



You make **possible**



Deep Dive into Secure Agile Exchange

Design, Deploy and Debug your Secure Multicloud Access using Automation and Assurance

Dinesh Ranjit, Technical Architect SAE/CSP

Sujay Murthy, NSO Application Team/SAE

TECCLD-2107

CISCO *Live!*

Barcelona | January 27-31, 2020



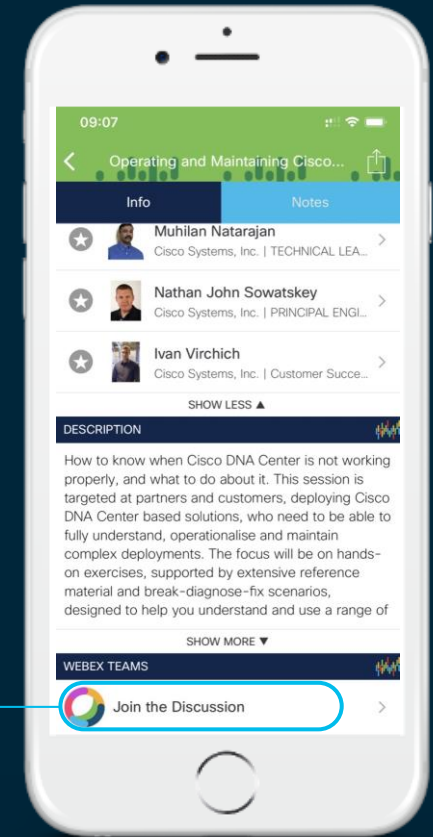
Cisco Webex Teams

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

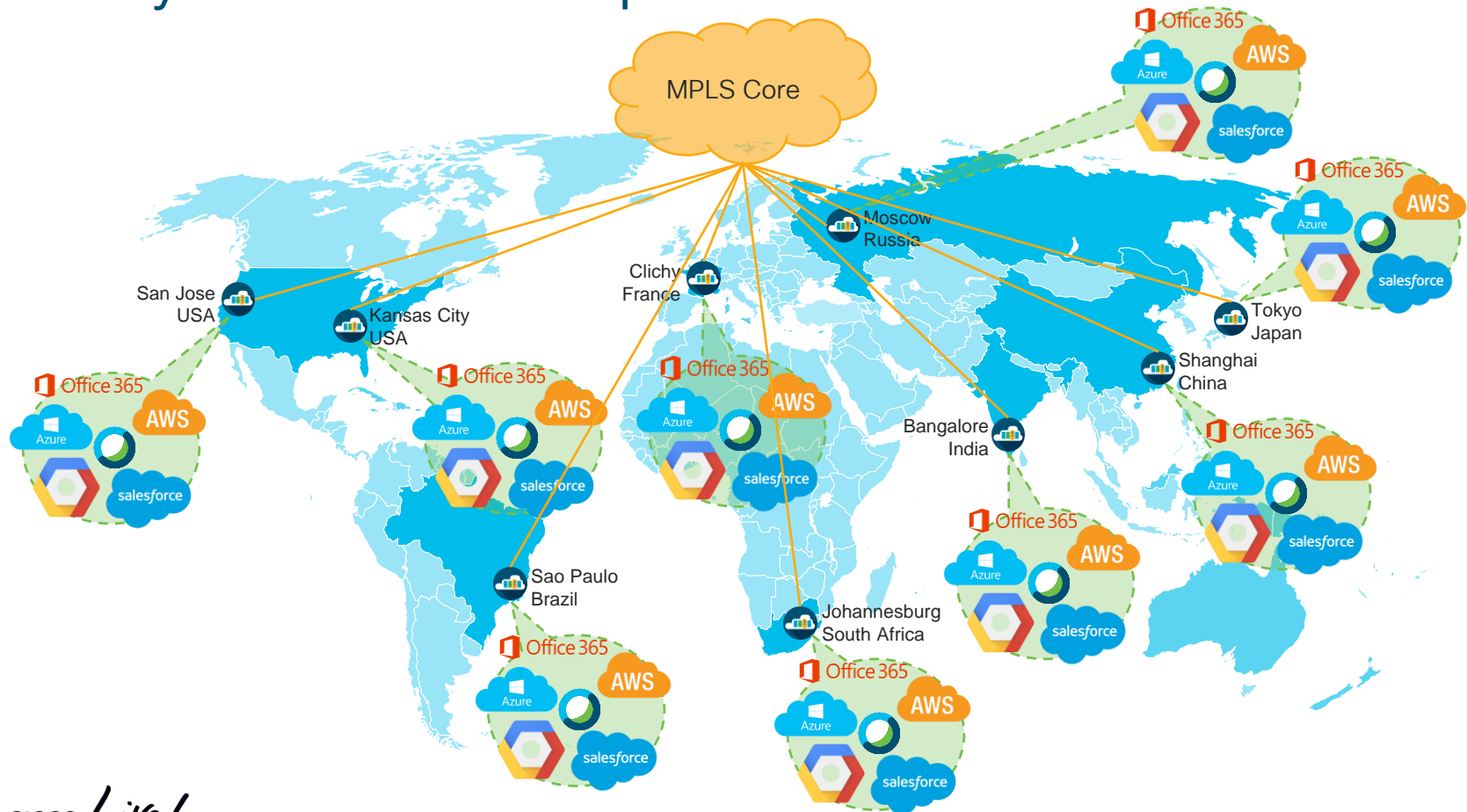


Agenda

- Secure Agile Exchange (SAE) Overview
- SAE Planning
- SAE Design
- SAE Infrastructure
- Break ----
- SAE Deployment
 - End to End Service Chains
 - SAE Assurance and Day2 Service Operation.
 - Shared Endpoint Gateway and Half Service Chains
 - Stitching Service Chains and Shared End Point Gateway
- SAE Debug and Troubleshooting
- SAE Roadmap and References
- SAE Conclusion / Q & A

Secure Agile Exchange (SAE) Overview

Today's Global Enterprise Network



Challenges of multi-cloud access by disparate user groups

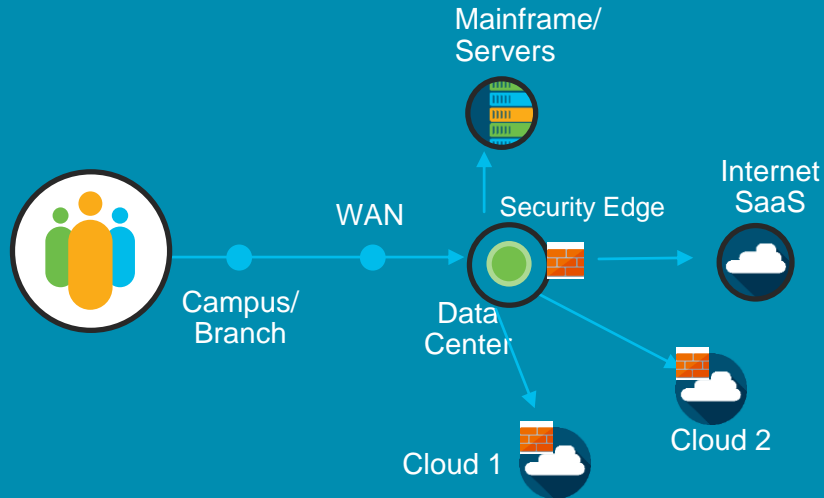


Business Challenges

- Efficient IaaS and SaaS access keeping app SLA intact
- Distributed internet access
- Operationally efficient

Multi-Cloud Access Changes the Network

Data Center Centric



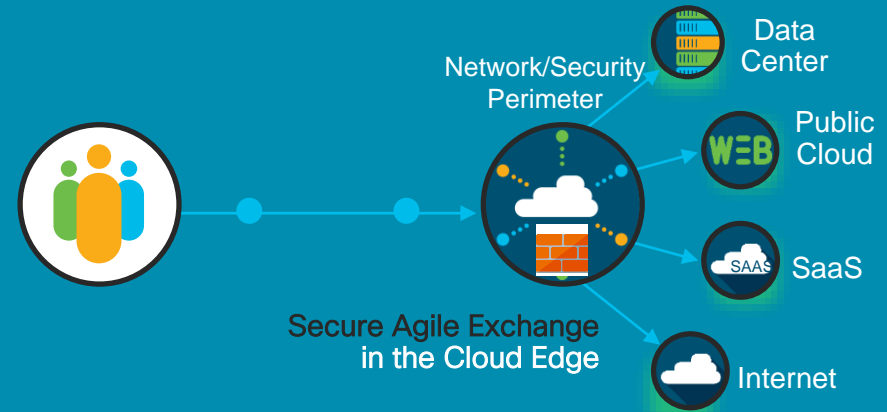
Security challenges for distributed cloud services

Suboptimal routing adds latency (roundtrip)

Multi-Cloud access adds more security services

Network growing in complexity, no scalability

Multi-Cloud Centric with Cloud Edge



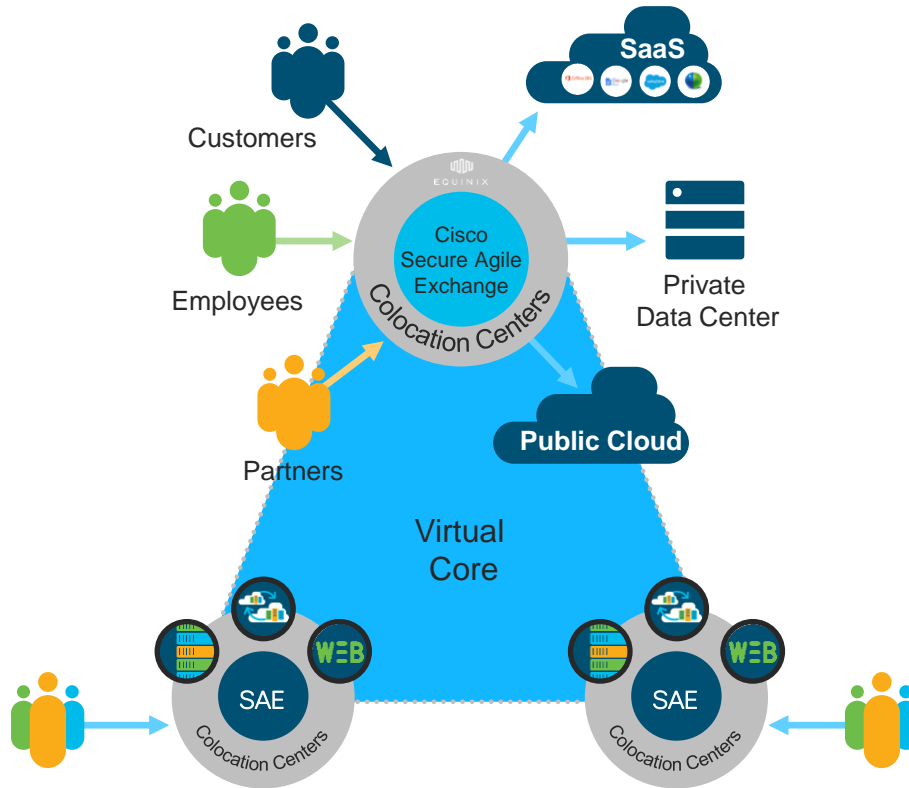
Centralized security and policy management

Lower cloud connectivity charges

Faster provisioning of new cloud based services

Scale for any multicloud environment

Cloud Edge is the New Network Hub



Virtualized network services can be automatically deployed on demand.

Centralized policy management simplifies secure communication between employees, customers, partners.

Reduced Latency improves user experience. Segmentation of flows brings agility to enable connectivity

Create New Virtual Core Network to significantly reduce Transport Costs

Gartner Paper (Aug 2019)

- The legacy data center model is becoming obsolete due to cloud adoption
- Defines SASE (Secure Access Service Edge) (“sassy”).
- “Tromboning” traffic is inefficient and costly, inspection engines should be located closest to the where the data is stored.
- The enterprise network perimeter is no longer a location but more a set of capabilities delivered from the cloud.

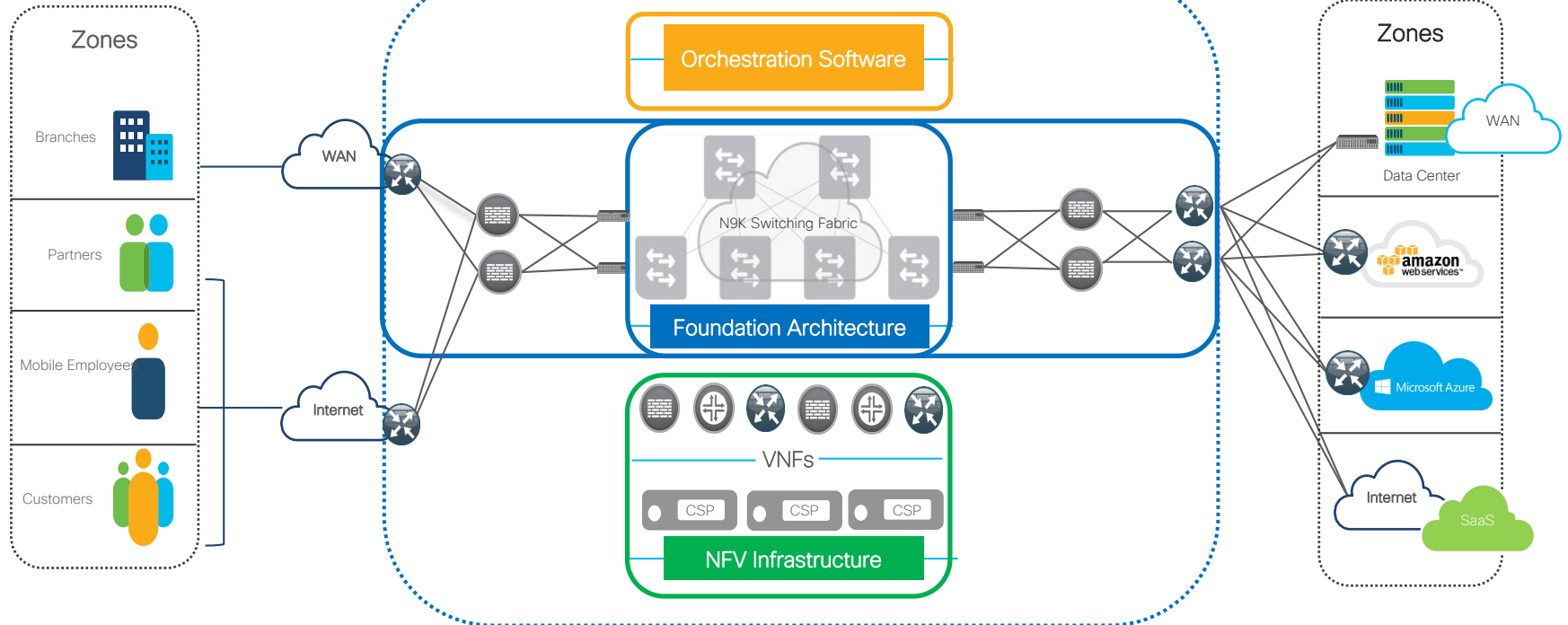
<https://www.gartner.com/en/documents/3953690/market-trends-how-to-win-as-wan-edge-and-security-conver>

Secure Agile Exchange Peering Architecture

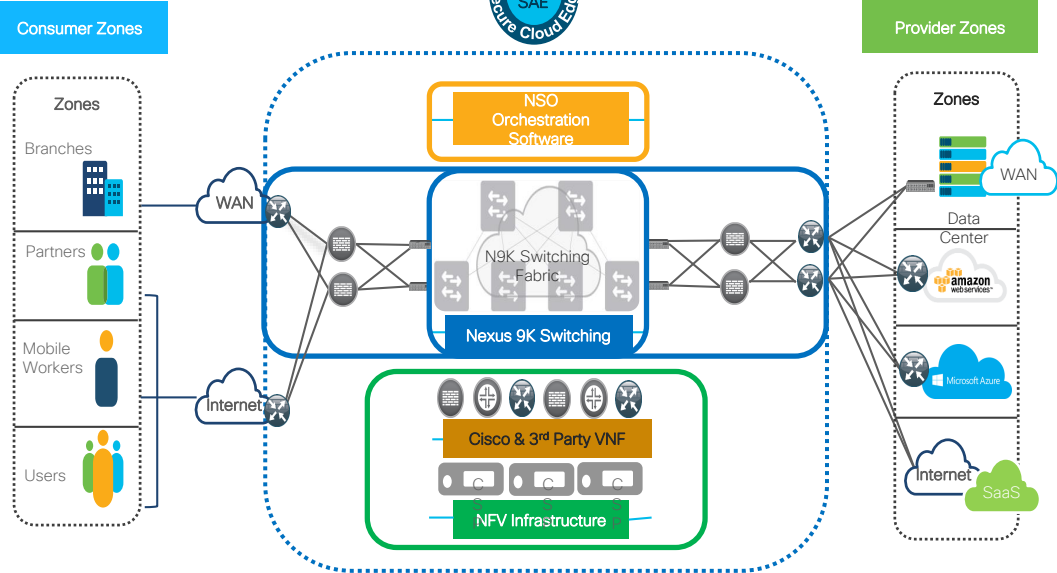


Consumer Zones

Provider Zones



Secure Agile Exchange (SAE)



1. SD-WAN/SD-Branch Neutral

- Support Meraki

2. Design/Policy flexibility

- Route leaking
- Half chains
- Multi-cloud interconnectivity
- Endpoint Add/delete to VNF
- PNF blob(SAE 2.1)*

3. Orchestration support

- NSO license available
- Physical device mgmt
 - OOB switch
 - ASR, FTD
- Day2 automation via NED (separate SKU)

Scale

- N9K/NX-OS
- Leaf pair/VXLAN
- Multi-tenancy
- ACI(SAE 2.1)*

Visibility support

- Netflow/Sflow support
- 3rd party- Netrounds, LiveAction
- NAE, Stealthwatch (ACI 2.1) *

SAE HUB



Architecture Overview:

Global Network Access Points (Hubs)

Utilizing global SAE hubs allows Enterprises to deploy resources in proximity to their user population which reduces latency for digital communication, provide an internet first consumption model, includes both hybrid and multi-cloud usage, and facilitates decreased network traffic through appropriate distribution of the Hubs.

SAE Building Blocks



VNF Hypervisor
Performance Focused
Hardware
CLI, GUI, and API
Driven



Virtual First Focus
Consistent Software
Between Virtual and
Hardware

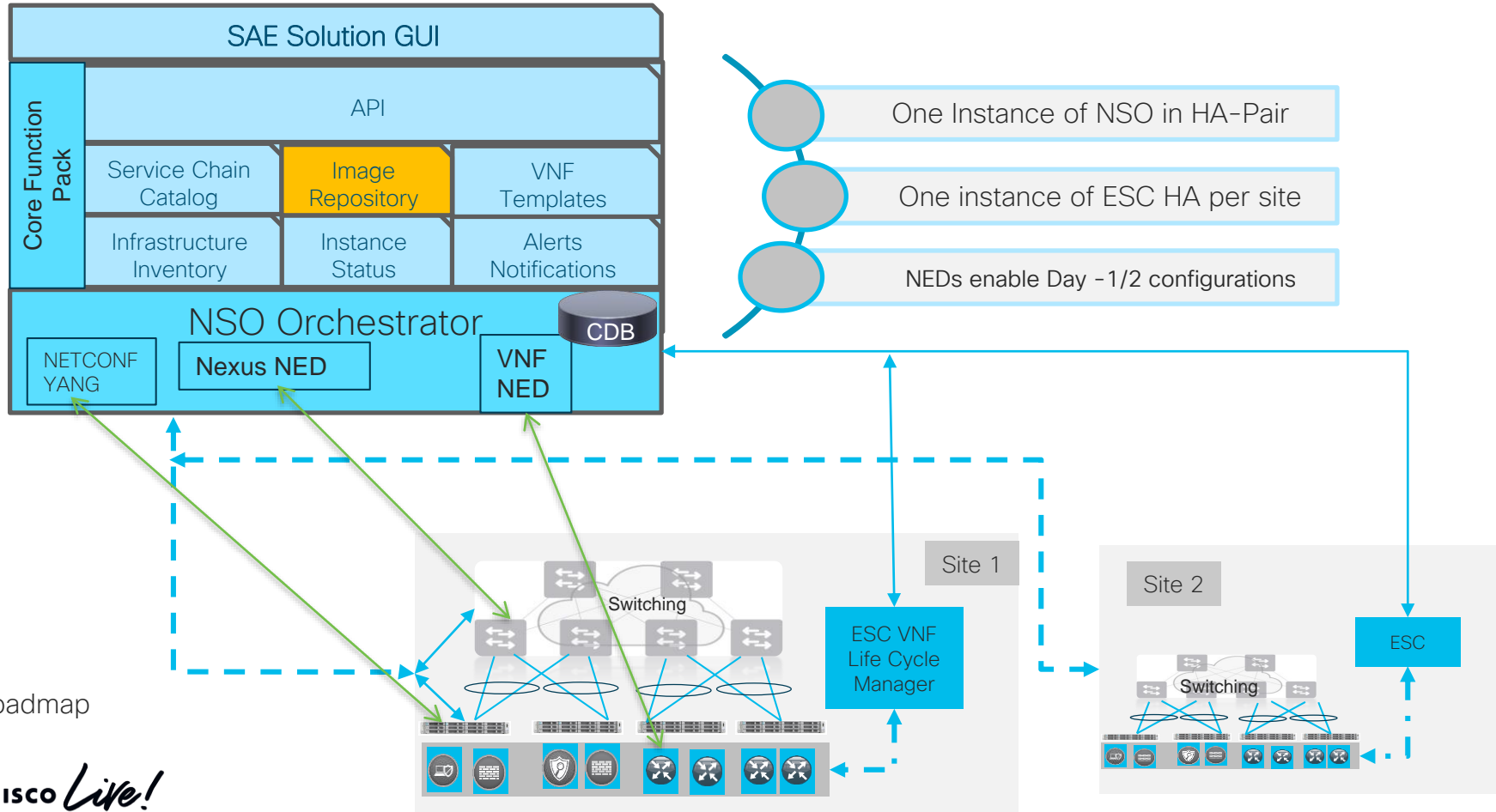


VNF Ready Fabric
Scales From Small to
Large Deployments



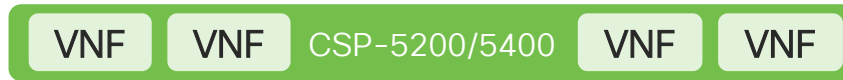
Automate and
Orchestrate Cisco and
3rd Party VNFs
Create Repeatable
Service Chain Models

SAE Solution Stack



 Roadmap

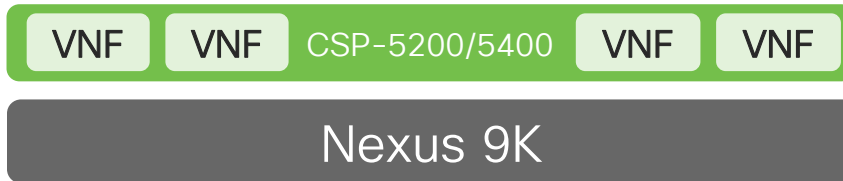
SAE Component Stack



NFV Infrastructure (NFVI)

- Support for any KVM based NFVs (QCOW2)
- Multiple networking options, including OVS DPDK, SRIOV and port-channels
- Hosting Cisco VNFs like CSR, ASA v and FTDv and 3rd party VNFs like Palo Alto, Fortinet as firewall and load balancers like AVI, F5 etc.

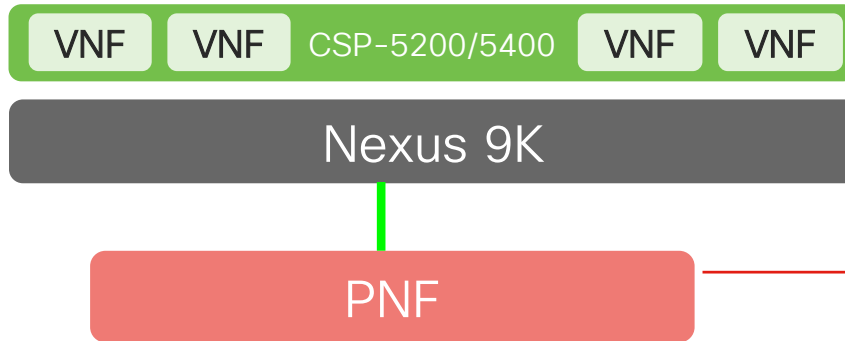
SAE Component Stack



Nexus Fabric

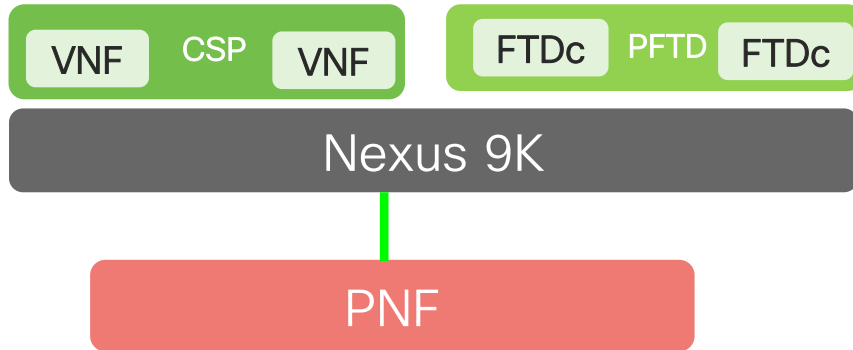
- Nexus Standalone or Spine/Leaf or ACI
- Support for VLAN and/or VXLAN,
- Support for ITD
- Multi-Tenancy with VRFs
- Full redundancy with port-channels and VPC

SAE Component Stack



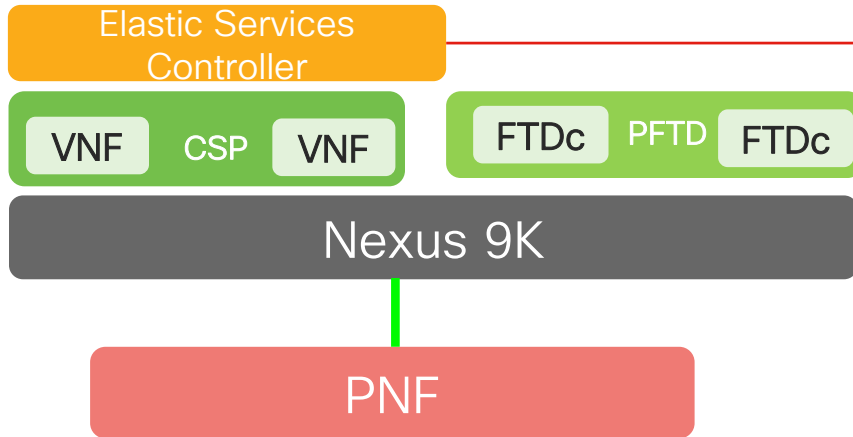
Physical Network Function
Support Physical Device in a SAE Service

SAE Component Stack



Cisco Firepower Appliance
Support Firepower Appliances – 4100/9300
for FTDC deployment in Service Chain

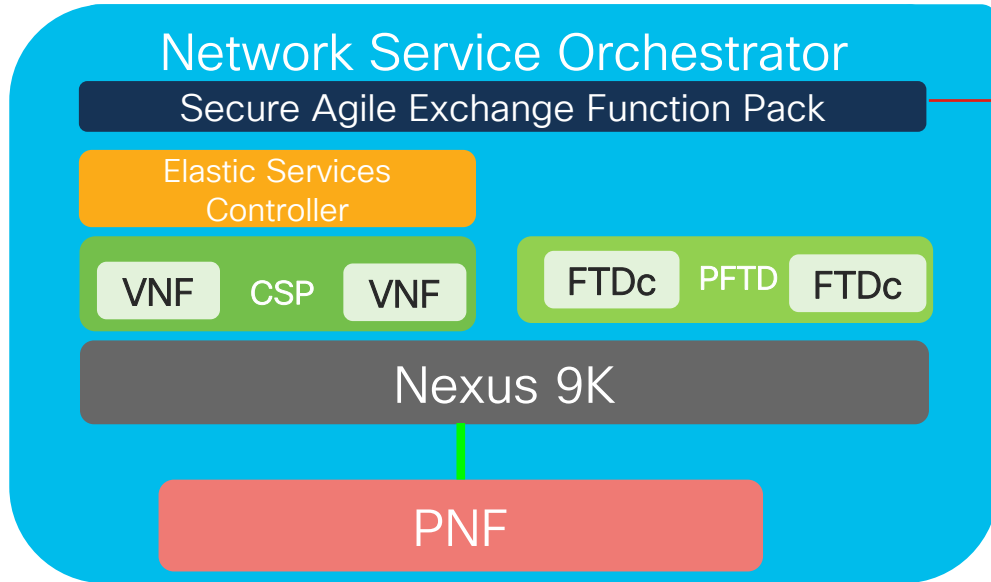
SAE Component Stack



VNF Lifecycle Manager (VNF) Manager

- Instantiate individual and/or groups of VNFs
- Provision Day0 configurations and network objects
- Monitor VNF health and perform recovery

SAE Component Stack



NSO and SAE Core Function Pack

- Model and deploy Service Chains (Day1,Day2)
- Manage Resource Pools (IP, VLAN, VXLAN, Compute, Endpoint Gateway)
- Manage Lifecycle of Service Chains (Create, Re-deploy, Update, Delete)
- Full northbound API support and extensibility (VRFs, Day 2 Policy, etc.)

Cloud Services Platform

CSP 5216/5228

Front View

8[^] SSD or HDD Slots



2 PCIe slots

Rear View



2x10G Ethernet

CIMC / OOB LOM

[^]RAID10 used disks in multiple of 4, only 8 used out of 10 slots
RAID 10 reduces the available storage by half

CSP 5436/5444/5456

Front View

24 SSD or HDD Slots



6 PCIe slots

Rear View



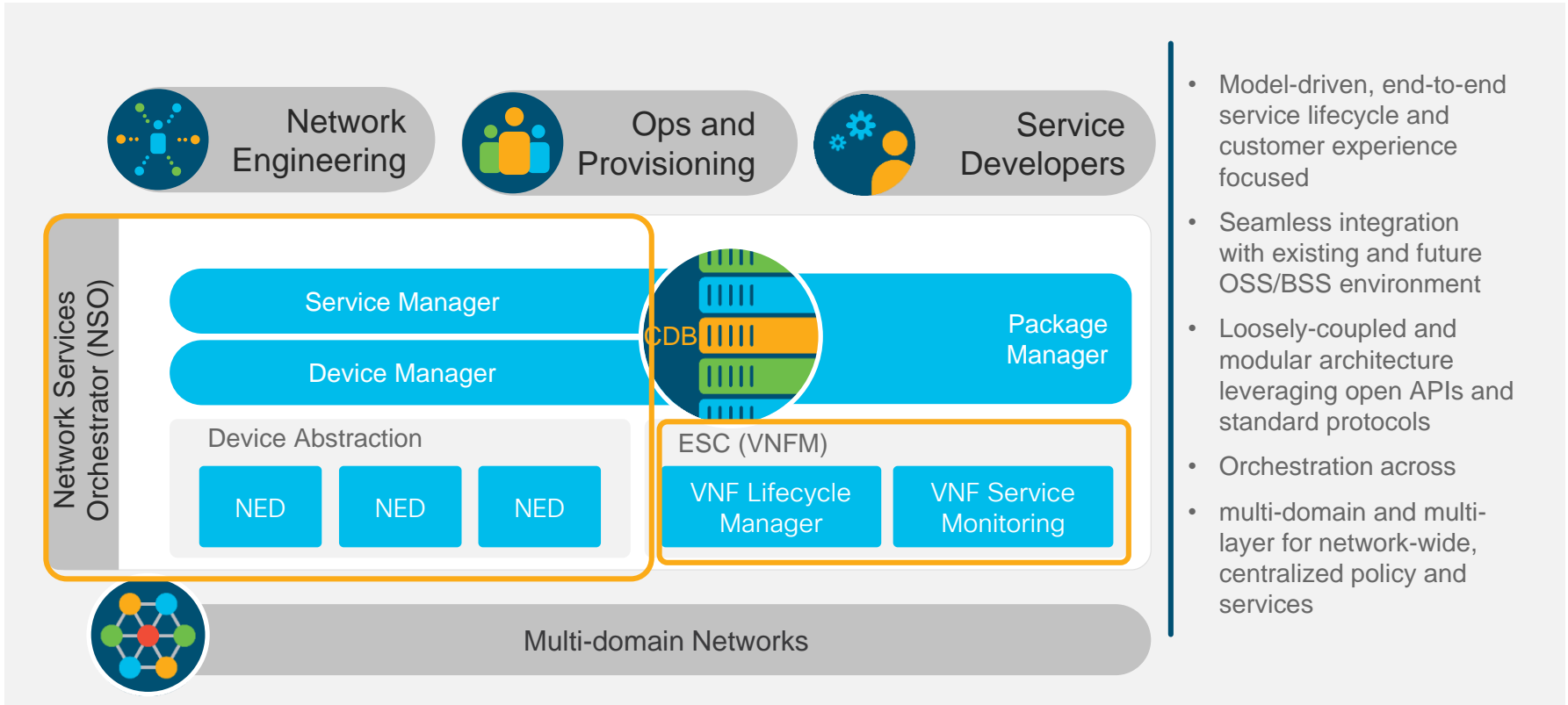
2x10G Ethernet

CIMC / OOB LOM

NICs: X520(2x10G), X710(4x10G), XL710 (2x40G), XXV710(2x25G)

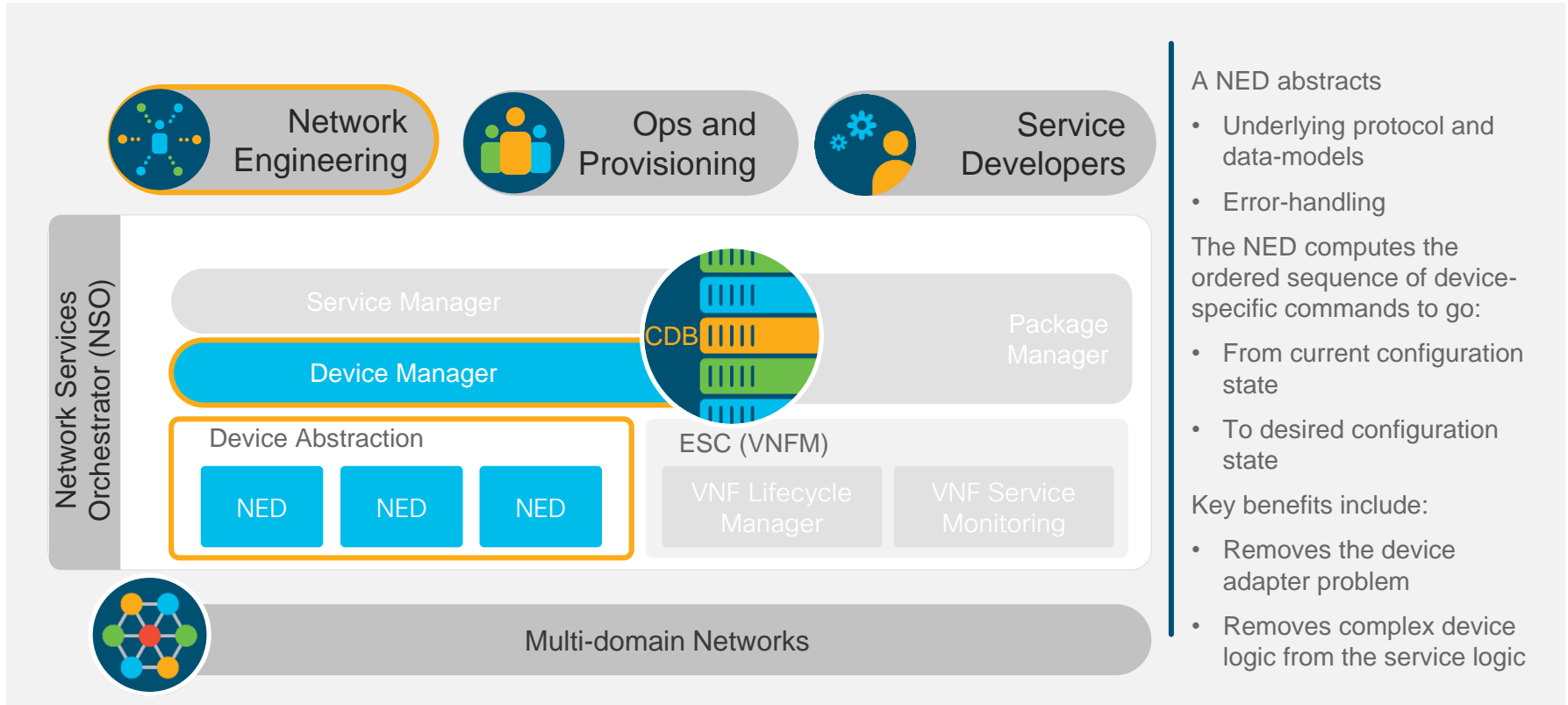
cisco Live!

System Overview – NSO and ESC



- Model-driven, end-to-end service lifecycle and customer experience focused
- Seamless integration with existing and future OSS/BSS environment
- Loosely-coupled and modular architecture leveraging open APIs and standard protocols
- Orchestration across
- multi-domain and multi-layer for network-wide, centralized policy and services

Network Element Drivers (NED's) – Multivendor Abstraction



A NED abstracts

- Underlying protocol and data-models
- Error-handling

The NED computes the ordered sequence of device-specific commands to go:

- From current configuration state
- To desired configuration state

Key benefits include:

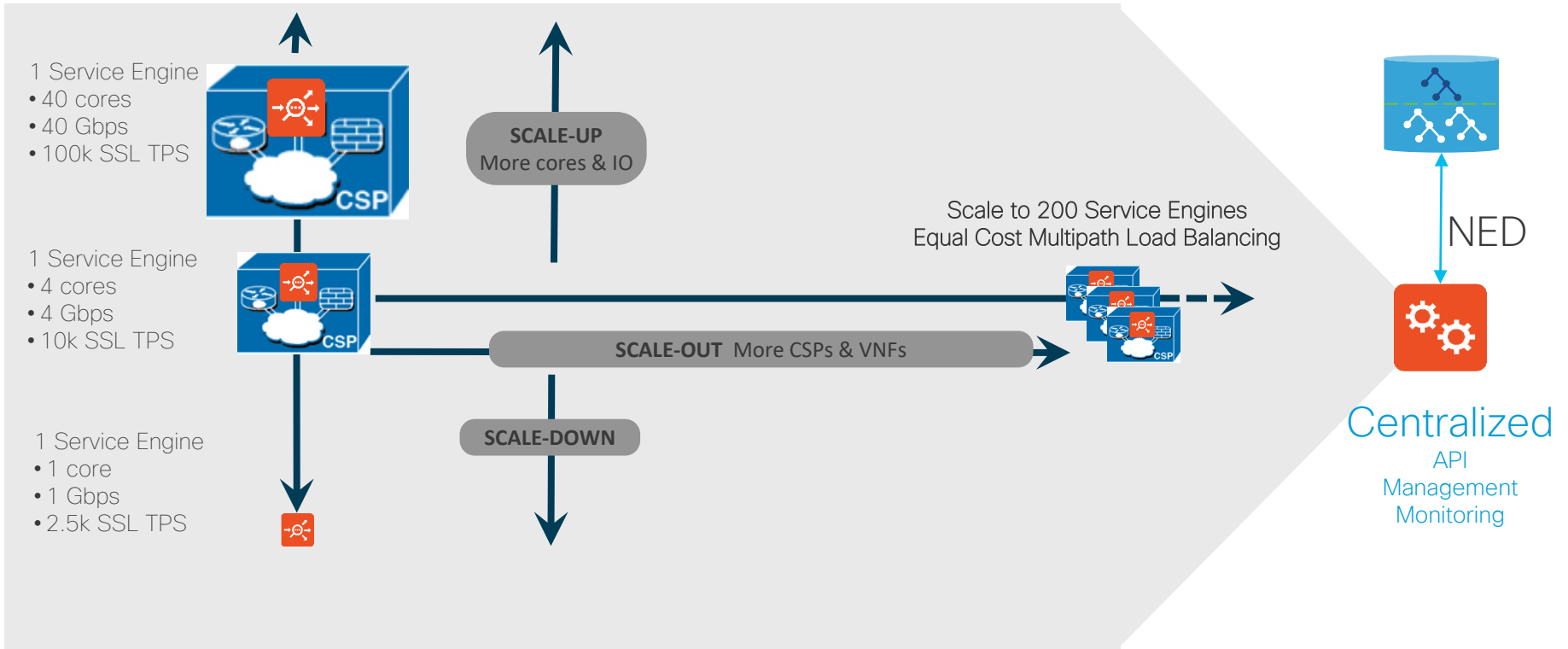
- Removes the device adapter problem
- Removes complex device logic from the service logic



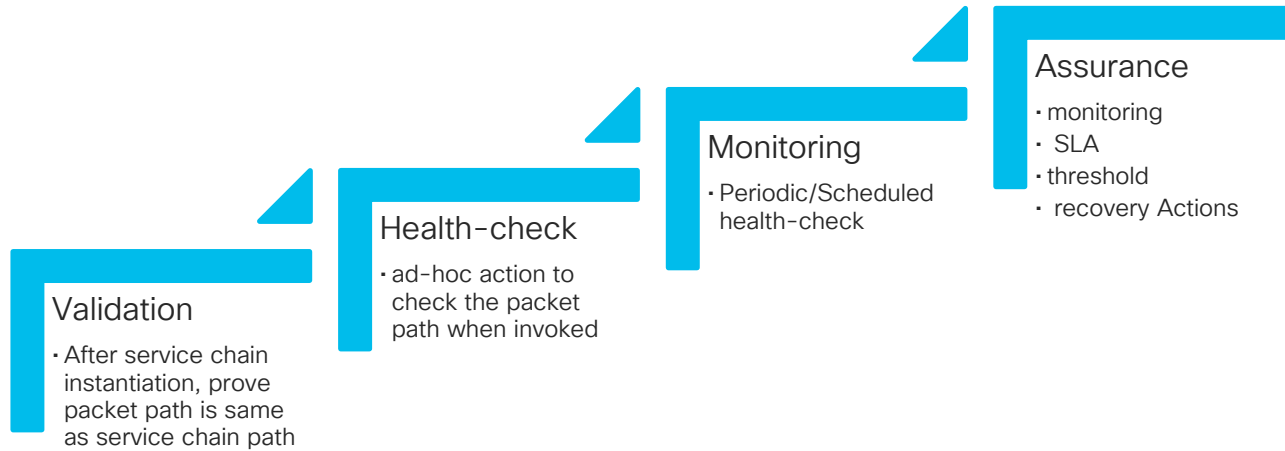
Industry's Broadest Multivendor Support Over 100 Supported NEDs – Customization Available



Virtualization - Scale Up, Out and Down



SAE Assurance Journey



Benefits of SAE

Flexibility



Cited as the #1 benefit of NFV

Agile



Reduce Complexity & Deployment Time

Cost



Reduces CapEx, saves space and power

Use Case 1: Onboard a new partner

SAE Solution

- Under an Hour
- Select or Create a Service chain
- Deploy Service chain at Site

Physical Solution

- Days/weeks
- Network team creates design & configuration
- Security/firewall team **instantiates firewall rules, ACLs**
- Solution reviewed & approved by Change Board
- Maintenance Window scheduled for production deployment

Use Case 2: Onboard a new application

SAE Solution

- Under an Hour
- Select or Create a Service Chain
- Deploy Service chain at Site

Physical Solution

- Days/Weeks
- Network team creates design & configuration, deploys and hardware for network connectivity
- Security team opens **ports & protocols** required
- Change Board reviews & approves
- Maintenance Window scheduled for production deployment

NFV TCO

Use case: Financial securities company doing a Firewall refresh.
Physical FW vs NFV

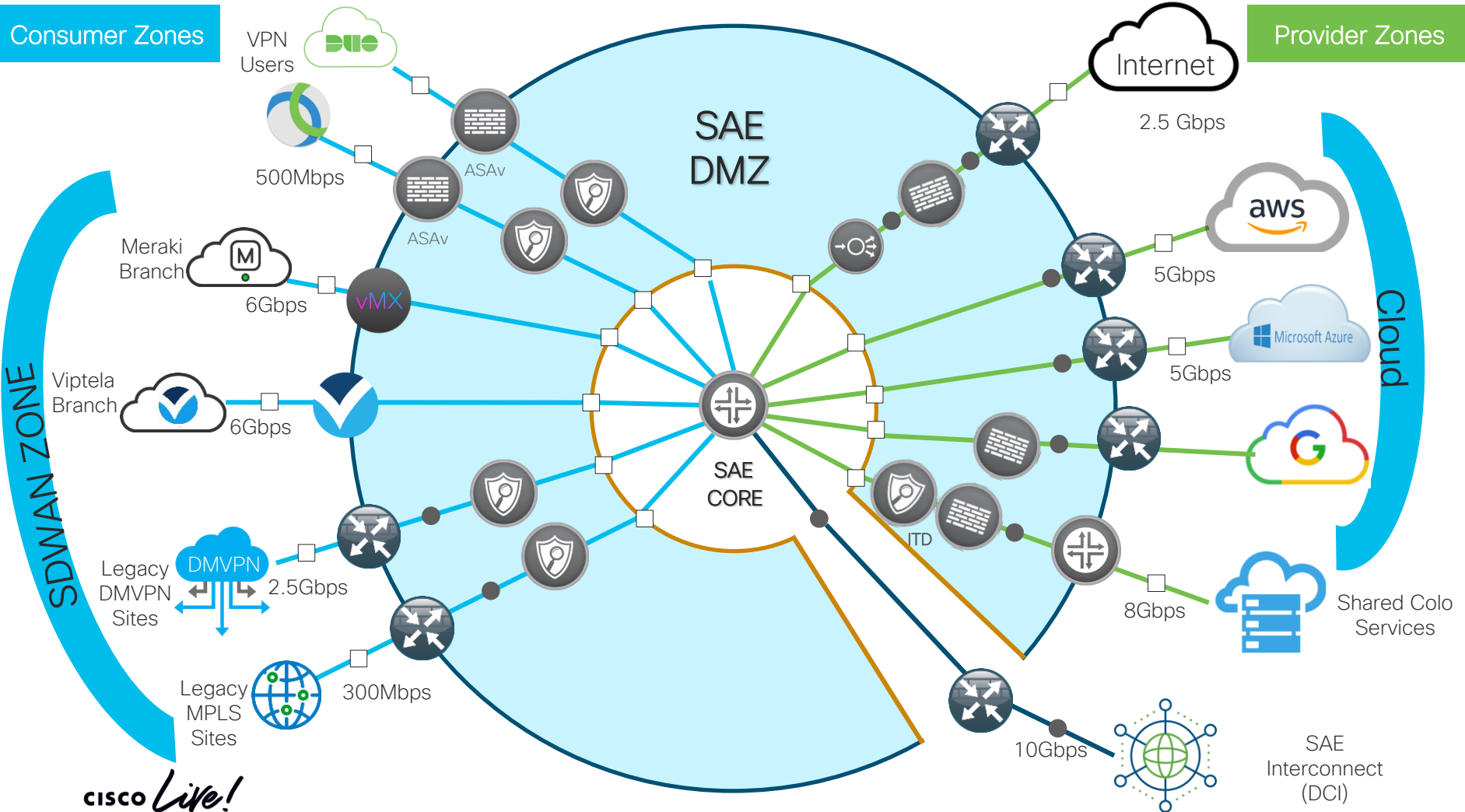
CapEx Savings	\$ 400k (~30%)
Power Savings	\$ 13K
Space Savings (RU)	38

Solution	Total PNF Cost	\$ 1,419,282	Total NFV/VNF Cost	\$ 1,000,000	\$ 419,282
Power	Power/Unit Watts	1,200		1,050	
	Total Watts for Units	21,600		6,300	15,300
	Cost/KwH	\$0.10		\$0.10	
	Cost/unit	\$1,046.40		\$915.60	
	Total power cost	\$ 18,835		\$ 5,494	\$ 13,338
RU	3RU*18	54	2RU*6	12	38

SAE Planning

Consumer Zones

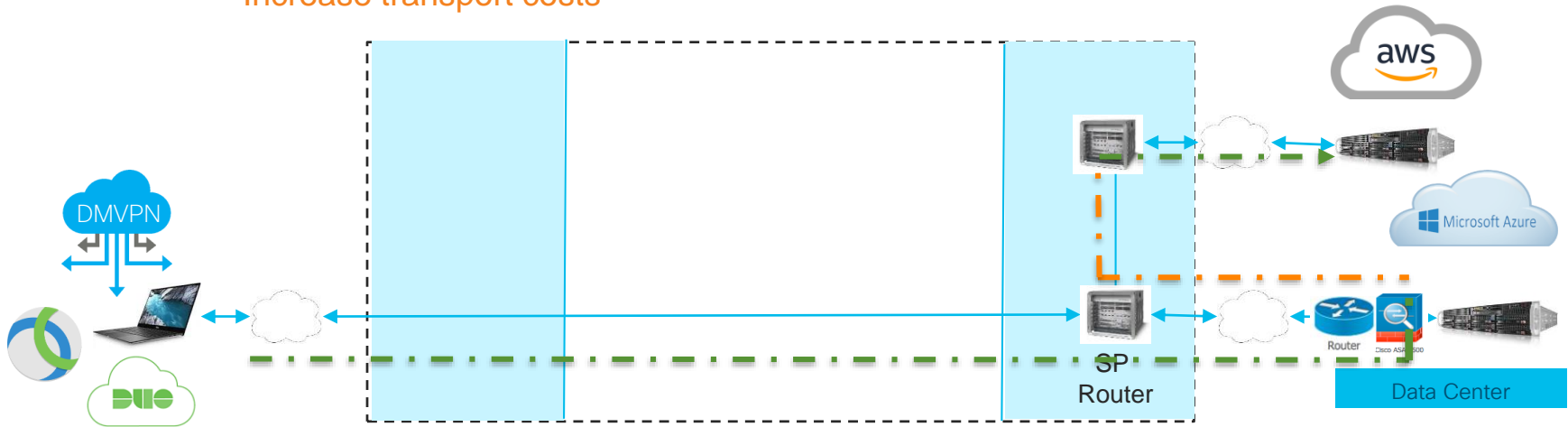
Provider Zones



Access to app hosted in Cloud

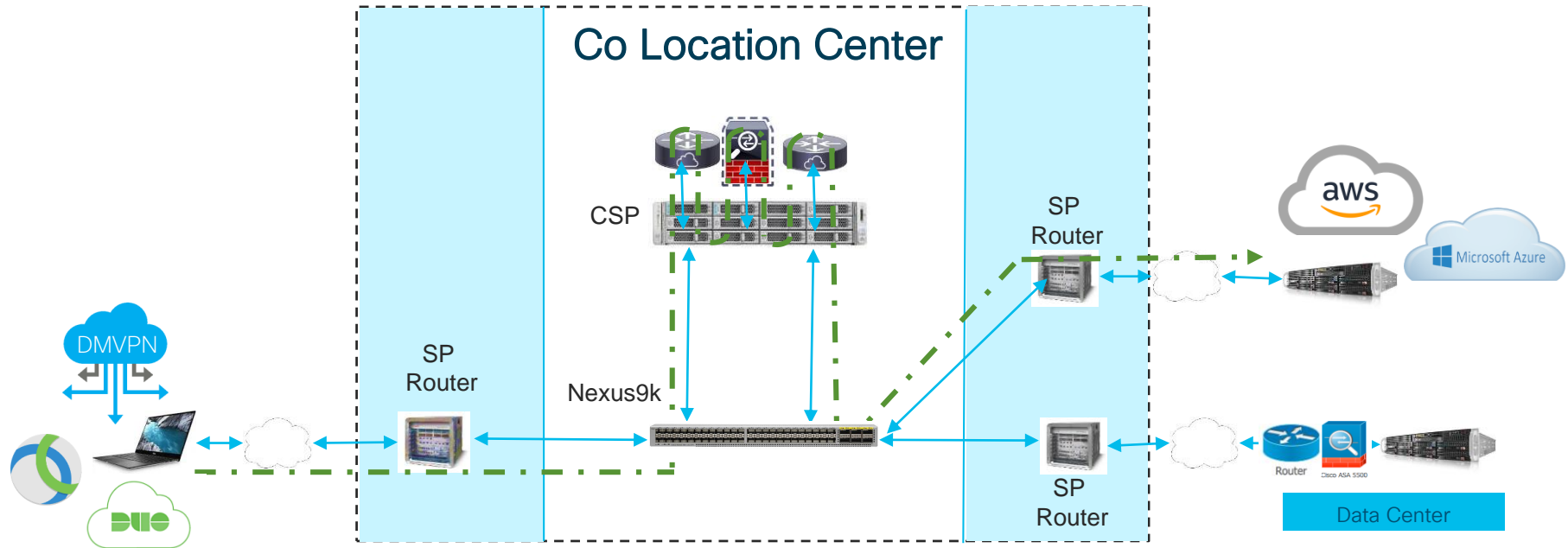
Effects, when traffic back-hauled to DC to apply security policies

- Hair pinning/tromboning of traffic
- Adds latency
- Increases BW requirements
- Increase transport costs

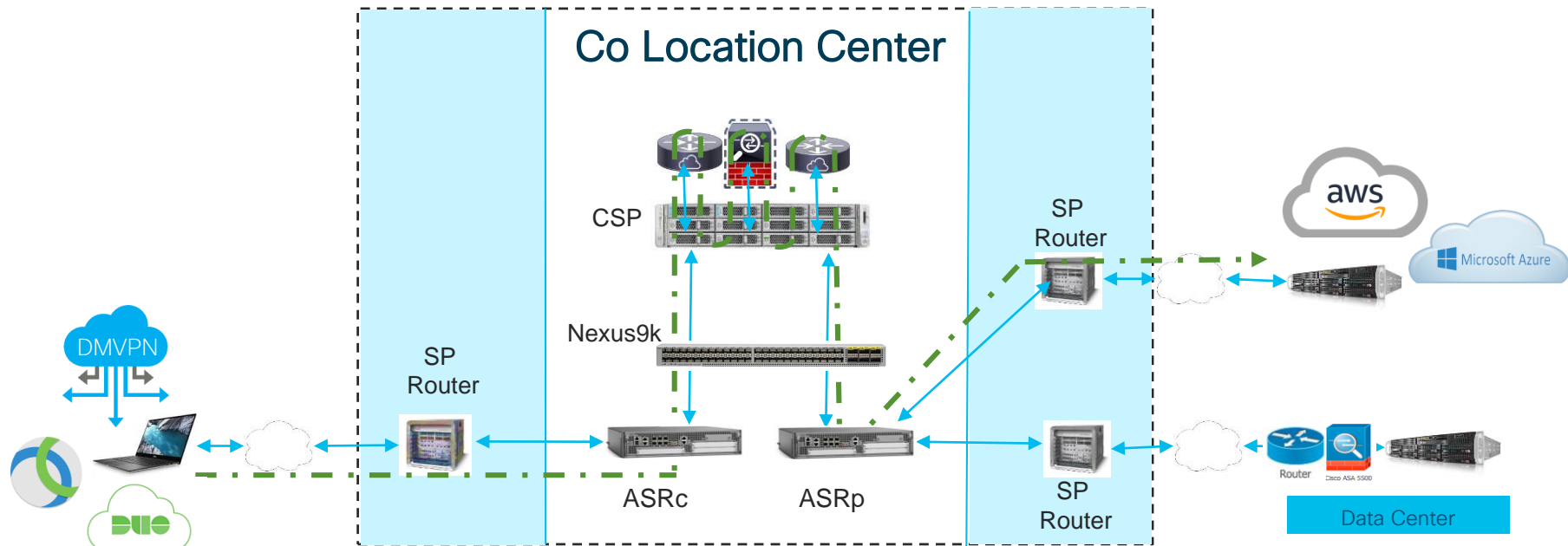


Traffic delivered to cloud App over internet or Hybrid Cloud Connect (Direct Connect/Express Route)

SAE: Centralized Secure Policy Application to Traffic Flows- Virtual Only

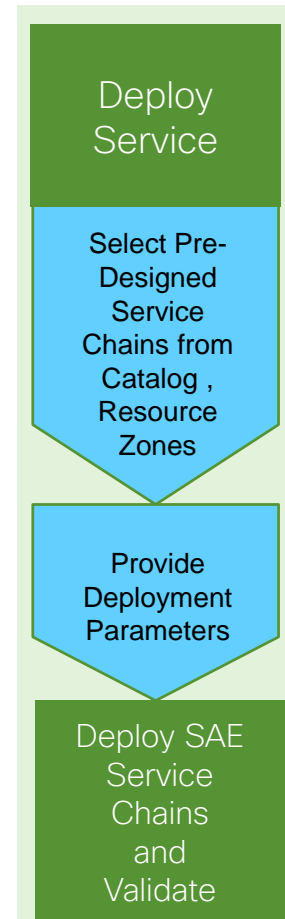
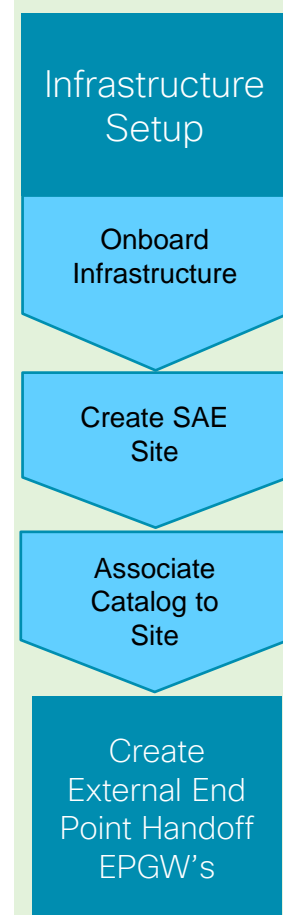
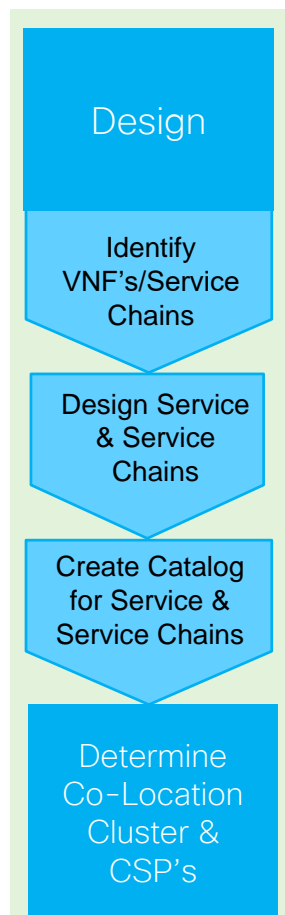
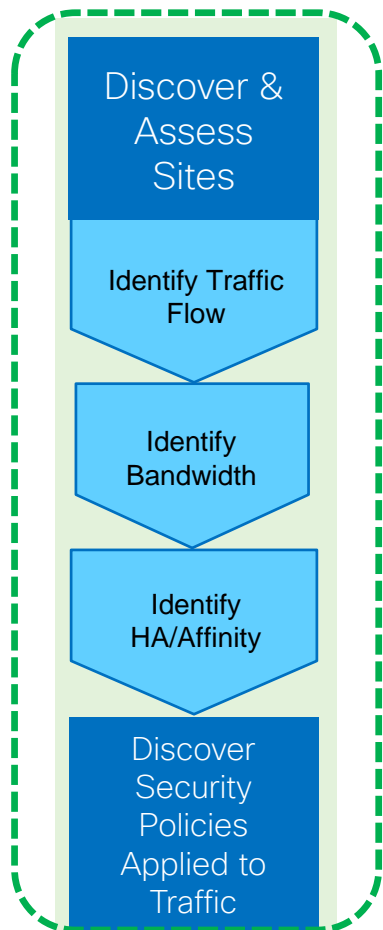


SAE: Centralized Secure Policy Application to Traffic Flows- Physical & Virtual



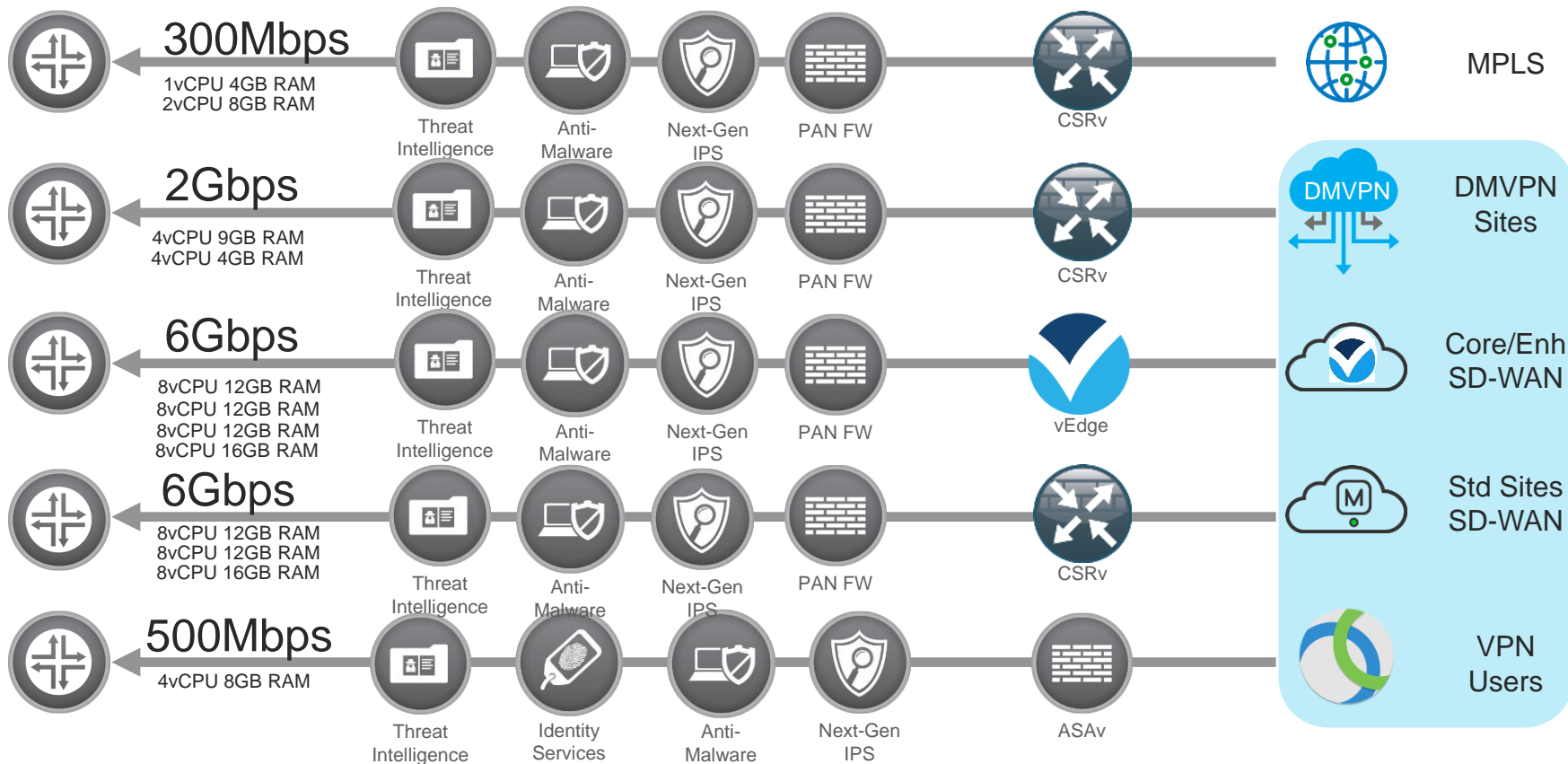
1. ASRc IN connected to Branch router, OUT to Nexus 9K leaf
2. ASRp IN connected to N9K and OUT to SP Router

SAE Workflow



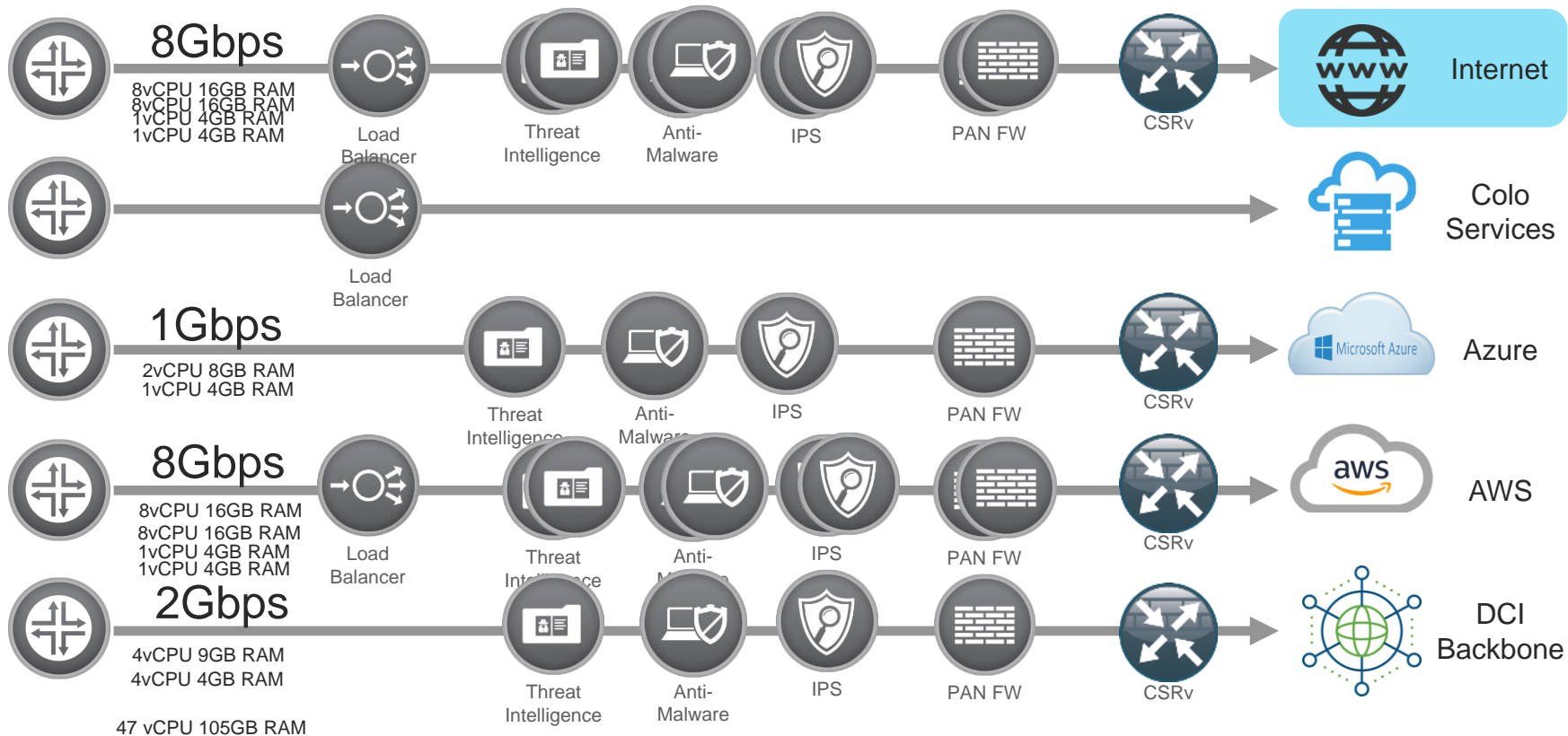
Consumer Zones Service Chain

Secure Agile Exchange



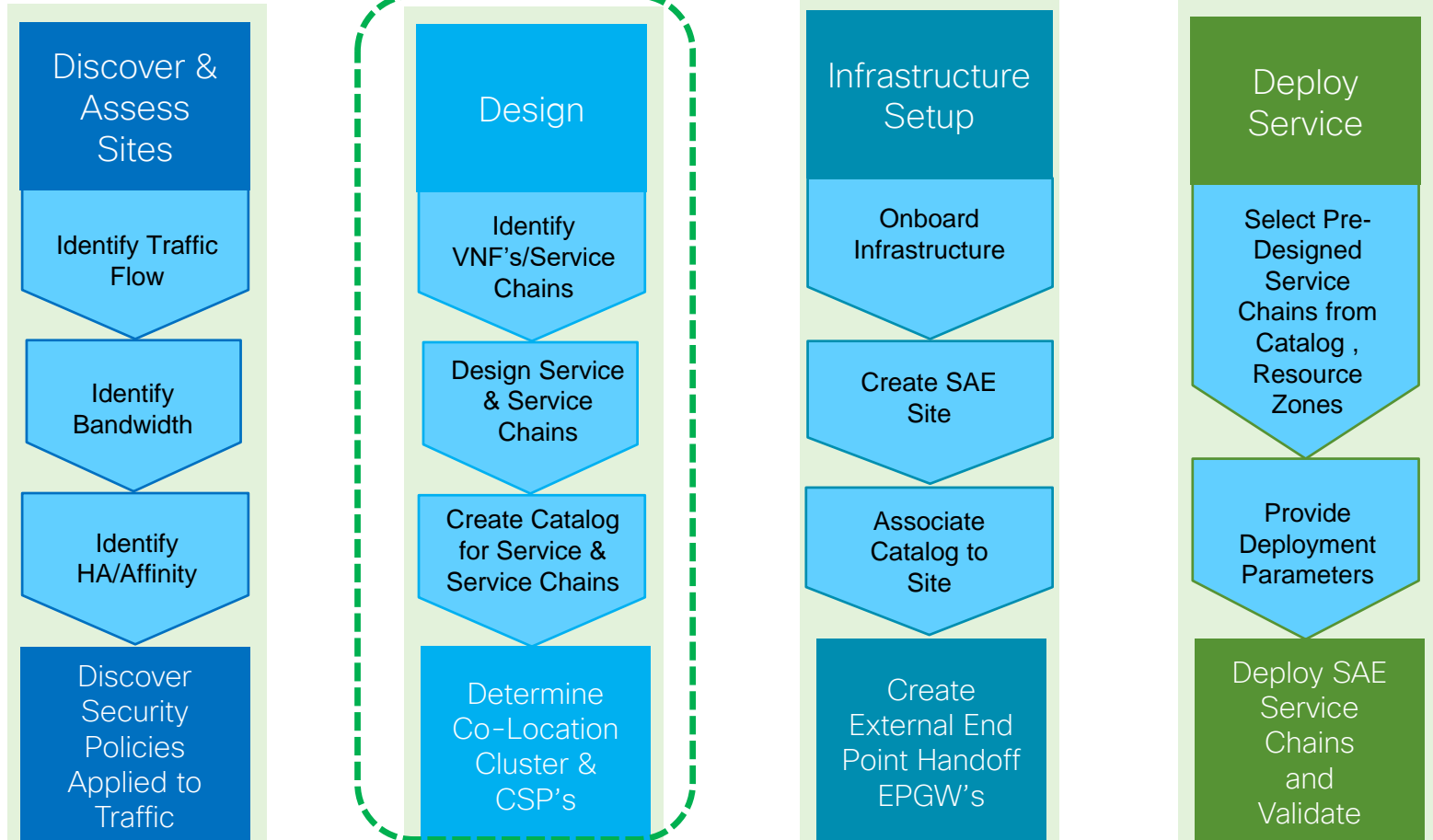
Provider Zones Service Chain

Secure Agile Exchange



SAE Design

SAE Workflow



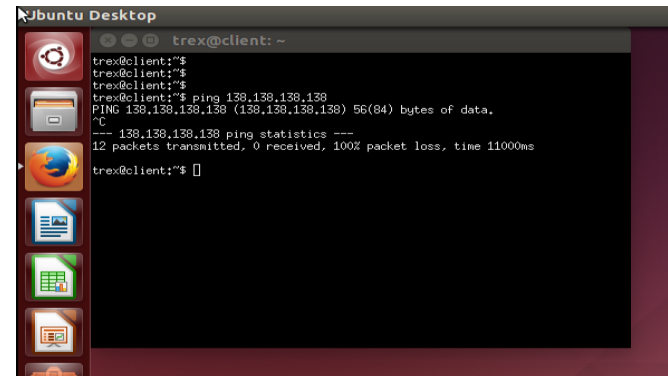
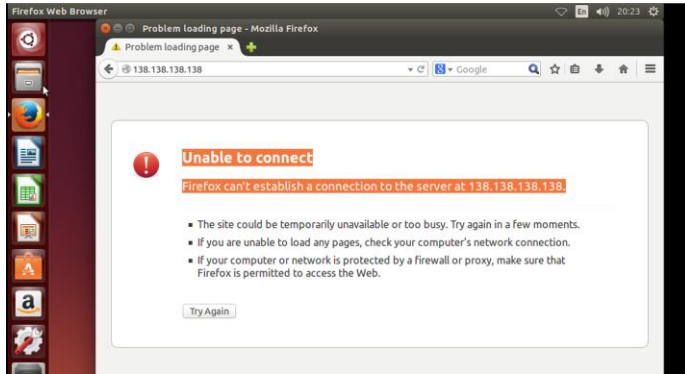
Intent: Branch needs connectivity to app in the cloud

Customer and Cloud Service Provider (CSP) have presence in Co-Location

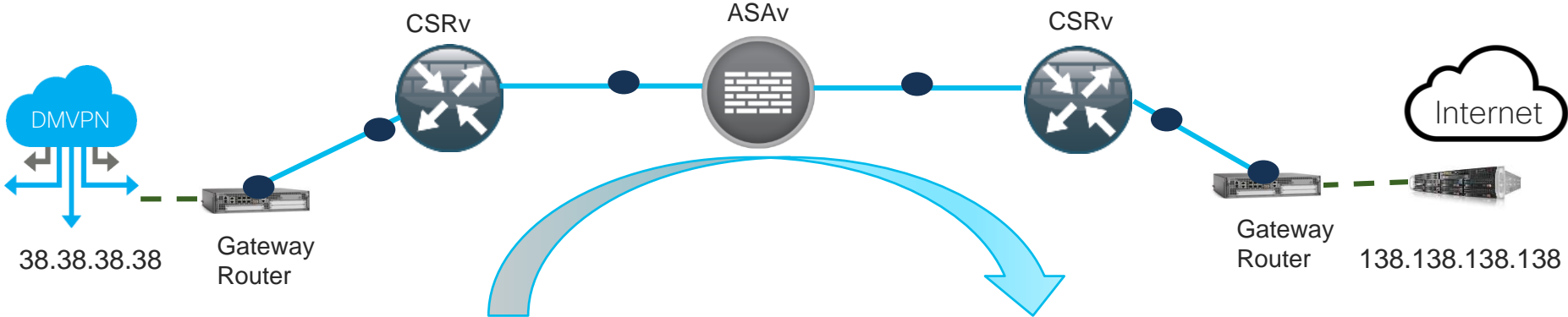


Unable to access application

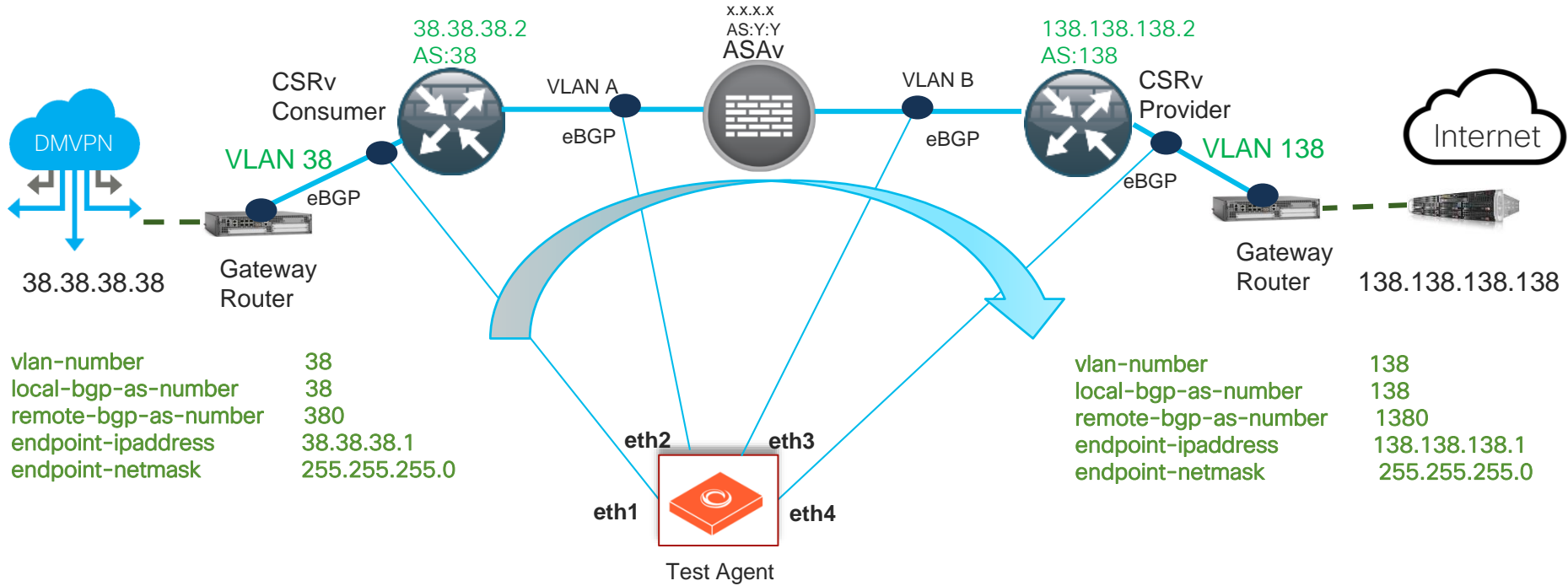
Unable to ping server



End-to-End Service Chain Traffic Flow



End-to-End Service Chain – Traffic Flow Configuration



CSR 1000v Resource Sizing

Table 7. Cisco CSR 1000v packaging

Features	Description
IP Base	<ul style="list-style-type: none"> Basic networking: BGP, OSPF, EIGRP, Routing Information Protocol (RIP), Intermediate System-to-Intermediate System (IS-IS), IPv6, GRE, VRF-Lite, NTP, QoS, BFD, and CLNS Multicast: Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM) High availability: HSRP, VRRP, and GLBP Addressing: 802.1Q VLAN, EVC, NAT, DHCP, and DNS Basic security: ACL, AAA, RADIUS, and TACACS+ Management: Cisco IOS XE CLI, SSH, Flexible NetFlow, SNMP, EEM, and NETCONF
Security	<ul style="list-style-type: none"> IPBase Plus Advanced security: ZBFW, IPsec VPN, Easy VPN, DMVPN, FlexVPN, and GetVPN Box-to-box high-availability for ZBFW and NAT
AppX	<ul style="list-style-type: none"> IPBase Plus Advanced networking: Layer 2 Tunneling Protocol Version 3 (L2TPv3), MPLS, VRF, and VXLAN Application experience: WCCPv2, AppXNAV, Network-Based Application Recognition Version 2 (NBAR2), AVC, and IP SLA Hybrid cloud connectivity: LISP, OTV, VPLS, and EoMPLS Subscriber management: PTA, LNS, and ISG
AX	<ul style="list-style-type: none"> All features

Table 8. Minimum server resource requirements per Cisco CSR 1000v instance

Throughput	Technology Package			
	IP Base	Security	AppX	AX
10 Mbps	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB
50 Mbps	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB
100 Mbps	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB
250 Mbps	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB
500 Mbps	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB
1 Gbps	1 vCPU/4 GB	1 vCPU/4 GB	1 vCPU/4 GB	2 vCPU/4 GB
2.5 Gbps	1 vCPU/4 GB	2 vCPU/4 GB	4 vCPU/4 GB	4 vCPU/4 GB
5 Gbps	1 vCPU/4 GB	2 vCPU/4 GB	8 vCPU/4 GB	8 vCPU/4 GB
10 Gbps	2 vCPU/4 GB	Not supported	Not supported	Not supported

ASAv Sizing







ASAv Specifications

Feature	ASAv5	ASAv10	ASAv30	ASAv50
Virtual CPUs	1	1	4	8
Memory	1 GB minimum 1.5 GB maximum	2 GB	8 GB	16 GB
Minimum disk storage ⁴	8 GB	8 GB	16 GB	16 GB
Stateful inspection throughput (maximum) ¹	100 Mbps	1 Gbps	2 Gbps	10 Gbps
Stateful inspection throughput (multiprotocol) ²	50 Mbps	500 Mbps	1 Gbps	5 Gbps
Advanced Encryption Standard (AES) VPN throughput ³	30 Mbps	125 Mbps	1 Gbps	3 Gbps
Connections per second	8,000	20,000	60,000	120,000
Concurrent sessions	50,000	100,000	500,000	2,000,000
VLANs	25	50	200	1024
Bridge groups	12	25	100	250
IPsec VPN peers	50	250	750	10,000
Cisco AnyConnect [®] or clientless VPN user sessions	50	250	750	10,000
Cisco Unified Communications phone proxy	50	250	1000	Not tested
Cisco Cloud Web Security users	250	1,000	5000	Not tested
High availability	Active/standby			
Modes	Routed and transparent			

Ordering Information: In Cisco Commerce Workspace (CCW) Order the Base Selection (Denoted by “K9” in the Part Number), Followed by the Desired License Type

Part Number	Description
L-ASAV5S-K9=	8-pack Cisco ASAv5 (100 Mbps) selection
L-ASAV5S-STD-8	8-pack Cisco ASAv5 (100 Mbps) with all firewall features licensed
L-ASAV10S-K9=	Cisco ASAv10 (1 Gbps) selection
L-ASAV10S-STD	Cisco ASAv10 (1 Gbps) with all firewall features licensed
L-ASAV10S-STD-16	16-pack Cisco ASAv10 (1 Gbps) with all firewall features licensed
L-ASAV30S-K9=	Cisco ASAv30 (2 Gbps) selection
L-ASAV30S-STD	Cisco ASAv30 (2 Gbps) with all firewall features licensed
L-ASAV30S-STD-4	4-pack Cisco ASAv30 (2 Gbps) with all firewall features licensed
L-ASAV50S-K9=	Cisco ASAv50 (10 Gbps) selection
L-ASAV50S-STD	Cisco ASAv50 (10 Gbps) with all firewall features licensed
L-ASAV50S-STD-4	4-pack Cisco ASAv50 (10 Gbps) with all firewall features licensed

Palo Alto Sizing

Feature	 VM-700 Remove	 VM-500 Remove	 VM-300 Remove	 VM-200 Remove	 VM-100 Remove	 VM-50 Remove	VM-50(Lite) VM-50(Lite) Remove
Performance*							
App-ID firewall throughput	16 Gbps*	8 Gbps*	4 Gbps*	2 Gbps*	2 Gbps*	200 Mbps*	200 Mbps*
Threat prevention throughput	8 Gbps*	4 Gbps*	2 Gbps*	1 Gbps*	1 Gbps*	100 Mbps*	100 Mbps*
IPSec VPN throughput	6 Gbps	4 Gbps	1.8 Gbps	1Gbps	1Gbps	100 Mbps	100 Mbps
Connections per second	120,000*	60,000*	30,000*	15,000*	15,000*	3,000*	3,000*
Sessions							
Max sessions (IPv4 or IPv6)	10,000,000	2,000,000	819,200	250,000	250,000	64,000	50,000

MODEL	SESSIONS	SECURITY RULES	DYNAMIC IP ADDRESSES	SECURITY ZONES	IPSEC VPN TUNNELS	SSL VPN TUNNELS	VM-SERIES MODEL	SUPPORTED HYPERVISORS	SUPPORTED VCPUS	MINIMUM MEMORY	MINIMUM HARD DRIVE
VM-50	50,000	250	1,000	15	250	250	VM-50	ESXi, KVM, Hyper-V	2	4.5GB	32GB (60GB at boot)
VM-100	250,000	1,500	2,500	40	1,000	500	VM-100 VM-200	ESXi, KVM, Hyper-V, AWS, Azure, NSX, SDX	2	6.5GB	60GB
VM-300	800,000	10,000	100,000	40	2,000	2,000	VM-300 VM-1000-HV	ESXi, KVM, Hyper-V, AWS, Azure, NSX, SDX	2, 4	9GB	60GB
VM-500	2,000,000	10,000	100,000	200	4,000	6,000	VM-500	ESXi, KVM, Hyper-V, AWS, Azure, NSX	2, 4, 8	16GB	60GB
VM-700	10,000,000	20,000	100,000	200	8,000	12,000	VM-700	ESXi, KVM, Hyper-V, AWS, Azure	2, 4, 8, 16	56GB	60GB

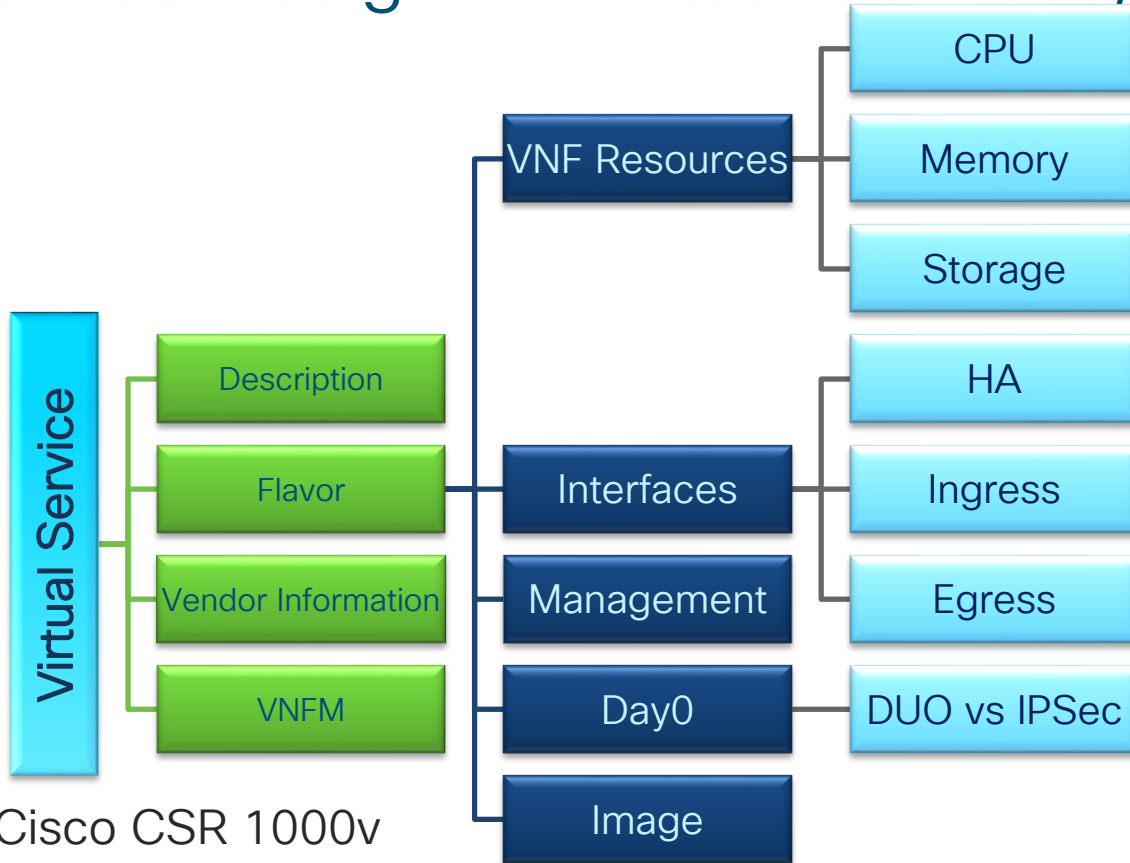
Virtual Network Function (VNF) Catalog

VNF Catalog			
vCPU	Memory (GB)	Storage (GB)	Vendor
16	56	2046	Palo Alto
8	16	2046	Palo Alto
2	8	2046	Palo Alto
8	16	10	F5
2	4	10	F5
1	4	8	Cisco
1	4	8	Cisco
2	4	8	Cisco
App Catalog			
12	96	2.4	Cisco
7	64	1.5	Cisco
4	4	50	Cisco
4	32	250	Infoblox

ASAv VNF Profile/Template

VSX Template	VSX profile
hostname \$VSD_ASA_HOSTNAME	✓# of interfaces: 4
nameif \$MGMT_IF	✓Interface naming:
ip address \$VSD_ASA_NICID_0_IP_ADDRESS	✓ Inside, Outside, HA, Management
\$VSD_ASA_NICID_0_IP_MASK	✓Resource profile:
username \$VFIREWALL_USERNAME	✓CPU, Memory, Storage
password \$VFIREWALL_PASSWORD	✓SR-IOV, NIC type
privilege 15	✓Image name, path
ssh 0.0.0.0 0.0.0.0 \$MGMT_IF	✓Ned, Day0
router bgp \$VSD_ASA_ASNUMBER	
bgp router-id \$VSD_ASA_NICID_0_IP_ADDRESS	
license smart register idtoken \$LICENSE_TOKEN force	

Service Design → Virtual Services/VNFD



E.g. Cisco CSR 1000v

*VNFD – Virtual Network Function Descriptor

Virtual Services



Secure Agile Exchange
VERSION 2.0.1



SITE

SERVICE DESIGN

SERVICE CATALOG

GLOBAL

VIRTUAL SERVICES

PHYSICAL SERVICES

SERVICE CHAINS

Search Service...

ADD

ASAv



Vendor Cisco
Version 1

AVI-SE



Vendor AVI Networks
Version 1

CSR1000v



Vendor Cisco
Version 1

Citrix_WebApp_FW



Vendor CITRIX
Version 1

F5-BigIP



Vendor F5
Version 1

FTDv



Vendor Cisco
Version 1

Fortinet



Vendor Fortinet
Version 1

Netrounds_Test_Agent



Vendor Netrounds
Version 1

PaloAltoFW



Vendor Palo Alto
Version 1

Symantec_Virtual_Sec_Gateway



Vendor Symantec
Version 1

Viptela_vEdge



Vendor Cisco
Version 1

WSAv

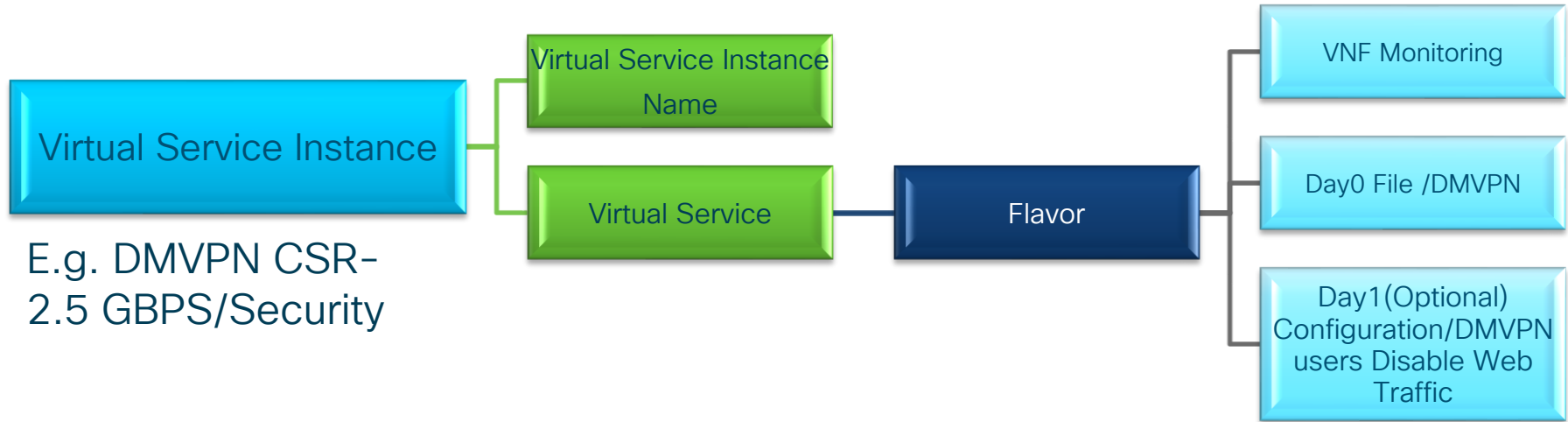


Vendor Cisco
Version 1

CISCO *Live!*

Service Catalog → Virtual Service Instance/VNFD-Deployment

- Catalog of various services
 - Day0 Configuration
 - Configuration parameter changes
 - Day1 Configuration



Virtual Service Instance



Secure Agile Exchange
VERSION 2.0.1



SITE



SERVICE DESIGN



SERVICE CATALOG



GLOBAL

CATALOG

VIRTUAL SERVICE INSTANCE

PHYSICAL SERVICE INSTANCE

SERVICE CHAIN INSTANCE

ORGANIZATION

SERVER PROFILE

Select Service...

Search Service Instance...

ADD

ASAv

ASAv-10

FLAVOR
SERVICE CONFIG

ASA
ASAv

ASAv-30

FLAVOR
SERVICE CONFIG

ASA
ASAv

ASAv-5

FLAVOR
SERVICE CONFIG

ASA
ASAv

ASAv-50

FLAVOR
SERVICE CONFIG

ASA
ASAv

CSR1000v

AWS-CSR

FLAVOR
SERVICE CONFIG

CSR
CSR-5G

DMVPN-CSR-2G

FLAVOR
SERVICE CONFIG

CSR
CSR-2G

EDGE-CSR-5G

FLAVOR
SERVICE CONFIG

CSR
CSR-5G

INET-CSR-2G

FLAVOR
SERVICE CONFIG

CSR
CSR-2G

PaloAltoFW

PAFW-VM-100

FLAVOR
SERVICE CONFIG

PaloAltoFW
PaloAltoFW

PAFW-VM-300

FLAVOR
SERVICE CONFIG

PaloAltoFW
PaloAltoFW

PAFW-VM-50

FLAVOR
SERVICE CONFIG

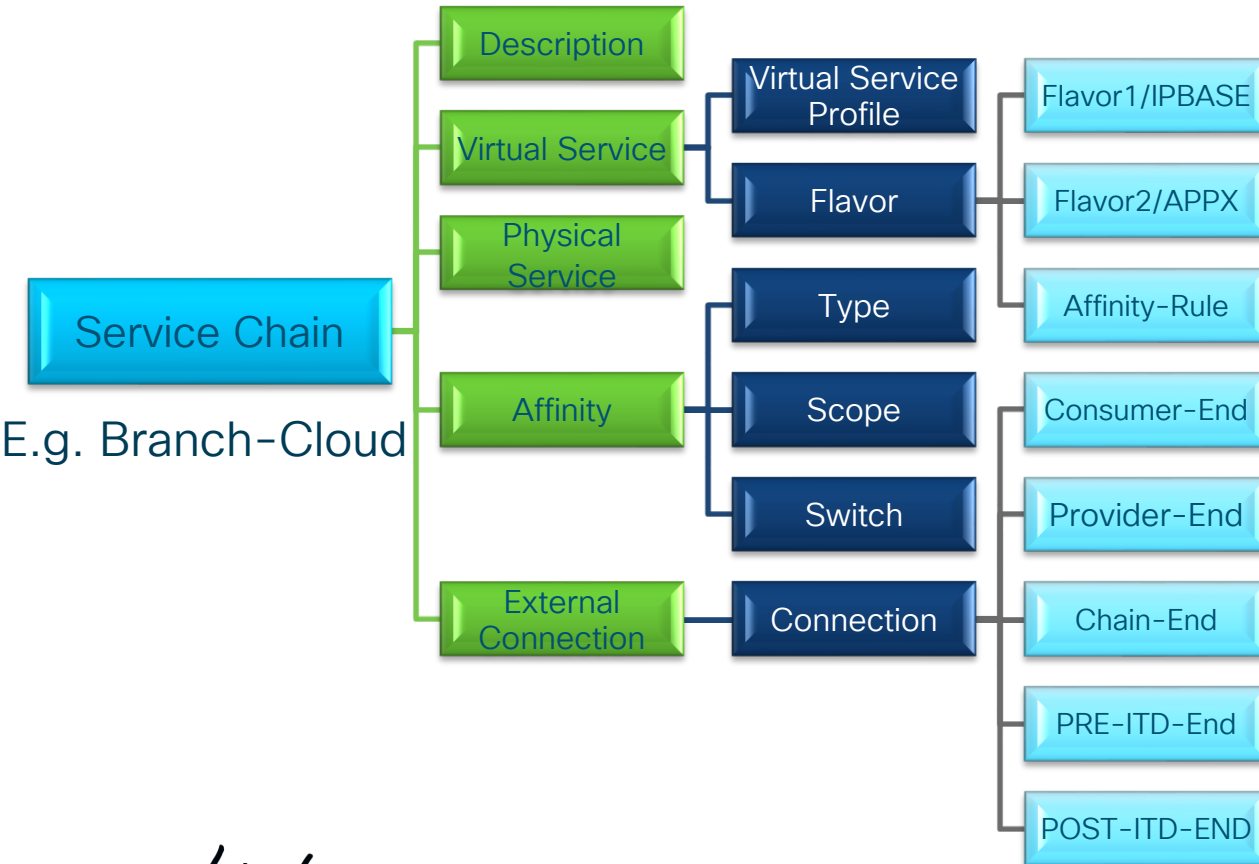
PaloAltoFW
PaloAltoFW

PAFW-VM-700

FLAVOR
SERVICE CONFIG

PaloAltoFW
PaloAltoFW

Service Design → Service Chain / NSD



*NSD=Network Service Descriptor

Service Chains



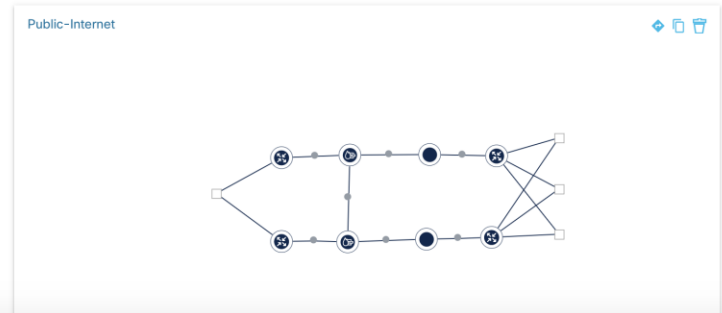
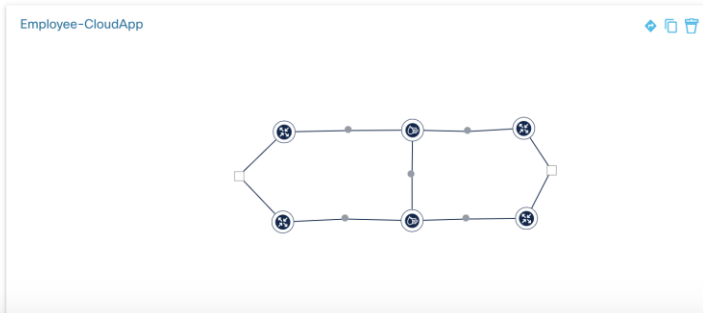
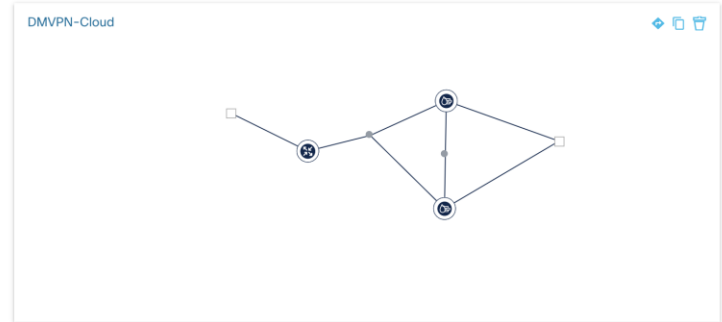
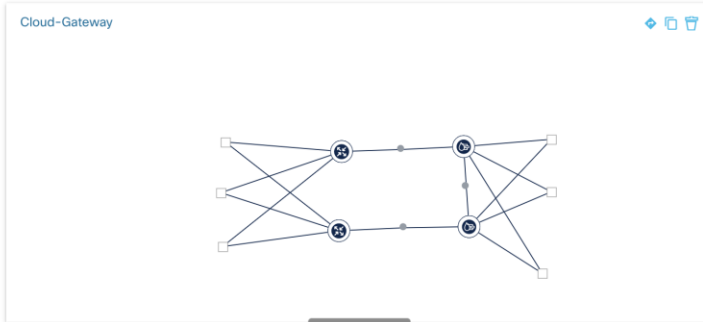
Secure Agile Exchange
VERSION 2.0.1



SITE SERVICE DESIGN SERVICE CATALOG GLOBAL

VIRTUAL SERVICES PHYSICAL SERVICES SERVICE CHAINS

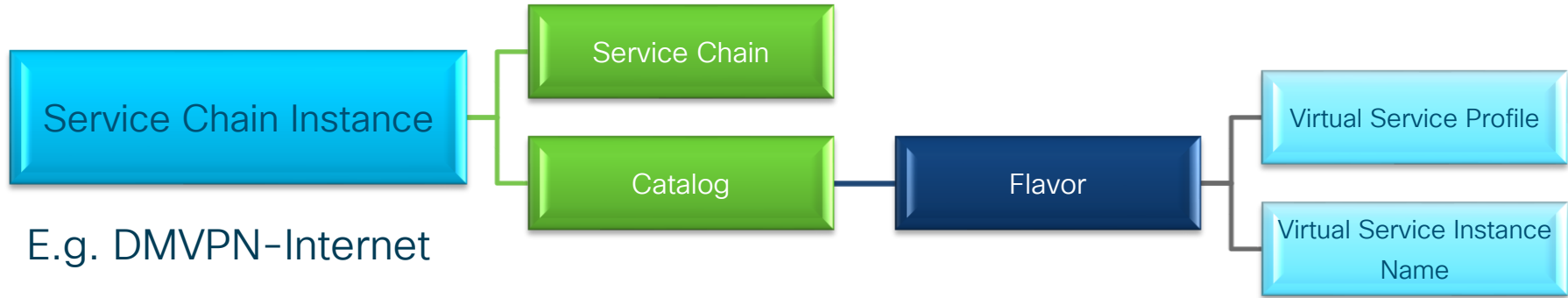
Search Service Chain... ADD



Service Catalog → Service Chain Instance/NSD-Deployment

Catalog of various service-chains

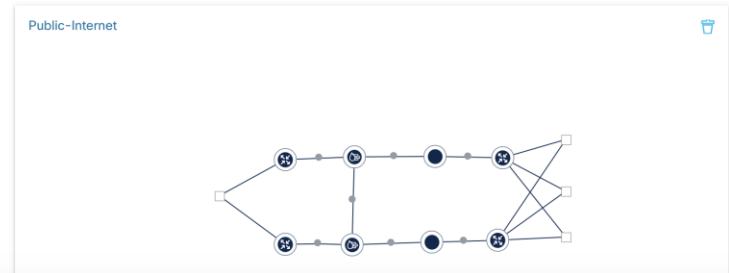
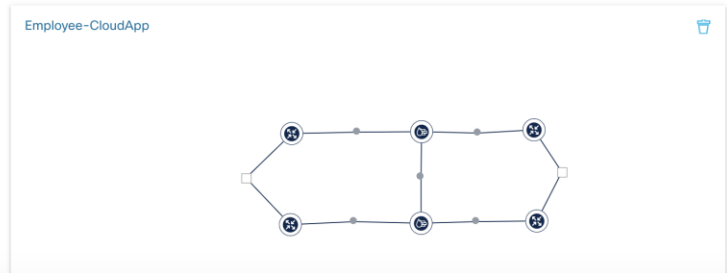
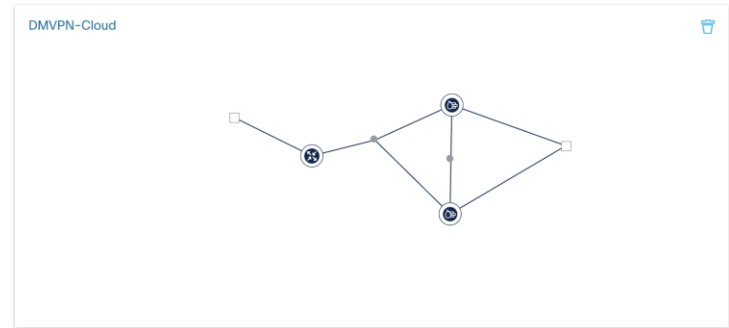
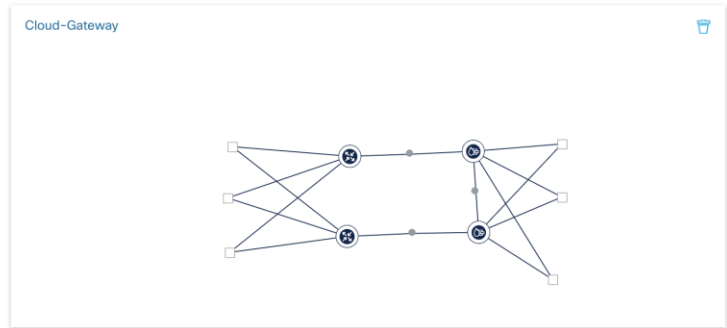
- Different Services
- Configuration parameter changes



Service Chain Instance

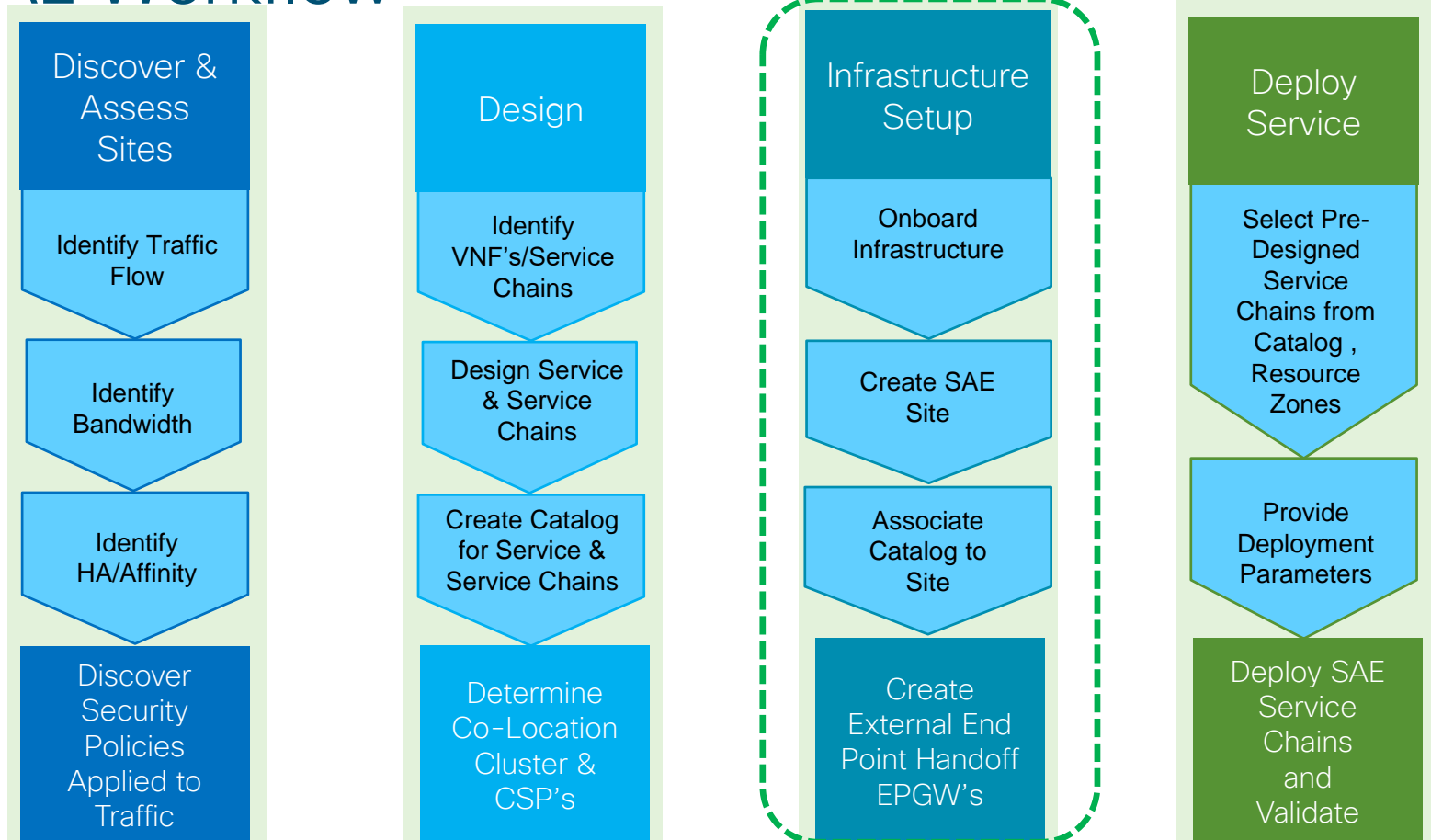


SAE_CATALOG

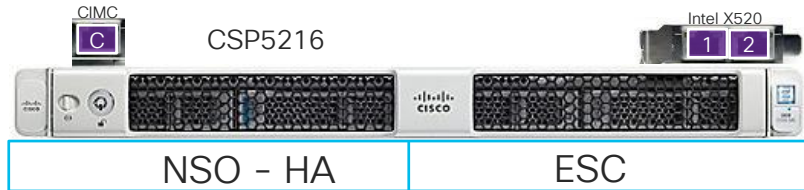
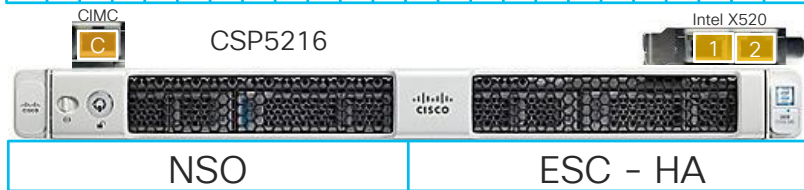
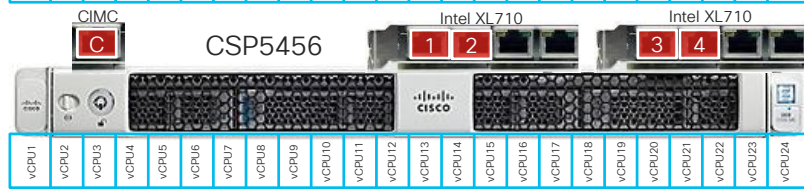
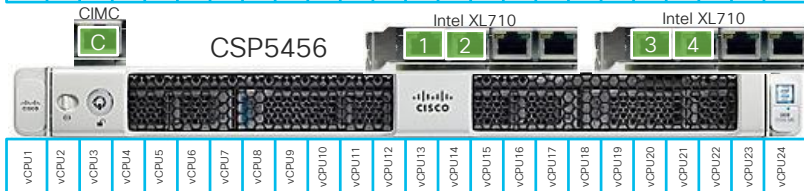
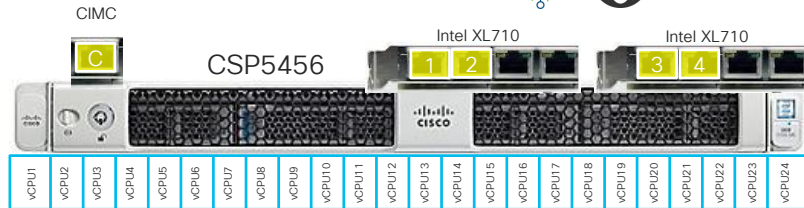
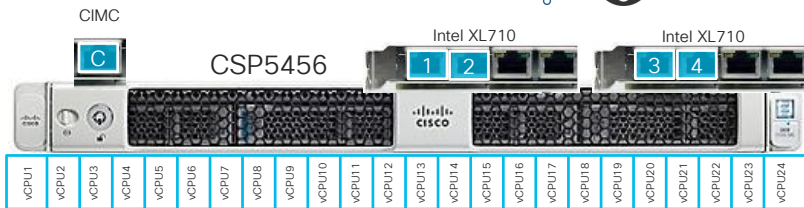
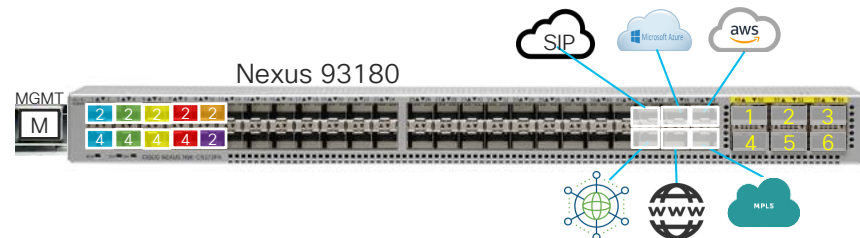
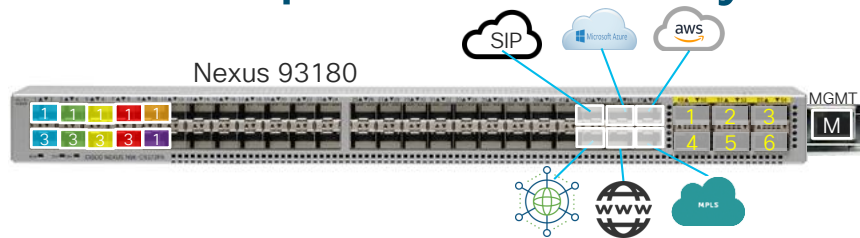


SAE Infrastructure

SAE Workflow



Example SAE Physical Buildout



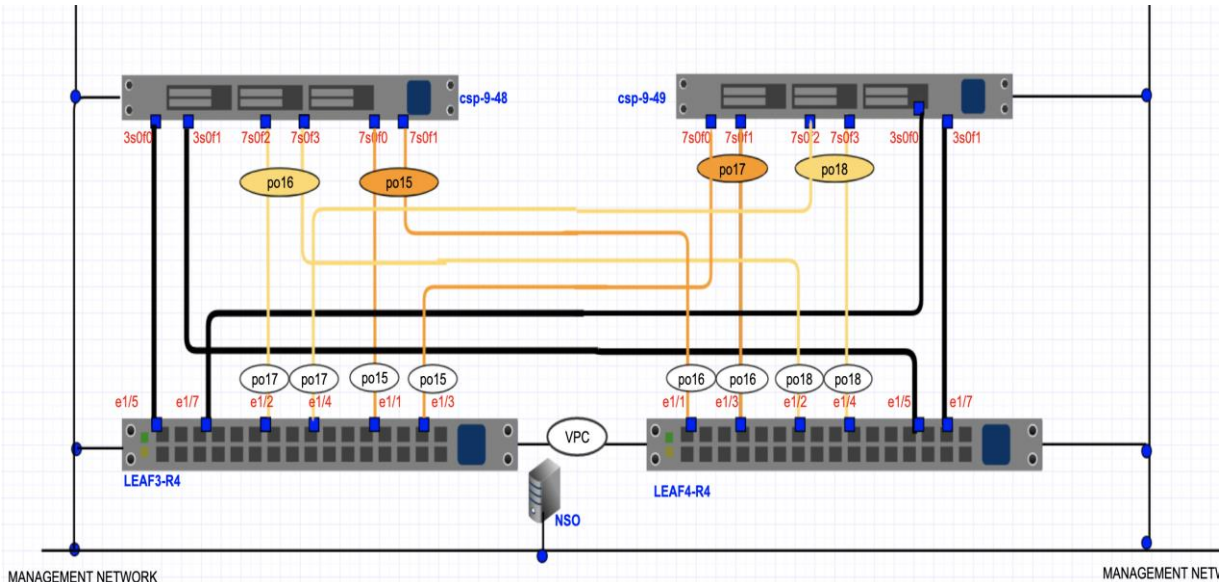
OoB: ISR4331 + EtherSwitch



cisco Live!

SAE Standalone – Wiring Topology

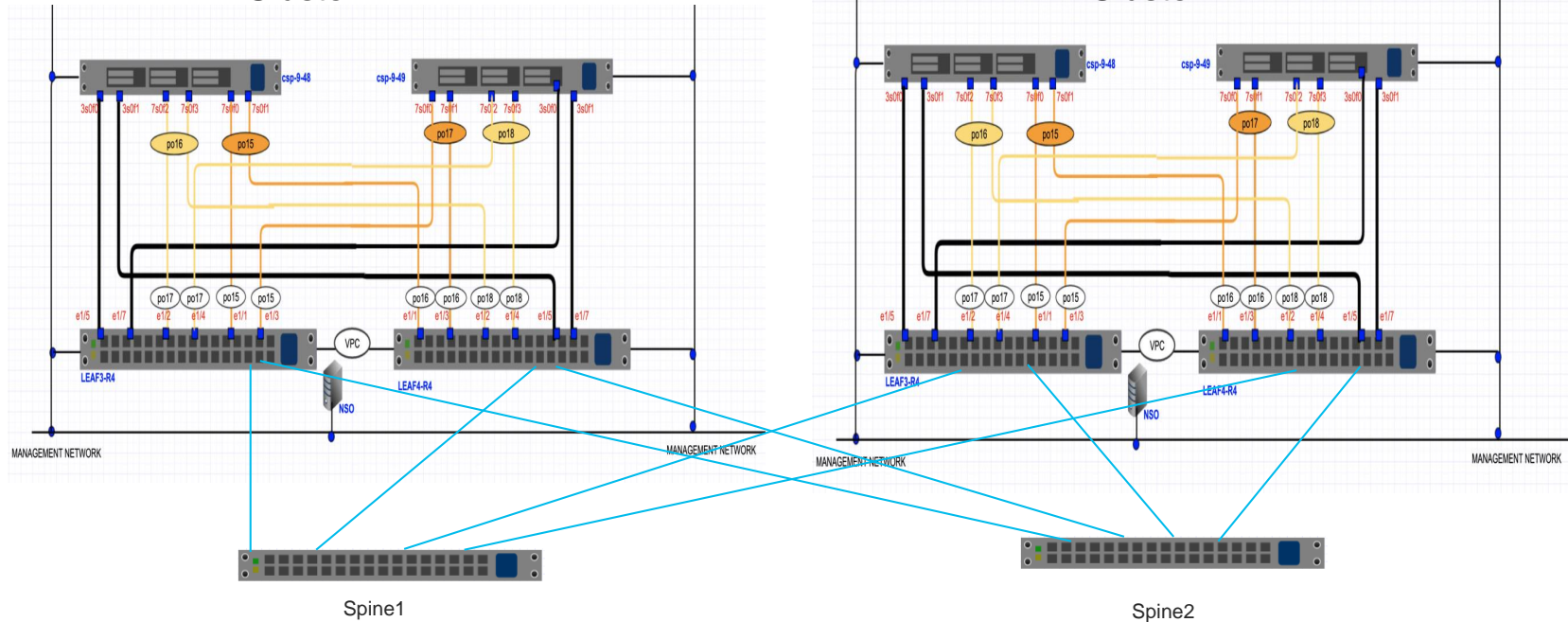
- Wire 2 N9K-C93180YC-FX to 2 CSP5K



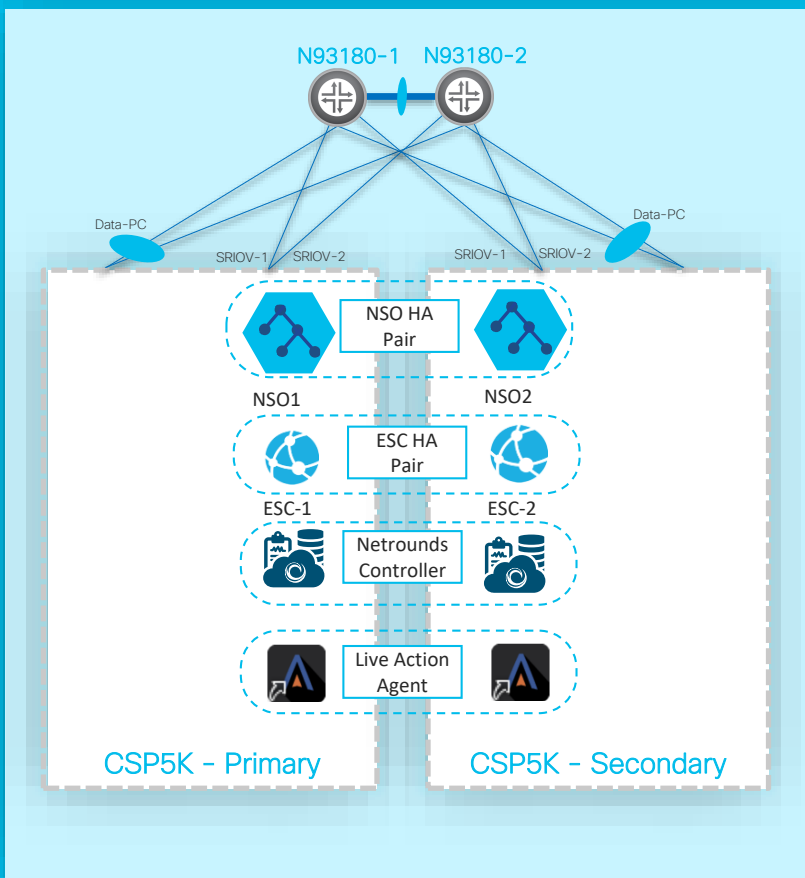
CSP	Pnic	Pnic-type	Port-channel/SRIOV	N9K	Port-Channel	Interface
csp-9-48	enp7s0f0	X710	DATA-PC	LEAF3-R4	port-channel15	Ethernet1/1
csp-9-48	enp7s0f1	X710	DATA-PC	LEAF4-R4	port-channel15	Ethernet1/1
csp-9-48	enp7s0f2	X710	HA-PC	LEAF3-R4	port-channel16	Ethernet1/2
csp-9-48	enp7s0f3	X710	HA-PC	LEAF4-R4	port-channel16	Ethernet1/2
csp-9-48	enp3s0f0	X520	SRIOV	LEAF3-R4		Ethernet1/5
csp-9-48	enp3s0f1	X520	SRIOV	LEAF4-R4		Ethernet1/5
csp-9-49	enp7s0f0	X710	DATA-PC	LEAF3-R4	port-channel17	Ethernet1/3
csp-9-49	enp7s0f1	X710	DATA-PC	LEAF4-R4	port-channel17	Ethernet1/3
csp-9-49	enp7s0f2	X710	HA-PC	LEAF3-R4	port-channel18	Ethernet1/4
csp-9-49	enp7s0f3	X710	HA-PC	LEAF4-R4	port-channel18	Ethernet1/4
csp-9-49	enp3s0f0	X520	SRIOV	LEAF3-R4		Ethernet1/7
csp-9-49	enp3s0f1	X520	SRIOV	LEAF4-R4		Ethernet1/7

SAE Spine Leaf - Wiring topology

- Wire 2 N9K-C93180YC-FX to 2 N9K-C9364C
- Wire 2 N9K-C93180YC-FX to 2 CSP5K
Cluster 1

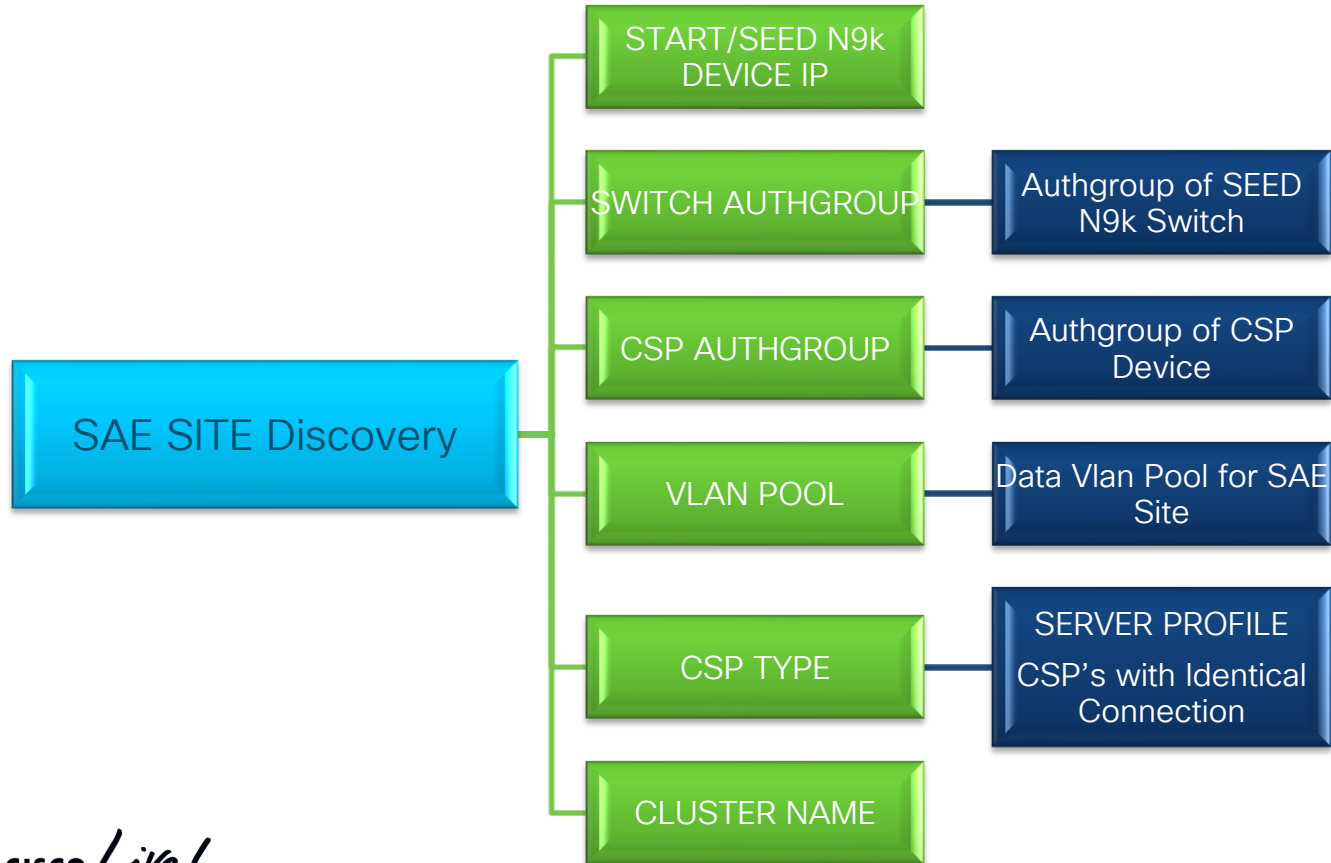


SAE Demo Topology- Infrastructure

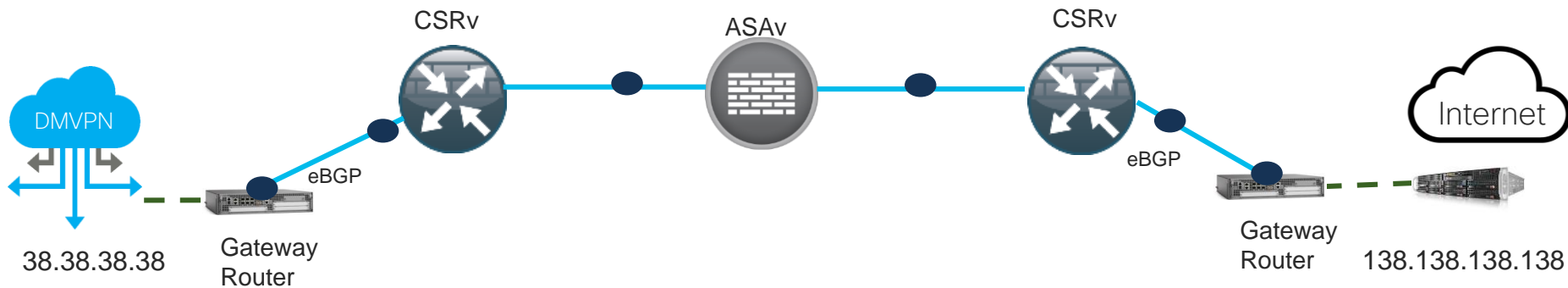


- **Management Domain** will be a separate domain from the SAE Core (Data & Service Plane) for remote management
-
- Dual Switches (N93180) in VPC Pair
- Dual CSP5K - (Min For Management Applications)
- NSO-HA SAE Service Orchestration
- ESC-HA (VNF Life Cycle Management
- Netrounds Controller for Traffic Assurance- Synthetic Traffic Monitoring
- Live Action - SAE Assurance -Active Traffic Monitoring

SAE SITE Infrastructure Discovery



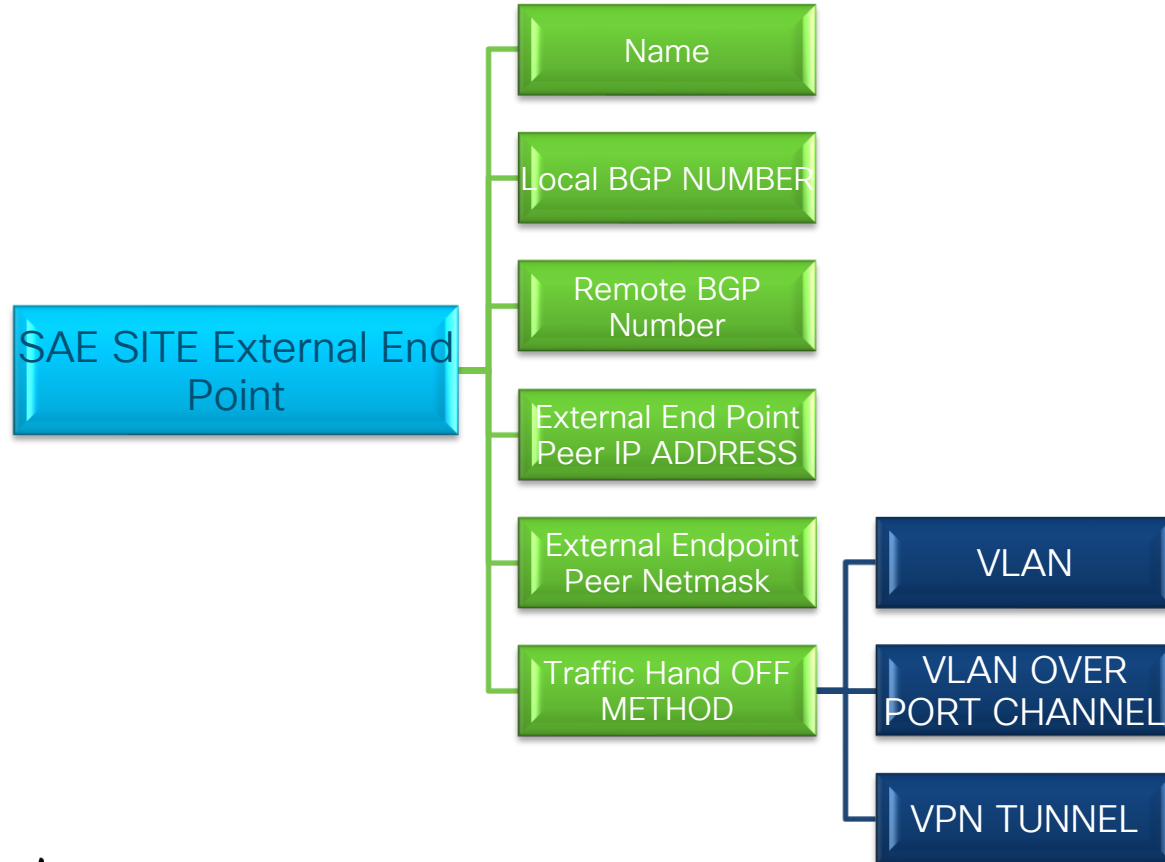
End-to-End Service Chain – External End Point



```
vlan-number          38
local-bgp-as-number  38
remote-bgp-as-number 380
endpoint-ipaddress   38.38.38.1
endpoint-netmask     255.255.255.0
```

```
vlan-number          138
local-bgp-as-number  138
remote-bgp-as-number 1380
endpoint-ipaddress   138.138.138.1
endpoint-netmask     255.255.255.0
```

SAE SITE – External End Point





Break

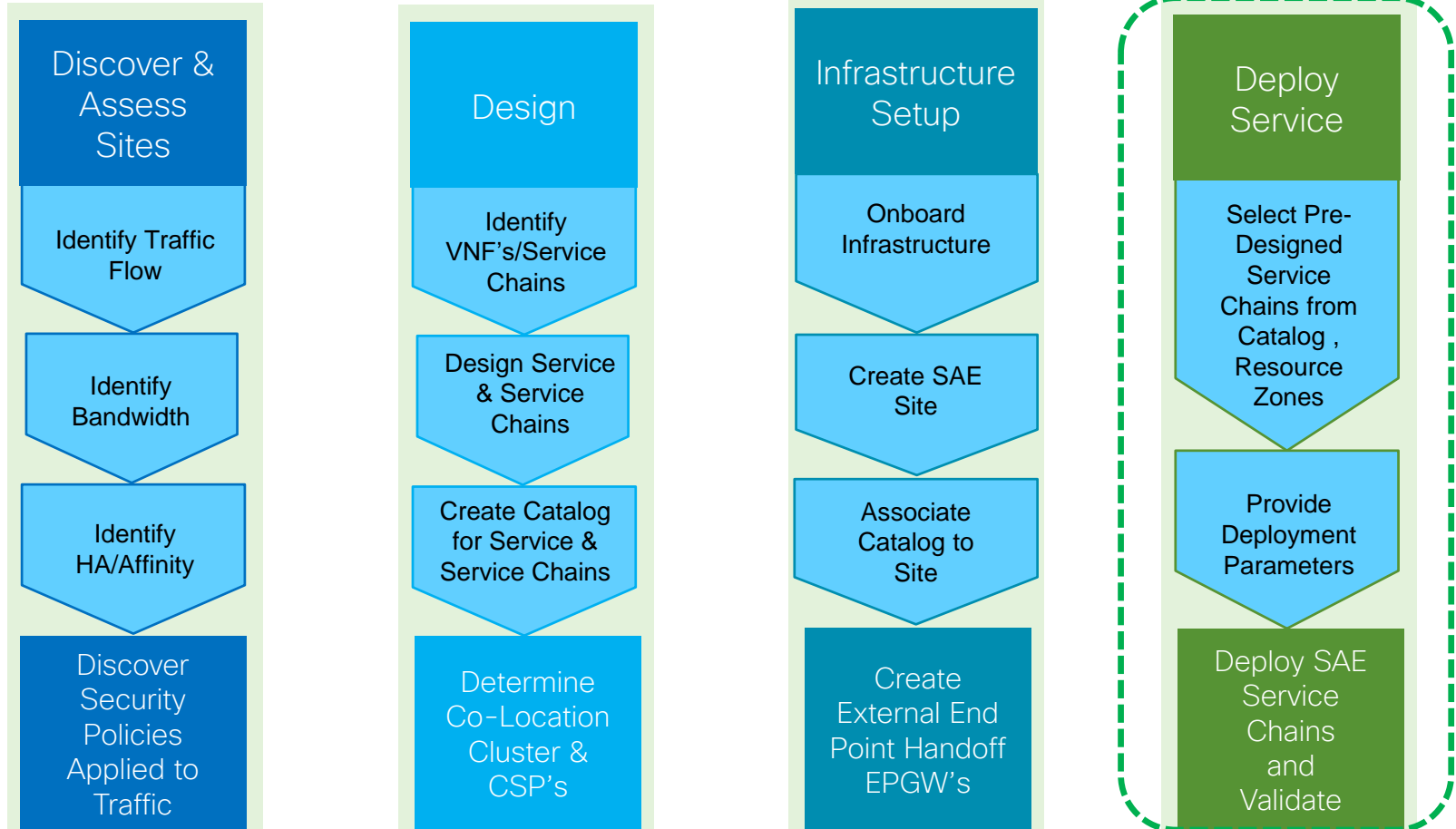
Agenda

- Secure Agile Exchange (SAE) Overview
- SAE Planning
- SAE Design
- SAE Infrastructure
- Break -----
- SAE Deployment
 - End to End Service Chains
 - SAE Assurance and Day2 Service Operation.
 - Shared Endpoint Gateway and Half Service Chains
 - Stitching Service Chains and Shared End Point Gateway
- SAE Debug and Troubleshooting
- SAE Roadmap and References
- SAE Conclusion / Q & A

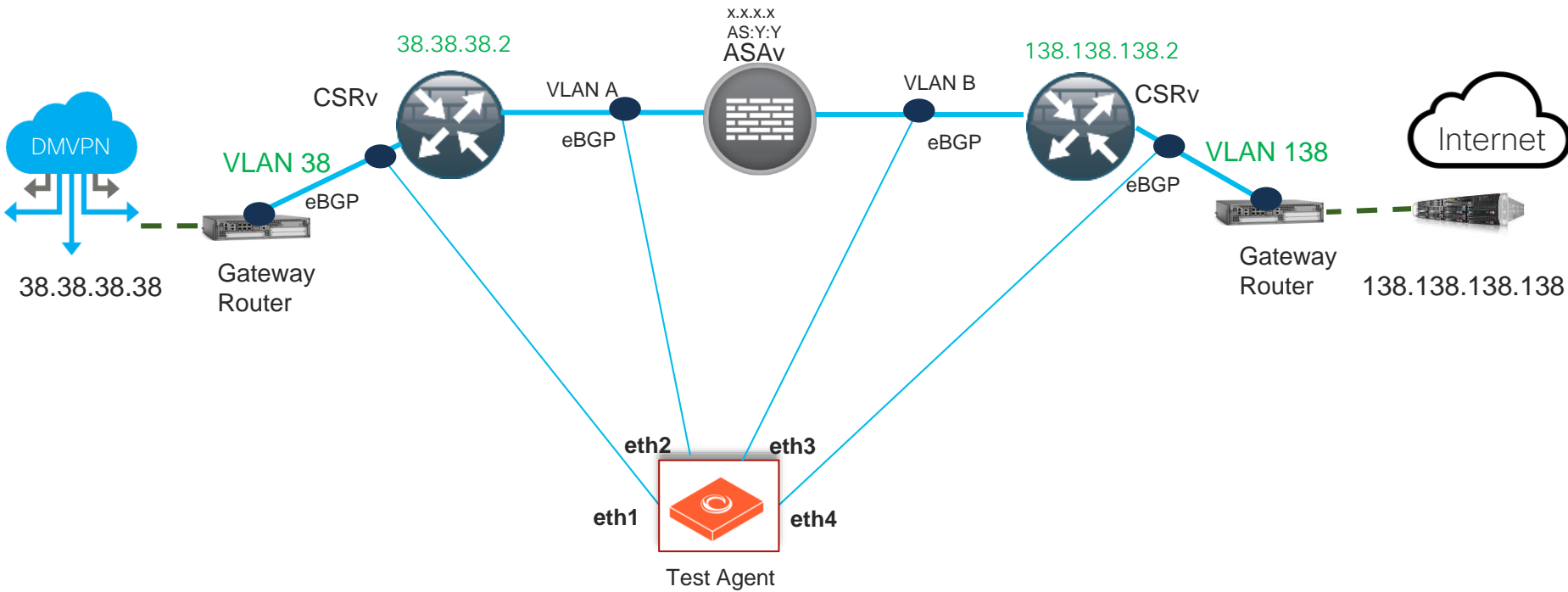
SAE Deployment

End to End Service Chains

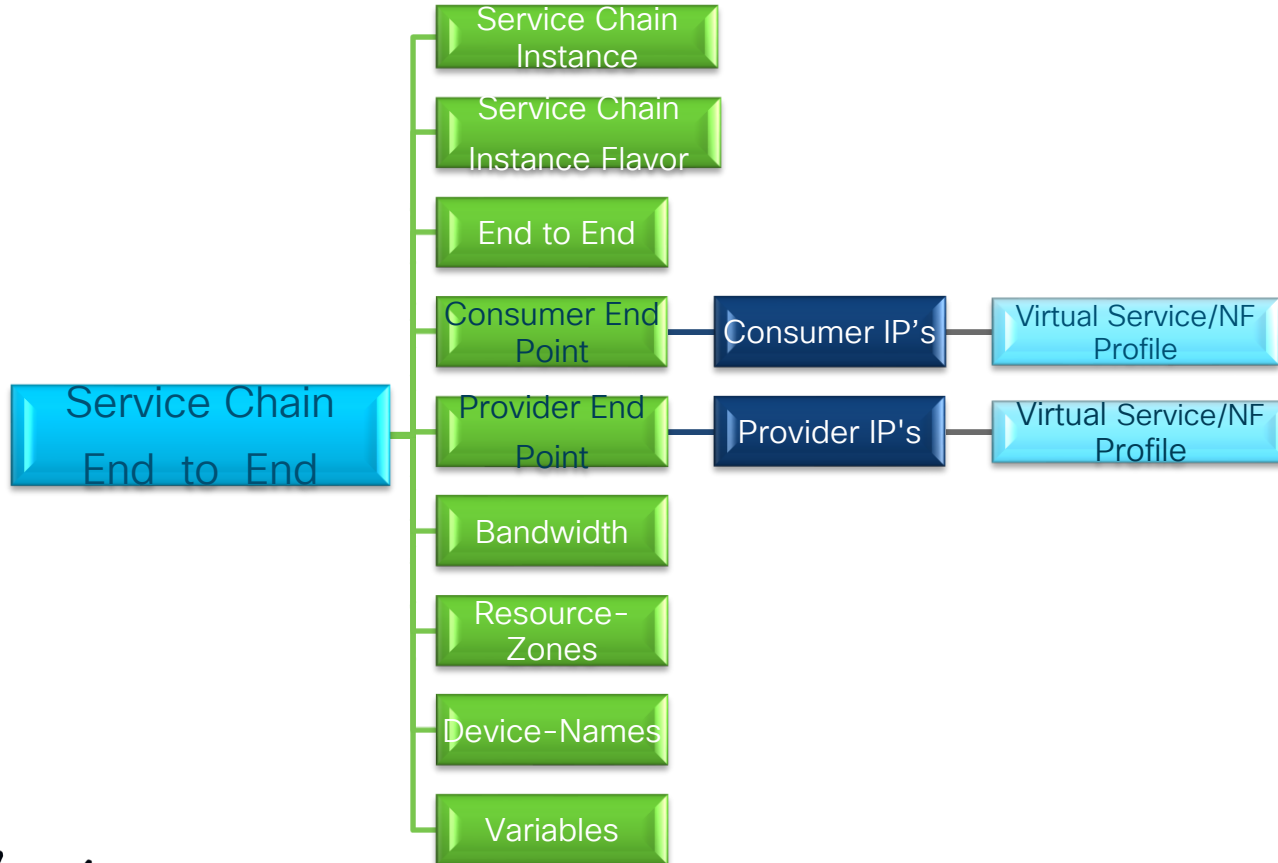
SAE Workflow



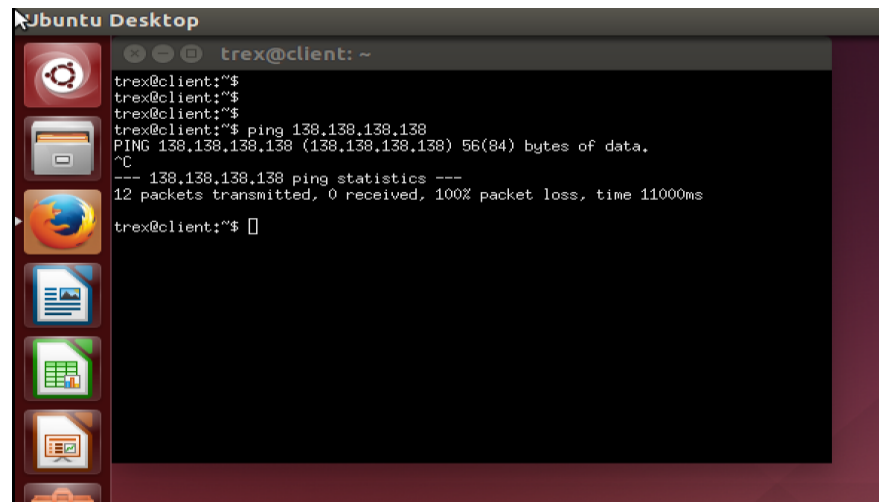
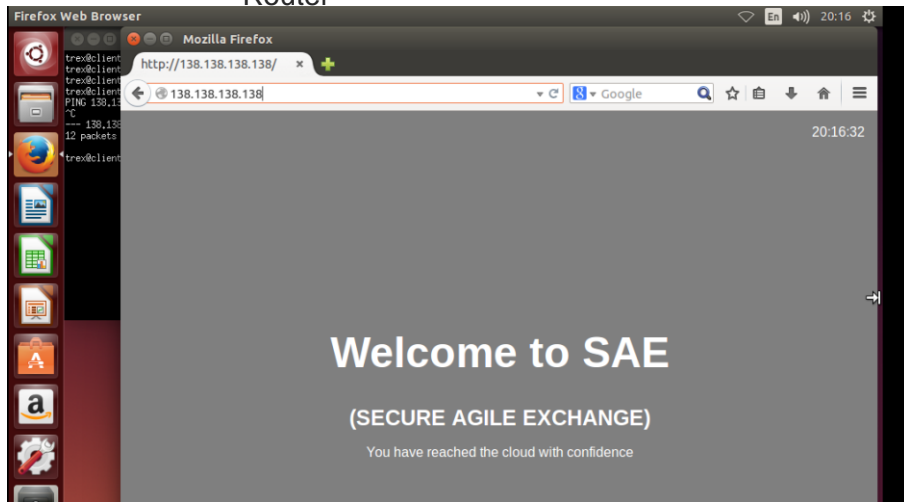
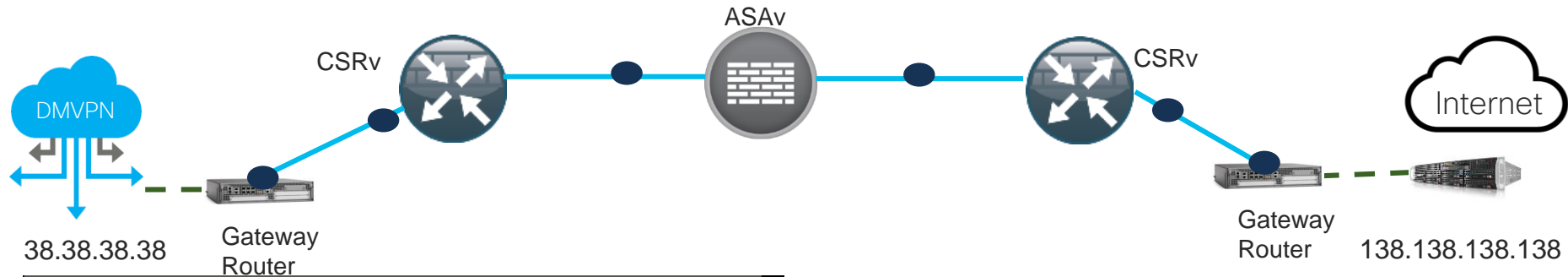
End-to-End Service Chain Deployment



Service Chain - End to End



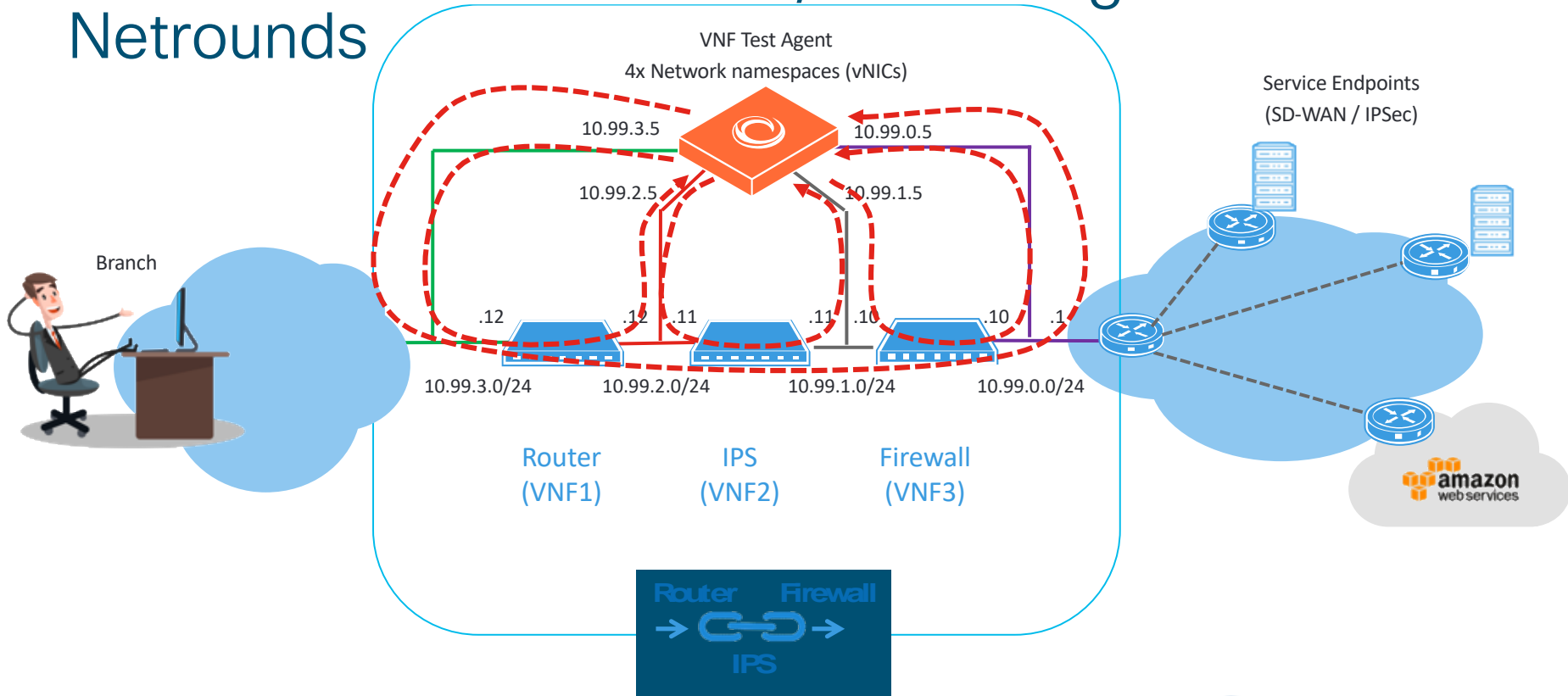
Branch connectivity to application in the Cloud



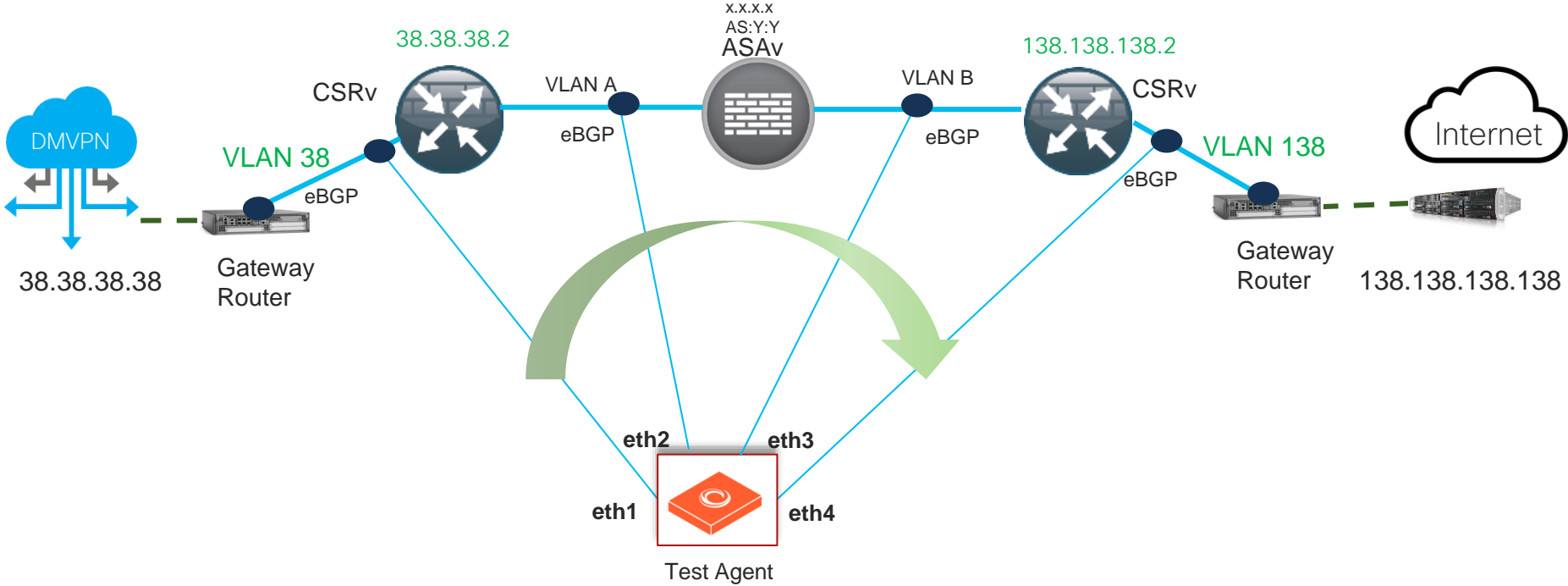
SAE Deployment

SAE Assurance and Day2 Service Operation.

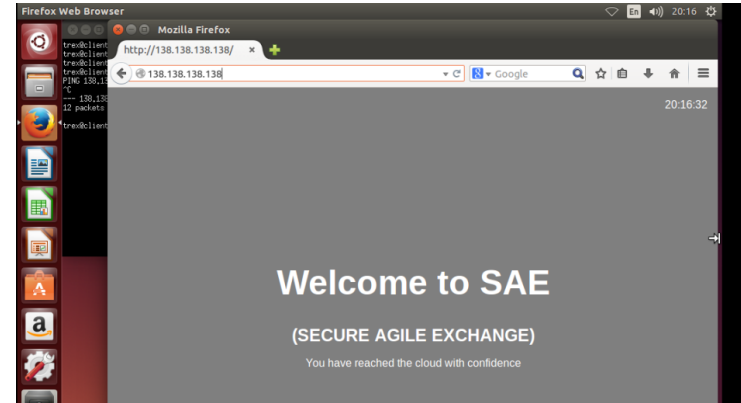
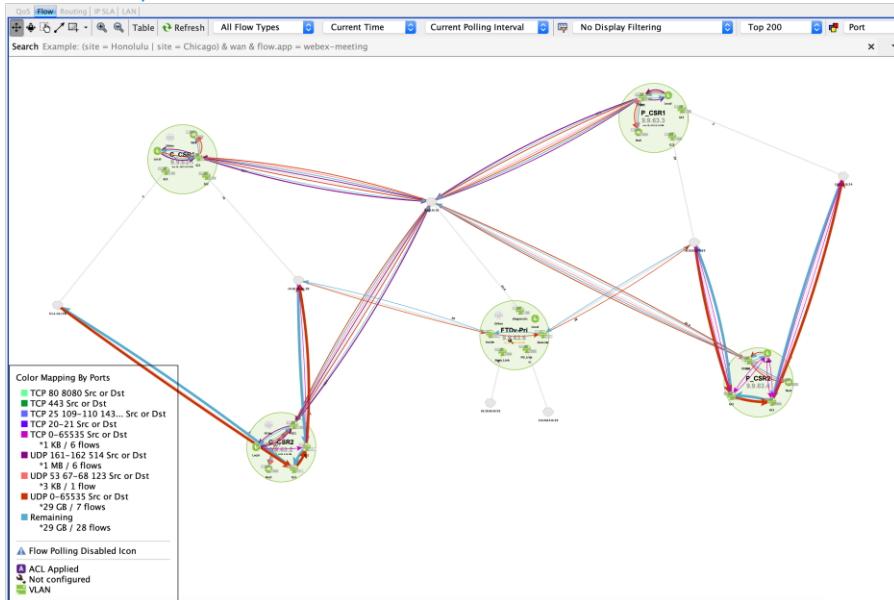
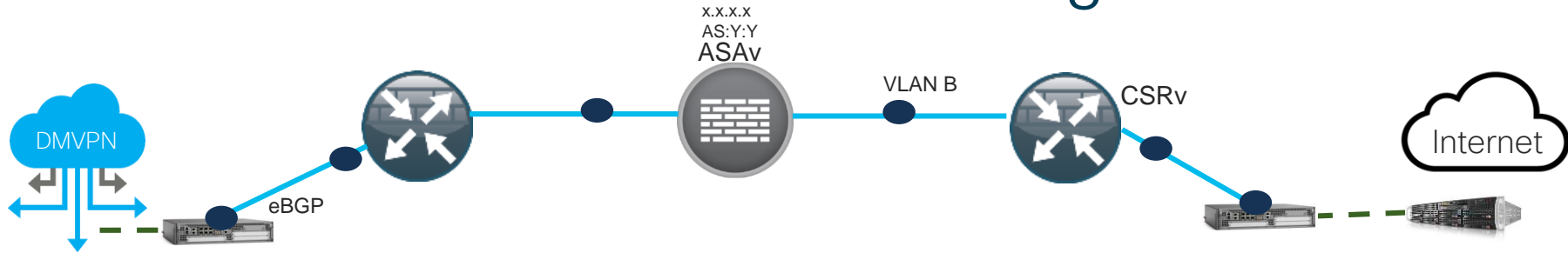
SAE Service - Validation/Monitoring with Netrounds



Service Chain Monitoring – DMVPN to Internet



Service Chain Active Traffic Monitoring – Live Action

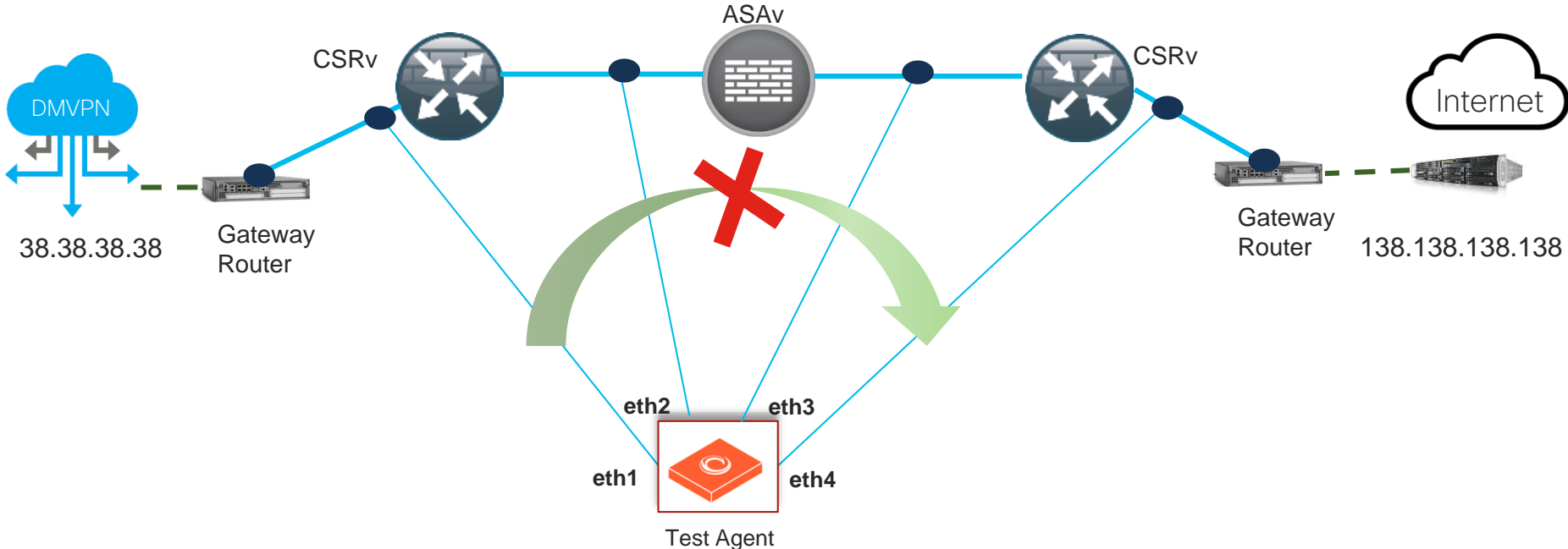


cisco Live!

LiveAction

SAE Service Chain - Day 2 operation

-Disable Web Access

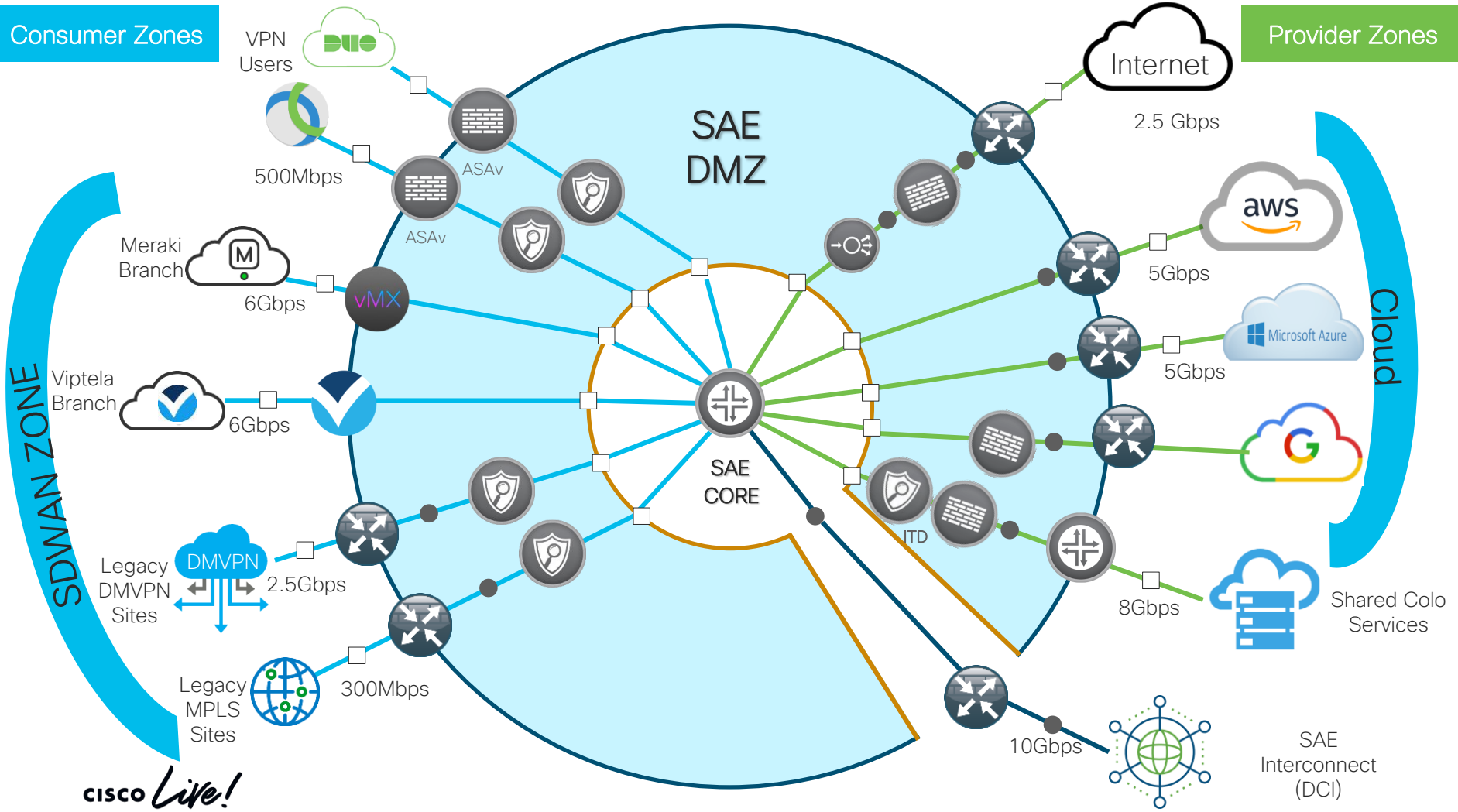


SAE Deployment

Shared Endpoint Gateway and Half
Service Chains

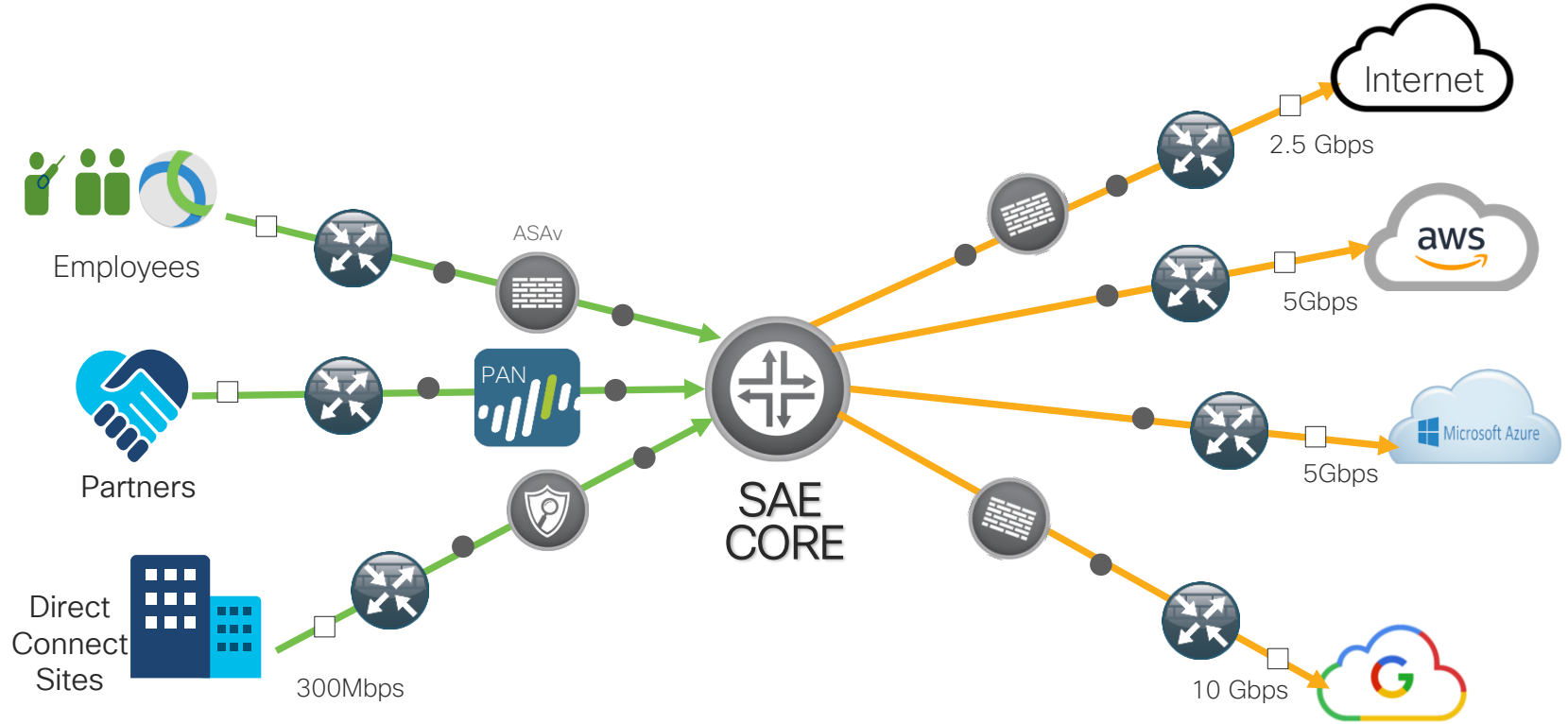
Consumer Zones

Provider Zones

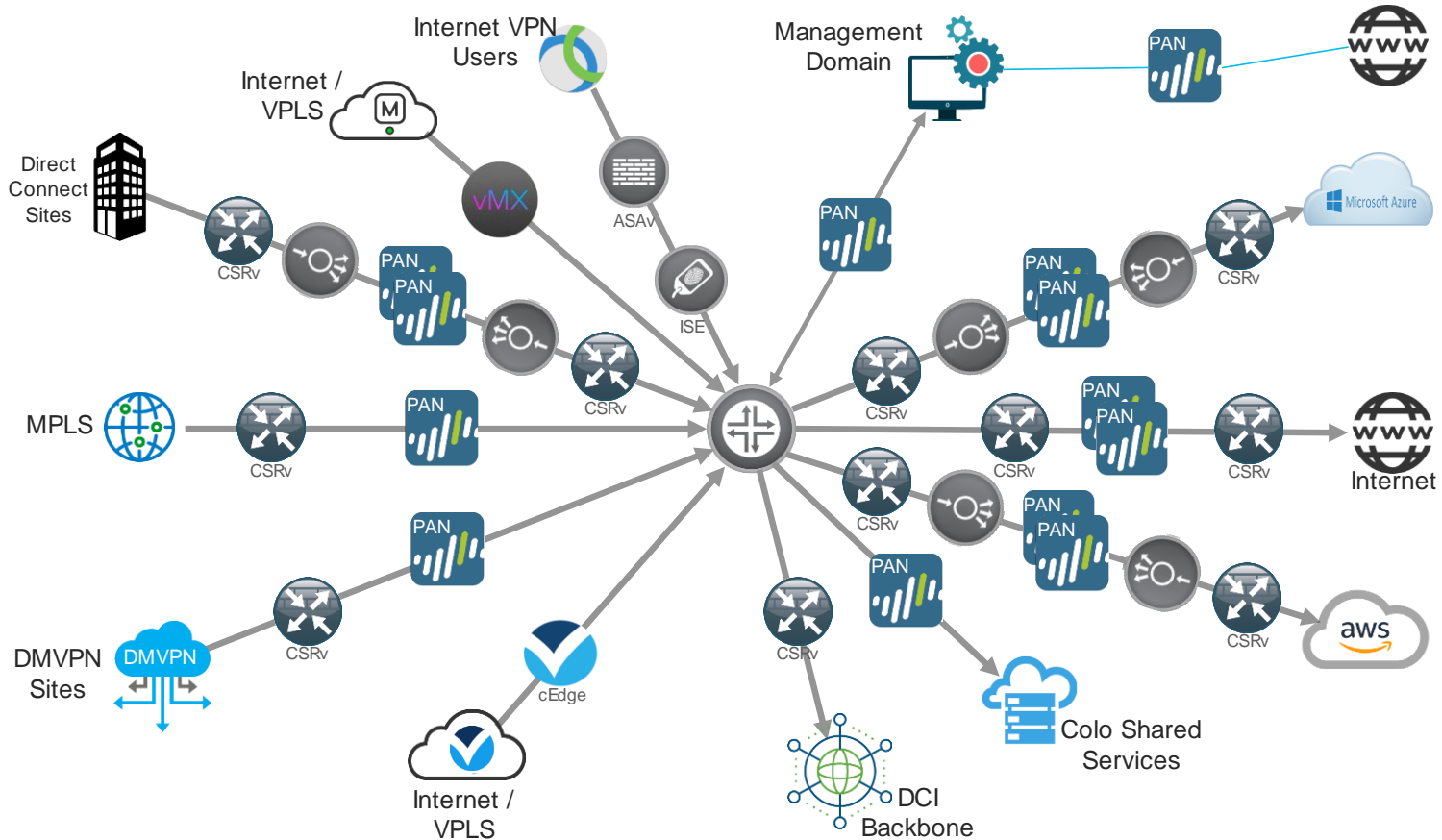


CISCO Live!

SAE Consumer and Provider Service Chain

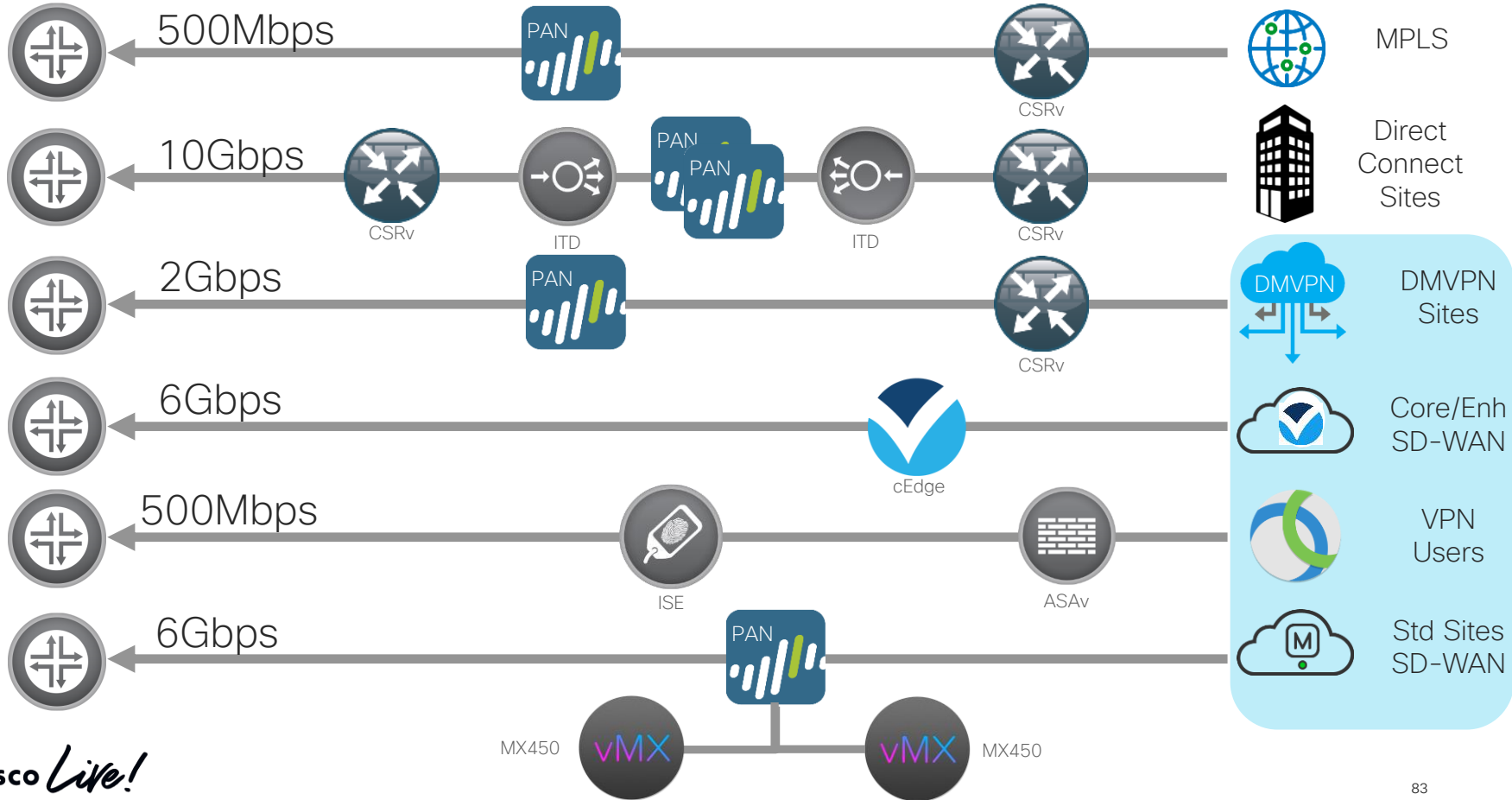


SAE Service Chain Connectivity

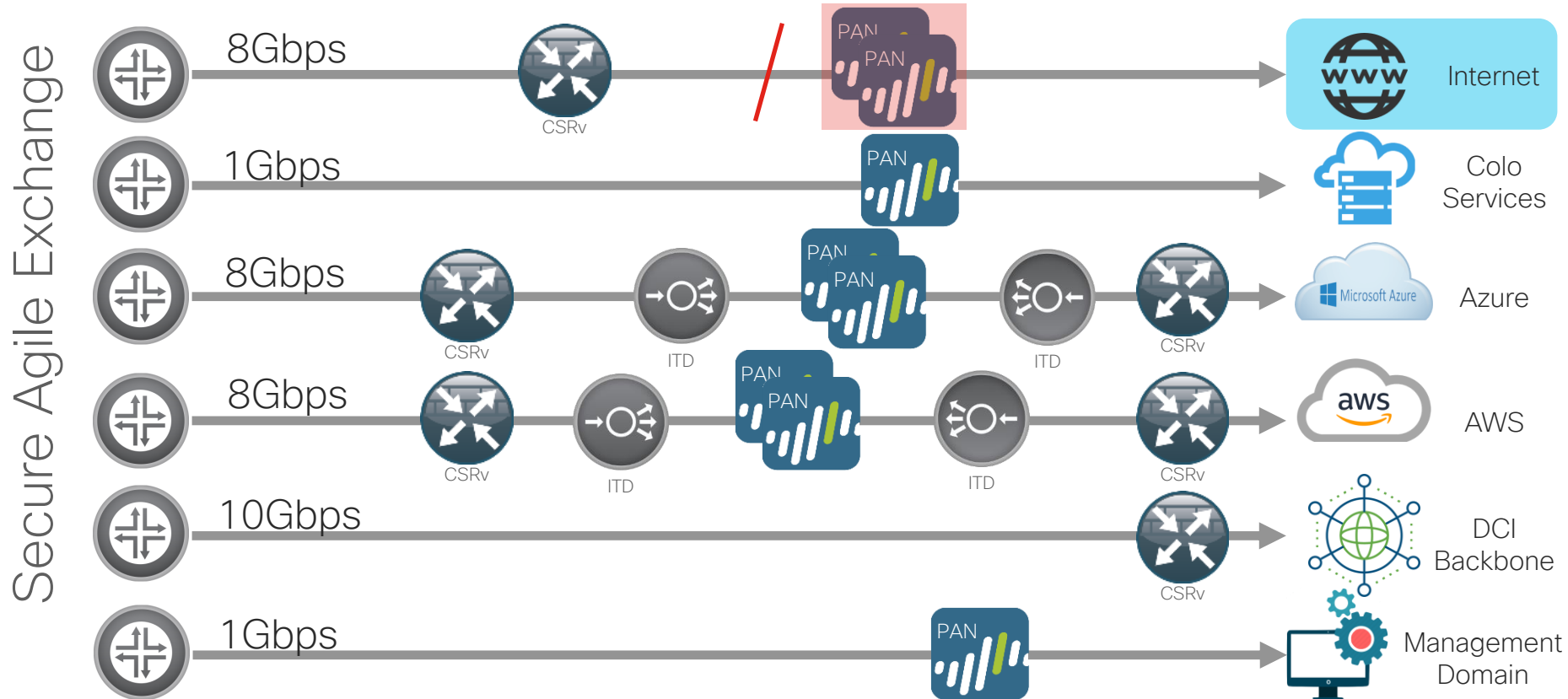


Inbound Service Chain Design

Secure Agile Exchange



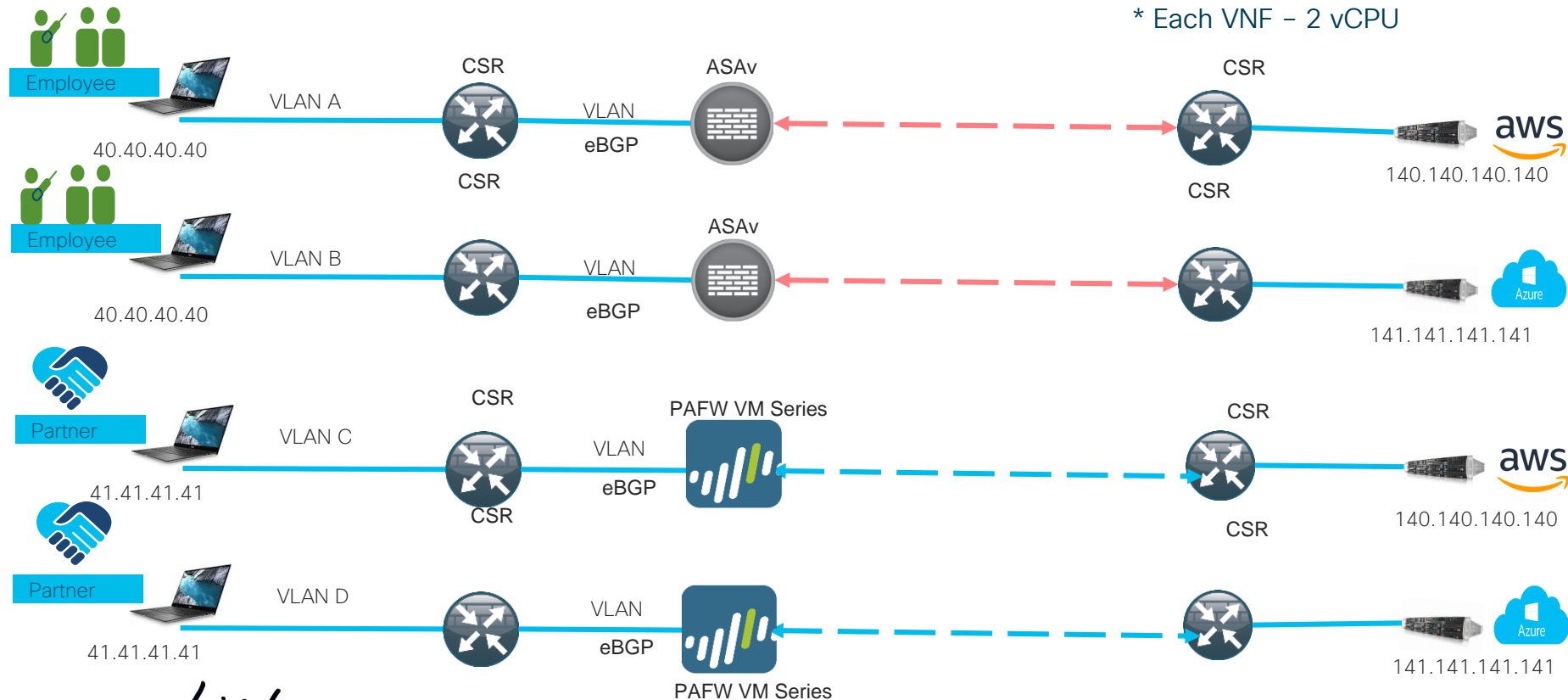
Outbound Service Chain Design



Static Chains

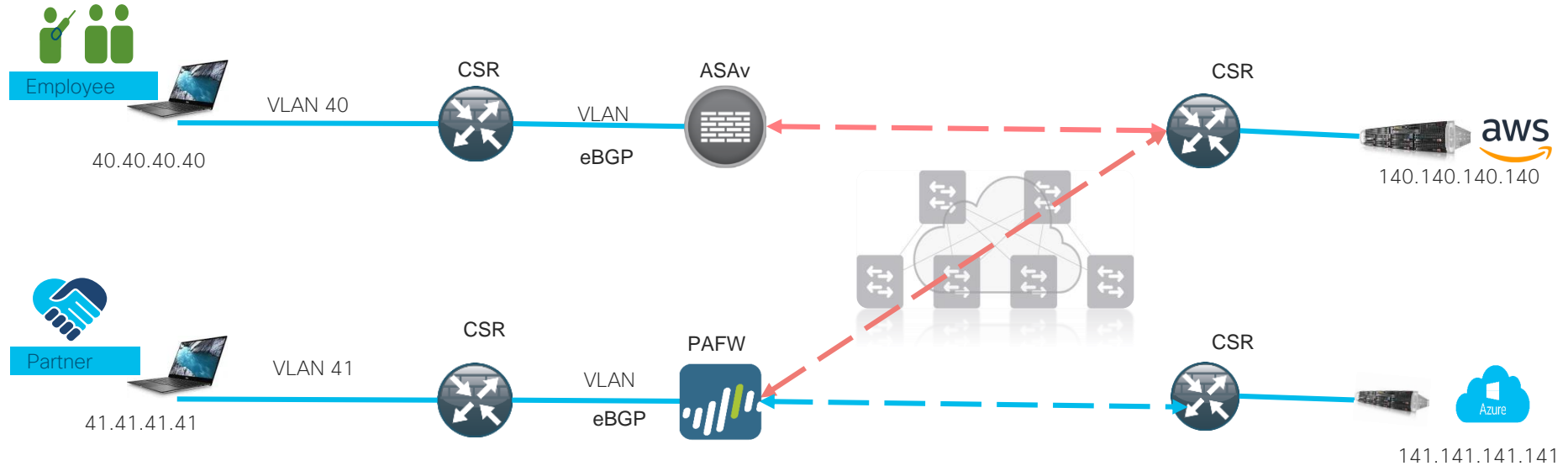
End to End chain Requirements - 4 chains/24 vCPU

* Each VNF - 2 vCPU



CISCO Live!

Dynamic Access using Chain Stitching



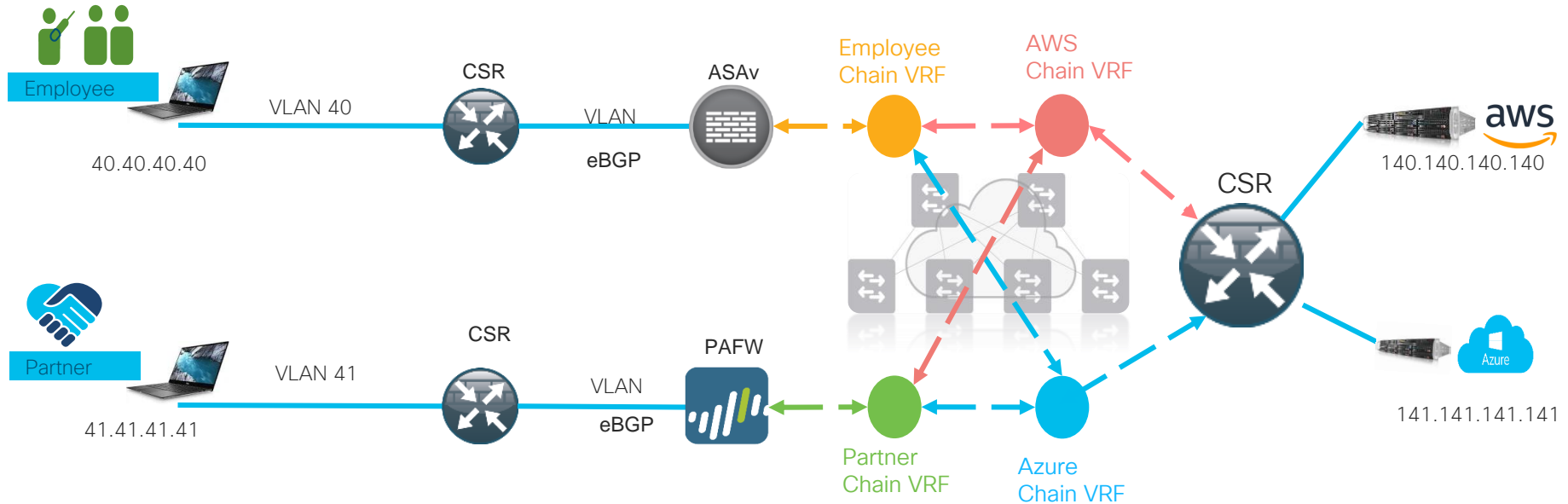
Benefit:

- ✓ Access to additional providers simplified
- ✓ Savings on compute resources

Dynamic Access enablement using Chain Stitching

Consumer Chain < ----- > Provider Chain Requirements – **3 chains/10 vCPU**

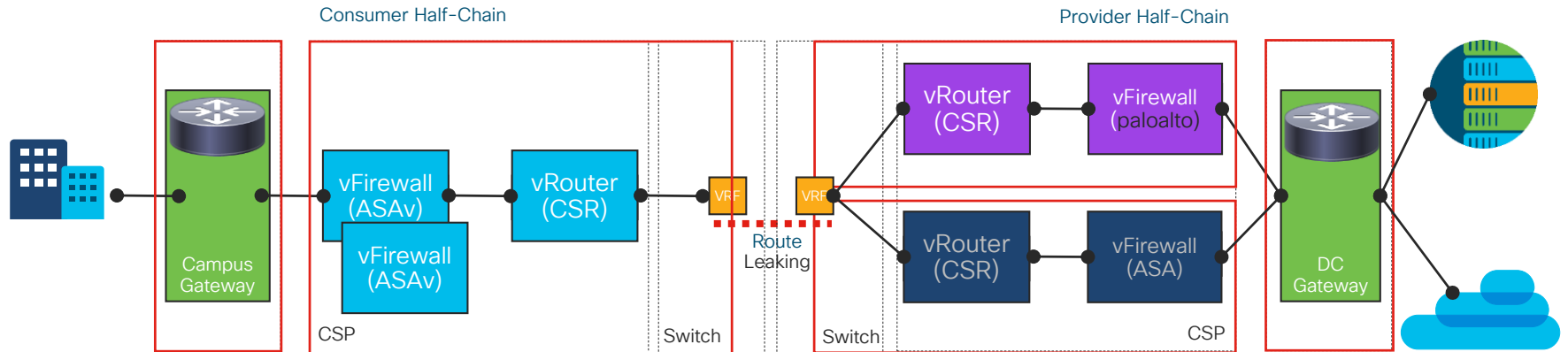
* Each VNF – 2 vCPU



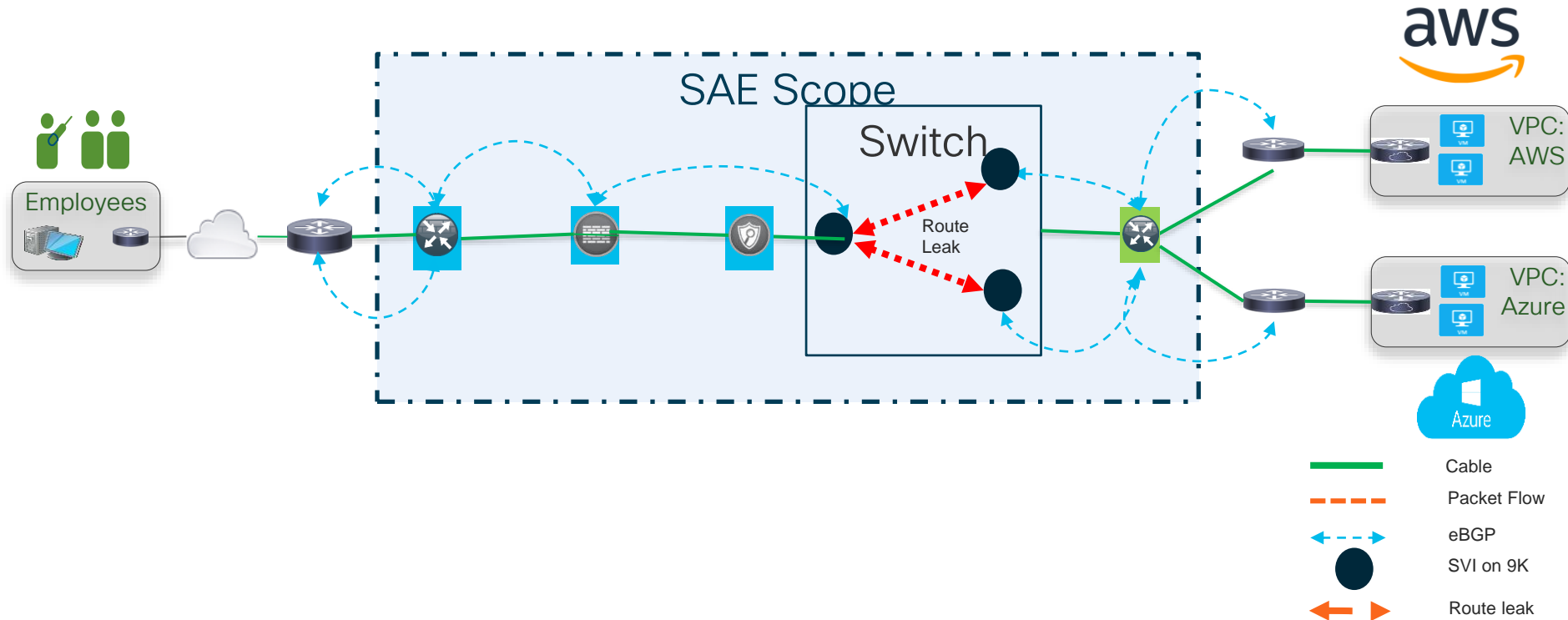
SAE Deployment

Stitching Service Chains and Shared End
Point Gateway

SAE Half Chain Use Case

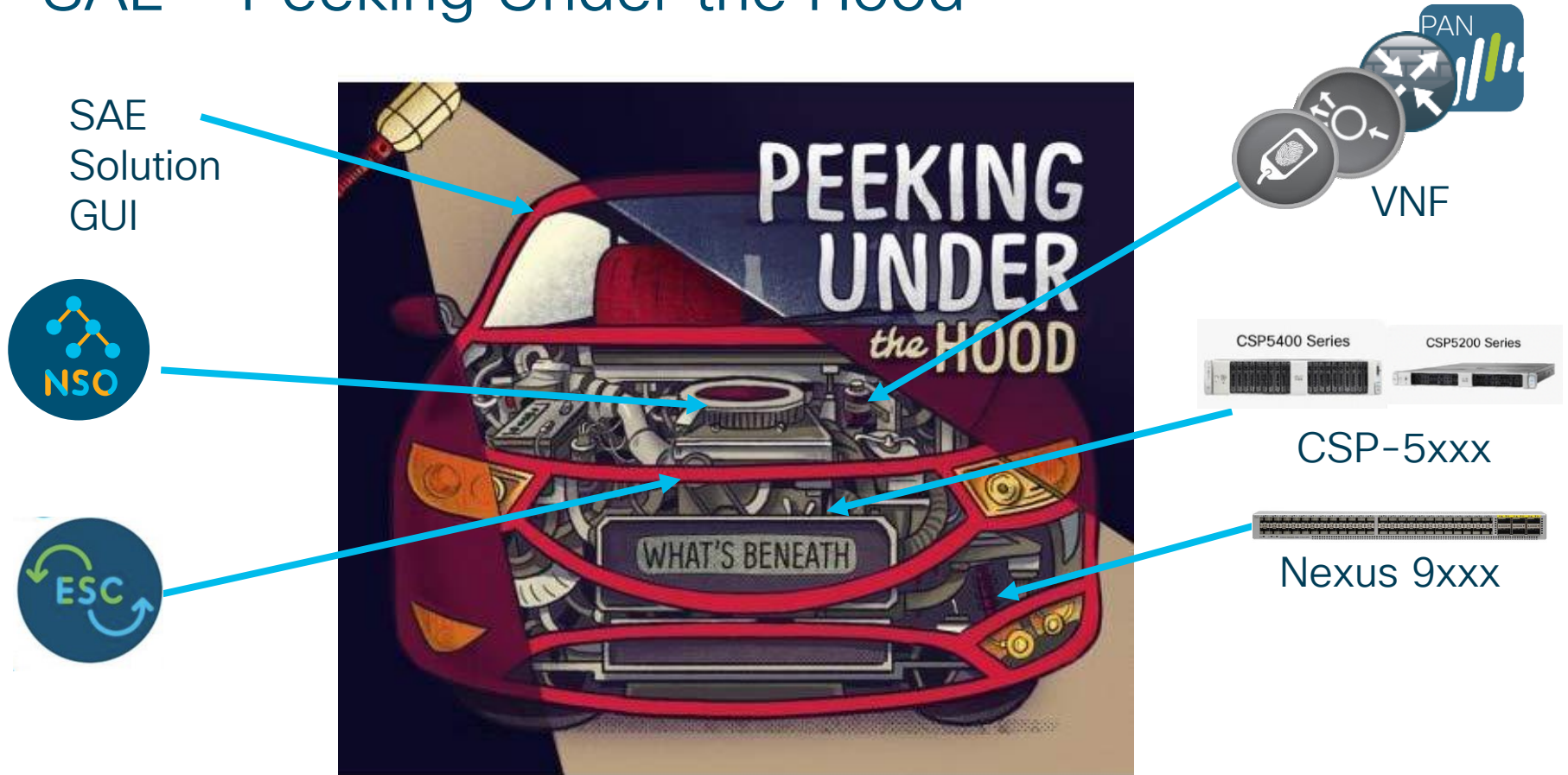


VNF Sharing Consumer: Logical view



SAE Debug and Troubleshooting

SAE – Peeking Under the Hood



System Requirements NSO SAE CFP with GUI.

- NSO + Core Function Pack + GUI can be installed on any Ubuntu/RedHat/CentOS System.

OS	Ubuntu	Red Hat	CentOS	MacOSX
Minimum Server Configuration	CPU-8 Cores RAM-24 GB Disk-300GB	CPU-8 Cores RAM-24 GB Disk-300GB	CPU-8 Cores RAM-24 GB Disk-300GB	CPU-8 Cores RAM-24 GB Disk-300GB
Version	16.04.4 LTS 17.10 18.04 LTS	7.3 (Maipo)	7.4 (Core)	10.12.6

❖ System ulimit set to 65535 (open file)

[Extensive Documentation for Deployment, Debugging and Troubleshooting available in below link:](#)

[SAE Solution GUI :](#)

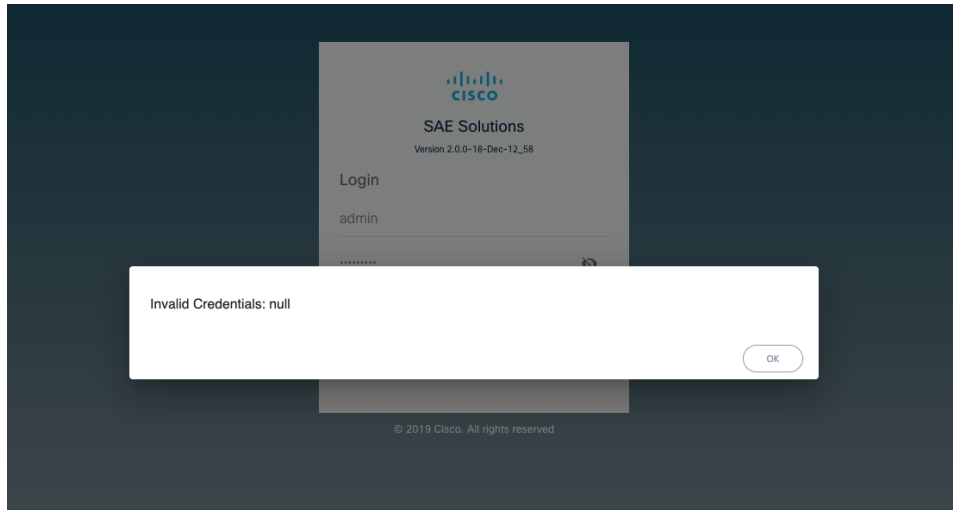
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/Cloud-Services-Platform/csp_5000/sae/release_notes/sae-ui-release-notes-2-0.html#

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/Cloud-Services-Platform/csp_5000/sae/user-guide/b-sae-user-guide/get-started.html#



SAE Solution GUI Troubleshooting

- SAE Solution GUI Installation has prerequisite checks defined.
- For SE-LINUX issue on Centos, set below to avoid invalid credentials: null
sudo setsebool -P httpd_can_network_connect on



NSO/SAE CFP Troubleshooting



- NSO + Core Function Pack Installation
 - NSO is installed on Ubuntu/CentOS as system installation and SAE Core Function Pack is installed post NSO installation .
- SAE Site Infra Discovery.
 - Performs the Infrastructure Discovery for SAE Site based on topology connected between N9k, CSP and PNF devices.
- Resource Orchestration Placement.
 - Performs placement of VNF based on various requirements defined in NFV - VNFD, NSD ,Affinity/Anti-Affinity , Bandwidth etc.

Extensive Documentation for Deployment, Debugging and Troubleshooting available in below links:

NSO: <https://www.cisco.com/c/en/us/support/cloud-systems-management/network-services-orchestrator/tsd-products-support-series-home.html>

NSO SAE Core Function Pack : - SAE User Guide, Installation Guide and Troubleshooting Guide

<https://software.cisco.com/download/home/286323467/type/286321795/release/2.0.0>

NSO SAE CFP Installation Troubleshooting



Problem

System Installation failed with following error

```
nso-4.7.1-cisco-sae-core-fp-1.0.0-9/installer/core-FP-installer$ ./install.py
```

```
PLAY *****
```

```
TASK [setup] *****
```

```
fatal: [172.25.86.74]: UNREACHABLE! => {"changed": false, "msg": "ERROR! SSH Error: data could not be sent to the remote host. Make sure this host can be reached over ssh", "unreachable": true}
```

Solution

Check NSO Host is reachable and re run installation .

Problem

Packages failed to come up, oper-status of some packages are down

Solution:

Check ulimit on NSO system set to allow 65535 open file systems.

Reload NSO System and perform restart of NSO with package-reload

Restart ncs process

```
sudo /etc/init.d/ncs restart-with-package-reload
```


NSO SAE CFP Logs Troubleshooting



- Enable Logs - detailed logging is disabled in NSO SAE CFP by default. Please enable logs as below:
set devices global-settings trace raw
set java-vm java-logging logger com.cisco level level-all
set python-vm logging level level-debug
- Log files are located under: `/var/log/ncs`

Components and logs - SAE-Site Components and logs can be seen as below

Component	Logs
SAE-Site Deployment	ncs-java-vm.log
Placement	ncs-python-vm-tailf-etsi-rel2-nfvo.log
Image	ncs-python-vm-tailf-etsi-rel2-nfvo-csp.log
Discovery	ncs-python-vm-infra-discovery.log ncs-python-vm.log
VNF Deployment	netconf-ESC-*.trace
Day1 config	ned logs for VNF -CSR,ASA, etc.
N9k	ned-cisco-nx-*.trace
CSP	netconf-csp-*.trace
Commands history	Audit.log

ESC - Troubleshooting



Login to ESC Device (VIP for HA)

Logs are located under: `sudo cd /var/log/esc`

Component	Logs
Main ESC log	esc-manager.log
VNF deployment	yangesc.log
VIM manager	vimmanager/vimmanager.log
Monitoring and Action	mona/mona.log

[Extensive Documentation for Deployment, Debugging and Troubleshooting for ESC available in below link:](https://www.cisco.com/c/en/us/support/cloud-systems-management/elastic-services-controller-esc/tsd-products-support-series-home.html)

<https://www.cisco.com/c/en/us/support/cloud-systems-management/elastic-services-controller-esc/tsd-products-support-series-home.html>

ESC - Troubleshooting Commands



		ESC-5.0 and above CLI
ESC version		esc_version
Operation/maintenance mode		escadm op_mode show escadm op_mode set --mode MAINTENANCE escadm op_mode set --mode OPERATION
current configurations		escadm dump(dump in yaml format)
Verification the vim settings are correctly populated		escadm vim show
ESC backup DB		escadm backup --file /tmp/db.tar.bz2
ESC restore DB		escadm restore --file /tmp/db.tar.bz2
Collect Logs		escadm log collect
ESC Service control (Start/Stop ESC service) in HA	check status	escadm status --v
	stop	sudo escadm stop
	start	sudo escadm start
	restart	sudo escadm restart

Cloud Services Platform(CSP)-5xxx-Troubleshooting

- CSP-5xxx used in SAE environment are being pre configured with connectivity to Nexus N9k
- VNF Deployment is deployed and monitored by ESC
- NSO SAE Service performs Infra Discovery based on configuration in N9k and CSP.
- NSO SAE Service initiates deployment of VNF on CSP after performing resource request checks.

[Extensive Documentation for Deployment, Debugging and Troubleshooting for CSP-5xxx available in below link:](#)

<https://www.cisco.com/c/en/us/support/switches/cloud-services-platform-5000/tsd-products-support-series-home.html>

Nexus 9xxx - Troubleshooting

- N9Ks used in SAE environment are being configured by NSO CFP. Therefore, avoid configure N9K out-of-band. All N9K configuration should be done via SAE CFP.
- If N9K is out-of-sync with NSO CFP, make sure to sync it with NSO CFP by issue command

```
request devices fetch-ssh-host-keys
```

```
request device sync-from
```

[Extensive Documentation for Deployment, Debugging and Troubleshooting for Nexus9xxx available in below link:](#)

<https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html>

Nexus N9xxx - Troubleshooting

Main routing protocol used in SAE is BGP. Commands useful to debug in Nexus N9k

```
show ip route
```

```
show bgp all
```

```
show bgp sessions
```

```
show ip bgp summary
```

```
show ip bgp neighbor
```

```
show ip bgp neighbor <IP-address-of-neighbor> routes
```

```
clear ip bgp *
```

```
terminal monitor  
debug ip bgp events
```

```
show ip bgp regexp ^$
```

VNF Troubleshooting - Scenario



Problem : VNF deployed is not reachable and ESC performing recovery

Solution :

Check VNF deployment has appropriate config needed to bootup :

1. day0 destination (ASA, FTDv - day0-config, CSR - iosxe-config , AVISE - avi_meta_se.yml, etc.)
2. day0 file has the minimum configuration \$NICID_0_IP_ADDRESS, \$NICID_0_CIDR_ADDRESS, \$NICID_0_GATEWAY gateway etc.
3. Verify the values are assigned that will be reachable by ESC and NSO .

Problem: After service is deployed , VNF SSH authentication failure and plan is failed.

Solution :

Check authgroups provided for the VNF correct them if needed, verify the connection is fine from NSO. Delete the service and create a new service.

or

Check connectivity and correct authgroup if incorrect. Perform replay of ESC notifications after ESC has sent VM_ALIVE as below.

```
admin@ncs> request devices device ESC-vmware netconf-notifications subscription cisco-etsi-nfvoreplay from-date-time
```

Possible completions:

```
<dateTime (CCYY-MM-DDTHH:MM:SS)>
```

SAE Solution Recovery Mechanism:

- SAE Solution offers various recovery mechanisms:
 - SAE-Site Actions :

SAE Site Actions Command	Description
<code>sae-actions recover-vnf-on-vim < sae-site> .. tab</code>	Initiate Recovery of VNF on SAE Service
<code>sae-actions recover-vnf-on-vim realloc-on-same < sae-site> .. tab</code>	Initiate Recovery of VNF on SAE Service and reallocate on same VIM (CSP)
<code>sae-actions services-on-csp</code>	List services on CSP device
<code>sae-actions undep-redep-services-on-csp</code>	Perform undeploy-redeploy of all services on CSP device

SAE Solution Cleanup

- SAE Solution offers various cleanup operations in event deletion of specific SAE Services fail
 - SAE Cleanup Actions are offered as below options :
 - NSO CDB cleanup
 - Network Wide cleanup (with more option)

SAE Site Actions Cleanup Command	Description
action-status-cleanup	Clear sae-action-status records
compute-cleanup	Will cleanup leftover data for compute day1 service
endpoint-gateway-vnf-cleanup with more	Will cleanup leftover data for endpoint-gateway-vnf service
service-chain-cleanup with more	Will cleanup leftover data for service-chain service
stitching-service-cleanup with more	Will cleanup leftover data for stitching service
vnf-manager-cleanup with more	Will cleanup leftover data for vnf-manager service

SAE Deployment Best Practice

- Setup NTP on NSO,ESC, CSP, N9k nodes and other nso-unmanaged devices , ensure ntp is enabled and time synch performed . Preferred to have these devices in same Time Zone.
- Controllers for VNF – FMC, AVI Controller, Panorama etc to be spun as pre-requisite.
- Individual IP address subnet for Management Pool and Data pool , with licensing enabled (optional). Provide proxy configuration for vnf's and nso-unmanaged devices to reach internet when needed.
- Check on NSO-SAE-Site-Status plan before proceeding to next steps , during multiple create and delete operations .
- N9k- VPC peer link (day-1) must be configured to allow VLAN 1 .
- Multiple SAE Cluster – Spine-Leaf switch method – Infra-Discovery, each cluster needs to have a unique CSP type name.
- SAE Customizations (custom templates available from NSO for users to perform any custom operation on specific devices managed by NSO.
- After every deletion operation please ensure there are no stale data left behind on any device and NSO plan status is cleared for the particular operation.
- Perform Cleanup operations as described in SAE Solution Cleanup for any deletion failures.

SAE Roadmap and References

SAE Completed Releases

SAE 1.1 Q2'19(Apr)

- Physical device- FTD
- Assurance Enablement
- CSR-IPSec support
- Sub-interface support
- Dynamic endpoint add

- X710-SR-IOV

- Production UI
 - Chain health status
 - Infra discovery

- Physical device orchestration

SAE 1.2 July '19

- Physical device-ASR
- Tested chain documentation

- 1.1 Catchup release

- Rockwell requirements

SAE 2.0 Q3'19

- Multi-tenancy
- Assurance update

Control Plane
Dynamic Diagnostics

- XL710 40G-Breakout

- Image management
- VNF image update

- Increased Ecosystem

Core capabilities

Hardware Platform

UI/UX
(Different AC/release)

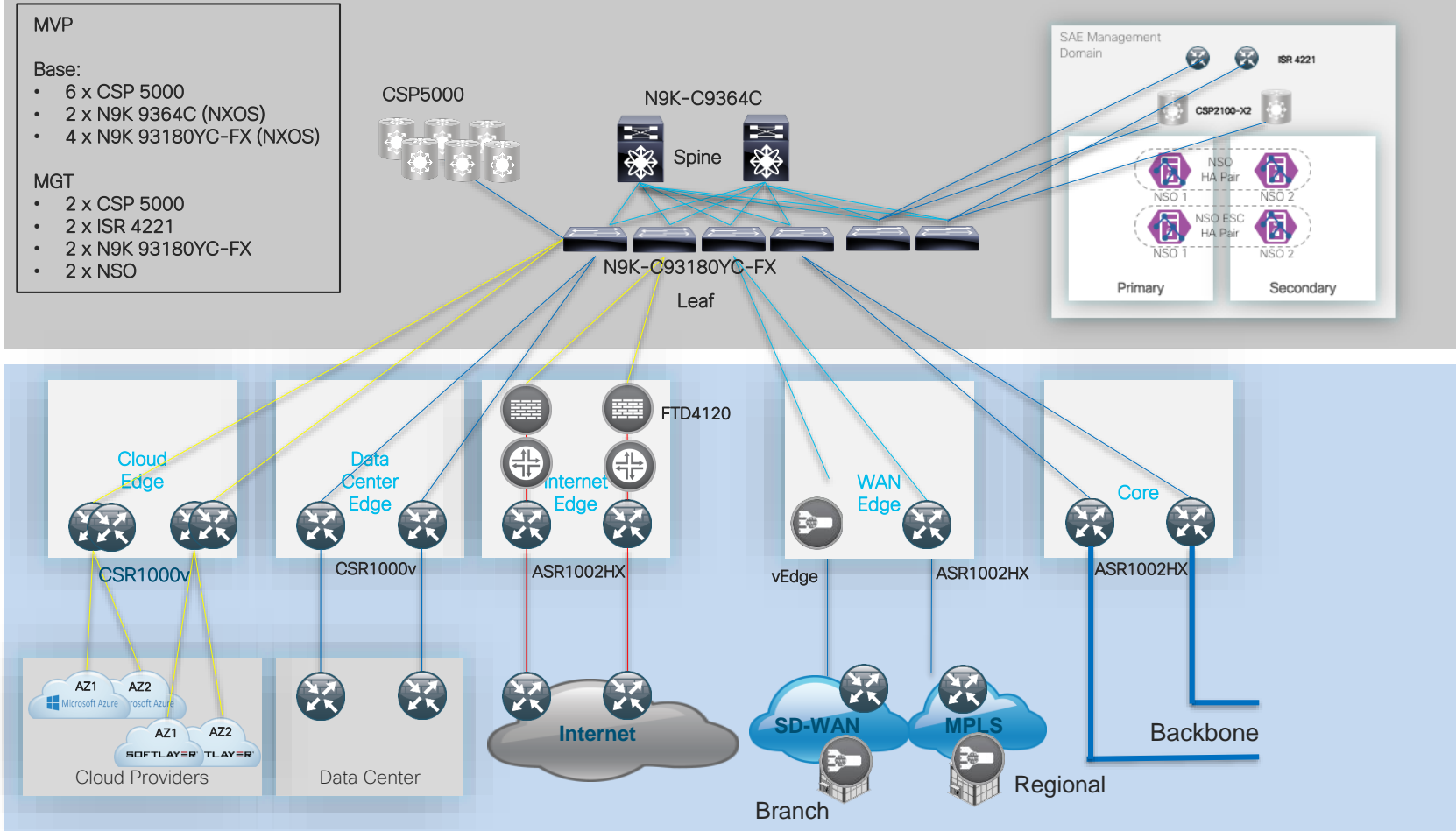
Focus

CISCO *Live!*

SAE Release and Roadmap

	SAE 2.0.1 Q4'19 (Jan CY20 release)	SAE 2.0.2 Q1'20 (Mar 20)	SAE 2.1 Q2'20 (June 2020)	SAE 2.2 Q3'20 (Sept 2020)
Core capabilities	<ul style="list-style-type: none"> Bug Fixes <ul style="list-style-type: none"> Customer UX risk with VNF licensing Spine-Leaf config fix Checkpoint onboarding 	<ul style="list-style-type: none"> QCOW2 packaging vNIC bandwidth control PNF anywhere 	<ul style="list-style-type: none"> VNF with Day2 recovery Control plane Network Assurance ACI Integration 	<ul style="list-style-type: none"> SAE as a Service (CX EX commit dependency)
Hardware Platform	<ul style="list-style-type: none"> CSP 2.6: <ul style="list-style-type: none"> LLDP enhancement 	<ul style="list-style-type: none"> TPM support on CSP in 2.6 	<ul style="list-style-type: none"> CSP 2.7 Storage Virtualization/NFS 100G <ul style="list-style-type: none"> Mellanox (pure bandwidth) 	<ul style="list-style-type: none"> CSP 2.8 Intel SmartNIC(N3000 FPGA) <ul style="list-style-type: none"> IPSEC & TLS acceleration possible through N3000
UI/UX (Different AC/release)	<ul style="list-style-type: none"> Operational updates UI parity with CLI for notifications 	<ul style="list-style-type: none"> Health & status enhancements 	<ul style="list-style-type: none"> SAE Wizard ACI support(VXLAN details) 	<ul style="list-style-type: none"> SaaS portal enhancements
Focus	<ul style="list-style-type: none"> Maintenance release 	<ul style="list-style-type: none"> Customer wins 	<ul style="list-style-type: none"> Pre SAE as a Service 	<ul style="list-style-type: none"> Launch SAE as a Service

Secure Agile Exchange Build Out



Secure Cloud Edge

- **Intent-based policies** across different **functions** and **locations** managed centrally

Infrastructure Providers & Authorities

Services

OEM Services

Policy Mgmt

Security & Visibility

Apps & Services

Data & Analytics

Internet & 3rd Party Apps

- SD-WAN overlay provides **secure connectivity, visibility** and **segmentation** throughout
- Secure Cloud Edge enables **distributed deployment** of applications & services
- Distributed **data and analytics** supported as well

Secure Cloud Edge

Apps & Services

Security & Visibility

Data & Analytics

Comp

Net

Secure Cloud Edge

Managed Connectivity & Distributed Compute

Unmanaged Connectivity (Internet)

SD-WAN

Data & Analytics

Apps & Services

Security & Visibility

Comp

Net

Secure Cloud Edge

- **Secure agent** in the vehicle provides secure 'on-ramp'
- Agent provides **application-aware telemetry** reporting, traffic segmentation and **policy enforcement**
- Flexible **Endpoint** management in the hands of the OEM
- SD-WAN provides **secure** data path from vehicle to high-value applications

Vehicle

App & Service Policies

Compute & Storage Policies

Applications & Services

Virtualization, Containers, etc.

Compute Platform(s)

In-Vehicle Network

Policies

Security

Policies

Connectivity

Policies

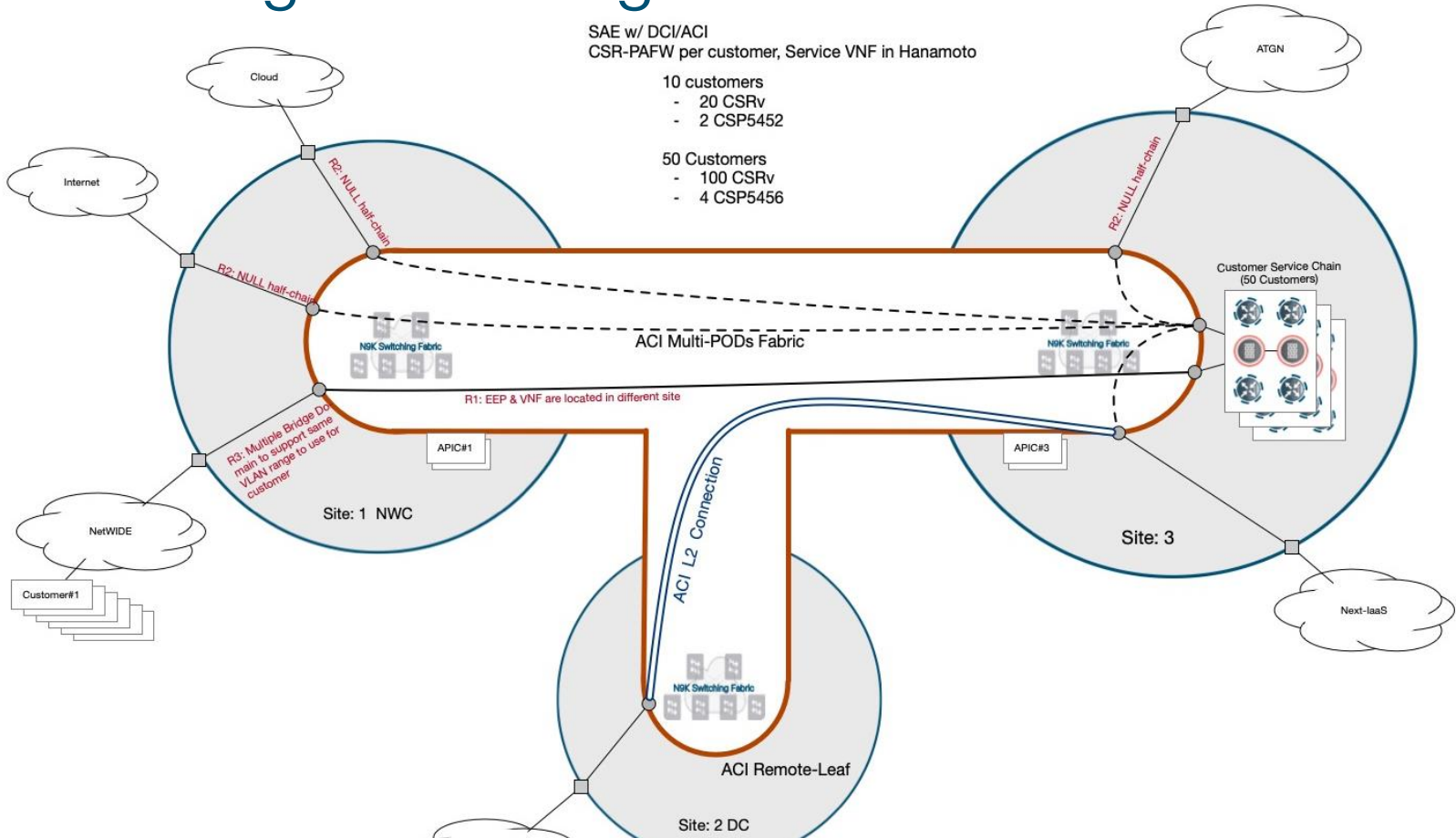
Telemetry/Data

Legacy ECUs

Legacy Network (CAN, etc.)

Mobile SD-WAN Control Point

Secure Agile Exchange ACI Fabric



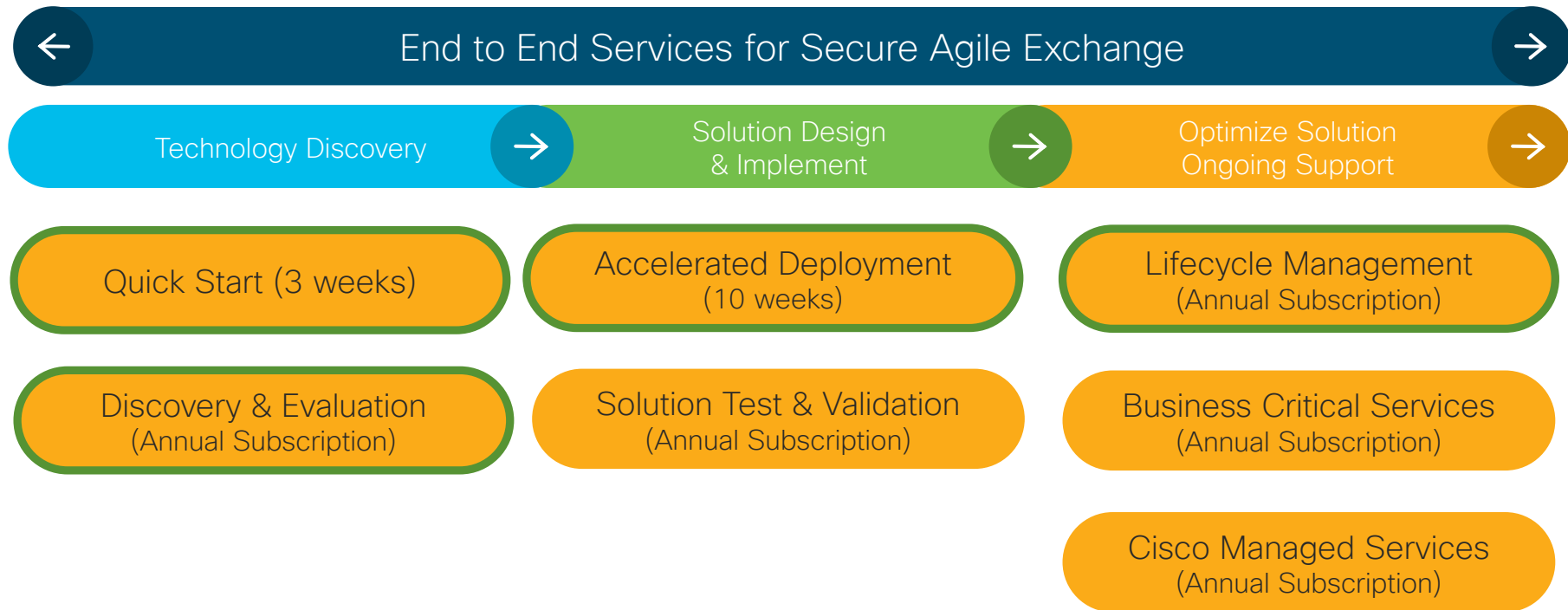
SAE w/ DCI/ACI
 CSR-PAFW per customer, Service VNF in Hanamoto

- 10 customers
 - 20 CSRv
 - 2 CSP5452

- 50 Customers
 - 100 CSRv
 - 4 CSP5456

R1: EEP & VNF are located in different site

Services for Secure Agile Exchange Portfolio



Resources

SAE Solution Overview - click [here](#)

SAE Solution Guide - click [here](#)

Dinesh Ranjit - Solution Architect
dranjit@cisco.com

Sujay Murthy - Lead Engineer
sujmurth@cisco.com

Ask SAE :
ask-sae-external@cisco.com

Secure Agile Exchange Key Takeaways !!!

- Secure Agile Exchange enables multi-cloud journey for customers
- Capitalize on the transformation in consumption model
- Considerable WAN cost savings
- Cloud service provider and WAN technology agnostic
- Turn-key with user friendly Graphical User Interface
- Programmable, customizable and extensible to fit into existing OSS/BSS stack

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



Engage with us NOW so you can put to
action what you learnt today

Enabling Secure access to multiple clouds
is absolutely EASY!



Thank you





You make **possible**