

CISCO *Live!*



#CiscoLive



The bridge to possible

ISE Consumption in AWS

Ashish Binjola, Sr Technical Solutions Architect, Cisco Systems.
Bilal Ahsan, Sr Network development engineer, Amazon.

CSSOPS-2001



#CiscoLive

About Speakers



Ashish Binjola, Sr. Technical
Solutions Architect, Cisco
Systems

CCIE#21941 – Security

Vmware Certified Professional

Certified Ethical Hacker

AWS solutions architect



Bilal Ahsan, Sr.
Network Development
Engineer, Amazon

CCIE#45877 – Security | RS
| SP

CCDP

CWNA | CWDP | CWDP |
CWAP

ACMP | ACCP

AWS Network | Security
Specialist

Cisco Webex App

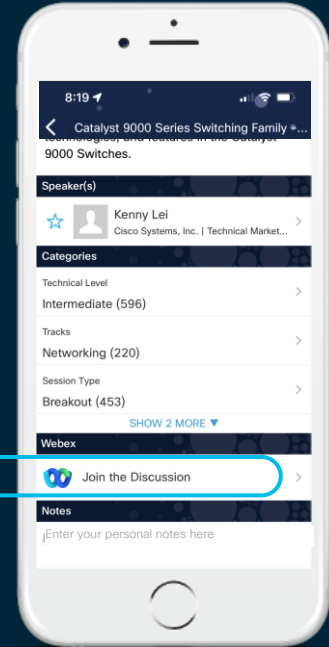
Questions?

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

How

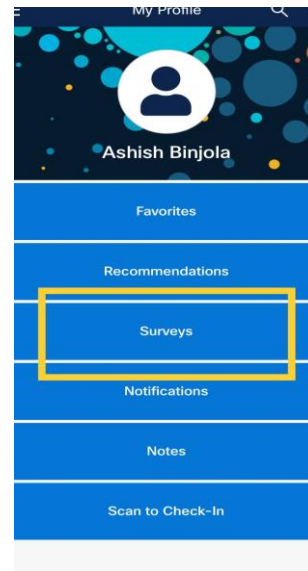
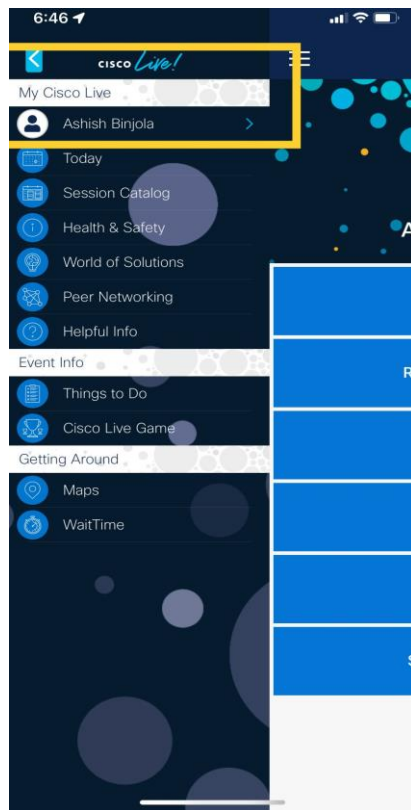
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

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



<https://ciscolive.ciscoevents.com/ciscolivebot/#CSSOPS-2001>

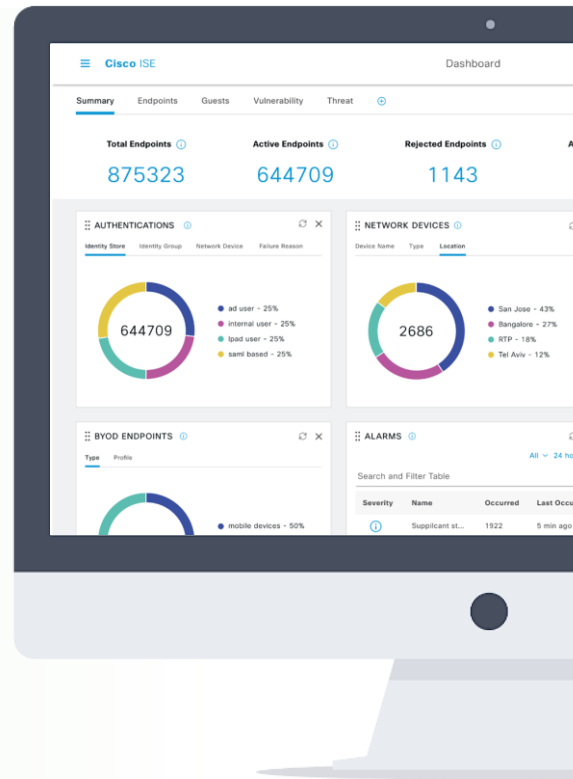
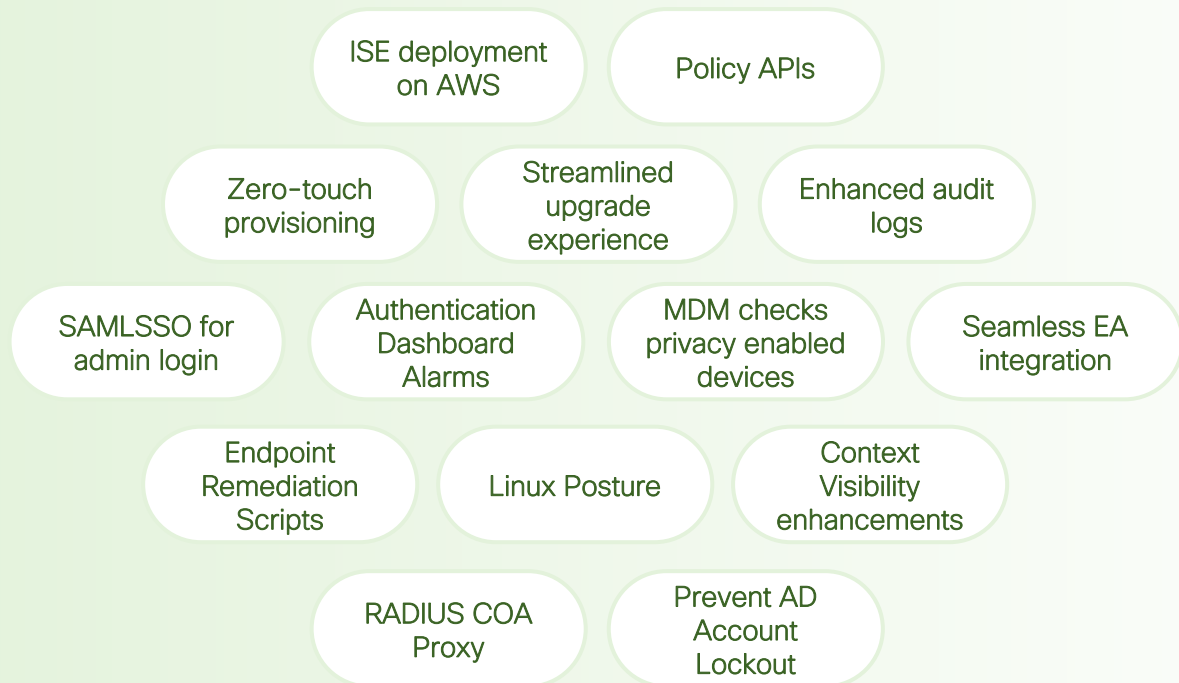
Survey Results Matter....



