
cisco Live!
ALL IN

The bridge to possible

Deploy and manage securely in AWS your 3 tiers App in 45 mins

Fabien Gandola – TSA Cyber Security for EMEA

BRKSEC-1831

Cisco Webex App

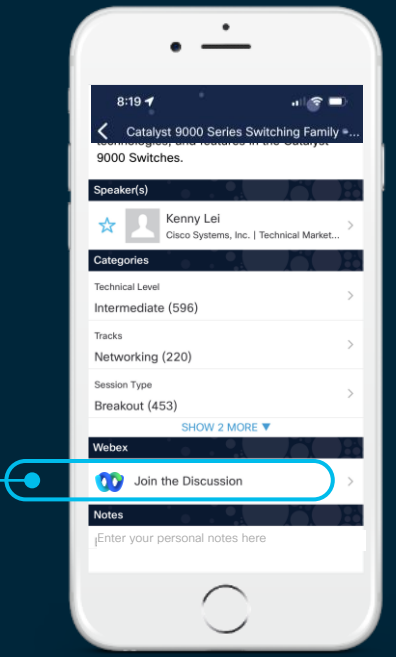
Questions?

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://ciscolive.ciscoevents.com/ciscolivebot/# BRKSEC-1831

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

What to expect and not to expect ?

- No deep dive AWS
- No deep dive Security
- No all scenarios
- No configuration
- No troubleshooting

- Introduction to key concepts of AWS
- Questions related to security to deploy an application in AWS
- Some Cisco security services useful

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Security Challenges in public cloud
- Use case of today
- What type of service and architecture to deploy my application ?
- How do I perform access control and Segmentation ?
- How do I insert NGFW ?
- How do I monitor my public Cloud ?
- *What about Remote Access ? (Hiden)*
- Conclusion

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

About me...

Fabien Gandola – fgandola@cisco.com

TSA Cyber Security EMEA

23 years in Cisco

TAG leader of Cloud Native Security and Application Security

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Use Cases

- Enterprise with on prem DC launching a new service

- New company

Cisco Live 2022 FOR REFERENCE TECSEC-2011

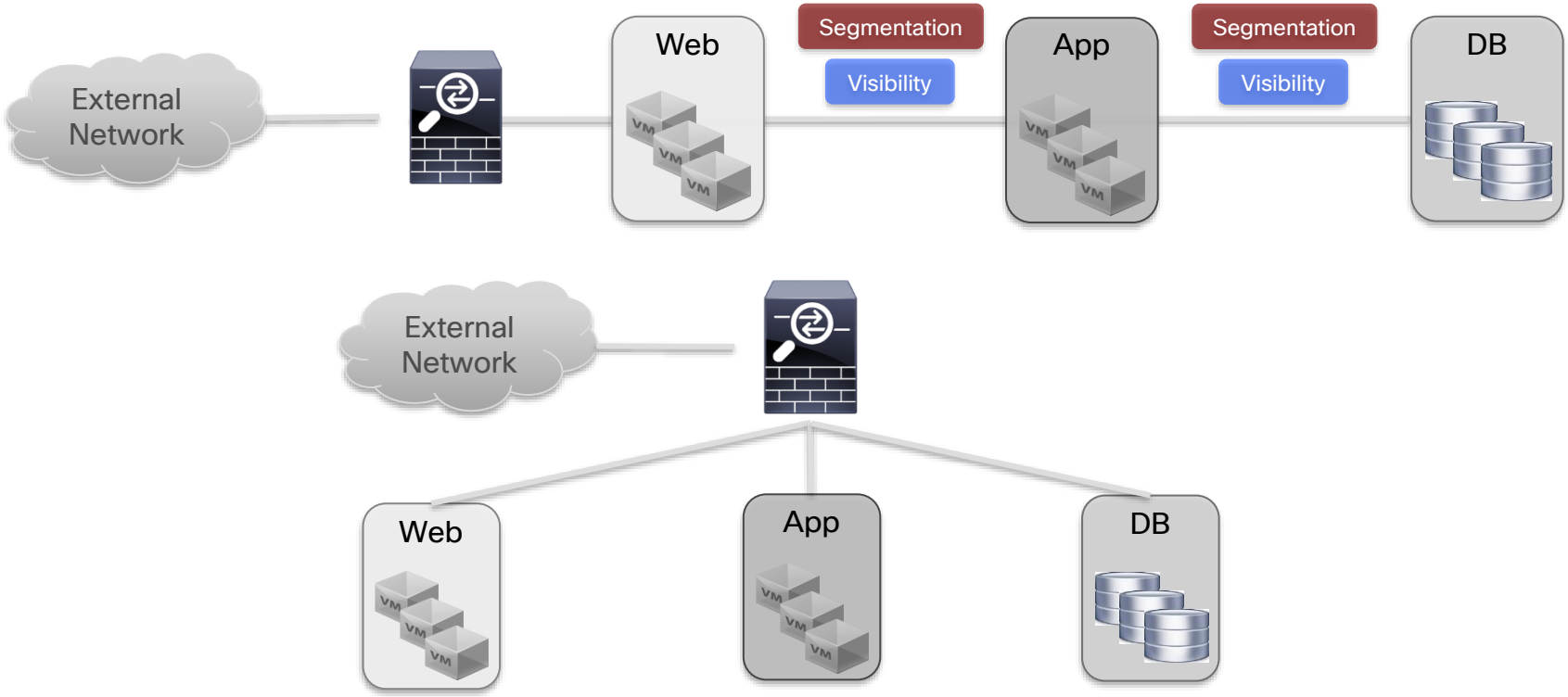
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

The application

- FabAstro (store images)
  - Public can access images
  - Users can add their images
  - Admin manage the app
- 3 tiers:
  - Static Web page
  - Dynamic part with web + php and business logic
  - Database with mysql

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

What an application looks like in a traditional on-prem DC

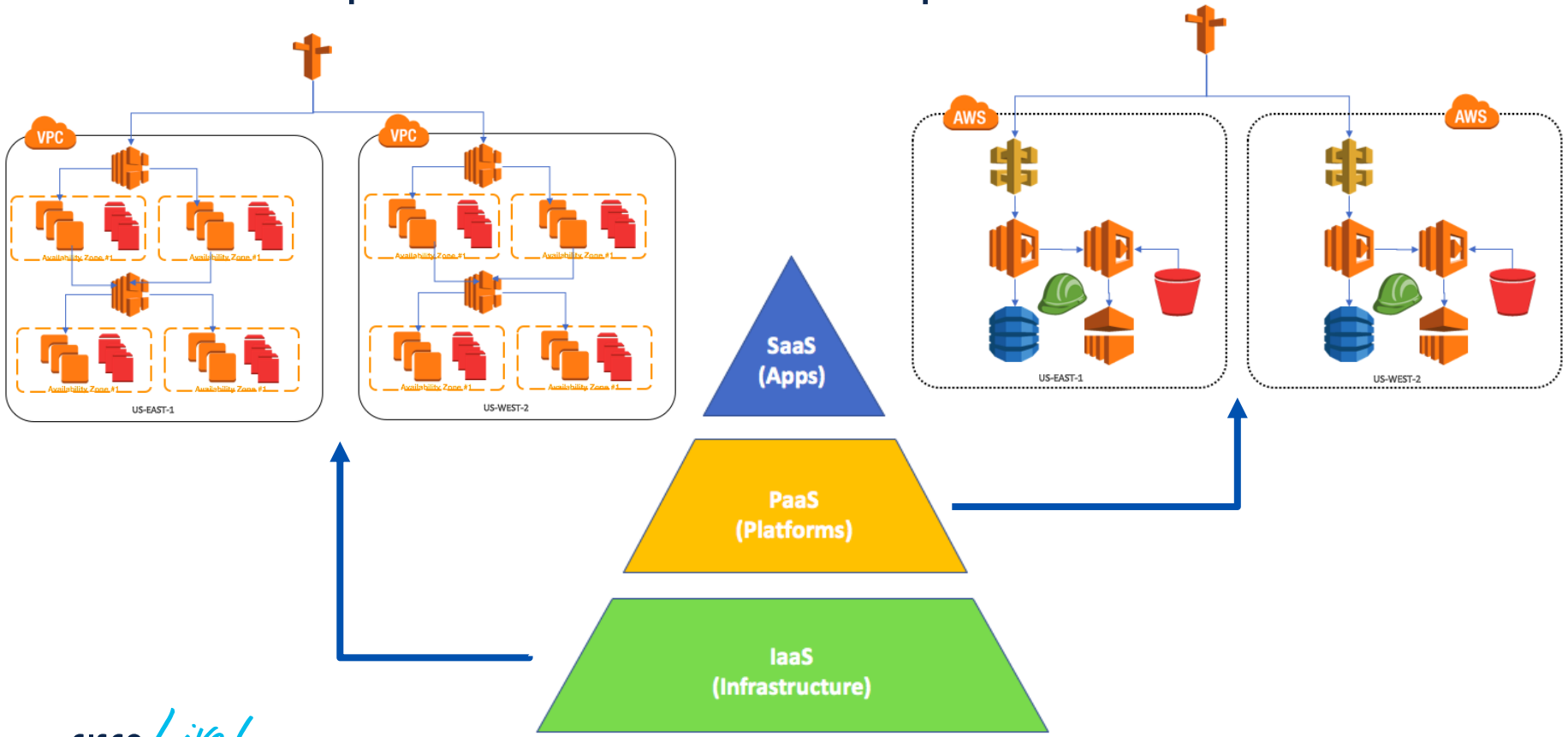


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

What type of service and architecture to deploy my application ?

- Infrastructure as a Service
- Platform as a Service
- Serverless

IaaS compared to PaaS Compared to SaaS



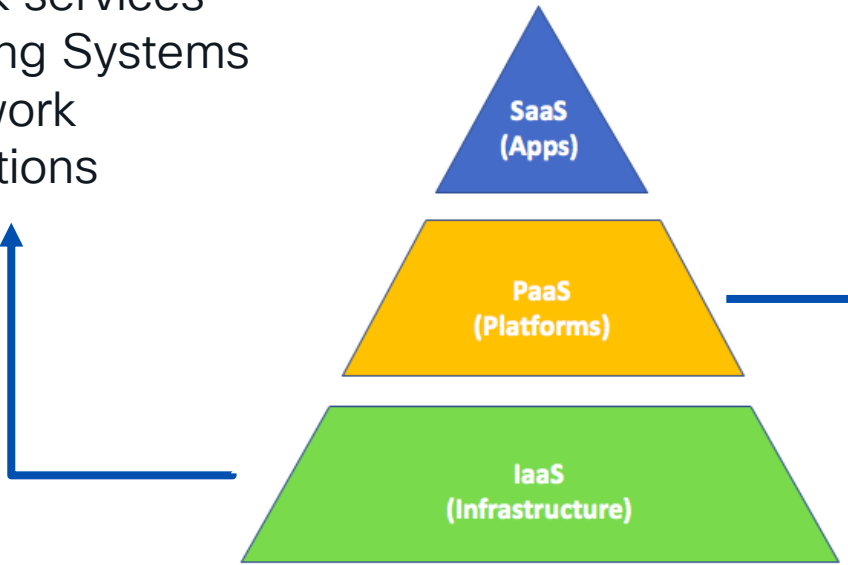
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

IaaS compared to PaaS Compared to SaaS

Manage :
- Nothing

Manage :
- Network services
- Operating Systems
- Framework
- Applications

Manage :
- Network limited
- Applications



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

What do all the XaaS options mean?

SaaS (Software as a Service)	FaaS (Functions as a Service)	PaaS (Platform as a Service)	CaaS (Container as a Service)	IaaS (Infrastructure as a Service)	On-Prem (private cloud)
Functions	Functions	Functions	Functions	Functions	Functions
Applications	Applications	Applications	Applications	Applications	Applications
Runtime	Runtime	Runtime	Runtime	Runtime	Runtime
Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers
Operating System	Operating System	Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking	Networking

Cloud Service Provider Responsible

Customer Responsible

Customer and Cloud Service Provider have Shared Responsibility

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Security Solutions

Identity

- AWS Identity & Access Management (IAM)
- AWS Organizations
- AWS Cognito
- AWS Directory Service
- AWS Single Sign-On

Detective control

- AWS Security Hub
- AWS CloudTrail
- AWS Config
- Amazon CloudWatch
- Amazon GuardDuty
- VPC Flow Logs

Infrastructure security

- AWS Control Tower
- Amazon EC2 Systems Manager
- AWS Shield
- AWS Web Application Firewall (WAF)
- Amazon Inspector
- Amazon Virtual Private Cloud (VPC)

Data protection

- AWS Key Management Service (KMS)
- AWS CloudHSM
- Amazon Macie
- Certificate Manager
- Server Side Encryption

Incident response

- AWS Config Rules
- AWS Lambda

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Securing the Cloud

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

FabAstro Application in AWS

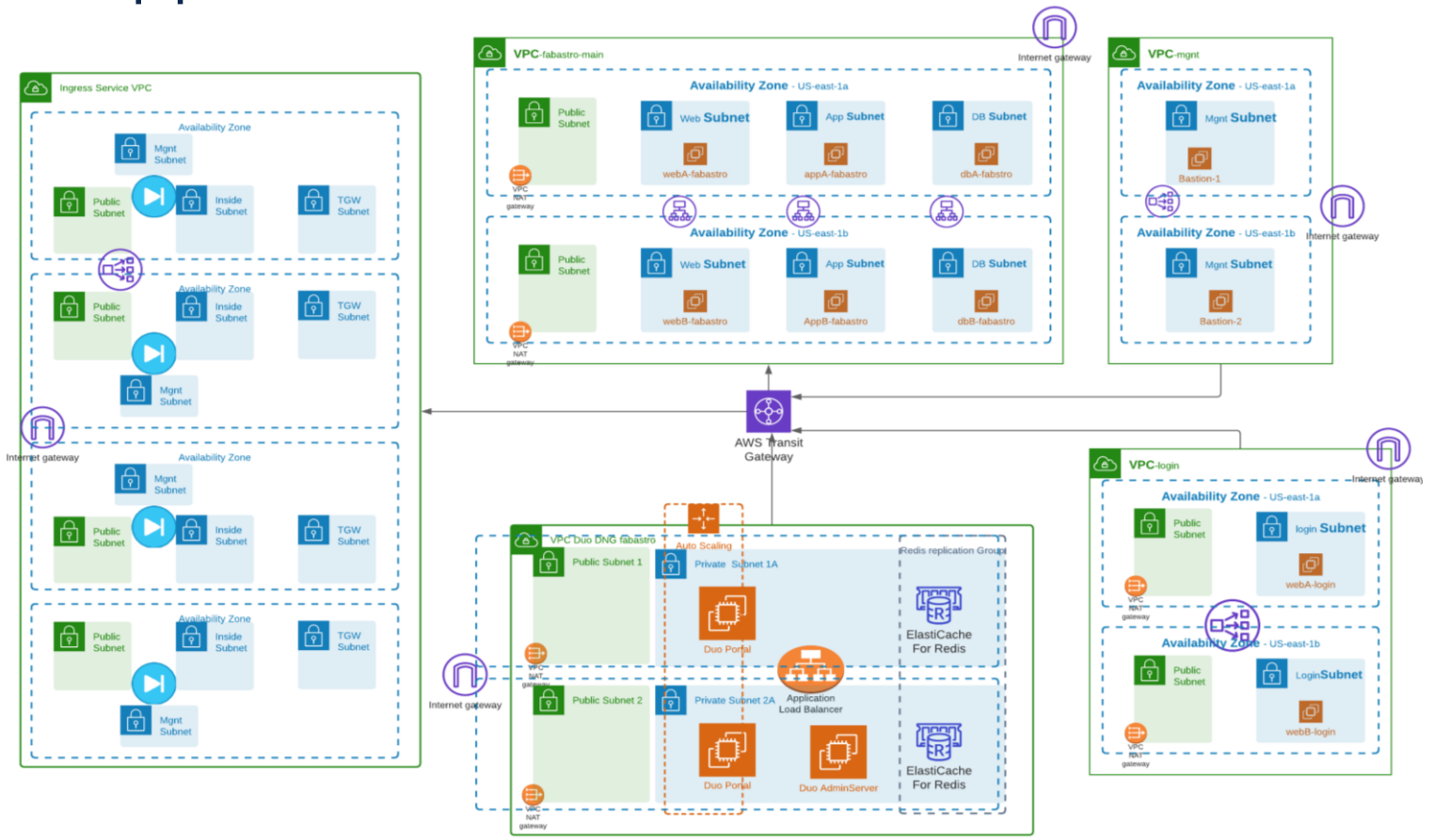
Amazon S3

AWS Route 53

AWS Certificate Manager

AWS CloudFormation

AWS IAM



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

First Step in AWS... IAM, EC2 and VPC

AAA with AWS

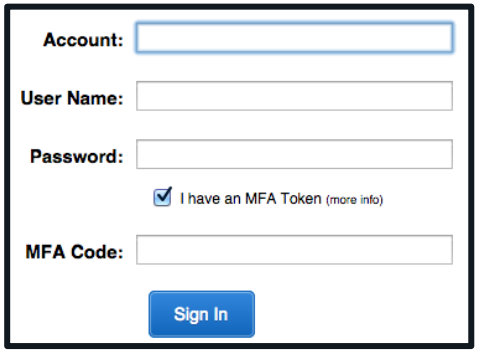
Authenticate	Authorize	Audit
IAM Username/Password Access Key (+ MFA) Federation	IAM Policies	CloudTrail

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Identity Authentication

AWS Management Console

Login with **Username/Password** with optional **MFA** (Cisco Secure Access)



For time-limited access: **a Signed URL can** provide temporary access to the Console

API access

Access API using **Access Key + Secret Key**, with optional MFA

ACCESS KEY ID

Ex: `AKIAIOSFODNN7EXAMPLE`

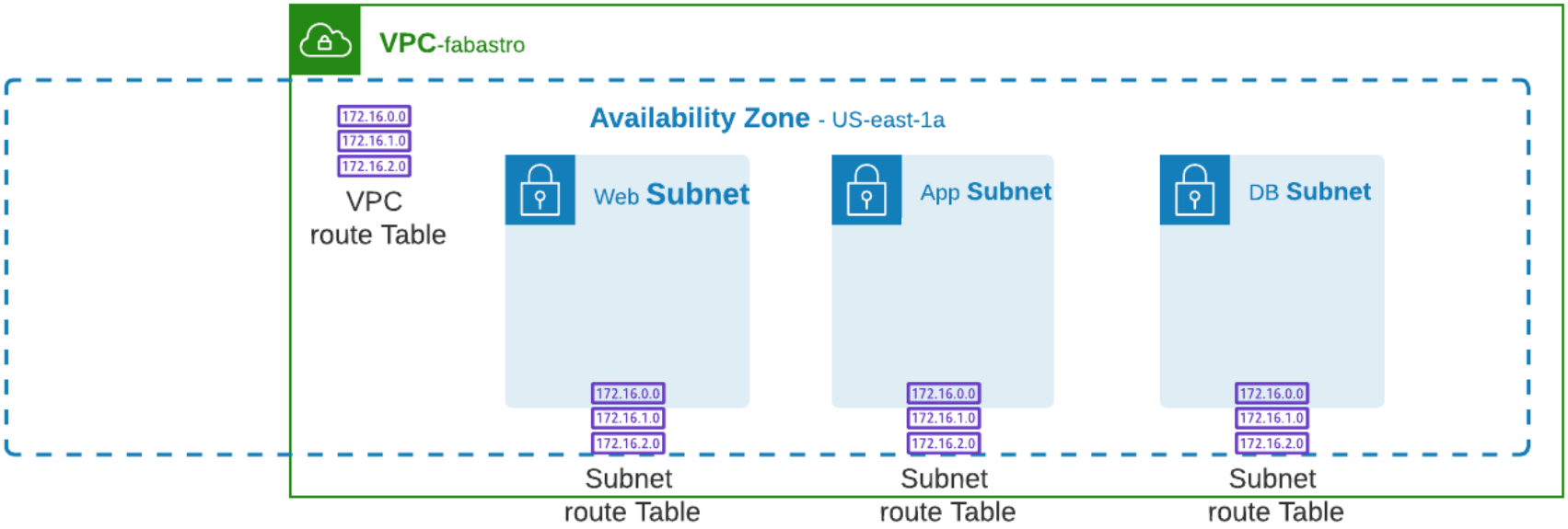
SECRET KEY

Ex: `UtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

For time-limited access: Call the AWS Security Token Service (STS) to get a temporary AccessKey + SecretKey + session token

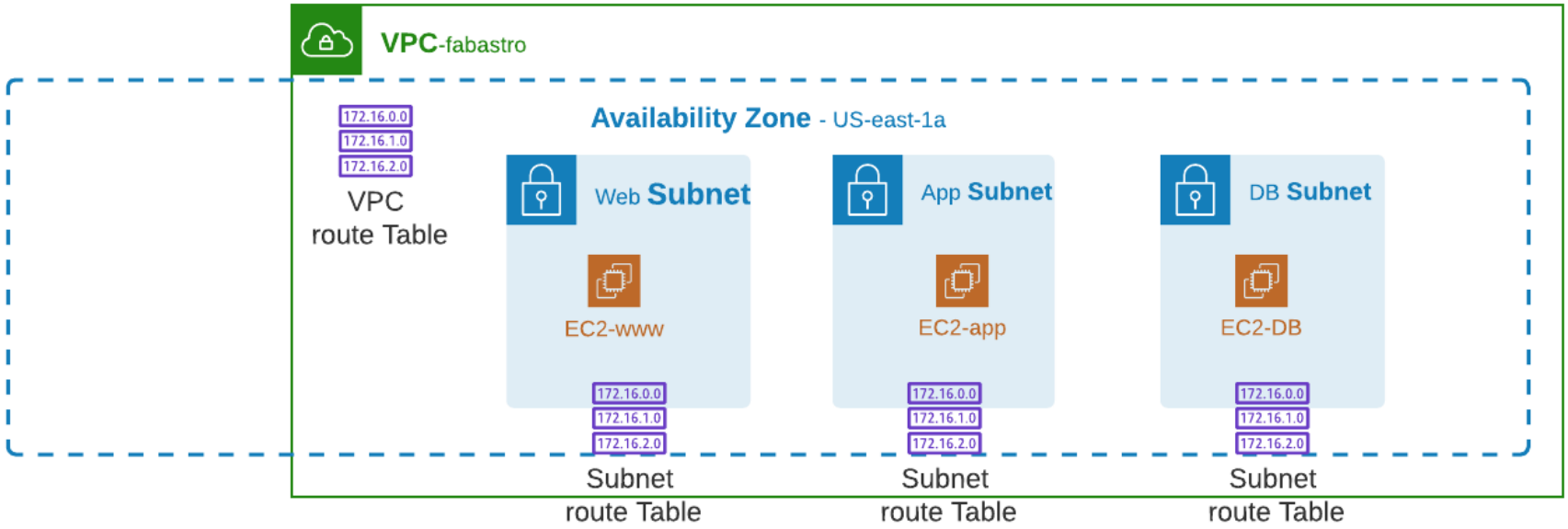
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

My VRF… VPC sort of (actually Route Tables)



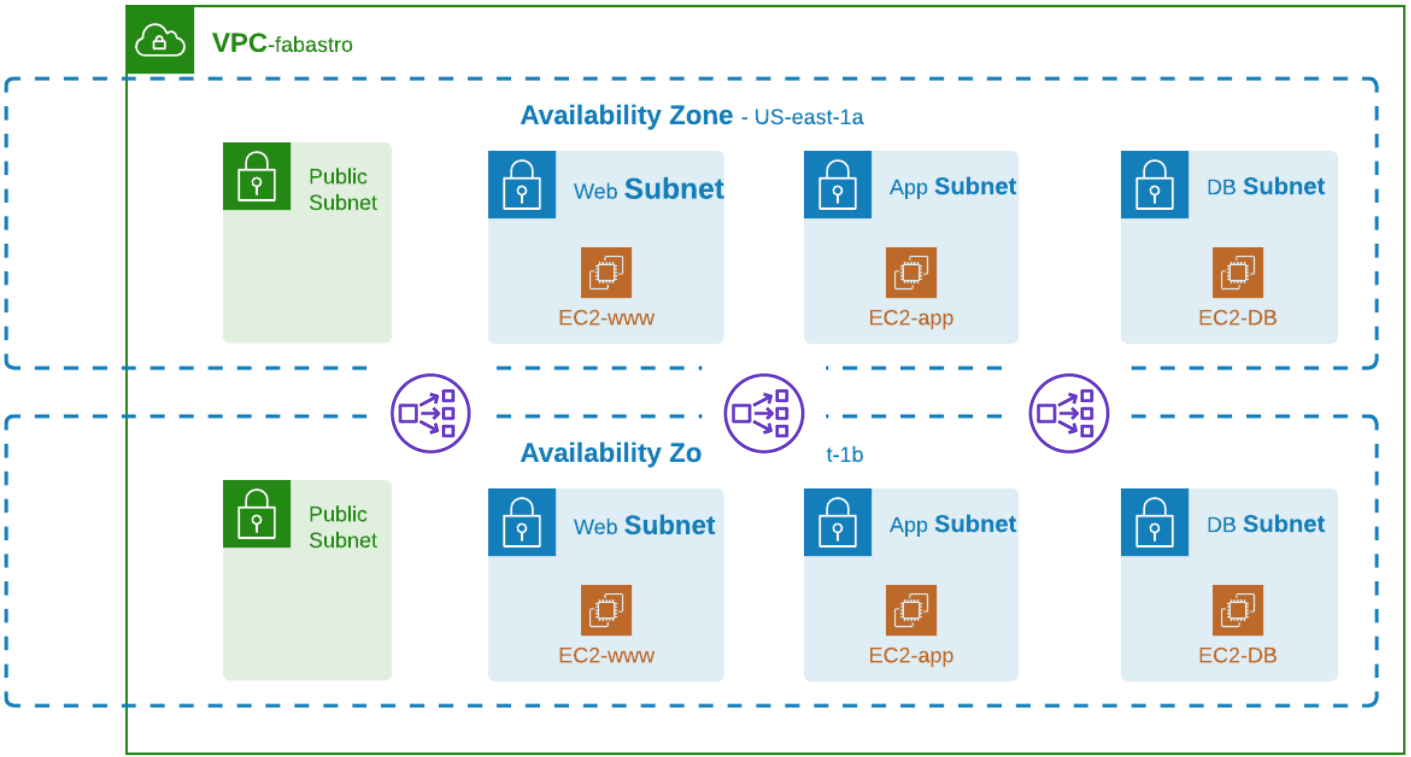
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

In AWS IaaS… my workloads = Instances



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

HA with multiple AZ and LB



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

How do I perform access control and Segmentation ?

- AWS security Groups at Instance level
- AWS ACLs at Subnet level
- Network Firewall
- Host Security

But first : WHY access control ?

Stealthwatch Cloud has discovered 1 new or updated alert on your network since our last email to you. We have included the

Alert	Source	Time	Description
Inbound Port Scanner	Network	Nov. 27, 2020, 10:19 a.m.	Device was port scanned by an external device. T

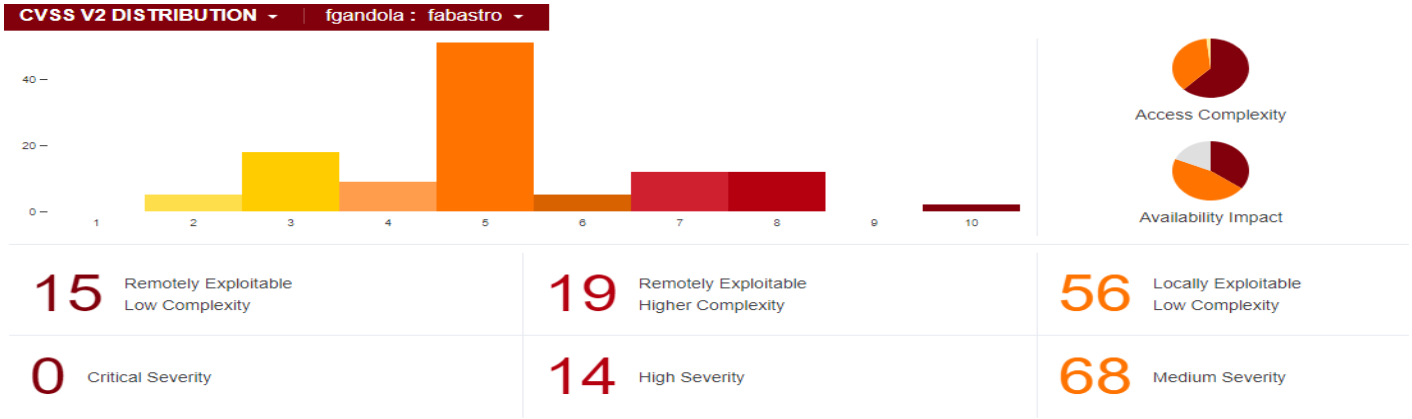
Alert	Source	Time	Description
Excessive Access Attempts (External)	Bastion_Host_1 (i-0f5c16650ace2e7ac)	Nov. 27, 2020, 7 a.m.	Device has many failed access attempts from an external device. For e The alert uses the Multiple Access Failures observation and may indica
Excessive Access Attempts (External)	virtualmachines/jumphost	Nov. 27, 2020, 7 a.m.	Device has many failed access attempts from an external device. For e The alert uses the Multiple Access Failures observation and may indica
Excessive Access Attempts (External)	virtualmachines/jumpbox	Nov. 27, 2020, 7 a.m.	Device has many failed access attempts from an external device. For e The alert uses the Multiple Access Failures observation and may indica

Alert	Source	Time	Description
Persistent Remote Control Connections	bastion1	Nov. 26, 2020, 11:59 p.m.	Device is receiving persistent connections from a new host observations and may indicate that a firewall rule or ACL is

--

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

CSW Vulnerability Assessment

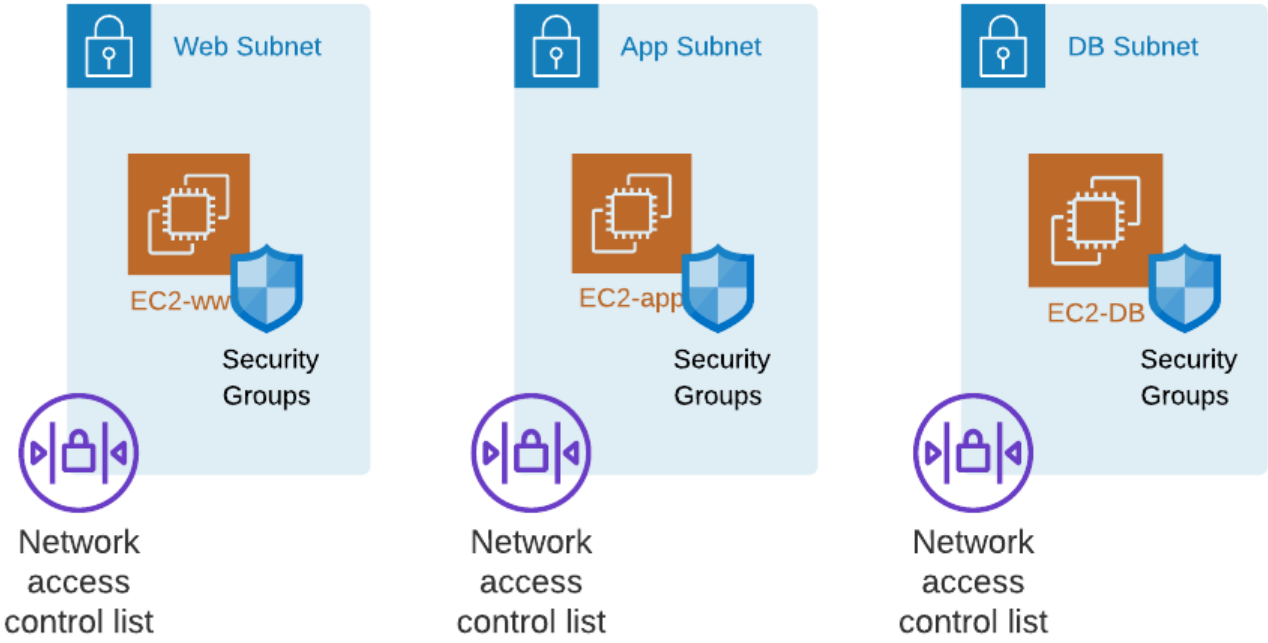


CVE	Score (V2)	Score (V3)	Severity (V2)	Base Severity (V3)	Access Vector (V2)	Access Complexity (V2)
CVE-2019-13638	9.3	7.8	HIGH	HIGH	NETWORK	MEDIUM
CVE-2018-20969	9.3	7.8	HIGH	HIGH	NETWORK	MEDIUM
CVE-2020-25643	7.5	7.2	HIGH	HIGH	NETWORK	MEDIUM
CVE-2020-10878	7.5	8.6	HIGH	HIGH	NETWORK	LOW
CVE-2020-12464	7.2	6.7	HIGH	MEDIUM	LOCAL	LOW
CVE-2020-12465	7.2	6.7	HIGH	MEDIUM	LOCAL	LOW

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Segmentation solutions

Security Groups and Network Access list



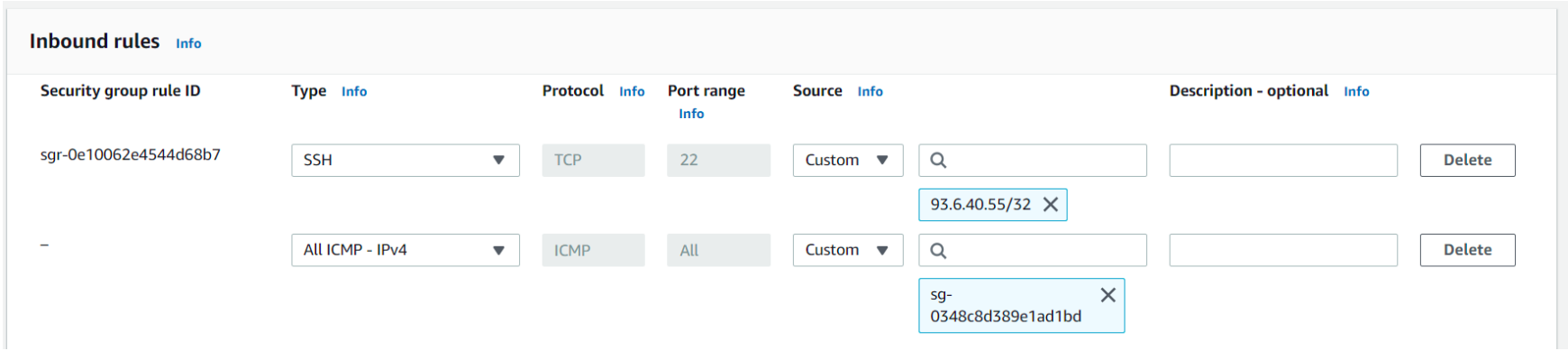
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network ACL and Security Groups

	 Network ACLs	 Security Groups
Scope	All the instances of a subnet	The instance it is attached
State	Stateless	Stateful
Rules action	Allow/Deny	Allow
Rule Process Order	Order matters. First match applied	All rules evaluated before decision
Occurence	Only 1 per Subnet	Multiple per Instance

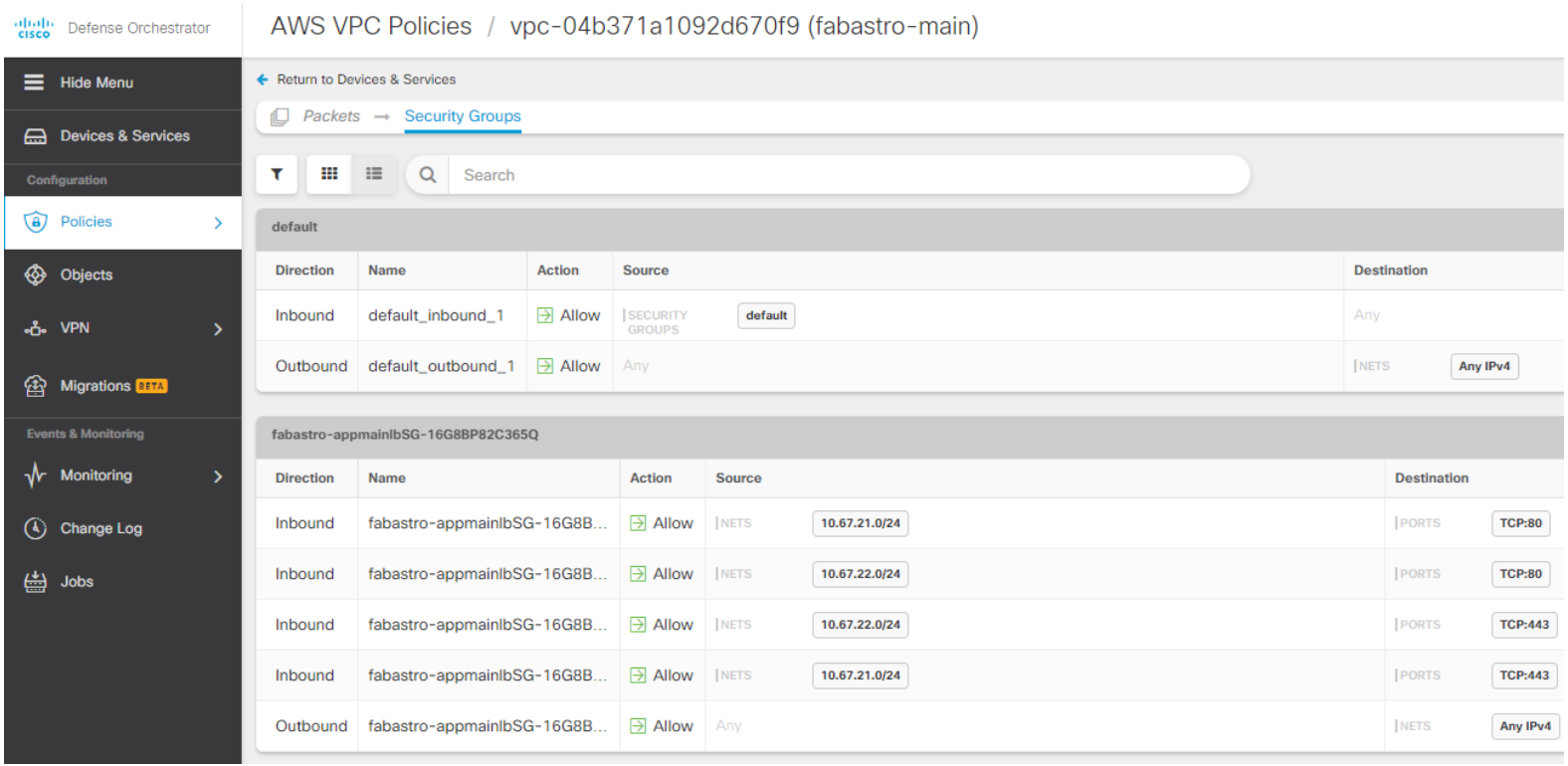
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use security group as Source in Policy



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Groups in CDO



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

How do we address this with Secure Workload?

Contain lateral movement

Microsegmentation

Continuously track security compliance

Policy compliance

Identify behavior anomalies

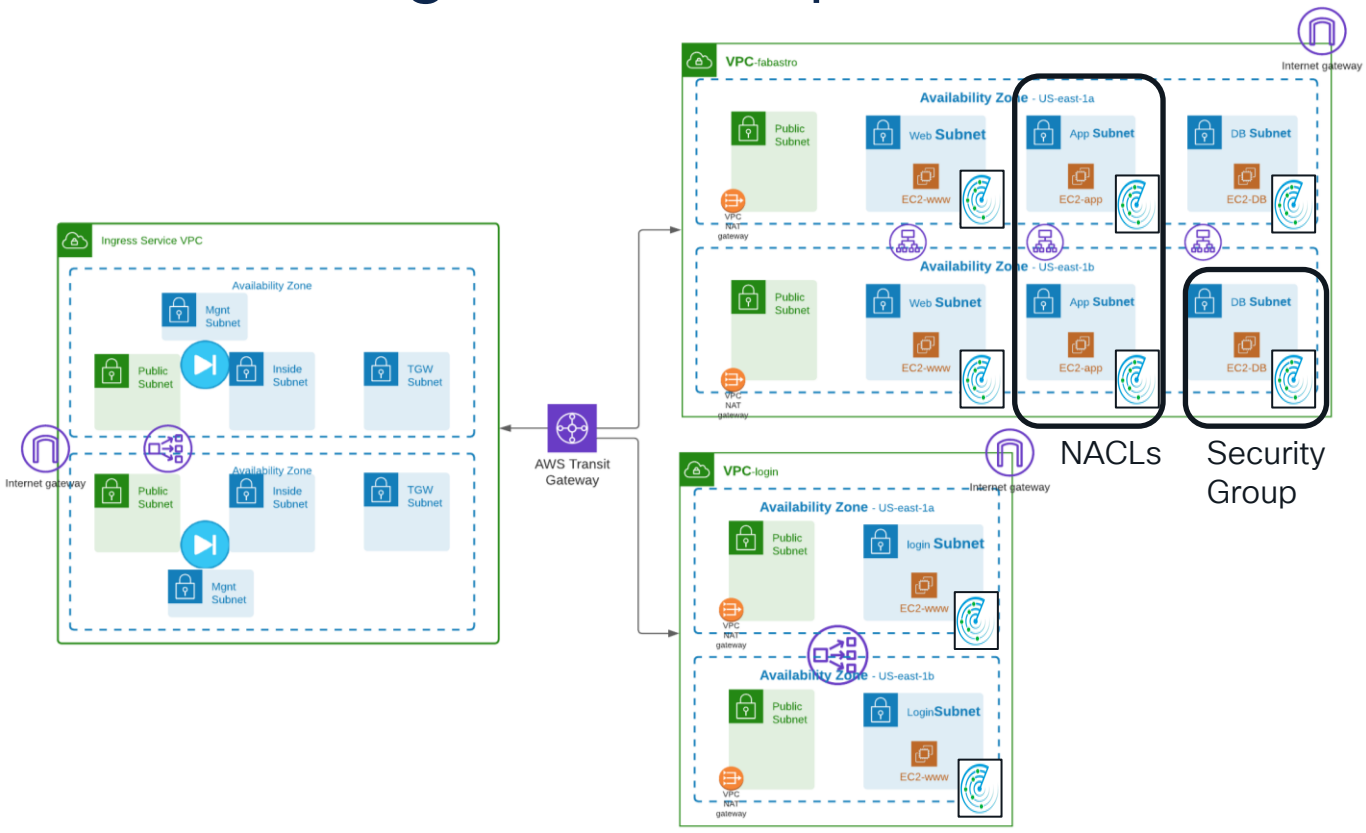
Process and communication

Reduce attack surface

Software vulnerability

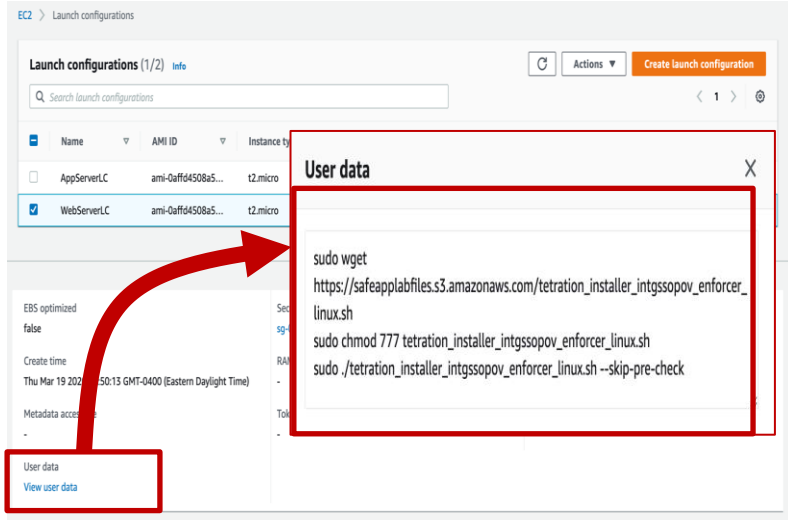
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Another segmentation point?



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

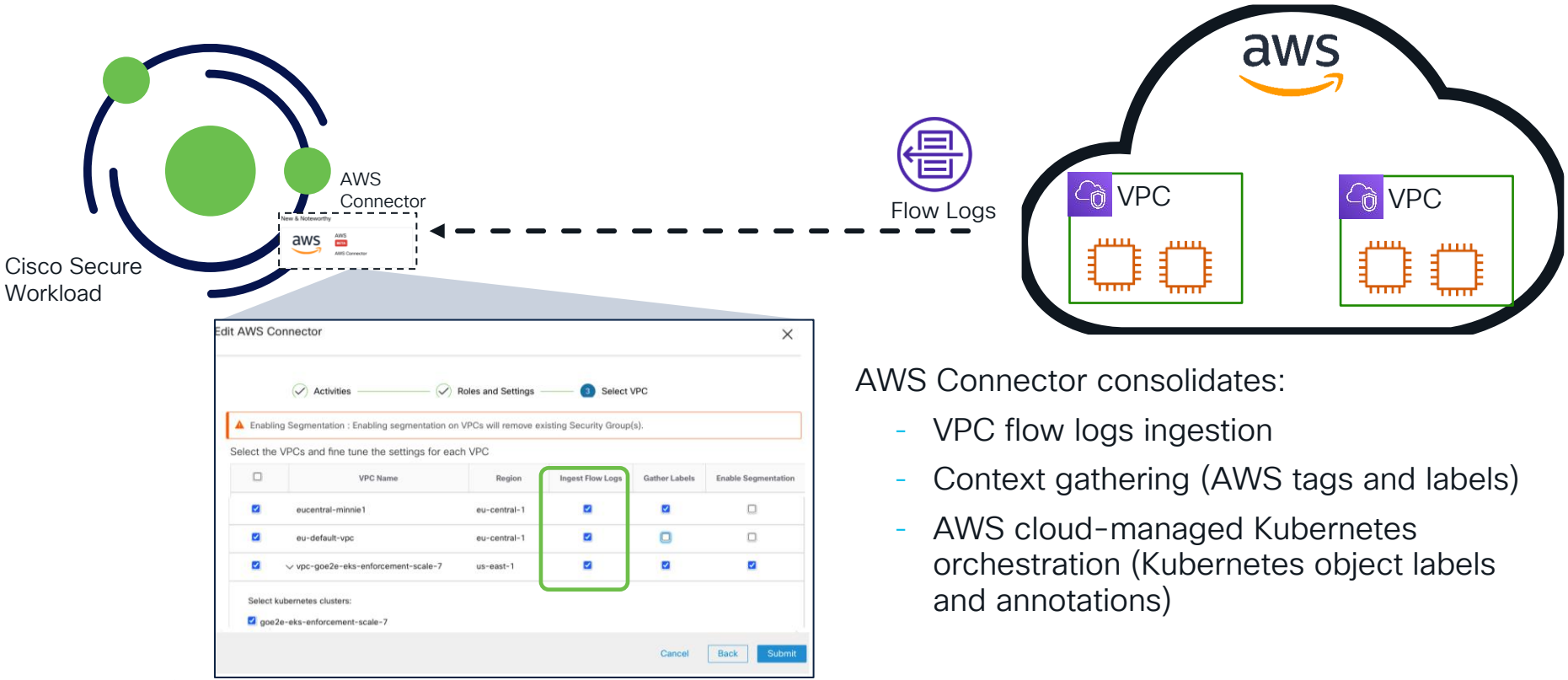
Deploy Enforcement Agent using AWS Launch Config or CloudFormation




```
webbfabastroinstance:
  Type: AWS::EC2::Instance
  DependsOn: NATgw4mainb
  Properties:
    KeyName: aws-Nvirginia-ec2
    ImageId: ami-0885b1f6bd170450c
    InstanceType: t2.micro
    IamInstanceProfile: fabastro_S3access
    SecurityGroupIds:
      - !GetAtt webSecurityGroup.GroupId
    SubnetId: !Ref webfabastroAZb
    UserData:
     Fn::Base64: !Sub |
      #!/bin/bash -ex
      sudo apt update -y
      sudo apt install awscli -y
      sudo apt install apache2  -y
      sudo systemctl enable apache2.service
      sudo systemctl start apache2.service
      sudo apt-get install curl -y
      sudo apt install net-tools
      sudo aws s3 cp s3://fabastro-init/www/index.html /var/www/html
      sudo mkdir /var/www/html/images
      sudo aws s3 cp s3://fabastro-init/www/team_ciel_austral_cropped.png /var/www/html/images
      sudo aws s3 cp s3://fabastro-init/www/landscape_milkyway_cropped.png /var/www/html/images
      sudo aws s3 cp s3://fabastro-init/www/fabastro-diapo.html /var/www/html/images
      sudo aws s3 cp s3://fabastro-init/tetration_installer_fgandola_enforcer_linux_tet-pov-rtp1.sh .
      sudo chmod u+x tetration_installer_fgandola_enforcer_linux_tet-pov-rtp1.sh
      sudo apt install unzip -y
      sudo apt install ipset -y
      sudo apt install rpm -y
      sudo hostnamectl set-hostname webB-fabastro
      sudo hostnamectl
      sudo ./tetration_installer_fgandola_enforcer_linux_tet-pov-rtp1.sh
```


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Workload Cloud-Based Sources



AWS Connector consolidates:

- VPC flow logs ingestion
- Context gathering (AWS tags and labels)
- AWS cloud-managed Kubernetes orchestration (Kubernetes object labels and annotations)

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Connector

Ingesting cloud telemetry – VPC flow logs and AWS tags/labels

1

Enable cloud connector and select the required **capabilities**

2

Download and **deploy** the **CloudFormation**, add the AWS API **credentials to** Secure Workload.

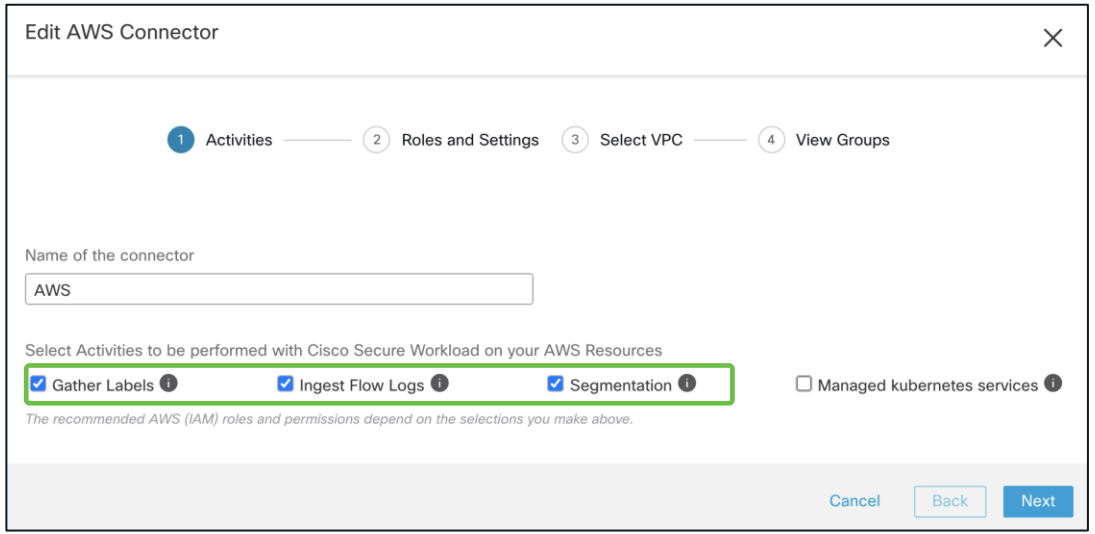
3

Select the AWS **VPCs** and refine the required **capabilities** for each VPC.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Connector – Select Capabilities

1 Enable and configure the connector capabilities

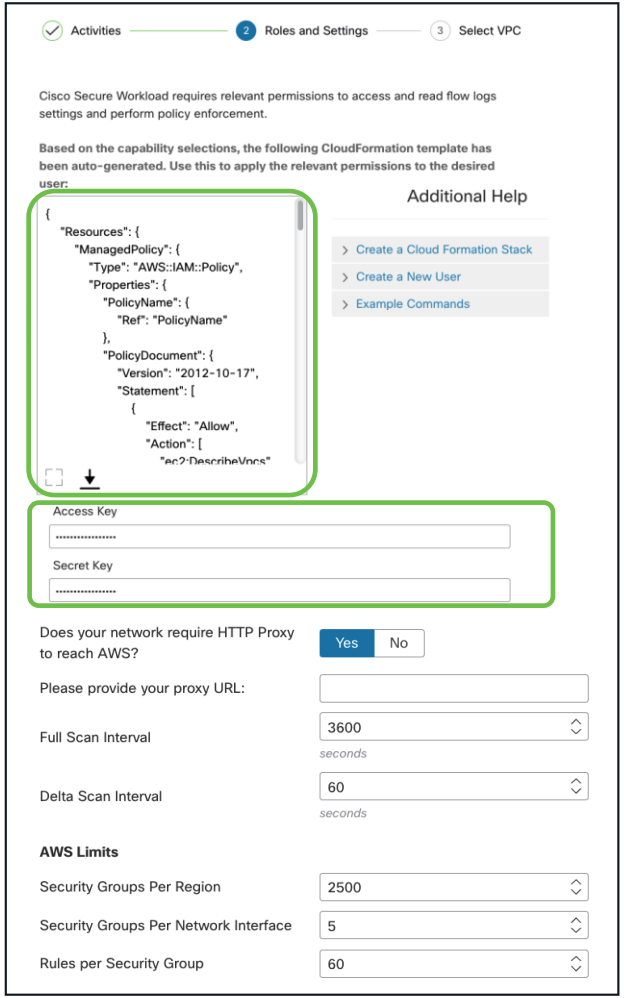


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Connector – IAM

- Secure Workload automatically generates a CloudFormation template with the required IAM policy
- Users can download and deploy the CloudFormation template.
- Proxy and AWS Security Groups limits can be configured

2

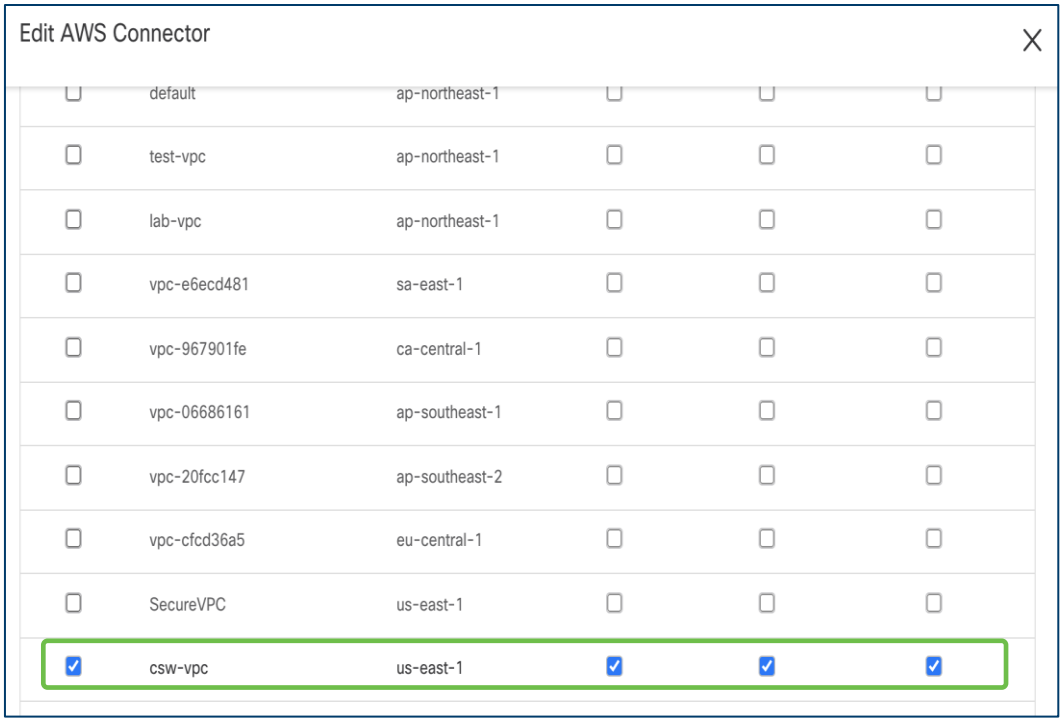


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS Connector – Select VPCs

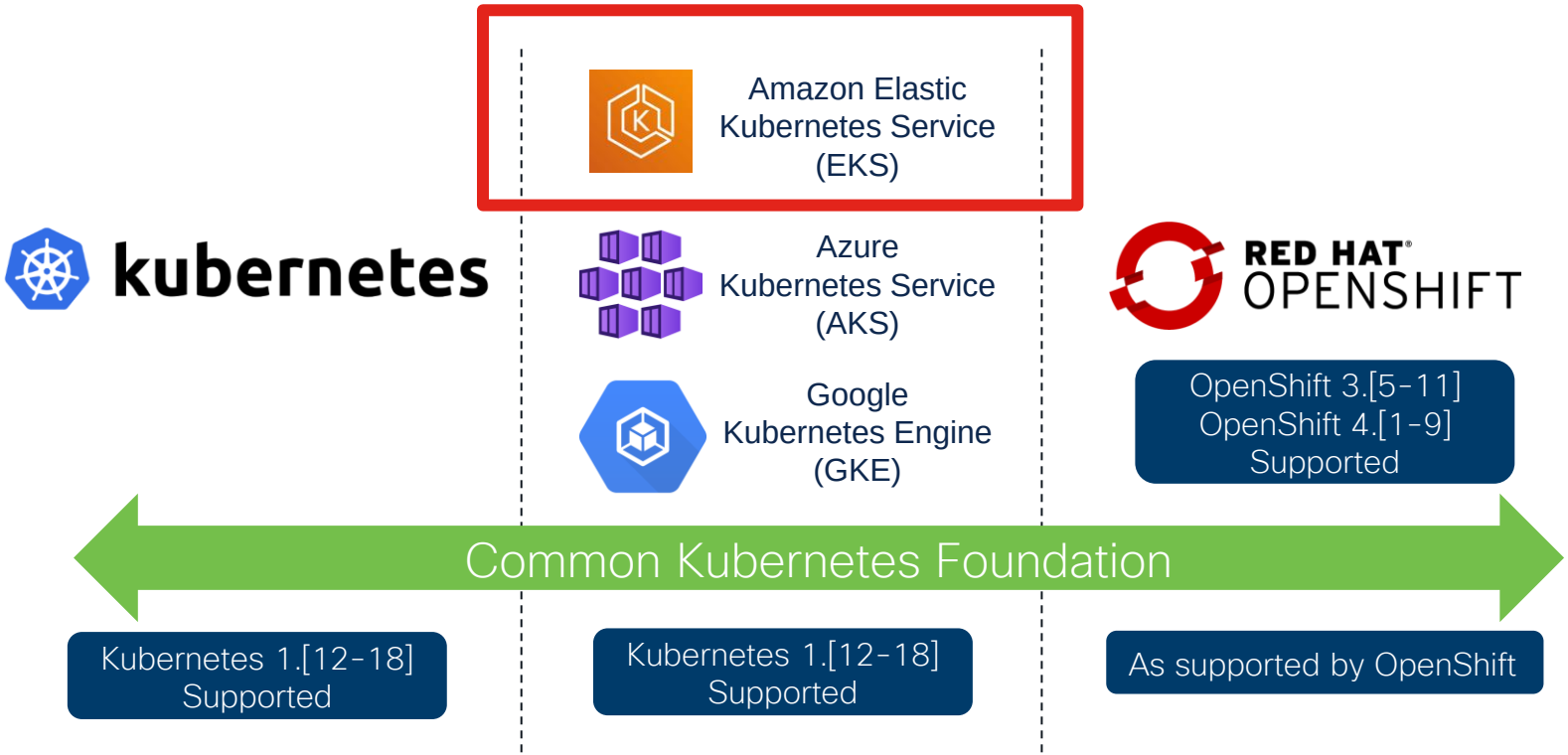
3

- Multiple VPCs can be selected
- Capabilities can be customized and refined for each VPC individually



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

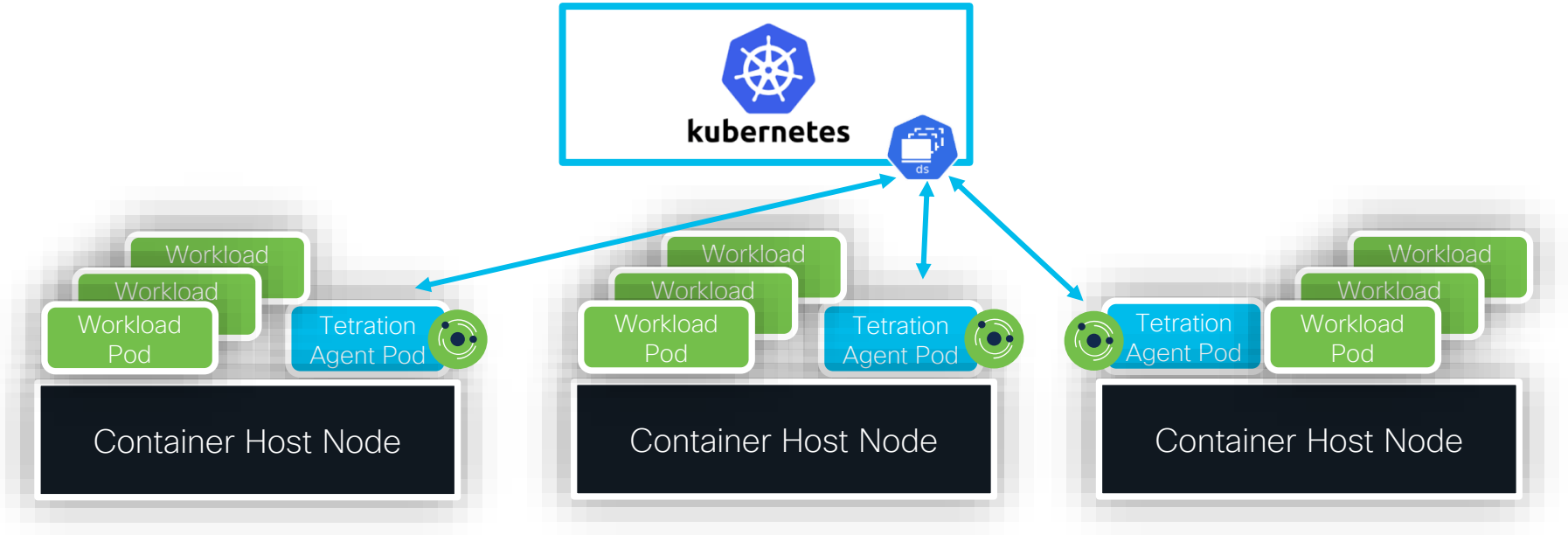
Kubernetes support



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Workload Agents as Daemonset

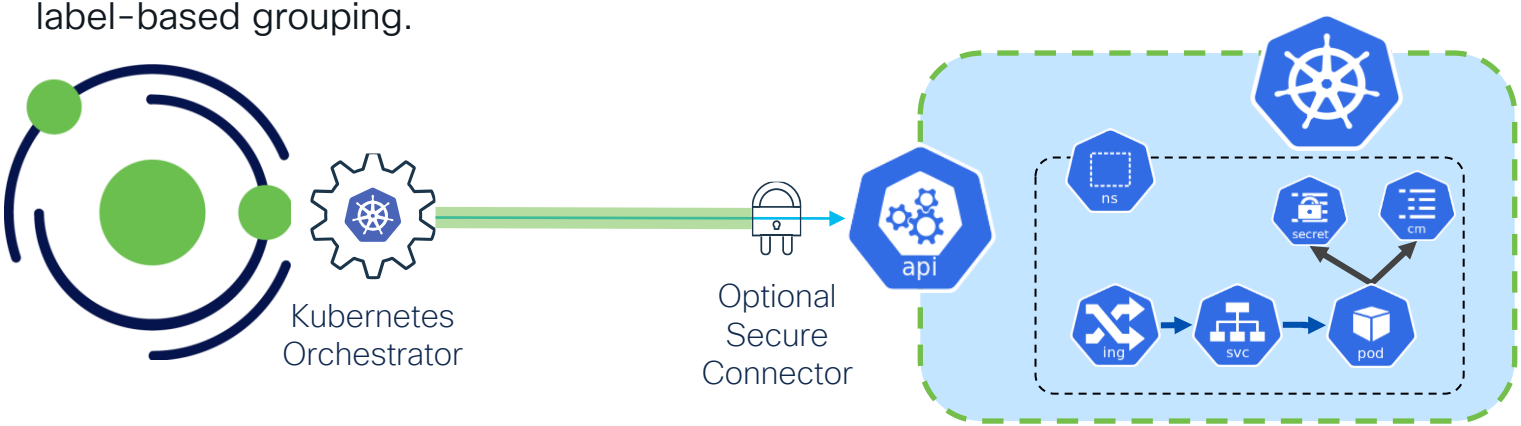
Daemonset pods run on all schedulable nodes in the container cluster



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Kubernetes Metadata Ingest

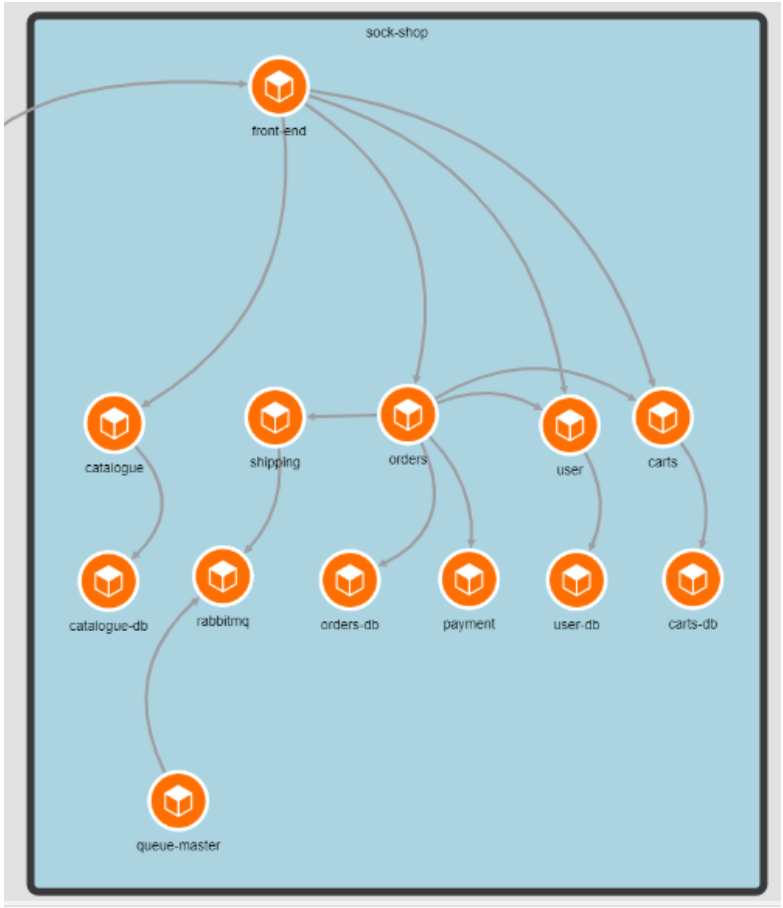
- Kubernetes applies metadata to objects through labels and annotations.
- Integration with Kubernetes is mandatory for container policy generation and enforcement through label-based grouping.



- Kubernetes metadata is ingested through an orchestrator which delivers rich context to the Secure Workload Inventory for dynamic policy enforcement
- Orchestrator connects via Read-Only service account to ingest metadata from all Nodes, Pods and Services to apply as inventory labels.

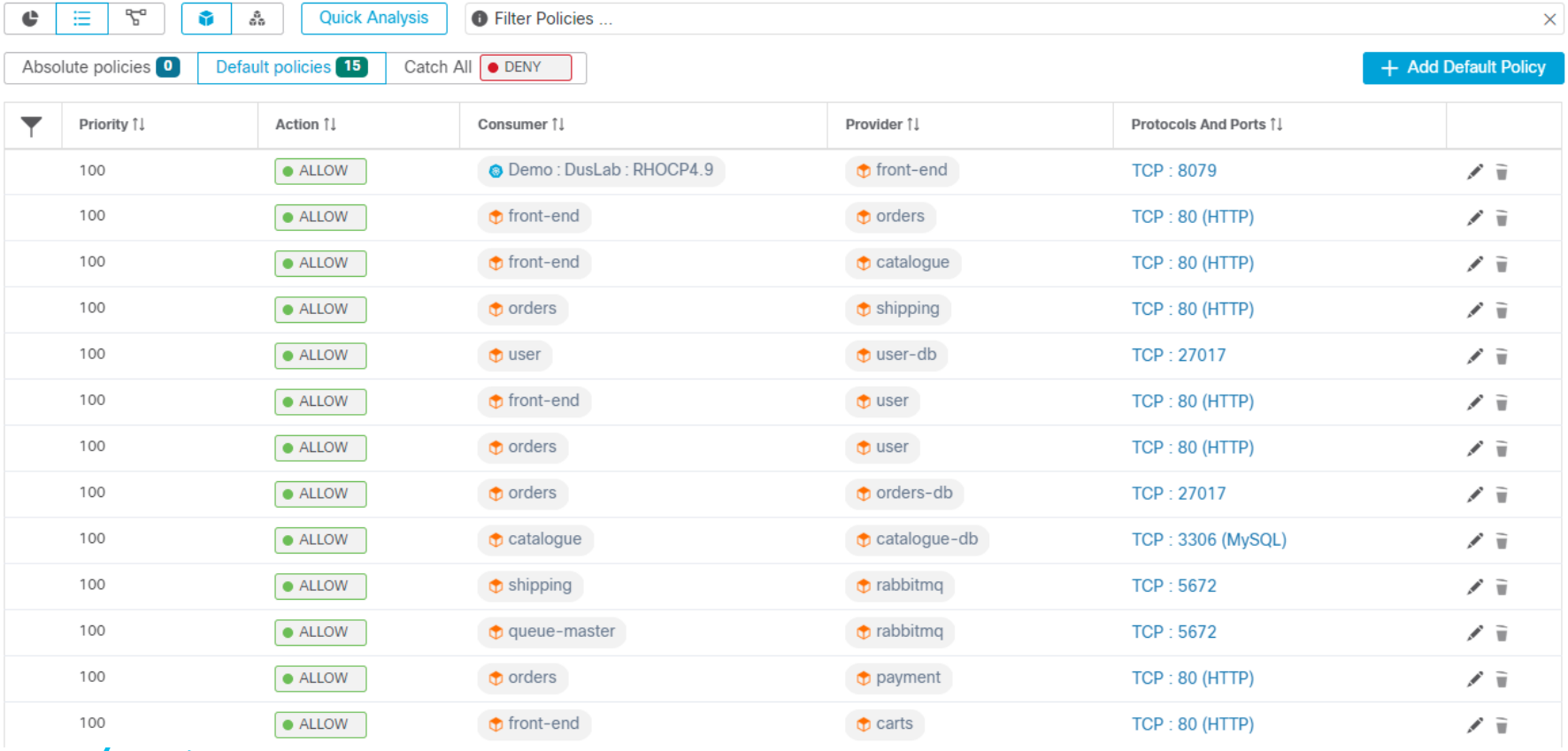
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Canvas view of my policy



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

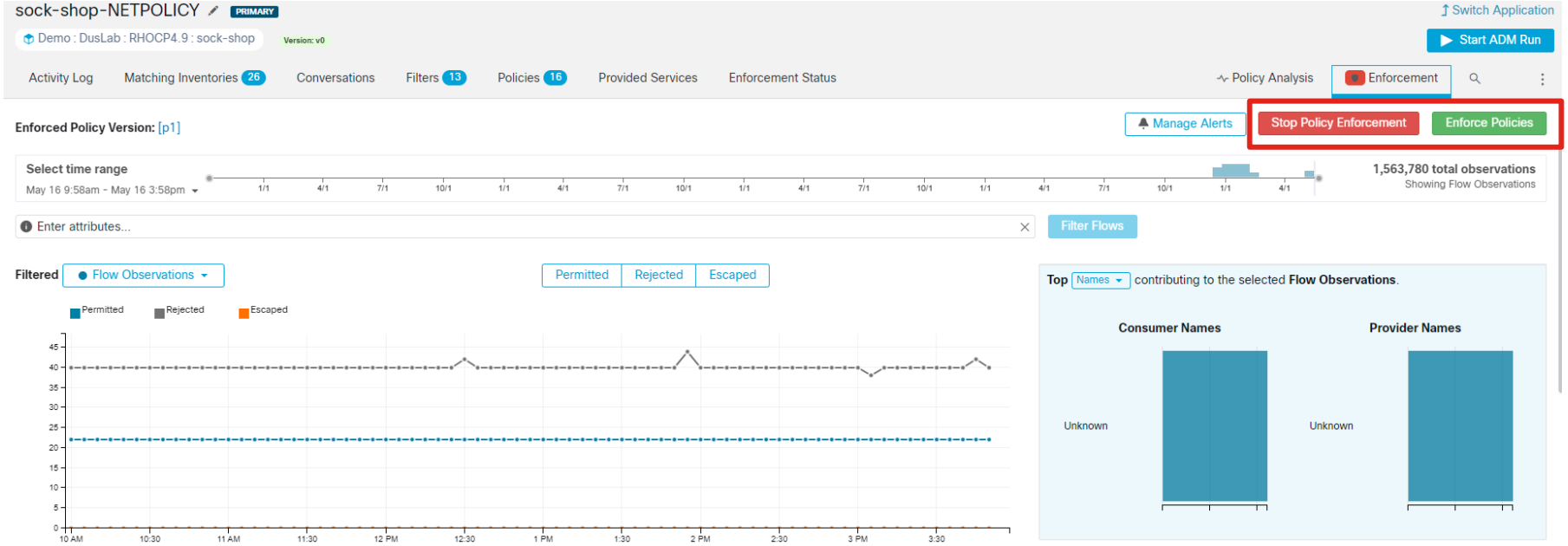
List view of the policy



Priority	Action	Consumer	Provider	Protocols And Ports
100	ALLOW	Demo : DusLab : RHOCP4.9	front-end	TCP : 8079
100	ALLOW	front-end	orders	TCP : 80 (HTTP)
100	ALLOW	front-end	catalogue	TCP : 80 (HTTP)
100	ALLOW	orders	shipping	TCP : 80 (HTTP)
100	ALLOW	user	user-db	TCP : 27017
100	ALLOW	front-end	user	TCP : 80 (HTTP)
100	ALLOW	orders	user	TCP : 80 (HTTP)
100	ALLOW	orders	orders-db	TCP : 27017
100	ALLOW	catalogue	catalogue-db	TCP : 3306 (MySQL)
100	ALLOW	shipping	rabbitmq	TCP : 5672
100	ALLOW	queue-master	rabbitmq	TCP : 5672
100	ALLOW	orders	payment	TCP : 80 (HTTP)
100	ALLOW	front-end	carts	TCP : 80 (HTTP)

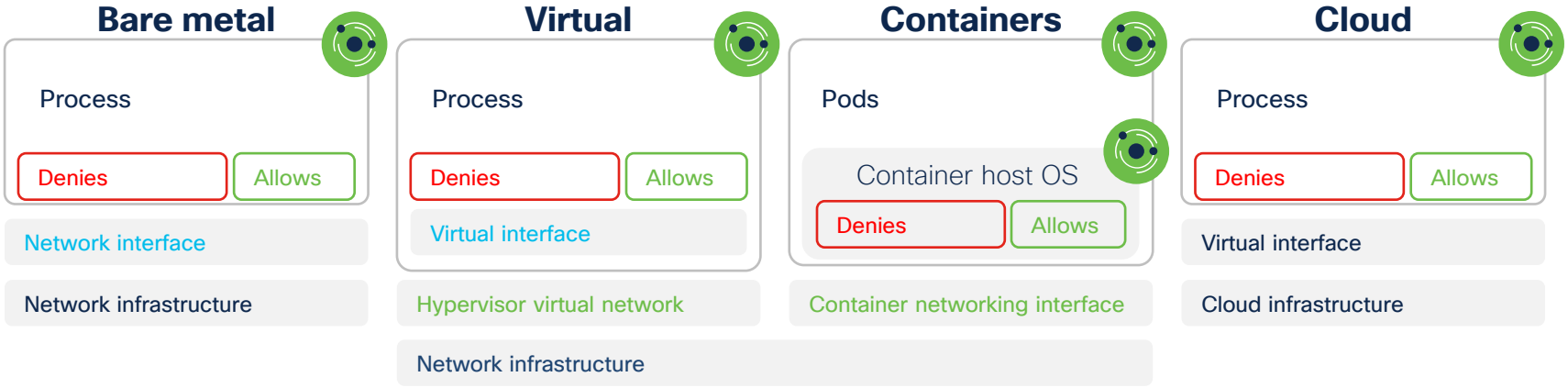
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enforce your policy in one click



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

How does CSW enforce the Policy ?



Intent is rendered as security rules in native environment

- IP sets on Linux servers
- Windows Advanced Firewall or Windows Filtering Platform on Windows servers
- Public cloud: AWS with Security Group and Azure with Network Security Group
- IP sets on EKS with daemon Set Deployment

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

How do I insert NGFW ?

AWS FW

High availability and automated scaling

Stateful firewall

Web filtering

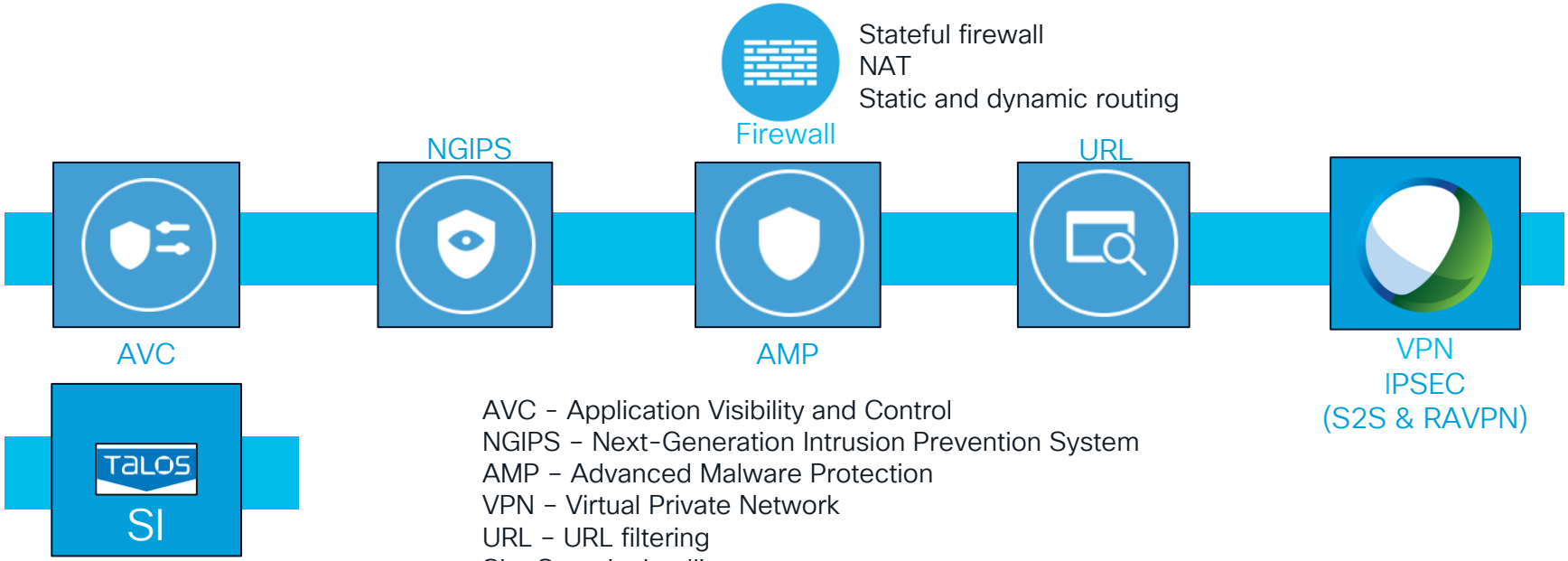
Intrusion prevention

Alert and flow logs

Central management and visibility

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Firewall – NGFWv



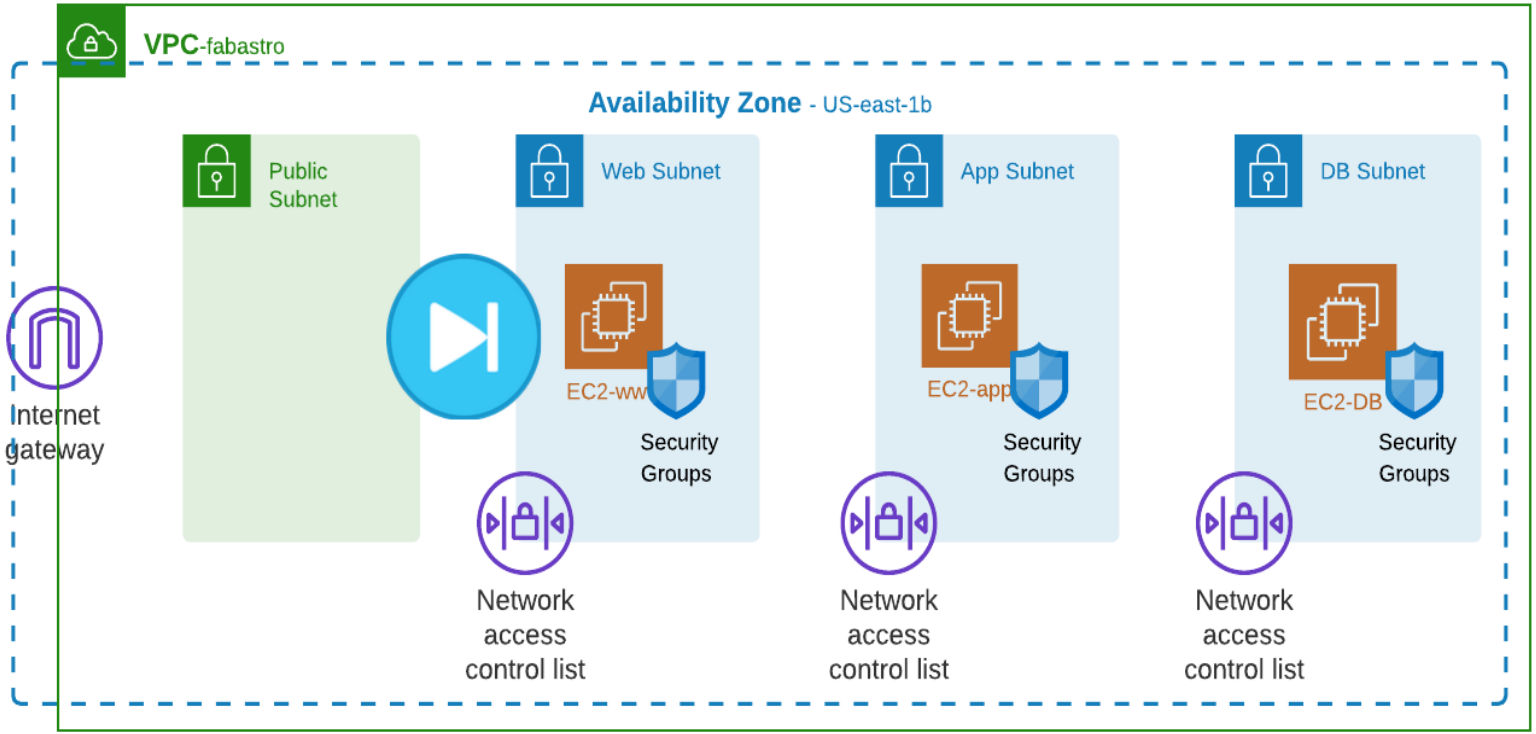
AVC – Application Visibility and Control
NGIPS – Next-Generation Intrusion Prevention System
AMP – Advanced Malware Protection
VPN – Virtual Private Network
URL – URL filtering
SI – Security Intelligence

FTD Appliance

vmware aws KVM Microsoft Azure Google Cloud Platform ORACLE Cloud Infrastructure

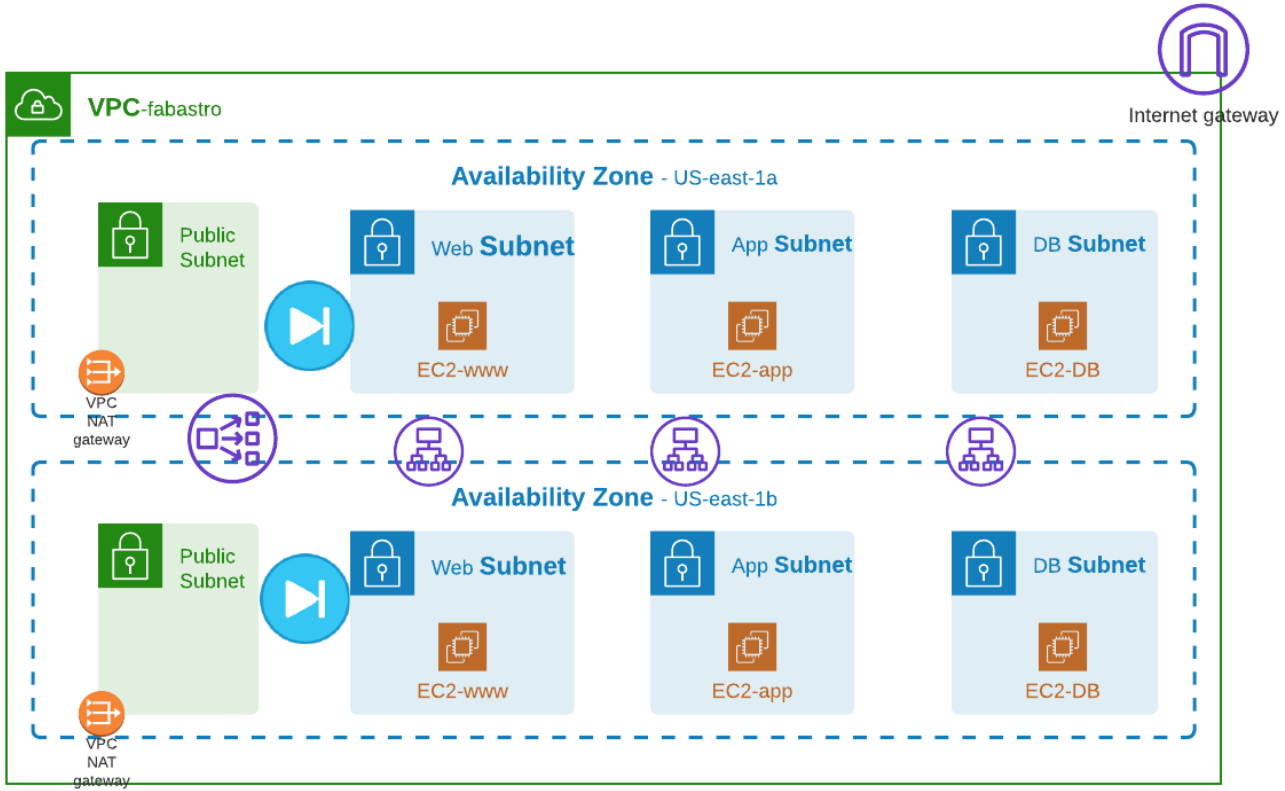
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Firewall in front of the “Application” VPC



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

FTD insertion with HA



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

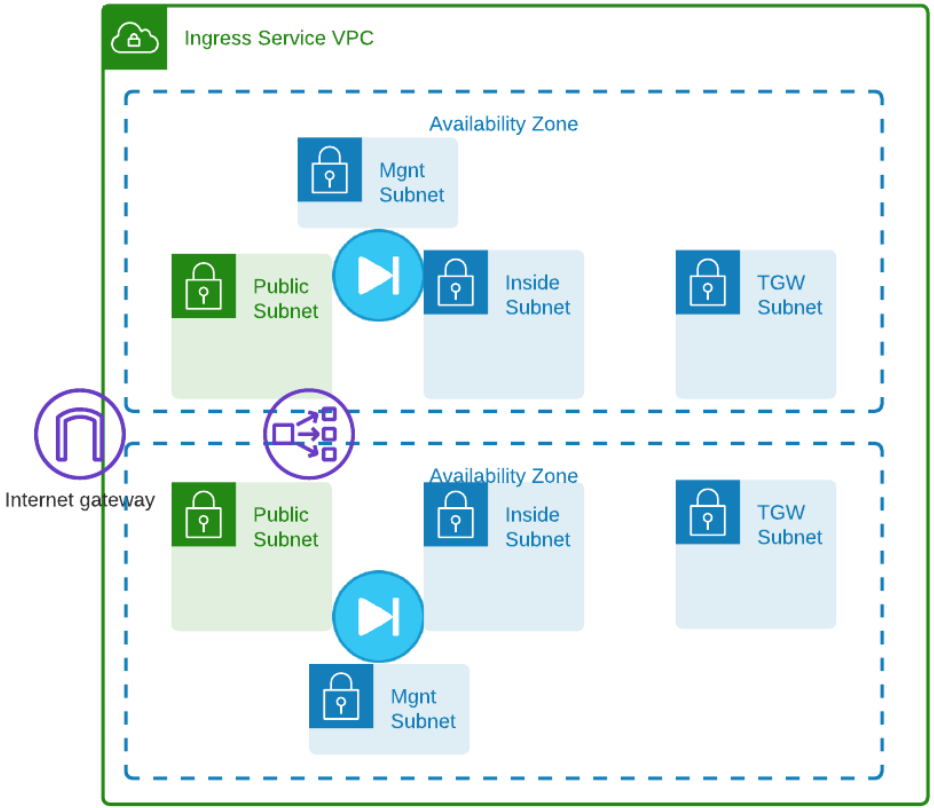
Limits of this design

New Firewall pair for each applications

Double inspection for inter-VPC

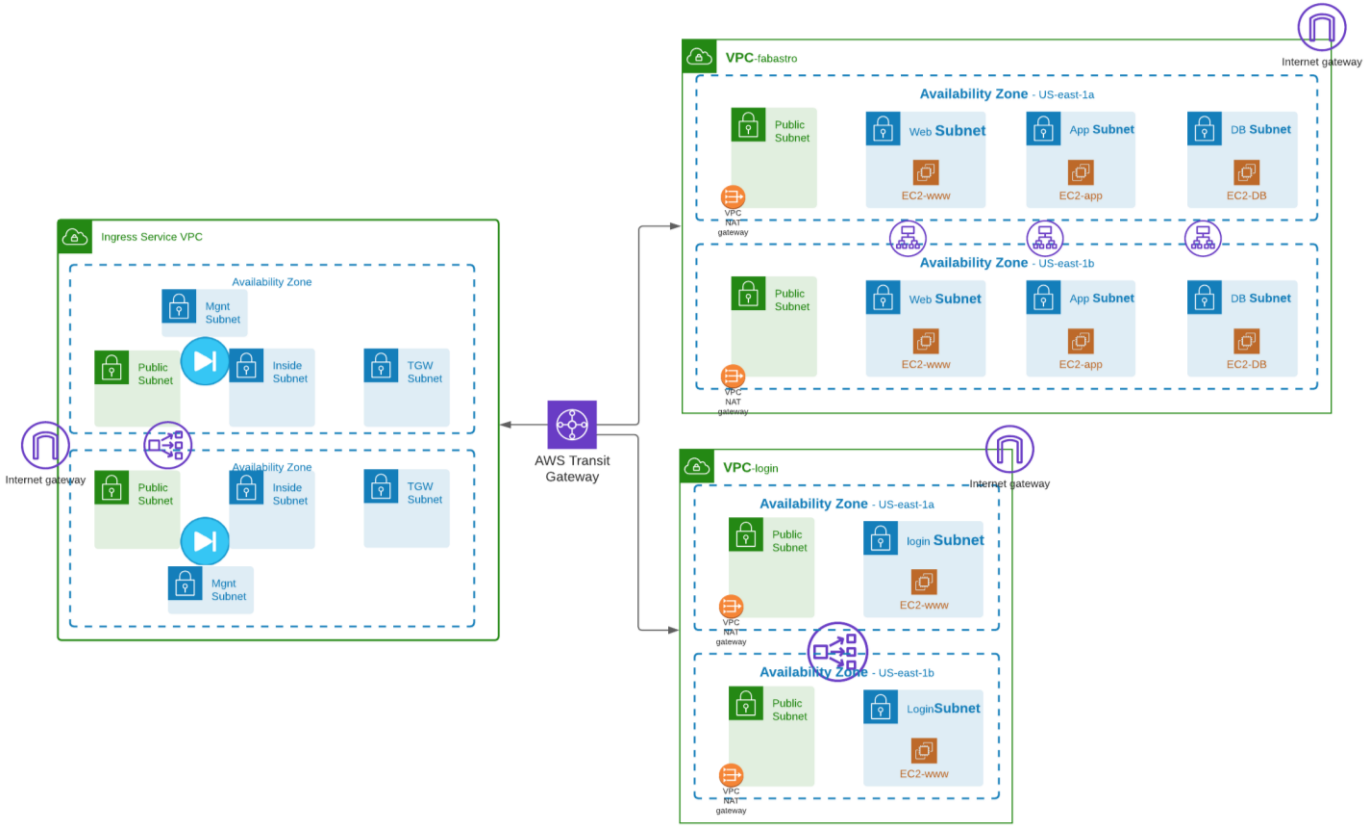
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ingress service VPC



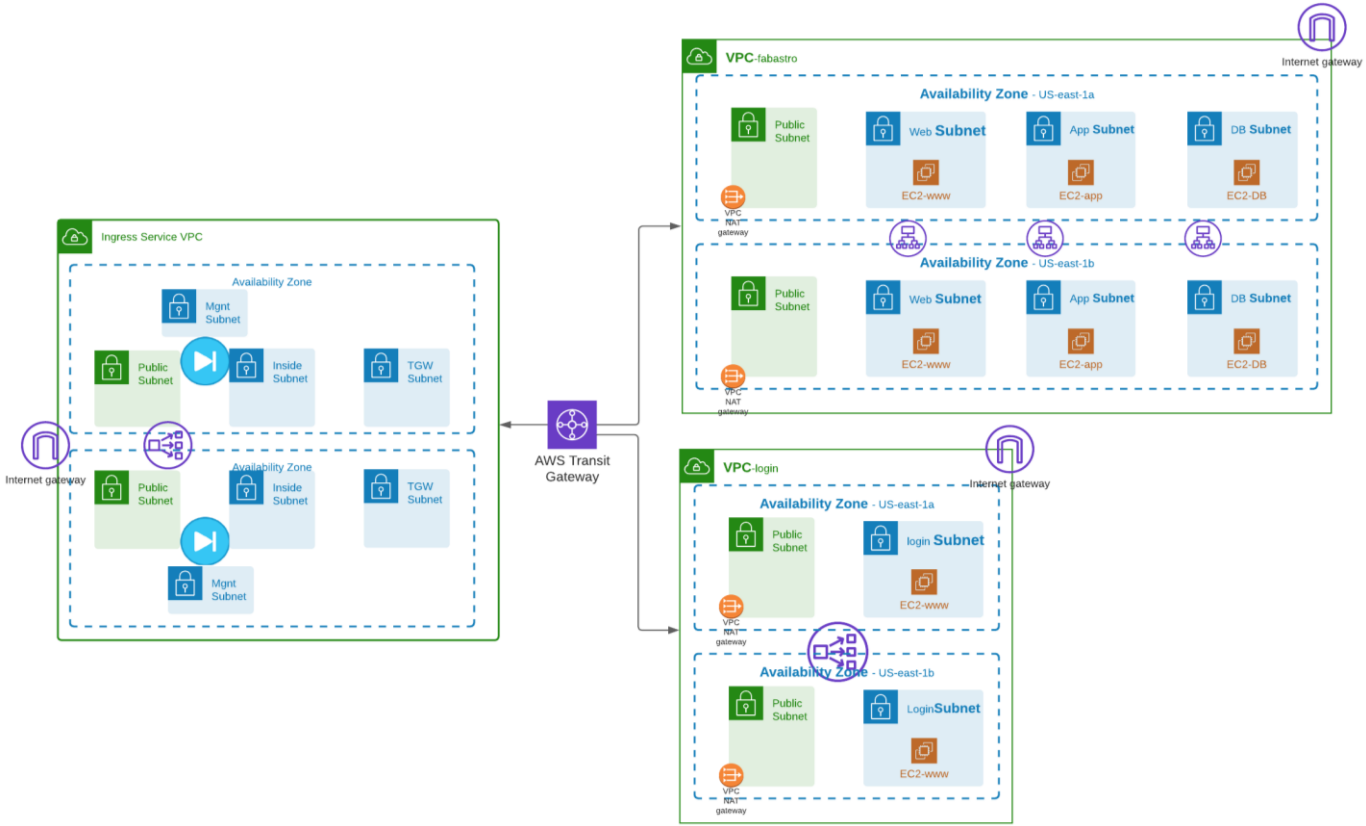
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ingress Service VPC with FTD



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

North/South and East/West Service VPC



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

FTD AWS Insertion Configuration

- Create Ingress VPC
- Create Subnets (Outside, Inside, Management, TransitGateway)
- Create Interfaces (Outside, Inside, Management, Diagnostic)
- Create Security group policies for FTD interfaces
- Create FTD instances with 4 interfaces
- Create Network load-balancer

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

What to configure on FTD ?

- Interface outside and Inside
- Static route to DG outside and for the web server LB inside
- NAT Twice :
  - Destination NAT from Outside interface to destination web servers LB
  - Source NAT using FTD inside interface (for stickiness of the sessions)
- Access policy to allow web traffic

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Multi-cloud and Hybrid Cloud Environments

Private Cloud

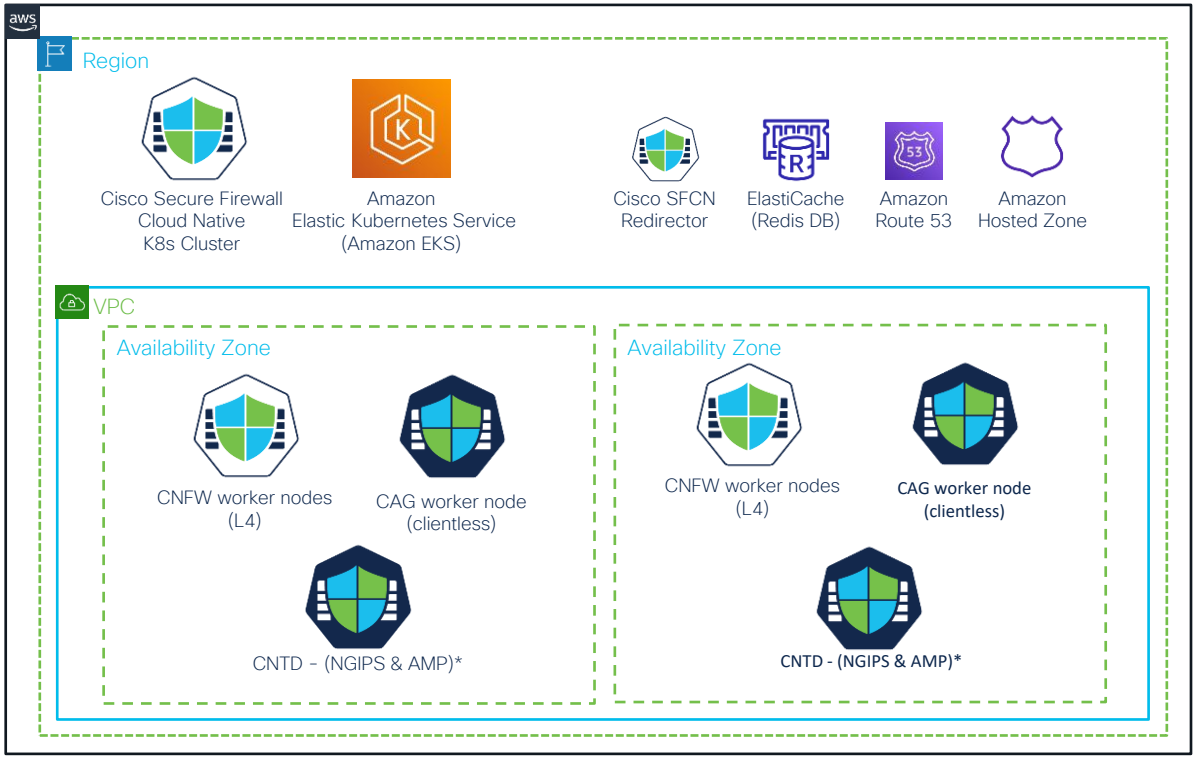
Public Cloud

New Features

- Clustering
- Dynamic Policy
- Better integration with public cloud infrastructure
- Infrastructure as Code and Automation
- Integration with GuardDuty
- Gateway Load balancer integration
- Auto Scaling
- Snapshot support

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Firewall Cloud Native for AWS

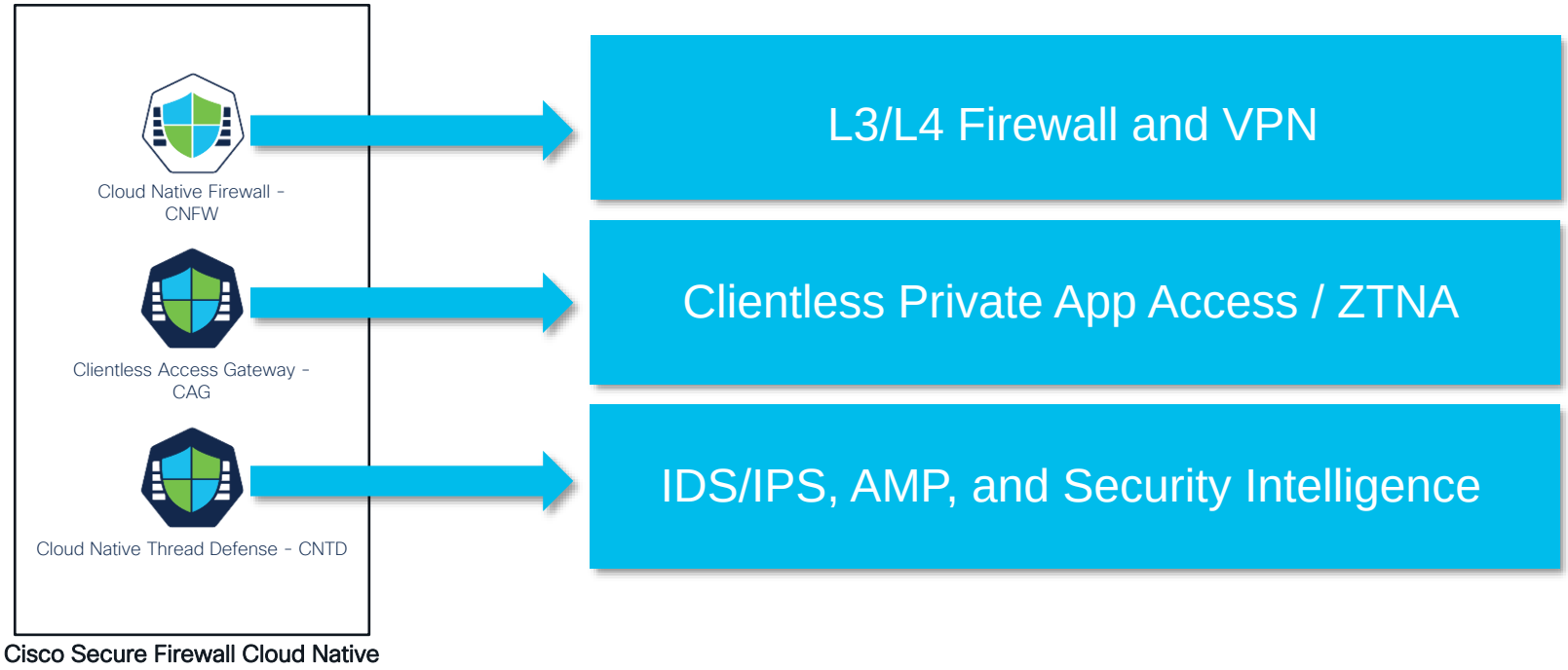


* Future

- 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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Firewall Cloud Native Enforcers



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

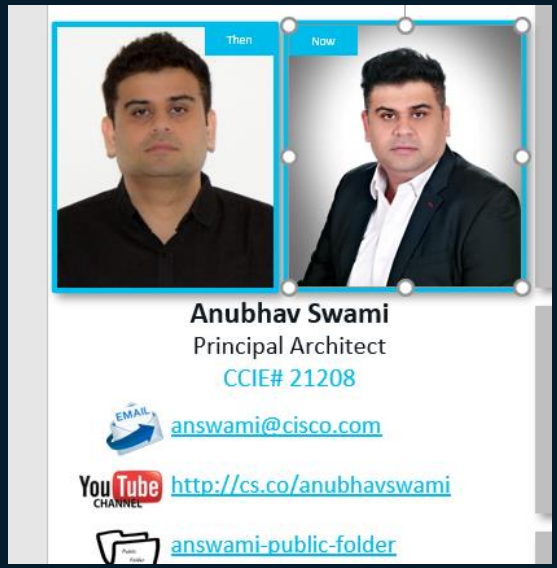
The bridge to possible

Cisco Secure Firewall Cloud Native on AWS

Building a Scalable Edge

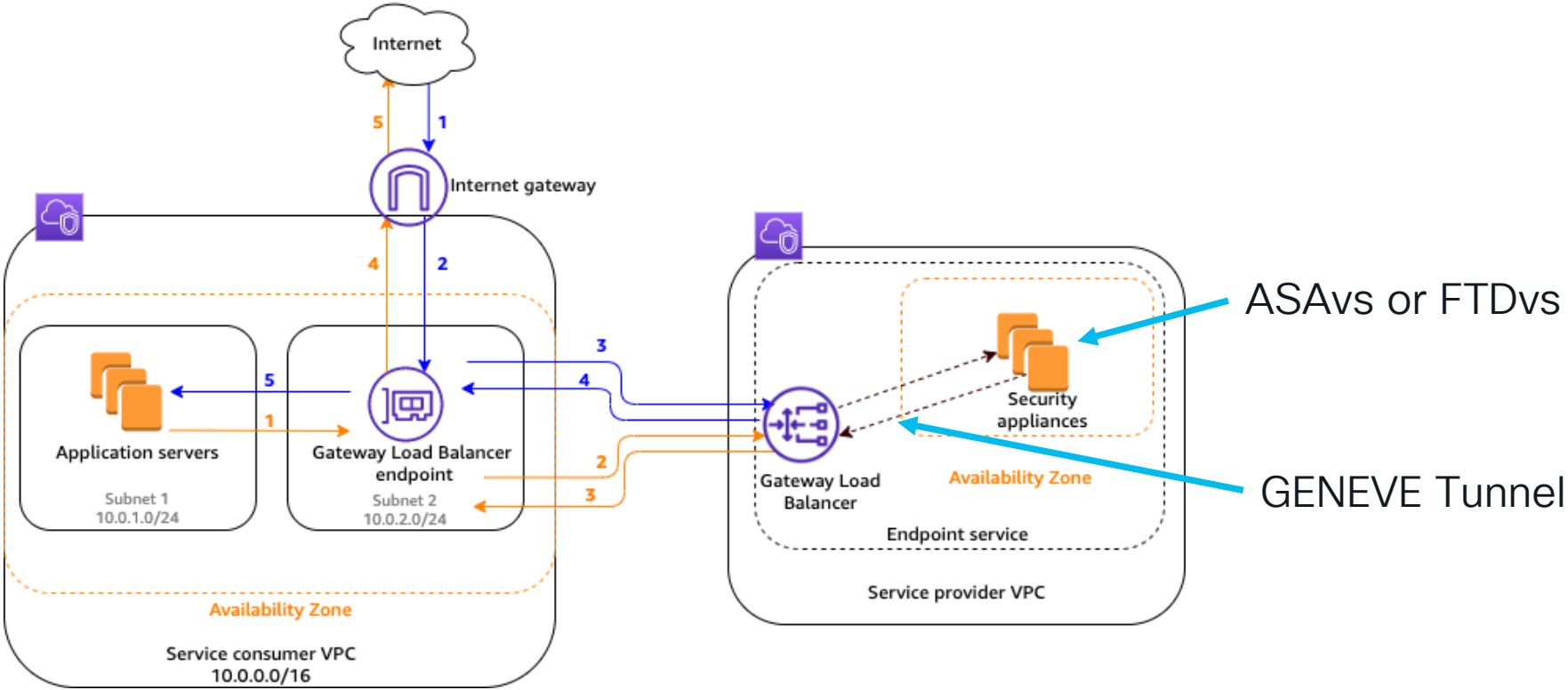
Anubhav Swami, Principal Architect
@swamianubhav

BRKSEC-3561



cisco Live!

AWS Gateway Load Balancer

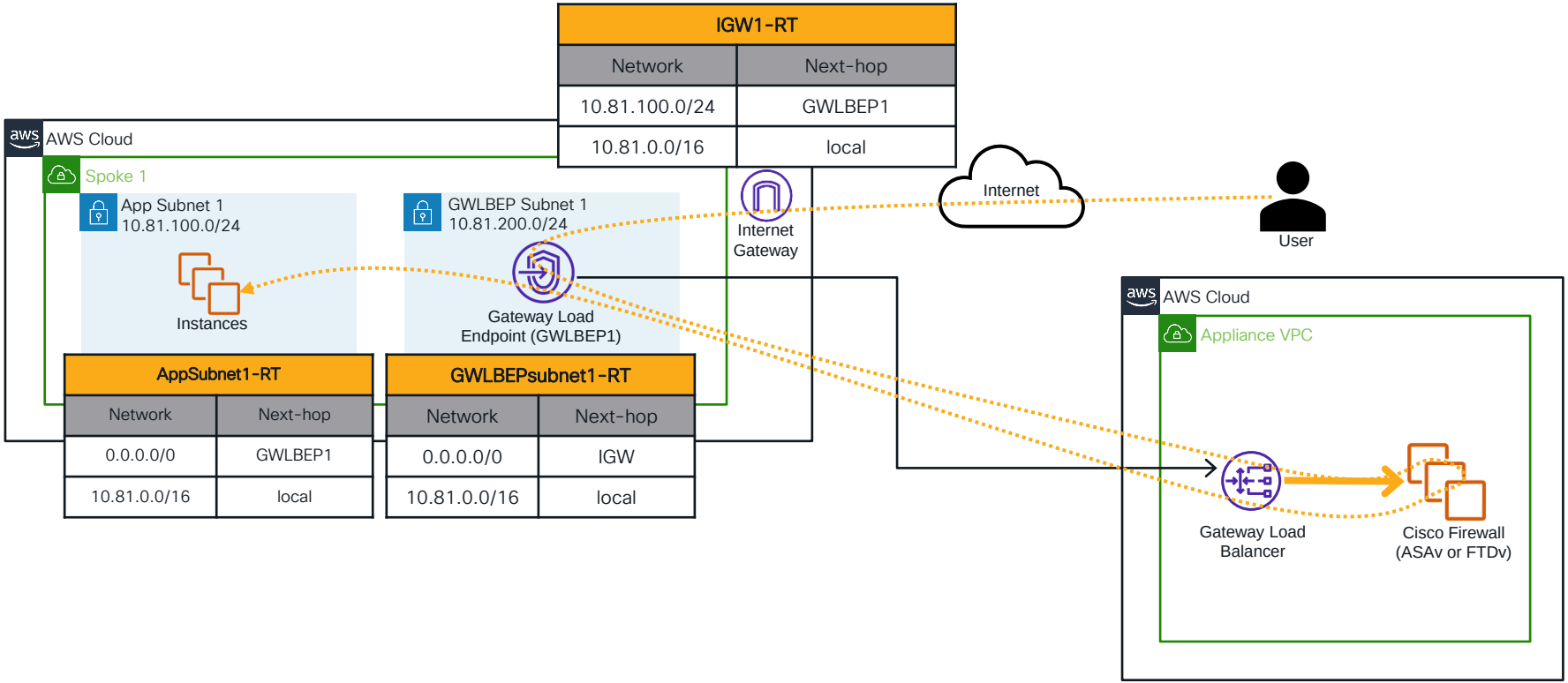


Source:https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Firewall and Amazon GWLB

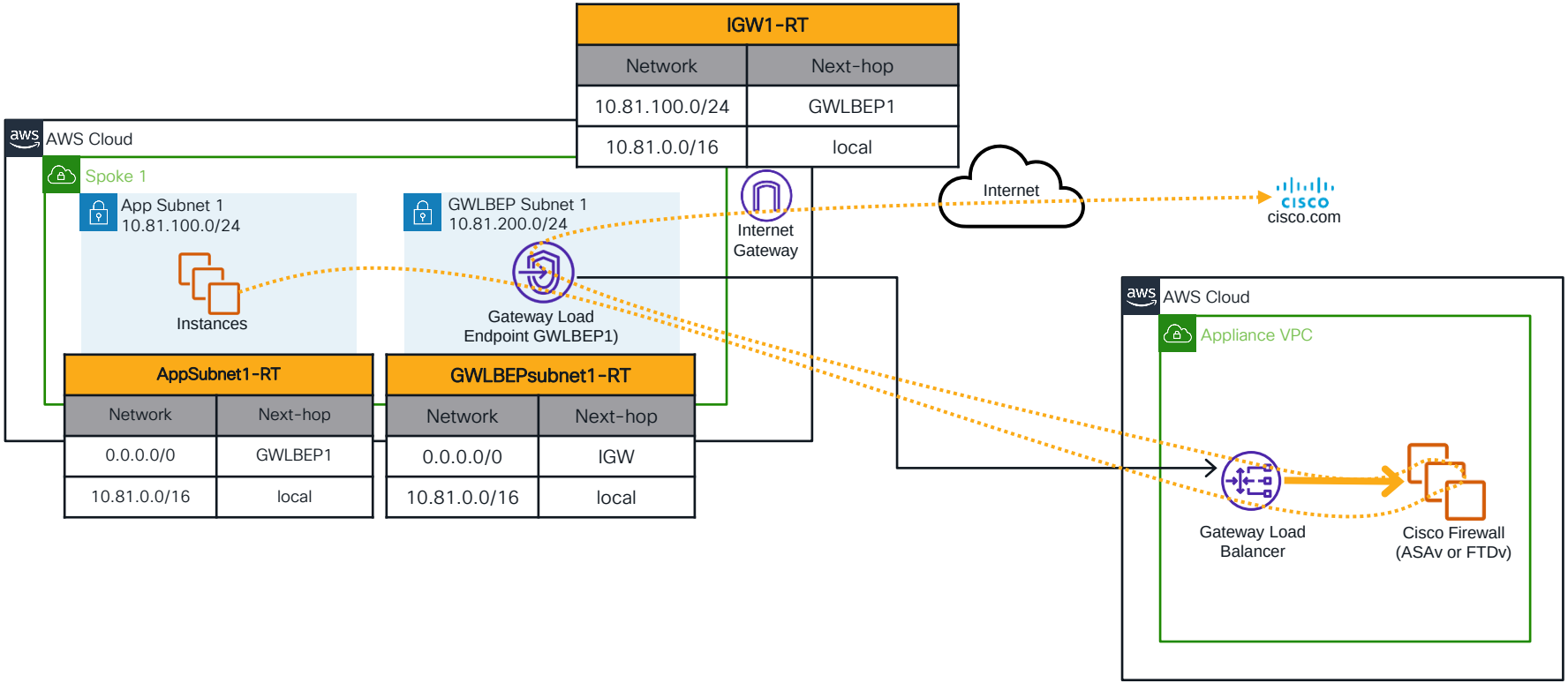
Inbound



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

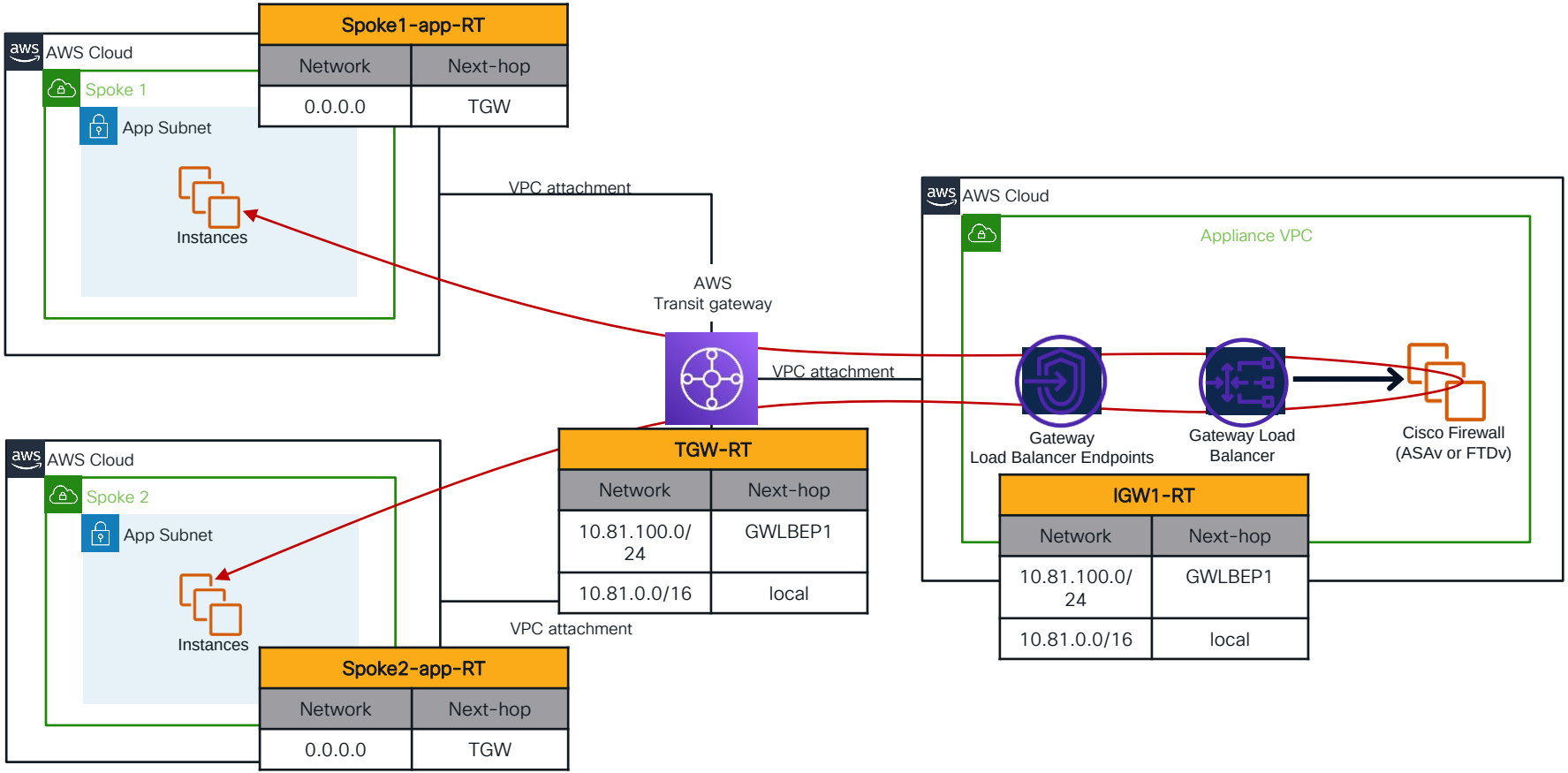
Cisco Secure Firewall and Amazon WLB

Outbound



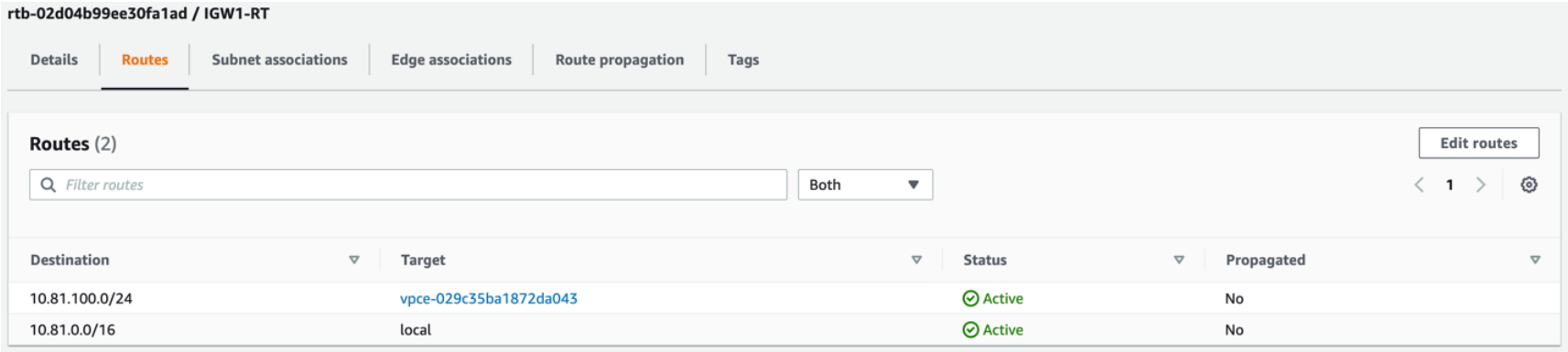
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

East/west traffic



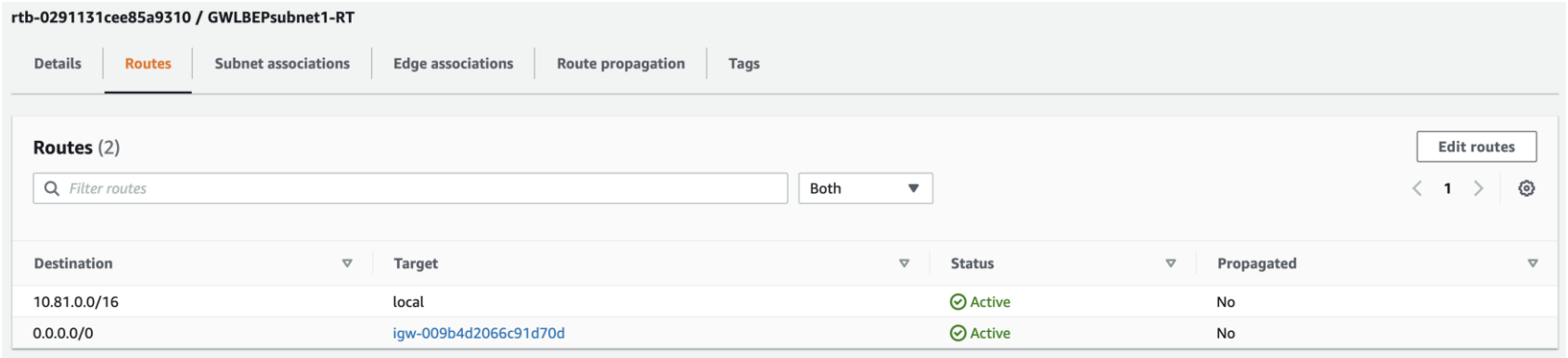
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

IGW1-RT



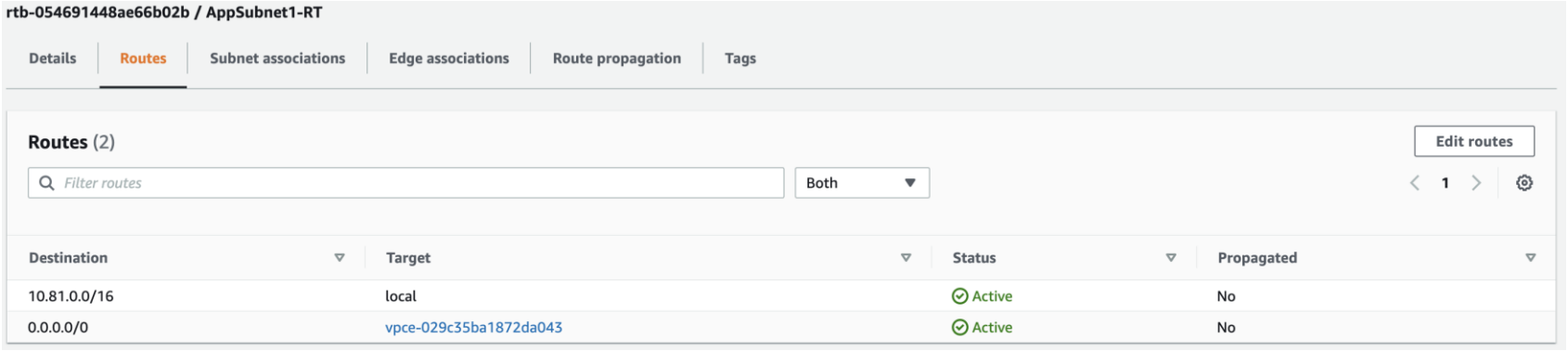
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

GWLBEsunet1-RT



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Route



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

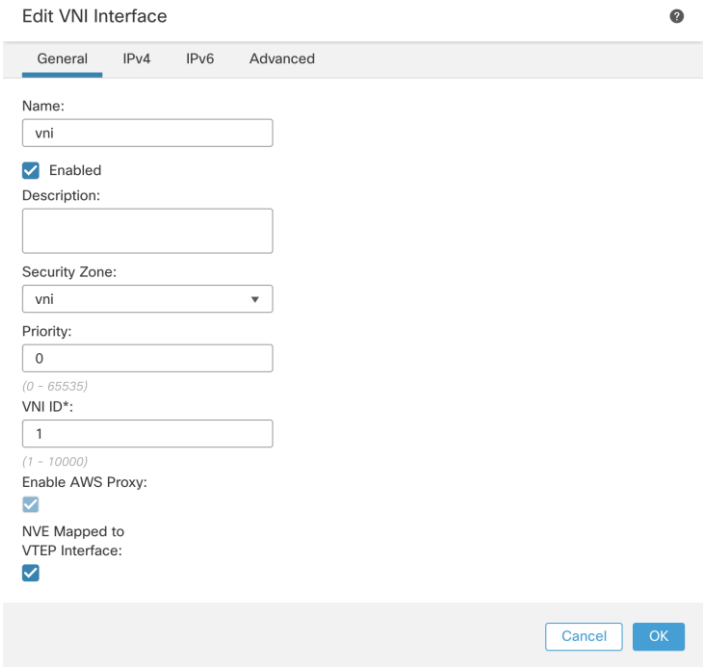
Outside interface Configuration

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Virtual Router	
Diagnostic0/0	diagnostic	Physical					
TenGigabitEthernet0/0	outside	Physical	outside				
TenGigabitEthernet0/1		Physical					
vni1	vni	VNIInterface	vni				

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

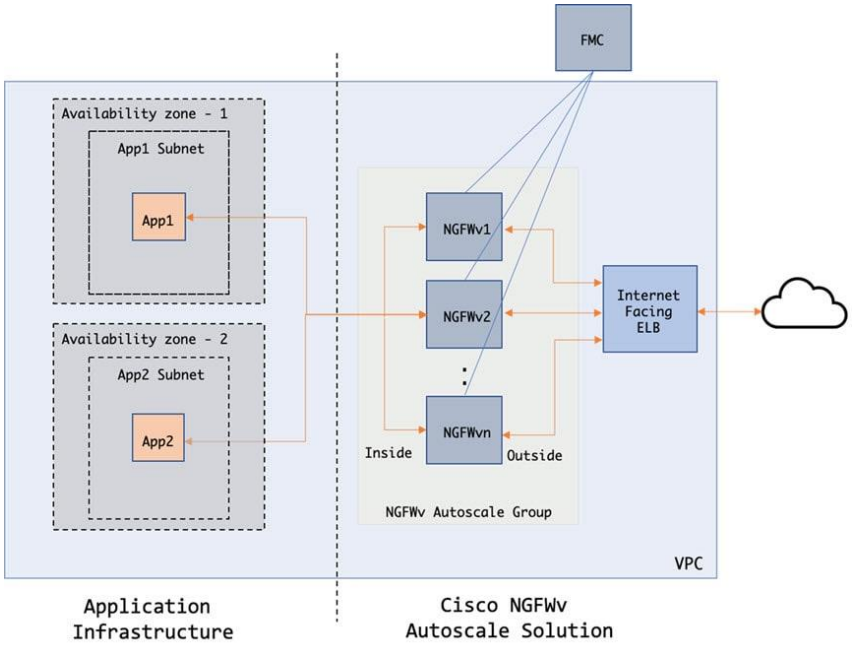
VNI interface Configuration

- Enable VNI interface and add a name for VNI interface
- Create and associate for Security Zone on VNI interface
- Enable AWS proxy
- Enable VTEP Interface



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

What about auto-scaling ?

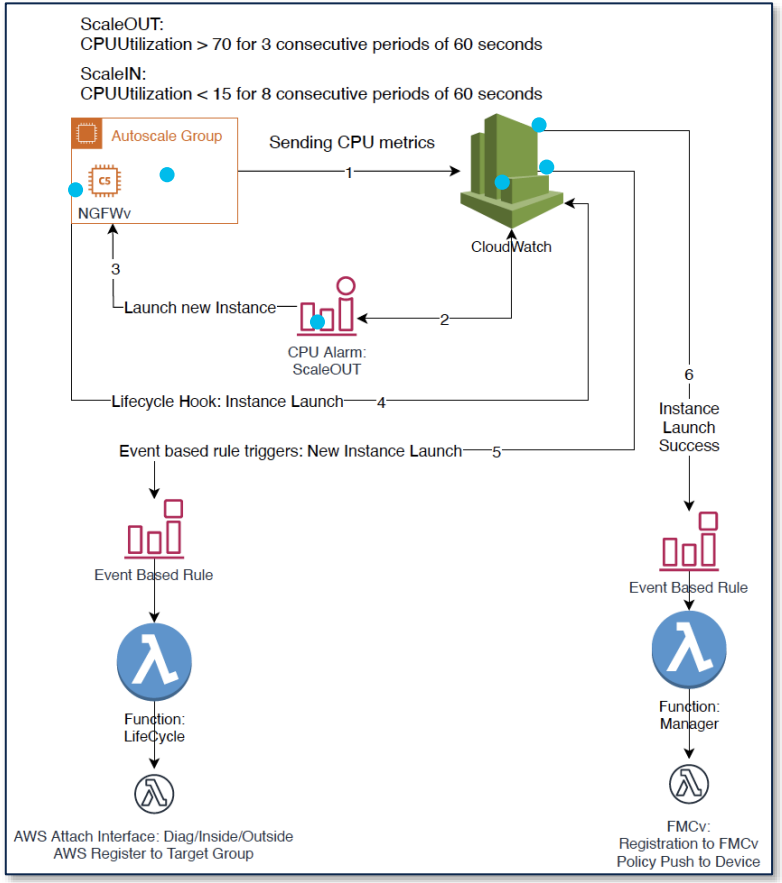


- Uses Lambda function
- Requires FMC
- Cloudformation templates provided

More information: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-gsg/ftdv-aws-autoscale.html

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

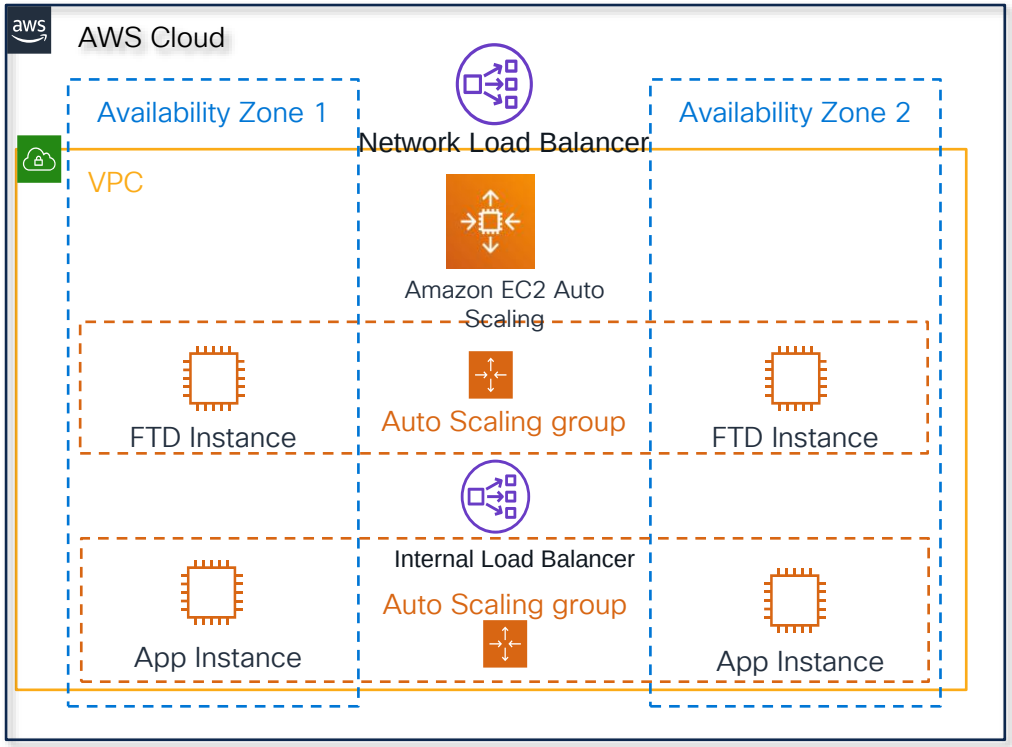
How it works?



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Autoscale in AWS

- The FTDv Auto Scale group is behind an external, internet-facing load balancer
- External load balancer monitors health of all the FTDv instances in Auto Scale group and distributes traffic from internet to healthy FTDv instances, FTDv instance will then forward traffic to application
- Auto Scale solution will increase or decrease FTDv instances in the autoscale group based on capacity needs



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introducing CloudWatch and Lamda Function

CloudWatch

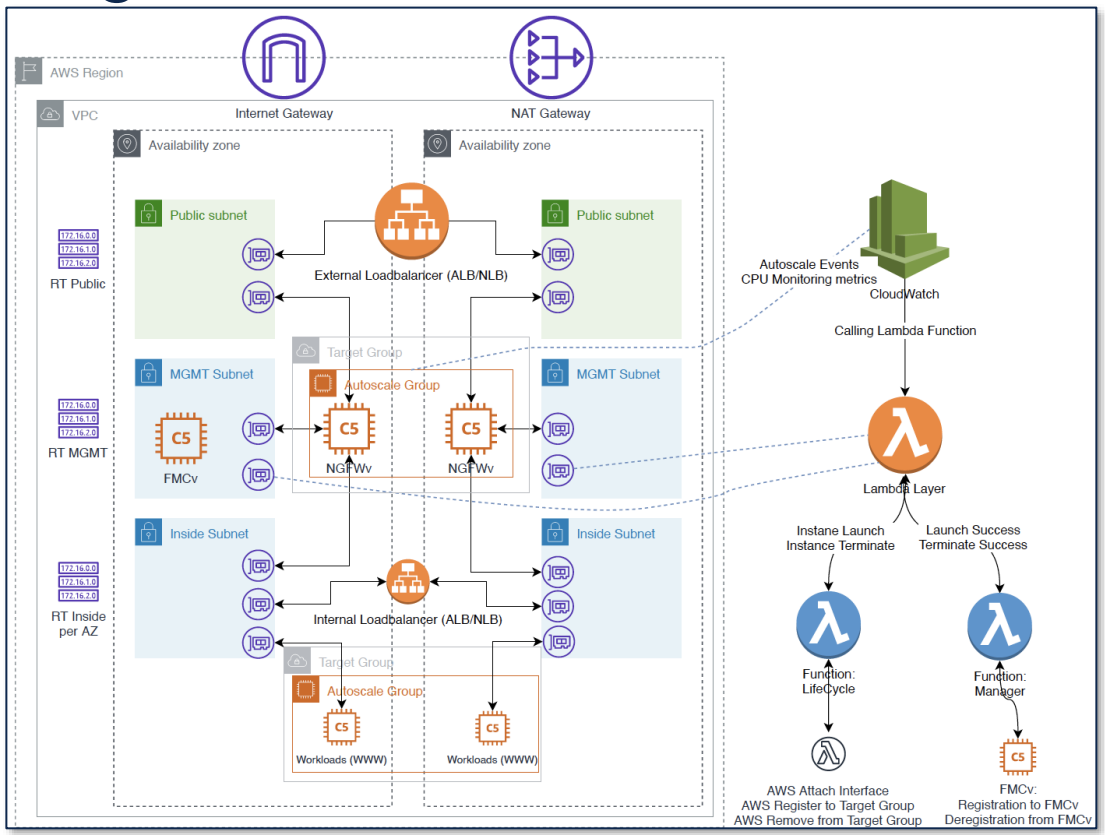
- Observability on a single platform across applications and infrastructure
- Easiest way to collect metrics in AWS and on-premises
- Improve operational performance and resource optimization
- Get operational visibility and insight
- Derive actionable insights from logs

Lambda Function

- Serverless architecture of AWS
- No servers to manage for the code
- Built-in fault tolerance
- Automatic-scaling
- Lambda code can interact with AWS infrastructure natively
- Support different languages: Python, Node.js, Ruby, Java, Go, .NET…

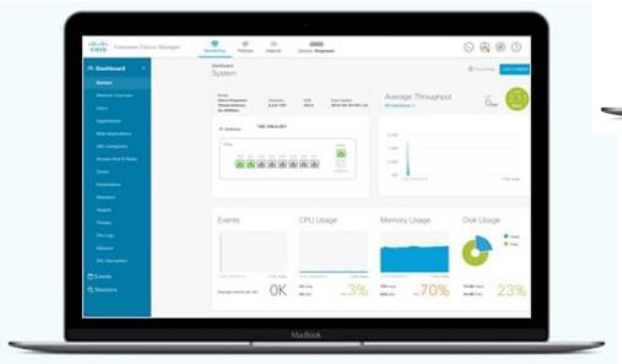
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Solution Design

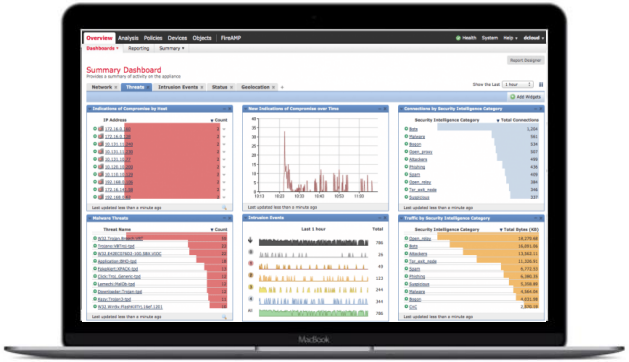


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

How do I manage my FTDs ?

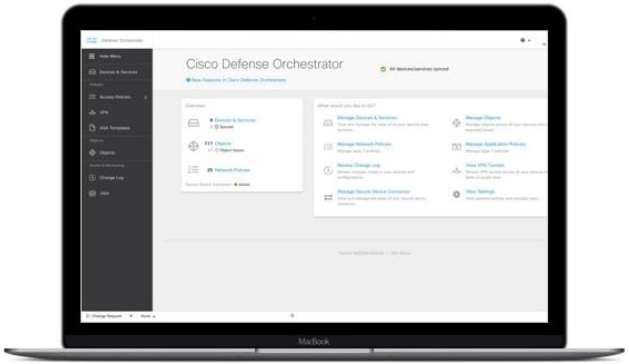


FDM



FirePower Management Center :

- On prem
- In AWS
- In CDO



CDO

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Question about automation ?

In AWS

Ecosystem solutions

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security through visibility

- Native to AWS
- Cisco Secure Cloud
- Cloud Insight
- Cisco Secure Workload

AWS Security Solutions

Identity

- AWS Identity & Access Management (IAM)
- AWS Organizations
- AWS Cognito
- AWS Directory Service
- AWS Single Sign-On

Detective control

- AWS Security Hub
- AWS CloudTrail
- AWS Config
- Amazon CloudWatch
- Amazon GuardDuty
- VPC Flow Logs
- AWS Detective

Secure Cloud Analytics

Infrastructure security

- AWS Control Tower
- Amazon EC2 Systems Manager
- AWS Shield
- AWS Web Application Firewall (WAF)
- Amazon Inspector
- Amazon Virtual Private Cloud (VPC)

Secure Cloud Workload

Data protection

- AWS Key Management Service (KMS)
- AWS CloudHSM
- Amazon Macie
- Certificate Manager
- Server Side Encryption

Incident response

- AWS Config Rules
- AWS Lambda

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

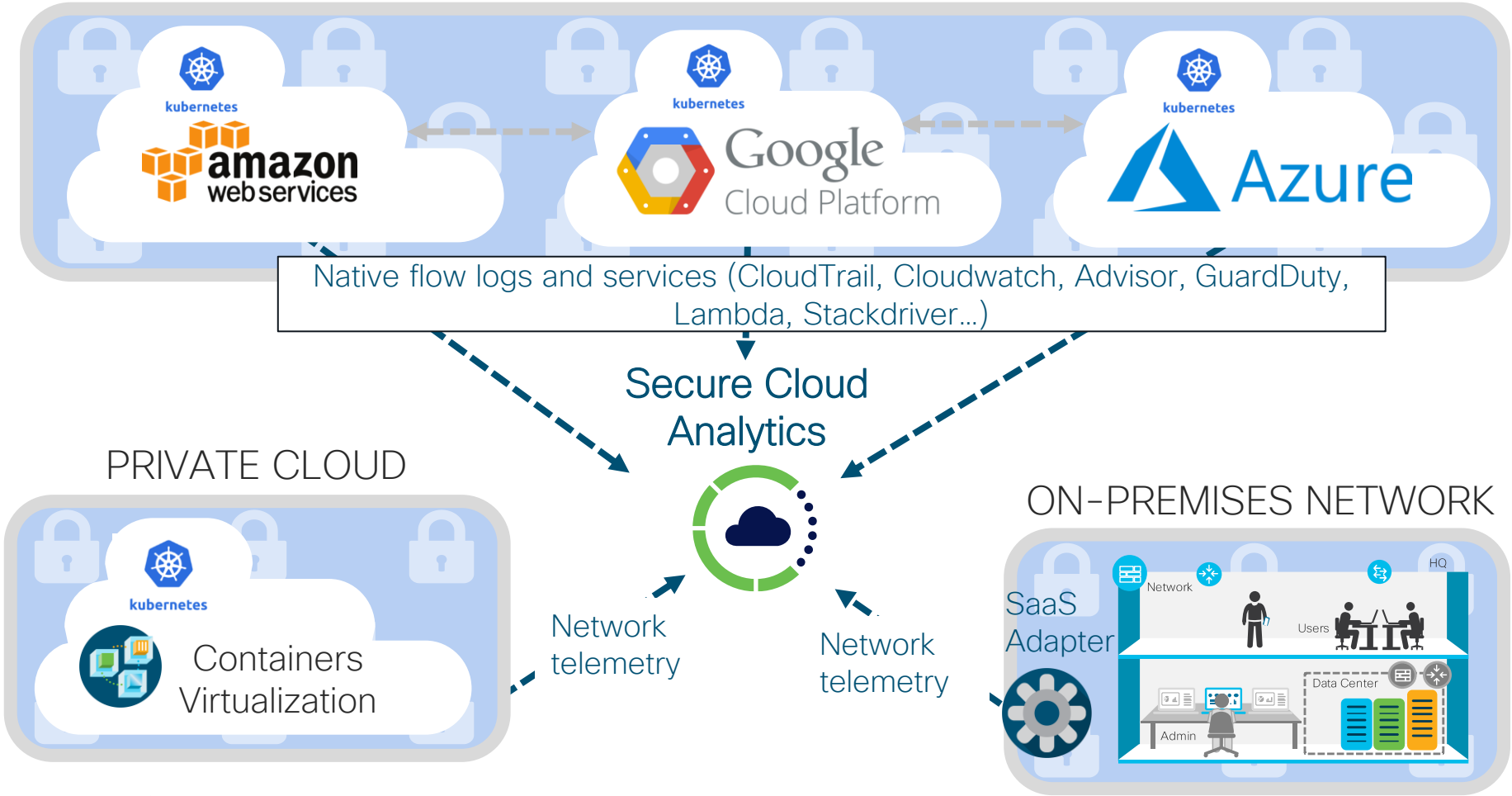
AWS GuardDuty & Secure Cloud Analytics

- ✓ DNS Detections with DNS logs
- ✓ Detections on EC2, S3, IAM
- ✓ Easy to activate & out-of-box detections
- ✓ Unsupervised Analytics

- ✓ Correlation of SCA Detections & GuardDuty
- ✓ Unsupervised & Supervised Analytics
- ✓ Advanced detections on network traffic (baselining >30 days)
- ✓ Encrypted Traffic Analytics
- ✓ Combined visibility of all logs
- ✓ Customized alerts for compliance
- ✓ Enhanced investigation with drill-down into dataset

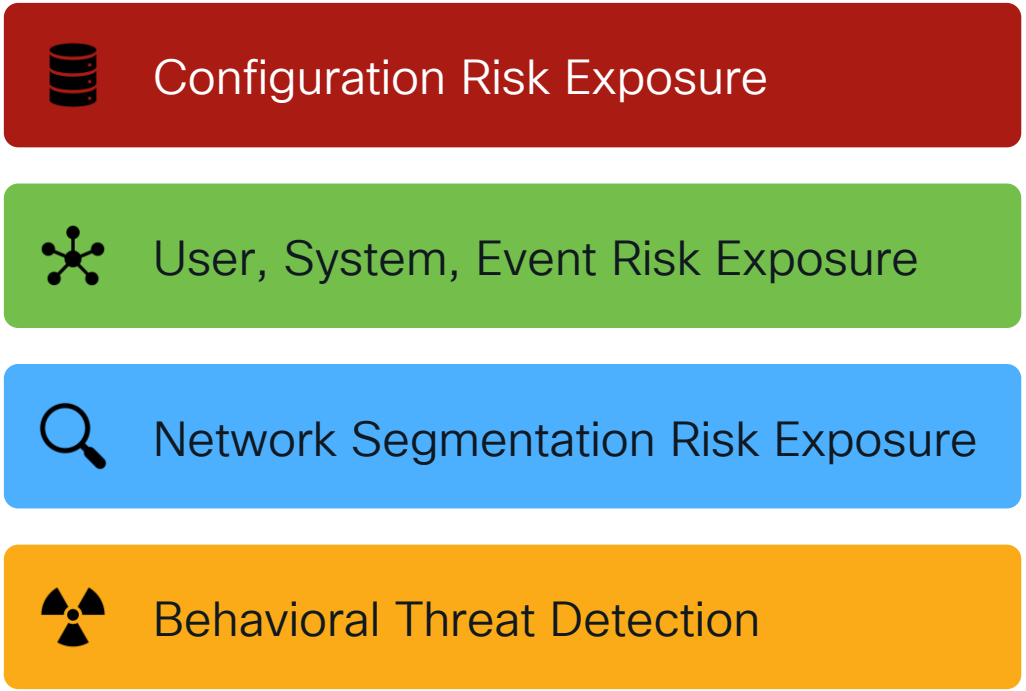
https://aws.amazon.com/blogs/apn/cloud-posture-and-threat-analytics-with-cisco-secure-cloud-analytics/

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Cloud Analytics Engine

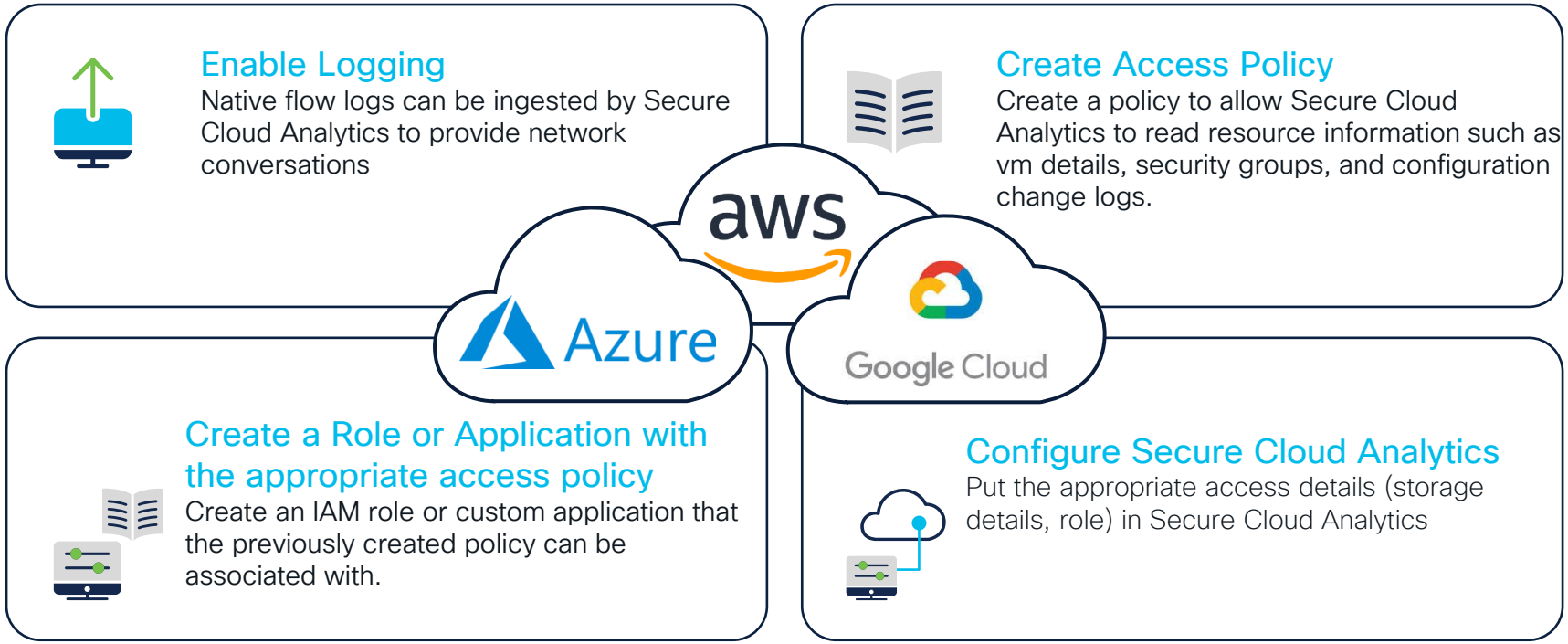


Cloud Security Maturity

- **Visibility**
  What do we have, and how important is it to our business?
- **Compliance**
  Am I following best practices and regulatory guidelines?
- **Security Posture**
  Are resources being locked down properly?
- **Internal Policy**
  Are resources & users following our established guidelines?
- **Advanced Detection and Response**
  How effectively can I detect and respond to a breach?

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

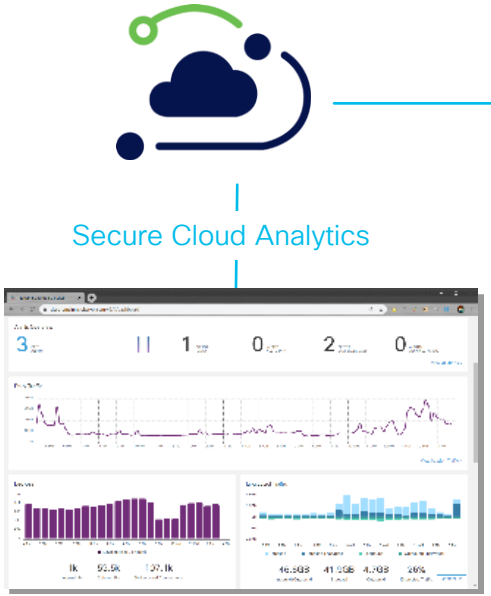
Common public cloud integration process



https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cloud/configuration/SWC_PCM_AWS_DV_1_5.pdf

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Accessing telemetry for AWS deployments



APIs

Amazon account

Role Created for Secure Cloud Analytics in Account

Permissions allow reading VPC flow logs

Permissions allow Secure Cloud Analytics to read AWS services

Amazon CloudWatch

Amazon Simple Storage Service (S3)

Amazon CloudTrail

AWS Identity and Access Management (IAM)

Flow logs

Flow logs

Amazon GuardDuty

AWS Lambda

Amazon VPC

Amazon VPC

Amazon VPC

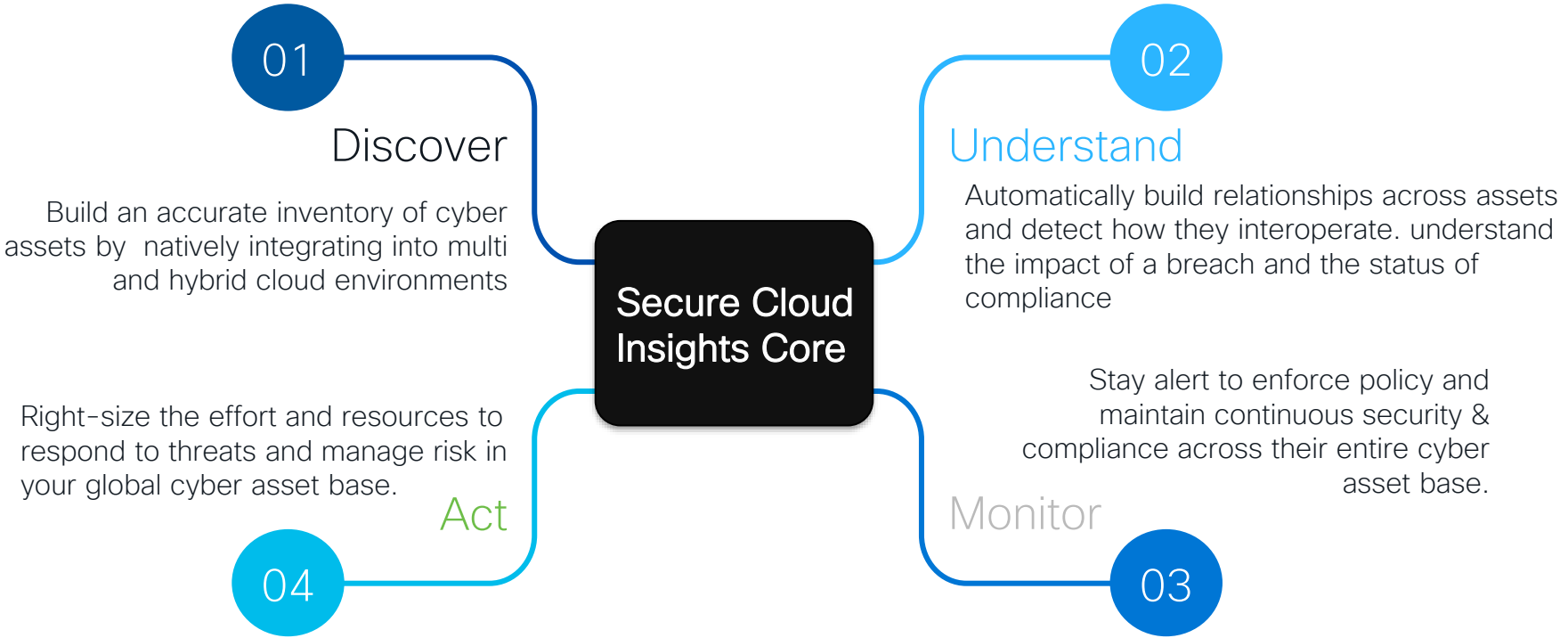
Amazon Inspector

AWS Config

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cloud Insight

Cloud Insight Use Cases



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Cloud Insights
Beyond Cloud Security Posture Management (CSPM)

Easily identify security and compliance gaps

Continuous audits with breadth and depth of standards out-of-box, fully customizable

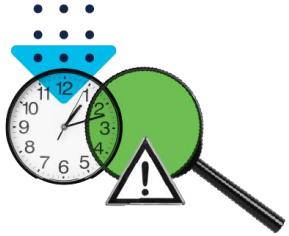
Simple evidence collection and helpful alerts to avoid compliance drift and security incidents

Complete visibility into your security posture

Inadvertent exposure of sensitive data in the cloud

Visualize and navigate complex relationships with ease

Natively detect Cyber Assets in the cloud based on multiple data types



Attack Surface Management

Identify the blast radius – who and what else could be affected by this incident

Identify the root cause – how did the attacker access assets

Identify Security gaps and risks – How cloud an attack access assets

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Cloud Insights High level Architecture

Native Data Ingestion

Integrate with data sources in the cloud or on prem natively through available APIs or data streams.

Asset discovery & mapping

Identity assets and entities across multiple data sources. Correlate and map asset relations across multiple data sources

Continuous Compliance Checks
Relationship Graph Visualization

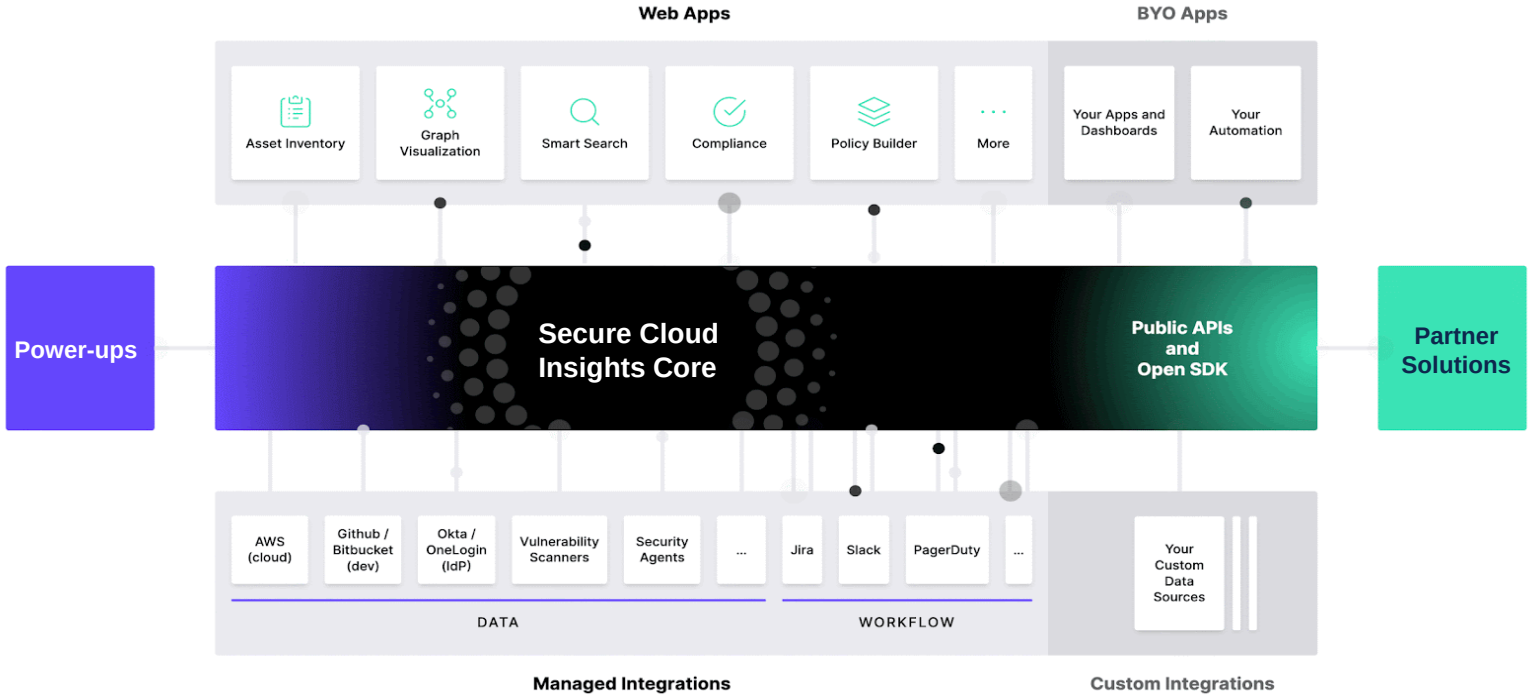
Simple Query Language
Periodic Data Polling

Alert and Respond

Shares alert findings to ticketing alert correlating systems upon detection

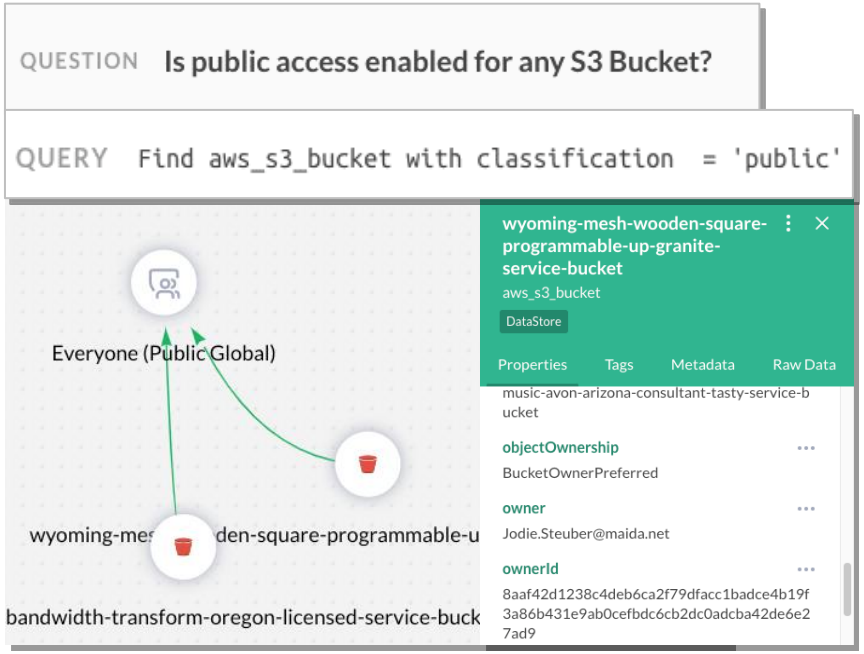
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

API First and Cloud Native



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

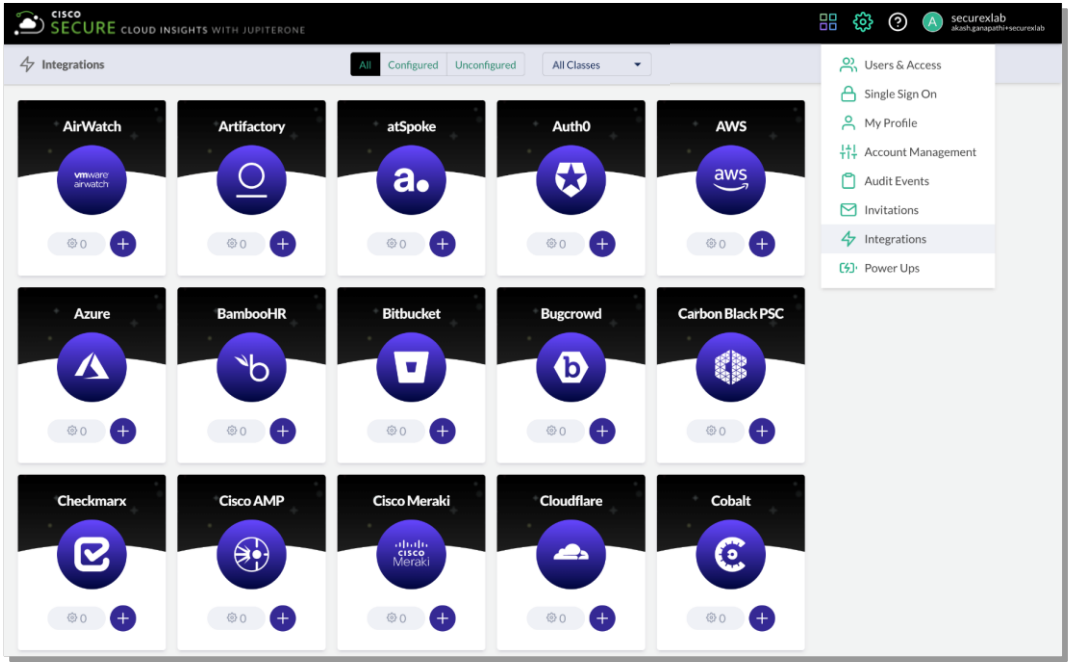
Query Through Use Cases



- Incident Scope and Response
- Compliance Check
- Attack Surface Management
- Configuration Change Detection

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

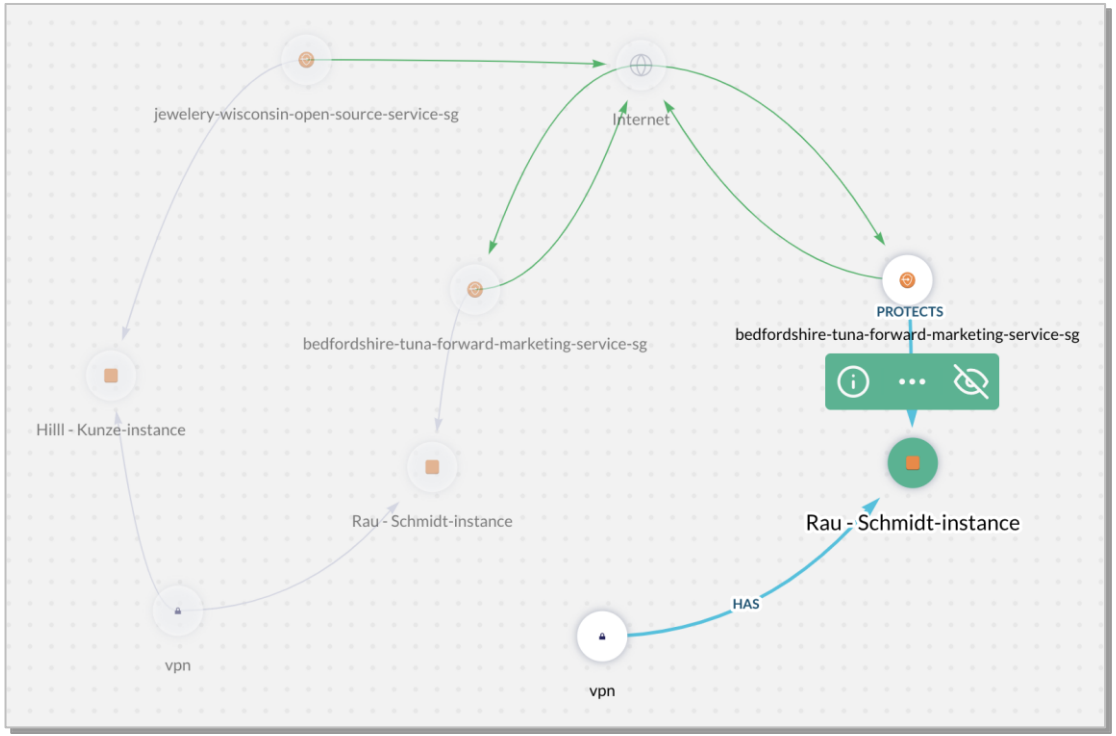
Asset Discovery



- Native integrations allow for simple discovery of assets from across the security program
- Agent-less, API-driven configurations use read only credentials to ingest data with no installations or deployments
- Discover and classify assets by type including endpoint, datastore, policies, security groups and many others

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Relationship Mapping

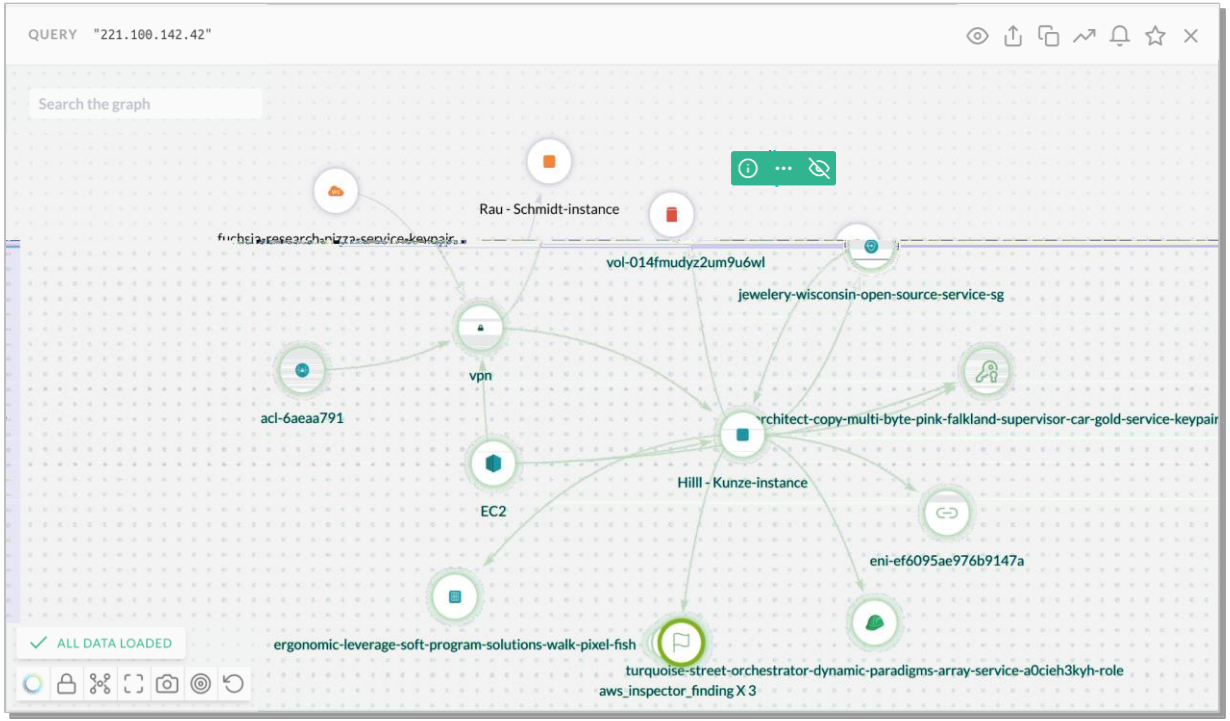


- Relationships between assets are discovered via the integrations and are mapped together automatically
- Here we see:
  - Security groups allowing access to the internet
  - The instances they protect
  - The subnets those instances are on

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

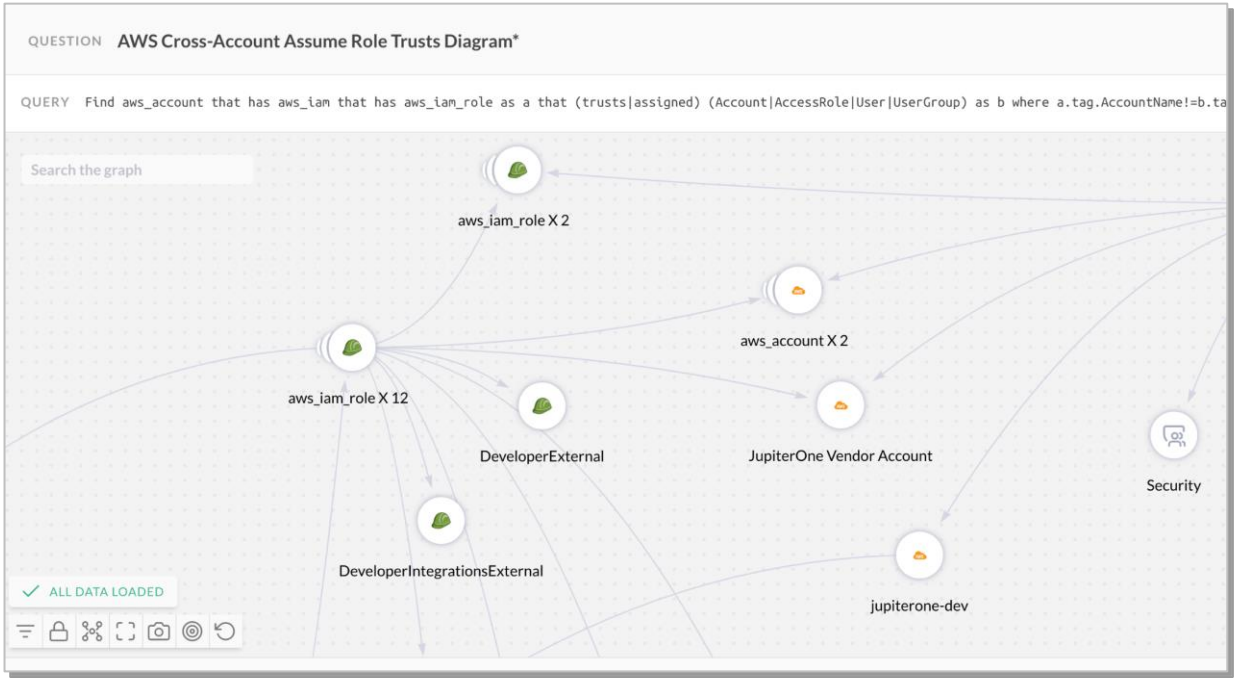
Context for Incident Response

- Walk the graph of data by expanding nodes and view their relationships
- Identify the impact of a compromised asset and what can an attacker do next
- Find relevant context to an incident in a matter of seconds



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

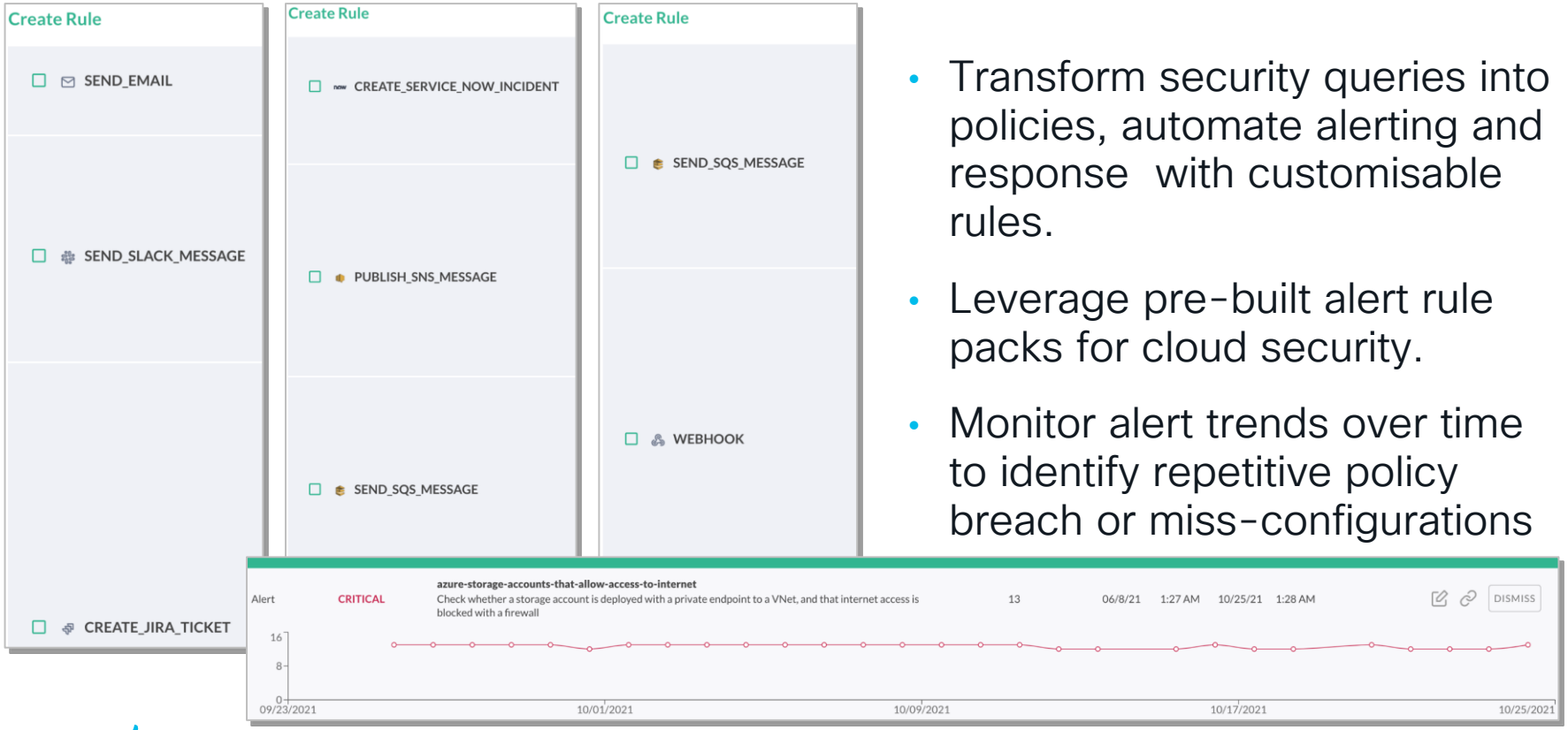
Cross Environment investigation



- Complex relationships cross-account trusts, vpc peering, vpc endpoint policies, IAM policies, load balancer configurations, and more are all automatically discovered
- Discover the cross environment “Blast Radius” and the risk of a threat propagating across cloud accounts

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Alert on security policies



- Transform security queries into policies, automate alerting and response with customisable rules.
- Leverage pre-built alert rule packs for cloud security.
- Monitor alert trends over time to identify repetitive policy breach or miss-configurations

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Host based security

Tetration

How do we address this with Secure Workload?

Contain lateral movement

Microsegmentation

Continuously track security compliance

Policy compliance

Identify behavior anomalies

Process and communication

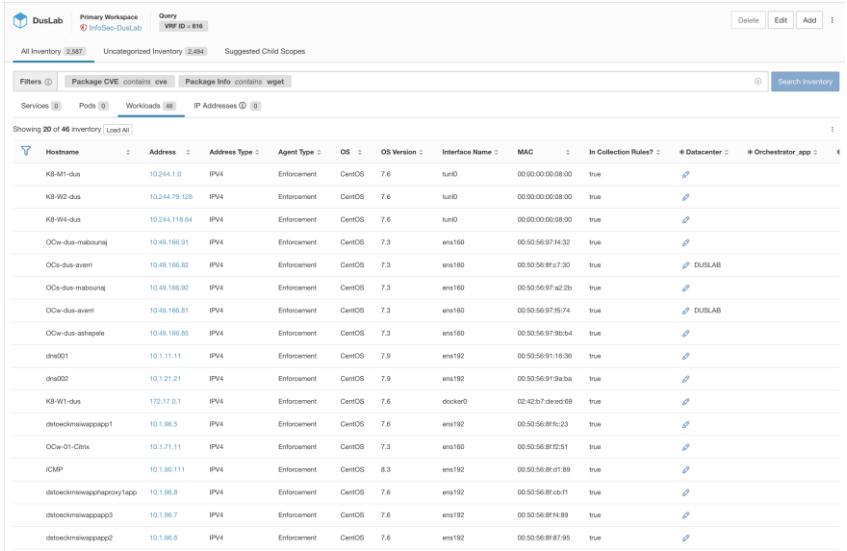
Reduce attack surface

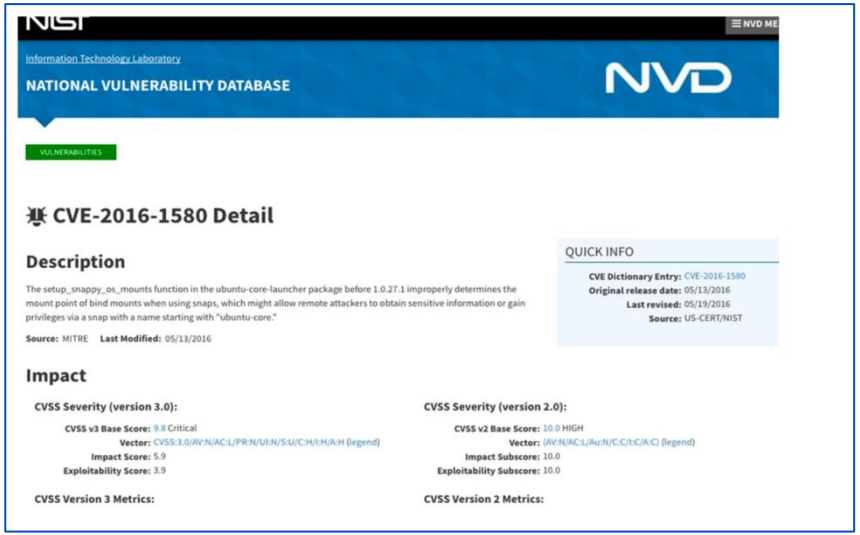
Software vulnerability

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Vulnerability Detection

Track Vulnerabilities in the Operating System or in User Space software in the workload.





Baseline Inventory based on Tags

Common Vulnerabilities Exposures CVE
https://nvd.nist.gov/

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Software package vulnerability – Policy action

Continually Verify Trust

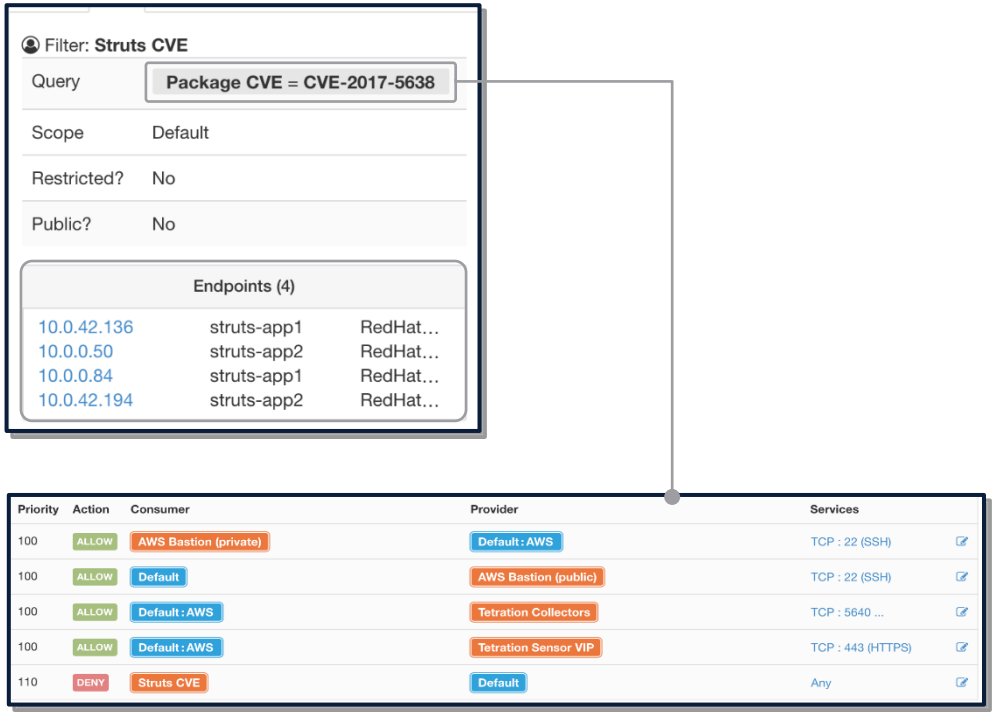
Set up filters to search for one or more vulnerabilities

Identify list of servers with the same vulnerability or software packages installed

Set up policy through UI or API to take specific action:

- Isolate a workload when servers are identified with the critical vulnerability

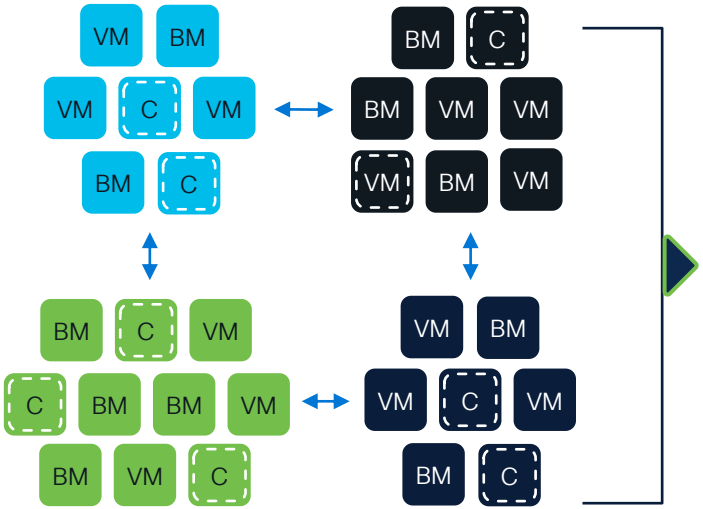
If a new workload has the same vulnerability, its communication will be restricted as well



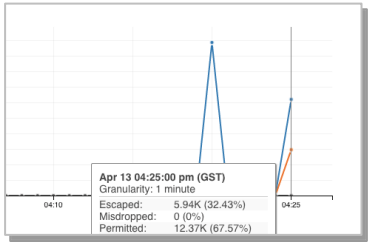
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Real-time policy compliance

Continually Verify Trust



Cisco Secure Workload Platform



Identify policy deviations in real time

Review and update segmentation policy

Integrate noncompliance policy events with SIEM systems

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Malicious or anomalous hash on a workload

Continually Verify Trust

- The process hash score of that workload will go to 0
- The security dashboard will display the process hash details

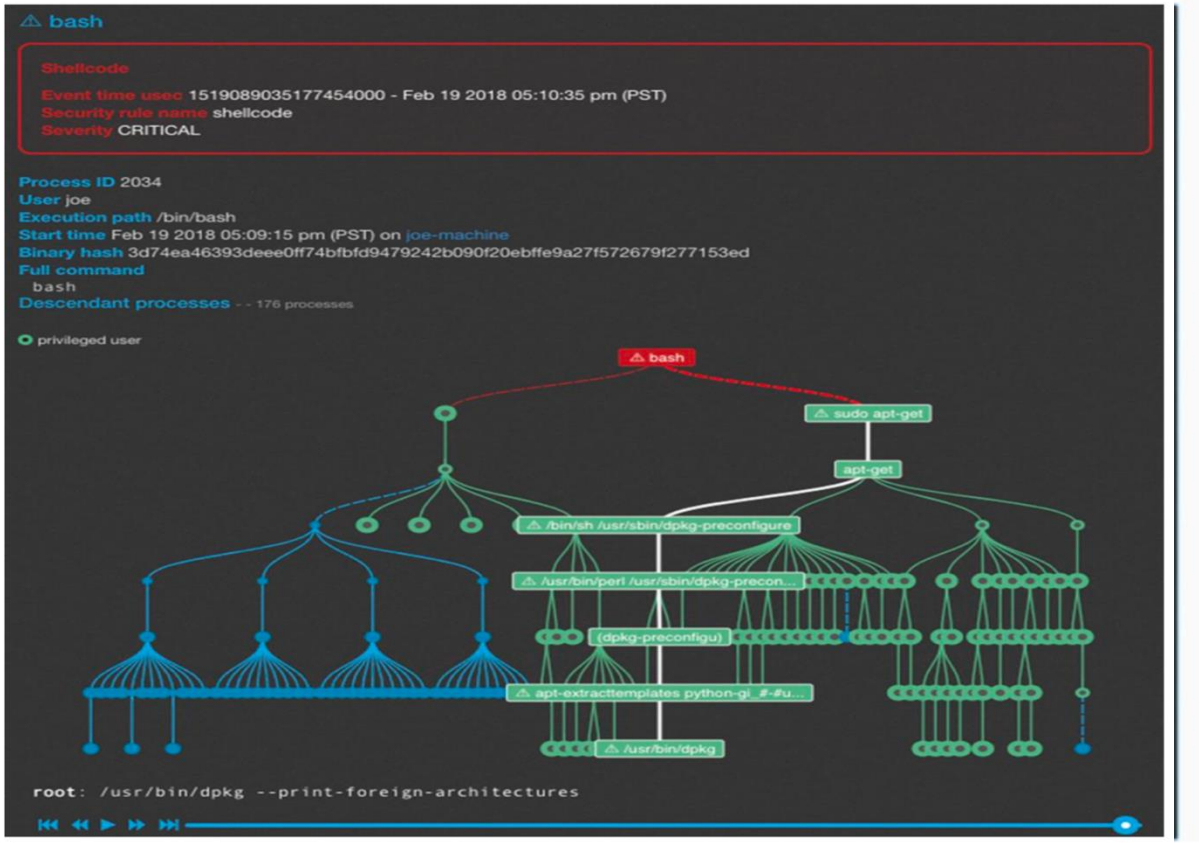
Workload profile, File Hashes tab:

SHA1 Hash	SHA256 Hash	File Path	Anomaly Score	Reason
d9a44b4	7eedeeb	/local/tmp/fakemw_linux_amd64	0.00	Malicious

SHA1 Hash	SHA256 Hash	File Path	Anomaly Score	Reason
d9a44b4	7eedeeb	/local/tmp/fakemw_linux_amd64	0.00	Malicious

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Detecting Code Execution



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

What about Remote Access ?

- Access your EC2
- Super User with DNG
- Full access with RaVPN

What about the EC2 instances management ?

- Direct access to the public IP Address?

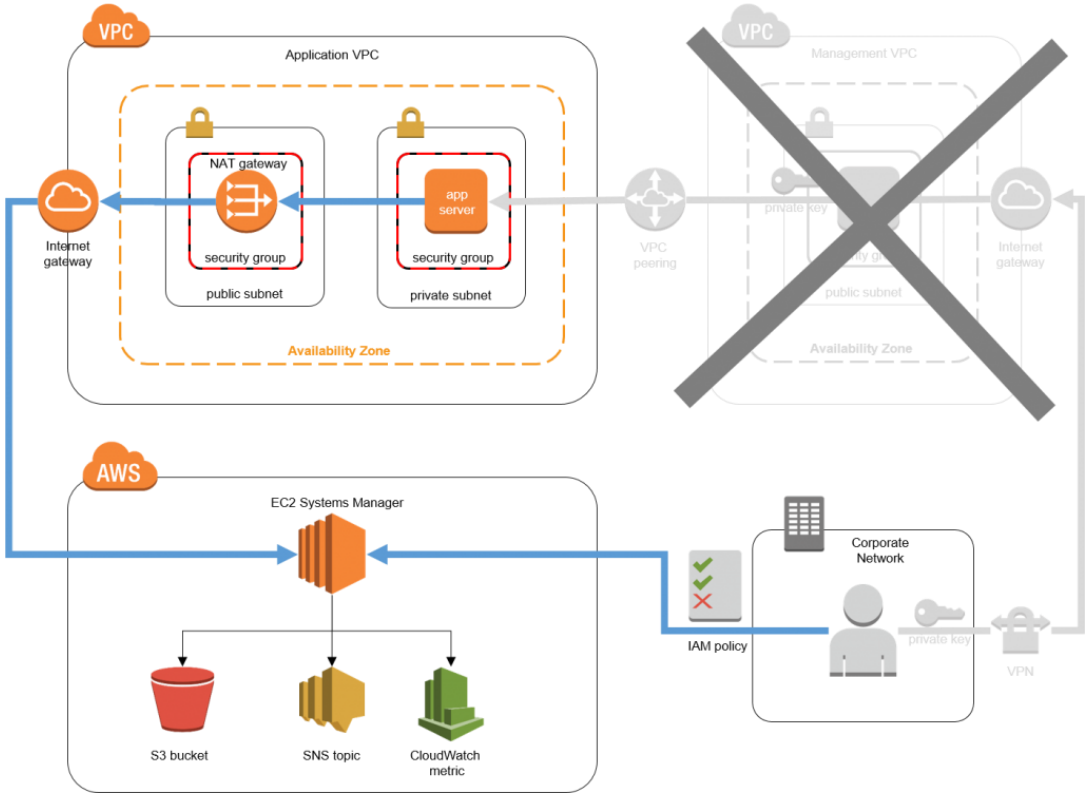
- Bastion host

- Direct Connect from on-Prem or VPN

- Leverage AWS EC2 System Manager

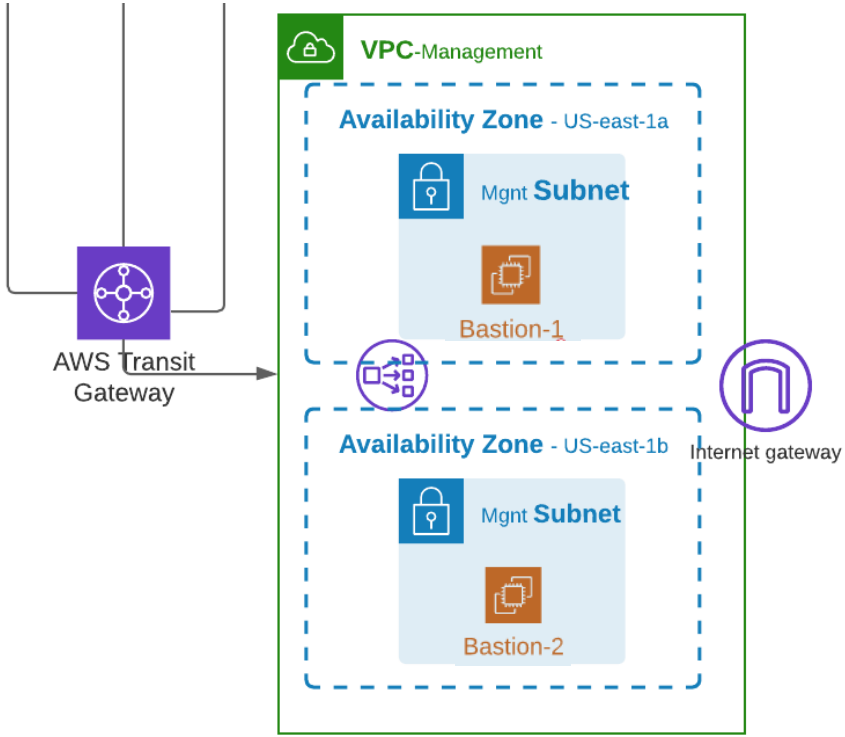
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

AWS EC2 System Manager



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Management VPC



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Provide SuperUser secured Access

DUO Network Gateway

DNG Use Cases for FabAstro...or else

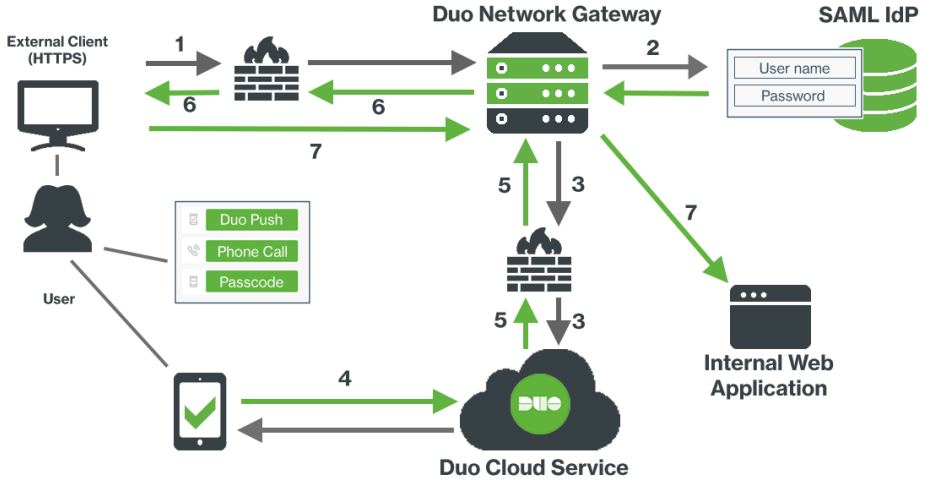
- An Accountant requires access to the on-premises Confluence instance to view internal documentation.
- A Software Engineer needs to push code to their internal repository.
- A Support Engineer needs access to a web portal that allows adjusting a feature flag for a customer.
- A Systems Architect wants to connect to a bastion host, switch, etc. without connecting to the VPN.

Cisco Live 2022 FOR REFERENCE TECSEC-2111

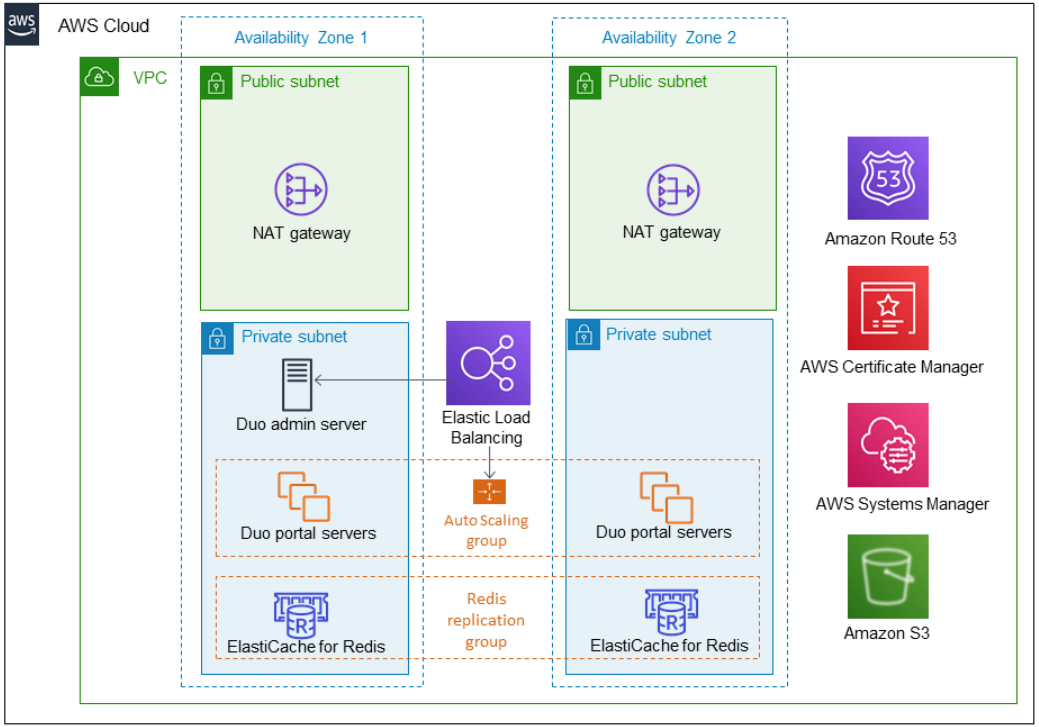
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is Duo Network Gateway ?

The Duo Network Gateway enables organizations to provide Zero Trust Remote Access to web applications, web pages and SSH servers without the requirement of a VPN.

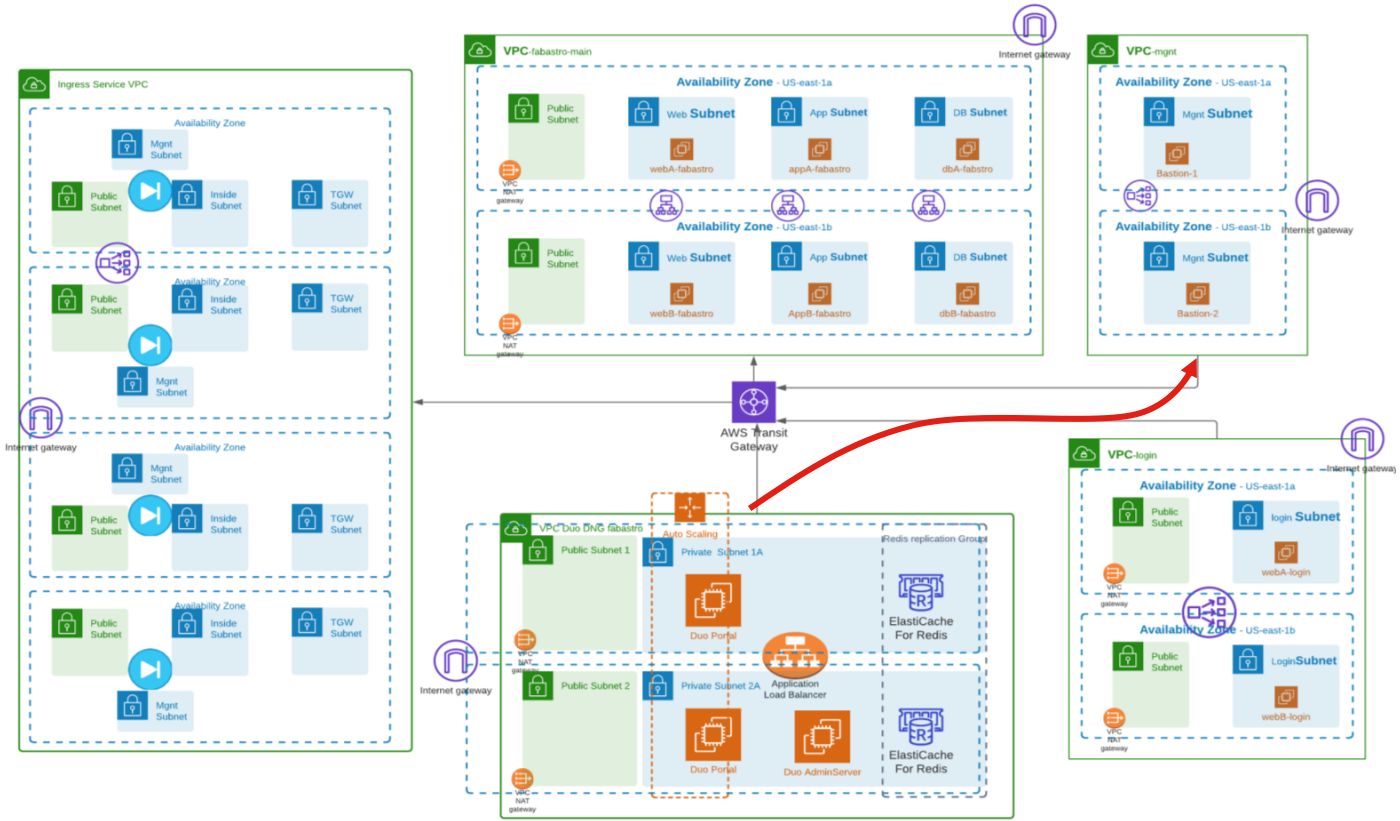


© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public



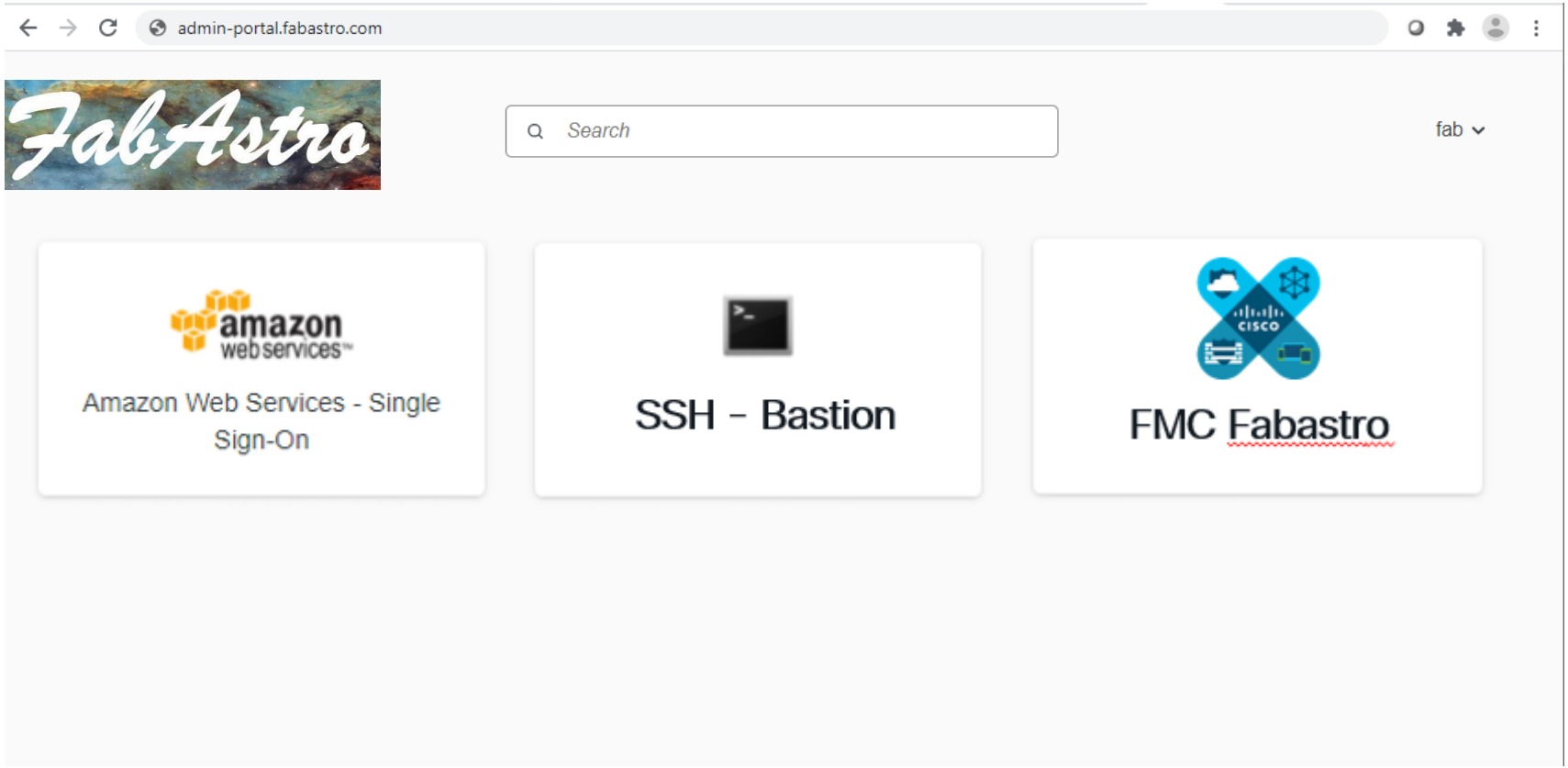
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

DNG in FabAstro: Access for Admins



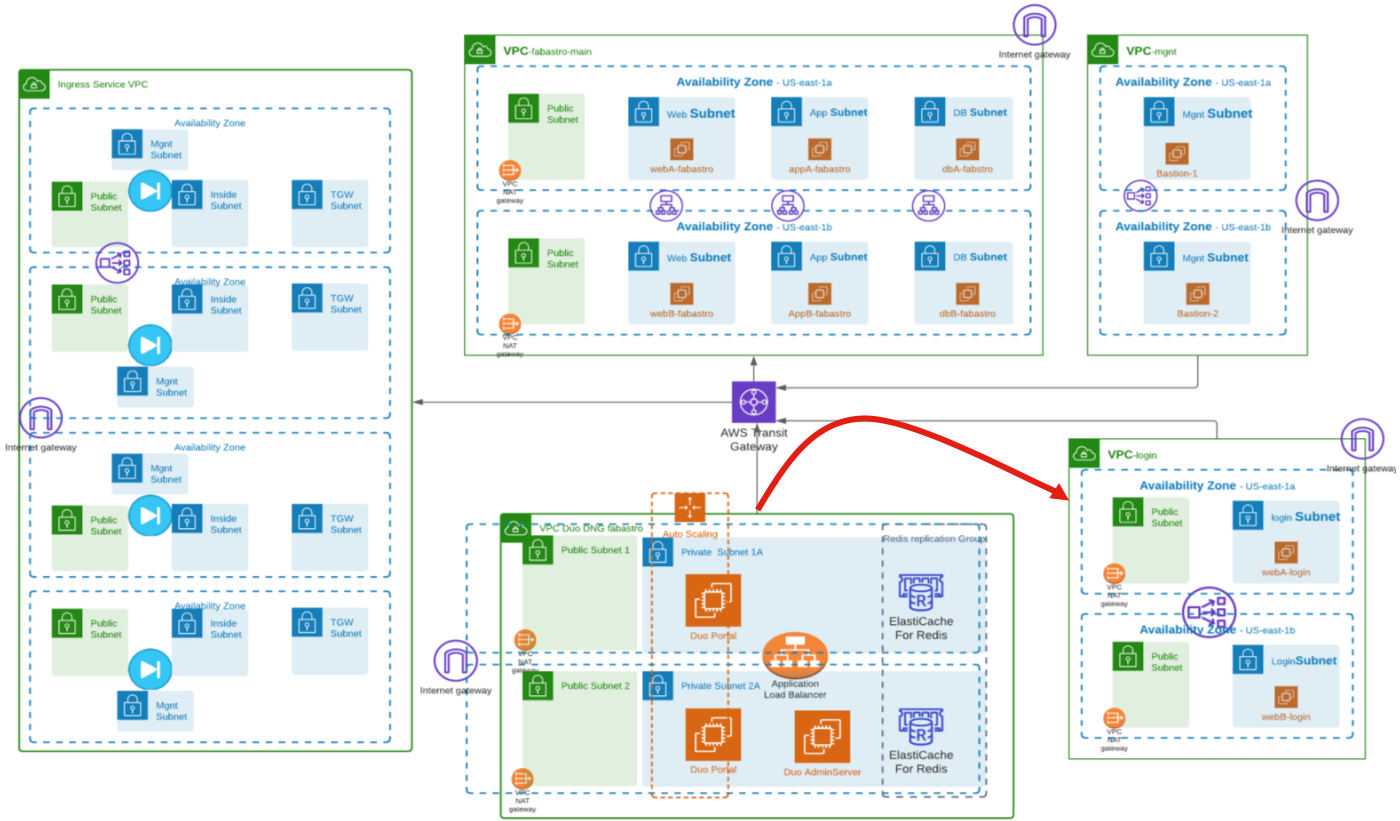
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Using DNG to access FabAstro Admin Portal



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

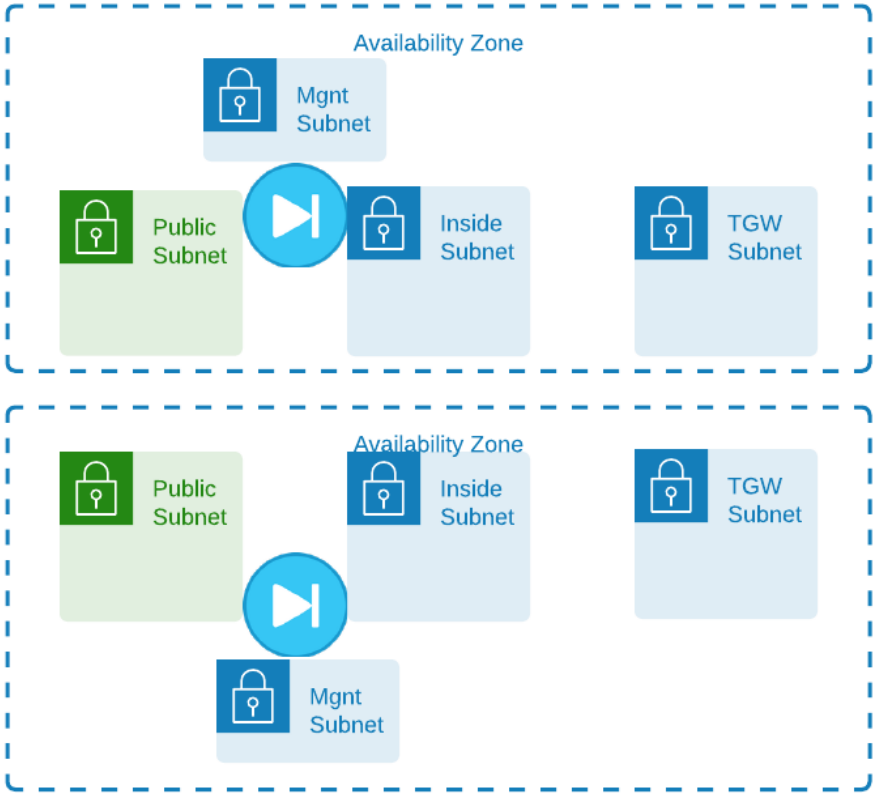
DNG in FabAstro: Web portal for Privileged Users



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

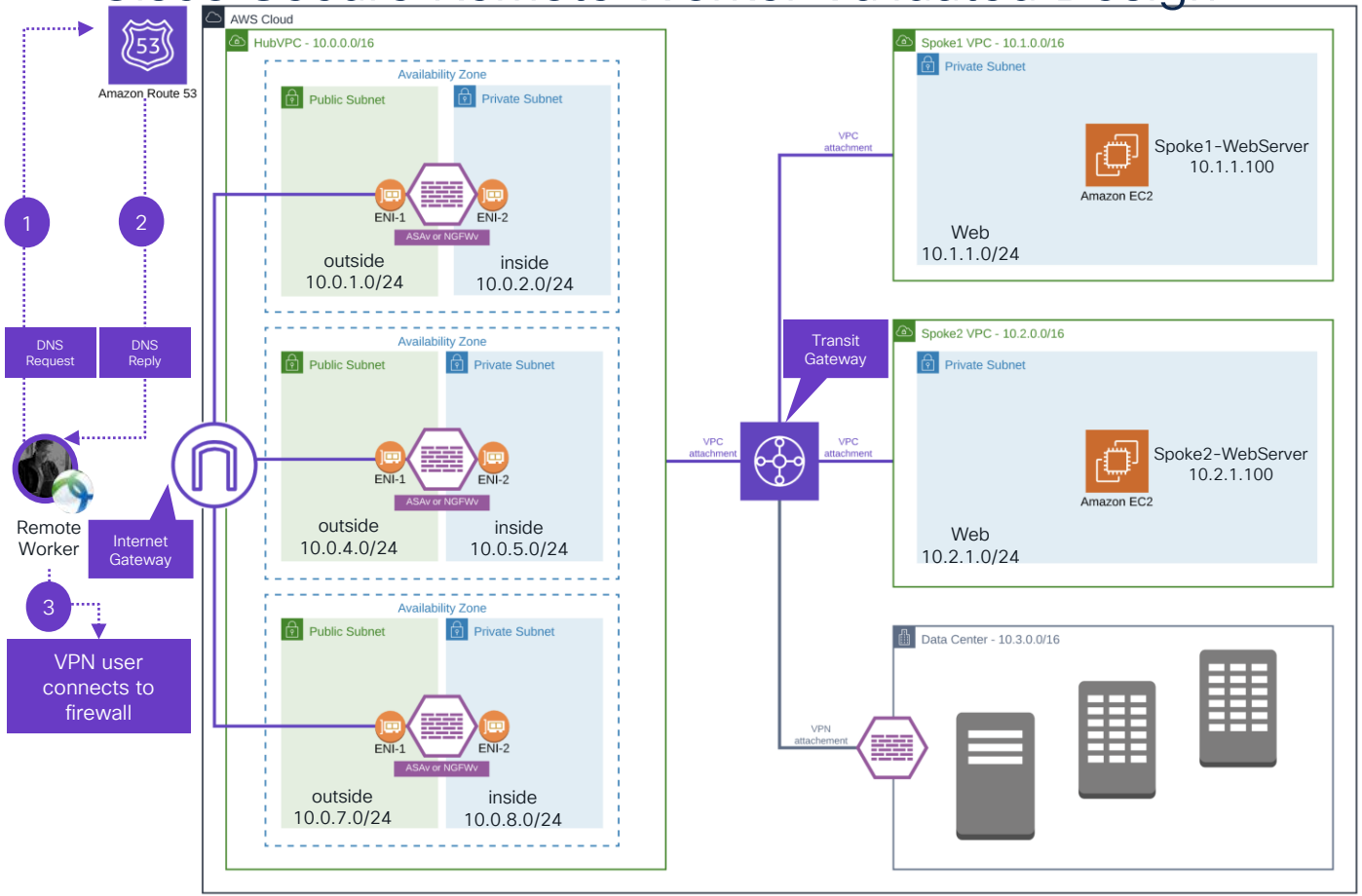
Deploy and configure remote access VPN

Remote Access to Management VPC



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

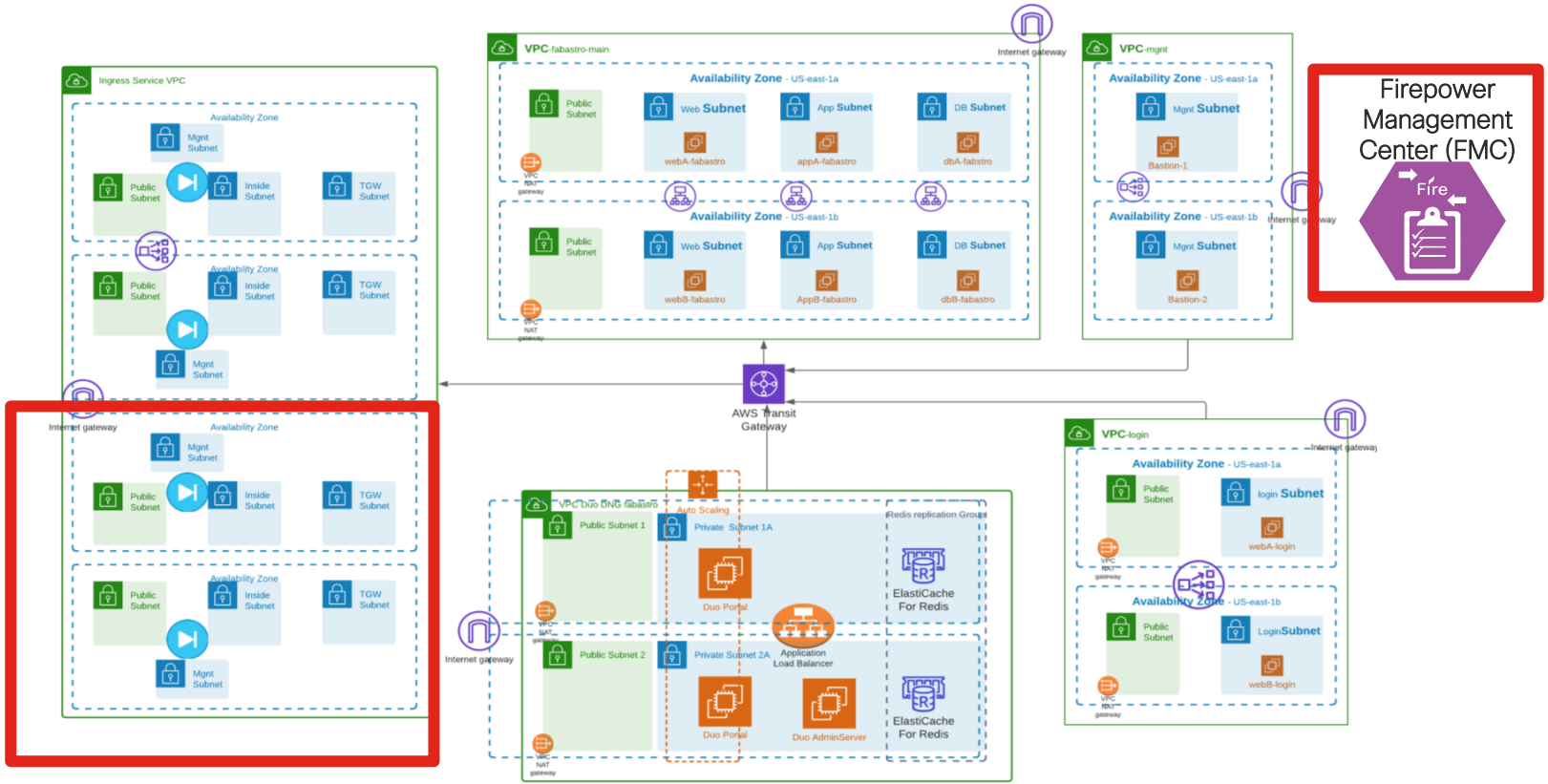
Cisco Secure Remote Worker Validated Design



- VPN Load balancing using Route53
- AWS Route 53 maintains host record for each firewall
- TTL is defined on AWS Route 53
- AWS Route53 health check to monitor firewall
- Each AZ may have multiple firewalls
- Cisco ASAv or NGFWv acts as a VPN concentrator
- Transit Gateway connects VPC using VPC attachment
- Transit Gateway connects to Data Center using VPN attachment

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

RAvpn with FTD and FMC in FabAstro



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

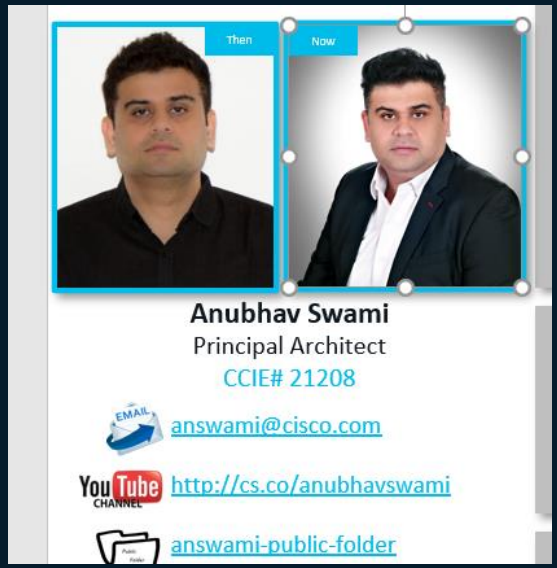
The bridge to possible

Cisco Secure Firewall Cloud Native on AWS

Building a Scalable Edge

Anubhav Swami, Principal Architect
@swamianubhav

BRKSEC-3561

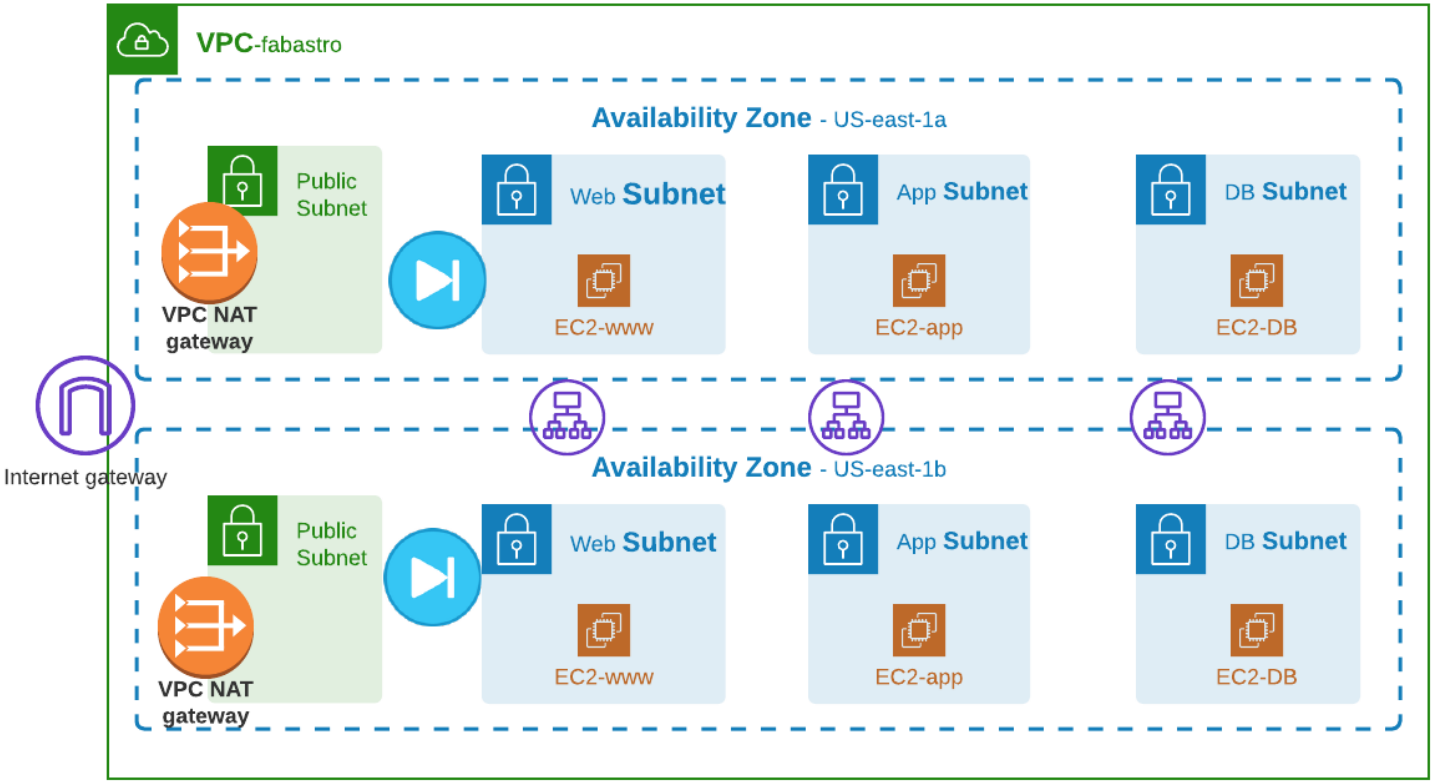


cisco Live!

EC2 Instances Outgoing sessions

- Nat Gateway for each availability Zone
- Egress transit VPC

Example using Nat Gateway



Cisco Live 2022 FOR REFERENCE TECSEC-2111

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Challenges with per VPC Nat Gateway

Scalability

Internet gateway and NatGateway per AZ for each VPC

Financial

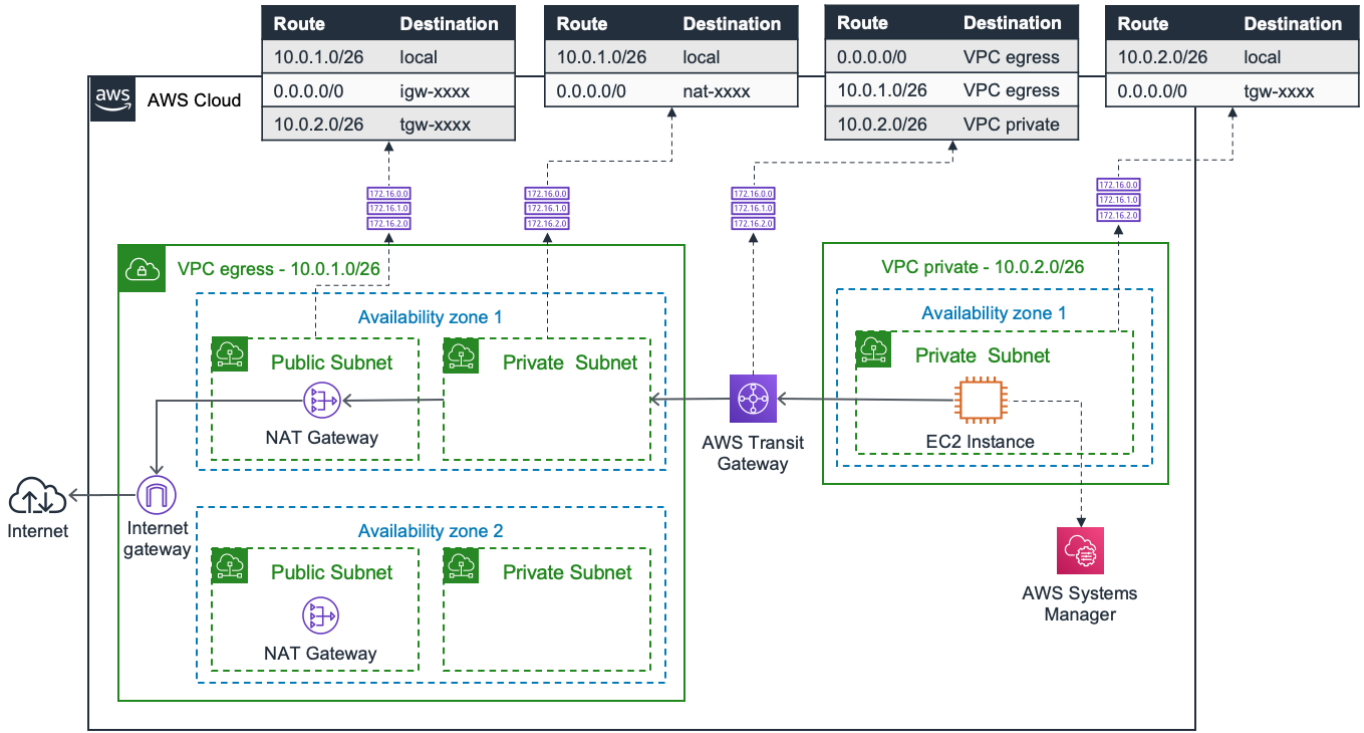
Refer to Scalability challenge

Security

No control nor visibility over outgoing sessionsh

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example using Egress Transit VPC



Possible to insert a single instance of NGFW per AZ

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conclusion

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.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

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
- Secure Web Appliance
- ISE TrustSec
- Cisco DNA Center

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

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**

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

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!

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you


cisco Live!
ALL IN