The bridge to possible

Cisco SD-WAN Cloud OnRamp for Multicloud

From Connectivity to Application Integration

Nikolai Pitaev, SD-WAN TME Leader, Cisco
@pitaev

cisco Live!

BRKENT-2060

Question:
what is this time slot about?

95,212,800 seconds

1,586,880 minutes

26,448 hours

1,102 days

Answer: … since last CL EMEA in Barcelona 2020

aws certified
Solutions Architect
Professional

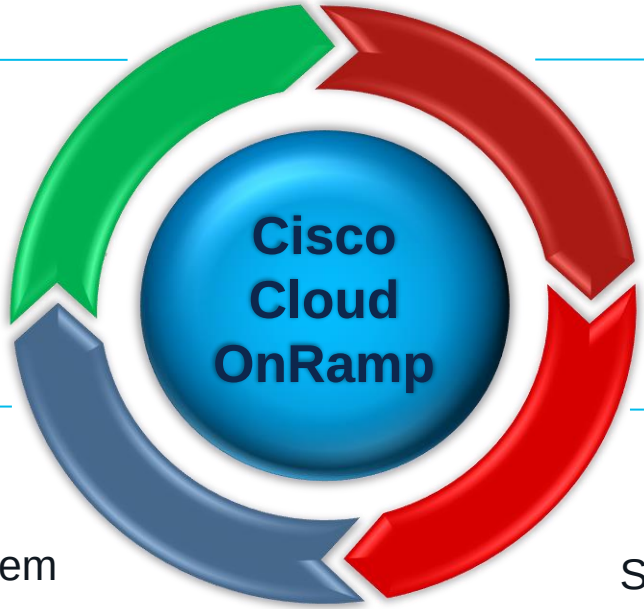
CISCO CERTIFIED
CCIE

cisco Live!

Cisco Cloud OnRamp solves your cloud problems

Automation

Site-to-Site, Site-to-Cloud, Cloud-to-Cloud



Operations

Cloud Audit, Monitoring, Prediction and Recommendation

Security

Cloud Security, SIG, On-Prem

App Performance

Service Directory Integration, Mid-Mile Optimization

Agenda

- Introduction
- Site-to-cloud:
  design, automation, performance, security
- Site-to-site over CSP
- Cloud / Custom App integration
- Conclusion

Cisco Webex App

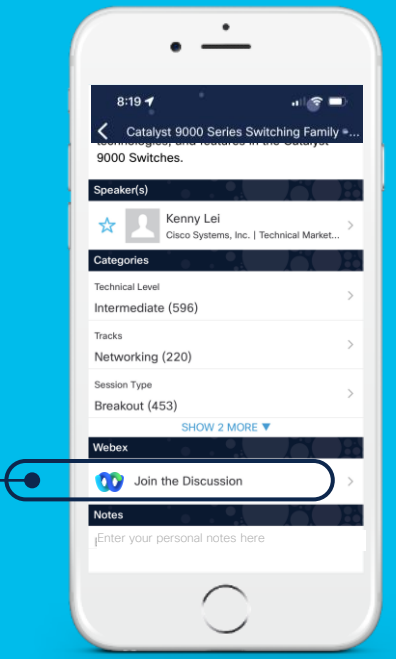
Questions?

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 until February 24, 2023.

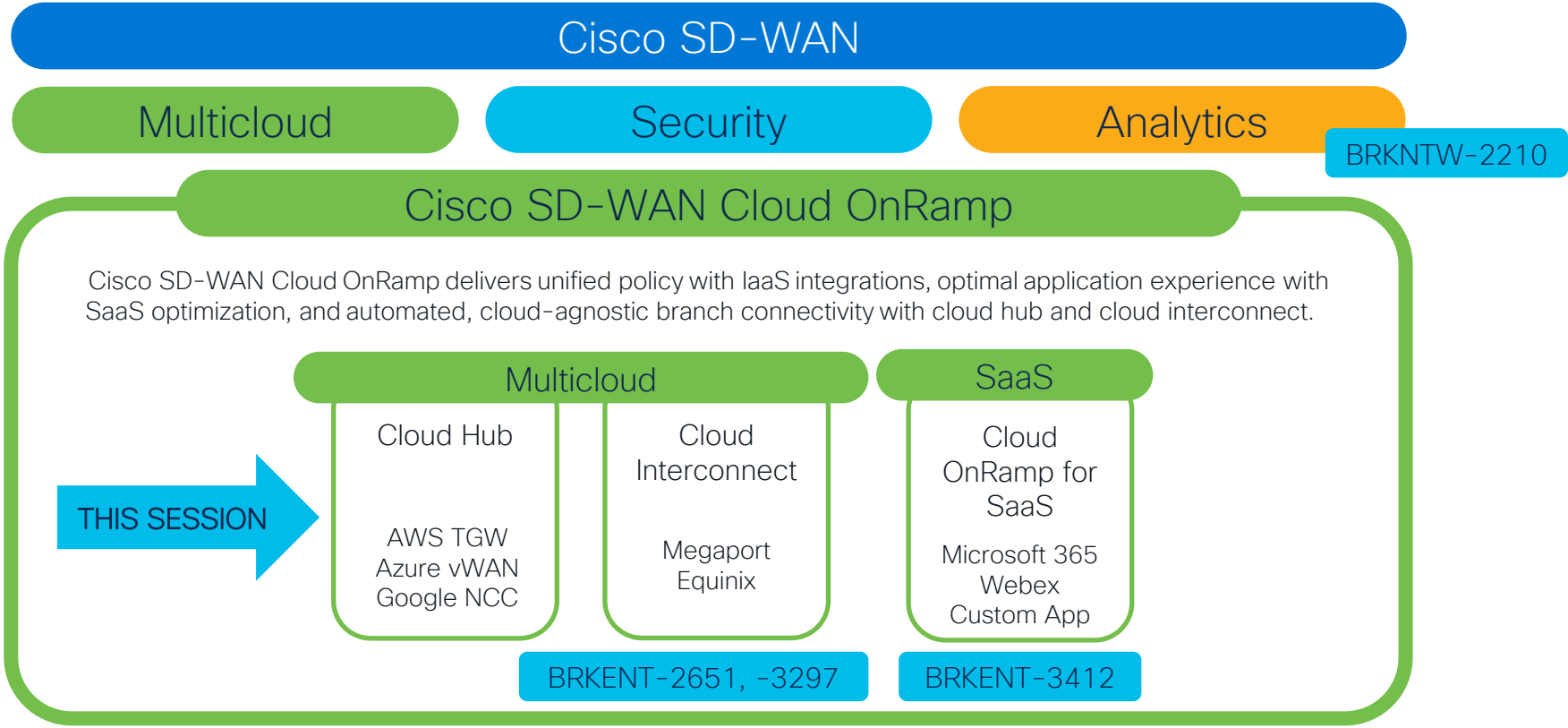


Your voice matters!
Live poll during this session.

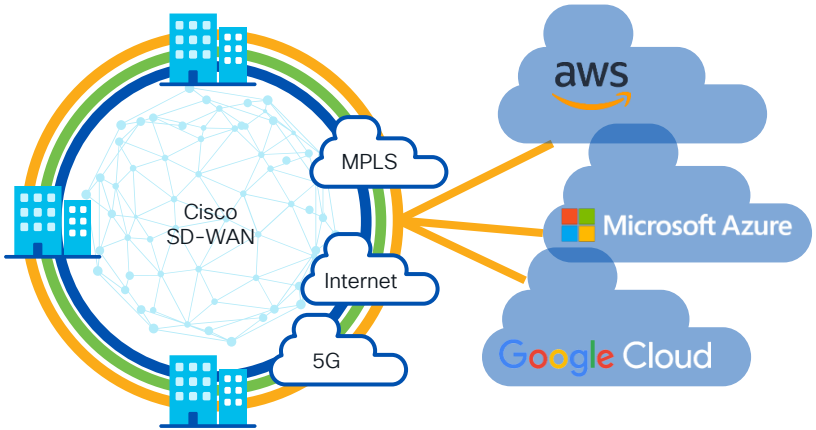
https://app.sli.do/event/d71oy65sDmvgK1YB67RkoU

Introduction

Cisco SD-WAN – Building Blocks



Introduction: Cloud Hub (aka IaaS)



Cisco delivers cloud trifecta with top 3 cloud providers

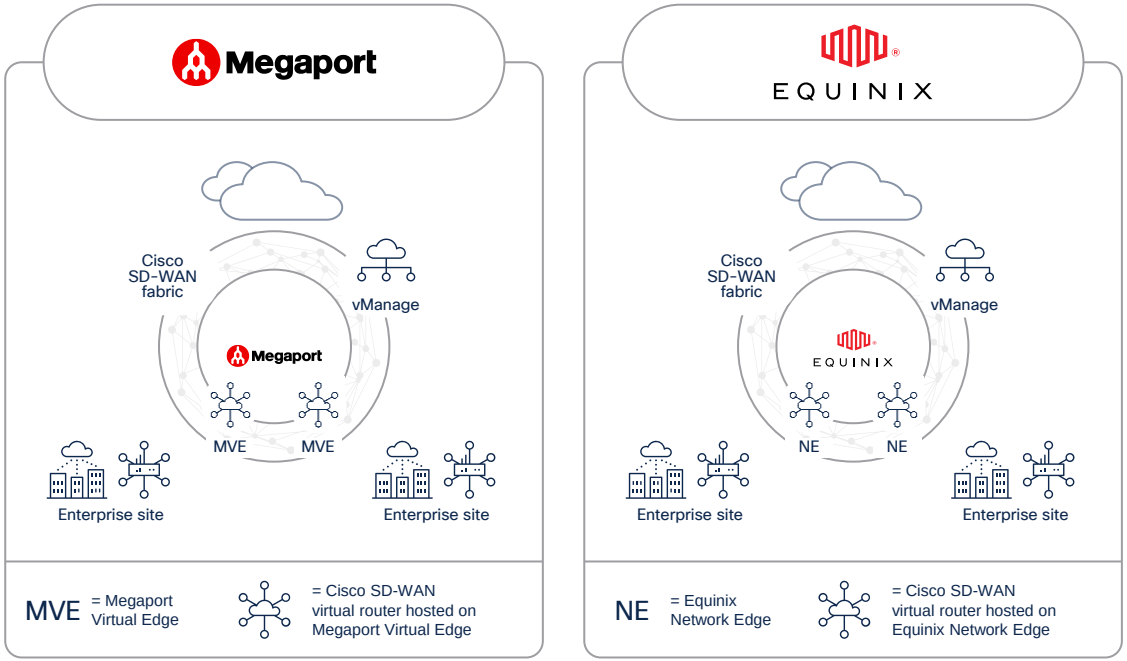
Greater automation
Automate SD-WAN extension to the cloud with just a few clicks in vManage

Normalized Multicloud experience
Consistent UI and workflow in vManage

Unified security policies
Extend consistent enterprise segmentation policy into the cloud

Ease of management
Orchestrate Cisco and cloud provider networking resources via vManage

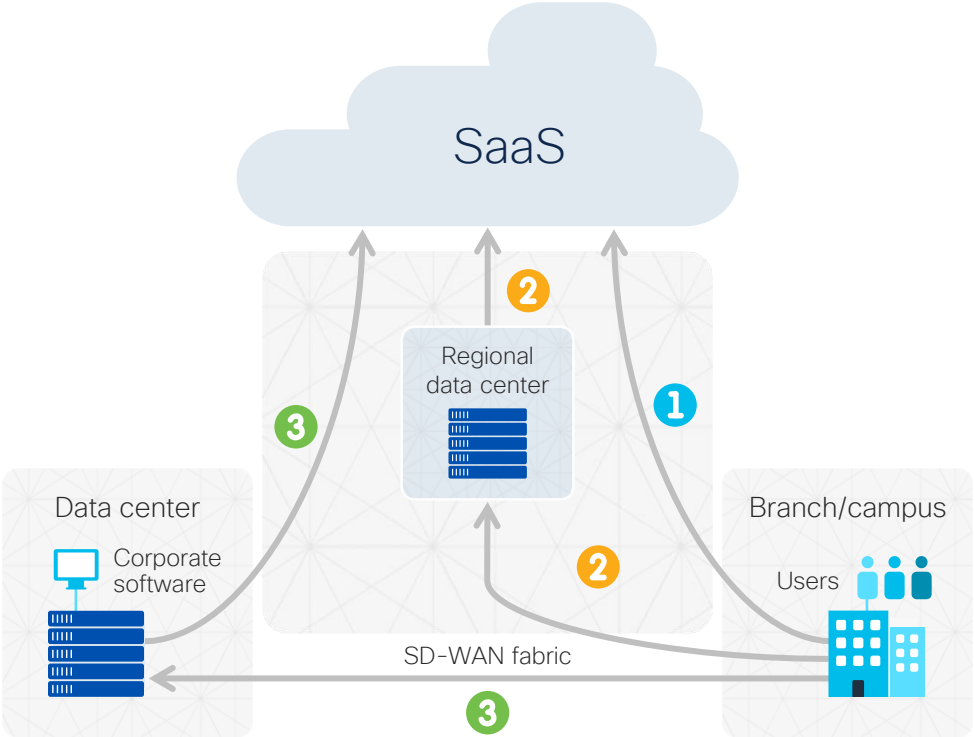
Introduction: Cloud Interconnect

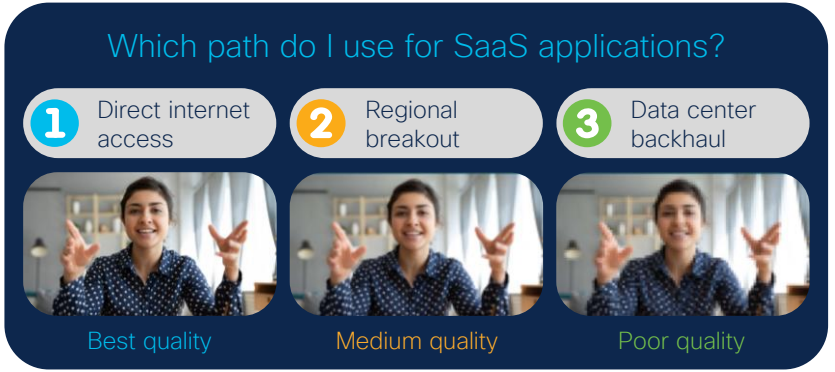


- Colocation
- CSP-independent
- SDN driven
- Same Use Cases

= Cisco SD-WAN router on-premises

Introduction: SaaS Optimization





- Own Probing to SaaS
- Cloud Telemetry for M365
- Custom App
- First Packet Match

Your voice matters!
Live poll during this session.

https://app.sli.do/event/d71oy65sDmvgK1YB67RkoU

PI

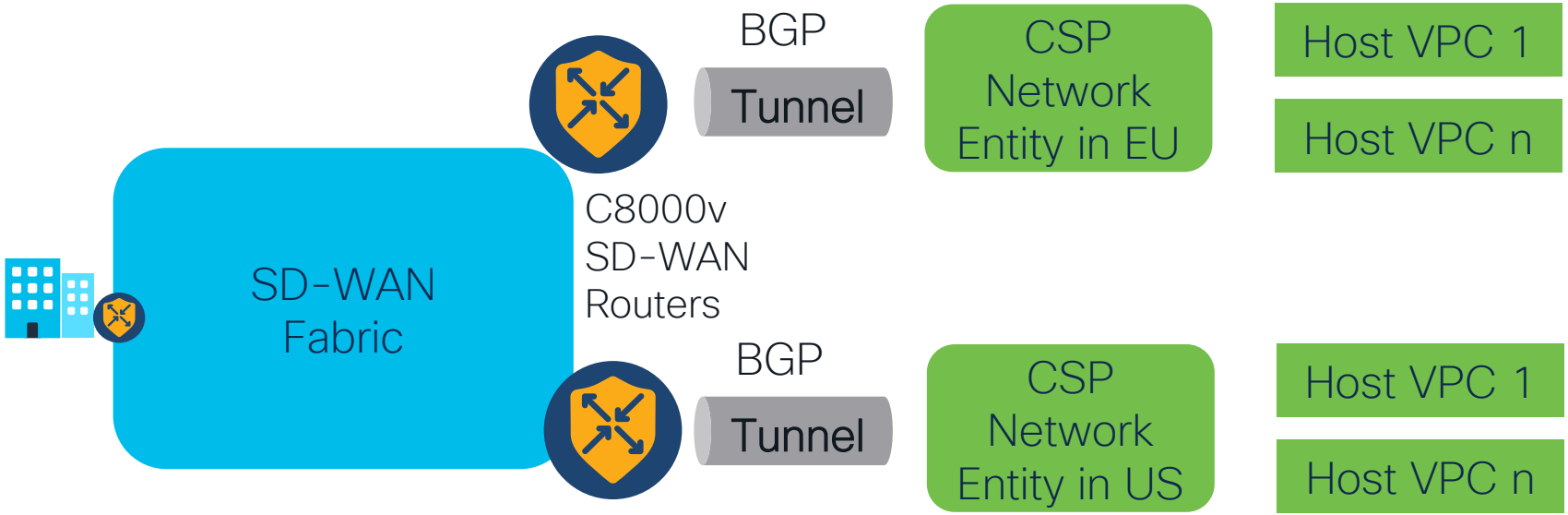
what are the most critical problems of public cloud?

The most critical problems of public cloud include:

1. Security concerns: As the data is stored on shared servers, there is always a risk of security breaches and cyber attacks.
2. Downtime and Availability: Public cloud services can experience downtime due to various reasons such as maintenance, server failures, and network outages.
3. Cost: While public cloud services can be cost-effective for small and medium-sized businesses, the cost can escalate quickly for larger organizations with high resource usage.
4. Interoperability: Different public cloud providers offer their services using proprietary technologies, which can make it difficult to seamlessly integrate with other cloud services or on-premise systems.
5. Complexity: The management of a large-scale public cloud infrastructure can be complex, requiring specialized skills and resources.
6. Compliance and Regulation: Certain industries, such as financial services and healthcare, have strict regulations that dictate the handling of sensitive data. Public cloud services may not always meet these regulatory requirements.

Site-to-cloud

Same design principle for all CSPs

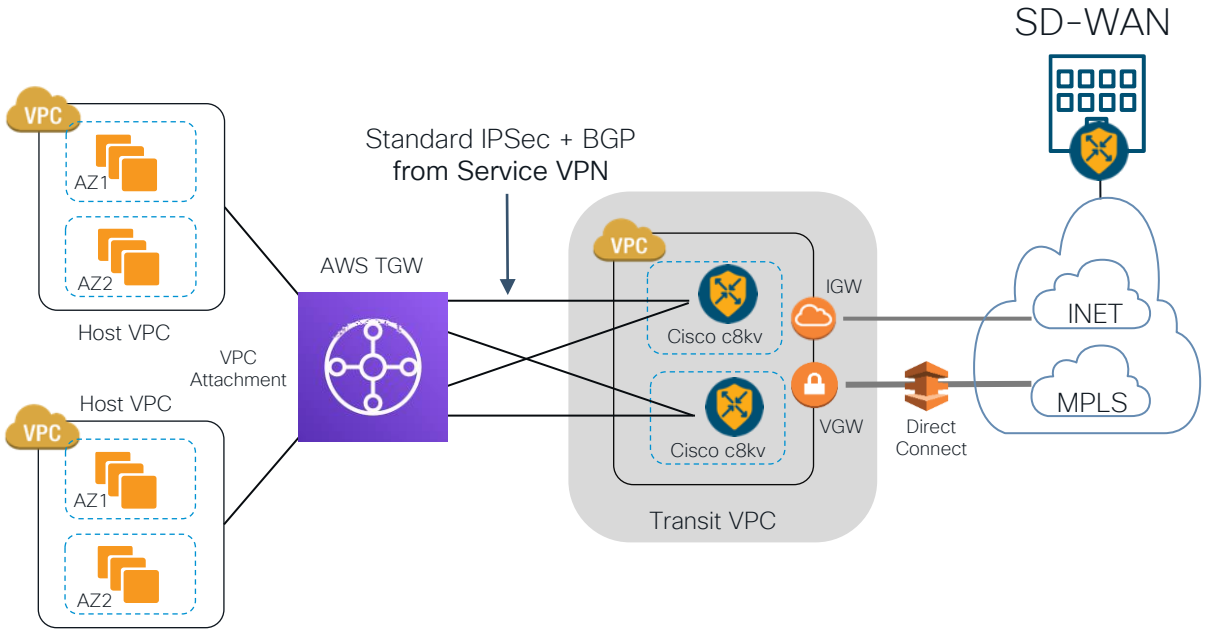


- Establish IPSec or GRE tunnel between c8kv and Cloud
- Learn cloud routes via BGP
- Mutually Redistribute OMP <-> BGP

Next step: automate this design
AWS as example

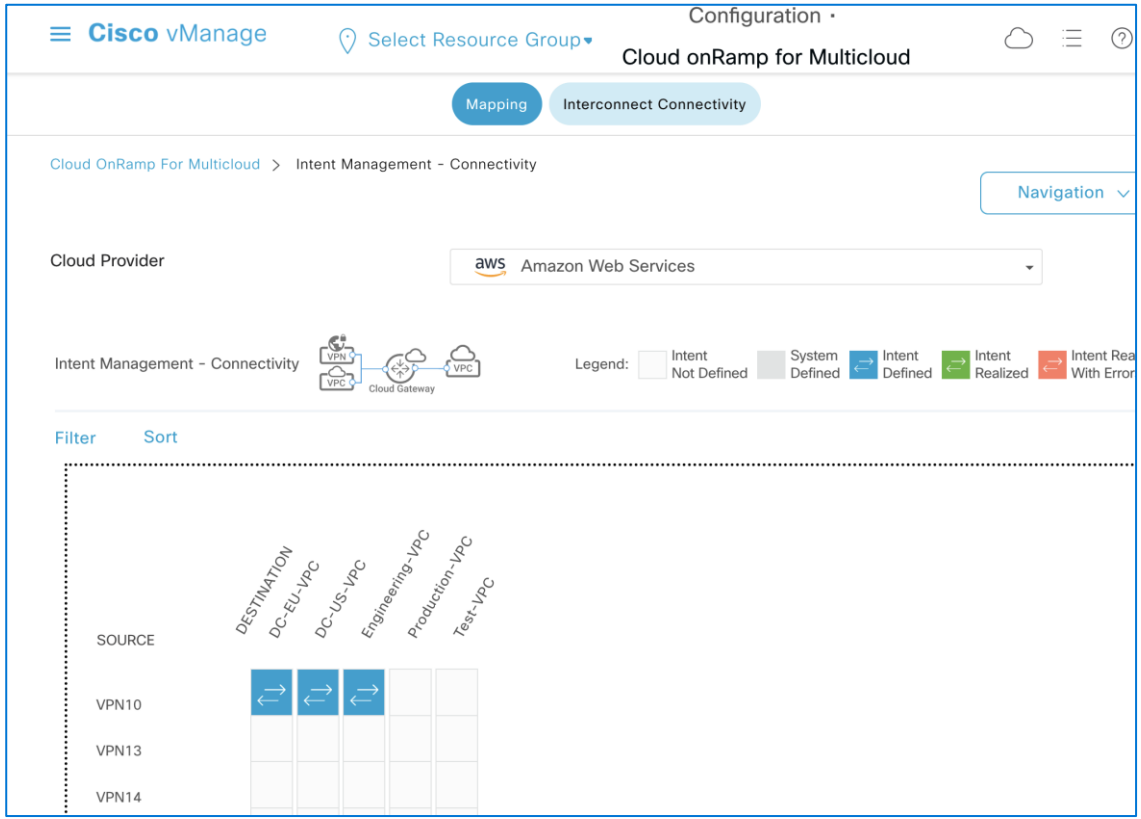
Single UI vManage Workflow:

1. have two c8kv ready
2. define AWS Account
3. discover and tag host VPCs
4. deploy CGW (c8kv + TGW)
5. Map host VPCs to SD-WAN



18

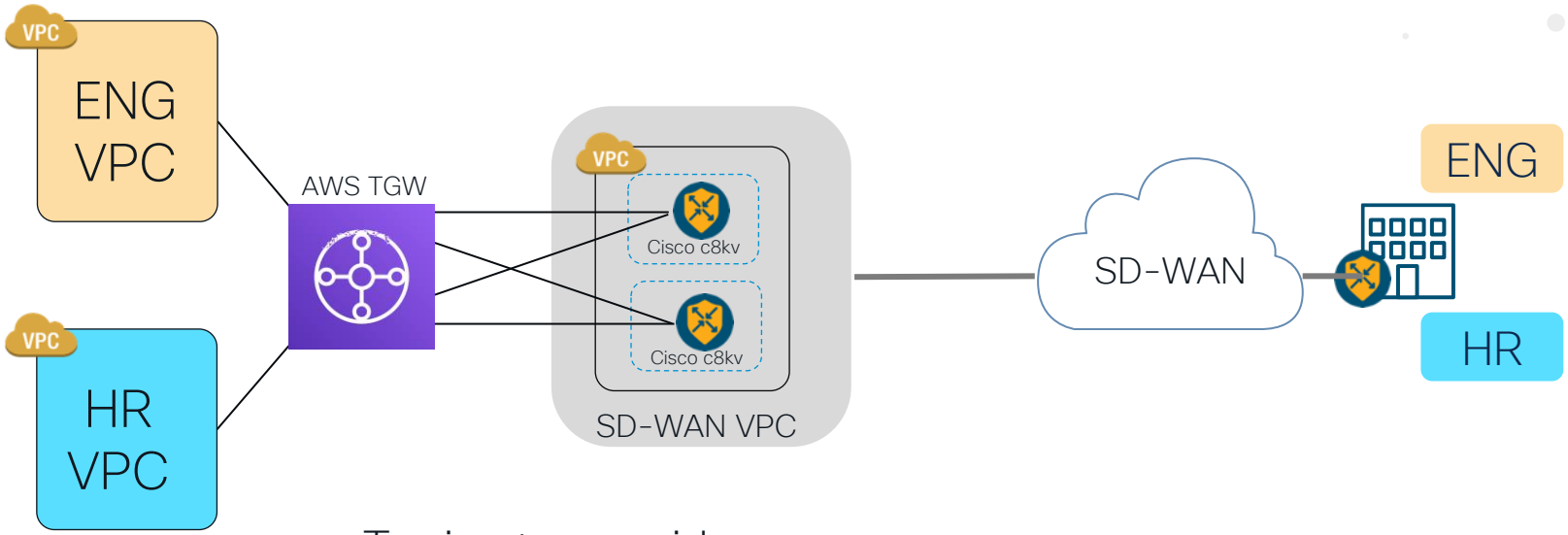
Your Main benefit: single UI for SD-WAN and Cloud



Same workflow for all CSPs!

Segmentation

Mapping different SD-WAN networks with different cloud VPCs



Topics to consider:

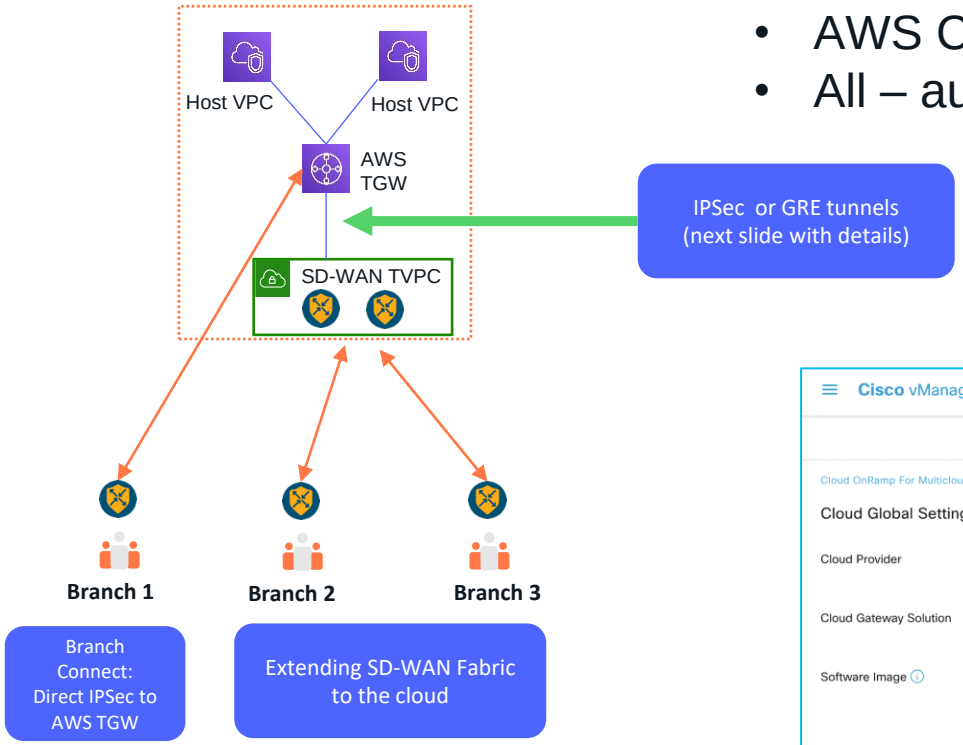
- Automated in vManage single UI
- Overlapping IP addresses

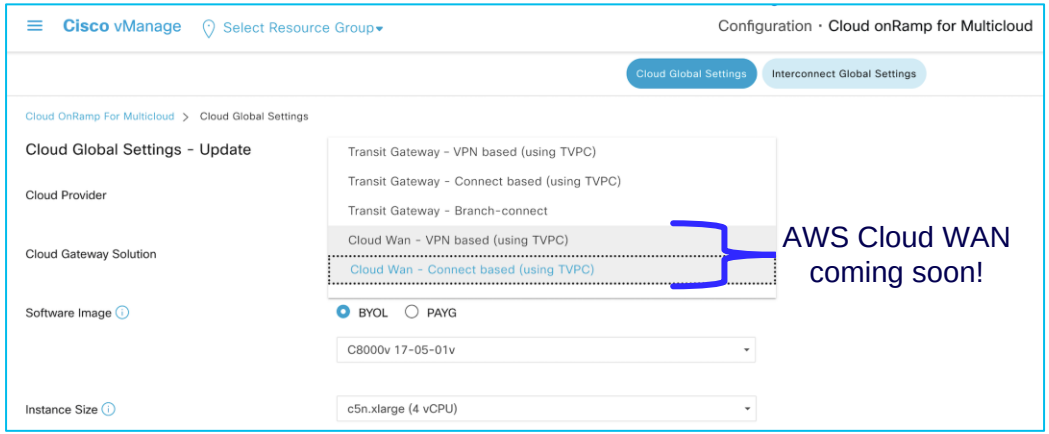
Under the hood: different route tables on TGW

SD-WAN on AWS

Design details for AWS

- 3 different Solutions supported today
- AWS Cloud WAN support coming soon
- All – automated in Cisco vManage!

