The bridge to possible

Nexus Hybrid Cloud : Connecting On-Prem VXLAN Fabric to Public Cloud

Ambrish Singh, Technical Marketing Engineer
Cloud Networking Group

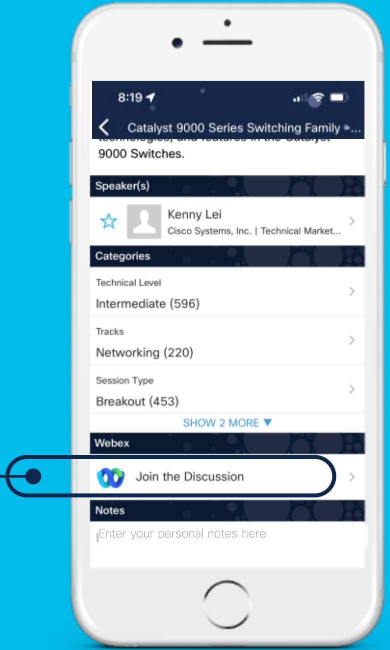
Cisco Webex App

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



8:19

Catalyst 9000 Series Switching Family ▪...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Webex spaces will be moderated until February 24, 2023.

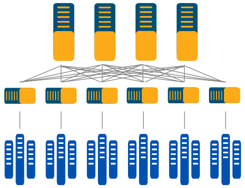
Agenda

- Introduction
- Challenges with Hybrid Cloud networking
- What’s Cisco Hybrid Cloud Solution
- Supported Topologies
- Demo

Introduction

What is Hybrid Cloud

Hybrid clouds are infrastructure combinations of two or more clouds, such as on-premises private, hosted private, or public, that can be centrally managed to enable interoperability for various use cases.



aws

Azure

Introduction

- Private Cloud – On-prem Data Center
- Public Cloud – AWS, Azure, GCP
- Hybrid Cloud – Private Cloud + Public Cloud
- Hybrid Multi Cloud - Private Cloud + 2 or more Public Clouds
- Multi Cloud – Public Cloud + Public Cloud

Hybrid Multicloud Networking – The requirements

Connectivity

Connecting applications across on-premises, public clouds and edge networks

Zero Trust and security

Maintaining a consistent security posture that is agnostic to where app and clients are located

Visibility

Observing and analyzing connectivity, traces, logs, and metrics across heterogeneous networks

Application networking

Enabling application intent to dynamically drive network behavior

Challenges with Hybrid Cloud Networking

Network Admin Challenges

- Heterogenous networks
- Multiple configuration touchpoints
- Human effort prone to errors
- No centralized control
- No consistent policy model

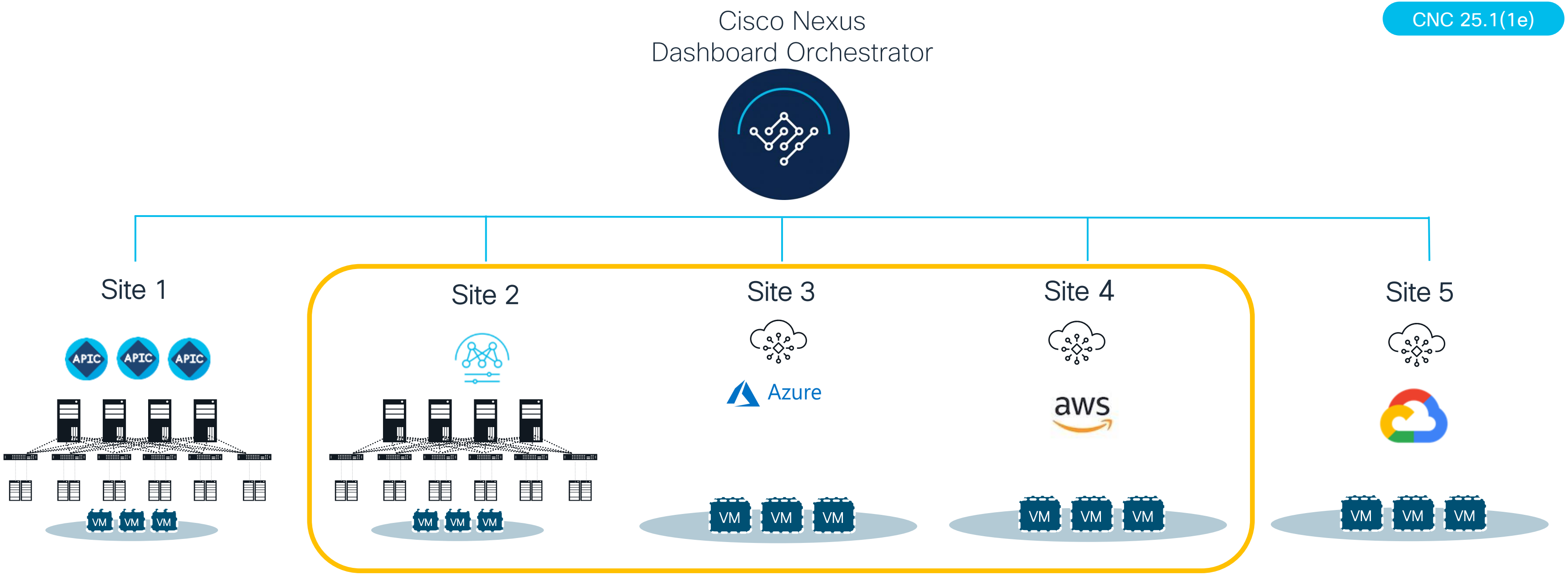
Network Admin Challenges

NX-OS	ACI	aws		
Separate Infrastructure + VXLAN	Tenant	Account	Subscription/ Resource Group	Account/Project
Data Center	Site/Pod	Region	Region	Region
VRF	VRF	VPC	VNet	VPC
VLAN	Bridge Domain/ Subnet	CIDR/Subnet	Subnet	Subnet
VLAN Tag	EPG	Security Groups	Application/Network Security Groups	Firewall
Access-list (ACL)	Contracts & Filters	Security Group Rules	Security Rules	Firewall Rules

What’s Cisco Hybrid Cloud Solution

Building Hybrid Multicloud

NDO 4.1(1)
NDFC 12.1.2e
CNC 25.1(1e)



- Consistent Network and Policy
- Secure Communication
- Single Point of Orchestration
- Automated Connectivity
- Cloud Only (Multi-Cloud)

Hybrid Cloud : Building Blocks

Catalyst 8000v

Cisco Cloud Network Controller

Nexus Dashboard

Catalyst 8000v

- IOS-XE based Cloud Native Router
- SAAS offering (ISO, BIN, OVA, and QCOW2 formats)
- Available on CCO and Cloud Marketplace (PAYG or BYOL)
- Up to 10 Gbps of Throughput per instance
- VM requirement –
  - CPU – 1 to 8 virtual CPUs
  - Memory – 4 GB to 16 GB
  - Disk space – 8 GB
  - Two or more vNICs, up to maximum allowed by hypervisor

https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8000v-edge-software/datasheet-c78-744101.html

Reference slide

Catalyst 8000v Feature Overview

- IPsec, DMVPN, Flex VPN, GetVPN
- BGP, OSPF, EIGRP
- VXLAN Gateway, VXLAN Multicast & Unicast
- ACL, AAA,
- GRE, QoS, IP SLA
- NAT, LISP, OTV
- DHCP, HSRP

Cisco Cloud Network Controller (CNC)

- Provides the ability to connect and consume public clouds, accelerating business agility to support hybrid or multicloud environments.
- Utilizes cloud-native constructs, the solution enables automation that accelerates infrastructure deployment and governance and simplifies management to easily connect workloads across multicloud environments.

Cisco Cloud Network Controller (CNC)

- Manage multiple regions through a single Cloud Network Controller instance
- Provide secure interconnect for multi cloud environment and automate network connectivity across multiple On Premises and Public Cloud environments
- Enable Consistent Policy, Security and Operations between On-Premises and Public Cloud environments

Reference slide

Cisco Cloud Network Controller feature overview

Cloud networking

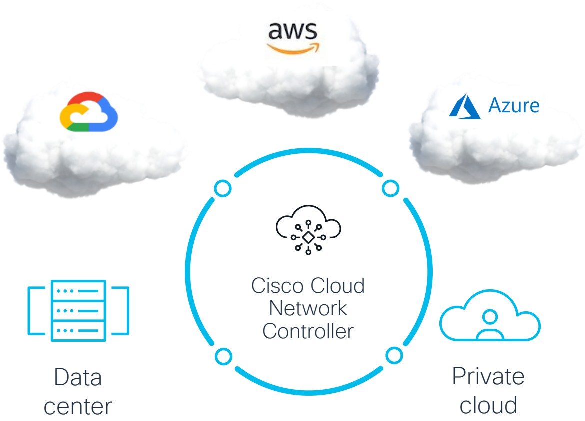
- Intra-Cloud: TGW, VNET peering
- Inter-Cloud: C8Kv automation
- Connectivity: IPsec, direct connect, express route

Visibility

- View and connect to brownfield VPC networks
- Inventory and topology view

L4-L7 services

- Automate service insertion and service chaining (load balancers, firewalls, …)



Segmentation

- Extend segments from on-premises to cloud
- Extend segments from cloud to cloud
- Security group rule management

Support on Public

- AWS, Azure, Google Cloud

Open APIs

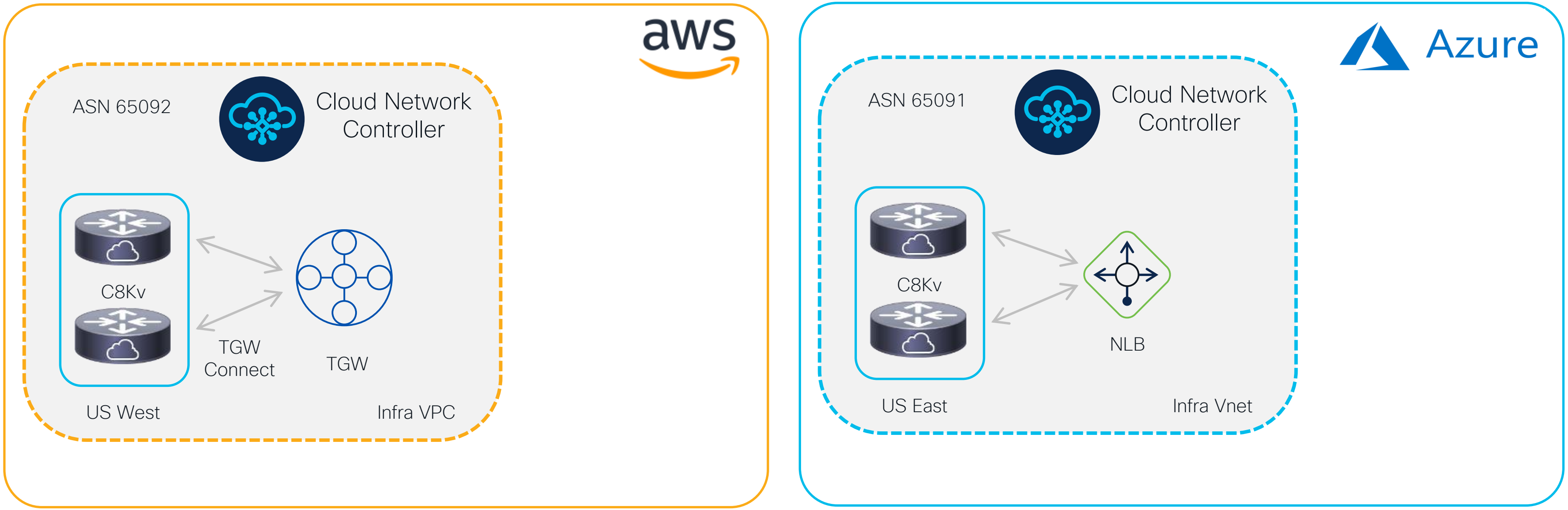
- Enable automation using Terraform and Ansible

Cloud Network Controller

Public cloud policy mappings

Cloud Network Controller	AWS	Azure	GCP
Tenant	Account	Subscription	Project
VRF	VPC	Virtual Network	VPC
Bridge Domain Subnet	Subnet	Subnet	Subnet
EPG	Security Group	App Security Group	Firewall
Contracts, Filters	Security Group Rule	Network Security Group	Firewall Rule
Consumed Contracts	Inbound Rule	Inbound Rule	Inbound Rule
Provided Contracts	Outbound Rule	Outbound Rule	Outbound Rule

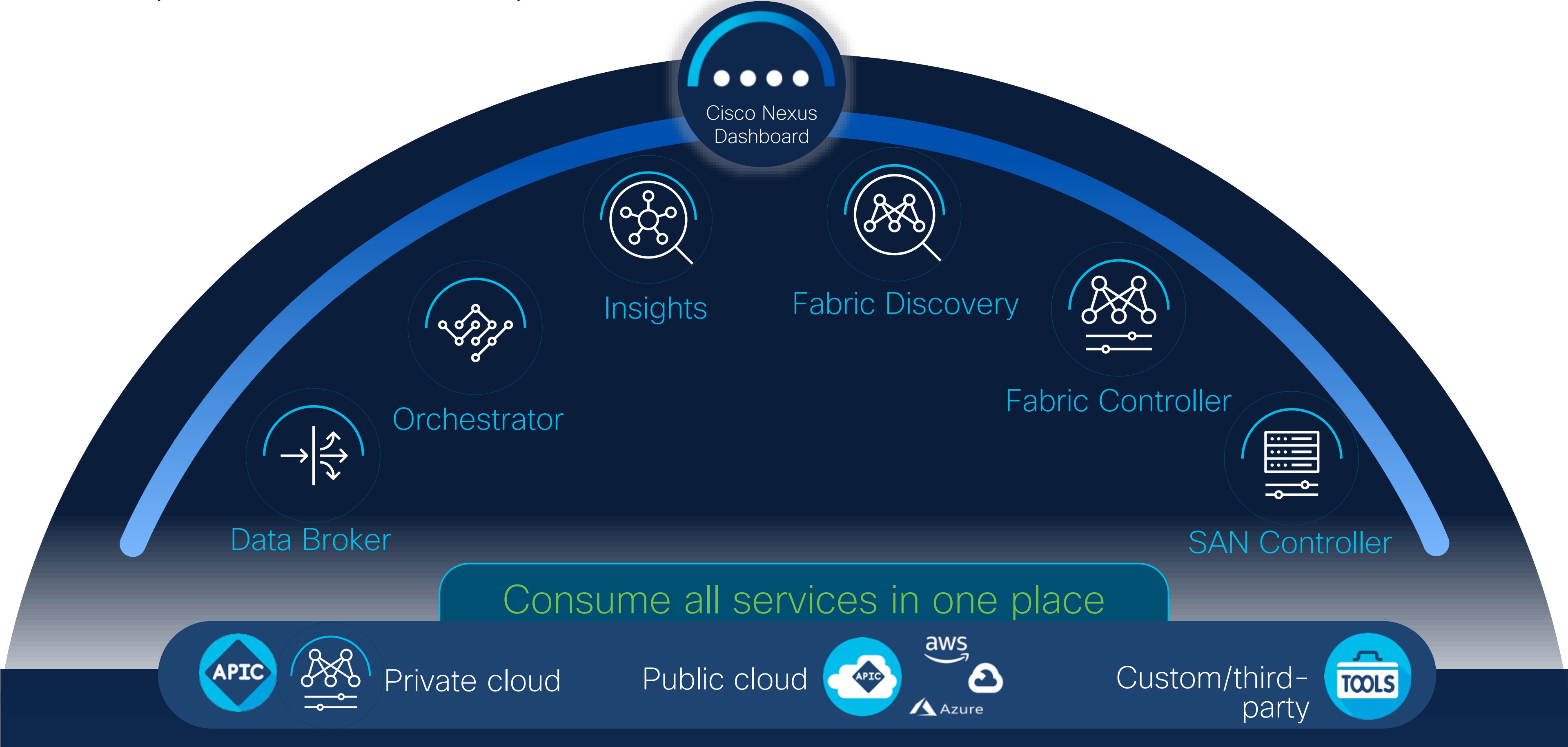
Cisco Cloud Network Controller



Cisco Nexus Dashboard

Simple to automate, simple to consume

Powering automation
Unified agile platform



Nexus Dashboard Fabric Controller

A comprehensive data center automation tool

NDFC helps you easily and reliably deploy, operate and maintain
VXLAN-EVPN, LAN, SAN, and Media fabrics
for Cisco NX-OS Nexus and MDS, IOS-XE, IOS-XR infrastructure
and interconnect with public clouds

Day-0
Bootstrap, deploy

Day-1
Provision, maintain, monitor, operate

Day-2 with ND Insights
Troubleshoot, plan, grow

Scale out with ND Orchestrator
Multi-site and cloud acceleration

It addresses challenges by providing comprehensive solution-level control, automation, visibility, monitoring, and integration

Nexus Dashboard Fabric Controller

Automation

Accelerate provisioning
and simplify deployments

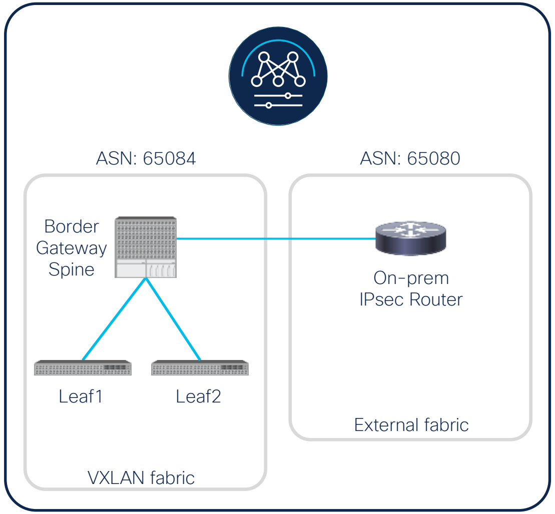
Management

In depth Management
and control for all
network deployments

Visibility

Get Centralized Visibility
and Monitoring views

Nexus Dashboard Fabric Controller



- Manages On-prem VXLAN fabric
- Built-in templates for building on-prem VXLAN fabric
- VXLAN fabric must have one or more Border Gateways (BGW)
- External fabric for Managed or Unmanaged IPsec devices
- IPsec device should be in Core Router role

Nexus Dashboard Orchestrator

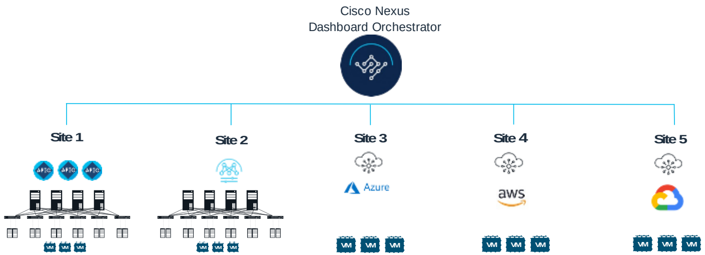
Multi-site Orchestrator

NDO offers multi-site networking orchestration and policy management, disaster recovery and high availability, as well as provisioning and health monitoring.

