

CISCO *Live!*



#CiscoLive



The bridge to possible

Service Provider's Zero Trust Journey

Ashish Binjola, Sr. Technical Solutions Architect, Cisco Systems
Bilal Ahsan, Sr Network development engineer, Amazon
CSSSPG-2000

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

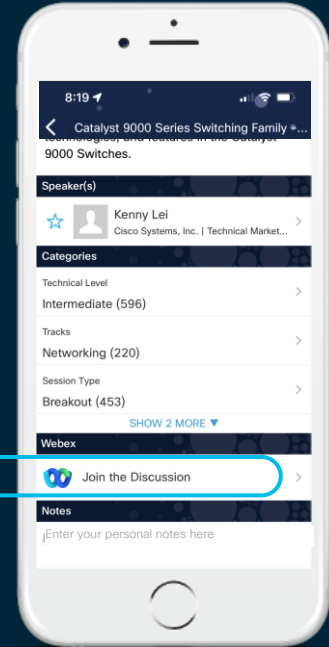
Questions?

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

How

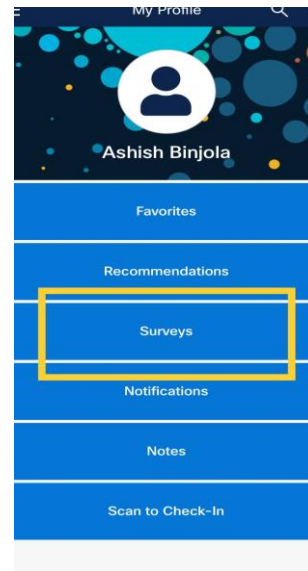
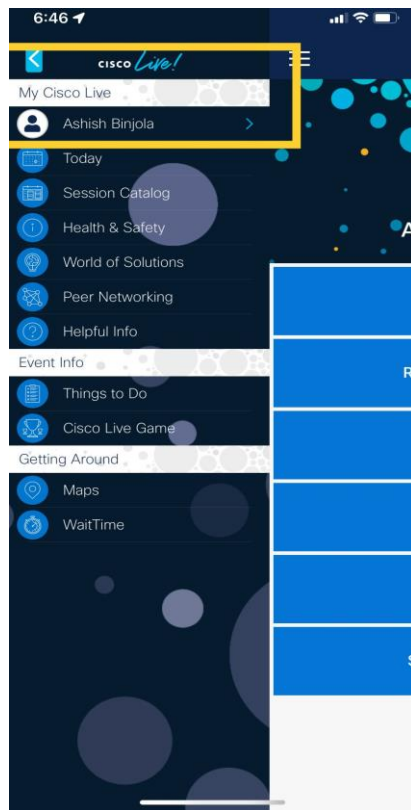
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

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



<https://ciscolive.ciscoevents.com/ciscolivebot/#CSSSPG-2000>

Survey Results Matter....



Agenda

- Introduction
- Cisco's stance on Zero Trust
- Amazon Enterprise business objectives
- Legacy Network : Scale, numbers and challenges
- Zero Trust Evolved Network
- Conclusion

Key Take Aways

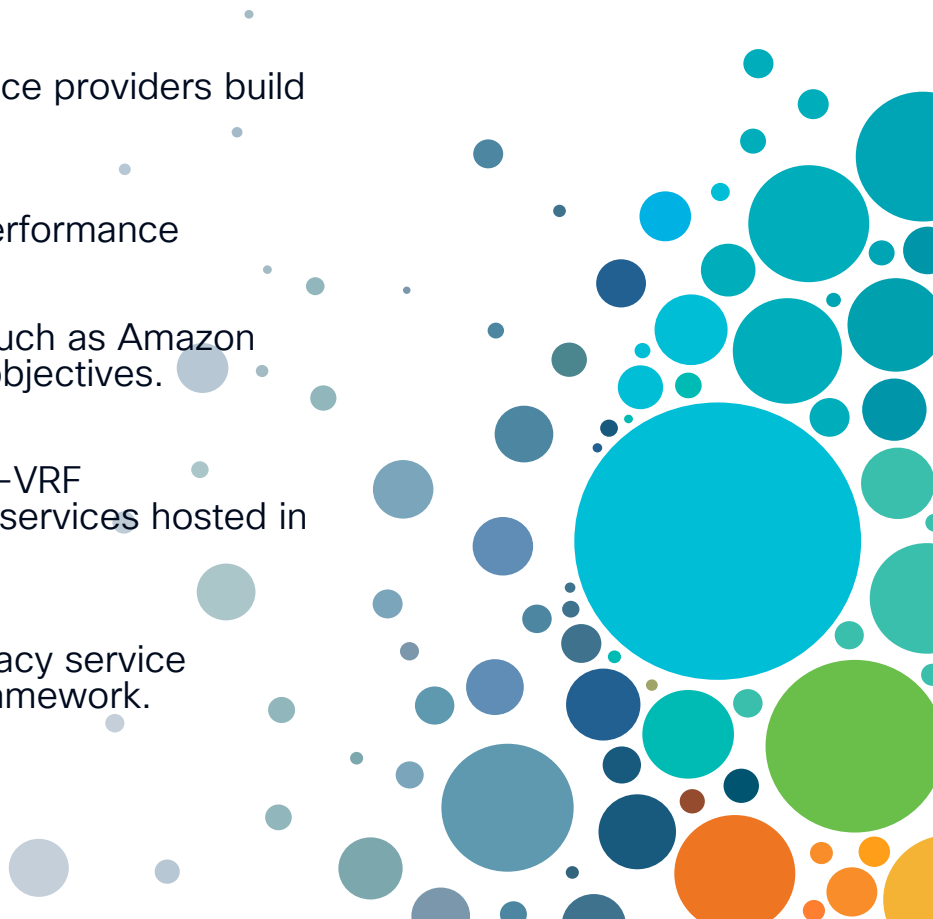
Guidance on how a large enterprise and other service providers build a secure agile network

Address challenges due to sheer scale, size and performance

Learn and understand how large service provider such as Amazon IT partnered with Cisco and met the key business objectives.

Build firewall/firepower in a service provider's multi-VRF infrastructure to get a seamless secured access to services hosted in AWS VPC.

Build a clear understanding to migrate complex legacy service provider network to a next-generation zero trust framework.

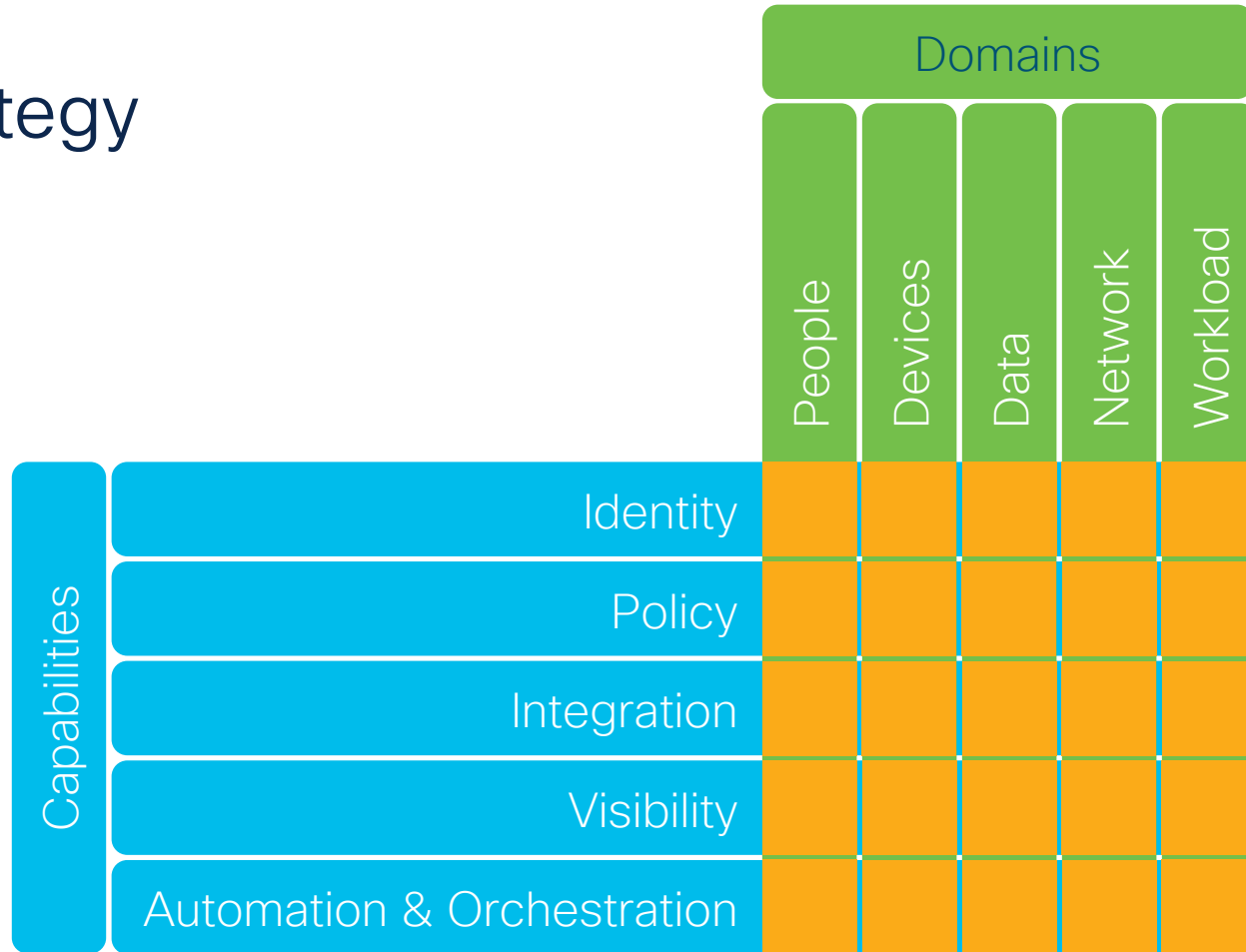


Contextualising Zero Trust



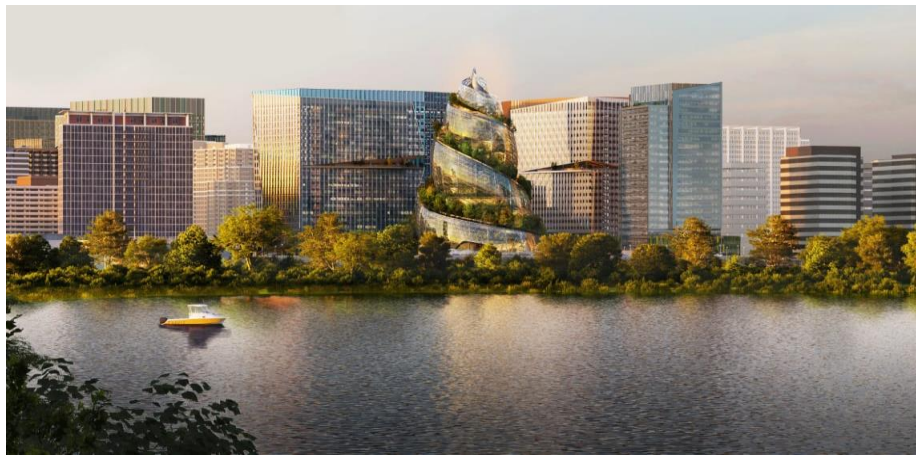
Zero Trust Strategy

- 5 **capability** areas
- 5 **domains** in which threats operate
- 25 Zero Trust **elements** considered for your strategy
- This is the bedrock of the needs analysis process



Zero Trust Sample Matrix

		Domains				
		People	Devices	Data	Network	Workload
Capabilities	Identity (SAML/RADIUS/other)	Employee/ Guest/ Contractor	Managed/ Unmanaged	Public / Private	Inside/ Outside /DMZ	Containers / Hyper-V/ SaaS apps / Legacy apps
	Policy	X	X	X	X	X
	Integration	X	X	X	X	X
	Visibility	X	X	X	X	X
	Automation & Orchestration	X	X	X	X	X



- 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
- Close to 500k remote users with 250+ VPN headends running in AWS

Business Objectives



- 1 seamless access to workforce regardless of the physical location. Regulatory compliance
- 2 Reduce global Corp footprints. Migration to cloud
- 3 Provide least privilege access to resources
- 4 Connect to resources in cloud/w reduce attack surface
- 5 Identify and protect critical assets

Business Objectives



6 Flexible work experience

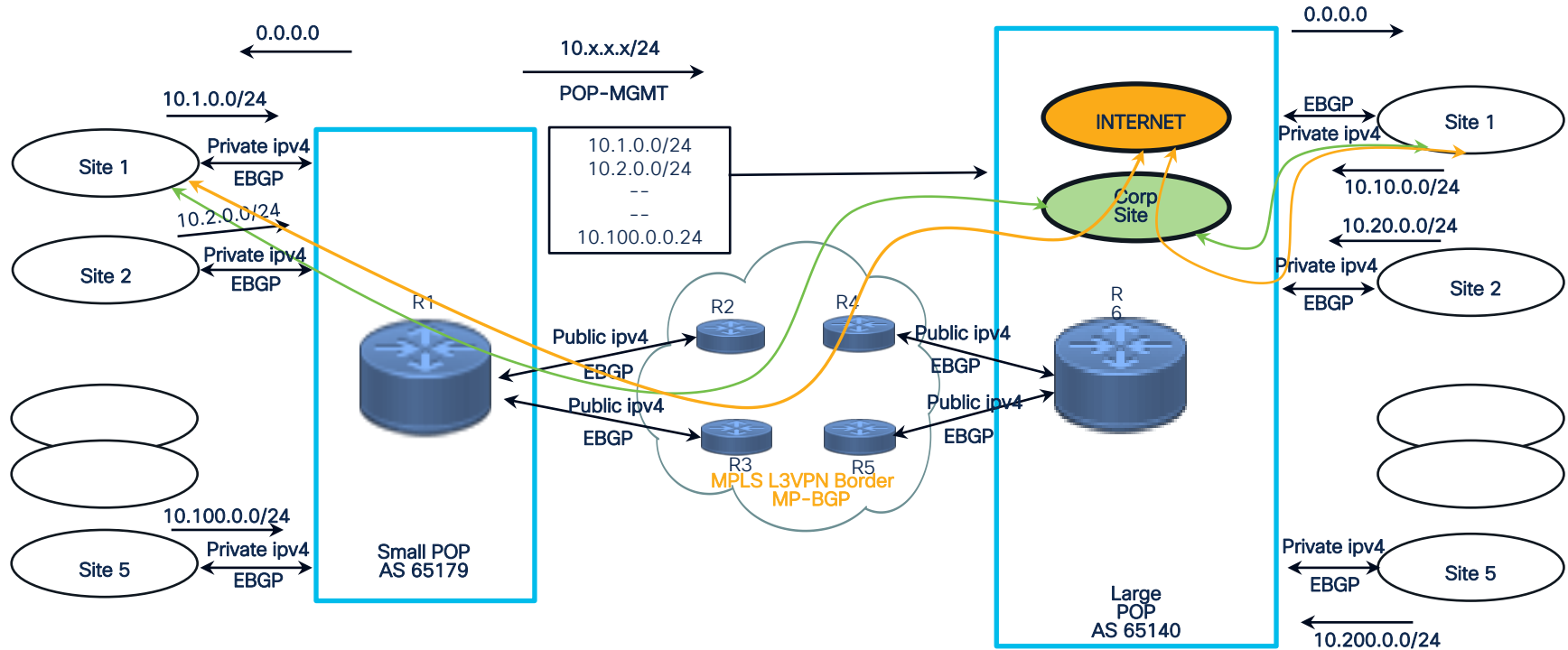
7 Remove service dependencies from Corporate Network

8 Client isolation and segmentation

9 Security with a dissolved perimeter

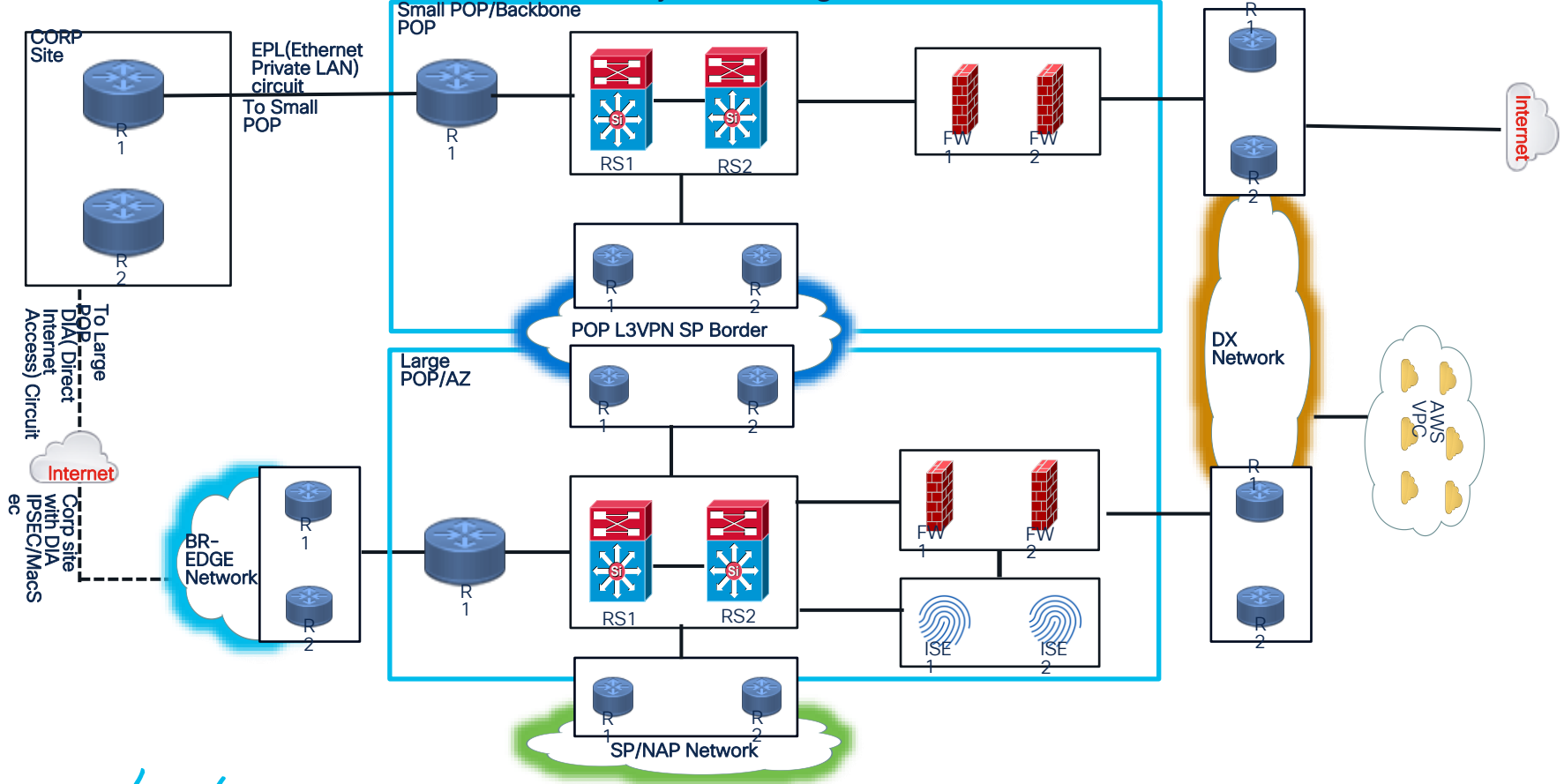
10 Resiliently respond to evolving threats

Classic Network

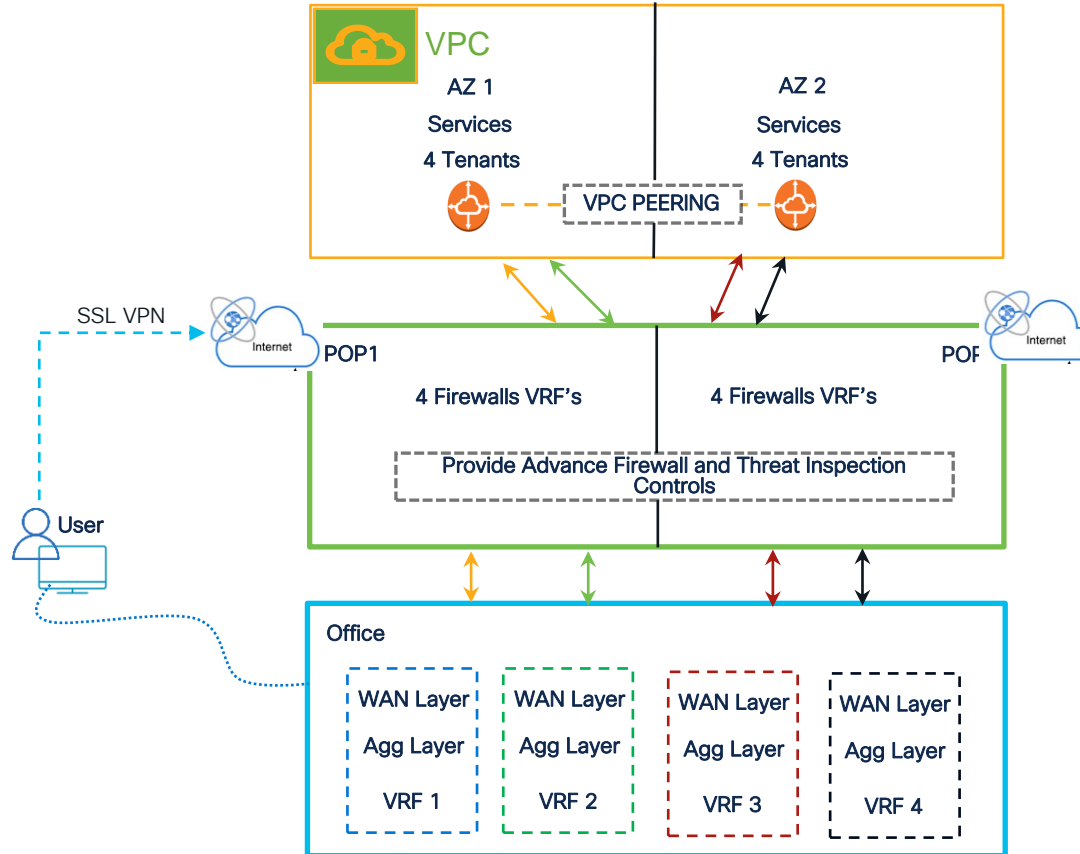


Zero Trust physical Design

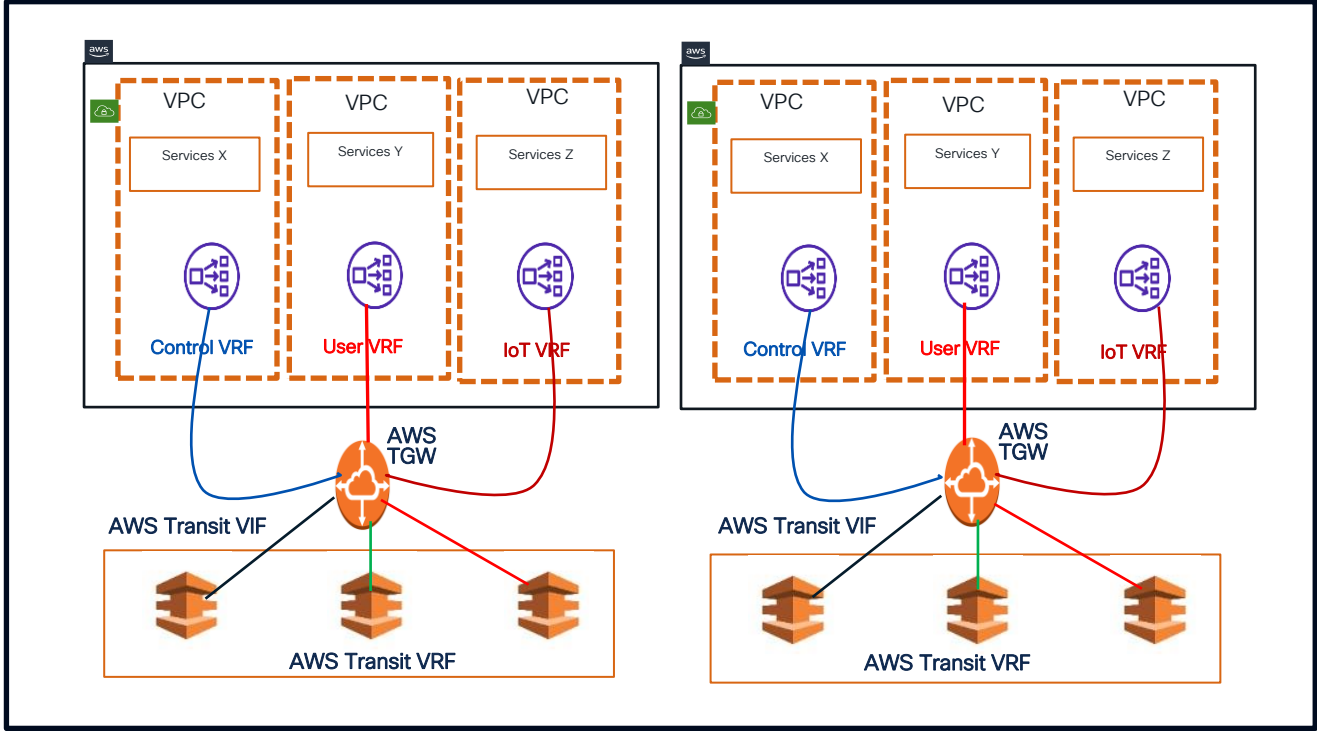
POP & WAN Physical Design



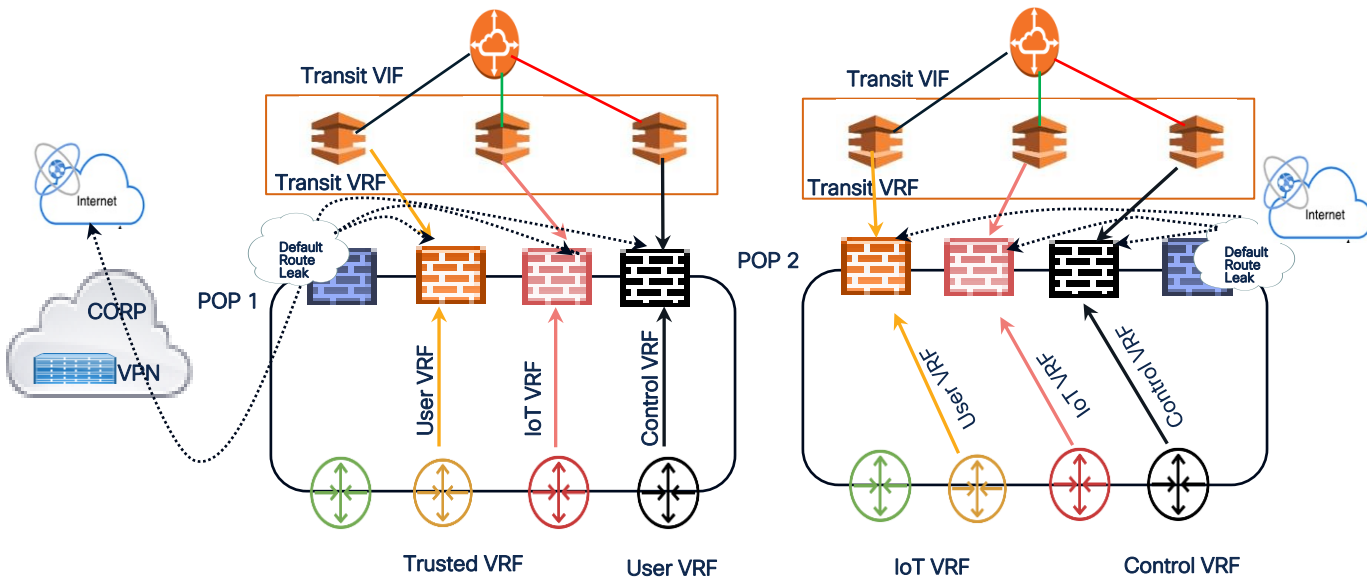
Bird's-eye view



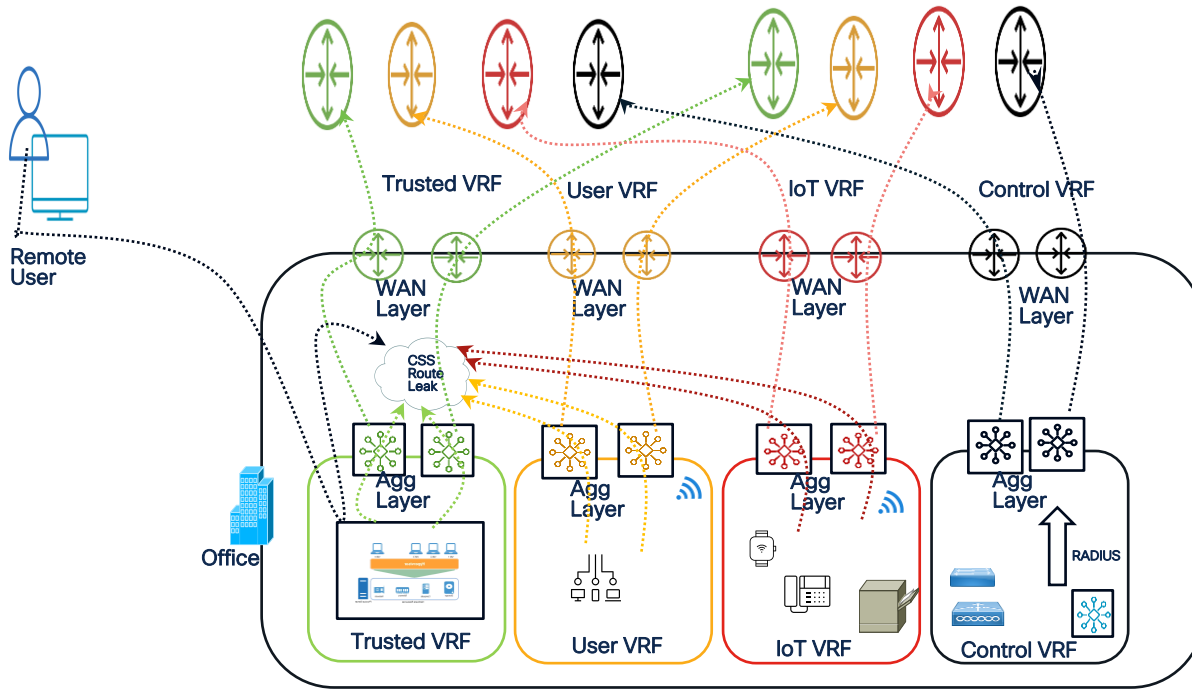
- A 3-x layer design
- Top AWS VPC layer hosts services
- Services segmentation at VPC
- Firewalls to provide control at a VRF level
- Security controls pushed via TAGs
- Advance threat/control inspection
- Corporate Office connectivity
- Device insight and profiling



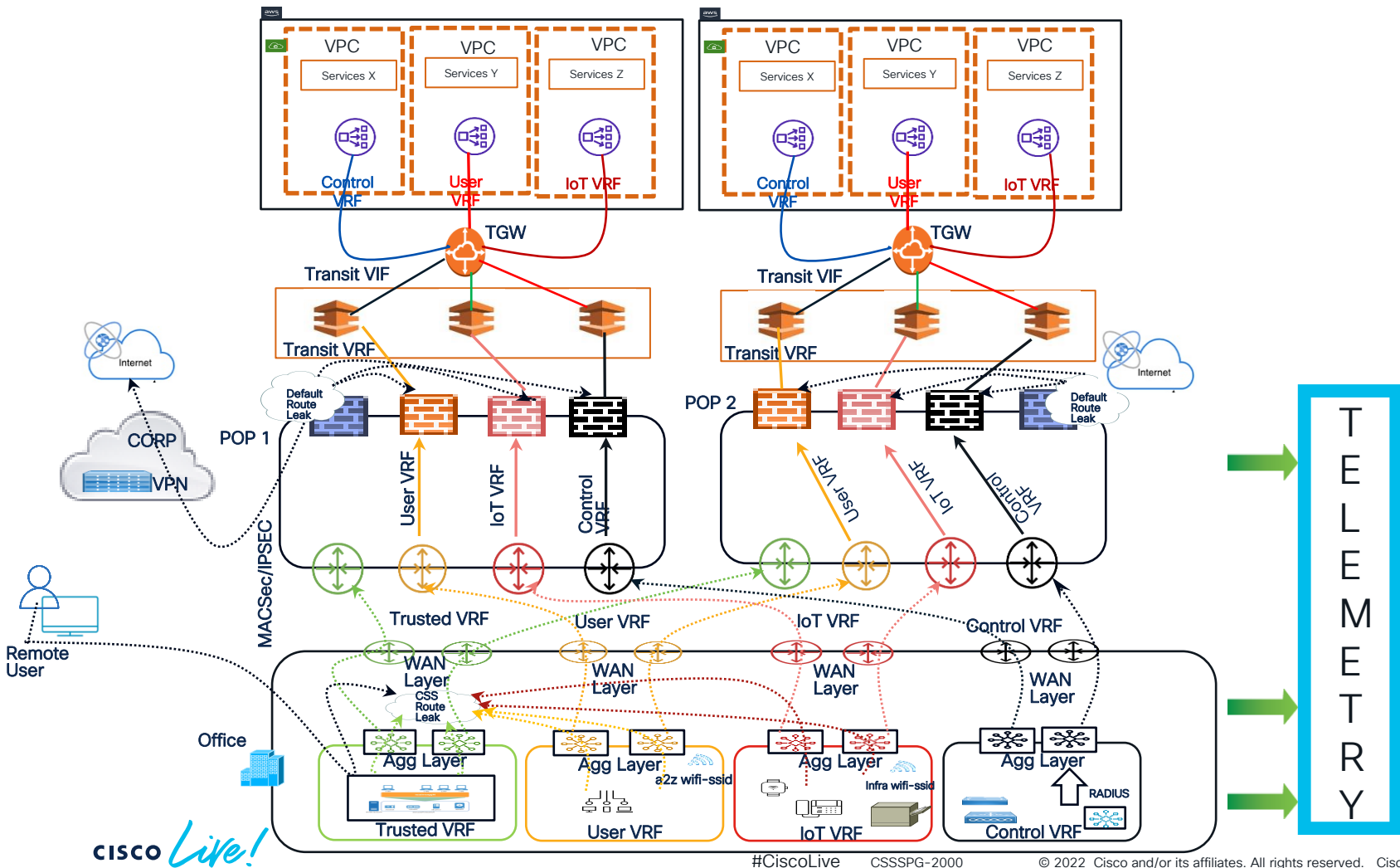
- AWS cloud Infrastructure
- Applications / Services in VPCs
- Segmentation in AWS fabric
- VPC peering (Interconnect)
- Policy Enforcement
- Automation / Orchestration



- Firewalls in Multi tenancy
- eBGP with ECMP
- Policy Control per VRF
- Group Tag Enforcement
- Route leak for inter VRF traffic



- Campus/ Office
- Infrastructure
- MACSec/IPSEC to DIA
- Device Insights
- User /Device TAG's
- Profiling
- Policy Enforcement



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

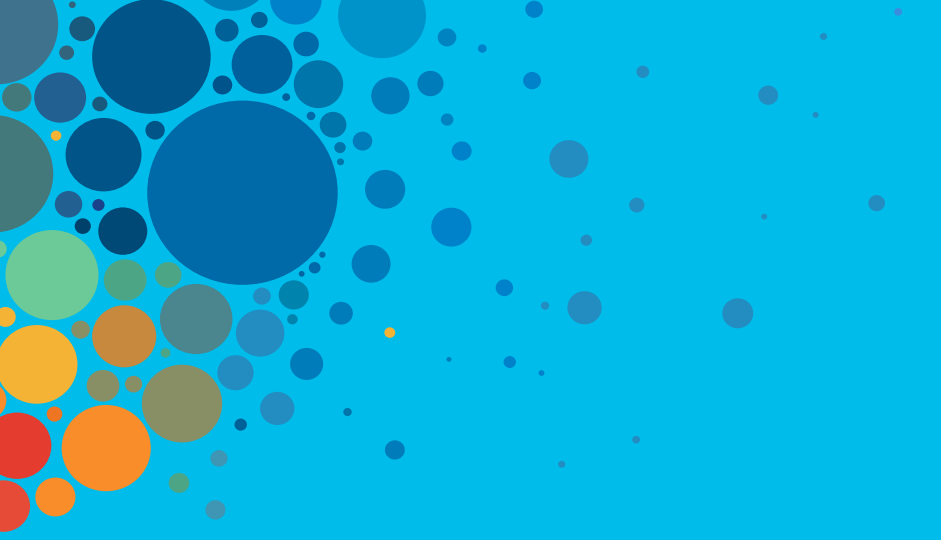
Cisco Guided Study Groups

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