Cisco Catalyst SD-WAN Remote Access

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

Information About Cisco Catalyst SD-WAN Remote Access

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

Deployment

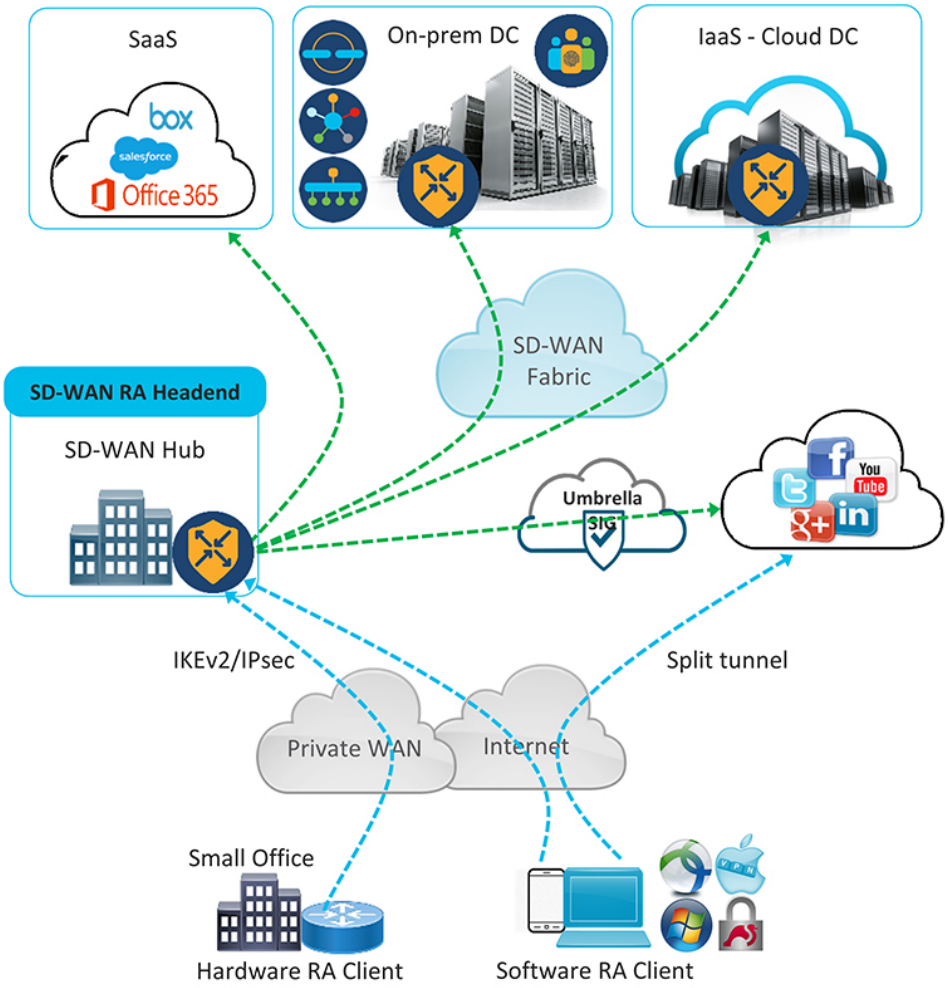
As shown in the following figure, an SD-WAN RA headend device may be deployed as follows:

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

SD-WAN RA enables remote access users to access applications hosted on-premises, applications hosted in IaaS, SaaS applications, or the internet. The connectivity between remote access clients and the SD-WAN

RA headend is commonly through the internet. For small office hardware remote access clients, the connectivity may be through a private WAN.

Figure 1: Cisco Catalyst SD-WAN Remote Access Architecture



Benefits of Cisco Catalyst SD-WAN Remote Access

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

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

Supported Devices for Cisco Catalyst SD-WAN Remote Access

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

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

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

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

- Cisco Catalyst 8000V Edge Software

Prerequisites for Cisco Catalyst SD-WAN Remote Access

Table 1: Summary of Prerequisites

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

Prerequisite Details

1. Public IP address

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

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

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

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

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

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

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

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

     - Static public IP on a non-TLOC interface

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

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

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

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

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

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

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

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

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

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

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

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

5. Summary-route configuration

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

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

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

6. Capacity planning for the SD-WAN RA headend

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

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

7. CA server

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

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

8. RADIUS/EAP server

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

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

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

Restrictions for Cisco Catalyst SD-WAN Remote Access

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

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

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

Use Cases for SD-WAN RA

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