Cisco Catalyst SD-WAN Remote Access Configuration Guide, Releases 26.x and Later

Cisco SD-WAN
Updated September 28, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

Full Cisco Trademarks with Software License....ii

1 SD-WAN remote access features....5

SD-WAN remote access feature history....6

2 Information About SD-WAN Remote Access....7

Supported devices for Cisco Catalyst SD-WAN Remote Access....9
Prerequisites for Cisco Catalyst SD-WAN Remote Access....10
Restrictions for Cisco Catalyst SD-WAN Remote Access....13
Use cases for SD-WAN RA....13

3 Configure Cisco Catalyst SD-WAN Remote Access....15

Configure IKEv2 ciphers and parameters....16
Configure a PKI trustpoint for certificate enrollment....17
Configure an IKEv2 profile....17
Configure IPsec ciphers, parameters, and template interface....19
Configure AnyConnect profile download....21
Configure a unique local private IP pool on the SD-WAN RA headend....22
Configure AAA parameters and RADIUS server parameters....23
Configure the RADIUS server with user credentials and policy....24
Configure remote access traffic rate limiting....27
Configure remote access traffic symmetry....28
Cisco Catalyst SD-WAN features for remote access traffic....30
Requirements to configure Cisco Catalyst SD-WAN Remote Access....30
Configure Cisco Catalyst SD-WAN remote access using a configuration group....31
Add the SD-WAN remote access feature profile to an existing configuration group....35

4 Verify and Monitor Cisco Catalyst SD-WAN Remote Access....37

Verify and monitor SD-WAN remote access....38
Monitor Cisco Catalyst SD-WAN Remote Access devices....40

5 Troubleshoot Cisco Catalyst SD-WAN Remote Access....41

Support document links....42
Support articles....42
Submit feedback for a support document....42
Disclaimer and caution....43

6 Example Configuration for Cisco Catalyst SD-WAN Remote Access, RADIUS, and AnyConnect 45
Example configuration for SD-WAN remote access, RADIUS, and AnyConnect.....46

1 SD-WAN remote access features

Topics:

- SD-WAN remote access feature history

Describes the key capabilities and functionality available in the system, including configuration options, operational modes, and supported protocols that enable network administrators to effectively manage and monitor their infrastructure.

SD-WAN remote access feature history

Provides the feature history for Cisco Catalyst SD-WAN Remote Access capabilities and enhancements across software releases.

This reference documents the evolution of Cisco Catalyst SD-WAN Remote Access features, showing when specific capabilities were introduced and enhanced across different software releases. Remote access refers to enabling secure access to an organization's network from devices at remote locations.

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.
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 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.

2 Information About SD-WAN Remote Access

Topics:

- Supported devices for Cisco Catalyst SD-WAN Remote Access
- Prerequisites for Cisco Catalyst SD-WAN Remote Access
- Restrictions for Cisco Catalyst SD-WAN Remote Access
- Use cases for SD-WAN RA

Explains how Cisco Catalyst SD-WAN Remote Access integrates remote access functionality into the Cisco Catalyst SD-WAN fabric.

Cisco Catalyst SD-WAN Remote Access (SD-WAN RA) is a remote access solution that

- fully integrates remote access functionality into the Cisco Catalyst SD-WAN fabric
- extends the benefits of Cisco Catalyst SD-WAN to remote access users, and
- enables Cisco IOS XE Catalyst SD-WAN devices to provide remote access headend functionality, managed through Cisco SD-WAN Manager.

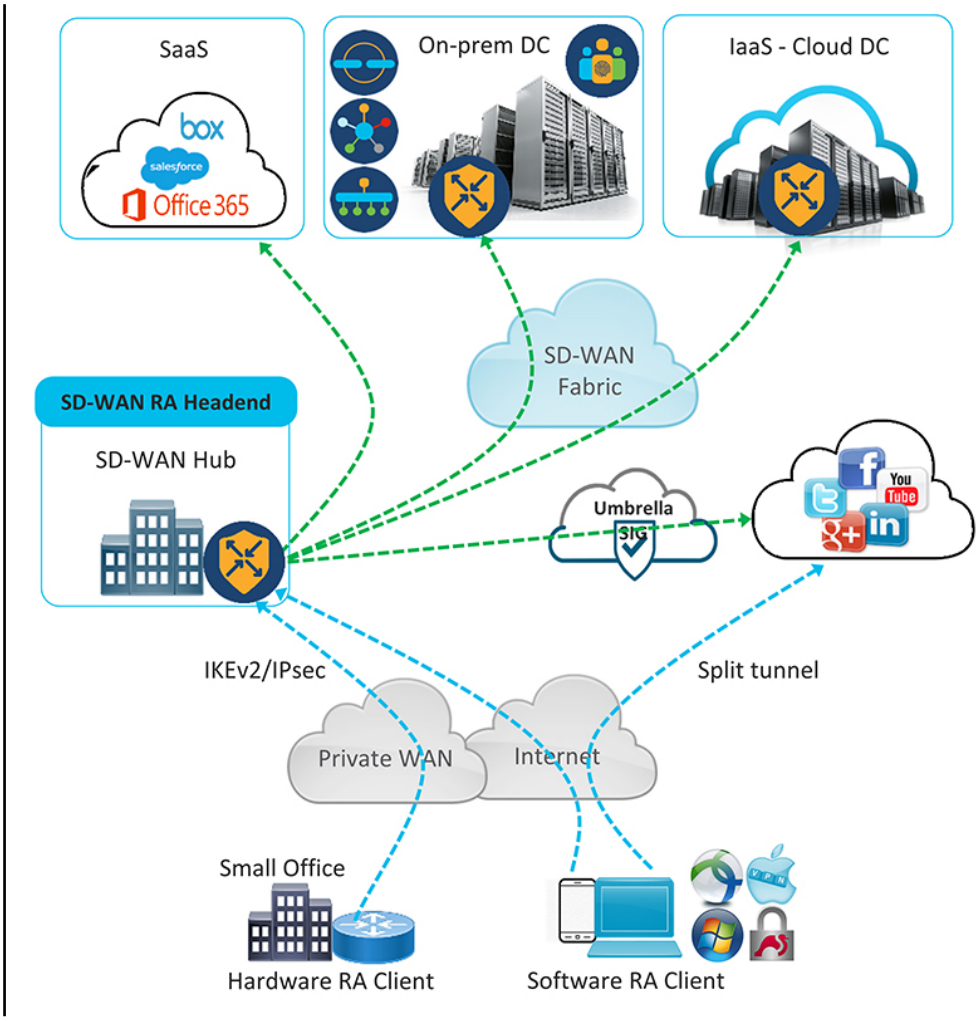
Deployment

An SD-WAN RA headend device may be deployed in these locations:

- 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


SaaS
box
salesforce
Office 365
On-prem DC
IaaS - Cloud DC
SD-WAN
Fabric
SD-WAN RA Headend
SD-WAN Hub
Umbrella
SIG
IKEv2/IPsec
Split tunnel
Private WAN
Internet
Small Office
Hardware RA Client
Software RA Client

Supported devices for Cisco Catalyst SD-WAN Remote Access

Lists the devices that support SD-WAN RA headend functionality with Cisco Catalyst SD-WAN in IPsec and SSL modes.

This reference identifies the specific devices that, operating with Cisco Catalyst SD-WAN, support SD-WAN RA headend functionality in both IPsec and SSL modes, along with their minimum supported release requirements.

IPsec mode support

These 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

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.x and Cisco Catalyst SD-WAN Manager Release 20.15.3

- C8475-G2
- C8455-G2
- C8550-G2
- C8570-G2
- C8375-E-G2

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and Cisco Catalyst SD-WAN Manager Release 20.18.1

- C8355-G2
- C8151-G2
- C8235-G2
- C8231-E-G2

SSL mode support

These 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

Lists the prerequisites required for implementing Cisco Catalyst SD-WAN Remote Access including network configuration, client setup, firewall policies, and server requirements.

This reference provides a comprehensive list of prerequisites that must be met before implementing Cisco Catalyst SD-WAN Remote Access. These prerequisites ensure proper headend reachability, client connectivity, security policies, and supporting infrastructure for successful remote access deployment.

Table 2: 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 these:

   - 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 these 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

Outlines key restrictions and limitations when configuring SD-WAN RA functionality for remote access headend devices.

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

Describes scenarios where Cisco IOS XE Catalyst SD-WAN devices can be configured as remote access headends in Cisco Catalyst SD-WAN networks.

Use cases for SD-WAN RA are scenarios that

- enable remote users to connect to a Cisco Catalyst SD-WAN network through Cisco IOS XE Catalyst SD-WAN devices configured as headends
- eliminate the need for separate devices outside of the Cisco Catalyst SD-WAN fabric to manage remote access headend tasks, and
- provide load distribution by employing multiple Cisco IOS XE Catalyst SD-WAN devices as remote access headends when scaling up to meet remote access demands.

3 Configure Cisco Catalyst SD-WAN Remote Access

Topics:

- Configure IKEv2 ciphers and parameters
- Configure a PKI trustpoint for certificate enrollment
- Configure an IKEv2 profile
- Configure IPsec ciphers, parameters, and template interface
- Configure AnyConnect profile download
- Configure a unique local private IP pool on the SD-WAN RA headend
- Configure AAA parameters and RADIUS server parameters
- Configure the RADIUS server with user credentials and policy
- Configure remote access traffic rate limiting
- Configure remote access traffic symmetry
- Cisco Catalyst SD-WAN features for remote access traffic
- Requirements to configure Cisco Catalyst SD-WAN Remote Access
- Configure Cisco Catalyst SD-WAN remote access using a configuration group
- Add the SD-WAN remote access feature profile to an existing configuration group

Describes how to configure system settings and parameters through the command-line interface or web-based management console to customize device behavior and functionality.

Configure IKEv2 ciphers and parameters

Configure IKEv2 proposals, policies, and parameters for an SD-WAN RA headend device using CLI add-on templates in Cisco SD-WAN Manager.

Configure the IKEv2 encryption settings required for an SD-WAN RA headend device to establish secure VPN connections.

When configuring a device to function as an SD-WAN RA headend, you can combine all the required configuration commands into a single CLI add-on template. Use the configuration commands in config-transaction mode.

Procedure

1. Configure an IKEv2 proposal.

   Example

   ```
   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.

   Example

   ```
   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.

   Example

   ```
   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
```

The IKEv2 encryption settings are configured for the SD-WAN RA headend device.

Configure a PKI trustpoint for certificate enrollment

Configure a PKI trustpoint that specifies a CA server for SCEP-based auto enrollment when the remote access headend uses certificate authentication.

This task configures a PKI trustpoint for certificate enrollment when the remote access headend is configured to use certificate authentication.

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.

Procedure

Configure the PKI trustpoint with the required parameters for certificate enrollment.

Example

```
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
```

The PKI trustpoint is configured with SCEP-based auto enrollment for certificate authentication.

Configure an IKEv2 profile

Configure an IKEv2 profile to enable grouping of peers by identity and specify authentication and authorization policy.

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

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

Procedure

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

      Example

      ```
      crypto ikev2 profile sdra_ikev2_profile
      ```

   b) Match peer identities and specify a local identity.

      Example

      ```
      match identity remote any id-type id-value
      identity local id-type id-value
      ```

   c) Specify authentication types and credentials.

      Example

      ```
      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.

      Example

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

   e) Specify group authorization parameters.

      Example

      ```
      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.

      Example

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

   g) Specify an IPsec virtual-template interface.

      Example

      ```
      virtual-template interface-number mode auto
      ```

Example

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.

Example

```
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 @
```

The IKEv2 profile is configured with authentication and authorization policy, and the name mangler is configured to extract the domain portion from peer identities.

Configure IPsec ciphers, parameters, and template interface

Configure IPsec ciphers, parameters, and virtual template interface for the SD-WAN RA headend device using a CLI add-on template in Cisco SD-WAN Manager.

This task configures the IPsec settings required for the SD-WAN RA headend device to establish secure tunnel connections.

Use this procedure to set up IPsec encryption settings, security parameters, and the virtual template interface that enables secure communication for remote access connections.

Before you begin

Define the VRF for the service VPN before beginning this procedure. You can use a Cisco SD-WAN Manager feature template to define the VRF.

Follow these steps to configure IPsec ciphers, parameters, and template interface:

Procedure

1. Configure IPsec ciphers.

   Example

   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.

   Example

   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.

   Example

   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
```

The IPsec ciphers, parameters, and virtual template interface are configured for the SD-WAN RA headend device.

Configure AnyConnect profile download

Configure AnyConnect profile download on the SD-WAN RA headend device using a CLI add-on template in Cisco SD-WAN Manager.

Configure AnyConnect profile download functionality on the Cisco Catalyst SD-WAN remote access headend device to enable client profile distribution.

In Cisco SD-WAN Manager, use a CLI add-on template for the SD-WAN RA headend device to configure the AnyConnect profile download functionality.

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.

Follow these steps to configure AnyConnect profile download:

Procedure

1. Disable HTTP secure server functionality.

   Example

   ```
   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.

   Example

   ```
   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.

   Example

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

> **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.

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

Example

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

The AnyConnect profile download is configured on the headend device. The following example shows the complete configuration:

```
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
```

Configure a unique local private IP pool on the SD-WAN RA headend

Configure each SD-WAN RA headend with a unique private IP pool to assign IP addresses to remote access clients.

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.

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

Procedure

---

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.

Example

```
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.

The SD-WAN RA headend is configured with a unique private IP pool for assigning IP addresses to remote access clients.

Configure AAA parameters and RADIUS server parameters

Configure AAA parameters and RADIUS server parameters using a CLI add-on template in Cisco SD-WAN Manager for the SD-WAN RA headend device.

This task configures AAA parameters and RADIUS server parameters to enable authentication, authorization, and accounting services for the SD-WAN RA headend device.

Use a CLI add-on template in Cisco SD-WAN Manager to configure both RADIUS server parameters and AAA method lists for your SD-WAN RA headend device.

Procedure

---

1. Configure RADIUS server parameters.

   Example

   ```
   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.

   Example

   ```
   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
   ```

The AAA parameters and RADIUS server parameters are configured with the specified settings. The following example shows the complete configuration:

```
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
```

Configure the RADIUS server with user credentials and policy

Provides parameters and configuration details for setting up a RADIUS server to support SD-WAN RA headend authentication and policy management.

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.

This task requires a working knowledge of RADIUS server configuration.

To support the SD-WAN RA headend, ensure that these 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 this subset of RADIUS parameters. These parameters are required, to enable SD-WAN RA to establish remote access connections.

Table 3: 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.
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 4: 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.
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.

Configure remote access traffic rate limiting

Configure quality of service (QoS) policers and shapers to limit the rate of aggregate upstream and downstream remote access traffic.

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

Remote access traffic rate limiting helps control bandwidth usage and ensure network performance by managing traffic flow between remote access clients and Cisco Catalyst SD-WAN sites.

Procedure

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.

   - 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.

   - 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.

Remote access traffic is rate limited according to the configured QoS policers, controlling bandwidth usage for both upstream and downstream traffic flows.

Configure remote access traffic symmetry

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 to ensure return traffic is correctly routed to remote access clients.

This task ensures 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.

At Cisco Catalyst SD-WAN sites with multiple Cisco IOS XE Catalyst SD-WAN devices acting as SD-WAN RA headends, traffic symmetry configuration is required to prevent routing issues.

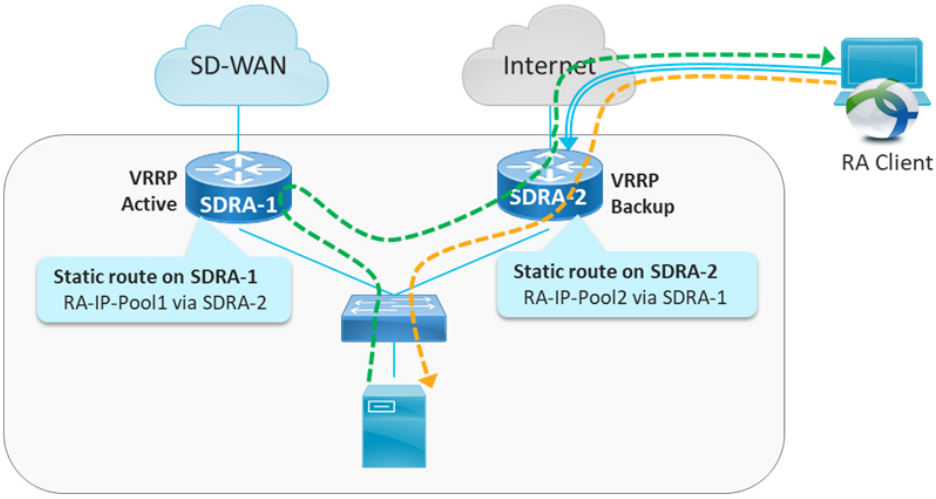
Procedure

---

1. Choose the appropriate configuration method based on your site configuration.
   - For sites that use VRRP, follow procedure A below.
   - For sites that use routing protocols such as OSPF or EIGRP, follow procedure B below.
2. 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 return traffic reachability.

   Figure 2: Site with Service-Side VRRP



a. 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.

b. 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:

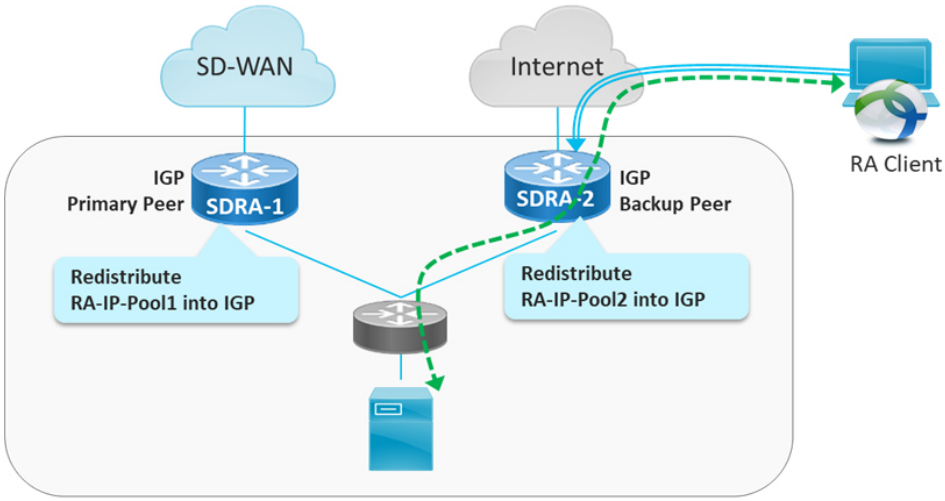
In the example shown in the figure, there are two SD-WAN RA headend devices (SDRA-1 and SDRA-2) at the same site. They are interconnected with a service VPN. Each has a unique local IP pool.

- 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

3. 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 return traffic reachability.

Figure 3: Site with Service-Side routing protocol



a. 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.

b. 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).

Remote access traffic symmetry is configured, ensuring that return traffic is correctly routed to remote access clients at sites with multiple SD-WAN RA headends.

Cisco Catalyst SD-WAN features for remote access traffic

Explains how Cisco Catalyst SD-WAN features apply to remote access traffic after the headend establishes connections with remote access users.

Cisco Catalyst SD-WAN features for remote access traffic are security and networking capabilities that

- apply to remote access traffic after it is decrypted and becomes inbound traffic on the assigned service VPN
- are configured for the service VPN where the SD-WAN RA headend places remote access users based on their identity, and
- include NAT-DIA, UTD, and ZBF capabilities.

Configuration requirements

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. 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.

Requirements to configure Cisco Catalyst SD-WAN Remote Access

Lists the prerequisites required to configure SD-WAN Remote Access using vManage.

This reference provides the prerequisites and requirements for configuring Cisco Catalyst SD-WAN Remote Access using Cisco SD-WAN Manager.

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

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

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

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

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

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

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

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

Configure Cisco Catalyst SD-WAN remote access using a configuration group

Configure Cisco SD-WAN remote access using the remote access feature in a configuration group.

Configure remote access capabilities for Cisco SD-WAN using configuration groups to enable secure connectivity for remote users.

Remote access configuration allows users to securely connect to the SD-WAN network from remote locations. This task uses configuration groups to deploy the Remote Access feature across multiple devices.

Before you begin

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

Follow these steps to configure Cisco Catalyst SD-WAN Remote Access using a configuration group:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Create and configure a remote access feature in a system profile.
   a. Configure remote access.

Table 5: Remote Access Settings

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

b. Configure authentication.

Table 6: Authentication

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

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

c. Configure AAA policy.

Table 7: AAA Policy

Field	Description
Specify Name	Choose this option to specify the name of the policy to look up on the RADIUS server. In the **Policy Name** field, which appears only for the **Specify Name** option, enter the name of the policy.

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

d. Configure private IP-Pool.

Table 8: Private IP-Pool

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

e. Configure IKEv2 and IPsec settings.

Table 9: IKEv2 and IPsec settings

Field	Description
Local IKE Identity Type	Enter the local IKEv2 identity type. The options are: • IPv4 Address or IPv6 Address • Email • FQDN • Key-ID

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

The Remote Access feature is configured in the System Profile. Remote users can now securely connect to the SD-WAN network using the configured authentication and security settings.

What to do next

Also see Deploy a configuration group.

Add the SD-WAN remote access feature profile to an existing configuration group

Configure the SD-WAN Remote Access feature profile for an existing configuration group to enable remote access functionality.

This task enables SD-WAN Remote Access functionality by adding the remote access feature profile to an existing configuration group and configuring the necessary VPN settings.

Use this procedure when you need to add remote access capabilities to an existing SD-WAN configuration group. This allows devices in the group to support remote access connections.

Procedure

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. Choose 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**.

The SD-WAN Remote Access feature profile is successfully added to the configuration group, enabling remote access functionality for devices assigned to this group.

What to do next

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

4 Verify and Monitor Cisco Catalyst SD-WAN Remote Access

Topics:

- Verify and monitor SD-WAN remote access
- Monitor Cisco Catalyst SD-WAN Remote Access devices

Describes the process of checking system configurations and continuously observing network performance to ensure proper functionality and identify potential issues before they impact operations.

Verify and monitor SD-WAN remote access

Provides commands and methods to verify that the remote access headend is configured and functioning properly on the Cisco IOS XE Catalyst SD-WAN device hosting the SD-WAN RA headend.

On the Cisco IOS XE Catalyst SD-WAN device hosting the SD-WAN RA headend, use the commands and methods described in this reference 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 this 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

Provides information about monitoring devices in the overlay operating as remote access headends using Cisco SD-WAN Manager dashboards and session details.

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 these 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, these 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.

5 Troubleshoot Cisco Catalyst SD-WAN Remote Access

Topics:

- Support document links
- Support articles
- Submit feedback for a support document
- Disclaimer and caution

Describes common issues and resolution steps for remote access connectivity problems, including VPN connection failures, authentication errors, and network configuration troubleshooting procedures.

Support document links

Explains links to Cisco-authored support documents that help resolve technical issues without requiring a support ticket.

A support document link is a resource that

- provides access to documents authored by Cisco subject matter experts
- helps resolve technical issues without requiring a support ticket, and
- offers guidance about the data to collect and add to a support ticket if escalation is needed.

Community and support escalation information

This section describes additional resources for resolving technical issues and guidance for support escalation.

- If the documents do not resolve your issue, visit the applicable Cisco Community for information and advice from fellow Cisco customers.
- If you cannot find a resolution on the Community, raise a support ticket at Cisco Support.
- When raising a support ticket, specify the support document you referred to so TAC can create an improvement request with the document owner.

Support articles

Lists support articles associated with this technology.

The 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.

Submit feedback for a support document

Configure feedback submission for Cisco support documents. Use the Feedback button to notify document owners and provide detailed information about any issues or improvements needed.

Procedure

1. 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.

2. Include information regarding the section, area, or issue you had with the document and what could be improved.

   Provide as much detail as possible to help the document owner understand and address your feedback.

After submitting feedback, the document owner will review your input and may update the article or flag it for removal based on your suggestions.

Disclaimer and caution

Outlines that the information in this document is based on devices in a specific lab environment and advises you to understand the potential impact of any command before applying it to a live network.

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.

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

Topics:

- Example configuration for SD-WAN remote access, RADIUS, and AnyConnect

Describes how to configure RADIUS authentication and AnyConnect VPN client integration, providing step-by-step configuration examples for establishing secure remote access connectivity with centralized user authentication.

Example configuration for SD-WAN remote access, RADIUS, and AnyConnect

Provides configuration examples for SD-WAN Remote Access HEADEND device, RADIUS SERVER, and AnyConnect remote access client with AnyConnect-EAP user authentication and SCEP-based certificate enrollment.

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 10: 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

Variable	Description
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.
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
```