The bridge to possible

# Enhance AWS Native Security with Cisco Security

Fabien Gandola, EMEA Cyber Security TSA
fgandola@cisco.com

cisco Live!

BRKSEC-1831

# Cisco Webex App

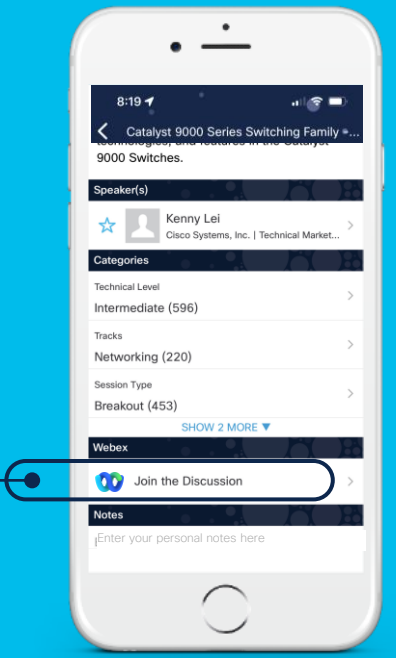
## Questions?

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

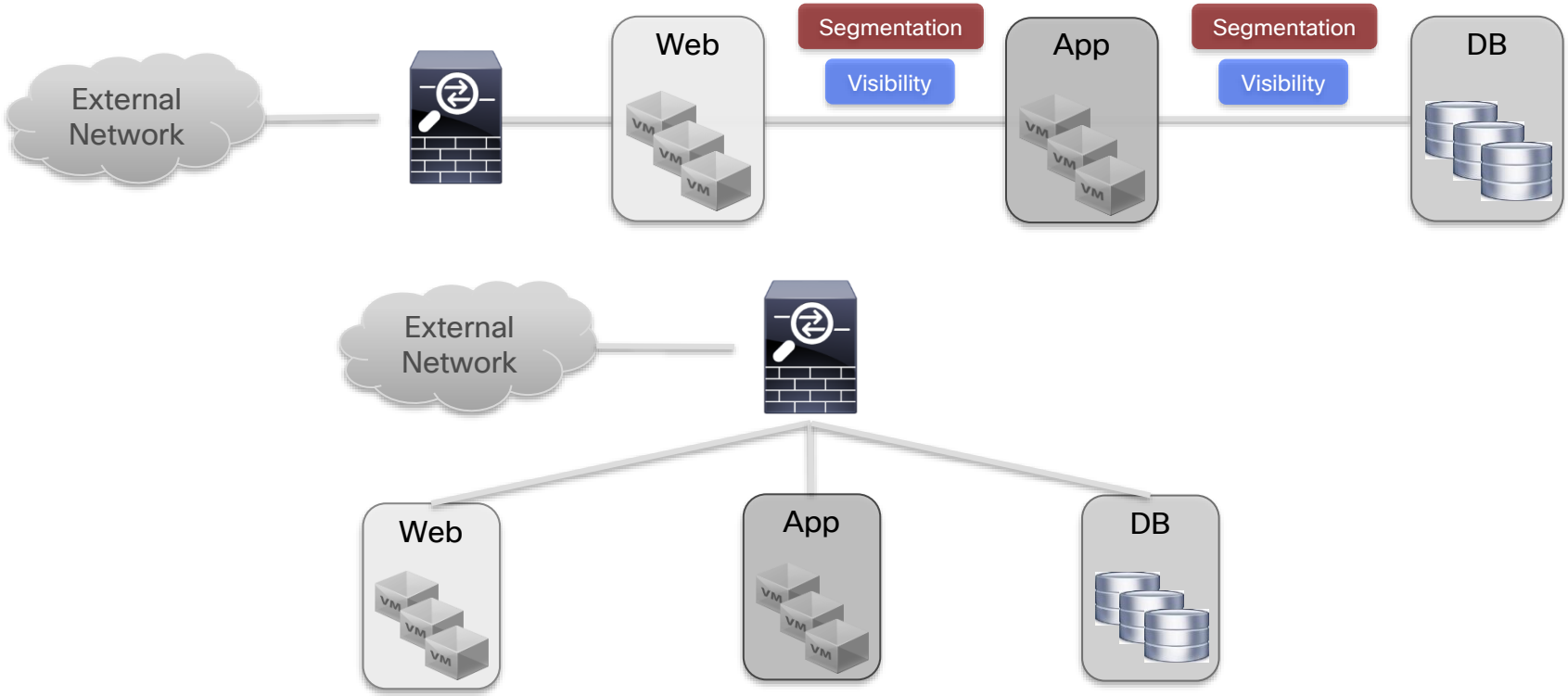
## How

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 until February 24, 2023.

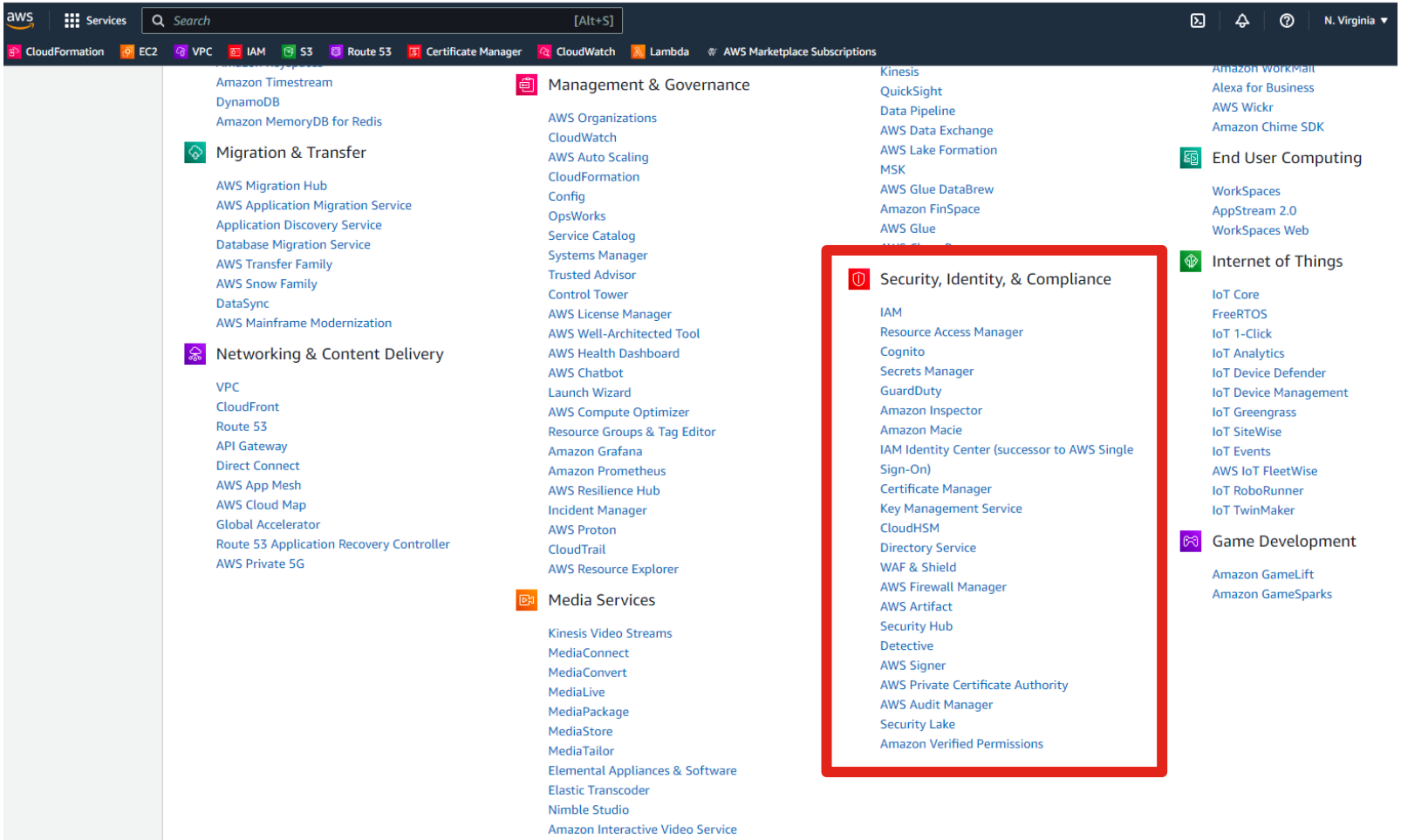


# We need that …



# Into that…

# Keeping coherent and consitent Security



# AWS Security Solutions

## Identity

**AWS Identity & Access Management (IAM)**

AWS Organizations

AWS Cognito

AWS Directory Service

AWS Single Sign-On

AWS Secrets Manager

## 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**

# What to expect and not to expect ?

- No deep dive AWS
- No deep dive in Cisco Security
- No all scenarios (little about remote)
- Very little configuration
- No troubleshooting

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

# Agenda

- Security Challenges in public cloud
- What type of service and architecture to deploy my application ?
- **How do I perform access control and Segmentation ?**
- **How do I insert NGFW ?**
- What about Remote Access ?
- Increasing Visibility
- Conclusion

# About Me

**Fabien Gandola**
fgandola@cisco.com

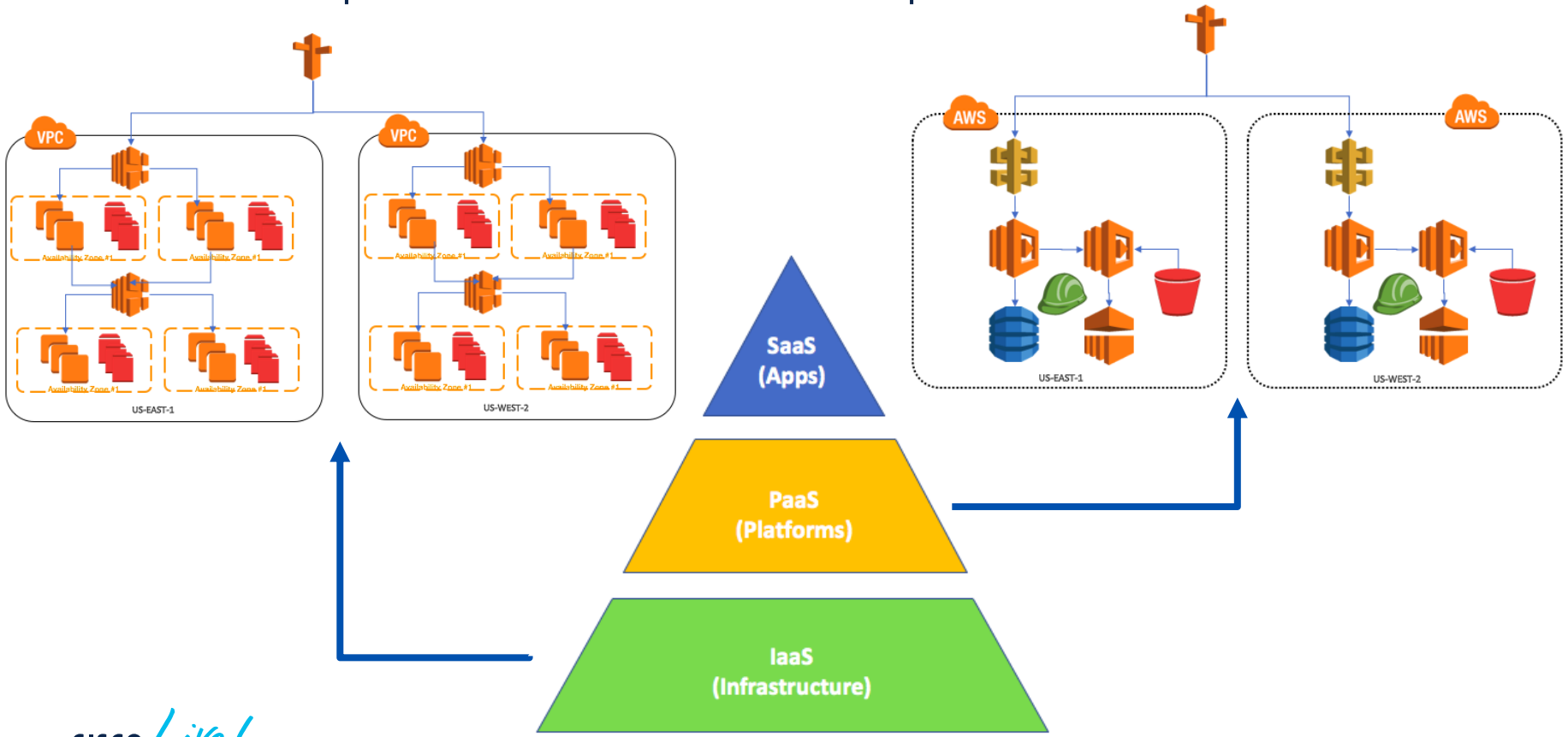
TSA Cyber Security EMEA

23 years in Cisco

# 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

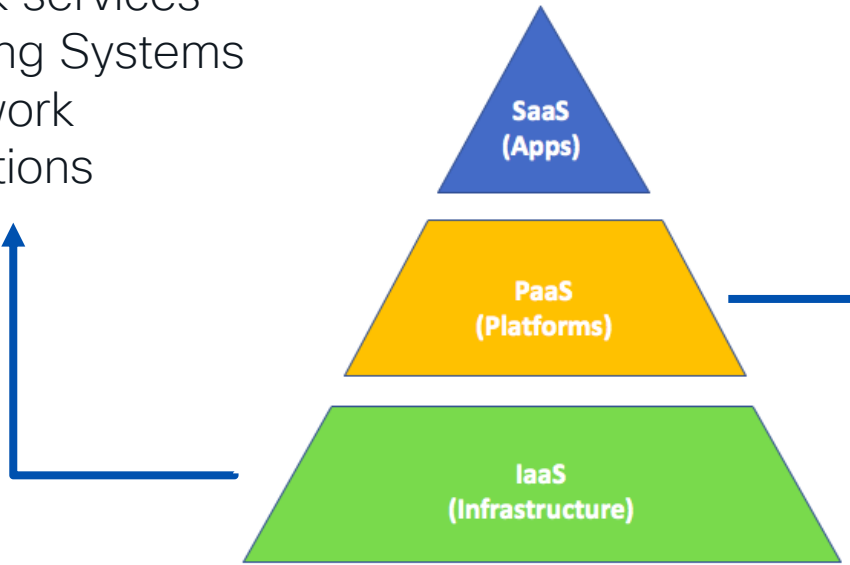


# IaaS compared to PaaS Compared to SaaS

Manage :
- Nothing

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

Manage :
- Network limited
- Applications



# 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

# Securing the Cloud


Network Segmentation

Visibility & Threat Detection

Identity

Cloud Security Posture Management

# FabAstro Application in AWS

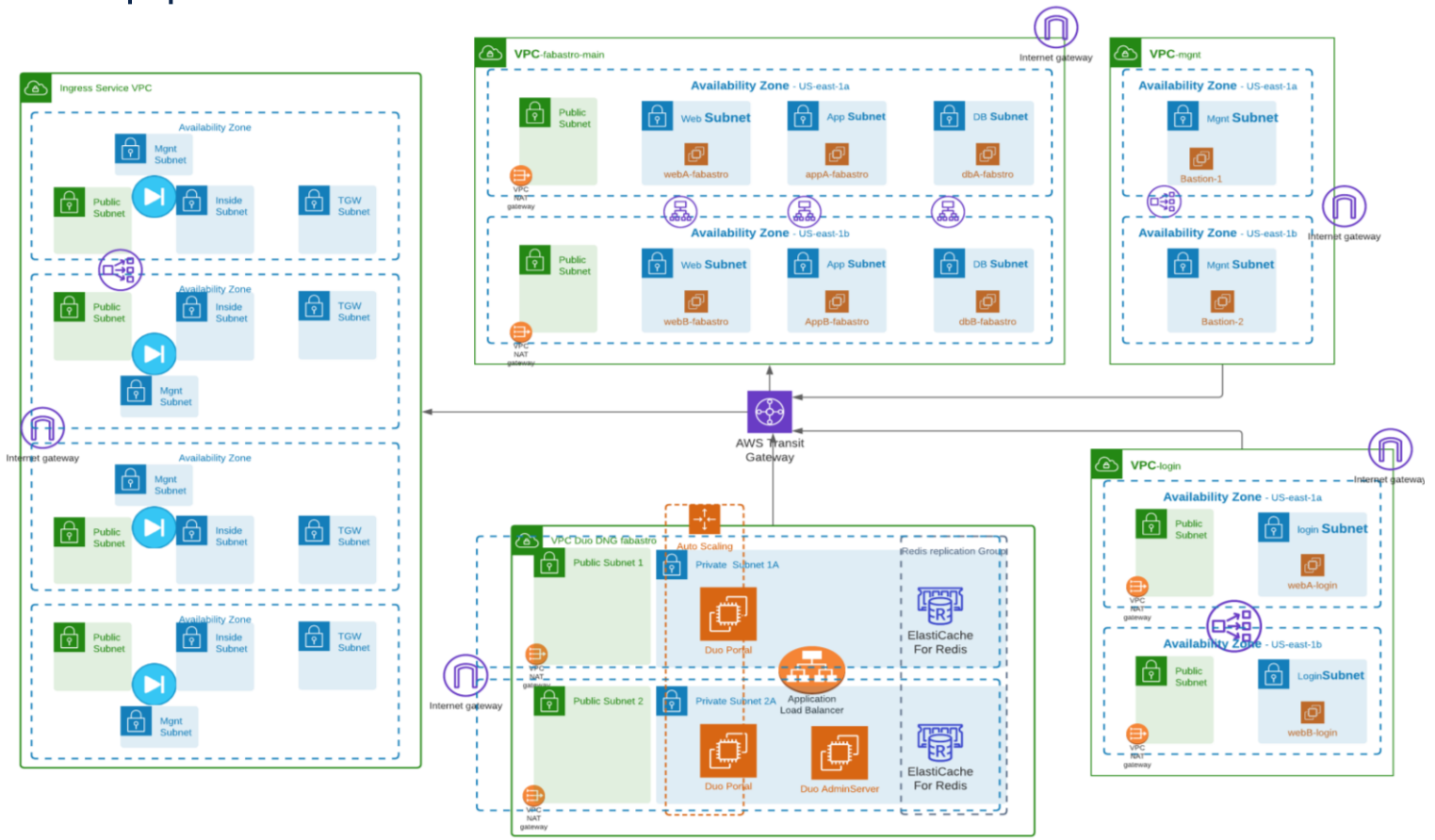
Amazon S3

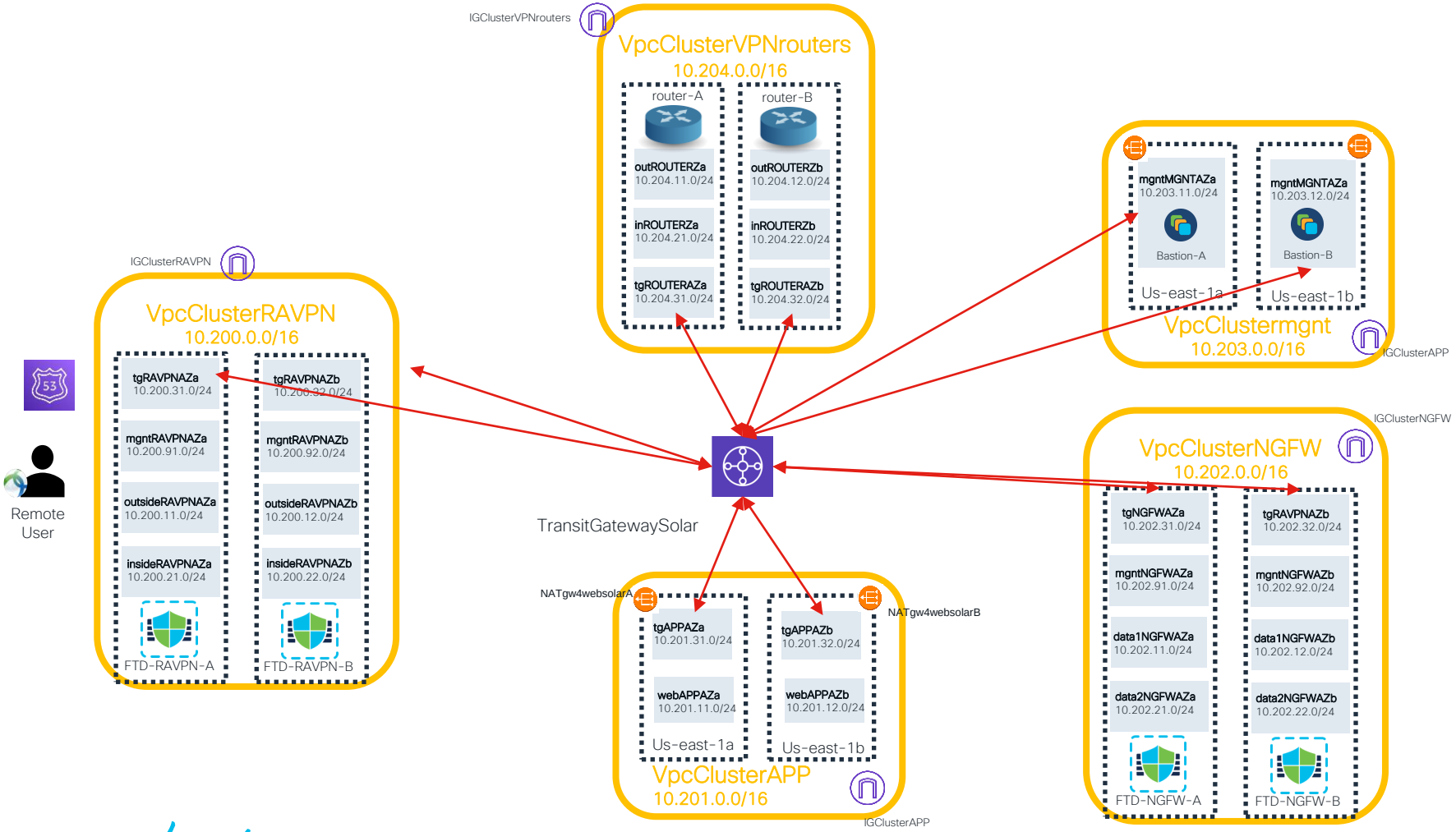
AWS Route 53

AWS Certificate Manager

AWS CloudFormation

AWS IAM





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

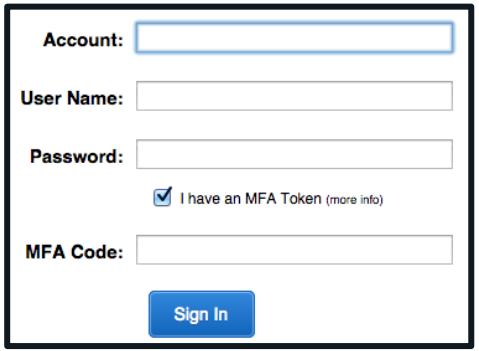
# AAA with AWS

| Authenticate | Authorize | Audit |
| --- | --- | --- |
| IAM Username/Password<br>Access Key<br>(+ MFA)<br>Federation | IAM Policies | CloudTrail |

# 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**

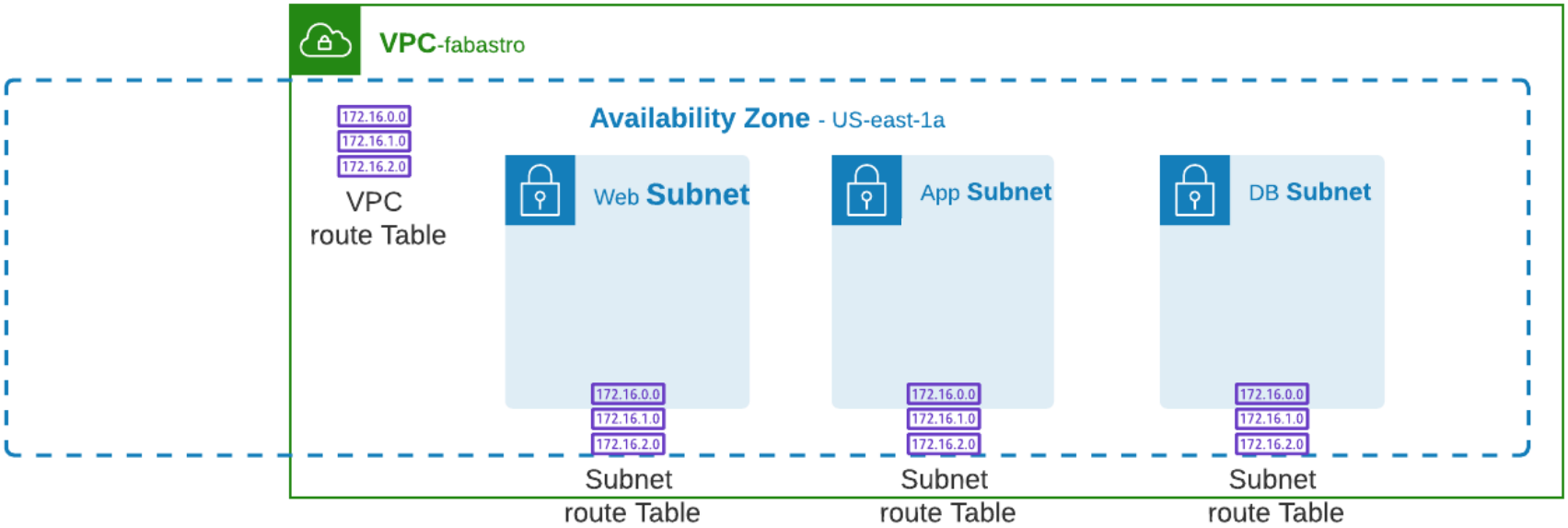
Ex: `AKIAIOSFODNN7EXAMPLE`

**SECRET KEY**

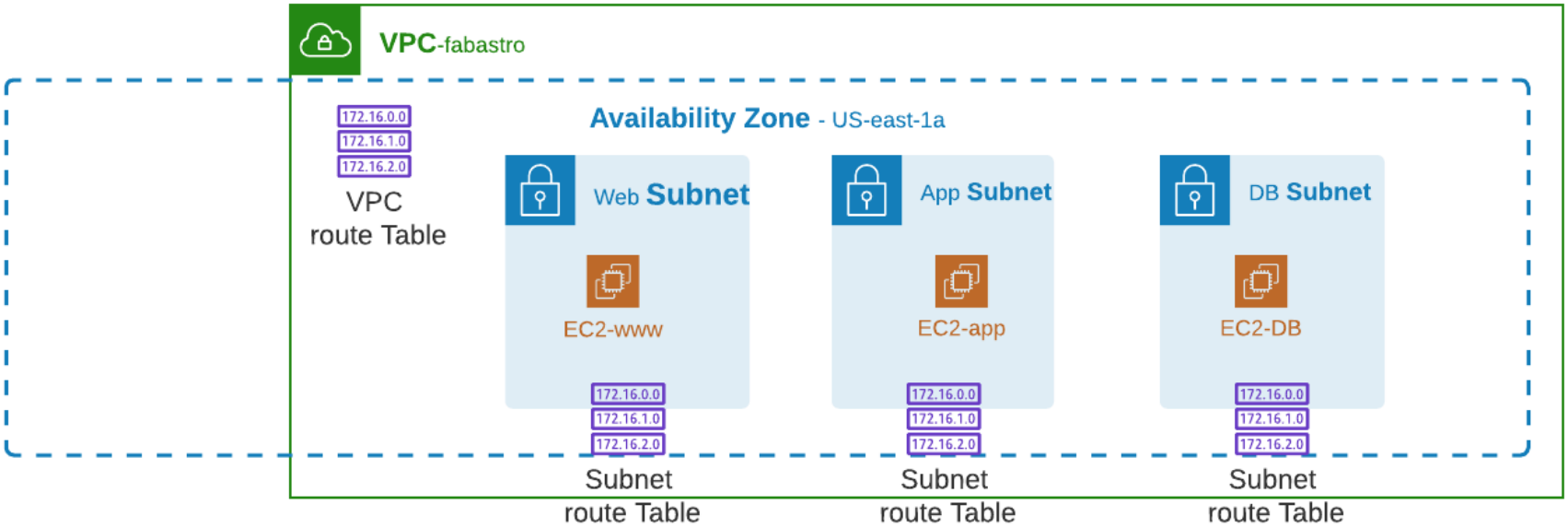
Ex: `UtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

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

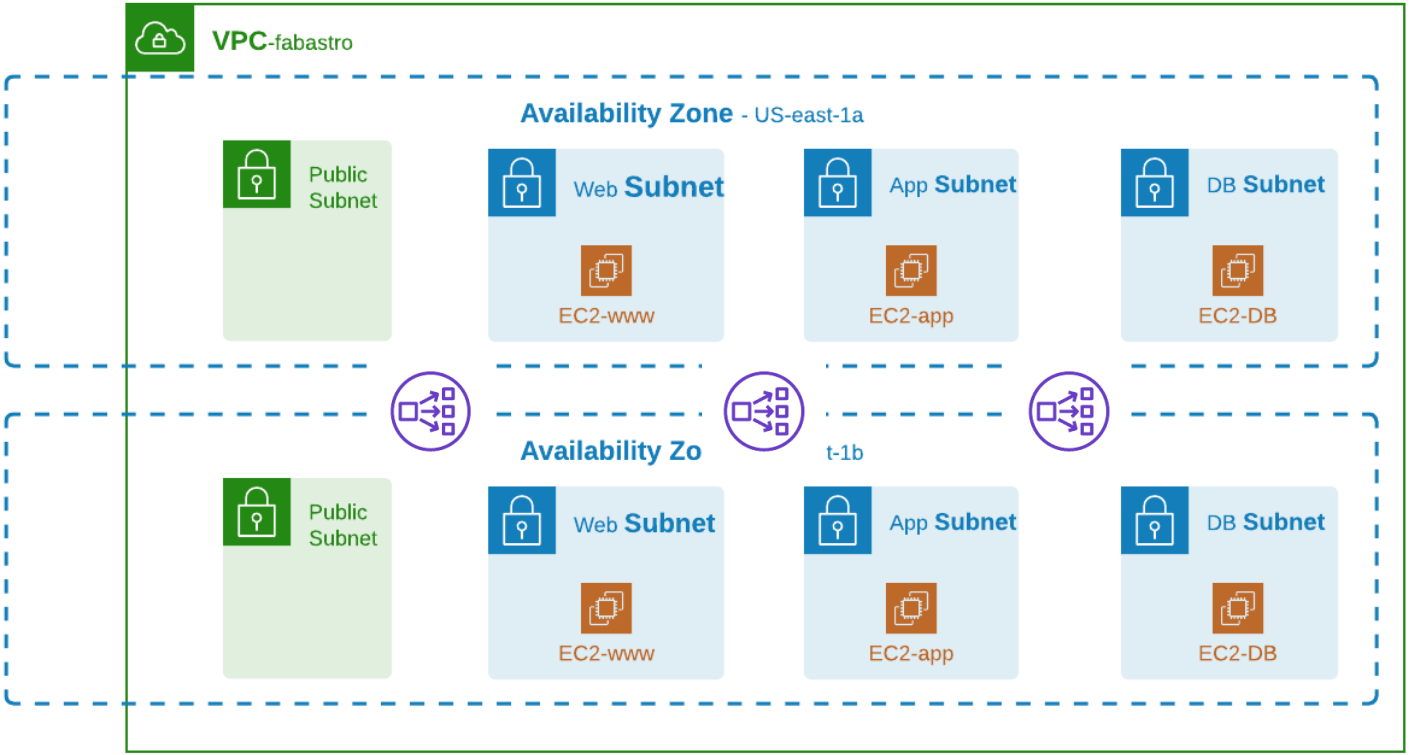
# My VRF… VPC sort of ( actually Route Tables)



# In AWS IaaS… my workloads = Instances



# HA with multiple AZ and LB



# 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

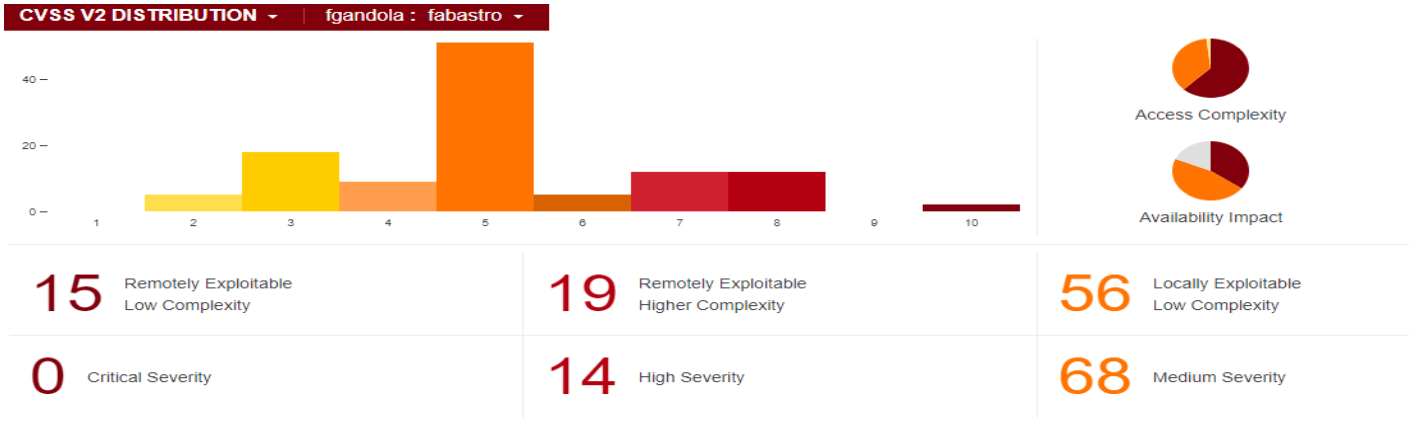
| Alert | Source | Time | Description |
|---|---|---|---|
| Inbound Port Scanner | Network | Nov. 27, 2020, 10:19 a.m. | Device was port scanned by an external device. T |

| 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 |

--

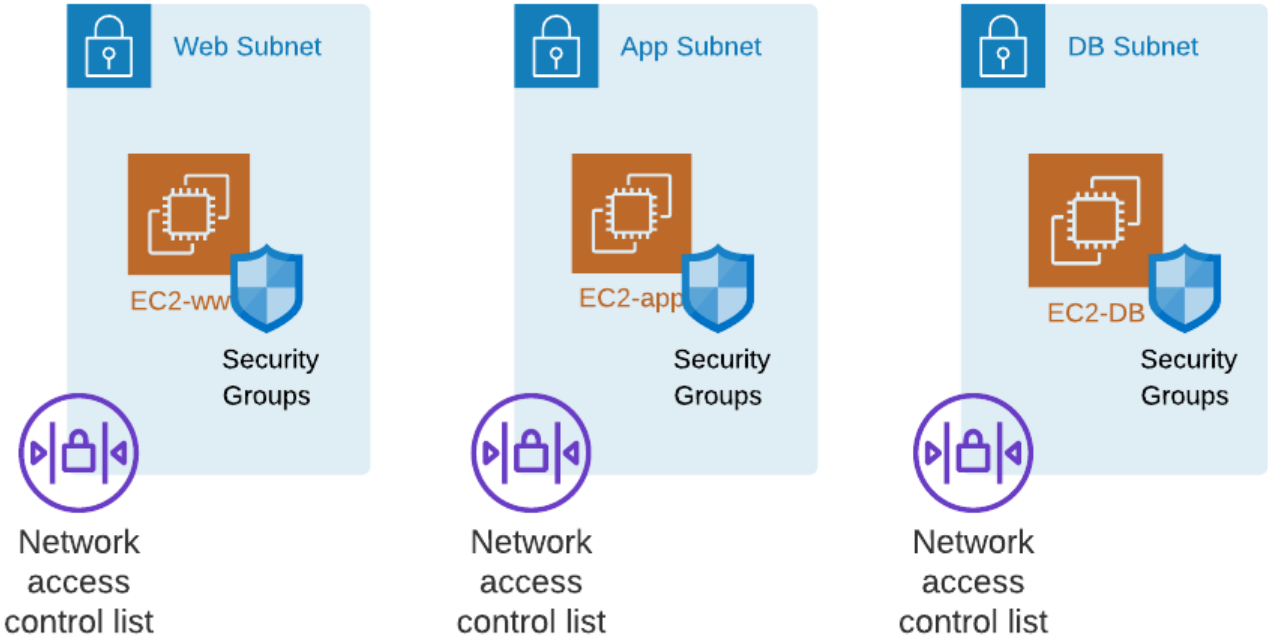
# CSW Vulnerability Assessment




| 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 |

# AWS Segmentation solutions

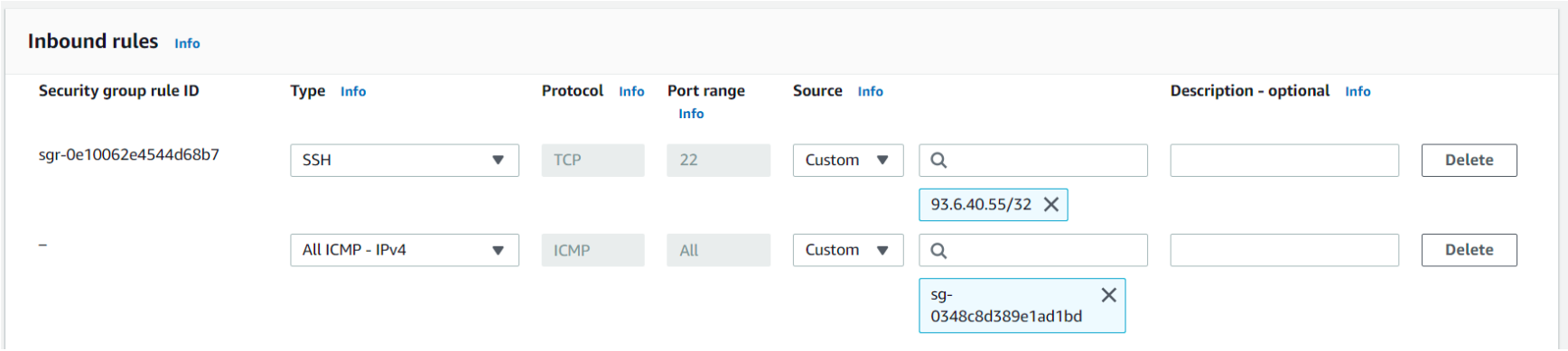
## Security Groups and Network Access list



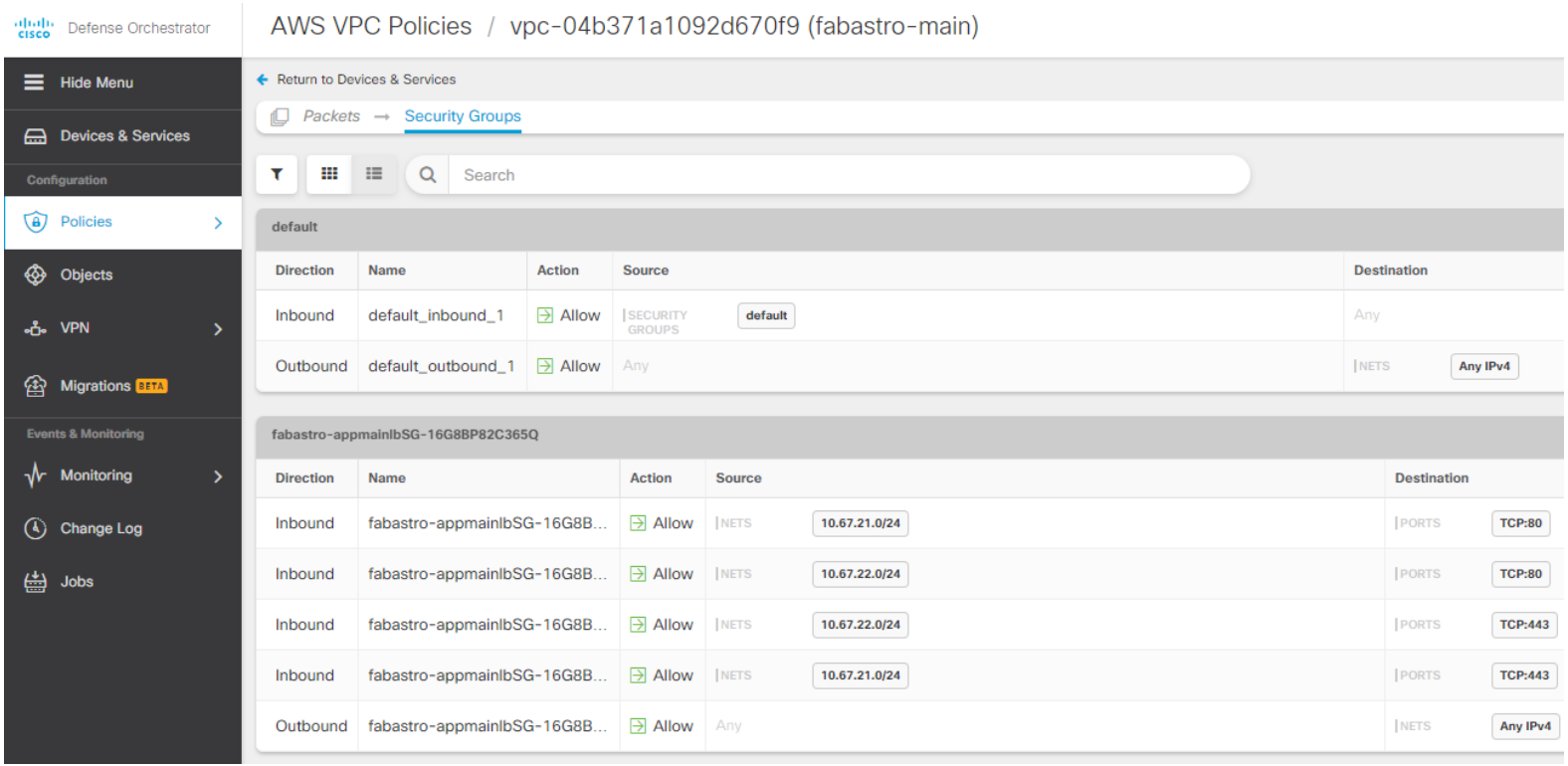
# Network ACL and Security Groups

| |  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.<br>First match applied | All rules evaluated before decision |
| Occurence | Only 1 per Subnet | Multiple per Instance |

# Use security group as Source winthin VPC



# Security Groups in CDO



# Quick Overview

- EC2
- VPC
- S3
- IAM
- Cloudformation

- Network ACL
- Use security group

# How do we address this with Secure Workload?

Contain lateral movement

Microsegmentation

Continuously track security compliance

Policy compliance

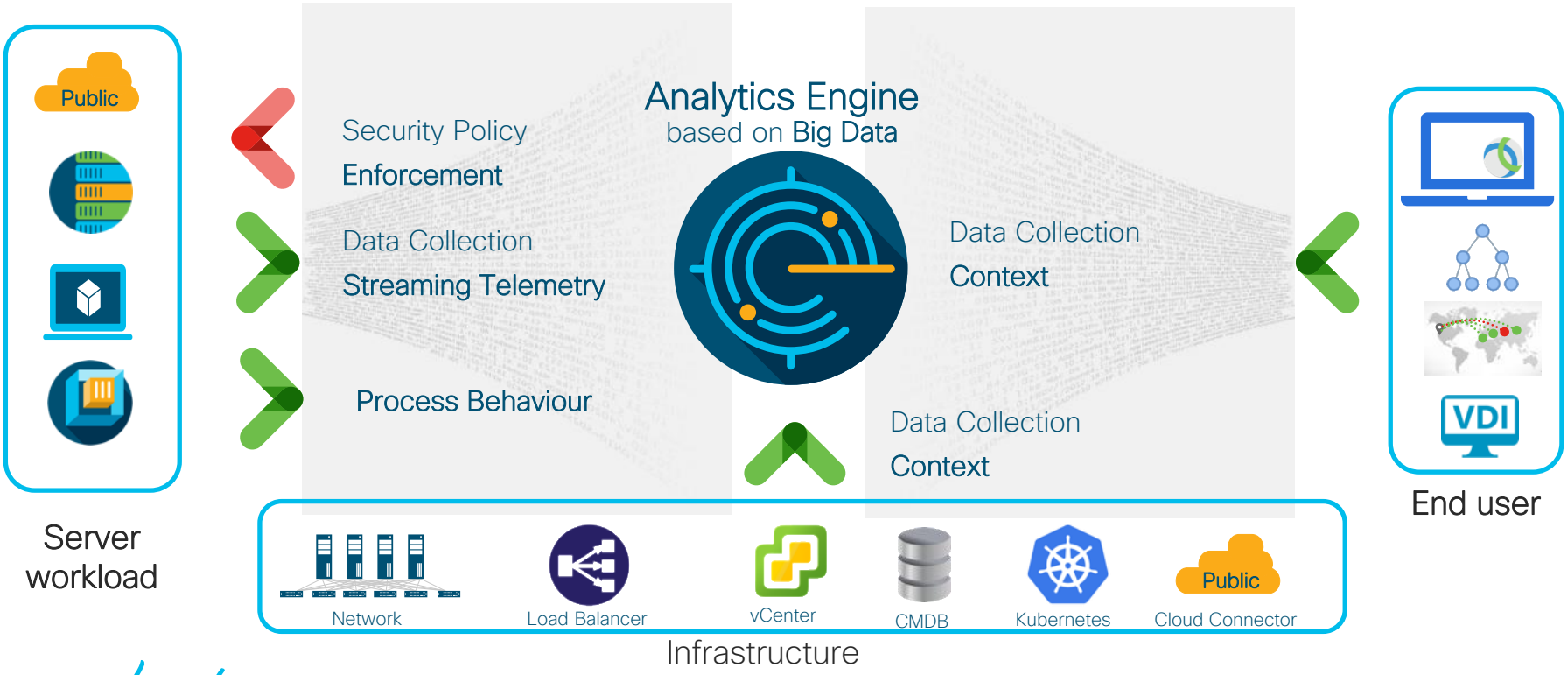
Identify behavior anomalies

**Process and communication**

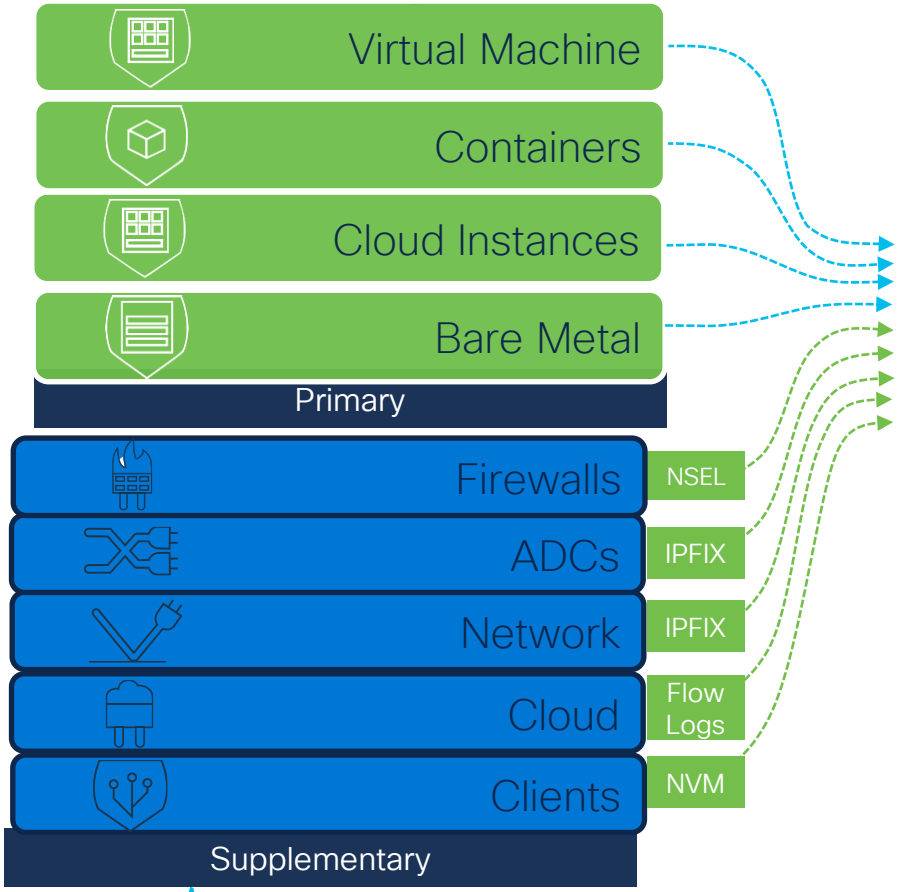
Reduce attack surface

Software vulnerability

# Secure Workload Architecture



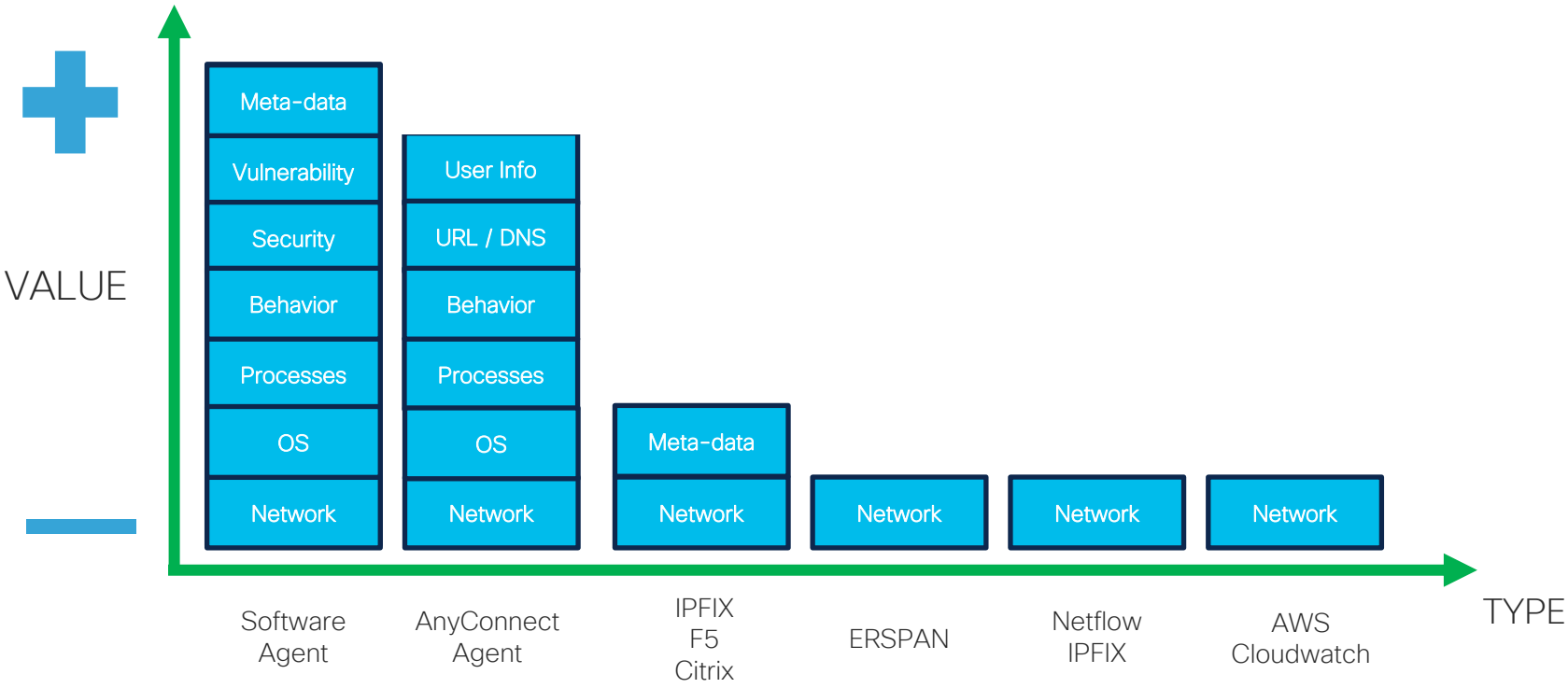
# Rich visibility and workload behavior baseline




Telemetry

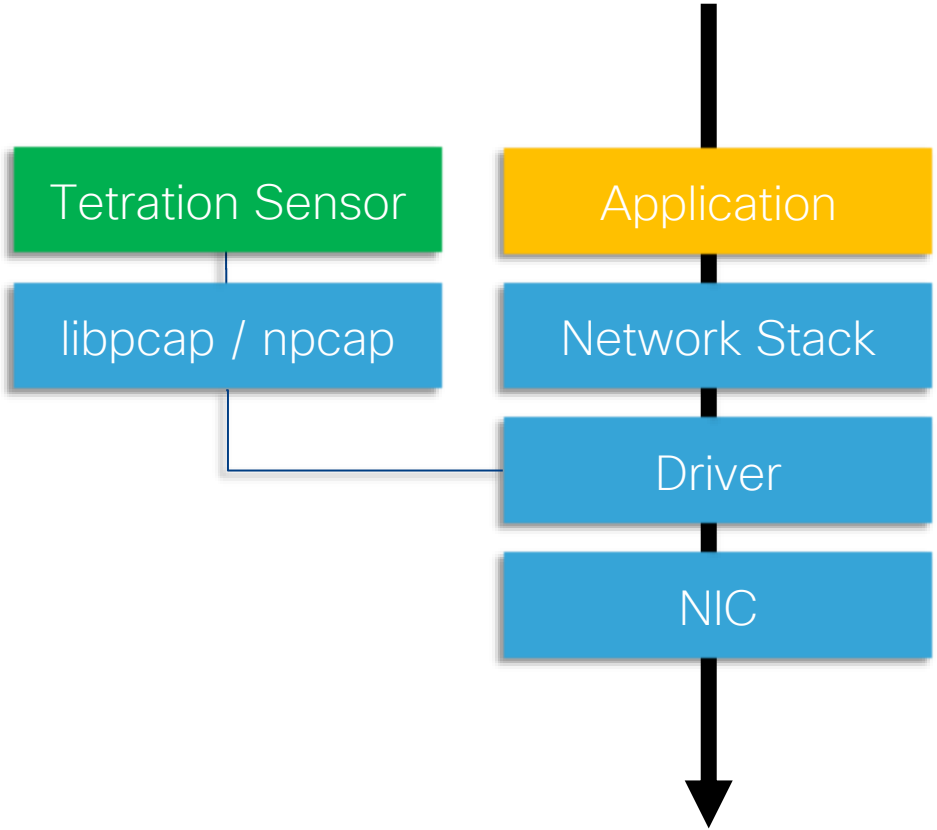
- Visibility of all communications
- Detailed machine/process info
- Any environment, any cloud
- Construct inventory of every endpoint

# Different Data Sources provide different value



# Software sensors

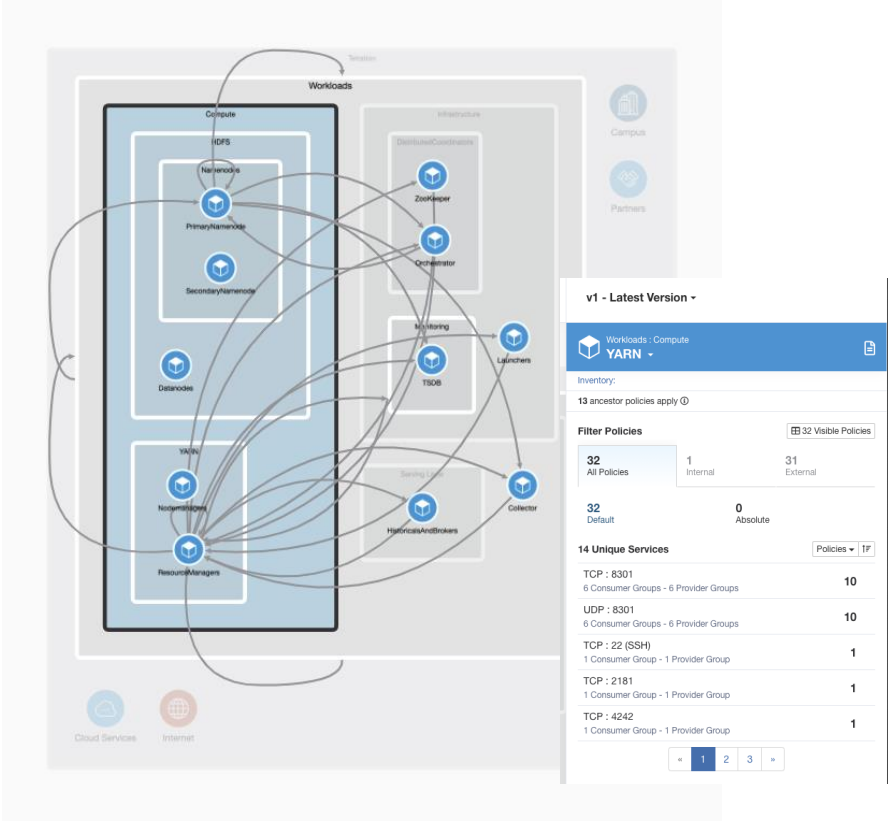
1. Minimum impact
   - Sits in User Space
   - Low CPU (< 3%)
   - Designed by Kernel Developers
2. Secure
   - Code Signed
3. Internal SLA enforcement with smart QoS
   - CPU protection
4. No latency effect



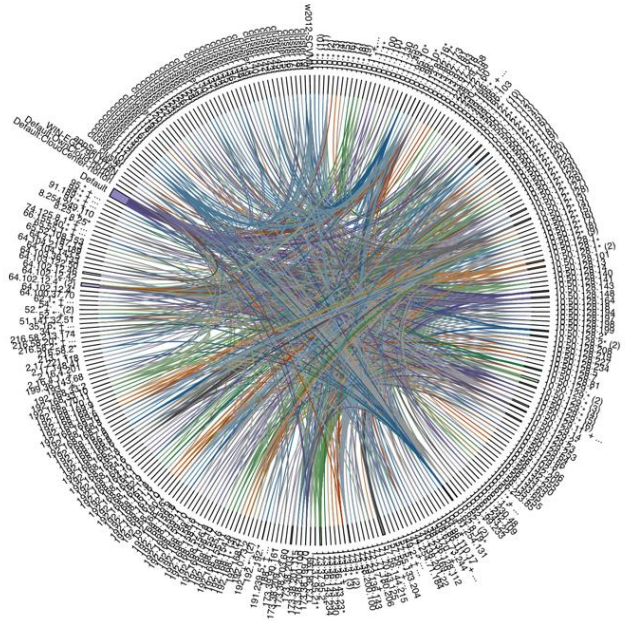
# Relationship among application components

Secure Workload provides the blueprint for communication dependencies between application components as well as other IT services

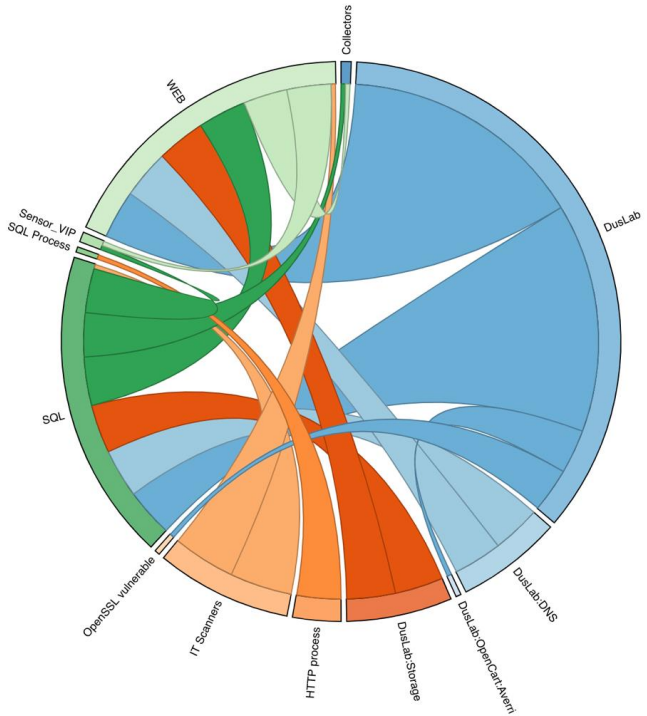
- How are the different application tiers communicating?
- Are there direct connections coming to database servers?
- Which communication is going through load balancers?
- How are users connecting to the application?
- Are there connections going out that should not be allowed? For example, a production database talking to a nonproduction database?



# Application Dependency Mapping
## Artificial Intelligence & Machine Learning



Unfiltered data collection results




Application Dependency Map provided by ML & AI

# Automated Application Policy Discovery

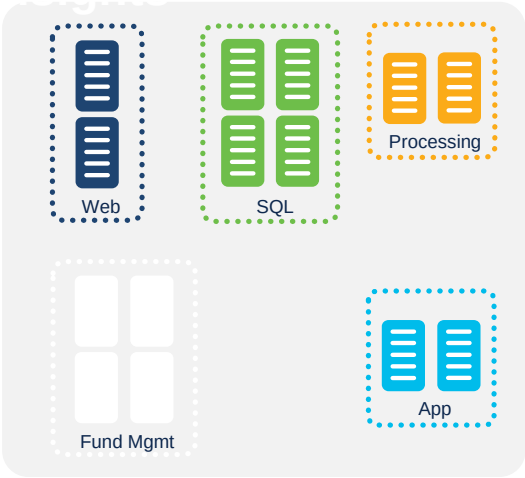
Baseline workload protection posture

- Network communications
- Process behaviour
- Labels

# Automated Application Policy Discovery

Baseline workload protection posture

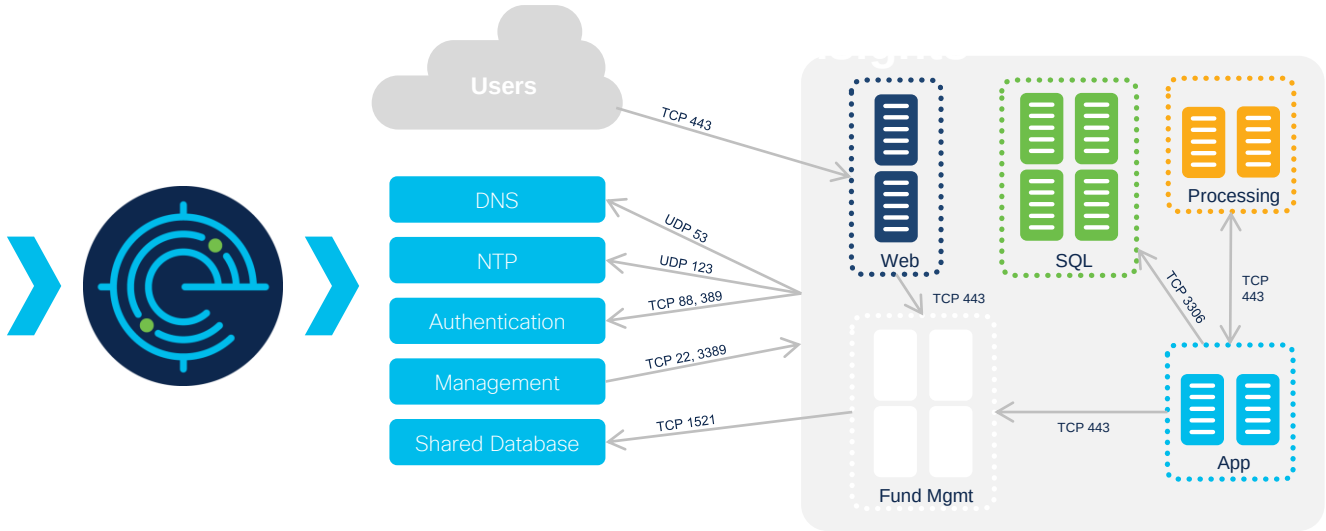
- Network communications
- Process behaviour
- Labels



# Automated Application Policy Discovery

Baseline workload protection posture

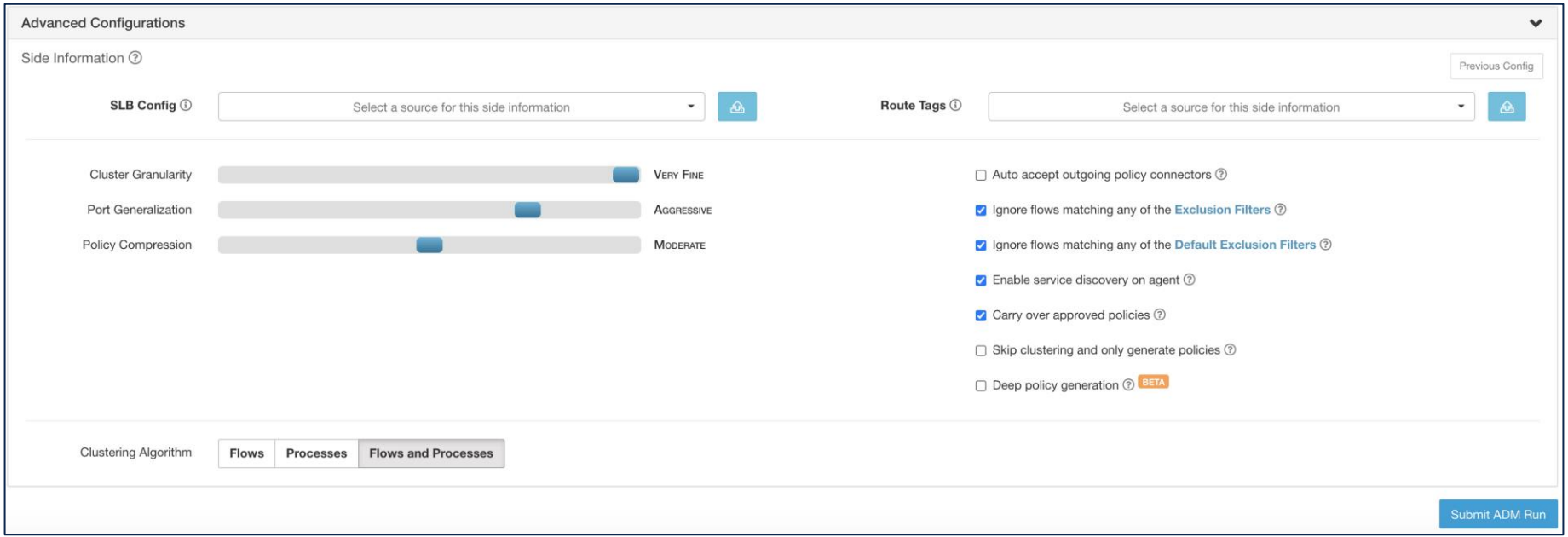
- Network communications
- Process behaviour
- Labels



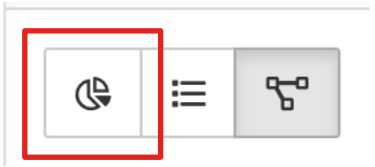
# Application Policy Discovery Review


- “Absolute” Policies take precedent and are evaluated first
- “Default” policies represent the policies Secure Workload has discovered and recommended.
- Catch All Policy is applied when neither an absolute or default policy applies.

# Tuning ADM



# Auto-generated Policies
## Initial Relational Graph



Cisco Secure Workload

opencart PRIMARY

pod_102 : opencart Version: v1 Last Run: 9:28 AM

Switch Application

Start ADM Run

Activity Log | Matching Inventories 4 | Conversations 69 | Filters 3 | Policies 9 | Provided Services | Enforcement Status | Policy Analysis | Enforcement

Quick Analysis | Filter chart...

database

load_balancer

pod_102

Scope: opencart

Full Name: pod_102:opencart

Primary App: opencart

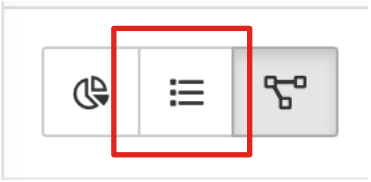
Query: * Application-Name *contains* opencart

View Scope Details

Workloads 4

IP Addresses 0

# Auto-generated policies
## Policy list view



Cisco Secure Workload

opencart PRIMARY

pod_102 : opencart | Version: v1 | Last Run: 9:28 AM

Switch Application | Start ADM Run

Activity Log | Matching Inventories 4 | Conversations 69 | Filters 3 | Policies 9 | Provided Services | Enforcement Status | Policy Analysis | Enforcement

Quick Analysis | Filter Policies ...

Absolute policies 0 | Default policies 8 | Catch All DENY | + Add Default Policy

| Priority | Action | Consumer | Provider | Protocols And Ports |
|---|---|---|---|---|
| 100 | ALLOW | pod_102 : opencart | pod_102 | UDP : 53 (DNS) ...4 more |
| 100 | ALLOW | webserver* | database | TCP : 3306 (MySQL) |
| 100 | ALLOW | load_balancer | webserver* | TCP : 80 (HTTP) |
| 100 | ALLOW | pod_102 | load_balancer | TCP : 80 (HTTP) |

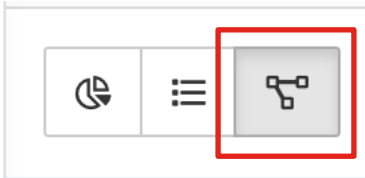
Download table data as JSON | Download table data as CSV

Scope: opencart
Full Name: pod_102:opencart
Primary App: opencart
Query: * Application-Name *contains* opencart

View Scope Details

Workloads 4
IP Addresses 0

# Auto-generated policies
## Canvas App view



Cisco Secure Workload

opencart PRIMARY

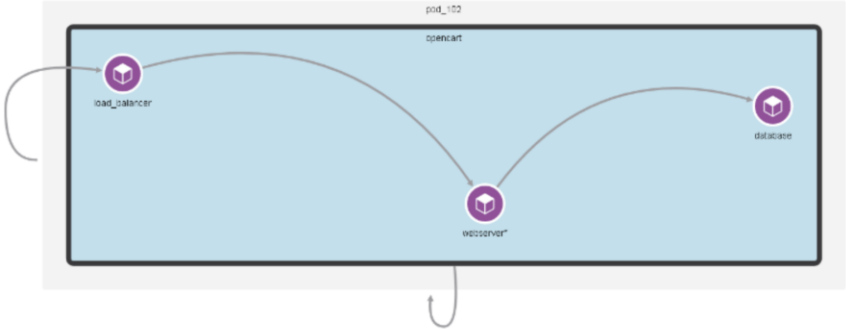
pod_102 : opencart  Version: v1  Last Run: 9:28 AM

Switch Application

Start ADM Run

Activity Log | Matching Inventories 4 | Conversations 69 | Filters 3 | Policies 9 | Provided Services | Enforcement Status | Policy Analysis | Enforcement

Quick Analysis | Filter Policies ... | + Policy




Scope: opencart

Full Name: pod_102:opencart

Primary App: opencart

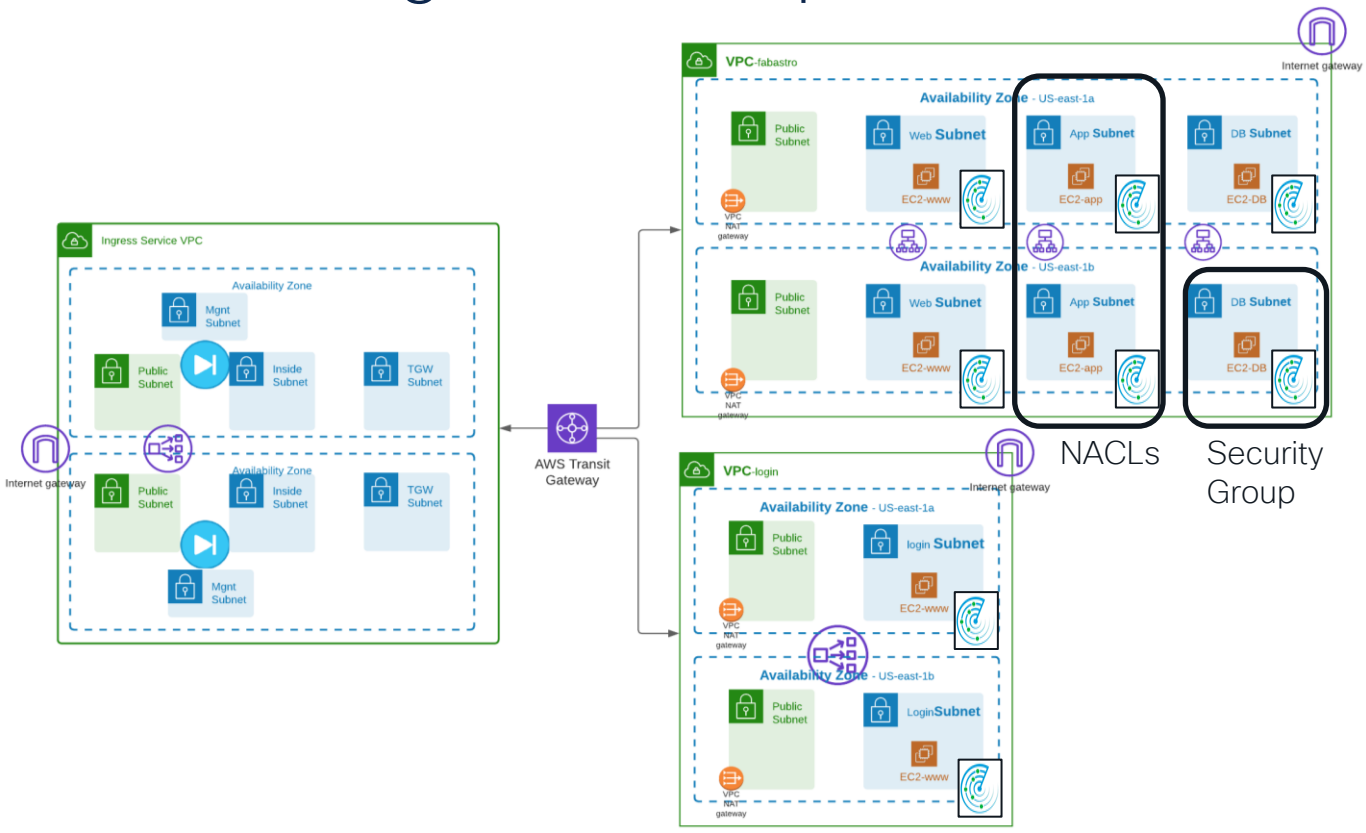
Query: * Application-Name *contains* opencart

View Scope Details

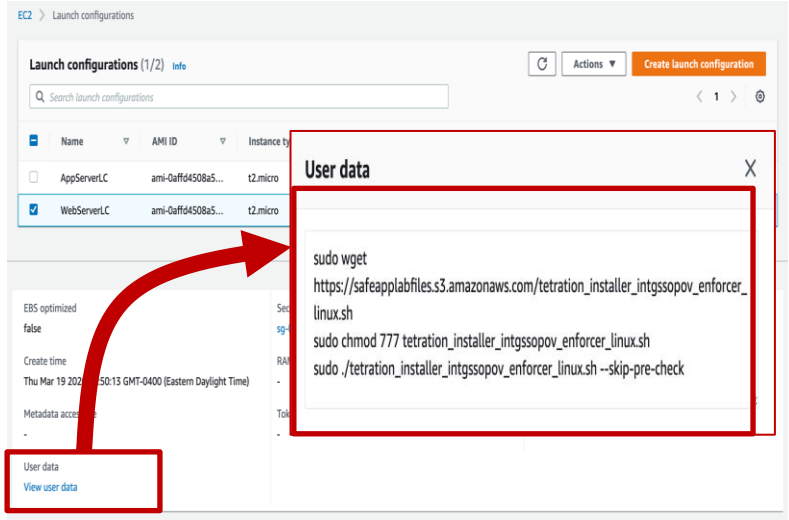
Workloads 4

IP Addresses 0

# Another segmentation point?



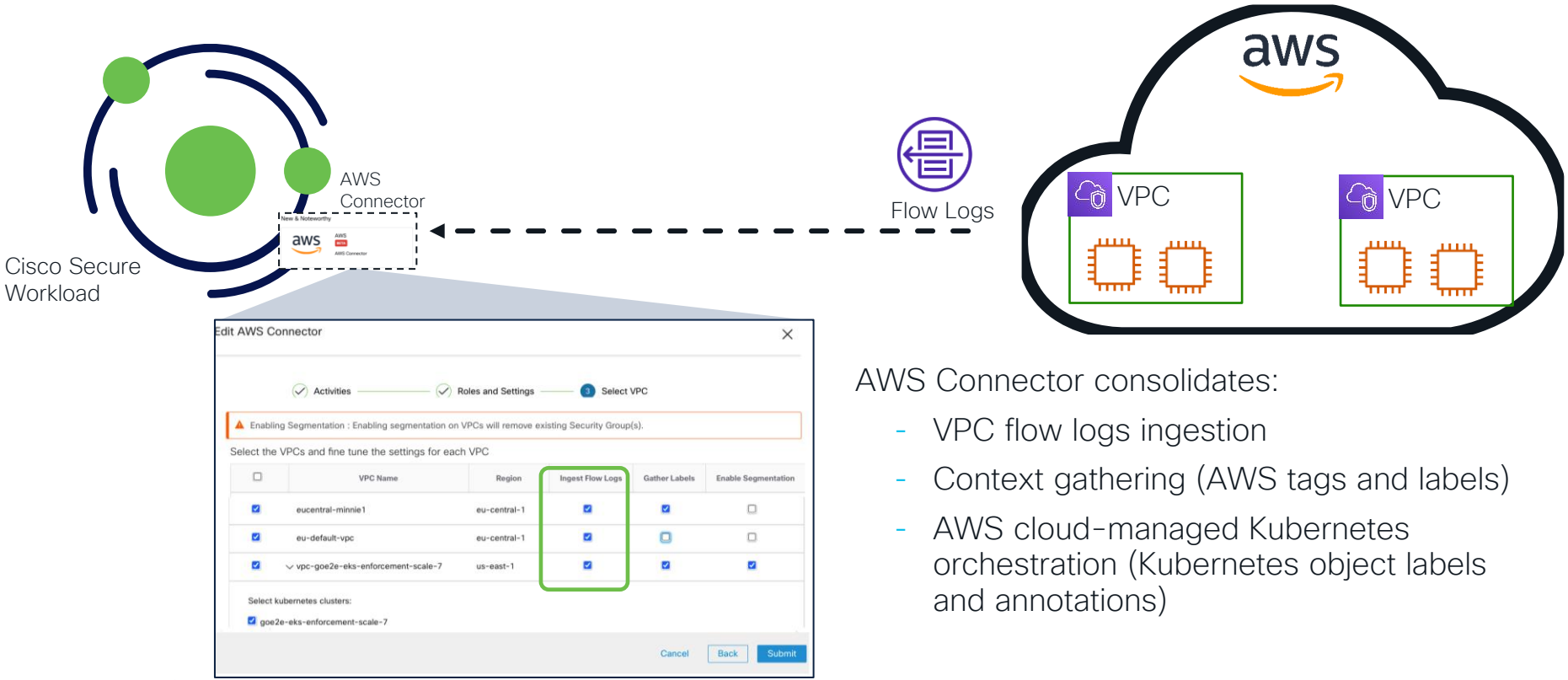
# Deploy Enforcement Agent using AWS Launch Config or CloudFormation




```
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
```

# But Fabien, if in AWS i might not be able to install an agent ???

# 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)

# AWS Connector

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

1

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

2

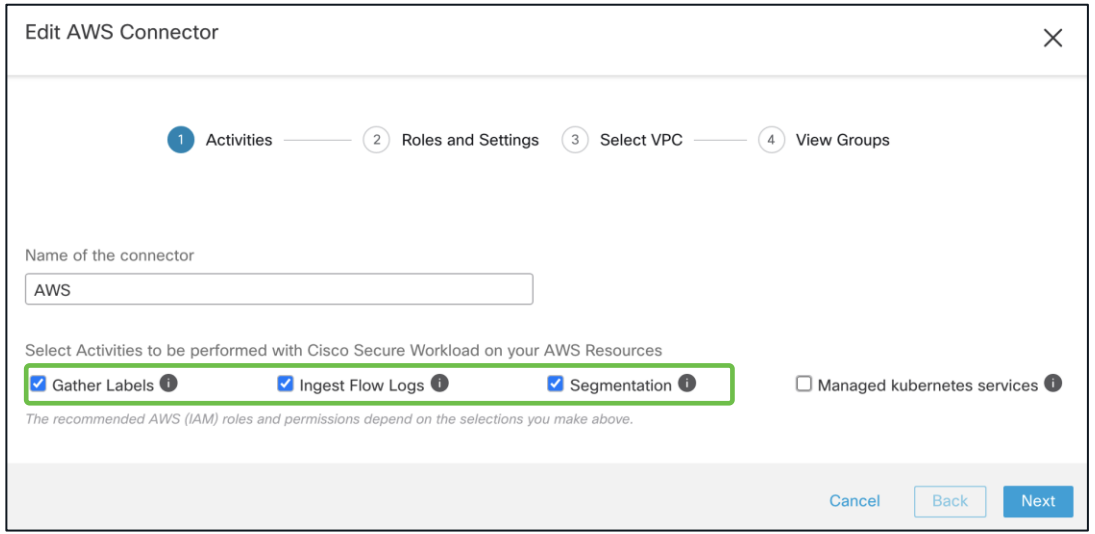
**Download** and **deploy** the **CloudFormation**, add the AWS API **credentials to** Secure Workload.

3

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

# AWS Connector – Select Capabilities

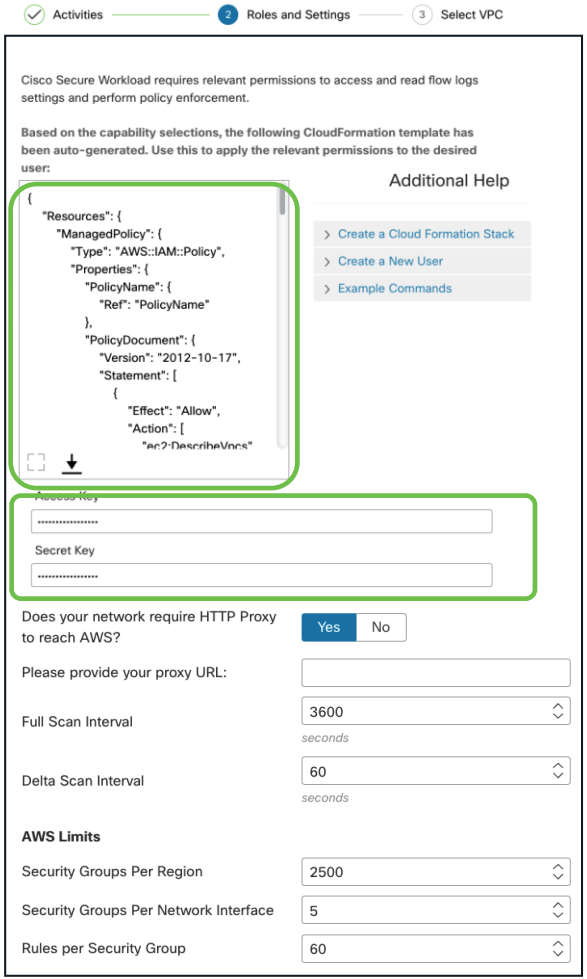
1 Enable and configure the connector capabilities

# 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

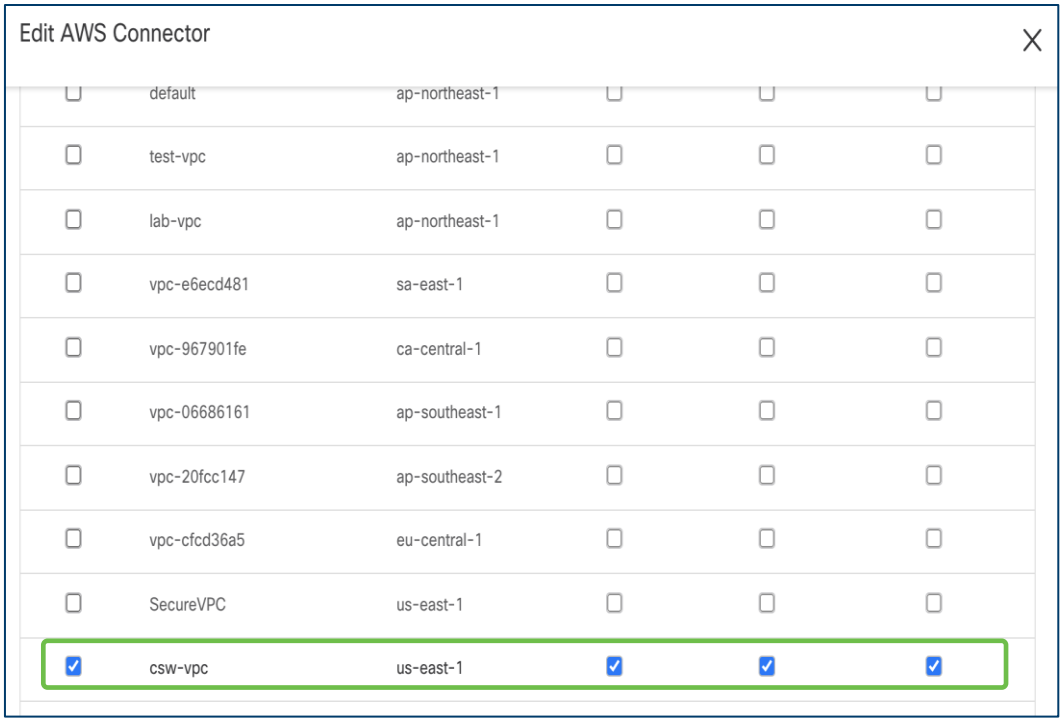
2



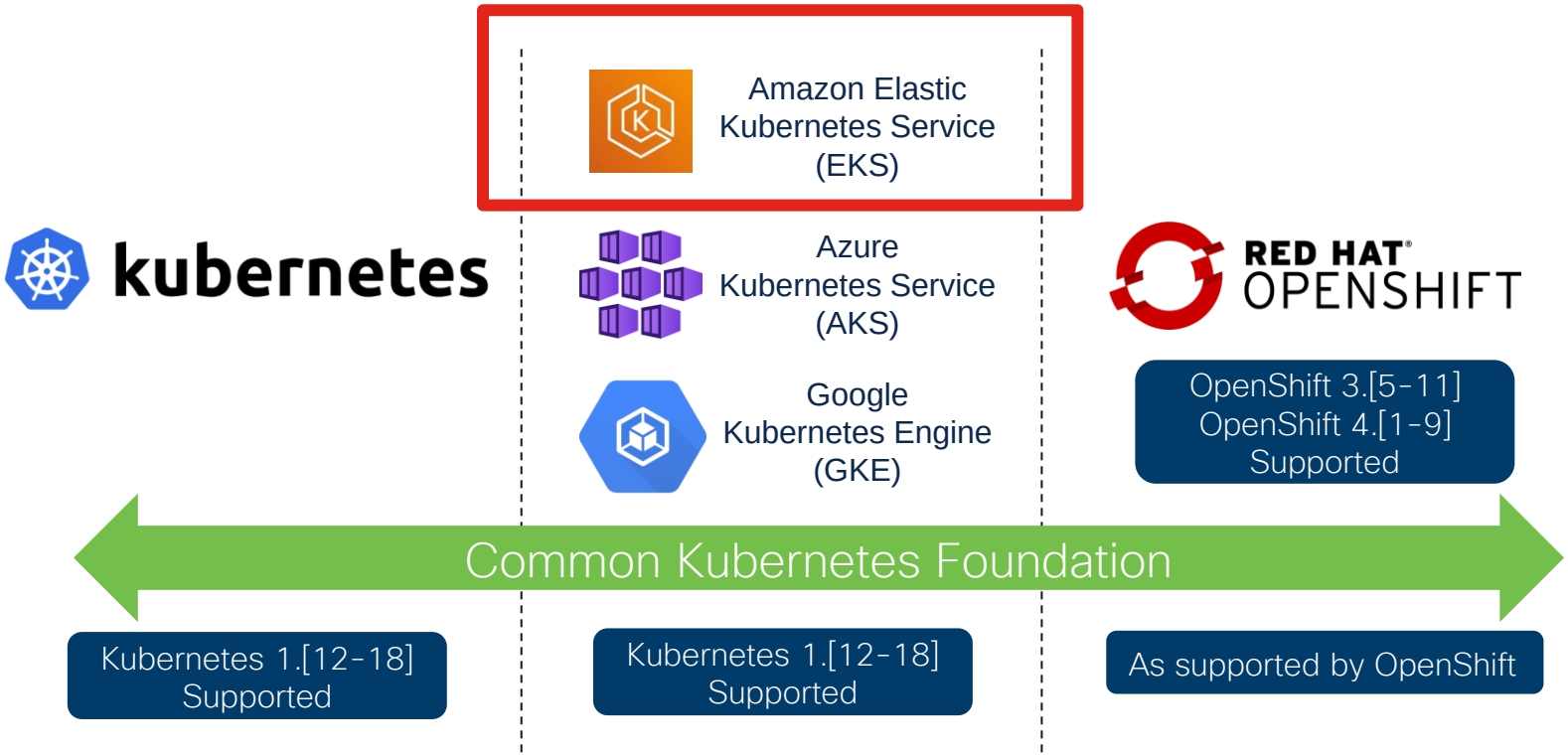
# AWS Connector – Select VPCs

3

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

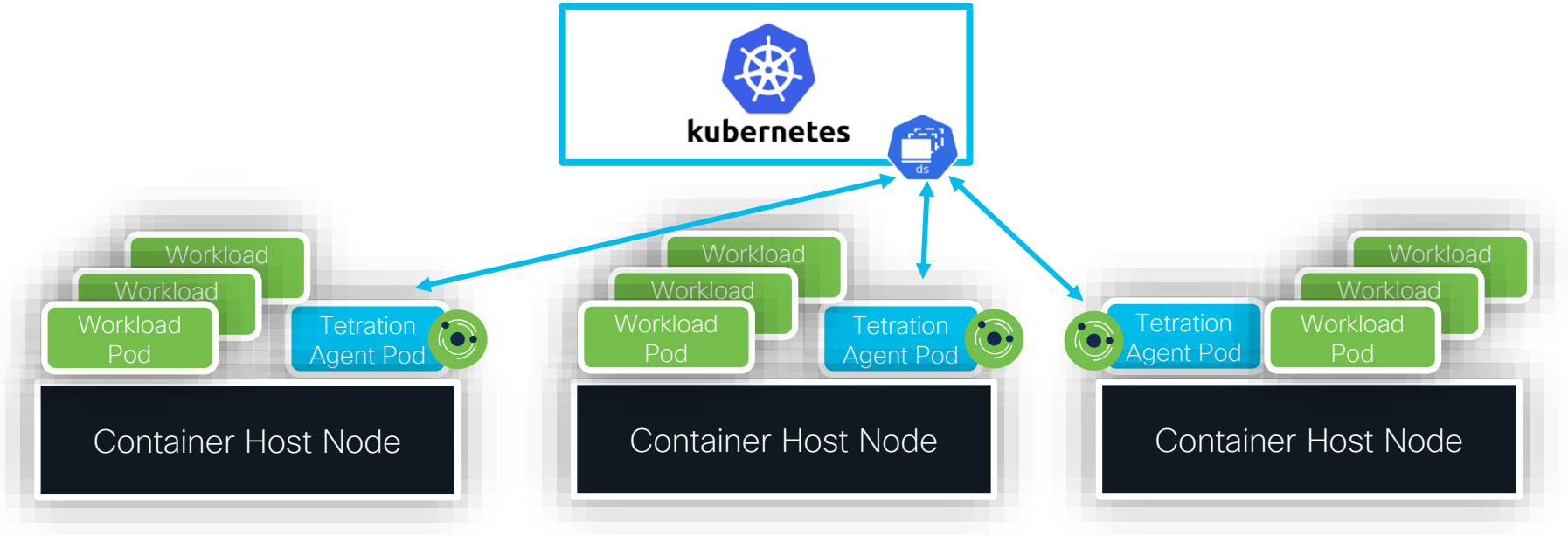


# Kubernetes support



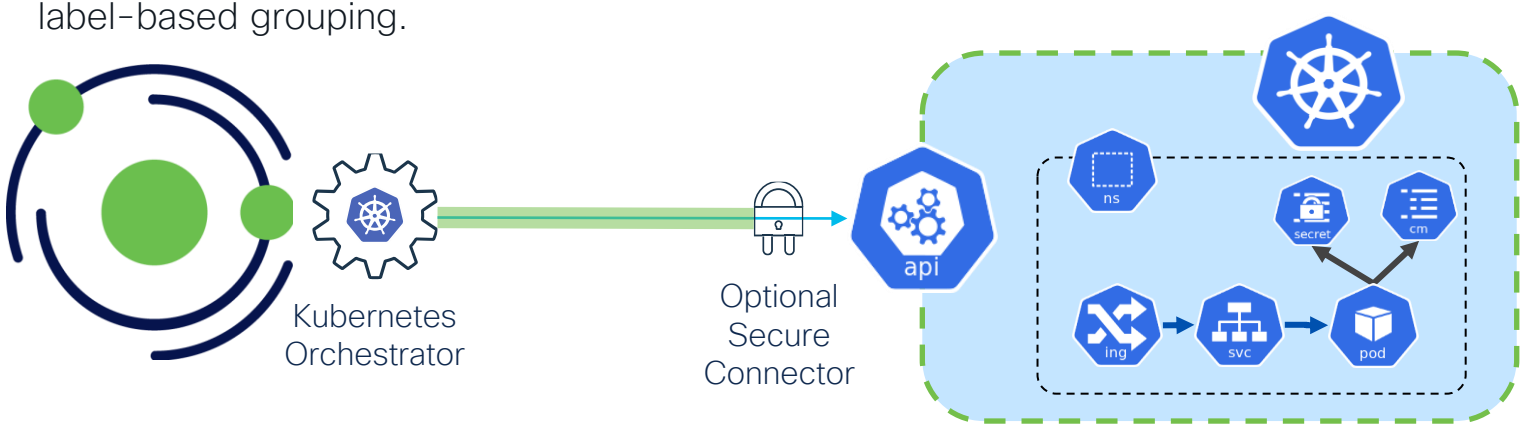
# Cisco Secure Workload Agents as Daemonset

## Daemonset pods run on all schedulable nodes in the container cluster



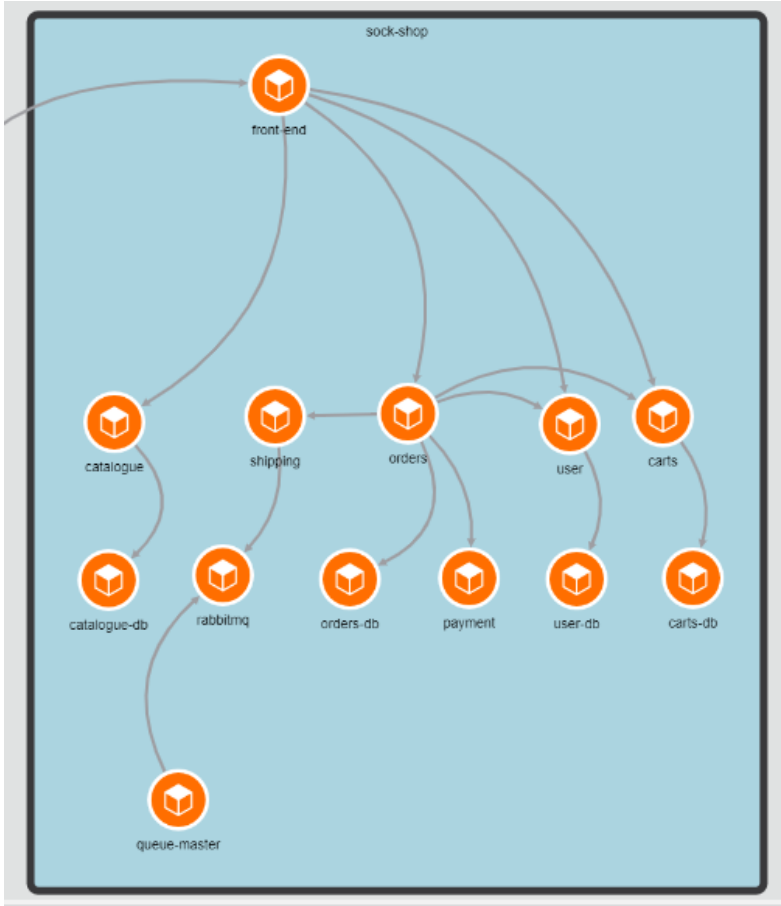
# Kubernetes Metadata Ingest

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

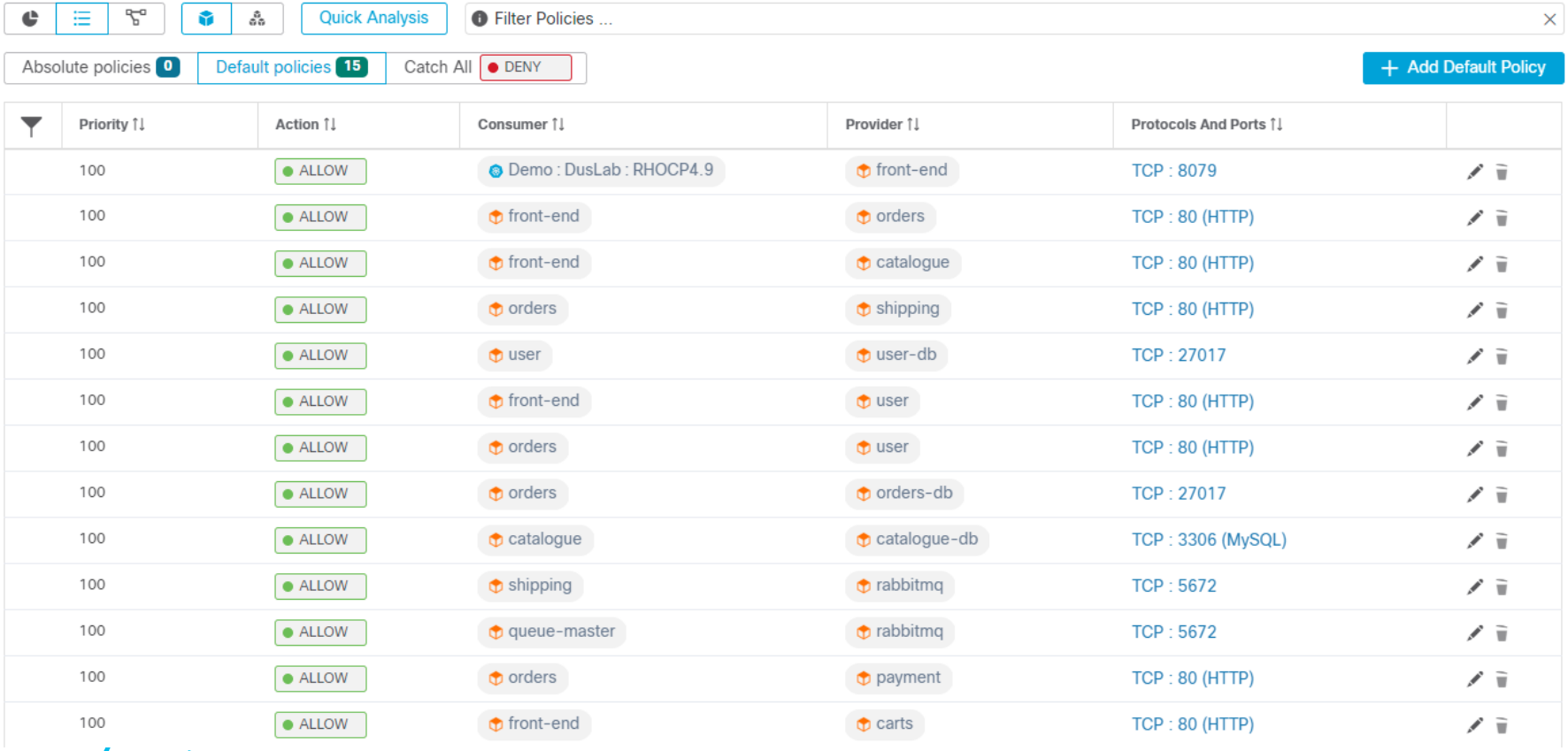



- Kubernetes metadata is ingested through an orchestrator which delivers rich context to the Secure Workload Inventory for dynamic policy enforcement
- Orchestrator connects via Read-Only service account to ingest metadata from all Nodes, Pods and Services to apply as inventory labels.

# Canvas view of my policy

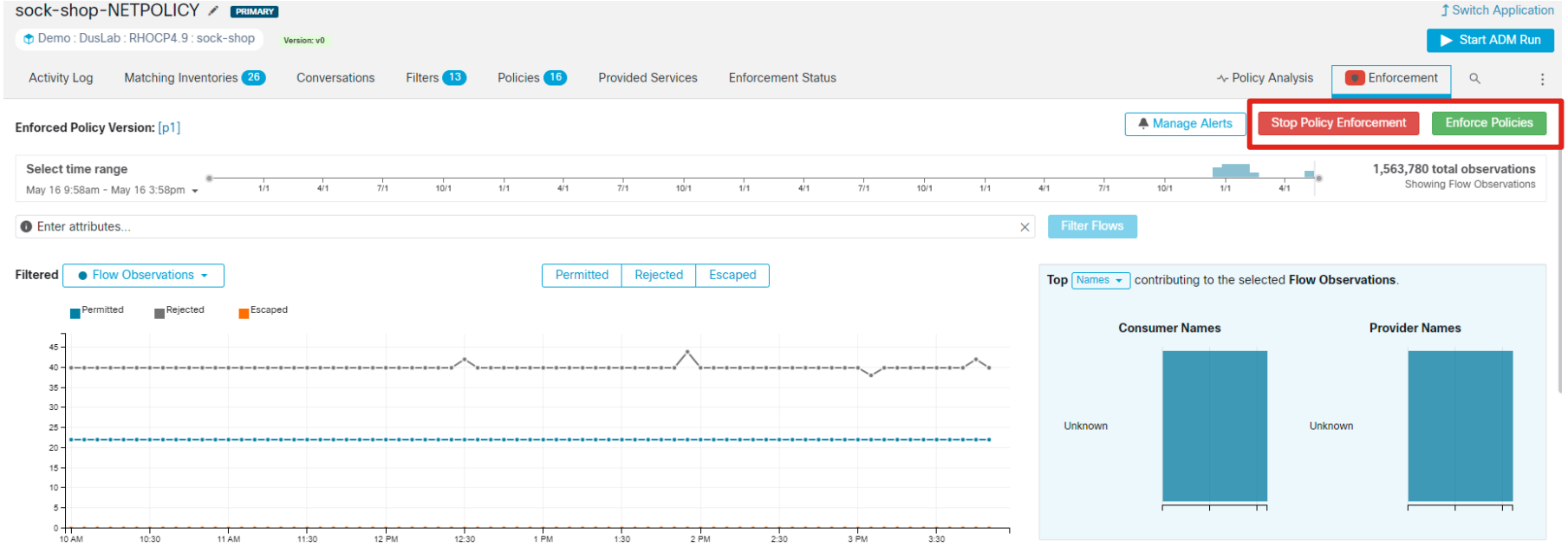


# List view of the policy

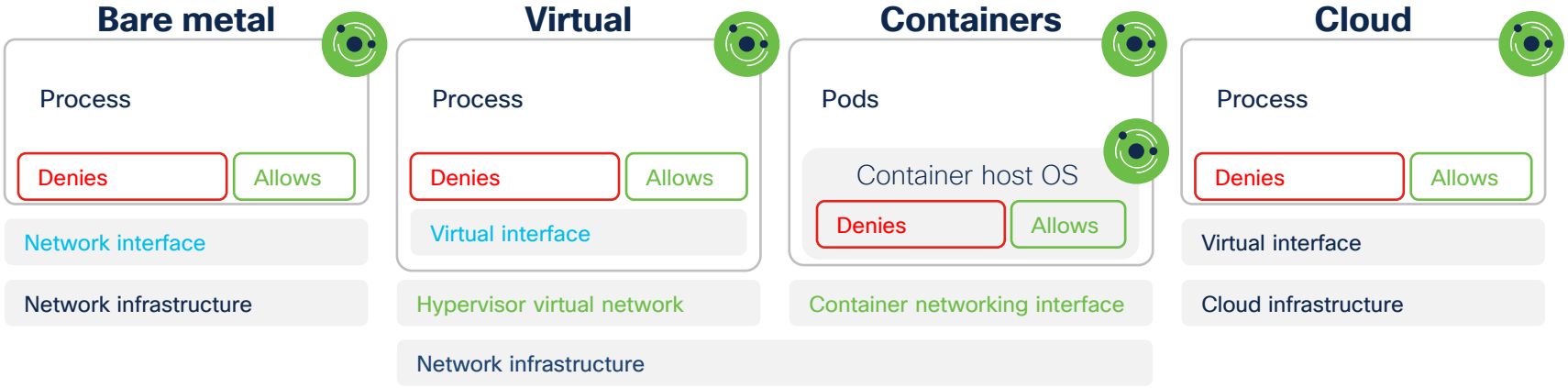



| Priority | Action | Consumer | Provider | Protocols And Ports |
|---|---|---|---|---|
| 100 | ALLOW | Demo : DusLab : RHOCP4.9 | front-end | TCP : 8079 |
| 100 | ALLOW | front-end | orders | TCP : 80 (HTTP) |
| 100 | ALLOW | front-end | catalogue | TCP : 80 (HTTP) |
| 100 | ALLOW | orders | shipping | 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) |

# Enforce your policy in one click



# 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

# How do I insert NGFW ?

# AWS FW

**High availability and automated scaling**

**Stateful firewall**

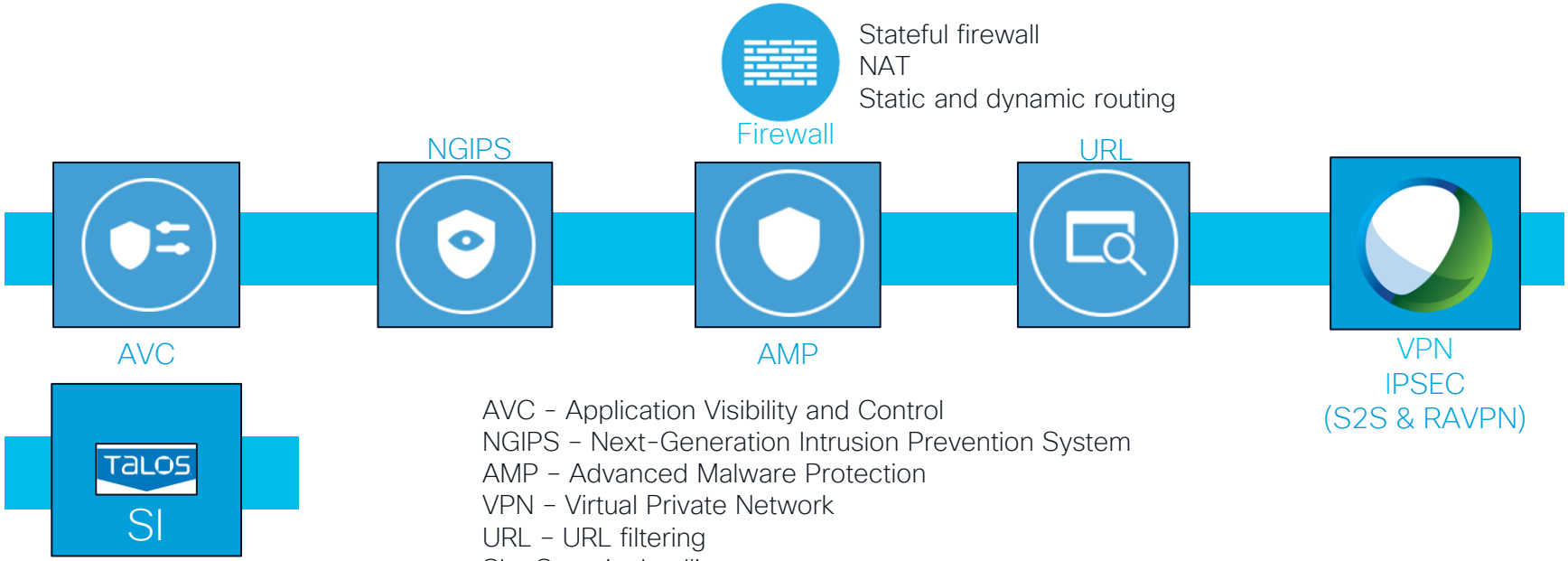
**Web filtering**

**Intrusion prevention**

**Alert and flow logs**

**Central management and visibility**

# 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

# Multi-cloud and Hybrid Cloud Environments

## Private Cloud






## Public Cloud







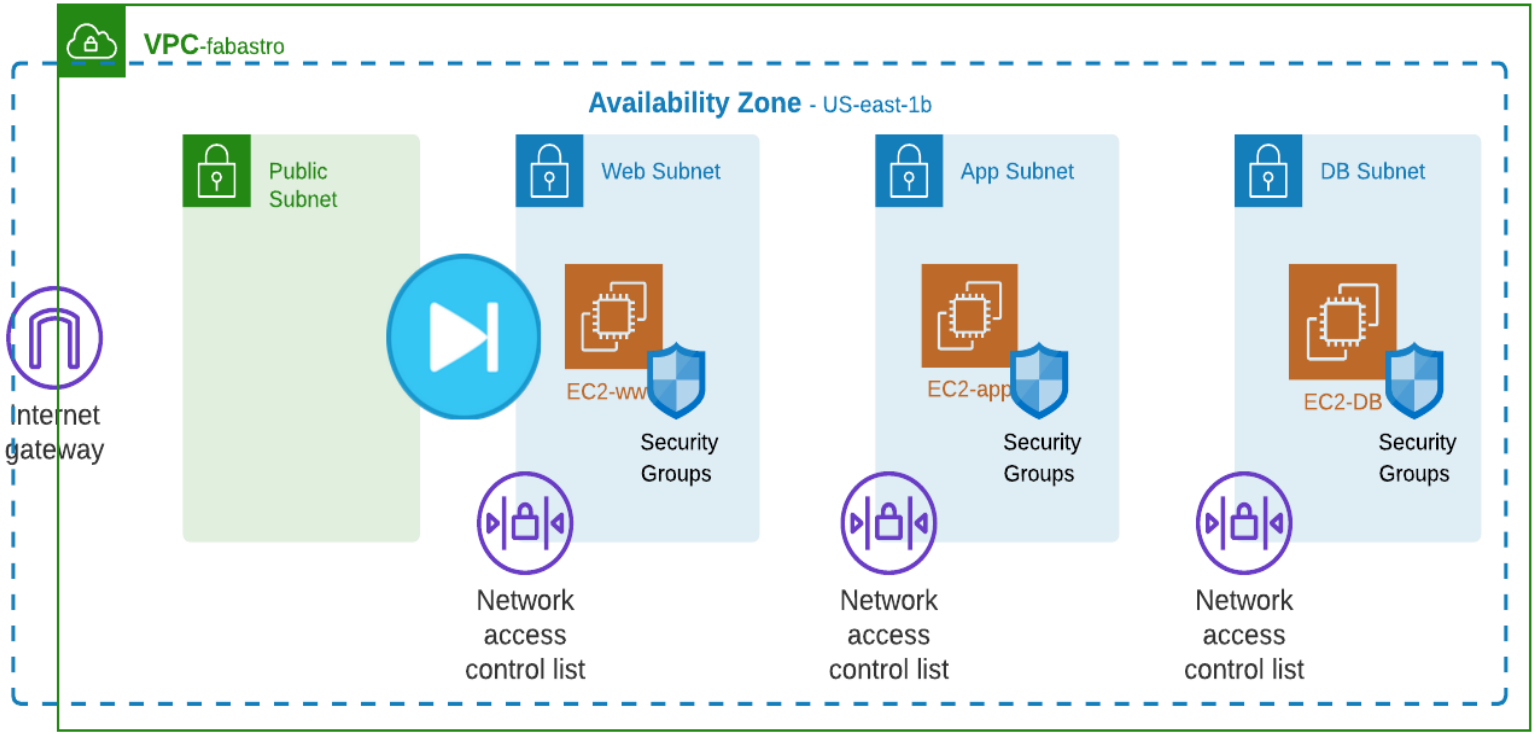


## New Features

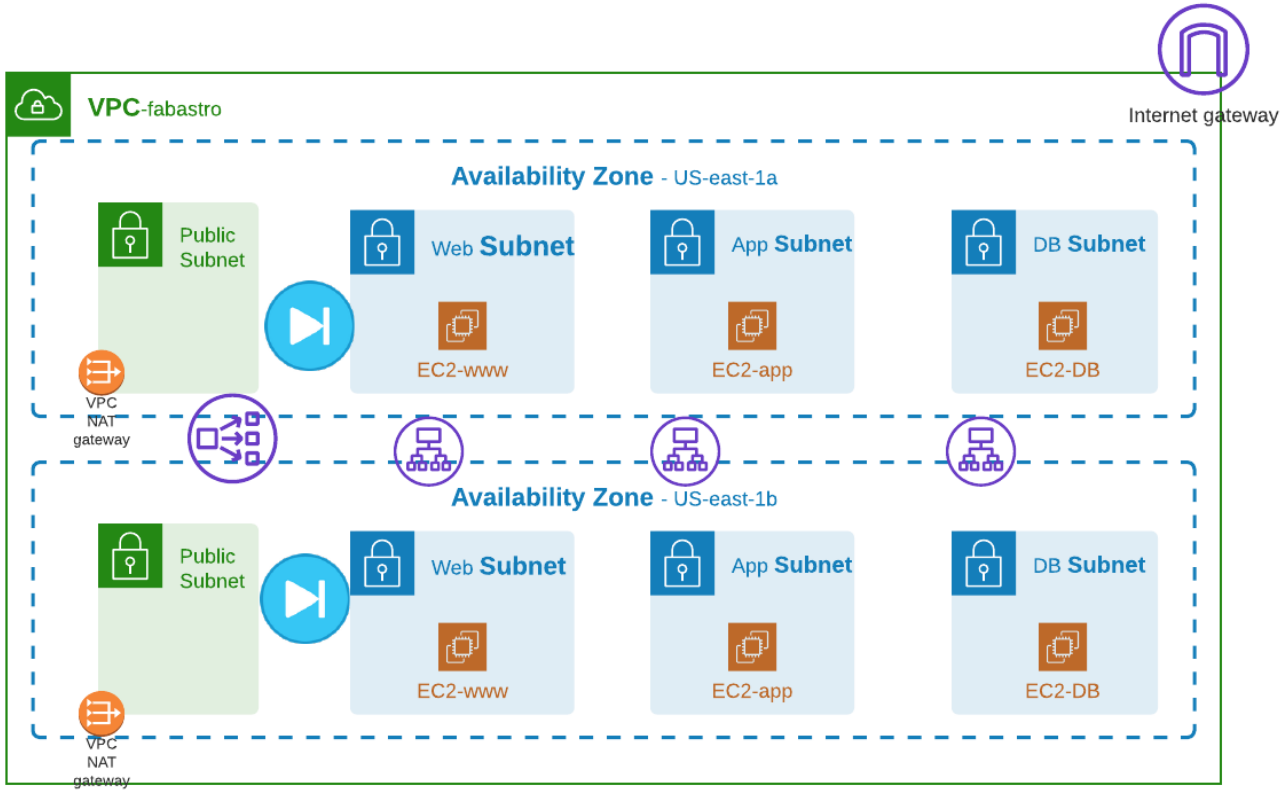
- Clustering
- Dynamic Policy
- Better integration with public cloud infrastructure
- Infrastructure as Code and Automation
- Integration with GuardDuty
- Gateway Load balancer integration
- Auto Scaling
- Snapshot support

# Basic FTD insertion

# Firewall in front of the “Application” VPC



# FTD insertion with HA

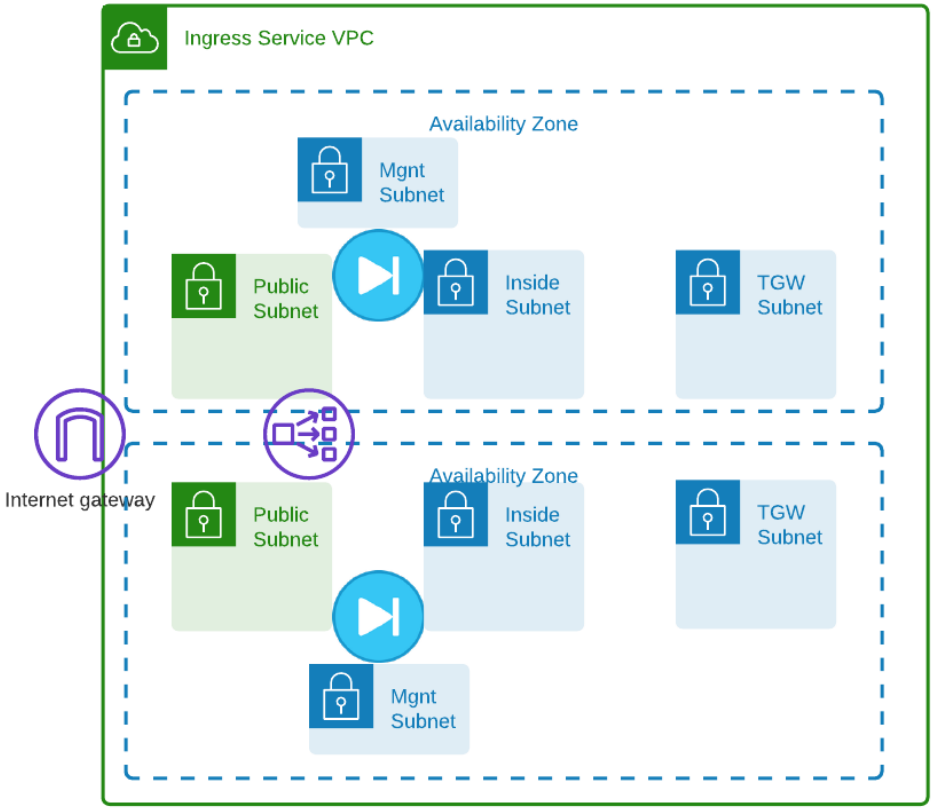


# Limits of this design

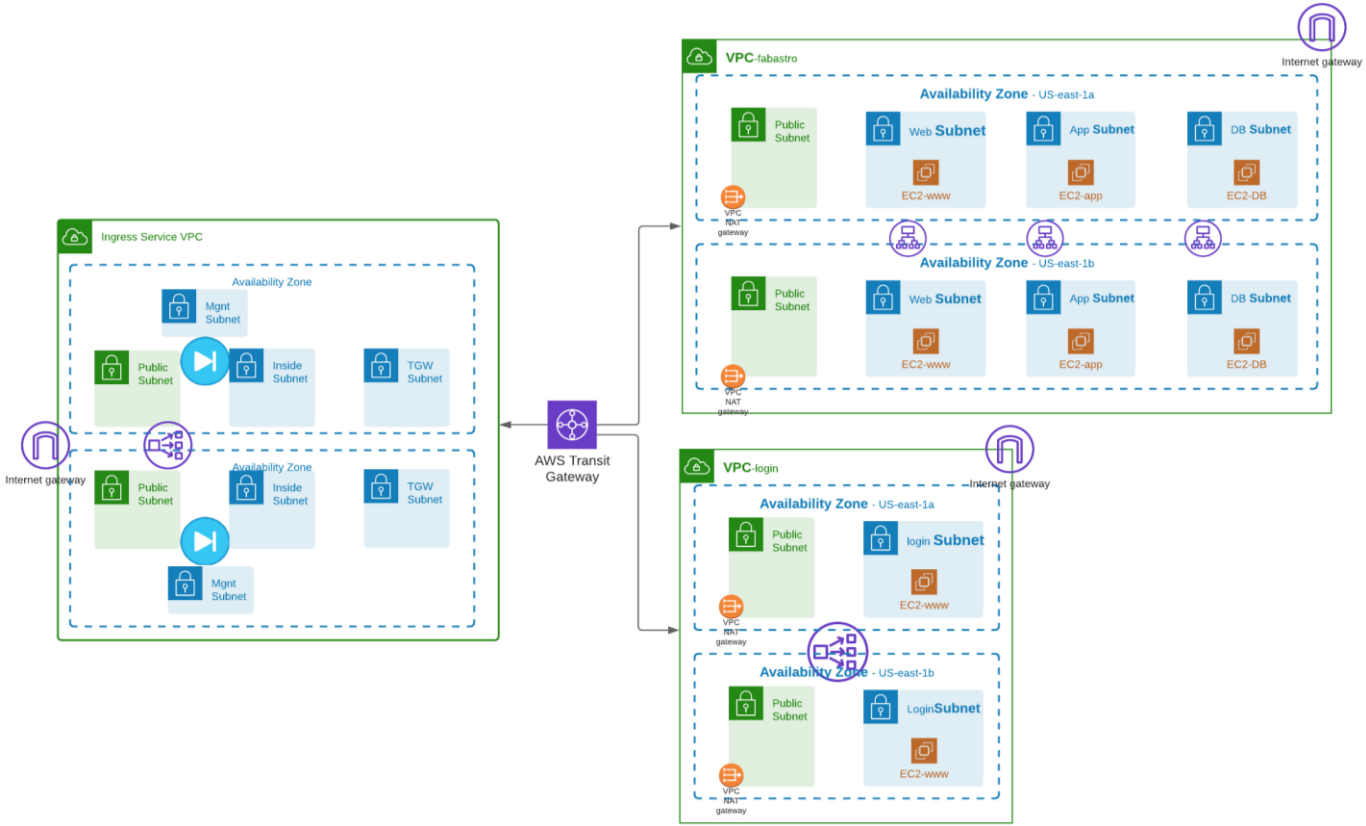

New Firewall pair for each applications


Double inspection for inter-VPC

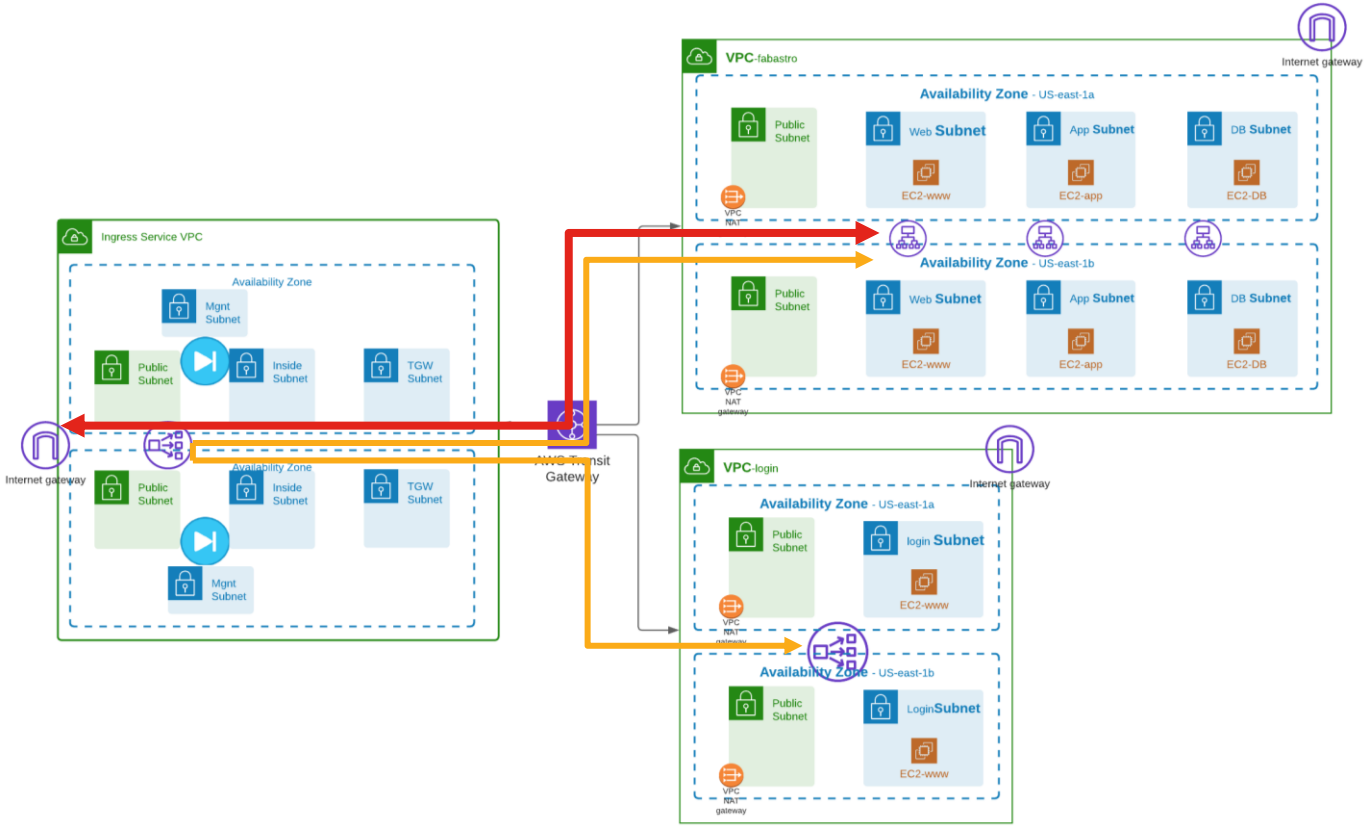
# Ingress Service VPC



# Service VPC with FTD



# North/South and East/West Service VPC



# FTD AWS Insertion Configuration

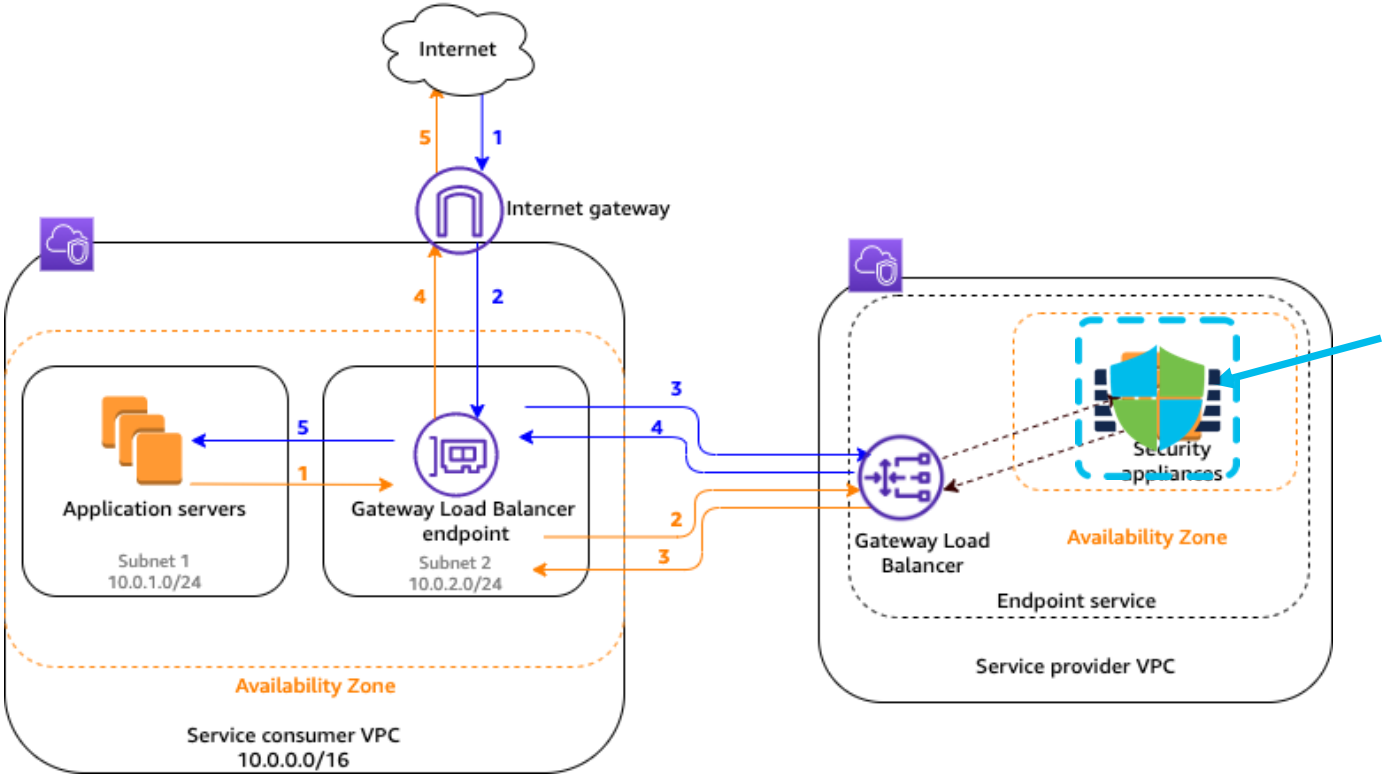
- Create Ingress VPC
- Create Subnets (Outside, Inside, Management, TransitGateway)
- Create Interfaces (Outside, Inside, Management, Diagnostic)
- Create Security group policies for FTD interfaces
- Create FTD instances with 4 interfaces
- Create Network load-balancer

# 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

# Leveraging GWLB

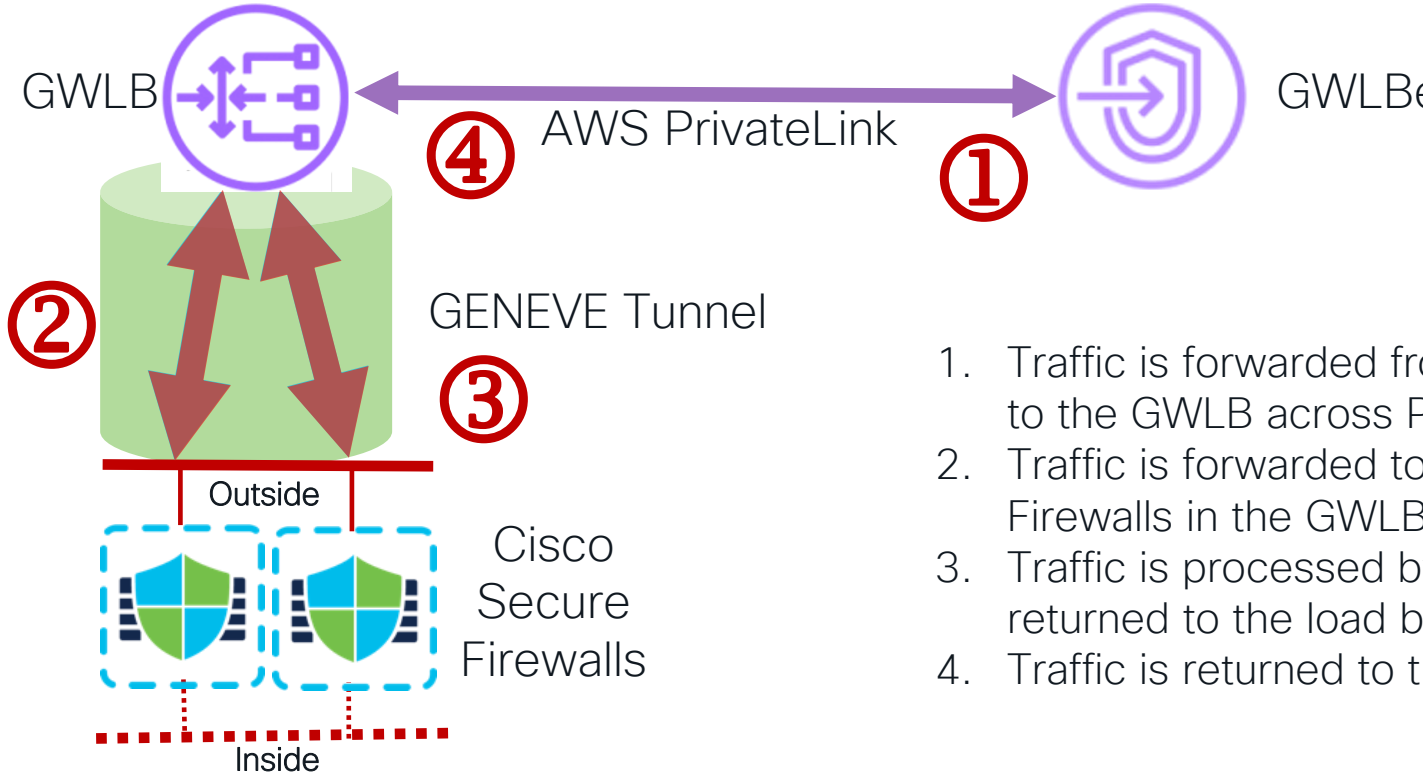
# AWS Gateway Load Balancer




ASAvs or FTDvs

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

# Traffic Flow Between the GWLBe, GWLB, and Firewalls




1. Traffic is forwarded from the GWLBe to the GWLB across PrivateLink
2. Traffic is forwarded to one of the Firewalls in the GWLB Target Group
3. Traffic is processed by the firewall and returned to the load balancer
4. Traffic is returned to the GWLBe

# Gateway Load Balancer Endpoint (GWLBe)



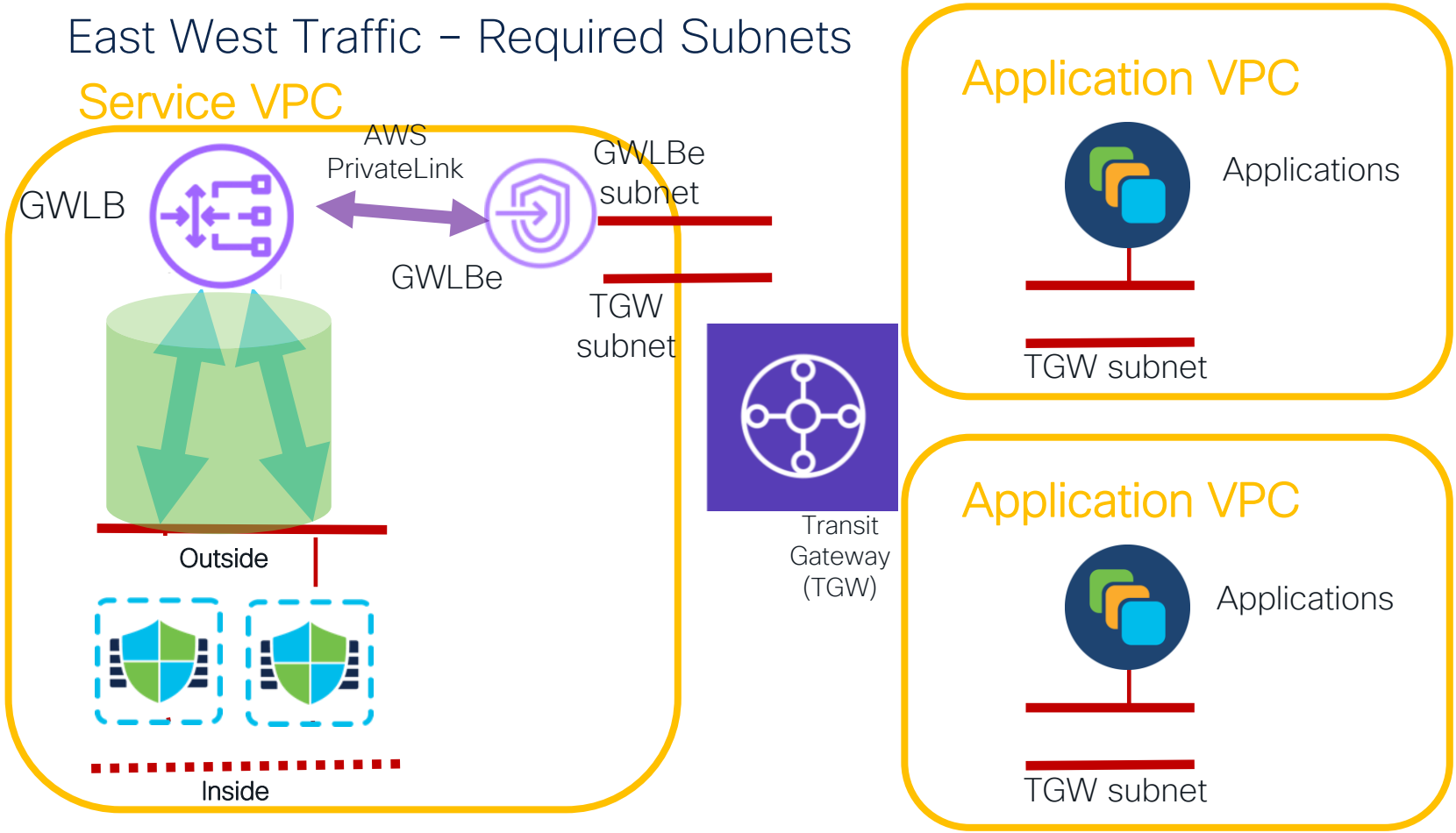
- Gateway Load Balancer Endpoint is a next hop type in a VPC route table
- Intercepts traffic transparently
- Forwards traffic transparently to the Gateway Load Balancer
- Associated with a single subnet
  - Associated with a single Availability Zone
  - AWS delivers packets to this subnet after the GWLBe received the packets from the GLWB
  - Has a private IP address on a subnet that is not referenced in any configuration

# Gateway Load Balancer (GWLB)

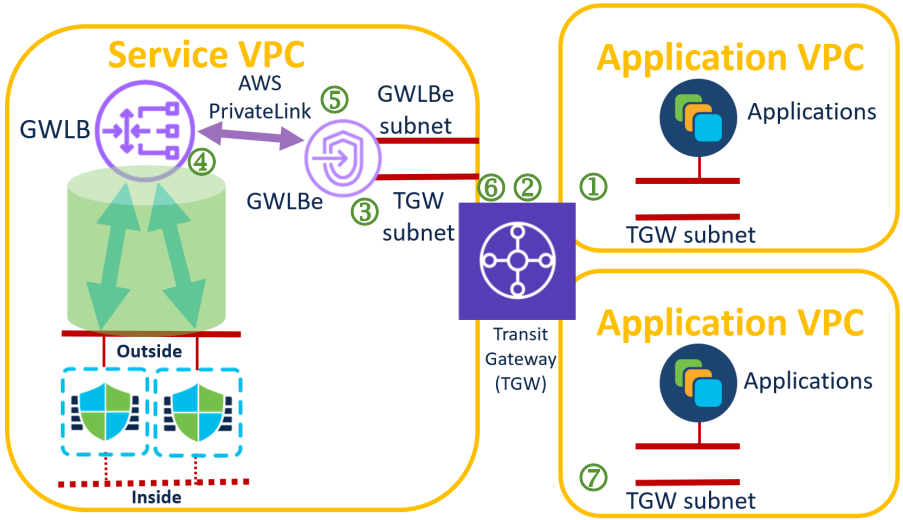


- Forwards traffic to the firewalls inside a GENEVE tunnel
  - Load  balances between firewalls in a *Target Group*
  - Does not modify packets or packet headers
  - Forwards all packets associated with a particular connection to the same firewall
- Associate with one or more subnets
  - Can load balance across multiple Availability Zones

# East West Traffic – Required Subnets

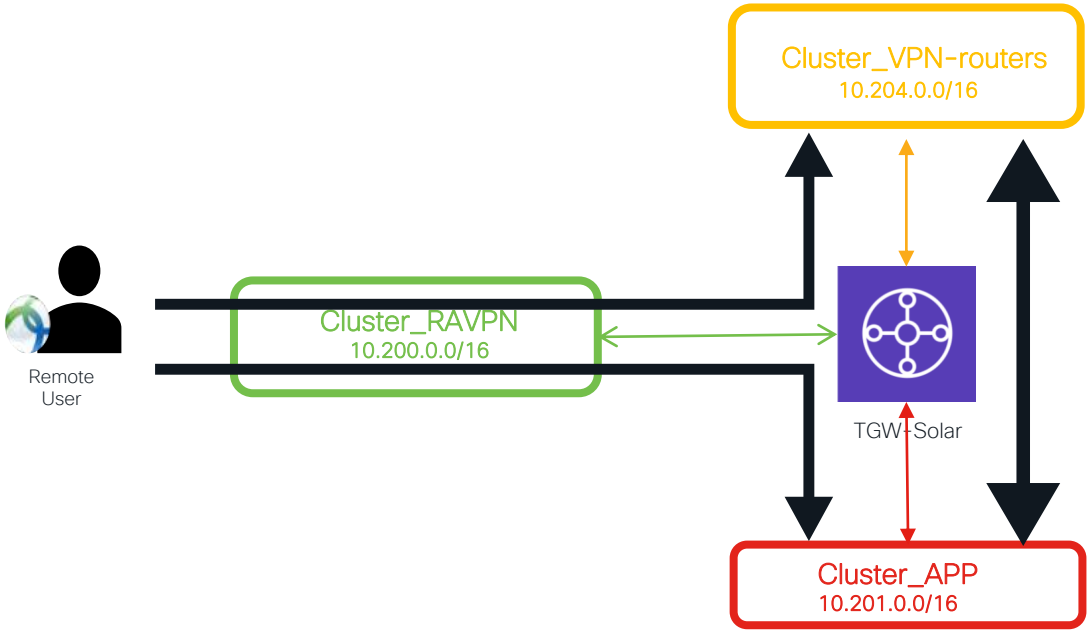


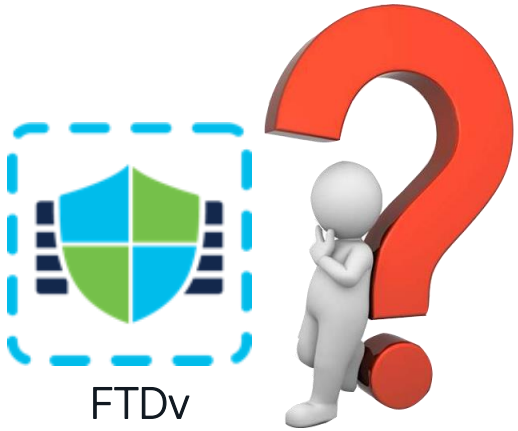
# Routing East-WestTraffic



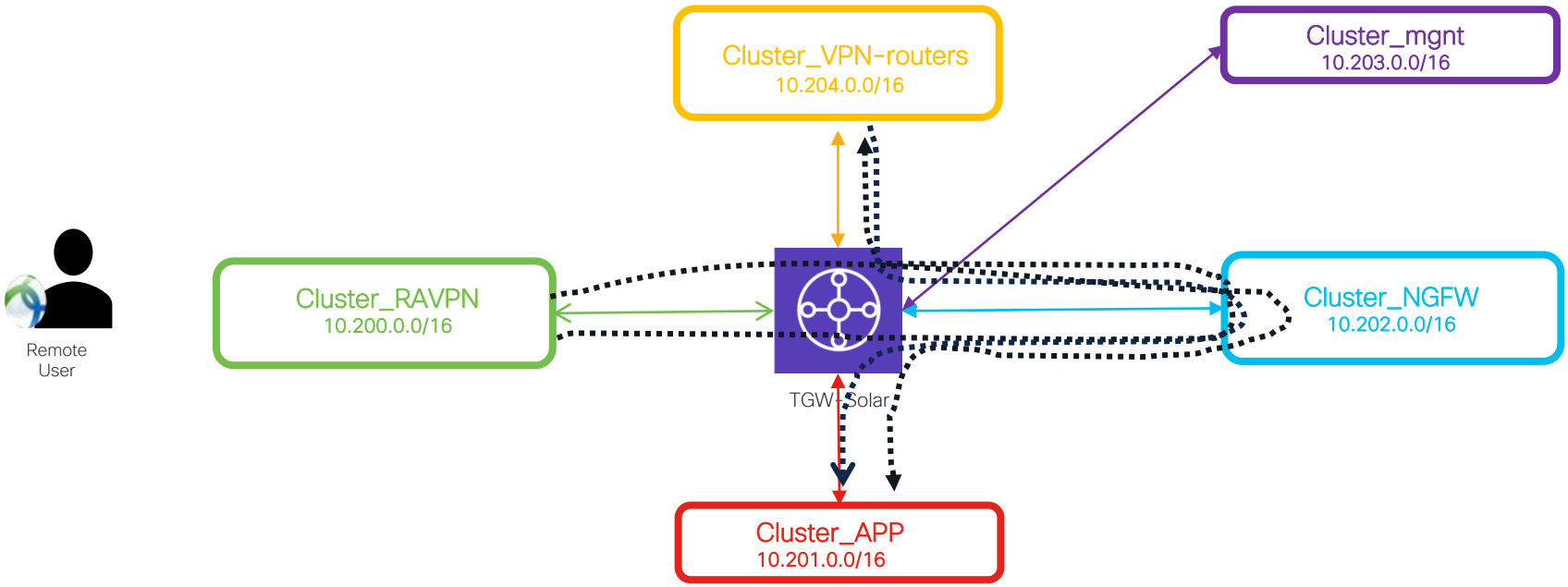

1. Application subnet (in source VPC) next hop is TGW attachment
2. TGW route table (for source VPC attachment) forwards traffic to Service VPC
3. TGW subnet in Service VPC next hop is GWLBe
4. GWLBe forwards traffic to GLWB, traffic is inspected and returned to GWLBe
5. GWLBe subnet next hop is TGW attachment
6. TGW route table (for Service VPC attachment) forwards traffic to destination VPC
7. TGW subnet in destination VPC is local

# Solar High level design

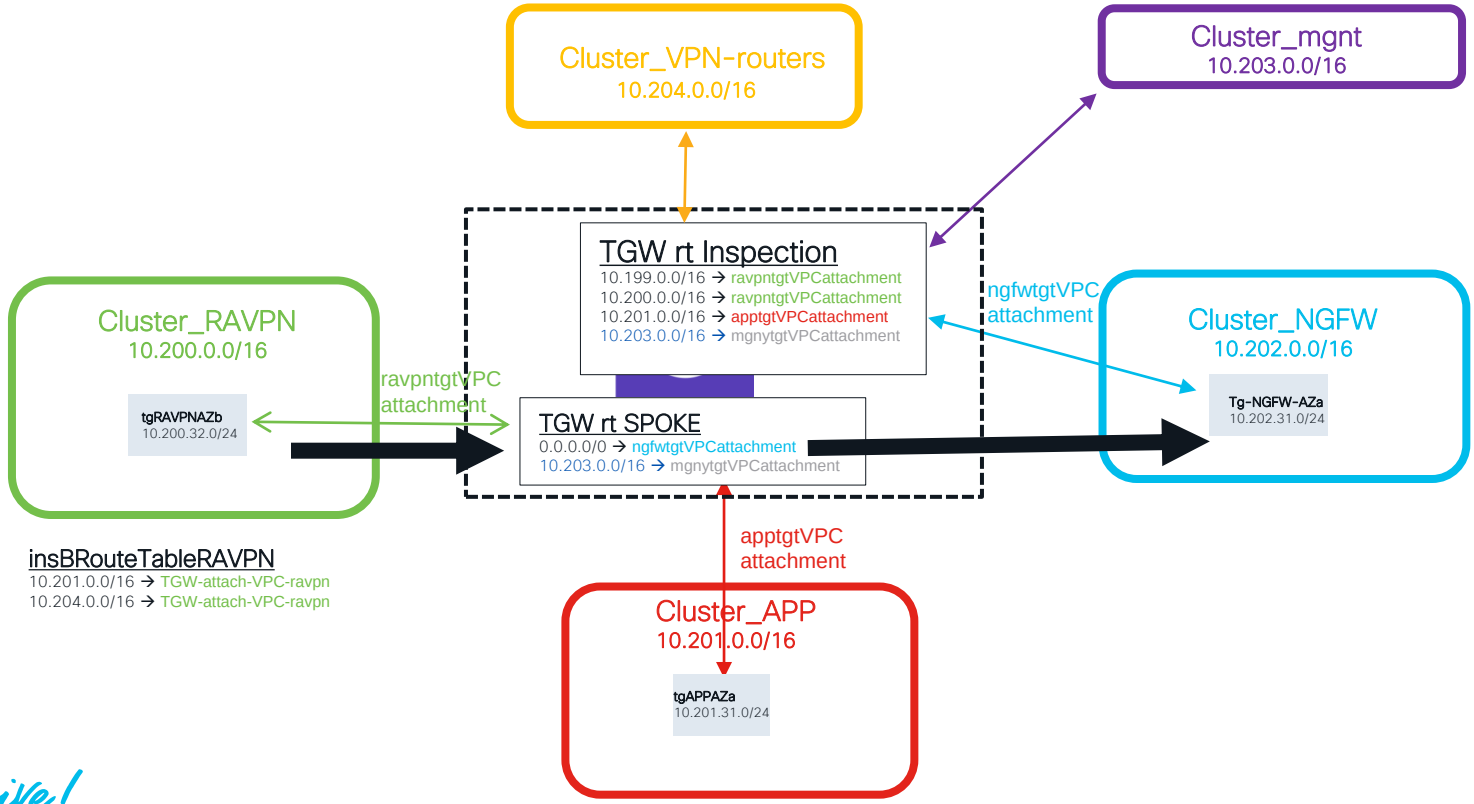


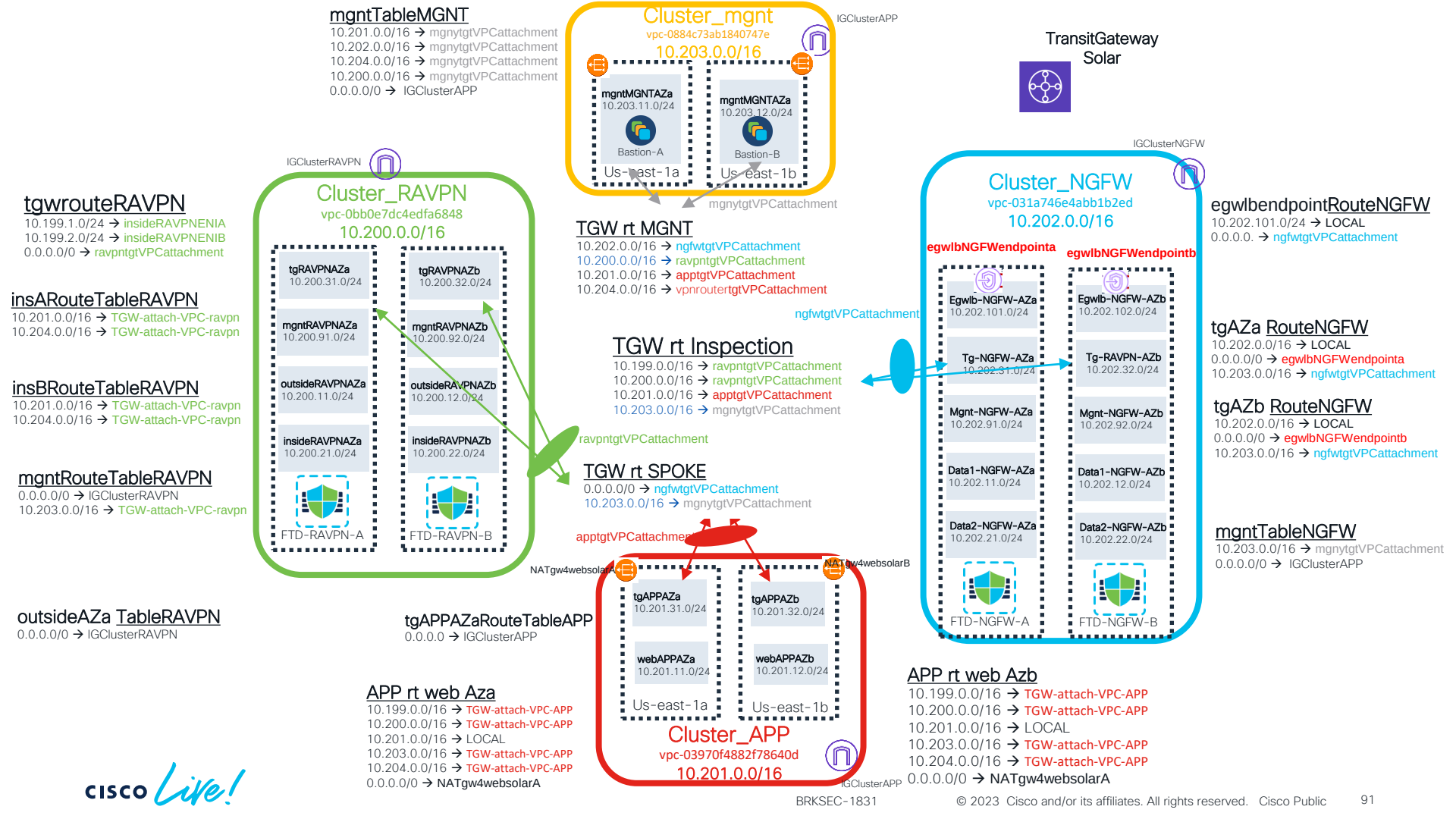



# Solar Security Insertion

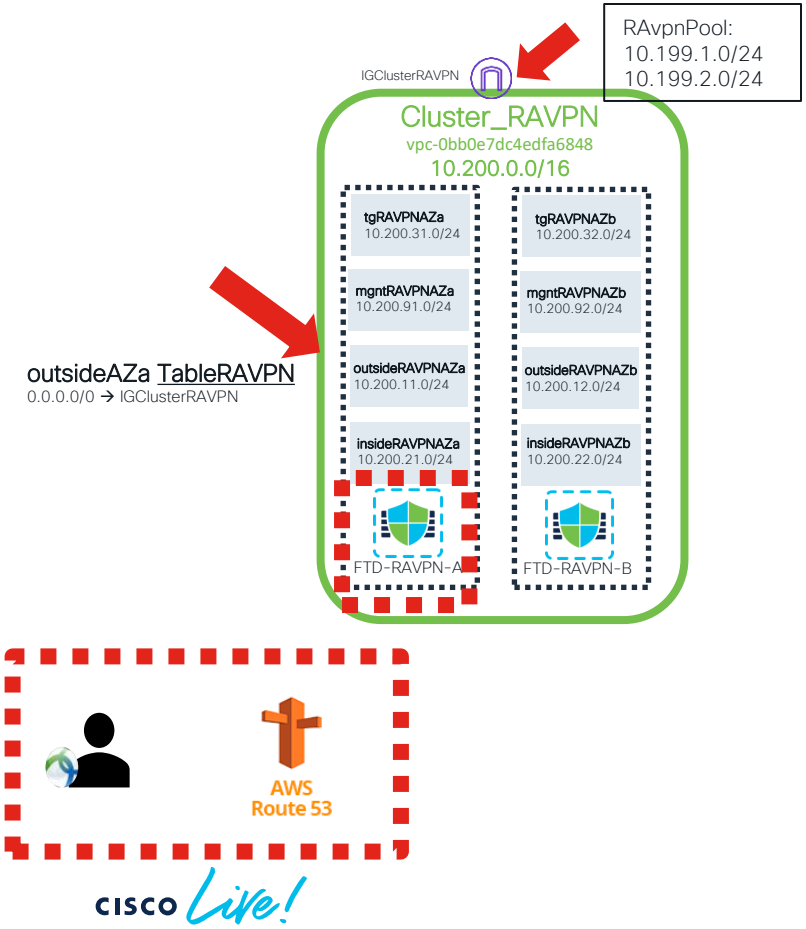


# Fastest TGW Introduction ever…

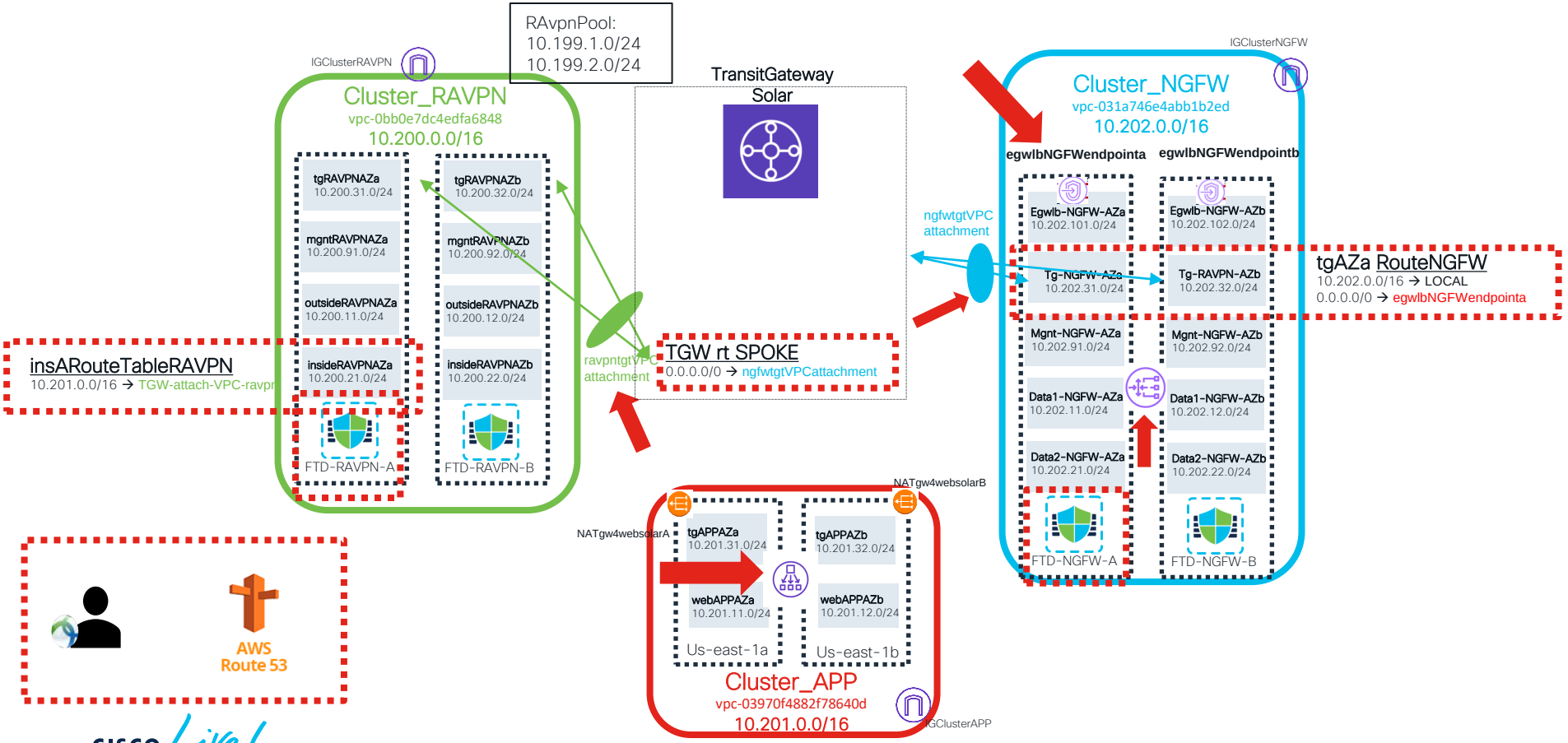




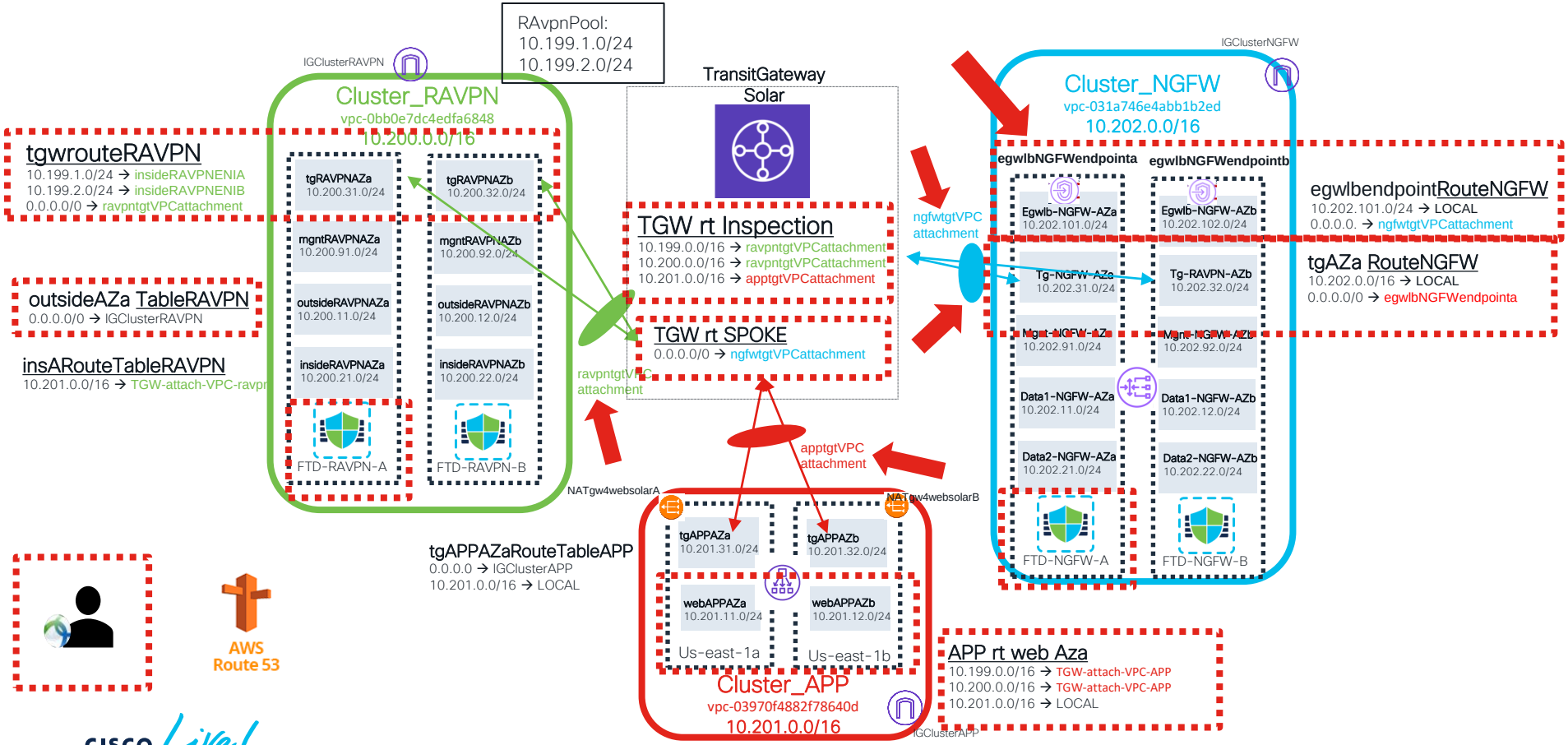
# Establish Tunnel



# Access Fabastro Web page



# Access Fabastro Web page



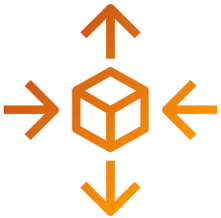
# Handling High Availability and Scallability

cisco Live!

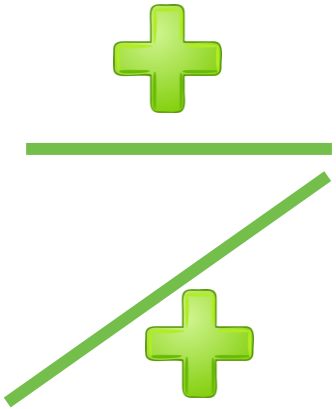
# Working Together



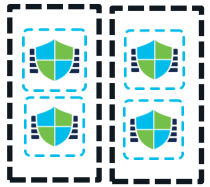
Loadbalancing



Autoscalling



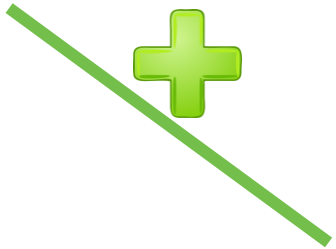
Several independant FTDv



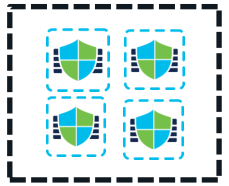
# Working Together



Loadbalancing

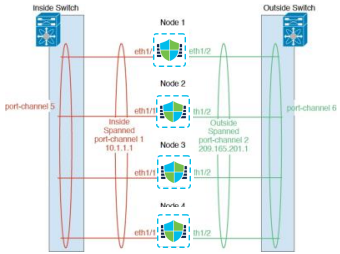


Several independant FTDv



Autoscalling

FTDv Clustering

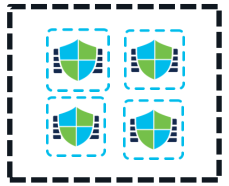


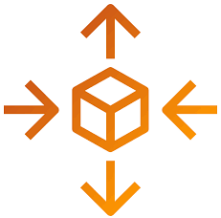
# No AutoScalling with Clustering YET



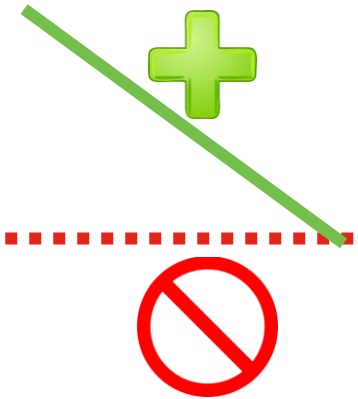
Loadbalancing

Several independant FTDv

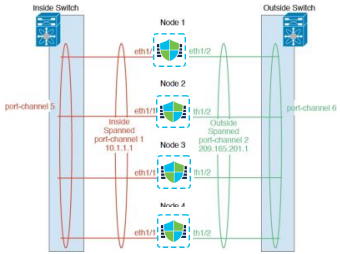




Autoscalling



FTDv Clustering

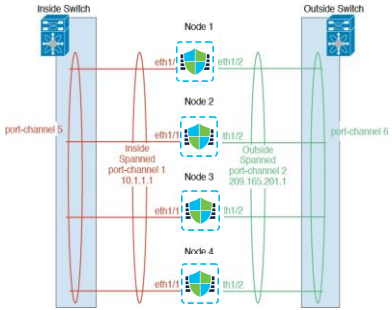


# AutoScaling or Clustering ?

TODAY

Autoscalling

SOMEDAY

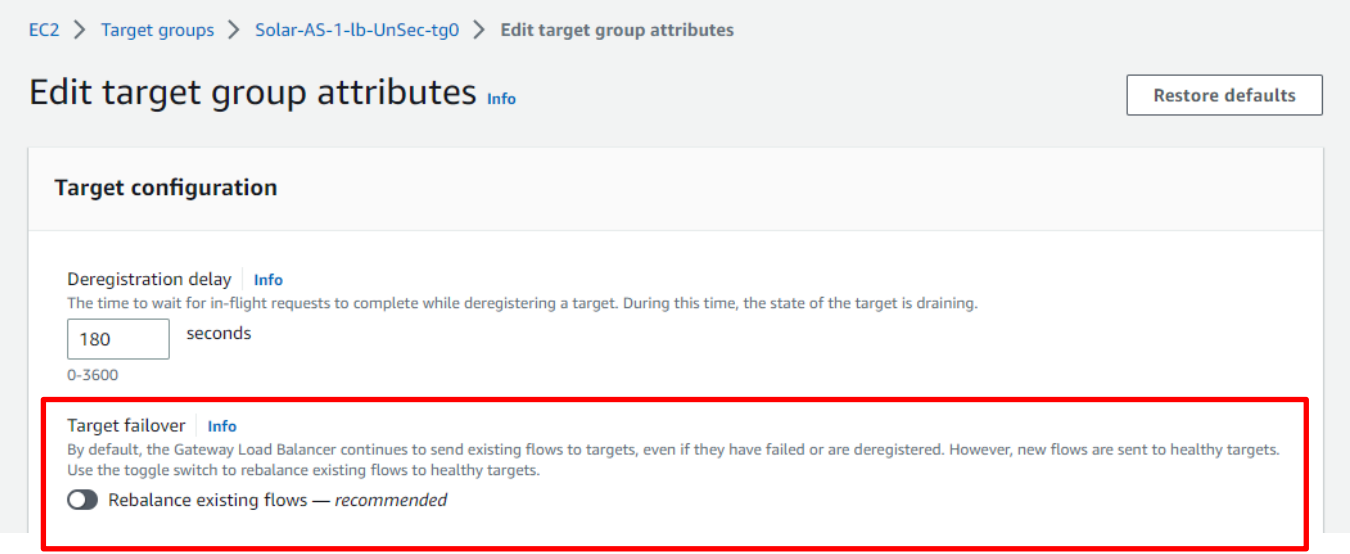



FTDv
Clustering

# But WHY ????

- AutoScaling more relevant ?
- Usefull Stateful HA ?
- Only Single Availability Zone

# GWLB did not support Stateful Failover until…




This attribute allows you to choose how the Gateway Load Balancer handles existing traffic flows after a target becomes unhealthy or is deregistered. The possible values are rebalance and no_rebalance. The default option (no_rebalance) continues to send existing flows to failed or drained targets. However, new flows are sent to healthy targets.

When you turn **Rebalance flows** on, the load balancer sends new and existing flows to healthy targets.

# Time to redirect traffic can be … long

**Considerations:**

- It is important to understand the time intervals involved in this feature. The total target failover time is a combination of multiple time intervals. Target Failover time = (time taken to detect failed target/drain the target) + (time taken to synchronize the GWLB data plane and to rebalance the flow to the new target). Sum of all these times may add up significantly and it may cause a delay in rebalancing existing flows to the healthy targets. Specifically,
  - This feature does not change the time it takes to detect target deregistration or failure. That timing is determined by the deregistration delay or the health check configuration. For example, when a customer configures 10 second health check interval and 3 missed heartbeats for failure detection, then the target detection time is 10 X 3 = 30 seconds.
  - For a target that is deregistered, GWLB waits for the deregistration delay time to expire, before it starts rebalancing the flows.
  - GWLB depends on TCP data segments to trigger rebalancing away from an unhealthy target. If a client's TCP stack is retransmitting segments (because the target became unhealthy or because of other unrelated packet drops in the network) TCP's exponential backoff can delay retransmissions increasing the time taken by GWLB to rebalance flows. The combination of failed target health check and drastically reduced traffic because of exponential backoff can cause the traffic to stall for a few minutes until a new TCP segment is retransmitted and arrives at the GWLB.
  - In order for flows to rebalance faster, we recommend using the lowest possible values for health check setting and the deregistration delay timeout. For example, setting "Deregistration Delay" to 60 seconds allows flow to rebalance to healthy target in ~120 seconds.
- Enabling this feature results in rebalancing the existing flows to a healthy target appliance. Healthy target appliances will receive these new flows without the 3-way TCP handshake. AWS partners, independent software vendors (ISVs) and/or customer organizations building their own solutions should have logic in place that allows target appliances to handle these new "in-transit" flows.
- Customers should check with their ISVs to understand how they have integrated their product with this feature. Specifically, pay attention to whether the ISV appliance is sending a reset and causing the client to restart the connection or whether it is rebalancing the flow to a healthy target without affecting the existing flow.

# Differences Between Physical and Virtual Cluster

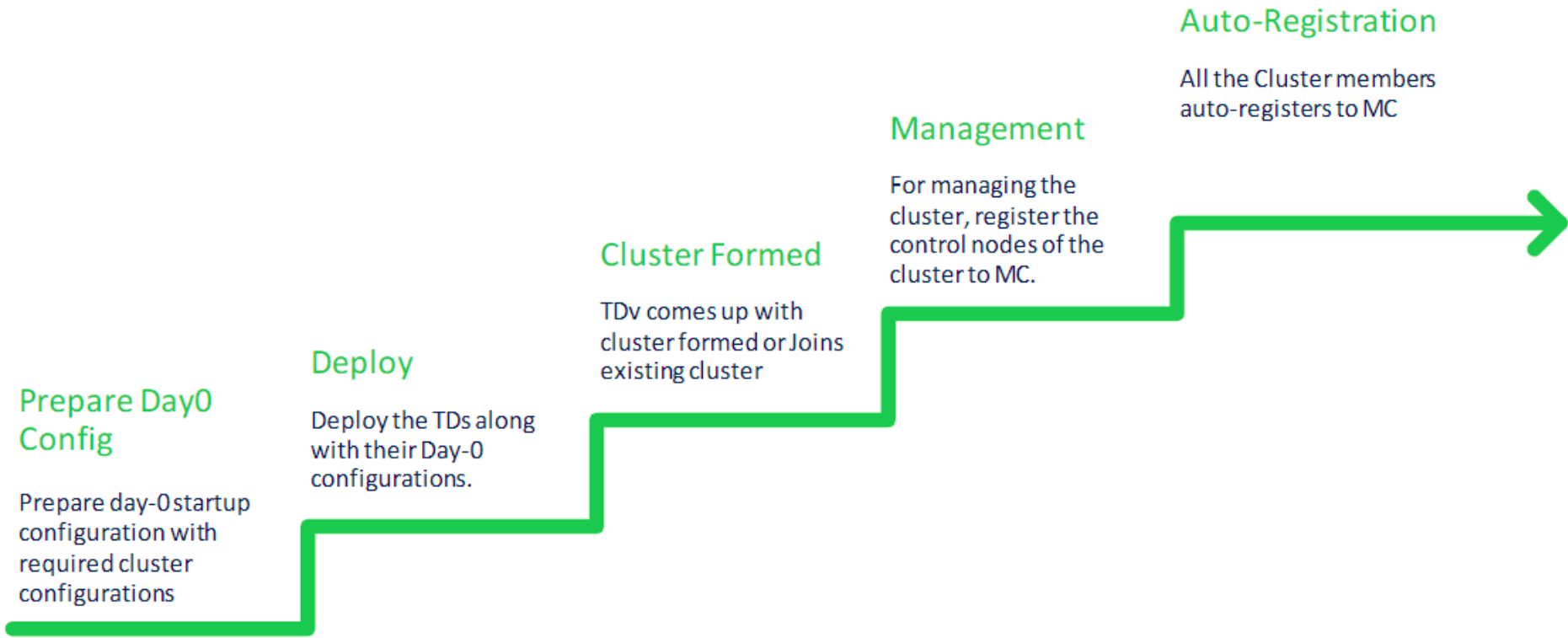
## Physical Cluster

- Data interfaces have two modes
  - Individual interface mode (different IP addresses on different nodes)
  - Spanned interface mode (uses EtherChannel)
- CCL uses proprietary protocol over IP (no transport layer protocol)
- CCL uses broadcast for internode communication
  - Dynamic node discovery

## Virtual Cluster

- Data interfaces are in Individual interface mode (different IP addresses on different nodes)
- CCL uses VXLAN over UDP
- CCL uses unicast
  - Cluster requires static peer list

# Public Cloud Workflow – AWS and GCP



# Day0 Config Overview

- Supports Day0 configuration on AWS and GCP platform. The cluster bootstrap configuration can be included in the Day0 config to create each node in the cluster.

- Two different options of Day0 supported for cluster creation.
  - Option 1: deploys FTDv cluster with fixed set of commands.

  - Option 2: deploys FTDv cluster with user configurable commands.

# Day0 optio-1

```
{
    "AdminPassword": "Cisco@123123",
    "Hostname": "ciscoftdv",
    "FirewallMode": "routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "10.10.55.2 10.10.55.253",
        "ClusterGroupName": "ngfwv-cluster",
        ”Geneve": "Yes",
        "HealthProbePort": "7777"
    }
```

Only for AWS GWLB

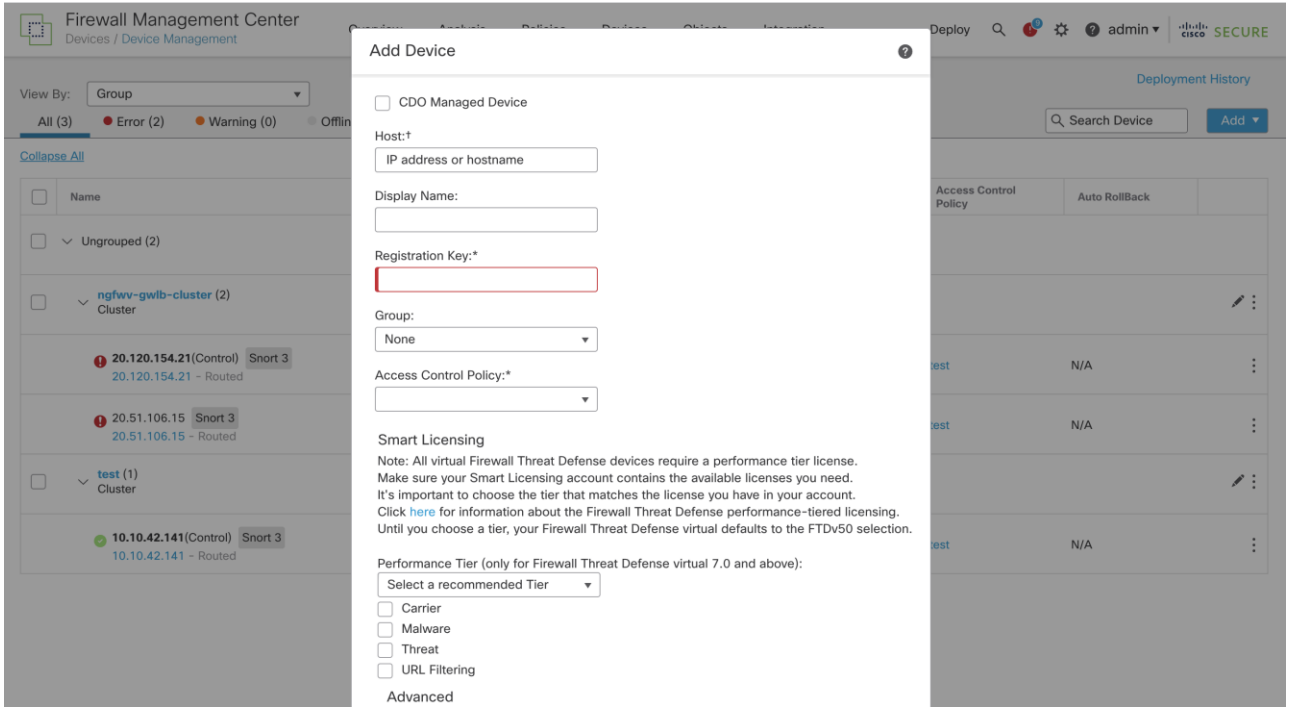
# Day0 option-2

```
{
        "AdminPassword": "Cisco@123123",
        "Hostname": "ciscoftdv",
        "FirewallMode": "routed",
        "ManageLocally": "No",
        "run_config": [ <<comma separated ftdv configuration>>]
}
```

# Day0 Option-2: run_config on AWS

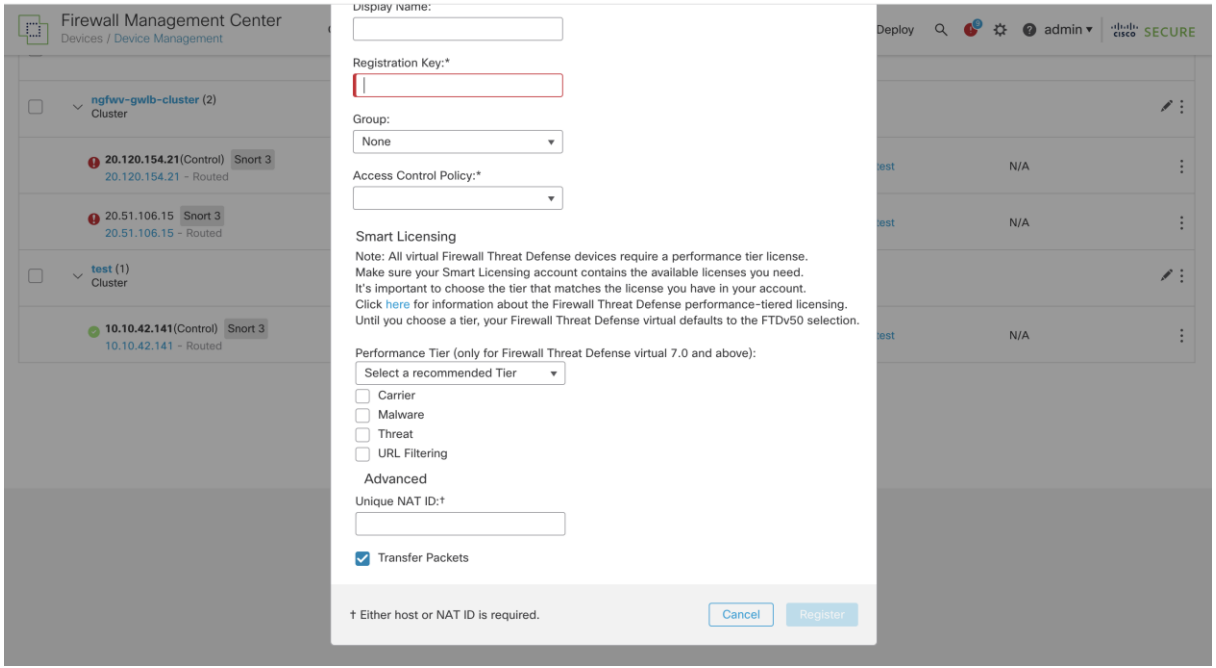
```
"run_config": [
"cluster interface-mode individual force",
"policy-map global_policy",
"class inspection_default",
"no inspect h323 h225",
"no inspect h323 ras",
"no inspect rtsp",
"no inspect skinny",
"interface TenGigabitEthernet0/0",
"nameif geneve-vtep-ifc",
"security-level 0",
"ip address dhcp",
"no shutdown",
"interface TenGigabitEthernet0/1",
"nve-only cluster",
"nameif ccl_link",
"security-level 0",
"ip address dhcp",
"no shutdown",
"interface vni1",
"description Clustering Interface",
"segment-id 1",
"vtep-nve 1",
"interface vni2",
"proxy single-arm",
"nameif ge",
"security-level 0",
"vtep-nve 2",
"object network ccl_link",
"range 10.1.90.4 10.1.90.254",
"object-group network cluster_group",
"network-object object ccl_link",
"nve 2",
"encapsulation geneve",
"source-interface geneve-vtep-ifc",
"nve 1",
"encapsulation vxlan",
"source-interface ccl_link",
"peer-group cluster_group",
"cluster group ftd-cluster",
"local-unit 1",
"cluster-interface vni1 ip 1.1.1.1 255.255.255.0",
"priority 1",
"enable",
"mtu geneve-vtep-ifc 1806",
"aaa authentication listener http geneve-vtep-ifc port 7575"
]
```

# Auto-Registering FTD Cluster to FMC – Step 1



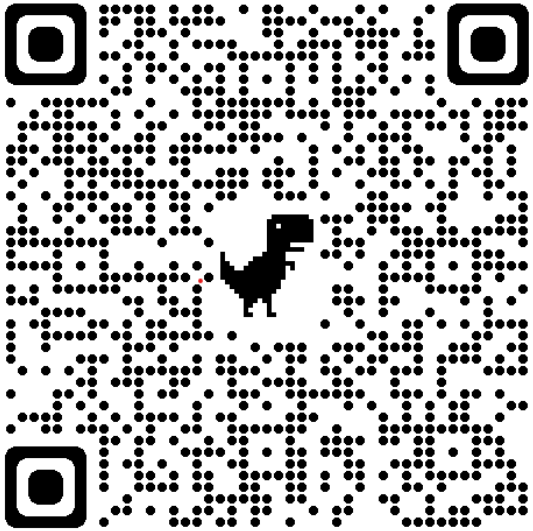

1. Once the AWS cluster is created, it can be managed by FMC by just registering a node in the cluster.
2. The Add device option present under Add -> Add Device section

# Auto-Registering FTD Cluster to FMC – Step 2




1. Manager details are to be added manually to one node of the cluster which is been discovered.
2. The auto-registration process will automatically take care of adding managers to all the other nodes and register them into the FMC and represent them a s a cluster

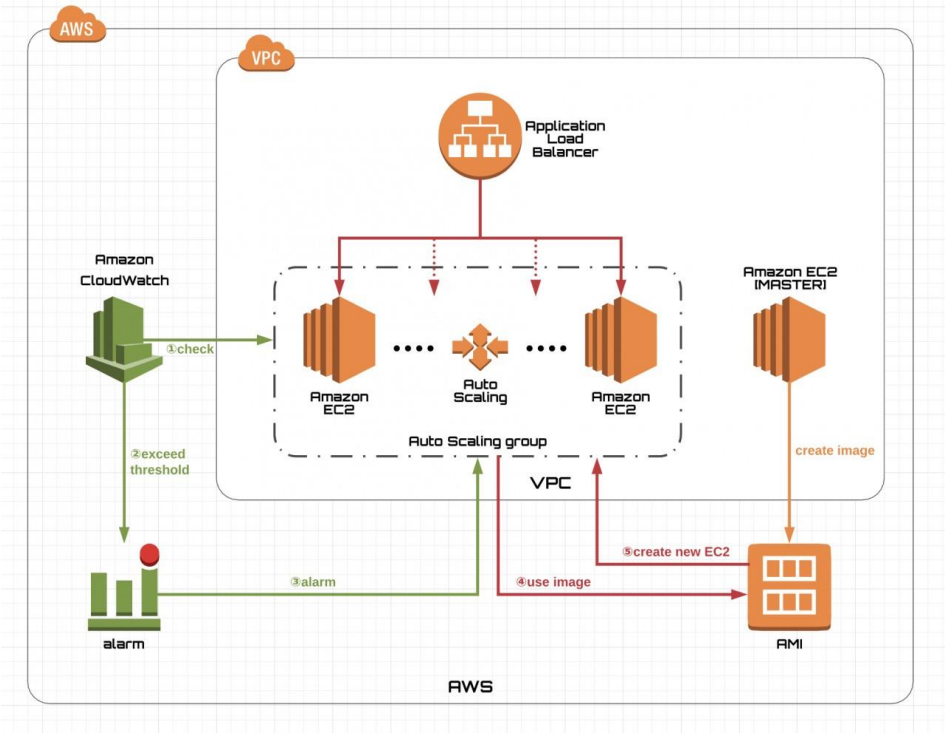
# Clustering in AWS



https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/cluster/ftdv-cluster-public.html

# AUTO-SCALING

# What about auto-scaling ?




**Group details**

| Desired capacity | Minimum capacity | Maximum capacity |
|---|---|---|
| 1 | 1 | 3 |

**Launch template**

| Launch template | AMI ID | Instance type |
|---|---|---|
| Solar-AS-1-ftd-launch-template<br>lt-0bed5c9e6494007cf | ami-0d1a9996bf3d5c6fd | c5.xlarge |

**Network**

| Availability Zones | Subnet ID |
|---|---|
| us-east-1a, us-east-1b | subnet-0644fec4721d524b5, subnet-02d9dc571dabe007f |

**Dynamic scaling policies** (4) Info — Actions

**Solar-AS-ScaleInCPUpolicy-kQz7JLK1h977**
Simple scaling
Enabled
Solar-AS-1Cpu-low-threshold
breaches the alarm threshold: CPUUtilization < 10 for 10 consecutive periods of 60 seconds for the metric dimensions:
AutoScalingGroupName = Solar-AS-1
Remove 1 capacity units
420 seconds before allowing another scaling activity

**Solar-AS-ScaleInMempolicy-OHLOpSvUkiV0**
Simple scaling
Enabled
Solar-AS-1Memory-low-threshold
breaches the alarm threshold: GroupAvgMem < 40 for 5 consecutive periods of 120 seconds for the metric dimensions:
fmcDeviceGroupName = aws-device-grp
AutoScalingGroupName = Solar-AS-1
Remove 1 capacity units
420 seconds before allowing another scaling activity

**Solar-AS-ScaleOutCPUpolicy-F84GrV891DMi**
Simple scaling
Enabled
Solar-AS-1Cpu-up-threshold
breaches the alarm threshold: CPUUtilization > 50 for 1 consecutive periods of 60 seconds for the metric dimensions:
AutoScalingGroupName = Solar-AS-1
Add 1 capacity units
420 seconds before allowing another scaling activity

**Solar-AS-ScaleOutMempolicy-aYakjU4SNZB7**
Simple scaling
Enabled
Solar-AS-1Memory-up-threshold
breaches the alarm threshold: GroupAvgMem > 70 for 4 consecutive periods of 120 seconds for the metric dimensions:
fmcDeviceGroupName = aws-device-grp
AutoScalingGroupName = Solar-AS-1
Add 1 capacity units
420 seconds before allowing another scaling activity

# But how FTDs get configured and register to FMC ?

# Introducing CloudWatch and Lamda Function

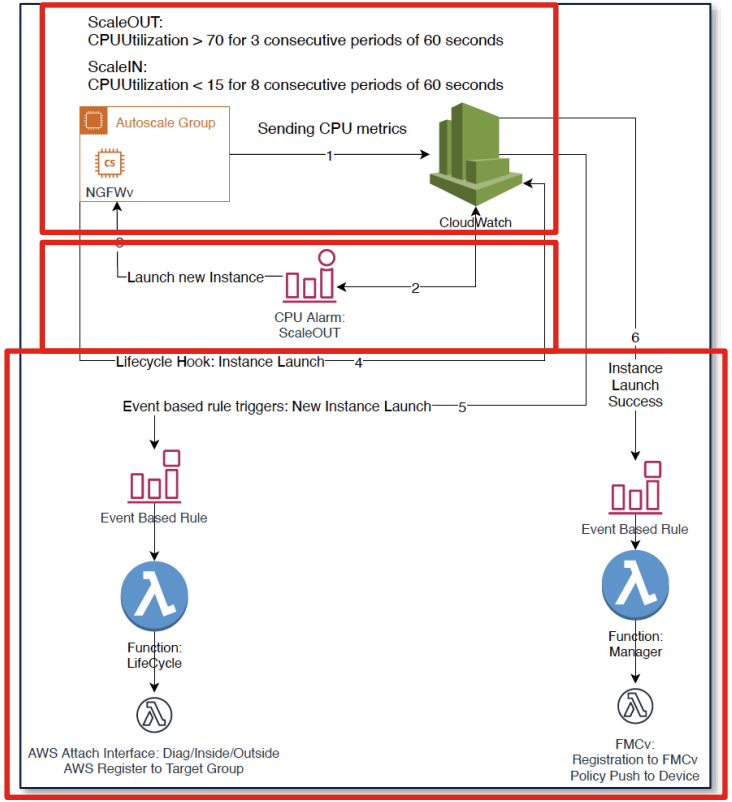
## CloudWatch

- 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

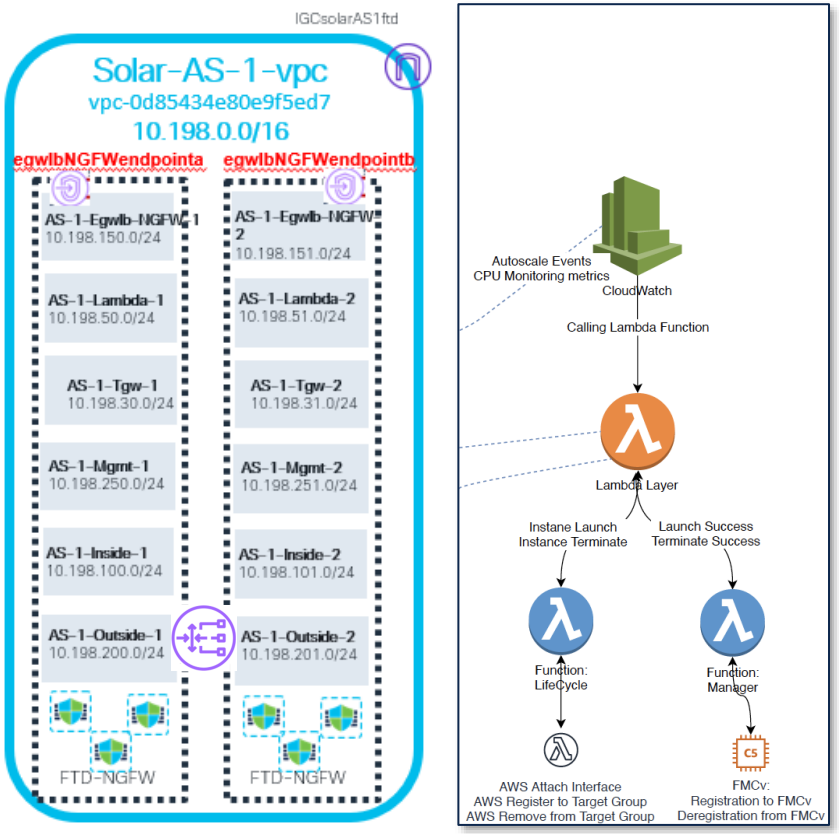
- Serverless architecture of AWS
- No servers to manage for the code
- Built-in fault tolerance
- Automatic-scaling
- Lambda code can interact with AWS infrastructure natively
- Support different languages: Python, Node.js, Ruby, Java, Go, .NET…

# How it works?




- CloudWatch monitors metrics
- Based on policies new instance is started
- Lambda functions triggered to:
  - Attach interfaces
  - Add instance to Target group
  - Register to FMC
  - Push config from FMC to FTDv

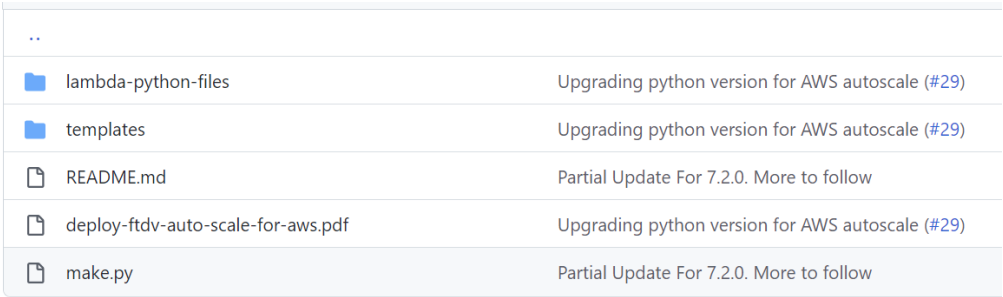
# In my lab



# That seems complicated to deploy…

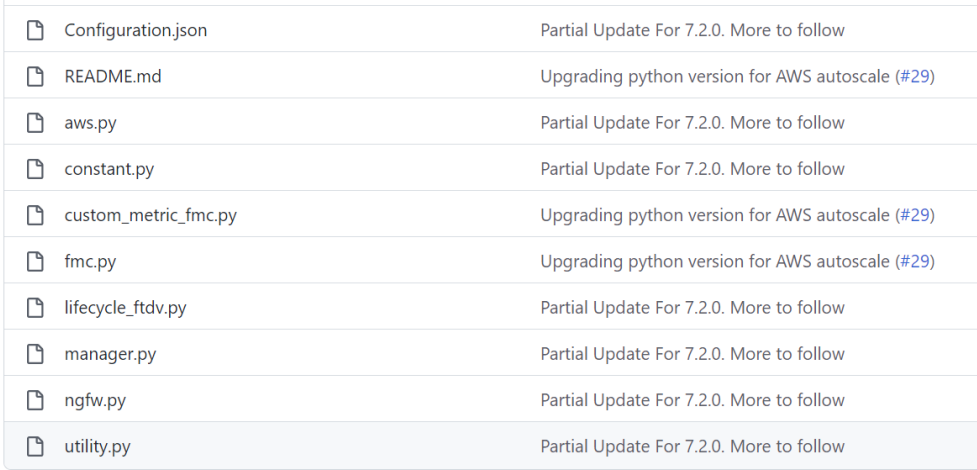
# How to deploy GWLB with AutoScaling ?

- Clone repository



# How to deploy GWLB with AutoScaling ?

- Clone repository
- Create autoscale_layer.zip

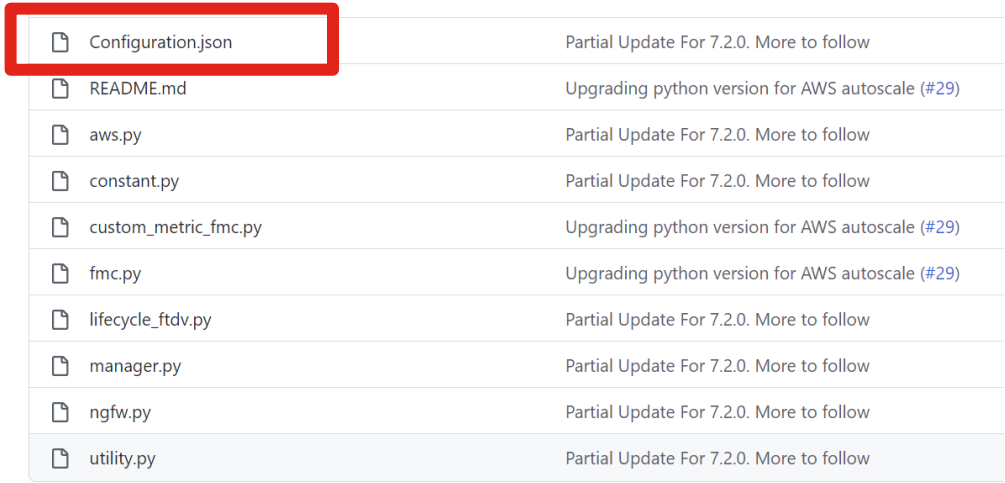


| | |
|---|---|
| Configuration.json | Partial Update For 7.2.0. More to follow |
| README.md | Upgrading python version for AWS autoscale (#29) |
| aws.py | Partial Update For 7.2.0. More to follow |
| constant.py | Partial Update For 7.2.0. More to follow |
| custom_metric_fmc.py | Upgrading python version for AWS autoscale (#29) |
| fmc.py | Upgrading python version for AWS autoscale (#29) |
| lifecycle_ftdv.py | Partial Update For 7.2.0. More to follow |
| manager.py | Partial Update For 7.2.0. More to follow |
| ngfw.py | Partial Update For 7.2.0. More to follow |
| utility.py | Partial Update For 7.2.0. More to follow |

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install cffi==1.15.1
pip3 install cryptography==2.9.1
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
pip3 install pycryptodome==3.15.0
echo "Copy from ./layer directory to ./python\n"
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r autoscale_layer.zip ./python
```

# How to deploy GWLB with AutoScaling ?

- Clone repository
- Create autoscale_layer.zip
- Tune configuration.json file



| | |
|---|---|
| Configuration.json | Partial Update For 7.2.0. More to follow |
| README.md | Upgrading python version for AWS autoscale (#29) |
| aws.py | Partial Update For 7.2.0. More to follow |
| constant.py | Partial Update For 7.2.0. More to follow |
| custom_metric_fmc.py | Upgrading python version for AWS autoscale (#29) |
| fmc.py | Upgrading python version for AWS autoscale (#29) |
| lifecycle_ftdv.py | Partial Update For 7.2.0. More to follow |
| manager.py | Partial Update For 7.2.0. More to follow |
| ngfw.py | Partial Update For 7.2.0. More to follow |
| utility.py | Partial Update For 7.2.0. More to follow |

# Configuration.json

IP@ of FMC, must be routable to Lambda network and FTDv mgnt subnets

Change to TenGig if you use C5.xLarge

DO NOT set a gateway, trust me !

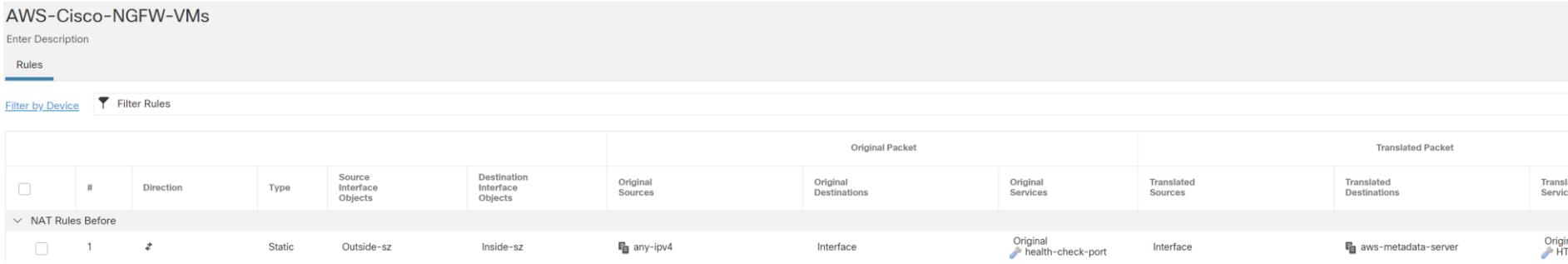

MUST match the names in FMC

# How to deploy GWLB with AutoScaling ?

- Clone repository
- Create autoscale_layer.zip
- Tune configuration.json file
- Pre-configure FMC

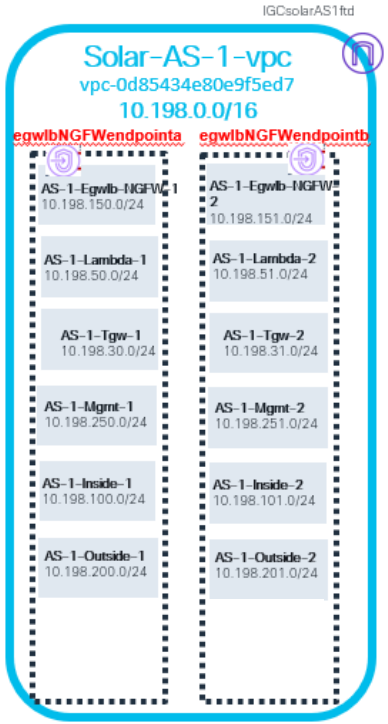
| Object Type | Name | Value |
|---|---|---|
| Host | aws-metadata-server | 169.254.169.254 |
| Port | health-check-port | 8080/any other port as required |
| Zone | Intside-sz | — |
| Zone | Outside-sz | — |

| Access Control Policy | Domain | Status | Last Modified |
|---|---|---|---|
| aws-asg-policy | Global | Targeting 1 devices<br>*Out-of-date on 1 targeted devices* | 2023-01-27 06:11:34<br>Modified by "Firepower System" |



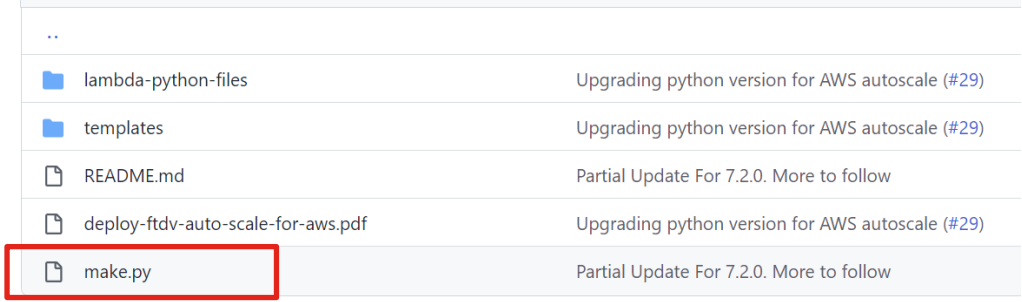
# How to deploy GWLB with AutoScaling ?

- Clone repository
- Create autoscale_layer.zip
- Tune configuration.json file
- Pre-configure FMC
- Deploy in CloudFormation  infrastructure_gwlb.yaml

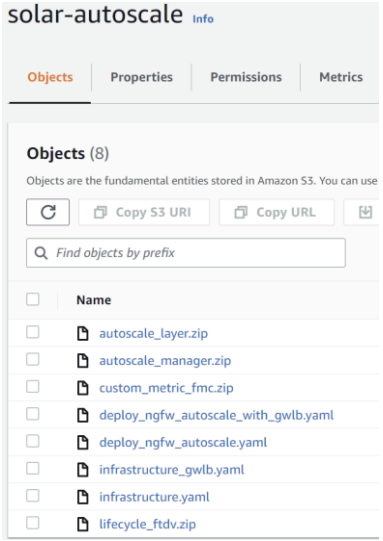


# How to deploy GWLB with AutoScaling ?

- Clone repository
- Create autoscale_layer.zip
- Tune configuration.json file
- Pre-configure FMC
- Deploy in CloudFormation  infrastructure_gwlb.yaml
- Use « python3 make.py build » to create all ZIP file needed in Target



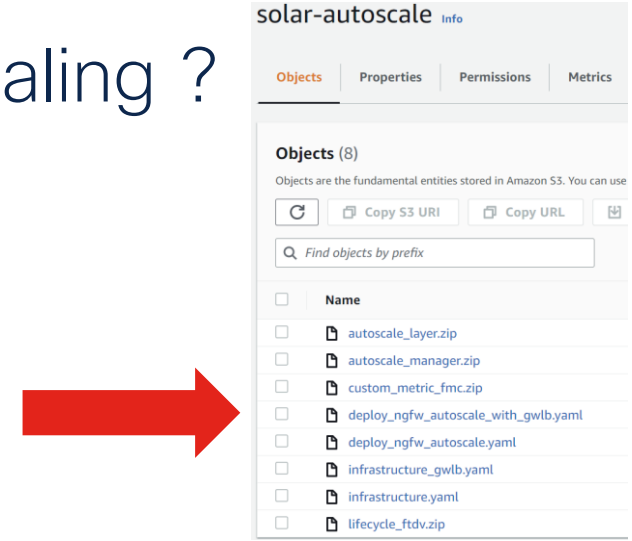
# How to deploy GWLB with AutoScaling ?




- Clone repository
- Create autoscale_layer.zip
- Tune configuration.json file
- Pre-configure FMC
- Deploy stack in CloudFormation  infrastructure_gwlb.yaml
- Use « python3 make.py build » to create all ZIP file needed in Target
- Copy all files in S3 bucket created by infrastructure_gwlb.yaml

# How to deploy GWLB with AutoScaling ?

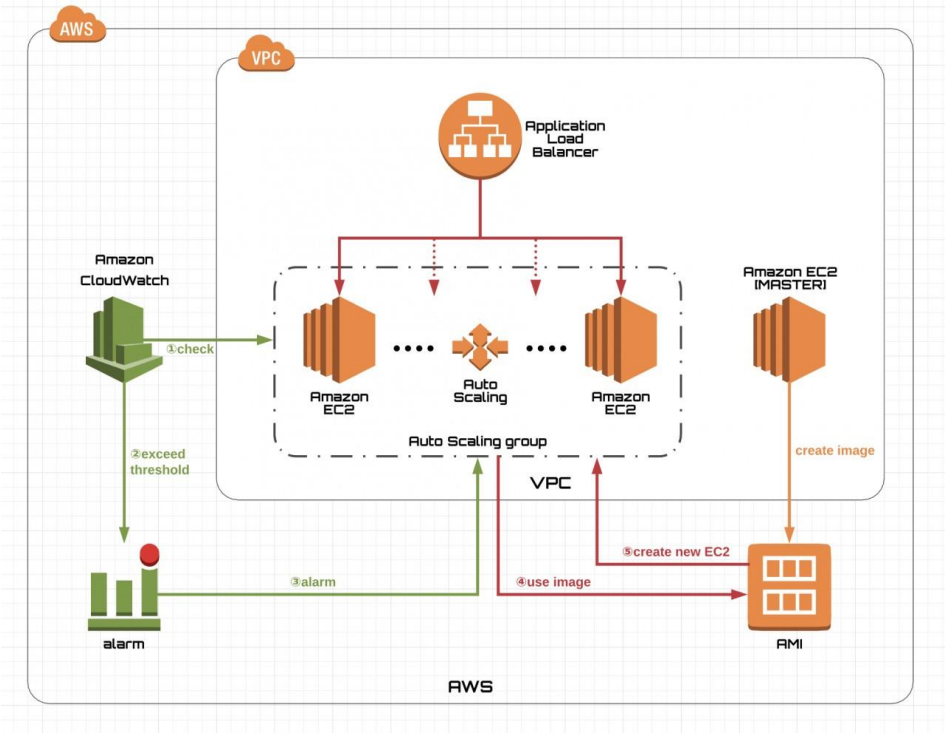
- Clone repository
- Create autoscale_layer.zip
- Tune configuration.json file
- Pre-configure FMC




- Deploy stack in CloudFormation  infrastructure_gwlb.yaml
- Use « python3 make.py build » to create all ZIP file needed in Target
- Copy all files in S3 bucket created by infrastructure_gwlb.yaml
- Deploy stack in CloudFormation **deploy_ngfw_autoscale_with_gwlb.yaml**

# SNAPSHOT

# What about auto-scaling ?




**Group details**

Desired capacity
1

Minimum capacity
1

Maximum capacity
3

**Launch template**

| Launch template | AMI ID | Instance type |
|---|---|---|
| Solar-AS-1-ftd-launch-template<br>lt-0bed5c9e6494007cf | ami-0d1a9996bf3d5c6fd | c5.xlarge |

**Network**

| Availability Zones | Subnet ID |
|---|---|
| us-east-1a, us-east-1b | subnet-0644fec4721d524b5, subnet-02d9dc571dabe007f |

**Dynamic scaling policies** (4) Info — Actions

Solar-AS-ScaleInCPUpolicy-kQz7JLK1h977
Simple scaling
Enabled
Solar-AS-1Cpu-low-threshold
breaches the alarm threshold: CPUUtilization < 10 for 10 consecutive periods of 60 seconds for the metric dimensions:
AutoScalingGroupName = Solar-AS-1
Remove 1 capacity units
420 seconds before allowing another scaling activity

Solar-AS-ScaleInMempolicy-OHLOpSvUkiV0
Simple scaling
Enabled
Solar-AS-1Memory-low-threshold
breaches the alarm threshold: GroupAvgMem < 40 for 5 consecutive periods of 120 seconds for the metric dimensions:
fmcDeviceGroupName = aws-device-grp
AutoScalingGroupName = Solar-AS-1
Remove 1 capacity units
420 seconds before allowing another scaling activity

Solar-AS-ScaleOutCPUpolicy-F84GrV891DMi
Simple scaling
Enabled
Solar-AS-1Cpu-up-threshold
breaches the alarm threshold: CPUUtilization > 50 for 1 consecutive periods of 60 seconds for the metric dimensions:
AutoScalingGroupName = Solar-AS-1
Add 1 capacity units
420 seconds before allowing another scaling activity

Solar-AS-ScaleOutMempolicy-aYakjU4SNZB7
Simple scaling
Enabled
Solar-AS-1Memory-up-threshold
breaches the alarm threshold: GroupAvgMem > 70 for 4 consecutive periods of 120 seconds for the metric dimensions:
fmcDeviceGroupName = aws-device-grp
AutoScalingGroupName = Solar-AS-1
Add 1 capacity units
420 seconds before allowing another scaling activity

# Time to start Instances in Average

FTDv FIRST start : 15 mins

FTDv other starts : 5 mins

FTDv snapshot starts : 5 mins

# Deploy FTDv Instance For Snapshot

- Deploy FTDv with the 7.2 cloud image.
  - Ref: FTDv install in AWS / FTDv install in Azure
- Make sure it is not registered to any manager.
  - It is expected to have clean setup for snapshot creation.

```
> show version
-------------------[ firepower ]--------------------
Model                     : Cisco Firepower Threat Defense for AWS (75) Version 7.2.0 (Build 10)
UUID                      : c6aa6530-e00d-11eb-af9d-86dd290d6c1b
VDB version               : 344
----------------------------------------------------
> show snapshot detail
Not a snapshot instance.
>
> show managers
No managers configured.
```

# Prepare Deployed FTDv For Snapshot:

- Go to expert mode -> sudo prompt
- Execute "prepare_snapshot"
  - This step shuts down the instance after required processing.

```
> expert
admin@FTDvbaseimg:~$ sudo su
root@FTDvbaseimg:/home/admin# prepare_snapshot
Hypervisor type is AWS...


**************** Prepare the instace for image snapshot ****************


This script will remove all lina config,  deployed policies,
configured manager, uuids. After all operation it will shutdown
the instance. Post shutdown, you can take snapshot from the instance.

Do you want to coninue [Y/N]:
```

Above example is from AWS FTDv Instance. Same steps can be followed for Azure.

# Prepare Deployed FTDv For Snapshot: (Contd…)

- Optionally you execute “prepare_snapshot -f”
  - "-f" option removes user input prompt and directly execute the script without any warning.
  - This step shuts down the instance after required processing.
- Once the instance stopped properly, you can create snapshot image.

```
> expert
admin@FTDvbaseimg:~$ sudo su
root@FTDvbaseimg:/home/admin# prepare_snapshot -f
Hypervisor type is AWS...
Collect data for current instance
Removing manager from device.
Removing all managers from device.
Manager is going to be removed permanently.
Waiting for 397d75ac-5d6d-11ec-aa2f-c6b540e3df74 instance 1 socket
Waiting for 397d75ac-5d6d-11ec-aa2f-c6b540e3df74 instance 1 socket
Waiting for 397d75ac-5d6d-11ec-aa2f-c6b540e3df74 instance 1 socket
Manager has been removed permanently from FTD.
Clean all DE_Config...
Clean all sensor policy uuid from the system.
Clean DE_engine ID: 397d75ac-5d6d-11ec-aa2f-c6b540e3df74
copy exiting uuid as orig_uuid to snapshot instance
Remove uuid from ims.conf
sed: couldn't open temporary file /ngfw/etc/rc.d/init.d/sedzLASnr: Read-only file system
Touch snapshot flag for FSIC optimization
Remove device serial no
Clean all lina config...
The lina config command is executed.

Check for file system integrity before taking snapshot.
Shutdown the instance to take snapshot...

Broadcast message from root@FTDvbaseimg (pts/0) (Wed Dec 15 06:23:13 2021):
The system is going down for system halt NOW!
root@FTDvbaseimg:/home/admin#
```

# DEMO

# Cisco Secure Dynamic Attribute Connector and FTD Dynamic Groups

cisco Live!

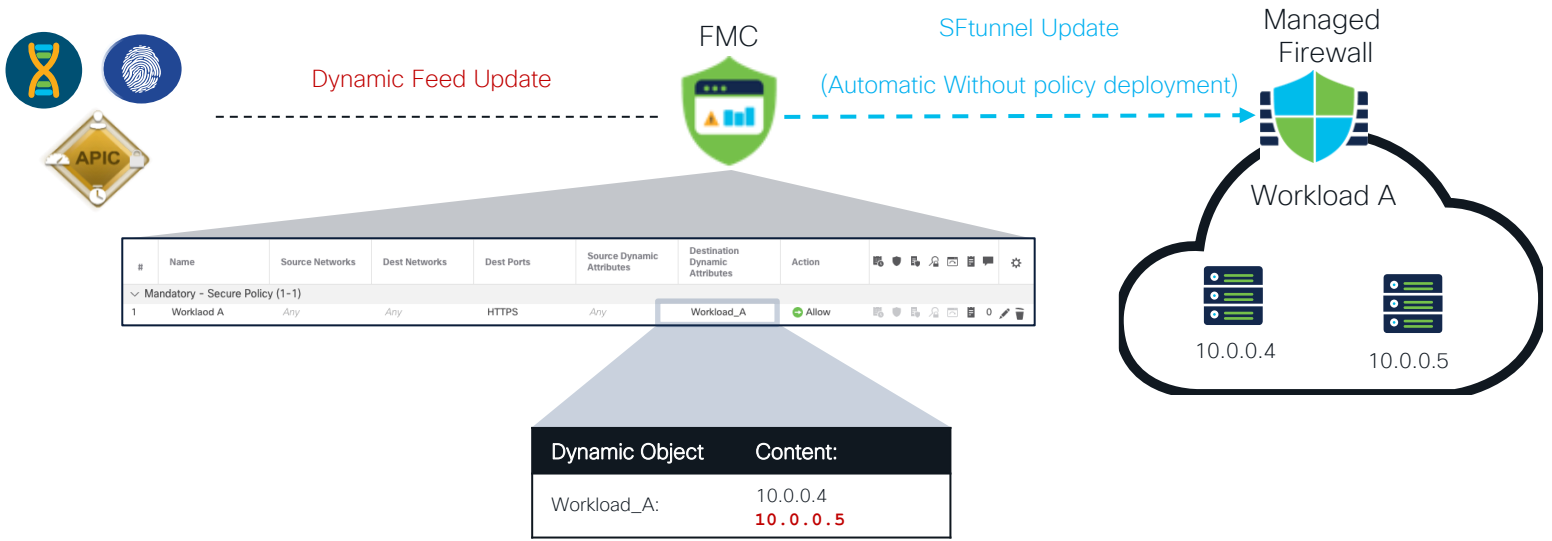
# Problem Statement

- Application/workload changes happen more often

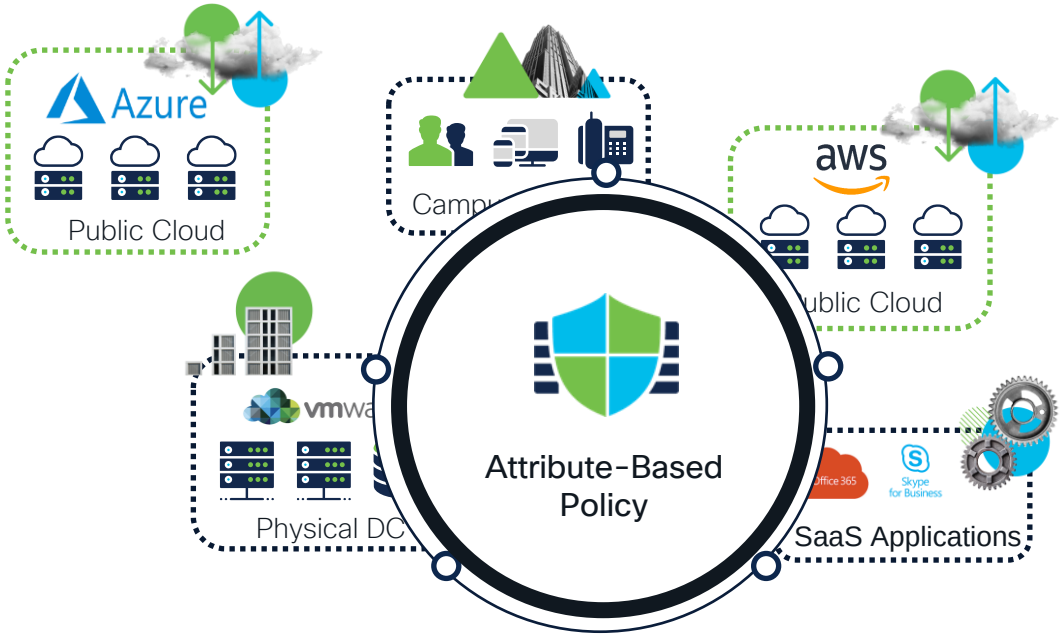
- Multiple Security domains

# Dynamic Objects in Action

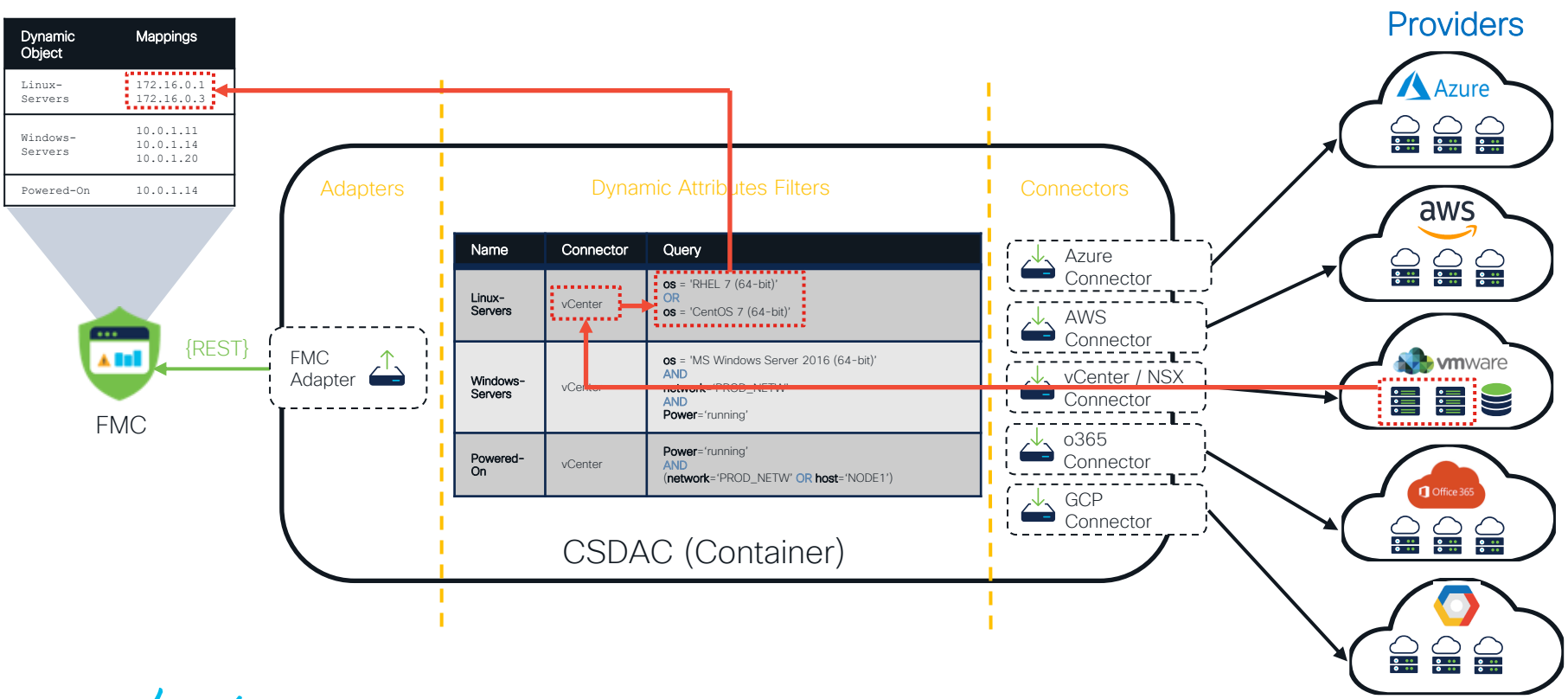
## Automatic Without policy deployment



# How do I ingest all those different attributes to build firewall Policies ?



# Cisco Secure Dynamic Attribute Connector



# Attribute Based Policy – CSDAC Attributes

| # | Name | Source Zones | Dest Zones | Users | Applications | Dest Ports | Source Dynamic Attributes | Destination Dynamic Attributes | Action |
|---|---|---|---|---|---|---|---|---|---|
| > Mandatory - Attribute-Based Policy (-) | | | | | | | | | |
| v Default - Attribute-Based Policy (1-9) | | | | | | | | | |
| 1 | Workload_1 | Any | Any | Any | Any | HTTPS | WorkloadObj_615c486dc9 | WorkloadObj_615c8066483 | Allow |
| 2 | IoT Support Service | External | IoT_VN | Any | Any | HTTPS SSH | IoT_Support | IoT | Allow |
| 3 | Machine Authentication | Corporate_VN | Shared_Services | Any | Any | AD_Services | Machine_Auth | VMWare_Active_Directory | Allow |
| 4 | Printing Service | Corporate_VN | Data_Center_Edge | Any | Any | SNMP -PING ler_Service | RICOH-Aficio-SP-C410DN RICOH-Aficio-SP-C820DN Xerox-WorkCentre-5030 Xerox-WorkCentre-5135 | APIC_A_ESG_Print_Servers | Allow |
| 5 | Block Social Media | Corporate_VN | External | Any | Instagram Tinder Twitter | | Contractors Branch_Locations | Any | Block |
| 6 | o365 Access | Corporate_VN | External | lab-local/Domain Users | Any | HTTPS HTTP | Any | o365_Common o365_Exchange o365_SharePoint | Allow |
| 7 | SecureX Threat Containment | Corporate_VN | Data_Center_Edge | Any | Any | | SecureX_Quarantined_IPs SecureX_Suspicious_IPs | Honeypot_Service | Allow |
| 8 | ISE Threat Containment | Corporate_VN | Data_Center_Edge | Any | Any | | Quarantined_Systems | Honeypot_Service | Allow |
| 9 | Cloud App Access | Corporate_VN | WAN | Any | Any | HTTP HTTPS | Employees | Azure_HR_Workload Azure_Intranet_Service | Allow |

vCenter / NSX Dynamic Objects

o365 Public

Public Cloud Tags

# Attribute Based Policy

| # | Name | Source Zones | Dest Zones | Users | Ap... | Dest Ports | Source Dynamic Attributes | Destination Dynamic ...es | Action |
|---|---|---|---|---|---|---|---|---|---|
| > | Mandatory - Attribute-Based Policy (-) | | | | | | | | |
| v | Default - Attribute-Based Policy (1-9) | | | | | | | | |
| 1 | Workload_1 | Any | Any | Any | Any | HTTP<br>HTTPS | WorkloadObj_615c486dc9 | WorkloadObj_615c8066483 | A... |
| 2 | IoT Support Service | External | IoT_VN | Any | | HTTPS<br>SSH | IoT_Support | IoT | Allow |
| 3 | Machine Authentication | Corporate_VN | Shared_Services | Any | Any | AD_Services | Machine_Auth | VMWare_Active_Directory | Allow |
| 4 | Pri... | Corporate_VN | Data_Center_Edge | Any | | SNMP<br>ICMP-PING<br>Spooler_Service | RICOH-Aficio-SP-C410DN<br>RICOH-Aficio-SP-C820DN<br>Xerox-WorkCentre-5030<br>Xerox-WorkCentre-5135 | APIC_A_ESG_Print_Servers | Allow |
| 5 | Block Social Media | ...VN | External | Any | Facebook<br>Google+<br>Instagram<br>Tinder<br>Twitter | Any | Contractors<br>Branch_Locations | Any | Block |
| 6 | o365 Access | Corporate_VN | External | lab-local/Domain Users | Any | HTTPS<br>HTTP | Any | o365_Common<br>o365_Exchange<br>o365_SharePoint | Allow |
| 7 | SecureX Threat Containment | Corporate_VN | Data_Center_Edge | Any | Any | Any | SecureX_Quarantined_IPs<br>SecureX_Suspicious_IPs | Honeypot_Service | Allow |
| 8 | ISE Threat Containment | Corporate_VN | Data_Center_Edge | Any | Any | Any | Quarantined_Systems | Honeypot_Service | Allow |
| 9 | Cloud App Access | Corporate_VN | WAN | Any | Any | HTTP<br>HTTPS | Employees | Azure_HR_Workload<br>Azure_Intranet_Service | Allow |













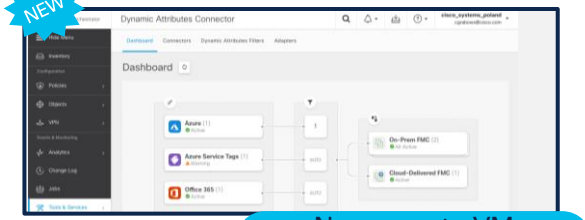
# The New Cloud Form Factor

CSDAC
(Linux Machine)


Standalone

CSDAC in CDO's
Tools & Services

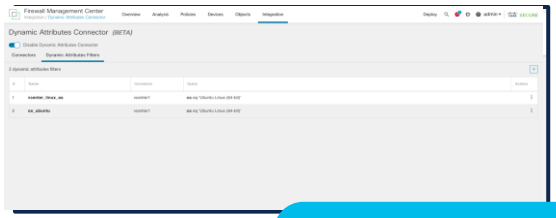
NEW




No separate VM required!!

Cloud Delivered

CSDAC in FMC



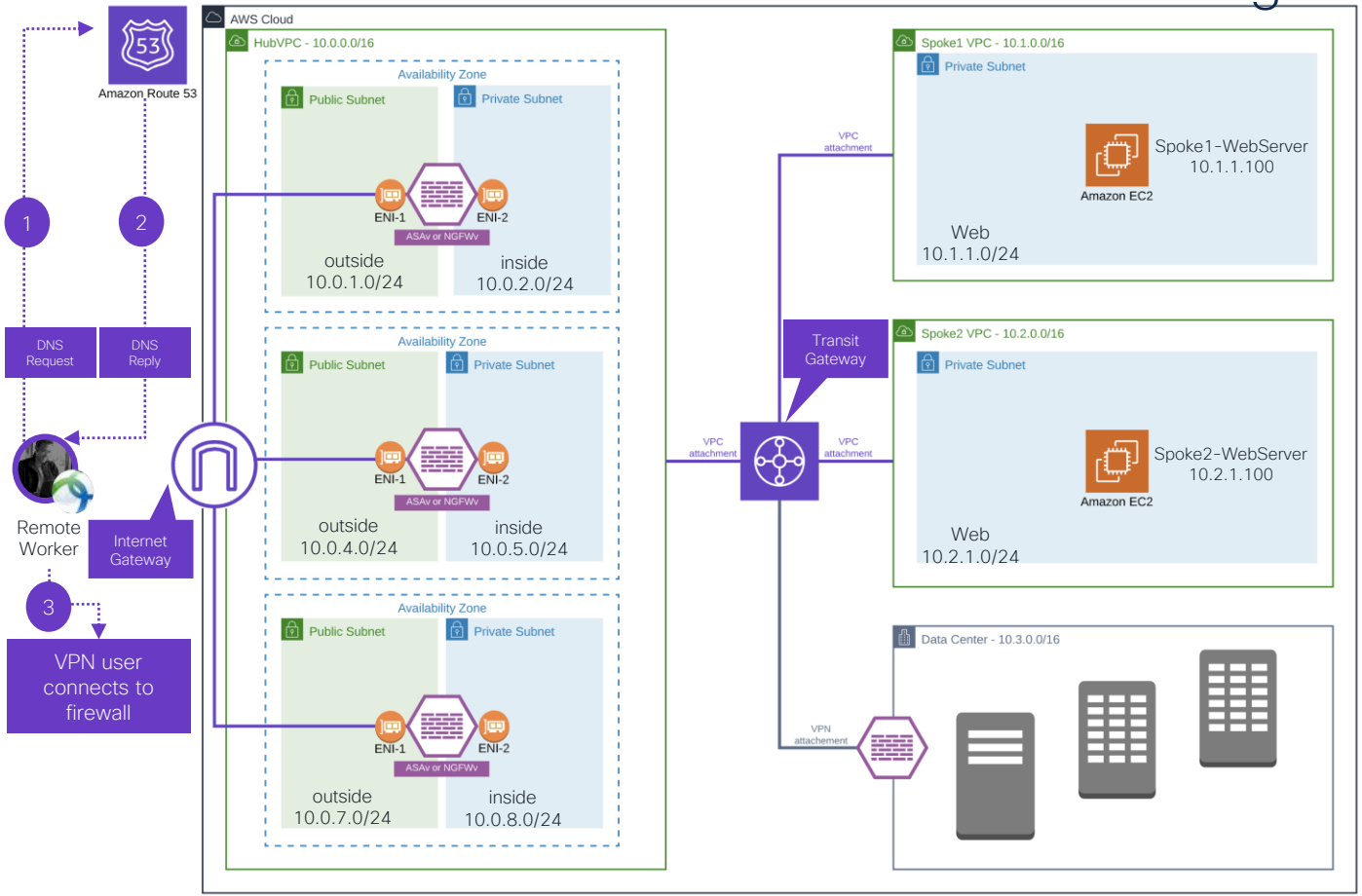

Coming Fall 2023

Built In

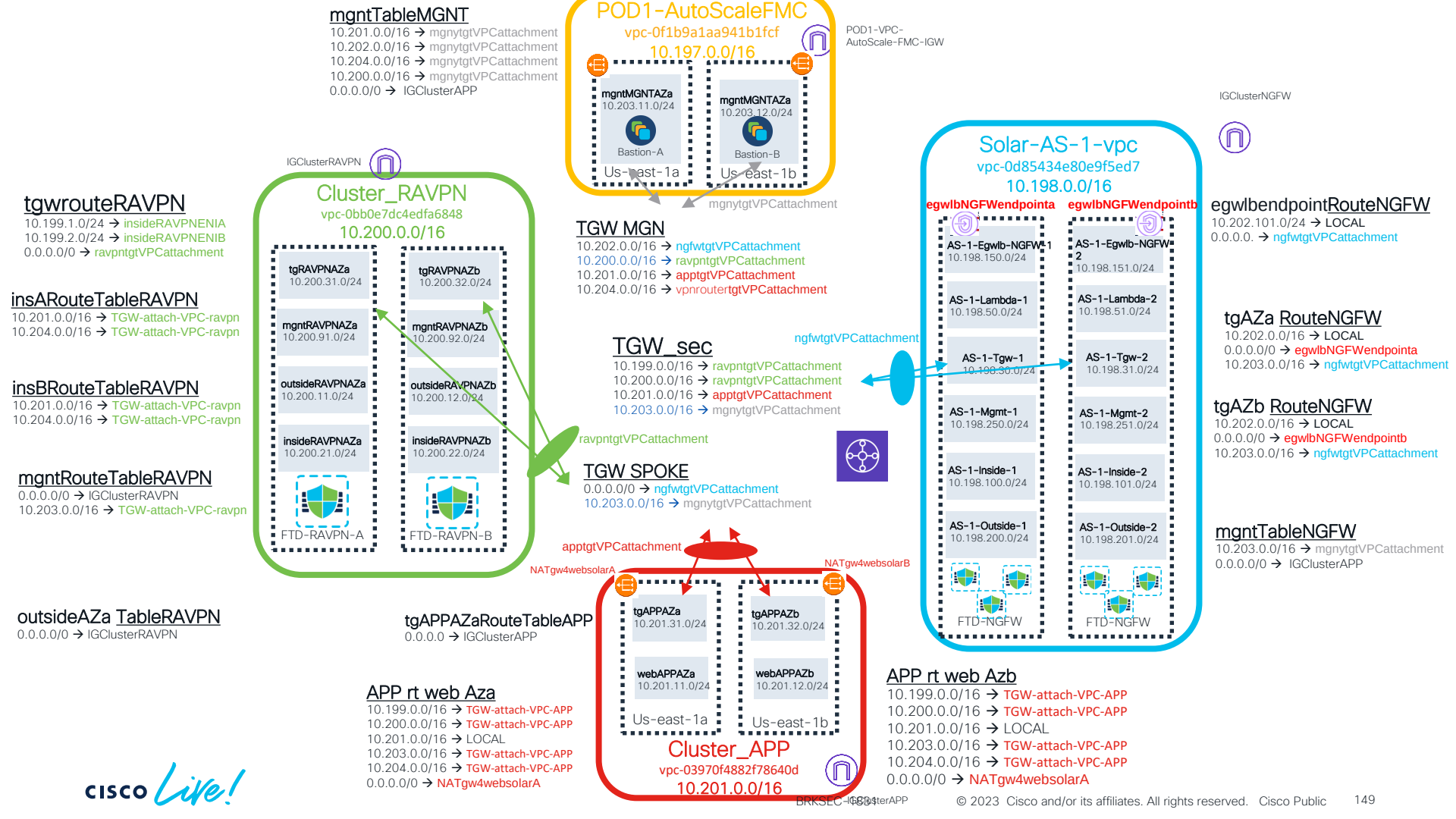
# Provide Remote Access

- FTDv with Anyconnect
- DUO Network Gateway

# Cisco Secure Remote Worker Validated Design

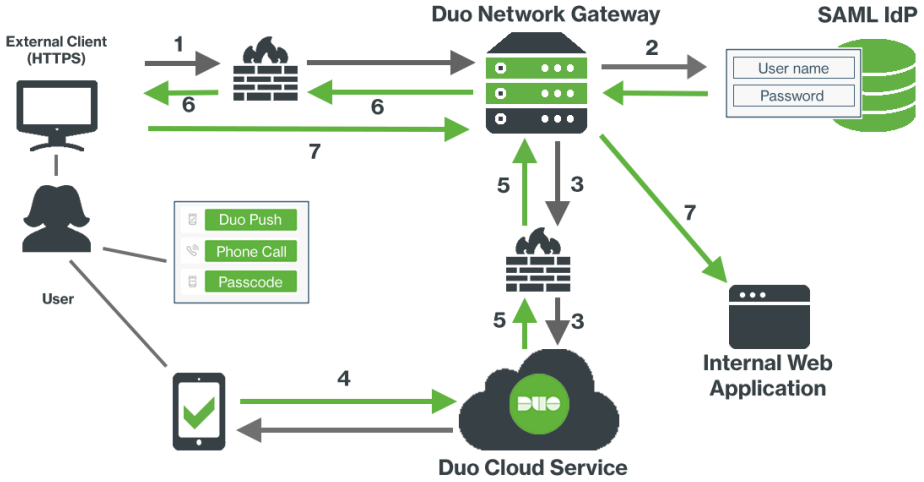



- VPN Load balancing using Route53
- AWS Route 53 maintains host record for each firewall
- TTL is defined on AWS Route 53
- AWS Route53 health check to monitor firewall
- Each AZ may have multiple firewalls
- Cisco ASAv or NGFWv acts as a VPN concentrator
- Transit Gateway connects VPC using VPC attachment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



# What is Duo Network Gateway ?

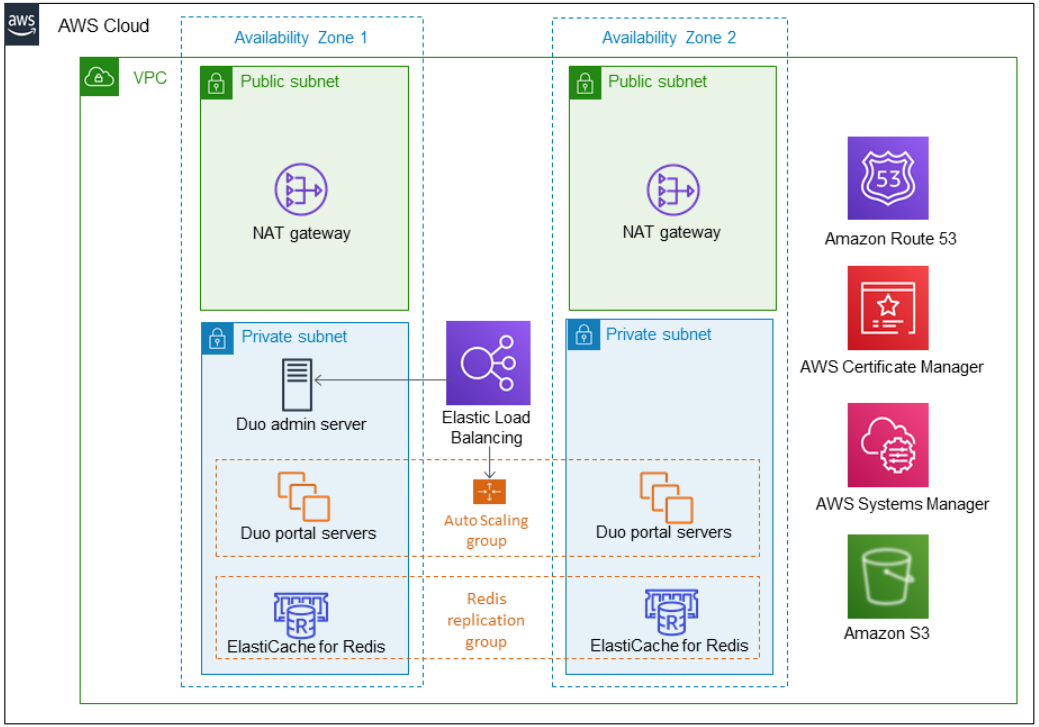
The Duo Network Gateway enables organizations to provide Zero Trust Remote Access to web applications, Remote Desktop or SSH servers without the requirement of a VPN.



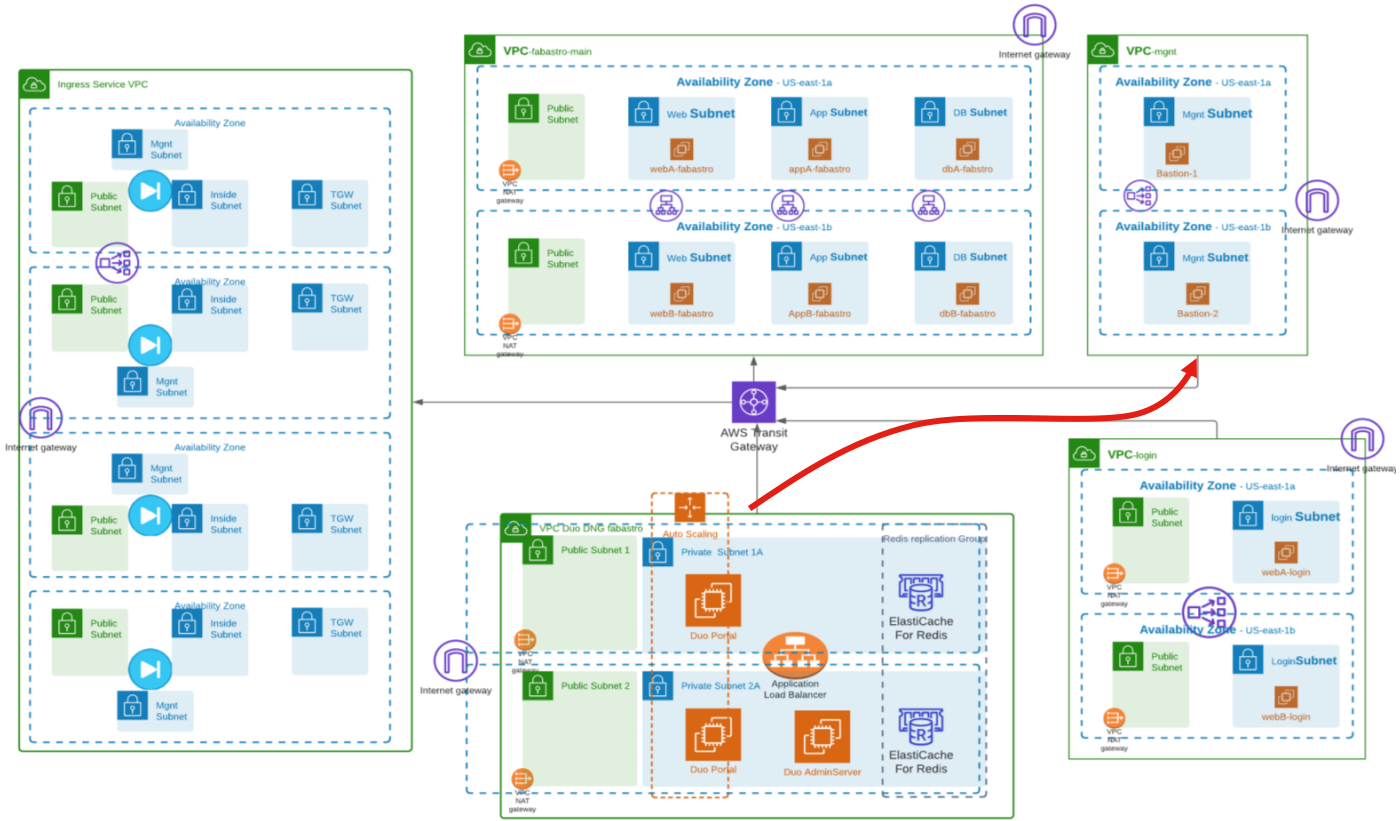
# DNG Use Cases for FabAstro…or else

- 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.

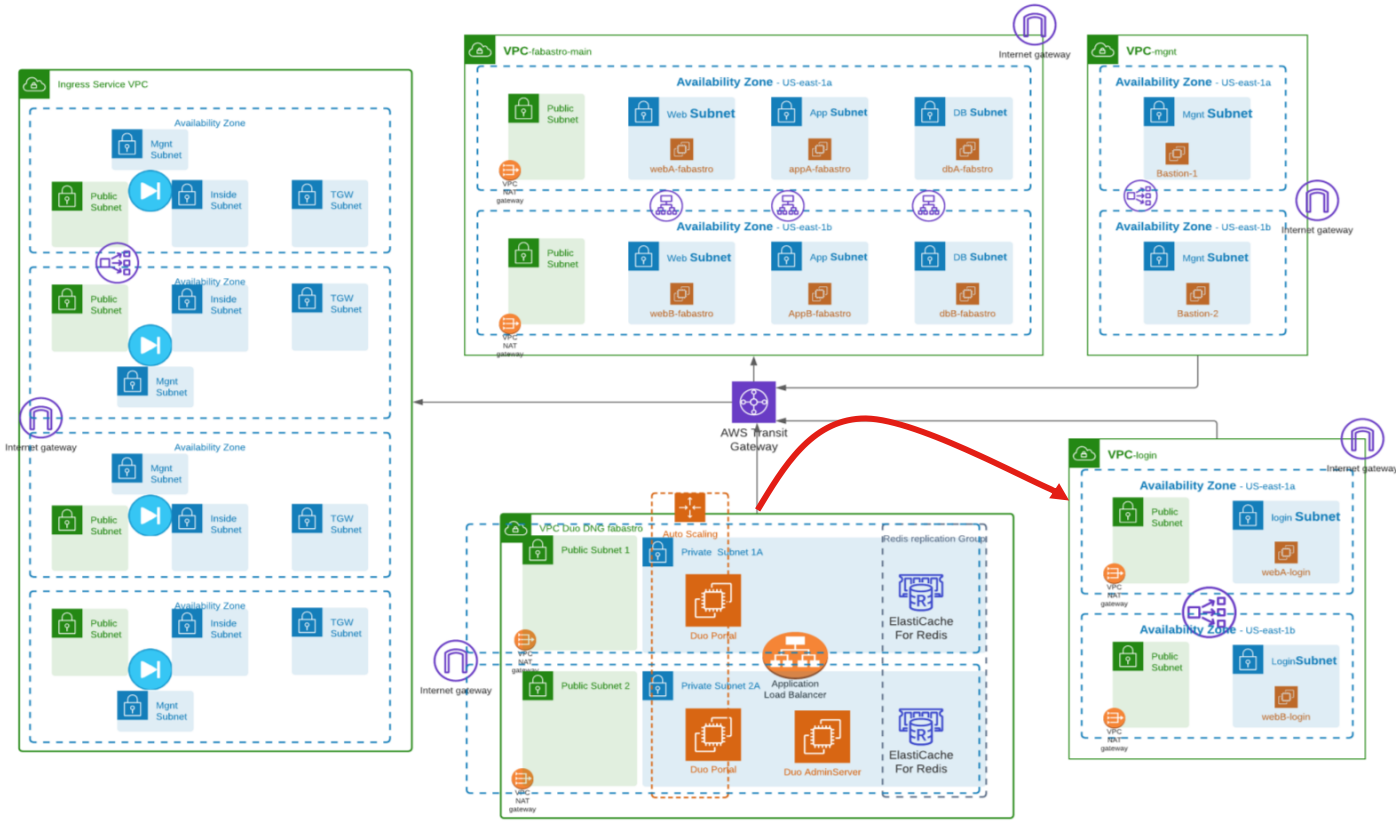
# What the CloudFormation Deployes



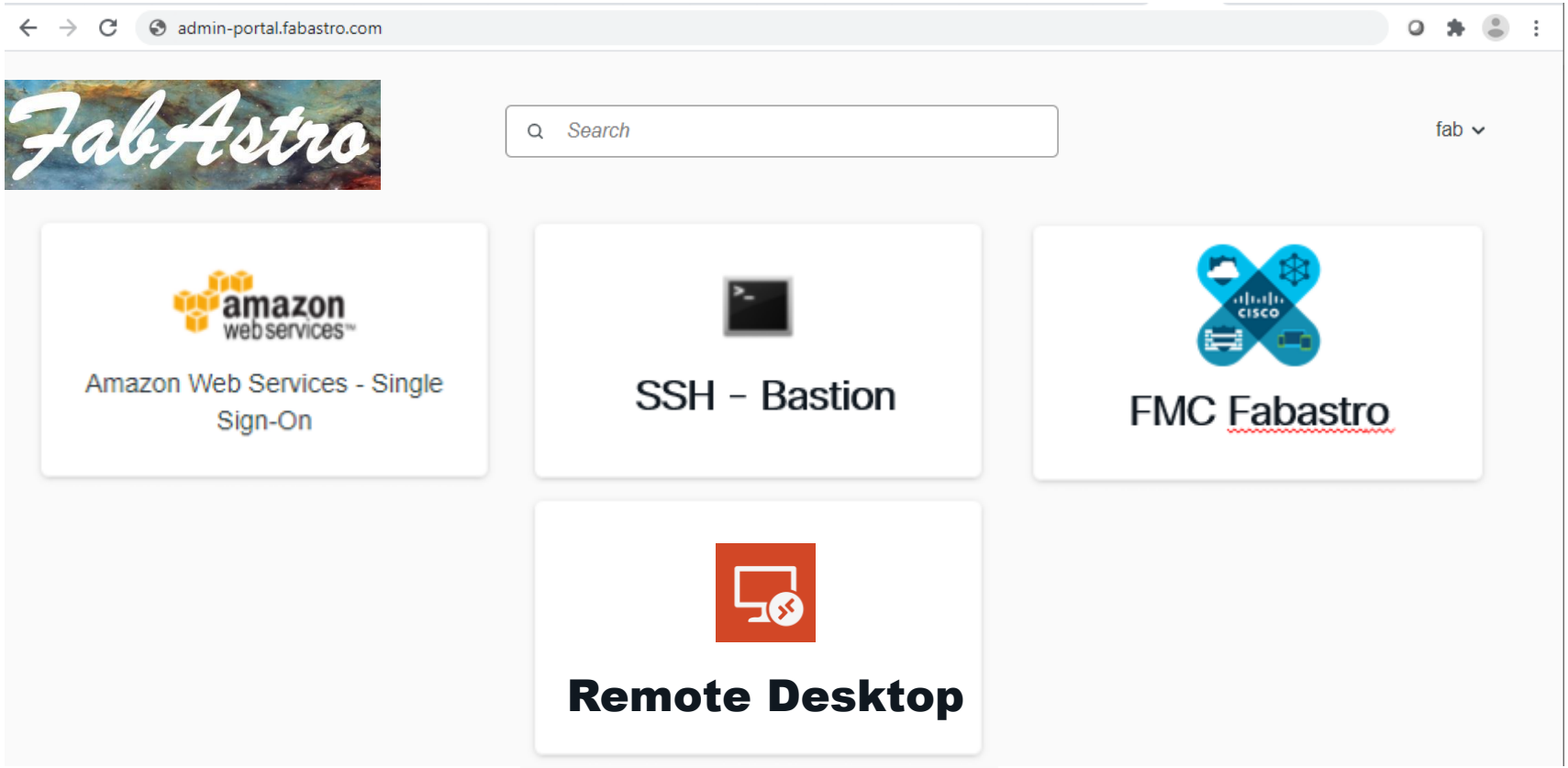
# DNG in FabAstro: Access for Admins



# DNG in FabAstro: Web portal for Privileged Users

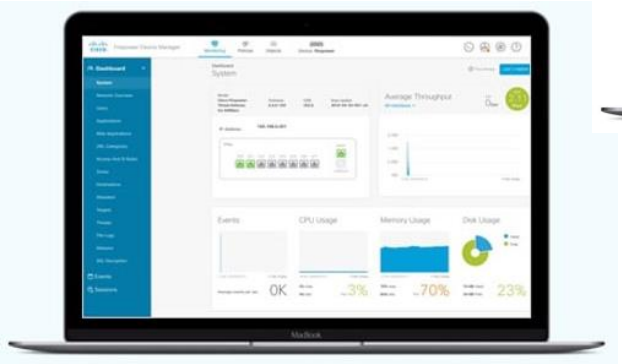


# Using DNG to access FabAstro Admin Portal

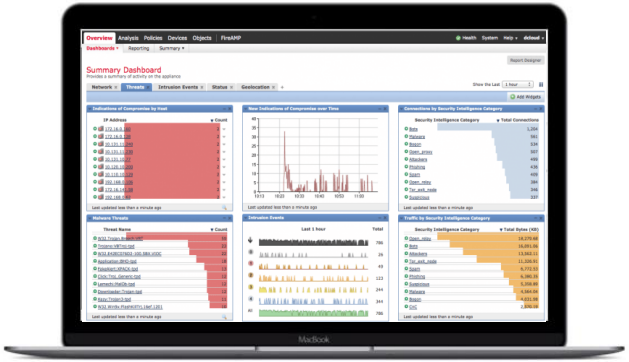


# Management and automation

# How do I manage my FTDs ?

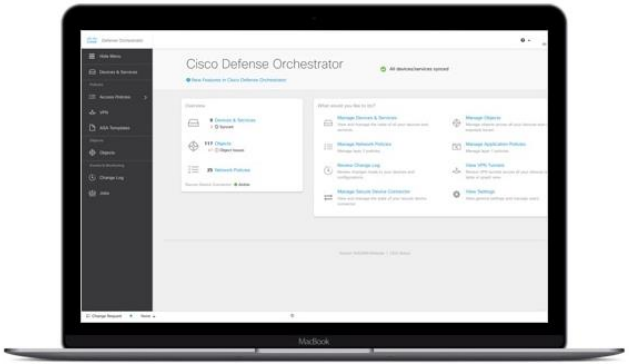


FDM



Cisco Secure Firewall Management Center :

- OnPrem (hw & virtual)
- In AWS
- Cloud-Delivered ->



CDO

# Logging and Analytics

- OnPrem (&inside *your* AWS)
  - “inside your FMC”
  - Additional Log retention via SAL onPrem available

- Cloud Delivered FMC
  - Can retain onPrem FMC for Logging & Analytics only
    (Additional Log retention via SAL onPrem available)
  - With no extra License
    - Only Security Events in SSE/Sec X/ CTR
  - License Logging&Troubleshooting
    - CDO Unified Event Viewer
    - CDO Dashboards
  - License Logging, Analytics & Detection
    - The Above + Secure Cloud Analytics applied on Firewall Logs
  - License Total Network A & D
    - The Above + Internal Network Telemetry (Local Sensors)

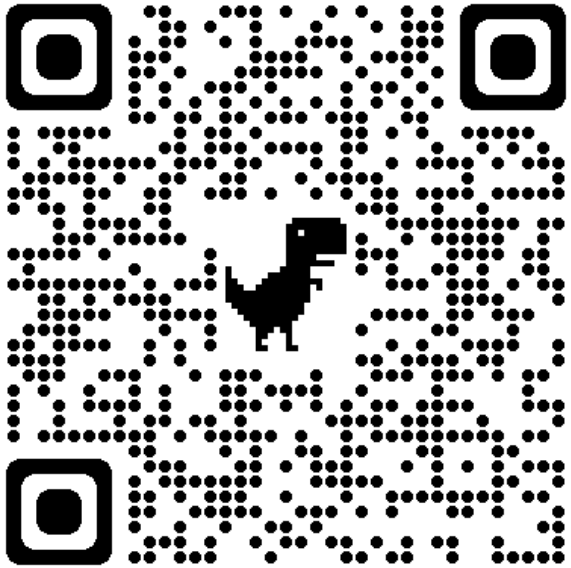
- Common
  - Syslog
  - Netflow
  - estreamer

# Question about automation ?

In AWS


Ecosystem solutions


# Better than slides...



https://developer.cisco.com/secure-firewall/cloud-resources/#directory-cisco

# Security through visibility

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

# How do we address this with Secure Workload?

Contain lateral movement

Microsegmentation

Identify behavior anomalies

**Process and communication**

Continuously track security compliance

Policy compliance

Reduce attack surface

Software vulnerability

# 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

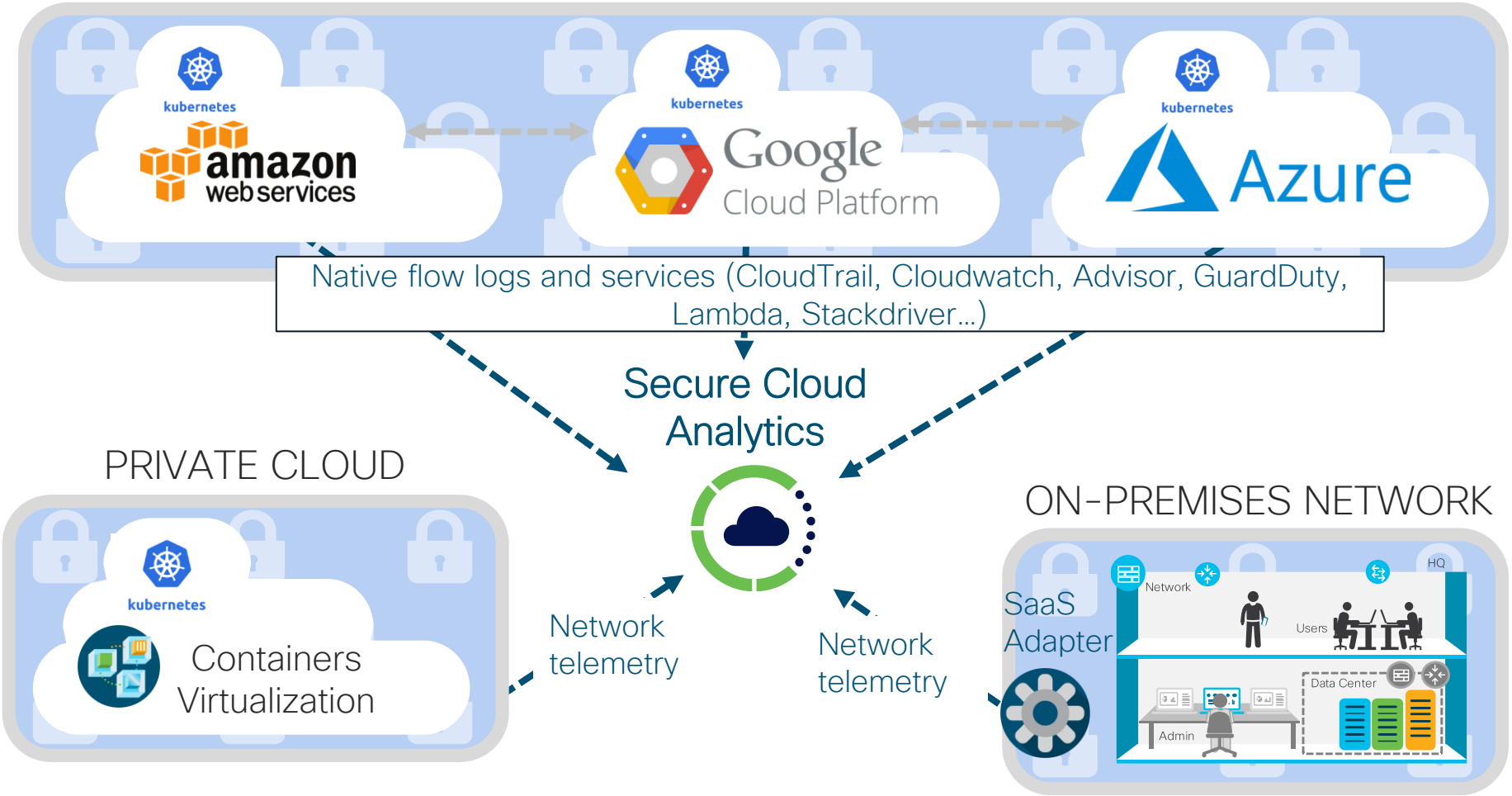
AWS Lambda

# AWS GuardDuty & Secure Cloud Analytics

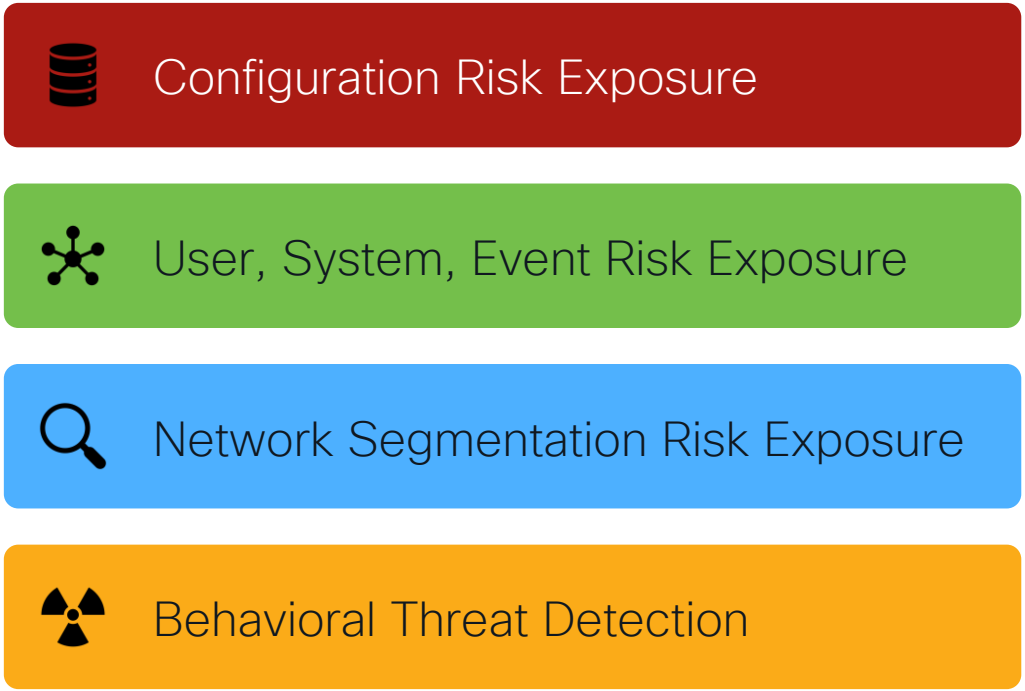
- ✓ DNS Detections with DNS logs
- ✓ Detections on EC2, S3, IAM
- ✓ Easy to activate & out-of-box detections
- ✓ Unsupervised Analytics

- ✓ 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/



# Secure Cloud Analytics Engine

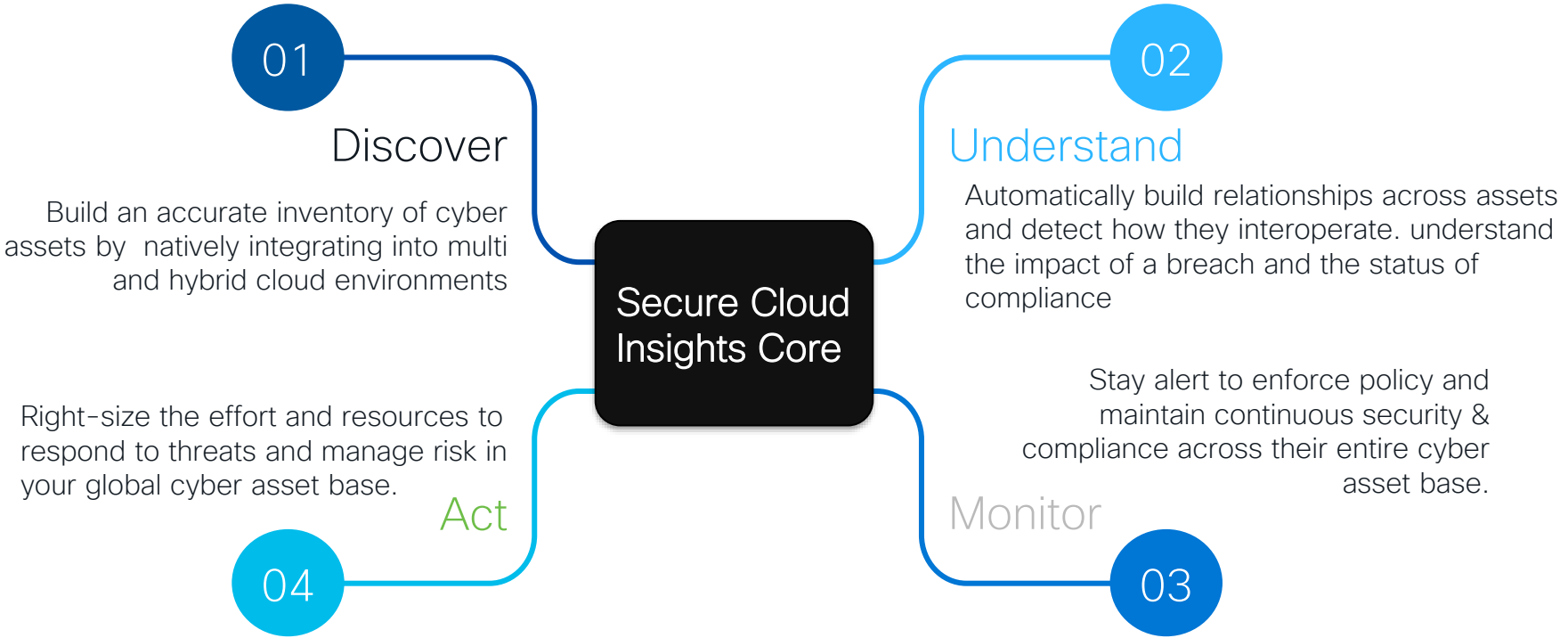



## Cloud Security Maturity

- **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?

# Cloud Insight

# Cloud Insight Use Cases



# 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

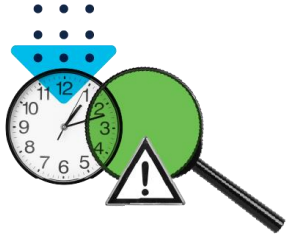
Simple evidence collection and helpful alerts to avoid compliance drift and security incidents

### 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

# 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

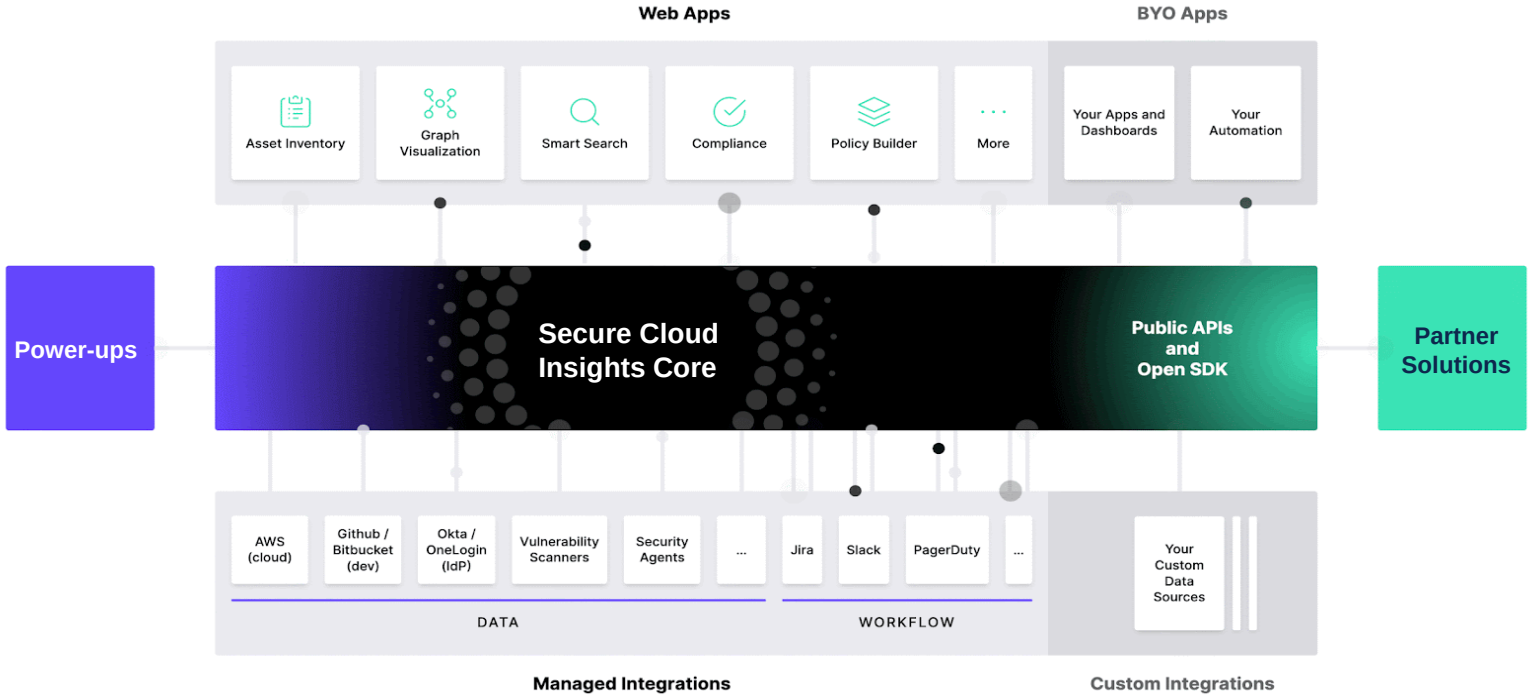
Continuous Compliance Checks
Relationship Graph Visualization

Simple Query Language
Periodic Data Polling

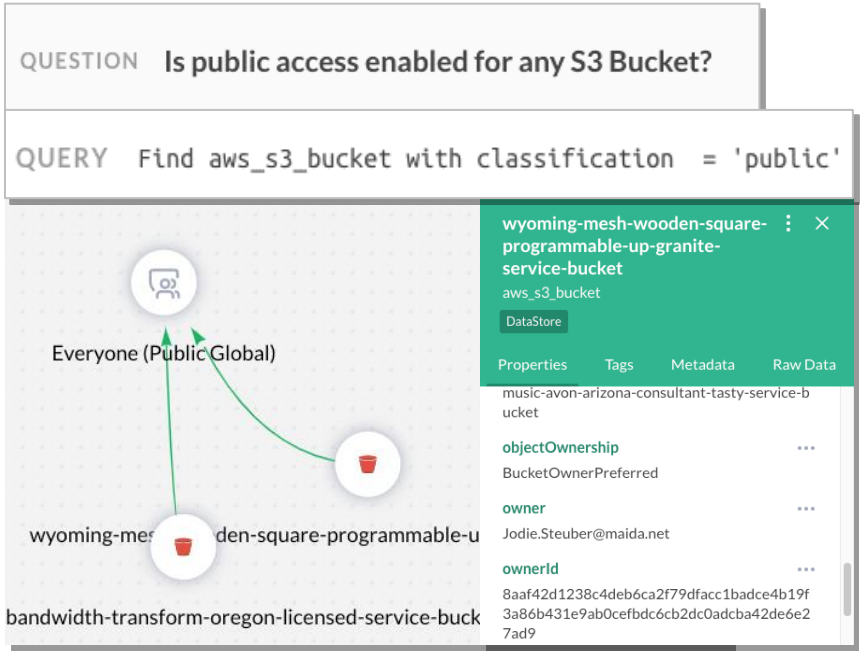
## Alert and Respond

Shares alert findings to ticketing alert correlating systems upon detection

# API First and Cloud Native

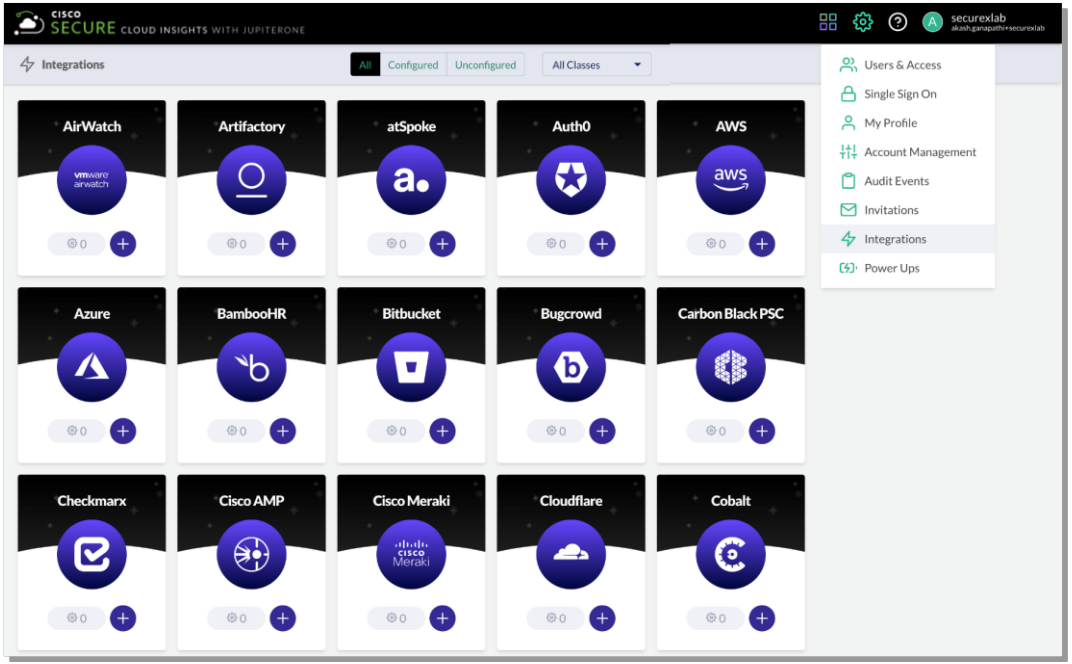


# Query Through Use Cases



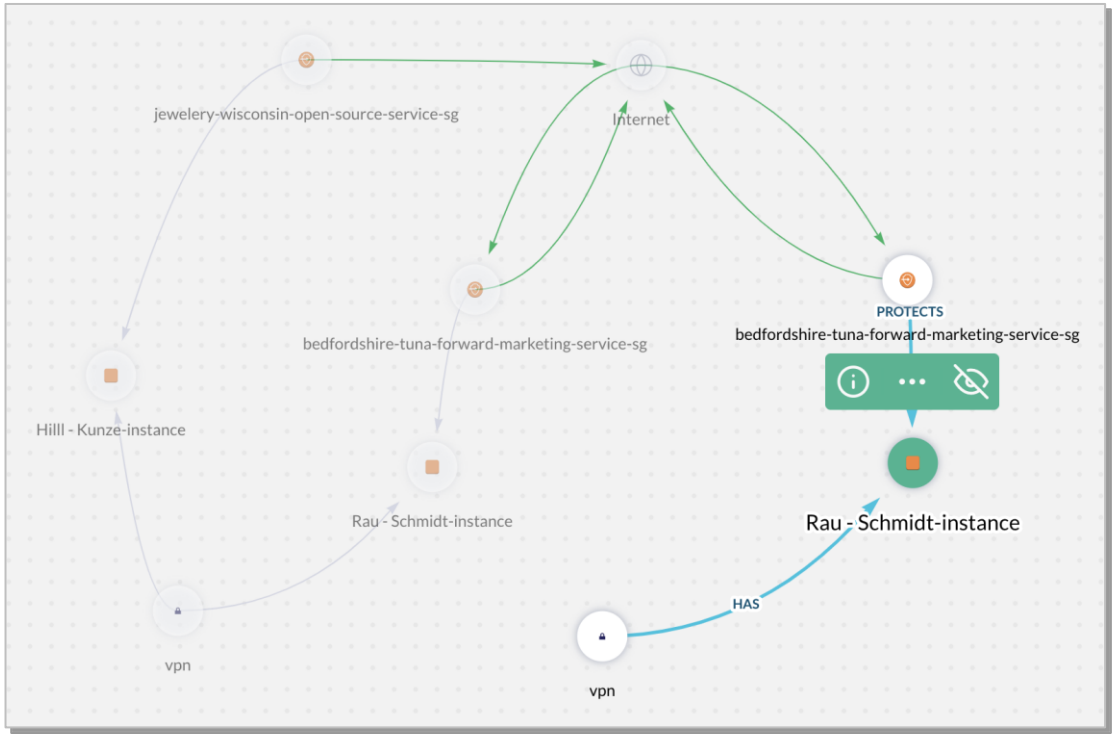

- Incident Scope and Response
- Compliance Check
- Attack Surface Management
- Configuration Change Detection

# 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

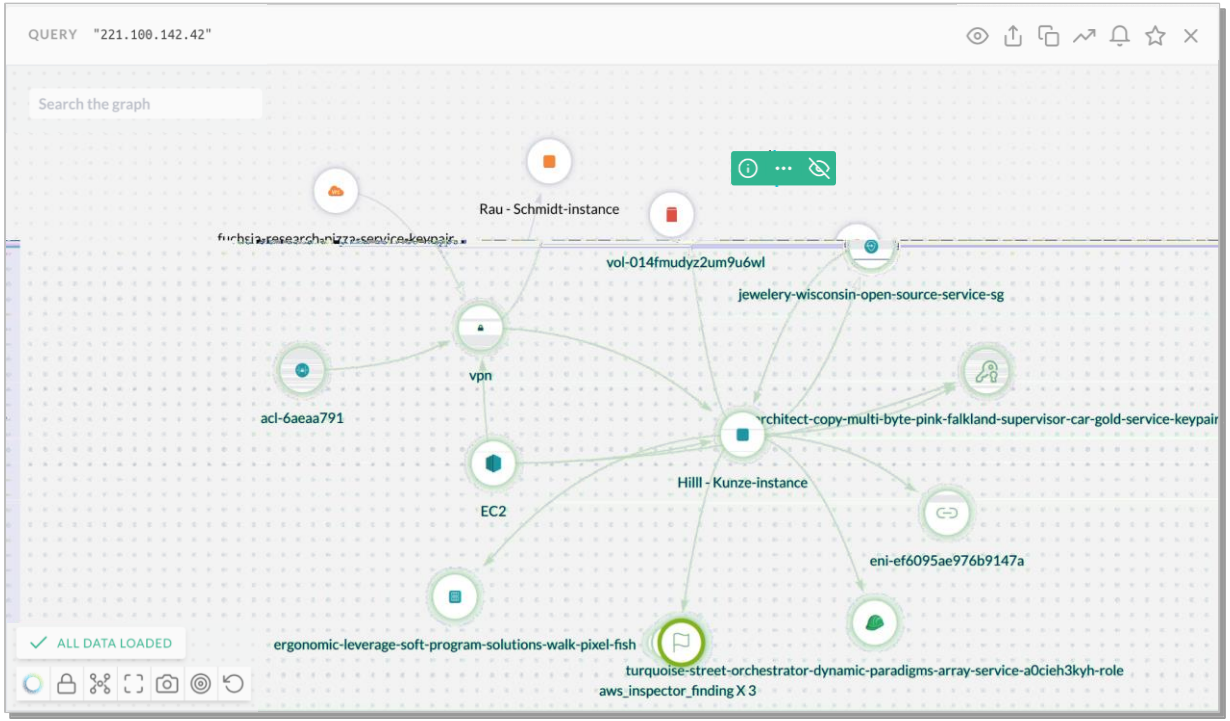
# Relationship Mapping



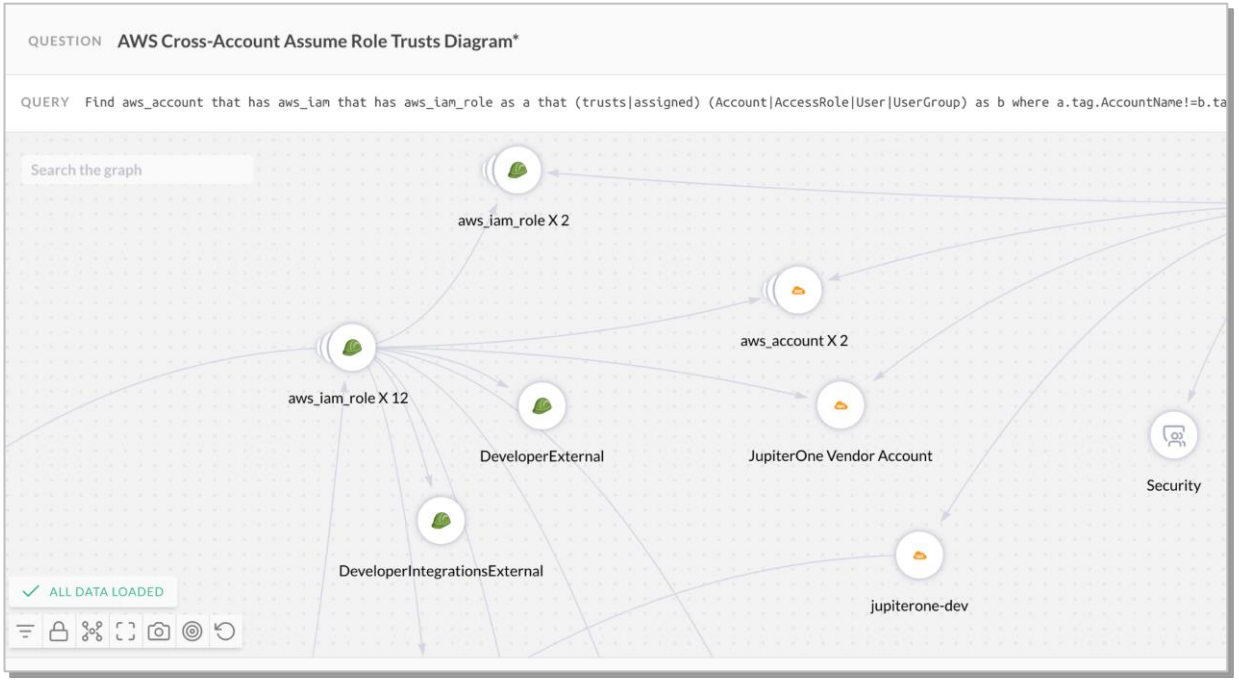

- Relationships between assets are discovered via the integrations and are mapped together automatically
- Here we see:
  - Security groups allowing access to the internet
  - The instances they protect
  - The subnets those instances are on

# 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

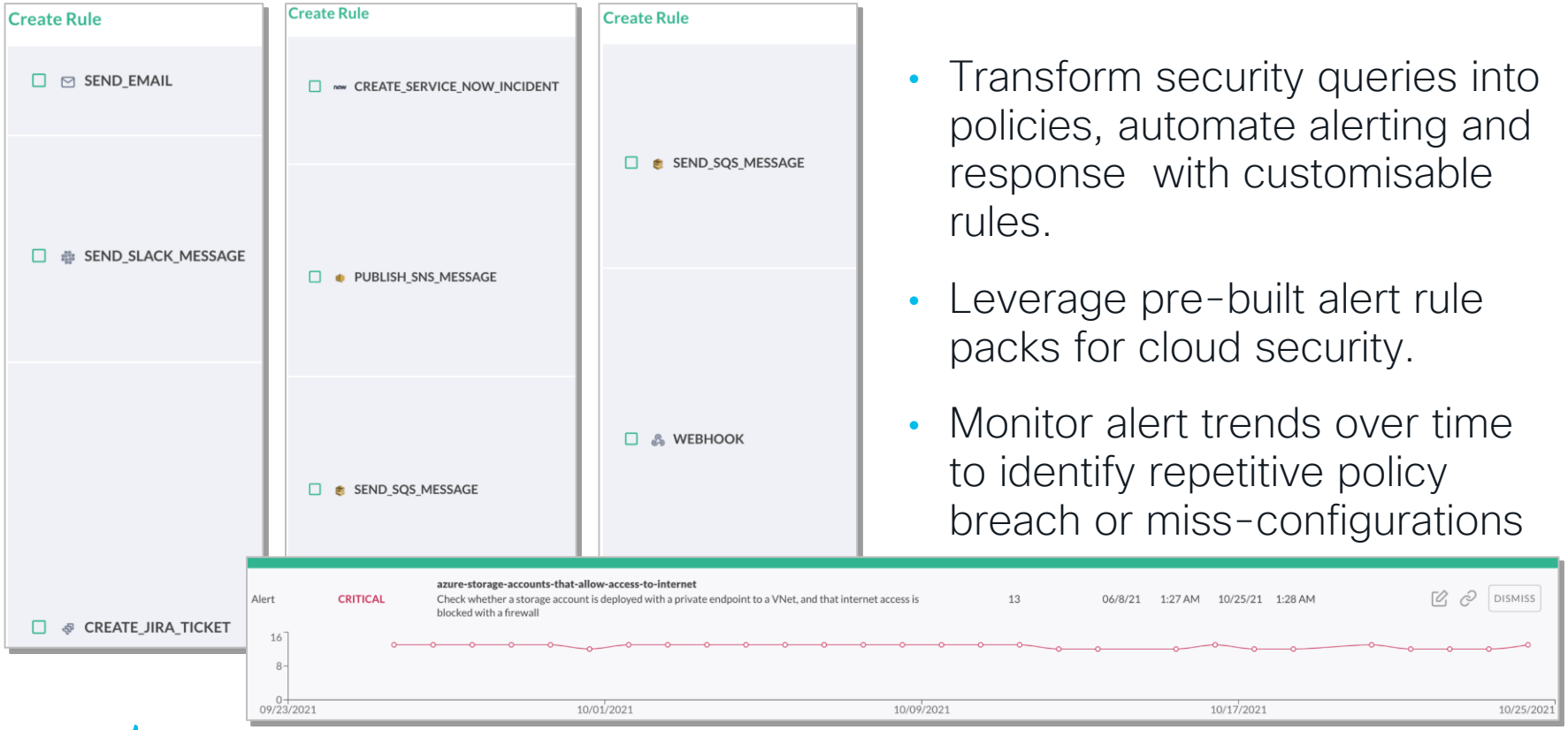


# Cross Environment investigation




- 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

# 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

# Almost finished...

# I DO VALUE YOUR COMMENTS

# Key Takeways

- Good same old challenges in Public Cloud
- Cisco has solution to enhance or complement AWS security
- It becomes even more relevant in hybrid/multi clouds

# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.


- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

# Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN