Cisco Secure Access SD-WAN Integration with Arista VeloCloud

About Secure Access SD-WAN integration with Arista VeloCloud SD-WAN

Integrating VeloCloud SD-WAN with Secure Access lets you leverage a powerful cloud-native security fabric. By establishing a remote network tunnel, you redirect branch traffic through Cisco's global security infrastructure, enabling advanced protection for all internet-bound activities, SaaS platforms, and public-facing partner apps.

You can harden your VeloCloud environment using two flexible deployment models:

- VeloCloud edge devices—These user-friendly, plug-and-play units secure remote sites by funneling traffic directly into the Secure Access cloud.
- VeloCloud gateways—Serving as a central SD-WAN headend, the gateway aggregates traffic from multiple locations to streamline security enforcement.

Whether you are connecting a single branch to one gateway or orchestrating a complex mesh of multiple sites and gateways, Secure Access provides consistent, high-performance security across your entire SD-WAN fabric.

Prerequisites

Full Admin account in Secure Access.

Configure a Secure Access network tunnel group

Configure Secure Access to connect to the EdgeConnect device.

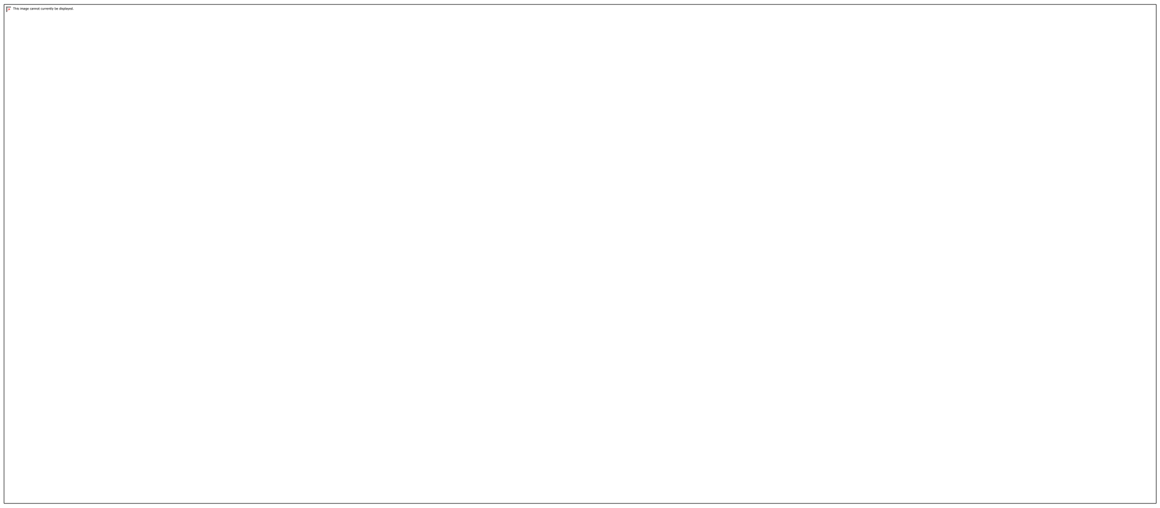
Procedure

Step 1. Navigate to your Secure Access organization:

https://dashboard.sse.cisco.com

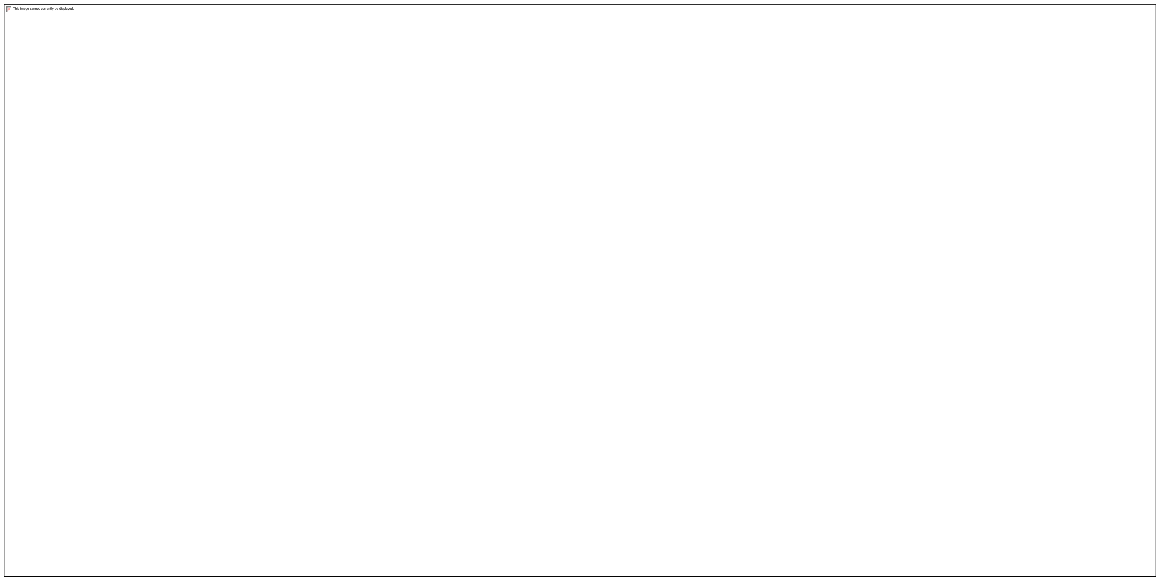
Step 2. Choose **Connect > Network Connections**.

Step 3. Click **Network Tunnel Groups** and click **Add**.



This image cannot currently be displayed.

Step 4. On the **General Settings** page, enter the following values.



This image cannot currently be displayed.

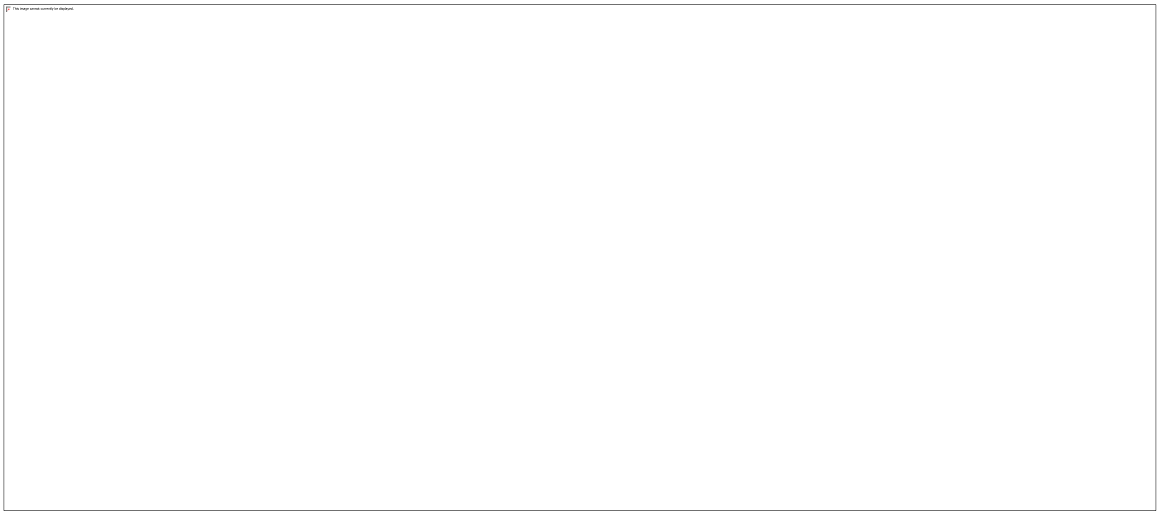
Tunnel Group Name–Enter a meaningful name for the tunnel group.

Region–Select the one closest to your SD-WAN infrastructure.

Device Type–**Other**.

Step 5. Click **Next**.

Step 6. On the **Tunnel ID and Passphrase** page, enter the following values.



Tunnel ID Format–Click **Email** or **IP Address**.

For an email, enter the tunnel name you assigned to the tunnel group. Secure Access will format it as *tunnel_id@org-hub*-sse.cisco.com.

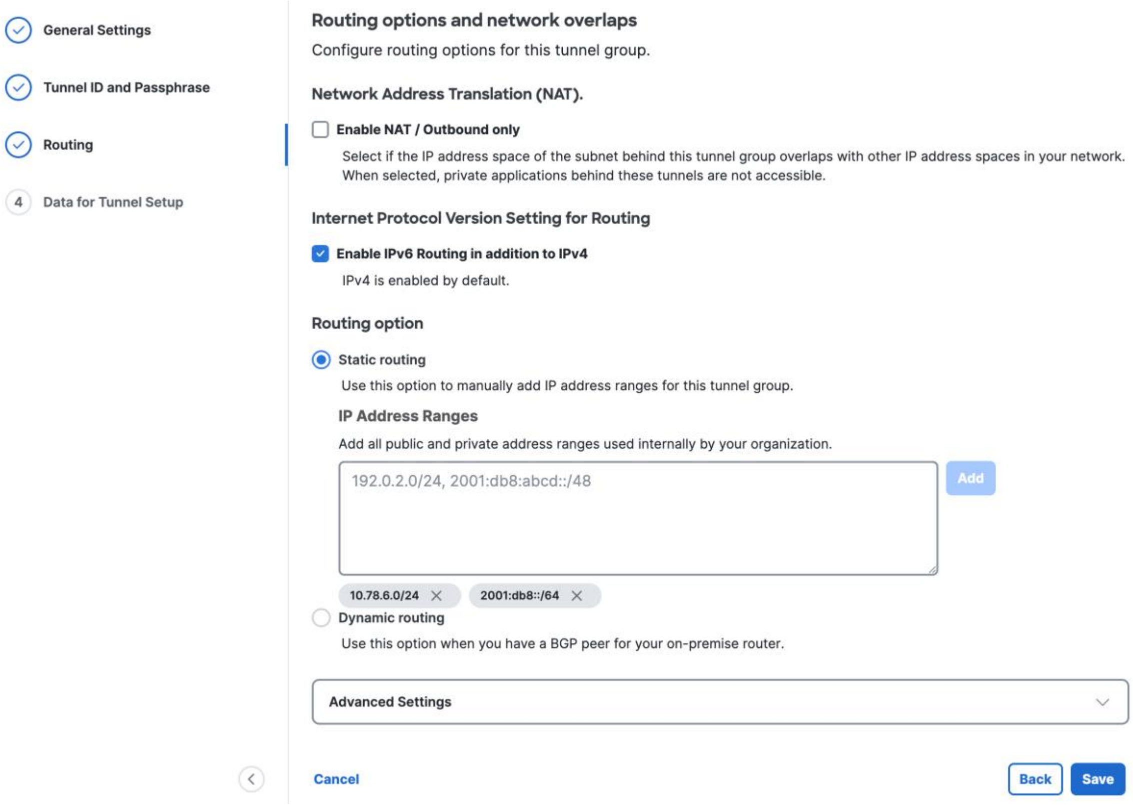
For an IP address, tunnel IDs require both a primary and a secondary IP address. You can specify either IPv4 or IPv6.

Passphrase–Enter a passphrase between 16 and 64 characters in length. The passphrase must contain at least one upper-case letter and one number. The passphrase can’t include any special characters.

Confirm Passphrase–Re-enter your passphrase to confirm.

Step 7. Click **Next**.

Step 8. On the **Routing** page, set the following values.



✓ General Settings

✓ Tunnel ID and Passphrase

✓ Routing

4 Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

Network Address Translation (NAT).

□ **Enable NAT / Outbound only**

Select if the IP address space of the subnet behind this tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels are not accessible.

Internet Protocol Version Setting for Routing

☑ **Enable IPv6 Routing in addition to IPv4**

IPv4 is enabled by default.

Routing option

● Static routing

Use this option to manually add IP address ranges for this tunnel group.

IP Address Ranges

Add all public and private address ranges used internally by your organization.

192.0.2.0/24, 2001:db8:abcd::/48

10.78.6.0/24 ✕ 2001:db8::/64 ✕

○ Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

(Optional) **Network Address Translation (NAT)**–To use NAT, check **Enable NAT / Outbound only**. If you check this option, the routing settings are disabled.

(Optional) **Internet Protocol Version Setting for Routing**–Check **Enable IPv6 Routing in addition to IPv4**.

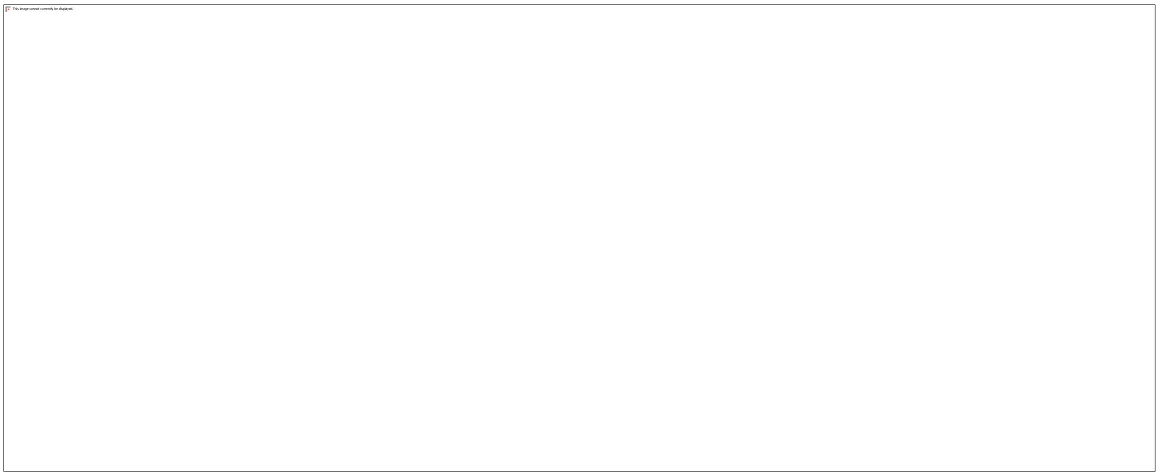
Click a **Routing** option for this tunnel group:

Static routing–Manually add IP Address subnets (IPv4 and IPv6) for this tunnel group separated by commas and then click **Add**. You can click **Add** multiple times until you add all the subnets you need. Add all public and private address ranges used internally by your organization.

Dynamic routing–Use this option for BGP. Enter the SD-WAN **Device AS Number**. If you enabled IPv6 routing, check one or both **Enable IPv4** and **Enable IPv6**. Under **Advanced Settings**, you can enable other options.

Step 9. Click **Save**.

Step 10. On the **Data for Tunnel Setup** page, review the information and click **Done**.



This page shows the primary and secondary tunnel IDs and data center IP addresses that you should use when you set up the tunnels on your branch devices. You can view these later by choosing **Connect > Network Connections**, clicking **Network Tunnel Groups**, and then choosing **View Details** for your network tunnel group. You can't view the passphrase later, so be sure to note the passphrase in a safe place.

Configure VeloCloud gateway devices

Configure the IPSec tunnel on the VeloCloud gateway to enable the redundant connections to Secure Access.

Procedure

Step 1. Log into Arista Edge Cloud Orchestrator.

Step 2. In the **SD-WAN** service of the Enterprise portal, choose **Configure > Network Services**.

Step 3. Under **Non SD-WAN Destinations**, expand **Non SD-WAN Destinations via Gateway**.

Step 4. Click **New**.

Step 5. Configure the following values.

Table 1. Non SD-WAN Destinations via Gateway values

Field	Value
Name	Enter a name for the SD-WAN tunnel.
Type	**Generic IKEv2 Router (Route Based VPN)**
Tunnel Mode	**Active/Hot-Standby**
ECMP Load Sharing Method	**Flow Load Based**

Field	Value
VPN Gateway 1 (Primary)	Specify the Secure Access primary data center IP address. You can view this tunnel information in Secure Access. Choose **Connect > Network Connections**, click **Network Tunnel Groups**, and then choose **View Details** for your network tunnel group.
VPN Gateway 2 (Secondary)	Specify the Secure Access secondary data center IP address. You can view this tunnel information in Secure Access. Choose **Connect > Network Connections**, click **Network Tunnel Groups**, and then choose **View Details** for your network tunnel group.

Step 6. Click **Create.**

Step 7. Configure the following additional values.

Table 2. Generic IKEv2 Router (Route Based VPN) values

Field	Value
Enable Tunnel(s)	Toggle on.
Public IP	Shows the Secure Access primary data center IP address.
PSK	Enter the passphrase you set when you added the network tunnel group in Secure Access.
Encryption	**AES-256**
DH Group	**14**
PFS	Accept the default value.
Authentication Algorithm	**SHA1**
IKE SA Lifetime(min)	Accept the default value.
IPsec SA Lifetime(min)	Accept the default value.
DPD Type	Accept the default value.
DPD Timeout(sec)	Accept the default value.
Redundant Cloud VPN	Leave unselected.
Secondary VPN Gateway	Leave as-is.
Local Auth Id	Accept the default value.
Sample IKE / IPsec	Select to view the information needed to configure the Non SD-WAN Destination Gateway.
Location	Click **Edit** to set the Secure Access location. The latitude and longitude are used to determine the best Edge or Gateway to connect to in the network.
Site Subnets	Use the toggle button to activate or deactivate the **Site Subnets**. Select **Add** to add subnets for Secure Access.

Step 8. Click **Save Changes**.

Step 9. Verify the status of the connection by choosing **Monitor > Network Services.**

A Status in green indicates that the connection has been successfully established

Step 10. Configure the customer profile establish the VPN connection to Secure Access.

1. Choose **Configure > Profiles** and select a profile.
2. On the **Device** tab under **VPN Services**, toggle **Cloud VPN** to **On.**
3. Under **Edge to Non SD-WAN Sites**, check **Enable Edge to Non SD-WAN via Gateway.**
4. Select the Secure Access site you created from the drop-down list.
5. Click **Save Changes**.

Configure VeloCloud edge devices

Configure the IPSec tunnel on the VeloCloud edge to enable the redundant connections to Secure Access.

Procedure

Step 1. Log into Arista Edge Cloud Orchestrator.

Step 2. In the **SD-WAN** service of the Enterprise portal, choose **Configure > Network Services**.

Step 3. Under **Non SD-WAN Destinations**, expand **Non SD-WAN Destinations via Edge**.

Step 4. Click **New.**

Step 5. Configure the following **General** tab values.

Table 3. Non SD-WAN Destinations via Edge General values

Field	Value
Service Name	Enter a name for the SD-WAN tunnel.
Service Type	**Generic IKEv2 Router (Route Based VPN)**
Tunnel Mode	**Active/Hot-Standby**

Step 6. Click the **IKE/IPSec Settings** tab and set the following values.

Table 4. Non SD-WAN Destinations via Edge IKE/IPSec Settings values

Field	Value
IP Version	Choose **IPv4** or **IPv6**.
Primary VPN Gateway Public IP	Specify the Secure Access primary data center IP address. You can view this tunnel information in Secure Access. Choose **Connect > Network Connections**, click **Network Tunnel Groups**, and then choose **View Details** for your network tunnel group.

Step 7. Expand **View advanced settings for IKE Proposal** and set the following values.

Table 5. Advanced Settings for IKE Proposal values

Field	Value
Encryption	**AES-256**
DH Group	**14**
Hash	**SHA 1**
IKE SA Lifetime(min)	Accept the default value.
DPD Timeout(sec)	Accept the default value.

Step 8. Click **View advanced settings for IPsec Proposal** and set the following values.

Table 6. Advanced Settings for IPSec Proposal values

Field	Value
Encryption	**AES-256**
PFS	Accept the default value.
Hash	**SHA 1**
IPsec SA Lifetime(min)	Accept the default value.

Step 9. **Add** a **Secondary VPN Gateway** and set the **Public IP** to the Secure Access secondary data center IP address.

You can view this tunnel information in Secure Access. Choose **Connect > Network Connections**, click **Network Tunnel Groups**, and then choose **View Details** for your network tunnel group.

Step 10. Click the **Site Subnets** tab and click **Add** to add subnets for Secure Access.

Step 11. Click **Save**.

Step 12. Configure the customer profile establish the VPN connection to Secure Access.

6. Choose **Configure > Profiles** and select a profile.
7. On the **Device** tab under **VPN Services**, toggle **Cloud VPN** to **On**.
8. Under **Non SD-WAN Destination via Edge**, check **Enable Non SD-WAN via Edge.**
9. Select the Secure Access site you created from the drop-down list.
10. Click **Save Changes**.

Legal information

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.