Revised: October 3, 2024

Configure Secure Access for SD-Routing Devices

What is Cisco Secure Access

Cisco Secure Access is a cloud Security Service Edge (SSE) solution that is a convergence of network security services delivered from the cloud to connect a hybrid workforce. This solution provides seamless, transparent, and secure Direct Internet Access (DIA) to users helping them connect from anything to anywhere.

In Cisco IOS XE 17.14.1a, Cisco SSE provides the capability for SD-Routing devices to connect with SSE providers using IPSec tunnels.

Feature	Release Information	Description
Configure Cisco Secure Access	Cisco IOS XE Release 17.14.1a	Cisco Secure Access is a cloud Security Serv Edge (SSE) solution that provides seamless transparent, and secure Direct Internet Acce (DIA). This solution can be configured using policy groups in Cisco SD-WAN Manager.

Restrictions

- Cisco Secure Access does not support API Throttling
- After integrating CiscoSecure Access with Cisco SD-Routing, any changes made to the network tunnel group name in Cisco Secure Access dashboard is not reflected in Cisco SD-WAN Manager

Workflow to Set Up Cisco Secure Access

This workflow outlines the high-level steps required to set up Cisco Secure Access. The detailed instructions are covered in the following sections.

Task	Description
Preliminary configurations on Cisco Secure Access Portal	
Check credentials on the portal and ensure that the API credentials have write access.	Go to **Admin** > **Management** > **API Keys** and generate and manage API keys. Ensure that you have write access to Tunnel Group and tunnel creation. Having this ensures seamless connection between Cisco Secure Access and the SD-Routing device, after tunnels have been set up and deployed using the SD-WAN Manager.
Preliminary configurations on Cisco SD-WAN Manager	
Ensure that you have created a Configuration Group and assigned it to the SD-Routing device.	Go to Configuration Groups

Task	Description
Configure the following using the CLI template available on the SD -WAN Manager.	Go to Configuration Groups select any SD-Routing config group, click Edit and select the corresponding CLI Profile dialog box. In the **Add Feature Profile** window, select **Create New** and enter a name and description followed by the command in the **CLI Configuration** section. Save it to add this feature parcel.
• Ensure DNS configuration for the sd-routing device.	By doing this you are allowing the device to interact with DNS servers. You can configure any DNS server on the device which connects to HTTPS to get the public IP address. To configure a source interface for HTTPS, use the **ip http client source-interface** *name and number of the interface* command on Cisco SD-WAN Manager.

• Ensure NAT is enabled on WAN and LAN interface (outside/inside)	By doing this you are ensuring that multiple private addresses inside a local network get mapped to a public IP address before transferring the information onto the internet. For example, all source addresses of the packets that match *access-list nat acl1* will be converted to *Loopback 1* IP address when exiting the router.
	`ip nat inside source list wan-acl1 interface GigabitEthernet2 overload`
	OR
	`ip nat inside source list nat_acl1 interface Loopback1 overload`

Enable domain look up for the device	Go to **Configuration Groups** > **System Profile** > **Global** and enable **Global Lookup**
SSE related configurations on Cisco SD-WAN Manager	
Set up Cloud Provider credentials	Go to **Administration** > **Settings** > **Cloud Provider Credentials** > **Cisco SSE**
Configure source interface address	Go to **Configuration** > **Configuration Groups**
Create SSE Policy using Policy Groups	Go to **Configuration** > **Policy Groups** > **Secure Internet Gateway/Secure Service Edge**
Configure Traffic Redirection	By configuring this, you are creating a service route to redirect traffic through the SSE tunnels Go to **Configuration Groups** select any SD-Routing config group, click Edit and select the corresponding CLI Profile dialog box. In the **Add Feature Profile** window, select **Create New** and enter a name and description followed by the command in the **CLI Configuration** section. Save it to add this feature parcel.

Task	Description
Associate the SSE Policy with Policy Group	Go to **Configuration** > **Policy Groups** > **Add Policy Group** , select the SSE policy created earlier and click **Save** to associate the SSE Policy with the Policy Group. Next associate this policy group with the device and deploy.
Verify the SSE Configuration	Verify the configuration.
Monitor the SSE Tunnels	**Monitor** > **Audit Logs** **Monitor** > **Security** for SSE Tunnels **Monitor** > **Tunnels** > **SSE Tunnels**

Set up Cloud Provider Credentials

Configure credentials to enable Cisco SD-WAN Manager for automated tunnel provisioning to Cisco SSE.

Step 1 Click **Administration** > **Settings** > **Cloud Credentials** > **Cloud Provider Credentials** enable **Cisco Secure Access** and enter the following details. These credentials are used to initiate authentication for a session and are later used in subsequent sessions.

Field	Description
Organization ID	Cisco Secure Access organization ID for your organization.
API Key	Cisco Secure Access API Key.
Secret	Cisco Secure Access API Secret.

Step 2 Save these details.

Configure Loopback Interface as the Source Interface

Configure a loopback interface as source. As this loopback interface is not tied to any interface, there is no risk of interruptions in connections.

