Cisco SD-WAN: Enabling Direct Internet Access

Prescriptive Deployment Guide

November, 2019

Table of contents

Introduction

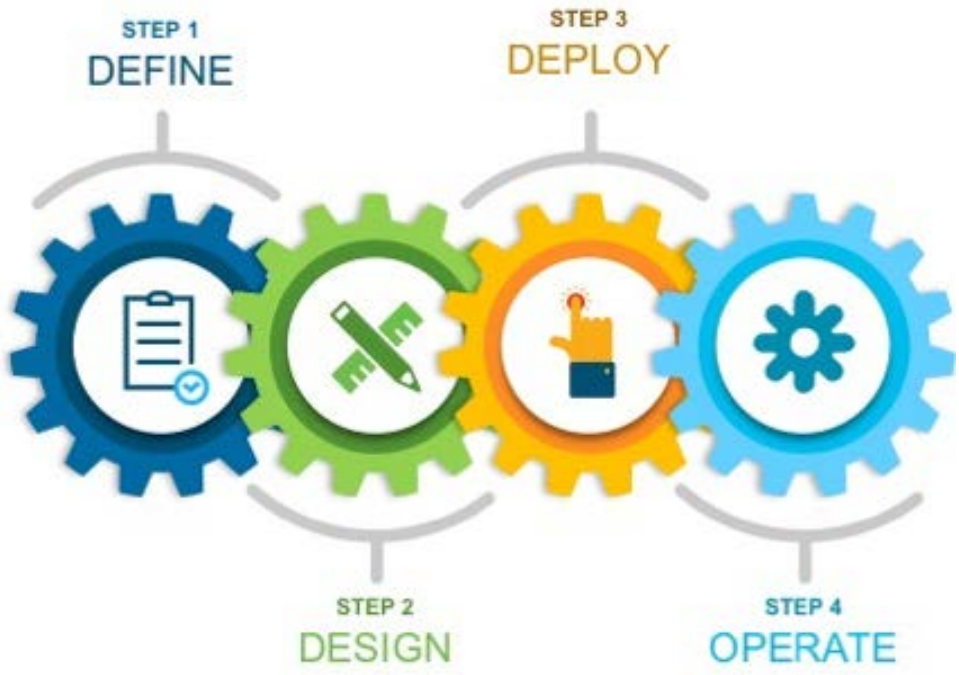
About the Solution

This solution focuses on deploying Cisco SD-WAN Direct Internet Access within remote sites to allow certain Internet-bound traffic or public cloud traffic from the branch to be routed directly to the Internet instead of tunneling the Internet traffic to a central site or datacenter for Internet access.

About the Guide

This guide is intended to provide technical guidance to design, deploy, and operate the Cisco SD-WAN Direct Internet Access solution using a mix of both Cisco IOS XE SD-WAN and vEdge devices.

Figure 1 Implementation flow



This document contains four major sections:

- The **Define** section discusses shortcomings of traditional central Internet model and introduces Cisco SD-WAN Direct Internet Access.
- The **Design** section shows the Direct Internet Access design models used, along with an in-depth explanation of individual components to support Direct Internet Access. This section also covers two major use cases.
- The **Deploy** section is divided into two parts. The first part provides information about the prerequisites necessary for deploying Direct Internet Access. The second part discusses the automated deployment of Direct Internet Access to support the two use cases presented within the **Design** section.

- The **Operate** section shows some of the monitoring and troubleshooting tools for the SD-WAN Direct Internet Access features through the vManage web-based GUI.

Define – SD-WAN Direct Internet Access Introduction

Audience

This document is intended for network design engineers, network operations personnel, and security operations personnel who wish to implement Direct Internet Access within each remote-site to allow local breakout of Internet-bound traffic directly from the branch.

Purpose of this Document

This guide will help you deploy Direct Internet Access within the Cisco SD-WAN solution and secure your branch, preparing your organization for future growth. In this guide, the deployment models discussed include a mix of both Cisco IOS XE SD-WAN and vEdge devices, collectively referred to as *WAN Edge routers*. The guide focuses on methods to reduce the consumption WAN bandwidth, providing a better user experience by enabling secure direct access to the Internet at each remote site, without routing traffic to central network locations. This is not an exhaustive guide and does not cover all the options. It does, however, highlight the best practices and assists with a successful configuration and deployment of Direct Internet Access for local Internet breakout. This guide assumes that a fully functional SD-WAN overlay is in place.

The implementation includes one data center with two Cisco vEdge 5000 routers and four remote sites with a mix of Cisco ISR4331, ISR4351, and vEdge1000 routers. Refer to the Cisco SD-WAN deployment guide for configuration, deployment guidance, and background information on the SD-WAN solution.

Overview

Digital innovation is overwhelming the branch and WAN. A majority of employees and customers work in branch offices, leading to a significant increase in devices accessing Internet-based applications. However, the digital transformation of many enterprises is hindered owing to the adoption of legacy network architectures. The traditional WAN topology backhauls all Internet traffic to the datacenters resulting in packet latency, drops, and jitter. In addition, the network is being constantly challenged with high costs associated with deployment and complex management.

One of the many ways to overcome these challenges within an organization is to use Direct Internet Access (DIA) with Cisco Software Defined WAN (SD-WAN). DIA is a component of the Cisco SD-WAN architecture in which certain Internet-bound traffic or public cloud traffic from the branch can be routed directly to the Internet, thereby bypassing the latency of tunneling Internet-bound traffic to a central site.

Benefits of using DIA include

- Reduced bandwidth consumption, latency and cost savings on WAN links by offloading Internet traffic from the private WAN circuit.
- Improved branch office user experience by providing Direct Internet Access (DIA) for employees at remote site locations

Prerequisites to Deploying Direct Internet Access

Ensure the following is in place before deploying Direct Internet Access:

- The SD-WAN controllers are set up and deployed.
- The Cisco IOS XE SD-WAN and vEdge routers are configured using device templates in order to establish a functional and secure overlay fabric to pass data traffic across the organization's distributed sites. An example of template configuration is explained in the Deploy: SD-WAN Direct Internet Access Prerequisites section of this guide.
- The network devices adjacent to the Cisco IOS SD-WAN and vEdge routers are configured.

Refer to Appendix B for the hardware models and software versions used in this guide. Refer to Appendix C for the network topology and site ID/ IP address details ,and Appendix D for portions of the supporting network device configuration templates. Appendix E details the CLI configurations of the WAN Edge devices deployed in this guide.

Design – Cisco SD-WAN Direct Internet Access Use Cases

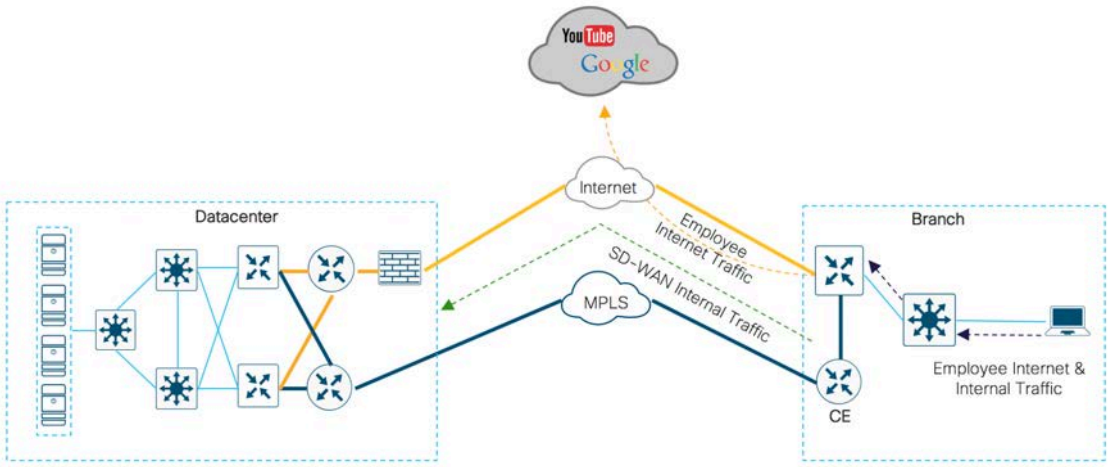
Use Cases

Two main use cases discussed in this guide are DIA for remote-site internal employees and DIA for guest users.

Use case #1 – DIA for remote-site internal employees

As shown in the figure, branch (remote-site) employees are allowed direct access to the Internet for cloud-based applications and user web access. This is achieved by configuring the WAN edge routers as an Internet exit point. Designated employee Internet traffic uses the directly connected Internet transport for direct Internet access, while the rest of the Internal traffic exits via the MPLS or INET tunnel to the destination.

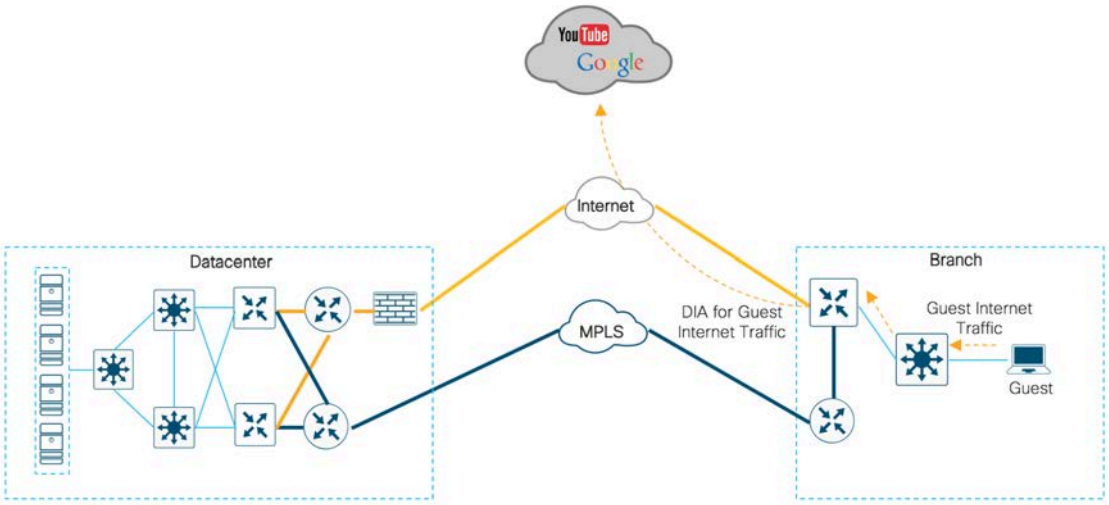
Figure 2 Internet traffic flow from employee network



Use case #2 - DIA for guest user access

Remote-site guest users access the Internet directly for user web access and cloud-based applications, without routing their traffic via the internal network and through the central site.

Figure 3 Internet traffic flow from guest network



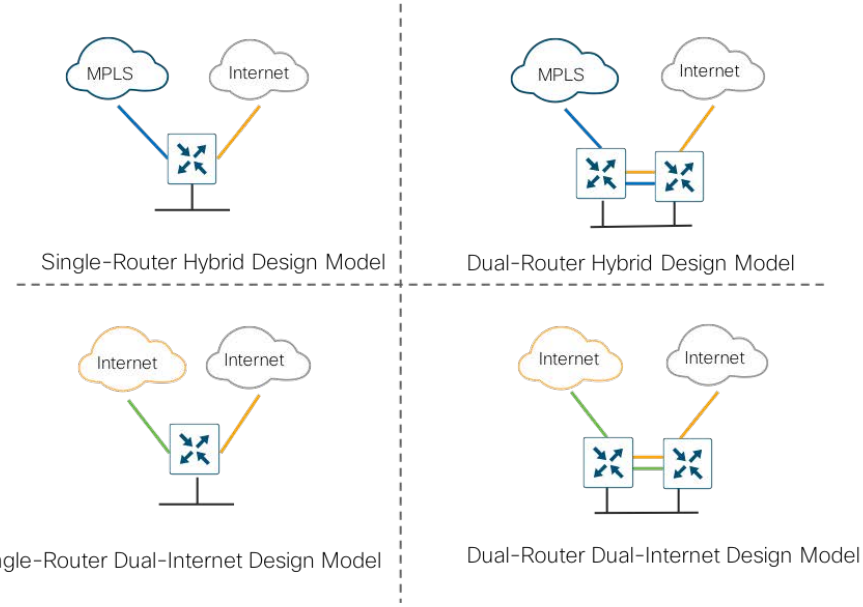
Design – Cisco SD-WAN Direct Internet Access Design Components and Considerations

Direct Internet Access Design

This guide focuses on four remote-site designs with DIA:

- Single-router remote site with MPLS WAN services and Internet connectivity, known as the single-router hybrid design model.
- Dual-router remote site with MPLS WAN services and Internet connectivity using TLOC extension, known as the dual-router hybrid design model.
- Single-router remote site with dual-Internet connections to different Internet Service Providers (ISPs), known as the single-router dual-Internet design model.
- Dual-router remote site with dual-Internet connections to different ISPs using TLOC extension, known as the dual-router dual-Internet design model.

Figure 4 Internet access design models



These designs provide configuration and guidance for enabling localized Internet access in remote office locations.

SD-WAN DIA Design Components

The design components required to establish local Internet exit at each branch are explained in the following sections.

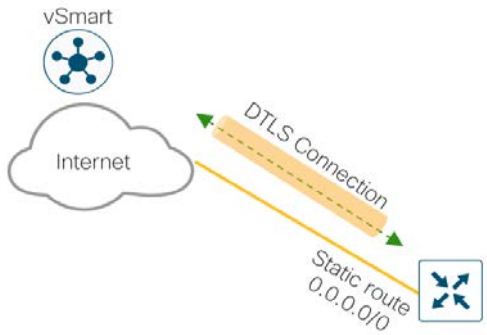
Segmentation

In DIA, segmentation is useful in keeping authenticated employee or users separate from the guest users. All SD-WAN designs are based on the use of VPN to segment the routing table, thus allowing multiple default routes to exist on the same WAN edge.

In SD-WAN, VPN 0, the transport VPN, is similar to a Front-Door VRF (FVRF) used in IWAN. In WAN Edge devices, each VPN is a VRF and completely isolated from one another. All VPNs other than VPN 0 and VPN 512 are used to carry data traffic across the overlay network. These VPNs, 1-511 and 513-65530, are referred to as service-side VPNs. For these VPNs to operate, each one must have an operational interface (or sub-interface). The remainder of what is configured in these VPNs depends on the network needs. You can configure features specific for the user segment, such as BGP and OSPF routing, VRRP, QoS, traffic shaping, and policing.

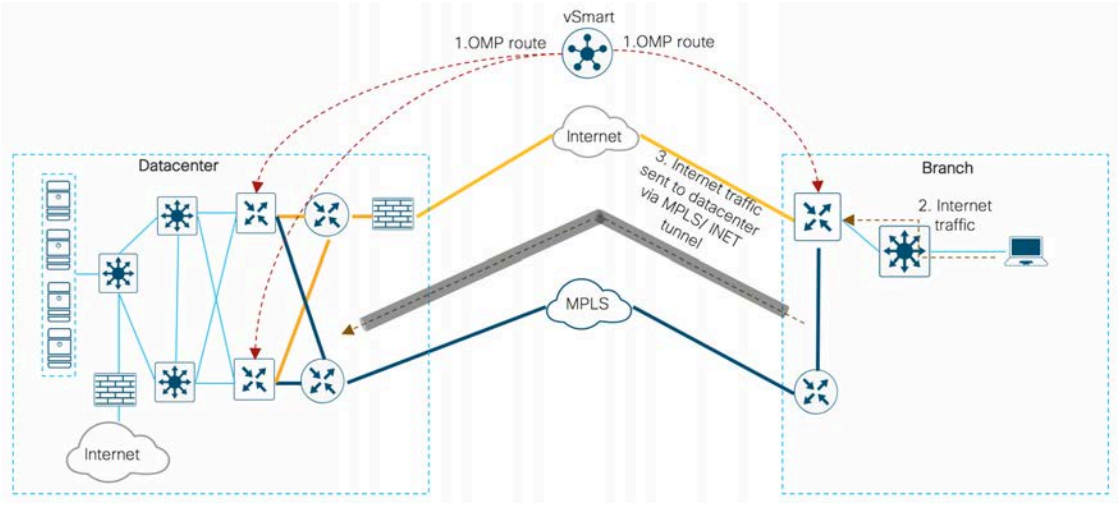
As shown in figure, if the interface in VPN 0 is assigned a static IP address, a default static route can be configured in VPN 0 pointing to the ISP device as its next hop router. Alternatively, an IP address and default route could be obtained dynamically with DHCP. After authenticating with the vBond orchestrator, the WAN edge device uses this route to authenticate itself with vSmart controller and then establish an OMP session over the DTLS tunnel.

Figure 5 Authentication via DTLS



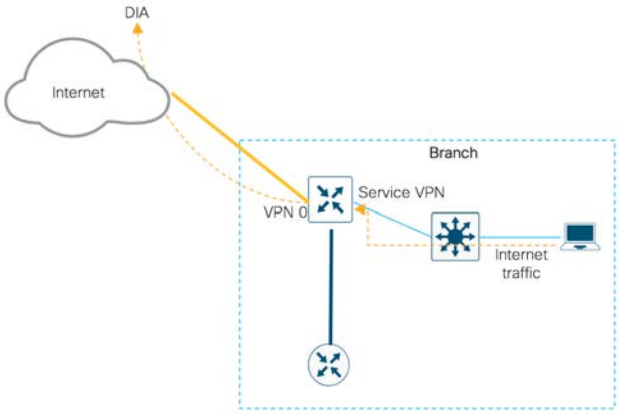
Once the IPsec tunnel is established between the WAN Edges, all Internet traffic from the site will use the OMP default route learnt over the DTLS tunnels in the service side VPN to reach the Internet via datacenter, in the absence of local branch DIA.

Figure 6 Internet exit via tunnel



As explained in figure 7, within the direct Internet model, segmentation is leveraged by deploying centralized data policies or a NAT DIA route to leak Internet traffic from the service-side VPN (VPNs 0 – 511,513 – 65530) into the Internet transport VPN (VPN 0), which allows traffic to exit directly to the Internet through the NAT- enabled interface in VPN 0.

Figure 7 Local Internet breakout



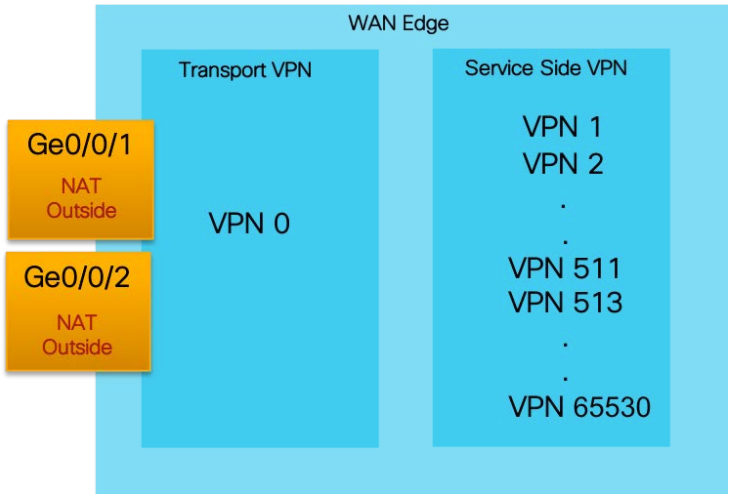
Network Address Translation

Network Address Translation (NAT) is designed for IP address conservation. It enables private IP networks that uses unregistered IP addresses to connect to the Internet. NAT usually connects two networks together by translating the private addresses in the internal network into legal addresses, before forwarding traffic to another network.

For DIA, NAT translation for packets exiting into the internet within the branch is enabled on the WAN edge devices via NAT overload. NAT overload is the mapping of multiple unregistered IP addresses to a single registered IP address by using different ports. To achieve this functionality on WAN edge devices, configure NAT on all WAN transport interfaces that face the Internet. The NAT operation on outgoing traffic is

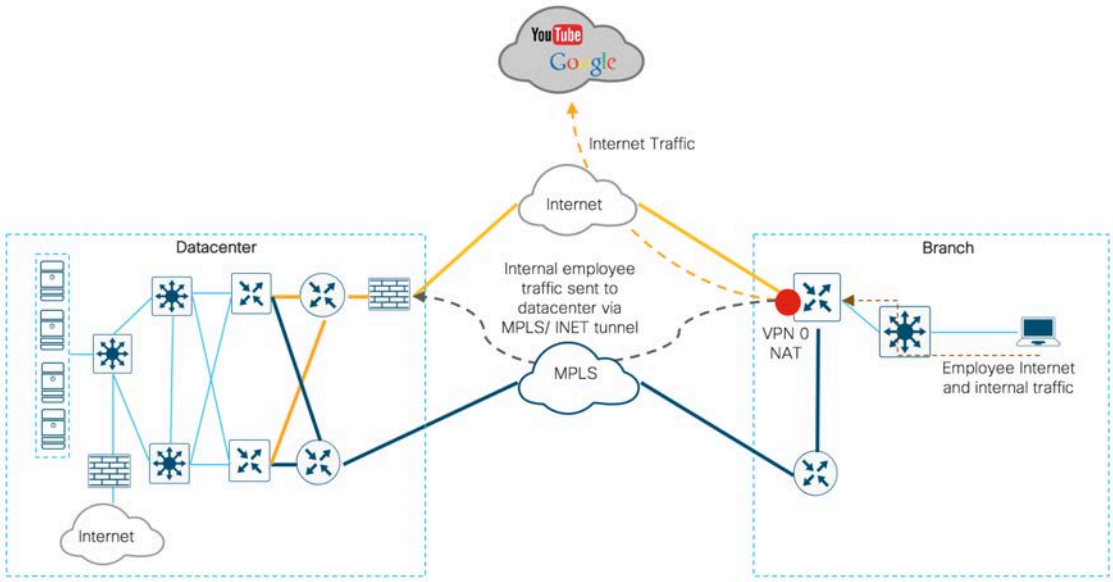
performed in VPN 0, which is always only a transport VPN. The router's connection to the Internet is in VPN 0.

Figure 8 NAT configuration on transport VPN Interface



For DIA, as shown in the figure, NAT overload can be configured on the physical Internet transport interfaces connecting to the Internet Service Provider's network. The source IP address of internal traffic destined for the Internet is translated to the interface IP address and exits directly to the Internet. The rest of the traffic remains within the overlay network and travels between two routers on the secure IPsec tunnels.

Figure 9 WAN edge acting as a NAT device



Centralized Data Policy

Data policies influence the flow of data traffic through the network based on fields in the IP packet headers and VPN membership. Centralized policies can be used in configuring application firewalls, service chaining, traffic engineering, Quality of Service (QOS), and Cflowd. Localized data policies allow you to configure data traffic at a specific site, such as ACLs, QoS, mirroring, and policing. Some centralized data policies may affect handling on the WAN edge itself, as in the case of app-route policies or a QOS classification policy.

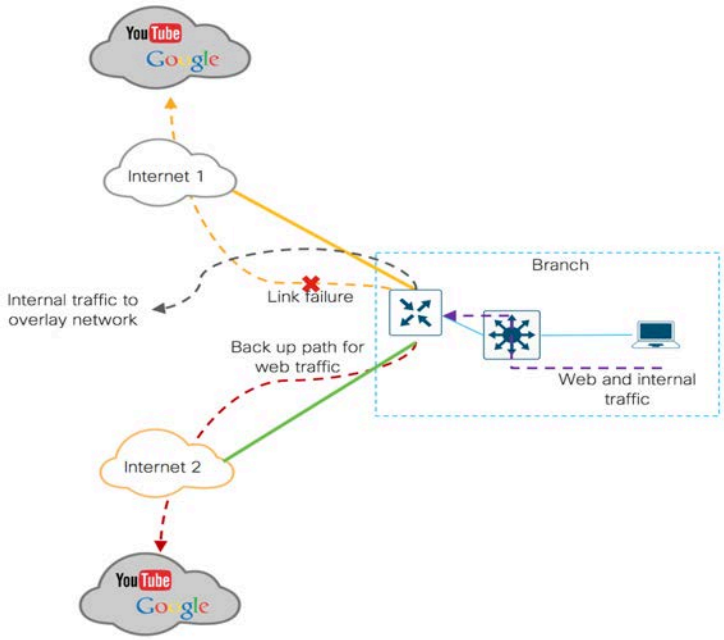
Centralized policies are built using vManage, and then stored in its database. They are then sent via NETCONF to the vSmart controller to become a part of vSmart configurations. The vSmart controller then uses OMP to send the policy parameters as updates in the routing protocol to all of the WAN edge devices. WAN edge devices learn the policy and then execute them in memory. As a result, all configurations are backed up in vManage configuration database.

In a centralized data policy, when a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packet stops. Bear this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy, because if a packet matches no parameters in any of the sequences in the policy, it is dropped and discarded by default.

Working of Centralized Data Policy

In WAN edge devices, new flows hash based on ECMP. However, it is possible to route data traffic to a specific DIA interface by setting a path preference by using a traffic data policy within the centralized policy. Such centralized policies are configured on the vSmart controller and set two actions-VPN NAT and local-TLOC color. In this case, the flow is based on the preference set within the traffic data policy (preferred and backup path). In the figure, Internet 2 (bronze) is set as backup preferred path, on failure of preferred path which is Internet 1(biz-internet), the web traffic rerouted based on the policy.

Figure 10 Centralized data policy with set path preference



Technical Tip: In IOS XE SD-WAN routers with two transports, the new flows hash according to ECMP and no path preference can be set.

Design Considerations for using Centralized Data Policy

- When applying policy definitions to a site-list, you can apply only one of each type of policy in a particular direction.
- Because a site-list is a grouping of many sites, you should be careful about not including a site in more than one site-list while designing a data policy. Ensure that the site IDs across all the site lists are unique.

Technical Tip: Data policies that come from the vSmart controller are always implicitly applied in the inbound direction.

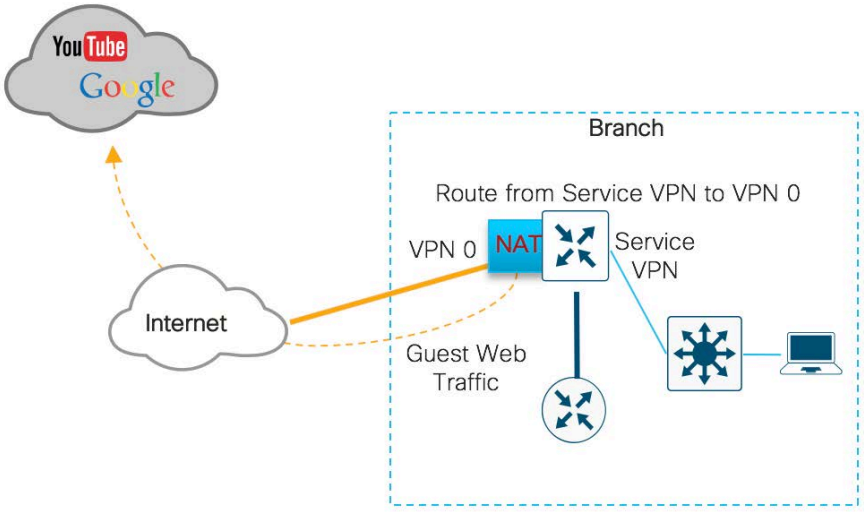
NAT DIA Route

One of the three types of NAT routes include NAT DIA route. In the DIA use case, a service side VPN is statically defined as a nat-route prefix, pointing the next hop towards VPN 0.

How NAT DIA Routes Work

While configuring a NAT DIA route, you can direct local Internet traffic to exit directly to the Internet cloud from the service-side VPN, through the next hop transport VPN, VPN 0. Refer to the figure, to see the flow of Internet traffic from service-side VPN (VPN 2) on the WAN edge device to the Internet.

Figure 11 NAT DIA route for guest traffic



Design Considerations on using NAT DIA

- Along with the configuration of a NAT DIA route within the service side VPN, ensure that you enable NAT on the Internet facing interface within VPN 0, as Internet traffic is redirected based on the NAT DIA route from the service-side to the NAT-enabled transport side interface.

- If you are using one of routing protocols on the service-side VPN, ensure that you redistribute the NAT DIA route into it. Refer to the deployment section for specific configuration.
- In NAT DIA, it is assumed that NAT/PAT is configured on one or more interfaces in VPN 0.
- By default, an IP static route has an administrative distance of 1, a NAT DIA route has a distance of 6, and OMP has a distance of 251. Therefore, the NAT DIA route overwrites the OMP advertised default to prefer the local Internet exit, instead of taking the remote data center Internet exit within a VPN.

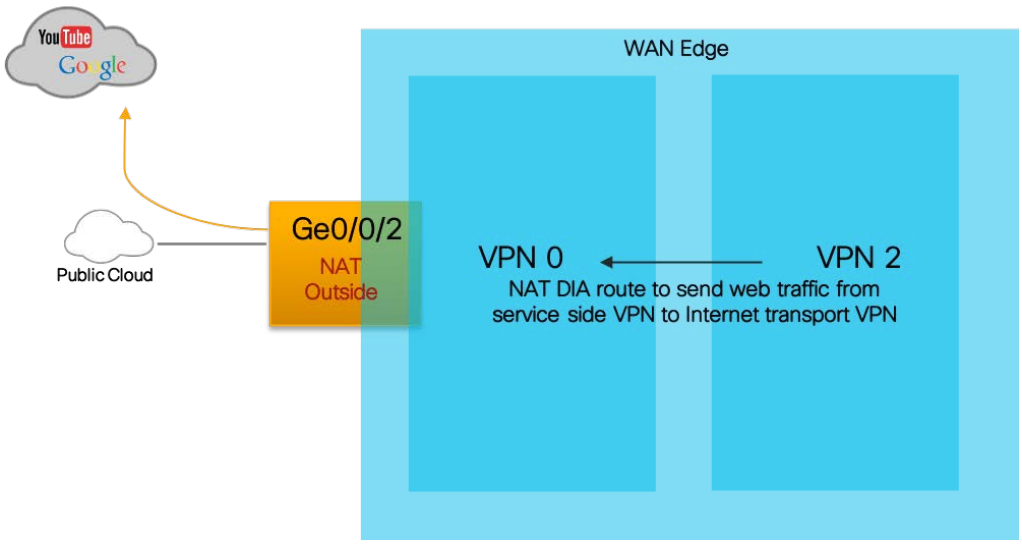
Leverage centralized data policy and NAT DIA route to deploy DIA

This section explains the adoption of centralized data policies and NAT DIA routes to allow Internet traffic to have a local Internet-exit within the branch for specific use cases. As both of the options explained below will help configure DIA , choose the one that best fits the network. For instance, to filter out traffic based on the IP prefixes and IP packet headers, you can deploy centralized data policy (option 2), if not to allow flow of all the traffic from LAN side to exit directly to the Internet from the branch, configure NAT DIA (option 1).

Option 1: DIA using NAT DIA Route

As show in the figure, traffic is routed to a NAT-enabled WAN transport VPN (VPN 0) from the service-side VPN (VPN 2) based on the destination prefix in the NAT DIA route. Then, the source IP address of the packet is translated to the interface IP address using NAT and forwarded to the destination prefix. In this scenario, traffic flowing from the LAN side is not filtered, but sent directly to the interface IP address that has been translated using NAT.

Figure 12 Traffic flow with NAT DIA route

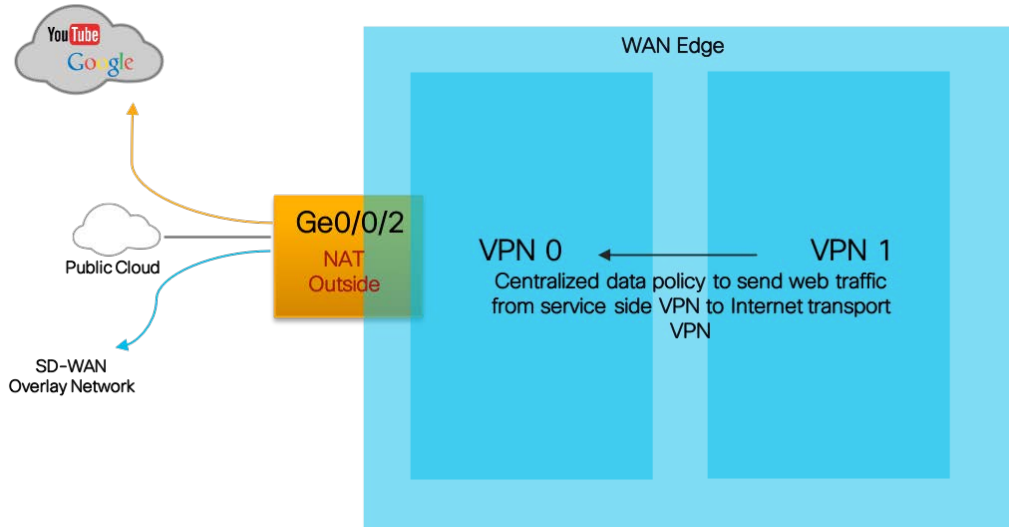


Option 2: DIA using Centralized Policy

To enable DIA from the branch, enable NAT within the Internet transport interface on the WAN Edge router, and a centralized data policy is created using vManage, which is then applied to the vSmart controller to

establish DIA within the remote-site. The LAN traffic here is filtered within the policy based on IP prefixes and IP headers and the result of the policy is pushed to the WAN edge devices. Based on the policy configuration used in this deployment scenario, the Internet traffic is redirected from the service VPN to the transport VPN (VPN 0). All other traffic remains in VPN 1 and travels directly through the IPSec data plane tunnel to the destination WAN edge router. This traffic never passes through VPN 0, therefore, it is never touched by NAT. Only the traffic destined for the public network passes from the service-side VPN to VPN 0, where its source IP address is translated using NAT.

Figure 13 Traffic flow using centralized data policy



Technical Tip: The other option to enable DIA on vEdge router platforms is by using Cloud onRamp for SaaS, for more information refer to SD-WAN: Cloud onRamp for SaaS Deployment Guide. Note that this feature is not yet supported on IOS XE SD-WAN platforms.

NAT Tracker

If the Internet or external network becomes unavailable, for example, due to a brownout, the router has no way to learn of this disruption, and it continues to forward traffic based on the policy rules. The result is that traffic that is being forwarded to the Internet is silently dropped. To prevent the Internet bound traffic from being dropped, configure the WAN edge device to track the status of the transport interface, using System Tracker, if local Internet is unavailable, redirect the traffic to the IPsec tunnel that hasn't had its address translated using NAT.

The SD-WAN System Tracker can be configured to track the status of the transport interfaces that connect to the Internet. The tracking feature is useful when NAT is enabled on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the Internet.

With tracking enabled, the router periodically probes the path to the Internet to determine whether it is up. When it detects that the path is down, the router withdraws the NAT route to the Internet destination, and reroutes the traffic to the IPsec tunnel, that doesn't have NAT enabled. The local router continues to

periodically check the status of the path to the interface. When it detects that the path is functioning again, the router reinstalls the NAT route to the Internet.

Minimum Requirements for NAT Tracker

- At a minimum, you must specify the IP address or DNS name of a destination on the Internet. This is the destination to which the router sends probes to determine the status of the transport interface. You can configure either one IP address or one DNS name. Ensure that you use an endpoint IP address that responds to HTTP/HTTPS requests.
- By default, a status probe is sent every minute (60 seconds) and only after sending three probes and receiving no responses does the router declare that the transport interface is down. To modify this value, change the time in the interval command to a value from 10 through 600 seconds and the number of retries to a value from 1 through 10.
- Also note that, by default, the router waits 300 milliseconds to receive a response from the Internet destination. To modify the time to wait for a response, change the time in the threshold command to a value from 100 through 1000 milliseconds.

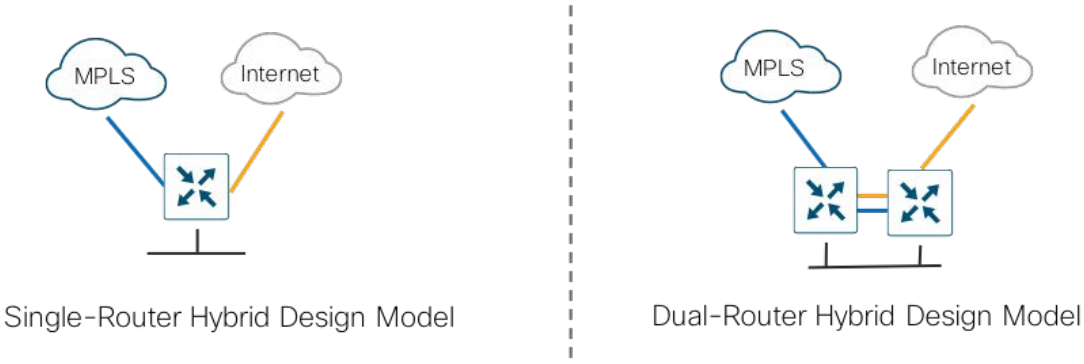
Technical Tip: You can configure up to eight interface trackers and each transport interface must have a different tracker name associated with it. The same tracker name cannot be used on all NAT interfaces.

SD-WAN DIA Failover Scenarios

Based on the type of remote-site, the WAN edge design varies. While most remote sites are designed with a single-router WAN edge, there are certain dual-router, remote-site branches that run business critical applications that justify the need for redundancy to remove a single point of failure.

In the figure below, the remote sites are classified as single and dual SD-WAN edge devices with Internet failover to central Internet model in the event of local Internet link failure.

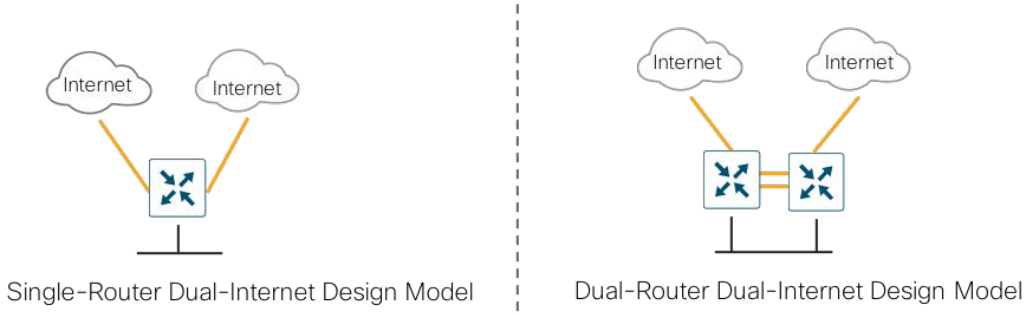
Figure 14 Single-router and dual-router hybrid design models



In the SD-WAN single-router, hybrid design model and SD-WAN dual-router hybrid design model, a failure of the local Internet link causes failover of Internet traffic to the central Internet model. Therefore, the Internet traffic exits via the central site or datacenter to the internet.

In the figure below, the remote sites are classified as single and dual SD-WAN edge devices with Internet failover to secondary Internet link in the event of primary Internet link failure.

Figure 15 Single router and dual router dual-internet design models



Single-Router Dual-Internet Design Model

Dual-Router Dual-Internet Design Model

In the SD-WAN single-router, dual-Internet design model and dual-router, dual-Internet design model, redundancy allows for local Internet connectivity to failover to the secondary local Internet connection on WAN edge device.

SD-WAN L3 Distribution Switch

The switch connected to the WAN edge device must be configured with either a default/static route to direct traffic to the Internet-connected WAN Edge device or through redistribution into a dynamic protocol that runs between them. In this deployment scenario, the traffic is segmented. Guest traffic traverses through GUEST VRF, while the rest of the traffic follows the global routing table.

SD-WAN Remote-Site Design Details

In the following section, each of the components explained earlier are tied together and the design details per remote-site are explained in depth.

Note that the common technical details are repeated in each section.

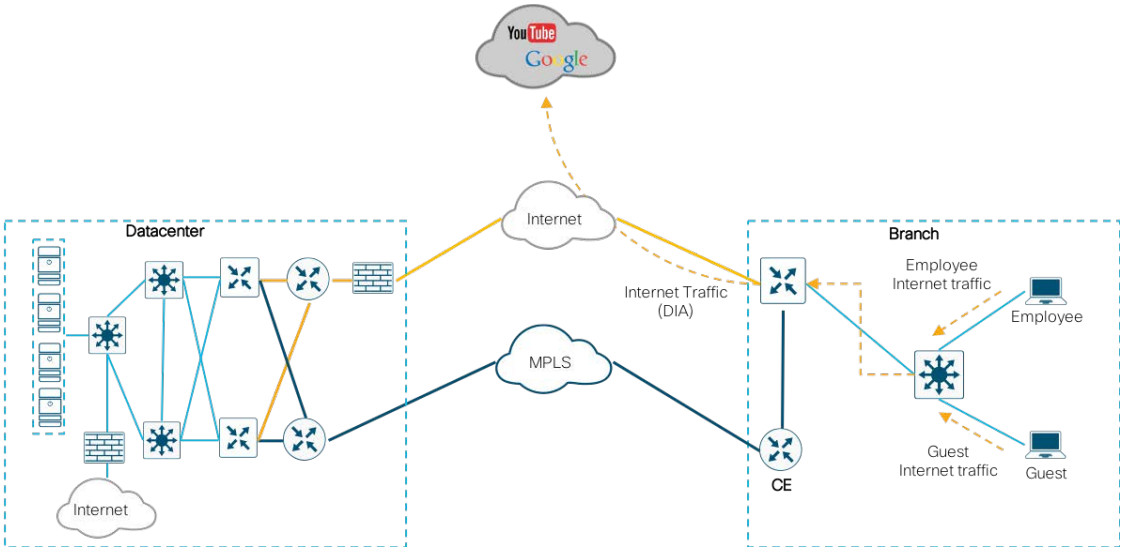
SD-WAN Single-Router Hybrid Remote-Site Design

The remote-site is configured with a single WAN edge router with MPLS tunnel and Internet transport tunnel. In this hybrid design with DIA configured, the Internet traffic is routed outside the tunnel to exit via the local Internet interface. The configuration is based on maintaining the Internet path as the primary one with failover to the central site Internet connectivity using the MPLS based tunnel.

On the Internet facing interface, DHCP can be used to obtain an IP address from the Internet Service Provider with the WAN edge device installing a default route into transport VPN from the ISP. Alternatively, a

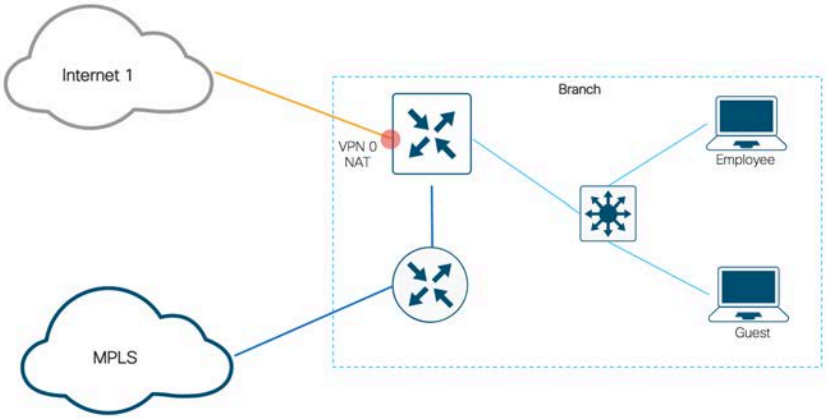
static IP address and static route can be configured on the WAN edge device as done in this deployment. As shown in the figure below, the local Internet traffic exits directly to the Internet from the branch using this route.

Figure 16 Remote site DIA exit



NAT is enabled on the Internet transport interface.

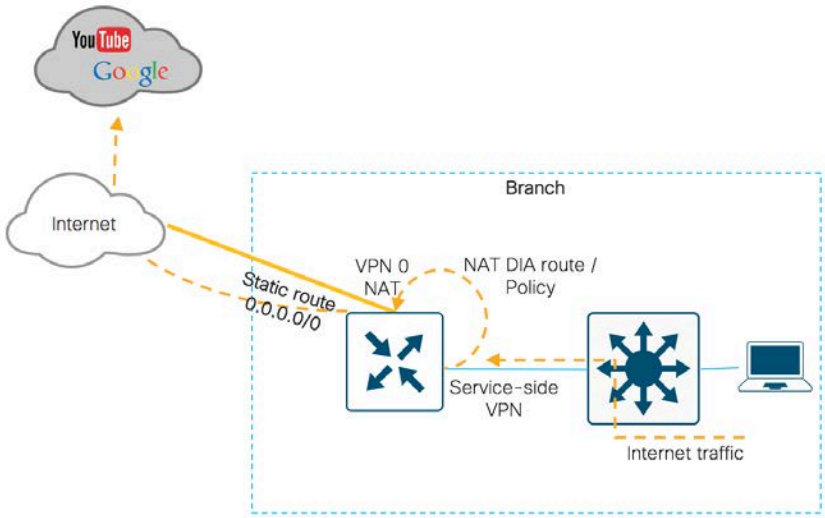
Figure 17 NAT Enabled Interfaces



As discussed within the components section, to enable DIA, a centralized data policy can be configured to filter the incoming traffic based on match/action and route the traffic from service side VPN to transport side

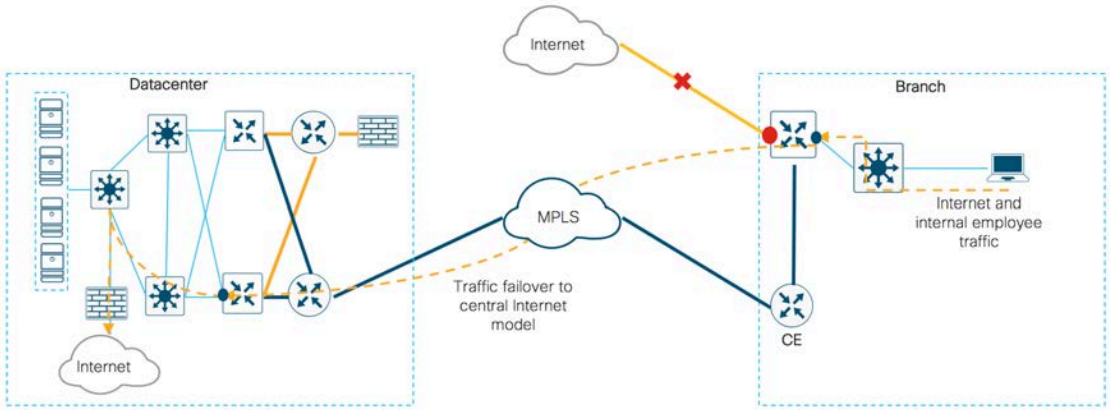
VPN. Another solution for DIA is to configure IP NAT route using device templates to route traffic from service side to the transport side VPN 0 NAT enabled interface.

Figure 18 Internet traffic flow using DIA route or data policy



In figure 19, MPLS based transport tunnel is used as a backup path for all Internet traffic on failure of the local Internet connection. A default route is advertised from the central site to roll back to the central Internet model.

Figure 19 Internet traffic flow via datacenter



On WAN edge routers, tracking the interface status is useful when NAT on the transport interface in VPN 0 allows data traffic to flow directly to the Internet. On enabling transport tunnel tracking, the software periodically probes the path to the Internet to determine whether it is up, based DNS or endpoint IP address.

If the software detects that this path is down, the NAT feature on the interface is disabled and all Internet traffic exits via the central Internet model. Ensure that you use an endpoint IP address that responds to HTTP/HTTPS requests. For instance, Google DNS server 8.8.8.8 cannot be used as an endpoint IP address.

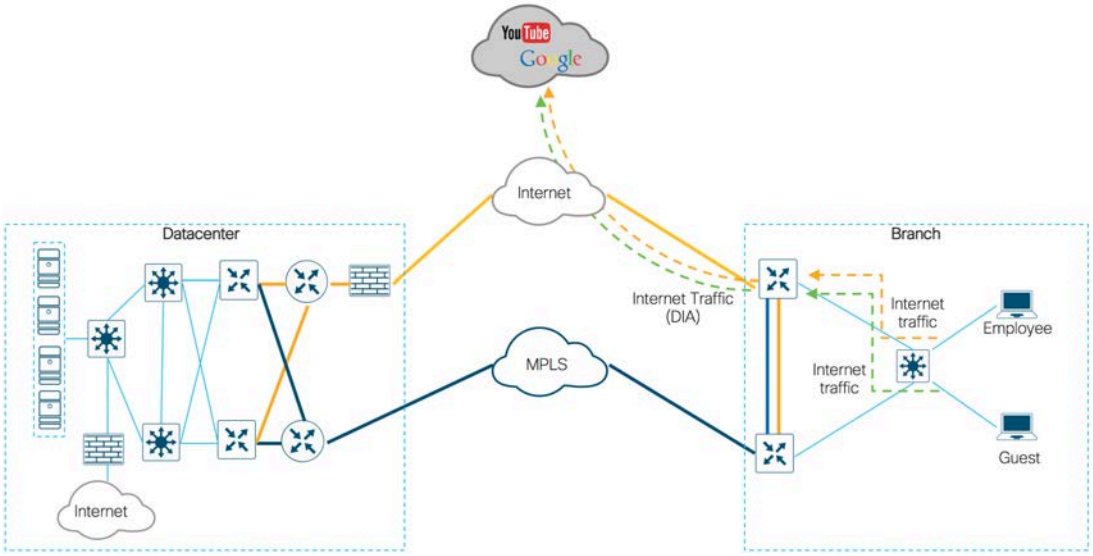
Technical Tip: NAT tracker is currently unavailable on devices running IOS XE SD-WAN software.

SD-WAN Dual-Router Hybrid Remote-Site Design

In this design, the remote-site is configured with a single WAN edge router with the MPLS tunnel and Internet transport tunnel. In this hybrid design with DIA configured, the Internet traffic is routed outside the tunnel to exit via the local Internet interface. The configuration is based on maintaining the Internet path as the primary one with failover to the central site Internet connectivity using the MPLS based tunnel via TLOC interface.

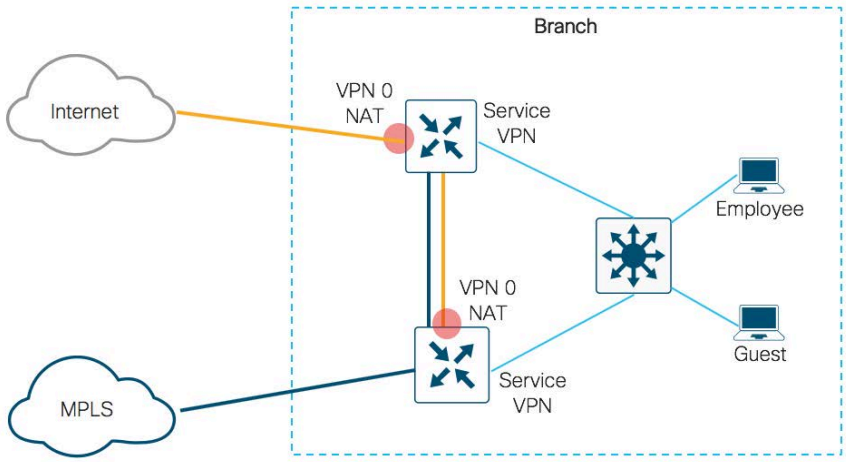
On the Internet facing interface, DHCP can be used to obtain an IP address from the Internet Service Provider with the WAN Edge device installing a default route into transport VPN from the ISP. Alternatively, a static IP address and static route can be configured on the WAN Edge device as done in this deployment. As shown in the figure below, the local Internet traffic exits directly to the Internet from the branch using this route.

Figure 20 Remote-site DIA exit



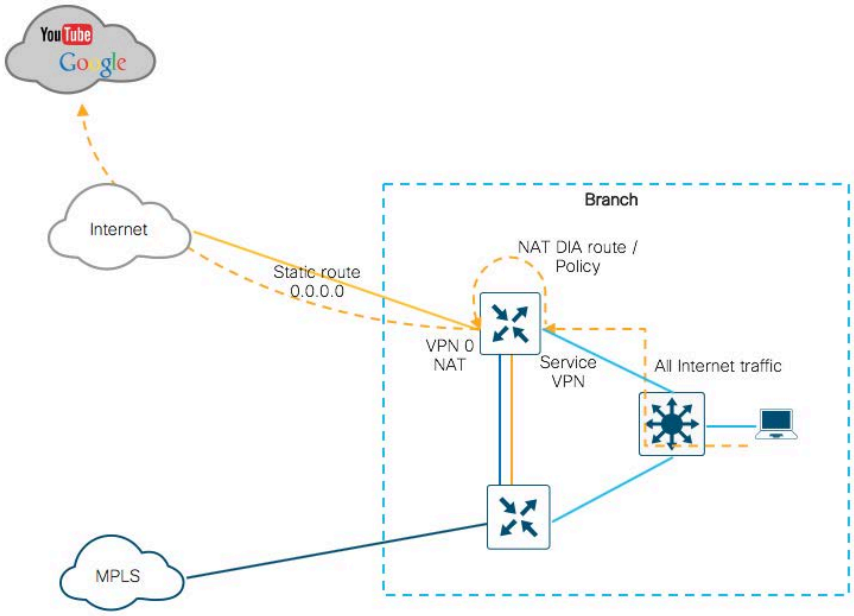
In the figure below, NAT is enabled on the Internet transport interfaces in both the WAN edge devices. Note that here NAT is also enabled on the TLOC interface to allow the internet traffic that hits the WAN Edge device (device with a direct MPLS transport) to flow via the TLOC port towards the device that has the Internet transport interface. The internet traffic then exits from the second WAN edge device (device connected to the Internet transport) directly to the Internet without being routed to the datacenter.

Figure 21 NAT enabled Interfaces



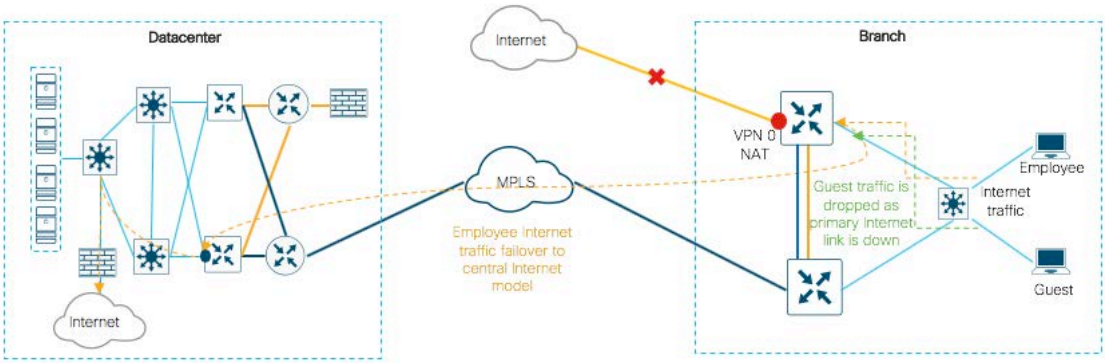
As discussed in the components section, to enable DIA, a centralized data policy can be configured to filter the incoming traffic based on match/action and route the traffic from service side VPN to transport side VPN. Another solution for DIA is to configure IP NAT route using device templates to route traffic from service side to the transport side VPN 0, NAT-enabled interface.

Figure 22 Internet traffic flow using DIA route or data policy



In figure 23, MPLS-based transport tunnel is used as a backup path for all Internet traffic when the local Internet connection fails. A default route is advertised from the central site over the MPLS tunnel to roll back to the central Internet model.

Figure 23 Internet traffic failover



On WAN edge routers, tracking the interface status is useful when NAT on the transport interface in VPN 0 allows data traffic to flow directly to the Internet. At a minimum, the tracker name along with endpoint IP address is specified. On enabling transport tunnel tracking, the software periodically probes the path to the Internet to determine whether it is up based endpoint-dns-name or endpoint-IP address. If the software detects that this path is down, NAT is disabled on the interface and all Internet traffic exits via the central Internet model. Ensure that you use an endpoint IP address that responds to HTTP/HTTPS requests and apply only one tracker to an interface. For instance, Google DNS server 8.8.8.8 cannot be used as an endpoint IP address.

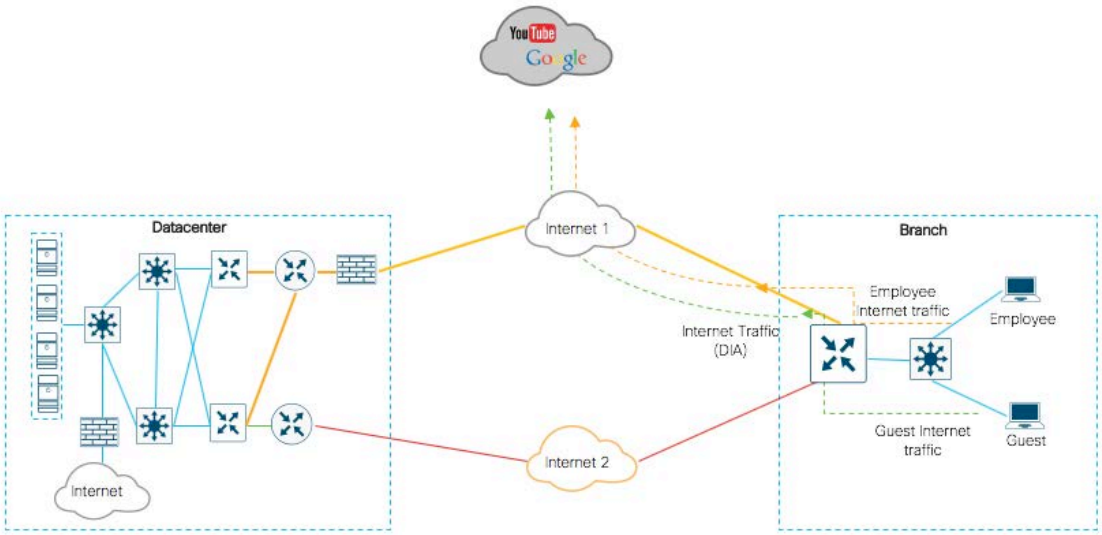
Technical Tip: NAT tracker is currently unavailable on devices running IOS XE SD-WAN software.

SD-WAN Single-Router Dual Internet Remote-Site Design

The remote-site is configured with a single WAN Edge router with two Internet tunnels. In this dual-internet design with DIA configured, the Internet traffic is routed outside the tunnel to exit via the local Internet interface. The configuration is based on maintaining dual Internet path with traffic load-balancing for SD-WAN XE devices and vEdge router platforms.

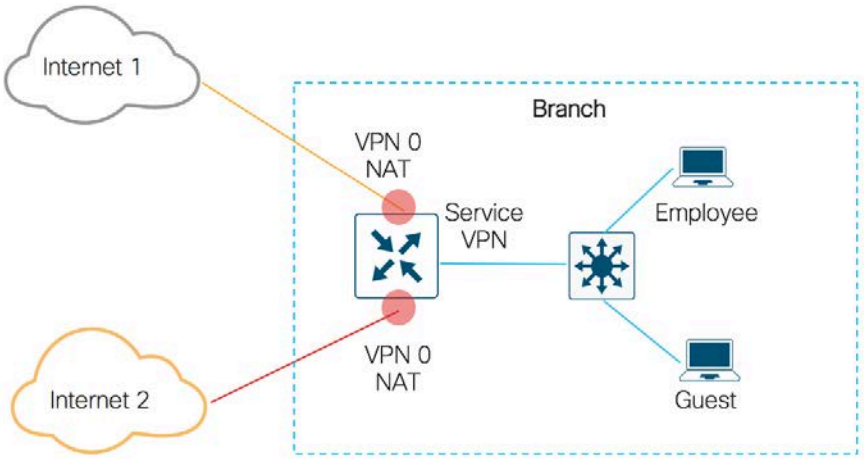
On the Internet facing interface, DHCP can be used to obtain an IP address from the Internet Service Provider with the WAN edge device installing a default route into transport VPN from the ISP. Alternatively, a static IP address and static route can be configured on the WAN Edge device as done in this deployment. As shown in the figure below, the local Internet traffic exits directly to the Internet from the branch using this route.

Figure 24 Remote-Site DIA exit



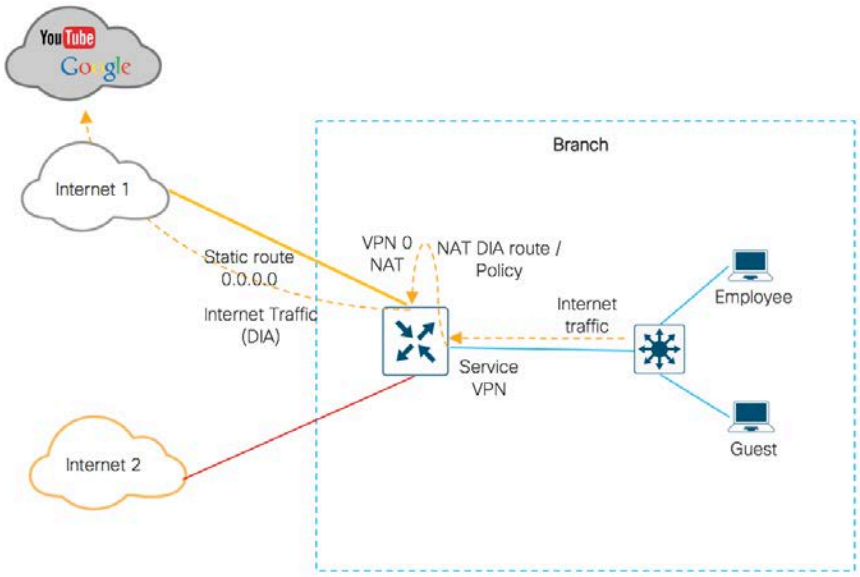
In the figure below, NAT is enabled on the Internet transport interface in both WAN Edge devices.

Figure 25 NAT enabled Interfaces



As discussed in the components section, to enable DIA, a centralized data policy can be configured to filter the incoming traffic based on match/action and route the traffic from service side VPN to transport side VPN. Another solution for DIA is to configure an IP NAT route using device templates to route traffic from service side to the transport side VPN 0, NAT-enabled interface.

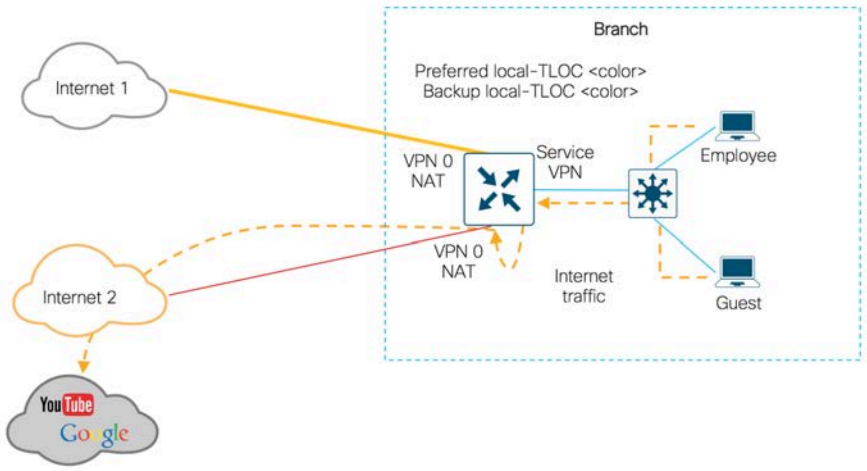
Figure 26 Internet traffic flow using DIA route or data policy



When a WAN edge router has two or more NAT interfaces, and hence two or more DIA connections to the Internet, data traffic is forwarded on the NAT interfaces using ECMP by default. To direct data traffic to a specific DIA interface, a centralized data policy can be configured on the vSmart controller that sets two actions—NAT and local-TLOC color. In the local-TLOC color action, the preferred color of the TLOC that connects to the desired DIA connection is chosen. In this design example, Internet 1 is labelled color biz-

internet and Internet 2 is labelled color bronze. The local-TLOC color is set as biz-internet with failover to bronze. When Internet 1 is down, web traffic fails over to Internet 2.

Figure 27 Path preference for Internet traffic



Technical Tip: On IOS XE SD-WAN routers, the traffic can be forwarded to the NAT interfaces based on ECMP, as path preference is not yet supported on these router platforms.

On WAN edge routers, tracking the interface status is useful when NAT on the transport interface in VPN 0 allows data traffic to flow directly to the Internet. At a minimum, the tracker name along with the endpoint IP address is specified. On enabling transport tunnel tracking, the software periodically probes the path to the Internet to determine whether it is up based on endpoint-dns-name or endpoint-IP address. If the software detects that this path is down, NAT is disabled on the interface and all Internet traffic exits via the central Internet model. Ensure that you use an endpoint IP address that responds to HTTP/HTTPS requests and apply only one tracker to an interface. For instance, Google DNS server 8.8.8.8 cannot be used as an endpoint IP address.

Technical Tip: In this design, two different NAT tracker names must be configured and enabled under each NAT interface. NAT must be enabled before the trackers are configured.

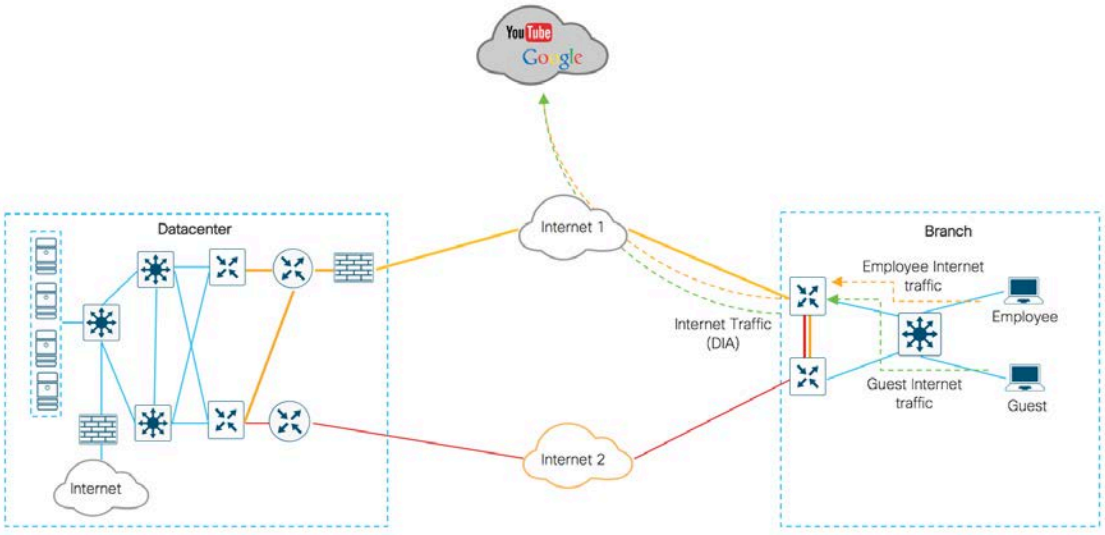
SD-WAN Dual-Router Dual Internet Remote-Site Design

The remote-site is configured with dual WAN edge routers and two Internet transport links. In this dual-internet design with DIA configured, the Internet traffic is routed outside the tunnel to exit via the local Internet interface. The transport links are labelled with a specific TLOC color, for instance biz-Internet, bronze etc. In this design, the primary local Internet is Internet transport biz-internet and on link failure, a fail-over is initiated to the bronze Internet transport.

On the Internet facing interface, DHCP can be used to obtain an IP address from the Internet Service Provider with the WAN edge device installing a default route into transport VPN from the ISP. Alternatively, a static IP address and static route can be configured on the WAN edge device as done in this deployment. As

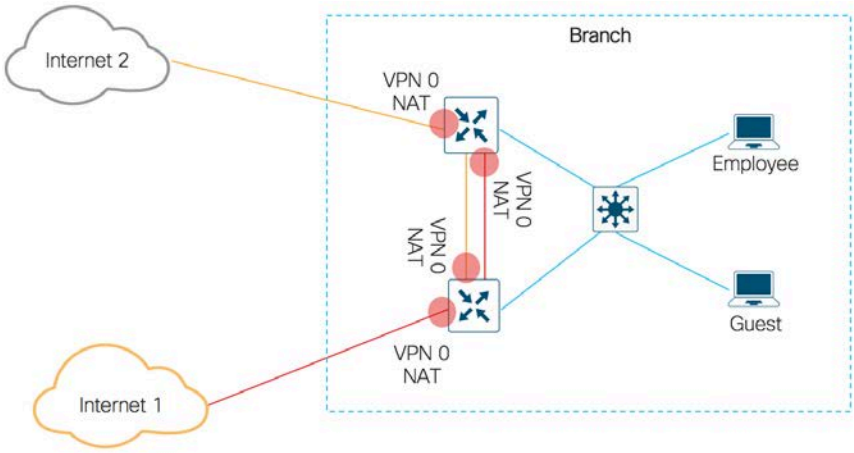
shown in the figure below, the local Internet traffic exits directly to the Internet from the branch using this route.

Figure 28 Remote-Site DIA exit



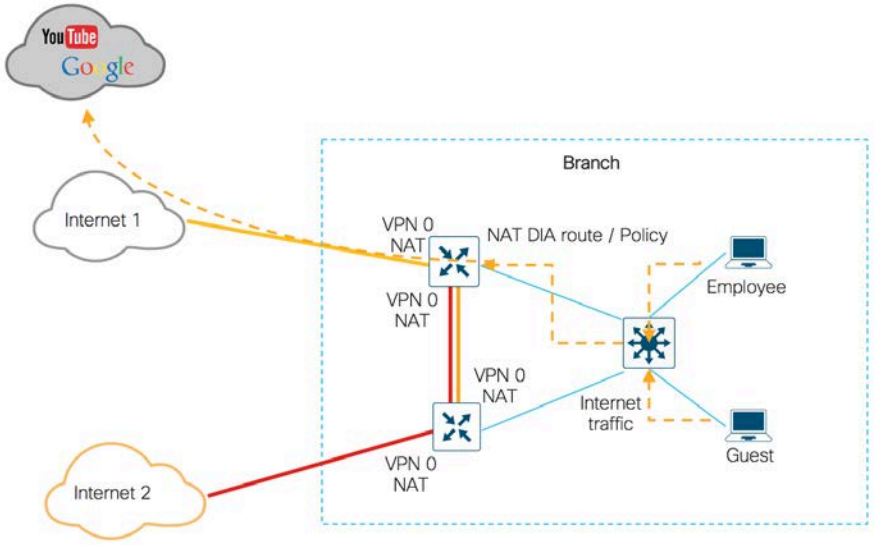
In the figure below, NAT is enabled on the Internet transport interface in both WAN Edge devices. Note that, NAT here is enabled on the TLOC Interfaces to allow flow of Internet traffic via the TLOC interface to then exit directly via the Internet transport interface of the second WAN edge device. This configuration is particularly useful in a situation where one of the two Internet transports has failed.

Figure 29 NAT enabled Interfaces



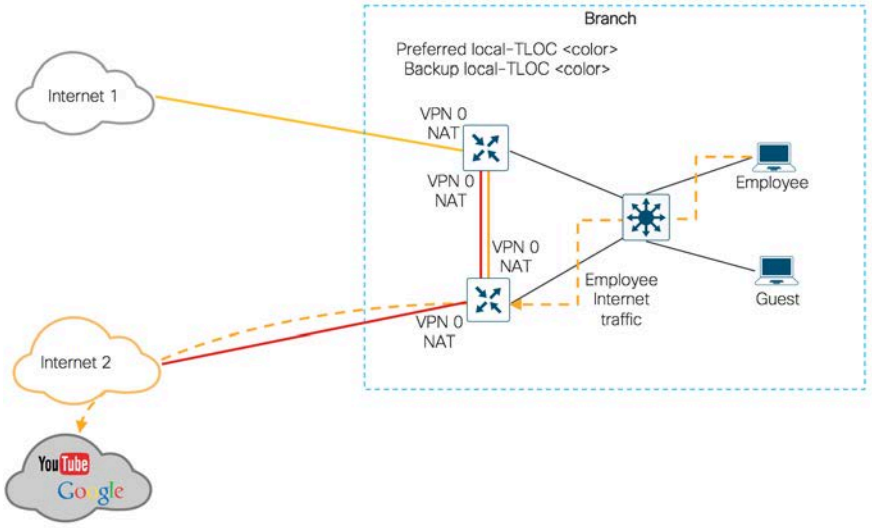
As discussed in the components section, to enable DIA, a centralized data policy can be configured to filter the incoming traffic based on match/action and route the traffic from service side VPN to transport side VPN. Another solution for DIA is to configure IP NAT route using device templates to route traffic from service side to the transport side (VPN 0) NAT enabled interface.

Figure 30 Internet traffic flow using DIA route or data policy



When a WAN edge router has two or more NAT interfaces, and hence two or more DIA connections to the Internet, by default, data traffic is forwarded on the NAT interfaces using ECMP. To direct data traffic to a specific DIA interface, a centralized data policy can be configured on the vSmart controller that sets two actions—NAT and local-TLOC color. In the local-TLOC color action, the preferred color of the TLOC that connects to the desired DIA connection is chosen. In this design example, Internet 1 is labelled color biz-internet and Internet 2 is labelled color bronze. The local-TLOC color is set as biz-internet with failover to bronze. When Internet 1 is down, web traffic fails over to Internet 2.

Figure 31 Path preference for Internet traffic



Note that path preference is set for the vEdge platform to biz-internet in this design. If the interface configured with color biz-internet goes to down state, the Internet traffic automatically chooses the second Internet link (Bronze) as the DIA path. With centralized policy configured, if the Internet link on WAN edge device wherein Biz-Internet color is configured on the main physical interface goes down, and Internet traffic is being routed towards this router from the TLOC interface of the neighboring WAN edge device, the traffic will be blackholed. To prevent this, a possible solution is to configure NAT DIA route to enable DIA with system tracker.

Technical Tip: On IOS XE SD-WAN routers, traffic forwarding to the NAT interfaces using path preference is not yet supported on IOS XE SD-WAN platforms.

On WAN edge routers, tracking the interface status is useful when NAT on the transport interface in VPN 0 allows data traffic to flow directly to the Internet. At a minimum, the tracker name along with endpoint IP address is specified. On enabling transport tunnel tracking, the software periodically probes the path to the Internet to determine whether it is up based on endpoint-dns-name or endpoint-IP address. If the software detects that this path is down, NAT is disabled on the interface and all Internet traffic exits via the central Internet model. Ensure that you use an endpoint IP address that responds to HTTP/HTTPS requests and apply only one tracker to an interface. For instance, Google DNS server 8.8.8.8 cannot be used as an endpoint IP address.

Technical Tip: In this design, two different NAT tracker names must be configured and enabled under each NAT interface. NAT must be enabled before the trackers are configured.

Deploy - Cisco SD-WAN Direct Internet Access Prerequisites

Prerequisites

This section of the guide focuses on the prerequisites for each remote site design which involves onboarding devices into the vManage NMS, building and deploying templates, followed by validating NAT configuration.

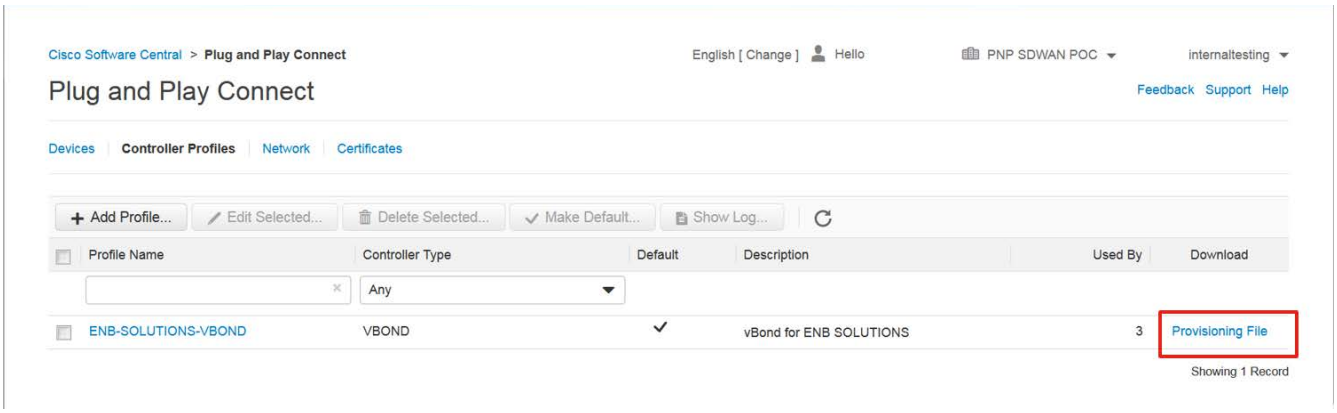
Process: Verify WAN Edge router prerequisites

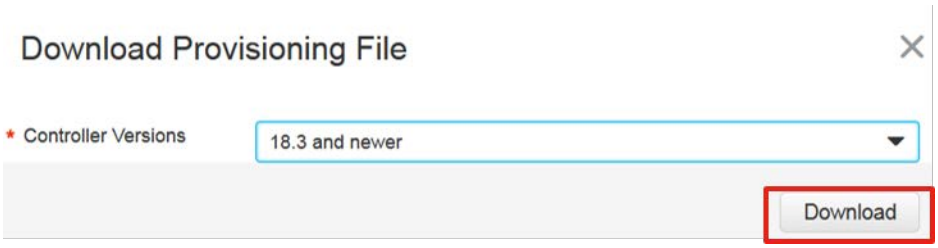
For the procedures below, you will need to login to the vManage web console using the IP address or fully qualified domain name of your vManage instance. For example:

https://<vManage_ipaddr_or_FQDN>:8443/

Step 1: Verify Cisco Edge devices in vManage

1. In order to add WAN edge devices to the list of available devices, navigate to **Plug and Play Connect** on Cisco Software Central and provision the devices based on a serial and chassis numbers. An authorized serial file of .viptela format is generated and uploaded to the vManage dashboard.



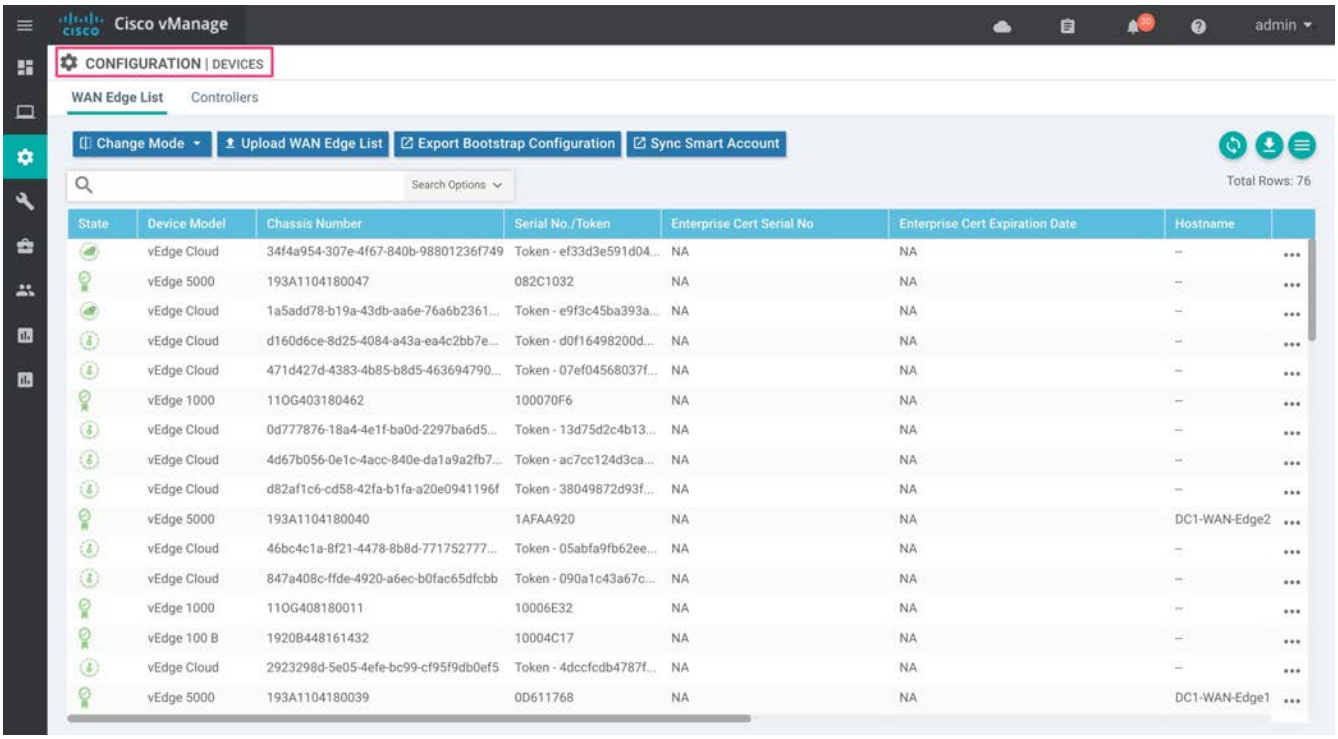


The serial file list contains both vEdge and SD-WAN XE routers. Legacy serial files for vEdge routers are available on the Cisco SD-WAN support website. However, most of these serial files are also available within Plug and Play (PnP) Connect Portal now.

Technical Tip: The Sync Smart Account option introduced in version 18.3 and above allows vManage to automatically connect to the PnP Connect portal and pull up the authorized serial file. For more details, refer to the latest SD-WAN Deployment Guide.

2. In the navigation panel on the left of the screen, select **Configuration > Devices**.

This will bring up the **Devices** screen. An example is shown in the figure below.



Step 2: Configure Device Template for the Cisco WAN Edge Devices to Participate in SD-WAN Overlay

The templates used in this deployment guide are similar to those used in Cisco SD-WAN Deployment Guide. In this guide we have one datacenter and four branches. The templates used are:

Model	Template
Datacenter	DC_Hybrid_Type_A_BGP
Dual-route dual-internet remote-site model	Branch_A_Bronze_BGP_TLOC_SubInt_OSPF Branch_A_INET_ TLOC_SubInt_OSPF
Dual-router hybrid remote-site model	Branch_B_MPLS_BGP_TLOC_VRRP Branch_B_INET_TLOC_VRRP
Single-router hybrid remote-site model	Branch_C_MPLS_CE_LAN_OSPF
Single-router dual-internet remote-site model	Branch_D_Bronze_BizInternet_LAN_OSPF

The device template, as well as the various feature templates which make up the device template, are discussed in **Appendix D**. Also, to further understand the topology of each branch and datacenter design, refer to **Appendix C**.

However, for detailed step-by-step instructions on creating individual feature templates and device templates, refer to the Cisco SD-WAN Deployment Guide.

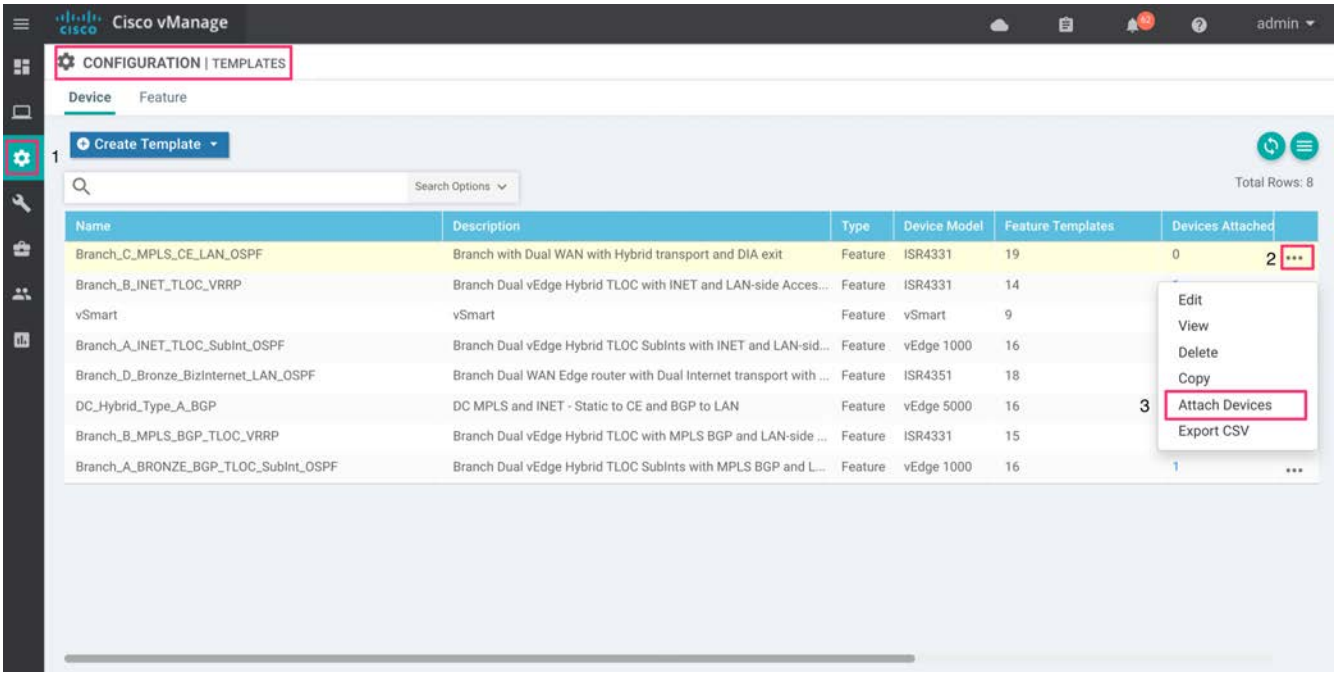
Step 3: Deploy the Device Template to the Cisco WAN Edge devices that will be used

On attaching the device template to a WAN edge router, vManage attaches the configurations based on the feature templates and pushes the configuration to the devices. There are two ways to build your feature templates: either by entering values within the variables configured or by uploading a .csv file with a list of the variables and their values. Note that within a feature template, the radio buttons against certain features can be configured as globally on/off or as variables through either of the methods explained earlier.

In this deployment guide, we will only discuss the values that are being entered manually in the device template.

1. Go to **Configuration > Templates** and select the **Device** tab.
2. Find the desired device template.
3. Select the three dots to the right of the template, and from the drop-down menu, select **Attach Devices**.

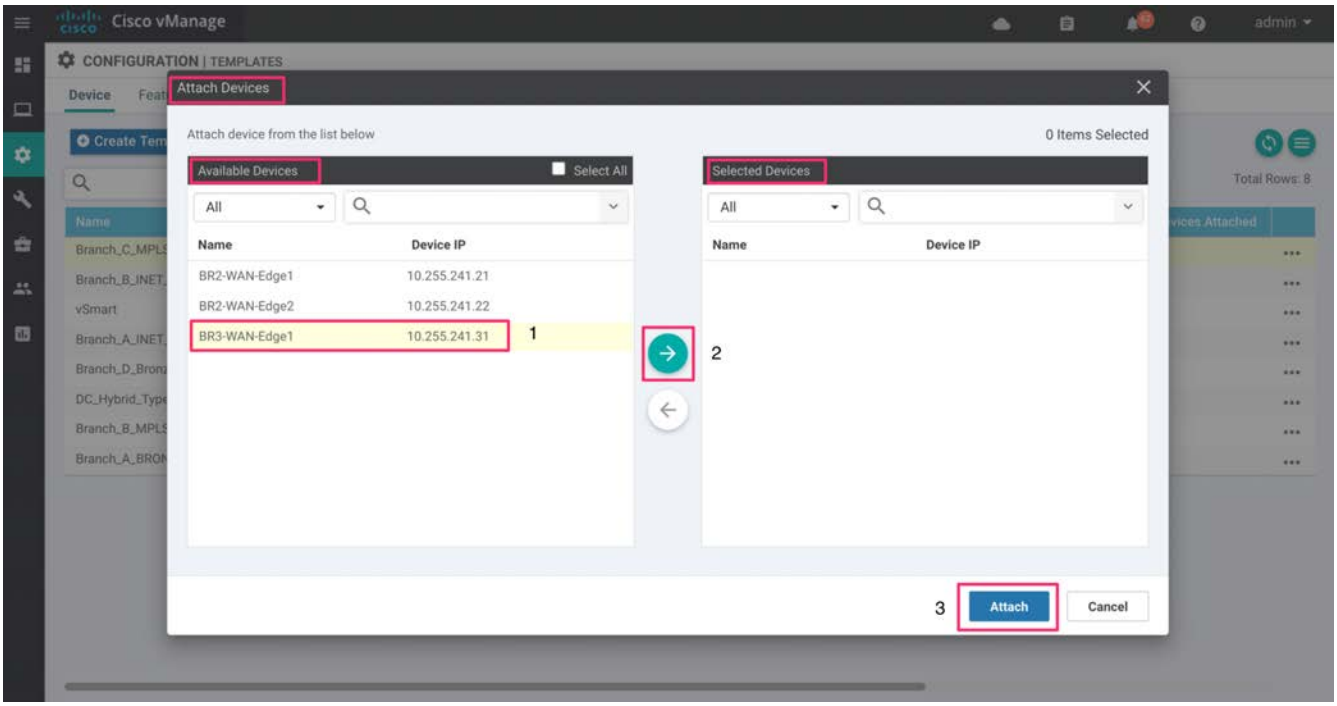
An example is shown in the following figure.



A pop-up window lists the available devices to be attached to this configuration.

4. Select the devices to which the template should be applied and click the arrow to move the device from the **Available Devices** box to the **Selected Devices** box.

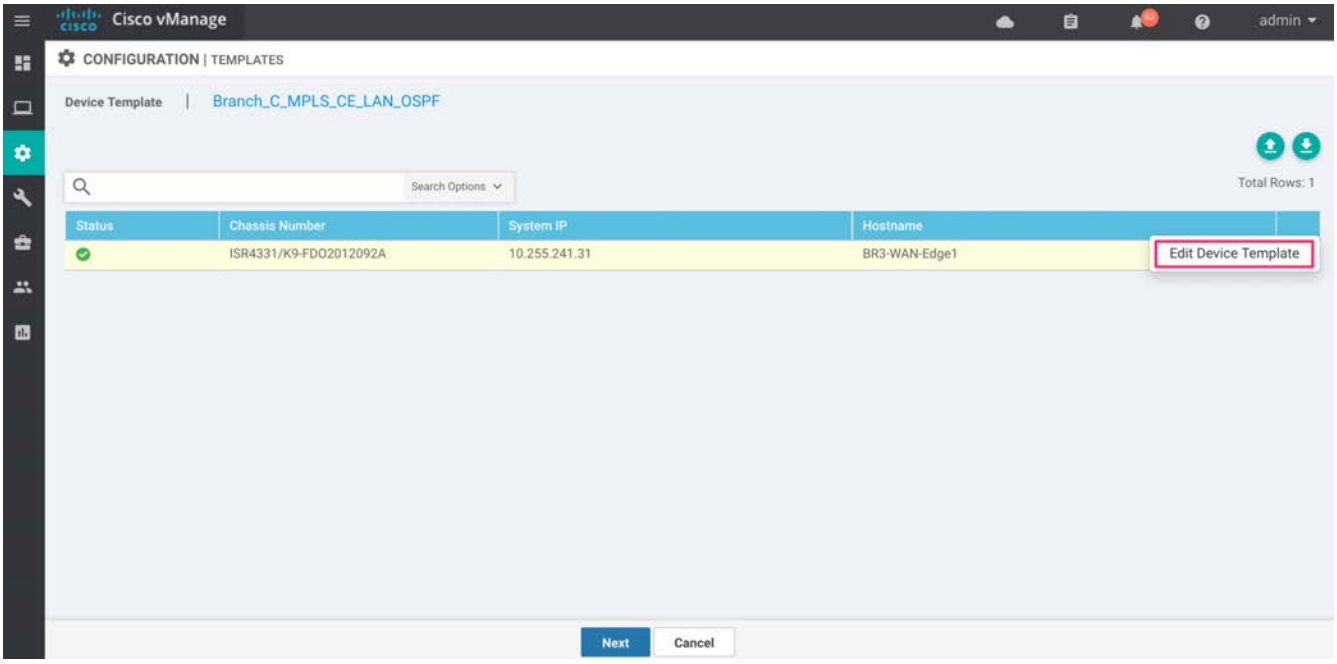
You can select multiple devices at one time by simply clicking each desired device.



Click the **Attach** button.

5. A new screen appears, click the **three dots . . .** at the right and then select **Edit Device Template**.

An example is shown in the following figure.



In this deployment, the feature templates are configured using variables. Therefore, when you click Edit, a list of variables and empty boxes appear. There may also be variables with check boxes to check/uncheck for on/off values.

6. Fill in the values of the variables in the text boxes.

All text boxes must be filled in. Check boxes can be left unmarked. For check boxes, checked means "Yes" and unchecked means "No". If you leave a text field empty, the text box will be highlighted red when you try to move to the next page. Fill in the variables using information from the table below.

Because you will be configuring DIA later, ensure that NAT is enabled on all interfaces that face Internet transport.

