
Configure Site-to-Site Tunnels



For supported software information, click [here](#).

Site-to-site tunnels provide a way to encapsulate packets inside of a transport protocol. You configure a tunnel as a virtual interface that provides the services necessary to implement any standard point-to-point encapsulation scheme.

You can create secure IPsec tunnels and generic routing encapsulation (GRE) tunnels between a Versa Operating System™ (VOS™) CPE device and a device hosted in the cloud, in a data center, or by an SSE provider, to optimize the connectivity between the VOS device and cloud peer devices. The VOS CPE device can be either a physical device or a cloud-based SD-WAN device. The peer device can be a cloud-managed service or a third-party device that supports IPsec tunnels.

The site-to-site IPsec tunnel provides VOS device users with secure access to applications and workloads hosted in the cloud. When you create a site-to-site IPsec tunnel between a VOS device and a managed virtual WAN, no manual IPsec tunnel and VPN configuration is required on the virtual WAN. Instead, the Director node configures the IPsec tunnel and VPN site on the virtual WAN.

Site-to-Site Tunnel Peers

You can configure IPsec or GRE tunnels between VOS devices and the following cloud or third-party devices:

- AWS Transit Gateway (IPsec and GRE [for Releases 22.1.1 and later])
- Azure Virtual WAN (IPsec)
- Zscaler (IPsec and GRE)
- Provider Versa Director and tenant Versa Director
- Others (IPsec)

The following sections describe how to configure site-to-site tunnels on these peer types.

Configure Site-to-Site Tunnels for AWS Transit Gateway

For Releases 21.1.1 and later.

For AWS, you use the AWS Transit Gateway Network Manager. To use the Network Manager, you create a global network to represent your network. Initially, the global network is empty. You then register your existing Transit

Gateways and define your on-premise resources in the global network. This allows you to visualize and monitor your AWS resources and on-premises networks.

You can create secure IPsec tunnels and GRE tunnels between a VOS device and an AWS Transit Gateway that is registered to the AWS global network under the Network Manager. When you create an IPsec tunnel, no manual IPsec tunnel and VPN configuration is required in AWS. Instead, the Director node fully automates creation of site-to-site IPsec tunnels, using AWS APIs to create Network Manager objects such as the device, site, link, and customer gateway, and then to create a VPN connection between the Transit Gateway and the customer gateway.


To configure an AWS Transit Gateway site-to-site tunnel, you configure the tunnel in a Workflows template and then associate the template with a device. Note the following for the tunnel configuration:

- For Releases 21.1 and later:
 - You must assign a static public IP address to the WAN interface or network used in the cloud tunnel connection.
 - A cloud tunnel configuration with a NATed environment on a WAN interface is not supported.
 - You can configure site-to-site tunnels using Workflows only for tunnels originating from an on-premise physical CPE and going to the Transit Gateway.
- For Releases 21.2.1 and later:
 - On a WAN interface, you can configure a cloud tunnel in a NATed environment.

Prerequisites for GRE Tunnels

- Create an AWS transit gateway in the region:
 - Configure a transit gateway CIDR IP address range.
 - Create Transit Gateway VPC attachments to the VOS VPC and any other spoke VPCs, as necessary.
 - Add a route in the proper subnet for the transit gateway CIDR range that has as its next hop the proper transit gateway. You can use the route table in either the WAN or LAN subnet for transit gateway connections over internal IP addresses.

Configure a Site-to-Site Tunnel

1. In Director view:
 - a. Select the Workflows tab in the top menu bar.
 - b. In the horizontal menu bar, select Template > Templates. The Template screen displays.
 - c. Click the  Add icon to create a template.;
2. Enter the required information on the Basic and Interfaces tabs. For more information, see [Create and Manage Staging and Post-Staging Templates](#).
3. Select the Tunnels tab. In the Site-to-Site Tunnels table, enter information for the following fields.

Director View

Appliance View

Template View

Monitor

Configuration

Workflows

Administration

Analytics

Commit Template

Director-QA

You are currently in Director View

Workflows > Template > Templates

Infrastructure

Template

Devices

✓

BASIC

✓

INTERFACES

3

TUNNELS

4

ROUTING

5

INBOUND NAT

6

MANAGEMENT SERVERS

7

REVIEW

Configure Tunnels

Tunnels

Template: Template-AWS-GRE-TGW-1

Split Tunnels

VRF Names	WAN Interfaces	Direct Internet Access	Gateway	
---Please Select---	---Please Select---	<input type="checkbox"/>	<input type="checkbox"/>	<div>+</div>

No Records to Display

☐ Load Balance

Site to Site Tunnels

Name	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile	BGP Enable	NAT Enabled	
	---Please Sel...	---Please Sel...	---Please Sel...	---Please Sel...	---Please Sel...	<input type="checkbox"/>	<input type="checkbox"/>	<div>+</div>
GRE-S2S	AWSTransitGW	GRE	WAN-Network	Director-QA-Tena...		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>✎</div> <div>🗑</div>



Cancel

Back

Save

Skip To Review


Next

Field	Description
Name	Enter a name for the site-to-site tunnel.
Peer Type	Select AWSTransitGW.
Tunnel Protocol	Select a tunnel protocol for AWS Transit Gateway peer type: <ul style="list-style-type: none"> ◦ IPsec ◦ GRE (for Releases 22.1.1 and later)
WAN/LAN Network	Select the network to use for AWS Transit Gateway. For Release 21.1.1, you can select
LAN VRF	Select the virtual routing instance to use to reach the LAN, to allow users in the routing in instance is the termination endpoint of the tunnel.
BGP Enable	For the peer type AWSTransitGW, BGP is automatically enabled.
NAT Enable	(For Releases 21.2.1 and later.) For the IPsec tunnel protocol for AWS Transit Gateway disabled for a GRE tunnel.
 Add icon	Click the  Add icon to add the site-to-site tunnel to the template.

- Click Continue if you are adding a template or Recreate if you are editing a template.

Configure a Site-to-Site Tunnel in a Device Workflow

To associate the workflow that contains the AWS Transit Gateway tunnel with a VOS device:

- In Director view:
 - Select the Workflows tab in the menu bar.
 - Select Devices > Devices in the left menu bar.
 - Click the  Add icon to create a device.
- Select the Tunnel Information tab, and enter information for the following fields. Note that if you are editing an existing device, you cannot edit existing tunnels. You can delete the existing row and add a new row if you want to edit the existing tunnel configuration. For more information, see [Create Devices and Device Groups](#).

Director View | Appliance View | Template View

Monitor | Configuration | **Workflows** | Administration | Analytics

Organization: Director-QA | You are currently in Director View | Workflows > Devices > Devices

Infrastructure | Template | **Devices**

Workflow Progress: BASIC (1) | CLOUD PROFILE (2) | **TUNNEL INFORMATION (3)** | DEVICE SERVICE TEMPLATE (4) | BIND DATA (5) | REVIEW (6)

Configure Tunnel Information

Names: GRE-S2S | Peer Type: AWSTransitGW | + Add | Device Name: Branch-AWS-GRE-TGW-1

Name	Peer Type	Connector	Region	Global Network ID	Transit Gateway	BGP As No	Transit Gateway Address	Transit GW CIDR	Actions
GRE-S2S	AWSTransitGW	AWS-Versa-Engg	us-west-1	amawsnetworkmanager-542139586608/global-network/global-network-0171asac7434f036	amawssec2us-west-1-542139586608/transit-gateway/tgw-09ed02176762d2111	64516	192.168.0.85	169.254.120/29	

Showing 1 - 1

Buttons: Cancel, Back, Save, Skip To Review, Next

Field	Description
Names	Select a site-to-site tunnel. The drop-down lists all the site-to-site tunnels that are in the te
Peer Type	Select AWSTransitGW as the peer type.
+ Add Add icon	Click the + Add Add icon to add the site-to-site tunnel to the device workflow.
Connector	Select the connector that contains authentication details to log on to AWS.
Region	Select the region in which the transit gateway object is created.
Global Network ID	(For Releases 22.1.1 and later.) Select the AWS global network name to which the transit
Transit Gateway	(For Releases 22.1.1 and later.) Select the transit gateway for AWS.
NAT Address	(For Releases 21.2.1 and later.) For the IPsec tunnel protocol for AWS Transit Gateway p Configure this address when a public IP address on a WAN port is NATed.
BGP AS Number	Enter the BGP local AS number.
Transit Gateway Address	(For Releases 22.1.1 and later.) For the GRE tunnel protocol for AWS Transit Gateway p the transit gateway. By default, the first available address from the transit gateway CIDR b

Transit Gateway CIDR	(For Releases 22.1.1 and later.) For the GRE tunnel protocol for AWS Transit Gateway peering addresses that are used for BGP peering. Specify a /29 CIDR block from the 169.254.0.0/16 range.
Actions	(For Releases 22.1.1 and later.) Select the action: <ul style="list-style-type: none"> ◦ Click the Delete icon to delete the tunnel. ◦ Click the Edit icon to edit the tunnel information.

3. Complete the procedure to add a device. For more information, see [Create Devices and Device Groups](#).

Configure Site-to-Site Tunnels for Azure Virtual WAN


You can create secure IPsec tunnels between VOS CPE devices and a Microsoft Azure Virtual WAN to allow VOS users to securely access applications and workloads that are hosted in the Azure Virtual WAN. This integration assumes that the VOS CPE device is a physical device that has a public IP assigned on WAN interface (without NATing). The secure IPsec tunnels that you create optimize the connectivity between the VOS device and the Azure Virtual WAN. You can create the IPsec tunnels between a VOS device and Azure Virtual WAN using Workflows.

Azure Virtual WAN supports only WAN networks. You must create virtual WAN and associated hub to the WAN on Azure. The virtual routing instance, which is the termination endpoint of the tunnel, allows users in the routing instance to access the tunnel to communicate with the gateway.

To configure an Azure Virtual WAN site-to-site tunnel, you configure the tunnel in a Workflows template and then associate the template with a device. Note the following for the tunnel configuration:

- In Releases 21.1.x and later:
 - You must assign a static public IP address to the WAN interface or network used in the cloud tunnel connection.
 - A cloud tunnel configuration with a NATed environment on a WAN interface is not supported.
 - You can configure site-to-site tunnels using workflows only for tunnels originating from an on-premise physical CPE and going to Azure Virtual WAN.
- In Releases 21.2.1 and later:
 - On a WAN interface, you can configure a cloud tunnel in a NATed environment.

Configure a Site-to-Site Tunnel

1. In Director view:
 - a. Select the Workflows tab in the top menu bar.
 - b. Select Template > Templates in the left menu bar.
 - c. Click the  Add icon to create a template. The Create Template popup window displays.

2. Enter the required information on the Basic and Interfaces tabs. For more information, see [Create and Manage Staging and Post-Staging Templates](#).
3. Select the Tunnels tab. In the Site-to-Site Tunnels table, enter information for the following fields.

MonitorConfigurationWorkflowsAdministrationAnalyticsCommit Template

Organization: --Please Select--

Infrastructure>Template>Templates>Application Steering>Spoke Groups>Service Chains>Devices>Devices

Edit Template Template-Azure-vWAN

BasicInterfacesTunnelsRoutingInbound NATServicesManagement Servers

Split Tunnels

VRF Names

WAN Interfaces

DIA

Gateway

--Please Select--

--Please Select--

☐

☐

+

No Records to Display

☐ Load Balance

Site to Site Tunnels

Name	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile	BGP Enable	NAT Enable	
	AzurevWAN	IPSEC	--Please Select--	--Please Select--	--Please Select--	<input type="checkbox"/>	<input type="checkbox"/>	+
S2S	AzurevWAN	IPSEC	WAN-Network-1	Director-QA-LAN-VR		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Back


CancelContinueRecreate

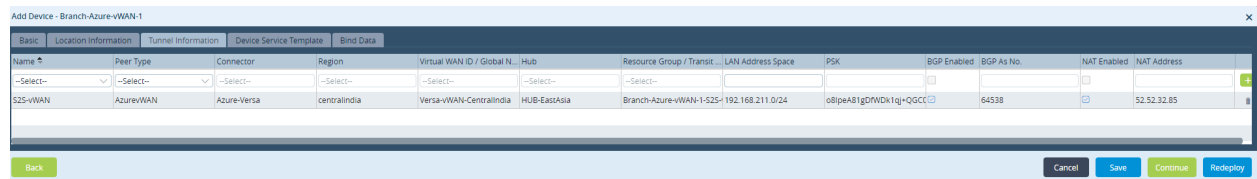
Field	Description
Name	Enter a name for the site-to-site tunnel.
Peer Type	Select Azure vWAN.
Tunnel Protocol	The default tunnel protocol for Azure virtual WAN peer type is IPsec.
WAN/LAN Network	Select the network to use for Azure virtual WAN. In Release 21.1.1, you can select only
LAN VRF	Select the virtual routing instance to use to reach the LAN, to allow users in the routing instance is the termination endpoint of the tunnel.
BGP Enable	For the peer type Azure virtual WAN, click to enable BGP.
NAT Enable	(In Releases 21.2.1 and later.) For the peer type Azure virtual WAN, click to enable NAT
<div>+</div> Add icon	Click the <div>+</div> Add icon to add the site-to-site tunnel to the template.

4. Click Continue if you are adding a template, or click Re-Create if you are editing a template.



Configure a Site-to-Site Tunnel in a Device Workflow

To associate the workflow that contains the Azure virtual WAN tunnel with a VOS device:

- In Director view:
 - Select the Workflows tab in the menu bar.
 - Select Devices > Devices in the left menu bar.
 - Click the  Add icon to create a device. The Add Device popup window displays.
- Select the Tunnel Information tab, and enter information for the following fields. Note that if you are editing an existing device, you cannot edit existing tunnels. You can delete the existing row and add a new row if you want to edit an existing tunnel configuration. For more information, see [Create Devices and Device Groups](#).



Field	Description
Name	Select a site-to-site tunnel.
Peer Type	Select AzurevWAN.
Connector	Select the connector that contains authentication details to log on to Azure.
Region	Select the region in which the Azure Virtual WAN object is created.
Virtual WAN ID/Global Network	Select the ID of the Azure virtual WAN.
Resource Group/Transit Gateway	Select the resource group from the specified region. If you do not select any value in this field, a new resource group is created.
LAN Address Space	Enter the IPv4 LAN address prefix on the VOS CPE device. This is the local LAN address space.

PSK	Enter the preshared key (PSK) to use to create a tunnel. The PSK cannot include any of the following five special characters: " < > # /. For more information about special characters, see Configure IPsec Profiles .
BGP Enabled	This field is checked automatically if the BGP is enabled in the workflow template.
BGP AS Number	Enter the BGP local AS number.
NAT Enabled	(In Releases 21.2.1 and later.) This field is checked automatically if NAT is enabled in the Workflow template.
NAT Address	(In Releases 21.2.1 and later.) Enter the NATed public IP address. Configure this address when a public IP address on a WAN port is NATed.
 Add icon	Click the  Add icon to add the site-to-site tunnel to the device workflow.

3. Complete the procedure to add a device. For more information see [Create Devices and Device Groups](#).

Configure Site-to-Site Tunnels for Zscaler


You can create secure IPsec tunnels and GRE tunnels between VOS CPE devices (either physical CPE devices or SD-WAN gateways in the cloud) and Zscaler third-party devices for optimized and secure branch connectivity. You can create more than one site-to-site tunnel from a CPE device to a Zscaler third-party device.

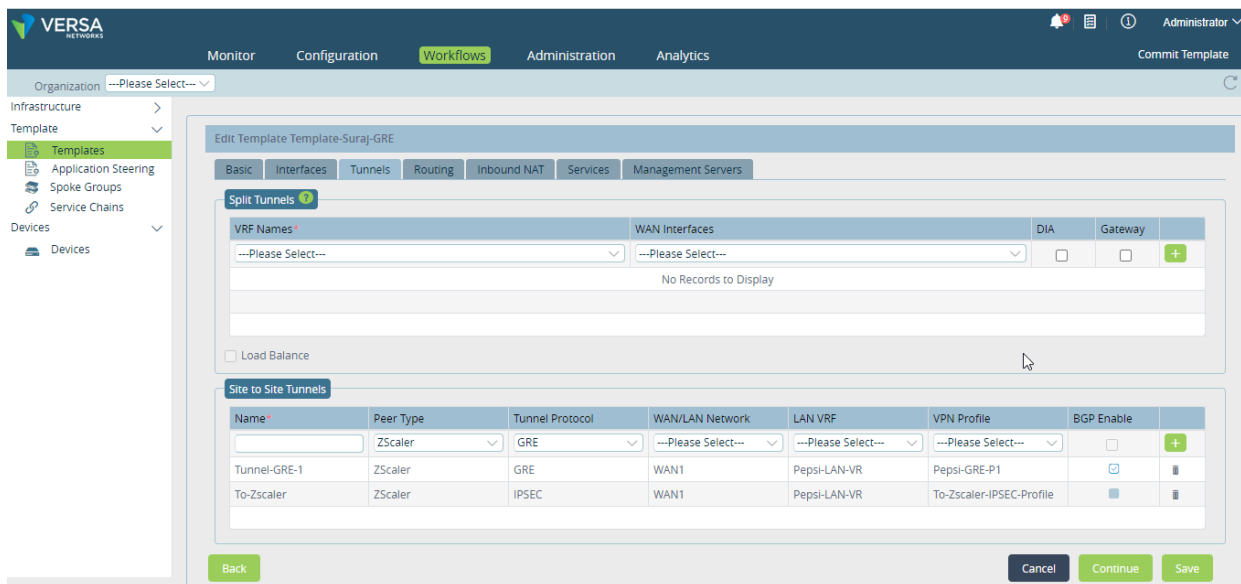
The Zscaler peer type supports WAN and LAN networks as originating endpoint of the tunnel. For Zscaler peer type, you must provision two tunnels for redundancy as recommended by Zscaler. For the virtual routing instance, you select a VPN profile to associate with the tunnel and with the LAN VRF organization. If an existing VPN profile is not available, you create a new profile.

To configure a site-to-site tunnel, configure the tunnel in a Workflows template and associate the template with a CPE device.

Configure a Site-to-Site Tunnel

1. In Director view:
 - a. Select the Workflows tab in the top menu bar.
 - b. Select Template > Templates in the left menu bar.

- c. Click the  Add icon to create a template. The Create Template popup window displays.
2. Enter the required information on the Basic and Interfaces tabs. For more information, see [Create and Manage Staging and Post-Staging Templates](#).
3. Select the Tunnels tab. In the Site-to-Site Tunnels table, enter information for the following fields.



The screenshot shows the Versa Networks configuration interface. The 'Edit Template' window for 'Template-Suraj-GRE' is open, with the 'Tunnels' tab selected. The 'Site to Site Tunnels' table is displayed with the following data:

Name	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile	BGP Enable
Tunnel-GRE-1	Zscaler	GRE	WAN1	Pepsi-LAN-VR	Pepsi-GRE-P1	<input checked="" type="checkbox"/>
To-Zscaler	Zscaler	IPSEC	WAN1	Pepsi-LAN-VR	To-Zscaler-IPSEC-Profile	<input type="checkbox"/>

Field	Description
Name	Enter a name for the site-to-site tunnel.
Peer Type	Select Zscaler.
Tunnel Protocol	Select a tunnel protocol: <ul style="list-style-type: none"> IPsec GRE
WAN/LAN Network	Select the network to use. You can select any WAN or LAN network. This network is the originating endpoint of the tunnel.
LAN VRF	Select the virtual routing instance to use to reach the LAN, to allow users in the routing instance to access the tunnel to communicate with the gateway. The virtual routing instance is the termination endpoint of

Field	Description
	the tunnel.
VPN Profile	<p>When you select a virtual routing instance, select a VPN profile to associate with the tunnel. The VPN profile is attached to LAN VRF. If an existing VPN profile is not available, create one, as described in Steps 4 and 5.</p> <p>You must create two tunnels, and this field lists only VPN profiles associated with the two tunnels.</p>
BGP Enable	This field is checked automatically if BGP is enabled in the VPN profile, and it is not checked if BGP is not enabled in the VPN profile.

- If an existing VPN profile is not available, click the + Add New VPN option in the VPN Profile field.

Name*	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile	BGP Enable	
	ZScaler	IPSEC	---Please Select---	---Please Select---	<div> <div>---Please Select---</div> <div>+ Add New VPN</div> </div>	<input type="checkbox"/>	
Tunnel-GRE-1	ZScaler	GRE	WAN1	Pepsi-LAN-VR	---	<input checked="" type="checkbox"/>	
To-Zscaler	ZScaler	IPSEC	WAN1	Pepsi-LAN-VR	To-Zscaler-IPSEC-Profile	<input checked="" type="checkbox"/>	

- In the Create VPN Profile popup window, enter information for the following fields.

Create VPN Profile

Tunnel Protocol*

IPSEC

VPN Profile Name*

IKE Transform*

aes128-sha1

IKE Version*

v2

IPSec Transform*

esp-aes128-sha1

BGP

☒ Disable
 ☐ Enable

No. of Tunnels*

2

Primary Tunnel Peer Auth PSK Key

Primary Tunnel Peer Auth IP Identifier Identity

Secondary Tunnel Peer Auth PSK Key

Secondary Tunnel Peer Auth IP Identifier Identity

Tunnel config*

Policy Based

Route Based

Policy Based

+

-

1

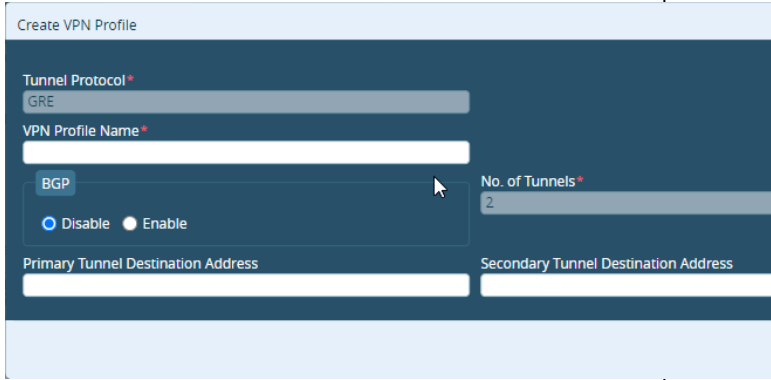

25

<input type="checkbox"/>	Name	Protocol	Source IPv4 Address/Prefix	Destination IPv4 Address/Prefix
No Row Added				

OK

Cancel

Field	Description
Tunnel Protocol (Required)	Displays the tunnel protocol that you selected in Step 3, above. The protocol is either IPsec or GRE.
VPN Profile Name (Required)	Enter a name for the VPN profile.
IKE Version (Required)	<p>Select the IKE version:</p> <ul style="list-style-type: none"> ◦ v1 ◦ v2 ◦ v2-or-v1
IKE Transform (Required)	Select the IKE transform algorithm to use for data encryption.
IPsec Transform (Required)	Select the IPsec transform algorithm to use for data encryption.
BGP	<p>Select the BGP state:</p> <ul style="list-style-type: none"> ◦ Disable ◦ Enable <p>If BGP is disabled, you must add one static route in the Router Information tab for this tunnel. For more Information, see Create Device Templates.</p>
Number of Tunnels (Required)	Enter how many tunnels to create between the VOS device and the Zscaler endpoint. For Zscaler tunnels, you must create two tunnels.
For the IPsec tunnel protocol	Enter tunnel peer information in the following fields.
<ul style="list-style-type: none"> ◦ Primary Tunnel Peer Authentication PSK Key 	Enter the primary tunnel preshared key (PSK) of the Zscaler endpoint. If you leave this field empty, you are prompted to enter the peer authentication key in the device bind data when you deploy the workflow. The PSK cannot include any of the following five special characters: " < > # /. For more information about special characters, see Configure IPsec Profiles .


<ul style="list-style-type: none"> Primary Tunnel Peer Authentication IP Identifier Identity 	Enter the primary tunnel IP address of the peer device. If you leave this field empty, you are prompted to enter the peer authentication IP identifier identity under device bind data when you deploy the workflow.
<ul style="list-style-type: none"> Secondary Tunnel Peer Authentication PSK Key 	Enter the secondary tunnel preshared key (PSK) of the Zscaler endpoint. If you leave this field empty, you are prompted to enter the peer authentication key in the device bind data when you deploy the workflow. The PSK cannot include the following five special characters: " < > # / .
<ul style="list-style-type: none"> Secondary Tunnel Peer Authentication IP Identifier Identity 	Enter the secondary tunnel IP address of the peer device. If you leave this field empty, you are prompted to enter the peer authentication IP identifier identity under device bind data when you deploy the workflow.
For the GRE tunnel protocol	<p>Enter information for the following fields.</p> 
<ul style="list-style-type: none"> Primary Tunnel Destination Address 	Enter the primary tunnel destination IP address of the device.
<ul style="list-style-type: none"> Secondary Tunnel Destination Address 	Enter the secondary tunnel destination IP address of the device.
Tunnel Configuration (Required)	Select the tunnel configuration to use.
<ul style="list-style-type: none"> Route Based 	Use a route-based configuration.
<ul style="list-style-type: none"> Policy Based 	Use a policy-based configuration. If you select this option, click the  Add icon to add a policy. In the

Add Policy popup window, enter information for the following fields:

The screenshot shows the 'Add Policy' dialog box. It includes a 'Name' field, a 'Protocol' dropdown menu, and two sections for 'Source' and 'Destination'. Each section contains an 'Address' dropdown, an 'IPv4 Address/Prefix' text field, and a 'Port' text field. The 'OK' button is highlighted in green at the bottom right.


- Name—Enter a name for the policy.
- Protocol—Select a protocol:
 - ICMP
 - TCP
 - UDP
- Source (Group of Fields)—Enter information about the traffic source:
 - Address—Select the IPv4 or IPv6 address type.
 - Address/Prefix—Enter the IPv4 or IPv6 source address or prefix as per the address type selected.
 - Port—Enter the source port number.
- Destination (Group of Fields)—Enter information about the traffic destination:
 - Address—Select the IPv4 or IPv6 address type.
 - Address/Prefix—Enter the IPv4 or IPv6 destination address or prefix as per the address type selected.
 - Port—Enter the destination port number.
- Click OK.

6. Click OK.

- 7. Click the  Add icon at the end of the row to add the site-to-site tunnel.
- 8. Create a Workflows configuration template based on your requirements. For more information, see [Create and Manage Staging and Post-Staging Templates](#).



Configure a Site-to-Site Tunnel in a Device Workflow

To associate a Workflow templates that contains the site-to-site tunnel with a VOS device:

- 1. In Director view:
 - a. Select the Workflows tab in the top menu bar.
 - b. Select Devices > Devices in the left menu bar.
 - c. Click the  Add icon to create a device. The Add Device popup window displays.
- 2. In the Basic tab, select or add the device group with which to associate the template. Also, enter the other required information. For more information, see [Create Devices and Device Groups](#). If you select a device group that has a template associated with it and the template includes tunnels, the Tunnel Information tab displays.
- 3. Select the Location Information tab, and enter the required information. For more information, see [Create Devices and Device Groups](#).
- 4. Select the Tunnel Information tab, and enter information for the following fields. Note that if you are editing an existing device, you cannot edit existing tunnels. You can delete the existing row and add a new row if you want to edit an existing tunnel configuration.

Add Device - Branch-GRE


BasicLocation InformationTunnel InformationDevice Service TemplateBind Data

Name	Peer Type	Connector	Region	Virtual WAN Group / Transit	LAN Address Space	PSK	BGP Enabled	BGP As No.	
--Select--	--Select--	--Select--	--Select--	--Select--			<input type="checkbox"/>		
GRE	Zscaler				192.168.21.0/24		<input checked="" type="checkbox"/>		

Back

CancelSaveContinueRedeploy

Field	Description
Name	Select a site-to-site tunnel. The drop-down lists all the site-to-site tunnels t
Peer Type	Select Zscaler
LAN Address Space	Enter the IPv4 LAN address prefix on the VOS CPE device. This is the loc
BGP Enabled	This field is checked automatically if the BGP is enabled in the VPN profile

- 5. Click the  Add icon at the end of the row to add the tunnel information.

6. Click Continue.
7. In the Bind Data tab, enter device-specific details. For example, enter the local and peer BGP AS numbers and the local BGP address if BGP is enabled, enter the local authentication key and local IP identifier, and enter the authentication key and peer IP identifier if no value is provided in the VPN profile. When you configure a device for site-to-site tunnel, you can see the forced fields in Bind Data tab.
8. Complete the procedure to add a device. For more information, see [Create Devices and Device Groups](#).

Configure a Versa Director-Managed Site-to-Site Tunnel

In Releases 21.2.1 and later.

You can create a Versa Director-managed IPsec site-to-site tunnel between a provider Versa Director and tenant Versa Director so that the tenant can use services available from the provider Director as if the services were available directly from the tenant Director. These services include:

- On-ramp to SaaS providers, such as Google, Office, Box, and Salesforce
- Cloud Service Gateways (CSGs)
- Application reverse proxies
- Titan hubs

Versa Director managed site-to-site tunnel integration supports the following protocols:


- EBGP
- IKE
- IPsec

The following sections describe how to configure a Versa Director-managed site-to-site tunnel.

Configure a Versa CMS Connector

To establish a Versa Director-managed site-to-site connection between a tenant and a provider, you first configure a CMS connector on the tenant Versa Director.

To configure the Versa CMS connector:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Connectors > CMS in the left menu bar.
3. Click the  Add icon in the main pane. In the Add CMS Connector popup window, enter information for the following fields.

Add CMS Connector

CMS Name*

Organization*

Organization

CMS Flavor

Versa

Primary Versa Director Hosted IP*

Secondary Versa Director Hosted IP

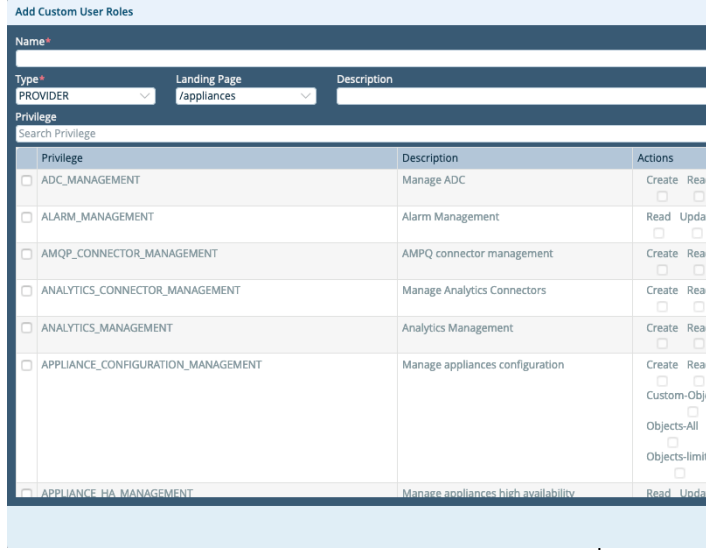
User Name*

Password*

OK

Cancel

Field	Description
CMS Name (Required)	Enter a name for the CMS connector.
Organization (Required)	Select the tenant organization, which should be present in the provider Versa Director.
CMS Flavor	Select Versa.
Primary Versa Director Hosted IP (Required)	Enter the IP address of the primary provider Versa Director.
Secondary Versa Director Hosted IP	If HA is configured, enter the IP address of the secondary provider Versa Director.
Username (Required)	<p>Enter a username for the primary Versa Director. The user must have the role of <code>ProviderDataCenterSystemAdmin</code>, or you must create a custom provider role for the user.</p> <p>To create a custom provider user role:</p> <ol style="list-style-type: none"> In Director view, select the Administration tab in the top menu bar. Select Director User Management > Custom User Roles in the left menu bar. Click the Add icon to add a custom user role. The Add Custom User Role screen displays.

Field	Description
	 <p>4. Enter the following information:</p> <ol style="list-style-type: none"> In the Name field, enter a name for the custom role. In the Type field, select Provider. In the Landing Page field, select a landing page. In the Privilege column, select the privileges to grant to the new role. In the Action column, select the actions to grant to the new role. <p>5. Click Deploy.</p>
Password (Required)	Enter a password for the primary Versa Director.

4. Click OK.

Configure the Template Workflow

To configure the template workflow for a Versa Director–managed IPsec site-to-site tunnel:

- In Director view:
 - Select the Workflows tab in the top menu bar.
 - Select Template > Templates in the left menu bar.
 - Select a post-staging template in the main pane. The Edit Template screen displays.
- Select the Tunnels tab. In the Site-to-Site Tunnels table, enter information for the following fields.

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configura...

Updated: Wed, 23 Oct 2024 07:24:09 GMT

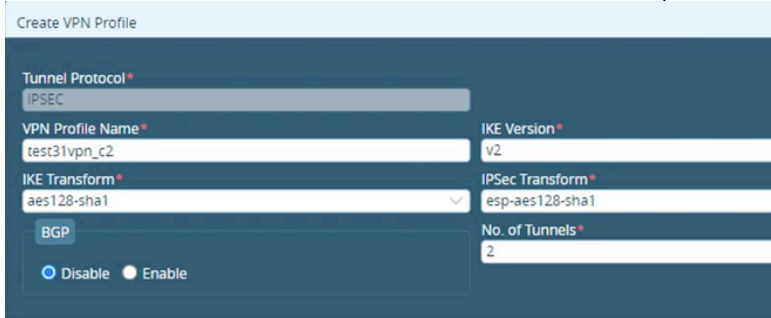
Copyright © 2024, Versa Networks, Inc.


The screenshot displays the Versa Networks configuration interface. The 'Tunnels' tab is selected, showing a 'Split Tunnels' configuration. The 'Split Tunnels' table has the following data:

VRF Names	WAN Interfaces	DIA	Gateway
---Please Select---	---Please Select---	<input type="checkbox"/>	<input type="checkbox"/>
Tenant1-LAN-VR	WAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tenant2-LAN-VR	WAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Below the 'Split Tunnels' table is a 'Site to Site Tunnels' section, which is currently empty. The 'Site to Site Tunnels' table has the following columns: Name, Peer Type, Tunnel Protocol, WAN/LAN Network, LAN VRF, VPN Profile, BGP Enable, and NAT Enable. The table shows 'No Records to Display'.

Field	Description
Name	Enter a name for the site-to-site tunnel.
Peer Type	Select Versa.
Tunnel Protocol	Select a tunnel protocol. If you select IPsec as the tunnel protocol, you must configure a static route. For more information about configuring static routes, see Create Post-Staging Templates .
WAN/LAN Network	Select a WAN or LAN transport network.
LAN VRF	Select a LAN routing instance for the tenant.
VPN Profile	Select a VPN profile, or Click + Add New VPN to create a new VPN profile and enter information for the following fields:

Field	Description
	 <ul style="list-style-type: none"> VPN Profile Name—Enter a name for the VPN profile IKE Version—Select the IKE version IKE Transform—Select the IKE transform algorithm to use for data encryption IPsec Transform—Select the IPsec transform algorithm to use for data encryption. BGP Disable/Enable—Select the BGP state. No. of Tunnels—Enter how many tunnels to create between the provider Director node and the tenant Director node. <p>Click OK to create the VPN profile.</p>
BGP Enable	Click to enable BGP on the site-to-site tunnel. By default, BGP is disabled. If you do not enable BGP, you must configure a static route. For more information about configuring static routes, see Create Post-Staging Templates . If you enable BGP, you do not need to configure a static route.
NAT Enable	Click to enable NAT on the site-to-site tunnel. By default, NAT is disabled.


- Click the  Add icon to add the site-to-site tunnel.
- To create more than one site-to-site tunnel between the tenant Director node and the provider Director node, add additional rows in the Site-to-Site Tunnels table.
- Click Recreate to recreate the template.

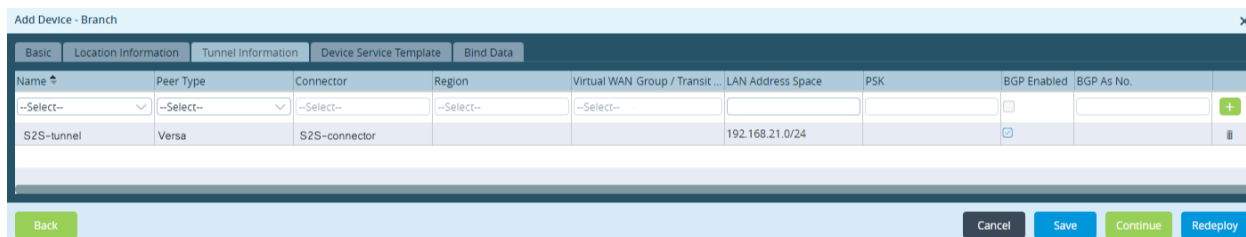
Configure the Device Workflow

When you deploy the device workflow, the tenant Director node receives the provider Director's credentials from the CMS connector configuration, creates a tunnel configuration on the provider Director node, and exposes its configuration to allow the tenant Director node to connect to it. The tenant Director node downloads the configuration and applies the tunnel configuration to the branch.

Based on demand, multiple WAN subinterfaces are created dynamically to handle multiple site-to-site tunnels to the same branch.

To configure the device workflow for a Versa Director–managed IPsec site-to-site tunnel:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Devices > Devices in the left menu bar.
3. Click the  Add icon to create a device. The Add Device popup window displays.
4. In the Basic tab, select or add the device group with which to associate the template, and enter any other required information. For more information, see [Create Devices and Device Groups](#). If you select a device group that has a template associated with it and the template includes tunnels, the Tunnel Information tab displays.
5. Select the Location Information tab, and enter information for the following fields. For more information, see [Create Devices and Device Groups](#).
6. Select the Tunnel Information tab, and enter information for the following fields. Note that if you are editing an existing device, you cannot edit existing tunnels. To edit an existing tunnel configuration, you must delete the row for the existing and then add a new row.




Field	Description
Name	Enter a name for the site-to-site tunnel.
Peer Type	Select Versa.
Connector	Select the CMS connector that you created in the Configure a Versa CMS Connector section, above.
Region	Select a region. Regions are configured on the provider Versa Director. At least one region must be listed in this field.
PSK	Enter the preshared key (PSK) to use to create a

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configura...

Updated: Wed, 23 Oct 2024 07:24:09 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
	tunnel. The PSK cannot include any of the following five special characters: " < > # / . For more information about special characters, see Configure IPsec Profiles .
BGP Enabled	Click to enable BGP.
BGP AS No.	If you enable BGP, enter the BGP AS number.
 Add icon	Click the Add icon to add the tunnel to the device.

7. Select the Bind Data tab.
8. On the User Input tab, click the device name. A pop-up window displays the bind data.
9. In the IPsec section, enter information for the following fields:
 - a. For the first tunnel in the *tunnel-name-first_Local_auth_ip_identifier* field, enter the IP address of the WAN interface.
 - b. In the *tunnel-name-first_Local_auth_key_IKELKey* field, enter the IKE key for the first tunnel.
 - c. For the second tunnel in the *tunnel-name-second_Local_auth_ip_identifier* field, enter the IP address of the WAN interface of the first tunnel.
 - d. In the *tunnel-name-second_Local_auth_key_IKELKey* field, enter the IKE key for the first tunnel.

In the example screen below, two tunnels have been created, test31tunnel4-1 and test31tunnel4-2. The IP address of the WAN1 interface is 10.192.172.233, as shown in the Interfaces section. This IP address is used as the *Local_auth_ip_identifier* value for both the test31tunnel4-1 and the test31tunnel4-2 tunnels. Test@124 is used as the *Local_auth_key_IKELkey* for both the test31tunnel4-1 and test31tunnel4-2 tunnels.

Serial# : Branch11 Appliance : SDWAN-Branch11

Variable	Value
Interfaces	
LAN-Network-T1_IPv4__staticaddress	172.18.11.1/24
LAN-Network-T2_IPv4__staticaddress	172.18.12.1/24
LAN-Spirent-1_IPv4__staticaddress	201.201.201.1/24
WAN1_IPv4__staticaddress	10.192.172.233/16
WAN2_IPv4__staticaddress	192.168.12.101/24
WAN3_IPv4__staticaddress	10.192.172.244/16
IPSEC	
test31 tunnel4-1_Local_auth_ip_identifier_...	10.192.172.233
test31 tunnel4-1_Local_auth_key__IKELKey	Test@123
test31 tunnel4-2_Local_auth_ip_identifier_...	10.192.172.233
test31 tunnel4-2_Local_auth_key__IKELKey	Test@123
Static Routes	
Tenant1-LAN-VR-0_srPrefix	192.168.12.0/24
Virtual Routers	

10. Click OK.
11. Click Redeploy in the Add Device pop-up window to redeploy the device.
12. In Director view, select the Monitor tab in the top menu bar.

VERSA NETWORKS Administrator

Monitor Configuration Workflows Administration Analytics Commit Template

Search Summary Devices

Total Appliances : 3 Search Appliance Tags

	Appliance	IP	Role	Version	Organization	Tags	Status	Health	Uptime	Actions
<input type="checkbox"/>	SDWAN-Branch...	10.0.0.18	Branch	Tue, Dec 15 2...	21.2.1-GA	provider-org			Up	
<input type="checkbox"/>	SDWAN-Contr...	10.192.249.161	Controller	Mon, Oct 05 2...	21.2.1-GA	Tenant1,Tena...			Up	
<input type="checkbox"/>	SDWAN-Contr...	10.192.249.162	Controller	Mon, Oct 05 2...	21.2.1-GA	Tenant1,Tena...			Up	

13. Click Commit Template. In the Commit Template to Devices popup window, enter information for the following fields.

Commit Template to Devices

Organization*
Tenant1

Select Devices By
☒ Template ☐ Service Template
 Select Template*
 tenant1_template

Schedule Commit
 YYYY/MM/DD HH:mm:ss
☐ Retry on Device Unreachable

☐ Auto Merge ☒ Overwrite
☐ Reboot

Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
<input type="checkbox"/> tunnel4						
<input checked="" type="checkbox"/> SDWAN-Branch11	Branch	OUT_OF_SYNC	IN_SYNC			

Field	Description
Organization	Select the organization whose devices should receive the new device template.
Select Template	Select the template to commit.
Device Groups	Click the checkbox next to the device to which to commit the template.


14. Click OK to commit the selected template to the devices.

Delete Site-to-Site Tunnels

You can delete site-to-site tunnels by doing the following:

- Delete the tunnel from the device, and redeploy the device.
- Remove the device's bind data that was associated with the deleted tunnel from the template, remove the static route from the template, and recreate the template.
- Deploy and commit the newly regenerated template.

To delete site-to-site tunnel from a device:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Devices > Devices in the left menu bar.
3. In the main pane, select the device containing the tunnel to be deleted. The Add Device popup window displays.
4. Select the Tunnel Information tab.
5. Locate the row containing the tunnel to be deleted, and then click the  Trash icon at the end of that row.

Name	Peer Type	Connector	Region	Virtual WAN Group / Transit	LAN Address Space	PSK	BGP Enabled	BGP As No.
--Select--	--Select--	--Select--	--Select--	--Select--			<input type="checkbox"/>	
S2S-tunnel	Versa	S2S-connector			192.168.21.0/24		<input checked="" type="checkbox"/>	

6. Click Redeploy.

7. To verify that the device has been redeployed, click the Tasks icon to view task messages.

To remove the bind data and static route that were associated with the deleted tunnel:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the left menu bar.
3. In the main pane, select the template containing the tunnel to be deleted. The Edit Template popup window displays.
4. Select the Tunnels tab.
5. In the Site-to-Site Tunnels table, locate the row containing the tunnel to be deleted, and then click the Trash icon at the end of that row.

Name	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile	BGP Enable	NAT Enable
--Please Select--	--Please Select--	--Please Select--	--Please Select--	--Please Select--	--Please Select--	<input type="checkbox"/>	<input type="checkbox"/>
test31tunnel4	Versa	IPSEC	WAN1	Tenant1-LAN-VR	test31vpn1_c2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

6. Select the Routing tab.

7. In the Static Routes table, locate the row containing the static route to be deleted, and then click the Trash icon at the end of that row.

Template

- Templates
- Application Steering
- Spoke Groups
- Service Chains

Devices

- Devices

Edit Template tenant1_template

Basic Interfaces Tunnels Routing Inbound NAT Services Management Servers

BGP

Network	IBGP	Local AS	Neighbor IP	Peer AS	BFD
---Please Select---	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

No Records to Display

OSPF / OSPFv3

Network Name	Area	BFD
---Please Se---	<input type="text"/>	<input type="checkbox"/>

No Records to Display

Static Routes

Routing Instance	Prefix	Nexthop Address	Nexthop Tunnel	Monitor
---Please Select---	<input type="text"/>	<input type="text"/>	---Please Select---	<input type="checkbox"/>
Tenant1-LAN-VR	{5v_Tenant1-LAN-VR-...		test31 tunnel4	true

Back Cancel Continue Recreate

8. Click Recreate to update the template. The Diff and Merge screen displays.

VERSA NETWORKS

Monitor Configuration Workflows Administration Analytics

Organization: ---Please Select---

Infrastructure

- Template
- Templates
- Application Steering
- Spoke Groups
- Service Chains

Devices

- Devices

Diff and Merge

Active Template

Current (Read Only)

```

49  }
50  }
51  vni "vni-0/802" {
52    enable "true";
53    mode "ipsec";
54    type "ipsec";
55    unit "0" {
56      enable "true";
57      family {
58        inet {
59          address "XXX.XXX.XX.XX.XX";
60        }
61      }
62    }
63  }

```

Newly Generated (Editable)

```

49  }
50  }
51  vni "vni-0/0" {

```

Deploy Cancel

9. Click Deploy to deploy the newly generated template. The following screen displays.

Commit Template to Devices

Organization*
Tenant1

Select Devices By ?
☒ Template ☐ Service Template
 Select Template*
 tenant1_template

Schedule Commit ?
 YYYY/MM/DD HH:mm:ss

☐ Retry on Device Unreachable

☐ Auto Merge ☒ Overwrite ?

☐ Reboot ?

Device Groups

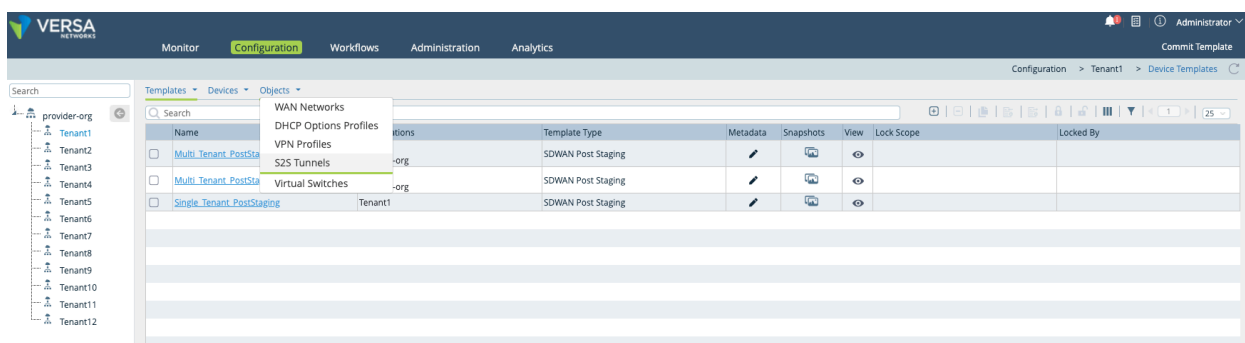
Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
<input checked="" type="checkbox"/>	SDWAN-Branch11	Branch	OUT_OF_SYNC	IN_SYNC		

10. Click OK to commit the selected template.

Verify the Site-to-Site Connection

To verify the managed site-to-site connection between a tenant Director node and a provider Director node:

1. In Director view, select the Configuration tab in the top menu bar.



2. Select Objects > S2S Tunnels in the horizontal menu bar. The main pane displays the site-to-site tunnels that have been created between the tenant Director node and the provider Director node.

Configuration > Tenant1 > VPN Profile

Profile Name	Tenant Name	Primary PSK ID	Primary PSK Key	Primary Peer PSK ID	Primary Peer PSK Key	IKE Version	Tunnel Count	BGP Enabled	BGP As No.
s2stunneldemo	Tenant1	192.168.31.101	OxyQY8zwuoWGNHdBlk...	192.168.31.101	FvktAUjxOjrgU41zuAr...	v2	1	false	
news2stunnel	Tenant1	192.168.31.101	DgdEaeCfpWw38IdDv6...	192.168.31.101	WlqFgHuVA7qNn7yXZC...	v2	1	false	

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration...


Updated: Wed, 23 Oct 2024 07:24:09 GMT

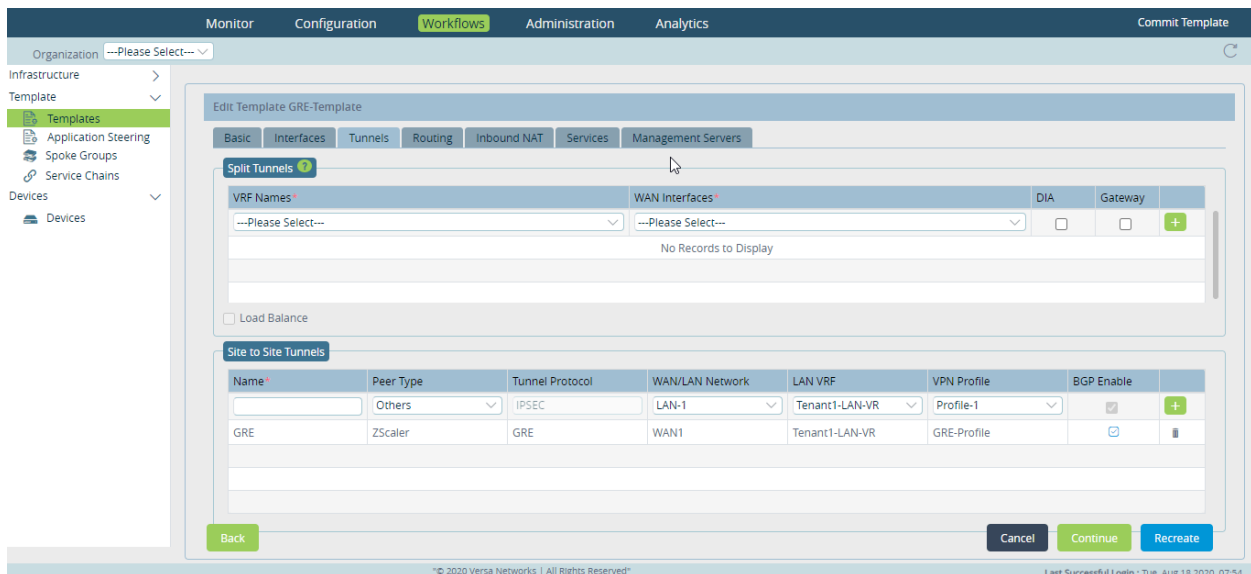
Copyright © 2024, Versa Networks, Inc.

Configure Site-to-Site Tunnels for Other Peer Types

You can deploy a tunnel on a third-party device that supports IPsec tunnels, such as Cisco, Juniper, and Palo Alto.

Configure a Site-to-Site Tunnel

1. In Director view:
 - a. Select the Workflows tab in the top menu bar.
 - b. Select Template > Templates in the left menu bar.
 - c. Click the  Add icon to create a template. The Create Template popup window displays.
2. Enter the required information on the Basic and Interfaces tabs. For more information, see [Create and Manage Staging and Post-Staging Templates](#).
3. Select the Tunnels tab. In the Site-to-Site Tunnels table, enter information for the following fields.



The screenshot shows the 'Edit Template GRE-Template' window in the Versa Networks Director. The 'Tunnels' tab is selected. The 'Split Tunnels' section is empty. The 'Site to Site Tunnels' table has two rows: one for 'GRE' with 'ZScaler' peer type and 'GRE' protocol, and another for 'IPsec' with 'Others' peer type and 'IPsec' protocol. The 'IPsec' row is highlighted.

Field	Description
Name	Enter a name for the site-to-site tunnel.
Peer Type	Select Others.
Tunnel Protocol	The default tunnel protocol for Others peer type is IPsec.

Field	Description
WAN/LAN Network	Select the WAN or LAN network to use. This network is the originating endpoint of the tunnel.
LAN VRF	Select the virtual routing instance to use to reach the LAN, to allow users in the routing instance to access the tunnel to communicate with the gateway. The virtual routing instance is the termination endpoint of the tunnel.
VPN Profile	When you select a virtual routing instance, select a VPN profile to associate with the tunnel. The VPN profile is attached to LAN VRF. If an existing VPN profile is not available, create one, as described in Steps 4 and 5.
BGP Enable	This field is checked automatically if BGP is enabled in the VPN profile, and it is not checked if BGP is not enabled in the VPN profile.

- If an existing VPN profile is not available, click the + Add New VPN option in the VPN Profile field.

The screenshot shows the 'Site to Site Tunnels' configuration interface. It contains a table with columns: Name, Peer Type, Tunnel Protocol, WAN/LAN Network, LAN VRF, VPN Profile, BGP Enable, and an action column. The 'VPN Profile' dropdown for the 'Tunnel-GRE-1' entry is open, showing a red box around the '+ Add New VPN' option.

Name	Peer Type	Tunnel Protocol	WAN/LAN Network	LAN VRF	VPN Profile	BGP Enable	
	ZScaler	IPSEC	---Please Select---	---Please Select---	---Please Select---	<input type="checkbox"/>	+
Tunnel-GRE-1	ZScaler	GRE	WAN1	Pepsi-LAN-VR	---Please Select---	<input checked="" type="checkbox"/>	
To-Zscaler	ZScaler	IPSEC	WAN1	Pepsi-LAN-VR	To-Zscaler-IPSEC-Profile	<input type="checkbox"/>	

- In the Create VPN Profile popup window, enter information for the following fields.

Create VPN Profile

Tunnel Protocol*

IPSEC

VPN Profile Name*

IKE Transform*

aes128-sha1

IKE Version*

v2

IPSec Transform*

esp-aes128-sha1

BGP

☒ Disable
 ☐ Enable

No. of Tunnels*

2

Primary Tunnel Peer Auth PSK Key

Primary Tunnel Peer Auth IP Identifier Identity

Secondary Tunnel Peer Auth PSK Key

Secondary Tunnel Peer Auth IP Identifier Identity

Tunnel config*

Policy Based

Route Based

Policy Based

+

-

1


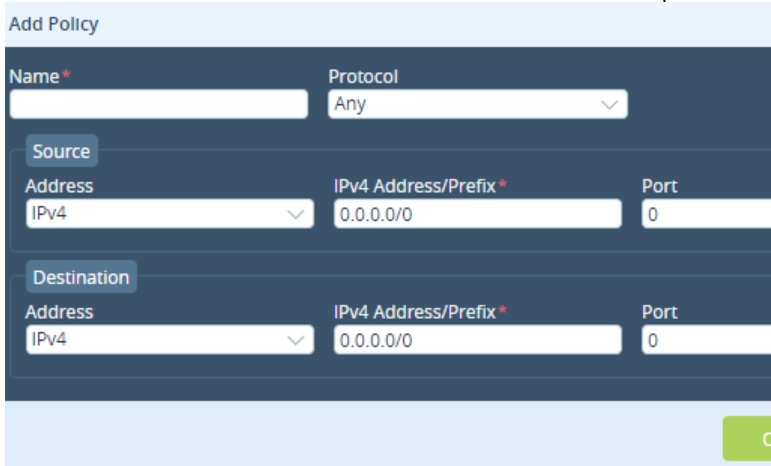
25

<input type="checkbox"/>	Name	Protocol	Source IPv4 Address/Prefix	Destination IPv4 Address/Prefix
No Row Added				


OK

Cancel

Field	Description
Tunnel Protocol (Required)	Displays the tunnel protocol that you selected in Step 3, above. The tunnel protocol must be IPsec for peer type Others.
VPN Profile Name (Required)	Enter a name for the VPN profile.
IKE Version (Required)	<p>Select the IKE version:</p> <ul style="list-style-type: none"> ◦ v1 ◦ v2 ◦ v2-or-v1
IKE Transform (Required)	Select the IKE transform algorithm to use for data encryption.
IPsec Transform (Required)	Select the IPsec transform algorithm to use for data encryption.
BGP	<p>Select the BGP state:</p> <ul style="list-style-type: none"> ◦ Disable ◦ Enable <p>If BGP is disabled, You must add one static route in Router Information tab for this tunnel. For more information, see Create Device Templates</p>
Number of Tunnels (Required)	Enter how many tunnels to create between the VOS device and the third-party unmanaged device.
For the IPsec tunnel protocol	Enter tunnel peer information in the following fields.
<ul style="list-style-type: none"> ◦ Primary Tunnel Peer Authentication PSK Key 	<p>Enter the primary tunnel preshared key (PSK) of the third-party peer endpoint. If you leave this field empty, you are prompted to enter the peer authentication key in the device bind data when you deploy the workflow. The PSK cannot include any of the following five special characters: " < > # /. For more information about special characters, see Configure IPsec Profiles.</p>


<ul style="list-style-type: none"> Primary Tunnel Peer Authentication IP Identifier Identity 	Enter the primary tunnel IP address of the peer device. If you leave this field empty, you are prompted to enter the peer authentication IP identifier identity under device bind data when you deploy the workflow.
<ul style="list-style-type: none"> Secondary Tunnel Peer Authentication PSK Key 	Enter the secondary tunnel preshared key (PSK) of the third-party peer endpoint. If you leave this field empty, you are prompted to enter the peer authentication key in the device bind data when you deploy the workflow. The PSK cannot include any of the following five special characters: " < > # / .
<ul style="list-style-type: none"> Secondary Tunnel Peer Authentication IP Identifier Identity 	Enter the secondary tunnel IP address of the peer device. If you leave this field empty, you are prompted to enter the peer authentication IP identifier identity under device bind data when you deploy the workflow.
Tunnel Configuration (Required)	Select the tunnel configuration to use.
<ul style="list-style-type: none"> Route Based 	Use a route-based configuration.
<ul style="list-style-type: none"> Policy Based 	<p>Use a policy-based configuration. If you select this option, click the  Add icon to add a policy. In the Add Policy popup window, enter information for the following fields:</p>  <ul style="list-style-type: none"> Name—Enter a name for the policy. Protocol—Select a protocol: <ul style="list-style-type: none"> ICMP

	<ul style="list-style-type: none"> ▪ TCP ▪ UDP ◦ Source (Group of Fields)—Enter information about the traffic source: <ul style="list-style-type: none"> ▪ Address—Select the IPv4 or IPv6 address type. ▪ Address/Prefix—Enter the IPv4 or IPv6 source address or prefix as per the address type selected. ▪ Port—Enter the source port number. ◦ Destination (Group of Fields)—Enter information about the traffic destination: <ul style="list-style-type: none"> ▪ Address—Select the IPv4 or IPv6 address type. ▪ Address/Prefix—Enter the IPv4 or IPv6 destination address or prefix as per the address type selected. ▪ Port—Enter the destination port number. ◦ Click OK.
--	---


6. Click OK.
7. Click the  Add icon at the end of the row to add the site-to-site tunnel.
8. Create a Workflows configuration template based on your requirements. For more information, see [Create and Manage Staging and Post-Staging Templates](#).

Configure a Site-to-Site Tunnel in a Device Workflow

To associate a Workflow templates that contains the site-to-site tunnel with a VOS device:

1. In Director view:
 - a. Select the Workflows tab in the top menu bar.
 - b. Select Devices > Devices in the left menu bar.
 - c. Click the  Add icon to create a device. The Add Device popup window displays.
2. In the Basic tab, select or add the device group with which to associate the template. Also, enter the other required information. For more information, see [Create Devices and Device Groups](#). If you select a device group that has a template associated with it and the template includes tunnels, the Tunnel Information tab displays.
3. Select the Location Information tab, and enter the required information. For more information, see [Create Devices and Device Groups](#).
4. Select the Tunnel Information tab, and enter information for the following fields. Note that if you are editing an existing device, you cannot edit existing tunnels. You can delete the existing row and add a new row if you want to edit an existing tunnel configuration.

Field	Description
Name	Select a site-to-site tunnel. The drop-down lists all the site-to-site tunnels
Peer Type	Select Others.
LAN Address Space	Enter the IPv4 LAN address prefix on the VOS CPE device. This is the loc
BGP Enabled	This field is checked automatically if the BGP is enabled in the VPN profile

- Click the  Add icon at the end of the row to add the tunnel information.
- Click Continue.
- In the Bind Data tab, enter device-specific details. For example, enter the local and peer BGP AS numbers and the local BGP address if BGP is enabled, enter the local authentication key and local IP identifier, and enter the authentication key and peer IP identifier if no value is provided in the VPN profile. When you configure a device for site-to-site tunnel, you can see the forced fields in Bind Data tab.
- Complete the procedure to add a device. For more information, see [Create Devices and Device Groups](#).

Configure the TCP Adjust MSS Option

The maximum segment size (MSS) is a parameter of the TCP header options field that specifies the largest amount of data, specified in bytes, that a network device can receive in a single TCP segment. It does not count the TCP header (20 bytes) or the IP header (20 bytes). To avoid fragmentation at the IP layer, a network device must specify the maximum segment size as equal to the largest IP datagram that the host can handle minus the IP and TCP header sizes. For example, the default MTU value for a PC is 1500 bytes, so, the MSS is be set to 1460 bytes (1500 less 20 bytes for the IP header and less 20 bytes for the TCP header).

On VOS devices, the default TCP MSS is 1500 bytes. If a host, such as a VOS device, wants to set the maximum segment size to a value other than the default, it can change it in the TCP SYN and TCP SYN ACK packets during the three-way handshake that occurs when TCP is establishing a session.

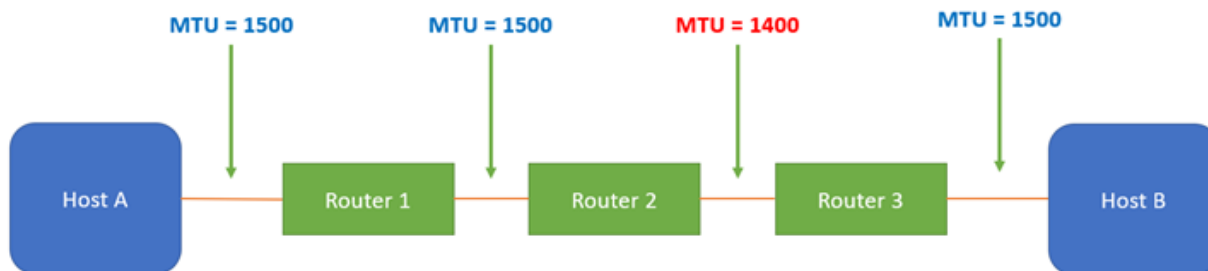
You configure the TCP MSS to avoid a problem similar to that shown in the following figure, where one of the routers

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configura...

Updated: Wed, 23 Oct 2024 07:24:09 GMT

Copyright © 2024, Versa Networks, Inc.

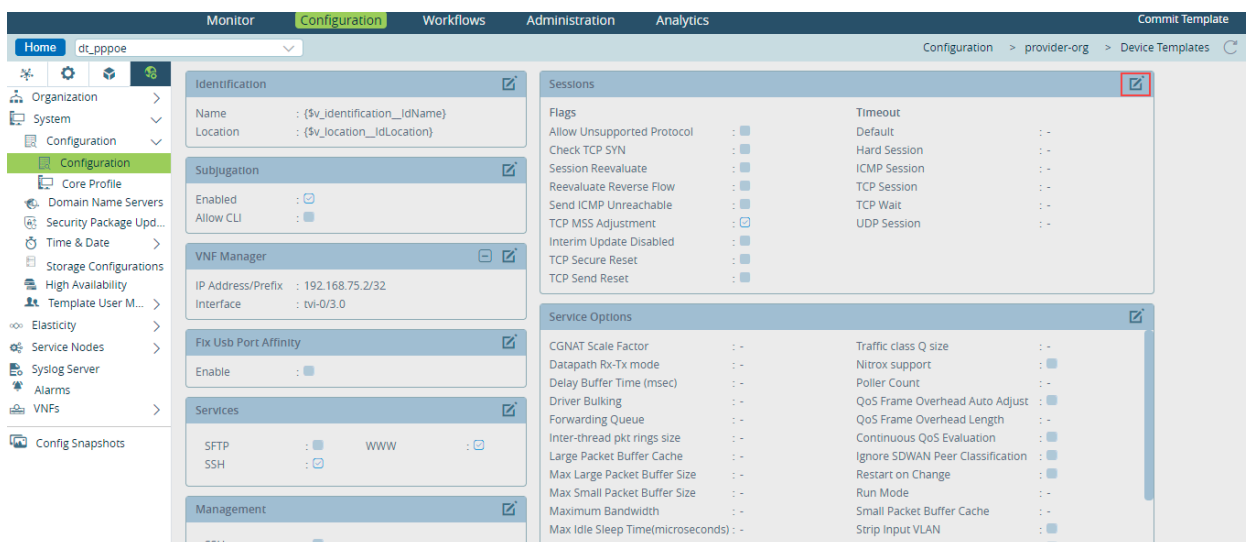
along the path between hosts has an interface MTU value less than the default MTU of 1500 bytes that is used by the other routers in the path. In this case, even though both Host A and Host B have MTU sizes of 1500 bytes on their interfaces, IP packets are fragmented on the link between Router 2 and Router 3, which can cause additional delay and extra load on both the hosts and the routers. To avoid this situation, you adjust the TCP MSS, which allows the VOS device to intercept TCP SYN packets passing through the router and adjust the MSS value.




You can configure the TCP Adjust MSS option either for all interfaces or only for the traffic going through the tunnel interfaces.

To configure the TCP Adjust MSS option:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a template in the main pane. The view changes to Appliance view.
2. Select Others > System > Configuration > Configuration in the left menu bar. The main pane displays various configuration-related panes.



3. In the Sessions pane, click the  Edit icon. In the Edit Sessions popup window, enter information for the following fields.

Edit Sessions

Timeout

Default

Hard Session

ICMP Session

TCP Session

TCP Wait

UDP Session

Flags

☐ Allow Unsupported Protocol

☐ Check TCP SYN

☐ Reevaluate Reverse Flow

☐ Send ICMP Unreachable

☐ Session Reevaluate

☐ TCP Secure Reset

☐ TCP Send Reset

TCP MSS Adjustment

☒ Enable

Interface Types

All

MSS Value

Interim Update

☐ Disable

Interim Update Interval

OK

Cancel

Field	Description
TCP MSS Adjustment (Group of Fields)	Configure the largest packet, in bytes, that the VOS device can receive in a single TCP segment.
<div>◦ Enable</div>	Click to allow the TCP MSS to be adjusted.

Field	Description
<ul style="list-style-type: none"> Interface Types 	Select the interface on which to adjust the TCP MSS adjustment: <ul style="list-style-type: none"> All—Set on all interfaces. Tunnel—Set only for the traffic that goes through the tunnel interface.
<ul style="list-style-type: none"> MSS Value 	Enter the TCP MSS value. Range: 536 through 8960 bytes Default: 1500 bytes

4. Click OK.

Configuration Examples

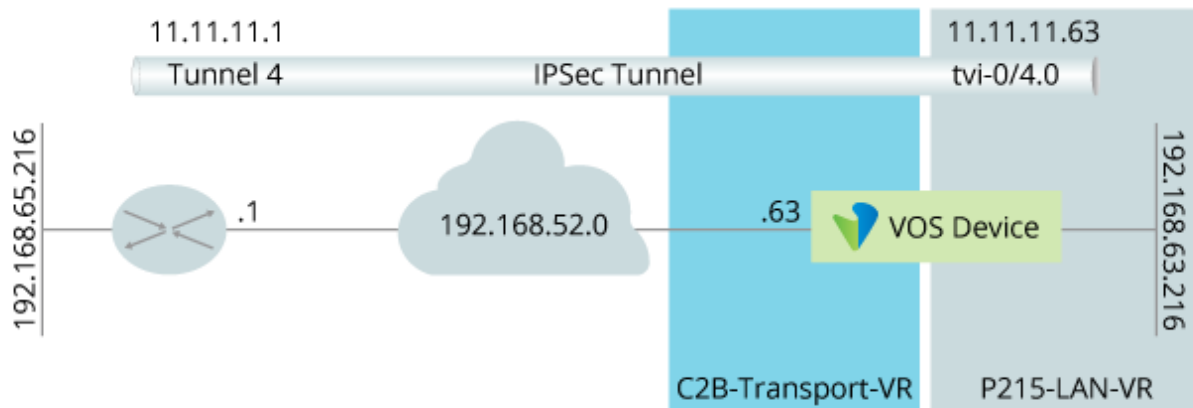
While it is strongly recommended that you to configure site-to-site tunnels using the Configuration and Workflows tabs in the Director GUI, you can also perform the configuration using CLI. You might find the presentation of the configuration in the CLI easier to follow, especially when you are configuring a large number of tunnels, and you might find it easier to cut and paste configuration parameters that are identical among devices. The examples in this section show the CLI versions of the site-to-site tunnel configurations between VOS and third-party devices.

IKEv2 Route-Based Site-to-Site Tunnel to a Cisco ASR Device

The following example shows the steps to configure an IKEv2 route-based site-to-site tunnel from a VOS device to a Cisco ASR device:

- Configure an IKEv2 route-based IPsec tunnel from a VOS device to a Cisco ASR1K device.
- Configure Layer 3 connectivity from the VOS LAN (here, 192.168.63.0/24) to the Cisco ASR1K LAN (here, 192.168.65.0/24).
- Use preshared keys and IP addresses for peer authentication.

The following figure illustrates the components of the configuration.



To configure an IKEv2 route-based site-to-site tunnel:

1. Configure the following parameters for the VOS interface on which to create the site-to-site tunnel. This interface is part of the C2B-Transport-VR virtual router. Note that this interface must already be defined. For more information, see [Configure Interfaces](#).

```
set interfaces vni-0/0 enable true
set interfaces vni-0/0 unit 0 enable true
set interfaces vni-0/0 unit 0 family
set interfaces vni-0/0 unit 0 family inet
set interfaces vni-0/0 unit 0 family inet address 192.168.52.63/24
```

2. Configure the tunnel interface on the branch that is part of the P215-LAN-VR virtual router. Traffic to the ASR1K LAN uses this tunnel through a static route.

```
set interfaces tvi-0/4 description To-ASR1K
set interfaces tvi-0/4 enable true
set interfaces tvi-0/4 family
set interfaces tvi-0/4 family inet
set interfaces tvi-0/4 family inet address 11.11.11.63/24
set routing-instances p215-LAN-VR networks [ Branch-LAN ]
set routing-instances p215-LAN-VR interfaces [ tvi-0/4.0 ]
```

3. Configure the VPN type to be site to site.

```
set orgs org-services p215 ipsec vpn-profile To-ASR1k vpn-type site-to-site
```

4. Define the authentication type, preshared key, IP address, key, local IP address, and source IP address for the VPN.

```
set orgs org-services p215 ipsec vpn-profile To-ASR1k local-auth-info
set orgs org-services p215 ipsec vpn-profile To-ASR1k local-auth-info auth-type psk
set orgs org-services p215 ipsec vpn-profile To-ASR1k local-auth-info id-type ip
set orgs org-services p215 ipsec vpn-profile To-ASR1k local-auth-info key versa123
set orgs org-services p215 ipsec vpn-profile To-ASR1k local-auth-info id-string 192.168.52.63
set orgs org-services p215 ipsec vpn-profile To-ASR1k local
set orgs org-services p215 ipsec vpn-profile To-ASR1k local inet 192.168.52.63
```

5. Configure the routing instance to establish IPsec, which is the transport VR routing instance for the IPsec tunnel. After the routing instance is established, the LAN virtual routing tunnel is automatically initiated.

```
set orgs org-services p215 ipsec vpn-profile To-ASR1k routing-instance C2B-Transport-VR
set orgs org-services p215 ipsec vpn-profile To-ASR1k tunnel-routing-instance p215-LAN-VR
set orgs org-services p215 ipsec vpn-profile To-ASR1k tunnel-initiate automatic
```

6. Configure the IPsec transform, set the IPsec mode to tunnel, and set other IPsec parameters.

```
set orgs org-services p215 ipsec vpn-profile To-ASR1k ipsec fragmentation pre-fragmentation
set orgs org-services p215 ipsec vpn-profile To-ASR1k ipsec force-nat-t disable
set orgs org-services p215 ipsec vpn-profile To-ASR1k ipsec transform esp-aes128-sha1
set orgs org-services p215 ipsec vpn-profile To-ASR1k ipsec mode tunnel
set orgs org-services p215 ipsec vpn-profile To-ASR1k ipsec pfs-group mod-none
set orgs org-services p215 ipsec vpn-profile To-ASR1k ipsec anti-replay disable
set orgs org-services p215 ipsec vpn-profile To-ASR1k ipsec keepalive-timeout 10
```

7. Define the IKE version as v2, and define the group transform and lifetime.

```
set orgs org-services p215 ipsec vpn-profile To-ASR1k ike version v2
set orgs org-services p215 ipsec vpn-profile To-ASR1k ike group mod2
set orgs org-services p215 ipsec vpn-profile To-ASR1k ike transform aes128-sha1
set orgs org-services p215 ipsec vpn-profile To-ASR1k ike lifetime 28800
```

8. Define peer authentication information such as authentication type, identification type, key, and the ID string expected from the Cisco ASR1K.

```
set orgs org-services p215 ipsec vpn-profile To-ASR1k peer-auth-info
set orgs org-services p215 ipsec vpn-profile To-ASR1k peer-auth-info auth-type psk
set orgs org-services p215 ipsec vpn-profile To-ASR1k peer-auth-info id-type ip
set orgs org-services p215 ipsec vpn-profile To-ASR1k peer-auth-info key versa123
set orgs org-services p215 ipsec vpn-profile To-ASR1k peer-auth-info id-string 192.168.52.1
```

9. Define the peer IP address.

```
set orgs org-services p215 ipsec vpn-profile To-ASR1k peer
set orgs org-services p215 ipsec vpn-profile To-ASR1k peer inet 192.168.52.1
```

10. Associate the site-to-site tunnel interface with the IPsec VPN profile.

```
set orgs org-services p215 ipsec vpn-profile To-ASR1k tunnel-interface tvi-0/4.0
```

11. Add a static route in the P215-LAN-VR virtual router for the tunnel to use for traffic destined to the 192.168.65.0 network.

```
set routing-instances p215-LAN-VR routing-options static route 192.168.65.0/24 11.11.11.1 none
  preference 1
set routing-instances p215-LAN-VR routing-options static route 192.168.65.0/24 11.11.11.1 none tag 0
```

To verify the site-to-site tunnel configuration:

1. Verify that IKE is configured. If IKE is successfully configured, the Event field under Event History shows the message IKE Done.


```

admin@VOS-cli> show orgs org-services p215 ipsec vpn-profile To-ASR1k ike history
Local Gateway: 192.168.52.63   Remote Gateway: 192.168.52.1
Last Known State      : Active
Last State Timestamp  : 2016-11-16T08:48:44.034025-21:**
Event History:
0. Event      : IKE Done
  Timestamp   : 2016-11-16T08:48:44.034027-59:20
  Role        : initiator
  Inbound SPI  : 0x2585b188f17a0002
  Outbound SPI : 0xb9a7a093c412fdb4

```

2. Verify that the tunnel interface is active. If the interface is active, the Administrative Status and Operational Status fields both show Up.

```

admin@VOS-cli> show interfaces detail tvi-0/4.0
Interface: tvi-0/4.0
Tenant      : 0
Vlan-Id     : n/a
Administrative status : up
Operational status   : up
Protocols Down : n/a
Interface index : 1058
Interface Role  : external
MAC address    : n/a
IP address     : [ 11.11.11.63/24 ]
Obtained from DHCP : False
DHCP Server IP  : n/a
DHCP Lease Time : n/a
DHCP Lease Expiry : n/a
Name Server 1 Address : n/a
Name Server 2 Address : n/a
Routing instance : p215-LAN-VR (12)
Host interface  : n/a
MTU            : 1400
Duplex / Speed  : auto / auto
  RX packets:13 errors:0
  RX bytes:2136
  TX packets:13 errors:0
  TX bytes:1252

```

3. Verify that traffic is being routed through the tunnel interface using the static address:

```

admin@VOS-cli> show route routing-instance p215-LAN-VR
Routes for Routing instance : p215-LAN-VR AFI: ipv4
Codes: E1 - OSPF external type 1, E2 - OSPF external type 2
IA - inter area, iA - intra area,
L1 - IS-IS level-1, L2 - IS-IS level-2
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
+ - Active Route
Prot Type Dest Address/Mask Next-hop Age Interface name
----
BGP N/A +0.0.0.0/0 169.254.24.1 04:25:39 Indirect
conn N/A +11.11.11.0/24 0.0.0.0 02:19:29 tvi-0/4.0
local N/A +11.11.11.63/32 0.0.0.0 02:19:29 directly connected

```

```

conn N/A +169.254.24.0/24 0.0.0.0 1w1d04h tvi-0/625.0
local N/A +169.254.24.2/32 0.0.0.0 1w1d04h directly connected
BGP N/A +192.168.0.0/16 10.1.64.104 1w1d02h Indirect
conn N/A +192.168.63.0/24 0.0.0.0 1w1d04h vni-0/1.0
local N/A +192.168.63.63/32 0.0.0.0 1w1d04h directly connected
static N/A +192.168.65.0/24 11.11.11.1 03:31:47 Indirect

```

4. Ping and verify connectivity to the remote end of the tunnel:

```

admin@VOS-cli> ping 11.11.11.1 routing-instance p215-LAN-VR
PING 11.11.11.1 (11.11.11.1) 56(84) bytes of data.
64 bytes from 11.11.11.1: icmp_seq=1 ttl=255 time=16.2 ms
64 bytes from 11.11.11.1: icmp_seq=2 ttl=255 time=1.25 ms
64 bytes from 11.11.11.1: icmp_seq=3 ttl=255 time=1.22 ms

```

5. Ping and verify connectivity to the remote LAN over the tunnel interface:

```

admin@VOS-cli> ping 192.168.65.1 routing-instance p215-LAN-VR
PING 192.168.65.1 (192.168.65.1) 56(84) bytes of data.
64 bytes from 192.168.65.1: icmp_seq=1 ttl=255 time=1.27 ms
64 bytes from 192.168.65.1: icmp_seq=2 ttl=255 time=1.15 ms
64 bytes from 192.168.65.1: icmp_seq=3 ttl=255 time=1.15 ms
64 bytes from 192.168.65.1: icmp_seq=4 ttl=255 time=9.29 ms

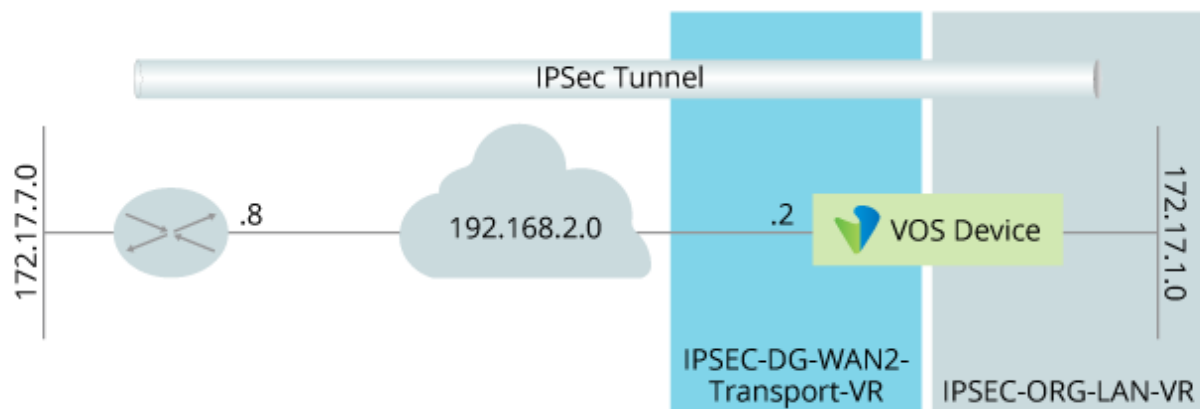
```

IKEv1 Policy-Based Site-to-Site Tunnel to a Cisco ASA Device

The following example shows the steps to configure an IKEv1 policy-based site-to-site tunnel from a VOS device to a Cisco ASA device:

- Configure an IKEv1 policy-based IPsec tunnel from a VOS device to a Cisco ASA device.
- Configure Layer 3 connectivity from a VOS LAN (here, 172.17.1.0/24) to Cisco ASA LAN (here, 172.17.7.0/24).
- Use preshared keys and IP addresses for peer authentication.

The following figure illustrates the components of the configuration.



To configure an IKEv1 policy-based site-to-site tunnel:

1. Configure the following parameters for the VOS interface on which to create the site-to-site tunnel. This interface is part of the IPSEC-DG-WAN2-Transport-VR virtual router. Note that this interface must already be defined. For more information, see [Configure Interfaces](#).

```
set interfaces vni-0/1 enable true
set interfaces vni-0/1 unit 0 vlan-id 0
set interfaces vni-0/1 unit 0 enable true
set interfaces vni-0/1 unit 0 family
set interfaces vni-0/1 unit 0 family inet
set interfaces vni-0/1 unit 0 family inet address 192.168.2.2/24
```

2. Configure the VPN type to be site to site.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA vpn-type site-to-site
```

3. Define the authentication type, PSK, IP address, key, local IP address, and source IP address for the VPN.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA local-auth-info
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA local-auth-info auth-
type psk
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA local-auth-info id-type
ip
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA local-auth-info key
versa123
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA local-auth-info id-
string 192.168.2.2
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA local
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA local address 192.
168.2.2
```

4. Configure the routing instance to establish IPsec, which is the transport VR routing instance for the IPsec tunnel. After the routing instance is established, the LAN virtual routing tunnel is automatically initiated.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA routing-instance
IPSEC-DG-WAN2-Transport-VR
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA tunnel-routing-
instance IPSEC-ORG-LAN-VR
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA tunnel-initiate
automatic
```

5. Configure the IPsec transform, IPsec mode to tunnel, and other IPsec parameters.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ipsec fragmentation
pre-fragmentation
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ipsec force-nat-t
disable
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ipsec transform esp-
aes128-md5
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ipsec mode tunnel
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ipsec pfs-group mod-
none
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ipsec anti-replay
```

```
enable
```

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ipsec life duration 800
```

6. Define the IKE version as v1, and define the group transform and lifetime.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ike version v1
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ike mode aggressive
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ike group mod2
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ike transform aes256-sha1
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ike lifetime 900
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ike dpd-timeout 30
```

7. Define the peer authentication information such as authentication type, identification type, key, and the ID string expected from the Cisco ASA.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA peer-auth-info
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA peer-auth-info auth-type psk
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA peer-auth-info id-type ip
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA peer-auth-info key versa123
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA peer-auth-info id-string 192.168.2.8
```

8. Define the peer IP address.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA peer
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA peer address [ 192.168.2.8 ]
```

9. Configure the IKEv1 policy.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA rule RULE1 src inet 172.17.1.0/24
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA rule RULE1 src port 0
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA rule RULE1 dst inet 172.17.7.0/24
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA rule RULE1 dst port 0
```

To verify the site-to-site tunnel configuration:

1. Verify that IKE is configured. If IKE is successfully configured, the Event field under Event History shows the message IKE Done.

```
admin@VOS-cli> show orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-ASA ike history
Local Gateway: 192.168.2.2    Remote Gateway: 192.168.2.8
Last Known State      : Active
Last State Timestamp  : 2020-04-29T19:04:27.246568-08:00
Event History:
  0. Event      : IKE Done
    Timestamp   : 2020-04-29T19:04:27.246593-08:00
```

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration...

Updated: Wed, 23 Oct 2024 07:24:09 GMT

Copyright © 2024, Versa Networks, Inc.

```
Role      : initiator
Inbound SPI : 0x200243fa3029b20
Outbound SPI : 0xa02058c9546045b8
```

2. Verify that the IPsec is active. If IPsec is active, the Last Known State field shows the message Active (Rekey).

```
admin@VOS-cli> show orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-
ASA ipsec history
Local Gateway: 192.168.2.2    Remote Gateway: 192.168.2.8
Last Known State      : Active (Rekey)
Last State Timestamp   : 2020-04-29T19:08:57.460422-08:00
Event History:
0. Event      : IPsec Rekey
   Timestamp   : 2020-04-29T19:08:57.460447-08:00
   Inbound SPI  : 0x20073eb
   Outbound SPI : 0xedcb26b1
```

3. Verify the status of the security associations (SA).

```
admin@VOS-cli> show orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-
ASA security-associations brief
Remote Gateway Transform Inbound SPI Bytes/sec Outbound SPI Bytes/sec Up Time Next Rekey
Time
-----
192.168.2.8    aes-cbc 0x20073eb 0 0xedcb26b1 0 6d18h59m 00:09:22
```

4. Ping and verify connectivity to the remote end of the tunnel.

```
admin@VOS-cli> ping 11.11.11.1 routing-instance p215-LAN-VR
PING 11.11.11.1 (11.11.11.1) 56(84) bytes of data.
64 bytes from 11.11.11.1: icmp_seq=1 ttl=255 time=16.2 ms
64 bytes from 11.11.11.1: icmp_seq=2 ttl=255 time=1.25 ms
64 bytes from 11.11.11.1: icmp_seq=3 ttl=255 time=1.22 ms
```

5. Ping and verify connectivity to the remote LAN over the tunnel interface.

```
versa@Client1:~$ sudo ip netns exec Flex-V1 ping 172.17.7.10
PING 172.17.7.10 (172.17.7.10) 56(84) bytes of data.
64 bytes from 172.17.7.10: icmp_seq=1 ttl=63 time=3.34 ms
64 bytes from 172.17.7.10: icmp_seq=2 ttl=63 time=3.56 ms
64 bytes from 172.17.7.10: icmp_seq=3 ttl=63 time=2.10 ms
64 bytes from 172.17.7.10: icmp_seq=4 ttl=63 time=3.69 ms64 bytes from 172.17.7.10: icmp_seq=5 ttl=63
time=1.52 ms
```

6. Check IPsec statistics.

```
admin@VOS-cli> show orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV1-CISCO-
ASA statistics
Statistics:
# IPsec Established      : 722
# IPsec Rekeys           : 794
# IKE Notify - Invalid SPI : 58
# IKE Are you There messages : 28810
# IKE Are you There Ack messages : 398
```

```

Inbound Statistics:
# IKE packets : 0
# IKE Packets - Trigger PM : 0
# ESP/AH Packets (to decap) : 178154
# ESP/AH Bytes (to decap) : 27079408
# ESP Packets (to decap) : 178154
# AH Packets (to decap) : 0
# Packets - After IPsec processing : 178154
# Anti-replay failure - out of order : 0
# Anti-replay failure - duplicate : 0
# NAT-T packets : 0
# NAT-T keep-alive packets : 0
# Packets dropped - Invalid IKE : 0
# Packets dropped - Unknown SPI : 0
# Packets dropped - Invalid SPI : 0
# Packets dropped - No SA : 0
# Packets dropped - Anti-replay : 0
# Packets dropped - Auth failure : 0
# Packets dropped - Invalid : 0

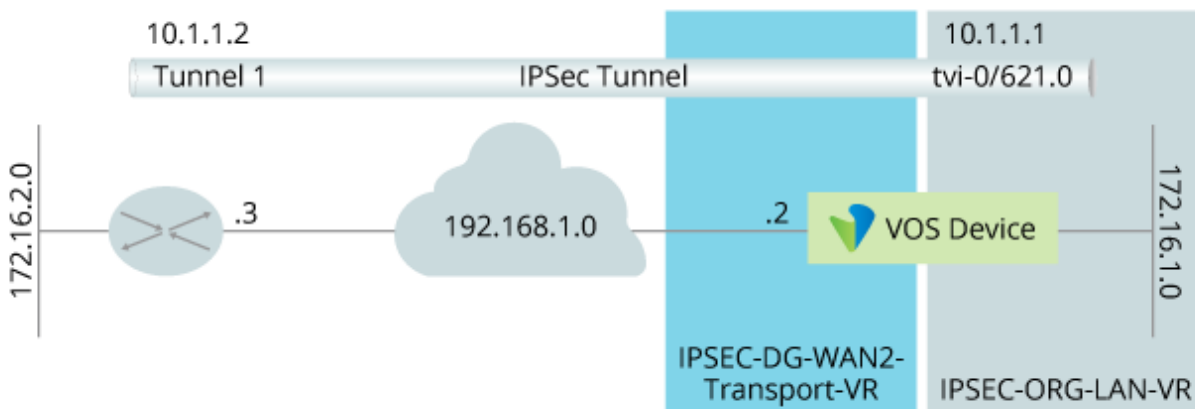
```

IKEv2 Route-Based Site-to-Site Tunnel to a Cisco CSR Device

The following example shows the steps to configure an IKEv2 route-based site-to-site tunnel from a VOS device to a Cisco CSR device:

- Configure an IKEv2 route-based IPsec tunnel from a VOS device to a Cisco CSR device.
- Configure Layer 3 connectivity from a VOS LAN (here, 172.16.1.0/24) to Cisco DSR LAN (here, 172.16.2.0/24).
- Use preshared keys and IP addresses for peer authentication.

The following figure illustrates the components of the configuration.



To configure an IKEv2 route-based site-to-site tunnel:

1. Configure the following parameters for the VOS interface on which to create the site-to-site tunnel. This interface is part of the IPSEC-DG-WAN2-Transport-VR virtual router. Note that this interface must already be defined. For

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configura...

Updated: Wed, 23 Oct 2024 07:24:09 GMT

Copyright © 2024, Versa Networks, Inc.

more information, see [Configure Interfaces](#).

```
set interfaces vni-0/0 enable true
set interfaces vni-0/0 unit 0 vlan-id 0
set interfaces vni-0/0 unit 0 enable true
set interfaces vni-0/0 unit 0 family
set interfaces vni-0/0 unit 0 family inet
set interfaces vni-0/0 unit 0 family inet address 192.168.1.2/24
```

2. Configure the tunnel interface on the branch that is part of the IPSEC-ORG-LAN-VR virtual router. Traffic to the Cisco CSR LAN uses this tunnel through a static route.

```
set interfaces tvi-0/621 enable true
set interfaces tvi-0/621 mtu 1400
set interfaces tvi-0/621 mode ipsec
set interfaces tvi-0/621 type ipsec
set interfaces tvi-0/621 unit 0 enable true
set interfaces tvi-0/621 unit 0 family
set interfaces tvi-0/621 unit 0 family inet
set interfaces tvi-0/621 unit 0 family inet address 10.1.1.1/24
```

3. Configure the VPN type to be site to site.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR vpn-type site-to-site
```

4. Define the authentication type, PSK, IP address, key, local IP address, and source IP address for the VPN.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR local-auth-info
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR local-auth-info auth-
type psk
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR local-auth-info id-type
ip
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR local-auth-info key
versa123
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR local-auth-info id-
string 192.168.1.2
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR local
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR local interface-name
vni-0/0.0
```

4. Configure the routing instance to establish IPsec, which is the transport VR routing instance for the IPsec tunnel. After the routing instance is established, the LAN virtual routing tunnel is automatically initiated.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR routing-instance
IPSEC-DG-WAN1-Transport-VR
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR tunnel-routing-
instance IPSEC-ORG-LAN-VR
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR tunnel-initiate
automatic
```

5. Configure the IPsec transform, IPsec mode to tunnel, and other IPsec parameters.

```
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ipsec fragmentation
pre-fragmentation
```

```

set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ipsec force-nat-t
disable
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ipsec transform esp-
aes128-sha1
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ipsec mode tunnel
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ipsec pfs-group mod-
none
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ipsec anti-replay
disable
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ipsec life duration 900

```

6. Define the IKE version as v2, and define the group transform and lifetime.

```

set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ike version v2
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ike group mod2
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ike transform aes128-
sha1
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ike lifetime 900
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR ike dpd-timeout 30

```

7. Define the peer authentication information such as authentication type, identification type, key, and the ID string expected from the Cisco CSR device.

```

set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR peer-auth-info
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR peer-auth-info auth-
type psk
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR peer-auth-info id-type
ip
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR peer-auth-info key
versa123
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR peer-auth-info id-
string 192.168.1.3

```

8. Define the peer IP address.

```

set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR peer
set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR peer address [ 192.
168.1.3 ]

```

9. Associate the site-to-site tunnel interface with an IPsec VPN profile.

```

set orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-CSR tunnel-interface tvi-0/
621.0

```

9. Add a static route in the IPSEC-ORG-LAN-VR virtual router to use the tunnel for traffic destined to the 172.16.2.0 network.

```

set routing-instances IPSEC-ORG-LAN-VR routing-options static route 172.16.2.0/24 10.1.1.2 none
preference 1
set routing-instances IPSEC-ORG-LAN-VR routing-options static route 172.16.2.0/24 10.1.1.2 none tag 0

```

To verify the site-to-site tunnel configuration:

1. Verify that IKE is configured. If IKE is successfully configured, the Event field under Event History shows the

message IKE Done.

```
admin@VOS-cli> show orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-
CSR ike history
Local Gateway: 192.168.1.2    Remote Gateway: 192.168.1.3
Last Known State      : Active (Rekey)
Last State Timestamp  : 2020-04-29T20:39:04.814583-08:00
Event History:
0. Event      : IKE Done
  Timestamp   : 2020-04-29T20:39:04.814608-08:00
  Role        : initiator
  Inbound SPI  : 0x2005ec193252605
  Outbound SPI : 0xaf1d00b6a3f770da
```

2. Verify that IPsec is active. If the IPsec is active, the Event field under Event History shows the message IPsec Rekey.

```
admin@VOS-cli> show orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-
CSR ipsec history
Local Gateway: 192.168.1.2    Remote Gateway: 192.168.1.3
Last Known State      : Active (Rekey)
Last State Timestamp  : 2020-04-29T20:40:36.875453-08:00
Event History:
0. Event      : IPsec Rekey
  Timestamp   : 2020-04-29T20:40:36.875478-08:00
  Inbound SPI  : 0x200760b
  Outbound SPI : 0x521e3318
```

3. Verify the status of the security associations (SA).

```
admin@VOS-cli> show orgs org-services IPSEC-ORG ipsec vpn-profile SITE-2-SITE-IKEV2-CISCO-
CSR security-associations brief
Remote Gateway Transform Inbound SPI Bytes/sec Outbound SPI Bytes/sec Up Time Next Rekey
Time
-----
192.168.1.3    aes-cbc 0x200760b 10    0x521e3318 0    6d20h33m 00:09:05
```

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Releases 20.2.1 adds support for the unmanaged and Zscaler unmanaged peer types.
- Release 21.1.1 adds support for the AWS transit gateway peer type and the GRE tunnel protocol for peer type Zscaler.
- Releases 21.2.1 adds support for configuring NATed public IP address for Azure virtual WAN and AWS transit gateway, and for configuring a Versa Director–managed site-to-site tunnel.
- Releases 22.1.1 adds support for the GRE tunnel protocol for AWS transit gateway.

Additional Information

[Configure Basic Features](#)

[Configure Interfaces](#)

[Create and Manage Staging and Post-Staging Templates](#)

[Troubleshoot Connectivity Issues](#)