

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Managing Automation Workloads on Public Clouds Complying with Cloud Security Best Practices

Weigang Huang, Senior Software Architect
Sanka Chen, Technical Leader
DEVNET-1063

CISCO *Live!*

#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 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-1063>

Agenda

- Cloud Security Compliance Overview
 - Cloud Security Alliance (CSA) and Cloud Security Standards
 - Security Compliances with public cloud providers
- Customer Delivery Use Cases
 - Security requirements and challenges
- Two Practical Examples
 - Manage work loads on AWS
 - Securely share customized AMLs
- Conclusion

Cloud Security Compliance Overview



The Changes: Cloud vs On-Prem

- Insecure access points
- Changes to Identity and Access Management (IAM)
- Trust the provider?
- Requires a proactive and strategic approach
- Best practices
 - Conducting risk assessments
 - Implementing strong security controls
 - Training on security awareness
 - Monitoring/auditing security controls
- Cloud Security Compliance

Cloud Security Compliance

- Ensuring cloud services meet the security and compliance requirements
- Adopting a security strategy that covers all aspects of cloud computing
 - IAM
 - Network security
 - Data protection
 - Compliance monitoring and reporting.

Cloud Security Standards and Frameworks

- Cloud Security Alliance (CSA)
 - [Cloud Security Alliance Controls Matrix](https://hyperproof.io/resource/cloud-compliance-frameworks/#:~:text=Cloud%20Security%20Alliance%20Controls%20Matrix) (https://hyperproof.io/resource/cloud-compliance-frameworks/#:~:text=Cloud%20Security%20Alliance%20Controls%20Matrix)
- Center of Internet Security (CIS) Controls,
- NIST cyber security framework, ISO (27001), FISMA,
- Cloud Well Architecture Framework
 - AWS Well-Architecture
 - Azure Architecture
 - Google Cloud-Architecture

Shared Responsibility

- Cloud security requires the collaboration of service providers , venders, and customers
 - Shared responsibility
 - Clearly defined and documented
- Examples: AWS Shared Responsibility Model
 - AWS: Security *of* the Cloud
 - Customer: Security *in* the Cloud

Focus of the Session

- This session is not to cover details of cloud security compliance
- This session is to share
 - Manage workloads on AWS VPC when strict security is enforced to comply “security *in* the cloud”
 - Access workloads when public access is disallowed
 - Enhance/update/patch workloads
- Use case driven
 - Cisco Crosswork Network Controller as target application on AWS

A Delivery Use Case



A Use Case

- Automation solution: Cisco Crosswork Network Controller (CNC)
 - Provide network automation and observability
 - Deployed on the public cloud (AWS) to manage hybrid networks (on cloud and on-prem)
- Cloud provider: AWS
- To comply to “Security *in* the Cloud”
 - The solution needs to be deployed on VPC with limited access
 - Security enforcement
 - Network, security group, IAM roles, SCP.....

Two Practical Examples

- Example 1
 - AWS System Session Manager (SSM) to access application workloads deployed at an isolated VPC
 - Application (Crosswork)
- Example 2
 - Update workloads when public access is restricted

Practical Example 1



Manage Workloads

- Manage workloads without public access
 - Workload VMs does not allow to be accessed via public IP
 - VPC is restricted with no internet gateway
- Recall: common ways to access workloads of VPC
 - Access through EC2 instance with public IP and IGW (Internet Gateway)
 - VPN connections
 - VPW/CGW + tunnels
 - AWS direct connect
 -
 - AWS System Session Manager(SSM) to access isolated VPC

IGW + Public IP

VPC with Internet Gateway (IGW)

- A public subnet in VPC is required
- Access your instances from the EC2 with public IP

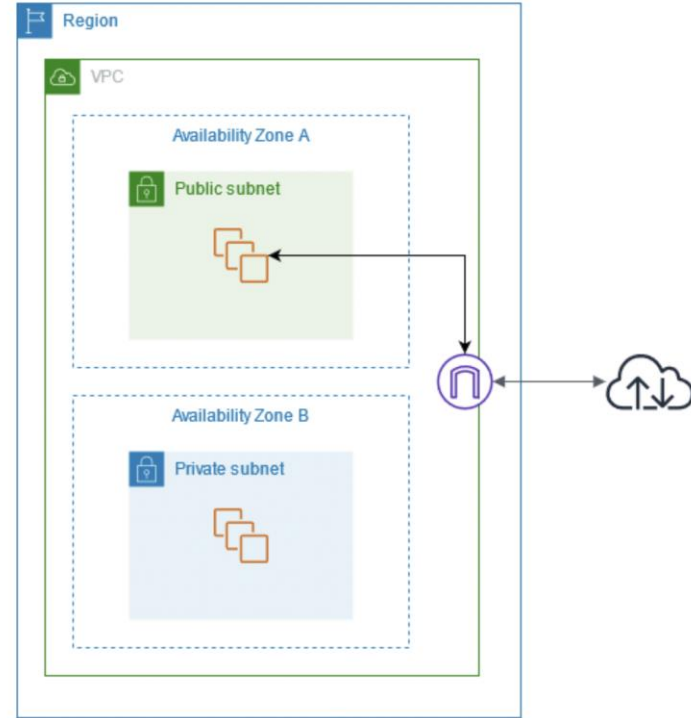


Diagram: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

~~IGW + Public IP~~

~~VPC with Internet Gateway (IGW)~~

- ~~• A public subnet in VPC is required~~
- Access your instances from the EC2 with public IP

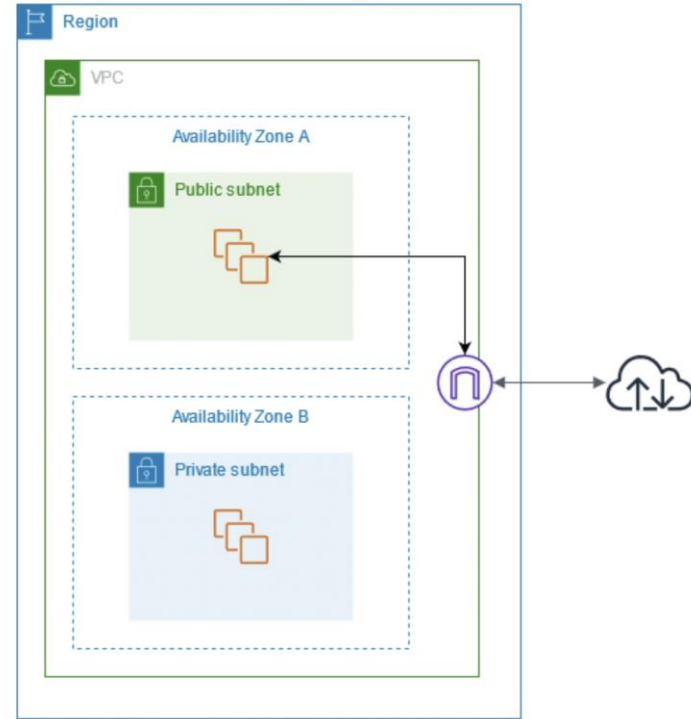


Diagram: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Site-to-site VPN

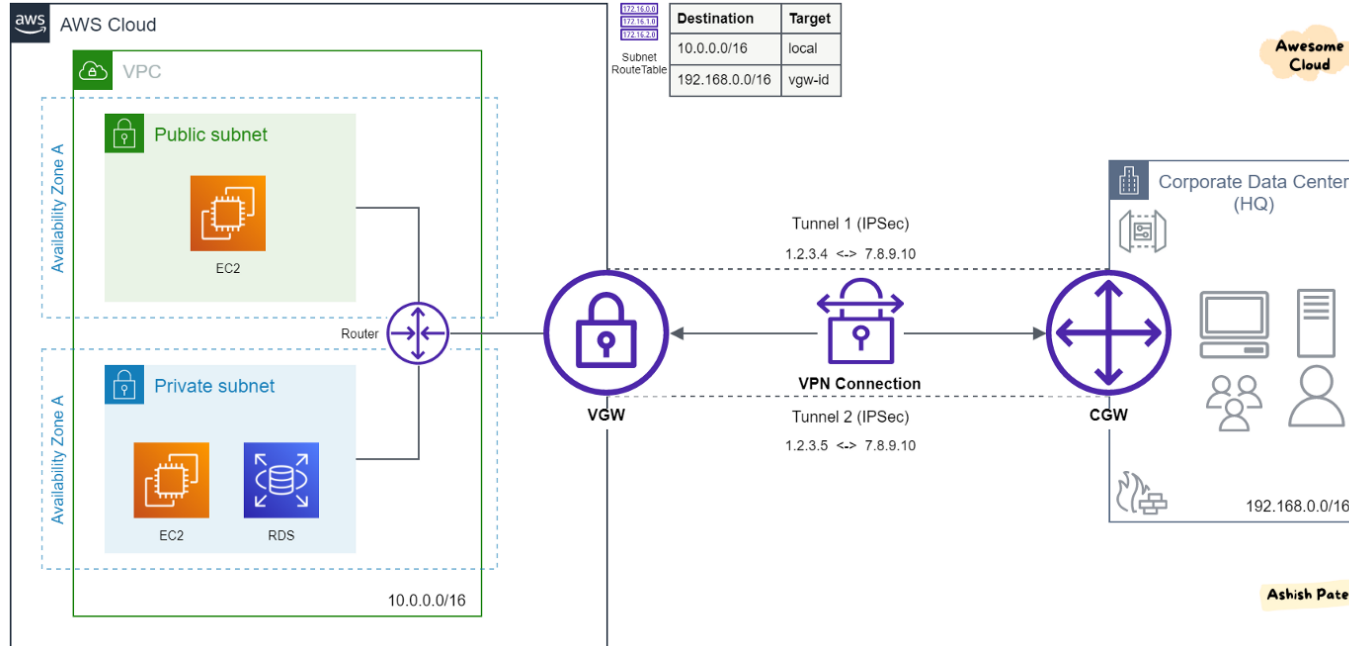


Diagram from: <https://medium.com/awesome-cloud/aws-site-to-site-vpn-connections-overview-introduction-to-aws-vpn-getting-started-ba889c2f1849>

Site-to-site VPN

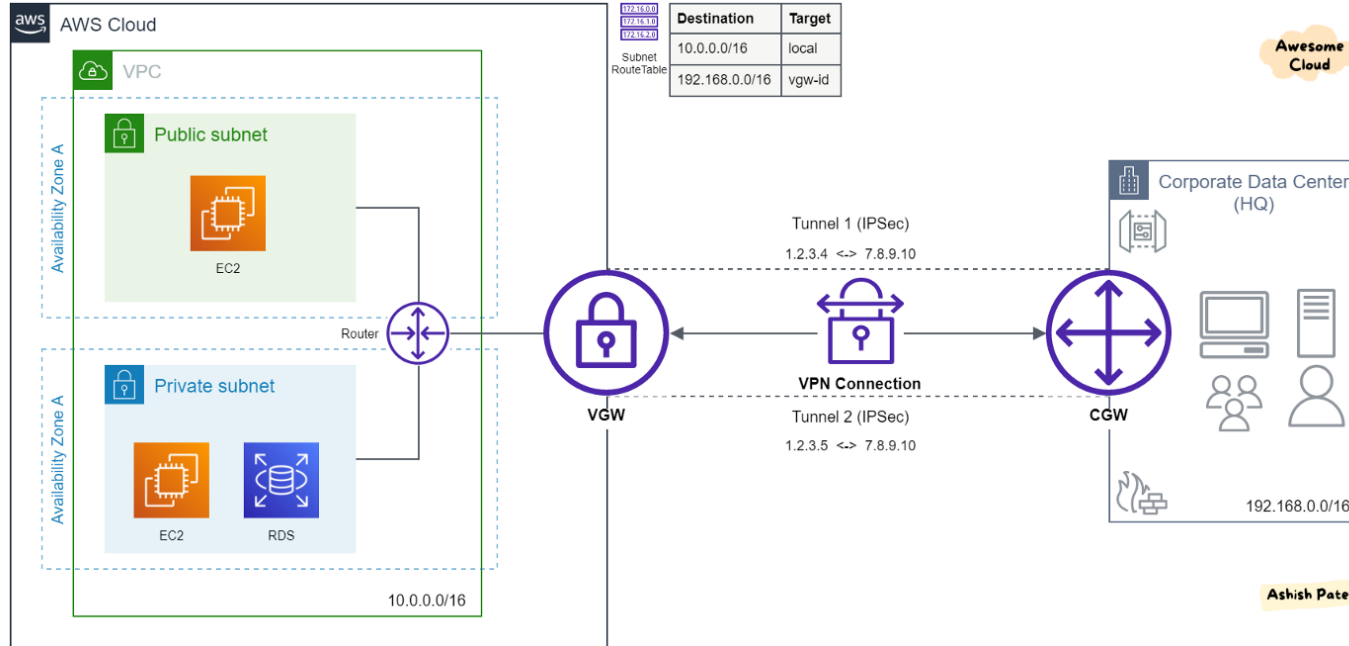


Diagram from: <https://medium.com/awesome-cloud/aws-site-to-site-vpn-connections-overview-introduction-to-aws-vpn-getting-started-ba889c2f1849>

Direct Connect

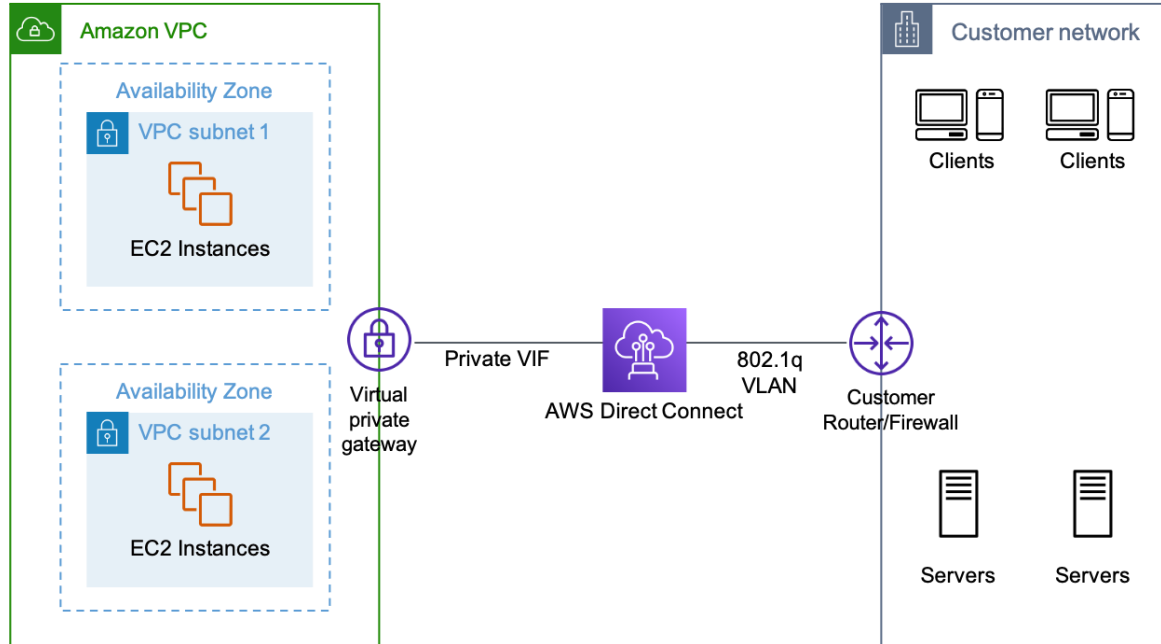


Diagram: <https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect.html>

Direct Connect

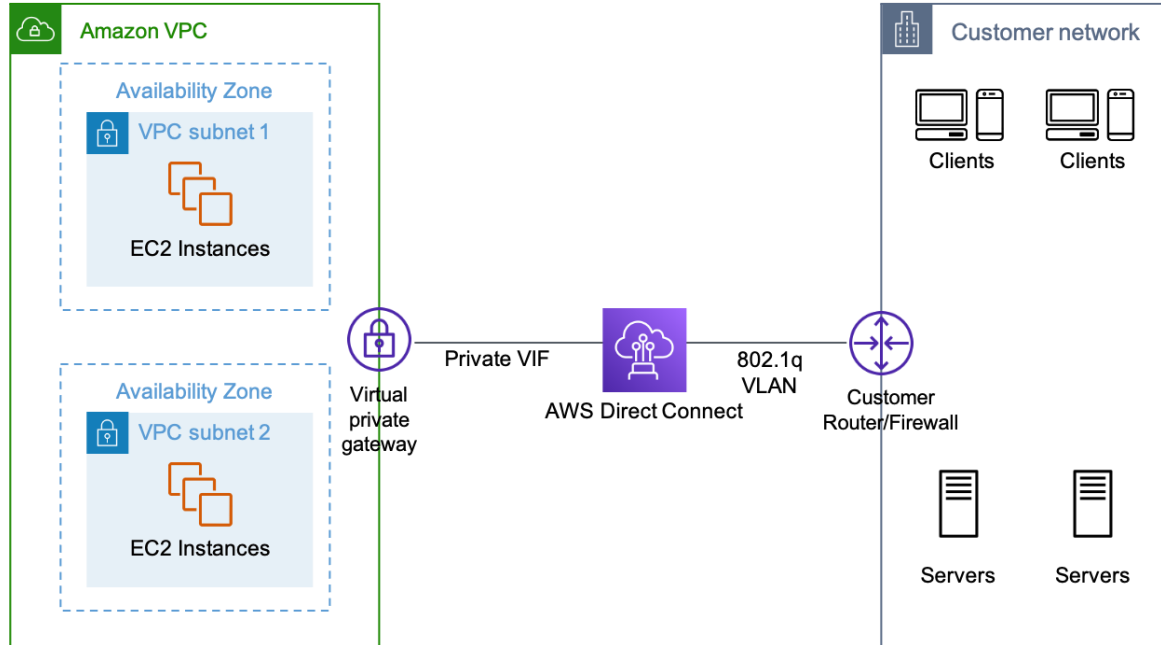
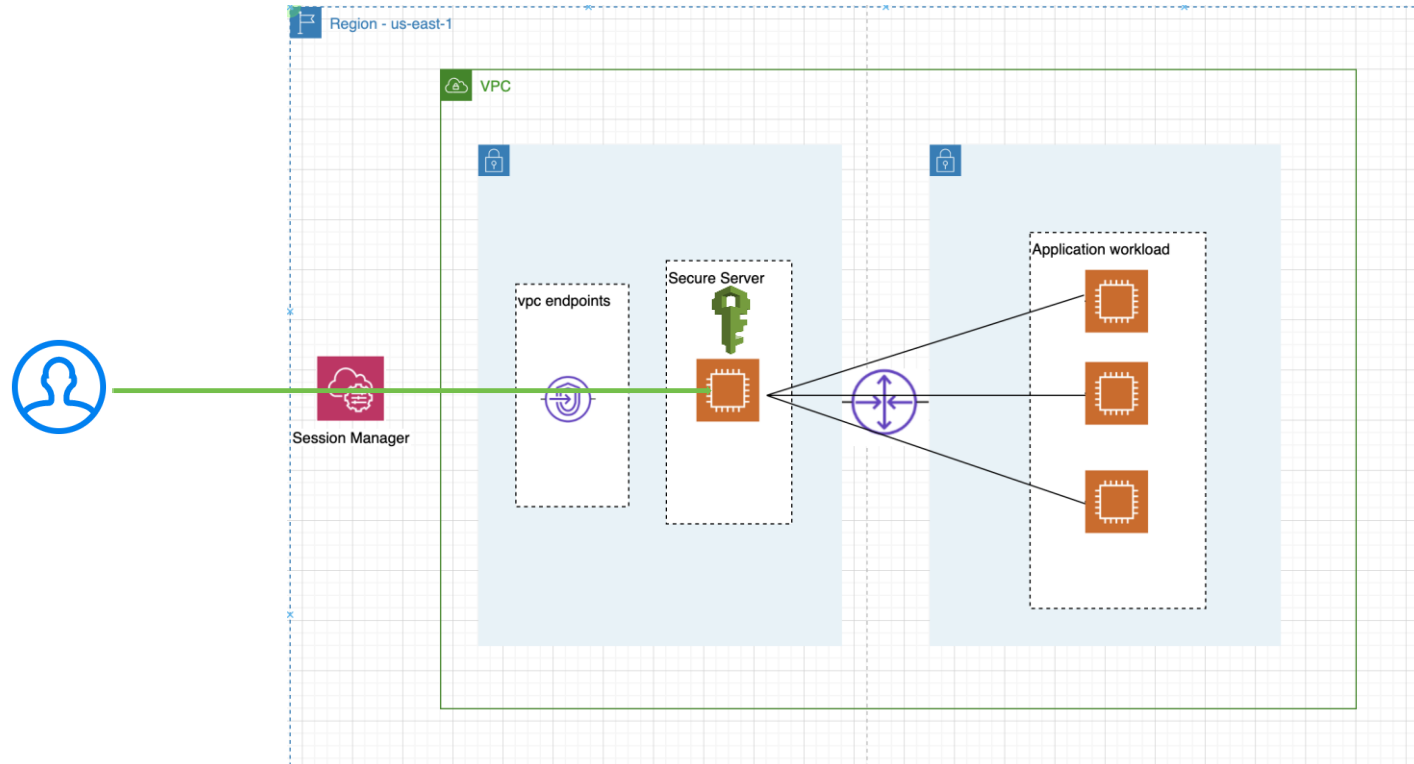


Diagram: <https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect.html>

Using AWS System Session Manager (SSM)



Manage Workloads

- Manage workloads without public access
 - Workload VMs does not allow to be accessed via public IP
 - VPC is isolated, with no internet gateway
- Recall: common ways to access workloads of VPC
 - Access through EC2 instance with public IP and IGW (Internet Gateway)
 - VPN connections
 - VPW/CGW + tunnels
 - AWS direct connect
 - AWS System Session Manager(SSM) to access isolated VPC

Manage Workloads

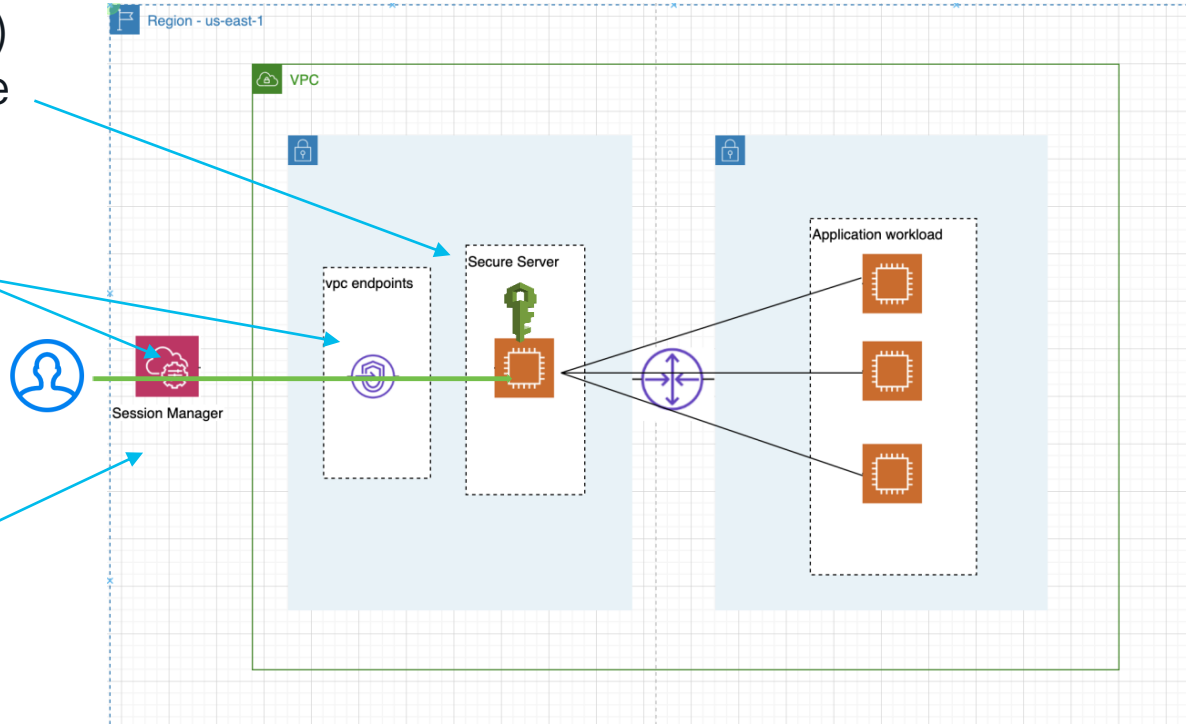
- Manage workloads without public access
 - Workload VMs does not allow to be accessed via public IP
 - VPC is isolated, with no internet gateway
- Recall: common ways to access workloads of VPC
 - ~~Use EC2 instance with public IP and IGW (Internet Gateway)~~
 - ~~VPN connections~~
 - ~~VPW/CGW + tunnels~~
 - ~~AWS direct connect~~
 - **AWS System Session Manager (SSM) to access isolated VPC**

AWS Systems Manager Session Manager (SSM)

- Session
 - Secure channel between an end user and work nodes in AWS
- Provides secure management without the need of opening inbound ports
- Comply with strict security practices.
- Fully auditable logs with node access details
- AWS managed service

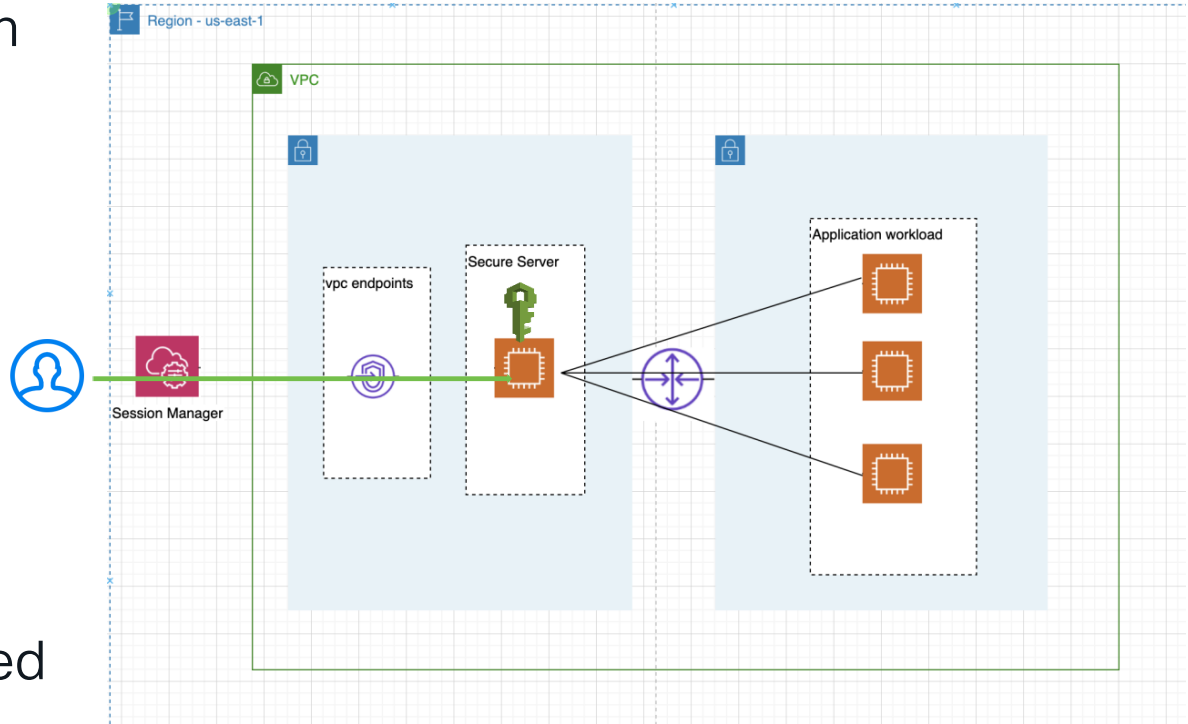
Establish SSM Sessions to Access Workloads

1. Secure server (EC2) with proper IAM role
2. SSM
3. VPC endpoints
4. User request to access secure Server via SSM
5. SSM checks permission
6. Session established



Establish SSM Sessions to Access Workloads

1. Secure server with proper IAM role
2. SSM
3. VPC endpoints
4. User request to access via SSM
5. SSM checks permission
6. Session established



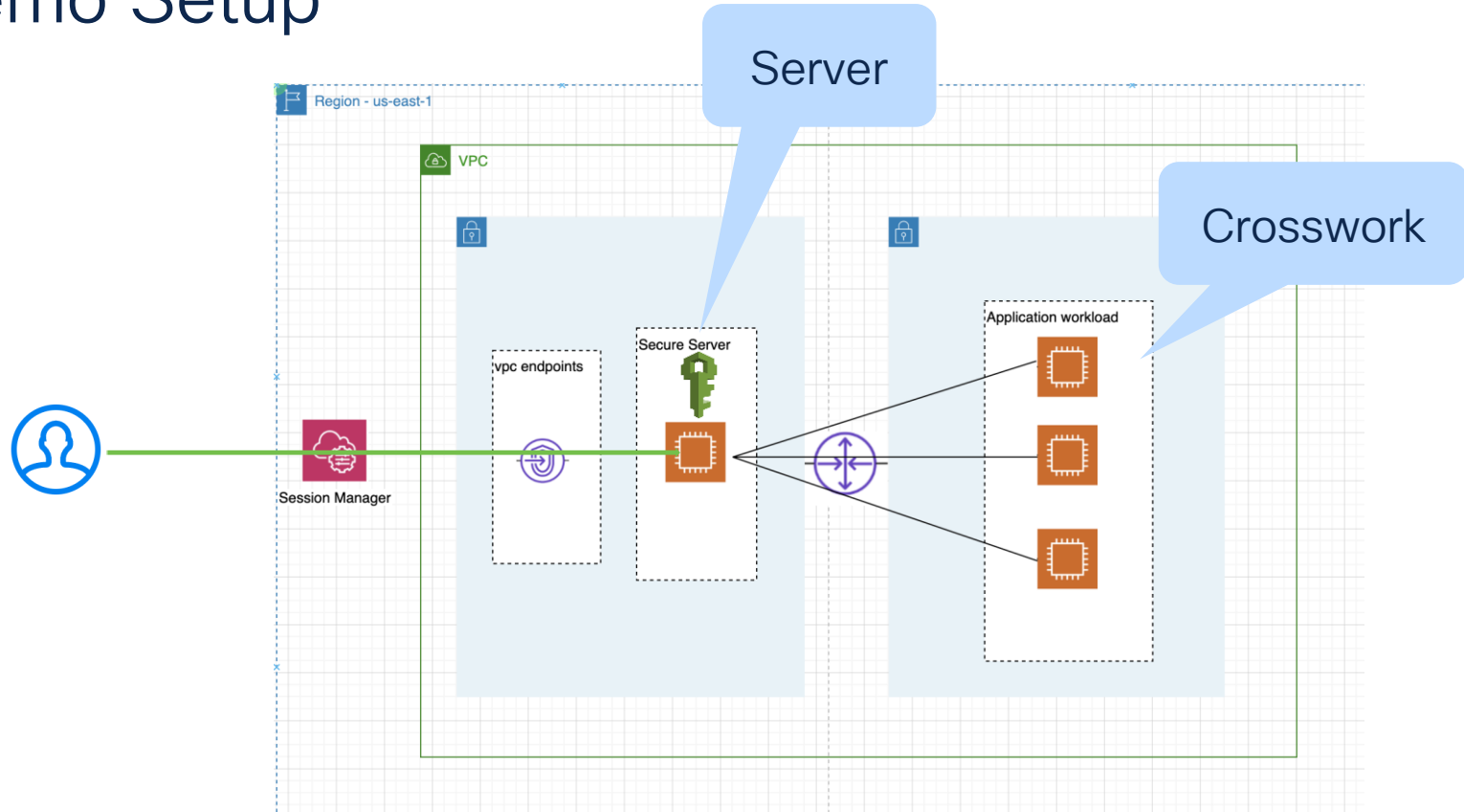
Set Up SSM

- SSM agent installed on the secure server
 - EC2 instances with AMI (AMI linux 2023, Amazon Linux 2 with .NET 6, PowerShell, Mono, and MATE Desktop Environment)
- Proper IAM role associated with the secure server
 - Permission policy to allow accessing SSM VPC services
- Managed work nodes to allow https outbound traffic for the VPC endpoints
 - `ec2messages.region.amazonaws.com`
 - `ssm.region.amazonaws.com`
 - `ssmmessages.region.amazonaws.com`

Demo



Demo Setup



Demo

- Access CNC portal from ssm host
 - curl -k <https://eks-cw-mgmt-vip.cwcisco.com:30603>
 - Browser: <https://eks-cw-mgmt-vip.cwcisco.com:30603>
- Access CNC CLI
 - ssh [cw-admin@eks-cw-mgmt-vip.cwcisco.com](https://eks-cw-mgmt-vip.cwcisco.com)
 - "kubectl get pods" as root

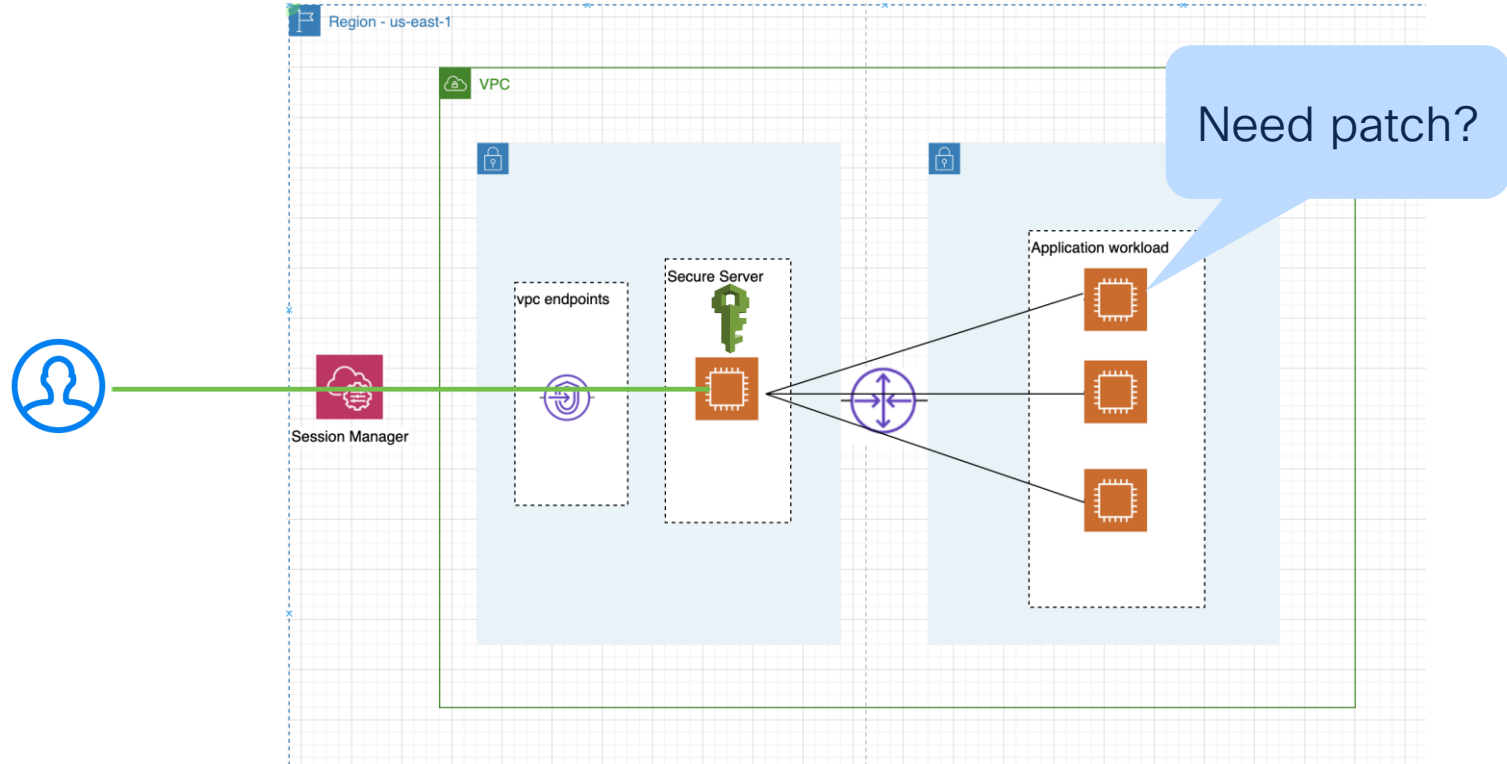
Quick Recap



Practical Example 2



Practical Example 2



AWS AMI's

- AMI's are built from EC2 instances
- EBS backed AMIs
 - root device for an instance launched from the AMI is an Amazon EBS (Elastic Block Storage) volume created from an Amazon EBS snapshot.
- Instance store backed AMIs
 - root device for an instance launched from the AMI is an instance store volume created from a template stored in Amazon S3
- This presentation is for sharing EBS backed AMIs

AWS AMI's

- AMI's are built from EC2 instances
- EBS backed AMIs
 - root device for an instance launched from the AMI is an **Amazon EBS (Elastic Block Storage) volume** created from an Amazon EBS snapshot.
- Instance store backed AMIs
 - root device for an instance launched from the AMI is an instance store volume created from **a template stored in Amazon S3**
- This presentation is for sharing EBS backed AMIs

When The Workload Needs a Patch

- Install additional packages to workload (feature enhancement)
 - It is challenging without internet access
- Alternatives
 - Transfer the packages over to the workload
 - Painful to deal with package dependencies
 - Build a customized AMI from an instance with public access (different account)
 - Share the AMI across accounts
 - To comply, the EBS backed AMI needs be encrypted

When The Workload Needs a Patch

- Install additional packages to workload (feature enhancement)
 - It is challenging without internet access
- Alternatives
 - Transfer the packages over to the workload
 - Painful to deal with package dependencies
 - Build a customized AMI from an instance with public access (different account)
 - Share the AMI across accounts
 - To comply, the EBS backed AMI needs be encrypted

Share AMI's Across Accounts

- Prerequisite to securely share AMI's across accounts
 - The AMI must be encrypted with Customer Managed Key (CMK) through AWS Key Management Service (KMS)
 - Create a CMK for the source account
 - Encrypt storage: EBS with the CMK
- Share the CMK with the target account
- Share the encrypted AMI's to the target account
- Reference: Encryption options
 - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#ebs-volume-encryption-outcomes>

Steps to Securely Share AMI's Across Accounts

1. Source account: create a customer managed key (CL-demo)
2. Encrypt the EBS of source AMI's with the customer managed key (CL-demo)
3. Share the key (CL-demo) with the target account
4. Share the AMI through Edit Permission
5. When launching instances of the shared AMI, the EBS storage is re-encrypted by the target account key
 - A CMK or a default key

AMI Creation Encryption Options

Encryption outcomes

The following table describes the encryption outcome for each possible combination of settings.

Is encryption enabled?	Is encryption by default enabled?	Source of volume	Default (no customer managed key specified)	Custom (customer managed key specified)
		that you own		Encrypted by a specified customer managed key
No	Yes	Unencrypted snapshot that is shared with you	Encrypted by default customer managed key	
No	Yes	Encrypted snapshot that is shared with you	Encrypted by default customer managed key	
Yes	Yes	New volume	Encrypted by default customer managed key	
Yes	Yes	Unencrypted snapshot that you own	Encrypted by default customer managed key	
Yes	Yes	Encrypted snapshot that you own	Encrypted by same key	
Yes	Yes	Unencrypted snapshot that is shared with you	Encrypted by default customer managed key	
Yes	Yes	Encrypted snapshot that is shared with you	Encrypted by default customer managed key	

Build Customized AMI's

EC2 > Instances > i-0a9663120c176574c > Create image

Create image [Info](#)
An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance.


Instance ID
 i-0a9663120c176574c (SSM-CL)

Image name

Maximum 127 characters. Can't be modified after creation.

Image description - optional

Maximum 255 characters

No reboot
☐ Enable

Instance volumes

Storage type	Device	Snapshot	Size	Volume type	IOPS	Throughput	Delete on termination	Encrypted
EBS ▾	/dev/... ▾	Create new snapshot fr... ▾	<input type="text" value="8"/>	EBS General Purpose S... ▾	<input type="text" value="100"/>	<input type="text"/>	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Add volume


Share AMI to Another Account



Edit AMI permission

Edit AMI permissions [Info](#)

By editing the permissions of an AMI, you can share it with the AWS accounts, organizations, or OUs that you specify.

AMI share settings

AMI ID
 `ami-0c8e358cf62c839b5`

Associated snapshot IDs
 `snap-0bad4308746b5279a`
 `snap-0d138425bb8ccaeba`

☐ Add 'Create volume' permission to associated snapshots when creating account permissions.
This setting only applies when you share an AMI with specific AWS accounts.

AMI availability

☐ Public
Share the AMI publicly with all AWS users.

☒ Private - (current setting)
Share the AMI with specific accounts, organizations, or OUs.

Shared accounts (1)

Remove selectedAdd account ID

<input type="checkbox"/>	Shared account ID
<input type="checkbox"/>	250541750349

Demo



Summary



Take Aways

- Cloud security compliance is an essential aspect of cloud computing
- To comply with cloud security shared responsibility model, customers are required to ensure Security *in* the Cloud
- Workloads in highly secured VPC's should be managed with alternatives
- Two examples of securely managing workloads of AWS
 - Setup AWS SSM to manage workloads
 - Customize AMI creation and securely sharing across accounts

Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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



The bridge to possible

Thank you

CISCO *Live!*

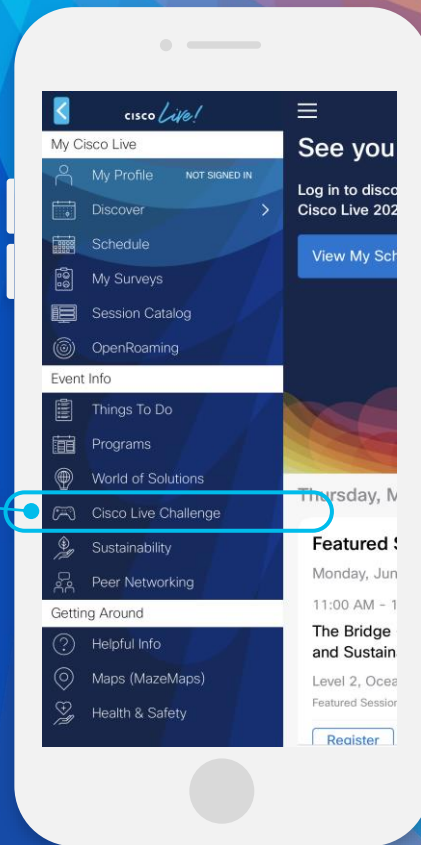
#CiscoLive

Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors: yellow, orange, red, and then various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive