

CISCO *Live!*



#CiscoLive



The bridge to possible

Extending Enterprise Network into Public Cloud with Cisco Catalyst 8000V Edge Software

Jason Yang, Technical Marketing Engineer
CCIE#10467, AWS Certified Advanced Networking Specialty
BRKXAR-2003



#CiscoLive

Cisco Webex App

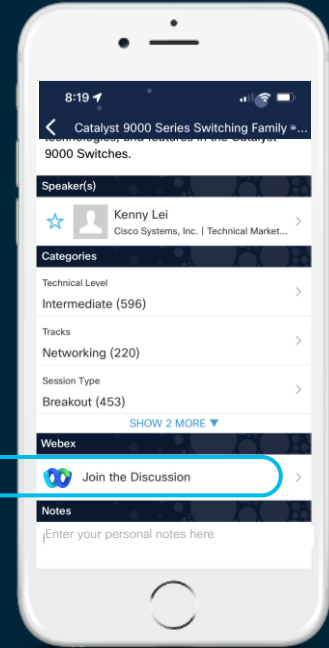
Questions?

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/#BRKXAR-2003>



Agenda

- Platform Overview
- Software Architecture
- Catalyst 8000V Edge in Public Cloud use cases
- Conclusion

Introducing Cisco Catalyst 8000V Edge Software



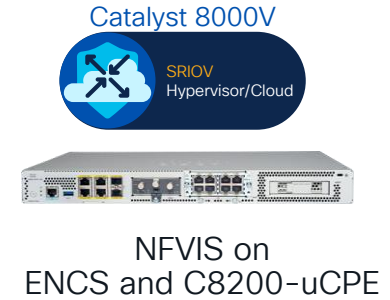
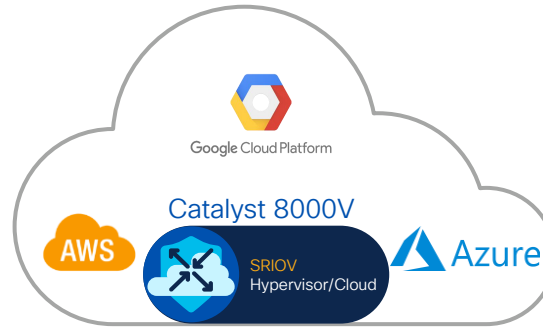
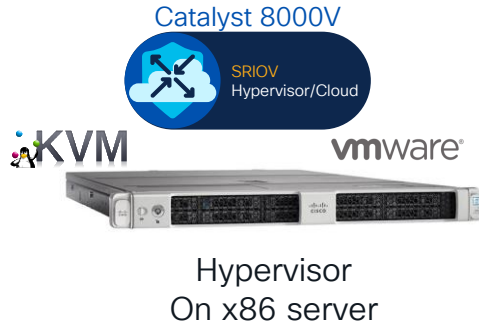
Cisco Catalyst 8000V Edge Software

