

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

# Cisco Secure Firewall Cloud Native on AWS

Anubhav Swami, Principal Architect  
@swamianubhav  
BRKSEC-3561

CISCO *Live!*

#CiscoLive

# Cisco Webex App

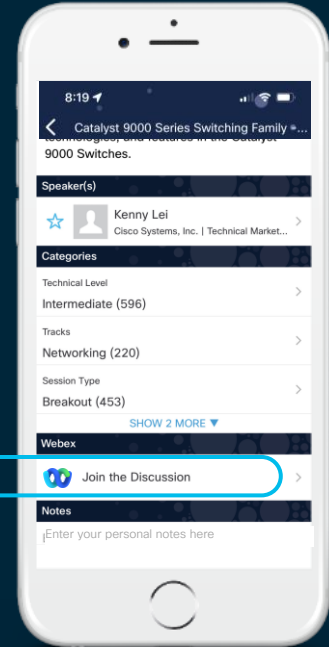
## Questions?

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

## How

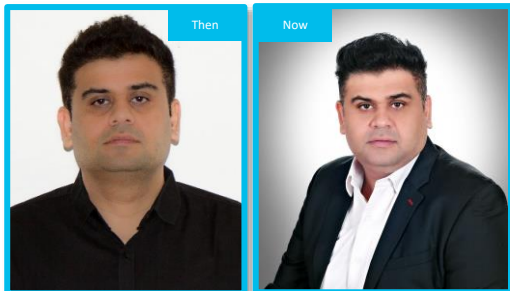
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

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



<https://cicolive.ciscoevents.com/cicolivebot/#BRKSEC-3561>

# Speaker



**Anubhav Swami**  
Principal Architect  
CCIE# 21208

 [answami@cisco.com](mailto:answami@cisco.com)

 <http://cs.co/anubhavswami>

 [www.linkedin.com/in/anubhavswami/](http://www.linkedin.com/in/anubhavswami/)



**Microsoft**  
Specialist  
Implementing Microsoft  
Azure Infrastructure  
Solutions

**CISCO** *Live!*

## 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



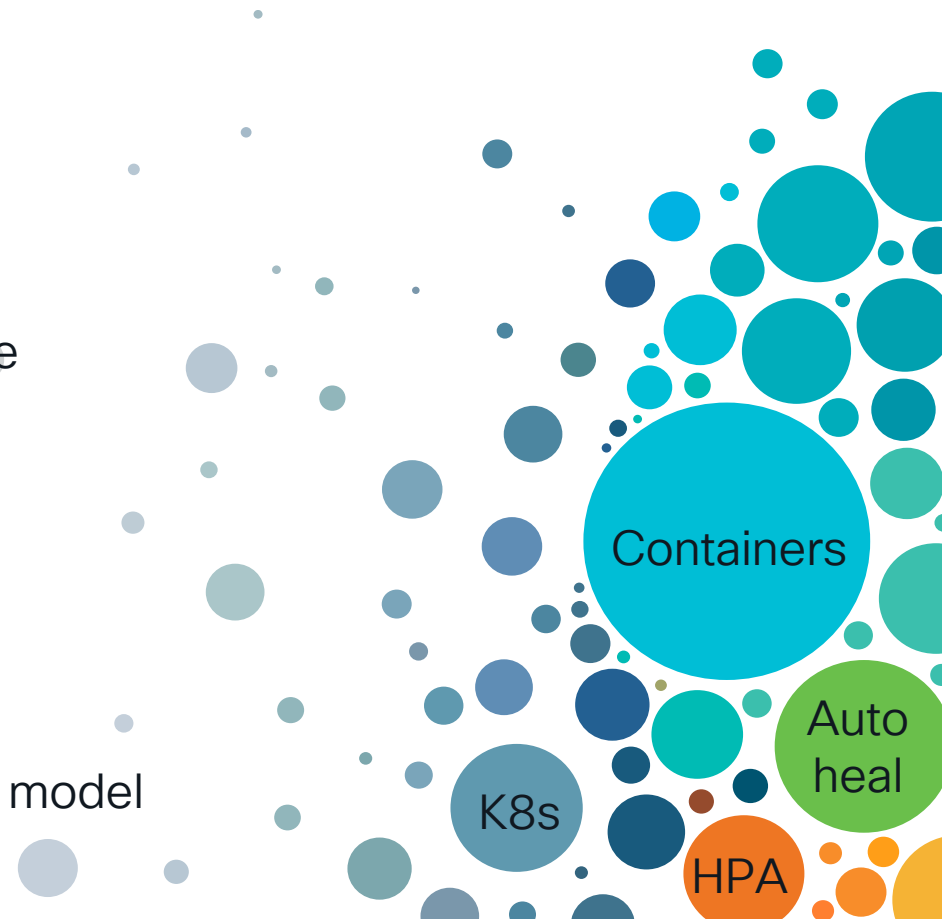
Faster automated bootstrapping



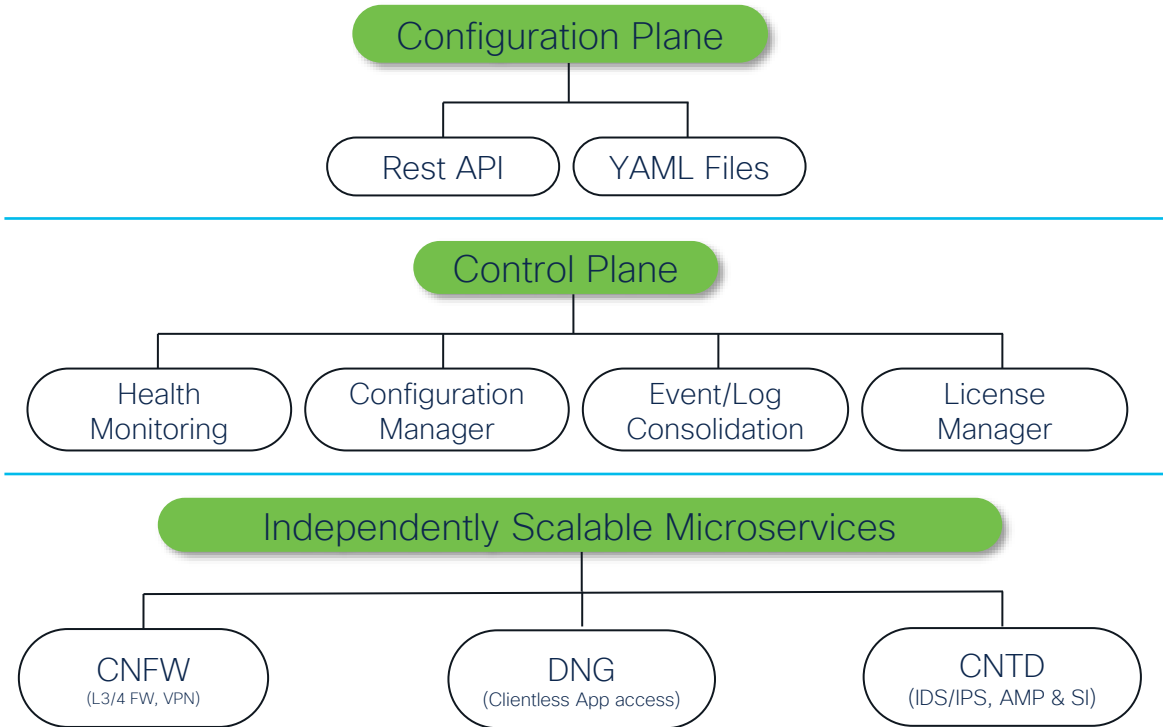
Faster recovery and healing



Infrastructure as Code & DevOps model



# Cisco Secure Firewall Cloud Native Architecture

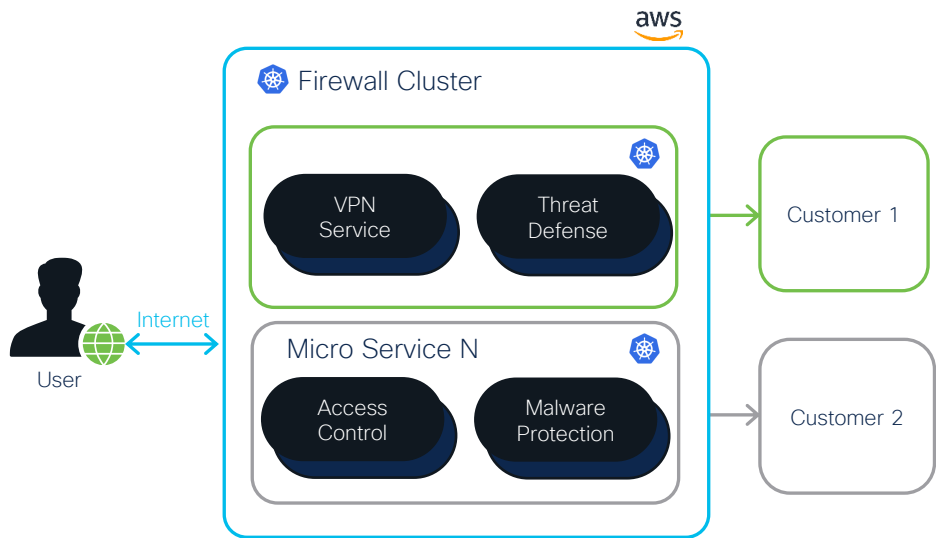


- Independent microservices
- Independent scalability and resiliency
- Control Plane for policy abstraction
- Programmability using Rest API/YAML

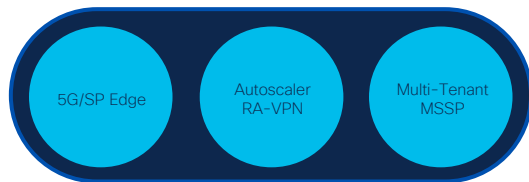
## Target Customer

- 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

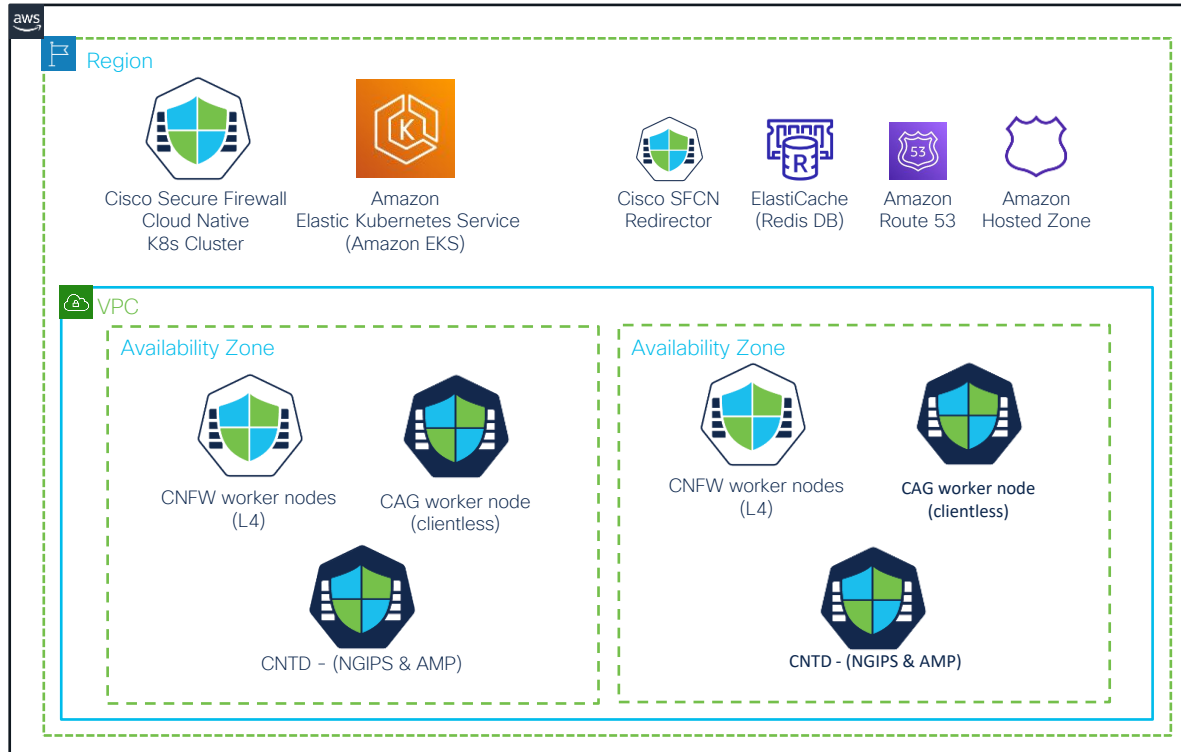


# Architecture



# Cisco Secure Firewall Cloud Native

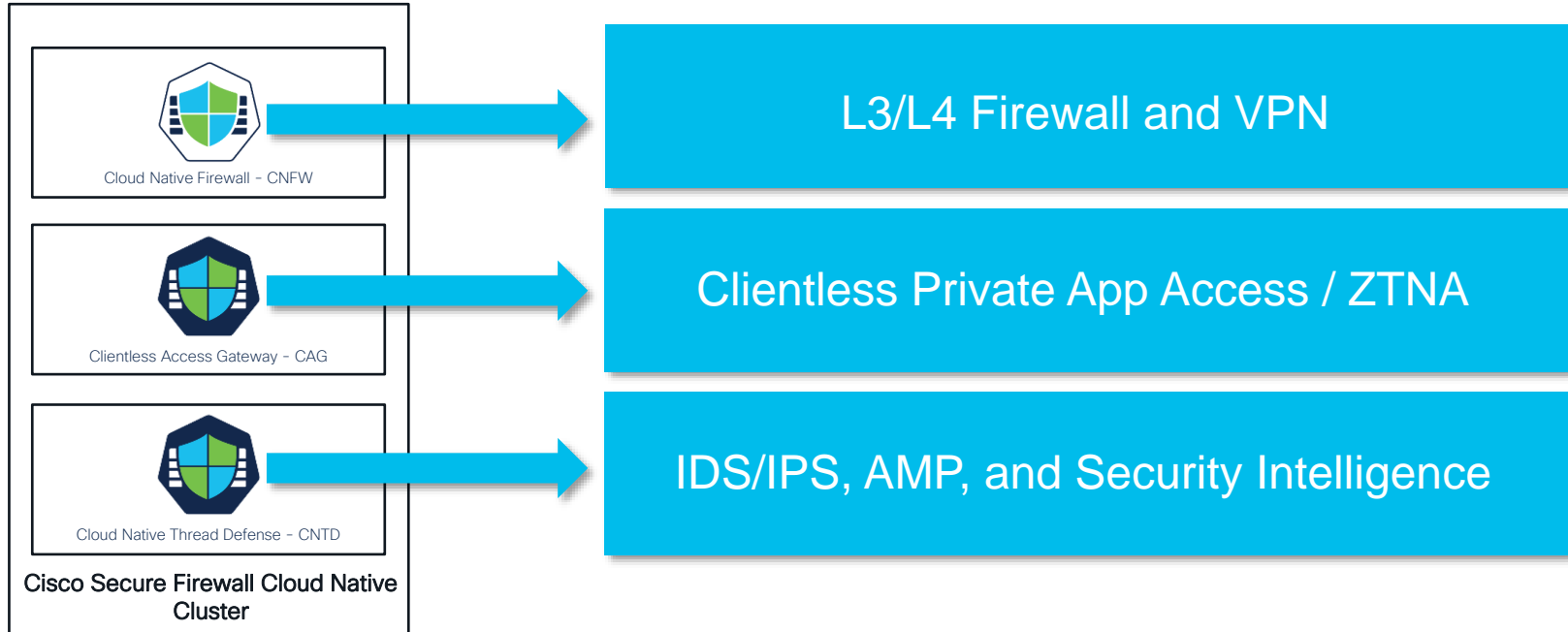
## Building Blocks



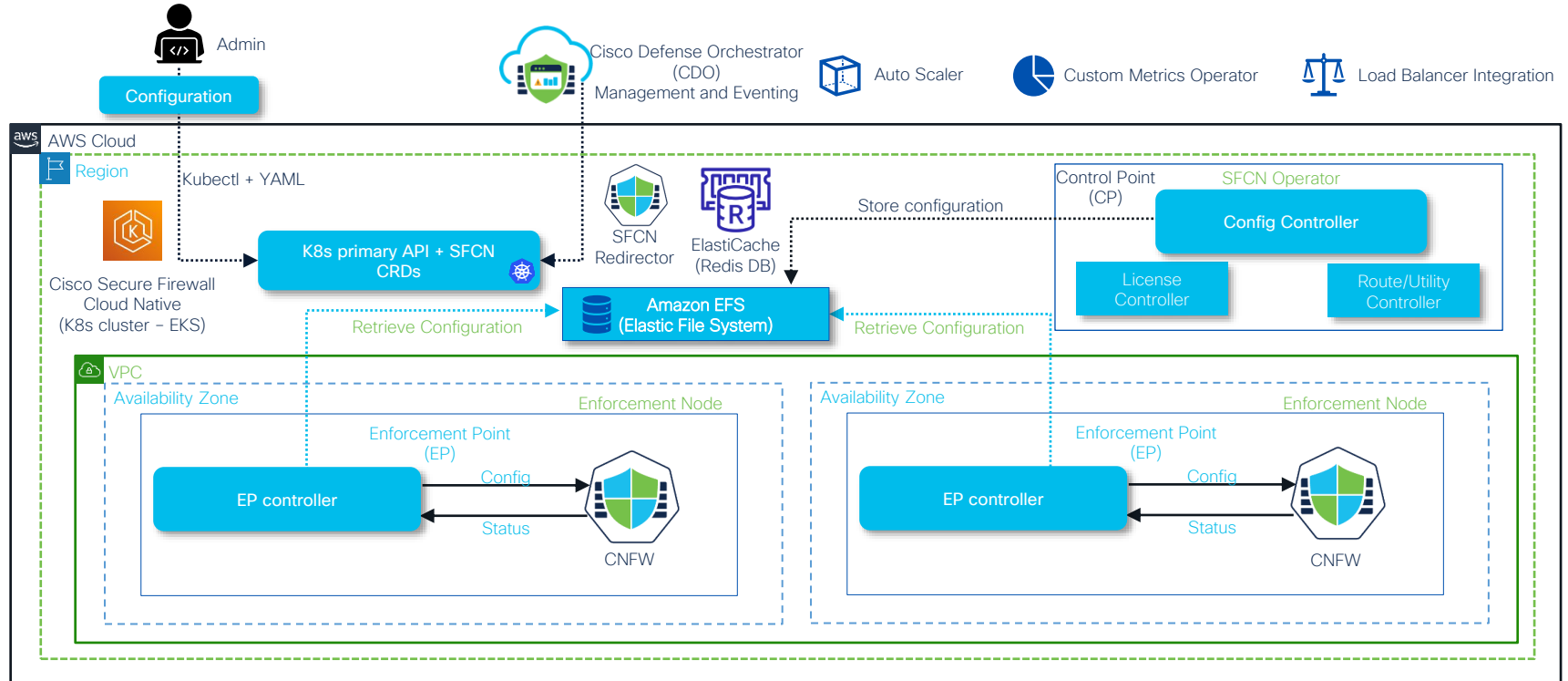
- Scalable architecture  
(Horizontal Pod Autoscaler - HPA)
- Modular security architecture
- K8s orchestrated deployments  
(Amazon EKS)
- DevOps friendly  
(YAML + CI/CD + GitOps)
- CRDs and Helm Charts
- Config management  
(REST API/YAML/CDO UI)
- Data externalization (Redis)  
for stateless services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

# Cisco Secure Firewall Cloud Native Enforcers

Enforcer = Pod



# 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*

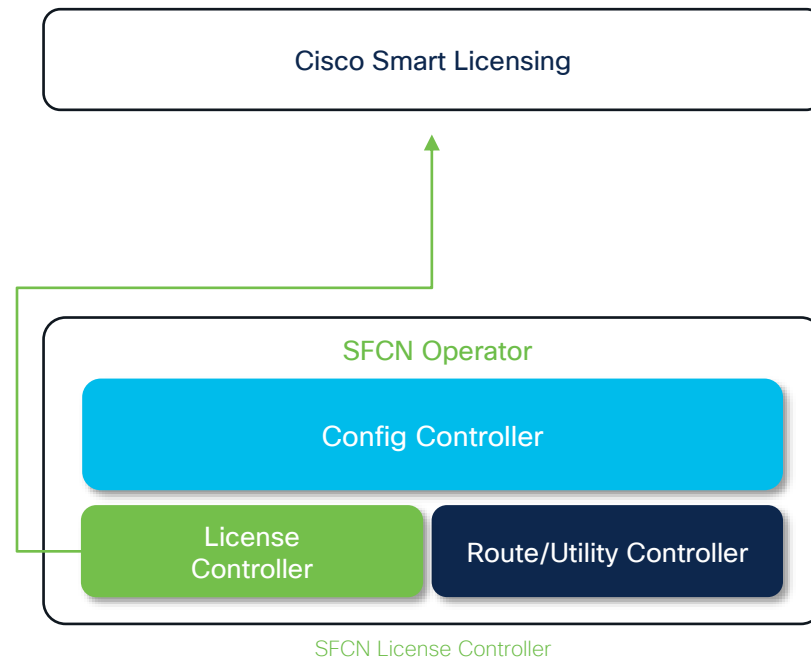
Type	Throughput
IPsec VPN throughput (AES 450B UDP test)	1.5 Gbps

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



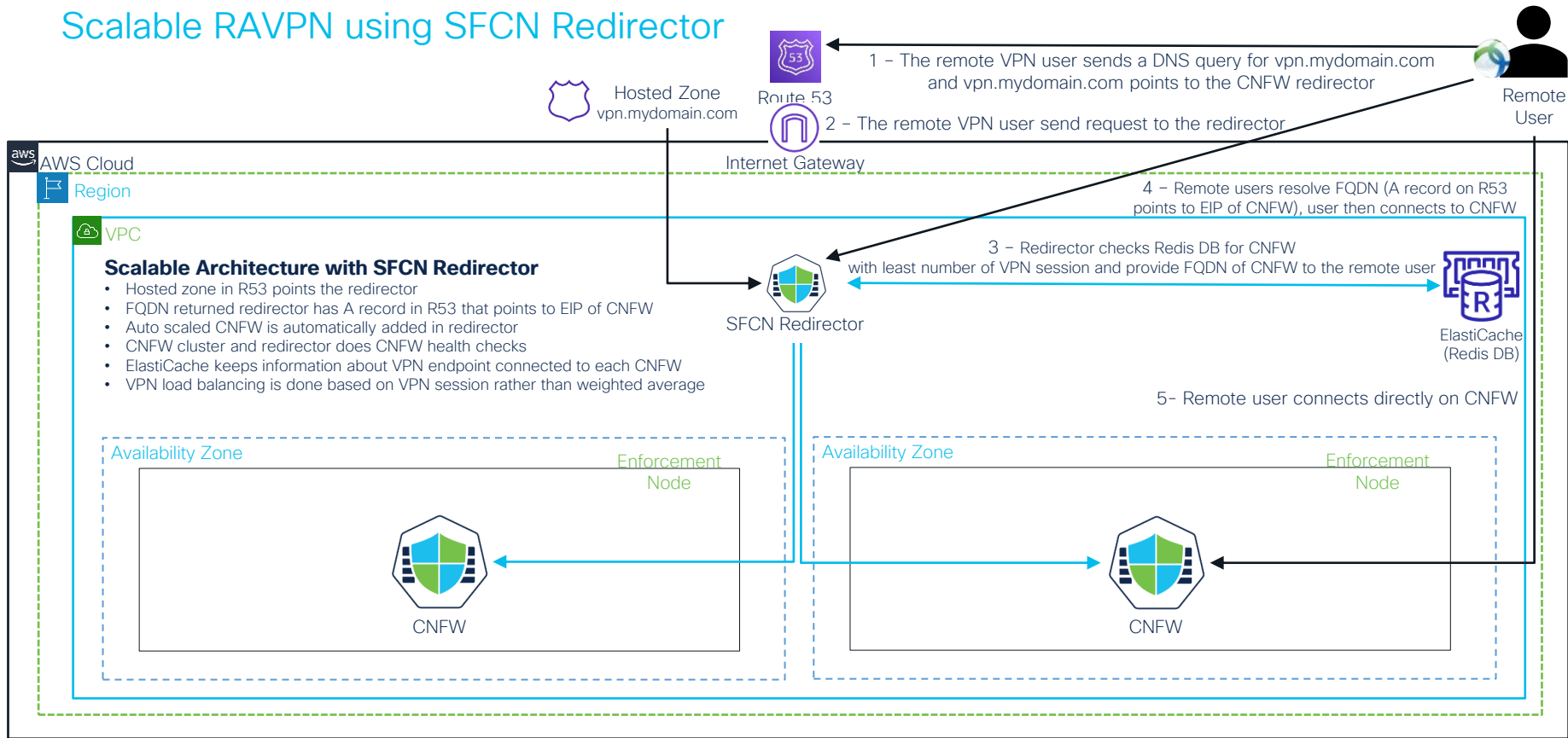
# Use Cases

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

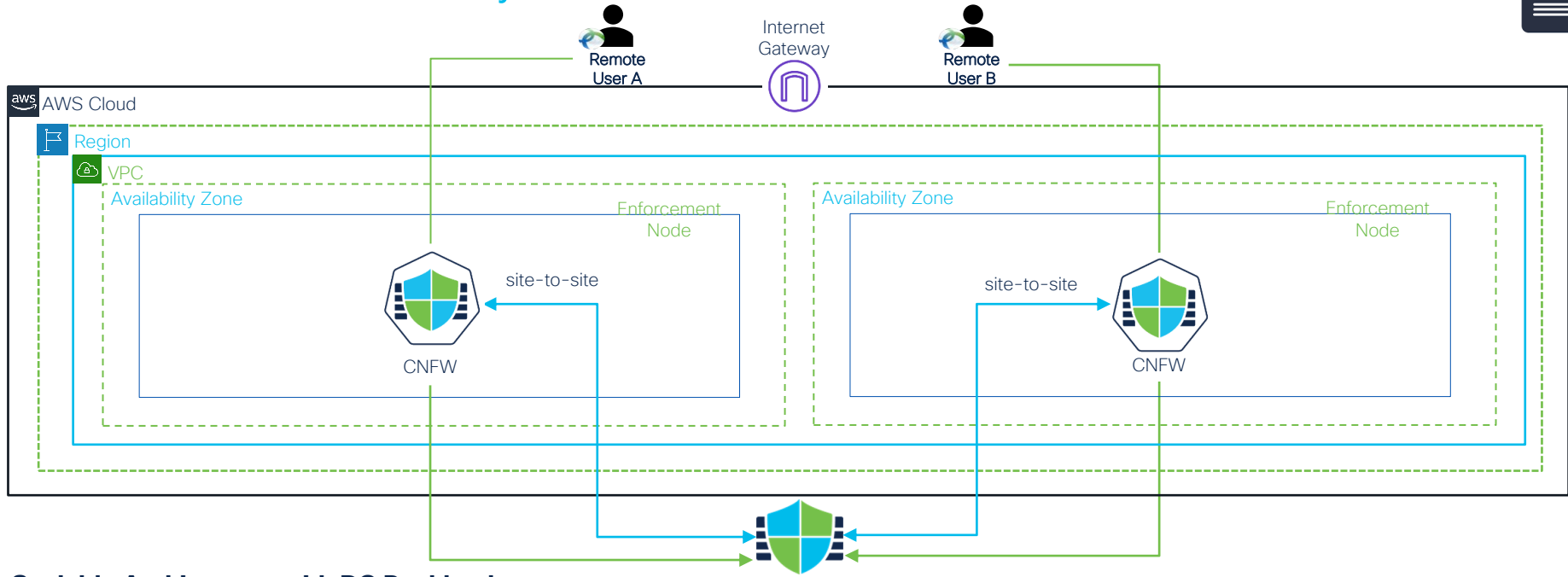


# Cisco Secure Firewall Cloud Native

## Scalable RAVPN using SFCN Redirector

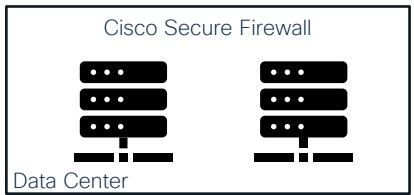


# Cisco Secure Firewall Cloud Native Backhaul Connectivity



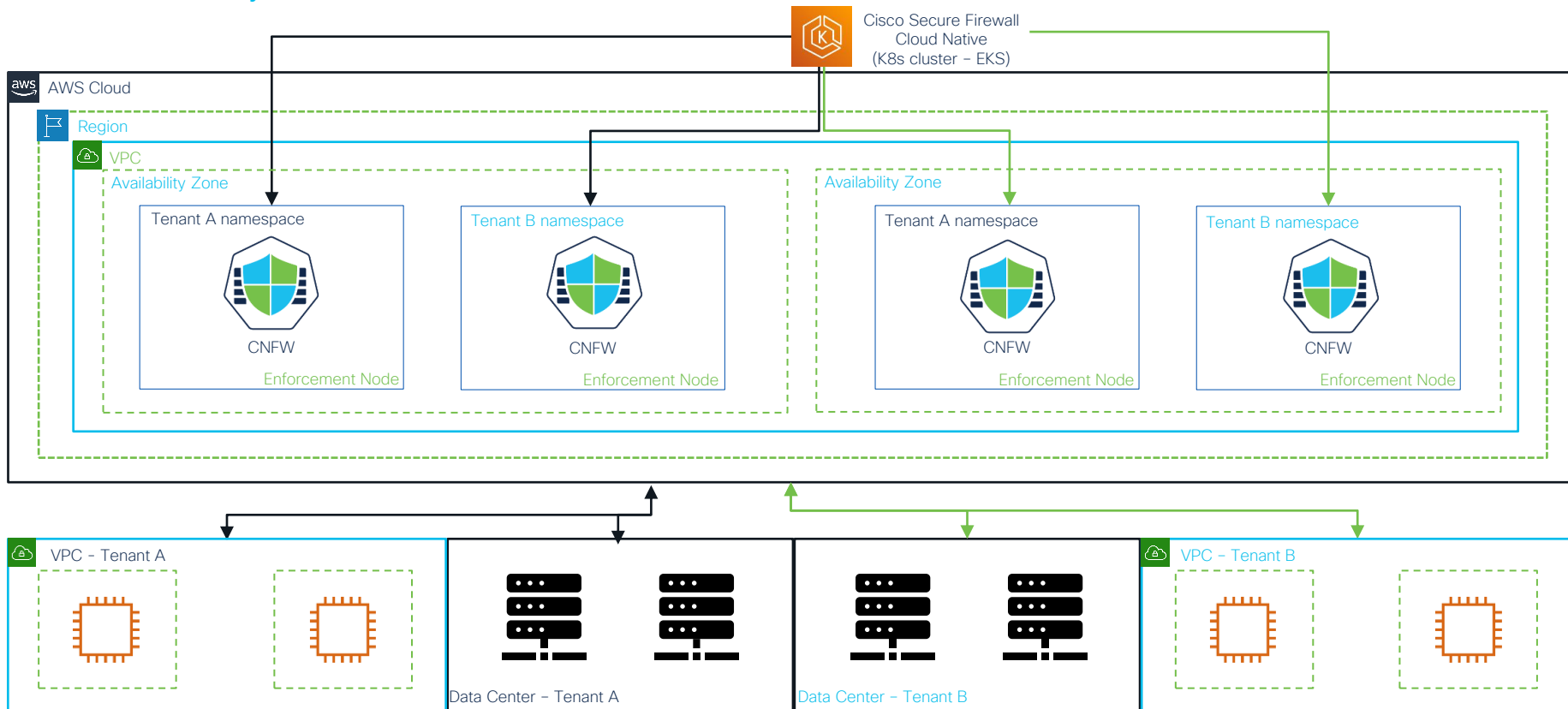
## Scalable Architecture with DC Backhaul

- 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



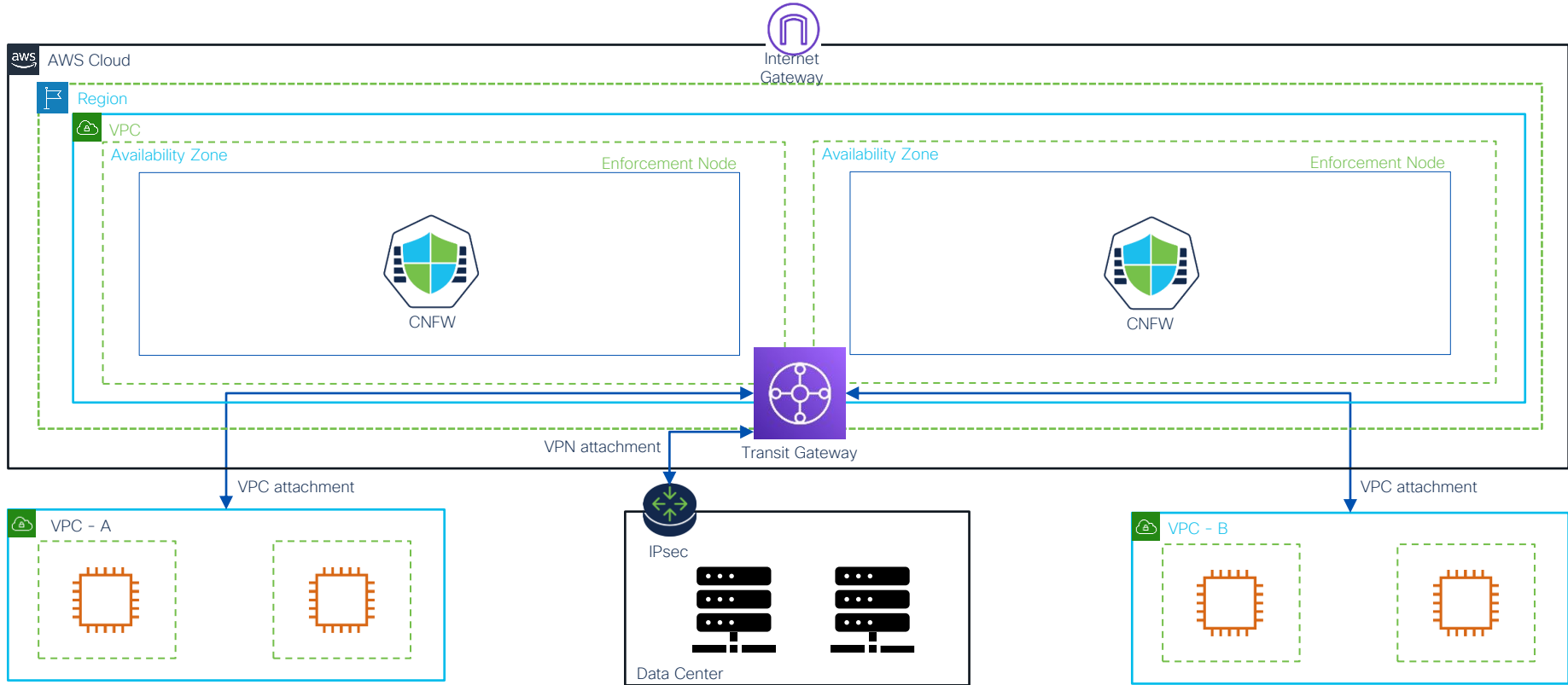
# Cisco Secure Firewall Cloud Native

## Multi Tenancy





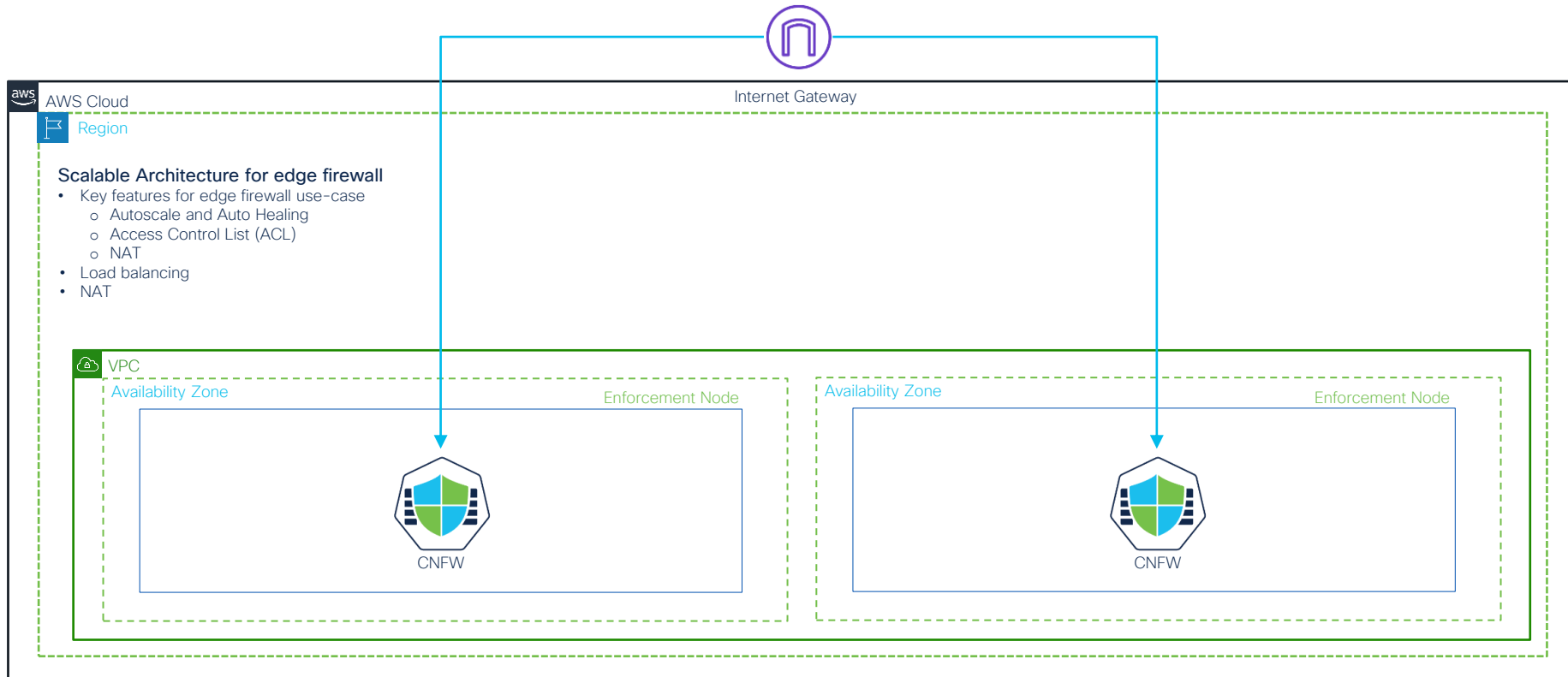
# Cisco Secure Firewall Cloud Native Scalable Cloud Hub





# Cisco Secure Firewall Cloud Native

## Scalable Edge Firewall






# What's new in Cisco Secure Firewall Cloud Native?





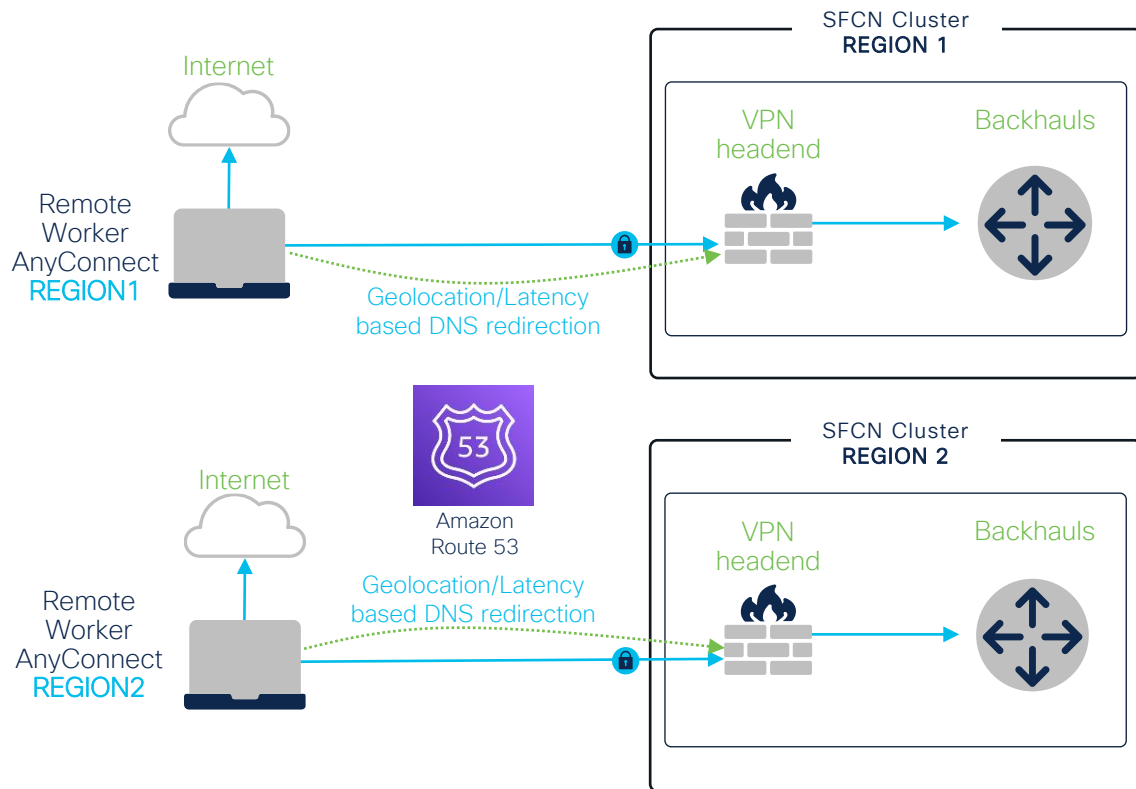
# Cisco Secure Firewall Cloud Native 1.1

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





# Multi region architecture



## SFCN 1.1

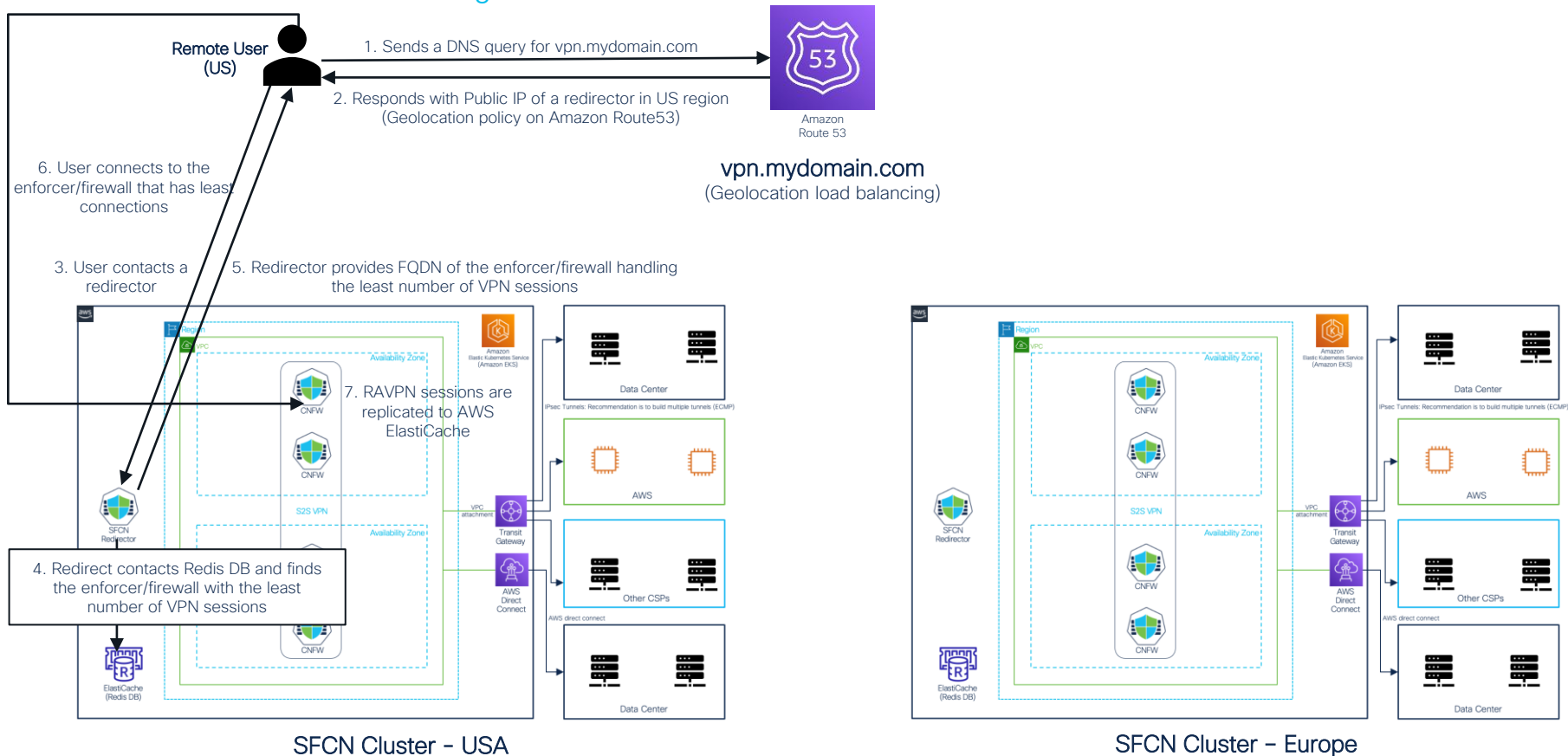
- Multi-region RAVPN
- SAML authentication

## 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



# Multi-Region SFCN Architecture

Geolocation based load balancing



vpn.mydomain.com  
(Geolocation load balancing)

Remote User  
(Europe)

1. Sends a DNS query for vpn.mydomain.com

2. Responds with Public IP of a redirector in EU region  
(Geolocation policy on Amazon Route53)

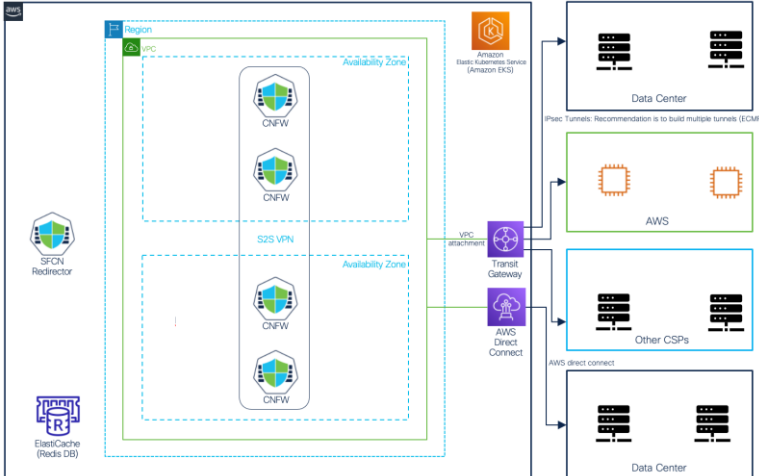
3. Firewall contacts a redirector

5. Redirector provides FQDN of the enforcer/firewall handling the least number of VPN sessions

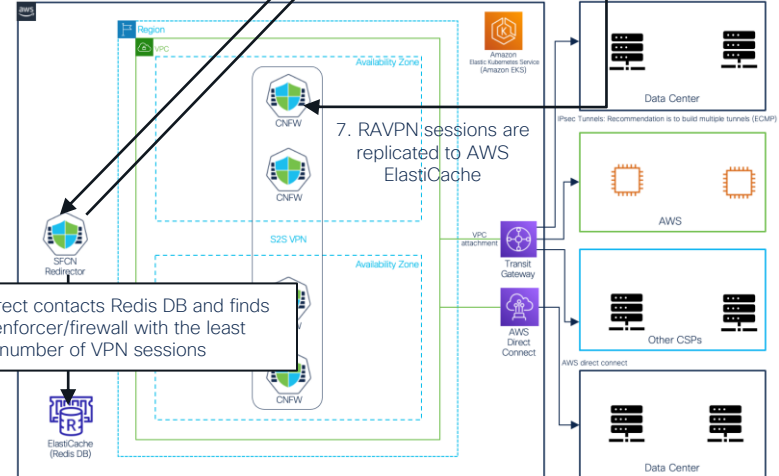
6. User connects to the enforcer/firewall that has least connections

4. Redirector contacts Redis DB and finds the enforcer/firewall with the least number of VPN sessions

7. RAVPN sessions are replicated to AWS ElastiCache



SFCN Cluster - USA

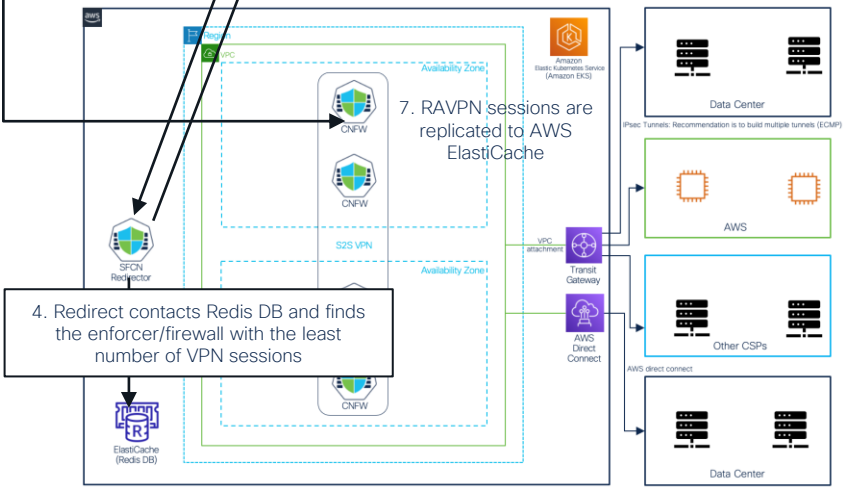
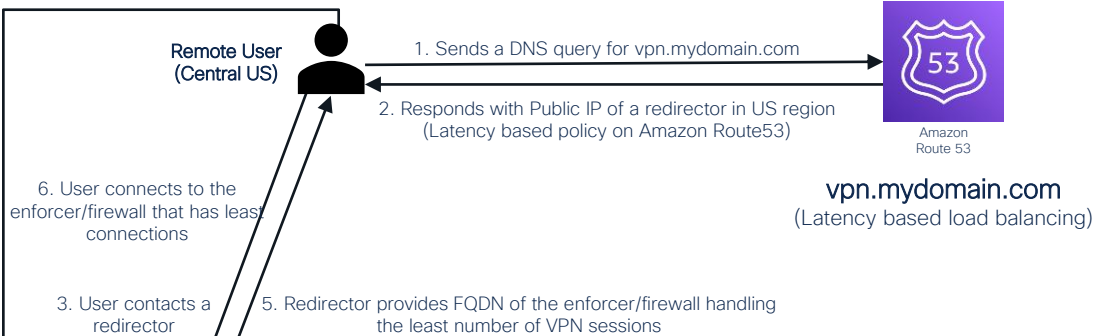


SFCN Cluster - Europe

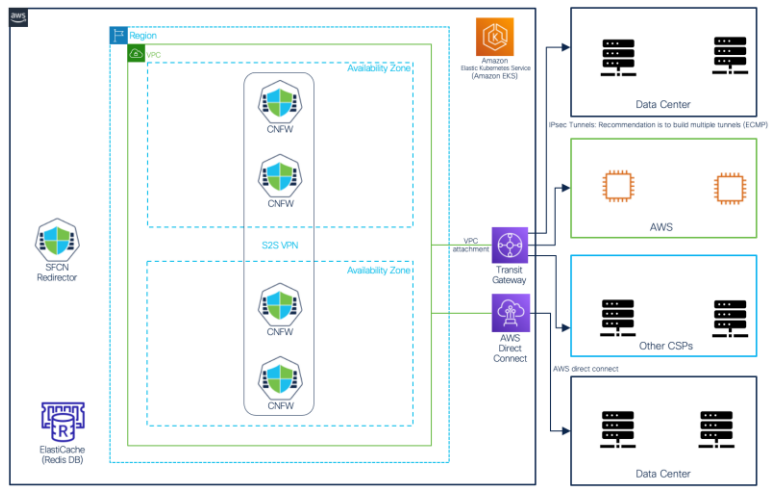


# Multi-Region SFCN Architecture

Latency based load balancing



SFCN Cluster - US WEST

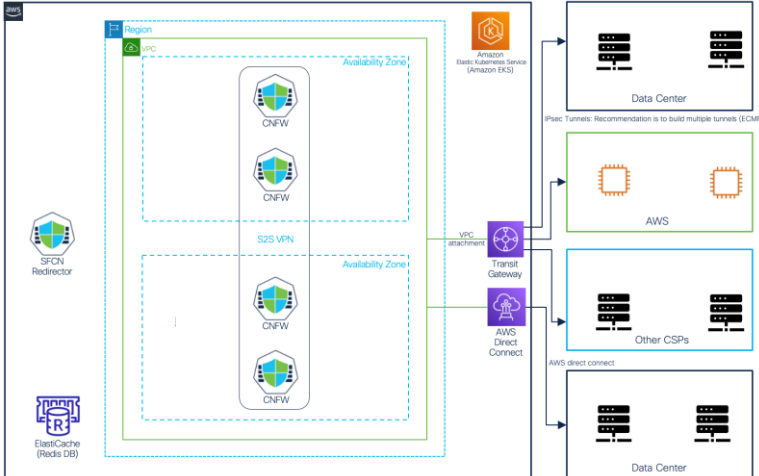
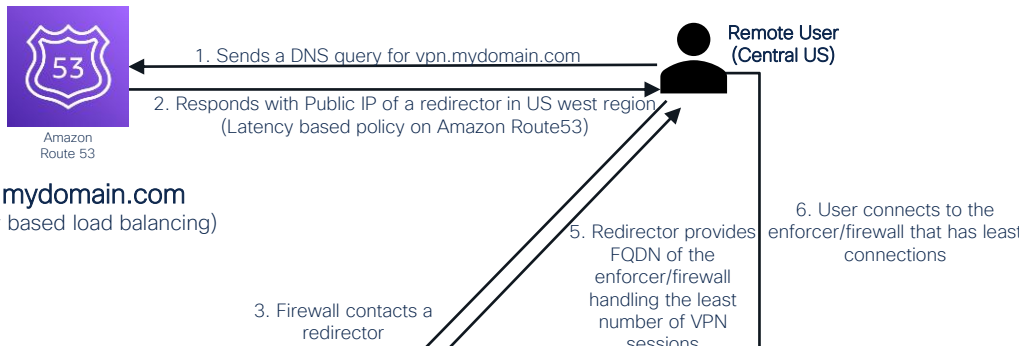


SFCN Cluster - US EAST

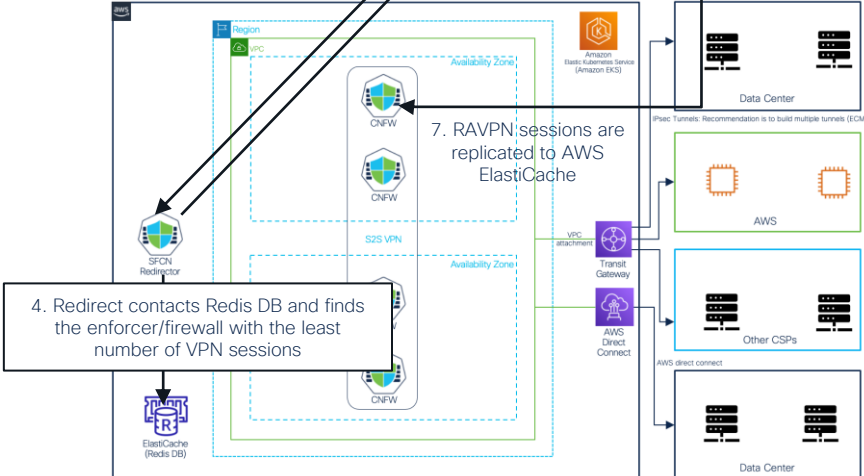


# Multi-Region SFCN Architecture

Latency based load balancing



SFCN Cluster - WEST

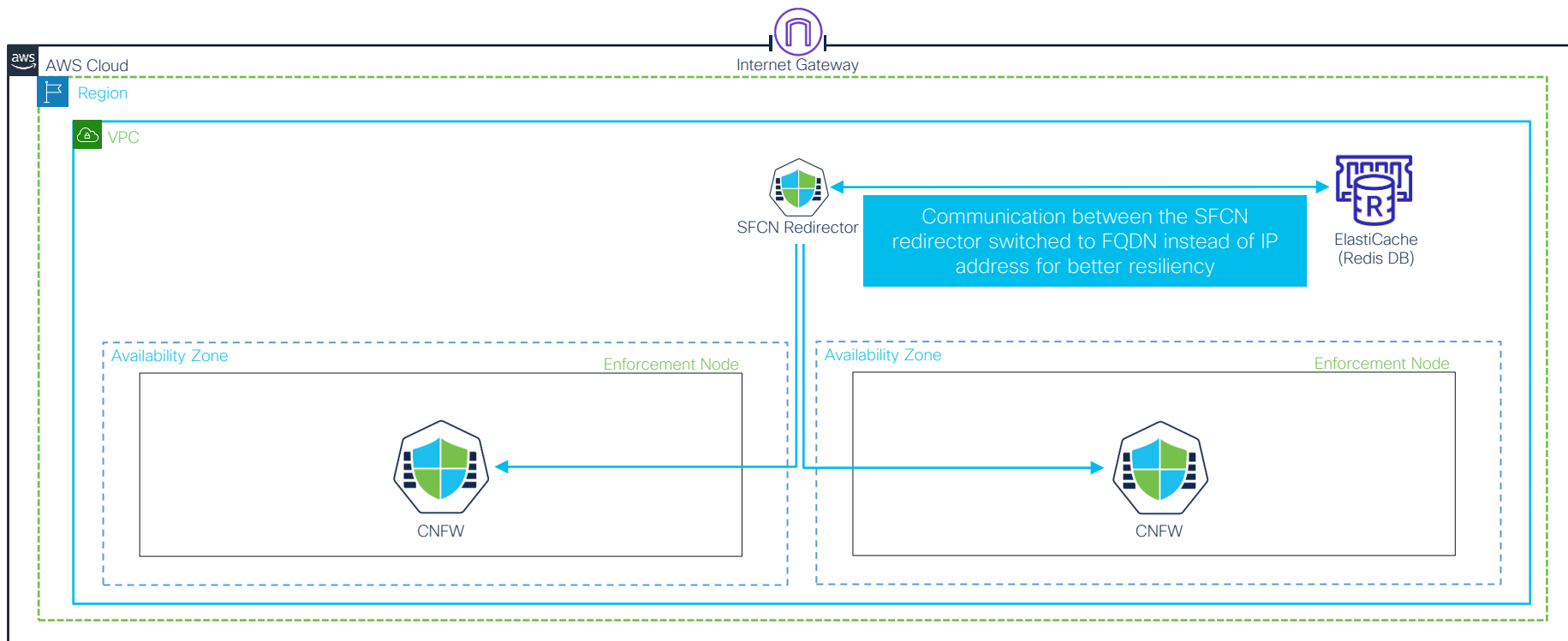


SFCN Cluster - EAST





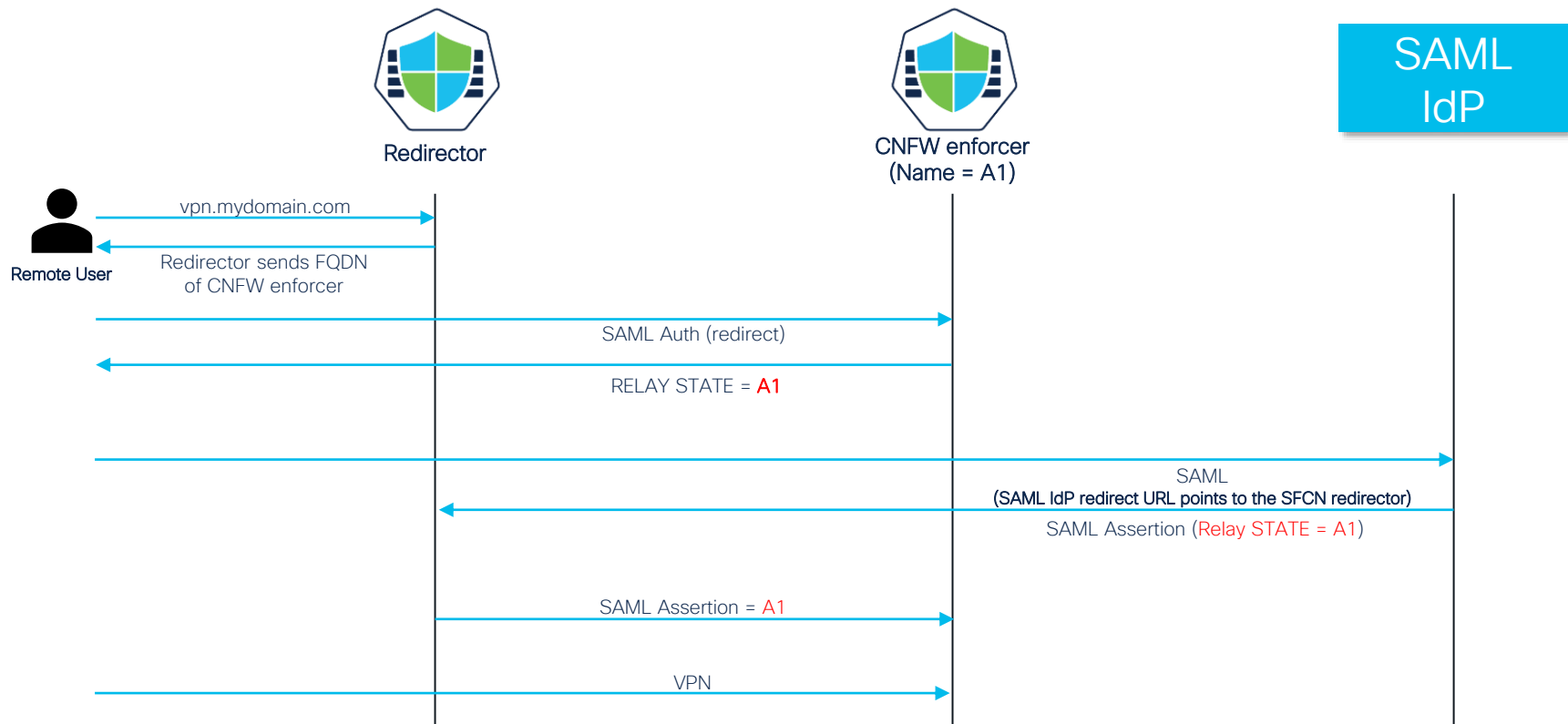
# FQDN support for Redis DB



# 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

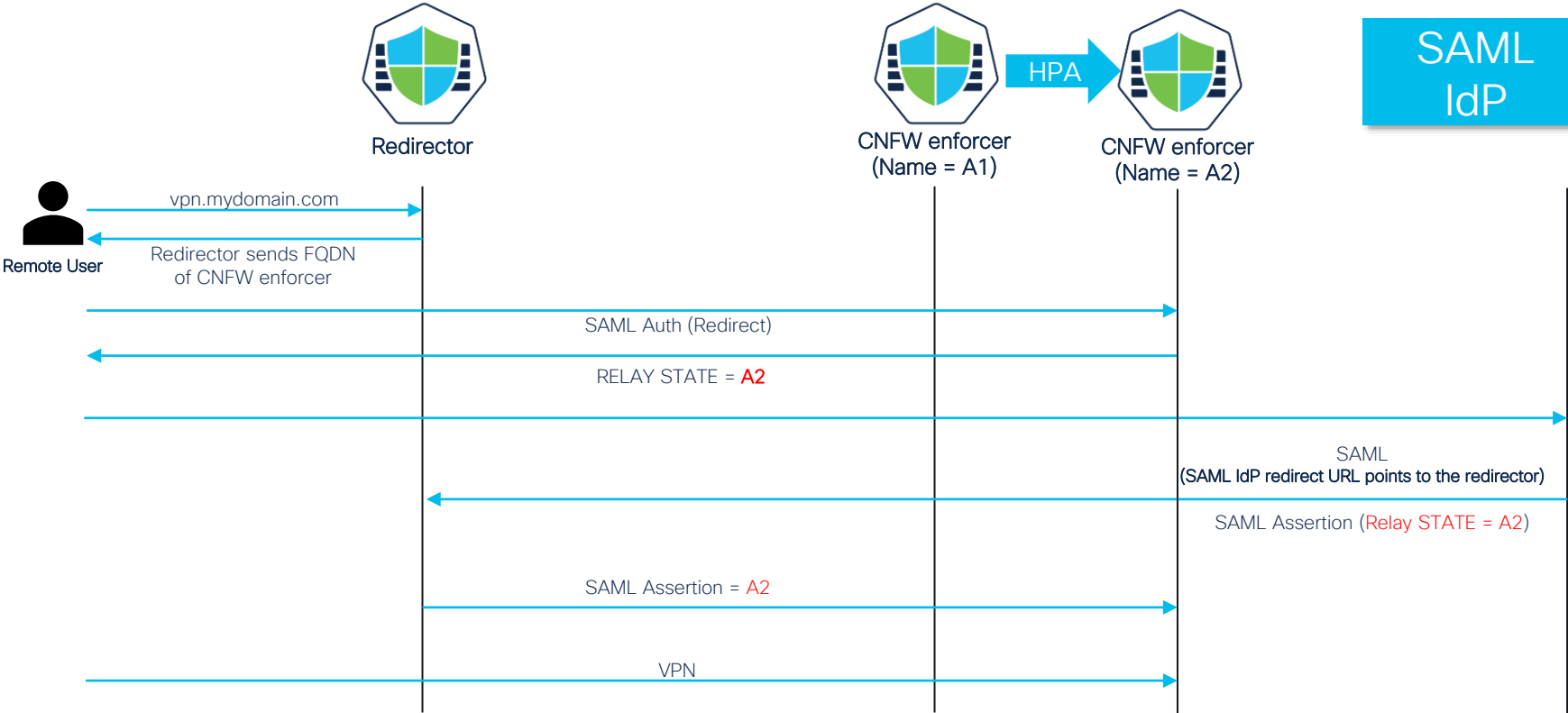
# SAML authentication support



# SAML authentication support (cont.)

## Horizontal Pod Autoscaler (HPA)

SAML IdP



# 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

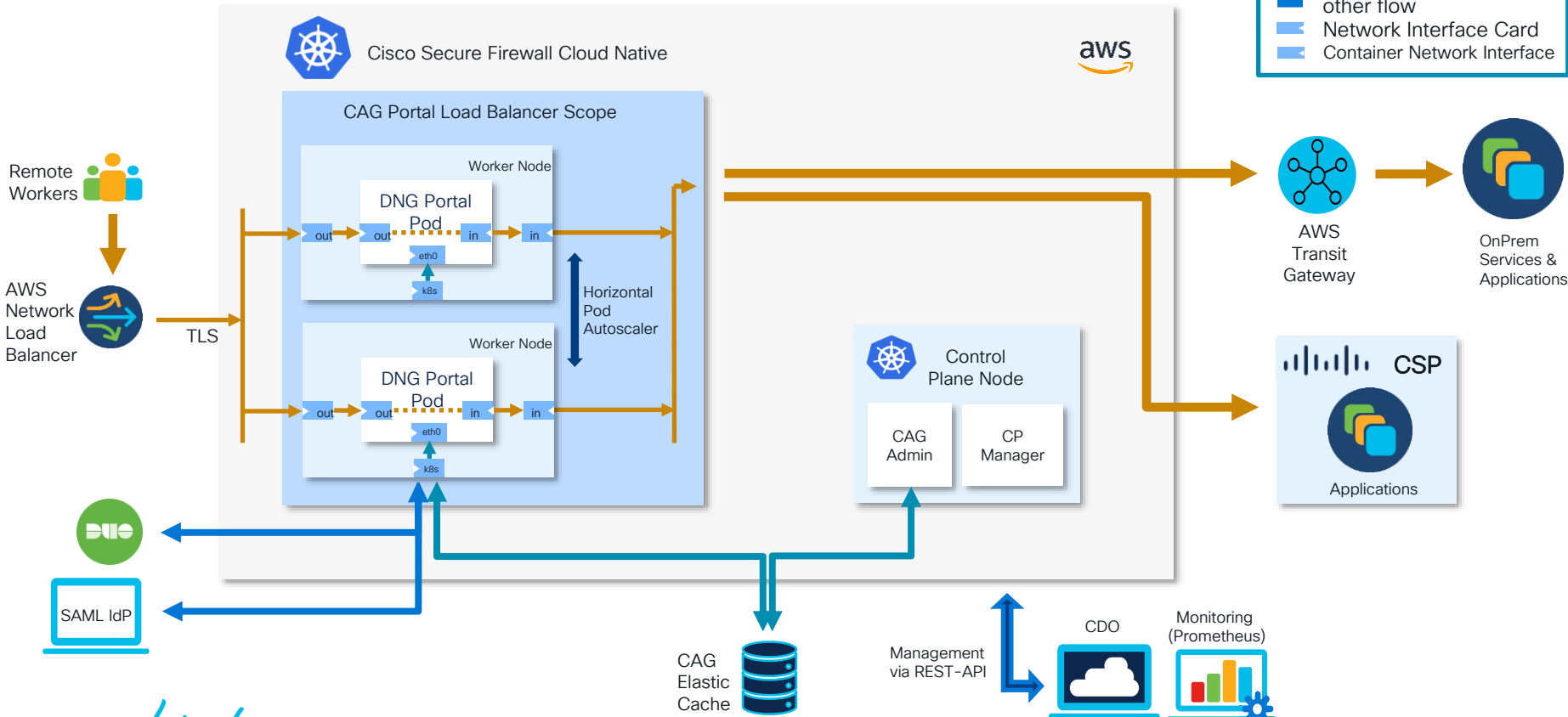
## Service Role and Topology

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

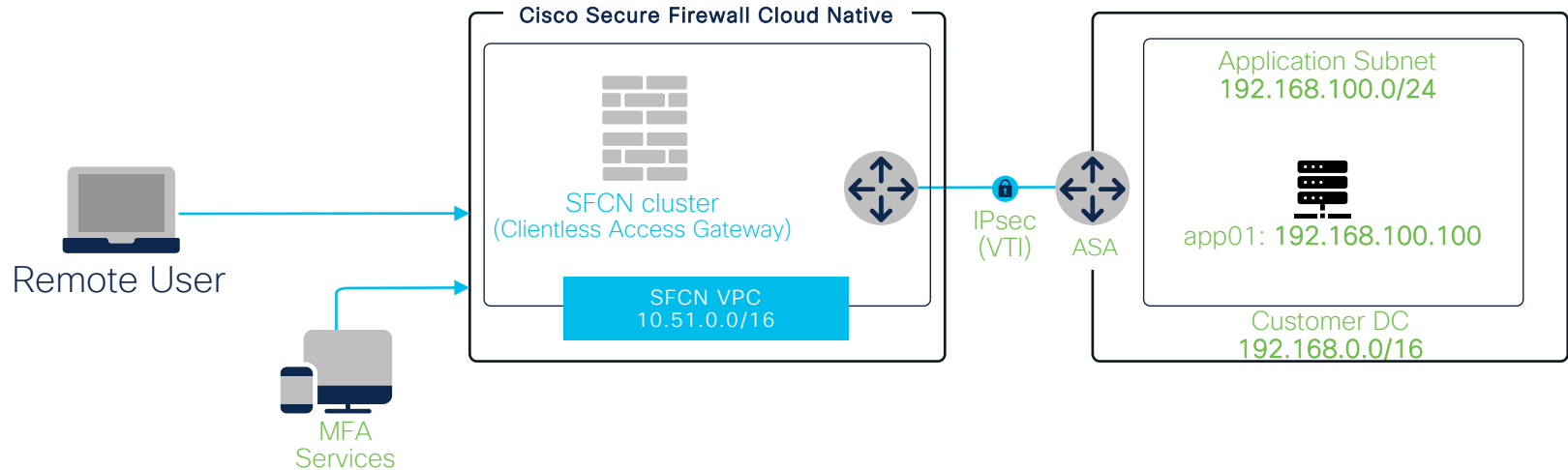
Service Role Combination	Topology
default	default
vpnredirector, default	vpnredirector → default
cag	NLB → cag

# Clientless Access Gateway (CAG)



# Cisco Secure Firewall Native

use-case: Private App Access

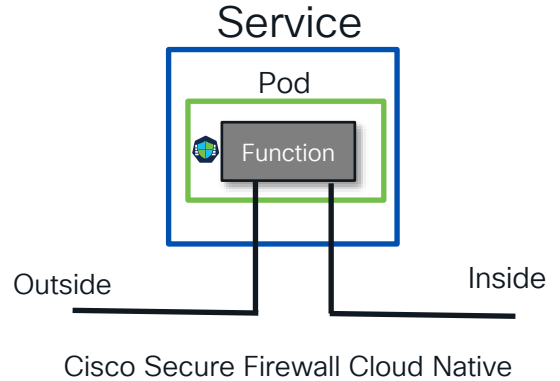


Clientless access gateway provides secure access to the private application

# Service Function Chaining (CNTD)

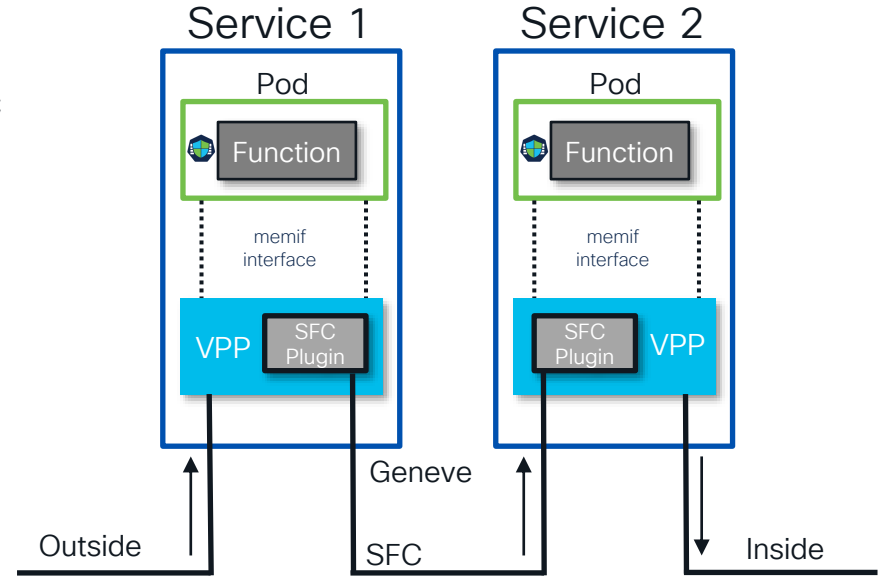
# Cisco Secure Firewall without service chain

- 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

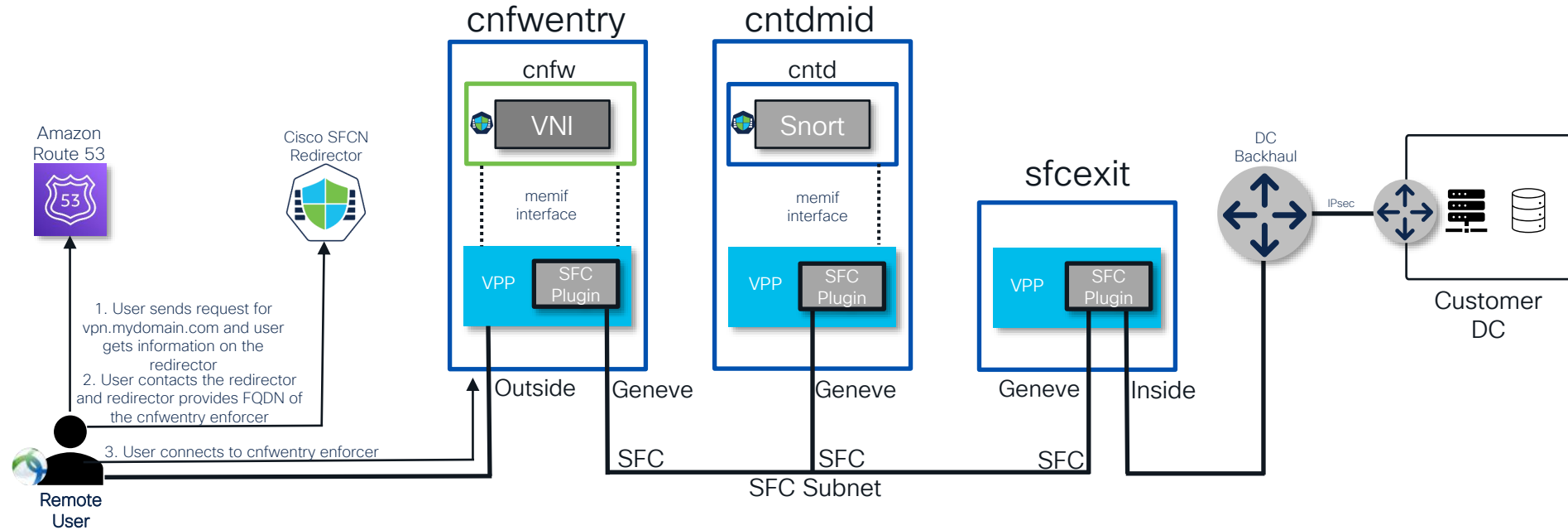
## Service Role and Topology

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

Service Role Combination	Topology
cnfwenry, cntdmid, sfccexit	cnfwenry -> cntdmid -> sfccexit
vpnredirector, cnfwenry, cntdmid, sfccexit	vpnredirector, cnfwenry -> cntdmid -> sfccexit <b>(recommended)</b>

# Cisco Secure Firewall Cloud Native Architecture

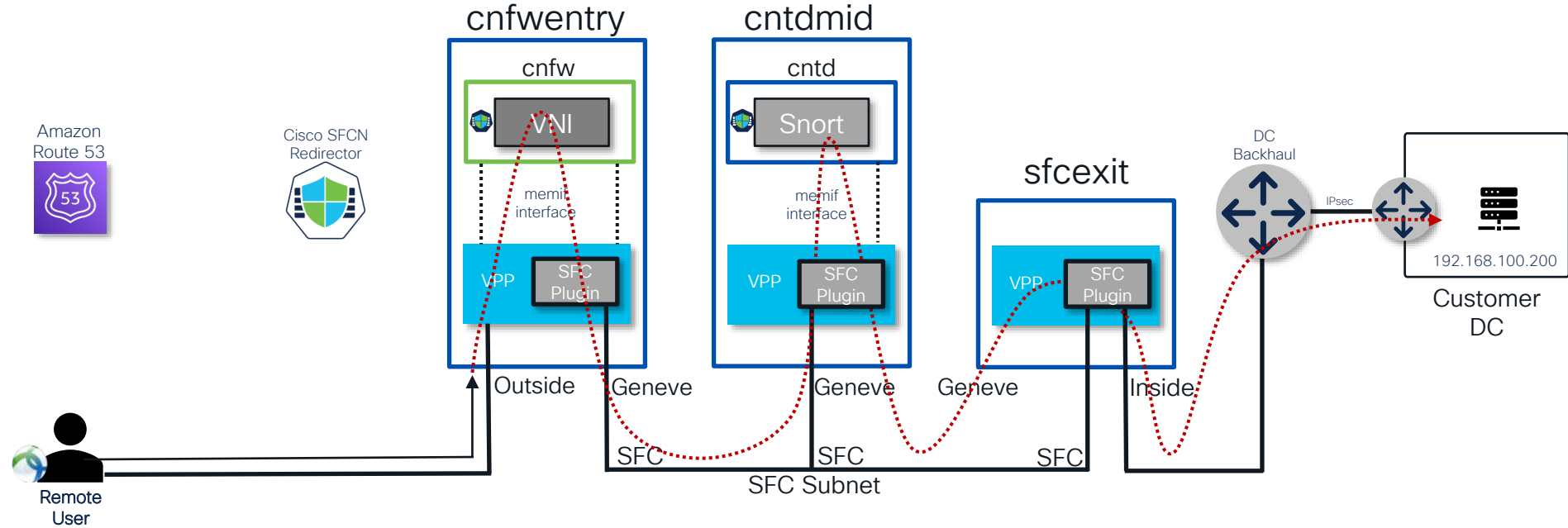
Topology: vpnredirector, cnfwentry -> cntdmid -> sfcexit



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

# Cisco Secure Firewall Cloud Native Architecture

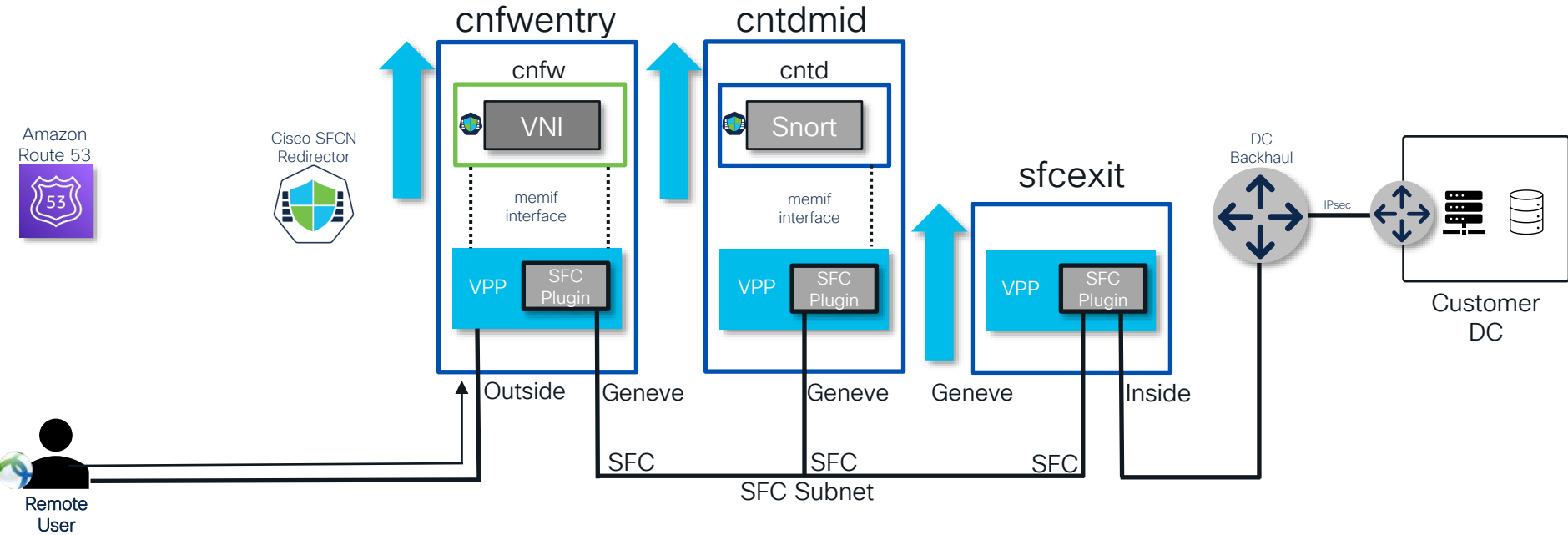
Traffic Flow: vpnredirector, cnfwentry -> cntdmid -> sfccxit



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

# Cisco Secure Firewall Cloud Native Architecture

Scalability: vpnredirector, cnfwentry -> cntdmid -> sfccxit



Services can scalable independently using Horizontal Pod Autoscaler

# Demo

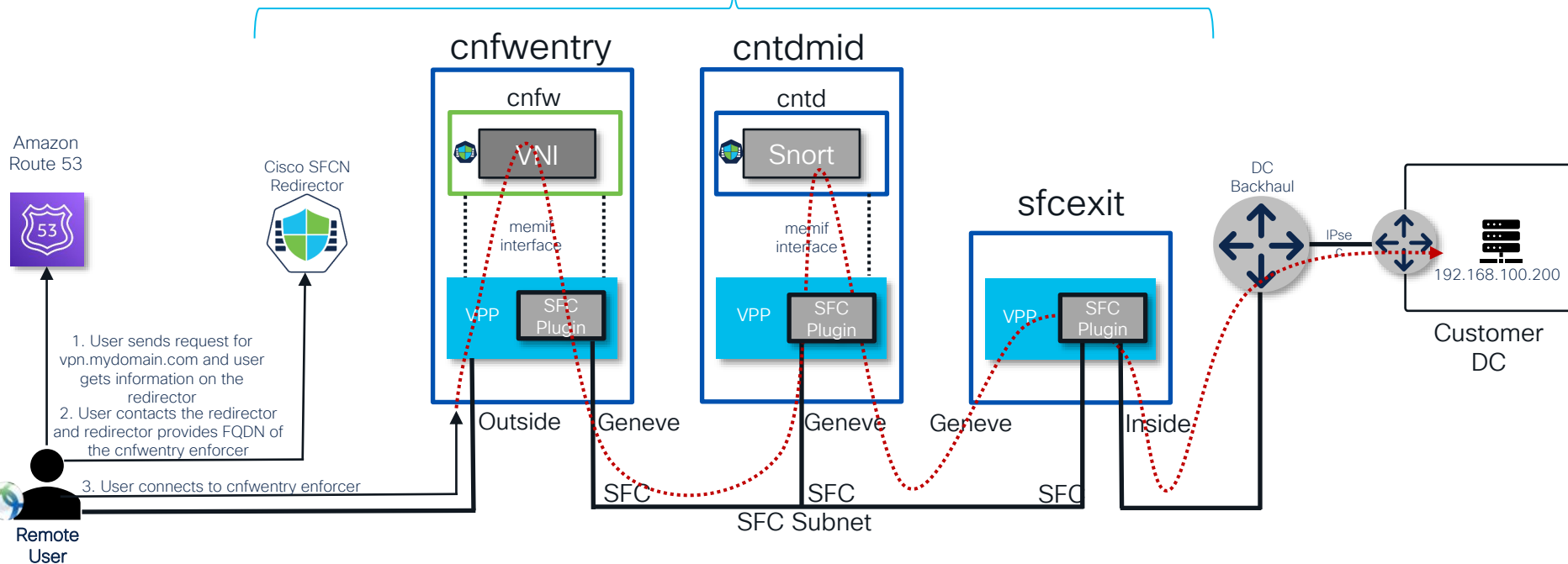
(Service Function Chaining)



# Cisco Secure Firewall Cloud Native Architecture

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

Management & Monitoring → Cisco Defense Orchestrator (CDO)



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

# Inventory

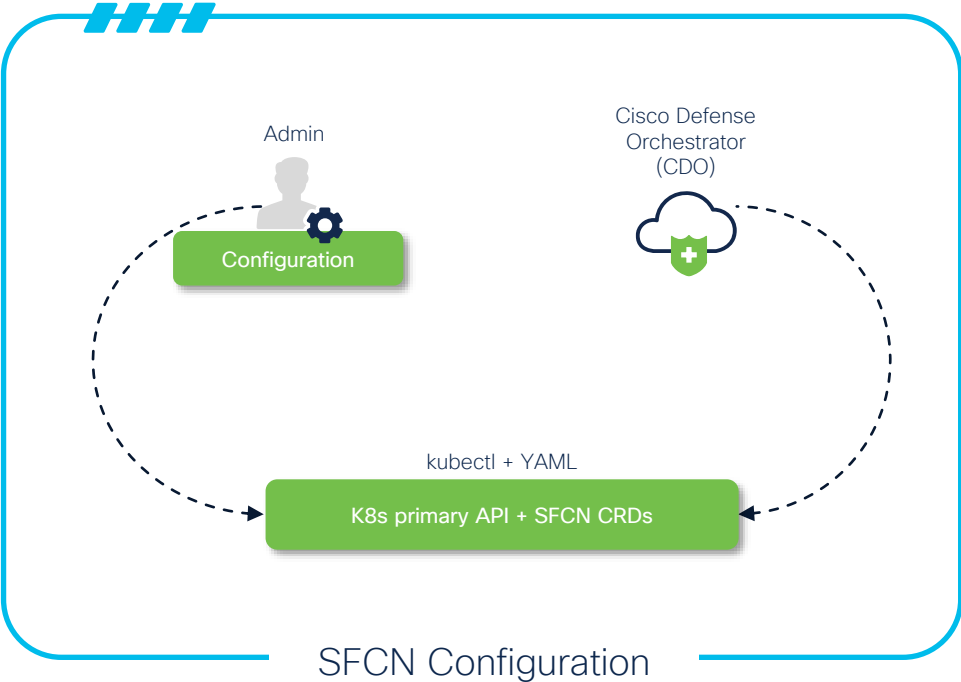
- Hide Menu
- Secure Connect Choice
- Inventory**
- Configuration
  - Policies
  - Objects
  - VPN and Zero Trust
- Events & Monitoring
  - Analytics
  - Change Log
  - Jobs
  - Tools & Services
  - Settings

Devices  Templates
 
Displaying 2 of 2 results

All	SFCN	SFCN STS
Name	Configuration Status	Connectivity
<input type="checkbox"/> sfcn-sfcdemo <small>SFCN</small>	<input type="checkbox"/> Synced	<input type="checkbox"/> Online
<input type="checkbox"/> sfcn-sfcdemo-sts <small>SFCN STS</small>	<input type="checkbox"/> Synced	<input type="checkbox"/> Online

# Configuration

- ▶▶ K8s API + SFCN CRDs
- ▶▶ Cisco Defense Orchestrator



# SFCN deployment

## Step 1

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

The screenshot shows the AWS Marketplace listing for Cisco Secure Firewall Cloud Native BYOL. The page includes a navigation bar with 'aws marketplace' and a search bar. The main content area features the product title, a 'Continue to Subscribe' button (highlighted with a red box), and a 'Save to List' button. Below the product details, there are tabs for 'Overview', 'Pricing', 'Usage', and 'Support'. The 'Overview' tab is selected, showing a 'Product Overview' section with text about the product's capabilities and a 'Highlights' section with a bulleted list of features. A blue oval overlay on the right side of the page contains the text 'SFCN 1.1 is now available'.

aws marketplace

Categories ▾ Delivery Methods ▾ Solutions ▾ AWS IQ ▾ Resources ▾ Your Saved List

Hello, assumed-role/admin/a... ▾

Partners Sell in AWS Marketplace Amazon Web Services Home Help

**Cisco Secure Firewall Cloud Native BYOL**

By: [Cisco](#) Latest Version: v1.0.0

**Continue to Subscribe**

Save to List

**SECURE**

The Secure Firewall Cloud Native seamlessly extends Cisco's industry-leading security to a cloud-native form factor using Kubernetes (K8s) orchestration to achieve scalability and

▾ Show more

Linux/Unix

**BYOL**

Overview Pricing Usage Support

### Product Overview

Cisco Secure Firewall Cloud Native is the latest addition to the Secure Firewall family, modernizing the way enterprises and service providers secure applications at scale. Isolate and protect workloads, application stacks, and services. Protect the ingress and egress from external networks and legacy applications. Use AWS CloudFormation to model and set up your Secure Firewall Cloud Native resources consistently and repeatedly, empowering your NetOps and SecOps teams to run at DevOps speed.

**SCALABLE ARCHITECTURE**

Enjoy automated scaling features for security services based on demand. Additional features include container health monitoring and automatic unhealthy container replacement, ensuring high availability during maintenance, surge conditions, and partial outages. Secure Firewall Cloud Native uses industry-standard Kubernetes orchestration to provide linear scalability and resiliency for containers.

### Highlights

- Leverages AWS CloudFormation templates to easily deploy the Secure Firewall Cloud Native into an Amazon EKS cluster using a simple wizard-driven process. You can choose standalone or multi-tenant deployments.
- Smart load balancing automates horizontal scaling thresholds with custom metrics.
- Enjoy simplified configuration. The integrated control plane ensures configuration changes are applied to all containers.

BRKSEC-3561

# SFCN deployment (cont.)

## Step 2

On the [Subscribe to this software](#) page, click on “continue to configuration”

The screenshot shows the AWS Marketplace interface for the Cisco Secure Firewall Cloud Native BYOL product. The page title is "Subscribe to this software". A red box highlights the "Continue to Configuration" button. Below the button, there is a section for "Terms and Conditions" and a "Cisco Offer" section. At the bottom, there is a table with columns for Product, Effective date, Expiration date, and Action.

Product	Effective date	Expiration date	Action
Cisco Secure Firewall Cloud Native BYOL	6/11/2021	N/A	<a href="#">Show Details</a>

# 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”

The screenshot displays the AWS Marketplace interface for the Cisco Secure Firewall Cloud Native BYOL solution. The page title is "Configure this software". Below the title, there is a section for "Delivery Method" with a dropdown menu set to "Cloud Formation Quickstart". To the right of this dropdown, it lists "Supported Amazon Services" including "Amazon EKS". Below the delivery method, there is a "Software Version" dropdown menu set to "v1.0.0 (Jun 09, 2021)". A red box highlights the "Continue to Launch" button and the configuration fields. A blue oval on the right contains the text "SFCN 1.1 is now available".

# 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.

The screenshot shows the AWS Marketplace interface for the Cisco Secure Firewall Cloud Native BYOL product. The page is titled "Launch this software" and provides configuration details and deployment options. The "Deployment template" section is highlighted with a red box, showing three options: "Install in a new VPC", "Install in an existing VPC", and "Add tenant to an existing installation".

**Configuration Details**

Fulfillment Option	Cloud Formation Quickstart
Software Version	v1.0.0
Supported Amazon Services	<a href="#">Amazon EKS</a>

[Usage Instructions](#)

**Container Images**

This product has 24 container images. Use the following options to deploy the product.

**Deployment template**

- [Install in a new VPC](#)
- [Install in an existing VPC](#)
- [Add tenant to an existing installation](#)

[View container image details](#)

# SFCN deployment (cont.)

Step 5

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

The screenshot shows the AWS console interface for creating a stack. The page title is "Quick create stack". The "Template" section shows the URL `https://sfcn-quickstart.s3.amazonaws.com/quickstart-cisco-secure-firewall-cloud-native/templates/endpoint-new-vc.template.yaml` and the description "Deploys Cisco Secure Firewall Cloud Native into a new EKS cluster in a new VPC." The "Stack name" section has a text input field containing "answami-sfcn". The "Parameters" section is highlighted with a red box and contains two fields: "SSH key name" with a dropdown menu showing "key-answami", and "EKS admin user" with a text input field containing "arn:aws:iam:::user/answami-cli".

# SFCN deployment (cont.)

## Step 6

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

The screenshot displays the AWS Management Console configuration page for SFCN. The interface is organized into several sections:

- Basic Configuration - Global**
  - Storage type**: The type of a storage used to keep logs and deployments files. The dropdown menu is set to `efs`.
- Basic Configuration - Control Plane**
  - Desired nodes**: The desired number of control plane worker nodes. The input field contains the value `1`.
  - Maximum nodes**: The maximum number of control plane worker nodes. The input field contains the value `2`.
- Basic Configuration - Data Plane**
  - Desired nodes**: The desired number of data plane worker nodes. The input field contains the value `1`.
  - Maximum nodes**: The maximum number of data plane worker nodes. The input field contains the value `5`.
- Elastic IP attachment mode**: CNFW interfaces to attach Elastic IPs. The dropdown menu is set to `both`.
- Cache type**: Type of External Cache to use for CNFW. The dropdown menu is set to `elasticache`.

The bottom right corner of the console shows the identifier `BRKSEC-3561`.

# SFCN deployment (cont.)

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

The screenshot displays the AWS IAM console configuration page for the SFCN Enforcer role. The page is titled "Basic Configuration - Firewall" and includes several sections for configuring the role's behavior and permissions.

- Enforcer installation:** A dropdown menu is set to "Enabled".
- Enforcer service roles:** A dropdown menu is set to "default,vpnredirector".
- Enforcer autoscaling:** A dropdown menu is set to "Enabled".
- Smart License token:** A text input field contains a long string of asterisks, representing a masked token.
- Maximum licenses count:** A text input field contains the number "4".
- Advanced Configuration - Cluster:**
  - Kubernetes version:** A dropdown menu is set to "1.18".
  - Additional EKS admin role:** An empty text input field.
  - Cluster logging types:** An empty text input field.

The bottom right corner of the screenshot contains the identifier "BRKSEC-9561".

# SFCN deployment (cont.)

## Step 8

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

The screenshot shows the AWS IAM console interface for configuring SFCN. The 'Advanced Configuration - Control Plane' section is visible, with the 'Controller instance tier' set to 'vCPU4'. The 'Advanced Configuration - Data Plane' section is also visible, with the 'Enforcer instance tier' set to 'vCPU4'. The 'Cache node type' is set to 'cache.m5.large'. The 'Redis authentication token' field is highlighted with a red box, with a note: 'Blank or 16-128 alphanumeric characters. Only permitted special characters are !, &, #, \$, ^, \, >, and -. Takes effect only when in-transit encryption is enabled.' The 'Redis key to encrypt sensitive data' field is also highlighted with a red box, with a note: 'User provided key to encrypt sensitive data in the cache. Must consist of 64 uppercase hexadecimal characters (A-F,0-9). Required when 'elasticache' cache type is specified.' The 'In-Transit encryption' dropdown is set to 'Disabled'. The 'Advanced Configuration - Firewall' section is visible below, with the 'Product version' set to 'v1.0.0' and the 'System namespace' set to 'sfcn-system'.

Redis authentication key is required if Redis DB is selected.

# SFCN deployment (cont.)

## Step 9 Define advanced network configuration

The screenshot displays the AWS Management Console interface for configuring a VPC network. The page title is "Advanced Configuration - Network". The left sidebar shows the AWS logo and "Services" with a dropdown arrow. The top navigation bar includes a search bar with the text "Search for services, features, marketplace products, and docs" and a placeholder "[Option+S]". On the right side of the navigation bar, it shows "N. Virginia" with a dropdown arrow and "Support" with a dropdown arrow. The main content area is divided into two columns. The left column contains the following configuration items, each with a label, a description, and an input field:

- VPC CIDR**  
CIDR block for the VPC  
Input field: 10.37.0.0/16
- Public subnet 1 CIDR**  
CIDR block for the public DMZ subnet 1 (CNFW default 1), located in Availability Zone 1.  
Input field: 10.37.0.0/20
- Private subnet 1 CIDR**  
CIDR block for private subnet 1, located in Availability Zone 1.  
Input field: 10.37.128.0/20
- Public subnet 2 CIDR**  
CIDR block for the public DMZ subnet 2 (CNFW default 2), located in Availability Zone 2.  
Input field: 10.37.48.0/20
- Private subnet 2 CIDR**  
CIDR block for private subnet 2, located in Availability Zone 2.  
Input field: 10.37.144.0/20
- CNFW outside subnet 1 CIDR**  
CIDR block for the CNFW outside subnet 1, located in Availability Zone 1.  
Input field: 10.37.16.0/20
- CNFW inside subnet 1 CIDR**  
CIDR block for the CNFW inside subnet 1, located in Availability Zone 1.  
Input field: 10.37.32.0/20
- CNFW outside subnet 2 CIDR**  
CIDR block for the CNFW outside subnet 2, located in Availability Zone 2.  
Input field: 10.37.64.0/20

The right column of the page is currently empty.

# SFCN deployment (cont.)

## Step 10 Check I acknowledge boxes and create stack

aws Services Search for services, features, marketplace products, and docs [Option+S] N. Virginia Support

**CNFW inside subnet 2 CIDR**  
CIDR block for the CNFW inside subnet 2, located in Availability Zone 2.

10.37.80.0/20

**(Read-only, do not change) AWS Quick Start configuration**

**Quick Start S3 bucket name**  
S3 bucket name for the Quick Start assets. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).

sfcn-quickstart

**Quick Start S3 key prefix**  
The S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), periods (.) and forward slashes (/).

quickstart-cisco-secure-firewall-cloud-native/

**Quick Start S3 bucket Region**  
AWS Region where the Quick Start S3 bucket (QSS3BucketName) is hosted. If you use your own bucket, you must specify this value.

us-east-1

**Capabilities**

**The following resource(s) require capabilities: [AWS::CloudFormation::Stack]**

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY\_AUTO\_EXPAND. Check the capabilities of these

- I acknowledge that AWS CloudFormation might create IAM resources with custom names.
- I acknowledge that AWS CloudFormation might require the following capability:  
CAPABILITY\_AUTO\_EXPAND

Cancel Create change set 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

```
1  apiVersion: cnfw.cisco.com/v1
2  kind: Route53Ingress
3  metadata:
4    finalizers:
5      - sfcn.cisco.com/route53ingressreconciler_finalizer
6    generation: 2
7    name: vpn
8    namespace: sfcn-system
9  spec:
10   attributes:
11     geolocation: {}
12   endpointSelector:
13     addressType: public
14     interfaceIndex: 2
15     serviceRole: default
16   hostedZone: Z02384461D5I212LXYZF
17   recordSetName: demo.cisco-vpn.com
18   recordType: A
19   recordUpdate: SUBDOMAIN
20  status:
21   appliedHostedZone: Z02384461D5I212LDUWSP
22   appliedRecordSetName: demo.cisco-vpn.com
23   endpoints:
24     - 54.187.127.167
25   pendingPods: []
26   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

```
1  apiVersion: cnfw.cisco.com/v1
2  kind: FileObject
3  metadata:|
4    generation: 1
5    name: ravpnprofile
6    namespace: sfcn-system
7  spec:
8    fileName: ravpn-profile.xml
9    localPath: /
10   s3:
11     auth:
12       accessKeyField: access_key
13       secretKeyField: secret_key
14       secretName: s3-auth-secret
15     bucket: kasavpnshared
16     item: ravpn-profile.xml
17     region: us-east-1
18   status:
19     conditions:
20       - lastTransitionTime: '2022-05-31T01:26:56Z'
21         lastUpdateTime: '2022-05-31T01:26:56Z'
22         reason: Successful
23         status: 'True'
24         type: Downloaded
25     lastDownloadHash: 055658d4333a00c5c81556e263dd4b66
26
```

# 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

```
1  apiVersion: cnfw.cisco.com/v1
2  kind: ASAConfiguration
3  metadata:
4    name: ravpn-enforcer-config
5    namespace: sfcn-system
6  spec:
7    order: 1
8    cliLines: >
9      webvpn
10     enable outside
11     anyconnect profiles my_AC_profile {{ .fileObjects.ravpnprofile.path }}
12     anyconnect image {{ .fileObjects.anyconnectwin.path }} 1
13     anyconnect image {{ .fileObjects.anyconnectmac.path }} 2
14     anyconnect image {{ .fileObjects.anyconnectlinux.path }} 3
15     anyconnect enable
16     tunnel-group-list enable
17     group-policy VPN_group_policy internal
18     domain-name {{ .route53Ingresses.vpn.recordSetName }}
19     ...
20   description: RA-VPN Configuration
21   fileObjects:
22     - ravpnprofile
23     - anyconnectlinux
24     - anyconnectwin
25     - anyconnectmac
26   ipv4SubnetPools:
27     - ravpnpool
28   route53Ingresses:
29     - vpn
30   secrets:
31     - userinfo
32   status:
33     conditions:
34     - lastTransitionTime: '2022-05-31T01:26:46Z'
35       lastUpdateTime: '2022-05-31T01:26:46Z'
36       reason: ValidationSuccessful
37       status: 'True'
38       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

```
1  apiVersion: cnfw.cisco.com/v1
2  kind: IPv4SubnetPool
3  metadata:
4    annotations:
5      aws.cnfw.cisco.com/interface-index: '3'
6      aws.cnfw.cisco.com/route-table-id: rtb-0286c00532732c282
7      aws.cnfw.cisco.com/type: route-table
8    finalizers:
9      - sfcn.cisco.com/ipv4subnetpoolreconciler_finalizer
10   generation: 1
11   name: ravnpool
12   namespace: sfcn-system
13   resourceVersion: '51894'
14   uid: 4d2b152e-f788-4669-a7ed-76221ffd9c85
15   selfLink: /apis/cnfw.cisco.com/v1/namespaces/sfcn-system/ipv4subnetpools/ravnpool
16  spec:
17    address: 10.10.0.0
18    rangeStart: 1
19    subnetPrefix: 24
20    supernetPrefix: 16
21  status:
22    assigned:
23      - ip-10-37-11-14.us-west-2.compute.internal/10.10.1.0/24
24      - ip-10-37-58-96.us-west-2.compute.internal/10.10.0.0/24
25    observedAWSRouteTableState:
26      interfaceIndex: 3
27      routeTableId: rtb-0286c00532732c282
28    observedGeneration: 1
29    summary: 'PoolSize: 256, Number of hosts: 254, Assigned: 2, Unassigned: 0'
30
```

# 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

```
1  apiVersion: cnfw.cisco.com/v1
2  kind: Counter
3  metadata:
4    name: sample
5  spec:
6    start: 3
7    allocatedPerNode: 2
8  ---
9  apiVersion: cnfw.cisco.com/v1
10 kind: ASAConfiguration
11 metadata:
12   name: networks
13 spec:
14   order: 1
15   counters:
16     - sample
17     cliLines: |
18       {{range .counters.sample}}
19         object network n{{.}}
20         host 8.8.3.{{.}}
21       {{end}}
22 ---
23
```

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 ASA configuration
- Spec
  - Subnet
  - Netmask Prefix
- Status
  - Assigned IPV4 Addresses

```
1  apiVersion: cnfw.cisco.com/v1
2  kind: IPv4AddressPool
3  metadata:
4    name: ipv4addresspoolsample
5    namespace: default
6  status:
7    observedGeneration: 1
8    summary: 'PoolSize: 256, Assigned: 0, Unassigned: 0'
9  spec:
10   address: 10.20.30.0
11   networkPrefix: 24
12  ---
13  apiVersion: cnfw.cisco.com/v1
14  kind: ASAConfiguration
15  metadata:
16    name: asaconfiguration-sample
17  spec:
18    order: 1
19    description: "example configuration"
20    ipv4AddressPools:
21      - "ipv4addresspool1"
22      - "ipv4addresspool2"
23    ipv4SubnetPools:
24      - "ipv4subnetpool1"
25      - "ipv4subnetpool2"
26    cliLines:
27      interface GigabitEthernet0/0
28      | nameif testinf
29      | ip address {{.ipv4AddressPools.ipv4addresspool1.assignedIP}} 255.255.255.0
30      | exit
31      | object network asac
32      | | host 8.8.8.{{next "counter1"}}
33      | | dhcpd address {{.ipv4SubnetPools.ipv4subnetpool2.assignedRange}} inside
```

# Deployment & Configuration



# Cisco Secure Firewall Cloud Native

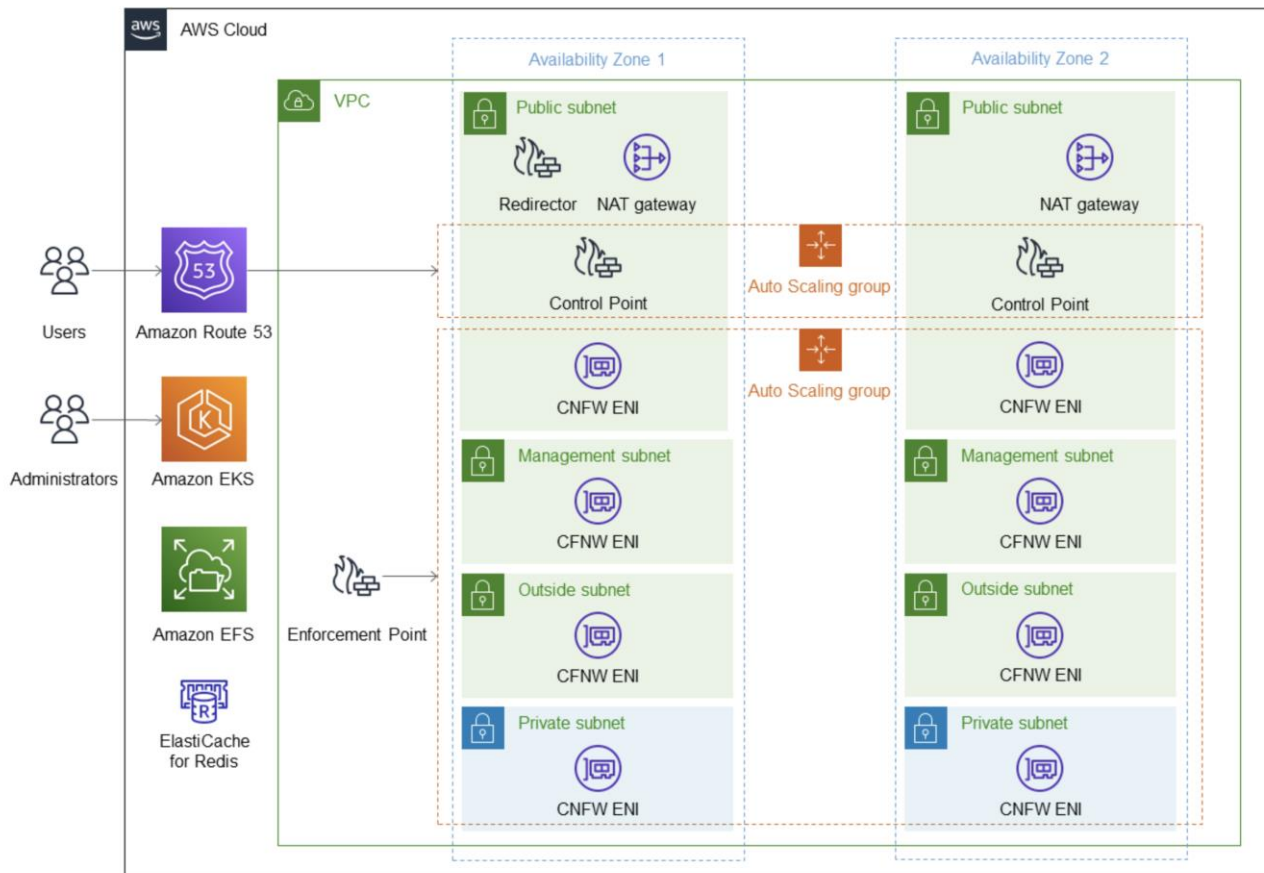
## Deployment

- ▶ 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/>

The screenshot shows the AWS APN blog interface. At the top, there's a navigation bar with the AWS logo, menu items like 'Products', 'Solutions', 'Pricing', 'Documentation', 'Learn', 'Partner Network', 'AWS Marketplace', 'Customer Enablement', 'Events', and 'Explore More', along with 'Contact Us', 'Support', 'My Account', 'Sign In', and a 'Create an AWS Account' button. Below the navigation is a search bar and filters for 'Blog Home', 'Category', 'Edition', and 'Follow'. The main content area features the article title 'Manage Multi-Tenant Remote Access with Cisco Secure Firewall Cloud Native on Amazon EKS' by Muffadal Quettawala and Anubhav Swami, dated 13 JUN 2022. The article text discusses modernizing application workloads into containerized forms and the benefits of Cisco Secure Firewall Cloud Native (SFCN) as a cloud-native security solution. A Cisco logo is displayed in a box. To the right, there are 'Resources' and 'Follow' sections. The 'Resources' section lists links for 'Why Work with AWS Partners', 'Training for Partners', 'AWS Competency Partners', 'Managed Service Providers (MSPs)', 'Partner Central Login', 'Case Studies and References', and 'AWS Sponsorship Opportunities'. The 'Follow' section includes checkboxes for 'AWS Partners', 'AWS Cloud', 'APN LinkedIn', 'APN YouTube', 'RSS Feed', and 'APN Email Updates'. At the bottom right, there is a diagram showing a cloud with a plus sign, a laptop displaying a network diagram, and two user icons.

# 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.



**Security Operations**

**Managed Detection and Response Services**

**Security, Orchestration, Automation and Response**

**Incident Response and Remediation Services**

**SECURE X (XDR)**

**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** | **PRIVATE CLOUD EDGE (MSP or CUSTOMER)**  
Threat Protection | Secure Access Control | Managed Remote Access | 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**

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

**On-Premises**

**SASE/SDWAN** | **ZERO TRUST**

Scalable | Flexible | Visibility | Comprehensive Security | Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

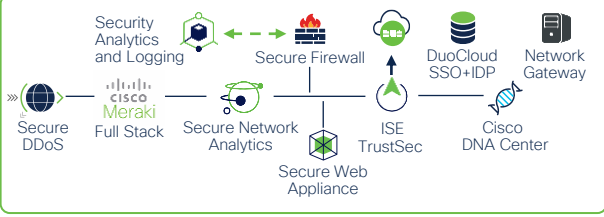
**Network Edge**

- cisco 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



**Application Security**

**ZERO TRUST**

Policy | API Security  
Application Segmentation  
Run-time Application Security

**Application Security Stack**

- Cloud Native Security (SCN)
- API 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](http://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

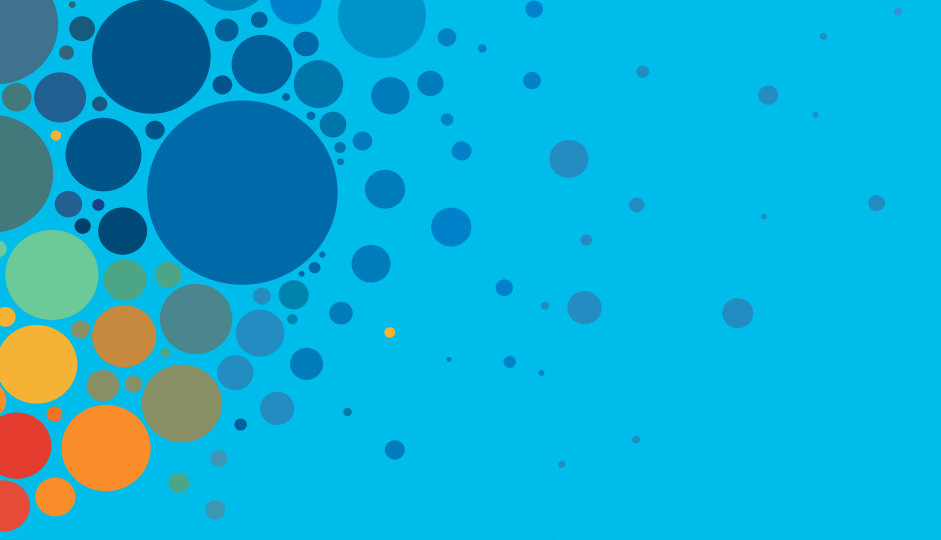
### Cisco Guided Study Groups

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](http://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*

ALL IN

#CiscoLive