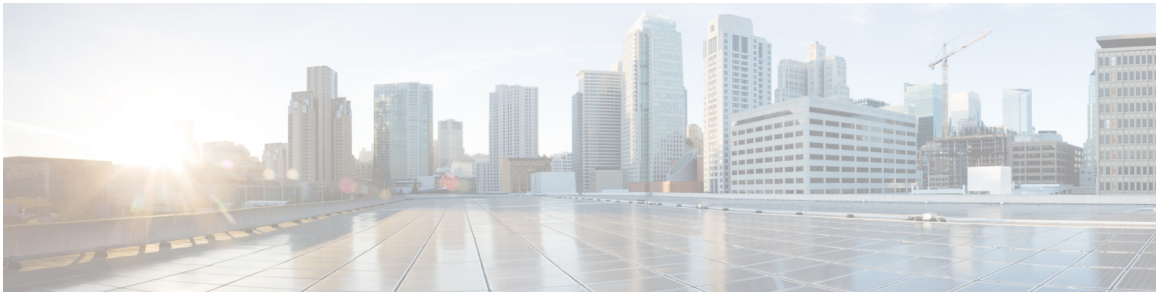
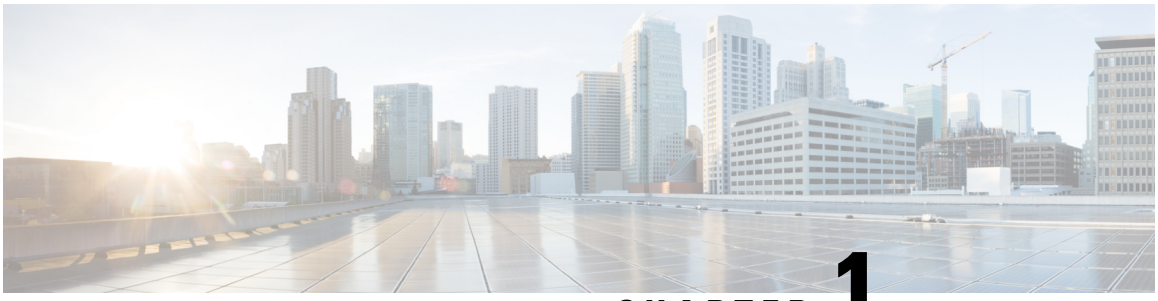
Cisco Secure Agile Exchange (SAE) Solution Guide

Last Modified: 2018-09-25

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS



CHAPTER 1

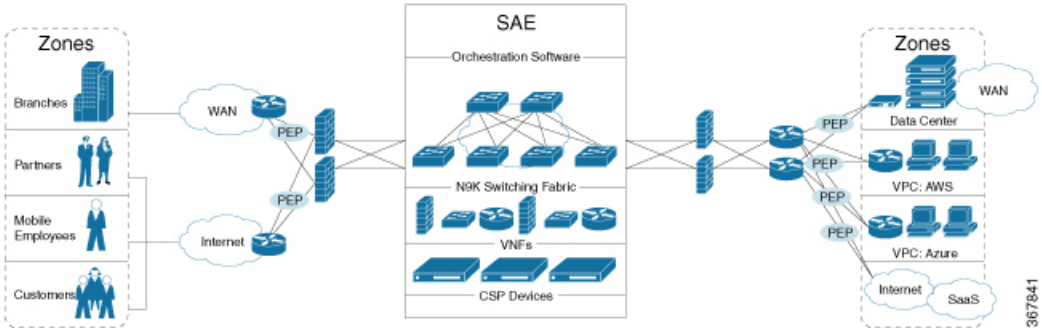
Solution Overview of Cisco Secure Agile Exchange

Cisco® Secure Agile Exchange (SAE) is a solution that enables enterprises to interconnect users to applications quickly and securely by virtualizing the network edge (DMZ) and extending it to colocation centers, the crossroads of Internet traffic.

About Cisco Secure Agile Exchange (SAE)

Cisco® Secure Agile Exchange (SAE) provides orchestration and automation of Cisco products like CSR and ASAv, along with third-party VNFs using Cisco Cloud Services Platform (CSP). CSP is an open Cisco Network Function Virtualization (NFV) appliance.

The flexible architecture of this solution connects distributed consumers with distributed data and applications that potentially reside in many clouds and private data centers.



This single-vendor, turnkey solution reduces the operational complexity of deploying different services from multiple vendors.

Problem Statement

The interconnections between users and applications are evolving to complex digital business architectures due to emergence of multi-cloud IaaS and SaaS vendors. This requires the network to be both fast and flexible to meet the expanding changes and demand.

Current Landscape

Distribution of Applications from Data Centers to IaaS and SaaS

Applications reside in multiple locations, including the private data center; in the cloud in the form of infrastructure as a service (IaaS) with providers like AWS, Azure, and Google Cloud Platform; or as software as a service (SaaS) with providers such as ServiceNow and Salesforce, Box, Office 365, to name a few. Regardless of an organization's cloud strategy, most will have applications across all locations.

Digitization is placing unprecedented demands on IT to increase the speed of services and products delivered to customers, partners, and employees, all while maintaining a high level of security. With the adoption of multi-cloud infrastructure, the need to connect multiple user groups in an agile and secure manner places additional demands on the IT teams.

Challenges

- It is becoming increasingly difficult to apply security policies uniformly across multi-cloud applications.
- Some IaaS and SaaS vendors may not provide the required security options.
- The IaaS and SaaS providers that do the security options you need may not necessarily do so in a way that is consistent with your enterprise policy.
- There is inconsistency in application of policies across products and applications.

Business Impact

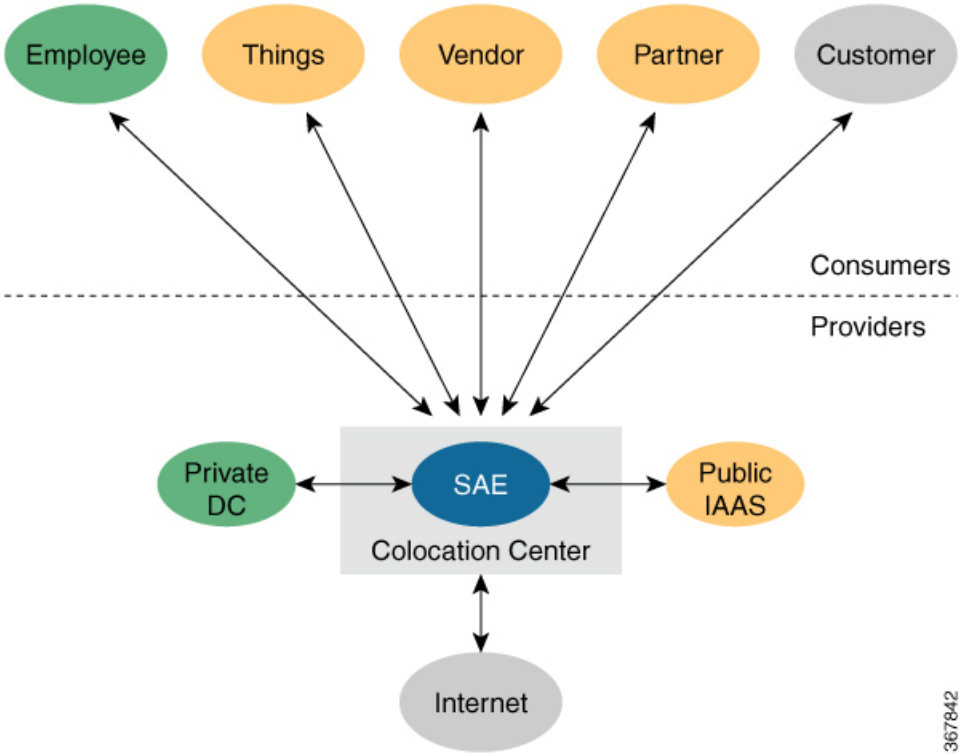
The business impact of the rising complexity resulting from multi-cloud adoption and the increasing demand for flexibility and security can be categorized as follows.

- **Latency and Increased Costs:** As enterprises embrace cloud, they are required to backhaul traffic to their data centers to apply security policies and to gain visibility in the incoming and outgoing IaaS and SaaS traffic. This hairpinning of traffic causes latency and increases costs.
- **Inefficiency:** A majority of changes that are being implemented in response to the changing IT landscape are still being implemented manually. This lack of network agility and automation has led to inefficiency in service enablement.
- **Under-utilization** The existing infrastructure is designed for maximum capacity, but has low utilization.
- **Security:** The attack surfaces are expanding due to increasing numbers of security vendors and connectivity to cloud-hosted services. This has led to an increased time in detecting and remediating network attacks.

How SAE can Help Overcome the Challenges

As enterprises adopt a multi-cloud strategy, they must look at optimizing traffic patterns for experience, securing interactions, reducing circuit costs, and providing flexibility.

The success of multi-cloud solutions depends on a new cloud-edge capability, where all consumer networks terminate in a carrier-neutral facility and security policies can be enforced centrally.



This is where SAE comes in. SAE offers the capability of virtualizing your network edge and extending it to colocation centers. SAE provides segmentation, virtualization, automation, and orchestration for your enterprise within a carrier-neutral facility.

Virtualization, automation, and orchestration are foundational to SAE. Virtualization negates the need to design infrastructure for future requirements of scale by providing an agile way of scaling up and down as required.

Note It is possible to place SAE in your private data center; however, we recommend deploying SAE in a carrier-neutral facility to truly benefit from the agility it offers. Deploying SAE in a carrier-neutral or colocation facility offers the following benefits.

- Proximity to clouds, which helps maintain app SLAs
- Security and telemetry across multiple clouds
- Single location to view and audit traffic and user-app relationships

Benefits of SAE

Security: Centralized policy enforcement offers simple and secure access, deployment, and control.

Scale-out Architecture: The flexible architecture of SAE allows you to scale out the VNFs and compute as required. Cloud Servces Platform (CSP), the x86 compute platform negates the need to order, cable, rack, and stack dedicated appliances when capacity needs to increase or changes need to be made.

Performance Agility: The ability to spin up networks and VNFs on demand offer improved performance agility. You can optimize application performance by strategically placing SAE in colocation centers that are closest to your Saas and IaaS cloud providers.

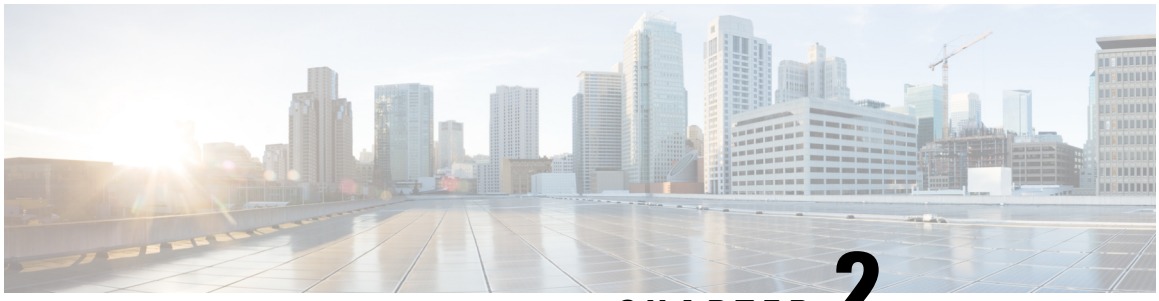
Flexibility: The solution supports both–Cisco VNFs and third-party VNFs that Cisco supports.

Cost Savings: By having a central location to connect to various clouds (including private clouds), enterprises can optimize the costs of circuits to connect their users to applications. Circuit costs for a colocation facility are significantly lower than in a private data center.

Components of SAE

The SAE solution consists of the following components and services, which integrate to address the challenges described in the previous sections of this guide.

- **Orchestration:** SAE core function pack provides network services orchestration. SAE core function pack enables VNF workflow management, fabric configuration, routing of layer 2 and 3 networks and inter-virtual devices. The core function pack also provides intelligent VNF placement logic that is based on the availability of compute resources and high availability (HA) requirements.
- **CSP NFV Appliance:** CSP, a x86 Kernel-based KVM platform is used to host VNFs. CSP supports high-throughput internal switching technologies such as Single Root I/O virtualization (SR-IOV) and 10 GBPs physical network cards (pNICs). It also uses a central network file system (NFS) to host the images of shared VNFs and configuration templates.
- **Nexus 9000 Switching Fabric:** The SAE switching fabric is built in a carrier-neutral facility and uses high-performance Cisco 9000 series switches. SAE switching can be built in either standalone topology or spine-leaf topology. The Nexus 9000 fabric supports the following:
  - Full redundancy with port channels and virtual port channel (vPC)
  - Multi tenancy with VRFs
  - VLAN and VXLAN
- **Virtual Network Functions (VNFs):** The solution has been tested with both, Cisco VNFs and third-party VNFs that are supported by Cisco.



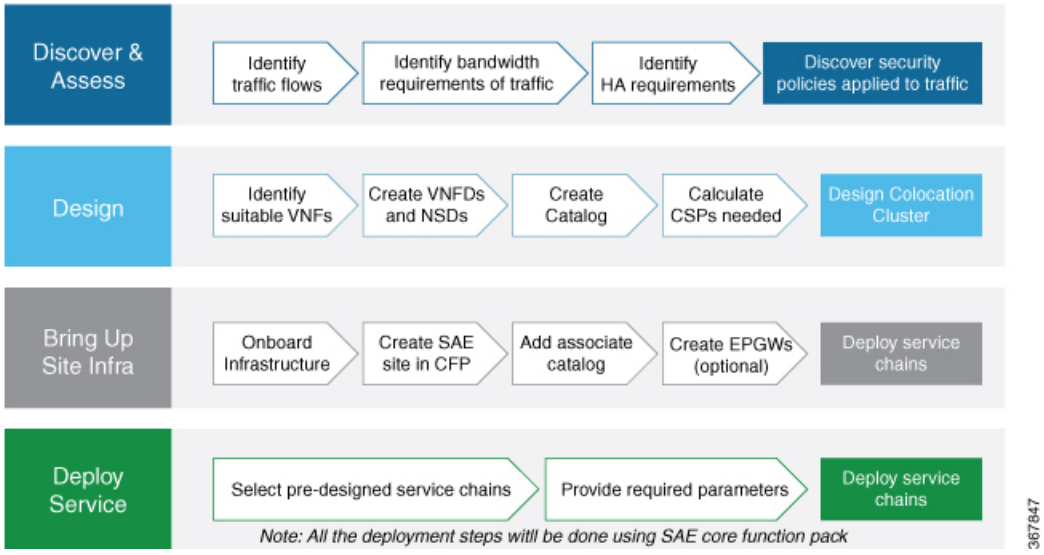
CHAPTER 2

About This Document

Document Flow

The document is structured according to the stages an enterprise would go through when they decide to deploy SAE. Typically, enterprises would go through the following milestones in their SAE journey.

- Assess and analyze existing infrastructure and traffic flows
- Design services based on existing patterns so that they can be instantiated as required
- Deploy hardware and compute requirements based on your service requirements and design
- Deploy service chains



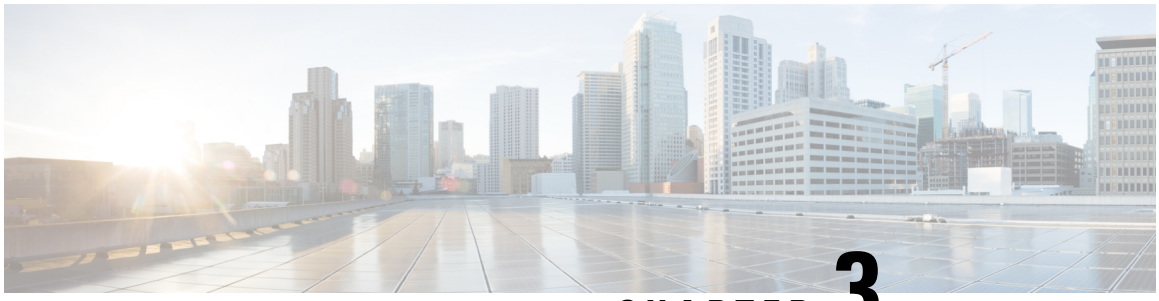
Target Audience

This guide is intended to assist enterprises that have some presence in colocation or carrier-neutral facilities and are looking at migrating to virtualized DMZs in such colocation centers. Essentially, such enterprises have data and applications spread over private data centers and clouds; and have traffic coming in from a wide range of trusted, semi-trusted and untrusted connections such as employees, partners, customers etc.

The target audience of this guide includes:

- IT decision makers in multinational corporations that have a global presence
- IT decision makers in enterprises with presence in carrier-neutral, colocation centers
- Network architects, security professionals, application architects
- CIOs

Note This guide assumes that readers have a broad understanding of networking terminologies and principles. It also assumes prior exposure to current trends in multi-cloud offerings.



CHAPTER 3

Assess Infrastructure and Challenges

Identifying repeatable connections patterns is foundational for orchestration–one of the key services that SAE provides. An enterprise would typically begin their SAE journey by assessing their existing traffic patterns. This acts as the basis of your service design.

Assess Infrastructure and Challenges

This document explains the various stages of SAE journey taking the example of an enterprise, Acme Corp.

About Acme Corp

Acme Corp is a multinational, financial enterprise with global presence. It currently has to bear the expenses of maintaining several global data centers as well as operational expenses of hosting some of its newer applications in cloud environments.

Where Acme is Today

Application Infrastructure

- Acme currently maintains multiple global data centers where most of its applications are hosted.
- Some of the newer applications are also hosted in Azure and AWS clouds.
- Currently, its infrastructure is designed for maximum capacity, which lacks optimum utilization.

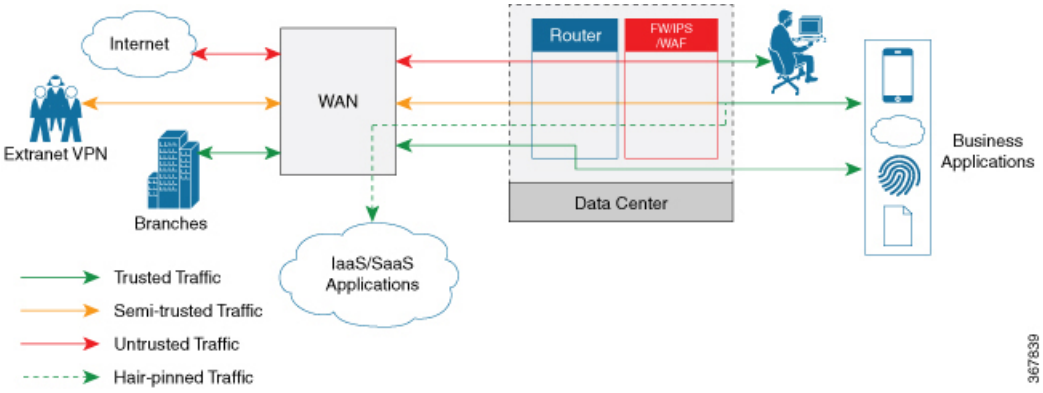
Application Consumers

Acme's application consumers are accessing the applications through MPLS and SD-WAN. Such application consumers can be categorized as follows:

- Regional branches and extranet partners connecting over MPLS
- Remote employees connecting through remote VPN
- Partners connecting remotely through IPSec extranet as well as through the internet

Application Providers

Acme's application providers can be categorized as follows: existing private data centers, emerging cloud providers like Azure, and other SaaS providers on the internet.



Challenges

Acme currently faces the following challenegs.

- The cost of maintaining private data centers is very high.
- The dedicated physical infrastructure and conventional methods of configuring operating systems and applications limit the speed of data centers to respond to new customers and services.
- Currently, all traffic terminates into the data center before it can be rerouted appropriately. The security policies are applied in the data center and the traffic is hairpinned back through WAN to reach applications in SaaS and IaaS. This rerouting causes latency.
- There is no visibility into end-to-end traffic flow, which leads to complexity in troubleshooting and workload analysis.
- The infrastructure relies on manual configuration and maintenance, which is error-prone.
- Any new connections and traffic flows require additional hardware such as routers and firewalls. This is not cost-effective at scale. It also limits the speed of responding to new customers and services.

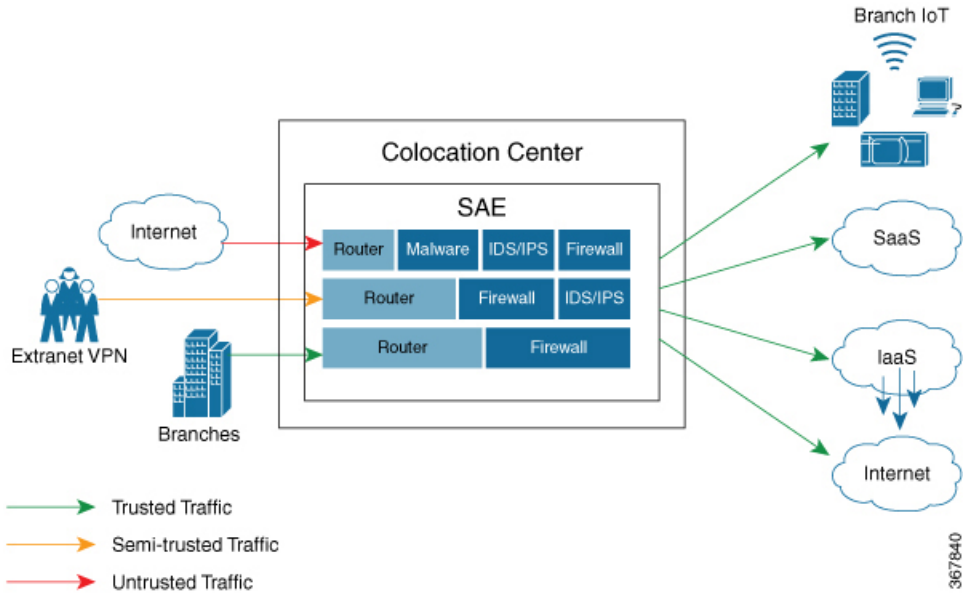
Identify Connectivity Goals

After analyzing its existing traffic flow and the challenges associated with it, Acme Corp has identified the following goals to overcome its connectivity challenges.

- Migrate to the new, next-generation, virtualized DMZ
- Have a single physical network that provides the required logical connectivity to interconnect its different user groups to its applications
- Scale out its network services as needed without having to invest in additional physical infrastructure
- Apply policies uniformly and securely across different traffic flows
- Have visibility into its traffic and network performance

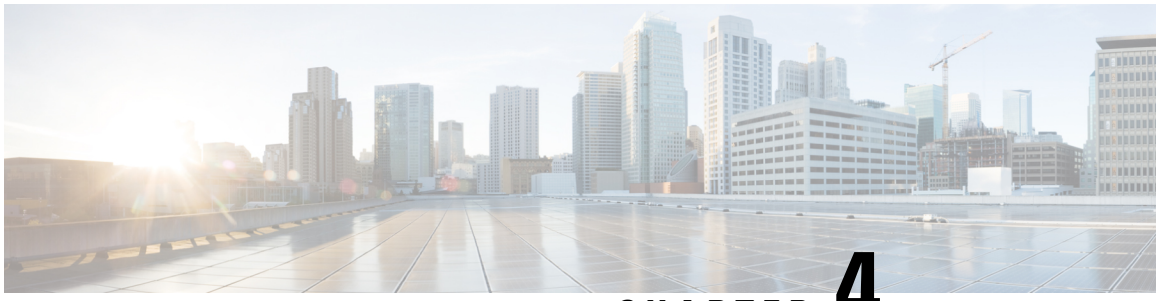
How SAE can Help

SAE can enable Acme to meet their target by offering virtualization at scale, orchestration, and automation. The following image shows how Acme's traffic would look after adopting SAE.



Once Acme deploys SAE, here is how its traffic flow would flow.

- The traffic originating from various sources would terminate into SAE, which is hosted in a carrier-neutral facility or colocation facility.
- The security policies would then be applied depending on the trust-level of the traffic source centrally within SAE.
- The traffic will then move forward, through service chains formed by connecting VNFs, to its destination such as data centers, SaaS, IaaS, as the case maybe.



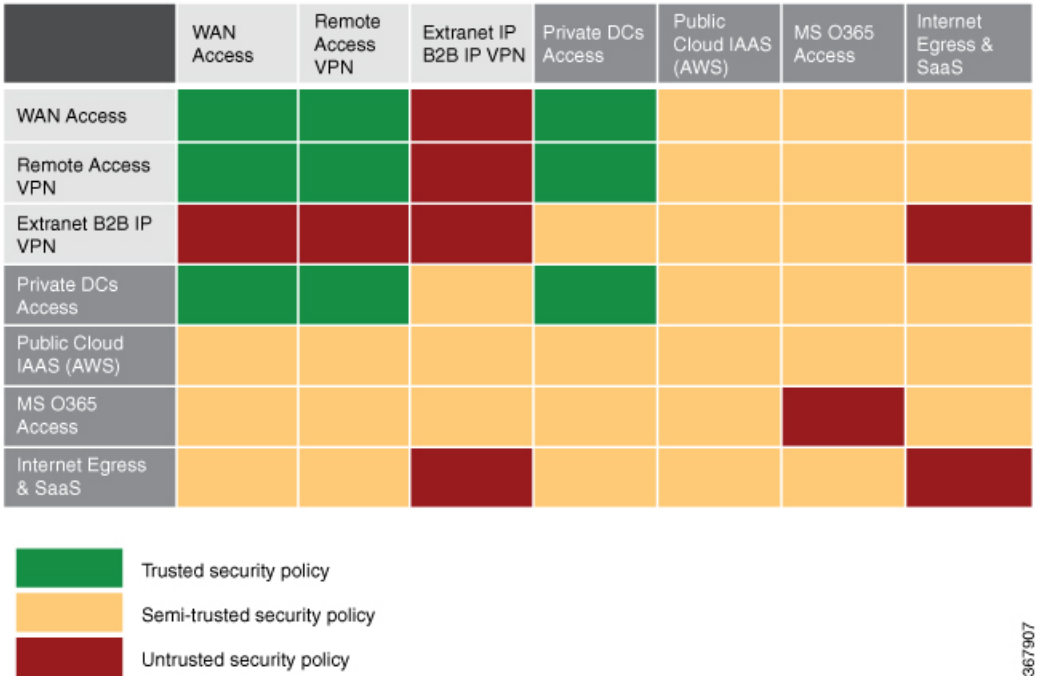
CHAPTER 4

Service Design

An enterprise would typically go through the following stages while designing their service for SAE.

Identify VNFs

The following connection patterns emerge from the analysis of Acme Corp's consumers and providers.



The table above shows which groups cannot interact with each other (red), which groups can interact, but with certain controls (orange), and which groups can interact without additional security services (green).

Partners accessing application through MPLS, WAN, Internet, and employees represent the consumers.

How to Identify VNFs for your Design

The type of VNFs you need depends on your traffic patterns and volume. For example, if you are creating a consumer chain for traffic coming from your employees, you require fewer firewalls as the source of such traffic is considered to be trusted.

SAE supports both–Cisco VNFs and third-party VNFs supported by Cisco. Based on your traffic patterns and volume, select the VNF that suits you best. The following are some possible options.

- Routing: CSR
- Firewall: FTDv, ASAv, Palo Alto Firewall
- Load Balancing: AVI, F5

VNF features and licensing costs are the additional criteria that you must consider while selecting the VNFs for your service chains.

See Cisco CSP 5000 Series Datasheet for a complete list of supported VNFs.

Design Service Chains

Consumers and providers interact with each other through a set of service chains. Service chains are built by connecting VNFs together.

About Service Chains

Service chains are designed to meet the traffic flow discovered in the audit phase. The service design is based on your connection patterns and security policies. Security policies depend on the trust level of the connections. Therefore, the design of your service chains also depends on the following.

- Trust level of your connections
- The security policies you wish to apply to your connections
- The bandwidth associated with your traffic flows

You must consider the following factors while designing your service chains.

- SR-IOV versus DPDK: Your service chain design depends on the VNFs that you have identified and their support in each of these modes.
- High Availability (HA)
- Port channel
- Licensing

Design SAE Site

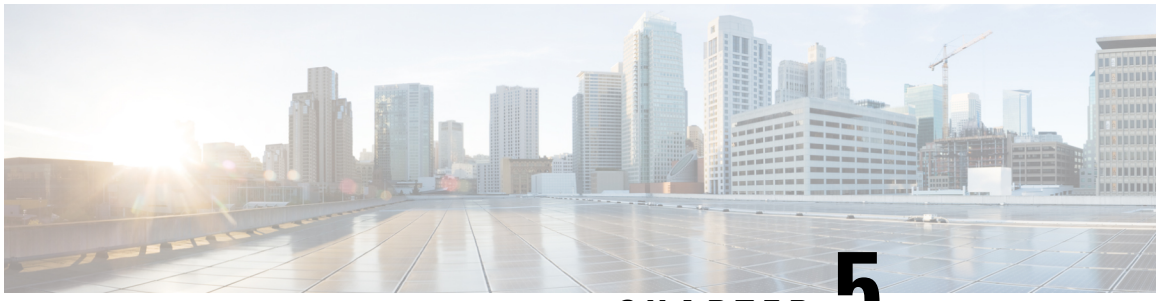
The number of CSP devices required for your SAE site depends on the following:

- Number of service chains required for your enterprise traffic
- VNFs in each service chain and their bandwidth requirements

- Throughput per service chain
- Cores per site and NIC types

Switching Requirements

- The switches must be in VEPA mode to enable visibility into the traffic.
- Whether the switching fabric is in standalone mode or spine-leaf mode depends on the number of port requirements that your design requires.



CHAPTER 5

Deploy Hardware

Wiring

For Acme Corp, it's proposed that SAE designates two interconnected domains: services and shared-services. The services domain would contain the VNFs and networking of service chains. The services domain is dynamic and capable of scaling out as required.

The shared services domain contains all the services that SAE consumes–NSO, ESC, Firepower Configuration Center (FMC-2500) etc. The shared services domain mainly static and can host SAE-independent platforms.

Hardware Components

Table 1: Hardware Specifications

Device	Note
2 x (n) CSP Devices	• For SAE to work, you need a minimum of two CSP devices for redundancy. • However, you can scale the devices (in pairs) as required.
2 x (n) N9K 93180YC-FX leaves	• For every two spines in your design, you would require four leaf switches for redundancy. • You can always scale the leaf switches as required in multiples of four.

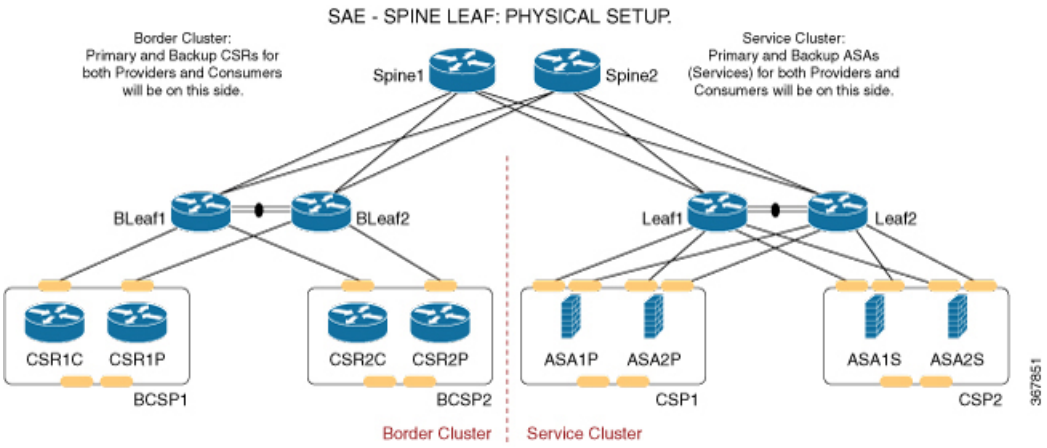
CSP devices support SR-IOV high throughput virtual switching. CSP provides REST APIs and a ConfD interface for managing and creating VNFs and NSO modelled service chains and zones.

Nexus 9000 switches provide the networking fabric for interconnecting VNFs and the physical devices. N9K-C93180YC-FX pairs support Virtual Port Channel (vPC). A vPC can provide Layer 2 multipathing,

which allows you to create redundancy by increasing bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

Note This section details the wiring topology that Cisco recommends.

Recommended Wiring Topology



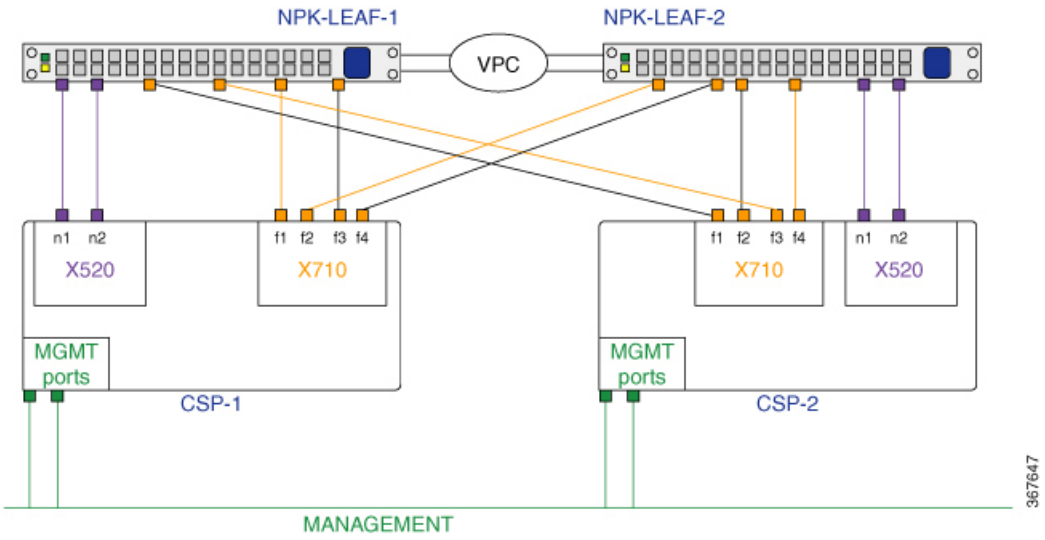
Switching Basics

- Each leaf must be connected to each spine.
- No spines must be connected to each other.
- No leaves must be connected to each other, except for the vPC pairs.

Note If you don’t order spines, only the leaves would be connected through vPC pairing.

CSP Devices

Connect the CSP devices as per the topology specified below.



- Connect each CSP device to both the Nexus 9000 switches using two 10G ports in port-channel configuration. Each CSP device has four XL710 interfaces, which enable port channeling. Two of these ports must be connected to leaf 1 and two to leaf 2.

  The figure above shows the formation of two separate port channels. However, you can also form a single aggregate port channel using all four ports on the CSP device.

- Connect the two X520 interfaces to the switches in a non port-channel configuration.
- Connect all CSP devices to a separate management L3 network.

This same wiring must be repeated for any new CSP pairs you add to your SAE cluster.

Configure Hardware

Enter the consoles of each of the devices that is part of your SAE site, and complete the day-1 configuration.

Configure CSP Devices

See the following guides for more information on configuring the management IPs, OVS port-channels, and SR-IOV on your CSP devices.

- Cisco Cloud Services Platform Configuration Guide
- Cisco Cloud Services Platform Quick Start Guide

Configure Nexus 9000 Switches

See the following configuration guide for more information on configuring the management IP addresses, port-channels, vPC, VEPA, and EVPN.

- Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.x

Install and Configure Software

Install NSO and SAE Core Function Pack

SAE supports NSO version 4.7.1.

Note If you already have NSO installed, uninstall it and do a fresh installation of NSO 4.7.1.

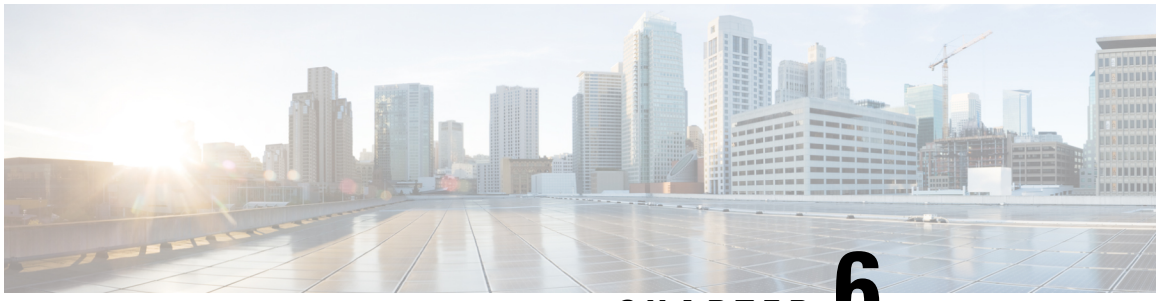
Supported Operating Systems for NSO

- Ubuntu
  - v17.10 – Artful
  - v16.04.4 LTS – Xenial
  - v18.04 LTS – Bionic
  - v14.04.5 LTS – Trusty
- CentOS v7.4

Note To install SAE core function pack. see SAE Core Function Pack Installation Guide.

Install and Configure ESC

SAE supports ESC 4.3.0.121 + patch. To install ESC, see Cisco Elastic Services Controller 4.3 Install and Upgrade Guide.

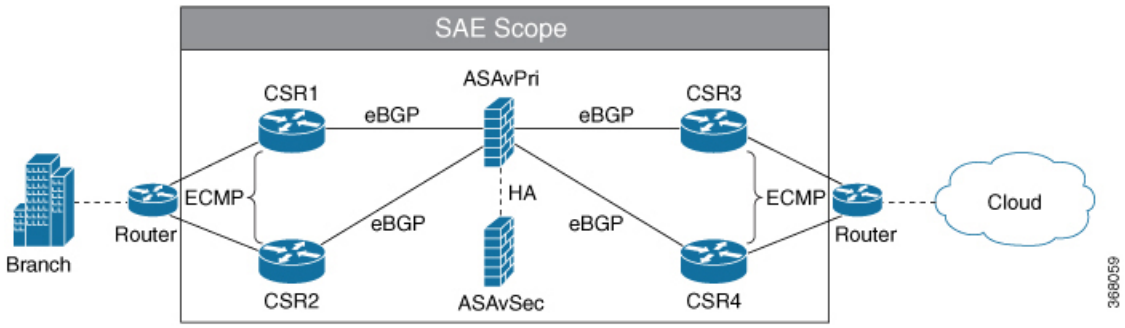


CHAPTER 6

Deploy SAE

The steps to deploy SAE using the SAE core function pack are shown using a service chain example. The overall deployment procedure remains the same for different service chains with varying VNFs.

Service Chain Example: This chapter describes how to deploy a full service chain that uses CSRs as both–the consumer and the provider side endpoint gateways; and connects them through two ASAv VNFs: one as active and the other as a stand-by VNF. A single network service descriptor (NSD) is created for the entire service chain and consists of four CSRv VNFs and and two ASAv VNFs.



The procedure assumes that Nexus 9000 leaf switches are connected as a VPC switch pair.

The VNFs in the example are SR-IOV VNFs, which means that they are connected to SR-IOV interfaces on the CSP devices.

The following topics show a complete example of deploying SAE for the service chain described above.

Verify Prerequisites

Ensure that the following prerequisites are met before proceeding to the next step.

- All switches are booted, and the users are configured with the required privileges.
- All CSP devices are booted.
- CSP devices and Nexus 9000 switches are wired according to the prescribed physical topology.

- The switches and CSP are configured to enable link discovery using LLDP.
- The switches are configured as a Virtual Port Channel (VPC) pair.
- Management ports of all CSPs are connected to redundant L3 networks and the correct IP addresses are assigned.
- Ensure that you have the pNIC information for your CSP devices. For more information, click here.
- The status of LLDP neigbors and VPC configuration on your Nexus 9000 switches have been verified. For more information, click here.
- The VNF images used in the example are uploaded to the CSP repository.
- The required routing configuration is done to enable management connectivity between the NSO server and all the devices.
- NTP server is ready for use and configured on devices used in the topology being used.
- All platform versions and requirements are verified.
- NSO has been installed. See Cisco Network Services Orchestrator (NSO) Solutions for more information.
- ESC has been installed. See Cisco Elastic Services Controller 4.3 User Guide for more details.
- SAE core function pack has been installed. See Cisco SAE Core Function Pack Installation Guide for details.

Create SAE Site

Step 1: Create authgroups for switches and CSP devices

The following example shows how to create authgroups for your CSP devices and switches. Replace the variables values such as passwords and IP addresses with values specific to your environment.

1. Create a file called AUTHGROUP.cli with the following content.

```
devices {
  authgroups {
        group SWITCH_AUTHGROUP {
                default-map {
                        remote-name     admin;
                        remote-password password123;
                }
        }
        group CSP_AUTHGROUP {
                default-map {
                        remote-name               admin;
                        remote-password           password123;
                        remote-secondary-password password567;
                }
        }
    }
}
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
```

```
load merge AUTHGROUP.cli
commit
```

Step 2: Create resource pools

In this step, you will create the following respurce pools.

- **IP address pool:** SAE core function pack assigns IP addresses to virtual links between VNFs from this pool.
- **VLAN Pool:** The VLAN range that is allocated for service chains.
- **Management IP Pool:**The subnet or range of IP addresses.

The following example shows how to create resource pools. Ensure that you replace the values for IP_DATA_POOL, IP_MGMT_POOL with values specific to your environment.

1. Create a file called RESOURCE_POOL.cli with the following content.

```
resource-pools {
        id-pool VLAN_POOL {
                range {
                        start 101;
                        end   1000;
                }
        }
        id-pool default-as-pool {
                range {
                        start 4200000000;
                        end   4294967294;
                }
        }
        ip-address-pool IP_DATA_POOL {
                subnet X.X.X.X;
        }
        ip-address-pool IP_MGMT_POOL {
                subnet X.X.X.X;
        }
}
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge RESOURCE_POOL.cli
commit
```

Step 3: Create SAE catalog

The following example shows how to create your SAE catalog. Replace the name for CSP type with the corresponding name in your environment.

1. Create a file called CATALOG.cli with the following content.

```
sae-catalog SAE_CATALOG {
   csp CSP2100_SH {
   }
}
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge CATALOG.cli
commit
```

Step 4: Create SAE provider

The following example shows how to create an SAE provider and tenant for your site. You can replace the provider and tenant names with suitable names for your environment.

1. Create a file called PROVIDER.cli with the following content.

```
sae-provider SAE_PROVIDER {
    sae-provider-catalog SAE_CATALOG;
    sae-tenant SAE_TENANT;
}
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge PROVIDER.cli
commit
```

Step 5: Create SAE site

The following example shows how to create an SAE site and tenant for your site. Replace all variable values like site name, server name, etc. with values specific to your environment.

1. Create a file called SITE.cli with the following content.

```
sae-site SANJOSE  {
    sae-provider SAE_PROVIDER;
    sae-tenant   SAE_TENANT;
        vnf-mgmt-resources {
            vnf-mgmt-netmask X.X.X.X;
            vnf-mgmt-vlan    X;
            vnf-mgmt-gateway X.X.X.X;
        }
    var NTP_SERVER {
        val ntp.esl.cisco.com;
    }
    var DOMAIN_NAME {
        val cisco.com;
    }
    var NAME_SERVER1 {
        val X.X.X.X;
    }
    var NAME_SERVER2 {
        val X.X.X.X;
    }
    var PROXY_SERVER {
        val X.X.X.X;
    }
    var PORT {
        val 80;
    }
    var LICENSE_TOKEN {
        val FIX_ME;
    }
    resource-pools {
```

```
            as-pool          default-as-pool;
            mgmt-ip-pool     IP_MGMT_POOL;
            internal-ip-pool IP_DATA_POOL;
        }
        infrastructure {
            switching {
                type    n9k-switch-pair;
                bgp-asn 100;
            }
            compute-clusters Cluster1 {
                vlan-pool VLAN_POOL;
            }
        }
    }
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge SITE.cli
commit
```

Step 6: Create Inventory Discovery File

Create a file called discovery.cfg in your home directory with the following content.

```
{
    "site"              :       "SANJOSE",
    "cluster"           :       "CLUSTER1",
    "cspType"           :       "CSP2100_SH",
    "switch_seed_address":       "X.X.X.X",
    "rest_username"     :       "admin",
    "rest_password"     :       "Cisco123#",
    "csp_authgroup"     :       "CSP_AUTHGROUP",
    "n9k_authgroup"     :       "SWITCH_AUTHGROUP"
}
```

Ensure that your inventory discovery file includes the following information specific to your environment.

- `cspType` is the category defined in the Create Catalog step above.
- `csp_authgroup` and `n9k_authgroup` represent the authgroups you created in Step 1 of Create Site.
- `rest_username` and `rest_password` represent the rest API credentials of Nexus 9000 switches.

Step 7: Run the inventory discovery file to populate site infrastructure

The following example shows how to populate your site infrastructure by running the inventory discovery file you created in the previous step.

```
ncs_cli -u admin
admin@ncs>request discovery_action discover configFile /home/sae/discovery.cfg
```

Step 8: Add authgroups for VNFs used in your service chain

The following example shows how to create authgroups for the VNFs being used in the example service chain—CSR and ASA.

1. Create a file called VNF_AUTHGROUPS.cli with the following content.

```
devices authgroups {
    group CSR_AUTHGROUP {
```

```
            default-map {
               remote-name               admin;
               remote-password           password111;
               remote-secondary-password password222;
               }
            }
        group asa_authgroup {
        default-map {
                remote-name               admin;
                remote-password           password333;
                remote-secondary-password password444;
                }
        }
        group ESC_AUTHGROUP {
        default-map {
                    remote-name     admin;
                    remote-password password555;
                    }
            }
    }
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge VNF_AUTHGROUPS.cli
commit
```

Step 9: Bring up ESC and Create VNF Site Manager

Create only one VNF manager per SAE site.

```
ncs_cli -u admin
configure

---Bring up ESC---

set devices device ESC-0 authgroup ESC_AUTHGROUP address X.X.X.X port 830 state admin-state
 unlocked
set devices device ESC-0 device-type netconf ned-id netconf
set devices device ESC-0 trace pretty
commit

---Fetch SSH key and sync from ESC---

request devices fetch-ssh-host-keys
commit

---Sync from ESC0---

request devices sync-from device
commit

devices global-settings connect-timeout 3600 read-timeout 3600 write-timeout 3600
devices global-settings trace raw
commit
```

Step 10: Verify the list of devices onboarded on NSO device tree

```
show devices list

NAME     ADDRESS    DESCRIPTION  NED ID     ADMIN STATE
-------------------------------------------------------
```

```
CSP-1    X.X.X.X   -           netconf    unlocked
CSP-2    X.X.X.X   -           netconf    unlocked
ESC-0    X.X.X.x   -           netconf    unlocked
N9K-1    X.X.X.X   -           cisco-nx   unlocked
N9K-2    X.X.X.X   -           cisco-nx   unlocked
```

Design Your Services

Note All the configuration examples are representative only. The variables in your configuration such as: IP addresses, passwords, license information etc. would differ based on your environment and specifications.

All the sample configuration used in this service chain example can be downloaded here.

Configure and Deploy VNFD

Create VNFD for CSR

Note You can download the zipped folder containing all the configuration files for VNFs, VNFDs, and NSDs here.

Step 1: Create a file called V_CSR.cli with content from this location.

Step 2: Log in to NCS CLI and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge V_CSR.cli
commit
top
```

Create VNFD for ASA

Step 1: Create a file called V_ASA.cli with content from this location.

Step 2: Log in to NCS CLI by running the command and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge V_ASA.cli
commit
top
```

Configure VNFD Deployment For Primary Consumer CSR

1. Create a text file called VD_CSR_PC.txt with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_CSR_PC.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_CSR_PC.cli
commit
top
```

Configure VNFD Deployment For Secondary Consumer CSR

1. Create a text file called VD_CSR_SC.txt with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_CSR_SC.cli, with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_CSR_SC.cli
commit
top
```

Configure VNFD Deployment For Primary Provider CSR

1. Create a text file called VD_CSR_PP.txt for day-0 VNF with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_CSR_PP.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_CSR_PP.cli
commit
top
```

Configure VNFD Deployment For Secondary Provider CSR

Create day-0 VNF for your secondary provider CSR

1. Create a text file called VD_CSR_SP.txt for day-0 VNF with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_CSR_SP.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_CSR_SP.cli
commit
top
```

Configure VNFD Deployment For Primary ASA

1. Create a text file called VD_ASA_PM.txt with content from this location.

2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_ASA_PM.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_ASA_PM.cli
commit
top
```

Configure VNFD Deployment For Secondary ASA

Create day-0 VNF for your secondary ASA.

1. Create a text file called VD_ASA_SM.txt for day-0 VNF with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_ASA_SM.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_ASA_SM.cli
commit
top
```

Configure and Deploy NSD

Note You can download the zipped folder containing all the text files referenced in this document here.

Create NSD for CSR_ASA_CSR

Step 1: Create a file called N_CSR_ASA_CSR_E2E.cli with content from the following location: https://github.com/Cisco-SAE/CSRv_ECMP-ASAv_HA-CSRv_ECMP/blob/master/N_CSR_ASA_CSR_E2E.cli.

The preceeding NSD includes six VNF profiles. The NSD includes the following Service Access Point Descriptors (SAPD).

- FACING_CONSUMER_SAPD INSIDE: Represents the consumer endpoint and indicates traffic flow from the consumer endpoint gateway.
- MANAGEMENT: Represents VNF management.
- FACING_CONSUMER_SAPD OUTSIDE: Represents the provider endpoint and indicates traffic flow from the provider endpoint gateway.
- software-image-descriptor image: Represents the file on the web server.

Step 2: Log in to NCS CLI and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge N_CSR_ASA_CSR_E2E.cli
commit
top
```

Configure NSD Deployment For VNFs

In this step, you will create an NSD deployment for the consumer CSR, the provider CSR, and the ASA, that form part of your service design.

1. Create a text file called ND_CSR_ASA_CSR_E2E .cli with content from the following location: https://github.com/Cisco-SAE/CSRv_ECMP-ASAv_HA-CSRv_ECMP/blob/master/ND_CSR_ASA_CSR_E2E.cli.

Note The names of the VNFDs and NSDs referenced in the text file above should match the VNFD and NSD names created in the preceding sections.

2. Log in to NCS CLI and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge ND_CSR_ASA_CSR_E2E .cli
commit
top
```

Deploy Service Chain

Configure External Endpoints

The following example show how to configure external endpoints using pre-allocated resources such as IP address, gateways, netmasks, and VLANs.

Note All the configuration examples are representative only and are specific to the service chain example being used in this chapter. The variables in your configuration such as: IP addresses, passwords, license information etc. would differ based on your environment and specifications.

1. Create a text file called EEP_CSR_ASA_CSR.cli with content from the this location.
2. Login to NCS CLI and load merge the file you created in step 1 as shown below.

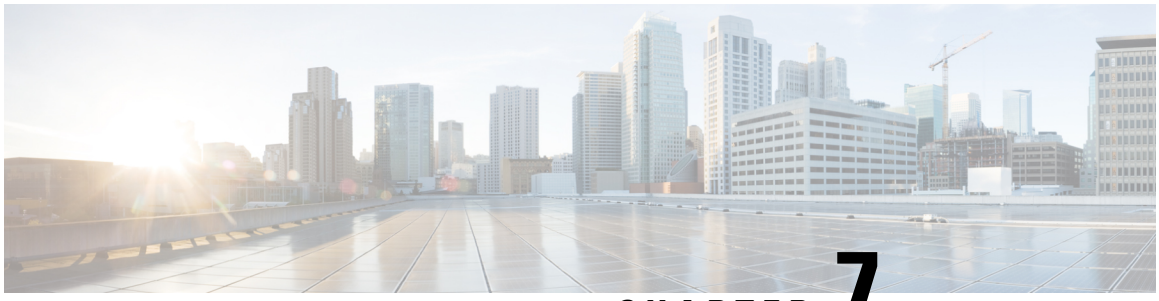
```
ncs_cli -C -u admin
configure
load merge EEP_CSR_ASA_CSR.cli
commit
top
```

Deploy Full Service Chain (CSR-ASA-CSR)

1. Create a text file called E2E_1_CSR_ASA_CSR.cli with content from this location.

2. Login to NCS CLI and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge E2E_CSR_ASA_CSR.cli
commit
```



CHAPTER 7

Related Documentation

- Release Notes for Cisco Secure Agile Exchange 1.0—Release Notes for the Cisco Secure Agile Exchange solution.
- Release Notes for CiscoSAE Core Function Pack—Release Notes for the Cisco SAE core function pack.
- Cisco SAE Core Function Pack Installation Guide—Contains details on how to install SAE core function pack.
- Cisco SAE Core Function Pack User Guide—Contains details on how to use the SAE core function pack.
- Cisco Network Services Orchestrator Datasheet—Contains details on features and specifications of NSO.
- Cisco Network Services Orchestrator (NSO) Solutions—Documentation for Cisco NSO and related solutions.
- Cisco Elastic Services Controller Release Notes—Release Notes for ESC 4.3.
- Cisco Elastic Services Controller 4.3 User Guide—Explains how to manage reources using ESC, onboard, deploy, and configure VNFs, and more.
- Cisco Elastic Services Controller Install and Upgrade Guide—Explains how to install ESC 4.3 and upgrade ESC.
- Cisco Cloud Services Platform Release Notes—Release notes for Cisco Cloud Services Platform
- Cisco Cloud Services Platform Datasheet—Contains details on the features and specifications of CSP 5000
- Cisco Cloud Services Platform Configuration Guide—Describes how to configure SNMP, SR-IOB, create port channels and more for CSP devices
- Cisco Cloud Services Platform Quick Start Guide
- Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.x—Describes how to configure basic interface parameters, port channels, vPCS, and more for the Cisco Nexus 9000 series switches
- CSRv-ASAv-CSRv Full Service Chain—Contains downloadable text files for day-0 VNF configuration, VNFDs, and NSDs used in the service chain example used in this document