White paper
Cisco public

The bridge to possible

Cisco Catalyst SD-WAN Remote Access (SD-WAN RA)

Contents

Redefine the remote-access network with Catalyst SD-WAN Remote Access.

Background

Remote work has been around for many years, but it has gathered momentum in recent years, driven largely by the pandemic. COVID-19 has introduced a host of changes, including a dramatic shift from office-based work to a work-from-home or work-from-anywhere environment. These changes have placed an onus on existing enterprise infrastructure.

Enterprises are realizing that legacy VPN network architectures and security stacks are inadequate and overly restrictive for the new work-from-anywhere era.

In addition, as digital enterprises move from having workforces that are hybrid by circumstance to ones that are hybrid by design, we will see the evolution of both physical and digital workspaces moving to cloud-based services for better worker experience and business resiliency.

Due to these trends, a greater number of employees now expects to work from home or anywhere. The distribution of the workforce has led to a new hybrid work era, which is reducing the office footprint. Enterprises are planning to rearchitect, build, and manage VPN infrastructure that leverages the internet.

As a result, enterprises are evolving toward a unified networking and security service that increases scalability, agility, and security in a user and application environment that is now highly distributed and mobile across the internet.

Introduction

This white paper discusses why traditional VPN approaches no longer work in the rapidly changing hybrid work environment. We describe the requirements that enterprises need to consider as they shift from their legacy architectures toward the work from-anywhere era. We propose the Cisco® SD-WAN Remote Access for enterprises to provide employees with a better work-from-anywhere environment that can satisfy all requirements.

Traditional VPN architecture and challenges

Traditionally, networks were designed with centralized architectures, with all traffic routed through the corporate data center over Multiprotocol Label Switching (MPLS) or VPN.

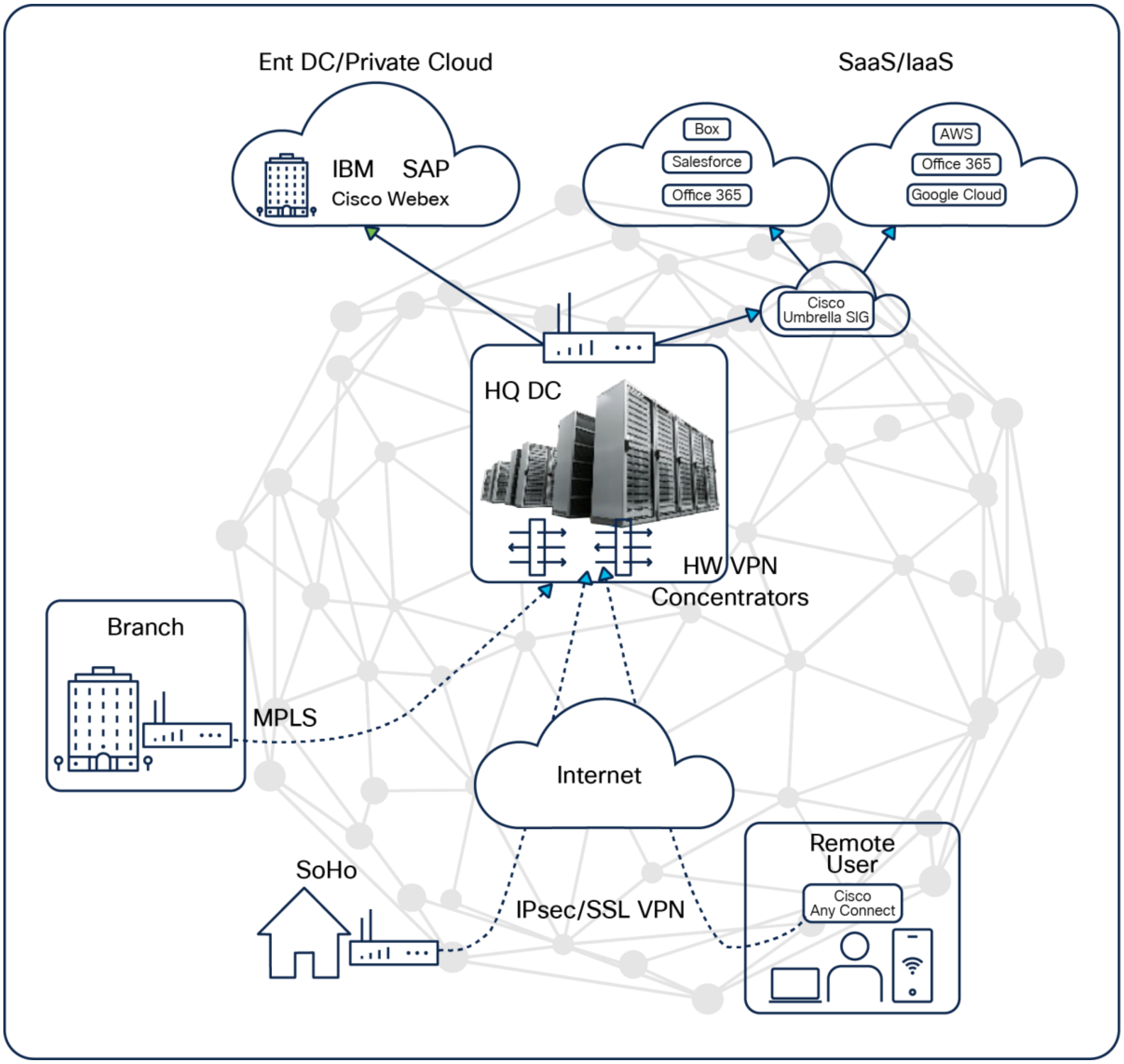


Figure 1.
Traditional VPN topology

In the legacy VPN network topology, remote users relied on VPN agents based on IP Security (IPsec) or Secure Sockets Layer (SSL) on each endpoint (that is, mobile phone or laptop) to connect over the internet back to VPN concentrator devices located at corporate headquarters. VPN concentrators were one of multiple network security appliances, such as firewalls, intrusion prevention systems (IPS), email gateways, and secure web gateway (SWG) appliances, composing the enterprise security stack.

Traditional remote access required multiple VPN concentrators in the enterprise data center/HQ location (hub-and-spoke topology) when the number of remote users increased or decreased. A remote-access client would connect from the internet to a pair of VPN concentrators positioned in the data center/HQ. All network security enforcement took place within the centralized security stack as traffic traversed the boundary between remote user, the enterprise network, and the internet.

Traditional remote-access solutions have been reliable in most use cases and have worked well for many decades for these reasons:

- The amount of bandwidth per user was low due to the lower requirements of legacy applications.
- The number of applications accessed was limited.
- The number of remote users remained low.
- VPN users were considered internal. All internal network traffic was assumed to be safe by perimeter security policies.
- The costs of MPLS/internet catering to remote-access clients were controlled.

But with highly distributed workforces and more applications moving to the cloud, this traditional VPN design has proven to be inefficient, as more users require remote access and resources have become split between the internal enterprise and the cloud.

With traditional remote access designs, like the one illustrated in Figure 1, traffic backhaul through the enterprise data center is one of many factors that may be causing remote users' poor application experience. The traditional VPN model of deploying VPN concentrators at the enterprise data center is no longer efficient for a number of reasons and has limitations related to cost, application experience, and security problems:

- **Poor application experience:** Backhauling of remote-access client traffic through the corporate HQ leads to poor application experience over the internet for remote users.
- **Capacity challenges:** A VPN concentrator is a separate piece of hardware, and with the increasing number of remote users, the enterprise needs to add more VPN hardware at the data center.
- **Operational complexity:** The traditional remote-access network is independent, and all the policies, configuration, management, and monitoring must be done separately, which increases the operational complexity and cost.
- **Security blind spots:** Remote users access software-as-a-service (SaaS) applications via the internet without going through the security stack at the data center/HQ, which creates enormous security blind spots. Enforcing corporate security is impossible in such scenarios.

Network readiness for hybrid work

As we step into a new realm of work, enterprises and organizations are scrambling to adapt to the new hybrid work culture. A company's workforce is no longer confined to the designated workplace, such as branches or the campus. Rather, its workers are increasingly spread across geography and multiple types of locations, such as homes, hotels and resorts, cafes, and public hotspots.

Similarly, applications are no longer centralized. We have already seen them deployed in public and private clouds along with the traditional on-premises data center. This evolution throws various challenges to CIOs and CTOs, with top-of-mind concerns being:

- **Network security:** Consistent security policy for the network and users.
- **Network simplicity:** A simplified global network infrastructure that is easy to operate.
- **Network agility:** Scalability, flexibility, and automation.
- **User-to-application experience:** Optimized for SaaS, infrastructure-as-a- service (IaaS), and on-premises applications.
- **Total cost of ownership (TCO):** Cost-effectiveness.

The Catalyst SD-WAN Remote Access (SD-WAN RA) is the stepping-stone to the emerging hybrid work environment to meet all goals.

Catalyst SD-WAN evolution for hybrid work

Over the last few years, Cisco's SD-WAN solution has evolved from a simple, secure site-to-site software-defined WAN infrastructure to incorporating secure access service edge (SASE), multicloud interconnects, the middle mile, and multiregion fabrics catering to use cases such as

- Site to site
- Site to cloud
- Cloud to cloud

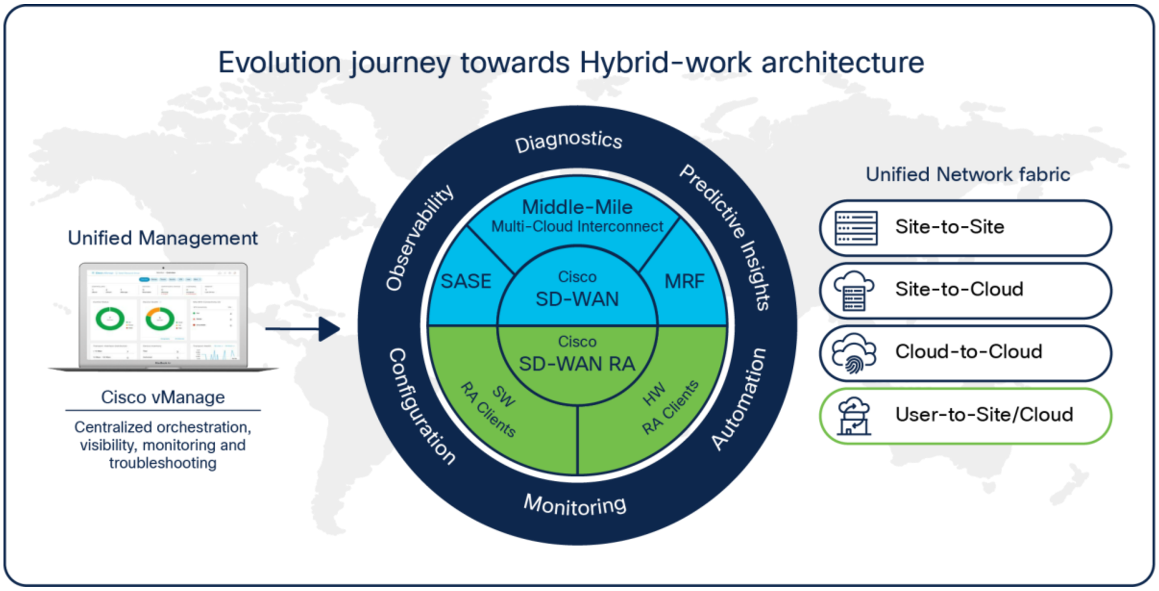


Figure 2.
SD-WAN evolution for remote access

As a part of the latest SD-WAN innovation, we have now integrated remote-access capability as well as catering to the missing use cases:

- User to site
- User to cloud

which will result in a truly unified network fabric for all hybrid work scenarios.

As such, providing remote-access users secure, easy, and seamless access to all applications (SaaS, IaaS, on-premises), as well as consistent and always-on internet availability, is the basis of the Catalyst SD-WAN RA.

The addresses all the top concerns of the hybrid work environment.

Catalyst SD-WAN RA architecture

The goal of the Catalyst SD-WAN RA is to reduce those long-haul remote-access VPN connections terminating on a pair of dedicated centralized firewalls. Instead, it onboards remote users to the nearest SD-WAN edge router. This significantly improves the last mile connectivity and delivers enterprise-grade SD-WAN fabric benefits to the remote user. The application experience is highly optimized for the remote user.

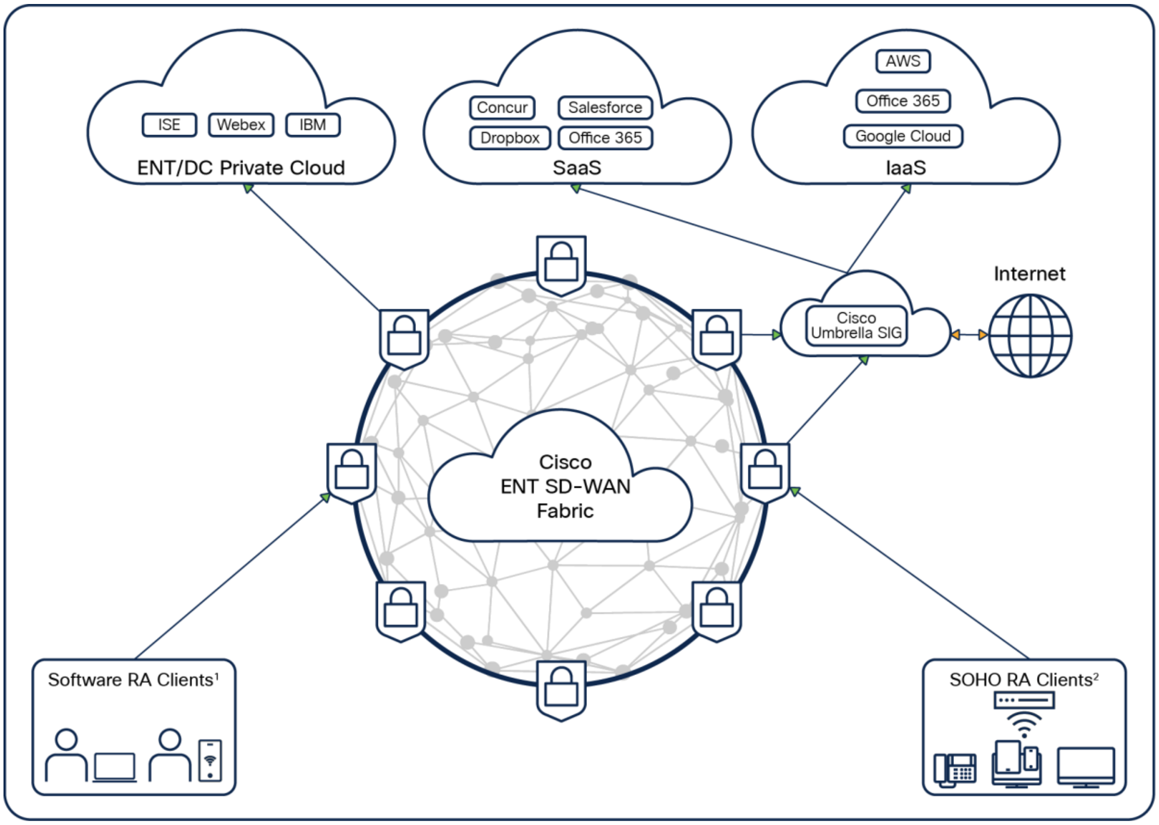


Figure 3.
SD-WAN RA architecture

Catalyst SD-WAN RA is built simply by repurposing your existing SD-WAN edge routers to terminate both software-based and hardware-based remote-access clients using the Internet Key Exchange (IKE) v2 protocol, making this a highly scalable and distributed architecture.

You no longer need to factor in dedicated hardware VPN concentrators and separate management consoles for remote access, as Catalyst SD-WAN becomes a single unified networking architecture for SD-WAN as well as a remote-access network.

With this unified console, you can centrally configure, monitor, automate, and have visibility across the entire unified fabric using Cisco Catalyst SD-WAN Manager and Cisco Catalyst SD-WAN Analytics.

Catalyst SD-WAN RA also seamlessly integrates with your existing security architecture, such as RADIUS, Cisco Identity Services Engine (ISE), and SASE.

On the endpoint side, nothing really changes, as organizations can continue to use their existing software-based clients such as Cisco AnyConnect®, which work seamlessly with SD-WAN RA. Third-party native OS-based VPN clients can also be supported.

Catalyst SD-WAN RA can also integrate with hardware-based remote-access clients such as classic Cisco IOS® or Cisco IOS XE (which support IKEv2-based FlexVPN).

Catalyst SD-WAN RA functional overview

Catalyst SD-WAN RA integrates FlexVPN (IKEv2/IPsec) remote-access architecture capability onto a Cisco IOS XE SD-WAN controller-mode stack.

This enables Catalyst SD-WAN devices to function as VPN concentrators to support remote-access headend functionality with:

- **Tunnel support**: IKEv2-based IPsec tunnel connectivity between the SD-WAN edge device and remote-access client users.
- **VPN client support**:
    - Software clients: Cisco AnyConnect, Cisco FlexVPN, native OS-based clients.
    - Hardware clients: Cisco IOS and Cisco IOS XE based routers as hardware clients for small offices and home offices.
- **VPN client authentication**:
    - Certificate-based authentication (for software AnyConnect clients).
    - EAP-based authentication (for software AnyConnect clients).
    - Pre-shared key (PSK) authentication (for hardware clients).

With Catalyst SD-WAN RA, you can convert any of your SD-WAN-enabled branch or data center routers into an SD-WAN RA headend or provision a new SD-WAN RA headend into the SD-WAN infrastructure.

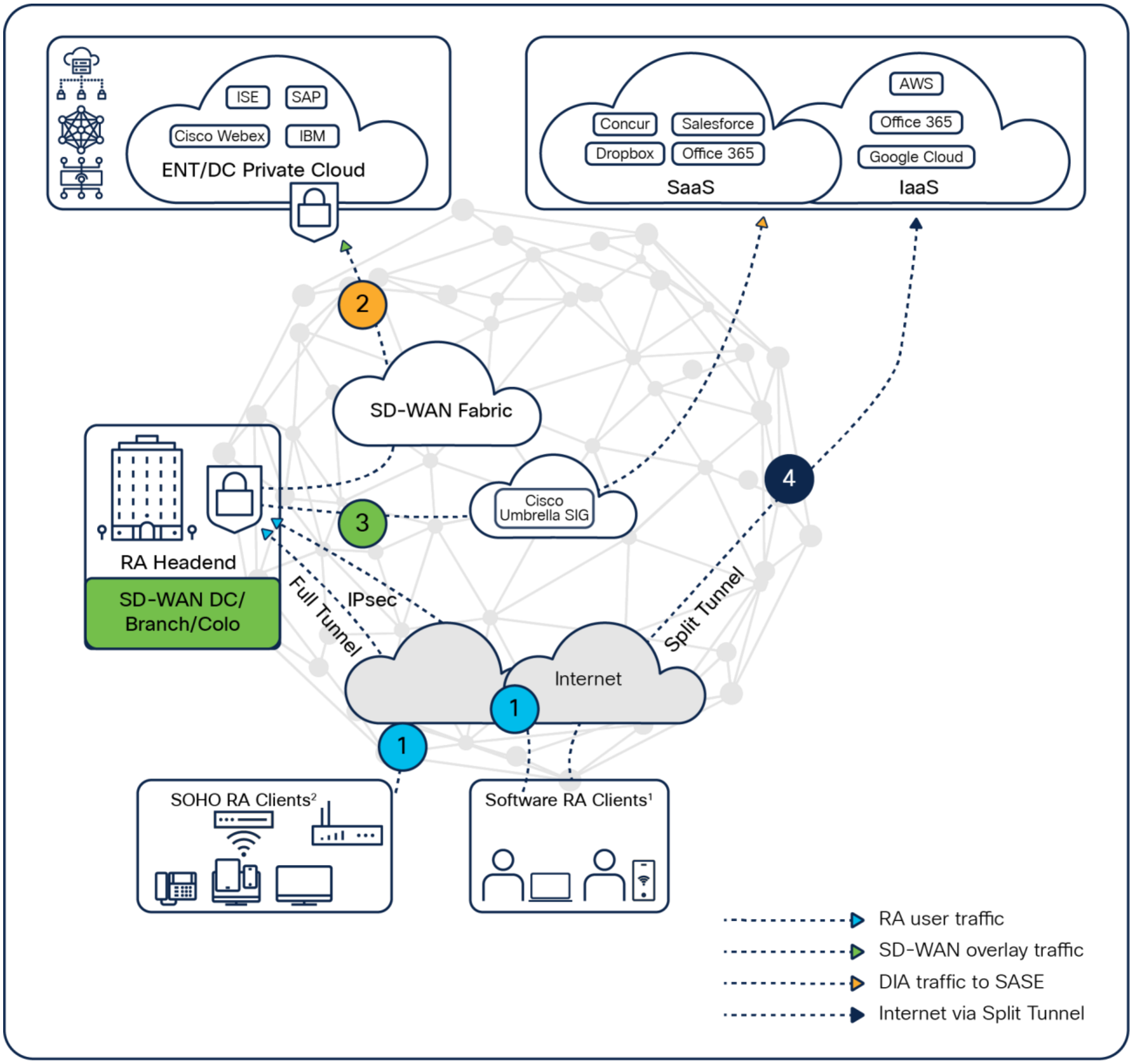


Figure 4.
SD-WAN RA functionality

Once an SD-WAN edge device is ready for the SD-WAN RA headend, the remote-access client can initiate an IPsec tunnel request using IKEv2 to the public IP of the SD-WAN RA headend.

The endpoints can be software-based AnyConnect remote-access clients or hardware-based remote-access clients. Endpoints that are able to initiate an IPsec tunnel or SSL VPN tunnel can connect to the SD-WAN RA headend. However, the remote-access client will be terminated within the SD-WAN fabric onto the SD-WAN RA headend device nearest to its location, spreading bandwidth demand and reducing the logical distance to reach enterprise or SaaS applications.

The SD-WAN RA headend can use a RADIUS, EAP, or Cisco ISE server for authentication of remote-access clients and for managing per-user or group-based authorization policy and can be located anywhere in the SD-WAN fabric if it's reachable from all SD-WAN RA headends in a service VPN.Once authenticated and authorized, an SD-WAN RA headend establishes an IPsec tunnel between SD-WAN RA and the remote-access client.

The remote-access client becomes part of the service VPN on the SD-WAN edge device, and all remote-access traffic will be treated as service-side LAN traffic on the SD-WAN edge device.

For each remote-access client, the SD-WAN RA headend assigns an IP address. The SD-WAN RA headend device automatically adds a host route for this remote-access client IP (via a VPN tunnel toward the remote-access client connection) in the service VPN in which the remote-access user is placed. This static route is automatically advertised by Overlay Management Protocol (OMP) to other SD-WAN sites to make sure that return traffic goes efficiently to the remote-access client.

Remote-access client establishment can be either a full-tunnel or split-tunnel mechanism based on the AnyConnect client's capacity.

Full tunnel

The remote-access client accesses the enterprise network as well as the internet through the SD-WAN RA headend.

If enterprise policy is to aggregate everything to the company network, the authorization policy pushes the default route via the SD-WAN RA headend to the AnyConnect client. All remote-access user traffic comes directly to the SD-WAN RA headend and is then re-encrypted back to the data center or sent to the internet.

In this full tunnel, the remote-access client

- Establishes an IPsec tunnel to the SD-WAN RA headend in either in the data center, a branch, or a colocation facility.
- Accesses on-premises enterprise IT via the SD-WAN RA headend.
- Accesses the internet through the SD-WAN RA headend via a corporate direct internet access (DIA) breakout at SD-WAN RA.
- Accesses cloud SaaS applications via Cisco Umbrella® Secure Internet Gateway (SIG) securely from the SD-WAN RA headend.
- Leverages enterprise SD-WAN features to the remote-access client traffic, such as application-aware routing, AppQoE, security stack, etc.

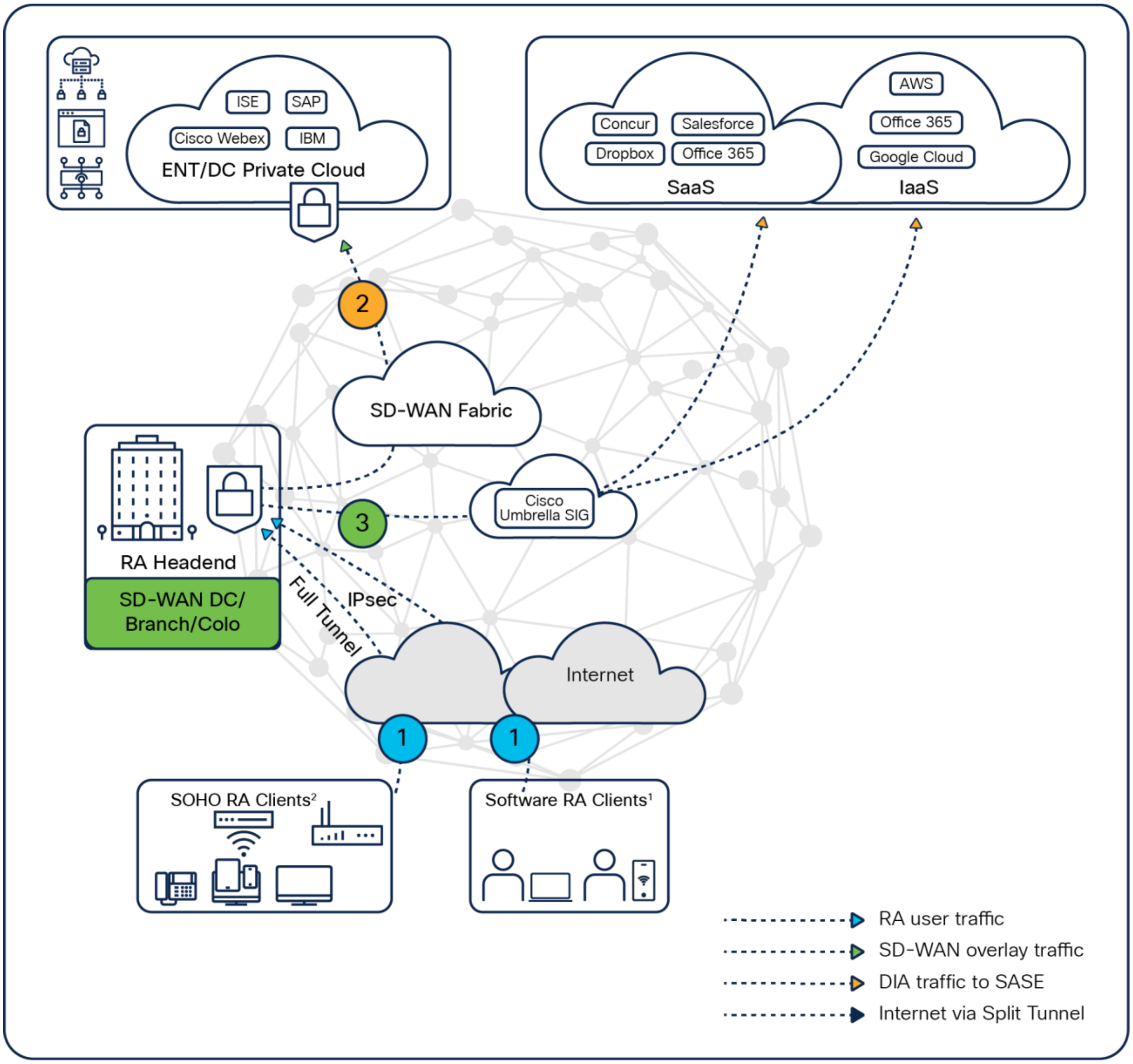


Figure 5.
AnyConnect – full tunnel

Split tunnel

If the enterprise doesn't want the remote-access client to come to its SD-WAN RA device for the internet-bound traffic, it can use split tunneling. In this approach, the remote-access client goes to SD-WAN RA only for enterprise applications, and internet breakout can happen directly from the remote-access client, which is from the client endpoint itself using a split tunnel. The policy can push a prefix-based or domain-based split tunnel to the AnyConnect client and the traffic will be split based on the policy. A split tunnel effectively reduces the amount of traffic coming to the SD-WAN RA headend.

In the split tunnel, the remote-access client can

- Access on-premises enterprise IT only via the SD-WAN RA headend.
- Access internet or cloud-based SaaS applications directly from their local internet access.

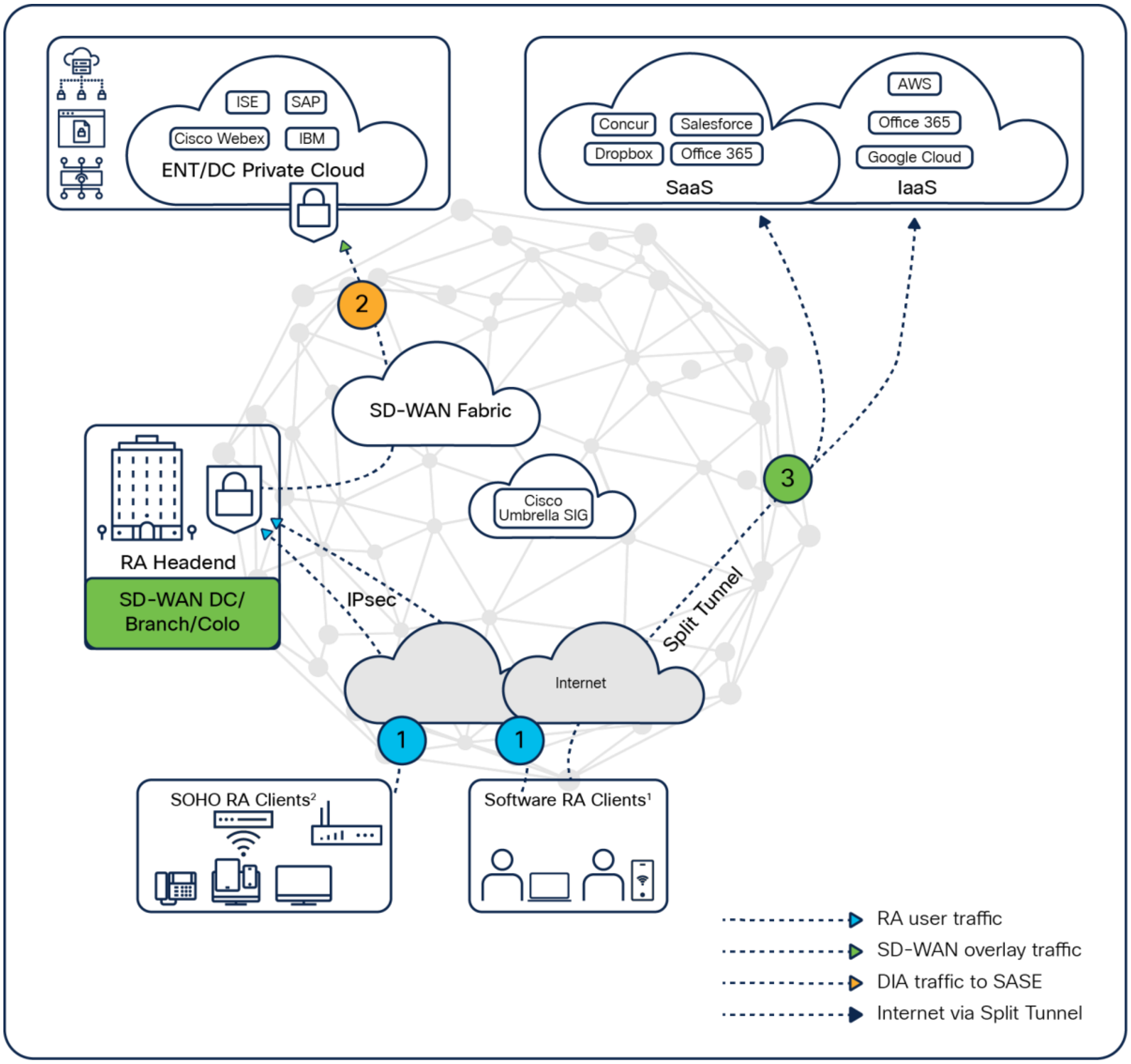


Figure 6.
AnyConnect – split tunnel

Catalyst SD-WAN RA advantage

Catalyst SD-WAN RA brings the ability to onboard remote-access VPN users directly onto Catalyst SD-WAN edge devices. The benefits of such integration are multifold:

- **Consistent and optimized application experience:** Remote users can be onboarded to the nearest Catalyst SD-WAN edge device, which drastically cuts down the last-mile distance, thereby extending all the benefits of Catalyst SD-WAN has to offer.
- **Unified security policy:** Network access and internet access policies can be streamlined to users based on their identity regardless of whether they are on-premises or remote.
- **Lower TCO:** No extra cost for VPN hardware for horizontal scaling. Simply reuse the existing SD-WAN infrastructure or factor in the remote access traffic when designing SD-WAN fabric for the future.
- **Flexibility, elasticity, and resiliency:** Remote users can be onboarded onto any Catalyst SD-WAN RA qualified branch, data center, cloud, or colocation. This allows for a distributed framework with no single point of failure.

- **Simplified operations:** The entire Catalyst SD-WAN RA can be centrally deployed, configured, and monitored using SD-WAN Manager, eliminating the need for multiple management consoles.
- **Ability to extend SD-WAN features to remote users:** With FlexVPN support on SD-WAN, you can extend the SD-WAN features (application-aware-routing, AppQoE, security policies) to remote-access clients, which is not possible today.
- **Keeping remote-access traffic within the enterprise network:** Remote-access traffic remains completely secure from end to end, as it doesn't leave the enterprise network. This is important for data-sensitive customers, including defense and financial customers, to secure end-to-end traffic from remote-access clients.

Use cases

- Connecting the hybrid workforce to an SD-WAN network.
- Extending a secure enterprise network to remote users, including home offices.
- Accessing enterprise IT and cloud-based applications with a consistent application experience.
- Providing unified network and security policies for the hybrid work era.
- Scaling up remote-access demands: Just distribute the load by employing one or more Cisco IOS XE SD-WAN devices as SD-WAN RA headends.

Design and deployment considerations

These design considerations provide guidance for implementing the SD-WAN RA.

This white paper does not provide a step-by-step configuration guide. Refer to the online Configuration Guide for configuration-related details.

SD-WAN RA edge platform

On the platform side, Cisco offers a portfolio from which you can choose the right platform for your needs. Catalyst SD-WAN RA headend functionality is supported on the Cisco Catalyst™ 8000 Edge Platforms Family, which includes branch, aggregation, and virtual routers. The table below lists the platforms supported as Catalyst SD-WAN RA headends.

Table 1. Catalyst SD-WAN RA qualified headend routers

Branch platforms	Aggregation platforms	Cloud platform
C8300-2N2S-4T2X	C8500-12X4QC	C8000V (On-Prem)
C8300-1N1S-6T	C8500-12X	
	C8500L-8S4X	
	ASR1002-HX	

C8000V (Cloud)* - In the Roadmap

Capacity planning for SD-WAN RA

The remote-access client traffic contends for the crypto engine and bandwidth resources of the SD-WAN edge platform. The SD-WAN RA headend thus shares the crypto engine, WAN bandwidth, and throughput capacity with the SD-WAN IPsec.

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

Additional capacity might be needed based on the number of remote-access connections and remote-access throughput that the Cisco IOS XE SD-WAN device is expected to support.

Things to keep in mind when selecting SD-WAN RA headend platforms:

- Platform crypto throughput capacity.
- WAN link bandwidth or throughput.
- IPsec tunnel scale to handle SD-WAN RA IPsec and SD-WAN IPsec tunnels.

SD-WAN RA scaling guideline:

SD-WAN IPsec security associations (SAs) + RA IKEv2/IPsec SAs must not exceed the platform's IPsec SA limit

Table 2. Catalyst SD-WAN IPsec plus RA IPsec scale

Platform	IPsec SA limit	SD-WAN IPsec + RA IPsec	
		e.g.1 SD-WAN IPsec + RA IPsec	e.g.2 SD-WAN IPsec + RA IPsec
C8500-12X	8000	4000 + 4000	2000 + 6000
C8500-12X4Q	8000	4000 + 4000	3000 + 5000
C8500L-8S4X	6000	3000 + 3000	2000 + 4000
C8300-1N1S-6T	6000	3000 + 3000	1000 + 5000
C8300-2N2S-4T2X	6000	3000 + 3000	2000 + 4000
C8000v on-premises **(ESXi, 16 vCPU 32 GB RAM)**	2000	1000 + 1000	500 + 1500
ASR1002-HX	8000	4000 + 4000	2000 + 6000

SD-WAN RA headend public WAN IP

- Reachable from internet
- For inbound remote-access VPN connections

Firewall policy for SD-WAN RA headend behind firewalls

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

- Inbound traffic to be allowed:
  - Source IP: any; destination IP: SD-WAN RA headend WAN IP
  - Protocol/ports: IKEv2 (UDP ports 500, 4500)
  - IPsec (IP ESP)
  - TLS (TCP 443) for AnyConnect profile download
- Outbound traffic to be allowed:
  - Source IP: SD-WAN RA headend WAN IP; destination IP: any
  - Protocol/ports: IKEv2 (UDP ports 500, 4500),
  - IPsec (IP ESP)
  - TLS (TCP 443) for AnyConnect profile download

Certificate authority (CA) server

The CA server provisions certificates on Cisco IOS XE 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.

It is common for the CA server to be deployed at a data center site in the service VPN, together with the RADIUS server.

RADIUS/EAP server

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

- If a Cisco ISE server exists in your infrastructure, it can be used for all remote-access client authentication and authorization policy.
- The RADIUS/EAP server must be reachable from all the SD-WAN RA headends in a service VPN.

License

The licensing structure for SD-WAN RA is the same as for any other Catalyst 8000 edge platform.

The Catalyst SD-WAN RA edge platform has two prerequisites:

- Cisco DNA Advantage license
- Catalyst SD-WAN RA user count add-on license

To repurpose an existing Catalyst SD-WAN edge device as a Catalyst SD-WAN RA headend device, you must be running a Cisco DNA Advantage license on that device, as this is the minimum feature package for enabling the Catalyst SD-WAN RA on your SD-WAN fabric.

In addition to the above, you will need to order an add-on SD-WAN RA scale license for the entire fabric. This add-on license will entitle you to bring up remote users in a distributed fashion on any of your Catalyst SD-WAN edge locations (refer to Table 1 for qualified platforms).

Deployment options

The purpose of these design recommendations is to provide guidance on Cisco's preferred recommendations for implementing the SD-WAN RA based on the common customer use cases or to optimally use the existing SD-WAN infrastructure.

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

- Local SD-WAN branch
- On-premises data center or regional hub
- In a colocation facility
- Hosted in a public cloud (using Cisco Virtual Platform)

Local branch SD-WAN RA headend

Deploy an SD-WAN RA headend at local SD-WAN branch routers:

In a branch infrastructure with a capable platform with higher-capacity WAN links from branches to the data center headend or internet links to a public cloud or SASE, remote access can be deployed as an SD-WN RA headend.

- Preferred closest branch location as SD-WAN RA headend to the remote-access client
- Distributed architecture for better tunnel and throughput scale
- Remote-access clients can split among the different branch platforms or locations

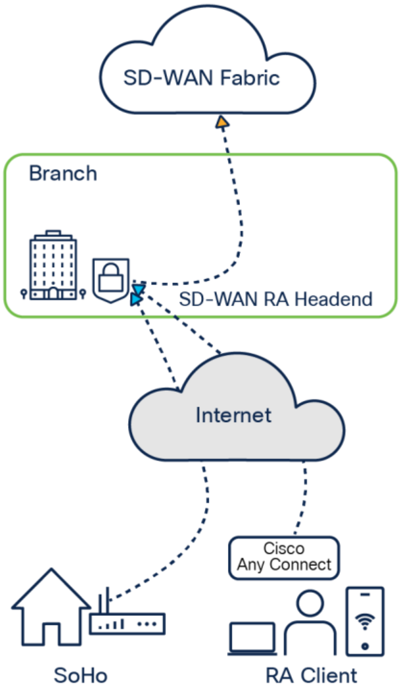


Figure 7.
Branch as an SD-WAN RA headend

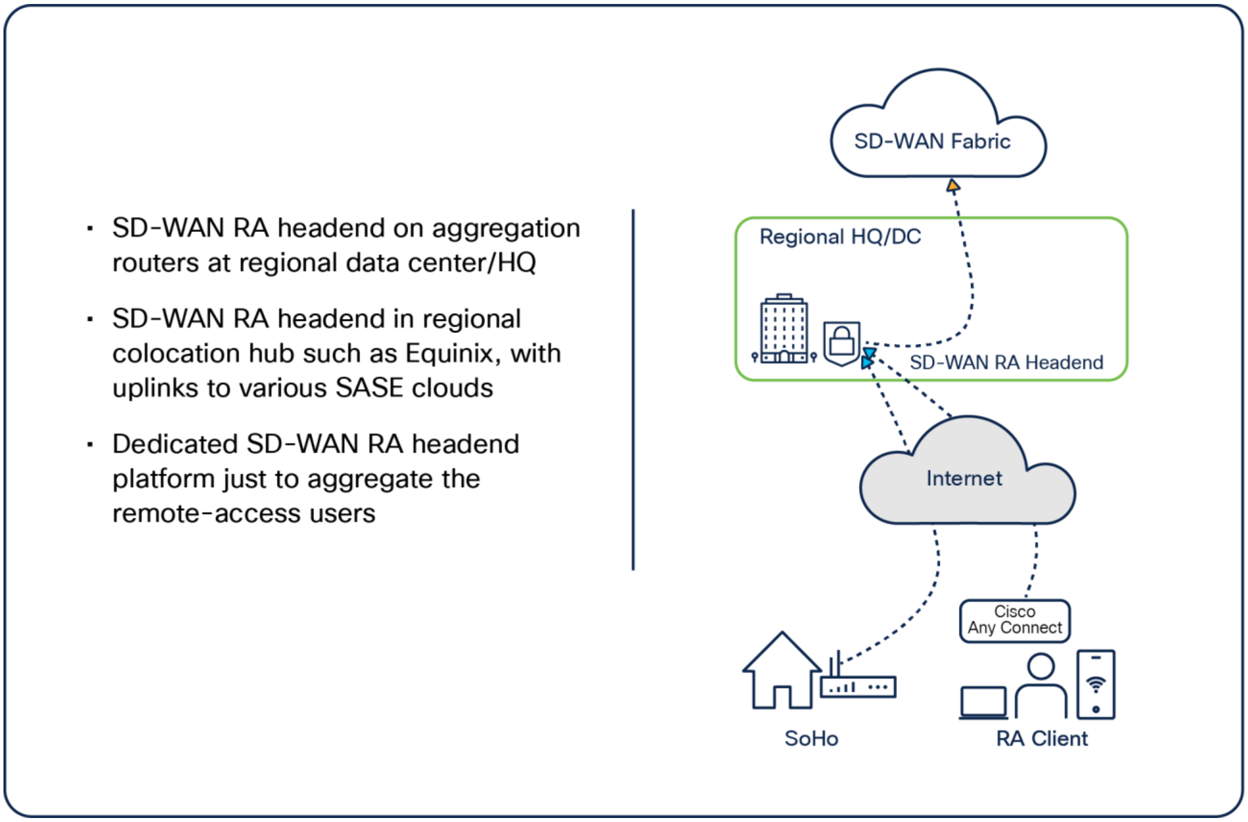
Data center/HQ or regional colocation hub SD-WAN platform as SD-WAN RA headend

The aggregation platforms, which are quite capable in terms of controlling scale, tunnels, and aggregation, can be used to terminate all remote-access clients.

The remote-access clients can also be split among the primary and secondary types of headend routers to divide the load.

You could use your colocation hub; for example, if you have a hub in Equinix that has uplinks to various SASE clouds, you could use that directly as an SD-WAN RA headend.

Dedicated platform as SD-WAN RA headend



- SD-WAN RA headend on aggregation routers at regional data center/HQ
- SD-WAN RA headend in regional colocation hub such as Equinix, with uplinks to various SASE clouds
- Dedicated SD-WAN RA headend platform just to aggregate the remote-access users

Figure 8.
Data center/HQ as SD-WAN RA headend – dedicated platform for remote access

Multiple platforms as SD-WAN RA headends for scale

- Multiple SD-WAN RA headends for horizontal scale-out for higher capacity
- Existing DMZ setup to protect public IP
- Proper security protection to be implemented for SD-WAN RA headend (Zone-Based Firewall)

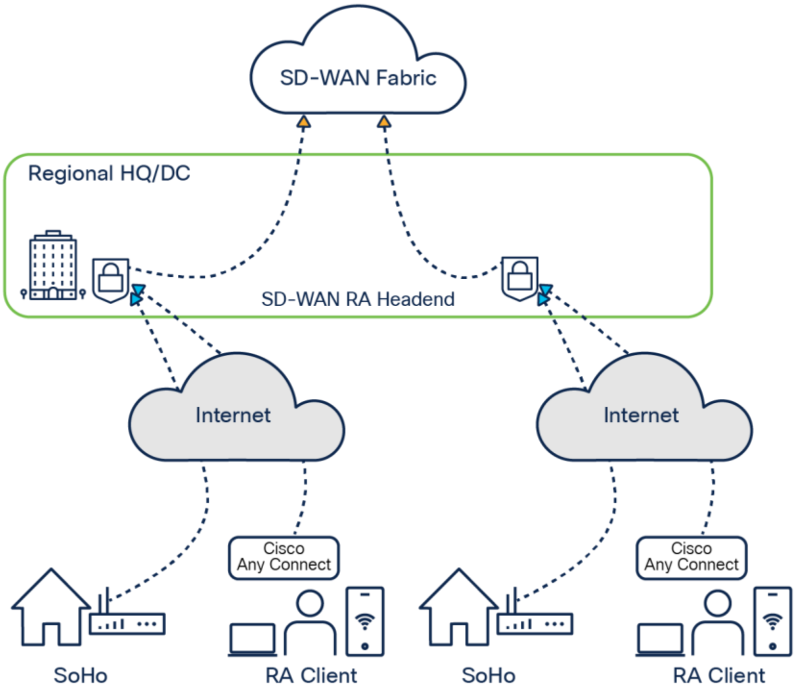
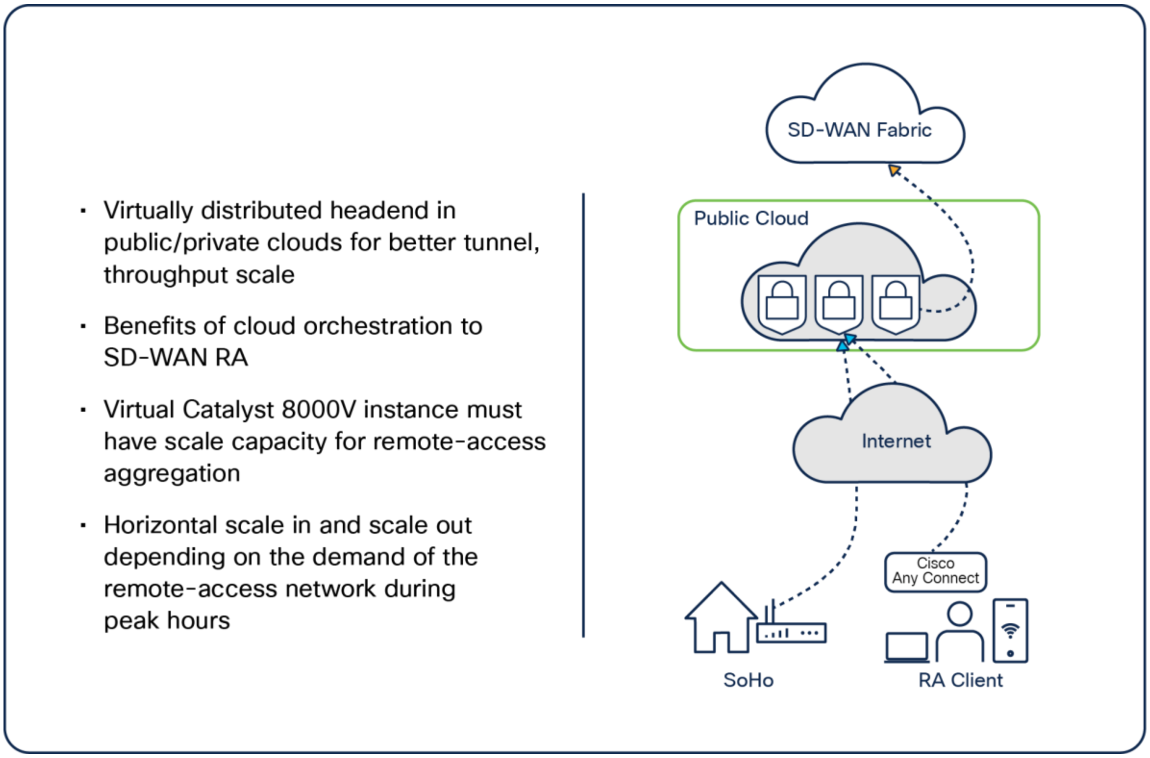


Figure 9.
Data center/HQ SD-WAN RA headend – multiple SD-WAN RA headends

Cloud-based SD-WAN RA headend

Deploy a virtual Cisco Catalyst 8000V instance in AWS or in an Azure instance and make that instance an SD-WAN RA headend in the SD-WAN fabric. This virtual Catalyst 8000V instance can be used to terminate the remote-access client in that region.

Based on the features enabled on the Catalyst 8000V—the tunnel scale limit considerations, for instance—the CPU and memory services given to that instance and virtual form will be the key considerations when you approach this virtual SD-WAN RA headend using the Catalyst 8000V platform.



- Virtually distributed headend in public/private clouds for better tunnel, throughput scale
- Benefits of cloud orchestration to SD-WAN RA
- Virtual Catalyst 8000V instance must have scale capacity for remote-access aggregation
- Horizontal scale in and scale out depending on the demand of the remote-access network during peak hours

Figure 10.
SD-WAN RA headend in a public cloud

Unified policies for hybrid work

As hybrid work is the new norm, every organization is looking for unified policy for all users, regardless of their location. SD-WAN RA supports a hybrid work environment.

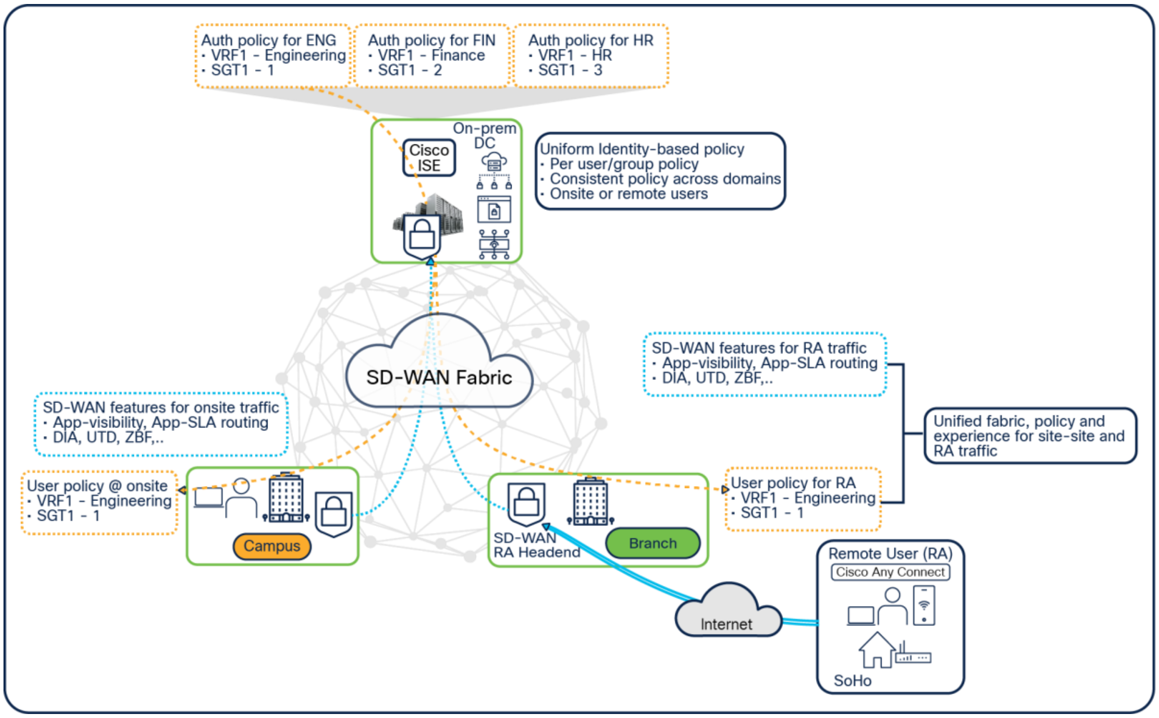


Figure 11.
Unified policy for hybrid work

The SD-WAN RA uses uniform identity-based policy, which remains the same across domains, whether users are onsite or remote.

The Cisco ISE server, along with the SD-WAN RA, enables organizations to maintain all their security policies, including perimeter security policies across remote access as well as across the SD-WAN fabric on the same Cisco ISE server. Cisco ISE is the single point where you can define all the policies, which can percolate down into your entire network.

The policies are location independent, and if the user moves away from the branch or campus and starts working from home, the same user policies or group policies will be applied based on the user's identity. This remote-access user will get the same level of access and application experience from home as at the office.

Apply SD-WAN features to RA traffic SD-WAN RA traffic pattern

Remote-access clients will have different traffic patterns, and we can apply various SD-WAN features to a remote user's traffic.

The traffic originated from the remote-access client comes in through either the Transport Locator (TLOC) or non-TLOC interface on the SD-WAN RA headend and terminates on the IPsec virtual interface. Depending on the packet's destination—a local application server on the LAN, a server in a remote data center, or a SaaS application via the internet—remote-access traffic is decrypted and reencrypted.

The different packet workflows for the remote-access clients are as follows:

Remote-access client accessing local resources on an SD-WAN RA headend:

- The remote-access client is accessing the local LAN resources at the SD-WAN RA headend, which, if it's a branch or regional hub, can have some applications hosted.
- So an IKEv2/IPsec tunnel from the remote-access client to the SD-WAN RA headend accesses the LAN server.

Remote-access client accessing data center resources:

- The remote-access client is accessing resources in the data center over an SD-WAN overlay fabric or anywhere else on the fabric. So the remote-access client traffic comes through the IPsec interface and, after decryption, lands in a service VPN on the SD-WAN device.
- From the service VPN it would hairpin back into the SD-WAN transport VPN0 interface by being re-encrypted and then would be sent over to the SD-WAN fabric to access data center resources.

Remote-access client accessing SaaS application over the internet:

- The remote-access client is accessing SaaS applications or internet applications through direct internet access (DIA) from the SD-WAN RA headend.OR
- The internet breakout can happen directly from the remote-access client using the split-tunnel option.

A remote user is placed in a service VPN based on identity, and therefore the traffic from the remote user, after decryption on the SD-WAN RA headend, is treated as inbound traffic from the remote-access user's service VPN. Therefore, all the SD-WAN features that are applicable for local LAN traffic are applicable for remote-access traffic, including 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.

Based on the remote-access client traffic pattern, you can make use of these different SD-WAN features for remote-access client traffic or data packets.

Rate-limiting of remote-access client traffic

Below are a few examples of applying SD-WAN features to remote user traffic. This may vary depending on the organization's scenarios.

Rate-limiting of remote-access upstream traffic (from a remote-access client)

One of the key functionalities is the rate-limiting of remote-access client traffic.

The traffic originated from the remote-access client comes in through the TLOC or non-TLOC interface and terminates on the IPsec virtual interface. We can precisely control, or rate-limit, the remote-access upstream traffic from remote-access clients by applying ingress policers at the right points for the upstream traffic coming in from the remote users.

This is for all upstream traffic, irrespective of whether the remote-access client is trying to access LAN resources at the SD-WAN RA headend, is accessing a file server in the data center, or is accessing SaaS applications via the internet.

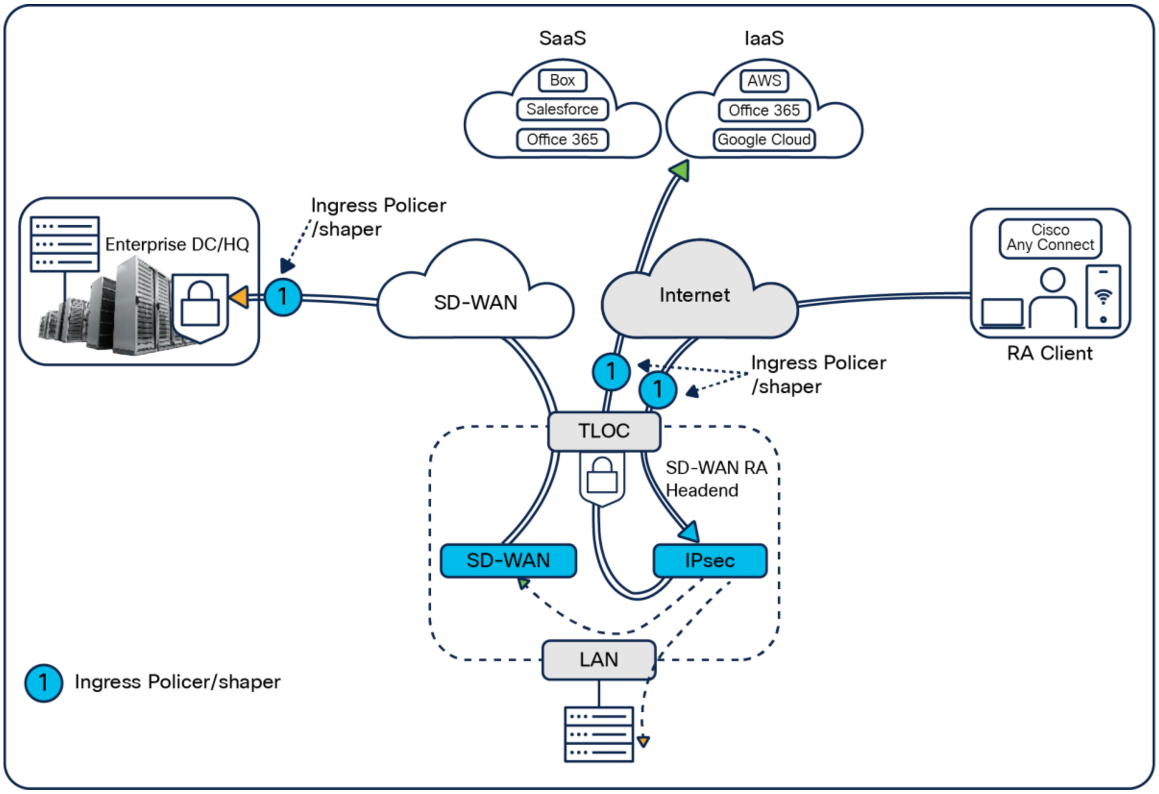


Figure 12.
Remote-access client upstream traffic

In this example, an ingress policer is applied to rate-limit remote-access client traffic at the TLOC interface, or going to the data center over the SD-WAN overlay transport VPN0, or going to the internet via Umbrella SIG. This process is shown in the figure with the number 1.

Considerations

Policing of encrypted remote-access upstream traffic

An inbound QoS policer can be applied on the SD-WAN RA interface using local data policy (access list).

- Match: IKEv2 and encrypted IPsec traffic.
    - UDP 500/4500.
    - IP Encapsulating Security Payload (ESP) protocol.
- Action: Police to a required rate.

This will drop the excess remote-access traffic before decryption, but the traffic drop is unconditional regardless of the remote-access client and application type. This will rate-limit upstream traffic irrespective of the traffic destination–SD-WAN RA headend LAN, data center, or internet.

Policing and shaping of decrypted remote-access upstream traffic

An inbound QoS policer can be applied using a from-service centralized data policy.

- Match: Remote-access inner traffic.
  - Remote-access user service VPN.
  - Source IP as the remote-access client assigned IP address(es).
  - Application.
- Action: Police or shape to a required rate.

This will drop or shape the excess remote-access traffic after decryption and hence can be selective based on remote-access clients and application types.

In this way we can use the ingress policer to control the flow of the remote-access client traffic.

Rate-limiting of remote-access downstream enterprise traffic (toward the remote-access client)

For the return, remote-access traffic from SD-WAN sites, such as an SD-WAN RA headend or data center, as well as from the internet or SaaS, to the remote-access clients can be rate-limited. Figure 13 shows the remote-access return traffic from the data center or internet, labeled with the number 1. Here the match would be the destination of the remote-access client IP, which would be assigned from a Dynamic Host Configuration Protocol (DHCP) pool by the SD-WAN RA headend (if you already know the pool, you can match the pool). You would apply a policer as shown here to control how much traffic the remote users can download from the data center.

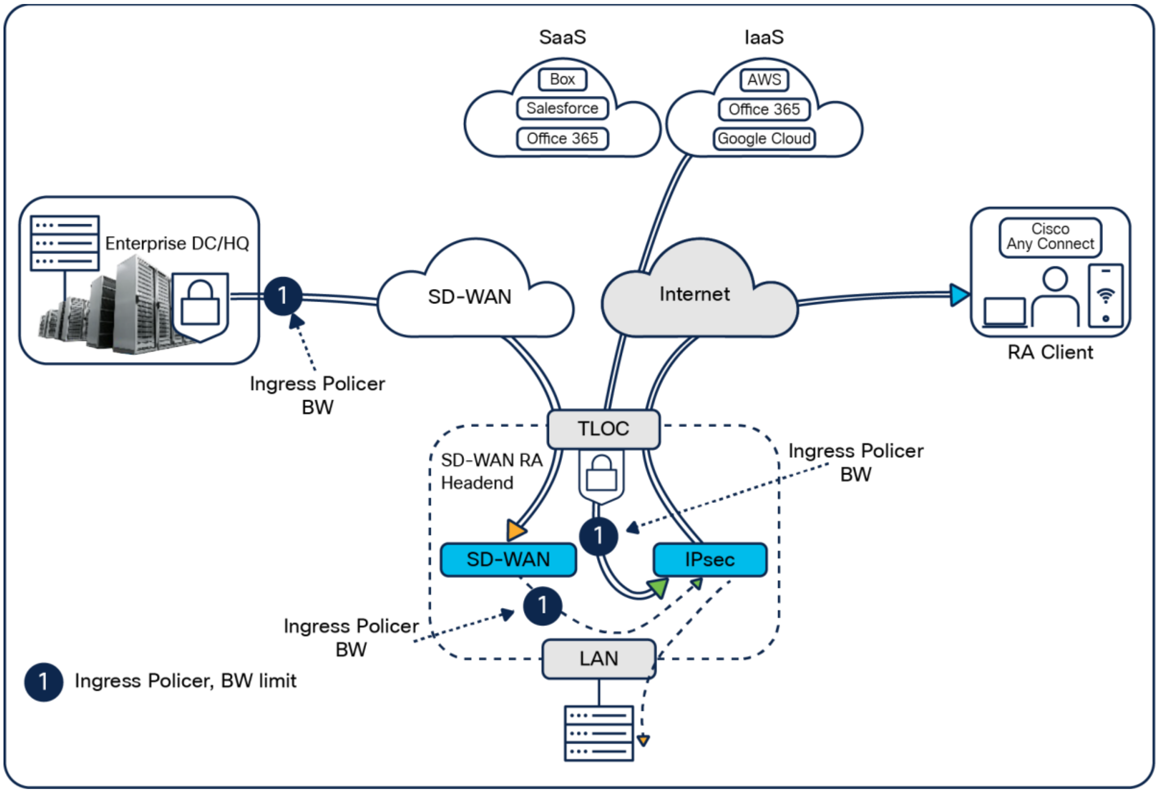


Figure 13.
Remote-access client downstream traffic

Considerations

Inbound QoS – post-decryption.

- Centralized data policy with policer/shaper/QoS.
    - From-service policy for headend-to-LAN return traffic.
    - From-tunnel policy for SD-WAN-to-site and internet return traffic.
- Match: Remote-access inner traffic.
    - Remote-access user service VPN.
    - Destination IP as the remote-access client assigned IP address(es).
    - Application.
- Action: Police or shape to a required rate.

Similarly, we can apply a policer at the TLOC interface for return traffic coming from the internet or SaaS to prevent remote users from consuming more bandwidth than has been allotted.

This will ensure that the enterprise and internet/SaaS remote-access return traffic is rate-limited as close to the traffic source (application server) as possible.

By applying these polices at the appropriate points, we can precisely control how much traffic can be used by all the remote users, both upstream and downstream.

Applying the SD-WAN egress feature to remote-access traffic

For all the remote-access client traffic flows, we can apply the SD-WAN data policies and egress features to remote-access traffic.

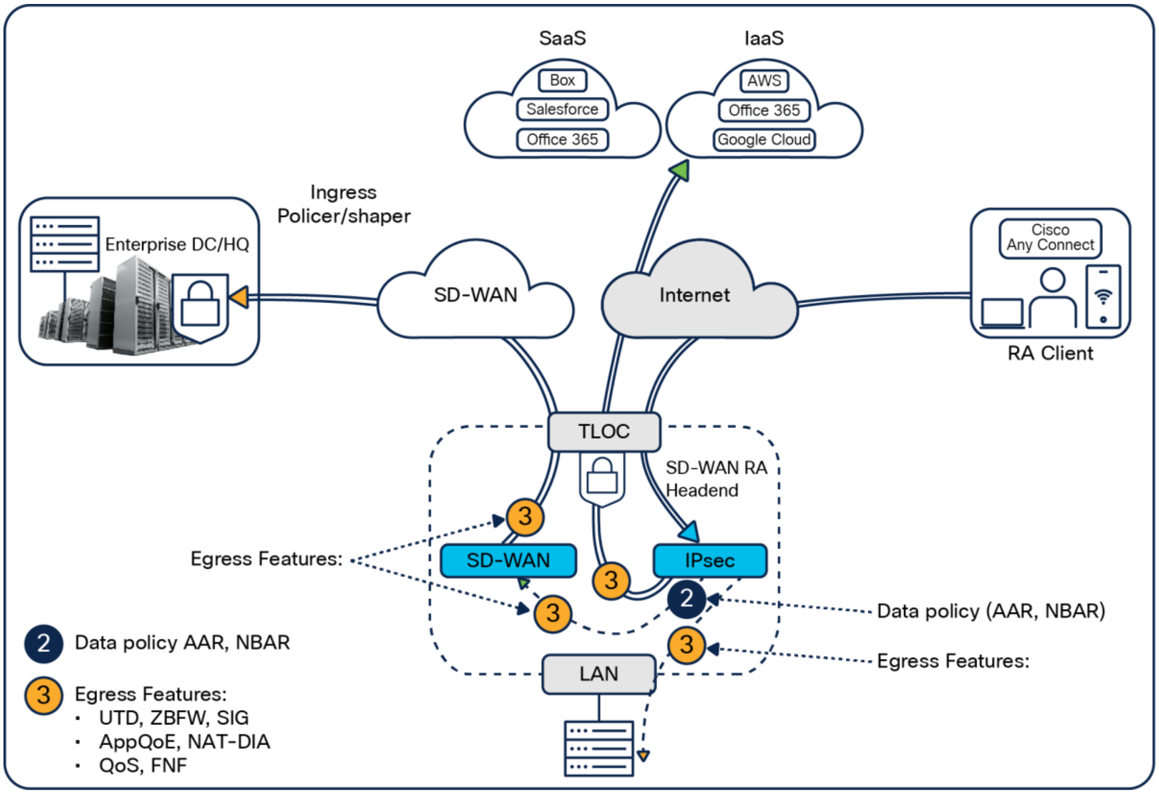


Figure 14.
SD-WAN egress features applied to remote-access client traffic

The remote-access traffic lands on the SD-WAN RA headend through the IPsec interface, after it gets decrypted. As it's coming out of the IPsec interface, all the data policies, such as application-aware routing, Network Based Application Recognition (NBAR), and application visibility, get executed. This is labeled as number 2 in Figure 14.

Then, based on the policy actions, all of these data policies, such as UTD, ZBFW, SIG, QoS, etc. will be executed on the egress interface of the SD-WAN edge router, and the traffic can be sent to the data center or to the internet through an Umbrella SIG, or we can apply AppQoE WAN optimization This is labeled as number 3 in Figure 14.

Key takeaways

Catalyst SD-WAN RA provides an enterprise SD-WAN infrastructure-centric remote-access that:

- Provides the option to connect a hybrid workforce to an enterprise SD-WAN network.
- Integrates seamlessly with on-premises and cloud-based advanced SD-WAN security.
- Has the inherent ability to terminate remote-access users, whereby the VRF and user identity is maintained from end to end.
- Can support a software client (AnyConnect) and native OS-based clients as well as Cisco hardware-based clients on Cisco IOS XE devices.
- Can provide a consistent user application experience to remote-access/home office users in a hybrid work environment.

Conclusion

While remote work is not new, we are entering a new era in which many enterprises are realizing that their legacy WAN and VPN architectures are inadequate. To ensure a seamless transition from office to home, or anywhere, employees need a technical environment that closely duplicates the experience they would have in the office. The Catalyst SD-WAN RA addresses the needs of the hybrid workforce by unifying the network and security.

An SD-WAN RA that builds upon SD-WAN should be at the top of the list for any enterprise seeking to address the needs of the new work-from-anywhere era.

Learn more

To learn more about Catalyst SD-WAN RA, visit the following:

- Catalyst SD-WAN Remote Access End-User Guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-3307455-01 10/23