Configure Cisco Catalyst SD-WAN Remote Access

- Configure Cisco Catalyst SD-WAN Remote Access Using a Configuration Group, on page 1
- Configure SD-WAN RA, on page 4
- Configure Cisco Catalyst SD-WAN Remote Access Using Cisco SD-WAN Manager, on page 18
- Configure Cisco Catalyst SD-WAN Remote Access Using a Configuration Group, on page 18
- Add the SD-WAN Remote Access Feature Profile to an Existing Configuration Group, on page 22

Configure Cisco Catalyst SD-WAN Remote Access Using a Configuration Group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Remote Access feature in a System Profile.

a. Configure Remote Access.

Table 1: Remote Access Settings

Field	Description
Type	Choose Remote Access feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.

Field	Description
Connection Type	Choose the connection type from the following: • **IPsec** • **SSL-VPN** By default, IPsec is selected. We recommend using IPsec mode. SSL-VPN mode is supported only on Cisco Catalyst 8000v Edge Software with limited features.

b. Configure Authentication.

Table 2: Authentication

Field	Description
Radius Group Name	Choose an existing RADIUS group or create a new RADIUS group. Click **Add Radius Group** to add a RADIUS server and group to the AAA feature profile in the System Profile.
Pre-Shared Key (PSK) Authentication	Enable Pre-Shared Key (PSK) authentication. • **AAA-based-PSK**: Choose this option to fetch the pre-shared keys from the RADIUS server. This option allows configuring a pre-shared key on the RADIUS server that is unique per remote access client or a group of remote access clients. • **Groups PSK**: Choose this option to configure a common pre-shared key for all remote access clients connecting to a device. **Note** **Pre-Shared Key (PSK) Authentication** is applicable only for connection-type IPsec and not for SSL-VPN.
CA Server Setup	Choose a CA server for certificate-based authentication. The certificate from the selected CA is used by the device to authenticate the remote access clients. Before choosing a CA server, configure the CA server from **Configuration** > **Certificate Authority**.
User Authentication	Choose the user authentication option for AnyConnect Extensible Authentication Protocol (EAP) authentication used by remote access client. **Note** The **User Authentication** setting is applicable only for the IPsec connection type and not for SSL-VPN.
User & Device Authentication	Choose the user and device authentication option for AnyConnect EAP authentication used by remote access client. The **User & Device Authentication** setting is applicable only for the IPsec connection type and not for SSL-VPN.

Field	Description
Enable Profile Download	Enable download of an AnyConnect profile XML file to Cisco AnyConnect clients from the remote access headend devices. In the **Upload Profile XML File** pane, choose an XML file or drag and drop to upload. The maximum file size is 20 KB.

c. Configure AAA Policy.

Table 3: AAA Policy

Field	Description
Specify Name	Choose this option to specify the name of the policy to look up on the RADIUS server. In the **Policy Name** field, which appears only for the **Specify Name** option, enter the name of the policy.
Derive Name from Peer Identity	Choose this option to use the identity of the peer as the name of the policy to lookup on the RADIUS server. **Note** This setting is applicable only for the IPsec connection type and not for SSL-VPN.
Derive Name from Peer Identity Domain	Choose this option to use the domain portion of the identity of the peer as the name of the policy to look up on the RADIUS server. **Note** This setting is applicable only for the IPsec connection type and not for SSL-VPN.
Policy Password	Enter the policy password.
Enable Accounting	Enable accounting.

d. Configure Private IP-Pool.

Table 4: Private IP-Pool

Field	Description
Maximum Number of Clients	Enter the maximum number of remote access clients that can connect to a remote access headend device. This number determines the size of the IPv4 pool allocated to the device. If a global IPv6 pool is defined for remote access in the network hierarchy, each SD-WAN RA headend device will be allocated an IPv6 pool sufficient for the maximum number of remote access clients (8000).

e. Configure IKEv2 and IPsec settings.

Table 5: IKEv2 and IPsec Settings

Field	Description
Local IKE Identity Type	Enter the local IKEv2 identity type. The options are: • IPv4 Address or IPv6 Address • Email • FQDN • Key-ID
Local IKE Identity Value*	Enter the value of the local IKEv2 identity based on the identity type selected.
Security Association (SA) Lifetime	Enter the lifetime in seconds for the IKEv2 security association. The range is from 3600 to 86400. The default lifetime is 86400 seconds.
Enable Anti - Denial of Service (DOS) Check	Enable an Anti-Denial of Service (DOS) check.
Anti-DOS Threshold	Enter the Anti-DOS threshold value. Range: 10 to 1000. Default: 100.

What to do next

Also see Deploy a configuration group.

Configure SD-WAN RA

To configure SD-WAN RA headend functionality on a Cisco IOS XE Catalyst SD-WAN device, complete the following tasks.

Important The configuration steps described here are presented as high-level tasks. For details about using Cisco SD-WAN Manager feature templates and CLI add-on templates, see the Cisco Catalyst SD-WAN documentation. For information about configuring Cisco AnyConnect or a RADIUS server, see the documentation for those products.

Note We recommend using a RADIUS server for per-user credentials, and for per-user and group policy. We do not recommend configuring credentials and policy locally, as this method does not scale.

Configuration Tasks

	Task
Task 1	Configure IKEv2 ciphers and parameters
Task 2	Configure a PKI trustpoint for certificate authentication
Task 3	Configure IKEv2 profiles to group remote access clients based on identity, and specify authentication and authorization policy
Task 4	Configure IPsec ciphers, parameters, and virtual-template interface
Task 5	(Optional) Configure Cisco AnyConnect profile download
Task 6	Configure private IP pool to assign IP address to remote access clients, if applicable
Task 7	Configure AAA to specify a RADIUS server for remote access user authentication, policy, and accounting
Task 8	Configure remote access user credentials and policy on the RADIUS server
Task 9	(Optional) Configure remote access traffic rate limiting
Task 10	Configure remote access traffic symmetry, if applicable
Task 11	(Optional) Configure SD-WAN features for remote access traffic

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure task 1 to task 8 using Cisco SD-WAN Manager configuration groups.

References

For detailed information about IKEv2, IPsec, and PKI configuration, see the documentation for these technologies. We recommend the following:

- FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS XE 17
- Security for VPNs with IPsec Configuration Guide, Cisco IOS XE 17
- Public Key Infrastructure Configuration Guide, Cisco IOS XE 17

Task 1: Configure IKEv2 Ciphers and Parameters

Note When configuring a device to function as an SD-WAN RA headend, we recommend using a single CLI add-on template for all of the required configuration commands. The tasks are described separately, but you can combine the configuration commands into one template. Use the configuration commands in config-transaction mode.

In Cisco SD-WAN Manager, use a CLI add-on template for the SD-WAN RA headend device to configure the following:

1. Configure an IKEv2 proposal.

   crypto ikev2 proposal *ikev2-proposal-name*
   encryption *encryption-algorithms*
   integrity *integrity-algorithms*
   group *DH-group-numbers*
   prf *prf-algorithms*

   Example:

   ```
   crypto ikev2 proposal sdra_ikev2_proposal
   encryption aes-cbc-256
   integrity sha256
   group 19
   prf sha384
   ```

2. Configure an IKEv2 policy.

   crypto *ikev2 policy ikev2-policy-name*
   proposal *ikev2-proposal-name*

   Example:

   ```
   crypto ikev2 policy sdra_ikev2_policy
   proposal sdra_ikev2_proposal
   ```

3. Configure IKEv2 parameters.

   crypto ikev2 cookie-challenge *threshold-half-open-connections*
   crypto ikev2 fragmentation mtu *ikev2-mtu*

   Example:

   ```
   crypto ikev2 cookie-challenge 100
   crypto ikev2 fragmentation mtu 1400
   ```

Task 2: Configure a PKI Trustpoint for Certificate Enrollment

Perform this task if the remote access headend is configured to use certificate authentication.

In Cisco SD-WAN Manager, use a CLI add-on template for the SD-WAN RA headend device to configure a PKI trustpoint that specifies a CA server for SCEP-based auto enrollment.

crypto pki trustpoint *sdra_trustpoint*
auto-enroll *renewal_percentage*
enrollment url http://*ca-ip-address***:80**
fingerprint *ca_certificate_fingerprint*
subject-name cn= *subj-name-string*
revocation-check none
auto-trigger
vrf *ca-vrf*

Example:

```
crypto pki trustpoint sdra_trustpoint
auto-enroll 80
enrollment url http://10.1.1.11
fingerprint 0123456789ABCDEF0123456789ABCDEF
```

```
subject-name cn=sdra_headend_1
revocation-check none
auto-trigger
vrf 1
```

Task 3: Configure an IKEv2 Profile

The IKEv2 profile enables grouping of peers by identity, and specifies authentication and authorization policy.

