Cisco SD-WAN Remote Access

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.

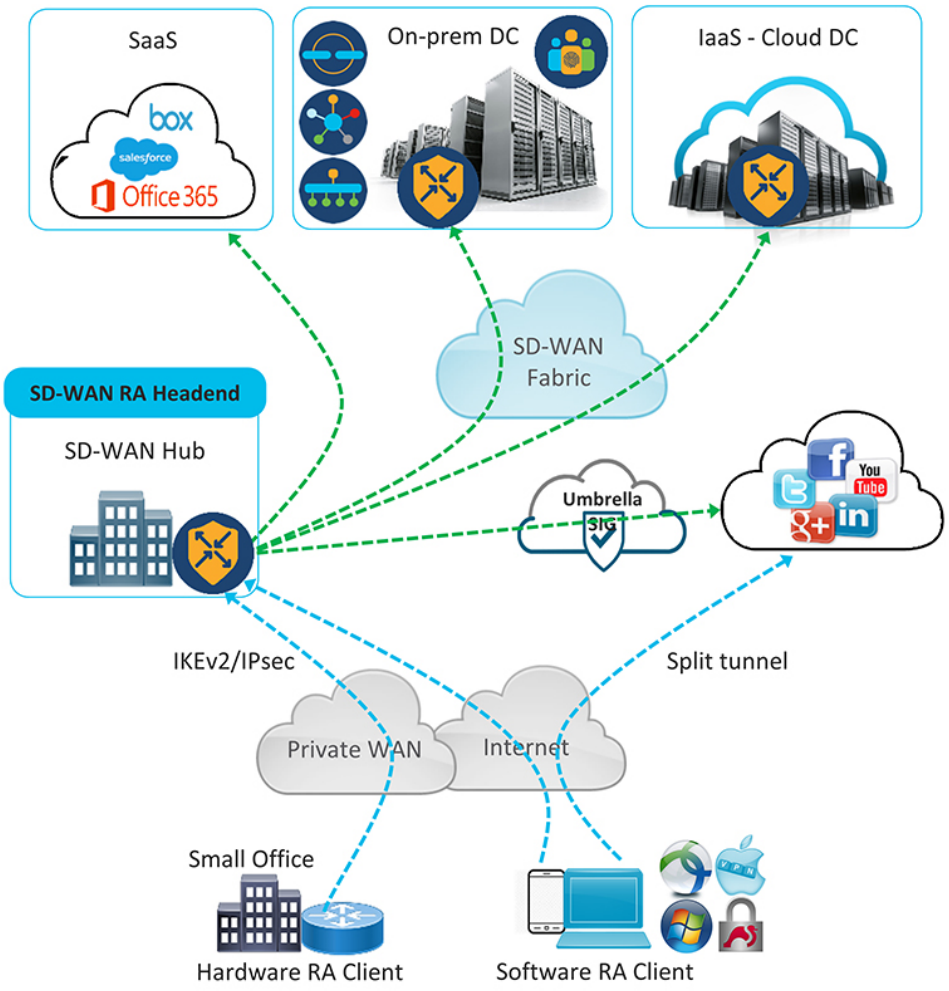
Deployment

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 1: 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.