
cisco Live!
ALL IN

The bridge to possible

Cisco Secure Firewall Cloud Native on AWS

Anubhav Swami, Principal Architect
@swamianubhav
BRKSEC-3561

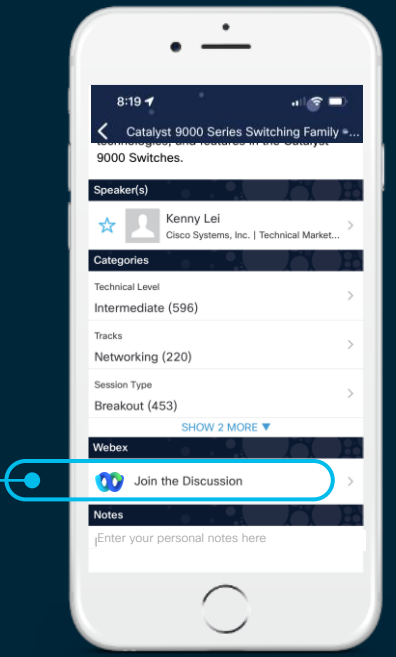
Cisco Webex App

Questions?

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

How

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



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3561

Webex spaces will be moderated by the speaker until June 17, 2022.

Speaker

Anubhav Swami
Principal Architect
CCIE# 21208

answami@cisco.com
http://cs.co/anubhavswami
www.linkedin.com/in/anubhavswami/

Cisco Experience

TAC Engineer (Security) – 5 Years
ASA Business Unit – 2 Years
Technical Marketing Engineer – 5 Years
Secure Solutions Architect – 2.5 Years

Current role: Principal Architect

SFCN | K8s | Cloud Native
ZTNA SASE | ASA NGFW | Cloud Security
AWS | Azure | GCP

From Delhi (India)

Based in North Carolina - USA

Photography

Important: Hidden Slide Alert!

Look for this “For Your Reference” symbol in your PDF

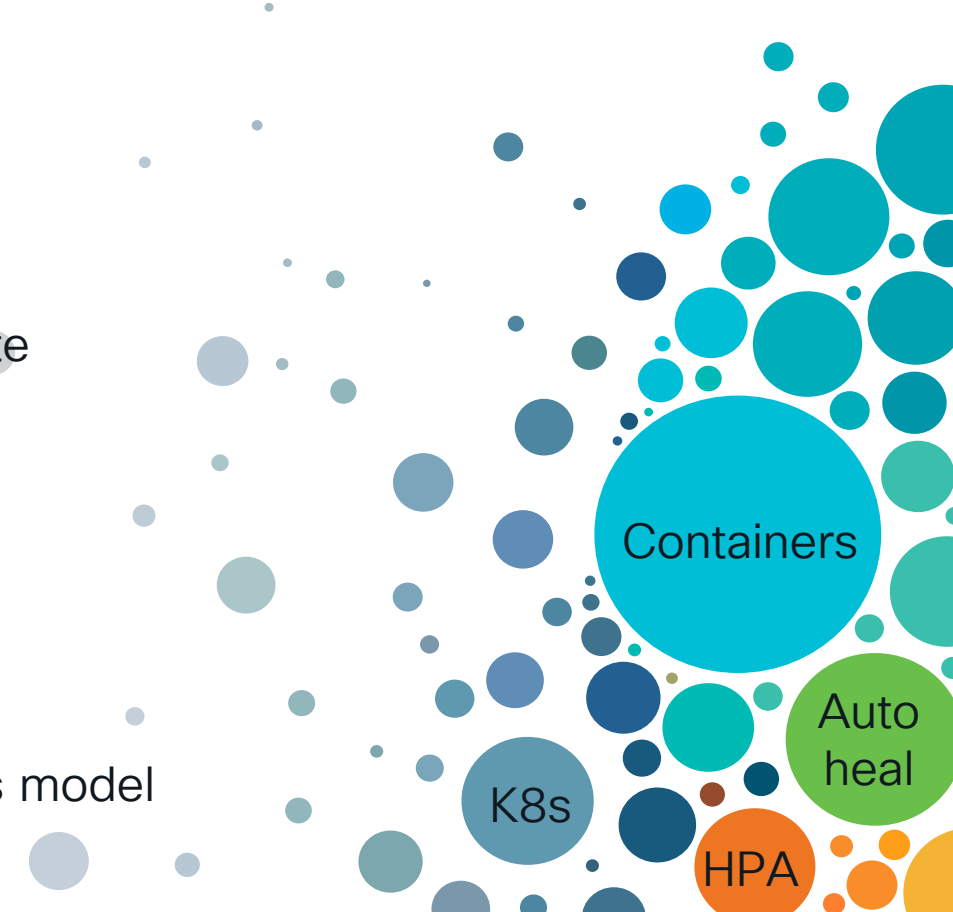
Agenda

- Introduction
- Cisco Secure Firewall Cloud Native Architecture
- Use-cases
- What's new?
- Demo
- CRDs
- Deployment
- AWS Quick Start
- Resources

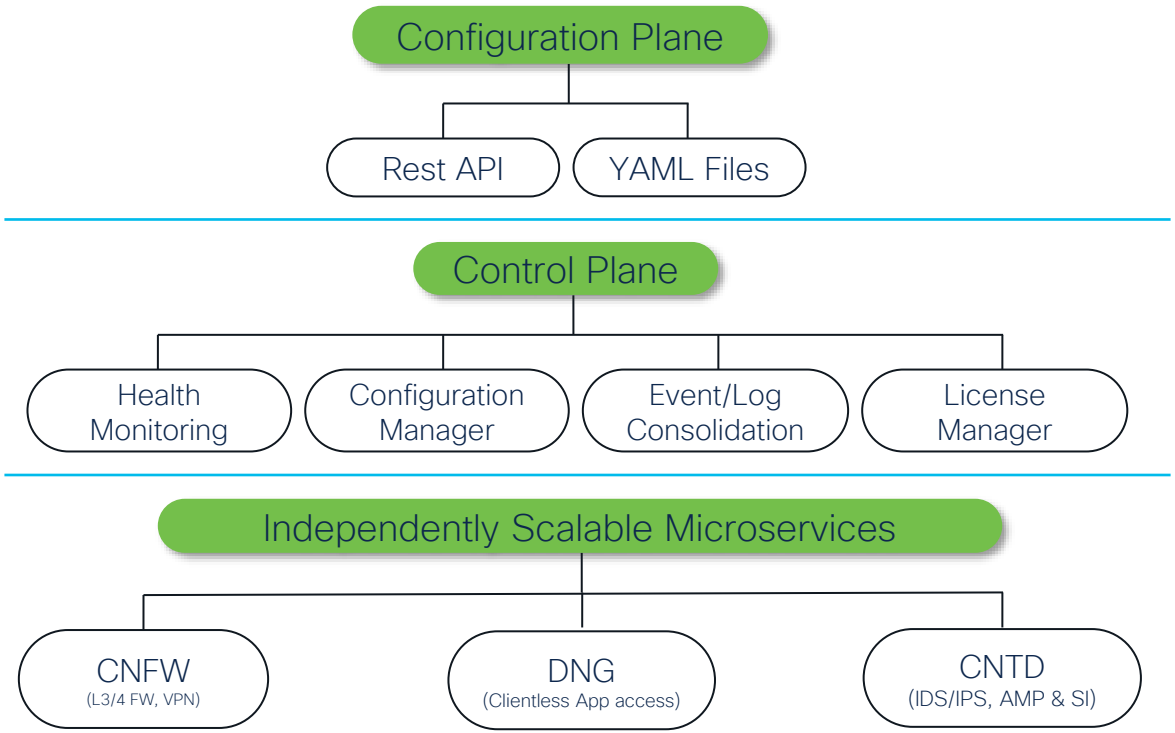
Introduction

Why Cloud Native?

- Scalable and resilient
- Light weight Containers
- Easy to Orchestrate and automate
- Faster automated bootstrapping
- Faster recovery and healing
- Infrastructure as Code & DevOps model



Cisco Secure Firewall Cloud Native Architecture

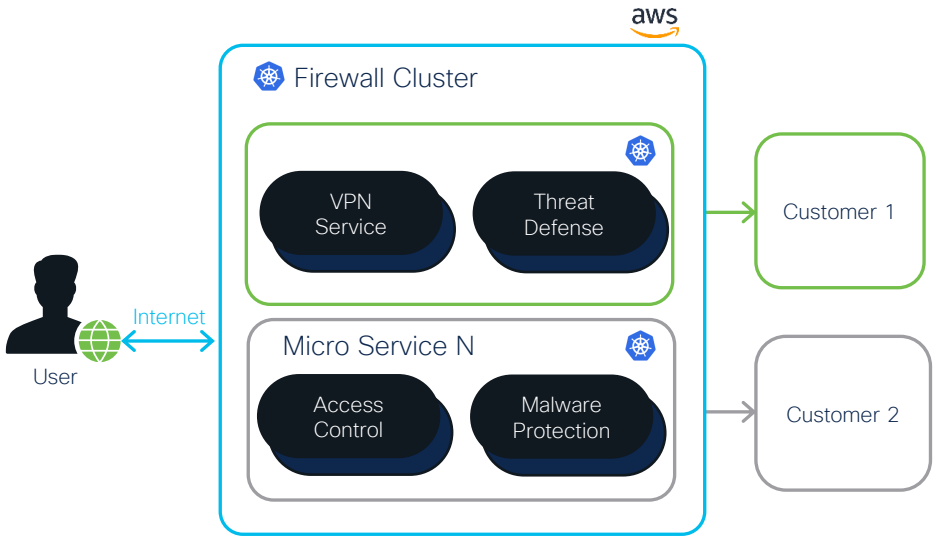


- Independent microservices
- Independent scalability and resiliency
- Control Plane for policy abstraction
- Programmability using Rest API/YAML

Target Customer

- Large enterprises
- Service Providers
- Managed Security Service Providers

Highly Scalable Secure Edge Built with Cloud Native Firewall



Highly Scalable and Multi-Tenant Architecture

Differentiation

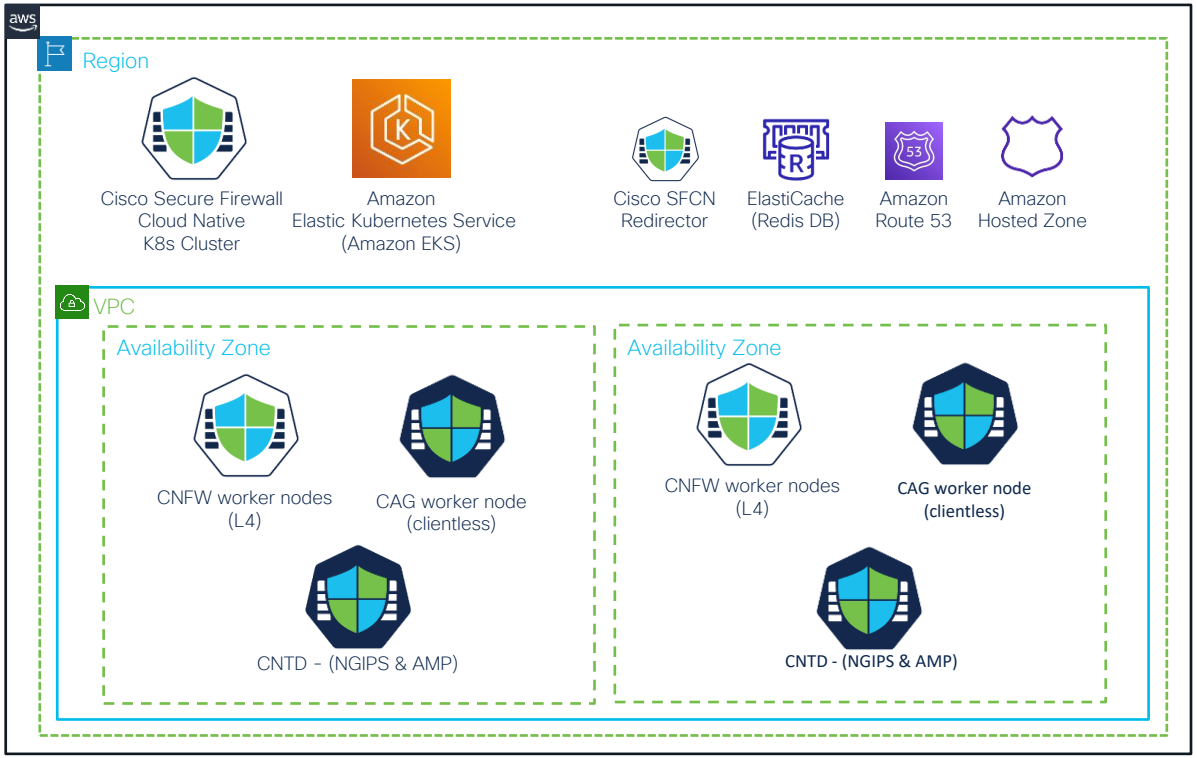
- Linearly scalable – Not a step function
- Real time auto-scale and auto-heal
- Scale up to 100s of Gbps
- Capability to insert additional security services
- Enables ZTNA readiness

Target customer profiles

- Large enterprises
  - Simplify the deployment of scalable (and elastic) security stack
- Service Providers
  - Massive scale capability
- Managed Security Service Providers
  - Automation and scalability

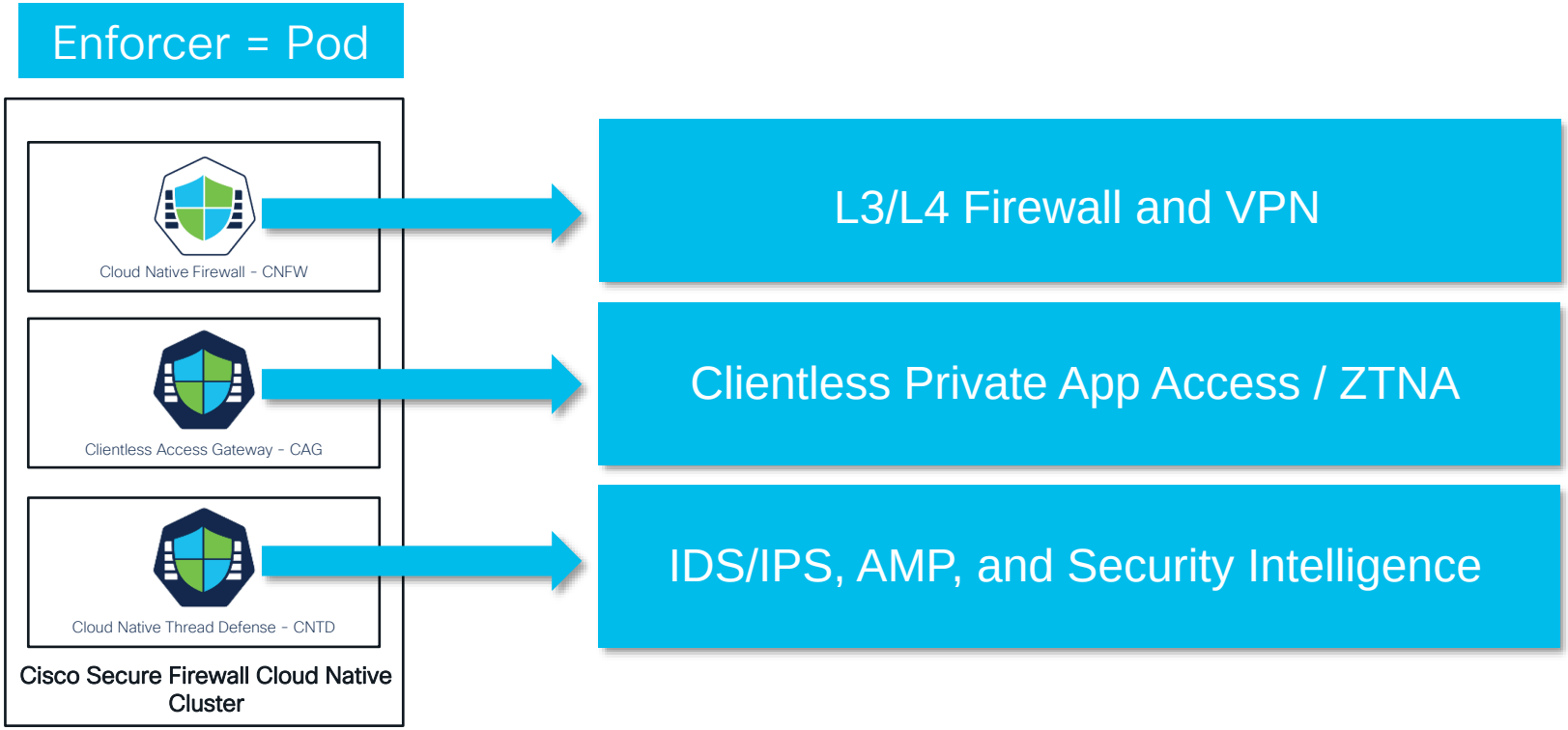
Architecture

Cisco Secure Firewall Cloud Native
Building Blocks

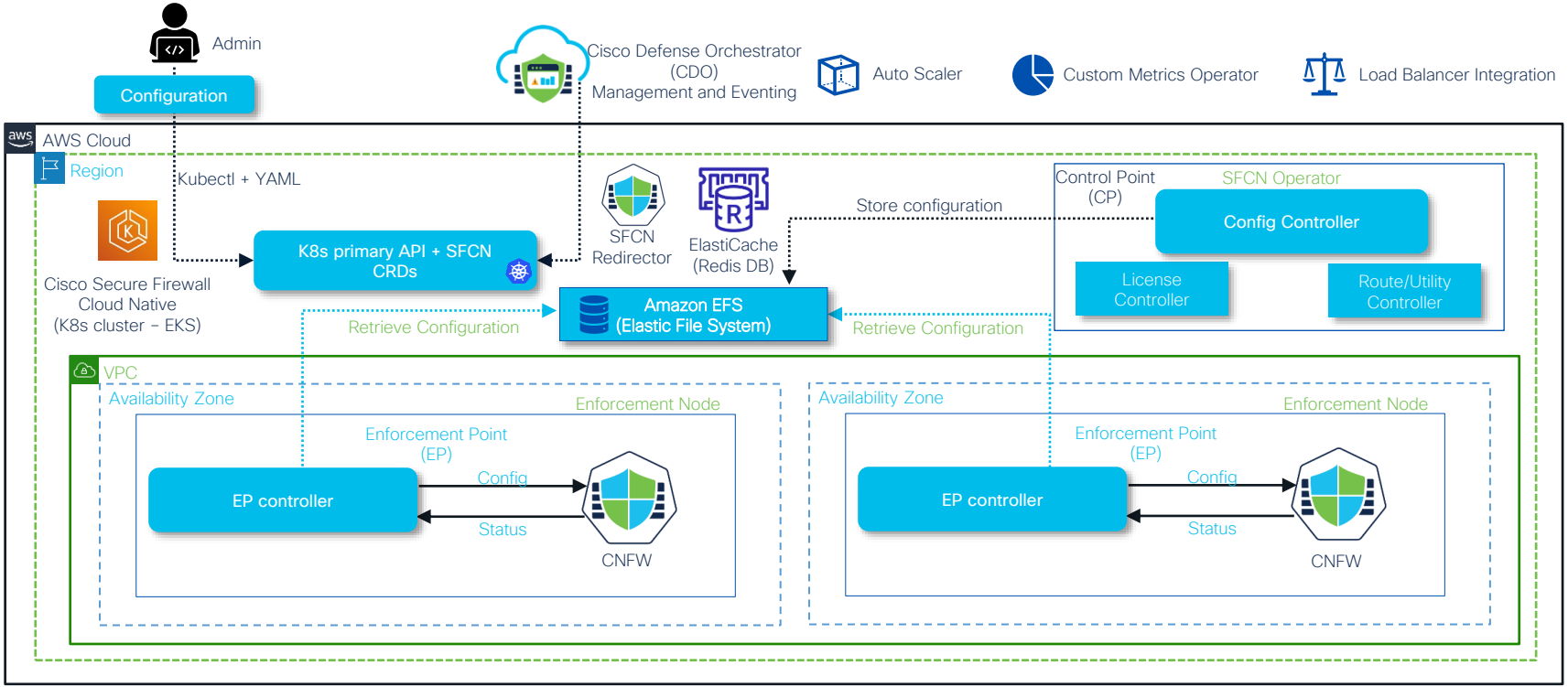


- Scalable architecture
  (Horizontal Pod Autoscaler - HPA)
- Modular security architecture
- K8s orchestrated deployments
  (Amazon EKS)
- DevOps friendly
  (YAML + CI/CD + GitOps)
- CRDs and Helm Charts
- Config management
  (REST API/YAML/CDO UI)
- Data externalization (Redis) for stateless services
- Multi-region and multi-AZ support
- Multi-tenant aware
- Bring your own license (BYOL)
- Enforcer footprint
  4 core

Cisco Secure Firewall Cloud Native Enforcers



Cisco Secure Firewall Cloud Native Architecture



CNFW performance and support instance type

Component	Instance Type
Control Point (CP)	m5.xlarge, c5.2xlarge
Enforcement Point (EP)	m5.xlarge, c5.2xlarge
Redirector (Pod on EP)	m5.xlarge, c5.2xlarge
Redis	cache.m5.large (default), cache.m5.xlarge*

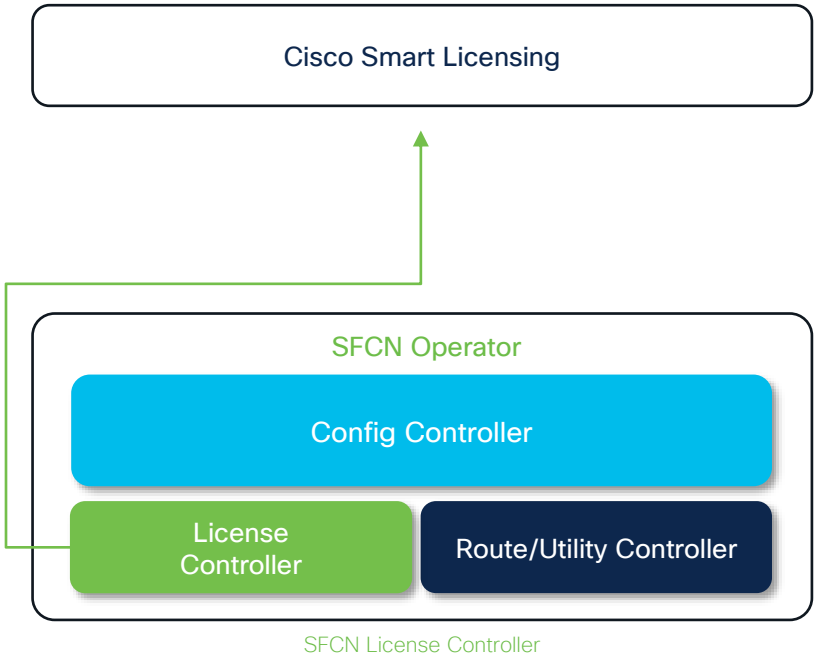
Type	Throughput
IPsec VPN throughput (AES 450B UDP test)	1.5 Gbps

Type	Max VPN peers
IPsec VPN peers	2000
Cisco AnyConnect or Clientless VPN sessions	2000

*can be changed to handle more VPN sessions

Cisco Secure Firewall Cloud Native Licensing

- Cisco Secure Firewall Cloud Native supports BYOL using Cisco Smart Licensing
- Cisco CNFW is based on ASA 9.16
- License is based on CPU Cores used by EP
- Unlicensed SFCN EP runs at 100 Kbps
- Supports multi-tenancy
- License controller (LC)
  - LC is part of the SFCN operator
  - LC handles licensing
- AnyConnect license model is same as ASA AnyConnect license model



Cisco Secure Firewall Cloud Native
Service Role and Topology

Service Role	Feature
vpnredirector	Redirector
default	VPN headend

Service Role Combination	Topology
default	Default (VPN headend without redirector)
vpnredirector -> VPN headend (default)	vpnredirector → VPN headend (recommended)

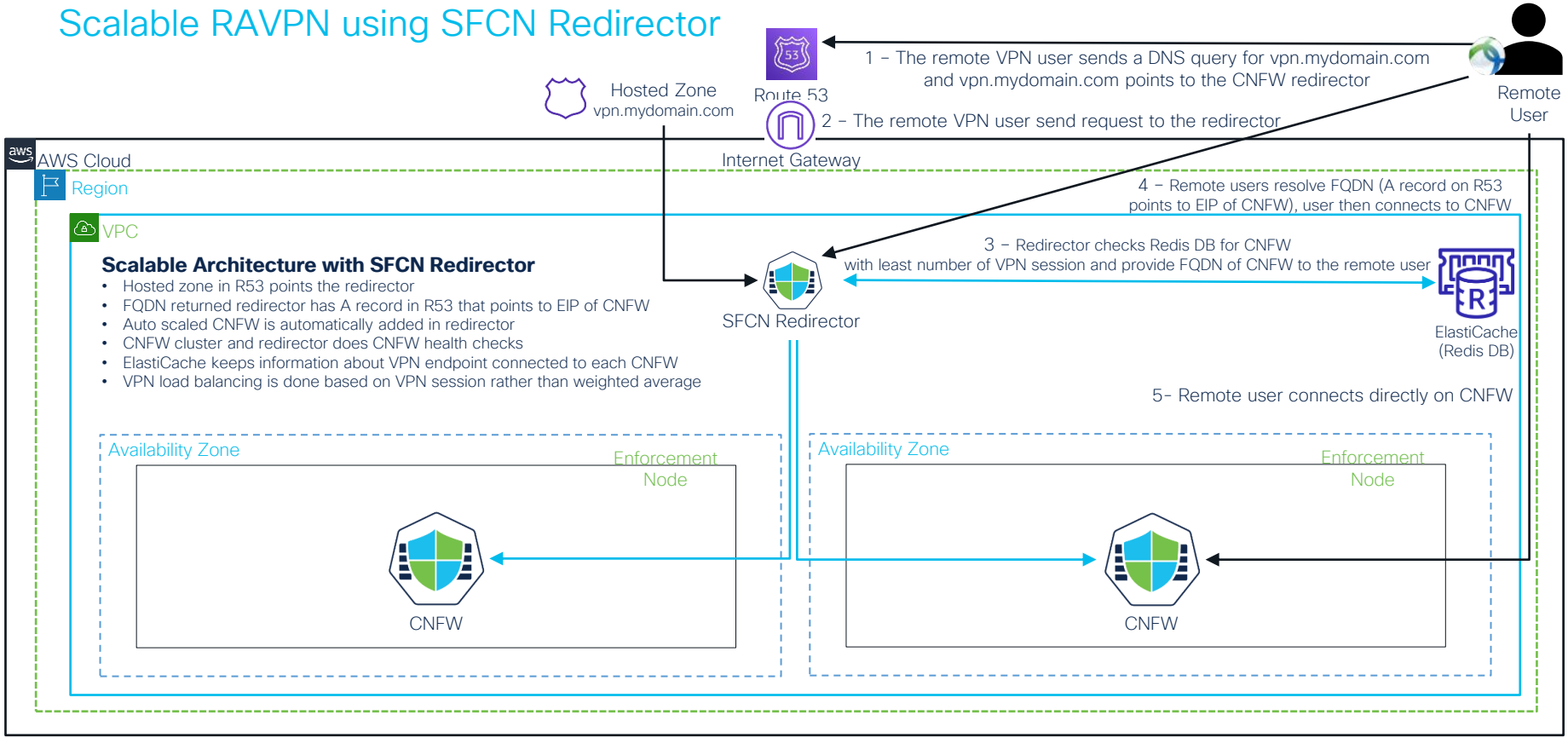
Use-cases

Use Cases

- Scalable RAVPN architecture with Redirector, Amazon Route 53 and Redis DB
- DC backhaul
- Multi-tenancy
- Scalable cloud hub
- Scalable edge firewall

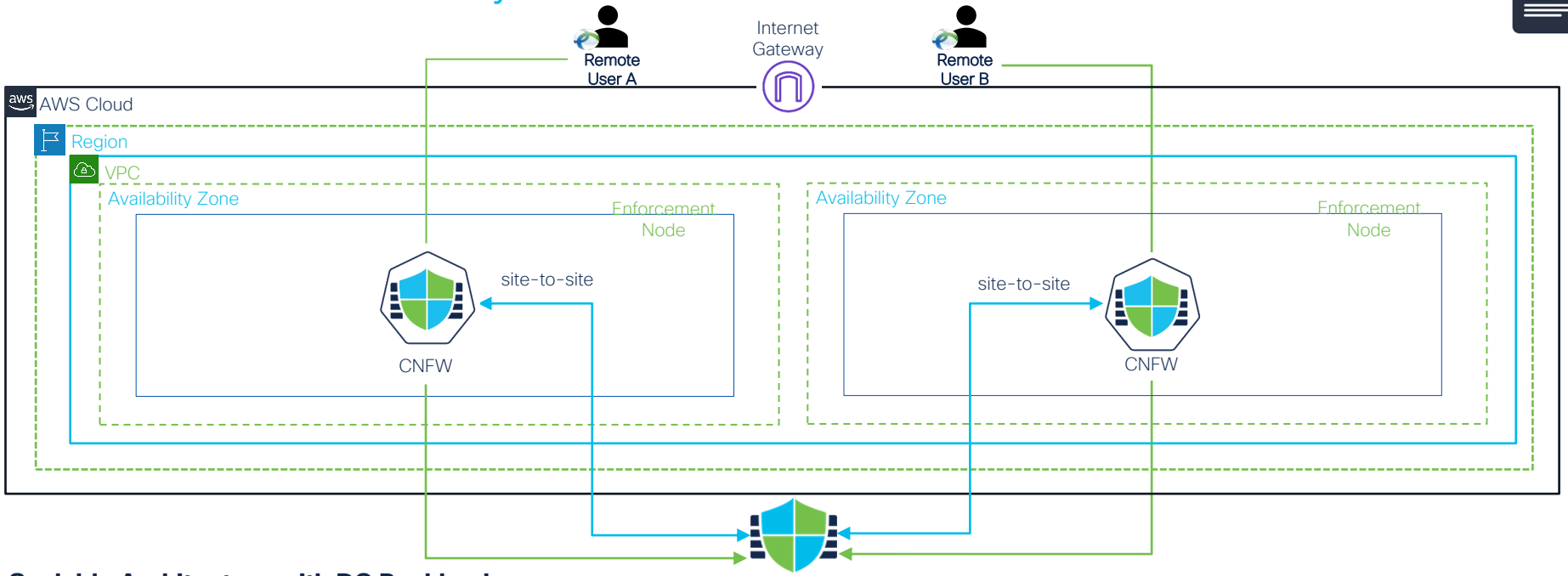
Cisco Secure Firewall Cloud Native

Scalable RAVPN using SFCN Redirector



Cisco Secure Firewall Cloud Native

Backhaul Connectivity

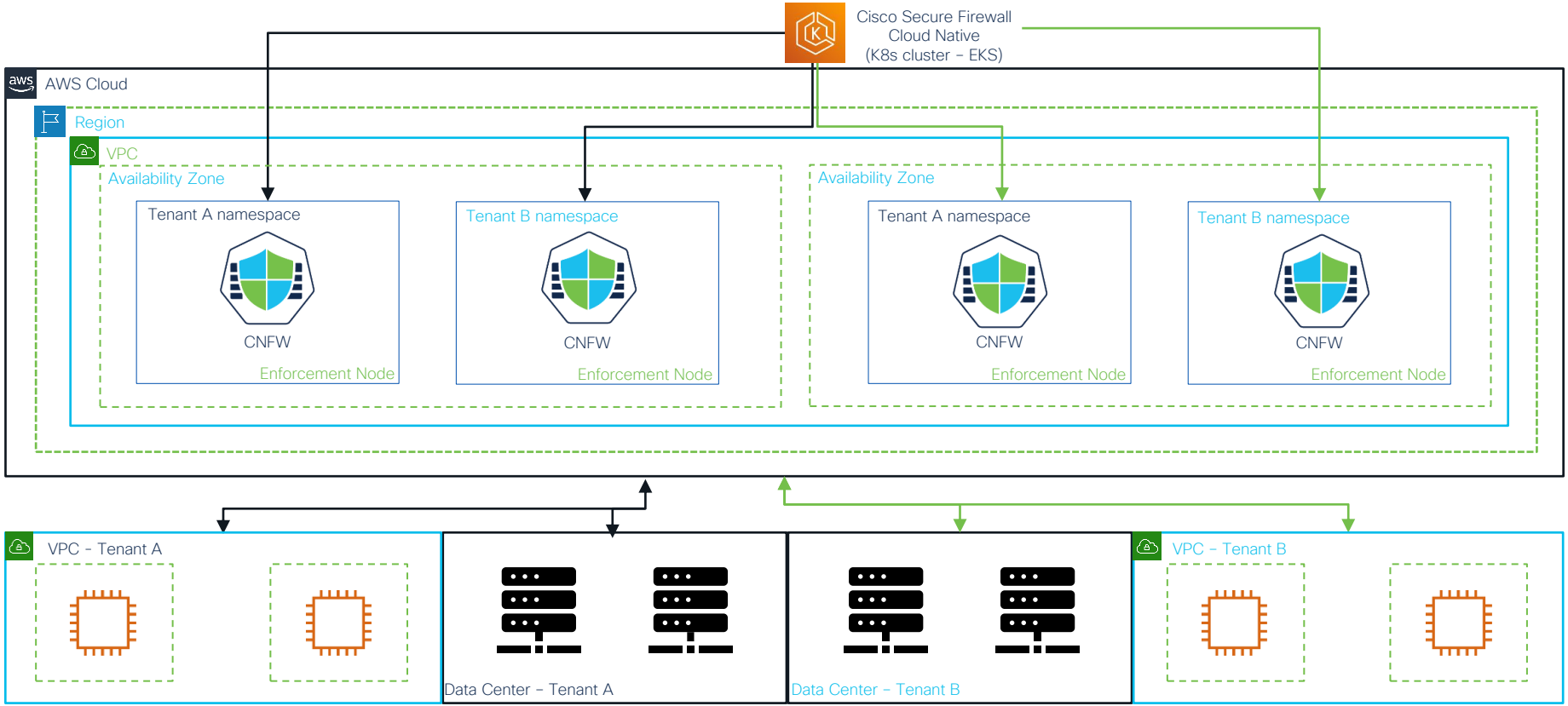


Scalable Architecture with DC Backhaul

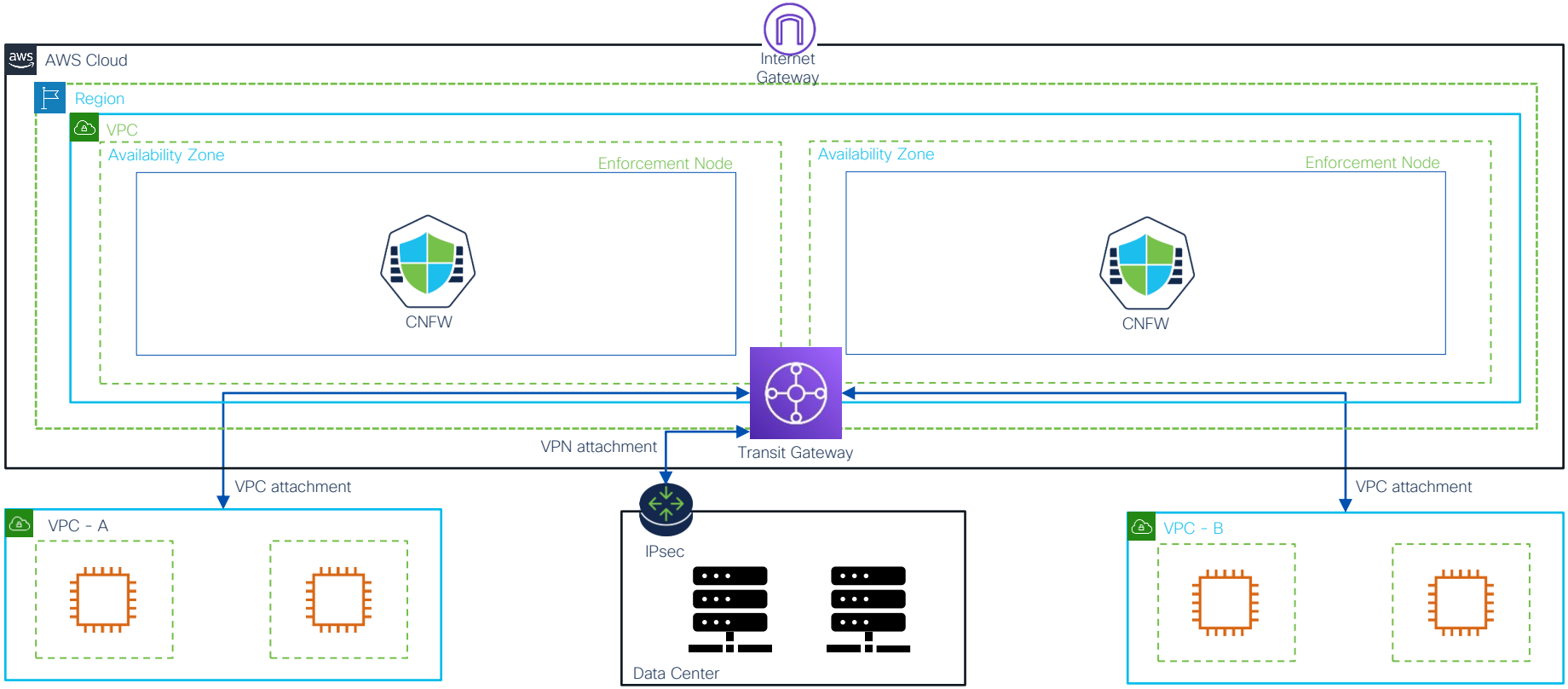
- Auto-scaled CNFW builds tunnel back to DC
- Each CNFW adds are tunnel back to DC
- CNFW and DC Firewall runs BGP
- VPN pool network is redistributed in BGP

