Cisco SD-WAN Remote Access

First Published: 2021-11-22

Last Modified: 2021-11-22

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 Read Me First 1

CHAPTER 2 SD-WAN Remote Access Features 3

- SD-WAN Remote Access Feature History 3
- SD-WAN Remote Access Feature Summary, By Release 3

CHAPTER 3 Cisco SD-WAN Remote Access 5

- Information About SD-WAN Remote Access 5
  - Benefits of SD-WAN RA 6
- Supported Devices for SD-WAN RA 7
- Prerequisites for SD-WAN RA 8
- Restrictions for Cisco SD-WAN RA 11
- Use Cases for SD-WAN RA 11

CHAPTER 4 Configure SD-WAN Remote Access 13

- Configure SD-WAN RA 13
- Task 1: Configure IKEv2 Ciphers and Parameters 14
- Task 2: Configure a PKI Trustpoint for Certificate Enrollment 15
- Task 3: Configure an IKEv2 Profile 16
- Task 4: Configure IPsec Ciphers, Parameters, and Template Interface 17
- Task 5: Configure AnyConnect Profile Download 18
- Task 6: Configure a Unique Local Private IP Pool on the SD-WAN RA Headend 19
- Task 7: Configure AAA Parameters and RADIUS Server Parameters 20
- Task 8: Configure the RADIUS Server with User Credentials and Policy 20

Task 9: Configure RA Traffic Rate Limiting 23

Task 10: Configure RA Traffic Symmetry 25

Task 11: Configure Cisco SD-WAN Features for RA Traffic 27

CHAPTER 5 **Verify and Monitor SD-WAN Remote Access** 29

APPENDIX A **Example Configuration for SD-WAN Remote Access, RADIUS, and AnyConnect** 31

CHAPTER 1

Read Me First

Related References

- Release Notes
- Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations

User Documentation

- User Documentation for Cisco IOS XE (SD-WAN) Release 17

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

SD-WAN Remote Access Features

- SD-WAN Remote Access Feature History, on page 3
- SD-WAN Remote Access Feature Summary, By Release, on page 3

SD-WAN Remote Access Feature History

Table 1: Feature History

Feature Name	Release Information	Description
SD-WAN Remote Access	Cisco IOS XE 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 SD-WAN remote access (SD-WAN RA) integrates remote access functionality into Cisco SD-WAN. SD-WAN RA enables Cisco IOS XE SD-WAN devices to function as RA headends, managed through Cisco vManage. This eliminates the need for separate Cisco SD-WAN and RA infrastructure, and enables rapid scalability of RA services. RA users can use the same software- or hardware-based RA clients as with solutions that do not integrate with Cisco SD-WAN. For RA users, benefits include extending Cisco SD-WAN features to remote users. RA users can access applications hosted on-premises, applications hosted in IaaS, SaaS applications, or the internet.

SD-WAN Remote Access Feature Summary, By Release

Table 2: SD-WAN RA Feature Summary, Cisco IOS XE Release 17.7.1a

Feature	Description
RA VPN mode	Internet key exchange version 2 (IKEv2) and the internet protocol security (IPsec) protocol suite.

Feature	Description
Supported RA clients	SD-WAN RA enables Cisco IOS XE SD-WAN devices to terminate IKEv2/IPsec VPN connections from the following types of client: • Software: Cisco AnyConnect • Hardware: Cisco IOS-XE router functioning as a small office/home office (SOHO) RA client **Note** RA clients must be pre-configured with the DNS names or public IP addresses of the primary and backup SD-WAN RA headends.
Supported platforms for the SD-WAN RA headend	• Cisco Catalyst 8300-1N1S-6T • Cisco Catalyst 8300-2N2S-4T2X • Cisco Catalyst 8500-12X • Cisco Catalyst 8500-12X4QC • Cisco Catalyst 8500L • 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 SD-WAN devices that enable the RA headend to authenticate itself to RA 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 RA 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 vManage CLI template
Monitoring	Monitoring is through **show** commands and syslogs on the RA headend devices.

CHAPTER 3

Cisco SD-WAN Remote Access

- Information About SD-WAN Remote Access, on page 5
- Supported Devices for SD-WAN RA, on page 7
- Prerequisites for SD-WAN RA, on page 8
- Restrictions for Cisco SD-WAN RA, on page 11
- Use Cases for SD-WAN RA, on page 11

Information About SD-WAN Remote Access

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

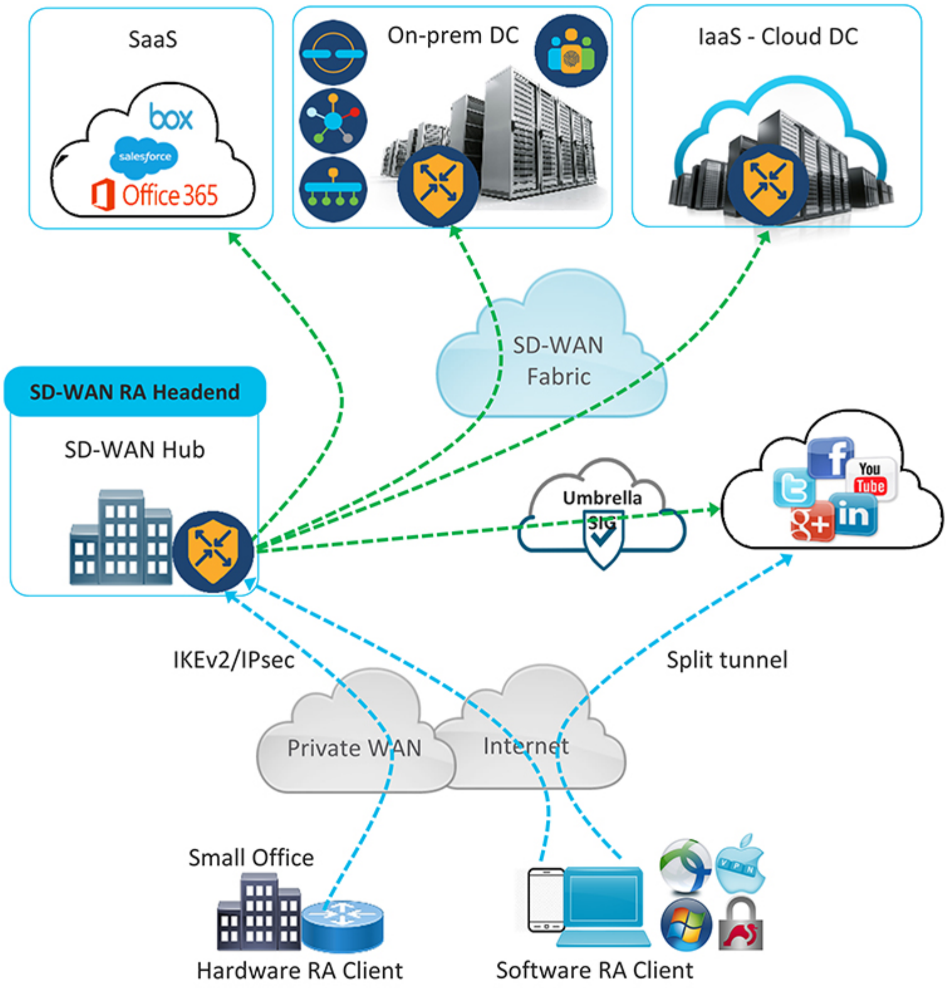
Deployment

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

Figure 1: SD-WAN Remote Access Architecture



Benefits of SD-WAN RA

- Integrated fabric for Cisco SD-WAN and RA: The integration of RA functionality into Cisco SD-WAN eliminates the need for separate Cisco SD-WAN and RA networks, as Cisco IOS XE SD-WAN devices in the Cisco SD-WAN overlay network can function as RA headend devices.
- Extends Cisco SD-WAN features and benefits to RA users. RA 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 RA solution, which is feature-rich and widely deployed. It includes the following capabilities:

  - Scalability
  - Support for IKEv2/IPsec and SSL based RA 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 RA clients
  - Support for dual-stack, link, and headend redundancy, and for horizontal scaling
  - Automated routing to RA clients
  - Split tunneling

- RA users can use the same RA clients as with solutions that do not integrate with Cisco SD-WAN. The RA client connects to the SD-WAN RA headend in the same way as it would with RA headends that are not part of Cisco SD-WAN.
- Extends the Cisco SD-WAN solution to RA users without requiring each RA user's device to be part of the Cisco SD-WAN fabric. Scaling to a large number of RA clients has minimal impact on Cisco SD-WAN scale limitations. There is no requirement of Cisco vManage connections to the RA clients, and there is no need to configure the overlay management protocol (OMP) or bidirectional forwarding detection (BFD) for the RA client devices.
- By configuring multiple Cisco IOS XE SD-WAN devices as RA headend devices, you gain the following advantages:
  - Enabling large scale RA deployment
  - Ability to distribute the RA load across numerous Cisco IOS XE SD-WAN devices in the Cisco SD-WAN fabric
  - Improving the ability of an RA user to connect to an RA headend close to the user's location
- RA termination is within the enterprise fabric, which provides the security advantage that RA clients connect to enterprise-owned Cisco 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 RA traffic: Aggregate RA traffic can be rate-limited to a specific percentage of overall throughput.

Supported Devices for SD-WAN RA

The following devices, operating with Cisco SD-WAN, support SD-WAN RA headend functionality.

- Cisco Catalyst 8300-1N1S-6T
- Cisco Catalyst 8300-2N2S-4T2X
- Cisco Catalyst 8500-12X

- Cisco Catalyst 8500-12X4QC
- Cisco Catalyst 8500L Edge
- Cisco Catalyst 8000V Edge Software

Prerequisites for SD-WAN RA

Table 3: Summary of Prerequisites

	Prerequisite
1	Public IP address for SD-WAN RA headend reachability, when connecting by internet
2	Configure RA 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 RA client This is optional if all RA users connect to the headend by hardware RA 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 RA client authentication and policy

Prerequisite Details

1. Public IP address

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

   Note When RA 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 RA headend
   - Static public IP on the RA headend device
     - Static public IP on a TLOC interface

       A TLOC interface has built-in security, only allowing the protocols required for Cisco 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 SD-WAN automatically detects that SD-WAN RA is enabled and allows the IKEv2 and IPsec protocols required for RA operation.

To enable Cisco AnyConnect RA 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.

- 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 RA clients to download the AnyConnect VPN profile from the SD-WAN RA headend, enable the HTTPS/TLS protocol (TCP port 443).

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

   RA 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 RA clients connect by public internet, the addresses are static public IP addresses. In a scenario where RA 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 RA client

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

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

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

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

5. Summary-route configuration

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

   When SD-WAN RA assigns an IP address to an RA client, it creates a static route for the assigned IP address. The static route specifies the VPN tunnel of the RA client connection. The SD-WAN RA headend advertises the static IP within the service VPN of the RA client. Cisco 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 RA 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 SD-WAN IPsec Depending on the number of RA connections, and on the amount of RA throughput that you intend for each Cisco IOS XE SD-WAN device to support, you may require additional capacity.

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

7. CA server

   The CA server provisions certificates on Cisco IOS XE SD-WAN devices for SD-WAN RA headend authentication with the RA 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 RA 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 SD-WAN RA

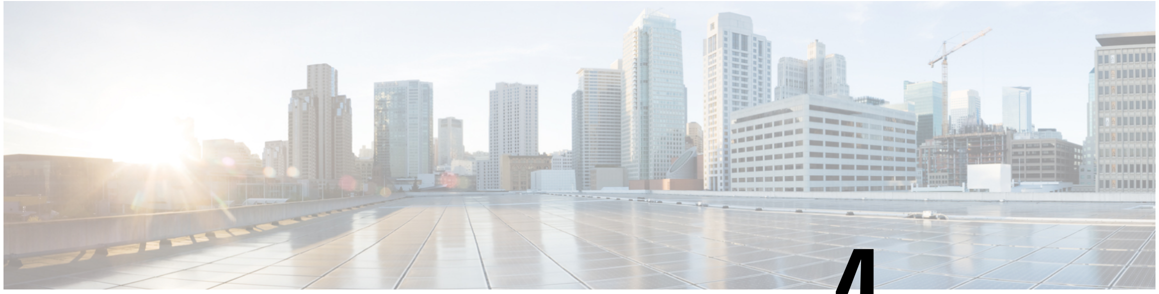
- You can configure SD-WAN RA headend functionality only by using Cisco vManage CLI add-on templates for the devices functioning as RA headends.

> **Note** Before configuring SD-WAN RA functionality for an RA headend device, first use Cisco vManage 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.
- RA VPN support is limited to IKEv2/IPsec-based tunnels. SSL-based tunnels are not supported.

Use Cases for SD-WAN RA

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



CHAPTER 4

Configure SD-WAN Remote Access

- Configure SD-WAN RA, on page 13
- Task 1: Configure IKEv2 Ciphers and Parameters, on page 14
- Task 2: Configure a PKI Trustpoint for Certificate Enrollment, on page 15
- Task 3: Configure an IKEv2 Profile, on page 16
- Task 4: Configure IPsec Ciphers, Parameters, and Template Interface, on page 17
- Task 5: Configure AnyConnect Profile Download, on page 18
- Task 6: Configure a Unique Local Private IP Pool on the SD-WAN RA Headend, on page 19
- Task 7: Configure AAA Parameters and RADIUS Server Parameters, on page 20
- Task 8: Configure the RADIUS Server with User Credentials and Policy, on page 20
- Task 9: Configure RA Traffic Rate Limiting, on page 23
- Task 10: Configure RA Traffic Symmetry, on page 25
- Task 11: Configure Cisco SD-WAN Features for RA Traffic, on page 27

Configure SD-WAN RA

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

Important The configuration steps described here are presented as high-level tasks. For details about using Cisco vManage feature templates and CLI add-on templates, see the Cisco 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
Task 2	Configure a PKI trustpoint for certificate authentication This is optional if the RA headend uses an authentication method that does not require certificates.
Task 3	Configure IKEv2 profiles to group RA 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 RA clients, if applicable
Task 7	Configure AAA to specify a RADIUS server for RA user authentication, policy, and accounting
Task 8	Configure RA user credentials and policy on the RADIUS server
Task 9	(Optional) Configure RA traffic rate limiting
Task 10	Configure RA traffic symmetry, if applicable
Task 11	(Optional) Configure SD-WAN features for RA traffic

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 vManage, 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 RA headend is configured to use certificate authentication.

In Cisco vManage, 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 vManage, 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 vManage 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 vManage feature template to define the VRF.

Configure IPsec Ciphers, Parameters, and Template Interface

In Cisco vManage, 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 Virtual-Templatesdwan-ra_unnum_intf_num type tunnel
 vrf forwarding sdwan-ra_service_vpn
 ip address private_ipv4_addr subnet_mask
```

```
interface Virtual-Templatesdwan-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 Virtual-Template100 type tunnel
 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 vManage, 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 SD-WAN RA 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 SDRA headend bootflash and specify the path.

   Note You can copy the AnyConnect profile XML file to the Cisco SD-WAN RA headend bootflash from a host reachable in a service VPN, using the **secure copy** command on the Cisco SD-WAN RA 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 RA users connect to the headend by hardware RA client.

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

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

1. In Cisco vManage, 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 RA 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 RA service VPN, use a Cisco vManage OMP feature template to advertise the RA IP pool range as a summary-only route.

   If the SD-WAN RA IP pool summary is not advertised, OMP automatically advertises, for each RA 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 RA clients across the Cisco SD-WAN fabric.

Task 7: Configure AAA Parameters and RADIUS Server Parameters

In Cisco vManage, 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 RA 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 RA 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 RA 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 RA 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 RA user is assigned to
  - IP pool name: Name of the IP pool defined on the RA headend
  - Server subnets: Subnet access to provide to the RA 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 RA connections.

Table 4: Subset of the Parameters in a User Profile

Parameter	Description
Profile name	RA user identity. Example: user1@example.com
Cleartext-password := "*password***"**	RA user password specified by the RA user on the RA client. This is required for AnyConnect EAP authentication.
Tunnel-Password = *pre-shared-key-string*	Pre-shared-key string to use for the RA user. This is required for pre-shared key authentication.
cisco-avpair+="ip:interface-config=vrf forwarding *vrf-name***"**	VRF (service VPN) that the RA user 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 RA, 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-RA-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 RA headend uses to assign an IP address to the RA user.
cisco-avpair+="ipsec:route-set=prefix *prefix/prefix-length*"	IP prefixes to which the RA user requires access over the RA 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 RA user that is destined to a Cisco SD-WAN tunnel.

Table 5: Subset of the Parameters in a User Group Profile

Parameter	Description
Group profile name	Domain portion of the RA user identity. The group profile enables grouping of RA users based on the domain portion of the RA 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.

Parameter	Description
Cleartext-password := "*password***"**	For an authorization request from RA headend to the RADIUS server, the password is configured on the RA 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 RA users 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 RA, 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-RA-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 RA headend uses to assign IP addresses to this group of RA users.
cisco-avpair+="ipsec:route-set=prefix *prefix/prefix-length*"	IP prefixes to which the group of RA users require access over the RA VPN tunnel. You can configure this attribute multiple times to specify multiple prefixes.

Task 9: Configure RA Traffic Rate Limiting

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

Configure RA Traffic Rate Limiting

1. Rate limit RA upstream traffic (from the RA client).

Note The upstream traffic may be destined to Cisco 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 vManage, 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 RA traffic, irrespective of the traffic destination, RA 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 vManage, 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 RA clients and application types.

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

   Configure the following match conditions and action:

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

2. Using Cisco vManage, add an inbound QoS policer to the centralized policy to rate limit RA downstream (toward the RA 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) RA return traffic as close as possible to the traffic source (application server). When rate limiting unencrypted traffic, you can specify RA clients and application types.

   Configure the following match conditions and action:

- Match RA inner (within the IPsec tunnel) traffic. Specify the following:
    - RA user service VPN
    - For the destination IP, specify the IP address(es) assigned to the RA 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.

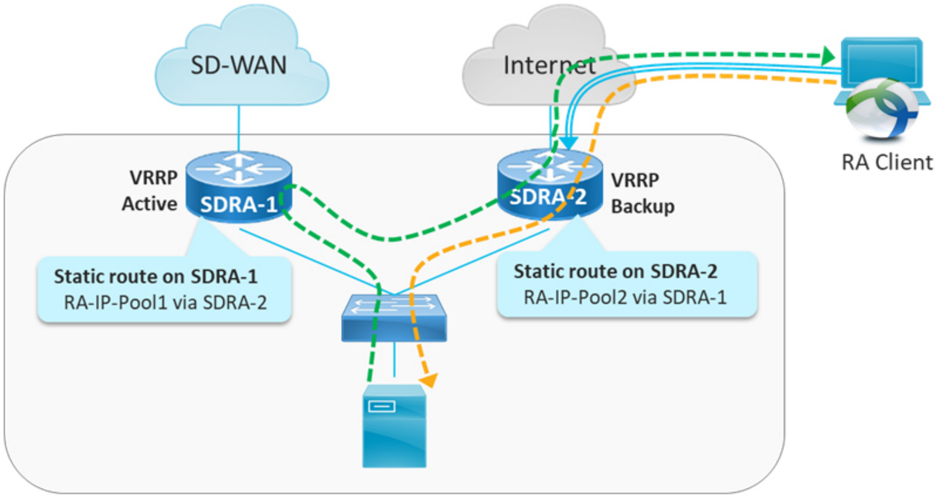
Task 10: Configure RA Traffic Symmetry

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

A. Configure RA Traffic Symmetry for Sites That Use VRRP

At a site with multiple Cisco IOS XE 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 RA 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 (RA IP pool) for assigning IP addresses to RA clients. RA 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 RA 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 RA client.

Example:

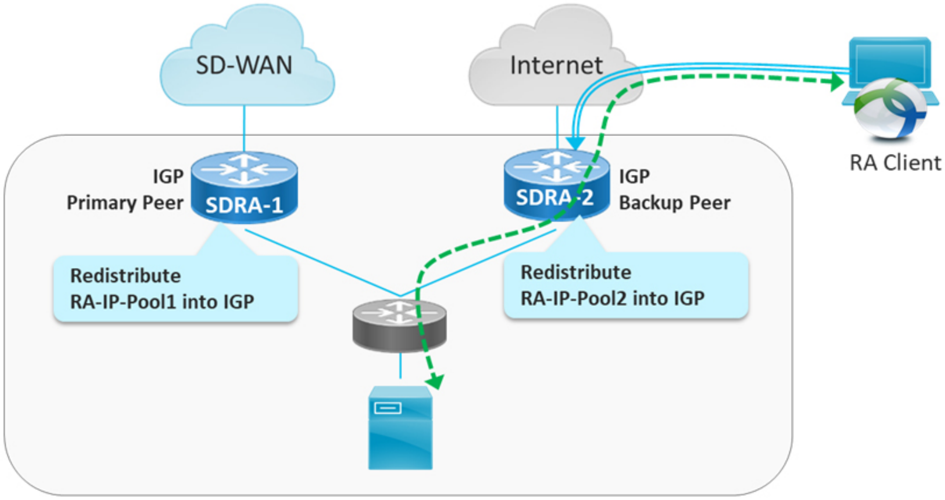
In the example shown in the figure, there are two SD-WAN RA headend devices (SDRA-1 and SDRA-2) at the same site. They are interconnected with a service VPN. Each has a unique local IP pool.

- 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 RA Traffic Symmetry for Sites That Use Routing Protocols

At a site with multiple Cisco IOS XE 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 RA 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 RA clients (RA IP pool). RA 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 RA IP pool into the service side routing protocol, so that the LAN-side router/L3 switch forwards any return traffic destined to RA clients to the correct device, based on the assigned IP address (return traffic destination IP).

Task 11: Configure Cisco SD-WAN Features for RA Traffic

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

- NAT-DIA
- UTD
- ZBF

Configure Cisco SD-WAN Features for RA Traffic

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

CHAPTER 5

Verify and Monitor SD-WAN Remote Access

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

Verification requires at least one remote user to be connected.

Client Connections

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

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
```

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
```

APPENDIX A

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 RA client

The following RA connection details apply to the example:

- RA client type: Cisco AnyConnect
- RA 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 vManage, 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 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 an RA 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.
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 Virtual-Template100 type tunnel
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 Virtual-Template100",
 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 RA Client Configuration

The AnyConnect client connects to an SD-WAN RA headend similarly to how it connects to any other RA 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
  ```