



The bridge to possible

Enhance AWS Native Security with Cisco Security

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

Cisco Webex App

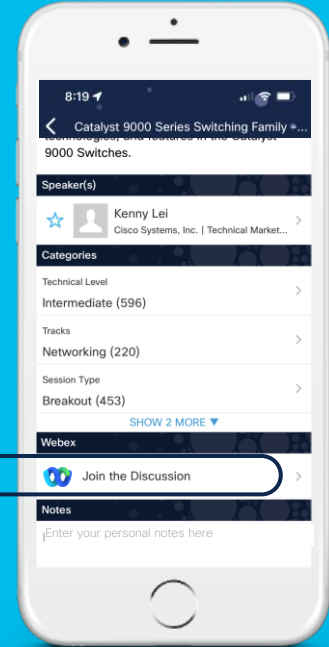
Questions?

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

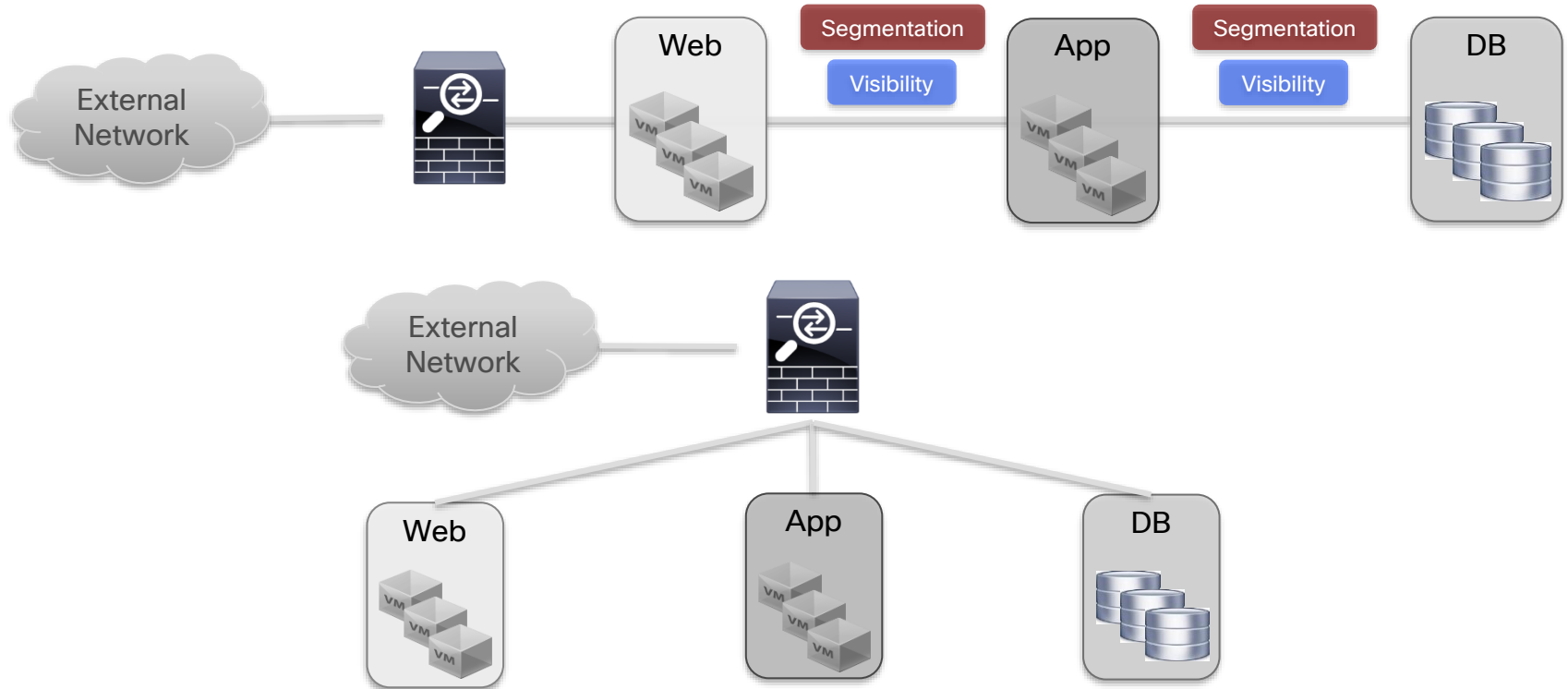
How

- 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 consistent Security



aws Services Search [Alt+S] N. Virginia

CloudFormation EC2 VPC IAM S3 Route 53 Certificate Manager CloudWatch Lambda AWS Marketplace Subscriptions

- Amazon Timestream
- DynamoDB
- Amazon MemoryDB for Redis
- Migration & Transfer**
 - AWS Migration Hub
 - AWS Application Migration Service
 - Application Discovery Service
 - Database Migration Service
 - AWS Transfer Family
 - AWS Snow Family
 - DataSync
 - AWS Mainframe Modernization
- Networking & Content Delivery**
 - VPC
 - CloudFront
 - Route 53
 - API Gateway
 - Direct Connect
 - AWS App Mesh
 - AWS Cloud Map
 - Global Accelerator
 - Route 53 Application Recovery Controller
 - AWS Private 5G
- Management & Governance**
 - AWS Organizations
 - CloudWatch
 - AWS Auto Scaling
 - CloudFormation
 - Config
 - OpsWorks
 - Service Catalog
 - Systems Manager
 - Trusted Advisor
 - Control Tower
 - AWS License Manager
 - AWS Well-Architected Tool
 - AWS Health Dashboard
 - AWS Chatbot
 - Launch Wizard
 - AWS Compute Optimizer
 - Resource Groups & Tag Editor
 - Amazon Grafana
 - Amazon Prometheus
 - AWS Resilience Hub
 - Incident Manager
 - AWS Proton
 - CloudTrail
 - AWS Resource Explorer
- Media Services**
 - Kinesis Video Streams
 - MediaConnect
 - MediaConvert
 - MediaLive
 - MediaPackage
 - MediaStore
 - MediaTailor
 - Elemental Appliances & Software
 - Elastic Transcoder
 - Nimble Studio
 - Amazon Interactive Video Service
- Security, Identity, & Compliance**
 - IAM
 - Resource Access Manager
 - Cognito
 - Secrets Manager
 - GuardDuty
 - Amazon Inspector
 - Amazon Macie
 - IAM Identity Center (successor to AWS Single Sign-On)
 - Certificate Manager
 - Key Management Service
 - CloudHSM
 - Directory Service
 - WAF & Shield
 - AWS Firewall Manager
 - AWS Artifact
 - Security Hub
 - Detective
 - AWS Signer
 - AWS Private Certificate Authority
 - AWS Audit Manager
 - Security Lake
 - Amazon Verified Permissions
- Kinesis
- QuickSight
- Data Pipeline
- AWS Data Exchange
- AWS Lake Formation
- MSK
- AWS Glue DataBrew
- Amazon FinSpace
- AWS Glue
- AWS Glue Data Catalog
- Amazon WorkMail
- Alexa for Business
- AWS Wickr
- Amazon Chime SDK
- End User Computing**
 - WorkSpaces
 - AppStream 2.0
 - WorkSpaces Web
- Internet of Things**
 - IoT Core
 - FreeRTOS
 - IoT 1-Click
 - IoT Analytics
 - IoT Device Defender
 - IoT Device Management
 - IoT Greengrass
 - IoT SiteWise
 - IoT Events
 - AWS IoT FleetWise
 - IoT RoboRunner
 - IoT TwinMaker
- Game Development**
 - Amazon GameLift
 - Amazon GameSparks

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

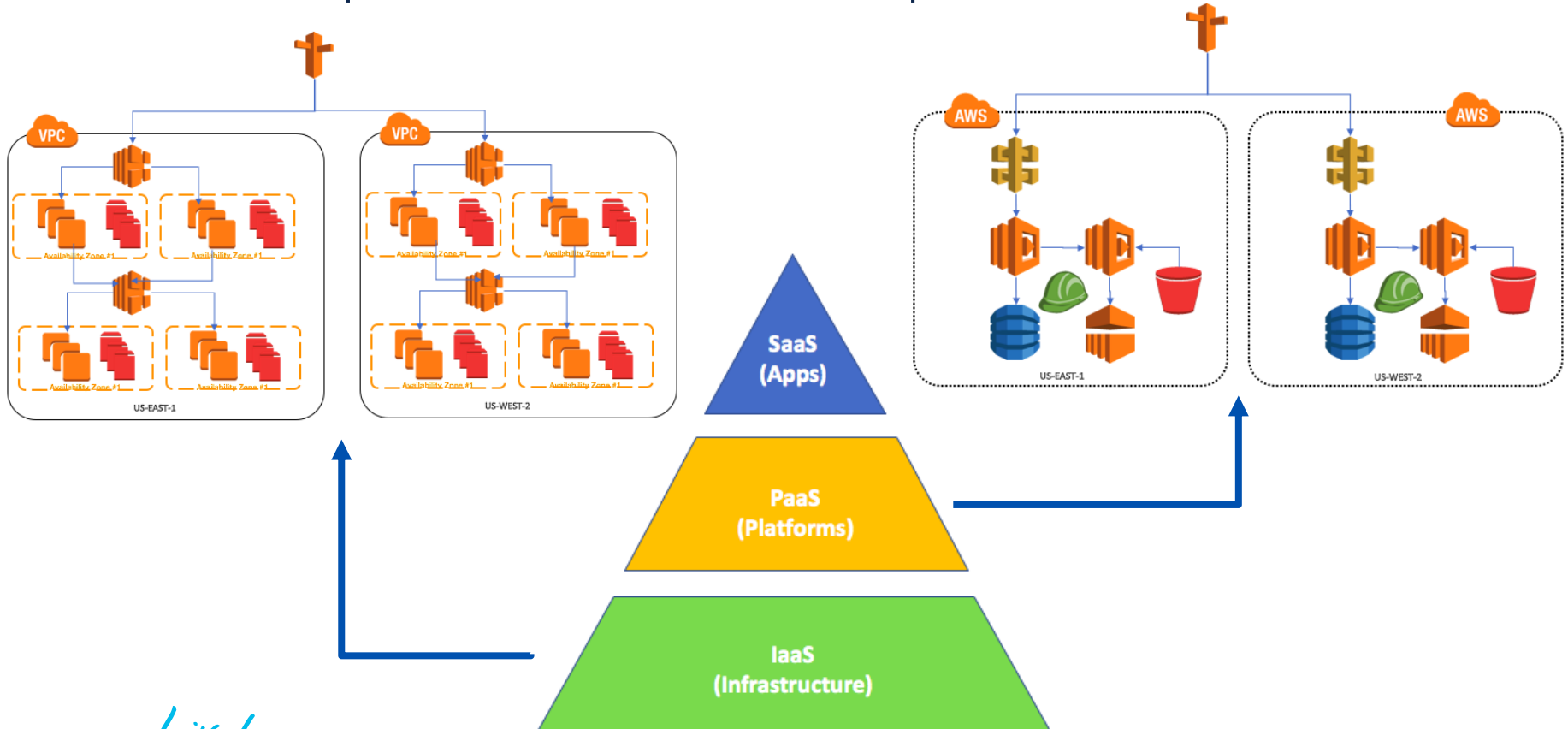


What type of service and architecture to deploy my application ?

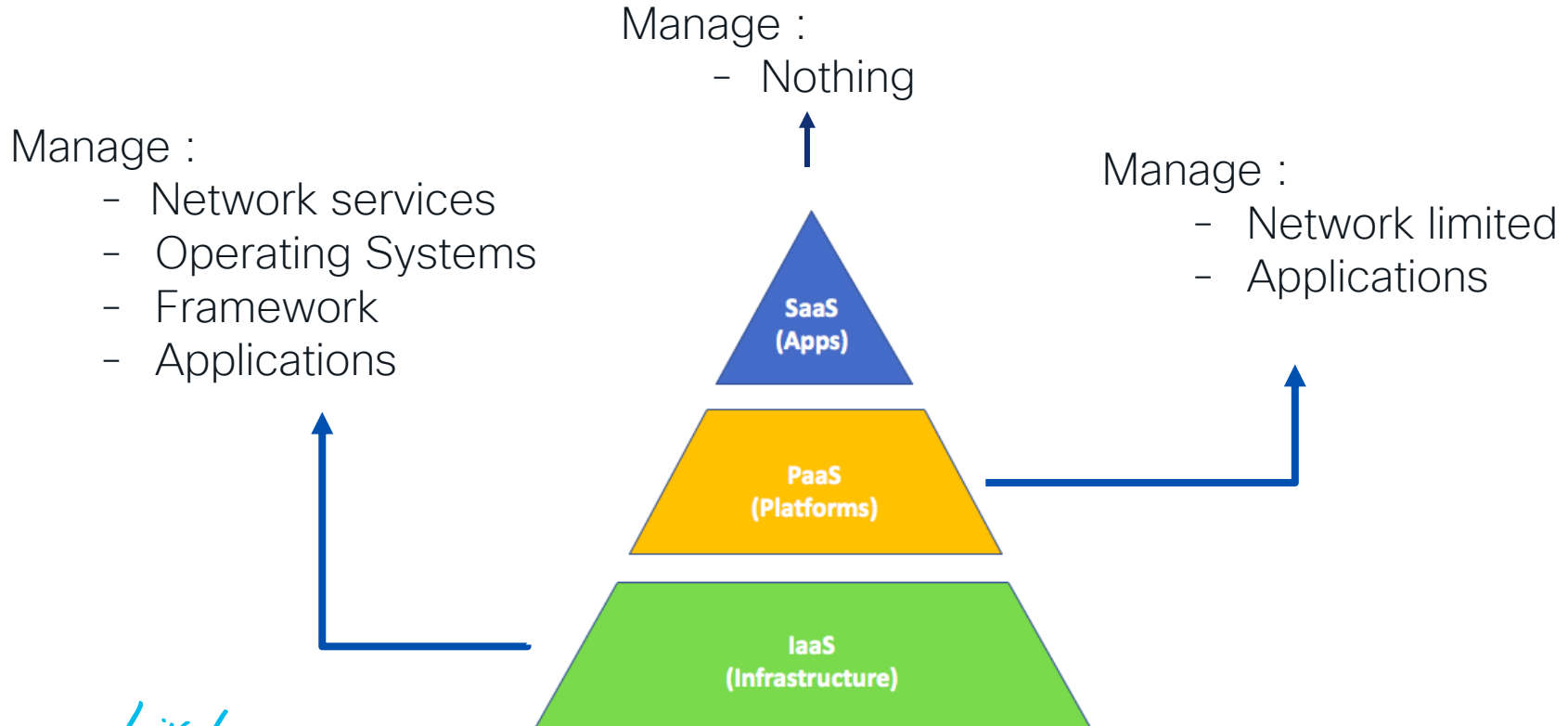
- Infrastructure as a Service
- Platform as a Service
- Serverless



IaaS compared to PaaS Compared to SaaS



IaaS compared to PaaS Compared to SaaS



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	Cloud Service Provider Responsible
Runtime	Runtime	Runtime	Runtime	Runtime	Runtime	
Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Customer Responsible
Operating System	Operating System	Operating System	Operating System	Operating System	Operating System	
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Customer and Cloud Service Provider have Shared Responsibility
Servers	Servers	Servers	Servers	Servers	Servers	
Storage	Storage	Storage	Storage	Storage	Storage	
Networking	Networking	Networking	Networking	Networking	Networking	

Securing the Cloud

Network Segmentation



Visibility & Threat
Detection

Cloud Security Posture Management

Identity

FabAstro Application in AWS



Amazon S3



AWS
Route 53



AWS Certificate Manager

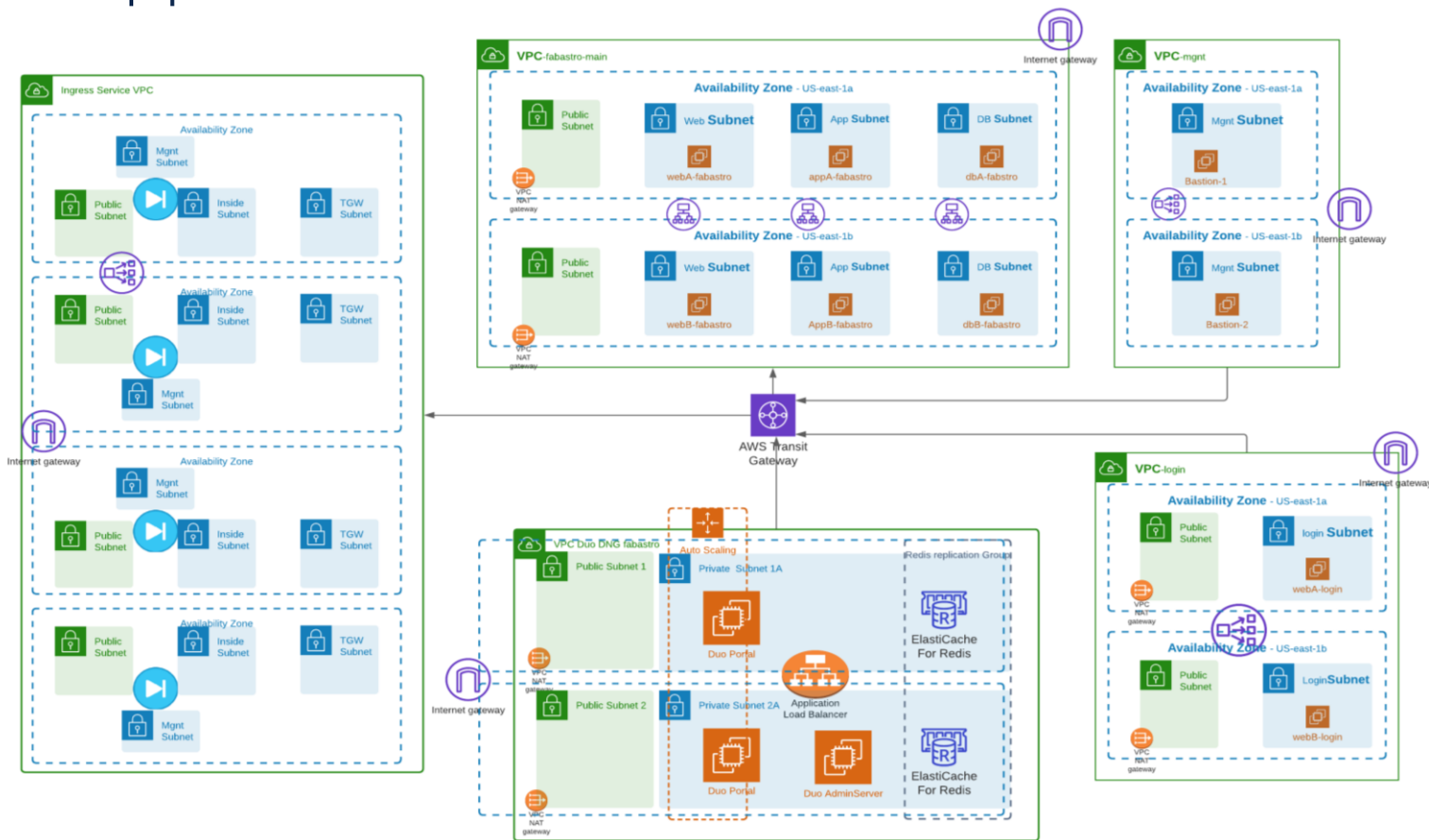


AWS
CloudFormation



AWS IAM

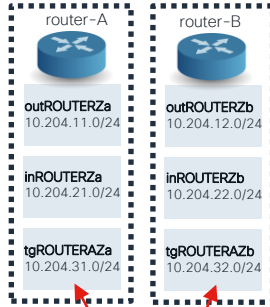
CISCO *Live!*





VpcClusterVPNrouters

10.204.0.0/16



IGClusterRAVPN



VpcClusterRAVPN

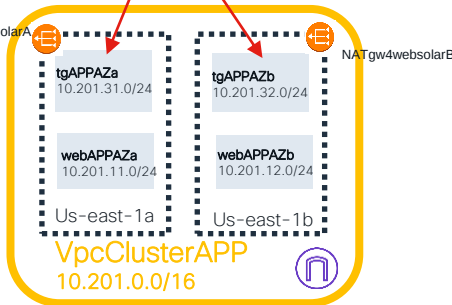
10.200.0.0/16

Remote
User

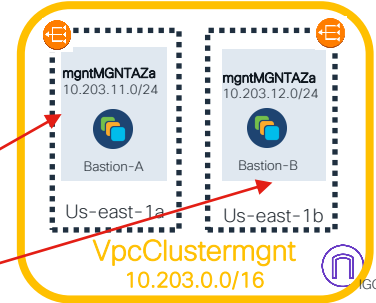
TransitGatewaySolar

NATgw4websolarA

NATgw4websolarB

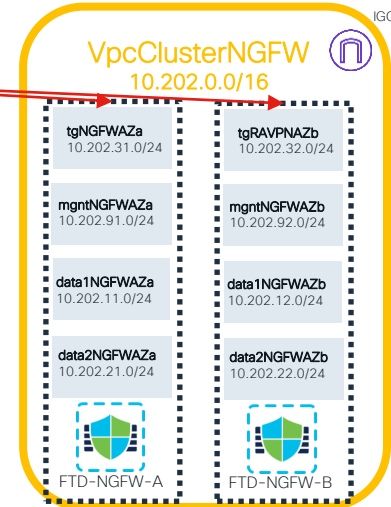


IGClusterAPP



IGClusterAPP

IGClusterNGFW



First Step in AWS...

IAM, EC2 and VPC



AAA with AWS

Authenticate

IAM Username/Password
Access Key
(+ MFA)
Federation

Authorize

IAM Policies

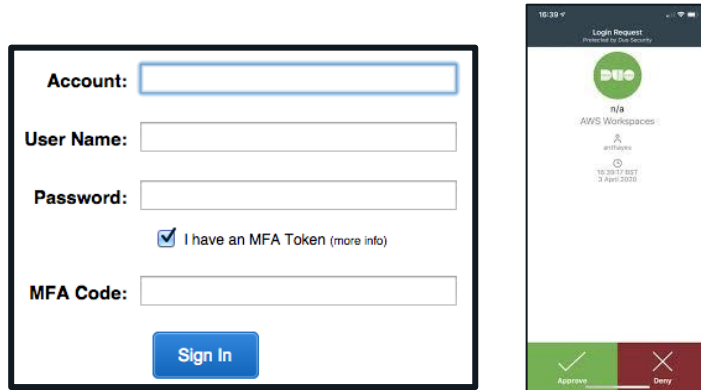
Audit

CloudTrail

AWS Identity Authentication

AWS Management Console

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



The image shows two side-by-side screenshots. The left screenshot is the AWS Management Console login page, featuring fields for 'Account:', 'User Name:', 'Password:', and 'MFA Code:'. There is a checkbox labeled 'I have an MFA Token (more info)' and a 'Sign In' button at the bottom. The right screenshot is a mobile MFA device screen showing a 'Login Request' from 'AWS Workspaces' with a green checkmark and a 'Deny' button.

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

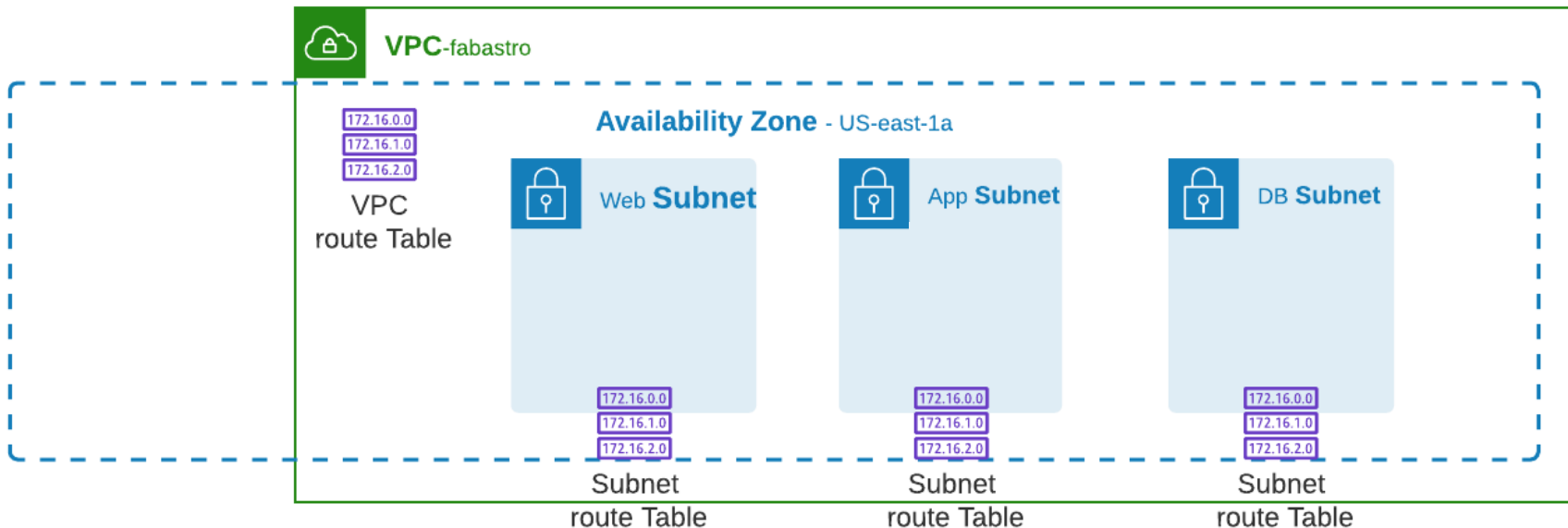
Ex: AKIAIOSFODNN7EXAMPLE

SECRET KEY

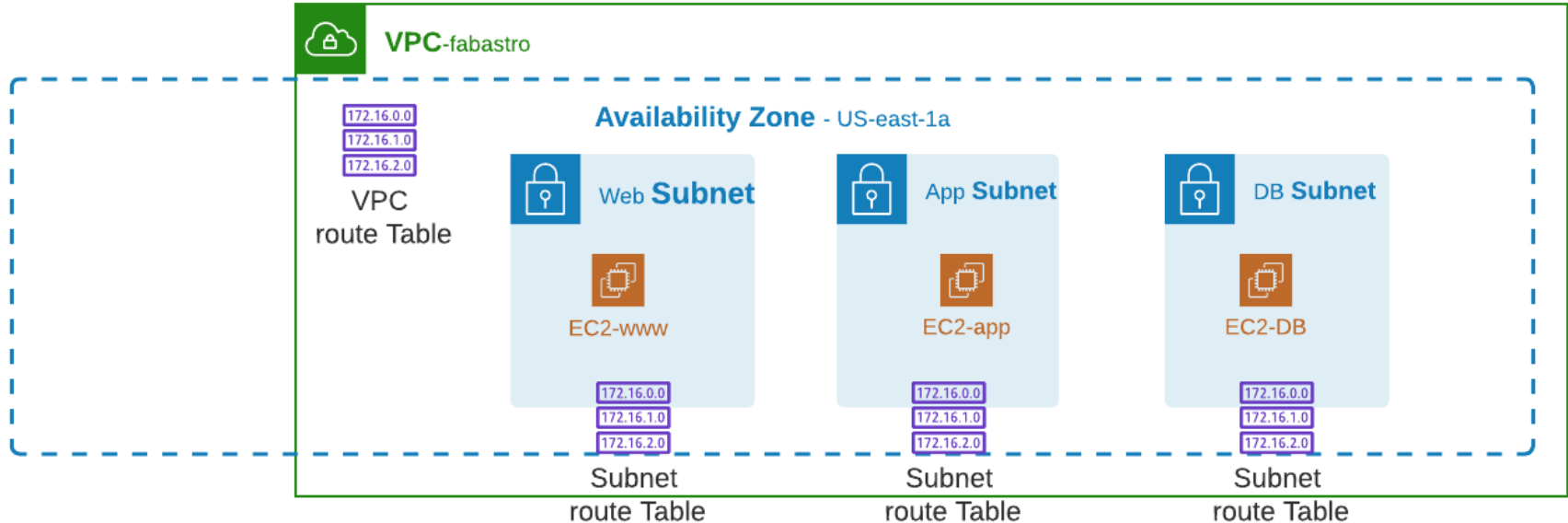
Ex: UtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY

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

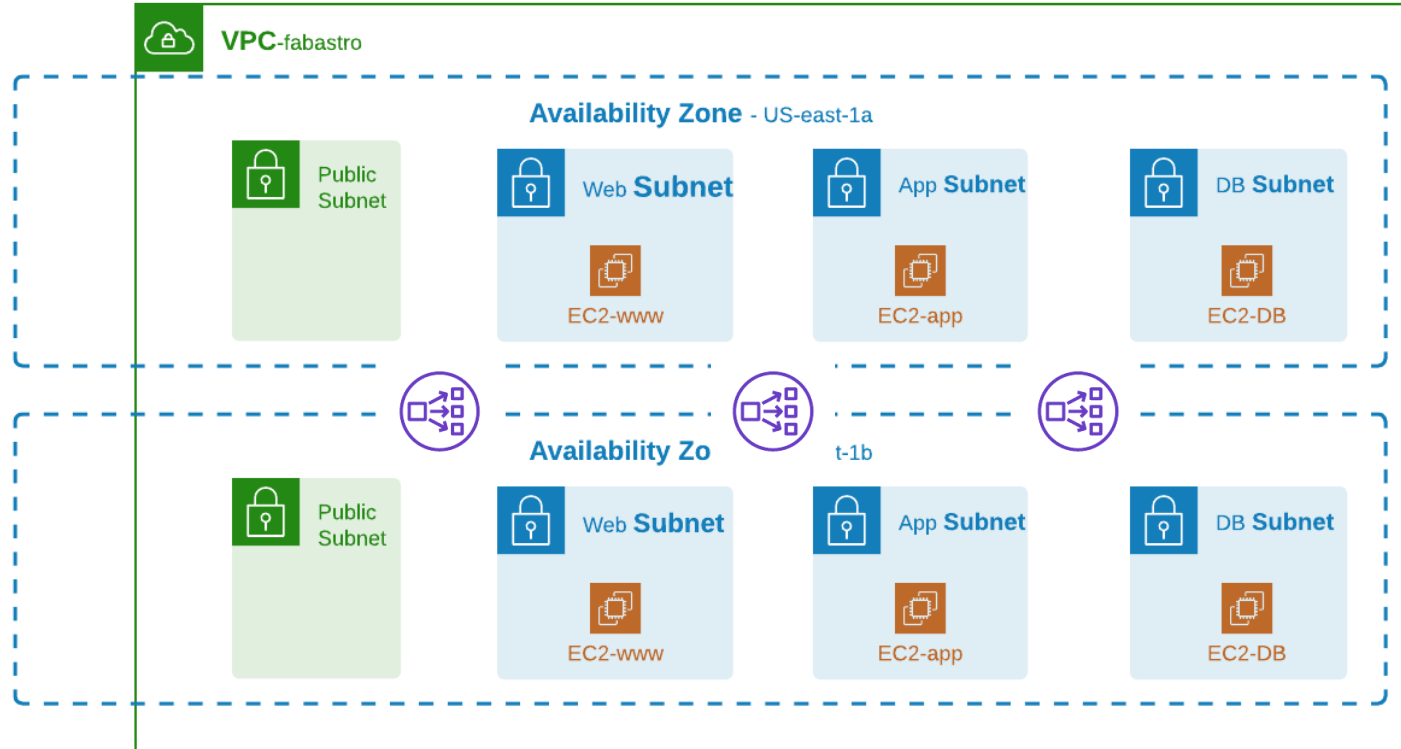
My VRF... VPC sort of (actually Route Tables)



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 ?

