Exam Questions NSE7_PBC-7.2

Fortinet NSE 7 - Public Cloud Security 7.2

https://www.2passeasy.com/dumps/NSE7_PBC-7.2/

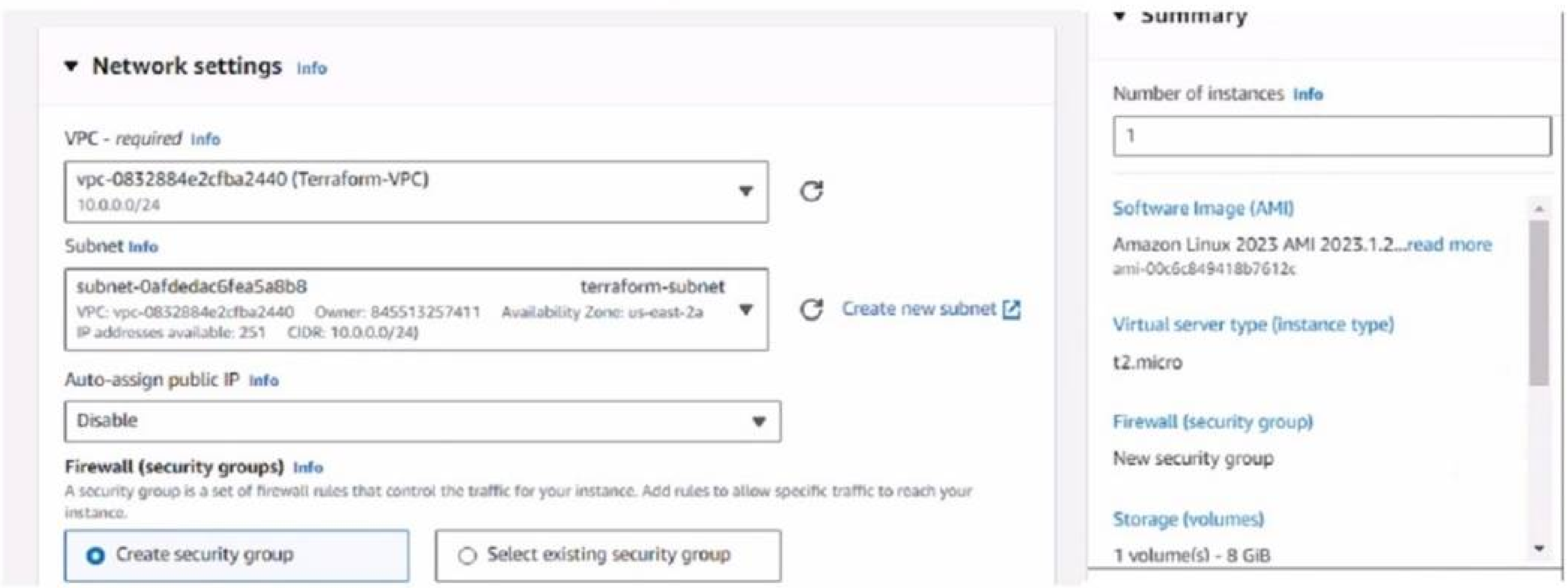
NEW QUESTION 1
Your goal is to deploy resources in multiple places and regions in the public cloud using Terraform.
What is the most efficient way to deploy resources without changing much of the Terraform code?

A. Use multiple terraform.tfvars files With a variables.tf file.
B. Use the provide
C. tf file to add all the new values
D. Install and configure two Terraform staging servers to deploy resources.
E. Use the variable, tf file and edit its values to match multiple resources

Answer: A

Explanation:
When deploying resources in multiple places and regions in the public cloud using Terraform, the most efficient way is:
A.Use multiple terraform.tfvars files with a variables.tf file.
? Terraform.tfvars File:This file is used to assign values to variables defined in your Terraform configuration. By having multiple.tfvarsfiles, you can define different sets of values for different deployments, such as for different regions or environments, without changing the main configuration.
? Variables.tf File:This file contains the definition of variables that will be used within your Terraform configuration. It works in conjunction withterraform.tfvarsfiles, allowing you to parameterize your configuration so that you can deploy the same template in multiple environments with different variables.
References:This method is outlined in Terraform's official documentation and is a best practice for reusing code for different environments in infrastructure as code (IaC) deployments.

NEW QUESTION 2
Refer to the exhibit.



▼ Network settings Info

VPC - *required* Info

vpc-0832884e2cfba2440 (Terraform-VPC)
10.0.0.0/24

Subnet Info

subnet-0afdedac6fea5a8b8 terraform-subnet
VPC: vpc-0832884e2cfba2440 Owner: 845513257411 Availability Zone: us-east-2a
IP addresses available: 251 CIDR: 10.0.0.0/24)

Create new subnet

Auto-assign public IP Info

Disable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

▼ Summary

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.1.2...read more
ami-00c6c849418b7612c

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

You have deployed a Linux EC2 instance in Amazon Web Services (AWS) with the settings shown on the exhibit
What next step must the administrator take to access this instance from the internet?

A. Configure the user name and password.
B. Enable source and destination checks on the instance
C. Enable SSH and allocate it to the device
D. Allocate an Elastic IP address and assign it to the instance

Answer: D

Explanation:
The next step the administrator must take to access the Linux EC2 instance from the internet is:
D.Allocate an Elastic IP address and assign it to the instance.
? Elastic IP (EIP) Requirement:By default, when an EC2 instance is launched in AWS, it receives a public IP address from Amazon's pool, which is not static. This IP address can change, for example, if the instance is stopped and started again. To have a static IP address, you need to allocate an Elastic IP (EIP), which is a persistent public IP address, and then associate it with the instance.
? Public Accessibility:Without an Elastic IP, the instance may not be accessible over the internet after a reboot or stop/start sequence. Assigning an Elastic IP ensures the instance can be accessed consistently using the same IP address.
References:The AWS documentation on EC2 instances details the process and need for Elastic IPs to ensure consistent internet access to instances.

NEW QUESTION 3
How does Terraform keep track of provisioned resources?

A. It uses the terrafor
B. tf state file
C. Terraform does not keep the state of resources created
D. It uses the terrafor
E. tfvars file.
F. It uses the databas
G. tf file.

Answer: A

Explanation:
Terraform manages and tracks the state of infrastructure resources through a file known as terraform.tfstate. This file is automatically created by Terraform and is updated after the application of a Terraform plan to capture the current state of the resources.
? State File Purpose:Theterraform.tfstatefile contains a JSON object that records the
IDs and properties of resources Terraform manages, so that it can map real-world resources to your configuration, keep track of metadata, and improve performance for large infrastructures.
? State File Management:This file is crucial for Terraform to perform resource
updates, deletions, and for creating dependencies. It's essentially the 'source of truth' for Terraform about your managed infrastructure and services.
References:This behavior is documented in Terraform's official documentation, which explains how theterraform.tfstatefile is used to keep track of the infrastructure Terraform is managing.

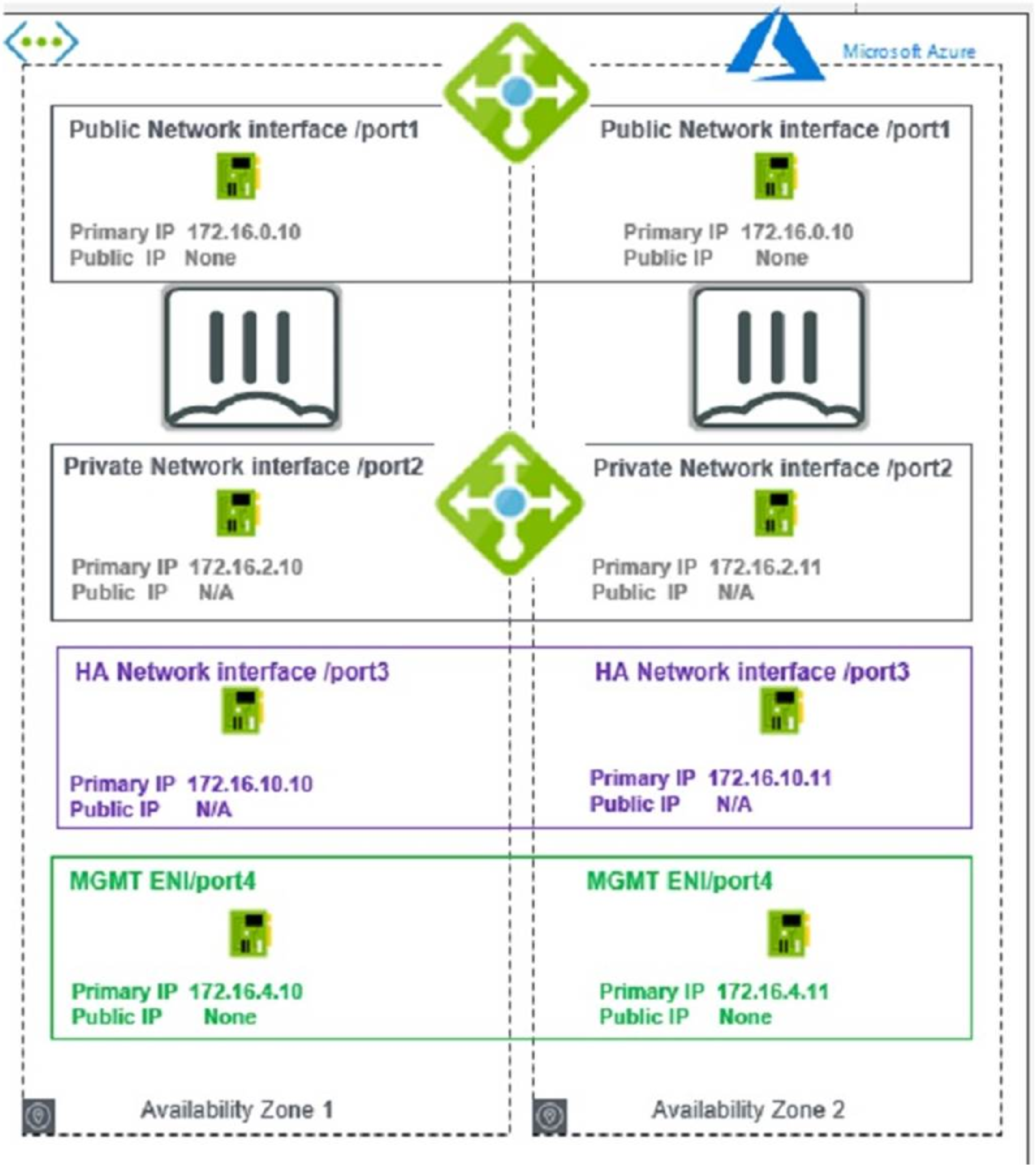
NEW QUESTION 4
What kind of underlying mechanism does Transit Gateway Connect use to send traffic from the virtual private cloud (VPC) to the transit gateway?

A. A BGP attachment
B. A GRE attachment
C. A transport attachment
D. Transit Gateway Connect attachment

Answer: D

Explanation:
? Transit Gateway Connect Specificity: AWS Transit Gateway Connect is a specific feature designed to streamline the integration of SD-WAN appliances and third-party virtual appliances into your Transit Gateway.expand_more It utilizes a specialized attachment type.exclamation
? BGP's Role: While Transit Gateway Connect attachments leverage BGP for dynamic routing, BGP itself is a routing protocol and not the core connectivity mechanism in this context.
? GRE Tunneling: GRE is a tunneling protocol commonly used with Transit Gateway Connect attachments to encapsulate traffic.

NEW QUESTION 5
Refer to the exhibit



You are deploying two FortiGate VMS in HA active-passive mode with load balancers in Microsoft Azure
Which two statements are true in this load balancing scenario? (Choose two.)

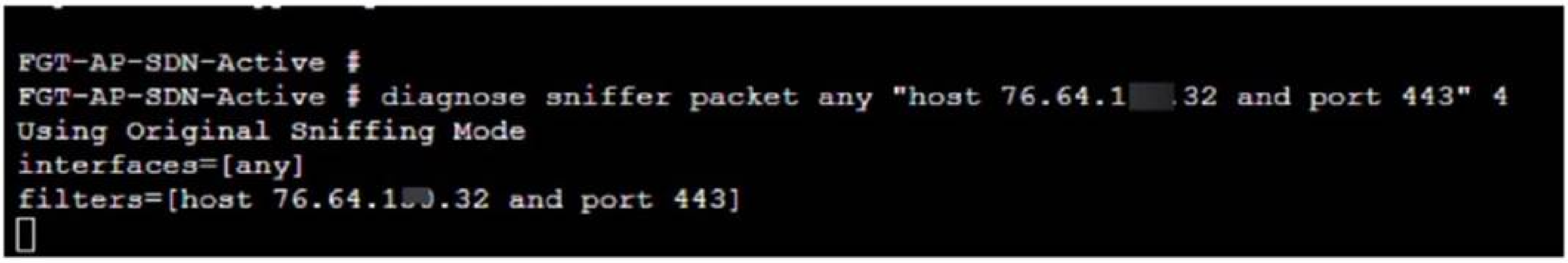
A. The FortiGate public IP is the next-hop for all the traffic.
B. An internal load balancer listener is the next-hop for outgoing traffic.
C. You must add a route to the Microsoft VIP used for the health check.
D. A dedicated management interface can be used for load balancing.

Answer: BD

Explanation:
? A is incorrect because the FortiGate public IP is not the next-hop for all the traffic.
The FortiGate public IP is only used for incoming traffic from the internet. The Azure load balancer distributes the incoming traffic to the active FortiGate VM based on a health probe123. The FortiGate public IP is not used for outgoing traffic or internal traffic.
? B is correct because an internal load balancer listener is the next-hop for outgoing traffic. The internal load balancer listener is configured with a floating IP address that is assigned to the active FortiGate VM. The internal load balancer listener also has a health probe to monitor the status of the FortiGate VMs123. The internal load balancer listener forwards the outgoing traffic to the internet through the public load balancer.
? C is incorrect because you do not need to add a route to the Microsoft VIP used for the health check. The Microsoft VIP is an internal IP address that is used by the Azure load balancer to send health probes to the FortiGate VMs123. The Microsoft VIP is not reachable from outside the Azure network and does not require

any routing configuration on the FortiGate VMs.
? D is correct because a dedicated management interface can be used for load balancing. In this deployment, port4 is used as a dedicated management interface that connects to the management network3. The dedicated management interface can be used to access the FortiGate VMs for configuration and monitoring purposes. The dedicated management interface can also be used to synchronize the configuration and session information between the primary and secondary devices in an HA cluster2.

NEW QUESTION 6
Refer to the exhibit.



```
FGT-AP-SDN-Active #
FGT-AP-SDN-Active # diagnose sniffer packet any "host 76.64.1[redacted].32 and port 443" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 76.64.1[redacted].32 and port 443]
```

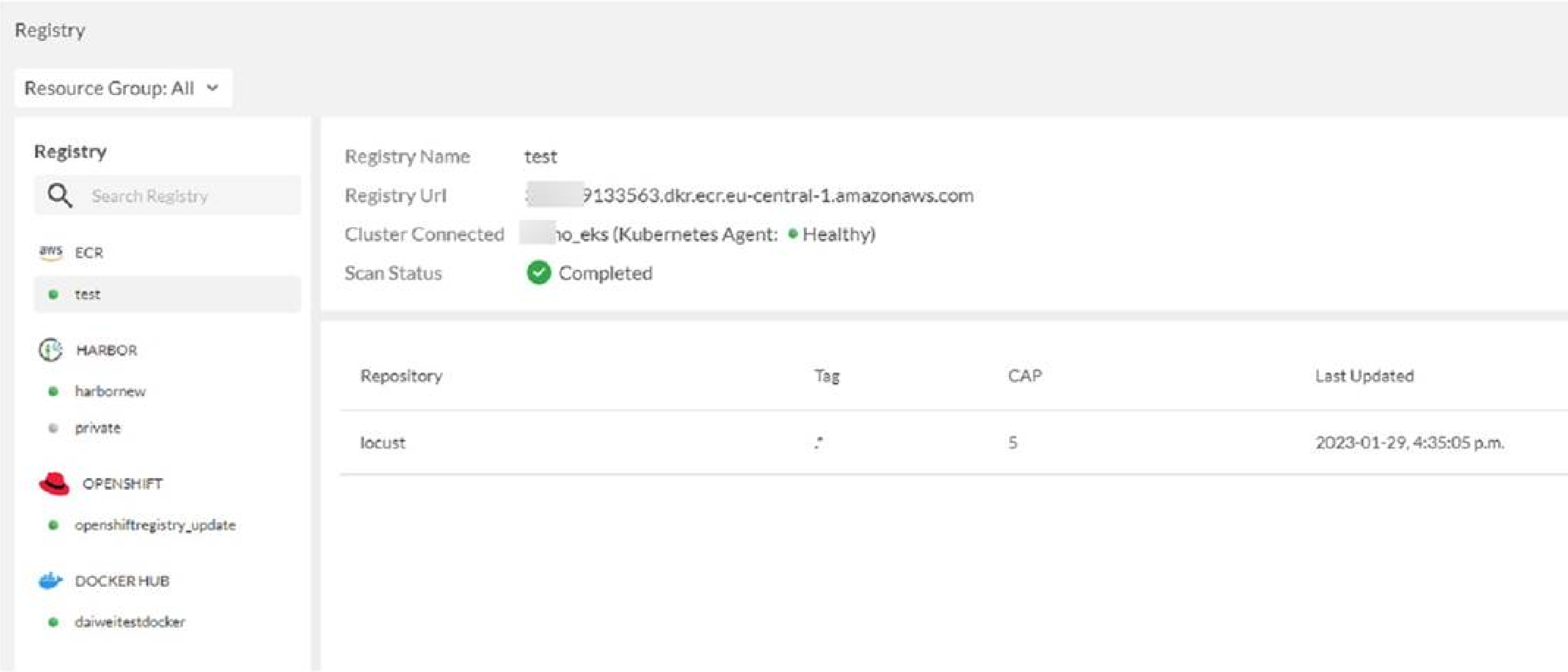
An administrator has deployed a FortiGate VM in Amazon Web Services (AWS) and is trying to access it using its public IP address from their local computer However, the connection is not successful and at the same time FortiGate is not receiving any HTTPS or SSH traffic to its external interface
What should the administrator check for possible issue?

A. Run a debug flow to check any network ACLs
B. Check the FortiGate firewall policies
C. Check the FortiGate instance ID
D. Check the inbound network security group rules

Answer: D

Explanation:
Considering the situation where the administrator is unable to access the FortiGate VM using its public IP address and no traffic is reaching the FortiGate's external interface, the administrator should check: D.Check the inbound network security group rules.
? Network Security Group Rules:AWS uses security groups as a virtual firewall that controls inbound and outbound traffic to AWS resources such as EC2 instances. If the FortiGate VM??s public interface is not receiving HTTPS or SSH traffic, it's likely because the inbound security group rules associated with that interface are not allowing access on the necessary ports (HTTPS - port 443, SSH - port 22).
? Troubleshooting:The administrator should verify that the security group rules for the FortiGate VM??s network interface allow inbound traffic on the specific ports used for management access. If these rules are absent or misconfigured, the intended traffic will be blocked, resulting in the inability to connect.
References:The role of security groups in network traffic management is a core concept in AWS and is outlined in AWS documentation. Checking security group rules is a standard troubleshooting step when dealing with connectivity issues to AWS resources.

NEW QUESTION 7
Refer to the exhibit



Registry Name test
Registry Url [redacted]9133563.dkr.ecr.eu-central-1.amazonaws.com
Cluster Connected [redacted]o_eks (Kubernetes Agent: ● Healthy)
Scan Status ✓ Completed

Repository	Tag	CAP	Last Updated
locust	*	5	2023-01-29, 4:35:05 p.m.

The exhibit shows the results of a FortiCNP registry scan

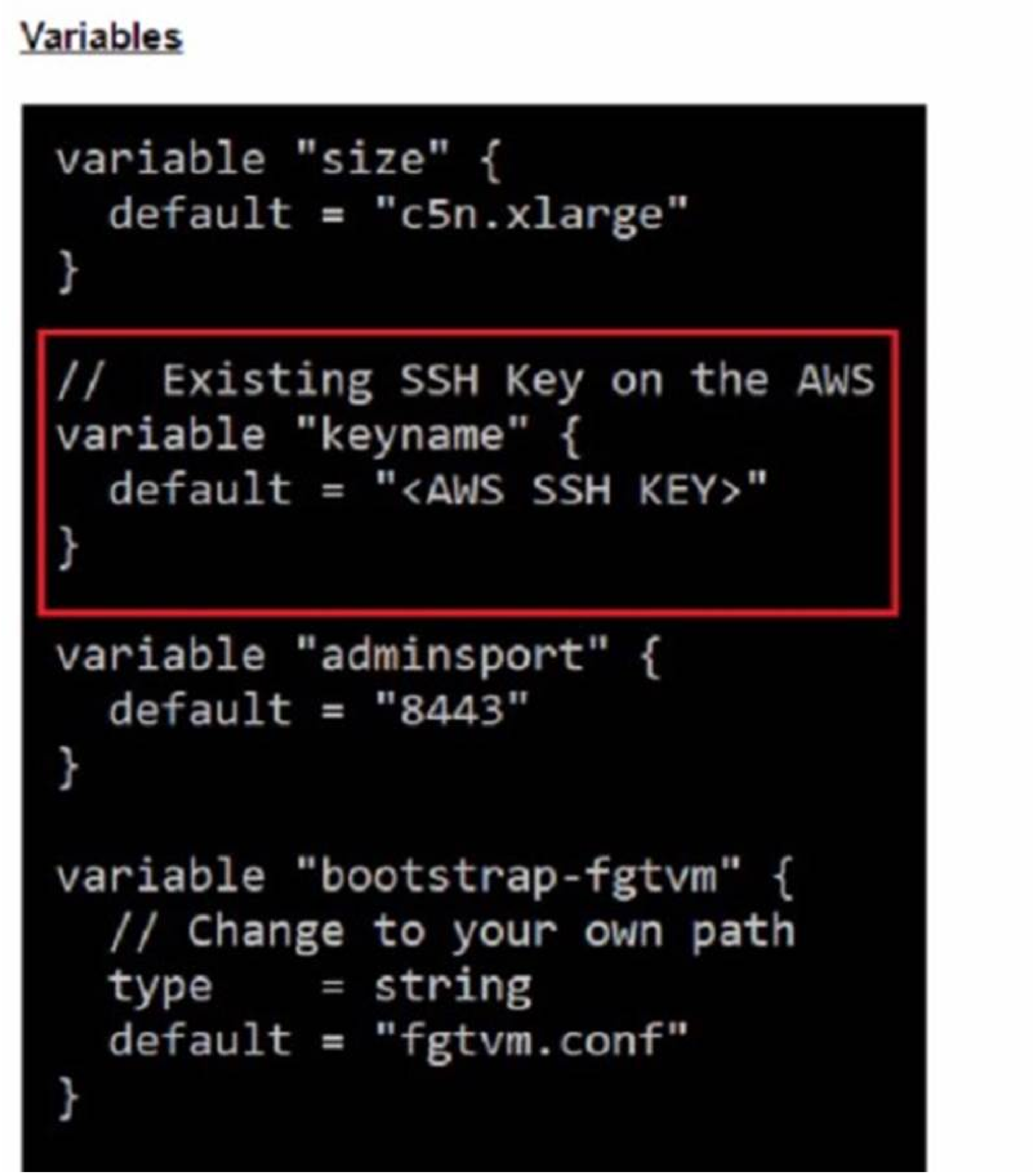
A. When adding a repository, you can leave the Tag section blank to scan all images-
B. The registry scan is part of the FortiCNP cloud protection.
C. The registry scan is part of the FortiCNP container protection.
D. When adding a repository, you can add a minimum number of images to be imported through the CAP section.

Answer: AC

Explanation:
The exhibit shows the results of a FortiCNP registry scan, which is part of the FortiCNP container protection. FortiCNP??s Container Protection provides deep visibility into the security posture of container registries and images1. The registry scan utilizes Common Vulnerabilities and Exposures (CVE) index regularly updated by NVD to detect underlying vulnerabilities, security flaws, and provides security best practices2. The registry scan is performed at the registry level, and it

can scan all images in a repository if the Tag section is left blank when adding a repository2. The CAP section stands for Container Assurance Policy, which defines the minimum number of images to be scanned per repository3. Therefore, the correct statements are A and C. References: Container Image Scan | FortiCNP 22.3.a, FortiCNP, Cloud Native Application Protection Platform | FortiCNP

NEW QUESTION 8
Refer to the exhibit.



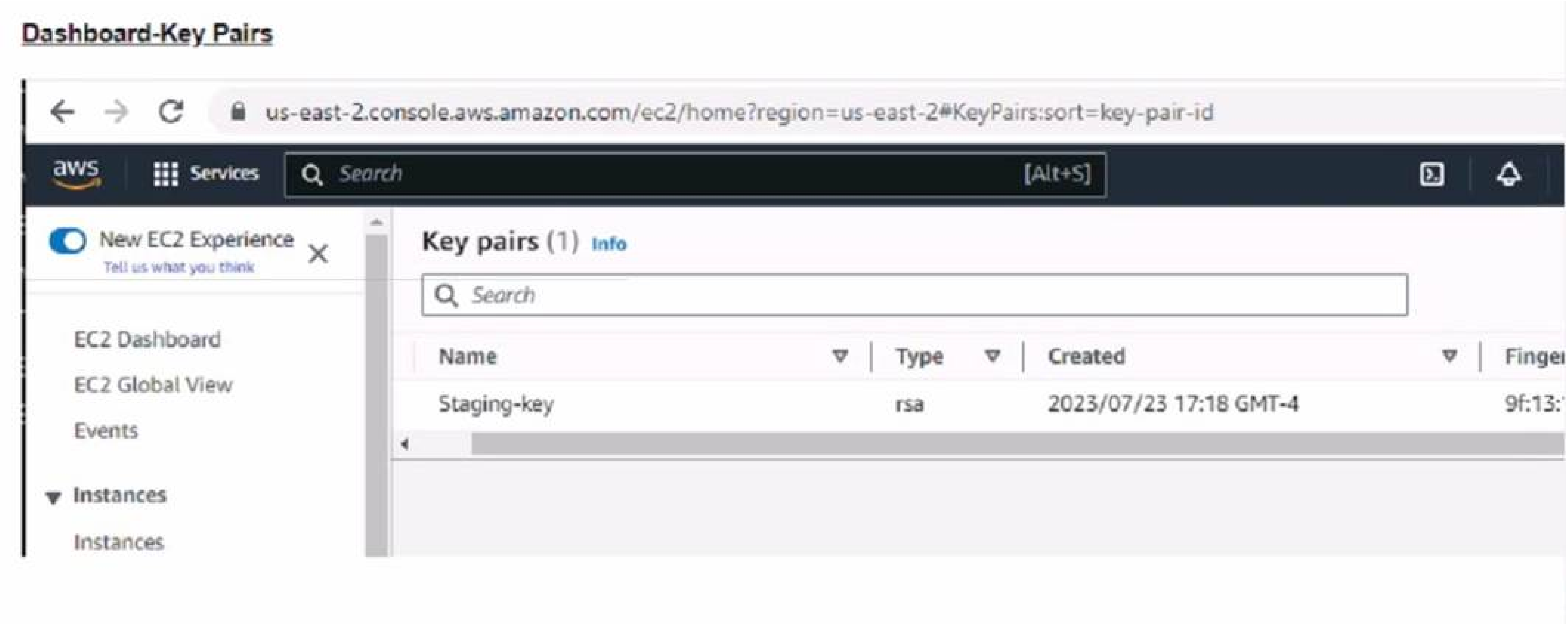
Variables

```
variable "size" {
  default = "c5n.xlarge"
}

//  Existing SSH Key on the AWS
variable "keyname" {
  default = "<AWS SSH KEY>"
}

variable "adminsport" {
  default = "8443"
}

variable "bootstrap-fgtvm" {
  // Change to your own path
  type    = string
  default = "fgtvm.conf"
}
```



Dashboard-Key Pairs

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#KeyPairs:sort=key-pair-id

aws Services Search [Alt+S]

New EC2 Experience
Tell us what you think

EC2 Dashboard
EC2 Global View
Events
Instances
Instances

Key pairs (1) Info

Search

Name	Type	Created	Finger
Staging-key	rsa	2023/07/23 17:18 GMT-4	9f:13:

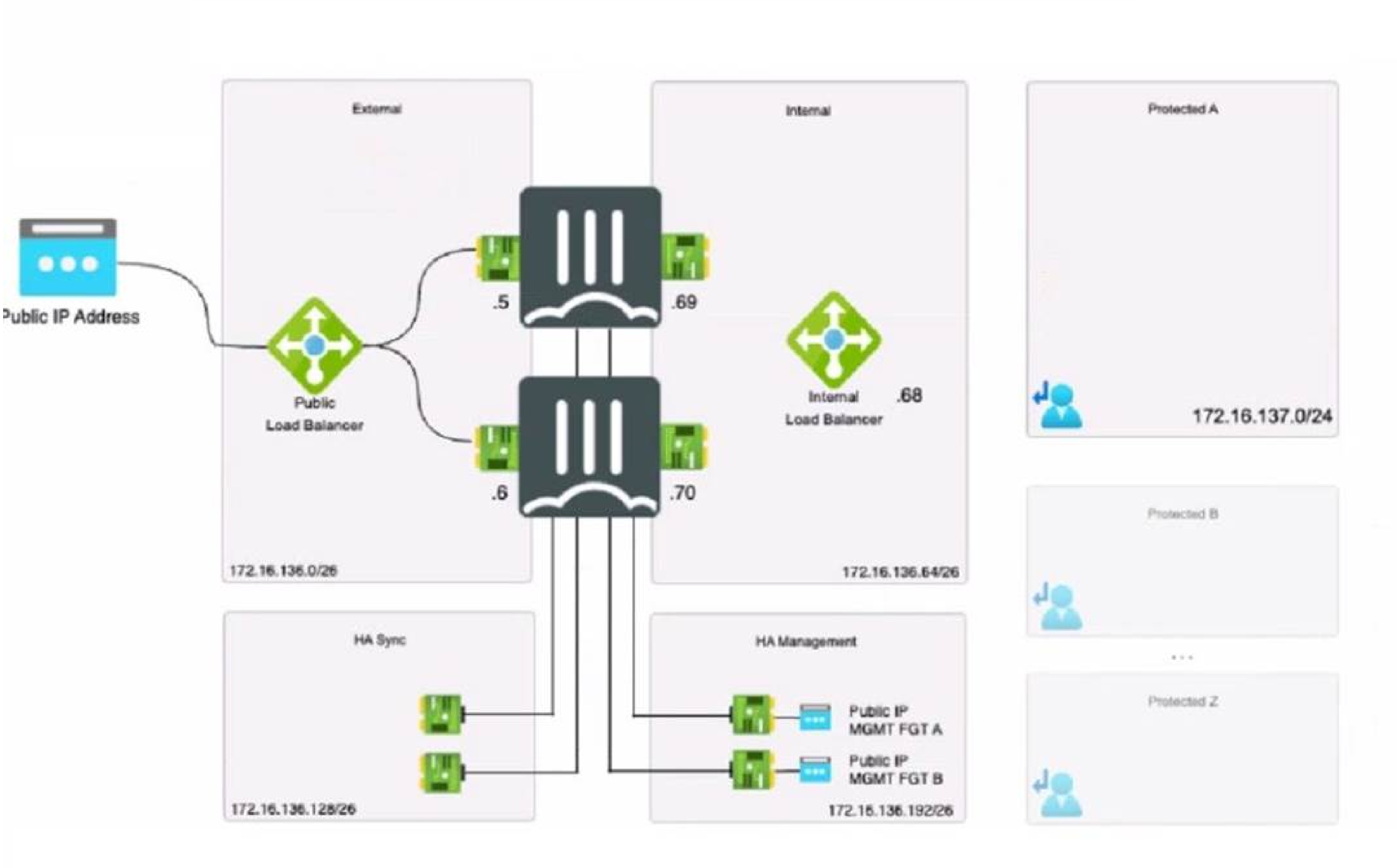
What value or values must the administrator use in the SSH Key section to deploy a FortiGate VM using Terraform in Amazon Web Services (AWS)?

A. Use the Name and ID values of the key pair
B. Use the Name of the key pair
C. Use the ID value of the key pair.
D. Use the Fingerprint value of the key pair

Answer: B

Explanation:
For deploying a FortiGate VM using Terraform in AWS, the administrator must use: B.Use the Name of the key pair.
? Terraform and AWS SSH Keys:When deploying instances in AWS using Terraform, it is required to specify the name of the SSH key pair to enable key- based authentication to the instance post-deployment.
? Configuration Syntax:The variablekeynamewithin the Terraform configuration should match the exact name of the SSH key pair as it is stored in AWS. This ensures that Terraform can reference the correct key during the deployment process to set up SSH access to the FortiGate VM.
? Terraform Variables:Thevariable "keyname"block in the Terraform configuration will look for the key pair name as it should be declared in theterraform.tfvarsfile or passed as a variable during execution. This does not require the key pair's ID or fingerprint, just its name.
References:The need for the SSH key pair's name in Terraform configurations for AWS deployments is outlined in the Terraform AWS Provider documentation, which specifies how resources should be provisioned using Terraform.

NEW QUESTION 9
Refer to the exhibit.



The exhibit shows an active-passive high availability FortiGate pair with external and internal Azure load balancers. There is no SDN connector used in this solution
Which configuration should the administrator implement?

A. Lambda IP address with one static route.
B. Probe IP address with two static routes
C. Probe IP address with one BGP route
D. Public load balancer IP address with two BGP routes.

Answer: B

Explanation:
Based on the provided exhibit showing an active-passive FortiGate High Availability (HA) pair with external and internal Azure load balancers and without the use of an SDN connector, the administrator should implement a Probe IP address with two static routes (Option B).
? Probe IP Address:Azure load balancers use a health probe to determine the health of the instances in the backend pool. The health probe ensures that the load balancer only directs traffic to the active (primary) FortiGate in an HA pair.
? Two Static Routes:Given that this is an active-passive setup, static routing should be used to ensure deterministic traffic flow. Two static routes would be configured to ensure that traffic can flow to the active unit and be correctly routed to the protected subnets in failover scenarios.
References:The recommendation for using a Probe IP address with static routes is based on Azure's best practices for load balancer configuration, particularly for HA scenarios, as well as on Fortinet's HA documentation for clouddeployments. This setup ensures high availability while allowing proper traffic distribution based on the health probe's findings.

NEW QUESTION 10
Which two attachments are necessary to connect a transit gateway to an existing VPC with BGP? (Choose two)

A. A transport attachment
B. A BGP attachment
C. A connect attachment
D. A GRE attachment

Answer: AC

Explanation:
The correct answer is A and C. A transport attachment and a connect attachment are necessary to connect a transit gateway to an existing VPC with BGP.
According to the AWS documentation for Transit Gateway, a transit gateway is a network transit hub that connects VPCs and on-premises networks. To connect a transit gateway to an existing VPC with BGP, you need to do the following steps:
? Create a transport attachment. A transport attachment is a resource that connects a VPC or VPN to a transit gateway. You can specify the BGP options for the transport attachment, such as the autonomous system number (ASN) and the BGP peer IP address.
? Create a connect attachment. A connect attachment is a resource that enables you to use your own appliance to provide network services for traffic that flows through the transit gateway. You can use a connect attachment to route traffic between the transport attachment and your appliance using GRE tunnels and BGP.
The other options are incorrect because:
? A BGP attachment is not a valid type of attachment for a transit gateway. BGP is a protocol that enables dynamic routing between the transit gateway and the VPC or VPN.
? A GRE attachment is not a valid type of attachment for a transit gateway. GRE is a protocol that encapsulates packets for tunneling purposes. GRE tunnels are established between the connect attachment and your appliance.
[Transit Gateways - Amazon Virtual Private Cloud] : [Transit Gateway Connect - Amazon Virtual Private Cloud]

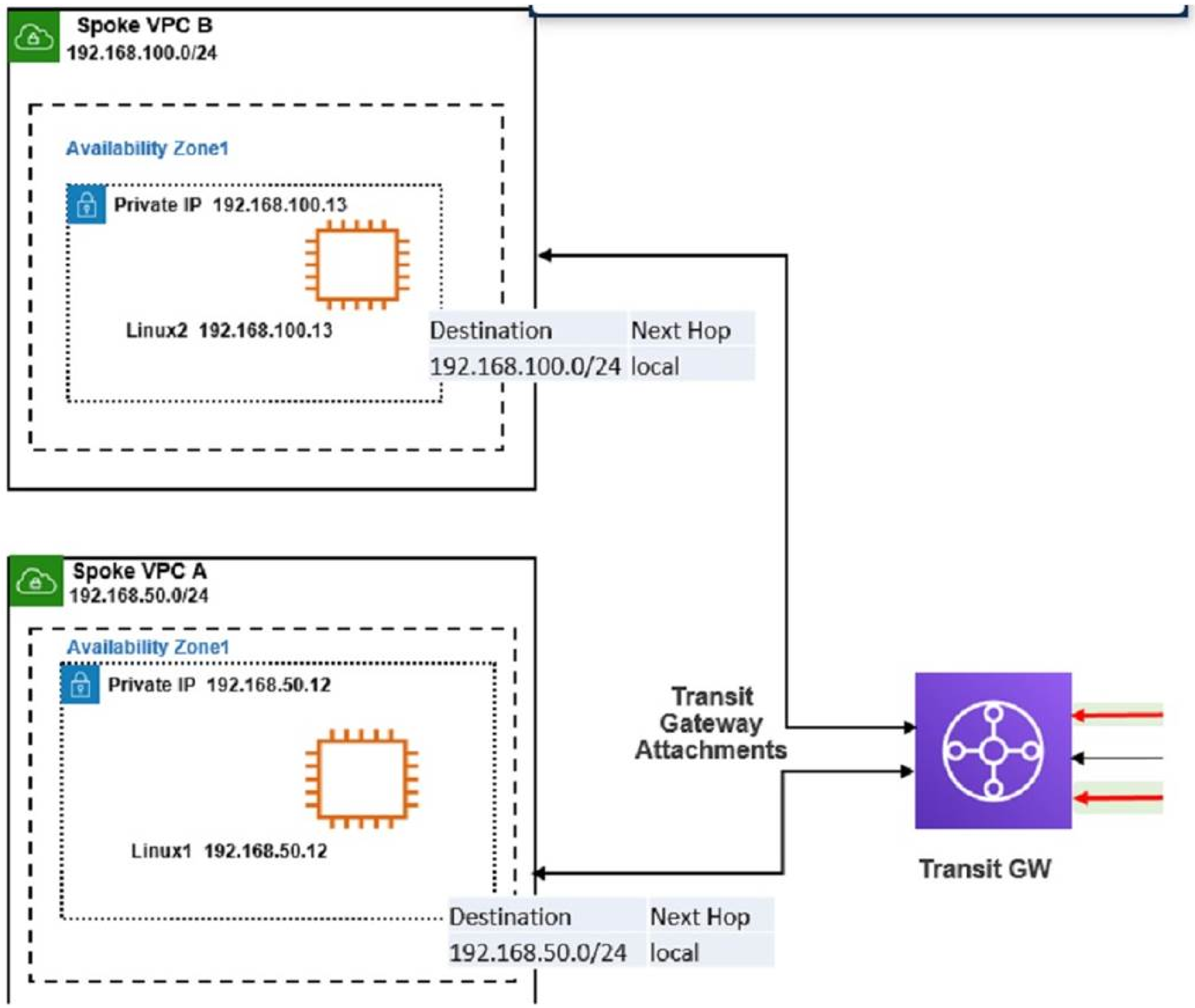
NEW QUESTION 10
Which two statements are true about Transit Gateway Connect peers in anlPv4 BGP configuration'? (Choose two.)

A. The inside CIDR blocks are used for BGP peering
B. You cannot use IPv6 addresses
C. You must specify a /29CIDR block from the 169.254.0.0/16 range
D. You must configure the second address from the IPv4 range on the device as the BGP IP address

Answer: AC

Explanation:
For Transit Gateway Connect peers in an IPv4 BGP configuration, the correct statements are:
? The inside CIDR blocks are used for BGP peering (Option A):In a BGP configuration for Transit Gateway Connect, the inside CIDR blocks, typically within the 169.254.0.0/16 range, are designated for the BGP peering connections. These blocks are reserved for internal network protocols and are commonly used in AWS for automatic IP address assignment within managed networking services.
? You must specify a /29 CIDR block from the 169.254.0.0/16 range (Option C):It is a requirement to specify a /29 CIDR block within the 169.254.0.0/16 range for setting up the network interfaces that facilitate BGP peering. This specific range allows for the necessary number of IP addresses to establish BGP sessions effectively between the transit gateway and on-premises or other virtual appliances.
References:These practices are in line with AWS guidelines for Transit Gateway Connect, which stipulate the use of specified CIDR blocks for internal networking and BGP configurations, ensuring seamless connectivity and routing management.

NEW QUESTION 15
Refer to the exhibit



Destination	Next Hop
192.168.100.0/24	local

Destination	Next Hop
192.168.50.0/24	local

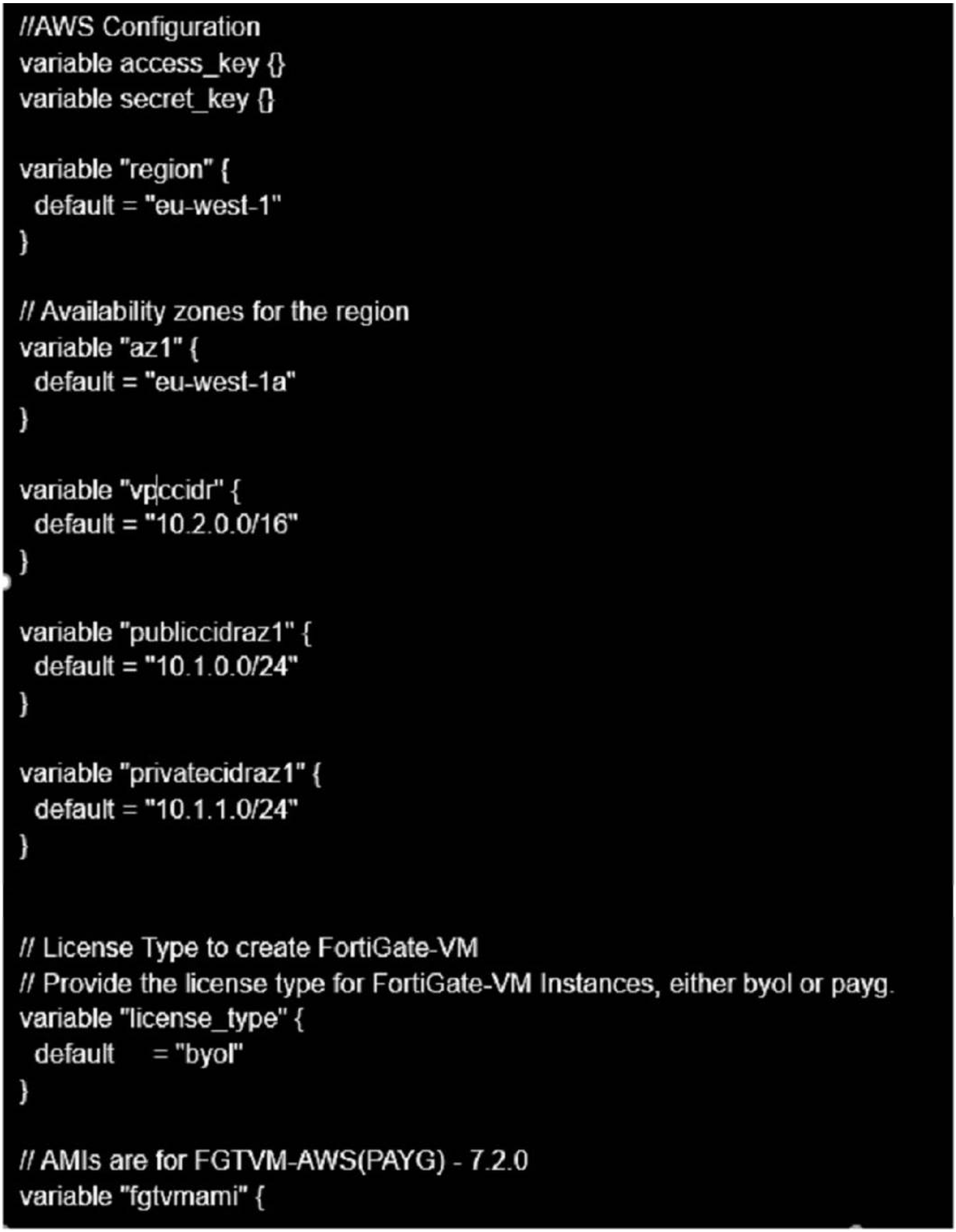
The exhibit shows a customer deployment of two Linux instances and their main routing table in Amazon Web Services (AWS). The customer also created a Transit Gateway (TGW) and two attachments
Which two steps are required to route traffic from Linux instances to the TGWQ (Choose two.)

A. In the TGW route table, add route propagation to 192.168.0 0/16
B. In the main subnet routing table in VPC A and B, add a new route with destination 0_0.0.0/0, next hop Internet gateway(IGW).
C. In the TGW route table, associate two attachments.
D. In the main subnet routing table in VPC A and B, add a new route with destination 0_0.0.0/0, next hop TGW.

Answer: CD

Explanation:
According to the AWS documentation for Transit Gateway, a Transit Gateway is a network transit hub that connects VPCs and on-premises networks. To route traffic from Linux instances to the TGW, you need to do the following steps:
? In the TGW route table, associate two attachments. An attachment is a resource that connects a VPC or VPN to a Transit Gateway. By associating the attachments to the TGW route table, you enable the TGW to route traffic between the VPCs and the VPN.
? In the main subnet routing table in VPC A and B, add a new route with destination 0_0.0.0/0, next hop TGW. This route directs all traffic from the Linux instances to the TGW, which can then forward it to the appropriate destination based on the TGW route table.
The other options are incorrect because:
? In the TGW route table, adding route propagation to 192.168.0 0/16 is not necessary, as this is already the default route for the TGW. Route propagation allows you to automatically propagate routes from your VPC or VPN to your TGW route table.
? In the main subnet routing table in VPC A and B, adding a new route with destination 0_0.0.0/0, next hop Internet gateway (IGW) is not correct, as this would bypass the TGW and send all traffic directly to the internet. An IGW is a VPC component that enables communication between instances in your VPC and the internet.
[Transit Gateways - Amazon Virtual Private Cloud]

NEW QUESTION 16
Refer to the exhibit



```
//AWS Configuration
variable access_key {}
variable secret_key {}

variable "region" {
  default = "eu-west-1"
}

// Availability zones for the region
variable "az1" {
  default = "eu-west-1a"
}

variable "vpccidr" {
  default = "10.2.0.0/16"
}

variable "publiccidraz1" {
  default = "10.1.0.0/24"
}

variable "privatecidraz1" {
  default = "10.1.1.0/24"
}


// License Type to create FortiGate-VM
// Provide the license type for FortiGate-VM Instances, either byol or payg.
variable "license_type" {
  default     = "byol"
}

// AMIs are for FGTVM-AWS(PAYG) - 7.2.0
variable "fgtvmami" {
```

You are tasked to deploy a FortiGate VM with private and public subnets in Amazon Web Services (AWS).
You examined the variables.tf file.
What will be the final result after running the terraform init and terraform apply commands?

A. Terraform will not deploy a FortiGate VM
B. Terraform will deploy a FortiGate VM in the eu-West-Ia region with private and publicsubnets.
C. Terraform will deploy a FortiGate VM in the eu-West-1a region with two subnets and byol license.
D. Terraform will deploy a FortiGate VM in the eu-West-Ia region without any subnets.

Answer: B

Explanation:
The variables.tf file shows that the FortiGate VM will be deployed in the eu-West-Ia region with private and public subnets. The region variable is set to ??eu-west-1?? and the availability_zone variable is set to ??eu-west-1a??. The vpc_id variable is set to ??vpc- 0e9d6a6f?? and the subnets variable is set to a list of two subnet IDs: ??subnet-0f9d6a6f?? and ??subnet-1f9d6a6f??. The license_type variable is set to ??on-demand?? and the ami_id variable is set to ??ami-0e9d6a6f??.
References: https://docs.fortinet.com/document/fortigate/6.4.0/aws- cookbook/236478/deploying-fortigate-vm-on-aws-using-terraform

NEW QUESTION 21
Which statement about immutable infrastructure in automation is true?

A. It is the practice of deploying a new server for every configuration change
B. It is the practice of modifying the existing server configuration after it is deployed
C. It is the practice of deploying two parallel servers for high availability.
D. It is the practice of applying hotfixes and OS patches after deployment

Answer: A

Explanation:
The statement that best describes the concept of immutable infrastructure in the context of automation is:
* A. It is the practice of deploying a new server for every configuration change.
? Immutable Infrastructure Concept:This approach to infrastructure management involves replacing servers or components entirely rather than making changes to existing configurations once they are deployed. When a change is needed, a new server instance is provisioned with the desired configuration and the old one is decommissioned after the new one is successfully deployed and tested.
? Benefits:Immutable infrastructure minimizes the risks associated with in-place updates, such as inconsistencies or failures due to configuration drift. It enhances reliability and predictability by ensuring that the deployed environment matches exactly what was tested in staging. Thispractice is particularly aligned with modern deployment strategies like blue/green or canary deployments.
References:The concept of immutable infrastructure is widely discussed in DevOps and cloud computing literature as a method to increase consistency and fault tolerance in automated environments.

NEW QUESTION 23
You need a solution to safeguard public cloud-hosted web applications from the OWASP Top 10 vulnerabilities. The solution must support the same region in which your applications reside, with minimum traffic cost
Which solution meets the requirements?

A. Use FortiADC
B. Use FortiCNP
C. Use FortiWebCloud
D. Use FortiGate

Answer: C

Explanation:
The correct answer is C. Use FortiWebCloud.
FortiWebCloud is a SaaS cloud-based web application firewall (WAF) that protects public cloud hosted web applications from the OWASP Top 10, zero day threats, and other application layer attacks1.FortiWebCloud also includes robust features such as API discovery and protection, bot mitigation, threat analytics, and advanced reporting2.FortiWebCloud supports multiple regions across the world, and you can choose the region that is closest to your applications to minimize traffic cost3.
The other options are incorrect because:
? FortiADC is an application delivery controller that provides load balancing, acceleration, and security for web applications.It is not a dedicated WAF solution and does not offer the same level of protection as FortiWebCloud4.
? FortiCNP is a cloud-native platform that provides security and visibility for containerized applications.It is not a WAF solution and does not protect web applications from the OWASP Top 10 vulnerabilities5.
? FortiGate is a next-generation firewall (NGFW) that provides network security and threat prevention. It is not a WAF solution and doesnot offer the same level of protection as FortiWebCloud for web applications.It also requires additional configuration and management to deploy in the public cloud6.
1:Overview | FortiWeb Cloud 23.3.0 - Fortinet Documentation2:Web Application Firewall (WAF) & API Protection | Fortinet3: [FortiWeb Cloud WAF-as-a-Service | Fortinet]4: [Application Delivery Controller (ADC) | Fortinet]5: [Fortinet Cloud Native Platform | Fortinet]6: [FortiGate Next-Generation Firewall (NGFW) | Fortinet]

NEW QUESTION 24
Which two Amazon Web Services (AWS) features support east-west traffic inspection within the AWS cloud by the FortiGate VM? (Choose two.)

A. A NAT gateway with an EIP
B. A transit gateway with an attachment
C. An Internet gateway with an EIP
D. A transit VPC

Answer: BD

Explanation:
The correct answer is B and D. A transit gateway with an attachment and a transit VPC support east-west traffic inspection within the AWS cloud by the FortiGate VM. According to the Fortinet documentation for Public Cloud Security, a transit gateway is a network transit hub that connects VPCs and on-premises networks. A transit gateway attachment is a resource that connects a VPC or VPN to a transit gateway.By using a transit gateway with an attachment, you can route traffic from your spoke VPCs to your security VPC, where the FortiGate VM can inspect the traffic1.
A transit VPC is a VPC that serves as a global network transit center for connecting multiple VPCs, remote networks, and virtual private networks (VPNs).By using a transit VPC, you can deploy the FortiGate VM as a virtual appliance that provides network security and threat prevention for your VPCs2.
The other options are incorrect because:
? A NAT gateway with an EIP is a service that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a connection with those instances.A NAT gateway with an EIP does not support east-west traffic inspection within the AWS cloud by the FortiGate VM3.

? An Internet gateway with an EIP is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.An Internet gateway with an EIP does not support east-west traffic inspection within the AWS cloud by the FortiGate VM4.
1:Fortinet Documentation Library - Deploying FortiGate VMs on AWS2: [Fortinet Documentation Library - Transit VPC on AWS]3: [NAT Gateways - Amazon Virtual Private Cloud]4: [Internet Gateways - Amazon Virtual Private Cloud]

NEW QUESTION 27
You are asked to find a solution to replace the existing VPC peering topology to have a higher bandwidth connection from Amazon Web Services (AWS) to the on-premises data center Which two solutions will satisfy the requirement? (Choose two.)

A. Use ECMP and VPN to achieve higher bandwidth.
B. Use transit VPC to build multiple VPC connections to the on-premises data center
C. Use a transit VPC with hub and spoke topology to create multiple VPN connections to the on-premises data center.
D. Use the transit gateway attachment With VPN option to create multiple VPN connections to the on-premises data center

Answer: CD

Explanation:
The correct answer is C and D. Use a transit VPC with hub and spoke topology to create multiple VPN connections to the on-premises data center. Use the transit gateway attachment with VPN option to create multiple VPN connections to the on-premises data center.
According to the Fortinet documentation for Public Cloud Security, a transit VPC is a VPC that serves as a global network transit center for connecting multiple VPCs, remote networks, and virtual private networks (VPNs). A transit VPC can use a hub and spoke topology to create multiple VPN connections to the on-premises data center, using the FortiGate VM as a virtual appliance that provides network security and threat prevention.A transit VPC can also leverage Equal-Cost Multi-Path (ECMP) routing to achieve higher bandwidth and load balancing across multiple VPN tunnels1.
A transit gateway is a network transit hub that connects VPCs and on-premises networks. A transit gateway attachment is a resource that connects a VPC or VPN to a transit gateway. You can use the transit gateway attachment with VPN option to create multiple VPN connections to the on-premises data center, using the FortiGate VM as a virtual appliance that provides network security and threat prevention.A transit gateway attachment with VPN option can also leverage ECMP routing to achieve higher bandwidth and load balancing across multiple VPN tunnels2.
The other options are incorrect because:
? Using ECMP and VPN to achieve higher bandwidth is not a complete solution, as it does not specify how to replace the existing VPC peering topology or how to connect the AWS VPCs to the on-premises data center.
? Using transit VPC to build multiple VPC connections to the on-premises data center is not a correct solution, as it does not specify how to use a hub and spoke topology or how to leverage ECMP routing for higher bandwidth.
1:Fortinet Documentation Library - Transit VPC on AWS2:Fortinet Documentation Library - Deploying FortiGate VMs on AWS

NEW QUESTION 30
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_PBC-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_PBC-7.2 Product From:

https://www.2passeasy.com/dumps/NSE7_PBC-7.2/

Money Back Guarantee

NSE7_PBC-7.2 Practice Exam Features:

* NSE7_PBC-7.2 Questions and Answers Updated Frequently

* NSE7_PBC-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_PBC-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_PBC-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year