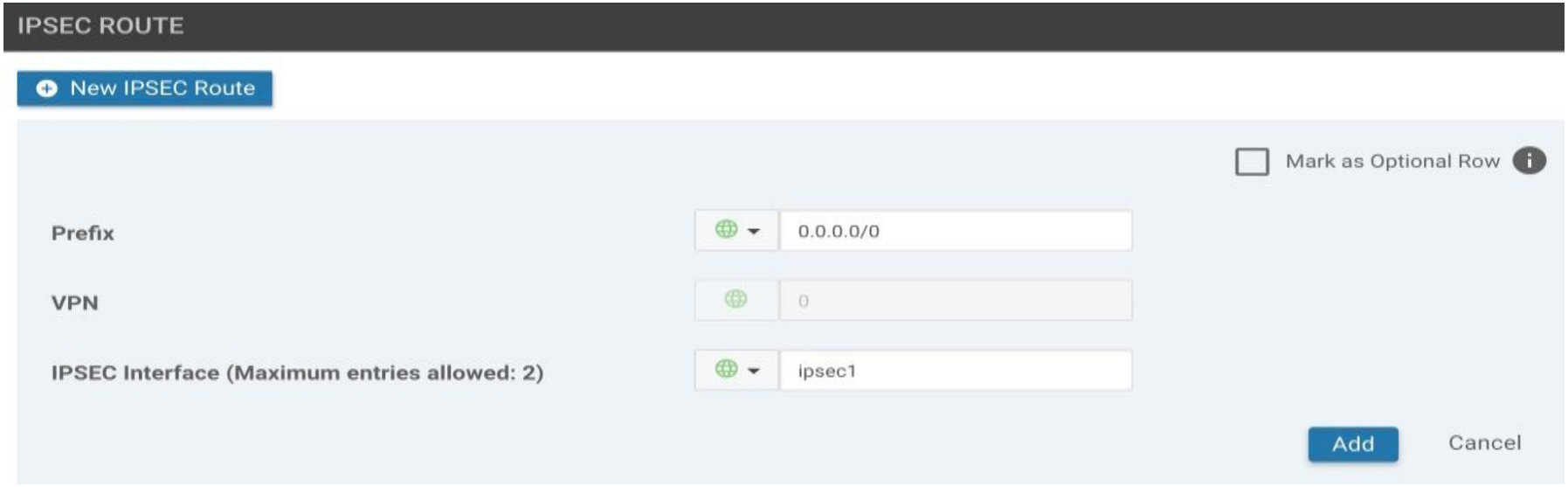


Figure 45: Provide destination prefix and IPSec tunnel interface name

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

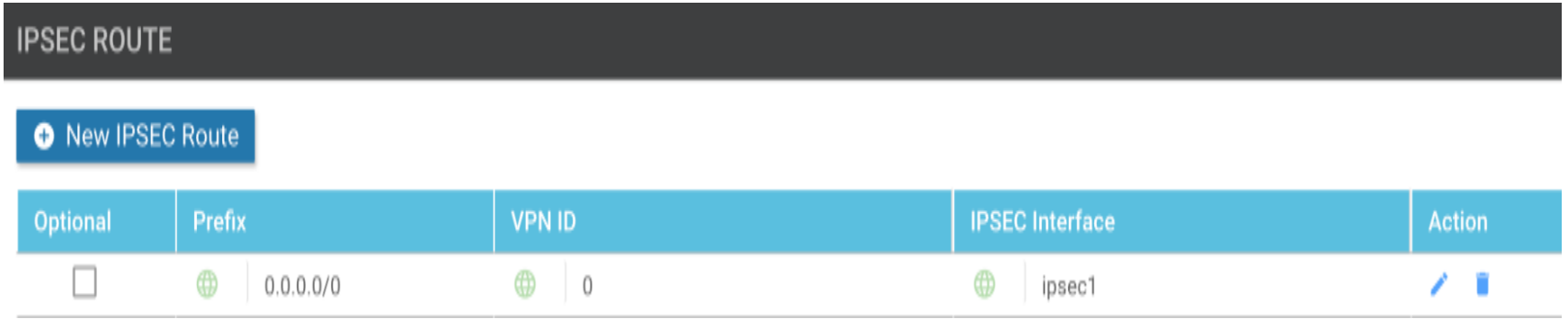


Figure 46: Check the added IPSec route

3.3.15 *Push Configuration to SD-WAN Edge Router*

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

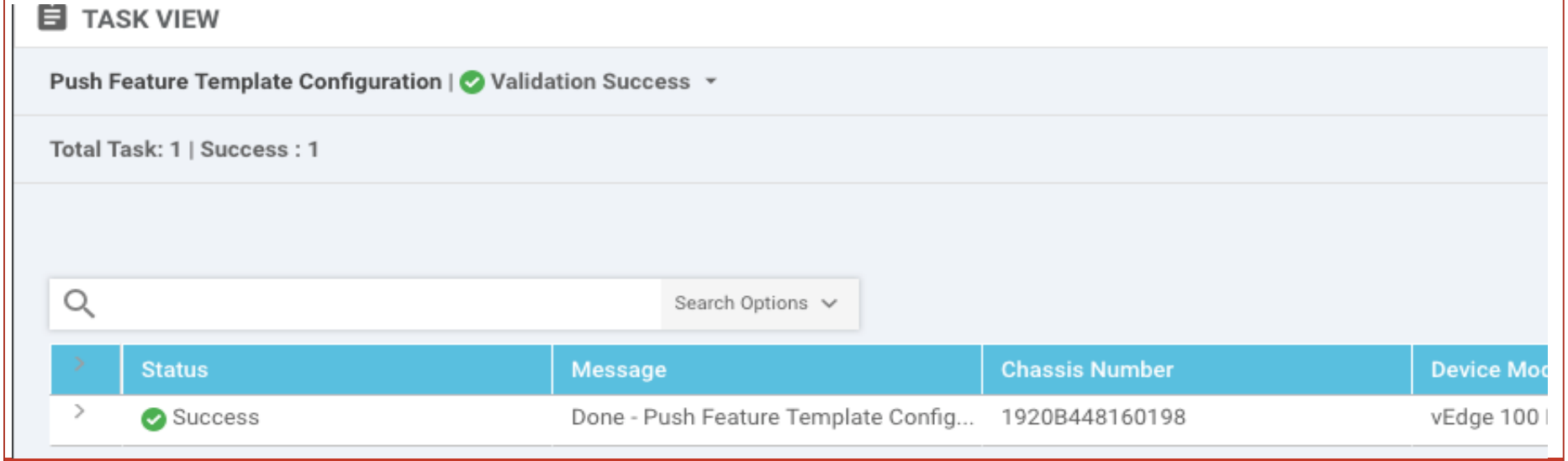


Figure 47: Successful configuration update

4 Verifying Service Configuration

4.1 Request Verification Page

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

Figure 48: Non-working Example

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

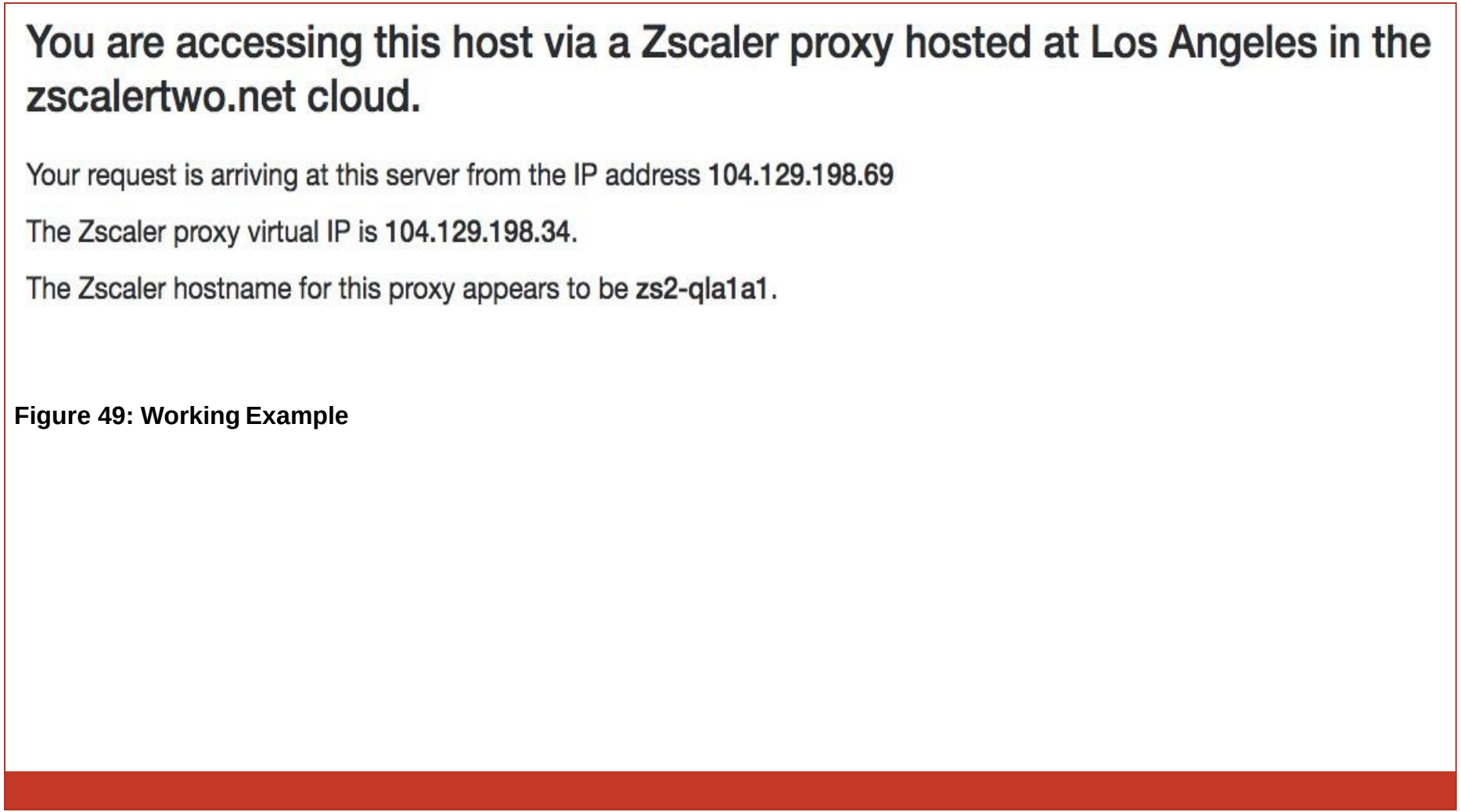


Figure 49: Working Example

5 Requesting Zscaler Support

5.1 Gather Support Information

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

5.1.1 Obtain Company ID

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

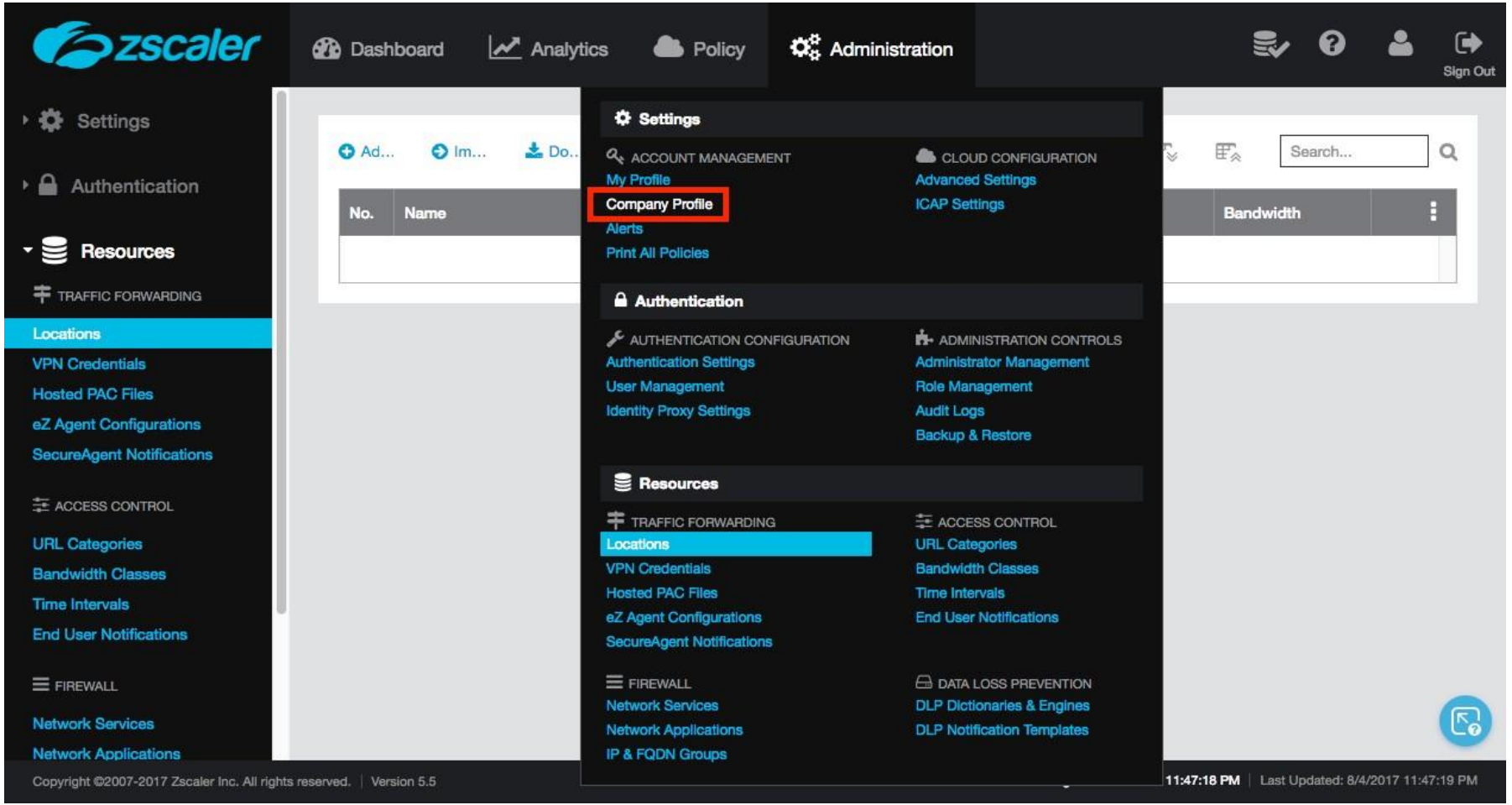


Figure 50: Obtaining Company ID

5.1.2 Save Company ID

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

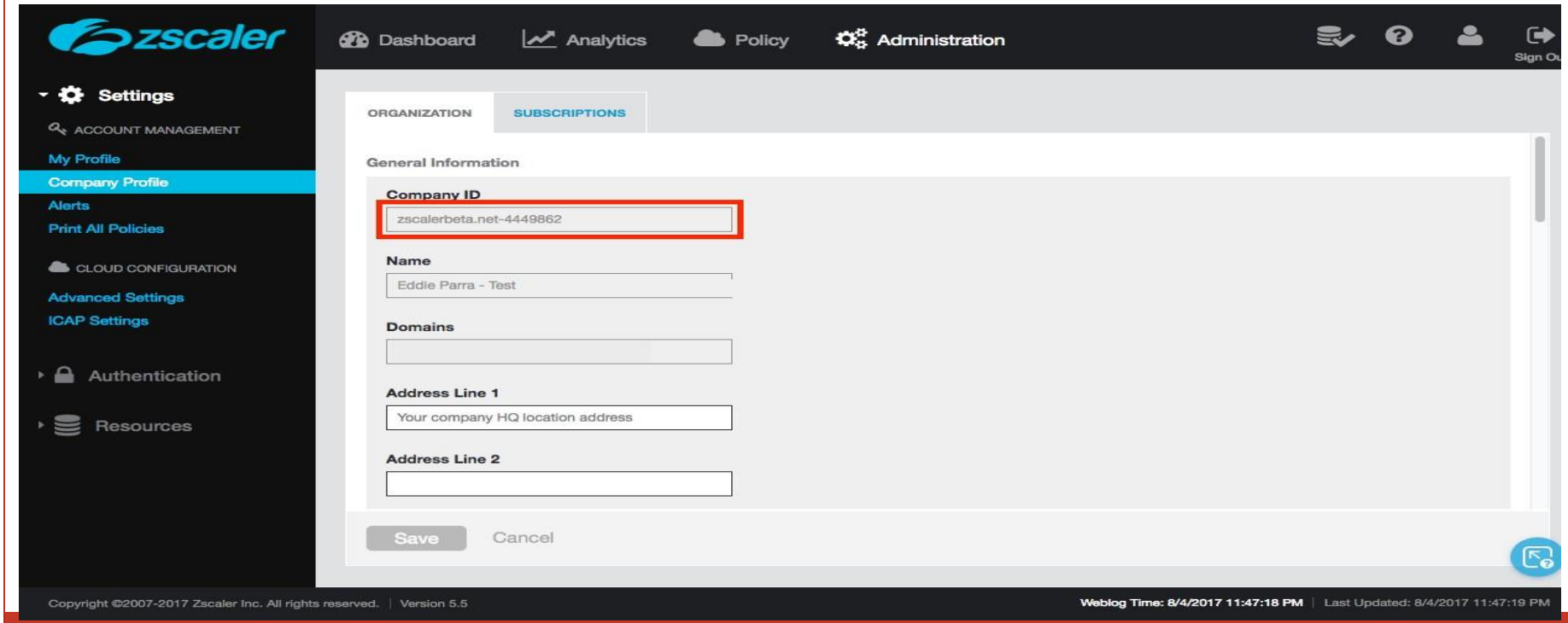


Figure 51: Save Company ID

5.1.3 Enter Support Section

Now that we have our company ID, we are ready to open a support ticket. The navigation is:
“?” -> **Support** -> and then click **Submit a Ticket**.

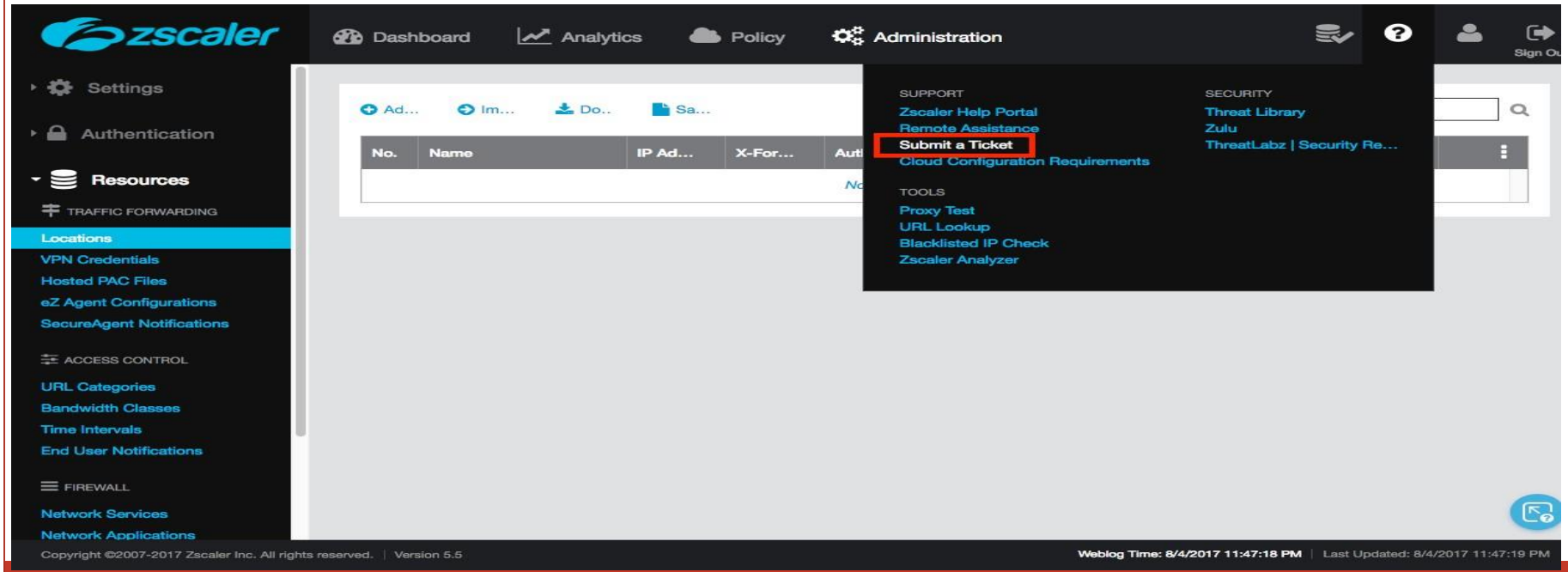


Figure 52: Enter Support Section

5.1.4 Create and Submit Support Request (GRE Provisioning)

It the example below, shows how a support ticket is generally made. Each support ticket will ask targeted questions as a Ticket Type is defined. In this example below, we are requesting GRE service be provisioned with our public IP information.

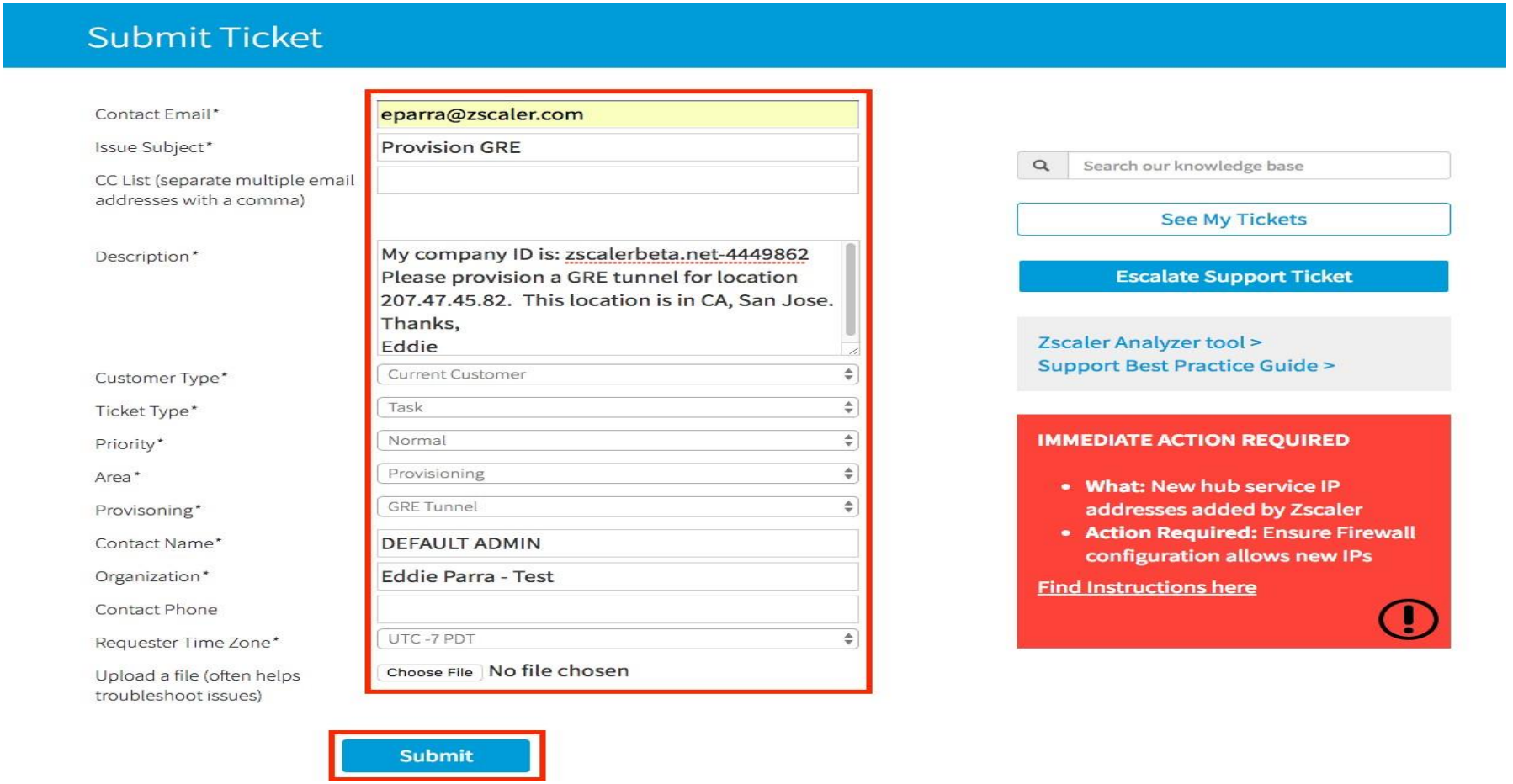


Figure 1: Creating a Support Ticket

5.1.5 Reviewing Provisioning Email

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

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

Please find the new configurations:

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

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

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

Figure 54: Provisioning Email

6 Appendix A: Zscaler Resources

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

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

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

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

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

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

7 Appendix B: Cisco SD-WAN Resources

7.1 Create a Device Template

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

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

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

Thanks ☺