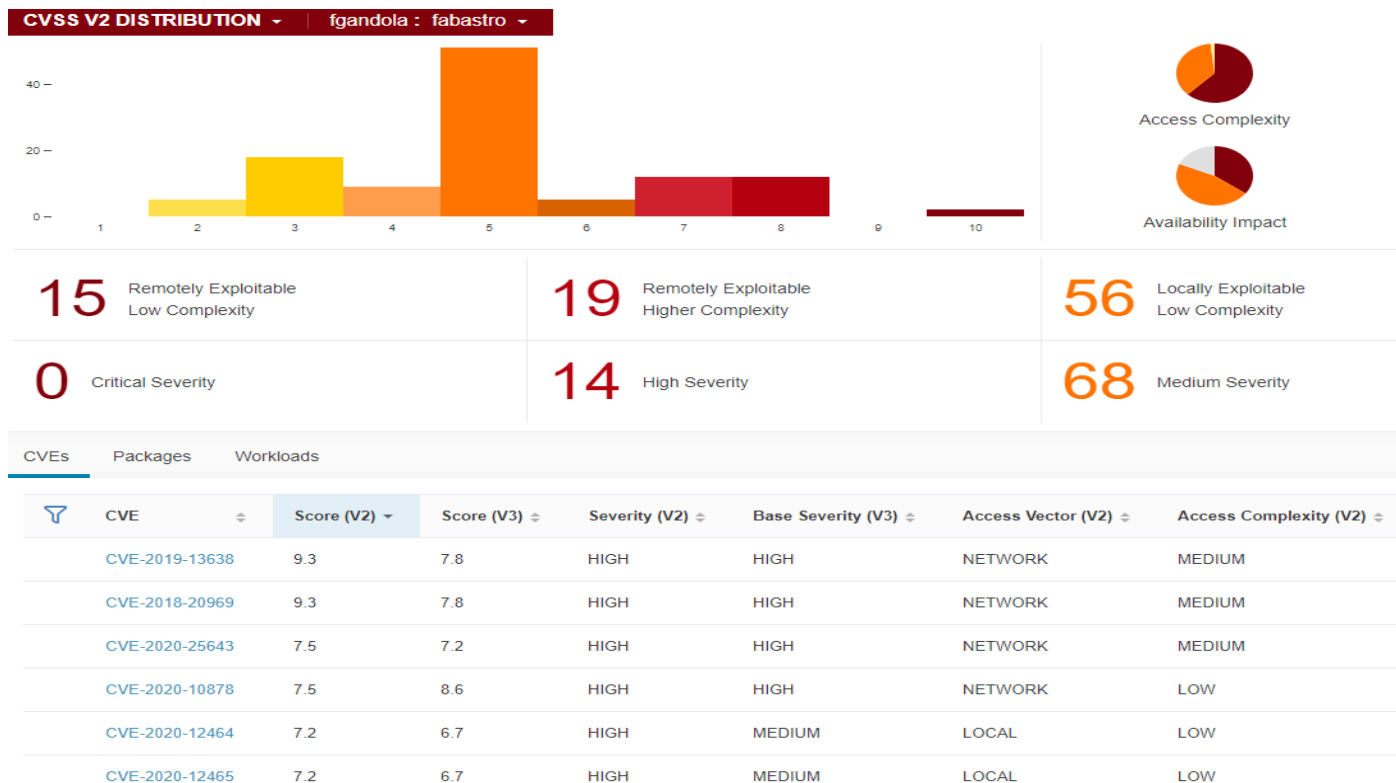
Stealthwatch Cloud has discovered [1 new or updated alert](#) on your network since our last email to you. We have included the

Alert	Source	Time	Description
Inbound Port Scanner	Network	Nov. 27, 2020, 10:19 a.m.	Device was port scanned by an external device. 1

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

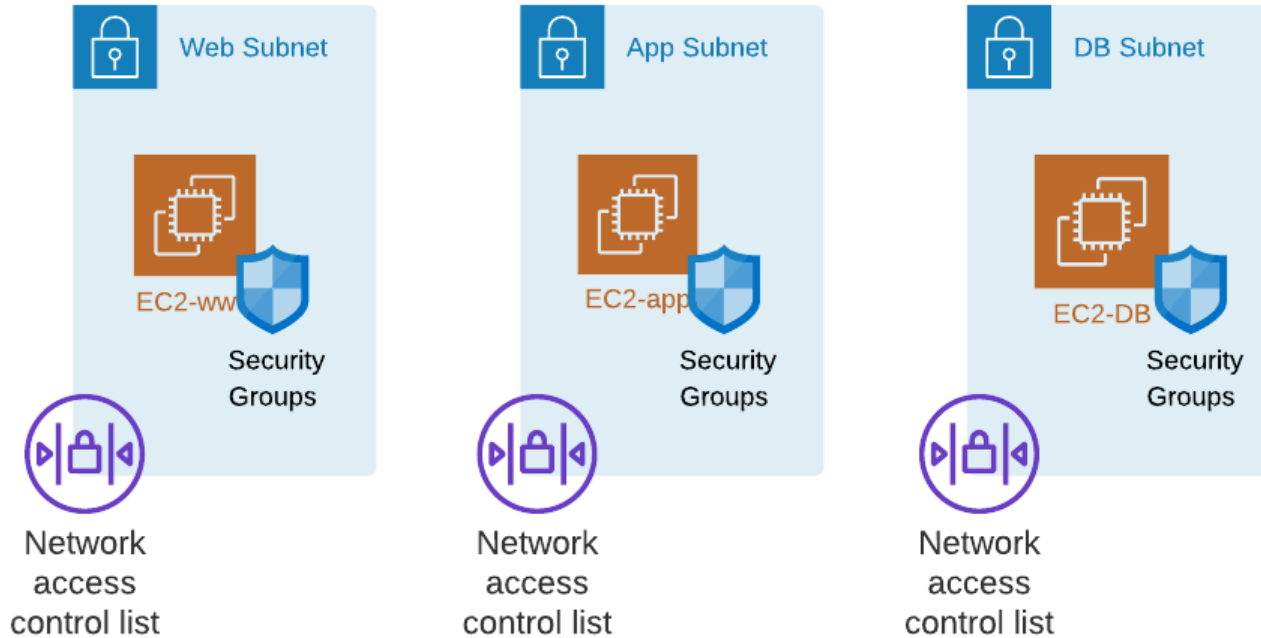
Alert	Source	Time	Description
Persistent Remote Control Connections	bastion1	Nov. 26, 2020, 11:59 p.m.	Device is receiving persistent connections from a new host observations and may indicate that a firewall rule or ACL is

CSW Vulnerability Assessment



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

Use security group as Source within VPC

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info		
sgr-0e10062e4544d68b7	SSH ▼	TCP	22	Custom ▼	93.6.40.55/32		Delete
-	All ICMP - IPv4 ▼	ICMP	All	Custom ▼	sg-0348c8d389e1ad1bd		Delete

Security Groups in CDO

Defense Orchestrator

Hide Menu

Devices & Services

Configuration

Policies

Objects

VPN

Migrations **BETA**

Events & Monitoring

Monitoring

Change Log

Jobs

AWS VPC Policies / vpc-04b371a1092d670f9 (fabastro-main)

Return to Devices & Services

Packets → Security Groups

Y

Grid

Search

default

Direction	Name	Action	Source	Destination
Inbound	default_inbound_1	Allow	SECURITY GROUPS default	Any
Outbound	default_outbound_1	Allow	Any	NETS Any IPv4

fabastro-appmainlbSG-16G8BP82C365Q

Direction	Name	Action	Source	Destination
Inbound	fabastro-appmainlbSG-16G8B...	Allow	NETS 10.67.21.0/24	PORTS TCP:80
Inbound	fabastro-appmainlbSG-16G8B...	Allow	NETS 10.67.22.0/24	PORTS TCP:80
Inbound	fabastro-appmainlbSG-16G8B...	Allow	NETS 10.67.22.0/24	PORTS TCP:443
Inbound	fabastro-appmainlbSG-16G8B...	Allow	NETS 10.67.21.0/24	PORTS TCP:443
Outbound	fabastro-appmainlbSG-16G8B...	Allow	Any	NETS Any IPv4

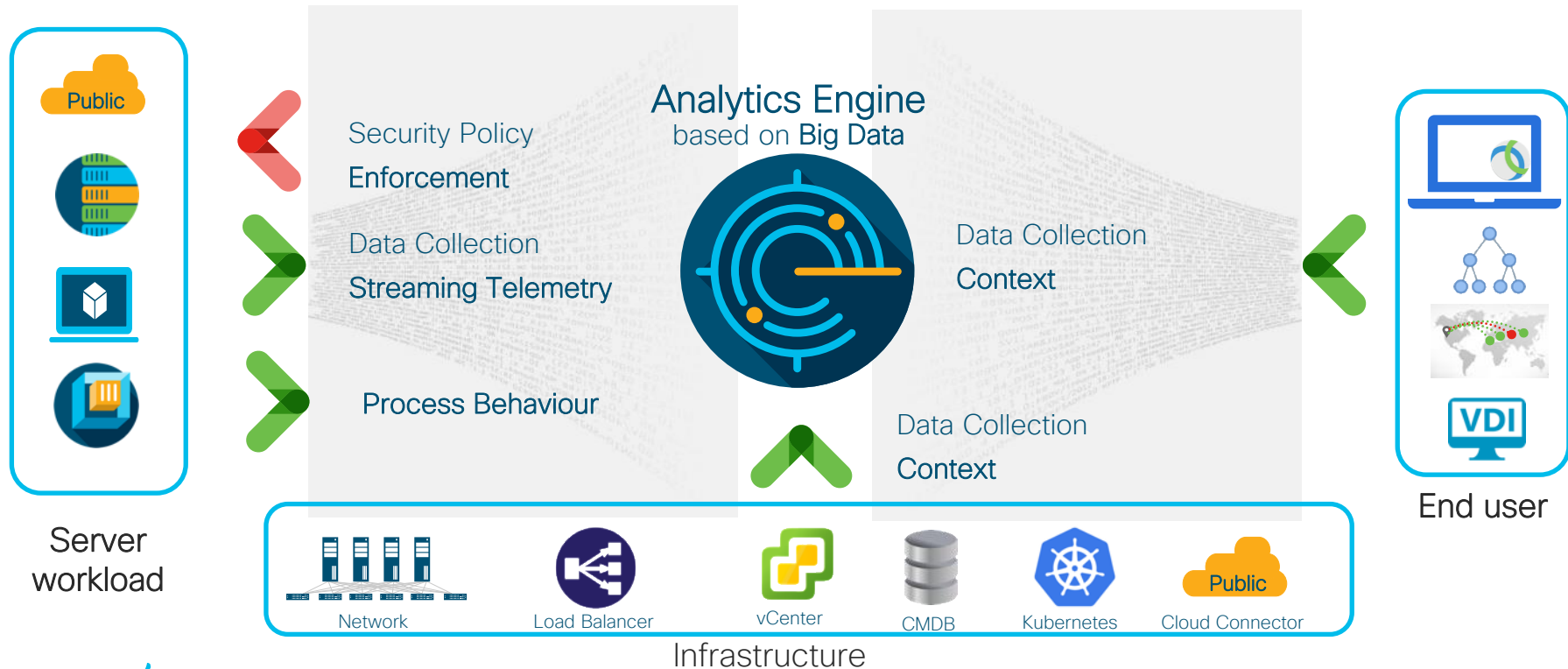
Quick Overview

- EC2
- VPC
- S3
- IAM
- Cloudformation
- Network ACL
- Use security group

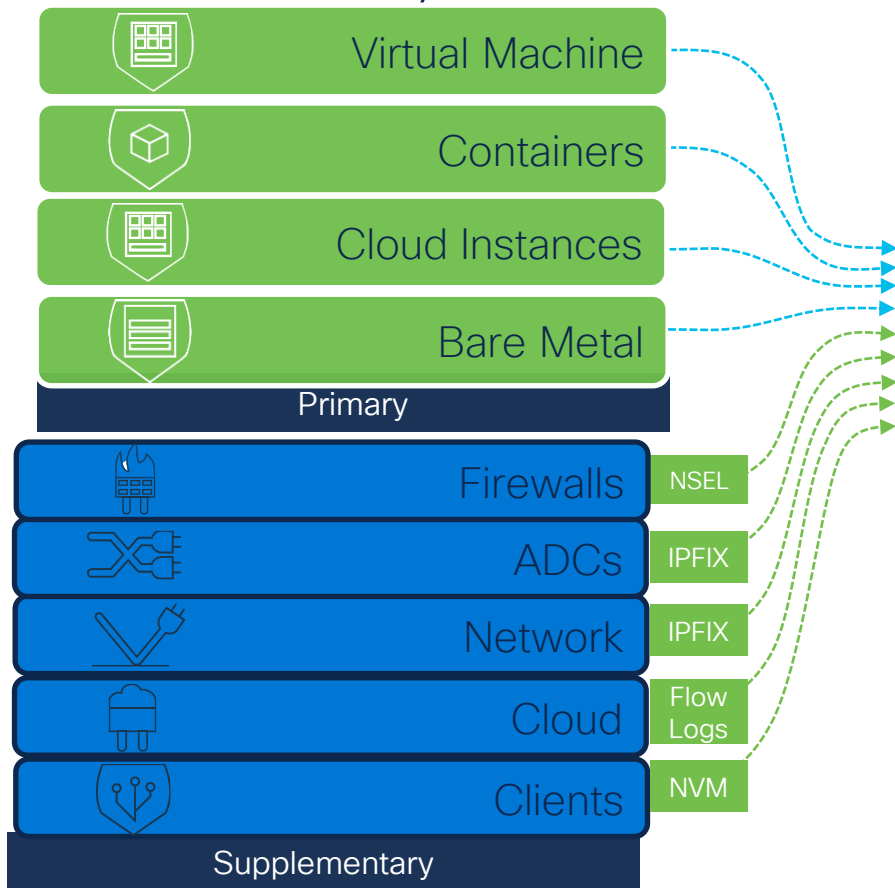
How do we address this with Secure Workload?



Secure Workload Architecture

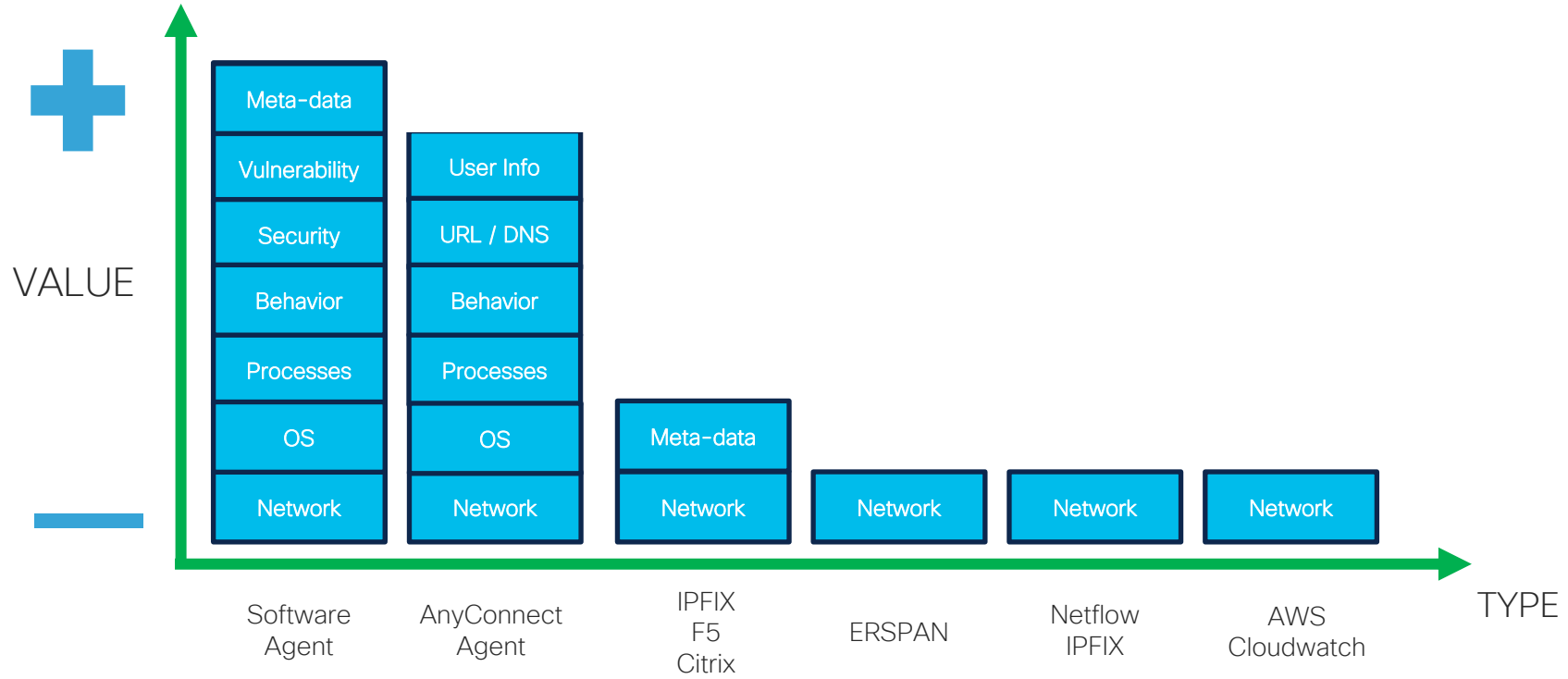


Rich visibility and workload behavior baseline



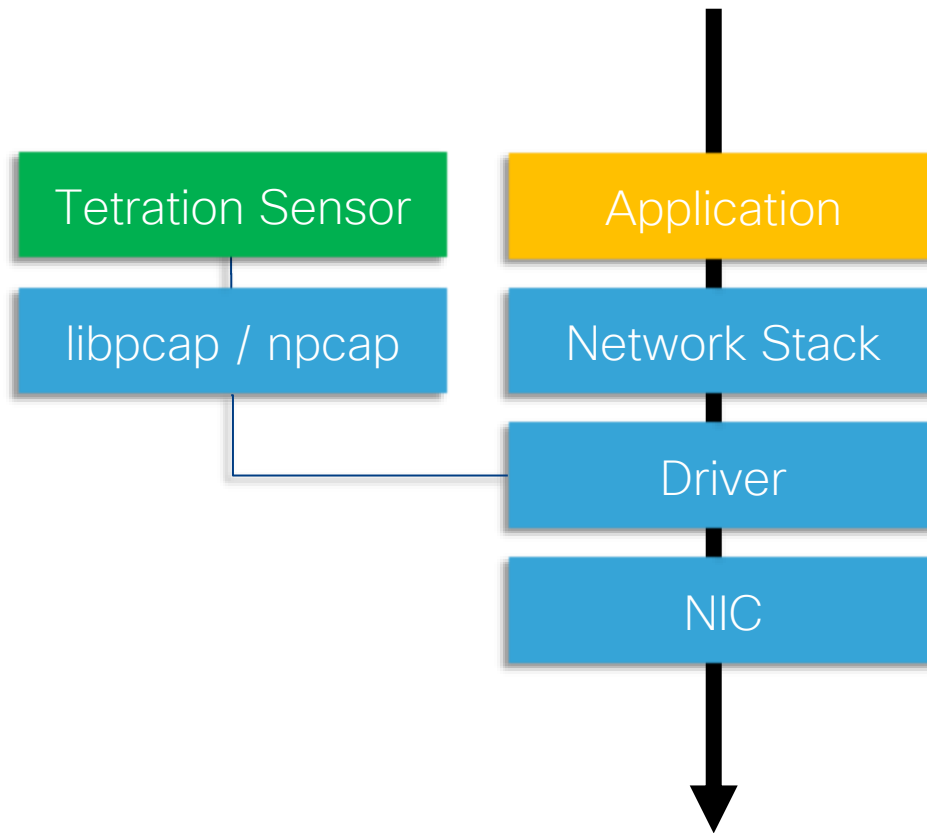
- Visibility of all communications
- Detailed machine/process info
- Any environment, any cloud
- Construct inventory of every endpoint

Different Data Sources provide different value



Software sensors

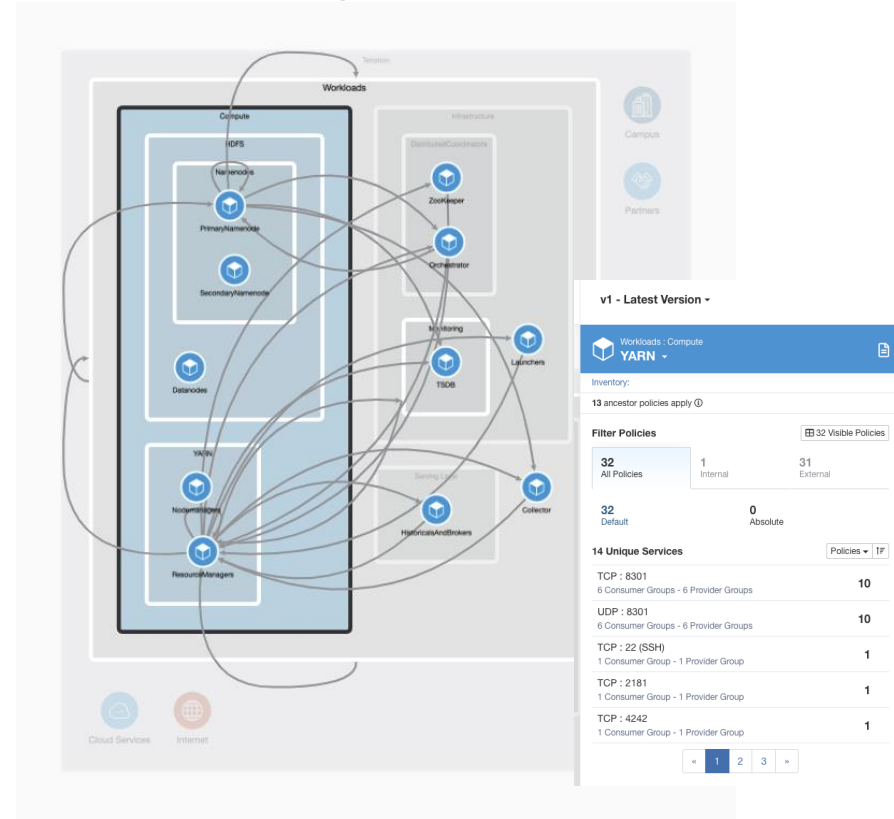
1. Minimum impact
 - Sits in User Space
 - Low CPU (< 3%)
 - Designed by Kernel Developers
2. Secure
 - Code Signed
3. Internal SLA enforcement with smart QoS
 - CPU protection
4. No latency effect



Relationship among application components

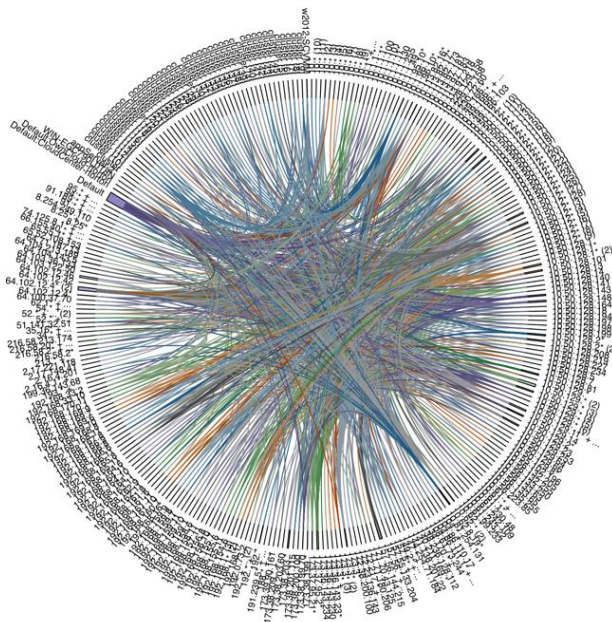
Secure Workload provides the blueprint for communication dependencies between application components as well as other IT services

- 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?

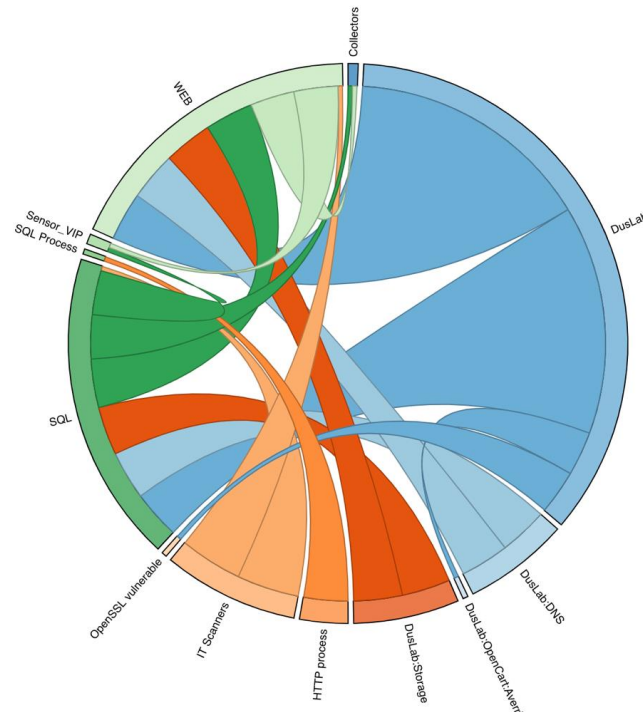


Application Dependency Mapping

Artificial Intelligence & Machine Learning

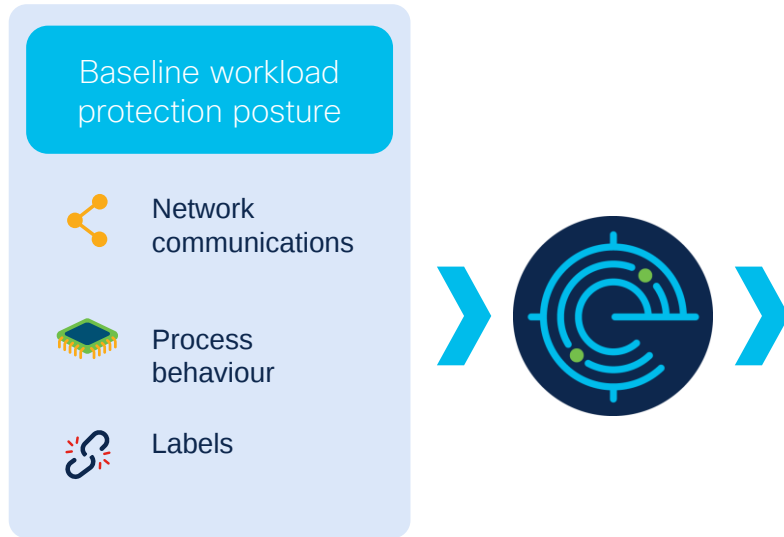


Unfiltered data collection results



Application Dependency Map provided by ML & AI

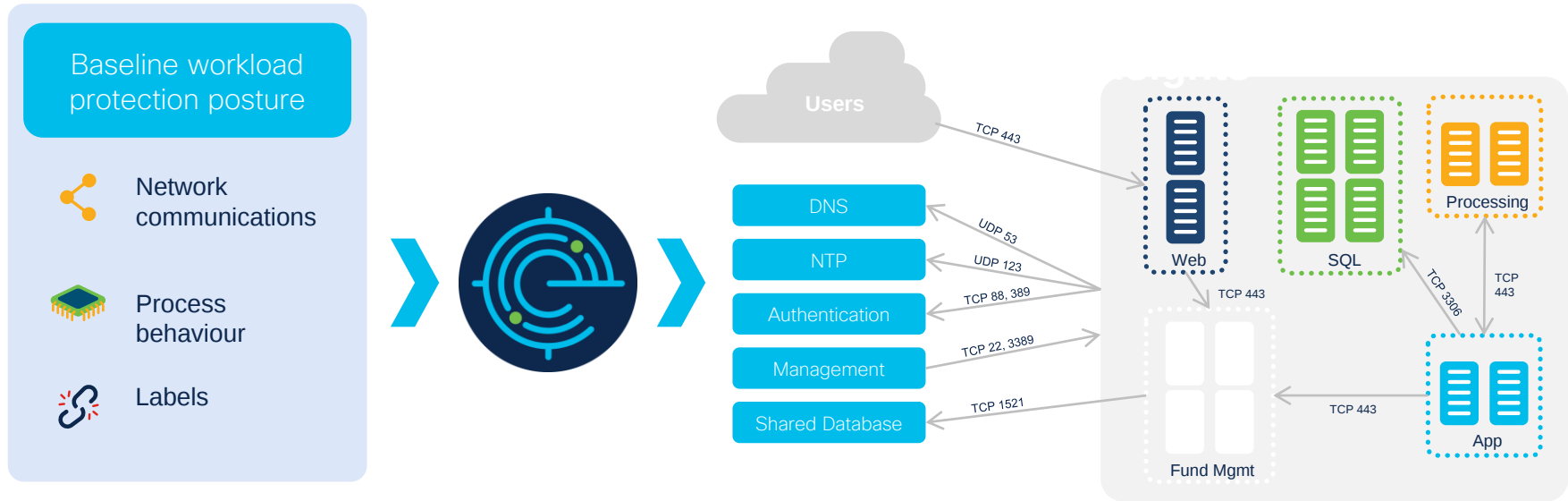
Automated Application Policy Discovery



Automated Application Policy Discovery



Automated Application Policy Discovery



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

Advanced Configurations

Side Information ?

SLB Config ?

Select a source for this side information

Route Tags ?

Select a source for this side information

Cluster Granularity

VERY FINE

Port Generalization

AGGRESSIVE

Policy Compression

MODERATE

☐ Auto accept outgoing policy connectors ?

☒ Ignore flows matching any of the [Exclusion Filters](#) ?

☒ Ignore flows matching any of the [Default Exclusion Filters](#) ?

☒ Enable service discovery on agent ?

☒ Carry over approved policies ?

☐ Skip clustering and only generate policies ?

☐ Deep policy generation ? **BETA**

Clustering Algorithm

Flows

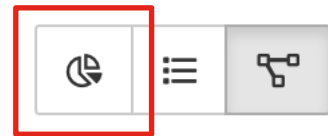
Processes

Flows and Processes

Submit ADM Run

Auto-generated Policies

Initial Relational Graph



Cisco Secure Workload

Switch Application
Start ADM Run
Policy Analysis
Enforcement

opencart PRIMARY

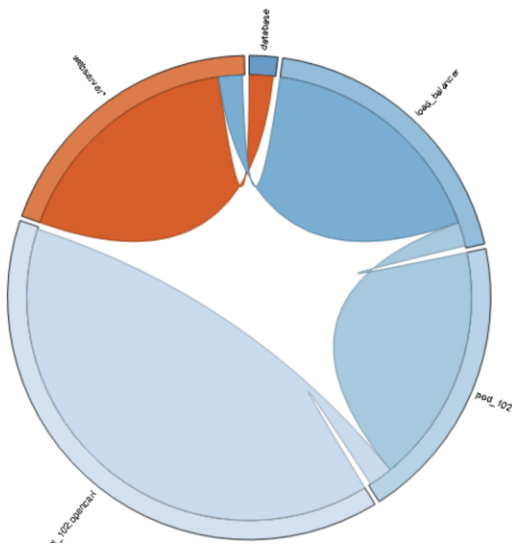
pod_102: opencart Version: v1 Last Run: 9:28 AM

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



Quick Analysis

Filter chart...



Search icon and close button.

Scope **opencart**

Full Name pod_102:opencart

Primary App opencart

Query * Application-Name contains opencart

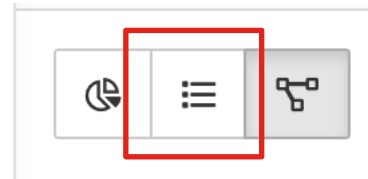
[View Scope Details](#)

> Workloads 4

> IP Addresses 0

Auto-generated policies

Policy list view



Cisco Secure Workload

Switch Application Start ADM Run Policy Analysis Enforcement

opencart PRIMARY

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

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

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

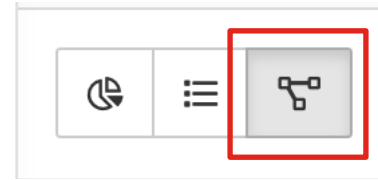
View Scope Details

> Workloads 4

> IP Addresses 0

Auto-generated policies

Canvas App view



Cisco Secure Workload

SEARCH USER | CISCO SECURE

opencart PRIMARY

↑ Switch Application

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

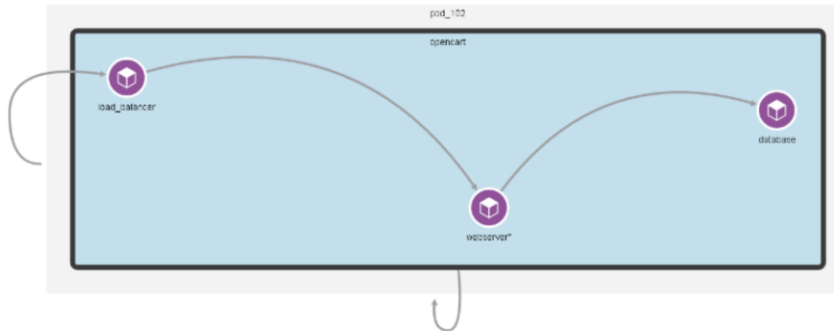
▶ Start ADM Run

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

Policy Analysis Enforcement

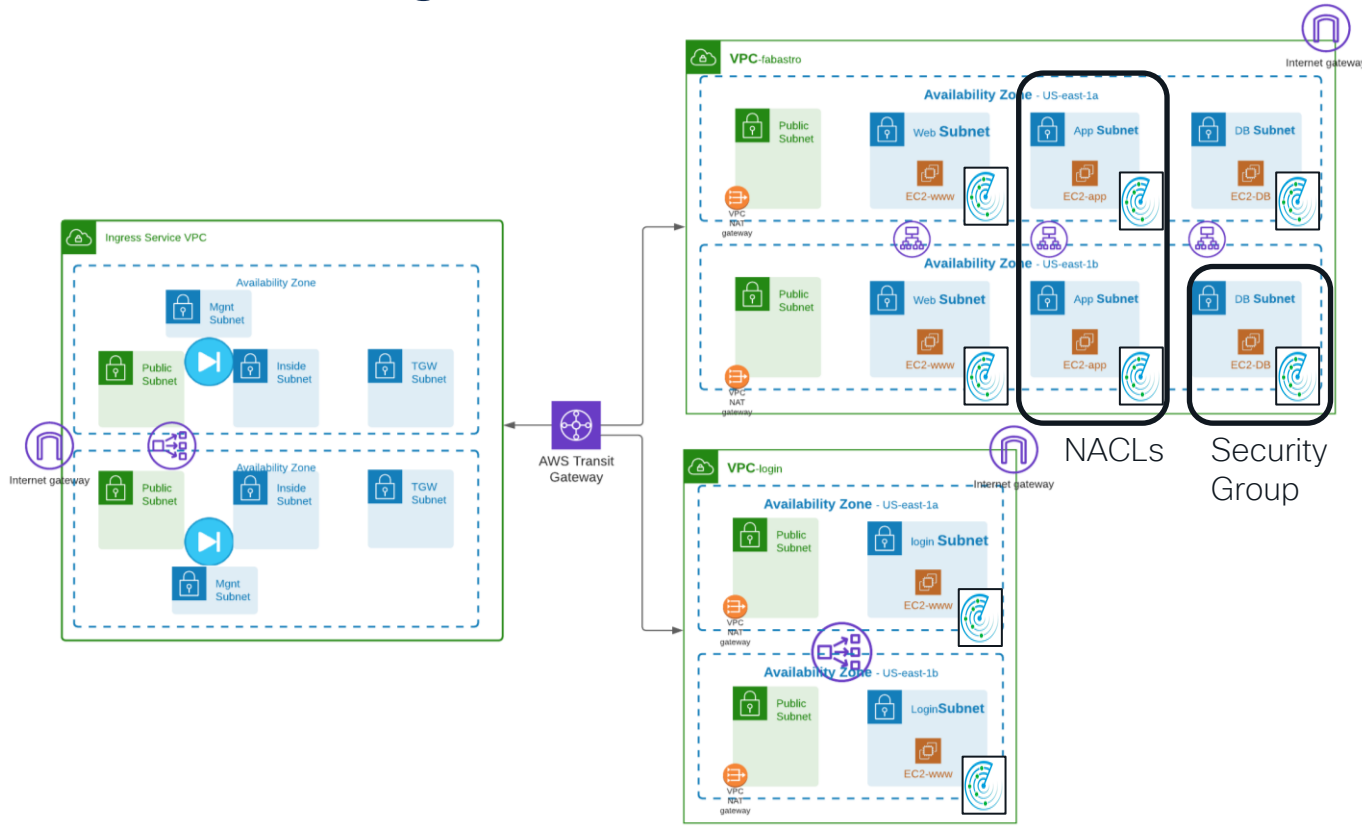
Quick Analysis Filter Policies ... + Policy

Search Information Close



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?



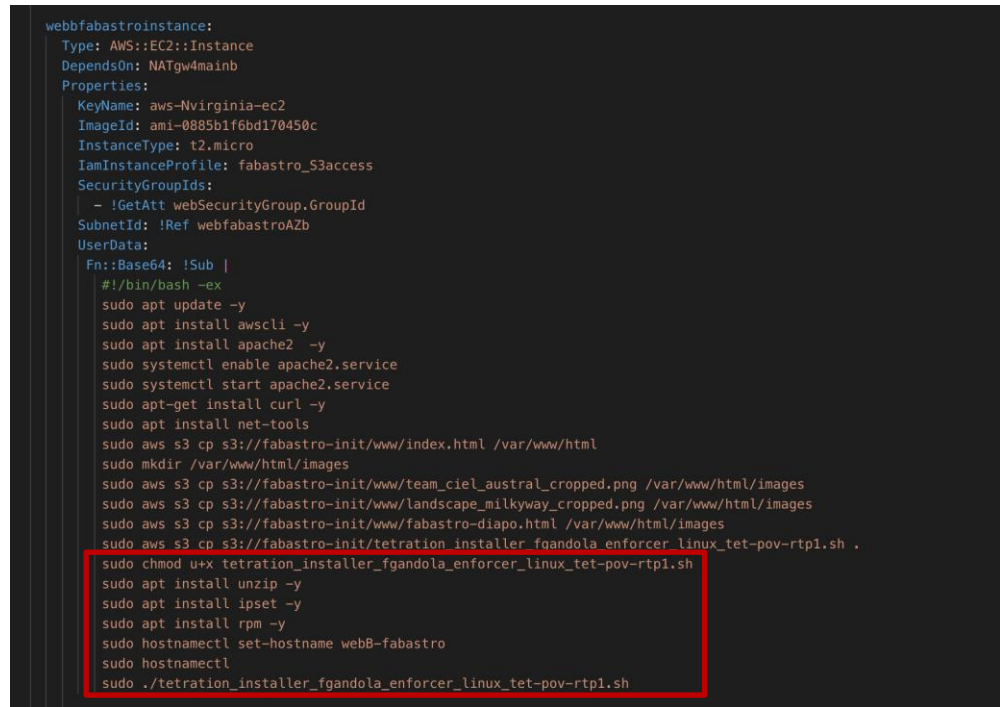
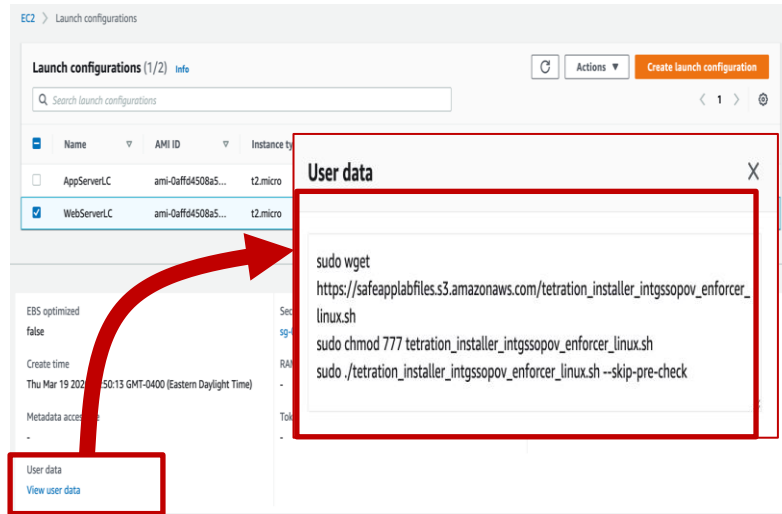
Micro-segmentation

Dynamic segmentation

Application discovery

No scaling issues

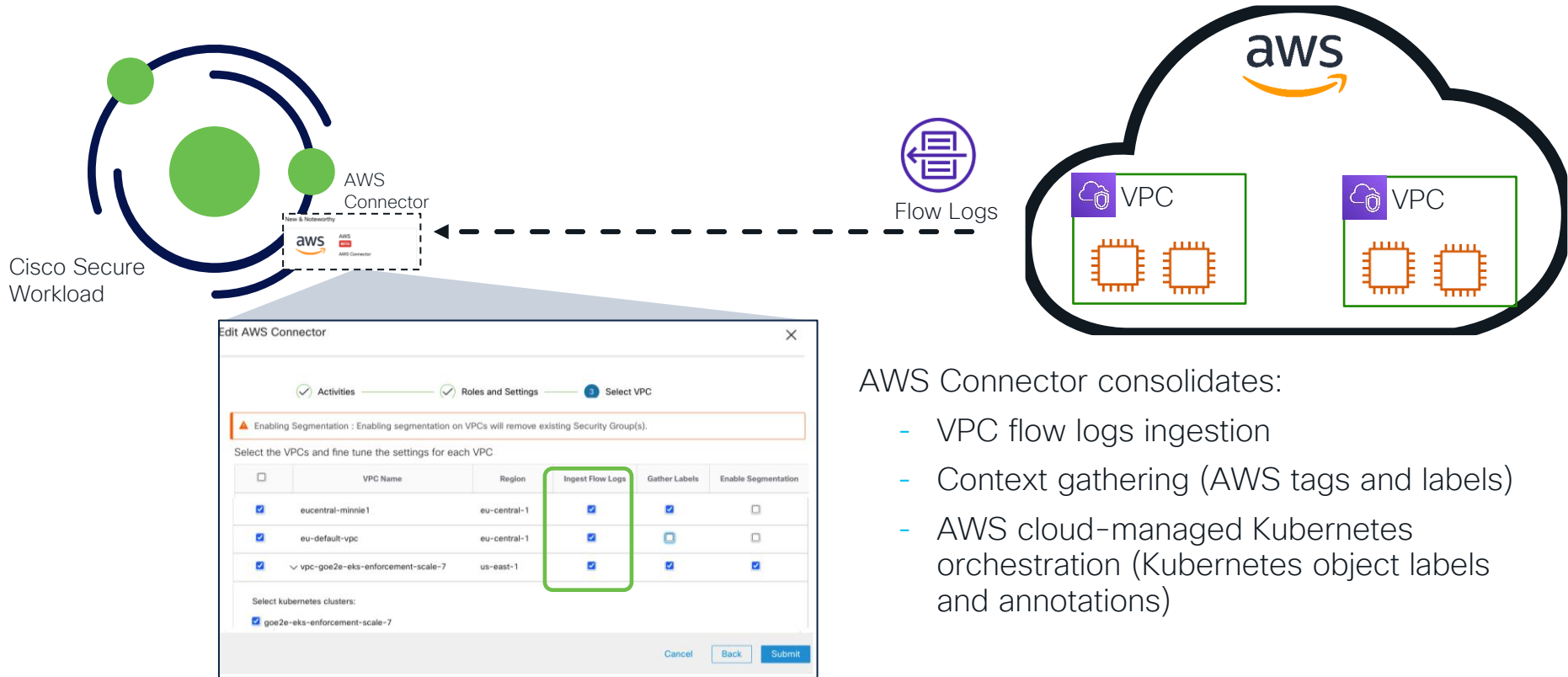
Deploy Enforcement Agent using AWS Launch Config or CloudFormation



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



Cisco Secure Workload Cloud-Based Sources

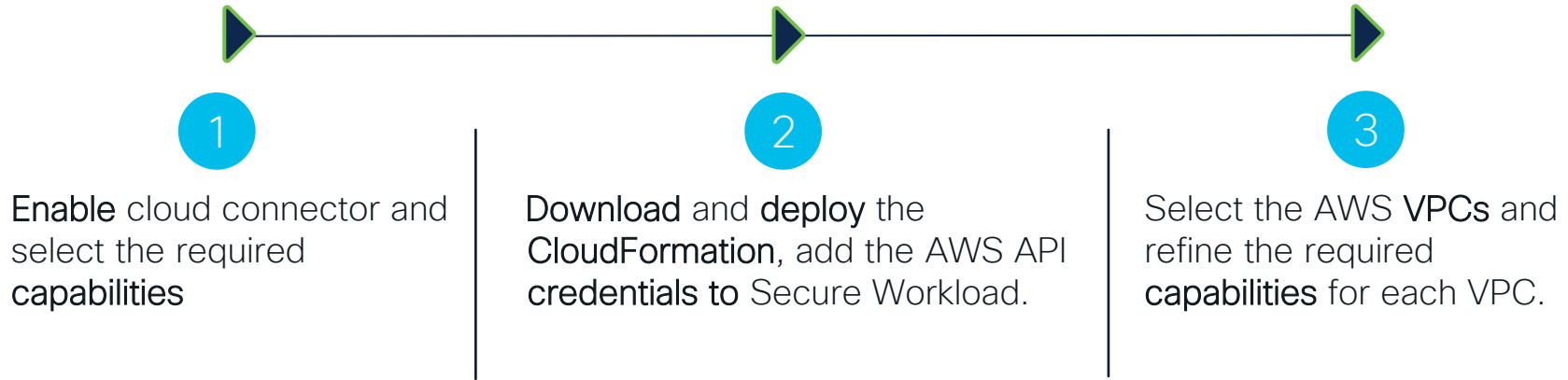


AWS Connector consolidates:

- 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



AWS Connector – Select Capabilities

1 Enable and configure the connector capabilities



The 'Edit AWS Connector' dialog shows a four-step process: 1. Activities, 2. Roles and Settings, 3. Select VPC, and 4. View Groups. The 'Name of the connector' field is set to 'AWS'. Under 'Select Activities to be performed with Cisco Secure Workload on your AWS Resources', three options are checked and highlighted with a green box: 'Gather Labels', 'Ingest Flow Logs', and 'Segmentation'. There is also an unchecked option for 'Managed kubernetes services'. A note states: 'The recommended AWS (IAM) roles and permissions depend on the selections you make above.' At the bottom right are 'Cancel', 'Back', and 'Next' buttons.

AWS Connector – IAM



2

- 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

Activities — 2 Roles and Settings — 3 Select VPC

Cisco Secure Workload requires relevant permissions to access and read flow logs settings and perform policy enforcement.

Based on the capability selections, the following CloudFormation template has been auto-generated. Use this to apply the relevant permissions to the desired user:

Additional Help

- > Create a Cloud Formation Stack
- > Create a New User
- > Example Commands

```
{
  "Resources": {
    "ManagedPolicy": {
      "Type": "AWS::IAM::Policy",
      "Properties": {
        "PolicyName": {
          "Ref": "PolicyName"
        },
        "PolicyDocument": {
          "Version": "2012-10-17",
          "Statement": [
            {
              "Effect": "Allow",
              "Action": [
                "ec2:DescribeVpcs"
              ]
            }
          ]
        }
      }
    }
  }
}
```

Access Key

Secret Key

Does your network require HTTP Proxy to reach AWS? ☒ Yes ☐ No

Please provide your proxy URL:

Full Scan Interval seconds

Delta Scan Interval seconds

AWS Limits

Security Groups Per Region

Security Groups Per Network Interface

Rules per Security Group

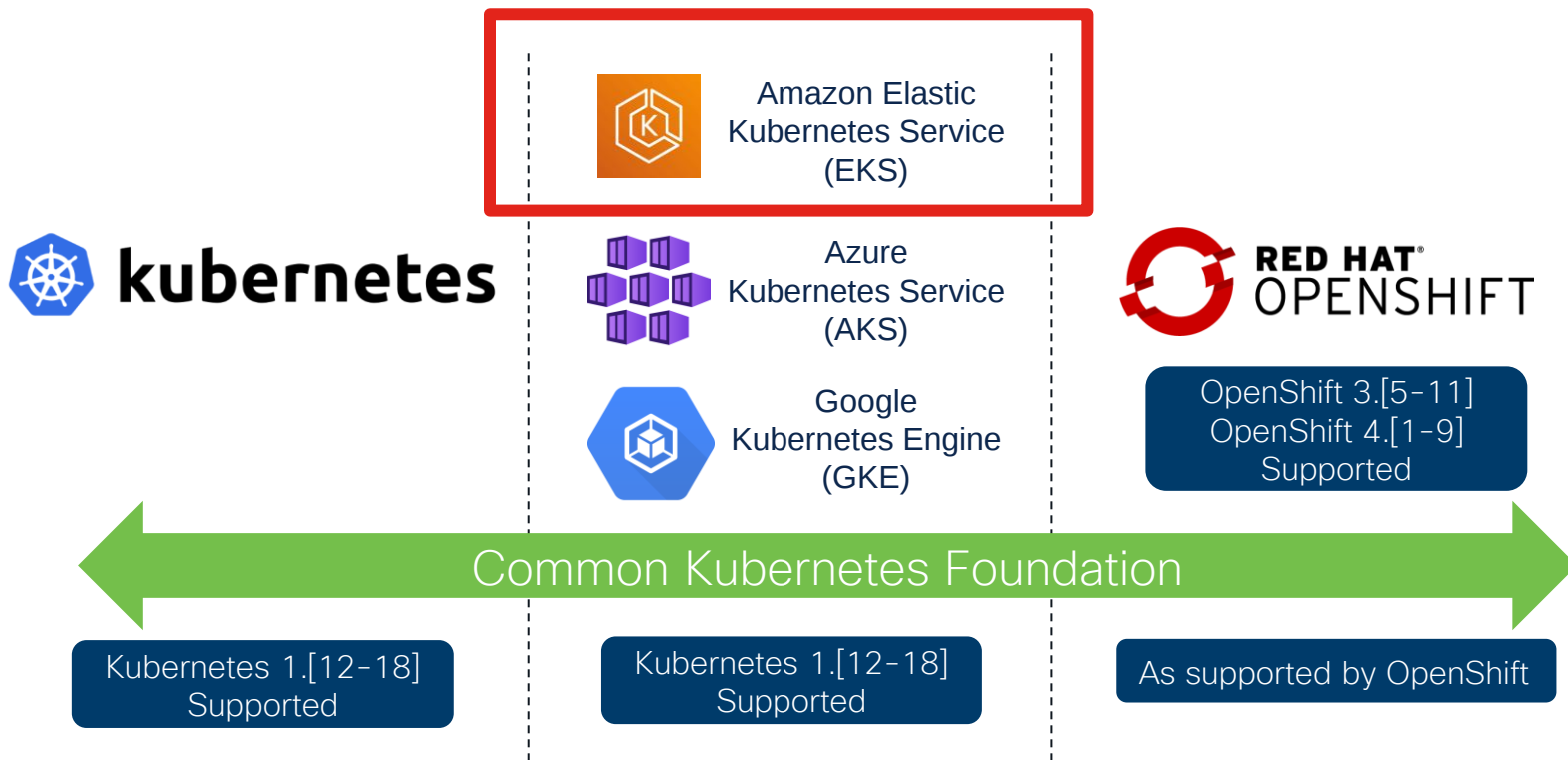
AWS Connector – Select VPCs

3

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

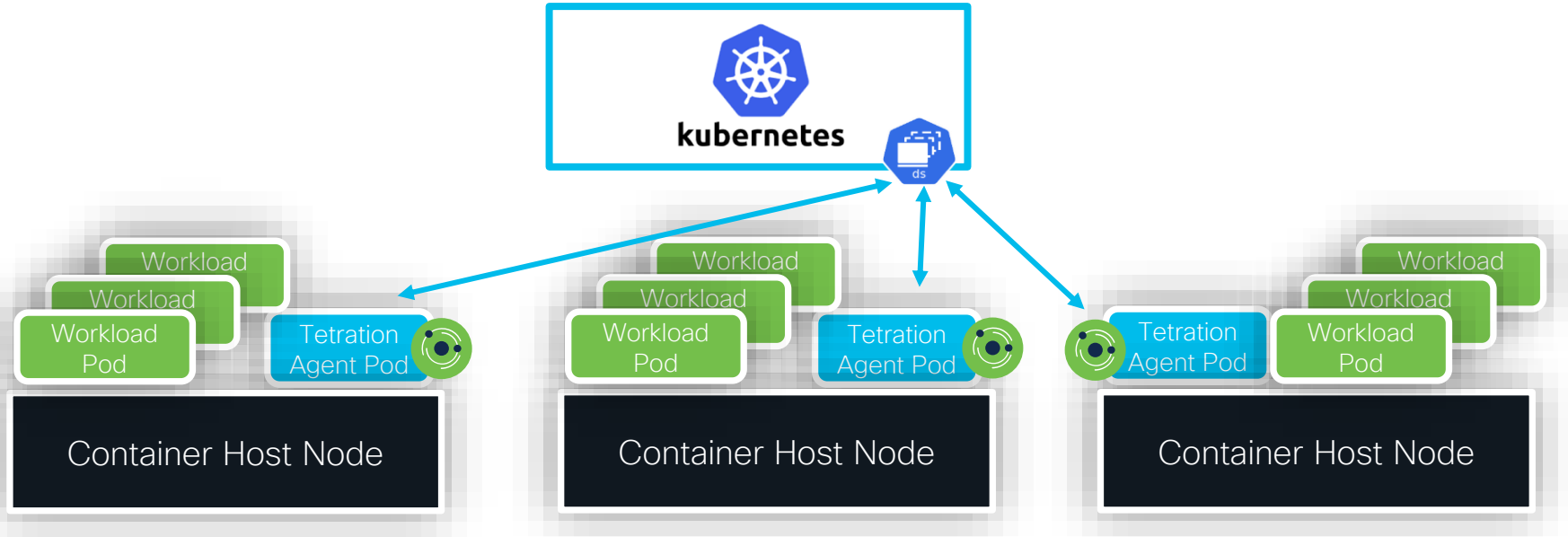
☐	VPC Name	Region	☐	☐	☐
☐	default	ap-northeast-1	☐	☐	☐
☐	test-vpc	ap-northeast-1	☐	☐	☐
☐	lab-vpc	ap-northeast-1	☐	☐	☐
☐	vpc-e6ecd481	sa-east-1	☐	☐	☐
☐	vpc-967901fe	ca-central-1	☐	☐	☐
☐	vpc-06686161	ap-southeast-1	☐	☐	☐
☐	vpc-20fcc147	ap-southeast-2	☐	☐	☐
☐	vpc-cfcd36a5	eu-central-1	☐	☐	☐
☐	SecureVPC	us-east-1	☐	☐	☐
☒	csw-vpc	us-east-1	☒	☒	☒

Kubernetes support



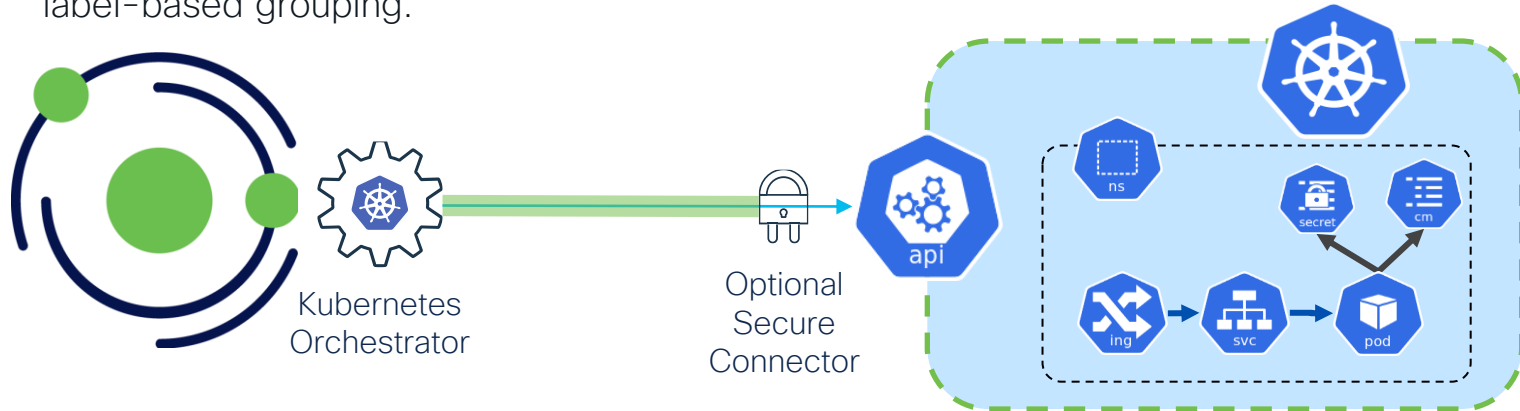
Cisco Secure Workload Agents as Daemonset

Daemonset pods run on all schedulable nodes in the container cluster



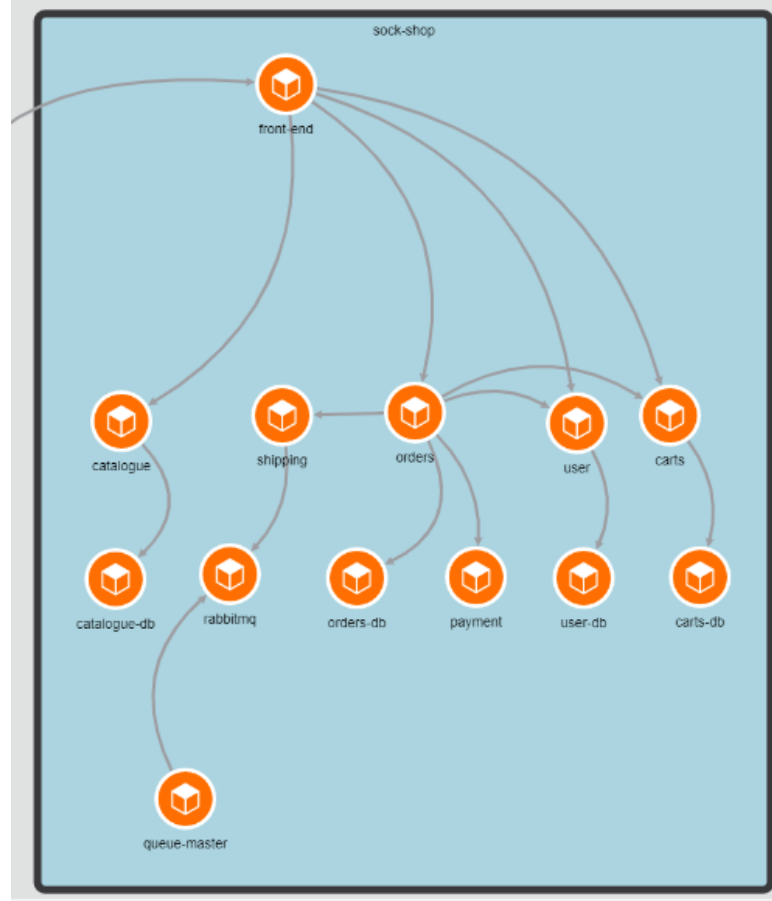
Kubernetes Metadata Ingest

- 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.

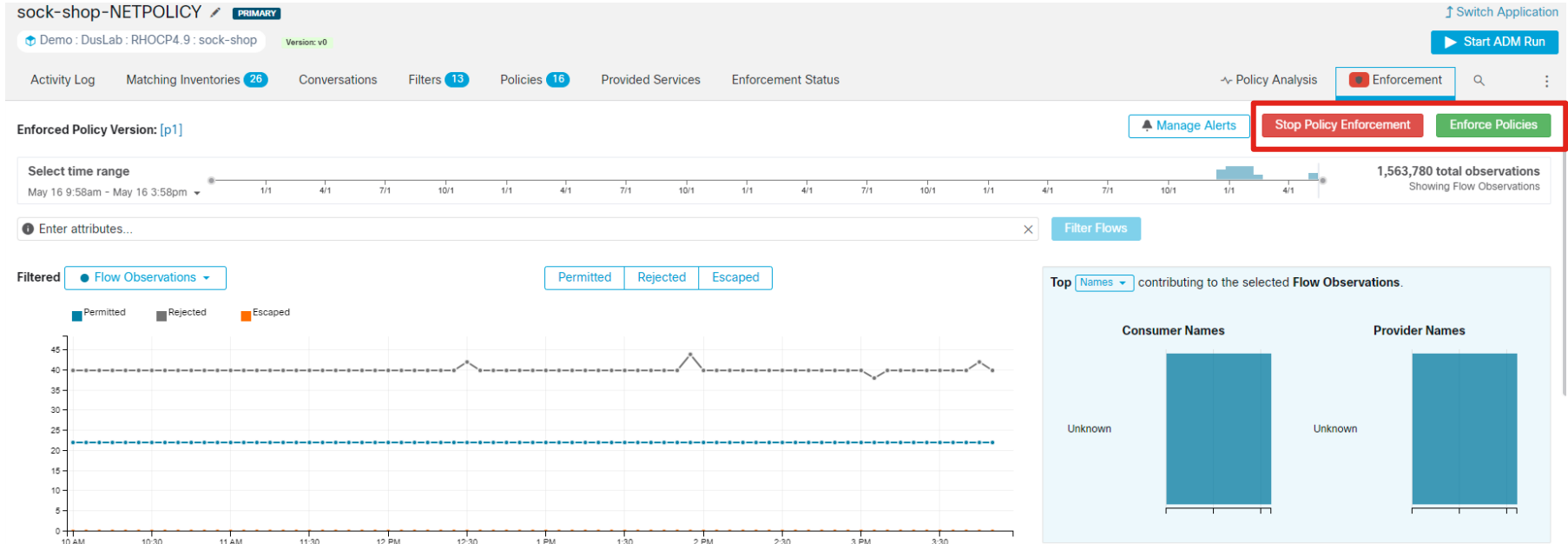
Canvas view of my policy



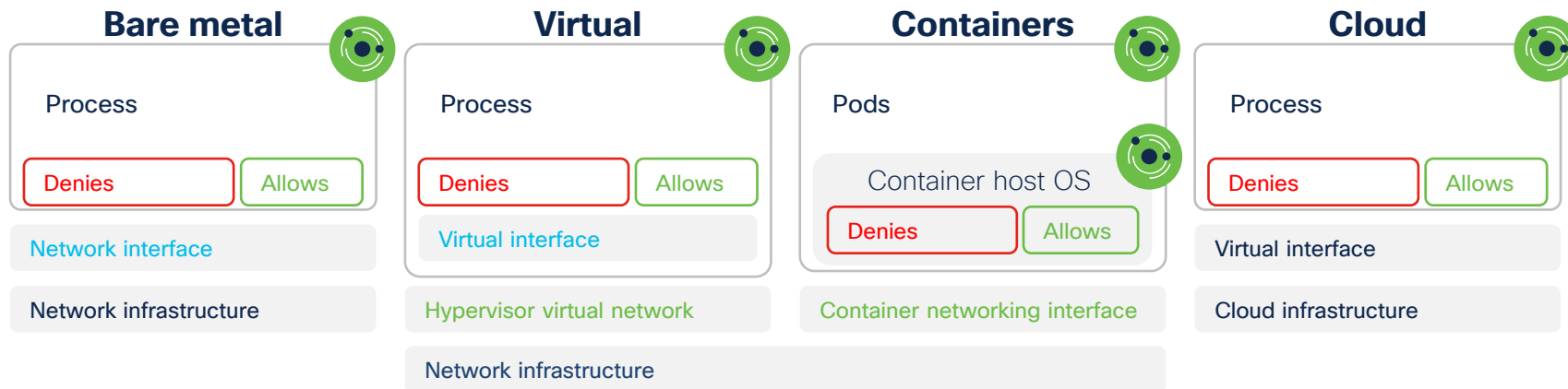
List view of the policy

Quick Analysis Filter Policies ...						
Absolute policies 0 Default policies 15 Catch All DENY + Add Default Policy						
	Priority ↑↓	Action ↑↓	Consumer ↑↓	Provider ↑↓	Protocols And Ports ↑↓	
	100	ALLOW	Demo : DusLab : RHOC4.9	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

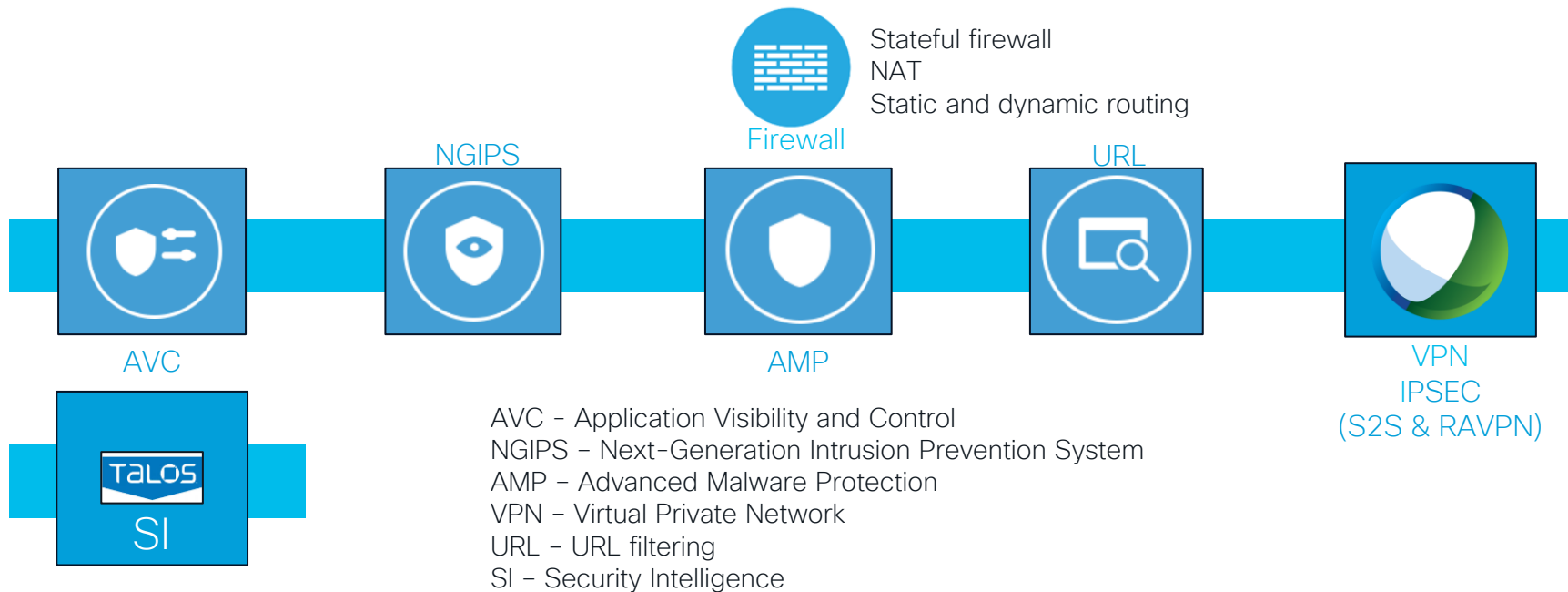
Intrusion prevention

Alert and flow logs

Central management
and visibility



Cisco Secure Firewall - NGFWv



FTD Appliance

vmware

aws

KVM

Microsoft Azure



Google Cloud Platform

ORACLE
Cloud Infrastructure

Multi-cloud and Hybrid Cloud Environments

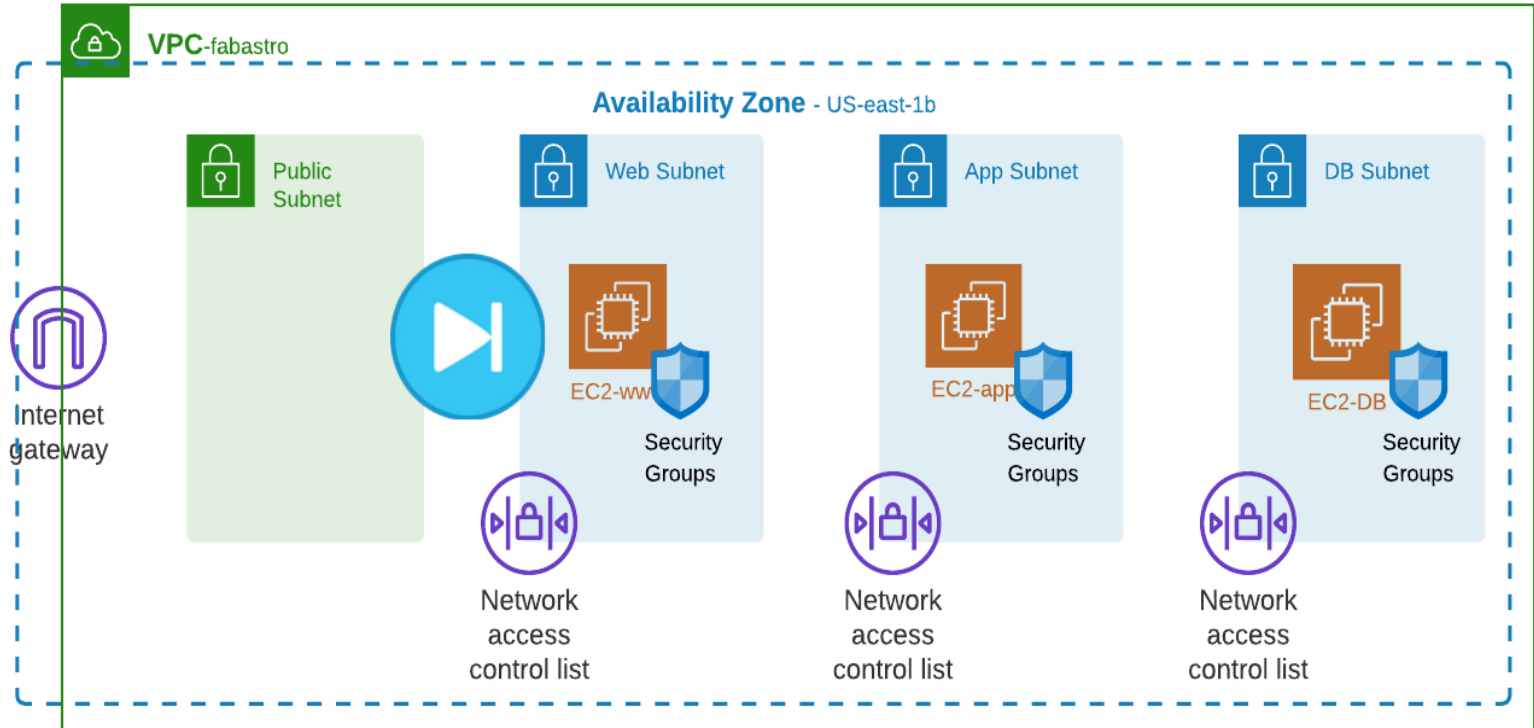


- Clustering
- Dynamic Policy
- Better integration with public cloud infrastructure
- Infrastructure as Code and Automation
- Integration with GuardDuty
- Gateway Load balancer integration
- Auto Scaling
- Snapshot support

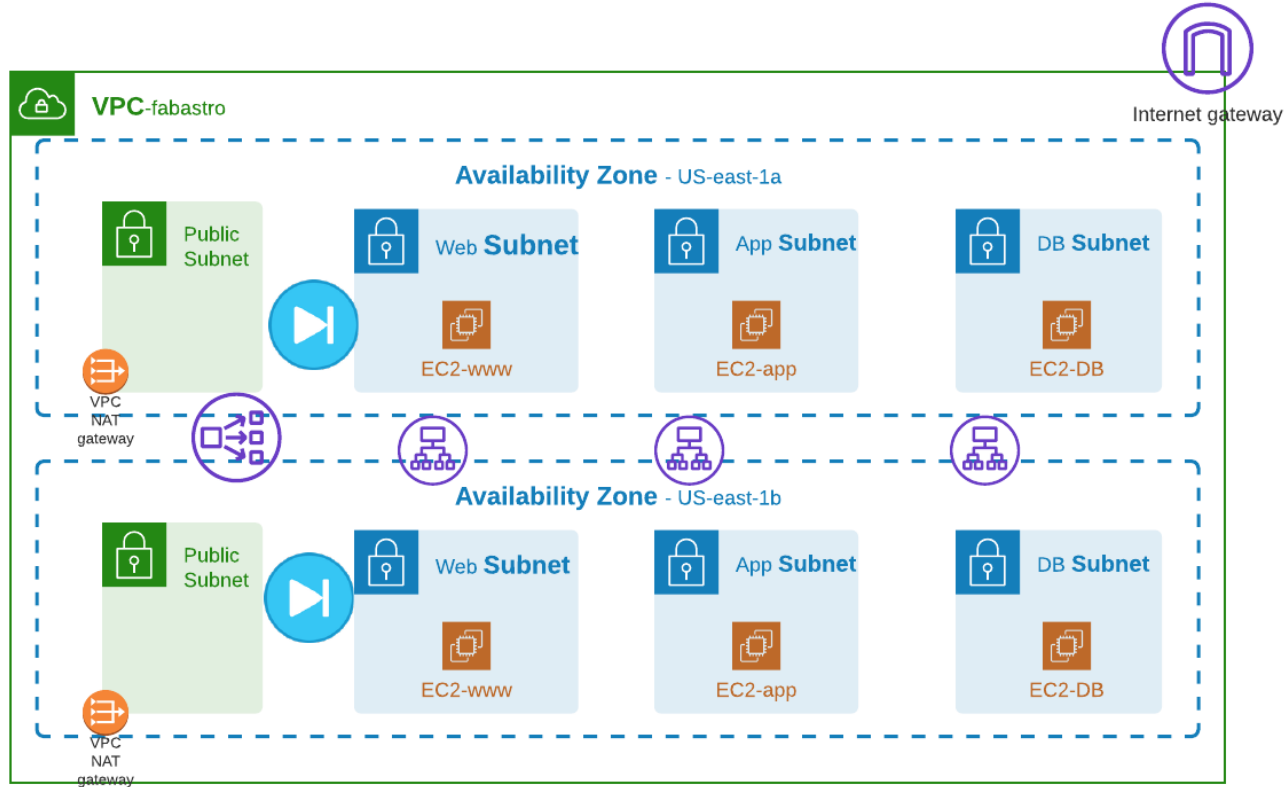
Basic FTD insertion



Firewall in front of the “Application” VPC



FTD insertion with HA



Limits of this design

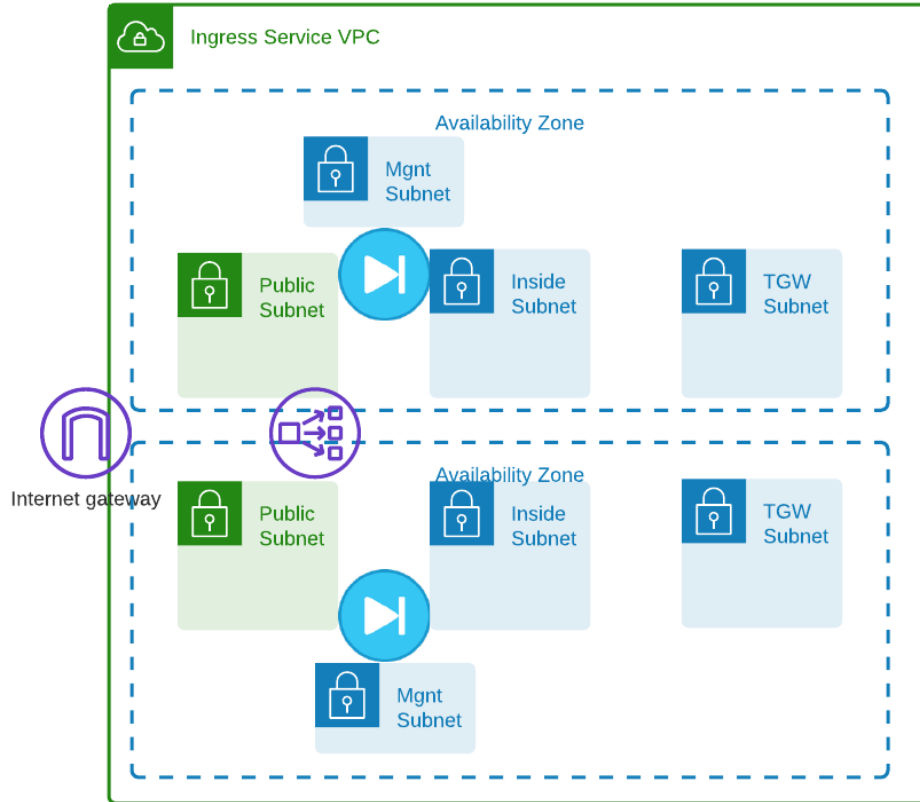


New Firewall pair for each applications

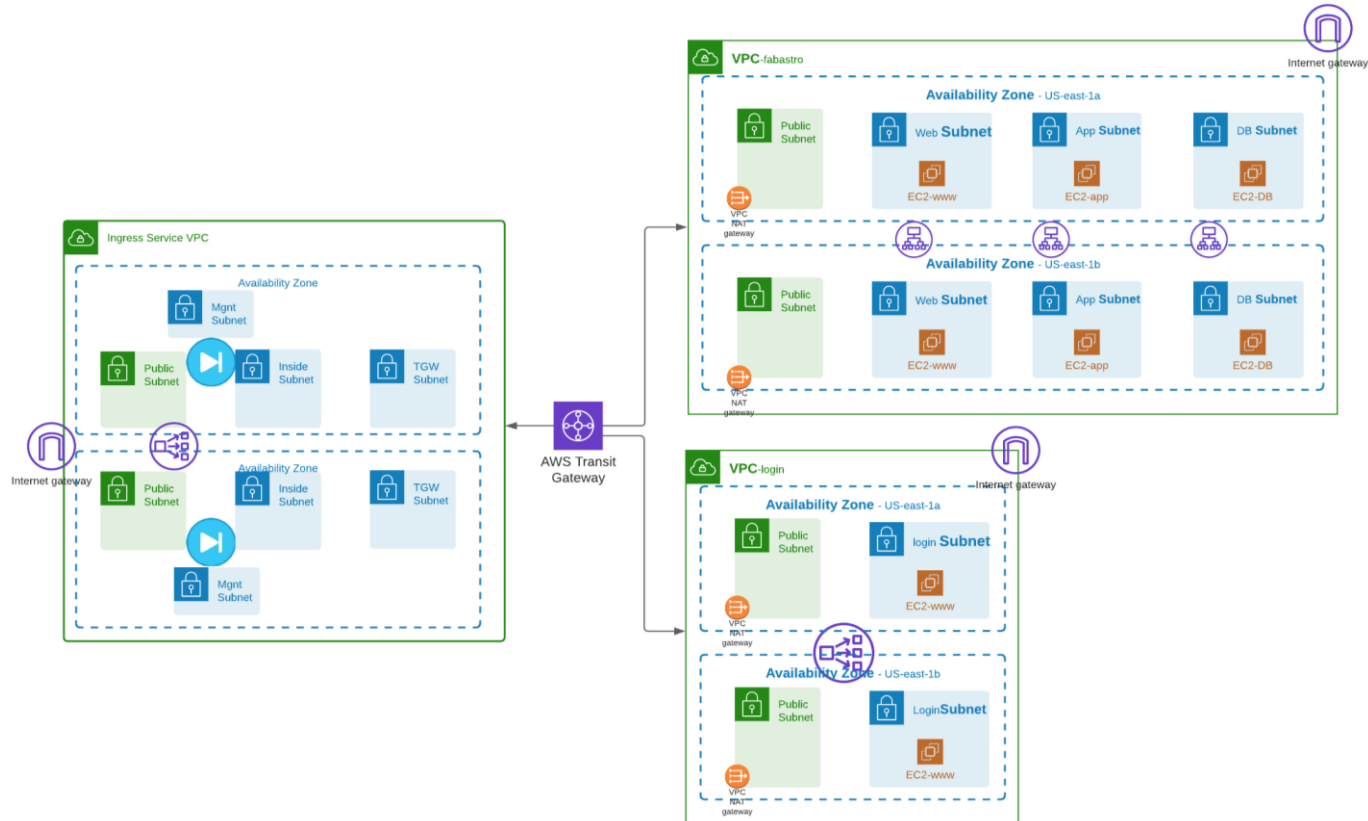


Double inspection for inter-VPC

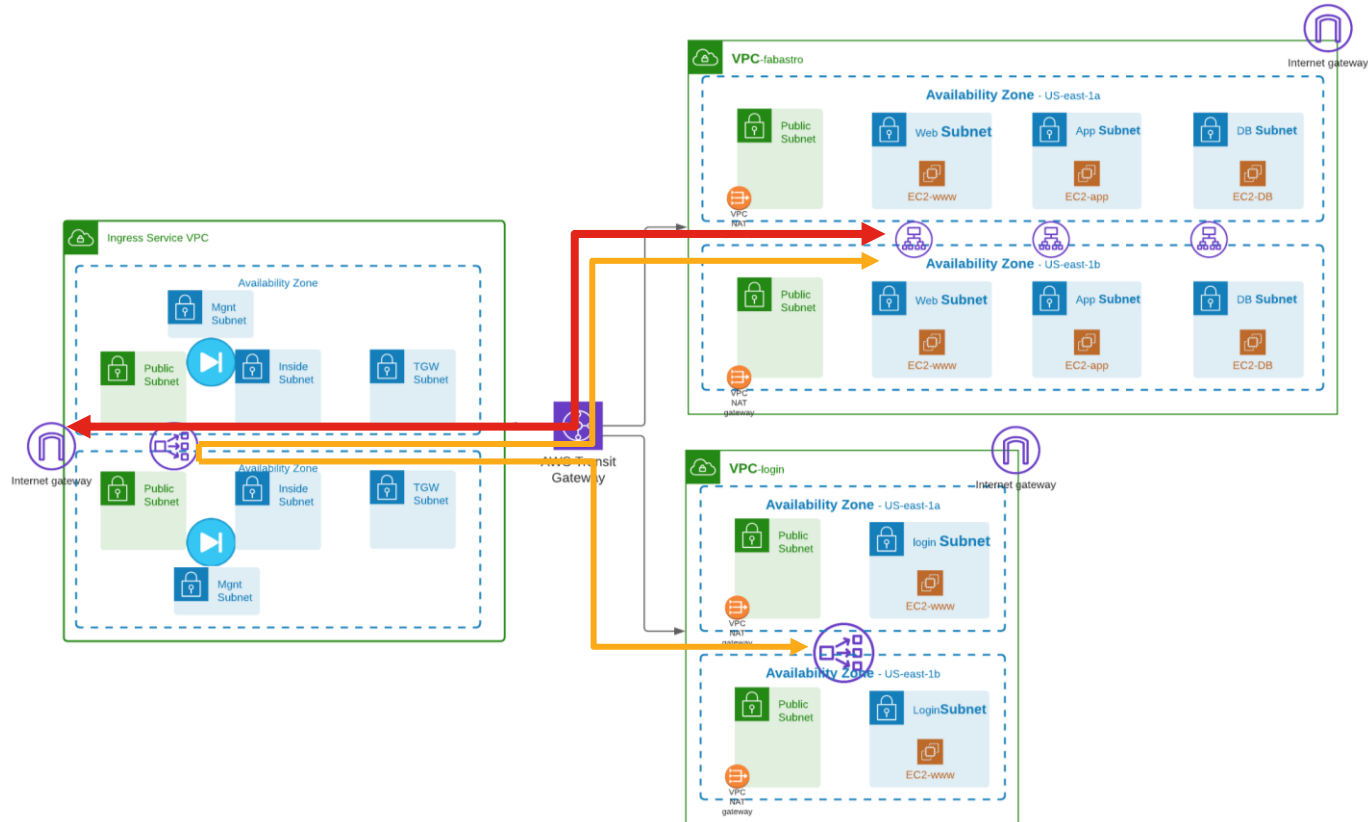
Ingress Service VPC



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

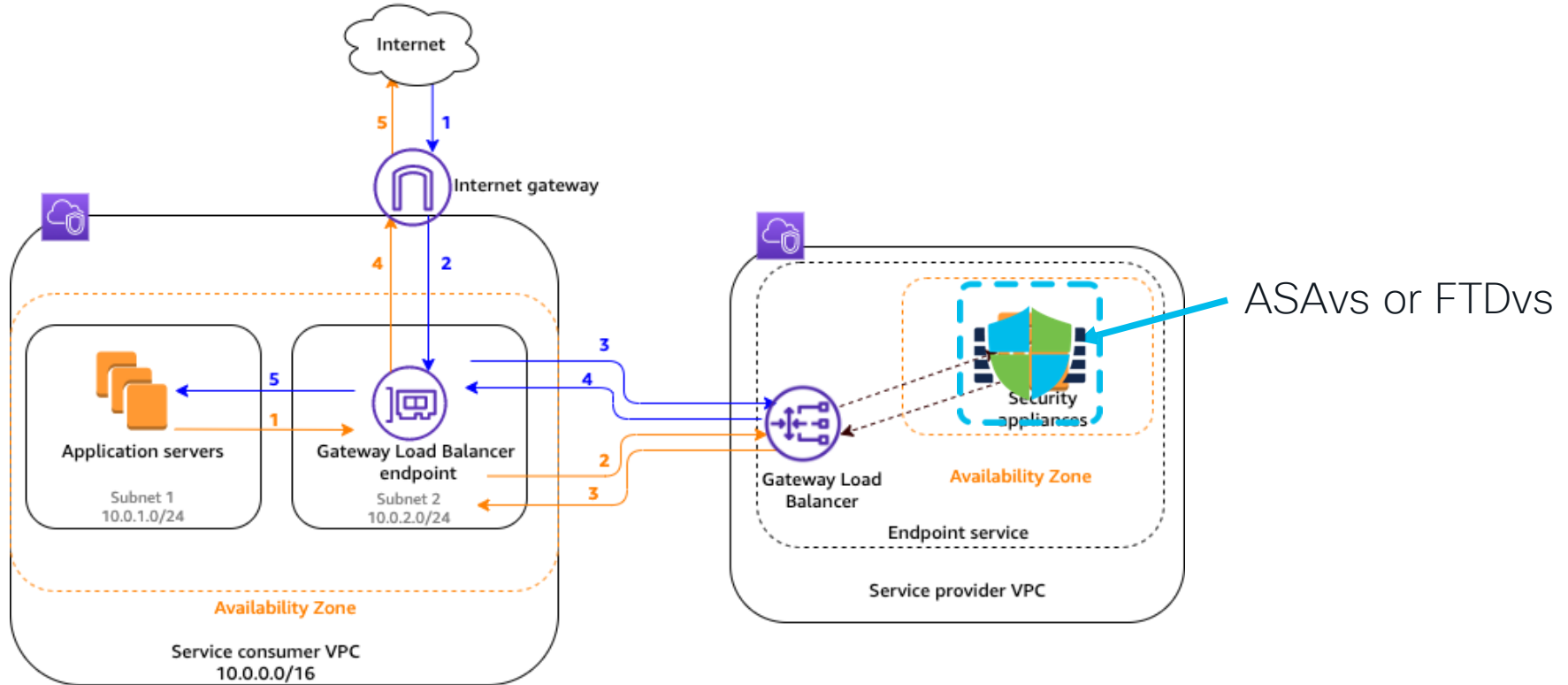
What to configure on FTD ?

- 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

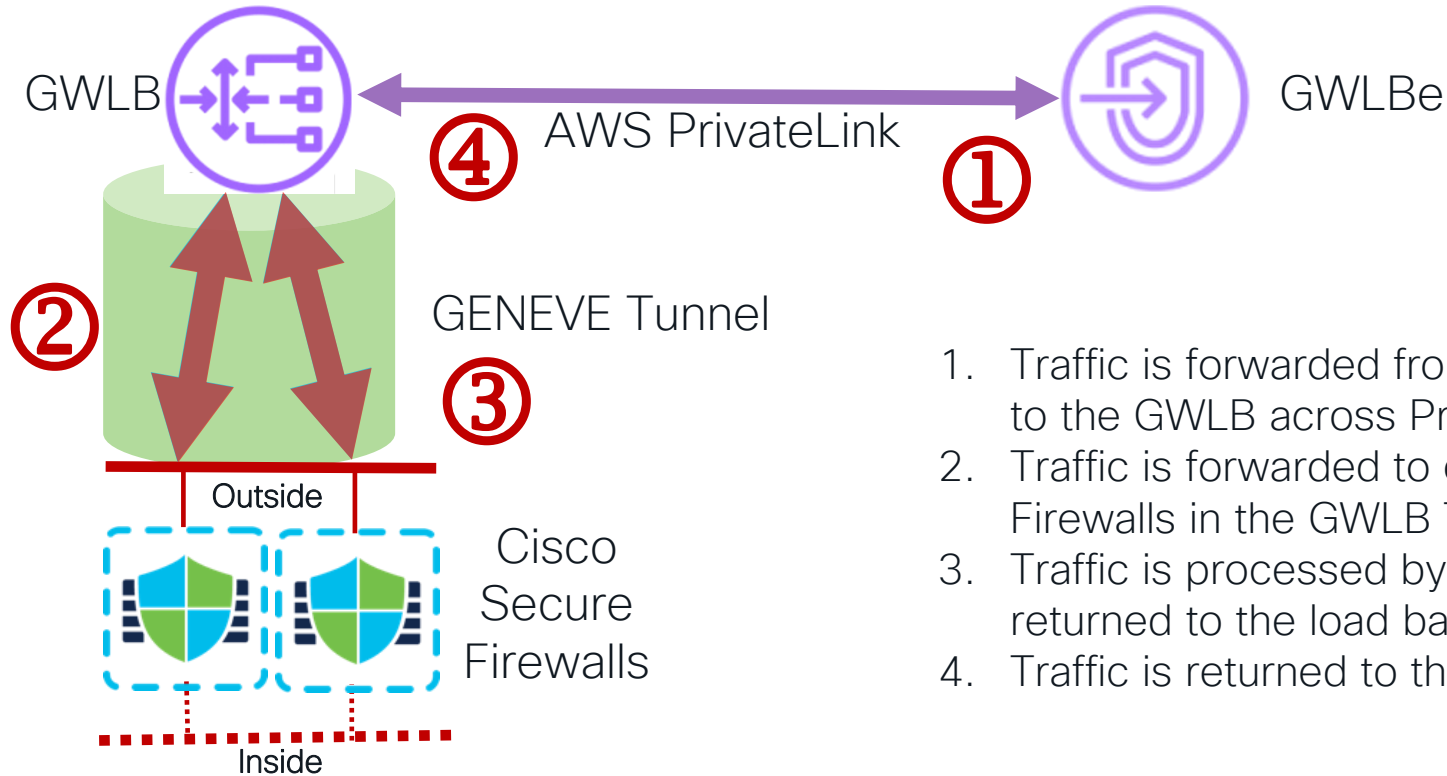


AWS Gateway Load Balancer



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

Traffic Flow Between the GWLBe, GWLB, and Firewalls

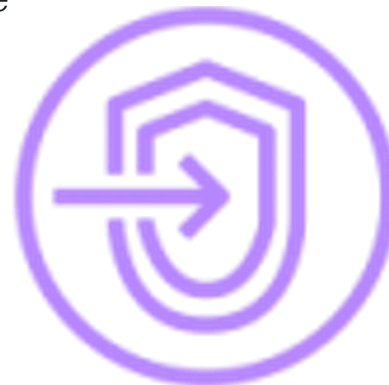


1. Traffic is forwarded from the GWLBe to the GWLB across PrivateLink
2. Traffic is forwarded to one of the Firewalls in the GWLB Target Group
3. Traffic is processed by the firewall and returned to the load balancer
4. Traffic is returned to the GWLBe

Gateway Load Balancer Endpoint (GWLBBe)



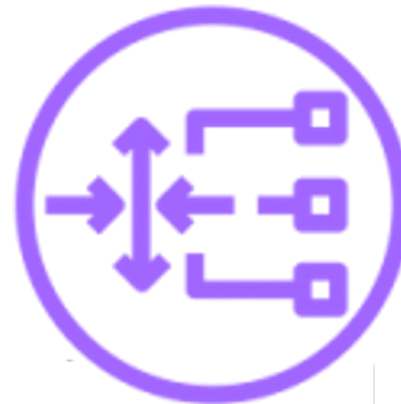
- Gateway Load Balancer Endpoint is a next hop type in a VPC route table
- Intercepts traffic transparently
- Forwards traffic transparently to the Gateway Load Balancer
- Associated with a single subnet
 - Associated with a single Availability Zone
 - AWS delivers packets to this subnet after the GWLBBe 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)

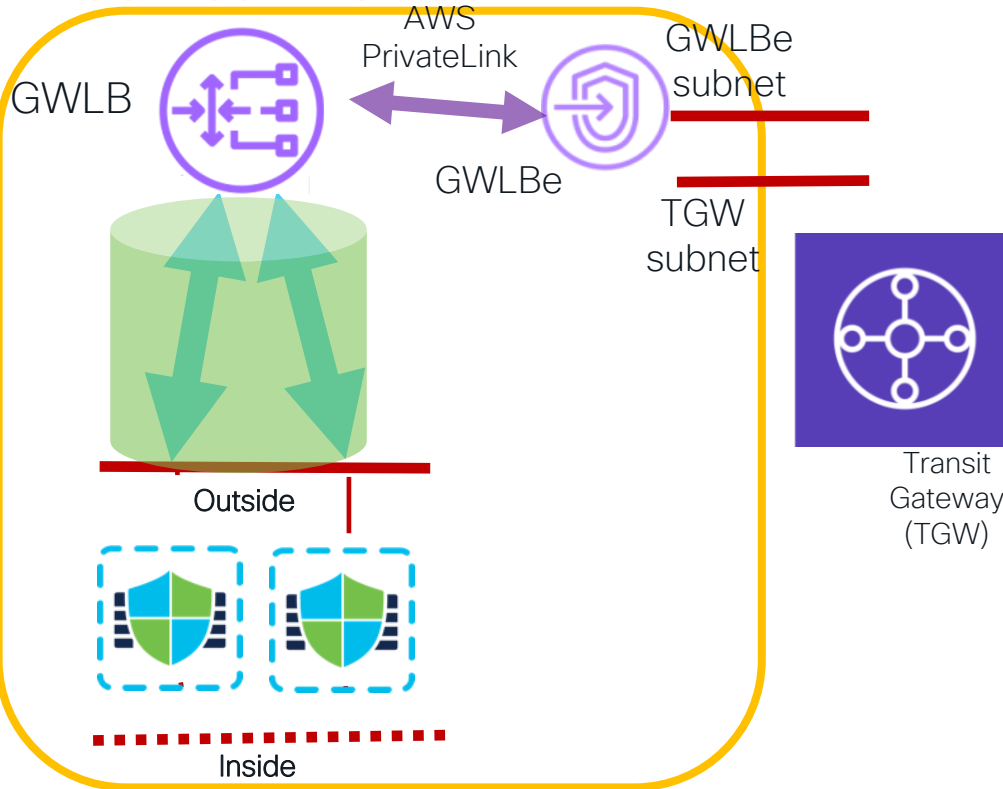


- Forwards traffic to the firewalls inside a GENEVE tunnel
 - Load balances between firewalls in a *Target Group*
 - Does not modify packets or packet headers
 - Forwards all packets associated with a particular connection to the same firewall
- Associate with one or more subnets
 - Can load balance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

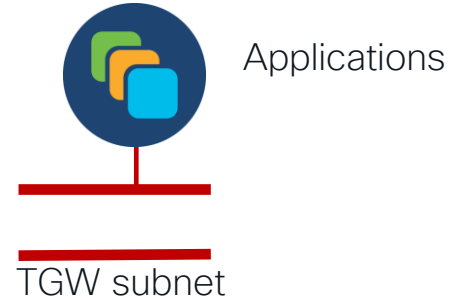


East West Traffic – Required Subnets

Service VPC



Application VPC

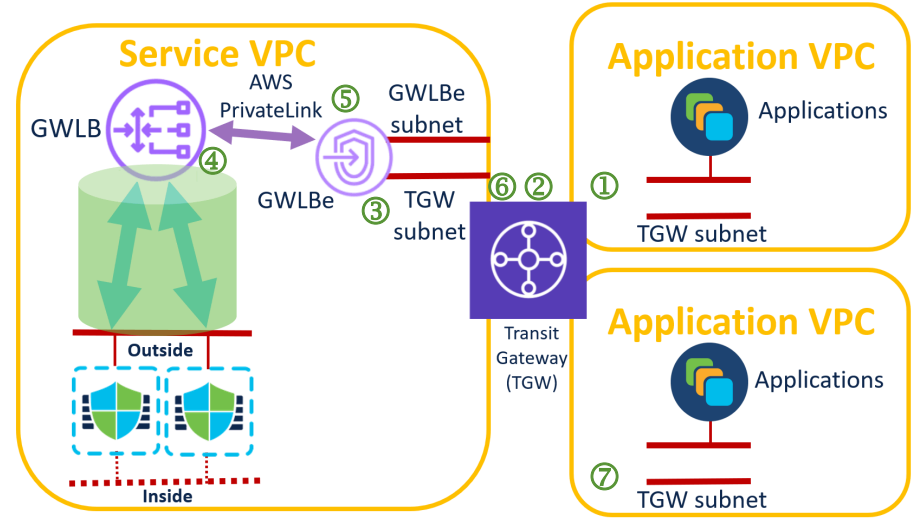


Application VPC

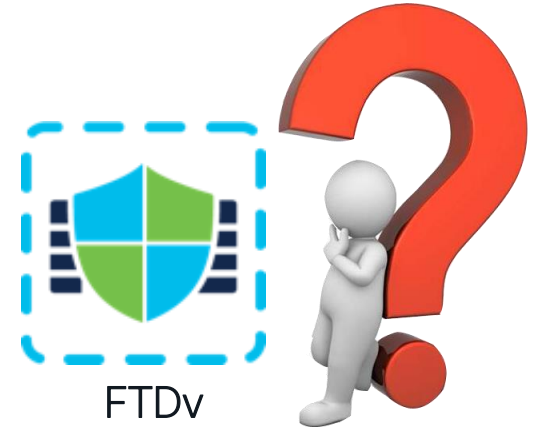
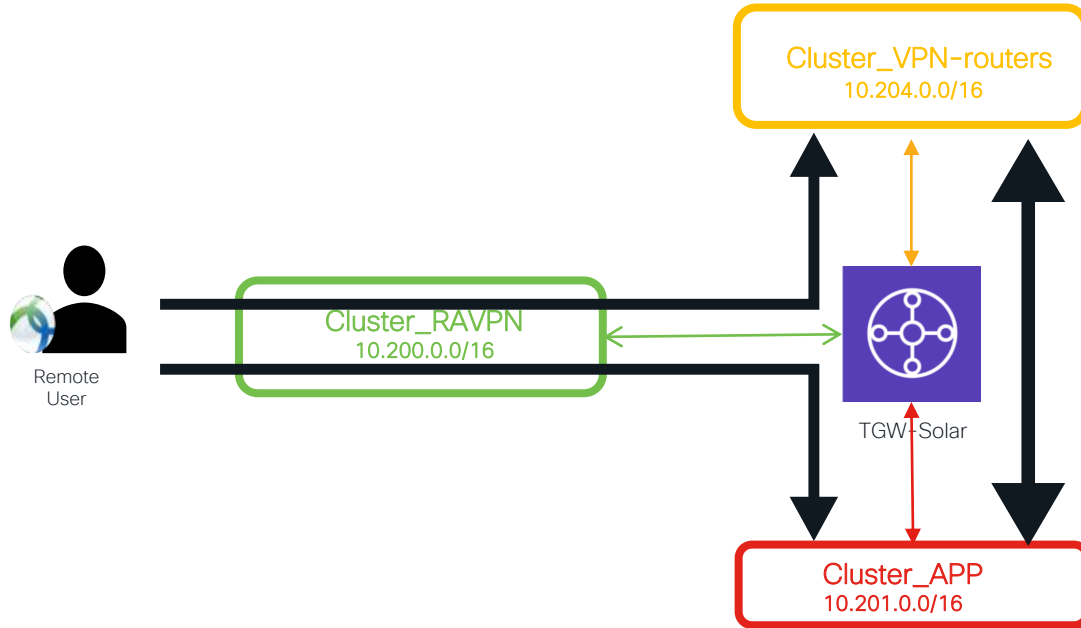


Routing East-West Traffic

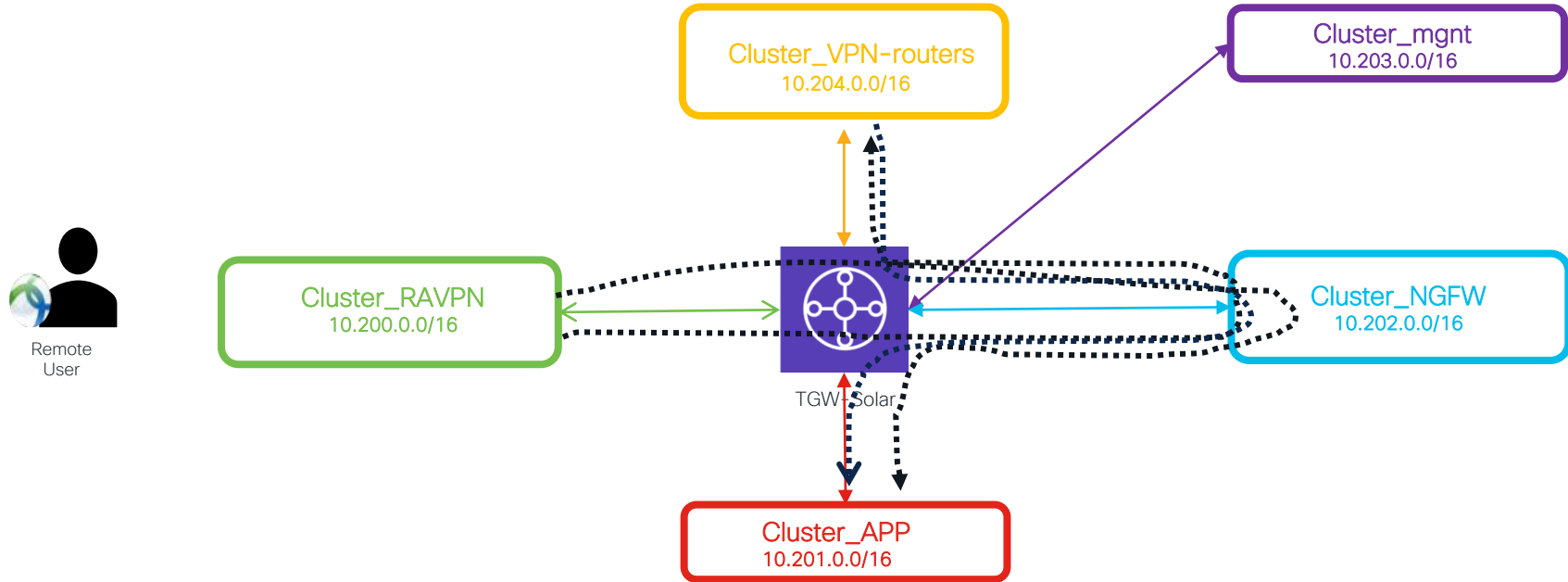
1. Application subnet (in source VPC) next hop is TGW attachment
2. TGW route table (for source VPC attachment) forwards traffic to Service VPC
3. TGW subnet in Service VPC next hop is GWLBe
4. GWLBe forwards traffic to GLWB, traffic is inspected and returned to GWLBe
5. GWLBe subnet next hop is TGW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



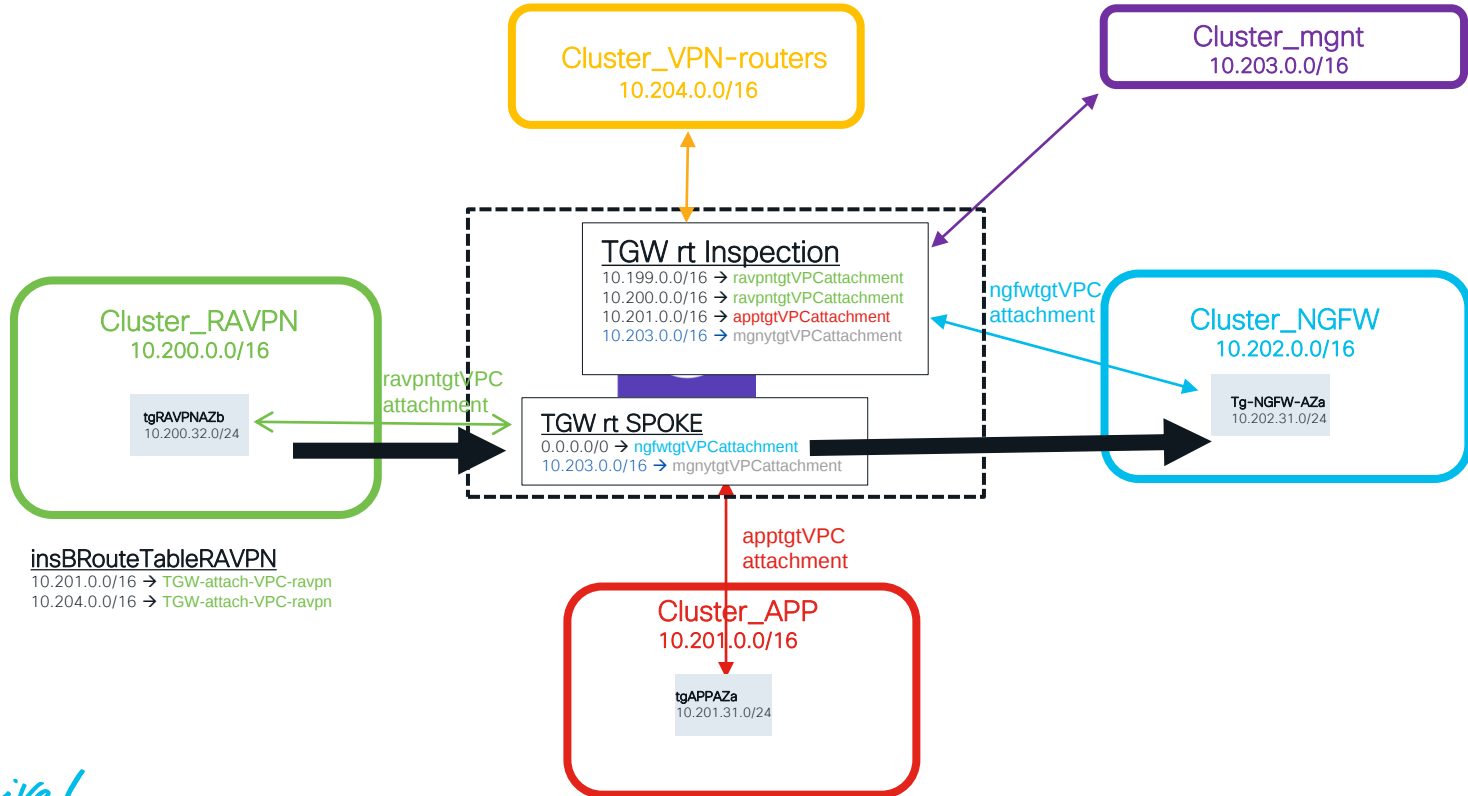
Solar High level design



Solar Security Insertion



Fastest TGW Introduction ever...

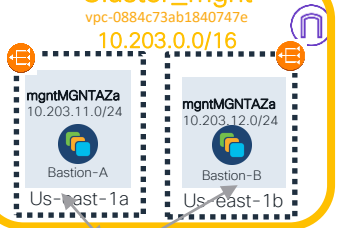


mgntTableMGNT

10.201.0.0/16 → mgnytgtVPCattachment
10.202.0.0/16 → mgnytgtVPCattachment
10.204.0.0/16 → mgnytgtVPCattachment
10.200.0.0/16 → mgnytgtVPCattachment
0.0.0.0/0 → IGClusterAPP

Cluster_mgnt

vpc-0884c73ab1840747e
10.203.0.0/16



IGClusterAPP

TransitGateway Solar



IGClusterNGFW

Cluster_NGFW

vpc-031a746e4abb1b2ed
10.202.0.0/16



egwlbendpointRouteNGFW

10.202.101.0/24 → LOCAL
0.0.0.0 → ngfwtgtVPCattachment

tgAZa RouteNGFW

10.202.0.0/16 → LOCAL
0.0.0.0 → egwlbNGFWendpointa
10.203.0.0/16 → ngfwtgtVPCattachment

tgAZb RouteNGFW

10.202.0.0/16 → LOCAL
0.0.0.0 → egwlbNGFWendpointb
10.203.0.0/16 → ngfwtgtVPCattachment

mgntTableNGFW

10.203.0.0/16 → mgnytgtVPCattachment
0.0.0.0/0 → IGClusterAPP

tgwrouteRAVPN

10.199.1.0/24 → insideRAVPNENIA
10.199.2.0/24 → insideRAVPNNIB
0.0.0.0/0 → ravpntgtVPCattachment

insARouteTableRAVPN

10.201.0.0/16 → TGW-attach-VPC-ravpn
10.204.0.0/16 → TGW-attach-VPC-ravpn

insBRouteTableRAVPN

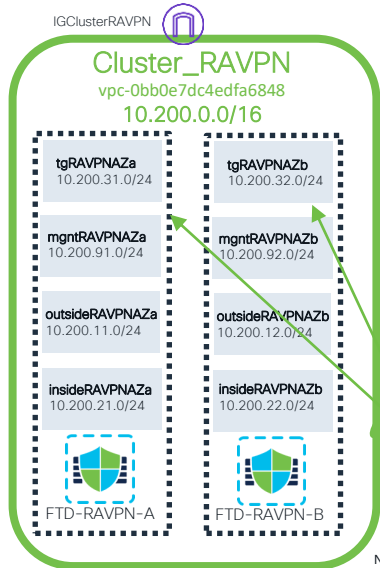
10.201.0.0/16 → TGW-attach-VPC-ravpn
10.204.0.0/16 → TGW-attach-VPC-ravpn

mgntRouteTableRAVPN

0.0.0.0/0 → IGClusterRAVPN
10.203.0.0/16 → TGW-attach-VPC-ravpn

outsideAZa TableRAVPN

0.0.0.0/0 → IGClusterRAVPN



tgAPPAZaRouteTableAPP
0.0.0.0 → IGClusterAPP

APP rt web AZa

10.199.0.0/16 → TGW-attach-VPC-APP
10.200.0.0/16 → TGW-attach-VPC-APP
10.201.0.0/16 → LOCAL
10.203.0.0/16 → TGW-attach-VPC-APP
10.204.0.0/16 → TGW-attach-VPC-APP
0.0.0.0/0 → NATgw4websolarA

TGW rt MGNT

10.202.0.0/16 → ngfwtgtVPCattachment
10.200.0.0/16 → ravpntgtVPCattachment
10.201.0.0/16 → apptgtVPCattachment
10.204.0.0/16 → vpnroutertgtVPCattachment

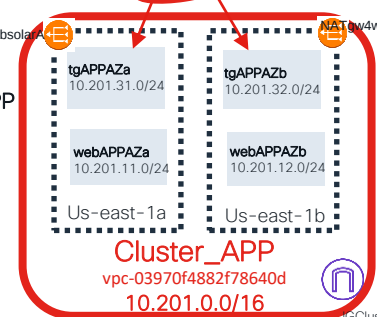
TGW rt Inspection

10.199.0.0/16 → ravpntgtVPCattachment
10.200.0.0/16 → ravpntgtVPCattachment
10.201.0.0/16 → apptgtVPCattachment
10.203.0.0/16 → mgnytgtVPCattachment

TGW rt SPOKE

0.0.0.0/0 → ngfwtgtVPCattachment
10.203.0.0/16 → mgnytgtVPCattachment

apptgtVPCattachment



Cluster_APP

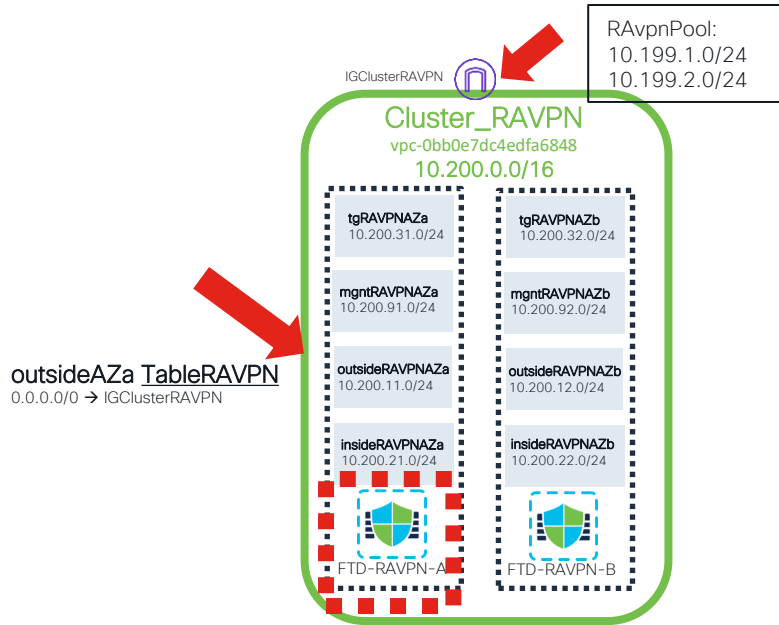
vpc-03970f4882f78640d
10.201.0.0/16

IGClusterAPP

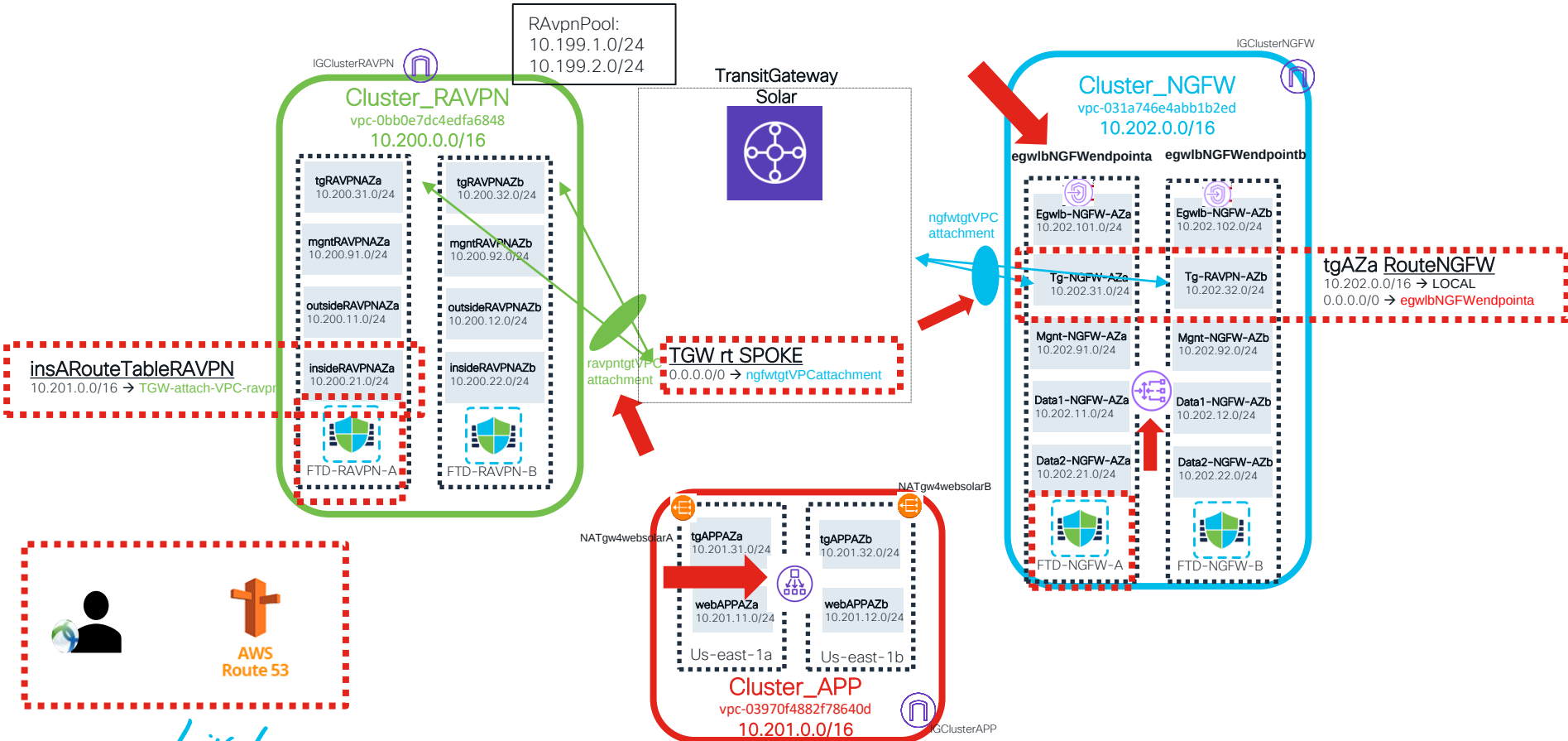
APP rt web AZb

10.199.0.0/16 → TGW-attach-VPC-APP
10.200.0.0/16 → TGW-attach-VPC-APP
10.201.0.0/16 → LOCAL
10.203.0.0/16 → TGW-attach-VPC-APP
10.204.0.0/16 → TGW-attach-VPC-APP
0.0.0.0/0 → NATgw4websolarA

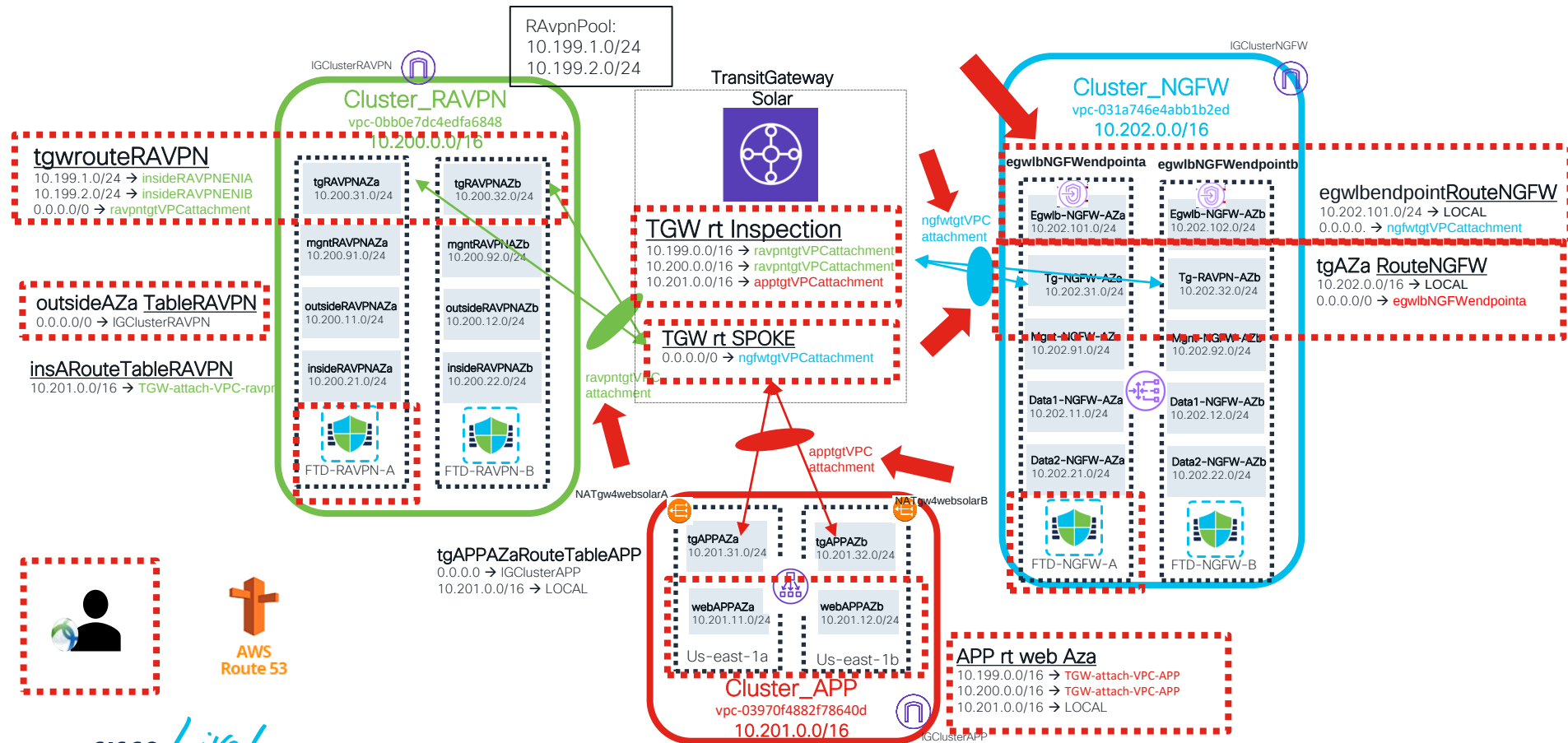
Establish Tunnel



Access Fabastro Web page



Access Fabastro Web page



Handling High Availability and Scalability



Working Together



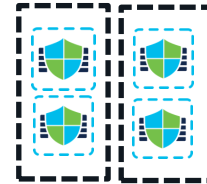
Loadbalancing



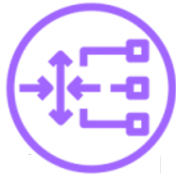
Autoscaling



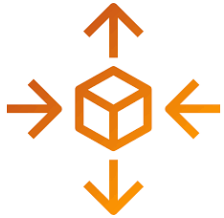
Several
independant
FTDv



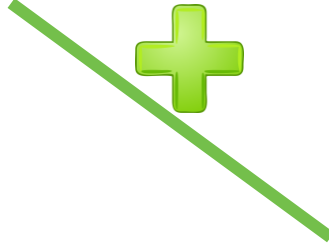
Working Together



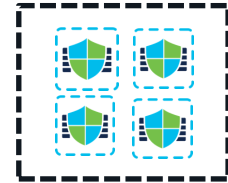
Loadbalancing



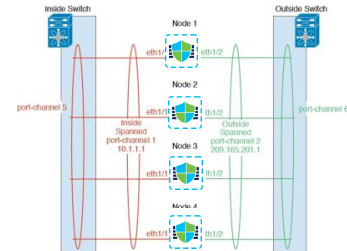
Autoscaling



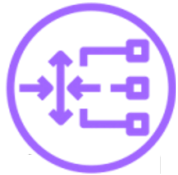
Several
independant
FTDv



FTDv
Clustering



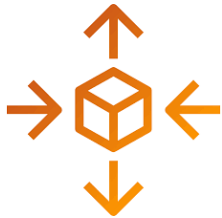
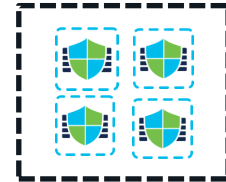
No AutoScaling with Clustering YET



Loadbalancing



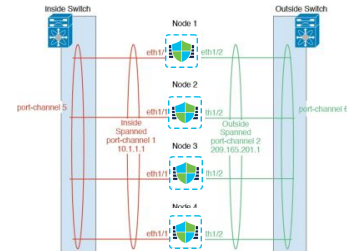
Several
independant
FTDv



Autoscaling



FTDv
Clustering



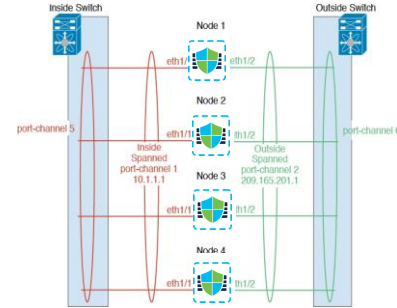
AutoScaling or Clustering ?

TODAY



Autoscaling

SOMEDAY



FTDv
Clustering

But WHY ????

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

GWLB did not support Stateful Failover until...

EC2 > Target groups > Solar-AS-1-lb-UnSec-tg0 > Edit target group attributes

Edit target group attributes [Info](#)

Restore defaults

Target configuration

Deregistration delay [Info](#)

The time to wait for in-flight requests to complete while deregistering a target. During this time, the state of the target is draining.

seconds

0-3600

Target failover [Info](#)

By default, the Gateway Load Balancer continues to send existing flows to targets, even if they have failed or are deregistered. However, new flows are sent to healthy targets. Use the toggle switch to rebalance existing flows to healthy targets.

☒ Rebalance existing flows — *recommended*

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 $10 \times 3 = 30$ 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 **time**out. 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

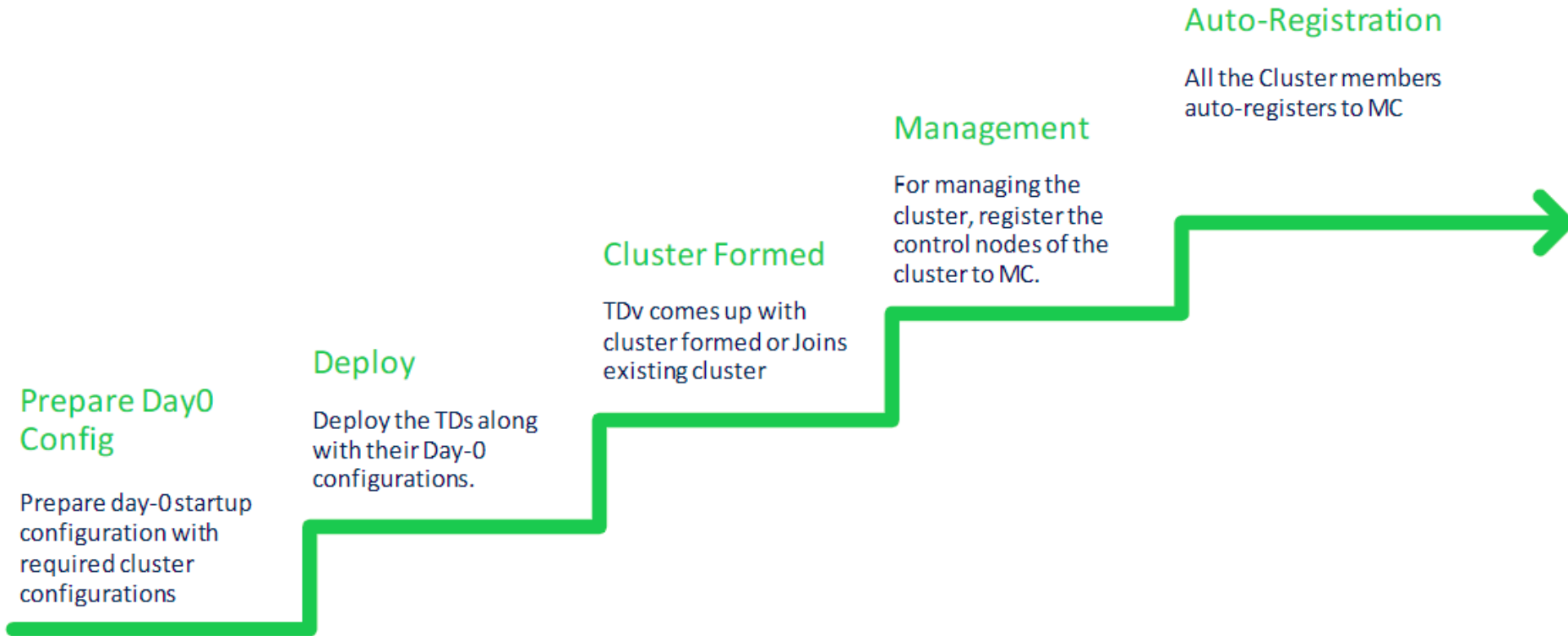
Physical Cluster

- 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>> ]  
}
```

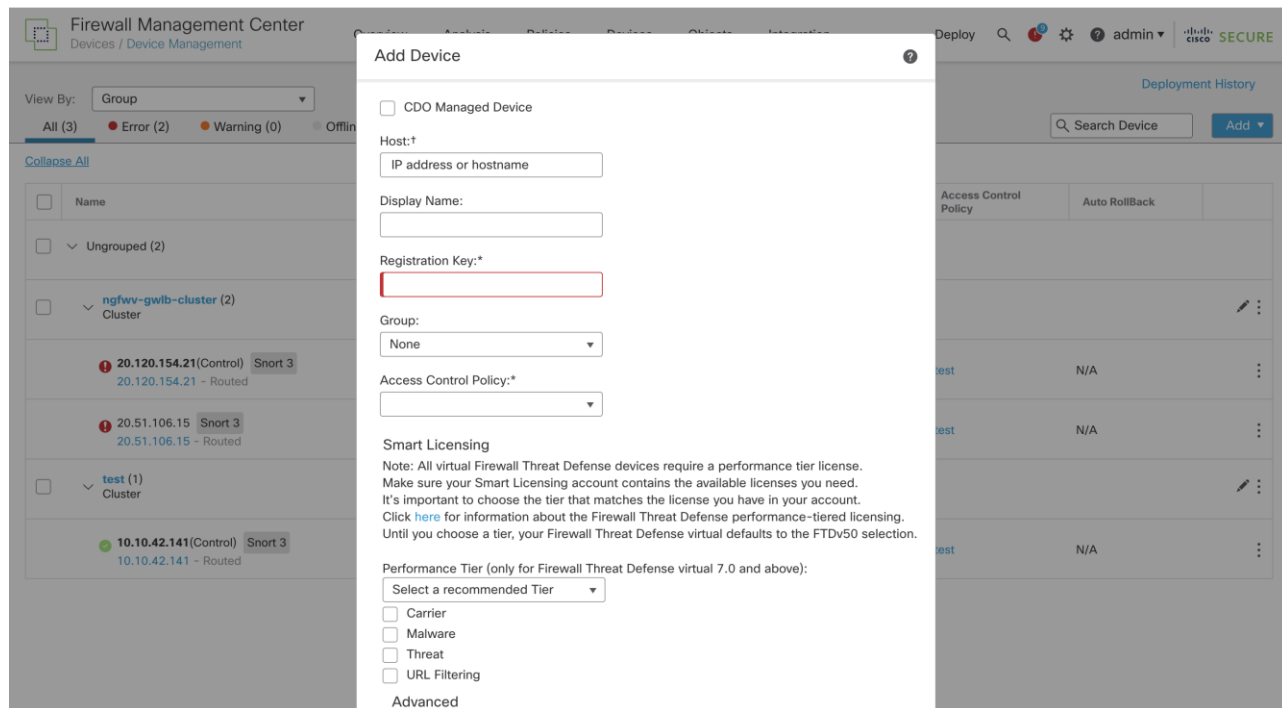
Day0 Option-2: run_config on AWS

```

"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-am",
  "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



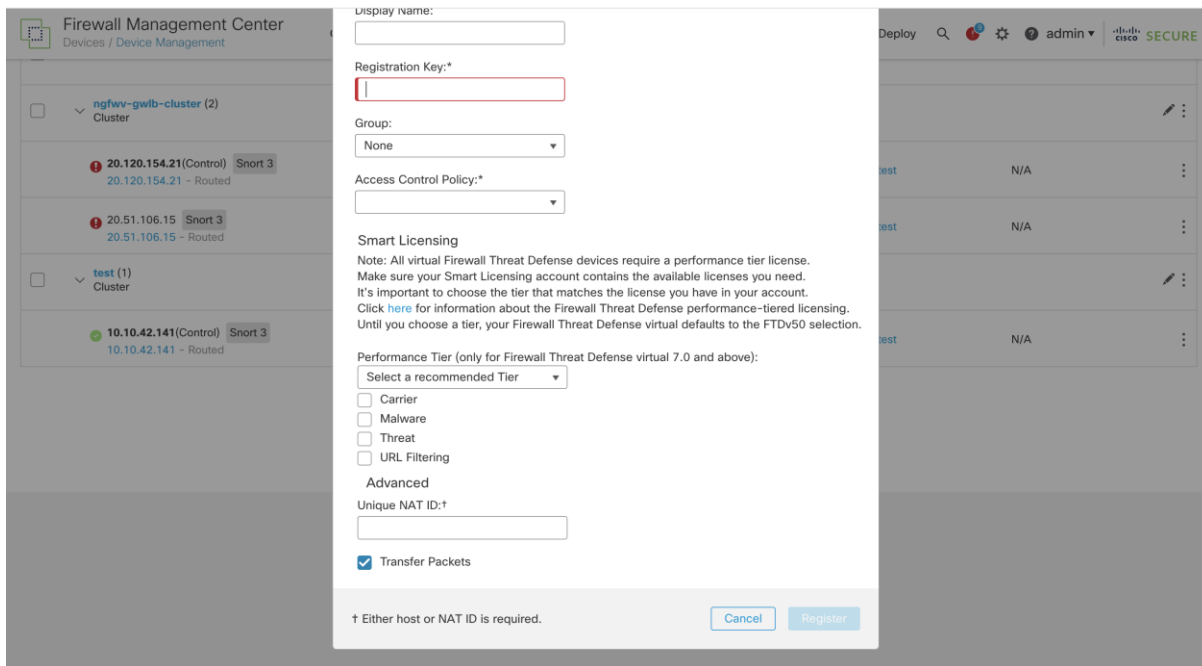
The screenshot shows the Cisco Firewall Management Center (FMC) interface. The 'Add Device' dialog box is open, displaying the following fields and options:

- ☐ CDO Managed Device
- Host: IP address or hostname
- Display Name:
- Registration Key:*
- Group: None
- Access Control Policy:*
- Smart Licensing:
 - Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.
- Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):
 - Select a recommended Tier
 - ☐ Carrier
 - ☐ Malware
 - ☐ Threat
 - ☐ URL Filtering
- Advanced

The background interface shows a list of devices with columns for Name, IP address, and Status. The 'ngfwv-gwib-cluster' is highlighted.

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



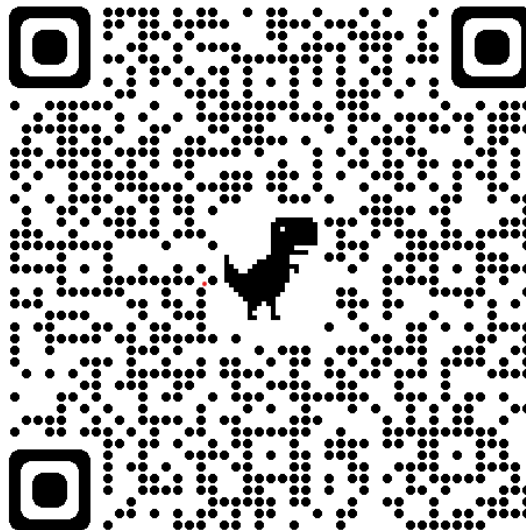
The screenshot shows the Firewall Management Center (FMC) interface. On the left, there is a sidebar with a tree view showing two clusters: 'ngfw-gwlb-cluster (2)' and 'test (1)'. The main area displays a 'Register' dialog box for the 'test (1)' cluster. The dialog box contains the following fields and options:

- Display name:** A text input field.
- Registration Key:** A text input field with a red border.
- Group:** A dropdown menu set to 'None'.
- Access Control Policy:** A dropdown menu.
- Smart Licensing:** A section with a note about performance tier licenses and a link for more information.
- Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):** A dropdown menu set to 'Select a recommended Tier'.
- Advanced:** A section with checkboxes for 'Carrier', 'Malware', 'Threat', and 'URL Filtering'.
- Unique NAT ID:** A text input field.
- Transfer Packets:** A checkbox that is checked.

At the bottom of the dialog box, there is a note: '† Either host or NAT ID is required.' and two buttons: 'Cancel' and 'Register'.

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 as a cluster

Clustering in AWS

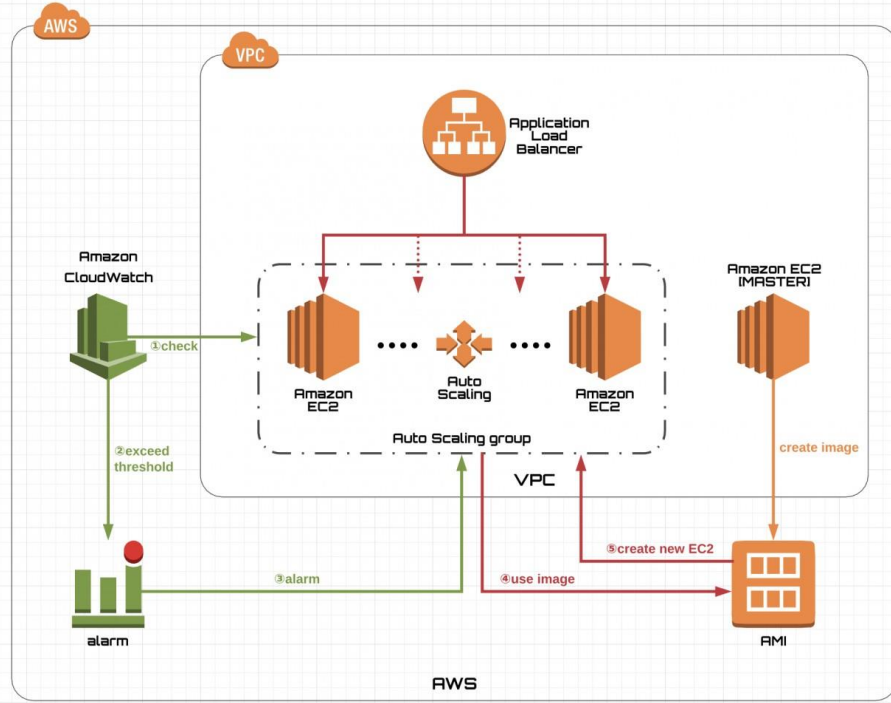


<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/cluster/ftdv-cluster-public.html>

AUTO-SCALING



What about auto-scaling ?



Group details

Desired capacity
1

Minimum capacity
1

Maximum capacity
3

Launch template

Launch template Solar-AS-1-ftd-launch-template	AMI ID ami-0d1a9996bf3d5c6fd	Instance type c5.xlarge
---	---------------------------------	----------------------------

Network

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

Dynamic scaling policies (4)

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-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-ScaleInMempolicy-OHOp5vUkiV0

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-ScaleOutMempolicy-aYakJU45NZ87

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 Lambda Function

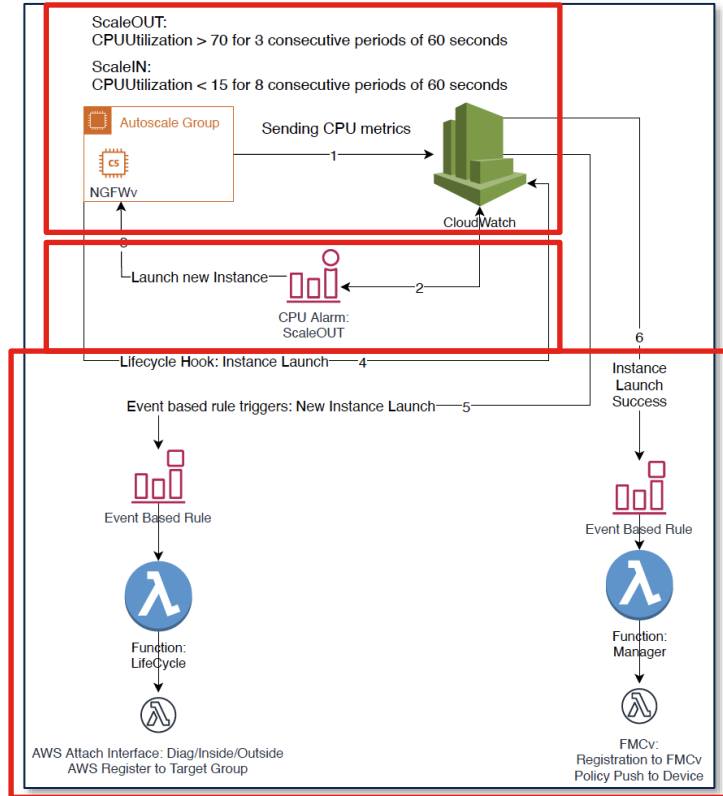
CloudWatch

- 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

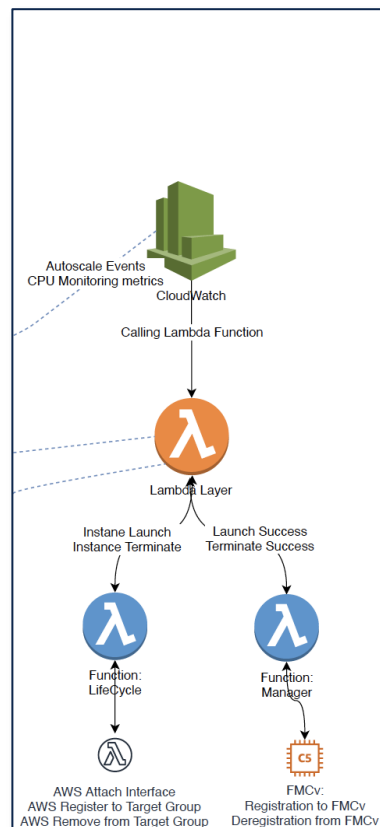
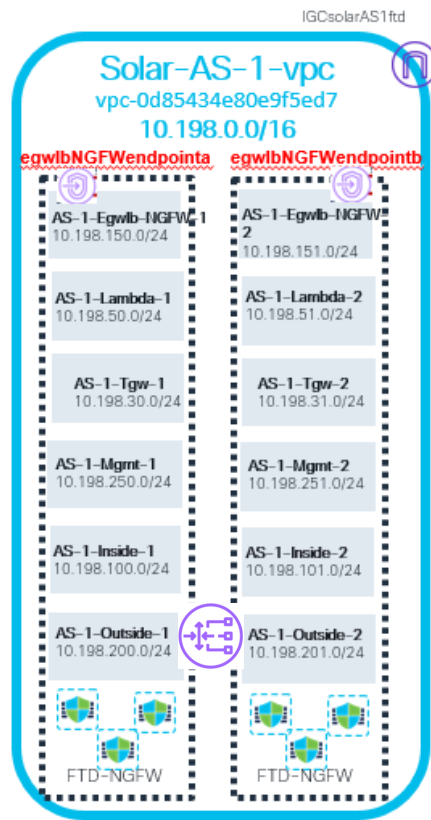
- Serverless architecture of AWS
- No servers to manage for the code
- Built-in fault tolerance
- Automatic-scaling
- Lambda code can interact with AWS infrastructure natively
- Support different languages: Python, Node.js, Ruby, Java, Go, .NET...

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

..	
lambda-python-files	Upgrading python version for AWS autoscale (#29)
templates	Upgrading python version for AWS autoscale (#29)
README.md	Partial Update For 7.2.0. More to follow
deploy-ftdv-auto-scale-for-aws.pdf	Upgrading python version for AWS autoscale (#29)
make.py	Partial Update For 7.2.0. More to follow

How to deploy GWLB with AutoScaling ?

- Clone repository
- Create autoscale_layer.zip

```
#!/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
```

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

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 !

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "fmcIpforDeviceReg": "10.197.100.69",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "aws-asg-policy",
  "fmcNatPolicyName": "AWS-Cisco-NGFW-VMs",
  "fmcInsideNicName": "inside",
  "fmcOutsideNicName": "outside",
  "fmcInsideNic": "TenGigabitEthernet0/0",
  "fmcOutsideNic": "TenGigabitEthernet0/1",
  "fmcOutsideZone": "Outside-sz",
  "fmcInsideZone": "Inside-sz",
  "MetadataServerObjectName": "aws-metadata-server",
  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Inside-sz"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "TenGigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Outside-sz"
      },
      "mode": "NONE",
      "ifname": "outside",
      "name": "TenGigabitEthernet0/1"
    }
  ],
  "trafficRoutes": [
    {
      "interface": "inside",
      "network": "aws-metadata-server",
      "gateway": "",
      "metric": "1"
    }
  ]
}
```

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	Inside-sz	—
Zone	Outside-sz	—

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

AWS-Cisco-NGFW-VMs

Enter Description

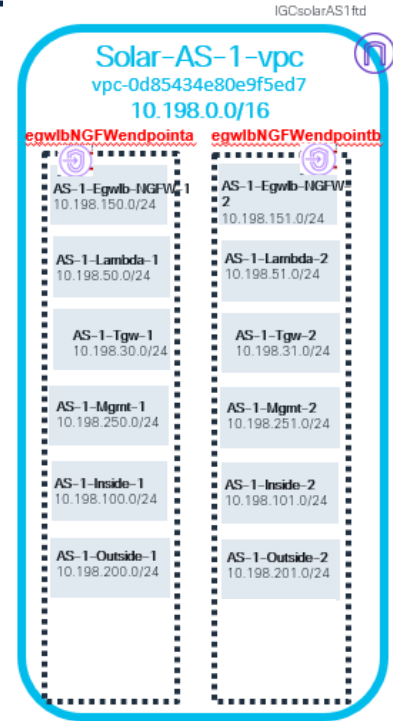
Rules

[Filter by Device](#)  Filter Rules

						Original Packet			Translated Packet		
☐	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
▼ NAT Rules Before											
☐	1		Static	Outside-sz	Inside-sz	 any-ipv4	Interface	 health-check-port	Interface	 aws-metadata-server	 HT

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`



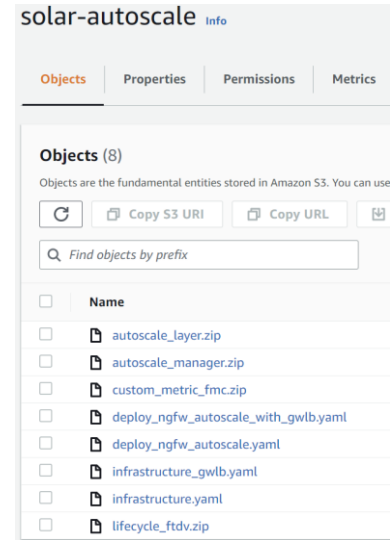
How to deploy GWLB with AutoScaling ?

- 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

..	
lambda-python-files	Upgrading python version for AWS autoscale (#29)
templates	Upgrading python version for AWS autoscale (#29)
README.md	Partial Update For 7.2.0. More to follow
deploy-ftdv-auto-scale-for-aws.pdf	Upgrading python version for AWS autoscale (#29)
make.py	Partial Update For 7.2.0. More to follow

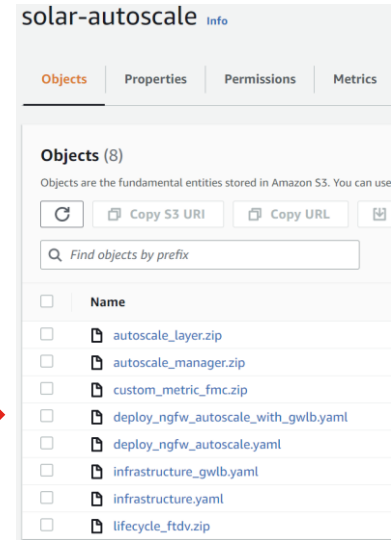
How to deploy GWLB with AutoScaling ?

- 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 ?

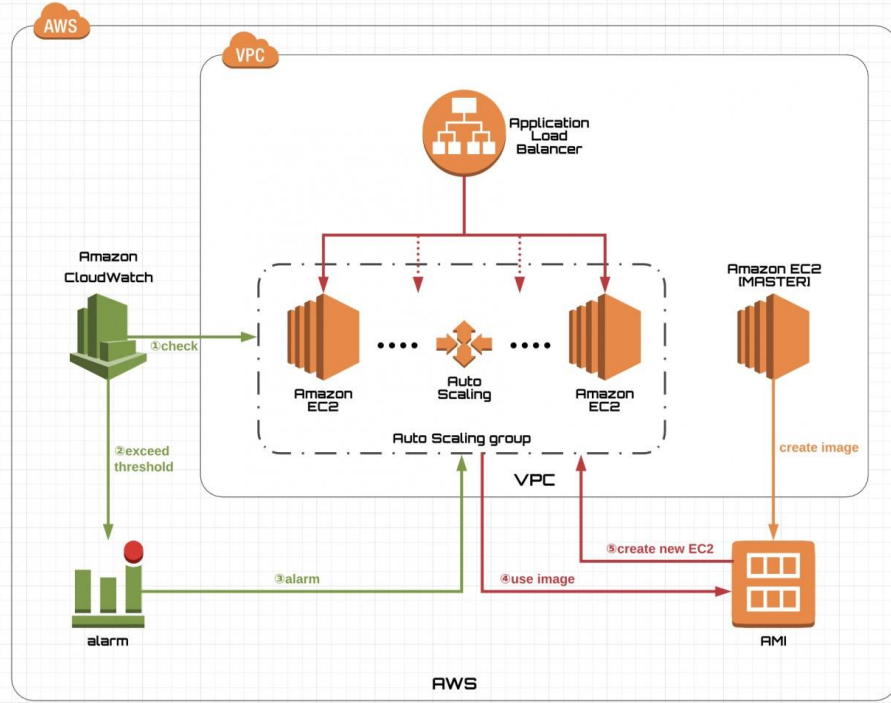
- Clone repository
- Create autoscale_layer.zip
- Tune configuration.json file
- Pre-configure FMC
- Deploy stack in CloudFormation infrastructure_gwlb.yaml
- Use « python3 make.py build » to create all ZIP file needed in Target
- Copy all files in S3 bucket created by infrastructure_gwlb.yaml
- Deploy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

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-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-ScaleInMempolicy-OHOp5vUkiV0

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-ScaleOutMempolicy-aYakJU45NZ87

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

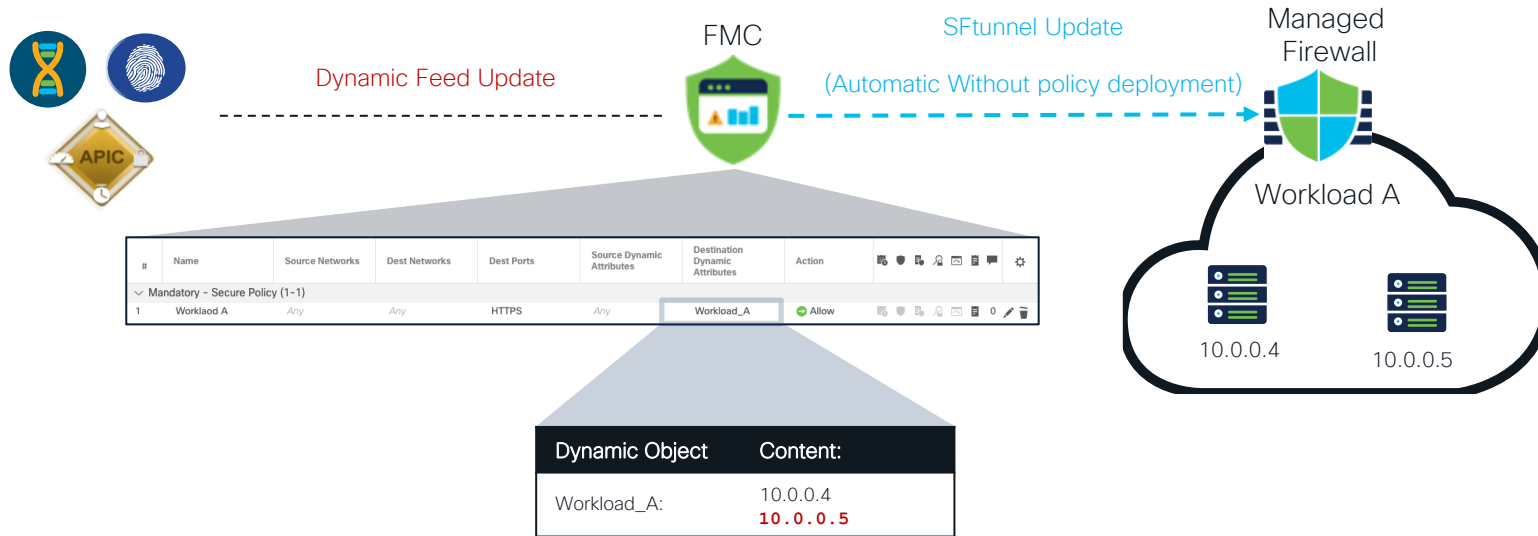


# Problem Statement

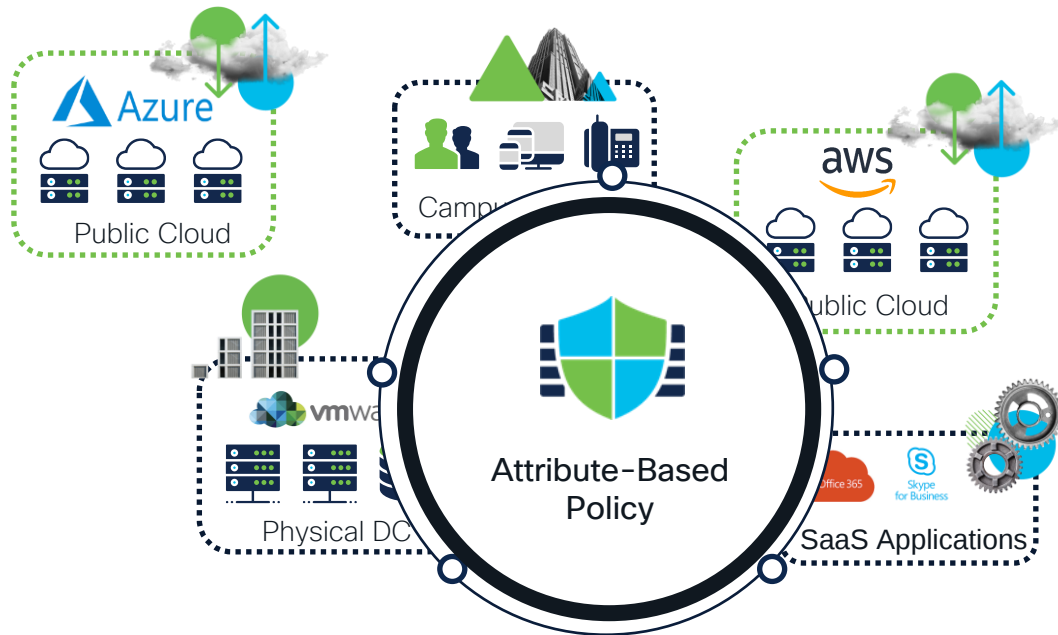
- Application/workload changes happen more often
- Multiple Security domains

# Dynamic Objects in Action

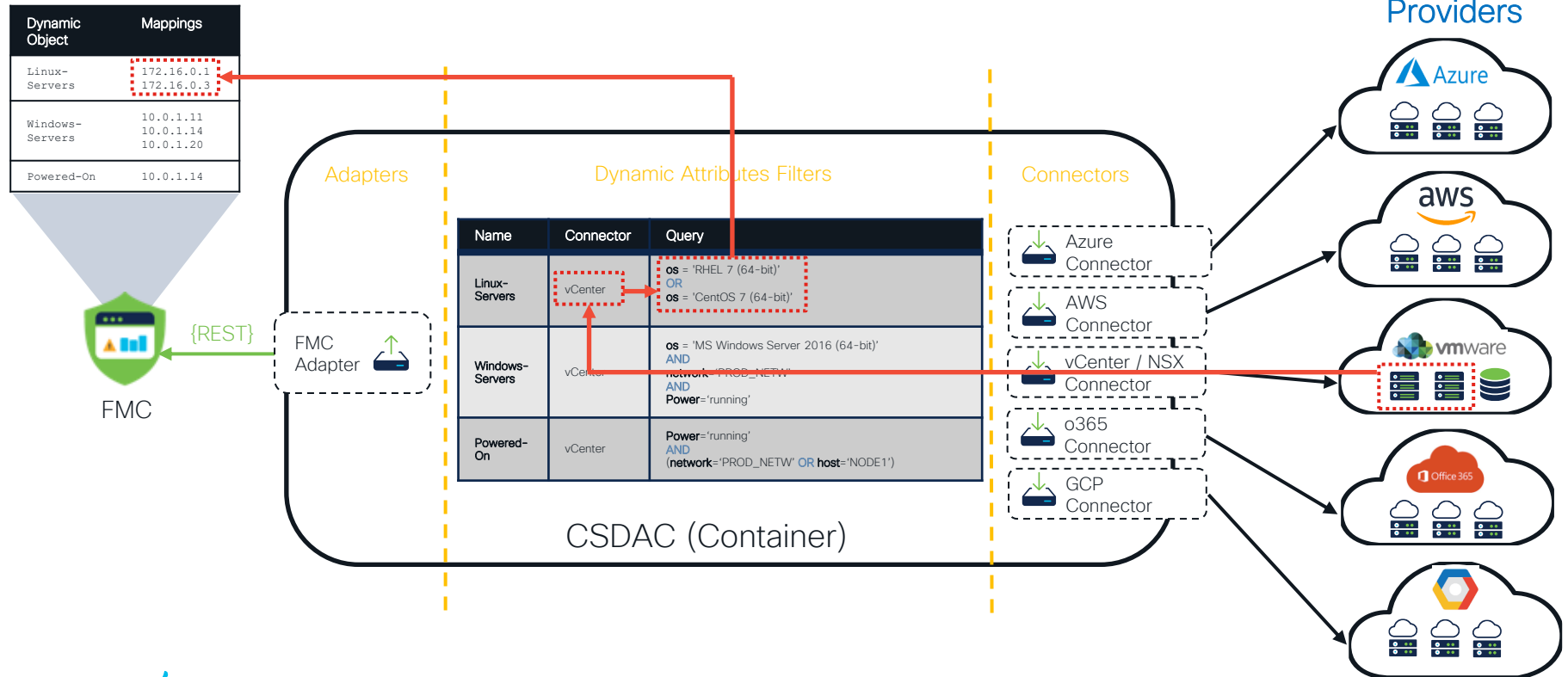
## Automatic Without policy deployment



# 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<br>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<br>-PING<br>Printer_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         | Corporate_VN | External         | Any                    | Any          | Instagram<br>Tinder<br>Twitter   | 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  |

vCenter / NSX  
Dynamic Objects



o365 Public



Public Cloud Tags





# Attribute Based Policy

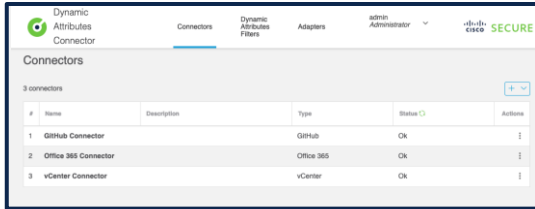
| #                                        | Name                       | Source Zones | Dest Zones       | Users                  | App. Prot.                                            | Dest Ports                           | Source Dynamic Attributes                                                                        | Destination Dynamic Attributes                  | Action  |
|------------------------------------------|----------------------------|--------------|------------------|------------------------|-------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------|---------|
| > Mandatory - Attribute-Based Policy (-) |                            |              |                  |                        |                                                       |                                      |                                                                                                  |                                                 |         |
| v Default - Attribute-Based Policy (1-9) |                            |              |                  |                        |                                                       |                                      |                                                                                                  |                                                 |         |
| 1                                        | Workload_1                 | Any          | Any              | Any                    | Any                                                   | HTTP<br>HTTPS                        | WorkloadObj_615c486dc9                                                                           | WorkloadObj_615c8066483                         | → Allow |
| 2                                        | IoT Support Service        | External     | IoT_VN           | Any                    | 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                                        | Print                      | Corporate_VN | Data_Center_Edge | Any                    | Any                                                   | SNMP<br>ICMP-PING<br>Spooler_Service | RICOH-Afcio-SP-C410DN<br>RICOH-Afcio-SP-C820DN<br>Xerox-WorkCentre-5030<br>Xerox-WorkCentre-5135 | APIC_A_ESG_Print_Servers                        | → Allow |
| 5                                        | Block Social Media         | Corporate_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 diagram illustrates the configuration of attribute-based policies. It features a table of policies with columns for Name, Source Zones, Dest Zones, Users, App. Prot., Dest Ports, Source Dynamic Attributes, Destination Dynamic Attributes, and Action. Red dashed boxes highlight specific attributes and actions. Red arrows point from icons to specific attributes or actions. The icons include a document, a magnifying glass, a location pin, a person, a SecureX logo, a camera, a tag, and logos for VMware, APIC, Office 365, AWS, and Azure.

# The New Cloud Form Factor



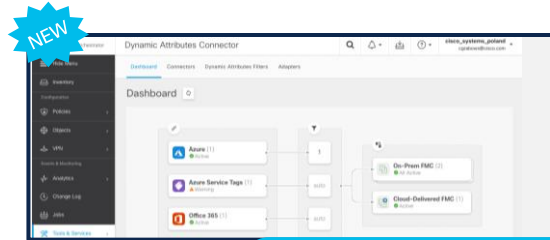
CSDAC  
(Linux Machine)



Standalone

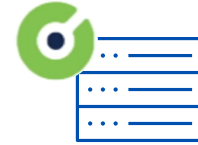


CSDAC in CDO's  
Tools & Services

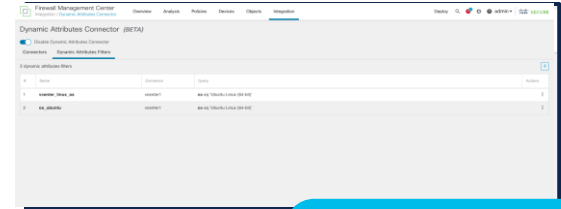


No separate VM  
required!!

Cloud Delivered



CSDAC in FMC



Coming Fall 2023

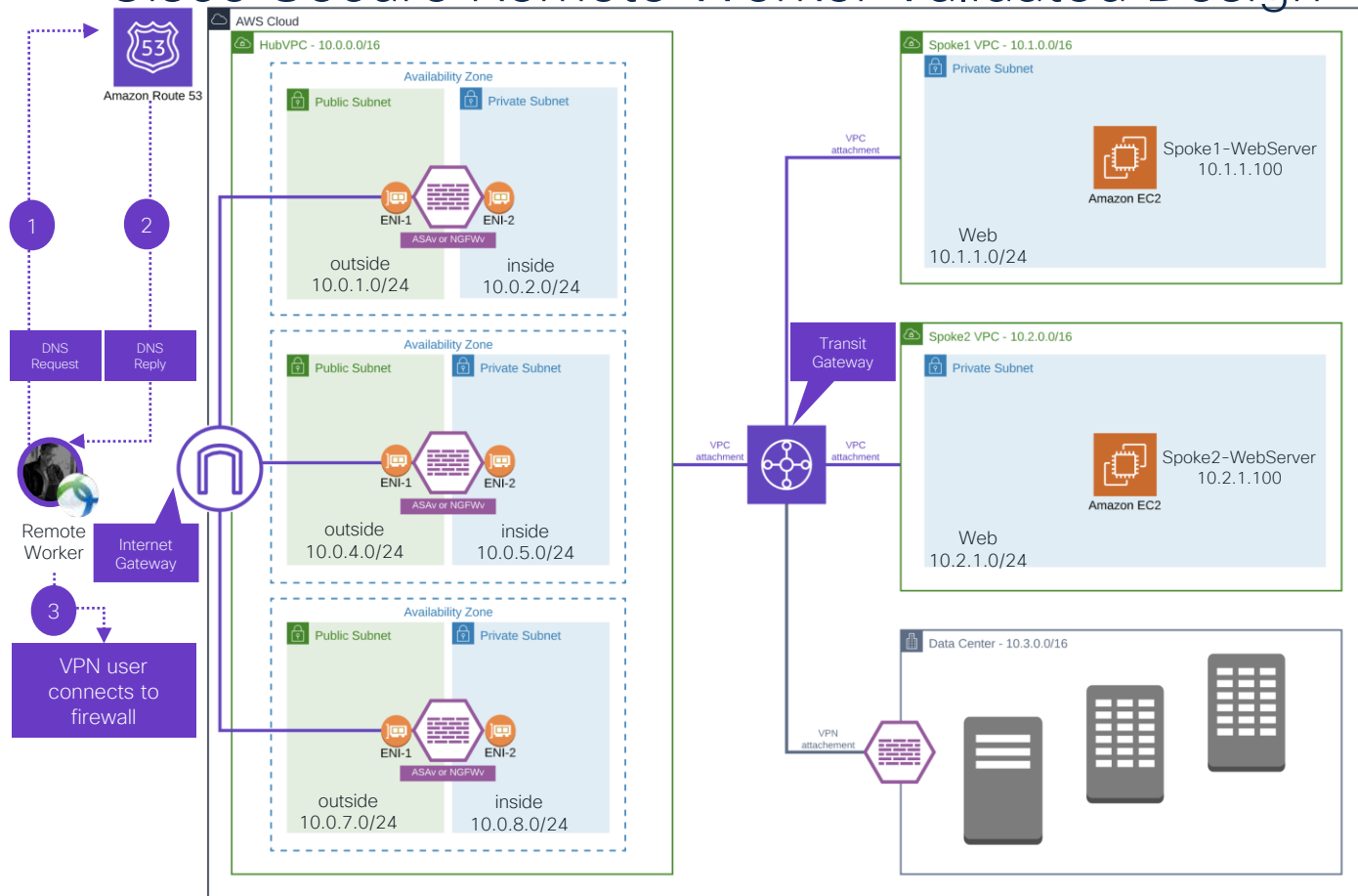
Built In

# 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

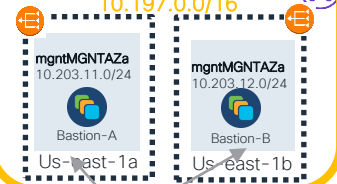
Transit Gateway connects to Data Center using VPN attachment

## mgntTableMGNT

10.201.0.0/16 → mgnytgtVPCattachment  
10.202.0.0/16 → mgnytgtVPCattachment  
10.204.0.0/16 → mgnytgtVPCattachment  
10.200.0.0/16 → mgnytgtVPCattachment  
0.0.0.0/0 → IGClusterAPP

## POD1 - AutoScaleFMC

vpc-0f1b9a1aa941b1fcf  
10.197.0.0/16



POD1 - VPC-  
AutoScale-FMC-IGW

IGClusterNGFW

## tgwrouteRAVPN

10.199.1.0/24 → insideRAVPNENIA  
10.199.2.0/24 → insideRAVPNENIB  
0.0.0.0/0 → ravpntgtVPCattachment

## insARouteTableRAVPN

10.201.0.0/16 → TGW-attach-VPC-ravpn  
10.204.0.0/16 → TGW-attach-VPC-ravpn

## insBRouteTableRAVPN

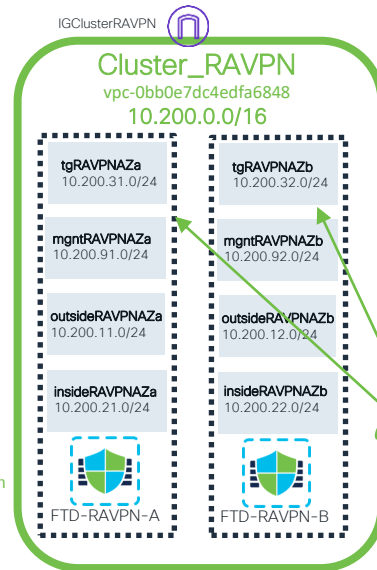
10.201.0.0/16 → TGW-attach-VPC-ravpn  
10.204.0.0/16 → TGW-attach-VPC-ravpn

## mgntRouteTableRAVPN

0.0.0.0/0 → IGClusterRAVPN  
10.203.0.0/16 → TGW-attach-VPC-ravpn

## outsideAZa TableRAVPN

0.0.0.0/0 → IGClusterRAVPN



## TGW MGN

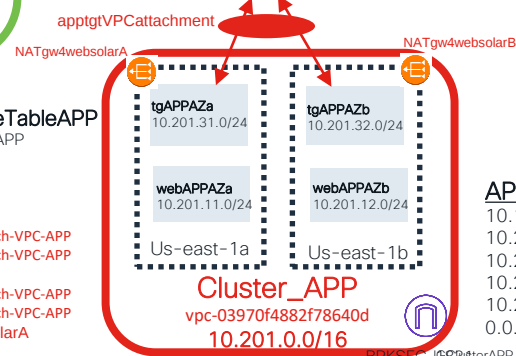
10.202.0.0/16 → ngfwtgtVPCattachment  
10.200.0.0/16 → ravpntgtVPCattachment  
10.201.0.0/16 → apptgtVPCattachment  
10.204.0.0/16 → vpnroutertgtVPCattachment

## TGW\_sec

10.199.0.0/16 → ravpntgtVPCattachment  
10.200.0.0/16 → ravpntgtVPCattachment  
10.201.0.0/16 → apptgtVPCattachment  
10.203.0.0/16 → mgnytgtVPCattachment

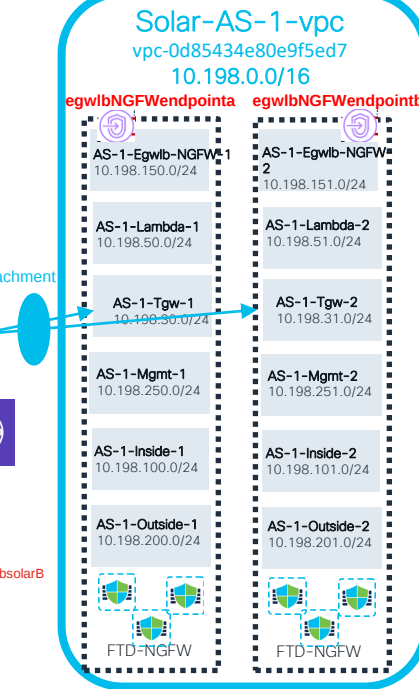
## TGW SPOKE

0.0.0.0/0 → ngfwtgtVPCattachment  
10.203.0.0/16 → mgnytgtVPCattachment



## APP rt web Aza

10.199.0.0/16 → TGW-attach-VPC-APP  
10.200.0.0/16 → TGW-attach-VPC-APP  
10.201.0.0/16 → LOCAL  
10.203.0.0/16 → TGW-attach-VPC-APP  
10.204.0.0/16 → TGW-attach-VPC-APP  
0.0.0.0/0 → NATgw4websolarA



## APP rt web Azb

10.199.0.0/16 → TGW-attach-VPC-APP  
10.200.0.0/16 → TGW-attach-VPC-APP  
10.201.0.0/16 → LOCAL  
10.203.0.0/16 → TGW-attach-VPC-APP  
10.204.0.0/16 → TGW-attach-VPC-APP  
0.0.0.0/0 → NATgw4websolarA

## egwlbendpointRouteNGFW

10.202.101.0/24 → LOCAL  
0.0.0.0 → ngfwtgtVPCattachment

## tgAZa RouteNGFW

10.202.0.0/16 → LOCAL  
0.0.0.0/0 → egwlbNGFWendpoints  
10.203.0.0/16 → ngfwtgtVPCattachment

## tgAZb RouteNGFW

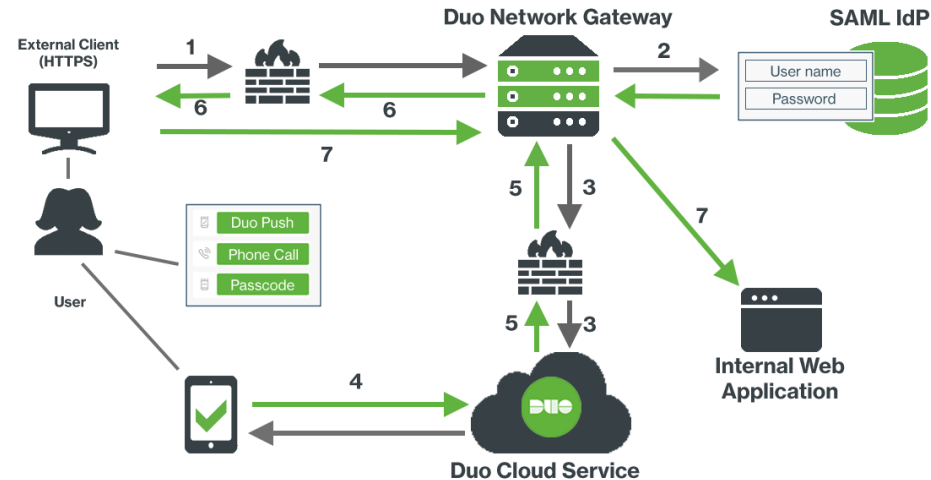
10.202.0.0/16 → LOCAL  
0.0.0.0/0 → egwlbNGFWendpoints  
10.203.0.0/16 → ngfwtgtVPCattachment

## mgntTableNGFW

10.203.0.0/16 → mgnytgtVPCattachment  
0.0.0.0/0 → IGClusterAPP

# What is Duo Network Gateway ?

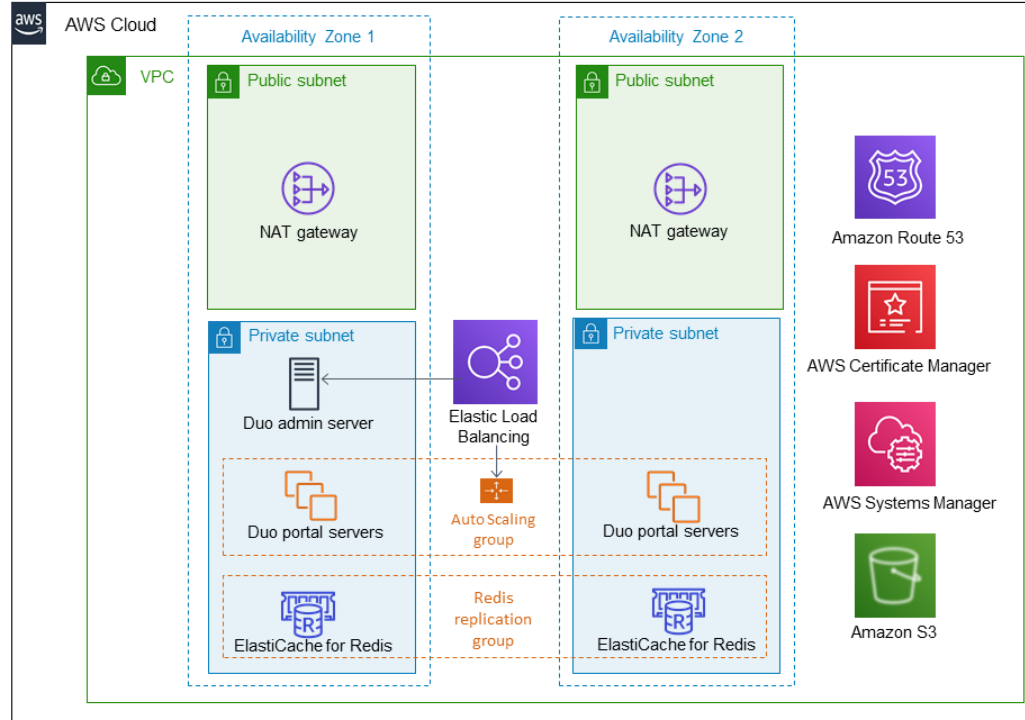
The Duo Network Gateway enables organizations to provide **Zero Trust Remote** Access to web applications, Remote Desktop or SSH servers **without the requirement of a VPN**.



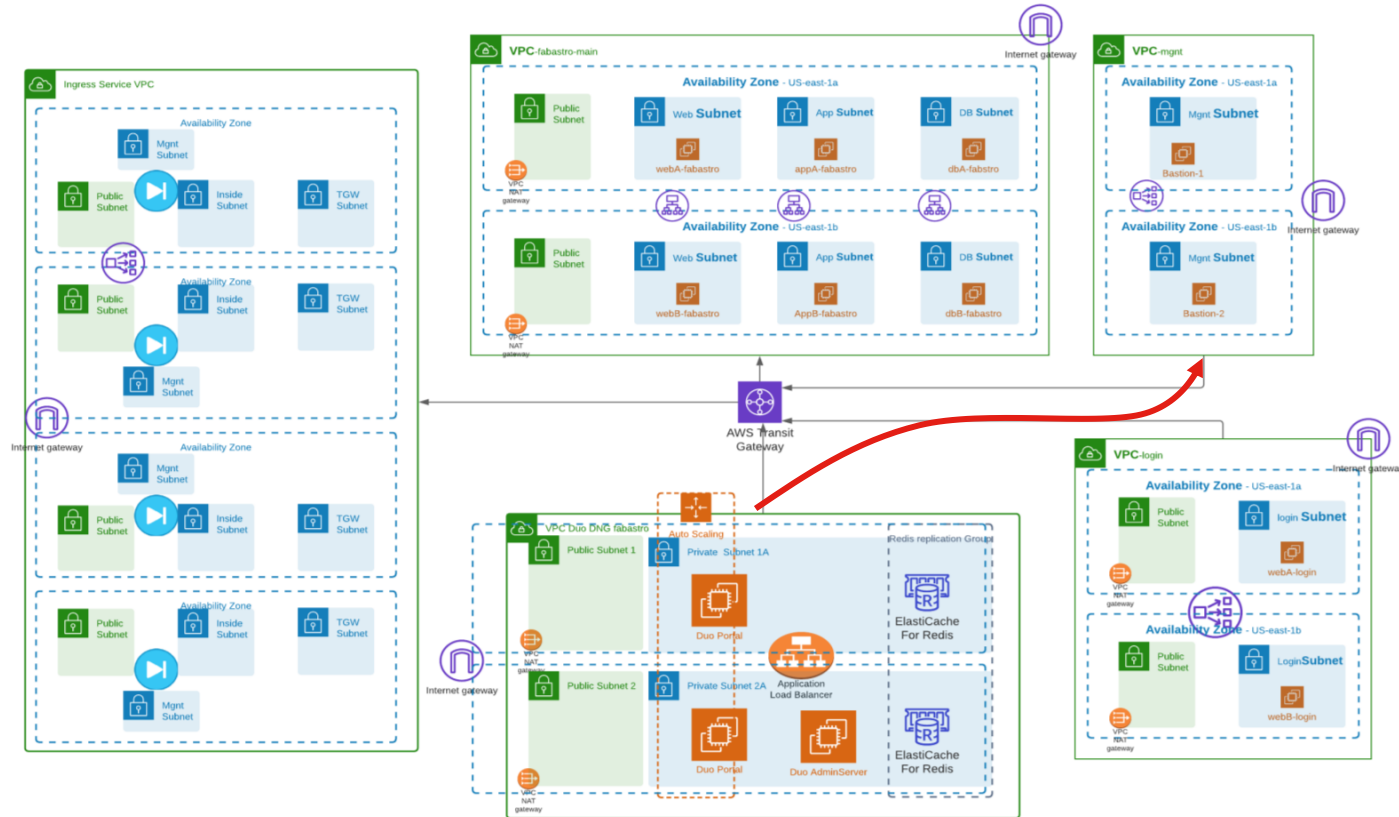
# DNG Use Cases for FabAstro...or else

- 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.

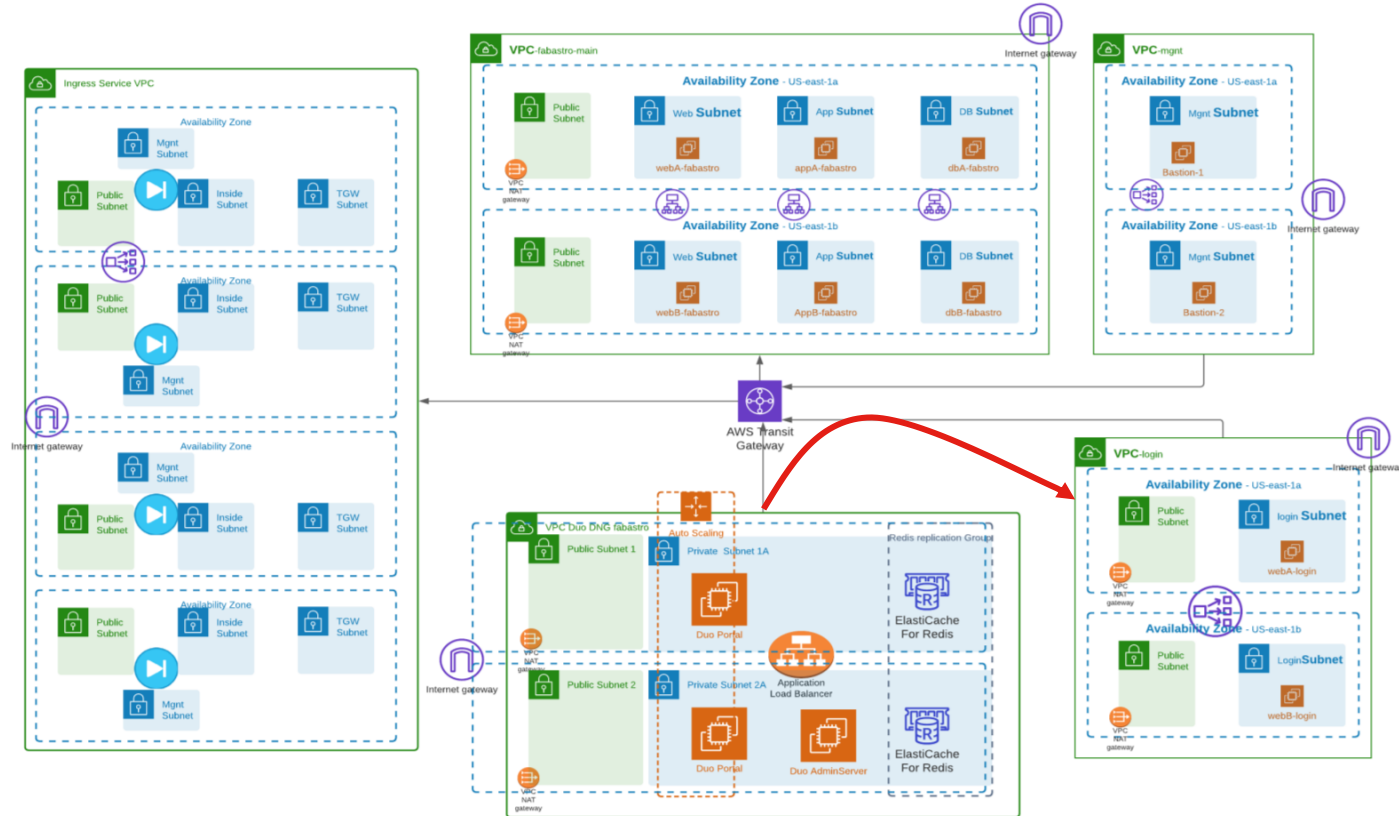
# What the CloudFormation Deploys



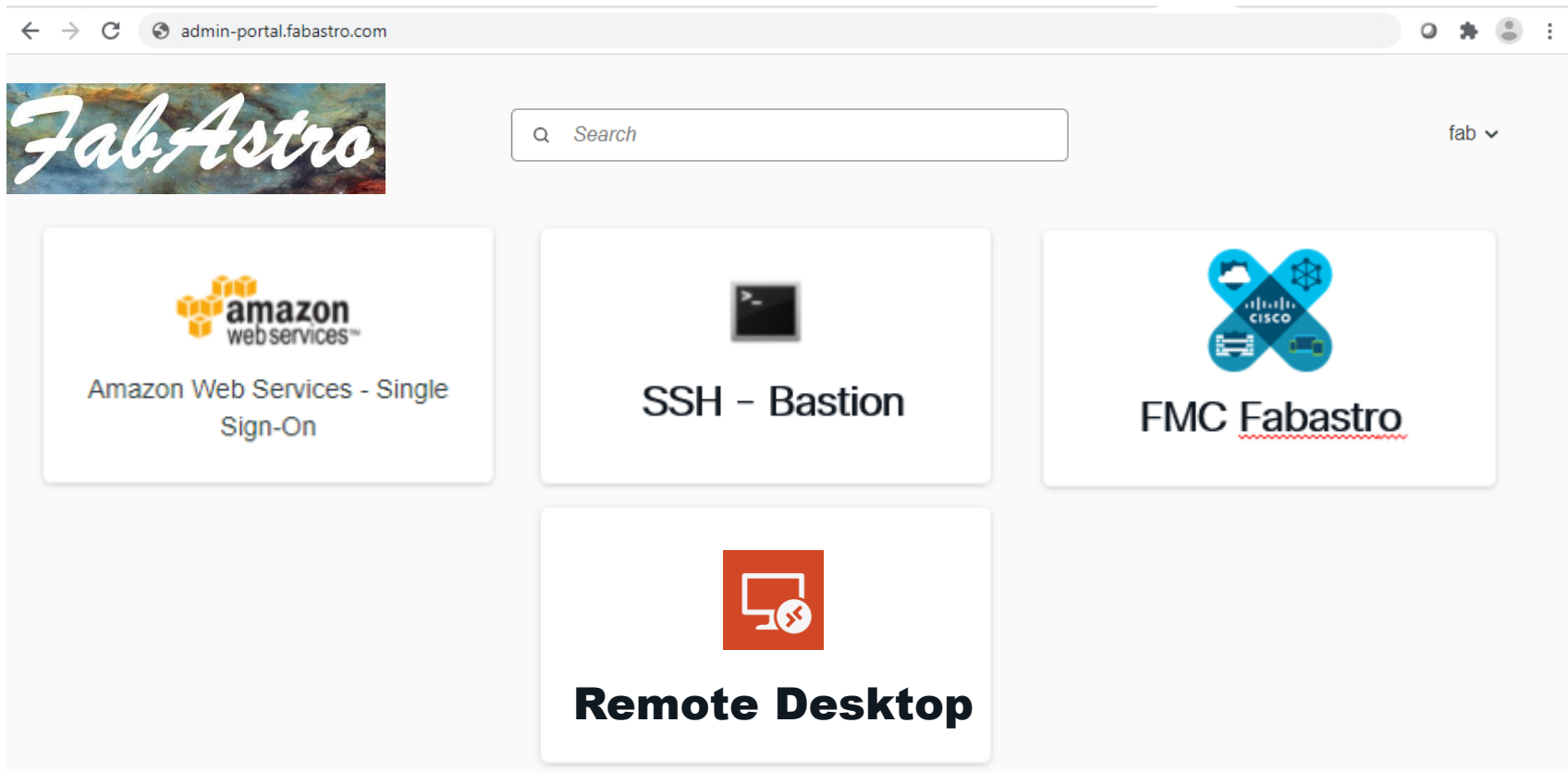
# DNG in FabAstro: Access for Admins



# DNG in FabAstro: Web portal for Privileged Users



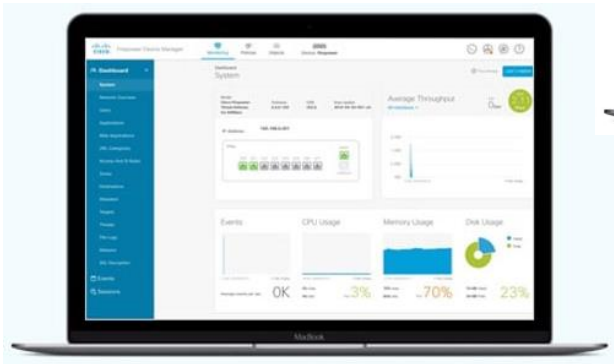
# Using DNG to access FabAstro Admin Portal



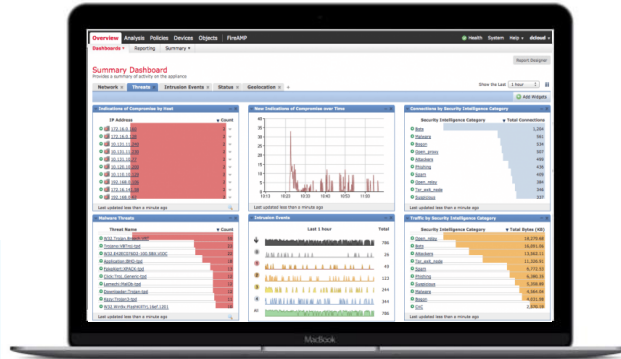
# Management and automation



# How do I manage my FTDs ?

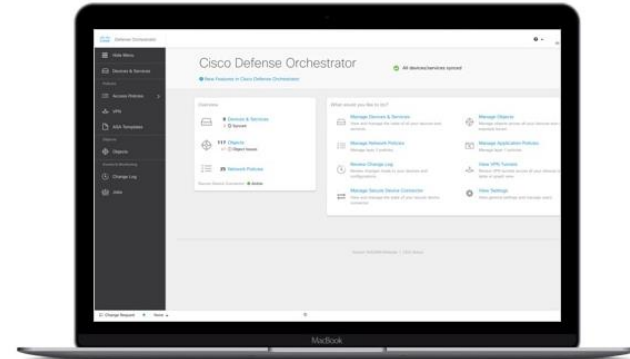


FDM



## 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>

**CISCO** *Live!*



# Security through visibility

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



# 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**

# 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

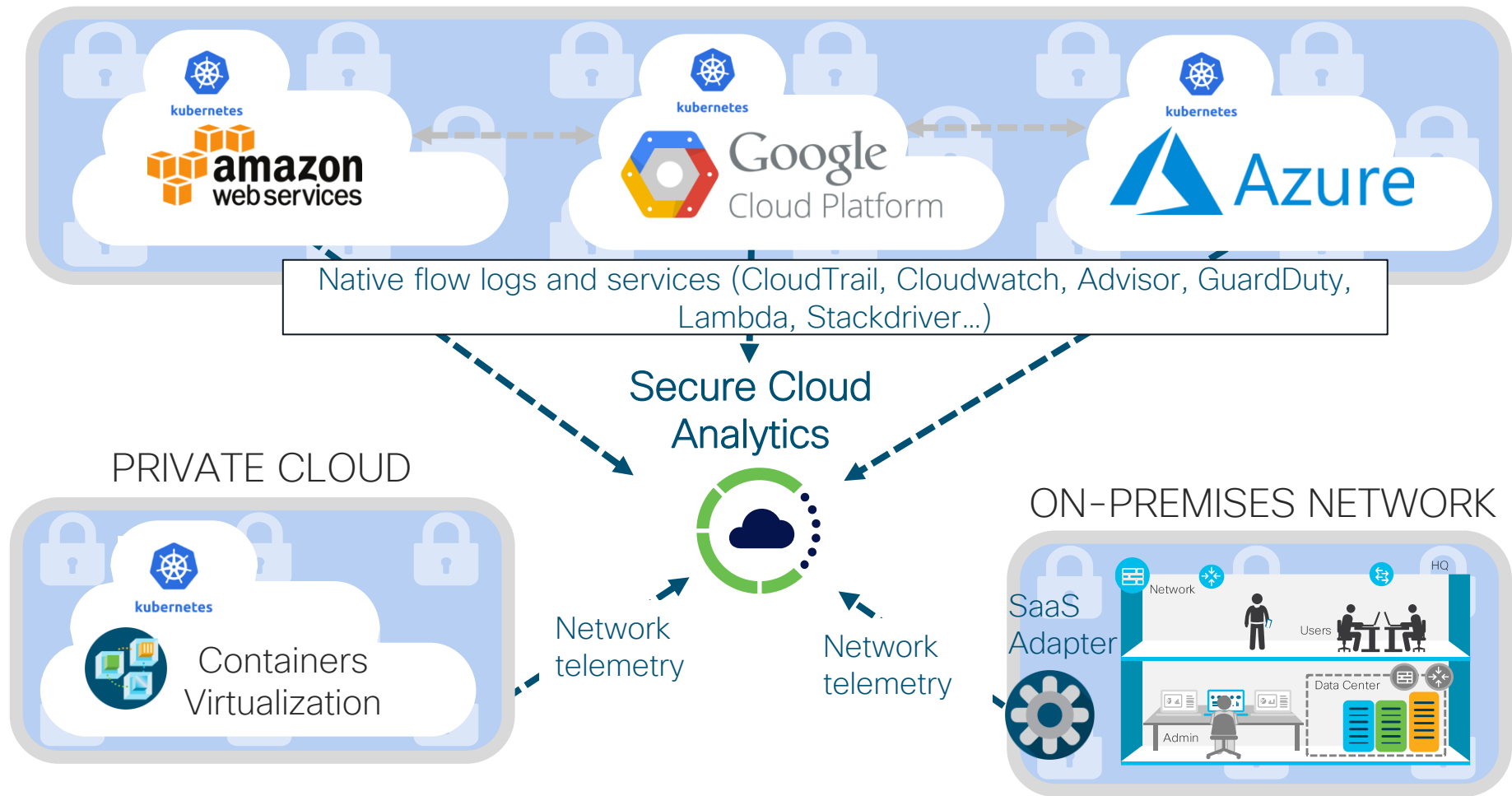
# AWS GuardDuty

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

# & Secure Cloud 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



Configuration Risk Exposure



User, System, Event Risk Exposure



Network Segmentation Risk Exposure



Behavioral Threat Detection

## Cloud Security Maturity

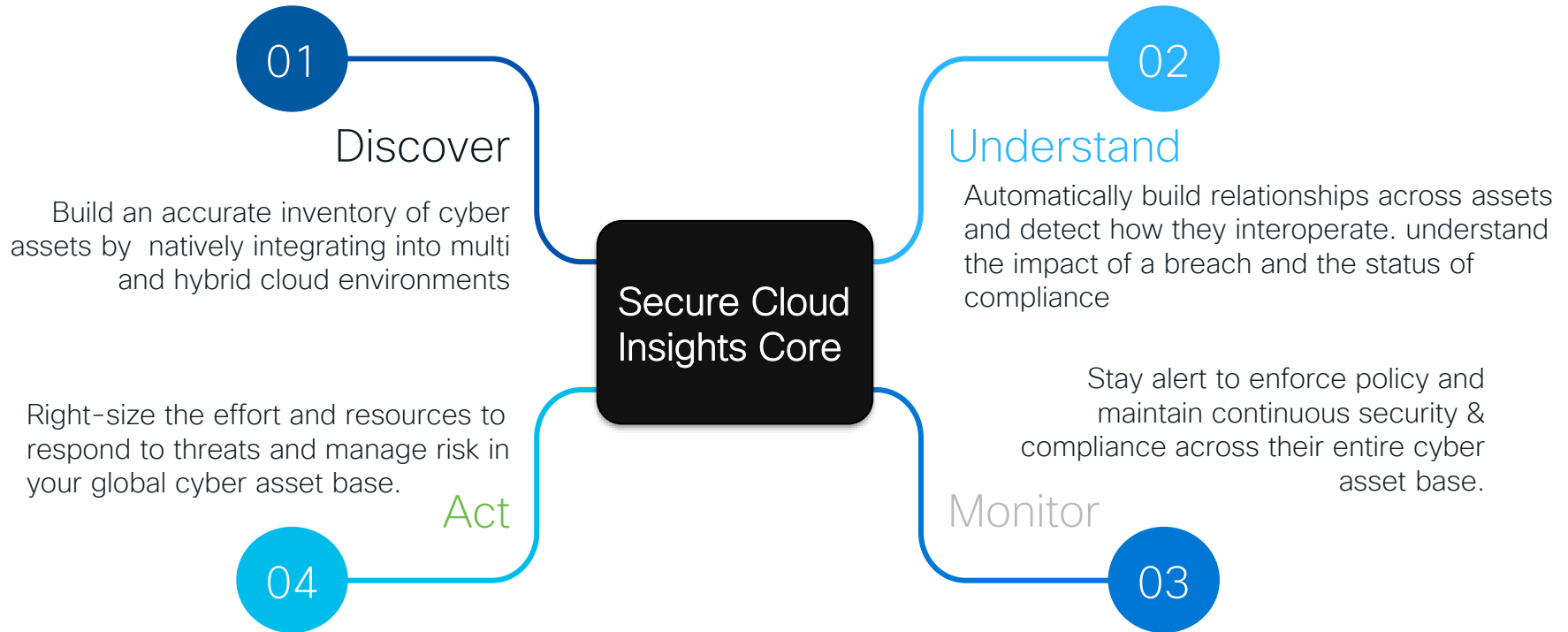


- **Visibility**  
What do we have, and how important is it to our business?
- **Compliance**  
Am I following best practices and regulatory guidelines?
- **Security Posture**  
Are resources being locked down properly?
- **Internal Policy**  
Are resources & users following our established guidelines?
- **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

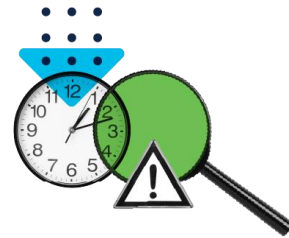


### Complete visibility into your security posture

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



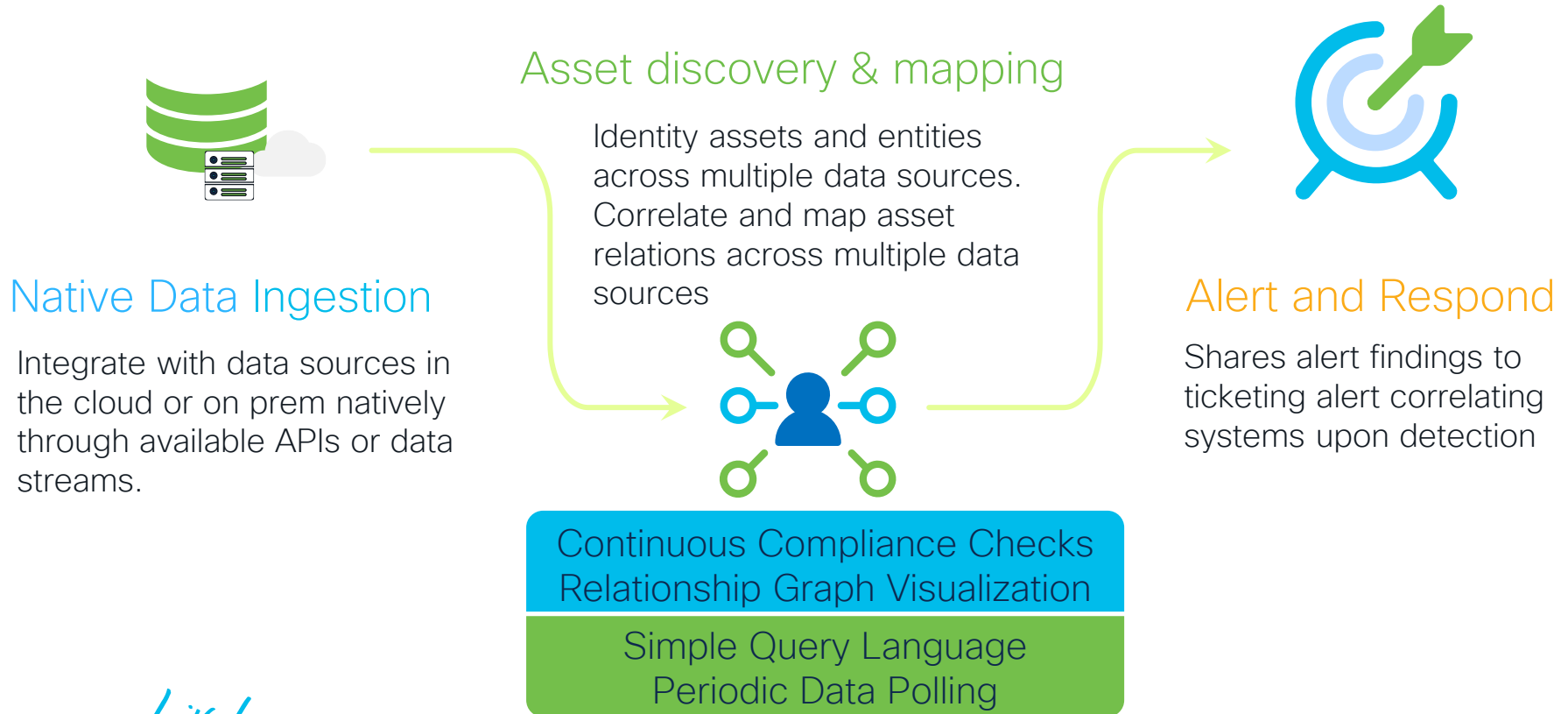
### Attack Surface Management

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

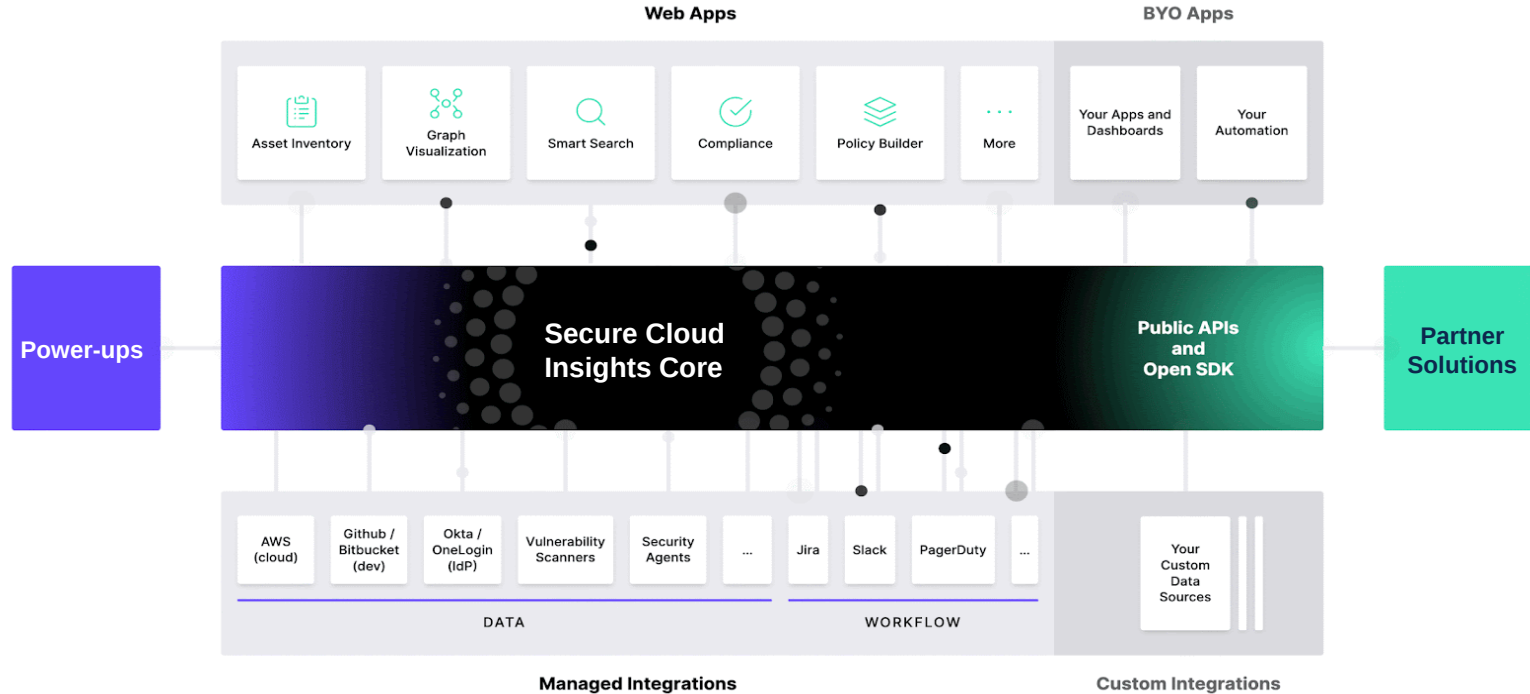
Identify the root cause – how did the attacker access assets

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

# Secure Cloud Insights High level Architecture



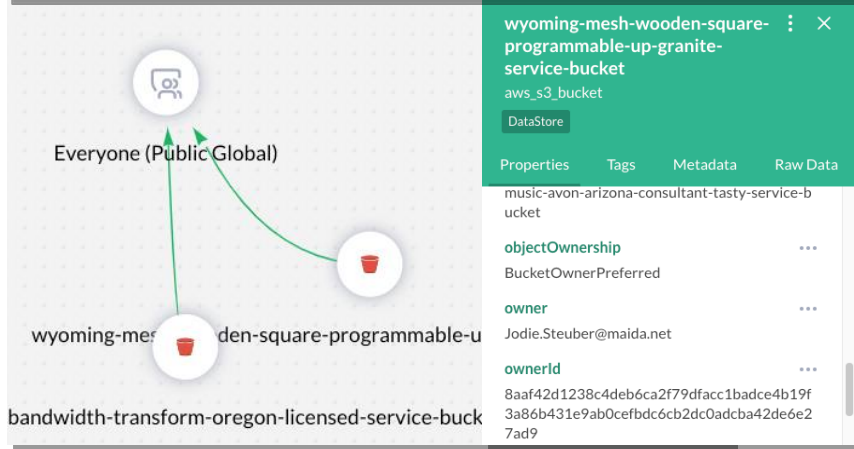
# API First and Cloud Native



# Query Through Use Cases

**QUESTION** Is public access enabled for any S3 Bucket?

**QUERY** Find aws\_s3\_bucket with classification = 'public'



| Properties                                                                        | Tags | Metadata | Raw Data |
|-----------------------------------------------------------------------------------|------|----------|----------|
| music-avon-arizona-consultant-tasty-service-bucket                                |      |          |          |
| objectOwnership                                                                   |      | ...      |          |
| BucketOwnerPreferred                                                              |      |          |          |
| owner                                                                             |      | ...      |          |
| Jodie.Steuber@maida.net                                                           |      |          |          |
| ownerId                                                                           |      | ...      |          |
| 8aaf42d1238c4deb6ca2f79dfacc1badce4b19f3a86b431e9ab0cefbdc6cb2dc0adcb442de6e27ad9 |      |          |          |



Incident Scope and Response



Compliance Check

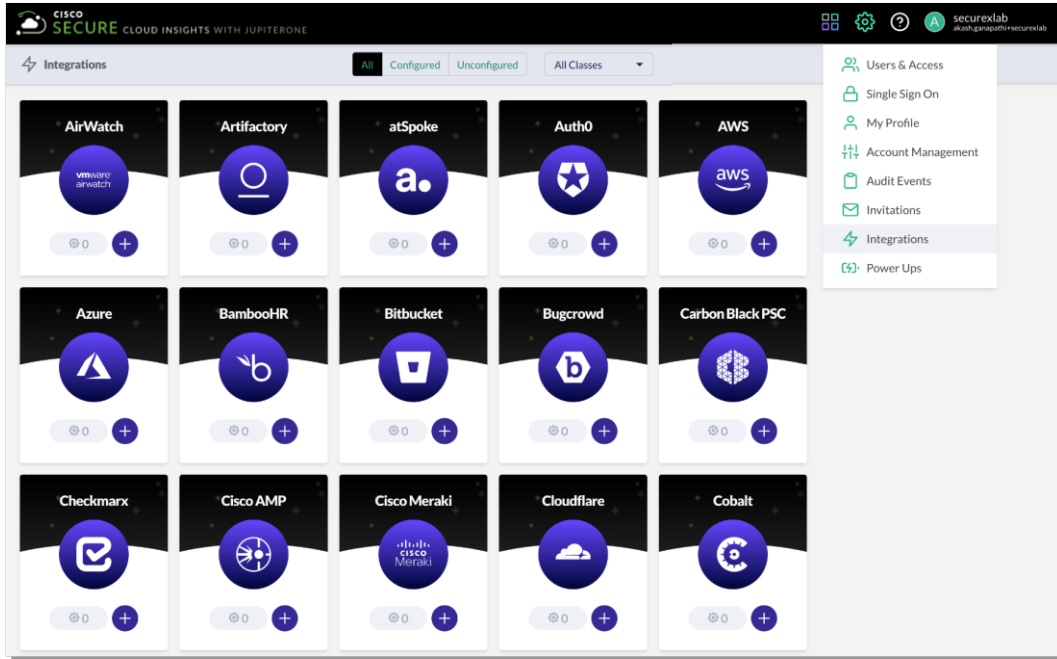


Attack Surface Management



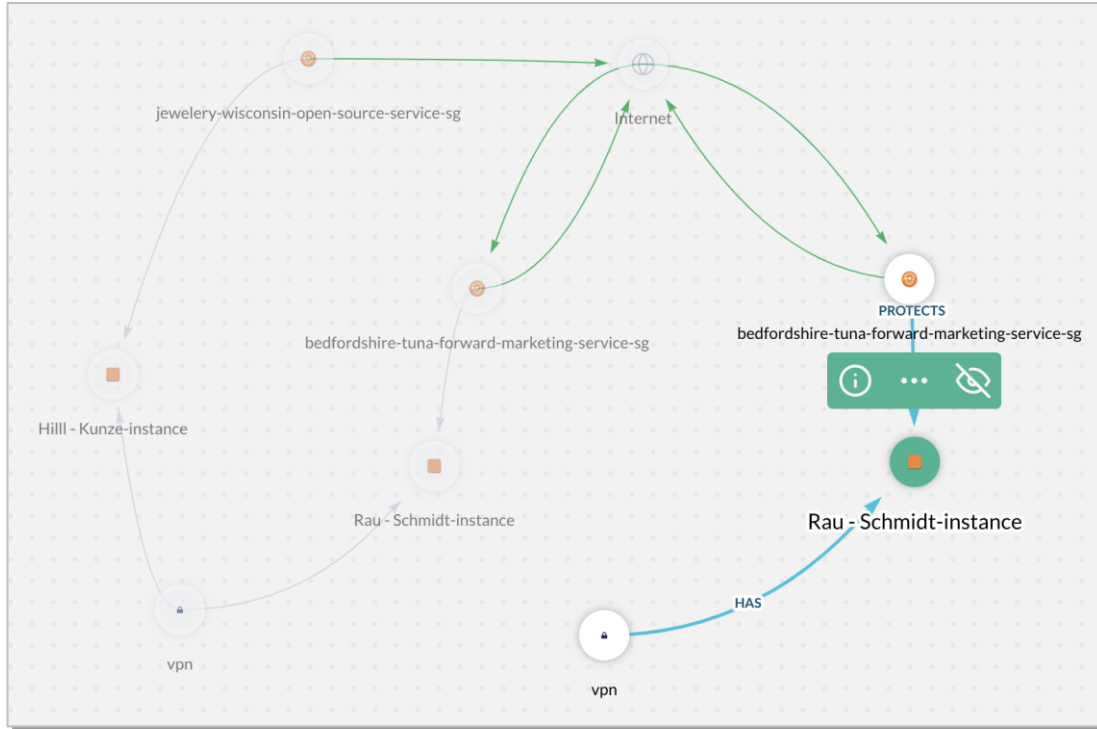
Configuration Change Detection

# 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

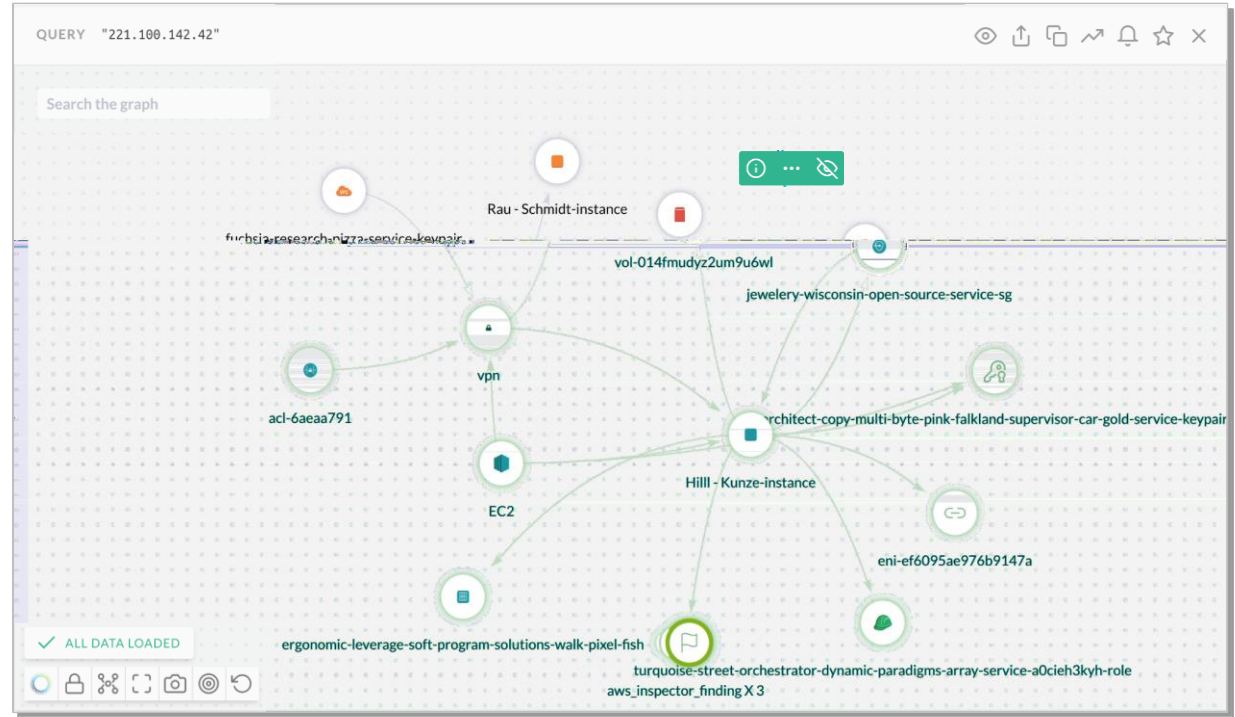
# Relationship Mapping



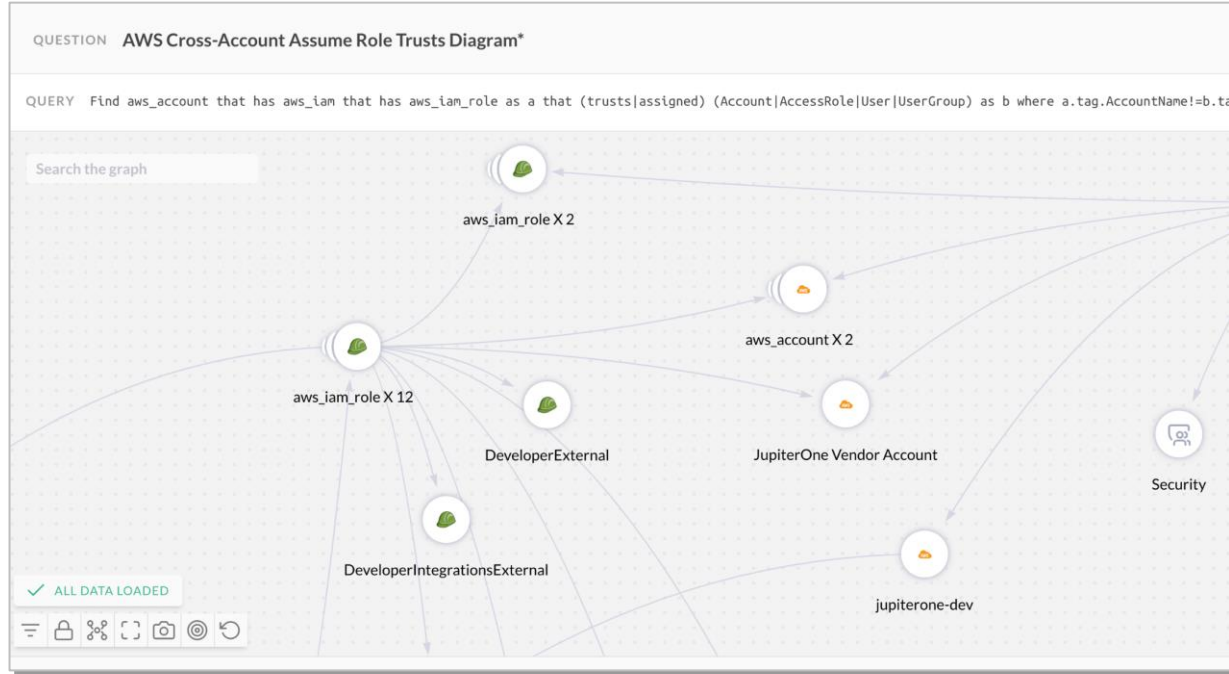
- Relationships between assets are discovered via the integrations and are mapped together automatically
- Here we see:
  - Security groups allowing access to the internet
  - The instances they protect
  - The subnets those instances are on

# 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

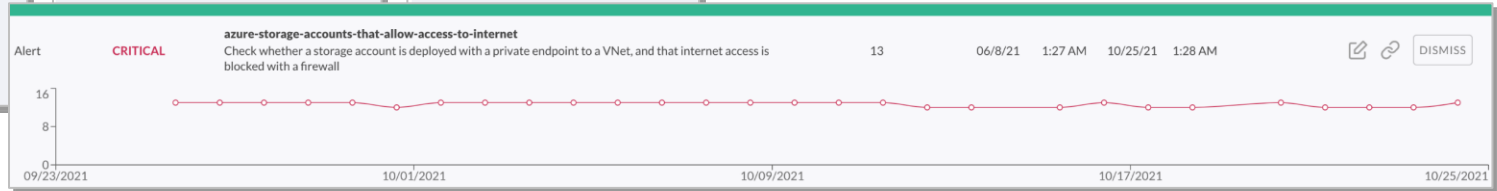


- Complex relationships cross-account trusts, vpc peering, vpc endpoint policies, IAM policies, load balancer configurations, and more are all automatically discovered
- Discover the cross environment “Blast Radius” and the risk of a threat propagating across cloud accounts

# 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

« The speaker BUTCHERED english ! »

« Best session of the week but it is only the first day... »

« The chairs ain't suitable for long session. »

« Room temperature would have been perfect ... if i was a PINGUIN !»

« Could you teach English to my husband speaking with your sexy accent ? »

« They should create a 6th star for you »

# Key Takeaways

- 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](https://ciscolive.com/on-demand).



The bridge to possible

# Thank you

CISCO *Live!*

CISCO *Live!*

ALL IN