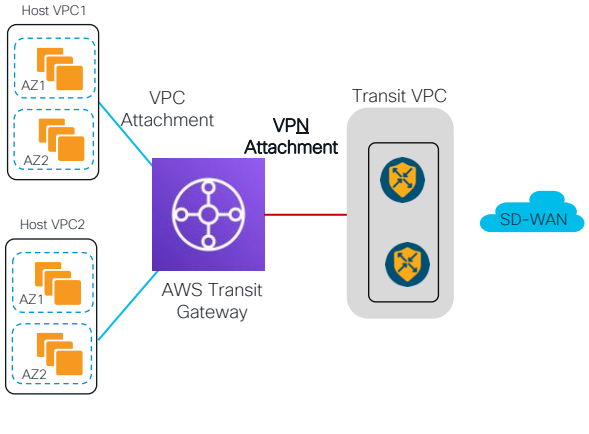




Different connectivity options to AWS TGW available today

vManage

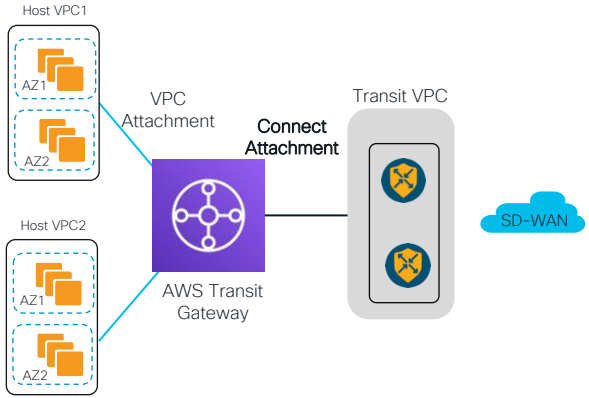
SD-WAN via VPN Attachment



- SD-WAN Routers in Transit VPC establish BGP over IPSec tunnels to TGW
- Automated workflow including inter-region use case with Cloud onRamp for Multicloud
- AWS TGW Limit of 1.25 Gbps for one IPSec Tunnel

vManage

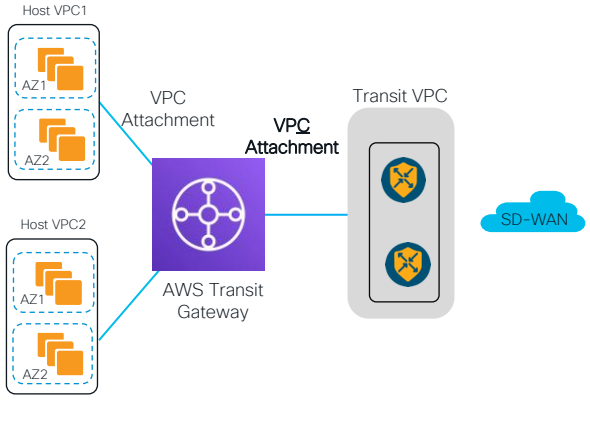
SD-WAN via TGW Connect



- GRE tunnel to TGW instead of IPSec: 5 instead of 1.25 Gbps
- Usage of private IP for GRE tunnel possible
- Automated as Cloud onRamp for Multicloud

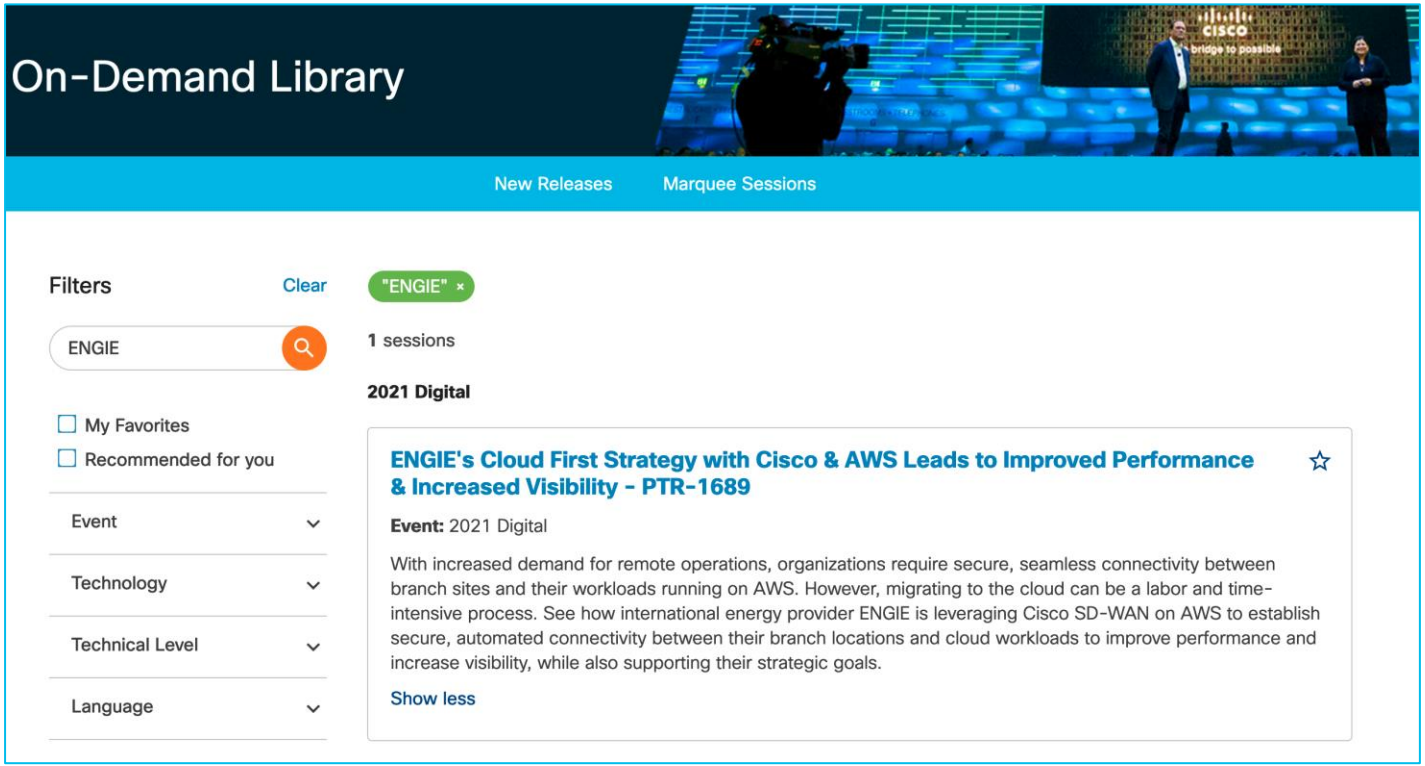
Custom automation

SD-WAN via VPC Attachment



- No dynamic routing between SD-WAN routers and TGW
- SD-WAN Routers in Transit VPC have TGW as next hop for cloud routes
- Scales up to 50 Gbps TGW Limit.
- C8kv VM performance depends on the AWS VM type
- No Cloud onRamp automation, custom automation needed

Adoption: Customer Case Study



https://aws.amazon.com/partners/success/engie-cisco/

SD-WAN on Azure

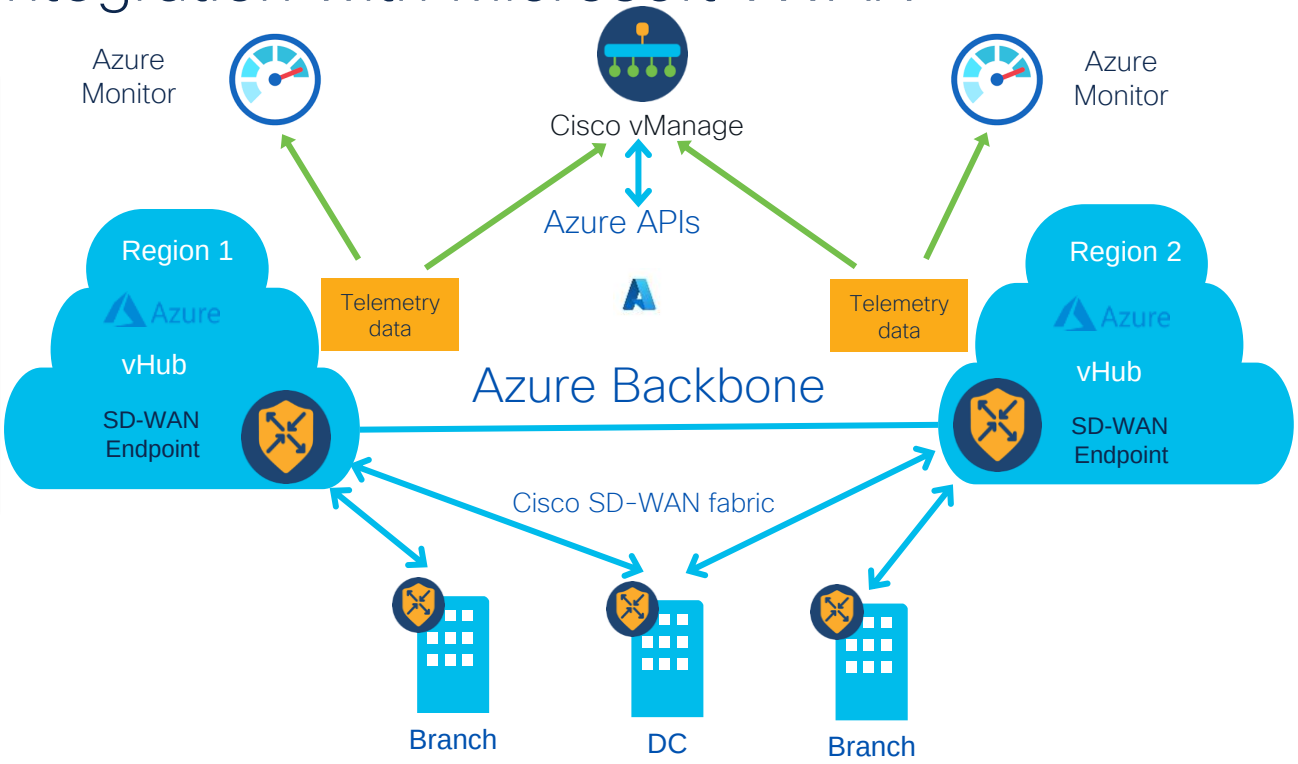
Cisco SD-WAN integration with Microsoft vWAN

Different Terminology
vWAN, vHub and VNet

Very similar design, same use cases
C8kv as vHub Service Endpoint

Segmentation
One Route Table, no n:m segmentation yet

Security
Integration with Azure Firewall.



Multiple vHubs per Azure Region

From 20.11 SW Release

Problem

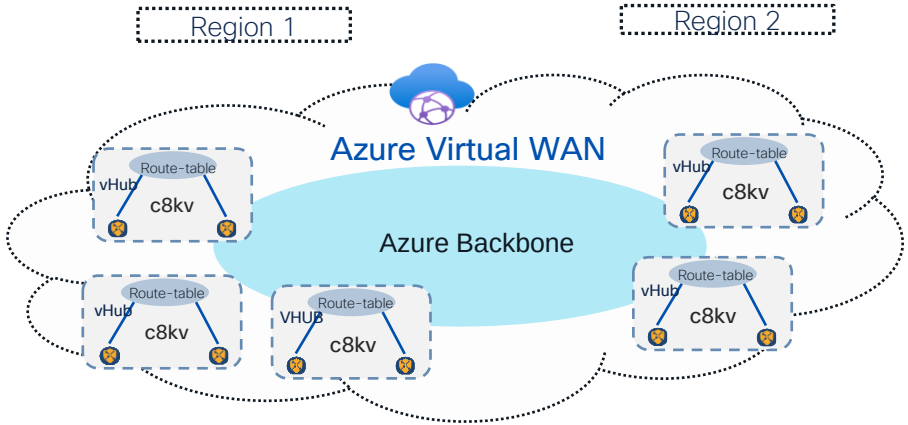
CoR Azure vWAN solution supports only one vHub in single region. For large scale deployments would like to extend the SD-WAN Fabric to more than one vHub per Region as Single vHub can only scale up to 1000 sites per region.

