Versa Secure SD-WAN Integration with SSE

For supported software information, click here.

Unified Secure Access Services Edge (SASE) is the term used to describe the combination of Secure SD-WAN and Secure Service Edge (SSE) in an architecture where both components are hosted on the Versa Cloud on behalf of a service provider or enterprise.

Alternatively, Secure SD-WAN can be hosted by a service provider on behalf of an enterprise, or or it can be hosted by the enterprise directly. In such an architecture, IPsec tunnels are used to integrate the Secure SD-WAN to the Versa-hosted SSE cloud. In this sense, blending Secure SD-WAN with SSE creates the same coherent SASE architecture using a different architecture than the unified SASE design hosted by Versa Networks.

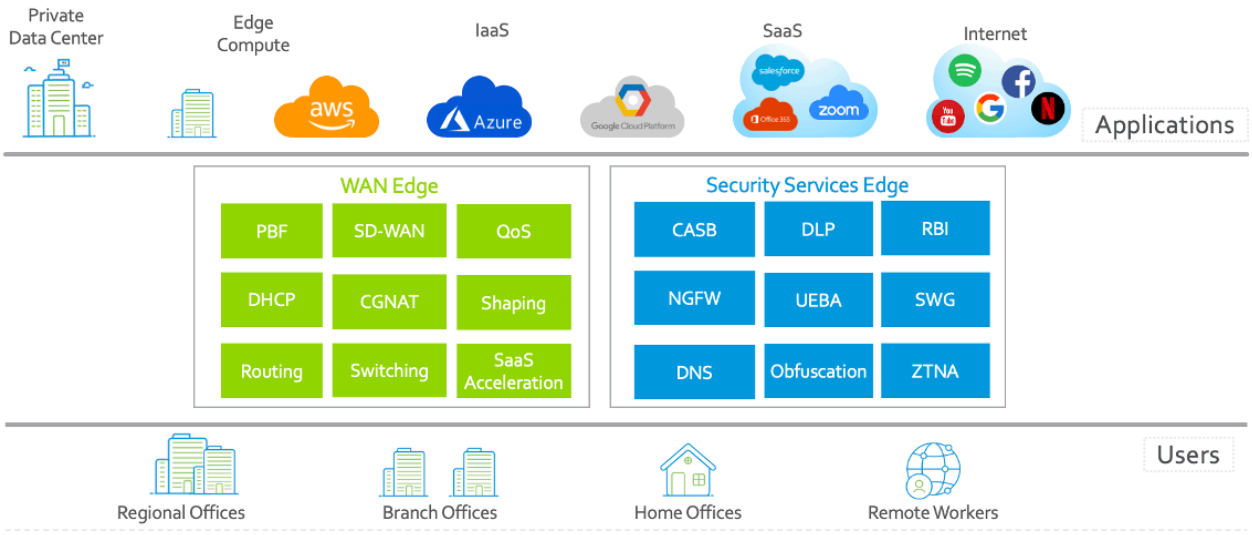
This solution article focuses on how to integrate service provider– and enterprise-hosted Secure SD-WAN with Versa Networks hosted SSE. This article provides the following:

- Simplified overview of SASE
- Overview of the key components of the Versa Networks SASE solution
- Two use cases for integrating Secure SD-WAN hosted by the service provider or the enterprise and SSE hosted by Versa Networks
- Step-by-step configuration for stitching together components based on the following Secure SD-WAN branch topologies:
  - Single CPE and single WAN link based on static routes
  - Single CPE and dual WAN links based on BGP
  - Dual CPE and single WAN link per CPE based on BGP
- Various sections that describe tuneable features that you can use to customize the architectures

Simplified Overview of SASE

SASE is the blending of two components: WAN Edge and Security Services Edge (SSE), as illustrated in Figure 1.

Figure 1: SASE Architecture Components



WAN Edge enables network connectivity between users (shown at the bottom of the figure) and applications (shown at the top of the figure). WAN Edge includes multiple capabilities, such as SD-WAN, quality of service (QoS), Dynamic Host Configuration Protocol (DHCP), and routing. An example of a WAN Edge is a VOS-enabled appliance or device.

SSE secures access between users and applications. SSE includes multiple capabilities, such as access control, threat protection, data security, security monitoring, and usage control.

In summary, a SASE architecture provides connectivity between users and applications while at the same time providing connectivity in a secure manner using a variety of security tools.

Key Components of the Versa Networks SASE Solution

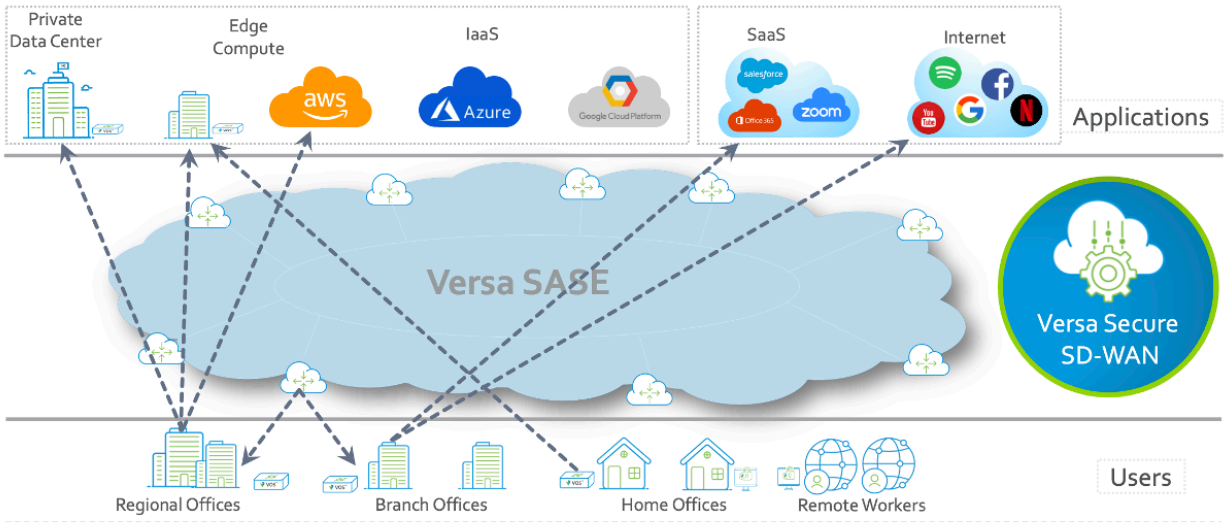
Versa Networks SASE solutions are built using the following key components:

- Versa Secure SD-WAN—Securely connects offices into a SASE architecture
- Versa Secure Access—Securely connects remote workers into a SASE architecture
- Versa Secure Web Gateway—Securely connects users through the SASE architecture to public clouds, SaaS applications, and the internet

The following sections provide more detail on these three components.

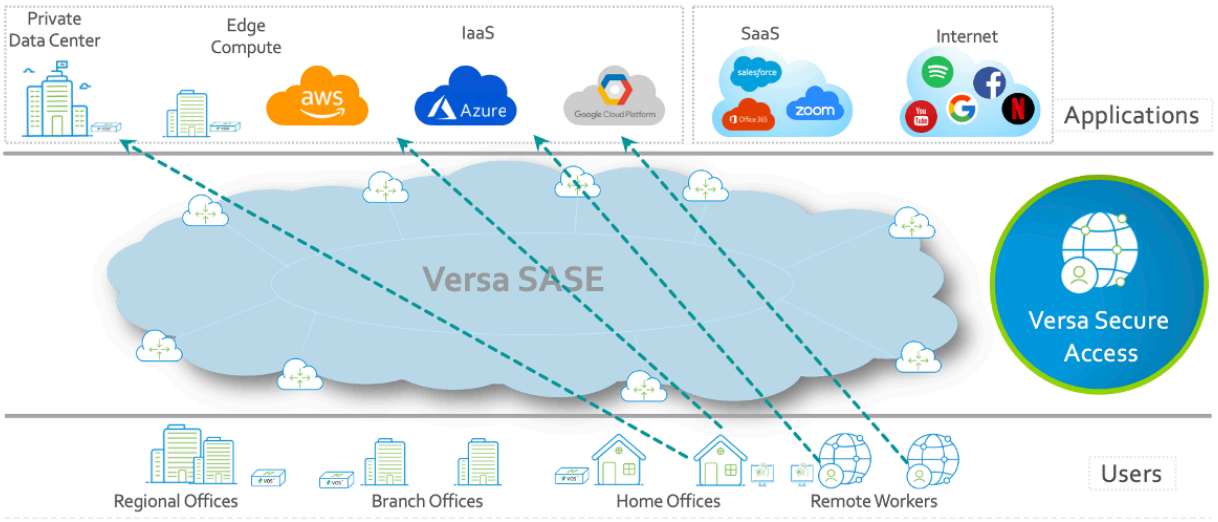
Versa Secure SD-WAN enables branch and home office users to connect to private data centers and clouds as well as to SaaS applications and the internet, as illustrated in Figure 2.

Figure 2: Versa Secure SD-WAN



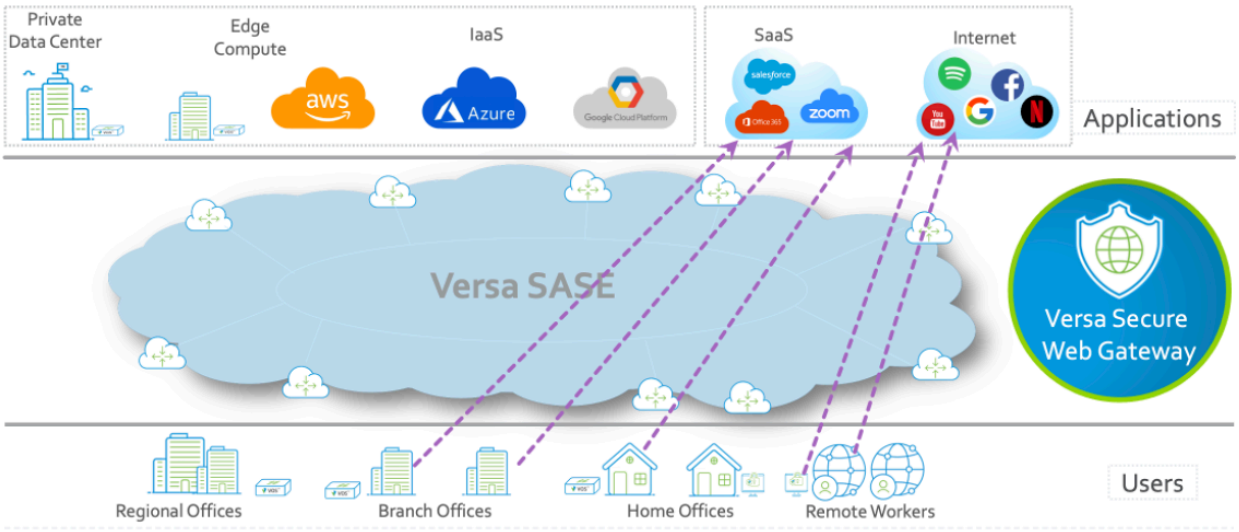
Versa Secure Access (VSA) enables remote workers and home office users to connect securely to private clouds and data centers, as illustrated in Figure 3.

Figure 3: VSA



Versa Secure Web Gateway (SWG) enables users to connect securely to public and private clouds, and to SaaS applications and the internet from anywhere, no matter where those users are accessing the network from, whether from branch offices, home offices, or anywhere else, as illustrated in Figure 4.

Figure 4: SWG



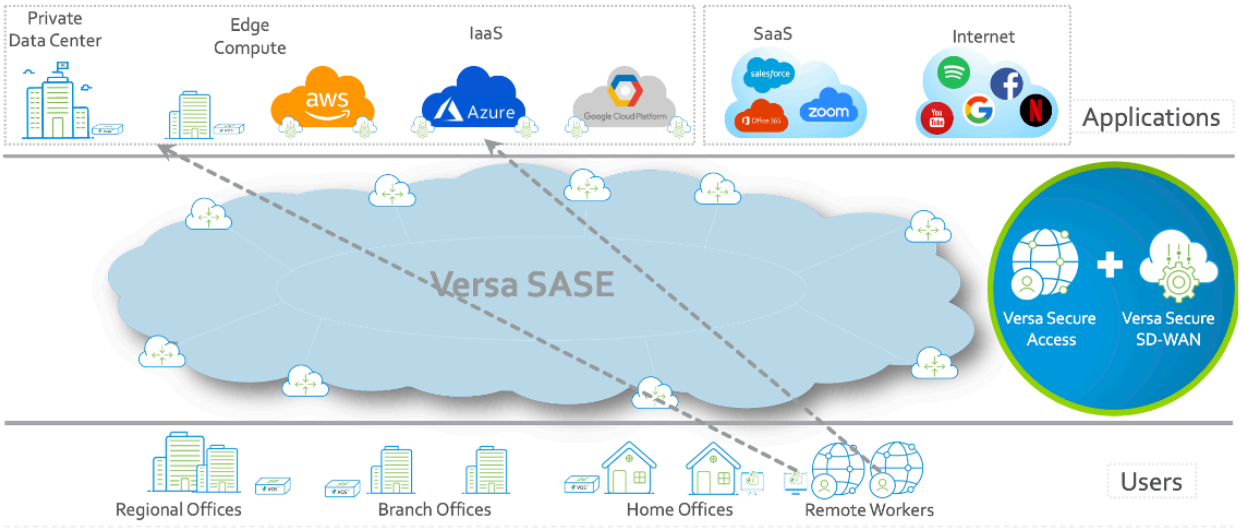
Integrating Secure SD-WAN and SSE SASE Components

As mentioned above, unified SASE is the term used to describe the combination of Secure SD-WAN and SSE in an architecture where both components are hosted on the Versa Cloud on behalf of a service provider or enterprise. Alternatively, Secure SD-WAN can be hosted by a service provider on behalf of an enterprise, or it can be hosted by the enterprise directly. In such an architecture, you use static IPSec or GRE tunnels to integrate the Secure SD-WAN into the Versa Networks–hosted SSE cloud. In this sense, blending Secure SD-WAN with SSE creates the same coherent SASE architecture using a different architecture than the unified SASE design hosted by Versa Networks. In such architectures, tunnels are used to integrate Secure SD-WAN and SSE.

For unified SASE, you use IPsec tunnels to integrate Secure SD-WAN and SSE. There are two common use cases for integrating the Secure SD-WAN and SSE components.

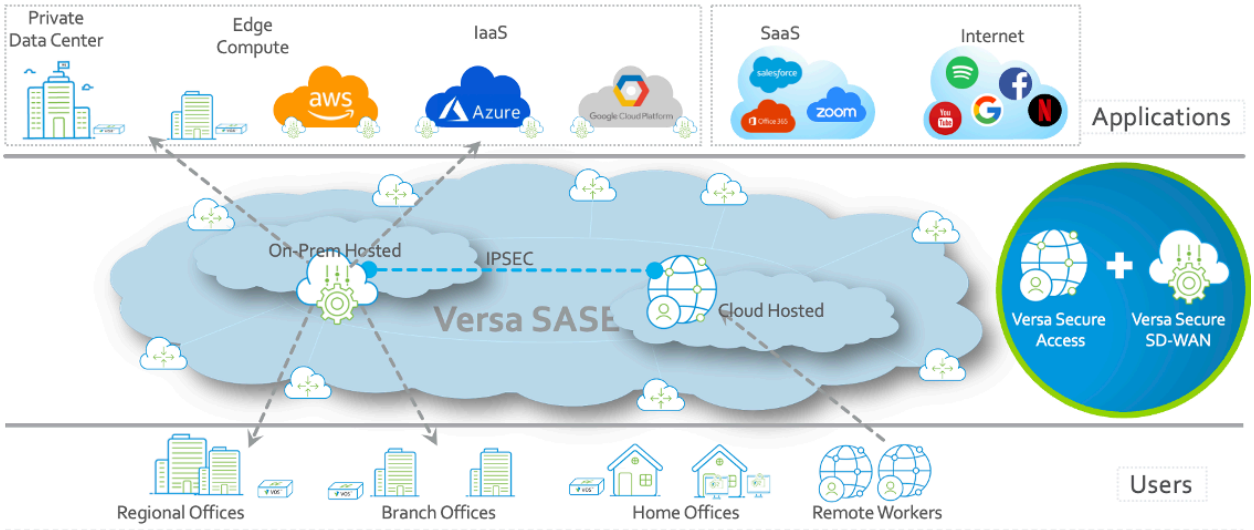
One integration use case is that VSA users may require access to Secure SD-WAN–hosted private data centers and clouds or offices. See Figure 5.

Figure 5: VSA Integration with Secure SD-WAN



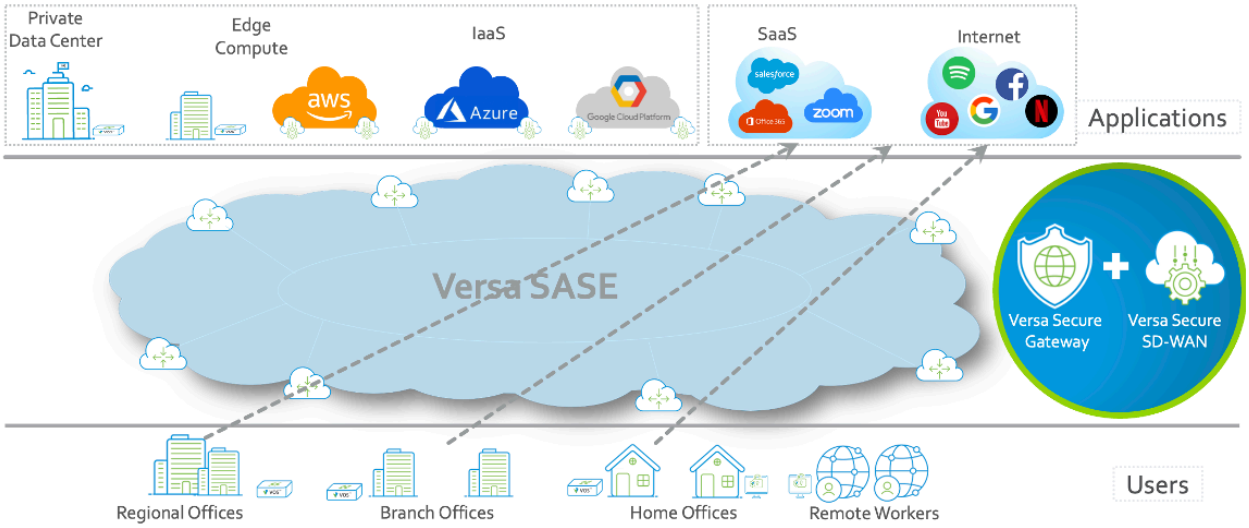
In such a design, you use IPsec tunnels to stitch cloud-hosted SSE and on-premises–hosted Secure SD-WAN as illustrated in Figure 6.

Figure 6: Stitching VSA and Secure SD-WAN



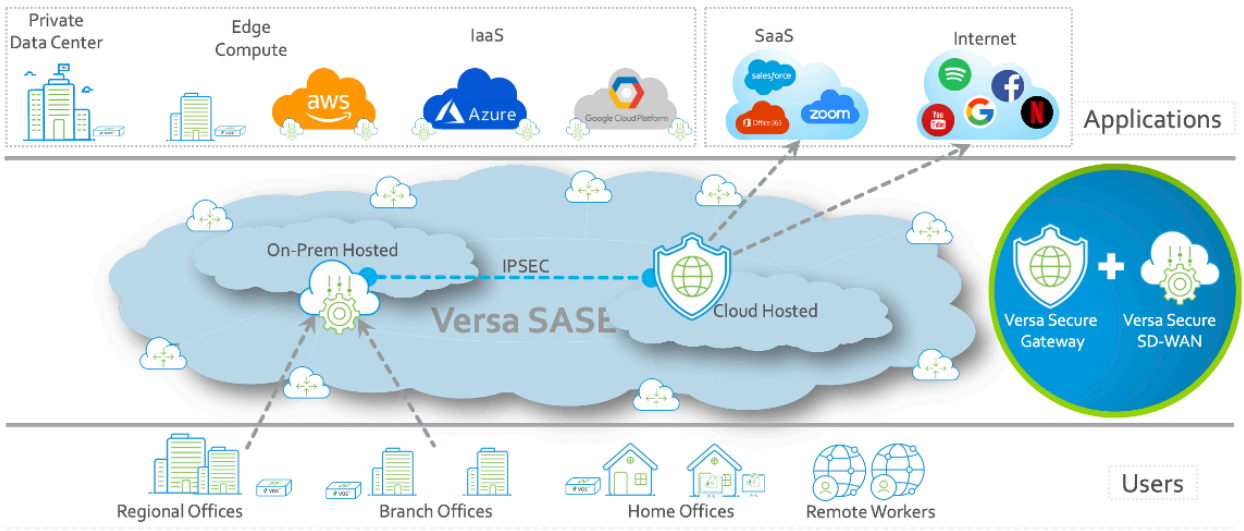
A second integration use case is when offices require a cloud-hosted SWG to connect users to SaaS and Internet applications, as illustrated in Figure 7.

Figure 7: SWG Integration with Secure SD-WAN



In such a design, you use IPsec tunnels to stitch cloud-hosted SSE and on-premises–hosted Secure SD-WAN as illustrated in Figure 8.

Figure 8: Stitching SWG and Secure SD-WAN



Step-by-Step Configurations for Building IPsec Tunnels

The following sections describe the configuration procedures for configuring IPsec tunnels to integrate Secure SD-WAN and SSE components for three different topologies:

- Single CPE, single WAN
- Single CPE, dual WAN
- Dual CPE, dual WAN

Procedures are provided for configuring from Versa Concerto to the Versa Operating System™ (VOS™) VCG and from Versa Director to a VOS branch.

The screenshots used in the procedures are based on the following software versions:

- Versa Director—Release 21.3. Note, though, that the screenshots and configurations are the same as in Release 21.2.
- Versa Concerto—Release 11.2.3

Best Practices

The following are general best practices guidelines to supplement the step-by-step configuration guidelines:

- It is recommended that you use fully qualified domain names (FQDNs) to refer to site-to-site peers regardless of whether you are configuring the VOS branch or the VOS VCG. Note that while we have used IP addresses in this article, it is recommended that you use FQDNs for production environments. For more information about FQDNs, see Configure with FQDNs, below.
- Adjust the MTU of IPsec tunnels to avoid fragmentation and reassembly. Modifying the MTU is described in the step-by-step procedures. The recommended IP MTU size is 1336 bytes, which is the default MTU on the VOS VCG.
- If there are multiple IPsec connections between the on-premises–hosted and cloud-hosted devices, it is recommended that you use BGP, in combination with BFD, rather than using static routing. Doing so ensures that either platform fails over seamlessly and promptly. For an example of a deployment based on static routing, see Configure a Single-CPE, Single-WAN Topology, below. For an example of a deployment based on BGP and BFD, see Configure a Single-CPE, Dual-WAN Topology or Configure a Dual-CPE, Dual-WAN Topology, below.
- You may need to associate interfaces with zones, and you may need to associate zones with firewall rules, to permit traffic over an IPsec tunnel. If traffic between platforms fails and yet IPsec and routing appear to be functioning correctly, check the session table to determine whether traffic is being dropped by the firewall. For more information, see Tune Firewall Rules, below.
- If you are using BGP between platforms, ensure that a BGP policy is associated with peers to control routing. Otherwise, traffic may be load-balanced across all available paths. For more information, see Configure BGP Policy, below.
- For dual-CPE deployments, it is recommended that you move the LAN to the VOS branch with the active site-to-site tunnel. For reference, based on default timers, failover will take 15-18 seconds following failure of the primary Site-to-Site tunnel. This can be tuned, if required, by adjusting whichever is the largest timer until the failover time meets the business objective. In the first instance, this is the VRRP timer. For more information, see Configure VRRP at the VOS Branch, below.
- In the configuration examples provided in this article, we build a site-to-site tunnel from each WAN link of the VOS Branch to the VOS VCG. So, if the CPE has one WAN link, there is one site-to-site tunnel, and if there are two WAN links, there are two site-to-site tunnels, one on each WAN link. Alternatively, you can build two or more site-to-site tunnels per WAN link. For example, if the CPE has one WAN link, it can support two site-to-site tunnels. For more information, see Configure Multiple Site-to-Site Tunnels per WAN Link, below.
- By default, only the VOS branch and VOS VCG that are directly connected can pass end user traffic.There are many use cases where you may need to modify this to allow access to or from other Secure SD-WAN sites. For more information, see Advertise Networks between the VOS VCG and the VOS Branch, below.
- An enterprise might want to perform local internet breakout at the VOS branch and central internet breakout (through the SWG) at the VOS VCG to optimize the internet architecture. For more information, see Configure LBO

and CBO through the VOS VCG, below.

- Using Workflow templates, Versa Director automatically creates tunnel virtual interfaces (TVIs) and allocates IP addresses to these tunnel interfaces in the range 169.254.0/24. Two issues may drive the need to modify this default behavior. For more information about how to reconfigure IP addressing information, see Modify the VOS Branch TVI IP Addressing, below.
- MSS adjust is enabled by default, so no further changes are required.

Architecture Caveats

The following are the architecture caveats for configuration guidelines provided in this article:

- You must build site-to-site IPsec tunnels between two devices that both have static IP addresses. IP addresses for VOS VCGs are always statically assigned. However, for customers whose VOS branches are dynamically assigned, this requirement is more problematic. The following are possible alternatives:
  - Register with a dynamic DNS service, and then configure the site-to-site tunnel with an FQDN.
  - Allow VOS branches that use dynamic addresses to use Secure SD-WAN to connect to other VOS branches that use static IP address assignment. Then you configure the site-to-site tunnels to the VOS VCGs on these "transit" VOS branches. Note that for Secure SD-WAN hub-and-spoke topologies, this is the likely model of connectivity.

  For more information, see Advertise Networks between the VOS VCG and the VOS Branch, below.

- VOS VCGs operate in IKE passive mode, and so they never initiate a site-to-site tunnel to the VOS Branch. Instead, the VOS branch must always initiate the IPsec connection. Therefore, do *not* configure the VOS branch in passive mode. Otherwise the IPsec connection is never initiated.
- While it is unlikely, if the WAN IP address of the VOS VCG changes, any allow listing (also called whitelisting) that the customer has enabled on cloud platforms (for example, to avoid two-factor authentication [2FA] for users accessing applications from a trusted source IP address) must be modified. This change may be required because the end users who are accessing the internet via the VOS VCG are NATed to a new public IP address, which the SaaS platform may not consider to be trusted until the customer makes the necessary changes. Customers are notified, via a maintenance request email from the Versa Networks Global Support Center, of any changes to WAN IP addresses of VOS VCGs before the WAN IP addresses change.

Naming Conventions Used in this Section

For the purposes of clarity, the following definitions are used:

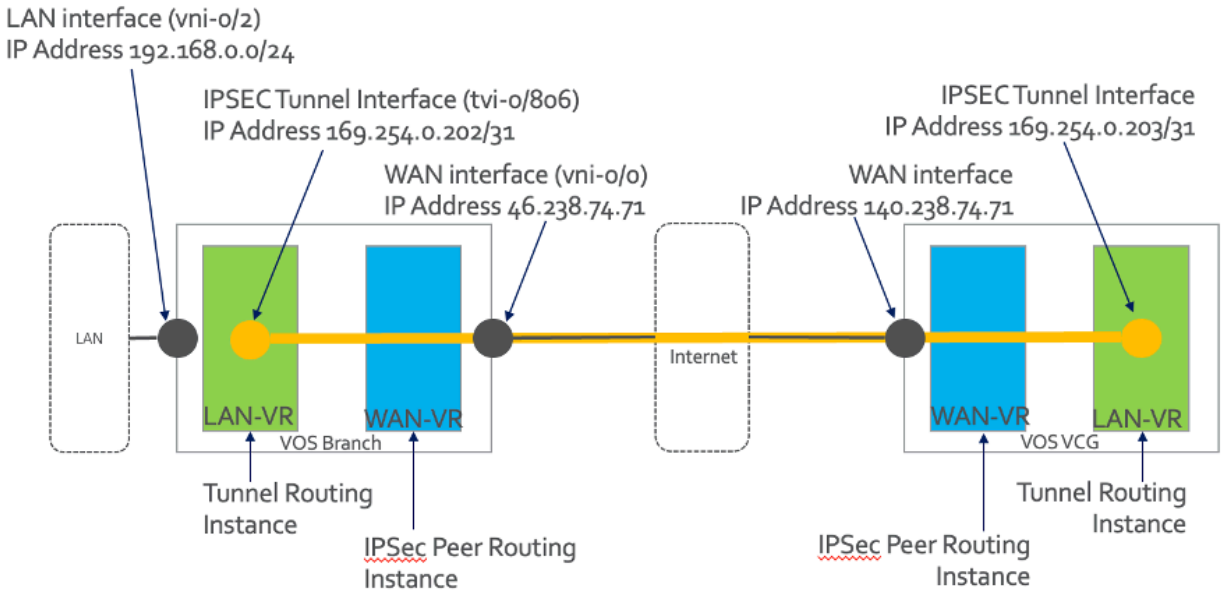
Term	Definition
VOS Branch	Any Versa CPE, including physical devices (such as a Versa CSG 350) and virtual appliances (such as one hosted in Azure). The CPE is hosted and managed by the service provider on behalf of the enterprise or wholly by the enterprise on a separate Versa headend to the VOS VCG.

Term	Definition
VOS VCG (Versa Cloud Gateway)	Any Versa appliance that is hosted and managed by Versa Networks, on behalf of the service provider or enterprise, on a separate headend to the VOS branch.

Configure a Single-CPE, Single-WAN Topology

For the single-CPE, single-WAN configuration, we use the topology shown in Figure 9.

Figure 9: Single-CPE, Single-WAN Deployment



To configure this topology, you perform the following high-level steps:

1. Configure the site-to-site tunnel using Concerto, which controls the VOS VCG shown in Figure 9.
2. Configure the site-to-site tunnel using Versa Director, which controls the VOS branch shown in Figure 9.
3. Verify that the site-to-site tunnel is established between the VOS branch and the VOS VCG.

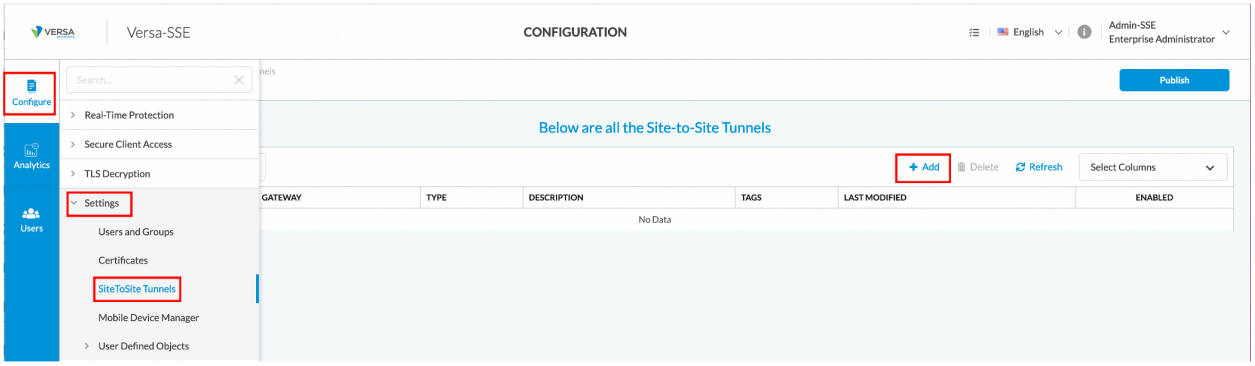
For this configuration example, the following are assumed:

- Static routing is enabled. Note that you can also configure BGP.
- Preshared keys (PSKs) are used between devices. Note that you can also configure certificates.
- Local and peer identity is established using IP addresses, although you can also configure FQDNs and email. The IP identity uses WAN IP addressing.
- IKE is established using AES256-SHA1 encryption and Diffie-Hellman Group 19. Note that you can also configure other transform sets and DH groups.

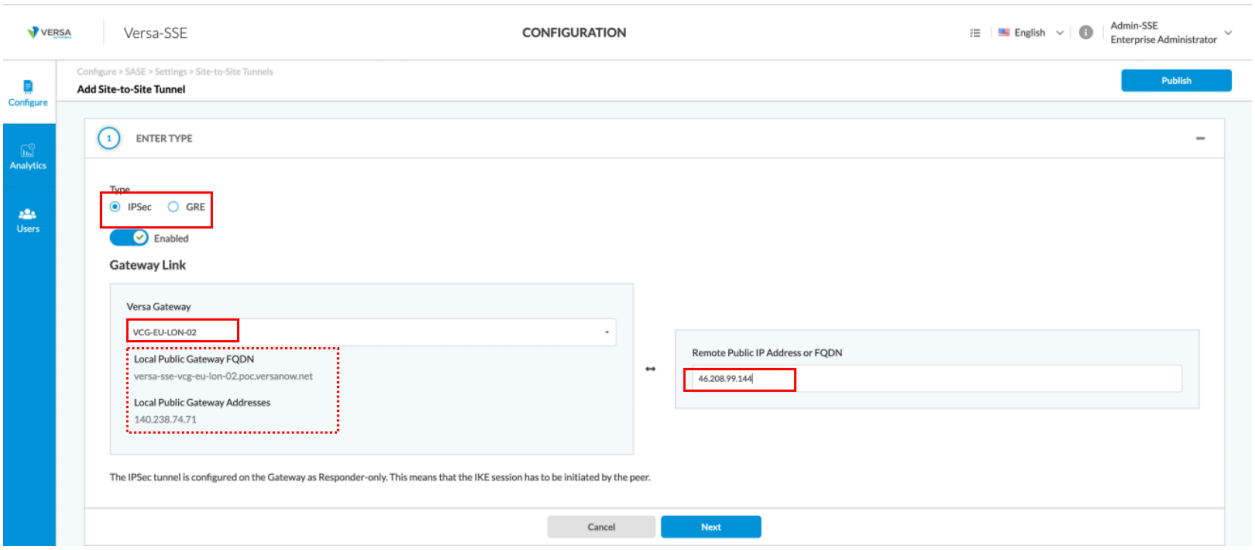
- IPsec is established using ESP-AES256-SHA1 encryption and Diffie-Hellman Group 19. Note that you can also configure other transform sets and DH groups.
- The VOS branch has a single LAN VRF. Note that you can also configure multiple LAN VRFs.
- The VOS VCG and the VOS branch are already built and deployed. The scope of this article is limited to building a site-to-site tunnel between devices.

Configure the VOS VCG Using Versa Concerto

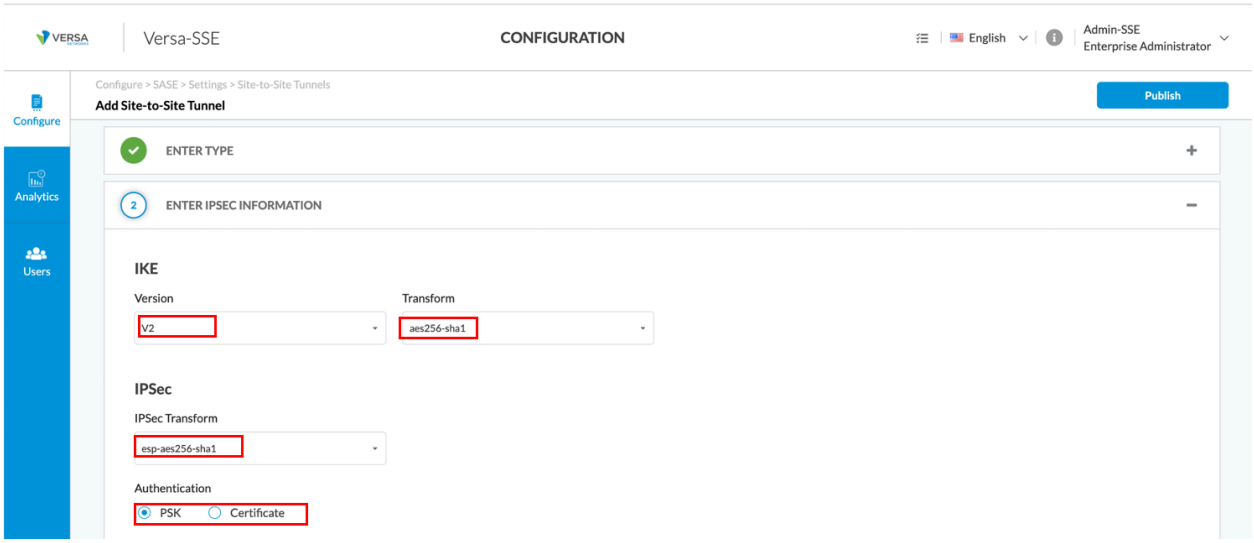
1. Log in to Versa Concerto
2. Select Configure > Settings > Site-To-Site Tunnels, and then click + Add.



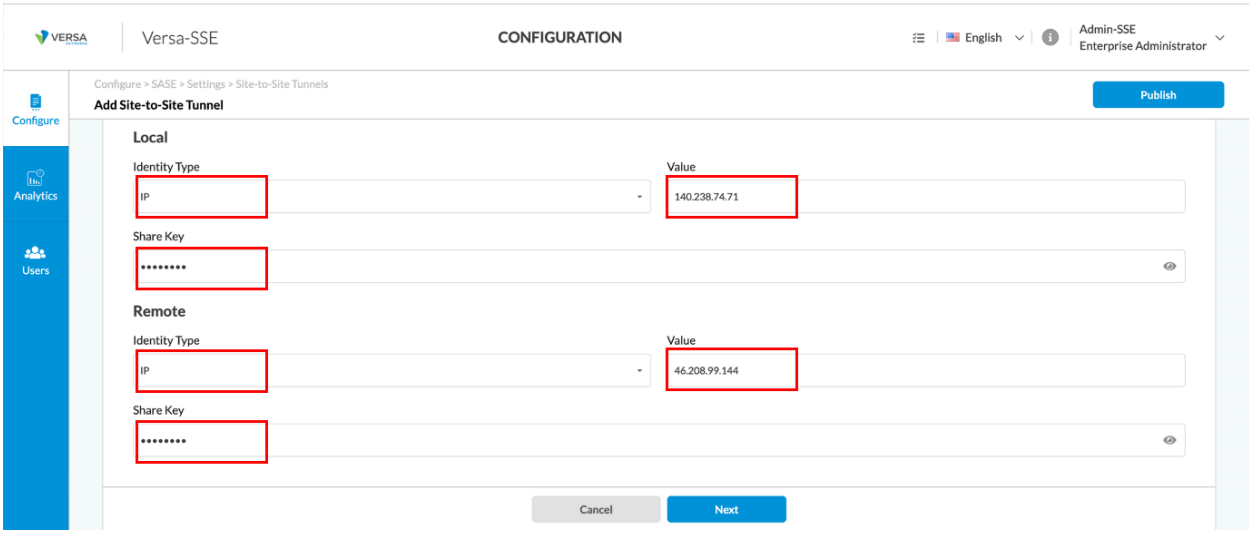
3. Select the VOS VCG that you want to connect to the VOS branch:
   a. In this example, select the Type of Site-To-Site Tunnel as IPsec.
   b. In this example, we select the Europe/London Service Gateway.
   c. After you select the gateway, make a note of the local public gateway address or FQDN, because it is required when you configure the VOS branch and it may be required if you set the local identity is set to IP.
   d. Enter the IP address (or FQDN) of the WAN interface of the VOS branch you want the VOS VCG to connect to. In this example, the IP address is 46.208.99.144.
   e. Click Next.



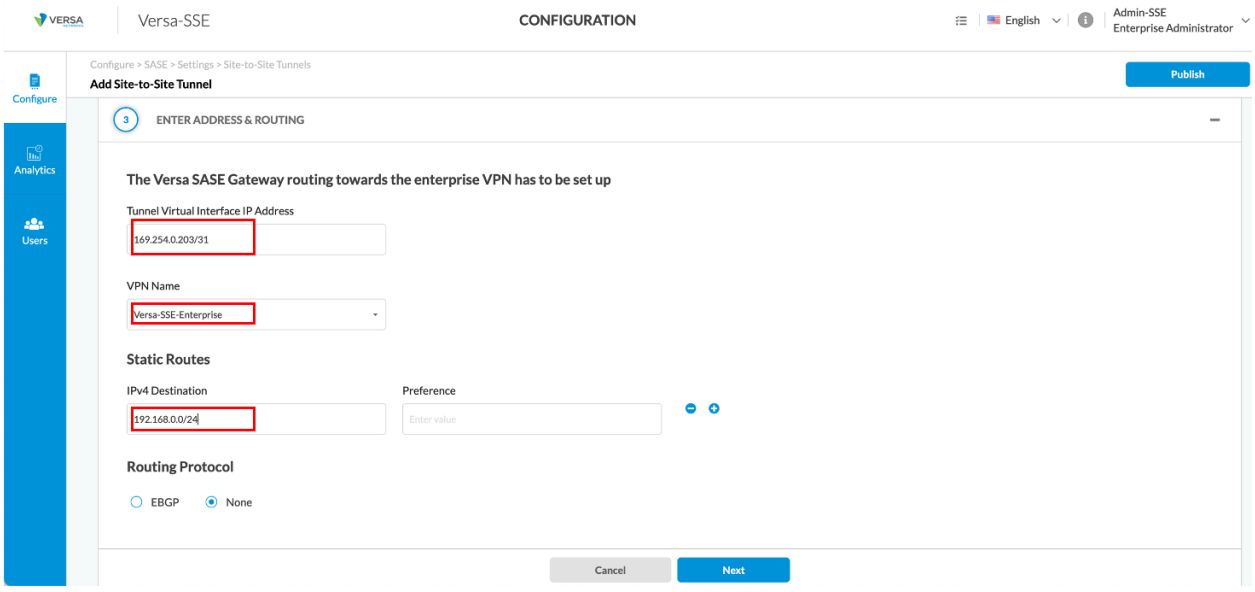
4. Configure the IPsec tunnel information. The following screenshot shows the IKE and IPsec defaults. Modify them as necessary for your deployment.



5. Configure to enter details for the IPsec tunnel.
   a. In this example, we change the local identity type to IP, and we set the value to the IP address of the VOS VCG noted in Step 3c.
   b. In this example, we also set the remote identity type to IP, and we set the value to the WAN IP address of the VOS branch, here, 46.208.99.144. This is the IP address we used in Step 3d.
   c. Make a note of the shared key, because you must also configure it on the VOS branch.
   d. Click Next.



6. Configure the IP addressing information.
    a. In this example, we set the tunnel virtual interface IP address to 169.254.0.203/31. (Note that we will configure the VOS branch as 169.254.0.202/31). This address range resides in the LAN VRF, so it must be globally unique within your organization. Note that when you configure IPsec on the VOS branch, Versa Director automatically assigns 169.254.0.*x* addresses to the IPsec tunnel interface. For information about potential issues and about how to use Workflow templates to modify the IP addressing and static routing configured on Versa Director, see Modify the VOS Branch TVI IP Addressing, below.
    b. Select the correct LAN VPN/VRF name.
    c. This example uses static routes, although BGP is also supported. The VOS branch LAN address space is 192.168.0.0/24. This is configured on the VOS VCG, so its routing table is populated with the remote subnet.
    d. Click Next.

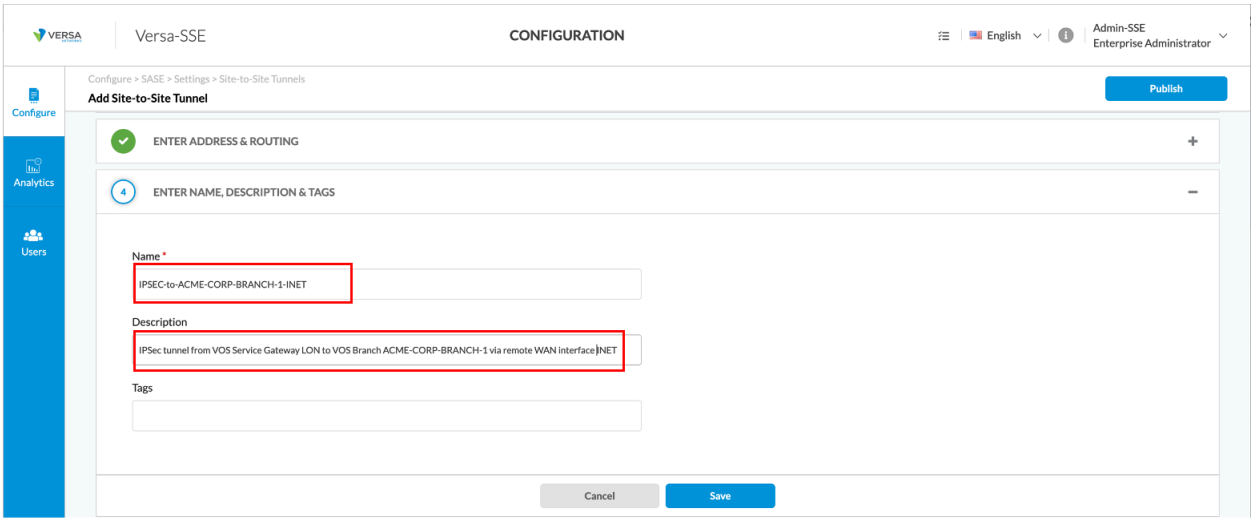


7. Configure name and description information.
    a. Enter a name for the site-to-site configuration that you are creating. This example illustrates one naming

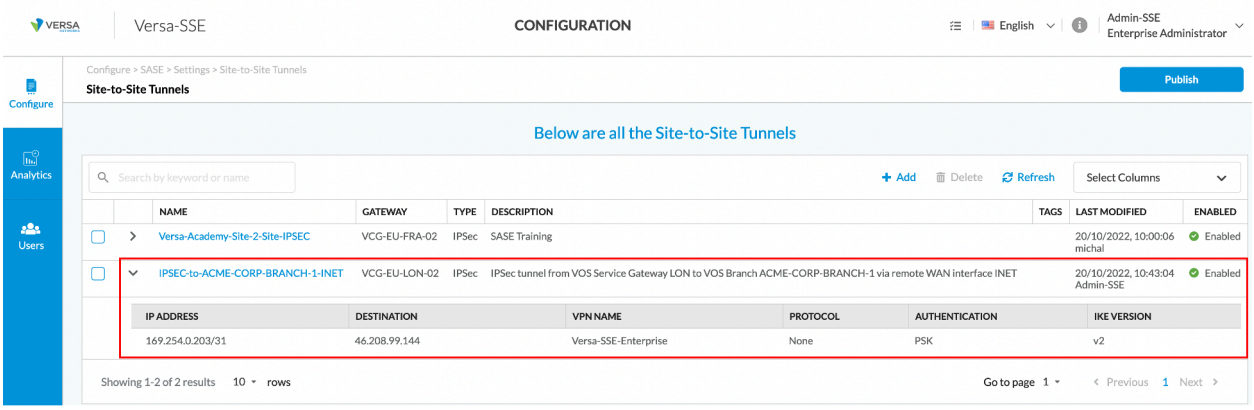
convention, in which the type of tunnel (IPsec), where it connects from (LON), where it connects to (ACME-CORP-BRANCH-1), and the WAN interface used on ACME-CORP-BRANCH-1 (INET) are used to provide a descriptive name for the configuration. You can modify the configuration naming convention as needed.

b. We configure a description for this example.

c. Click Save.



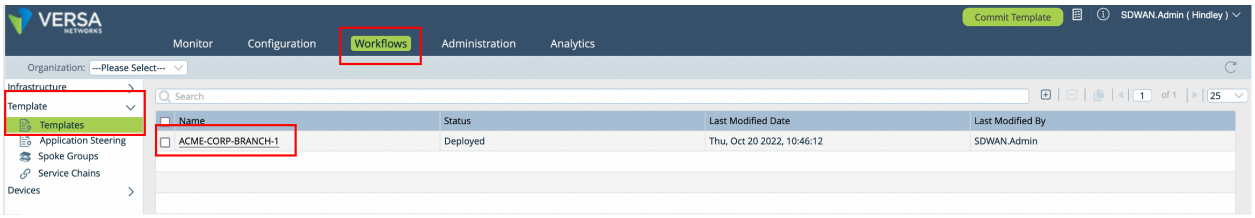
8. A summary of the site-to-site tunnel from the perspective of the VOS VCG displays.



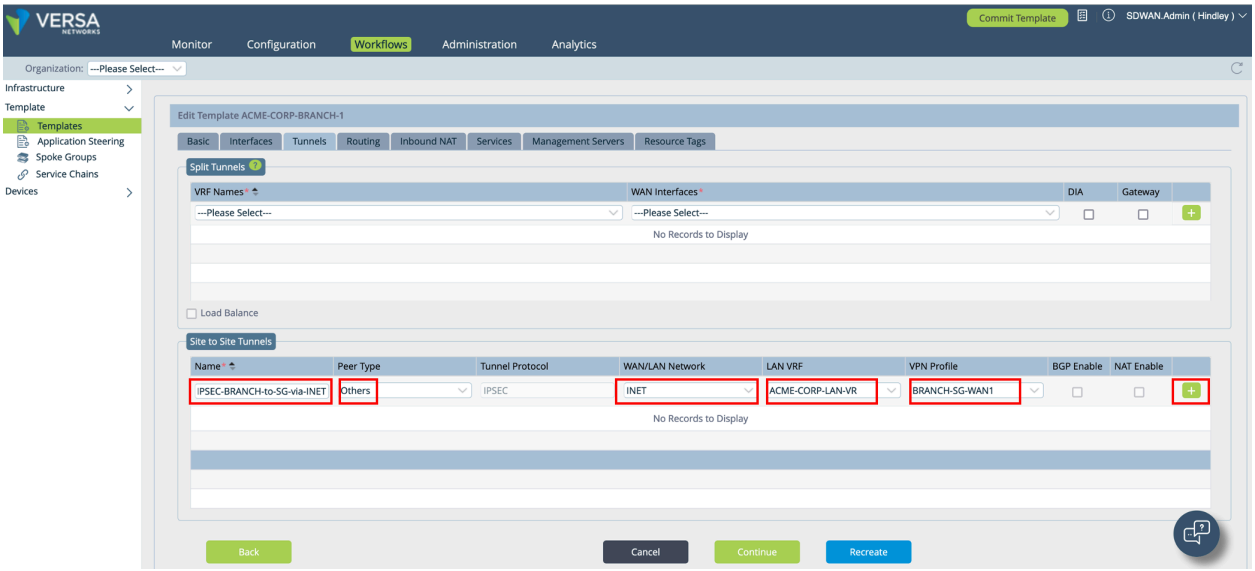
9. Click Publish to push the configuration to the VOS VCG.

Configure the VOS Branch Using Versa Director

1. Log in to Versa Director.
2. Select Workflows > Template > Templates, and then select the template associated with the VOS branch or branches that terminate the IPsec tunnel from the VOS VCG. In this example, the template is ACME-CORP-BRANCH-1.

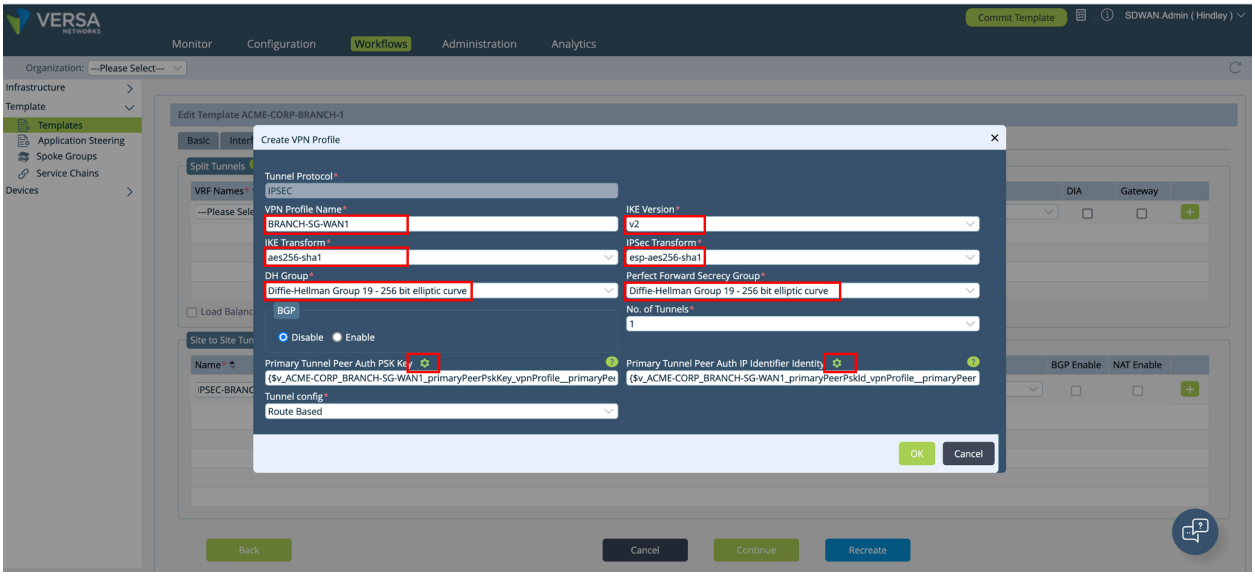


3. Select the Tunnels tab, and then configure the following:
   a. Enter a name. This example illustrates one naming convention, in which the name is composed of the tunnel type (IPsec), the source (branch), the destination (SG – Service Gateway), and the local WAN interface (INET). You can modify the naming convention as needed.
   b. Set the peer type to Others.
   c. The WAN/LAN network is the WAN interface of the VOS branch. In this example, the interface is the network name known as INET.
   d. The LAN VRF is the LAN side VRF of the VOS branch. Typically, end users or devices reside in this VRF.
   e. Select a VPN profile or create one, as described in Step 4.
   f. Click the + icon to add the site-to-site tunnel configuration.



4. A VPN profile is an organization-wide template that you can associate with other VOS branches if required. To configure a VPN profile:
   a. In the VPN Profile Name field, enter a unique name to use to reference the VPN profile.
   b. Configuration the same IPSec parameters as you configured in Steps 3 through 6 in Configure the VOS VCG using Versa Concerto, above, modifying the values as necessary for your deployment.
   c. If the identity of the IPsec tunnel is based on IP address, as is the case in this example, click the ⚙ Parameterize icon to parameterize the values, as shown in the screenshot below. You add the actual IP information later using bind data. Using the ⚙ Parameterize icon creates a variable, which allows you to use the template across multiple devices. If you were to statically assign IP identity information, the template would be specific to a single VOS branch.

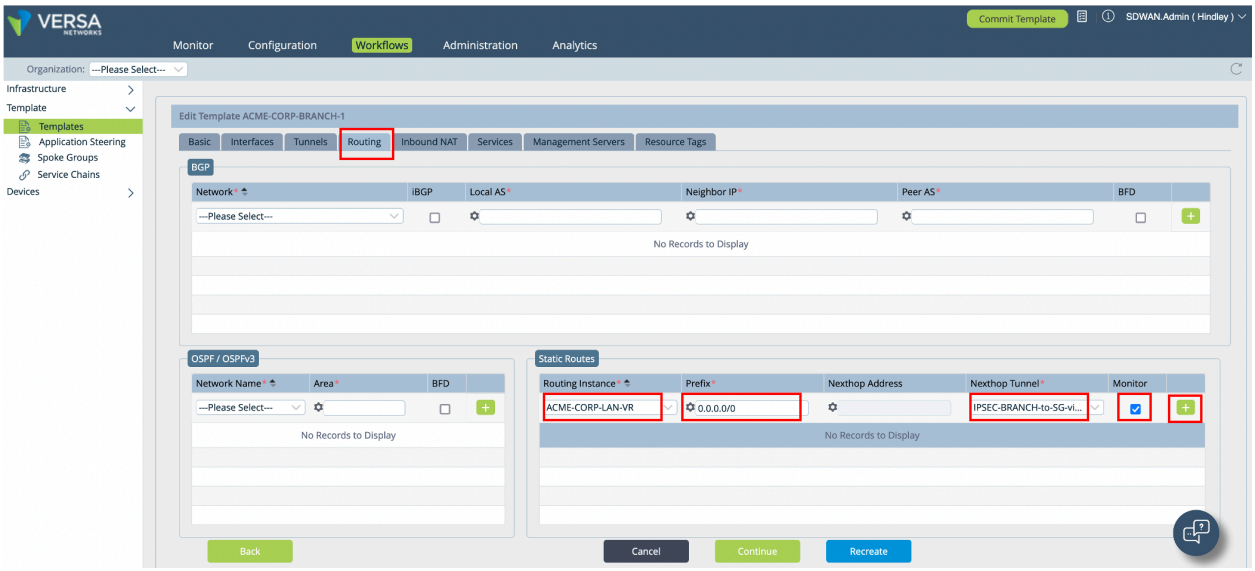
d. Click OK.



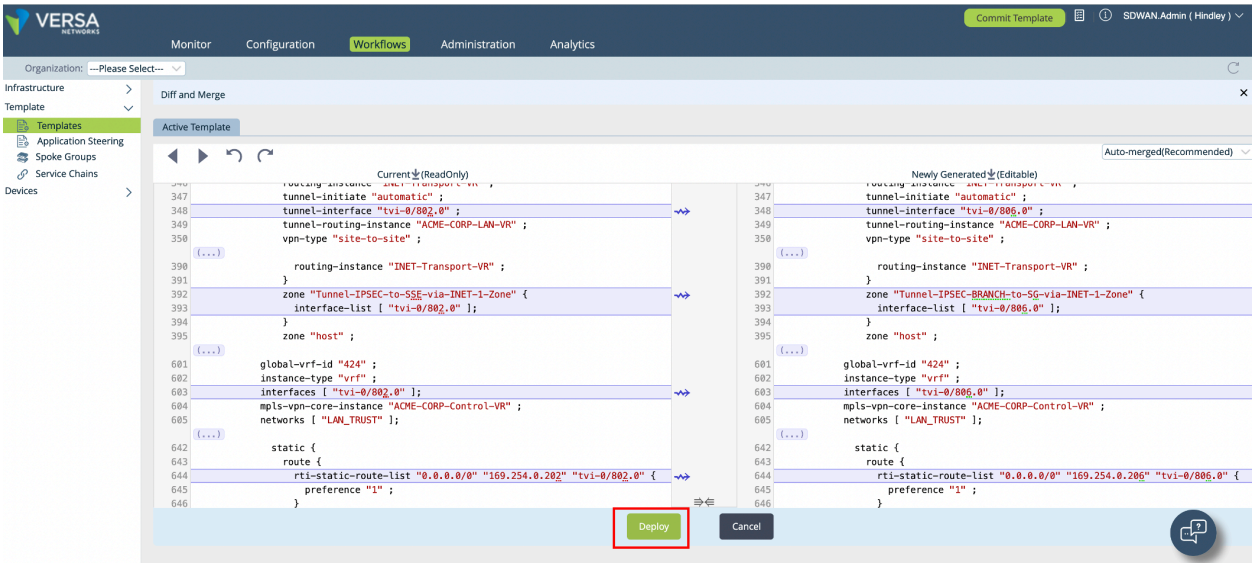
5. Select the Routing tab, and then configure the following:

   a. This example uses static routes (although you can also use BGP). In this example, the VOS VCG is acting as an SWG. Therefore, in these screenshots, we configure the default route of VOS branch with a default route whose next hop is the VOS VCG. Alternatively, if you are integrating VSA clients with Secure SD-WAN, replace the default route with the address space of the VSA clients. Regardless of which routes you configured, they are applied to the VOS branch, so its routing table is populated with the remote subnets hosted by the VOS VCG. Note that to configure additional subnets to the list, click the + Add icon.

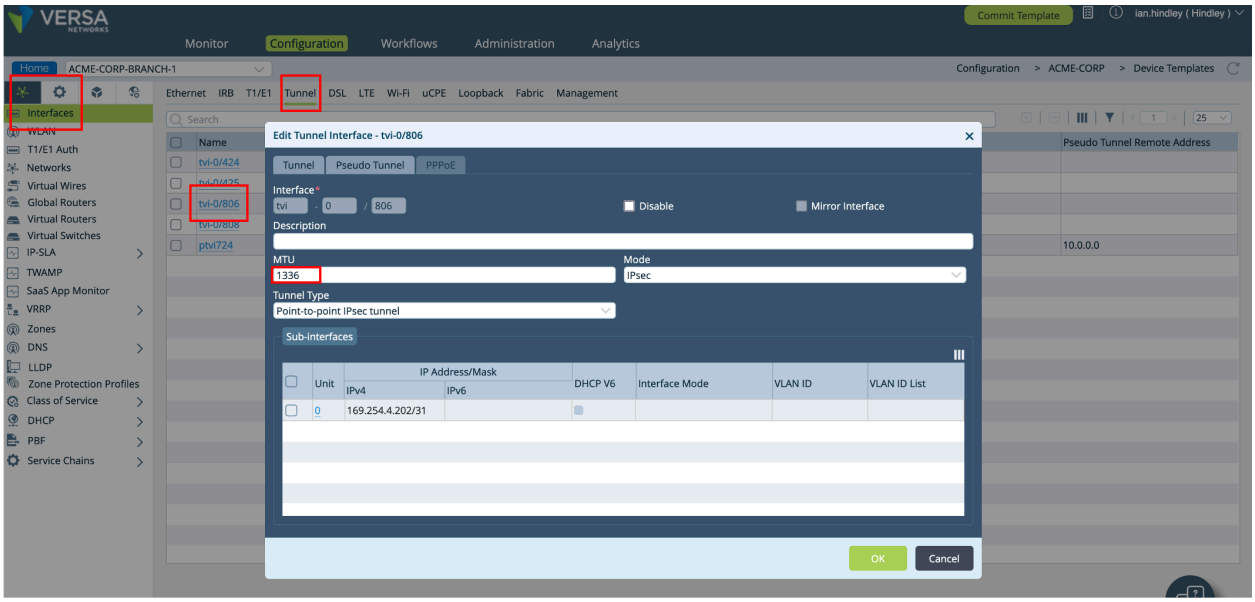
   b. Click Recreate.



6. After sanity-checking the configuration, click Deploy. Deploying updates the device template with configuration associated with the newly configured site-to-site tunnel.

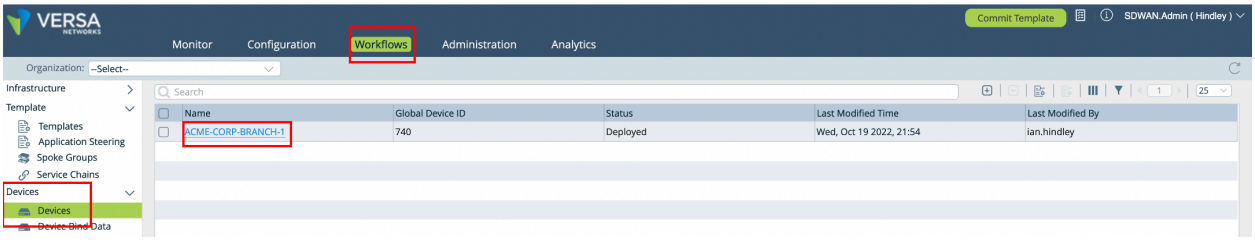


7. From the Device Template, select Networking > Interfaces > Tunnel > tvi-0/*tvi-interface*, and then configure the following:
   a. Set the MTU to 1336, and then click OK. Note that if you experience fragmentation, you may need to modify the MTU.

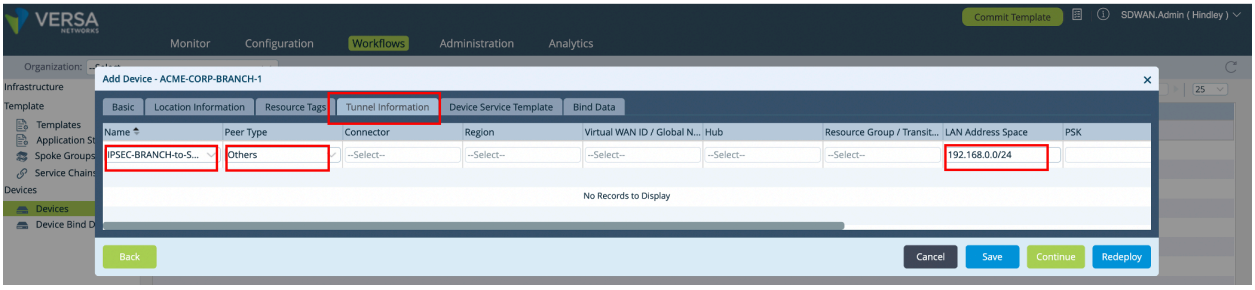


   b. Note that when the VOS branch IPSec configuration is created, Versa Director automatically assigns 169.254.0.*x* addresses to the IPsec tunnel interface. An example is shown in the screenshot above, which shows the address 169.254.0.202/31. To modify the default IP addressing, see Modify VOS Branch TVI IP Addressing, below.

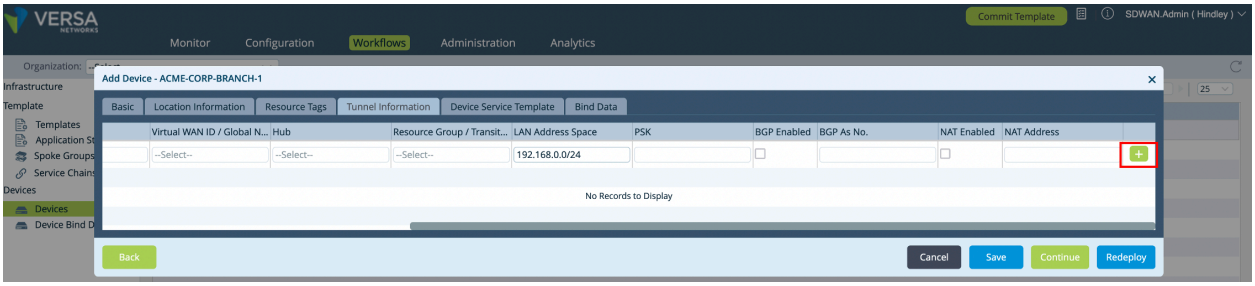
8. Select Workflows > Devices > Devices. Select the VOS branch that terminates the IPsec tunnel from the VOS VCG. In this example, the VOS branch is ACME-CORP-BRANCH-1.



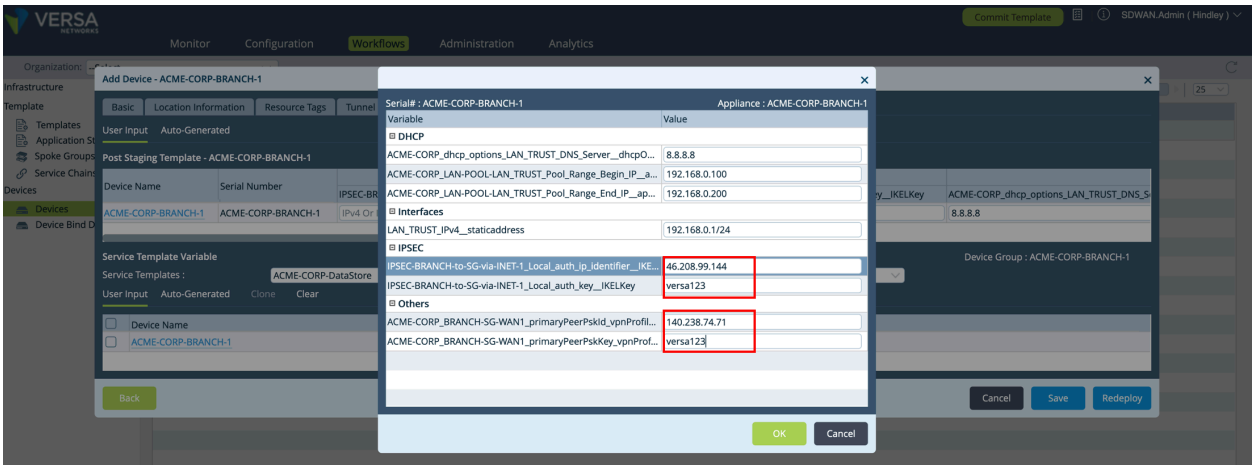
9. Select the Tunnel Information tab, and then enter the following information:
   a. Select the newly created site-to-site tunnel
   b. Select Others.
   c. Enter the LAN VRF address space. In this example, the LAN VRF is configured with the address space 192.168.0.0/24.



10. Click the + Add icon to add the LAN address space. To configure additional LAN address spaces, repeat Step 9.



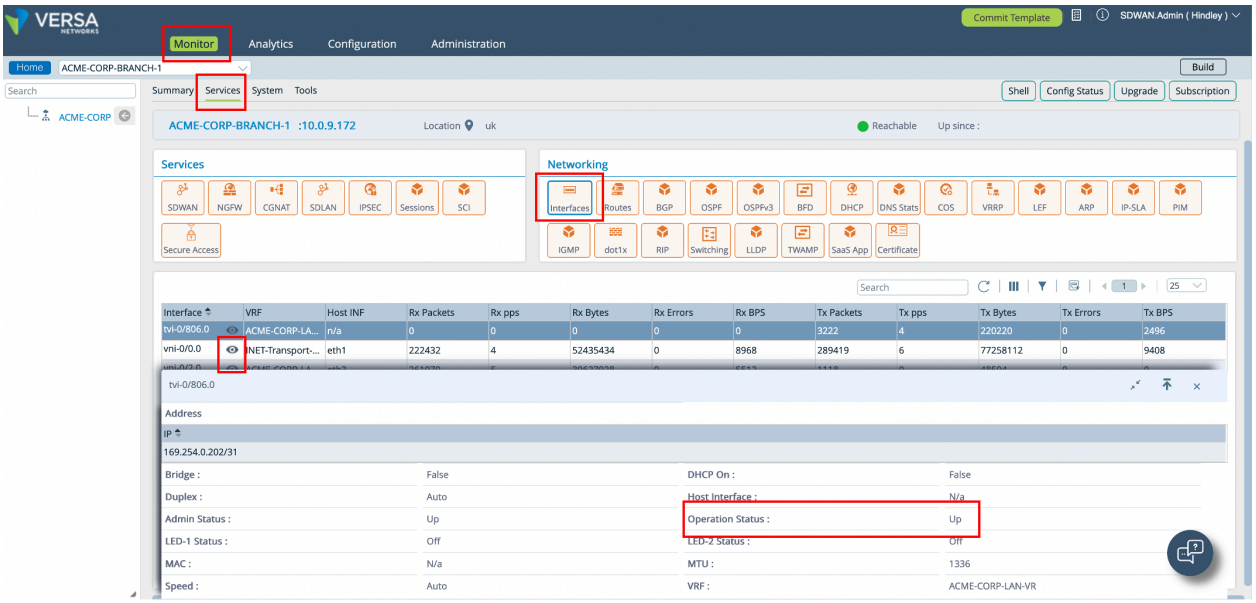
11. Click the Bind Data tab, and configure the following:
   a. Enter values for the following IPsec parameters:
      - Local Authentication IP Identifier—In this example, this is the WAN IP address of the VOS Branch
      - Local Authentication PSK—In this example, we use "versa123". This is the same value that we configured earlier on the VOS VCG
   b. Enter values for the Other parameters:
      - Peer Authentication IP Identifier—In this example, this is the WAN IP address of the VOS Secure Gateway.
      - Peer Authentication PSK—In this example, we use "versa123". This is the same value that we configured earlier on the VOS VCG.
   c. Click OK.
   d. Click Redeploy.



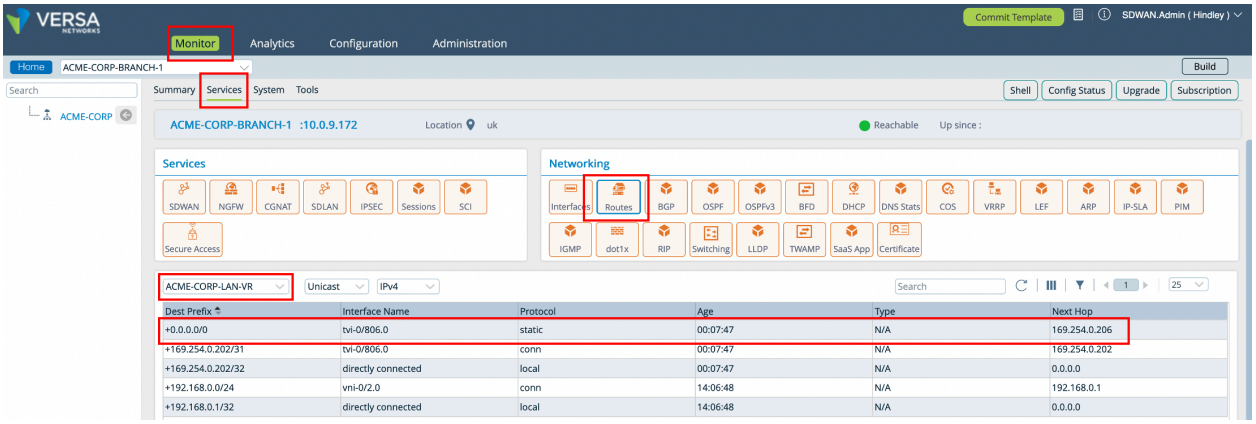
12. To apply the site-to-site configuration to the VOS Branch, follow the normal process to Commit Template.

Verify the Site-to-Site Tunnel

1. On the VOS branch, check that the IPsec tunnel is Up by viewing its Operational Status.

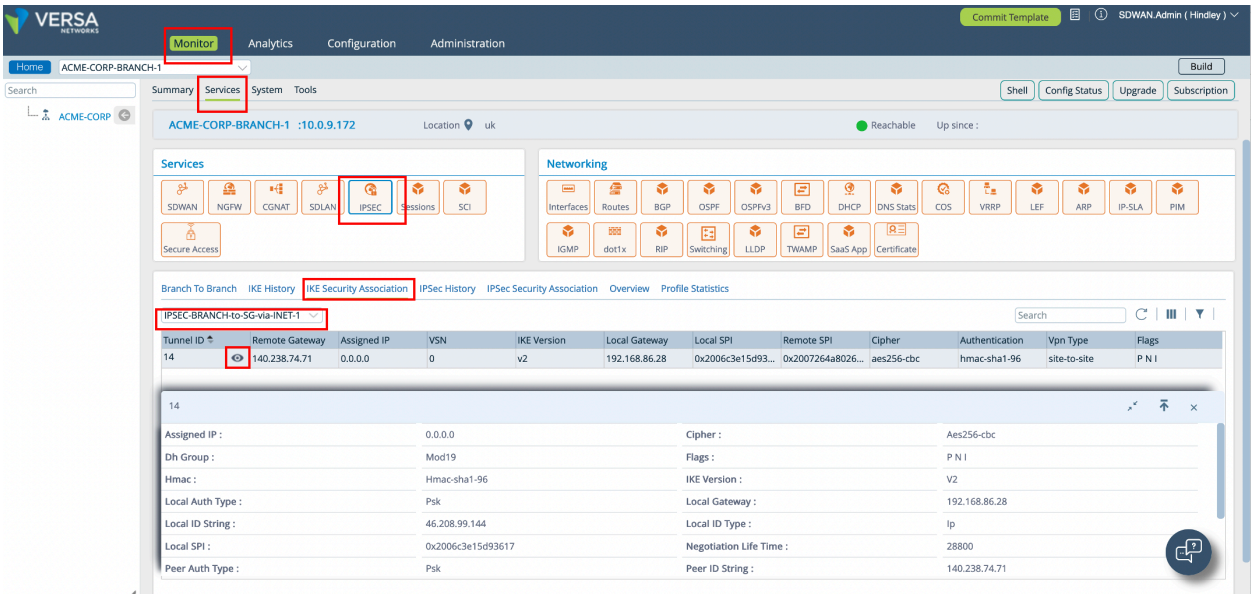


2. If the tunnel interface is operationally Up, check that the route configured on the VOS branch with the VOS VCG as the next hop is installed in the routing table. In this example, a default route is installed with a next hop of the VOS VCG. A + sign to the left of the route indicates that this is the most preferred route.

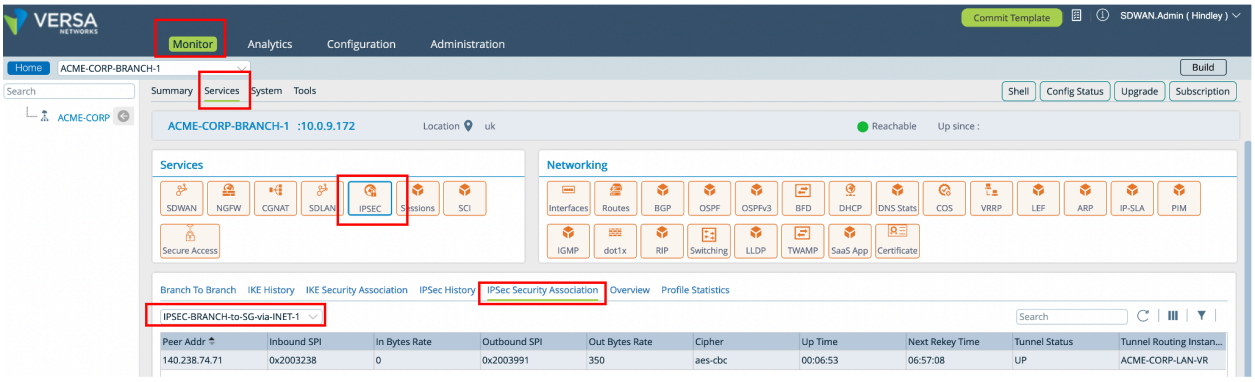


3. If the IPsec tunnel is up, you can view information about the tunnel.

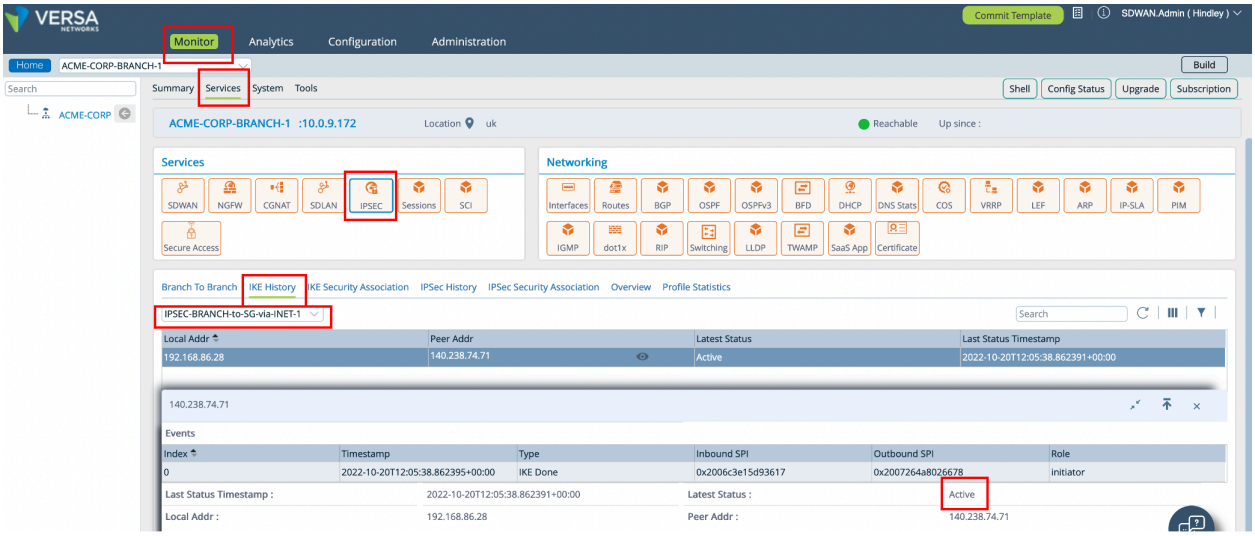
   a. To view Phase 1 (IKE negotiation), select the IKE Security Association tab. Confirm the transform set used for IKE establishment. In this example, we can see that AES256-SHA1 and DH Group 19 are used.



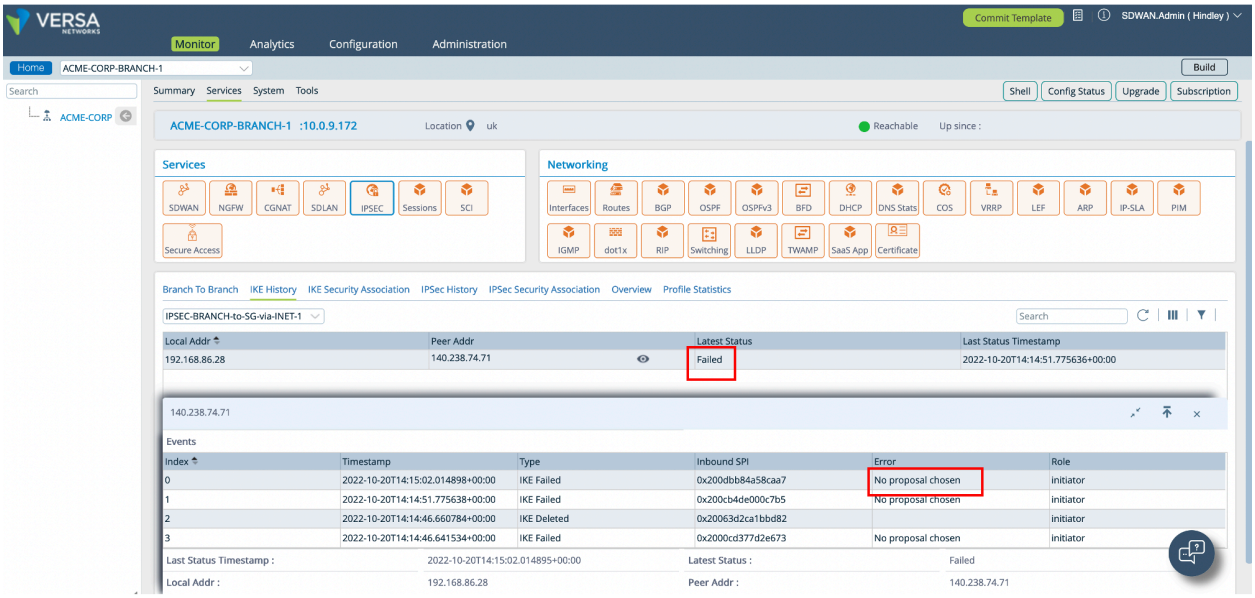
   b. To view Phase 2 (IPsec negotiation), select the IPsec Security Association tab. Confirm the transform set used for IPsec establishment.



4. If the IPsec tunnel does not come up, check whether IKE has been established (Phase 1). If it has been established, check IPsec (Phase 2).
    a. Select the IKE History tab to display a historical view of IKE negotiation between the VOS branch and the VOS VCG.The following screenshot displays what normal should look like. Note the Latest Status is Active.



    b. In contrast, the following screenshot displays when IKE has been misconfigured. Note the Latest Status is Failed. In this case, the specific issue is that Transform Set between the VOS branch and the VOS VCG was not agreed upon (No proposal chosen). In this circumstance, check the configuration of IKE on the VOS branch and on the VOS VCG and ensure that both are configured with the same parameters.

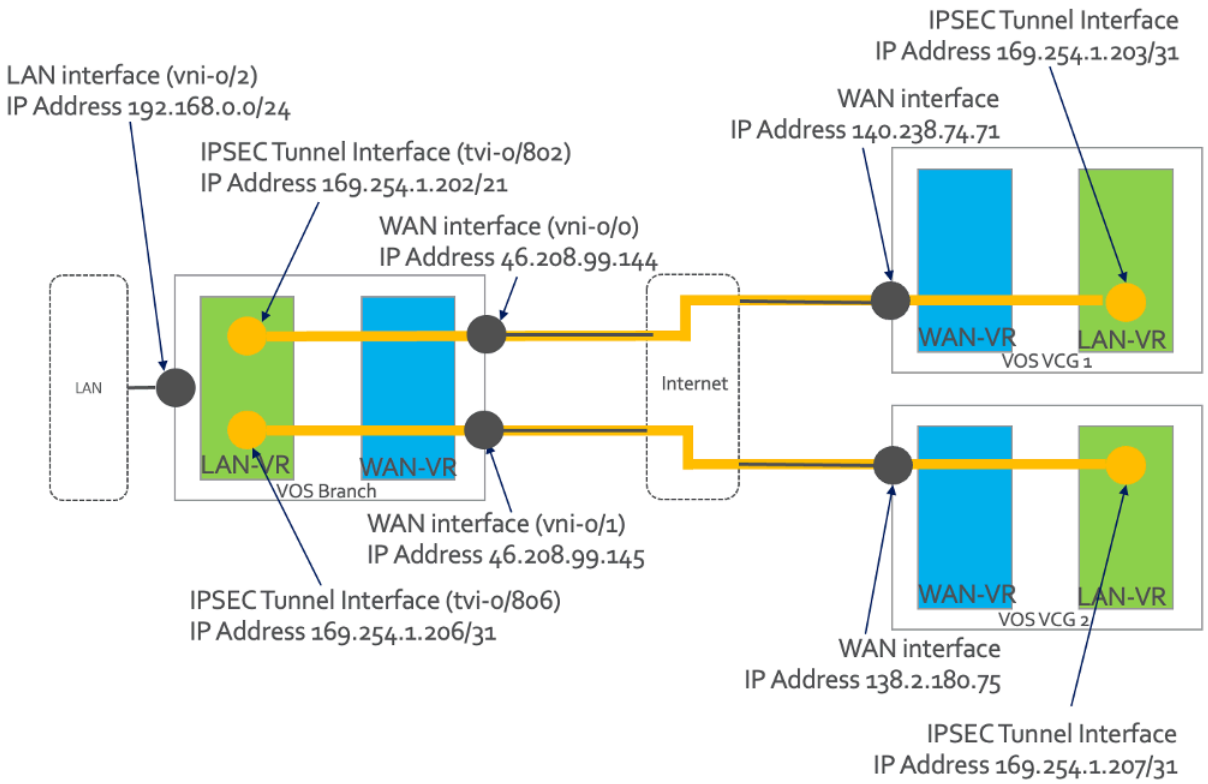


5. For more troubleshooting steps related to IPsec, see Troubleshoot IKE and IPsec.

Configure a Single-CPE, Dual-WAN Topology

For the single-CPE, dual-WAN configuration, we use the topology shown in Figure 10.

Figure 10: Single-CPE, Dual-WAN Deployment



To configure this topology, you perform the following high-level steps:

1. Configure the site-to-site tunnel using Concerto, which controls the VOS VCG shown in Figure 10.
2. Configure the site-to-site tunnel using Versa Director, which controls the VOS branch shown in Figure 10.
3. Verify that the site-to-site tunnel is established between the VOS branch and the VOS VCG.

For this configuration example, the following are assumed:

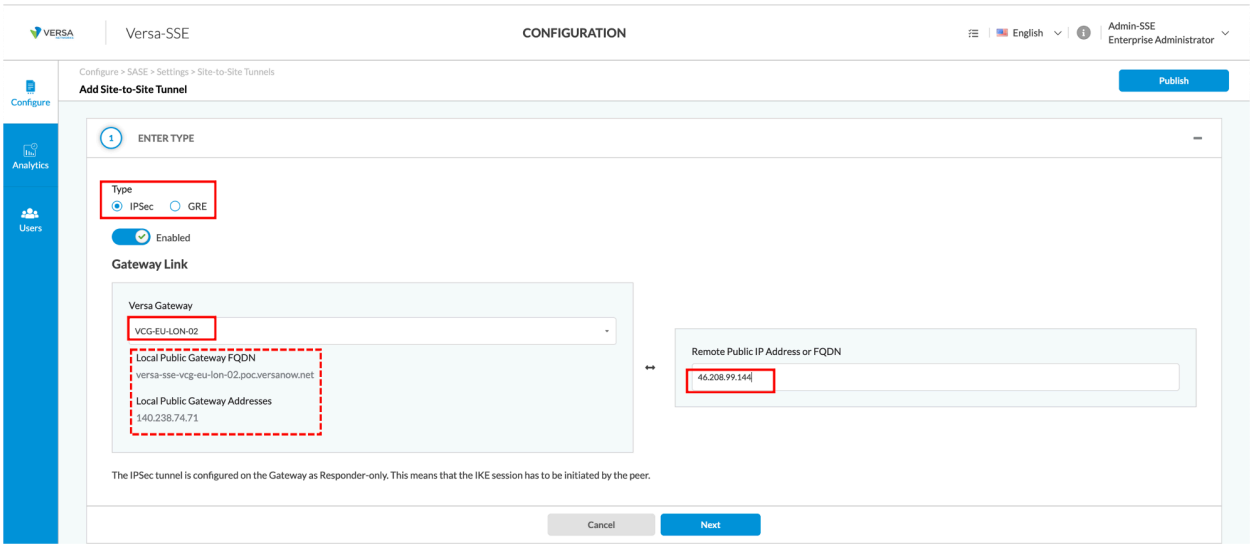
- BGP is enabled. Note that you can also configure static routing.
- Preshared keys (PSKs) are used between devices. Note that you can also configure certificates.
- Local and peer identity is established using IP addresses, although you can also configure FQDNs and email. The IP identity uses WAN IP addressing.
- IKE is established using AES256-SHA1 encryption and Diffie-Hellman Group 19. Note that you can also configure other transform sets and DH groups.
- IPsec is established using ESP-AES256-SHA1 encryption and Diffie-Hellman Group 19. Note that you can also configure other transform sets and DH groups.
- The VOS branch has a single LAN VRF. Note that you can also configure multiple LAN VRFs.

- The VOS VCG and the VOS branch are already built and deployed. The scope of this article is limited to building a site-to-site tunnel between devices.

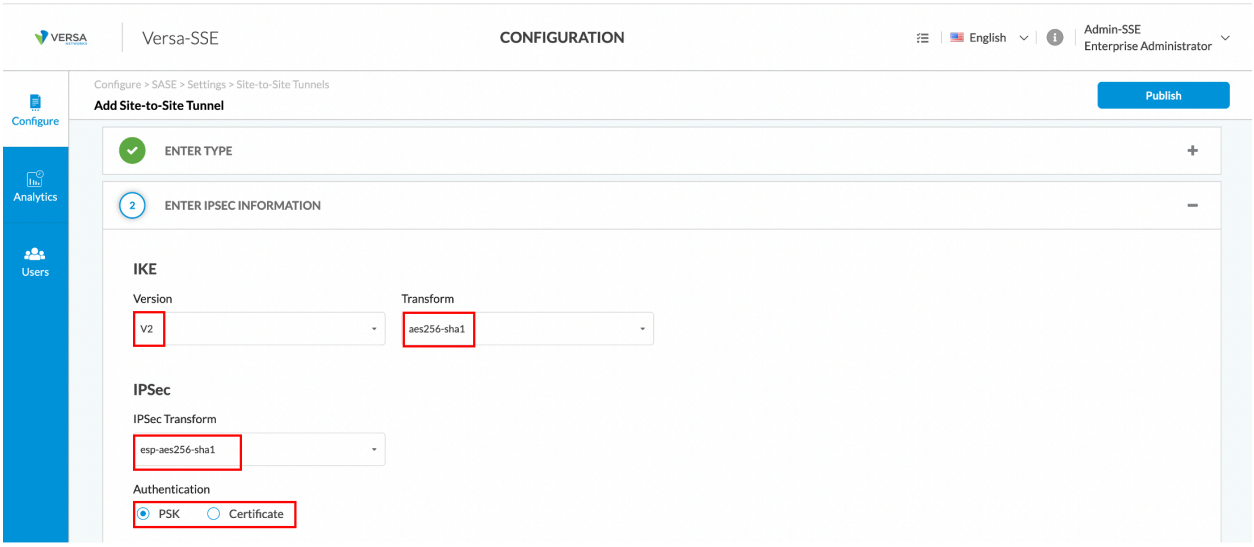
Configure the VOS VCG Using Versa Concerto

1. Log in to Versa Concerto.
2. Select Configure > Settings > Site-To-Site Tunnels, and then click + Add.

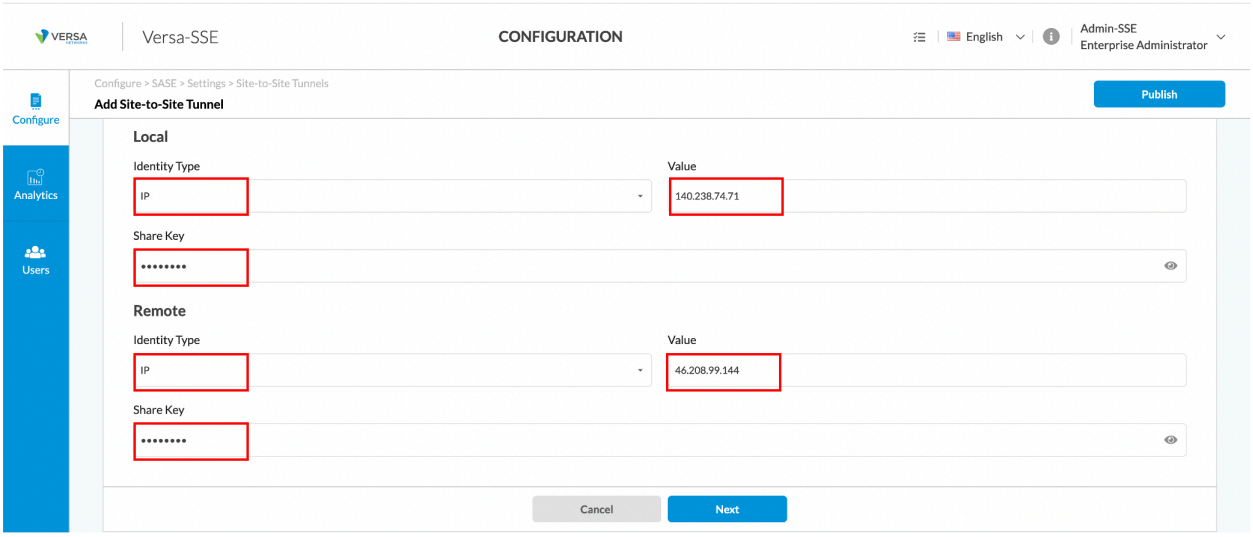
3. Select the VOS VCG you want to connect to the VOS branch. Then configure the following:
   a. In this example, select the Type of Site-To-Site tunnel as IPsec.
   b. In this example, we select the Europe/London Service Gateway.
   c. After you select the gateway, make a note of the local public gateway address or FQDN, because it is required when you configure the VOS branch and it may be required if you set the local identity is set to IP.
   d. Enter the IP address (or FQDN) of the WAN interface of the VOS branch you want the VOS VCG to connect to. In this example, the IP address is 46.208.99.144.
   e. Click Next.



4. Configure the IPsec tunnel information. The following screenshot shows that this example retains the IKE and IPsec defaults. Modify them as necessary for your deployment.



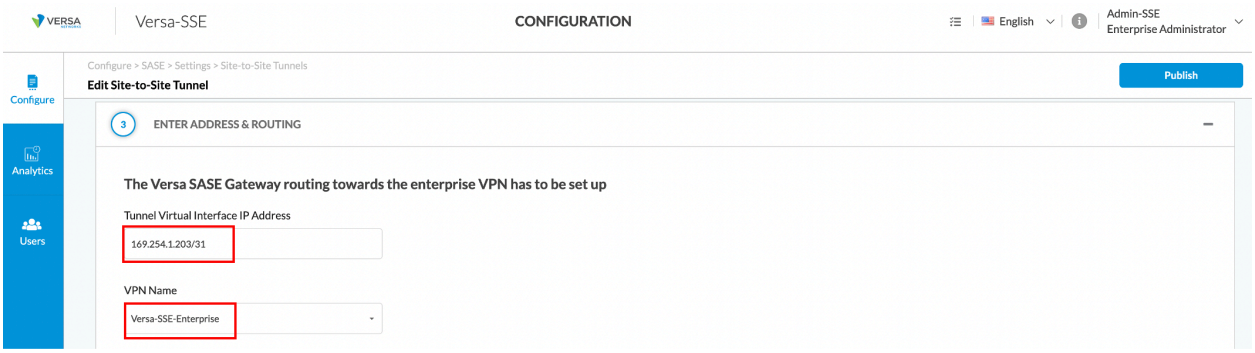
5. Configure additional IPsec tunnel information.
   a. In this example, we change the local identity type to IP, and we set the value to the IP address of the VOS VCG highlighted noted in Step 3c.
   b. In this example, we also set the remote identity type to IP, and we set the value to the WAN IP address of the VOS branch, which, here, is 46.208.99.144, which we also used in Step 3d.
   c. Make a note of the shared key, because you must also configure it on the VOS branch.
   d. Click Next.



6. Configure IP addressing information.
   a. In this example, we set the tunnel virtual interface IP address to 169.254.0.203/31. (Note that we will configure the VOS branch as 169.254.0.202/31). This address range resides in the LAN VRF, so it must be globally unique within your organization. Note that when you configure IPsec on the VOS branch, Versa Director automatically assigns 169.254.0.*x* addresses to the IPsec tunnel interface. For information about potential issues and about how to use Workflow templates to modify the IP addressing and static routing

configured on Versa Director, see Modify the VOS Branch TVI IP Addressing, below.

b. Select the correct LAN VPN/VRF name.



c. This example uses BGP (although static routing is also supported). To configure BGP, enter the following information:

   i. Click EBGP.

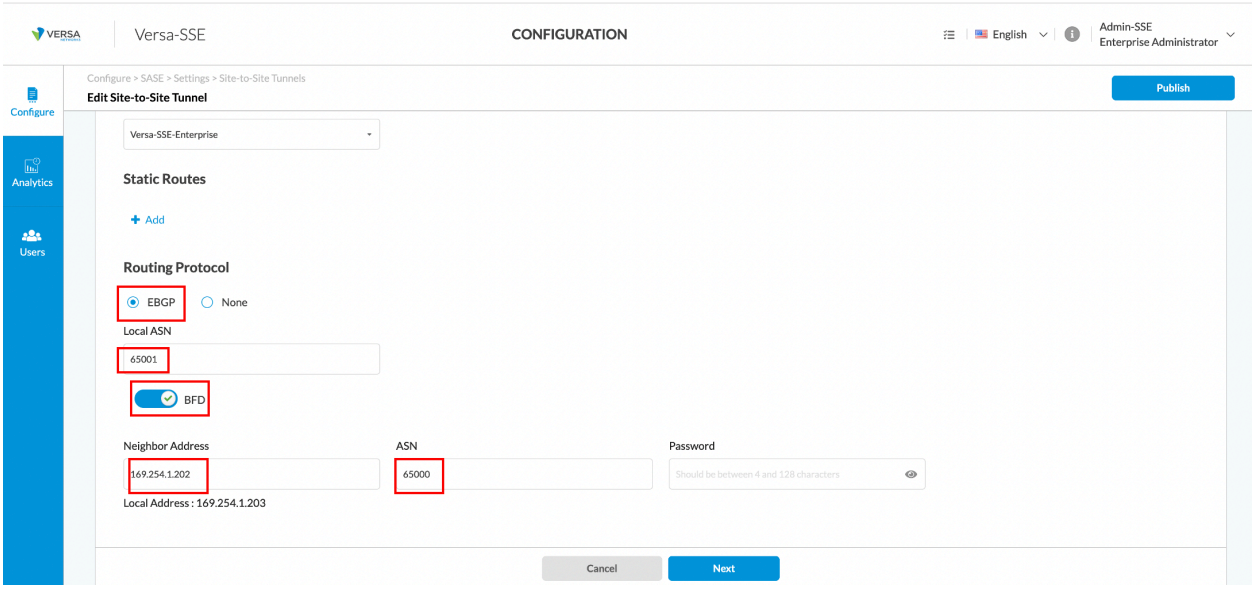
   ii. Enter the local AS number (ASN), which can be whatever number you want to use. In this example, we use 65001 is used. It is recommended that you do not use ASNs 64512, 64513, or 64514 and that you do not any ASNs already in use in your network.

   iii. It is recommended that you enable BFD for faster network failover, because the VOS branch and the VOS VCG are not directly connected.

   iv. For Neighbor Address, enter the tunnel interface of the VOS branch. In this example, it is 169.254.1.202

   v. In the ASN field, enter the ASN of the VOS branch. As with the local ASN, this can be whatever ASN you want to use. In this example, 65000 is used. It is recommended that you do not use ASNs 64512, 64513, or 64514 and that you do not any ASNs already in use in your network.

d. Click Next.

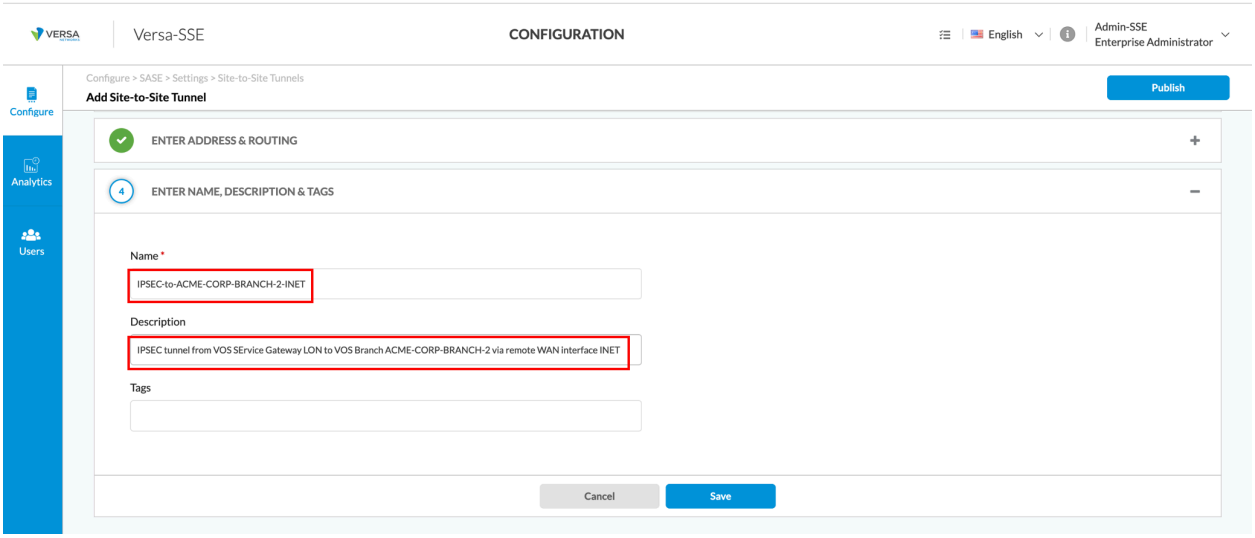


7. Configure name and description information.

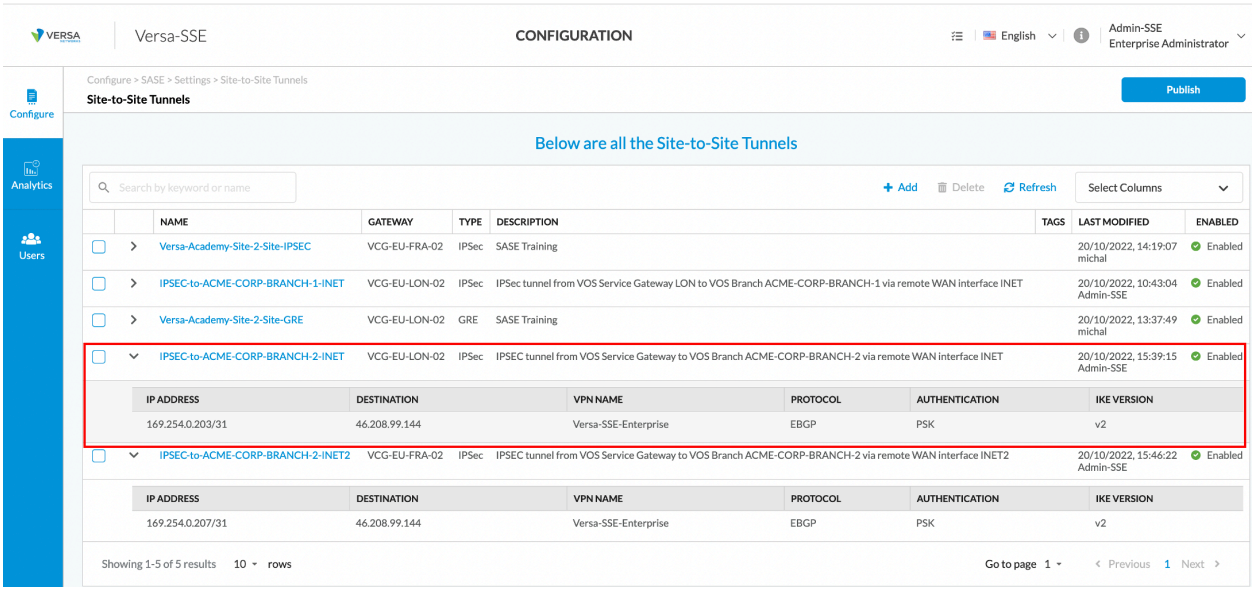
a. Enter a name for the site-to-site configuration that you are creating. This example illustrates one naming convention, in which the type of tunnel (IPsec), where it connects from (LON), where it connects to (ACME-CORP-BRANCH-2), and the WAN interface used on ACME-CORP-BRANCH-2 (INET) are used to provide a descriptive name for the configuration. You can modify the configuration naming convention as needed.

b. We configure a description for this example.

c. Click Save.



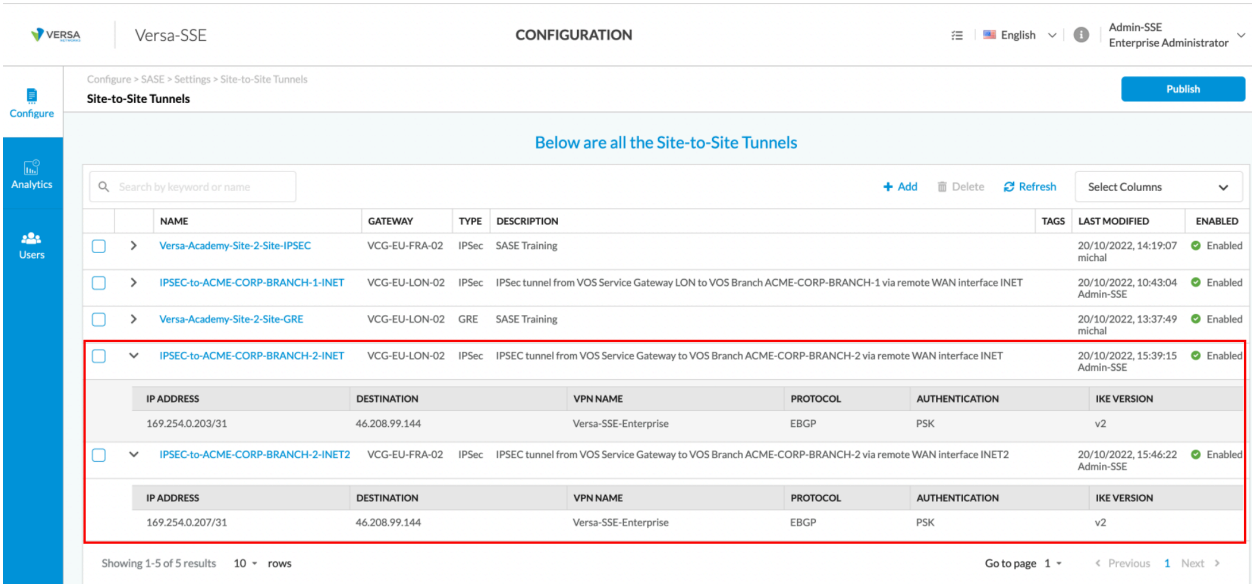
8. A summary of the site-to-site tunnel displays.



9. Repeat Steps 2 through 8 to build the second tunnel to the VOS branch. When you configure the second tunnel, select a different VOS VCG so as to provide geographical redundancy.

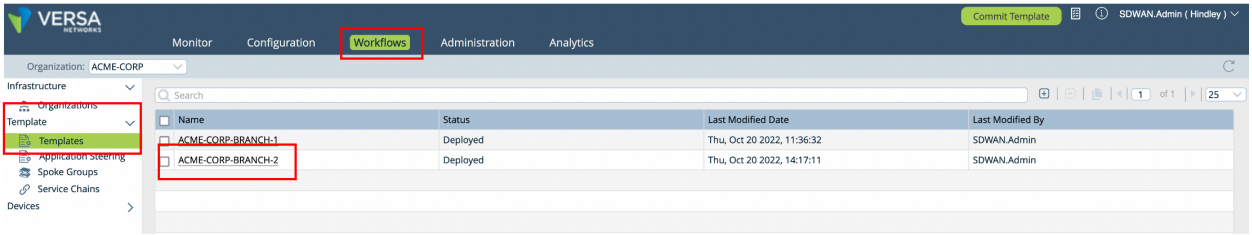
10. A summary of both site-to-site tunnels displays. You see that, in this example, one tunnel is built from the London VOS VCG to the VOS branch and, for geographical resilience of the VOS VCGs, a second tunnel is built between the Frankfurt VOS VCG to the VOS branch. Note that this screenshot shows the same destination address, 46.208.99.144, for both tunnels. In the lab, there is a NAT device between the VOS VCG and the VOS branch.

However, as shown in screenshots from Versa Director shown in the next section, the VOS branch is configured with two WAN interfaces, which are NATed by the upstream device to the same IP address. This is purely cosmetic and should be ignored.



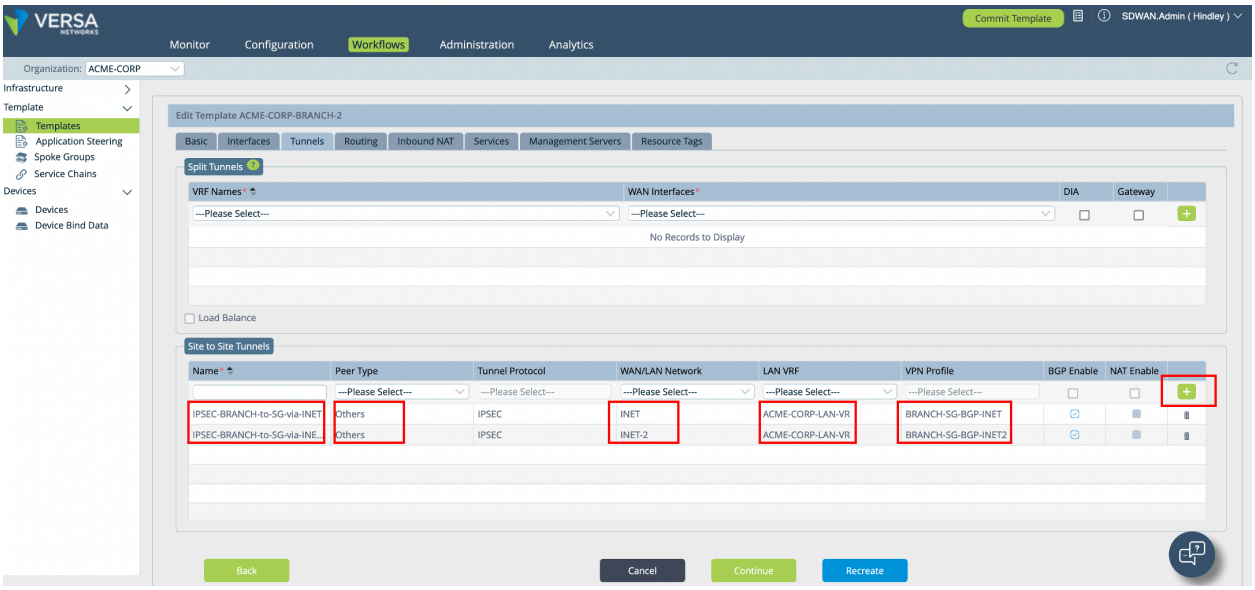
Configure the VOS Branch Using Versa Director

1. Log in to Versa Director.
2. Select Workflows > Template > Templates, and then select the template associated with the VOS branch or branches that terminate the IPsec tunnel from the VOS VCG. In this example, the template is ACME-CORP-BRANCH-2.

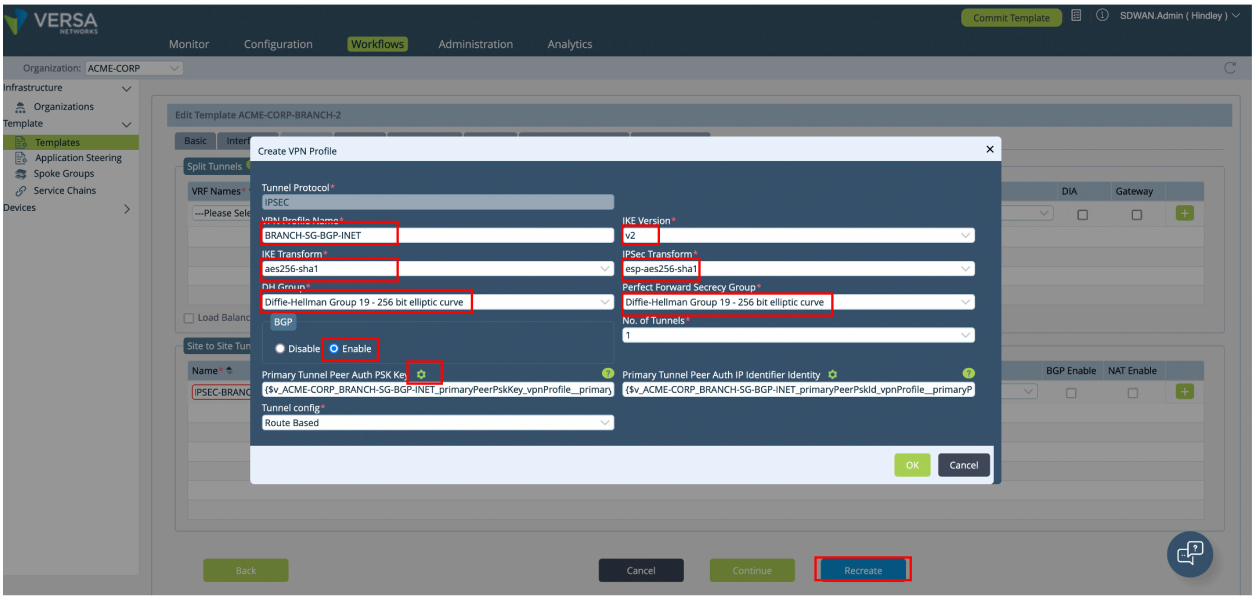


3. Select the Tunnels tab, and then configure the first site-to-site tunnel:
   a. Enter a name. This example illustrates one naming convention, in which the name is composed of the tunnel type (IPsec), the source (branch), the destination (SG – Service Gateway), and the local WAN interface (INET). You can modify the naming convention as needed.
   b. Set the peer type to Others.
   c. The WAN/LAN network is the WAN interface of the VOS branch. In this example, the interface is the network name known as INET.
   d. The LAN VRF is the LAN side VRF of the VOS branch. Typically, end users or devices reside in this VRF.
   e. Select a VPN profile or create one, as described in Step 5.

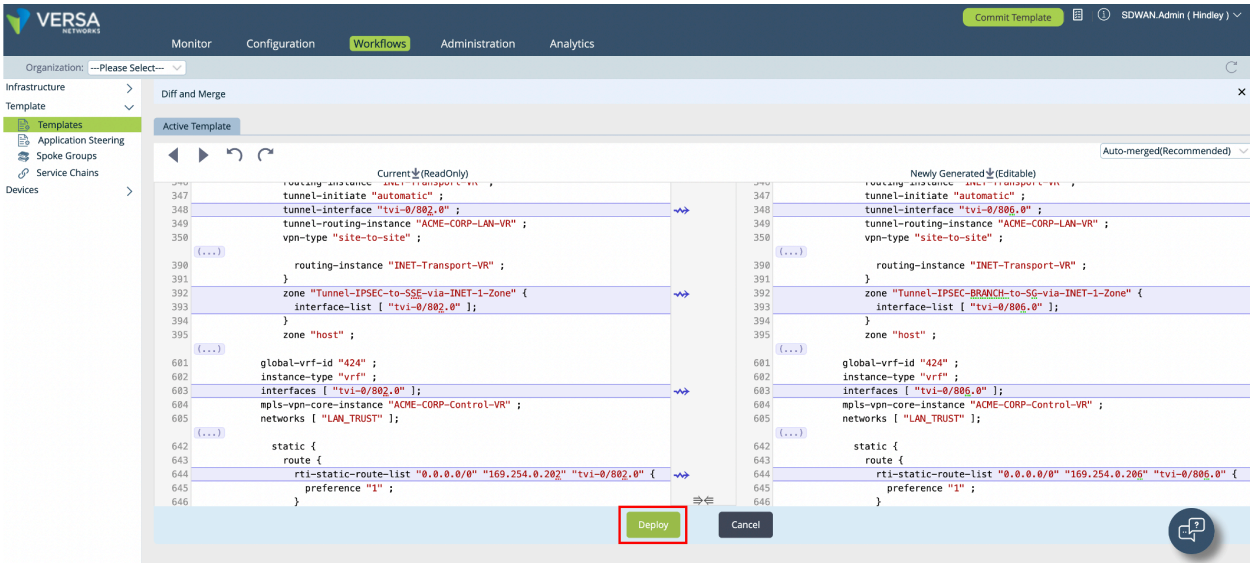
f. Click the + icon to add the site-to-site tunnel configuration.



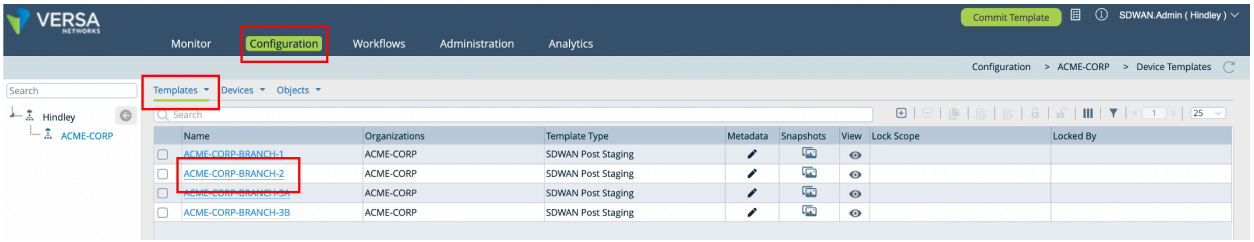
4. Repeat Step 3 to configure the second tunnel. Note the following differences:
   a. In the Name field, enter a different name for the tunnel. In this example, we use INET2 instead of INET in the name.
   b. The WAN/LAN network is the WAN interface of the VOS branch. In this example, the interface is the network name known as INET2.
   c. Create another VPN profile. Do not reuse the one that is already created. This is because the same parameterized variable name is used for both VPN profiles and so you can only add the peer IP address of one of the VOS VCG in bind data.
5. A VPN profile is an organization-wide template that you can associate with other VOS branches if required. To configure a VPN profile:
   a. In the VPN Profile Name field, enter a unique name to use to reference the VPN profile.
   b. Configuration the same IPSec parameters as you configured in Steps 3 through 6 in Configure the VOS VCG using Versa Concerto, above, modifying the values as necessary for your deployment.
   c. Enable BGP.
   d. If the identity of the IPsec tunnel is based on IP address, as is the case in this example, click the ⚙ Parameterize icon to parameterize the values, as shown in the screenshot below. You add the actual IP information later using bind data. Using the ⚙ Parameterize icon creates a variable, which allows you to use the template across multiple devices. If you were to statically assign IP identity information, the template would be specific to a single VOS branch.
   e. Click OK.
   f. Click Recreate.



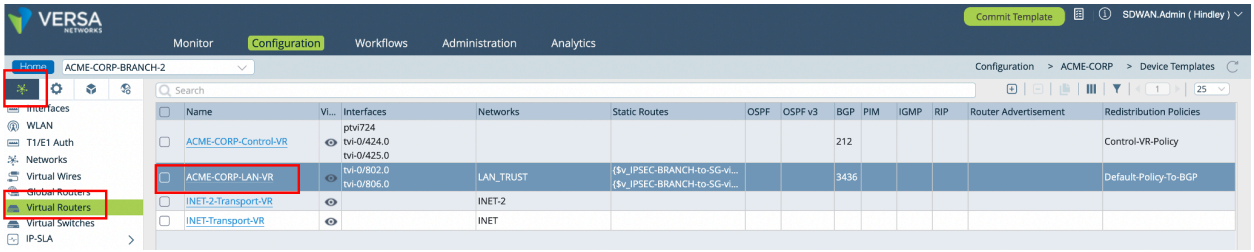
6. After sanity-checking the configuration, click Deploy. Deploying updates the device template with configuration associated with the newly configured site-to-site tunnels.



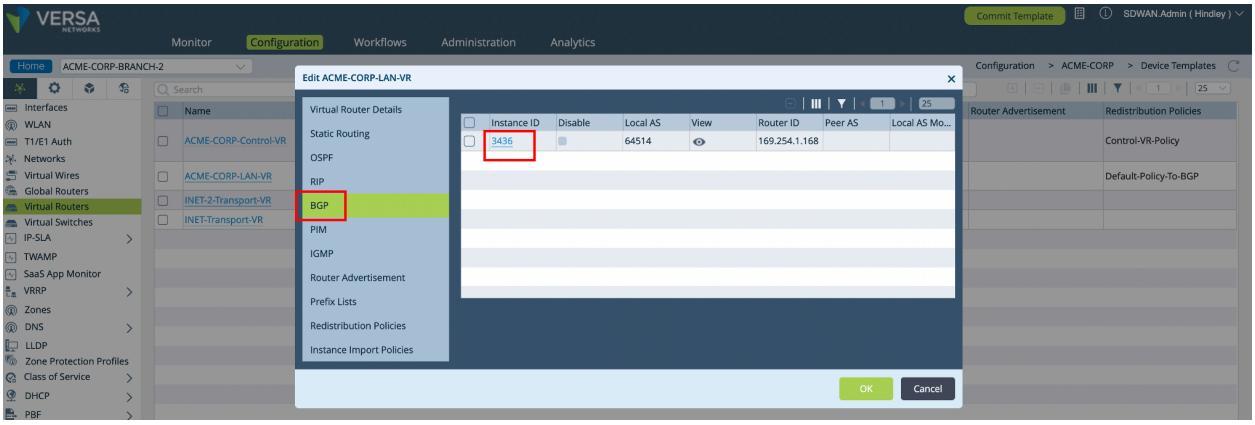
7. Select Configuration > Templates > Device. Select the VOS branch that terminates the IPsec tunnel from the VOS VCG.



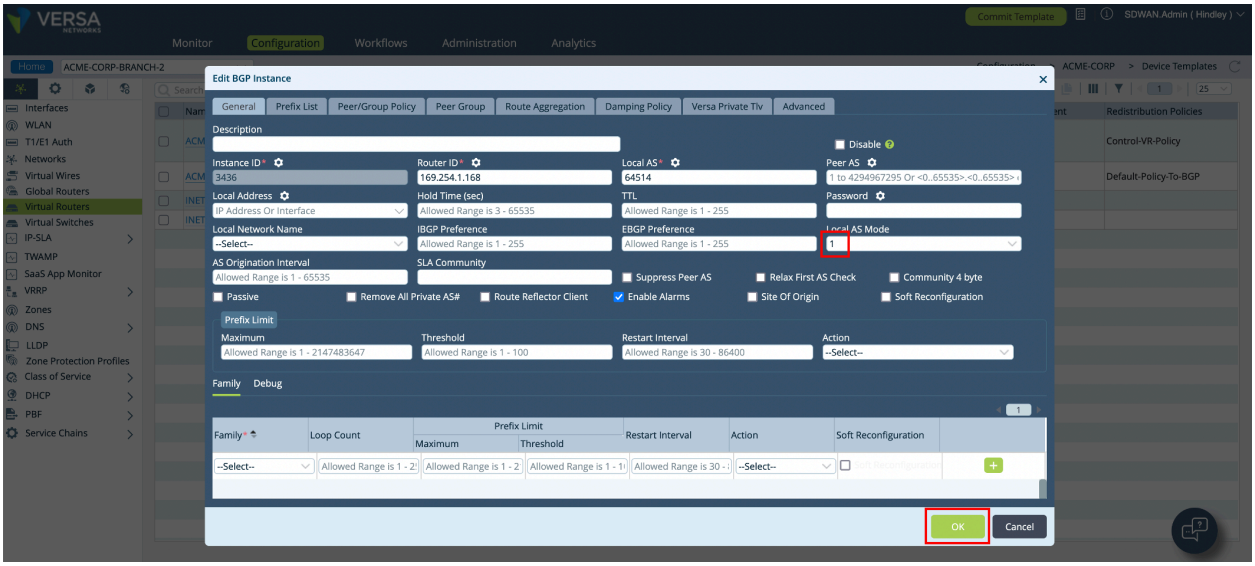
8. Select Networking > Virtual Routers > *organization-name*-LAN-VR. In this example, we select ACME-CORP-LAN-VR.