Configure an IKEv2 Profile

In Cisco SD-WAN Manager, use a CLI add-on template for the SD-WAN RA headend device to configure the following:

1. Configure an IKEv2 profile.
   a. Specify a name for the profile.

      crypto ikev2 profile *sdra_ikev2_profile*

   b. Match peer identities and specify a local identity.

      match identity remote {**any** | *id-type id-value*}
      identity local *id-type id-value*

   c. Specify authentication types and credentials.

      authentication local *auth-type* [**key** *pre-shared-key*]
      authentication remote *auth-type*
      keyring aaa *sdra-author-aaa-mlist* **password** *sdra-radius-password*
      pki trustpoint *sdra_trustpoint*
      aaa authentication eap *sdra_authen_mlist*

   d. Specify user authorization parameters.

      aaa authorization user *peer-auth-type* **cached**

   e. Specify group authorization parameters.

      aaa authorization group *peer-auth-type* **list** *sdra_author_mlist* **name-mangler** *sdra-group-author-name-mangler* **password** *sdra-radius-password*

   f. Enable AAA accounting.

      aaa accounting *peer-auth-type* **list** *sdra_acc_mlist*

   g. Specify an IPsec virtual-template interface.

      virtual-template *interface-number* **mode auto**

   Example:

```
crypto ikev2 profile sdra_ikev2_profile
 match identity remote any
 identity local email sdra_headend1@abc.com
 authentication local rsa-sig
 authentication remote anyconnect-eap aggregate
 pki trustpoint sdra_pki_trustpoint
 aaa authentication anyconnect-eap sdra_authen_mlist
 aaa authorization user anyconnect-eap cached
 aaa authorization group anyconnect-eap list sdra_author_mlist name-mangler
```

```
sdra_group_author_name_mangler password sdra_radius_author_passwd
 aaa accounting anyconnect-eap sdra_acc_mlist
 virtual-template 1 mode auto
```

2. Configure the IKEv2 name mangler to extract the domain portion from the peer identity, using a Cisco SD-WAN Manager CLI template.

   crypto ikev2 name-mangler *sdra_group_author_name*
   fqdn domain
   email domain
   eap suffix delimiter @

   Example:

   ```
   crypto ikev2 name-mangler sdra_group_author_name_mangler
   fqdn domain
   email domain
   eap suffix delimiter @
   ```

Task 4: Configure IPsec Ciphers, Parameters, and Template Interface

Before You Begin

In step 3, the **interface Virtual-Template** command specifies a service VPN VRF. Before beginning this procedure, define the VRF. You can use a Cisco SD-WAN Manager feature template to define the VRF.

Configure IPsec Ciphers, Parameters, and Template Interface

In Cisco SD-WAN Manager, use a CLI add-on template for the SD-WAN RA headend device to configure the following:

1. Configure IPsec ciphers.

   crypto ipsec transform-set *sdwan-ra_transform_se ipsec-cipher*
   mode tunnel

   Example:

   ```
   crypto ipsec transform-set sdwan-ra_ipsec_ts esp-gcm 256
   mode tunnel
   ```

2. Configure IPsec parameters.

   crypto ipsec profile *sdwan-ra_ipsec_profile*
   set transform-set *sdwan-ra_transform_set*
   set security-association lifetime seconds *ipsec_sa_life_sec*
   set security-association replay window-size *window-size*
   set ikev2-profile *sdwan-ra_ikev2_profile*

   Example:

   ```
   crypto ipsec profile sdwan-ra_ipsec-profile
    set security-association lifetime seconds 33600
    set security-association replay window-size 64
    set transform-set sdwan-ra_transform_set
    set ikev2-profile sdwan-ra_ikev2_profile
   ```

3. Configure the IPsec virtual-template interface.

```
interface Loopback 65515
 vrf forwarding sdwan-ra_service_vpn
 ip address private_ipv4_addr subnet_mask

interface Virtual-Template sdwan-ra_vt_intf_num type tunnel
 vrf forwarding sdwan-ra_service_vpn
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile sdwan-ra_ipsec_profile
```

Example:

```
vrf definition sdwan-ra_service_vpn
!
interface interface Loopback 65515
 vrf forwarding sdwan-ra_service_vpn
 ip address 10.0.0.100 255.255.255.0
!
interface Virtual-Template101 type tunnel
 vrf forwarding sdwan-ra_service_vpn
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile sdwan-ra_ipsec-profile
```

Task 5: Configure AnyConnect Profile Download

Before You Begin

Ensure that you have an AnyConnect profile XML file available. Step 3 uses the file. For information about AnyConnect profiles, see the documentation for AnyConnect.

Configure AnyConnect Profile Download

In Cisco SD-WAN Manager, use a CLI add-on template for the SD-WAN RA headend device to configure the following:

1. Disable HTTP secure server functionality.

   ```
   no ip http secure-server
   ```

2. Configure SSL policy and specify the Cisco Catalyst SD-WAN remote access WAN IP as the local address for profile download.

   ```
   crypto ssl policy sdra_anyconnect_profile_download
    pki trustpoint sdra_pki_trustpoint  sign
    ip address local sdra_wan_ip port 443
   ```

3. Copy the AnyConnect profile XML file to the SDremote access headend bootflash and specify the path.

Note You can copy the AnyConnect profile XML file to the Cisco Catalyst SD-WAN remote access headend bootflash from a host reachable in a service VPN, using the **secure copy** command on the Cisco Catalyst SD-WAN remote access headend.

```
crypto vpn anyconnect profile sdra_anyconnect_profile  bootflash:
sdra_anyconnect_profile.xml
```

4. Specify the AnyConnect profile name in the IKEv2 profile.

```
crypto ikev2 profile sdra_ikev2_profile
 anyconnect profile sdra_anyconnect_profile
```

Example:

```
no ip http secure-server
!
crypto ssl policy sdra_anyconnect_profile_download
 pki trustpoint sdra_pki_trustpoint sign
 ip address local 172.16.1.1 port 443
!
crypto vpn anyconnect profile sdra_anyconnect_profile bootflash: sdra_anyconnect_profile.xml
!
crypto ikev2 profile sdra_ikev2_profile
anyconnect profile sdra_anyconnect_profile
```

Task 6: Configure a Unique Local Private IP Pool on the SD-WAN RA Headend

Note This task is optional if all remote access users connect to the headend by hardware remote access client.

Configure each SD-WAN RA headend with a unique private IP pool from which to assign IP addresses to remote access clients. The IP pool can be shared across the service VPNs in which remote access clients connect to the SD-WAN RA headend.

Configure a Unique Local Private IP Pool on the SD-WAN RA Headend

1. In Cisco SD-WAN Manager, use a CLI add-on template for the SD-WAN RA headend device to configure the local IP pool. Ensure that the IP pool range is sufficient for the expected number of remote access connections.

   ```
   ip local pool sdra-ip-pool ip-address-range-start ip-address-address-end
   ```

   Example:

   ```
   ip local pool sdra_ip_pool 10.0.0.1 10.0.0.100
   ```

2. On the RADIUS server, configure the per-user or group policy to specify the IP pool name configured in the previous step.

3. Optionally, for each remote access service VPN, use a Cisco SD-WAN Manager OMP feature template to advertise the remote access IP pool range as a summary-only route.

   If the SD-WAN RA IP pool summary is not advertised, OMP automatically advertises, for each remote access client, static host routes that are dynamically programmed by the SD-WAN RA headend. This may not be optimal if there is a large number of remote access clients across the Cisco Catalyst SD-WAN fabric.

Task 7: Configure AAA Parameters and RADIUS Server Parameters

In Cisco SD-WAN Manager, use a CLI add-on template for the SD-WAN RA headend device to configure the following:

1. Configure RADIUS server parameters.

```
aaa new-model
aaa group server radius sdra_radius_grp
server-private radius-ip key encr_key
ip vrf forwarding radius-vrf
```

2. Configure AAA method lists for authentication, authorization and accounting.

```
aaa authentication login sdra_authen_mlist group sdra_radius_grp
aaa authorization network sdra_author_mlist group sdra_radius_grp
aaa accounting network sdra_acc_mlist group sdra_radius_group
```

Example:

```
aaa new-model
aaa group server radius sdra_radius_group
server-private 10.0.8.100 key sdra-encr-key
ip vrf forwarding 1
!
aaa authentication login sdra_authen_mlist group sdra_radius_grp
aaa authorization network sdra_author_mlist group sdra_radius_grp
aaa accounting network sdra_acc_mlist group sdra_radius_group
```

Task 8: Configure the RADIUS Server with User Credentials and Policy

Before You Begin

This task requires a working knowledge of RADIUS server configuration.

Configure the RADIUS Server with User Credentials and Policy

The SD-WAN RA headend relies on the RADIUS server as the repository of remote access user authentication credentials, and of policy configuration details, such as VRF, security group tag (SGT), IP pool name, and server subnets. Using the RADIUS server for these functions is preferable to trying to manage credential and policy configuration on each remote access headend device, as the RADIUS server centralizes this configuration and provides scalability.

The RADIUS server also functions as an extensible authentication protocol (EAP) server when remote access clients use the EAP authentication method.

To support the SD-WAN RA headend, ensure that the following parameters are configured on the RADIUS server. These parameters are required for enabling remote access connections:

- User authentication credentials
  - Username and password for AnyConnect-EAP connections
  - Pre-shared keys for the pre-shared key authentication method
  - EAP credentials for EAP authentication method
- Policy parameters that apply to a user or to a user group
  - VRF: Service VPN that the remote access user is assigned to
  - IP pool name: Name of the IP pool defined on the remote access headend
  - Server subnets: Subnet access to provide to the remote access user

- SGT: Trustsec SGT tag to assign to the user traffic

For full configuration information, see the RADIUS documentation. For a list of supported attributes, see FlexVPN RADIUS Attributes.

For reference, see the following subset of RADIUS parameters. These parameters are required, to enable SD-WAN RA to establish remote access connections.

Table 6: Subset of the Parameters in a User Profile

Parameter	Description
Profile name	Remote access user identity. Example: user1@example.com
Cleartext-password := "*password*"	Remote access user password specified by the remote access user on the remote access client. This is required for AnyConnect EAP authentication.
Tunnel-Password = *pre-shared-key-string*	Pre-shared-key string to use for the remote access user. This is required for pre-shared key authentication.
cisco-avpair+="ip:interface-config=vrf forwarding *vrf-name*"	VRF (service VPN) that the remote access user is assigned to. Prerequisite: Define the VRF locally on the headend.
cisco-avpair+="ip:interface-config=ip unnumbered *interface-name*"	The IP unnumbered interface for the virtual-template and virtual-access interfaces. • Prerequisite: On the SD-WAN RA headend, configure the interface to use for remote access, and a private IP address, preferably from the IP pool subnet range. • The SD-WAN RA headend re-uses the private IP address described above for virtual-template and per-remote-access-user virtual-access interfaces. **Note** If the VRF attribute is configured in a RADIUS profile, then the **ip numbered interface** attribute must also be configured after the VRF attribute.
Framed-Pool=*pool-name*	Name of the IP pool, defined on the headend, that the remote access headend uses to assign an IP address to the remote access user.

Parameter	Description
cisco-avpair+="ipsec:route-set=prefix *prefix/prefix-length*"	IP prefixes to which the remote access user requires access over the remote access VPN tunnel. You can configure this attribute multiple times to specify multiple prefixes.
cisco-avpair+="ip:interface-config=cts role-based sgt-map sgt *sgt-value*"	The SGT to assign to the traffic from this remote access user that is destined to a Cisco Catalyst SD-WAN tunnel.

Table 7: Subset of the Parameters in a User Group Profile

Parameter	Description
Group profile name	Domain portion of the remote access user identity. The group profile enables grouping of remote access users based on the domain portion of the remote access user identity. Grouping enables you to specify common policy parameters. Specifying example.com would include in the group any user with example.com domain after the @ character. The RADIUS server applies the parameters specified in this group profile to any users included in this group.
Cleartext-password := "*password*"	For an authorization request from remote access headend to the RADIUS server, the password is configured on the remote access headend as part of the authorization command in IKEv2 profile. If the password is not configured, the default password is **cisco**.
cisco-avpair+="ip:interface-config=vrf forwarding *vrf-name*"	VRF (service VPN) that the group of remote access users is assigned to. Prerequisite: Define the VRF locally on the headend.

Parameter	Description
cisco-avpair+="ip:interface-config=ip unnumbered *interface-name*"	The IP unnumbered interface for the virtual-template and virtual-access interfaces. • Prerequisite: On the SD-WAN RA headend, configure the interface to use for remote access, and a private IP address, preferably from the IP pool subnet range. • The SD-WAN RA headend re-uses the private IP address described above for virtual-template and per-remote-access-user virtual-access interfaces. **Note** If the VRF attribute is configured in a RADIUS profile, then the **ip numbered interface** attribute must also be configured after the VRF attribute.
Framed-Pool=*pool-name*	Name of the IP pool, defined on the headend, that the remote access headend uses to assign IP addresses to this group of remote access users.
cisco-avpair+="ipsec:route-set=prefix *prefix*/*prefix-length*"	IP prefixes to which the group of remote access users require access over the remote access VPN tunnel. You can configure this attribute multiple times to specify multiple prefixes.

Task 9: Configure Remote Access Traffic Rate Limiting

You can limit the rate of the aggregate upstream and downstream aggregate remote access traffic by applying quality of service (QoS) policers and shapers.

Configure remote access Traffic Rate Limiting

1. Rate limit remote access upstream traffic (from the remote access client).

Note The upstream traffic may be destined to Cisco Catalyst SD-WAN sites such as the SD-WAN RA headend, a data center LAN, or the internet.

Use one or both of the following options to rate limit to the required rate.

a. For encrypted upstream traffic: Using Cisco SD-WAN Manager, add an inbound QoS policer on the SD-WAN RA WAN interface, using the local data policy (access list), to rate limit encrypted upstream traffic.

   Rate limiting encrypted traffic drops excess remote access traffic, irrespective of the traffic destination, remote access client type, or application type.

Configure the following match conditions and action:

- Match IKEv2 and encrypted IPsec traffic. Include the following:
  - UDP ports 500 and 4500
  - IP protocol ESP
- Action: Configure the required rate for the policing.

b. For decrypted upstream traffic: Using Cisco SD-WAN Manager, add an inbound QoS policer on the SD-WAN RA WAN interface, using the centralized data policy, to rate limit decrypted upstream traffic.

When rate limiting decrypted traffic, you can specify remote access clients and application types.

Note SD-WAN RA places a remote access user in a service VPN based on the user identity. After decryption, the traffic from a remote access user is treated as inbound traffic from the VPN of the remote access user.

Configure the following match conditions and action:

- Match remote access inner (within the IPsec tunnel) traffic. Specify the following:
  - Remote access user service VPN
  - For the source IP, specify the IP address(es) assigned to the remote access client.
  - Application
- Action: Configure the required rate for the policing.

2. Using Cisco SD-WAN Manager, add an inbound QoS policer to the centralized policy to rate limit remote access downstream (toward the remote access client) traffic.

The traffic may originate from sources such as traffic from the site where the SD-WAN RA headend is located, a data center LAN, software-as-a-service (SaaS) applications, or the internet.

Effect: This step rate limits the enterprise and internet (including SaaS) remote access return traffic as close as possible to the traffic source (application server). When rate limiting unencrypted traffic, you can specify remote access clients and application types.

Configure the following match conditions and action:

- Match remote access inner (within the IPsec tunnel) traffic. Specify the following:
  - Remote access user service VPN
  - For the destination IP, specify the IP address(es) assigned to the remote access client.
  - Application
- Action: Configure the required rate for the policing.

  For information, see Cisco SD-WAN Forwarding and QoS Configuration Guide, Cisco IOS XE Release 17.x.

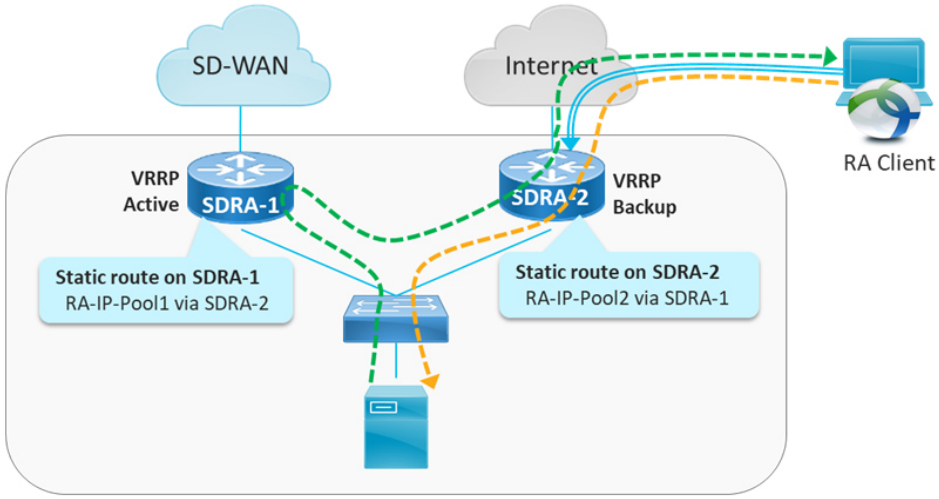
Task 10: Configure Remote Access Traffic Symmetry

At Cisco Catalyst SD-WAN sites with multiple Cisco IOS XE Catalyst SD-WAN devices acting as SD-WAN RA headends, you must ensure remote access traffic symmetry (both directions of a flow using the same path) to enable return traffic to be correctly routed to remote access clients.

A. Configure Remote Access Traffic Symmetry for Sites That Use VRRP

At a site with multiple Cisco IOS XE Catalyst SD-WAN devices functioning as SD-WAN RA headends, and with a LAN that uses the virtual router redundancy protocol (VRRP), use this procedure to ensure remote access traffic symmetry and retrun traffic reachability.

Figure 1: Site With Service-Side VRRP



1. Ensure that each SD-WAN RA headend has a unique local private IP pool (remote access IP pool) for assigning IP addresses to remote access clients. remote access clients use the assigned private IP as the source IP for all inner (within the IPsec tunnel) traffic.
2. On each SD-WAN RA headend, in each of the end user service VPNs, add a static route to the remote access IP pool of each of the neighbor SD-WAN RA headends. For the static route, configure the corresponding SD-WAN RA headend as the next hop.

   The effect of this step is that if there is an asymmetric traffic flow, where return traffic arrives at a different device at the site than forward traffic, the static route forwards the traffic to the correct SD-WAN RA headend device, which is the headend device with the IPsec tunnel and host route to the remote access client.

Example:

In the example shown in the figure, there are two SD-WAN RA headend devices (SDRA-1 and SDRA-2) at the same site. They are interconnected with a service VPN. Each has a unique local IP pool.

