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
An administrator decides to use the Use managed identity option on the FortiGate SDN connector with Microsoft Azure However, the SDN connector is failing on the connection What must the administrator do to correct this issue?

A. Make sure to add the Tenant ID on FortiGate side of the configuration
B. Make sure to set the type to system managed identity on FortiGate SDN connectorsettings
C. Make sure to enable the system assigned managed identity on Azure
D. Make sure to add the Client secret on FortiGate side of the configuration

Answer: C

Explanation:
When an administrator decides to use the 'Use managed identity' option for the FortiGate SDN connector with Microsoft Azure and faces a connection failure, the correct action to take is:
C.Make sure to enable the system assigned managed identity on Azure.
? Managed Identity Configuration:The system assigned managed identity is a feature in Azure that provides an identity for the Azure service instance (in this case, the FortiGate SDN connector) within Azure Active Directory and eliminates the need for credentials to be stored in the configuration.
? Troubleshooting Connection Issues:If the SDN connector is failing to connect, it could be because the system assigned managed identity has not been enabled or configured properly in Azure for the FortiGate service.
References:Azure documentation on managed identities explains the need to enable and configure this feature for services to authenticate and interact securely with Azure resources.

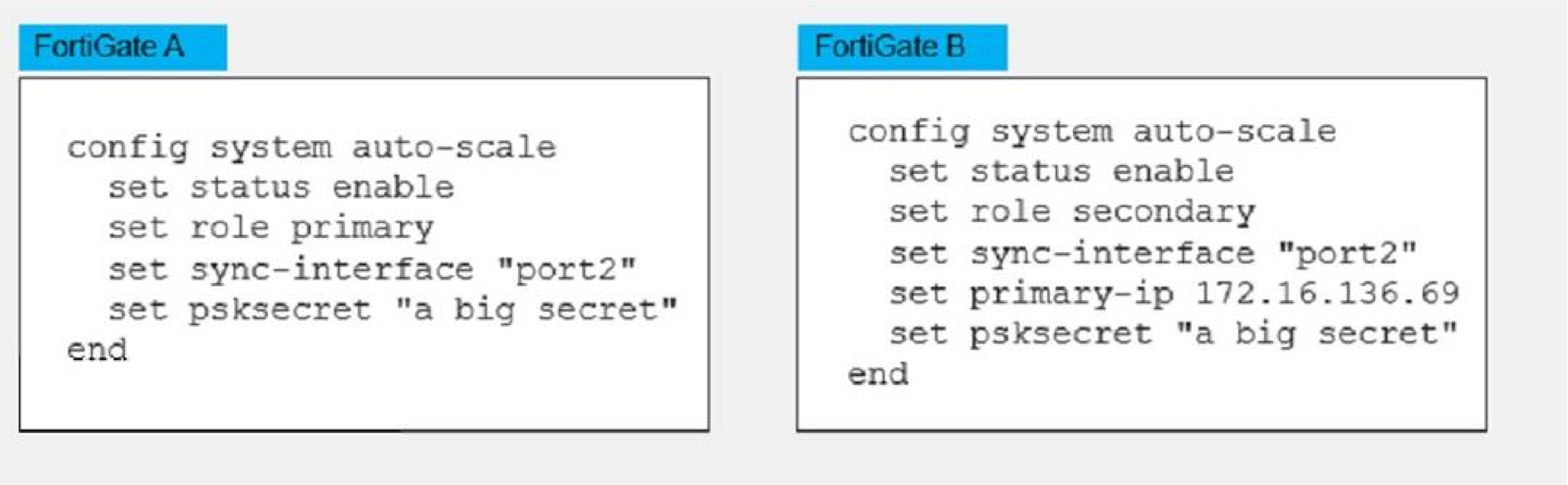
NEW QUESTION 2
You are adding more spoke VPCs to an existing hub and spoke topology Your goal is to finish this task in the minimum amount of time without making errors. Which Amazon AWS services must you subscribe to accomplish your goal?

A. GuardDuty, CloudWatch
B. WAF, DynamoDB
C. Inspector, S3
D. CloudWatch, S3

Answer: D

Explanation:
The correct answer is D. CloudWatch and S3.
According to the GitHub repository for the Fortinet aws-lambda-tgw script1, this function requires the following AWS services:
? CloudWatch: A monitoring and observability service that collects and processes
events from various AWS resources, including Transit Gateway attachments and route tables.
? S3: A scalable object storage service that can store the configuration files and logs
generated by the Lambda function.
By using the Fortinet aws-lambda-tgw script, you can automate the creation and
configuration of Transit Gateway Connect attachments for your FortiGate devices.This can help you save time and avoid errors when adding more spoke VPCs to an existing hub and spoke topology1.
The other AWS services mentioned in the options are not required for this task. GuardDuty is a threat detection service that monitors for malicious and unauthorized behavior to help protect AWS accounts and workloads. WAF is a web application firewall that helps protect web applications from common web exploits. Inspector is a security assessment service that helps improve the security and compliance of applications deployed on AWS. DynamoDB is a fast and flexible NoSQL database service that can store various types of data.
1:GitHub - fortinet/aws-lambda-tgw

NEW QUESTION 3
Refer to the exhibit


FortiGate A

```
config system auto-scale
  set status enable
  set role primary
  set sync-interface "port2"
  set psksecret "a big secret"
end
```

FortiGate B

```
config system auto-scale
  set status enable
  set role secondary
  set sync-interface "port2"
  set primary-ip 172.16.136.69
  set psksecret "a big secret"
end
```

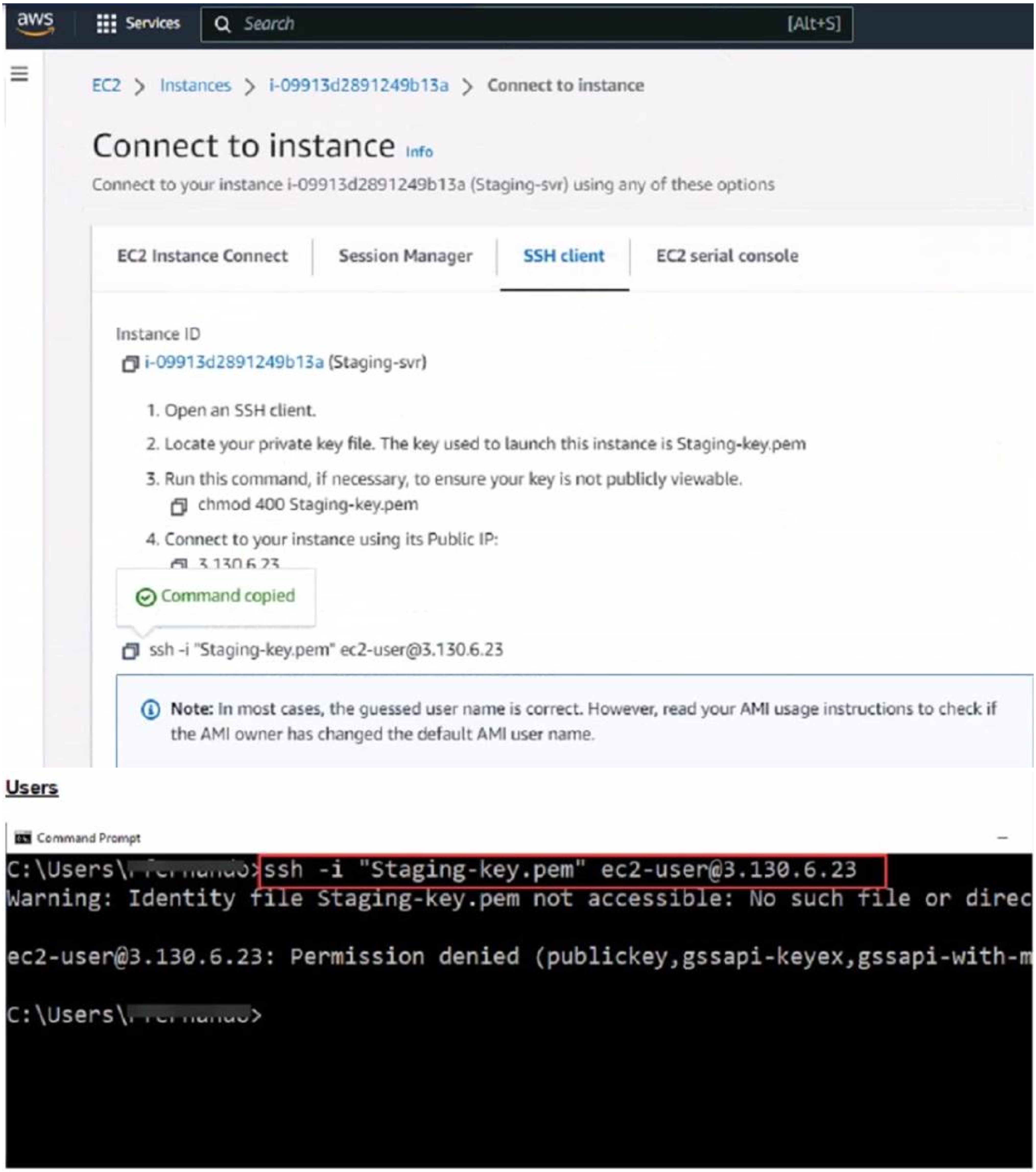
An administrator deployed an HA active-active load balance sandwich in Microsoft Azure. The setup requires configuration synchronization between devices- What are two outcomes from the configured settings? (Choose two.)

A. FortiGate-VM instances are scaled out automatically according to predefined workload levels.
B. FortiGate A and FortiGate B are two independent devices.
C. By default, FortiGate uses FGCP
D. It does not synchronize the FortiGate hostname

Answer: BD

Explanation:
* B. FortiGate A and FortiGate B are two independent devices. This means that they are not part of a cluster or a high availability group, and they do not share the same configuration or state information. They are configured as standalone FortiGates with standalone configuration synchronization enabled1. This feature allows them to synchronize most of their configuration settings with each other, except for some settings that identify the FortiGate to the network, such as the hostname1. D. It does not synchronize the FortiGate hostname. This is one of the settings that are excluded from the standalone configuration synchronization, as mentioned above. The hostname is a unique identifier for each FortiGate device, and it should not be changed by the synchronization process1.
The other options are incorrect because:
? FortiGate-VM instances are not scaled out automatically according to predefined workload levels. This is a feature of the auto scaling solution for FortiGate-VM on Azure, which requires a different deployment and configuration than the one shown in the exhibit2. The exhibit shows a static deployment of two FortiGate-VM instances behind an Azure load balancer, which does not support auto scaling.
? By default, FortiGate does not use FGCP. FGCP stands for FortiGate Clustering Protocol, which is used to synchronize configuration and state information between FortiGate devices in a cluster or a high availability group3. However, the exhibit shows that the FortiGates are not in a cluster or a high availability group, and they use standalone configuration synchronization instead of FGCP.

NEW QUESTION 4
Refer to the exhibit.



Connect to instance Info

Connect to your instance i-09913d2891249b13a (Staging-svr) using any of these options

Instance ID
i-09913d2891249b13a (Staging-svr)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is Staging-key.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 Staging-key.pem
4. Connect to your instance using its Public IP:
   3.130.6.23

Command copied

ssh -i "Staging-key.pem" ec2-user@3.130.6.23

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Users

```
C:\Users\[redacted]>ssh -i "Staging-key.pem" ec2-user@3.130.6.23
Warning: Identity file Staging-key.pem not accessible: No such file or direc

ec2-user@3.130.6.23: Permission denied (publickey,gssapi-keyex,gssapi-with-m

C:\Users\[redacted]>
```

What could be the reason that the administrator cannot access the EC2 instance?

A. You must elevate the permissions to access the EC2 instance
B. You must run the chmod 400 Staging-key.peracommand before accessing the instance.
C. There is no . pem key created on in Amazon Web Services (AWS)
D. The directory location of the . pem file is incorrect.

Answer: D

Explanation:
The reason the administrator cannot access the EC2 instance could be: D.The directory location of the .pem file is incorrect.
? SSH Key Location:When initiating an SSH connection to an AWS EC2 instance,
you must specify the private key file (.pem file) location that corresponds to the public key used when the instance was launched. The error "Warning: Identity file Staging-key.pem not accessible: No such file or directory" indicates that the SSH client cannot find the .pem file at the specified location.
? Correct File Path:The administrator needs to ensure that the path to theStaging- key.pemfile is correctly specified when running the SSH command. If the file is not in the current directory from which the command is executed, the full or relative path to the file must be provided.
References:This behavior is in line with standard SSH connection practices and AWS guidelines for accessing EC2 instances. It is a common issue that occurs when the private key file is not located in the directory from which the SSH command is being executed or the path provided is incorrect.

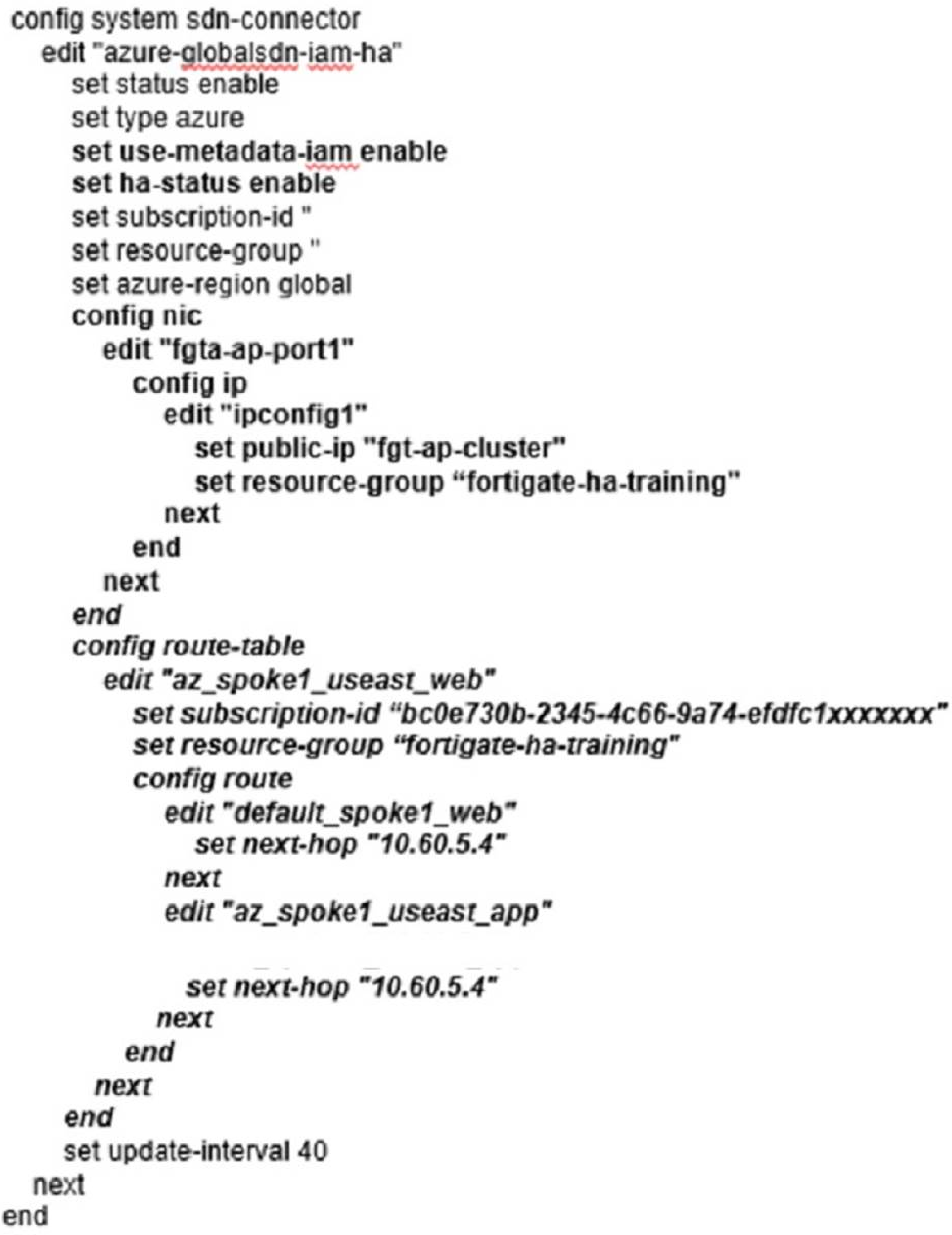
NEW QUESTION 5
What are three important steps required to get Terraform ready using Microsoft Azure Cloud Shell? (Choose three.)

A. Set up a storage account in Azure.
B. use the -O command to download Terraform.
C. Subscribe to Terraform in Azure.
D. Move the Terraform file to the bin directory.
E. Use the wget (te=aform vession) command to upload Terraform.

Answer: ADE

Explanation:
To get Terraform ready using Microsoft Azure Cloud Shell, you need to perform the following steps:
? Set up a storage account in Azure. This is required to store the Terraform state file in a blob container, which enables collaboration and persistence of the infrastructure configuration1.
? Use the wget (terraform_version) command to upload Terraform. This command downloads the latest version of Terraform from the official website and saves it as a zip file in the current directory2.
? Move the Terraform file to the bin directory. This step extracts the Terraform executable from the zip file and moves it to the bin directory, which is part of the PATH environment variable. This allows you to run Terraform commands from any directory in Cloud Shell2.
The other options are incorrect because:
? You do not need to use the -O command to download Terraform. This command is used to specify a different output file name for the downloaded file, but it is not necessary for this task3.
? You do not need to subscribe to Terraform in Azure. Terraform is an open-source tool that can be used with any cloud provider, and there is no subscription or registration required to use it with Azure4. References:
? Updating the route table and adding an IAM policy
? Configure Terraform in Azure Cloud Shell with Bash
? wget(1) - Linux man page
? Terraform by HashiCorp

NEW QUESTION 6
Refer to the exhibit



```
config system sdn-connector
  edit "azure-globalsdn-iam-ha"
    set status enable
    set type azure
    set use-metadata-iam enable
    set ha-status enable
    set subscription-id ''
    set resource-group ''
    set azure-region global
    config nic
      edit "fgta-ap-port1"
        config ip
          edit "ipconfig1"
            set public-ip "fgt-ap-cluster"
            set resource-group "fortigate-ha-training"
          next
        end
      next
    end
    config route-table
      edit "az_spoke1_useast_web"
        set subscription-id "bc0e730b-2345-4c66-9a74-efdfc1xxxxxxx"
        set resource-group "fortigate-ha-training"
        config route
          edit "default_spoke1_web"
            set next-hop "10.60.5.4"
          next
          edit "az_spoke1_useast_app"

            set next-hop "10.60.5.4"
          next
        end
      next
    end
    set update-interval 40
  next
end
```

You deployed an HA active-passive FortiGate VM in Microsoft Azure.
Which two statements regarding this particular deployment are true? (Choose two.)

A. During the failover, the passive FortiGate issues API calls to Azure
B. Use the vdom-excepticn command to synchronize the configuration.
C. There is no SLA for API calls from Microsoft Azure.
D. By default, the configuration does not synchromze between the primary and secondary devices.

Answer: AD

Explanation:
? A is correct because in this deployment, the passive FortiGate issues API calls to Azure to update the routing table and the public IP address of the active FortiGate123. This way, the traffic is redirected to the new active FortiGate after a failover.
? B is incorrect because the vdom-exception command is used to exclude specific VDOMs from being synchronized in an HA cluster.This command is not related to this deployment scenario.
? C is incorrect because Microsoft Azure does provide an SLA for API calls.
According to the Azure Service Level Agreements, the API Management service has a monthly uptime percentage of at least 99.9% for the standard tier and higher.
? D is correct because by default, the configuration is not synchronized between the
primary and secondary devices in this deployment. The administrator needs to manually enable configuration synchronization on both devices123. Alternatively, the administrator can use FortiManager to manage and synchronize the configuration of both devices4.

NEW QUESTION 7
You have created a TGW route table to route traffic from your spoke VPC to the security VPC where two FortiGate devices are inspecting traffic. Your spoke VPC CIDR block is already propagated to the Transit Gateway (TGW) route table.
Which type of attachment should you use to advertise routes through BGP from the spoke VPC to the security VPC?

A. Connect attachment
B. VPC attachment
C. Route attachment
D. GRE attachment

Answer: B

Explanation:
A VPC attachment is the type of attachment that allows you to connect a VPC to a TGW and advertise routes through BGP. A VPC attachment creates a VPN connection between the VPC and the TGW, and enables dynamic routing with BGP. A connect attachment is used to connect a VPN or Direct Connect gateway to a TGW. A route attachment is not a valid type of attachment for TGW. A GRE attachment is used to connect a FortiGate device to a TGW using GRE tunnels.
References:
? Creating the TGW and related resources
? Configuring TGW route tables
? FortiGate Public Cloud 7.2.0 - Fortinet Documentation
? Updating the route table and adding an IAM policy

NEW QUESTION 8
You are configuring the failover settings on a FortiGate active-passive SDN connector solution in Microsoft Azure. Which two mandatory settings are required after the initial deployment? (Choose two)

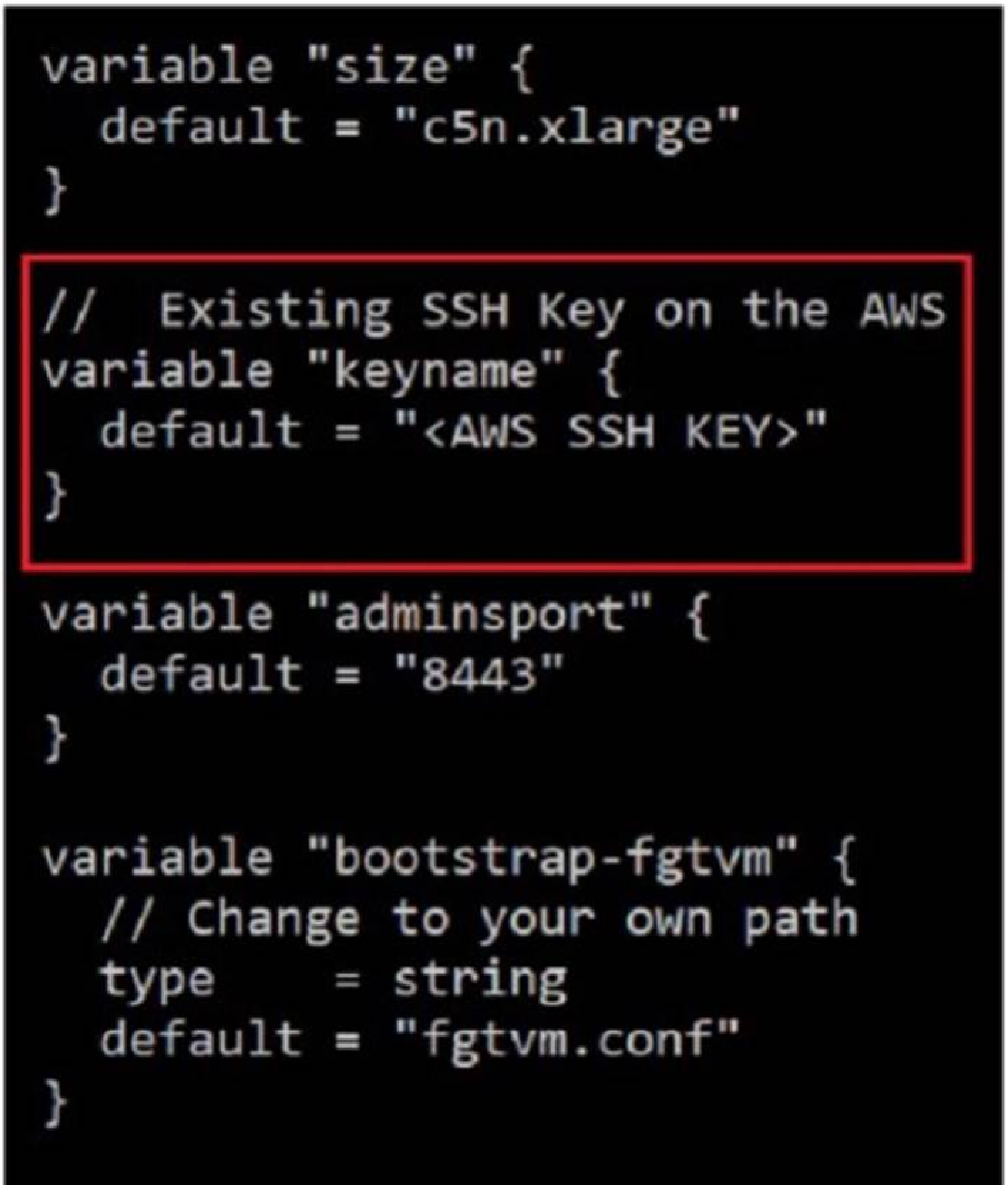
A. Subscription-id
B. FortiGate license file
C. Active FortiGate serial number
D. Resource group name

Answer: AD

Explanation:
For configuring the failover settings on a FortiGate active-passive SDN connector solution in Microsoft Azure, the two mandatory settings required after the initial deployment are: A.Subscription-id D.Resource group name
? Subscription ID:This is a unique identifier for your Azure subscription under which all resources are created and billed. FortiGate needs this to interact with the Azure resources associated with that subscription.
? Resource Group Name:A resource group in Azure is a container that holds related resources for an Azure solution. The SDN connector requires the resource group name to correctly identify and manage the resources it should control, especially in a failover scenario.
References:The requirement for these specific details is found in Azure's best practices for resource management and Fortinet's documentation on deploying and configuring FortiGate appliances in Azure environments.

NEW QUESTION 9
Refer to the exhibit.

Variables



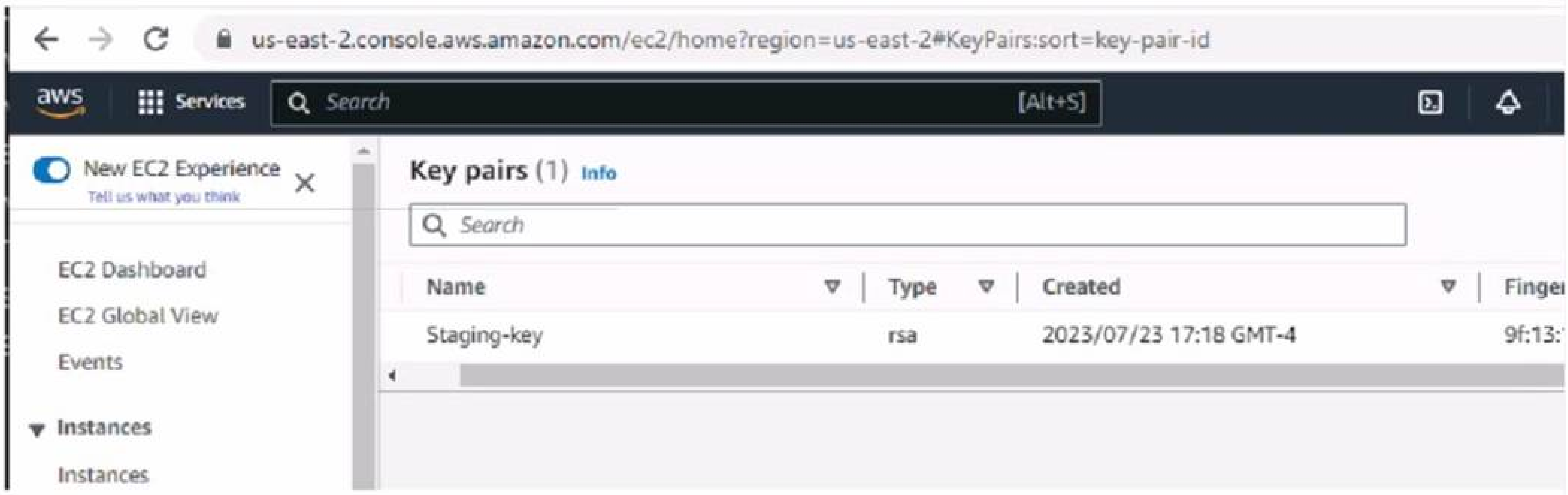
```
variable "size" {
  default = "c5n.xlarge"
}

// 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

Key pairs (1) Info

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.

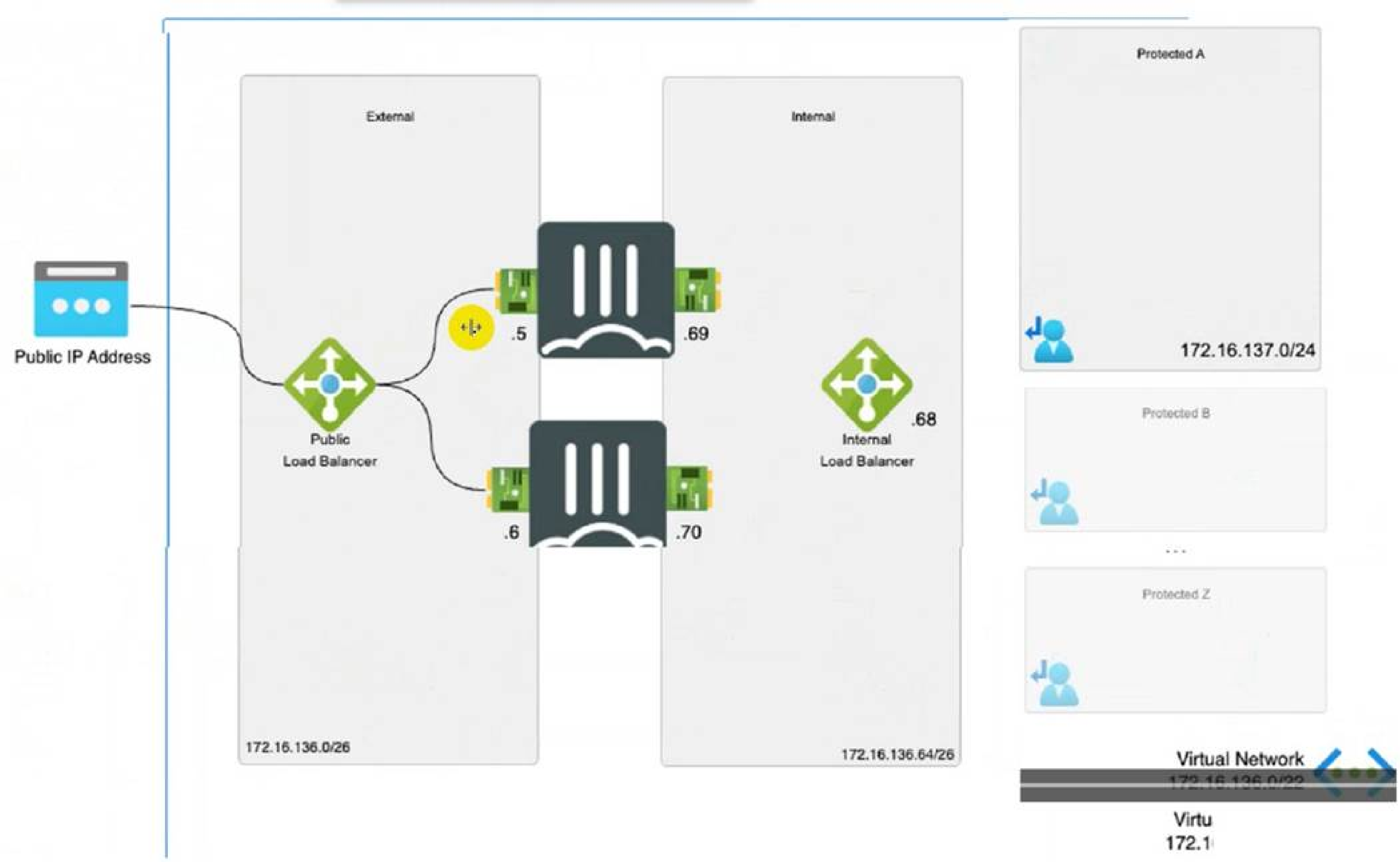
NEW QUESTION 10
An administrator is looking for a solution that can provide insight into users and data stored in major SaaS applications in the multicloud environment Which product should the administrator deploy to have secure access to SaaS applications?

A. FortiProxy
B. FortiSandbox
C. ForliCASB
D. FortiWeb

Answer: C

Explanation:
For administrators seeking to gain insights into user activities and data within major SaaS applications across multicloud environments, deploying FortiCASB (Cloud Access Security Broker) is the most effective solution (Option C).
? Role of FortiCASB:FortiCASB is specifically designed to provide security visibility, compliance, data security, and threat protection for cloud-based services. It acts as a mediator between users and cloud service providers, offering deep visibility into the operations and data handled by SaaS applications.
? Capabilities of FortiCASB:This product enables administrators to monitor and control the access and usage of SaaS applications. It helps in assessing security configurations, tracking user activities, and evaluating data movement across the cloud services. By doing so, it assists organizations in enforcing security policies, detecting anomalous behaviors, and ensuring compliance with regulatory standards.
? Integration and Functionality:FortiCASB integrates seamlessly with major SaaS platforms, providing a centralized management interface that allows for comprehensive analysis and real-time protection measures. This integration ensures that organizations can maintain control over their data across various cloud services, enhancing the overall security posture in a multicloud environment.
References:Fortinet??s official documentation on FortiCASB details its functionalities and integration capabilities with SaaS applications, highlighting its role in providing enhanced security measures for cloud-based services.

NEW QUESTION 10
Refer to the exhibit



Consider the active-active load balance sandwich scenario in Microsoft Azure.
What are two important facts in the active-active load balance sandwich scenario? (Choose two)

A. It uses the vdom-exception command to exclude the configuration from being synced
B. It is recommended to enable NAT on FortiGate policies.
C. It uses the FGCP protocol
D. It supports session synchronization for handling asynchronous traffic.

Answer: BD

Explanation:
* B. It is recommended to enable NAT on FortiGate policies. This is because the Azure load balancer uses a hash-based algorithm to distribute traffic to the FortiGate instances, and it relies on the source and destination IP addresses and ports of the packets1. If NAT is not enabled, the source IP address of the packets will be the same as the load balancer??s frontend IP address, which will result in uneven distribution of traffic and possible asymmetric routing issues1. Therefore, it is recommended to enable NAT on the FortiGate policies to preserve the original source IP address of the packets and ensure optimal load balancing and routing1. D. It supports session synchronization for handling asynchronous traffic. This means that the FortiGate instances can synchronize their session tables with each other, so that they can handle traffic that does not follow the same path as the initial packet of a session2. For example, if a TCP SYN packet is sent to FortiGate A, but the TCP SYN-ACK packet is sent to FortiGate B, FortiGate B can forward the packet to FortiGate A by looking up the session table2. This feature allows the FortiGate instances to handle asymmetric traffic that may occur due to the Azure load balancer??s hash-based algorithm or other factors.
The other options are incorrect because:
? It does not use the vdom-exception command to exclude the configuration from being synced. The vdom-exception command is used to exclude certain configuration settings from being synchronized between FortiGate devices in a cluster or a high availability group3. However, in this scenario, the FortiGate devices are not in a cluster or a high availability group, but they are standalone devices with standalone configuration synchronization enabled. This feature allows them to synchronize most of their configuration settings with each other, except for some settings that identify the FortiGate to the network, such as the hostname.
? It does not use the FGCP protocol. FGCP stands for FortiGate Clustering Protocol, which is used to synchronize configuration and state information between FortiGate devices in a cluster or a high availability group. However, in this scenario, the FortiGate devices are not in a cluster or a high availability group, and they use standalone configuration synchronization instead of FGCP.

NEW QUESTION 15
An administrator would like to keep track of sensitive data files located in the Amazon Web Services (AWS) S3 bucket and protect it from malware. Which Fortinet product or feature should the administrator use?

A. FortiCNP application control policies
B. FortiCNP web sensitive polices
C. FortiCNP DLP policies
D. FortiCNP compliance scanning policies

Answer: C

Explanation:
To keep track of sensitive data files located in AWS S3 buckets and protect them from malware, the administrator should use: C.FortiCNP DLP policies.
? Data Loss Prevention (DLP):DLP policies are designed to detect and prevent unauthorized access or sharing of sensitive data. In the context of AWS S3, DLP policies can be used to scan for sensitive information stored in S3 objects and enforce protective measures to prevent data exfiltration or compromise.
? FortiCNP Integration:FortiCNP is Fortinet??s cloud-native protection platform that offers security and compliance solutions across cloud environments. By applying DLP policies within FortiCNP, the administrator can ensure sensitive data within S3 is monitored and protected consistently.
References:Fortinet's FortiCNP documentation provides information on implementing DLP policies within cloud environments, highlighting the capabilities for protecting sensitive data within cloud storage services like AWS S3.

NEW QUESTION 20
How does an administrator secure container environments from newly emerged security threats?

A. Use distributed network-related application control signatures.
B. Use Amazon AWS-related application control signatures
C. Use Amazon AWS_S3-related application control signatures
D. Use Docker-related application control signatures

Answer: D

Explanation:
Securing container environments from newly emerged security threats involves employing specific security mechanisms tailored to the technology and structure of containers. In this context, the use of Docker-related application control signatures (Option D) is critical for effectively managing and mitigating threats in containerized environments.
? Docker-Specific Threats:Docker containers, being a prevalent form of container technology, are targeted by various security threats, including those that exploit vulnerabilities specific to the Docker environment and runtime. Using Docker- related application control signatures means implementing security measures that are specifically designed to detect and respond to anomalies and threats that are unique to Docker containers.
? Application Control Signatures:These are sets of definitions that help identify and block potentially malicious activities within application traffic. By focusing on Docker-related signatures, administrators can ensure that the security tools are finely tuned to the operational specifics of Docker containers, thereby providing a robust defense against exploits that target container-specific vulnerabilities.
References:The recommendation to use Docker-related application control signatures is based on best practices for securing container environments, emphasizing the need for specialized security measures that address the unique challenges posed by container technologies.

NEW QUESTION 22
A Network security administrator is searching for a solution to secure traffic going in and out of the container infrastructure.
In which two ways can Fortinet container security help secure container infrastructure?(Choose two.)

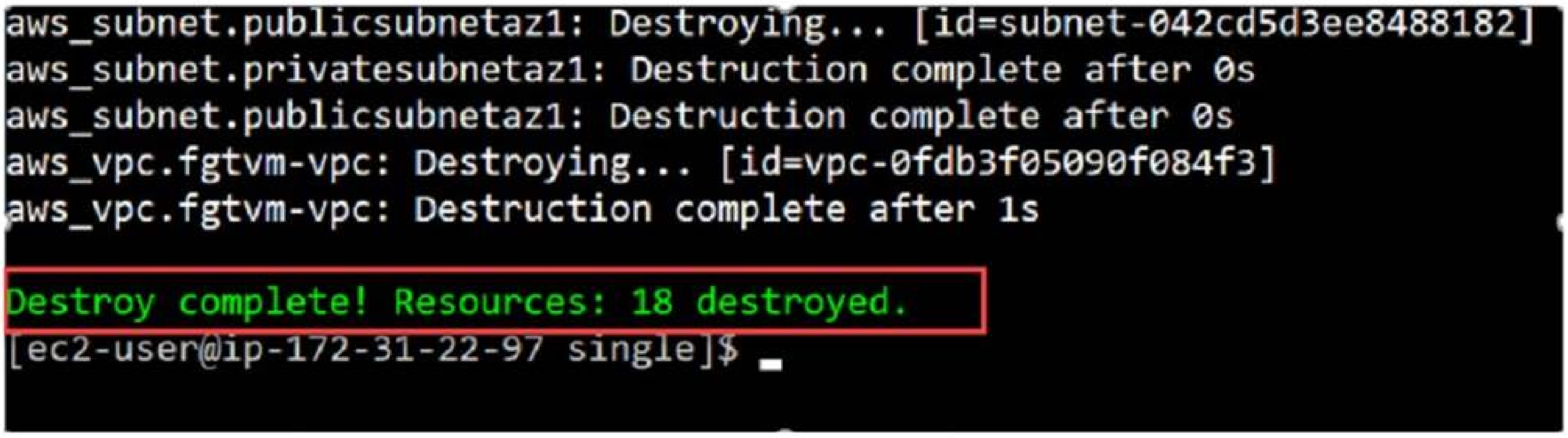
A. FortiGate NGFW can be placed between each application container for north-south traffic inspection
B. FortiGate NGFW can connect to the worker node and protects the container-
C. FortiGate NGFW can inspect north-south container traffic with label aware policies
D. FortiGate NGFW and FortiSandbox can be used to secure container traffic

Answer: CD

Explanation:

The correct answer is C and D. FortiGate NGFW can inspect north-south container traffic with label aware policies and FortiGate NGFW and FortiSandbox can be used to secure container traffic.
According to the Fortinet documentation for container security1, FortiGate NGFW can provide the following benefits for securing container infrastructure:
? It can inspect north-south traffic between containers and external networks using label aware policies, which allow for dynamic policy enforcement based on Kubernetes labels and metadata.
? It can integrate with FortiSandbox to provide advanced threat protection for
container traffic, by sending suspicious files or URLs to a cloud-based sandbox for analysis and detection.
? It can leverage FortiGuard Security Services to provide real-time threat intelligence
and updates for container traffic, such as antivirus, web filtering, IPS, and application control.
The other options are incorrect because:
? FortiGate NGFW cannot be placed between each application container for north- south traffic inspection, as this would create unnecessary complexity and overhead. Instead, FortiGate NGFW can be deployed at the edge of the container network or as a sidecar proxy to inspect traffic at the ingress and egress points.
? FortiGate NGFW cannot connect to the worker node and protect the container, as this would not provide sufficient visibility and control over the container traffic. Instead, FortiGate NGFW can leverage the native Kubernetes APIs and services to monitor and secure the container traffic.
1:Fortinet Documentation Library - Container Security

NEW QUESTION 24
Refer to the exhibit



```
aws_subnet.publicsubnetaz1: Destroying... [id=subnet-042cd5d3ee8488182]
aws_subnet.privatesubnetaz1: Destruction complete after 0s
aws_subnet.publicsubnetaz1: Destruction complete after 0s
aws_vpc.fgtvm-vpc: Destroying... [id=vpc-0fdb3f05090f084f3]
aws_vpc.fgtvm-vpc: Destruction complete after 1s

Destroy complete! Resources: 18 destroyed.
[ec2-user@ip-172-31-22-97 single]$ _
```

An administrator deployed a FortiGate-VM in a high availability (HA) (active/passive) architecture in Amazon Web Services (AWS) using Terraform for testing purposes. At the same time, the administrator deployed a single Linux server using AWS Marketplace
Which two options are available for the administrator to delete all the resources created in this test? (Choose two.)

A. Use the terraform destroy command
B. Use the terraform validate command.
C. Use the terraform destroy all command.
D. The administrator must manually delete the Linux server.

Answer: AD

Explanation:
A. Use the terraform destroy command. This command is used to remove all the resources that were created using the Terraform configuration1. It is the opposite of the terraform apply command, which is used to create resources. The terraform destroy command will first show a plan of what resources will be destroyed, and then ask for confirmation before proceeding. The command will also update the state file to reflect the changes. D. The administrator must manually delete the Linux server. This is because the Linux server was not deployed using Terraform, but using AWS Marketplace2. Therefore, Terraform does
not have any information about the Linux server in its state file, and cannot manage or destroy it. The administrator will have to use the AWS console or CLI to delete the Linux server manually.
The other options are incorrect because:
? There is no terraform validate command. The correct command is terraform plan,
which is used to show a plan of what changes will be made by applying the configuration3. However, this command does not delete any resources, it only shows what will happen if terraform apply or terraform destroy is run.
? There is no terraform destroy all command. The correct command is terraform
destroy, which will destroy all the resources in the current configuration by default1. There is no need to add an all argument to the command.

NEW QUESTION 26
......

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