- Multi-site Network Orchestration
- Multicloud Orchestration
- Consistent Policy Management
- Disaster Recovery and Agility

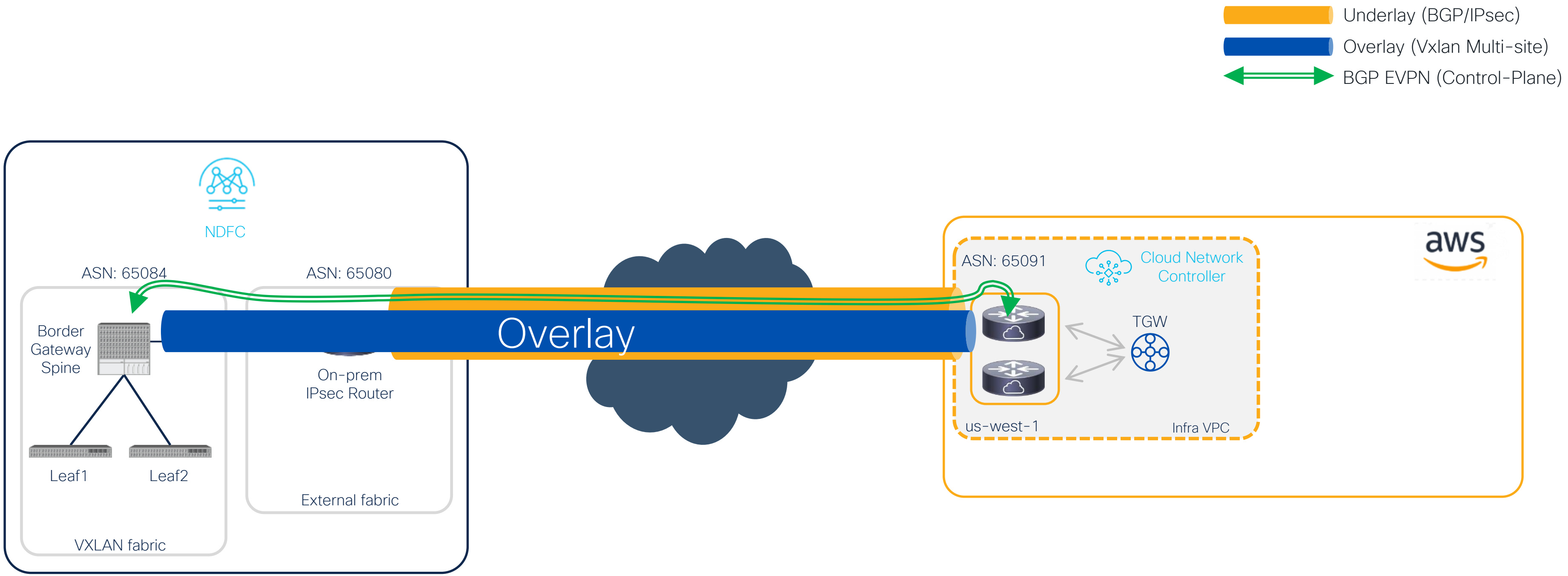
Private Cloud, Hybrid Cloud, Multiple Cloud Data Centers

Nexus Dashboard Orchestrator



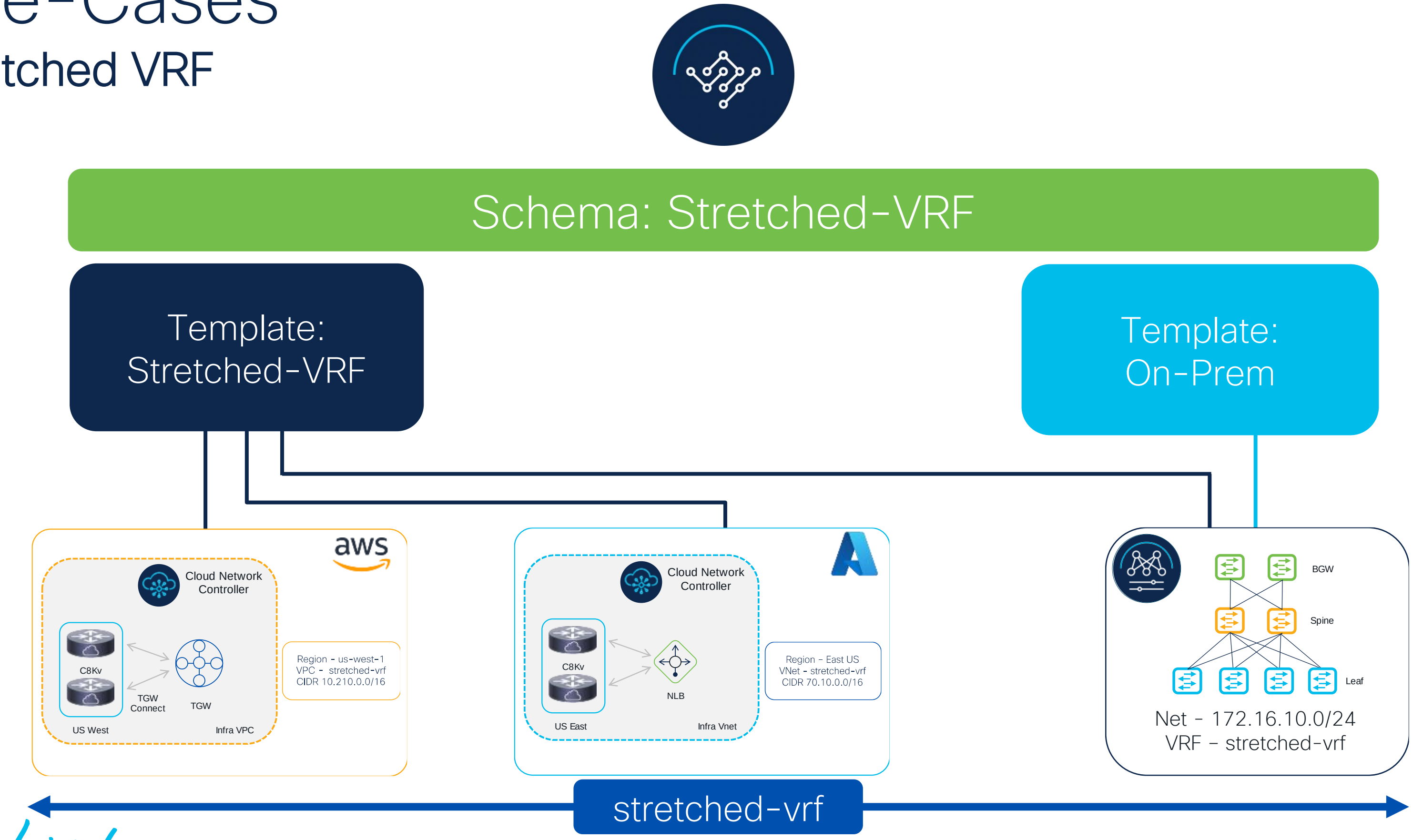
- Single point of control
- Orchestrating end-to-end connectivity between –
  - On-premises to Cloud sites
  - Cloud to Cloud
- Centralized deployment of –
  - VRFs/Networks in on-prem VXLAN fabric
  - VPCs/VNets in Cloud sites

Hybrid Cloud : Under the Hood



Use-Cases

Stretched VRF



Schema: Stretched-VRF

Template: Stretched-VRF

Template: On-Prem

Cloud Network Controller

C8Kv

TGW Connect

TGW

US West

Infra VPC

Region - us-west-1
VPC - stretched-vrf
CIDR 10.210.0.0/16

Cloud Network Controller

C8Kv

NLB

US East

Infra Vnet

Region - East US
VNet - stretched-vrf
CIDR 70.10.0.0/16

BGW

Spine

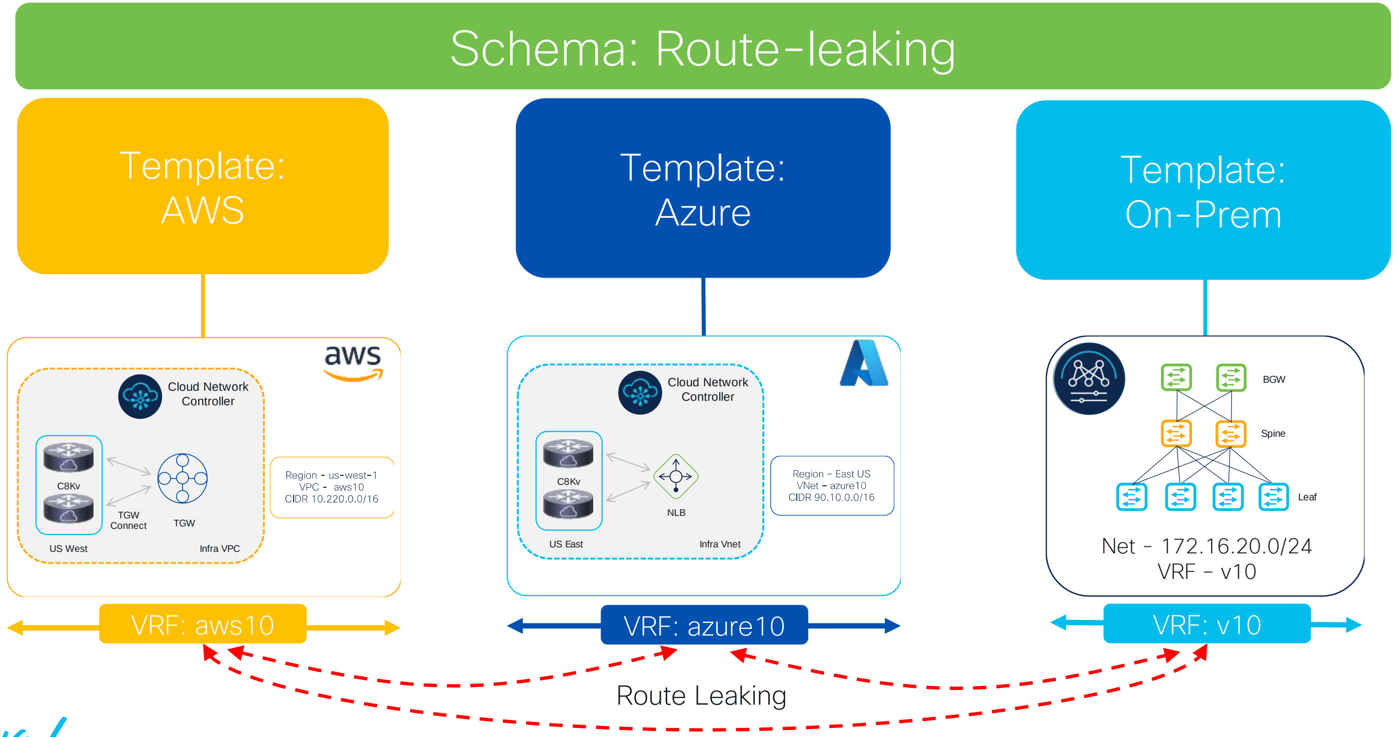
Leaf

Net - 172.16.10.0/24
VRF – stretched-vrf

stretched-vrf

Use-Cases

VRF Route Leaking



Schema: Route-leaking

Template: AWS

Template: Azure

Template: On-Prem

Region - us-west-1
VPC - aws10
CIDR 10.220.0.0/16

Region – East US
VNet – azure10
CIDR 90.10.0.0/16

Net – 172.16.20.0/24
VRF – v10

VRF: aws10

VRF: azure10

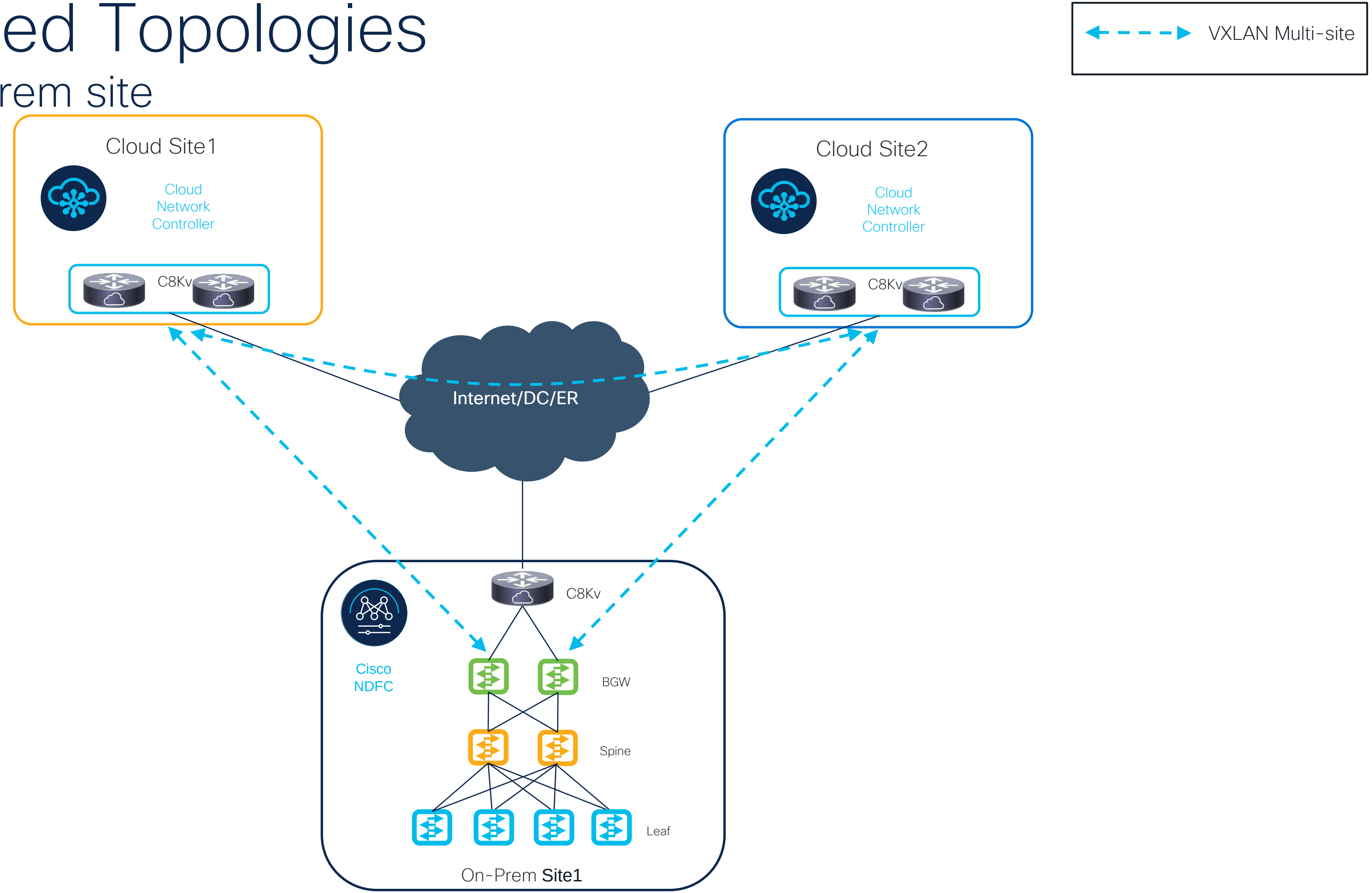
VRF: v10

Route Leaking

Supported Topologies

Supported Topologies

Single On-prem site

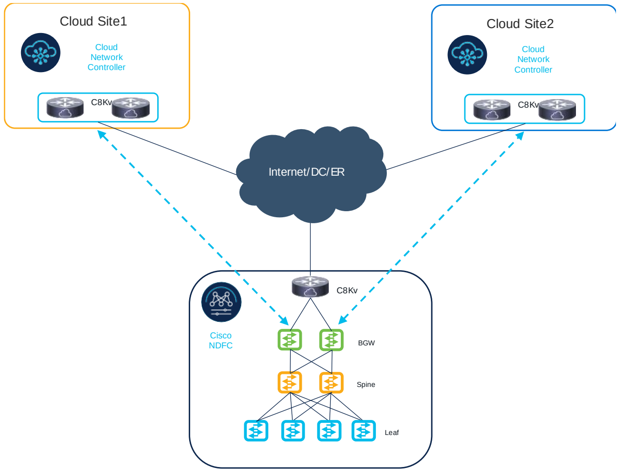


Supported Topologies

Single On-prem site

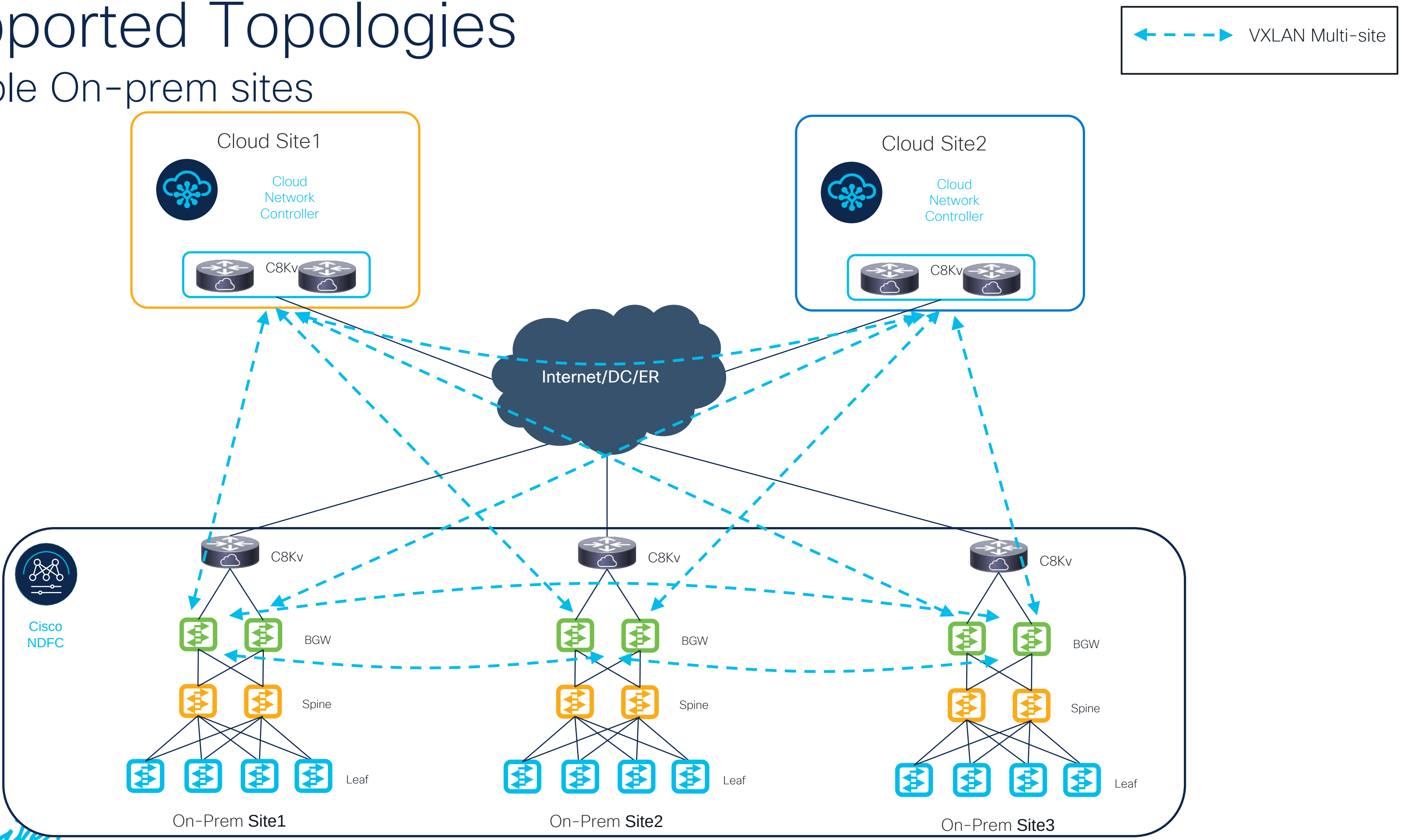
Reference slide

- Full-mesh BGP EVPN peering between On-Prem BGWs and each Cloud sites C8Kv
- IPsec tunnel between C8Kv for secure communication
- Full-mesh BGP EVPN peering between clouds for Cloud-to-Cloud connectivity



Supported Topologies

Multiple On-prem sites

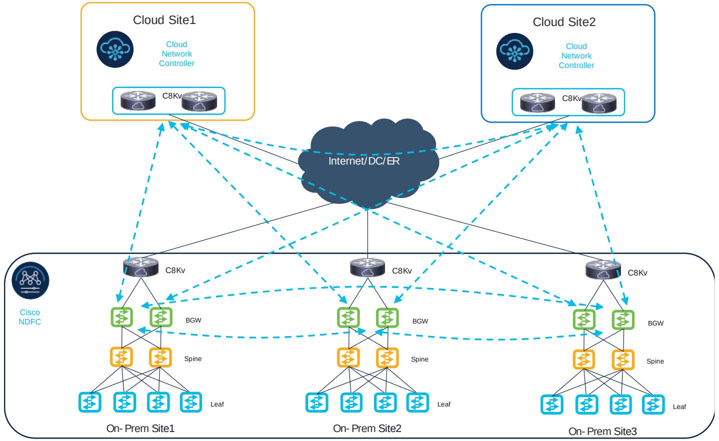


Reference slide

Supported Topologies

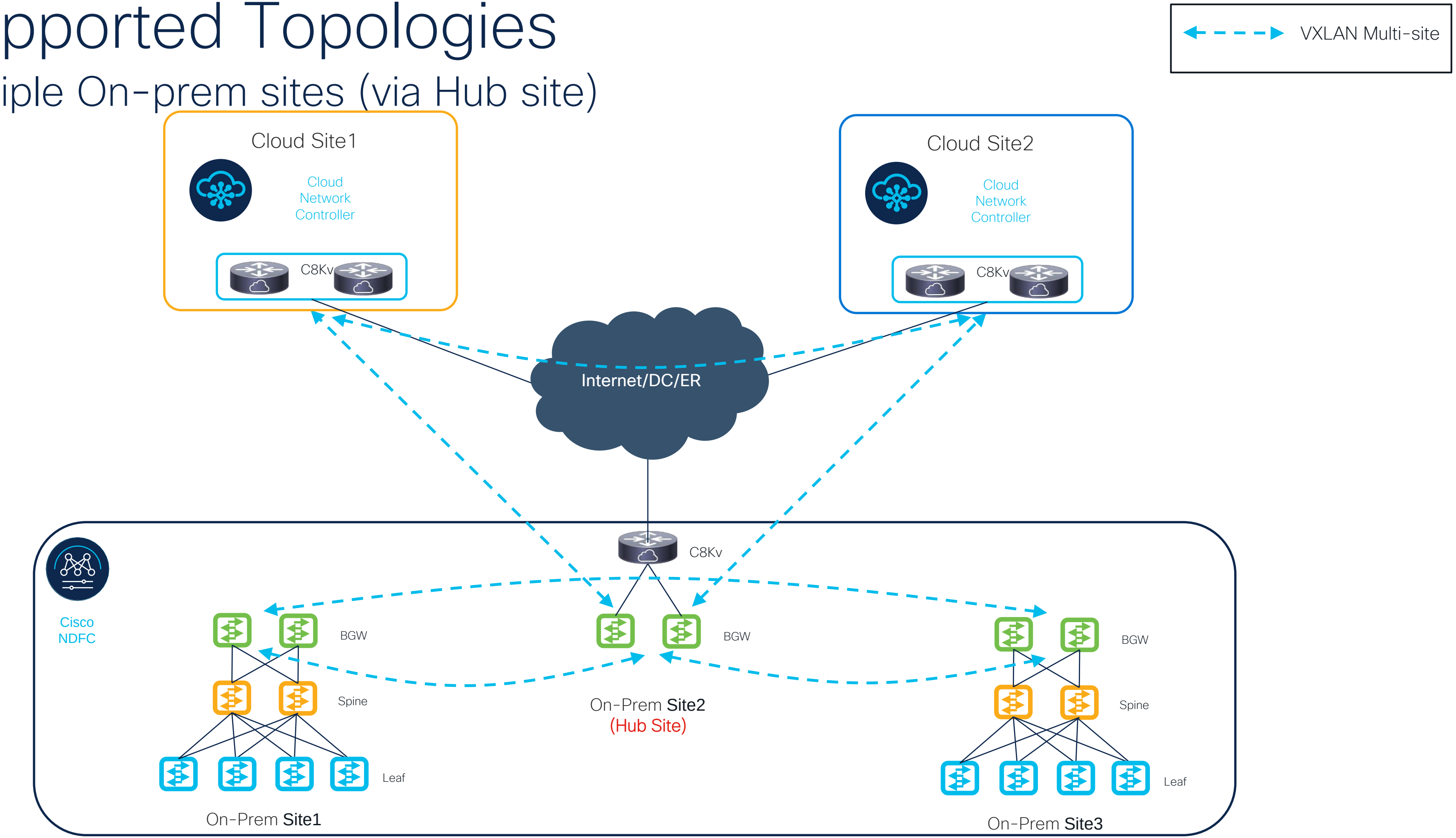
Multiple On-prem sites

- Three On-prem sites, each with its own IPsec device
- Full-mesh or RS based BGP EVPN peering between on-premises sites
- Full-mesh BGP EVPN peering between on-premises BGWs and cloud sites C8Kv
- IPsec tunnel between C8Kv for secure communication
- Full-mesh BGP EVPN peering between clouds for Cloud-to-Cloud connectivity



Supported Topologies

Multiple On-prem sites (via Hub site)

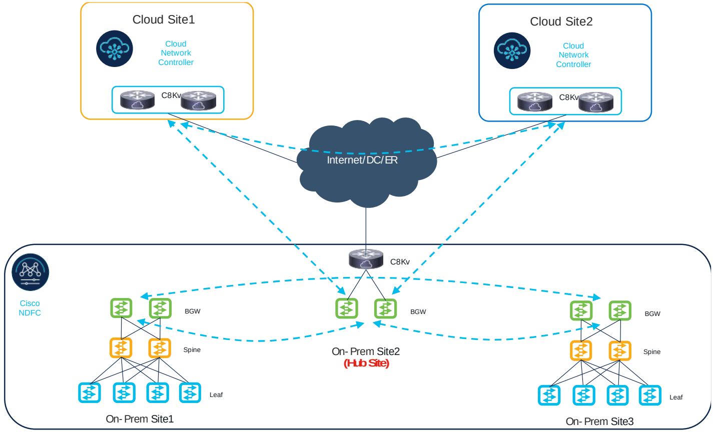


Supported Topologies

Multiple On-prem sites (via Hub site)

Reference slide

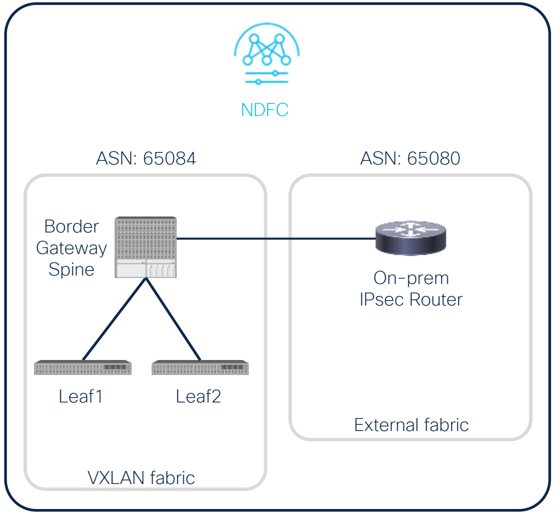
- Three On-prem sites (one Hub site)
- Only Hub site has IPsec device
- Hub site can't have any endpoints attached
- Full-mesh or RS based BGP EVPN peering between on-premises sites
- Full-mesh BGP EVPN peering between on-premises Hub site BGWs and cloud sites C8Kv
- IPsec tunnel between C8Kv for secure communication
- Full-mesh BGP EVPN peering between clouds for Cloud-to-Cloud connectivity

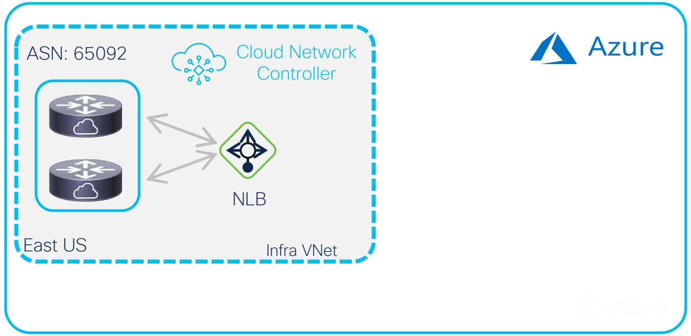


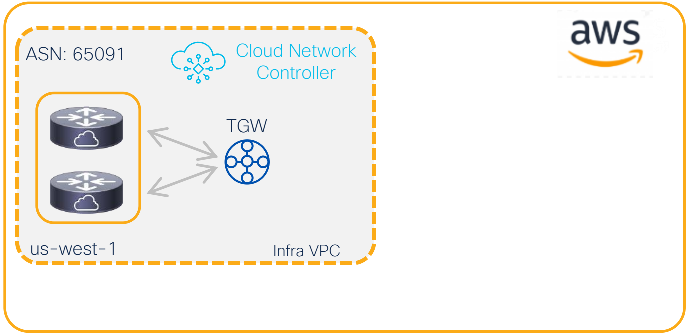
Demo

Topology

Starting Point

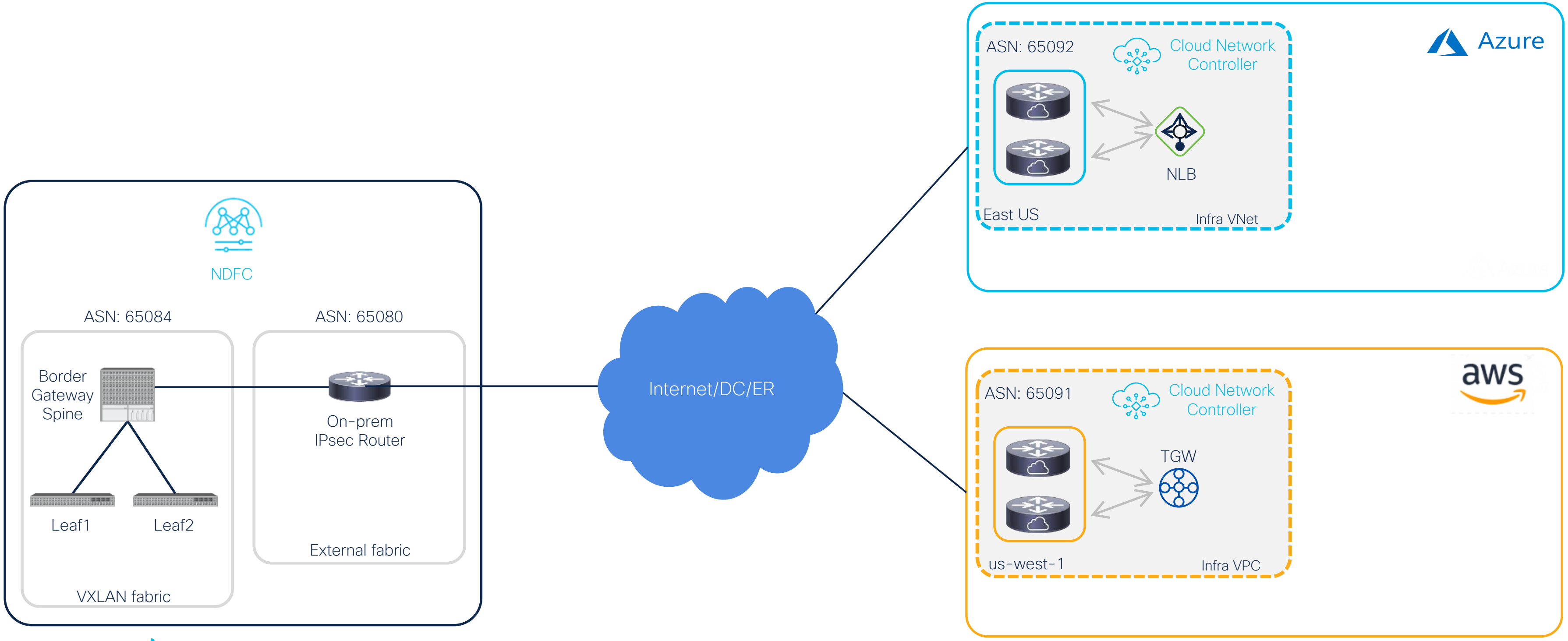






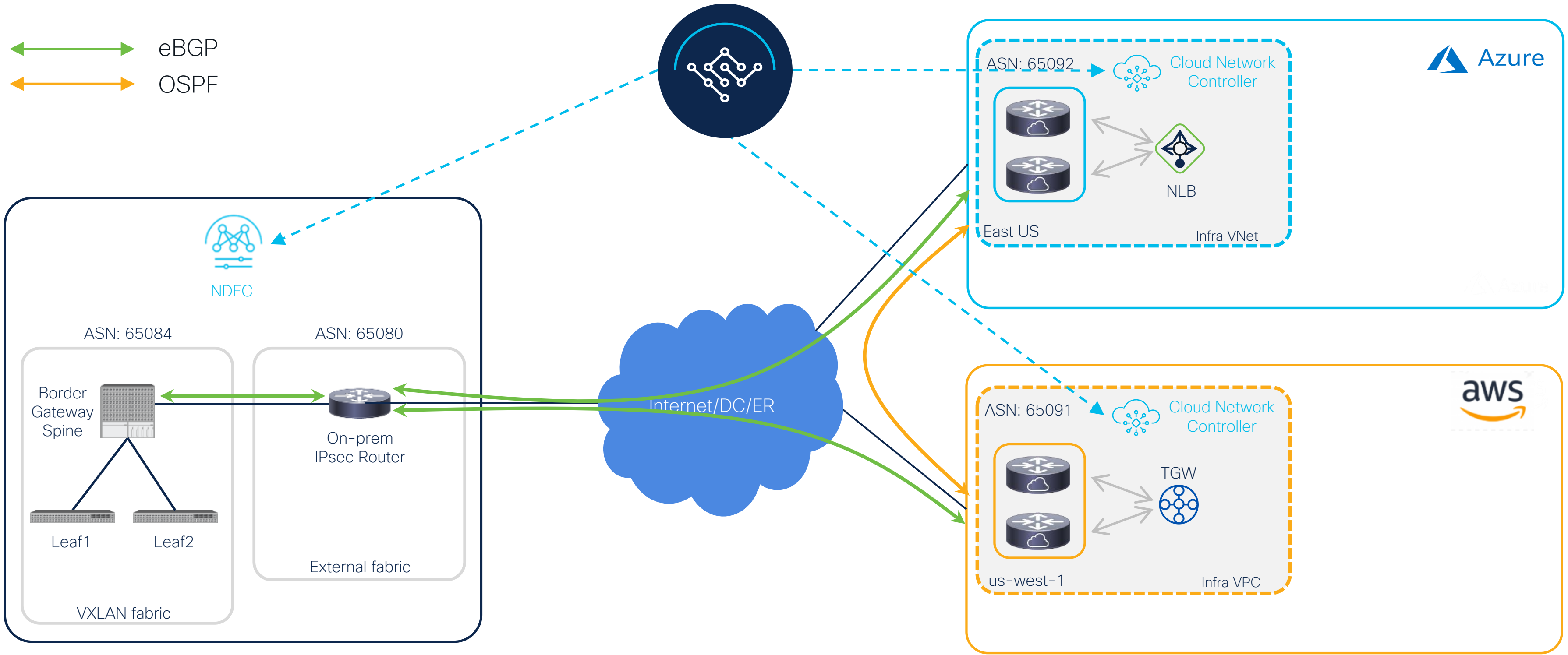
Topology

Step 1 : Build Underlay



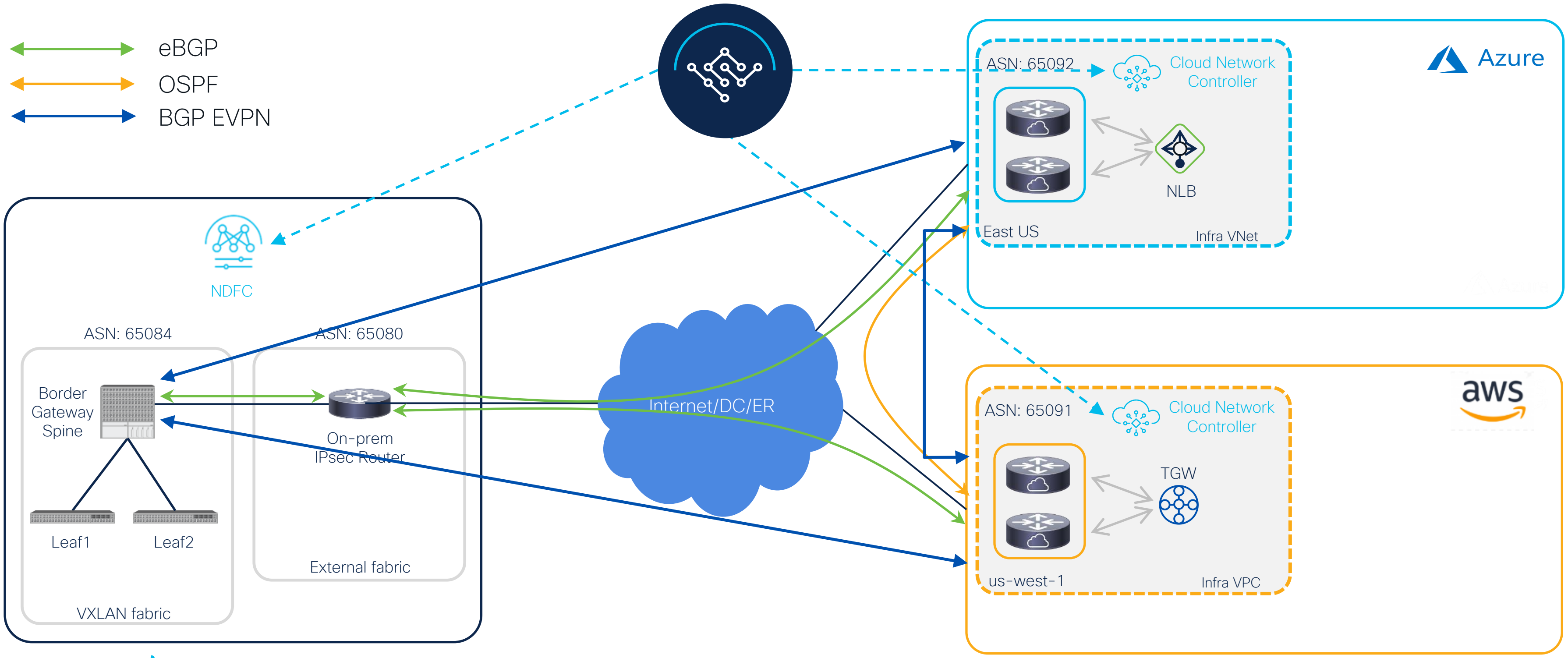
Topology

Step 2 : Build Underlay



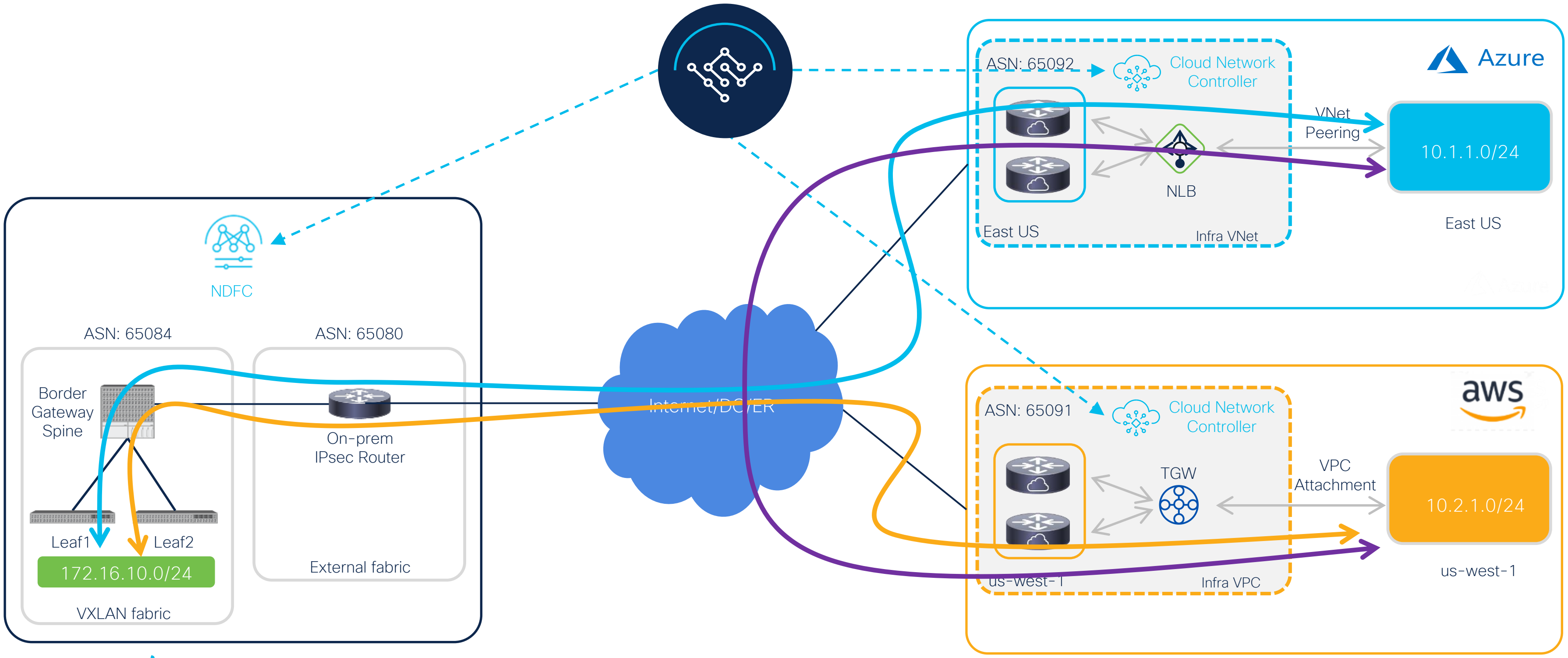
Topology

Step 2 : Build Overlay



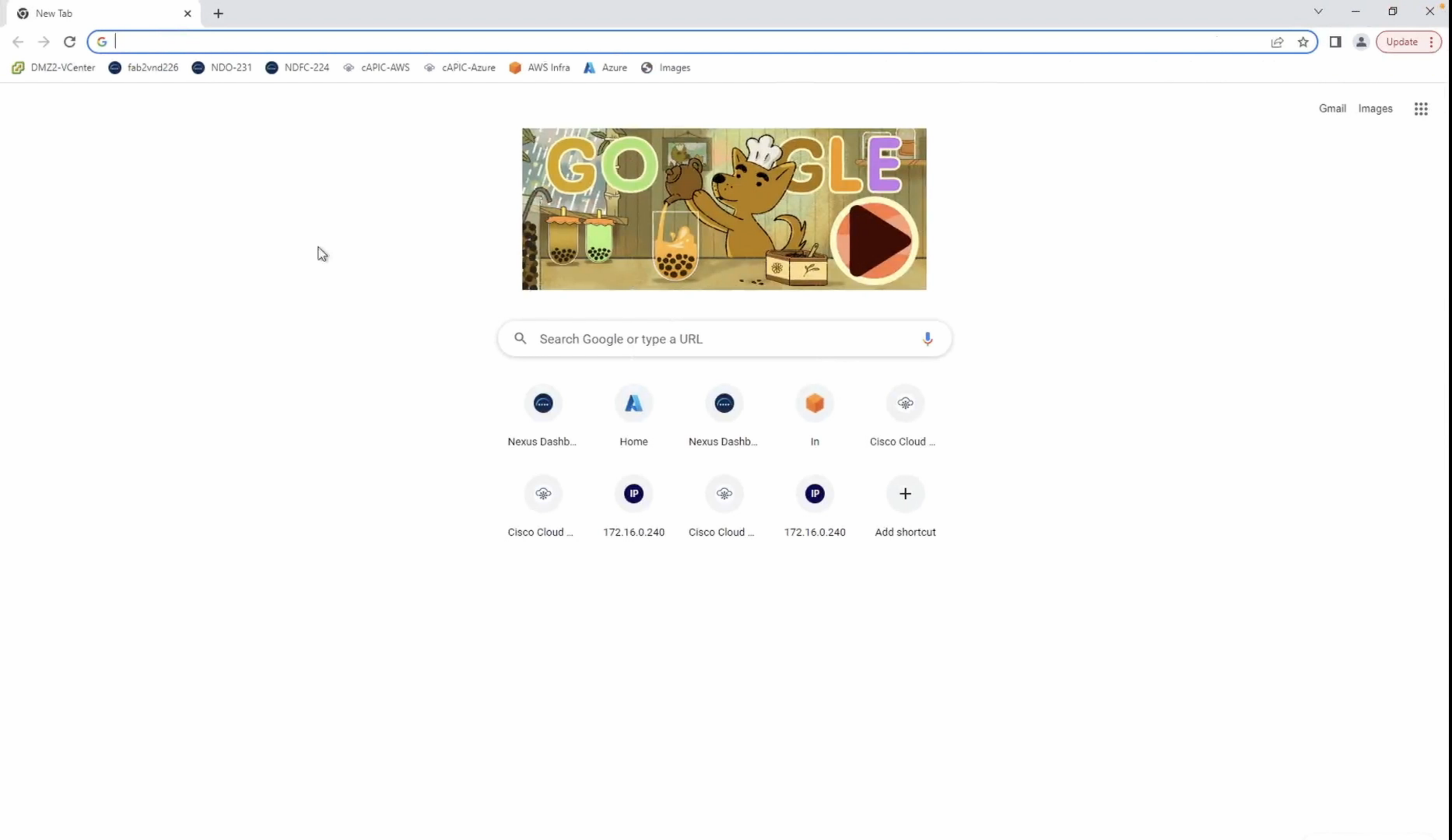
Topology

Step 3 : Deploy VRFs and Networks

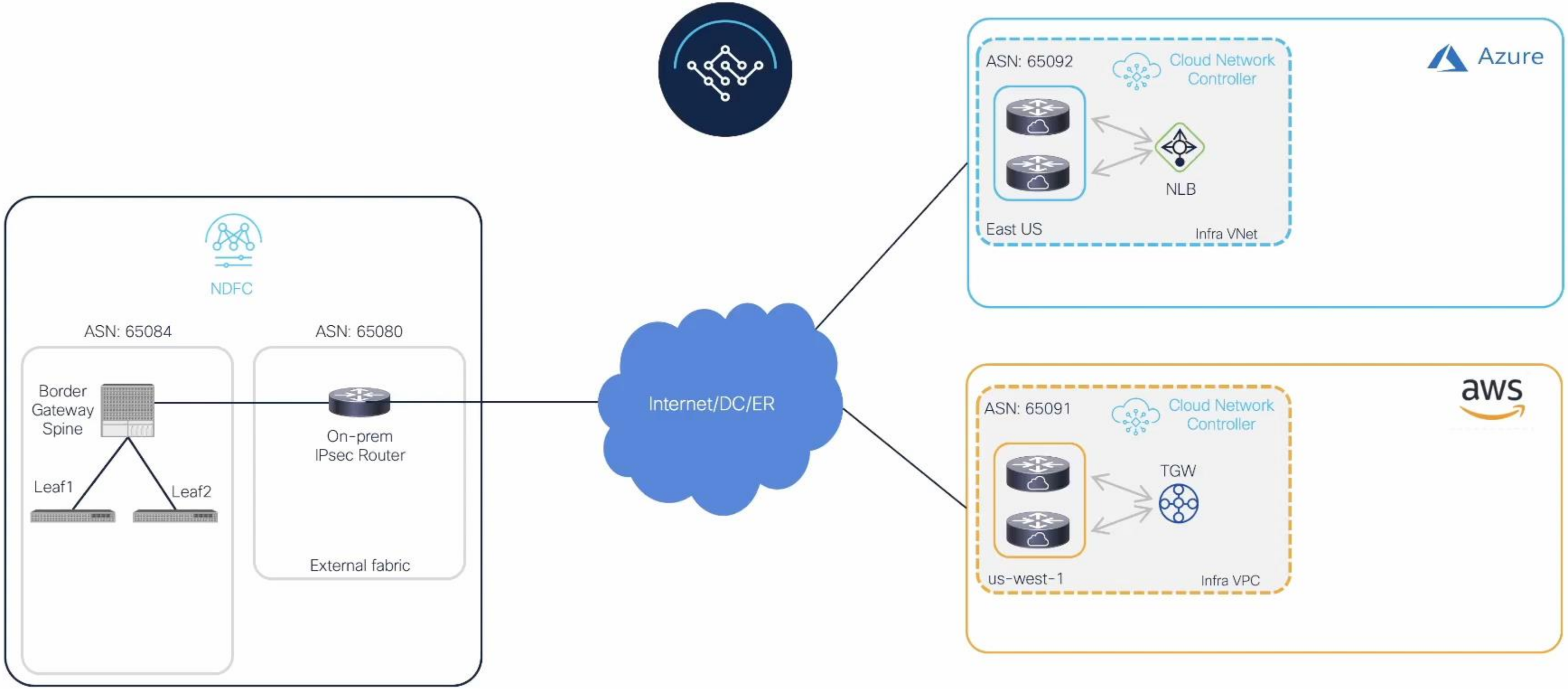


DEMO VIDEOS

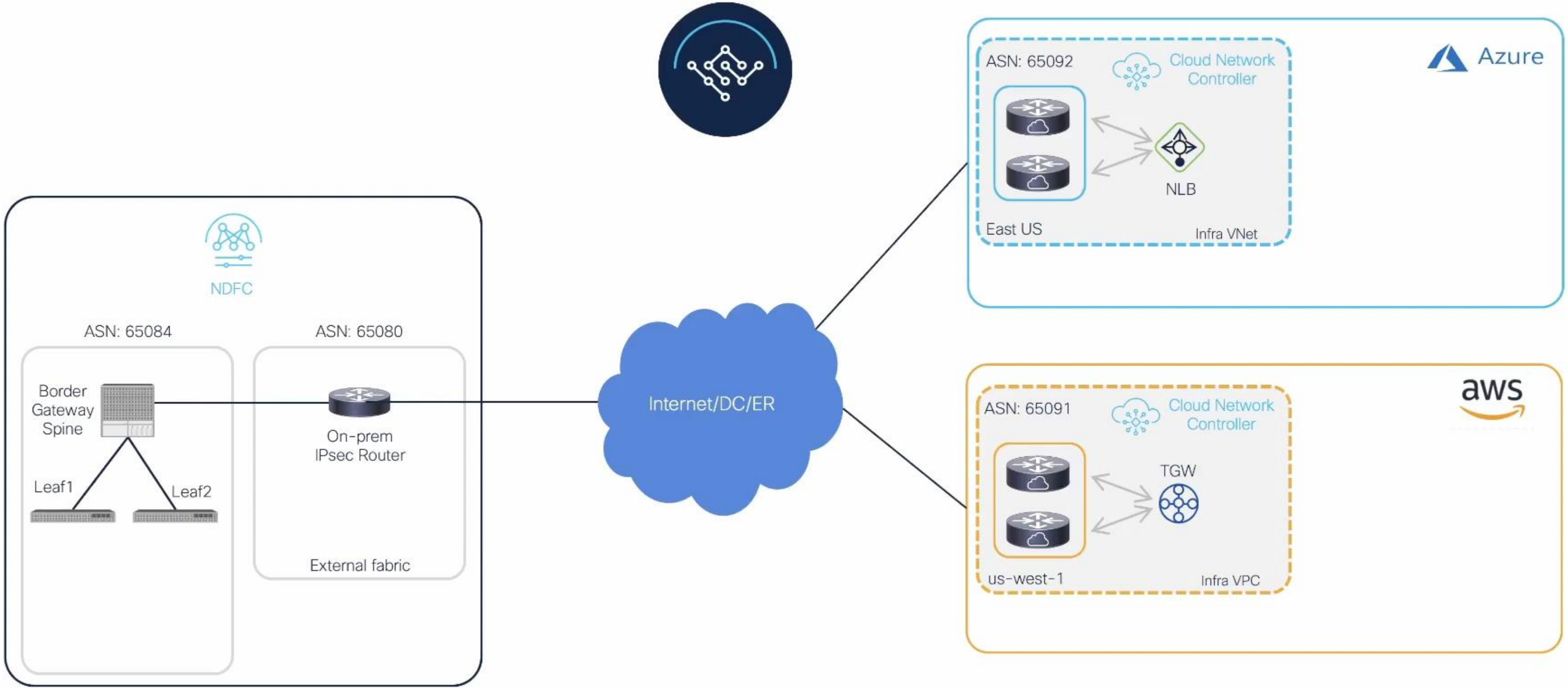
Demo Video


New Tab
Update
DMZ2-VCenter
fab2vnd226
NDO-231
NDFC-224
cAPIC-AWS
cAPIC-Azure
AWS Infra
Azure
Images
Gmail
Images
Search Google or type a URL
Nexus Dashb...
Home
Nexus Dashb...
In
Cisco Cloud ...
Cisco Cloud ...
172.16.0.240
Cisco Cloud ...
172.16.0.240
Add shortcut

Stretched VRF Use-case



VRF Route Leaking Use-case



Further References

- Cisco Cloud ACI on AWS White Paper
- Cisco Cloud ACI on Microsoft Azure White Paper
- Hybrid Cloud Connectivity Deployment for Cisco NX-OS

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

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.

The bridge to possible

Thank you

cisco Live!