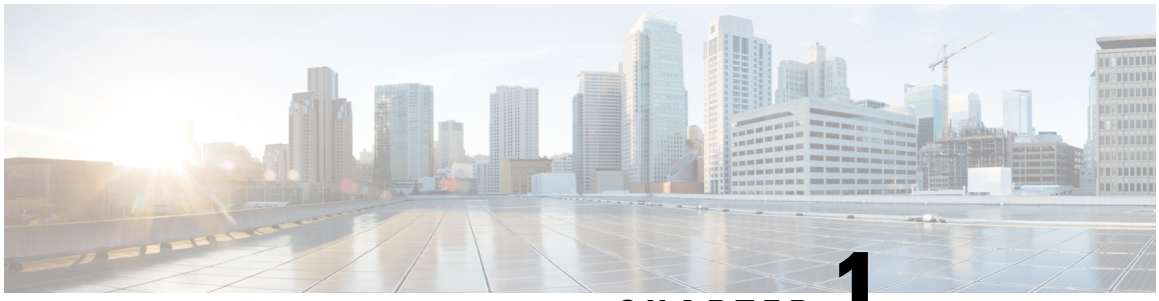
Cisco Catalyst SD-WAN Remote Access

First Published: 2021-11-22

Last Modified: 2024-08-27

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

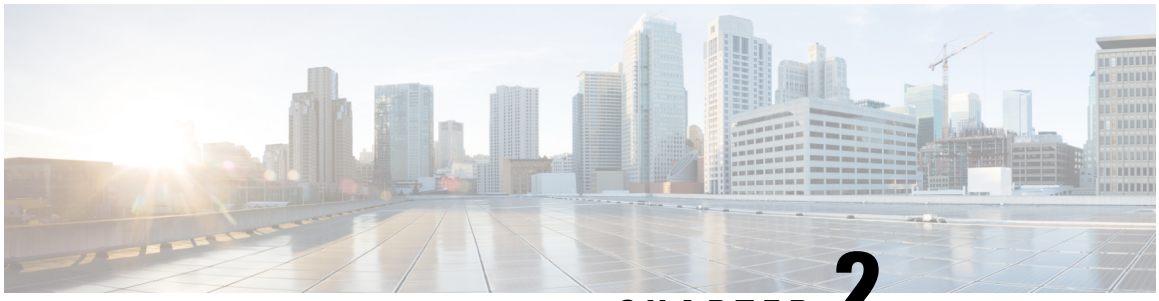
User Documentation

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

Cisco Catalyst SD-WAN Remote Access Features

Cisco Catalyst SD-WAN Remote Access Feature History

Table 1: Feature History

Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Remote Access	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	Remote access refers to enabling secure access to an organization's network from devices at remote locations. Cisco Catalyst SD-WAN Remote Access (SD-WAN RA) integrates remote access functionality into Cisco Catalyst SD-WAN. SD-WAN RA enables Cisco IOS XE Catalyst SD-WAN devices to function as remote access headends, managed through Cisco SD-WAN Manager. This eliminates the need for separate Cisco Catalyst SD-WAN and remote access infrastructure, and enables rapid scalability of remote access services. Remote access users can use the same software- or hardware-based remote access clients as with solutions that do not integrate with Cisco Catalyst SD-WAN. For remote access users, benefits include extending Cisco Catalyst SD-WAN features to remote users. Remote access users can access applications hosted on-premises, applications hosted in IaaS, SaaS applications, or the internet.
Cisco Catalyst SD-WAN Remote Access Configuration Using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enables you to configure Cisco Catalyst SD-WAN Remote Access for a device, using Cisco SD-WAN Manager. Configure Remote Access using the System feature profile in a configuration group.

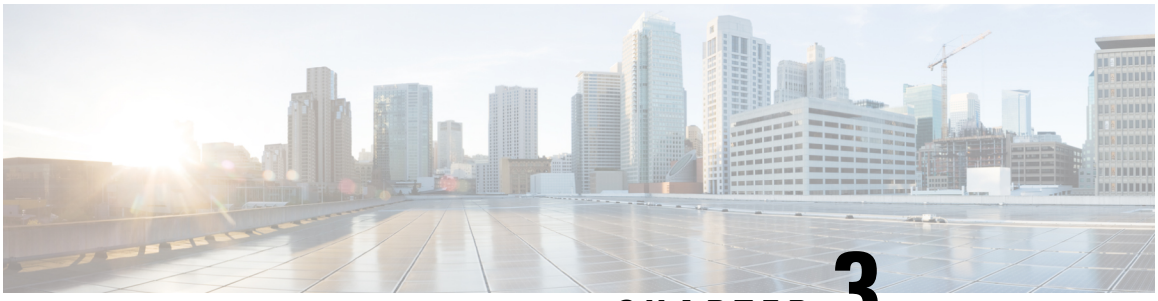
Feature Name	Release Information	Description
Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN mode Using Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature enables you to configure Cisco Catalyst SD-WAN Remote Access for a device in SSL-VPN mode, using Cisco SD-WAN Manager.
Monitor Cisco Catalyst SD-WAN Remote Access Devices	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature enhances the monitoring of remote access devices. Cisco SD-WAN Manager can provide the following information: • Number of remote access (RA) headends in the network and the supported RA mode (IPsec/SSLVPN). • Number of remote access sessions in the network and sessions per remote access headend, categorized into remote access client type.

SD-WAN Remote Access Feature Summary

Table 2: SD-WAN RA Feature Summary

Feature	Description
Cisco Catalyst SD-WAN Remote Access connection type (also referred to as mode)	• IKEv2/IPsec • SSL-VPN (TLS) **Note** IKE2/IPsec is the recommended and the default mode when configured from Cisco SD-WAN Manager.
Supported remote access clients	Cisco Catalyst SD-WAN Remote Access enables Cisco IOS XE Catalyst SD-WAN devices to terminate connections from the following types of client: IPsec mode: • Software: Cisco AnyConnect (IKEv2/IPsec) • Hardware: Cisco IOS-XE router functioning as a small office/home office (SOHO) remote access client SSL mode: • Software: Cisco AnyConnect (SSL mode) **Note** Remote access clients must be pre-configured with the DNS names or public IP addresses of the primary and backup Cisco Catalyst SD-WAN Remote Access headends.

Feature	Description
Supported platforms for the Cisco Catalyst SD-WAN Remote Access headend	IPsec mode: • Cisco Catalyst 8300-1N1S-6T • Cisco Catalyst 8300-1N1S-4T2X • Cisco Catalyst 8300-2N2S-4T2X • Cisco Catalyst 8300-2N2S-6T • Cisco Catalyst 8500-12X • Cisco Catalyst 8500-12X4QC • Cisco Catalyst 8500L • Cisco Catalyst 8000V Edge Software SSL(TLS) mode: • Cisco Catalyst 8000V Edge Software
Supported certificate authority (CA) servers	Any simple certificate enrollment protocol (SCEP)-capable CA server. The CA server provisions certificates on the Cisco IOS XE Catalyst SD-WAN devices that enable the remote access headend to authenticate itself to remote access clients when the headend is configured to use certificate-based authentication. It is common for the CA server to be deployed at a data center site in the service VPN, together with the RADIUS server.
Authentication, authorization, and accounting (AAA) management	RADIUS/extensible authentication protocol (EAP) server for authentication of remote access clients and for per-user policy management. It is common for the RADIUS server to be deployed at a data center site, together with the CA server.
Configuration method	Cisco SD-WAN Manager CLI template and using configuration groups.
Monitoring	• Monitoring Cisco Catalyst SD-WAN Remote Access devices through Cisco SD-WAN Manager. • Monitoring also through **show** commands and syslogs on the remote access headend devices.



CHAPTER 3

Cisco Catalyst SD-WAN Remote Access

Information About Cisco Catalyst SD-WAN Remote Access

Cisco Catalyst SD-WAN Remote Access (SD-WAN RA) fully integrates remote access functionality into the Cisco Catalyst SD-WAN fabric, extending the benefits of Cisco Catalyst SD-WAN to remote access users. Cisco Catalyst SD-WAN Remote Access enables Cisco IOS XE Catalyst SD-WAN devices to provide remote access headend functionality, managed through Cisco SD-WAN Manager.

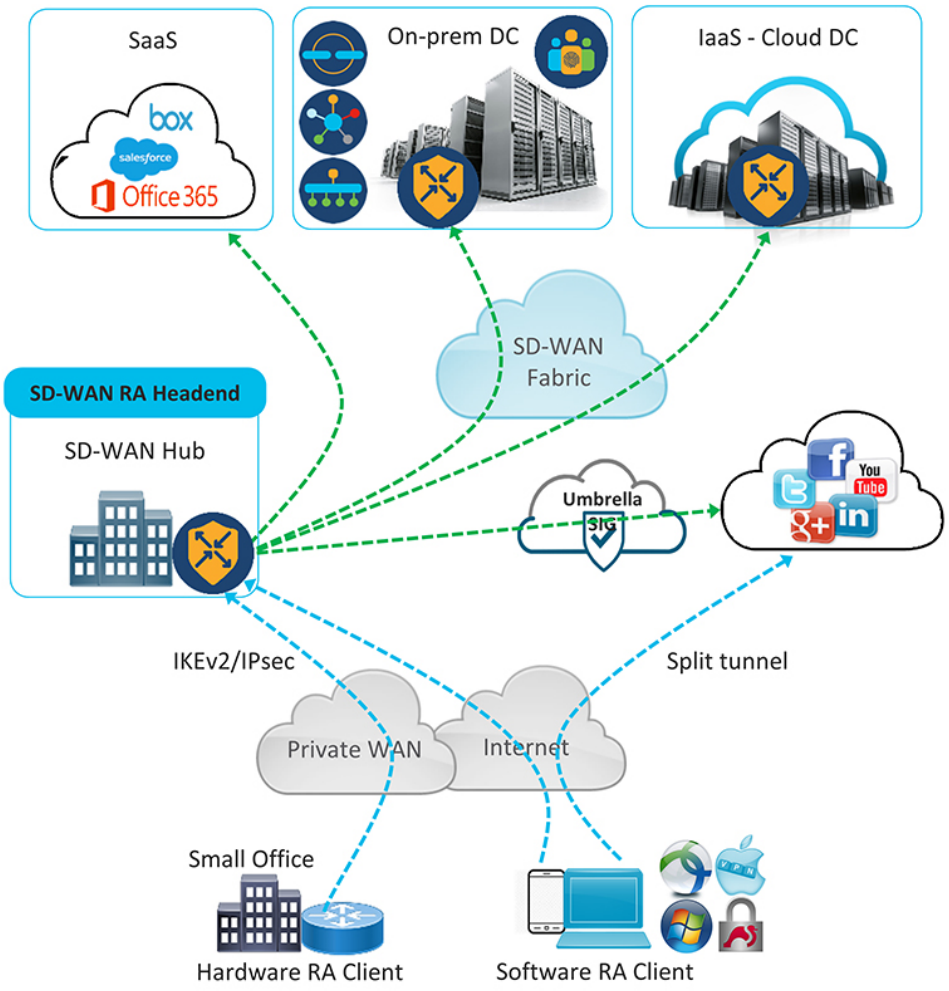
Deployment

As shown in the following figure, an SD-WAN RA headend device may be deployed as follows:

- On-premises (in a hub or data center)
- Hosted in a public cloud (for a software device)
- In a colocation facility

SD-WAN RA enables remote access users to access applications hosted on-premises, applications hosted in IaaS, SaaS applications, or the internet. The connectivity between remote access clients and the SD-WAN RA headend is commonly through the internet. For small office hardware remote access clients, the connectivity may be through a private WAN.

Figure 1: Cisco Catalyst SD-WAN Remote Access Architecture



Benefits of Cisco Catalyst SD-WAN Remote Access

- Integrated fabric for Cisco Catalyst SD-WAN and remote access (RA): The integration of remote access functionality into Cisco Catalyst SD-WAN eliminates the need for separate Cisco Catalyst SD-WAN and remote access networks, as Cisco IOS XE Catalyst SD-WAN devices in the Cisco Catalyst SD-WAN overlay network can function as remote access headend devices.
- Extends Cisco Catalyst SD-WAN features and benefits to remote access users. Remote access users become essentially branch LAN-side users. Features include the following:
  - Application visibility, application-aware routing, AppQoE, quality of service (QoS), network address translation direct internet access (NAT-DIA)
  - Enterprise-level security features: Cisco Unified Threat Defense (UTD), zone-based firewall (ZBFW), secure internet gateway (SIG), and so on

- Leverages the Cisco FlexVPN remote access solution, which is feature-rich and widely deployed. It includes the following capabilities:
  - Scalability
  - Support for IKEv2/IPsec and SSL based remote access VPNs
  - Full integration with AAA/RADIUS for identity-based policy
  - Full integration with Cisco IOS public key infrastructure (PKI) for automated certificate lifecycle management
  - Support for Cisco and third party software and hardware remote access clients
  - Support for dual-stack, link, and headend redundancy, and for horizontal scaling
  - Automated routing to remote access clients
  - Split tunneling
- Remote access users can use the same remote access clients as with solutions that do not integrate with Cisco Catalyst SD-WAN. The remote access client connects to the SD-WAN RA headend in the same way as it would with remote access headends that are not part of Cisco Catalyst SD-WAN.
- Extends the Cisco Catalyst SD-WAN solution to remote access users without requiring each remote access user's device to be part of the Cisco Catalyst SD-WAN fabric. Scaling to a large number of remote access clients has minimal impact on Cisco Catalyst SD-WAN scale limitations. There is no requirement of Cisco SD-WAN Manager connections to the remote access clients, and there is no need to configure the overlay management protocol (OMP) or bidirectional forwarding detection (BFD) for the remote access client devices.
- By configuring multiple Cisco IOS XE Catalyst SD-WAN devices as remote access headend devices, you gain the following advantages:
  - Enabling large scale remote access deployment
  - Ability to distribute the remote access load across numerous Cisco IOS XE Catalyst SD-WAN devices in the Cisco Catalyst SD-WAN fabric
  - Improving the ability of a remote access user to connect to a remote access headend close to the user's location
- Remote access termination is within the enterprise fabric, which provides the security advantage that remote access clients connect to enterprise-owned Cisco Catalyst SD-WAN edge devices.
- Enables a unified Cisco Identity Services Engine (ISE) user policy for on-site and remote access—for example, identity-based segmentation of users with virtual routing and forwarding (VRF) and security group tag (SGT)
- Rate limiting of remote access traffic: Aggregate remote access traffic can be rate-limited to a specific percentage of overall throughput.

Supported Devices for Cisco Catalyst SD-WAN Remote Access

The following devices, operating with Cisco Catalyst SD-WAN, support SD-WAN RA headend functionality in IPsec mode:

- Cisco Catalyst 8300-1N1S-6T
- Cisco Catalyst 8300-1N1S-4T2X
- Cisco Catalyst 8300-2N2S-4T2X
- Cisco Catalyst 8300-2N2S-6T
- Cisco Catalyst 8500-12X
- Cisco Catalyst 8500-12X4QC
- Cisco Catalyst 8500L Edge
- Cisco Catalyst 8000V Edge Software

The following devices, operating with Cisco Catalyst SD-WAN, support SD-WAN RA headend functionality in SSL mode:

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

- Cisco Catalyst 8000V Edge Software

Prerequisites for Cisco Catalyst SD-WAN Remote Access

Table 3: Summary of Prerequisites

	Prerequisite
1	Public IP address for SD-WAN RA headend reachability, when connecting by internet
2	Configure remote access clients to connect to the SD-WAN RA headend
3	Firewall policy to allow IKEv2/IPsec and TLS traffic
4	Private IP pool to assign a unique address to each remote access client This is optional if all remote access users connect to the headend by hardware remote access client.
5	Capacity planning for the SD-WAN RA headend
6	CA server for provisioning of certificates to the SD-WAN RA headend, when the headend is configured to use certificate-based authentication
7	RADIUS/EAP server for remote access client authentication and policy

Prerequisite Details

1. Public IP address

   Remote access clients connecting by internet must be able to connect to an SD-WAN RA headend through a static public IP address. Configure the remote access clients with the DNS name or the static public IP address of the SD-WAN RA headend.

Note When remote access clients connect through a private WAN, the SD-WAN RA headend does not require a static public IP address.

   The static public IP address may be one of the following:

   - Static public IP address on a firewall that provides access to the remote access headend
   - Static public IP on the remote access headend device
     - Static public IP on a TLOC interface

       A TLOC interface has built-in security, only allowing the protocols required for Cisco Catalyst SD-WAN operation, such as transport layer security/data datagram transport layer security (TLS/DTLS) and IPsec on predetermined ports. To enable any additional protocols, explicitly configure the TLOC interface to allow the protocols.

       When you use a TLOC interface as the WAN interface providing a static IP for an SD-WAN RA headend, Cisco Catalyst SD-WAN automatically detects that SD-WAN RA is enabled and allows the IKEv2 and IPsec protocols required for remote access operation.

       To enable Cisco AnyConnect remote access clients to download the AnyConnect VPN profile from the SD-WAN RA headend, enable the HTTPS/TLS protocol (TCP port 443) on the TLOC interface.

       Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, HTTPS/TLS protocol (TCP port 443) on the TLOC interface is automatically enabled on detecting SD-WAN RA configuration.

     - Static public IP on a non-TLOC interface

       In contrast with a TLOC interface, a non-TLOC interface does not have any built-in security and does not block any traffic. When you use a non-TLOC interface as the WAN interface providing a static IP for an SD-WAN RA headend, we recommend that you configure an inbound and outbound access-list on the WAN interface to allow only the protocols required for SD-WAN RA. These are IKEv2 and IPsec. To enable Cisco AnyConnect remote access clients to download the AnyConnect VPN profile from the SD-WAN RA headend, enable the HTTPS/TLS protocol (TCP port 443).

2. Configure remote access clients to connect to the SD-WAN RA headend

   Remote access clients must be pre-configured with the DNS names or the IP addresses of the SD-WAN RA headend devices, including primary and backup devices if you have configured backup devices.

   In a scenario where remote access clients connect by public internet, the addresses are static public IP addresses.
   In a scenario where remote access clients connect by private WAN, the addresses are private IP addresses.

3. Firewall policy to allow IKEv2/IPsec and TLS traffic

   If the SD-WAN RA headend is behind a firewall, then the firewall must allow the following protocols and ports in the inbound and outbound directions:

   - Inbound:
     - IKEv2: UDP ports 500 and 4500
     - IPsec: IP protocol ESP
     - TLS: TCP 443
     - Source IP address: Any
     - Destination IP address: SD-WAN RA headend public IP
   - Outbound:
     - IKEv2: UDP ports 500 and 4500
     - IPsec: IP protocol ESP
     - TLS: TCP 443
     - Source IP address: SD-WAN RA headend public IP
     - Destination IP address: Any

4. Private IP pool to assign a unique address to each remote access client

   This is optional if all of the remote access users connect by hardware remote access client.

   In remote access solutions, the remote access headend assigns a private IP address to each remote access client. The remote access client uses the assigned IP as the source IP address for the remote access VPN inner traffic (traffic that has not yet been encrypted for VPN). The assigned IP enables the remote access headend to identify and route return traffic to the remote access client.

   Each SD-WAN RA headend requires a unique private IP pool from which to assign IP addresses to remote access clients. An SD-WAN RA headend can share the private IP pool across all the service VPNs that a remote access user may be placed in.

   This is optional if the remote access clients are limited to small office clients using a hardware remote access client.

5. Summary-route configuration

   For each remote access client, the SD-WAN RA headend adds a static host route to the assigned IP address in the service VPN in which the remote access user is placed, based on the user's identity.

   When SD-WAN RA assigns an IP address to a remote access client, it creates a static route for the assigned IP address. The static route specifies the VPN tunnel of the remote access client connection. The SD-WAN RA headend advertises the static IP within the service VPN of the remote access client. Cisco Catalyst SD-WAN uses the overlay management protocol (OMP) to advertise the static routes to all edge devices in the service VPN. Advertising each route to all edge devices creates a problem for scaling because individually advertising the static routes for thousands of remote access clients may diminish performance.

   To avoid advertising a large number of static routes, you can configure OMP to advertise the IP pool subnet as a summary-route in each service VPN.

6. Capacity planning for the SD-WAN RA headend

   The SD-WAN RA headend shares the cryptographic accelerator, WAN bandwidth, and the router throughput capacity with Cisco Catalyst SD-WAN IPsec Depending on the number of remote access connections, and on the amount of remote access throughput that you intend for each Cisco IOS XE Catalyst SD-WAN device to support, you may require additional capacity.

Note The maximum number of IPsec sessions supported on a Cisco IOS XE Catalyst SD-WAN device is shared between Cisco Catalyst SD-WAN IPsec/BFD and remote access IPsec sessions. Similarly, the IPsec throughput capacity of a device is shared between Cisco Catalyst SD-WAN and remote access IPsec.

7. CA server

   The CA server provisions certificates on Cisco IOS XE Catalyst SD-WAN devices for SD-WAN RA headend authentication with the remote access clients, if the headend is configured to use certificate-based authentication.The CA server must support the simple certificate enrollment protocol (SCEP) for certificate enrollment.

   The CA server must be reachable from all the SD-WAN RA headends in a service VPN.

8. RADIUS/EAP server

   SD-WAN RA headends use a RADIUS/EAP server for authentication of remote access clients and for managing per-user policy.

   The RADIUS/EAP server must be reachable from all the SD-WAN RA headends in a service VPN.

Note It is common to deploy the CA server and the RADIUS server together at a data center site in the service VPN.

Restrictions for Cisco Catalyst SD-WAN Remote Access

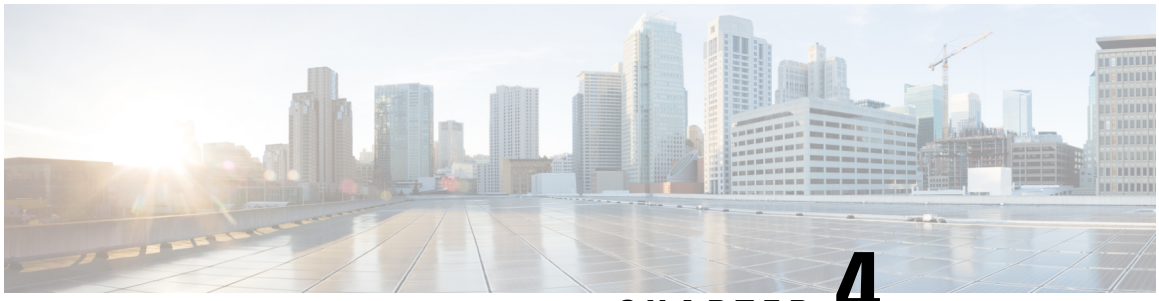
Note Before configuring SD-WAN RA functionality for a remote access headend device, first use Cisco SD-WAN Manager feature templates to configure any prerequite configurations, such as service VPN VRF definition and static public IP for the TLOC interface.

- The tools for monitoring and troubleshooting are limited to **show** commands and viewing syslogs on the SD-WAN RA headend device.
- Traffic that reaches a Cisco Catalyst SD-WAN edge device operating as a remote access headend goes through two IPsec tunnels—one from the remote device to the remote access headend, and another from the remote access headend to other endpoints within the enterprise network or outside of the network. Because packets use two separate tunnels, the remote access headend device may reach its licensed throughput limit sooner than expected. To check whether any packets are being dropped due to a throughput limit use the **show platform hardware qfp active feature ipsec data drop** command on the edge device to view the counters for packets dropped due to exceeding the throughput limit.

- Cisco SD-WAN RA in SSL-VPN mode only supports TLS and not DTLS.

Use Cases for SD-WAN RA

- In scenarios where remote users connect to a Cisco Catalyst SD-WAN network, you can configure one or more Cisco IOS XE Catalyst SD-WAN devices to manage remote access headend tasks instead of requiring separate devices, outside of the Cisco Catalyst SD-WAN fabric, to manage remote access headend tasks.
- In scenarios where it is necessary to scale up to meet remote access demands, it may be helpful to distribute the load by employing one or more Cisco IOS XE Catalyst SD-WAN devices as remote access headends.



CHAPTER 4

Configure Cisco Catalyst SD-WAN Remote Access

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 This is optional if the remote access headend uses an authentication method that does not require certificates.
Task 3	Configure IKEv2 profiles to group remote access clients based on identity, and specify authentication and authorization policy

	Task
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 4: 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 5: 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.

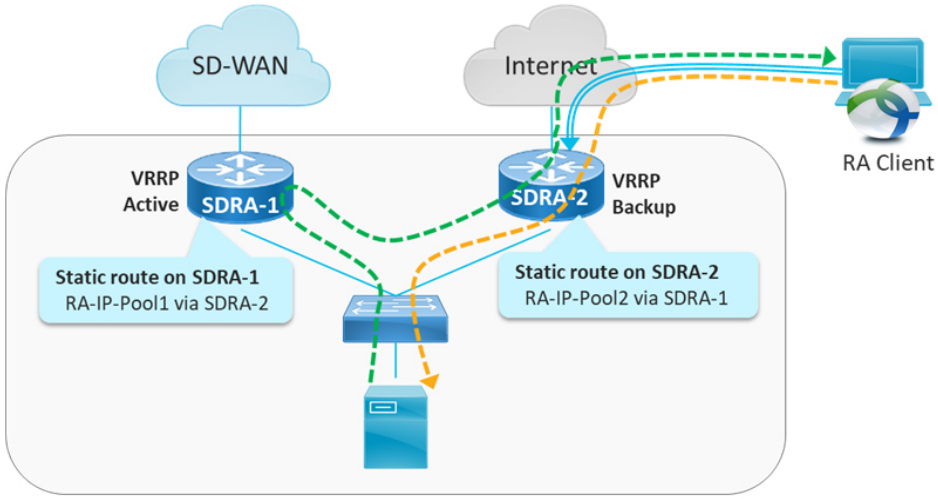
Task 10: Configure Remote Access Traffic Symmetry

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 2: 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.

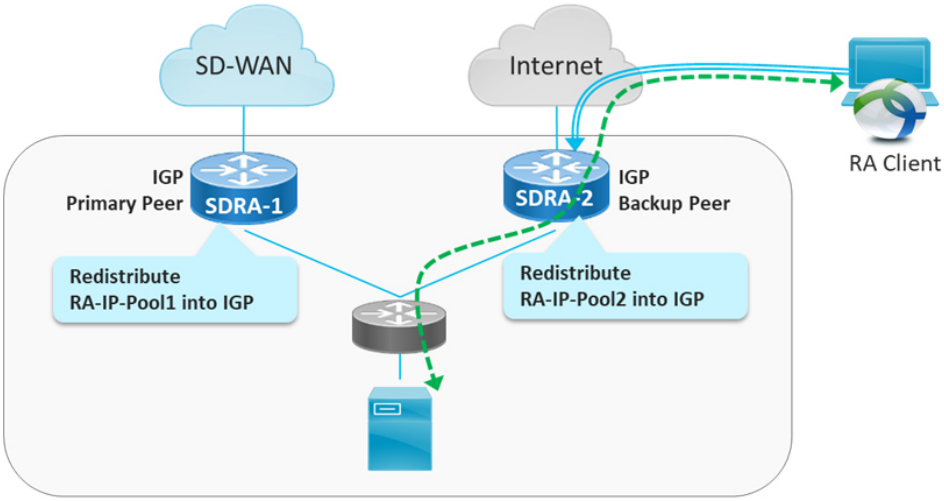
- On SDRA-1, configure a static route as follows:
  - Route destination: SDRA-2 IP pool subnet
  - Route next-hop: SDRA-2 service VPN IP

- 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 3: 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

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Create Configuration Group**.
2. Enter the configuration group name and the description in the **Name** and **Description** fields.
3. Click **Next**.

   The **Additional Features** page opens.
4. Enable **Remote Access**.

5. For **Radius Server Address**, enter the IP address of the RADIUS server.
6. For **Radius Server Key**, enter the RADIUS server key.
7. Choose the service VPN to reach the RADIUS server from the **Select Service VPN** drop-down list.
8. Click **Create Configuration Group**.

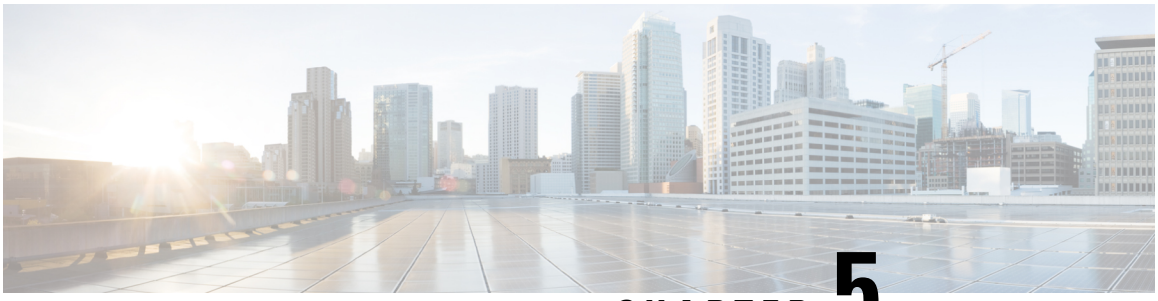
   Cisco SD-WAN Manager creates a new configuration group with the SD-WAN RA feature enabled. The **Remote Access** feature profile appears in the **System Profile**.

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

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.



CHAPTER 5

Verify and Monitor Cisco Catalyst SD-WAN Remote Access

Verify and Monitor SD-WAN Remote Access

On the Cisco IOS XE Catalyst SD-WAN device hosting the SD-WAN RA headend, use the following commands to verify that the remote access headend is configured and functioning.

Verification requires at least one remote user to be connected.

Client Connections in SD-WAN RA IPsec Mode

Use the **show crypto session** command and view the details in the "Interface: Virtual-Access" blocks in the command output. Each of these blocks corresponds to a connected client, and shows the IP address of the client and the details of the connection.

```
Device# show crypto session
…
Interface: Virtual-Access1
Profile: IKEV2_PROFILE
Session status: UP-ACTIVE
Peer: 10.0.12.40 port 500
  Session ID: 2
  IKEv2 SA: local 10.0.31.31/500 remote 10.0.12.40/500 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
```

IKEv2 Sessions in SD-WAN RA IPsec Mode

Use the **show crypto ikev2 sa detailed** command to view the details of the IKEv2 session. For each connected client, the command output includes a block similar to the one in the following example. In the output, verify that the status is READY.

```
Device# show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
3         10.100.0.1/500        10.200.0.1/500        none/10              READY
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA,
```

```
Auth verify: RSA
      Life/Active Time: 86400/82405 sec
      CE id: 0, Session-id: 3
      Status Description: Negotiation done
      Local spi: 0123456789ABCDEF       Remote spi: ABCDEF0123456789
      Local id: example1@example.com
      Remote id: example2@example.com
      Local req msg id:  0              Remote req msg id:  50
      Local next msg id: 0              Remote next msg id: 50
      Local req queued:  0              Remote req queued:  50
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: enabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Assigned host addr: 192.168.100.1
      Initiator of SA : No
```

Client Connections in SD-WAN RA SSL (TLS) mode

Use the **show crypto ssl session** command to view the details of the clients connected.

```
Device# show crypto ssl session

SSL profile name: sslvpn_sdra_profile
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
myssl              170.1.1.100               1         11:29:49  11:29:49

Device# show crypto ssl session user myssl

Interface         : Virtual-Access1
Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 4.9.06037
Username          : myssl                Num Connection : 1
Public IP         : 170.1.1.100
Profile           : sslvpn_sdra_profile
Policy            : sdra_sslvpn_policy
Last-Used         : 11:29:59             Created        : 23:35:52.695 UTC Sun Jul 16 2023
Tunnel IP         : 172.16.224.6         Netmask        : 0.0.0.0
Rx IP Packets     : 0                    Tx IP Packets  : 0
```

Route Information

Use the **show ip route vrf** *vrf* command to view route information. Specify the VRF assigned to a client. The command output shows information regarding the routes used in the VRF. Lines containing "Virtual-Access1" or similar indicate that a client is connected.

```
Device# show ip route vrf 10
Routing Table: 10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

```
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Loopback2
L        10.1.1.2/32 is directly connected, Loopback2
S        10.1.1.21/32 is directly connected, Virtual-Access1
      10.100.0.0/8 is variably subnetted, 4 subnets, 2 masks
m        10.100.7.0/24 [251/0] via 172.16.255.70, 2d23h, Sdwan-system-intf
m        10.100.17.0/24 [251/0] via 172.16.255.30, 02:29:17, Sdwan-system-intf
C        10.100.27.0/24 is directly connected, GigabitEthernet5
L        10.100.27.1/32 is directly connected, GigabitEthernet5
```

Monitor Cisco Catalyst SD-WAN Remote Access Devices

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1

Cisco SD-WAN Manager can monitor devices in the overlay operating as remote access headends.To set up monitoring, add the following dashlets in the **Overview** dashboard:

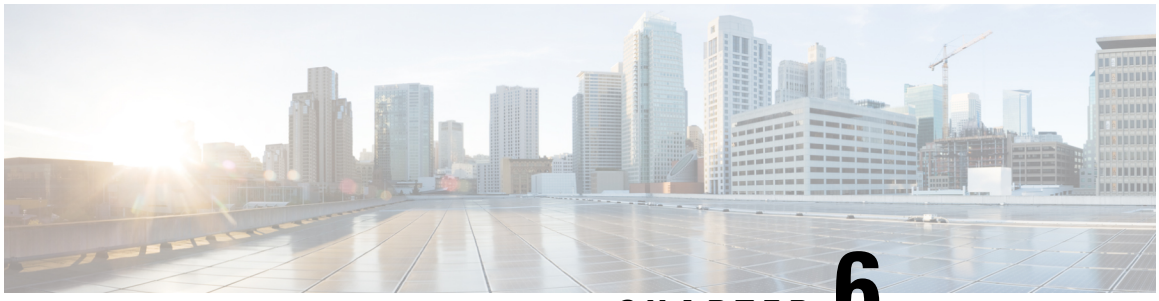
- **Remote Access Headends**: Shows the total number of remote access headends in the network, organized by mode.
- **Remote Access Sessions**: Shows the number of remote access sessions in the network, categorized by client type. Also, lists the remote access headend devices that have the most remote access sessions (only top five devices are listed).

View Remote Access Session Information for Devices

To view remote access session details for each remote access headend, click **View Details** on the **Remote Access Headends** dashlet or **Remote Access Sessions** dashlet.

In the devices table, the following columns provide information about remote access sessions:

- **RA Session**: Total number of remote access sessions in the network.
- **RA Session Breakdown**: Type of remote access session or client.



CHAPTER 6

Troubleshoot Cisco Catalyst SD-WAN Remote Access

Overview

This chapter provides links to documents authored by Cisco subject matter experts (SMEs). They aim to help you resolve technical issues without requiring a support ticket. If these documents are unable to resolve your issue, we recommend visiting the applicable Cisco Community. There is a wealth of information and advice available from fellow Cisco customers who may have experienced this issue already and provided a solution. If you are not able to find a resolution on the Community, it may be best that you raise a support ticket at Cisco Support. In cases where a support ticket has to be raised, these documents provide guidance about the data that should be collected and added to the support ticket. Specify the support document you referred, and TAC can create an improvement request with the document owner.

Support Articles

The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

The following support article is associated with this technology:

Document	Description
Configure Cisco Catalyst SD-WAN Remote Access (SD-WAN RA) with AnyConnect and ISE Server	This document describes how to configure Cisco Catalyst SD-WAN Remote Access (SD-WAN RA) with AnyConnect Client using a Cisco IOS XE autonomous mode as a CA server, and a Cisco Identity Services Engine (ISE) server for the Authentication, Authorization, and Accounting.

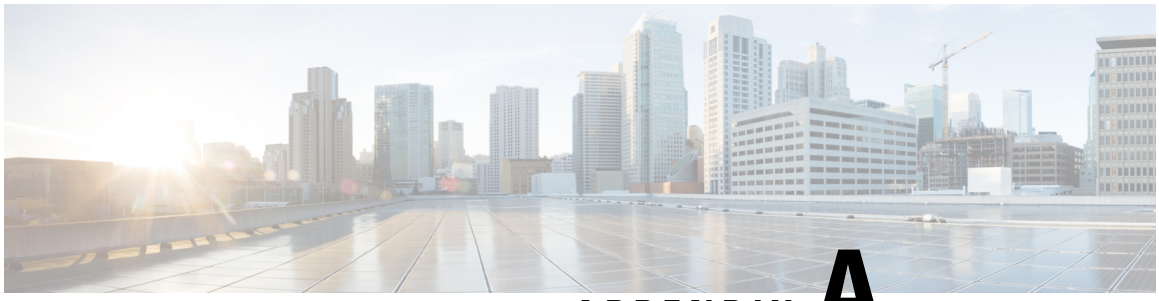
Feedback Request

Your input helps. A key aspect to improving these support documents is customer feedback. Note that these documents are owned and maintained by multiple teams within Cisco. If you find an issue specific to the document (unclear, confusing, information missing, etc):

- Provide feedback using the **Feedback** button located at the right panel of the corresponding article. The document owner will be notified, and will either update the article, or flag it for removal.
- Include information regarding the section, area, or issue you had with the document and what could be improved. Provide as much detail as possible.

Disclaimer and Caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.



APPENDIX A

Example Configuration for Cisco Catalyst SD-WAN Remote Access, RADIUS, and AnyConnect

Example Configuration for SD-WAN Remote Access, RADIUS, and AnyConnect

This example describes the configuration of the following:

- SD-WAN RA headend device
- RADIUS server
- AnyConnect remote access client

The following remote access connection details apply to the example:

- Remote access client type: Cisco AnyConnect
- Remote access client authentication type: AnyConnect-EAP user authentication
- CA server with SCEP-based certificate enrollment
- RADIUS server configured with following profiles and attributes:
  - User profile name: user1@example.com
  - User password: user1-passwd
  - Group profile name: example.com
  - Group profile attributes: VRF, ip unnumbered interface, IP pool name, server subnets

Before You Begin

- In Cisco SD-WAN Manager, configure the following using a feature template:

- VRF for the SD-WAN RA service VPN
- Public IP on the TLOC interface used for SD-WAN RA

- Ensure that the RADIUS server and CA server are reachable in the SD-WAN RA service VPN.

SD-WAN RA Headend Device Configuration

This example provides a generic template for configuring a Cisco IOS XE Catalyst SD-WAN device to function as an SD-WAN RA headend. The template uses variables that prompt you for details specific to your network, at runtime when you apply the template.

The following table describes the variables used in the template.

Table 6: CLI Template Variables

Variable	Description
SDRA_POOL_START_IP	First IP address of the private IP pool configured on the SD-WAN RA headend
SDRA_POOL_END_IP	Last IP address of the private IP pool configured on the SD-WAN RA headend
SDRA_UNNUM_INTF_IP	Private IP address to use on the SD-WAN RA unnumbered interface, preferably in the same subnet as private IP pool. The SD-WAN RA headend uses this interface as the source IP for communication with the RADIUS server. Configure this interface IP address as the SD-WAN RA headend IP on the RADIUS server.
SDRA_SERVICE_VPN	Service VPN in which the CA and RADIUS servers must be reachable. By default, the SD-WAN RA headend places a remote access user into this service VPN unless the RADIUS-based user and group policy specifies a different service VPN.
SDRA_RADIUS_IP	IP address of the RADIUS server reachable in the SDRA_SERVICE_VPN
SDRA_RADIUS_ENCR_KEY	Encryption key to use with the RADIUS server. This key must match the key configured on the RADIUS server.
SDRA_RADIUS_SOURCE_INTF	The interface in the SDRA_SERVICE_VPN to be used as source interface for RADIUS communication. The IP address configured on the SDRA_RADIUS_SOURCE_INTF must be configured on the RADIUS server for authorization.
SDRA_AUTHOR_RADIUS_PASSWD	The password used with the group authorization request to the RADIUS server. The group authorization name and password must match the group profile name and password configured on the RADIUS server.

Variable	Description
SDRA_CA_SERVER_IP	IP address of the CA server reachable in the SDRA_SERVICE_VPN
SDRA_CA_CERT_FINGERPRINT	Fingerprint of the CA certificate
SDRA_HEADEND_SUBJECT_NAME	Subject name to use in the SD-WAN RA headend certificate

Use the following in a CLI add-on template:

```
ip local pool SDRA_IP_POOL {{SDRA_POOL_START_IP}} {{SDRA_POOL_END_IP}}
!
aaa new-model
!
aaa group server radius SDRA_RADIUS_SERVER
server-private {{SDRA_RADIUS_IP}} key {{SDRA_RADIUS_ENCR_KEY}}
ip radius source-interface {{SDRA_RADIUS_SOURCE_INTF}}
ip vrf forwarding {{SDRA_SERVICE_VPN}}
!
no ip http secure-server
!
aaa authentication login SDRA_AUTHEN_MLIST group SDRA_RADIUS_SERVER
aaa authorization network SDRA_AUTHOR_MLIST group SDRA_RADIUS_SERVER
aaa accounting network SDRA_ACC_MLIST start-stop group SDRA_RADIUS_SERVER
!
crypto pki trustpoint SDRA_TRUSTPOINT
enrollment url http://{{SDRA_CA_SERVER_IP}}:80
fingerprint {{SDRA_CA_CERT_FINGERPRINT}}
revocation-check none
rsakeypair SDRA_TRUSTPOINT 2048
subject-name cn={{SDRA_HEADEND_SUBJECT_NAME}}
auto-enroll 80
auto-trigger
vrf {{SDRA_SERVICE_VPN}}
!
crypto ikev2 proposal SDRA_IKEV2_PROPOSAL
encryption aes-cbc-256
integrity sha256
group 19
!
crypto ikev2 policy SDRA_IKEV2_POLICY
proposal IKEV2_PROPOSAL
!
crypto ikev2 profile SDRA_IKEV2_PROFILE
match identity remote any
authentication local rsa-sig
authentication remote anyconnect-eap aggregate
pki trustpoint SDRA_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_NAME_MANGLER_DOMAIN password {{SDRA_AUTHOR_RADIUS_PASSWD}}
aaa accounting anyconnect-eap SDRA_ACC_MLIST
virtual-template 101 mode auto
reconnect
!
crypto ikev2 name-mangler SDRA_NAME_MANGLER_DOMAIN
eap suffix delimiter @
!
crypto ipsec transform-set SDRA_IPSEC_TS esp-gcm 256
mode tunnel
!
crypto ipsec profile SDRA_IPSEC_PROFILE
```

```
set ikev2-profile SDRA_IKEV2_PROFILE
set transform-set SDRA_IPSEC_TS
!
interface Loopback 65515
no shutdown
vrf forwarding {{SDRA_SERVICE_VPN}}
ip address {{SDRA_UNNUM_INTF_IP}} 192.168.0.1
!
interface Virtual-Template101 type tunnel
no shutdown
vrf forwarding {{SDRA_SERVICE_VPN}}
tunnel mode ipsec ipv4
tunnel protection ipsec profile SDRA_IPSEC_PROFILE
exit
!
```

RADIUS Server Configuration

The following is an example user profile:

```
user1@example.com  Cleartext-password := "user1-passwd"
 Service-Type = NAS-Prompt-User,
```

The following is an example group profile:

```
example.com   Cleartext-password := "group-passwd"
 Service-Type = NAS-Prompt-User,
 cisco-avpair+="ip:interface-config=vrf forwarding 20",
 cisco-avpair+="ip:interface-config=ip unnumbered Loopback 65515",
 cisco-avpair+="ipsec:addr-pool=IP_LOCAL_POOL",
 cisco-avpair+="ipsec:route-set=prefix 192.168.1.0/24",
 cisco-avpair+="ipsec:route-set=prefix 192.168.2.0/24"
```

AnyConnect Remote Access Client Configuration

The AnyConnect client connects to an SD-WAN RA headend similarly to how it connects to any other remote access headend. However, AnyConnect uses SSL by default, and SSL is not supported by SD-WAN RA, so it is necessary to change the mode to IKEv2/IPsec.

In this brief example, the AnyConnect client does not download the profile from the SD-WAN RA headend, but instead uses a locally defined profile.

Note the following points of AnyConnect configuration for this scenario:

- Disable AnyConnect profile download.

  In the AnyConnect local policy file, configure the **BypassDownloader** variable to **TRUE**.

- Specify IKEv2/IPsec mode

  ```
  PrimaryProtocol: IPsec
  ```