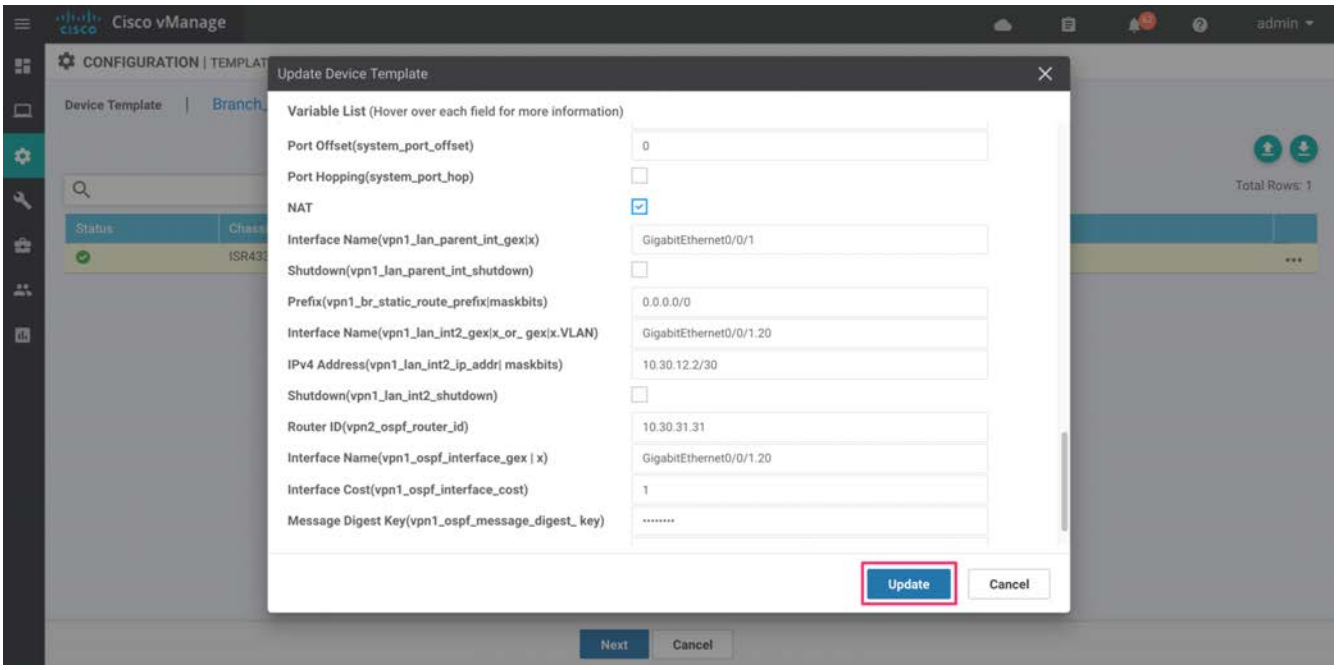
Table 1 **Single-Router Hybrid Design Model - Branch_C_MPLS_CE_LAN_OSPF**

Variable	Value
Interface Name(vpn1_lan_int1_gex|x_or_gex|x.VLAN)	GigabitEthernet0/0/1.10
Description(VPN1_lan_int1_description)	Service side Interface
IPv4 Address(vpn1_lan_int1_ip_addr|maskbits)	10.30.13.2/30
Shutdown(vpn1_lan_int1_shutdown)	☐
Router ID(vpn1_ospf_router_id)	10.30.31.31
Interface Name(vpn1_ospf_interface_gex|x)	GigabitEthernet0/0/1.10
Interface Cost(vpn1_ospf_interface_cost)	1
Message Digest Key(vpn1_ospf_message_digest_key)	********
Address(vpn1_ospf_area_range_address_0)	10.30.13.0/30
Interface Name(vpn512_mgmt_int_mgmt0_or gex)	GigabitEthernet0
IPv4 Address(vpn512_mgmt_int_ip_addr|maskbits)	100.119.118.6/24
Address(vpn0_inet_next_hop_ip_addr)	30.30.1.2
Address(vpn0_mpls_next_hop_ip_addr)	10.30.23.1
Interface Name(vpn0_mpls_int_ gex)	GigabitEthernet0/0/0
IPv4 Address(vpn0_mpls_int_ip_addr|maskbits)	10.30.23.2/30
Preference(vpn_if_tunnel_ipsec_preference)	100
IP MTU(vpn0_mpls_mtu)	1500
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	1000000
Bandwidth Upstream(vpn0_mpls_int_bandwidth_down)	1000000
Interface Name(vpn0_inet_int_ gex)	GigabitEthernet0/0/2

Variable	Value
IPv4 Address(vpn0_inet_int_ip_addr|maskbits)	30.30.1.1/30
Preference(vpn_if_tunnel_ipsec_preference)	100
IP MTU(vpn0_inet_mtu)	1500
Shutdown(vpn0_mpls_int_shutdown)	☐
Bandwidth Upstream(vpn0_mpls_int_bandwidth_up)	1000000
Bandwidth Upstream(vpn0_mpls_int_bandwidth_down)	1000000
Hostname(system_host_name)	BR3-WAN-Edge1
Latitude(system_latitude)	37.3541
Longitude(system_longitude)	-97.335
Device Groups(system_device_groups)	BR,ISR4331,US,West
System IP(system_system_ip)	10.255.241.31
Site ID(system_site_id)	112004
Port Offset(system_port_offset)	0
Port Hopping(system_port_hop)	☑
NAT	☑
Interface Name(vpn_lan_parent_int_gex|x)	GigabitEthernet0/0/1
Shutdown(vpn_lan_parent_int_shutdown)	☐
Interface Name(vpn2_lan_int2_gex|x_or_gex)	GigabitEthernet0/0/1.20
IPv4 Address(vpn2_lan_int2_ip_addr|maskbits)	10.30.12.2/30
Shutdown(vpn2_lan_int2_shutdown)	☐
Router ID(vpn1_ospf_router_id)	10.30.31.31
Interface Name(vpn1_ospf_interface_gex|x)	GigabitEthernet0/0/1.20
Interface Cost(vpn1_ospf_interface_cost)	1
Message Digest Key(vpn1_ospf_message_digest_key)	********
Address(vpn1_ospf_area_range_address_0)	10.30.12.0/30

Technical Tip: In dual-transport scenarios with TLOC extension, enable NAT on both, the TLOC interface and the physical Internet facing Interface. For more information, refer to the Design section of this document.

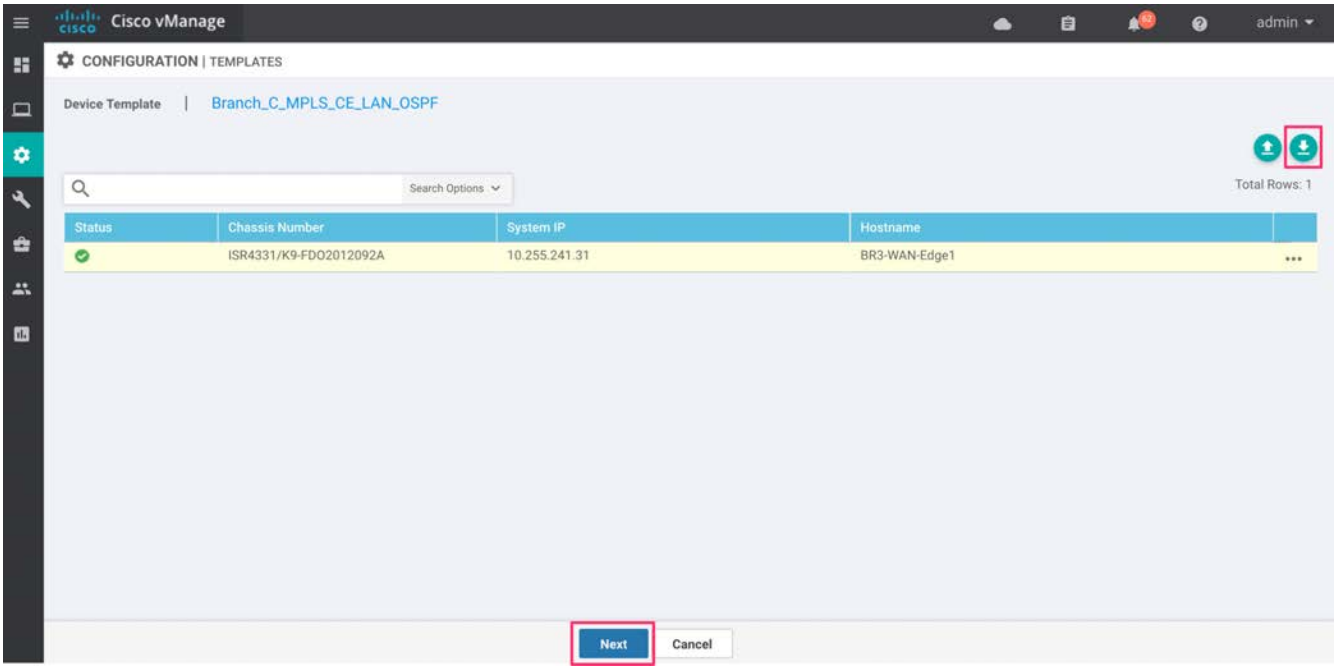
7. Select **Update** to add values within the device template.



8. Repeat **Steps 6 – 8** for the other WAN edge devices. You can find the templates for the rest of the branches in **Appendix D**.

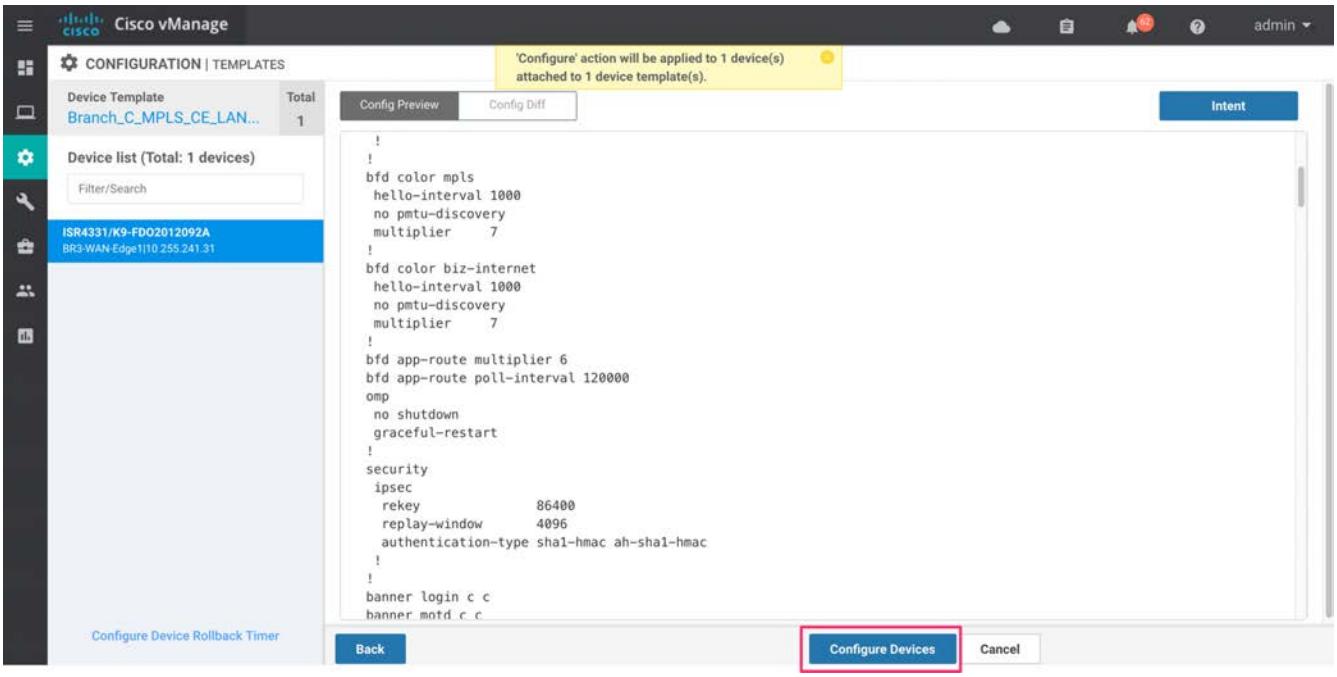
9. Before proceeding, ensure that you download the .csv file by clicking the down arrow on the upper right corner of the screen. The .csv file should be populated with the values you have filled in so far. If you deploy the configuration, and if for any reason there is an error in one of the input variables, the configuration may fail to deploy. When you come back to this page, all the values will be gone, and you will need to enter them again.

   If you downloaded the populated .csv file, upload it by selecting the up arrow. Then you can select **…** to the right of the desired device and select **Edit Device Template.** Your latest values will be populated in the text boxes. You can then modify any input values and try to deploy the configuration again.



10. When you are ready to deploy, click **Next.**

The next screen will indicate that the **Configure** action will be applied to device attached to the template. An example is shown in the figure below.

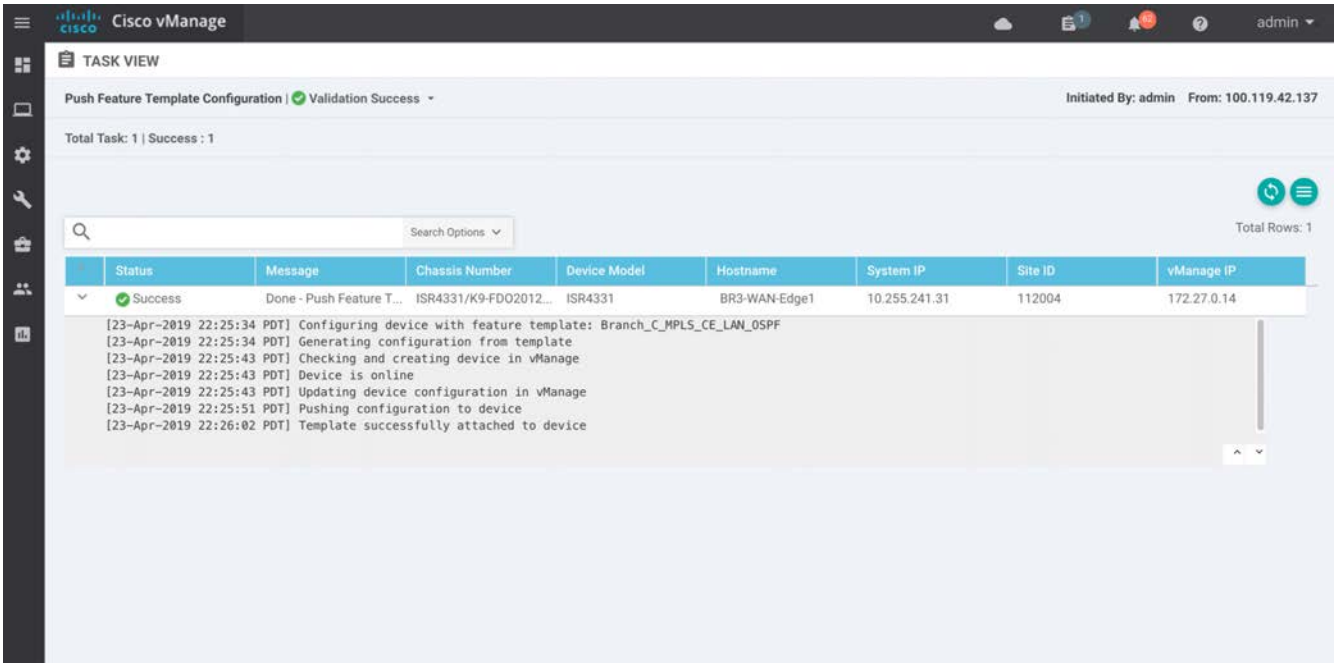


If you forget to add values for a device, you will get an error and won't be able to proceed until that is corrected.

Select the device in the left-hand panel to view the configuration associated with them, which will be pushed to the WAN Edge router (Config Preview tab). Click **Configure Devices** and confirm configuration changes on the device and then click **OK**.

The configuration pushed to all WAN edge devices in this deployment guide from the configuration template is shown in **Appendix E**.

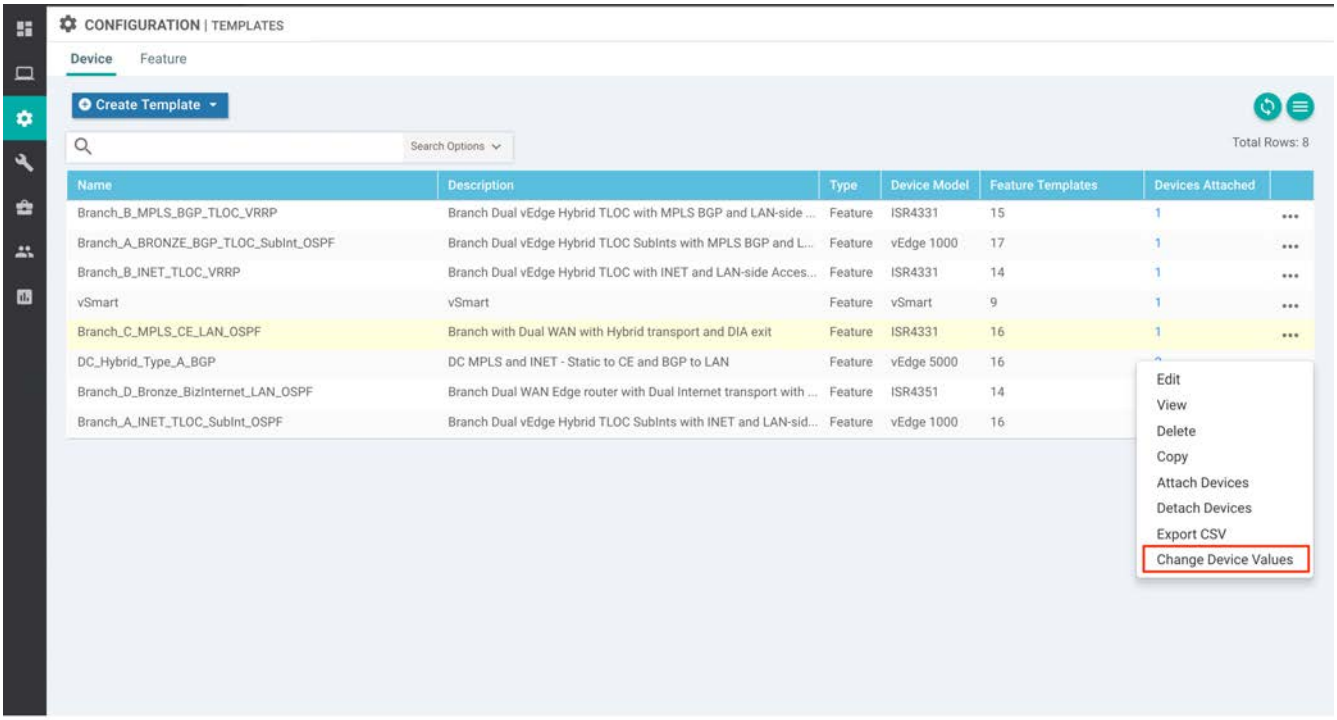
11. In the **Task View** screen verify if the templates were successfully pushed to the device based on the status. Click the arrow next to a device to view the deployment logs. If you encounter errors while applying a device template, you'll see the error logs here.



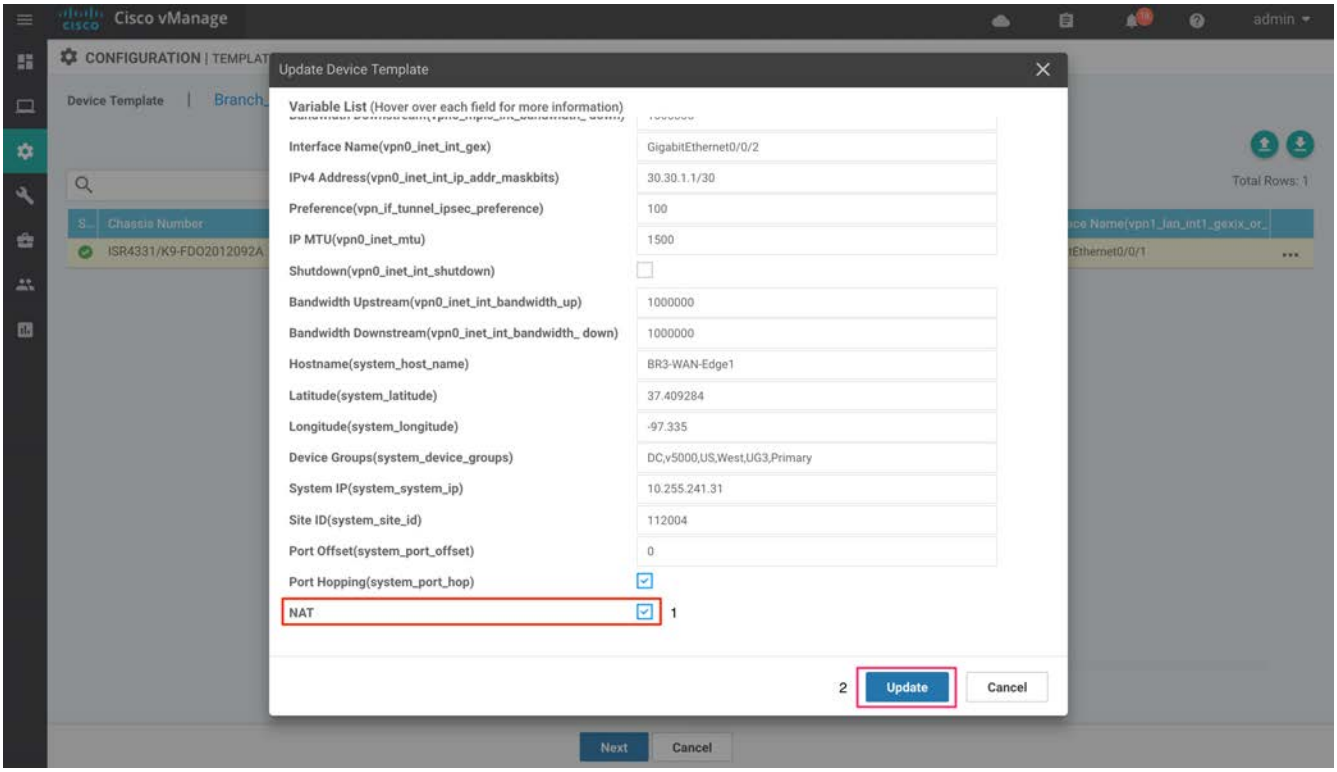
Step 4: Verify NAT Feature Configuration

Lastly, verify that NAT has been enabled in the internet-facing interfaces of all WAN edge devices. This step is crucial to enable DIA. If you find out that a device does not have NAT enabled, you can enable it later by editing the device or the feature template, without losing the previous configuration.

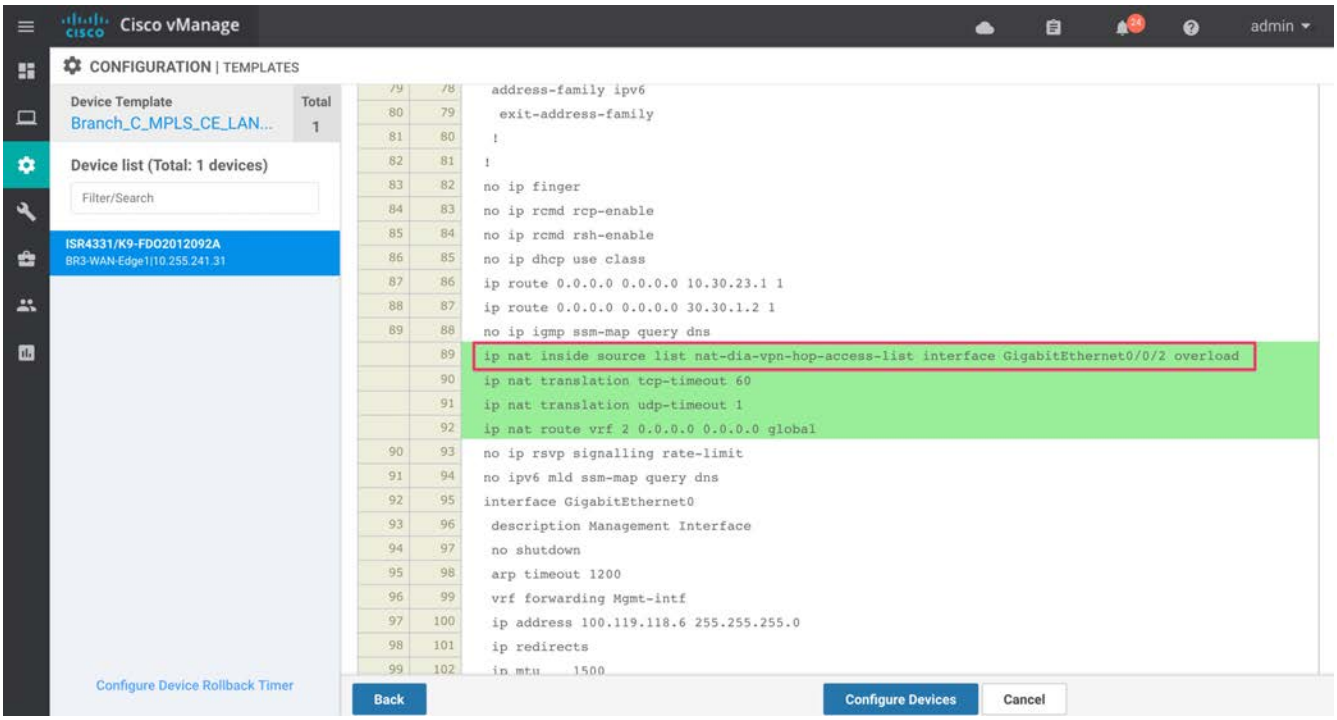
12. Navigate to **Configuration > Templates** and click on the three dots to the right of the device template you wish to enable NAT for. Click **Change Device Values**.

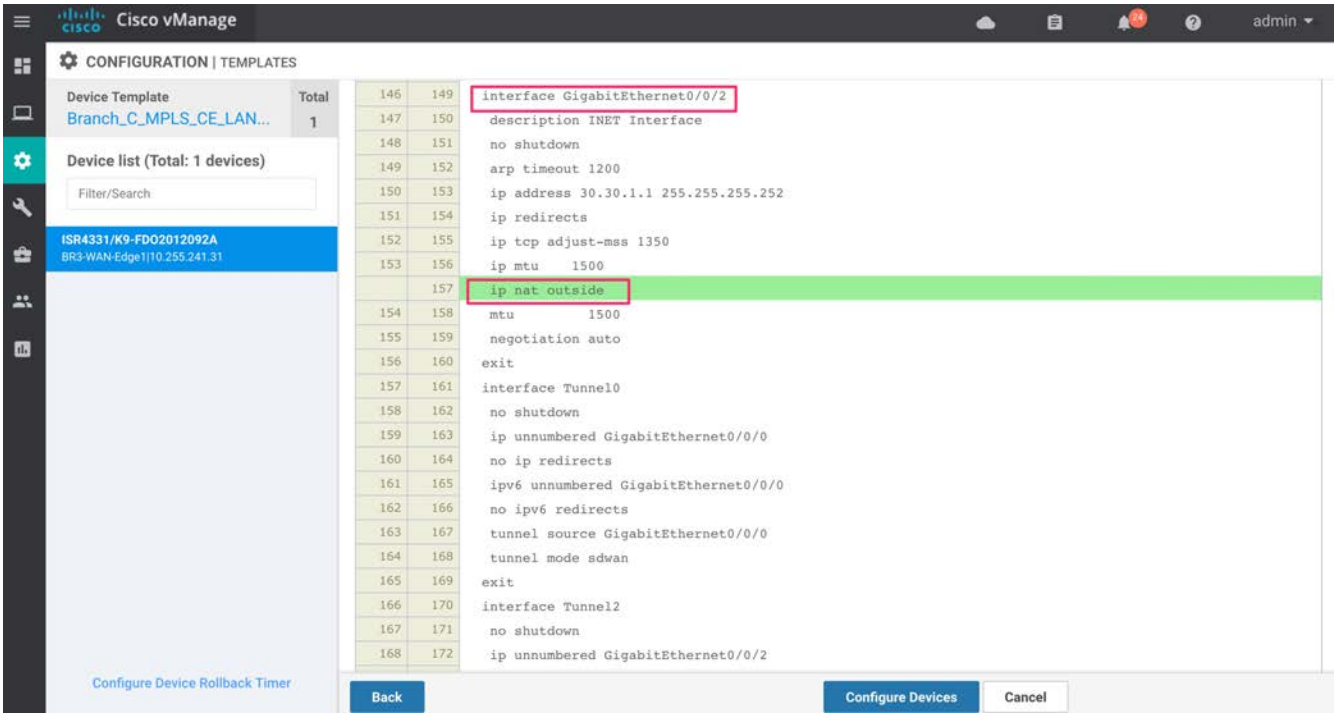


13. Enable NAT within the Update Device Template tab. Here we have enabled NAT under the Internet transport interface, Ge0/0/2.



14. Validate the configuration.





Alternatively, you can also edit an existing feature template to enable/disable NAT globally. In this deployment, one of the feature templates used to configure features within VPN 0 Internet facing Interface is BR_INET_INT.

15. To edit the feature template, click **Edit** within the configured feature template and configure NAT globally.

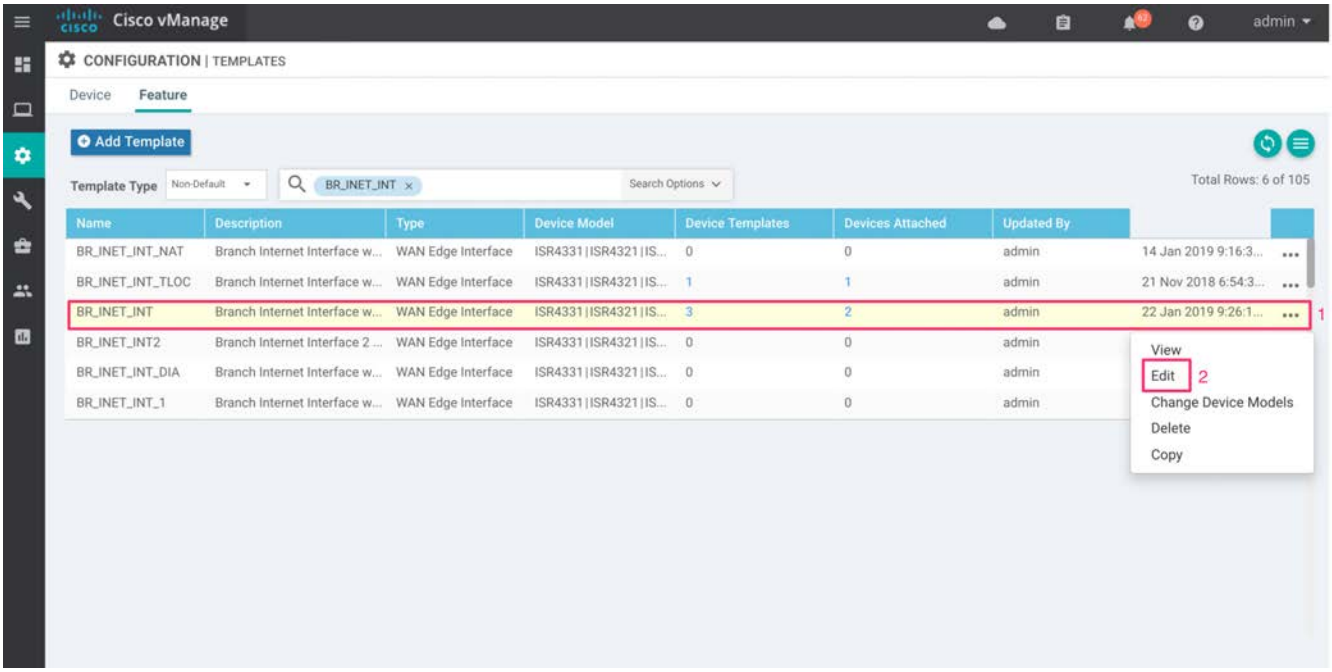


Figure 32 Edit using feature templates

Technical Tip: On SD-WAN XE devices, enabling NAT creates an additional line of NAT overload command within the configuration. The NAT overload feature works the same way on both vEdge and SD-WAN XE devices.

Deploy - Cisco SD-WAN Direct Internet Access Configuration

You must complete the following tasks for successful deployment of DIA with SD-WAN.

- Configure NAT DIA route or configure a centralized data policy to accomplish DIA.
- Optionally configure a system tracker.

Configure NAT DIA routing: Configure an IP NAT route to perform route lookup to redirect traffic from the service-side VPN to the transport-side VPN.

Configure centralized data policy: Configure centralized data policies within vManage. These policies are provisioned on a vSmart controller and are applied only to the vSmart controller. The effects of the policy reflect on the WAN edge routers.

[Optional] Configure a (System tracker) transport interface tracker: Configure a global interface tracker (system tracker) within system template and apply it to the transport NAT-enabled interface. This configuration helps redirect traffic to the tunnel on the transport interface, that is not NAT-enabled, if the Internet or external network becomes unavailable. Also, in a design scenario that has dual-internet exits, if the internet link that is not enabled with NAT is down, the Internet traffic can still traverse via the second Internet NAT-enabled interface.

Deploying Cisco SD-WAN DIA Configuration

This section of the guide focuses on the configuration and activation of DIA within remote sites via policies or a NAT DIA route through the vManage dashboard.

This section addresses both the use cases. The network is deployed such that in each design scenario, VRF 1 or VPN 1 are dedicated for employee traffic and VRF 2 or VPN 2 for guest traffic. In this deployment network, a centralized data policy is used to allow DIA for all employee traffic and the NAT DIA route type is configured to allow Internet access for guest traffic. However, either of these DIA configurations can be configured irrespective of the type of traffic based on the requirement. The guide also covers the configuration of a system tracker to enable fallback on vEdge router platforms, on configuring NAT DIA route.

Procedure 1: Use Case #1 - Create Centralized Data Policy to Redirect Employee Traffic

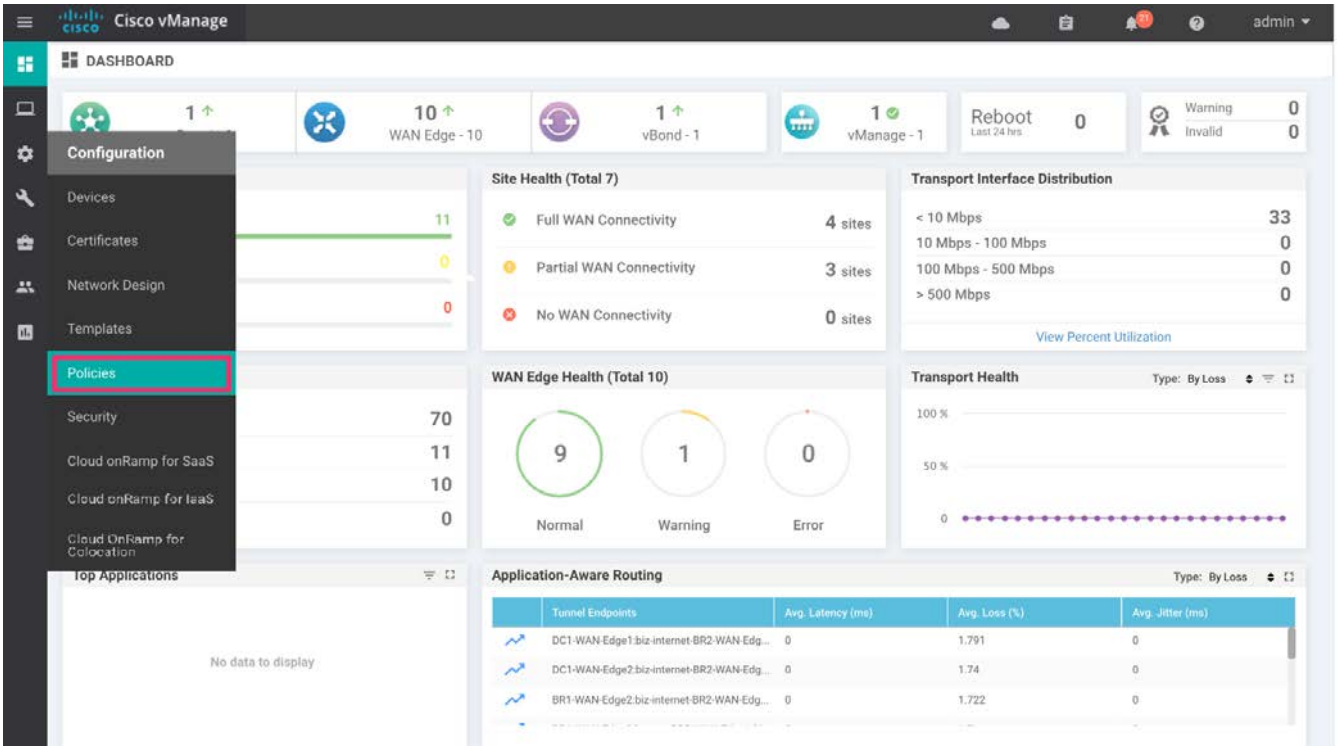
To route the specific employee web traffic from service-side VPN to transport-side VPN, a centralized data policy is built. This policy is configured on the vSmart controller and the result of the policy is pushed into the affected WAN Edge routers based on the site list.

1. Login to the vManage web console using the IP address or fully qualified domain name of your vManage instance. For example:

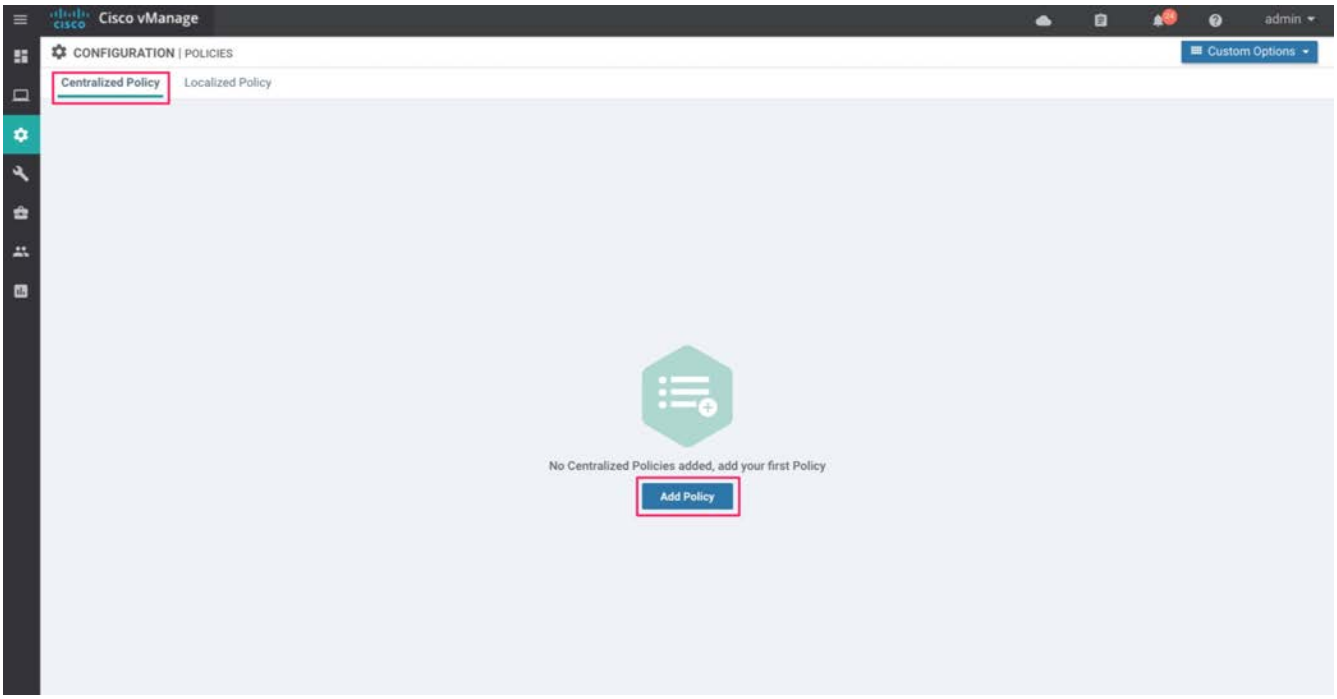
   https://vManage_ip_addr_or_FQDN:8443/

2. This brings up the vManage dashboard.

   Navigate to **Configuration > Policies** from the vManage GUI.



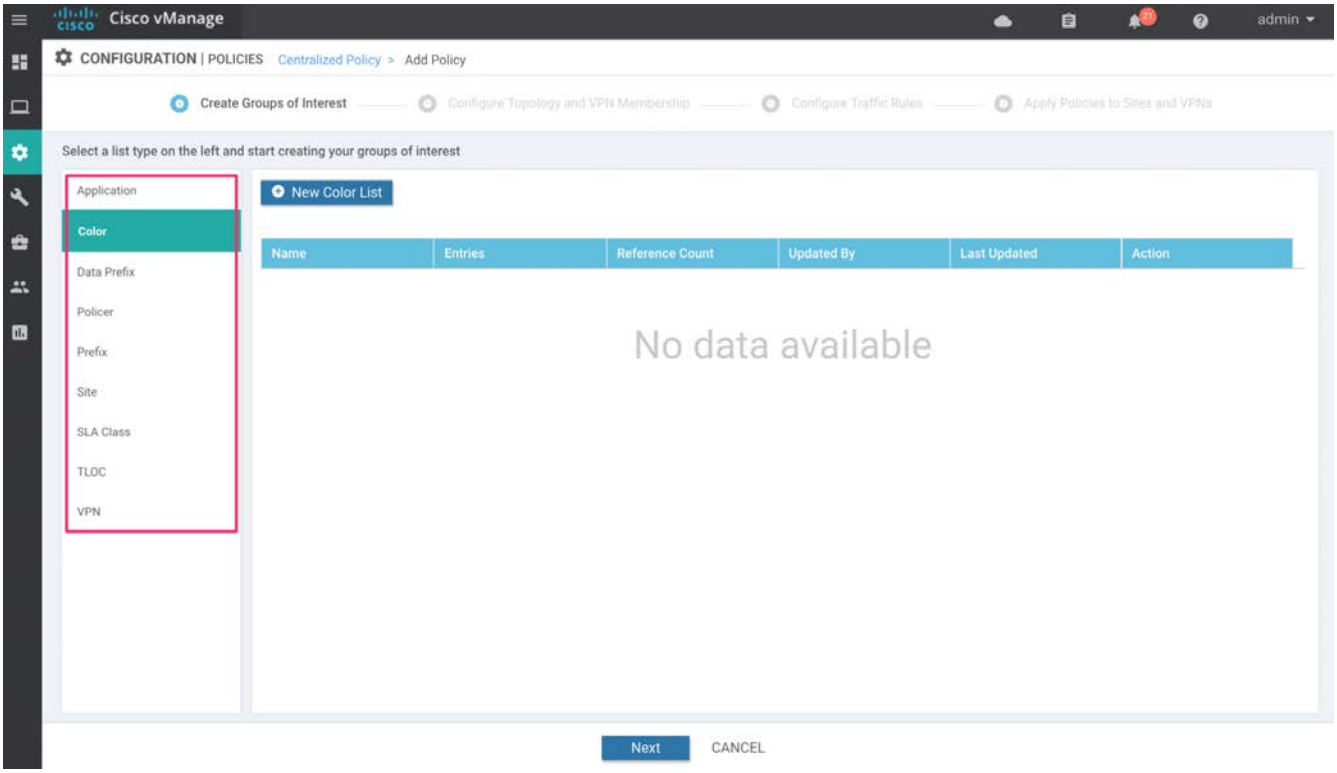
3. Click the **Add Policy** tab within the centralized policy to navigate to groups of interest.



Step 1: Create Groups of Interest

Select the type of list from left pane and create lists based on the network requirements.

The groups of Interest configured here will help you create specific lists such as Prefix list, VPN list, list of Site IDs and more. Use these lists later within the centralized data policy to filter the incoming traffic and to reflect the result of the policy on specific VPNs and site IDs.



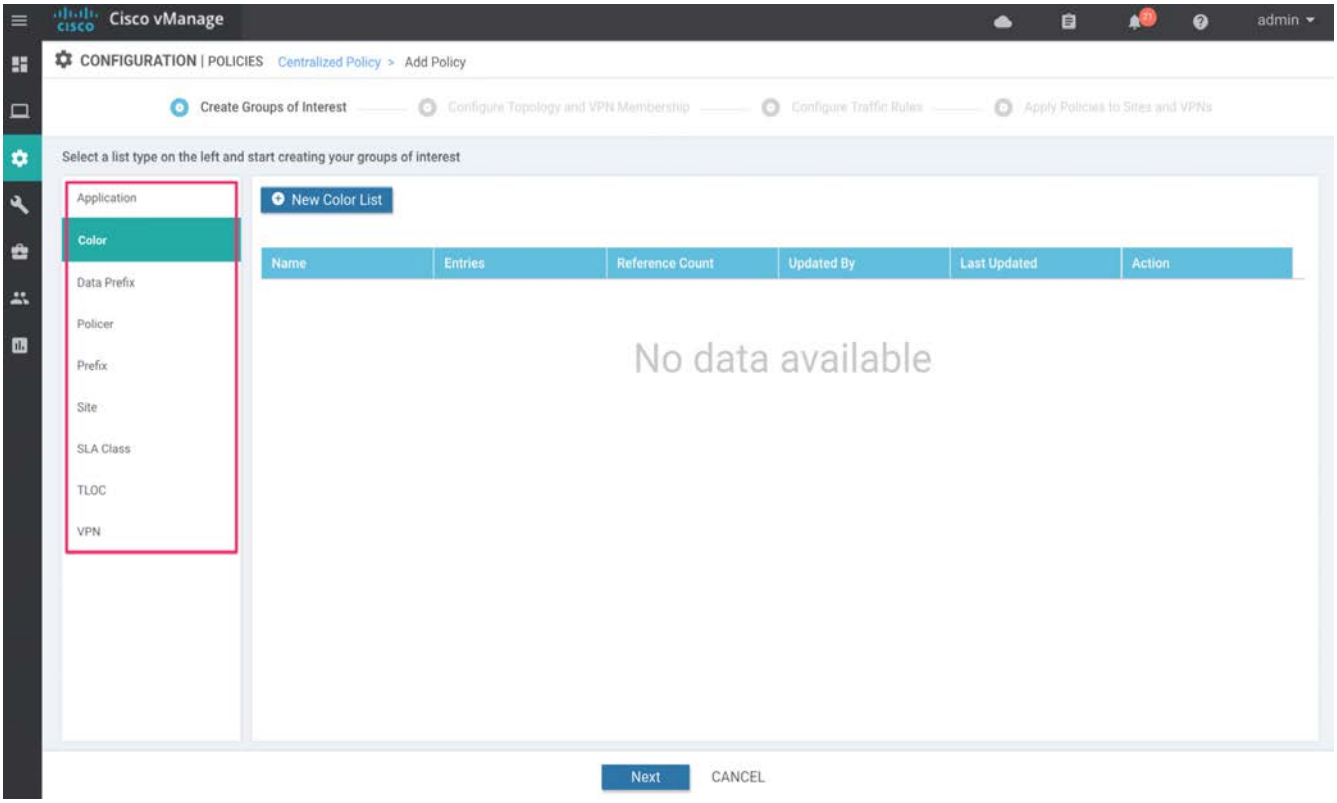
In this DIA deployment, centralized data policy is built to filter traffic based on the prefix list configured (i.e. Source data prefix) and this policy is then applied to the vSmart controller. The result of the policy is pushed from vSmart controller to the WAN edge devices based on the list of site IDs configured within the centralized data policy. Within the affected WAN edge devices, all traffic entering specific VPNs that are a part of the VPN list, is filtered based on its source data prefix configured within the policy match statement, and routed to the transport-side interface, VPN 0.

Groups of Interest configured in this guide include the following:

- Data prefix list
- Site ID list
- VPN list

Data Prefix List

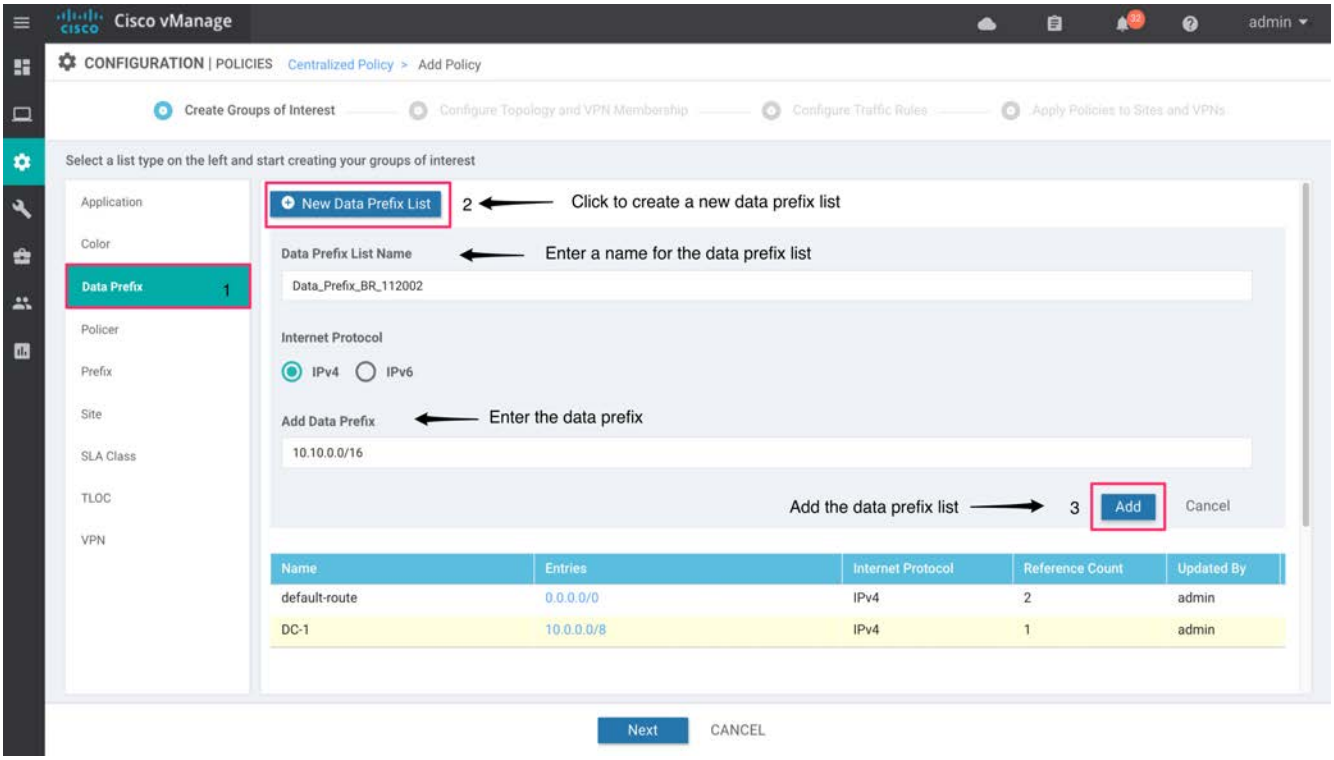
1. Select Data Prefix from the panel on the left.

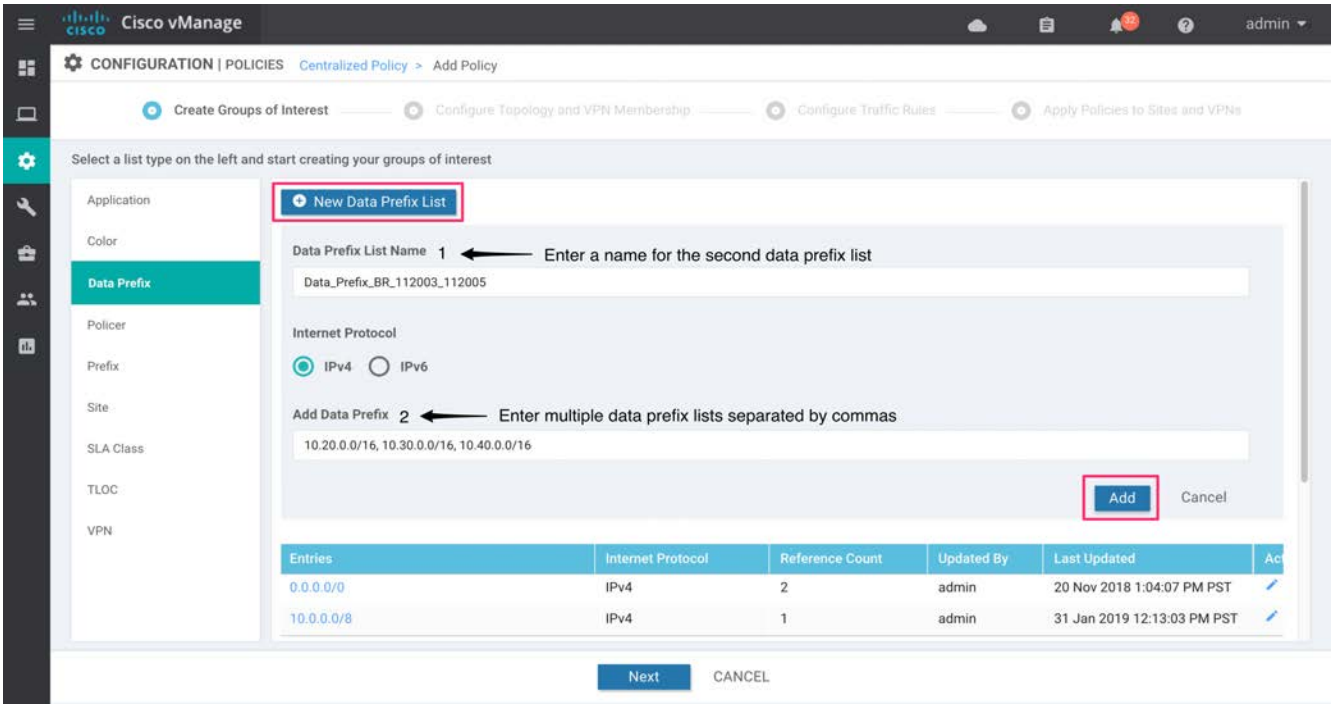


2. On the resulting screen

    1. Click **New Data Prefix List**. Enter a name for the Data Prefix List (Data_Prefix_BR_112002).
    2. Enter the Data Prefix (10.10.0.0/16).
    3. Click the **Add** button.

    Repeat steps 1-3 to add a second Data Prefix List.





Note that prefix lists configured can be used to match source or destination data prefixes. These lists in this guide are configured to match source data prefixes. All the employee traffic from the IOS XE SD-WAN devices is added under a single data prefix and a separate data prefix is created for vEdge devices.

Note that a separate data prefix list of 10.10.0.0/16 is created in this deployment for the purpose of building a separate data policy to show how path preference is set in vEdge router platforms. Also, a separate data prefix list Overlay_Traffic is created. This is to be used later in the policy within a sequence rule to allow flow of Internal traffic across SD-WAN overlay network.

An example of data prefix list build for each of the branches is provided below.

Table 2 **The data prefix lists built are summarized in the following table List of data prefixes**

Data Prefix List Name	Add Data Prefix
Data_Prefix_BR_112002	10.10.0.0/16
Data_Prefix_BR_112003_112005	10.20.0.0/16, 10.30.0.0/16, 10.40.0.0/16
Overlay_Traffic	10.0.0.0/8

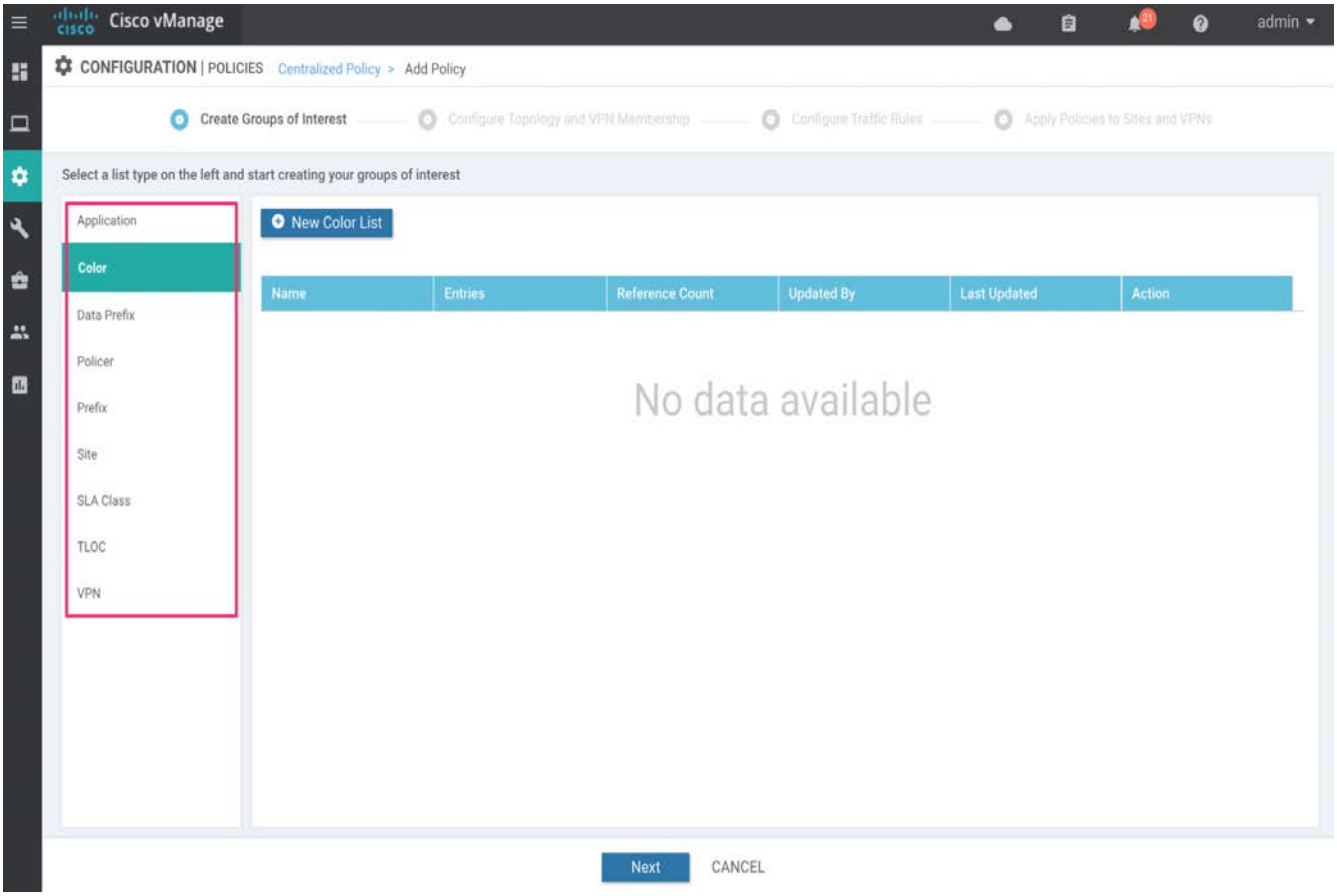
The data prefixes are deployed based on the policy deployed in this document.

Site ID List

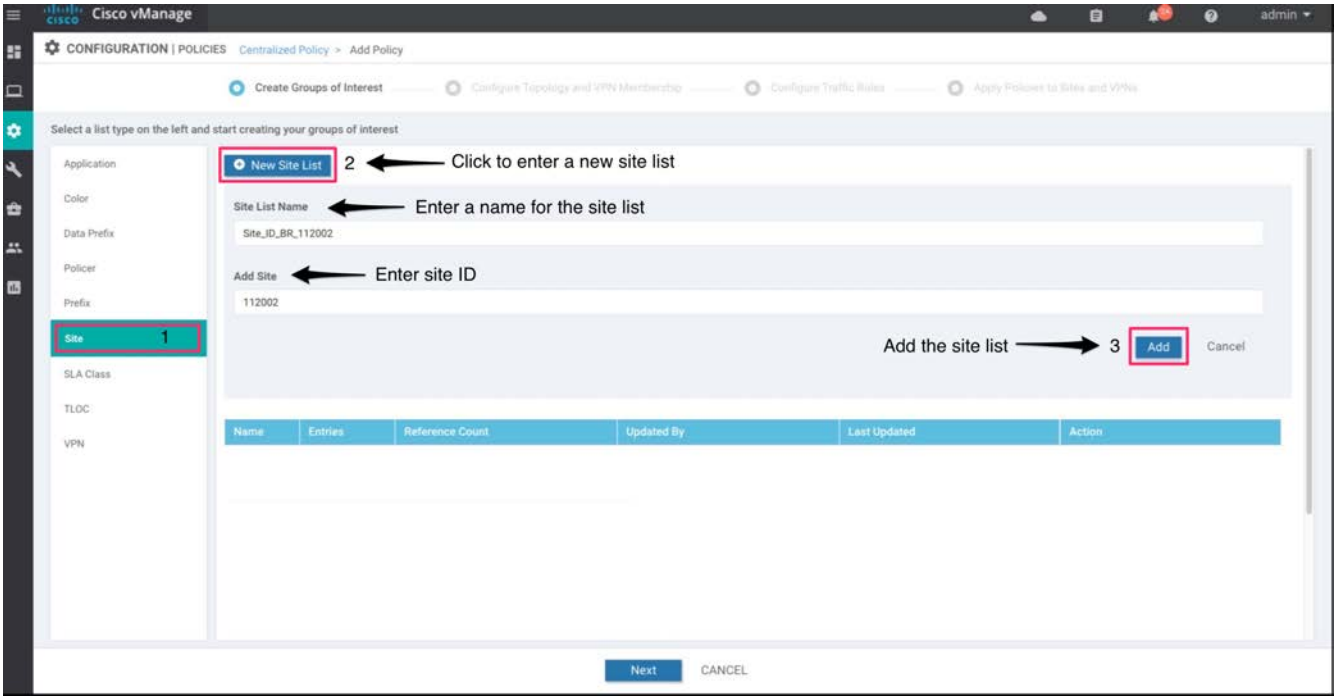
Within list type site, create a new site list. If you already have a site list defined that you will apply the DIA policy to, skip this section. Here's an example of creating site lists for each of the branches.

An example of the list of Site ID's for each of the branches, along with the necessary steps are mentioned below.

1. Select Site from the panel on the left.



2. On the resulting screen,
    1. Click **New Site List**.
    2. Enter a name for the Site List (Site_ID_BR_112002).
    3. Enter the Site ID (112002). Click the **Add** button.



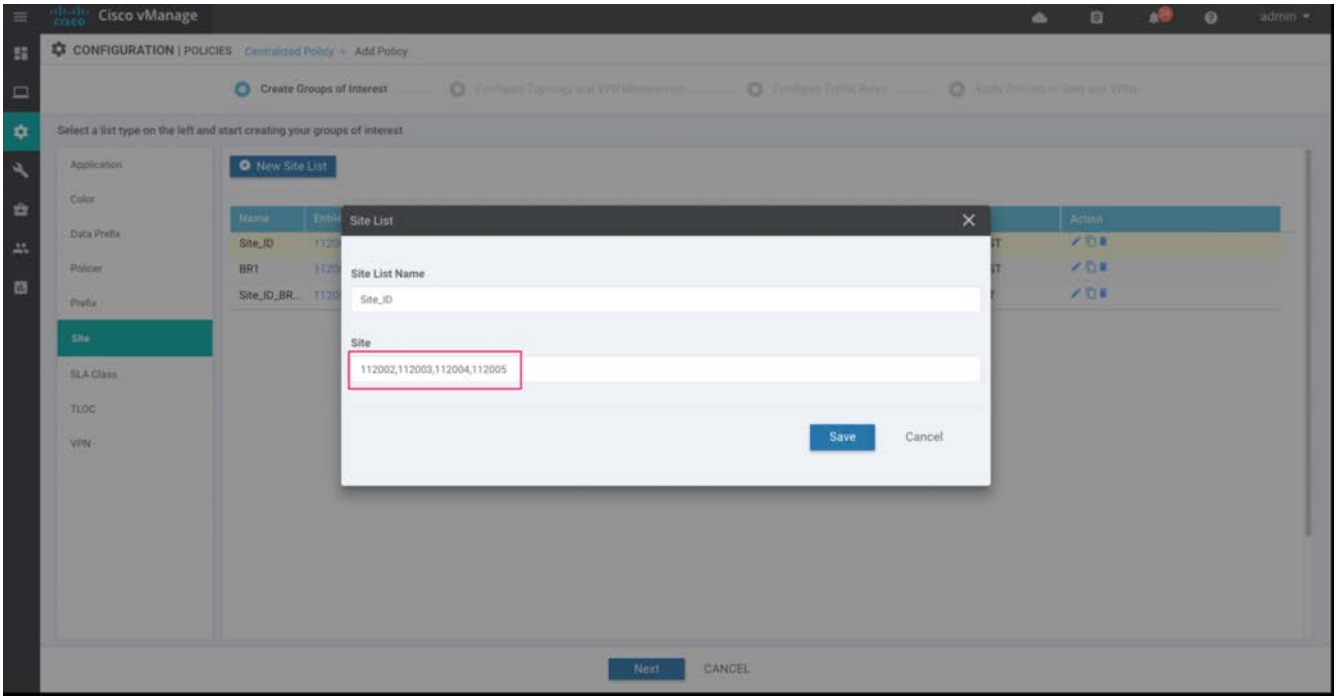
Repeat steps 1-3 to configure the remaining site ID lists.

The Site ID lists that are built are summarized in the following table:

Table 3 **List of Sites**

Site List Name	Add Site
Site_ID_BR_112002	112002
Site_ID_BR_112003	112003
Site_ID_BR_112004	112004
Site_ID_BR_112005	112005

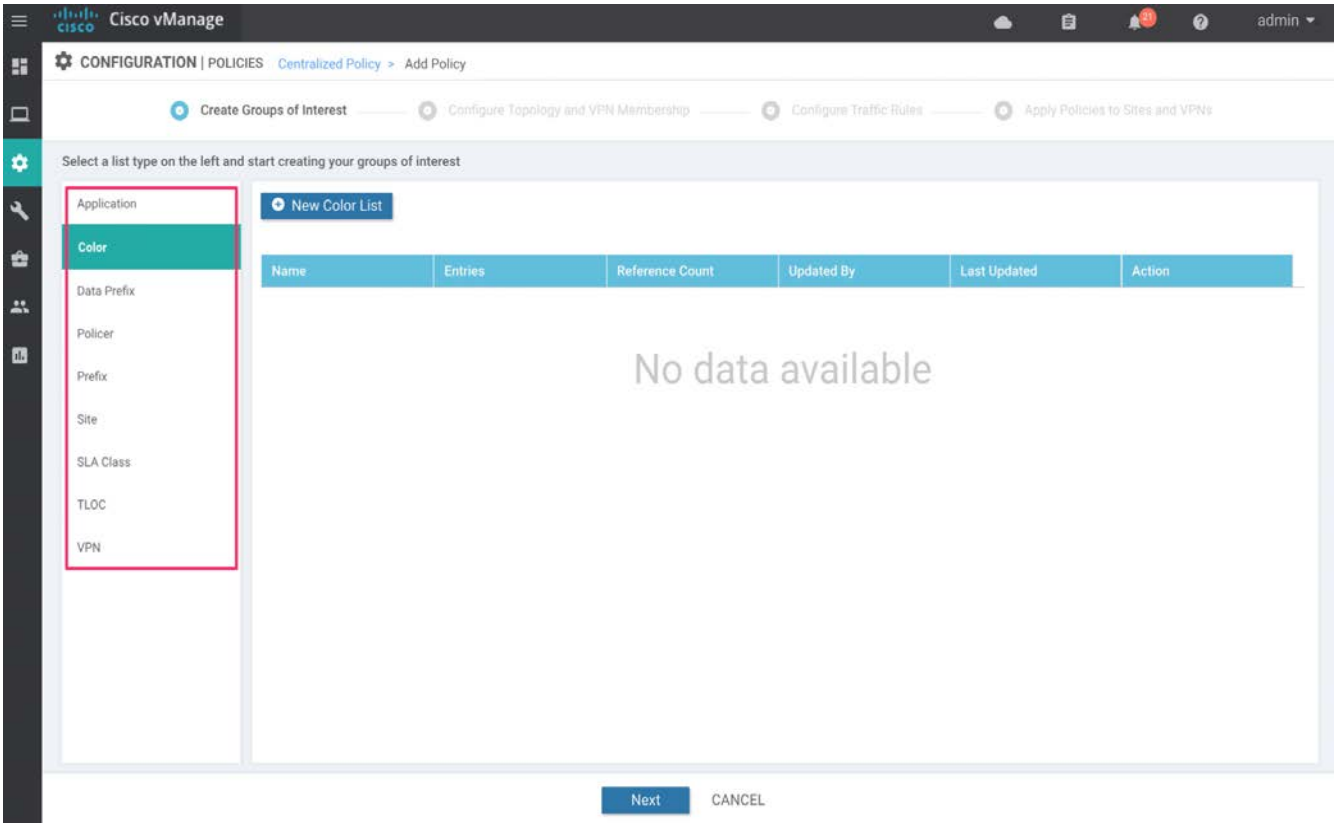
Alternatively, the Site IDs can be added under a single Site List separated by commas as shown below.



VPN List

Within list type VPN, create a new VPN list. This VPN list includes the service VPN IDs you will apply the policy to. If you already have a VPN list defined that you will apply the DIA policy to, skip this section. Here's an example of creating VPN lists.

1. Select VPN from the panel on the left.

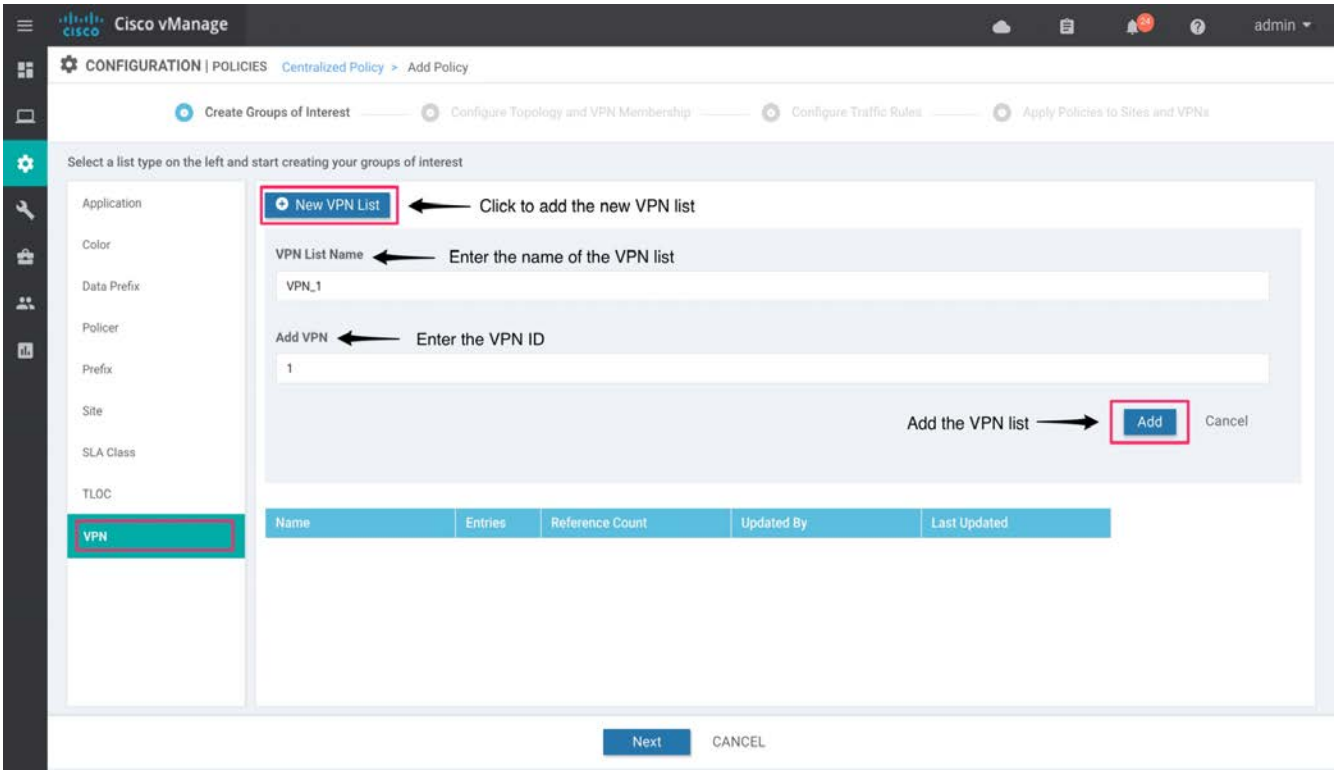


2. On the resulting screen, click **New VPN List**.

    1. Enter a name for the VPN List (VPN_1).

    2. Enter the VPN ID (1).

    3. Click the **Add** button



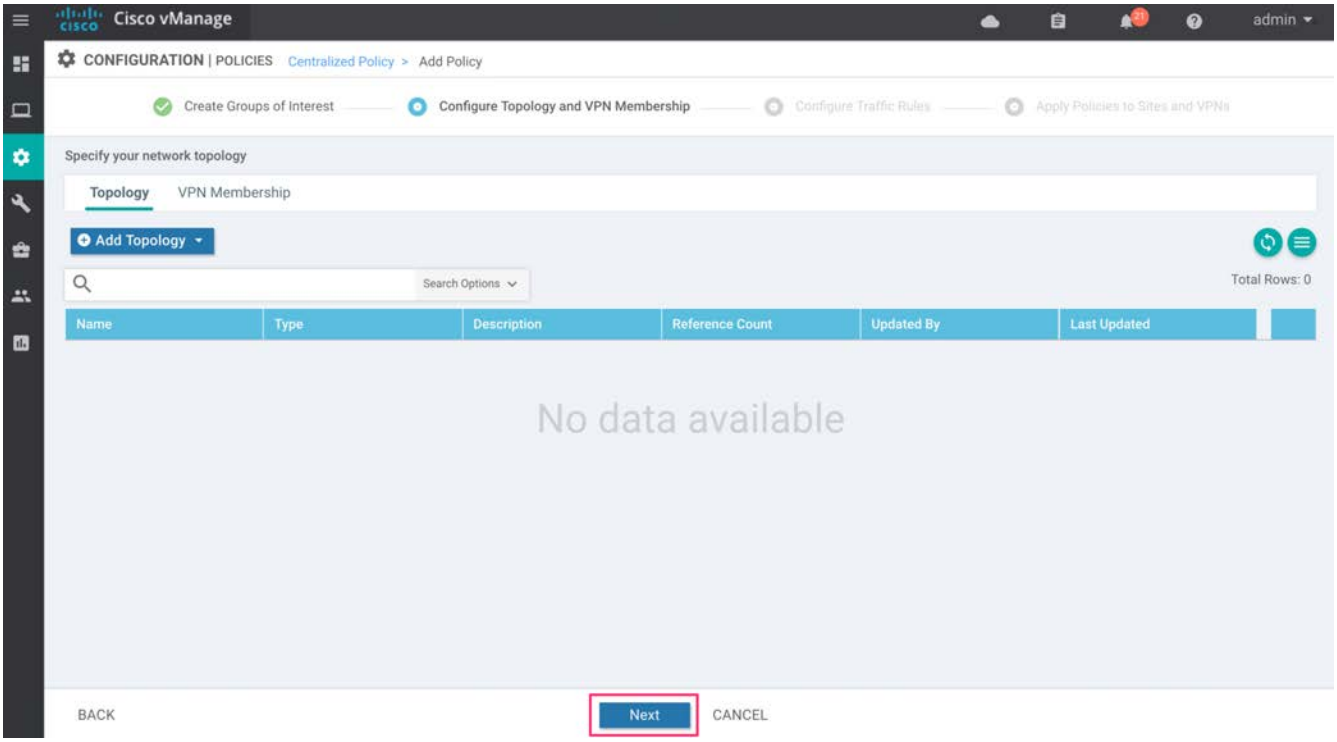
The following table summarizes the Site VPN list built.

Table 4 **List of VPNs**

VPN List Name	VPN
VPN_1	1

Once the lists are created, proceed to the next page and configure the traffic rules for the policy.

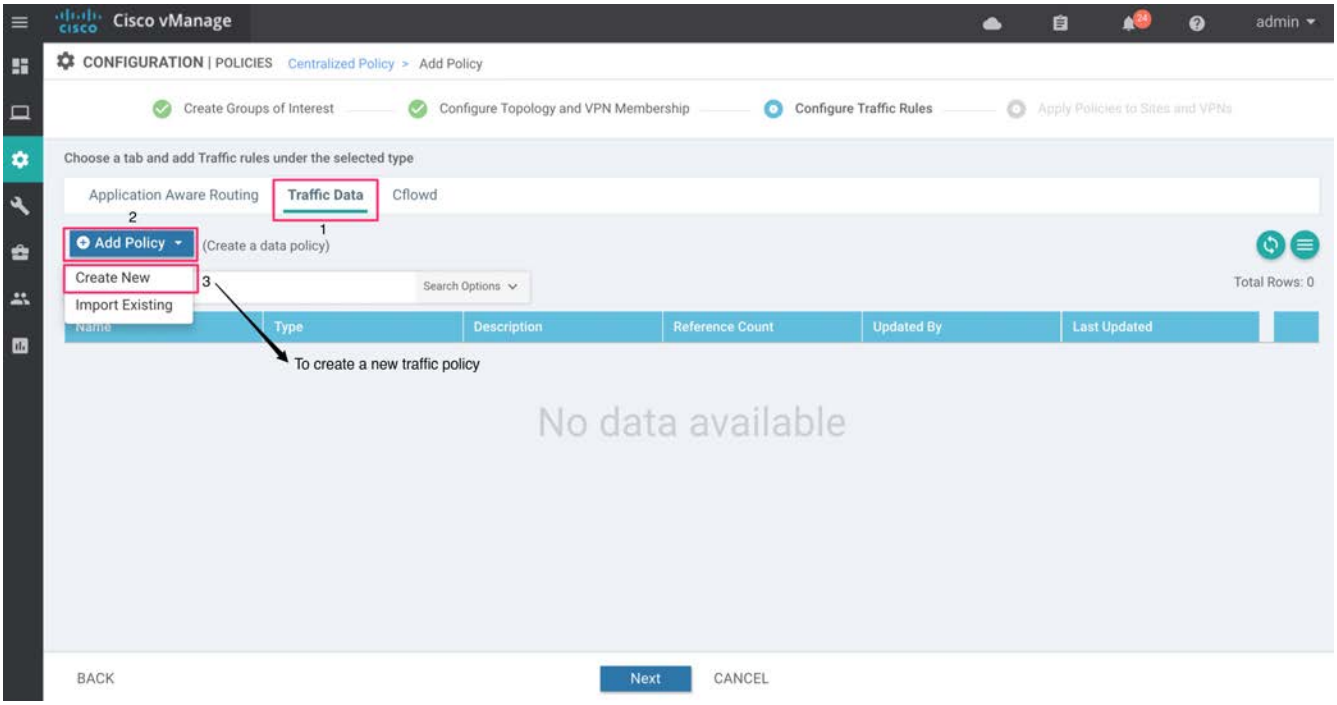
3. Click the **Next** button twice at the bottom of the page to arrive at the **Configure Traffic Rules** page.



Step 2: Configure Traffic Rules

In this example, three separate sequence rules are added. The first rule is to maintain the overlay or internal traffic flow, second sequence rule is to enable DIA for the SD-WAN XE devices without path preference and the third sequence rule is to again enable DIA for the vEdge router platform with path preference set.

4. To create a new data policy, click **Add Policy.** Next, select **Create New** from the drop-down list.



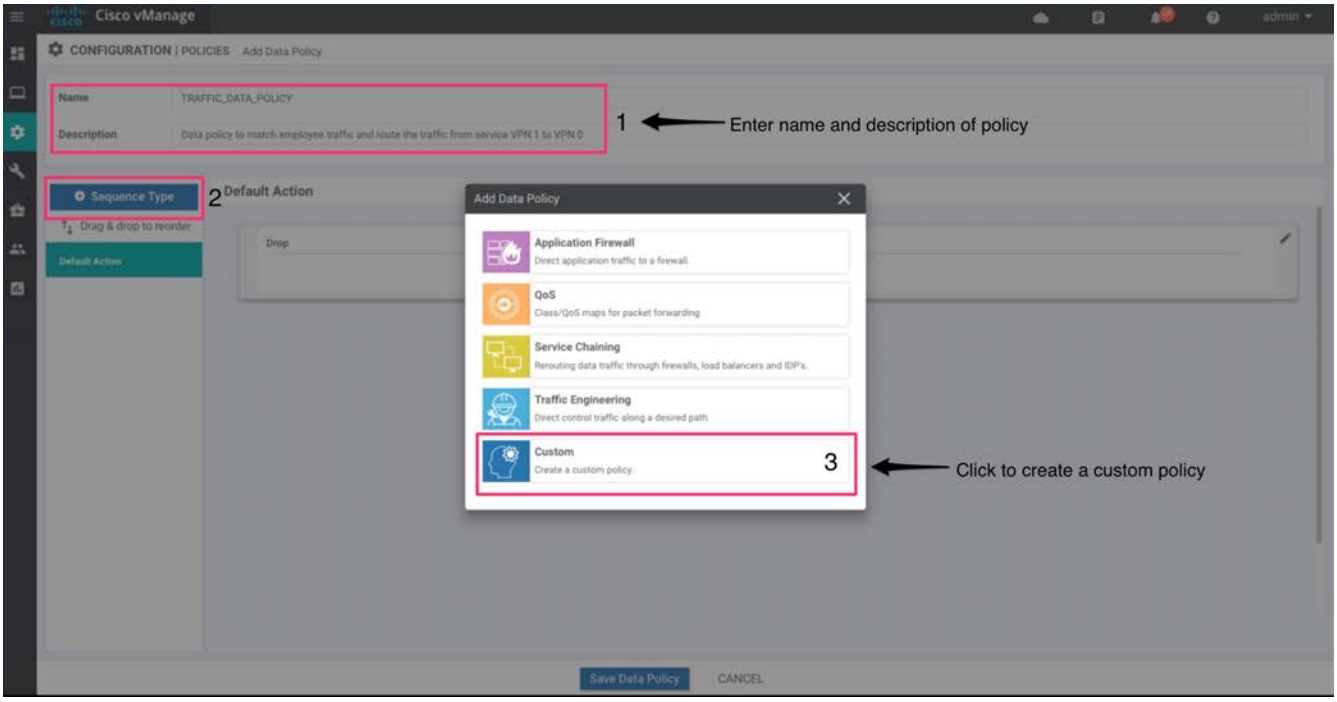
Technical Tip: Alternatively, the entire traffic data policy can be configured using the custom option found on the top right of the main policy page and then later imported into the centralized policy. Within the **Traffic Data** tab, there is an Import option under **Configure Traffic Rules**, to import an existing traffic policy. For more information, refer to the section **Alternate method to deploy traffic data policy.**

5. Create the new traffic policy and enter the traffic data policy name and policy description. The details are summarized in the following table:

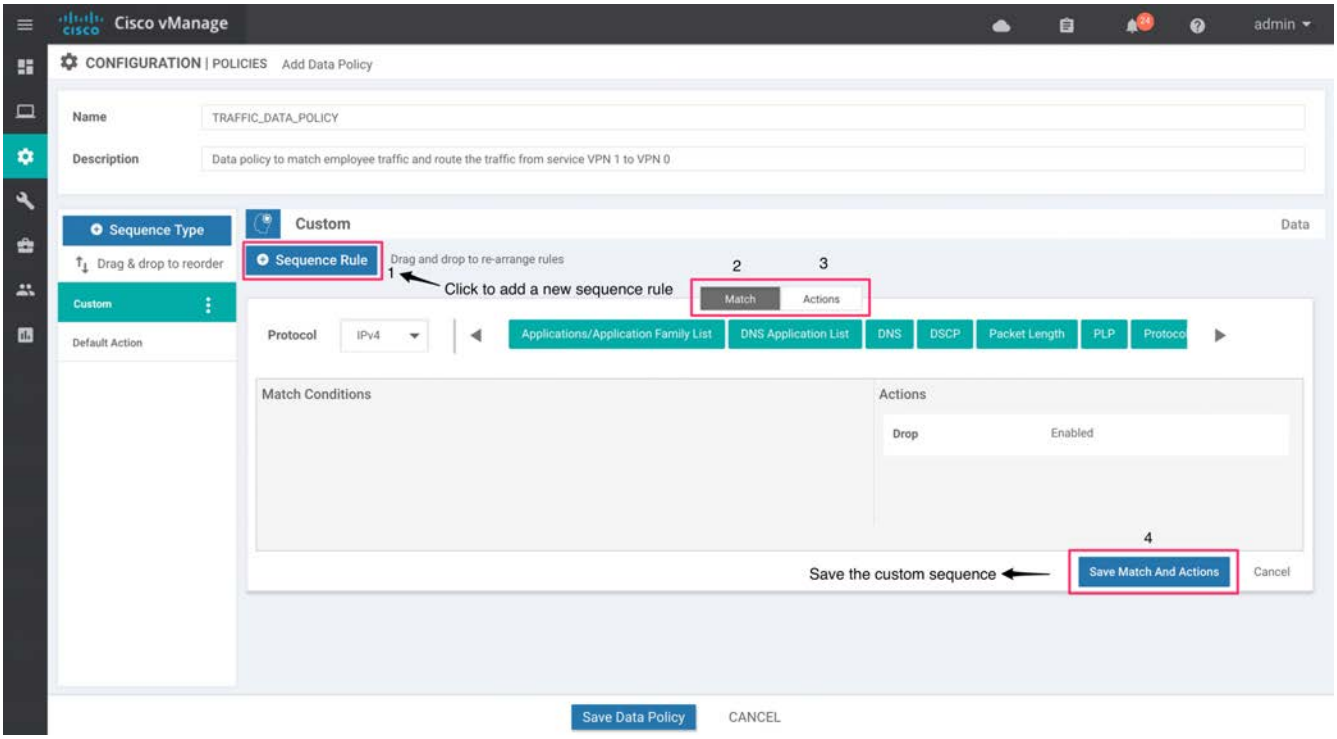
Table 5 **Traffic Data Policy Description**

Policy Name	Policy Description
TRAFFIC_DATA_POLICY	Data policy to match employee traffic and route the traffic from service VPN 1 to VPN 0

6. From the right pane, click **Sequence Type** and choose **Custom** from the list of available types of data policy.

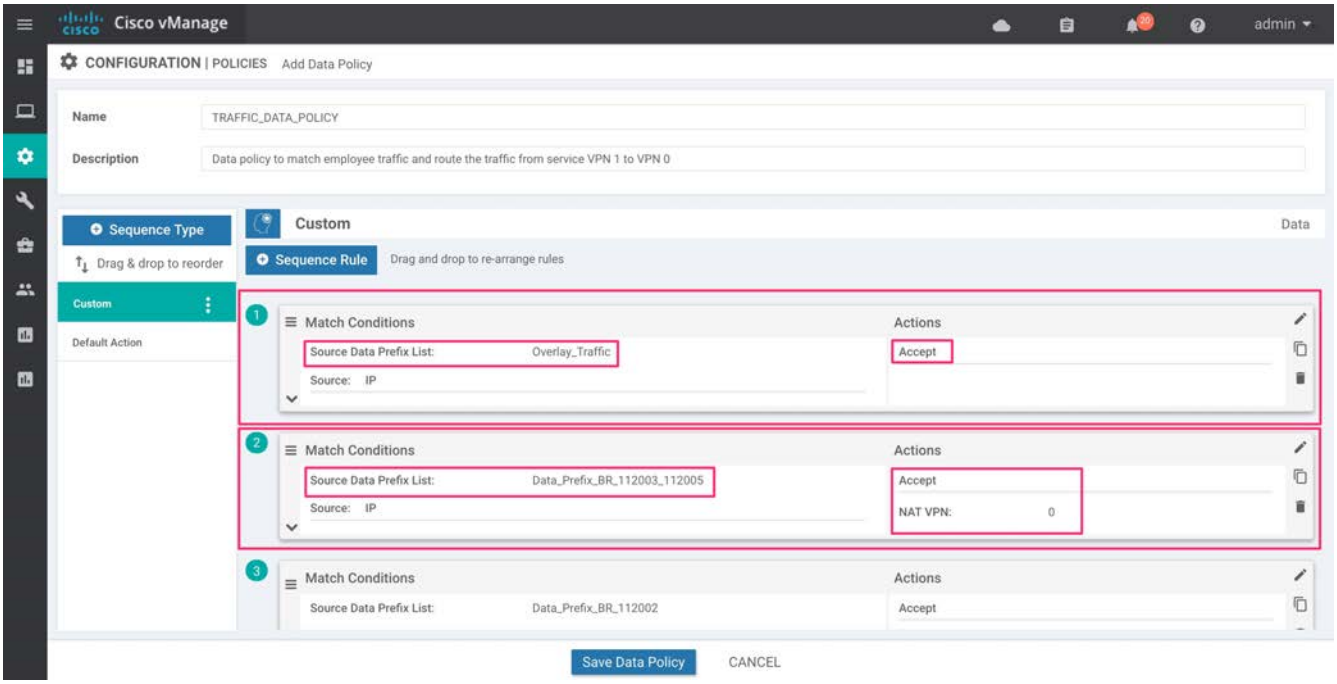


7. Under **Custom**, click on **Sequence Rule** and add the created groups of interests under **Match** condition. The lists are added as part of the match condition within the data policy. Within the **Action** tab, click **Accept** and add NAT VPN 0. Click **Save Match and Actions**.

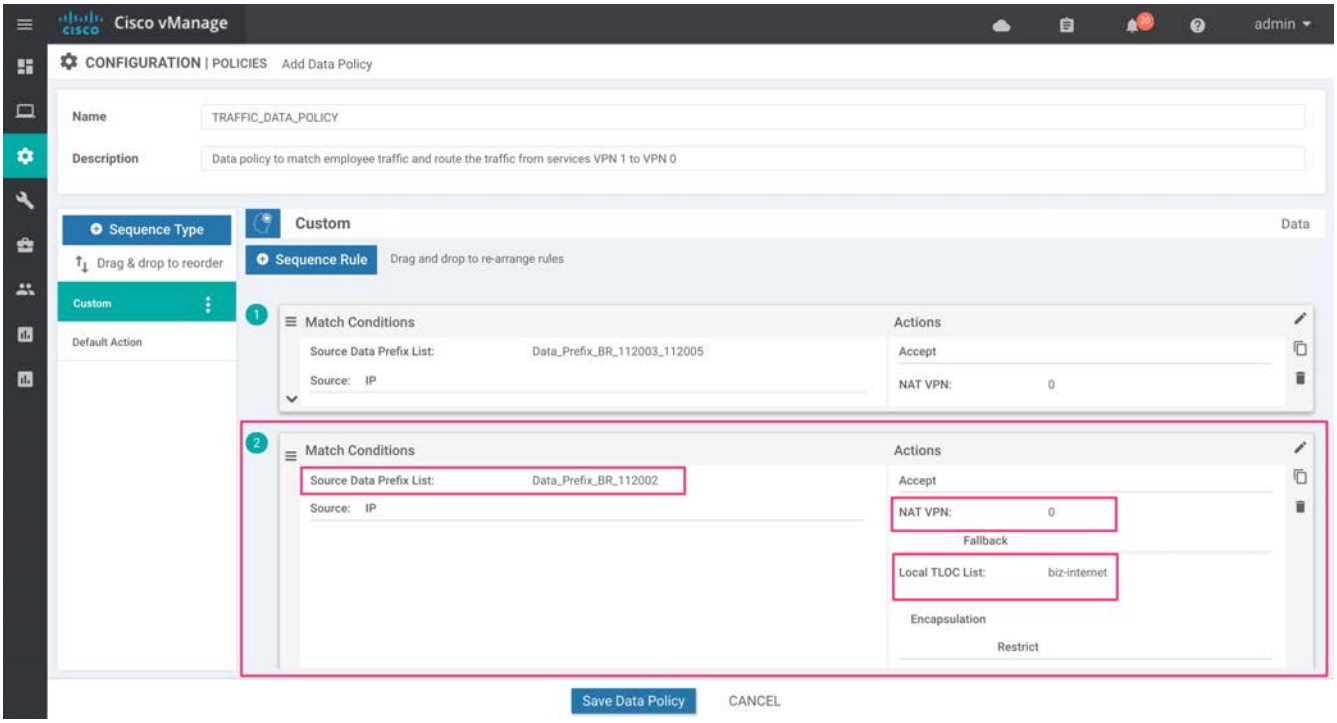


Here's an example of how the traffic data policy can be created. Two separate sequence rules are added to allow DIA, and a separate sequence rule is configured before the DIA sequence rule to maintain the flow of internal branch to branch or branch to datacenter traffic across SD-WAN overlay network.

In the following screenshot, the first sequence rule accepts the flow of internal traffic based on the destination prefix, and the second sequence rule is configured to enable DIA for SD-WAN XE platforms based on source data prefix.

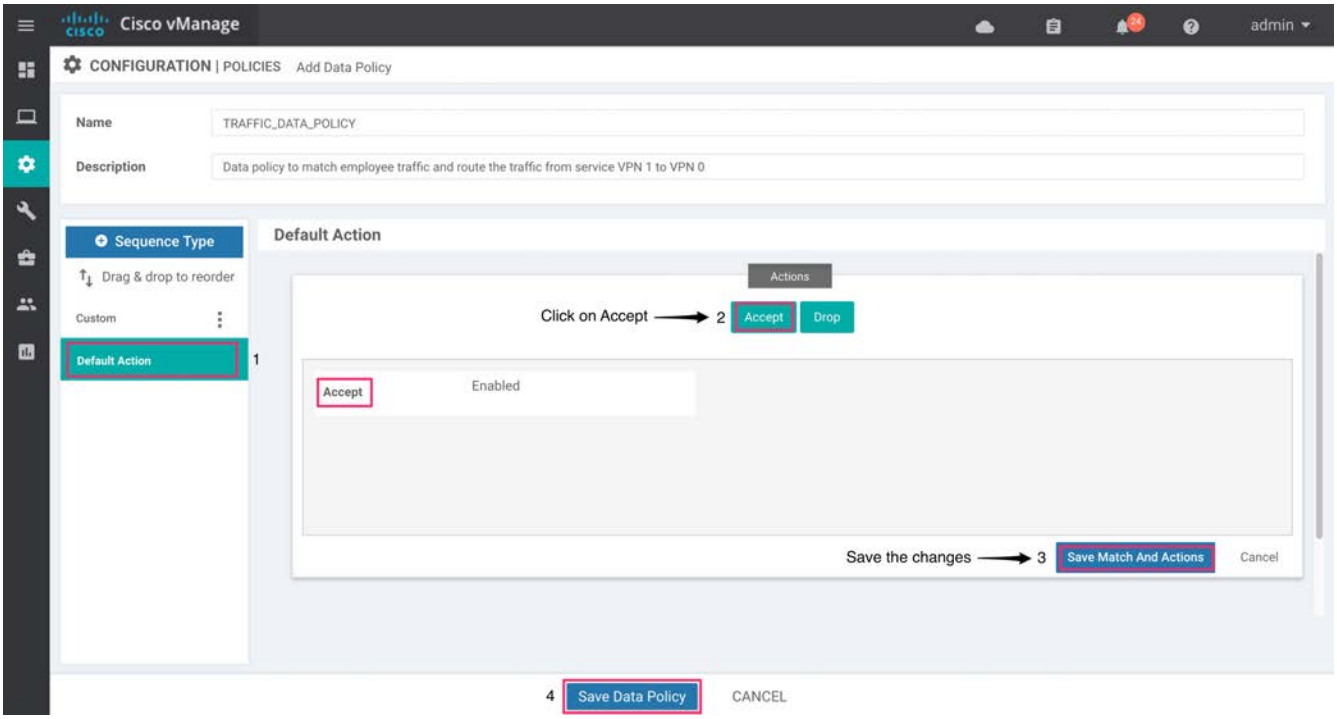


The third sequence rule allows DIA for vEdge router platforms based on the source data prefix. Within the tab **Action**, path preference is set using **Local TLOC List.**



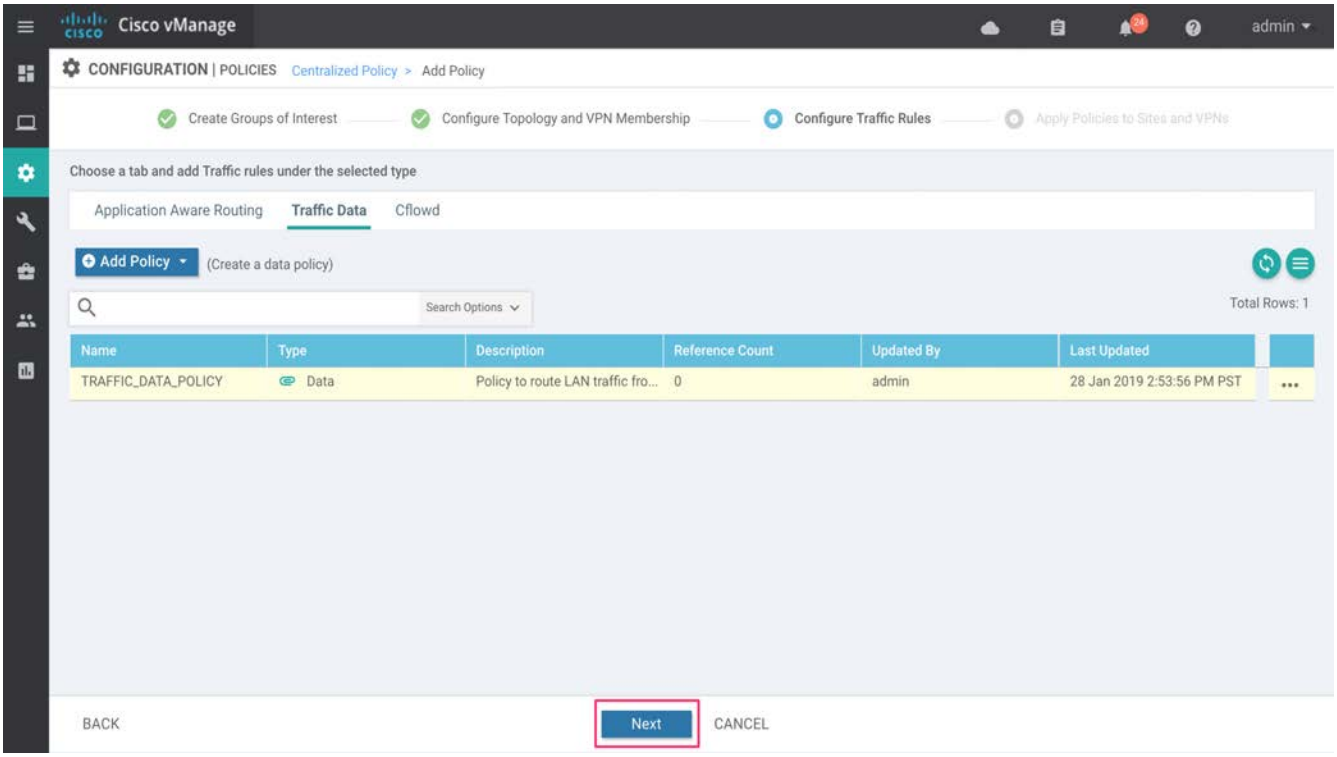
8. If a packet matches none of the parameters configured in any of the sequences within the policy, it is dropped and discarded by default. To avoid packet drops, within the tab **Custom**, modify the **Default Action** and click **Accept**.

   Select **Save Data Policy** to save the parameters.



Technical Tip: If a centralized policy is already configured with a traffic data policy embedded in it, then you can either edit the existing data policy to include additional sequence rules, as listed earlier, to enable DIA or add a new traffic data policy under same centralized data policy to enable DIA. However, preview the policy configuration to ensure that the order of traffic data policy is correct and does not break the flow of overlay traffic.

9. Select **Next** to apply policies to sites and VPNs in the wizard.



Step 3: Apply Policy to Sites and VPNs

Apply the policy to sites and VPNs configured within the groups of interest.

10. Firstly, provide a **Policy Name** and **Policy Description.**

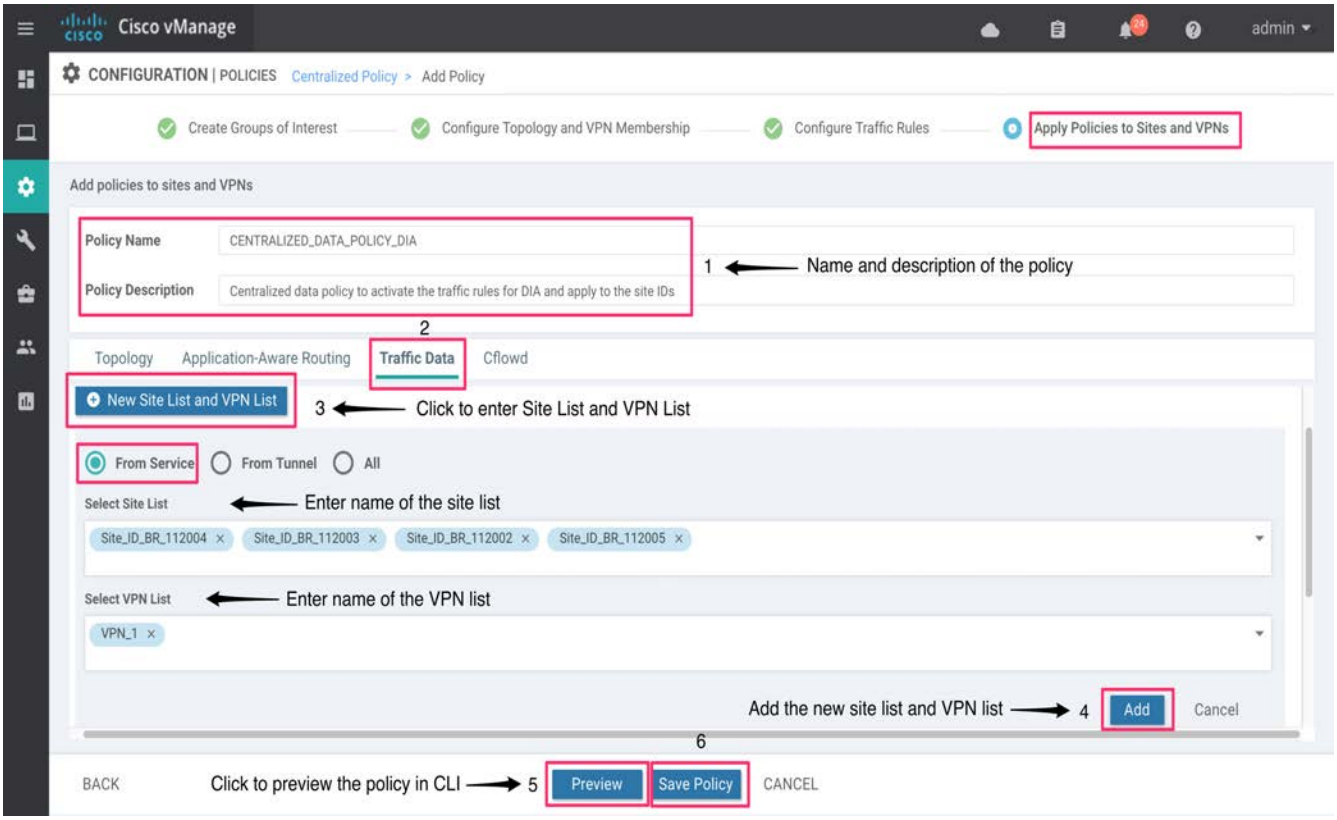
Policy Name	Policy Description
CENTRALIZED_DATA_POLICY_DIA	Centralized data policy to activate the data policy and apply to the site IDs.

11. Select the **Traffic Data** tab.

    1. Click **New Site List and VPN List**
    2. By default, the data policy applies to all data traffic passing through the WAN edge router. To have the data policy apply only to the traffic coming from the service side, select the **From Service** option.
    3. Choose the sites that you want the data policy to be applied to by selecting one or more site lists.

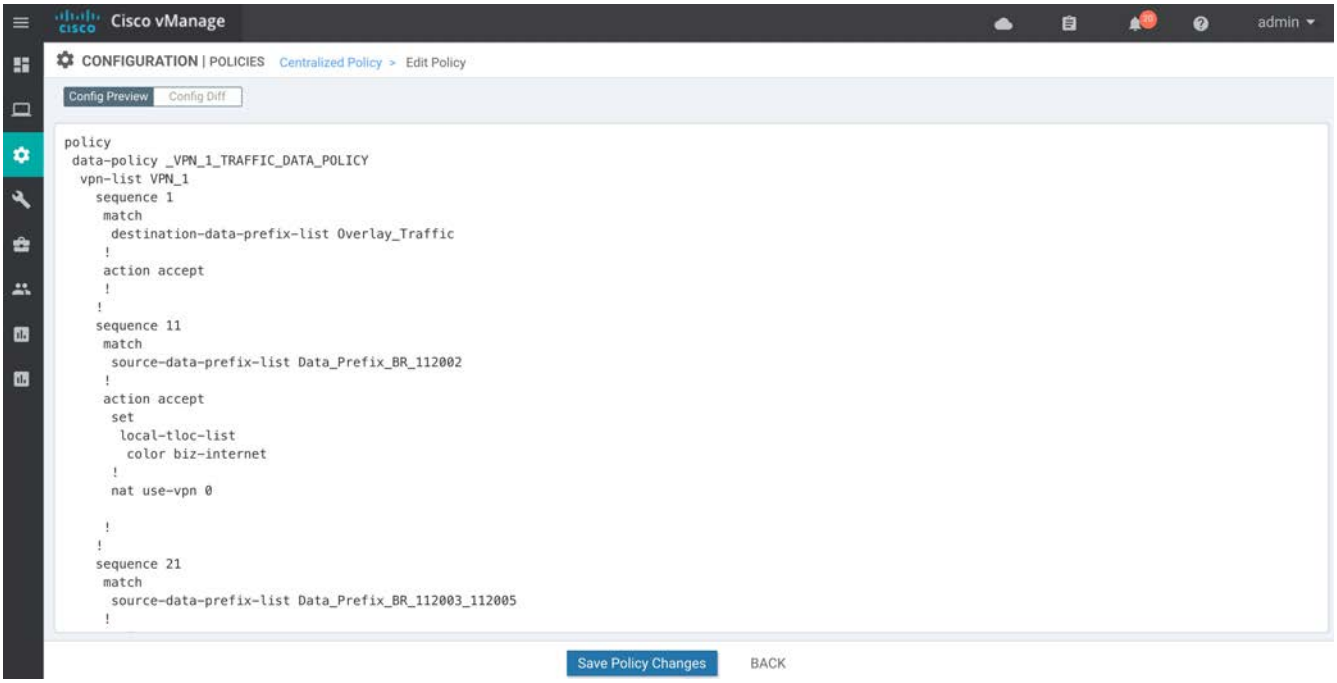
4. Choose the service VPNs that you want the data policy to be applied to by selecting one or more VPN lists.

5. Click the **Add** button to complete the data policy.

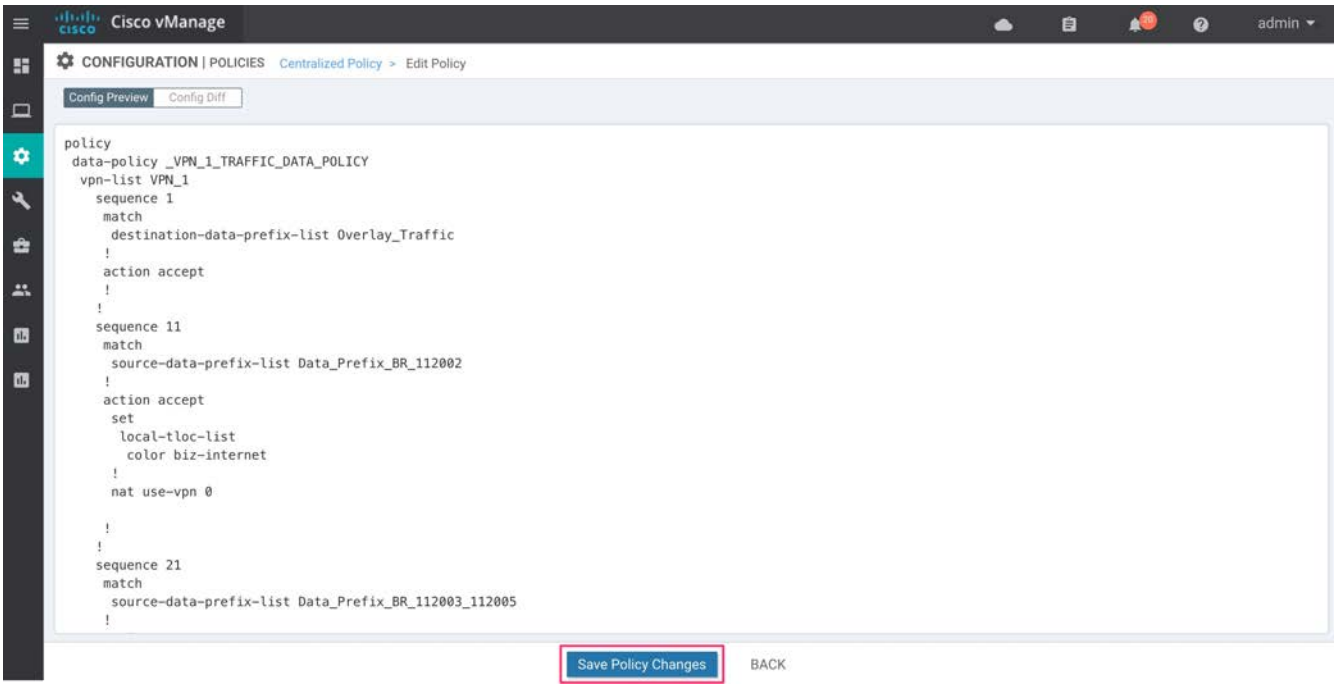


Technical Tip: For all data-policy policies that you apply, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs is when two site lists, site-list 1 containing site-id 1-100, and site-list 2 containing site-id 70-130. Here, sites 70 through 100 are part of both lists. If you were to apply these two site lists to two different data-policy policies, the attempt to commit the configuration on the vSmart controller would fail.

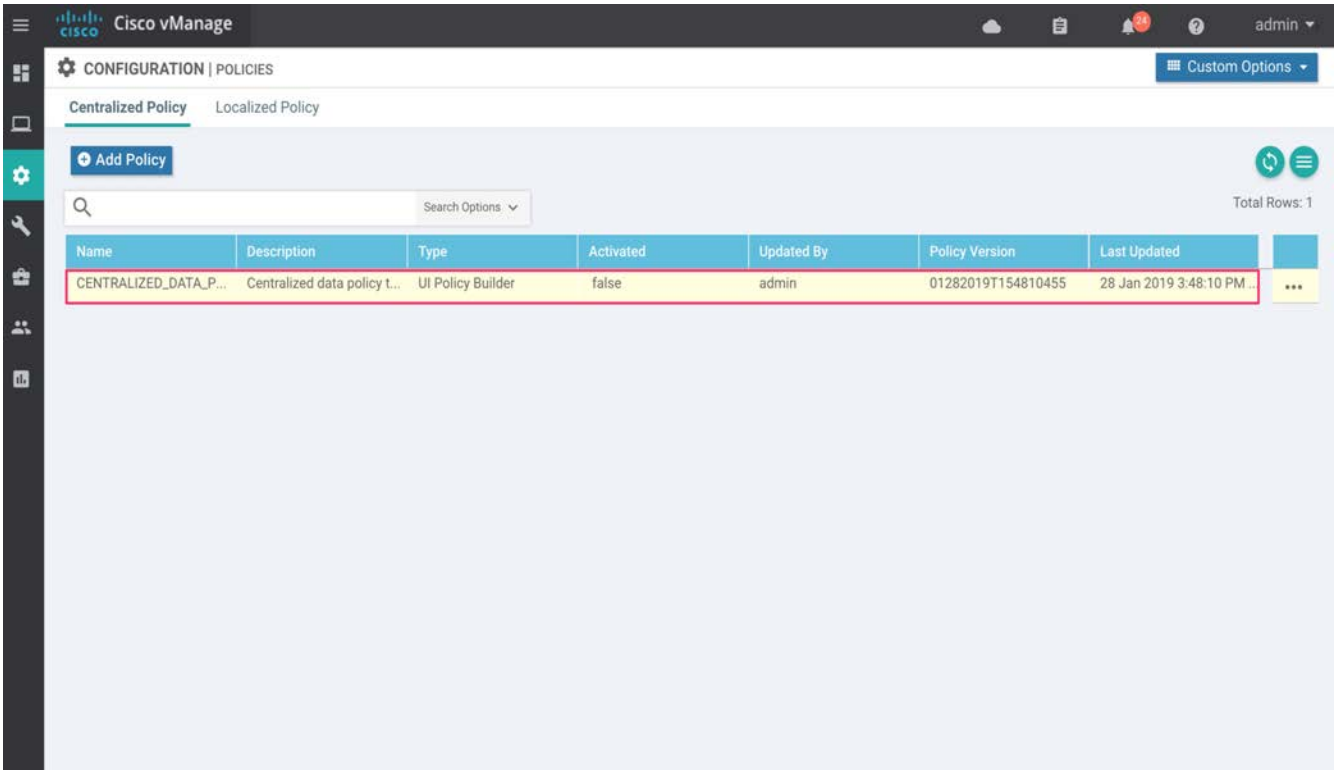
12. Click **Preview** to view the configured policy. The policy is displayed in CLI format.



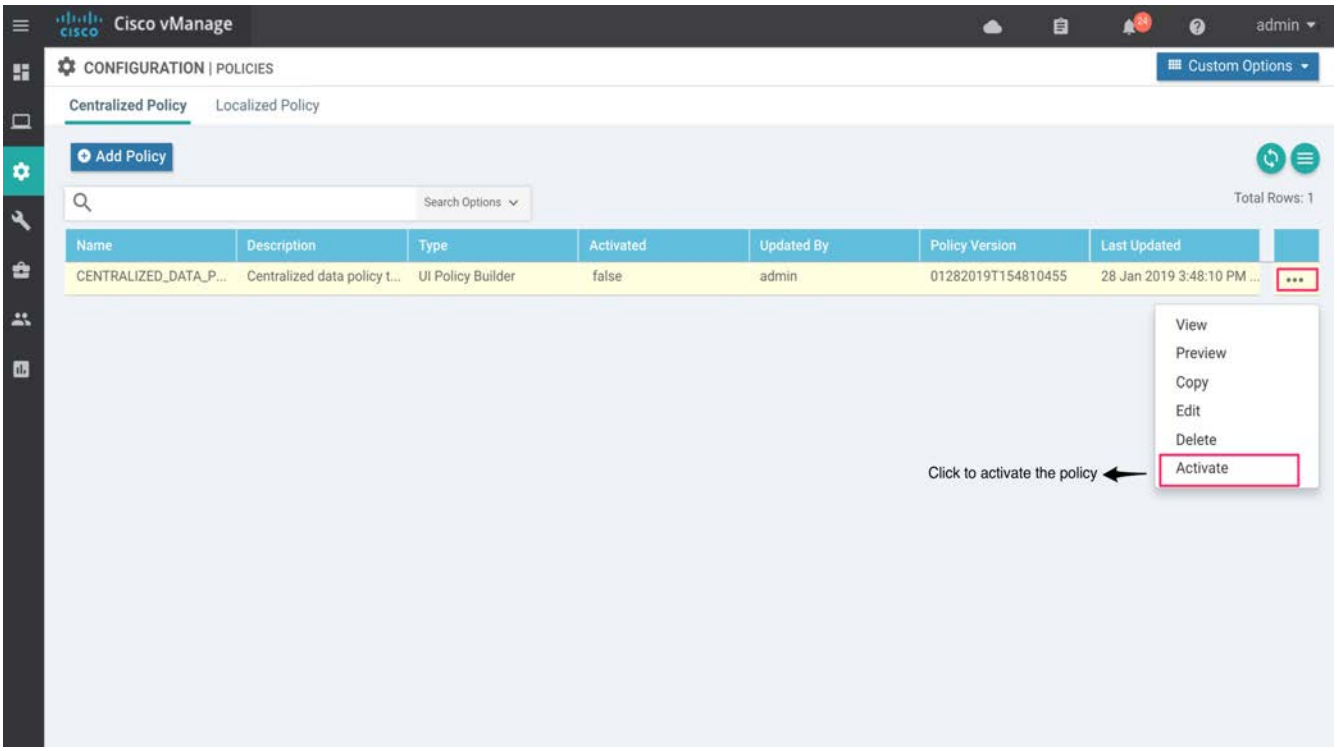
13. Click **Save Policy** to save the new centralized policy.



14. Within **CONFIGURATION | POLICIES** tab, the newly created policy is added under the **Centralized Policy** section.



15. To activate the centralized policy, click the three dots at the right of the policy screen and select **Activate**.

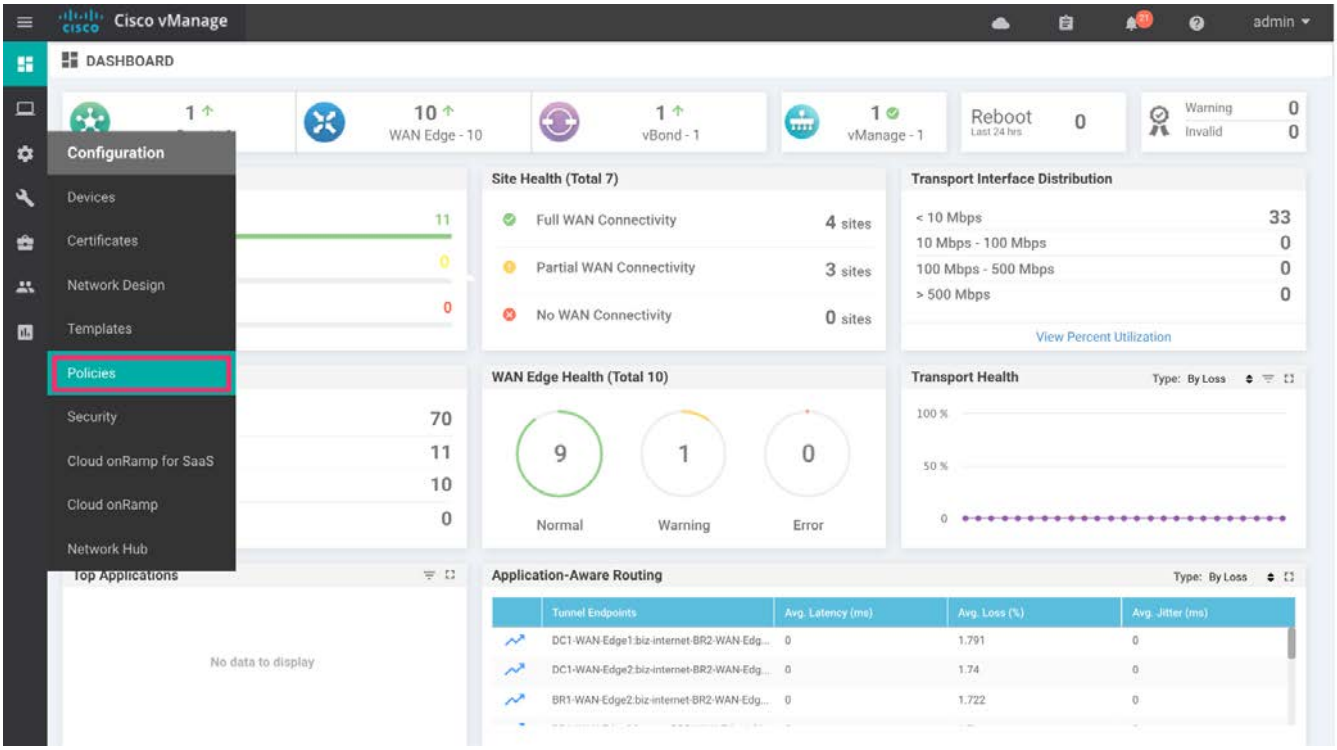


Once activated, the policy is pushed into the vSmart controller. Next, based on the site ID list, the results of the data policy are pushed to the designated WAN Edge devices via OMP.

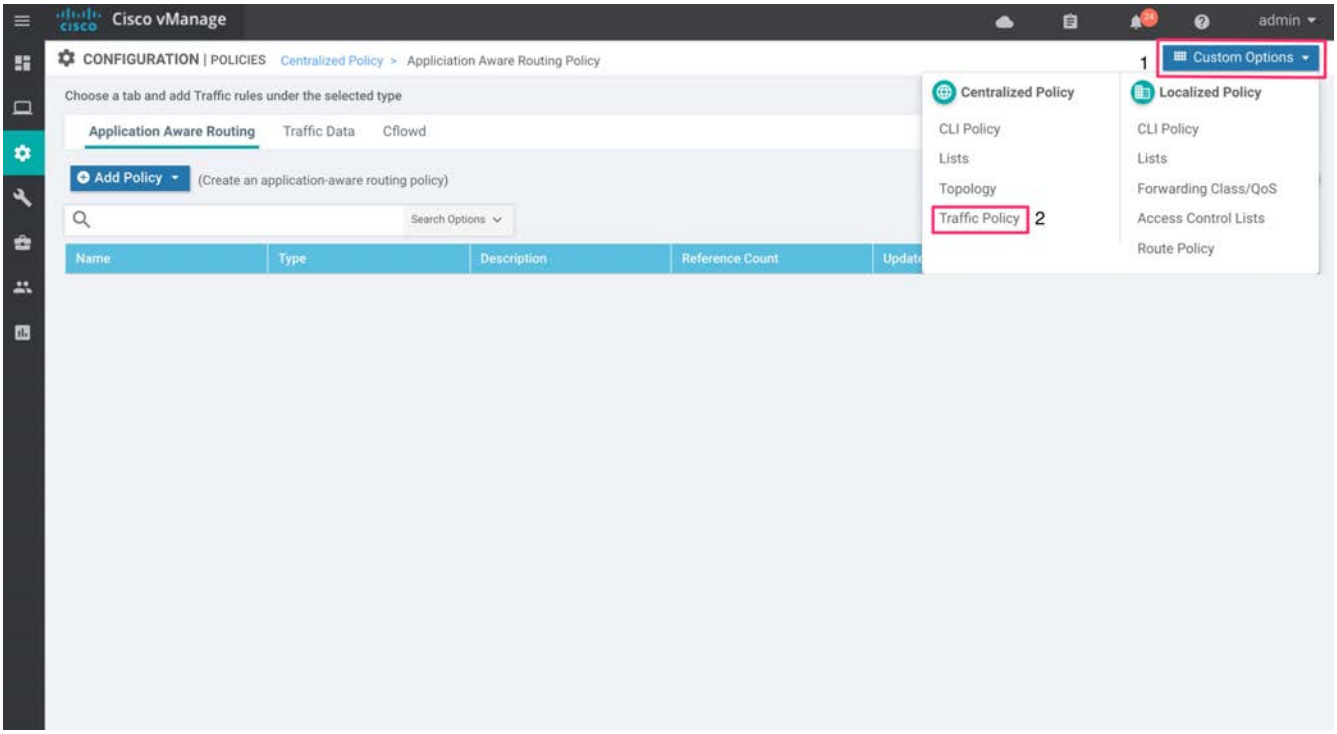
Alternate Method to Deploy Traffic Data Policy

This section explains an alternate method to build traffic data policy and import an existing traffic data policy into the centralized policy. Skip this section if the traffic policy was built based on the steps above and is already attached to the centralized policy.

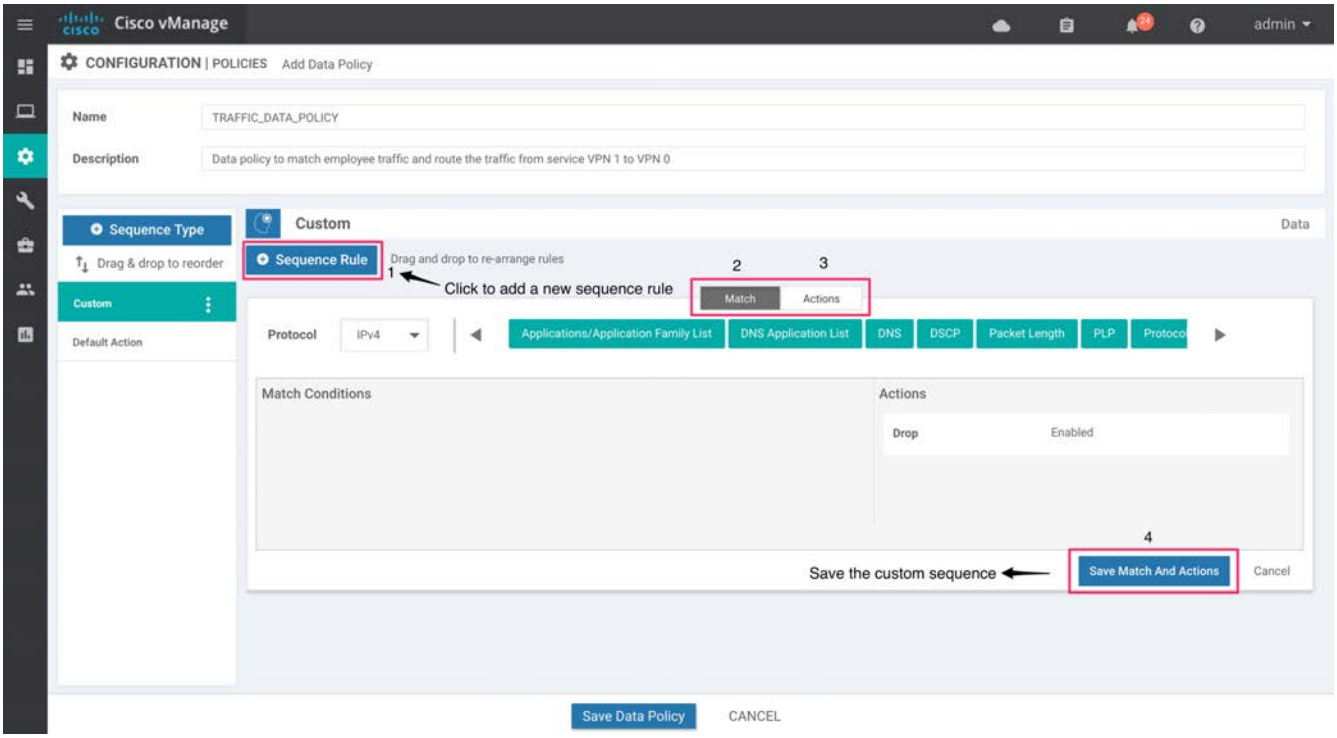
1. Go to **Configuration** > **Policies.**



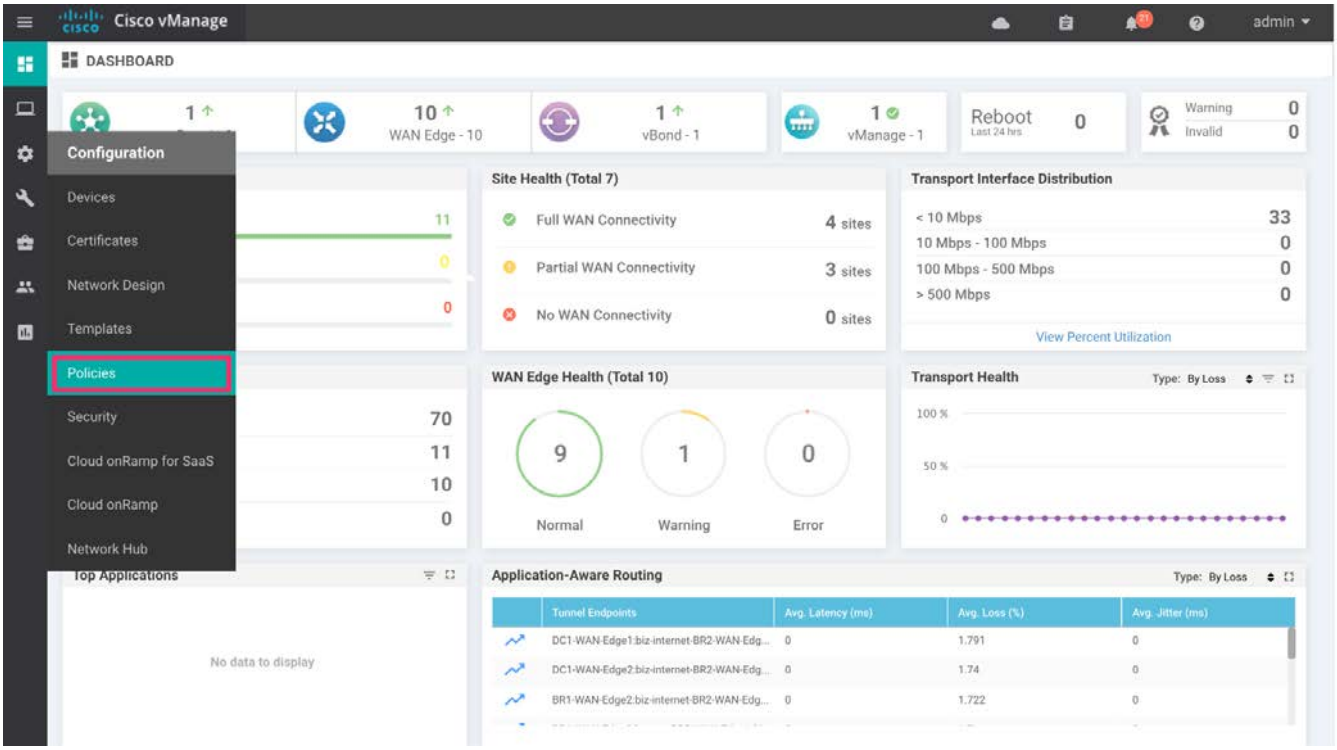
2. Click **Custom Options** on the top right and navigate to **Traffic Policy** under Centralized Policy.



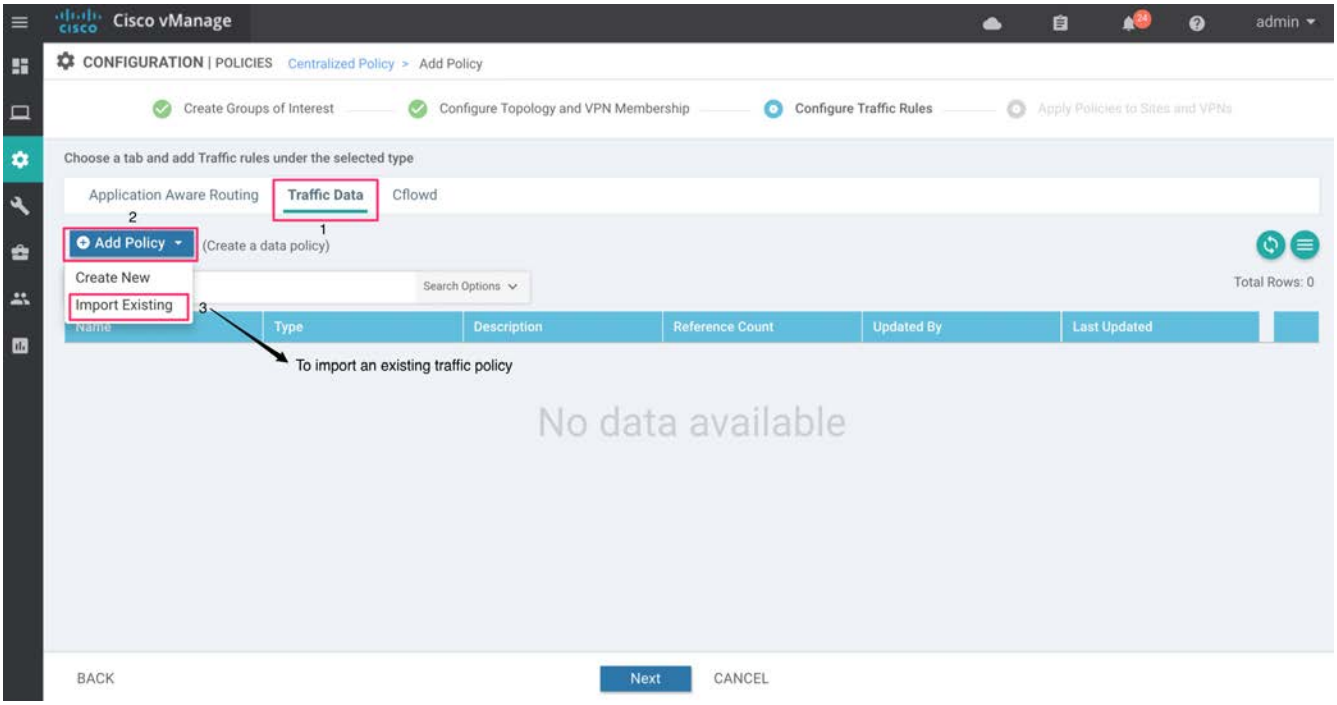
3. The configured lists are added under the **Match/Action** condition within the traffic data policy.



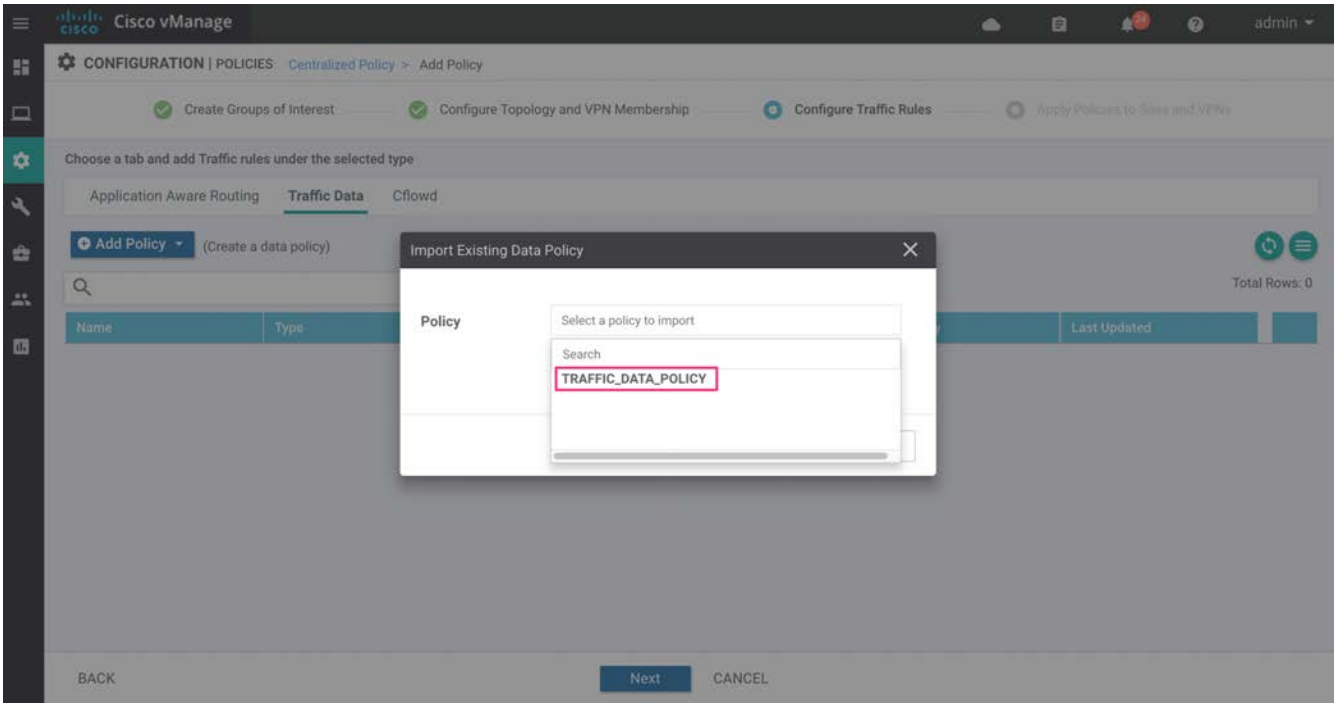
4. Next, import the configured traffic data policy to centralized data policy. Navigate back to Centralized Policy and click **Policies**.



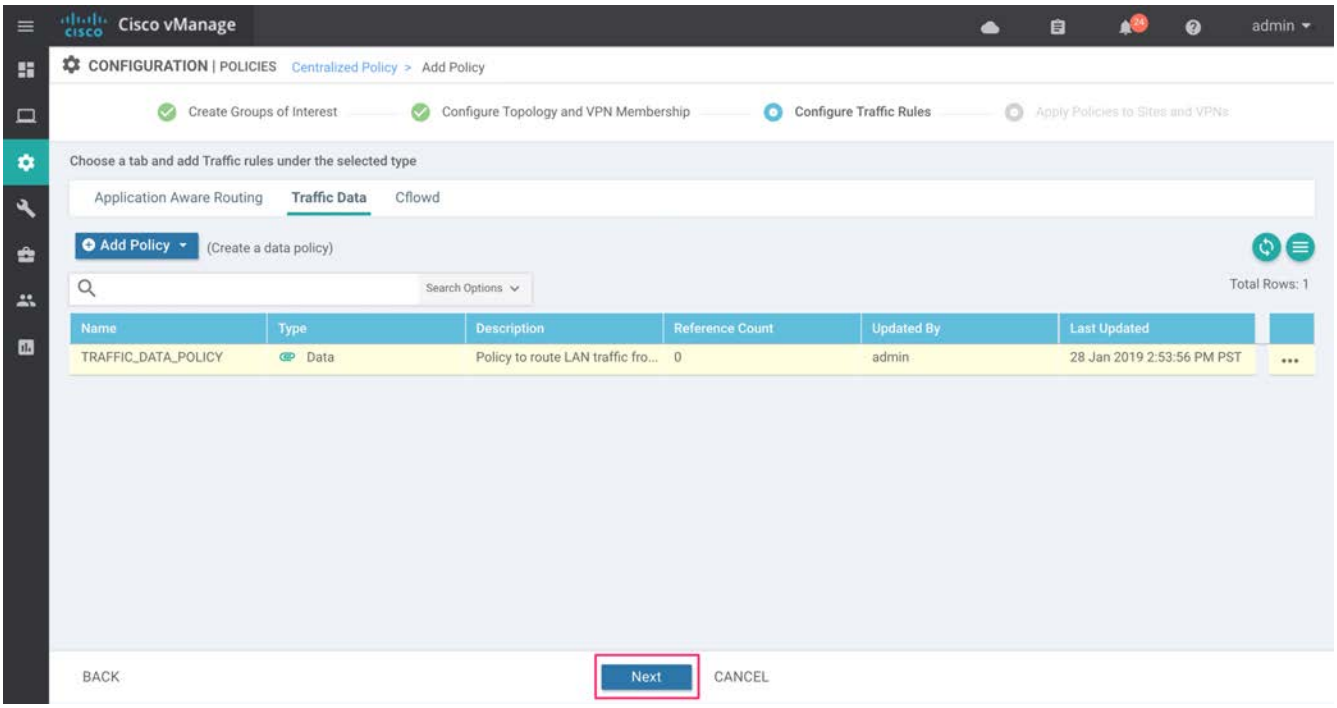
5. On the **CONFIGURATION | POLICIES** page, navigate to **Configure Traffic Rules**, and click **Import Existing** to import an existing traffic data policy.



6. Select the policy from the list and click **Import**.



7. The traffic policy is attached to the centralized data policy. Click **Next** to provide a name to the new centralized data policy and attach VPN/Sites.



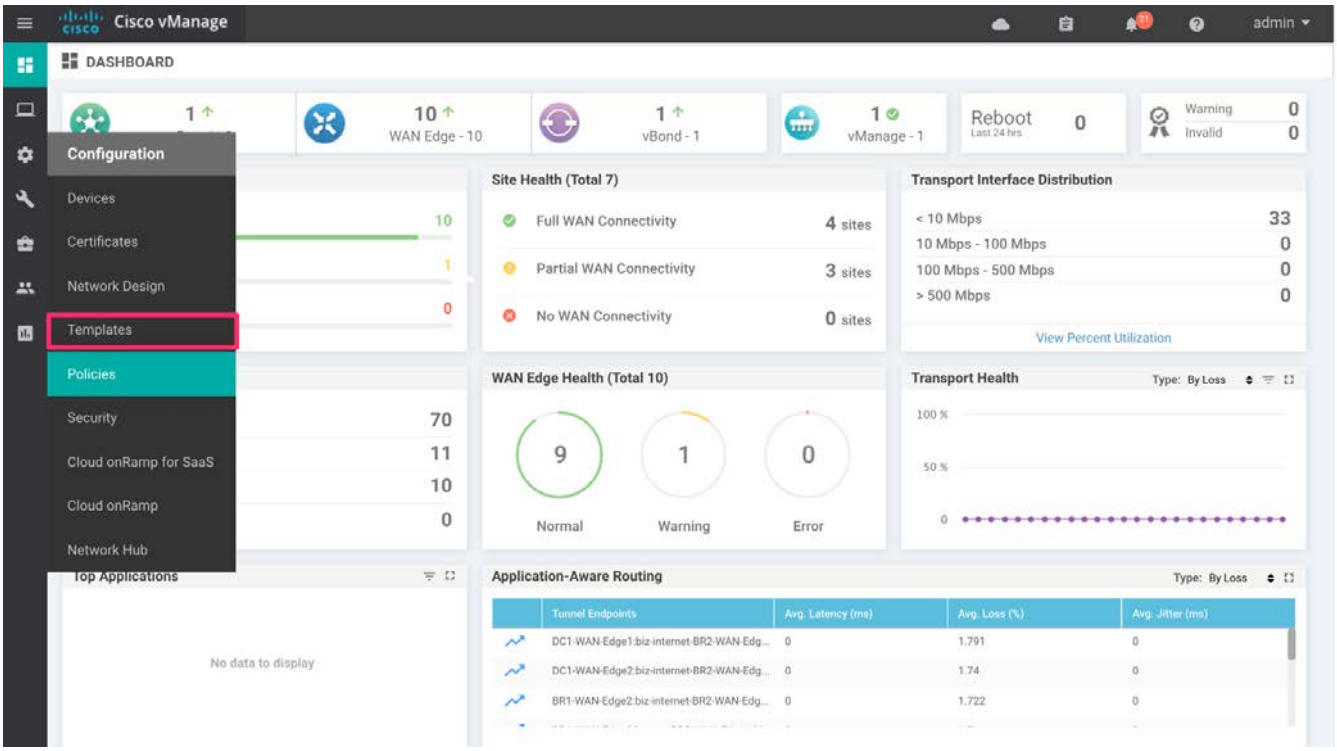
Procedure 2: Use Case #2 - Create NAT DIA Route to Redirect Guest Internet

In this procedure, a NAT DIA route is configured to route all remote-site guest Internet traffic from service side VPN 2 to VPN 0, which will allow the traffic to exit directly to the local Internet.

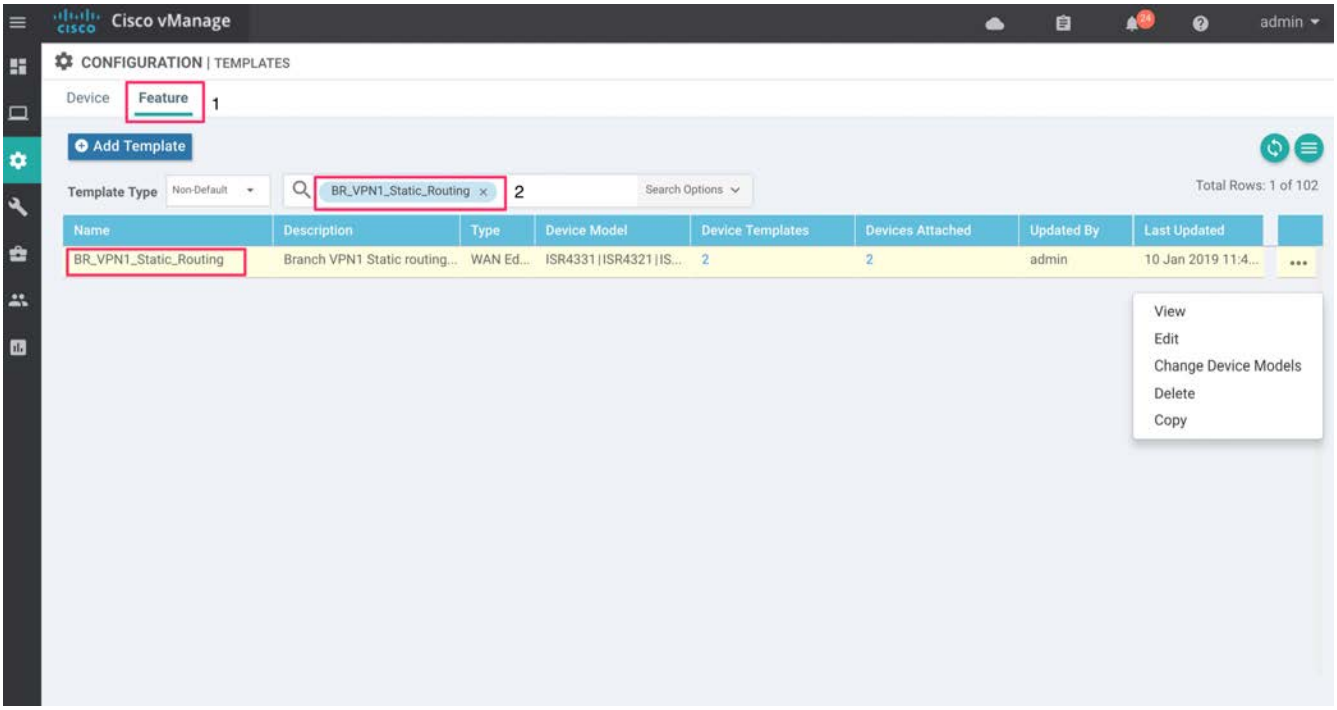
Step 1: Create Feature Template with NAT DIA Route

Configure a NAT DIA route within VPN 2 by creating a new template from one of the existing branch templates. Use a VPN template corresponding to a service VPN. In this guide, we have generated a copy of an existing service VPN branch template **BR_VPN1_Static _Routing** (Refer to SDWAN deployment guide to build new templates).

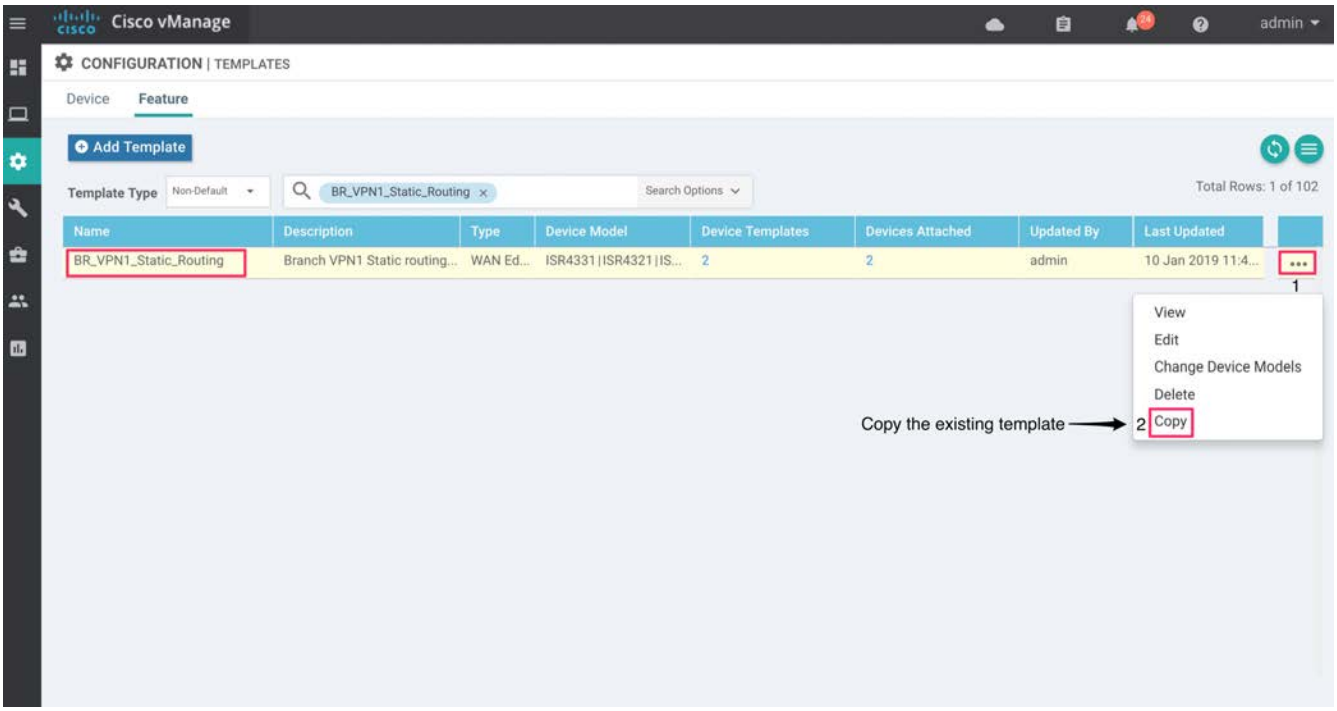
1. Go to **Configuration** > **Templates.**



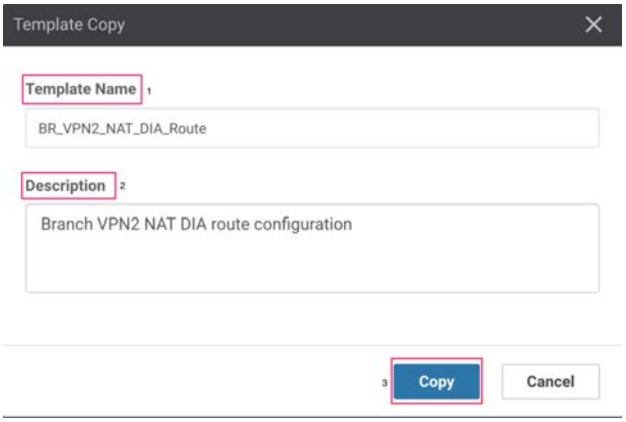
2. Click the **Feature** tab. Find the desired feature template (**BR_VPN1_Static _Routing).**



3. Click three dots (…) to the right of the feature template and select **Copy** from the drop-down list.



4. In the pop-up window, enter a Template Name (**BR_VPN2_NAT_DIA_Route**) and Description (**Branch VPN2 NAT route configuration**)



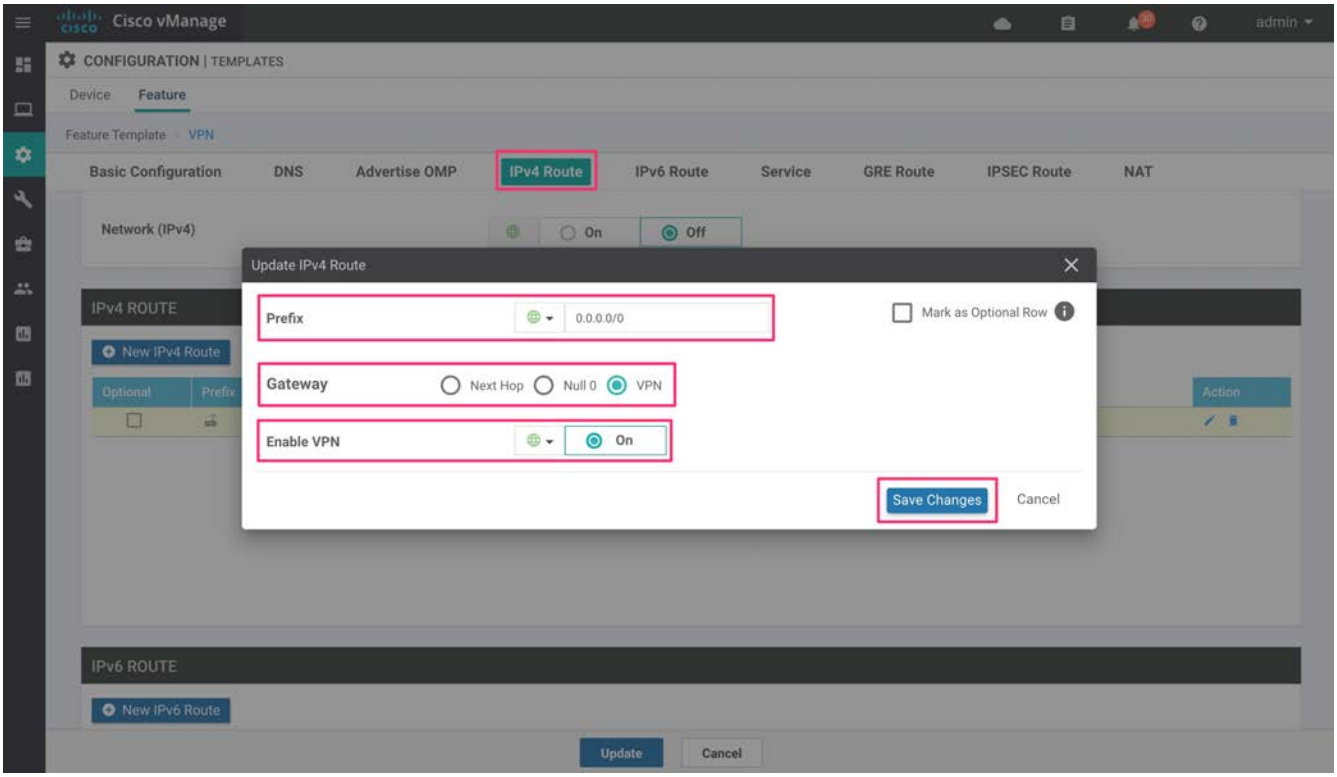
5. Click **Copy.**

   Once a copy of the template is generated, find the newly-created template (**BR_VPN2_NAT_DIA_Route**). To do so, click the three dots (…) next to the desired template and select **Edit**.

   Ensure that the following parameters are set within the template:

Table 6 **Template BR_VPN2_NAT_DIA_Route**

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	2
	Name	Global	Service Guest VPN
IPv4 Route	Prefix	Global	0.0.0.0/0
	Gateway	Radio button	VPN
	Enable VPN	Global	On



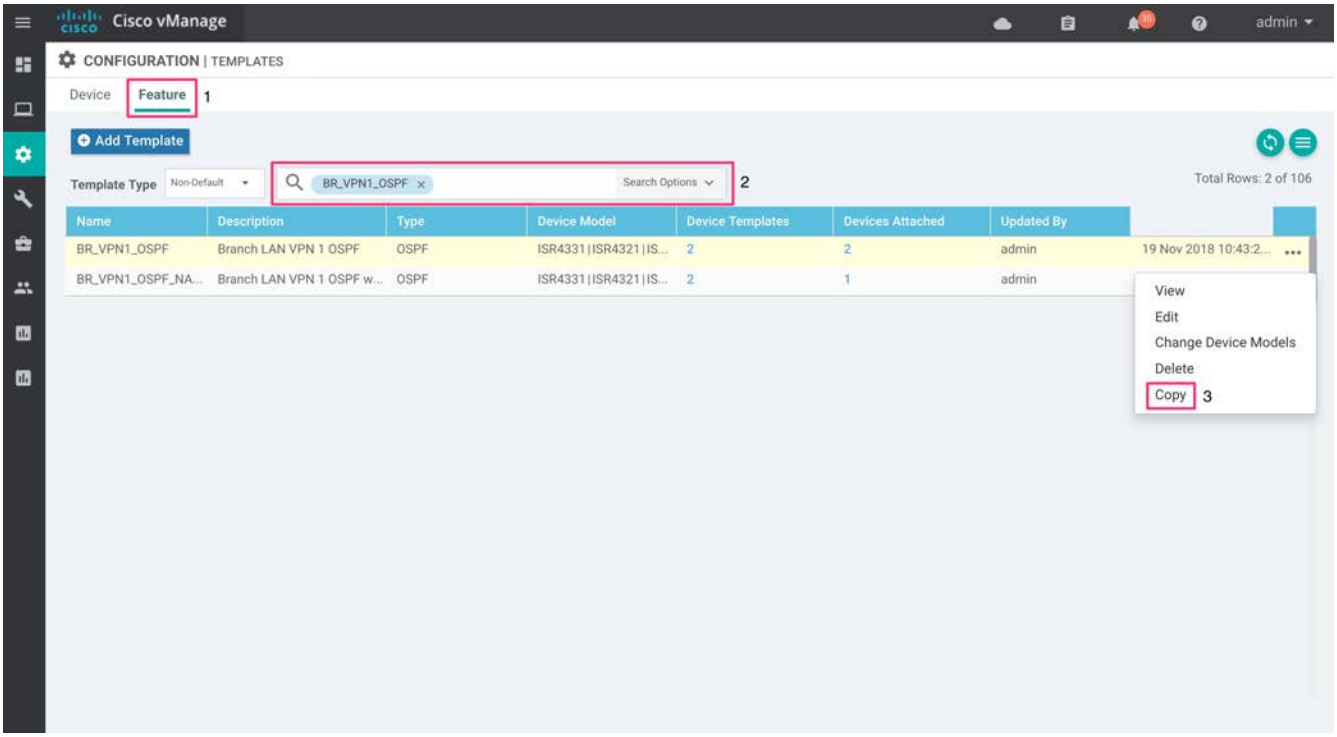
6. Update or save the modified template.

Based on the configuration above, when a packet hits an interface within Service VPN or VPN 2, the packet is forwarded to the NAT-enabled transport VPN (VPN 0) interface. The packet then exists directly to the Internet. To understand how NAT DIA configuration works in detail, refer to the Design Section of this guide. See Appendix D for all the templates used within this guide.

Step 2: Redistribute the NAT DIA Route into the Routing Protocol

In this guide OSPF is running between the LAN or service side of each WAN edge device and L3 distribution switch. Therefore, proceed to redistribute the NAT DIA route into the routing protocol.

7. To redistribute the NAT DIA route into OSPF, copy the existing OSPF feature template, **BR_VPN1_OSPF** as done earlier in step 3.



8. Enter a new name for the template (**BR_VPN2_OSPF_NAT_REDISTRIBUTE**) along with a description (**Branch LAN VPN 2 OSPF with NAT redistribute**) and click **Copy**.

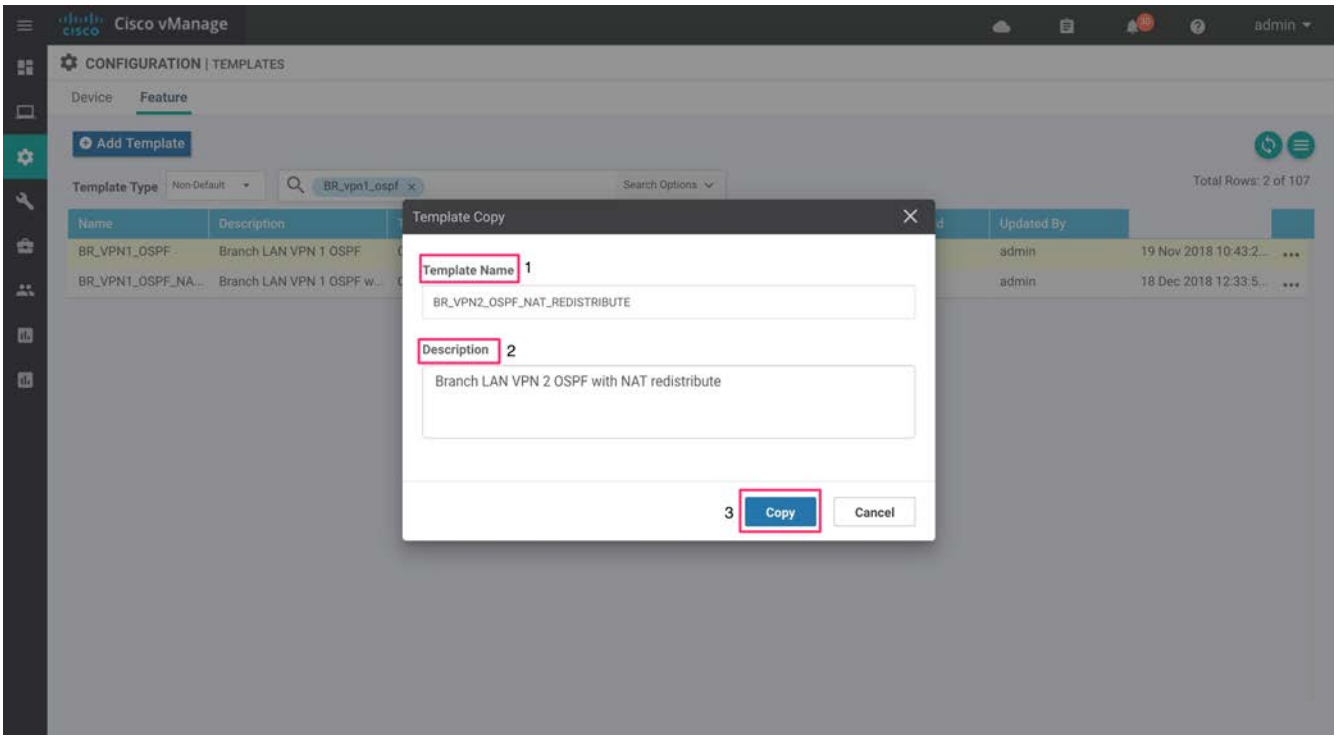
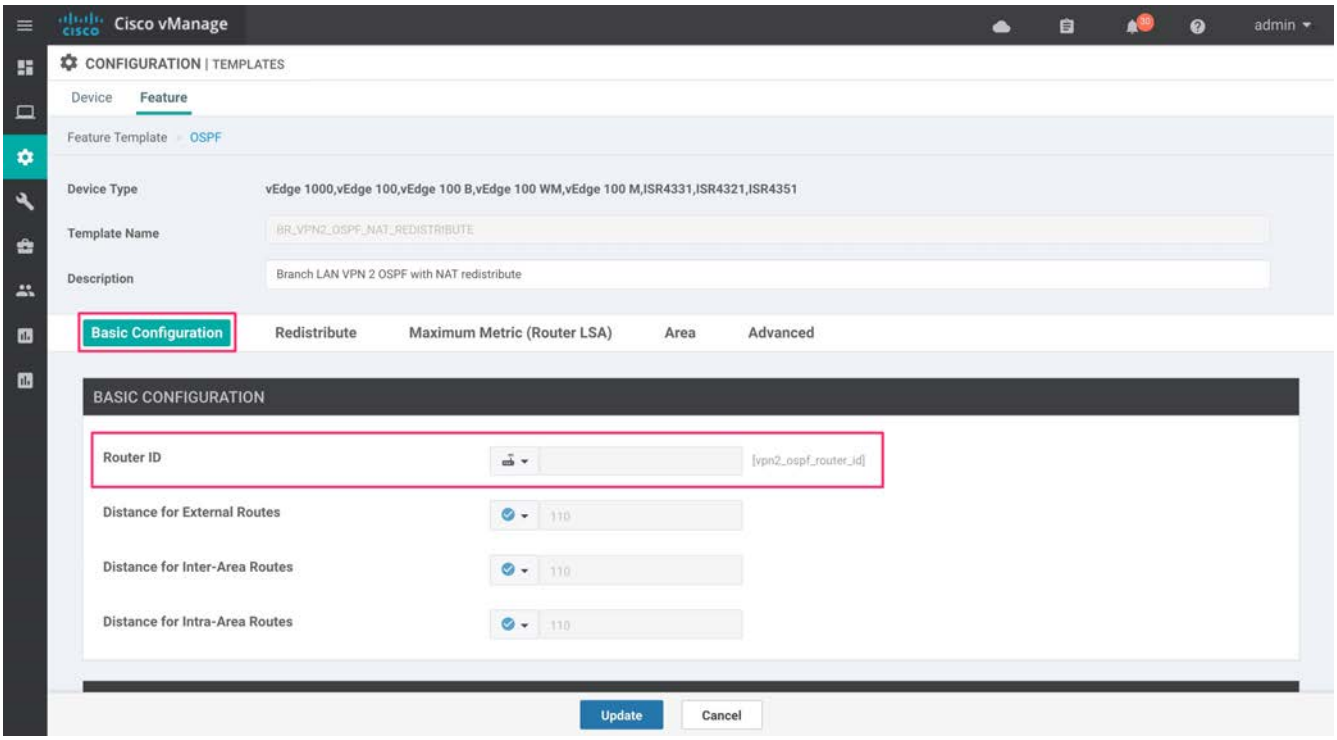


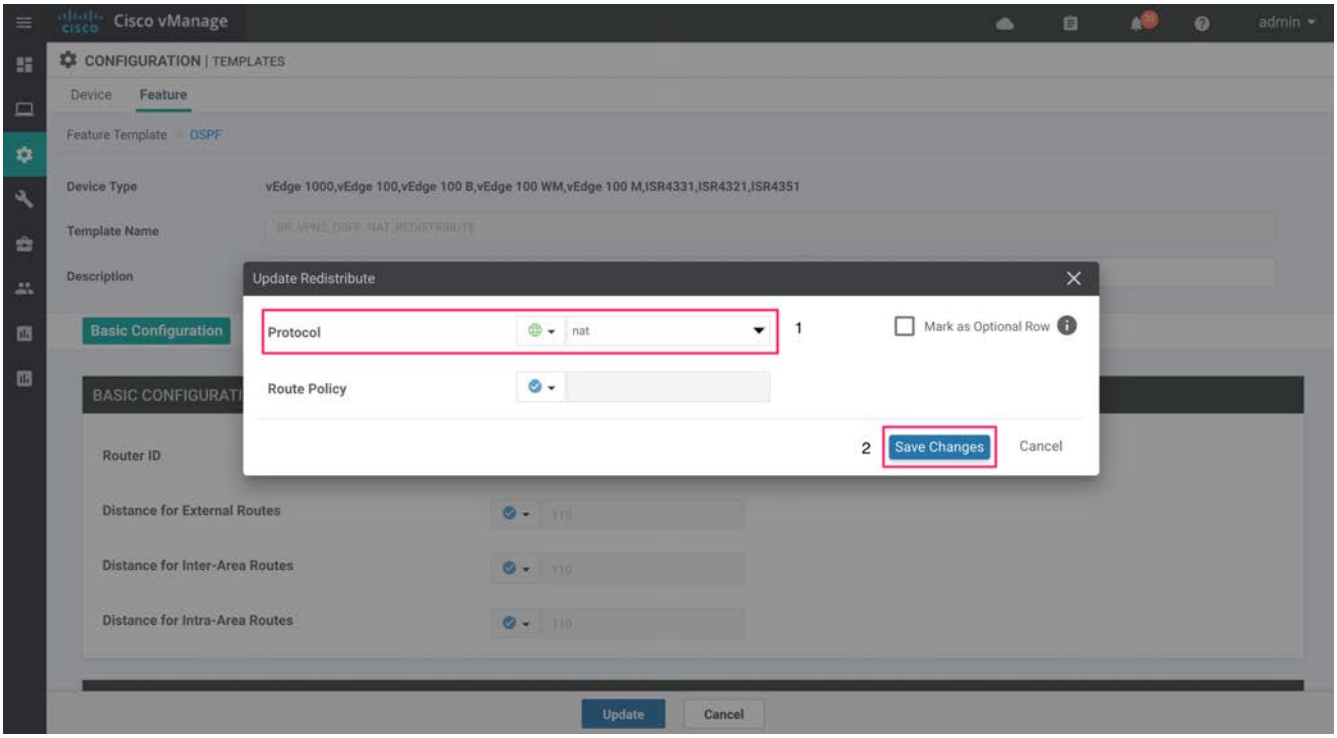
Figure 33 Name and description of the new feature template

9. Edit the **BR_VPN2_OSPF_NAT_REDISTRIBUTE** template and add the following:

Table 7 **Template BR_VPN2_OSPF_NAT_REDISTRIBUTE**

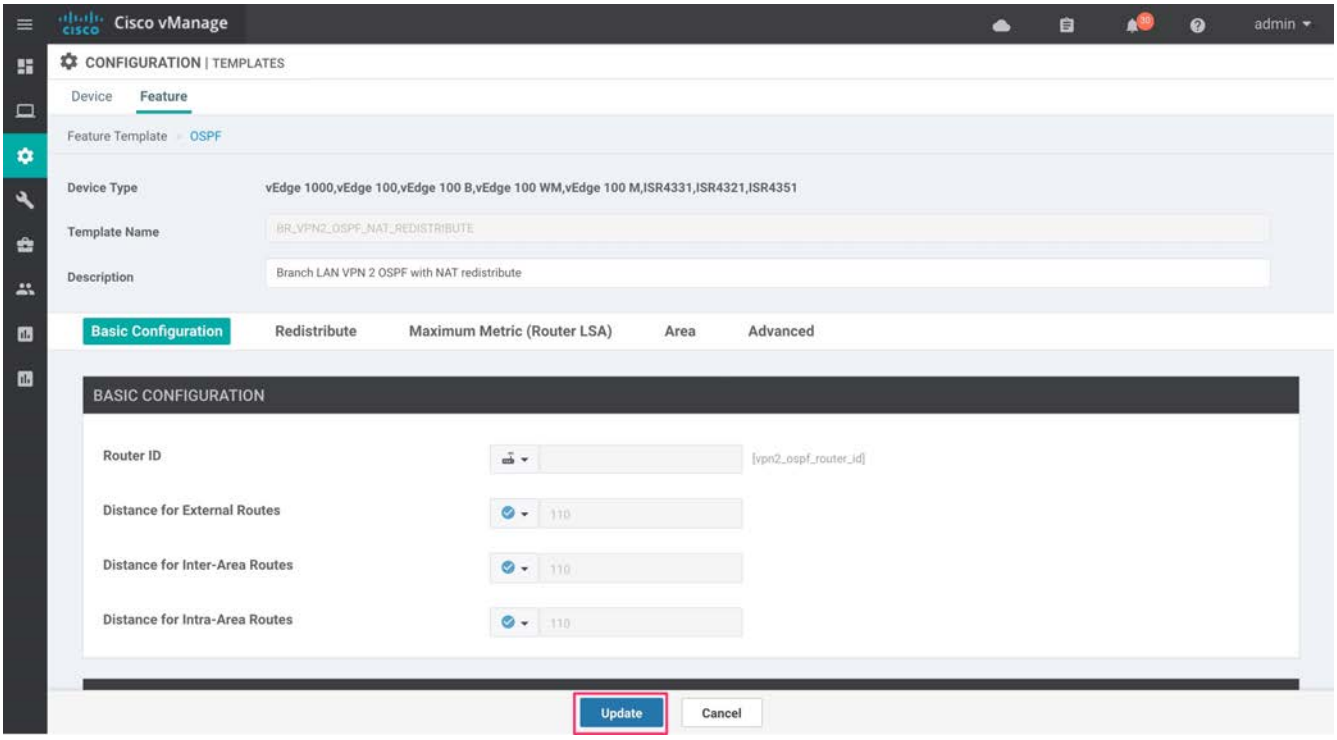
Section	Parameter	Type	Variable/Value
Basic Configuration	Router ID	Device Specific	vpn2_ospf_router_id
Redistribute	Protocol	Global	nat





Click **Save Changes** to add the redistribute NAT statement into the template.

10. Finally, click **Update** or save the **BR_VPN2_OSPF_NAT_REDISTRIBUTE** template.



Process 3: Add the Configured Feature Templates to Device Template

11. Go to **Configuration > Templates** to see the list of device templates.
12. Edit the desired WAN Edge device template.
    1. Under **Service VPN** next to **VPN**, select the feature template modified to include the NAT DIA route (**BR_VPN2_NAT_DIA_Route**)
    2. Under **Service VPN** next to **OSPF**, select the feature template modified to redistribute the NAT route into OSPF (**BR_VPN2_OSPF_NAT_REDISTRIBUTE**).

    Here's an example of the device template with the new feature templates attached to it.

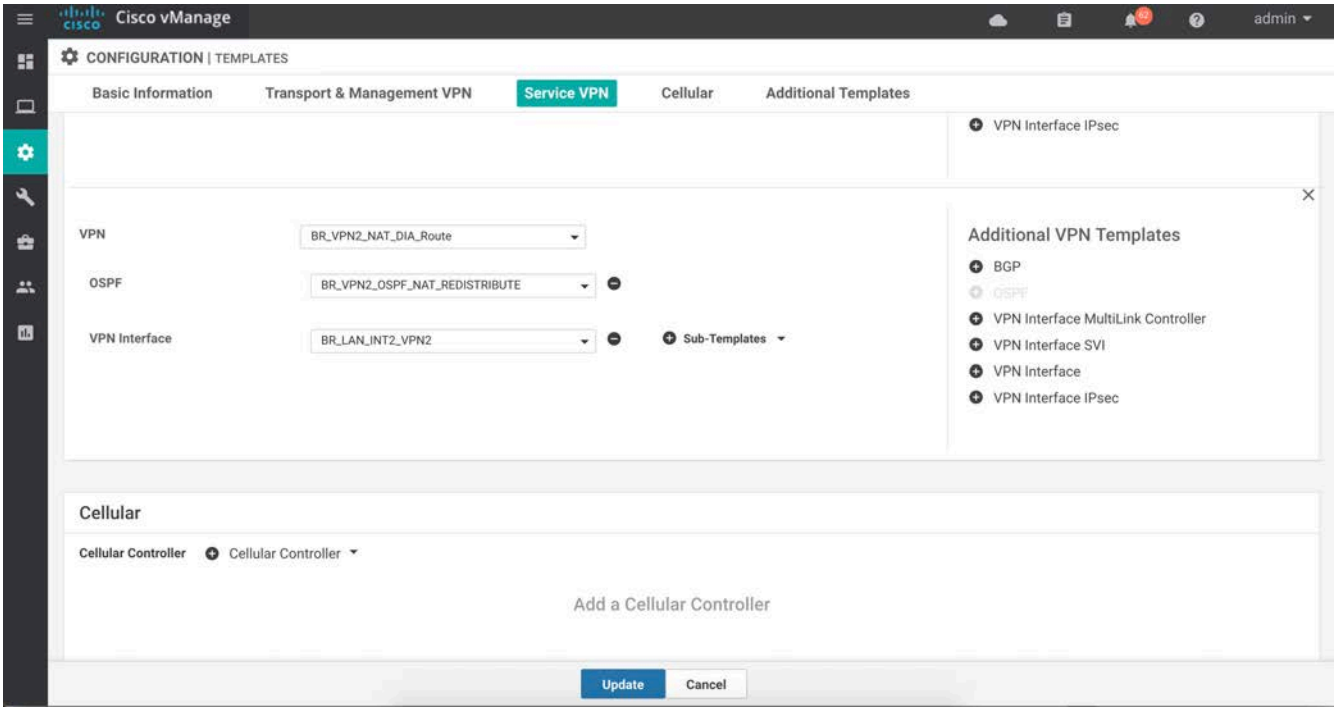


Figure 34 Device Template with NAT DIA configured

Based on the configuration added, 0.0.0.0/0 route is installed into the IOS-XE Routing Information base as a 'nat-dia' type. This route is then redistributed into OSPF protocol on the LAN side.

Once the templates are pushed through the configuration, this is how they would appear.

On IOS XE SD-WAN Router Platforms

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/2
overload

  ip nat translation tcp-timeout 60

  ip nat translation udp-timeout 1

  ip nat route vrf 2 0.0.0.0 0.0.0.0 global

router ospf 2 vrf 2
```

```
    auto-cost reference-bandwidth 100000
    timers throttle spf 200 1000 10000
    router-id 10.30.31.31
    default-information originate
    distance ospf external 110
    distance ospf inter-area 110
    distance ospf intra-area 110
    redistribute omp subnets
    redistribute nat-route dia
   !
```

On vEdge Router Platform

```
vpn 2
   name "Service VPN"
   ecmp-hash-key layer4
   router
    ospf
     router-id 10.10.12.12
     auto-cost reference-bandwidth 100000
     default-information originate
     timers spf 200 1000 10000
     redistribute omp
     redistribute nat

!
   ip route 0.0.0.0/0 vpn 0
```

Technical tip: To track the status of the Internet transport link when a NAT DIA route is used for local Internet exit, a system tracker can be configured on vEdge router platforms. This eliminates the issue of internet traffic blackholing when an internet link is down.

Configuration of System Tracker

This section explains how to configure a system tracker to track the status of the Internet transport link when a NAT DIA route is configured.

Step 1: Build the System Tracker Template

To track the status of transport interfaces that are connected to the Internet, system tracker configuration is added to the existing feature template **System_Template**. Note that this feature template would be initially used within the section **System** in your device template to add configurations such as system IP, hostname and so on.

13. Go to **Configuration** > **Templates** and click the **Feature** tab.

14. Find the WAN Edge System template (**System_Template**), click **…** on the far right of the screen and select the **Copy** option.

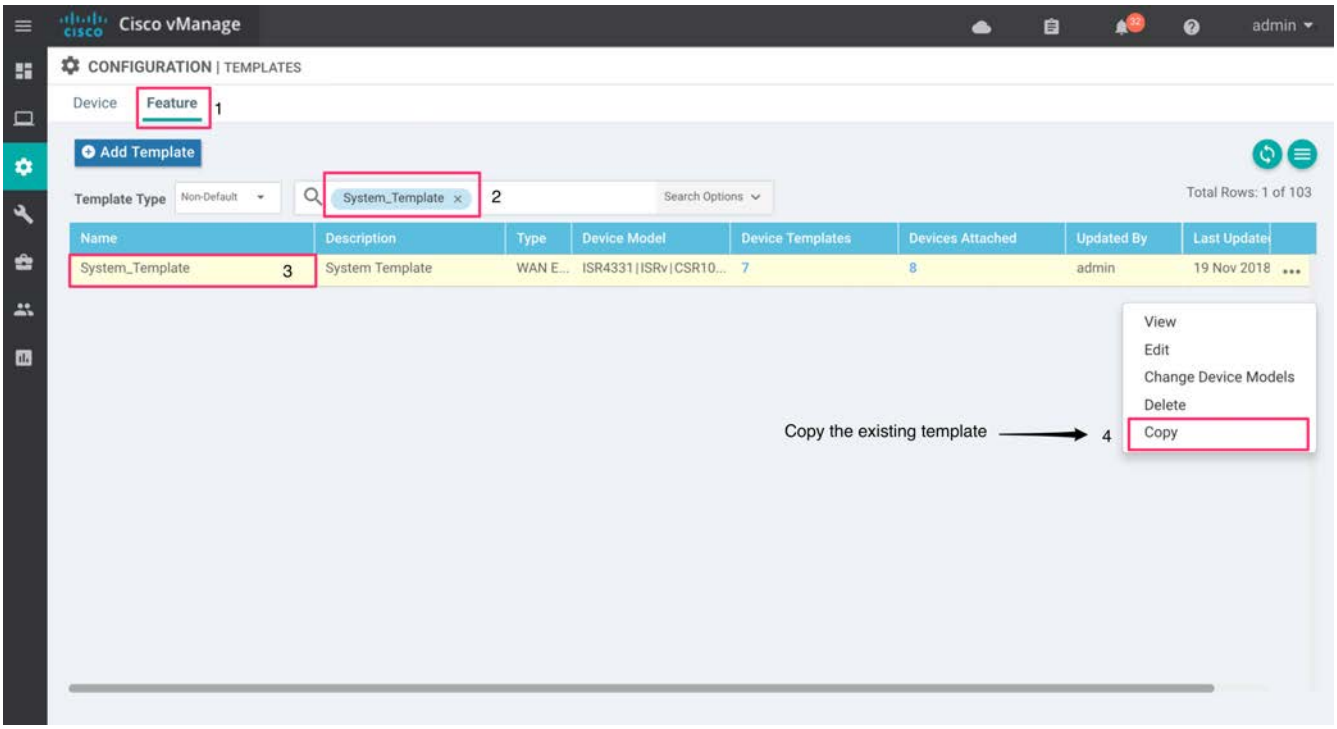


Figure 35 Copy the old template System_Template

15. Enter a new name for the template (**System_Template_Interface_Tracker**) and description (**System Template to track the Internet Interfaces**)

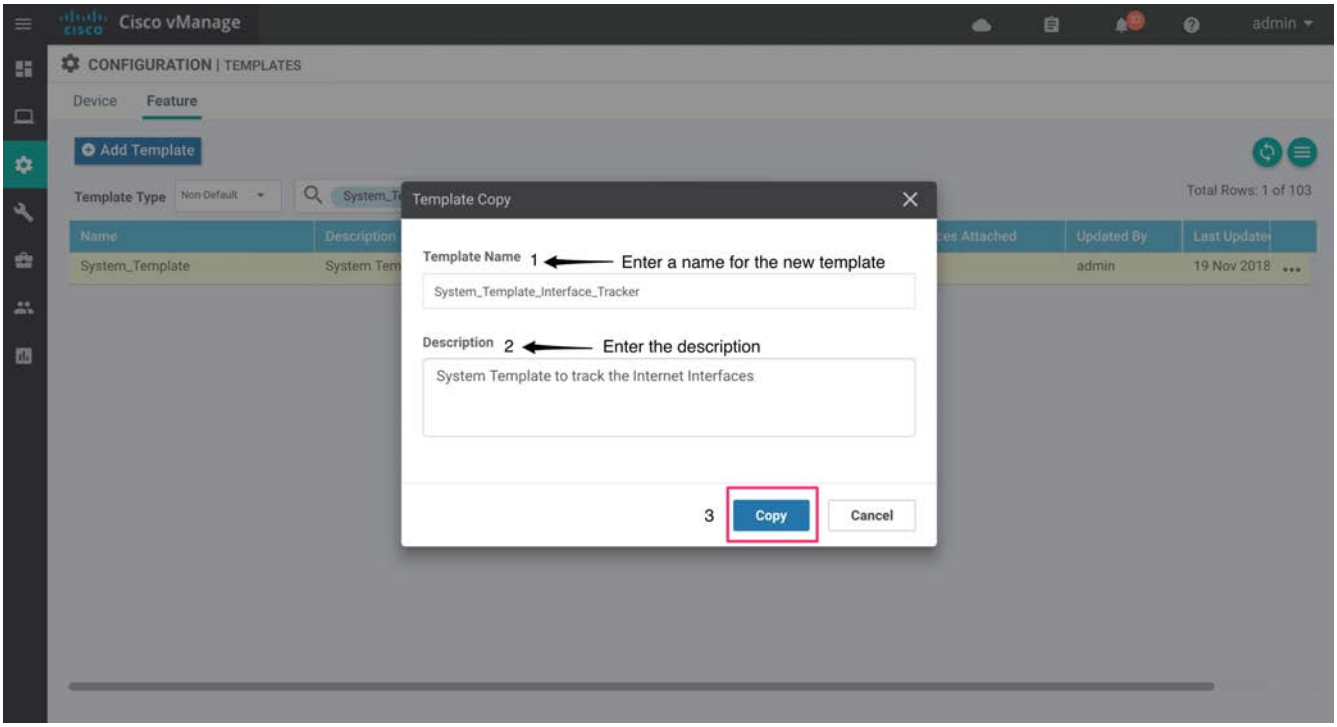


Figure 36 Name and description of template - System_Template_ Interface_Tracker.

16. Edit the System_Template_Interface_Tracker template to add the following:

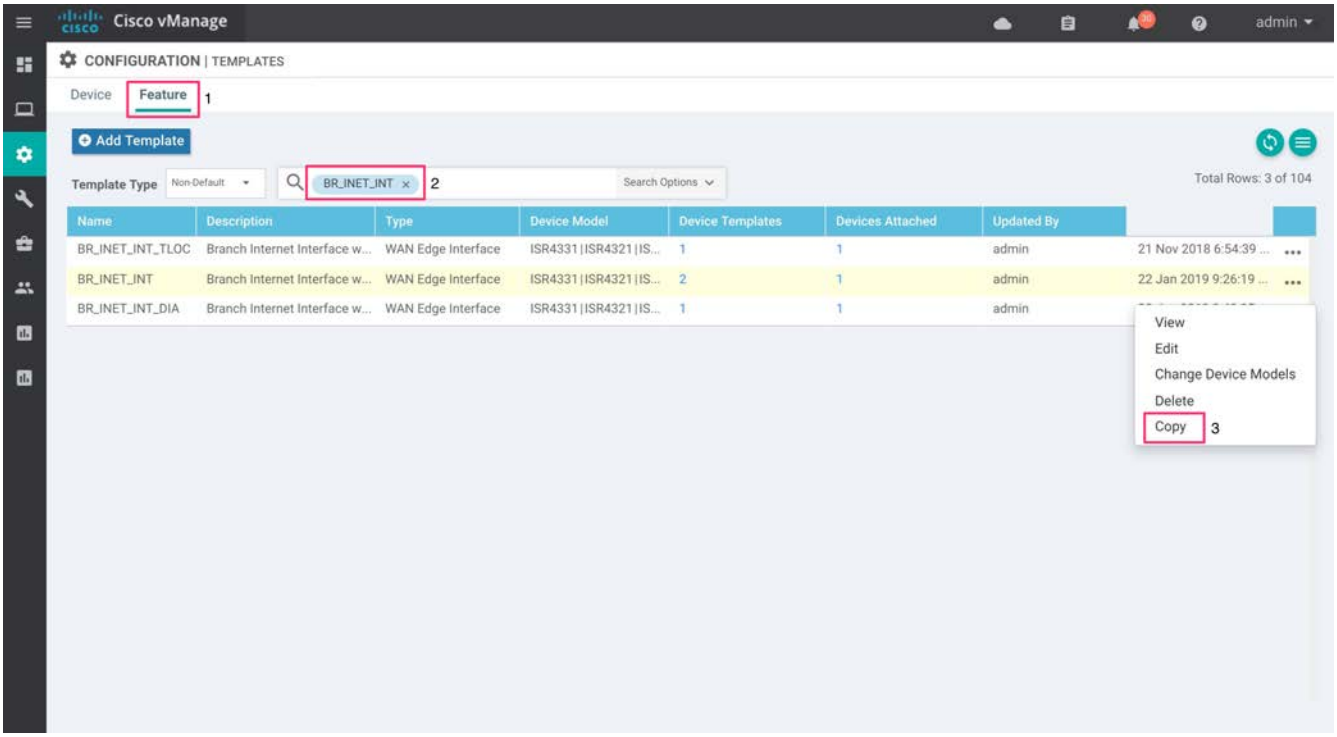
Table 8 **Template System_Template _Interface_Tracker**

Section	Parameter	Type	Variable/Value
Tracker	Name	Global	nat_tracker
	Endpoint Type	Radio button	IP Address
	Endpoint IP Address	Global	208.67.222.222
	Name	Global	nat_tloc_tracker
	Endpoint Type	Radio button	IP Address
	Endpoint IP Address	Global	216.58.194.174

Step 2 : Add Tracker Name to Internet Interface

Add the tracker name (nat_tracker / nat_tloc_tracker) to the Interface feature template used to deploy the Internet facing interface of each WAN edge device.

17. Generate a copy of the previously used interface feature templates by clicking the **copy** option as explained earlier. Next, enter the **name/description** for the generated template and attach the tracker to each of these generated feature templates.



In this guide, the following templates were used in remote-sites. These templates were copied to create a new template.

Table 9 **Internet facing VPN 0 Templates**

Existing Template	New Template
BR_INET_INT	BR_INET_INT_DIA
BR_INET_ SUBINT	BR_INET_ SUBINT_DIA
BR_BRONZE_INT	BR_BRONZE_INT_DIA
BR_BRONZE_SUBINT	BR_BRONZE_SUBINT_DIA

The new template is edited such that the tracker is enabled on each Internet facing interface.

18. Changes made to BR1-WAN-Edge1 (vEdge Site 112002)

Table 10 **Template BR_BRONZE_INT**

Section	Parameter	Type	Variable/Value
Advanced	Tracker	Global	nat_tracker

Table 11 **Template BR_INET_SUBINT**

Section	Parameter	Type	Variable/Value
Advanced	Tracker	Global	nat_tloc_tracker

Changes made to device BR1-WAN-Edge2 (vEdge Site 112002)

Table 12 **Template BR_INET_INT**

Section	Parameter	Type	Variable/Value
Advanced	Tracker	Global	nat_tracker

Table 13 **Template BR_BRONZE_SUBINT**

Section	Parameter	Type	Variable/Value
Advanced	Tracker	Global	nat_tloc_tracker

Note, to associate each of the trackers to only one NAT-enabled Internet-facing interface. The same tracker cannot be used on two NAT-enabled Internet facing interfaces within the same device.

Technical Tip: System Tracker and path preference using local-TLOC color is not yet supported on IOS XE SD-WAN release. These features are currently supported only on vEdge router platforms.

Operate - Cisco SD-WAN Direct Internet Access Monitoring

Monitor, Troubleshoot and Manage Cisco SD-WAN Direct Internet Access

Using the vManage NMS Dashboard, you can monitor, troubleshoot and manage your SD-WAN overlay network, including the features being deployed. Within DIA,

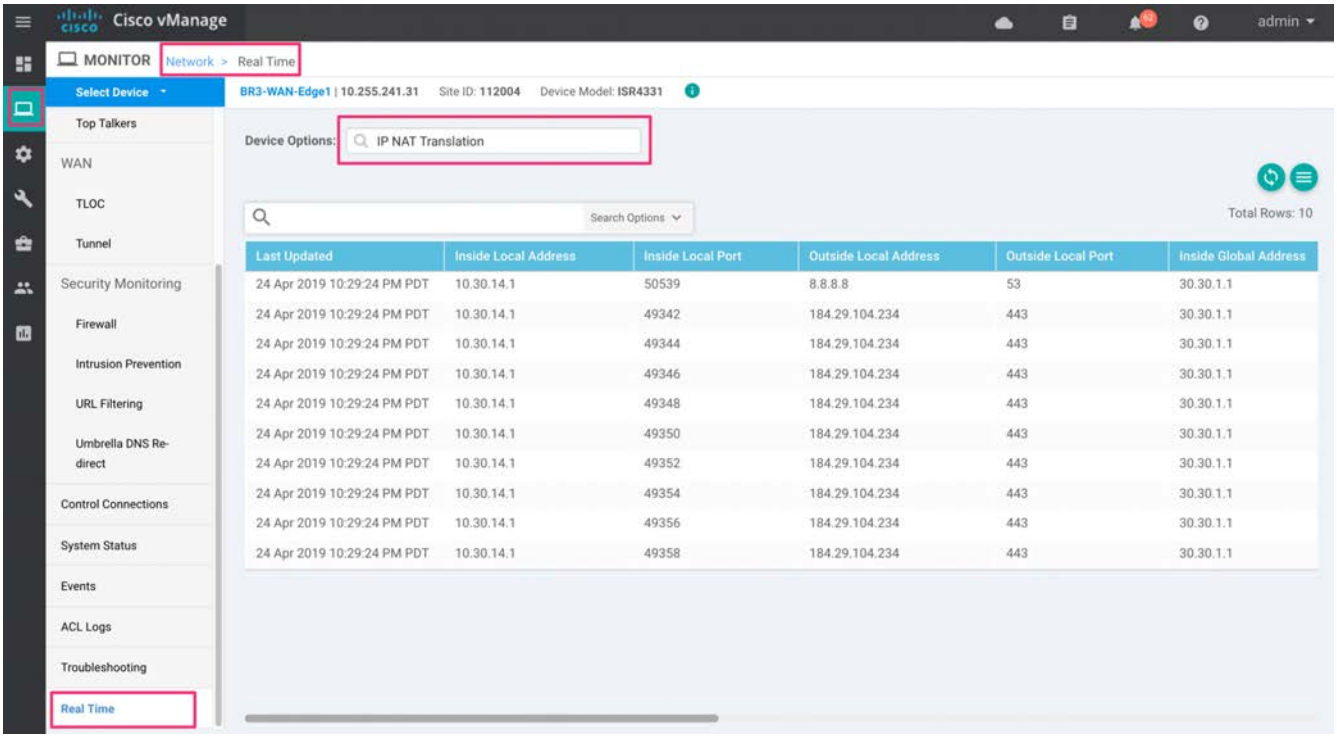
- Monitor DIA sessions based on the NAT translations
- Monitor the configured data policy for traffic flow
- Understand the interface status and routing table for service-side VPN for NAT DIA route

Step 1: Monitor DIA sessions based on the NAT Translations

Using the vManage NMS dashboard, you can view the NAT translations for traffic exiting the NAT-enabled interface on VPN 0.

1. Navigate to **Monitor > Network** on the left pane and click the WAN edge device you wish to monitor.
2. In the panel on the left, select **Real Time** and a screen appear with **Device Options**. Click the box next to the device options. This populates a list of options that can be chosen to monitor, troubleshoot, and manage your device and the features deployed on it.

The figure below shows an example of NAT translations being monitored on the WAN Edge device using the IP NAT Translation option.



Technical Tip: The device options populated to monitor NAT translations are different for vEdge router platforms. In the vEdge platform, use the **IP NAT Filters** option to verify the NAT translation filters.

Note, you can also view NAT translations from the CLI mode on the routers. To do so, navigate to **Tools** > **SSH** and click the desired WAN edge device.

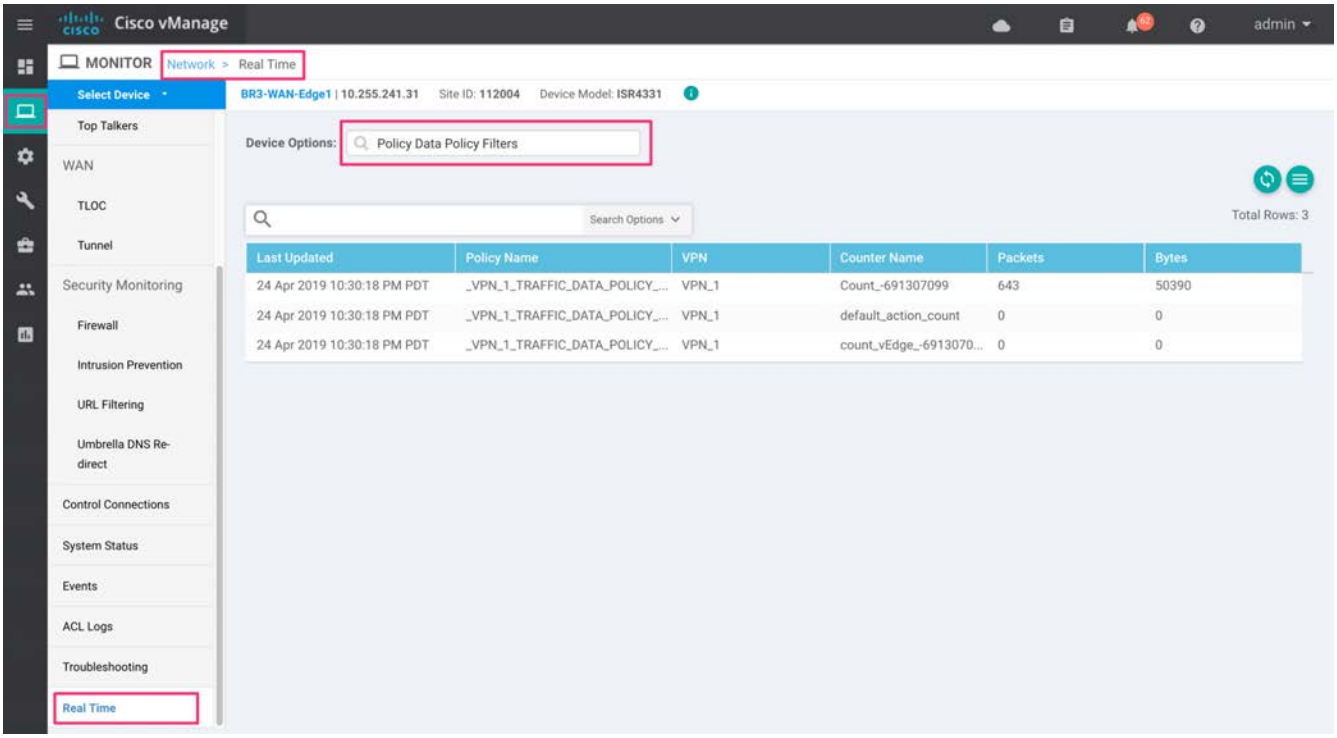
The basic show commands to view NAT translations include – **show ip nat translations** and **show ip nat statistics** on SD-WAN XE platforms, and **show ip nat filter | tab** on vEdge router platforms.

Step 2: Monitor the configured data policy for traffic flow

Using vManage NMS dashboard, you can monitor the traffic flow through the policy based on the overall packets/bytes.

1. Navigate to **Monitor > Network** on the left pane and click the WAN edge device you wish to monitor.
2. In the panel on the left, select **Real Time** and a screen will appear with Device Options. Click the box next to the device options. This shows a list of options that can be chosen to monitor, troubleshoot, and manage your device and the features deployed on it.

In the example figure below, packets/bytes of traffic hitting the data policy embedded within the centralized policy are monitored on the WAN Edge device.



Use CLI commands, such as show (sdwan) policy from vSmart controllers to view the policy and to monitor the flow of traffic, show (sdwan) policy data-policy-filter.

Technical Tip: To determine whether the data policy is sending packets via DIA path or SD-WAN overlay, you can use the CLI command - show sdwan app-fwd dpi flows on SD-WAN XE devices or show app dpi flows on vEdge platform. This command output, will display the type of application and whether that packet was IPsec encapsulated or not.

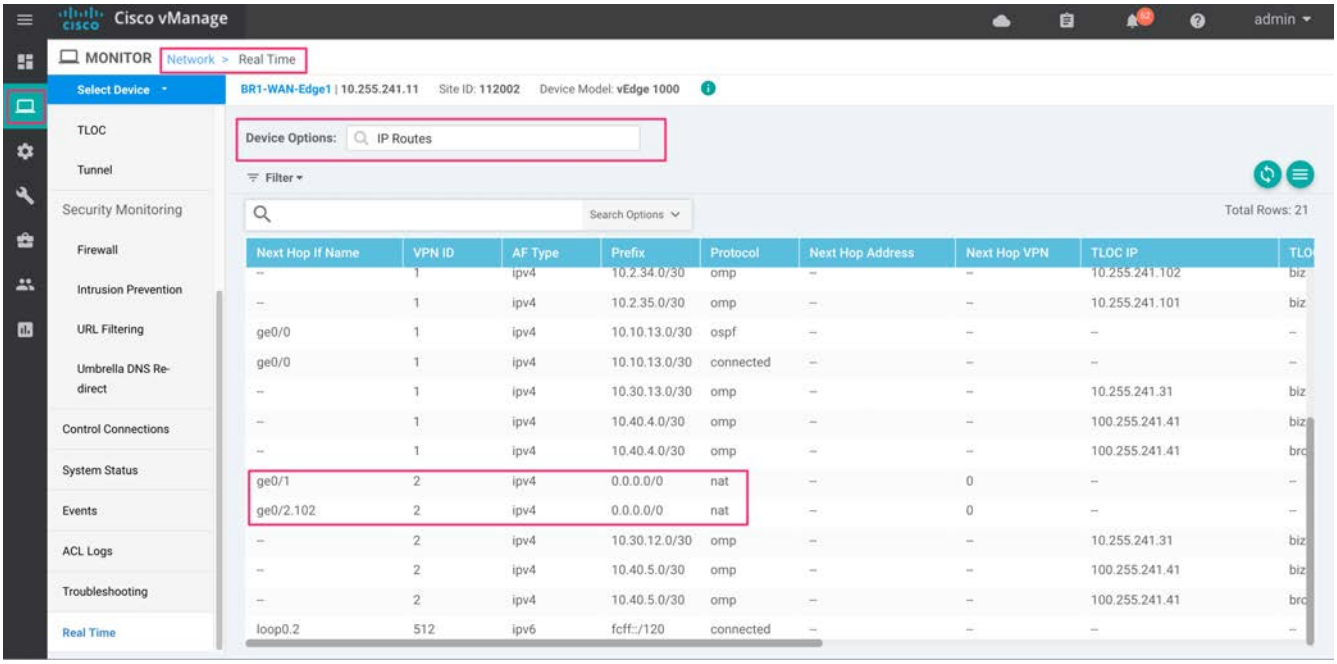
Step 3: Understand the overall routing table for Service Side VPN for NAT DIA route

Using vManage NMS dashboard, you can monitor for traffic flow through the policy based on the overall packets/bytes.

1. Navigate to **Monitor > Network** available on the left pane and click on the WAN edge device you wish to monitor.

2. Select Real time and pop-up screen will appear with device options. Click the tab next to the device options. A You will then see a list of options that can be chosen to monitor, troubleshoot, and manage your device and the features deployed on it.

The example below shows the monitoring of IP routes for the WAN Edge device.



Note, you can also filter the view populated on the vManage dashboard.

Technical Tip: The option to view routes on SD-WAN XE devices via vManage NMS is yet to be added. You can view the routes, by navigating to **Tools** > **SSH Terminal**. Next, click the WAN Edge device and enter CLI command **show ip route**.

Appendix A: New in this guide

This guide is new and is not updated from a previous version.

Appendix B: Hardware and software used for validation

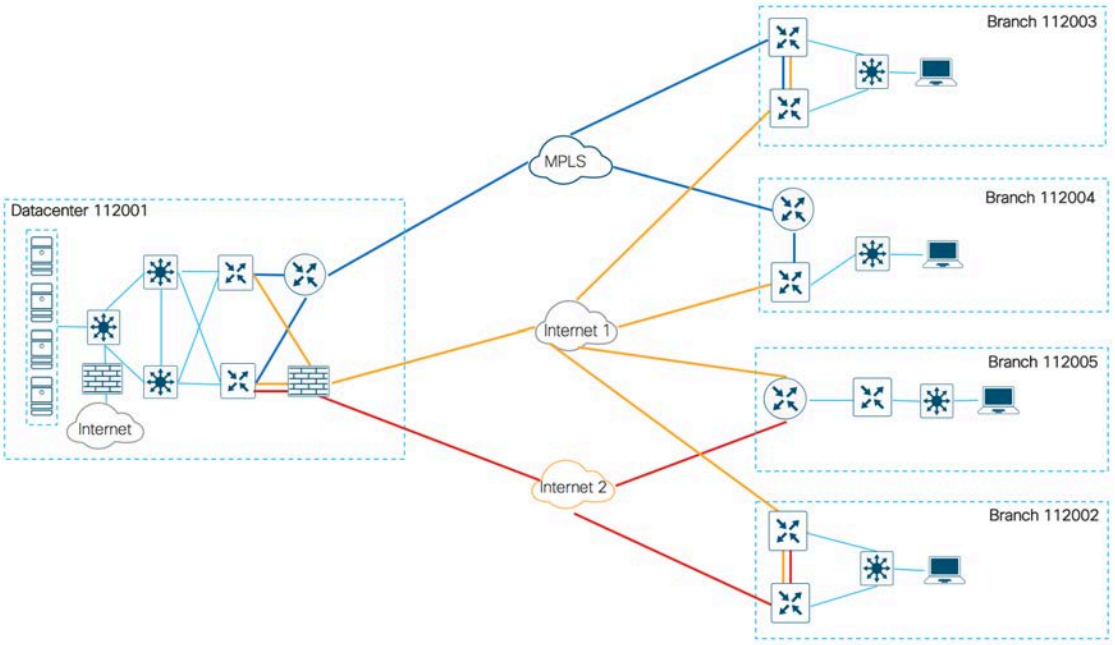
This guide was validated using the following hardware and software.

Table 14 **System feature template settings**

Functional Area	Product	Software Version
Cloud	Cisco vManage NMS	19.1.0
Cloud	Cisco vBond Controller	19.1.0
Cloud	Cisco vSmart Controller	19.1.0
Data center	Cisco vEdge 5000 Series Routers	18.4.0
Branch office	Cisco vEdge 1000 Series Routers	18.4.0
Branch office	Cisco ISR 4331 Series Routers	16.10.2
Branch office	Cisco ISR 4351 Series Routers	16.10.2

Appendix C: DIA Deployment Example

The following figure is a high-level overview of the example network in this deployment guide.



In this topology, there is one data center and 4 remote sites. The transports shown are one MPLS and two Internet Service Providers. The SD-WAN controllers are deployed using Cisco's cloud-managed service and reachable via Internet transport. On the U.S. West Coast there is one vManage, one vSmart controller and one vBond orchestrator.

Each of the WAN edge devices are running SD-WAN code, configured using the templates similar to those used in the SD-WAN deployment guide and the devices are a part of the SD-WAN overlay network.

System IP address and site ID

The following table explains the system IP addresses and site ID's chosen for this deployment guide.

Table 15 **Example network site IDs and system IP addresses**

Hostname	Location	Site ID	System IP
DC1-WAN-Edge1	Datacenter 1/ West	112001	10.255.241.101
DC1-WAN-Edge2			10.255.241.102
BR1-WAN-Edge1	Branch 1/ West	112002	10.255.241.11
BR1-WAN-Edge2			10.255.241.12
BR2-WAN-Edge1	Branch 2/ West	112003	10.255.241.21

Hostname	Location	Site ID	System IP
BR2-WAN-Edge2			10.255.241.22
BR3-WAN-Edge1	Branch 3/ West	112004	10.255.241.31
BR4-WAN-Edge1	Branch 4/ West	112005	10.255.241.41
BR4-WAN-Edge2			10.255.241.42

The following table explains the color used for each transport in this deployment guide.

Table 16 **Color and transport details**

Color	Transport
MPLS	MPLS Transport
Biz-Internet	Internet Provider 1
Bronze	Internet Provider 2

The LAN side of each branch contains devices configured within the private IP address range of 10.0.0.0/8 subnet.

Appendix D: Cisco WAN Edge configuration summary (Templates)

This section summarizes the feature templates and device template for the Cisco WAN Edge routers deployed within this deployment guide.

System feature template

Devices: All devices except vManage and vSmart

Template: System

Template Name: System_Template

Description: System Template

Table 17 **System feature template settings**

Section	Parameter	Type	Variable/Value
Basic Configuration	Site ID	Device Specific	system_site_id
	System IP	Device Specific	system_system_ip
	Hostname	Device Specific	system_host_name
	Device Groups	Device Specific	system_device_groups
GPS	Latitude	Device Specific	system_latitude
	Longitude	Device Specific	system_longitude
Advanced	Port Hopping	Device Specific	system_port_hop
	Port Offset	Device Specific	system_port_offset

Logging feature template

Devices: All devices

Template: Other Templates/Logging

Template Name: Logging_Template

Description: Logging Template

Table 18 **Logging feature template settings**

Section	Parameter	Type	Variable/Value
Server (Optional)	Hostname/IP Address	Device Specific	logging_server_name
	VPN ID	Device Specific	logging_server_vpn
	Source Interface	Global	loopback0

This feature template is optional, deploy it based on your individual use cases. It will help monitor the network.

NTP feature template

Devices: All devices

Template: Basic Information/NTP

Template Name: NTP_Template

Description: NTP Template

Table 19 **NTP feature template settings**

Section	Parameter	Type	Variable/Value
Server	Hostname/IP Address	Global	time.nist.gov

The Cisco WAN Edge router syncs the time to an NTP server. For this deployment guide the NTP server **time.nist.gov** was used.

You should be careful to use only known and trusted NTP servers.

OMP feature template

Devices: All devices except vManage and vSmart

Template: Basic Information/OMP

Template Name: OMP_Template

Description: OMP Template

Table 20 **OMP feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Number of Paths Advertised per Prefix	Global	16
	ECMP Limit	Global	16
Advertise	Connected	Global	Off
	Static	Global	Off

The rest of the options are in type default.

VPN 1 interface Ethernet Loopback0

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1k, vEdge5k)

Template: VPN/VPN Interface Ethernet

Template Name: VPN1_Lo0

Description: Service VPN 1 Interface Loopback 0

Table 21 **OMP feature template settings**

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Global	loopback0
IPv4 Configuration	IPv4 Address	Radio Button	Static
	IPv4 Address	Device Specific	vpn1_lo0_int_ip_addr|maskbits

The rest of the options are in type default.

BFD feature template

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1k, vEdge5k)

Template: Basic Information/BFD_Template

Template Name: BFD_Template

Description: BFD Template for WAN Edge devices

Table 22 **BFD feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Poll Interval	Global	120000
Color (Biz Internet)	Color	Drop-down	Biz Internet
	Path MTU	Global	Off
Color (MPLS)	Color	Drop-down	MPLS
	Path MTU	Global	Off

The rest of the options are in type default.

The default BFD hello interval is 1,000 milliseconds. The BFD hello interval controls how fast the network converges in the case of an IPsec tunnel failure. The shorter the BFD hello interval, generally the faster the network recognizes a failure of one of the Cisco vEdge Cloud routers within the transit VPC and selects an alternate path.

Security feature template

Devices: All devices except vManage and vSmart

Template: Basic Information/Security

Template Name: Security_Template

Description: Security Template

Table 23 **NTP feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Replay window	Global / drop-down	4096

VPN 512 feature template

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1k, vEdge5k)

Template: VPN/VPN

Template Name: VPN512_Template

Description: VPN 512 Out-of-Band Management for WAN Edge devices

Table 24 **VPN512 feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	512
	Name	Global	Management VPN

The rest of the options are not altered.

VPN 512 interface feature template

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1k, vEdge5k)

Template: VPN/VPN Interface Ethernet

Template Name: VPN512_Interface

Description: VPN 512 Management Interface for WAN Edge devices

Table 25 **VPN512 interface feature template settings**

Section	Parameter	Type	Variable/Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_int_mgmt0_or_gex
	Description	Global	Management Interface
IPv4 Configuration	IPv4 Address	Radio Button	Static
		IPv4 Address	vpn512_int_mgmt_ip_addr|maskbits

VPN 0 feature template

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1k)

Template: WAN Edge VPN

Template Name: BR_ VPN0_Dual_Transport

Description: VPN0 Dual Transport Template

Table 26 **VPN0 dual transport feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	0
	Name	Global	Transport VPN
	Enahnced ECMP Keying	Global (Radio)	On
DNS	Primary DNS Address (IPv4)	Global	208.67.220.220
	Secondary DNS Address (IPv4)	Global	208.67.222.222
IPv4 Route	Address (Next Hop)	device specific	vpn0_inet_next_hop_ip_addr
			vpn0_mpls_next_hop_ip_addr
	Prefix	Global	0.0.0.0/0

VPN 0 BGP feature template

Devices: WAN Edge device (ISR4331)

Template: BGP

Template Name: BR_ VPN0_BGP

Description: VPN0 Template for BGP configuration for WAN Edge devices

Table 27 **VPN0 feature template for BGP settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	device specific	bgp_shutdown
	AS Number	device specific	bgp_as_num
	Propagate AS Path	Global (Radio)	On
Unicast Address Family	IPv4 Maximum Paths	Global	2
	Redistribute	Global	OMP
Neighbor	Address	device specific	bgp_neighbor1_address
	Description	device specific	bgp_neighbor1_description
	Remote AS	device specific	bgp_neighbor1_remote_as
	Address Family	device specific	On

Section	Parameter	Type	Variable/Value
	Address Family	device specific	IPv4-Unicast
	Shutdown	device specific	bgp_neighbor1_shutdown
	Advanced (source Interface)	Radio	Address
	Advanced (Password)	device specific	bgp_neighbor1_password
	Keepalive Time (seconds)	Global	3
	Hold Time (seconds)	Global	9

VPN 0 Interface feature template

Devices: WAN Edge device (ISR4331, ISR4351, Edge1000)

Template: WAN Edge Interface

Template Name: BR_WAN_PARENT_INT

Description: VPN0 INET Transport Template for WAN Edge devices

Table 28 **VPN0 WAN parent feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	device specific	vpn0_wan_parent_int_shutdown
	Interface Name	device specific	vpn0_wan_parent_int_gex|x
	Description	Global (Radio)	WAN Parent Interface
Advanced	IP MTU	Global	IP_MTU

Devices: WAN Edge device (ISR4331, ISR4351, Edge1000)

Template: WAN Edge Interface

Template Name: BR_LAN_PARENT_INT

Description: VPN1 LAN Parent Service Side Interface Template for WAN Edge devices

Table 29 **VPN0 LAN parent feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	device specific	vpn_lan_parent_int_shutdown
	Interface Name	device specific	vpn_lan_parent_int_gex|x
	Description	Global (Radio)	LAN Parent Interface

Section	Parameter	Type	Variable/Value
Advanced	IP MTU	Global	IP_MTU

Devices: WAN Edge device (ISR4331)

Template: WAN Edge Interface

Template Name: BR_MPLS_INT

Description: VPN0 MPLS Transport Template for WAN Edge devices

Table 30 **VPN0 MPLS transport template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	device specific	vpn0_mpls_int_shutdown
	Interface Name	device specific	vpn0_mpls_int_gex|x
	Description	Global (Radio)	MPLS Interface
	IPv4	Radio	Static
	IPv4 Address	device specific	vpn0_mpls_int_ip_addr|maskbits
	Bandwidth Upstream	device specific	vpn0_mpls_int_bandwidth_up
	Bandwidth Downstream	device specific	vpn0_mpls_int_bandwidth_ down
Tunnel	Tunnel Interface	Global (Radio)	On
	Color	Global	mpls
	Restrict	Global	On
Tunnel - Allow Service	All	Global	On
	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel - Advanced Options	IPsec	Global	On
	Preference	Global	vpn_mpls_tunnel_ipsec_preference
NAT	NAT	device specific	Nat_enable
Advanced	IP MTU	device specific	vpn0_mpls_mtu
	TCP MSS	Global	1350

Section	Parameter	Type	Variable/Value
	Clear-Don't-Fragment	Global	On

Devices: WAN Edge device (ISR4331)

Template: WAN Edge Interface

Template Name: BR_MPLS_SUBINT

Description: VPN0 MPLS Transport Template for WAN Edge devices

Table 31 **VPN0 MPLS transport sub-interface template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn0_mpls_int_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_gex|x.VLAN
	Description	Global (Radio)	MPLS Interface
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn0_mpls_int_ip_addr|maskbits
	Bandwidth Upstream	Device Specific	vpn0_mpls_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_mpls_int_bandwidth_ down
Tunnel	Tunnel Interface	Global (Radio)	On
	Color	Global	mpls
	Restrict	Global	On
Tunnel - Allow Service	All	Global	On
	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel - Advanced Options	IPsec	Global	On
	Preference	Global	vpn_mpls_tunnel_ipsec_preference
NAT	NAT	Device Specific	nat_enable
Advanced	IP MTU	Device Specific	IP MTU
	TCP MSS	Global	1350

Section	Parameter	Type	Variable/Value
	Clear-Don't-Fragment	Global	On

Devices: WAN Edge device (ISR4331, ISR4351, Edge1000)

Template: WAN Edge Interface

Template Name: BR_INET_INT

Description: VPN0 INET Transport Template for WAN Edge devices

Table 32 **VPN0 INET transport template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex|x
	Description	Global (Radio)	INET Interface
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn0_inet_int_ip_addr|maskbits
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_ down
Tunnel	Tunnel Interface	Global (Radio)	On
	Color	Global	Biz-internet
Tunnel - Allow Service	All	Global	On
	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel - Advanced Options	IPsec	Global	On
	Preference	Global	vpn_inet_tunnel_ipsec_preference
NAT	NAT	Device Specific	Nat_enable
Advanced	IP MTU	Device Specific	vpn0_inet_mtu
	TCP MSS	Global	1350
	Clear-Don't-Fragment	Global	On

Devices: WAN Edge device (ISR4331, ISR4351, Edge1000)

Template: WAN Edge Interface

Template Name: BR_INET_SUBINT

Description: VPN0 INET Transport Sub Interface Template for WAN Edge devices

Table 33 **VPN0 INET transport sub interface template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex|x.VLAN
	Description	Global (Radio)	INET Interface
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn0_inet_int_ip_addr|maskbits
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_ down
Tunnel	Tunnel Interface	Global (Radio)	On
	Color	Global	Biz-Internet
Tunnel - Allow Service	All	Global	On
	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel - Advanced Options	IPsec	Global	On
	Preference	Global	vpn_inet_tunnel_ipsec_preference
NAT	NAT	Device Specific	nat_enable
Advanced	IP MTU	Device Specific	IP MTU
	TCP MSS	Global	1350
	Clear-Don't-Fragment	Global	On

Devices: WAN Edge device (ISR4351)

Template: WAN Edge Interface

Template Name: BR_BRONZE_INT

Description: VPN0 Bronze Transport Template for WAN Edge devices

Table 34 **VPN0 feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn0_bronze_int_shutdown
	Interface Name	Device Specific	vpn0_bronze_int_gex|x
	Description	Global (Radio)	Bronze Interface
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn0_bronze_int_ip_addr|maskbits
	Bandwidth Upstream	Device Specific	vpn0_bronze_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_bronze_int_bandwidth_ down
Tunnel	Tunnel Interface	Global (Radio)	On
	Color	Global	Bronze
Tunnel - Allow Service	All	Global	On
	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel - Advanced Options	IPsec	Global	On
	Preference	Global	vpn_bronze_tunnel_ipsec_preference
NAT	NAT	Device Specific	Nat_enable
Advanced	IP MTU	Device Specific	vpn0_bronze_mtu
	TCP MSS	Global	1350
	Clear-Don't-Fragment	Global	On

Devices: WAN Edge device (vEdge1000)

Template: WAN Edge Interface

Template Name: BR_BRONZE_SUBINT

Description: VPN0 Bronze Transport Sub-Interface Template for WAN Edge devices

Table 35 **VPN0 Bronze transport sub-interface feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn0_bronze_int_shutdown
	Interface Name	Device Specific	vpn0_bronze_int_gex|x.VLAN
	Description	Global (Radio)	Bronze Interface
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn0_bronze_int_ip_addr|maskbits
	Bandwidth Upstream	Device Specific	vpn0_bronze_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_bronze_int_bandwidth_ down
Tunnel	Tunnel Interface	Global (Radio)	On
	Color	Global	Bronze
Tunnel - Allow Service	All	Global	On
	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel - Advanced Options	IPsec	Global	On
	Preference	Global	vpn_bronze_tunnel_ipsec_preference
NAT	NAT	Device Specific	nat_enable
Advanced	IP MTU	Device Specific	IP MTU
	TCP MSS	Global	1350
	Clear-Don't-Fragment	Global	On

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1000)

Template: WAN Edge Interface

Template Name: BR_TLOC_INT

Description: VPN0 TLOC Interface Template for WAN Edge devices

Table 36 **VPN0 TLOC Interface feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn0_yloc_int_shutdown

Section	Parameter	Type	Variable/Value
	Interface Name	Device Specific	vpn0_tloc_int_gex|x.VLAN
	Description	Global (Radio)	TLOC Interface
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn0_tloc_int_ip_addr|maskbits
Advanced	IP MTU	Device Specific	IP MTU

VPN 1 feature template

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1000)

Template: Service Side VPN

Template Name: BR_VPN1_Base

Description: VPN1 Base Template for WAN Edge devices

Table 37 **VPN1 base template feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	1
	Name	Global	Service VPN
	Enhanced ECMP Keying	Global	On
Advertise OMP	BGP (IPv4)	Global	Off
	Static (IPv4)	Global	On
	Connected (IPv4)	Global	On
	OSPF External (IPv4)	Global	On
	Network (IPv4)	Global	Off

VPN 1 Interface feature template

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1000)

Template: Service Side Interface

Template Name: BR_LAN_VPN1_INT1

Description: VPN1 LAN Interface Template for WAN Edge devices

Table 38 **VPN1 LAN interface template feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int1_shutdown
	Interface Name	Device Specific	vpn1_lan_int_gex|x.VLAN
	Description	Global (Radio)	vpn1_lan_int1_description
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn1_lan_int1_ip_addr|maskbits

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1000)

Template: Service Side Interface

Template Name: BR_LAN_VPN1_INT_VRRP

Description: VPN1 LAN Interface Template with VRRP for WAN Edge devices

Table 39 **VPN1 LAN Interface VRRP feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int1_shutdown
	Interface Name	Device Specific	vpn1_lan_int_gex|x _or_.VLAN
	Description	Global (Radio)	vpn1_lan_int1_description
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn1_lan_int1_ip_addr|maskbits
VRRP	Group ID	Global	1
	Priority	Device Specific	vpn1_vrrp_priority1
	Track OMP	Radio Button	On
	IP Address	Device Specific	vpn1_vrrp_ip_addr1

VPN 1 OSPF feature template

Devices: WAN Edge device (ISR4331, ISR4351, Edge1000)

Template: OSPF

Template Name: BR_VPN1_ OSPF_INT

Description: VPN1 OSPF Template for WAN Edge devices

Table 40 **VPN1 OSPF feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Router ID	Device Specific	vpn1_ospf_router_id
Redistribute	Protocol	Global	OMP
Area	Area Number	Global	0
Area (Interface)	Interface Name	Device Specific	vpn1_ospf_interface_gex|x
	Interface Cost	Device Specific	vpn1_ospf_interface_cost
Area (Interface Advanced Options)	OSPF Network Type	Global	point-to-point
	Authentic Type	Global	message-digest
	Message Digest Key ID	Global	22
Area (Range)	Address	Device Specific	vpn1_ospf_area_range_address_0
Advanced	Reference Bandwidth (Mbps)	Global	100000
	Originate	Radio Button	On

VPN 2 feature template

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1000)

Template: Service side VPN

Template Name: BR_ VPN2_NAT_DIA_ROUTE

Description: NAT DIA Route within VPN2

Table 41 **VPN2 LAN Interface VRRP feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	2
	Name	Global	Service VPN
	Enahnced ECMP Keying	Global (Radio)	On
Advertise OMP	Static (IPv4)	Global	On
	Connected (IPv4)	Global	On
IPv4 Route	Prefix (Next Hop)	Device Specific	vpn1_statuc_route_prefix|maskbits
	Gateway	Radio Button	VPN
	Enable VPN	Global	On

VPN 2 Interface feature template

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1000)

Template: WAN Edge Interface

Template Name: BR_LAN_VPN2_INT_VRRP

Description: VPN2 LAN Interface Template with VRRP for WAN Edge devices

Table 42 **VPN2 LAN Interface VRRP feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn2_lan_int1_shutdown
	Interface Name	Device Specific	vpn2_lan_int_gex|x _or_.VLAN
	Description	Global (Radio)	vpn2_lan_int1_description
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn2_lan_int1_ip_addr|maskbits
VRRP	Group ID	Global	1
	Priority	Device Specific	vpn2_vrrp_priority1
	Track OMP	Radio Button	On
	IP Address	Device Specific	vpn2_vrrp_ip_addr1

Devices: WAN Edge device (ISR4331, ISR4351, vEdge1000)

Template: Service Side Interface

Template Name: BR_LAN_VPN2_INT2

Description: VPN2 LAN Interface Template for WAN Edge devices

Table 43 **VPN0 feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn2_lan_int2_shutdown
	Interface Name	Device Specific	vpn2_lan_int_gex|x _or_.VLAN
	Description	Global (Radio)	vpn2_lan_int1_description
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn2_lan_int1_ip_addr|maskbits

VPN 2 OSPF feature template

Devices: WAN Edge device (ISR4331, ISR4351, Edge1000)

Template: OSPF

Template Name: BR_VPN2_ OSPF_NAT_REDISTRIBUTE

Description: VPN2 OSPF Template with NAT Redistribute WAN Edge devices

Table 44 **VPN2 OSPF template with redistribute feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Router ID	Device Specific	vpn2_ospf_router_id
Redistribute	Protocol	Global	OMP
	Protocol	Global	NAT
Area	Area Number	Global	0
Area (Interface)	Interface Name	Device Specific	vpn2_ospf_interface_gex|x
	Interface Cost	Device Specific	vpn2_ospf_interface_cost
Area (Interface Advanced Options)	OSPF Network Type	Global	point-to-point
	Authentic Type	Global	message-digest
	Message Digest Key ID	Global	22
Area (Range)	Address	Device Specific	vpn2_ospf_area_range_address_0
Advanced	Reference Bandwidth (Mbps)	Global	100000
	Originate	Radio Button	On

VPN 0 Datacenter feature template

Devices: WAN Edge device (vEdge5000)

Template: WAN Edge VPN

Template Name: DC_VPN0

Description: VPN0 Transport Template for Datacenter

Table 45 **VPN0 transport feature template settings for datacenter**

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	0
	Name	Global	Transport VPN

Section	Parameter	Type	Variable/Value
	Enahnced ECMP Keying	Global (Radio)	On
DNS	Primary DNS Address (IPv4)	Global	208.67.222.222
	Secondary DNS Address (IPv4)	Global	208.67.220.220
Advertise OMP	BGP (IPv4)	Global	On
	Static (IPv4)	Global	On
	Connected (IPv4)	Global	On
	OSPF External (IPv4)	Global	Off
	Network (IPv4)	Global	Off
IPv4 Route	Address (Next Hop)	device specific	vpn0_inet_next_hop_ip_addr
			vpn0_mpls_next_hop_ip_addr
	Prefix	Global	0.0.0.0/0

VPN 0 Datacenter Interface feature template

Devices: WAN Edge device (vEdge5000)

Template: WAN Edge Interface

Template Name: DC_MPLS_Interface

Description: VPN0 MPLS Transport Template for Datacenter

Table 46 **VPN0 MPLS transport feature template settings for datacenter**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn0_mpls_int_shutdown
	Interface Name	Device Specific	vpn0_mpls_int_gex|x.VLAN
	Description	Global (Radio)	MPLS Interface
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn0_mpls_int_ip_addr|maskbits
	Bandwidth Upstream	Device Specific	vpn0_mpls_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_mpls_int_bandwidth_ down
Tunnel	Tunnel Interface	Global (Radio)	On
	Color	Global	MPLS

Section	Parameter	Type	Variable/Value
	Restrict	Global	On
Tunnel - Allow Service	All	Global	On
	BGP	Global	On
	DHCP	Global	Off
	NTP	Global	On
Tunnel - Advanced Options	IPsec	Global	On
	Preference	Global	vpn_mpls_tunnel_ipsec_preference
Advanced	IP MTU	Device Specific	1500
	TCP MSS	Global	1350
	Clear-Don't-Fragment	Global	On

Devices: WAN Edge device (vEdge5000)

Template: WAN Edge Interface

Template Name: DC_INET_Interface

Description: VPN0 Internet Transport Template for Datacenter

Table 47 **VPN0 Internet transport feature template settings for datacenter**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn0_inet_int_shutdown
	Interface Name	Device Specific	vpn0_inet_int_gex|x.VLAN
	Description	Global (Radio)	INET Interface
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn0_inet_int_ip_addr|maskbits
	Bandwidth Upstream	Device Specific	vpn0_inet_int_bandwidth_up
	Bandwidth Downstream	Device Specific	vpn0_inet_int_bandwidth_ down
Tunnel	Tunnel Interface	Global (Radio)	On
	Color	Global	INET
Tunnel - Allow Service	All	Global	On
	BGP	Global	On

Section	Parameter	Type	Variable/Value
	DHCP	Global	Off
	NTP	Global	On
Tunnel - Advanced Options	IPsec	Global	On
	Preference	Global	vpn_inet_tunnel_ipsec_preference
Advanced	IP MTU	Device Specific	1500
	TCP MSS	Global	1350
	Clear-Don't-Fragment	Global	On

VPN 1 Datacenter feature template

Devices: WAN Edge device (vEdge5000)

Template: WAN Edge VPN

Template Name: DC_VPN1

Description: VPN1 Service Side Template for Datacenter

Table 48 **VPN1 service-side feature template settings for datacenter**

Section	Parameter	Type	Variable/Value
Basic configuration	VPN	Global	1
	Name	Global	Service side VPN 1
	Enahnced ECMP Keying	Global	On
	Enable TCP Optimization	Global	On
Advertise OMP	BGP (IPv4)	Global	On
	Static (IPv4)	Global	On
	Connected (IPv4)	Global	On
	OSPF External (IPv4)	Global	Off
	Network (IPv4)	Global	Off

VPN 1 Datacenter BGP feature template

Devices: WAN Edge device (vEdge5000)

Template: BGP

Template Name: DC_VPN1_BGP

Description: VPN1 Service Side BGP Template for Datacenter

Table 49 **VPN1 service-side BGP feature template settings for datacenter**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	device specific	bgp_shutdown
	AS Number	device specific	bgp_as_num
	Router ID	device specific	bgp_router_id
	Propagate AS Path	Global (Radio)	On
Unicast Address Family	IPv4 Maximum Paths	Global	2
	Re-distribute	Global	OMP
Neighbor (Neighbor 1)	Address	device specific	bgp_neighbor1_address
	Description	device specific	bgp_neighbor1_description
	Remote AS	device specific	bgp_neighbor1_remote_as
	Address Family	device specific	On
	Address Family	device specific	IPv4-Unicast
	Shutdown	device specific	bgp_neighbor1_shutdown
	Advanced (source Interface)	Radio	Address
	Advanced (Password)	device specific	bgp_neighbor1_password
	Keepalive Time (seconds)	Global	3
	Hold Time (seconds)	Global	9
Neighbor (Neighbor 2)	Address	device specific	bgp_neighbor2_address
	Description	device specific	bgp_neighbor2_description
	Remote AS	device specific	bgp_neighbor2_remote_as
	Address Family	device specific	On
	Address Family	device specific	IPv4-Unicast
	Shutdown	device specific	bgp_neighbor2_shutdown

Section	Parameter	Type	Variable/Value
	Advanced (source Interface)	Radio	Address
	Advanced (Password)	device specific	bgp_neighbor2_password
	Keepalive Time (seconds)	Global	3
	Hold Time (seconds)	Global	9

VPN 1 Datacenter Interface feature template

Devices: WAN Edge device (vEdge5000)

Template: WAN Edge Interface

Template Name: DC_VPN1_INT

Description: VPN1 Service Side Interface Template for Datacenter

Table 50 **VPN1 service-side Interface feature template settings**

Section	Parameter	Type	Variable/Value
Basic configuration	Shutdown	Device Specific	vpn1_lan_int1_shutdown
	Interface Name	Device Specific	vpn1_lan_int_gex|x
	Description	Global (Radio)	vpn1_lan_int1_description
	IPv4	Radio	Static
	IPv4 Address	Device Specific	vpn1_lan_int1_ip_addr|maskbits

Datacenter device template

The following table summarizes the device template for the Cisco WAN Edge devices deployed within the datacenter.

Device Model: vEdge5000

Template Name: DC_Hybrid_Type_A_BGP

Description: vEdge Template Branch DC MPLS and INET – Static to CE and BGP to LAN

Table 51 **Datacenter 112001 device template: DC_Hybrid_Type_A_BGP**

Template Type	Template Sub-Type	Template Name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		DC_VPN0
	VPN Interface	DC_MPLS_Interface
		DC_INET_Interface
VPN512		VPN512_Template
	VPN Interface	VPN512_Interface
Service VPN (1)	VPN	DC_VPN1
	BGP	DC_VPN1_BGP
	VPN Interface	DC_VPN1_Int1
		DC_VPN1_Int2
Banner		Banner_Template

Remote-site (branch) device template

The following tables summarize the device templates used for the Cisco WAN Edge devices deployed within the branch.

Device Model: vEdge1000

Template Name: Branch_A_INET_TLOC_SubInt_OSPF

Description: Dual-router Dual-Internet transport design with (TLOC, biz-Internet transport)

Table 52 **Branch 112002 device template: Branch_A_INET_TLOC_SubInt_OSPF**

Template Type	Template Sub-Type	Template Name
System		System_Template_Interface_Tracker
	Logging	Logging_Template
	NTP	NTP_Template
BFD		BFD_Template

Template Type	Template Sub-Type	Template Name
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0_Dual_Transport
	VPN Interface	BR_INET_INT_DIA
		BR_BRONZE_SUBINT_DIA
		BR_WAN_PARENT_INT
		BR_TLOC_INT
		BR_LAN_PARENT_INT
VPN512		VPN512_Template
	VPN Interface	VPN512_Interface
Service VPN (1)	VPN	BR_VPN1_BASE
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_VPN1_INT1
Service VPN (2)	VPN	BR_VPN2_NAT_DIA_ROUTE
	OSPF	BR_VPN2_OSPF_NAT_REDISTRIBUTE
	VPN Interface	BR_LAN_VPN2_INT2

Device Model: vEdge1000

Template Name: Branch_A_BRONZE_TLOC_SubInt_OSPF

Description: Dual-router Dual-Internet transport design with (TLOC, bronze transport)

Table 53 **Branch 112002 device template: Branch_A_INET_TLOC_SubInt_OSPF**

Template Type	Template Sub-Type	Template Name
System		System_Template_Interface_Tracker
	Logging	Logging_Template
	NTP	NTP_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0_Dual_Transport

Template Type	Template Sub-Type	Template Name
	VPN Interface	BR_INET_SUBINT_DIA
		BR_BRONZE_INT_DIA
		BR_WAN_PARENT_INT
		BR_TLOC_INT
		BR_LAN_PARENT_INT
VPN512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_BASE
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_VPN1_INT1
VPN2		BR_VPN2_NAT_DIA_ROUTE
	OSPF	BR_VPN2_OSPF_NAT_REDISTRIBUTE
	VPN Interface	BR_LAN_VPN2_INT2

Device Model: ISR4331

Template Name: Branch_B_INET_TLOC_VRRP

Description: Dual-router Hybrid transport design with (TLOC, biz-internet transport)

Table 54 **Branch 112003 device template: Branch_B_INET_TLOC_VRRP**

Template Type	Template Sub-Type	Template Name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0_Dual_Transport
	VPN Interface	BR_INET_INT
		BR_MPLS_SUBINT

Template Type	Template Sub-Type	Template Name
		BR_TLOC_INT
		BR_LAN_PARENT_INT
VPN512		VPN512_Template
	VPN Interface	VPN512_Interface
Service VPN (1)	VPN	BR_VPN1_BASE
	VPN Interface	BR_LAN_VPN1_INT_VRRP
Service VPN (2)	VPN	BR_VPN2_NAT_DIA_ROUTE
	OSPF	BR_VPN2_OSPF_NAT_REDISTRIBUTE
	VPN Interface	BR_LAN_VPN2_INT_VRRP

Device Model: ISR4331

Template Name: Branch_B_MPLS_TLOC_VRRP

Description: Dual-router Hybrid transport design with (TLOC, MPLS transport)

Table 55 **Branch 112003 device template: Branch_B_MPLS_TLOC_VRRP**

Template Type	Template Sub-Type	Template Name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0_Dual_Transport
	VPN Interface	BR_INET_SUBINT
		BR_MPLS_INT
		BR_TLOC_INT
		BR_LAN_PARENT_INT
	BGP	BR_VPN0_BGP
VPN512		VPN512_Template

Template Type	Template Sub-Type	Template Name
	VPN Interface	VPN512_Interface
Service VPN (1)	VPN	BR_VPN1_BASE
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_VPN1_INT_VRRP
Service VPN (2)	VPN	BR_VPN2_NAT_DIA_ROUTE
	OSPF	BR_VPN2_OSPF_NAT_REDISTRIBUTE
	VPN Interface	BR_LAN_VPN2_INT_VRRP

Device Model: ISR4331

Template Name: Branch_C_MPLS_CE_LAN_OSPF

Description: Single-router Hybrid transport

Table 56 **Branch 112004 device template: Branch_C_MPLS_CE_LAN_OSPF**

Template Type	Template Sub-Type	Template Name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0_Dual_Transport
	VPN Interface	BR_INET_INT
		BR_MPLS_INT
		BR_LAN_PARENT_INT
VPN512		VPN512_Template
	VPN Interface	VPN512_Interface
Service VPN (1)	VPN	BR_VPN1_BASE
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_VPN1_INT

Template Type	Template Sub-Type	Template Name
Service VPN (2)	VPN	BR_VPN2_NAT_DIA_ROUTE
	OSPF	BR_VPN2_OSPF_NAT_REDISTRIBUTE
	VPN Interface	BR_LAN_VPN2_INT2

Device Model: ISR4351

Template Name: Branch_D_Dual_Internet_LAN_OSPF

Description: Single-router Dual-Internet transport

Table 57 **Branch 112004 device template: Branch_D_Dual_Internet_LAN_OSPF**

Template Type	Template Sub-Type	Template Name
System		System_Template
	Logging	Logging_Template
	NTP	NTP_Template
BFD		BFD_Template
OMP		OMP_Template
Security		Security_Template
VPN0		BR_VPN0_Dual_Transport
	VPN Interface	BR_INET_INT
		BR_BRONZE_INT
		BR_LAN_PARENT_INT
VPN512		VPN512_Template
	VPN Interface	VPN512_Interface
VPN1		BR_VPN1_BASE
	OSPF	BR_VPN1_OSPF
	VPN Interface	BR_LAN_VPN1_INT
VPN2		BR_VPN2_NAT_DIA_ROUTE
	OSPF	BR_VPN2_OSPF_NAT_REDISTRIBUTE
	VPN Interface	BR_LAN_VPN2_INT2

Appendix E: Cisco WAN Edge CLI-equivalent configuration

The following is the configuration generated for the Cisco WAN Edge routers, based upon the templates explained in the previous sections device template.

Dual-Router Dual-Internet Model

Branch 112002: BR1-WAN-Edge1

```
system
 host-name               BR1-WAN-Edge1
 gps-location latitude 33.754
 gps-location longitude -84.386
 device-groups           BRANCH Primary UG5 US West v1000
 system-ip               10.255.241.11
 site-id                 112002
 port-offset             1
 admin-tech-on-failure
 no route-consistency-check
 sp-organization-name    "ENB-Solutions - 21615"
 organization-name       "ENB-Solutions - 21615"
 no port-hop
 tracker nat_tloc_tracker
  endpoint-ip 172.217.7.142
 !
 tracker nat_tracker
  endpoint-ip 172.217.7.142
 !
 vbond 10.10.60.2
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password
$6$siwKBQ==$wT2lUa9BSreDPI6gB8sl4E6PAJoVXgMbgv/whJ8F1C6sWdRazdxorYYTLrL6syiG6qnLABTnrE96HJiKF6QRq1
  !
 !
 logging
  disk
   enable
  !
 !
!
bfd color mpls
 no pmtu-discovery
!
bfd color biz-internet
 no pmtu-discovery
!
bfd app-route poll-interval 120000
```

```
omp
 no shutdown
 send-path-limit  16
 ecmp-limit       16
 graceful-restart
!
security
 ipsec
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
vpn 0
 name "Transport VPN"
 dns 208.67.220.220 secondary
 dns 208.67.222.222 primary
 ecmp-hash-key layer4
 interface ge0/0
  description "LAN Parent Interface"
  mtu         1504
  no shutdown
 !
 interface ge0/1
  description          "Bronze Interface"
  ip address 20.50.1.1/30
  nat
  !
  tracker              nat_tloc_tracker
  tunnel-interface
   encapsulation ipsec preference 0
   color bronze
   allow-service all
   allow-service bgp
   no 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
  !
  clear-dont-fragment
  mtu                  1496
  tcp-mss-adjust       1350
  no shutdown
  bandwidth-upstream   1000000
  bandwidth-downstream 1000000
 !
 interface ge0/2
  description "WAN Parent Interface"
  mtu         1504
  no shutdown
 !
 interface ge0/2.101
  description    "TLOC Interface"
  ip address 10.104.1.1/30
  mtu            1446
  tloc-extension ge0/1
  no shutdown
 !
 interface ge0/2.102
  description          "INET Interface"
```

```
  ip address 10.104.2.1/30
  nat
  !
  tracker              nat_tracker
  tunnel-interface
   encapsulation ipsec preference 0
   color biz-internet
   allow-service bgp
   no 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
  !
  clear-dont-fragment
  mtu                  1496
  tcp-mss-adjust       1350
  no shutdown
  bandwidth-upstream   1000000
  bandwidth-downstream 1000000
 !
 ip route 0.0.0.0/0 10.104.2.2
 ip route 0.0.0.0/0 20.50.1.2
!
vpn 1
 name "Service VPN"
 ecmp-hash-key layer4
 router
  ospf
   router-id 10.10.11.11
   auto-cost reference-bandwidth 100000
   default-information originate
   timers spf 200 1000 10000
   redistribute omp
   area 0
    interface ge0/0.10
     cost    1
     network point-to-point
     authentication type message-digest
     authentication message-digest message-digest-key 22 md5
$8$yqv1qBnH6ubDEPAb0itVNam9DmlWsmLuMeWt0Re9HxE=
    exit
    range 10.10.13.0/30
   exit
  !
 !
 interface ge0/0.10
  description Employee
  ip address 10.10.13.2/30
  no shutdown
 !
 omp
  advertise ospf external
  advertise connected
  advertise static
 !
!
vpn 2
 name "Service VPN"
 ecmp-hash-key layer4
```

```
 router
  ospf
   router-id 10.10.12.12
   auto-cost reference-bandwidth 100000
   default-information originate
   timers spf 200 1000 10000
   redistribute omp
   redistribute nat
   area 0
    interface ge0/0.20
     cost    1
     network point-to-point
     authentication type message-digest
     authentication message-digest message-digest-key 22 md5
$8$yLQTZaDYX6h36HKFiU1Xce2yM8Z7GJUQhNsuBwfXQuY=
    exit
    range 10.10.14.0/30
   exit
  !
 !
 interface ge0/0.20
  description vpn1_lan_int2_description
  ip address 10.10.14.2/30
  no shutdown
 !
 ip route 0.0.0.0/0 vpn 0
 omp
  advertise connected
  advertise static
 !
!
vpn 512
 name "Management VPN"
 interface mgmt0
  description "Management Interface"
  ip address 100.119.118.14/24
  no shutdown
 !
!
```

Branch 112002: BR1-WAN-Edge2

```
 system
 host-name               BR1-WAN-Edge2
 gps-location latitude 33.754
 gps-location longitude -84.386
 device-groups           BRANCH Secondary UG4 US West v100
 system-ip               10.255.241.12
 site-id                 112002
 port-offset             1
 admin-tech-on-failure
 no route-consistency-check
 sp-organization-name    "ENB-Solutions - 21615"
 organization-name       "ENB-Solutions - 21615"
 no port-hop
 tracker nat_tloc_tracker
  endpoint-ip 172.217.7.142
 !
 tracker nat_tracker
  endpoint-ip 172.217.7.142
 !
 vbond 10.10.60.2
 aaa
```

```
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password
$6$siwKBQ==$wT2lUa9BSreDPI6gB8sl4E6PAJoVXgMbgv/whJ8F1C6sWdRazdxorYYTLrL6syiG6qnLABTnrE96HJiKF6QRq1
  !
 !
 logging
  disk
   enable
  !
 !
!
bfd color mpls
 no pmtu-discovery
!
bfd color biz-internet
 no pmtu-discovery
!
bfd app-route poll-interval 120000
omp
 no shutdown
 send-path-limit  16
 ecmp-limit       16
 graceful-restart
!
security
 ipsec
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
vpn 0
 name "Transport VPN"
 dns 208.67.220.220 secondary
 dns 208.67.222.222 primary
 ecmp-hash-key layer4
 interface ge0/0
  description "LAN Parent Interface"
  mtu         1504
  no shutdown
 !
 interface ge0/1
  description          "INET Interface"
  ip address 30.50.1.1/30
  nat
   no block-icmp-error
   respond-to-ping
  !
  tracker              nat_tracker
  tunnel-interface
   encapsulation ipsec preference 0
```

```
  color biz-internet
  allow-service all
  allow-service bgp
  no 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
 !
 clear-dont-fragment
 mtu                  1496
 tcp-mss-adjust       1350
 no shutdown
 bandwidth-upstream   1000000
 bandwidth-downstream 1000000
!
interface ge0/2
 description "WAN Parent Interface"
 mtu         1504
 no shutdown
!
interface ge0/2.101
 description          "Bronze subinterface"
 ip address 10.104.1.2/30
 nat
 !
 tracker              nat_tloc_tracker
 tunnel-interface
  encapsulation ipsec preference 0
  color bronze
  allow-service bgp
  no 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
 !
 clear-dont-fragment
 mtu                  1496
 tcp-mss-adjust       1350
 no shutdown
 bandwidth-upstream   1000000
 bandwidth-downstream 1000000
!
interface ge0/2.102
 description    "TLOC Interface"
 ip address 10.104.2.2/30
 mtu            1446
 tloc-extension ge0/1
 no shutdown
!
ip route 0.0.0.0/0 10.104.1.1
ip route 0.0.0.0/0 30.50.1.2
!
vpn 1
 name "Service VPN"
```

```
 ecmp-hash-key layer4
 router
  ospf
   router-id 10.10.12.12
   auto-cost reference-bandwidth 100000
   default-information originate
   timers spf 200 1000 10000
   redistribute omp
   area 0
    interface ge0/0.30
     cost    1
     network point-to-point
     authentication type message-digest
     authentication message-digest message-digest-key 22 md5
$8$sHj+89X3B5p2Vlaj3ELIUD+X/s5KhroSDnk43yzf4hk=
    exit
    range 10.10.0.0/16
   exit
  !
 !
 interface ge0/0.30
  description "Employee traffic"
  ip address 10.10.24.2/30
  no shutdown
 !
 omp
  advertise ospf external
  advertise connected
  advertise static
 !
!
vpn 2
 name "Service VPN"
 ecmp-hash-key layer4
 router
  ospf
   router-id 10.10.12.12
   auto-cost reference-bandwidth 100000
   default-information originate
   timers spf 200 1000 10000
   redistribute omp
   redistribute nat
   area 0
    interface ge0/0.40
     cost    1
     network point-to-point
     authentication type message-digest
     authentication message-digest message-digest-key 22 md5
$8$vbKeCR/oQ+jbLMuFhu0xxlD/yM1dsXanYf094G3l7uw=
    exit
    range 10.10.25.0/30
   exit
  !
 !
 interface ge0/0.40
  description vpn1_lan_int2_description
  ip address 10.10.25.2/30
  no shutdown
 !
 ip route 0.0.0.0/0 vpn 0
 omp
  advertise connected
  advertise static
 !
```

```
!
vpn 512
 name "Management VPN"
 interface mgmt0
  description "Management Interface"
  ip address 100.119.118.13/24
  no shutdown
 !
!
```

Dual-Router Hybrid Transport design

Branch 112003: BR2-WAN-Edge1

```
system
 gps-location latitude 33.4484
 gps-location longitude -112.074
 device-groups         BRANCH Primary UG5 US West v1000
 system-ip             10.255.241.21
 overlay-id            1
 site-id               112003
 port-offset           1
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate     115200
 vbond 10.10.60.2 port 12346
!
no service pad
service password-encryption
service timestamps debug datetime msec
service timestamps log datetime msec
no service tcp-small-servers
no service udp-small-servers
hostname BR2-WAN-Edge1
username admin privilege 15 secret 9 $9$3VEF3VAI3lMM3E$awMmxogwHvRdxoHA5u1utUOAmKPBUvUbkD4PnwNWmWk
vrf definition 1
 description Service VPN
 rd          1:1
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition 2
 description Service VPN
 rd          1:2
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 description Management VPN
 rd          1:512
```

```
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
no ip dhcp use class
ip name-server 208.67.220.220 208.67.222.222
ip route 0.0.0.0 0.0.0.0 10.101.2.2 1
ip route 0.0.0.0 0.0.0.0 20.20.1.2 1
ip http authentication local
ip http server
ip http secure-server
no ip igmp ssm-map query dns
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/1.102 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60
ip nat route vrf 2 0.0.0.0 0.0.0.0 global
no ip rsvp signalling rate-limit
ipv6 unicast-routing
no ipv6 mld ssm-map query dns
cdp run
interface GigabitEthernet0
 description Management Interface
 no shutdown
 arp timeout 1200
 vrf forwarding Mgmt-intf
 ip address 100.119.118.8 255.255.255.0
 ip redirects
 ip mtu    1500
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/0
 description LAN Parent Interface
 no shutdown
 arp timeout 1200
 no ip address
 ip redirects
 ip mtu    1504
 mtu         1504
 negotiation auto
exit
interface GigabitEthernet0/0/0.10
 no shutdown
 encapsulation dot1Q 10
 vrf forwarding 1
 ip address 10.20.21.2 255.255.255.0
 ip mtu 1500
 vrrp 1 address-family ipv4
  vrrpv2
  address 10.20.21.1
  priority 100
  timers advertise 1000
  track omp shutdown
 exit
exit
interface GigabitEthernet0/0/0.20
 no shutdown
 encapsulation dot1Q 20
 vrf forwarding 2
 ip address 10.20.22.2 255.255.255.0
 ip mtu 1500
```

```
 ip ospf 2 area 0
 ip ospf authentication message-digest
 ip ospf network     point-to-point
 ip ospf cost        2
 ip ospf dead-interval 40
 ip ospf hello-interval 10
 ip ospf message-digest-key 22 md5 7 013057175804575D72
 ip ospf priority    1
 ip ospf retransmit-interval 5
 vrrp 2 address-family ipv4
  vrrpv2
  address 10.20.22.1
  priority 100
  timers advertise 1000
  track omp shutdown
 exit
exit
interface GigabitEthernet0/0/1
 no shutdown
 no ip address
exit
interface GigabitEthernet0/0/1.101
 no shutdown
 encapsulation dot1Q 101
 ip address 10.101.1.1 255.255.255.252
 ip mtu 1446
exit
interface GigabitEthernet0/0/1.102
 no shutdown
 encapsulation dot1Q 102
 ip address 10.101.2.1 255.255.255.252
 ip tcp adjust-mss 1350
 ip mtu 1496
 ip nat outside
exit
interface GigabitEthernet0/0/2
 description MPLS Interface
 no shutdown
 arp timeout 1200
 ip address 20.20.1.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1500
 mtu         1500
 negotiation auto
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
interface Tunnel102001
 no shutdown
 ip unnumbered GigabitEthernet0/0/1.102
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/1.102
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/1.102
 tunnel mode sdwan
exit
```

```
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging buffered 512000
no logging rate-limit
logging persistent
aaa authentication login default local
aaa authorization exec default local
multilink bundle-name authenticated
spanning-tree extend system-id
spanning-tree mode rapid-pvst
no crypto ikev2 diagnose error
router bgp 65201
 bgp log-neighbor-changes
 distance bgp 20 200 20
 maximum-paths eibgp 2
 neighbor 20.20.1.2 remote-as 70
 neighbor 20.20.1.2 description MPLS Service Provider
 neighbor 20.20.1.2 ebgp-multihop 1
 neighbor 20.20.1.2 maximum-prefix 2147483647 100
 neighbor 20.20.1.2 password 0 c1sco123
 neighbor 20.20.1.2 send-community both
 neighbor 20.20.1.2 timers 3 9
 address-family ipv4 unicast
  network 10.101.1.0 mask 255.255.255.252
  exit-address-family
 !
 timers bgp 60 180
!
router ospf 2 vrf 2
 area 0 range 10.20.22.0 255.255.255.0 advertise
 auto-cost reference-bandwidth 100000
 timers throttle spf 200 1000 10000
 router-id 10.20.20.20
 compatible rfc1583
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets
 redistribute nat-route dia
!
no router rip
line aux 0
 login authentication default
 stopbits 1
!
line con 0
 login authentication default
 speed    115200
 stopbits 1
!
line vty 0 4
 login authentication default
 transport input ssh
!
line vty 5 80
 login authentication default
 transport input ssh
!
diagnostic bootup level minimal
sdwan
 interface GigabitEthernet0/0/0
 exit
 interface GigabitEthernet0/0/0.10
```

```
exit
interface GigabitEthernet0/0/0.20
exit
interface GigabitEthernet0/0/1.101
 tloc-extension GigabitEthernet0/0/2
exit
interface GigabitEthernet0/0/1.102
 tunnel-interface
  encapsulation ipsec preference 0 weight 1
  no border
  color biz-internet
  no last-resort-circuit
  no low-bandwidth-link
  control-connections
  no vbond-as-stun-server
  vmanage-connection-preference 5
  port-hop
  carrier                       default
  nat-refresh-interval          5
  hello-interval                1000
  hello-tolerance               12
  no allow-service all
  allow-service bgp
  no 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
 exit
exit
interface GigabitEthernet0/0/2
 tunnel-interface
  encapsulation ipsec preference 0 weight 1
  no border
  color mpls restrict
  no last-resort-circuit
  no low-bandwidth-link
  control-connections
  no vbond-as-stun-server
  vmanage-connection-preference 5
  port-hop
  carrier                       default
  nat-refresh-interval          5
  hello-interval                1000
  hello-tolerance               12
  allow-service all
  allow-service bgp
  no 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
 exit
exit
vmanage-transaction vmanage-transaction-id 2019-05-27T08:30:07.034+00:00
omp
 no shutdown
 send-path-limit  16
```

```
  ecmp-limit       16
  graceful-restart
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4 vrf 1
   advertise ospf external
   advertise connected
   advertise static
  !
  address-family ipv4 vrf 2
   advertise connected
   advertise static
  !
 !
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
netconf-yang cisco-ia blocking cli-blocking-enabled
bfd color mpls
 hello-interval 1000
 no pmtu-discovery
 multiplier     7
!
bfd color biz-internet
 hello-interval 1000
 no pmtu-discovery
 multiplier     7
!
bfd app-route multiplier 6
bfd app-route poll-interval 120000
security
 ipsec
  rekey               86400
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
nacm cmd-read-default deny
nacm cmd-exec-default deny
```

Branch 112003: BR2-WAN-Edge2

```
 system
 gps-location latitude 33.4484
 gps-location longitude -112.074
 device-groups         BRANCH Primary UG5 US West v1000
 system-ip             10.255.241.22
 overlay-id            1
 site-id               112003
 port-offset           1
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 no port-hop
 track-transport
 track-default-gateway
```

```
 console-baud-rate     115200
 vbond 10.10.60.2 port 12346
!
no service pad
service password-encryption
service timestamps debug datetime msec
service timestamps log datetime msec
no service tcp-small-servers
no service udp-small-servers
hostname BR2-WAN-Edge2
username admin privilege 15 secret 9 $9$3VEF3VAI3lMM3E$awMmxogwHvRdxoHA5u1utUOAmKPBUvUbkD4PnwNWmWk
vrf definition 1
 description Service VPN
 rd          1:1
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition 2
 description Service VPN
 rd          1:2
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 description Management VPN
 rd          1:512
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
no ip dhcp use class
ip name-server 208.67.220.220 208.67.222.222
ip route 0.0.0.0 0.0.0.0 10.101.1.1 1
ip route 0.0.0.0 0.0.0.0 30.20.1.2 1
ip http authentication local
ip http server
ip http secure-server
no ip igmp ssm-map query dns
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/2 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60
ip nat route vrf 2 0.0.0.0 0.0.0.0 global
no ip rsvp signalling rate-limit
ipv6 unicast-routing
no ipv6 mld ssm-map query dns
interface GigabitEthernet0
 description Management Interface
 no shutdown
 arp timeout 1200
 vrf forwarding Mgmt-intf
 ip address 100.119.118.9 255.255.255.0
 ip redirects
 ip mtu    1500
```

```
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/0
 description LAN Parent Interface
 no shutdown
 arp timeout 1200
 no ip address
 ip redirects
 ip mtu    1504
 mtu         1504
 negotiation auto
exit
interface GigabitEthernet0/0/0.10
 no shutdown
 encapsulation dot1Q 10
 vrf forwarding 1
 ip address 10.20.21.3 255.255.255.0
 ip mtu 1500
 vrrp 1 address-family ipv4
  vrrpv2
  address 10.20.21.1
  priority 100
  timers advertise 1000
  track omp shutdown
 exit
exit
interface GigabitEthernet0/0/0.20
 no shutdown
 encapsulation dot1Q 20
 vrf forwarding 2
 ip address 10.20.22.3 255.255.255.0
 ip mtu 1500
 ip ospf 2 area 0
 ip ospf authentication message-digest
 ip ospf network     point-to-point
 ip ospf cost        1
 ip ospf dead-interval 40
 ip ospf hello-interval 10
 ip ospf message-digest-key 22 md5 7 141443180F0B7B797769
 ip ospf priority    1
 ip ospf retransmit-interval 5
 vrrp 2 address-family ipv4
  vrrpv2
  address 10.20.22.1
  priority 100
  timers advertise 1000
  track omp shutdown
 exit
exit
interface GigabitEthernet0/0/1
 no shutdown
 no ip address
exit
interface GigabitEthernet0/0/1.101
 no shutdown
 encapsulation dot1Q 101
 ip address 10.101.1.2 255.255.255.252
 ip tcp adjust-mss 1350
 ip mtu 1496
exit
interface GigabitEthernet0/0/1.102
 no shutdown
 encapsulation dot1Q 102
```

```
 ip address 10.101.2.2 255.255.255.252
 ip mtu 1446
exit
interface GigabitEthernet0/0/2
 description INET Interface
 no shutdown
 arp timeout 1200
 ip address 30.20.1.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1496
 ip nat outside
 mtu         1500
 negotiation auto
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
interface Tunnel101001
 no shutdown
 ip unnumbered GigabitEthernet0/0/1.101
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/1.101
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/1.101
 tunnel mode sdwan
exit
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging buffered 512000
no logging rate-limit
logging persistent
aaa authentication login default local
aaa authorization exec default local
multilink bundle-name authenticated
spanning-tree extend system-id
spanning-tree mode rapid-pvst
no crypto ikev2 diagnose error
router ospf 2 vrf 2
 area 0 range 10.20.22.0 255.255.255.0 advertise
 auto-cost reference-bandwidth 100000
 timers throttle spf 200 1000 10000
 router-id 10.21.21.21
 compatible rfc1583
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets
 redistribute nat-route dia
!
no router rip
line aux 0
 login authentication default
 stopbits 1
!
line con 0
 login authentication default
```

```
 speed    115200
 stopbits 1
!
line vty 0 4
 login authentication default
 transport input ssh
!
line vty 5 80
 login authentication default
 transport input ssh
!
diagnostic bootup level minimal
sdwan
 interface GigabitEthernet0/0/0
 exit
 interface GigabitEthernet0/0/0.10
 exit
 interface GigabitEthernet0/0/0.20
 exit
 interface GigabitEthernet0/0/1.101
  tunnel-interface
   encapsulation ipsec preference 0 weight 1
   no border
   color mpls restrict
   no last-resort-circuit
   no low-bandwidth-link
   control-connections
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   allow-service bgp
   no 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
  exit
 exit
 interface GigabitEthernet0/0/1.102
  tloc-extension GigabitEthernet0/0/2
 exit
 interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec preference 0 weight 1
   no border
   color biz-internet
   no last-resort-circuit
   no low-bandwidth-link
   control-connections
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
```

```
   allow-service all
   no allow-service bgp
   no 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
  exit
 exit
 vmanage-transaction vmanage-transaction-id 2019-05-25T23:22:20.21+00:00
 omp
  no shutdown
  send-path-limit  16
  ecmp-limit       16
  graceful-restart
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4 vrf 1
   advertise ospf external
   advertise connected
   advertise static
  !
  address-family ipv4 vrf 2
   advertise connected
   advertise static
  !
 !
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
netconf-yang cisco-ia blocking cli-blocking-enabled
bfd color mpls
 hello-interval 1000
 no pmtu-discovery
 multiplier     7
!
bfd color biz-internet
 hello-interval 1000
 no pmtu-discovery
 multiplier     7
!
bfd app-route multiplier 6
bfd app-route poll-interval 120000
security
 ipsec
  rekey               86400
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
nacm cmd-read-default deny
nacm cmd-exec-default deny
```

Single-Router Hybrid Transport Design

Branch 112004: BR3-WAN-Edge1

```
system
 gps-location latitude 37.409284
 gps-location longitude -97.335
 device-groups         DC Primary UG3 US West v5000
 system-ip             10.255.241.31
 overlay-id            1
 site-id               112004
 port-offset           0
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 no port-hop
 track-transport
 track-default-gateway
 upgrade-confirm       15
 console-baud-rate     115200
 vbond 10.10.60.2 port 12346
!
no service pad
service password-encryption
service timestamps debug datetime msec
service timestamps log datetime msec
no service tcp-small-servers
no service udp-small-servers
hostname BR3-WAN-Edge1
username admin privilege 15 secret 9 $9$3VEF3VAI3lMM3E$awMmxogwHvRdxoHA5u1utUOAmKPBUvUbkD4PnwNWmWk
vrf definition 1
 description Service VPN
 rd          1:1
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition 2
 description Service VPN
 rd          1:2
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 description Management VPN
 rd          1:512
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
no ip dhcp use class
ip name-server 208.67.220.220 208.67.222.222
ip route 0.0.0.0 0.0.0.0 10.30.23.1 1
ip route 0.0.0.0 0.0.0.0 30.30.1.2 1
no ip igmp ssm-map query dns
```

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/2 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60
ip nat route vrf 1 0.0.0.0 0.0.0.0 global
ip nat route vrf 2 0.0.0.0 0.0.0.0 global
no ip rsvp signalling rate-limit
ipv6 unicast-routing
no ipv6 mld ssm-map query dns
cdp run
interface GigabitEthernet0
 description Management Interface
 no shutdown
 arp timeout 1200
 vrf forwarding Mgmt-intf
 ip address 100.119.118.6 255.255.255.0
 ip redirects
 ip mtu    1500
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/0
 description MPLS Interface
 no shutdown
 arp timeout 1200
 ip address 10.30.23.2 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1500
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/1
 description LAN Parent Interface
 no shutdown
 arp timeout 1200
 no ip address
 ip redirects
 ip mtu    1504
 mtu         1504
 negotiation auto
exit
interface GigabitEthernet0/0/1.10
 no shutdown
 encapsulation dot1Q 10
 vrf forwarding 1
 ip address 10.30.13.2 255.255.255.252
 ip mtu 1500
 ip ospf 1 area 0
 ip ospf authentication message-digest
 ip ospf network     point-to-point
 ip ospf cost        1
 ip ospf dead-interval 40
 ip ospf hello-interval 10
 ip ospf message-digest-key 22 md5 7 08221D5D0A16544541
 ip ospf priority    1
 ip ospf retransmit-interval 5
exit
interface GigabitEthernet0/0/1.20
 no shutdown
 encapsulation dot1Q 20
 vrf forwarding 2
 ip address 10.30.12.2 255.255.255.252
 ip mtu 1500
 ip ospf 2 area 0
```

```
 ip ospf authentication message-digest
 ip ospf network     point-to-point
 ip ospf cost        1
 ip ospf dead-interval 40
 ip ospf hello-interval 10
 ip ospf message-digest-key 22 md5 7 141443180F0B7B7977
 ip ospf priority    1
 ip ospf retransmit-interval 5
exit
interface GigabitEthernet0/0/2
 description INET Interface
 no shutdown
 arp timeout 1200
 ip address 30.30.1.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1500
 ip nat outside
 mtu         1500
 negotiation auto
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
logging persistent size 104857600 filesize 10485760
logging buffered 512000
logging console debugging
no logging rate-limit
logging persistent
aaa authentication login default local
aaa authorization exec default local
multilink bundle-name authenticated
spanning-tree extend system-id
spanning-tree mode rapid-pvst
no crypto ikev2 diagnose error
router ospf 1 vrf 1
 area 0 range 10.30.13.0 255.255.255.252 advertise
 auto-cost reference-bandwidth 100000
 timers throttle spf 200 1000 10000
 router-id 10.30.31.31
 compatible rfc1583
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets
 redistribute nat-route dia
!
```

```
router ospf 2 vrf 2
 area 0 range 10.30.12.0 255.255.255.252 advertise
 auto-cost reference-bandwidth 100000
 timers throttle spf 200 1000 10000
 router-id 10.30.31.31
 compatible rfc1583
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets
 redistribute nat-route dia
!
no router rip
line aux 0
 login authentication default
 stopbits 1
!
line con 0
 login authentication default
 speed    115200
 stopbits 1
!
line vty 0 4
 login authentication default
 transport input ssh
!
line vty 5 80
 login authentication default
 transport input ssh
!
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec preference 200 weight 1
   no border
   color mpls restrict
   no last-resort-circuit
   no low-bandwidth-link
   control-connections
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                        default
   nat-refresh-interval           5
   hello-interval                 1000
   hello-tolerance                12
   allow-service all
   allow-service bgp
   no 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
  exit
 exit
 interface GigabitEthernet0/0/1
 exit
 interface GigabitEthernet0/0/1.10
 exit
 interface GigabitEthernet0/0/1.20
```

```
 exit
 interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec preference 100 weight 1
   no border
   color biz-internet
   no last-resort-circuit
   no low-bandwidth-link
   control-connections
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   allow-service all
   allow-service bgp
   no 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
  exit
 exit
 vmanage-transaction vmanage-transaction-id 2019-05-18T19:47:26.607+00:00
 omp
  no shutdown
  send-path-limit  16
  ecmp-limit       16
  graceful-restart
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4 vrf 1
   advertise connected
   advertise static
  !
  address-family ipv4 vrf 2
   advertise connected
   advertise static
  !
 !
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
netconf-yang cisco-ia blocking cli-blocking-enabled
bfd color mpls
 hello-interval 1000
 no pmtu-discovery
 multiplier     7
!
bfd color biz-internet
 hello-interval 1000
 no pmtu-discovery
 multiplier     7
```

```
!
bfd app-route multiplier 6
bfd app-route poll-interval 120000
security
 ipsec
  rekey               86400
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
nacm cmd-read-default deny
nacm cmd-exec-default deny
```

Single-Router Dual-Internet Design

Branch 112005: BR4-WAN-EDGE1

```
viptela-system:system
system
 gps-location latitude 37.409284
 gps-location longitude -121.928528
 device-groups         BRANCH Primary UG5 US West v1000
 system-ip             100.255.241.41
 overlay-id            1
 site-id               112005
 port-offset           1
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 no port-hop
 track-transport
 track-default-gateway
 console-baud-rate     115200
 vbond 10.10.60.2 port 12346
!
service internal
no service pad
service password-encryption
service timestamps debug datetime msec
service timestamps log datetime msec
no service tcp-small-servers
no service udp-small-servers
hostname BR4-WAN-Edge1
username admin privilege 15 secret 9 $9$3VEF3VAI3lMM3E$awMmxogwHvRdxoHA5u1utUOAmKPBUvUbkD4PnwNWmWk
vrf definition 1
 description Service VPN
 rd          1:1
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition 2
 description Service VPN
 rd          1:2
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
```

```
!
vrf definition Mgmt-intf
 description Management VPN
 rd          1:512
 address-family ipv4
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
no ip dhcp use class
ip route 0.0.0.0 0.0.0.0 10.40.34.2 1
ip route 0.0.0.0 0.0.0.0 10.40.35.2 1
no ip igmp ssm-map query dns
no ip rsvp signalling rate-limit
ipv6 unicast-routing
no ipv6 mld ssm-map query dns
interface GigabitEthernet0
 description Management Interface
 no shutdown
 arp timeout 1200
 vrf forwarding Mgmt-intf
 ip address 100.119.118.10 255.255.255.0
 ip redirects
 ip mtu    1500
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/0
 description WAN Parent Interface
 no shutdown
 arp timeout 1200
 no ip address
 ip redirects
 ip mtu    1504
 mtu         1504
 negotiation auto
exit
interface GigabitEthernet0/0/0.10
 no shutdown
 encapsulation dot1Q 10
 vrf forwarding 1
 ip address 10.40.4.2 255.255.255.252
 ip mtu 1500
 ip ospf 1 area 0
 ip ospf authentication message-digest
 ip ospf network     point-to-point
 ip ospf cost        1
 ip ospf dead-interval 40
 ip ospf hello-interval 10
 ip ospf message-digest-key 22 md5 7 06055E324F41584B56
 ip ospf priority    1
 ip ospf retransmit-interval 5
exit
interface GigabitEthernet0/0/0.20
 no shutdown
 encapsulation dot1Q 20
 vrf forwarding 2
 ip address 10.40.5.2 255.255.255.252
 ip mtu 1500
 ip ospf 2 area 0
 ip ospf authentication message-digest
 ip ospf network     point-to-point
```

```
 ip ospf cost        1
 ip ospf dead-interval 40
 ip ospf hello-interval 10
 ip ospf message-digest-key 22 md5 7 03070A180500701E1D
 ip ospf priority    1
 ip ospf retransmit-interval 5
exit
interface GigabitEthernet0/0/1
 description Bronze Interface
 no shutdown
 arp timeout 1200
 ip address 10.40.34.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1500
 mtu         1500
 negotiation auto
exit
interface GigabitEthernet0/0/2
 description INET Interface
 no shutdown
 arp timeout 1200
 ip address 10.40.35.1 255.255.255.252
 ip redirects
 ip tcp adjust-mss 1350
 ip mtu    1500
 mtu         1500
 negotiation auto
exit
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet0/0/1
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/1
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/1
 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
logging persistent size 104857600 filesize 10485760
logging buffered 512000
no logging rate-limit
logging persistent
aaa authentication login default local
aaa authorization exec default local
multilink bundle-name authenticated
spanning-tree extend system-id
spanning-tree mode rapid-pvst
no crypto ikev2 diagnose error
router ospf 1 vrf 1
 area 0 range 10.40.0.0 255.255.0.0 advertise
 auto-cost reference-bandwidth 100000
 timers throttle spf 200 1000 10000
 router-id 10.40.42.42
 compatible rfc1583
```

```
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets
!
router ospf 2 vrf 2
 area 0 range 10.40.5.0 255.255.255.252 advertise
 auto-cost reference-bandwidth 100000
 timers throttle spf 200 1000 10000
 router-id 10.40.42.42
 compatible rfc1583
 default-information originate
 distance ospf external 110
 distance ospf inter-area 110
 distance ospf intra-area 110
 redistribute omp subnets
 redistribute nat-route dia
!
no router rip
line aux 0
 login authentication default
 stopbits 1
!
line con 0
 login authentication default
 speed    115200
 stopbits 1
!
line vty 0 4
 login authentication default
 transport input ssh
!
line vty 5 80
 login authentication default
 transport input ssh
!
sdwan
 interface GigabitEthernet0/0/0
 exit
 interface GigabitEthernet0/0/0.10
 exit
 interface GigabitEthernet0/0/0.20
 exit
 interface GigabitEthernet0/0/1
  tunnel-interface
   encapsulation ipsec preference 0 weight 1
   no border
   color bronze
   no last-resort-circuit
   no low-bandwidth-link
   control-connections
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   allow-service all
   allow-service bgp
   no 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
  exit
 exit
 interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec preference 0 weight 1
   no border
   color biz-internet
   no last-resort-circuit
   no low-bandwidth-link
   control-connections
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   allow-service all
   allow-service bgp
   no 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
  exit
 exit
 vmanage-transaction vmanage-transaction-id 2019-05-28T00:54:15.496+00:00
 omp
  no shutdown
  send-path-limit  16
  ecmp-limit       16
  graceful-restart
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4 vrf 1
   advertise ospf external
   advertise connected
   advertise static
  !
  address-family ipv4 vrf 2
   advertise connected
   advertise static
  !
 !
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
netconf-yang cisco-ia blocking cli-blocking-enabled
bfd color mpls
 hello-interval 1000
```

```
 no pmtu-discovery
 multiplier     7
!
bfd color biz-internet
 hello-interval 1000
 no pmtu-discovery
 multiplier     7
!
bfd app-route multiplier 6
bfd app-route poll-interval 120000
security
 ipsec
  rekey               86400
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
nacm cmd-read-default deny
nacm cmd-exec-default deny
```

Datacenter 112001: DC1-WAN-Edge1

```
system
 host-name               DC1-WAN-Edge1
 gps-location latitude 37.409284
 gps-location longitude -121.928528
 device-groups           DC Primary UG3 US West v5000
 system-ip               10.255.241.102
 site-id                 112001
 admin-tech-on-failure
 no route-consistency-check
 sp-organization-name    "ENB-Solutions - 21615"
 organization-name       "ENB-Solutions - 21615"
 no port-hop
 vbond 10.10.60.2
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password $6$siwKBQ==$wT2lUa9BSreDPI6gB8sl4E6PAJoVXgMbgv/whJ8F1C6sWdRazdxorYYTLrL6syiG6qnLABTnrE9
6HJiKF6QRq1
  !
 !
 logging
  disk
   enable
  !
 !
!
bfd color mpls
 no pmtu-discovery
```

```
!
bfd color biz-internet
 no pmtu-discovery
!
bfd app-route poll-interval 120000
omp
 no shutdown
 send-path-limit  16
 ecmp-limit       16
 graceful-restart
!
security
 ipsec
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
vpn 0
 name "Transport VPN"
 ecmp-hash-key layer4
 interface 10ge0/2
  tunnel-interface
   encapsulation ipsec
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  shutdown
 !
 interface 10ge0/3
  description          "INET Interface"
  ip address 10.2.57.1/30
  tunnel-interface
   encapsulation ipsec preference 12
   color biz-internet
   allow-service all
   allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   allow-service ospf
   no allow-service stun
   allow-service https
  !
  clear-dont-fragment
  tcp-mss-adjust       1350
  no shutdown
  bandwidth-upstream   1000000
  bandwidth-downstream 1000000
 !
 ip route 0.0.0.0/0 10.2.56.2
 ip route 0.0.0.0/0 10.2.57.2
!
vpn 1
```

```
 name              "Service VPN 1"
 ecmp-hash-key layer4
 router
  bgp 65113
   router-id        10.100.102.102
   propagate-aspath
   address-family ipv4-unicast
    network 10.2.35.0/30
    maximum-paths paths 2
    redistribute omp
   !
   neighbor 10.2.25.1
    description Agg-Switch2
    no shutdown
    remote-as   65112
    timers
     keepalive 3
     holdtime  9
    !
    password    $8$EvJJRIC08Ufsso+3a4HFbKenlrhAToPCBiyA2RWRLY4=
    address-family ipv4-unicast
    !
   !
   neighbor 10.2.35.1
    description Agg-Switch1
    no shutdown
    remote-as   65112
    timers
     keepalive 3
     holdtime  9
    !
    password    $8$y86gFxlTwDb3aczIjc9BLYaCWQvaNi6q4ovLL1DL4fs=
    address-family ipv4-unicast
    !
   !
  !
 !
 interface 10ge0/0
  description "To DC1-SW2 G1/0/6"
  ip address 10.2.35.2/30
  no shutdown
 !
 interface 10ge0/1
  description "To DC1-SW1 G1/0/5"
  ip address 10.2.25.2/30
  no shutdown
 !
 omp
  advertise bgp
 !
 tcp-optimization
!
vpn 512
 name "Management VPN"
 interface mgmt0
  description "Management Interface"
  ip address 100.119.118.12/24
  no shutdown
 !
!
```

Datacenter 112001: DC1-WAN-Edge2

```
system
 host-name               DC1-WAN-Edge2
 gps-location latitude 37.409284
 gps-location longitude -121.928528
 device-groups           DC Primary UG2 US West v5000
 system-ip               10.255.241.101
 site-id                 112001
 admin-tech-on-failure
 no route-consistency-check
 sp-organization-name    "ENB-Solutions - 21615"
 organization-name       "ENB-Solutions - 21615"
 no port-hop
 vbond 10.10.60.2
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password $6$siwKBQ==$wT2lUa9BSreDPI6gB8sl4E6PAJoVXgMbgv/whJ8F1C6sWdRazdxorYYTLrL6syiG6qnLABTnrE9
6HJiKF6QRq1
  !
 !
 logging
  disk
   enable
  !
 !
!
bfd color mpls
 no pmtu-discovery
!
bfd color biz-internet
 no pmtu-discovery
!
bfd app-route poll-interval 120000
omp
 no shutdown
 send-path-limit  16
 ecmp-limit       16
 graceful-restart
!
security
 ipsec
  replay-window       4096
  authentication-type sha1-hmac ah-sha1-hmac
 !
!
vpn 0
 name "Transport VPN"
 ecmp-hash-key layer4
 interface 10ge0/2
  description          "INET Interface"
  ip address 10.2.47.1/30
```

```
  tunnel-interface
   encapsulation ipsec preference 10
   color biz-internet
   allow-service all
   allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   allow-service ospf
   no allow-service stun
   allow-service https
  !
  clear-dont-fragment
  tcp-mss-adjust       1350
  no shutdown
  bandwidth-upstream   1000000
  bandwidth-downstream 1000000
 !
 interface 10ge0/3
  description          "MPLS Interface"
  ip address 10.2.46.1/30
  tunnel-interface
   encapsulation ipsec preference 10
   color mpls restrict
   no control-connections
   allow-service all
   allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   allow-service ospf
   no allow-service stun
   allow-service https
  !
  clear-dont-fragment
  tcp-mss-adjust       1350
  no shutdown
  bandwidth-upstream   1000000
  bandwidth-downstream 1000000
 !
 ip route 0.0.0.0/0 10.2.46.2
 ip route 0.0.0.0/0 10.2.47.2
!
vpn 1
 name             "Service VPN 1"
 ecmp-hash-key layer4
 router
  bgp 65113
   router-id        10.100.101.101
   propagate-aspath
   address-family ipv4-unicast
    network 10.2.24.0/30
    maximum-paths paths 2
    redistribute omp
   !
   neighbor 10.2.24.1
    description Agg-Switch1
    no shutdown
```

```
    remote-as   65112
    timers
     keepalive 3
     holdtime  9
    !
    password    $8$VFBpKDv+e+ZUW1UZYKifUSJVwaLYhI1QyjWZnqdg8Ak=
    address-family ipv4-unicast
    !
   !
   neighbor 10.2.34.1
    description Agg-Switch2
    no shutdown
    remote-as   65112
    timers
     keepalive 3
     holdtime  9
    !
    password    $8$iRmY15bjPLQyJWVUfdv32zpfTK2i+Z7MHMSL2RmWGTI=
    address-family ipv4-unicast
    !
   !
  !
 !
 interface 10ge0/0
  description "To DC1-SW1 G1/0/6"
  ip address 10.2.24.2/30
  no shutdown
 !
 interface 10ge0/1
  description "To DC1-SW2 G1/0/5"
  ip address 10.2.34.2/30
  no shutdown
 !
 omp
  advertise bgp
 !
 tcp-optimization
!
vpn 512
 name "Management VPN"
 interface mgmt0
  description "Management Interface"
  ip address 100.119.118.11/24
  no shutdown
 !
!
```

Appendix F—Glossary

DIA Direct Internet Access

VPN Virtual Private Network

NAT Network Address Translation

LAN Local Area Network

WAN Wide Area Network

About this guide

Feedback & discussion

For comments and suggestions about our guides, please join the discussion on Cisco Community.