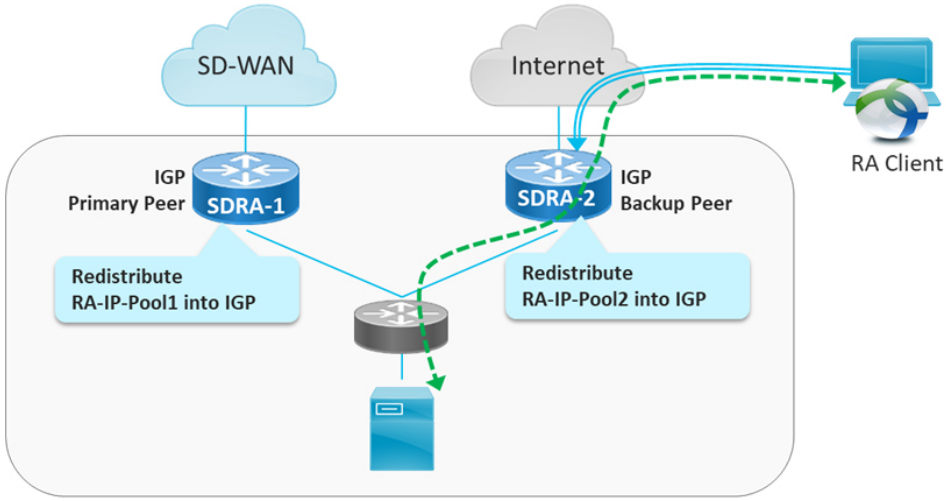
- On SDRA-1, configure a static route as follows:
  - Route destination: SDRA-2 IP pool subnet
  - Route next-hop: SDRA-2 service VPN IP

- On SDRA-2, configure a static route as follows:
  - Route destination: SDRA-1 IP pool subnet
  - Route next-hop: SDRA-1 service VPN IP

B. Configure Remote Access Traffic Symmetry for Sites That Use Routing Protocols

At a site with multiple Cisco IOS XE Catalyst SD-WAN devices functioning as SD-WAN RA headends, and with a LAN that uses routing protocols such as open shortest path first (OSPF) or enhanced interior gateway routing protocol (EIGRP), use this procedure to ensure remote access traffic symmetry and retrun traffic reachability.

Figure 2: Site With Service-Side Routing Protocol



1. Ensure that each SD-WAN RA headend has a unique local private IP pool for assigning IP addresses to remote access clients (remote access IP pool). remote access clients use the assigned private IP as the source IP for all inner (within the IPsec tunnel) traffic.
2. On each SD-WAN RA headend, redistribute the remote access IP pool into the service side routing protocol, so that the LAN-side router/L3 switch forwards any return traffic destined to remote access clients to the correct device, based on the assigned IP address (return traffic destination IP).

Task 11: Configure Cisco Catalyst SD-WAN Features for Remote Access Traffic

When the SD-WAN RA headend establishes a connection with a remote access user, it places the user in a service VPN based on the identity of the remote access user. After the remote access traffic is decrypted, it becomes inbound traffic on the assigned service VPN. The Cisco Catalyst SD-WAN features that are configured for the service VPN apply to the remote access traffic also. These feature include the following:

- NAT-DIA
- UTD
- ZBF

Configure Cisco Catalyst SD-WAN Features for remote access Traffic

Ensure that each service VPN is configured with the Cisco Catalyst SD-WAN features that you want to apply to the remote access traffic that uses that service VPN.

Configure Cisco Catalyst SD-WAN Remote Access Using Cisco SD-WAN Manager

Before You Begin

- Global private IP pool for SD-WAN RA: In the network hierarchy, define a global private IPv4 pool and IPv6 pool for remote access. Ensure that this pool address range is unique in the Cisco Catalyst SD-WAN overlay.

  This global private IP pool for remote access is used to allocate a unique IP pool to each device enabled for remote access. The devices use the allocated pool to assign a unique IP address to each remote access client. The remote access clients use the assigned IP address as the source IP address of the traffic from the client that is sent over an encrypted tunnel to the device.

- Certificate authority: Define the certificate authority for SD-WAN RA. The devices enabled for remote access receive a certificate from this certificate authority. The devices use the certificate to authenticate to remote access clients.

  From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificate Authority** and select **Enterprise CA and Simple Certificate Enrollment Protocol (SCEP)**.

Note The other CA options such as **Enterprise CA without SCEP**, **SD-WAN as CA** and **SD-WAN as intermediate CA** are not supported for the SD-WAN RA feature.

- RADIUS server: Define a RADIUS server in a configuration group using the **AAA** feature profile in the **System Profile**. The devices enabled for remote access use the RADIUS server to authenticate and to fetch an authorization policy for remote access clients.

  Configure the authentication and authorization policies and the attributes on the RADIUS server.

- Default service VPN for SD-WAN RA: Select one of the service VPNs as the default service VPN for remote access. The connection from each remote access client is placed in this service VPN unless the authorization policy from the RADIUS server specifies a different service VPN.