Solution

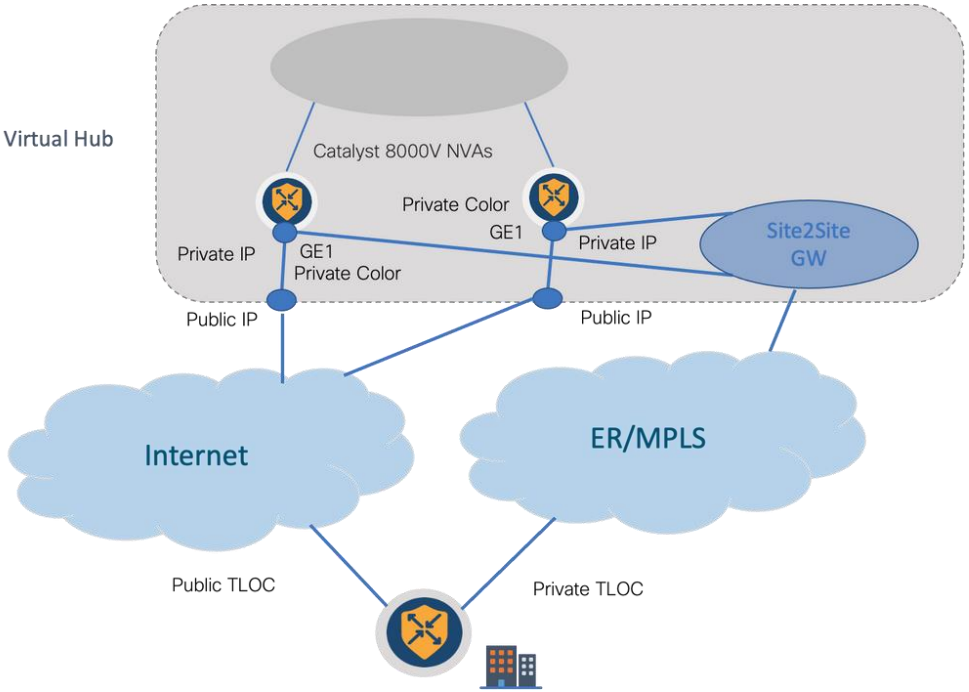
- Cloud OnRamp for Multi-Cloud now supports customers to deploy Cloud Gateways into multiple Virtual Hubs within the same region
- Cloud Gateways (c8kv) will advertise all VNets connected to all the vHubs, and we can direct traffic flows using SD-WAN Centralized policies.

Caveats

- No segmentation
- Supports up to 20 vHub per region



Azure Express Route as Transport with SD-WAN in a Click



Problem Statement:

- NVAs (c8kv) inside the vHub can only have two interfaces. One is for the service VPN and the other is for transport.
- Currently, the default template assigns a color of default to the transport interface. This means only TLOC with public colors can form tunnels to the NVA with public IPs.
- Express Route is a private link that uses a private IP address since the default template color is a public category that by nature tries to form the tunnels in public space where the express route can't reach.

Solution:

Change the color of GE1 of the NVAs inside the vHub from default to a private color. It allows the usage of both Express Route and Public Internet as SD-WAN transports.

Benefits:

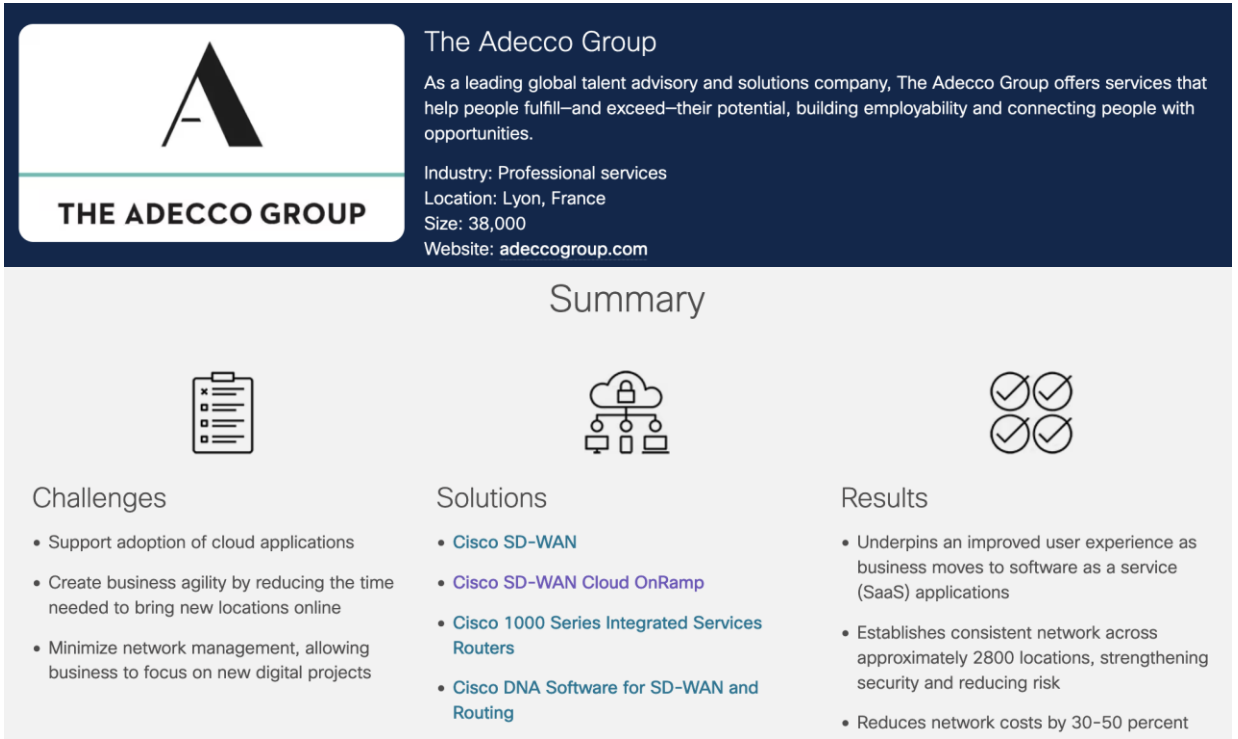
- redundant paths from edge locations to Azure Workload VNets
- higher throughput and lower latency

Private Colors:	Public Colors:
metro-ethernet mpls private1-private6	3g, lte biz-internet public-internet blue, green, red gold, silver, bronze

If two ends have a private color: private IP address used for SD-WAN connection.
If endpoint has public color: public IP is used.

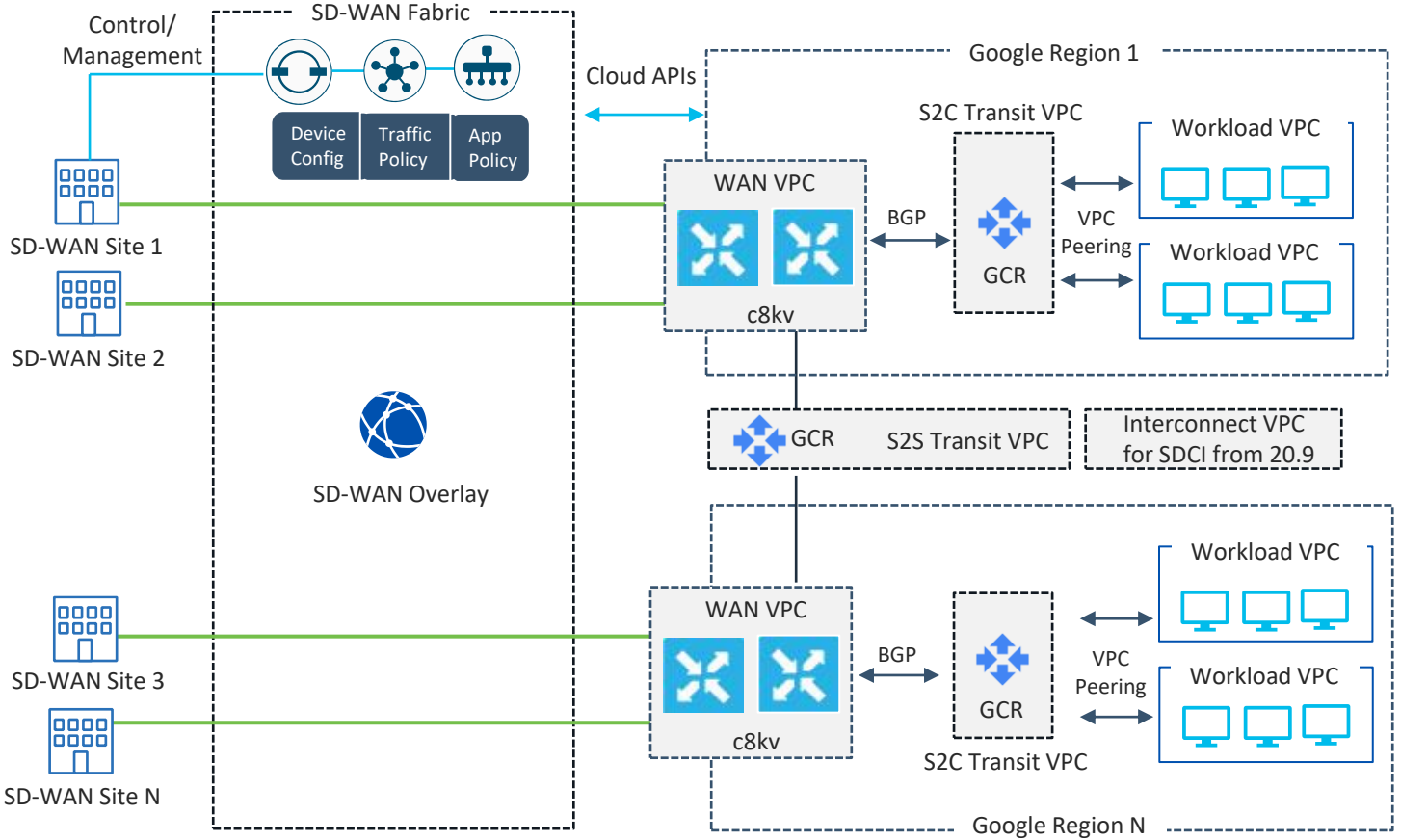
Adoption: CoR on Azure

- 100+ CoR Multicloud Deployments on Azure
- Azure examples: Adecco, URC Vietnam



SD-WAN on GCP

GCP Technical Design: High Level for site-to-cloud and site-to-site use cases



Google Network Connectivity Center (NCC)

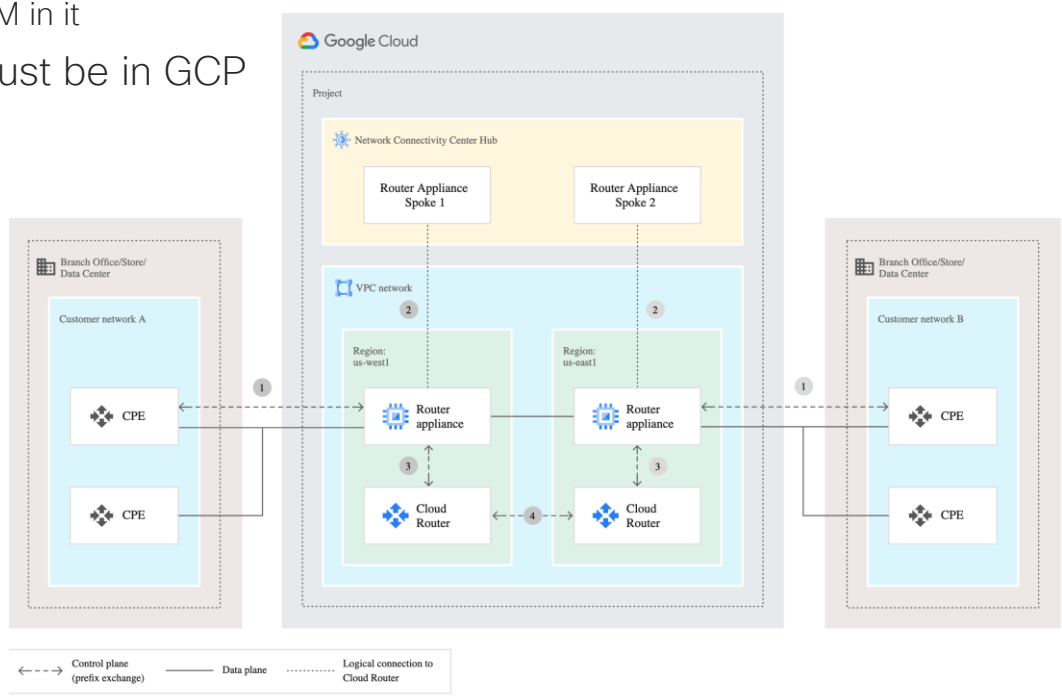
GCP Networking is different - global virtual networks that are truly global:

1. create a VPC network
2. create a subnet in the US, put your US VM in it
3. create a subnet in Singapore, put your Singapore VM in it

Non-technical reason: source and dest. IP must be in GCP

Details:

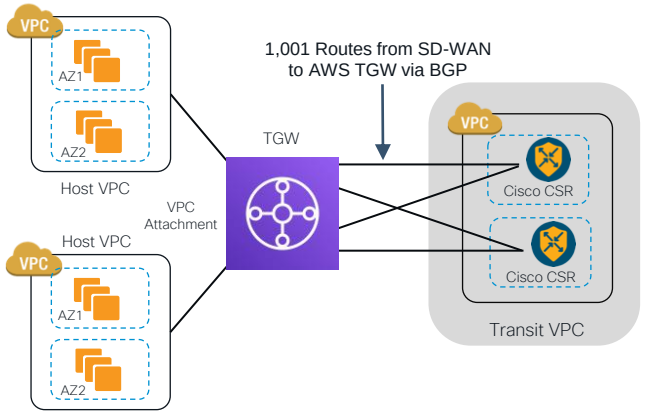
- Hub-and-spoke model
- Pure Connectivity Management
- Data plane – direct SD-WAN tunnel between two c8kv in different regions



Customizing Cloud onRamp

Problem definition

- You successfully deployed CoR for Multicloud with Transit VPC, AWS TGW and two SD-WAN Routers
- AWS TGW gets <u>all</u> routes, but you want to send only few of them to TGW.
- If you send more than 1,000 routes, BGP goes down.
- There is no BGP template for CoR in vManage, where you can do route filtering!



Solution: Add-on CLI Template!

Let's look at the configs

Router Config

```
route-map AWS_TGW_CSR_ROUTE_POLICY deny 1
 match as-path 15
!
route-map AWS_TGW_CSR_ROUTE_POLICY permit 11
 match as-path 25
!
route-map AWS_TGW_CSR_ROUTE_POLICY deny 65535
```

CLI Add-On Template

```
route-map AWS_TGW_CSR_ROUTE_POLICY permit 110
 match as-path 250
!
```

Result

```
route-map AWS_TGW_CSR_ROUTE_POLICY deny 1
 match as-path 15
!
route-map AWS_TGW_CSR_ROUTE_POLICY permit 11
 match as-path 25
!
route-map AWS_TGW_CSR_ROUTE_POLICY permit 110
 match as-path 250
!
route-map AWS_TGW_CSR_ROUTE_POLICY deny 65535
```

Performance

Performance in the cloud

Scale options:

- Horizontal Scale = spin up many VMs
- Single VM Scale = use the top instance type

Questions to consider:

- Packet size: Jumbo / Large / IMIX
- Automation for horizontal scale
- Cloud Limitations (may be not visible at the first look)

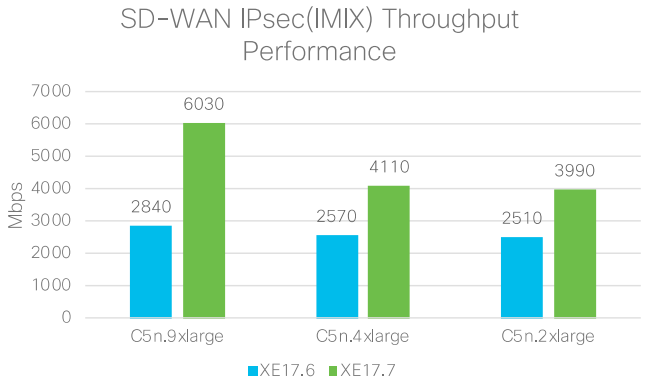
Performance Details for C8kv on AWS

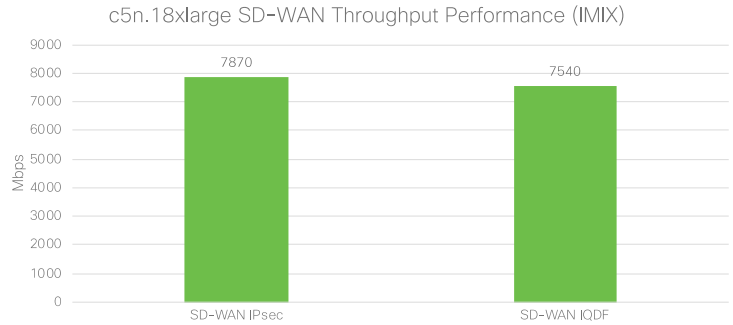
Performance

- With SD-WAN v17.9/20.9 c8kv can use c5n.18xlarge VM type
- Before that, then biggest VM size was single c8kv C5n.9xlarge, which had the following SD-WAN performance with IPSec+QoS+DPI+FNF profile : up to 15.2 Gbps with large packets
- IMIX performance jump: from 6 Gbps to 7.9 Gbps IMIX
- Jumbo Frame Performance 50+ Gbps VPC-to-VPC

Caveats

- 17.7 perf improvement is achieved with AWS Multi-TxQs, means a setup with 8 SD-WAN IPsec Tunnels. Same apply to c5n.18x in 17.9.





Performance Details for C8kv on Google Cloud

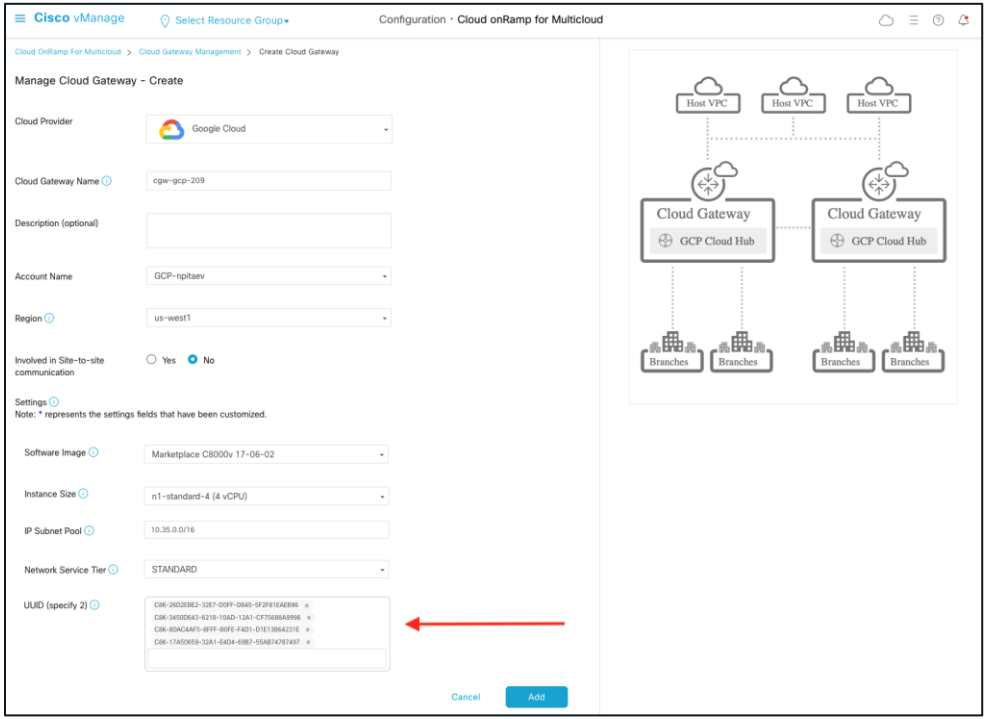
GCP Horizontal Scale

17.9 introduces ability to spin up up to 8 Catalyst 8000v SD-WAN routers as a part of Cloud Gateway creation, which address high bandwidth requirements for GCP.

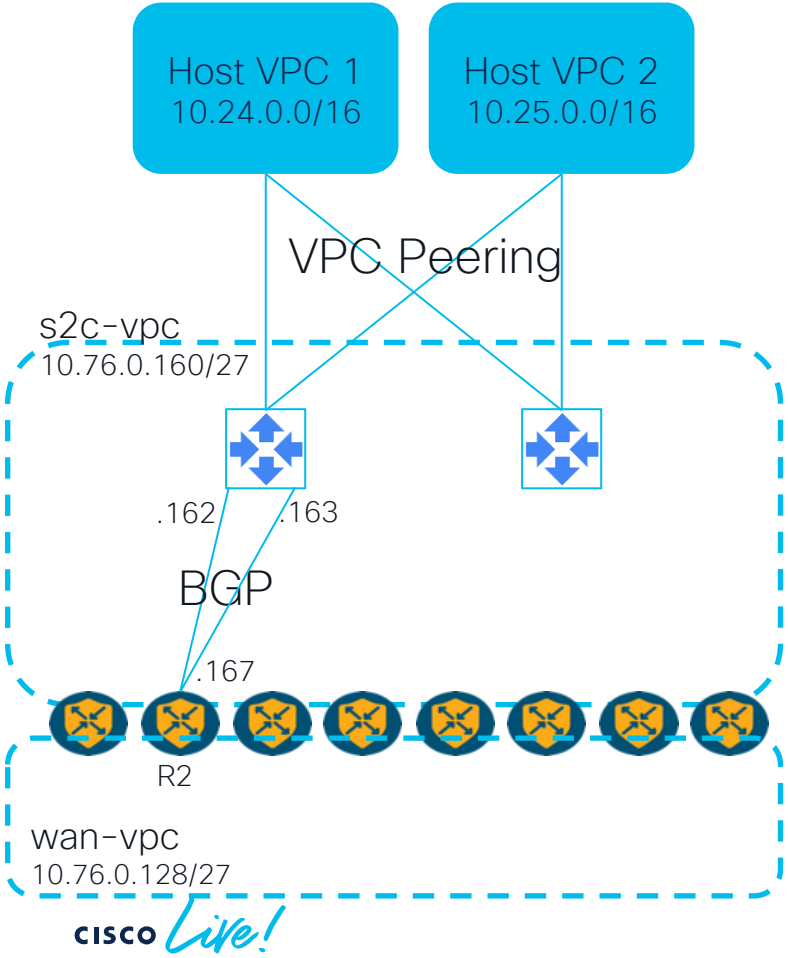
Single VM c8kv IMIX Performance is appr. 2 Gbps

Caveats

- Number of c8kv routers per region is between 2 and 8.
- Static configuration, no dynamic scale (yet) based on utilization or other KPIs.



Example with 8 x C8kv on Google Cloud



- Two BGP sessions for redundancy

R2 vrf 10 route table:
B 10.24.0.0/16 [20/100] via 10.76.0.161

- .161 is the default gateway for s2c VPC
- We do not have technical data for scale beyond this point.
- Assumption – GCP is not a bottleneck

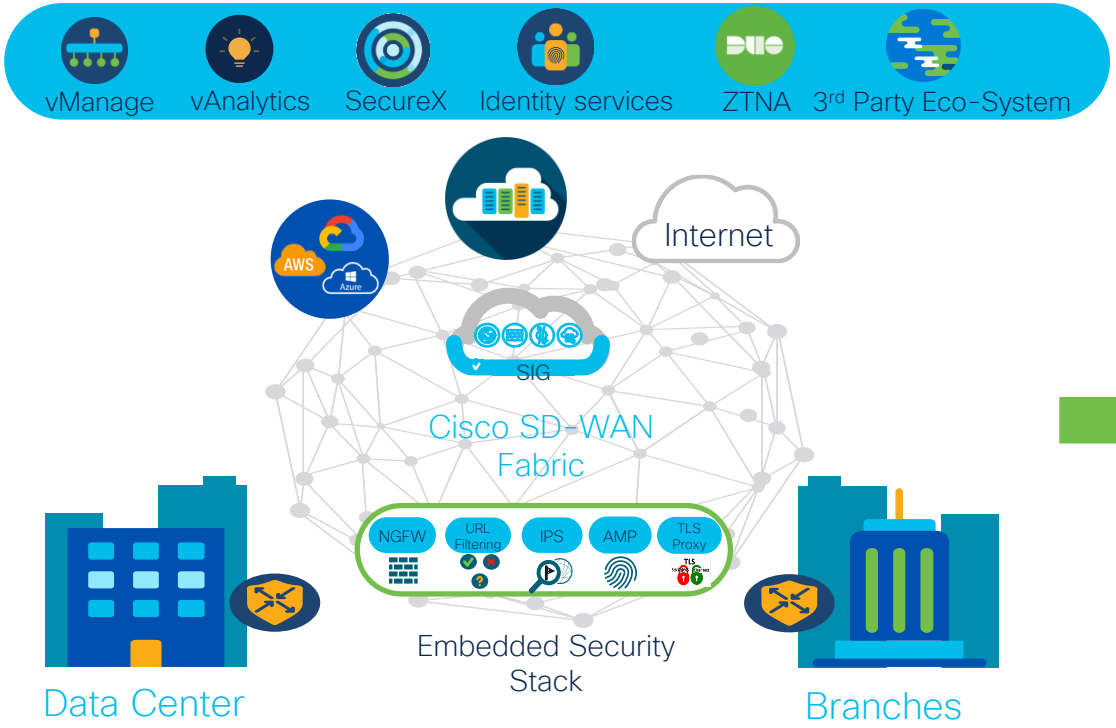
Performance on Azure

- Cloud onRamp (CoR) will spin up 2 c8000v in SD-WAN VPC

- Azure: SKU scale up to 5 Gbps
  Targeted for 20.12/17.12:
  20 Gbps (4 X sku 10 + 1n)
  40 Gbps (4 X sku 20 + 1n)

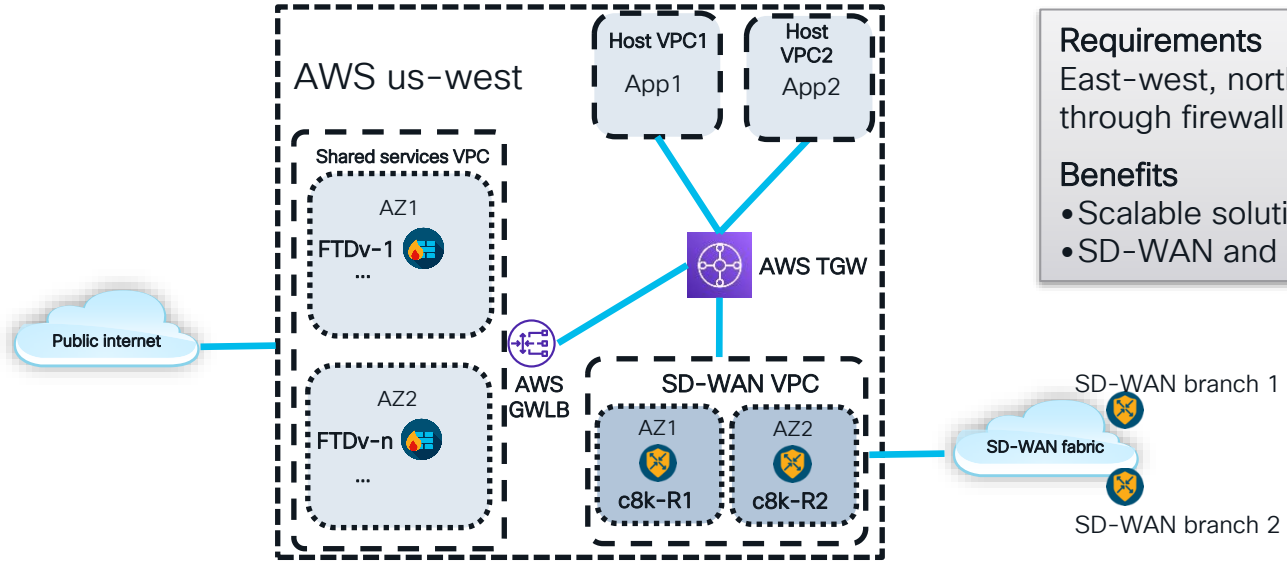
Security

SD-WAN Security – Overview



- SASE
- Identity Zero Trust
- Unified Policy Management
- Distributed Security Enforcement
- Secure Internet Gateway
- Visibility & Reporting

AWS: Centralized Firewall Design



Requirements

East-west, north-south traffic must go through firewall

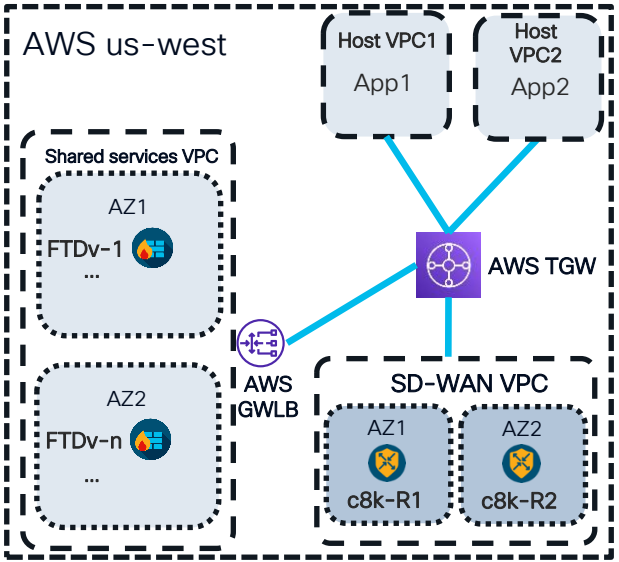
Benefits

- Scalable solution
- SD-WAN and security from one hand

Full Details: https://youtu.be/LHdW_0C3Y6E?t=351

GitHub Repo: https://github.com/CiscoDevNet/sdwan-cor-labinfra

Packet flow: Simplified



From Host VPC to SD-WAN
Host VPC ➔ AWS TGW ➔ GWLB ➔ FTDv ➔ TGW ➔ SD-WAN

Returning traffic
SD-WAN ➔ AWS TGW ➔ GWLB ➔ FTDv ➔ TGW ➔ Host VPC

GENEVE protocol for load balancing between GWLB and FTDv

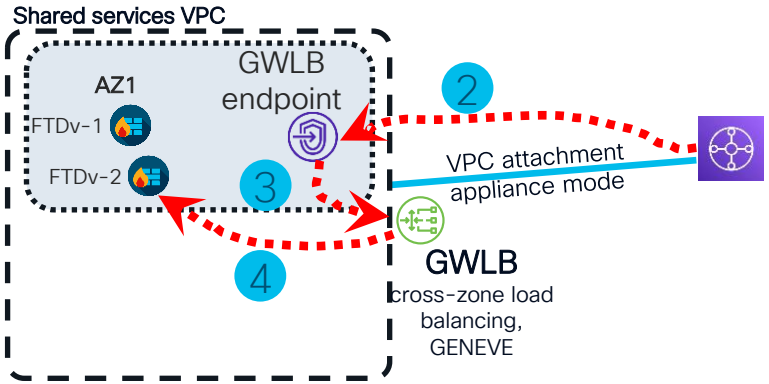
Appliance mode is required for symmetric routing

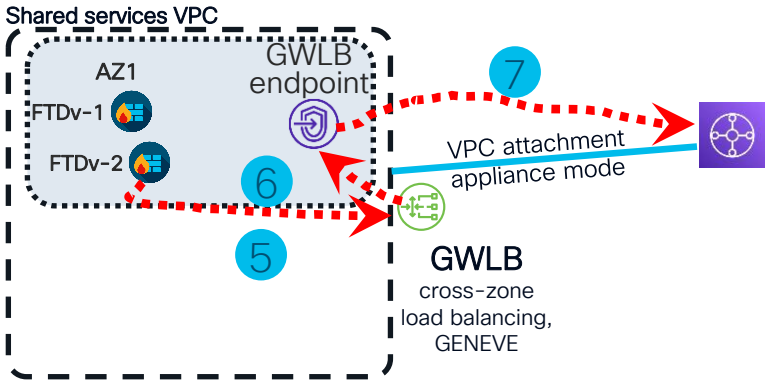
FTDv = Secure Firewall Threat Defense Virtual (aka FTDv / NGFWv)
GWLB = AWS Gateway Load Balancer

Geneve = Generic Network Virtualization Encapsulation
AZ = Availability Zone (AWS data center)

Packet flow: Details for shared services VPC

For Your Reference





Step 2: TGW routes to GWLB endpoint – shared services route table

10.102.0.0/16	local		
0.0.0.0/0	vpce-XYZ	FW-Endpoint-Service-AZ1	10.102.3.91

Step 3: GWLB endpoint routes traffic to GWLB using AWS PrivateLink

Step 4: GWLB routes traffic to a firewall using GENEVE

Target Group: FW-Target-Group-Geneve with 4 firewalls:

10.102.3.174	MC-FTD-IFT-1	6081	us-west-AZ1
10.102.13.67	MC-FTD-IFT-2	6081	us-west-AZ1

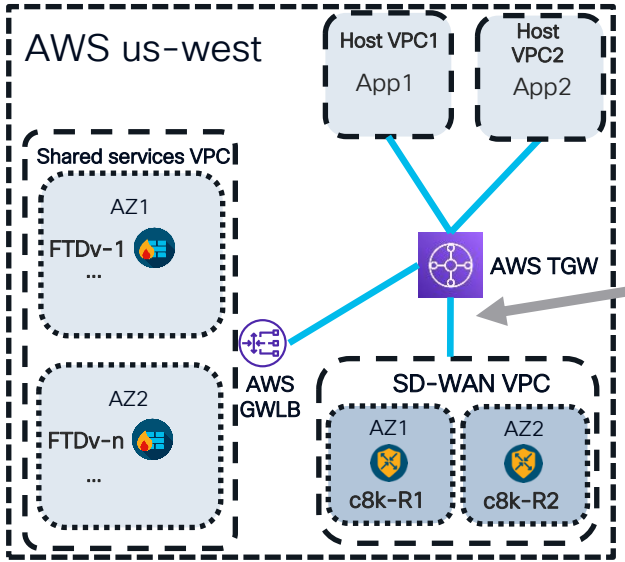
...

Step 5: Firewall decapsulates GENEVE, inspects the packet, re-encaps and sends it back to GWLB

Step 6: GWLB removes GENEVE header and forwards packet to the appropriate GWLB endpoint

Step 7: GWLB endpoint sends packet to TGW

Connecting SD-WAN



VPN or connect attachment for SD-WAN VPC

BGP between AWS TGW and SD-WAN routers

Cisco Catalyst 8000V as SD-WAN router

Multi-Region via TGW Peering, AWS Cloud WAN support in near future

Automation: GitHub repo SD-WAN CoR LabInfra

Site-to-Site over CSP

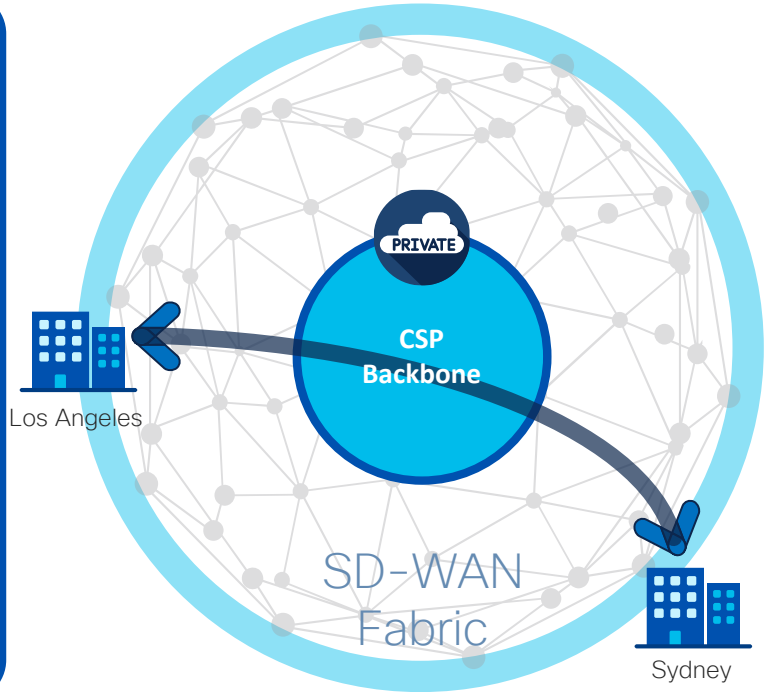
Site-to-Site over Cloud Service Provider

Key Highlights

Created in less than 5 minutes using vManage

Dedicated, global connectivity provisioned via CSP backbone

Premium, low-latency MPLS-like performance with Pay-as-you-Go model



Customer Benefits

Reduced provisioning time from months, to 5 minutes

Reduced latency from 560ms to 200ms

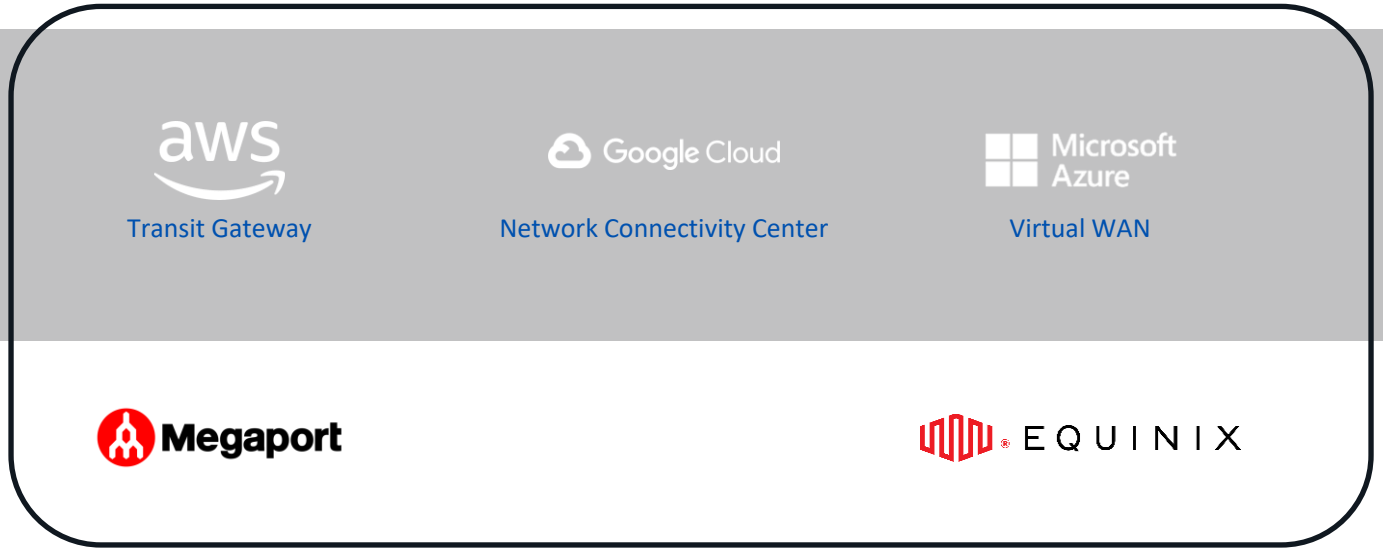
Reduced cost from $10K/mo to $2K/mo

Supported cloud networking integrations

Multicloud integration

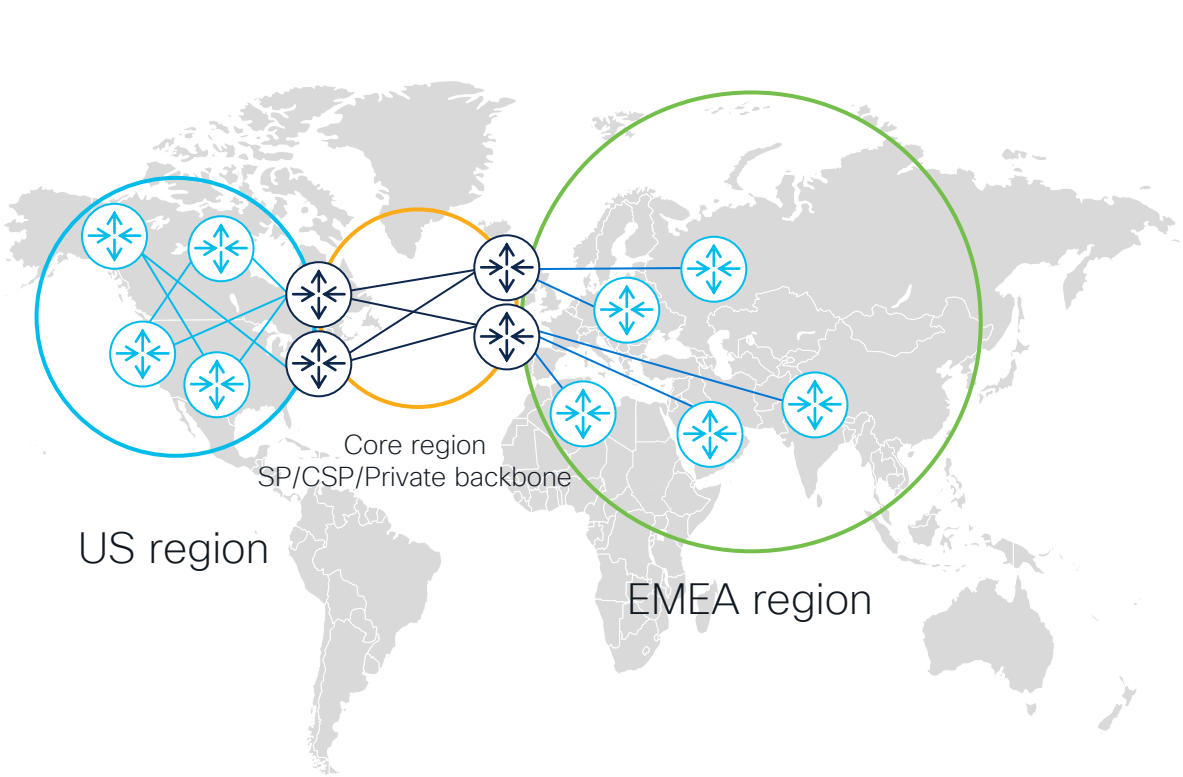
Cloud backbone

Cloud agnostic backbone



Site-to-Site automated in vManage

Multi Region Fabric solves many Multicloud S2S Challenges

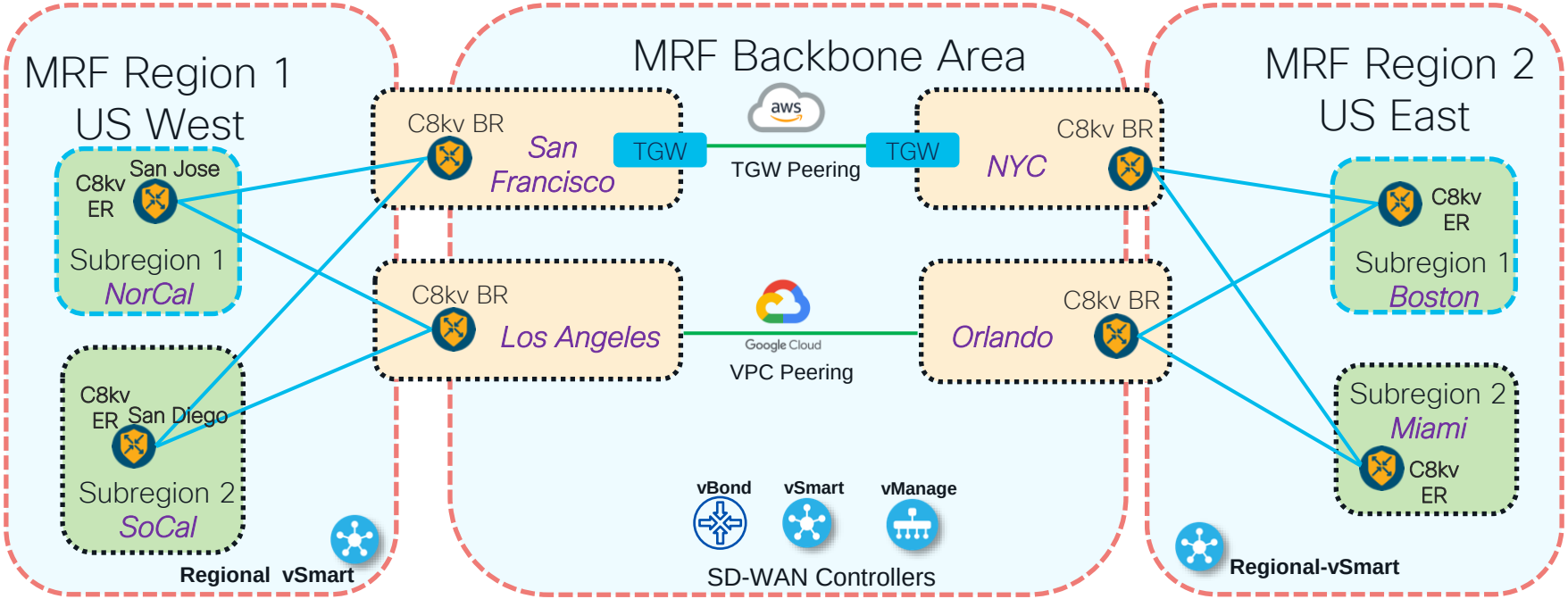


BR/regional hub

ER/branch

- Intuitive user-defined site grouping. E.g. based on geo
- Finer grouping using sub-regions
- Auto restrict overlay tunnels between regions
- Different topologies per region
- Mix access transports across regions
- Scale up control-plane per region(s)

Multi Region Fabric simplifies Multicloud Design

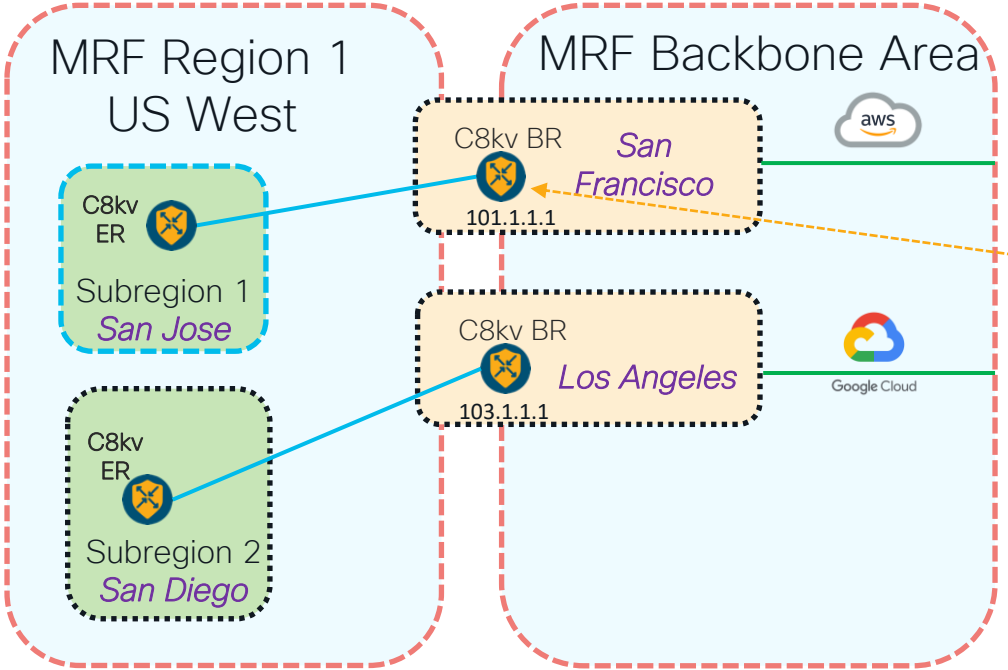


Two Key Customer Requirements / use cases:

1. Independent providers in the MRF backbone area for site-to-site communication
2. Easily isolate specific CSP subregions (cities or countries) in emergency case on demand

Terraform Scripts: https://github.com/CiscoDevNet/sdwan-cor-labinfra

Use Case 1: Redundancy / Load Balancing



Details:

- *Subregion 1 (SJ) uses by default San Francisco*
- *Subregion 2 (San Diego) uses LA*
- *In case of a single backbone failure -> auto failover*

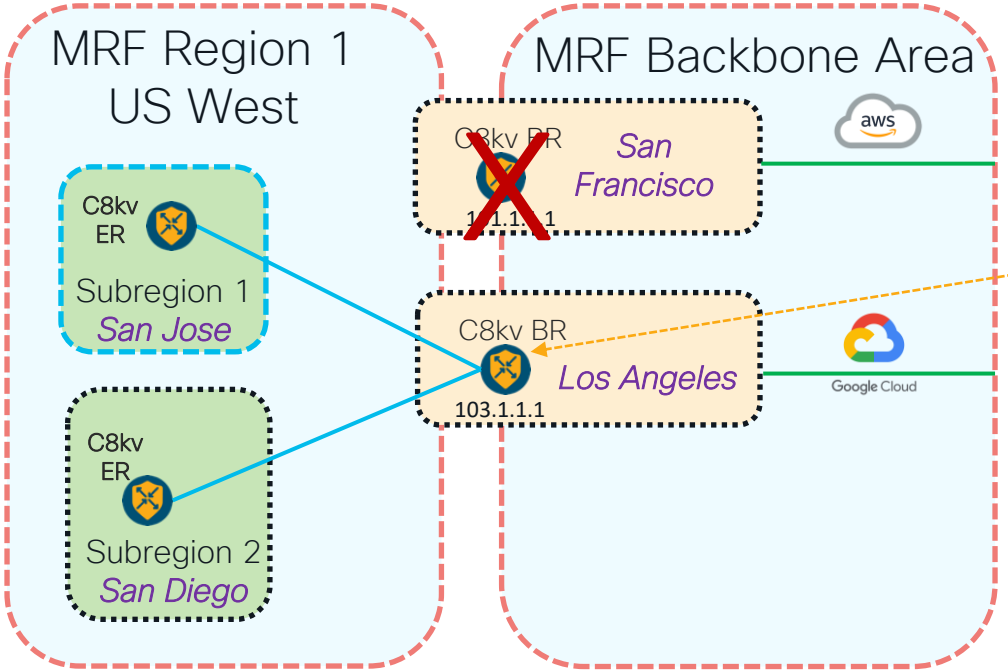
Border router 1 configuration:

```
system
 system-ip          101.1.1.1
 site-id            101
 region 1
 subregion 1
 !
 role               border-router
 organization-name  mrf-multicloud-demo
 vbond 44.227.177.103
!
```

Route Table Entry on Edge Router **for 10.211.1.11 on the** "east side"

```
Reg1-Sub1-ER1#sh ip ro vrf 10
...
m       10.211.1.11 [251/0] via 101.1.1.1, 06:58:01, Sdwan-system-intf
...
Reg1-Sub1-ER1#
```

Use Case 1: Redundancy / Load Balancing



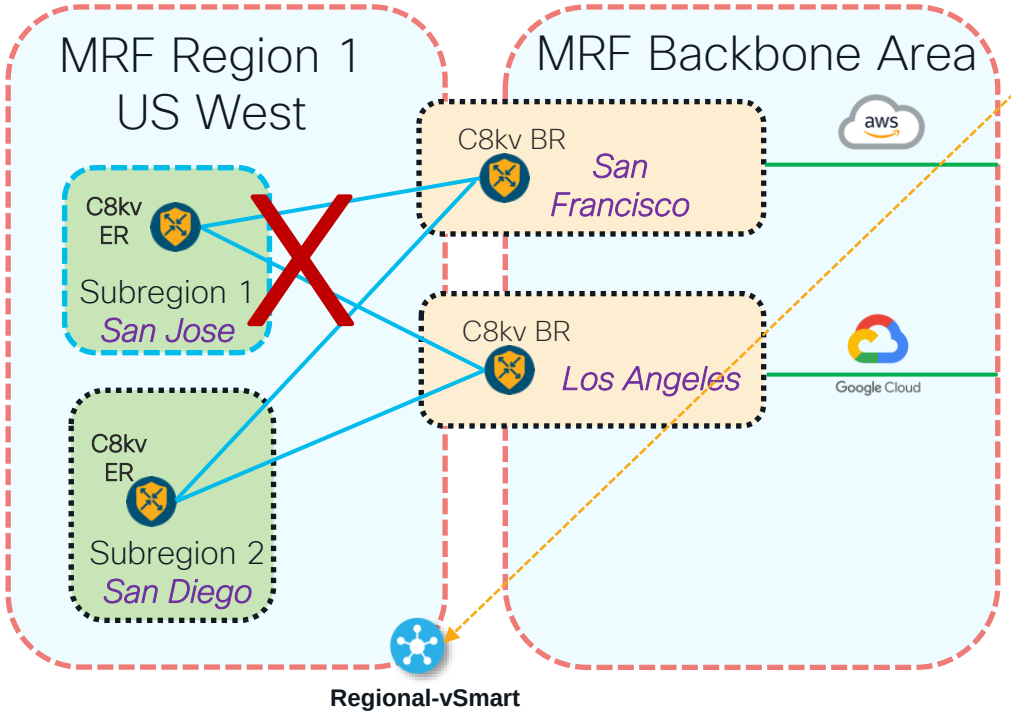
Border router 2 configuration:

```
system
 system-ip          103.1.1.1
 site-id            103
 region 1
 subregion 2
 !
 role               border-router
 organization-name  mrf-multicloud-demo
 vbond 44.227.177.103
!
```

Route Table Entry on Edge Router **for 10.211.1.11 on the** "east side"

```
Reg1-Sub1-ER1#sh ip ro vrf 10
...
m       10.211.1.11 [251/0] via 103.1.1.1, 06:58:01, Sdwan-system-intf
...
Reg1-Sub1-ER1#
```

Use Case 2: Isolate a subregion with a simple control policy

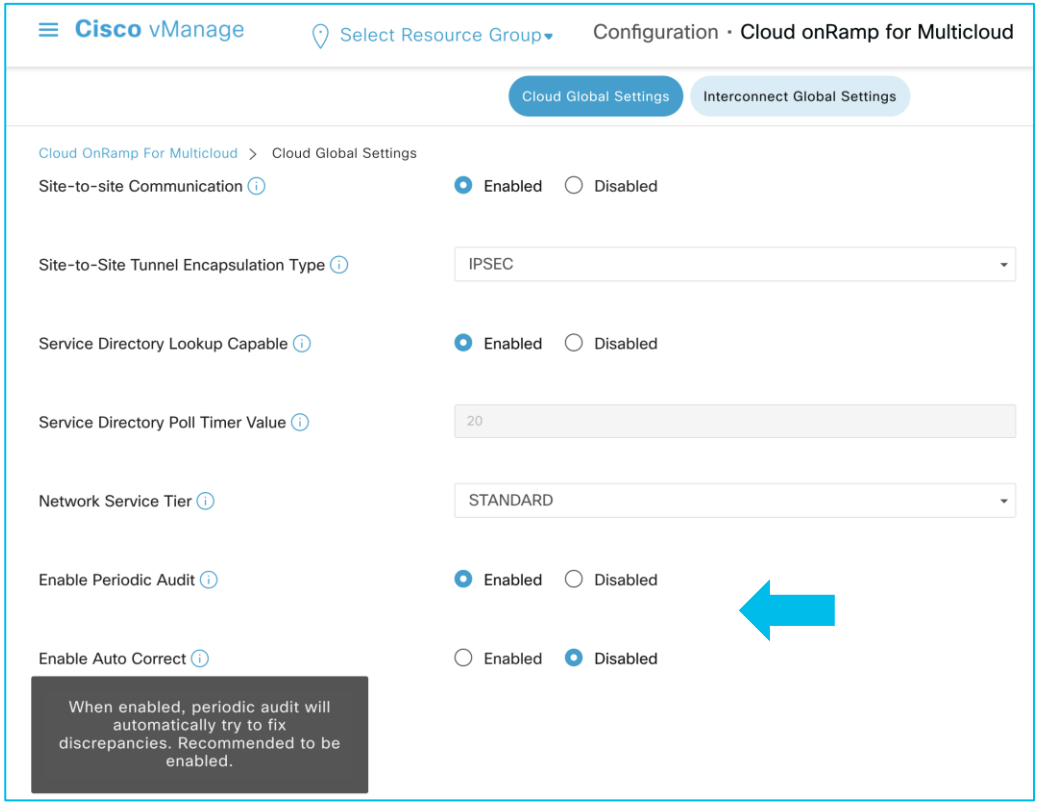



```
policy
 control-policy block-reg1-sub1
  sequence 1
   match route
    region-enhanced region 1
    region-enhanced subregion 1
   !
   action reject
   !
  !
  sequence 2
   match tloc
    region-enhanced region 1
    region-enhanced subregion 1
   !
   action reject
   !
  !
  default-action accept
 !
!
apply-policy
 region 1
  role border-router
  control-policy block-reg1-sub1 out
 !
!
```

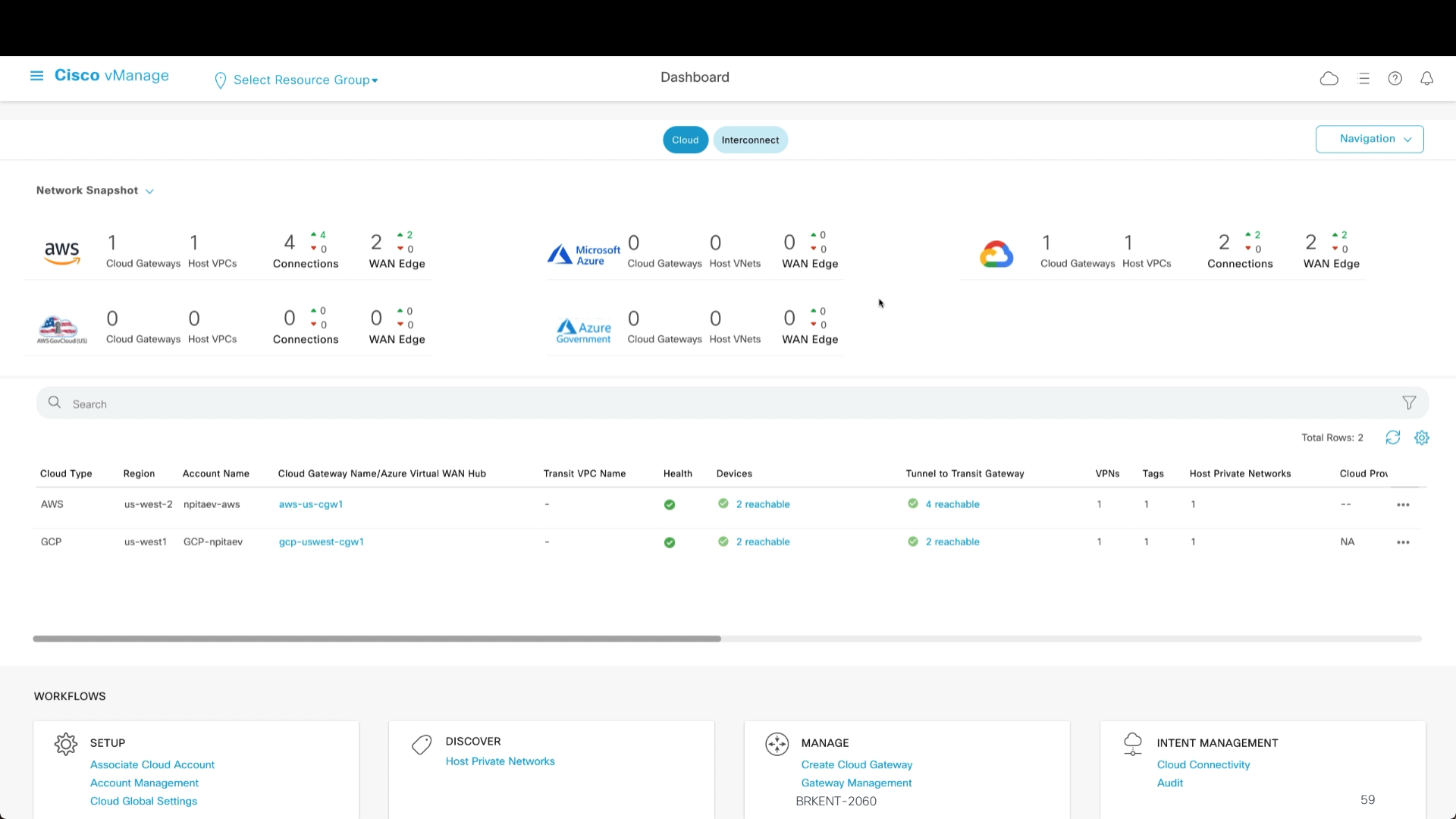
Audit simplifies daily operations

Cloud Audit

- State check
  vManage vs. Cloud
- Every two hours & on-demand
- Configurable Auto Correct



Demo:
Cloud Audit


Cisco vManage
Select Resource Group
Dashboard
Cloud
Interconnect
Navigation
Network Snapshot
1 Cloud Gateways 1 Host VPCs 4 Connections 2 WAN Edge
0 Cloud Gateways 0 Host VNets 0 WAN Edge
1 Cloud Gateways 1 Host VPCs 2 Connections 2 WAN Edge
0 Cloud Gateways 0 Host VPCs 0 Connections 0 WAN Edge
0 Cloud Gateways 0 Host VNets 0 WAN Edge
Search
Total Rows: 2
Cloud Type | Region | Account Name | Cloud Gateway Name/Azure Virtual WAN Hub | Transit VPC Name | Health | Devices | Tunnel to Transit Gateway | VPNs | Tags | Host Private Networks | Cloud Prov
AWS | us-west-2 | npitaev-aws | aws-us-cgw1 | - | 2 reachable | 4 reachable | 1 | 1 | 1 | --
GCP | us-west1 | GCP-npitaev | gcp-uswest-cgw1 | - | 2 reachable | 2 reachable | 1 | 1 | 1 | NA
WORKFLOWS
SETUP
Associate Cloud Account
Account Management
Cloud Global Settings
DISCOVER
Host Private Networks
MANAGE
Create Cloud Gateway
Gateway Management
INTENT MANAGEMENT
Cloud Connectivity
Audit
BRKENT-2060
59

Cloud Audit compares vManage and Cloud state

For Your Reference

Two types:

- On-demand
- Periodic – every 2 hours

Can be fixed on GCP with one click	Audit can NOT fix
• Deletion of the hub or the spokes • Deletion of Google cloud routers • Deletion of site-to-cloud peering of VPCs mapped to VPNs in vManage • Deletion of VPC peering of VPCs that are mapped to other VPCs in vManage • Missing custom routes • Missing BGP sessions • Stale BGP sessions	• Removal of a cloud gateway or any of its components • Issues with host VPCs with overlapping CIDRs • Issues with site-to-site VPCs • Issues with site-to-cloud VPCs • Issues with WAN VPCs

App Integration

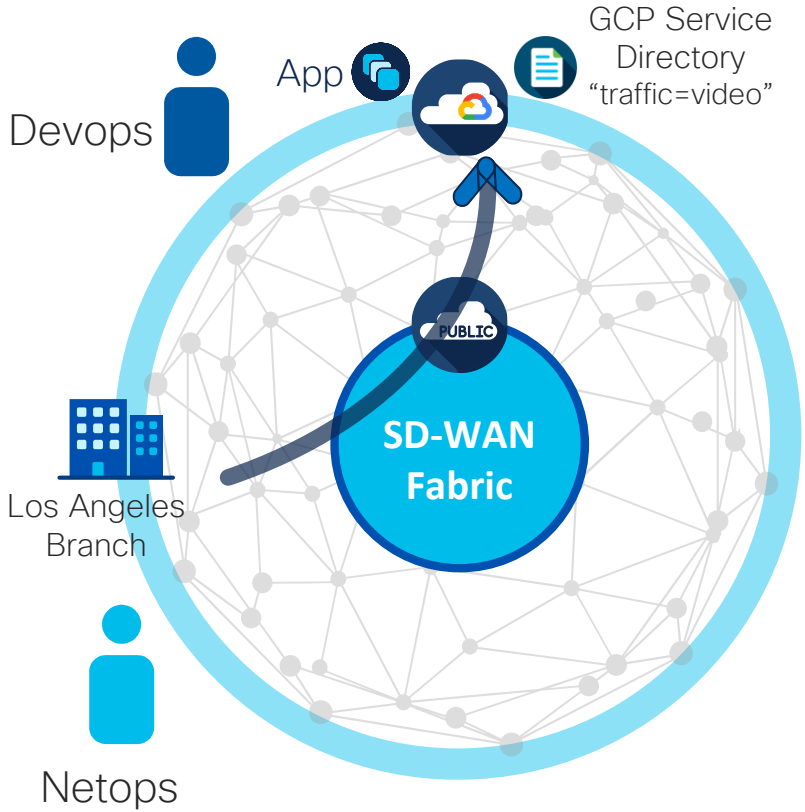
Creating a bridge between cloud apps and SD-WAN via Google Service Directory

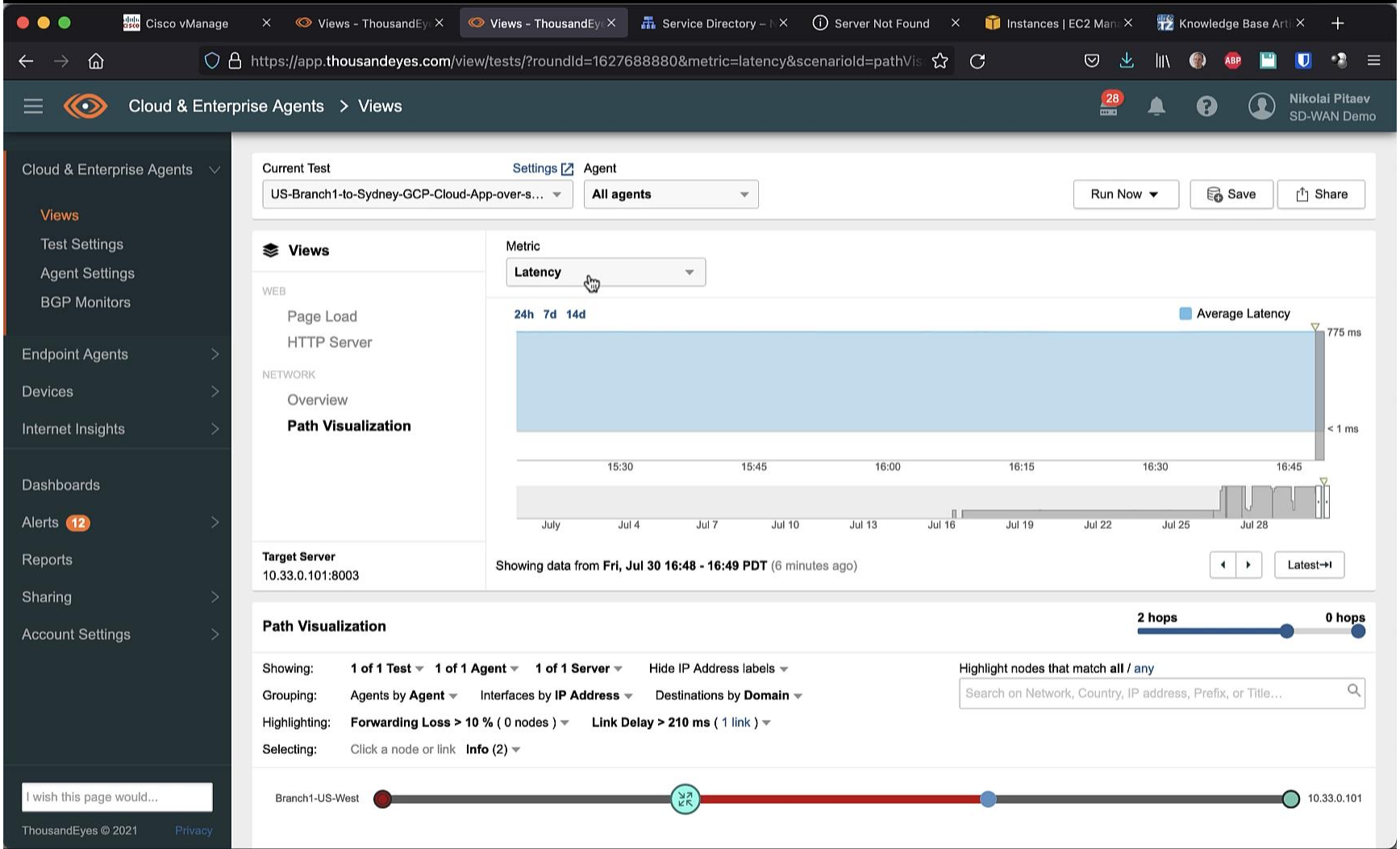
Use Case Summary

Devops register cloud-based apps at GCP Service Directory (write metadata “traffic”)

vManage detects cloud-based app automatically

Netops create SD-WAN policies and ensure required app experience in the network



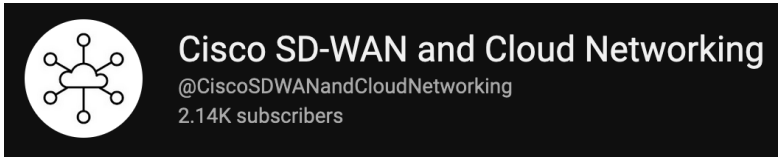

Cisco vManage
Views - ThousandEye
Views - ThousandEye
Service Directory – N
Server Not Found
Instances | EC2 Mana
Knowledge Base Arti
https://app.thousandeyes.com/view/tests/?roundId=1627688880&metric=latency&scenarioId=pathVis
Cloud & Enterprise Agents > Views
28
Nikolai Pitaev
SD-WAN Demo
Cloud & Enterprise Agents
Views
Test Settings
Agent Settings
BGP Monitors
Endpoint Agents
Devices
Internet Insights
Dashboards
Alerts 12
Reports
Sharing
Account Settings
I wish this page would...
ThousandEyes © 2021
Privacy
Current Test
Settings
Agent
US-Branch1-to-Sydney-GCP-Cloud-App-over-s...
All agents
Run Now
Save
Share
Views
WEB
Page Load
HTTP Server
NETWORK
Overview
Path Visualization
Metric
Latency
24h 7d 14d
Average Latency
775 ms
< 1 ms
15:30
15:45
16:00
16:15
16:30
16:45
July
Jul 4
Jul 7
Jul 10
Jul 13
Jul 16
Jul 19
Jul 22
Jul 25
Jul 28
Target Server
10.33.0.101:8003
Showing data from Fri, Jul 30 16:48 - 16:49 PDT (6 minutes ago)
Latest
Path Visualization
2 hops
0 hops
Showing: 1 of 1 Test 1 of 1 Agent 1 of 1 Server Hide IP Address labels
Grouping: Agents by Agent Interfaces by IP Address Destinations by Domain
Highlighting: Forwarding Loss > 10 % (0 nodes) Link Delay > 210 ms (1 link)
Selecting: Click a node or link Info (2)
Highlight nodes that match all / any
Search on Network, Country, IP address, Prefix, or Title...
Branch1-US-West
10.33.0.101

Summary

Call to Action

1. Learn

SD-WAN YouTube Channel



2. Test

- Cloud onRamp Sandbox: http://cs.co/CoR-Trial
- GitHub:

3. Use

SD-WAN Communities

Cisco Webex App

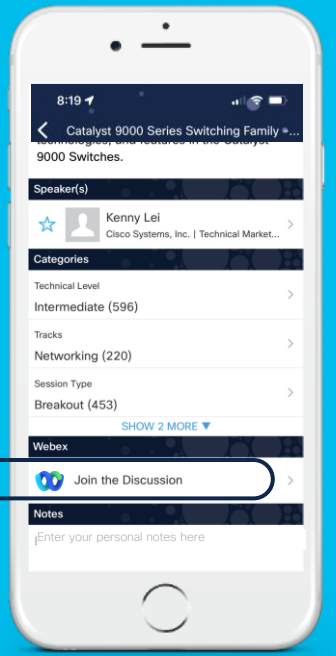
Questions?

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 until February 24, 2023.



Complete your Session Survey

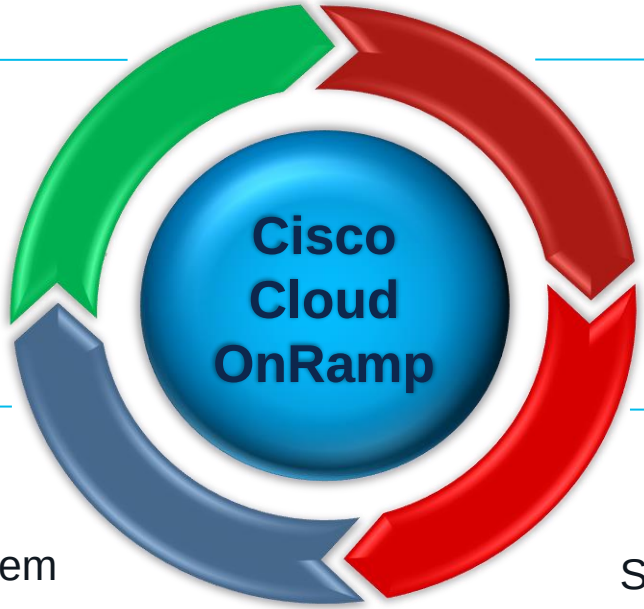
- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Cisco Cloud OnRamp solves your cloud problems

Automation

Site-to-Site, Site-to-Cloud, Cloud-to-Cloud



Operations

Cloud Audit, Monitoring, Predictions

Security

Cloud Security, SIG, On-Prem

App Performance

Service Directory Integration, Mid-Mile Optimization

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN