

CISCO *Live!*



#CiscoLive



The bridge to possible

# Securing Multi-VPC Architectures in AWS

Cisco Live 2022 Las Vegas

Ryan MacLennan, Technical Marketing Engineer  
BRKSEC-2144



#CiscoLive

# Cisco Webex App

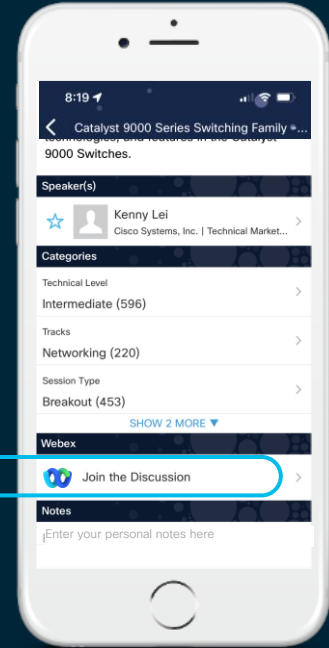
## Questions?

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

## How

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

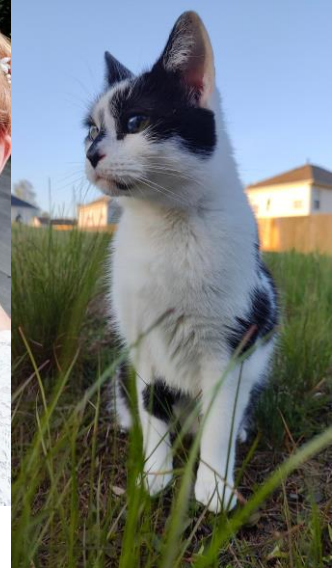
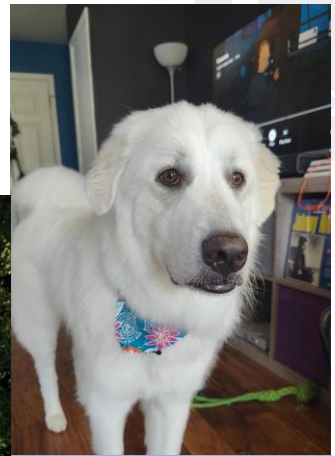
Webex spaces will be moderated by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2144>

# About Me

- Located in RTP
- Have a dog, cat, and three ferrets
- Went to Rochester Institute of Technology
- Been at Cisco since 2016
- Married less than a year



# Agenda

- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion



# Introduction

- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion



# Reasons to use multiple VPCs



Ease of management



Business function

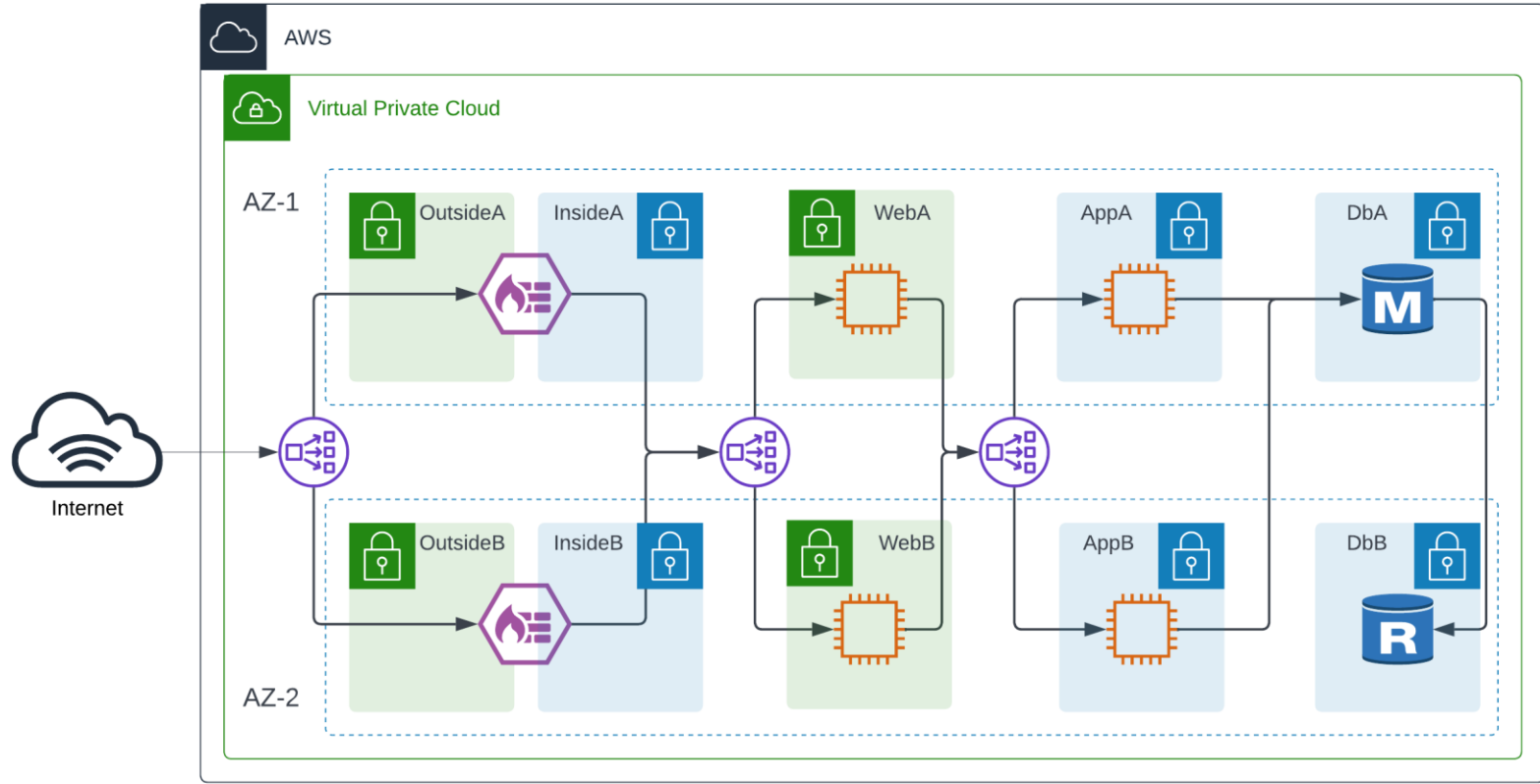


Security



Separate customers

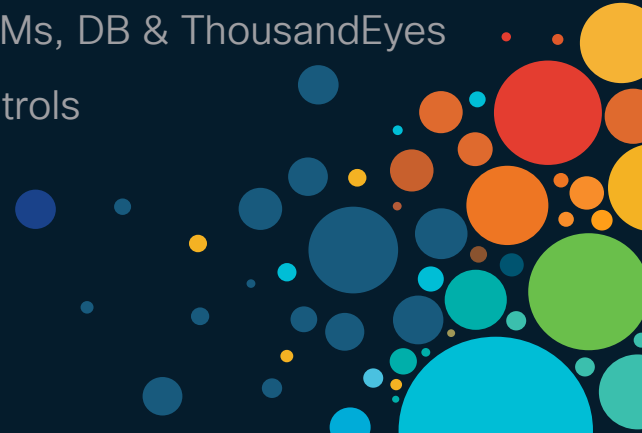
# Traditional Application (IaaS)





# Overall Design

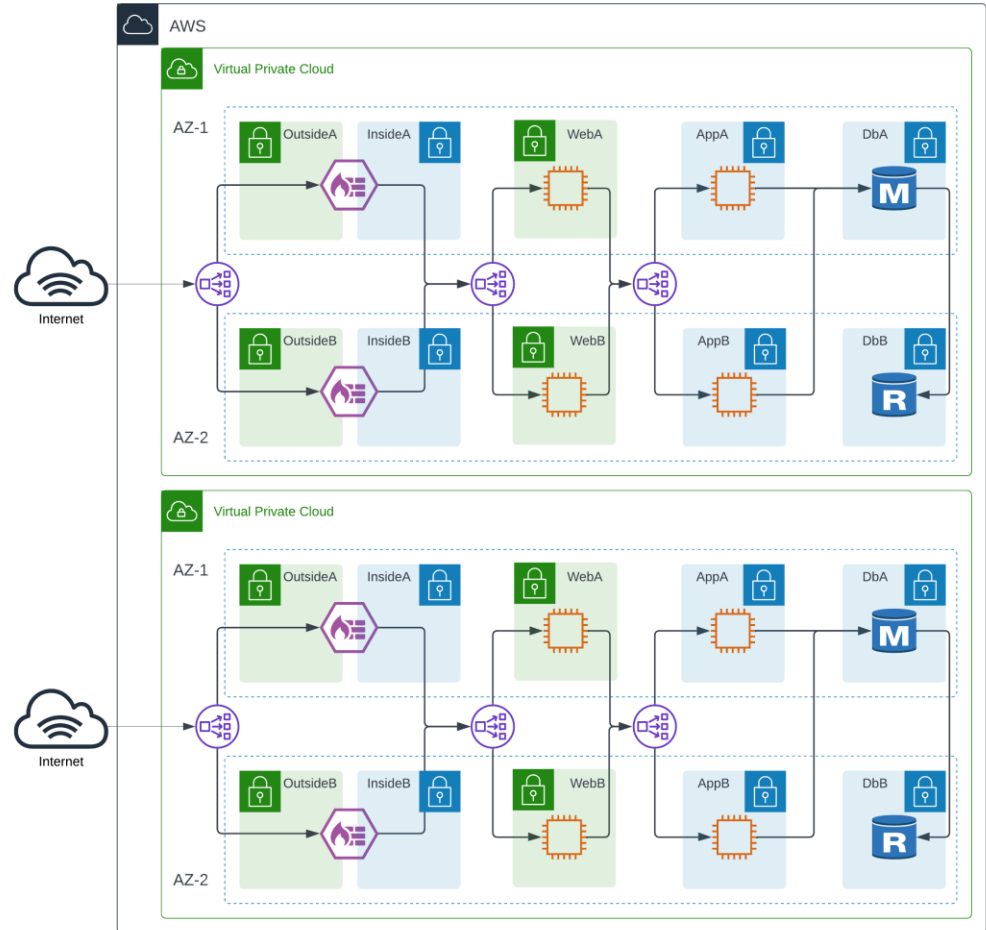
- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion



# Design Diagrams

## High-Level Diagram (Traditional)

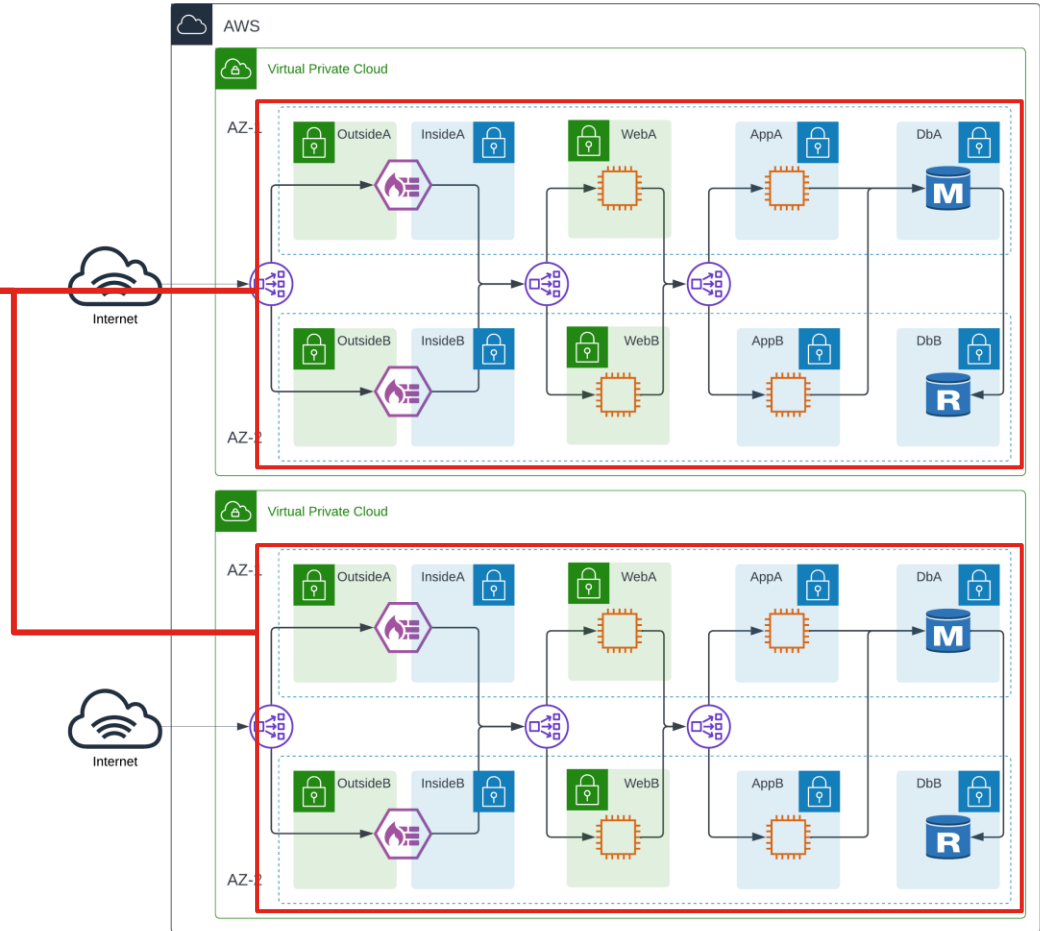
- Wasteful
- Expensive
- Extra maintenance
- Additional overhead



# Design Diagrams

## High-Level Diagram (Traditional)

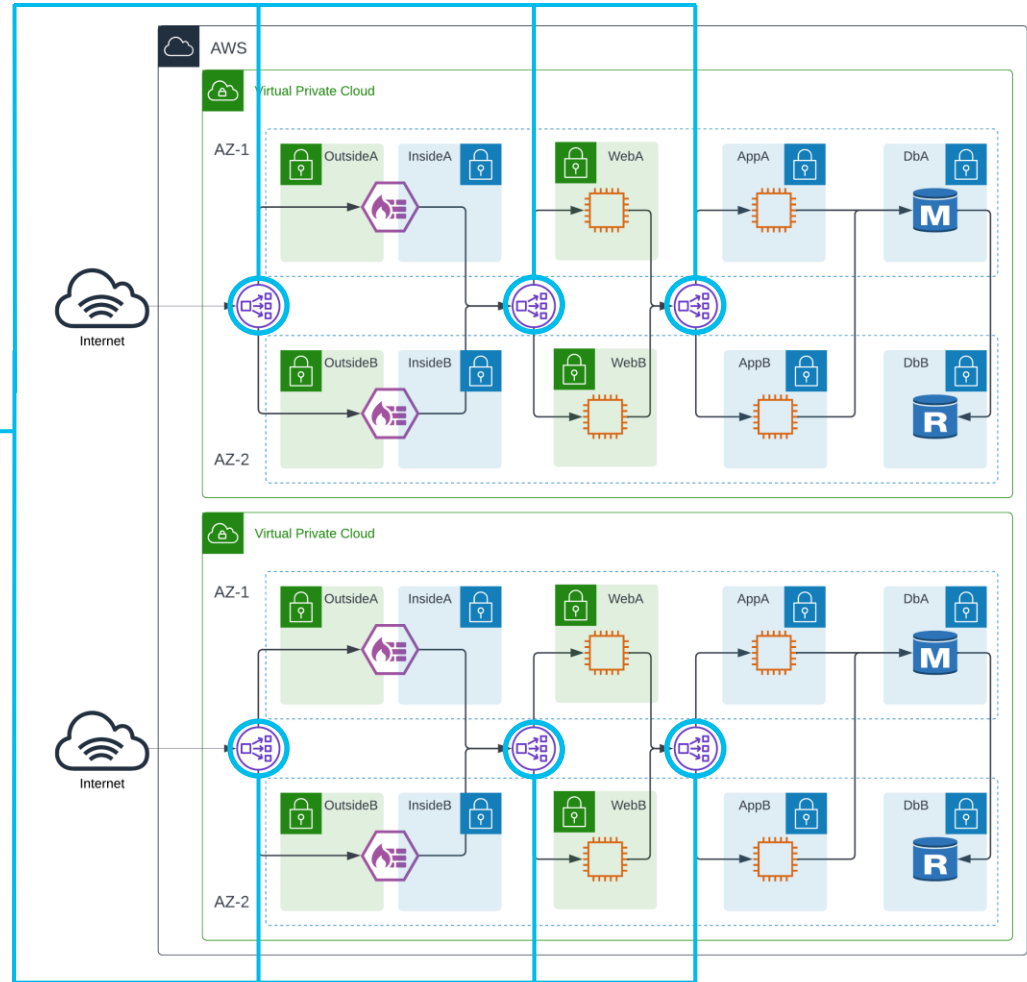
- Duplicate Workloads
- Multiple Load Balancers
- Four Firewalls



# Design Diagrams

## High-Level Diagram (Traditional)

- Duplicate Workloads
- Multiple Load Balancers
- Four Firewalls

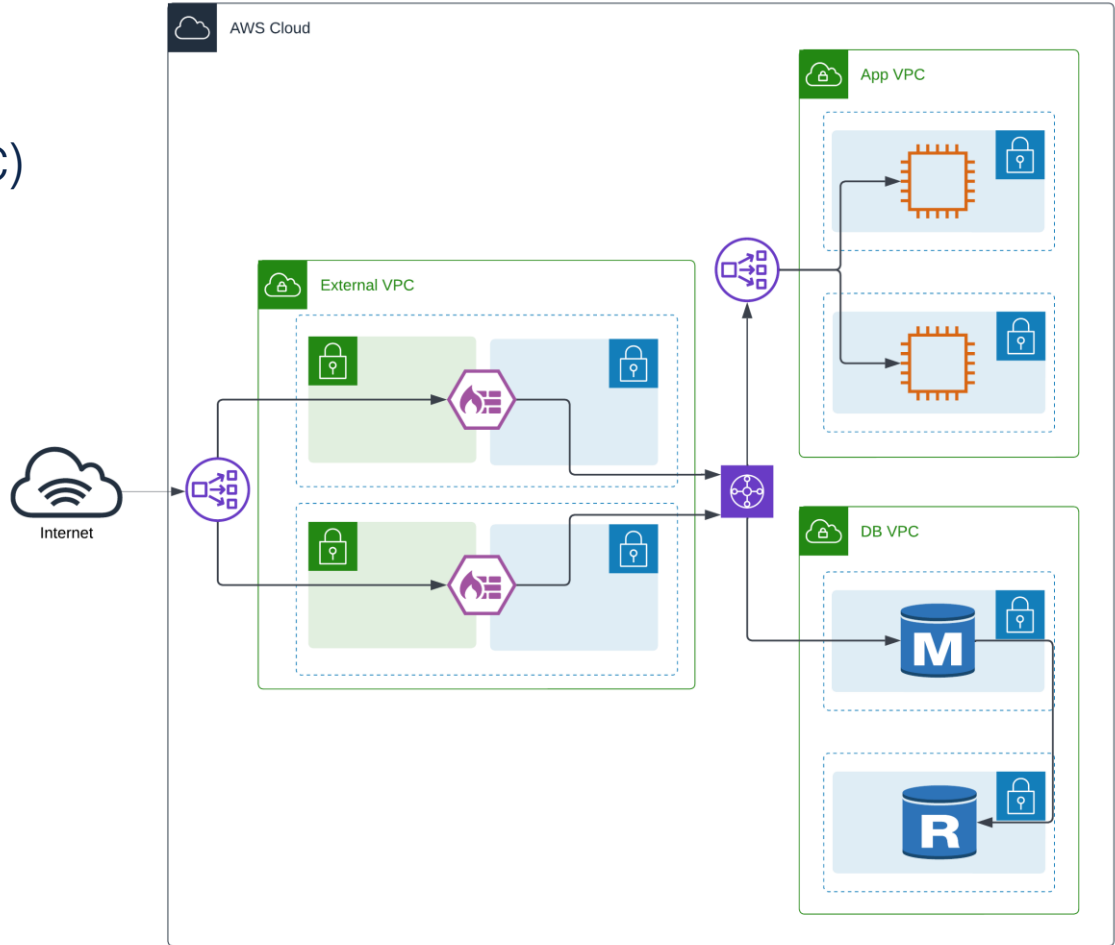




# Design Diagrams

## High-Level Diagram (M-VPC)

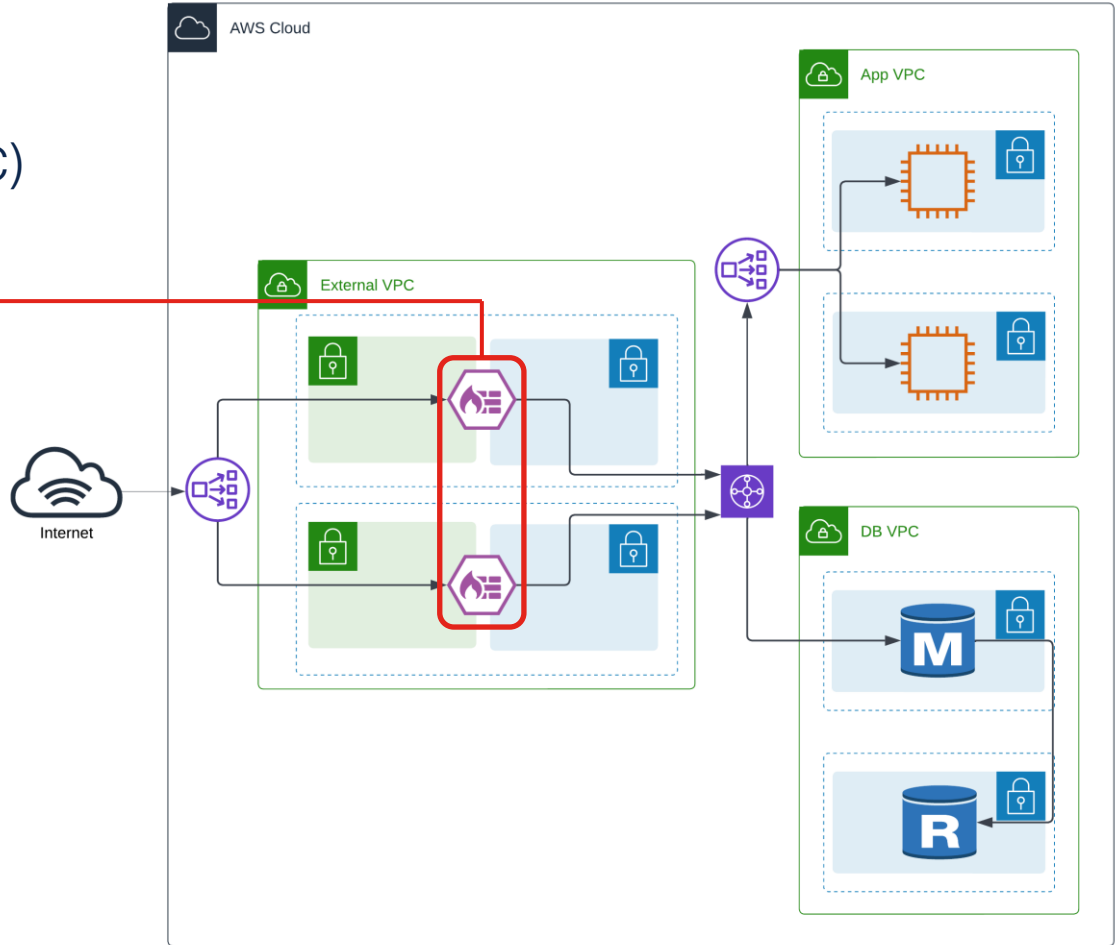
- Reduces complexity
- Less expensive
- Easier to maintain
- Less overhead