9. Select BGP > *instance-id*. In this example, the instance ID is 3436.



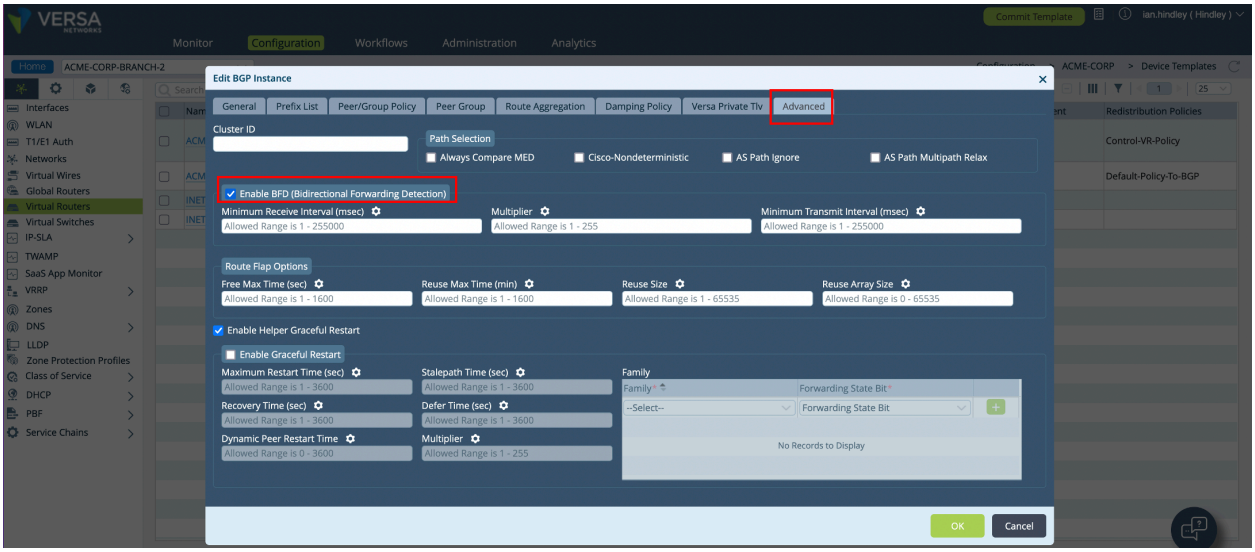
10. Set the local AS mode to 1. Doing this ensures that only the local AS is advertised to the VOS VCG. In this example, we want only 65000 to be prepended to the advertisement. By default, the reserved ASN 64514 is also prepended to the advertisement. The VOS VCG sees its own ASN in the path and rejects the route advertised by the VOS branch. The mode change ensures that 64514 is not prepended to the advertisement.



11. Select the Advanced tab, and configure the following:

a. Click Enable BFD.

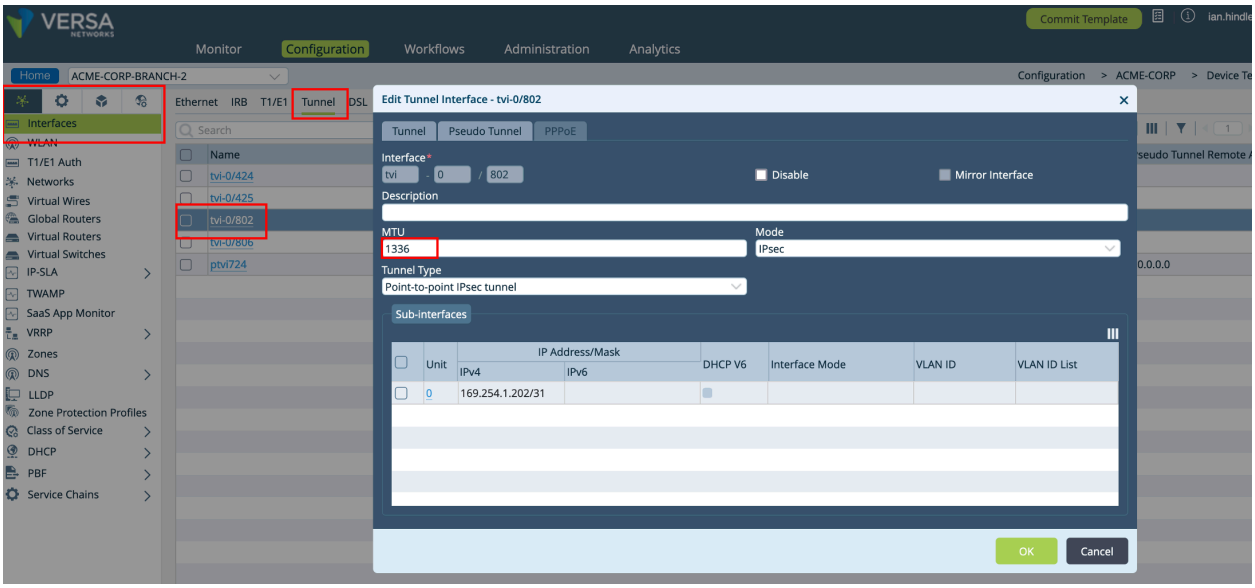
b. If desired, override the default BFD values by populating the fields shown in the following screenshot below. In this example, we accept the defaults (hello interval of 1 second and hello multiplier of 3), so we enter no values.



12. Click OK > OK.

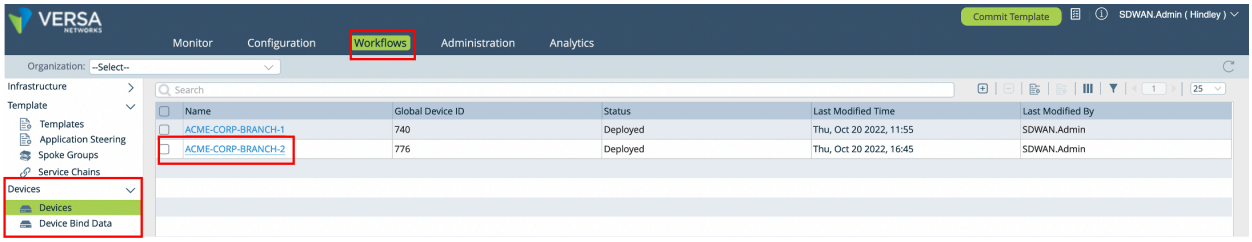
13. Select Networking > Interfaces > Tunnel > tvi-0/*tvi-interface*, and then configure the following.

a. Set the MTU to 1336, and then click OK. Note that if you experience fragmentation, you may need to modify the MTU.

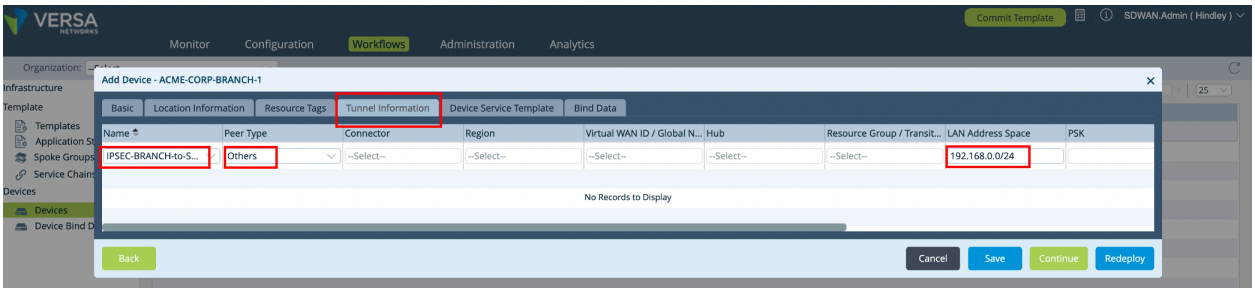


b. Note that when the VOS branch IPSec configuration is created, Versa Director automatically assigns 169.254.0.*x* addresses to the IPsec tunnel interface. An example is shown in the screenshot above, which shows the address 169.254.0.202/31. To modify the default IP addressing, see Modify the VOS Branch TVI IP Addressing, below.

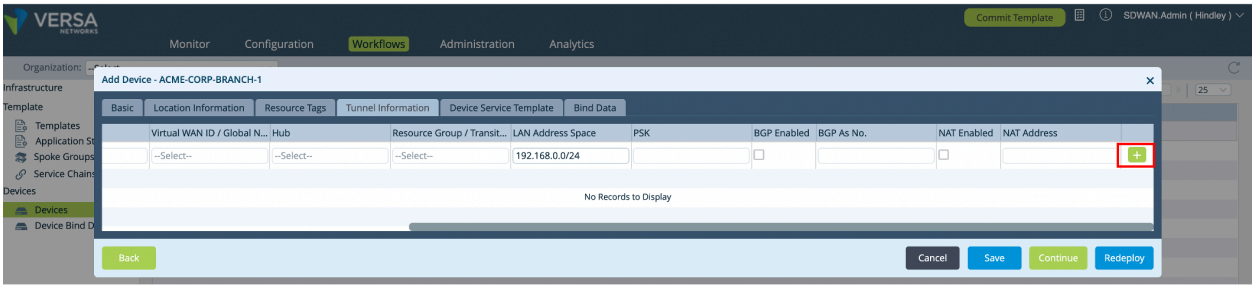
14. Select Workflows > Devices > Devices. Select the VOS branch that terminates the IPsec tunnel from the VOS VCG. In this example, the VOS branch is ACME-CORP-BRANCH-2.



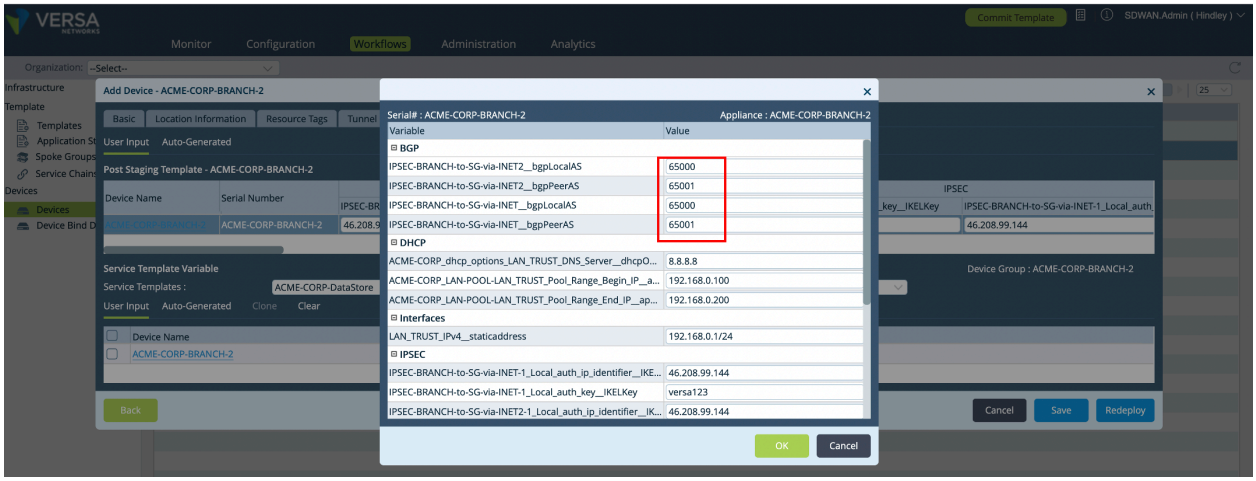
15. Select the Tunnel Information tab, and then enter the following information:
    a. Select the first newly created site-to-site tunnel.
    b. Select Others.
    c. Enter the LAN VRF address space. In this example, the LAN VRF is configured with the address space 192.168.0.0/24.



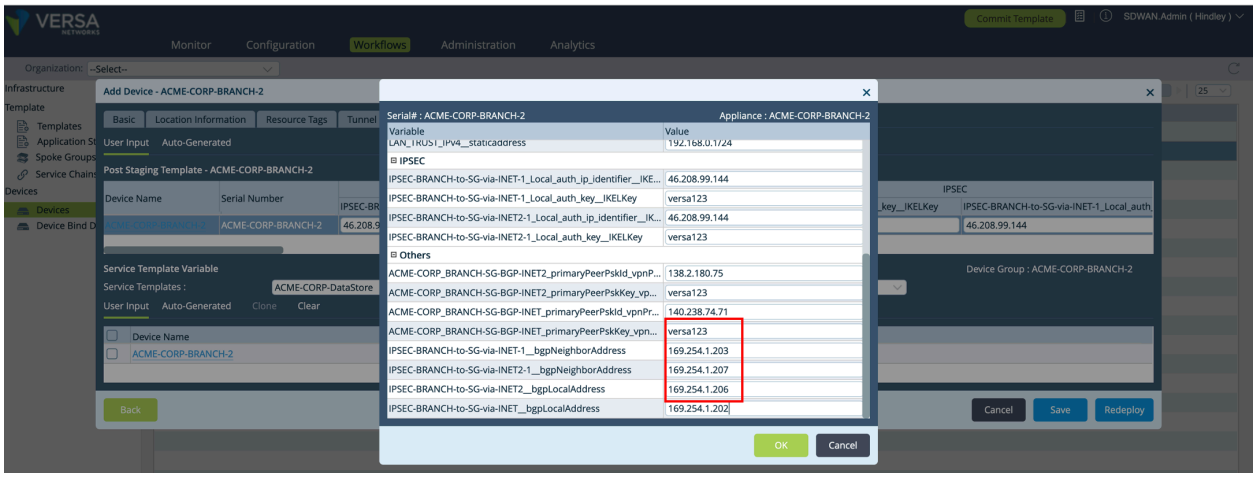
16. Click the + Add icon to add the LAN address space. To configure additional LAN address spaces, repeat Step 15.



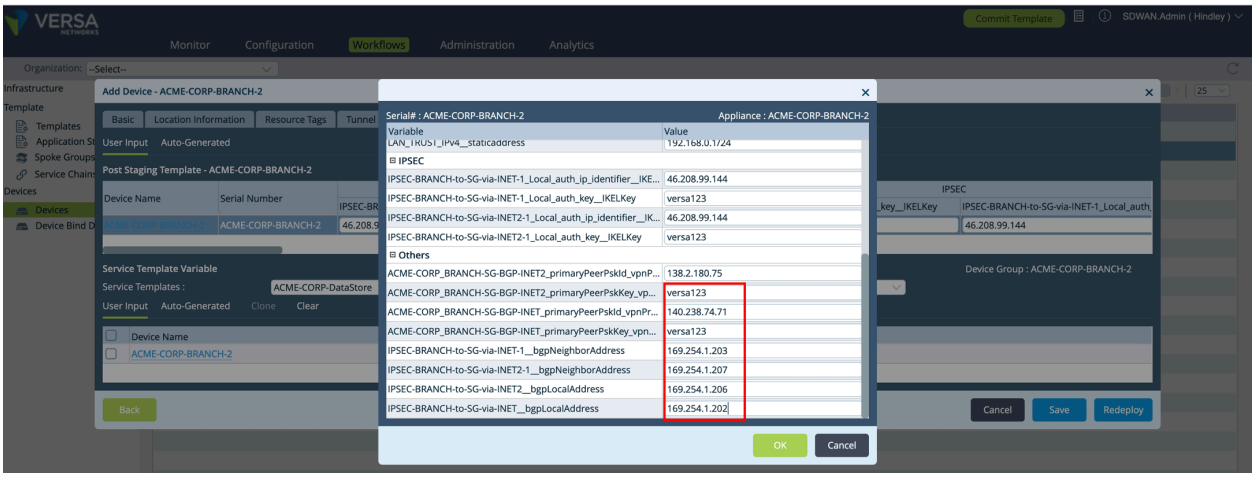
17. Repeat Steps 15 and 16 for the second IPsec tunnel.
18. Click the Bind Data tab, and configure the following:
    a. Enter values for the following BGP parameters:
        - Local AS and Peer AS for the BGP sessions over the IPsec tunnel—Note how this is per IPsec tunnel. In this example, the local ASN is 65000, and the remote ASN residing on the VOS VCGs is 65001.



- BGP Neighbor Address is the VOS VCG BGP peer IP address—In this example, it is also the IP address of the VOS VCG tunnel interface. Therefore, we configure it as either 169.254.1.203 or .207.
- BGP Local Address is the VOS Branch peer IP address—In this example, it is also the IP address of the VOS branch tunnel interface. Therefore, we configure it as either 169.254.1.202 or .206.



b. Enter values for the following IPsec parameters:
   - Local Authentication IP Identifier—In this example, this is the WAN IP address of the VOS branch.
   - Local Authentication PSK—In this example, we use "versa123". This is the same value that we configured earlier on the VOS VCG.
c. Enter values for the Other parameters:
   - Peer Authentication IP Identifier—In this example, this is the WAN IP address of the VOS VCG.
   - Peer Authentication PSK—In this example, we use "versa123". This is the same value that we configured earlier on the VOS VCG.
d. Click OK.
e. Click Redeploy.



19. To apply the site-to-site configuration to the VOS branch, follow the normal process to Commit Template.

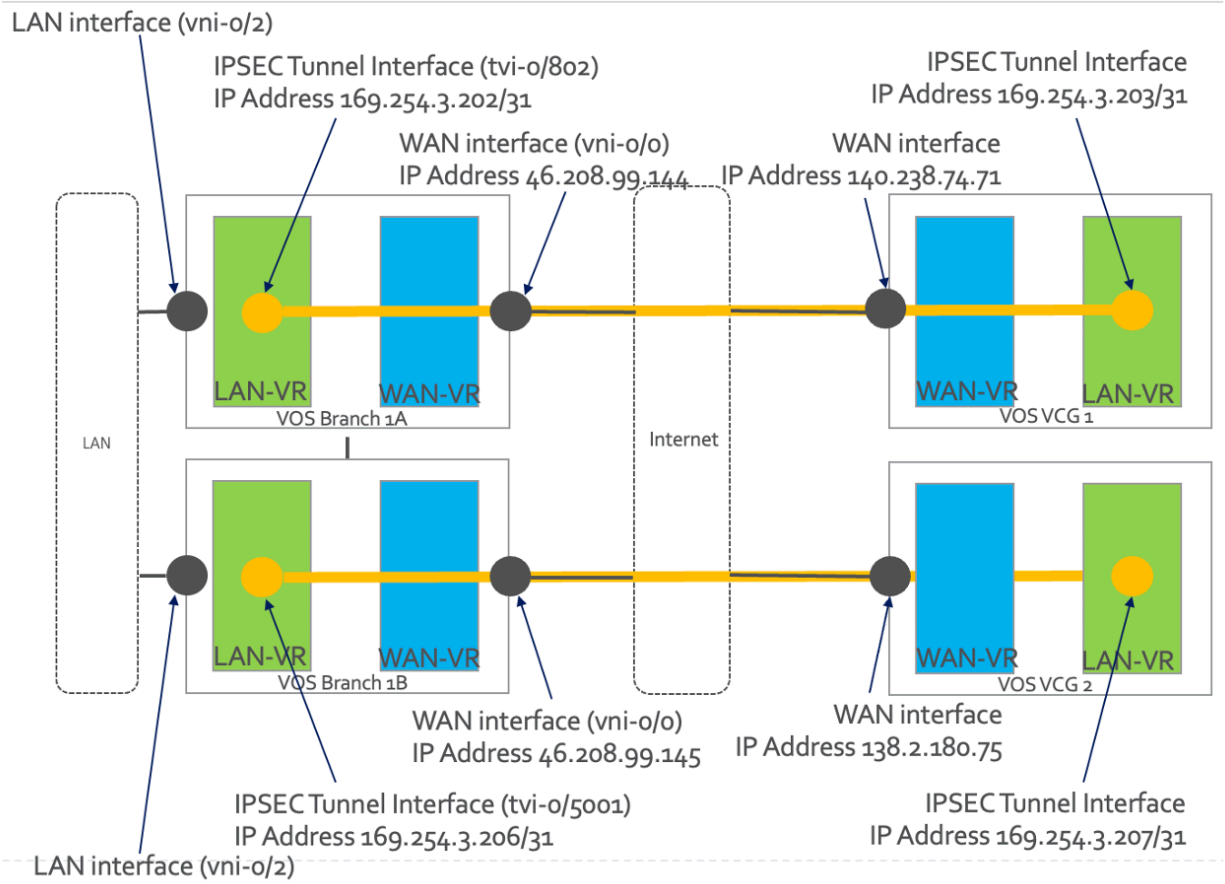
Verify the Site-to-Site Tunnel

Follow the same troubleshooting steps as shown in the Verify the Site-to-Site Tunnel in the Configure a Single-CPE, Single-WAN Topology section, above.

Configure a Dual-CPE, Dual-WAN Topology

For the dual-CPE, dual-WAN configuration, we use the topology shown in Figure 11.

Figure 11: Dual-CPE, Dual-WAN Deployment



To configure this topology, you perform the following high-level steps:

1. Configure the site-to-site tunnel using Concerto, which controls the VOS VCG shown in Figure 11.
2. Configure the site-to-site tunnel using Versa Director, which controls the VOS branch shown in Figure 11.
3. Verify that the site-to-site tunnel is established between the VOS branch and the VOS VCG.

For this example, the following are assumed:

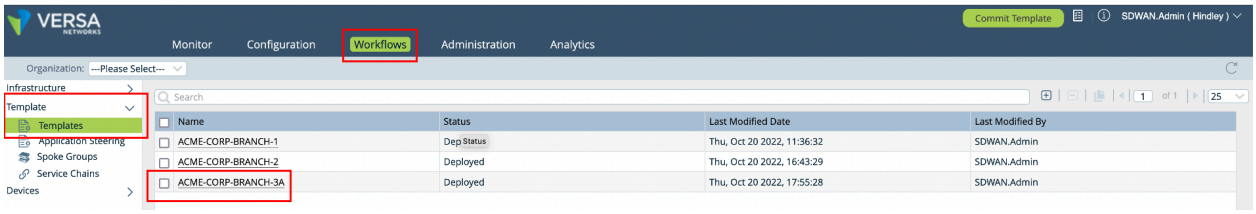
- BGP is enabled. Note that you can also configure static routing.
- Preshared keys (PSKs) are used between devices. Note that you can also configure certificates.
- Local and peer identity is established using IP addresses, although you can also configure FQDNs and email. The IP identity uses WAN IP addressing.
- IKE is established using AES256-SHA1 encryption and Diffie-Hellman Group 19. Note that you can also configure other transform sets and DH groups.
- IPsec is established using ESP-AES256-SHA1 encryption and Diffie-Hellman Group 19. Note that you can also configure other transform sets and DH groups.
- The VOS branch has a single LAN VRF. Note that you can also configure multiple LAN VRFs.
- The VOS VCG and the VOS branch are already built and deployed. The scope of this article is limited to building a site-to-site tunnel between devices.

Configure the VOS VCG Using Versa Concerto

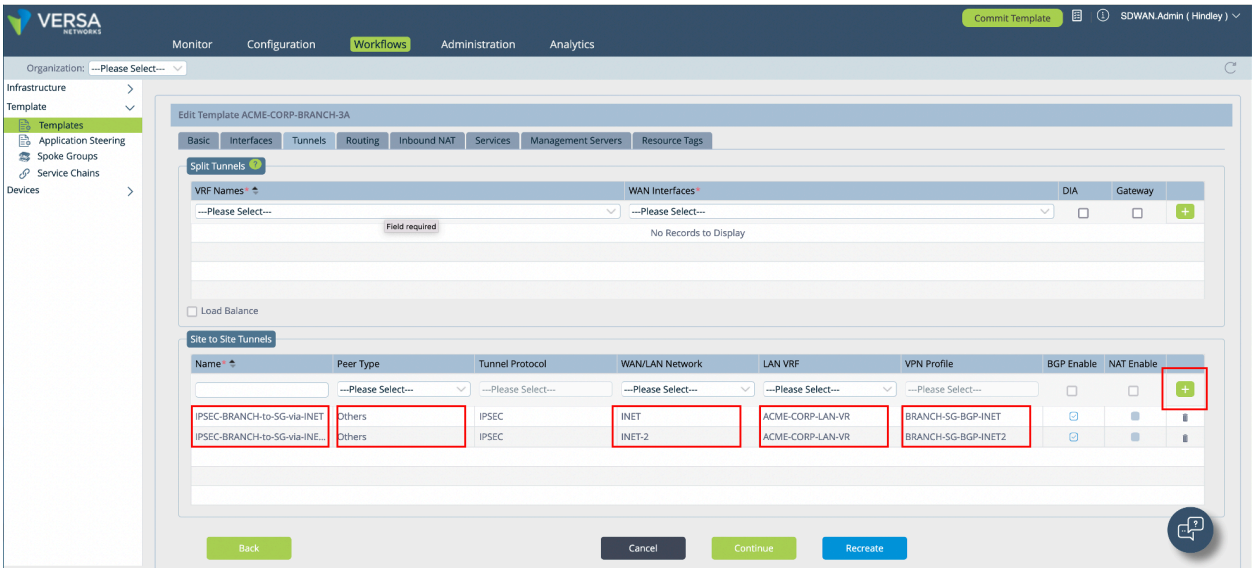
Follow the same procedure described in the Configure a Single-CPE, Dual-WAN Topology section, above.

Configure the VOS Branches Using Versa Director

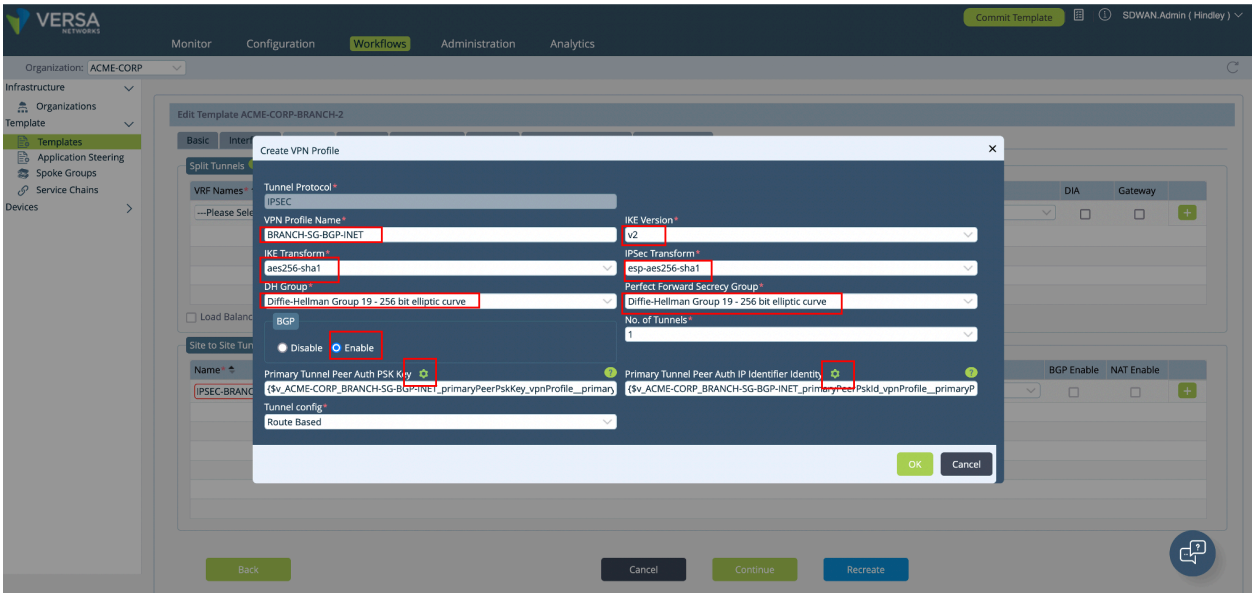
1. Log in to Versa Director
2. Select Workflows > Template > Templates, and then select the template associated with the VOS branch or branches that terminate the IPsec tunnel from the VOS VCG. In this example, the template is ACME-CORP-BRANCH-3A.



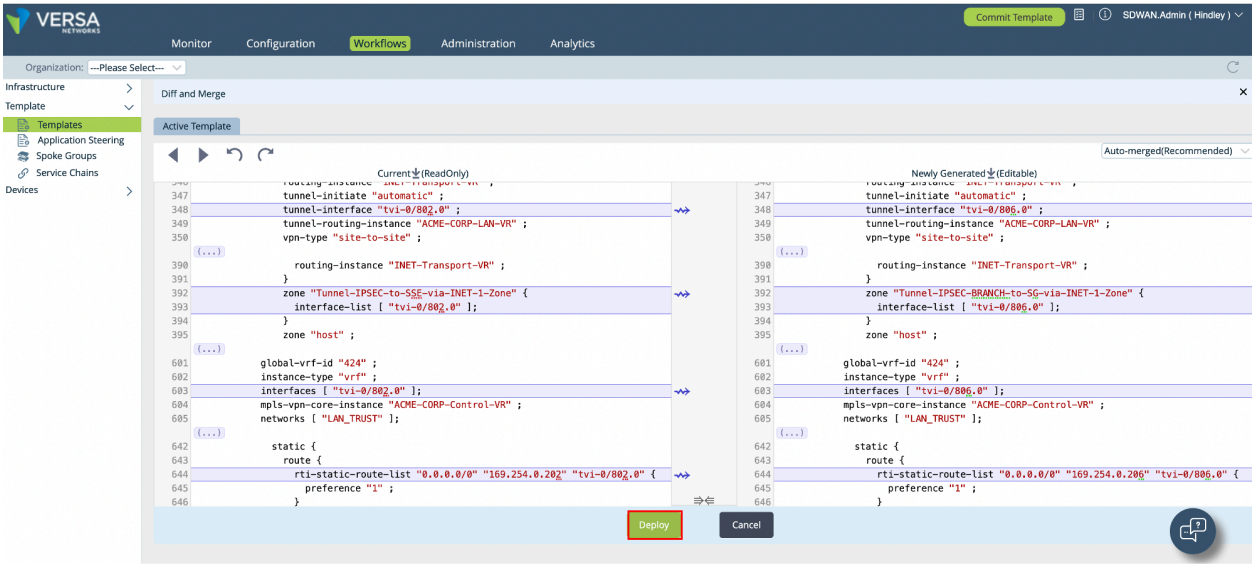
3. Select the Tunnels tab, and then configure the first site-to-site tunnel:
   a. Enter a name. This example illustrates one naming convention, in which the name is composed of the tunnel type (IPsec), the source (branch), the destination (SG – Service Gateway), and the local WAN interface (INET). You can modify the naming convention as needed.
   b. Set the peer type to Others.
   c. The WAN/LAN network is the WAN interface of the VOS branch. In this example, the interface is the network name known as INET.
   d. The LAN VRF is the LAN side VRF of the VOS branch. Typically, end users or devices reside in this VRF.
   e. Select a VPN profile or create one, as described in Step 5.
   f. Click the + icon to add the site-to-site tunnel configuration.
4. Repeat Step 3 to configure the second tunnel originating on the backup VOS branch. Note the following differences:
   a. In the Name field, enter a different name for the tunnel. In this example, we use INET2 instead of INET in the name.
   b. The WAN/LAN network is the WAN interface of the backup VOS Branch. In this case, it is the network name known as INET2.
   c. Create another VPN Profile. Do not reuse the one already created. This is because the same parameterized variable name is used for both VPN profiles and so you can only add the peer IP address of one of the VOS VCG in bind data.



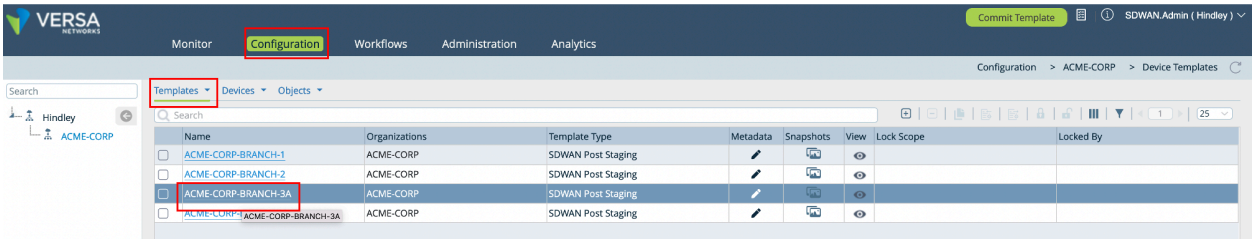
5. A VPN profile is an organization-wide template that you can associate with other VOS branches if required. To configure a VPN profile:
   a. In the VPN Profile Name field, enter a unique name to use to reference the VPN profile.
   b. Configuration the same IPSec parameters as you configured in Steps 3 through 6 in Configure the VOS VCG using Versa Concerto, above, modifying the values as necessary for your deployment.
   c. Enable BGP.
   d. If the identity of the IPsec tunnel is based on IP address, as is the case in this example, click the ⚙ Parameterize icon to parameterize the values, as shown in the screenshot below. You add the actual IP information later using bind data. Using the ⚙ Parameterize icon creates a variable, which allows you to use the template across multiple devices. If you were to statically assign IP identity information, the template would be specific to a single VOS branch.
   e. Click OK.



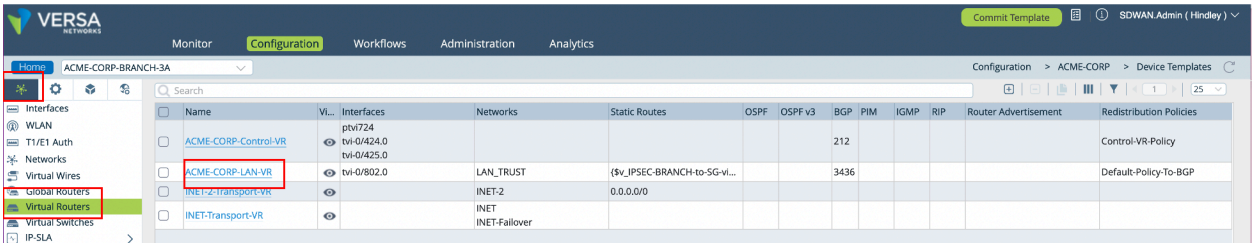
6. After sanity-checking the configuration, click Deploy. Deploying updates the device template with configuration associated with the newly configured site-to-site tunnels.



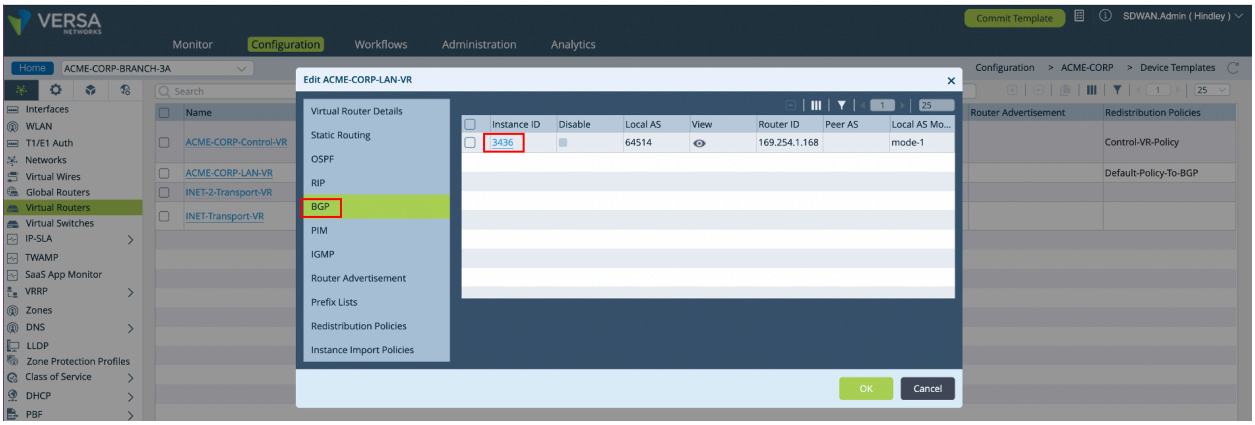
7. Select Configuration > Templates > Device Templates. Select the primary VOS branch that terminate the IPsec tunnel from the VOS VCG.



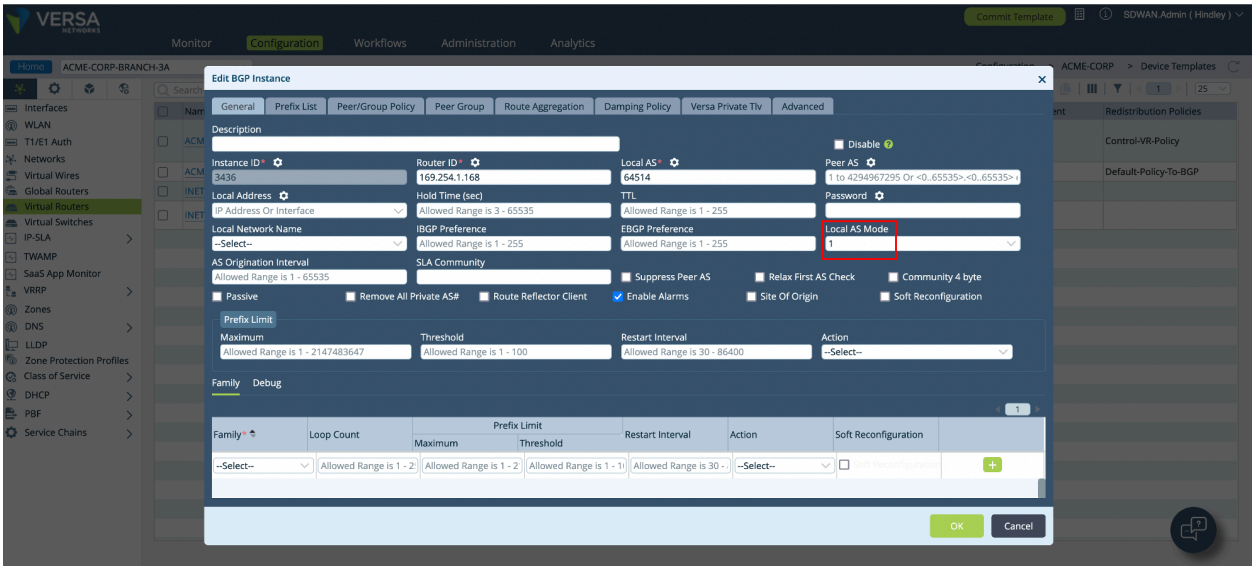
8. Select Networking > Virtual Routers > *organization-name*-LAN-VR. In this example, we select ACME-CORP-LAN-VR.



9. Select BGP > *instance-id*. In this example, the instance ID is 3436.



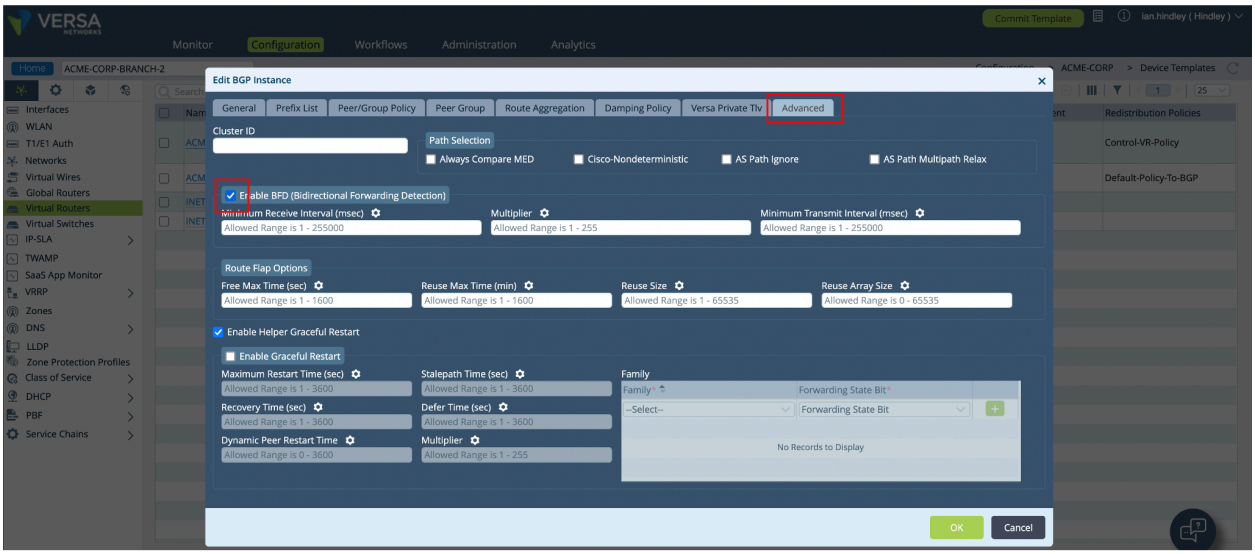
10. Set the local AS mode to 1. Doing this ensures that only the local AS is advertised to the VOS VCG. In this example, we want only 65000 to be prepended to the advertisement. By default, the reserved ASN 64514 is also prepended to the advertisement. The VOS VCG sees its own ASN in the path and rejects the route advertised by the VOS branch. The mode change ensures that 64514 is not prepended to the advertisement.



11. Select the Advanced tab, and configure the following:

a. Click Enable BFD.

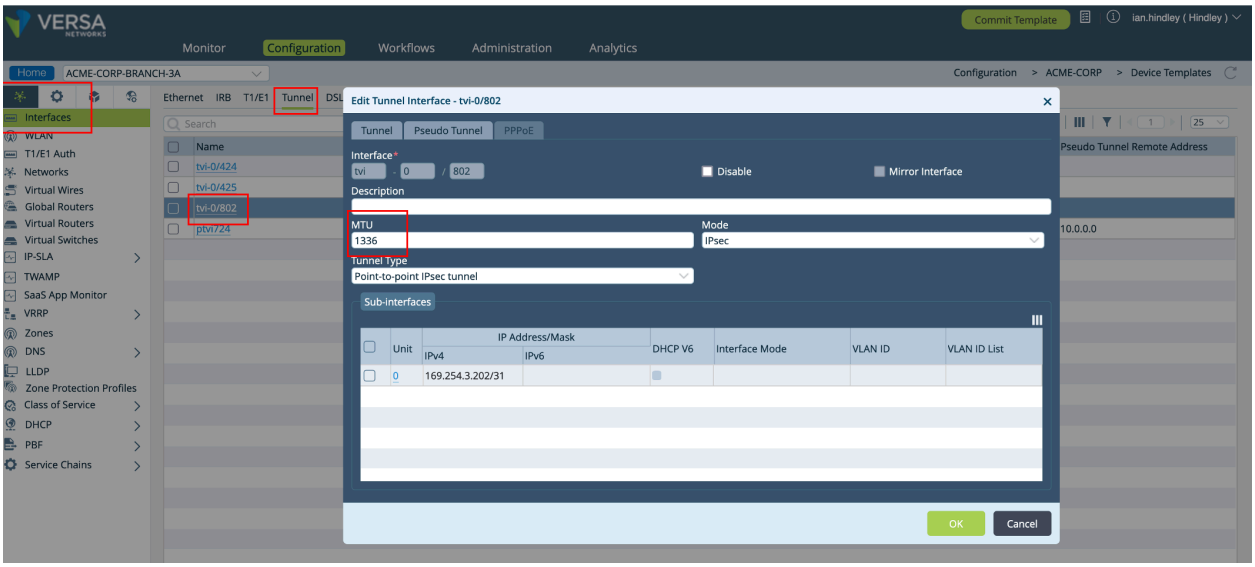
b. If desired, override the default BFD values by populating the fields shown in the following screenshot below. In this example, we accept the defaults (hello interval of 1 second and hello multiplier of 3), so we enter no values.



12. Click OK > OK.

13. Select Networking > Interfaces > Tunnel > tvi-0/*tvi-interface*, and then configure the following:

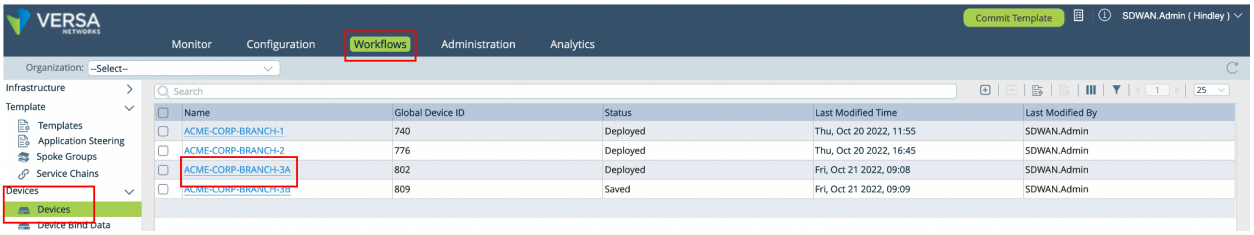
a. Set the MTU to 1336, and then click OK. Note that if you experience fragmentation, you may need to modify the MTU.



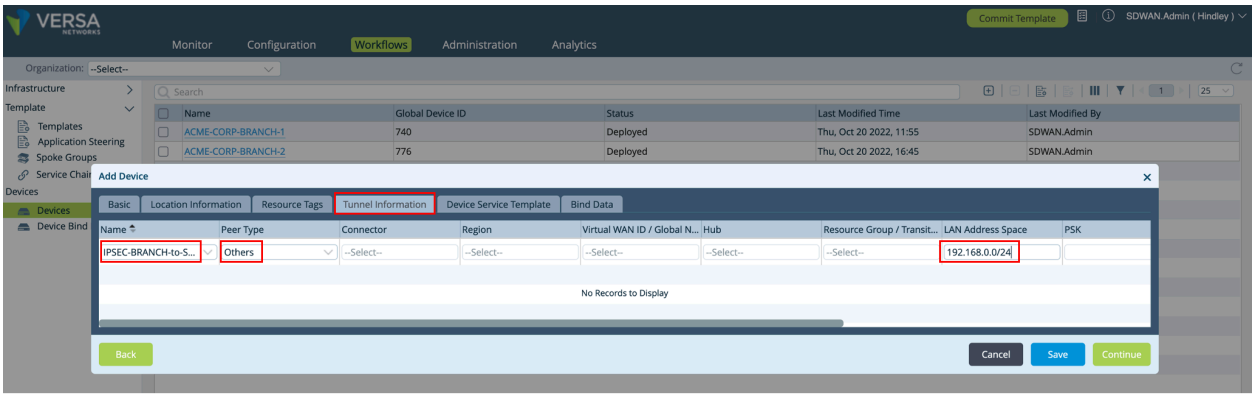
b. Note that when the VOS branch IPSec configuration is created, Versa Director automatically assigns 169.254.0.*x* addresses to the IPsec tunnel interface. An example is shown in the screenshot above, which shows the address 169.254.0.202/31. To modify the default IP addressing, see Modify the VOS Branch TVI IP Addressing, below.

14. Select Workflows > Devices > Devices. Select the VOS branch that terminates the IPsec tunnel from the VOS

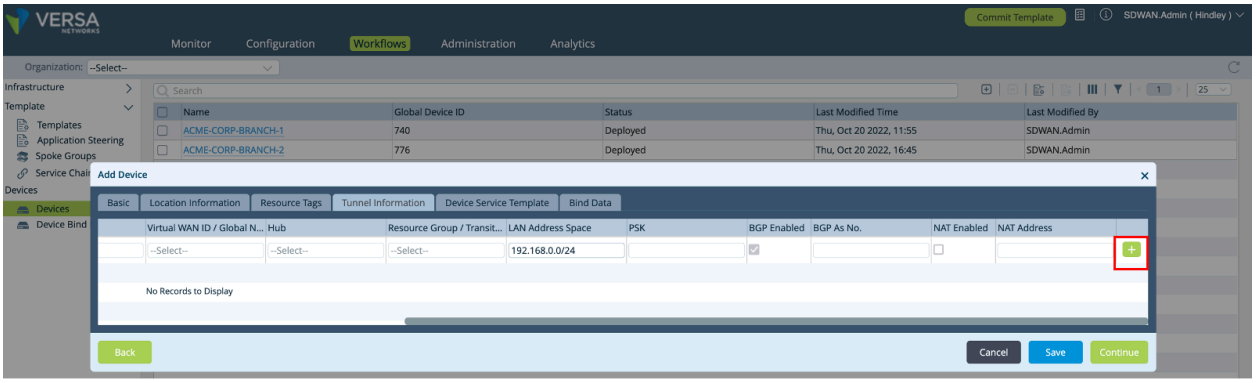
VCG. In this example, the VOS branch is ACME-CORP-BRANCH-3A.



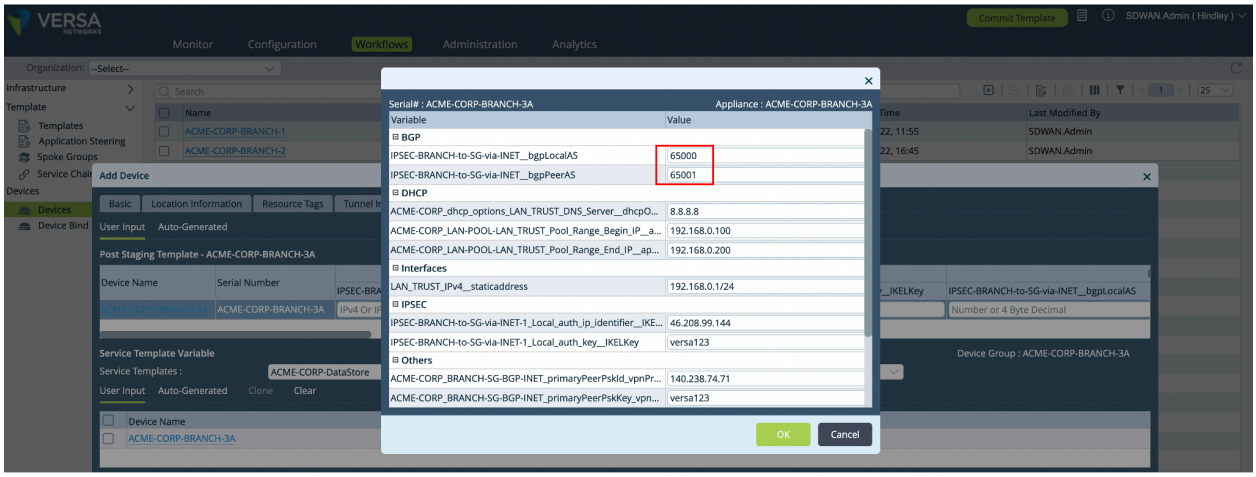
15. Select the Tunnel Information tab, and then enter the following information:
    a. Select the first newly created site-to-site tunnel.
    b. Select Others.
    c. Enter the LAN VRF address space. In this example, the LAN VRF is configured with the address space 192.168.0.0/24.



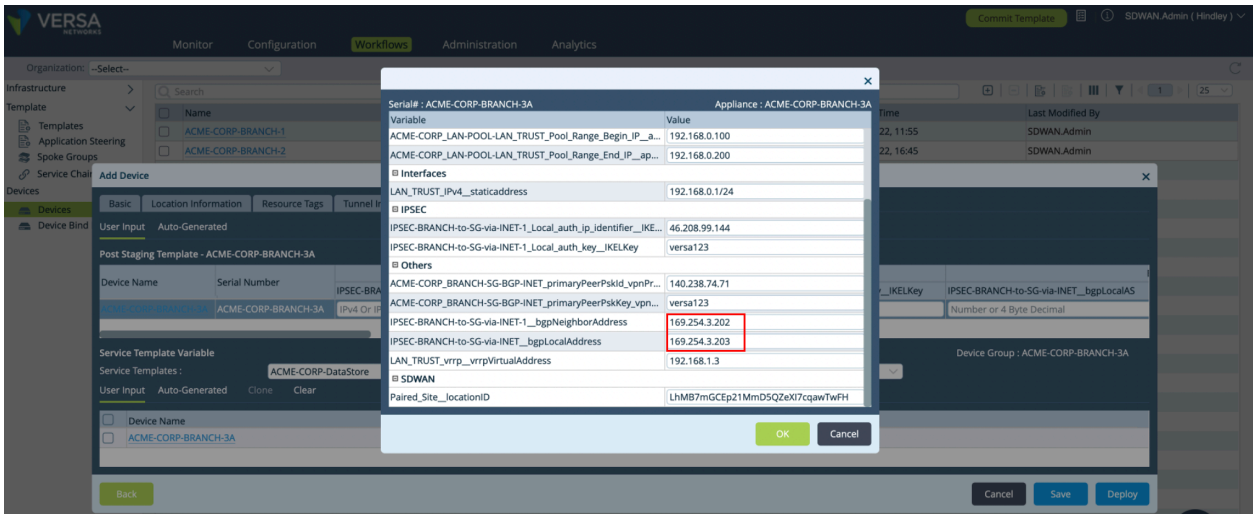
16. Click the + Add icon to add the LAN address space. To configure additional LAN address spaces, repeat Step 15.



17. Repeat Steps 15 and 16 for the second IPsec tunnel.
18. Select the Bind Data tab, and then configure the following:
    a. Enter values for the following BGP parameters:
        - Local AS and Peer AS for the BGP sessions over the IPsec tunnel—Note how this is per IPsec tunnel. In this example, the local ASN is 65000, and the remote ASN residing on the VOS VCGs is 65001.



- BGP Neighbor Address is the IP address of the primary VOS VCG BGP peer—In this example, it is also the IP address of the tunnel interface. Therefore, we configure it as 169.254.3.203.
- BGP Local Address is the IP address of the primary VOS branch peer—In this example, it is also the IP address of the tunnel interface. Therefore, we configure it as 169.254.3.202.

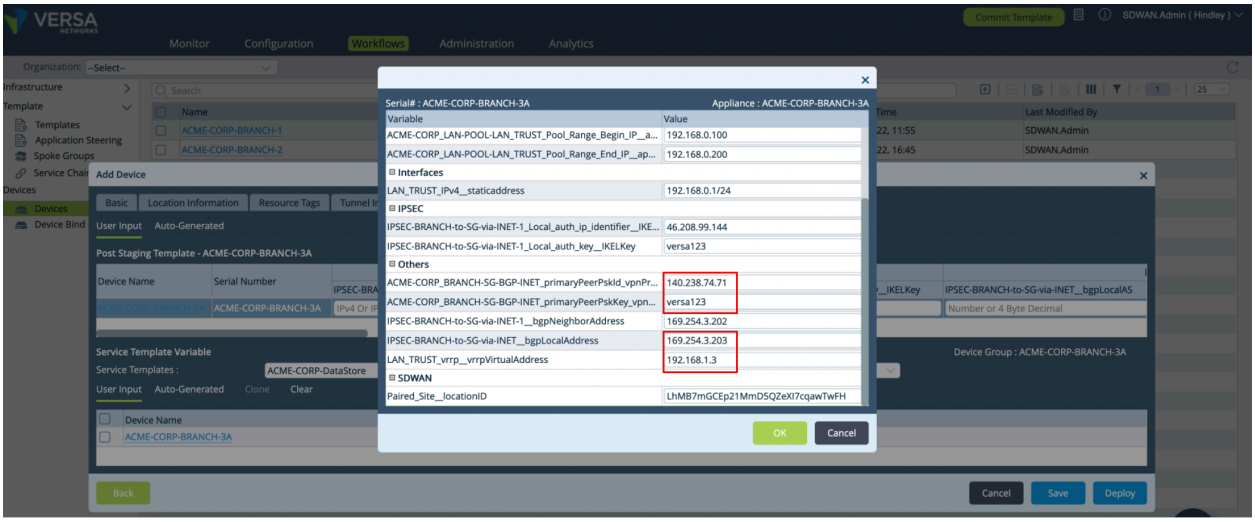


b. Enter values for the following IPsec parameters:
   - Local Authentication IP Identifier—In this example, this is the directly connected WAN IP address of the primary VOS branch.
   - Local Authentication PSK—In this example, we use "versa123". This is the same value that we configured earlier on the VOS VCG.

c. Enter values for the Other parameters:
   - Peer Authentication IP Identifier—In this example, this is the WAN IP address of the VOS Secure Gateway.
   - Peer Authentication PSK—In this example, we use "versa123". This is the same value that we configured earlier on the VOS VCG.

d. Click OK.

e. Click Redeploy.



19. Repeat steps 6 through 18 for the backup VOS branch.
20. To apply the site-to-site configuration to the VOS branches, follow the normal process to Commit Template.

Verify the Site-to-Site Tunnel

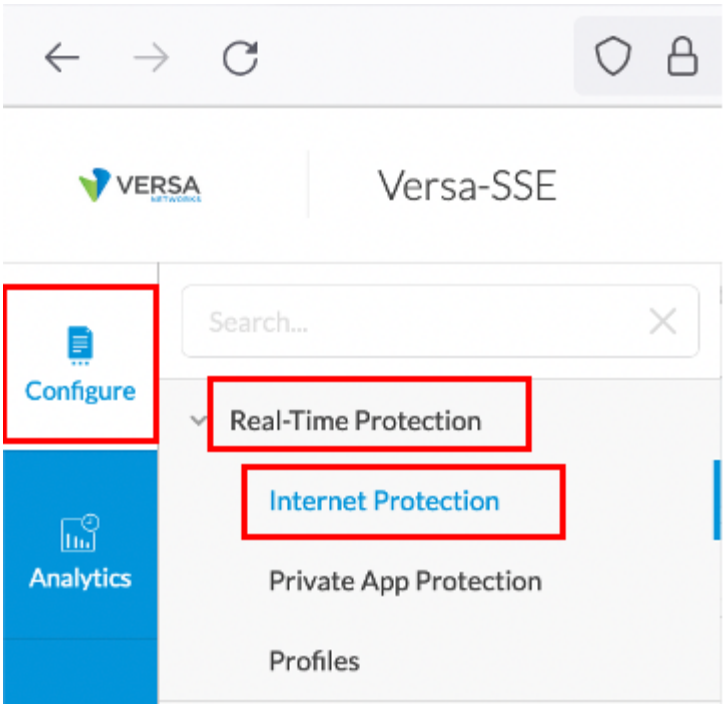
Follow the same troubleshooting steps as shown in the Verify the Site-to-Site Tunnel in the Configure a Single-CPE, Single-WAN Topology section, above.

Tune Firewall Rules

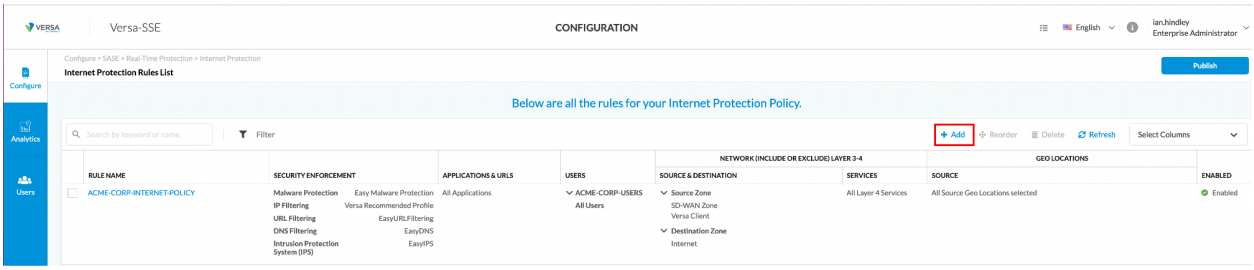
Depending on the use case, you may need to modify firewall rules, to permit traffic. You modify the rules either on the VOS branch, on the VOS VCG, or on both. For example, if the use case is integrating Secure SD-WAN and SWG to allow users of Secure SD-WAN to access the internet via the SWG, on the VOS secure gateway, you must associate additional source zones in the policy to permit traffic arriving over the IPsec tunnel from the VOS branch and to permit traffic being transmitted to the internet through the SWG.

Configure Firewall Rules on Concerto from the VOS Branch to the VOS VCG

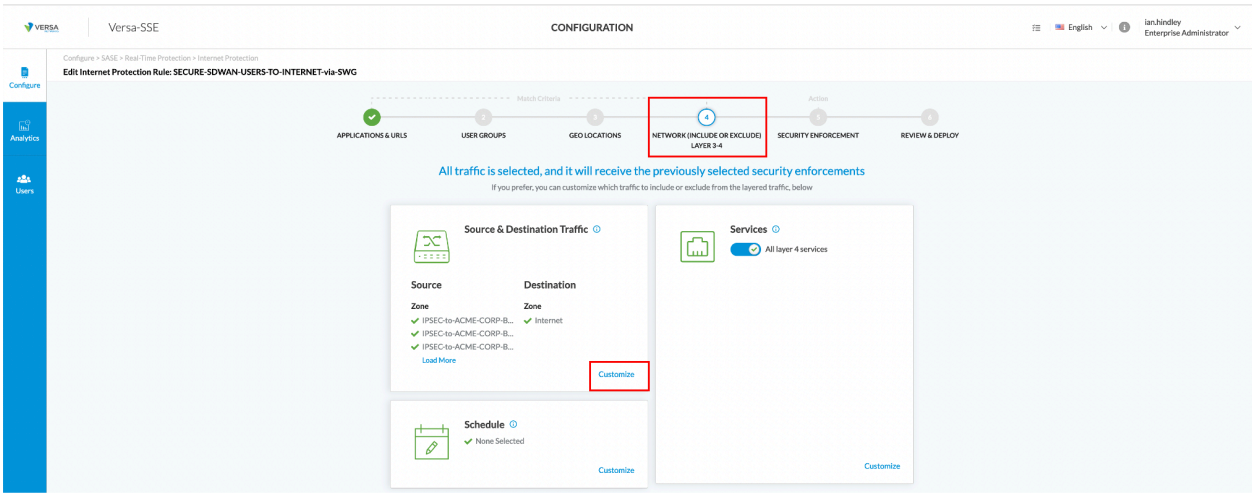
1. Log in to Concerto
2. To configure rules controlling flows of data from VOS branches that are destined to VOS VCGs, click Configure > Real-Time Protection > Internet Protection.



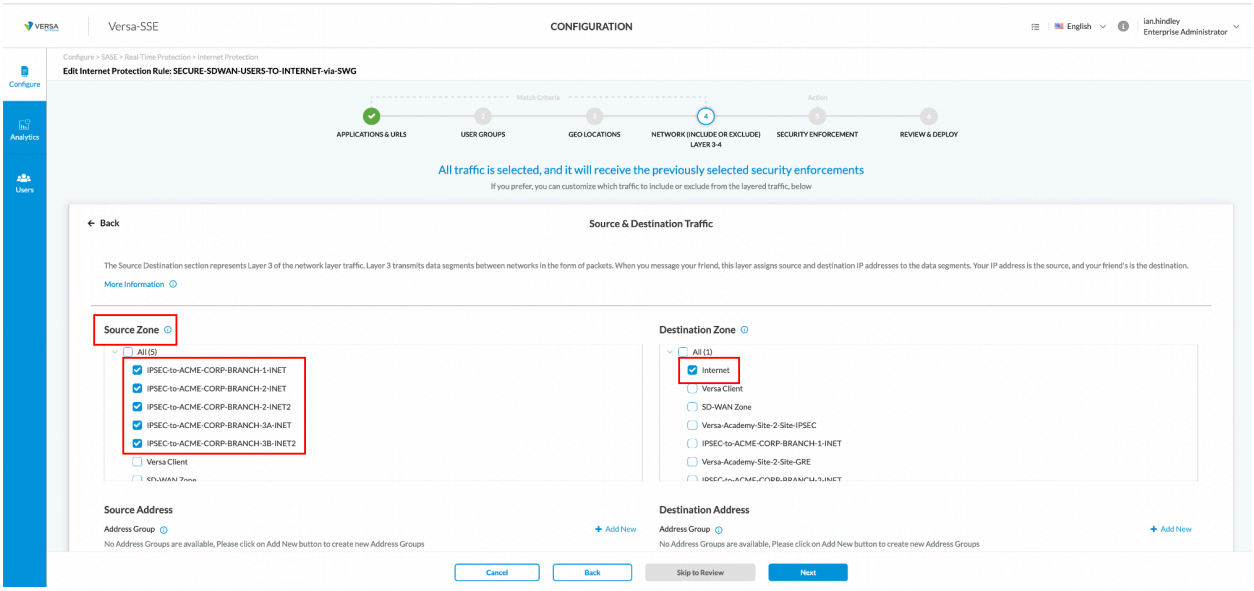
3. Select an existing rule and modify if, or, as in this example, click Add to create a new rule to control traffic sourced from the Secure SD-WAN.



4. Configure the rule as appropriate until you reach Step 4, NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4. Then, in Step 4, select Customize.



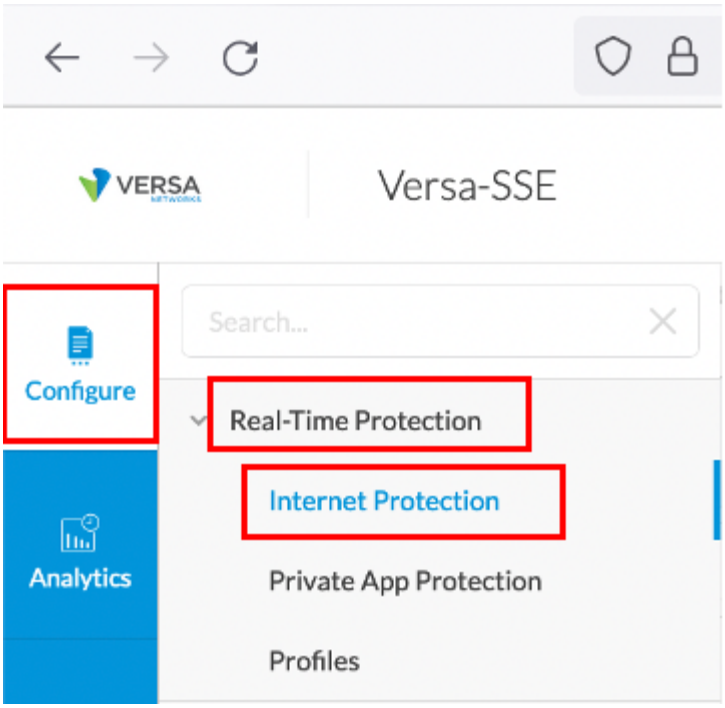
5. In the Source Zone section, modify the source zones to include the site-to-site tunnel or tunnels. Notice that the name of the zone is the same as to the name of the site-to-site tunnel name that you already created in Concerto. Therefore, simply select all the appropriate site-to-site tunnels. In the example here, the destination zone is prepopulated with the option Internet. Note that you can add source and destination IP addresses to refine control further.



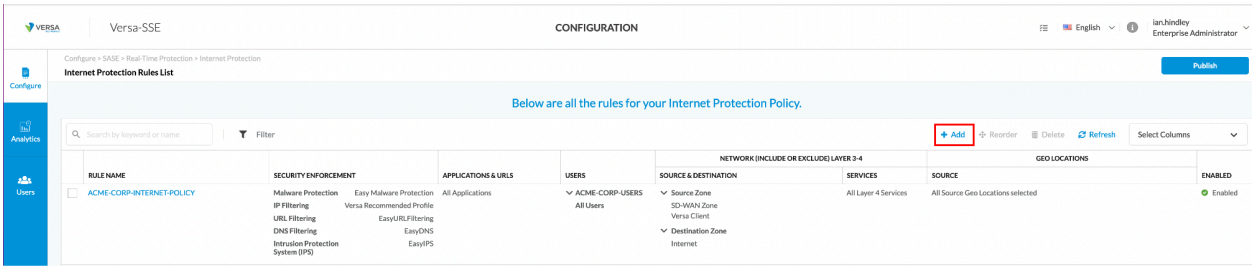
6. Click Next, and then complete Steps 5 and 6.
7. Click Publish to push the configuration to the VOS VCG.

Configure Firewall Rules on Concerto from the VOS VCG to the VOS Branch

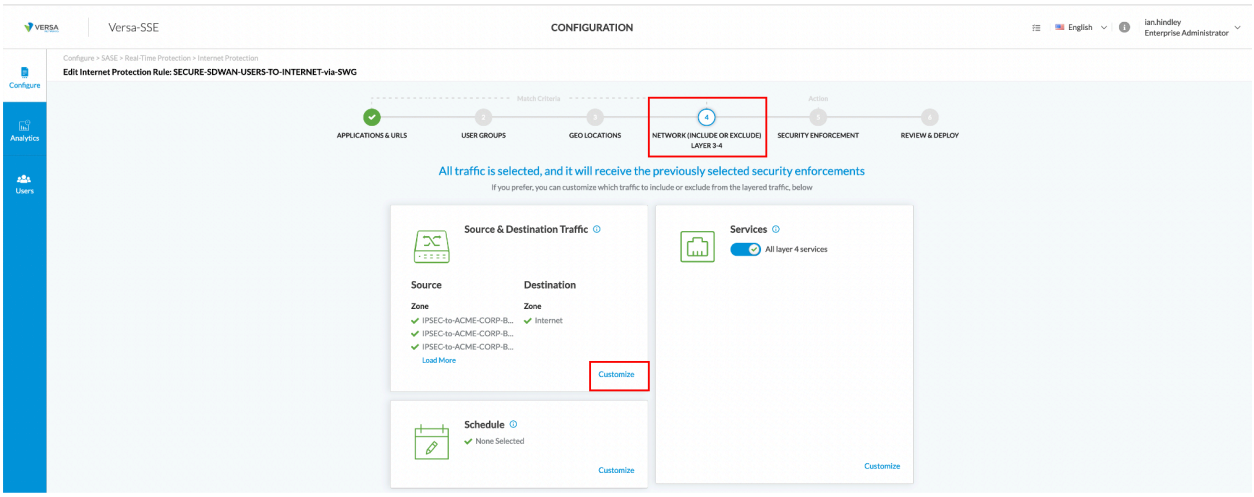
1. To configure rules controlling flows of data from VOS VCGs to VOS branches, click Configure > Real-Time Protection > Internet Protection.



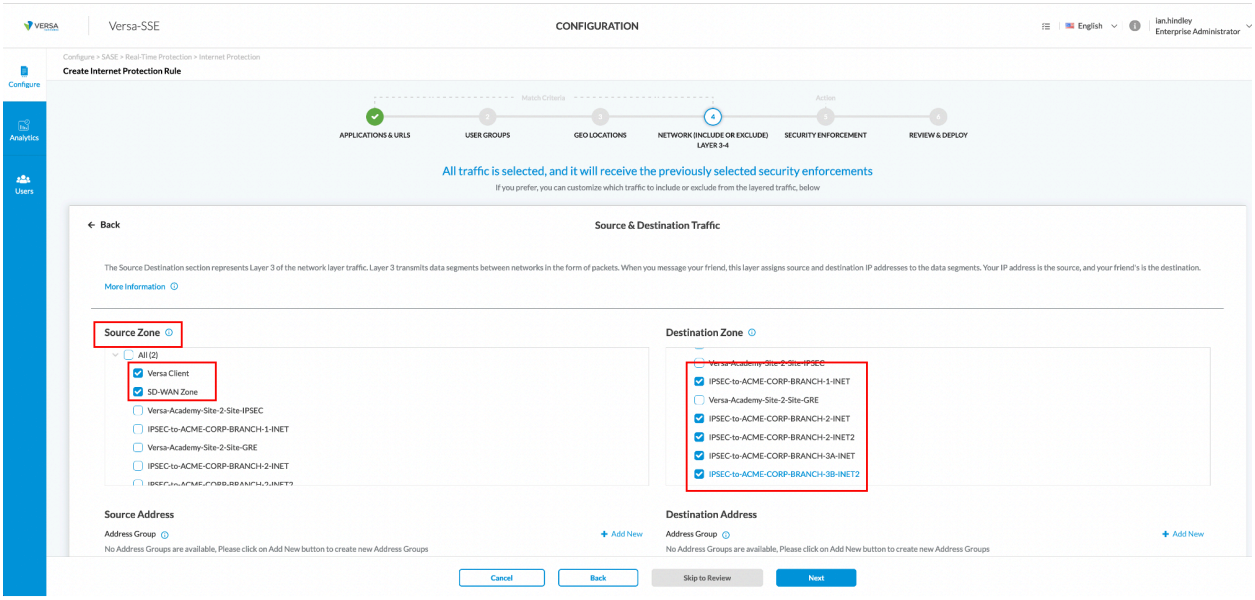
2. Select an existing rule and modify it, or, as in this example, click Add to create a new rule to control traffic sourced from the Secure SD-WAN.



3. Configure the rule as appropriate until you reach Step 4, NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4. Then, in Step 4, select Customize.



4. In the Source Zone section, modify the source zones to include the Versa client and, optionally, the SD-WAN zone. In the destination zone section, modify the destination zones to include the site-to-site IPsec tunnel or tunnels. Notice that the name of the zone is the same as to the name of the site-to-site tunnel name that you already created in Concerto. Therefore, simply select all the appropriate site-to-site tunnels. In the example here, the destination zone is prepopulated with the option Internet. Note that you can add source and destination IP addresses to refine control further.

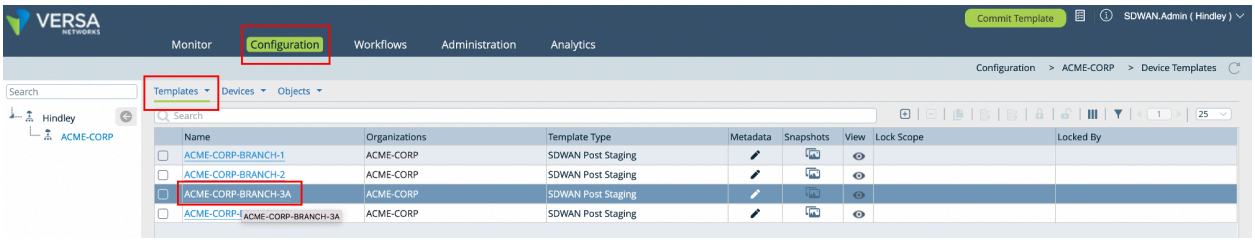


5. Click Next, and then complete Steps 5 and 6.
6. Click Publish to push the configuration to the VOS VCG

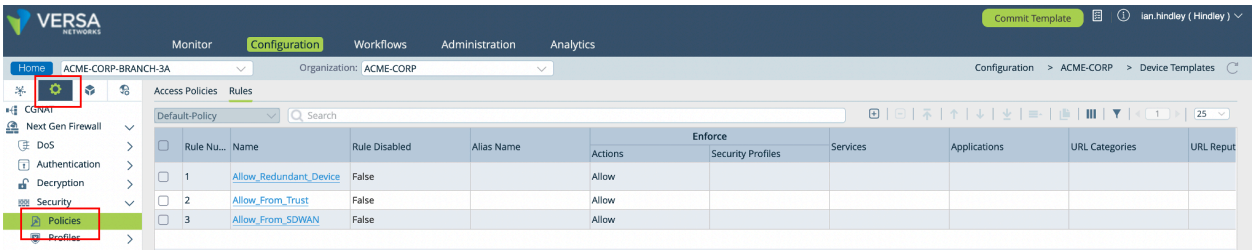
Configure Firewall Rules on Versa Director from the VOS Branch to the VOS VCG

1. Log in to Versa Director.
2. Select Configuration > Templates > Device Templates. Select the VOS branch that terminates the IPsec tunnel

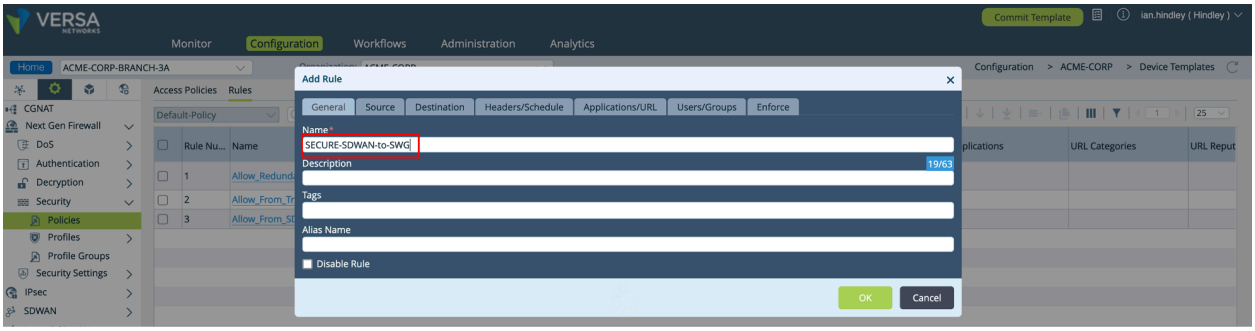
from the VOS VCG. In this example, the branch is ACME-CORP-BRANCH-3A.

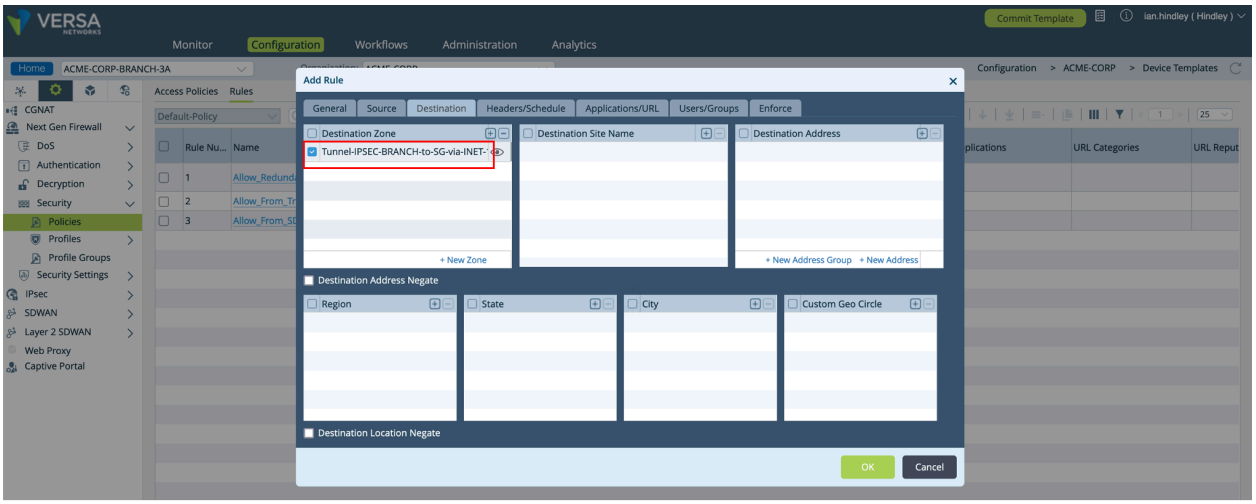


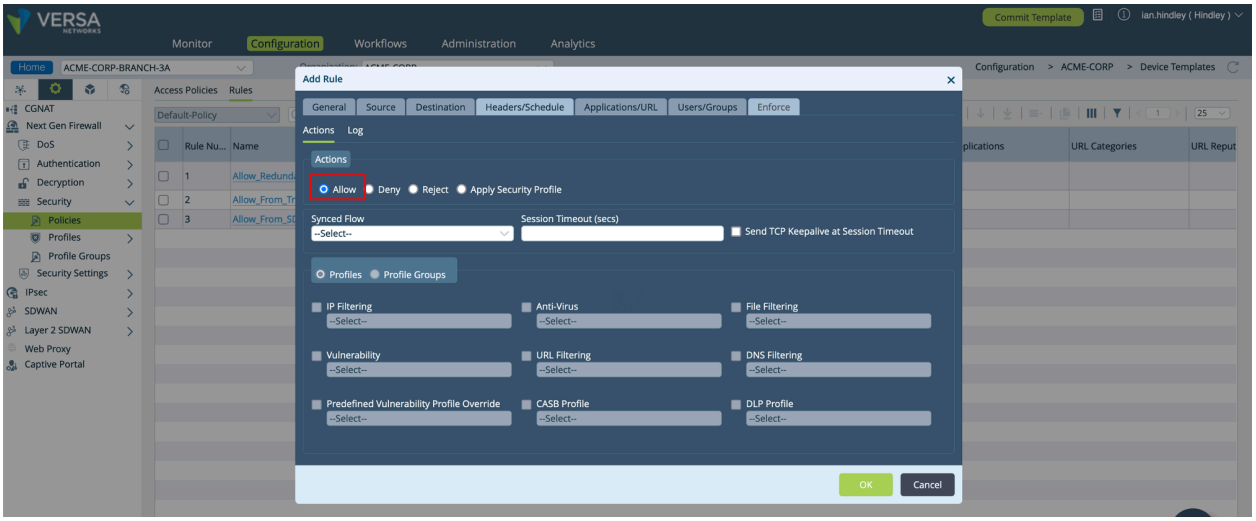
3. Select Configuration > Services > Next-Gen Firewall > Security > Policies.



4. By default, the rules (as shown in the screenshot above) permit traffic from the VOS branch to the VOS VCG for traffic that is sourced from the LAN of the CPE. Therefore, no modifications may be necessary. However, if you are not using the default rules, you need to use an existing rule or create a new one. In this example, we create a new rule that permits any traffic destined for the site-to-site IPsec zone. Note that you can modify the rule according to your specific requirements. For example, you may limit the rule to source zones or addresses.



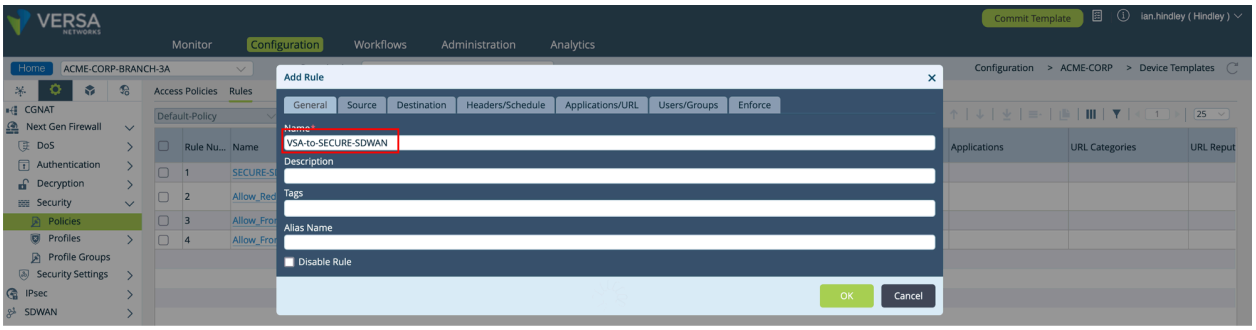


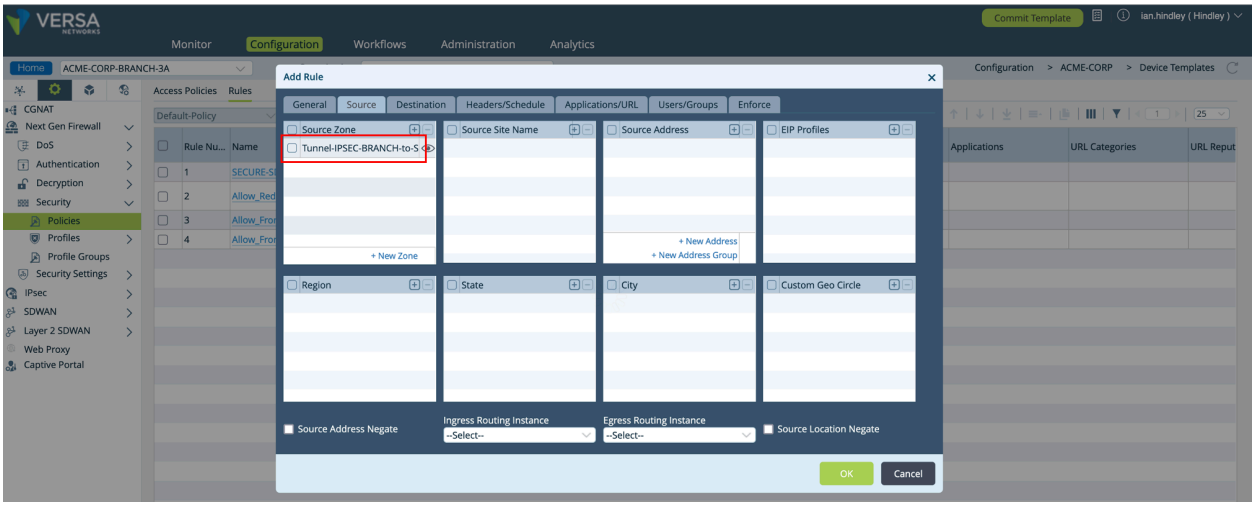


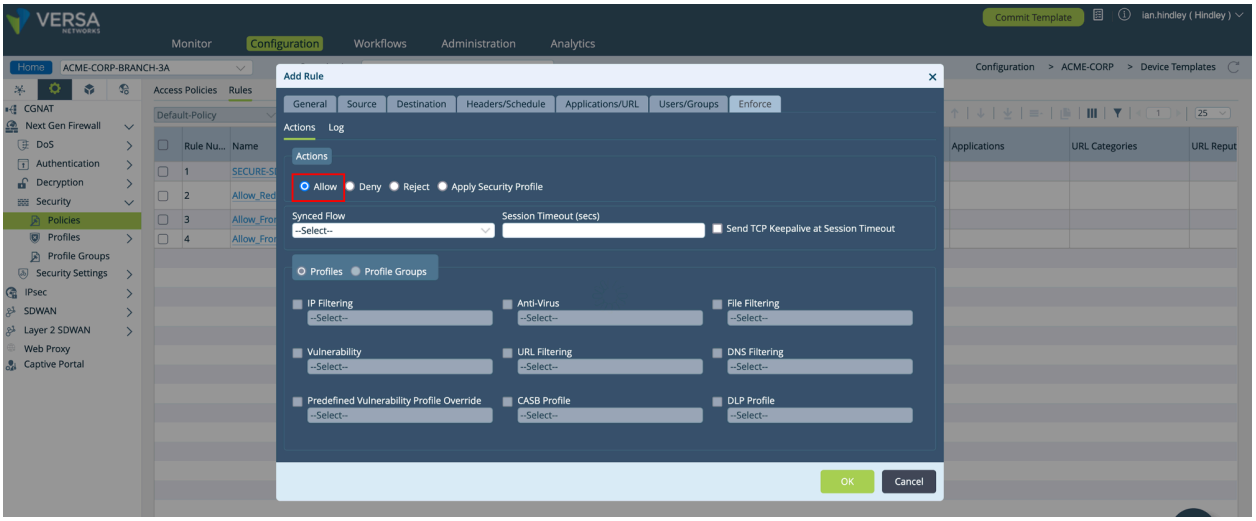
5. To apply the changes to the VOS branch, follow the normal process to Commit Template.

Configure Firewall Rules on Versa Director from the VOS VCG to the VOS Branch

1. By default, the rules shown in the previous section do *not* permit traffic from the VOS VCG to the VOS Branch. For use cases when Secure SD-WAN users require access to the internet through the SWG, this is not an issue because traffic is sourced from the VOS branch and destined for the VOS VCG. In other words, no traffic originates from the VOS VCG. However, for use cases in which VSA users want to access private data centers or cloud data centers and branches, you must configure firewall rules to permit the flow from the VOS VCG to the VOS branch.
   In this example, we create a new rule that permits any traffic sourced from the site-to-site IPsec zone. Note that you can modify the rule according to your specific requirements.







2. To apply the changes to the VOS branch, follow the normal process to Commit Template.

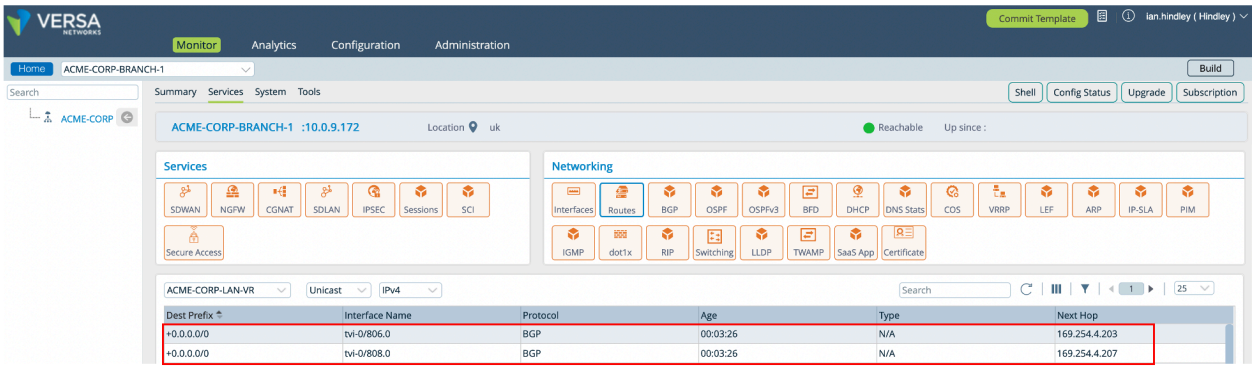
Configure BGP Policy

If a VOS branch has one of the following, it is recommended that you use BGP, along with BFD, over the site-to-site

tunnels with the VOS VCGs. This approach ensures that either platform fails over seamlessly and promptly.

- Branch has two WAN links, as described in Configure a Single-CPE, Dual-WAN Topology, above.
- Site has two VOS branches, each with one WAN link, as described in Configure a Dual-CPE, Dual-WAN Topology, above.
- Site has one WAN link, with multiple site-to-site tunnels per WAN link, as described in Configure Multiple Site-to-Site Tunnels per WAN Link, below.

By default, a VOS branch load-balances end user sessions between the two site-to-site tunnels. In the example here, the VOS branch ACME-CORP-BRANCH-1 has been reconfigured. Although it has one WAN link, using the procedure in Configure Multiple Site-to-Site Tunnels per WAN Link, below, it now has a site-to-site tunnel to London and Frankfurt using its single WAN link. This means that the VOS branch has two IPSec tunnels to two different VOS VCGs. Because of this, and based on the best practice, we have enabled BGP and BFD. Now, by default, the VOS branch now receives two default routes, one from each VOS VCG. Both routes are Preferred routes, as indicated by the + sign, and both are installed in the routing table.

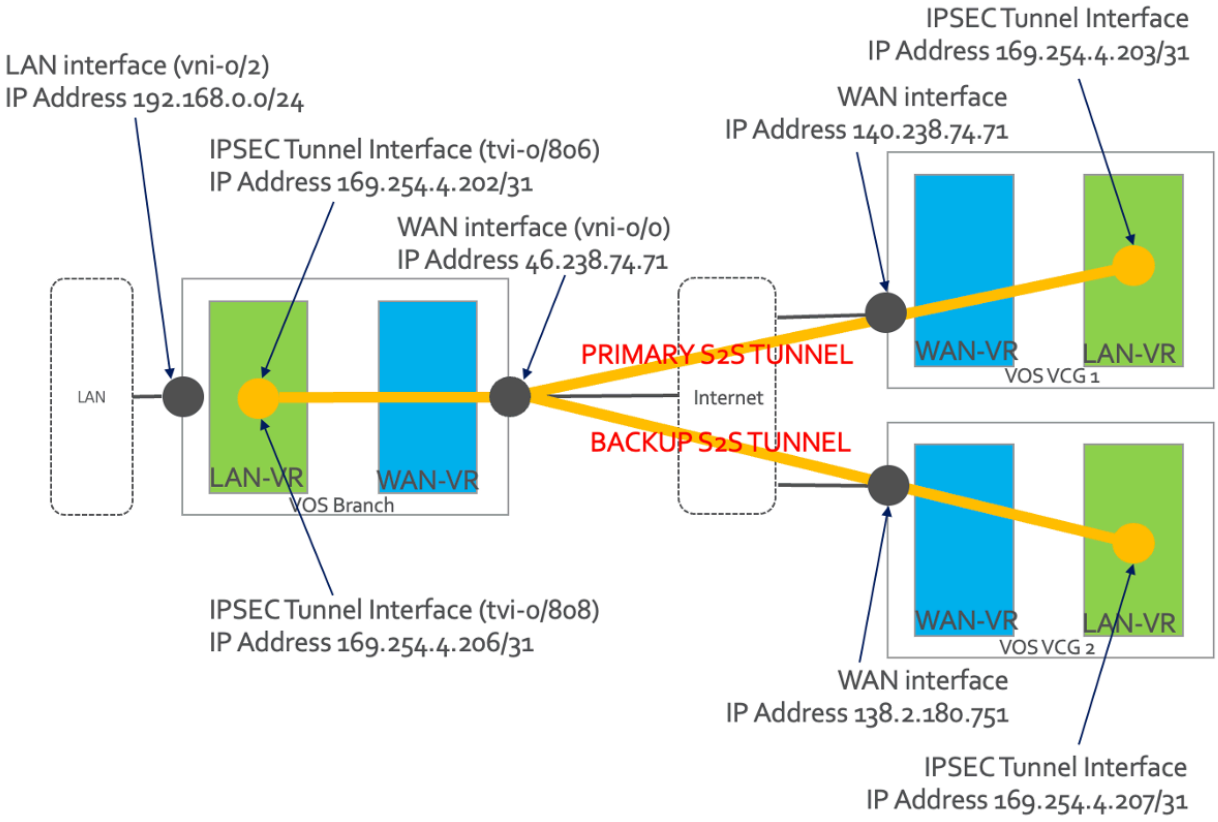


An enterprise may prefer the default behavior, and therefore no further changes are necessary. However, with no changes, troubleshooting and capacity planning become more complex, because end user sessions are load-balanced over the two IPsec tunnels.

An alternative architecture, which is described in this section, is to enable BGP policy so that one of the site-to-site tunnels is preferred over the other. In this way, all end user sessions traverse just one of the tunnels. Only if the primary tunnel fails do end user sessions traverse the other tunnel.

For this example, we use the topology shown in Figure 12, which continues the routing table example provided above). Here, the enterprise wants VOS VCG 1 (London) to be the primary site-to-site tunnel. If this tunnel fails, the enterprise wants traffic to fail over to VOS VCG 2 (Frankfurt).

Figure 12: BGP Policy Example



In this example, BGP policy is controlled from the VOS branch in the following ways:

- Use local preference on the VOS branch for routes received from the VOS VCG:
  - Configure the primary tunnel to use the default local preference value of 100.
  - Configure the backup tunnel to use the local preference value 90.
  - The higher the local preference value, the more preferred the route.
- Use AS path prepending on the VOS branch for routes advertised into the VOS VCG:
  - Primary tunnel does not prepend any AS to routes advertised to the VOS VCG.
  - Backup tunnel prepends the AS twice to routes advertised to the VOS VCG.
  - The shorter the AS_PATH, the more preferred the route.

In this configuration example, the VOS branch is controlling egress traffic to and ingress traffic from the VOS VCG using these BGP attributes. Therefore, there is no requirement for additional configuration on the VOS VCG.

This configuration example assumes there is one tunnel per VPN profile, as described in Configure Multiple Site-to-Site Tunnels per WAN Link, below. If your topology has two tunnels, do not forget to associate the BGP policy with the BGP peer rather than with the default of associating it with the BGP peer group. Failure to do this applies both the AS path and local preference modifications to both peers rather than to each peer separately.

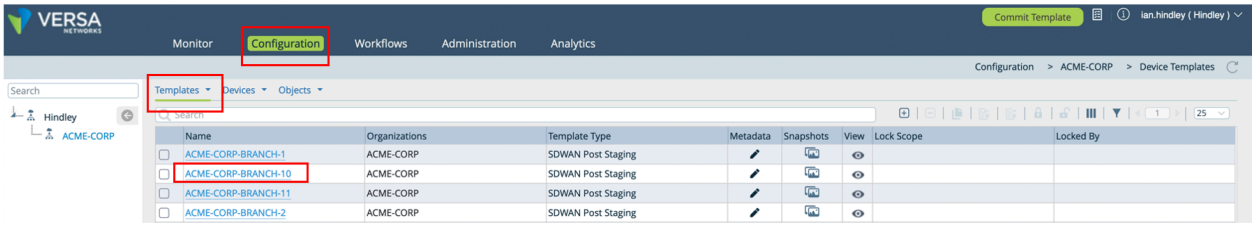
The following table summarizes the BGP policy that we use in this configuration example.

Table 1: Sample BGP Policy

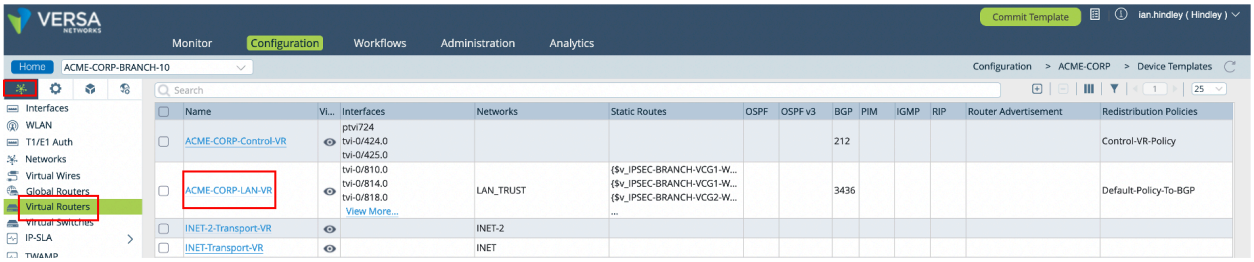
VPN Profile Name	AS Path Prepend	Local Preference Adjustment	Site-to-Site Tunnel Preference
BRANCH-VCG-BGP-PEER1-WAN	No Example 65000	No Example 100	Primary site-to-site tunnel
BRANCH-VCG-BGP-PEER2-WAN1	Yes Example – 65000, 65000	Yes Example 90	Secondary site-to-site tunnel

Configure BGP Using Versa Director to the VOS Branch

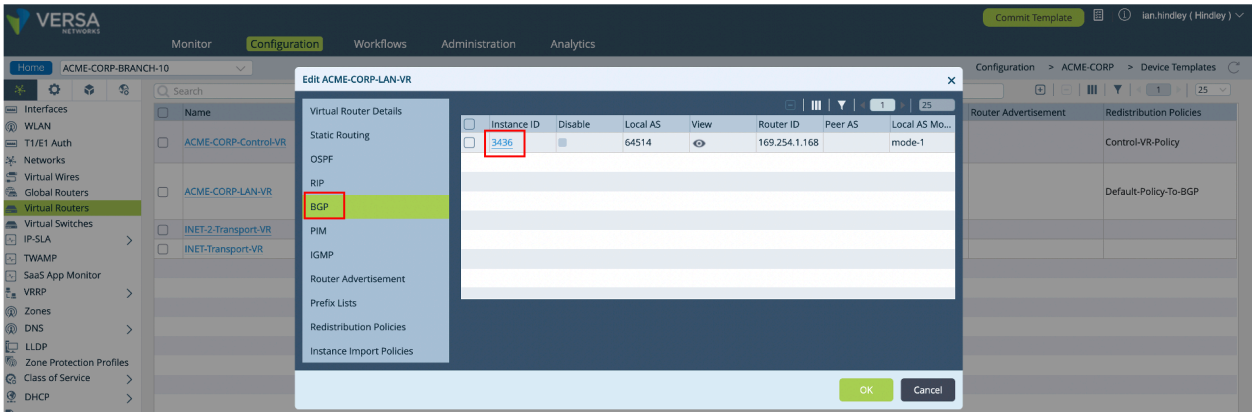
1. Log in to Versa Director.
2. Select Configuration > Templates > Device Templates. Select the VOS Branch that terminates the IPsec tunnels from the VOS VCG.



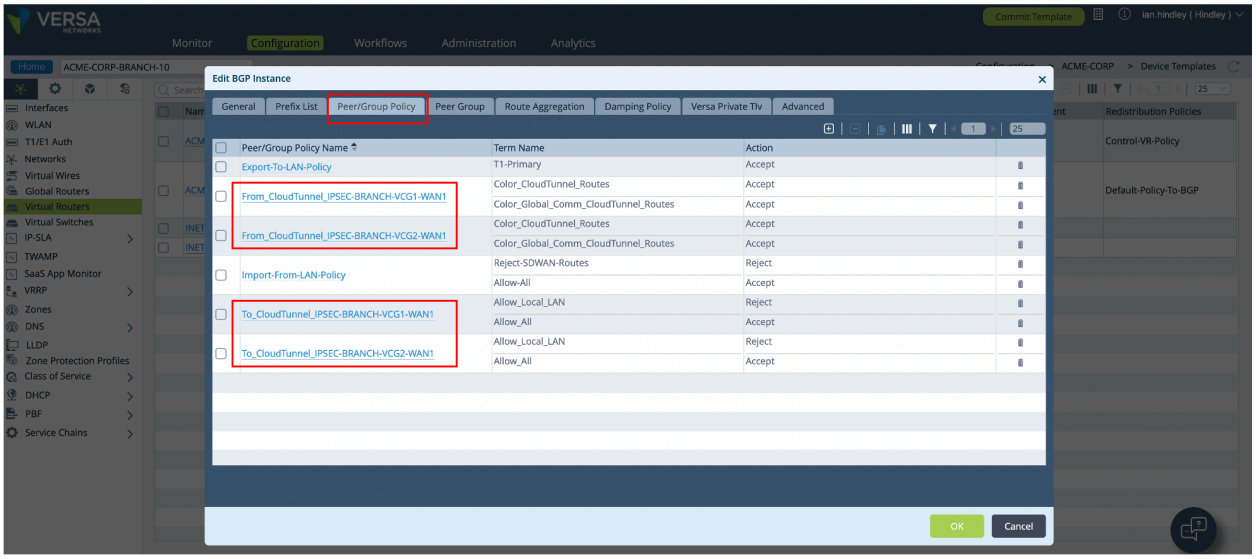
3. Select Networking > Virtual Routers > *organization-name*-LAN-VR. In this example, we select ACME-CORP-LAN-VR.



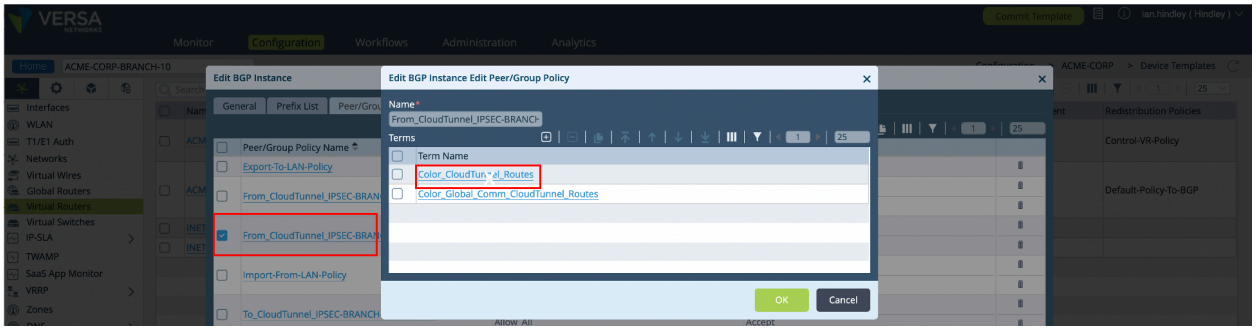
4. Select BGP > *instance-id*. In this example, the instance ID is 3436.



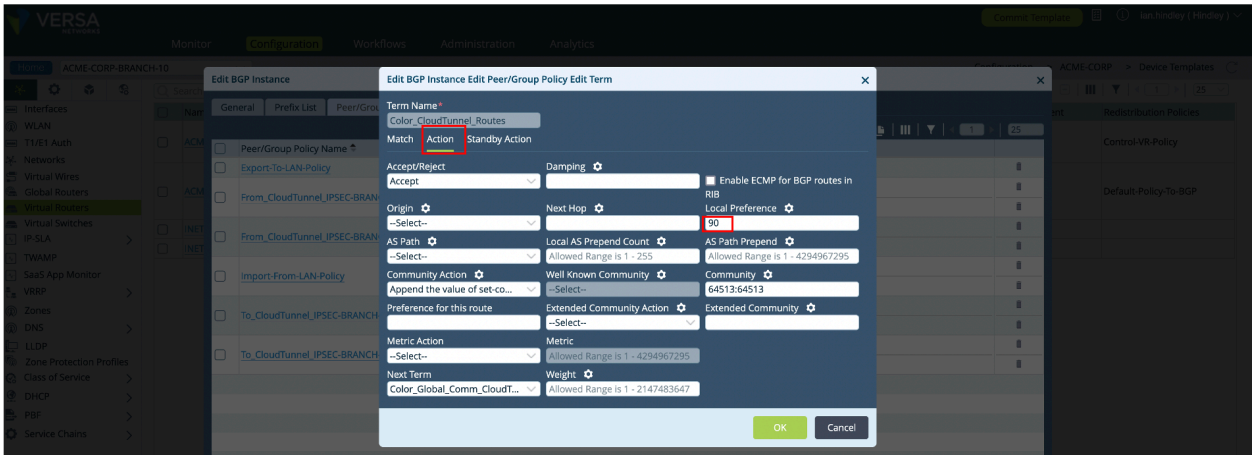
5. Optionally, make changes to BGP policy for the primary site-to-site BGP peer. Note that using the workflow template to build site-to-site tunnels as described in this article automatically creates BGP policy. In this example, we make no modifications to BGP policy for the primary site-to-site BGP peer. We make modifications only to the secondary site-to-site BGP peer.
6. Depending on your architecture, you may need to advertise address ranges other than the address range directly connected to this VOS Branch. If this is the case, see Advertise Networks between the VOS VCG and the VOS Branch, below.
7. In this example, there are two VOS VCGs and one WAN link, so there are four peer/group policies with four different names. There are two To policies, which influence the routes advertised to the VOS VCG BGP peers, and there are two From policies, which influence the routes received from the VOS VCG BGP peers. The following screenshot highlights the four policies.



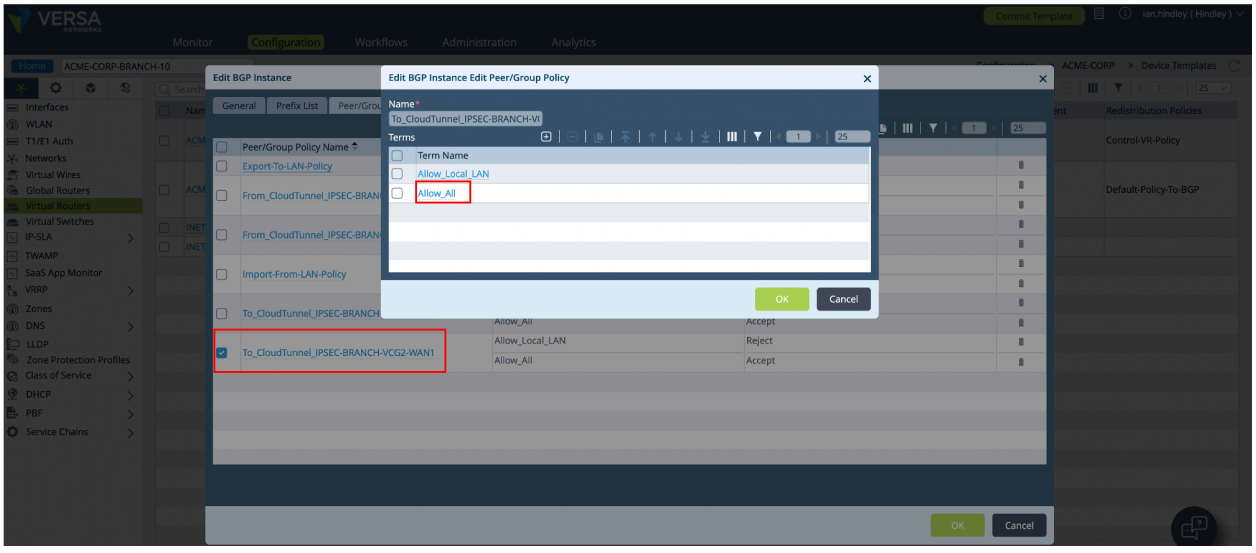
8. Select the secondary site-to-site tunnel BGP policy named From, and then select the Color_CloudTunnel_Routes term.



9. Select the Action tab, and then enter 90 in the Local Preference field.
10. Click OK, and then click OK a second time.

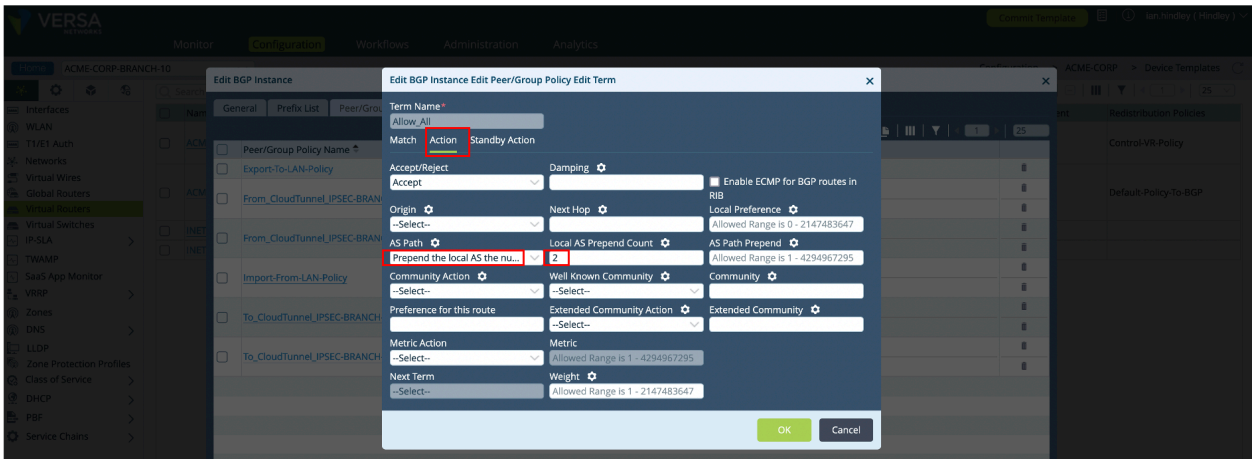


11. Select the secondary site-to-site tunnel BGP policy named To_CloudTunnel, and then select the Allow_All term name.

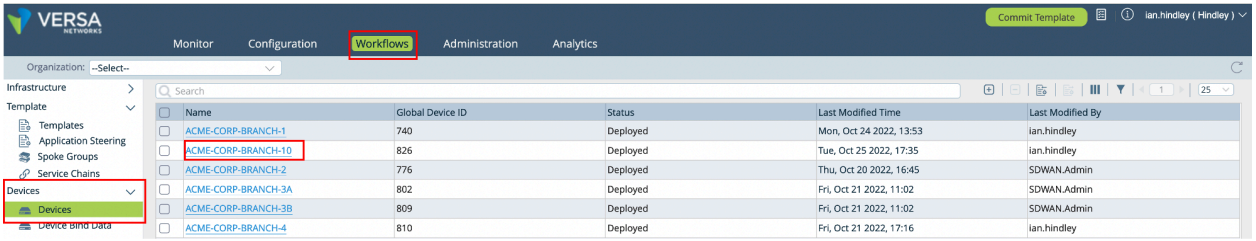


12. Select the Action tab, and then select Prepend the Local AS in the AS Path field.
13. In the Local AS Prepend Count field, enter 2.

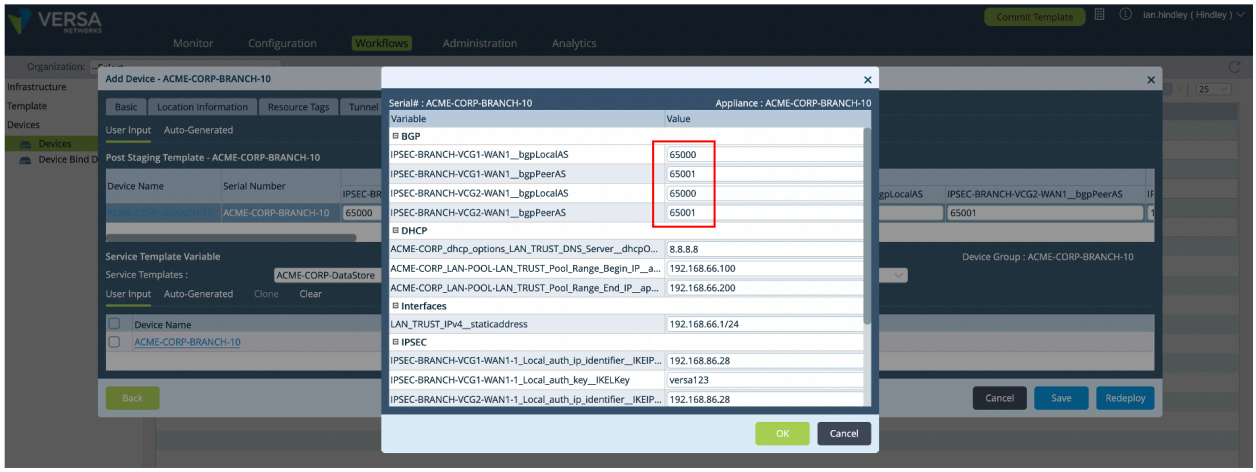
14. Click OK, and then click OK a second time.



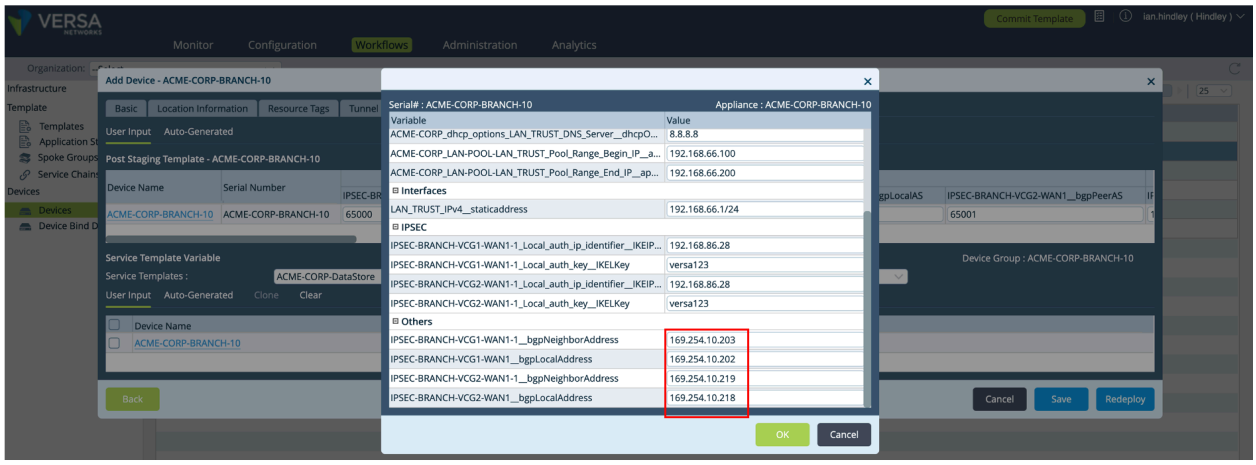
15. Remember to enable BFD under the Advanced tab, as described in the main part of this article.
16. Click OK, and then click OK a second time.
17. Select Workflows > Devices > Devices. Select the VOS Branch that terminates the IPsec tunnel from the VOS VCG. In this example, the VOS branch is called ACME-CORP-BRANCH-10.



18. Select Bind Data, and enter values for the following BGP parameters:
    - Local AS number for the BGP sessions over the IPsec tunnel. This is the local ASN residing on the VOS branch. In this example, it is 65000.
    - Peer AS number for the BGP sessions over the IPsec tunnel. This is the remote ASN residing on the VOS VCGs. In this example, it is 65001.



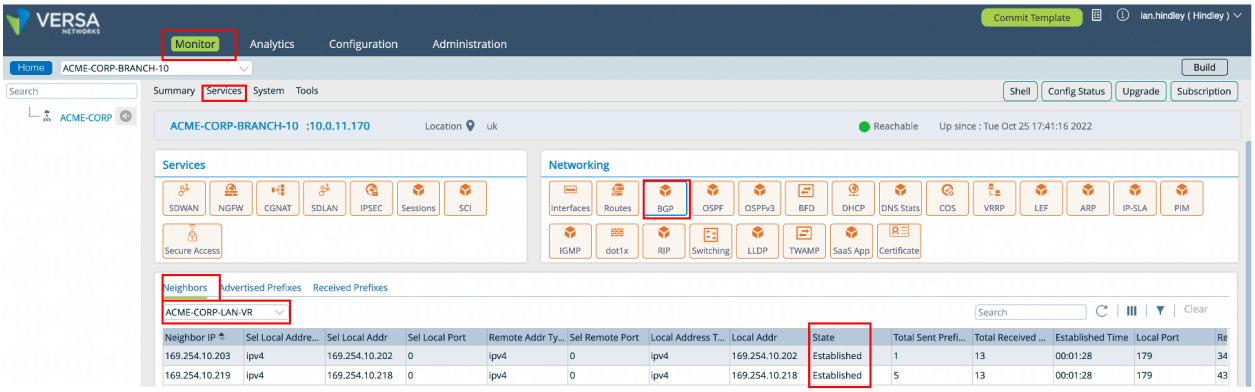
- BGP Neighbor Address (text boxes 1 and 3 below) are the VOS VCG BGP peer IP address (or addresses). In this example, the address is also the IP address of the tunnel interface. Therefore, it is configured as either 169.254.10.203 or 169.254.10.219.
- BGP Local Address (text boxes 2 and 4 below) are the VOS branch peer IP address (or addresses). In this example, the address is also the IP address of the tunnel interface. Therefore, it is configured as either 169.254.1.202 or 169.254.1.218.



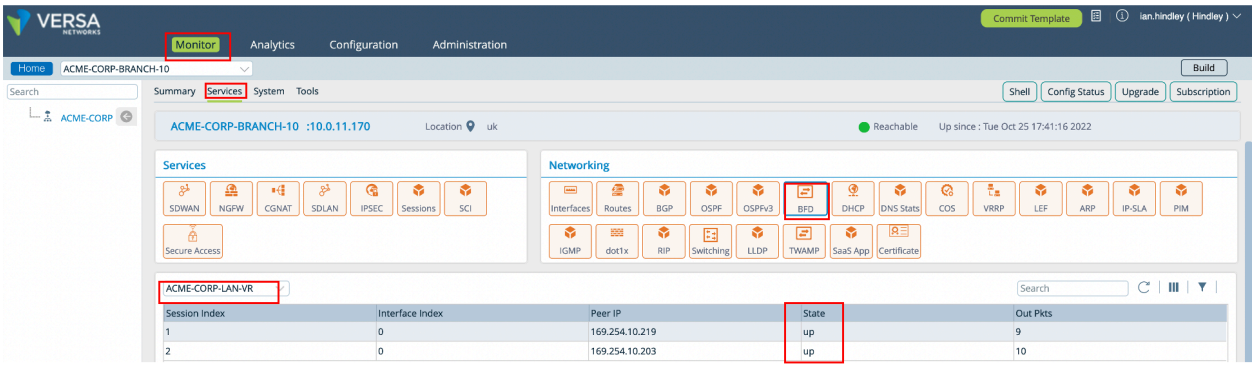
19. Click OK.
20. Click Redeploy.
21. To apply the site-to-site configuration to the VOS branch, follow the normal process to Commit Template.

Verify Routing

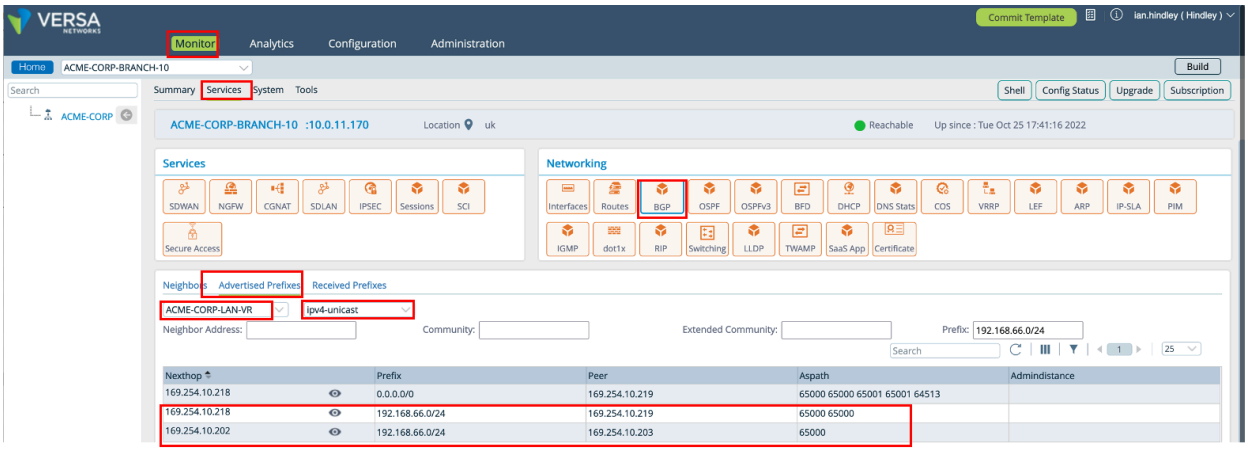
1. Check that BGP sessions are established between the VOS branch and the VOS VCG.



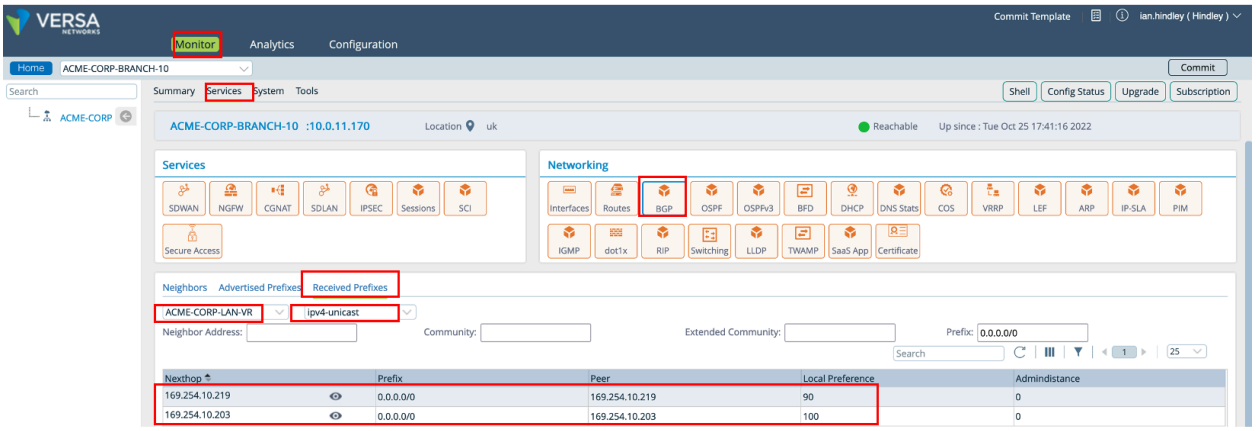
2. Check that BFD between the VOS branch and the VOS VCG is Up.



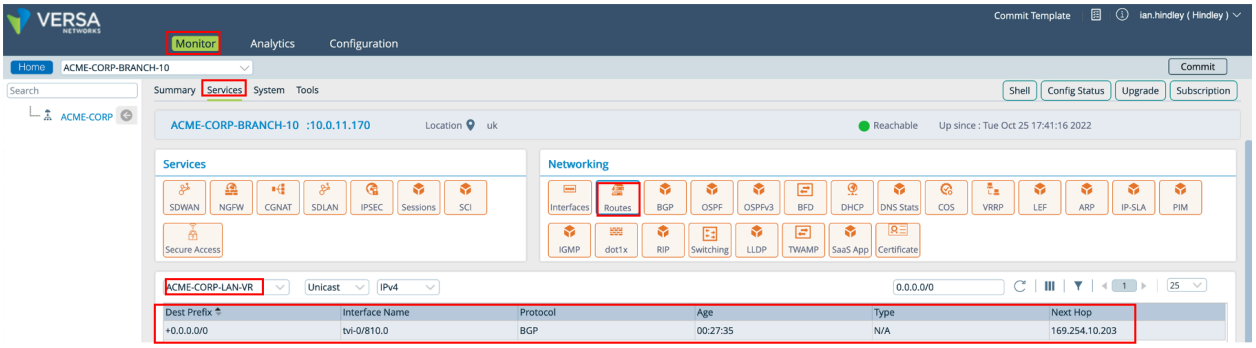
3. Check that the outbound BGP policy is correctly applying the AS path prepending. In this example, we expecting the VOS branch to advertise 192.168.66/24 with an AS path of 65000 (length of 1) over the primary site-to-site tunnel. Also, the same subnet is advertised with an AS path of 65000, 65000 (length of 2) over the secondary site-to-site tunnel.



4. Check that the inbound BGP policy is correctly applying the the amended local preference values. In this example, we are expecting the VOS branch to change the local preference of 0.0.0.0/0 as advertised by the two VOS VCGs. The primary site-to-site tunnel should have a local preference of 100, and the secondary site-to-site tunnel should have a local preference of 90. (The higher the local preference, the more preferred the route).



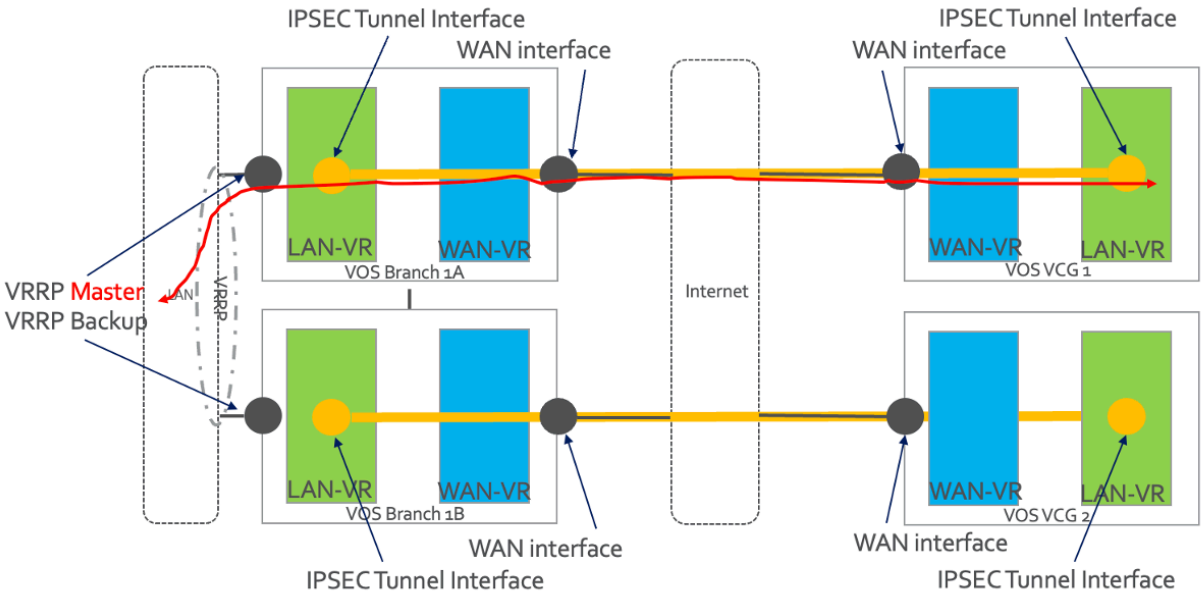
5. Based on the local preference values, the default route should be preferred using the primary VOS VCG. In this example, as expected, the primary route is preferred through 169.254.10.203 (London).



Configure VRRP at the VOS Branch

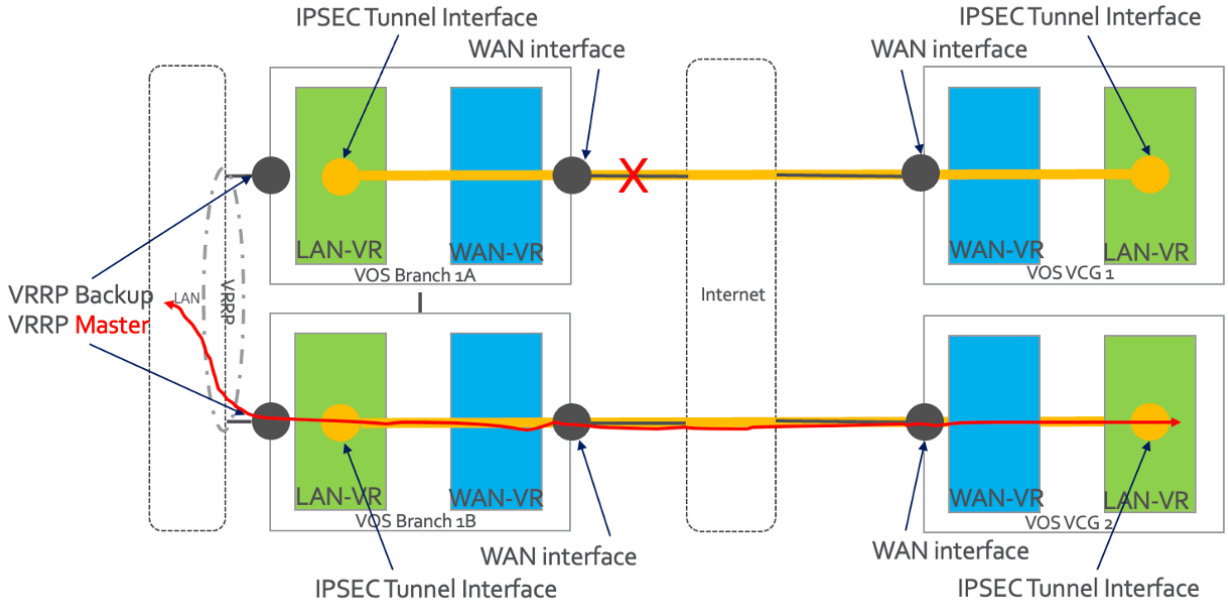
For dual VOS branch deployments, it is recommended the LAN moves to the VOS branch with the active site-to-site tunnel. For example, if the VRRP active device has a site-to-site tunnel to a cloud-hosted Secure Web Gateway and the IPSec tunnel between them fails, VRRP should fail over to the backup CPE. This is illustrated in Figure 13, which shows that the VRRP active device is VOS Branch 1A. Under normal conditions, traffic from the site is forwarded through VOS Branch 1A to VOS VCG 1.

Figure 13: VRRP under Normal Conditions

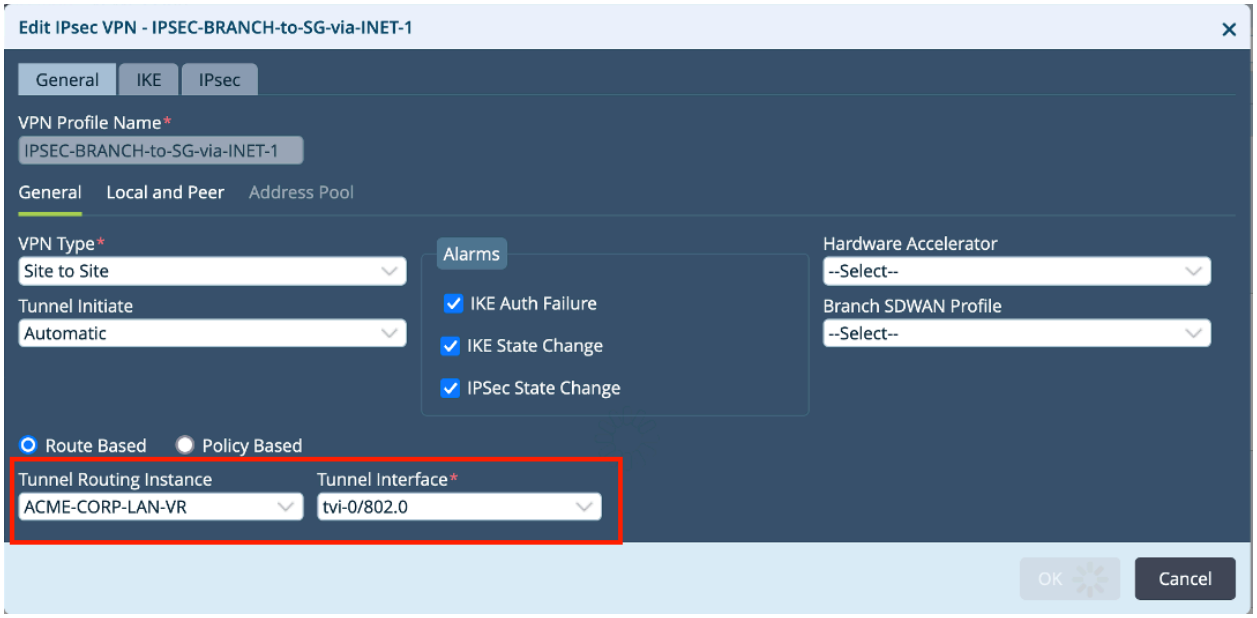


If the site-to-site tunnel between VOS Branch 1A and VOS VCG 1 fails, for example, because of a WAN failure, the VRRP active device switches to VOS Branch 1B. As shown in Figure 14, under failure conditions, traffic from the site is forwarded using VOS Branch 1B to VOS VCG 2.

Figure 14: VRRP under Failure Conditions



We need to explain why a VRRP state change is required. When we configure the IPsec tunnels, we place the tunnel interface in the VOS branch's LAN VR.

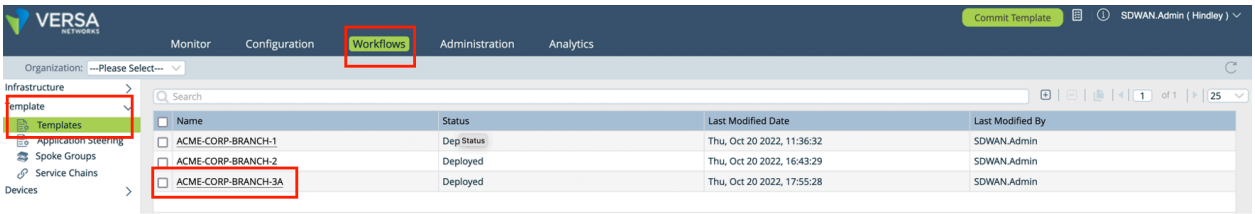


Therefore, end user traffic can be placed into the site-to-site tunnel only if the traffic arrives at the LAN VR from a LAN-facing port. Any other VR is unable to place traffic into the tunnel. For dual VOS branch sites, the LAN VR is accessible only through ports connected to the customer LAN. These ports do not include the interconnect link (that is, the cross-connect) that connects the VOS branches together, which are considered WAN VRFs. Consequently, if the site-to-site IPsec tunnel using the VRRP active device fails, end user traffic arriving from the LAN and destined for the VOS VCG fails to be forwarded to the VOS VCG. To address this, VRRP should track the liveliness of the site-to-site tunnel. Then, if the tunnel fails, VRRP state would fail over to the backup VOS branch.

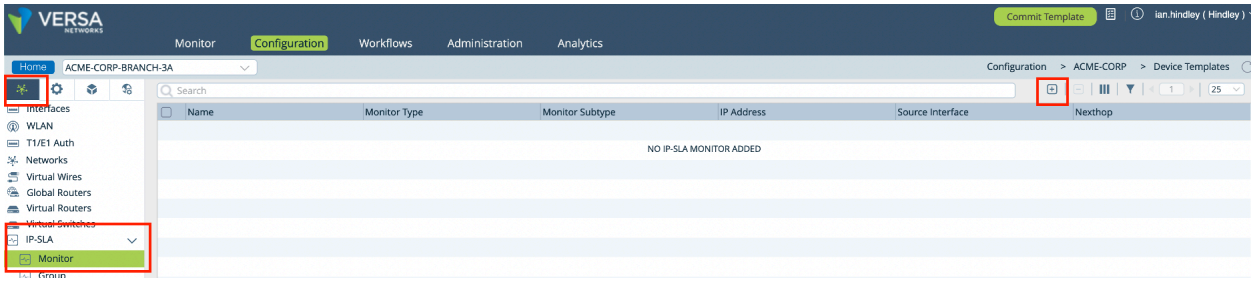
There are several different ways you can configure VRRP tracking for this use case. One such approach is shown below. You should carefully consider all options to ensure that the approach you take is optimized for your network.

As an example, we configure the following on the VRRP active VOS branch:

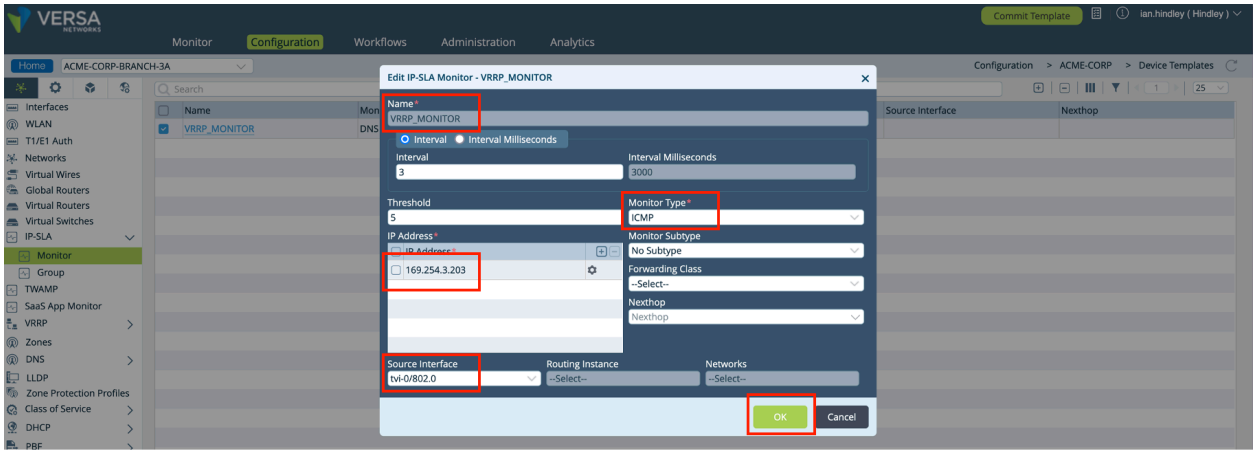
1. Log in to Versa Director
2. Select Workflows > Template > Templates, and then select the template associated with the VRRP active device. In this example, the template is ACME-CORP-BRANCH-3A.



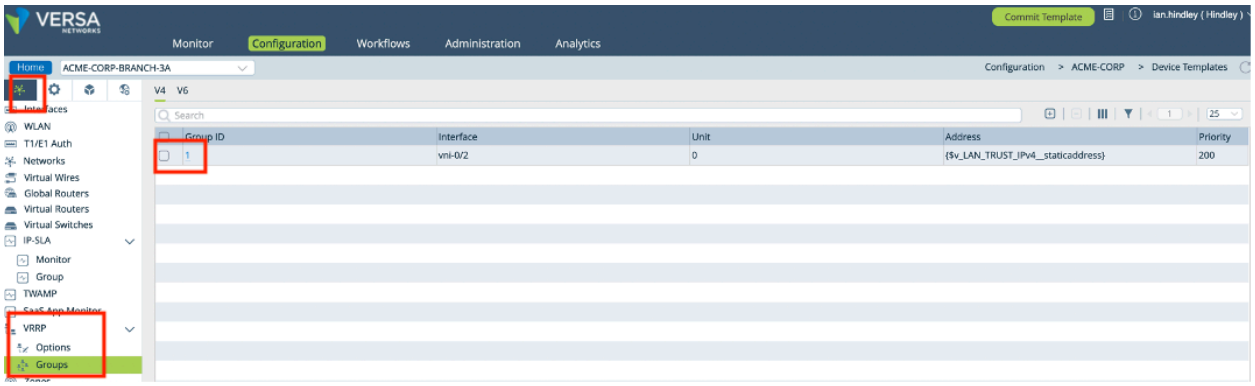
3. Select Networking > IP-SLA > Monitor, and then click the + Add icon.



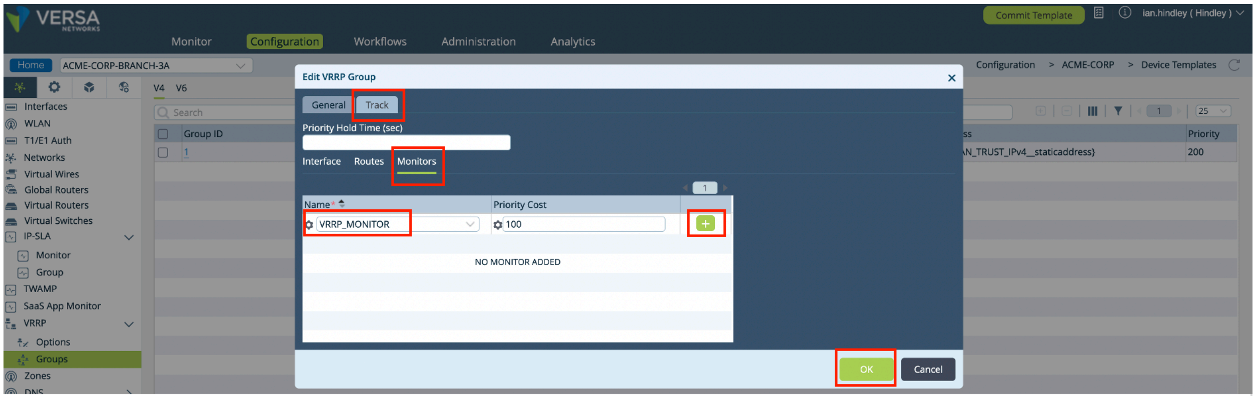
4. Configure the IP-SLA to ping the tunnel IP address (169.254.2.203) of the VOS VCG. Pings are sourced from the TVI interface (tvi-0/802.0) of the VOS branch.



5. Attach the IP-SLA to the VRRP group:. Select Networking > VRRP > Groups, and then select the VRRP Group (in this example it is 1).



6. Select Track > Monitors > Name > *ip-sla-name*, and then click the + Add icon.



7. Click OK.

After you configure VRRP, check the failover times. For reference, based on default timers, it takes around 15-18 seconds for end user traffic originating from the VOS branch to fail over to the backup VOS VCG.

In the screenshot below from the VRRP active VOS branch, the WAN interface is shut at 16:48:51. At 16:49:09, the VRRP state switches to the backup VRRP VOS branch, so the time elapsed is 18 seconds.

```
oam      configChange        2022-10-21T16:48:48+0100 ACME-CORP: Configuration changed : username (admin), context (netconf), time&date (Fri Oct 21 16:48:48 2022)
l2cd     l2LldpNbrChange     2022-10-21T16:48:51+0100 ACME-CORP: LLDP neighbor gi6 from chassis switch9e21c6 Deleted on interface vni-0/0
system   interfaceDown       2022-10-21T16:48:51+0100 ACME-CORP: Interface vni-0/0.0 is down (WAN interface: INET)
system   interfaceDown       2022-10-21T16:48:51+0100 ACME-CORP: Interface vni-0/0 is down (n/a)
system   interfaceUp         2022-10-21T16:48:51+0100 ACME-CORP: Interface vni-0/0.0 is up (WAN interface: INET)
system   interfaceDown       2022-10-21T16:48:51+0100 ACME-CORP: Interface vni-0/0.0 is down (WAN interface: INET)
routing  bfdNbrStateChange   2022-10-21T16:48:51+0100 routing-instance ACME-CORP-LAN-VR: BFD neighbor 169.254.3.203 changed from Up state to Down state
rtd      bgpNbrStateChange   2022-10-21T16:48:51+0100 ACME-CORP: BGP instance 3436: Peer 169.254.3.203 transitioned to Idle state
ipsec    ipsecTunnelDown     2022-10-21T16:49:01+0100 ACME-CORP: IPSEC tunnel with peer 140.238.74.71 (routing-instance INET-Transport-VR, interface tvi-0/802.0, vpn IPSEC-BRANCH-to-SG-via-INET-1) is d
own
vrrp     vrrpv3NewBackup     2022-10-21T16:49:09+0100 ACME-CORP: 192.168.66.1 became BACKUP [interface vni-0/2.0, index 1044, group-id 1] Reason: priority (local 100, remote 150)
rfd      monitorDown         2022-10-21T16:49:16+0100 ACME-CORP: Monitor VRRP_MONITOR (169.254.3.203/ACME-CORP-LAN-VR) is down
rfd      nexthopDown         2022-10-21T16:49:16+0100 ACME-CORP: Nexthop 169.254.3.203/ACME-CORP-LAN-VR is down
ipsec    ipsecIkeDown        2022-10-21T16:49:31+0100 ACME-CORP: IKE connection with peer 140.238.74.71 (routing-instance INET-Transport-VR, interface tvi-0/802.0, vpn IPSEC-BRANCH-to-SG-via-INET-1) is
 down
```

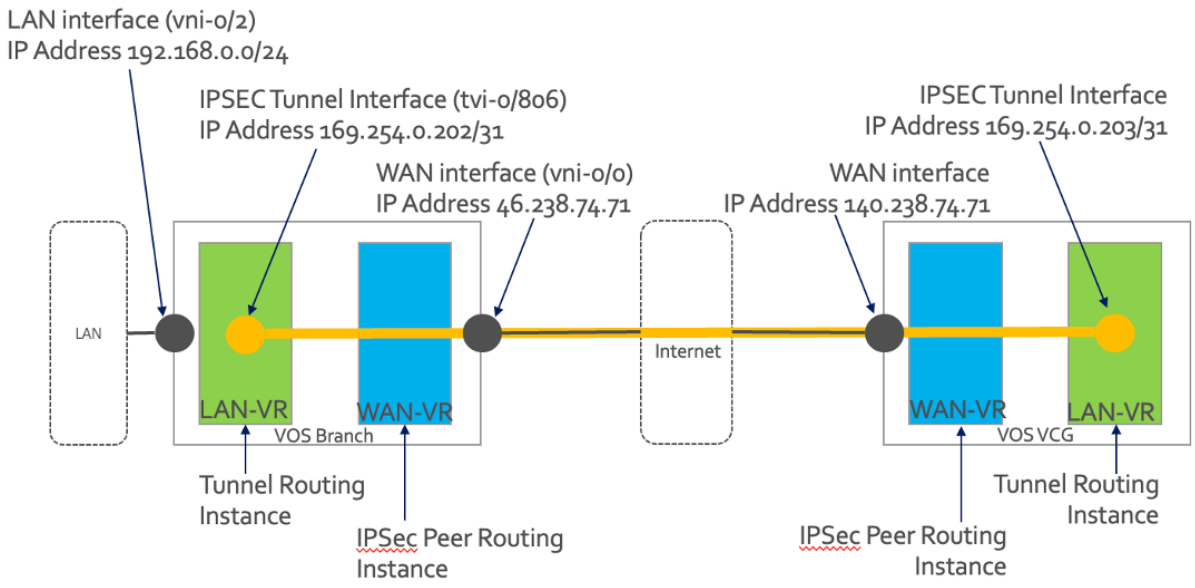
The longest of these timers is VRRP. It defaults to an interval of 3 seconds and a threshold of 5. This means VRRP takes 15-18 seconds to failover.

```
admin@ACME-CORP-BRANCH-3A-cli> show monitor detail VRRP_MONITOR
                                                                          LAST      SOURCE        SUB                            ADDRESS
NAME         VRF              TENANT     STATE  TYPE  INTERVAL  THRESHOLD  FLAPPED   INTERFACE     TYPE  NEXTHOP  ADDRESS        STATE
------------------------------------------------------------------------------------------------------------------------------------------
VRRP_MONITOR ACME-CORP-LAN-VR ACME-CORP  Down   icmp  3000      5          00:13:24  tvi-0/802.0   none  -        169.254.3.203  Down
[ok][2022-10-21 17:02:28]
```

Configure Multiple Site-to-Site Tunnels per WAN Link

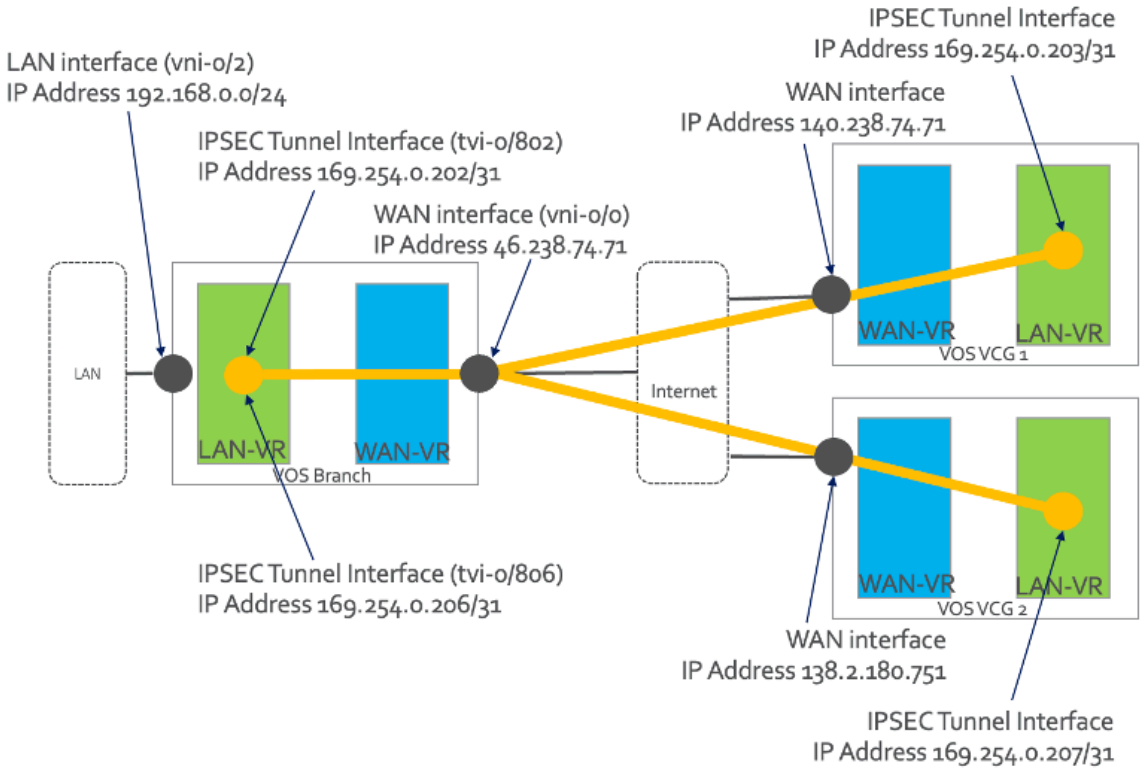
In the topologies described above, in sections Configure a Single-CPE, Single-WAN Topology, Configure a Single-CPE-Dual-WAN Topology, and Configure a Dual-CPE, Dual-WAN Topology sections, above, we build a single site-to-site tunnel per WAN link. For example, in the single-CPE, single-WAN topology, the VOS branch has a single WAN link and over that WAN link is a single site-to-site tunnel, as shown in Figure 15.

Figure 15: Single Site-to-Site Tunnel



It is also possible to configure two or more site-to-site tunnels per WAN link. The advantage of this architecture is that it provides site-to-site resilience per WAN link, albeit at the cost of having more configuration. For example, for geographical resilience between the VOS branch and the VOS VCG, we can build a site-to-site tunnel to the VOS VCG in London (VOS VCG1) as well as Frankfurt (VOS VCG2). This architecture is shown in Figure 16.

Figure 16: Multiple Site-to-Site Tunnels



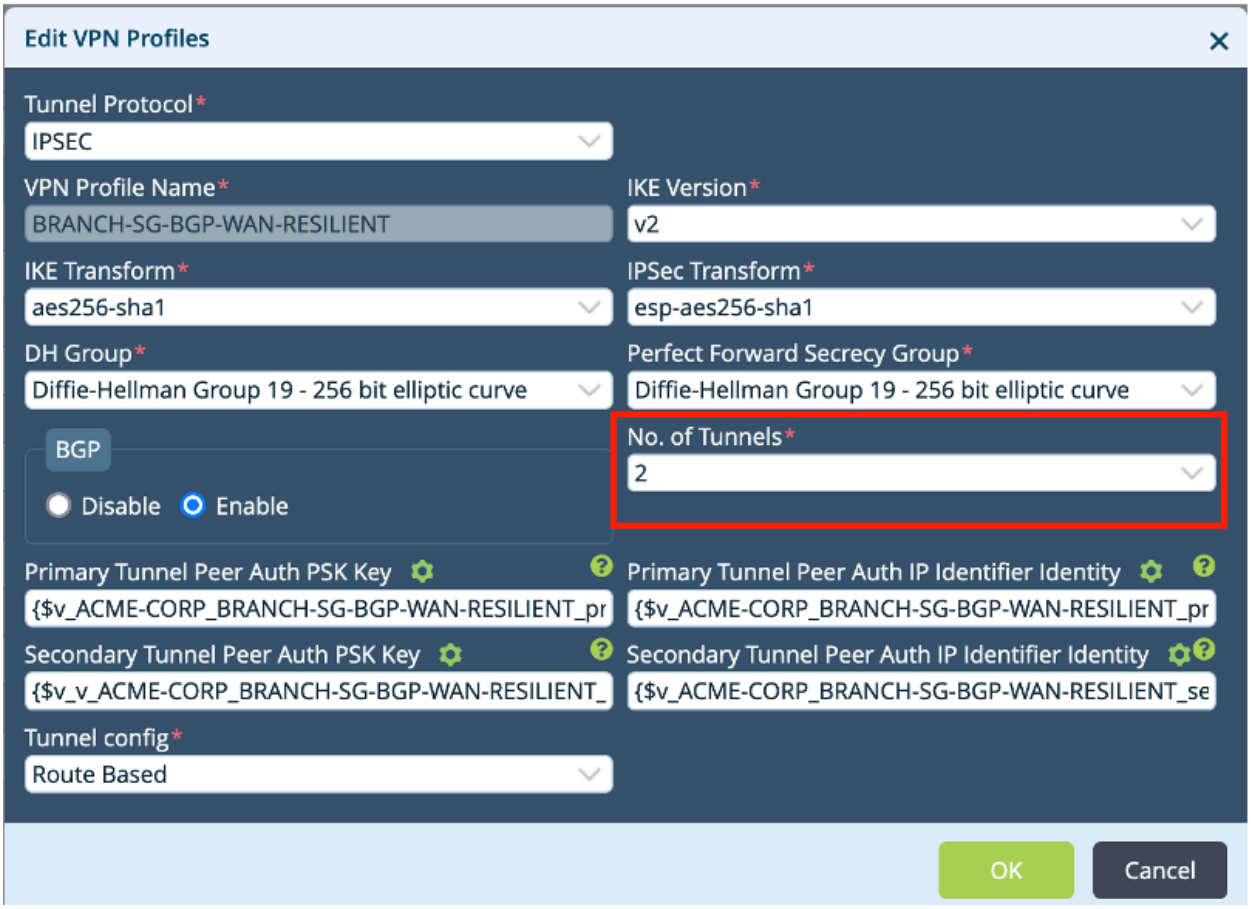
As the figure shows, the VOS branch has two IPsec tunnel interfaces (here, tvi-0/802 and tvi-0/806). One of these tunnels connects to the VOS VCG in London (VOS VCG1), and the other connects to Frankfurt (VOS VCG2). Having two tunnels provides geographical resilience to the VOS branch in the event that connectivity to the VOS VCG in London is lost.

Although the example here shows two site-to-site tunnels, you can configure any number of tunnels that use each WAN link to achieve your target architecture.

There are two approaches to configuring multiple site-to-site WAN links in Versa Director:

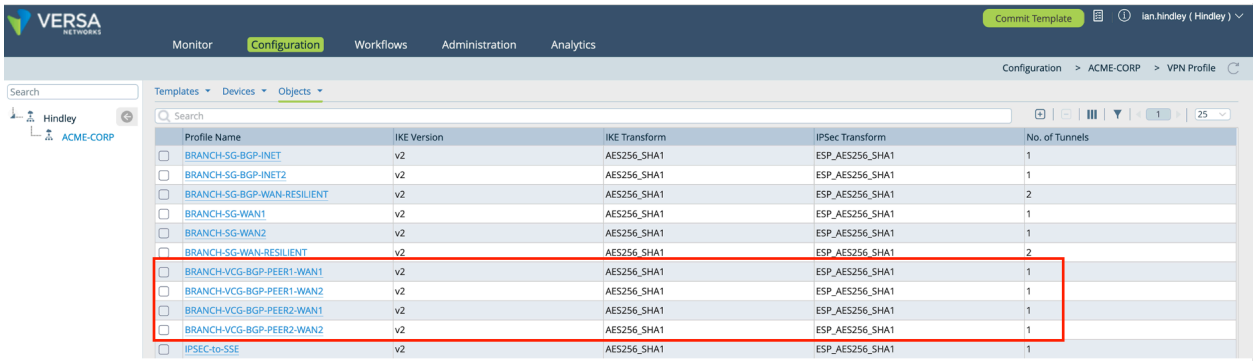
- Configure one tunnel per VPN profile
- Configure two tunnels per VPN profile

You configure this option in the Number of Tunnels field when you configure a VPN profile In this field, the allowable values are 1 and 2.

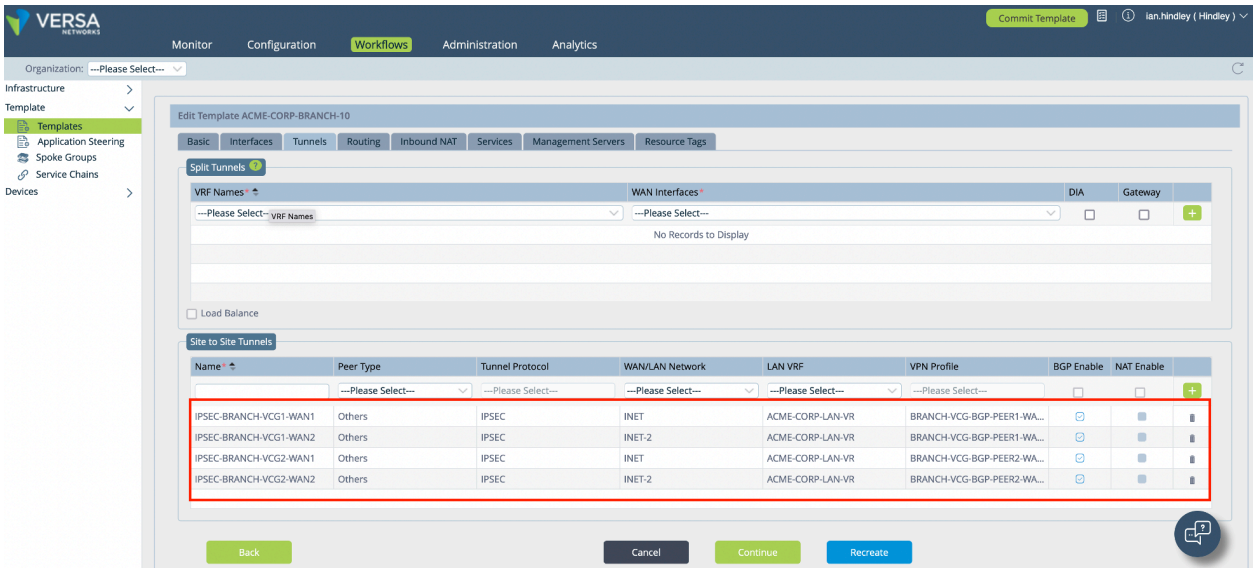


It is strongly recommended that you use the first approach, which configures one site-to-site tunnel per VPN profile. Configuring only one tunnel per VPN profile makes BGP Policy much simpler. Each VPN profile automatically creates a BGP peer/group, so with this approach there is a single BGP peer per peer/group. Changing a BGP attribute is then simple, because the change applies only to that BGP peer. In contrast, if there are two tunnels per VPN profile, the BGP peer/group has two peers, so to control routing, you need to modify BGP policy from the group level to the peer level, which results is a more complex configuration.

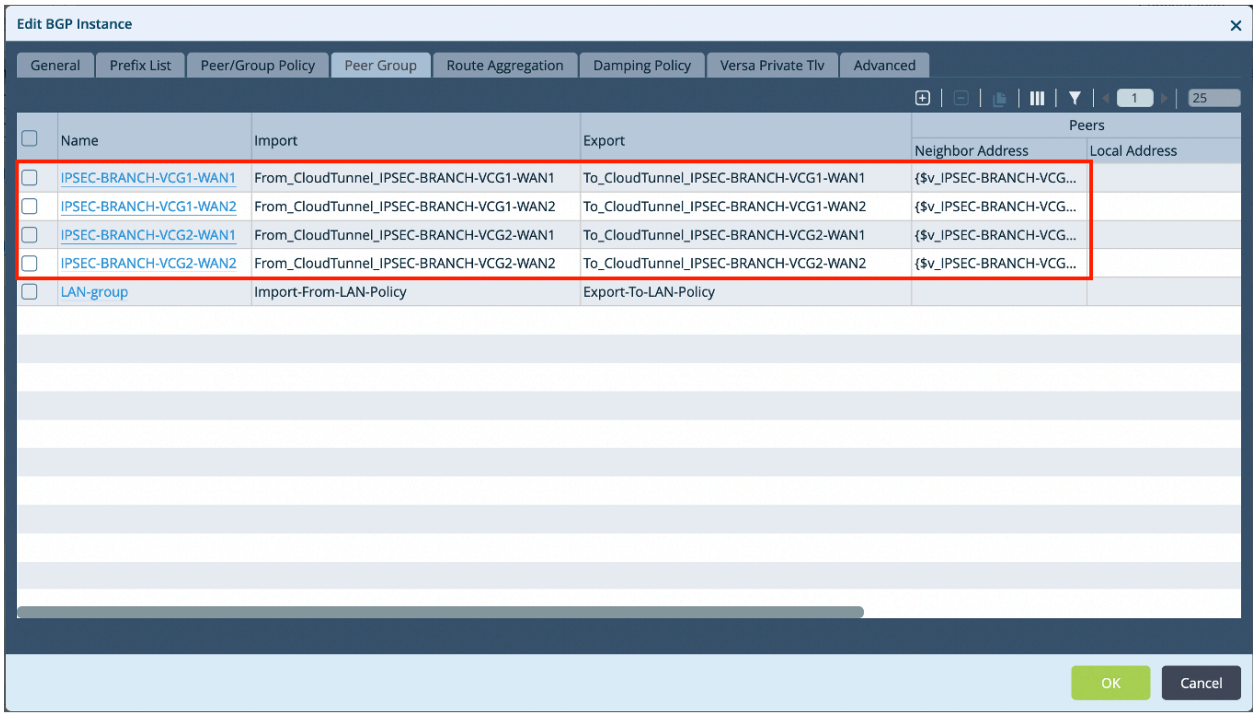
Assuming that you adopt the recommended approach, an example deployment could use the following VPN profiles. In this example, the enterprise wants to connect to two VCGs per VOS branch to provide geographical resilience. Additionally, the VOS branch is configured with two WAN links. Therefore, the enterprise creates a total of four VPN profiles (that is, four site-to-site tunnels) are created, as shown in the following screenshot. Note that the naming scheme of the VPN profiles should help you determine which VPN profile is associated with which VCG peer and which WAN link.



You then use a Workflow template to associate the VPN profiles with VOS branches. In the example here, the VOS branch is a single CPE with two WAN links. Because there are two IPsec peers (that is, two VCGs), we attach all four VPN profiles shown above to the Workflow template.

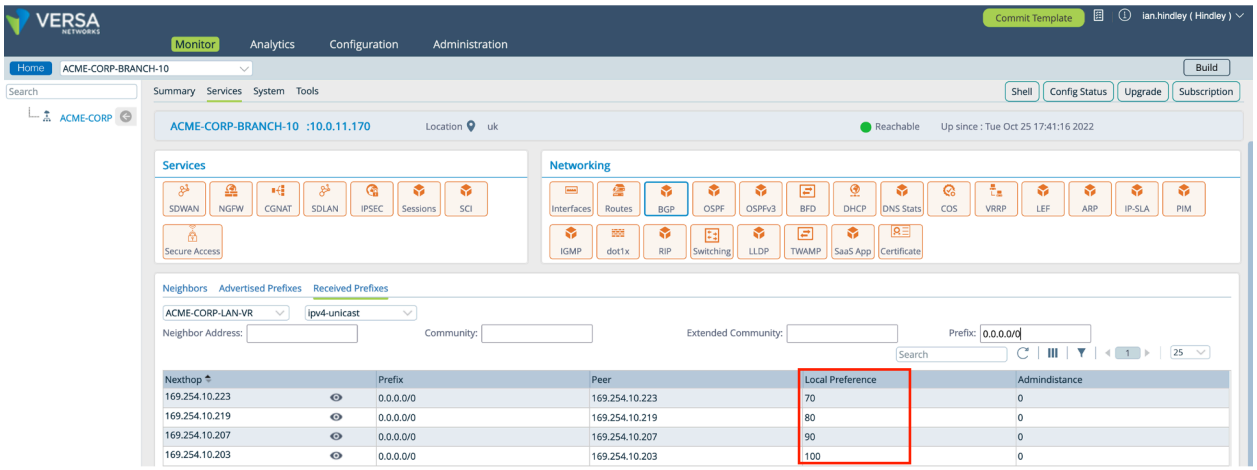


This approach creates four BGP peers. Each peer has two BGP policies to control inbound and outbound routing from the VOS branch to the VOS VCG. The following screenshot shows each import and export policy for each BGP peer.



For the import policy, we adjust the local preference. The default is 100. We leave the primary IPsec tunnel/BGP peer to use the default. We assign a value of 90 to the second preferred path/peer, we assign a value of 80 to the third preferred path/peer, and we assign a value of 70 to the fourth preferred path/peer. The larger the local preference value, the more preferred the route.

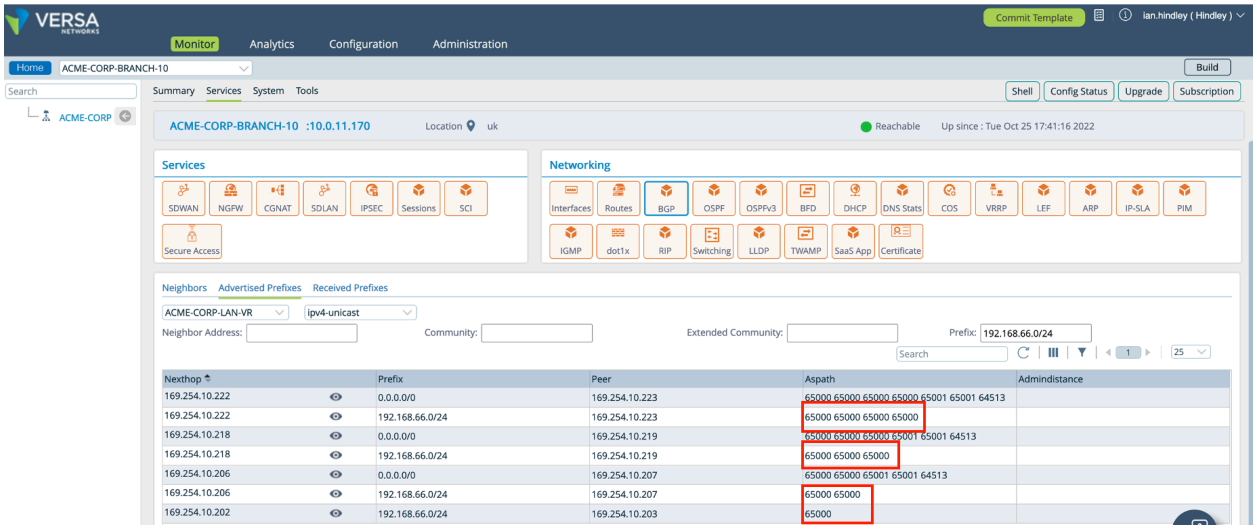
For this example, on the VOS branch, we can see that the local preference values of the default route received over the four IPsec tunnels range from 100 to 70, with 100 being the most preferred.



For the export policy, we adjust the AS path length. The default is no path prepending. We leave the primary IPsec tunnel/BGP peer to use the default. The second preferred path/peer prepends two of its local AS numbers to the advertised path. The third preferred path/peer prepends three of its local AS numbers to the advertised path, and the

fourth preferred path/peer prepends four of its local AS numbers to the advertised path. The shorter the AS path length, the more preferred the route.

For this example, on the VOS branch, we can see the AS path length for the VOS branch LAN address range 192.168.66.0/24. AS paths vary from one to four, with one being the preferred path from the perspective of the VOS VCG. The most preferred path is advertised to Peer 1 over WAN 1. Therefore, traffic from the VOS VCG traverses this tunnel to reach the network 192.168.66/24, which is hosted on the VOS branch.



The following table summarizes the BGP policy described in this section.

Table 2: Sample BGP Policy

VPN Profile Name	AS Path Prepend	Local Preference Adjustment	Site-to-Site Tunnel Preference
BRANCH-VCG-BGP-PEER1-WAN1	No Example: 65000	No Example 100	Primary site-to-site tunnel
BRANCH-VCG-BGP-PEER1-WAN2	Yes Example: 65000, 65000	Yes Example 90	Secondary site-to-site tunnel
BRANCH-VCG-BGP-PEER2-WAN1	Yes Example: 65000, 65000, 65000	Yes Example 80	Tertiary site-to-site tunnel

VPN Profile Name	AS Path Prepend	Local Preference Adjustment	Site-to-Site Tunnel Preference
BRANCH-VCG-BGP-PEER2-WAN2	Yes Example: 65000, 65000, 65000, 65000	Yes Example 70	Quaternary site-to-site tunnel

For more information about configuring BGP, see Configure BGP Policy, above.

Note that if dual CPEs use VRRP on the LAN side at the site and there are two or more site-to-site tunnels per WAN link, a minimum of four site-to-site tunnels originate from the site.

For VRRP at the site, ensure that you configure two IP SLAs. One IP SLA polls the primary VOS VCG. If this tunnel fails, the VOS branch decrements its VRRP priority by, for example, 50. VRRP does not fail over to the VRRP backup, because the VRRP active device can still, in theory, reach the backup VOS VCG. The second IP SLA polls the backup VOS VCG. If this tunnel fails, the VRRP priority is decremented by, for example, 50. Only if the VRRP active device cannot reach either the primary or backup VOS VCG does VRRP switch over to the VRRP backup. For more information, see Configure VRRP at the VOS Branch, above.

Advertise Networks between the VOS VCG and the VOS Branch

There may be several use cases in which connectivity between Secure SD-WAN and SWG or between VSA and Secure SD-WAN is required at multiple points in a SASE architecture. In such circumstances, it is perfectly feasible to build site-to-site tunnels between all Secure SD-WAN branches and SWG/VSA. However, it may also be beneficial to use a fewer number of interconnects. In such an architecture, networks need to be advertised between VOS VCG and VOS branch to provide connectivity.

This section explores a couple of use cases and how to advertise networks between Secure SD-WAN and SSE.

Site-to-site IPsec tunnels must be built between two static IP addressed devices. For VOS VCGs, the IP addresses are always statically assigned. However, for customers whose VOS branch IP addresses are dynamically assigned, this is more problematic because the addresses are dynamically assigned and therefore not static.

For such deployments, there are two alternative architectures:

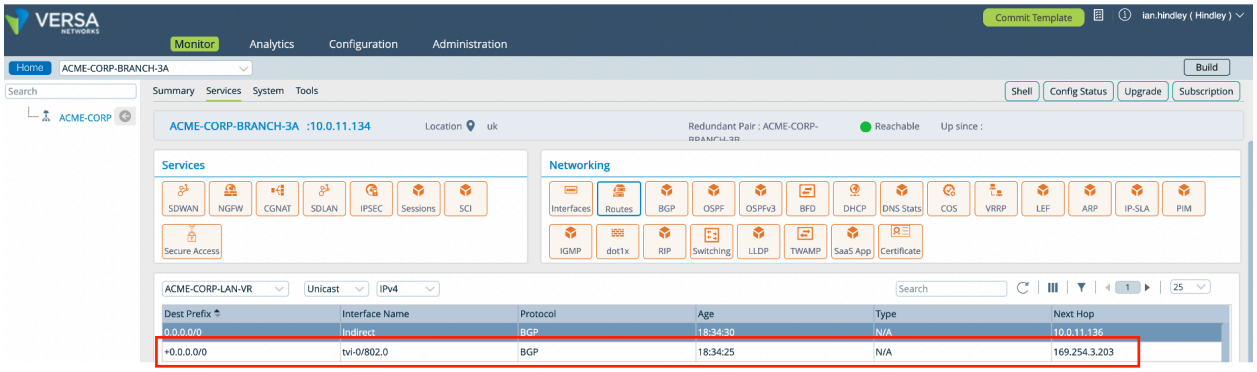
- Register the WAN interface of the VOS branch with a dynamic DNS service and configure the site-to-site tunnel using an FQDN.
- Allow VOS branches with dynamic addresses to use Secure SD-WAN to connect to other VOS branches that use static IP address assignment. Its these transit VOS branches that are configured with site-to-site tunnels to the VOS VCGs

This section describes this second architecture in more detail.

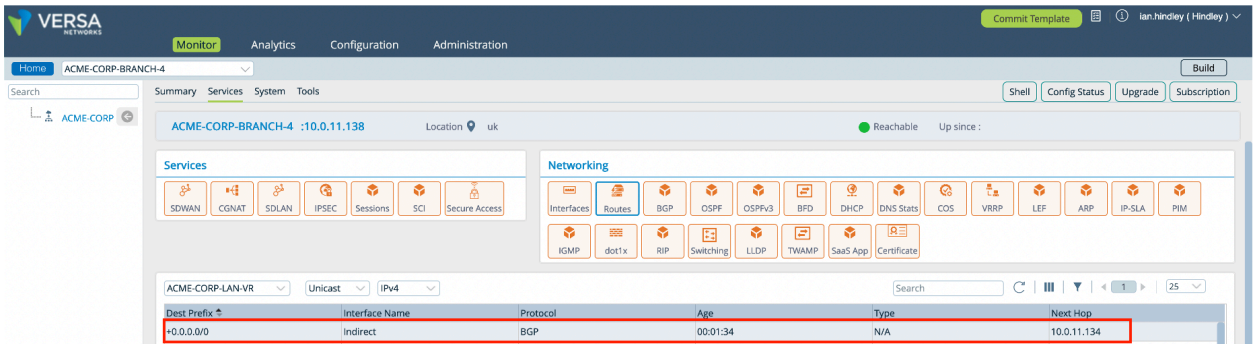
To minimize the number of site-to-site tunnels between VOS branches and VOS VCGs, you can build a few key VOS branches that have site-to-site tunnels to the VOS VCGs. In such an architecture, the VOS branches directly connected to the VOS VCGs act as transit, or hub, devices for all the other branches in the Secure SD-WAN.

By default, routes received from the VOS VCG are automatically advertised to other Secure SD-WAN VOS branches. The advertising is achieved using a BGP policy on the VOS branch directly connected to the VOS VCG through the site-to-site IPsec tunnel.

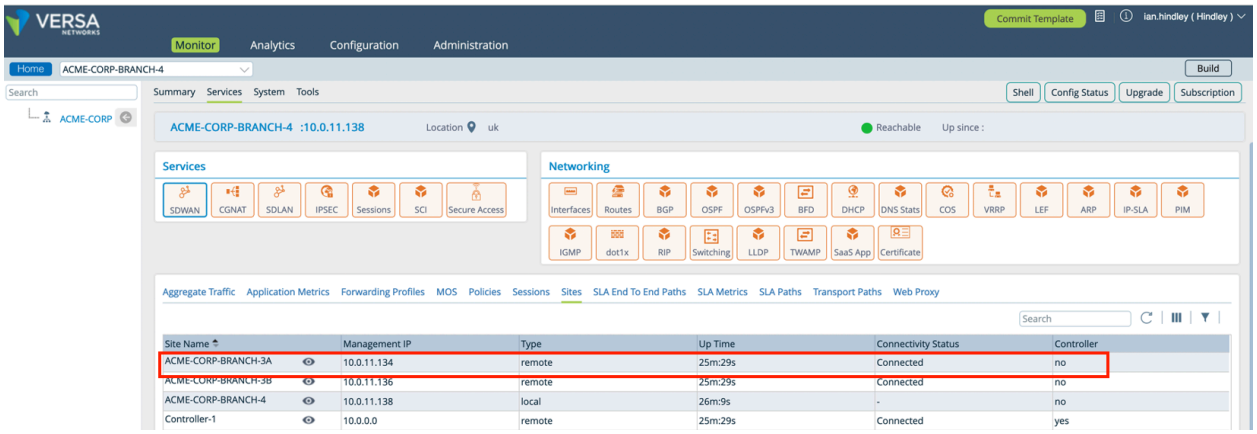
As an example, ACME-CORP-BRANCH-3A has 0/0 in its routing table through the IPsec tunnel (169.254.3.203), which is the preferred route, as indicated by the + sign and through ACME-CORP-BRANCH-3B (10.0.11.136).



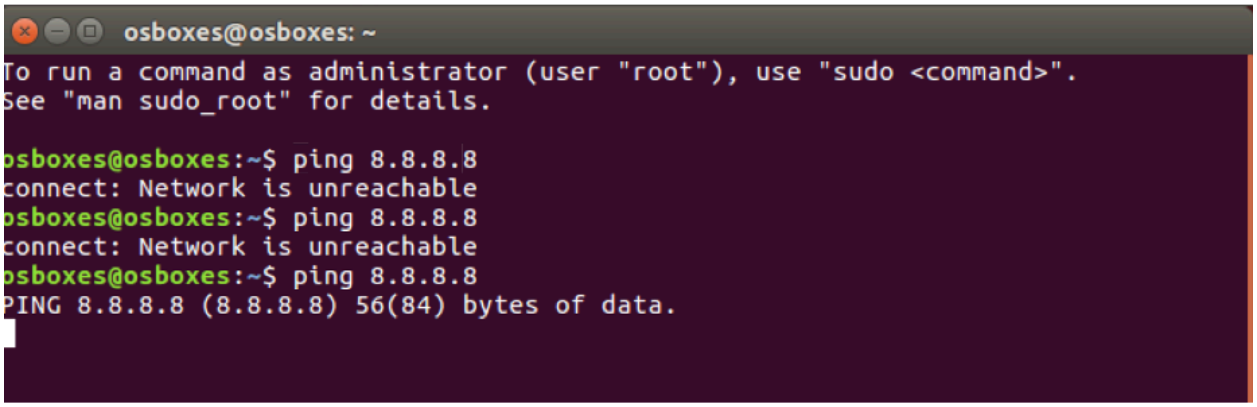
The default route in this example is advertised by this VOS branch to all other VOS branches in the network, even though the other branches are not directly connected to the VOS VCG. In effect, ACME-CORP-BRANCH-3A becomes a transit router in routing terms between the branches connected to the Secure SD-WAN and the VOS VCG. To demonstrate this, here's the routing table of ACME-CORP-BRANCH-4:



The default route next hop is 10.0.11.134. This next-hop is the transit VOS branch that provides onward connectivity to the VOS VCG:

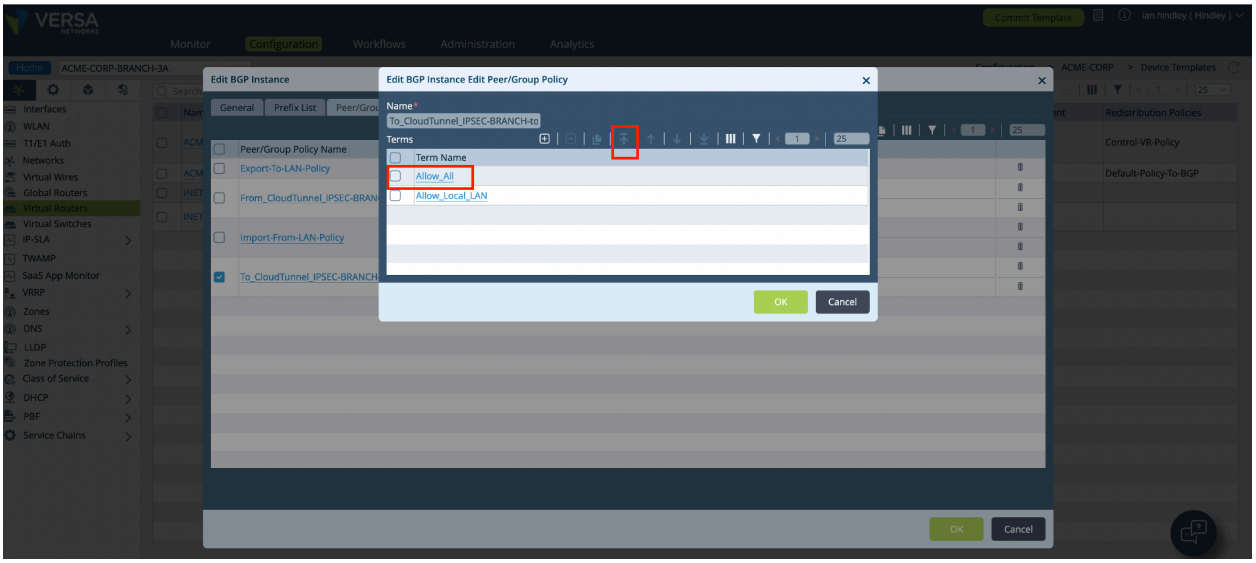


However, pings from an end user connected to ACME-CORP-BRANCH-4 to the internet fail:



The pings fail because the BGP policy on the transit router (ACME-CORP-BRANCH-3A) is advertising only its own directly connected LAN network to the VOS VCG over the site-to-site tunnel. To advertise all the other LANs of the Secure SD-WAN, we need to make the following configuration changes to reorder the policy rules:

1. Select the transit VOS branch device template.
2. Select Networking > Virtual Routers > *lan-vrf* > BGP > *bgp-instance-id* > Peer/Group Policy.
3. Select To_CloudTunnels_*ipsec-tunnel-name*.
4. Click Allow_All.
5. Select the Up arrow to reorder the rules. The idea here in reordering the rules, is that Allow_All needs to go above the Allow_Local_LAN. Allow_Local_LAN blocks the other Secure SD-WAN routes from being advertised by the transit router to the VOS VCG. By reordering the rules, the entire VOS branch address space is advertised.
6. Click OK three times.



Alternatively, you can build policy to select which VOS branch subnets to advertise to the VOS VCG. Just place this new rule at the top of the rule list. The deny goes next, to blocks all other Secure SD-WAN subnets. And finally, the Allow_All goes at the bottom to permit the local LAN of the transit router to be advertised to the VOS VCG.

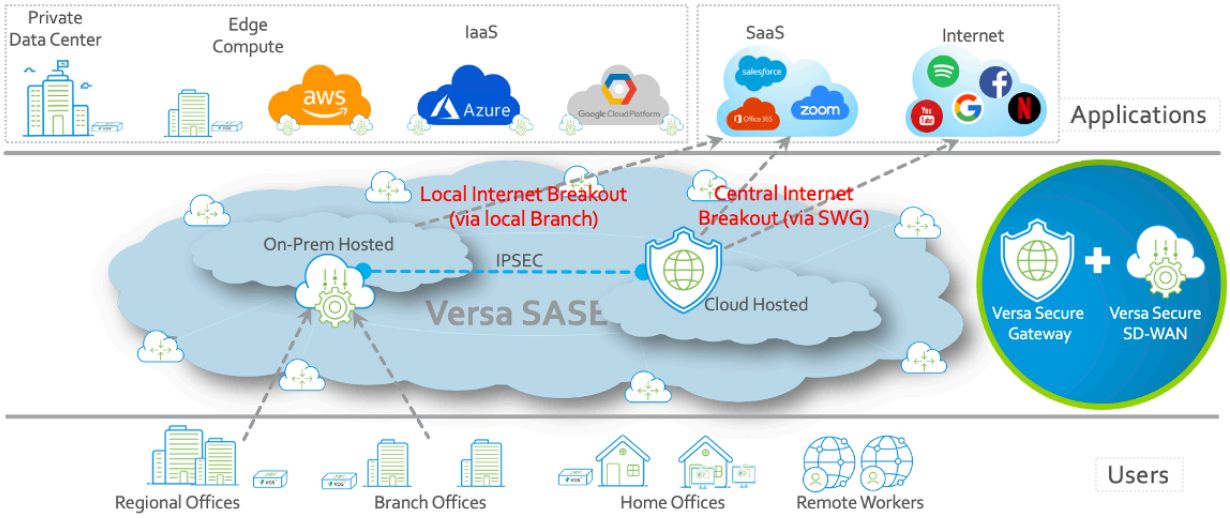
Once the subnet of the remote Secure SD-WAN site is advertised by the transit router to the VOS VCG, connectivity between an end user connected to a Secure SD-WAN site and the internet is built. To demonstrate, here's a successful ping from the end user to Google's DNS server through the SWG.

```
osboxes@osboxes: ~
osboxes@osboxes:~$
osboxes@osboxes:~$
osboxes@osboxes:~$
osboxes@osboxes:~$
osboxes@osboxes:~$
osboxes@osboxes:~$
osboxes@osboxes:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=187 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=166 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=167 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=167 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=168 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=117 time=166 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=117 time=167 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=117 time=165 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=117 time=168 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=117 time=166 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=117 time=175 ms
^C
--- 8.8.8.8 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10012ms
rtt min/avg/max/mdev = 165.100/169.588/187.024/6.053 ms
osboxes@osboxes:~$
```

Configure LBO and CBO through the VOS VCG

One of the advantages of Secure SD-WAN is the ability to break out trusted internet applications at the local VOS branch. This is known as LBO, or local internet breakout. You can prefer LBO to backhauling the traffic to a remote VOS branch for central internet breakout, also known as CBO. As shown in Figure 17, internet or SaaS destined traffic can still leverage LBO at the VOS branch. All other untrusted internet traffic that requires the additional features of the SWG can be forwarded to the VOS VCG. Figure 17 illustrates this architecture, and this section describes how to configure it. For more information, see VOS Edge Device Direct Internet Access.

Figure 17: CBO through SWG and LBO through Local Branch



On the VOS branch:

1. Configure a site-to-site tunnel or site-to-site tunnels, as described in Configure a Single-CPE, Single-WAN Topology, Configure a Single-CPE, Dual-WAN Deployment, or Configure a Dual-CPE, Dual WAN Deployment, above.
2. Configure Local Breakout, as described in VOS Edge Device Direct Internet Access.

On the VOS VCG:

1. Configure a site-to-site tunnel or site-to-site tunnels, as described in Configure a Single-CPE, Single-WAN Topology, Configure a Single-CPE, Dual-WAN Deployment, or Configure a Dual-CPE, Dual WAN Deployment, above.
2. Configure firewall rules as described in Configure Firewall Rules on Concerto from the VOS Branch to the VOS VCG, above. These rules are used for CBO traffic.

Modify the VOS Branch TVI IP Addressing

When you use Workflow templates, Versa Director automatically creates tunnel virtual interfaces (TVI) and allocates IP

addresses to these tunnel interfaces from the range 169.254.0/24.

There are two potential issues that may drive the need to change this default behavior:

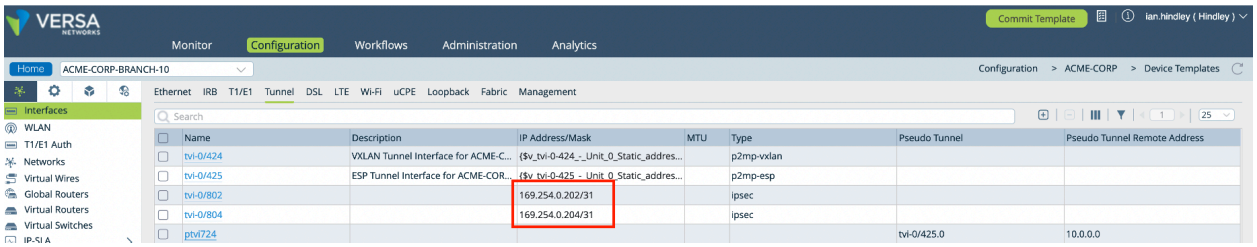
- TVI interfaces reside in the organization LAN VR. Therefore, the 169.254.0/24 address range can be used only if it is unique across the organization. If this address range is already in use, you must re-address the TVI interfaces to avoid IP address clashes.
- If VOS Branches A and B are configured with a site-to-site tunnel to the VOS VCG, VOS Branch A uses the range 169.254.0.0/31, and VOS Branch B uses the same range. While this is not an issue on the VOS branches, it is an issue on the VOS gateway. The VOS VCG is effectively configured with two site-to-site tunnels, one for Branch A and one for Branch B, and both interfaces use the same IP addressing. As a result, the VOS VCG rejects the configuration, because two or more interfaces in the same VR cannot use the same IP address. So, if there are multiple site-to-site tunnels terminating on the same VOS gateway, you must re-address the TVI interfaces to avoid IP address clashes

This section describes how to reconfigure the TVI IP addressing, showing the following:

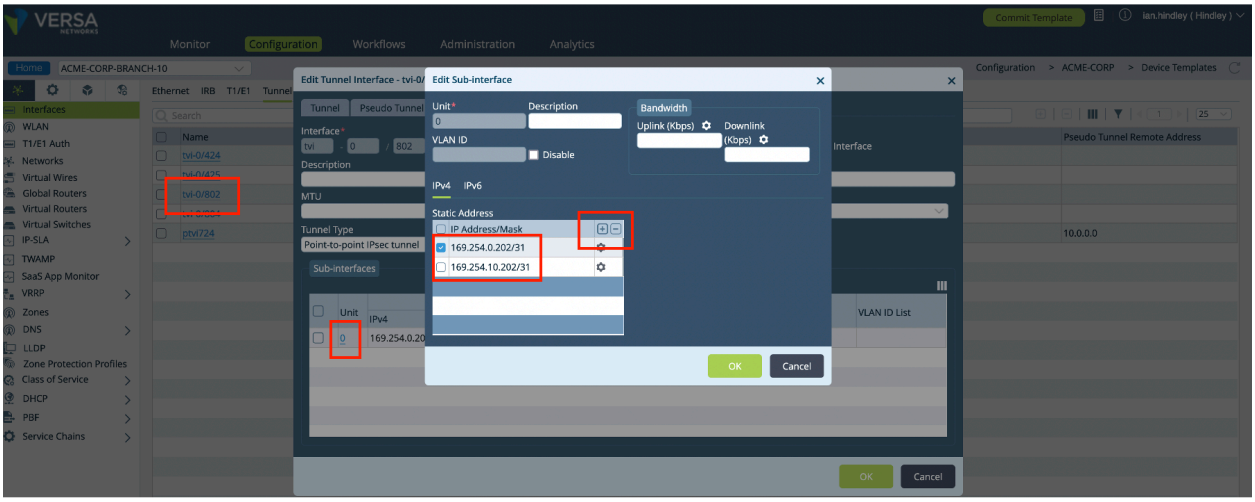
- How to change the default IP addressing allocated using the Workflow template on Versa Director to a unique IP address.
- How to amend static routes that are automatically configured by the Workflow template. Note that it does not matter whether the VPN profile uses BGP or static routes. Static routes are autoconfigured and must be changed to reflect the new IP addressing scheme used on the TVI interface or interfaces.

To reconfigure the TVI IP addressing:

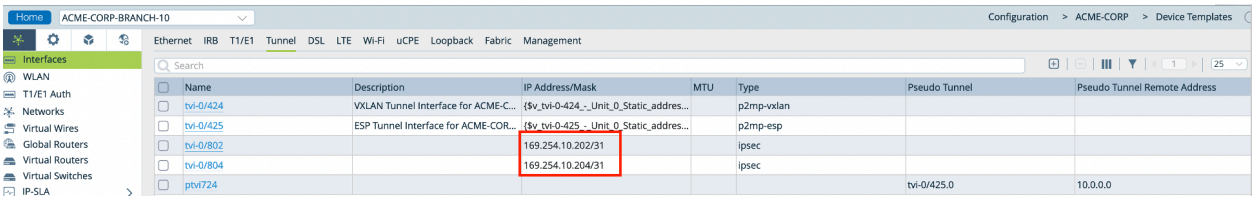
1. Log in to Versa Director.
2. We have ACME-CORP-BRANCH-10 using Workflow templates, as described in this article. This branch has one WAN link and two site-to-site tunnels to two VOS VCGs.
3. From the screenshot below, we can see that IP addressing has been automatically assigned to the VOS branch in the 169.254.0/24 range.



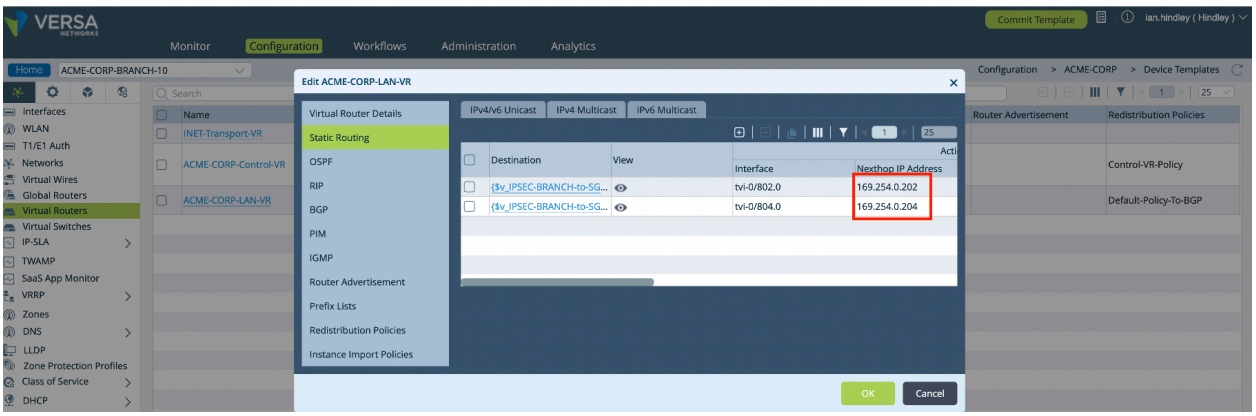
4. To change the IP addresses:
    a. Select the TVI, here, tvi-0/802.
    b. Select Unit 0.
    c. Click the + Plus sign.
    d. In the Static Address field, enter the new TVI IP address.
    e. In the Static Address field, select the old TVI IP address.
    f. Click the - Minus sign.
    g. Click OK, and then click OK a second time.



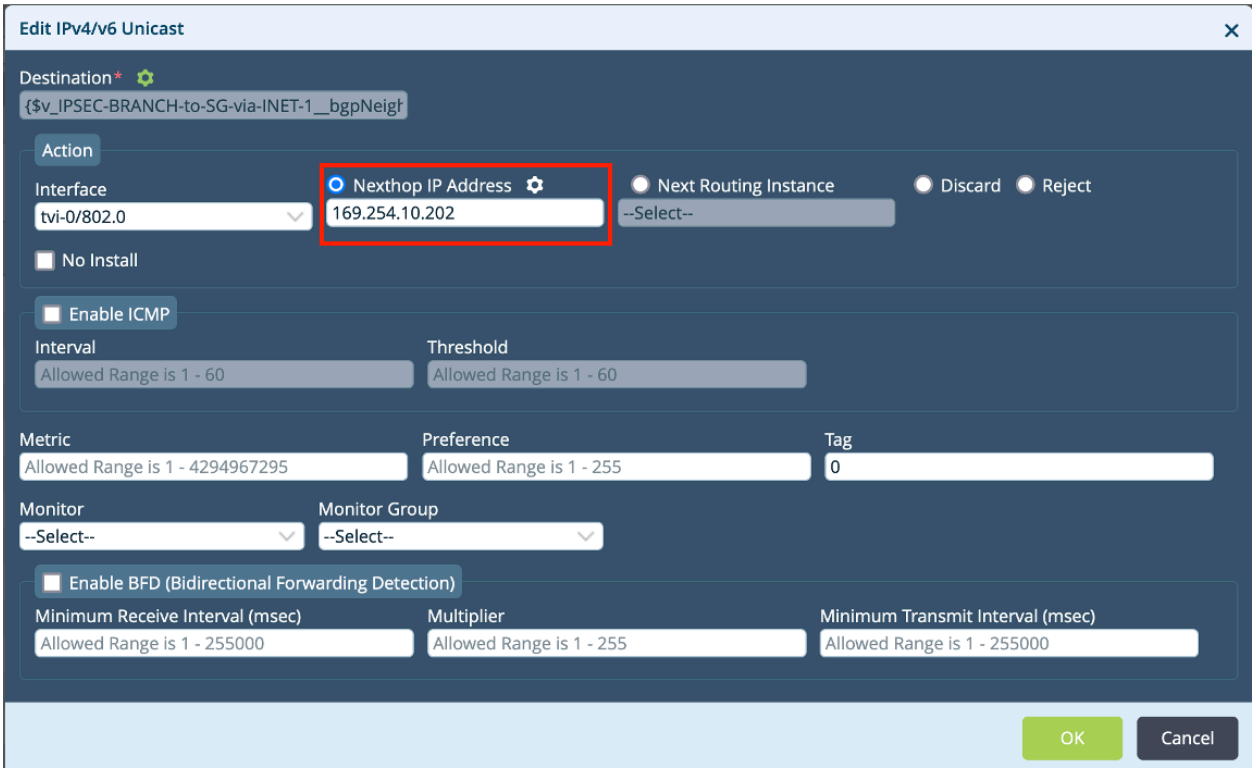
5. Repeat Step 4 for any other TVI interfaces on the VOS branch that require re-addressing.
6. As shown in the following screenshot, both TVI interfaces for this example have been re-addressed from 169.254.0.202/31 and 169.254.0.204/31 to 169.254.10.202/31 and 169.254.10.204/31, respectively.



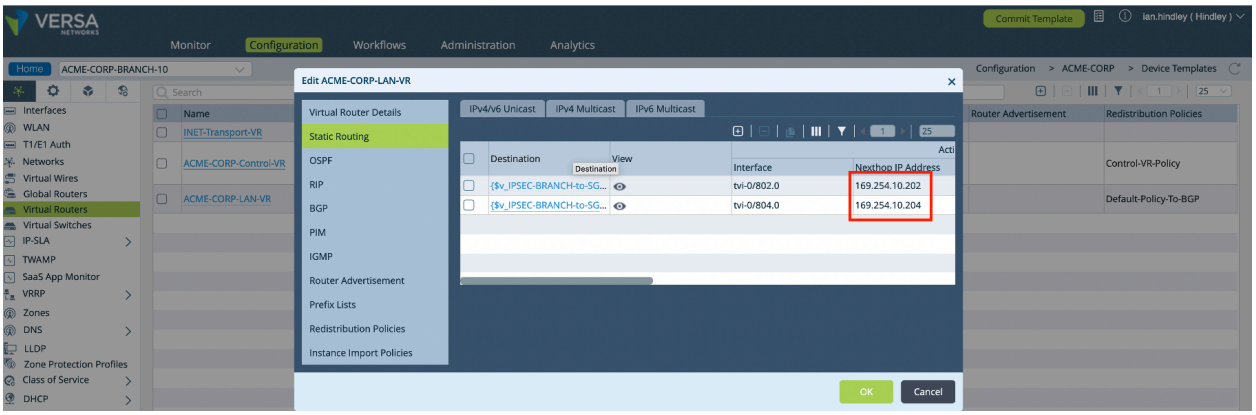
7. The Workflow template also creates static routes. The next-hop IP addresses need to be changed, as shown in the following screenshot. Currently, these are the incorrect next-hop IP addresses for ACME-CORP-BRANCH-10. They need to be changed from 169.254.0.202/31 and 169.254.0.204/31 to 169.254.10.202/31 and 169.254.10.204/31, respectively.



8. Select the first site-to-site tunnel from the list by clicking on $v_. or the equivalent name in your setup.
9. Change the Next-Hop IP Address from the original TVI IP address to the new TVI IP address. In this example, we are changing the TVI IP address from 169.254.0.202 to 169.254.10.202. Therefore, the next hop is 169.254.10.202.
10. Click OK.



11. Repeat the same steps for any other TVI interfaces on the VOS branch that require re-addressing.
12. As shown in the following screenshot, both next-hop IP addresses in this example have been re-addressed from 169.254.0.202 and 169.254.0.204 to 169.254.10.202 and 169.254.10.204, respectively.



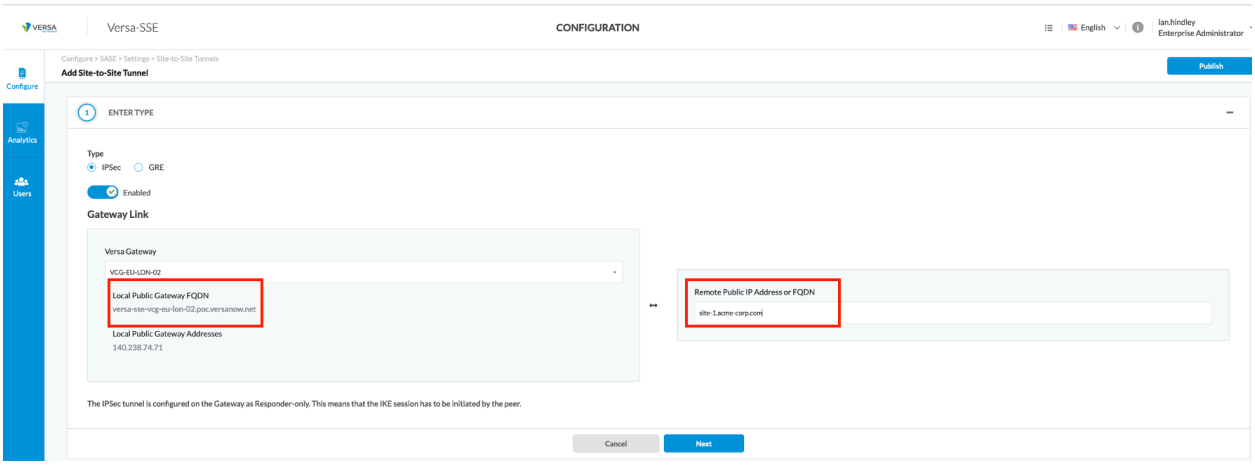
13. Click OK
14. To apply the site-to-site configuration to the VOS branch, follow the normal process to Commit Template.

Configure with FQDNs

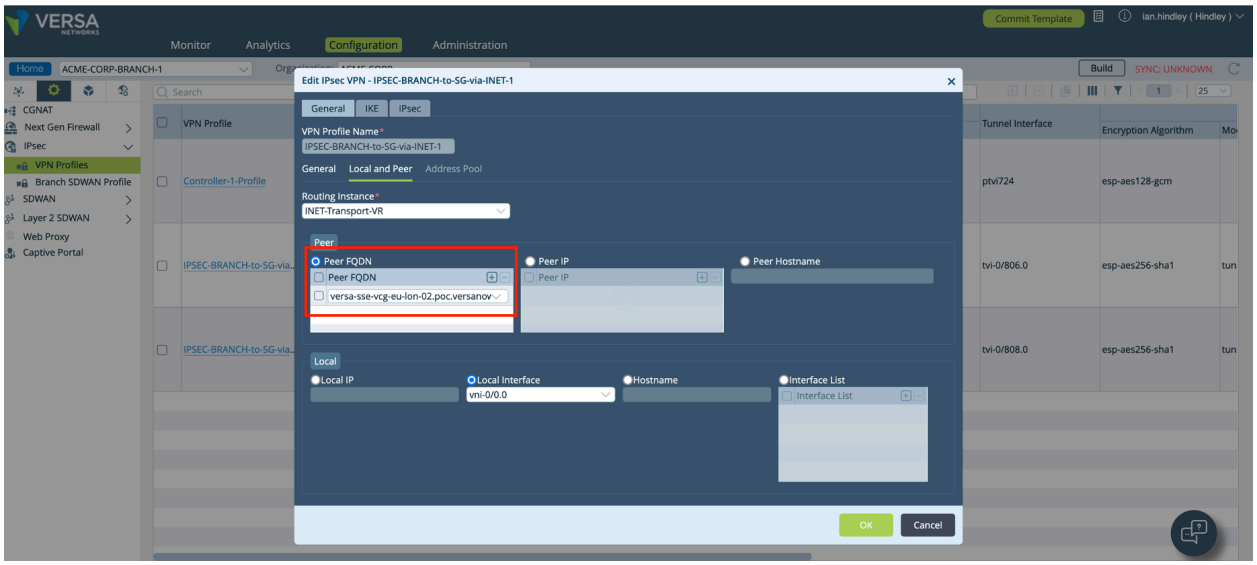
Although this article references IP addresses when configuring IPsec peers, it is recommended that you use FQDNs. There are several reasons for this recommendation:

- From a VOS Branch perspective, for customers whose VOS branch WAN interfaces are assigned by DHCP, configuring Concerto to build site-to-site tunnels to connect to a static IP address of the VOS branch can be problematic, because DHCP address are not static. If the VOS branch IP address ever changes, the site-to-site tunnel will fail. To circumvent this issue, you register the WAN interface of the VOS branch with a dynamic DNS service and then configure the site-to-site tunnel to use an FQDN.
- From a VOS VCG perspective, it cannot be guaranteed the WAN IP address of the VOS VCG remains the same throughout its lifecycle. Therefore, should it ever change, the site-to-site tunnel will fail. By configuring the FQDN rather than the IP address of the VOS VCG, customers do not need to change their site-to-site configuration. Instead, Versa Networks changes the A record in DNS, which effectively retires connectivity over the existing WAN IP and migrates over to the new IP address. Note that customers are notified by a Maintenance Request from the Versa Global Support Center if the need arises for Versa Networks to change the WAN IP address of the VCG. This allows customers to make the necessary changes to VOS branches configured with site-to-site tunnels that use an IP address rather than a FQDN.

For example, in Concerto, when configuring the site-to-site tunnel from the VOS VCG to the VOS branch, specify the FQDN of the VOS branch rather than its IP address. In this example, the WAN interface of the VOS branch is site-1.acme-corp.com, as highlighted in the solid red box:



You can also note that the FQDN and the IP address of the VOS VCG are displayed in the screenshot above below the red boxes. You can enter this information in the VPN profile for the VOS branch that you create on Versa Director, as shown in the following screenshot.



Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Configure Site-to-Site Tunnels
VOS Edge Device Direct Internet Access