Cisco Secure Access

Cisco Secure Access Unveiled

Anders Piilmann - Solution Engineer
apiilman@cisco.com

BRKSEC-1586

A little about me

- I have **29 years** of experience in the network and security
- Covered operations, design, and architecture.
- I have experience with most of the vendors in IT infrastructure and security.
- Done architecture, design, and leading implementations of solutions ranging from 100k+ of users down to SMBs.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is session about

- This session is a technical introduction to Cisco Secure Access
- Typical Use Cases
- Cisco Secure Access high level architecture
- Which components make up Cisco Secure Access

- So, if you are already familiar with Cisco Secure Access this session is probably not for you ☺

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is this session NOT about

How to configure Cisco Secure Access

Deep technical dive

How to sell Cisco Secure Access

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction to CSA
- The Architecture of CSA
- SD-WAN Integration
- Resource Connector
- Private Application Access (ZTNA) and Remote Access VPN
- Digital Experience Monitor

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Let’s dive in

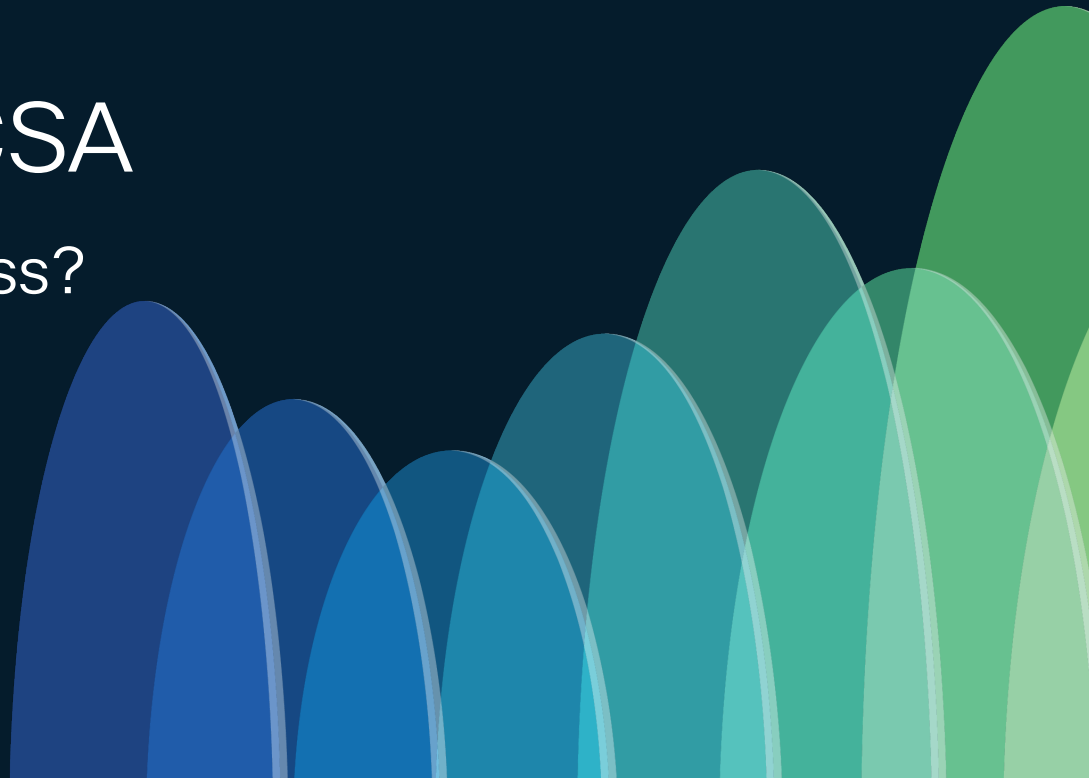
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Access gives your users easy and consistent access from anywhere in world.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

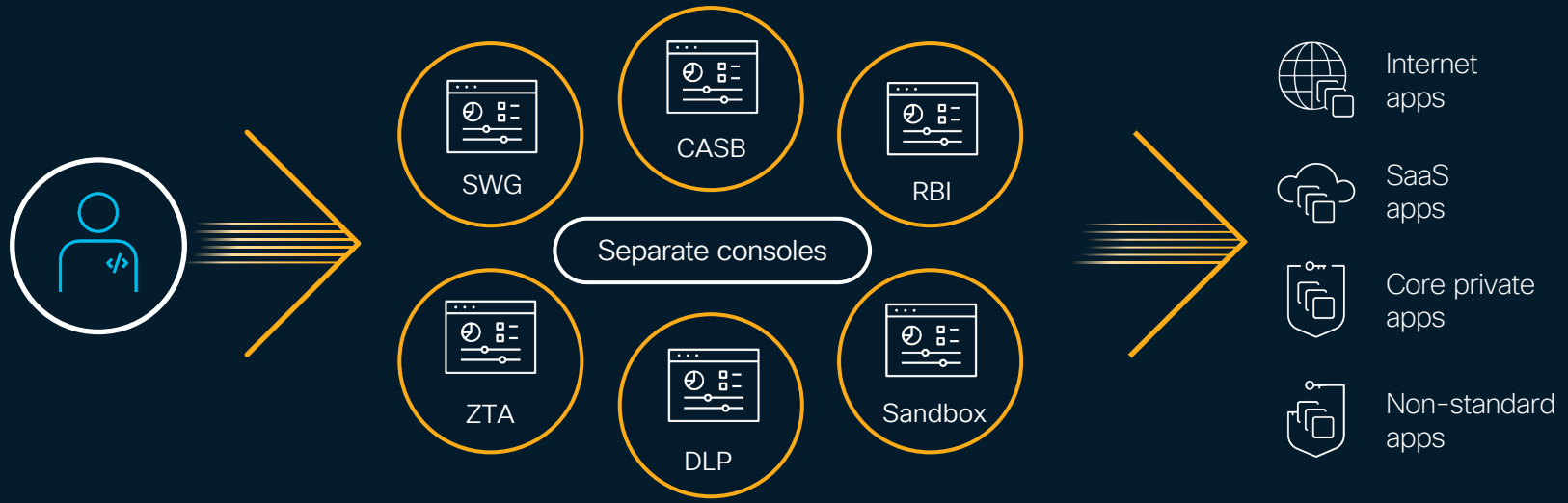
Introduction to CSA

Why Cisco Secure Access?



cisco Live!

IT Challenges

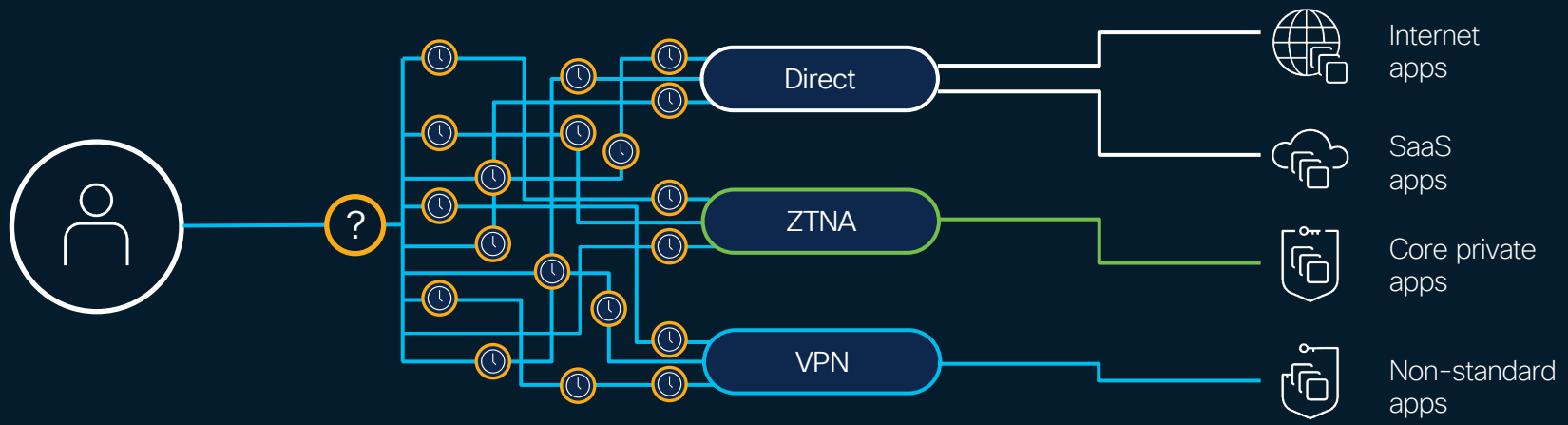


Multiple products increase cost and inefficiencies

- Licenses/hardware
- Policy management
- Client management
- Reporting
- Elevated staffing levels

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

User Challenges

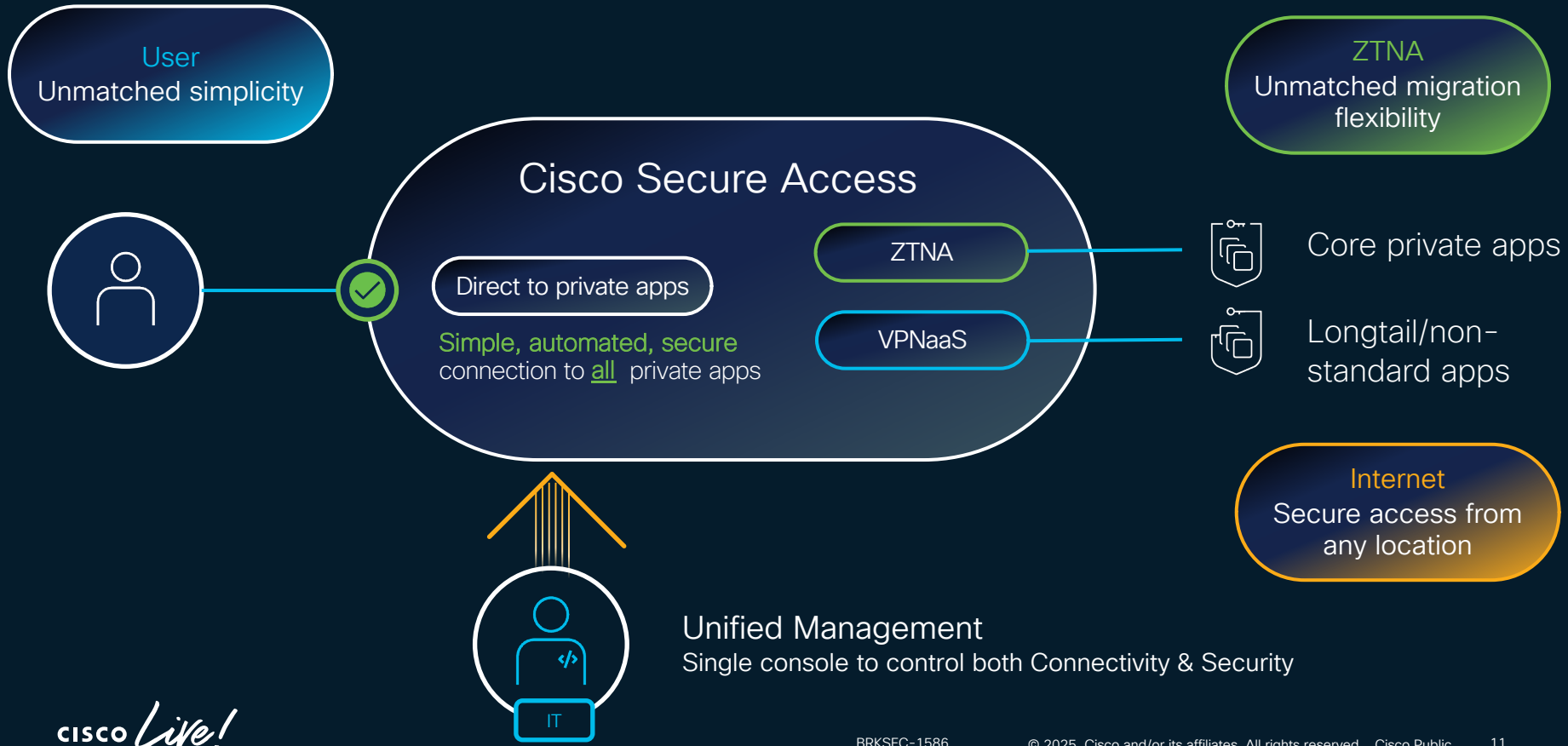


Varying connectivity methods ultimately create frustration

- Many connection decisions
- Various processes
- Multiple steps
- Repetitive authentication tasks

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

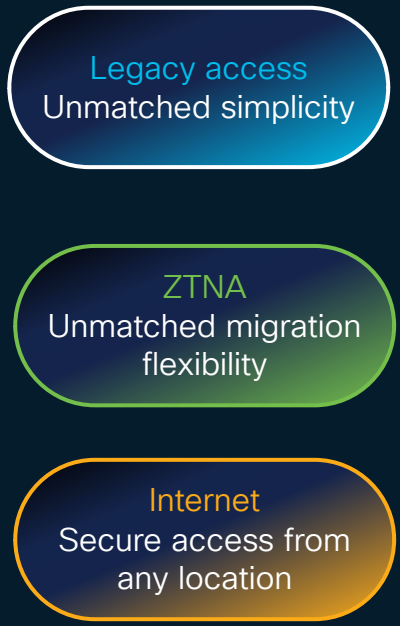
Modernize remote access to all private apps, and the Internet. In one unified solution



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

What are the primary Use Cases for CSA

- VPNaaS (typically for legacy applications)
- Private Application Access (cloud/private cloud, on-prem)
- Secure Internet Access

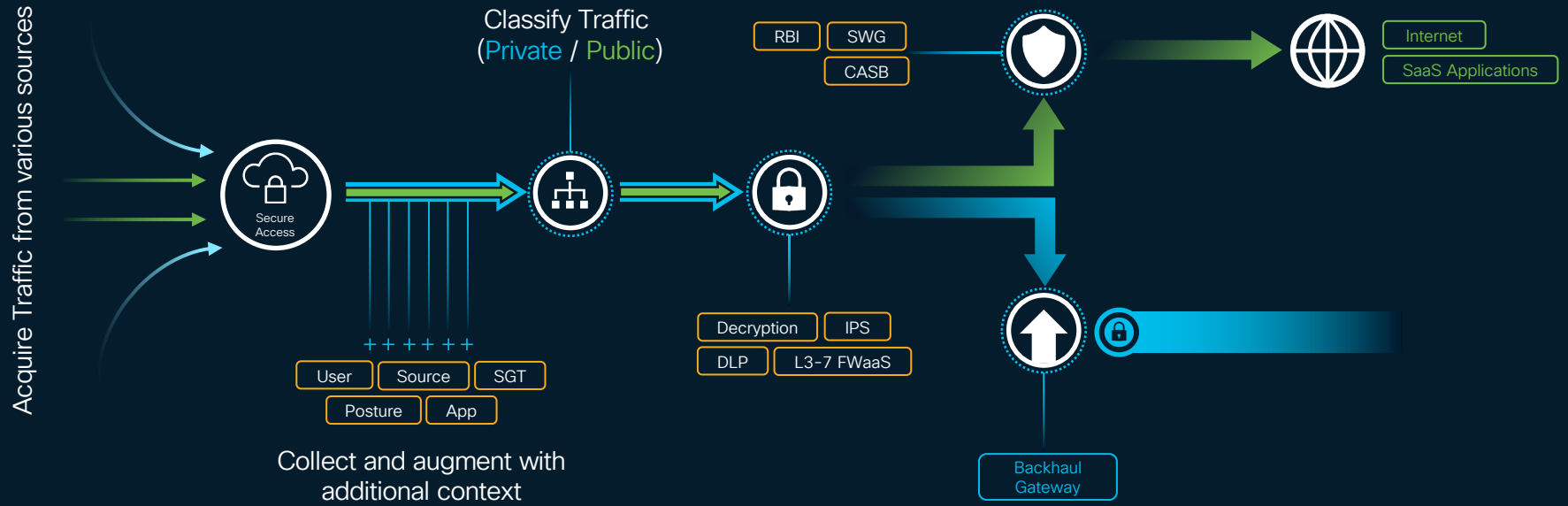


© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Architecture of CSA

Unified Cloud Architecture

Universal Traffic Acquisition & Single Data Path



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unified Cloud Architecture

Unified Policy Evaluation

941 Rules

Change view

	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
1		Any employee access to any...	Private	Allow	Any User... +3	Any Applic... +1		4.1K	
2		US-Canada Employees	Private	Block	North Ame... +4	Company... +4		1.2K	
3		Product Management Resour...	Internet	Warn	PM User Gr... +1	Product M... +2		924	
4		Europe Content Block List	Internet	Isolate	Europe Em... +7	EU Catego... +7		–	
5		Contractors access to Lab App	Private	Allow	Contractor... +6	Lab Applic... +9		1.2M	
6		Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	
7		Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	
8		Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	
9		Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	
10		Workday resources	Internet	Block	Any User G... +7	Cisco Wo... +12		73K	

Rows per page 100 1 2 ... 5

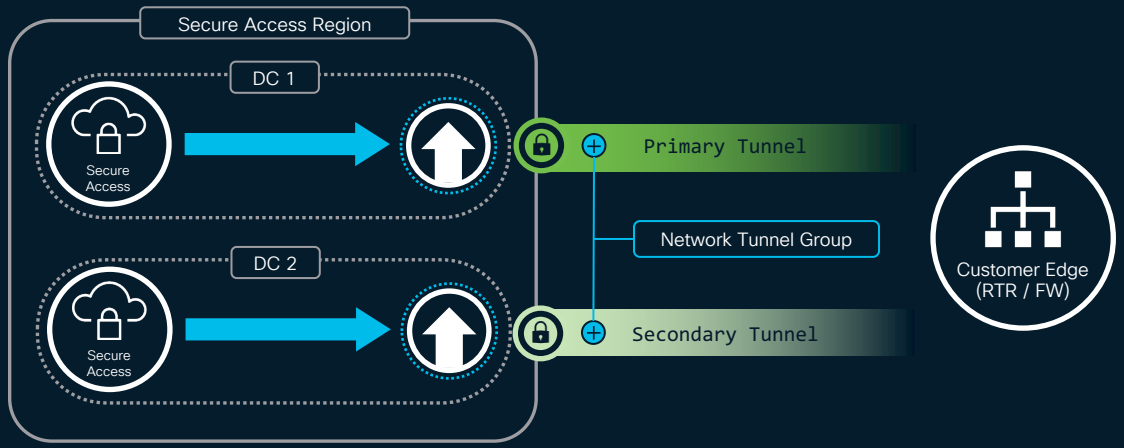
Default Access Rules

Rule name	Action	Sources	Destinations	Security	Posture
For all private destinations	Block	Any	Any private destination	–	–
For all internet destinations	Allow	Any	Any internet destination		–

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Connectivity

IPSec & SD-WAN Tunnels



Performance

- IPsec Support for any hardware
- Intra-DC Failover
- IKE Dead Peer Detection
- BGP Keep Alive
- ECMP (Across multiple tunnels)
- Up t0 8x Tunnels per group
- 1Gbps / Tunnel

Routing

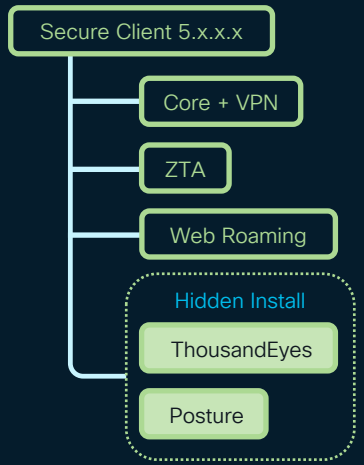
- Static Routes – manually configured
- BGP Peering, 1 neighbor per tunnel

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

End User Connectivity

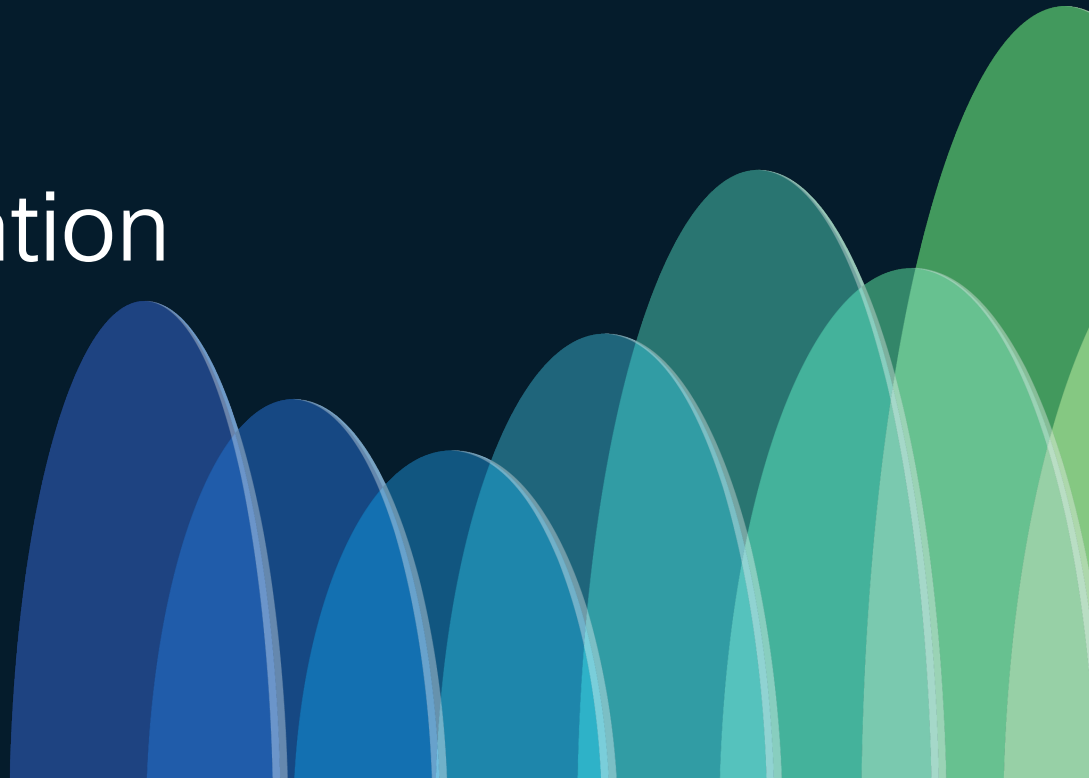
Remote User – Managed Endpoint

- Single Installer
- Customizable modules



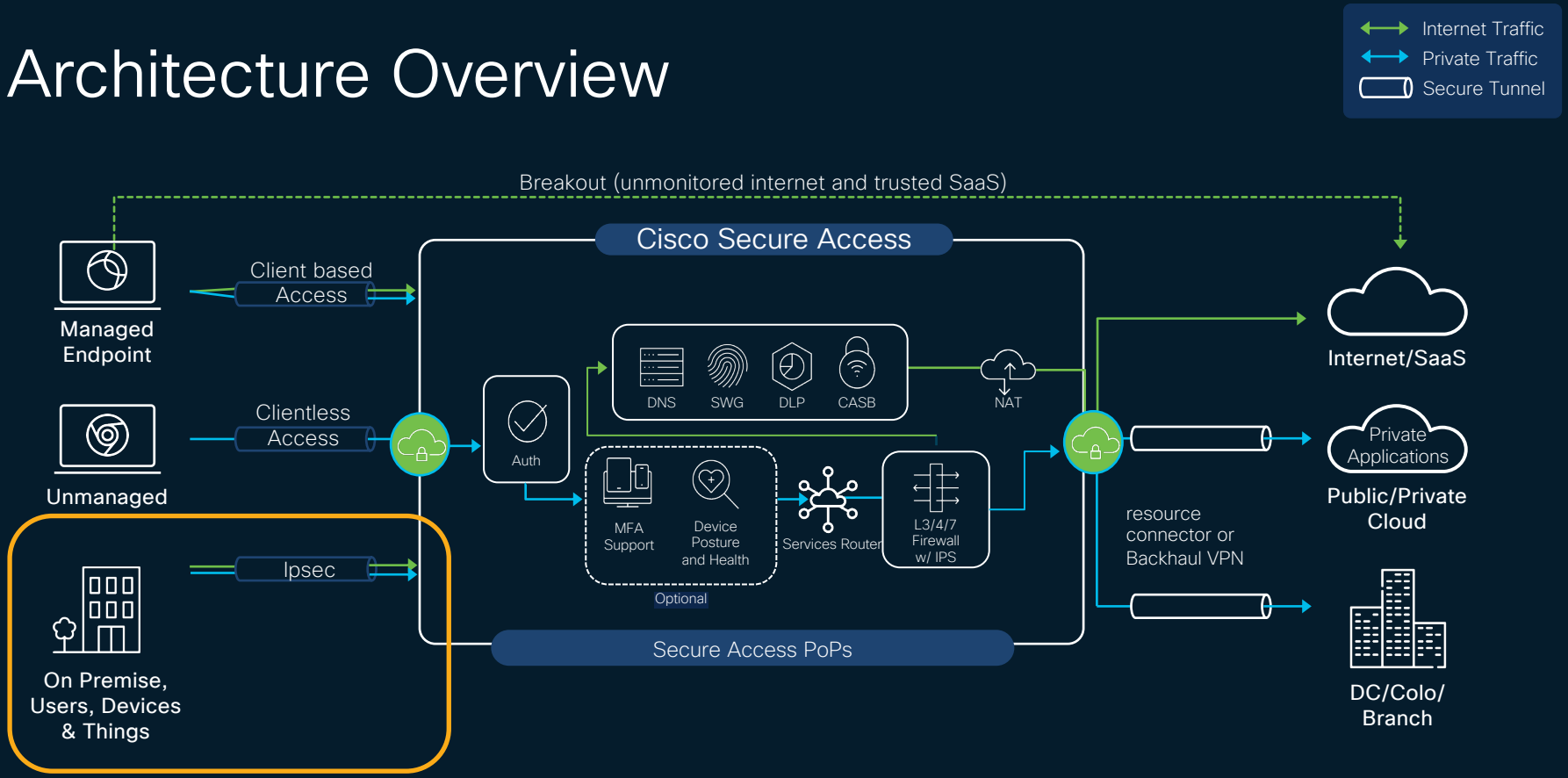
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN Integration



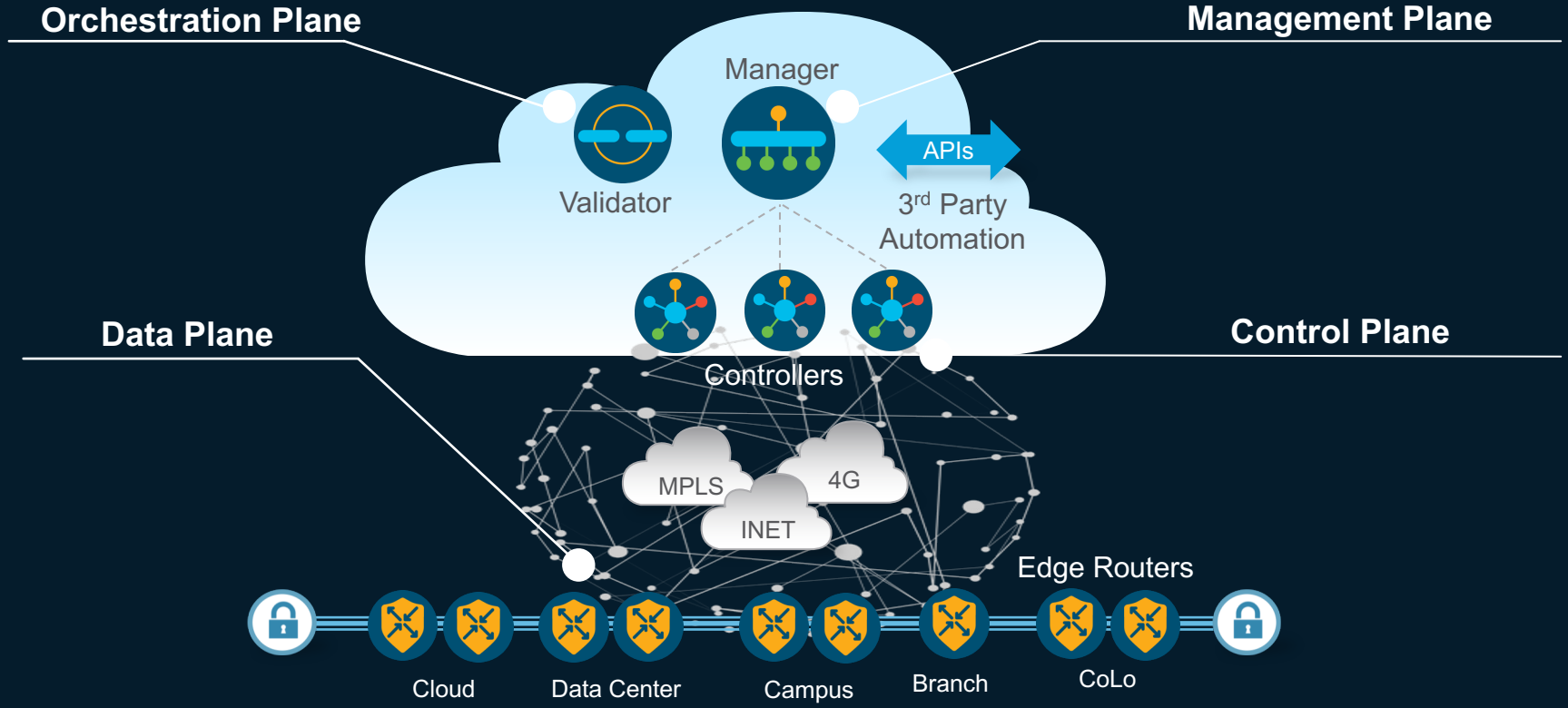
cisco Live!

Architecture Overview



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is Software Defined WAN (SDWAN)?

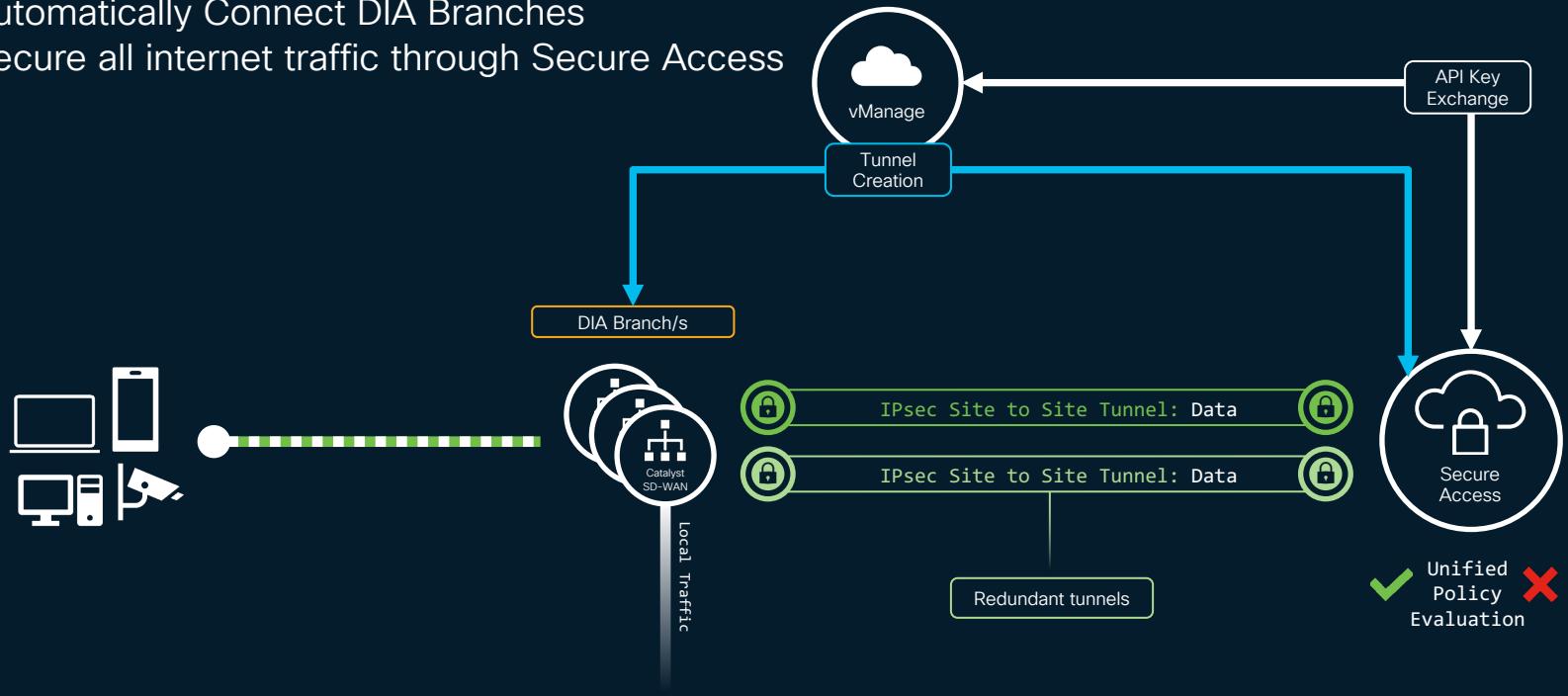


© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Device

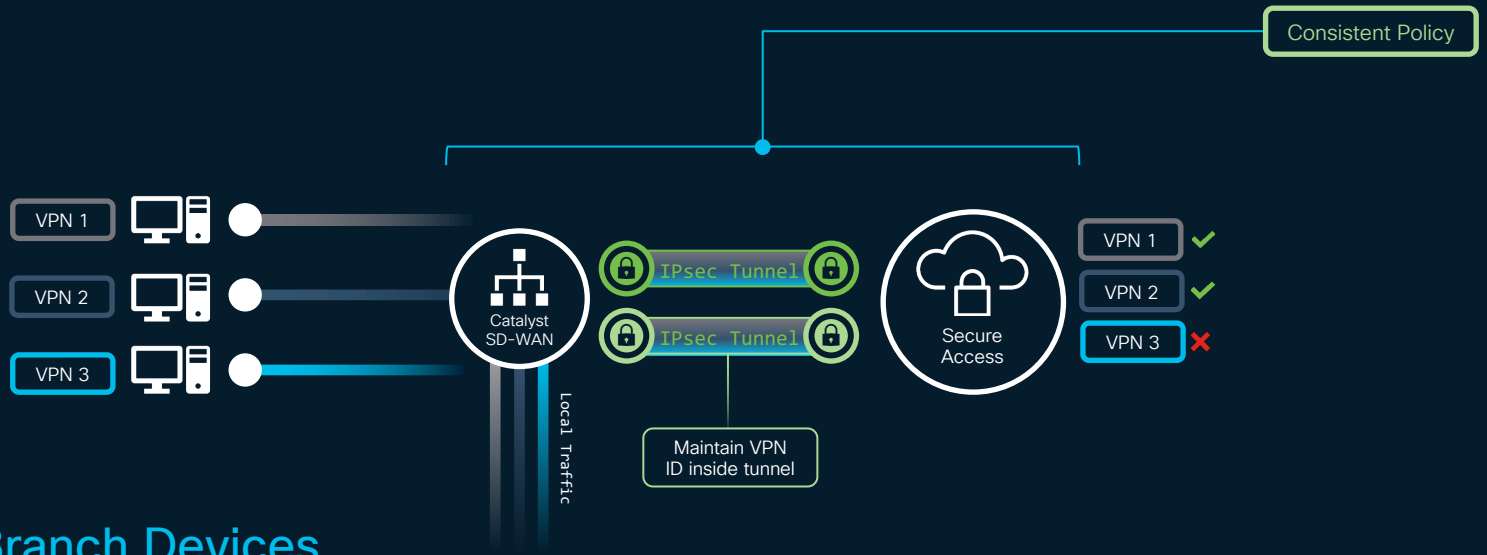
Tunnel Connectivity (DIA w/ Catalyst SD-WAN)

- Automatically Connect DIA Branches
- Secure all internet traffic through Secure Access



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Catalyst SD-WAN Integration

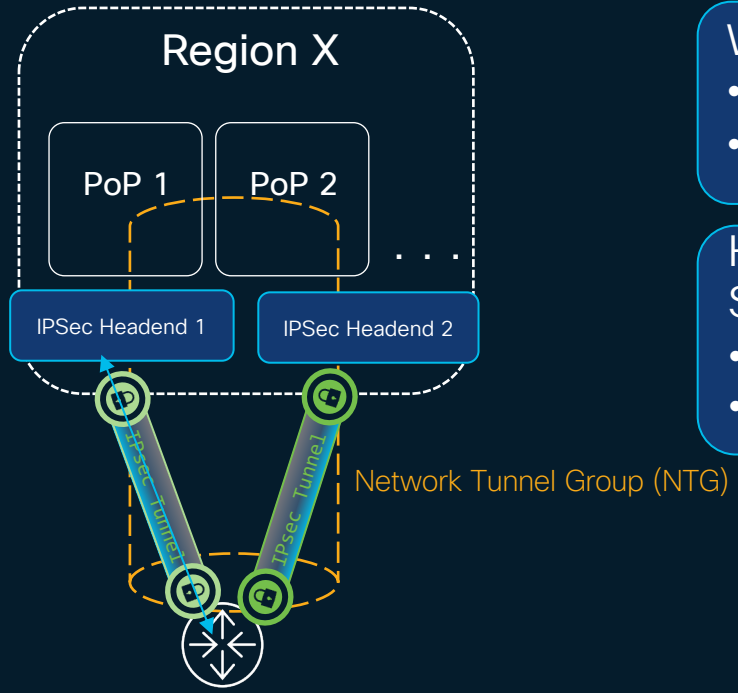


Branch Devices

- VPNID Based policy across both SDWAN & Secure Access
- Maintain Segmentation in branch & in the cloud
- All internet traffic is routed to Secure Access
- Auto Tunnels with Catalyst SD-WAN for Secure Internet Access

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

High Availability (SDWAN)



When do we switch from Primary to Secondary?

- DC out of rotation
- DC outage

How does CAT SDWAN switch from Primary to Secondary?

- API endpoint when static routing is enabled
- BGP

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

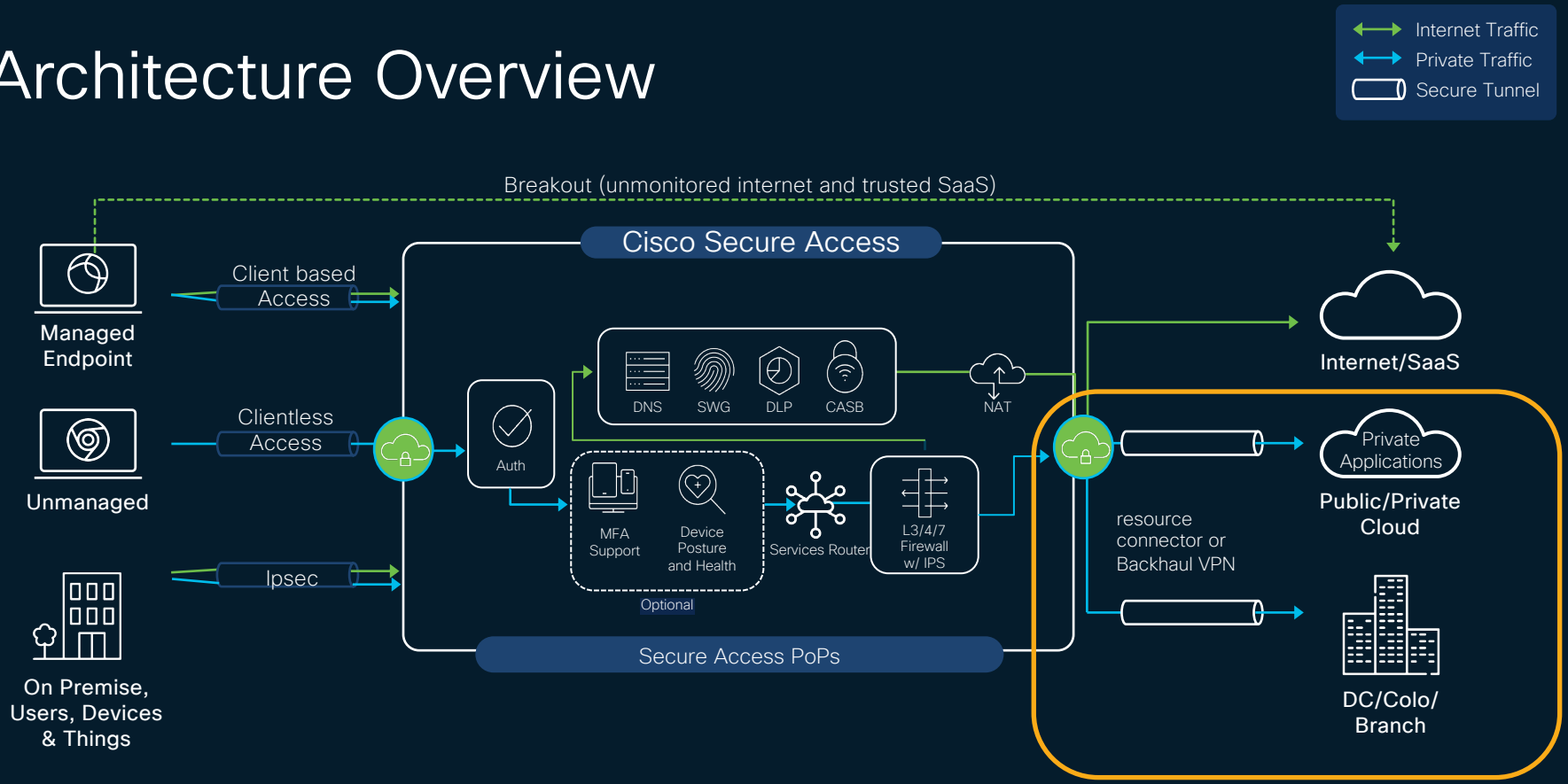
Key highlights

- Redundancy is based on BGP or API
- Fully integrated into Catalyst SD-WAN (Auto tunnel config)
- VPNID Support
- Auto Configuration Support
- Two types of redundancy:
  - Secure Access side: 1 primary DC and 1 secondary DC.
  - Client side:
    - Active/Active: both devices send traffic to IPSec headend. IPSec headend ECMP on the return path.
    - Active/Standby: Active device must advertise routes to IPSec headend with higher priority

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

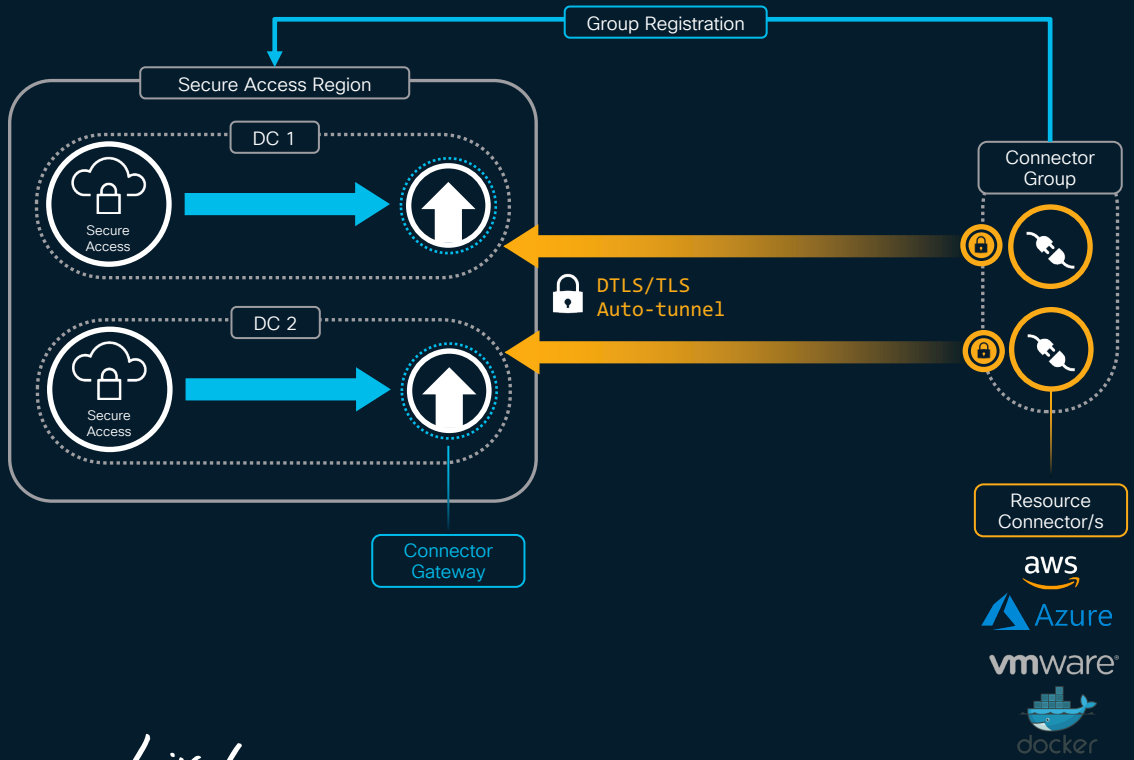
Resource Connector

Architecture Overview



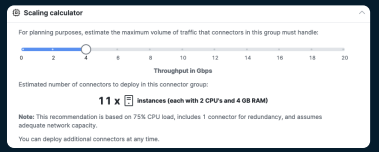
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Resource Connectors Connectivity



Performance

- Cloud side load balancing intra group + region
- 2x Connector / group recommended
- Cloud Managed (add/revoke/disable)
- Horizontal Scaling inside group
- 500Mbps / Connector

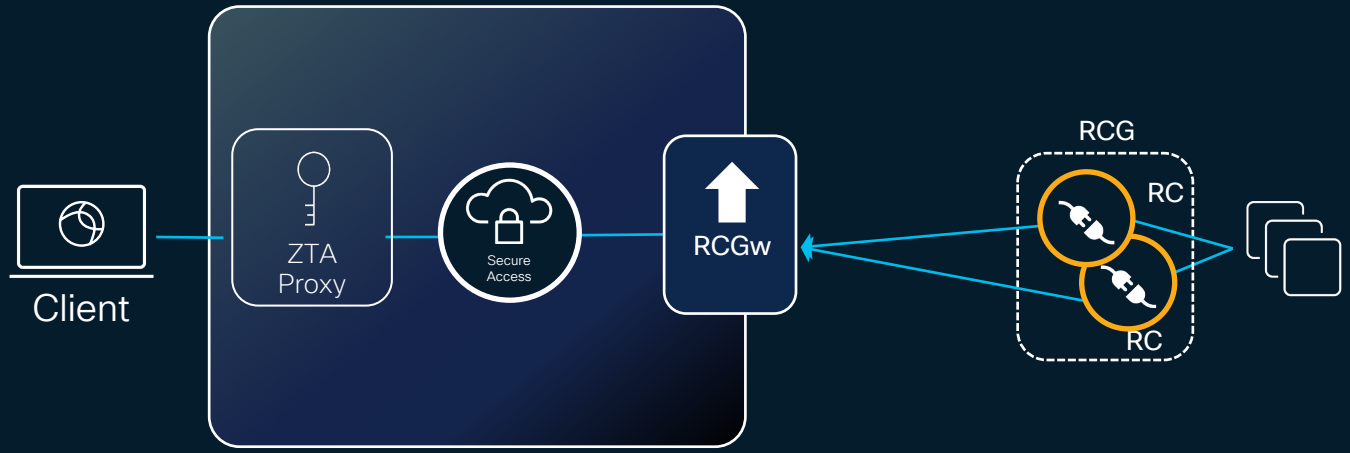


Routing

- Network Agnostic
- Support overlapping IPs

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Resource Connector Components



- Resource connector Gateway (RCGw) – Secure Access Edge for private app connectivity
- Resource connectors (RC) – Hosted on customer's Premises (On-Prem/Cloud)
- Resource connector Group (RCG) – Logical grouping of resource connectors for Scaling and Redundancy, All resource connectors within a group will connect to the same RCGw

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Differentiate with QUIC and MASQUE

QUIC:

A fast, secure web transport protocol over UDP

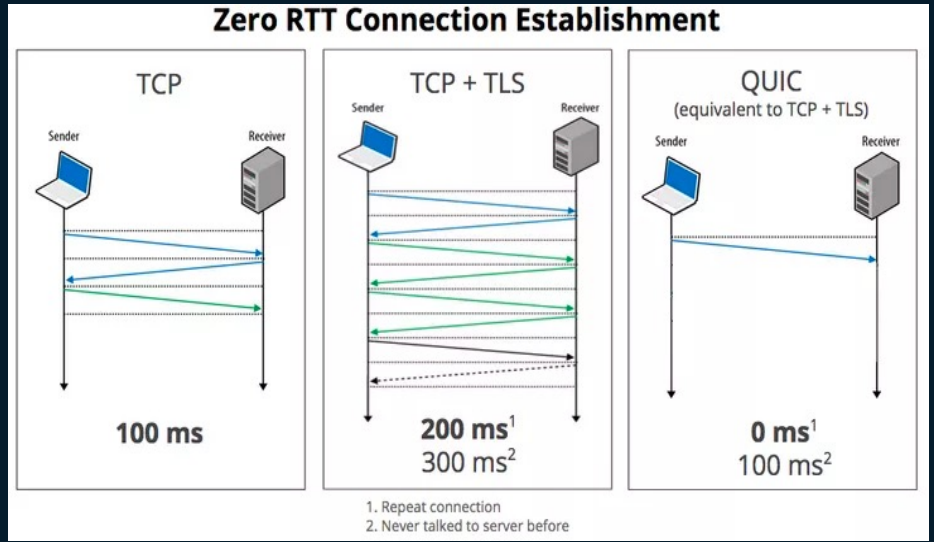
Provides its own layer of security, packet loss detection, data recovery, and congestion control.

HTTP/3 is based on QUIC

MASQUE:

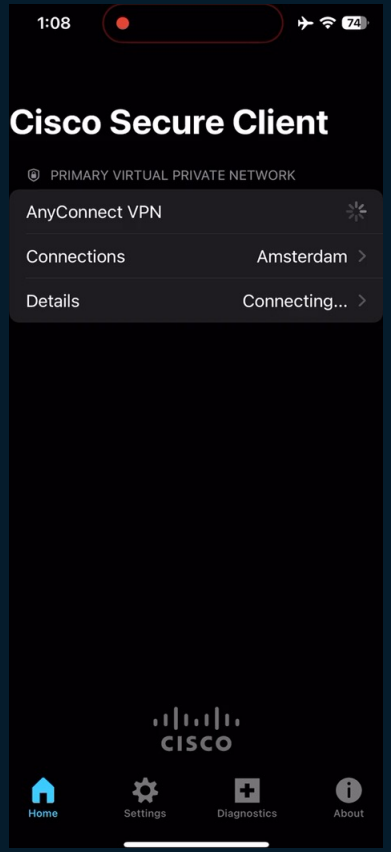
A proxy that routes multiple apps over one QUIC connection.

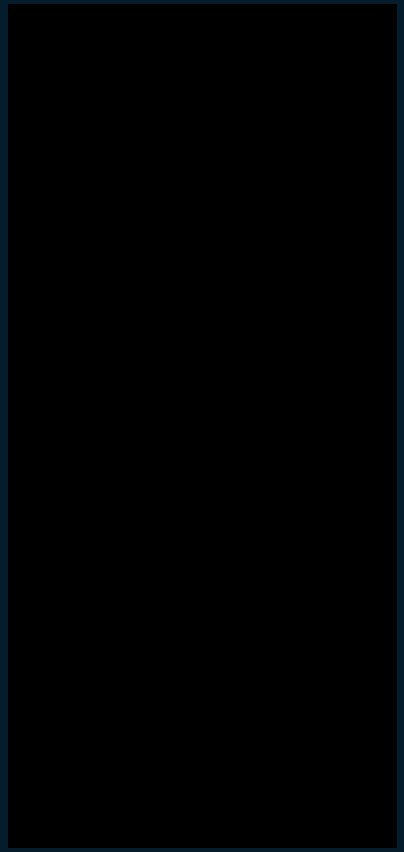
Efficient without little overhead.



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

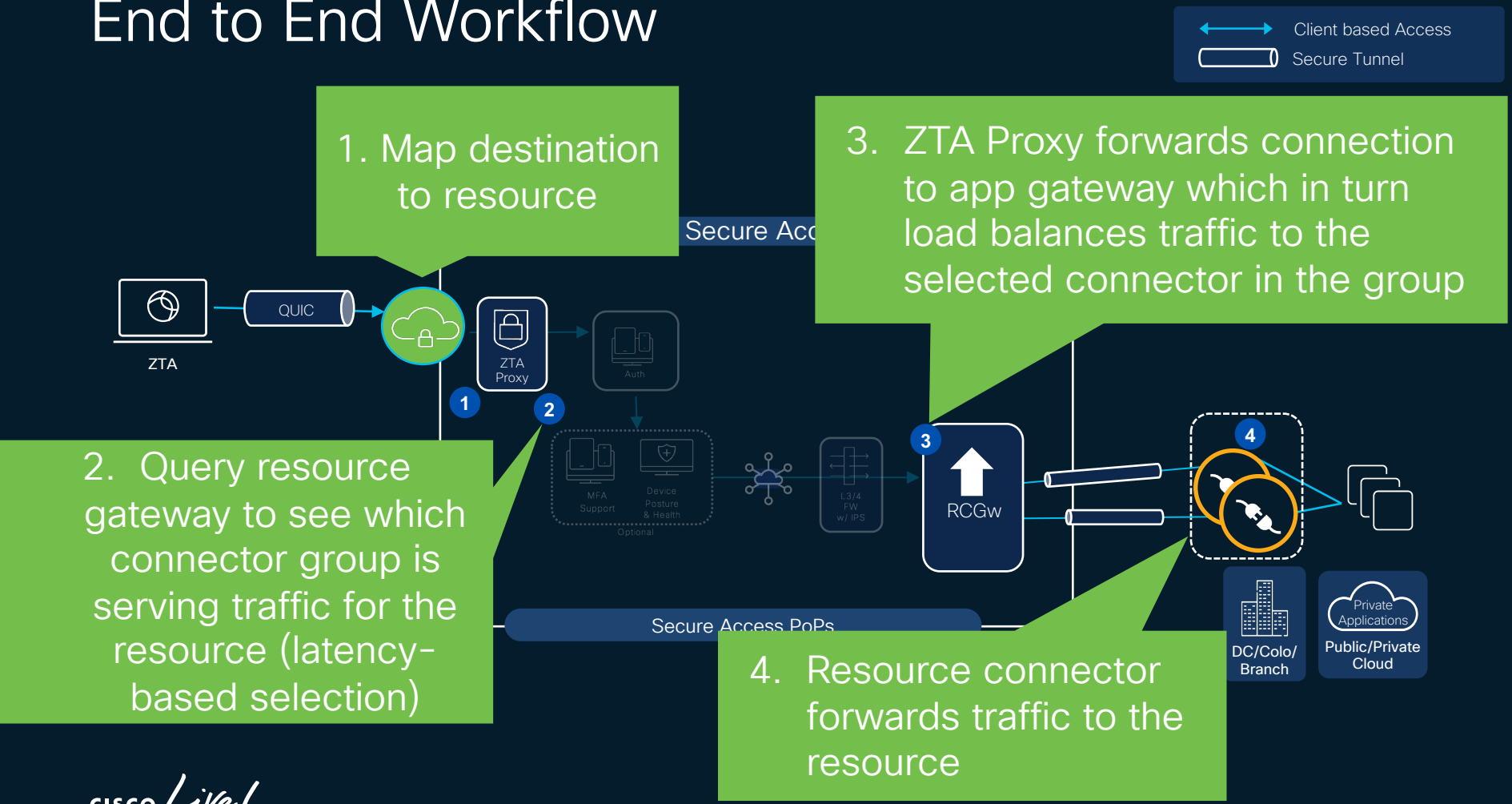
A Side by Side comparison from an Airplane WiFi





© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

End to End Workflow



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Benefits

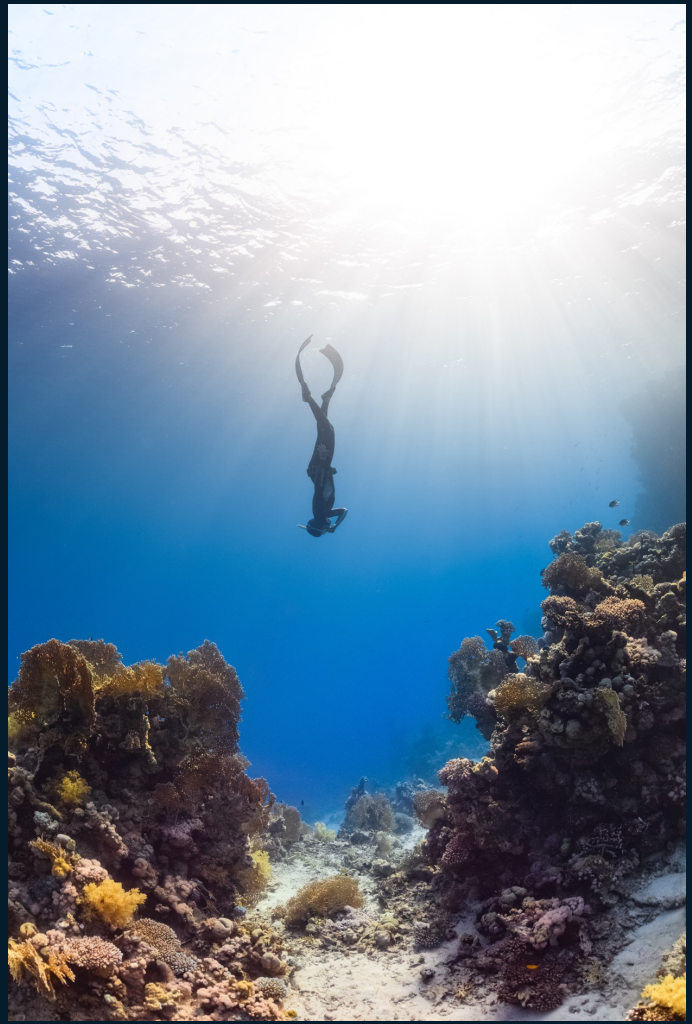
- Virtual appliance connector, deployed in front of private applications
- Simplified deployment vs IPSEC VPN
- All ports and protocols supported
- Automatic tunnel establishment using OUTBOUND connections only
- Minimize routing complexities
  - No setting up dynamic routing
  - Supports Overlapping subnets
  - Easy to Scale with high availability

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Access gives your users easy and consistent access from anywhere in world.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

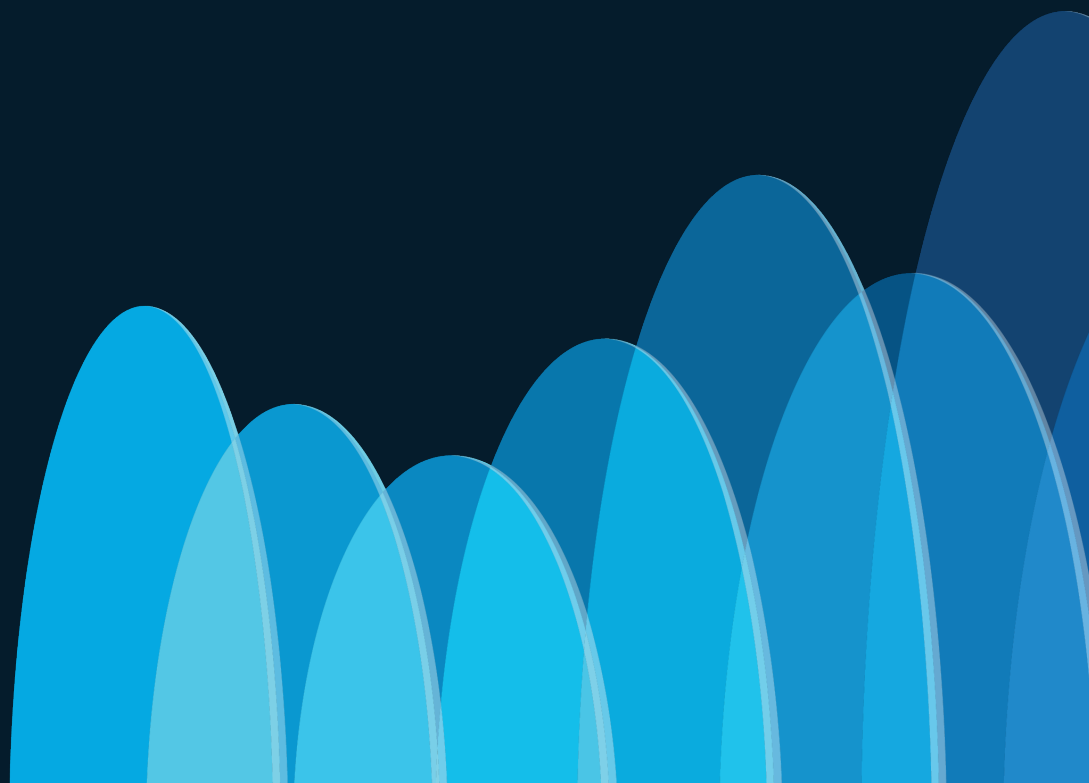
Let’s go a bit deeper....



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

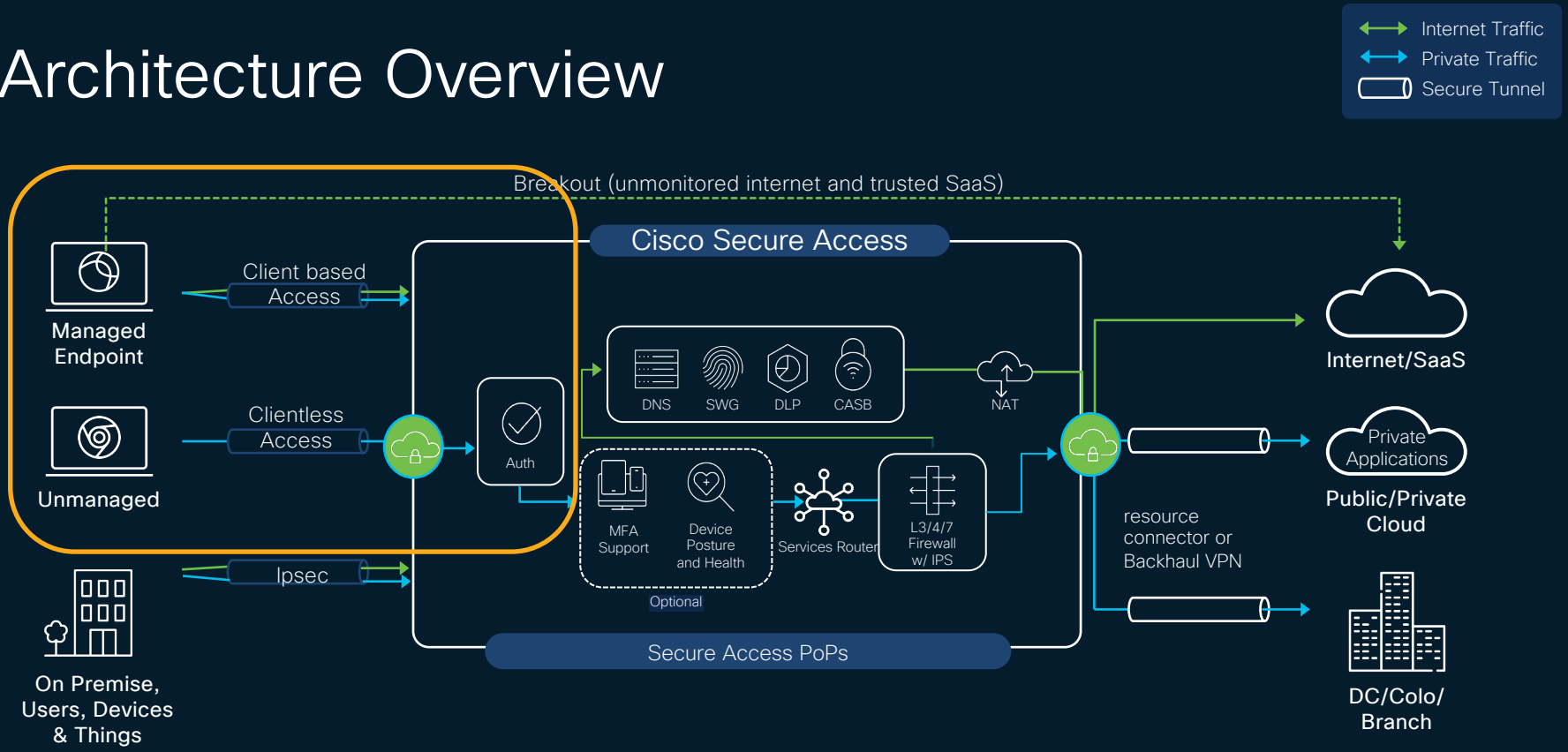
Private Application Access (ZTNA)

And Remote VPN



cisco Live!

Architecture Overview



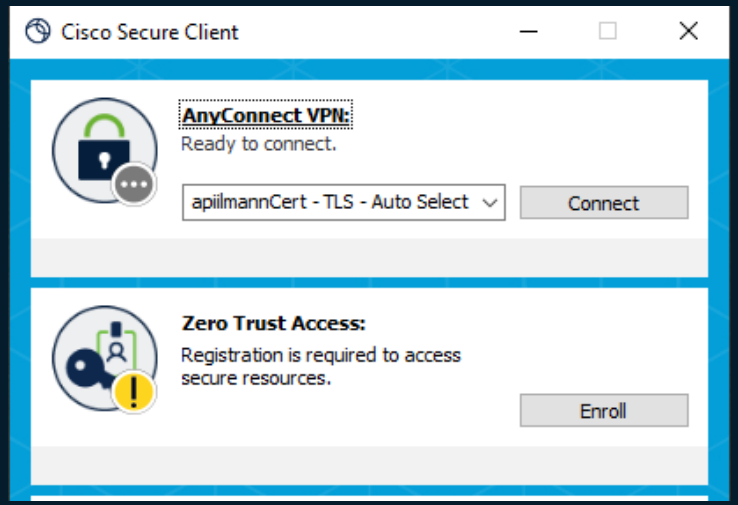
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Access: Simple, frictionless user experience

Note: Supports both client and clientless ZTNA connectivity

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Client Zero Trust Access Module

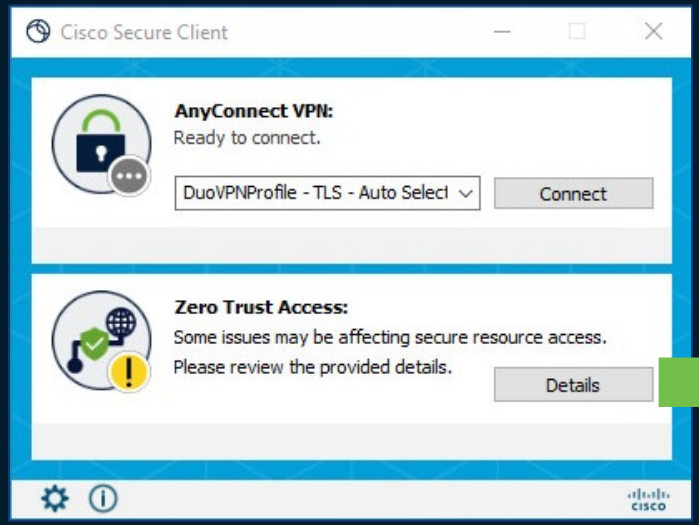


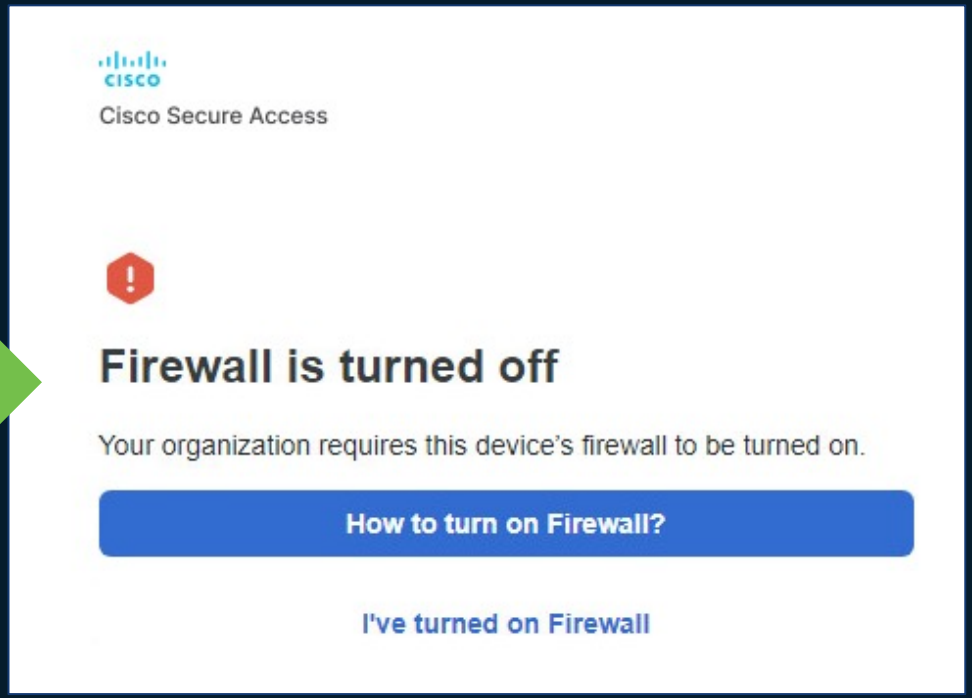
- Transparent user experience (When enrolled)
- Service managed client certificates with TPM/hardware enclave key storage

- Support for both TCP and UDP applications
- Cisco and third-party VPN client interop
- Next-generation protocol (MASQUE + QUIC)

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

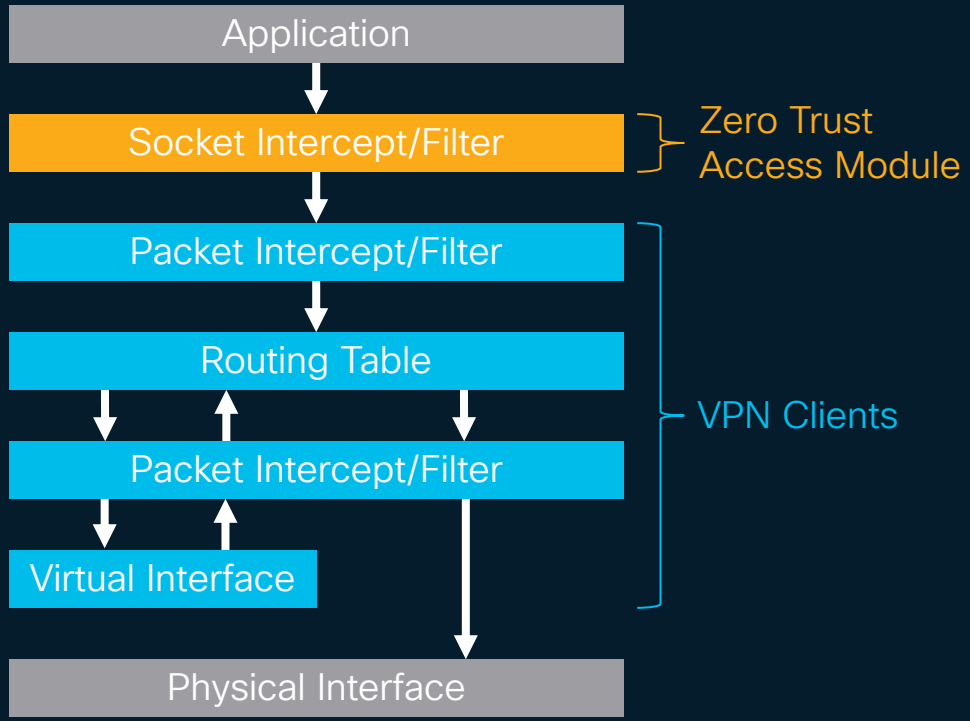
Client based Posture





© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Client ZTA Module: Socket Intercept



Why Socket Intercept?

- Control of DNS and application traffic *before* VPN clients
- No route table manipulation
- Ability to capture traffic by IP, IP subnet, FQDN and FQDN wildcard
- Interoperability with Cisco and non-Cisco VPNs

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Posture

Authorization check prior to application access

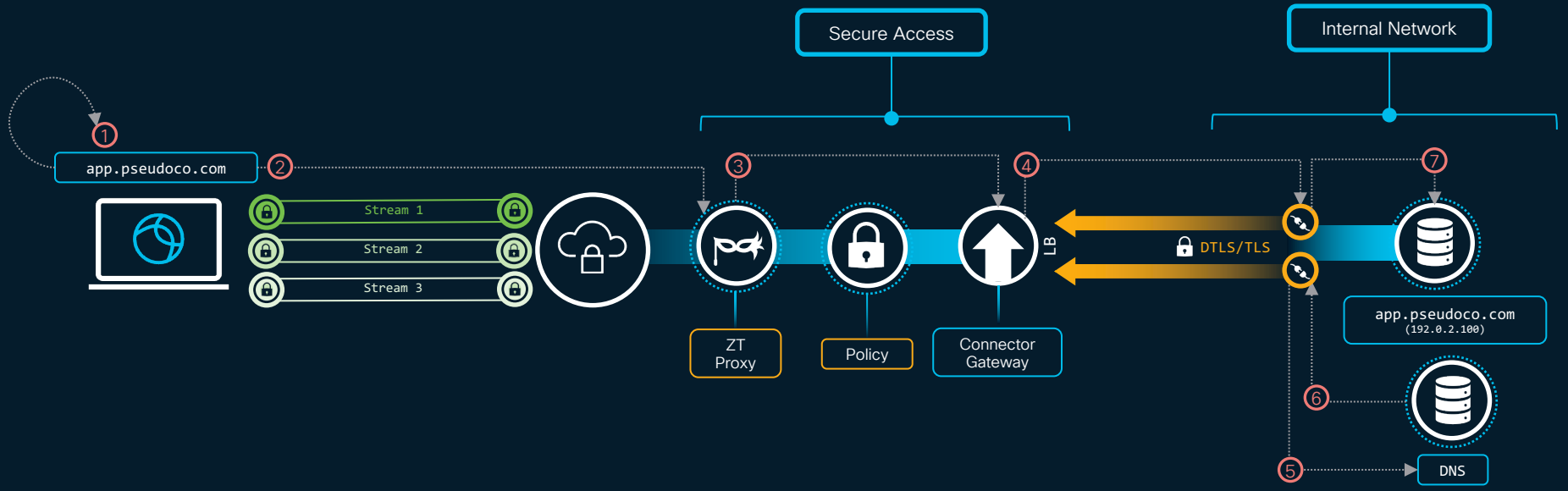
Authorization and access check per session

	VPN	ZTNA Browser	ZTNA Client-based
Operating System	✓	✓	✓
Geolocation Check (moved to access policy)	✓	✓	✓
Anti-Malware	✓		✓
Firewall	✓		✓
Disk Encryption	✓		✓
Certificate Check	✓		
Browser Check		✓	
System Password			✓
File Check	✓		
Registry Check (windows only)	✓		
Process Check	✓		

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

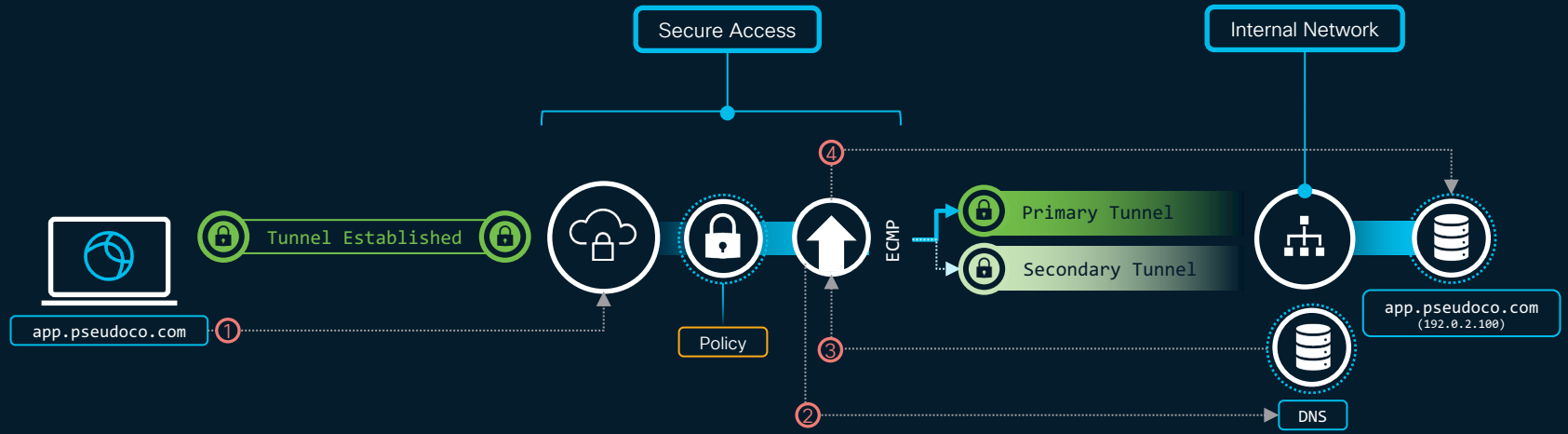
Secure Private Access using the ZTNA Client

Zero Trust Access to Resource Connectors



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Private Access using the RA-VPN Client



1. User Connected to VPNaaS requests DNS resolution from VPN-Pool DNS, App traffic sent down Tunnel
2. Secure Access Requests DNS resolution from internal DNS
3. Secure Access receives IP Address and Evaluates Policy
4. Secure Access routes traffic via Tunnel to App

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Benefits

- Same client for VPN and ZTNA (Cisco Secure Client)
- No need for on-prem concentrators
- All configuration done in the same dashboard
- Clientless support
- Built-in posturing
- Transparent for the end users

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Access gives your users easy and consistent access from anywhere in world.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Digital Experience Monitor

cisco Live!