Cisco Secure Firewall Cloud Native

Multi Tenancy

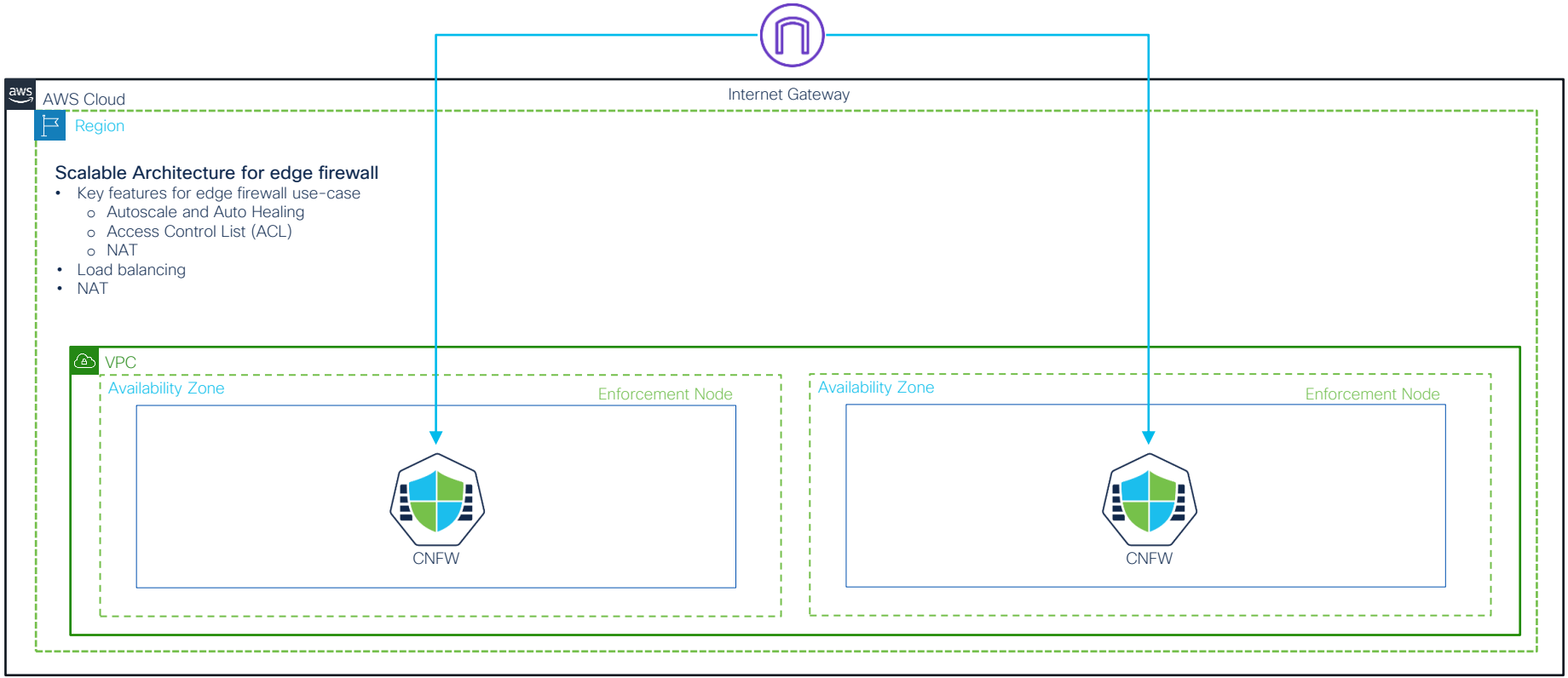


Cisco Secure Firewall Cloud Native
Scalable Cloud Hub



Cisco Secure Firewall Cloud Native

Scalable Edge Firewall



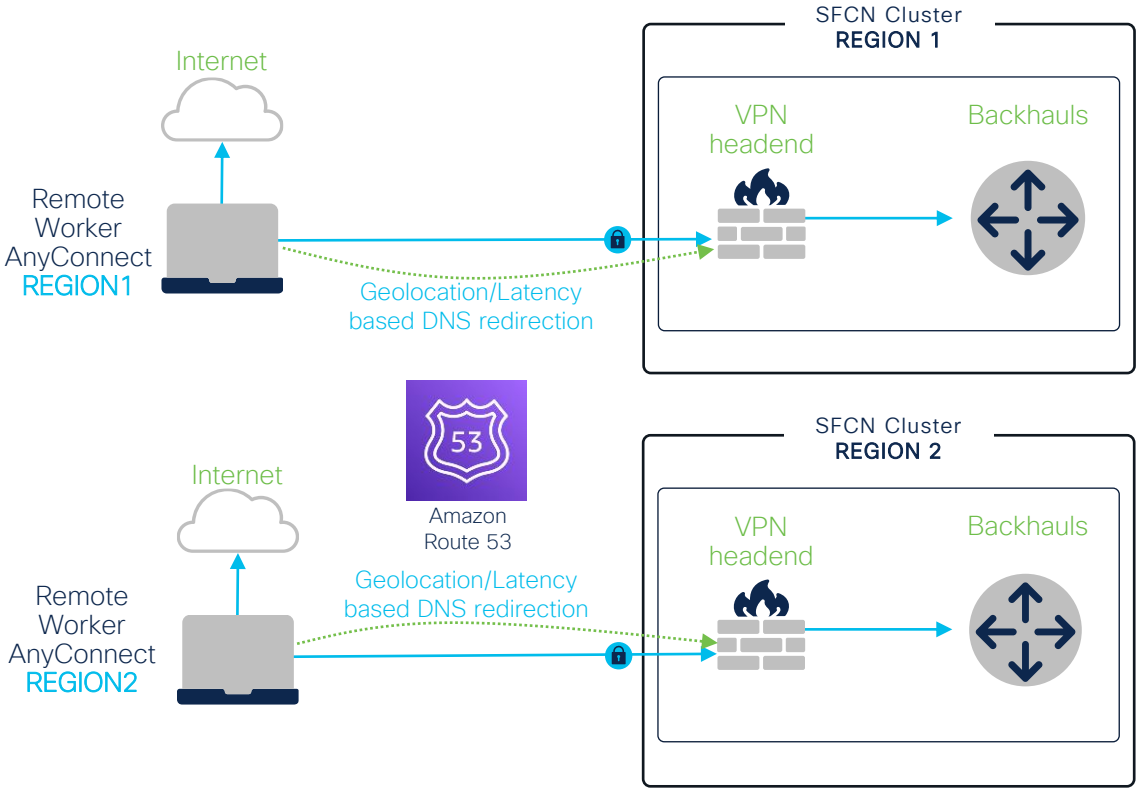
What's new in Cisco Secure Firewall Cloud Native?

cisco Live!

Cisco Secure Firewall Cloud Native 1.1

- Multi-region architecture
- Advanced VPN load balancing
  - Geolocation Latency based load balancing
- SAML authentication

Multi region architecture



SFCN 1.1

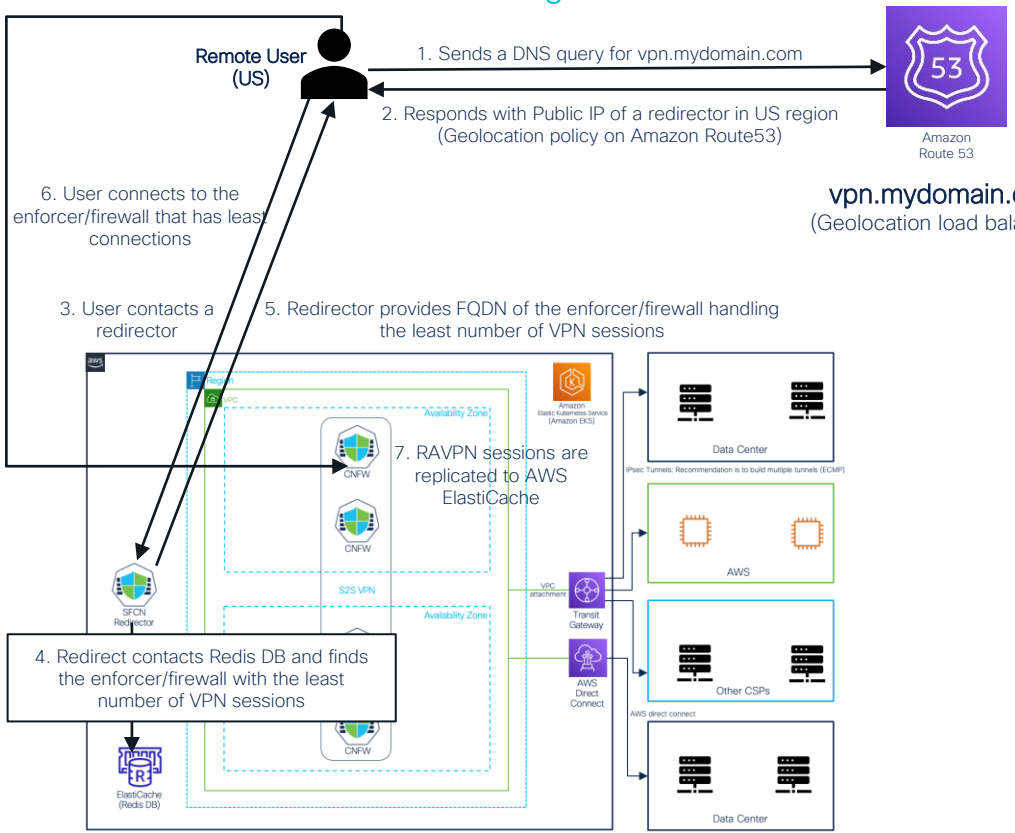
- Multi-region RAVPN
- SAML authentication

DNS load balancing policy

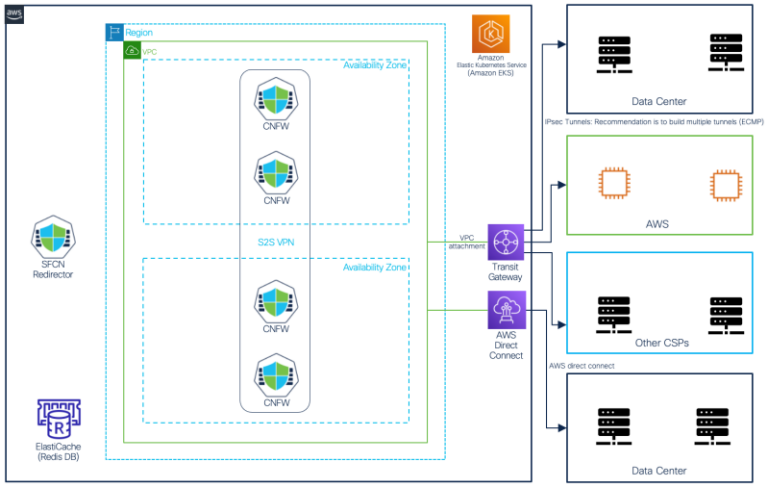
- Region 1 user connects to region 1
- Region 2 user connects to region 2
- Rest of the world connects to region 1

Multi-Region SFCN Architecture

Geolocation based load balancing



SFCN Cluster – USA

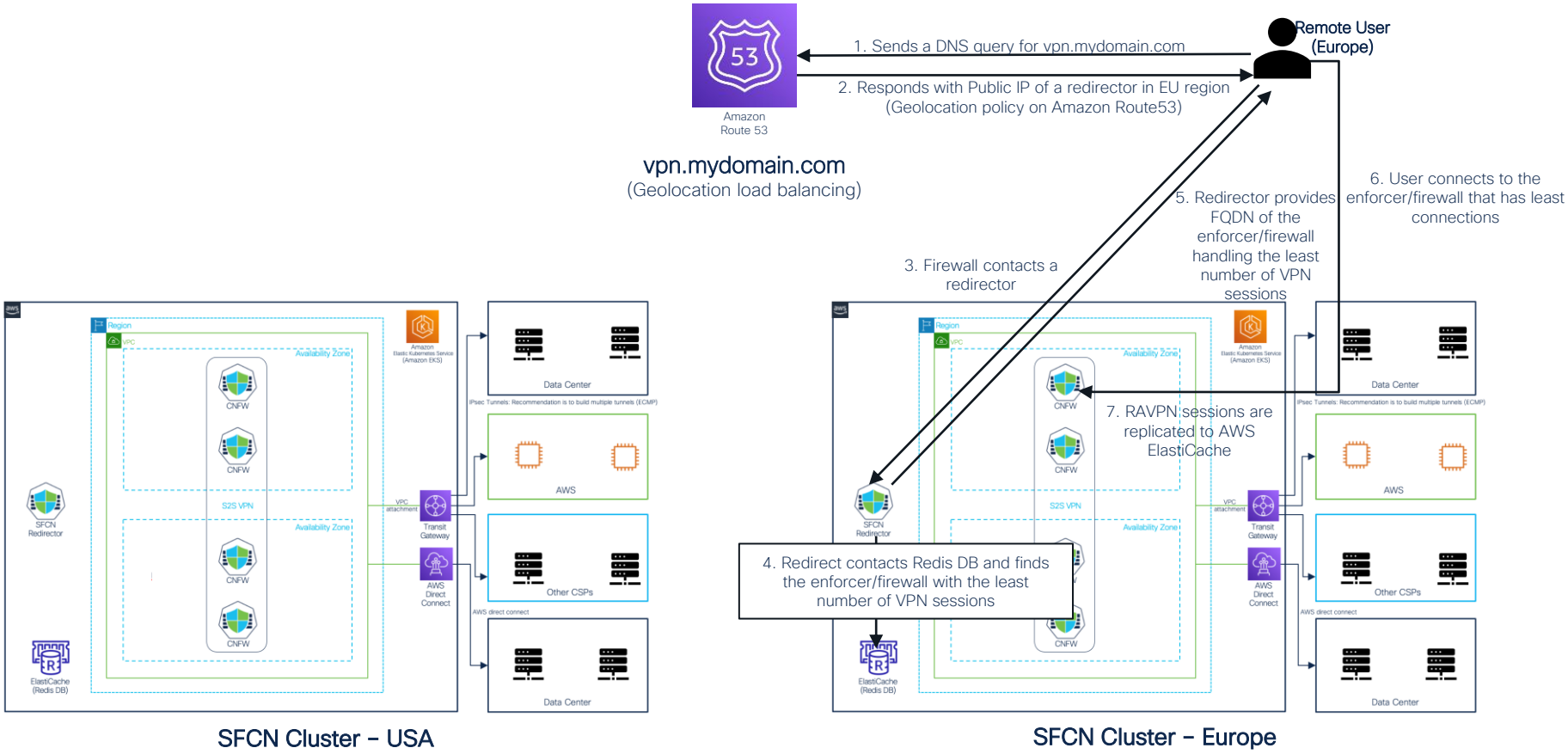


SFCN Cluster – Europe

Multi-Region SFCN Architecture

Geolocation based load balancing

Release 1.1

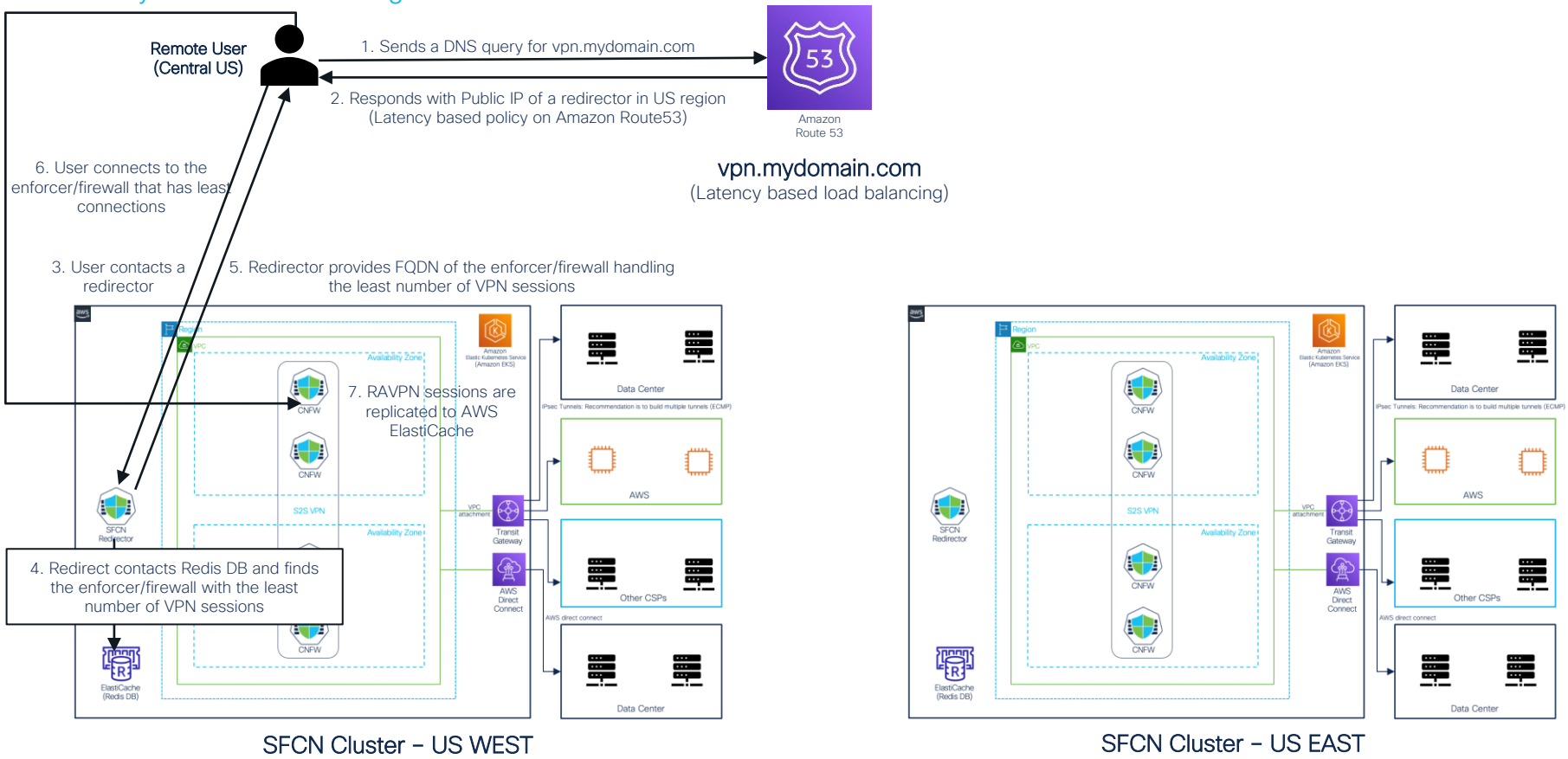


SFCN Cluster – USA

SFCN Cluster – Europe

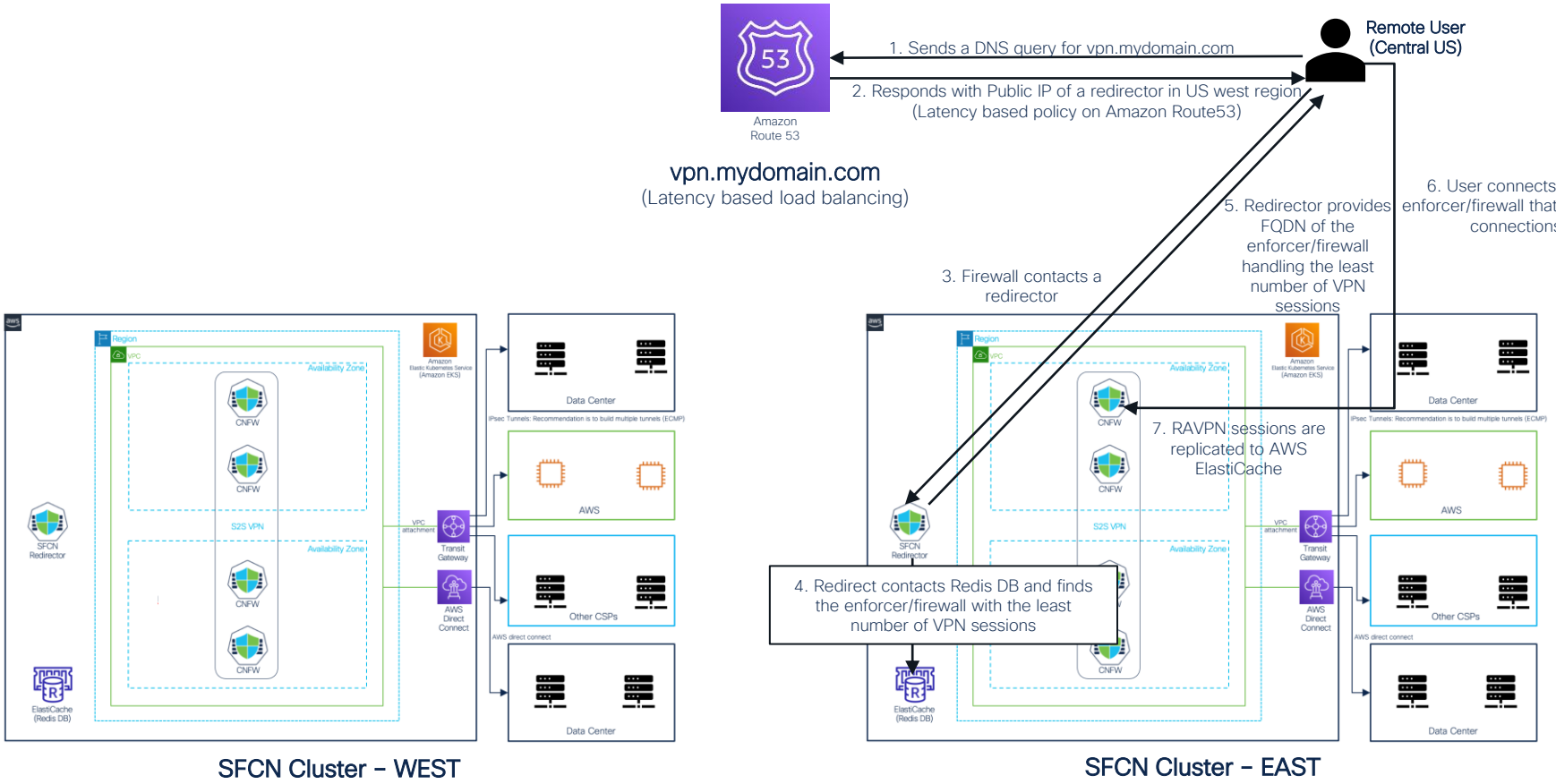
Multi-Region SFCN Architecture

Latency based load balancing



Multi-Region SFCN Architecture

Latency based load balancing

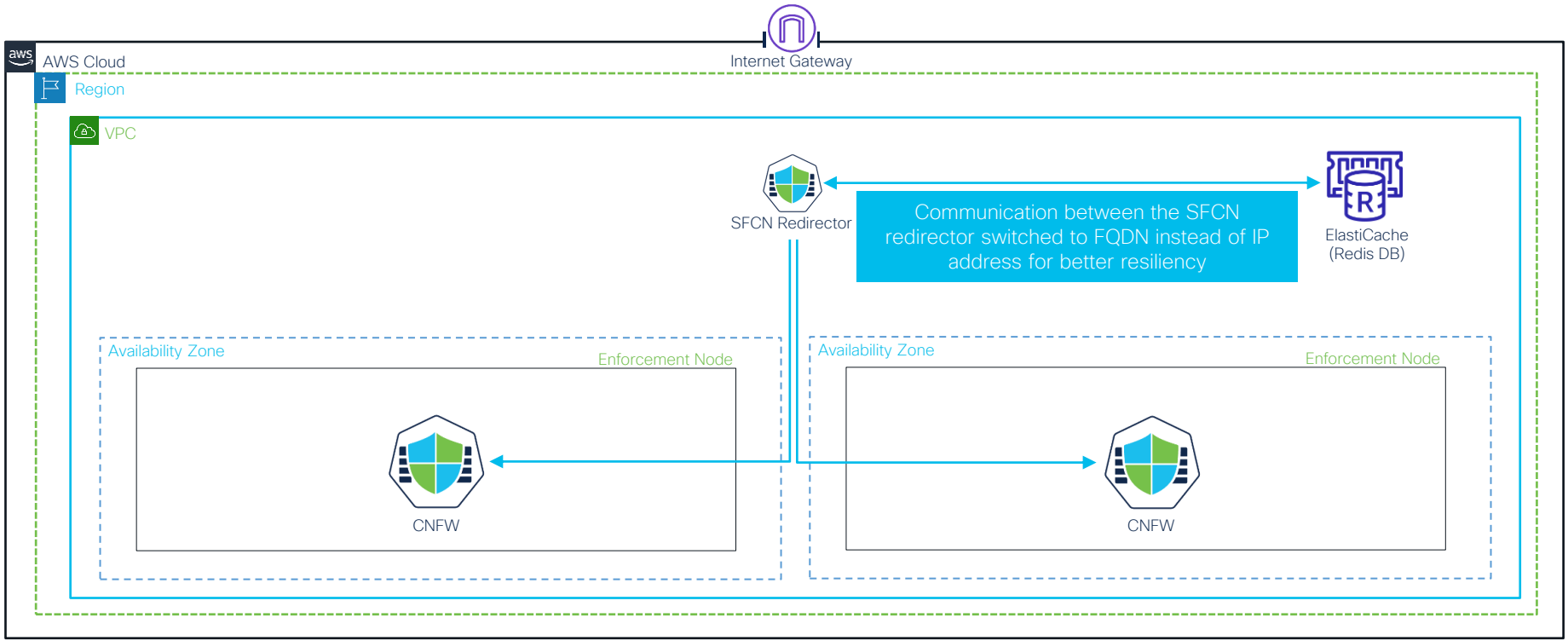


SFCN Cluster – WEST

SFCN Cluster – EAST

Reference

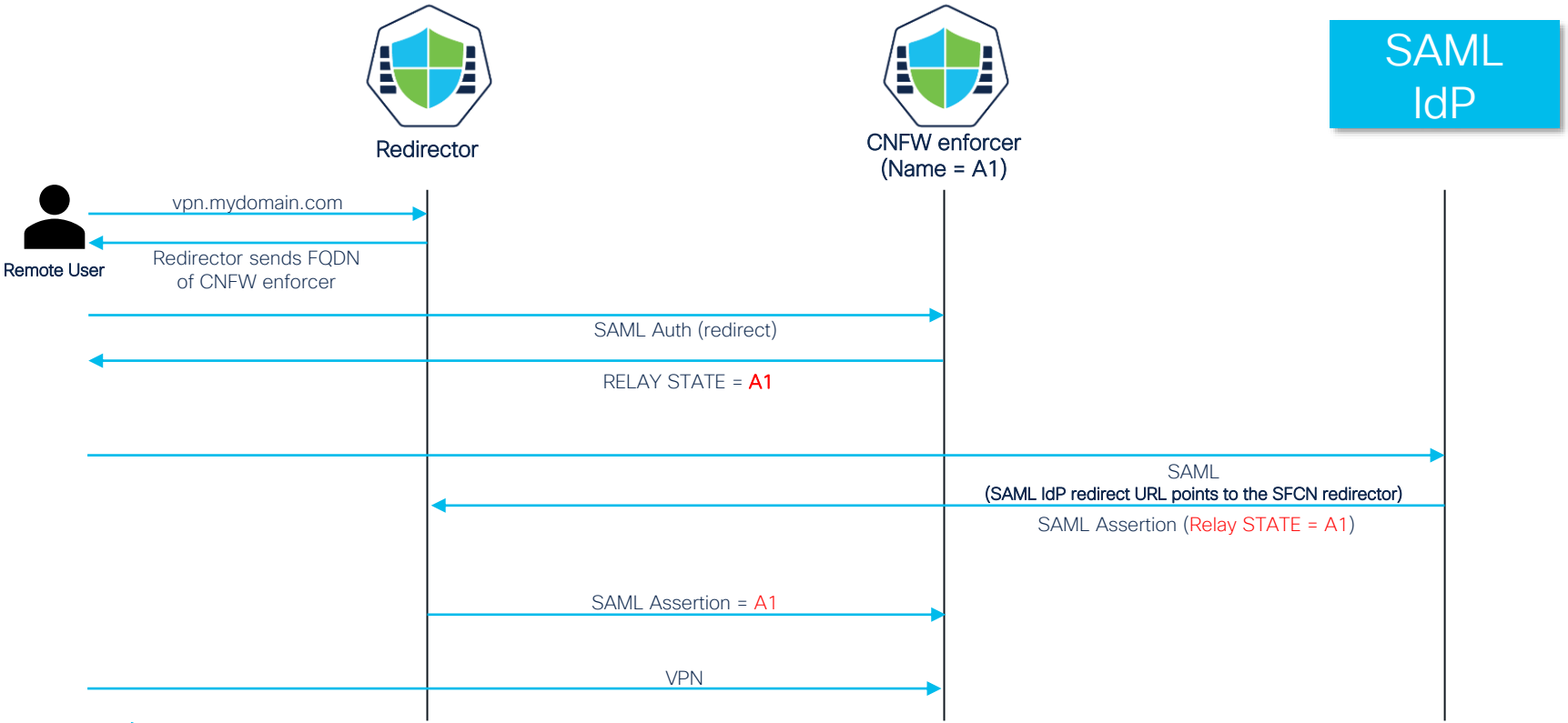
FQDN support for Redis DB



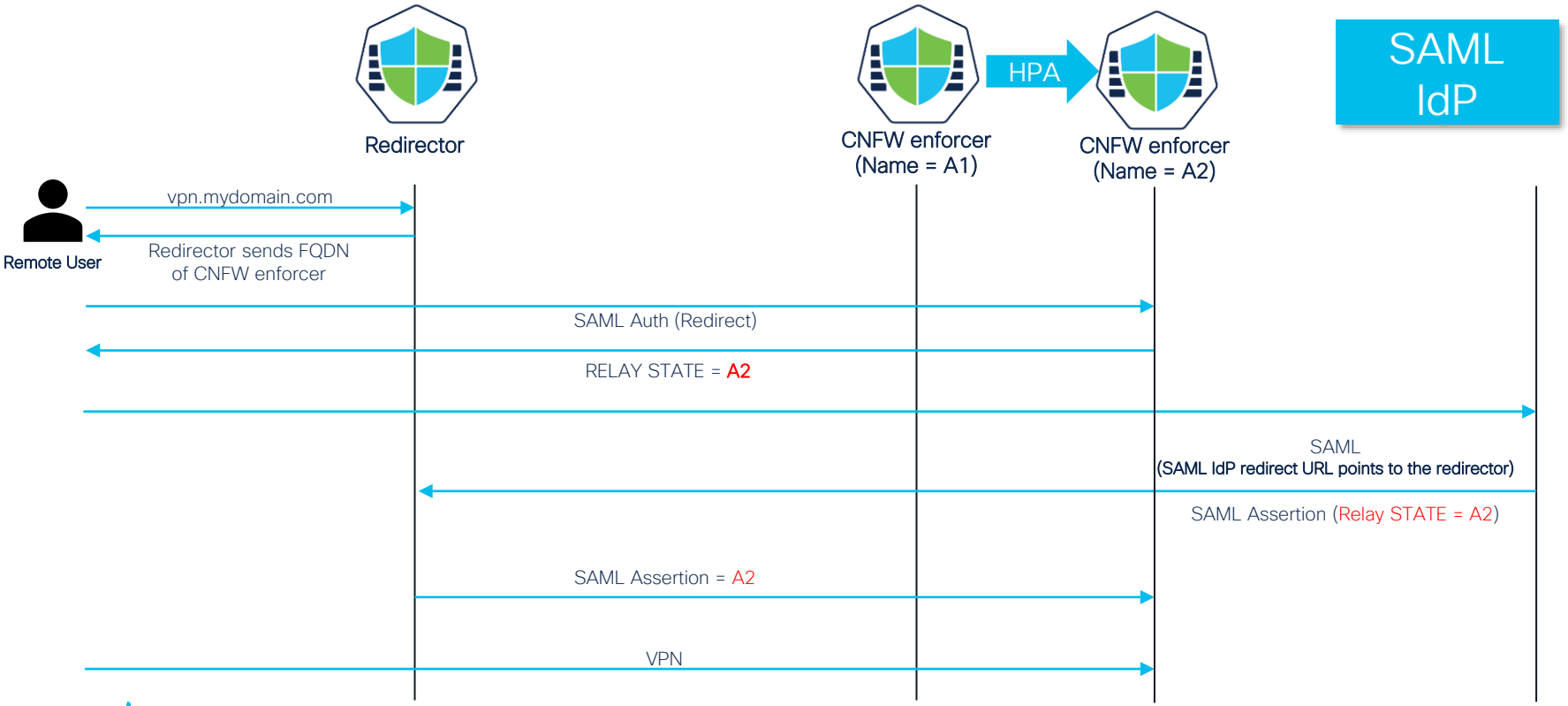
SAML authentication support

- SAML support
  - Single region
  - Multi region
- Works with any IdP and MFA (Duo, OKTA, Azure etc.)
- SAML configuration also works with SFCN Horizontal Pod Autoscaling

SAML authentication support



SAML authentication support (cont.)
Horizontal Pod Autoscaler (HPA)



Cisco Secure Firewall Cloud Native
release 1.5 and 2.0

- Clientless Access Gateway (CAG) for clientless private app access

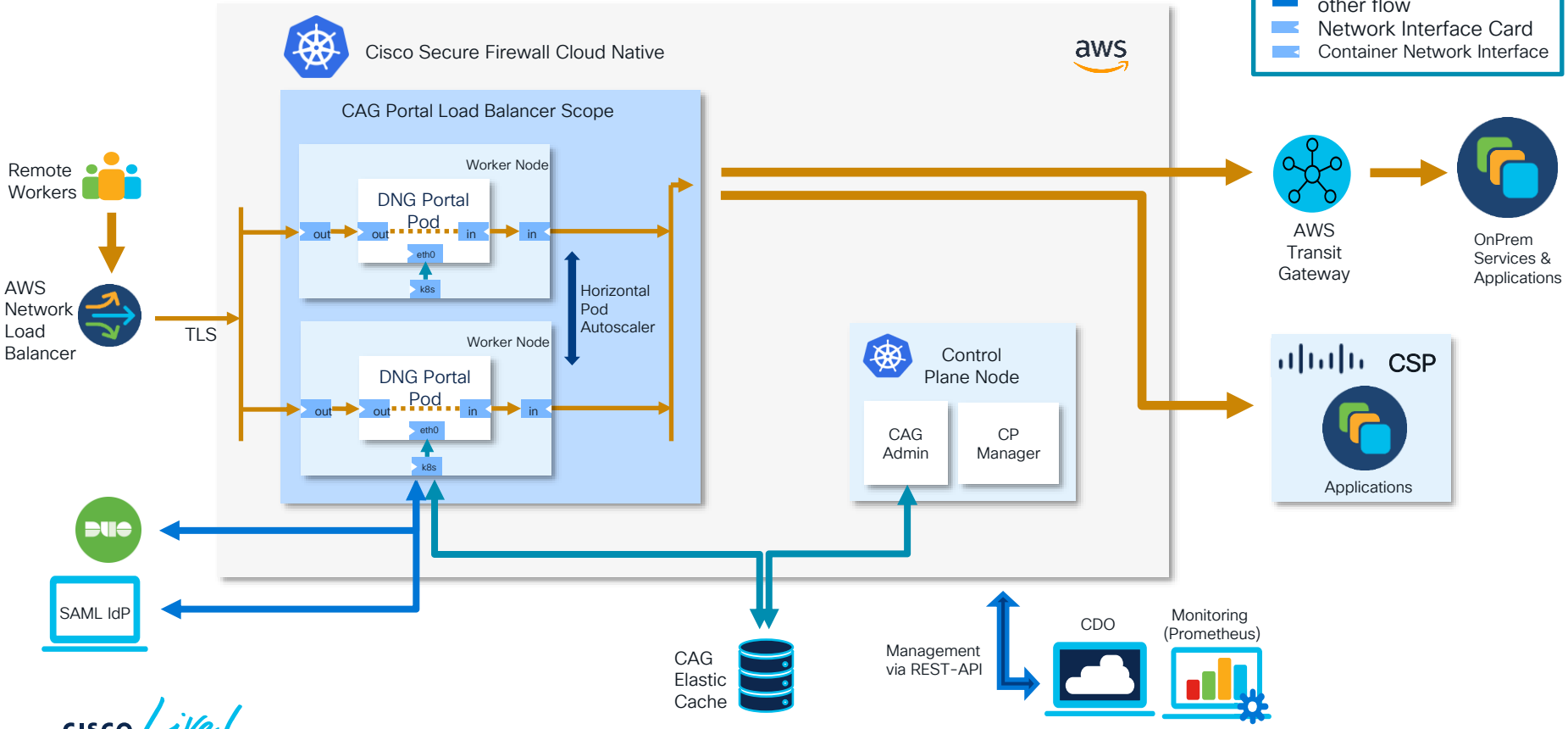
- Cloud Native Threat Defense (CNTD)

Cisco Secure Firewall Cloud Native
Service Role and Topology

Service Role	Feature
vpnredirector	VPN redirector
default	VPN headend
cag	Clientless Access Gateway

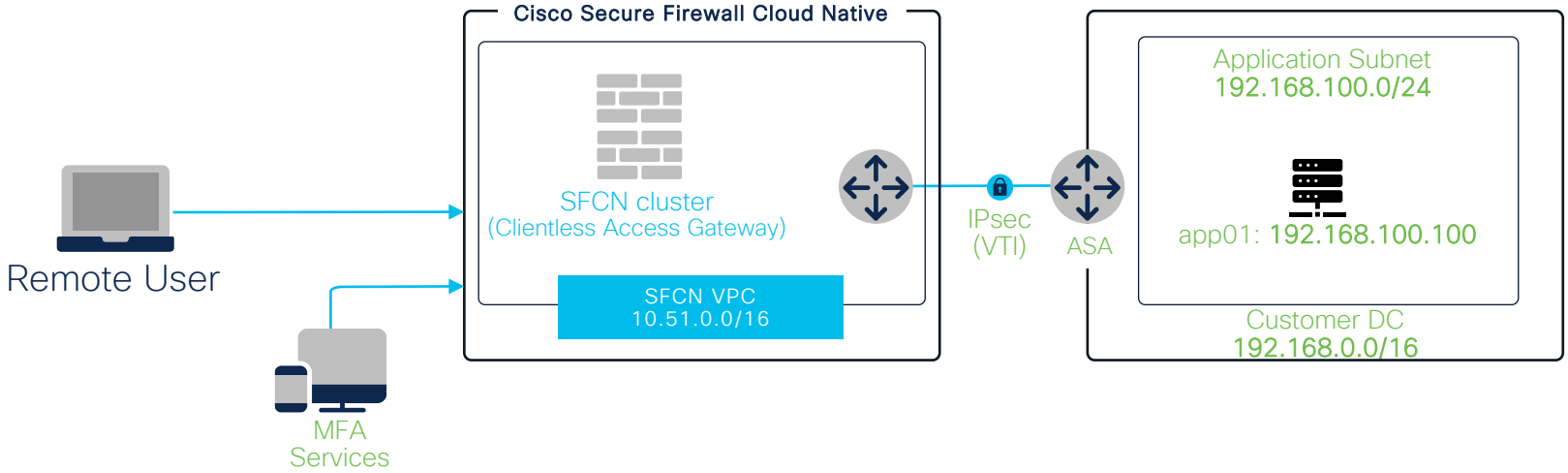
Service Role Combination	Topology
default	default
vpnredirector, default	vpnredirector → default
cag	NLB → cag

Clientless Access Gateway (CAG)



Cisco Secure Firewall Native

use-case: Private App Access

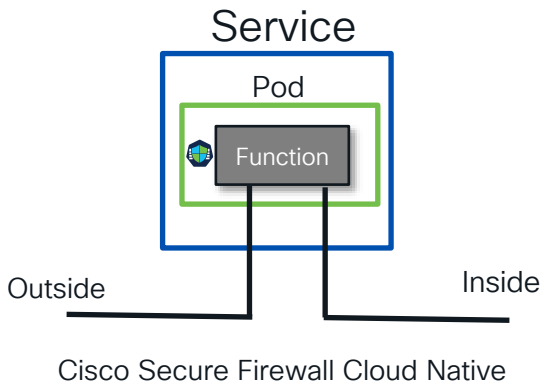


Clientless access gateway provides secure access to the private application

Service Function Chaining (CNTD)

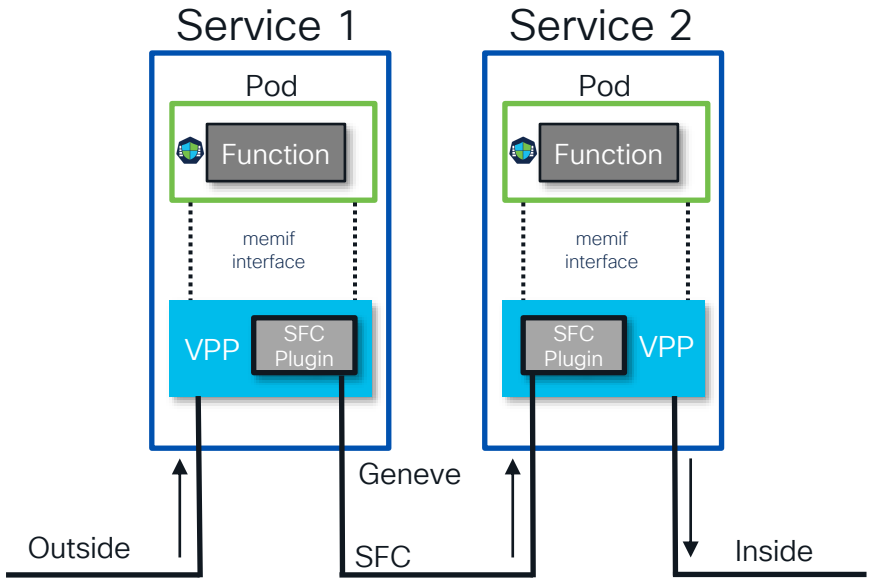
Cisco Secure Firewall without service chain

- Limited to single service
- Limited to only the functions of that service



Cisco Secure Firewall with service chain

- Allows for multiple Services
- Ability to perform multiple functions on traffic
- Traffic flow visibility & control



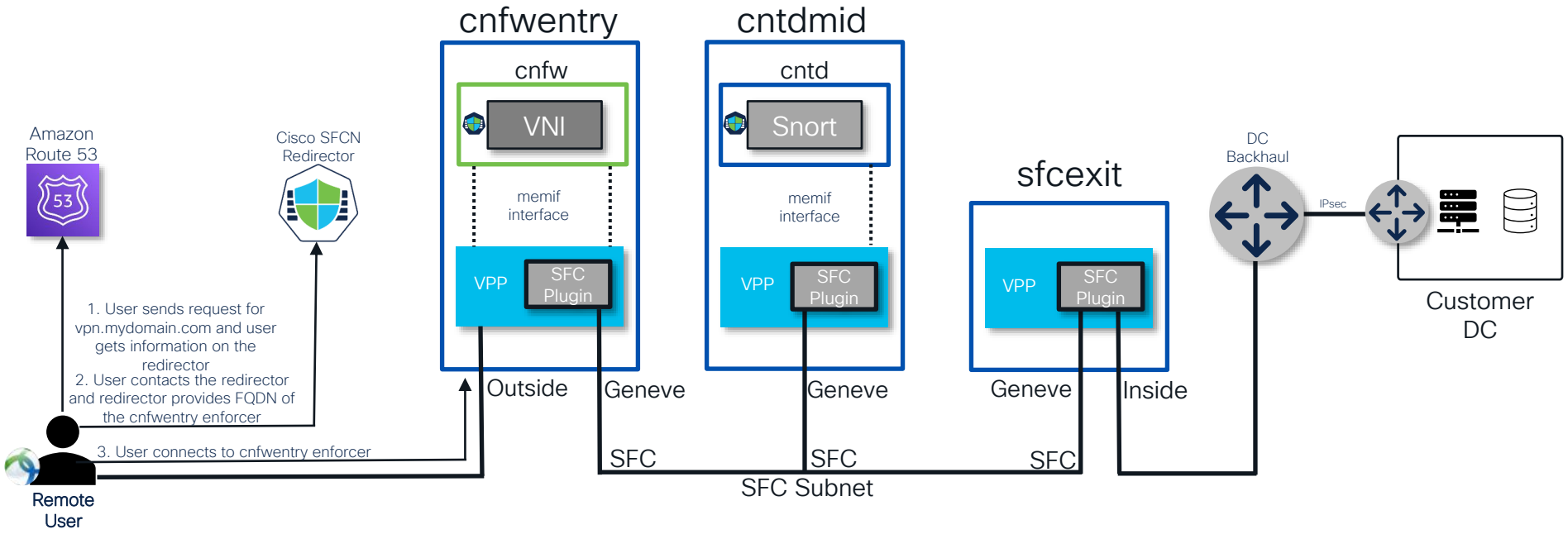
Cisco Secure Firewall Cloud Native
Service Role and Topology

Service Role	Feature
vpnredirector	VPN redirector
cnfwentry	VPN headend
cntdmid	Threat Protection (IDS/IPS, AMP and SI)
sfcexit	SFC exit node

Service Role Combination	Topology
cnfwentry, cntdmid, sfcexit	cnfwentry -> cntdmid -> sfcexit
vpnredirector, cnfwentry, cntdmid, sfcexit	vpnredirector, cnfwentry -> cntdmid -> sfcexit (recommended)

Cisco Secure Firewall Cloud Native Architecture

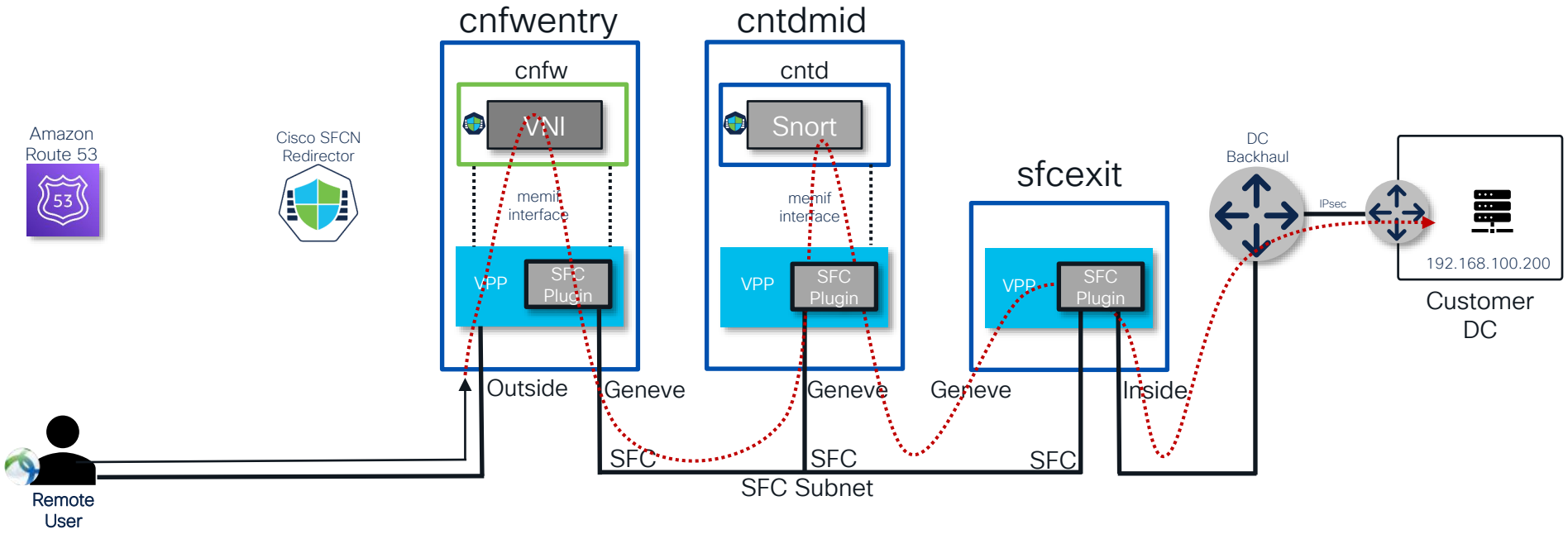
Topology: vpnredirector, cnfwentry -> cntdmid -> sfcexit



Management – API/YAML/CRD, Cisco Defense Orchestrator & CDFMC

Cisco Secure Firewall Cloud Native Architecture

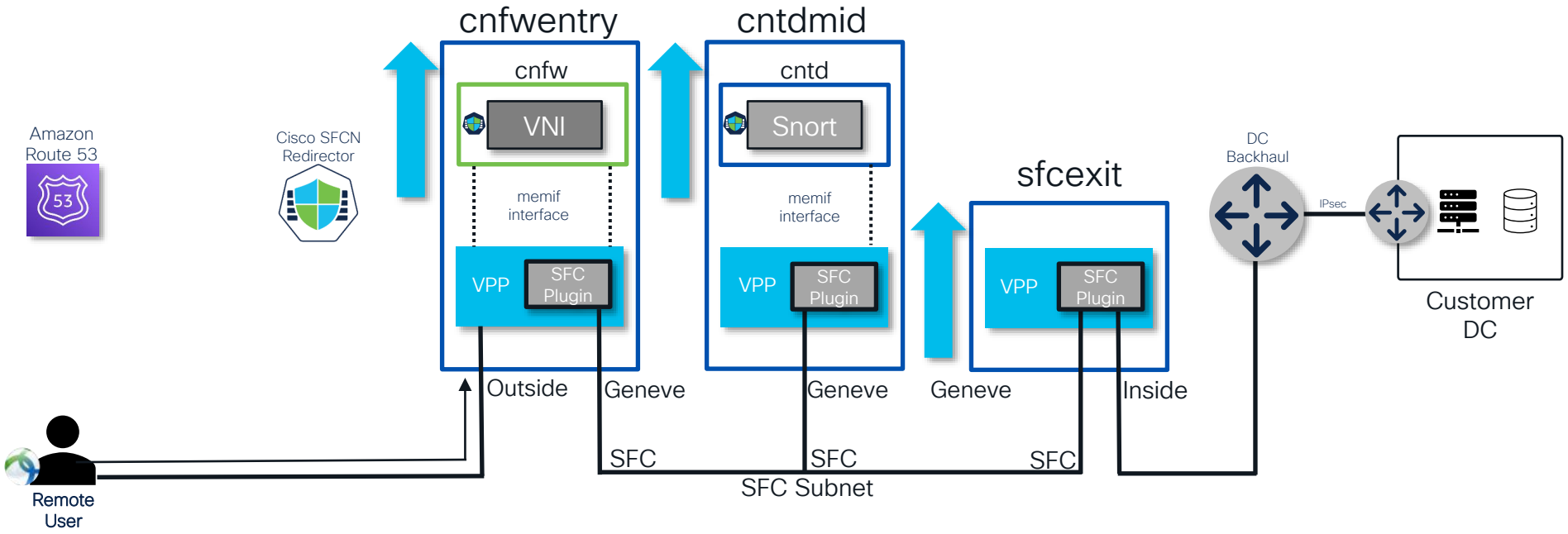
Traffic Flow: vpnredirector, cnfwentry -> cntdmid -> sfcexit



Management – API/YAML/CRD, Cisco Defense Orchestrator & CDFMC

Cisco Secure Firewall Cloud Native Architecture

Scalability: vpnredirector, cnfwentry -> cntdmid -> sfcexit

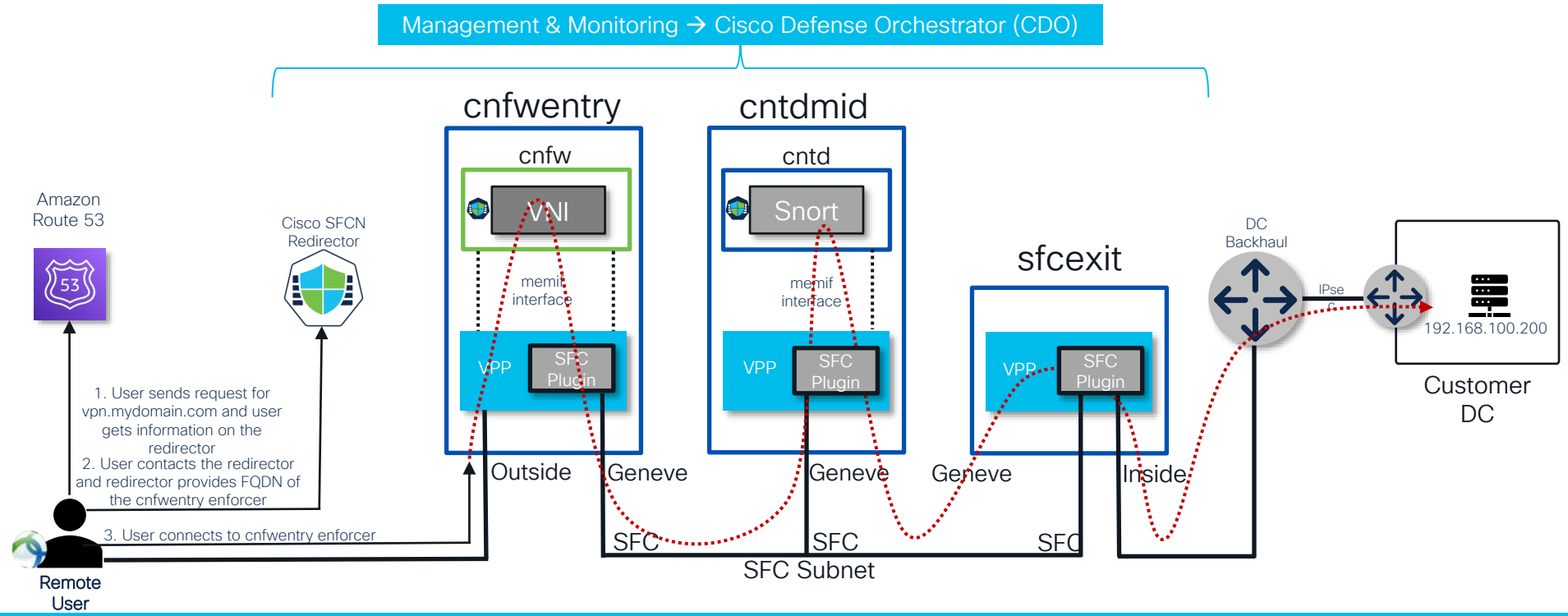


Services can scalable independently using Horizontal Pod Autoscaler

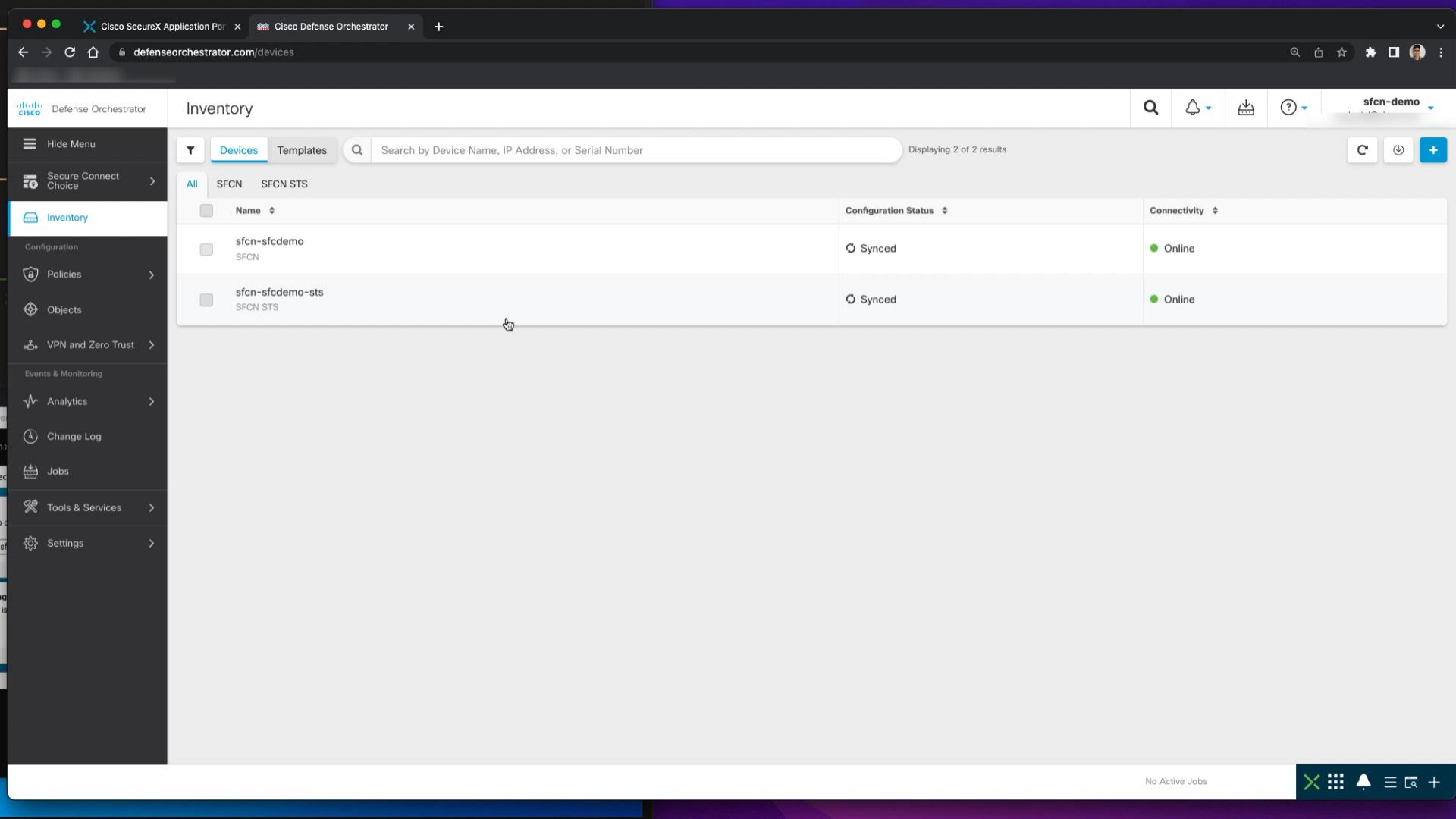
Demo
(Service Function Chaining)

Cisco Secure Firewall Cloud Native Architecture

Traffic Flow: vpnredirector, cnfwentry -> cntdmid -> sfcexit

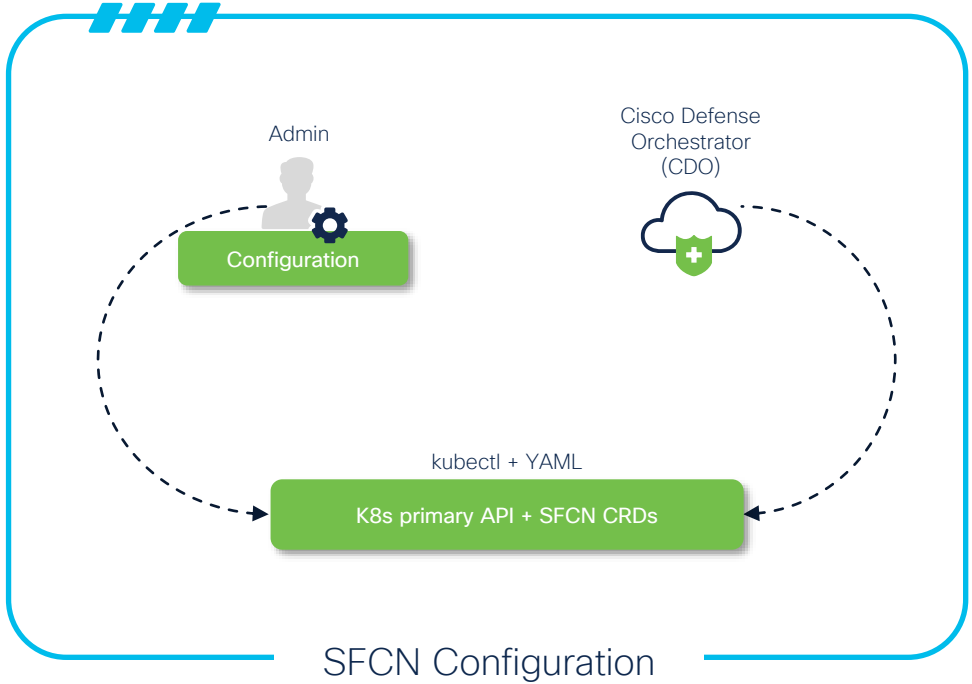


CNFW Management – API/YAML/CRD, Cisco Defense Orchestrator
CNTD Management – API/YAML/CRD, CDO – CDFMC


Cisco SecureX Application Por
Cisco Defense Orchestrator
defenseorchestrator.com/devices
Defense Orchestrator
Inventory
sfcn-demo
Hide Menu
Secure Connect Choice
Inventory
Configuration
Policies
Objects
VPN and Zero Trust
Events & Monitoring
Analytics
Change Log
Jobs
Tools & Services
Settings
Devices
Templates
Search by Device Name, IP Address, or Serial Number
Displaying 2 of 2 results
All
SFCN
SFCN STS
Name
Configuration Status
Connectivity
sfcn-sfcdemo
SFCN
Synced
Online
sfcn-sfcdemo-sts
SFCN STS
Synced
Online
No Active Jobs

Configuration

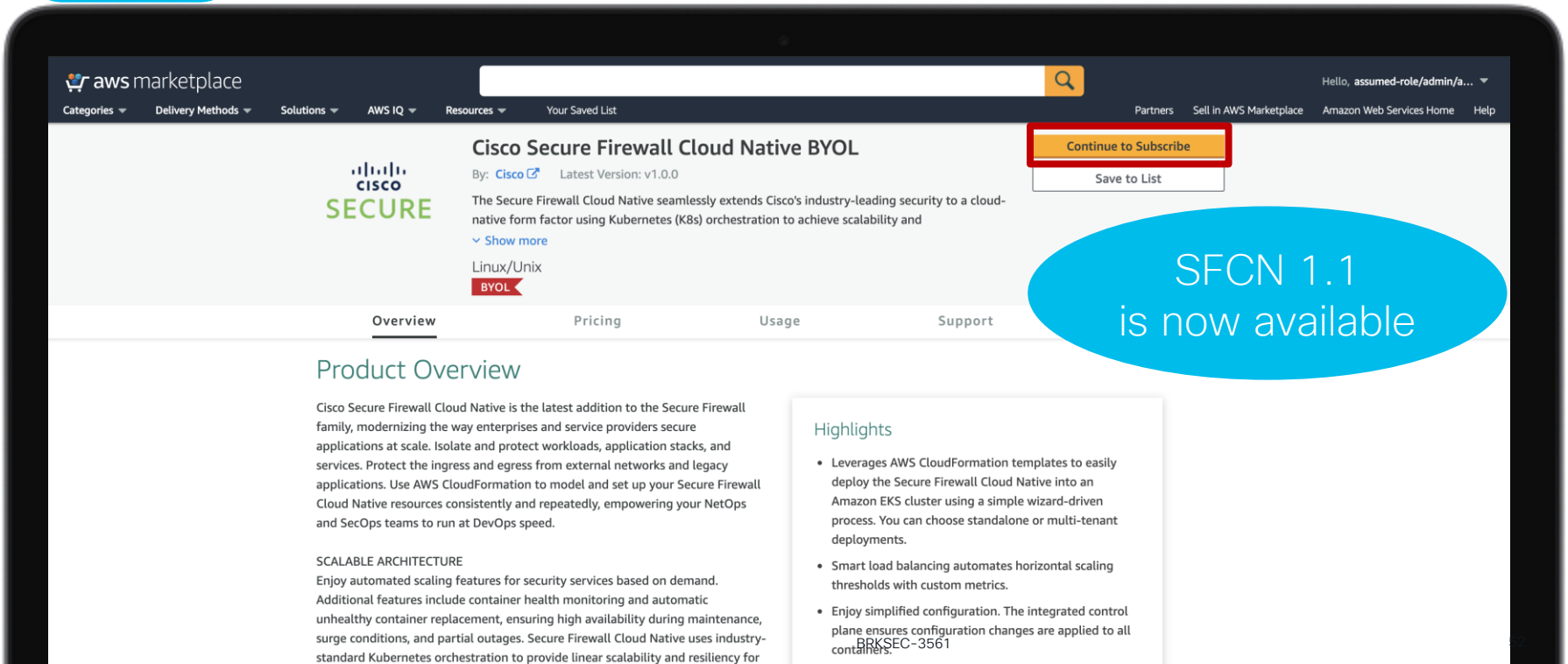
- K8s API + SFCN CRDs
- Cisco Defense Orchestrator



SFCN deployment

Step 1

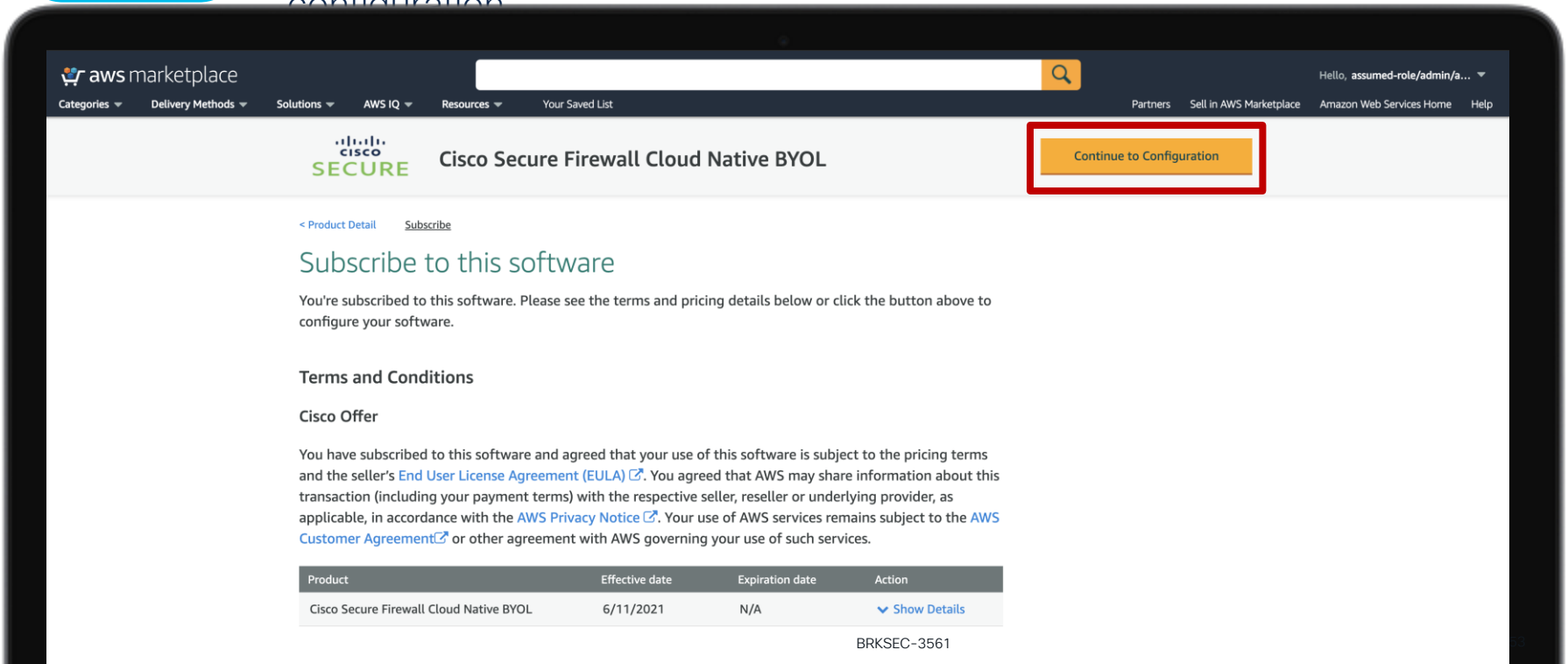
Access the SFCN marketplace listing and click on “continue to subscribe”



SFCN deployment (cont.)

Step 2

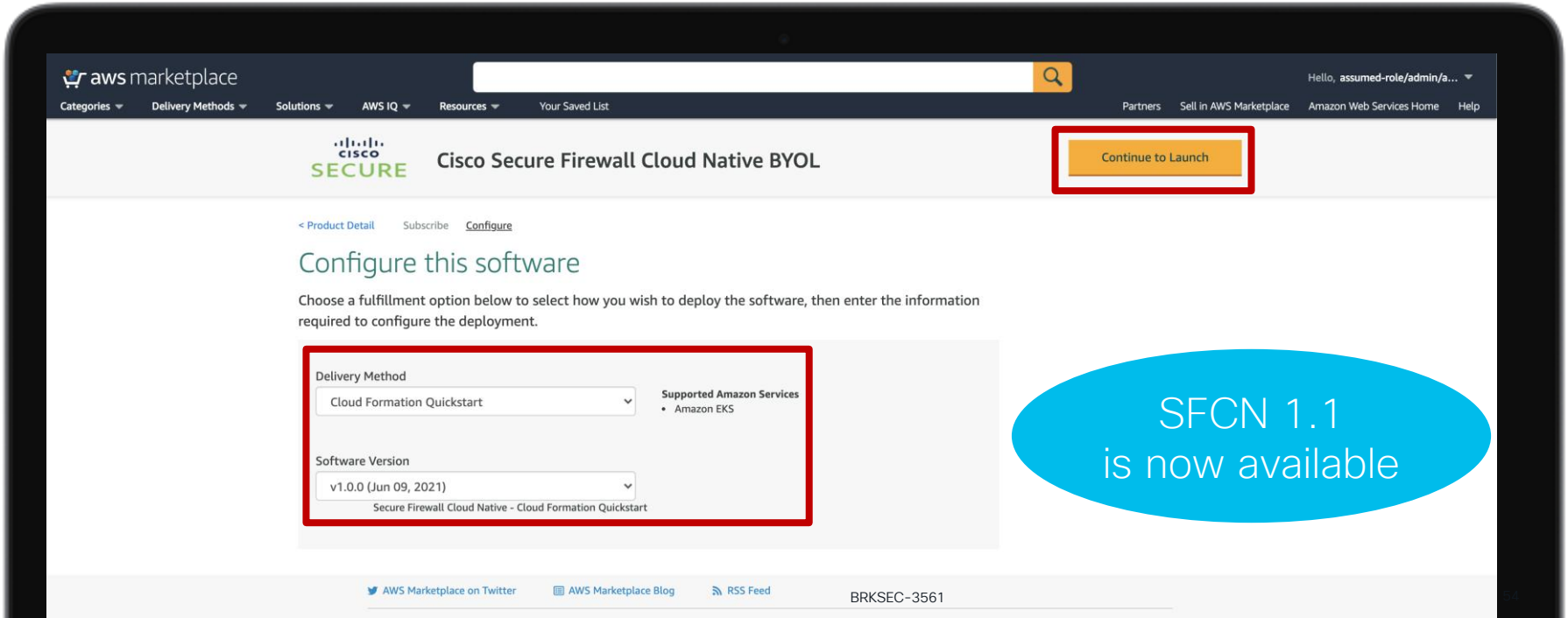
On the Subscribe to this software page, click on “continue to configuration”



SFCN deployment (cont.)

Step 3

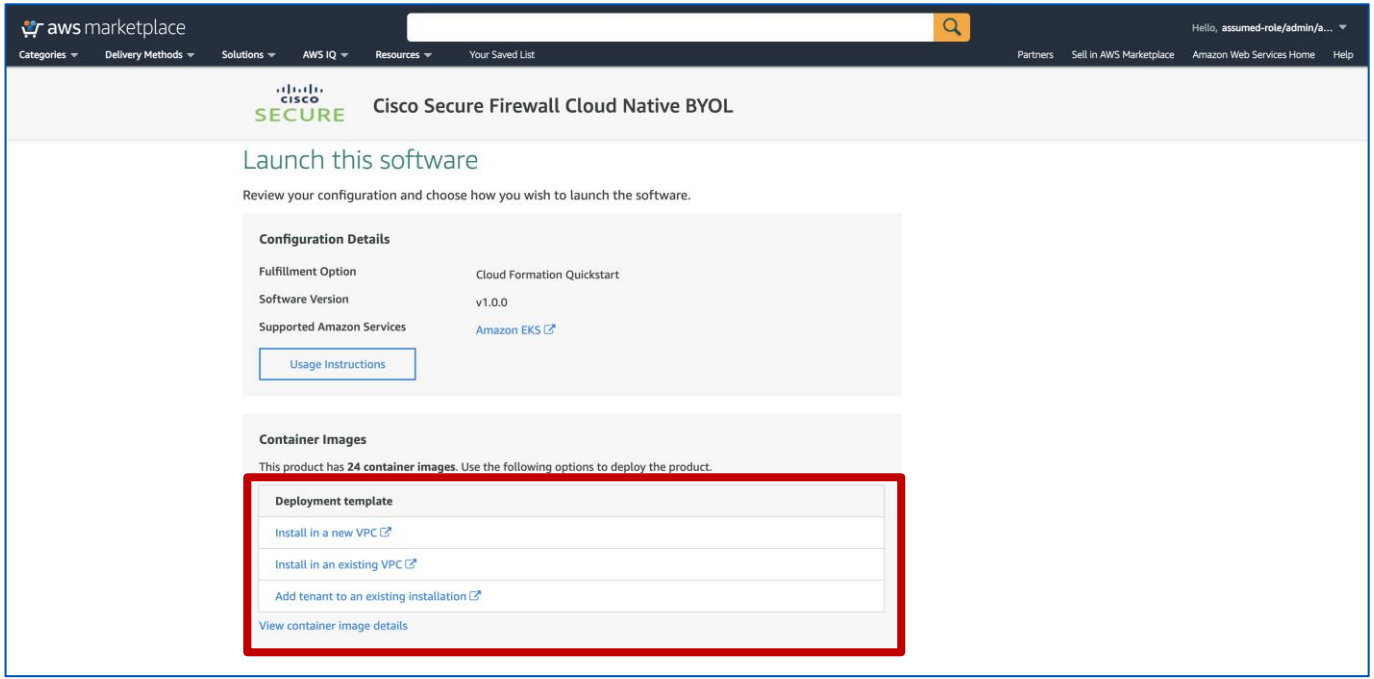
On the Configure this software page, select delivery method as “Cloud Formation Quickstart and then click on “Continue to Launch”



SFCN deployment (cont.)

Step 4

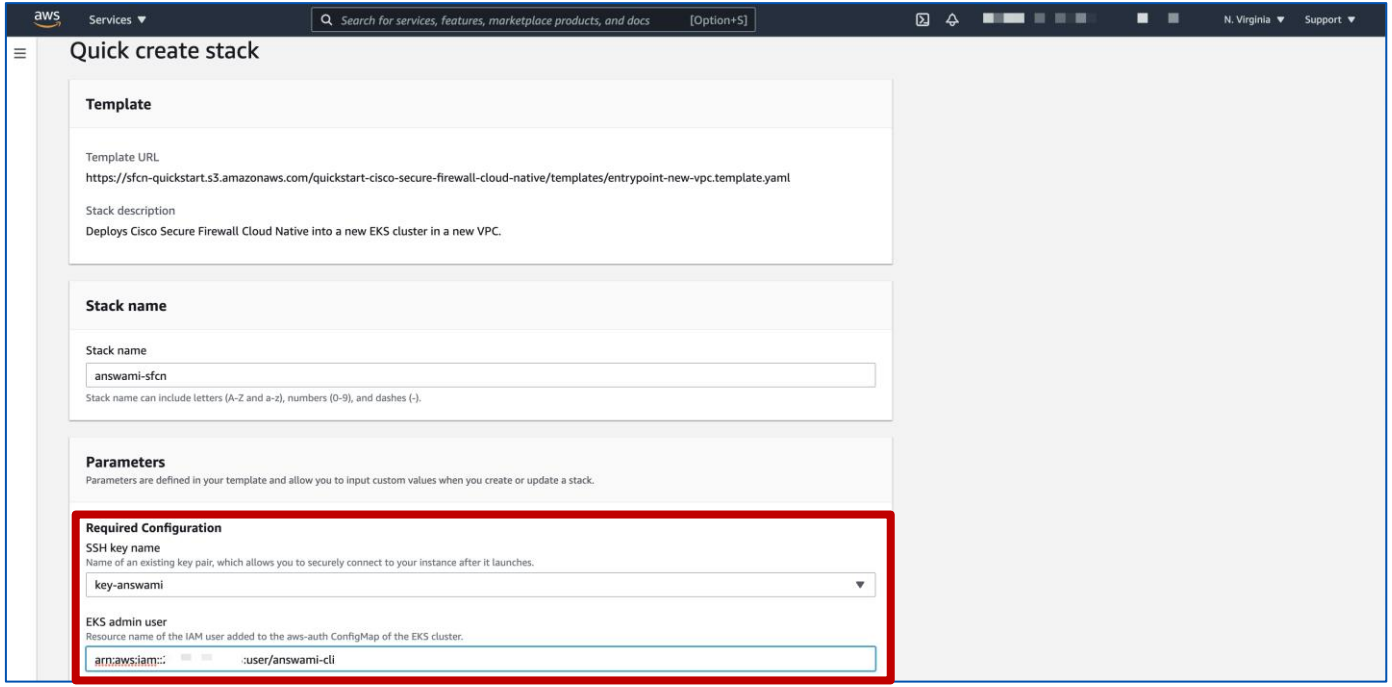
On the Launch this software page, select the deployment template as per your requirement (1. New VPC, 2. Existing VPC and 3. Add Tenant).
For this deployment: Click on Install in a new VPC.



SFCN deployment (cont.)

Step 5

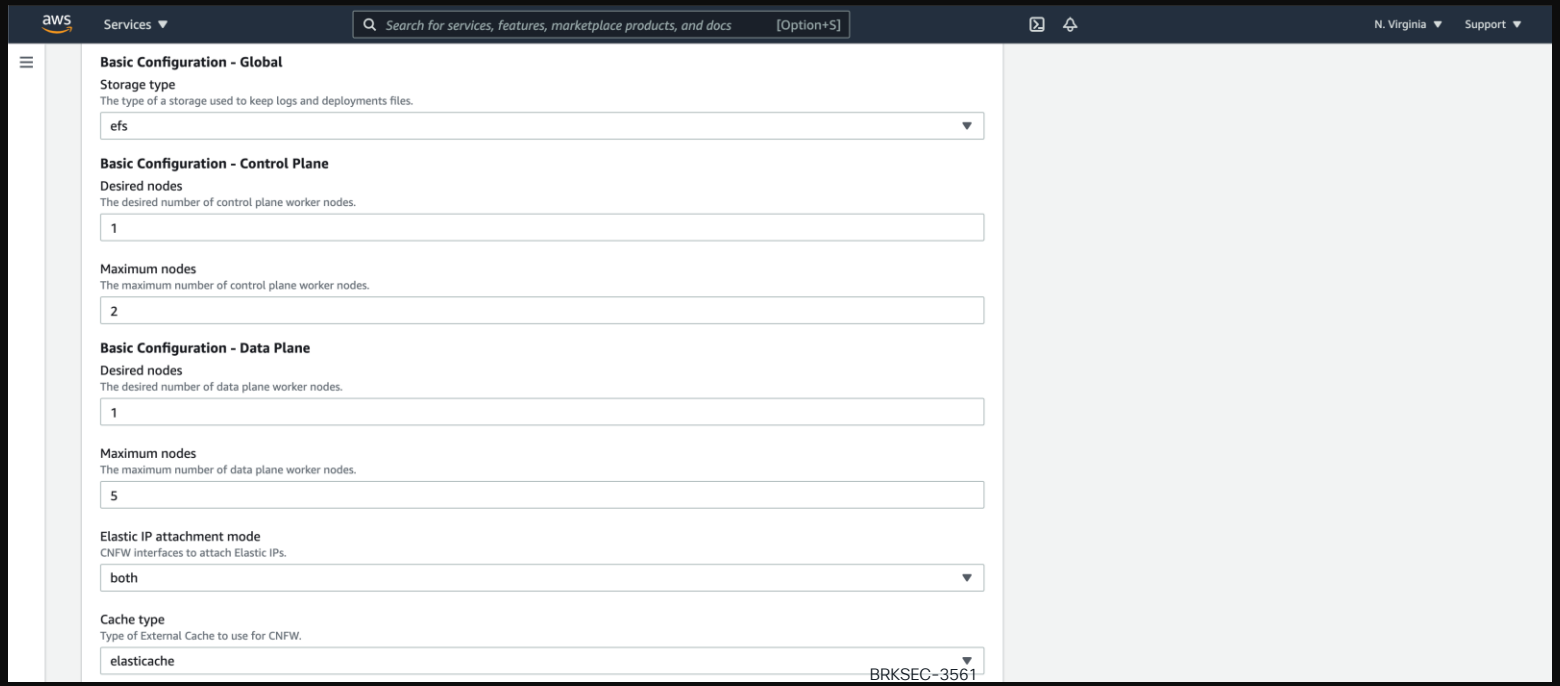
On create stack, add required information like: ssh key, arn for EKS admin user



SFCN deployment (cont.)

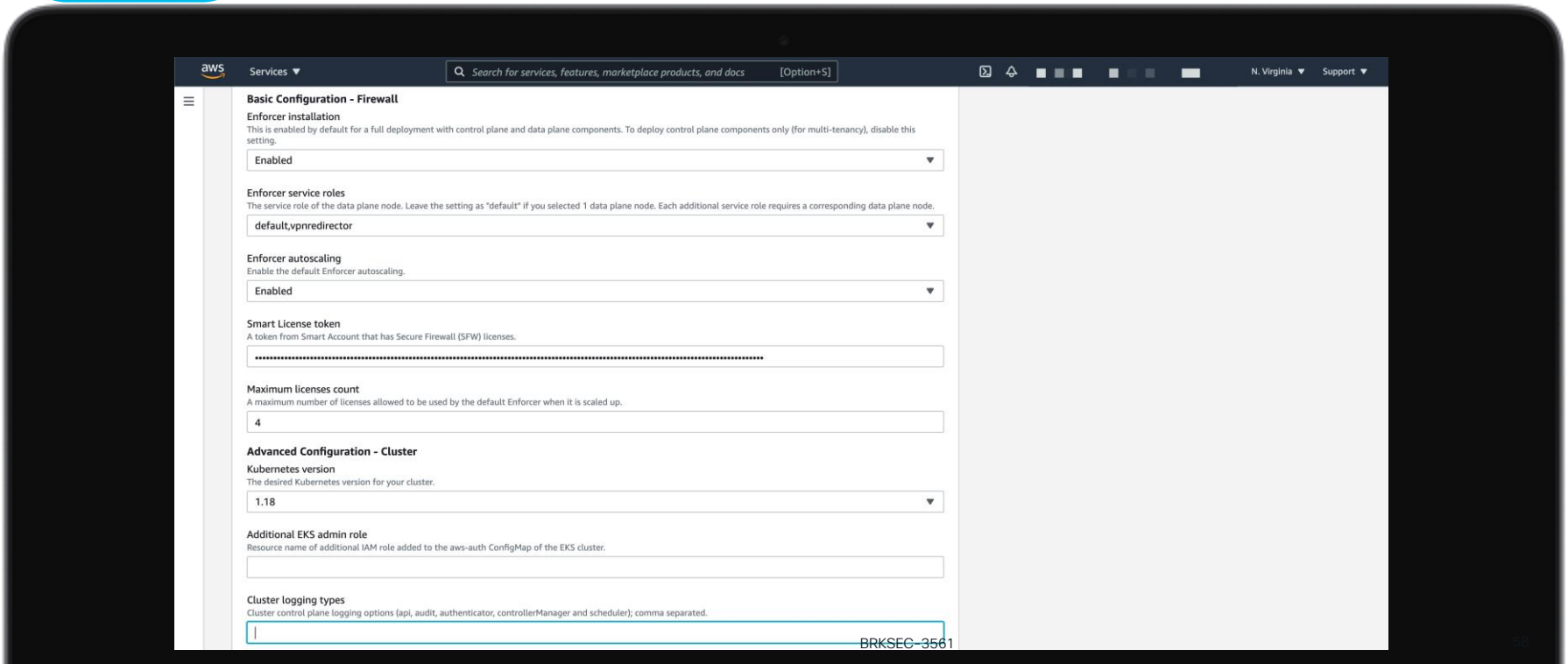
Step 6

Define storage, node information for CP and EP, assign EIP on EP interfaces, enable elasticache



SFCN deployment (cont.)

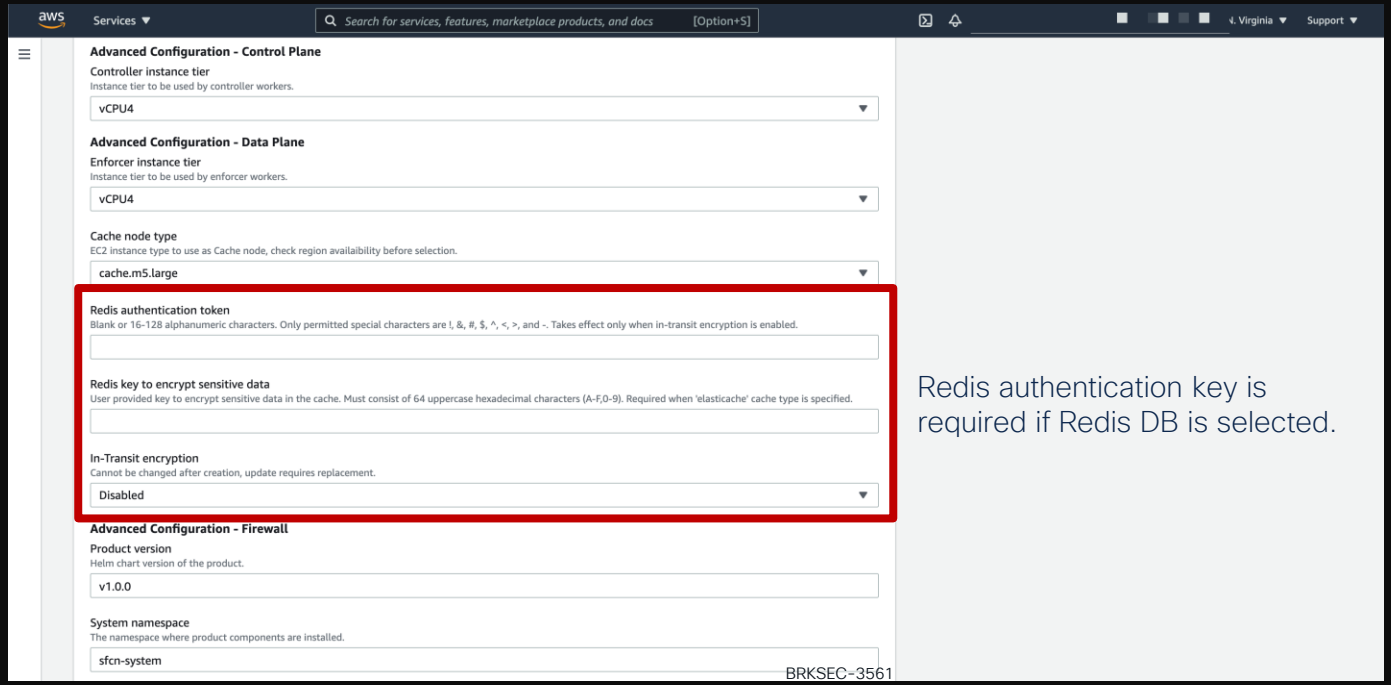
Step 7 Enable redirector role, enable autoscaling, and add a token.



SFCN deployment (cont.)

Step 8

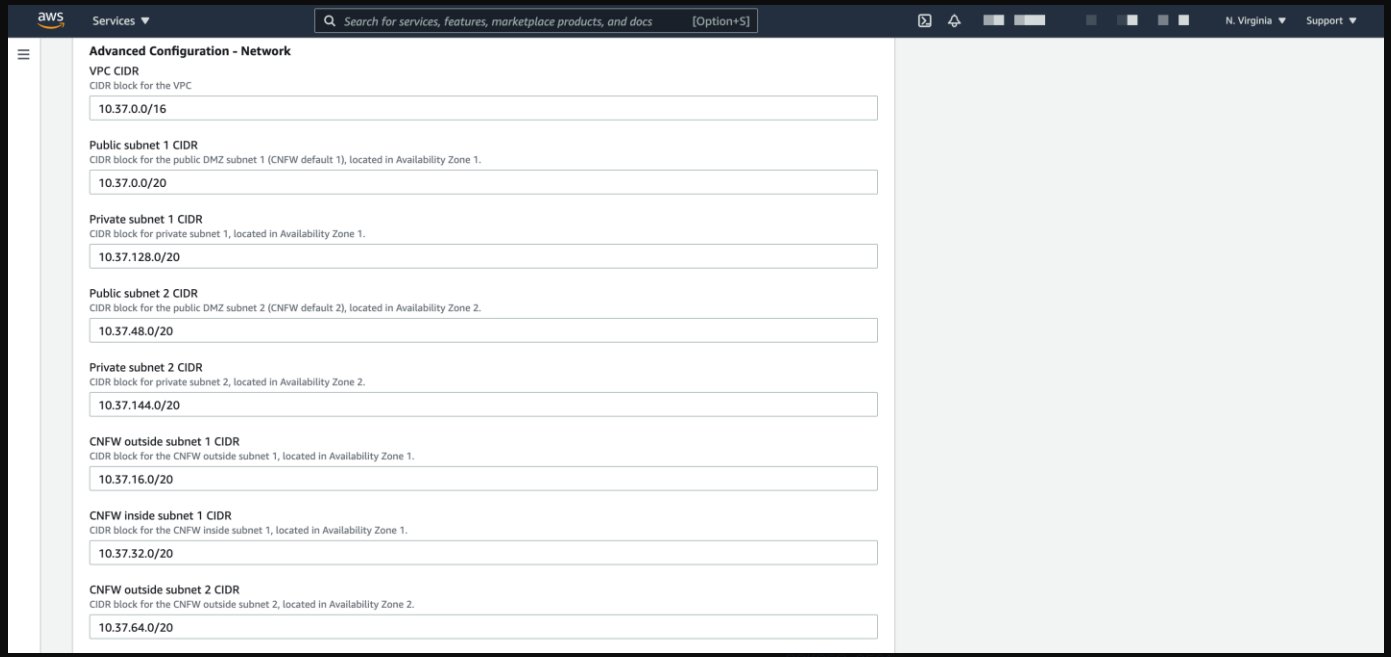
Define advance configuration for CP/EP, define Redis database instance size, and namespace



Redis authentication key is required if Redis DB is selected.

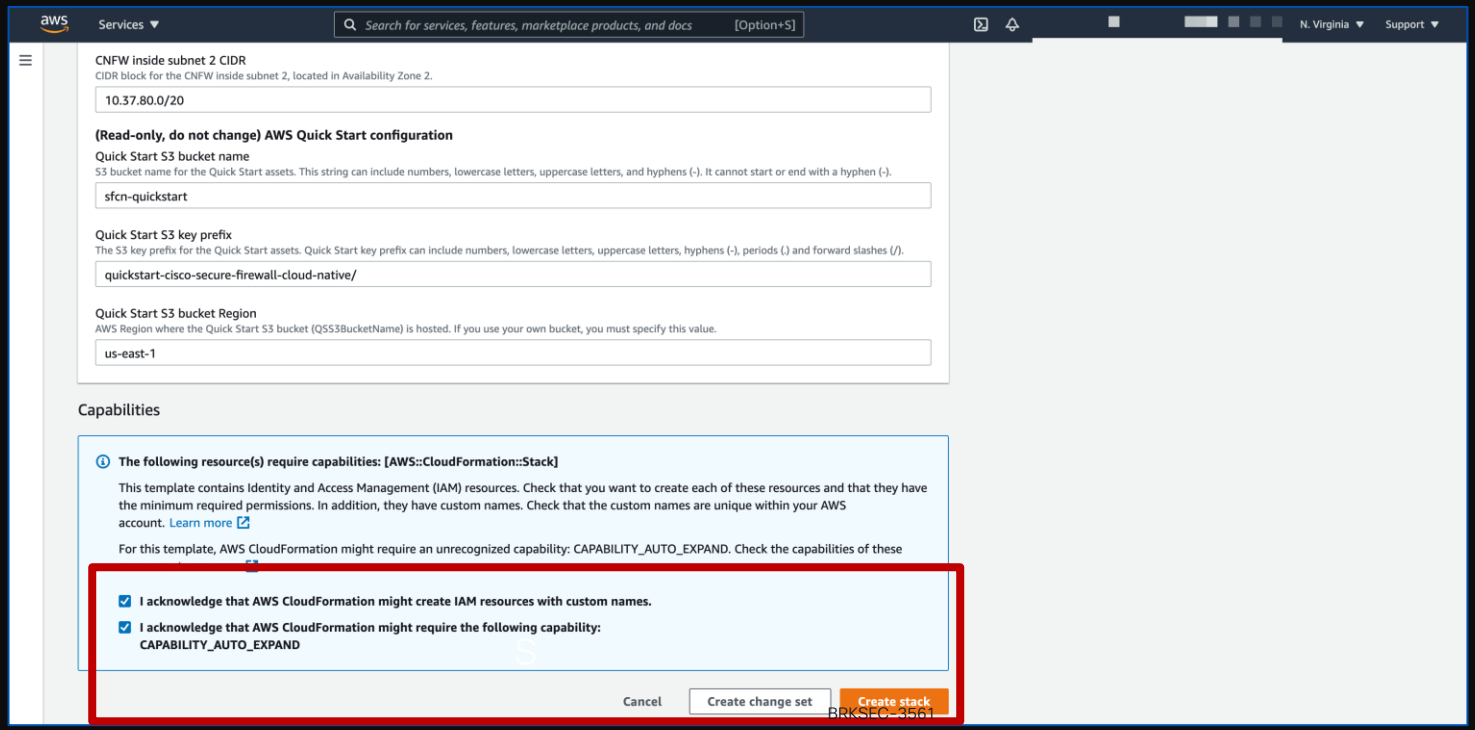
SFCN deployment (cont.)

Step 9 Define advanced network configuration



SFCN deployment (cont.)

Step 10 Check I acknowledge boxes and create stack



Custom Resource Definition
(CRDs)

What are CRDs?

In the Kubernetes API, a resource is an endpoint that stores a collection of API objects of a certain kind.

- For example, the built-in pods' resource contains a collection of Pod objects.
- The standard Kubernetes distribution ships with many inbuilt API objects/resources.
- CRD comes into picture when we want to introduce our own object into the Kubernetes cluster to full fill our requirements. Once we create a CRD in Kubernetes we can use it like any other native Kubernetes object thus leveraging all the features of Kubernetes like its CLI, security, API services, etc.

Route53Ingress

- Adds CNFW interface endpoints as DNS records.
- Spec
  - DNS name
  - Interface Index
  - Service Role
  - Record Type
  - HostedZone
  - Geolocation
- Status
  - Applied Endpoints

```yaml
apiVersion: cnfw.cisco.com/v1
kind: Route53Ingress
metadata:
  finalizers:
    - sfcn.cisco.com/route53ingressreconciler_finalizer
  generation: 2
  name: vpn
  namespace: sfcn-system
spec:
  attributes:
    geolocation: {}
  endpointSelector:
    addressType: public
    interfaceIndex: 2
    serviceRole: default
  hostedZone: Z02384461D5I212LXYZF
  recordSetName: demo.cisco-vpn.com
  recordType: A
  recordUpdate: SUBDOMAIN
status:
  appliedHostedZone: Z02384461D5I212LDUWSP
  appliedRecordSetName: demo.cisco-vpn.com
  endpoints:
    - 54.187.127.167
  pendingPods: []
  recordUpdate: SUBDOMAIN
```

FileObject

- Defines a remote file object to be downloaded and provisioned on the CNFW
- Spec
  - fileName
  - Path to download on
  - AWS S3 config
    - Access keys
    - Bucket
- Status
  - Download status

```yaml
apiVersion: cnfw.cisco.com/v1
kind: FileObject
metadata:
  generation: 1
  name: ravpnprofile
  namespace: sfcn-system
spec:
  fileName: ravpn-profile.xml
  localPath: /
  s3:
    auth:
      accessKeyField: access_key
      secretKeyField: secret_key
      secretName: s3-auth-secret
    bucket: kasavpnshared
    item: ravpn-profile.xml
    region: us-east-1
status:
  conditions:
    - lastTransitionTime: '2022-05-31T01:26:56Z'
      lastUpdateTime: '2022-05-31T01:26:56Z'
      reason: Successful
      status: 'True'
      type: Downloaded
  lastDownloadHash: 055658d4333a00c5c81556e263dd4b66
```

ASAConfiguration

- Defines the ASAConfiguration to deploy onto the CNFW
- Dynamically updates on any referenced dependency updates
- Spec
  - ASA Configuration
  - References to FileObjects, SubentPools, Route53 Records, Secrets
- Status
  - Applied Status

```yaml
apiVersion: cnfw.cisco.com/v1
kind: ASAConfiguration
metadata:
  name: ravpn-enforcer-config
  namespace: sfcn-system
spec:
  order: 1
  cliLines: >
    webvpn
      enable outside
      anyconnect profiles my_AC_profile {{ .fileObjects.ravpnprofile.path }}
      anyconnect image {{ .fileObjects.anyconnectwin.path }} 1
      anyconnect image {{ .fileObjects.anyconnectmac.path }} 2
      anyconnect image {{ .fileObjects.anyconnectlinux.path }} 3
      anyconnect enable
      tunnel-group-list enable
    group-policy VPN_group_policy internal
    domain-name {{ .route53Ingresses.vpn.recordSetName }}
    ...
  description: RA-VPN Configuration
  fileObjects:
    - ravpnprofile
    - anyconnectlinux
    - anyconnectwin
    - anyconnectmac
  ipv4SubnetPools:
    - ravpnpool
  route53Ingresses:
    - vpn
  secrets:
    - userinfo
status:
  conditions:
    - lastTransitionTime: '2022-05-31T01:26:46Z'
      lastUpdateTime: '2022-05-31T01:26:46Z'
      reason: ValidationSuccessful
      status: 'True'
      type: Valid
```

IPv4SubnetPool

- A pool of IPv4 subnets that can be used for configuration in CLI of ASAConfiguration CRD
- Also sets up reverse routes for traffic returning from Data Center
- Spec
  - Address pool config
- Status
  - Assigned Pools (for ASAc)
  - Reverse Route status

```yaml
apiVersion: cnfw.cisco.com/v1
kind: IPv4SubnetPool
metadata:
  annotations:
    aws.cnfw.cisco.com/interface-index: '3'
    aws.cnfw.cisco.com/route-table-id: rtb-0286c00532732c282
    aws.cnfw.cisco.com/type: route-table
  finalizers:
    - sfcn.cisco.com/ipv4subnetpoolreconciler_finalizer
  generation: 1
  name: ravpnpool
  namespace: sfcn-system
  resourceVersion: '51894'
  uid: 4d2b152e-f788-4669-a7ed-76221ffd9c85
  selfLink: /apis/cnfw.cisco.com/v1/namespaces/sfcn-system/ipv4subnetpools/ravpnpool
spec:
  address: 10.10.0.0
  rangeStart: 1
  subnetPrefix: 24
  supernetPrefix: 16
status:
  assigned:
    - ip-10-37-11-14.us-west-2.compute.internal/10.10.1.0/24
    - ip-10-37-58-96.us-west-2.compute.internal/10.10.0.0/24
  observedAWSRouteTableState:
    interfaceIndex: 3
    routeTableId: rtb-0286c00532732c282
  observedGeneration: 1
  summary: 'PoolSize: 256, Number of hosts: 254, Assigned: 2, Unassigned: 0'
```

Counters

- Counter CRD is used to define a range of numeric values that can be used for configuration in CLI of ASAConfiguration CRD
- Spec
  - Start count
  - Range

```yaml
apiVersion: cnfw.cisco.com/v1
kind: Counter
metadata:
  name: sample
spec:
  start: 3
  allocatedPerNode: 2
---
apiVersion: cnfw.cisco.com/v1
kind: ASAConfiguration
metadata:
  name: networks
spec:
  order: 1
  counters:
    - sample
  cliLines: |
    {{range .counters.sample}}
      object network n{{.}}
        host 8.8.3.{{.}}
    {{end}}
---
```

for 3 nodes will be rendered to different values among them

node-1

```
object network n3
  host 8.8.3.3
object network n4
  host 8.8.3.4
object-group network test
  group-object n3
  group-object n4
```

node-2

```
object network n5
  host 8.8.3.5
object network n6
  host 8.8.3.6
object-group network test
  group-object n5
  group-object n6
```

node-3

```
object network n7
  host 8.8.3.7
object network n8
  host 8.8.3.8
object-group network test
  group-object n7
  group-object n8
```

Ipv4AddressPool

- Defines a Pool of IP addresses to be used in ASAconfiguration
- Spec
  - Subnet
  - Netmask Prefix
- Status
  - Assigned IPV4 Addresses

```yaml
apiVersion: cnfw.cisco.com/v1
kind: IPv4AddressPool
metadata:
  name: ipv4addresspoolsample
  namespace: default
status:
  observedGeneration: 1
  summary: 'PoolSize: 256, Assigned: 0, Unassigned: 0'
spec:
  address: 10.20.30.0
  networkPrefix: 24
---
apiVersion: cnfw.cisco.com/v1
kind: ASAConfiguration
metadata:
  name: asaconfiguration-sample
spec:
  order: 1
  description: "example configuration"
  ipv4AddressPools:
    - "ipv4addresspool1"
    - "ipv4addresspool2"
  ipv4SubnetPools:
    - "ipv4subnetpool1"
    - "ipv4subnetpool2"
  cliLines:
    interface GigabitEthernet0/0
      nameif testinf
    ip address {{.ipv4AddressPools.ipv4addresspool1.assignedIP}} 255.255.255.0
    exit
    object network asac
      host 8.8.8.{{next "counter1"}}
    dhcpd address {{.ipv4SubnetPools.ipv4subnetpool2.assignedRange}} inside
```

Deployment & Configuration

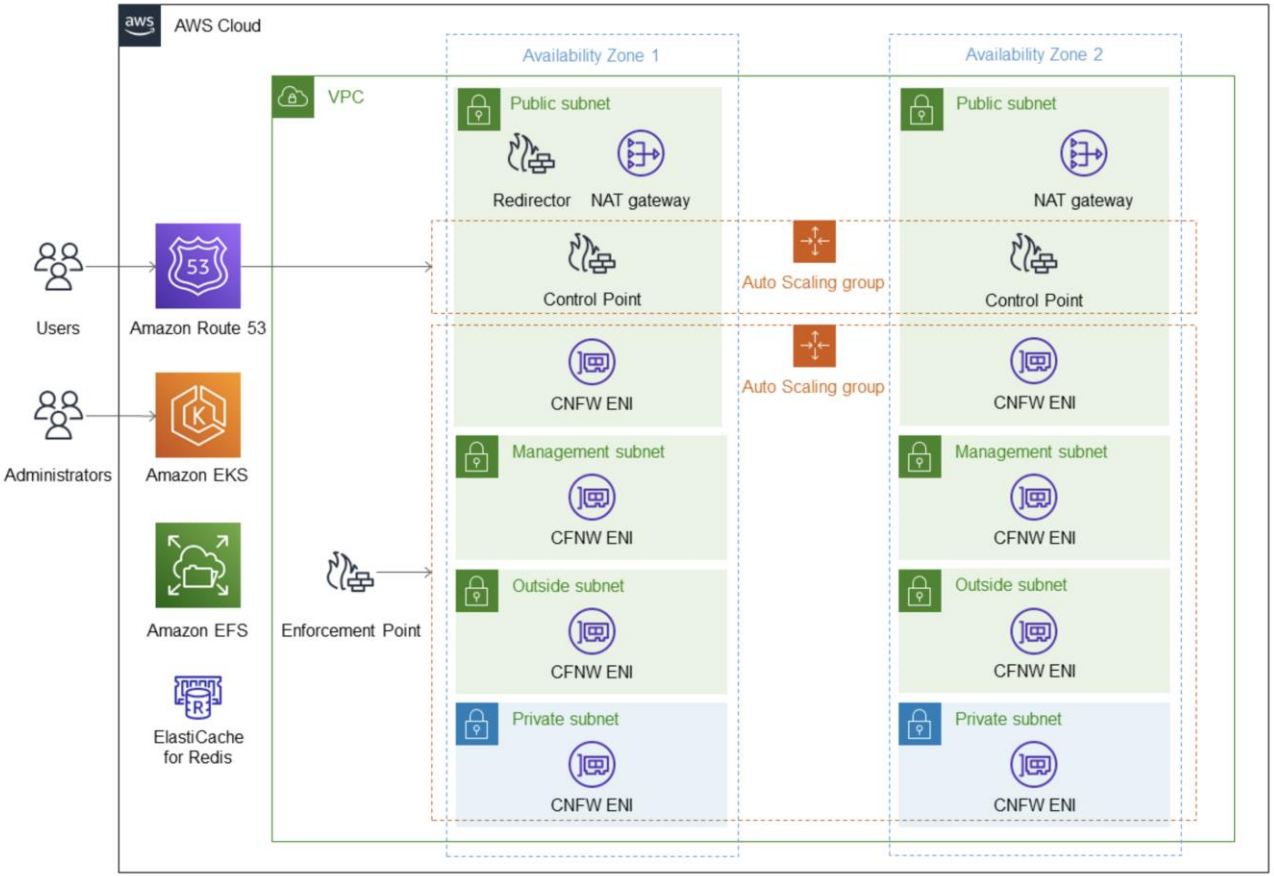
Cisco Secure Firewall Cloud Native

Deployment

- Cisco Secure Firewall Cloud Native (SFCN) is available in Amazon marketplace http://cs.co/SFCN-aws-listing
- SFCN Quick Start supports the following SFCN deployment models:
  - Install in a new VPC
  - Install in an existing VPC
  - Add tenant to an existing installation
- SCFN CFT builds the following component and makes deployment easy
  - Base infrastructure (VPC, Subnet, IGW, RT, EFS, SG)
  - EKS cluster (EP, CP, Worker Nodes and SFCN configuration)
  - SFCN redirector and Amazon ElastiCache (Redis DB)
  - Amazon Route 53 and Hosted Zone
- SFCN deploys enforcement node that covers CNFW (L4) security and VPN
- Management, configuration and monitoring
  - kubectl + YAML
  - Cisco Defense Orchestrator (CDO)
- SFCN cluster can be on-boarded in CDO
- CDO provides UI for management and monitoring SFCN cluster

AWS Quick Start

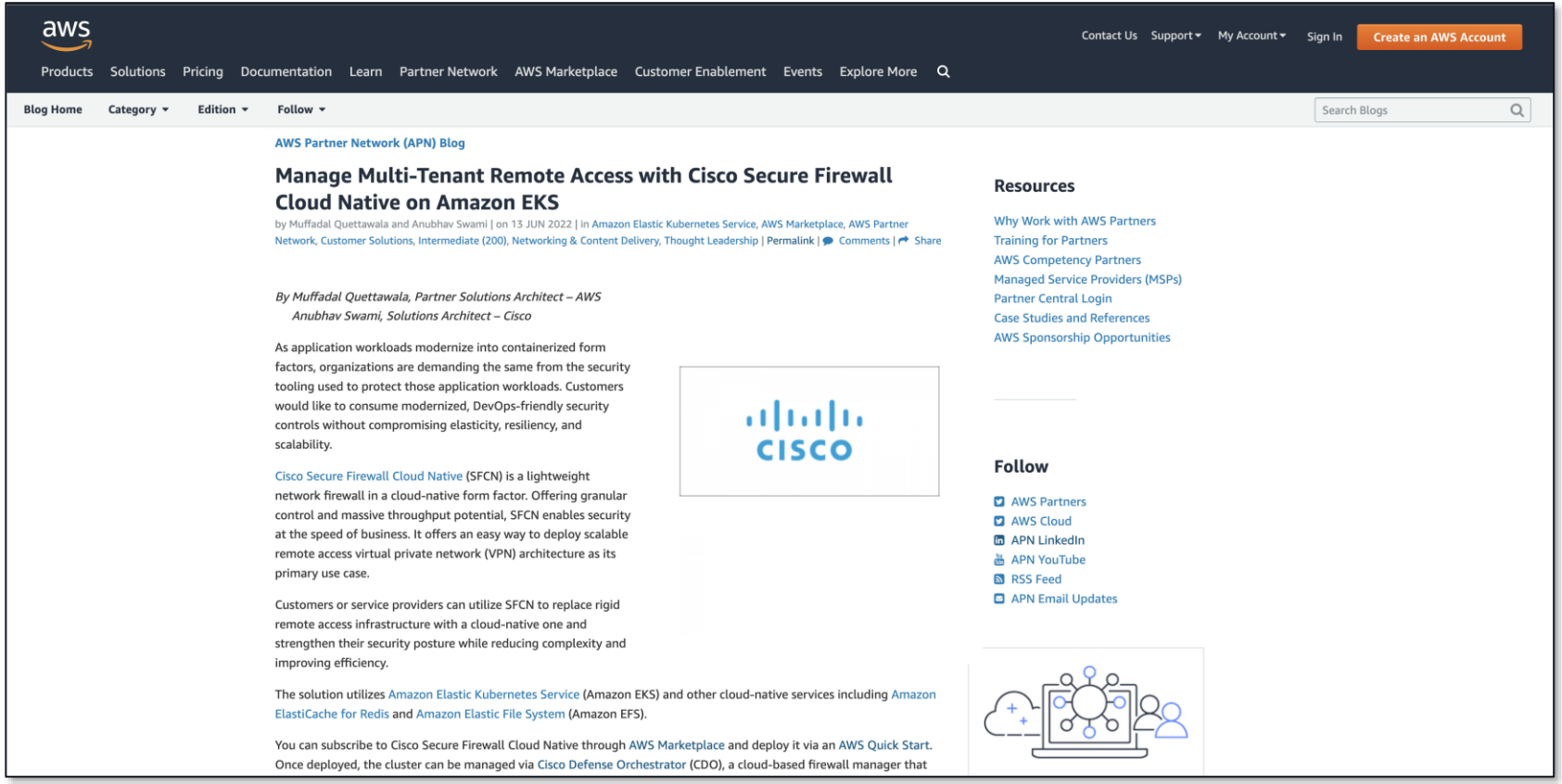
Cisco Secure Firewall Cloud Native AWS Quick Start



SFCN Quick Start: https://aws.amazon.com/quickstart/architecture/cisco-secure-firewall-cloud-native/

Cisco Secure Firewall on Amazon Partner Network (APN)

APN blog post: https://aws.amazon.com/blogs/apn/manage-multi-tenant-remote-access-with-cisco-secure-firewall-cloud-native-on-amazon-eks/



aws

Contact Us | Support | My Account | Sign In | Create an AWS Account

Products | Solutions | Pricing | Documentation | Learn | Partner Network | AWS Marketplace | Customer Enablement | Events | Explore More

Blog Home | Category | Edition | Follow | Search Blogs

AWS Partner Network (APN) Blog

Manage Multi-Tenant Remote Access with Cisco Secure Firewall Cloud Native on Amazon EKS

by Muffadal Quettawala and Anubhav Swami | on 13 JUN 2022 | in Amazon Elastic Kubernetes Service, AWS Marketplace, AWS Partner Network, Customer Solutions, Intermediate (200), Networking & Content Delivery, Thought Leadership | Permalink | Comments | Share

By Muffadal Quettawala, Partner Solutions Architect – AWS
Anubhav Swami, Solutions Architect – Cisco

As application workloads modernize into containerized form factors, organizations are demanding the same from the security tooling used to protect those application workloads. Customers would like to consume modernized, DevOps-friendly security controls without compromising elasticity, resiliency, and scalability.

Cisco Secure Firewall Cloud Native (SFCN) is a lightweight network firewall in a cloud-native form factor. Offering granular control and massive throughput potential, SFCN enables security at the speed of business. It offers an easy way to deploy scalable remote access virtual private network (VPN) architecture as its primary use case.

Customers or service providers can utilize SFCN to replace rigid remote access infrastructure with a cloud-native one and strengthen their security posture while reducing complexity and improving efficiency.

The solution utilizes Amazon Elastic Kubernetes Service (Amazon EKS) and other cloud-native services including Amazon ElastiCache for Redis and Amazon Elastic File System (Amazon EFS).

You can subscribe to Cisco Secure Firewall Cloud Native through AWS Marketplace and deploy it via an AWS Quick Start. Once deployed, the cluster can be managed via Cisco Defense Orchestrator (CDO), a cloud-based firewall manager that

Resources

Why Work with AWS Partners
Training for Partners
AWS Competency Partners
Managed Service Providers (MSPs)
Partner Central Login
Case Studies and References
AWS Sponsorship Opportunities

Follow

AWS Partners
AWS Cloud
APN LinkedIn
APN YouTube
RSS Feed
APN Email Updates

Additional Resources

- SFCN CCO page: http://cs.co/SFCN
- SFCN getting started guide: http://cs.co/SFCN-getting-started
- SFCN At-a-Glance: http://cs.co/SFCN-at-a-glance
- Cisco blog on SFCN
  - Technical Blog: http://cs.co/SFCN-blog
  - Business Blog: http://cs.co/SFCN-business-blog
  - APN Blog: APN blog
- SFCN Marketplace Listing: http://cs.co/SFCN-aws-listing
- SFCN GitHub: https://github.com/CiscoDevNet/sfcn
- SFCN datasheet: http://cs.co/SFCN-data-sheet
- SFCN YouTube Playlist: http://cs.co/SFCN-YT
- SFCN Quick Start: Quick Start

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Secure | Security Reference Architecture

Talos — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt: Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- ISE TrustSec
- Cisco DNA Center
- Secure Web Appliance

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Thank you


cisco Live!
ALL IN