

CISCO *Live!*



#CiscoLive



The bridge to possible

# Cisco Secure Remote Worker

## Overview of SD-WAN Remote Access

Wijendra Gnanendren, Technical Solutions Architect / Leader Col  
Competitive  
BRKENT-1614

# Agenda

- Introduction
- Challenges of remote working
- Traditional Remote access
- Cisco SD-WAN Remote Access
- Use Cases & Deployment Models
- Configuration
- Licensing
- Technology Roadmap

# Cisco Webex App

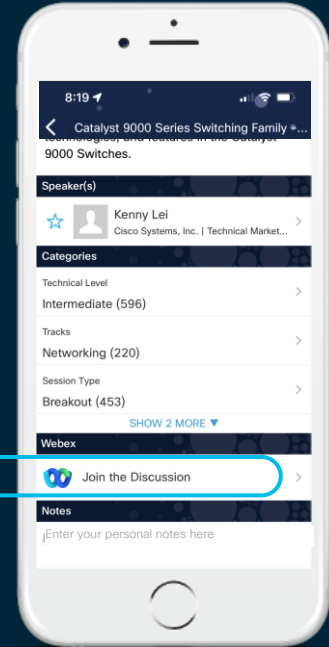
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.

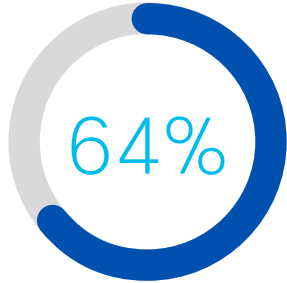


<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-1614>

# Introduction



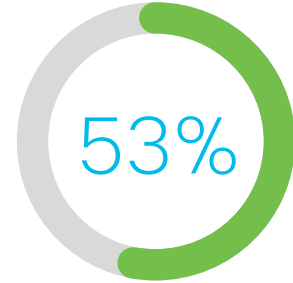
# Enterprises are moving to Hybrid by Design



Employees expect increased work flexibility<sup>1</sup>



Office workers anticipate to work 8 days per month from home<sup>2</sup>



Organizations plan to reduce their office footprint<sup>2</sup>

<sup>1</sup>IDC Futurescape: Worldwide Future of Work 2021 Predictions  
<sup>2</sup>Global Workforce Survey: The Rise of the Hybrid Workplace Report

# Challenges of Remote Working



# Work Is Changing. Is Your Network Ready?

People want to be **protected**, **productive**, and **engaged** wherever they choose to work

A distributed hybrid workforce needs a network that offers



## Unified Policy

Single unified security policy based on User identity irrespective of location



## End-point Flexibility

Flexible Hardware & Software client options for remote workforce



## Scalability

Highly scalable solution without compromising on cost & resiliency



## Application experience

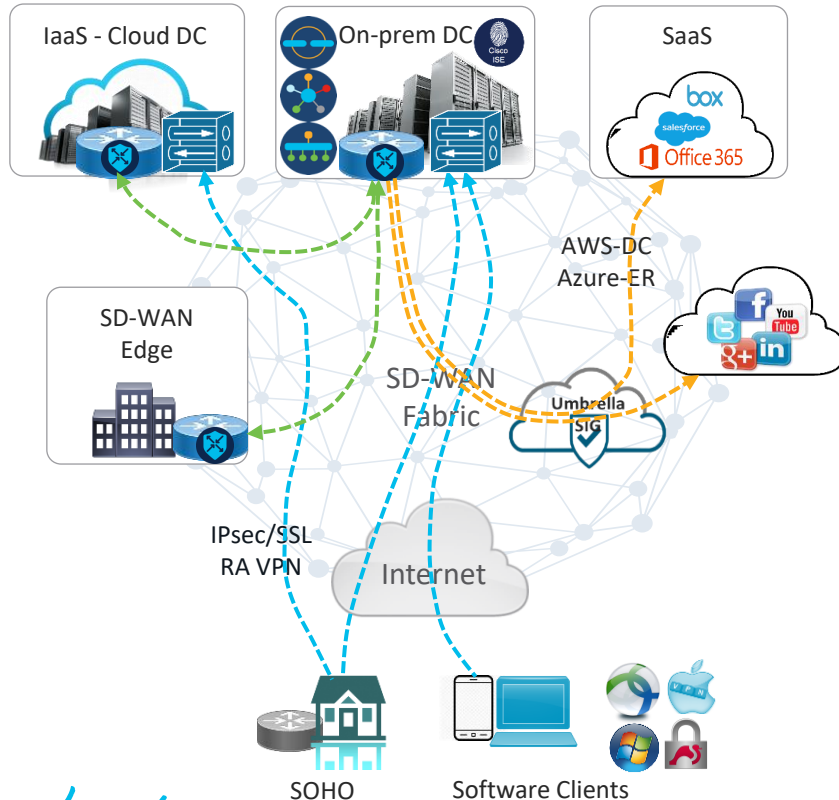
Consistent & optimized application experience (SaaS, IaaS, On-Prem Datacenter)



# Traditional Remote Access



# Traditional Remote Access – The challenges

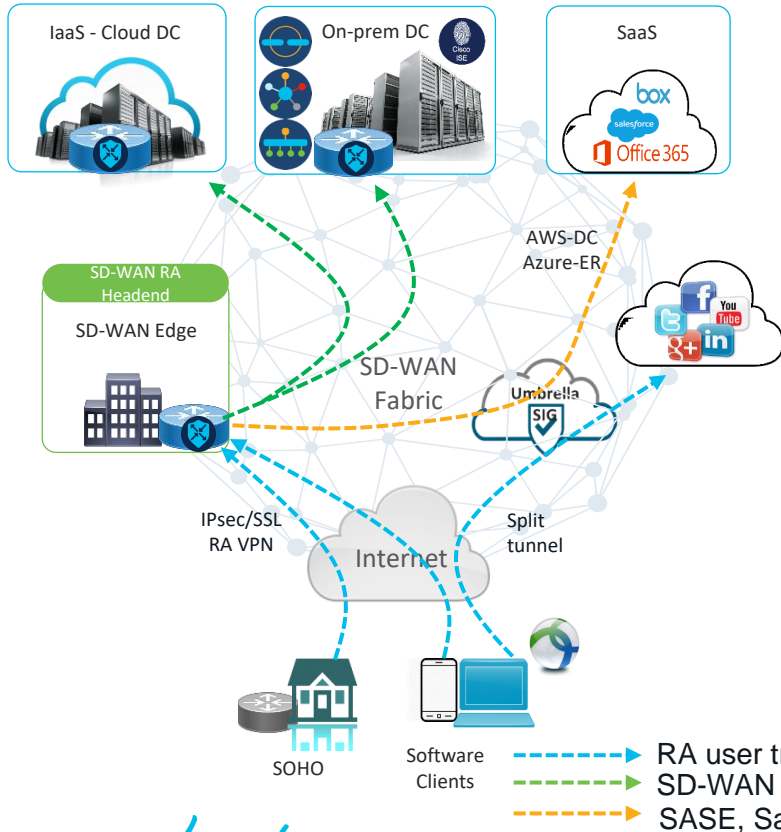


- SD-WAN & RA network treated as separate network fabrics
- Require additional VPN Hardware for scaling number of RA users
- Separate **Management** of Traditional RA network
- Separate **security** policies for RA and on-prem workforce
- Backhaul of RA traffic through DC, poor **application experience**
- RA traffic needs to be stitched to SD-WAN fabric at DC today

# Cisco SD-WAN Remote Access

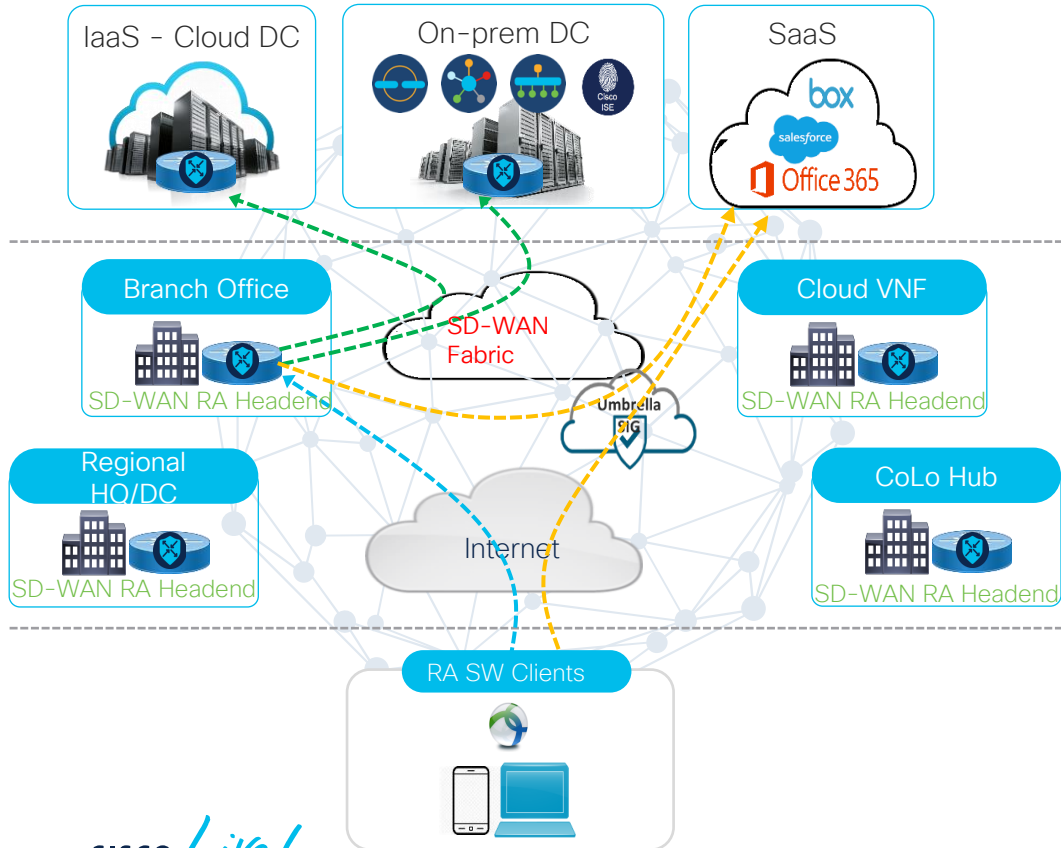


# Cisco SD-WAN Remote Access Solution



- 1) Cisco's proven FlexVPN Remote-access technology
- 2) SD-WAN fabric as RA headend network
  - a. IOS-XE supports RA-VPN headend functionality
    - i. FlexVPN(IKEv2/IPsec)
    - ii. SSLVPN (Support is in the Roadmap)
    - iii. IOS-XE SD-WAN devices inherit RA headend stack
  - b. Leverage IOS-XE SD-WAN device as RA Headend
- 3) vManage based RA-Headend config & monitoring
  - a. RA headend configs
  - b. Visibility into RA connections on SD-WAN RA Headend
- 4) RA client monitoring through ISE
- 5) Integration with Software (Anyconnect) RA client And Hardware RA Client (Cisco IOS-XE router)

# Cisco SD-WAN RA value proposition



Lower TCO, SD-WAN Lite control-plane



Unified fabric, Single-pane-of-glass management



Highly Scalable, Elastic & Distributed deployment



Enterprise-grade SD-WAN benefits extended to Remote workforce



Unified Security policy & posture using ISE for both On-Prem & RA workforce



RA termination within enterprise owned SD-WAN fabric

# Workflow



# Workflow

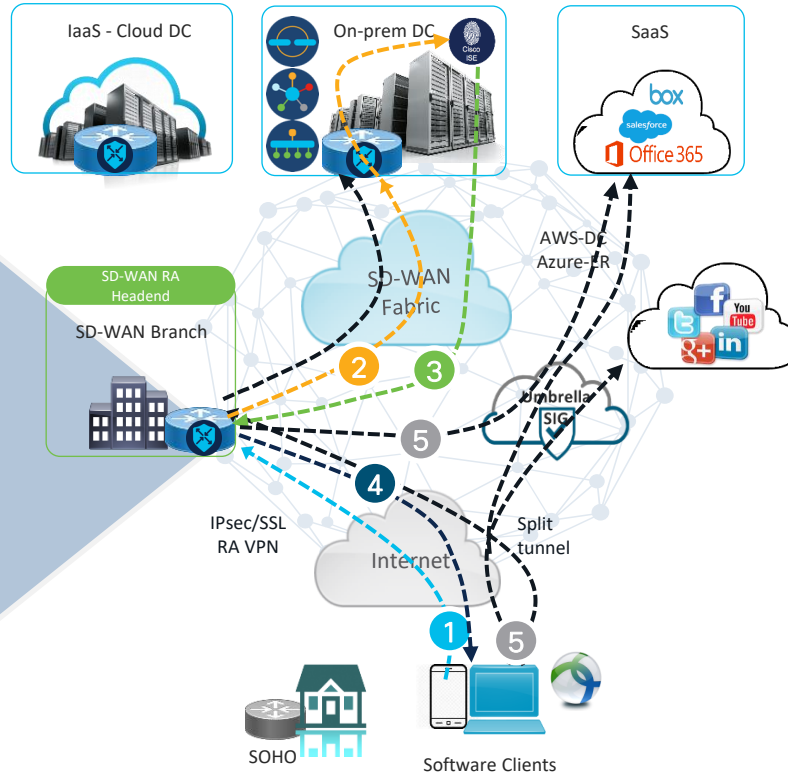
## SD-WAN RA Headend Consideration

Static WAN public routable IP address

Capacity planning for Crypto engine, WAN throughput

Certificate management - CA server for RA authentication

Private IP address pools for RA clients



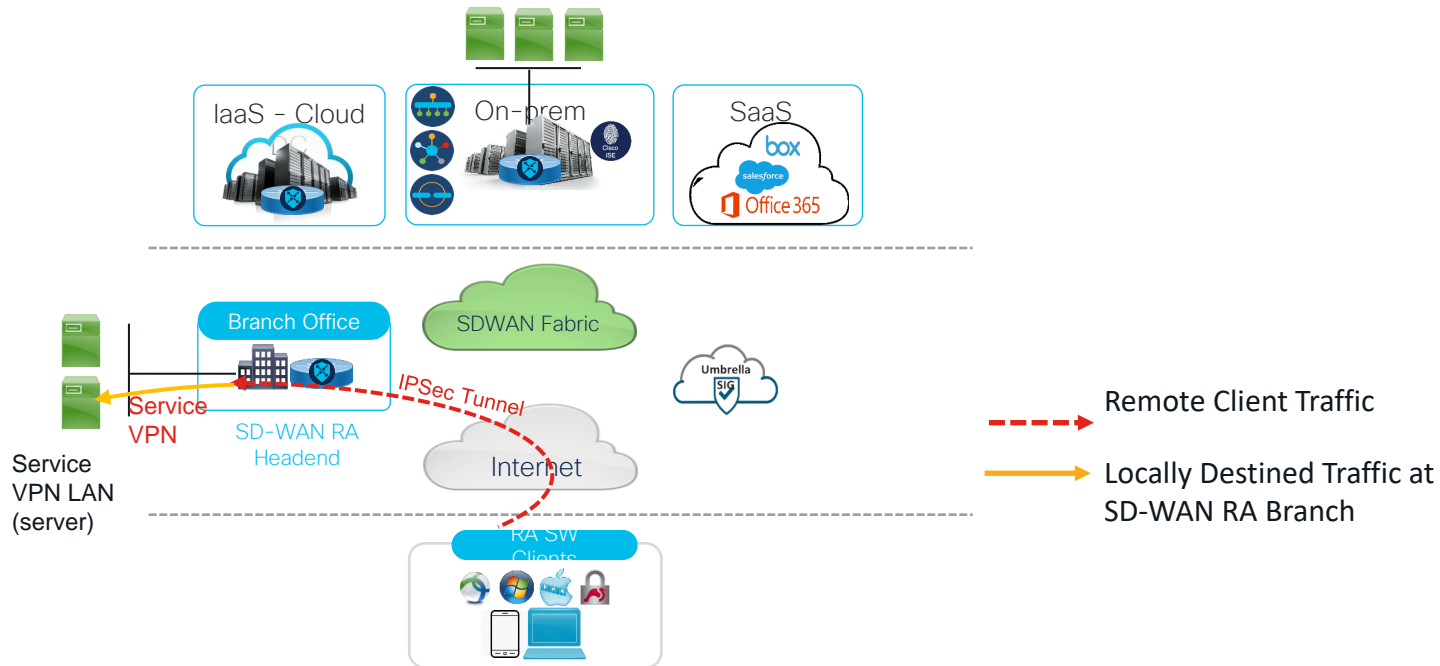
## Workflow

- 1 A remote user connects to the RA headend - Requests a IPsec connection
- 2 SD-WAN RA headend authenticates clients with cert or PSK
- 3 User/group policy from ISE VRF, SGT, Client-IP, Subnets, etc.
- 4 Create IPsec virtual interface (per RA user) & push attributes (IP assignment, DNS, Subnet etc ) to RA-client
- 5 Full/split-tunnel – Client routes traffic to all/specified subnets via VPN

# Traffic Pattern: Use Case 1

Remote Users Accessing Local LAN Servers in SD-WAN RA Headend Branch

RA-client -(IKEv2/IPsec)-->SD-WAN RA Headend --> LAN (server)

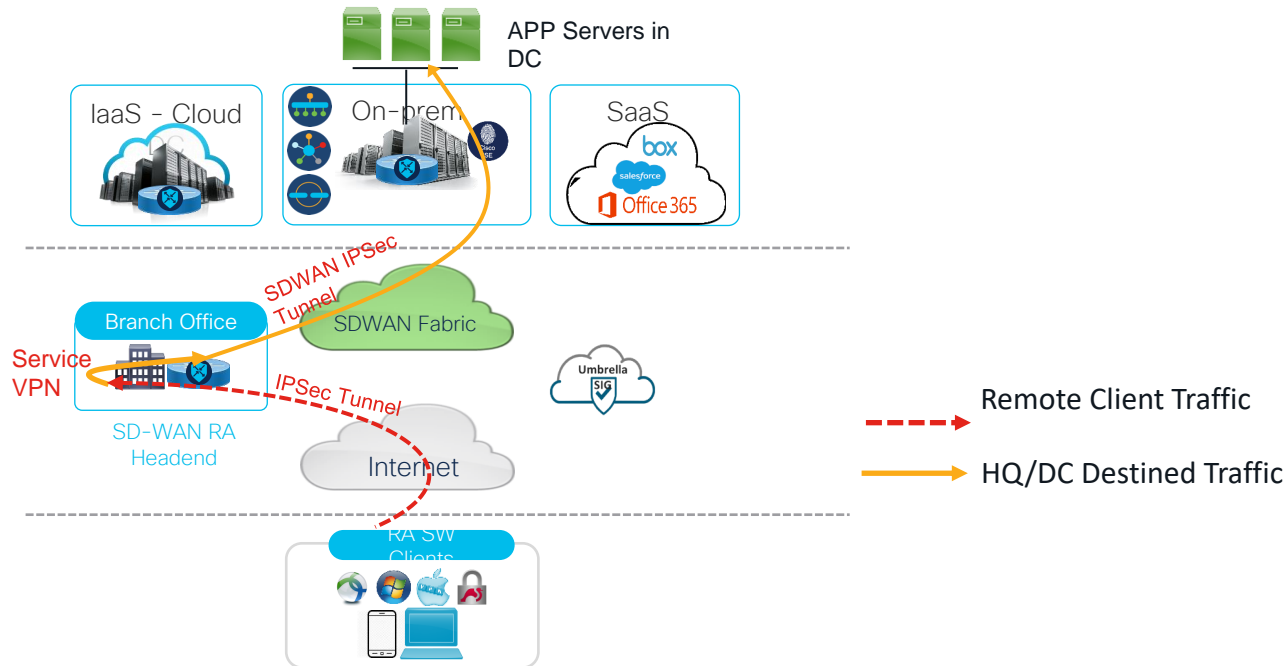




# Traffic Pattern: Use case 2

## Remote Users Accessing App Servers in DC LAN

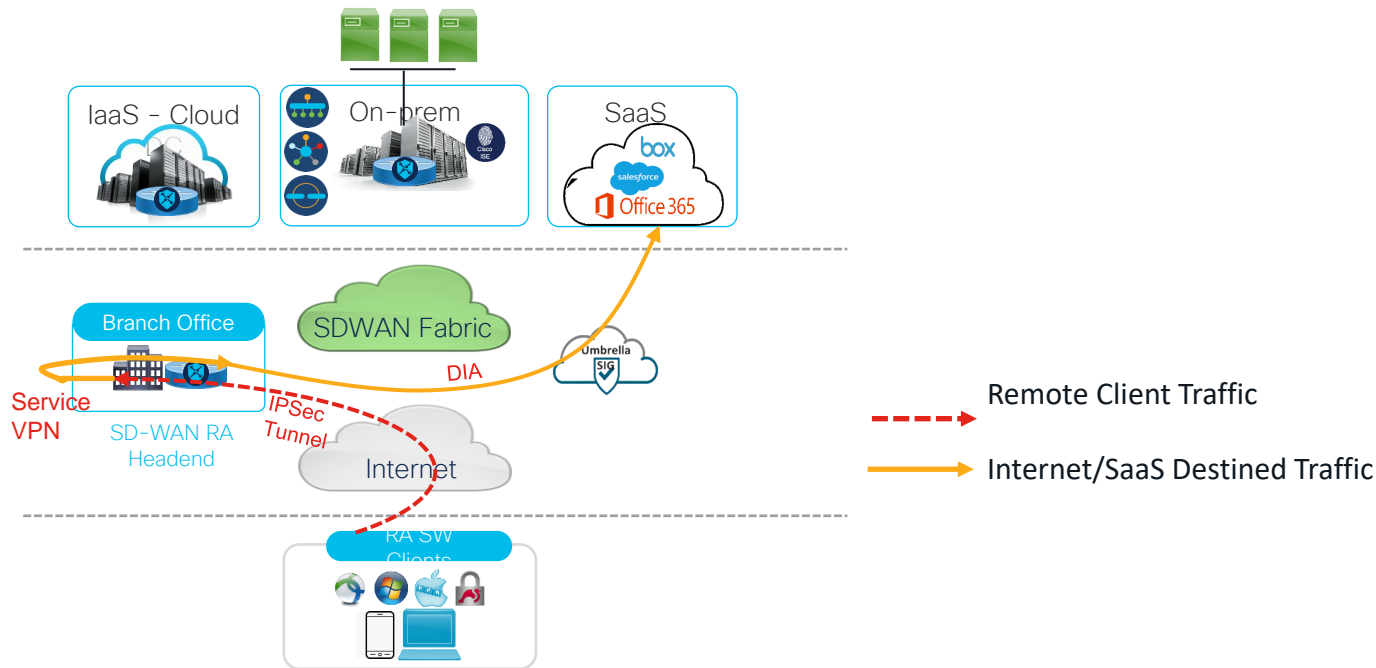
RA-client -(IKEv2/IPsec)--> SD-WAN RA Headend -(SDWAN-IPsec)-->DC --> LAN (server)



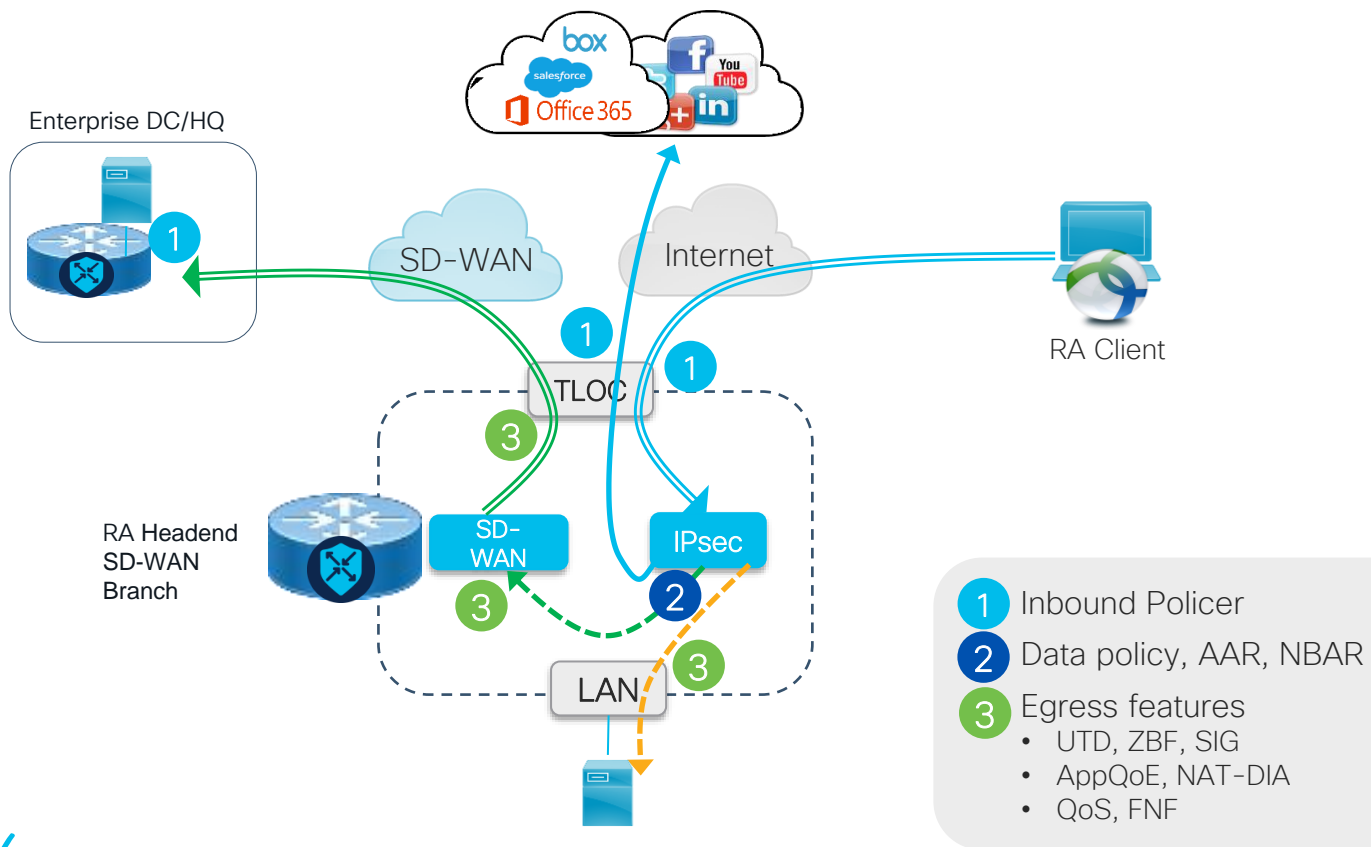
# Traffic Pattern: Use case 3

Remote Users Accessing SaaS Application From SD-WAN RA Headend Branch - through Local DIA

RA-client -(IKEv2/IPsec)--> SD-WAN RA Headend -(DIA)--> Internet/SaaS/IaaS

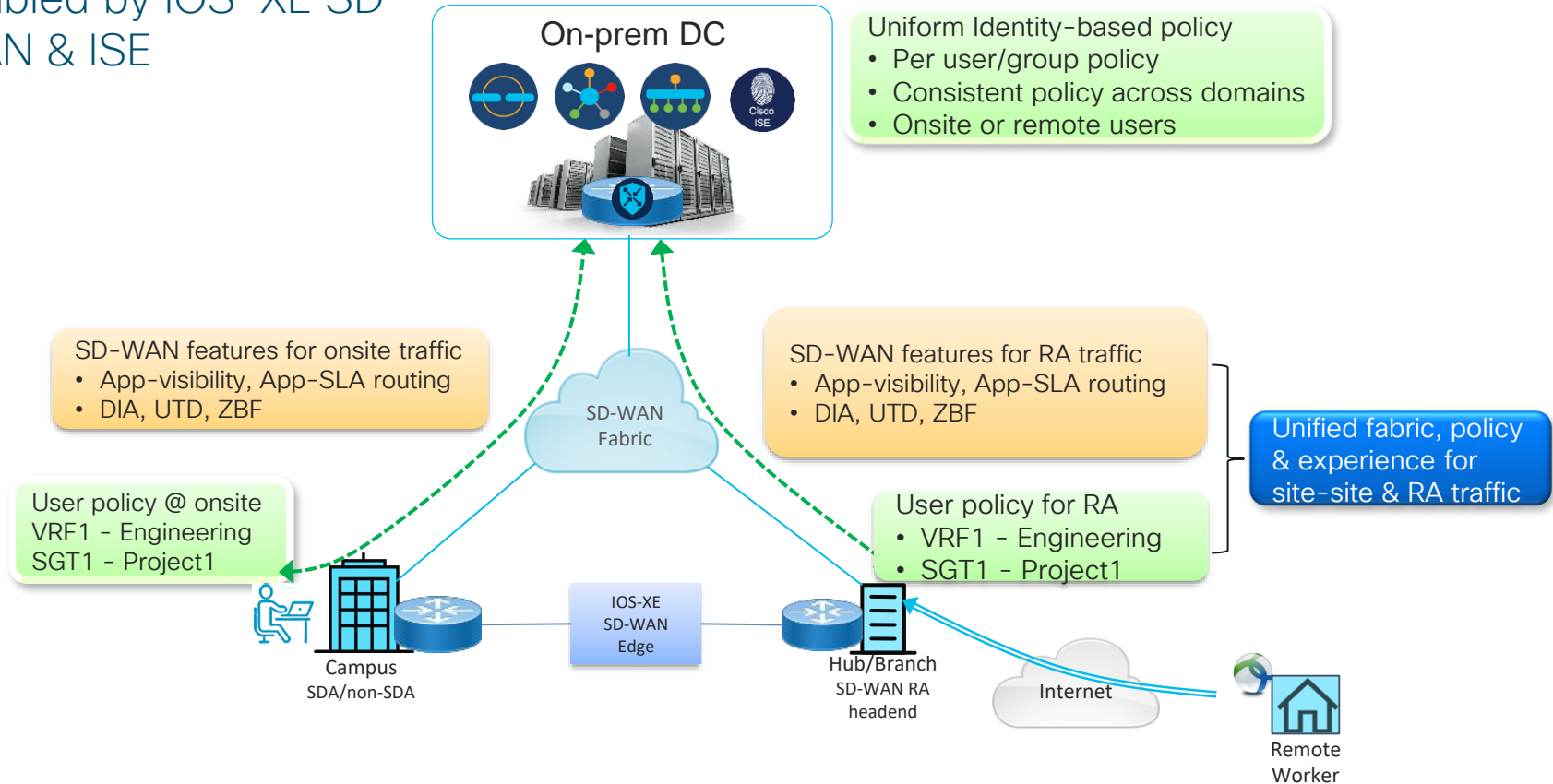


# Packet Flow – SD-WAN features for RA traffic



# SD-WAN for Hybrid Work

Enabled by IOS-XE SD-WAN & ISE



# Deployment Models

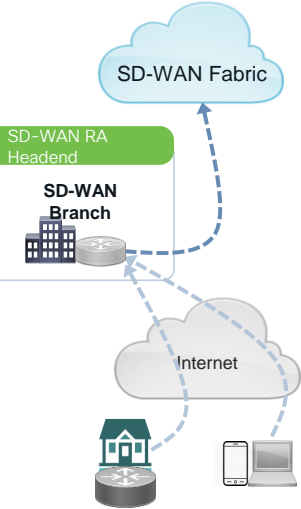


# Deployment Models

## Regional Hub, Colo, Cloud-based, Branch

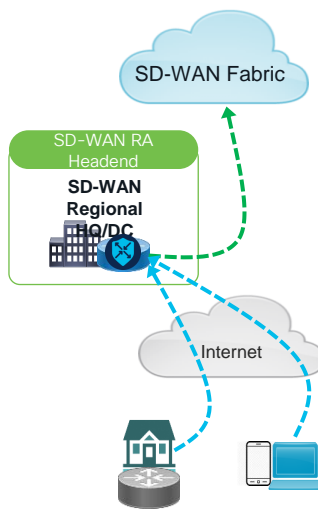
With 17.7 IOS XE :  
Platforms Supported - C8500, C8300

### Local Branch SD-WAN RA Headend

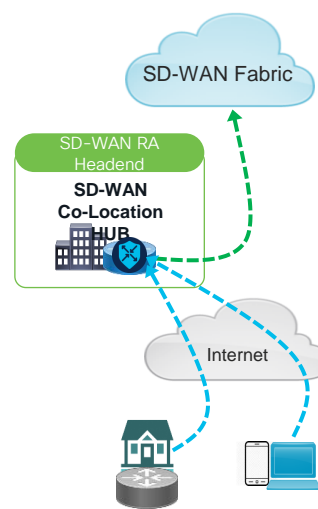


COMM/Small

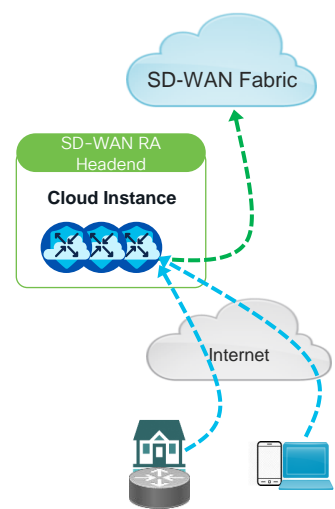
### Regional DC SD-WAN RA Headend



### Regional CoLo HUB as SD-WAN RA Headend



### Cloud-based SD-WAN RA Headend



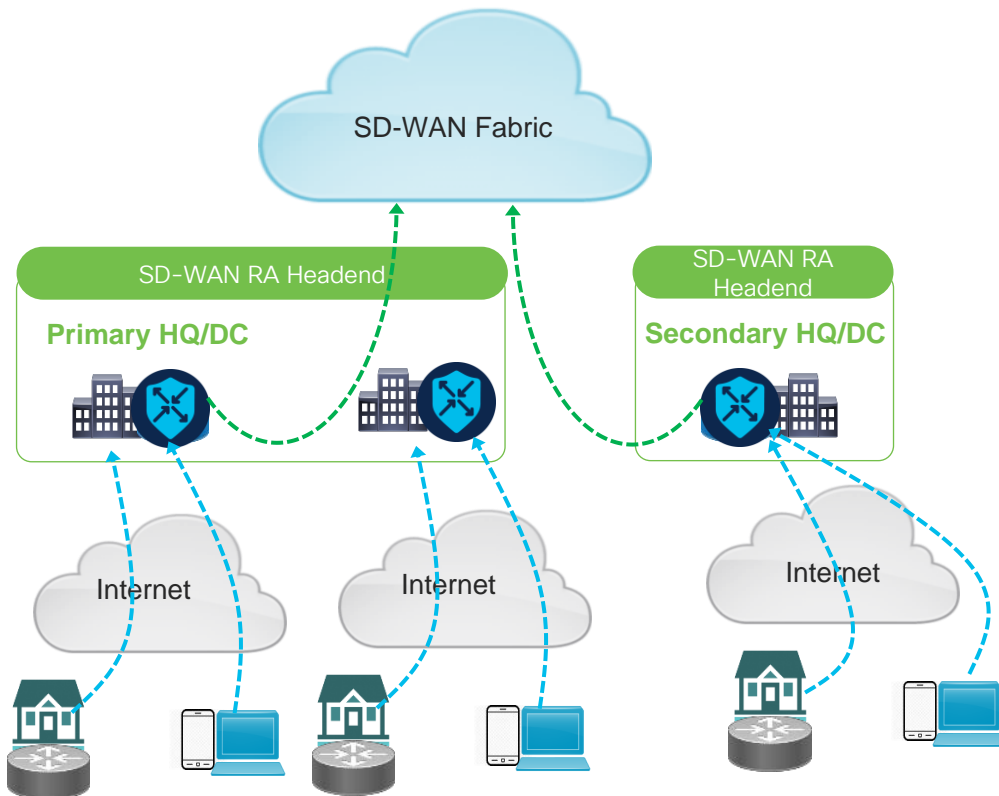
Cloud-First /Cloud-native

SMB, ENT

Large Enterprises

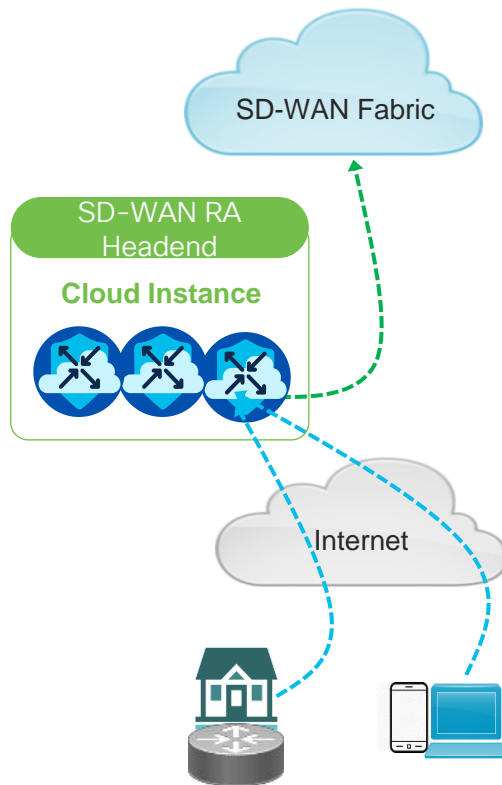
# Regional DC/HQ as SD-WAN RA Headend

On-prem, Data Center or Colocation Presence



# Virtual SD-WAN RA Headend

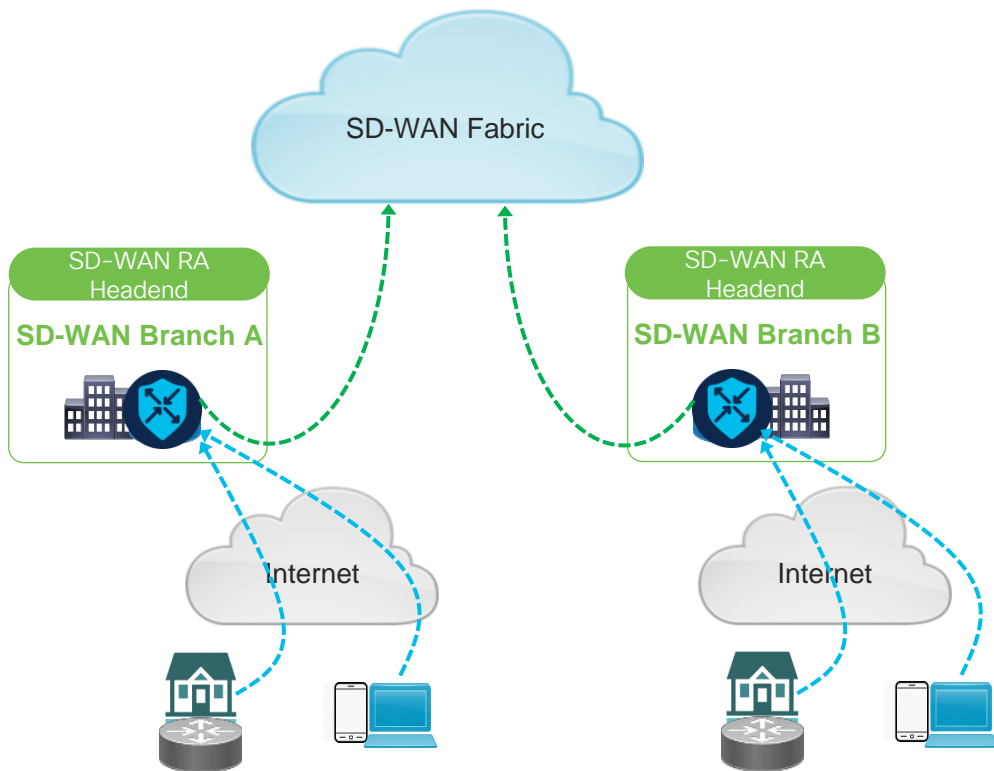
Public or Private Cloud Hosted using Catalyst 8000V










# Local SD-WAN RA Headend at Branch

Preferred closest RA Hub to the RA Client



# Supported VPN Client Types

Software & hardware(SOHO) clients

						
	Desktop	Mobile	Native IKEv2 Client	Hardware Client	StrongSwan	Native IKEv2 Client
Supported OS	Windows Apple	Android,	Windows 7, 8, 10	Cisco IOS-XE	Linux, Mac OS X, Android, FreeBSD, ...	iOS 9  OS X El Capitan
	Linux	BlackBerry				
	MAC OS X	FirePhone				
	Windows 8.1					
Supported IKEv2 Authentication Methods	Certificates		Certificates	Certificates	Certificates	Certificates
	EAP		EAP	EAP	EAP	EAP
				Pre-Shared Key	Pre-Shared Key	Pre-Shared Key
Supported EAP Authentication Methods	EAP-MSCHAPv2		EAP-MSCHAPv2	EAP-MSCHAPv2	EAP-MSCHAPv2	EAP-MSCHAPv2
	EAP-GTC		EAP-TLS <sup>1</sup>	EAP-GTC	EAP-TLS <sup>1</sup>	EAP-TLS
	EAP-MD5		EAP-PEAP <sup>1</sup>	EAP-MD5	EAP-PEAP <sup>1</sup>	
			... and more (Win8)		... and more (plugins)	
Dual Stack (IPv4 & IPv6)	Both (with GRE)		Planned (headend limitation)	Both (with GRE)	Planned (headend limitation)	Planned (headend limitation)
Split Tunneling		Yes	Very limited (classful)		Yes	Yes

# SD-WAN RA Configuration



# SD-WAN RA configuration

vManage feature template for pre-requisite SD-WAN configurations

CLI add-on template for SD-WAN RA configuration

RADIUS/ISE for per-user/group authentication credentials and policy

# Configuration steps

1. Configure IKEv2 ciphers and settings

2. Configure PKI trustpoint for certificate enrolment

3. Configure IKEv2 profile

4. Configure IPsec ciphers, parameters and virtual-template

# Configuration steps

5. Configure AnyConnect Profile download

6. Configure RA IP pool

7. Configure AAA

8. Configure RADIUS

9. Configure SD-WAN features for RA traffic

# SD-WAN RA Headend Configuration

≡ Cisco vManage

📍 Select Resource Group▼

Configuration • Templates

Device

Feature

🔍 Search

[Add Template](#)

Template Type **Non-Default** ▼

Name	Description	Type	Device Model	Device Templates	Resource Group
C8500-12X-VPN0-Template	C8500-12X-VPN0-Template	Cisco VPN	C8500-12X	1	global
C8500-12X-VPN0-Ten0/0/0	C8500-12X-VPN0-Ten0/0/0	Cisco VPN Interface Ethernet	C8500-12X	1	global
C8500-12X-Service-VPN1-template	C8500-12X-Service-VPN1-template	Cisco VPN	C8500-12X	1	global
C8500-12X-ServiceVPN_Ten0/0/11	C8500-12X-ServiceVPN_Ten0/0/11	Cisco VPN Interface Ethernet	C8500-12X	1	global
SDWAN-RA_Add-On_CLI_Template	SDWAN-RA_Add-On_CLI_Template	CLI Template	C8500-12X	1	global

1

VPN Feature  
Templates

2

SD-WAN-RA  
CLI Add-on Feature Template

CISCO *Live!*

#CiscoLive

© 2022 Cisco

Reserved. Cisco Public

# SD-WAN RA Headend – Feature Template

## Device Template

≡ Cisco vManage Select Resource Group ▼

Q C8500-12X × Search

Create Template ▼

Template Type Non-Default ▼

Name	Description	Type
1 C8500-12X_Device_template	C8500-12X_Device_template	Feature

### Transport & Management VPN

Cisco VPN 0 \*

VPN\_0

Cisco VPN Interface Ethernet

VPN\_0\_Interface\_Template

### Service VPN

Q Search

0 Rows Selected

Add VPN

Remove VPN

☐ ID

Template Name

Sub-Templates

☐ 407f10ae-b333-4a7a-9fea-a6c886e556be

VPN\_10\_Service\_VPN

Cisco VPN Interface Ethernet

```
interface GigabitEthernet2 -> Internet TLOC
tunnel-interface
encapsulation ipsec
color biz-internet restrict
!
interface GigabitEthernet5 -> MPLS TLOC
tunnel-interface
encapsulation ipsec
color mpls restrict
```

```
interface GigabitEthernet4
description service VPN
vrf forwarding 1
ip address 77.27.11.1 255.255.255.0
End
!
interface Loopback1
description engineering DC-LAN
vrf forwarding 10
ip address 196.168.1.1 255.255.255.0
end
!
```



# SD-WAN-RA add-on CLI Template

Add Template

Template Type Non-Default

Name	Description	Type	Device Model	Device Templates	Resource Group
C8500-12X-VPN0-Template	C8500-12X-VPN0-Template	Cisco VPN	C8500-12X	1	global
C8500-12X-VPN0-Ten0/0/0	C8500-12X-VPN0-Ten0/0/0	Cisco VPN Interface Ethernet	C8500-12X	1	global
C8500-12X-Service-VPN1-template	C8500-12X-Service-VPN1-template	Cisco VPN	C8500-12X	1	global
C8500-12X-ServiceVPN_Ten0/0/11	C8500-12X-ServiceVPN_Ten0/0/11	Cisco VPN Interface Ethernet	C8500-12X	1	global
SDWAN-RA_Add-On_CLI_Template	SDWAN-RA_Add-On_CLI_Template	CLI Template	C8500-12X	1	global

2

☐ Intent
 ☒ Device Configuration

CLI Configuration
 Load Running config from re

Config Preview

```

3  !
4  aaa new-model
5  !
6  aaa group server radius SDR_A_RADIUS_SERVER
7  server-private 10.9.18.11 key Cisco123$
8  ip radius source-interface TenGigabitEthernet0/0/11
9  ip vrf forwarding 10
10 !
11 no ip http secure-server
12 !
13 aaa authentication login SDR_AUTHEN_MLIST group SDR_A_RADIUS_SERVER
14 aaa authorization network SDR_AUTHOR_MLIST group SDR_A_RADIUS_SERVER
15 aaa accounting network SDR_ACC_MLIST start-stop group SDR_A_RADIUS_SERVER
16 !
17 crypto pki trustpoint SDR_A_TRUSTPOINT
18 auto-enroll 80
19 enrollment url http://128.107.69.63:80
20 fingerprint 0123456789ABCDEF0123456789ABCDEF
21 subject-name cn=sera_headend_1
22 revocation-check none
23 auto-trigger
24 vrf 10
25 !
26 crypto ikev2 proposal SDR_A_IKEV2_PROPOSAL
27 encryption aes-cbc-256
28 integrity sha256
29 group 19
30 !
31 crypto ikev2 policy SDR_A_IKEV2_POLICY
32 proposal SDR_A_IKEV2_PROPOSAL
33

```

AAA Config

PKI CA Config

Config Preview

```

38 proposal SDR_A_IKEV2_PROPOSAL
39 !
40 crypto ikev2 name-mangler SDR_A_NAME_MANGLER_DOMAIN
41 eap suffix delimiter @
42 !
43 crypto ikev2 profile SDR_A_IKEV2_PROFILE
44 match identity remote any
45 authentication local rsa-sig
46 authentication remote anyconnect-eap aggregate
47 pki trustpoint SDR_A_PKI_TRUSTPOINT
48 aaa authentication anyconnect-eap SDR_A_AUTHEN_MLIST
49 aaa authorization user anyconnect-eap cached
50 aaa authorization group anyconnect-eap list SDR_A_AUTHOR_MLIST name-mangler
51 SDR_A_NAME_MANGLER_DOMAIN password Cisco123$
52 aaa accounting anyconnect-eap SDR_A_ACC_MLIST
53 virtual-template 101 mode auto
54 reconnect
55 !
56 crypto ipsec transform-set SDR_A_IPSEC_TS esp-gcm 256
57 mode tunnel
58 !
59 crypto ipsec profile SDR_A_IPSEC_PROFILE
60 set ikev2-profile SDR_A_IKEV2_PROFILE
61 set transform-set SDR_A_IPSEC_TS
62 !
63 interface Virtual-Template100 type tunnel
64 no shutdown
65 vrf forwarding 10
66 ip address 10.9.18.254 255.255.255.0
67 !
68 interface Virtual-Template101 type tunnel
69 no shutdown
70 vrf forwarding 10
71 tunnel mode ipsec ipv4
72 tunnel protection ipsec profile SDR_A_IPSEC_PROFILE
73 !
74 ip local pool SDR_A_IP_POOL 10.9.18.129 10.9.0.254
75 !

```

IKEv2 Profile Config

IPSec Profile Config

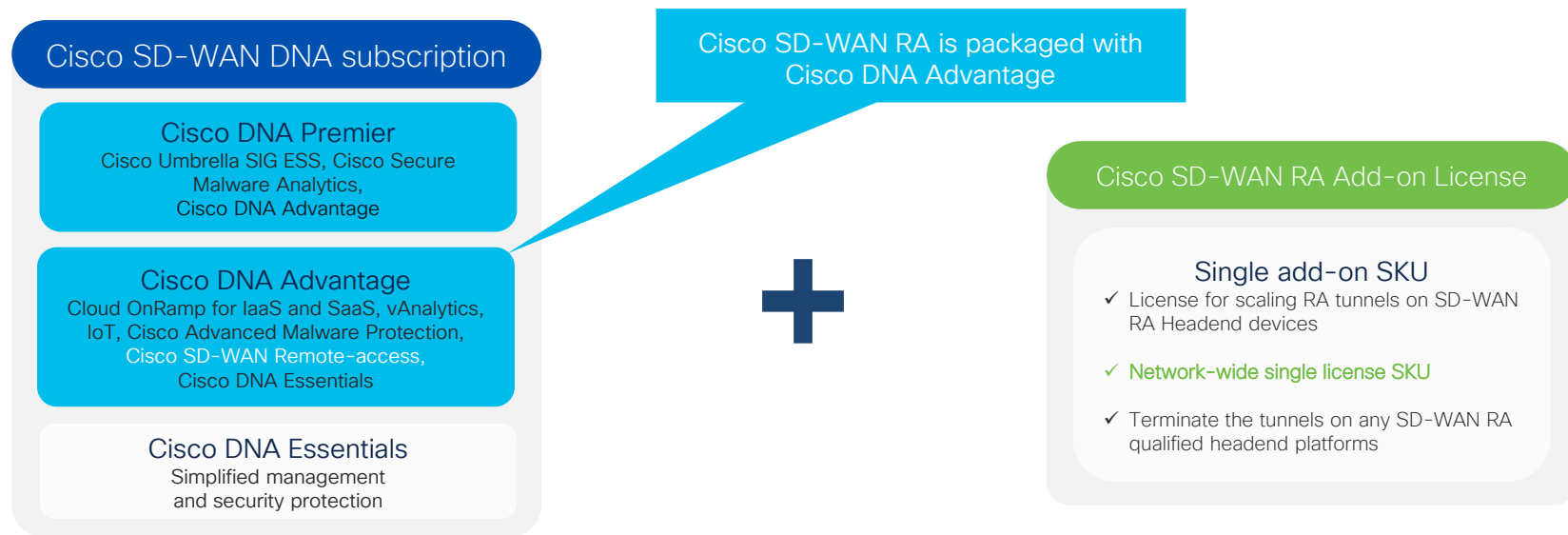
Virtual Access Interface config

IP pool config for RA Client

# Cisco SD-WAN RA Licensing



# Cisco SD-WAN RA Packaging & Licensing



A single add-on subscription SKU to transform your network to Hybrid work fabric

**NOTE**

Cisco AnyConnect Mobility Client end-point licenses are NOT included and they need to be ordered separately. Please go through: <https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-og.html>

# Roadmap



# Roadmap

## > XE SD-WAN 17.7

Dec 2021

### Phase-1 : Productization

- CLI-template support on vManage
- AnyConnect IPsec based RA VPN
- Macro Segmentation (VRF-Aware/SGT)
- Policing (ingress/egress) at SD-WAN TLOC
- RA Client split-Tunneling (Prefix Based)
- Enterprise CA / IOS-based CA
- Solution Licensing & Packaging

17.7

Platform Support - Catalyst8500, Catalyst8300

## \*Future Roadmap

### > Future Release

- vManage UI
- vManage Monitoring
- vManage CA server for RA certificate mgmt
- AnyConnect DUO integration
- AnyConnect SSLVPN RA (C8KV)
- Domain based split tunnelling

\* Feature-scoping on best-effort basis (Subject to change)

\*

Extend SD-WAN RA support on- C8KV & ASR1K

# SD-WAN RA Feature Support

Features Category	Features	XE-SD-WAN Releases 17.7	XE-SD-WAN Future Release
		Supported	Roadmap
AAA	<ul style="list-style-type: none"> <li>✓ Cisco ISE/Radius Server</li> <li>✓ Cisco IOS-XE CA server integration</li> <li>✓ Cisco EAP</li> </ul>	✓	
	<ul style="list-style-type: none"> <li>○ Cisco TACACS+, Cisco DUO support</li> </ul>	-	In Roadmap
RA Features	<ul style="list-style-type: none"> <li>✓ Standard IKEv2 features:</li> <li>✓ Macro Segmentation (VRF-Aware/SGT)</li> <li>✓ Policing (ingress/egress) at SD-WAN TLOC</li> <li>✓ RA Client split-Tunneling (Prefix Based)</li> <li>✓ RA Client DIA through SD-WAN RA Headend</li> <li>✓ Dual stack support</li> <li>✓ App QoE</li> </ul>	✓	
	<ul style="list-style-type: none"> <li>○ Per-Tunnel QoS</li> </ul>	-	In Roadmap
RA Security Features	<ul style="list-style-type: none"> <li>✓ ZBFW support on Virtual-Access</li> <li>✓ IP ACL</li> <li>✓ IP NA</li> </ul>	✓	
Redundancy	<ul style="list-style-type: none"> <li>○ SD-WAN RA Headend Redundancy (HA site)</li> </ul>	-	In Roadmap

# SD-WAN RA Feature Support

Features Category	Features	XE-SD-WAN Releases 17.7	XE-SD-WAN Future Release
		Supported	Roadmap
Management	<ul style="list-style-type: none"> <li>✓ vManage CLI template for Day0/Day-N configurations on SD-WAN RA Headend</li> <li>✓ ISE Monitoring for RA</li> </ul>	✓	
	<ul style="list-style-type: none"> <li>○ vManage Feature-template GUI for SD-WAN RA Headend</li> <li>○ vManage Monitoring of SD-WAN RA Headend</li> <li>○ vManage CA Server</li> </ul>	-	In Roadmap
Anyconnect VPN	✓ IPsec based VPN	✓	
	○ SSL based VPN for C8Kv	-	In Roadmap
ASA AnyConnect Feature Parity	✓ Prefix Based split tunnelling	✓	
	<ul style="list-style-type: none"> <li>○ Domain based split tunnelling</li> <li>○ ISE Posture management for Anyconnect clients</li> </ul>	-	In Roadmap
Application Visibility & Control	✓ FNF, AVC, NBAR, DPI, App-aware Policy	✓	

# Platform Support

Platform Series	Platform Support	XE-SD-WAN Releases 17.7	XE-SD-WAN Future Release
		Supported	Roadmap
Cisco Catalyst 8500 series	Catalyst 8500-12X Catalyst 8500-12X4QC Catalyst 8500L	✓	
Cisco Catalyst 8300 Series	Catalyst 8300-1N1S-6T Catalyst 8300-2N2S-4T2X	✓	
Cisco Catalyst8000v (On-Prem)	Catalyst8000v	✓	
Cisco Catalyst8000v* (AWS)	-	-	In Roadmap
Cisco Catalyst 8200 series			In Roadmap
Cisco *ASR 1000 series (Fixed) ASR1001X, ASR1002X ASR1001-HX, ASR1002-HX	-	-	In Roadmap



# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](https://www.cisco.com/go/certs)

## Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



## Learn

### Cisco U.

IT learning hub that guides teams and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology, and certification training

### Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

### Cisco Learning Network

Resource community portal for certifications and learning



## Train

### Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



## Certify

### Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

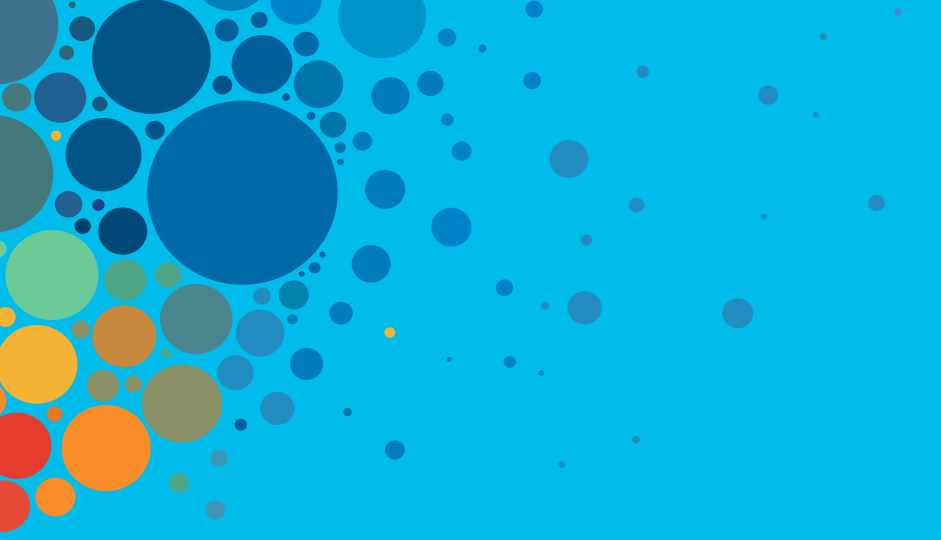
### Cisco Guided Study Groups

180-day certification prep program with learning and support

### Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



# Continue your education

- SDWAN-RA Lab  
session LTRARC-2440
- Visit the Cisco Showcase  
for related demos
- Book your one-on-one  
Meet the Engineer meeting
- Attend the interactive education  
with DevNet, Capture the Flag,  
and Walk-in Labs
- Visit the On-Demand Library  
for more sessions at  
[www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*



#CiscoLive