# Design Diagrams

## High-Level Diagram (M-VPC)

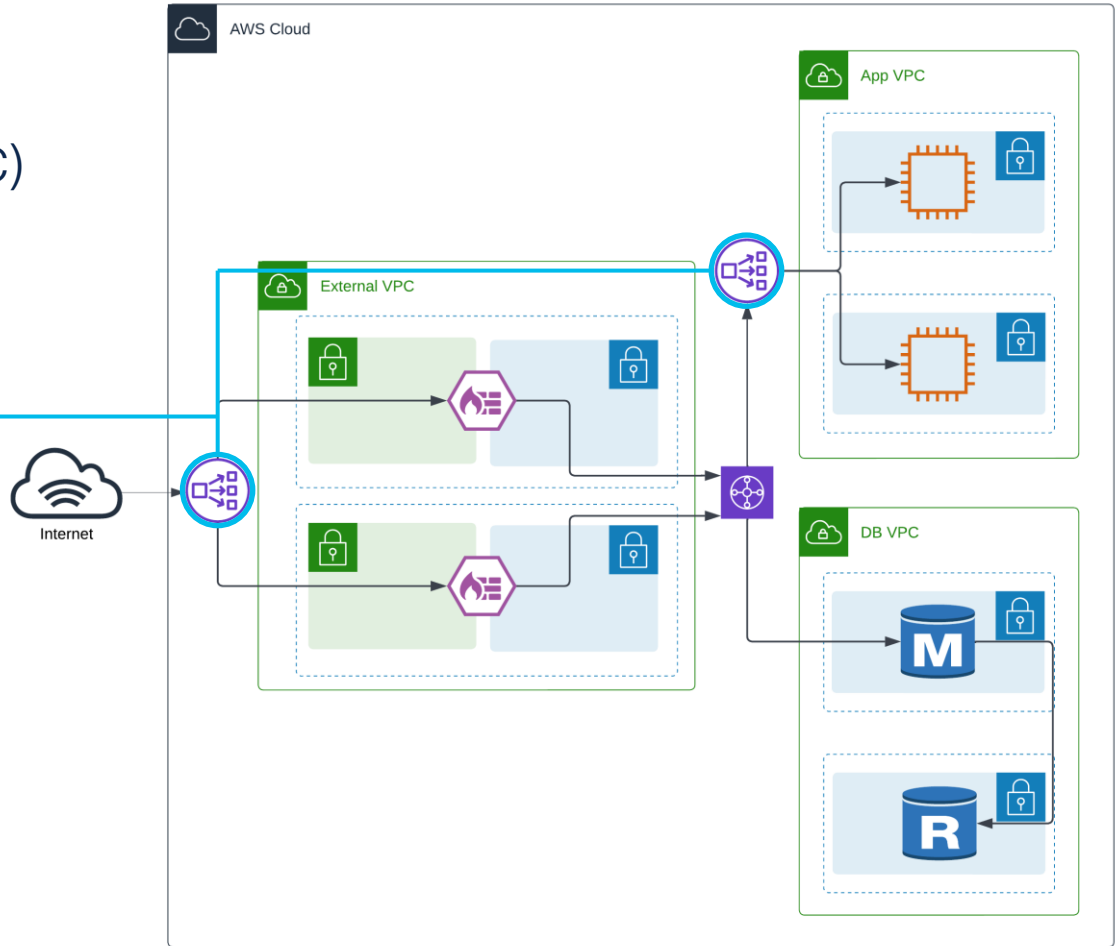
- 2 Firewalls
- 2 Load Balancers
- No Duplicate Workloads



# Design Diagrams

## High-Level Diagram (M-VPC)

- 2 Firewalls
- 2 Load Balancers
- No Duplicate Workloads

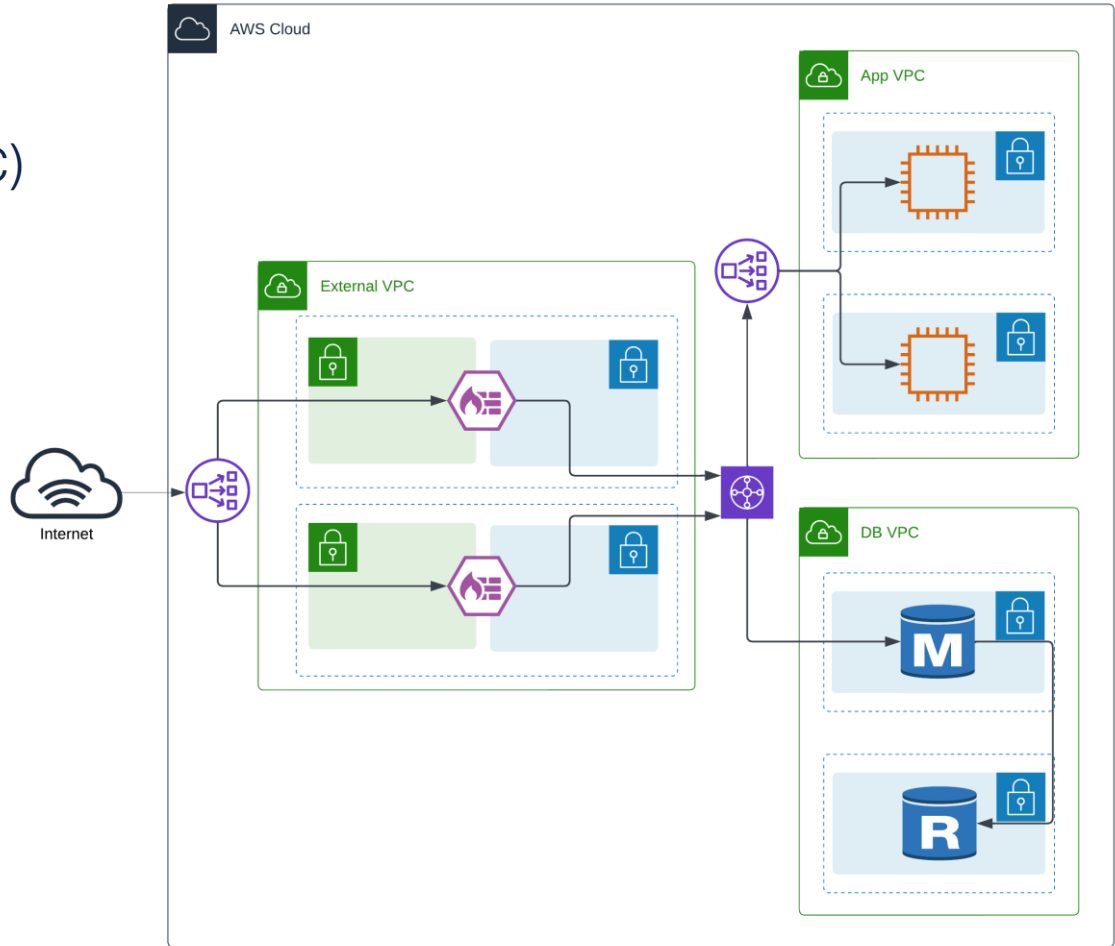




# Design Diagrams

## High-Level Diagram (M-VPC)

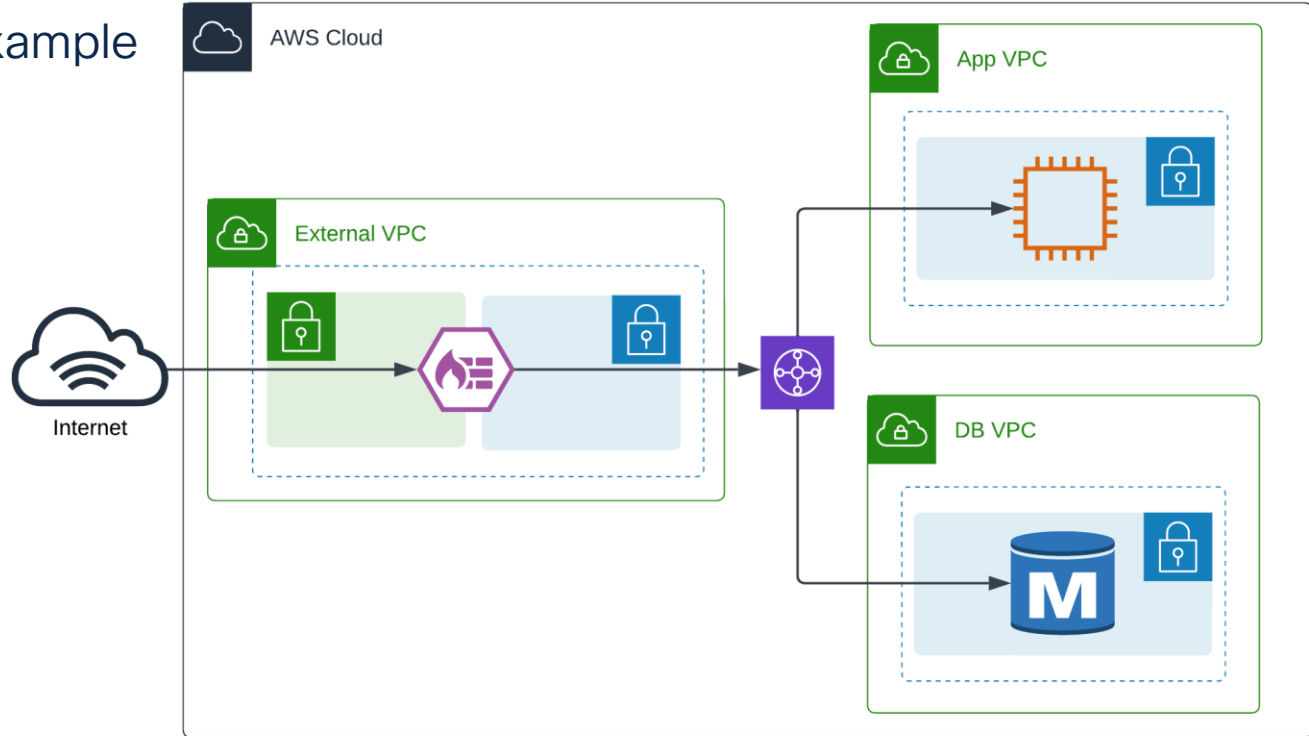
- 2 Firewalls
- 2 Load Balancers
- No Duplicate Workloads



# Design Diagrams

## High Level Simple Example

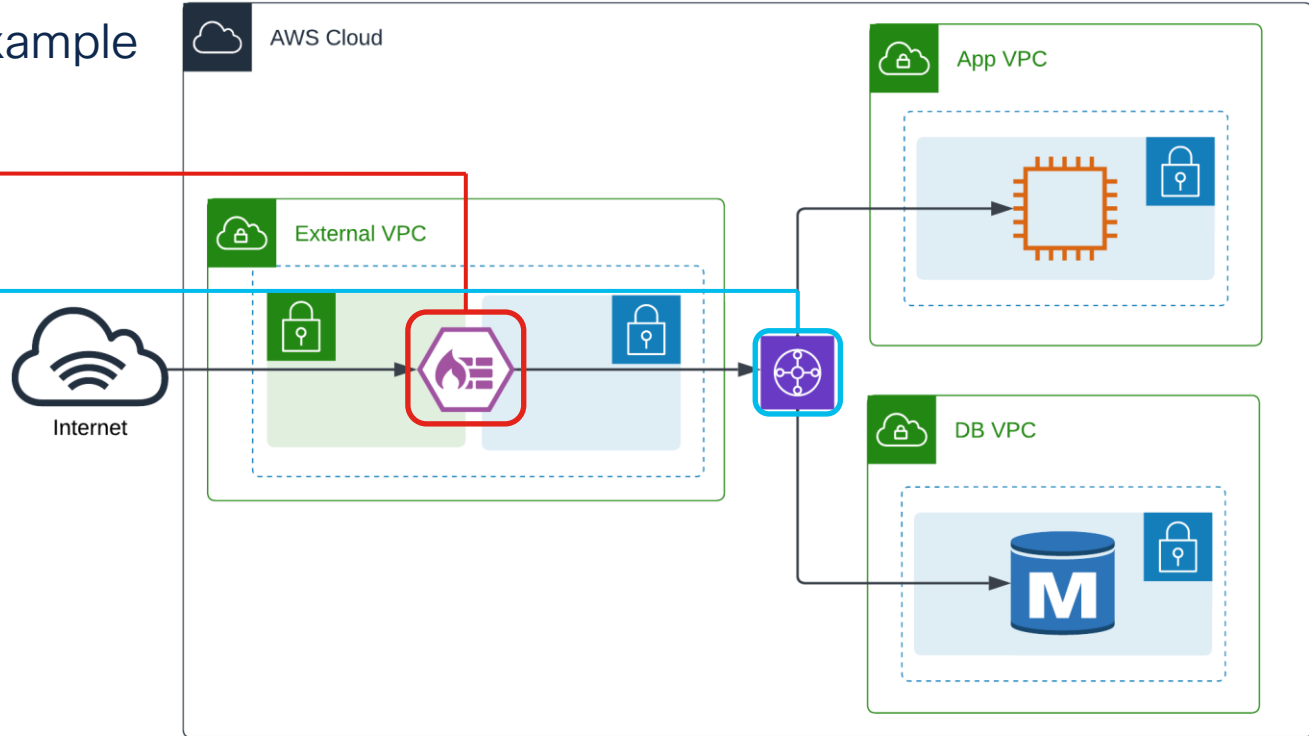
- Single FTD
- Transit Gateway
- No Load Balancer
- No Redundancy
- No Web Tier



# Design Diagrams

## High Level Simple Example

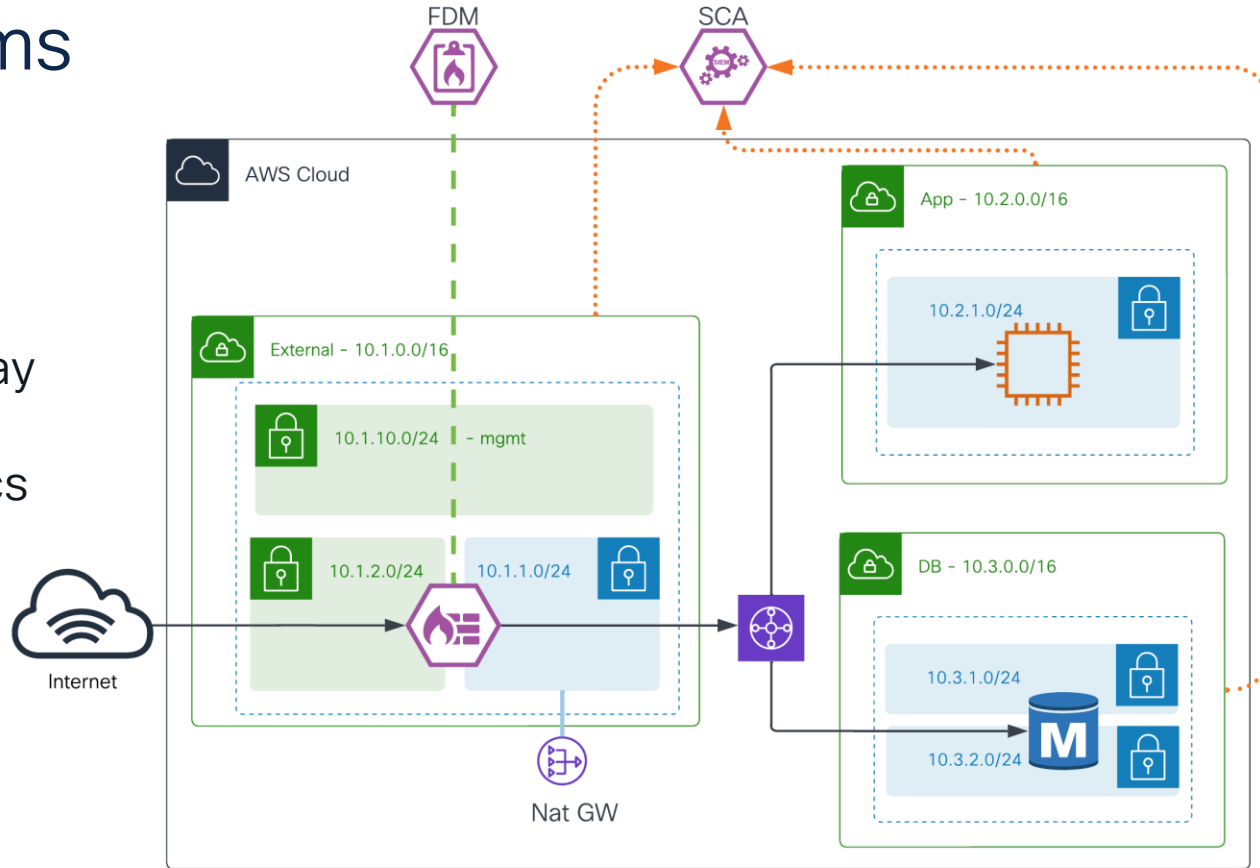
- Single FTD
- Transit Gateway
- No Load Balancer
- No Redundancy
- No Web Tier



# Design Diagrams

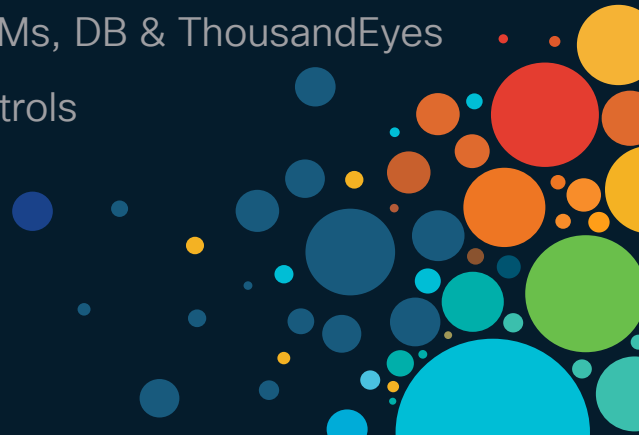
## Deep Dive Diagram

- FDM manages FTD
- Apps use NAT gateway
- Secure Cloud Analytics (SCA) monitors VPCs
- No auto-scaling



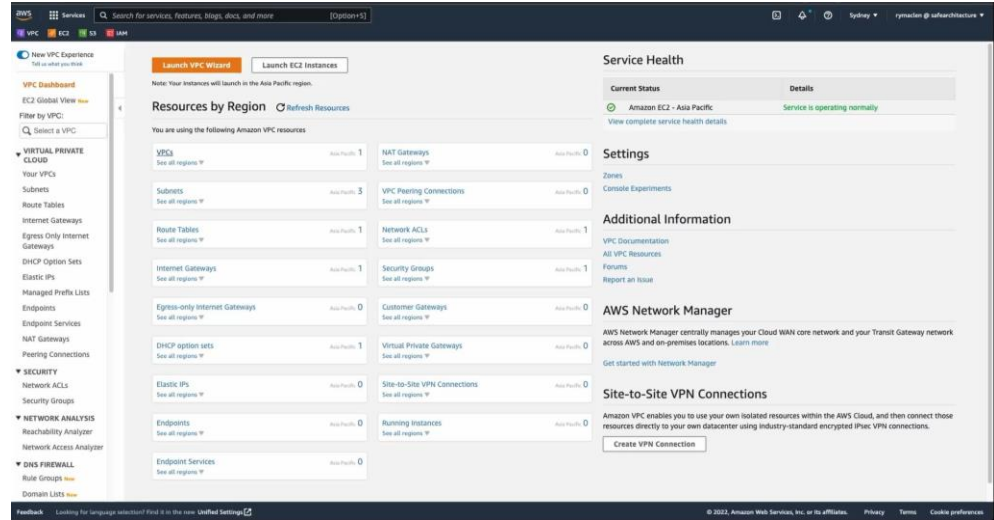
# VPC & Subnet creation

- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion



# VPC Setup

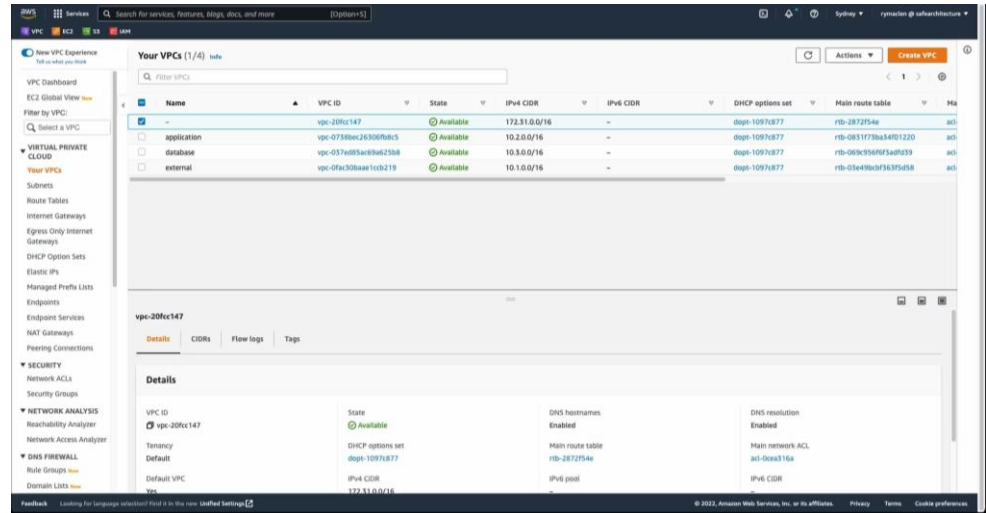
Name	CIDR
database	10.3.0.0/16
application	10.2.0.0/16
external	10.1.0.0/16



The screenshot shows the AWS Management Console VPC Dashboard for the Asia Pacific (Sydney) region. The left sidebar contains navigation links for VPC, EC2, IAM, and other services. The main content area displays 'Resources by Region' with a grid of VPC resources including VPCs, Subnets, Route Tables, Internet Gateways, Egress-only Internet Gateways, DHCP option sets, Elastic IPs, Endpoints, and Endpoint Services. A 'Service Health' panel on the right indicates that the Amazon EC2 - Asia Pacific service is operating normally. Below the health panel are sections for 'Settings', 'Additional Information', 'AWS Network Manager', and 'Site-to-Site VPN Connections'.

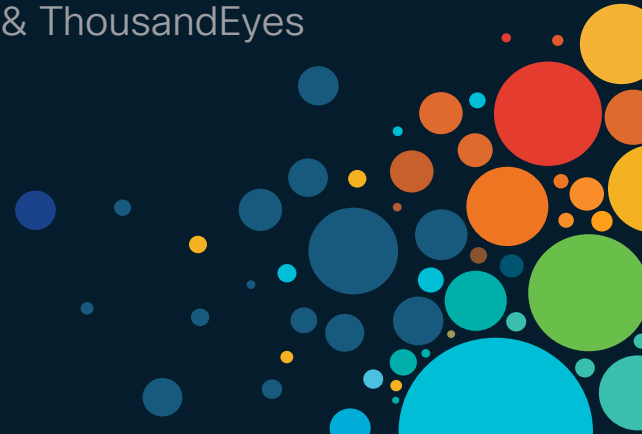
# Subnet Creation

Name	CIDR	VPC
dbNetA	10.3.1.0/24	database
dbNetB	10.3.2.0/24	database
appNet	10.2.1.0/24	application
outside	10.1.2.0/24	external
inside	10.1.1.0/24	external
mgmt	10.1.10.0/24	external



# Secure Cloud Analytics

- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion





# SCA Requirements

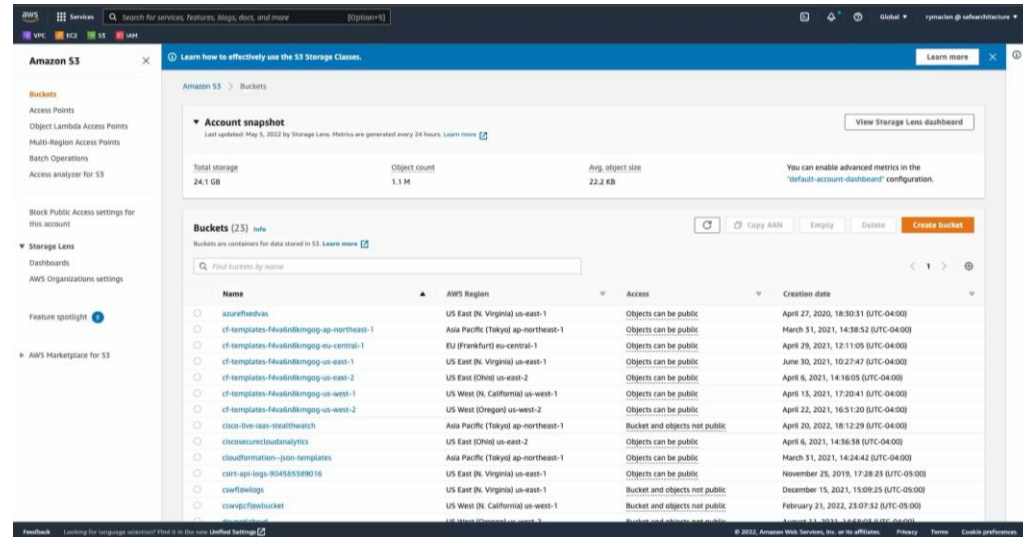
- S3 Bucket
- IAM Role & Policy
- VPC Flow Log Monitoring
- Finish on-boarding after VMs deployed

# SCA Requirements

- S3 Bucket
- IAM Role & Policy
- VPC Flow Log Monitoring
- Finish on-boarding after VMs deployed

# S3 Bucket

- Do not need to create first
- Will be created when doing Flow Log setup



# IAM Role & Policy

Settings

Alerts/Watchlists

Integrations

Entity Groups

Account Management

Subnets

Webhooks/Services

Sensors

aws

About AWS

1

**To integrate Secure Cloud Analytics with AWS, you will:**

- Create an IAM role that has read access to the resources in an account
- Save that role to the [Settings > Integrations > AWS > Credentials](#) page
- Generate a policy for granting read access to an S3 location in the [Settings > Integrations > AWS > VPC Flow Logs](#) page
- Save the S3 location in the [Settings > Integrations > AWS > VPC Flow Logs](#) page

2

**To create the IAM role:**

- Go to the [AWS Console for IAM](#)
- Create an IAM Role:
  - Select the *Another AWS account* type
  - Set the *Account ID* to XXXXXXXXXX
  - Select *Require external ID* and enter XXXXXXXXXX
- On the *Attach permissions policies* page, click the *Create policy* button:
  - Paste the **IAM Role Policy document** below into the *JSON* tab
  - Click *Next* until you're prompted to review the new policy
  - Give the policy a name (such as `obsrvbl_policy`) and then click *Create policy*
- When you return to the *Attach permissions policies* screen, click the refresh icon and then select the new policy from the list
- Click *Next* until you're prompted to review the new role
- Give the new role a name (such as `obsrvbl-role`) and then click *Create role*

3

**After the role is created:**

- Select it from the list in the AWS Console
- Copy its *Role ARN* to the clipboard
- Return to this page and select the [Settings > Integrations > AWS > Credentials](#) page
- Click the *Add New Credentials* button:
  - Give the role a descriptive name (such as `production account`)
  - Paste in the Role ARN
  - Click the *Create* button

# VPC Flow Logs

The screenshot displays the AWS Management Console VPC Dashboard. The top navigation bar includes the AWS logo, a search bar, and user information. The left sidebar contains a navigation menu with categories like VPC, EC2, S3, and IAM. The main content area is titled 'Resources by Region' and shows a list of VPC resources for the Asia Pacific region. The 'Service Health' section on the right indicates that Amazon EC2 - Asia Pacific is operating normally. The 'Settings' section includes links for Zones and Console Experiments. The 'Additional Information' section provides links to VPC Documentation, All VPC Resources, Forums, and Report an Issue. The 'AWS Network Manager' section describes its role in managing Cloud WAN core networks. The 'Site-to-Site VPN Connections' section explains how to use VPC for isolated resources within the AWS Cloud.

**Resources by Region** Refresh Resources

You are using the following Amazon VPC resources

Resource	Region	Count
VPCs	Asia Pacific	4
Subnets	Asia Pacific	8
Route Tables	Asia Pacific	2
Internet Gateways	Asia Pacific	2
Egress-only Internet Gateways	Asia Pacific	2
DHCP option sets	Asia Pacific	2
Elastic IPs	Asia Pacific	2
Endpoints	Asia Pacific	2
Endpoint Services	Asia Pacific	2
NAT Gateways	Asia Pacific	2
VPC Peering Connections	Asia Pacific	2
Network ACLs	Asia Pacific	2
Security Groups	Asia Pacific	2
Customer Gateways	Asia Pacific	2
Virtual Private Gateways	Asia Pacific	2
Site-to-Site VPN Connections	Asia Pacific	2
Running Instances	Asia Pacific	2

**Service Health**

Current Status	Details
Amazon EC2 - Asia Pacific	Service is operating normally

**Settings**

- Zones
- Console Experiments

**Additional Information**

- VPC Documentation
- All VPC Resources
- Forums
- Report an Issue

**AWS Network Manager**

AWS Network Manager centrally manages your Cloud WAN core network and your Transit Gateway network across AWS and on-premises locations. [Learn more](#)

[Get started with Network Manager](#)

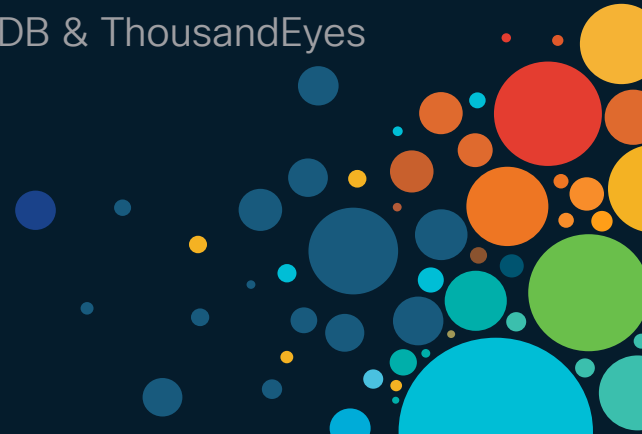
**Site-to-Site VPN Connections**

Amazon VPC enables you to use your own isolated resources within the AWS Cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

[Create VPN Connection](#)

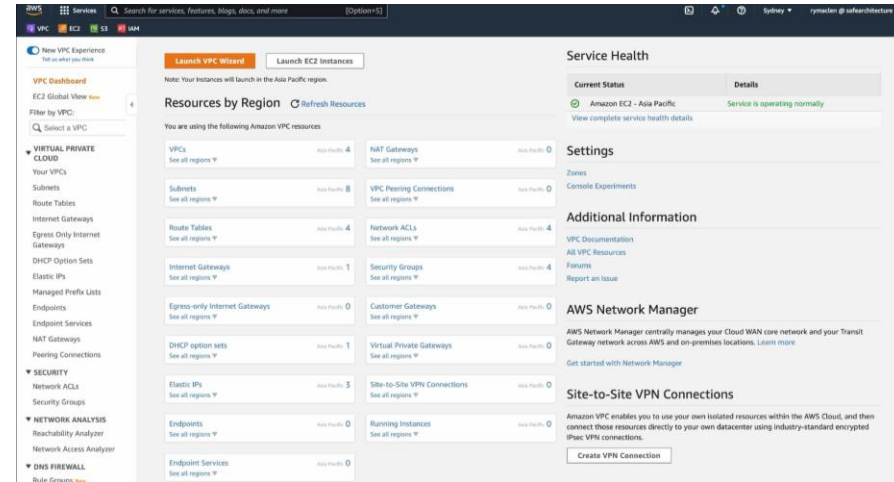
# Gateways & Routing

- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion



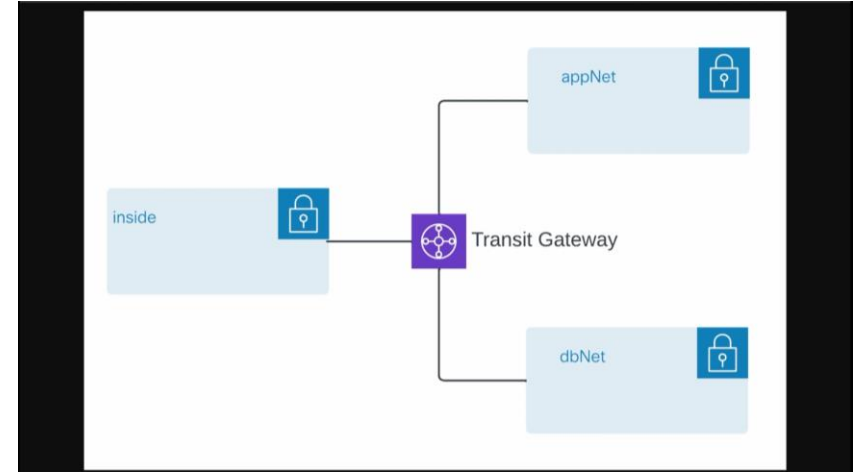
# Gateway Creation

Name	VPC	Type
internetGw	external	Internet gateway
appNatGw	external	NAT gateway
internalTransitGw		Transit gateway



# Transit Gateway Attachments

Name	VPC	Type	Subnets
tg-to-app	application	VPC	appNet
tg-to-db	database	VPC	dbNetA
tg-to-ext	external	VPC	inside





# VPC Routing

Route Table	CIDR	Dest.	Associated Subnets	VPC
mgmt	0.0.0.0/0	Internet gateway	mgmt	external
inside	0.0.0.0/0	Nat gateway	inside	external
inside	10.2.0.0/16	Transit gateway	inside	external
inside	10.3.0.0/16	Transit gateway	inside	external
outside	0.0.0.0/0	Internet gateway	outside	external
app	0.0.0.0/0	Transit gateway	appNet	application
database	0.0.0.0/0	Transit gateway	dbNetA	database

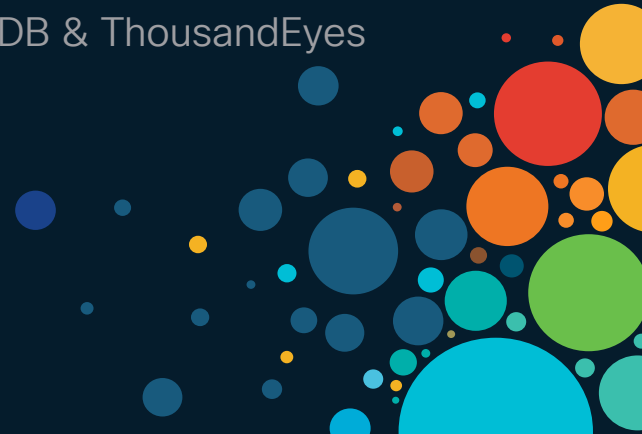
# VPC Routing Cont.