Agenda

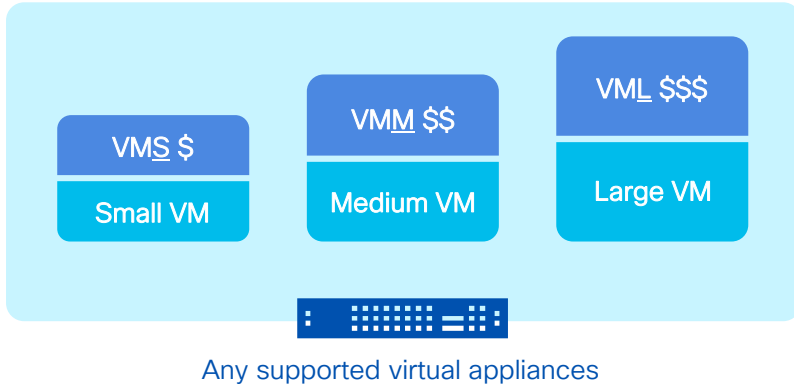
- ISE latest release highlights
- Common VM licenses
- ISE architecture in AWS/NLB
- ISE use cases in AWS NLB
- ISE policy orchestration and Automation
- Conclusion

ISE 3.1 Release Highlights

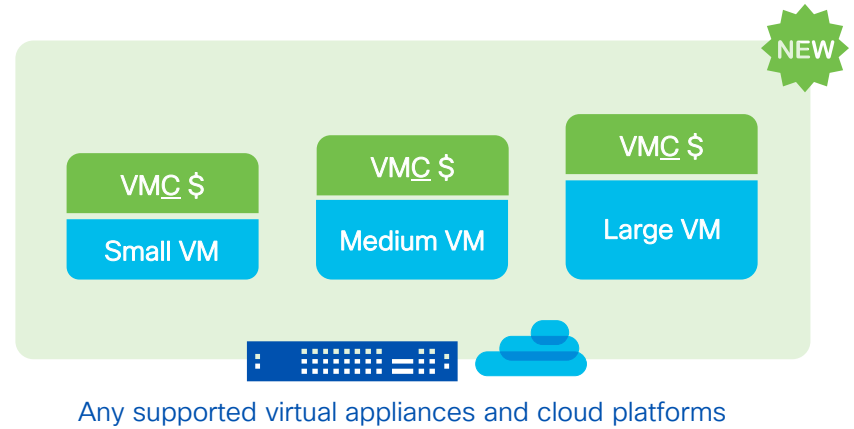


Common VM license

Before: ISE VM licenses based on node size



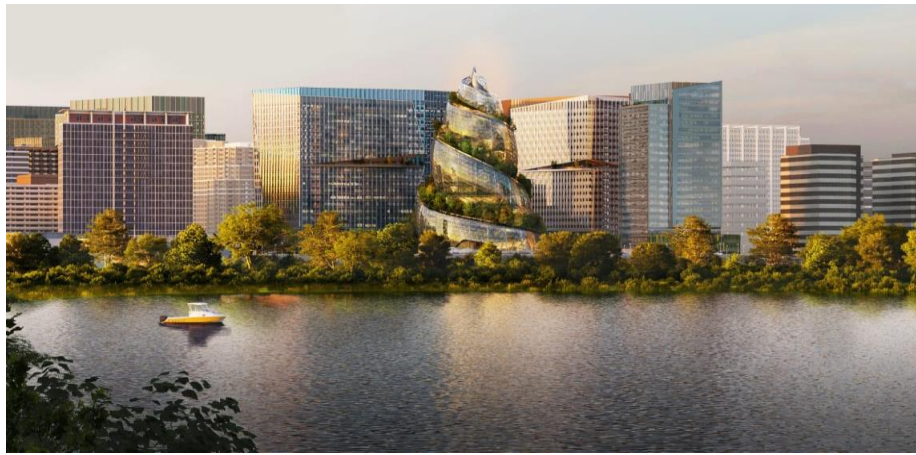
Now: Common ISE VM license for all node sizes



- New PID R-ISE-VMC-K9= now orderable!
- Obtain the \$0 Upgrade PID ("L-ISE-VMC-UPG=") in CCW
- Migrate the legacy VM licenses to VM Common license in CSSM
- You need as many Upgrade PIDs as the legacy VM licenses to be migrated to VM Common licenses

ISE services : AWS NLB

Use Case	Service	Loadbalancer Required?	Loadbalancer Requirements	NLB Support
A	ISE Admin CLI/GUI Visibility. Monitoring Dashboards (443)	NA- (ISE Allows only Limited sessions to Admins.)	NA	NA
B	Radius Authentication/Accounting (Listeners UDP 1812+1813 OR 1645+1646)	Required for scale traffic.	<ul style="list-style-type: none"> Health Probe on Radius Auth. Stickiness based on EP MAC/SourcIP. Client IP Preservation For Admin COA. 	<ul style="list-style-type: none"> Alt TCP 80 * Only SIP Available * Available
C	Cascaded Flows: Radius + CWA/PPP Flows Like Guest portal, Client Provisioning, Posture etc. (Listeners: UDP 1812+ UDP 1813)	Required for scale traffic.	<ul style="list-style-type: none"> Health Probe on Radius Auth. Stickiness based on EP MAC/SourcIP. Client IP Preservation. 	<ul style="list-style-type: none"> Alt TCP 80 * Only SIP Available * Available.
D	Tacacs+ (Listeners: TCP 49)	Required for scale traffic.	<ul style="list-style-type: none"> Health Probe on Tacacs Auth. Stickiness based on SourcIP. Client IP Preservation. 	<ul style="list-style-type: none"> Alt: TCP 49 Socket * Available Available



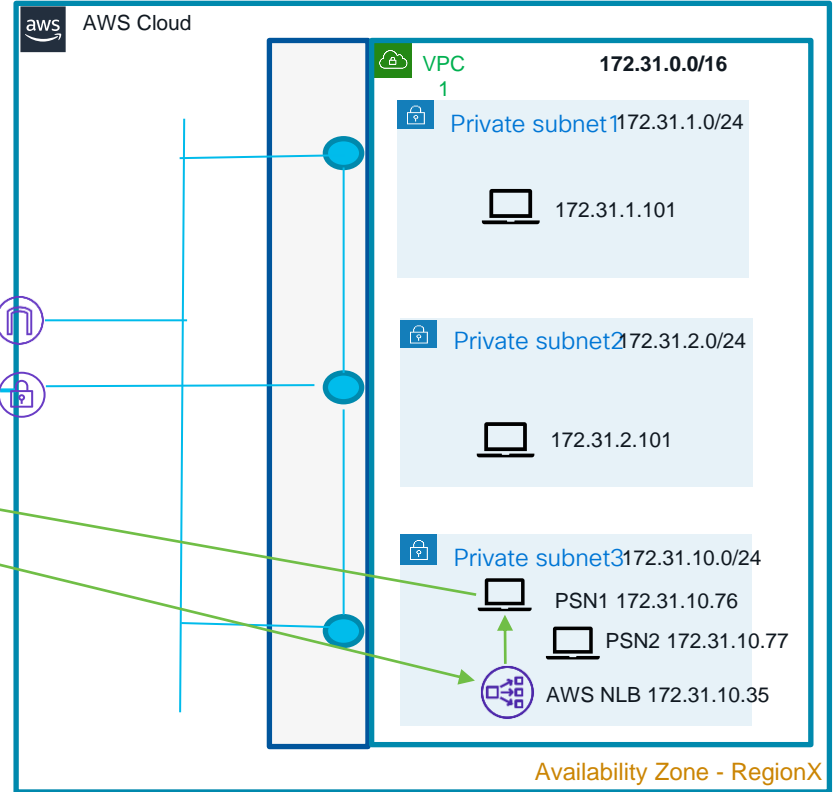
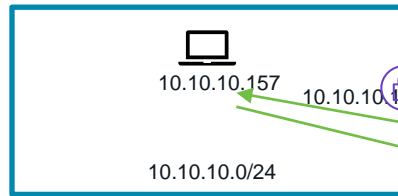
Amazon

- 1.3M+ Employees. >500K New Hires in 2021
- 3M SQ FT of Real Estate in Bellevue/Seattle (Primary HQ)
- Globally 60+ large pop locations
- 500+ large enterprise offices/sites globally
- Approx. 300k+ remote VPN users and several hundred of VPN head ends running in AWS
- Approximate 160 ISE nodes (till date) in AWS cloud

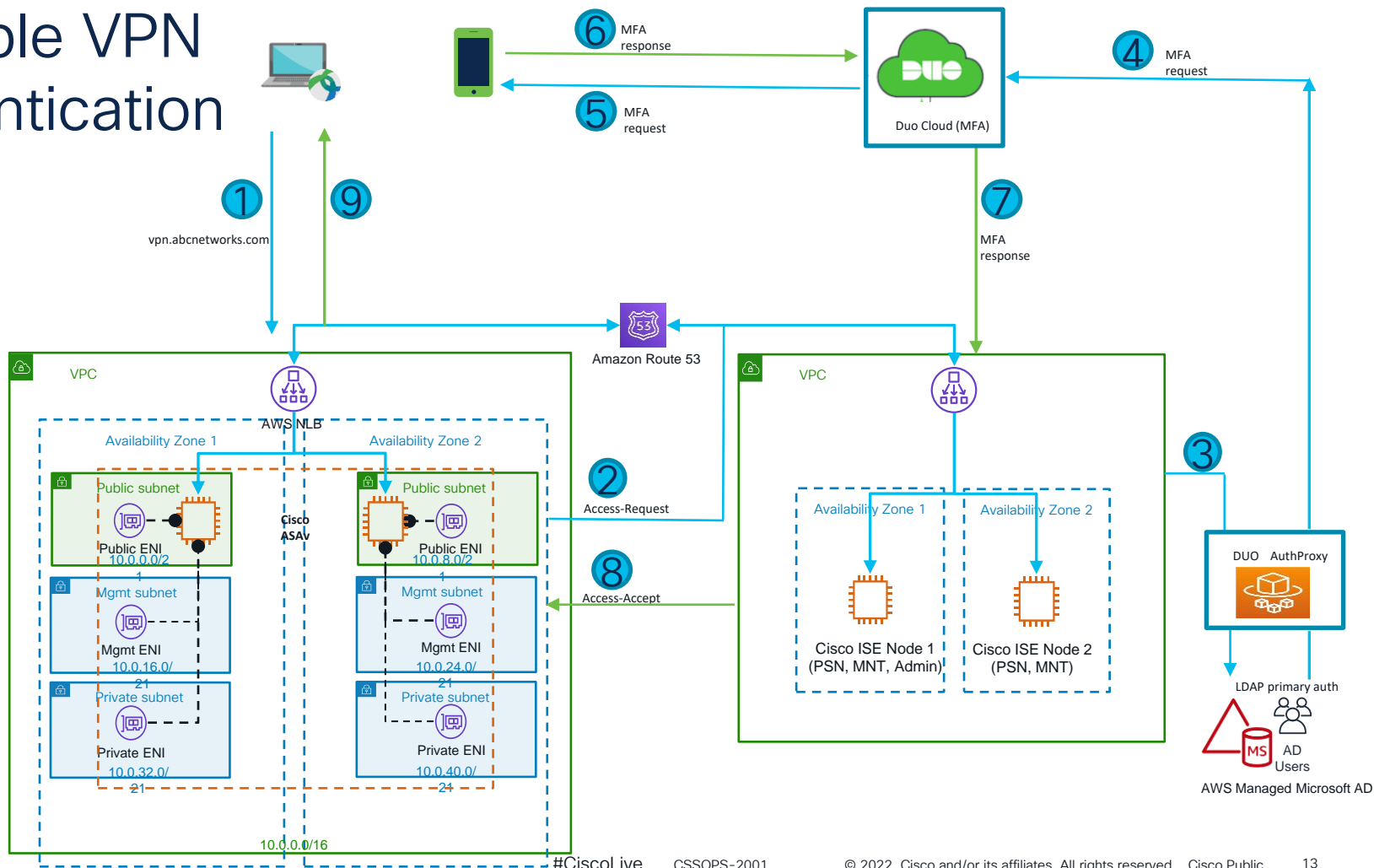
High level Design

SIP	DIP	
10.10.10.15	172.31.10.35	NAD-NLB
10.10.10.15	172.31.10.76	NLB-PSN1
172.31.10.7	10.10.10.157	PSN1-NAD

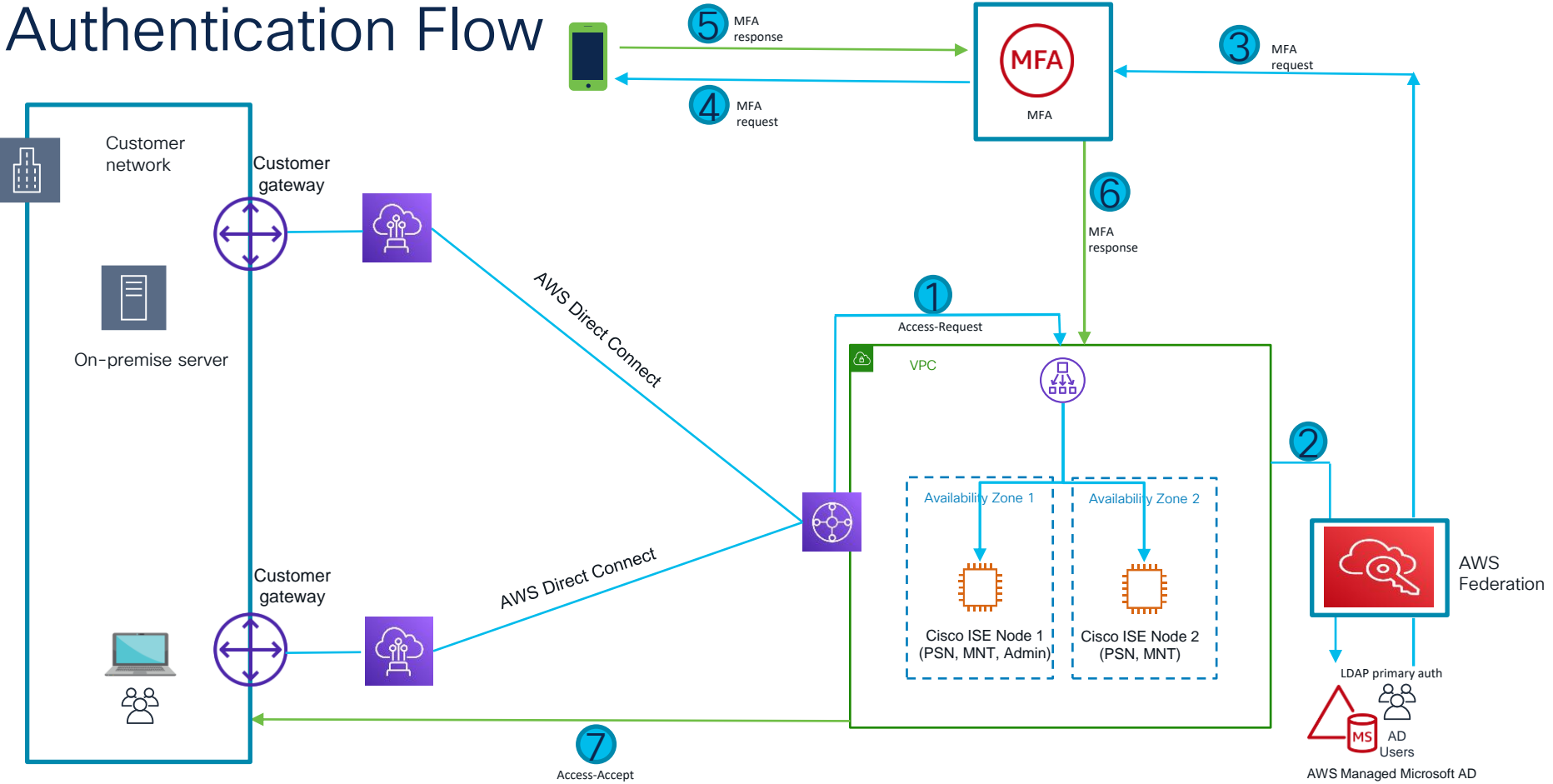
On-Prem



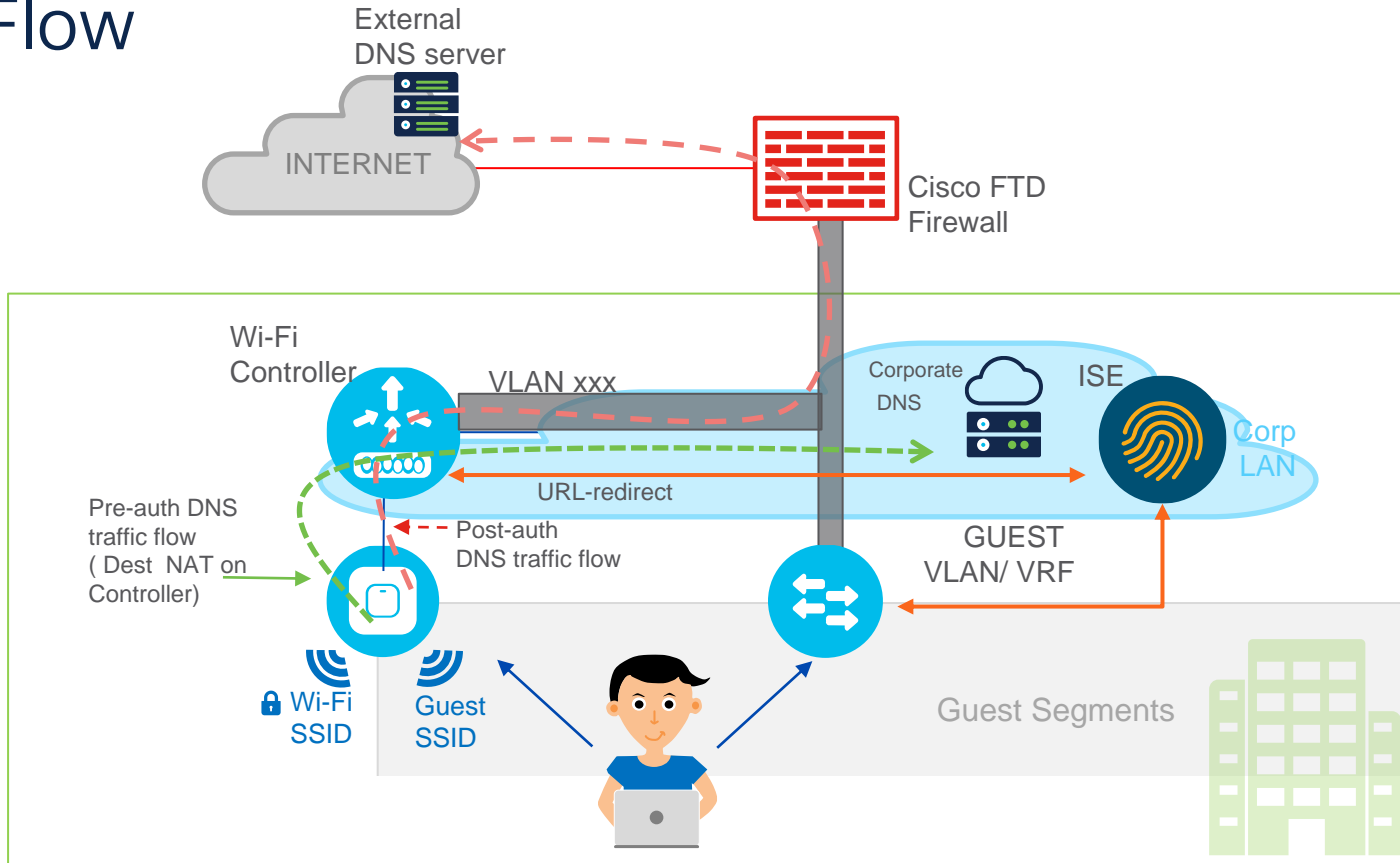
Scalable VPN Authentication



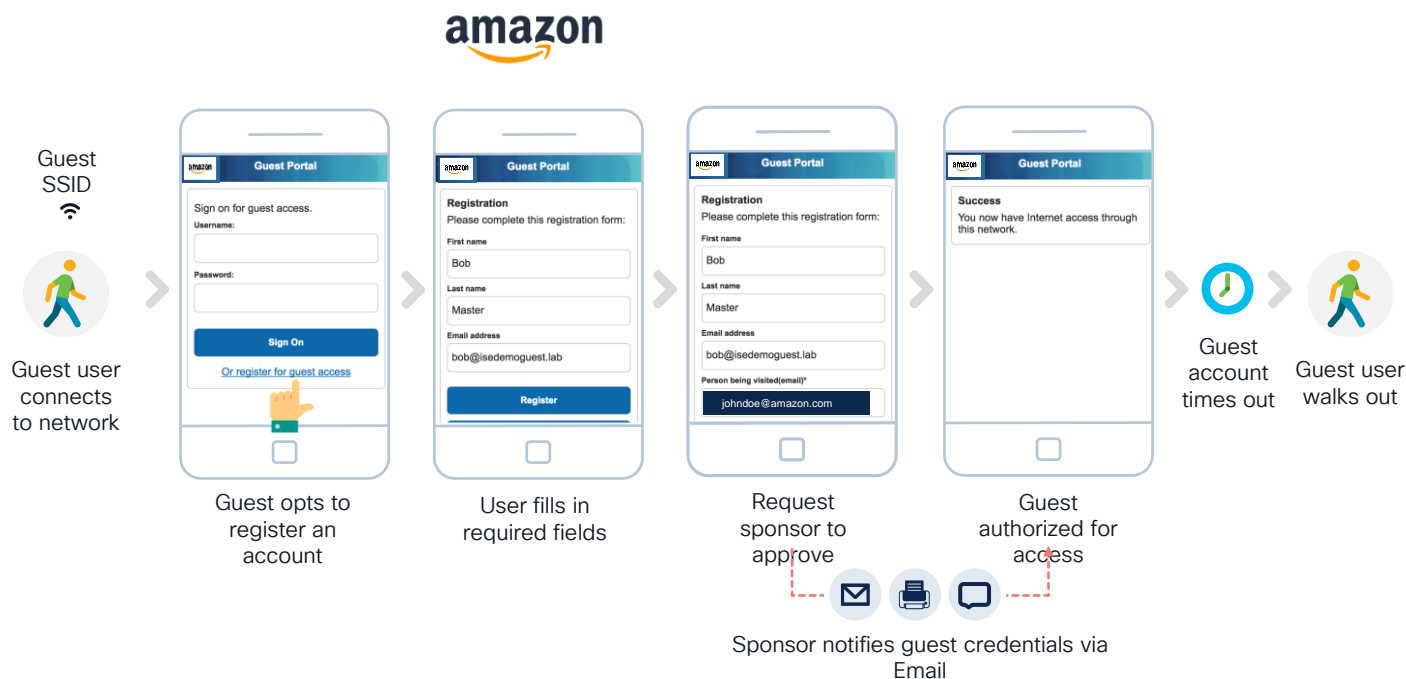
Authentication Flow



Guest Flow



Guest Flow Contd...

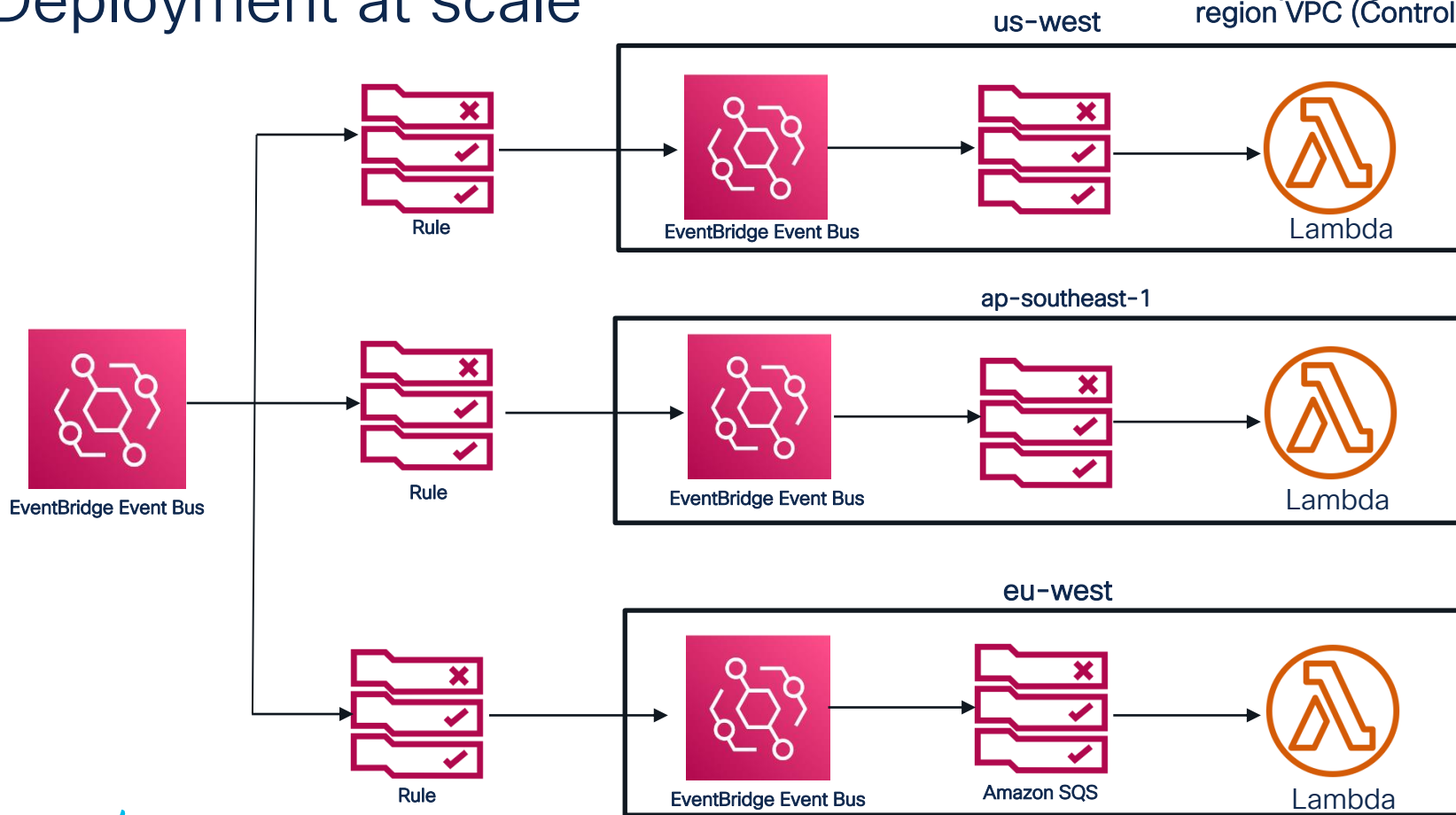


Automation Use Cases:

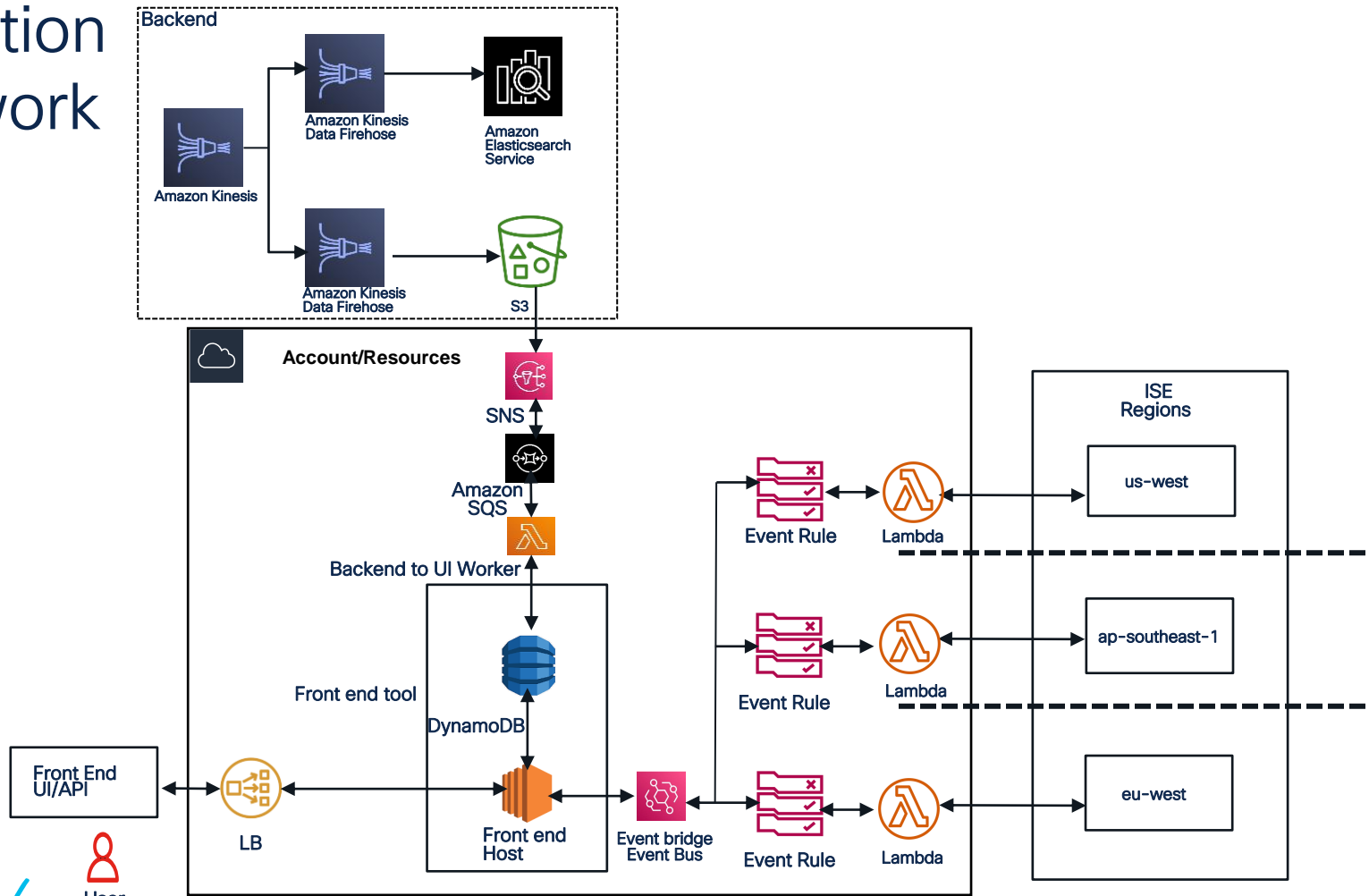


Deployment at scale

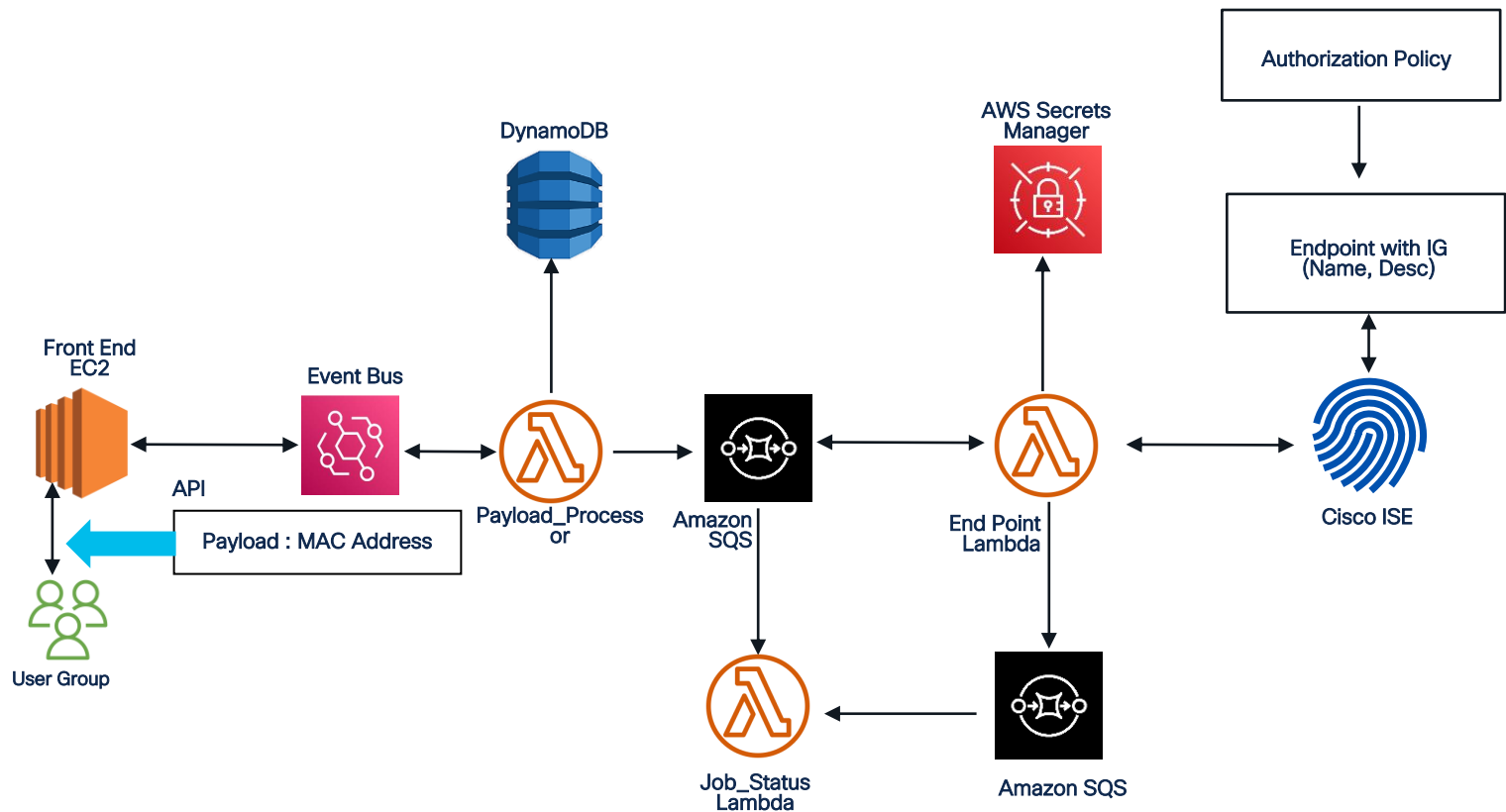
Lambda runs in a cluster corresponding to AWS region VPC (Control VRF)



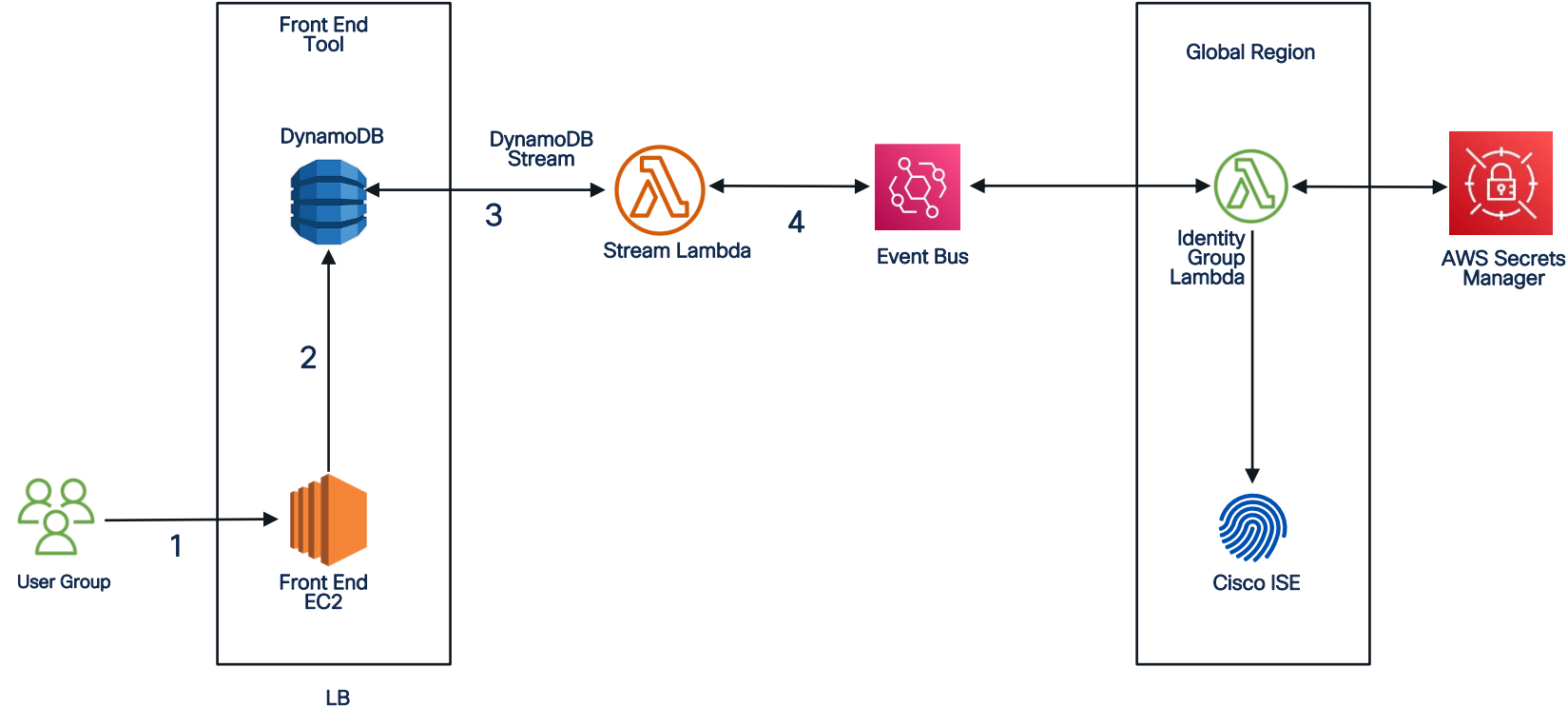
Automation Framework



Device and Policy whitelisting



Endpoint/Device Group



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

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

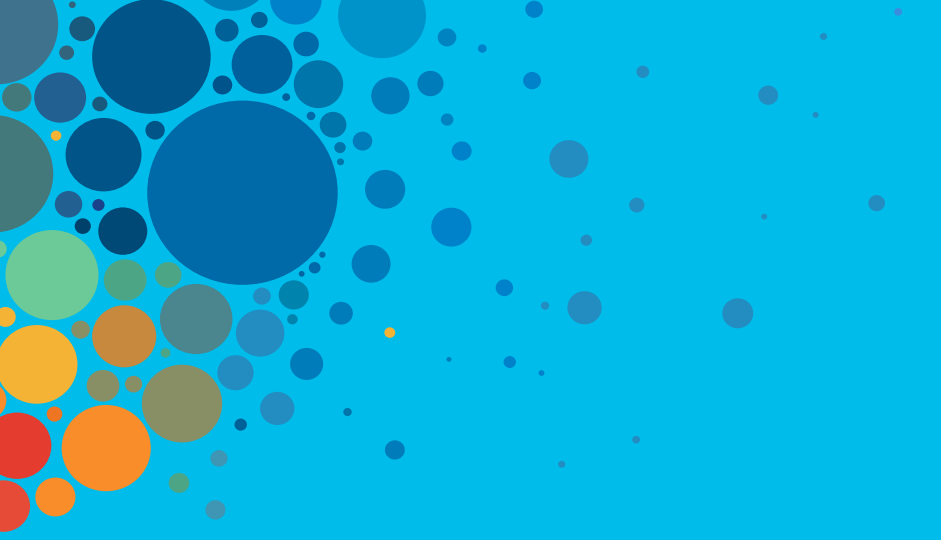
Cisco Guided Study Groups

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

- 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



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive