You make **possible**

SD-WAN, deployment strategies, managing and monitoring

Tony Hosseiny, TSA @HosseinyTony
Marko Tanaskovic, TSA @MarkoTanaskov10

BRKRST-2519

Barcelona | January 27-31, 2020

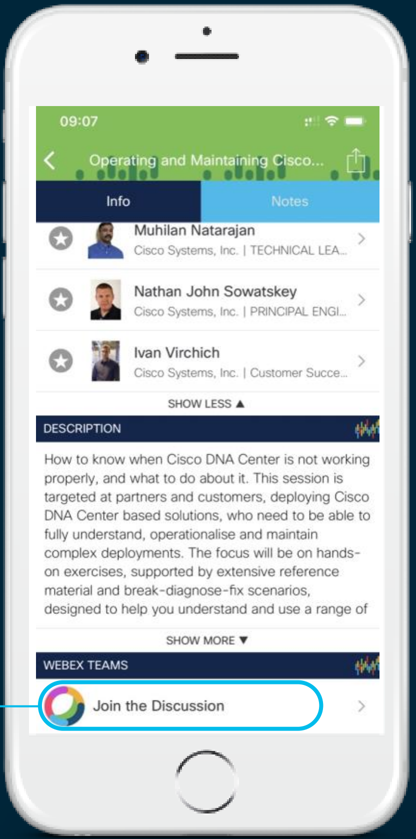
Cisco Webex Teams

Questions?

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

How

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



09:07

Operating and Maintaining Cisco...

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

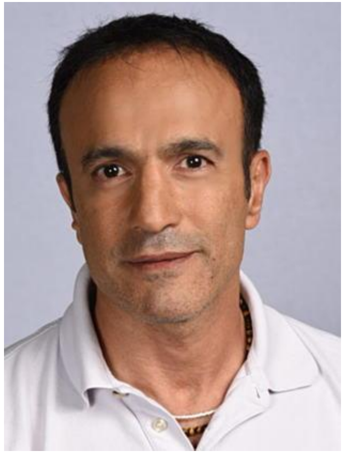
Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

WEBEX TEAMS

Speakers



Tony Hosseiny,
TSA Routing

Marko Tanaskovic,
TSA Cloud Security

“If you can not explain the problem in three simple sentences, then you do not understand the problem.”

Agenda

- Introduction
  - Branch virtualization
  - SD WAN + Edge Security : Integrated vs Cloud
- Planning and Provisioning
- Configure
  - Policies & Best Practices
  - Management tools
- Monitoring
  - Network, Resources & Security
- Takeaways

Introduction

Branch virtualization
SD WAN + Edge Security : Integrated vs Cloud

Introducing new Cisco SD-WAN software

Full-Stack Security

Integrated Firewall, IPS and URL-Filtering on SD-WAN platforms

Simplified Cloud Security

Faster deployment and greater visibility with Cisco Umbrella

40% Faster Office 365 performance

Increased reliability and utilization of all available paths with OnRamp

One console for SD-WAN and network security simplifies management

Cisco SD-WAN Platform Options

Branch

ISR 1100

- Viptela Code
- Next-gen connectivity
- Performance flexibility

ISR 4000

- Up to 2Gbps
- Modular
- Integrated service containers
- Compute with UCS E

vEdge 100

- 100Mbps
- 4G LTE & Wireless

vEdge 1000

- Up to 1Gbps
- Fixed

Data Center

ASR 1000

- 2.5-200Gbps
- High-performance service w hardware assits
- Hardware & software redundancy

vEdge 2000 /
vEdge 5000

- 10Gbps
- Modular

Virtualization

ENCS 5100

Up to 250Mbps

ENCS 5400

Up to 250Mbps

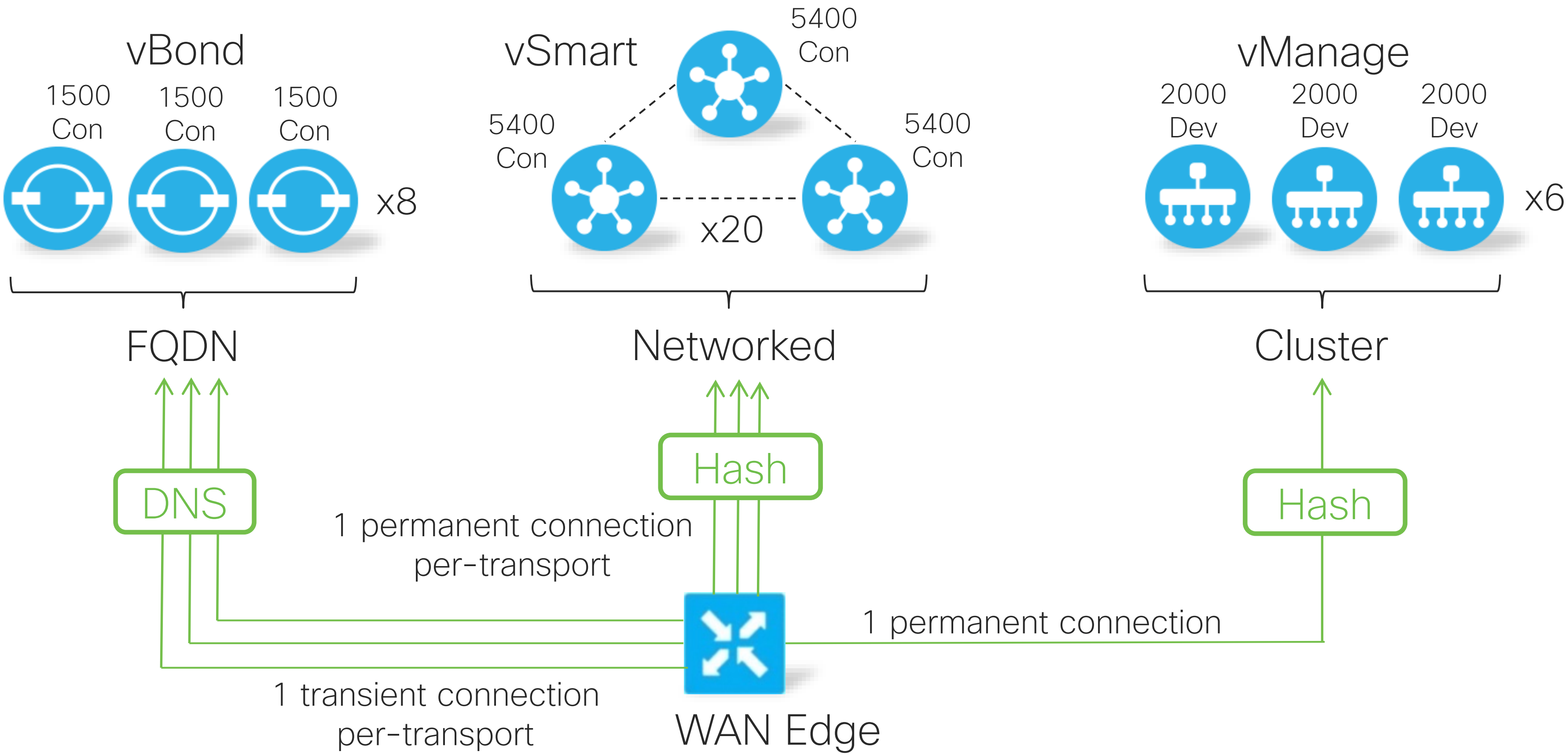
Public Cloud

Microsoft Azure

Google Cloud

aws

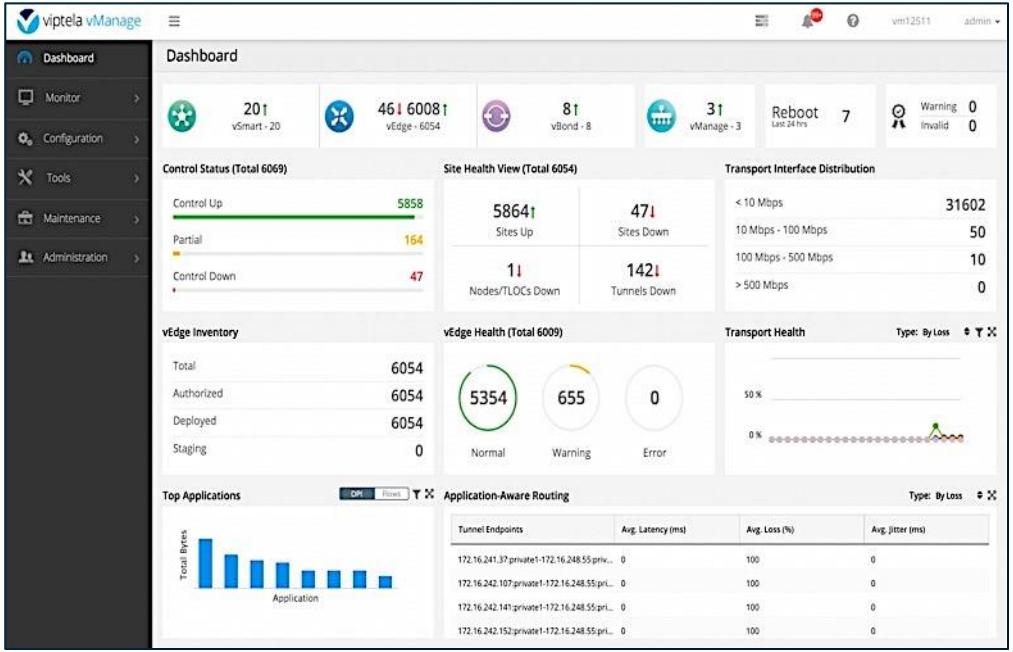
Horizontal Solution Scale



Note: Refer to wiki for WAN Edge scale
https://wiki.cisco.com/pages/viewpage.action?pageId=140876530

Single Pane of Glass Operations

vManage GUI



viptela vManage

vm12511 admin

Dashboard

Monitor

Configuration

Tools

Maintenance

Administration

Dashboard

20↑ vSmart - 20

46↓ 6008↑ vEdge - 6054

8↑ vBond - 8

3↑ vManage - 3

Reboot Last 24 hrs 7

Warning 0
Invalid 0

Control Status (Total 6069)

Control Up	5858
Partial	164
Control Down	47

Site Health View (Total 6054)

5864↑ Sites Up

47↓ Sites Down

1↓ Nodes/TLOCs Down

142↓ Tunnels Down

Transport Interface Distribution

< 10 Mbps	31602
10 Mbps - 100 Mbps	50
100 Mbps - 500 Mbps	10
> 500 Mbps	0

vEdge Inventory

Total	6054
Authorized	6054
Deployed	6054
Staging	0

vEdge Health (Total 6009)

5354 Normal

655 Warning

0 Error

Transport Health Type: By Loss

Top Applications DPI Flows

Application-Aware Routing Type: By Loss

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
172.16.241.37:private1-172.16.248.55:priv...	0	100	0
172.16.242.107:private1-172.16.248.55:pri...	0	100	0
172.16.242.141:private1-172.16.248.55:pri...	0	100	0
172.16.242.152:private1-172.16.248.55:pri...	0	100	0

REST NETCONF Syslog SNMP Flow Export

- Intuitive GUI driven operations
  - Management, monitoring and troubleshooting
- Cloud Delivered
  - Private, hosted or managed
- Single or Multi-tenant
- Role-based Access Control
- Clustered for scale and high availability
- REST APIs based

Cloud-hosted Deployment

Summary

- Recommended mode of deployment
  - Ease of deployment – Cisco orchestrated
  - No On-Prem design considerations
  - Easy to scale and to deliver redundancy / HA
- Requirements
  - Internet connectivity from every site (unless using DirectConnect)
  - If using MPLS Transport, Internet breakout required for Control Plane
- Challenge
  - With a single Internet connection, no DirectConnect or Internet Breakout from MPLS – No Controller Redundancy

On-prem Deployment Considerations

- Supporting NAT Traversal
  - vBond supporting Private + Public Discovery
- Supporting Hybrid Environments
  - Interconnected MPLS and Internet Domains
  - Separate MPLS and Internet Domains
- Redundancy
- Firewall Traversal

Release alignment and lifecycle

Release	Extended November 2018	Standard March 2019	Extended July 2019	Standard November 2019	Standard March 2020	Extended July 2020	Standard November 2020
IOS XE SD-WAN	16.10	16.11	16.12		17.2	17.3	17.4
Viptela OS	18.4	19.1	19.2	19.3	20.1	20.2	20.3

- 3 Cisco SD-WAN releases per year
  - March, July, November
  - July is the long-life release
- Cisco IOS XE versions start at ".1", e.g. 17.2.1
- Viptela OS releases prior to 20.X start at ".0", e.g. 19.2.0
  - Starting in 20.1, Viptela releases will also be .1 based, e.g. 20.1.1 will be the first Viptela release

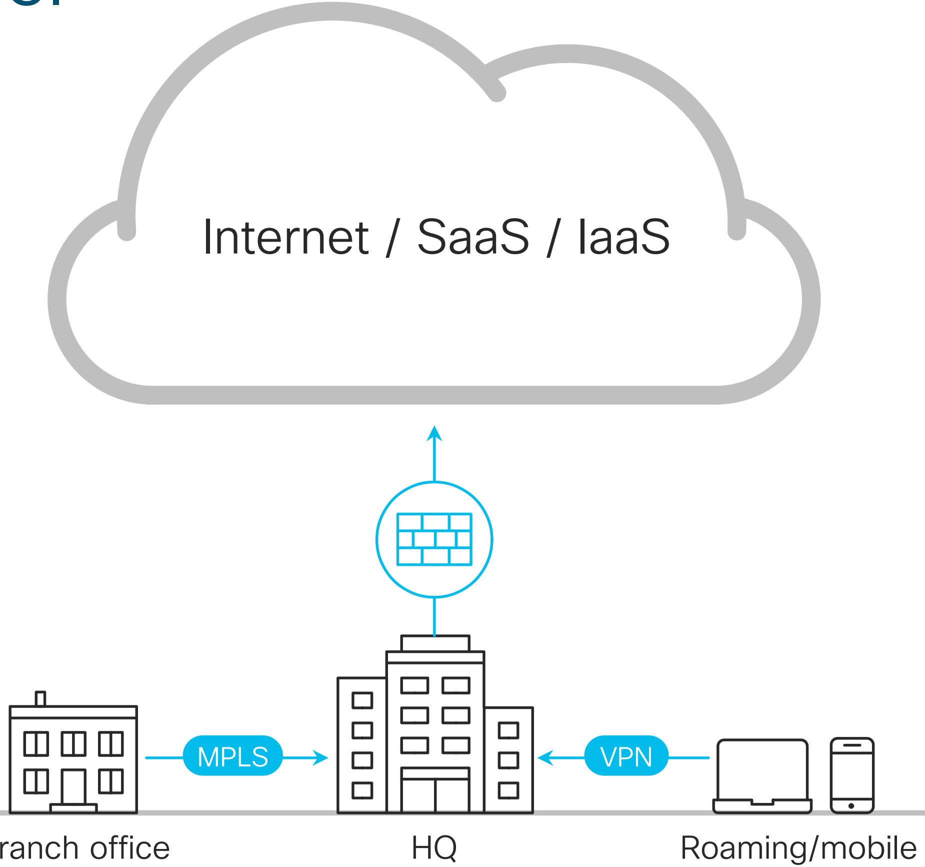
The Traditional Model

Network

Centralized

Security

Single place to enforce policies and protection



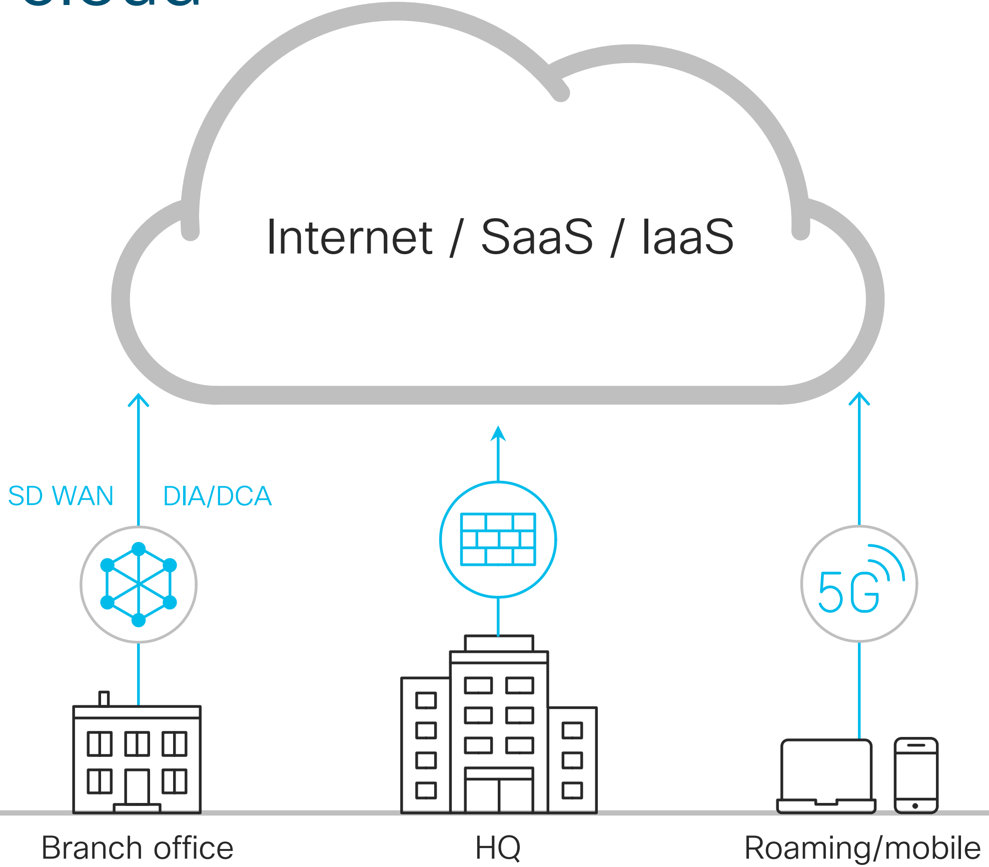
Disruption: To the cloud

Network

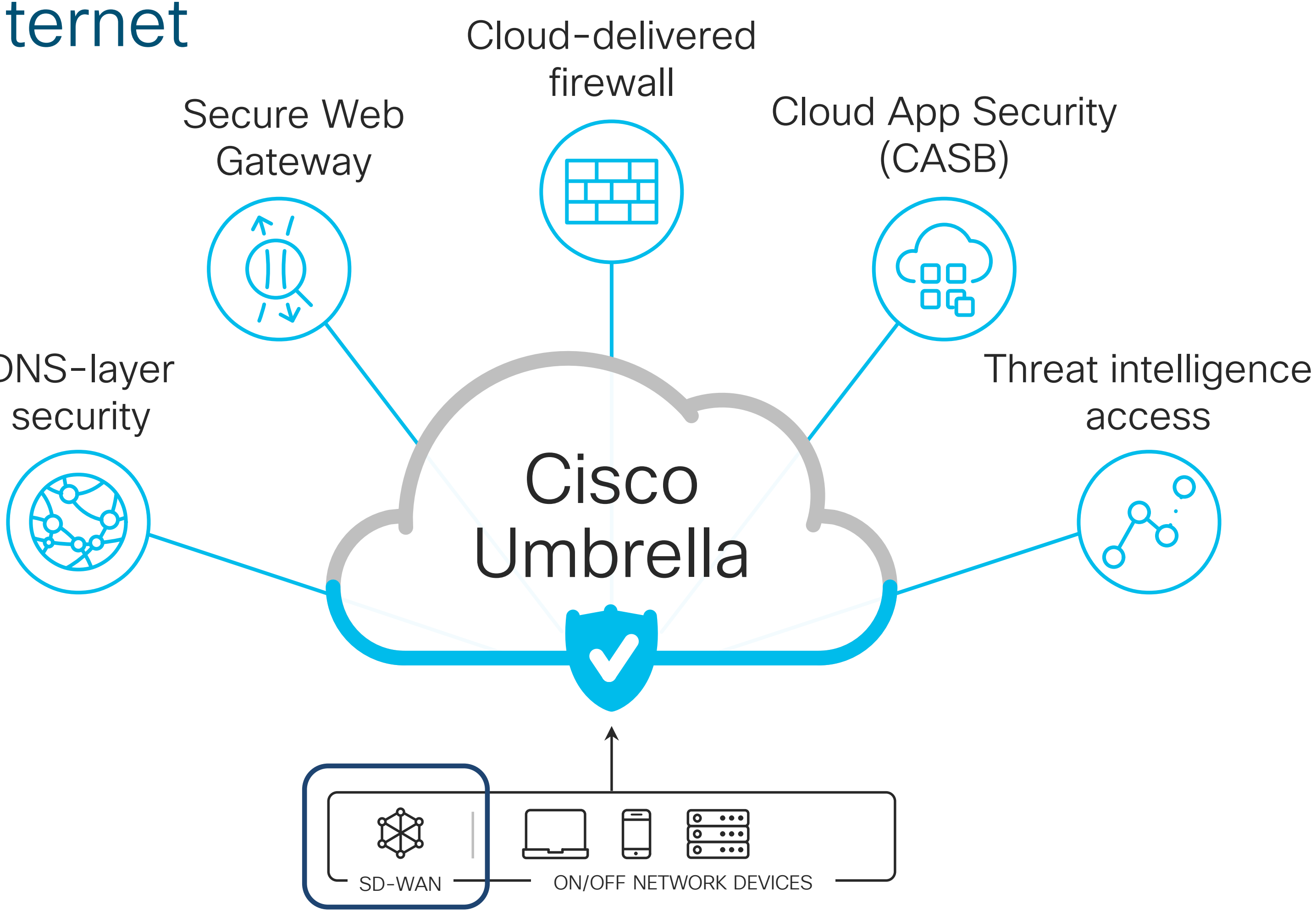
Decentralized

Security

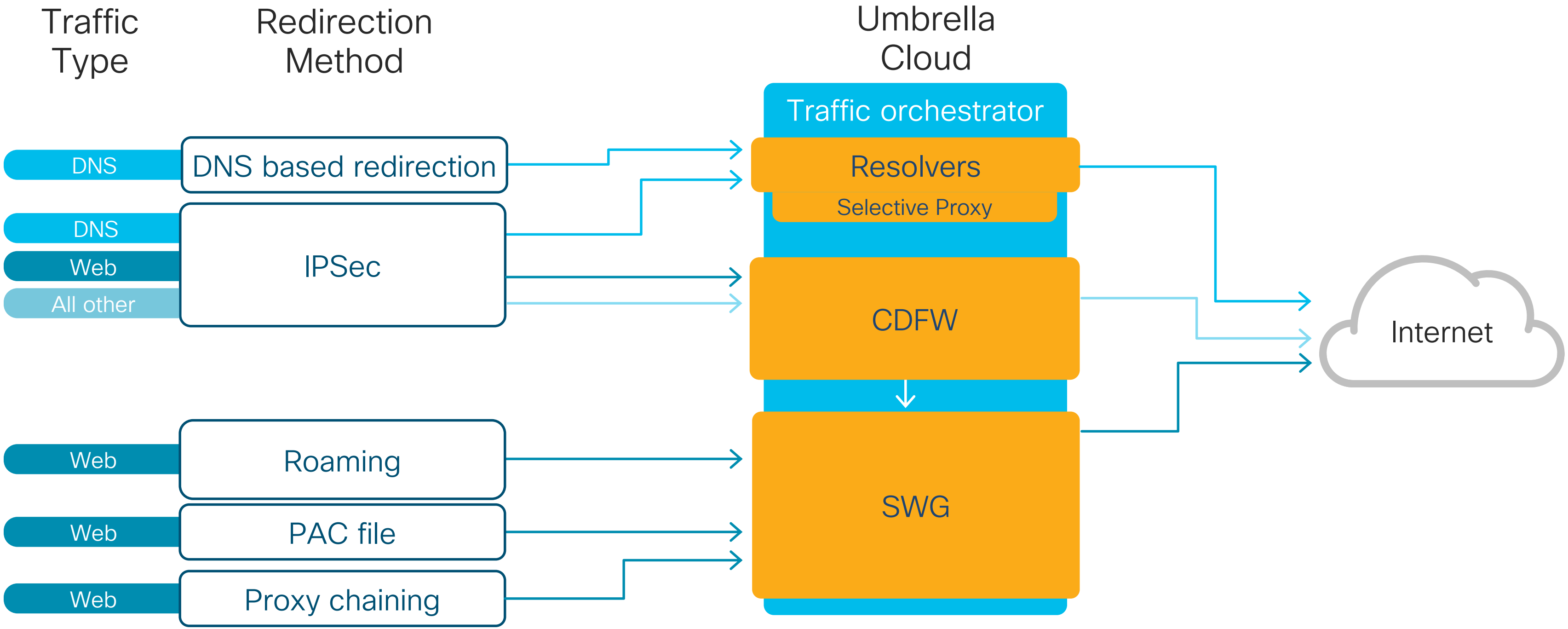
Protect at data center, cloud, and branch edge



Secure Internet Gateway



Traffic Redirection

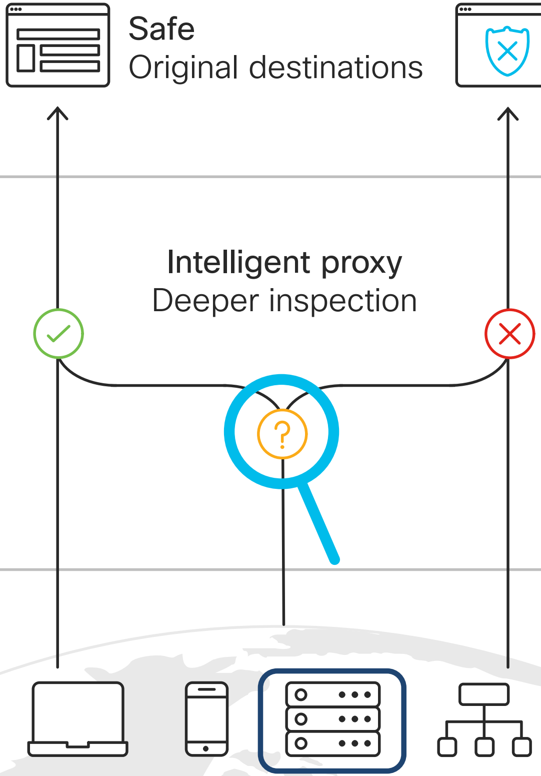


DNS Security

A good place to start

Destinations

Original destination or block page



Security controls

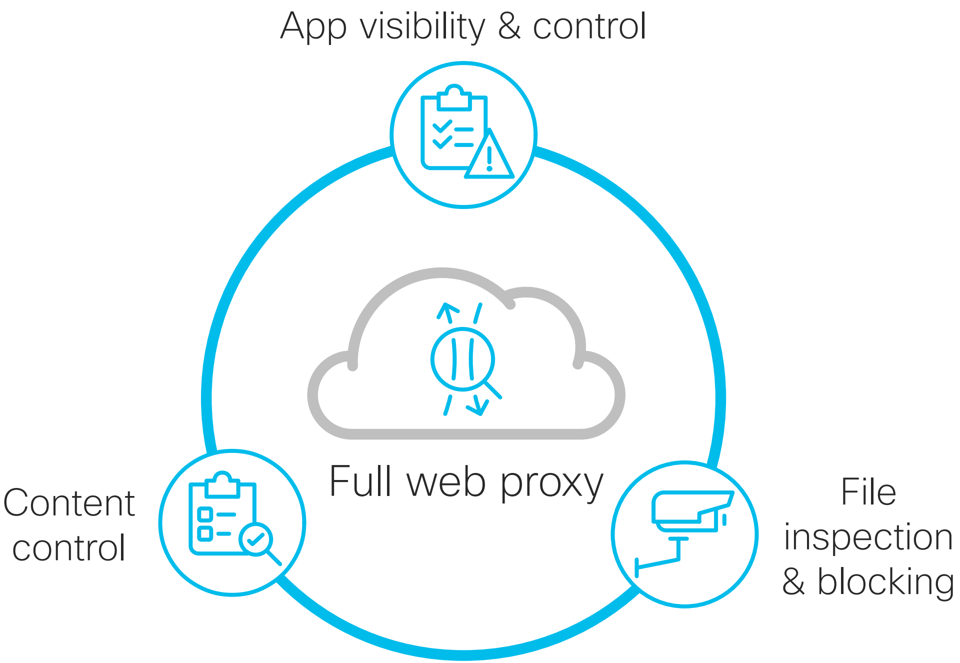
- DNS enforcement
- Risky domain inspection through proxy
- SSL decryption available
- Application blocking

Internet traffic

On and off-network

Secure Web Gateway: Full Web Proxy

Deep inspection and control of web traffic



Capture all web traffic with full URL logging

Enforce acceptable use policies with content filtering and URL blocking

Block more malware with URL scanning, file inspection (AMP/AV), and sandboxing (Threat Grid)

Advanced app control

Cloud-delivered firewall

Firewall for the cloud edge

Capabilities

- L3/L4 firewall; up next - L7 capabilities
- Supported today on IPSec tunnel
- Outbound firewall only

Identities

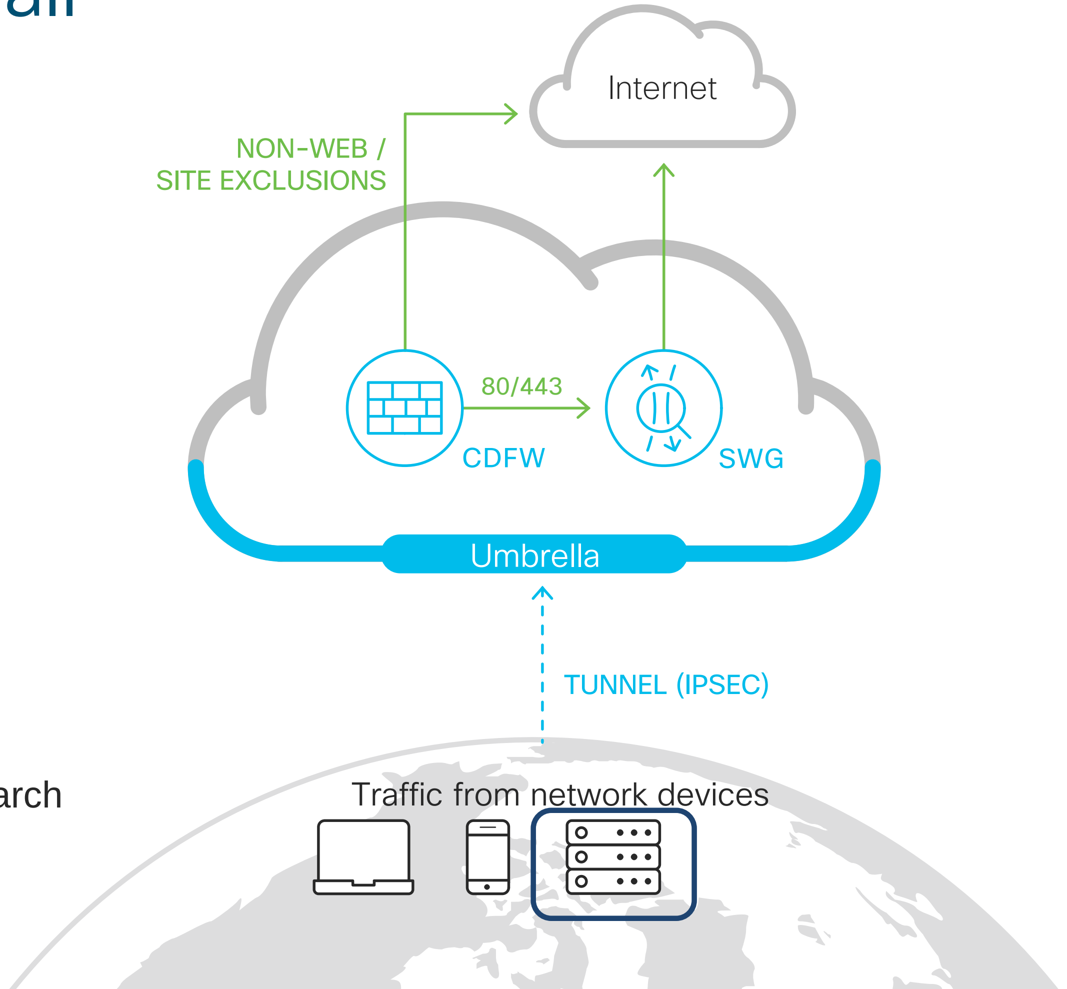
- Network Tunnel used as primary identity

Infrastructure

- Multi-geo datacenter support
- Auto-DC failover

Logging and Reporting

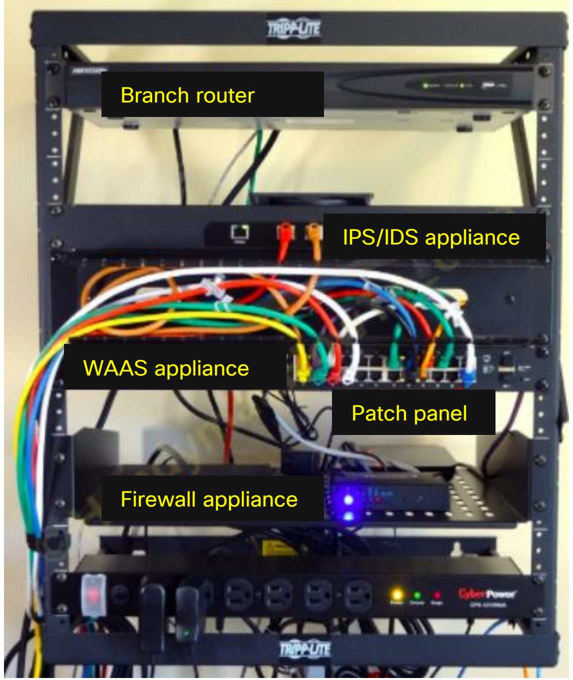
- Firewall logs included as part of Activity Search
- Log export supported via S3



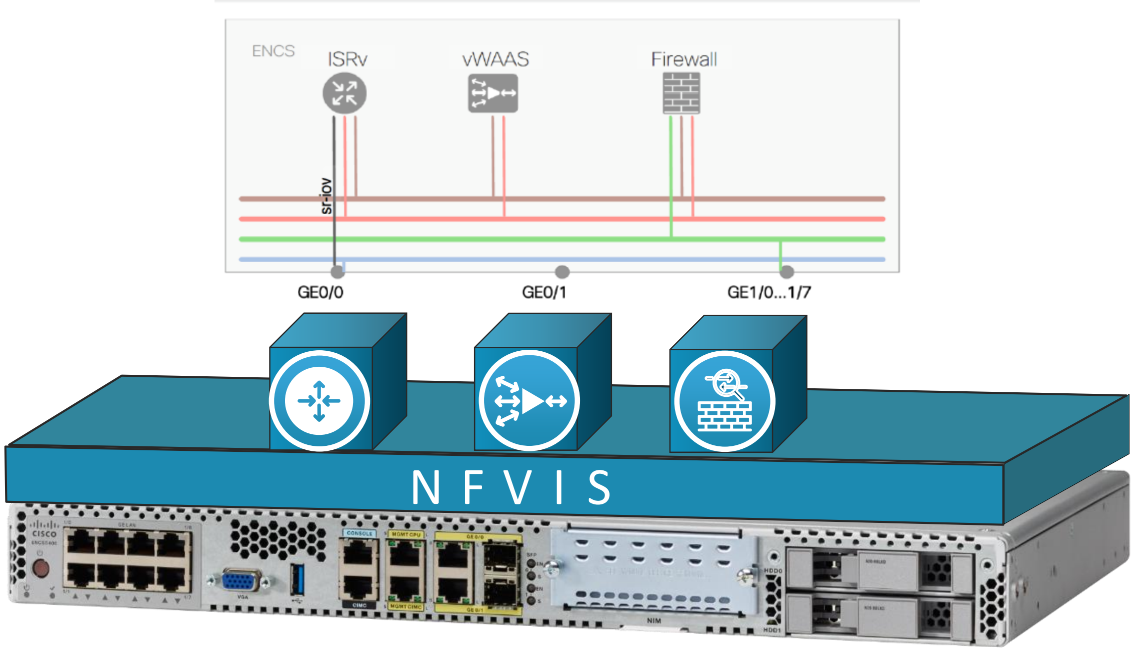
Planning and Provisioning Virtualized Branch

What changes with Cisco vBranch?

Before

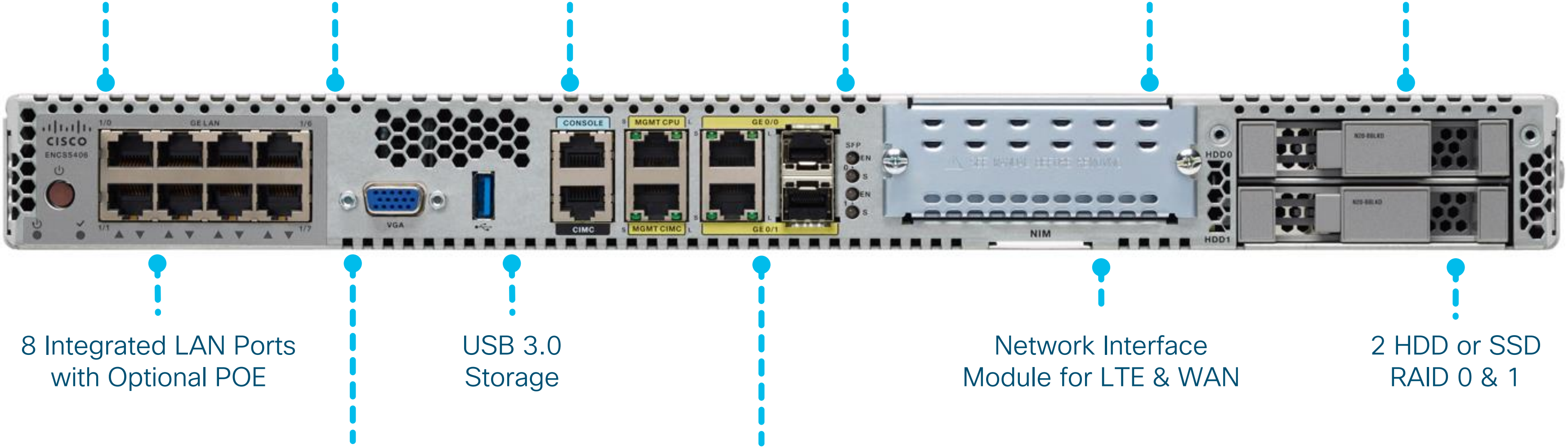


After



A single x86 compute platform housing multiple VNFs

ENCS 5400 Series – I/O Side



Integrated Power Supply

16 - 64 GB DRAM

6, 8, or 12-Core Intel Xeon-D

Dedicated Lights-out Management (CIMC)

(Optional) Hardware RAID Controller

Internal M.2 Storage 64 – 400 GB

8 Integrated LAN Ports with Optional POE

USB 3.0 Storage

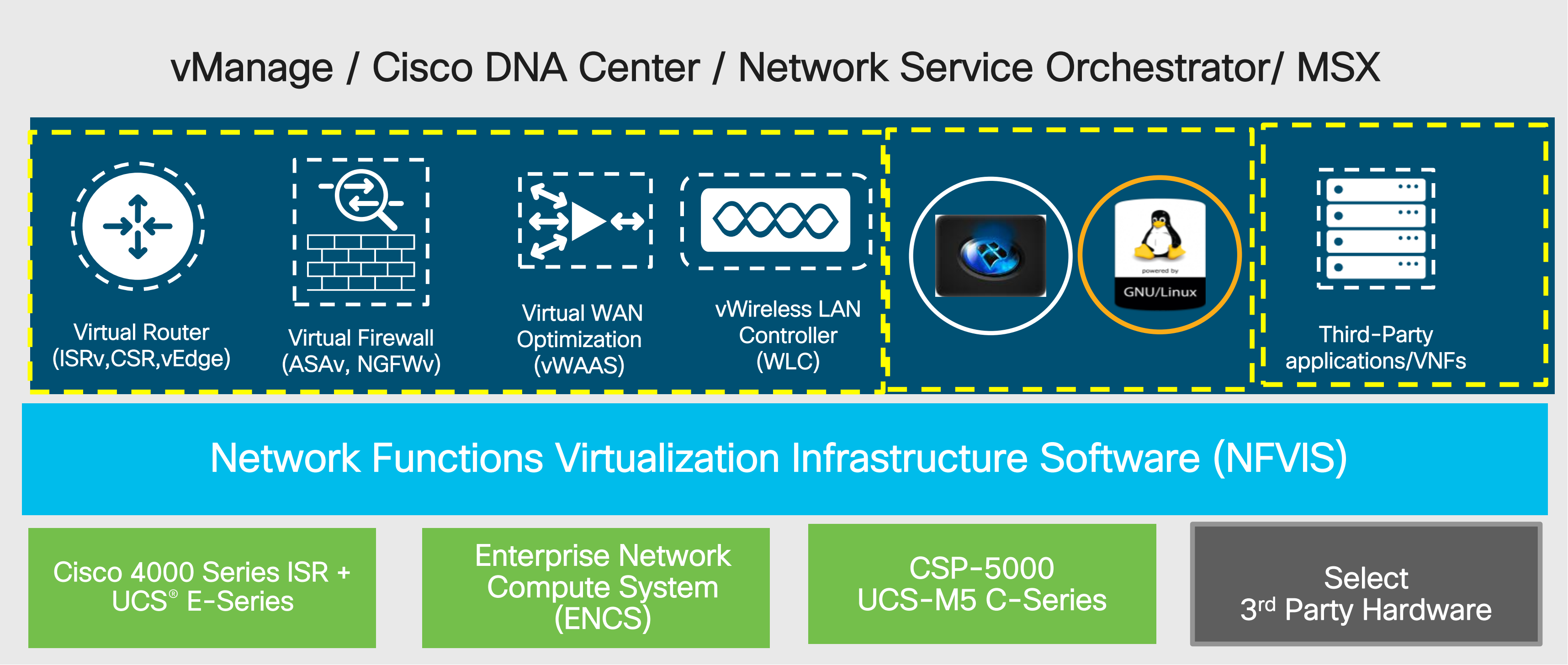
Network Interface Module for LTE & WAN

2 HDD or SSD RAID 0 & 1

Hardware Acceleration for VM Traffic

2 Onboard Gigabit Ethernet ports with SFP

Software Defined Branch
Deploy Services on Any Platform



vManage / Cisco DNA Center / Network Service Orchestrator/ MSX

Virtual Router (ISRv,CSR,vEdge)

Virtual Firewall (ASAv, NGFWv)

Virtual WAN Optimization (vWAAS)

vWireless LAN Controller (WLC)

Third-Party applications/VNFs

Network Functions Virtualization Infrastructure Software (NFVIS)

Cisco 4000 Series ISR + UCS® E-Series

Enterprise Network Compute System (ENCS)

CSP-5000 UCS-M5 C-Series

Select 3rd Party Hardware

Virtualization OS: NFVIS optimized for VNF Deployments

Network Hypervisor

- Enables segmentation of virtual networks
- Abstract CPU, memory, storage resources
- VNF deployment and update
- VNF status and monitoring

Zero Touch Deployment

- Automatic connection to PnP server
- Secure connection to the orchestration system
- Easy day 0 provisioning

Monitoring

- NETCONF notifications
- Host and VM statistics
- Packet Capture

Life Cycle Management

- Provisioning and launch of VNFs
- Failure and recovery monitoring
- Stop and restart services
- Dynamically add and remove services

Service Chaining

- External connectivity and to other services
- Multiple service access options
- No hardware offload with UCS

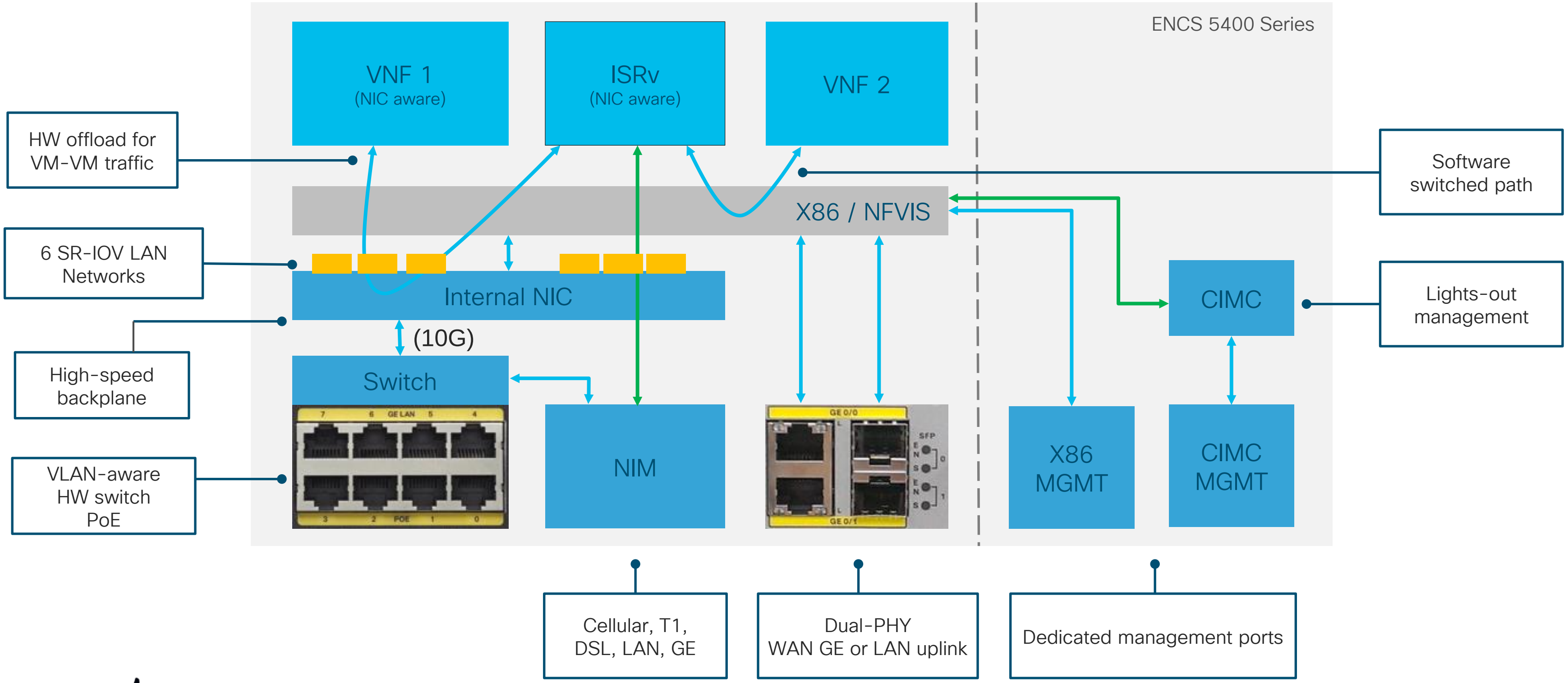
Open API

- Programmable API for service orchestration
- REST and NETCONF API

ENCS 5400 Internal Networking

↔ Data Path

↔ Control Path



ENCS 5400 Series

VNF 1 (NIC aware)

ISRv (NIC aware)

VNF 2

X86 / NFVIS

Internal NIC

(10G)

Switch

NIM

CIMC

X86 MGMT

CIMC MGMT

HW offload for VM-VM traffic

6 SR-IOV LAN Networks

High-speed backplane

VLAN-aware HW switch PoE

Software switched path

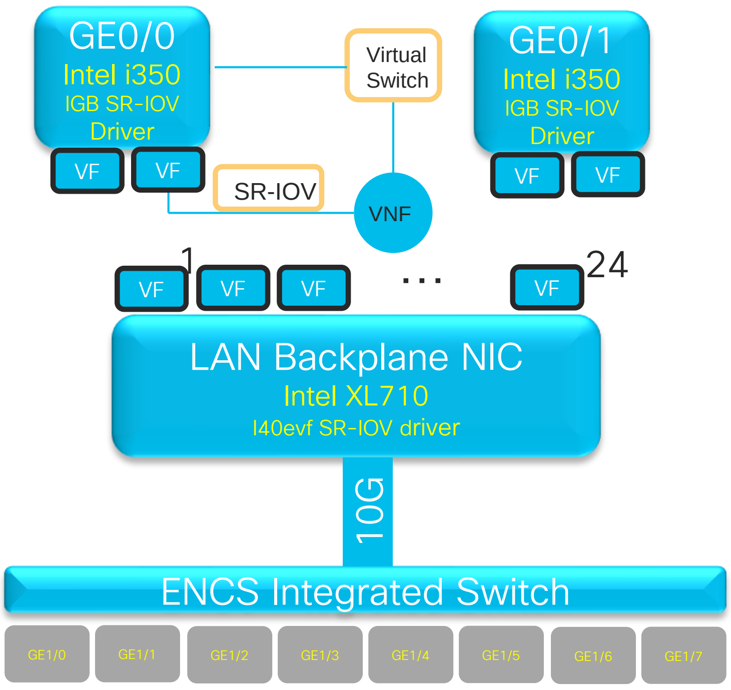
Lights-out management

Cellular, T1, DSL, LAN, GE

Dual-PHY WAN GE or LAN uplink

Dedicated management ports

Understanding SR-IOV on the ENCS 5400



- There are multiple ways a VNF can connect to a physical NIC of the underlying server/hardware
  - Virtual switch - introduced by the hypervisor
  - SR-IOV - by connecting the VNF directly to the physical NIC
  - PCI Passthrough – dedicating the entire NIC to the VNF directly
- **SR-IOV (Single root IO-Virtualization)** allows multiple VNFs to connect to a physical interface on the server/hardware
  - However for a VNF to use SR-IOV network that the NIC provides, the VNF needs to support the drivers that are required by the NIC
- On the ENCS, there are two NIC types on which SR-IOV has been enabled
  - WAN NIC GiG NIC – Intel i350, uses IGB Drivers
  - LAN back plane NIC - Intel XL710, uses i40vef Drivers
  - As long as the VNF supports these NIC drivers, the VNF can be deployed using SR-IOV
- VNFs can be service chained using SR-IOV VFs on ENCS
- Using SR-IOV provides the best performance
  - Eliminates performance issues due to the virtual switch
- VNFs can always be connected/service chained using virtual switch

NFVIS Compare Networking Options

	SR-IOV	DPDK-OVS	OVS
	← Performance		Flexibility →
Service Chain Throughput	Service Chain throughput better than DPDK/OVS	Service Chain throughput near SRIOV, better than non-DPDK OVS	Service chain throughput lower than DPDK and SRIOV
NFVIS Default Cores + Additional CPU	1 core < 16core system 2 cores >= 16 core system	1+1 CPU <=16 core system 2+2 >16 core system 1+1GB mem in <=32GB system 1+2GB mem in > 32GB system	1 core < 16core system 2 cores >= 16 core system
Driver requirements in VNF	SRIOV	NO Virtio required	NO Virtio required
Supported capability in platforms ***	**ENCS54xx** igb, igbvf, i40evf **UCSEM3** front_10G ixgbvf **UCS5K, CSP5K** i40evf, ixgbvf	Yes 3.10.1 onwards Yes 3.12.1 onwards Yes 3.12.1 onwards	Supported

***Default LAN-VF increase from 6-to-16 in NFVIS 3.12.1 onwards

***Dynamic VF addition in CSP5K, UCSM5 in NFVIS 3.12.1 onwards

Cisco and 3rd Party VNF Support

New

vEdge Cloud

- High performance
- SDWAN Edge
- NETCONF support

New

ISRv/ SD-WAN ISRv

- High performance
- Rich features
- End-to-end support

New

NGFWv

- Harden virtual services
- Enable secure access
- On-premise or cloud management

New

Third-Party VNFs

- VNF program
- Tested and certified
- Streamlined support from Cisco and third party

vWAAS

- ISR WAAS: Leader in Gartner MQ
- Superior caching with Akamai Connect

vWLC

- Survivability and scale
- Built for small and medium-sized branches

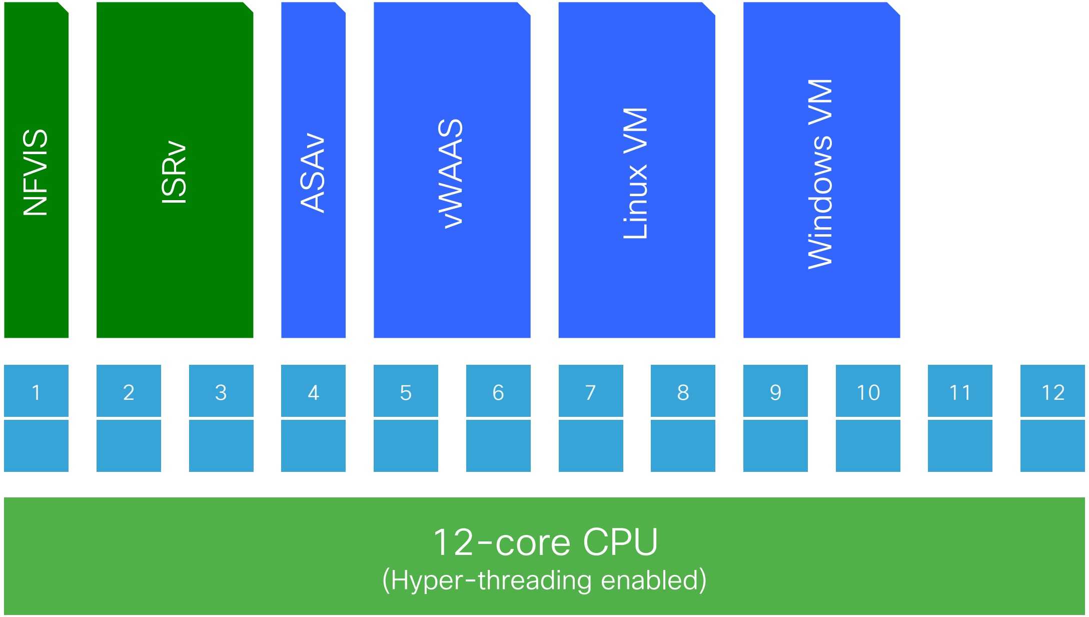
ASAv

- Comprehensive protection
- Full DC class Featured functionality
- Designed for NFV

Applications

- Microsoft Windows
- Custom applications

ENCS 5400 CPU Allocation Planning

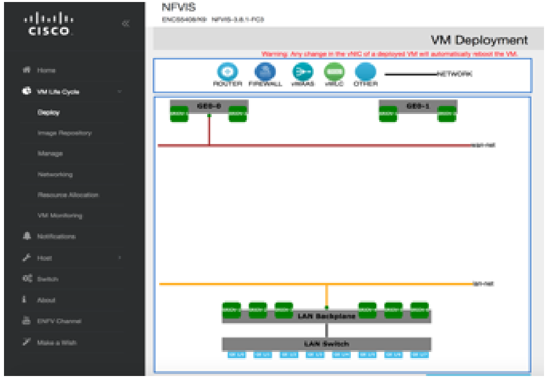


- 1 core = 1 vCPU = 1 physical core
- 1-core allocation for NFVIS to cover OS, Hypervisor & vSwitch functions
- 2-core minimum allocation for ISRv

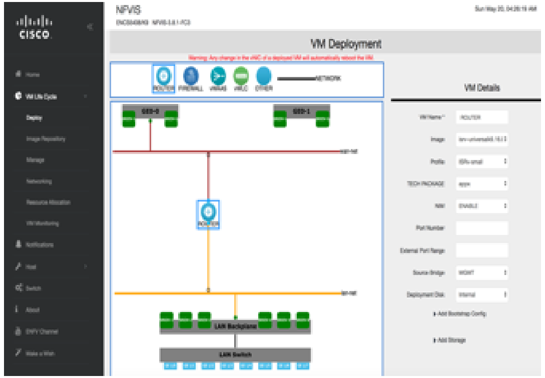
- Multiple VNF profiles target specific performance
- Cisco VNFs will be pinned to respective cores for performance.

Deploying VNFs Using NFVIS GUI

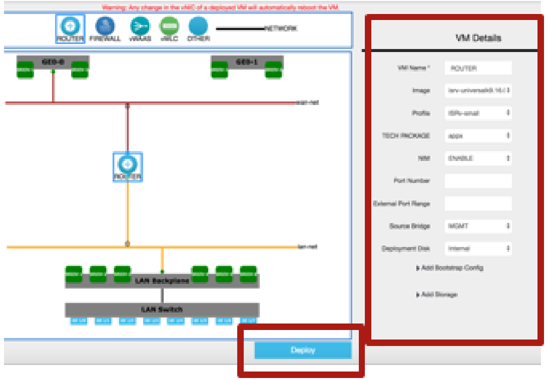
VM Life Cycle -> Deploy



"Draw" the desired topology



Enter VNF properties and Deploy


Warning: Any change in the vNIC of a deployed VM will automatically reboot the VM.
ROUTER
FIREWALL
vWAAS
vWLC
OTHER
NETWORK
GE0-0
GE0-1
wan-net
lan-net
LAN Backplane
LAN Switch

VM Details

VM Name * ROUTER
Image isrv-universalk9.16.(
Profile ISRv-small
TECH PACKAGE appx
NIM ENABLE
Port Number
External Port Range
Source Bridge MGMT
Deployment Disk Internal
▸ Add Bootstrap Config
▸ Add Storage

Deploy

Cloud on-ramp for CoLo

What problem does it solve?

For SDWAN

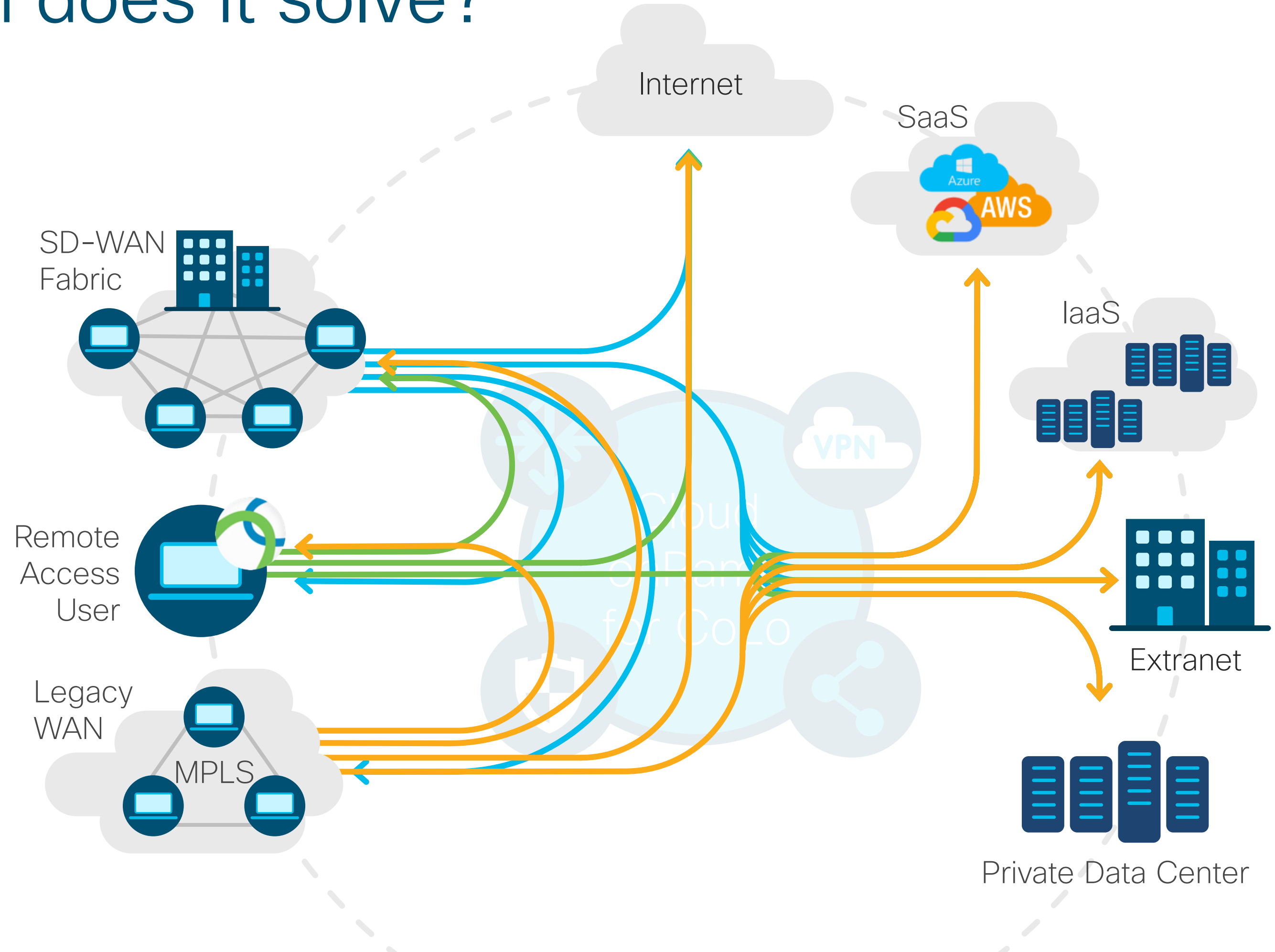
- Easier Migration(s)
- Remote Access VPN integration
- Optimized Cloud/DC Access
- Optimized Extranet Access

For Remote Access Users

- Optimized Cloud Access
- Anchor for IaaS, Extranet and optimized access to Private DC(s)
- Optimized Extranet Access

For Legacy WAN

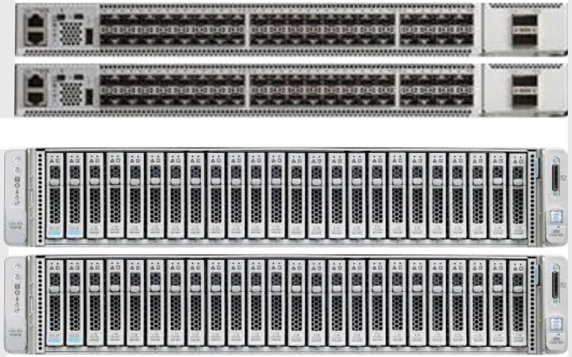
- Remote Access VPN integration
- Optimized Cloud/DC Access
- Optimized Internet Access
- Optimized Extranet Access



Cluster Physical Components

Cisco Catalyst 9500-40 Switches (Quantity: 2)

- Must run IOS-XE v16.9.1 with Network Advantage or greater
- Provides multi-gigabit backplane switching to VNFs, inbound/outbound WAN connectivity and access to Colo management networks
- Operates as one virtual switch (VSS)
- Highly redundant
- Configured via PNP through Colo-Configuration Manager (CCM) on Day0



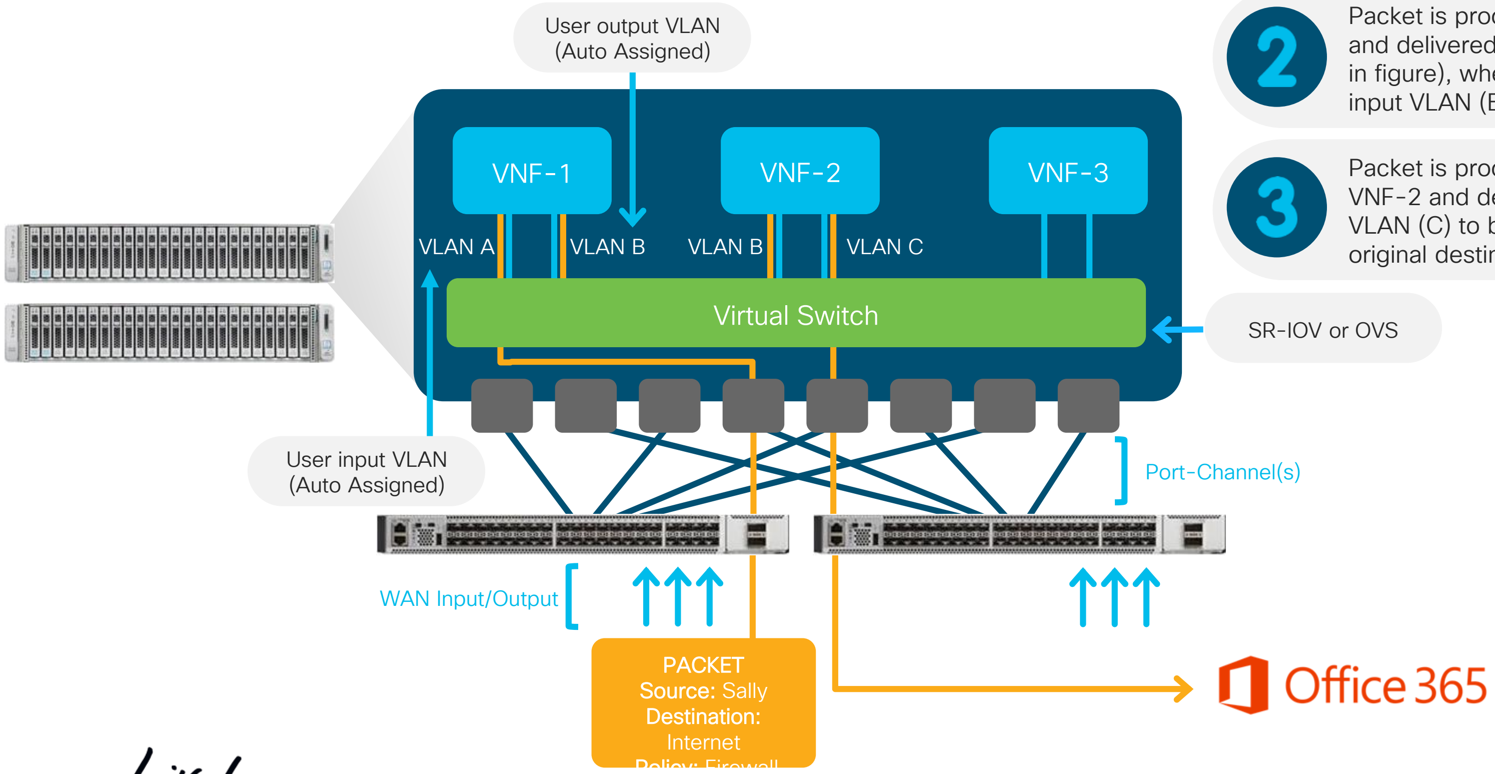
Cisco CSP 5444 Platform (Quantity: 2)

- 44 CPU cores, 192GB of RAM, 4.8TB onboard storage and 8 NICs (10Gb/ps) per chassis
- Runs NFVIS with vDaemon Day0 (Zero Touch Provisioning)
- Must run Cisco NFVIS v3.9.1a or greater
- Runs Colo-Configuration Manager (spawned via vManage after Zero Touch Provisioning)
- Hosts VNF Service Chains (Service Groups) instantiated within vManage

Cisco Cloud onRamp for CoLo Cluster

- Managed via vManage
- Requires vManage v18.4+
- Acts as a pool of resources with which to use to create service-chains
- Provides anchor between all Transports/SPs, Clouds, etc.

VNF Packet Walkthrough



1. Packet/frame delivered to C9500 from WAN on VNF-1 input VLAN ('A' in figure)

2. Packet is processed by VNF-1 and delivered to output VLAN ('B' in figure), where it is routed to input VLAN (B) of VNF-2

3. Packet is processed by VNF-2 and delivered to output VLAN (C) to be routed to its original destination

AppQoE

AppQoE Methodology

1. Detect:

- App Classification
- NBAR2
- SD-AVC

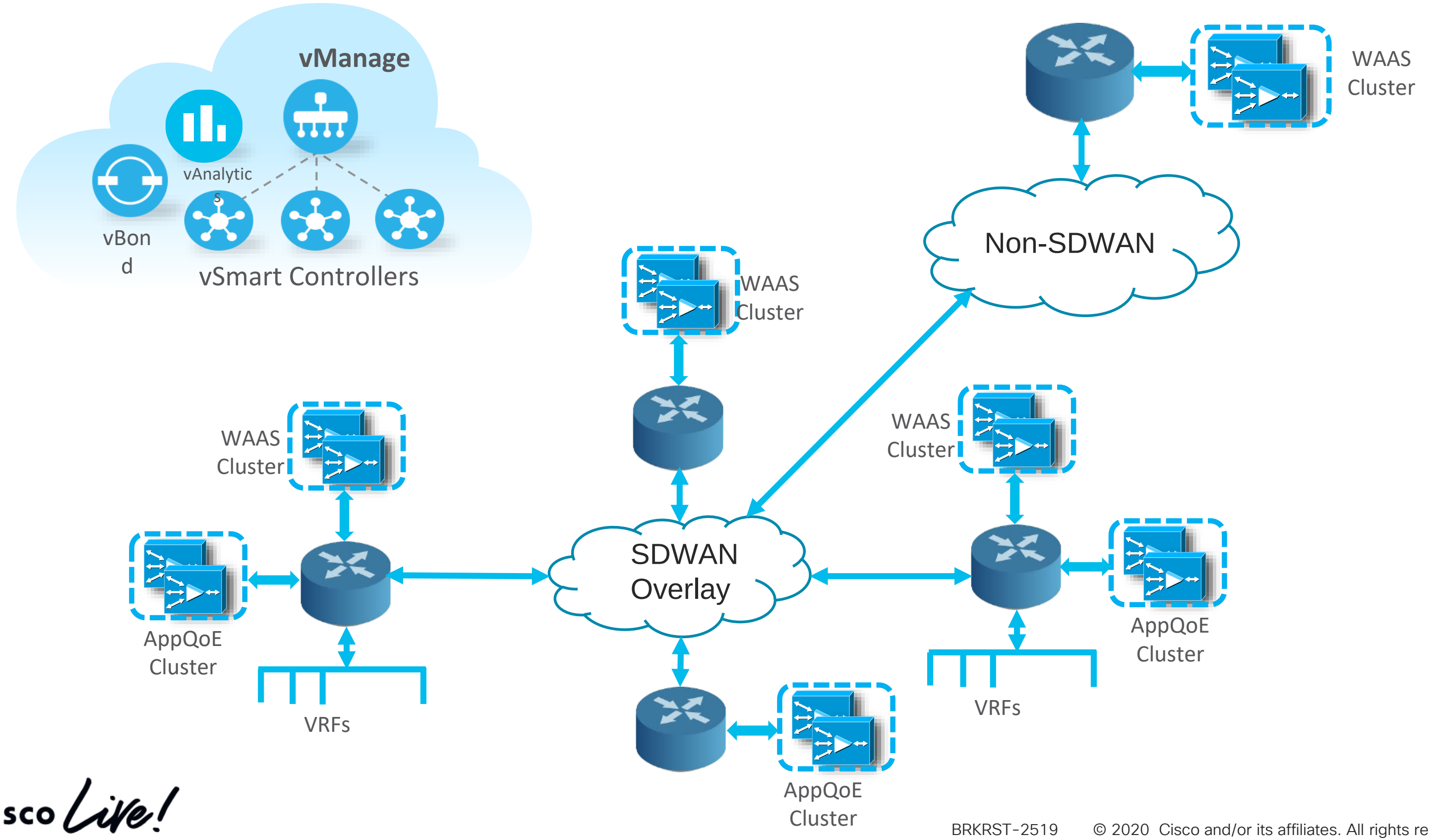
2. Measure:

- BFD
- App-Route Visualization
- Flow Simulation
- HTTP probing

3. Improve:

- App-aware Routing
- Data Policy TE
- FEC / Packet duplication
- QoS
- Compression, Caching
- Cloud OnRamp, DIA
- AppNav, WAAS

SD-WAN and AppQoE, Application acceleration with SD-WAN



App QoE Feature & Device Model Matrix

Main Feature	SubFeature	vEdge 100/Cloud	vEdge 1000/2000	cEdge ISR1000 C1111	cEdge ISR4000 ISR42xx,43xx,44xx	cEdge ASR1000 1001/1002-X/HX	CSR1kv, ISRv ENCS51xx,54xx
Bandwidth Optimization	CACHE	N/A	N/A	N/A	✓ (2H_2020)	N/A	✓ (2H_2020)
	DRE	N/A	N/A	N/A	✓ (2H_2020)	N/A	✓ (2H_2020)
Latency Optimization	TCP OPT	N/A	✓	N/A	✓ (July_2019)	✓ (when?)	✓ (July_2019)
	Session Persistence	N/A	N/A	N/A	✓ (2H_2020)	N/A	✓ (2H_2020)
SaaS Optimization	Cloud on Ramp – O365	✓	✓	✓ (July_2019)	✓ (July_2019)	✓ (July_2019)	✓ (July_2019)
	Cloud on Ramp – Others	✓	✓	✓ (2H_2020)	✓ (2H_2020)	✓ (2H_2020)	✓ (2H_2020)
Link Bonding	FEC	✓	✓	✓ (Apr_2019)	✓ (Apr_2019)	✓ (Apr_2019)	✓ (Apr_2019)
	Packet Duplication	✓	✓	✓ (July_2019)	✓ (July_2019)	✓ (July_2019)	✓ (July_2019)

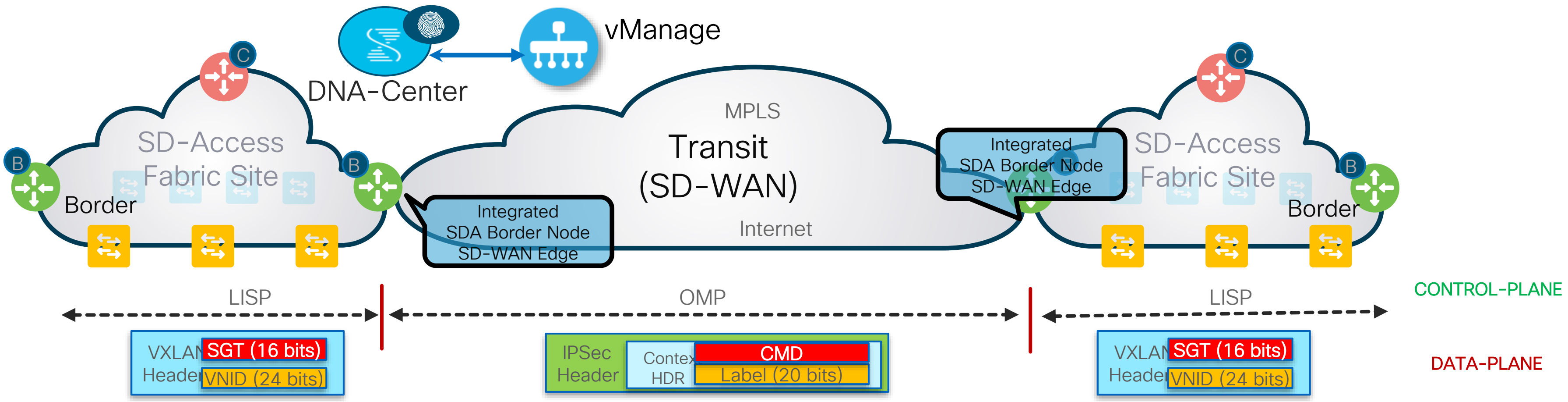
cisco Live!

SD-WAN Innovations across domains

SDA and SD-WAN Integration

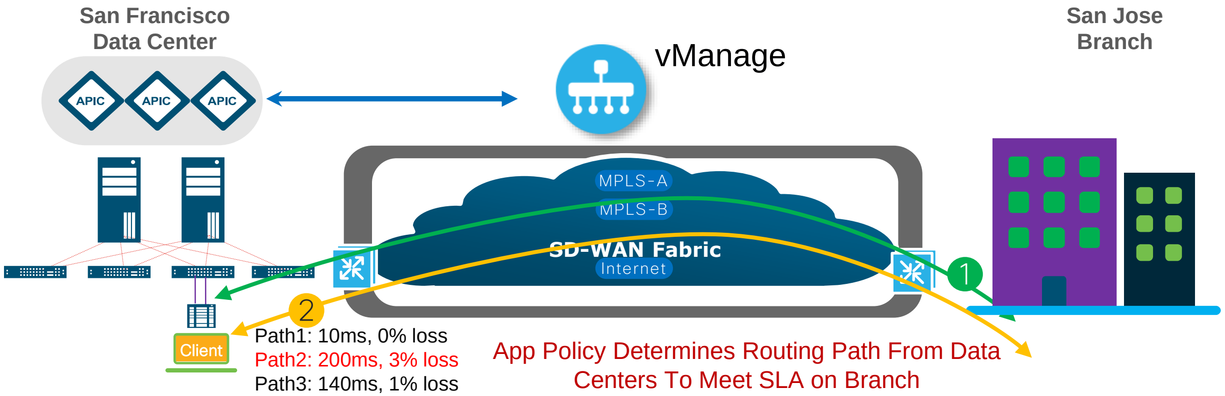
Preserve Identity across SDA fabric sites over SD-WAN

- ISR4K/ASR1K as SD-WAN edge and SDA Border node
- DNAC configures border node functionality via vManage API Integration
- LISP-OMP route redistribution on control path
- Extract and transport SGT across SD-WAN data plane



SD-WAN and ACI Integration

Application SLA exchange between ACI and SD-WAN



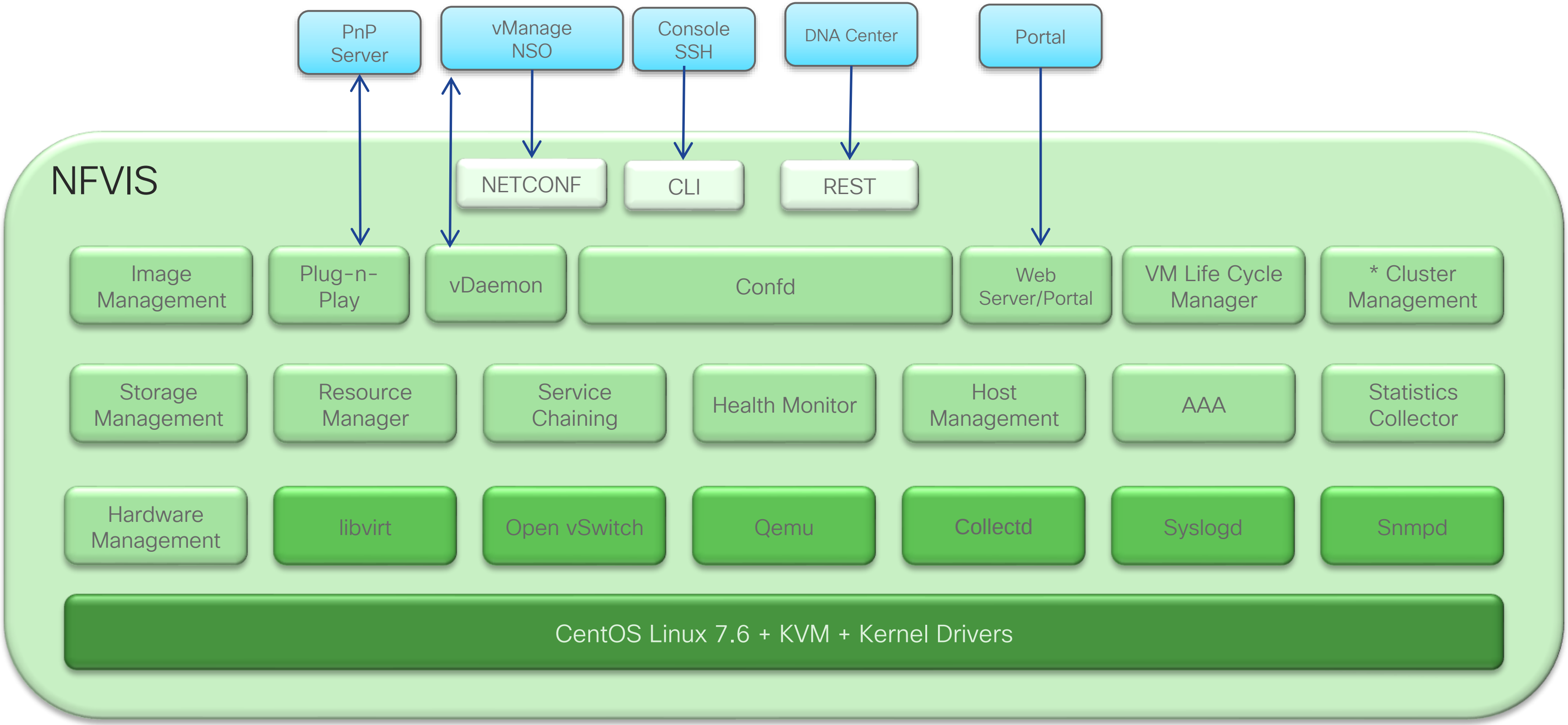
Path1: 10ms, 0% loss
Path2: 200ms, 3% loss
Path3: 140ms, 1% loss

App Policy Determines Routing Path From Data Centers To Meet SLA on Branch

ACI communicates application SLA policies to SD-WAN

NFVIS

NFVIS Architecture Not Just KVM, Power in software



* Roadmap

Enterprise NFV Open Ecosystem

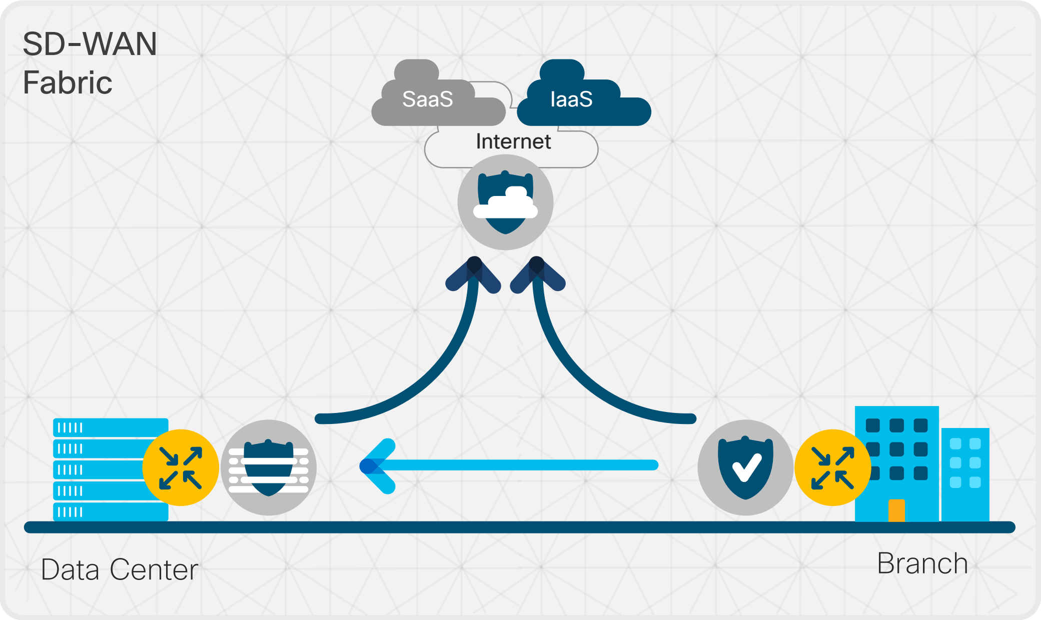
- Customers have flexibility to run third-party VNF of their choosing.
- Third-Party vendors may *choose* to submit their VNF for certification.
- No admission restrictions; third party may be complimentary to Cisco, or competitive. Requirements are the same regardless.
- Irrespective of certification, customers have flexibility to run third-party VNF of their choosing.
- More information: http://cs.co/3nfv

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-functions-virtualization-nfv/nfv-open-ecosystem-qualified-vnf-vendors.pdf

Security

On premise vs.Cloud

Customer challenges



WAN Edge Device

Existing Security Stack in DMZ

Separate Security Appliance

Separate Security Service

ONLY Cloud Security

PRO: Consistent user and device protection in all locations and scales on-demand

CON: Lacks visibility and control over internal traffic and threats

ONLY On-Prem Security

PRO: Visibility into all traffic and protects against internal and external threats

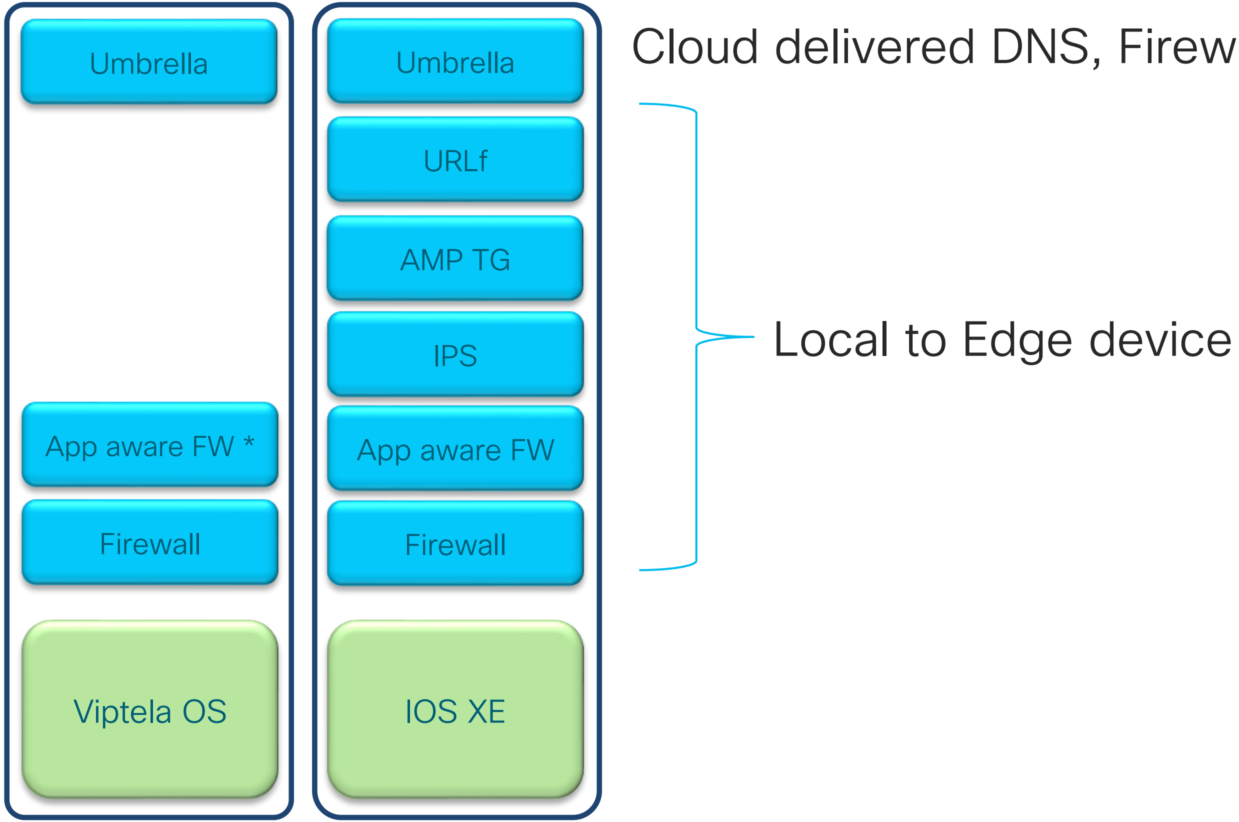
CON: Decrypting traffic for malware detection increases edge device footprint

Cloud AND On-Prem Security

PRO: Best balance of security and user experience for direct internet access

CON: Added complexity through security policy separation

Security capabilities accross platforms



* QOSMOS

Secure Internet Gateway Considerations

SD-WAN (Viptela) Integration

Secure direct internet access (DIA) locations

Today: Send DNS requests to Umbrella

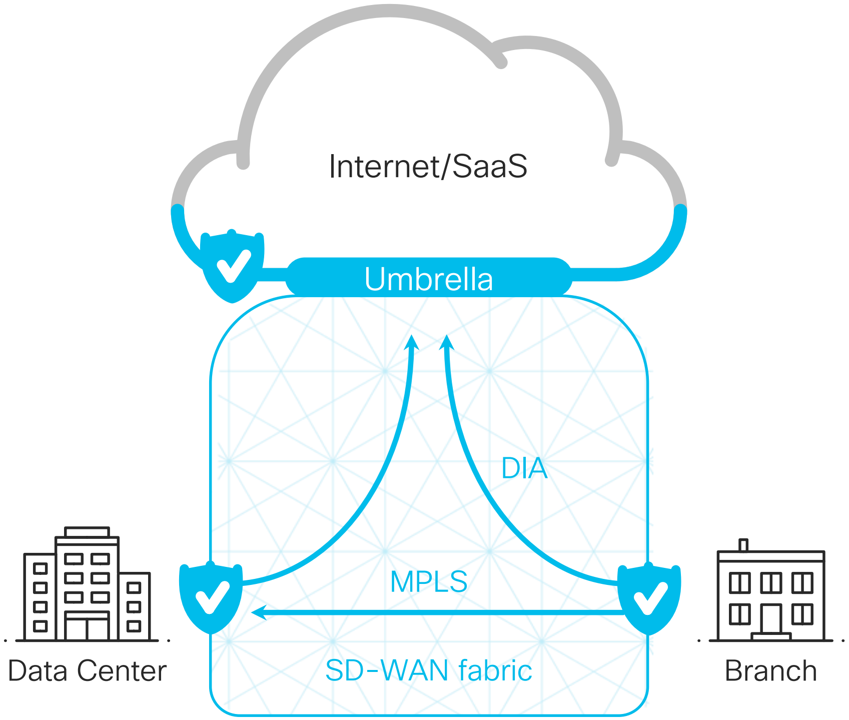
- Deploy to hundreds of devices in minutes, within a single dashboard
- Gain DNS-layer protection at branch office locations
- Create policies and view reports on a per-VPN basis

Today: Deploy tunnels to forward DIA traffic

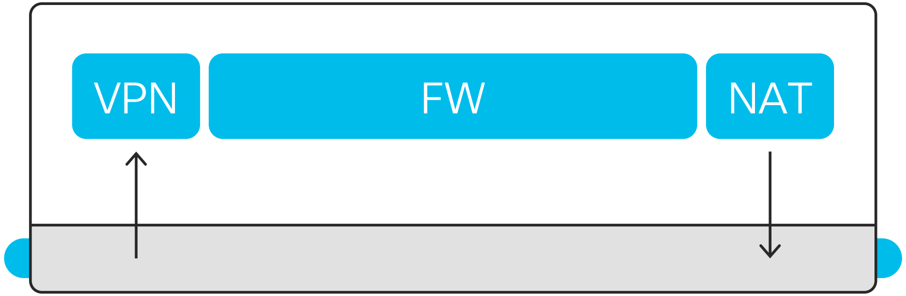
- Apply additional inspection/security (firewall, proxy)

Next: Automated provisioning to Umbrella

- Scale security with future SaaS/web traffic growth via minimal-touch provisioning in single dashboard



Firewall Considerations



VPN Capacity :

- 150 Mbps
  - 90% of branch locations using Viptela are below 100 Mbps
- Multiple tunnels increase throughput

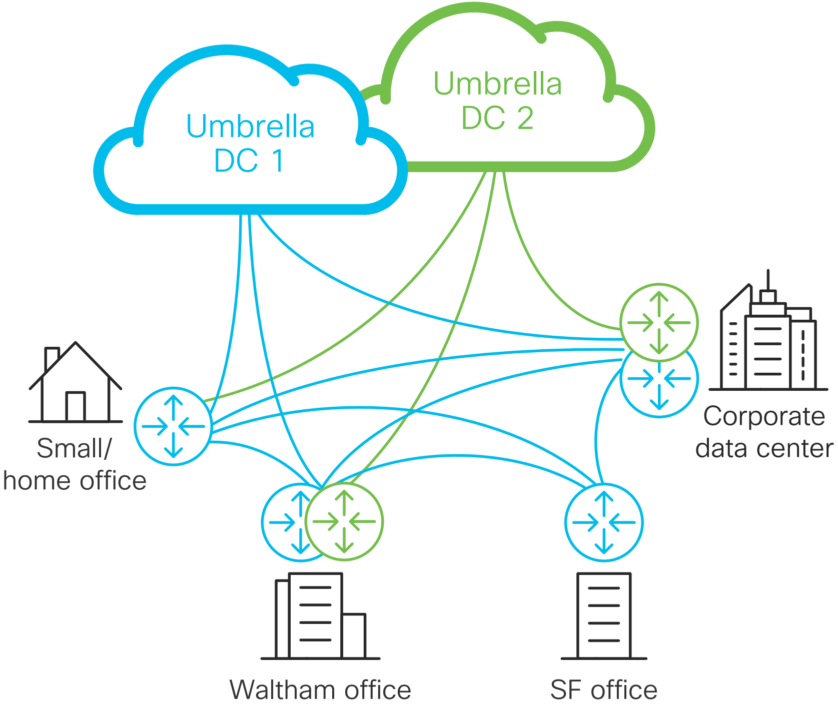
Firewall :

- IPv4
- Outbound firewall
- Expects RFC 1918 source IP-s
- Cisco IP Adresses

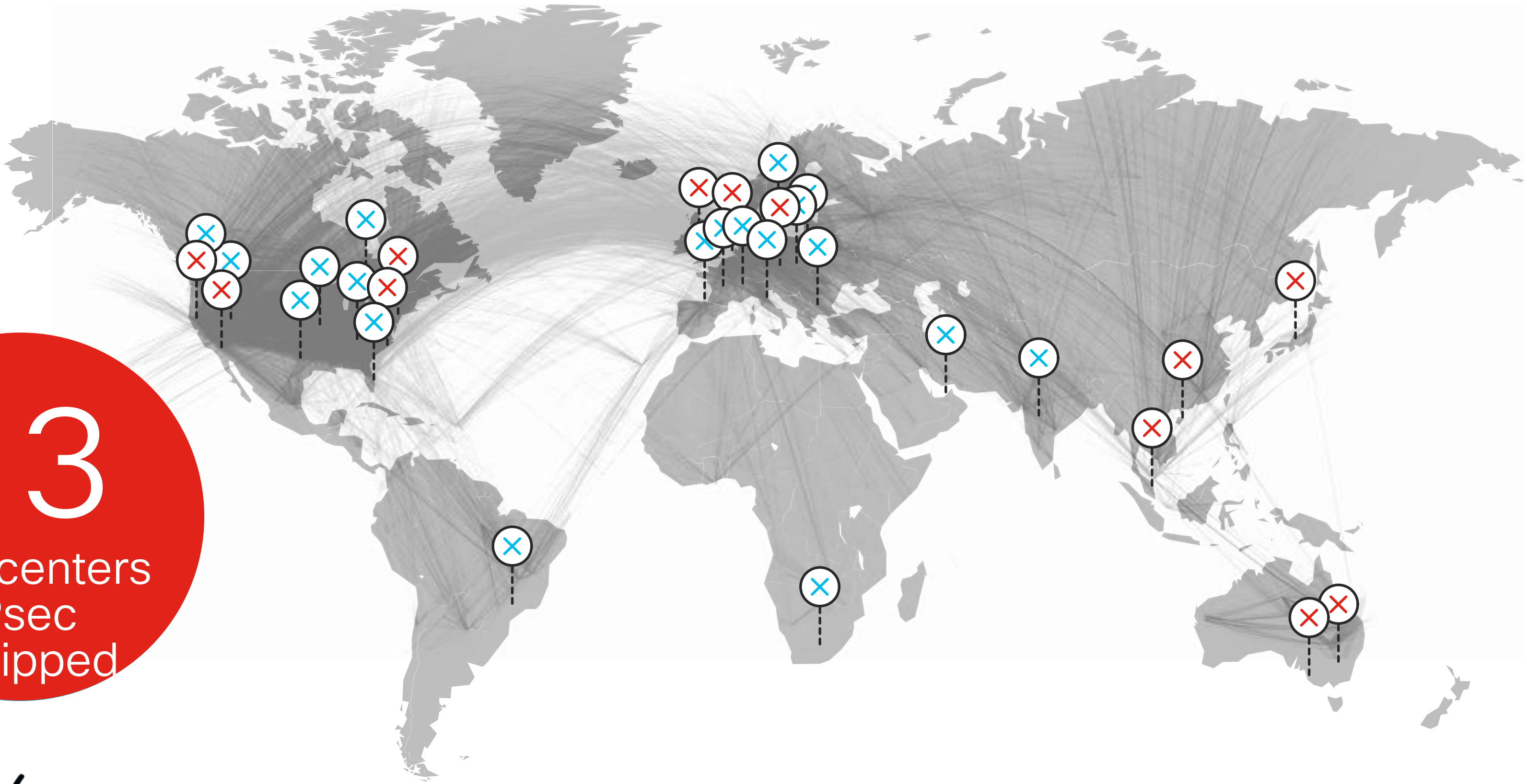
High Availability Considerations

- **Device, Path, Cloud Data Center**

- There are situations when the Umbrella service itself experiences issues
- In this case, there are multiple instances in each DC to handle customer traffic
- If the entire DC has issues, it is taken out automatically and another DC in the same region starts serving the old DC's IP address
- Tunnels moves from old DC to a new DC automatically



DC Worldwide Locations



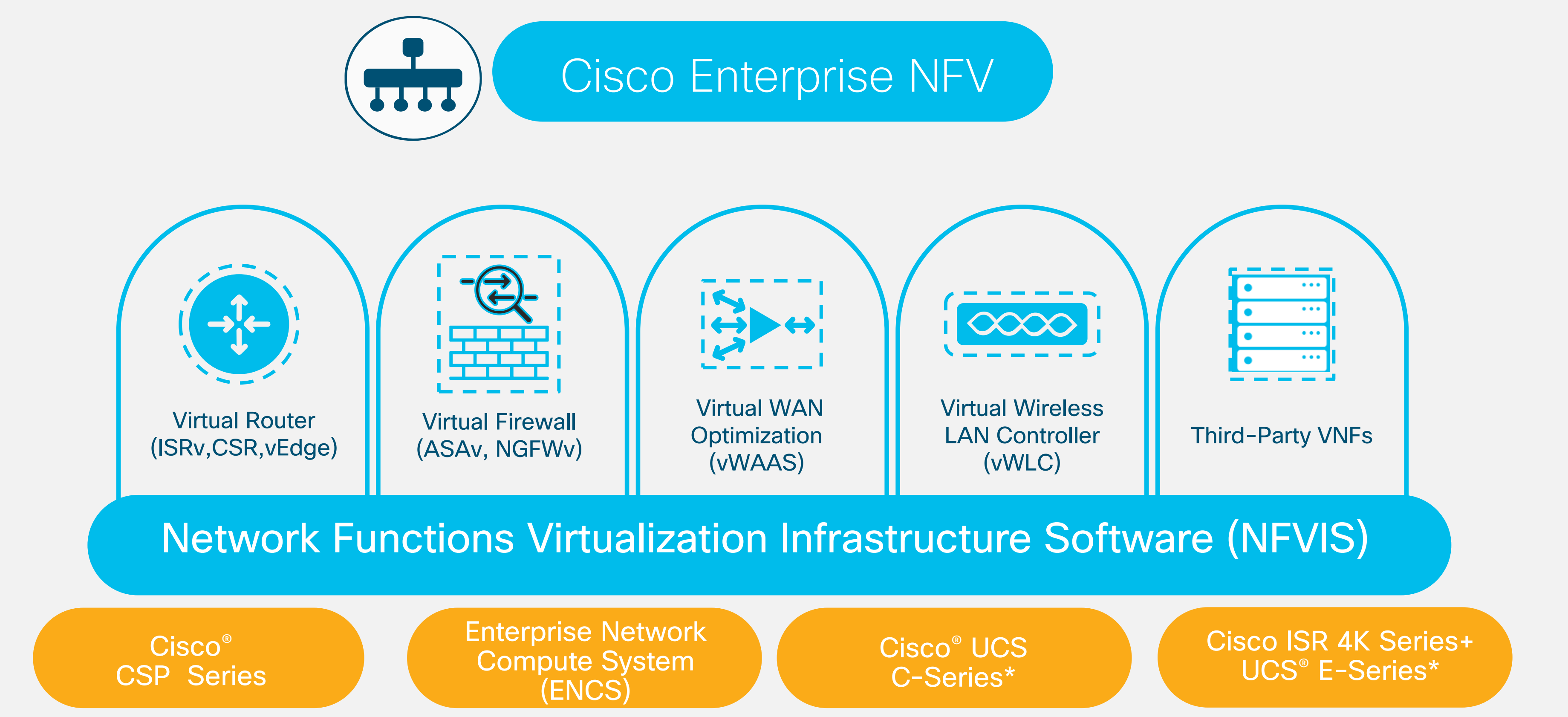
13

data centers IPsec equipped

Configure

Policies & Best Practices
Management tools

Automated Service Stitching for any VNFs



Cisco Enterprise NFV

Virtual Router (ISRv,CSR,vEdge)

Virtual Firewall (ASAv, NGFWv)

Virtual WAN Optimization (vWAAS)

Virtual Wireless LAN Controller (vWLC)

Third-Party VNFs

Network Functions Virtualization Infrastructure Software (NFVIS)

Cisco® CSP Series

Enterprise Network Compute System (ENCS)

Cisco® UCS C-Series*

Cisco ISR 4K Series+ UCS® E-Series*

* In roadmap with vManage Orchestration

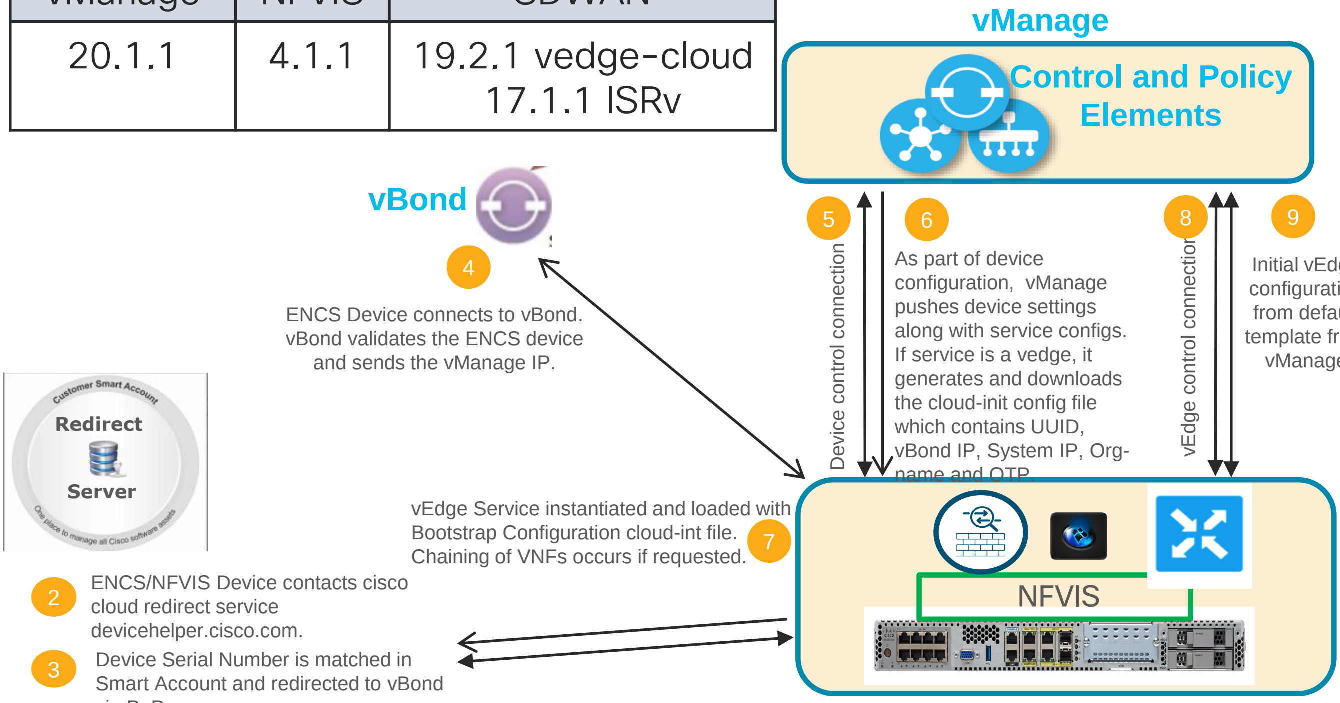
cisco Live!

vManage NFV Automation workflow for SDWAN

Mar 2020 Target

Minimum Releases Required		
vManage	NFVIS	SDWAN
20.1.1	4.1.1	19.2.1 vedge-cloud 17.1.1 ISRv

1 Define ENCS device profile with services (vEdge Router) through ND workflow
Upload Serial File from Viptela Operations. Associate Template to vEdge UUID.



vManage
Control and Policy Elements
vBond
Customer Smart Account
Redirect
Server
One place to manage all Cisco software assets
Device control connection
vEdge control connection
NFVIS

2 ENCS/NFVIS Device contacts cisco cloud redirect service devicehelper.cisco.com.

3 Device Serial Number is matched in Smart Account and redirected to vBond via PnP

4 ENCS Device connects to vBond. vBond validates the ENCS device and sends the vManage IP.

5 Device control connection

6 As part of device configuration, vManage pushes device settings along with service configs. If service is a vedge, it generates and downloads the cloud-init config file which contains UUID, vBond IP, System IP, Org-name and OTP.

7 vEdge Service instantiated and loaded with Bootstrap Configuration cloud-int file. Chaining of VNFs occurs if requested.

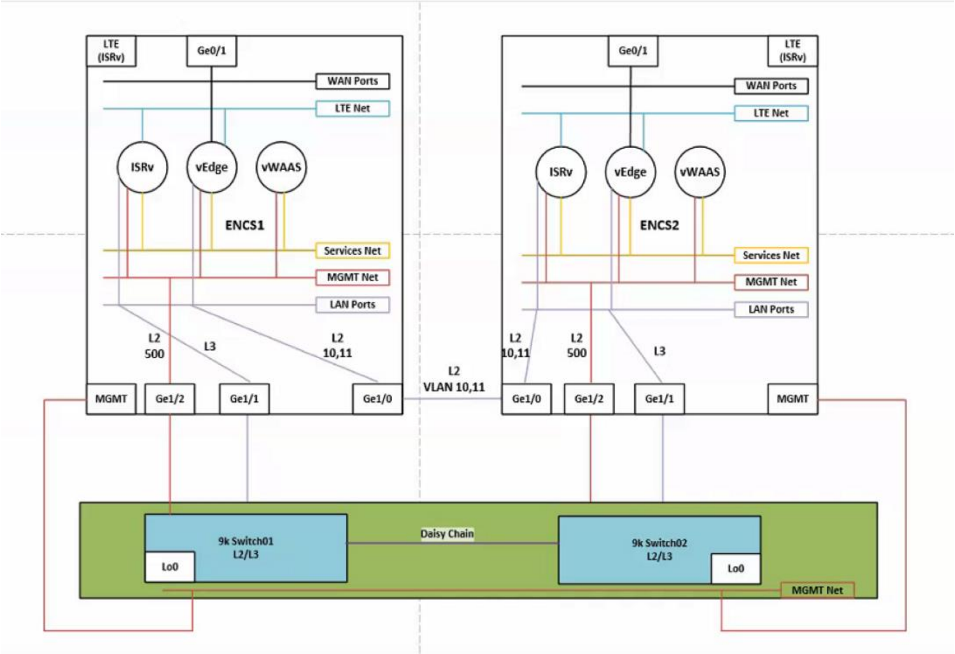
8 vEdge control connection

9 Initial vEdge configuration from default template from vManage

vManage Capabilities for NFV

Image Repository
Network Design
VNF design
Deploy
Upgrade/Maintenance
Platform and VNF Monitoring

Typical vBranch Deployment



Performance consideration – Best practice

Individual performance of a VNF depends on

- The underlying platform, the number of cores and the type and frequency of the processor used
- The resources available for the VNF
- How the VM connects to the physical NICS – PCI Passthrough, SR-IOV, virtIO
- Finally The VNF itself. VNF must also be optimized to run in a virtual environment

In case of a Multi-VNF environment, the net chained VNF performance also depends on

- The weakest-link VNF
- Use of virtual switches to copy packets from ingress to egress vNICs

Best Practice :

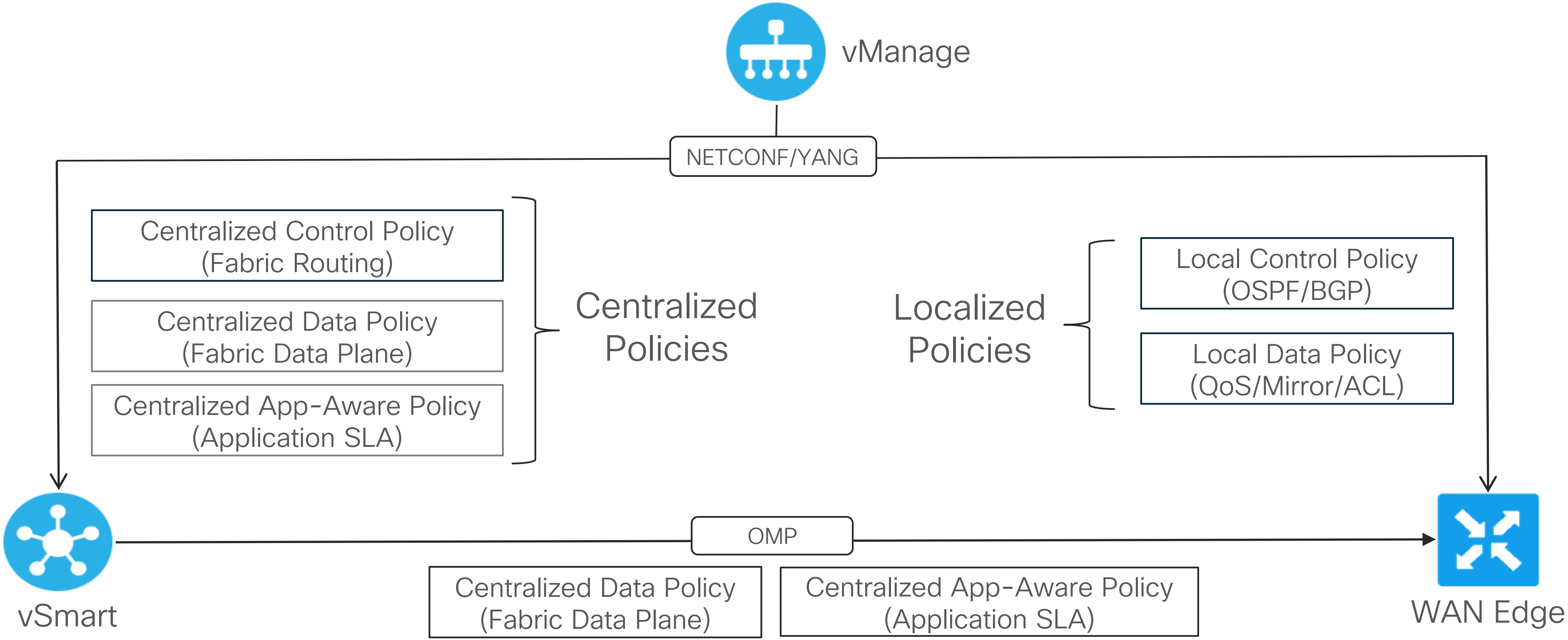
Dedicate CPU and utilize SRIOV for most optimal performance where possible.
Note : VNF needs to support the specific SR-IOV driver. ISRv, Cisco SDWAN have the required drivers for optimal performance in ENCS.

If SRIOV support is not available in the VNF, enable DPDK for OVS networking in NFVIS.

Cisco SD-WAN

Policies

Policy Framework



vManage

NETCONF/YANG

Centralized Control Policy (Fabric Routing)

Centralized Data Policy (Fabric Data Plane)

Centralized App-Aware Policy (Application SLA)

Centralized Policies

Localized Policies

Local Control Policy (OSPF/BGP)

Local Data Policy (QoS/Mirror/ACL)

vSmart

OMP

Centralized Data Policy (Fabric Data Plane)

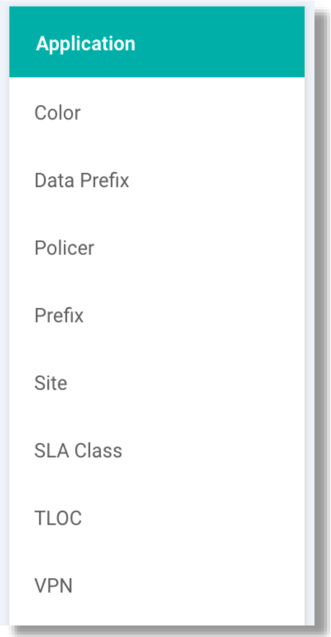
Centralized App-Aware Policy (Application SLA)

WAN Edge

Construction of SD-WAN Policies

- Policy Building Blocks

Lists



Application

Color

Data Prefix

Policer

Prefix

Site

SLA Class

TLOC

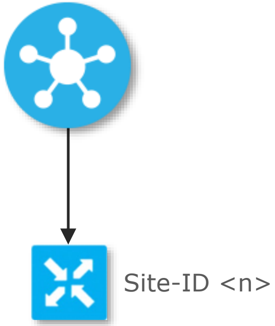
VPN

Policy

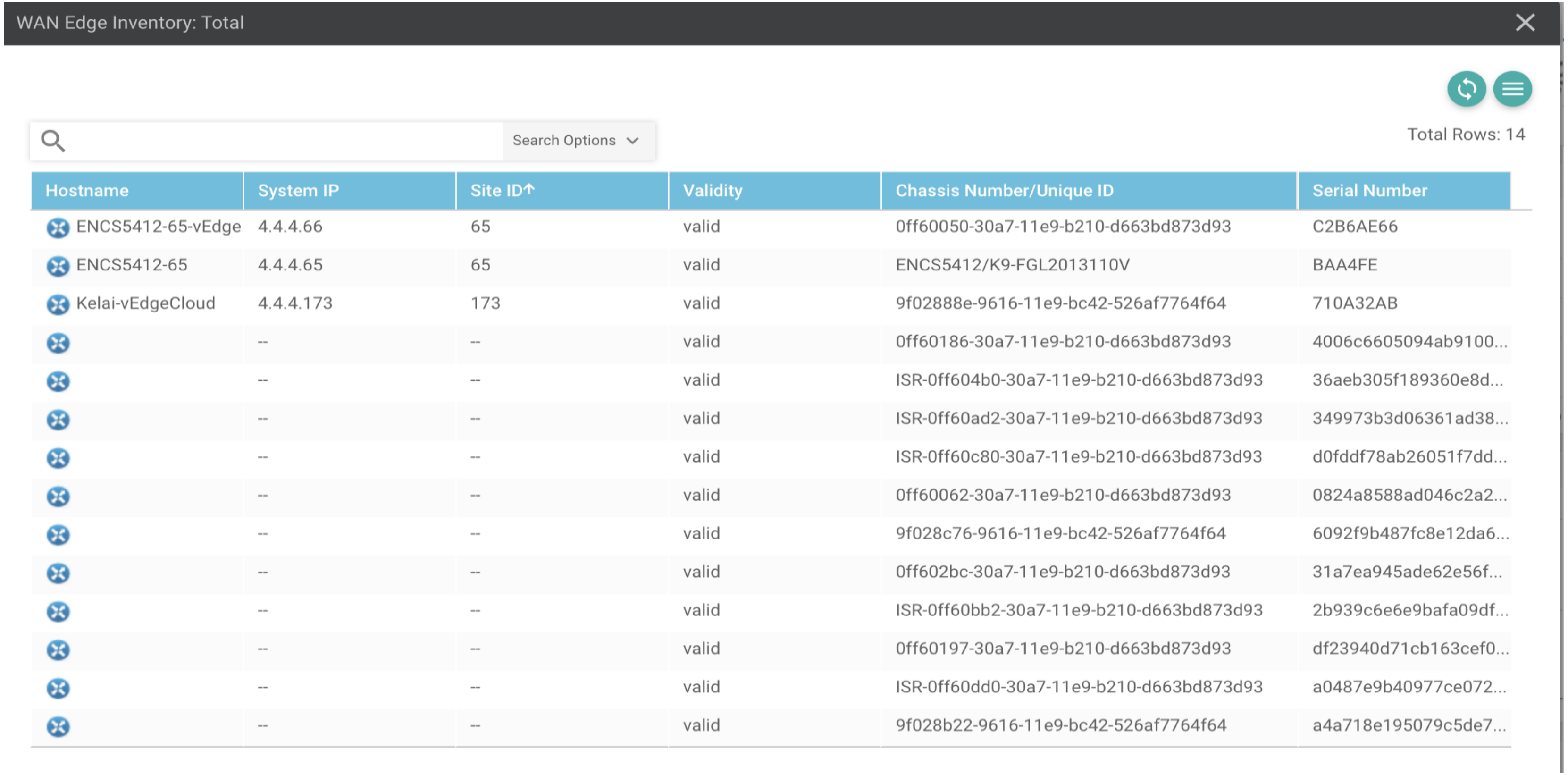
```
Policy Type

Policy Sequence 1
Match <route | tloc | Application>
Action <Accept | Reject | set >

Policy Sequence 2
Match <route | tloc | Application>
Action <Accept | Reject | set >

Default Action
<Accept | Reject>
```

Apply Policy

```
Site-List

Policy <type> <name>
Direction (if applicable)
```



From VA/SA to the inventory

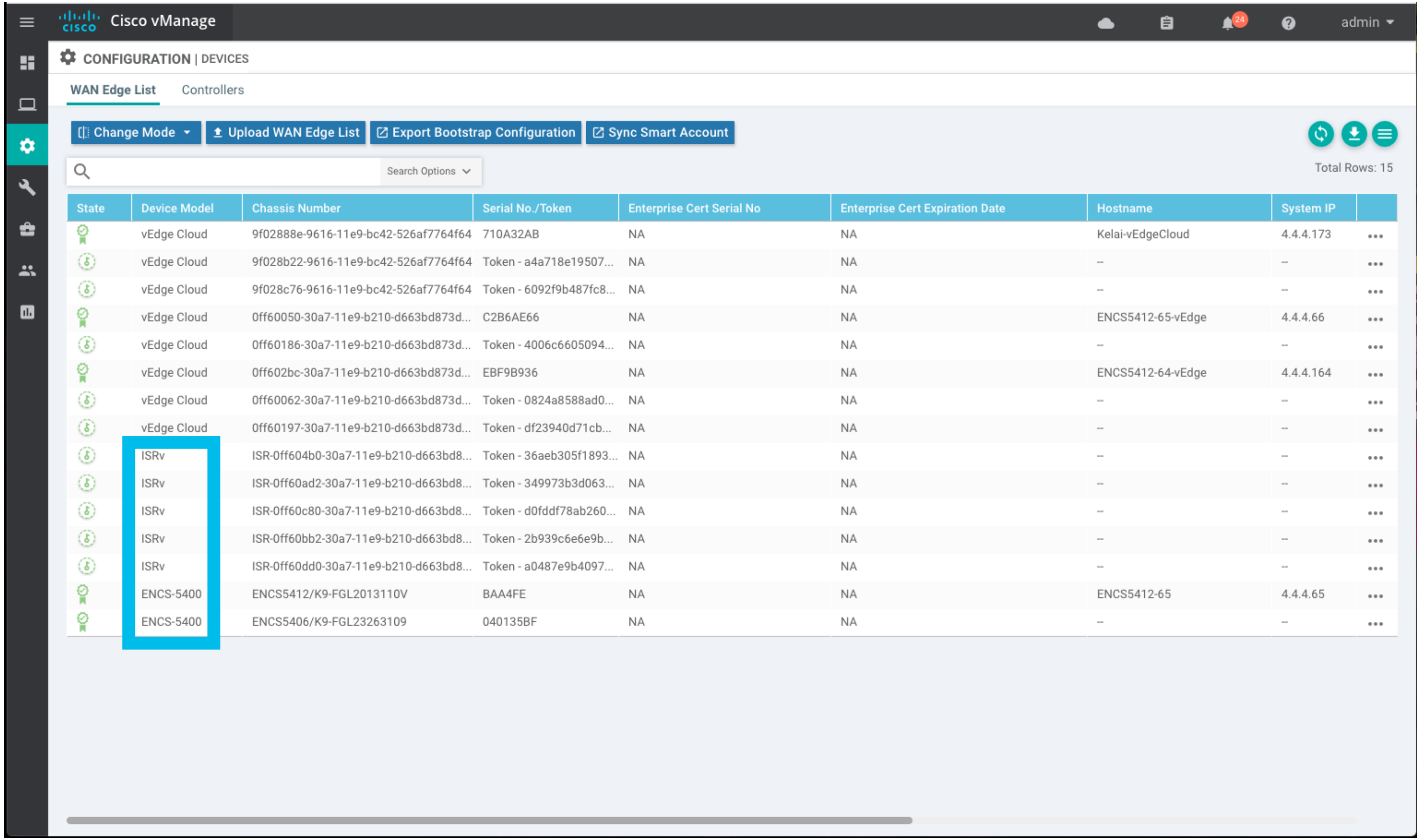


WAN Edge Inventory: Total

Total Rows: 14

Hostname	System IP	Site ID↑	Validity	Chassis Number/Unique ID	Serial Number
ENCS5412-65-vEdge	4.4.4.66	65	valid	0ff60050-30a7-11e9-b210-d663bd873d93	C2B6AE66
ENCS5412-65	4.4.4.65	65	valid	ENCS5412/K9-FGL2013110V	BAA4FE
Kelai-vEdgeCloud	4.4.4.173	173	valid	9f02888e-9616-11e9-bc42-526af7764f64	710A32AB
	--	--	valid	0ff60186-30a7-11e9-b210-d663bd873d93	4006c6605094ab9100...
	--	--	valid	ISR-0ff604b0-30a7-11e9-b210-d663bd873d93	36aeb305f189360e8d...
	--	--	valid	ISR-0ff60ad2-30a7-11e9-b210-d663bd873d93	349973b3d06361ad38...
	--	--	valid	ISR-0ff60c80-30a7-11e9-b210-d663bd873d93	d0fddf78ab26051f7dd...
	--	--	valid	0ff60062-30a7-11e9-b210-d663bd873d93	0824a8588ad046c2a2...
	--	--	valid	9f028c76-9616-11e9-bc42-526af7764f64	6092f9b487fc8e12da6...
	--	--	valid	0ff602bc-30a7-11e9-b210-d663bd873d93	31a7ea945ade62e56f...
	--	--	valid	ISR-0ff60bb2-30a7-11e9-b210-d663bd873d93	2b939c6e6e9bafa09df...
	--	--	valid	0ff60197-30a7-11e9-b210-d663bd873d93	df23940d71cb163cef0...
	--	--	valid	ISR-0ff60dd0-30a7-11e9-b210-d663bd873d93	a0487e9b40977ce072...
	--	--	valid	9f028b22-9616-11e9-bc42-526af7764f64	a4a718e195079c5de7...

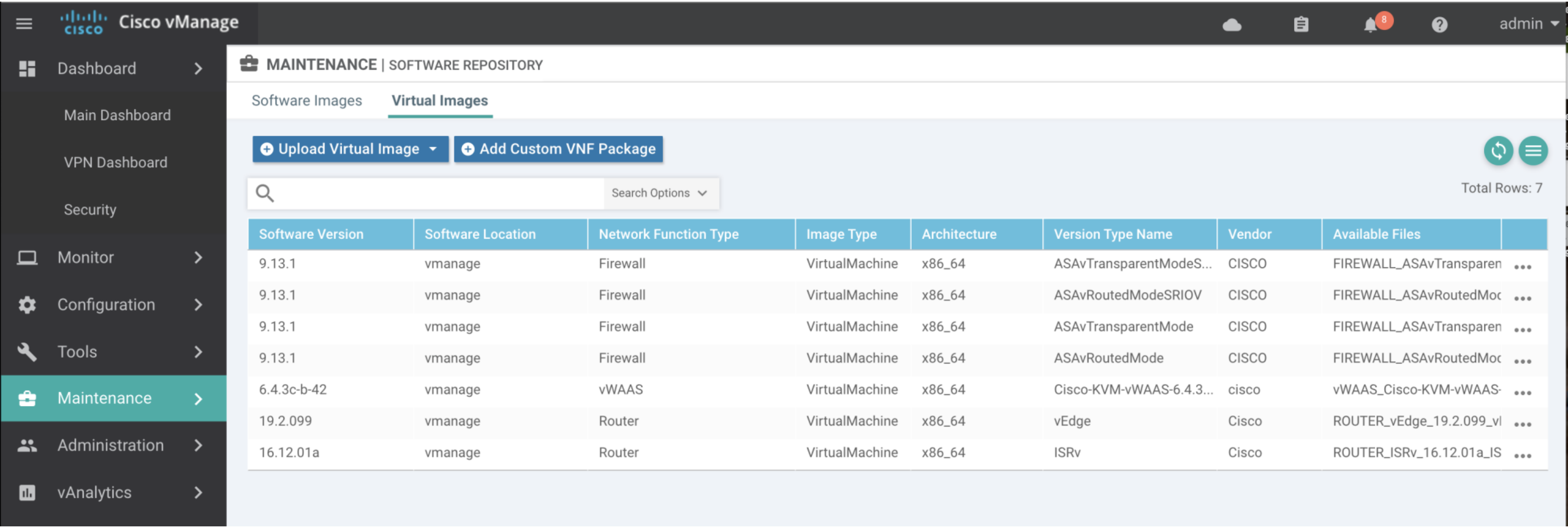
ENCS, ISRv integration provisioning with vManage



Total Rows: 15

State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Enterprise Cert Expiration Date	Hostname	System IP	
✓	vEdge Cloud	9f02888e-9616-11e9-bc42-526af7764f64	710A32AB	NA	NA	Kelai-vEdgeCloud	4.4.4.173	•••
○	vEdge Cloud	9f028b22-9616-11e9-bc42-526af7764f64	Token - a4a718e19507...	NA	NA	--	--	•••
○	vEdge Cloud	9f028c76-9616-11e9-bc42-526af7764f64	Token - 6092f9b487fc8...	NA	NA	--	--	•••
✓	vEdge Cloud	0ff60050-30a7-11e9-b210-d663bd873d...	C2B6AE66	NA	NA	ENCS5412-65-vEdge	4.4.4.66	•••
○	vEdge Cloud	0ff60186-30a7-11e9-b210-d663bd873d...	Token - 4006c6605094...	NA	NA	--	--	•••
✓	vEdge Cloud	0ff602bc-30a7-11e9-b210-d663bd873d...	EBF9B936	NA	NA	ENCS5412-64-vEdge	4.4.4.164	•••
○	vEdge Cloud	0ff60062-30a7-11e9-b210-d663bd873d...	Token - 0824a8588ad0...	NA	NA	--	--	•••
○	vEdge Cloud	0ff60197-30a7-11e9-b210-d663bd873d...	Token - df23940d71cb...	NA	NA	--	--	•••
○	ISRv	ISR-0ff604b0-30a7-11e9-b210-d663bd8...	Token - 36aeb305f1893...	NA	NA	--	--	•••
○	ISRv	ISR-0ff60ad2-30a7-11e9-b210-d663bd8...	Token - 349973b3d063...	NA	NA	--	--	•••
○	ISRv	ISR-0ff60c80-30a7-11e9-b210-d663bd8...	Token - d0fddf78ab260...	NA	NA	--	--	•••
○	ISRv	ISR-0ff60bb2-30a7-11e9-b210-d663bd8...	Token - 2b939c6e6e9b...	NA	NA	--	--	•••
○	ISRv	ISR-0ff60dd0-30a7-11e9-b210-d663bd8...	Token - a0487e9b4097...	NA	NA	--	--	•••
✓	ENCS-5400	ENCS5412/K9-FGL2013110V	BAA4FE	NA	NA	ENCS5412-65	4.4.4.65	•••
✓	ENCS-5400	ENCS5406/K9-FGL23263109	040135BF	NA	NA	--	--	•••

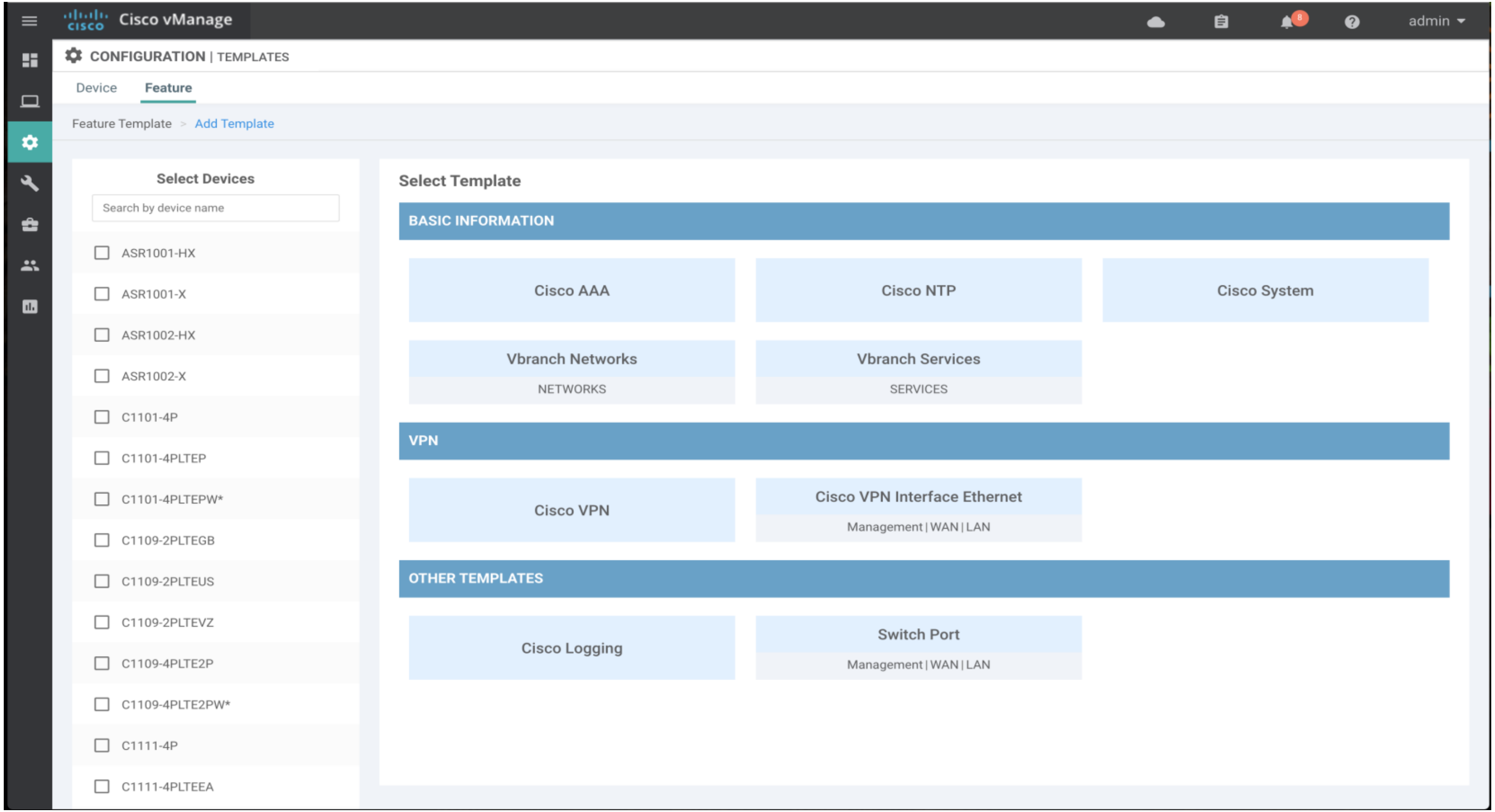
Uploading the Virtual Images



Total Rows: 7

Software Version	Software Location	Network Function Type	Image Type	Architecture	Version Type Name	Vendor	Available Files	
9.13.1	vmanage	Firewall	VirtualMachine	x86_64	ASAvTransparentModeS...	CISCO	FIREWALL_ASAvTransparen	•••
9.13.1	vmanage	Firewall	VirtualMachine	x86_64	ASAvRoutedModeSRIOV	CISCO	FIREWALL_ASAvRoutedMo	•••
9.13.1	vmanage	Firewall	VirtualMachine	x86_64	ASAvTransparentMode	CISCO	FIREWALL_ASAvTransparen	•••
9.13.1	vmanage	Firewall	VirtualMachine	x86_64	ASAvRoutedMode	CISCO	FIREWALL_ASAvRoutedMo	•••
6.4.3c-b-42	vmanage	vWAAS	VirtualMachine	x86_64	Cisco-KVM-vWAAS-6.4.3...	cisco	vWAAS_Cisco-KVM-vWAAS-	•••
19.2.099	vmanage	Router	VirtualMachine	x86_64	vEdge	Cisco	ROUTER_vEdge_19.2.099_vi	•••
16.12.01a	vmanage	Router	VirtualMachine	x86_64	ISRv	Cisco	ROUTER_ISRv_16.12.01a_IS	•••

Create or use existing features



Select Devices

Search by device name

□ ASR1001-HX
□ ASR1001-X
□ ASR1002-HX
□ ASR1002-X
□ C1101-4P
□ C1101-4PLTEP
□ C1101-4PLTEPW*
□ C1109-2PLTEGB
□ C1109-2PLTEUS
□ C1109-2PLTEVZ
□ C1109-4PLTE2P
□ C1109-4PLTE2PW*
□ C1111-4P
□ C1111-4PLTEEA

Select Template

BASIC INFORMATION

- Cisco AAA
- Cisco NTP
- Cisco System
- Vbranch Networks — NETWORKS
- Vbranch Services — SERVICES

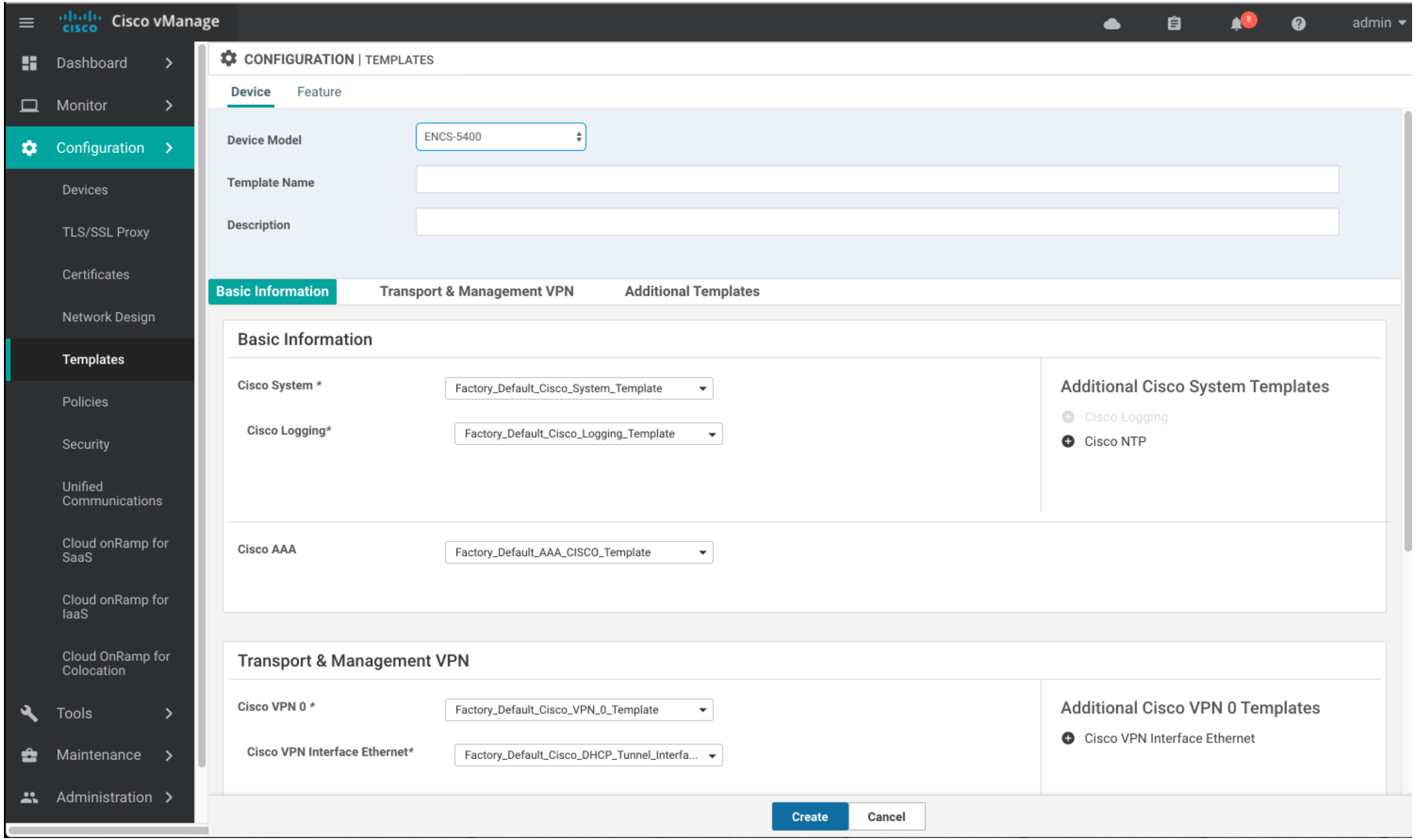
VPN

- Cisco VPN
- Cisco VPN Interface Ethernet — Management | WAN | LAN

OTHER TEMPLATES

- Cisco Logging
- Switch Port — Management | WAN | LAN

Create the Device Template



Device Model: ENCS-5400

Template Name:

Description:

Basic Information

Cisco System *: Factory_Default_Cisco_System_Template

Cisco Logging*: Factory_Default_Cisco_Logging_Template

Cisco AAA: Factory_Default_AAA_CISCO_Template

Additional Cisco System Templates
- Cisco Logging
- Cisco NTP

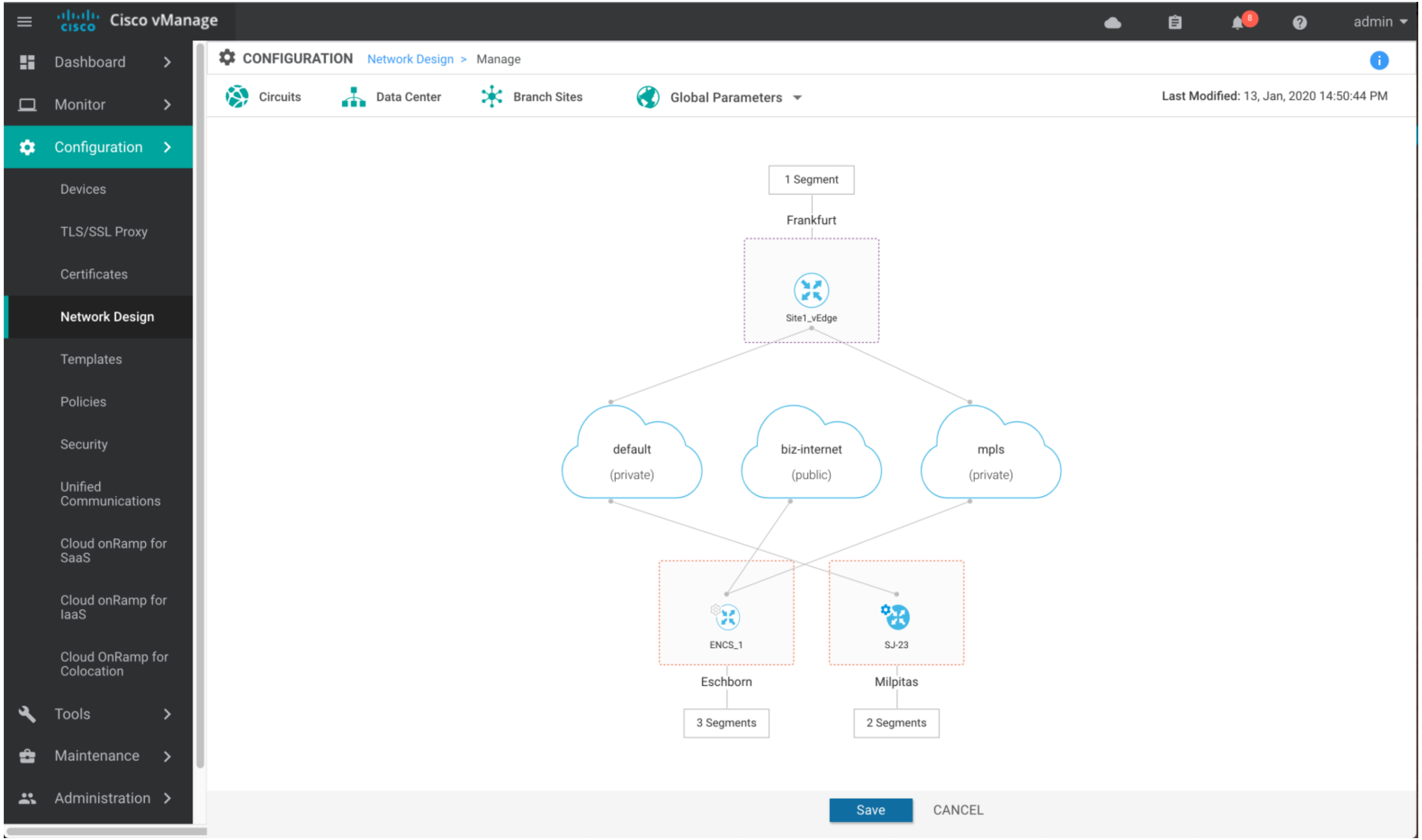
Transport & Management VPN

Cisco VPN 0 *: Factory_Default_Cisco_VPN_0_Template

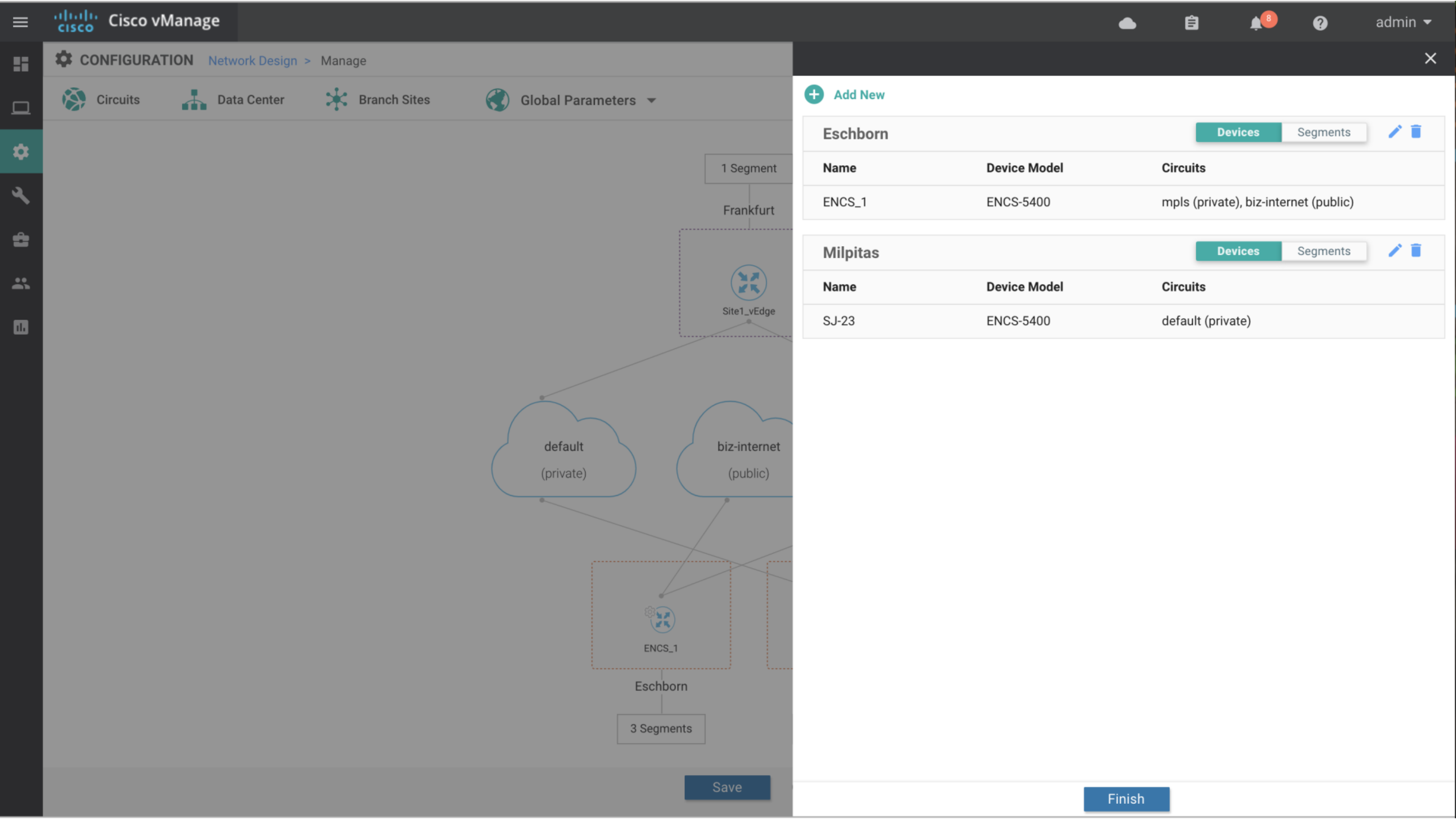
Cisco VPN Interface Ethernet*: Factory_Default_Cisco_DHCP_Tunnel_Interfa...

Additional Cisco VPN 0 Templates
- Cisco VPN Interface Ethernet

Add the device to the topology



Last Modified: 13, Jan, 2020 14:50:44 PM

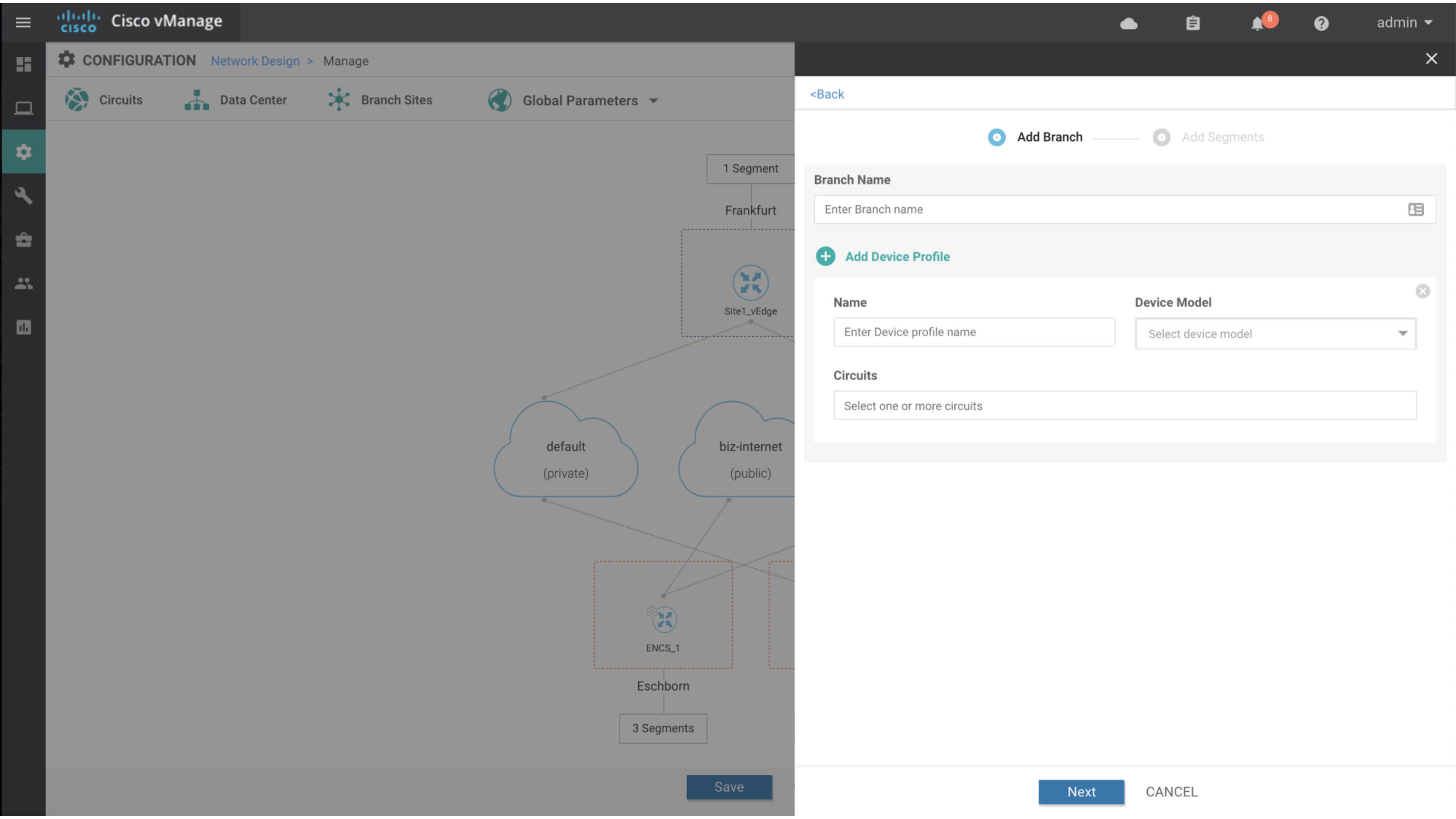


Eschborn

Name	Device Model	Circuits
ENCS_1	ENCS-5400	mpls (private), biz-internet (public)

Milpitas

Name	Device Model	Circuits
SJ-23	ENCS-5400	default (private)



Branch Name

Enter Branch name

Name

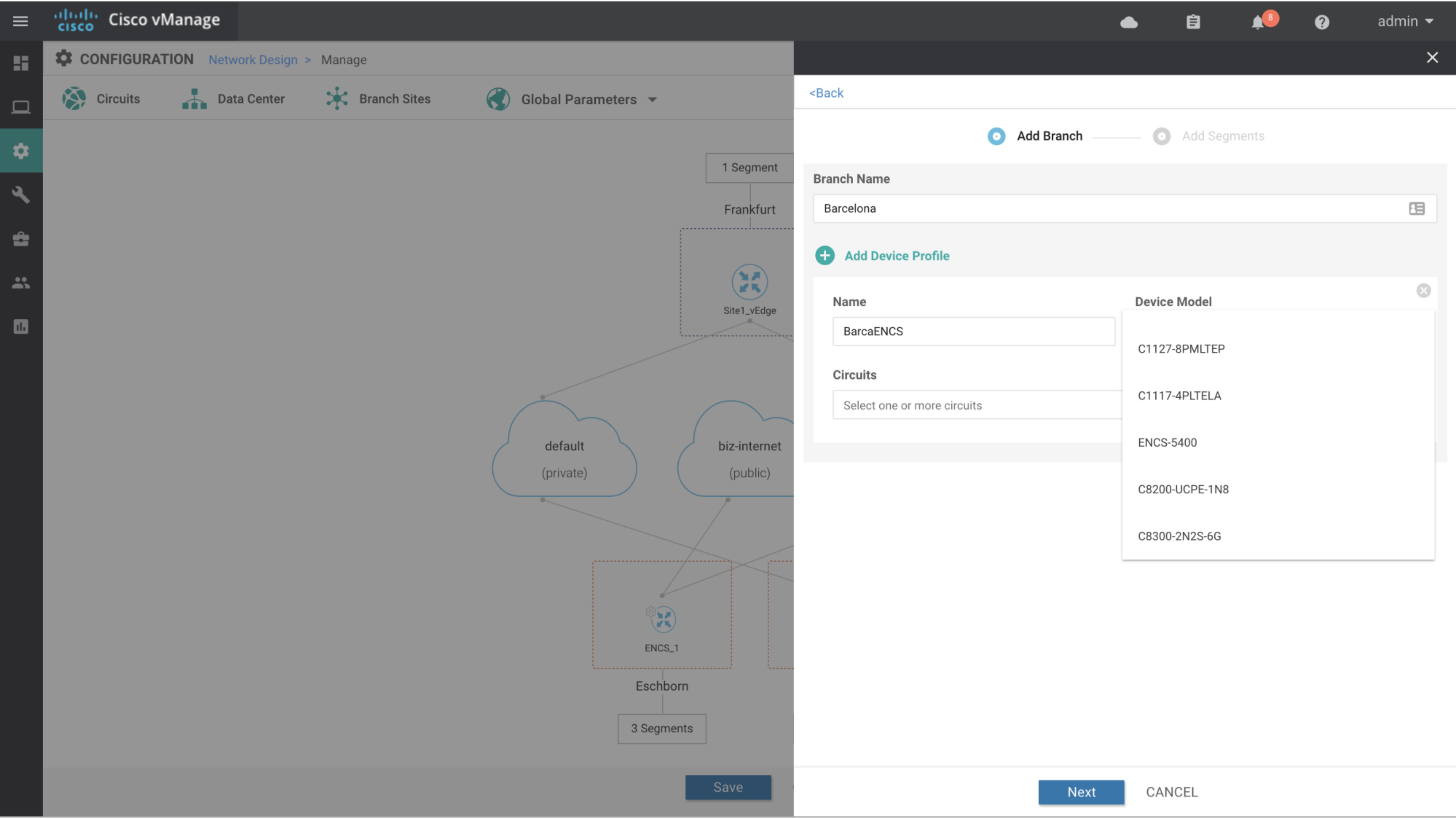
Enter Device profile name

Device Model

Select device model

Circuits

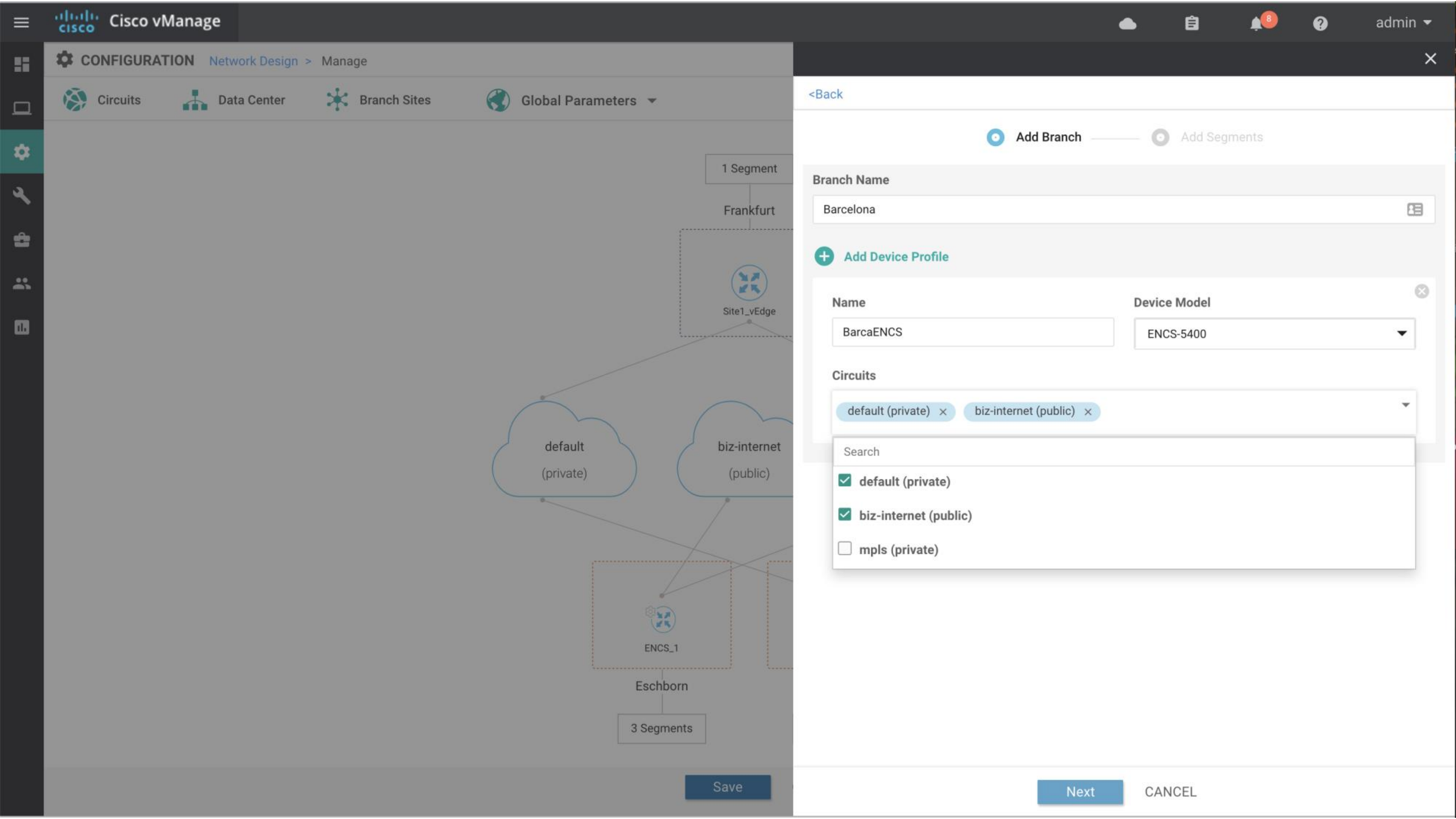
Select one or more circuits



Branch Name: Barcelona

Name: BarcaENCS

Circuits: Select one or more circuits



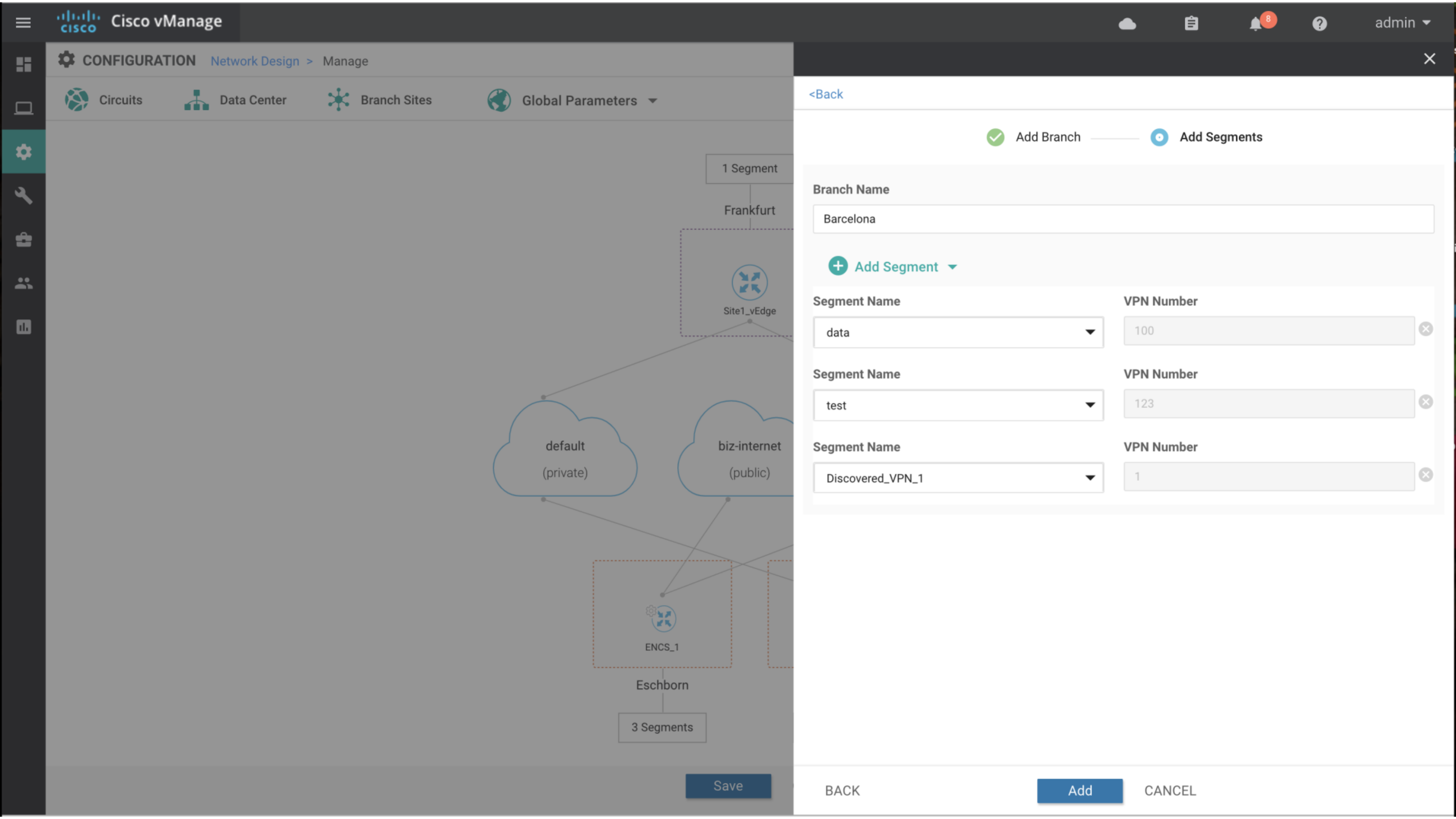
Branch Name: Barcelona

Name: BarcaENCS

Device Model: ENCS-5400

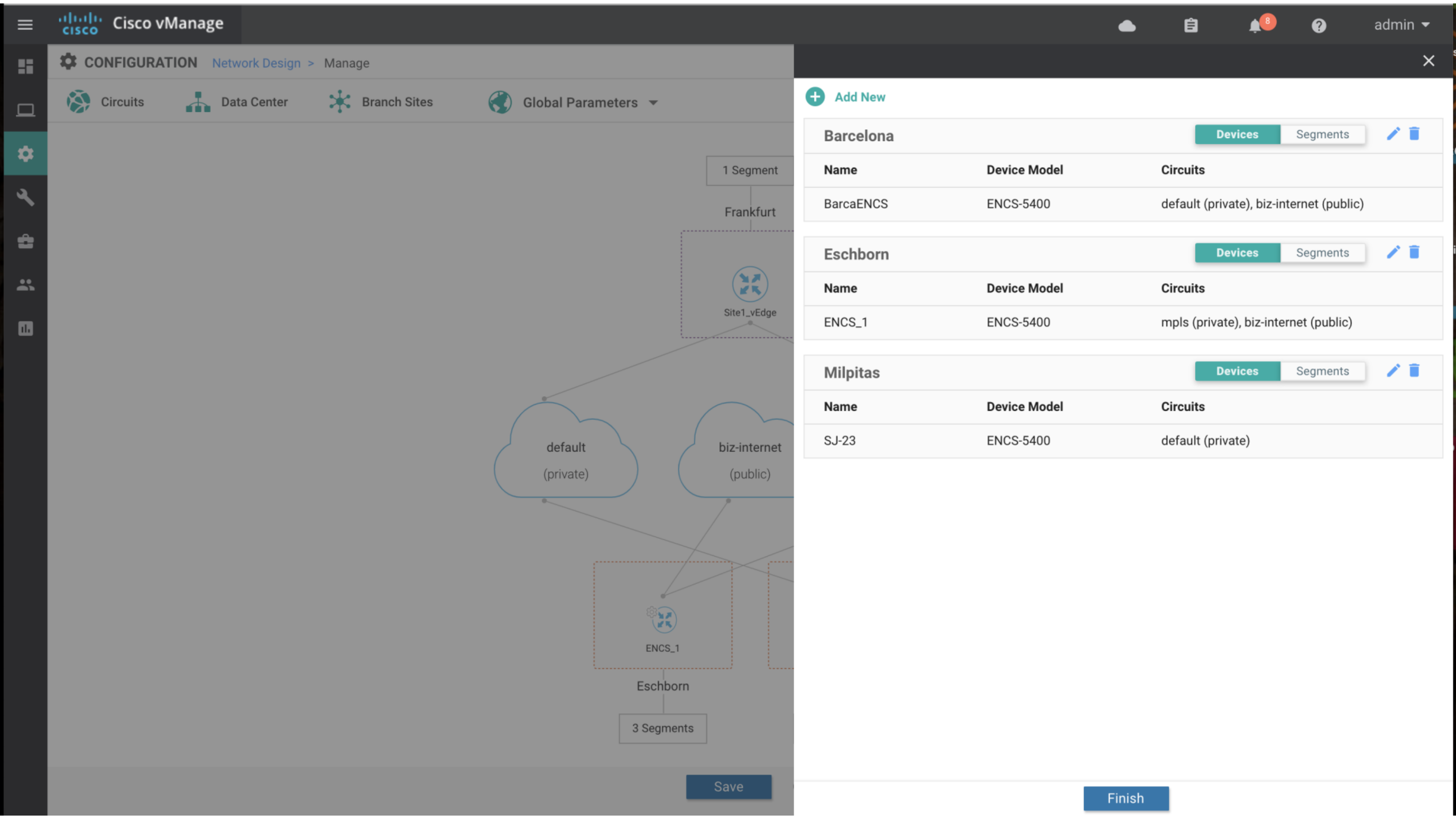
Circuits: default (private) ×   biz-internet (public) ×

☑ default (private)
☑ biz-internet (public)
□ mpls (private)



Branch Name: Barcelona

Segment Name	VPN Number
data	100
test	123
Discovered_VPN_1	1



Barcelona

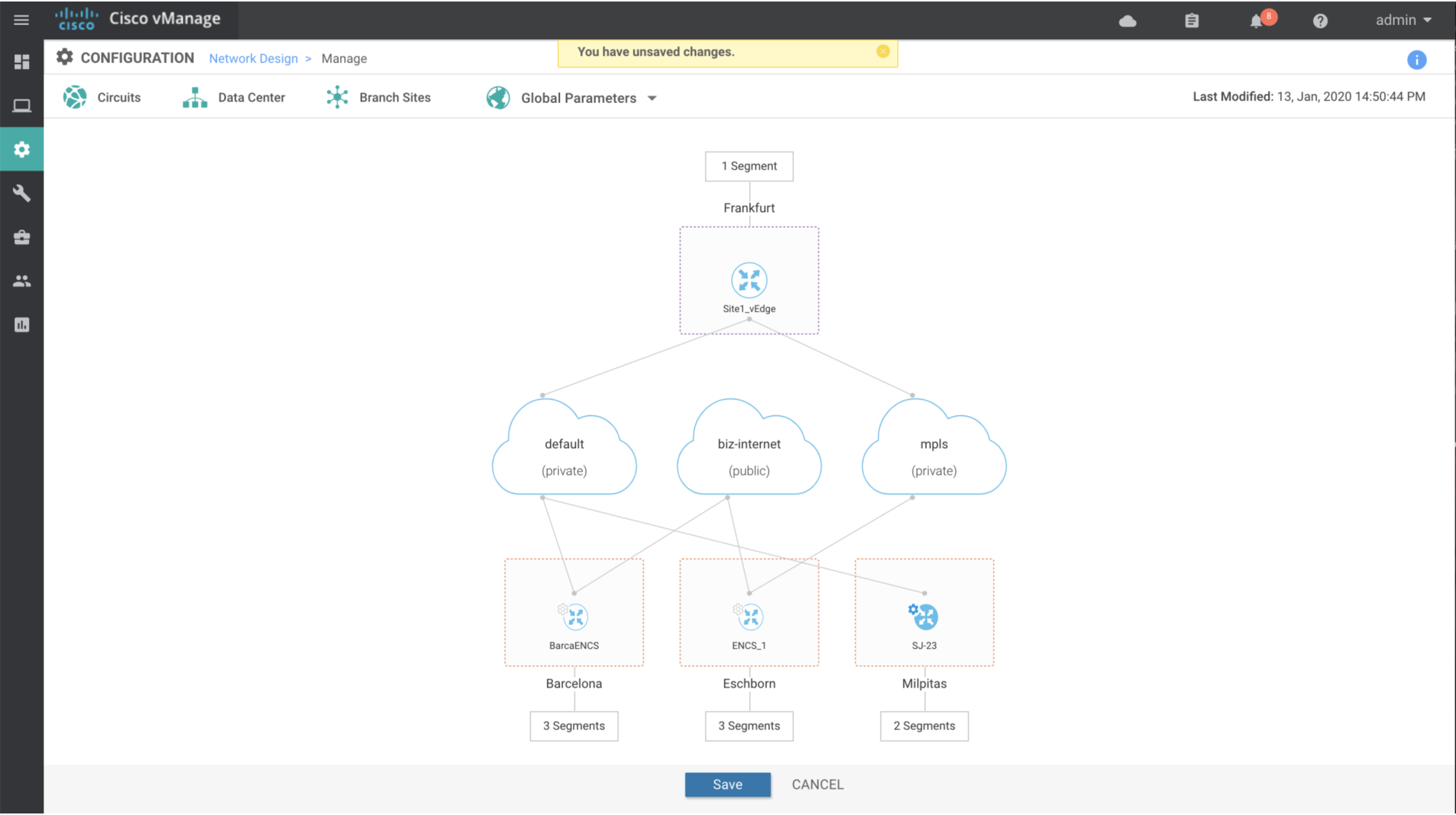
Name	Device Model	Circuits
BarcaENCS	ENCS-5400	default (private), biz-internet (public)

Eschborn

Name	Device Model	Circuits
ENCS_1	ENCS-5400	mpls (private), biz-internet (public)

Milpitas

Name	Device Model	Circuits
SJ-23	ENCS-5400	default (private)



You have unsaved changes.

Last Modified: 13, Jan, 2020 14:50:44 PM

Best Practices

- Connectivity and Design consideration
- Security and Licensing
- Monitoring and Management
- Performance consideration

Connectivity Design considerations and recommendation

1. Management Access connectivity
   a) If there is a dedicated OOB management path, consider connecting to CIMC and MGMT port.

   b) If OOB path is not available, Connect the dedicated Management port to LAN Switch and access NFVIS in-band. In addition Using Single-IP/Share-IP feature is recommended,
2. Device Bootstrap and Automation
   a) Plug-n-play : Atleast 1 wan link DHCP enabled, connect to GE0-0 for communication with service-chain orchestrator.

   b) Site-by-Site manual deployment can utilize the 1.1.a in-band connectivity.

   c) Packaging : ISRv VNF package with parameterized Custom Configuration. One package can be used for deploying multiple sites with resource profile and parameterized config template.

   d) Packaging : Alternately, If pre-created site specific custom config files are available at the time of deployment, it can be passed as a bootstrap config during deployment.

   e) Recommend that critical VNFs be deployed in Monitored mode.
3. WAN Link redundancy
   a) 2 WAN Links. Terminate on GE0-0 and GE0-1 connected to virtual router. Atleast 1 DHCP enabled.

   b) Starting 3.10 release, we have the ability to attempt DHCP on either of the WAN connection.
4. LAN side : port channel would provide link redundancy towards lan side. This would be recommended. Shutdown the LAN ports that are NOT in use.
5. Use of VLANs for segregating traffic from different VNFs, particularly on the LAN side. Note: All 8 switch ports are trunked to lan-bridge.
6. Storage : Utilize on-board storage network functions. For storage intensive application, utilize the external drive. For optimal disk IO, use eager-zero disk initialization option via vm-packaging image-properties.

Security and Licensing considerations and recommendation

1. Enterprise Certificate : Enterprise root-cert for authenticating NFVIS layer in the ENCS device.
2. TACACS Role Based Access : Define Administrator vs Operator users for monitoring Vs Day N change management.
3. L3 level NFVIS access restriction using system settings ip-receive-acl.
4. Configure Primary and Backup NTP source in NFVIS and Router/VNFs for certificate validity and license authorization. Utilize satellite license server incase connectivity to cisco smart license server is not reliable.
5. Note: Hardware and NFVIS software layer have inbuilt security defaults to ensure robust security of the system.

   •Secure UDI, Secure Boot, Tamper protection, HW Entropy, Session resource protection, privileged access for advanced debugging, traffic segmentation between VNFs and Host, Restricted storage access, input validation, etc.

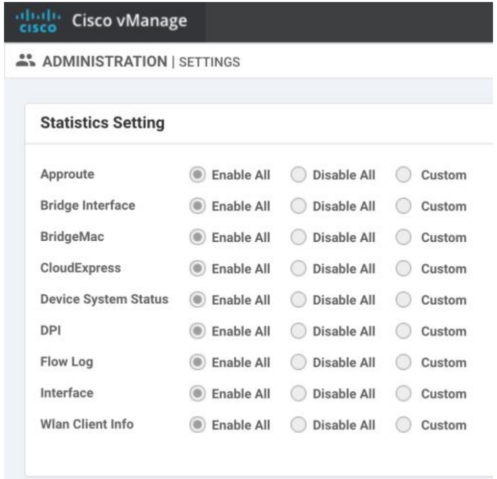
Monitoring and Management Design consideration and recommendation

- Syslog
  - NFVIS can send Syslog messages to Syslog servers. Syslogs are sent for NETCONF notifications from NFVIS.
  - This feature is used to configure the remote logging servers
  - Configuration can be done via Portal, CLI and API
- SNMPv3
  - CPU, Memory, Storage, Power / Voltage, Temperature, Fan
  - WAN port status, LAN port status
- Monitoring CLI
  - show system-monitoring host [cpu | disk | memory | port] stats
  - show system-monitoring host [cpu | disk | memory | port] table
  - Power / Voltage, Temperature, Fan
  - Default collecting duration is 5min
- NETConf
  - NFVIS sends notifications for
    - vmlcEvents (VM Lifecycle)
    - nfvisEvents (NFVIS)
  - Use NFVIS CLI or GUI to query notifications

Best Practices SD-WAN

vManage Statistics Collection

Configuration and Volumes



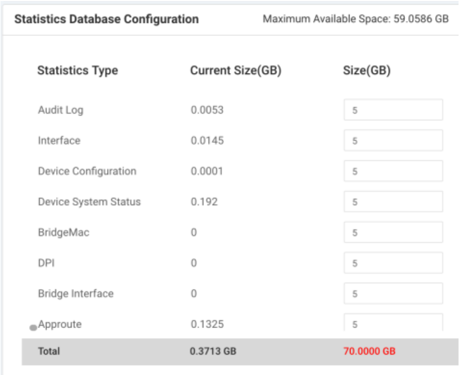
Cisco vManage

ADMINISTRATION | SETTINGS

Statistics Setting

Approute	● Enable All	○ Disable All	○ Custom
Bridge Interface	● Enable All	○ Disable All	○ Custom
BridgeMac	● Enable All	○ Disable All	○ Custom
CloudExpress	● Enable All	○ Disable All	○ Custom
Device System Status	● Enable All	○ Disable All	○ Custom
DPI	● Enable All	○ Disable All	○ Custom
Flow Log	● Enable All	○ Disable All	○ Custom
Interface	● Enable All	○ Disable All	○ Custom
Wlan Client Info	● Enable All	○ Disable All	○ Custom

- Configure collection per category and per device
- Custom allows to control collection of each category on a per device basis



Statistics Database Configuration Maximum Available Space: 59.0586 GB

Statistics Type	Current Size(GB)	Size(GB)
Audit Log	0.0053	5
Interface	0.0145	5
Device Configuration	0.0001	5
Device System Status	0.192	5
BridgeMac	0	5
DPI	0	5
Bridge Interface	0	5
Approute	0.1325	5
Total	0.3713 GB	70.0000 GB

- Storage can be assigned for individual categories to reflect:
  - Collection not being enabled
  - Storage assignments and data lifetime

Overlay and vEdge Recommended Settings

Useful Settings to get Right the First Time

- System-IP
  - Pick a range for the entire network that does not overlap with other addressing
  - Not routed but significant to anything present in VPN 0 / Transport
  - An incorrectly chosen range or System-IP setting can cause connectivity issues
- Site-ID
  - The target for policy application and identifier of routing sources (ref: BGP AS)
  - Several schemes documented and one is discussed later on
- Vmanage connection preference
  - Determines which TLOC is used for vManage traffic (statistics upload etc)
  - Advised to use the highest bandwidth link and avoid cellular interfaces
- Max-control-connections
  - Determines how many vSmart sessions are established per TLOC
  - For Transports without controller access, it must be set to Zero (0)

Template Creation Guidelines

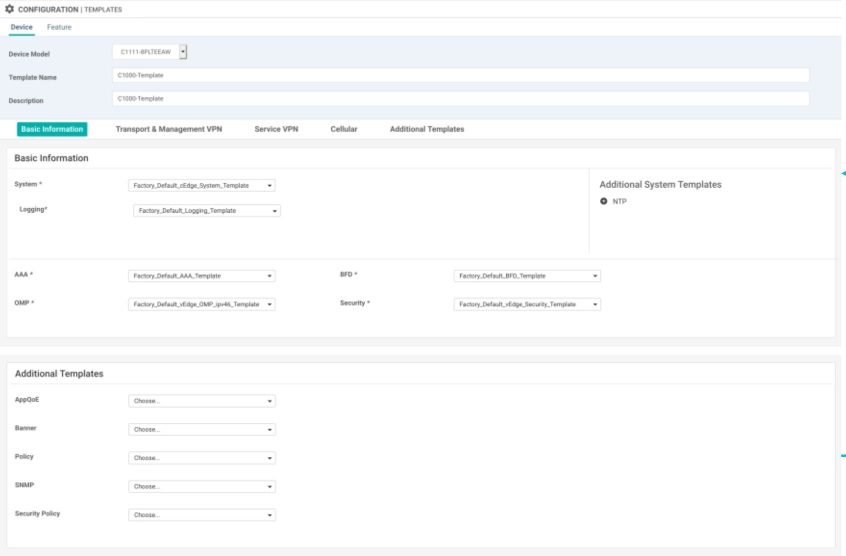
Templates are Friends

- Plan for template creation and test out features to be deployed
    - Allows for the optimization of template structure and maintenance
- Use a simple ”bootstrap” template for distributed devices that are not yet in production
    - The device is then in a known state and vManaged
    - Tracking events is easier if a logical name is applied
    - The local configuration of the device can’t be changed
    - The device can be moved to production (or any other state) at will from vManage
- The template can be changed at any time from within vManage
- Template Variables can be managed in several different ways:
    - Entered manually at time of template attachment
    - Stored in a .csv file that is referenced at time of template application
    - Using the REST API (possibly in conjunction with other platforms such as Infoblox)

Template Creation

Feature Template Components and Sources

Device Template - Aggregate Configuration Template



Device Model C1111-8PLTEEAW

Template Name C1000-Template

Description C1000-Template

Basic Information

System * Factory_Default_cEdge_System_Template

Logging* Factory_Default_Logging_Template

Additional System Templates

- NTP

AAA * Factory_Default_AAA_Template

BFD * Factory_Default_BFD_Template

OMP * Factory_Default_vEdge_OMP_ipv46_Template

Security * Factory_Default_vEdge_Security_Template

Additional Templates

AppQoE Choose...

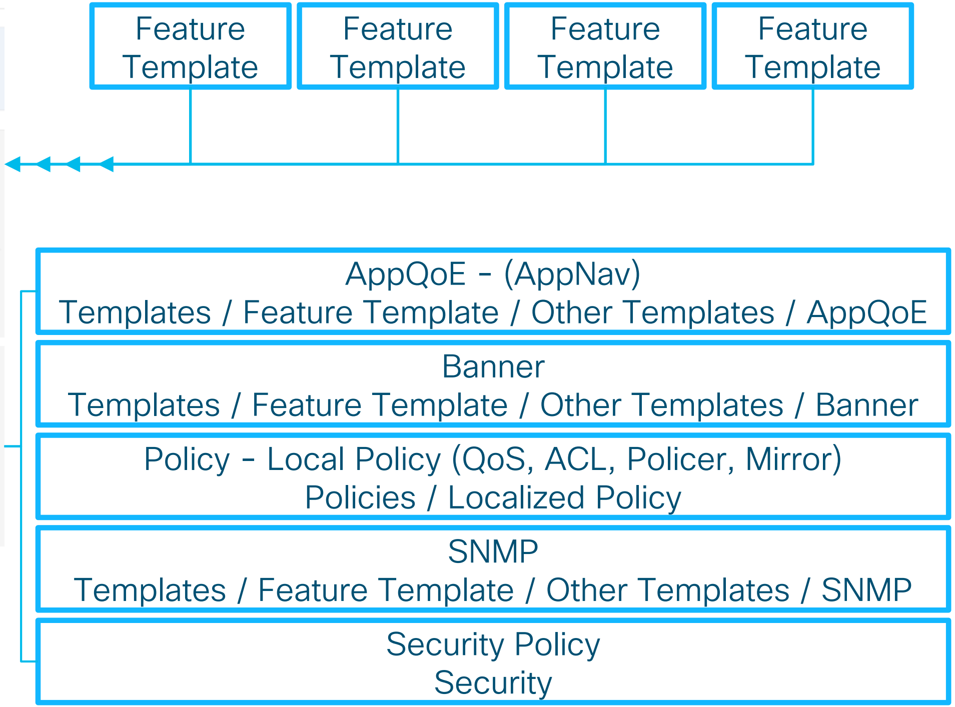
Banner Choose...

Policy Choose...

SNMP Choose...

Security Policy Choose...

Dedicated or Shared Feature Templates



Feature Template

Feature Template

Feature Template

Feature Template

AppQoE - (AppNav)
Templates / Feature Template / Other Templates / AppQoE

Banner
Templates / Feature Template / Other Templates / Banner

Policy - Local Policy (QoS, ACL, Policer, Mirror)
Policies / Localized Policy

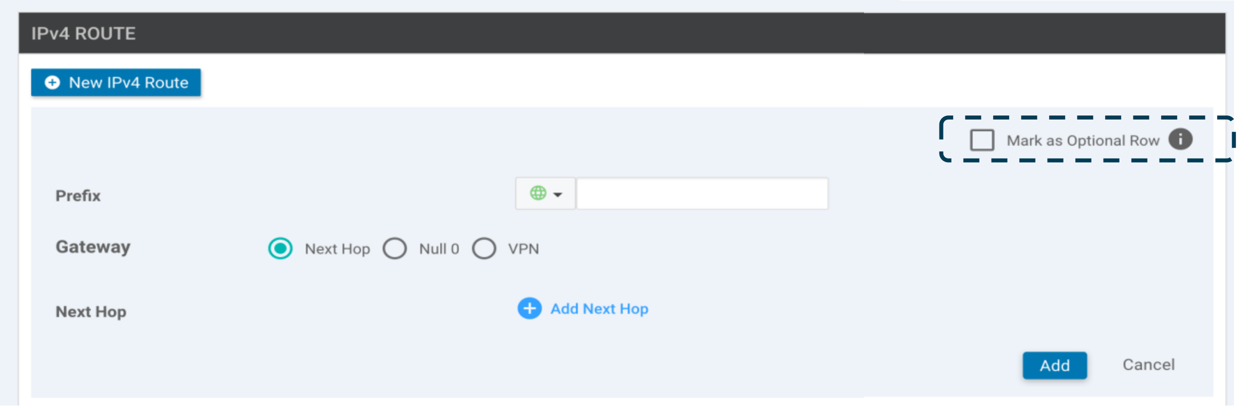
SNMP
Templates / Feature Template / Other Templates / SNMP

Security Policy
Security

cisco Live!

Template Creation - Device Template

Optimizing object use in a Device Template - Optional Objects



IPv4 ROUTE

□ Mark as Optional Row

Prefix

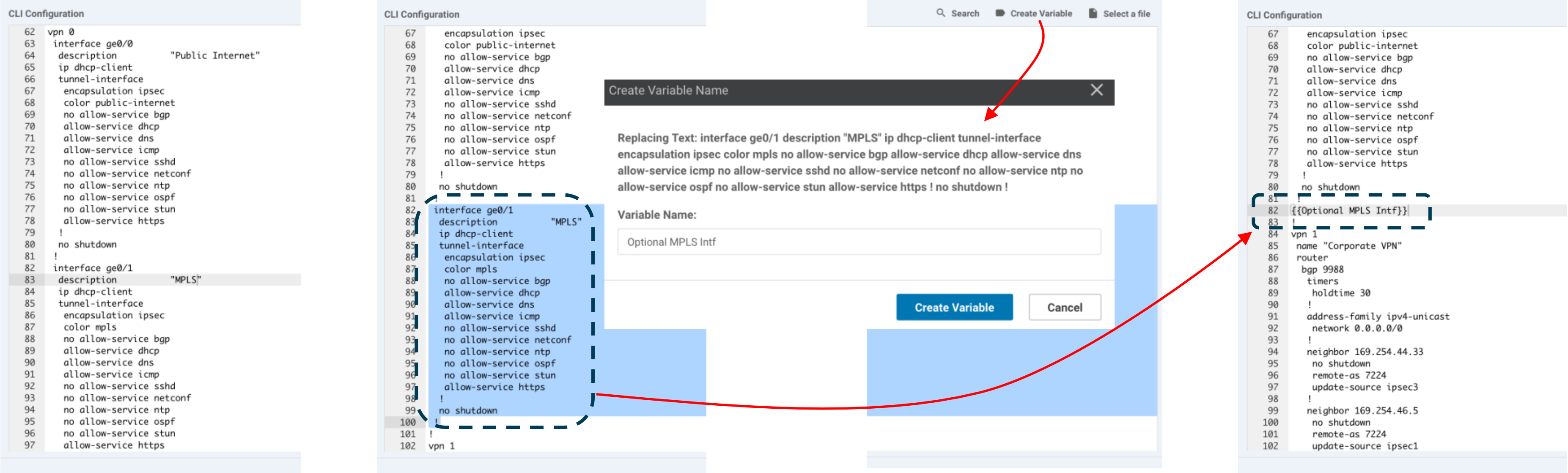
Gateway ● Next Hop ○ Null 0 ○ VPN

Next Hop

- Using Device Templates, quite a few objects can be tagged as Optional
- Simply not assigning a value at template application leaves the object out of the created configuration
- This makes Device Templates flexible to support a variety of different configurations

Template Creation - CLI Template

Optimizing object use in CLI template by means of variables



CLI Configuration

```
vpn 0
 interface ge0/0
  description          "Public Internet"
  ip dhcp-client
  tunnel-interface
   encapsulation ipsec
   color public-internet
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 interface ge0/1
  description          "MPLS"
  ip dhcp-client
  tunnel-interface
   encapsulation ipsec
   color mpls
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
```

CLI Configuration

```
   encapsulation ipsec
   color public-internet
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
 interface ge0/1
  description          "MPLS"
  ip dhcp-client
  tunnel-interface
   encapsulation ipsec
   color mpls
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
!
vpn 1
```

Create Variable Name

Replacing Text: interface ge0/1 description "MPLS" ip dhcp-client tunnel-interface encapsulation ipsec color mpls no allow-service bgp allow-service dhcp allow-service dns allow-service icmp no allow-service sshd no allow-service netconf no allow-service ntp no allow-service ospf no allow-service stun allow-service https ! no shutdown !

Variable Name: Optional MPLS Intf

CLI Configuration

```
   encapsulation ipsec
   color public-internet
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  !
  no shutdown
 !
{{Optional MPLS Intf}}
!
vpn 1
 name "Corporate VPN"
 router
  bgp 9988
   timers
    holdtime 30
   !
   address-family ipv4-unicast
    network 0.0.0.0/0
   !
   neighbor 169.254.44.33
    no shutdown
    remote-as 7224
    update-source ipsec3
   !
   neighbor 169.254.46.5
    no shutdown
    remote-as 7224
    update-source ipsec1
```

- In a CLI template, an arbitrary number of lines can be turned into a variable
- Assigning this variable a “;” at template application leaves the section out of the created configuration
- This makes CLI Templates flexible to support a variety of different configurations

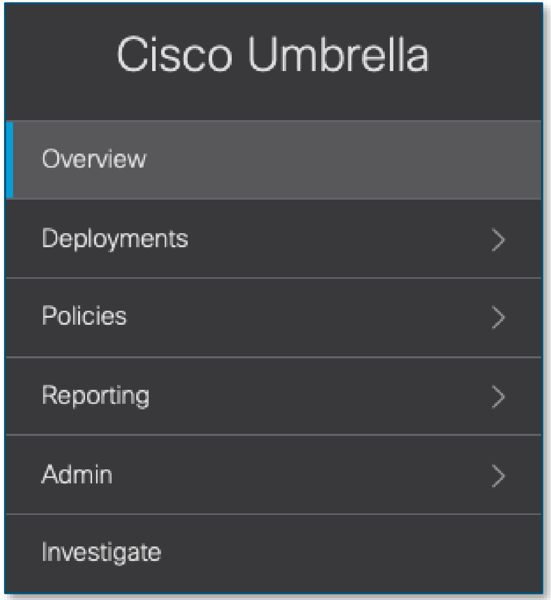
Policy Creation and Management Guidelines

Really not different from standard operations

- Define Requirements up front
  - Important Applications
  - Segmentation and Connectivity Models
  - SLA and QoS Requirements
  - Application Pinning, Breakout, Hosting, Routing i.e. Application Management Requirements
- Use a sandbox for verification and testing
  - A separate domain where policies and requirements can be tested
  - Can be part of the production network, simply a separate Site-ID range
- Limit Policy Management to a few capable resources

Umbrella Security Policies

Cisco Umbrella Grocery List



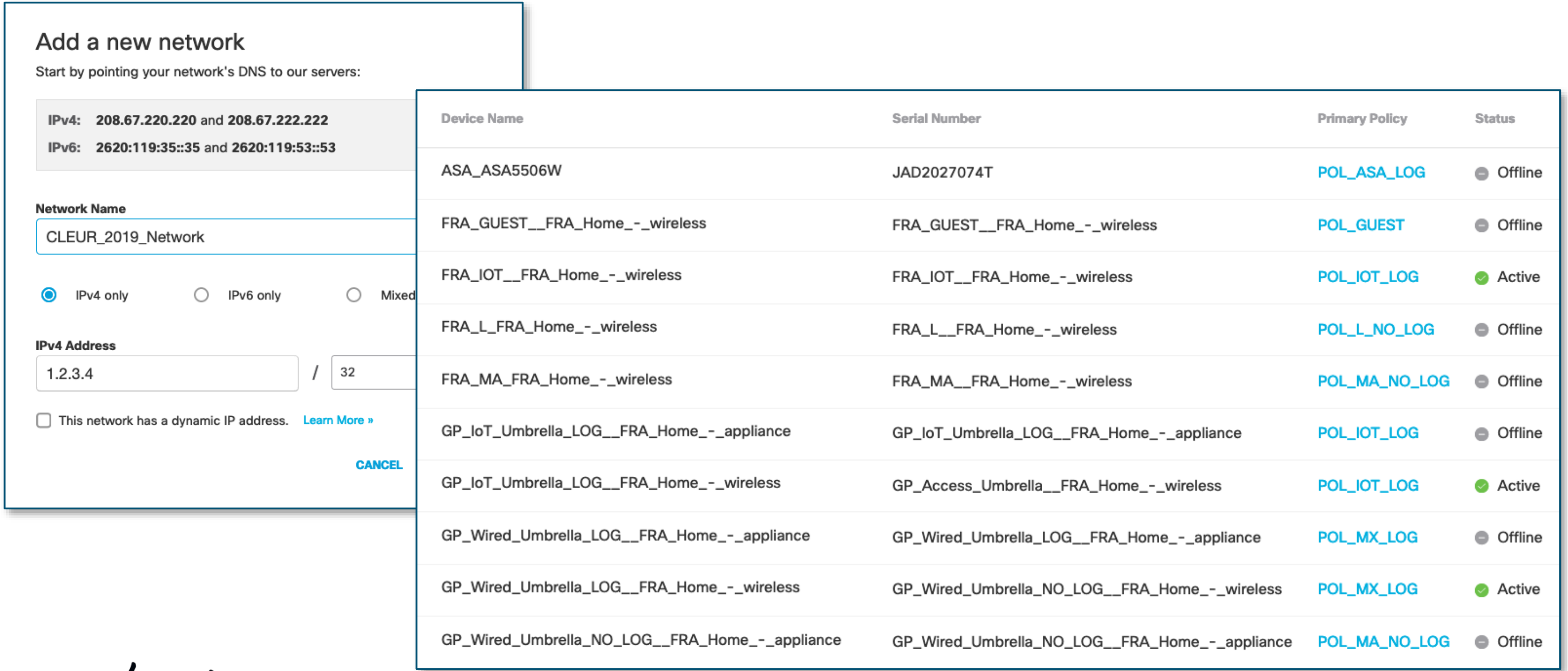
DEPLOYMENT IDENTITY

- Network
- Device
- Endpoint
- Tunnel
- *other identities*

SECURITY POLICY

- DNS
- Firewall
- Web

Umbrella Identities – Network and Device



Add a new network

Start by pointing your network's DNS to our servers:

IPv4: **208.67.220.220** and **208.67.222.222**

IPv6: **2620:119:35::35** and **2620:119:53::53**

Network Name

CLEUR_2019_Network

● IPv4 only ○ IPv6 only ○ Mixed

IPv4 Address

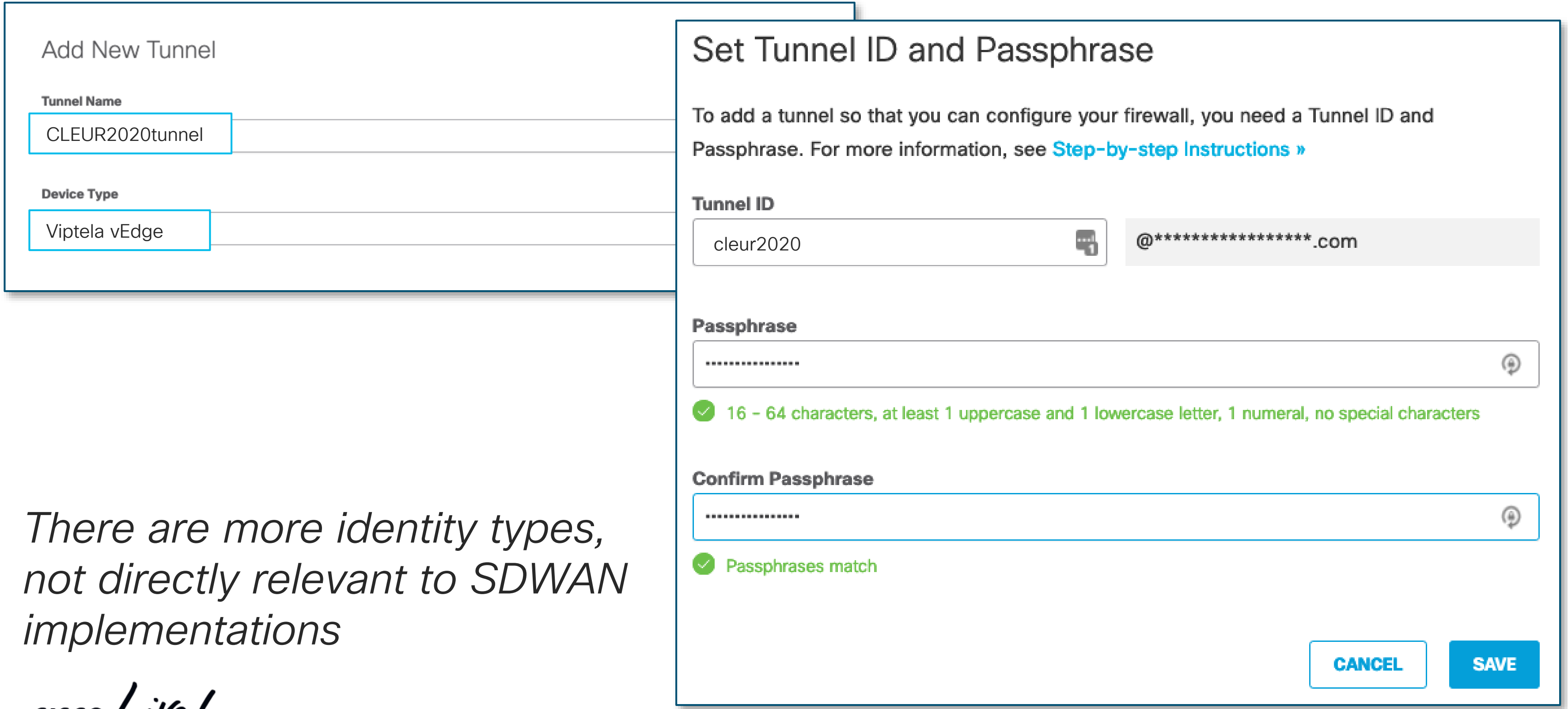
1.2.3.4 / 32

□ This network has a dynamic IP address. Learn More »

CANCEL

Device Name	Serial Number	Primary Policy	Status
ASA_ASA5506W	JAD2027074T	POL_ASA_LOG	Offline
FRA_GUEST__FRA_Home_-_wireless	FRA_GUEST__FRA_Home_-_wireless	POL_GUEST	Offline
FRA_IOT__FRA_Home_-_wireless	FRA_IOT__FRA_Home_-_wireless	POL_IOT_LOG	Active
FRA_L_FRA_Home_-_wireless	FRA_L__FRA_Home_-_wireless	POL_L_NO_LOG	Offline
FRA_MA_FRA_Home_-_wireless	FRA_MA__FRA_Home_-_wireless	POL_MA_NO_LOG	Offline
GP_IoT_Umbrella_LOG__FRA_Home_-_appliance	GP_IoT_Umbrella_LOG__FRA_Home_-_appliance	POL_IOT_LOG	Offline
GP_IoT_Umbrella_LOG__FRA_Home_-_wireless	GP_Access_Umbrella__FRA_Home_-_wireless	POL_IOT_LOG	Active
GP_Wired_Umbrella_LOG__FRA_Home_-_appliance	GP_Wired_Umbrella_LOG__FRA_Home_-_appliance	POL_MX_LOG	Offline
GP_Wired_Umbrella_LOG__FRA_Home_-_wireless	GP_Wired_Umbrella_NO_LOG__FRA_Home_-_wireless	POL_MX_LOG	Active
GP_Wired_Umbrella_NO_LOG__FRA_Home_-_appliance	GP_Wired_Umbrella_NO_LOG__FRA_Home_-_appliance	POL_MA_NO_LOG	Offline

Umbrella Identities - Tunnels



Add New Tunnel

Tunnel Name

CLEUR2020tunnel

Device Type

Viptela vEdge

Set Tunnel ID and Passphrase

To add a tunnel so that you can configure your firewall, you need a Tunnel ID and Passphrase. For more information, see Step-by-step Instructions »

Tunnel ID

cleur2020 @*****************.com

Passphrase

••••••••••••••••••

✓ 16 - 64 characters, at least 1 uppercase and 1 lowercase letter, 1 numeral, no special characters

Confirm Passphrase

••••••••••••••••••

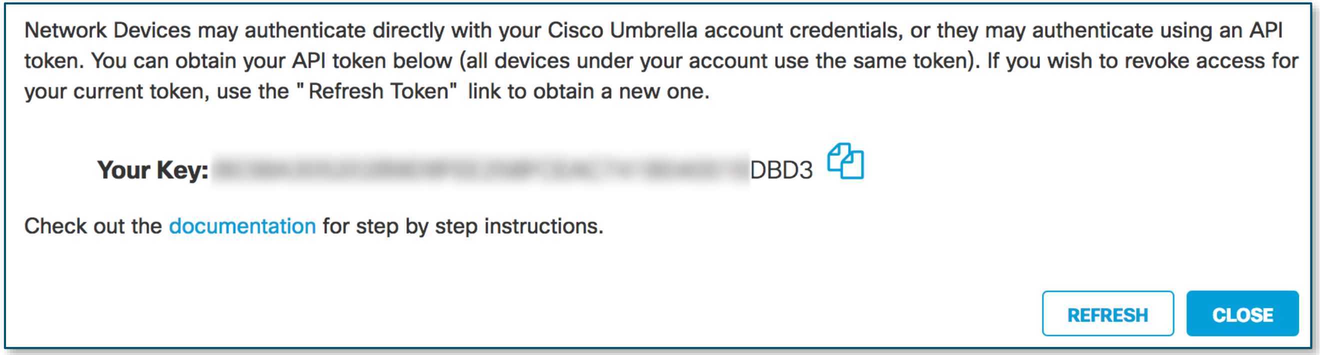
✓ Passphrases match

There are more identity types, not directly relevant to SDWAN implementations

DNS and IPsec Integrations

DNS Integration - API Key

Step 1: Copy API key in Umbrella dashboard

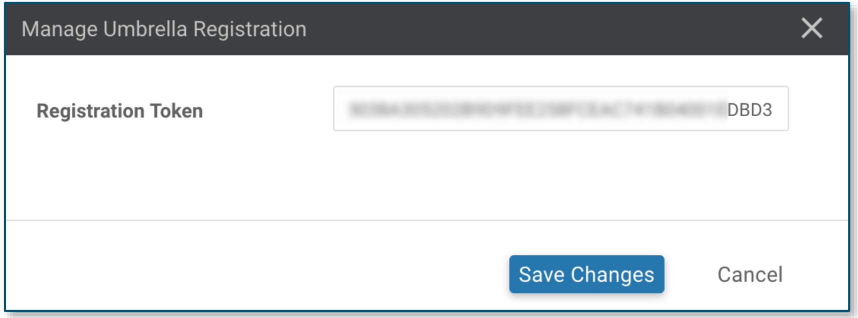


Network Devices may authenticate directly with your Cisco Umbrella account credentials, or they may authenticate using an API token. You can obtain your API token below (all devices under your account use the same token). If you wish to revoke access for your current token, use the " Refresh Token" link to obtain a new one.

Your Key: [redacted]DBD3

Check out the documentation for step by step instructions.

Step 2: Input API key in vManage dashboard

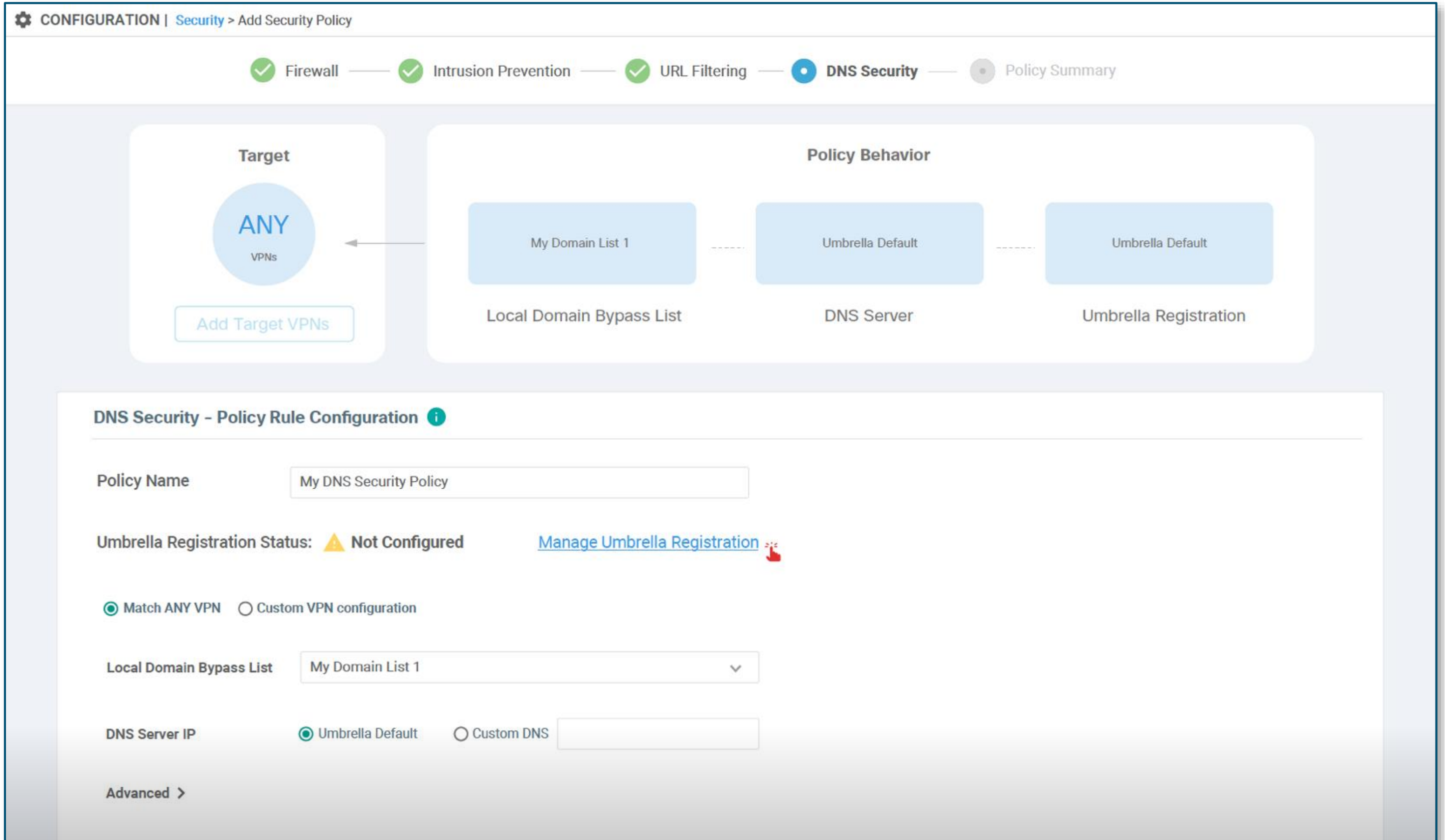


Manage Umbrella Registration

Registration Token [redacted]DBD3

DNS Integration – Configure Policy

Step 3: Configure Umbrella policy



DNS Security – Policy Rule Configuration

Policy Name: My DNS Security Policy

Umbrella Registration Status: ⚠ Not Configured   Manage Umbrella Registration

● Match ANY VPN ○ Custom VPN configuration

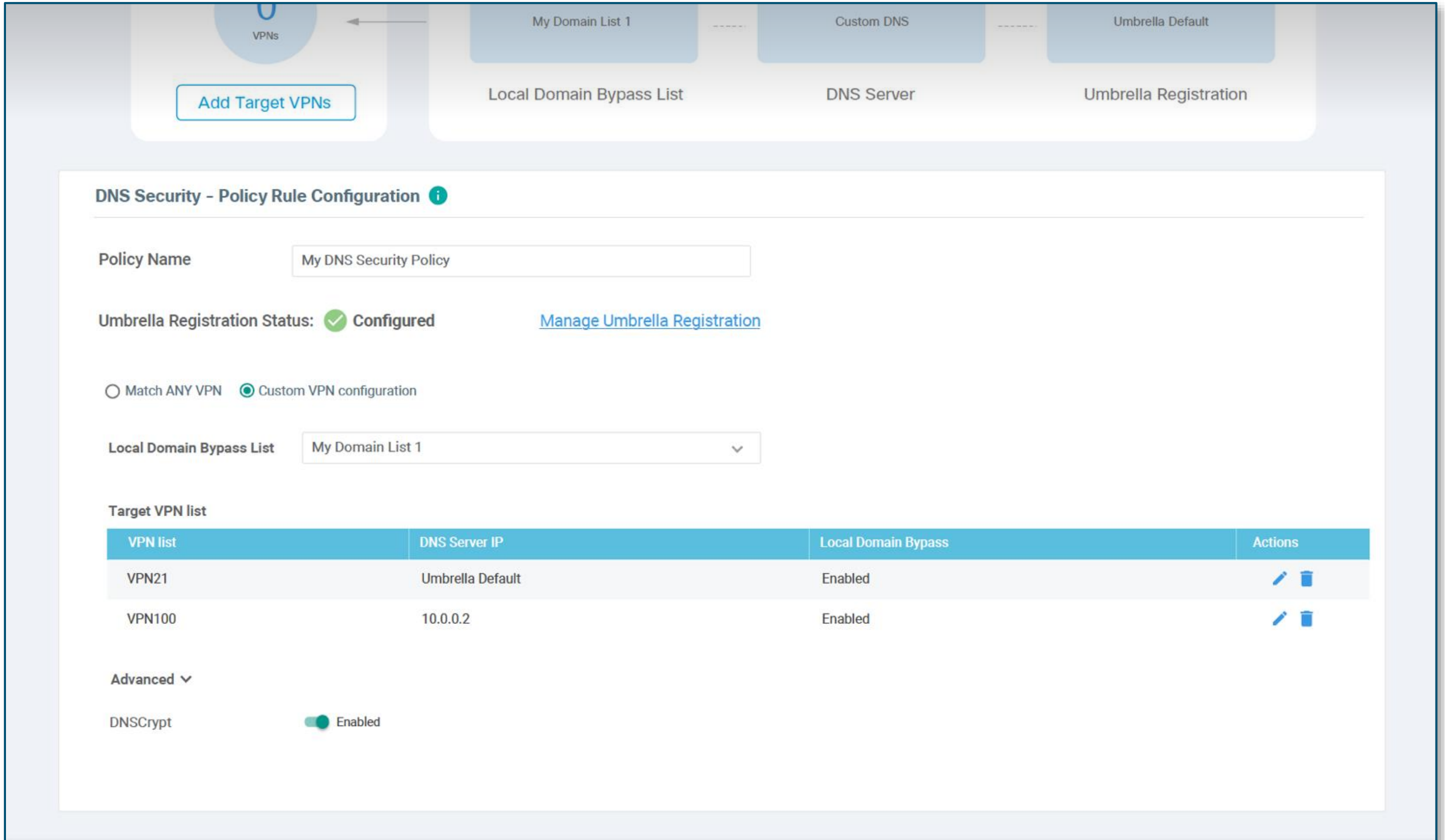
Local Domain Bypass List: My Domain List 1

DNS Server IP: ● Umbrella Default ○ Custom DNS

Advanced >

DNS integration – Final Touches

Step 4: Apply policy per-VPN and optionally enable DNScrypt



DNS Security - Policy Rule Configuration

Policy Name: My DNS Security Policy

Umbrella Registration Status: ✓ Configured — Manage Umbrella Registration

○ Match ANY VPN ● Custom VPN configuration

Local Domain Bypass List: My Domain List 1

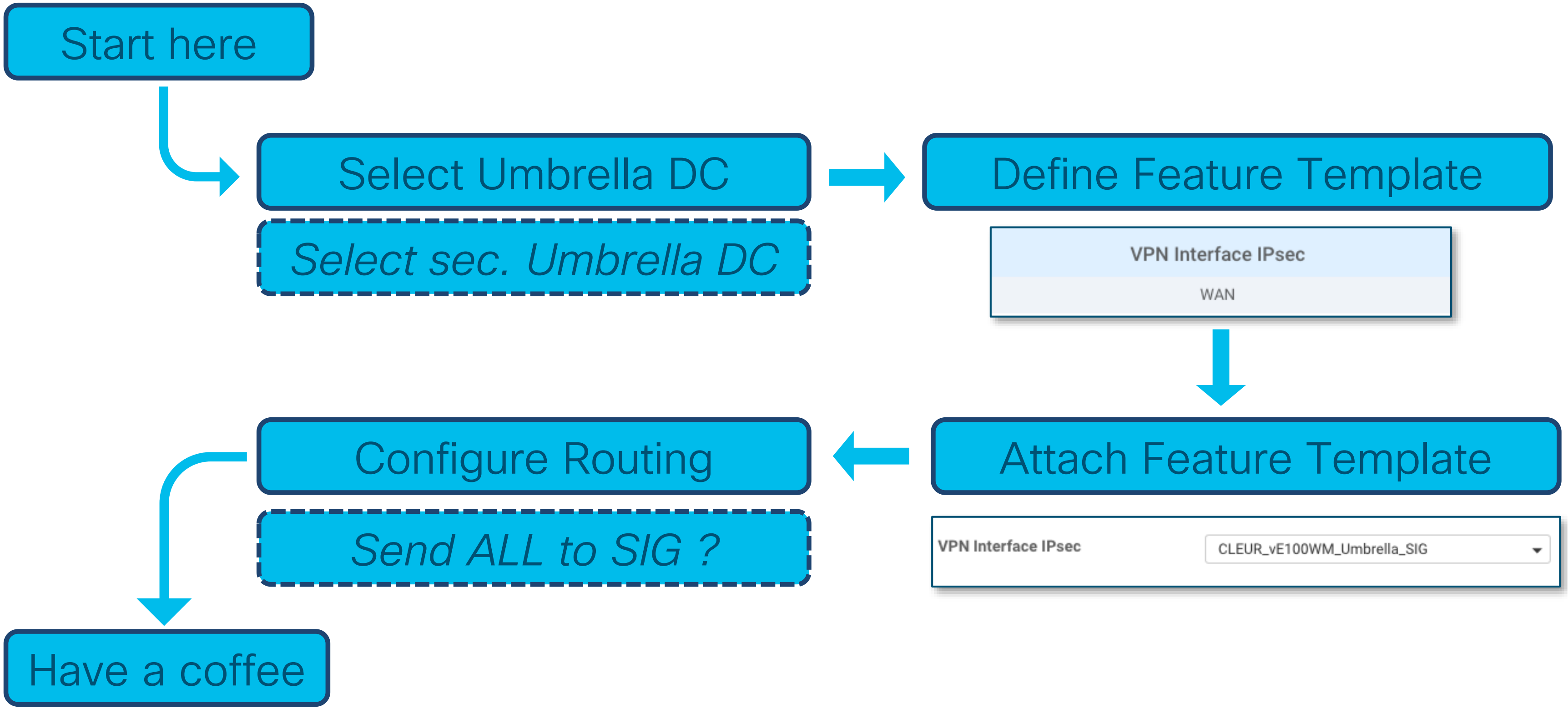
Target VPN list

VPN list	DNS Server IP	Local Domain Bypass	Actions
VPN21	Umbrella Default	Enabled	
VPN100	10.0.0.2	Enabled	

Advanced

DNSCrypt: Enabled

vEdge – IPsec Tunnel Setup – Grocery List



Start here

Select Umbrella DC

Select sec. Umbrella DC

Define Feature Template

VPN Interface IPsec
WAN

Attach Feature Template

VPN Interface IPsec: CLEUR_vE100WM_Umbrella_SIG

Configure Routing

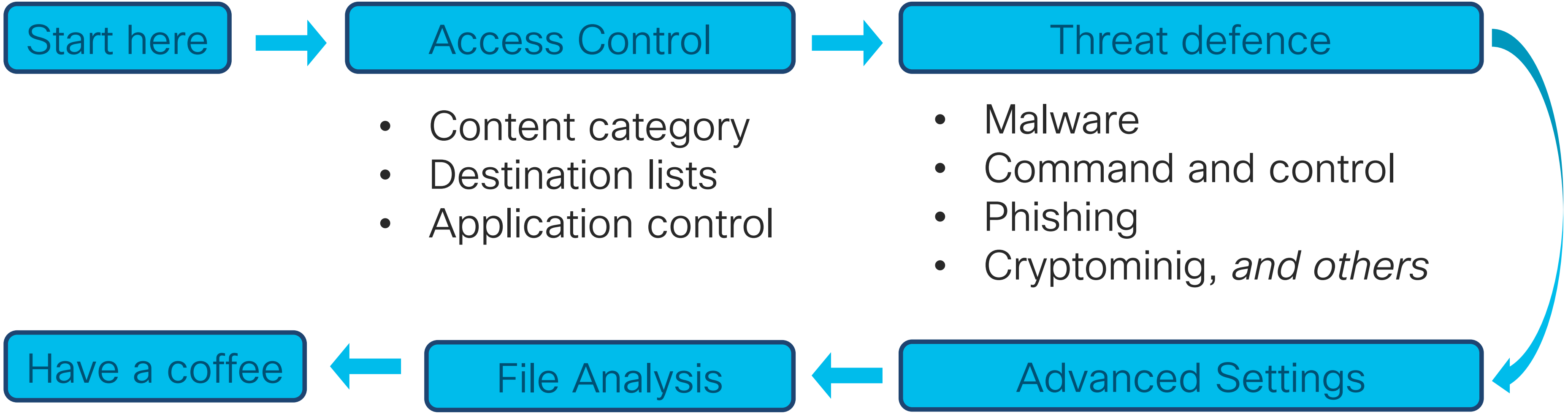
Send ALL to SIG ?

Have a coffee

Video –vManage Ipsec Tunnel configuration

SIG Policy configuration

DNS Policy configuration



Start here

Access Control

- Content category
- Destination lists
- Application control

Threat defence

- Malware
- Command and control
- Phishing
- Cryptominig, *and others*

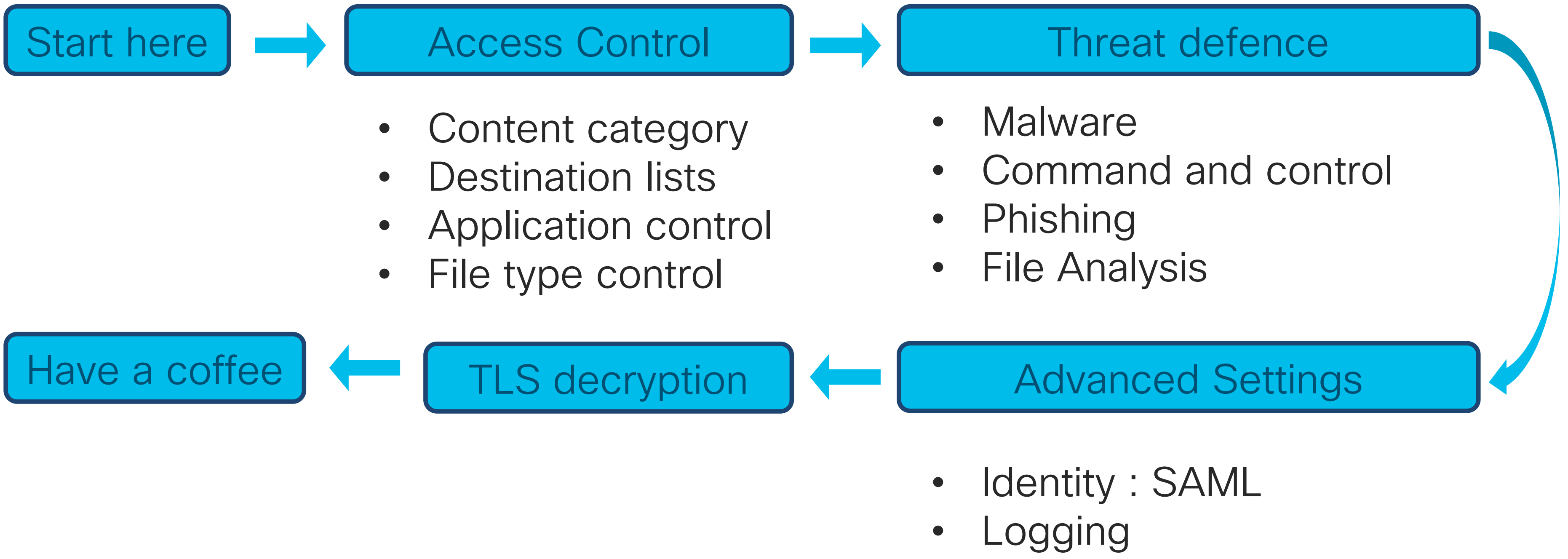
Advanced Settings

- Selective Proxy
- Logging

File Analysis

Have a coffee

WEB Policy configuration



Start here → Access Control → Threat defence → Advanced Settings → TLS decryption → Have a coffee

Access Control

- Content category
- Destination lists
- Application control
- File type control

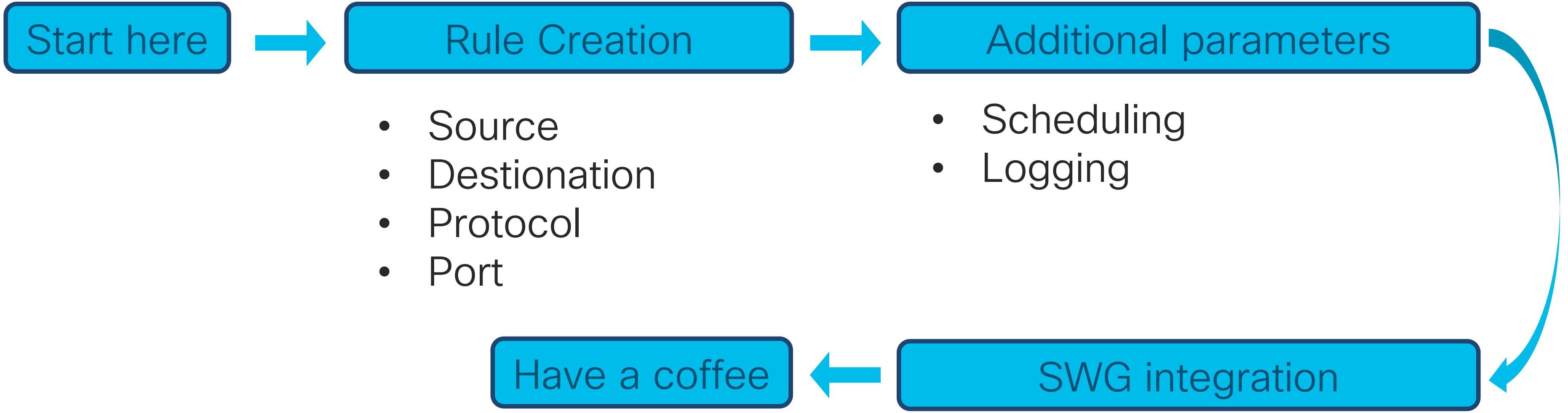
Threat defence

- Malware
- Command and control
- Phishing
- File Analysis

Advanced Settings

- Identity : SAML
- Logging

Firewall Policy configuration



Start here

Rule Creation

- Source
- Destionation
- Protocol
- Port

Additional parameters

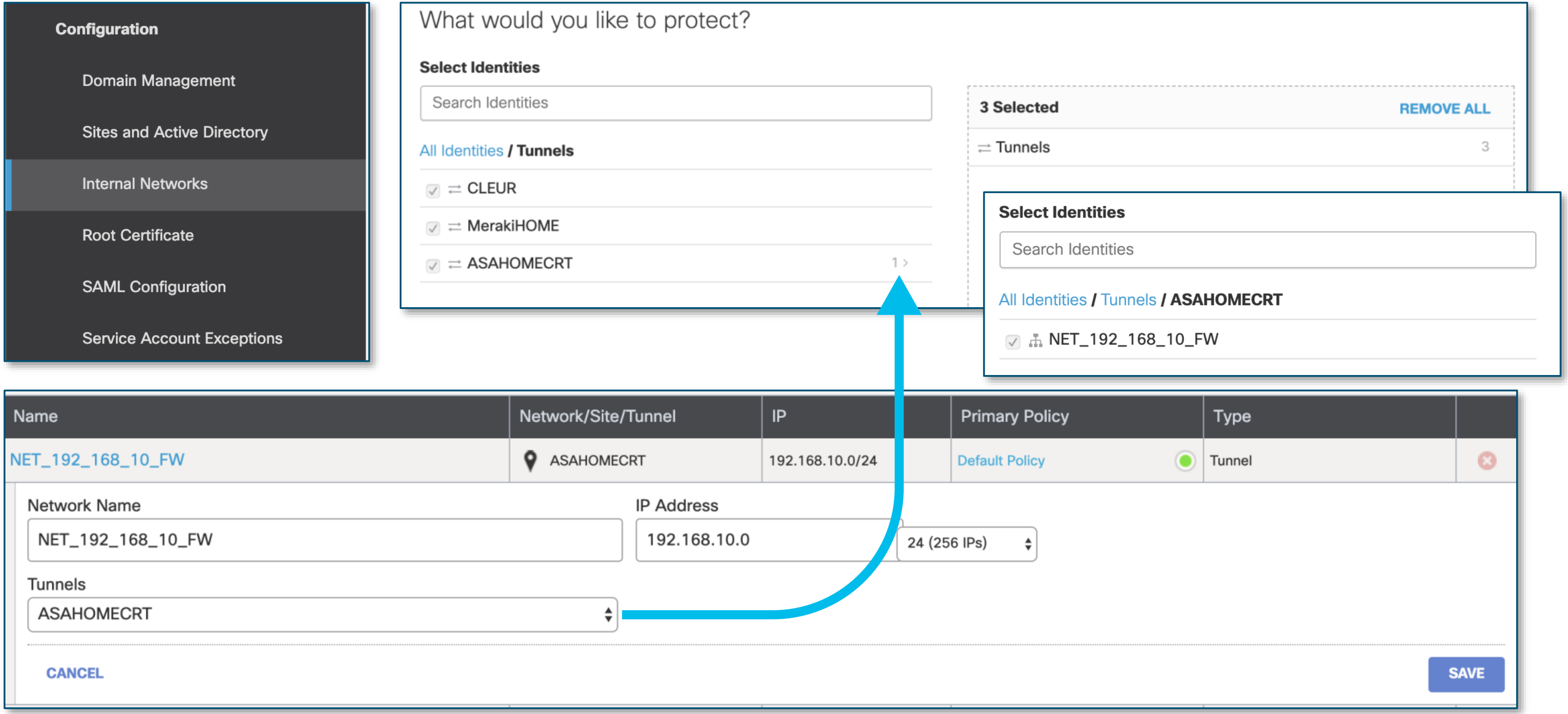
- Scheduling
- Logging

SWG integration

- Bind Private IP Subnets to a tunnel

Have a coffee

Web Policy – Divert IPsec traffic to Web Gateway



Configuration

- Domain Management
- Sites and Active Directory
- Internal Networks
- Root Certificate
- SAML Configuration
- Service Account Exceptions

What would you like to protect?

Select Identities

Search Identities

All Identities / **Tunnels**

- ☑ ⇄ CLEUR
- ☑ ⇄ MerakiHOME
- ☑ ⇄ ASAHOMECRT 1 >

3 Selected REMOVE ALL

⇄ Tunnels 3

Select Identities

Search Identities

All Identities / Tunnels / **ASAHOMECRT**

- ☑ NET_192_168_10_FW

Name	Network/Site/Tunnel	IP	Primary Policy	Type	
NET_192_168_10_FW	ASAHOMECRT	192.168.10.0/24	Default Policy ●	Tunnel	⊗

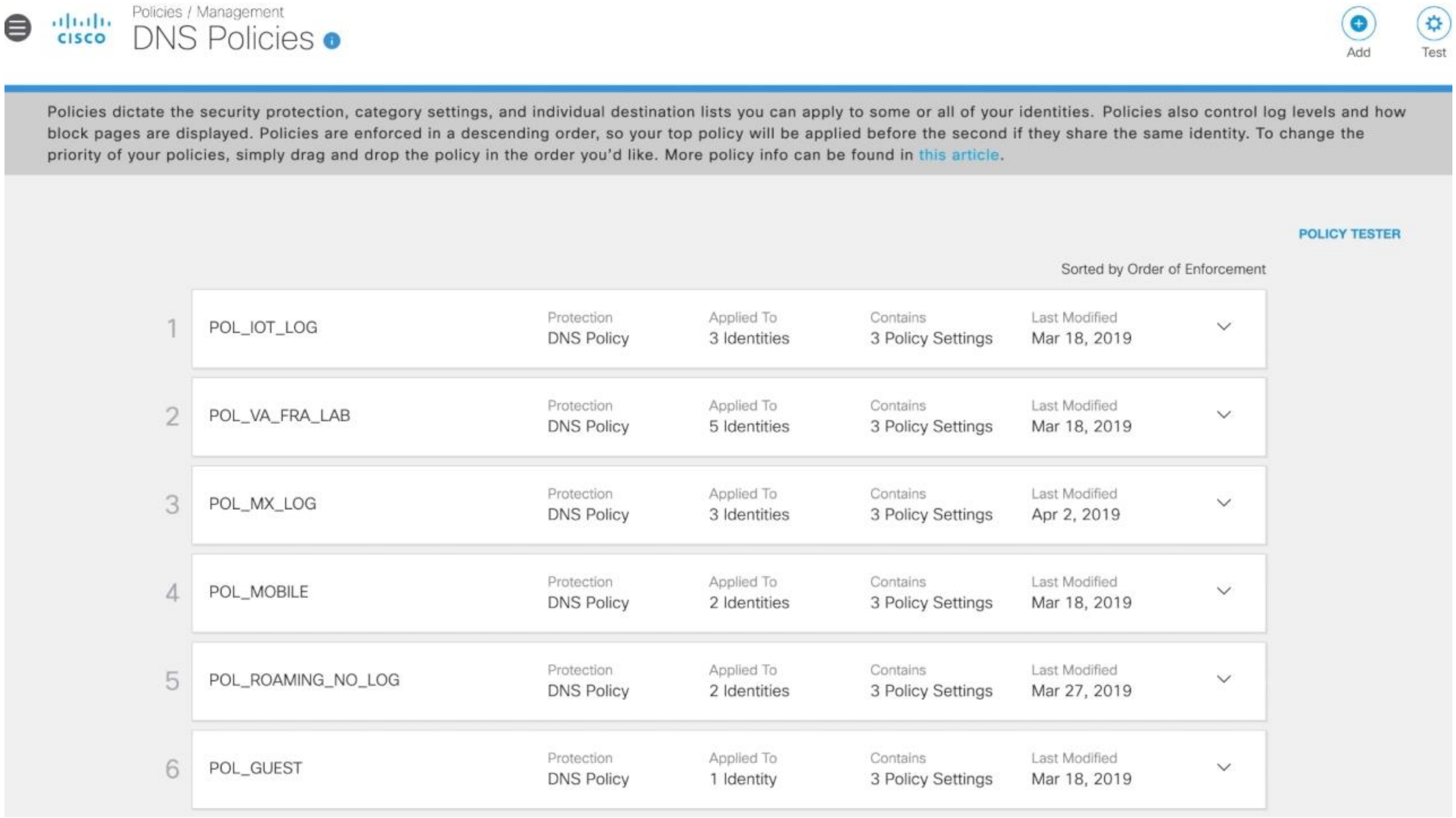
Network Name: NET_192_168_10_FW

IP Address: 192.168.10.0 24 (256 IPs)

Tunnels: ASAHOMECRT

CANCEL SAVE

Video –Umbrella policy configuration



Policies / Management

DNS Policies

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in this article.

Sorted by Order of Enforcement

		Protection	Applied To	Contains	Last Modified
1	POL_IOT_LOG	DNS Policy	3 Identities	3 Policy Settings	Mar 18, 2019
2	POL_VA_FRA_LAB	DNS Policy	5 Identities	3 Policy Settings	Mar 18, 2019
3	POL_MX_LOG	DNS Policy	3 Identities	3 Policy Settings	Apr 2, 2019
4	POL_MOBILE	DNS Policy	2 Identities	3 Policy Settings	Mar 18, 2019
5	POL_ROAMING_NO_LOG	DNS Policy	2 Identities	3 Policy Settings	Mar 27, 2019
6	POL_GUEST	DNS Policy	1 Identity	3 Policy Settings	Mar 18, 2019

MONITORING

Know before you get that call

Performance Dependencies

Individual performance of a VNF depends on several factors :

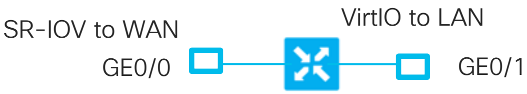
- The underlying platform, the number of cores and the type and frequency of the processor used
- The resources available for the VNF
- How the VM connects to the physical NICS – PCI Passthrough, SR-IOV, virtIO
- Finally The VNF itself. VNF must also be optimized to run in a virtual environment

In case of a Multi-VNF environment, the net chained VNF performance also depends on :

- The weakest-link VNF
- Use of virtual switches to copy packets from ingress to egress vNICs

SD-WAN Performance on ENCS

Deployment Option 1: WAN SR-IOV and LAN VirtIO



SR-IOV to WAN

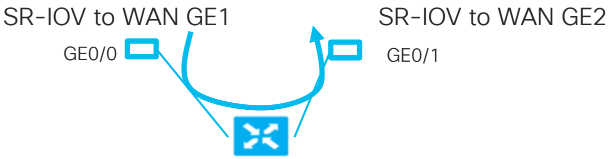
GE0/0

VirtIO to LAN

GE0/1

Platform	vEdge	Throughput
ENCS 5406	4vCPU, 4GB RAM, 8 GB HDD	400 Mbps
ENCS 5408	4vCPU, 4GB RAM, 8 GB HDD	400 Mbps
ENCS 5412	4vCPU, 4GB RAM, 8 GB HDD	250 Mbps

Deployment Option 2: WAN to WAN SR-IOV



SR-IOV to WAN GE1

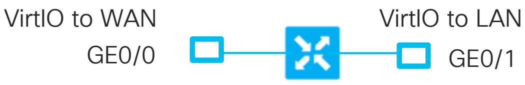
GE0/0

SR-IOV to WAN GE2

GE0/1

Platform	vEdge	Throughput
ENCS 5406	4vCPU, 4GB RAM, 8 GB HDD	900 Mbps
ENCS 5408	4vCPU, 4GB RAM, 8 GB HDD	900 Mbps
ENCS 5412	4vCPU, 4GB RAM, 8 GB HDD	700 Mbps

Deployment Option 3: WAN VirtIO and LAN VirtIO



VirtIO to WAN

GE0/0

VirtIO to LAN

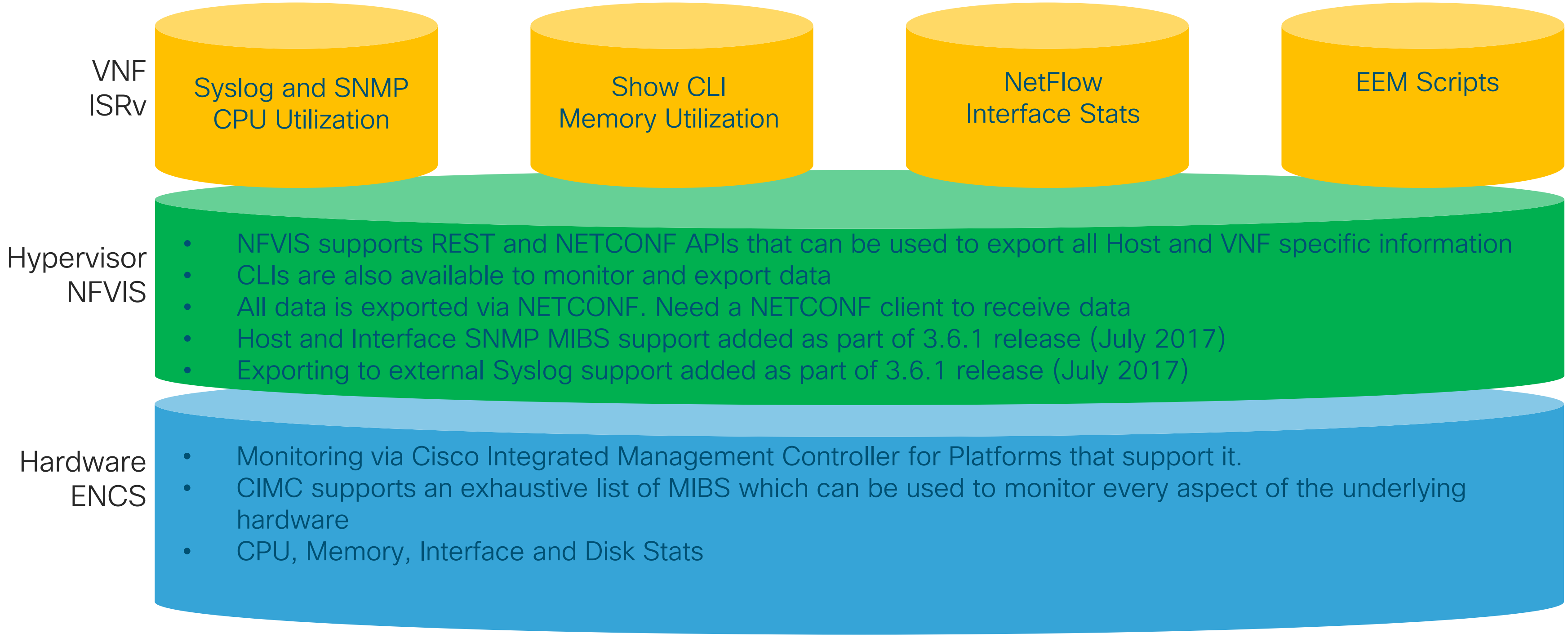
GE0/1

Platform	vEdge	Throughput
ENCS5104	2vCPU, 4GB RAM, 8 GB HDD	200 Mpbs
ENCS 5406	2vCPU, 4GB RAM, 8 GB HDD	260 Mbps
ENCS 5408	2vCPU, 4GB RAM, 8 GB HDD	260 Mbps
ENCS 5412	2vCPU, 4GB RAM, 8 GB HDD	160 Mbps

VNFs can be service chained using SR-IOV VFs on ENCS

Monitoring and Troubleshooting a Virtual Environment

Enterprise NFV Monitoring



VNF
ISRv

Syslog and SNMP
CPU Utilization

Show CLI
Memory Utilization

NetFlow
Interface Stats

EEM Scripts

Hypervisor
NFVIS

- NFVIS supports REST and NETCONF APIs that can be used to export all Host and VNF specific information
- CLIs are also available to monitor and export data
- All data is exported via NETCONF. Need a NETCONF client to receive data
- Host and Interface SNMP MIBS support added as part of 3.6.1 release (July 2017)
- Exporting to external Syslog support added as part of 3.6.1 release (July 2017)

Hardware
ENCS

- Monitoring via Cisco Integrated Management Controller for Platforms that support it.
- CIMC supports an exhaustive list of MIBS which can be used to monitor every aspect of the underlying hardware
- CPU, Memory, Interface and Disk Stats

vAanalytics
cFlowD
Netflow

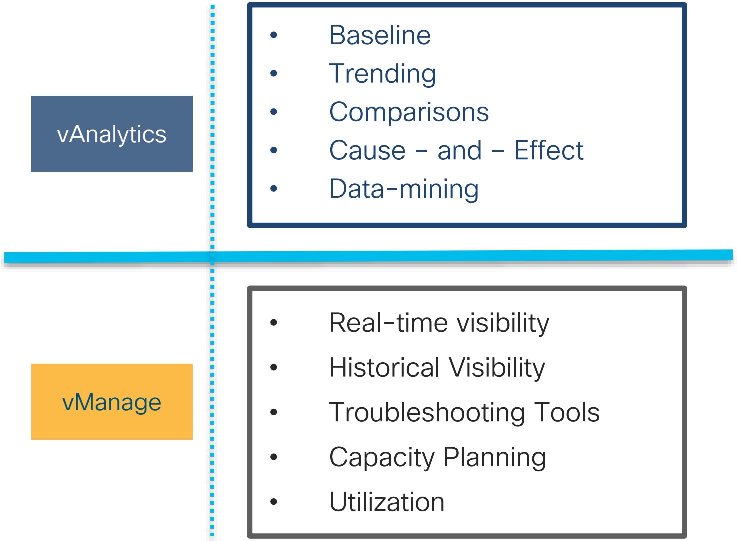
vAnalytics Overview

Analytics

- Offered only As-a-Service
- Multi-customer sourced data
- Anonymous Data-collection
- Reports for Customers, Partners & Viptela

Licensing

- Part of Enterprise License



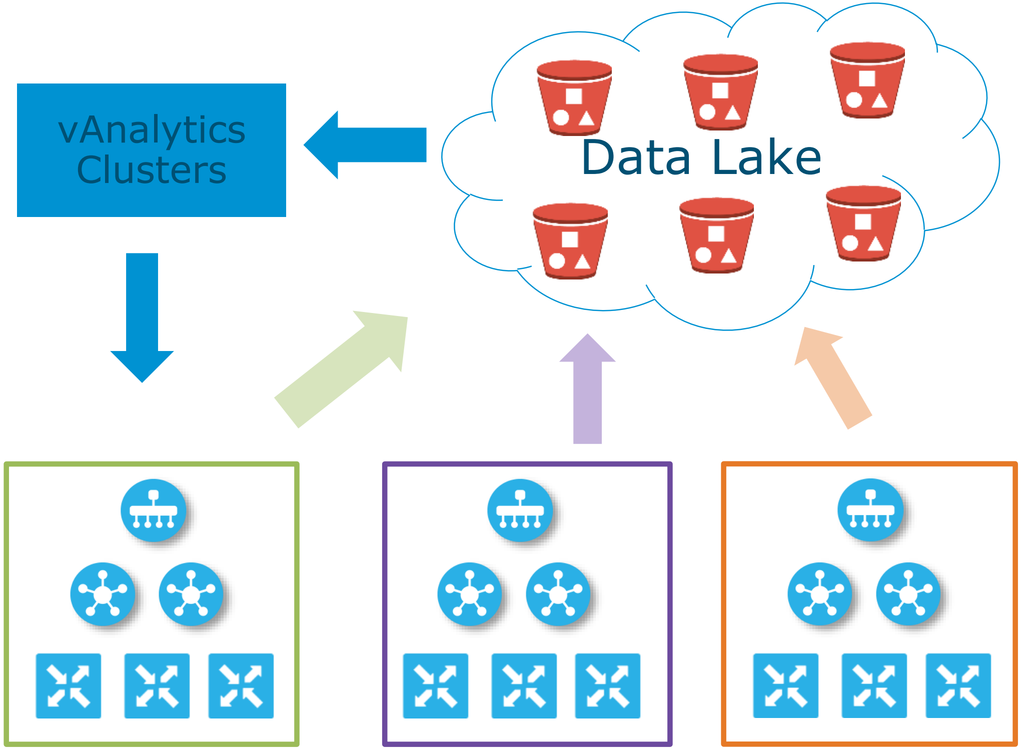
vAnalytics

- Baseline
- Trending
- Comparisons
- Cause – and – Effect
- Data-mining

vManage

- Real-time visibility
- Historical Visibility
- Troubleshooting Tools
- Capacity Planning
- Utilization

vAnalytics – Customer Data



Data Transfer and Storage

- Client authenticated and data securely transmitted from vManage to vAnalytics
- Data storage isolation between customers
- No PII (Personal Identifiable Information) is collected

Data Correlation and Algorithms

- Only management data (stats, flows) information collected
- All algorithms visualization done on a per-customer basis
- IP Addresses collected for provider look-ups
- Peer benchmarking (future use cases) only on a group basis. No individual customer data used

vAnalytics Main Characteristics

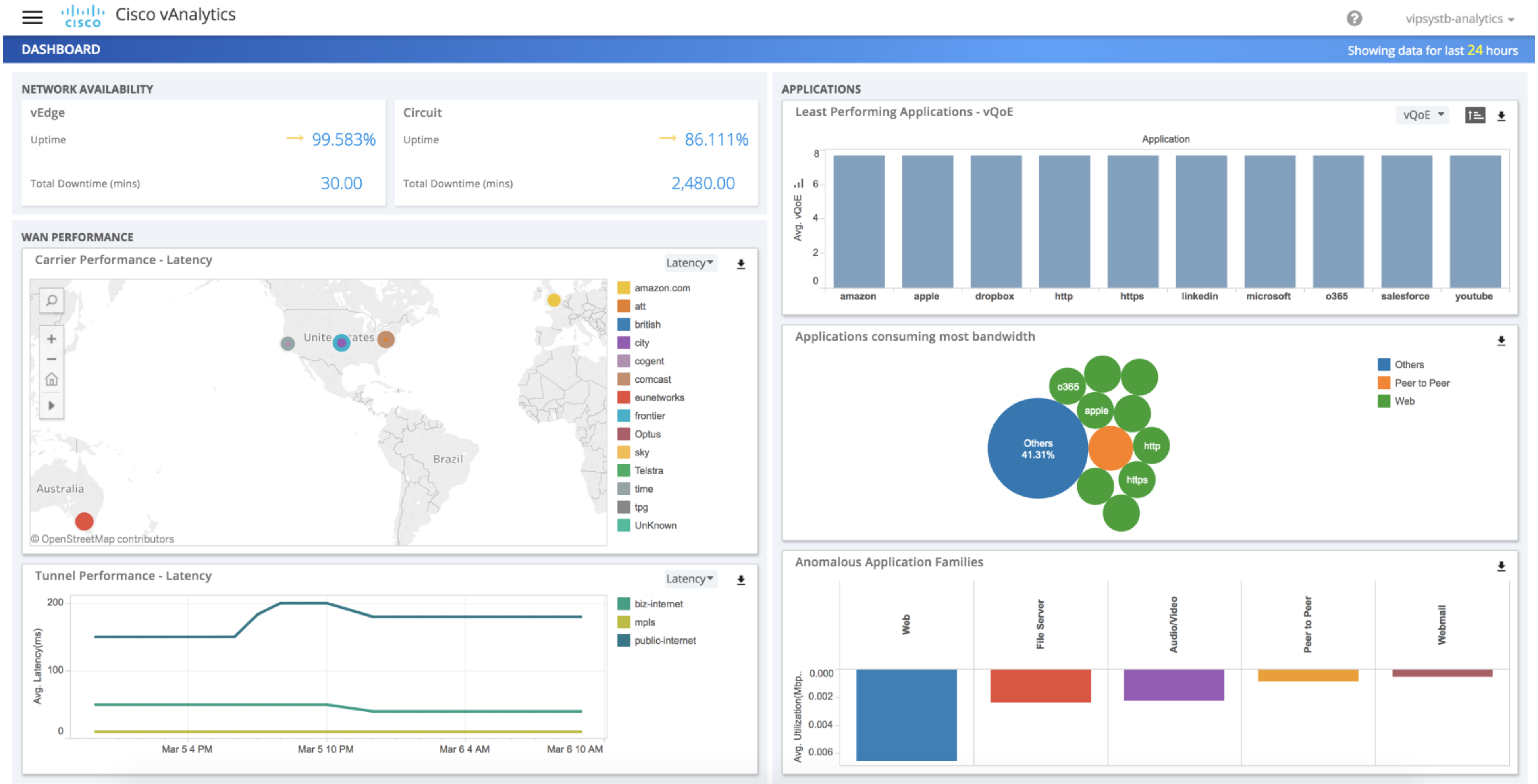
Network Centric

- Site Availability
- Network Availability
- Site Usage Analysis
  - Top sites by bandwidth consumption
  - Historical bandwidth consumption
- Carrier Performance
  - Approute stats on a per-carrier basis
  - Carriers health ranking

Application/Flow Centric

- Based on DPI and cflowd
- Bandwidth Usage
  - Top sources, destinations, apps
  - Per-Site basis
- Application Performance
  - Application to tunnel binding and performance information
- Anomaly Detection
  - Baseline of application usage
  - Anomaly detection based on overall application usage (by application family, by site)

vAnalytics Main Dashboard



Cisco vAnalytics

vipsystb-analytics

DASHBOARD

Showing data for last 24 hours

NETWORK AVAILABILITY

vEdge

Uptime → 99.583%

Total Downtime (mins) 30.00

Circuit

Uptime → 86.111%

Total Downtime (mins) 2,480.00

WAN PERFORMANCE

Carrier Performance - Latency

Latency

Tunnel Performance - Latency

Latency

APPLICATIONS

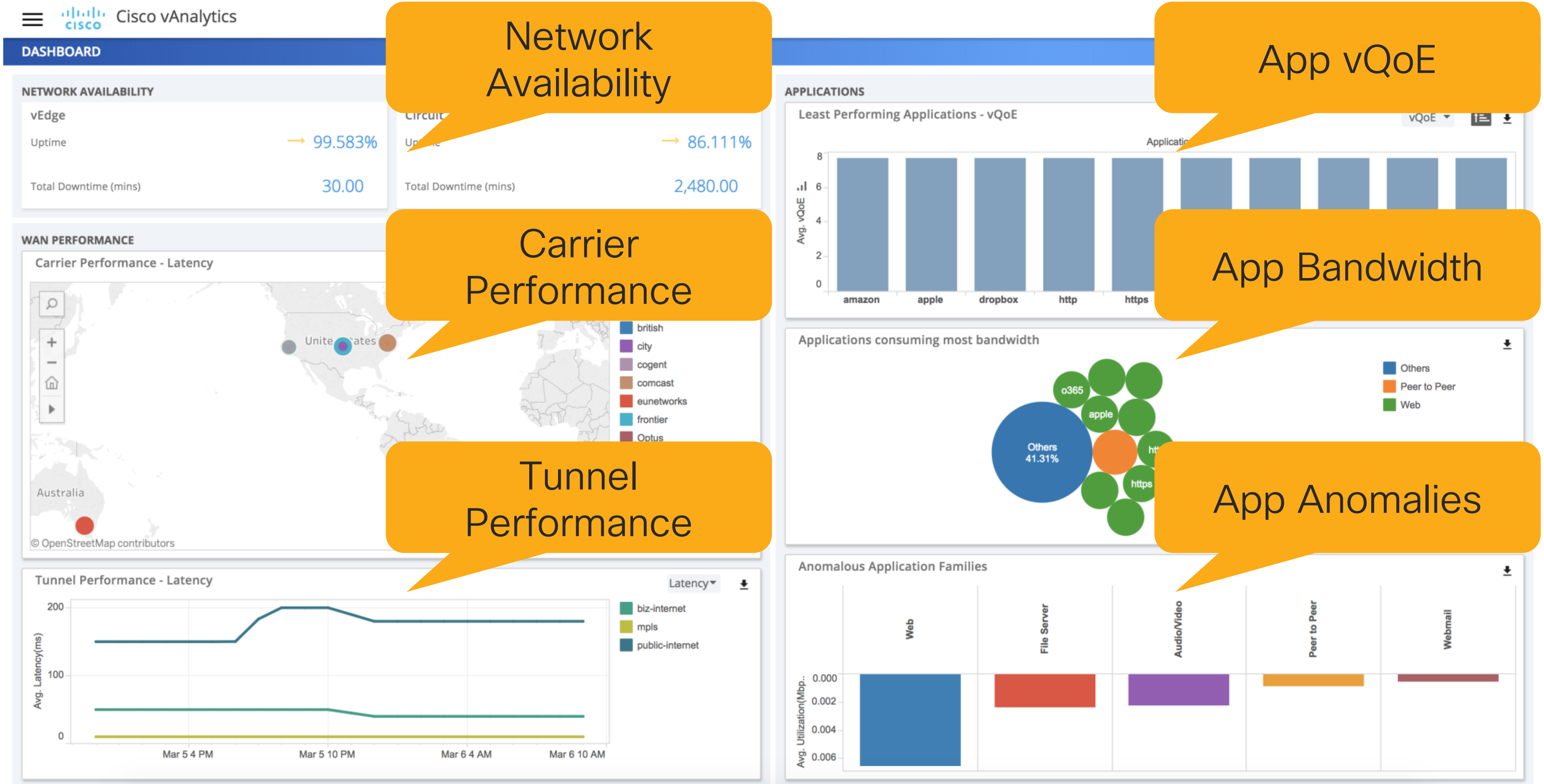
Least Performing Applications - vQoE

vQoE

Applications consuming most bandwidth

Anomalous Application Families

vAnalytics Main Dashboard



Network Availability

Carrier Performance

Tunnel Performance

App vQoE

App Bandwidth

App Anomalies

Cisco vAnalytics

DASHBOARD

NETWORK AVAILABILITY

vEdge

Uptime → 99.583%

Total Downtime (mins) 30.00

Circuit

Up... → 86.111%

Total Downtime (mins) 2,480.00

WAN PERFORMANCE

Carrier Performance - Latency

Tunnel Performance - Latency

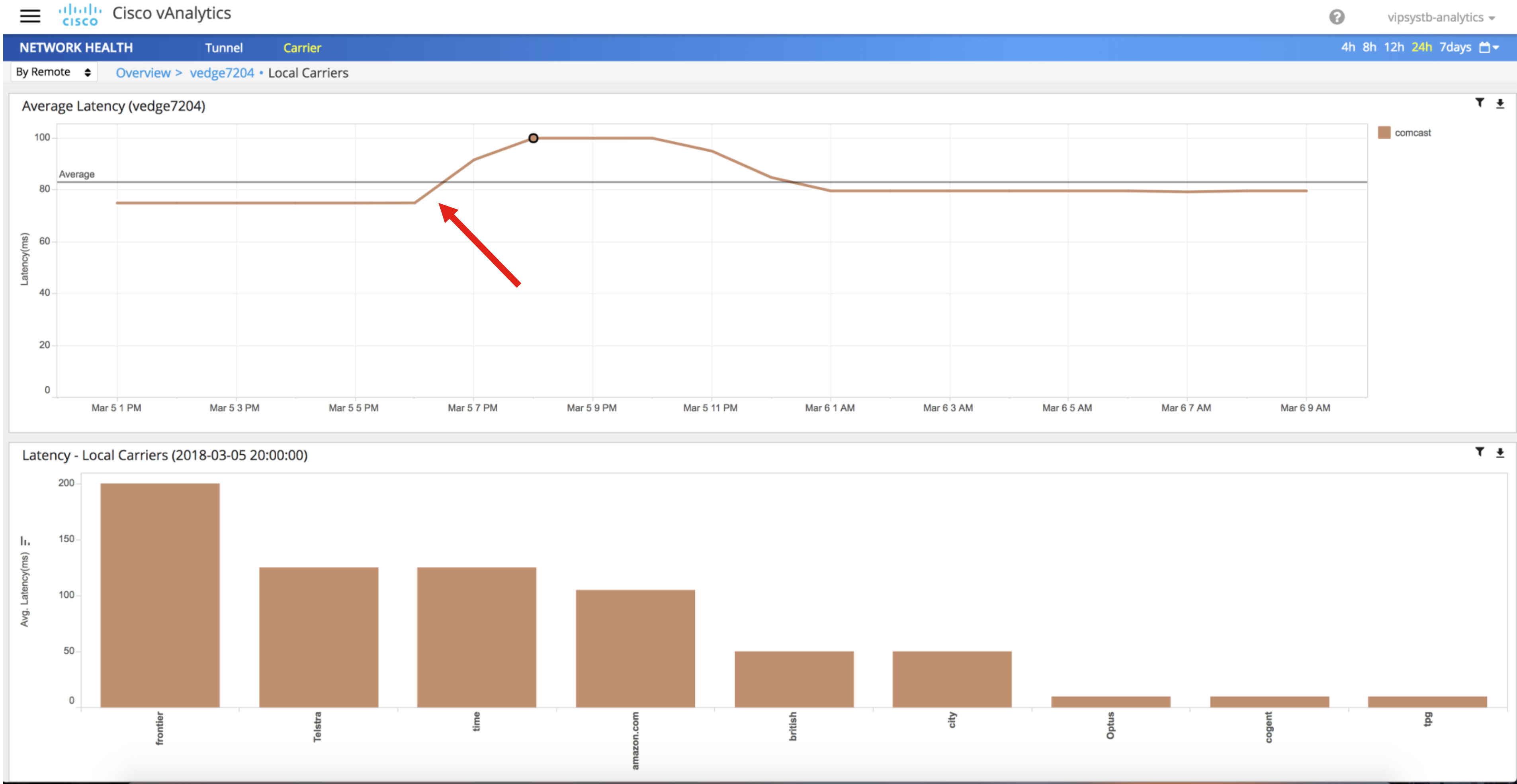
APPLICATIONS

Least Performing Applications - vQoE

Applications consuming most bandwidth

Anomalous Application Families

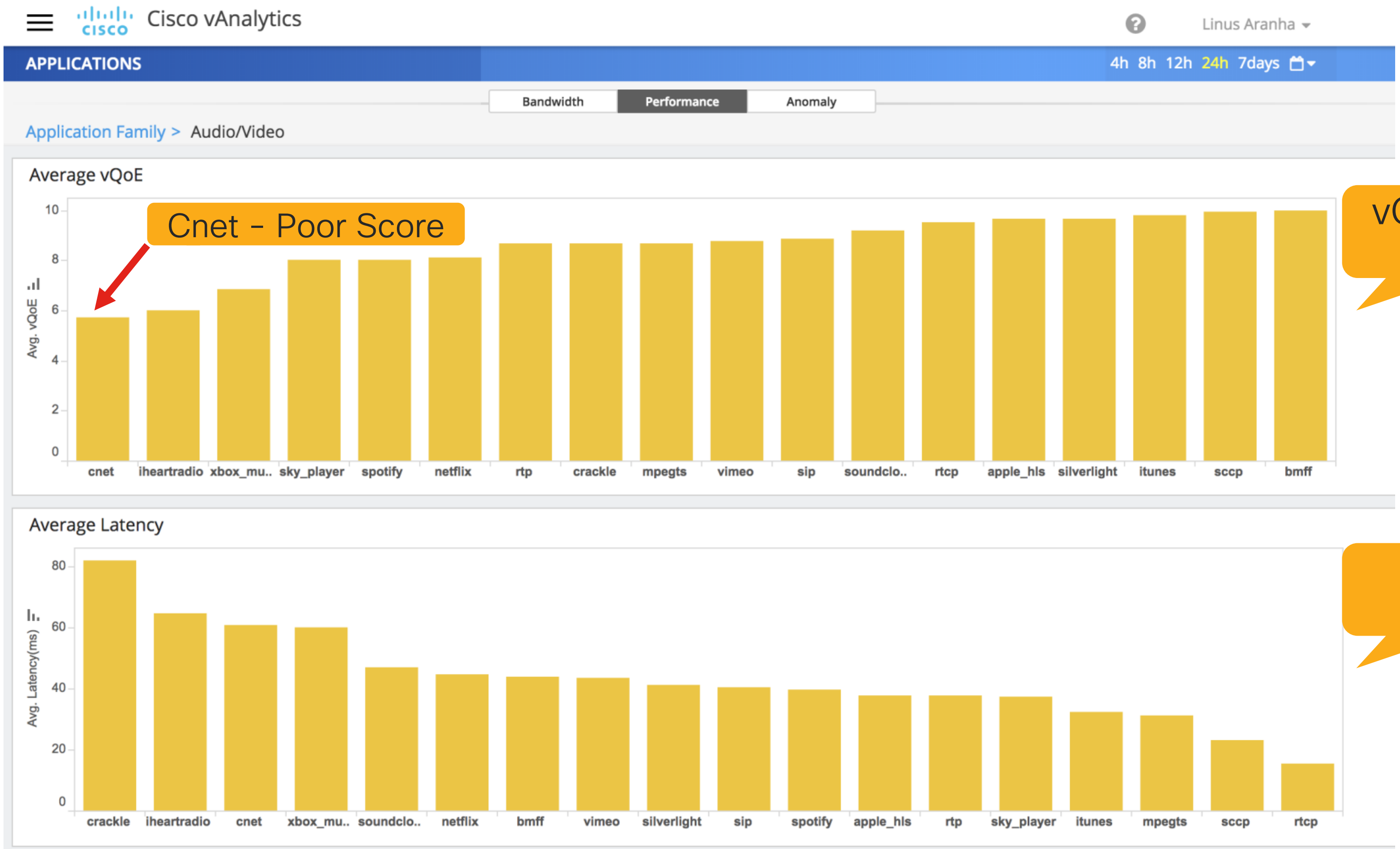
Carrier Performance & Latency



Average Latency (vedge7204)

Latency - Local Carriers (2018-03-05 20:00:00)

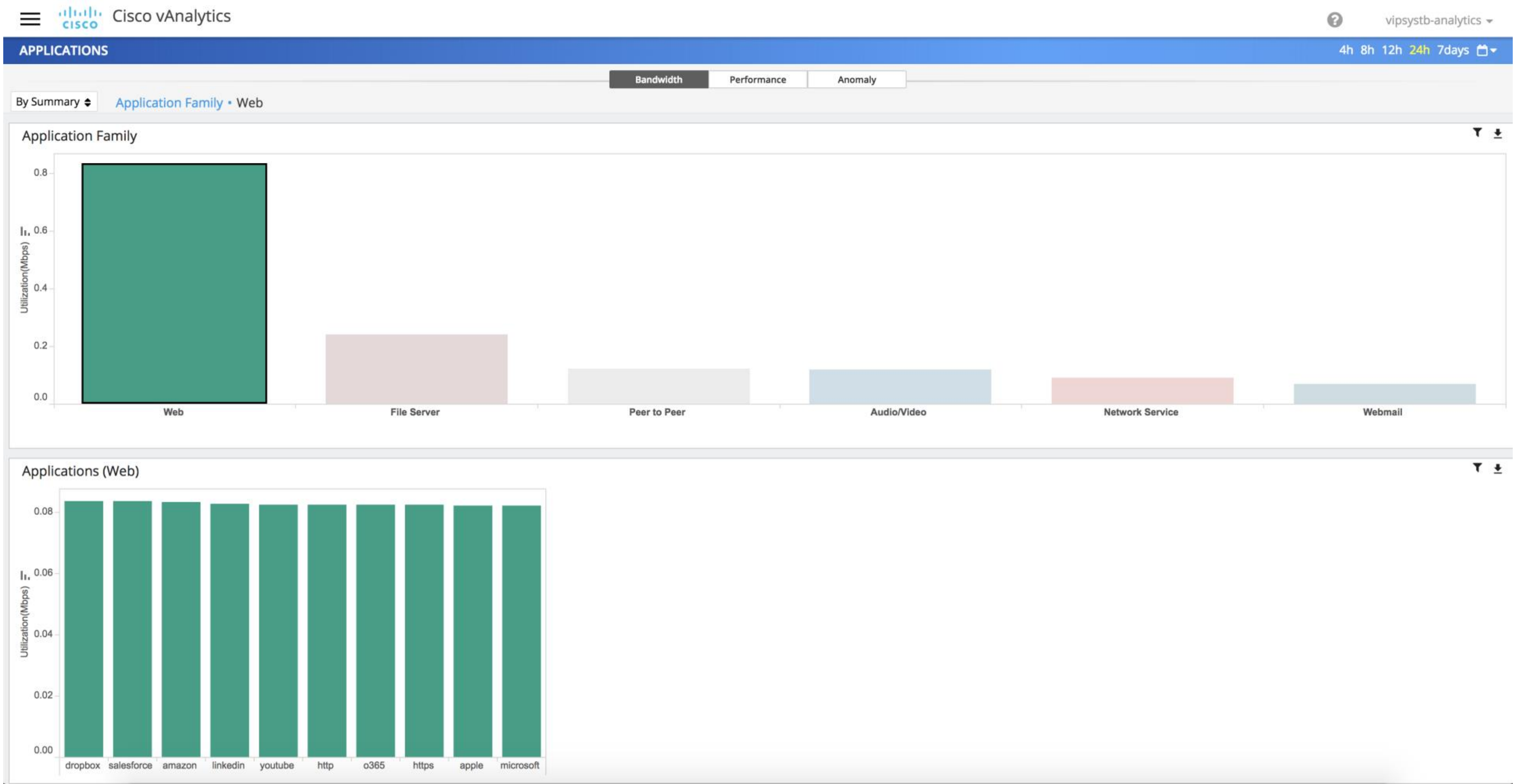
Application vQoE Score



vQoE Score 1 - 10

Latency

Application Bandwidth – Web Apps Drilldown



Cisco Enterprise NFV and Programmable API

NFVIS Programmability REST and NETCONF API

Life Cycle Management

VNF image registration

VNF deployment and update

VNF operations

VNF status and monitoring

Networking

Bridge and port association

Network and bridge association

Service Chain

Status

Monitoring and Debugging

Host system statistic

VNF statistics

Debug logs

Others

Host user management

Host settings

Platform details

Host system reboot

REST API’s

REST Web service

- What is REST?
  - REpresentational State Transfer (REST)
  - API framework built on HTTP
- What is a REST Web Service?
  - REST is architecture style for designing networked applications.
  - Popular due to performance, scale, simplicity, and reliability

GET

POST

PUT

DELETE

{REST}

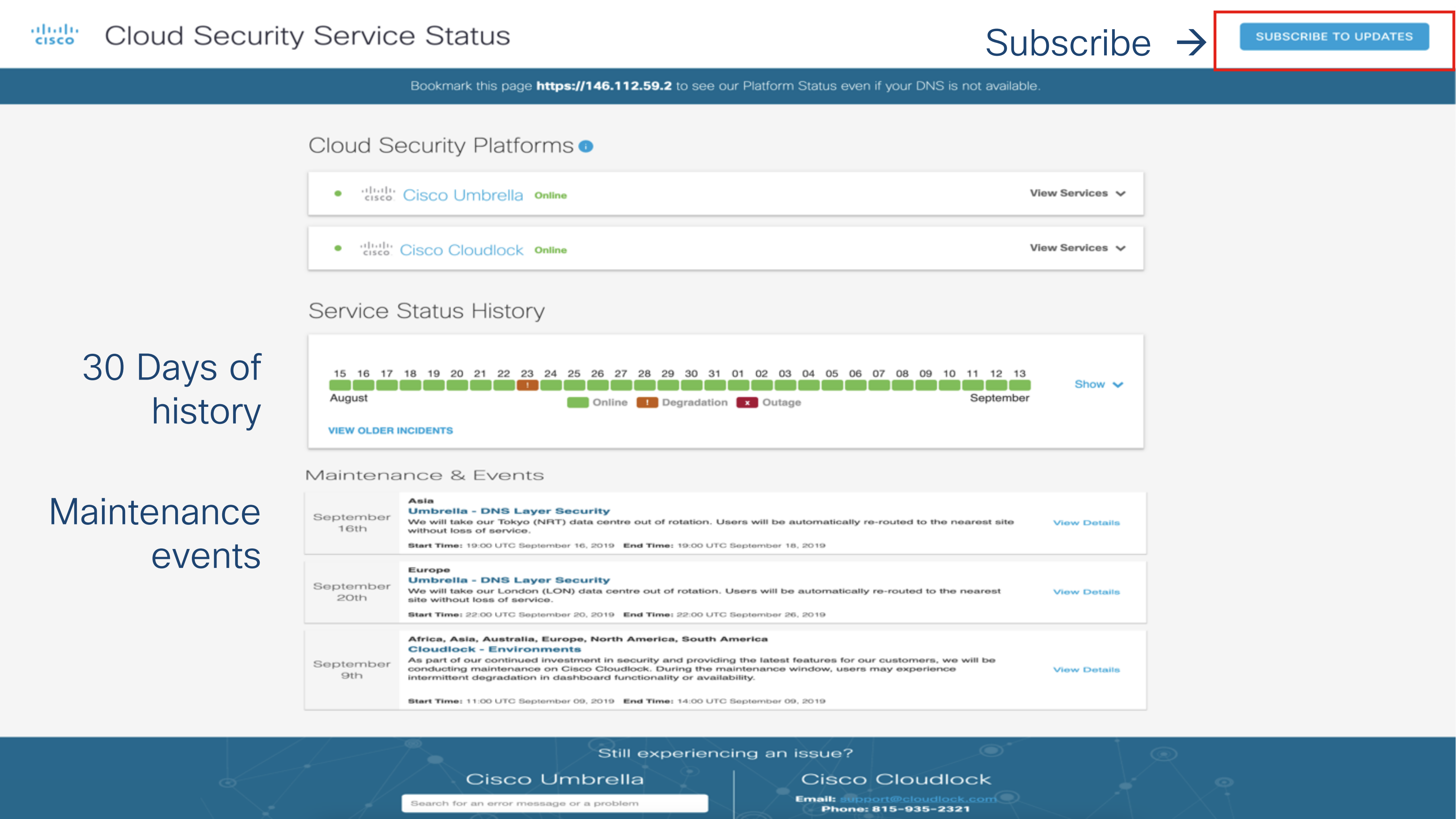
API categories

Device Action	**Certificate Management**	**Troubleshooting Tools**
Device Inventory	**Monitoring**	**Cross-Domain Integration API's**
Configuration	**Real-Time Monitoring**	

- Example URI’s: /certificate
- Example URI’s: /alarms, /statistics , /event
- Example URI’s: /device/app-route/statistics , /device/bfd/status
- Example URI’s: /device/action/software , /device/tools/ping/
- Example URI’s: /partner (Cross-Domain Integration API’s)

Umbrella SIG

Monitoring, Troubleshooting Logging



Cloud Security Service Status

Subscribe →

SUBSCRIBE TO UPDATES

Bookmark this page **https://146.112.59.2** to see our Platform Status even if your DNS is not available.

Cloud Security Platforms

● Cisco Umbrella **Online** — View Services

● Cisco Cloudlock **Online** — View Services

Service Status History

30 Days of history

15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 01 02 03 04 05 06 07 08 09 10 11 12 13

August — September

Show

🟩 Online ! Degradation x Outage

VIEW OLDER INCIDENTS

Maintenance & Events

Maintenance events

September 16th

Asia

Umbrella - DNS Layer Security

We will take our Tokyo (NRT) data centre out of rotation. Users will be automatically re-routed to the nearest site without loss of service.

Start Time: 19:00 UTC September 16, 2019 **End Time:** 19:00 UTC September 18, 2019

View Details

September 20th

Europe

Umbrella - DNS Layer Security

We will take our London (LON) data centre out of rotation. Users will be automatically re-routed to the nearest site without loss of service.

Start Time: 22:00 UTC September 20, 2019 **End Time:** 22:00 UTC September 26, 2019

View Details

September 9th

Africa, Asia, Australia, Europe, North America, South America

Cloudlock - Environments

As part of our continued investment in security and providing the latest features for our customers, we will be conducting maintenance on Cisco Cloudlock. During the maintenance window, users may experience intermittent degradation in dashboard functionality or availability.

Start Time: 11:00 UTC September 09, 2019 **End Time:** 14:00 UTC September 09, 2019

View Details

Still experiencing an issue?

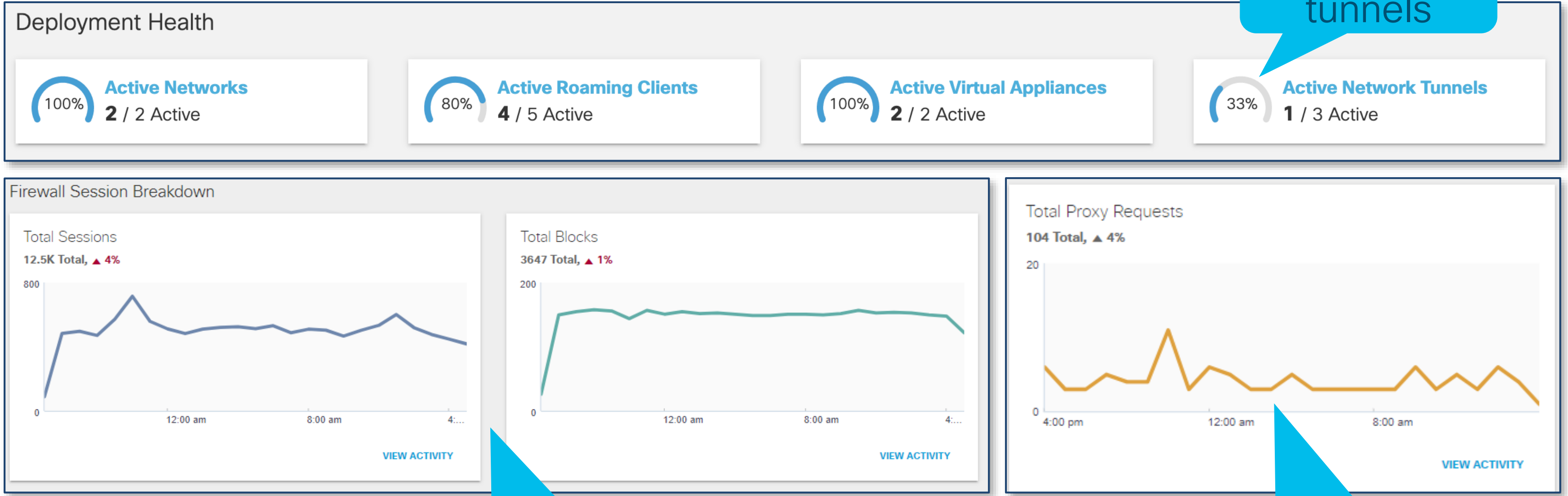
Cisco Umbrella

Search for an error message or a problem

Cisco Cloudlock

Email: support@cloudlock.com
Phone: 815-935-2321

Umbrella SIG Network Breakdown



Deployment Health

Active Networks
2 / 2 Active

Active Roaming Clients
4 / 5 Active

Active Virtual Appliances
2 / 2 Active

Active Network Tunnels
1 / 3 Active

Firewall Session Breakdown

Total Sessions
12.5K Total, ▲ 4%

Total Blocks
3647 Total, ▲ 1%

Total Proxy Requests
104 Total, ▲ 4%

Active tunnels

Firewall

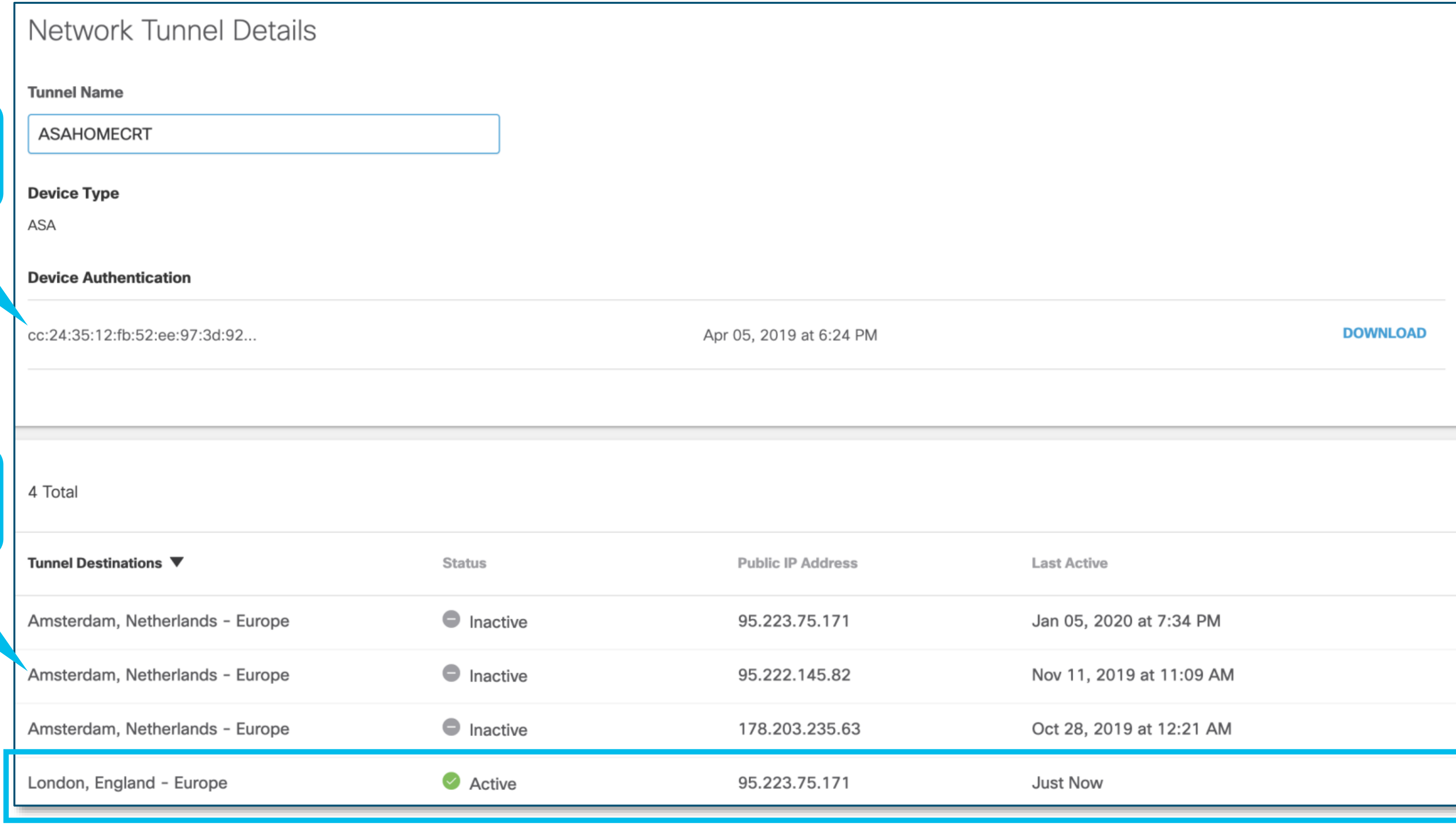
Secure Web Gateway

- Active Networks and Active Network Tunnels
- Proxy requests
- Firewall session breakdowns

Troubleshooting IPsec Tunnel

Tunnel information

Tunnel history and status



Network Tunnel Details

Tunnel Name

ASAHOMECRT

Device Type

ASA

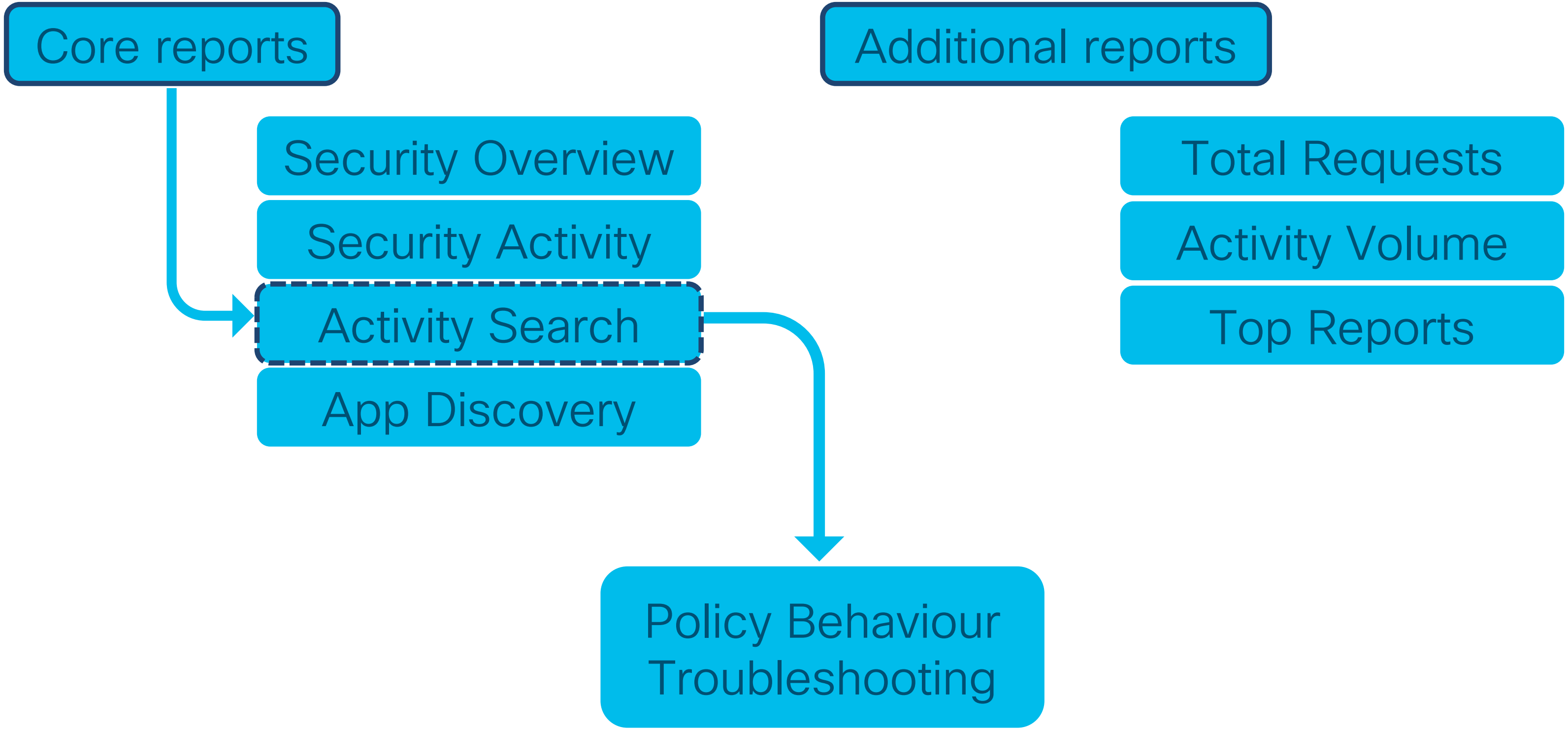
Device Authentication

cc:24:35:12:fb:52:ee:97:3d:92... Apr 05, 2019 at 6:24 PM DOWNLOAD

4 Total

Tunnel Destinations ▼	Status	Public IP Address	Last Active
Amsterdam, Netherlands - Europe	⊖ Inactive	95.223.75.171	Jan 05, 2020 at 7:34 PM
Amsterdam, Netherlands - Europe	⊖ Inactive	95.222.145.82	Nov 11, 2019 at 11:09 AM
Amsterdam, Netherlands - Europe	⊖ Inactive	178.203.235.63	Oct 28, 2019 at 12:21 AM
London, England - Europe	✓ Active	95.223.75.171	Just Now

Umbrella Traffic Reporting



Core reports

Security Overview

Security Activity

Activity Search

App Discovery

Additional reports

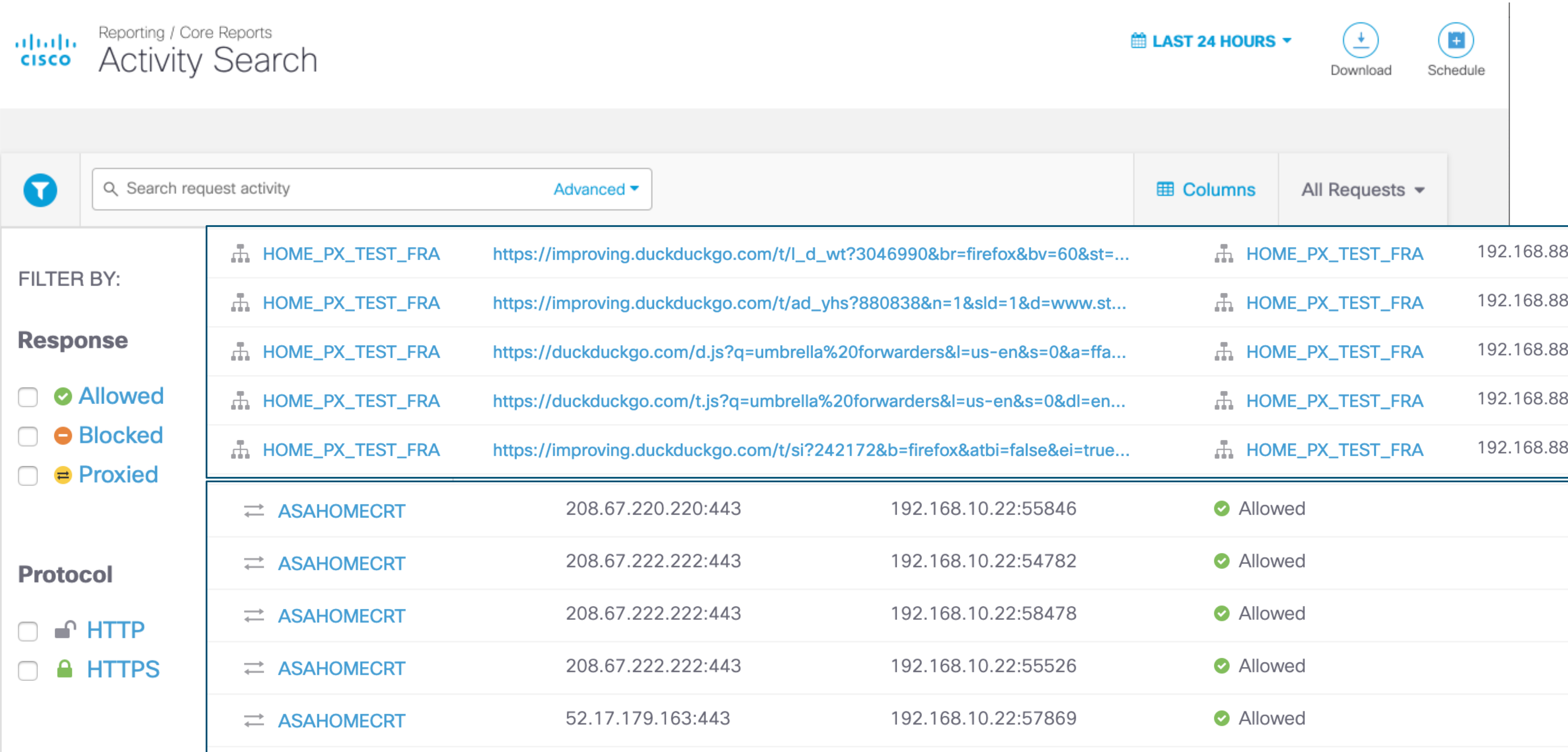
Total Requests

Activity Volume

Top Reports

Policy Behaviour Troubleshooting

Troubleshooting Policy



Activity Search

FILTER BY:

Response

□ Allowed
□ Blocked
□ Proxied

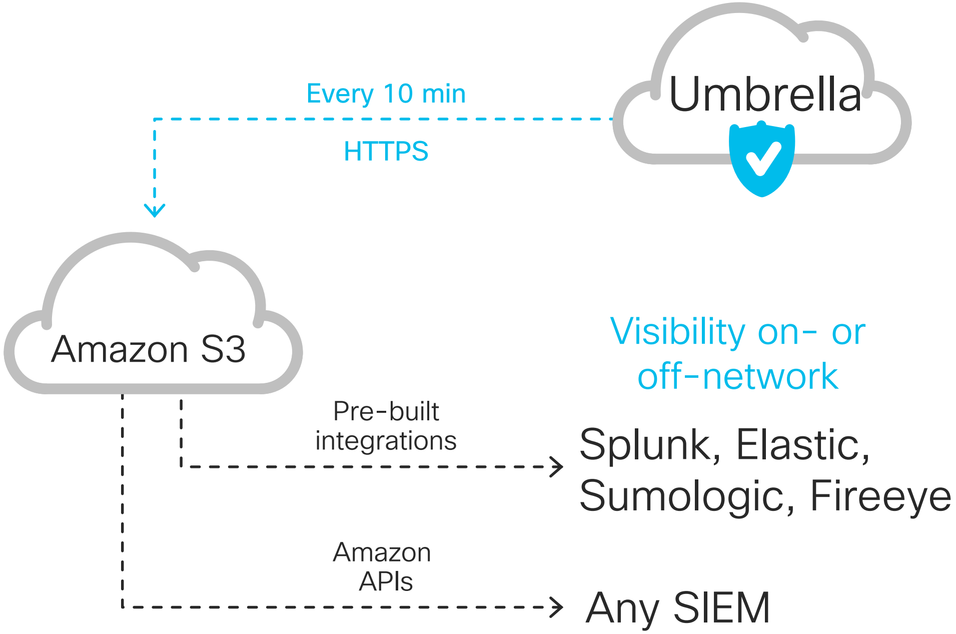
Protocol

□ HTTP
□ HTTPS

HOME_PX_TEST_FRA	https://improving.duckduckgo.com/t/l_d_wt?3046990&br=firefox&bv=60&st=...	HOME_PX_TEST_FRA	192.168.88
HOME_PX_TEST_FRA	https://improving.duckduckgo.com/t/ad_yhs?880838&n=1&sld=1&d=www.st...	HOME_PX_TEST_FRA	192.168.88
HOME_PX_TEST_FRA	https://duckduckgo.com/d.js?q=umbrella%20forwarders&l=us-en&s=0&a=ffa...	HOME_PX_TEST_FRA	192.168.88
HOME_PX_TEST_FRA	https://duckduckgo.com/t.js?q=umbrella%20forwarders&l=us-en&s=0&dl=en...	HOME_PX_TEST_FRA	192.168.88
HOME_PX_TEST_FRA	https://improving.duckduckgo.com/t/si?242172&b=firefox&atbi=false&ei=true...	HOME_PX_TEST_FRA	192.168.88

ASAHOMECRT	208.67.220.220:443	192.168.10.22:55846	✓ Allowed
ASAHOMECRT	208.67.222.222:443	192.168.10.22:54782	✓ Allowed
ASAHOMECRT	208.67.222.222:443	192.168.10.22:58478	✓ Allowed
ASAHOMECRT	208.67.222.222:443	192.168.10.22:55526	✓ Allowed
ASAHOMECRT	52.17.179.163:443	192.168.10.22:57869	✓ Allowed

Log storage with Amazon S3



S3 Benefits

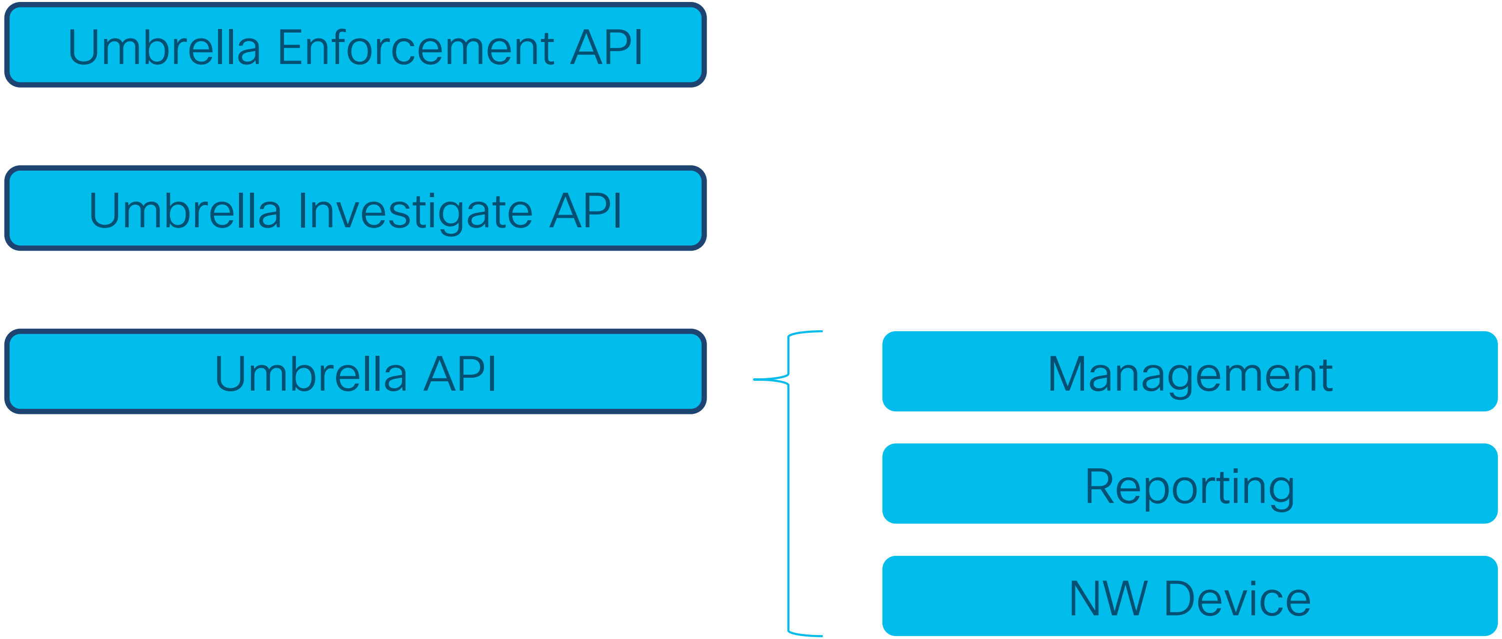
Triple redundant and encrypted storage

Pre-built SIEM / log analytic integrations

Use self-managed or Cisco-managed bucket

Centrally managed S3 logs

Using APIs



Umbrella Enforcement API

Umbrella Investigate API

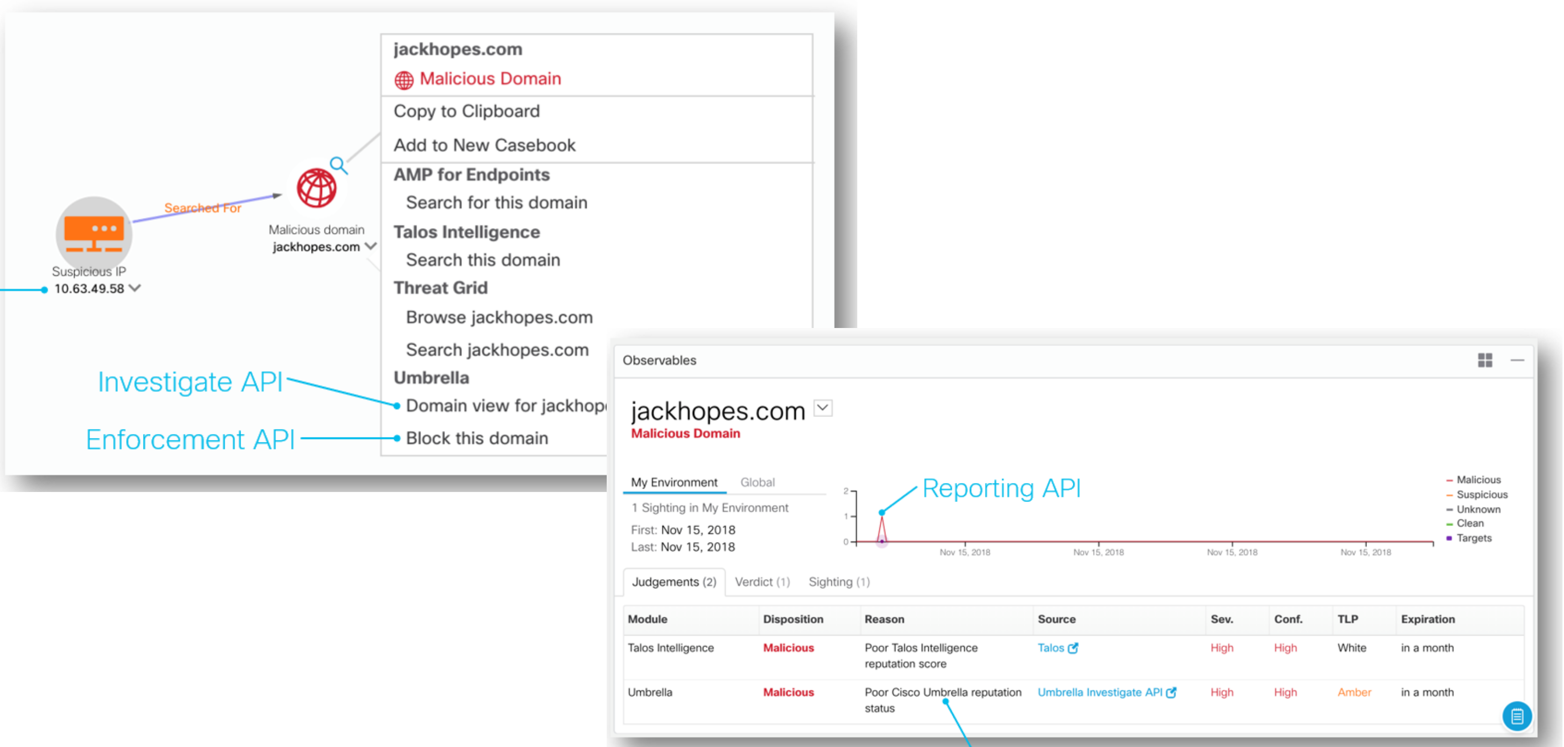
Umbrella API

Management

Reporting

NW Device

Cisco Threat Response and Umbrella



Module	Disposition	Reason	Source	Sev.	Conf.	TLP	Expiration
Talos Intelligence	Malicious	Poor Talos Intelligence reputation score	Talos	High	High	White	in a month
Umbrella	Malicious	Poor Cisco Umbrella reputation status	Umbrella Investigate API	High	High	Amber	in a month

Reporting API

Investigate API

Enforcement API

Reporting API

Investigate API

Key Takeaways

Start the journey

SD WAN   Umbrella   Automate

“If you can not explain the problem in three simple sentences, then you do not understand the problem.”

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on 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 Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

You make **possible**