TURN IT UP

cisco Live!

#CiscoLive

The bridge to possible

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

Fabien Gandola – TSA Cyber Security for EMEA

BRKSEC-1041

What to expect and not to expect ?

- No deep dive AWS
- No deep dive Security
- No all scenarios (no EKS or lambda)
- Visibility and advanced session in BRKSEC-3008 and BRKSEC-2044

- 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
- Use case of today
- What type of service and architecture to deploy my application ?
- How do I perform access control and Segmentation ?
- How do I insert NGFW ?
- What about Remote Access ?
- Some extra steps
- Conclusion

About me...

Fabien Gandola – fgandola@cisco.com

TSA Cyber Security EMEAR

21 years in Cisco

TAG leader of Cloud Native Security and Application Security

The Use Cases

- Enterprise with on prem DC launching a new service

- New company

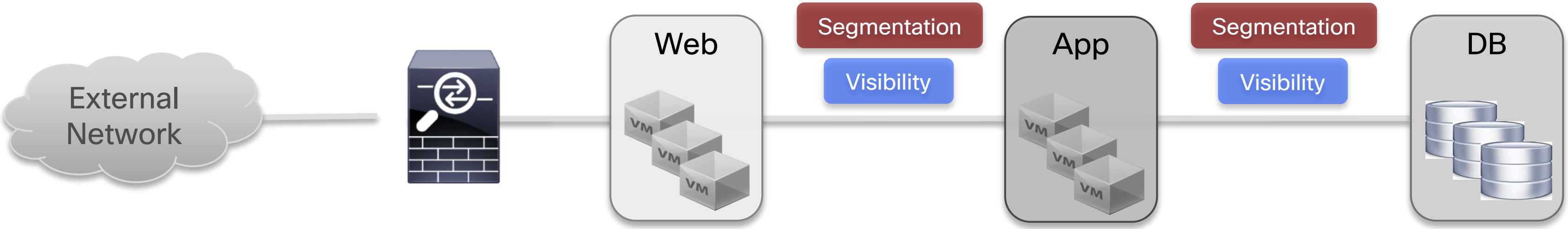
The application

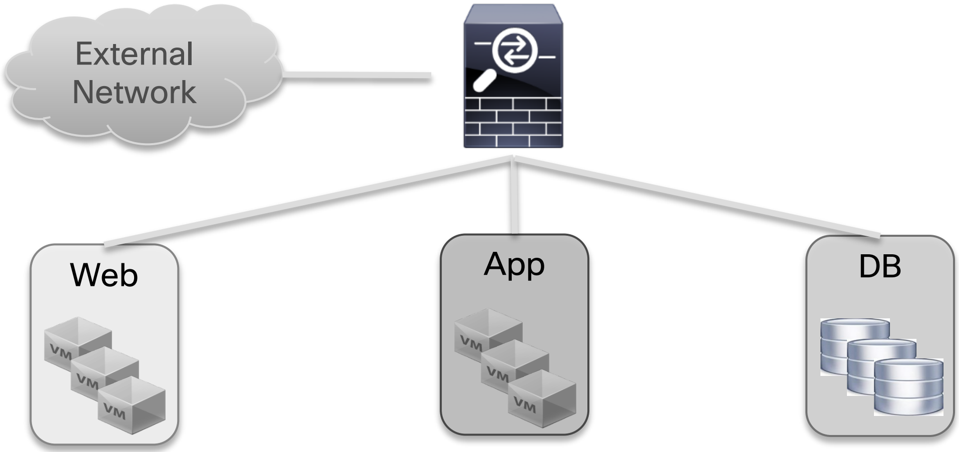
- FabAstro (store images)
  - Public can access images
  - Users can add their images
  - Admin manage the app
- 3 tiers:
  - Static Web page
  - Dynamic part with web + php and business logic
  - Database with mysql

"To confine our attention to terrestrial matters would be to limit the human spirit."

- Stephen Hawking, Astrophysicist

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



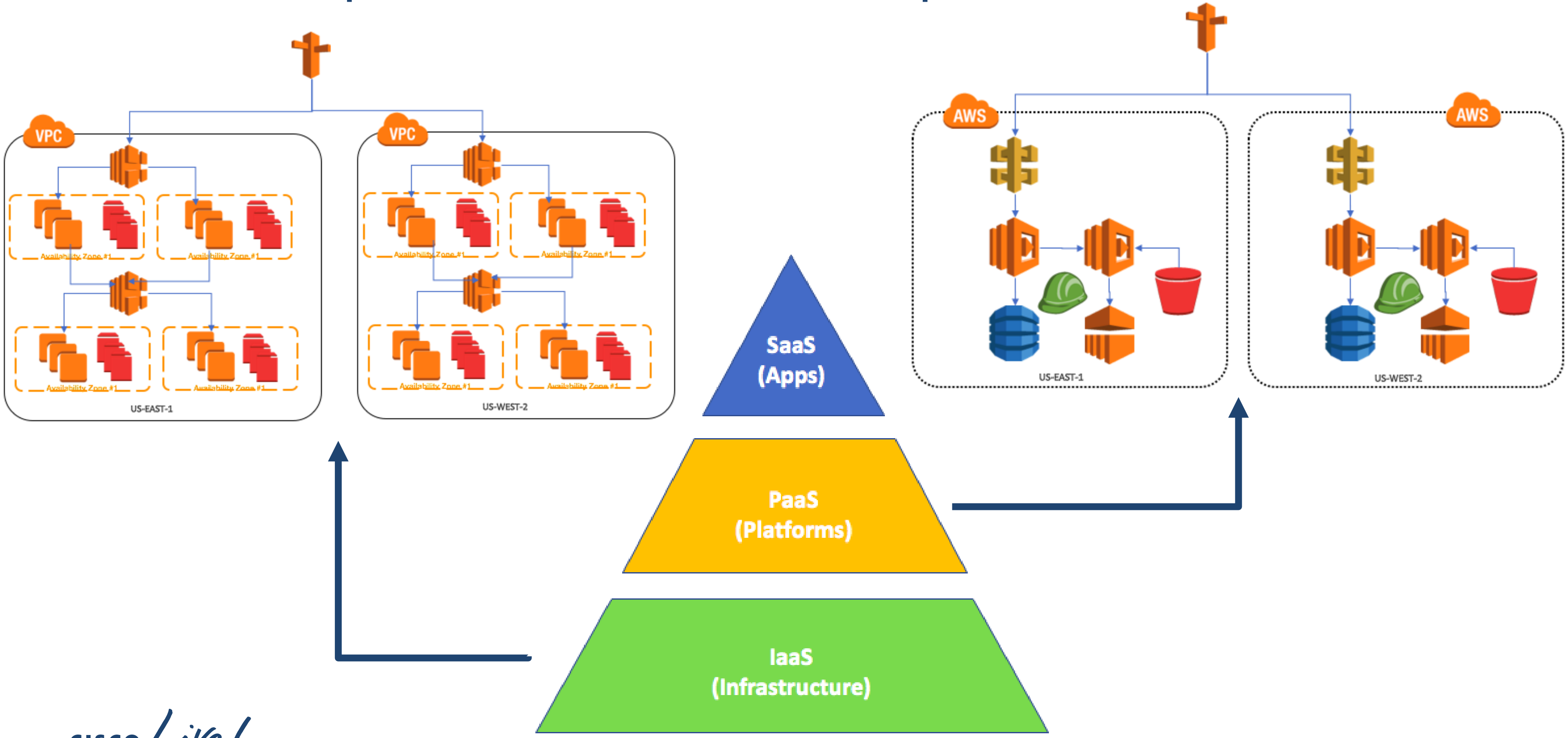


What type of service and architecture to deploy my application ?

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

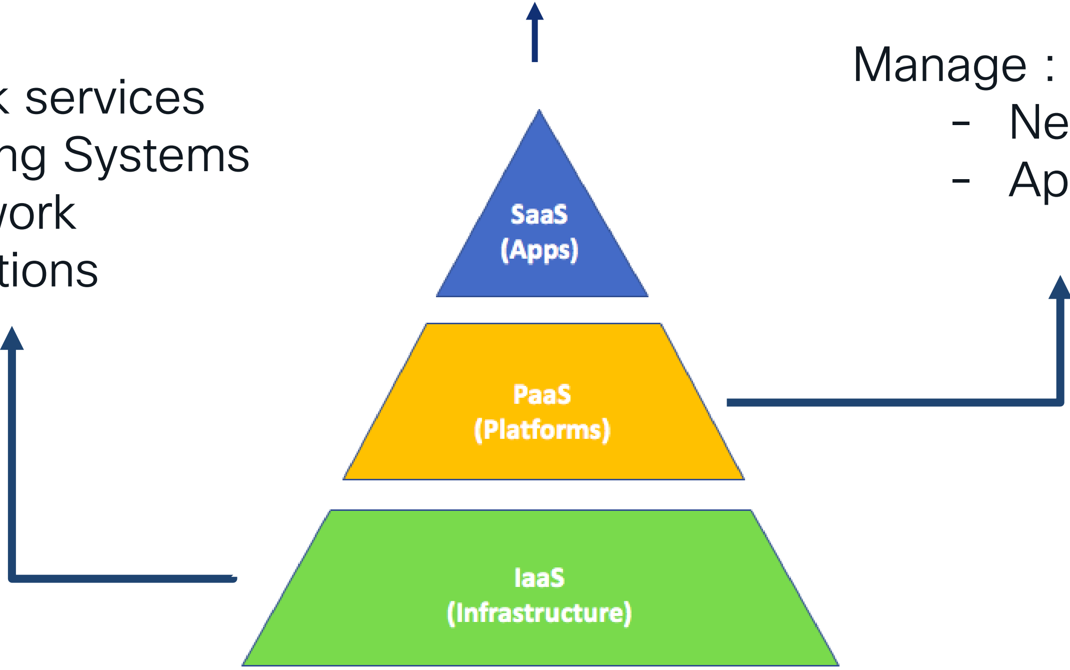


SaaS (Apps)

PaaS (Platforms)

IaaS (Infrastructure)

IaaS compared to PaaS Compared to SaaS

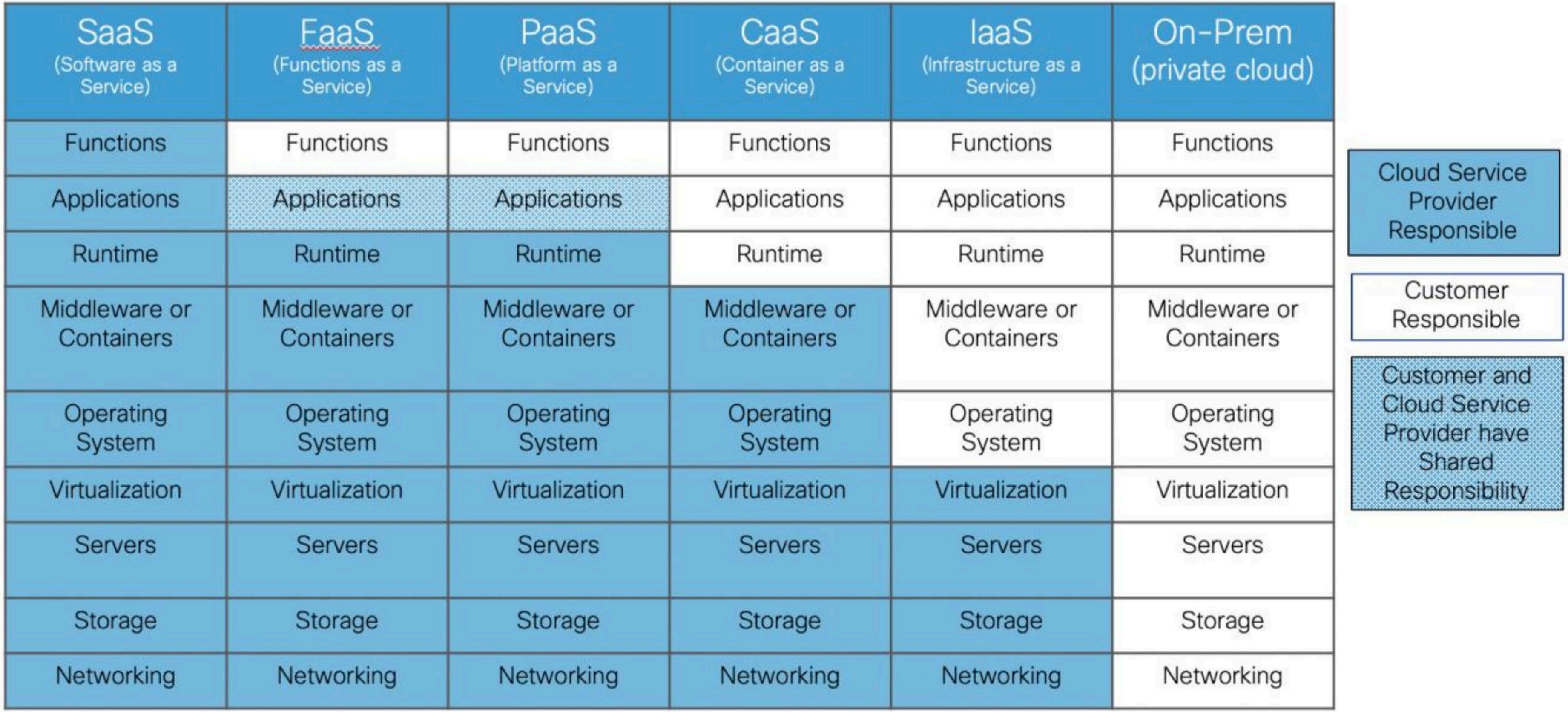


Manage :
- Nothing

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

AWS Security Solutions

Identity

AWS Identity & Access Management (IAM)

AWS Organizations

AWS Cognito

AWS Directory Service

AWS Single Sign-On

Detective control

AWS Security Hub

AWS CloudTrail

AWS Config

Amazon CloudWatch

Amazon GuardDuty

VPC Flow Logs

Infrastructure security

AWS Control Tower

Amazon EC2 Systems Manager

AWS Shield

AWS Web Application Firewall (WAF)

Amazon Inspector

Amazon Virtual Private Cloud (VPC)

Data protection

AWS Key Management Service (KMS)

AWS CloudHSM

Amazon Macie

Certificate Manager

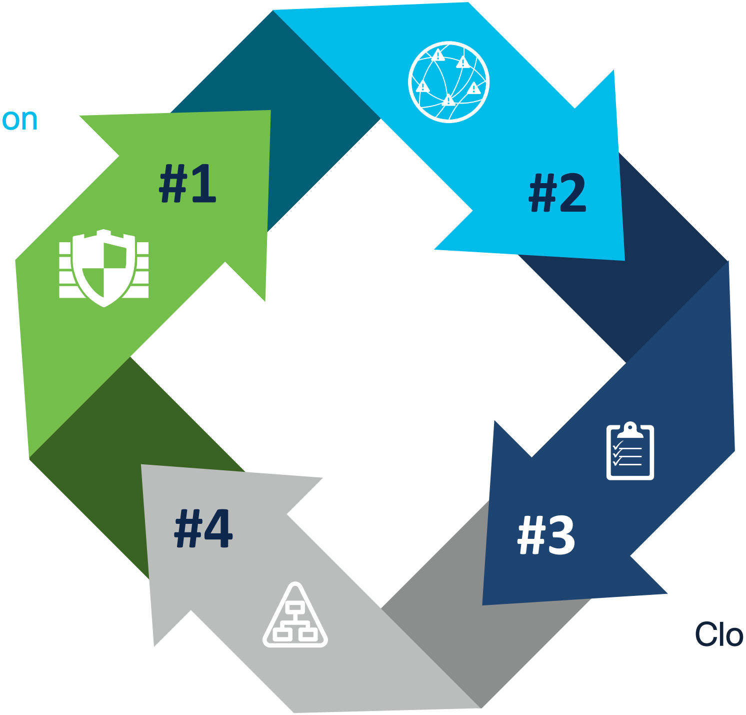
Server Side Encryption

Incident response

AWS Config Rules

AWS Lambda

Securing the Cloud



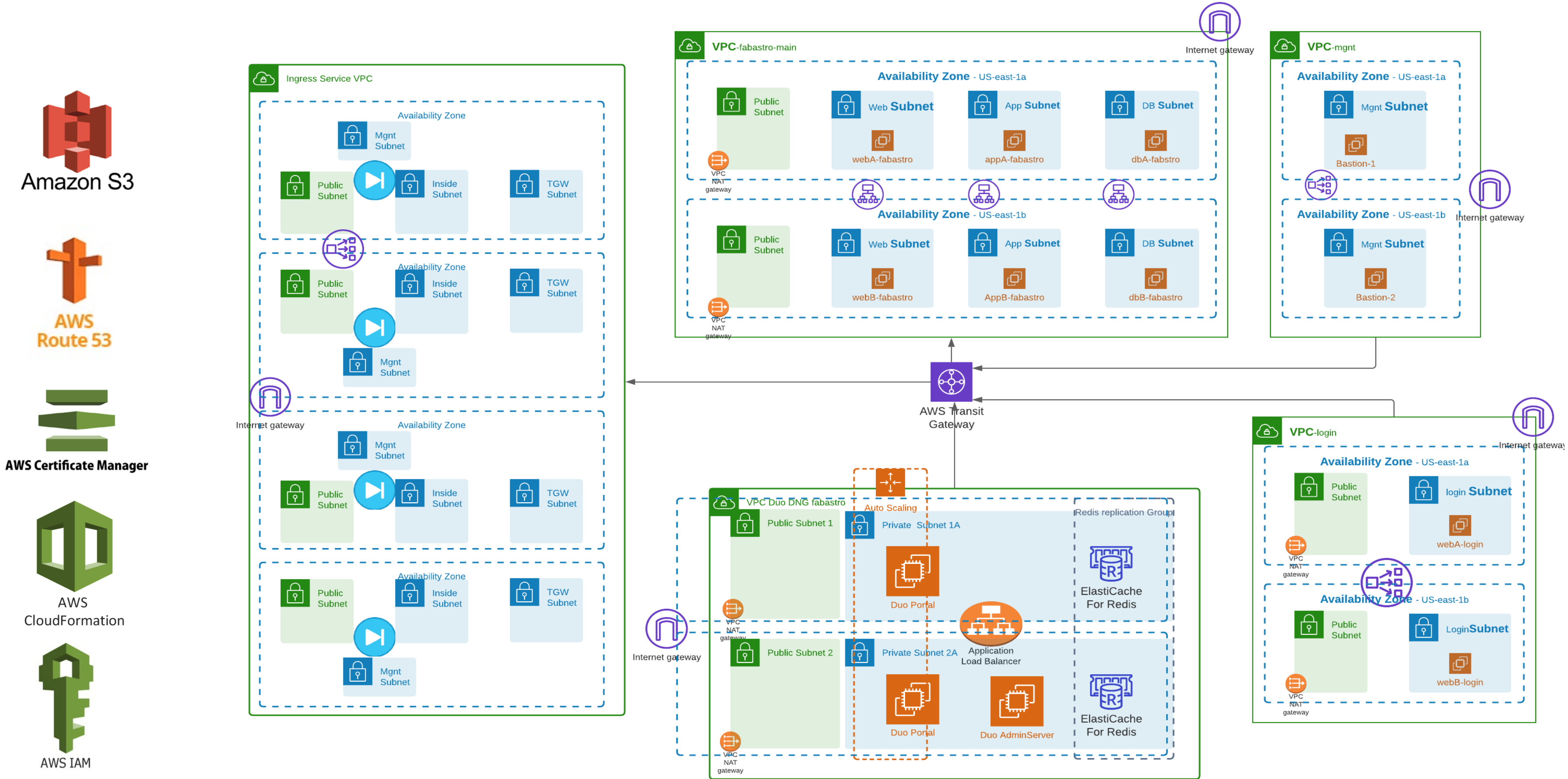
Network Segmentation

Visibility & Threat
Detection

Cloud Security Posture Management

Identity

FabAstro Application in AWS

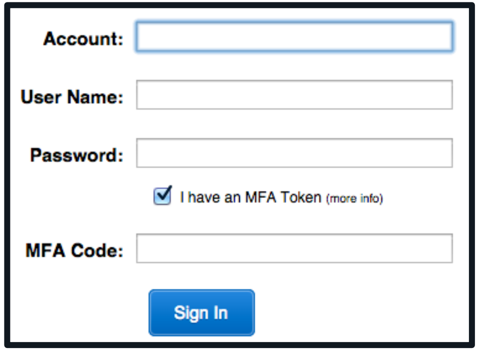


First Step in AWS… IAM, EC2 and VPC

AWS Identity Authentication

AWS Management Console

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



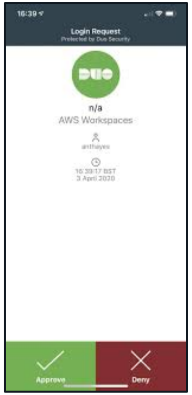
Account:

User Name:

Password:

☑ I have an MFA Token (more info)

MFA Code:



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

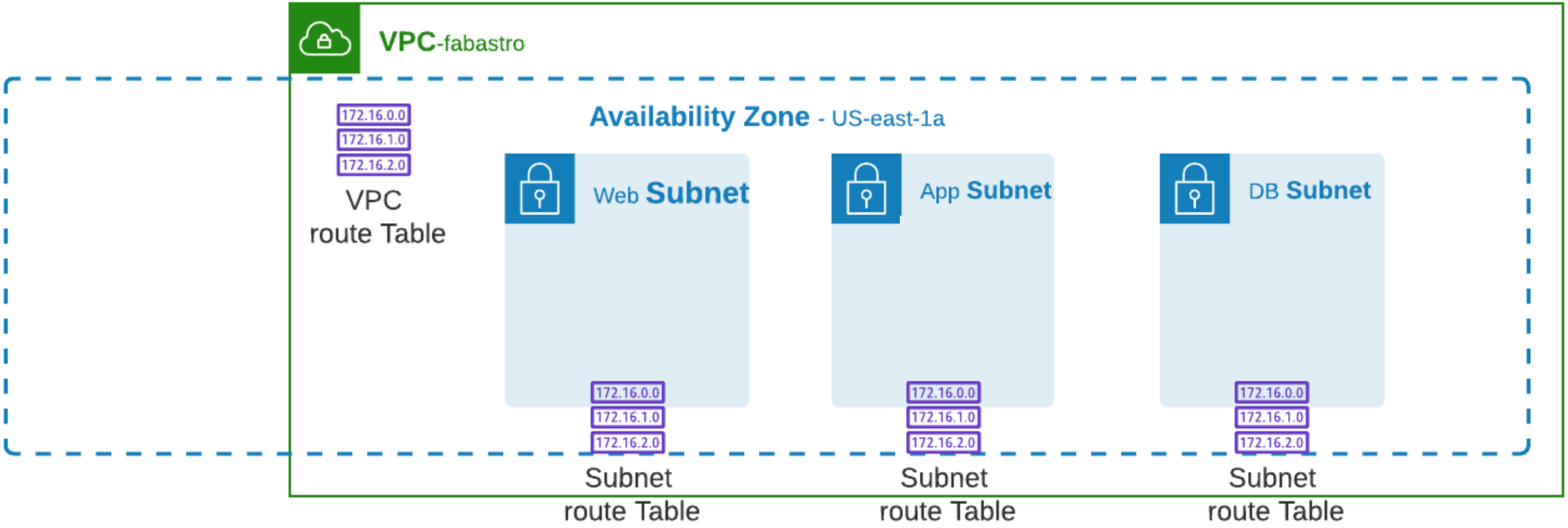
Ex: `AKIAIOSFODNN7EXAMPLE`

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)



VPC-fabastro

Availability Zone - US-east-1a

172.16.0.0
172.16.1.0
172.16.2.0

VPC
route Table

Web Subnet

App Subnet

DB Subnet

172.16.0.0
172.16.1.0
172.16.2.0

Subnet
route Table

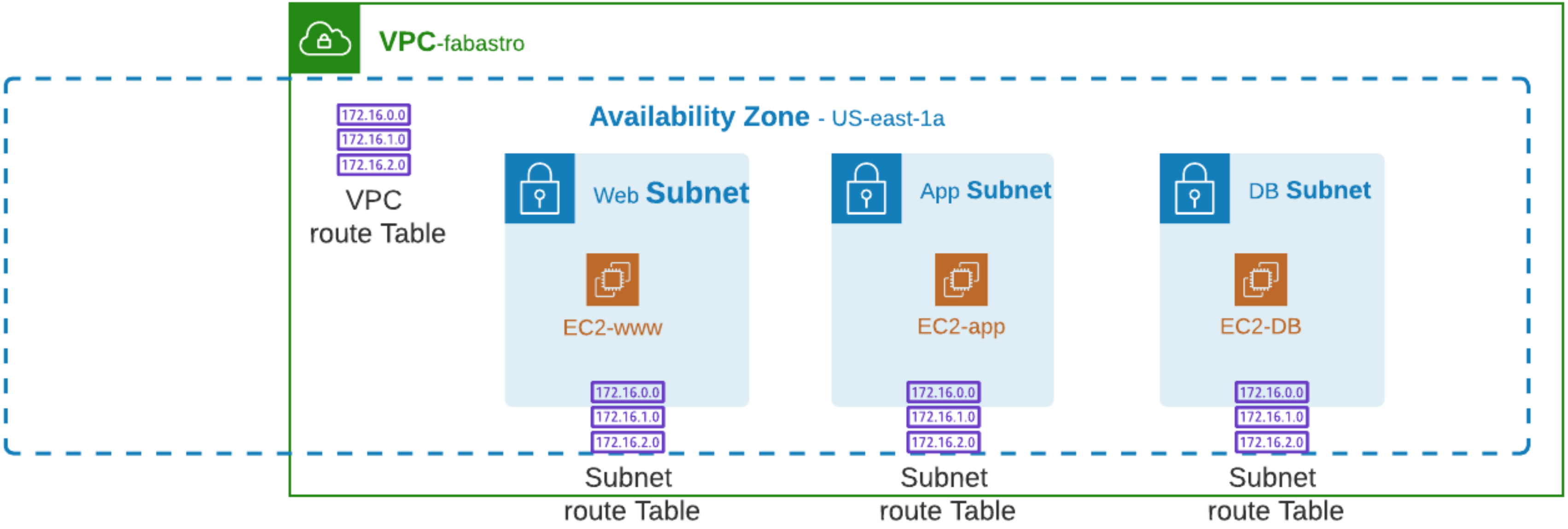
172.16.0.0
172.16.1.0
172.16.2.0

Subnet
route Table

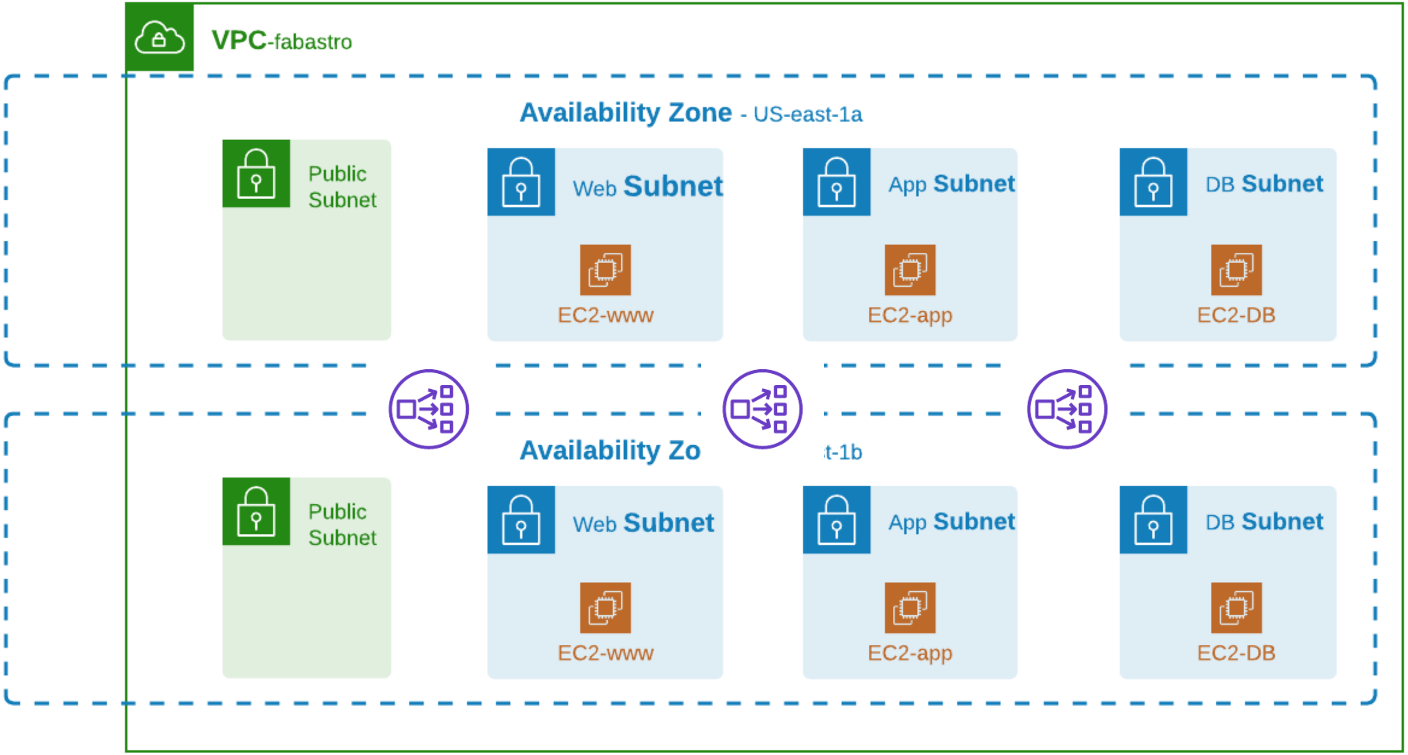
172.16.0.0
172.16.1.0
172.16.2.0

Subnet
route Table

In AWS IaaS… my workloads = Instances



HA with multiple AZ and LB



Quick demo

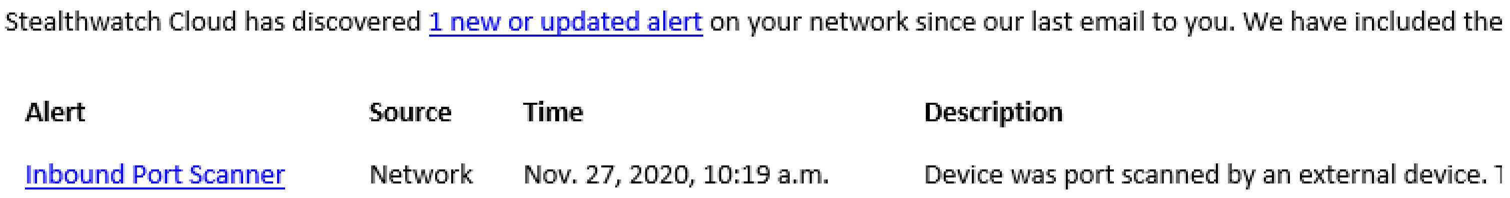
- EC2
- VRF
- S3
- IAM
- Cloudformation

How do I perform access control and Segmentation ?

How do I perform access control and Segmentation ?

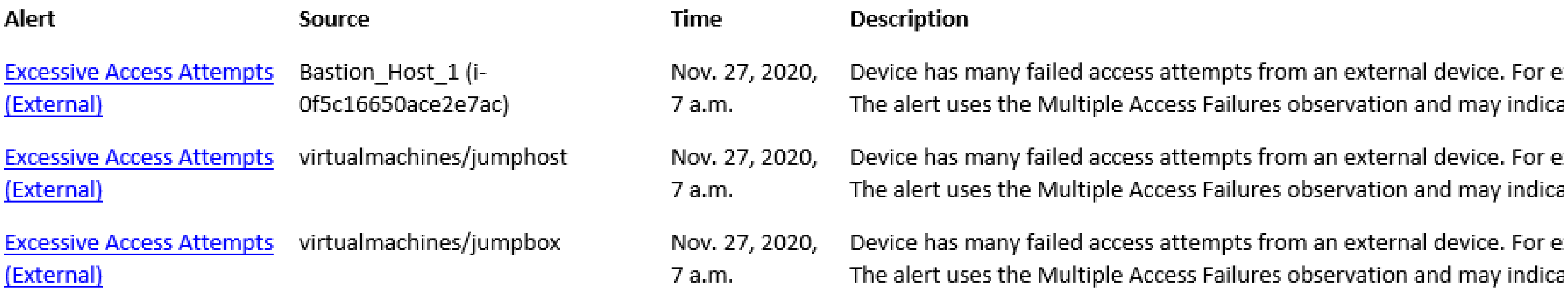
- AWS security Groups at Instance level
- AWS ACLs at Subnet level
- Network Firewall
- Host Security

But first : WHY access control ?

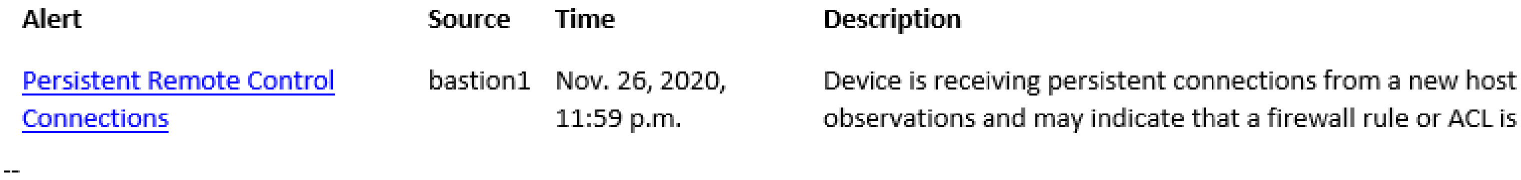


Stealthwatch Cloud has discovered 1 new or updated alert on your network since our last email to you. We have included the

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



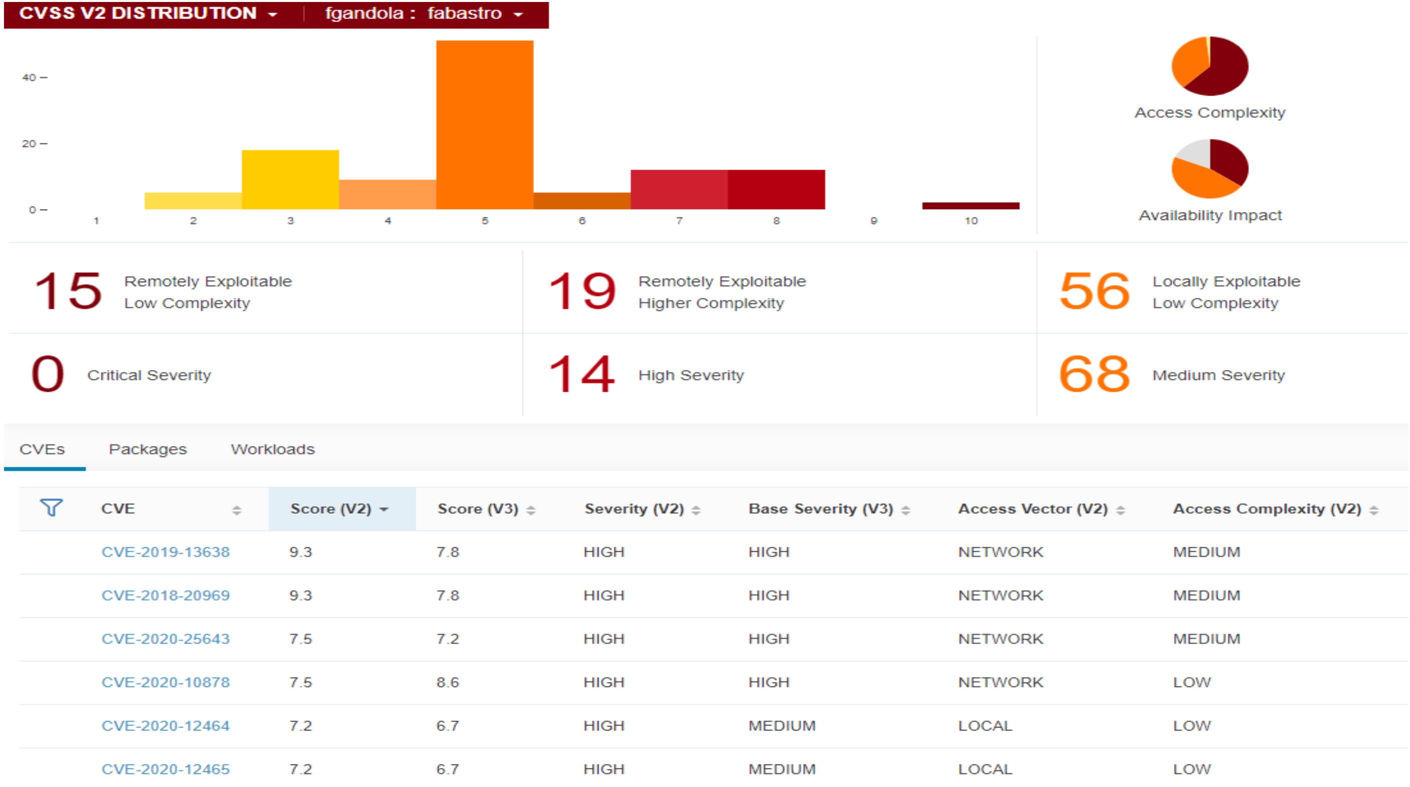
Alert	Source	Time	Description
Excessive Access Attempts (External)	Bastion_Host_1 (i-0f5c16650ace2e7ac)	Nov. 27, 2020, 7 a.m.	Device has many failed access attempts from an external device. For e The alert uses the Multiple Access Failures observation and may indica
Excessive Access Attempts (External)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

--

Tetration Vulnerability Assessment



15 Remotely Exploitable Low Complexity

19 Remotely Exploitable Higher Complexity

56 Locally Exploitable Low Complexity

0 Critical Severity

14 High Severity

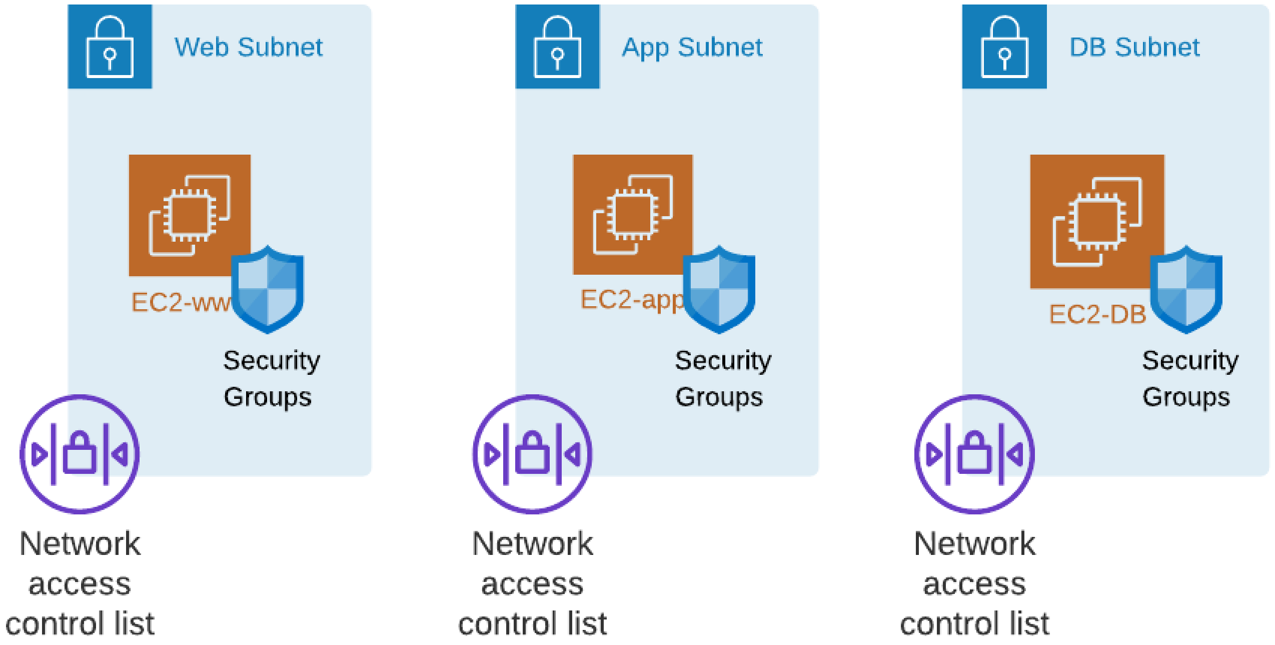
68 Medium Severity

CVEs | Packages | Workloads

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

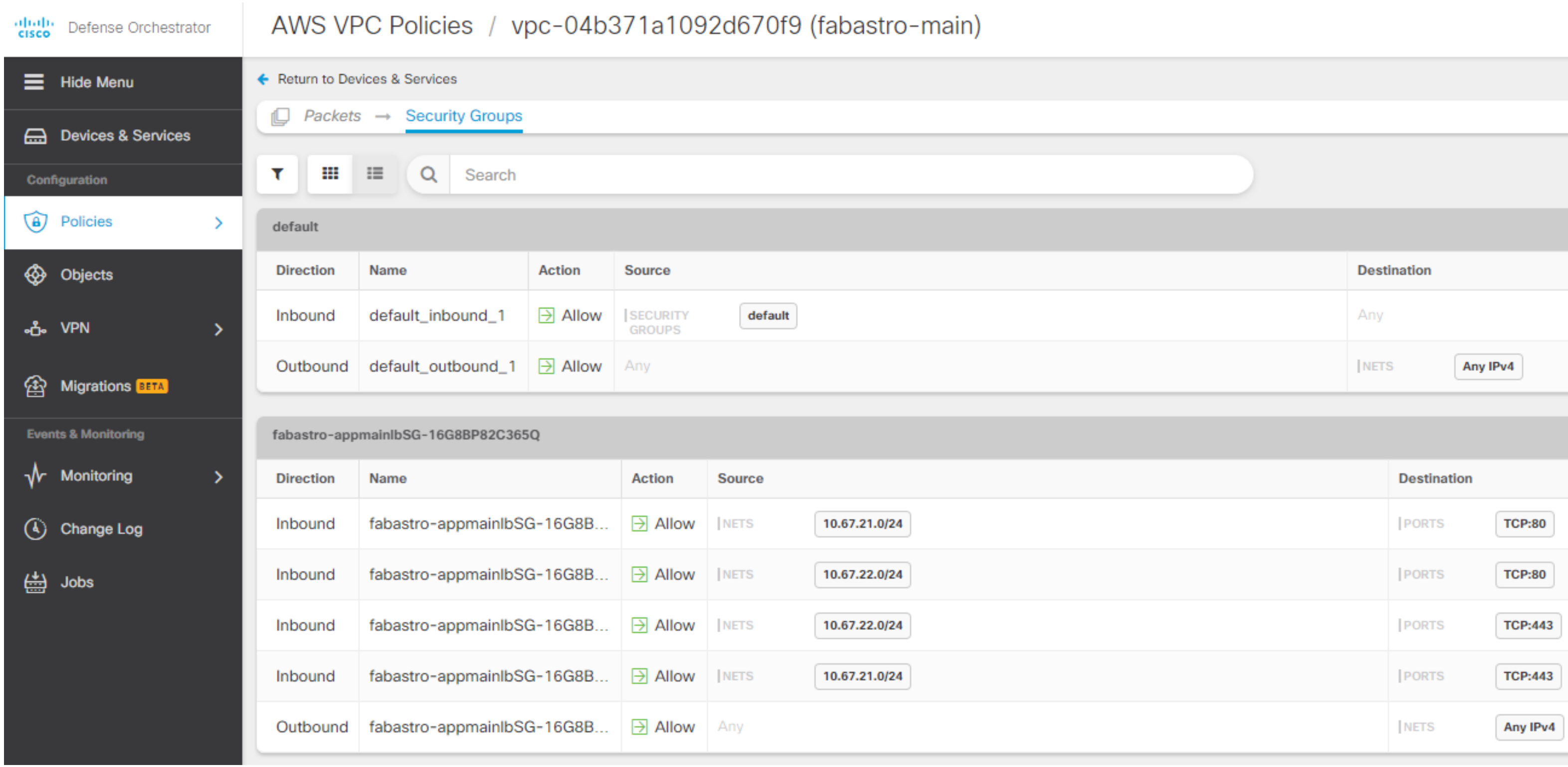
Security Groups and Network Access list



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

Security Groups in CDO



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

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 demo

- Network ACL
- Use security group

How do we address this with Secure Workload?

Contain lateral movement

Microsegmentation

Continuously track security compliance

Policy compliance

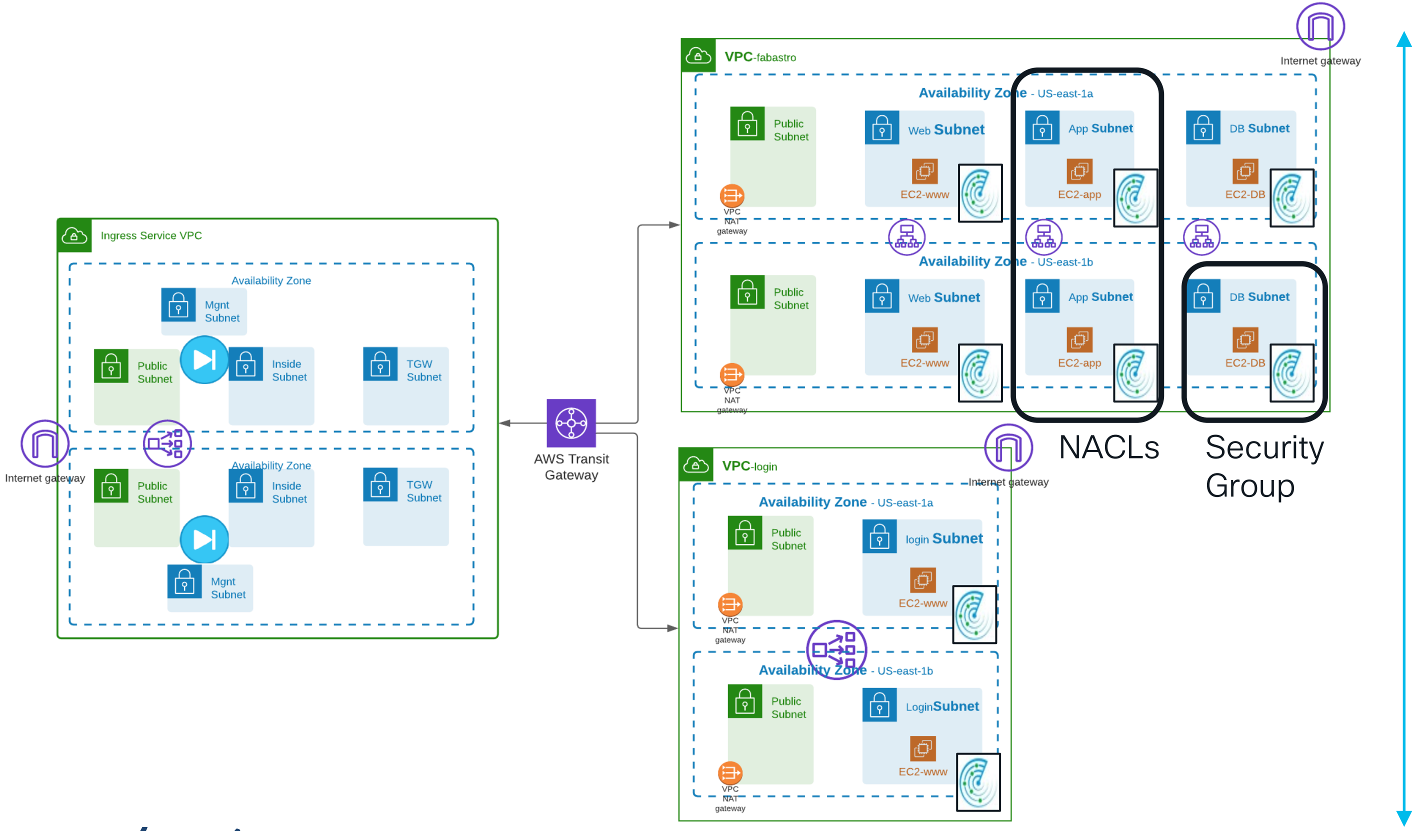
Identify behavior anomalies

Process and communication

Reduce attack surface

Software vulnerability

Another segmentation point?



NACLs

Security Group

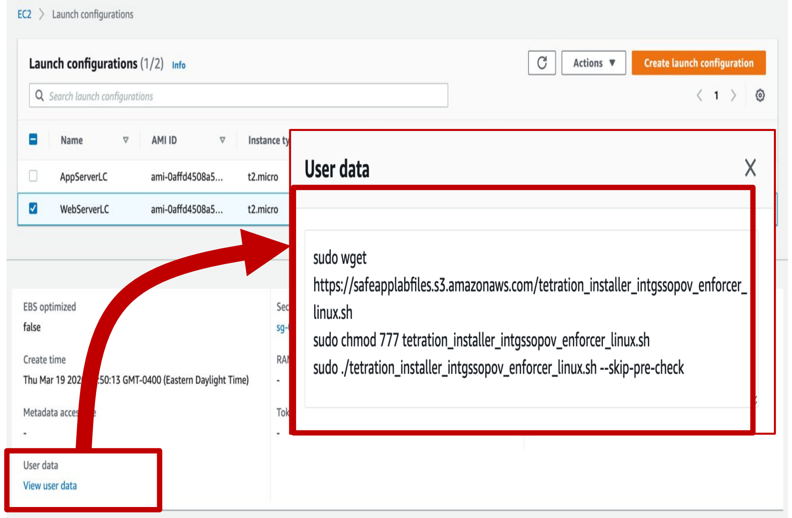
Micro-segmentation

Dynamic segmentation

Application discovery

No scaling issues

Deploy Enforcement Agent using AWS Launch Config or CloudFormation



EC2 > Launch configurations
Launch configurations (1/2) Info
Actions ▼
Create launch configuration
Search launch configurations
‹ 1 ›

	Name	AMI ID	Instance ty
□	AppServerLC	ami-0affd4508a5...	t2.micro
☑	WebServerLC	ami-0affd4508a5...	t2.micro

EBS optimized
false

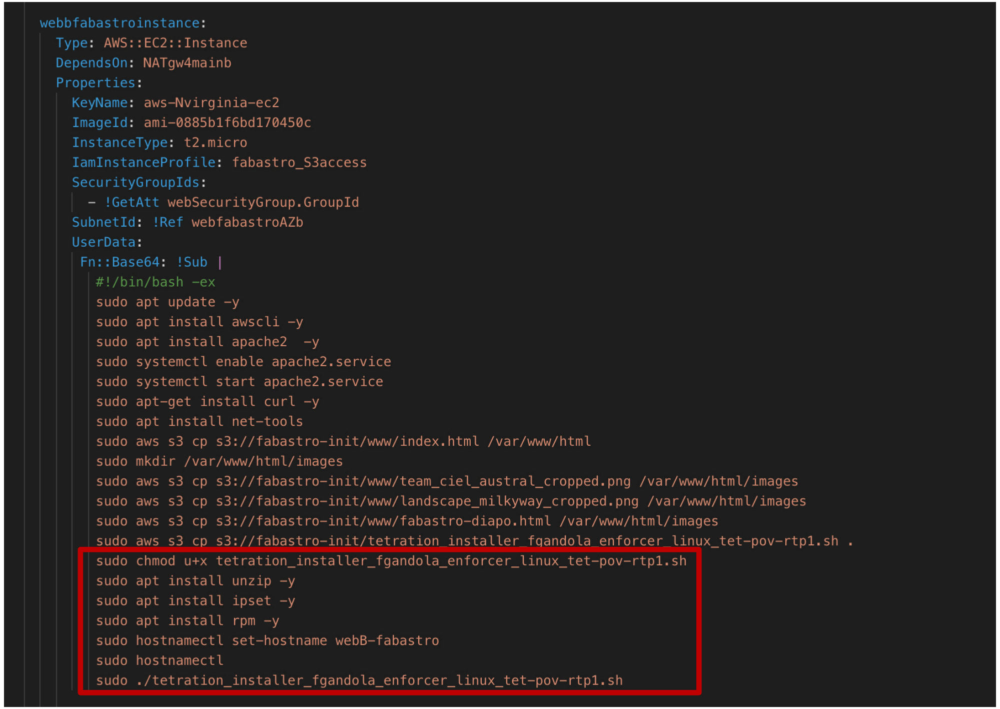
Create time
Thu Mar 19 202 :50:13 GMT-0400 (Eastern Daylight Time)

Metadata acces e
-

User data
View user data

User data

```
sudo wget
https://safeapplabfiles.s3.amazonaws.com/tetration_installer_intgssopov_enforcer_linux.sh
sudo chmod 777 tetration_installer_intgssopov_enforcer_linux.sh
sudo ./tetration_installer_intgssopov_enforcer_linux.sh --skip-pre-check
```



```
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
```

How do I insert NGFW ?

AWS FW

High availability and automated scaling

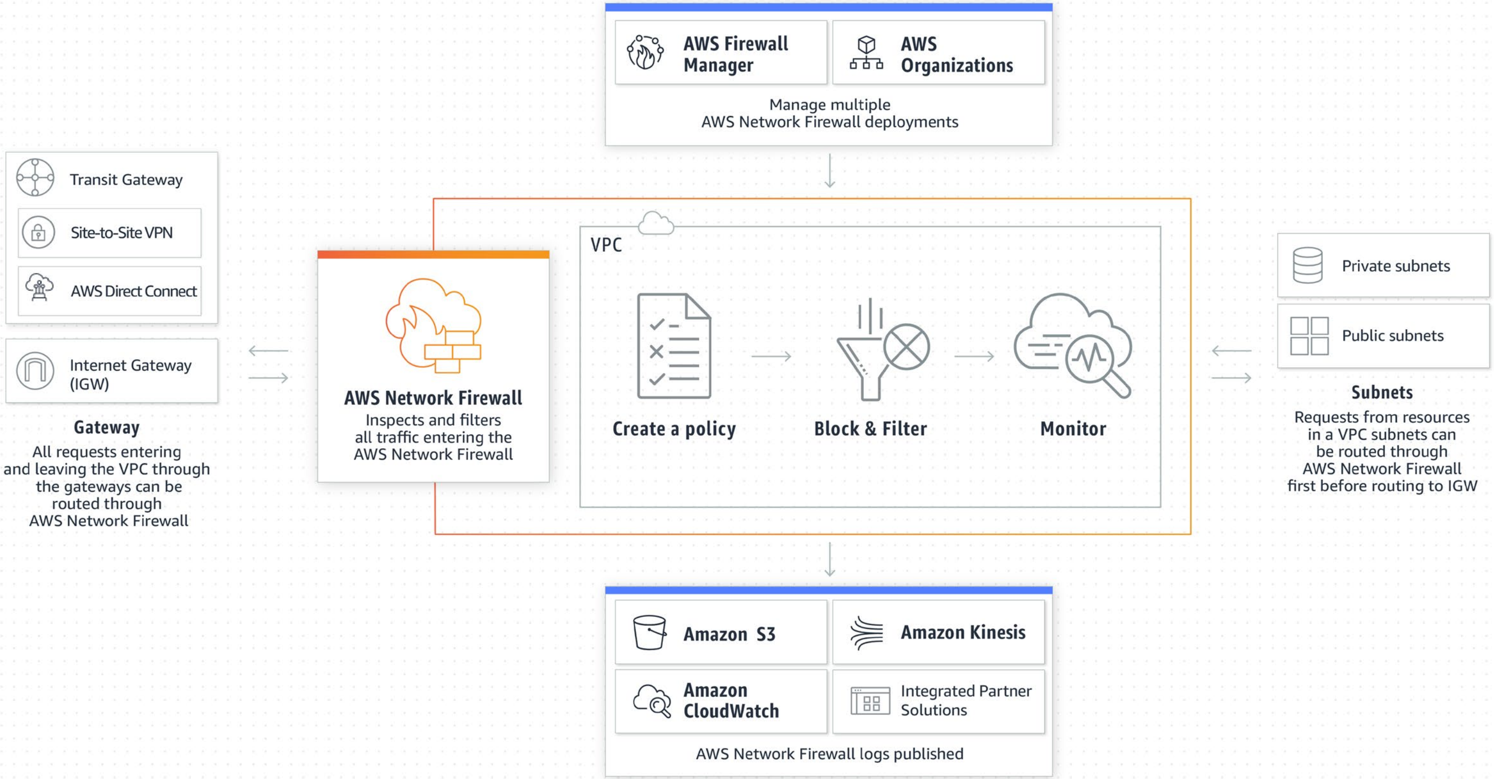
Stateful firewall

Web filtering

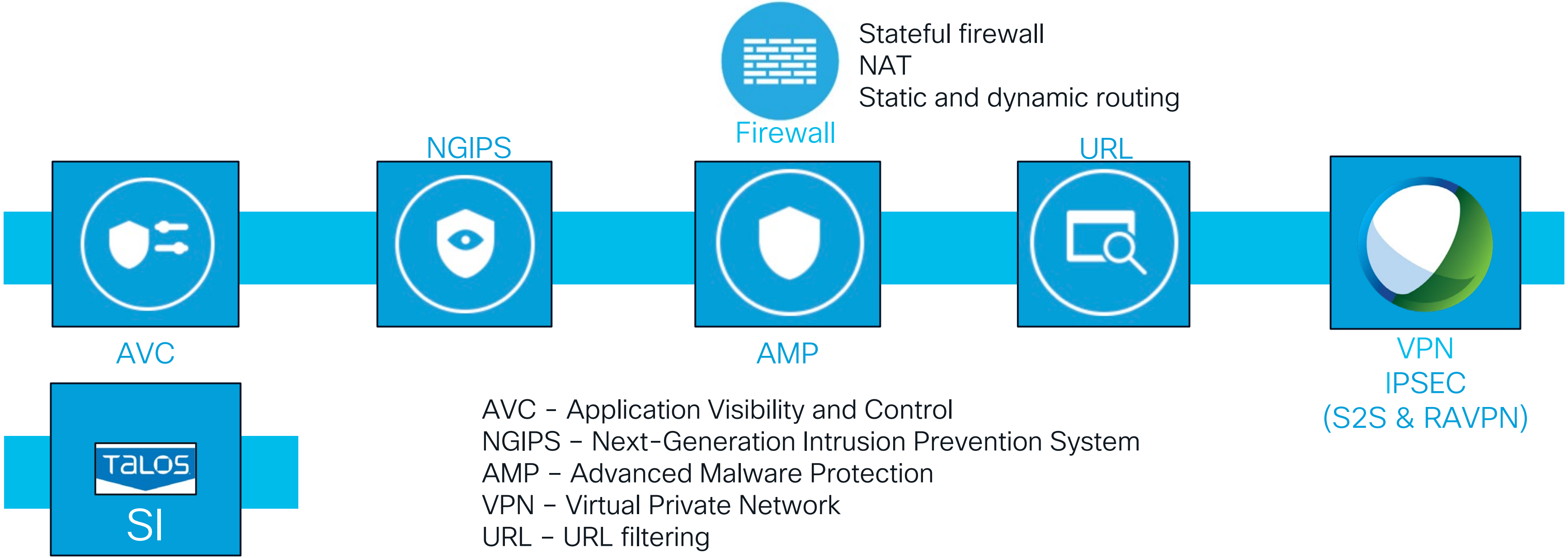
Intrusion prevention

Alert and flow logs

Central management and visibility


AWS Firewall Manager
AWS Organizations
Manage multiple AWS Network Firewall deployments
Transit Gateway
Site-to-Site VPN
AWS Direct Connect
Internet Gateway (IGW)
Gateway
All requests entering and leaving the VPC through the gateways can be routed through AWS Network Firewall
AWS Network Firewall
Inspects and filters all traffic entering the AWS Network Firewall
VPC
Create a policy
Block & Filter
Monitor
Private subnets
Public subnets
Subnets
Requests from resources in a VPC subnets can be routed through AWS Network Firewall first before routing to IGW
Amazon S3
Amazon Kinesis
Amazon CloudWatch
Integrated Partner Solutions
AWS Network Firewall logs published

Cisco Secure Firewall – NGFWv



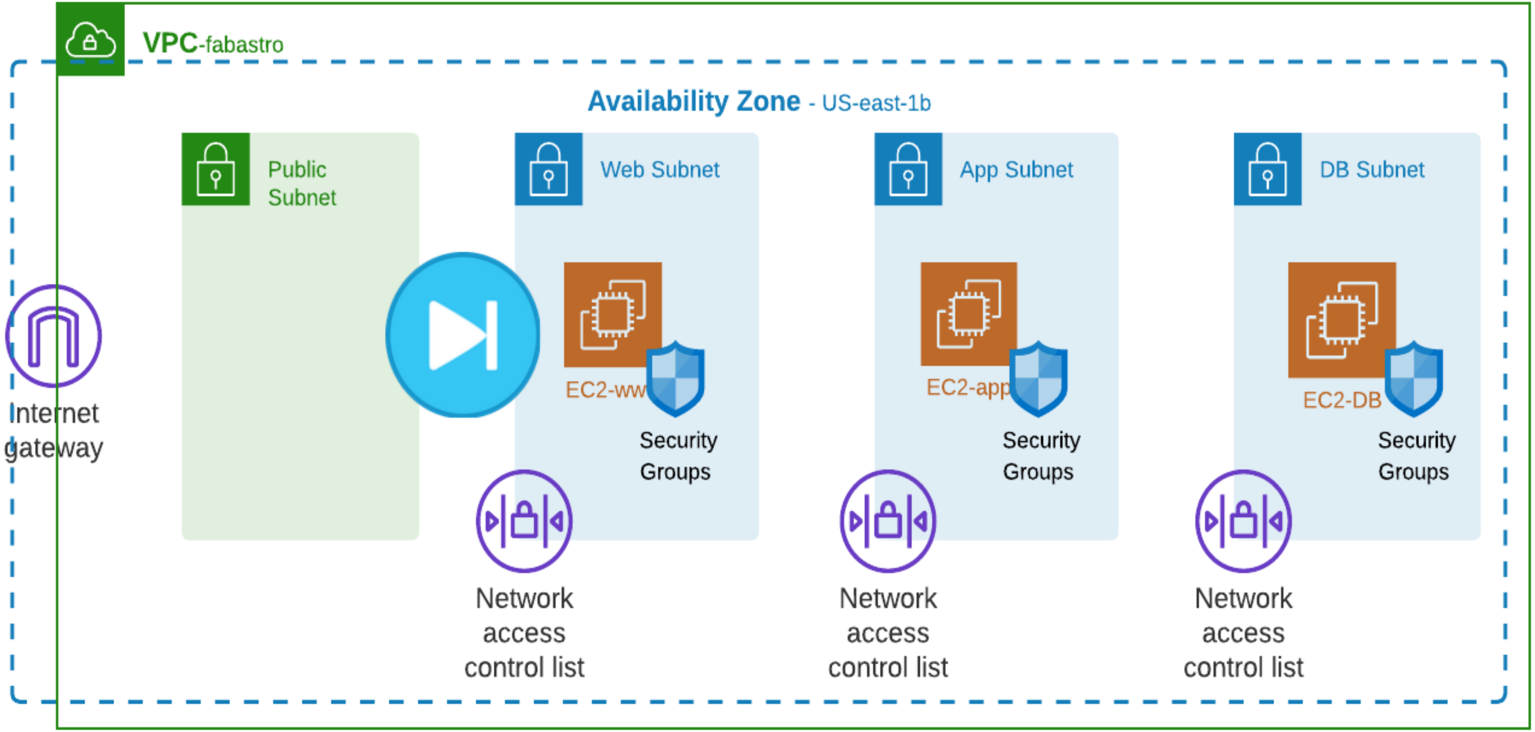
Stateful firewall
NAT
Static and dynamic routing

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

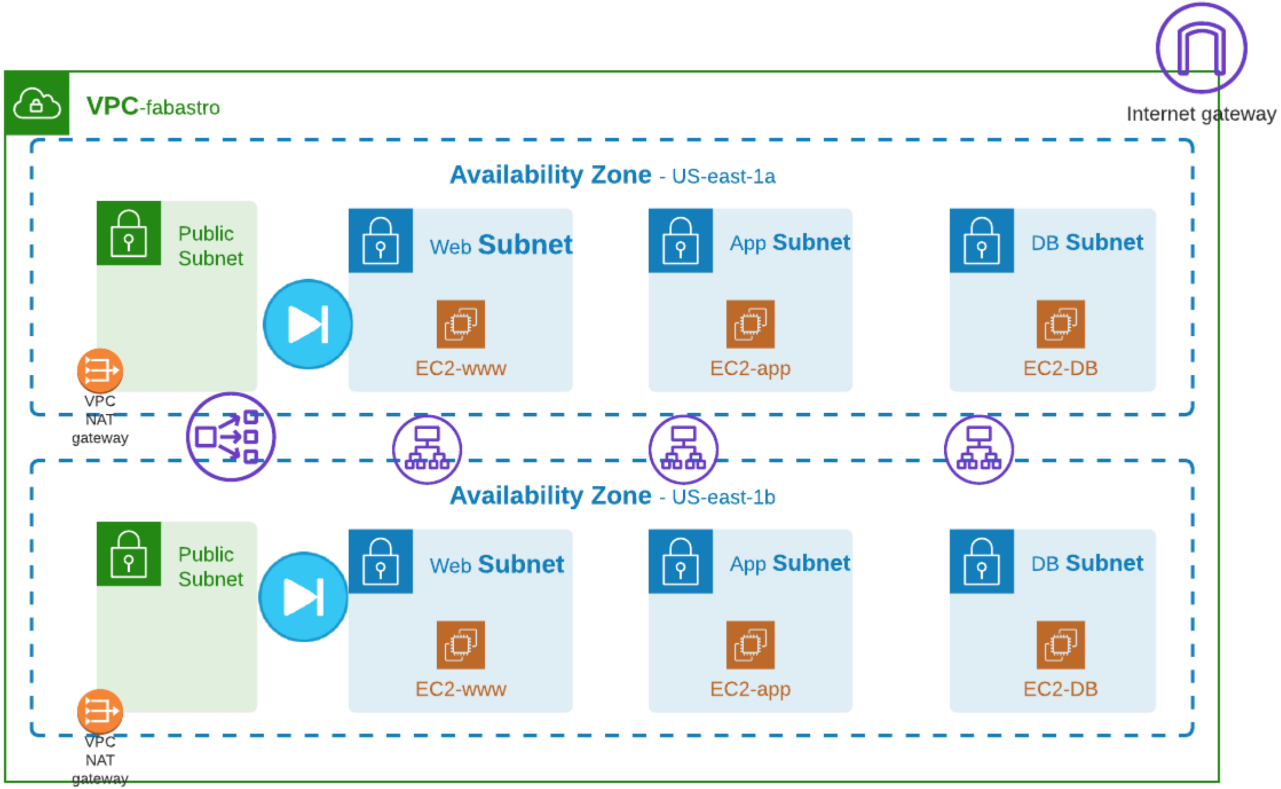
FTD Appliance

vmware aws KVM Microsoft Azure Google Cloud Platform ORACLE Cloud Infrastructure

Firewall in front of the “Application” VPC



FTD insertion with HA

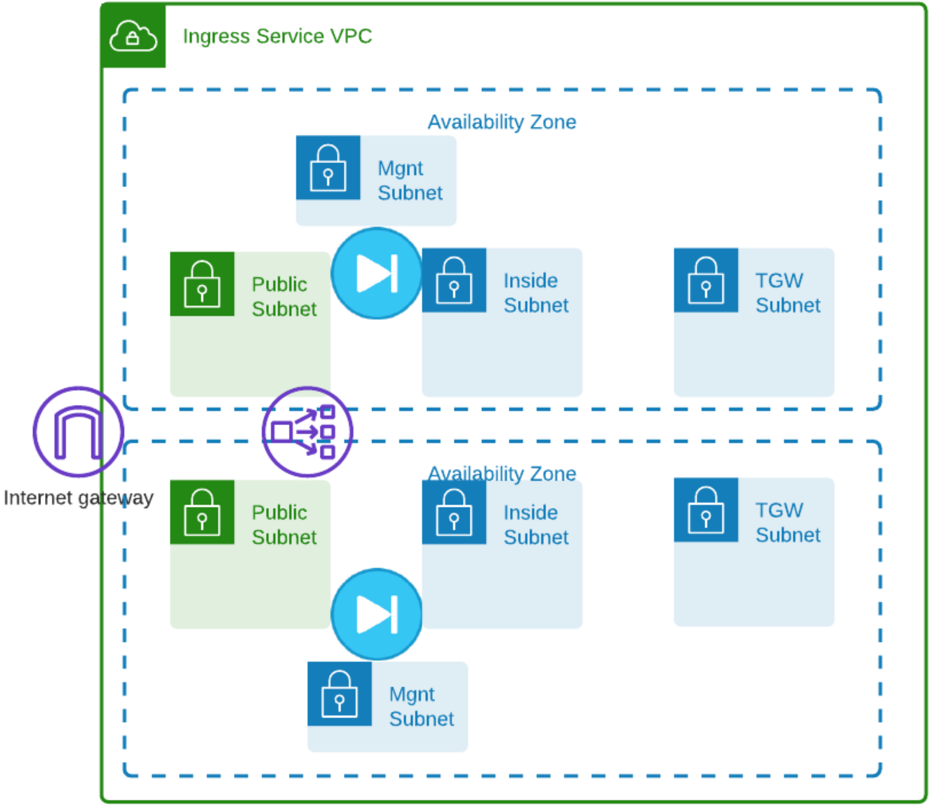


Limits of this design

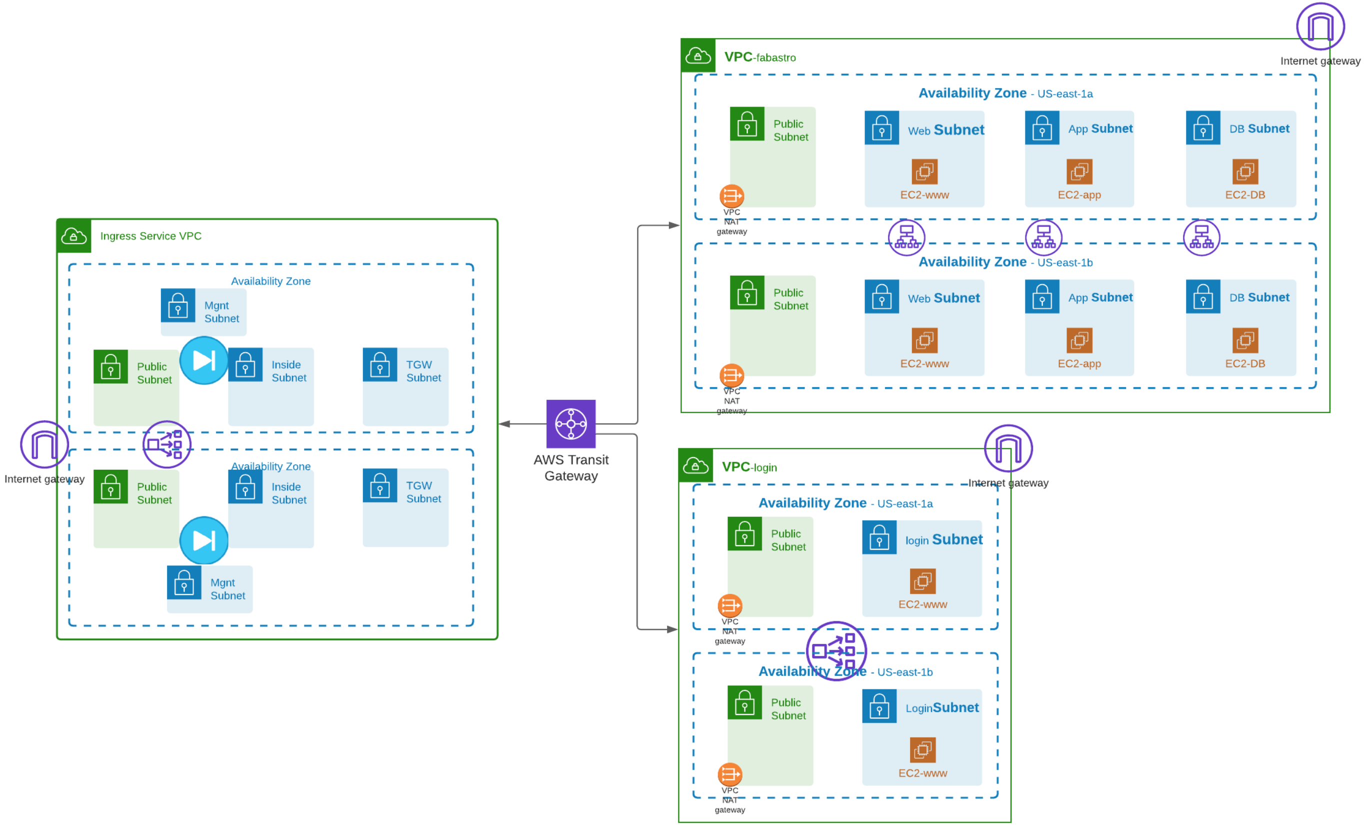
New Firewall pair for each applications

Double inspection for inter-VPC

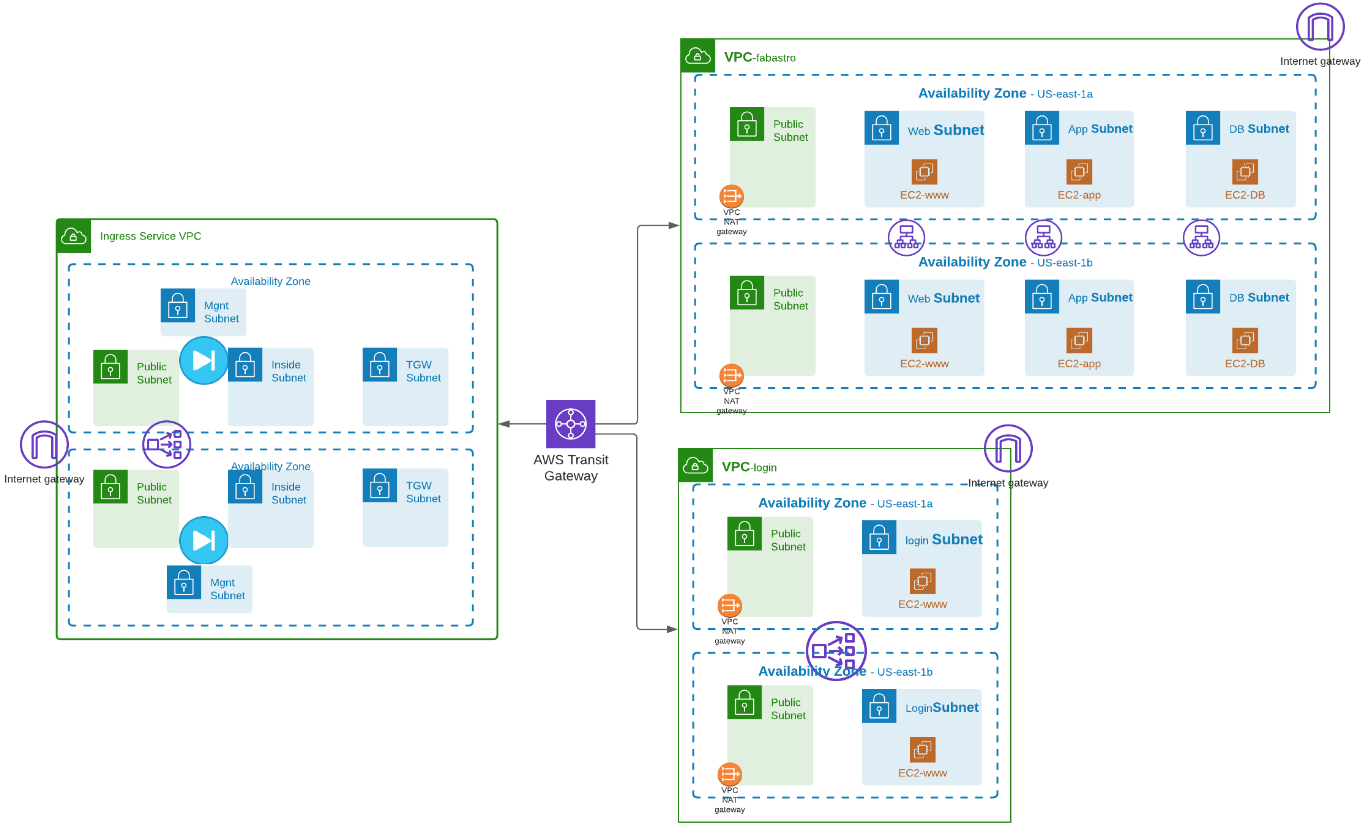
Ingress service VPC



Ingress Service VPC with FTD



North/South and East/West Service VPC



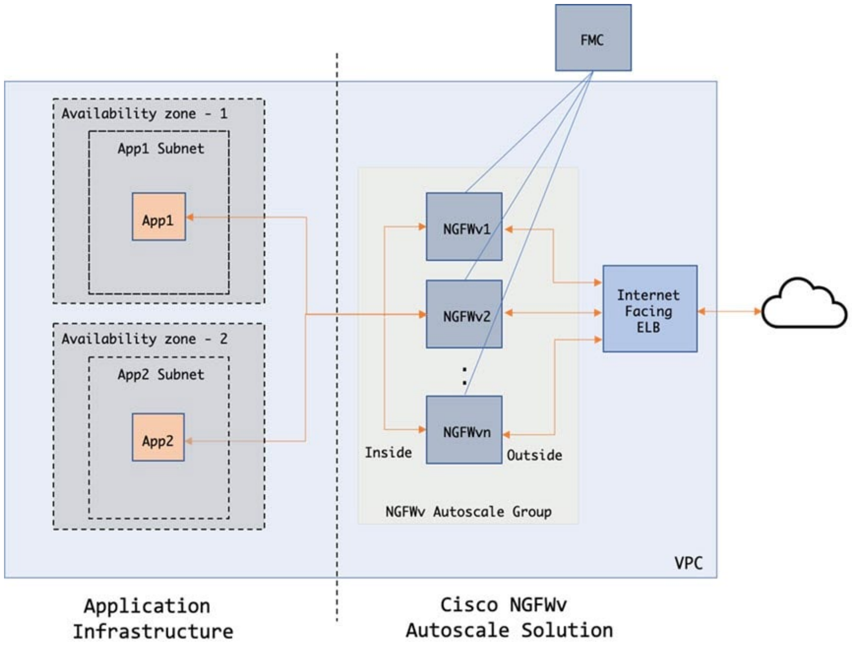
FTD AWS Insertion Configuration

- 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

What about auto-scaling ?



- Uses Lambda function
- Requires FMC
- Cloudformation templates provided

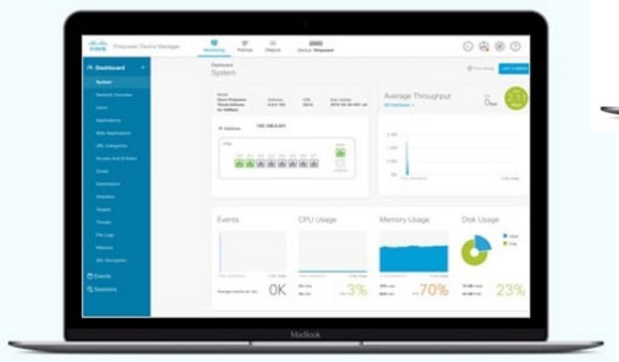
More information: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-gsg/ftdv-aws-autoscale.html

How do I manage my FTDs ?

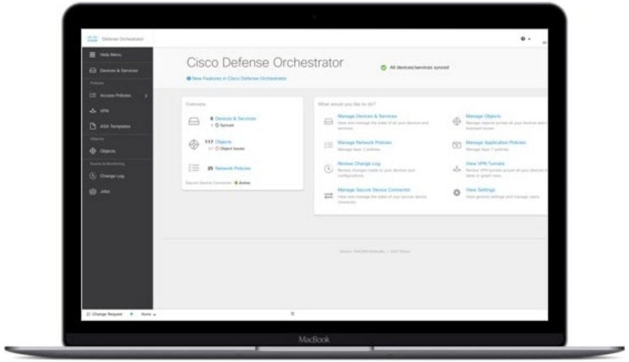
Overview
Analysis
Policies
Devices
Objects
FireAMP
Summary Dashboard
Network
Threats
Intrusion Events
Status
Geolocation
Indications of Compromise by Host
New Indications of Compromise over Time
Connections by Security Intelligence Category
Malware Threats
Intrusion Events
Traffic by Security Intelligence Category
MacBook

FirePower Management Center :

- On prem
- In AWS



FDM



CDO

Question about automation ?

In AWS

AWS CloudFormation

Ecosystem solutions

HashiCorp Terraform

ANSIBLE

Quick demo

- FTD Insertion
- FTD configuration
- Cloudformation

What about Remote Access ?

What about Remote Access ?

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

What about the EC2 instances management ?

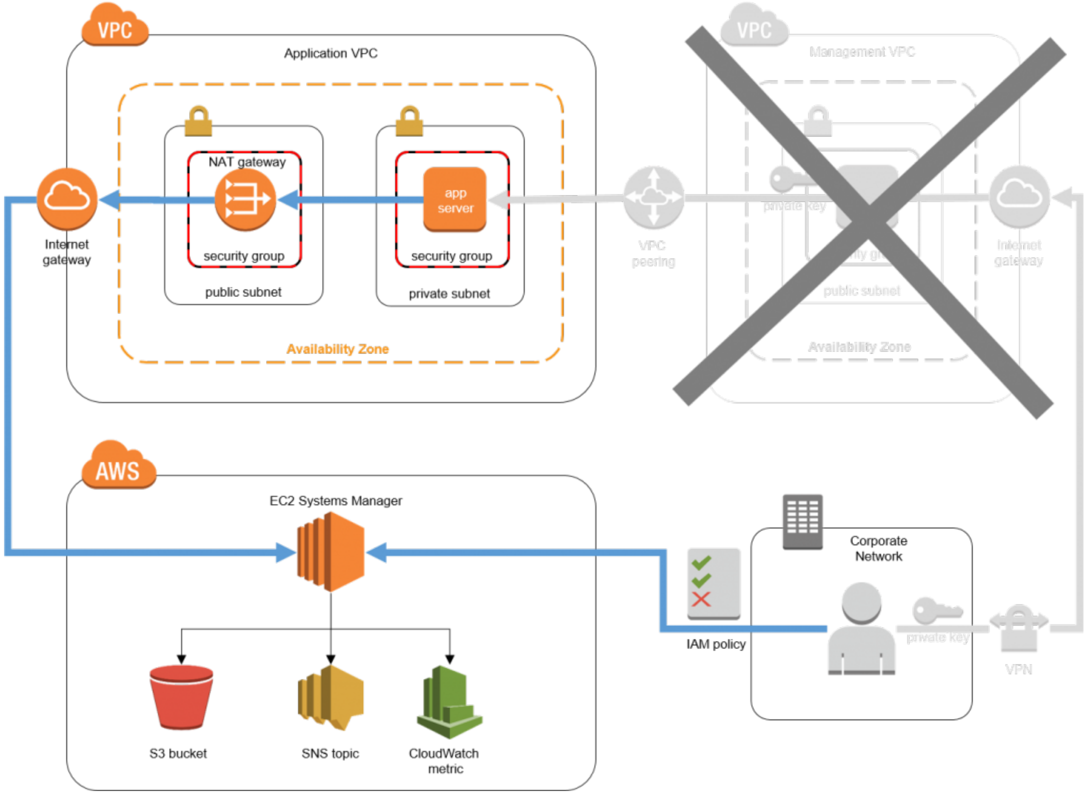
- Direct access to the public IP Address?
- Bastion host
- Direct Connect from on-Prem or VPN
- Leverage AWS EC2 System Manager

AWS KMS

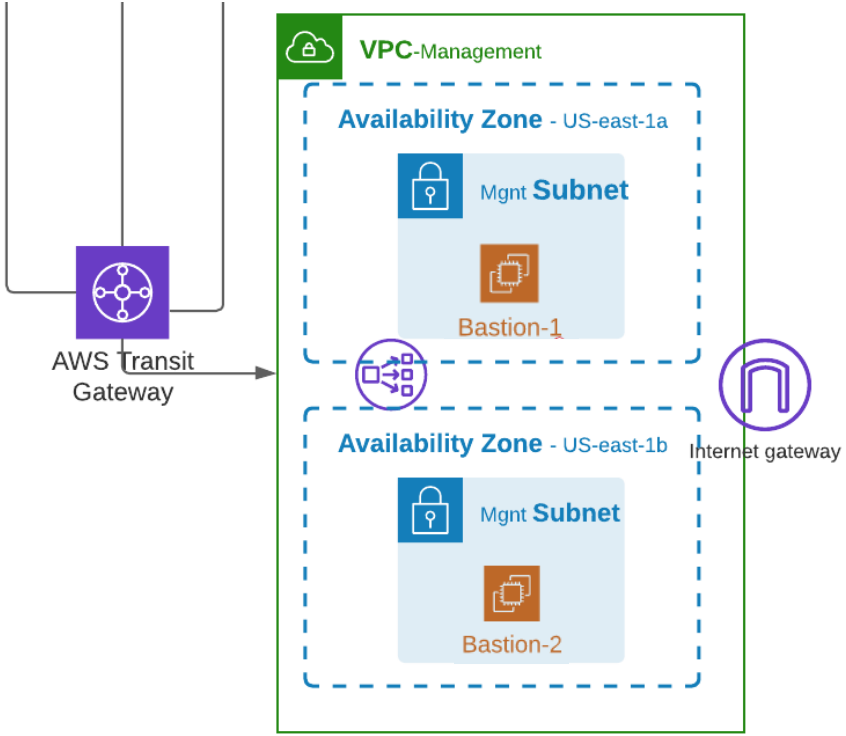
AWS Direct Connect

Amazon EC2
Systems Manager

AWS EC2 System Manager



Management VPC



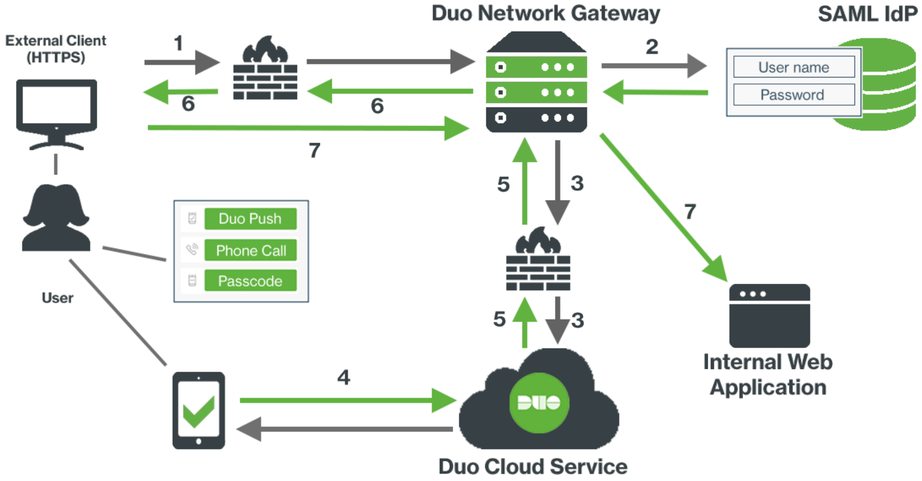
Provide SuperUser secured Access

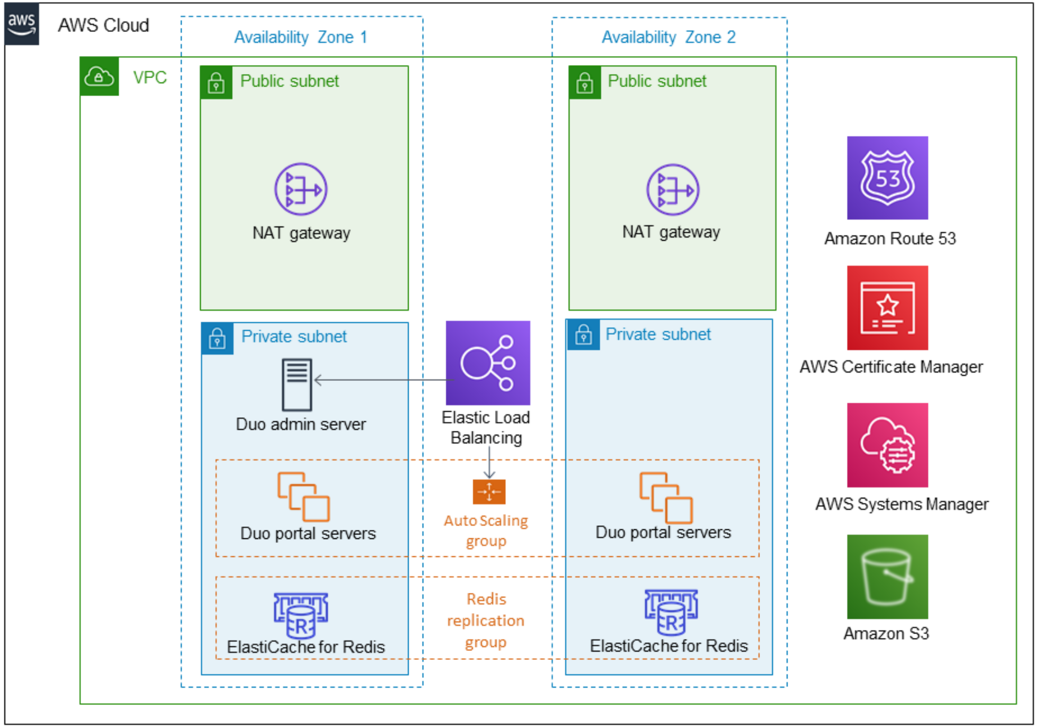
Provide SuperUser secured Access

DUO Network Gateway

What is Duo Network Gateway ?

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

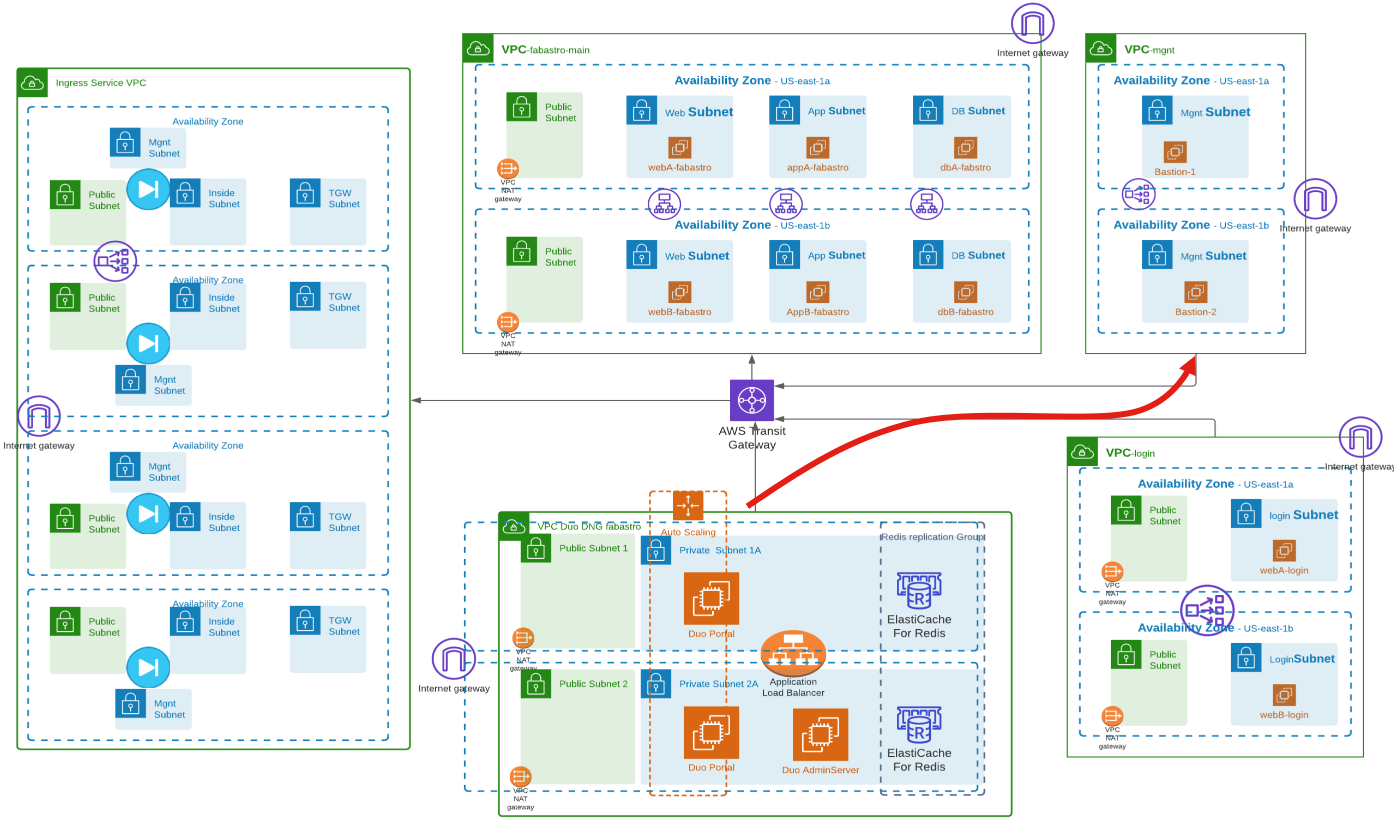



AWS Cloud
Availability Zone 1
Availability Zone 2
VPC
Public subnet
NAT gateway
Public subnet
NAT gateway
Amazon Route 53
AWS Certificate Manager
Private subnet
Duo admin server
Elastic Load Balancing
Private subnet
Duo portal servers
Auto Scaling group
Duo portal servers
AWS Systems Manager
ElastiCache for Redis
Redis replication group
ElastiCache for Redis
Amazon S3

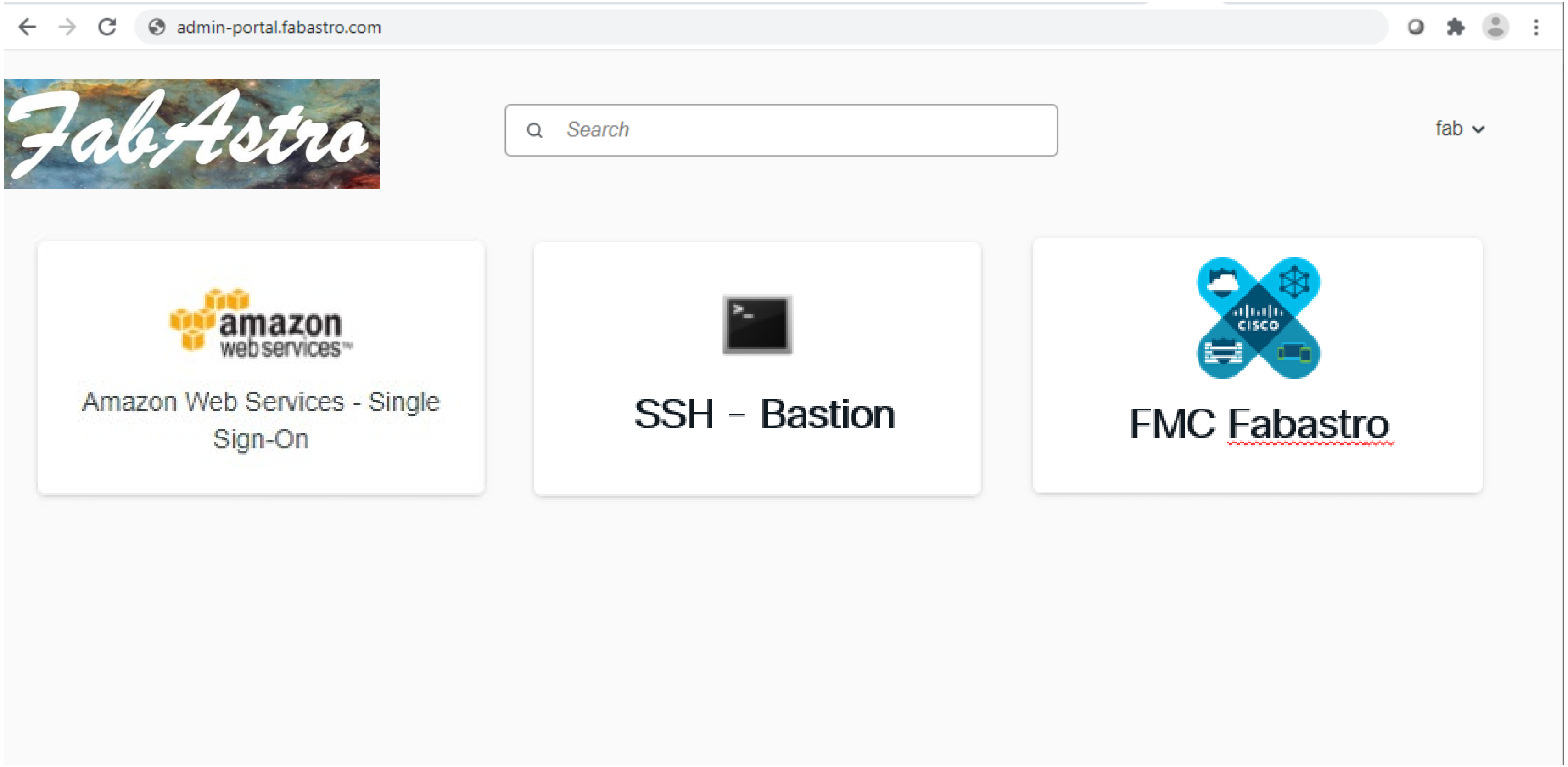
DNG Use Cases for FabAstro...or else

- 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.

DNG in FabAstro: Access for Admins

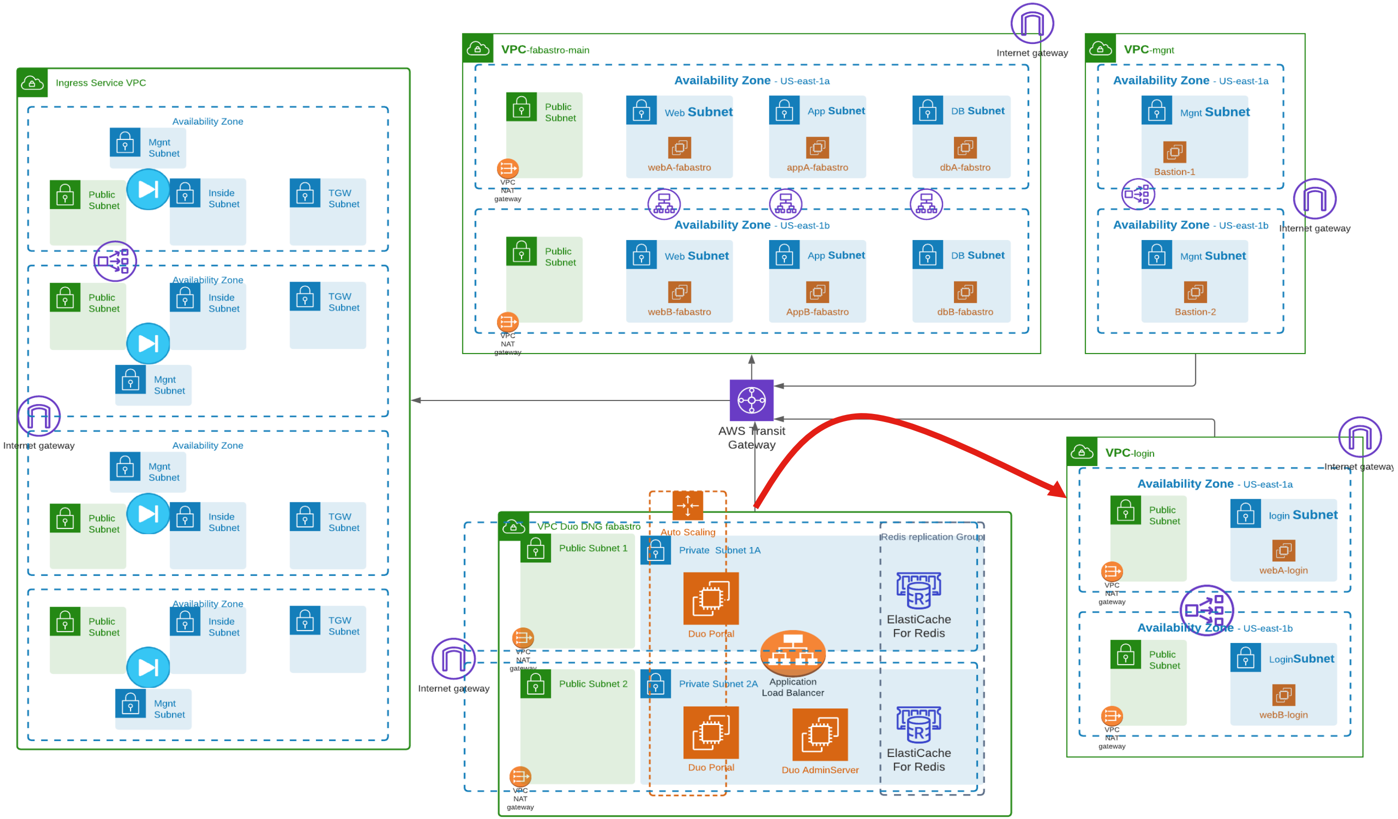


Using DNG to access FabAstro Admin Portal



admin-portal.fabastro.com

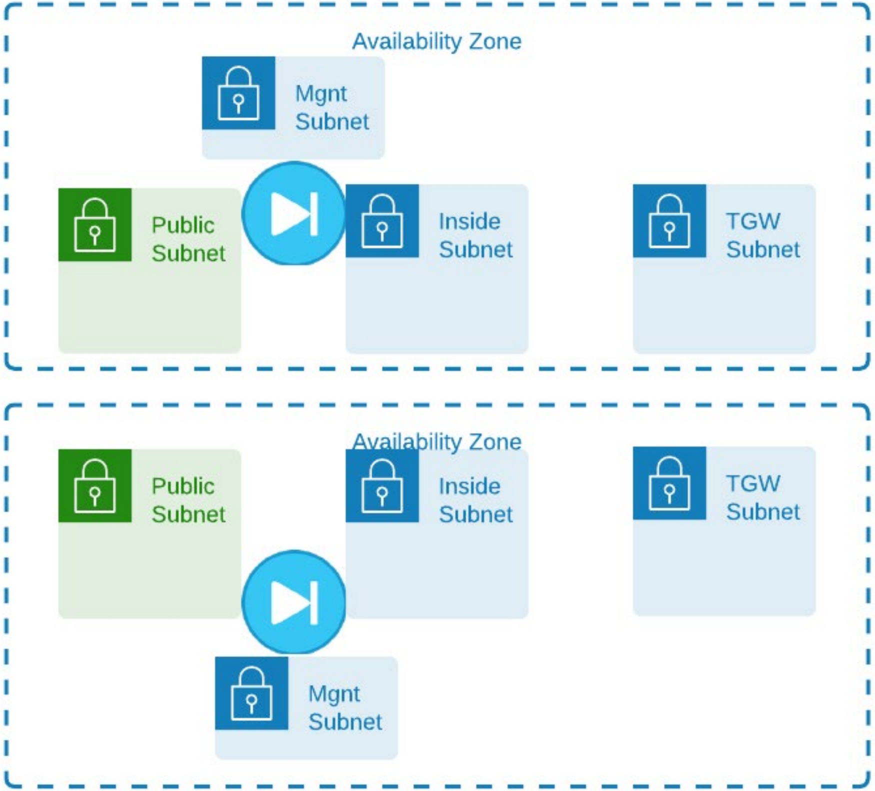
DNG in FabAstro: Web portal for Privileged Users



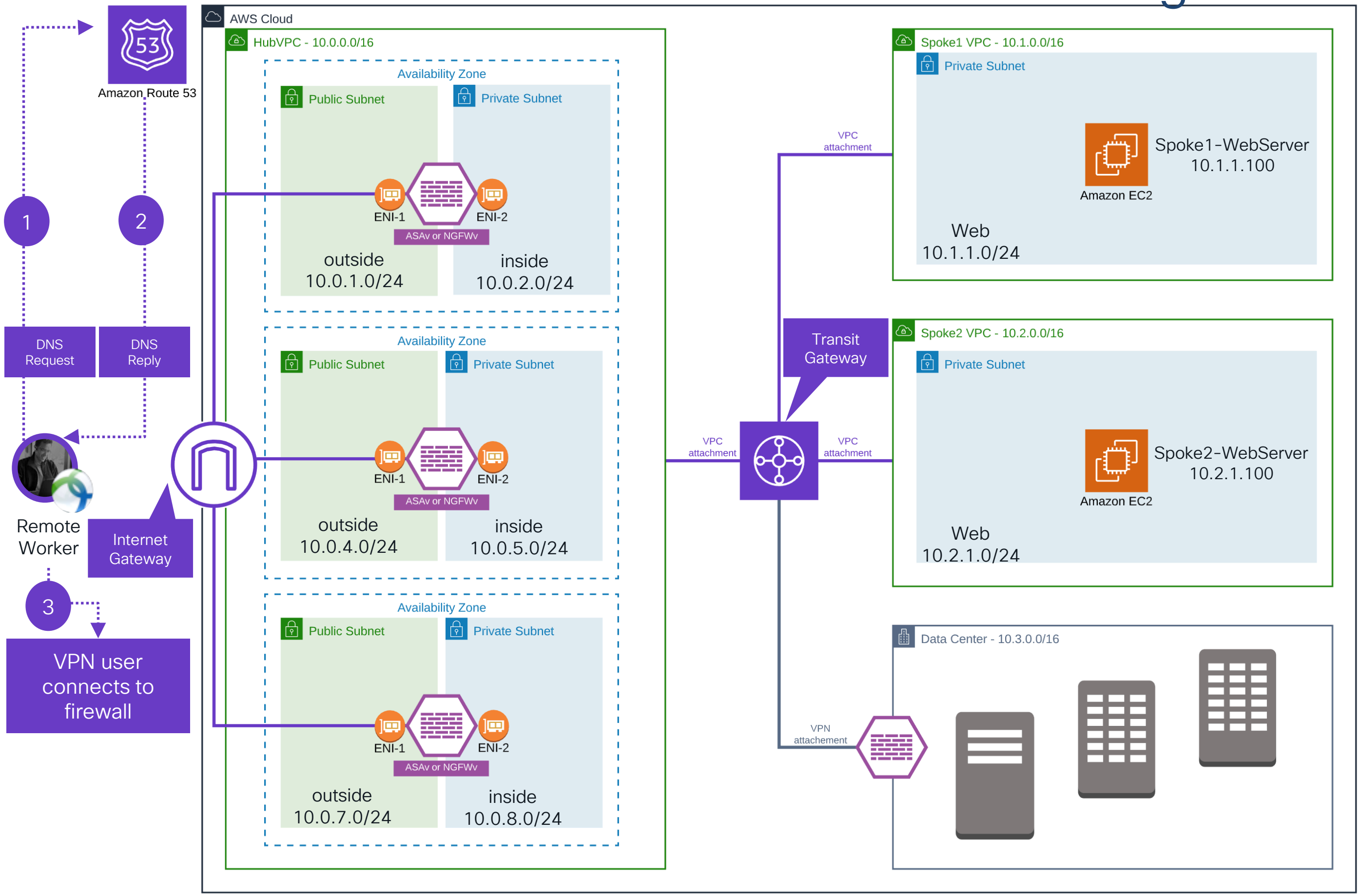
Quick demo

Deploy and configure remote access VPN

Remote Access to Management VPC



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

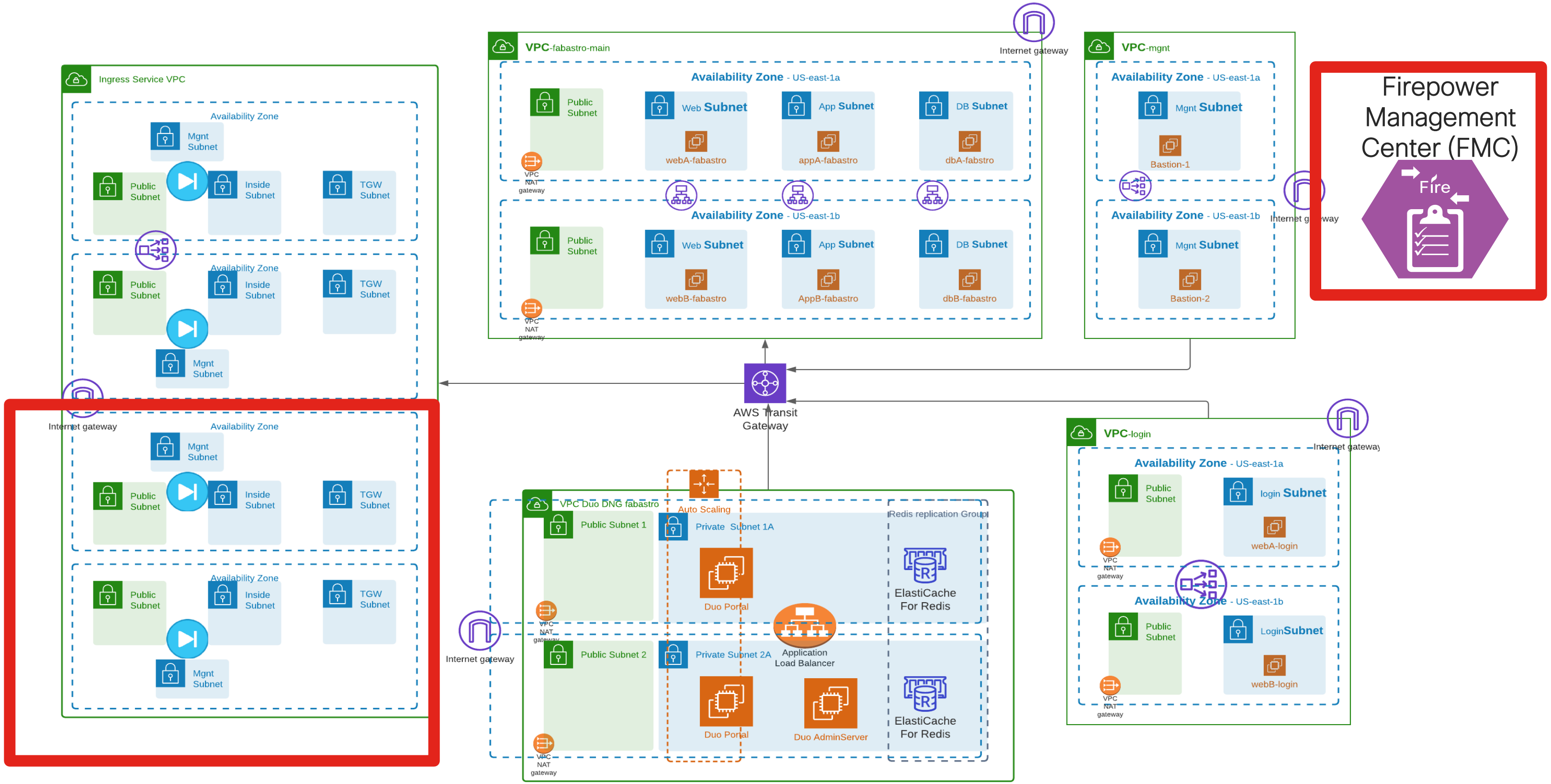
Each AZ may have multiple firewalls

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

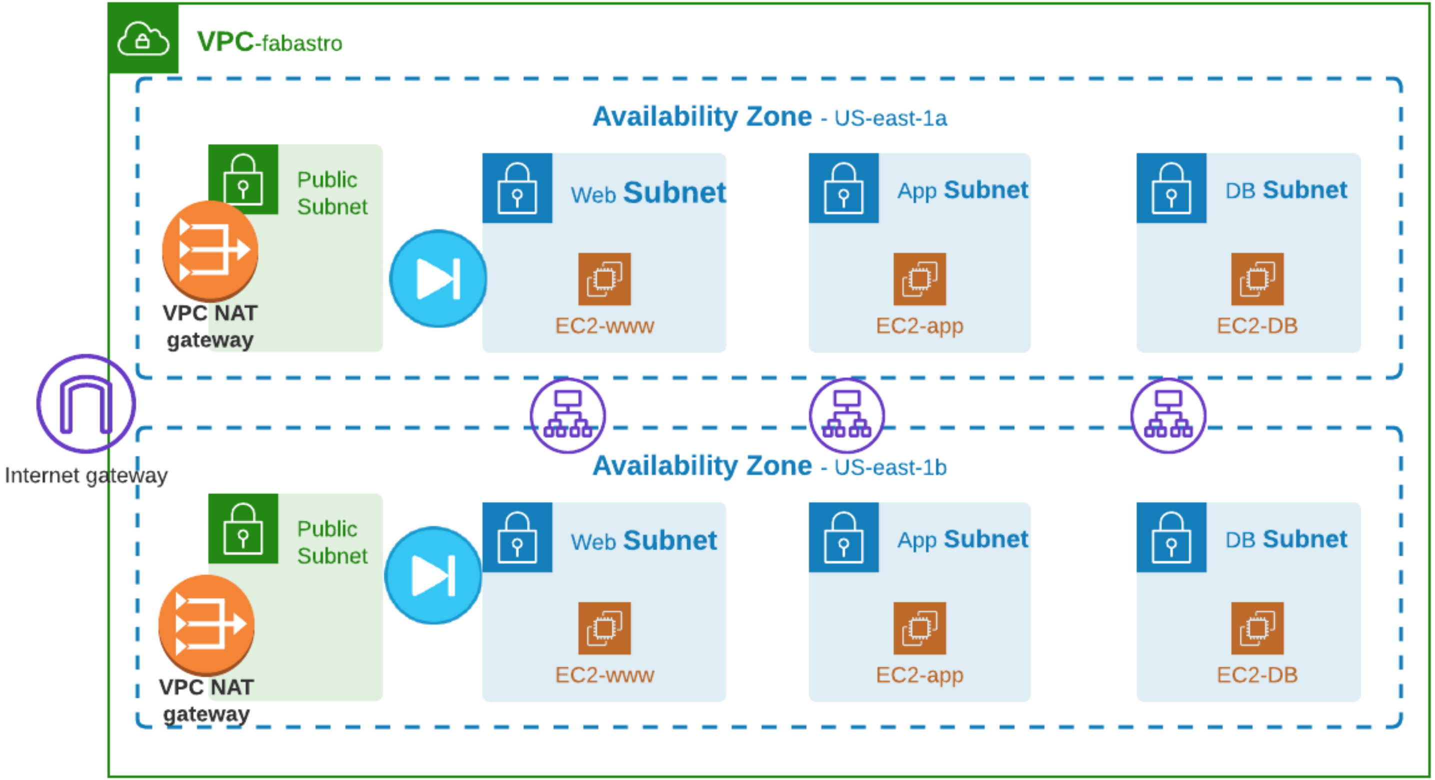
RAvpn with FTD and FMC in FabAstro



EC2 Instances Outgoing sessions

- Nat Gateway for each availability Zone
- Egress transit VPC

Example using Nat Gateway



Challenges with per VPC Nat Gateway

Scalability

Internet gateway and NatGateway per AZ for each VPC

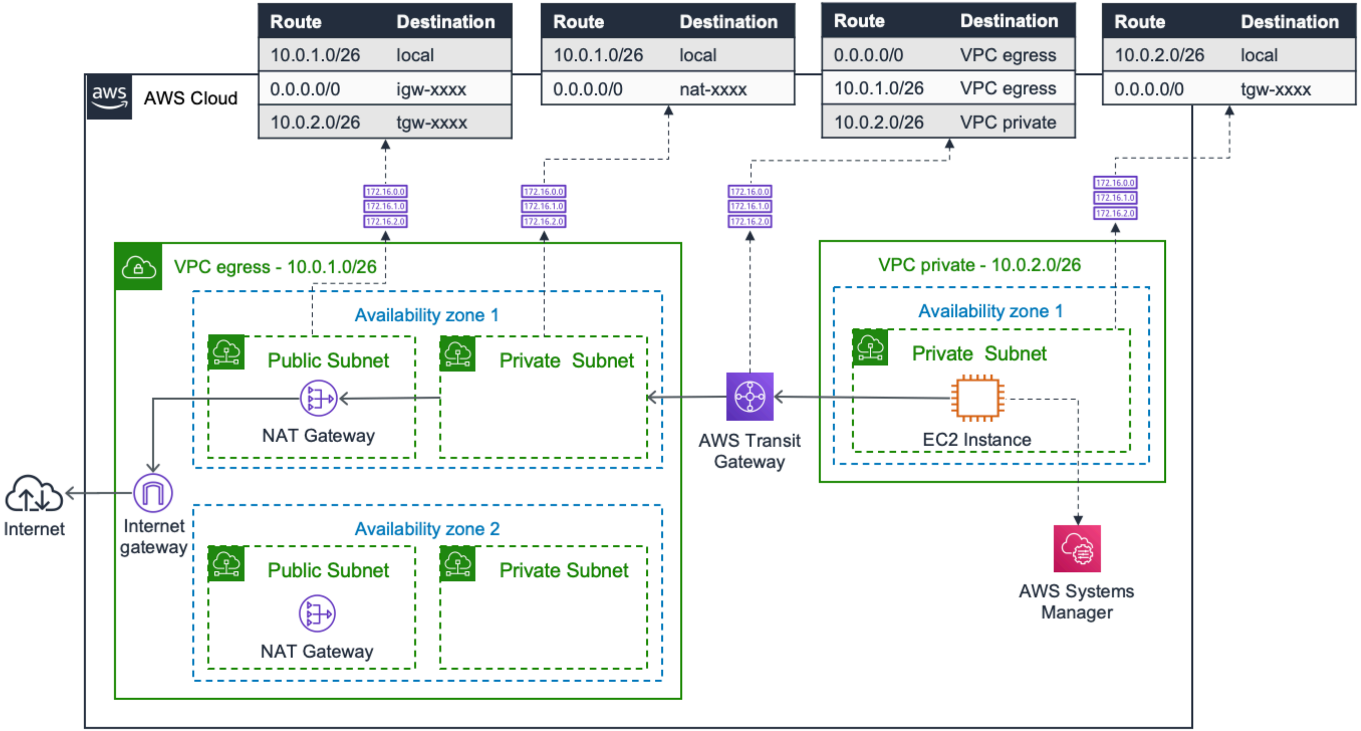
Financial

Refer to Scalability challenge

Security

No control nor visibility over outgoing sessionsh

Example using Egress Transit VPC



Route	Destination
10.0.1.0/26	local
0.0.0.0/0	igw-xxxx
10.0.2.0/26	tgw-xxxx

Route	Destination
10.0.1.0/26	local
0.0.0.0/0	nat-xxxx

Route	Destination
0.0.0.0/0	VPC egress
10.0.1.0/26	VPC egress
10.0.2.0/26	VPC private

Route	Destination
10.0.2.0/26	local
0.0.0.0/0	tgw-xxxx

Possible to insert a single instance of NGFW per AZ

Security through visibility

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

AWS Security Solutions

Identity

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

Detective control

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

Secure Cloud Analytics

Infrastructure security

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

Secure Cloud Workload

Data protection

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

Incident response

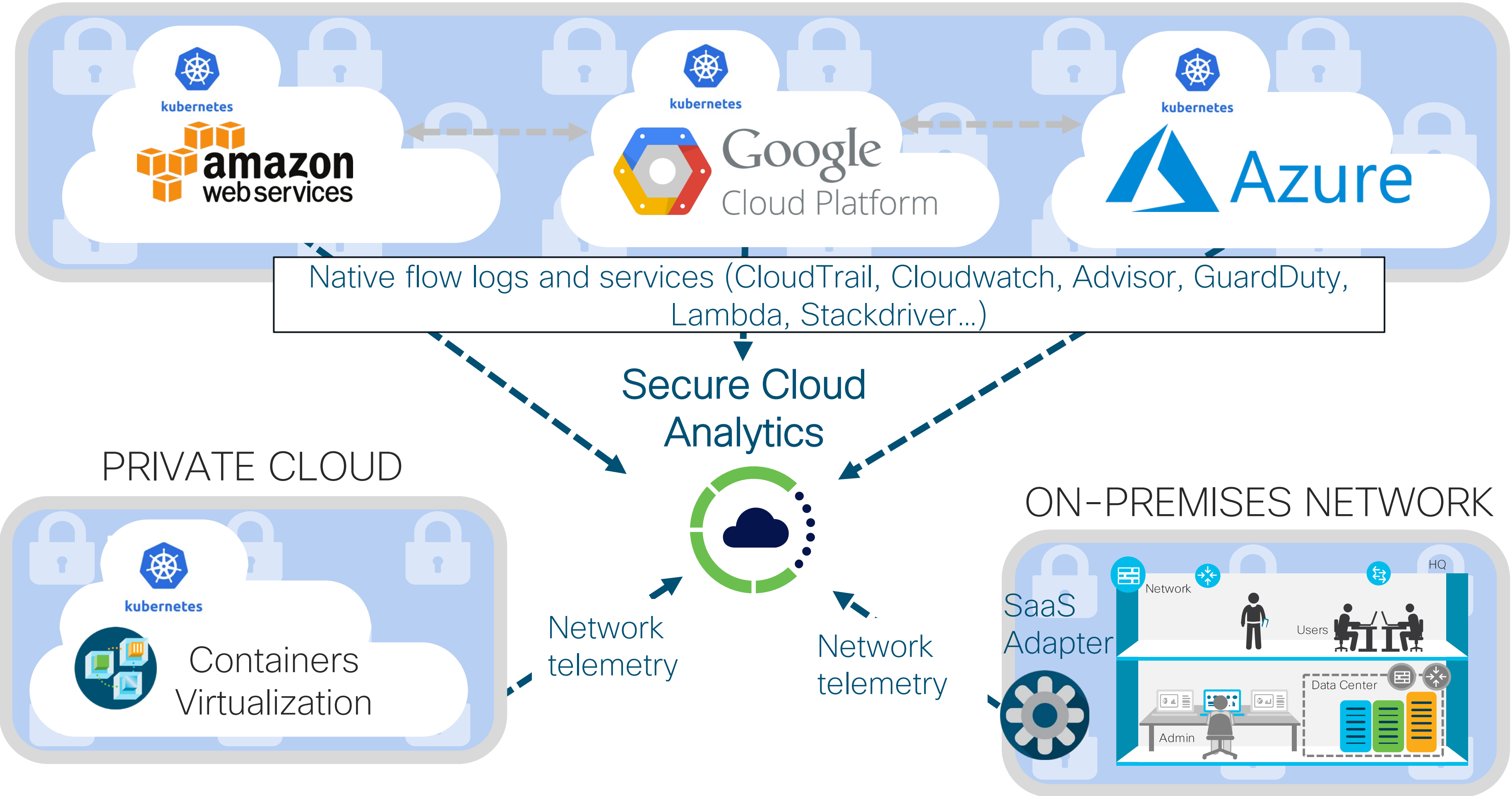
- AWS Config Rules
- AWS Lambda

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/



Native flow logs and services (CloudTrail, Cloudwatch, Advisor, GuardDuty, Lambda, Stackdriver…)

Secure Cloud Analytics

PRIVATE CLOUD

Containers Virtualization

Network telemetry

Network telemetry

ON-PREMISES NETWORK

SaaS Adapter

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?

Host based security

Tetration

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

Conclusion

SAFE Design Guide

Places in the Network: Secure Cloud

Secure Cloud for AWS - Design Guide

April 2020

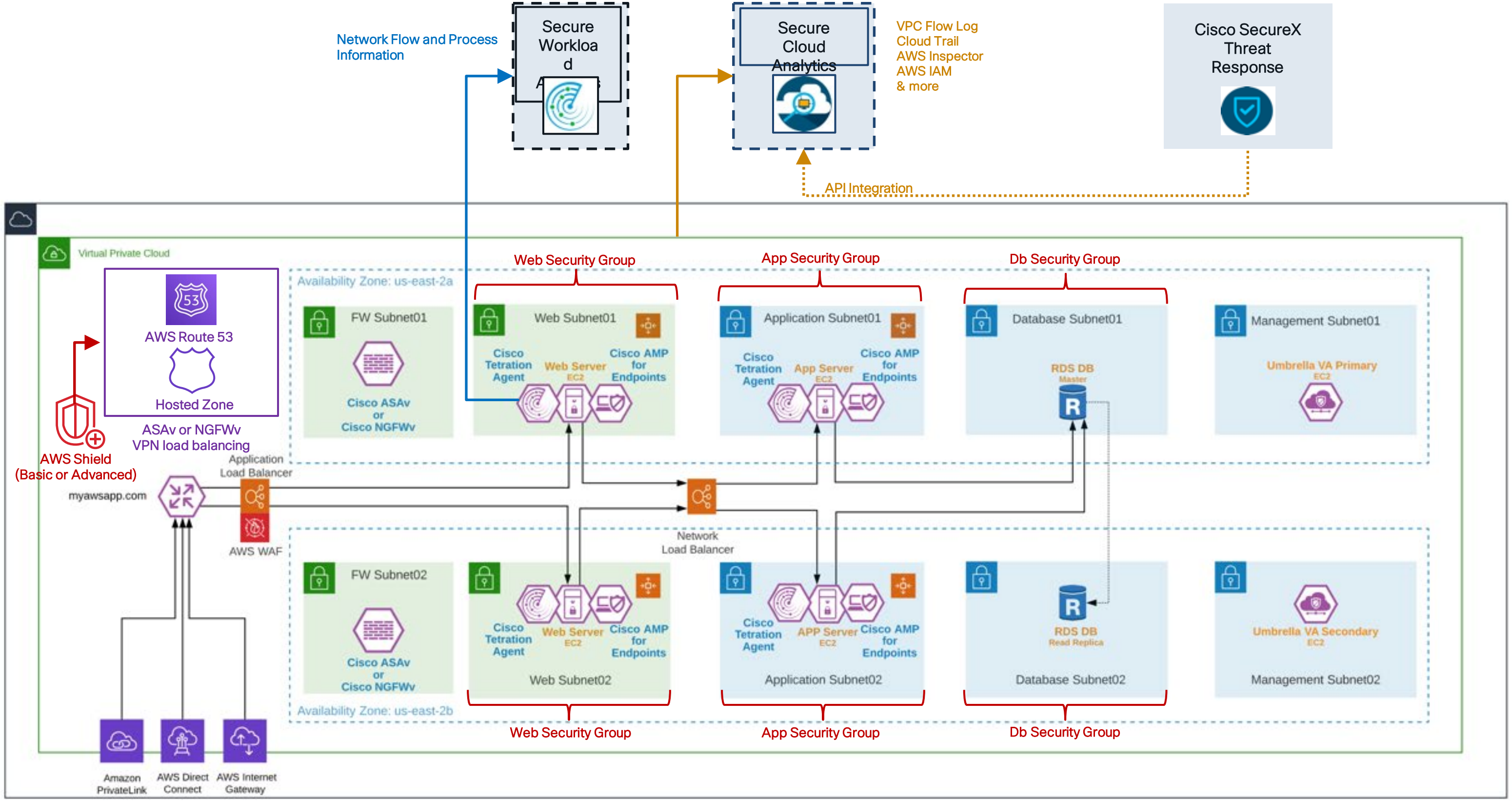
SAFE

SIMPLIFIES SECURITY

Cisco Validate Design Guide for AWS / Azure

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/secure-aws-design.pdf
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-azure-design-guide.pdf

Cisco Secure Cloud Architecture for AWS



Network Flow and Process Information

Secure Workloa d

Secure Cloud Analytics

VPC Flow Log
Cloud Trail
AWS Inspector
AWS IAM
& more

Cisco SecureX Threat Response

API Integration

Virtual Private Cloud

Availability Zone: us-east-2a

Web Security Group

App Security Group

Db Security Group

AWS Route 53

Hosted Zone

AWS Shield (Basic or Advanced)

ASAv or NGFWv VPN load balancing

Application Load Balancer

myawsapp.com

AWS WAF

FW Subnet01

Cisco ASAv or Cisco NGFWv

Web Subnet01

Cisco Tetration Agent

Web Server EC2

Cisco AMP for Endpoints

Application Subnet01

Cisco Tetration Agent

App Server EC2

Cisco AMP for Endpoints

Database Subnet01

RDS DB Master

Management Subnet01

Umbrella VA Primary EC2

Network Load Balancer

FW Subnet02

Cisco ASAv or Cisco NGFWv

Cisco Tetration Agent

Web Server EC2

Cisco AMP for Endpoints

Web Subnet02

Cisco Tetration Agent

APP Server EC2

Cisco AMP for Endpoints

Application Subnet02

RDS DB Read Replica

Database Subnet02

Umbrella VA Secondary EC2

Management Subnet02

Availability Zone: us-east-2b

Web Security Group

App Security Group

Db Security Group

Amazon PrivateLink

AWS Direct Connect

AWS Internet Gateway

The bridge to possible

Thank you

cisco Live!

#CiscoLive