Configure Cisco Catalyst SD-WAN Remote Access Using a Configuration Group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Remote Access feature in a System Profile.

a. Configure Remote Access.

Table 8: Remote Access Settings

Field	Description
Type	Choose Remote Access feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Connection Type	Choose the connection type from the following: • **IPsec** • **SSL-VPN** By default, IPsec is selected. We recommend using IPsec mode. SSL-VPN mode is supported only on Cisco Catalyst 8000v Edge Software with limited features.

b. Configure Authentication.

Table 9: Authentication

Field	Description
Radius Group Name	Choose an existing RADIUS group or create a new RADIUS group. Click **Add Radius Group** to add a RADIUS server and group to the AAA feature profile in the System Profile.
Pre-Shared Key (PSK) Authentication	Enable Pre-Shared Key (PSK) authentication. • **AAA-based-PSK**: Choose this option to fetch the pre-shared keys from the RADIUS server. This option allows configuring a pre-shared key on the RADIUS server that is unique per remote access client or a group of remote access clients. • **Groups PSK**: Choose this option to configure a common pre-shared key for all remote access clients connecting to a device. **Note** **Pre-Shared Key (PSK) Authentication** is applicable only for connection-type IPsec and not for SSL-VPN.

Field	Description
CA Server Setup	Choose a CA server for certificate-based authentication. The certificate from the selected CA is used by the device to authenticate the remote access clients. Before choosing a CA server, configure the CA server from **Configuration** > **Certificate Authority**.
User Authentication	Choose the user authentication option for AnyConnect Extensible Authentication Protocol (EAP) authentication used by remote access client. **Note** The **User Authentication** setting is applicable only for the IPsec connection type and not for SSL-VPN.
User & Device Authentication	Choose the user and device authentication option for AnyConnect EAP authentication used by remote access client. The **User & Device Authentication** setting is applicable only for the IPsec connection type and not for SSL-VPN.
Enable Profile Download	Enable download of an AnyConnect profile XML file to Cisco AnyConnect clients from the remote access headend devices. In the **Upload Profile XML File** pane, choose an XML file or drag and drop to upload. The maximum file size is 20 KB.

c. Configure AAA Policy.

Table 10: AAA Policy

Field	Description
Specify Name	Choose this option to specify the name of the policy to look up on the RADIUS server. In the **Policy Name** field, which appears only for the **Specify Name** option, enter the name of the policy.
Derive Name from Peer Identity	Choose this option to use the identity of the peer as the name of the policy to lookup on the RADIUS server. **Note** This setting is applicable only for the IPsec connection type and not for SSL-VPN.
Derive Name from Peer Identity Domain	Choose this option to use the domain portion of the identity of the peer as the name of the policy to look up on the RADIUS server. **Note** This setting is applicable only for the IPsec connection type and not for SSL-VPN.
Policy Password	Enter the policy password.

Field	Description
Enable Accounting	Enable accounting.

d. Configure Private IP-Pool.

Table 11: Private IP-Pool

Field	Description
Maximum Number of Clients	Enter the maximum number of remote access clients that can connect to a remote access headend device. This number determines the size of the IPv4 pool allocated to the device. If a global IPv6 pool is defined for remote access in the network hierarchy, each SD-WAN RA headend device will be allocated an IPv6 pool sufficient for the maximum number of remote access clients (8000).

e. Configure IKEv2 and IPsec settings.

Table 12: IKEv2 and IPsec Settings

Field	Description
Local IKE Identity Type	Enter the local IKEv2 identity type. The options are: • IPv4 Address or IPv6 Address • Email • FQDN • Key-ID
Local IKE Identity Value*	Enter the value of the local IKEv2 identity based on the identity type selected.
Security Association (SA) Lifetime	Enter the lifetime in seconds for the IKEv2 security association. The range is from 3600 to 86400. The default lifetime is 86400 seconds.
Enable Anti - Denial of Service (DOS) Check	Enable an Anti-Denial of Service (DOS) check.
Anti-DOS Threshold	Enter the Anti-DOS threshold value. Range: 10 to 1000. Default: 100.

What to do next

Also see Deploy a configuration group.

Add the SD-WAN Remote Access Feature Profile to an Existing Configuration Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**
2. Choose an existing configuration group and select **Edit**.
3. Choose **Feature Profiles** > **Service Profile** > **VPN**
4. Chosoe one of the service VPNs and select **Edit Feature** under **Actions**.
5. In **Basic Configuration**, select **Enable SDWAN Remote Access**.
6. Choose **Feature Profiles** > **System Profile** > **Add Feature** > **Remote Access**.

For information about working with configuration groups, see Configuration Groups and Feature Profiles.