Digital Experience Monitoring

Monitor the health and performance of users, applications, and network connectivity.

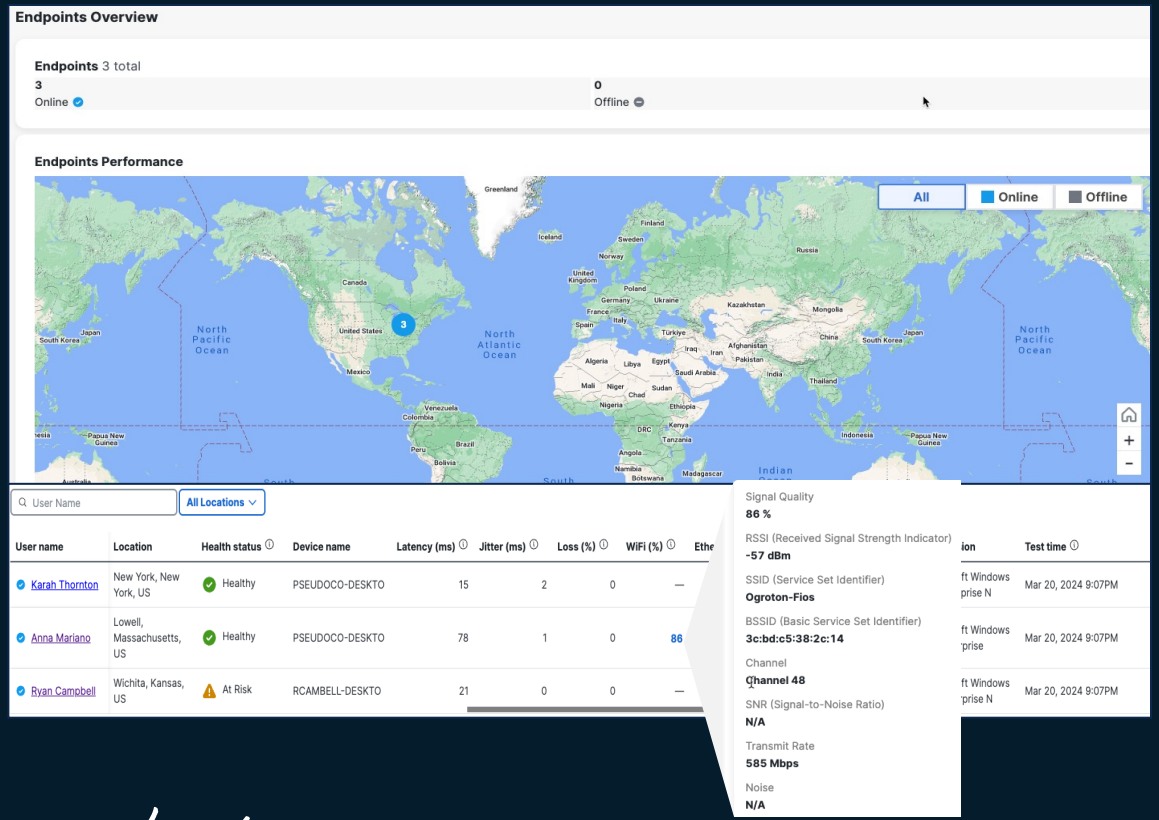
Optimize user productivity by automatically mining details on the user's end-to-end experience, enabling the IT/security staff to rapidly resolve the issue.

DEM monitoring examples:

- Endpoint performance – CPU, memory, Wifi
- Network performance –endpoint to Secure Access
- Top 20 SaaS applications performance
- User specific events

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Access Experience Insights



- Global visibility of registered endpoint status
- Is part of the Cisco Secure Access dashboard
- Includes ThousandEyes Embedded Endpoint Agent(EPA) as a module in Cisco Secure Client

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Top 20 SaaS Applications Health

Top 20 SaaS applications performance 1 London

You can see top 20 SaaS applications performance per region.

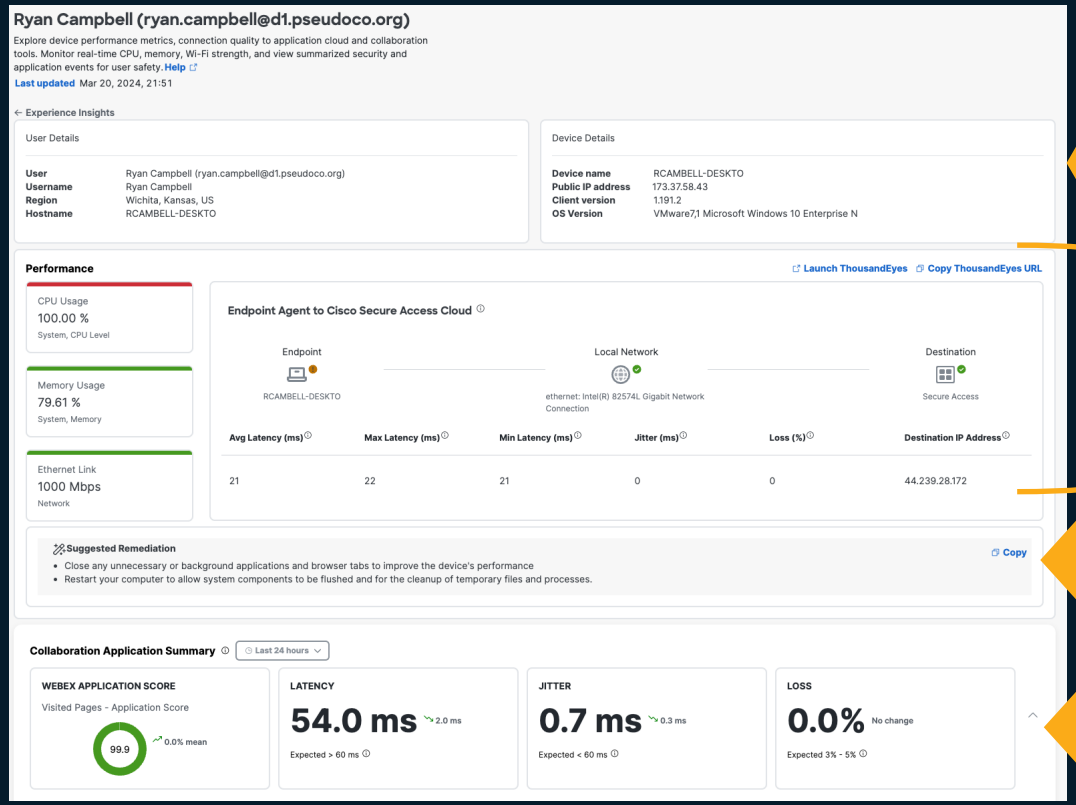
Search

Application	Reachable	URL (Domain)	Loss (%)	Avg Latency (ms)	Jitter (ms)	Type	Region	Time
Mail	✓	mail.ru	0,0	1.0	0.0	ping	London	2023-07-13 12:14:15
Outlook	✓	outlook.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Miro	✓	miro.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Slack	✓	slack.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Gmail	✓	slack.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Salesforce	✓	salesforce.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Box	✓	box.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Figma	✓	figma.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15
Notion	✓	notion.com	0.0	1.0	0.0	ping	London	2023-07-13 12:14:15

Rows per page 10 < 1 2 ... 10 >

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Digital Experience Monitoring



Connected user details: Identify local wifi, CPU, memory errors that influence connectivity to apps

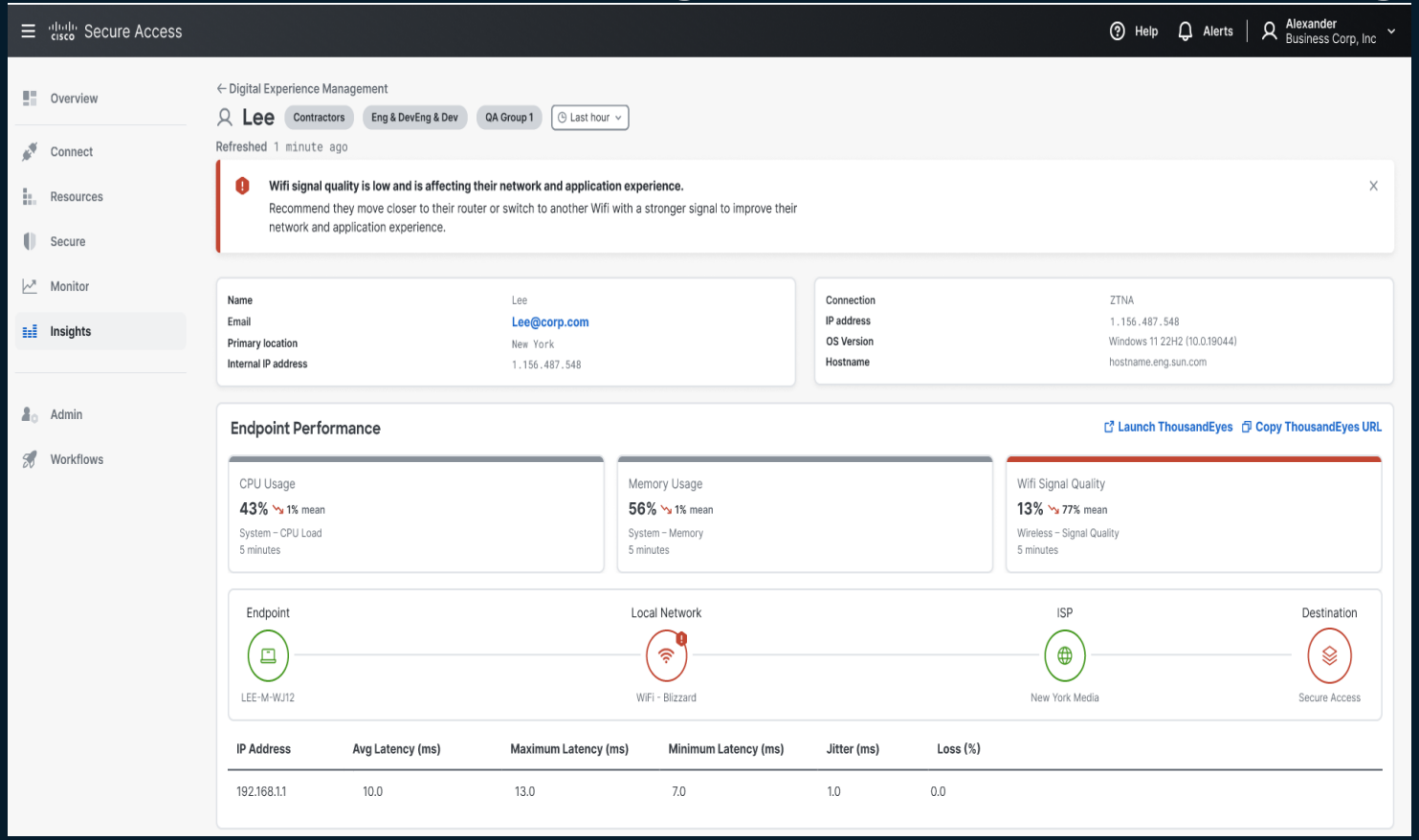
Connection quality from endpoint to Secure Access

Suggested remediation tips to help reduce mean time to resolution

UcaaS monitoring

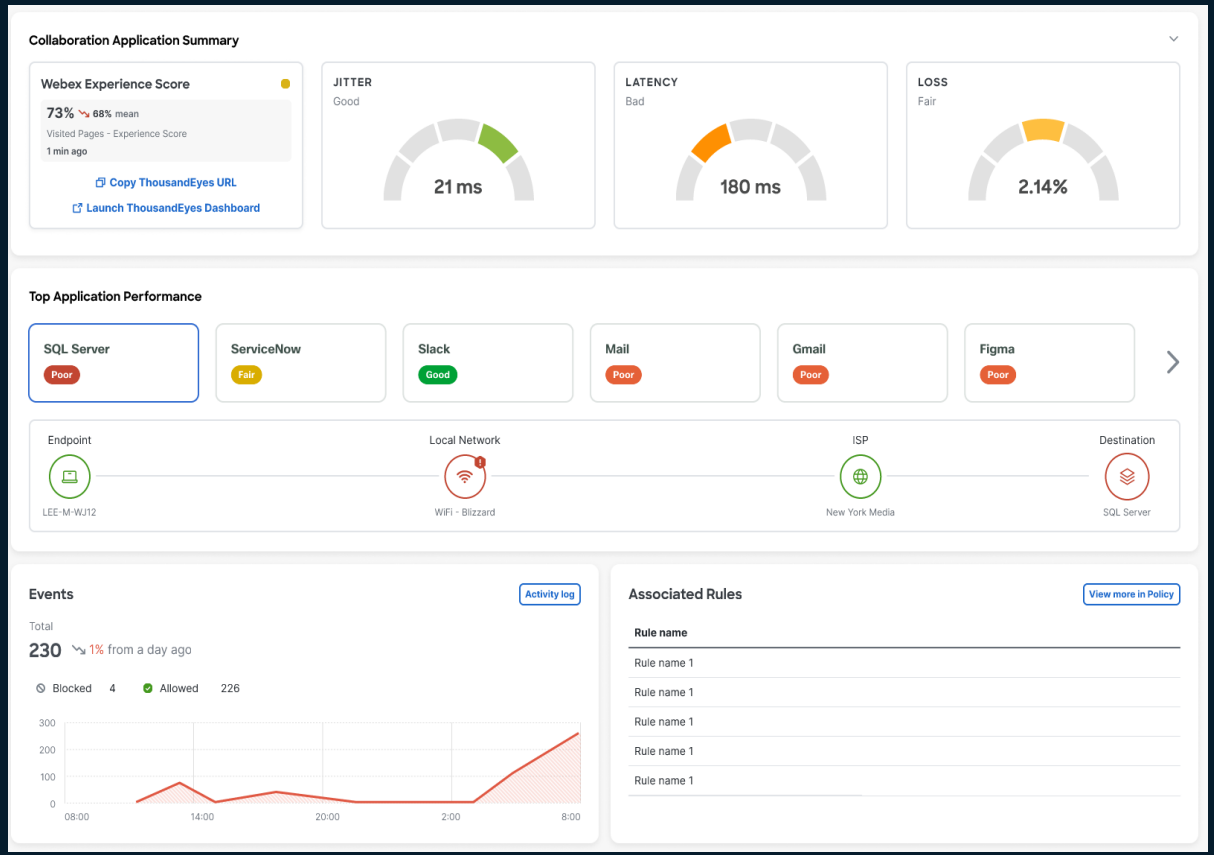
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

End User Monitoring and Troubleshooting



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

End User Monitoring and Troubleshooting



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Benefits

Built-in self remediation for end users

Cut down on time for troubleshooting

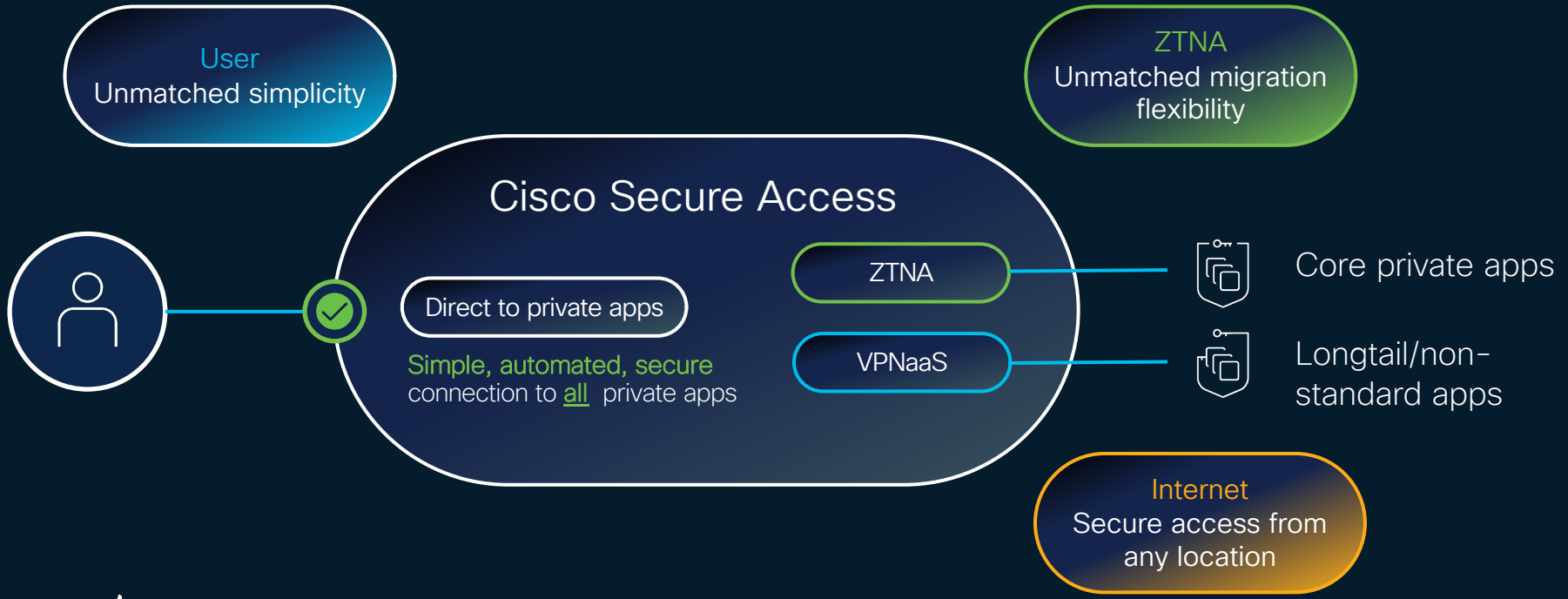
Visualize application health, both for SaaS and Private Apps

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Access gives your users easy and consistent access from anywhere in world.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Modernize remote access to all private apps, and the Internet. In one unified solution



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you for your time. If you would like to know more about CSA
Then these sessions will go into more detail:

- BRKSEC-2143 - Do You Know Where Your Data Is? A Deep Dive on Cisco Secure Access CASB and DLP and How to Protect Your Locations, Data and Users.
  Cloud Access Security Broker (CASB) provide the initial visibility to cloud app usage. Are your users only using business approved apps sanctioned by your company, or are they using unapproved apps to share and collaborate? This is what CASB is designed to find out. Umbrella also features DLP capabilities to monitor and enforce data for all web traffic.
  Wednesday, Feb 12 8:00 - 9:00 CET
  Hosted by Nitin Kumar, Technical Marketing Engineer

- BRKSEC-2285 - The Latest in Cisco Secure Access (SSE) Innovation
  We will take a closer look at the newest innovations in the entire security stack and applications of the latest AI and ML capabilities to help secure access and streamline management.
  Wednesday, Feb 12 16:00 - 17:00 CET
  Hosted by Neil Patal, Engineering Product Manager

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex App

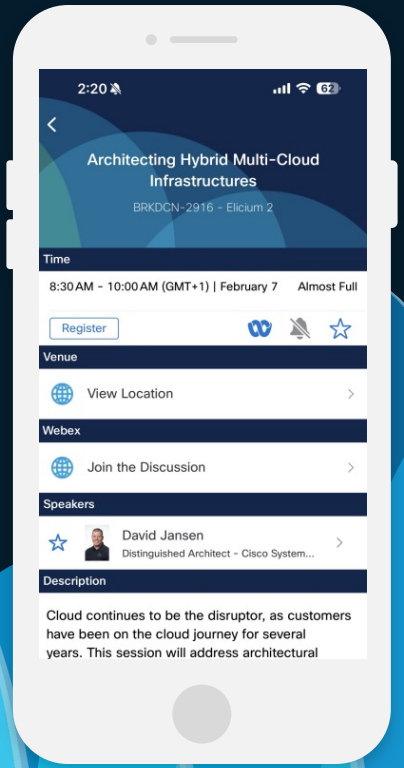
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

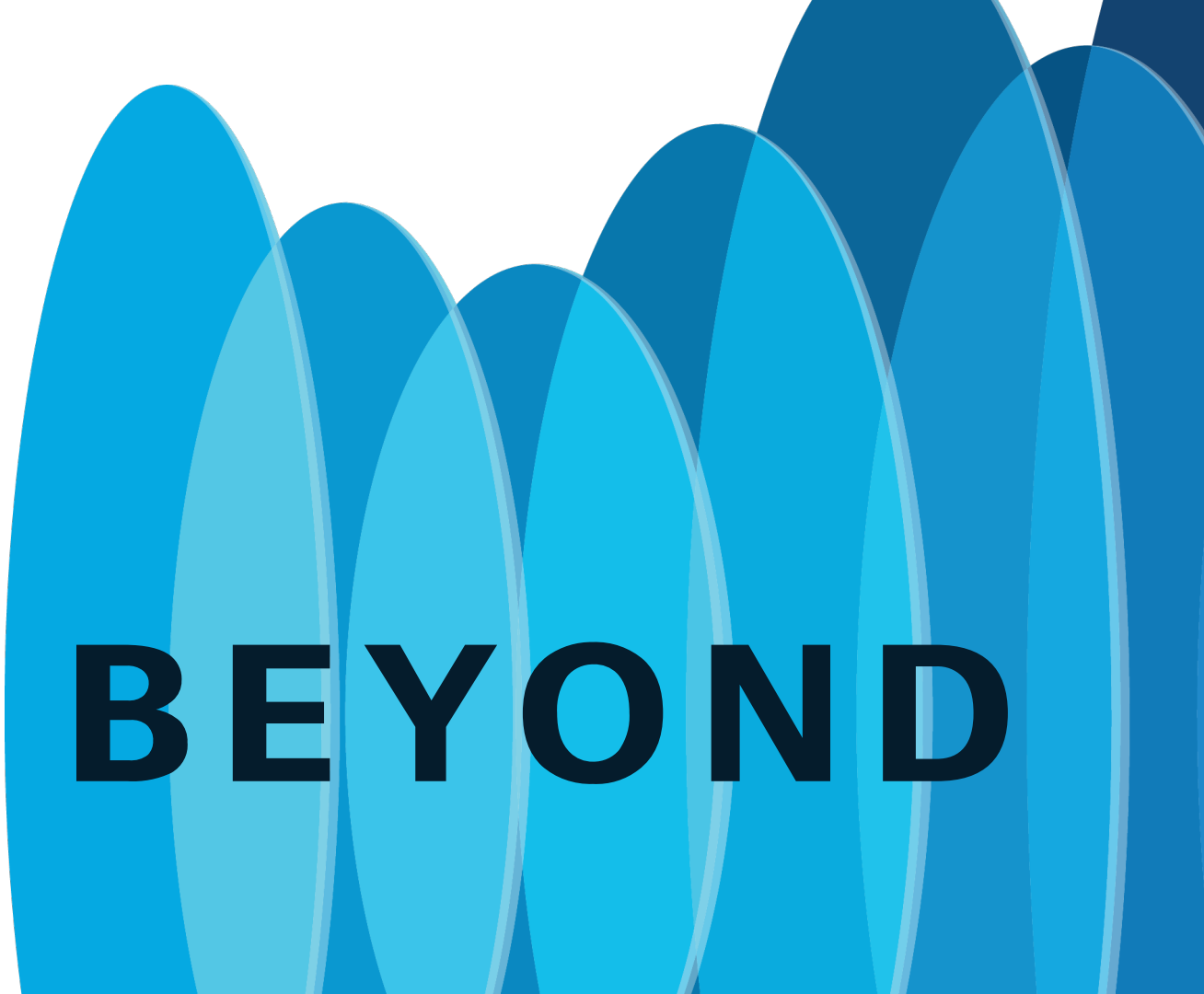
Continue your education

- 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 ciscolive.com/on-demand. Sessions from this event will be available from March 3.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND