

---

## Configure SASE Site-to-Site Tunnels

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

You can use site-to-site tunnels to encapsulate packets that are transmitted by a transport protocol. You can configure secure IPsec tunnels and generic routing encapsulation (GRE) tunnels from Versa Networks SASE gateways to data centers and to on-premises routers in an enterprise network. Site-to-site IPsec tunnels provide users with secure access to applications and workloads that are hosted in the cloud. The gateway device can be either a physical device or a cloud-based SD-WAN device. The remote (peer) device can be a cloud-managed service or a third-party device that supports IPsec tunnels.

Note: You must configure the following SASE rules, profiles, and settings in the following order:

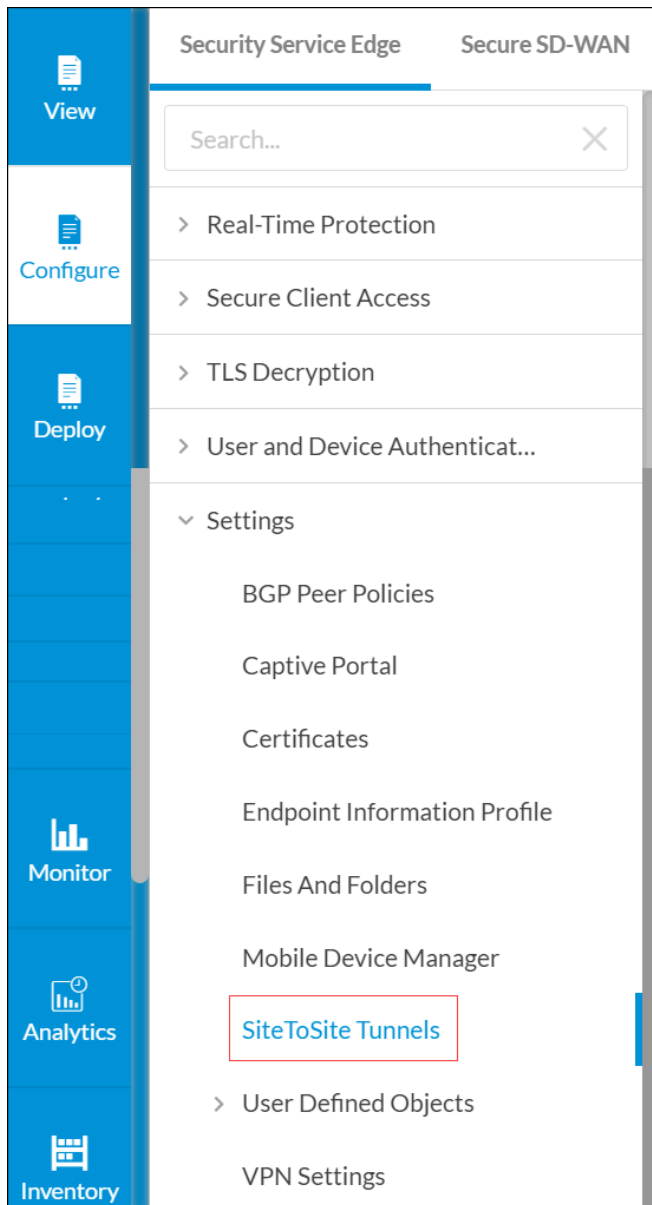
1. Configure users and user groups first, and then publish them to the gateway. For more information, see [Configure User and Device Authentication](#).
2. Configure site-to-site tunnels, as described in this article.
3. Configure secure client access profiles and rules. For more information, see [Configure SASE Secure Client Access Rules](#).

You do not need to configure the remaining SASE rules, profiles, and settings in any particular order.

---

## Configure Site-to-Site Tunnels

1. Go to Configure > Settings > SiteToSite Tunnels.



The following screen displays.

Configure > SASE > Settings > Site-to-Site Tunnels

Site-to-Site Tunnels Publish

Below are all the Site-to-Site Tunnels

	NAME	GATEWAY	TYPE	DESCRIPTION	TAGS	LAST MODIFIED	ENABLED
<input type="checkbox"/>	> GW1-Tunnel	USA-West-GW-2	IPSec	Tunnel between USA West and GW1	tunnel tunnel2	10/11/2022, 8:34:35 PM Administrator	Enabled
<input type="checkbox"/>	> GW2-Tunnel	USA-East-GW-1	GRE	GRE tunnel to GW in USA East	Tunnel	10/31/2021, 6:27:39 AM Administrator	Enabled

Showing 1-2 of 2 results 10 Rows per Page Go to page 1 < Previous 1 Next >

2. To customize which columns display, click to select or deselect the columns you want to display. Click Reset to return to the default columns settings.

Select Columns

☒ Gateway

☒ Type

☒ Description

☒ Tags

☒ Last Modified

☒ Enabled

Reset

3. Click + Add to create a new tunnel. In the Add Site-to-Site Tunnel screen, enter information for the following fields in the Enter Type section.

View

Configure

Deploy

Monitor

Analytics Configure

Deploy

Monitor

Analytics

Inventory

Configure > SASE > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

Publish

1 ENTER TYPE

Type

☒ IPsec
 ☐ GRE

☒ Enabled

Tunnel Type

Route Based

Gateway Link

Versa Gateway

Select

Remote Public IP Address or FQDN

Enter IP Address or FQDN

The IPsec tunnel is configured on the Gateway as Responder-only. This means that the IKE session has to be initiated by the peer.

Cancel

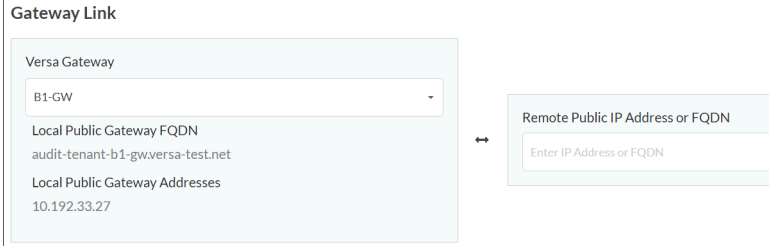
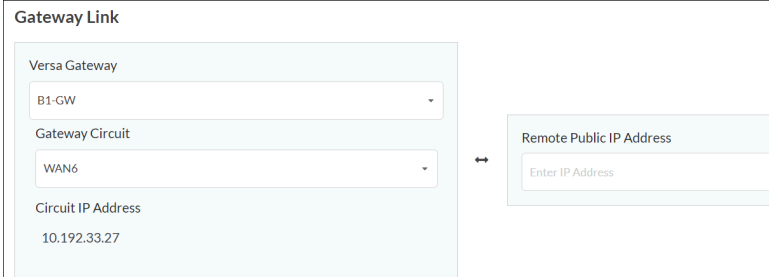
Next

2 ENTER IPSEC INFORMATION

3 ENTER ADDRESS & ROUTING / POLICY CONFIGURATIONS

4 ENTER NAME, DESCRIPTION & TAGS

Field	Description
Type	Select the tunnel type: <ul style="list-style-type: none"> <li>GRE</li> <li>IPsec (for Releases 11.4.1 and later)</li> </ul>
Enabled	Click the slider to enable the tunnel.
Tunnel Type	For the IPsec tunnel type, select the tunnel configuration to use: <ul style="list-style-type: none"> <li>Policy-based (for Releases 11.4.1 and later)</li> <li>Route-based</li> </ul>
Gateway Link (Group of Fields)	

Field	Description
<ul style="list-style-type: none"> <li>Versa Gateway</li> </ul>	<p>For an IPsec tunnel type, select a gateway, and then enter the IP address or FQDN of the remote device. For Releases 11.4.1 and later, optionally enter a remote public IP address or FQDN.</p> 
	<p>For the GRE tunnel type, select a gateway, then select a gateway circuit, and then enter the IP address of the remote device.</p> 

- Click Next. For the IPsec tunnel type, enter information for the following fields in the Enter IPsec Information section. For the GRE tunnel type, continue with the next step, Enter Address and Routing/Policy Configurations.

View

Configure

Deploy

Monitor Deploy

Monitor

Deploy

Monitor

Deploy

Monitor

Deploy

Monitor

Analytics

Inventory

Configure > SASE > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

Publish

1

ENTER TYPE

+

2

ENTER IPSEC INFORMATION

-

3

ENTER ADDRESS & ROUTING / POLICY CONFIGURATIONS

+

4

ENTER NAME, DESCRIPTION & TAGS

+

✓

ENTER TYPE

+

2

ENTER IPSEC INFORMATION

-

IKE

Version

Transform

Diffie Hellman Group (DH Group)

V2

aes256-sha1

Diffie-Hellman Group 19 - 256 bit elliptic

DPD Timeout

Unit Type

IKE Rekey Time

30

Seconds

28800

IPSec

IPSec Transform

Perfect Forward Secrecy Group (PFS Group)

esp-aes256-sha1

Diffie-Hellman Group 19 - 256 bit elliptic curve

Hello Interval

Unit Type

IPsec Rekey Time

10

Seconds

28800

Authentication

☒ PSK

☐ Certificate

Local

Identity Type

Value

Share Key

Select

Enter value

Enter key

Remote

Identity Type

Value

Share Key

Select

Enter value

Enter key

Cancel

Next

Field	Description
IKE (Group of Fields)	
<ul style="list-style-type: none"> <li>Version</li> </ul>	Select the IKE version: <ul style="list-style-type: none"> <li>V1</li> <li>V2</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>◦ V1 or V2</li> </ul>
<ul style="list-style-type: none"> <li>◦ Transform</li> </ul>	<p>Select the IKE transform type to use:</p> <ul style="list-style-type: none"> <li>◦ 3des-md5</li> <li>◦ 3des-sha1</li> <li>◦ aes128-sha1</li> <li>◦ aes128-md5</li> <li>◦ aes256-sha1</li> <li>◦ aes256-md5</li> <li>◦ aes128-sha256</li> <li>◦ aes256-sha256</li> <li>◦ aes128-sha384</li> <li>◦ aes256-sha384</li> <li>◦ aes128-sha512</li> <li>◦ aes256-sha512</li> </ul>
<ul style="list-style-type: none"> <li>◦ Diffie-Hellman Group (DH Group)</li> </ul>	<p>Select the Diffie-Hellman group to use:</p> <ul style="list-style-type: none"> <li>◦ Diffie-Hellman Group 1—768-bit modulus</li> <li>◦ Diffie-Hellman Group 2—1024-bit modulus. This is the default.</li> <li>◦ Diffie-Hellman Group 5—1536-bit modulus</li> <li>◦ Diffie-Hellman Group 14—2048-bit modulus</li> <li>◦ Diffie-Hellman Group 15—3072-bit modulus</li> <li>◦ Diffie-Hellman Group 16—4096-bit modulus</li> <li>◦ Diffie-Hellman Group 19—256-bit elliptic curve</li> <li>◦ Diffie-Hellman Group 20—384-bit elliptic curve</li> <li>◦ Diffie-Hellman Group 21—521-bit elliptic curve</li> <li>◦ Diffie-Hellman Group 25—192-bit elliptic curve</li> <li>◦ Diffie-Hellman Group 26—224-bit elliptic curve</li> <li>◦ No PFS</li> </ul> <p><i>Default:</i> Diffie-Hellman Group 2—1024-bit modulus</p>
<ul style="list-style-type: none"> <li>◦ DPD Timeout</li> </ul>	<p>Enter how long to wait for traffic from the destination peer on the tunnel before sending a dead-peer-</p>

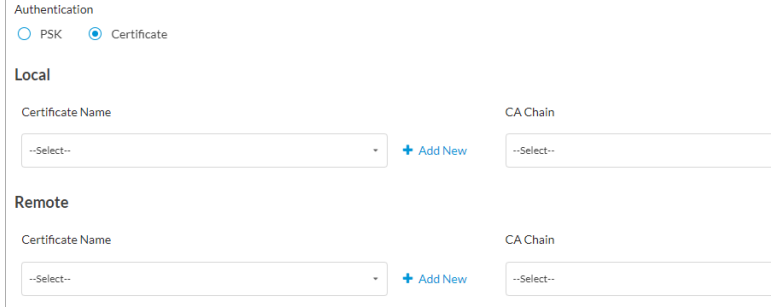
Field	Description
	<p>detection (DPD) request packet.</p> <p><i>Range:</i> 10 through 180 seconds</p> <p><i>Default:</i> 30 seconds</p>
<ul style="list-style-type: none"> <li>Unit Type</li> </ul>	<p>Select the time units for how often to regenerate the IKE key, and then enter the time interval:</p> <ul style="list-style-type: none"> <li>Hours</li> <li>Minutes</li> <li>Seconds</li> </ul>
<ul style="list-style-type: none"> <li>IKE Rekey Time</li> </ul>	<p>Enter how often to regenerate the IKE key. The value range depends on the units you select in the Unit Type field.</p> <p><i>Range:</i></p> <ul style="list-style-type: none"> <li>132 through 86400, for seconds</li> <li>3 through 1440, for minutes</li> <li>1 through 24, for hours</li> </ul> <p><i>Default:</i> 28800 seconds</p>
IPsec (Group of Fields)	
<ul style="list-style-type: none"> <li>IPsec Transform</li> </ul>	<p>Select the IPsec transform type to use:</p> <ul style="list-style-type: none"> <li>esp-3des-md5</li> <li>esp-3des-sha1</li> <li>esp-aes128-ctr-sha1</li> <li>esp-aes128-ctr-xcbc</li> <li>esp-aes128-gcm</li> <li>esp-aes128-md5</li> <li>esp-aes128-sha1</li> <li>esp-aes128-sha256</li> <li>esp-aes128-sha384</li> <li>esp-aes128-sha512</li> <li>esp-aes256-gcm</li> </ul>



Field	Description
	<ul style="list-style-type: none"> <li>◦ esp-aes256-md5</li> <li>◦ esp-aes256-sha1</li> <li>◦ esp-aes256-sha256</li> <li>◦ esp-aes256-sha384</li> <li>◦ esp-aes256-sha512</li> <li>◦ esp-null-md5</li> </ul>
<ul style="list-style-type: none"> <li>◦ Perfect Forward Secrecy Group (PFS Group)</li> </ul>	<p>Select the Diffie-Hellman groups to use for PFS:</p> <ul style="list-style-type: none"> <li>◦ Diffie-Hellman Group 1—768-bit modulus</li> <li>◦ Diffie-Hellman Group 2—1024-bit modulus.</li> <li>◦ Diffie-Hellman Group 5—1536-bit modulus</li> <li>◦ Diffie-Hellman Group 14—2048-bit modulus</li> <li>◦ Diffie-Hellman Group 15—3072-bit modulus</li> <li>◦ Diffie-Hellman Group 16—4096-bit modulus</li> <li>◦ Diffie-Hellman Group 19—256-bit elliptic curve</li> <li>◦ Diffie-Hellman Group 20—384-bit elliptic curve</li> <li>◦ Diffie-Hellman Group 21—521-bit elliptic curve</li> <li>◦ Diffie-Hellman Group 25—192-bit elliptic curve</li> <li>◦ Diffie-Hellman Group 26—224-bit elliptic curve</li> <li>◦ No PFS. This is the default.</li> </ul> <p><i>Default:</i> No PFS</p>
<ul style="list-style-type: none"> <li>◦ Hello Interval</li> </ul>	<p>Enter the IPsec keepalive timeout, which is how often to send a Hello message to the peer to determine whether the peer is still up and operational.</p> <p><i>Range:</i> 0 through 36000 seconds</p> <p><i>Default:</i> 10 seconds</p>
<ul style="list-style-type: none"> <li>◦ Unit Type</li> </ul>	<p>Select the time units for how often to regenerate the IPsec key, and then enter the time interval:</p> <ul style="list-style-type: none"> <li>◦ Hours</li> <li>◦ Minutes</li> <li>◦ Seconds</li> </ul>

Field	Description						
	<i>Default:</i> Seconds						
<ul style="list-style-type: none"><li>◦ IPsec Rekey Time</li></ul>	<p>Enter how often to regenerate the IPsec key. The value range depends on the units you select in the Unit Type field.</p> <p><i>Range:</i></p> <ul style="list-style-type: none"><li>◦ 132 through 86400, for seconds</li><li>◦ 3 through 1440, for minutes</li><li>◦ 1 through 24, for hours</li></ul> <p><i>Default:</i> 28800 seconds</p>						
<ul style="list-style-type: none"><li>◦ Authentication</li></ul>	<p>Select the authentication:</p> <ul style="list-style-type: none"><li>◦ Certificate Authentication</li><li>◦ PSK</li></ul>						
<ul style="list-style-type: none"><li>◦ Local—PSK Authentication (Group of Fields)</li></ul>	<p>For PSK authentication, enter information for the following fields:</p> <div><div><div>Authentication</div><div><input checked="" type="radio"/> PSK <input type="radio"/> Certificate</div></div><div><div>Local</div><div><div>Identity Type</div><div>Email</div></div><div><div>Value</div><div>Enter value</div></div></div><div><div>Remote</div><div><div>Identity Type</div><div>Email</div></div><div><div>Value</div><div>Enter value</div></div></div></div> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Local (Group of Fields)</td><td></td></tr><tr><td><ul style="list-style-type: none"><li>◦ Identity Type</li></ul></td><td>Select an identity type:</td></tr></table>	Field	Description	Local (Group of Fields)		<ul style="list-style-type: none"><li>◦ Identity Type</li></ul>	Select an identity type:
Field	Description						
Local (Group of Fields)							
<ul style="list-style-type: none"><li>◦ Identity Type</li></ul>	Select an identity type:						

Field	Description																
	<table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td></td><td> <ul style="list-style-type: none"> <li>◦ Email</li> <li>◦ FQDN</li> <li>◦ IP address</li> </ul> </td></tr> <tr> <td>◦ Value</td><td>           Enter a value for the identity type:           <ul style="list-style-type: none"> <li>◦ Email—Enter a valid email address.</li> <li>◦ FQDN—Enter a valid FQDN.</li> <li>◦ IP Address—Enter a valid IP address.</li> </ul> </td></tr> <tr> <td>◦ Share Key</td><td>Enter the share key for the local devices.</td></tr> <tr> <td colspan="2">Remote (Group of Fields)</td></tr> <tr> <td>◦ Identity Type</td><td>           Select an identity type:           <ul style="list-style-type: none"> <li>◦ Email</li> <li>◦ FQDN</li> <li>◦ IP address</li> </ul> </td></tr> <tr> <td>◦ Value</td><td>           Enter a value for the identity type:           <ul style="list-style-type: none"> <li>◦ Email—Enter a valid email address.</li> <li>◦ FQDN—Enter a valid FQDN.</li> <li>◦ IP Address—Enter a valid IP address.</li> </ul> </td></tr> <tr> <td>◦ Share Key</td><td>Enter the share key for the remote devices.</td></tr> </table>	Field	Description		<ul style="list-style-type: none"> <li>◦ Email</li> <li>◦ FQDN</li> <li>◦ IP address</li> </ul>	◦ Value	Enter a value for the identity type: <ul style="list-style-type: none"> <li>◦ Email—Enter a valid email address.</li> <li>◦ FQDN—Enter a valid FQDN.</li> <li>◦ IP Address—Enter a valid IP address.</li> </ul>	◦ Share Key	Enter the share key for the local devices.	Remote (Group of Fields)		◦ Identity Type	Select an identity type: <ul style="list-style-type: none"> <li>◦ Email</li> <li>◦ FQDN</li> <li>◦ IP address</li> </ul>	◦ Value	Enter a value for the identity type: <ul style="list-style-type: none"> <li>◦ Email—Enter a valid email address.</li> <li>◦ FQDN—Enter a valid FQDN.</li> <li>◦ IP Address—Enter a valid IP address.</li> </ul>	◦ Share Key	Enter the share key for the remote devices.
Field	Description																
	<ul style="list-style-type: none"> <li>◦ Email</li> <li>◦ FQDN</li> <li>◦ IP address</li> </ul>																
◦ Value	Enter a value for the identity type: <ul style="list-style-type: none"> <li>◦ Email—Enter a valid email address.</li> <li>◦ FQDN—Enter a valid FQDN.</li> <li>◦ IP Address—Enter a valid IP address.</li> </ul>																
◦ Share Key	Enter the share key for the local devices.																
Remote (Group of Fields)																	
◦ Identity Type	Select an identity type: <ul style="list-style-type: none"> <li>◦ Email</li> <li>◦ FQDN</li> <li>◦ IP address</li> </ul>																
◦ Value	Enter a value for the identity type: <ul style="list-style-type: none"> <li>◦ Email—Enter a valid email address.</li> <li>◦ FQDN—Enter a valid FQDN.</li> <li>◦ IP Address—Enter a valid IP address.</li> </ul>																
◦ Share Key	Enter the share key for the remote devices.																

Field	Description
<ul style="list-style-type: none"> <li>Local—Certificate Authentication (Group of Fields)</li> </ul>	<p>For Certificate Authentication, enter information for the following fields:</p>  <ul style="list-style-type: none"> <li>Certificate Name—Select a certificate name for both the local and remote devices.</li> <li>CA Chain—Select a CA chain for both the local and remote devices.</li> </ul> <p>Click + Add New to add new certificates names and CA chains for the local and remote devices. For more information, see <a href="#">Configure SASE Certificates</a>.</p>

- Click Next.
- For the GRE tunnel type and for a route-based tunnel configuration for an IPsec tunnel type, enter information for the following fields in the Enter Address and Routing/Policy Configurations section, and then continue with Step 8. Note that Enter IPsec Information section is not applicable for GRE tunnel type. For the Policy-based tunnel configuration for an IPsec tunnel type, continue with Step 7.

View

Configure

Deploy

Monitor

Deploy

Monitor

Monitor

Monitor

Analytics

Inventory

Configure > SASE > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

Publish

✓ ENTER TYPE

+

✓ ENTER IPSEC INFORMATION

+

3 ENTER ADDRESS & ROUTING / POLICY CONFIGURATIONS

-

Setup the Versa SASE Gateway routing towards the enterprise VPN.

Tunnel Virtual Interface IP Address

Tunnel Virtual Interface IP Address

VPN Name

Audit-Tenant-Enterprise

MTU

Static Routes

+ Add

Routing Protocol

☐ EBGP
☒ None



Cancel

Next

4 ENTER NAME, DESCRIPTION & TAGS

+

Field	Description
Tunnel Virtual Interface IP Address	Enter the tunnel virtual interface IP address.
VPN Name	Select the VPN through which the IP address is reachable.
MTU	<p>(For Releases 11.4.1 and later.) Enter the maximum transmission unit size, in bytes, of the largest protocol data unit that the port can receive or transmit.</p> <p><i>Range: 256 through 9000 bytes</i></p>
Static Routes (Group of Fields)	

Field	Description
<ul style="list-style-type: none"> <li>+ Add</li> </ul>	<p>Click to add a static route. Enter information for the following fields.</p> <div> <div>IPv4 Destination</div> <div>Enter IP Address</div> </div> <div> <div>Preference</div> <div>Enter value</div> </div> <ul style="list-style-type: none"> <li>IPv4 Destination—Enter the IPv4 destination address.</li> <li>Preference—Enter a preference value for the static route. <i>Range:</i> 1 through 255 <i>Default:</i> None</li> <li> Minus icon—Click to delete a static route entry.</li> <li> Plus icon—Click to add a static route entry.</li> </ul>
Routing Protocol	<p>Select the routing protocol:</p> <ul style="list-style-type: none"> <li>EBGP</li> <li>None</li> </ul> <p>If you select None, no further information is required. If you select EBGP, enter information for the following fields.</p> <div> <div>Routing Protocol</div> <div> <input checked="" type="radio"/> EBGP           <input type="radio"/> None         </div> <div>Local ASN</div> <div>Enter value</div> <div> <input type="checkbox"/> BFD         </div> <div> <div>Neighbor Address</div> <div>Enter IPv4/IPv6 address</div> </div> <div> <div>ASN</div> <div>Enter value</div> </div> <div> <div>Password</div> <div>Should be between 4 and 128 characters</div> </div> <div> <div>Local Address:</div> <div>Select</div> </div> <div> <div>Export Policy</div> <div>Select</div> </div> <div> <div>Cancel</div> <div>Next</div> </div> </div>

Field	Description
	<ul style="list-style-type: none"> <li>Local ASN—Enter the local AS number.</li> <li>BFD—Click the slider to enable Bidirectional Forwarding (BFD).</li> <li>Neighbor Address—Enter the IP address of the peer device.</li> <li>ASN—Enter the AS number of the peer device.</li> <li>Password—Enter the password for the peer device.</li> <li>Local Address (Group of Fields)— <ul style="list-style-type: none"> <li>Import Policy—(Optional) Select an EBGp import policy from the drop-down list.</li> <li>Export Policy—(Optional) Select an EBGp export policy from the drop-down list.</li> </ul> </li> </ul> <p>For information about creating import and export policies, see <a href="#">Configure SASE BGP Peer Policies</a></p>

7. (For Releases 11.4.1 and later.) For the policy-based tunnel configuration for an IPsec tunnel type, enter information for the following fields.

View

Configure

Deploy

Monitor

Deploy

Monitor

Deploy

Monitor

Analytics

Inventory

Configure > SASE > Settings > Site-to-Site Tunnels

Add Site-to-Site Tunnel

Publish

✓ ENTER TYPE

✓ ENTER IPSEC INFORMATION

3 ENTER ADDRESS & ROUTING / POLICY CONFIGURATIONS

4 ENTER NAME, DESCRIPTION & TAGS

Setup the Versa SASE Gateway routing towards the enterprise VPN.

VPN Name

Audit-Tenant-Enterprise

Policy Configurations

Protocol	Source IP Address/Prefix	Source Port	Destination IP Address/Prefix	Destination Port
ANY	Enter IP Address		Enter IP Address	

If there are multiple matches for the above policies, indicate this tunnel's precedence level. A number closer to 0 (zero) indicates a higher priority.

Precedence

0

Cancel

Next

Field	Description
VPN Name	Select the VPN through which the IP address is reachable.
Policy Configurations (Group of Fields)	
<ul style="list-style-type: none"> <li>Protocol</li> </ul>	Select a protocol: <ul style="list-style-type: none"> <li>Any</li> <li>ICMP</li> <li>TCP</li> <li>UDP</li> </ul>
<ul style="list-style-type: none"> <li>Source IP Address/Prefix</li> </ul>	Enter the IPv4 source prefix.



Field	Description
◦ Source Port	Enter the source port number. <i>Range: 0 through 65535</i>
◦ Destination IP Address/Prefix	Enter the IPv4 destination prefix.
◦ Destination Port	Enter the destination port number. <i>Range: 0 through 65535</i>
◦ Precedence	If there are multiple matches for the policies, indicate the precedence level of the tunnel. A number closer to 0 indicates a higher priority. <i>Range: 0 through 512</i>

8. Click Next.
9. In the Enter Name, Description, and Tags section, enter information for the following fields.

Configure > SASE > Settings > Site-to-Site Tunnels

**Add Site-to-Site Tunnel** Publish

- ✓ ENTER TYPE +
- ✓ ENTER IPSEC INFORMATION +
- ✓ ENTER ADDRESS & ROUTING / POLICY CONFIGURATIONS +
- 4 ENTER NAME, DESCRIPTION & TAGS -

Name \*

Description

Tags

Field	Description
Name (Required)	Enter a name for the tunnel.

Field	Description
Description	Enter a description for the tunnel.
Tags	Enter one or more tags for the tunnel.

10. Click Save.

---

## Supported Software Information

Releases 11.1.1 and later support all content described in this article, except:

- Release 11.4.1 adds support for policy-based IPsec site-to-site tunnels.

---

## Additional Information

[Configure SASE BGP Peer Policies](#)

[Configure SASE Secure Client Access Rules](#)

[Configure Users and Device Authentication](#)