Add the following command to the CLI template:

```
interface loopback1
no shutdown
ip nat inside
ip address 1.1.1.1 255.255.255.255
```

Create an SSE Policy Using Policy Group

Before you begin

Ensure that you have created the SSE credentials.You can do this on the SD-WAN Manager by going to **Administration** > **Settings** > **Cloud Provider Credentials** > **Cisco SSE** and enter the details.

Step 1 On the SD-WAN Manager go to **Configuration** > **Policy Groups** > **Secure Internet Gateway/Secure Service Edge**. Click on **Add Secure Service Edge (SSE)**.

Step 2 Enter a name for the SSE policy and specify the solution type as **sd-routing** and click **Create**.

Step 3 Create a tracker. While creating automatic tunnels, Cisco SD-WAN Manager creates and attaches a default tracker endpoint with default values for failover parameters. However, you can also create customized trackers with failover parameters that suit your requirements.

a) In the **Source IP Address** field, enter a source IP address without a subnet mask. This is used for sending http probes to tracker endpoint to detect if there is a unexpected network drops or any latency and is used under the vrf id 65330.

b) Click **Add Tracker**. In the **Add Tracker** window, configure the following and click **Add**.

Table 1: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
API URL of Endpoint	Specify the API URL for the Secure Service Edge endpoint of the tunnel. Default: service.sig.umbrella.com
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. The range is 100 to 1000 milliseconds, the default is 300 milliseconds.
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. The range is 20 to 600 seconds, the default is 60 seconds.
Multiplier	Enter the number of times to resend probes before determining that a tunnel is up or down. The range is 1 to 10, the default is 3.

Step 4 Create a Tunnel. Click **Configuration**.

a) Click **Add Tunnel**.

b) In the **Add Tunnel** pop-up window, under **Basic Settings**, configure the following and click **Add** .

Table 2: Basic Settings

Field	Description
Tunnel Type	Cisco Secure Access: (Read only) **ipsec**
Interface Name (1..255)	Name of the interface.

Field	Description
Description	Enter a description for the interface.
Tracker	By default, a tracker is attached to monitor the health of tunnels.
Tunnel Source Interface	Name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface. The tunnel source interface supports loopback. Depending on your intent you can configure up to 16 tunnels (8 Active/8 Backup).
Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.
Advanced Options (Optional)	
Shutdown	Click the radio button to enable this option. Default: Disabled
Enable Tracker	Click the radio button to enable this option.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 to 2000 bytes Default: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
DPD Interval	Specify the interval for Internet Key Exchange (IKE) to send Hello packets on the connection. Range: 10 to 3600 seconds Default: 10
DPD Retries	Specify the number of seconds between Dead Peer Detection (DPD) retry messages if the DPD retry message is missed by the peer. If a peer misses a DPD message, the router changes the state and sends a DPD retry message. The message is sent at a faster retry interval, which is the number of seconds between DPD retries. The default DPD retry message is sent every 2 seconds. The tunnel is marked as down after five DPD retry messages are missed. Range: 2 to 60 seconds Default: 3
IKE	

Field	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 Default: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2.
IPSec	
IPsec Rekey Interval	Specify the interval for refreshing IPsec keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Options: 64, 128, 256, 512, 1024, 2048, or 4096 packets. Default: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM Default: AEM 256 GCM

Field	Description
Perfect Forward Secrecy	Specify the Perfect Forward Secrecy (PFS) settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS

Step 5 Configure High Availability. To designate active and back-up tunnels and distribute traffic among tunnels, click **High Availability** and do the following:

a) Click **Add Interface Pair**. In the **Add Interface Pair** pop-up window, configure the following

b) Click Add to save these configurations.

Field	Description
Active Interface	Choose a tunnel that connects to the primary data center.
Active Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights to both the tunnels, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup Interface	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.
Backup Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

Step 6 Select the **Region**: When you choose the region, a pair of primary and secondary region is selected. Choose the primary region that Cisco Secure Service Edge provides from the drop-down list and the secondary region is auto-selected in Cisco SD-WAN Manager. If the primary region with a unicast IP address is not reachable then the secondary region with

a unicast IP address is reachable and vice versa. Cisco Secure Access ensures that both the regions are reachable at all times.

What's next

Create Route-Based Traffic Forwarding

After the tunnels are established, relevant traffic should be forwarded to the tunnels. In Cisco IOS XE 17.14.1a, configure traffic forwarding by using the CLI template to add the following command:

ip sdwan route vrf <*network*> <*subnetmask*> **service sse Cisco-Secure-Access**

Example: **ip sdwan route vrf 2 0.0.0.0/0 service sse Cisco-Secure-Access**

Associate the SSE Policy with a Policy Group and Deploy the Policy Group to a Device

The SSE policy created earlier needs to be associated with a Policy Group and later associated with a device for the policy to work on that device.

Step 1 On the SD-WAN Manager go to **Configuration** > **Policy Groups** > **Add Policy Group** to create a new policy group for sd-routing devices.

Step 2 Select the **Action** button and under **Policy** select the **SSE Policy** created earlier from the available policies.

Step 3 Click **Save** to create an association between the SSE Policy and the Policy Group. This association ensures that the SSE policy is now part of the Policy Group.

Step 4 Associate the Policy Group to the device. This association ensures that when you deploy this Policy group to a device, the device inherits all the policies associated with this Policy Group.

Step 5 Deploy the Policy Group to the device. Your device is now ready to use the SSE tunnels.

What's next

Verify Cisco Secure Access Tunnels

To view information about the Cisco Secure Access tunnels that you have configured for the SD-Routing device, use the **show sse all** command.

```
Device# show sse all

************************************
   SSE  Instance Cisco-Secure-Access
************************************
Tunnel name : Tunnel15000001
Site id: 2678135102
Tunnel id: 617865691
SSE tunnel name: C8K-63a9b72b-f1fa-4973-a323-c36861cf59ee
HA role: Active
Local state: Up
Tracker state: Up
Destination Data Center: 52.42.220.205
```

```
Tunnel type: IPSEC
Provider name: Cisco Secure Access
```

Monitor and Troubleshoot Cisco Secure Access Tunnels from SD-WAN Manager

The following sections show how to identify issues with the SSE tunnels and take corrective measures.

Monitoring SSE Tunnel State Using Cisco SD-WAN Manager

Monitor the state of the SSE tunnels using the following options in Cisco SD-WAN Manager:

- **Monitor** > **Security** > **SIG/SSE Tunnel** dashboard to view information about:
  - Down Tunnels
  - Degraded Tunnels: Degraded state indicates that the SSE tunnel is up but the Layer 7 health of the tunnel as detected by the tracker does not meet the configured SLA parameters. Therefore, the traffic is not routed through the tunnel.
  - Up Tunnels

- **Monitor** > **Tunnels** > **SIG/SSE Tunnel** to view information about :

  Data plane tunnels, tunnel end points, and health of the tunnel

Cisco SD-WAN Manager displays a table that provides the following details about each automatic tunnel created to Cisco Secure Access:

Field	**Description**
Host Name	Host name of the SD-Routing device.
Site ID	ID of the site where the WAN edge device is deployed.
Tunnel ID	Unique ID for the tunnel defined by the SIG/SSE provider.
Transport Type	IPSec
Tunnel Name	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SSE provider portal, you can use the tunnel name to find details about a particular tunnel.
HA Pair	Active or Backup
Provider	Cisco Secure Access
Destination Data Center	SIG/SSE provider data center to which the tunnel is connected.
Tunnel Status (Local)	Tunnel status as perceived by the device.
Tunnel Status (Remote)	Tunnel status as perceived by the SIG/SSE endpoint.

Field	Description
Events	Number of events related to the tunnel set up, interface state change, and tracker notifications. Click on the number to display an Events slide-in pane. The slide-in pane lists all the relevant events for the particular tunnel.
Tracker	Enabled or disabled during tunnel configuration.

Monitoring and Troubleshooting Using Commands

This section provides details on how to identify and troubleshoot SSE tunnel issues from device commands.

Troubleshooting Using Device Notifications

Note

Accessing the device shell needs a consent token. Consent Token is a security feature that is used to authenticate the network administrator of an organization to access system shell with mutual consent from the network administrator and Cisco Technical Assistance Centre (Cisco TAC).

To view information about a device on which an event was generated use the following steps:

1. Execute the **/opt/confd/bin/confd_cli -C -P 3010 -noaaa -g sdwan-oper** command. This command gives you access to the shell to run commands to view device notifications.
2. Execute **show notification stream viptela** command to view the device notifications

   Device**#show notification stream viptela**

```
notification
 eventTime 2023-11-09T06:21:19.95062+00:00
 sse-tunnel-params-absent
  severity major
  host-name vm6
  if-name TunnelSSE
  wan-if-ip 192.1.2.8
```

Troubleshooting Using Crypto Session Details

Execute **show crypto session** command to view the crypto session details

Device**#show crypto session**

```
Interface: Tunnel15000010
Profile: if-ipsec10-ikev2-profile
Session status: UP-ACTIVE
Peer: 3.76.88.203 port 4500
  Session ID: 7
  IKEv2 SA: local 10.1.15.15/4500 remote 3.76.88.203/4500 Active
  IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Troubleshooting Using Interface Details

Execute the **show interface brief** command. This command displays the interface details.

Device**#show interface brief**

```
Tunnel15000010         10.1.15.15      YES TFTP   up    up
```

Troubleshooting Using Endpoint Tracker Details

Execute the **show endpoint tracker** command. This command displays all the endpoint tracker details.

Device**#show endpoint-tracker**

```
Interface                      Record Name            Status        Address Family   RTT in msecs    Probe
ID   Next Hop
Tunnel16000002                 DefaultTracker         Up            IPv4             22              20
     None
```

Troubleshooting Using Tunnel Details

Execute the **show running config|sec sse** command. This command displays the tunnel and vrf details.

Device**#show running config|sec sse**

```
sse instance Cisco-Secure-Access
  ha-pairs
   interface-pair Tunnel15000010 active-interface-weight 1 None backup-interface-weight 1
!
ip sdwan route vrf 2 0.0.0.0/0 service sse Cisco-Secure-Access
```