The screenshot shows the AWS Management Console interface for the 'Route tables (5)' page. The left sidebar contains a navigation menu with categories like VPC, SECURITY, and NETWORK ANALYSIS. The main content area displays a table of route tables with columns: Name, Route table ID, Explicit subnet associations, Edge associations, Main, VPC, and Owner ID. The table lists five route tables: 'outside', 'app', '-', 'mgmt', and 'database'. Below the table, there is a section titled 'Select a route table' with three icons.

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
outside	rtb-03e49bcbf363f5d58	-	-	Yes	vpc-0fac30baae1ccb219   exte...	904585389016
app	rtb-0831f73ba34f01220	-	-	Yes	vpc-0738bec26306fb8c5   app...	904585389016
-	rtb-2872f54e	-	-	Yes	vpc-20fcc147	904585389016
mgmt	rtb-05b94e7bf0654961f	-	-	No	vpc-0fac30baae1ccb219   exte...	904585389016
database	rtb-069c956f6f3adfd39	-	-	Yes	vpc-037ed85ac69a625b8   dat...	904585389016

# Create Security Groups

- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion



# Create Security Groups

appSg

Type	Source	Rule Type
HTTP	0.0.0.0/0	Inbound
HTTPS	0.0.0.0/0	Inbound

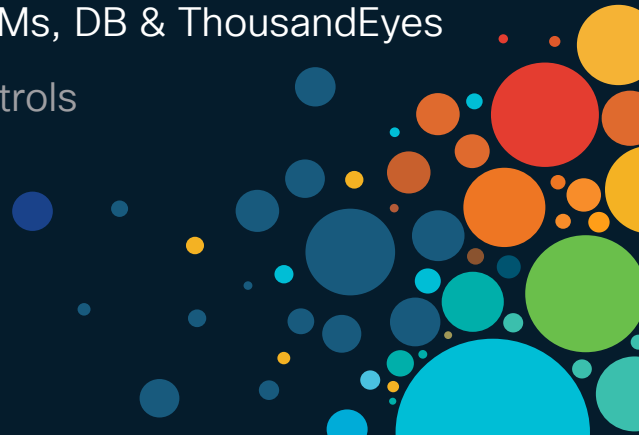
ftd-http-sg

Type	Source	Rule Type
HTTP	0.0.0.0/0	Inbound
HTTPS	0.0.0.0/0	Inbound

- Create two security groups
- Allow HTTP & HTTPS
- appSg
  - Application VPC
- ftd-http-sg
  - External VPC

# Deploy FTD, VMs, DB & ThousandEyes

- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion



# Deploy Firepower Threat Defense (FTD)



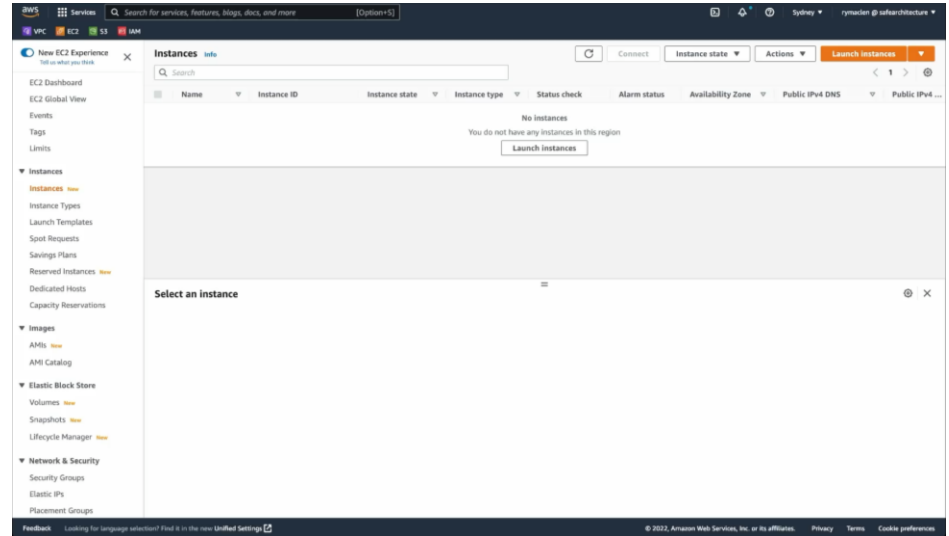
# Create vNICs

Name	Private IP	Public IP	Auto-Assign
inside	10.1.1.10	N/A	No
outside	10.1.2.10	Yes	No
diag	10.1.10.11	No	No

The screenshot shows the AWS Management Console interface for creating a new network interface. The breadcrumb navigation at the top indicates the path: EC2 > Network interfaces > Create network interface. The main heading is 'Create network interface', followed by a sub-header: 'An elastic network interface is a logical networking component in a VPC that represents a virtual network card.' Below this, there are two tabs: 'Details' (selected) and 'Info'. The 'Details' tab contains several sections: 'Description - optional' with a text input field; 'Subnet' with a dropdown menu labeled 'Select subnet' and a refresh icon; 'Private IPv4 address' with radio buttons for 'Auto-assign' (selected) and 'Custom'; 'Elastic Fabric Adapter' with an 'Enable' checkbox; and 'Advanced settings' which is currently collapsed. At the bottom, there is a 'Tags - optional' section with a text area for adding tags. The footer of the console shows the AWS logo, navigation icons, the user's location (Sydney), and their email address (rymcken@saatchiarchitecture.com).

# FTD Deployment

- Create vNICs
  - Allocate Elastic IP to outside vNIC
- Deploy FTD from marketplace
- Attach Interfaces while booting





# Database Deployment

The screenshot displays the Amazon RDS Management Console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and user information. The left sidebar contains a menu with options like Dashboard, Databases, Query Editor, Performance Insights, Snapshots, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Events, Event subscriptions, Recommendations, and Certificate update. The main content area is titled 'Amazon RDS' and features a 'Create database' button. Below this, there's a 'Resources' section listing various RDS resources in the Asia Pacific (Sydney) region, including DB Instances, DB Clusters, Snapshots, and Subnet groups. A 'Recommended for you' section on the right provides links to documentation for implementing Cross-Region DR, testing DR strategy, and time-series tables. The 'Create database' section includes a 'Restore from S3' button and a 'Create database' button, with a note that instances will be launched in the Asia Pacific (Sydney) region. The bottom of the console shows a 'Service health' section and a footer with copyright information and links to privacy and terms.

**Amazon RDS**

**Dashboard**

Databases

Query Editor

Performance Insights

Snapshots

Automated backups

Reserved instances

Proxies

Subnet groups

Parameter groups

Option groups

Custom engine versions

Events

Event subscriptions

Recommendations **0**

Certificate update

**Try the new Amazon RDS Multi-AZ deployment option for MySQL and PostgreSQL.**

For your Amazon RDS for MySQL and PostgreSQL workloads, improve transactional commit latencies by 2x, experience faster failover typically less than 35 seconds and, get read scalability with two readable standby DB instances by deploying the Multi-AZ DB cluster [Learn more](#)

**Create database**

Or, Restore Multi-AZ DB Cluster from Snapshot

**Resources** Refresh

You are using the following Amazon RDS resources in the Asia Pacific (Sydney) region (used/quota)

DB Instances (0/40)	Parameter groups (0)
Allocated storage (0 TB/100 TB)	Default (0)
<a href="#">Click here to increase DB instances limit</a>	Custom (0/100)
DB Clusters (0/40)	Option groups (0)
Reserved instances (0/40)	Default (0)
Snapshots (0)	Custom (0/20)
Manual (0/100)	Subnet groups (0/50)
Automated (0)	Supported platforms VPC
Recent events (0)	Default network vpc-20fcc147
Event subscriptions (0/20)	

**Create database**

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database in the cloud.

[Restore from S3](#) **Create database**

Note: your DB instances will launch in the Asia Pacific (Sydney) region

**Service health** View service health dashboard

**Recommended for you**

**Implementing Cross-Region DR**

Learn how to set up Cross-Region disaster recovery (DR) for Aurora PostgreSQL using an Aurora global database spanning multiple Regions. [Learn more](#)

**Test Your DR Strategy in Minutes**

Amazon Aurora Global Database now supports planned managed failover, making disaster recovery drills a breeze. [Learn more](#)

**Time-Series Tables in PostgreSQL**

Step-by-step guide to design high-performance time series data tables on Amazon RDS for PostgreSQL. [Learn more](#)

**Amazon RDS Backup and Restore using AWS Backup**

Learn how to backup and restore Amazon RDS databases using AWS Backup in just 10 minutes. [Learn more](#)

**Additional information**

[Getting started with RDS](#)

[Overview and features](#)

[Documentation](#)

Feedback Looking for language selection? Find it in the new [Unified Settings](#)

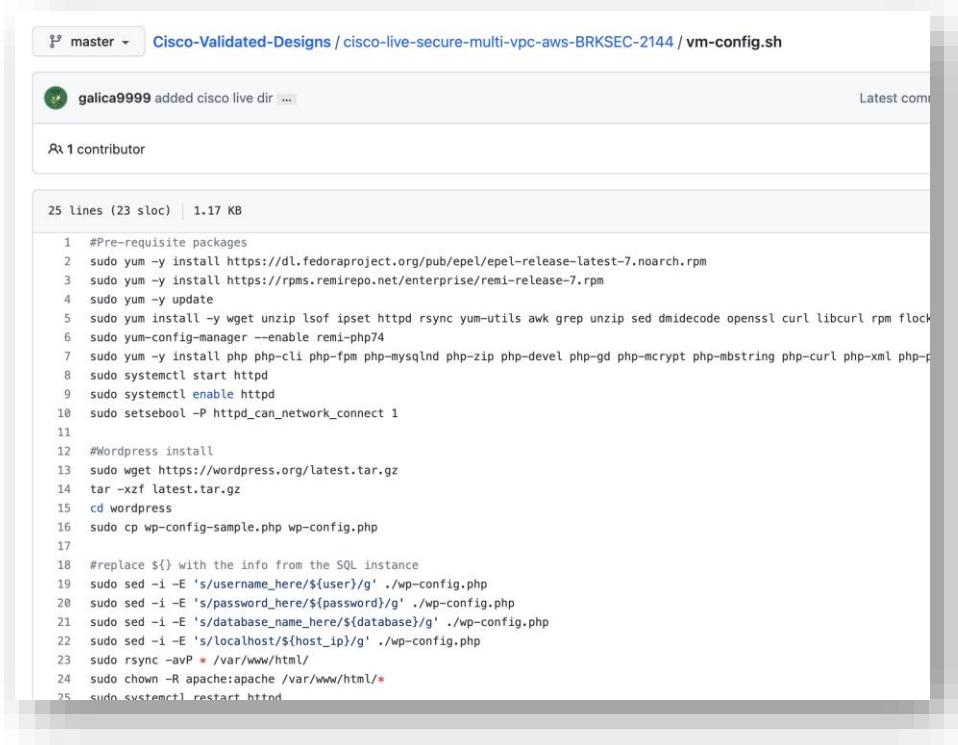
© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

# Database Deployment – Security Group

- 1 rule
  - Allow access from 10.2.0.0/16
  - Service is MYSQL/Aurora

# VM Deployment – Download Config File

- Obtain startup script
- Go to the [CVD github](#)
- Download the *vm-config.sh* file



The screenshot shows a GitHub repository page for the file `vm-config.sh` within the `cisco-live-secure-multi-vpc-aws-BRKSEC-2144` repository. The file is 1.17 KB and contains 25 lines of shell script. The script is a startup script for a VM, performing various system setup tasks including installing packages, enabling services, and installing WordPress.

```
1 #Pre-requisite packages
2 sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
3 sudo yum -y install https://rpms.remirepo.net/enterprise/remi-release-7.rpm
4 sudo yum -y update
5 sudo yum install -y wget unzip lsof ipset httpd rsync yum-utils awk grep unzip sed dmidecode openssl curl libcurl rpm flock
6 sudo yum-config-manager --enable remi-php74
7 sudo yum -y install php php-cli php-fpm php-mysqlnd php-xml php-gd php-mcrypt php-mbstring php-curl php-xml php-pdo
8 sudo systemctl start httpd
9 sudo systemctl enable httpd
10 sudo setsebool -P httpd_can_network_connect 1
11
12 #Wordpress install
13 sudo wget https://wordpress.org/latest.tar.gz
14 tar -xzf latest.tar.gz
15 cd wordpress
16 sudo cp wp-config-sample.php wp-config.php
17
18 #replace {} with the info from the SQL instance
19 sudo sed -i -E 's/username_here/${user}/g' ./wp-config.php
20 sudo sed -i -E 's/password_here/${password}/g' ./wp-config.php
21 sudo sed -i -E 's/database_name_here/${database}/g' ./wp-config.php
22 sudo sed -i -E 's/localhost/${host_ip}/g' ./wp-config.php
23 sudo rsync -avP * /var/www/html/
24 sudo chown -R apache:apache /var/www/html/*
25 sudo systemctl restart httpd
```

# VM Deployment – Edit Config File

- Replace all `${phrase}` with the proper data

```
sudo sed -i -E 's/username_here/${user}/g' ./wp-config.php
sudo sed -i -E 's/password_here/${password}/g' ./wp-config.php
sudo sed -i -E 's/database_name_here/${database}/g' ./wp-config.php
sudo sed -i -E 's/localhost/${host_ip}/g' ./wp-config.php
```

- Should look similar to this:

```
sudo sed -i -E 's/username_here/wpuser/g' ./wp-config.php
sudo sed -i -E 's/password_here/Admin/g' ./wp-config.php
sudo sed -i -E 's/database_name_here/wordpress/g' ./wp-config.php
sudo sed -i -E 's/localhost/wordpress.cvz2hhsfre1t.ap-southeast-2.rds.amazonaws.com/g' ./wp-config.php
```

# VM Deployment – Deploy

Launch an instance | EC2 Man

ap-southeast-2.console.aws.amazon.com/ec2/v2/home?region=ap-southeast-2#LaunchInstances:

Services Search for services, features, blogs, docs, and more [Option+S]

VPC EC2 S3 IAM RDS CloudFormation

You've been opted into the new launch experience. Find out more about this experience or send us feedback. You can still return to the previous version by opting-out. Opt-out to the old experience

EC2 > Instances > Launch an instance

## Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**Name and tags**

Name  
e.g. My Web Server Add additional tags

**Application and OS Images (Amazon Machine Image)**

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Recents Quick Start

Amazon Linux Ubuntu Windows Red Hat SUSE Linux

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-0c6120461d8b3949 (64-bit (x86)) / ami-0c3a5731b62546af (64-bit (arm))  
Virtualizations: hvm Linux enabled: true Root device type: ebs

Free tier eligible

**Summary**

Number of instances Info  
1

Software image (AMI)  
Amazon Linux 2 Kernel 5.10 AMI...read more  
ami-0c6120461d8b3949

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)  
1 volume(s) - 8 GiB

Free tier in your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet

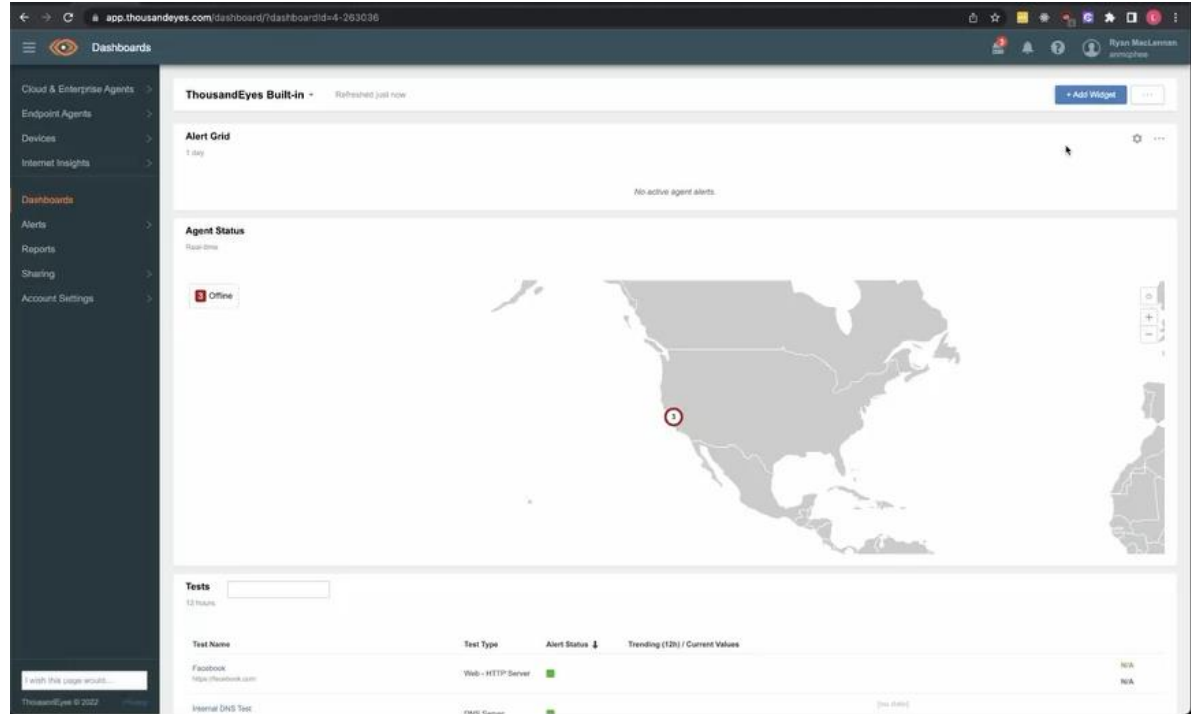
Cancel Launch instance

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

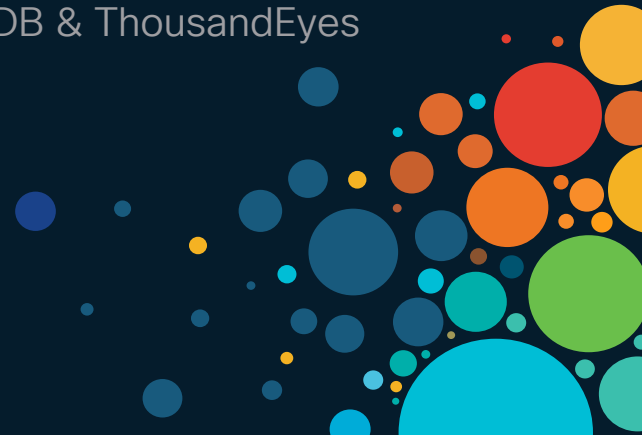
# ThousandEyes Deployment

- Two agents
  - App subnet
    - Checks Internet access
    - Checks appServer
  - Inside subnet
    - Checks Internet access
    - Checks appServer



# Policies & Controls

- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion



# FTD NAT Policy

Security Policies

→ ☐ SSL Decryption → ☐ Identity → ☐ Security Intelligence → ☒ NAT → ☒ Access Control → ☐ Intrusion

2 rules Filter +

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
Auto NAT Rules												
> #	httpPortForward	STATIC	↓ inside outside	appServerIp	ANY	HTTP	ANY	Interface	ANY	HTTP	ANY	
Manual NAT Rules (After)												
> 1	InsideOutside...	DYNAMIC	↓ inside outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	



# FTD Access List





## Security Policies

→ ☐ SSL Decryption → ☐ Identity → ☐ Security Intelligence → ☒ NAT → ☒ Access Control → ☐ Intrusion

2 rules

Filter



#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS		ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS					
> 1	allowAppHttp	 Allow	outside_zone	ANY	ANY	inside_zone	ANY	HTTP	ANY	ANY	ANY		
> 2	Inside_Outside...	 Allow	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY		

Default Action

Access Control

 Block



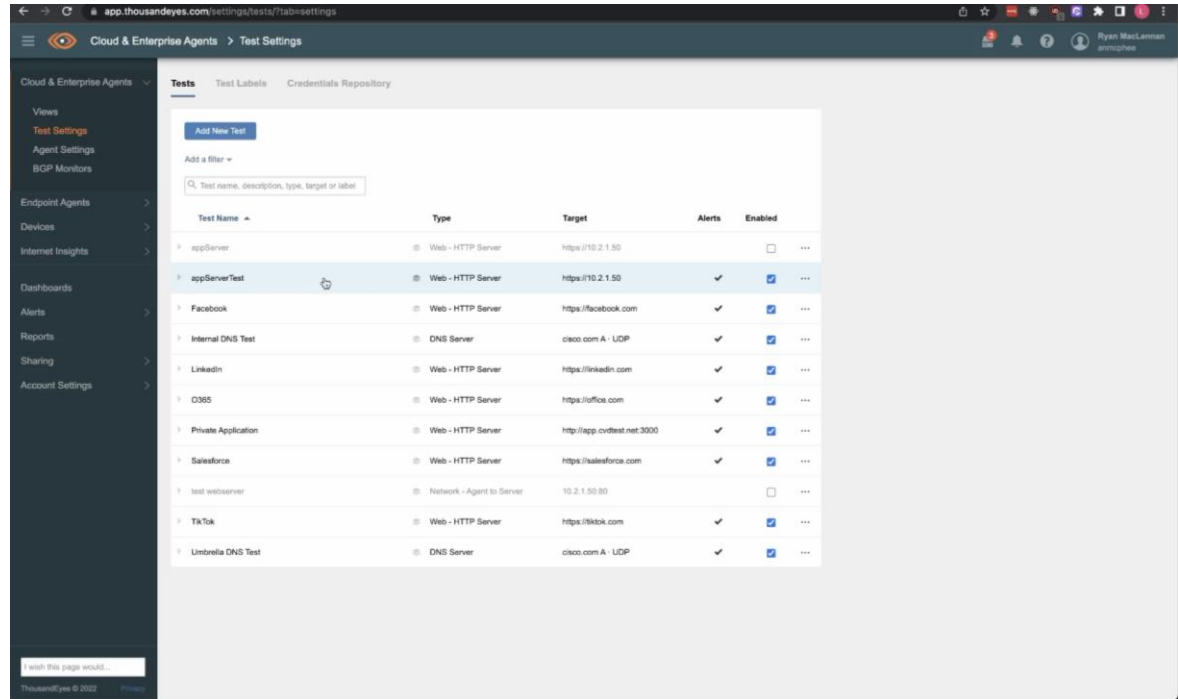
# Route Table Update

Change inside route table

- Change route for 0.0.0.0/0
  - Go to FTD inside interface

# ThousandEyes – Test

- Network test
  - Agent to server test
  - TCP port 80
  - appServer IP



# ThousandEyes – Data

- Checks
  - Jitter
  - Latency
  - Loss

Cloud & Enterprise Agents > Agent Settings

Enterprise Agents Cloud Agents Agent Labels Proxy Settings

Agents Notifications Kerberos Settings

Assigned to Account Group **anncphee** X Add a filter

Search... 5 Enterprise Agents Add New Enterprise Agent

<input type="checkbox"/> Agent Name	Hostname	Utilization	Status/Last Contact
<input type="checkbox"/> inside-te	inside-te	General 5%	3 minutes ago
<input type="checkbox"/> cisco-live-thousandeyes	thousandeyes-application	General 2%	1 minute ago
<input type="checkbox"/> thousandeyes-va-335286	thousandeyes-va	N/A	Sep 22, 2021
<input type="checkbox"/> te-sasebranch-isr4461-1	te	N/A	Dec 22, 2021
<input type="checkbox"/> te-sasebranch-isr4461-2	te	N/A	Dec 22, 2021

# Secure Cloud Analytics – Flow onboarding

- Integrations -> AWS -> VPC Flow Logs
  - Add VPC Flow Log
  - Paste URL from AWS Bucket

The screenshot displays the Cisco Secure Cloud Analytics web interface. On the left is a dark sidebar with navigation links: Settings, Alerts/Watchlists, Integrations, Entity Groups, Account Management, Subnets, Webhooks/Services, and Sensors. The main content area is titled 'Secure Cloud Analytics' and includes tabs for 'Monitor' and 'Investigate'. A modal dialog box titled 'Create VPC Flow Log' is open in the center. It contains three input fields: 'S3 Path\*' with the value '/myfolder/path', 'Credentials\*' with a dropdown arrow, and a 'Policy document' section with a right-pointing arrow. At the bottom of the dialog are 'Cancel' and 'Create' buttons. In the background, the 'VPC Flow Logs' section is visible, showing a table with columns for 'S3 Path', 'Credentials', and 'Policy document'. A table entry is partially visible with the S3 Path 'cisco-live-iaas-stealthwatch'. A '+ Add VPC Flow Log' button is located in the top right of the background interface. Below the table, there is a 'Monitor status' section with explanatory text.

Secure Cloud Analytics Monitor Investigate

Settings Alerts/Watchlists Integrations Entity Groups Account Management Subnets Webhooks/Services Sensors

aws VPC Flow Logs AWS

S3 Path

cisco-live-iaas-stealthwatch

20 Per Page

Monitor status

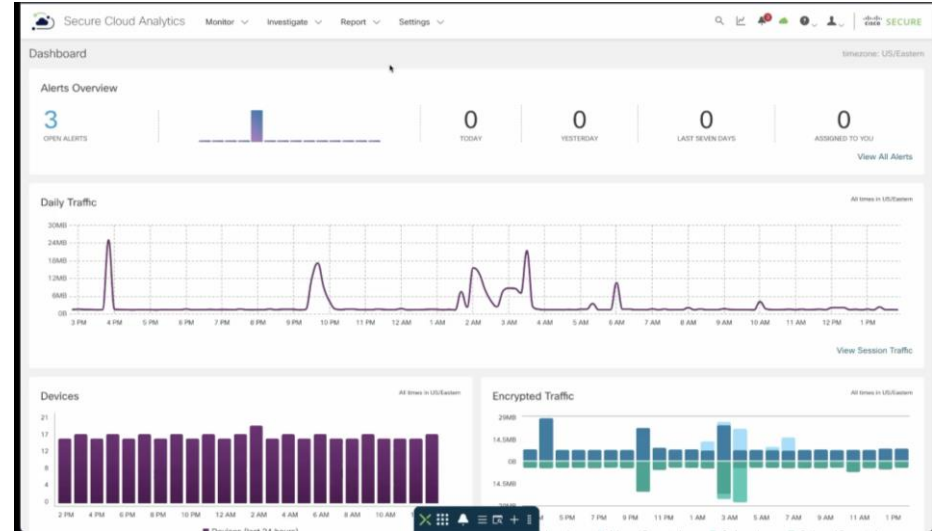
Below is a list of resources retrieved from AWS. The ones that have VPC Flow Log configurations suitable for monitoring can be added on this page. To monitor others, you'll need to set them up for VPC Flow Logging. This list updates every hour.

1-1 of 1 results |< < 1 / 1 > >|

1-1 of 1 results |< < 1 / 1 > >|

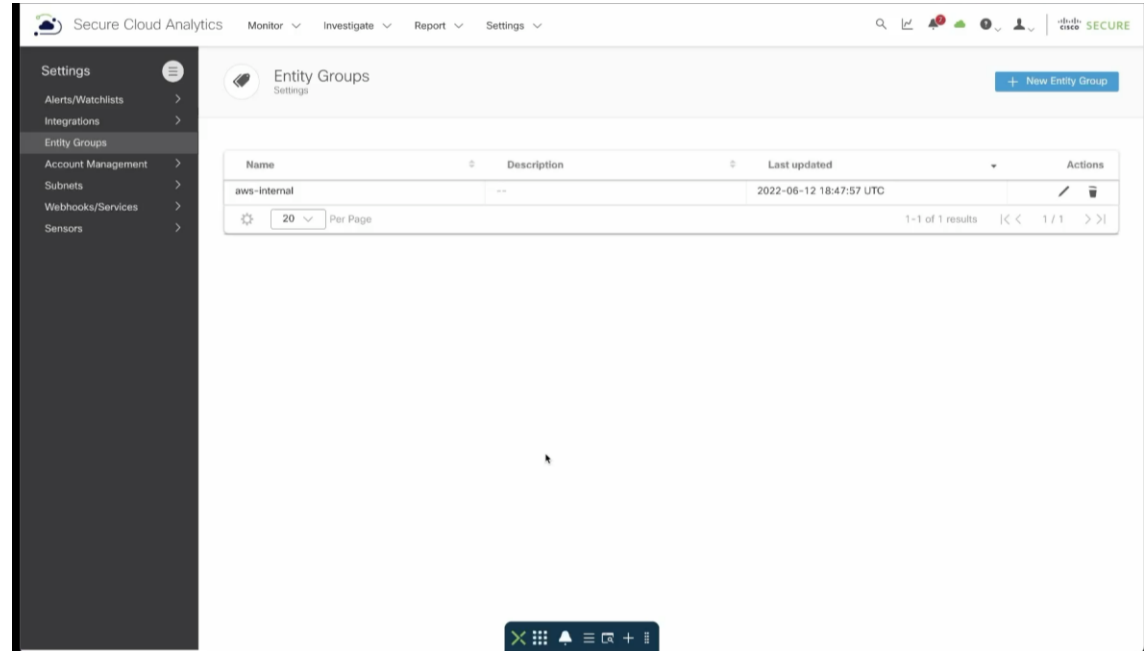
# Secure Cloud Analytics – Controls

- Add a third party watch list
  - Snort.org ->Downloads ->IP Block List
- Create Entity Groups
  - Better analysis, alerting, and control for specific subnets



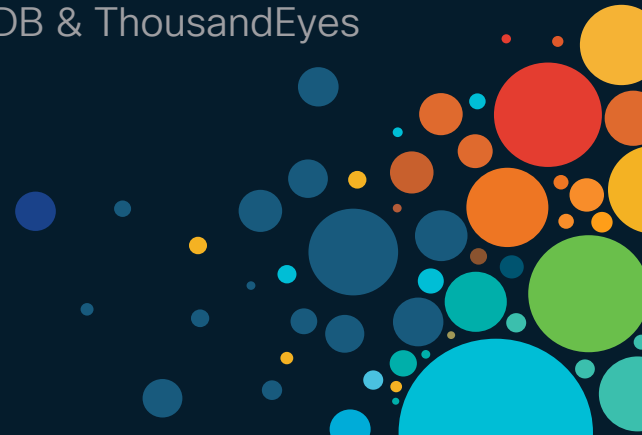
# Secure Cloud Analytics – Alerts

- Alert Settings
  - Minimum Time to alert
  - Enable/Disable alerts
- Monitoring



# Conclusion

- Introduction
- Overall Design
- VPC & Subnet Creation
- Secure Cloud Analytics
- Gateways & Routing
- Create Security Groups
- Deploy FTD, VMs, DB & ThousandEyes
- Policies & Controls
- Conclusion





# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



**Security Operations**

**SECURE X (XDR)**

**Managed Detection and Response Services**

**Security, Orchestration, Automation and Response**

**Incident Response and Remediation Services**

**Threat Visibility & Hunting**

**Device Insights**

**Kenna Vuln Mgmt**

**Secure Cloud Insights**

**3rd Party Integrations**

**User/Device Security**

**ZERO TRUST**

Adaptive MFA | Passwordless | Trust

Duo Secure Access Secure E-mail

**SASE/REMOTE WORKER**

Unified Client | EDR | Cloud Managed



**Cisco Secure Client**

VPN  
Posture  
Telemetry  
Threat  
Query

**ThousandEyes (Visibility)**

**Meraki SM OS, App Control**

**Network Security**

**Cloud Edge**

**SECURE ACCESS SERVICE EDGE (SASE)**

**ZERO TRUST**

**PRIVATE CLOUD EDGE (MSP or CUSTOMER)**

Threat Protection | Secure Access Control | Managed Remote Access

Reliable | Scalable | Flexible

**Umbrella/Duo**

ZTNA DNS-layer security Secure web gateway L7 firewall + IPS Cloud access security broker/shadow IT  
 RAaaS SSL decryption Remote browser isolation Data loss prevention Cloud malware detection

**SDWAN**

Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes Cloud DDoS, WAF

**On-Premises**

**SASE/SDWAN**

**ZERO TRUST**

Scalable | Flexible | Visibility | Comprehensive Security

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

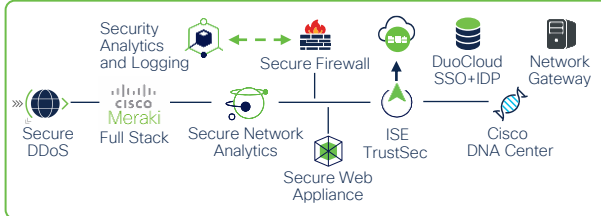
**Network Edge**

Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes

**IoT/OT SECURITY**

Secure Critical Infrastructure | Unified IT and OT

Industrial Router Industrial Firewall Industrial Switch/AP Cyber Vision ISE TrustSec



**Application Security**

**ZERO TRUST**

Policy | API Security  
Application Segmentation  
Run-time Application Security

**Application Security Stack**

Cloud Native Security APIC  
 Secure Workload Secure Application by AppDynamics

App Observability | Detection | Response

Hybrid Private Public Cloud  
 Secure Cloud Analytics Secure Firewall  
 ThousandEyes Secure DDoS, WAF/Bot

# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](https://www.cisco.com/go/certs)

Pay for Learning with  
Cisco Learning Credits

(CLCs) are prepaid training  
vouchers redeemed directly  
with Cisco.



## Learn

### Cisco U.

IT learning hub that guides teams  
and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology,  
and certification training

### Cisco Modeling Labs

Network simulation platform for design,  
testing, and troubleshooting

### Cisco Learning Network

Resource community portal for  
certifications and learning



## Train

### Cisco Training Bootcamps

Intensive team & individual automation  
and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting  
Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product,  
technology, and certification courses



## Certify

### Cisco Certifications and Specialist Certifications

Award-winning certification  
program empowers students  
and IT Professionals to advance  
their technical careers

### Cisco Guided Study Groups

180-day certification prep program  
with learning and support

### Cisco Continuing Education Program

Recertification training options  
for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*



#CiscoLive