Pervasive WAN
Deployment

Seamless SD-WAN
Extension in cloud

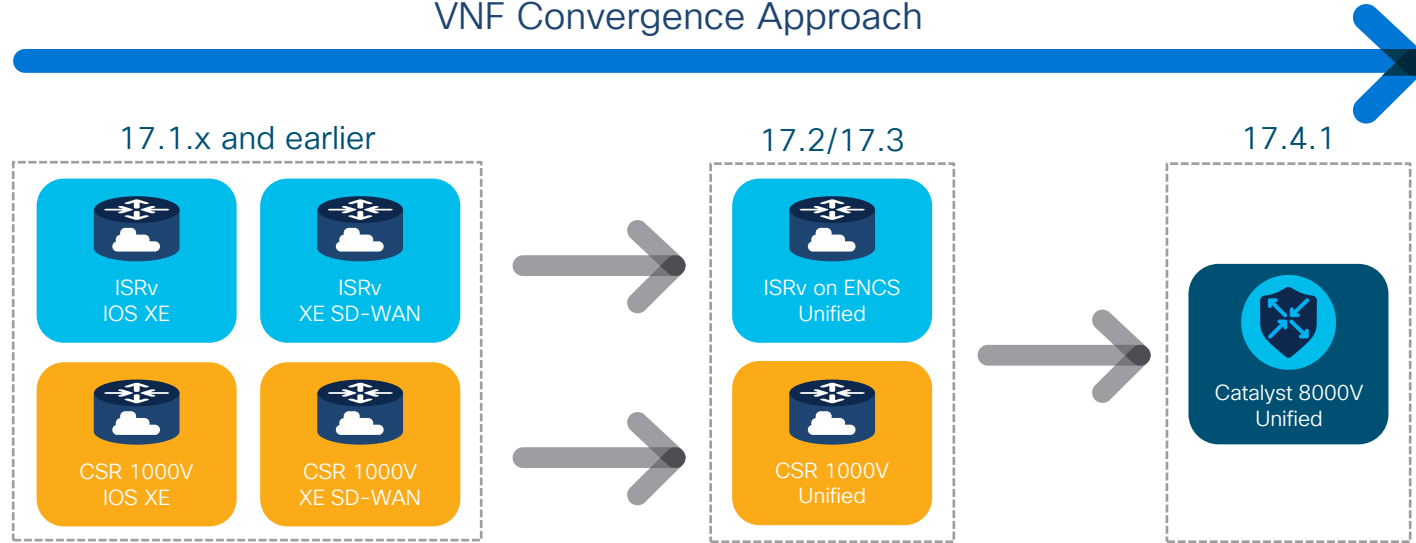
Infrastructure
Agnostic

Service Richness



Virtual Router Convergence

VNF Convergence Approach



CSR to Cat8KV upgrade in Autonomous Mode and Controller Mode:

<https://www.youtube.com/watch?v=plMIXFXdwww>

<https://www.youtube.com/watch?v=S1sRVQLkJhM>

Available in all major cloud marketplaces



C5n class, C5 class, T3.medium



F32s_v2, F16s_v2,
DS4_v2, DS3_v2, DS2_v2



Google Cloud Platform

N1-standard-8, 4, 2

Catalyst 8000V supports more than 20 different instance profiles across the three clouds

Effortlessly deploy on x86 hypervisors



Enterprise Linux 7.5
Enterprise Linux 7.7
Enterprise Linux 8.4



ESXi 6.5 Update 2
ESXi 6.7 Update 3
ESXi 7.0



Openstack TRAIN
RHEL 8.2
CVIM 3.4



NFVIS on
C8200-uCPE
ENC5 5000
CSP 5000

Elastic resource allocation



Physical Hardware:

- CPU - Intel or AMD
- CPU with clock frequency ≥ 2.0
- TenGigabit and Gigabit Ethernet interfaces

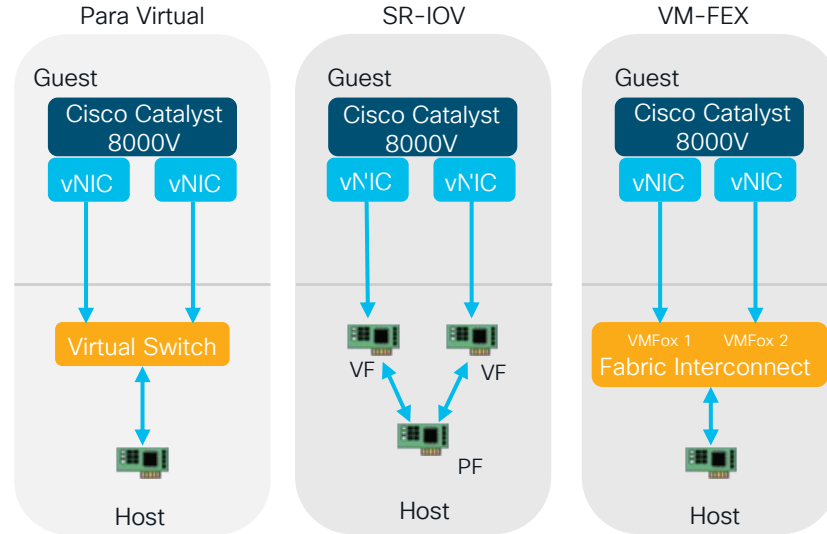


Catalyst 8000V Virtual Machine specs:

- CPU: 1 to 16 virtual CPUs
- Memory: 4 GB to 16 GB
- Disk space: 8 GB or 16GB
- Virtual Network Interface Cards (vNICs):
 - ESXI - A maximum of 8 vNICs is supported; VMXNET3, ixgbevf, and i40evf
 - KVM - A maximum of 26 vNICs is supported; Virtio, ixgbevf, and i40evf

Extended I/O support

- Paravirtual
- Single-root I/O virtualization (SR-IOV)
 - Accelerated Networking 
 - Enhanced Networking 
- Cisco Virtual Machine Fabric Extender (VM-FEX)
- DPDK support using poll-mode drivers



Tips of the day - #1

know my vnic driver



Tip!

```
C8KV-AWS#show platform software vnic interface-mapping
```

```
-----  
Interface Name      Driver Name      Mac Addr  
-----  
GigabitEthernet1   net_ena         061d.029b.c9a4  
-----
```

```
C8KV-Azure#show platform software vnic interface-mapping
```

```
-----  
Interface Name      Driver Name      Mac Addr  
-----  
GigabitEthernet1   mlx4_en         000d.3a5b.2760  
GigabitEthernet2   mlx5_core       000d.3a5b.eea3  
-----
```

Enhanced software security

Secure Object Store

- Storage partitions for NVRAM, licensing and other data are now created as Object stores
- Individual Object stores are encrypted to ensure data security
- Cisco Secure Development lifecycle (CSDL) compliant
- 16G disk cycle profile support

8G Disk Layout

EFI/GRUB (1MB)

boot (2GB)

objstore (1GB)

bootflash (rest)

16G Disk Layout

EFI/GRUB (1MB)

boot (4GB)

objstore (1GB)

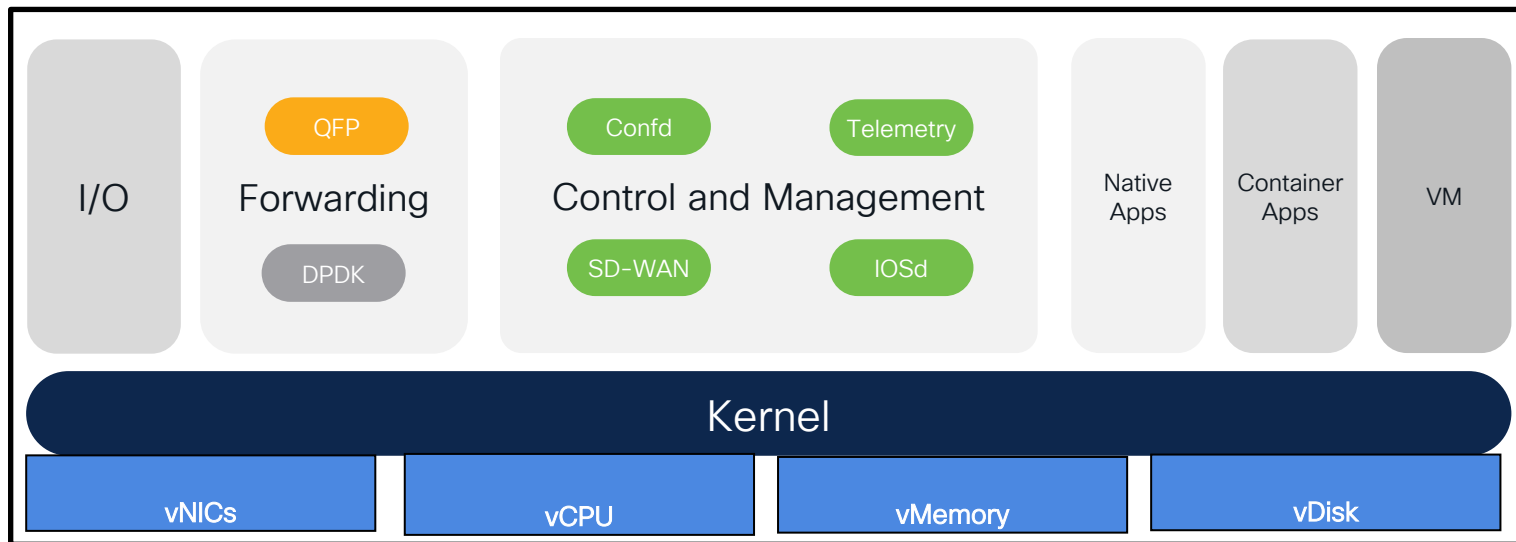
bootflash (rest)

Catalyst 8000V Edge Software Architecture

Virtualized IOS XE in Virtual Machine



Open and Extensible
IOS XE



TCO Savings

Automation

Continuous Innovation

Catalyst 8000V IOS XE Threads to vCPU Associations

- IOS XE processing threads in the Guest OS are statically mapped to vCPUs threads
- vCPU threads in turn are allocated to physical cores by the hypervisor scheduler
- PPE : Packet Processing Engine
- HQF: Hierarchical Queuing Framework

Catalyst 8000V footprint	Control Plane	Data Plane PPE	Data Plane HQF	Data Plane Rx processing
1	vCPU 0			
2	vCPU 0	vCPU 1		
4	vCPU 0	vCPU 1 & 2	vCPU 3	
8	vCPU 0	vCPU 1-5	vCPU 6	vCPU 7

NOTE: vCPU allocations subject to change without further notice

Tips of the day - #2

know my CPU alloc and usage



Tip!

```
C8KV#show platform software cpu alloc
```

```
CPU alloc information:
```

```
Control plane cpu alloc: 0-1
```

```
Data plane cpu alloc: 2-17
```

```
Service plane cpu alloc: 0-1
```

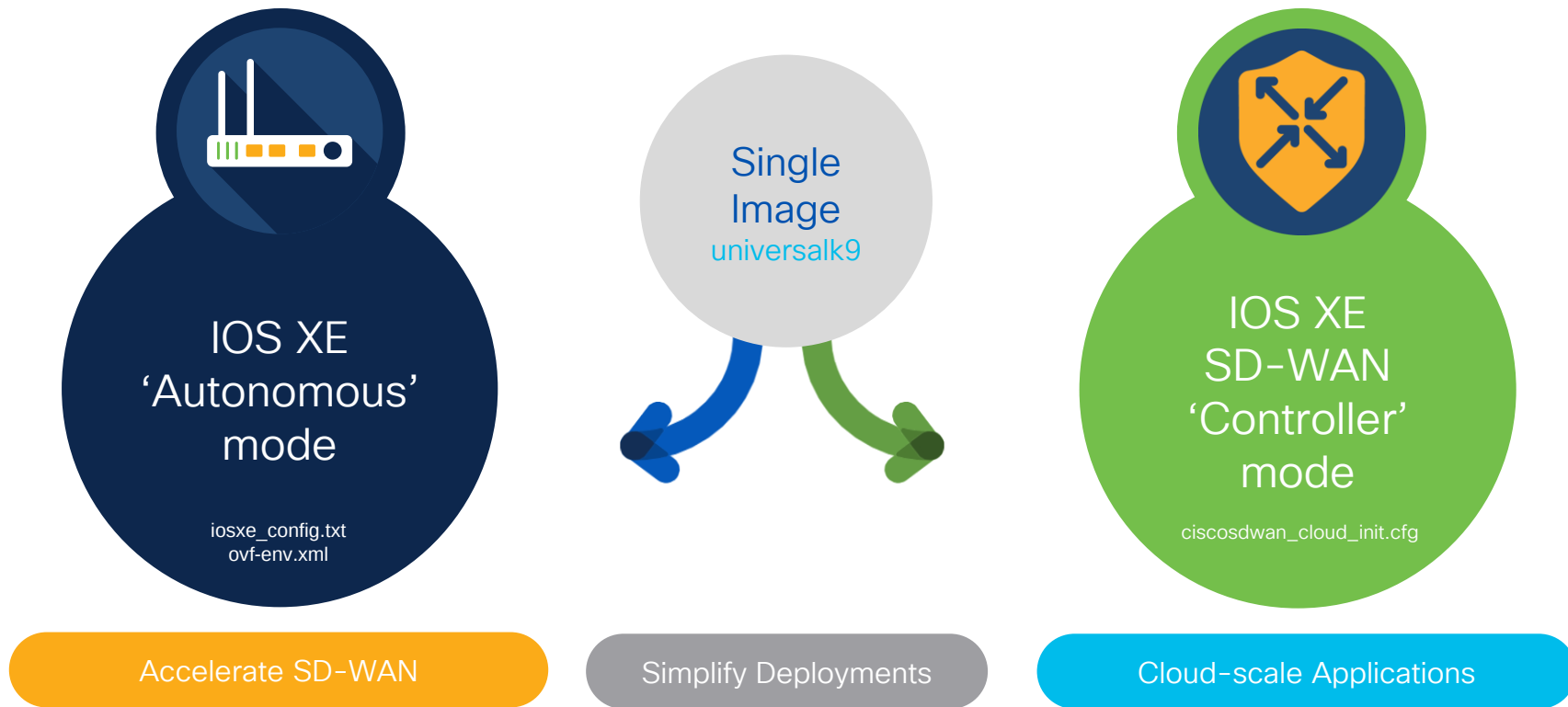
```
C8KV#show platform hardware qfp active datapath infrastructure sw-cio
```

```
<snipped>
```

```
Core Utilization over preceding 13.7132 seconds
```

```
-----  
ID:      0      1      2      3      4      5      6      7      8      9     10     11     12     13     14     15  
% PP: 85.80 85.74 85.91 85.72 85.75 85.65 85.81 85.72 85.76 85.69 85.78 85.79 85.69 85.62 0.00 0.00  
% RX: 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 18.01  
% TM: 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00 48.10 0.00  
% IDLE: 14.20 14.26 14.09 14.28 14.25 14.35 14.19 14.28 14.24 14.31 14.22 14.21 14.31 14.38 51.90 81.99
```

Easy Operations with Single Image



Cisco Catalyst 8000V Edge Software

Features & Technology



Routing & Multicast

SD-WAN routing (OMP)
IPv4/v6 routing protocols,
Multicast routing
PIM-SM/MLD
Policy-based routing (PBR)
First-Hop redundancy



Adv Security

SVTI	FW App Aware
IPsecGRE	Umbrella SIG
DMVPN	UTD
FlexVPN	Trustsec



Application Services

NAT	NBARv2
SD-Access	AppQoE
HQoS	TE



Cloud Connectivity

SD-WAN	Autonomous
Integration:	Mode:
• AWS TGW	HA Solution
• Azure vWAN	TGW



Automation

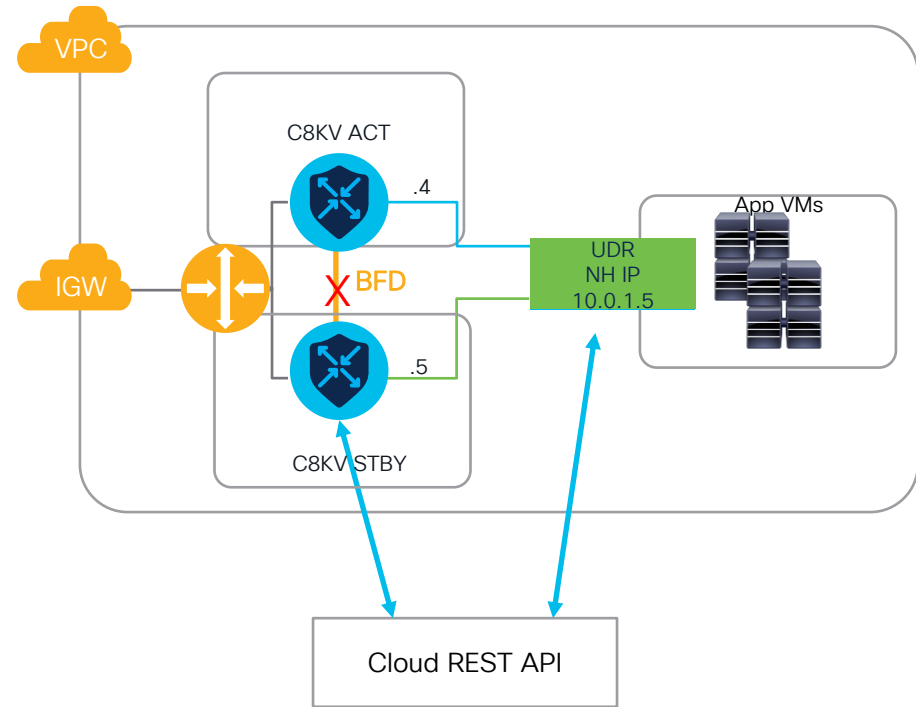
CloudFormation
Azure Resource Manager
Terraform
Netconf
Restconf

Catalyst 8000V in Public Cloud use cases

Catalyst 8000V High Availability on Cloud

AWS/Azure/GCP

- No virtual IP as with HSRP, since Cloud Provider doesn't allow multicast or broadcast.
- Deploy a pair of C8KV, one of them serve as the NH for the route table
- BFD and EIGRP over IPsec tunnel is enabled between two Catalyst 8000V to detect failure
- Upon failure detection of C8KV Active, C8KV STBY calls Cloud Provider's REST API to update RT's NH to it's own



Before HA Failover / After HA Failover

Tips of the day - #4

4 simple steps to deploy HA



Tip!

```
Step1[guestshell@guestshell ~]$ pip3 install csr_azure_ha --user
```

```
Step2(config)#interface Tunnel11
Step2(config-if)#ip address 192.168.101.1 255.255.255.252
Step2(config-if)#load-interval 30
Step2(config-if)#bfd interval 100 min_rx 100 multiplier 3
Step2(config-if)#tunnel source GigabitEthernet1
Step2(config-if)#tunnel mode ipsec ipv4
Step2(config-if)#tunnel destination a.b.d.c
Step2(config-if)#tunnel protection ipsec profile vti-1
Step2(config)#router eigrp 1
Step2(config-router)#bfd all-interfaces
Step2(config-router)#network 192.168.101.0 0.0.0.255
```

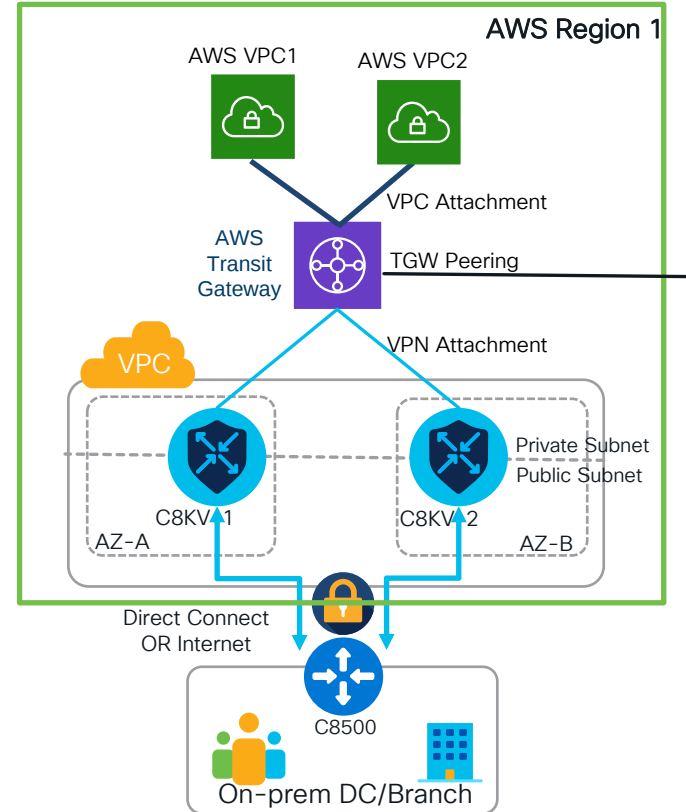
```
Step3[guestshell@guestshell ~]$ create_node.py -i 100 -p azure -s <subscriptionId> -g test -t haprivate-rt -n 10.0.1.4 -m primary
```

```
Step4 Authorize C8KV to update route-table in cloud
```

<https://youtu.be/nX0qYw7NTkk>

AWS TGW Integration

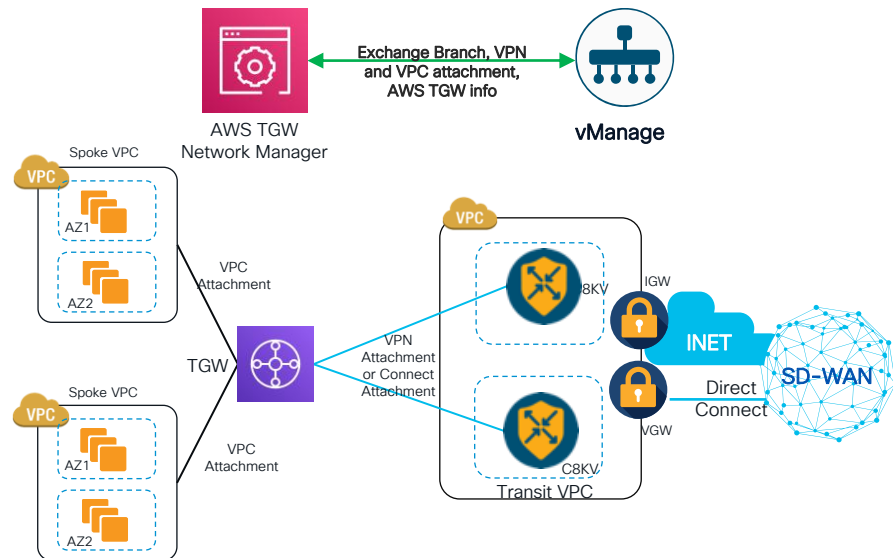
- Dedicated VPC: Simplifies routing by not combining with other shared services.
- Catalyst 8000V provides
 1. Flexibility and operation consistency to extend existing VPN (DMVPN, FlexVPN) to cloud
 2. Sophisticated routing and path selection between on-prem and cloud
 3. App aware visibility for cloud connection
 4. Rich services such as ZBFW and NAT
 5. Pair deployment for HA, active/active via BGP
 6. Scale out C8KV as throughput demand increase



SD-WAN Cloud onRamp for MultiCloud

AWS TGW Integration

- Automated provisioning of SD-WAN Transit VPC and TGW, route exchange for site to cloud and site to site traffic over AWS backbone
- Full Visibility into inter-regional transit traffic and telemetry with TGW Network Manager
- Consistent Policy and Segmentation across branch and cloud for enterprise class security
- Cloud onRamp saves much **time** and **cost** for building cloud connectivity!



Extend SD-WAN

Policy Framework

Unified Control

Cost Effective

Tips of the day - #5

Use Multiple Tunnels to get the most C8KV perf out of AWS instance



Tip!

- AWS instance has multiple PMD Transmit queues per interface
- For example, c5n.9xlarge has 8 Tx queues per interface
- Starting in IOS XE 17.7 C8KV is able to use all Tx queues in both SD-WAN mode and autonomous mode
- Traffic are hashed into Tx queues by using src/dst ip addresses, in case of tunnels it will be tunnel outer IP header address.
- Using Multi-TxQ in 17.7 C8KV throughput can be improved up to 2x

```
C8KV-sdwan-17.7#show platform hardware qfp active datapath
infrastructure sw-nic | i device Gi|pri-
pmd c19a3a40 device Gi1
pri-0: pkts 439223021 bytes 182817201772
pri-1: pkts 540702720 bytes 225244450017
pri-2: pkts 858886231 bytes 661651513881
pri-3: pkts 715066061 bytes 295970608574
pri-4: pkts 470350055 bytes 195911570347
pri-5: pkts 480646564 bytes 200203566739
pri-6: pkts 127095049 bytes 52820914792
pri-7: pkts 527331897 bytes 219311748149
```

Create 8 IPsec tunnels by using loopback intf

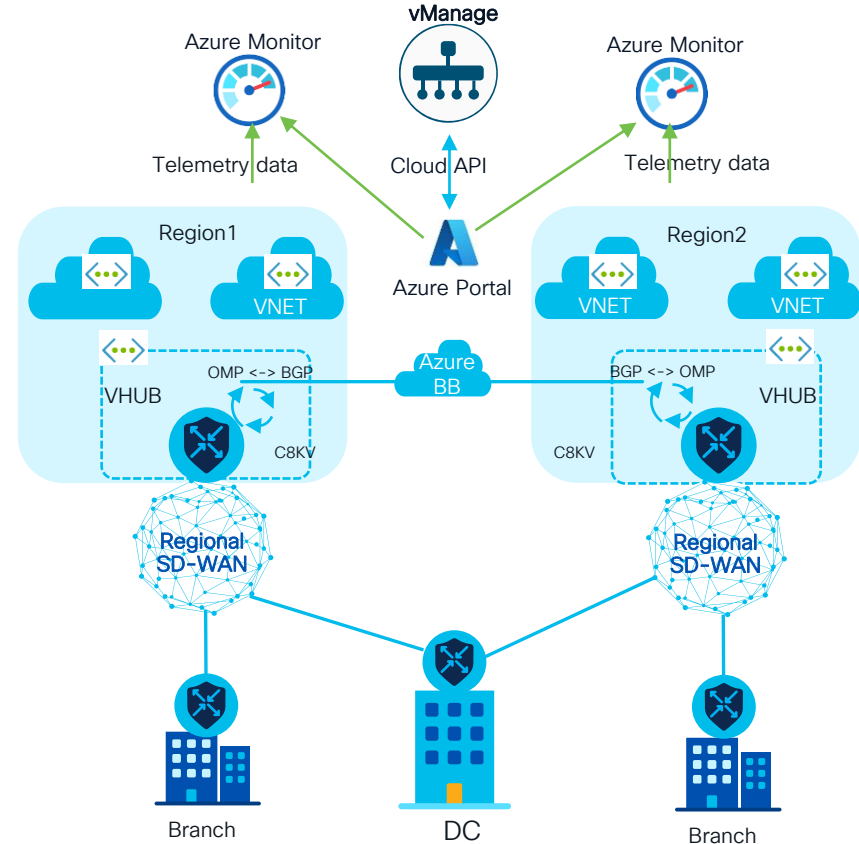
```
C8KV#
interface Loopback1
 ip address 192.168.1.21 255.255.255.255
interface Loopback2
 ip address 192.168.1.129 255.255.255.255
interface Loopback3
 ip address 192.168.1.20 255.255.255.255
interface Loopback4
 ip address 192.168.1.128 255.255.255.255
interface Loopback5
 ip address 192.168.1.23 255.255.255.255
interface Loopback6
 ip address 192.168.1.131 255.255.255.255
interface Loopback7
 ip address 192.168.1.22 255.255.255.255
interface Loopback8
 ip address 192.168.1.130 255.255.255.255
```

```
PEER#
interface Loopback1
 ip address 192.168.2.21 255.255.255.255
interface Loopback2
 ip address 192.168.2.129 255.255.255.255
interface Loopback3
 ip address 192.168.2.20 255.255.255.255
interface Loopback4
 ip address 192.168.2.128 255.255.255.255
interface Loopback5
 ip address 192.168.2.23 255.255.255.255
interface Loopback6
 ip address 192.168.2.131 255.255.255.255
interface Loopback7
 ip address 192.168.2.22 255.255.255.255
interface Loopback8
 ip address 192.168.2.130 255.255.255.255
```

SD-WAN Cloud onRamp for MultiCloud

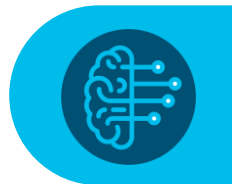
Native integration with Azure Virtual WAN

- Automated provisioning of Azure VWAN and VHUB infra
- Instantiate Cloud GW in VHUBs and extend SD-WAN fabric into the cloud via Internet and ExpressRoute
- Intent Management workflow enables connectivity between SD-WAN VPNs and VNets.
- Integrate with Azure Firewall
- Support 3 types of instances, deploy a pair of each:
 - D2_v2, D3_v2, D4_v2
- SKU scale up to 5Gbps



Key Takeaways

C8KV is the foundation for Secure Cloud networking



Fully Automated Deployment

- vManage Cloud onramp orchestration
- Cloudformation, ARM, terraform templates support
- Programmability NETCONF/RESTCONF



Ready for the Multicloud Journey

- Multi-cloud SD-WAN deployment
- TGW and Azure vWAN Integration
- HA and TGW solution



Agile and Elastic deployment

- Supports a large variety of cloud instance types
- Increase CPU and memory on demand
- Optimized IPsec performance in Cloud

Other Catalyst 8000V related sessions

- BRKENT-2060 Cisco SD-WAN Cloud OnRamp for Multicloud
- LABCLD-1615 AWS deployment of Catalyst 8000v

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

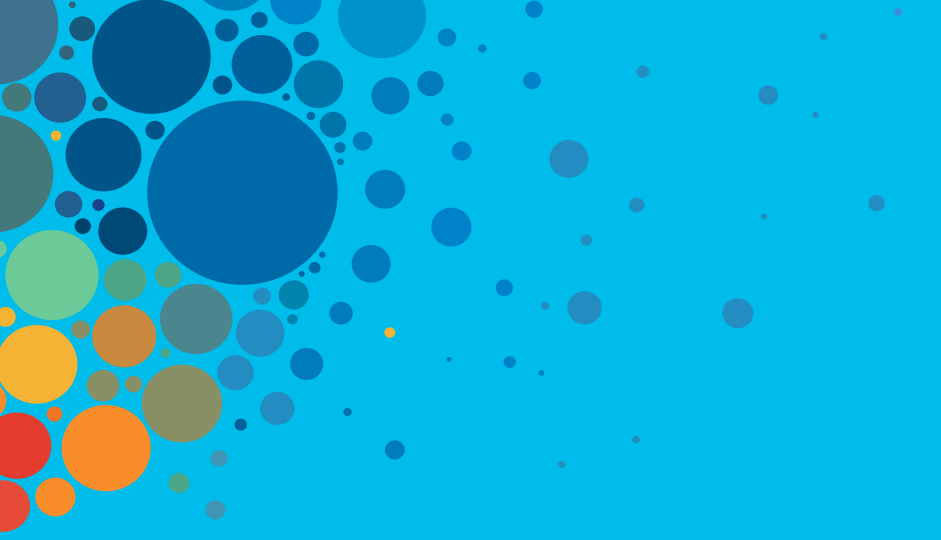
Cisco Guided Study Groups

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