Fortinet

Exam Questions NSE7_PBC-7.2

Fortinet NSE 7 - Public Cloud Security 7.2

NEW QUESTION 1
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 2
What are two main features in Amazon Web Services (AWS) network access control lists (ACLs)? (Choose two.)

A. You cannot use Network ACL and Security Group at the same time.
B. The default network ACL is configured to allow all traffic
C. NetworkACLs are stateless, and inbound and outbound rules are used for traffic filtering
D. Network ACLs are tied to an instance

Answer: BC

Explanation:
* B. The default network ACL is configured to allow all traffic. This means that when you create a VPC, AWS automatically creates a default network ACL for that VPC, and associates it with all the subnets in the VPC1. By default, the default network ACL allows all inbound and outbound IPv4 traffic and, if applicable, IPv6 traffic1. You can modify the default network ACL, but you cannot delete it1. C. Network ACLs are stateless, and inbound and outbound rules are used for traffic filtering. This means that network ACLs do not keep track of the traffic that they allow or deny, and they evaluate each packet separately1. Therefore, you need to create both inbound and outbound rules for each type of traffic that you want to allow or deny1. For example, if you want to allow SSH traffic from a specific IP address to your subnet, you need to create an inbound rule to allow TCP port 22 from that IP address, and an outbound rule to allow TCP port 1024-65535 (the ephemeral ports) to that IP address2.
The other options are incorrect because:
? You can use network ACL and security group at the same time. Network ACL and security group are two different types of security layers for your VPC that can work together to control traffic3. Network ACLacts as a firewall for your subnets, while security group acts as a firewall for your instances3. You can use both of them to create a more granular and effective security policy for your VPC.
? Network ACLs are not tied to an instance. Network ACLs are associated with subnets, not instances1. This means that network ACLs apply to all the instances in the subnets that they are associated with1. You cannot associate a network ACL with a specific instance. However, you can associate a security group with a specific instance or multiple instances3.

NEW QUESTION 3
A customer would like to use FortiGate fabric integration With FortiCNP
When configuring a FortiGate VM to add to FortiCNP, which three mandatory configuration steps must you follow on FortiGate? (Choose three.)

A. Enable send logs-
B. Create and IPS sensor and a firewall policy
C. Create an IPsec tunnel.
D. Create an SSL]SSH inspection profile.
E. Enable two-factor authentication.

Answer: ABD

Explanation:
To configure a FortiGate VM to add to FortiCNP, you need to perform three steps on FortiGate:
? Enable send logs in FortiGate to allow FortiCNP to receive the IPS logs from FortiGate.
? Create an SSL/SSH inspection profile on FortiGate to inspect the encrypted traffic and apply IPS protection.
? Create an IPS sensor and a firewall policy on FortiGate to enable IPS detection and prevention for the traffic.
References:
? FortiCNP 22.4.a Administration Guide, page 22-24
? FortiGate IPS Administration Guide, page 9-10

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
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
Which two Amazon Web Services (AWS) features do you use for the transit virtual private cloud (VPC) automation process to add new spoke N/PCs? (Choose two)

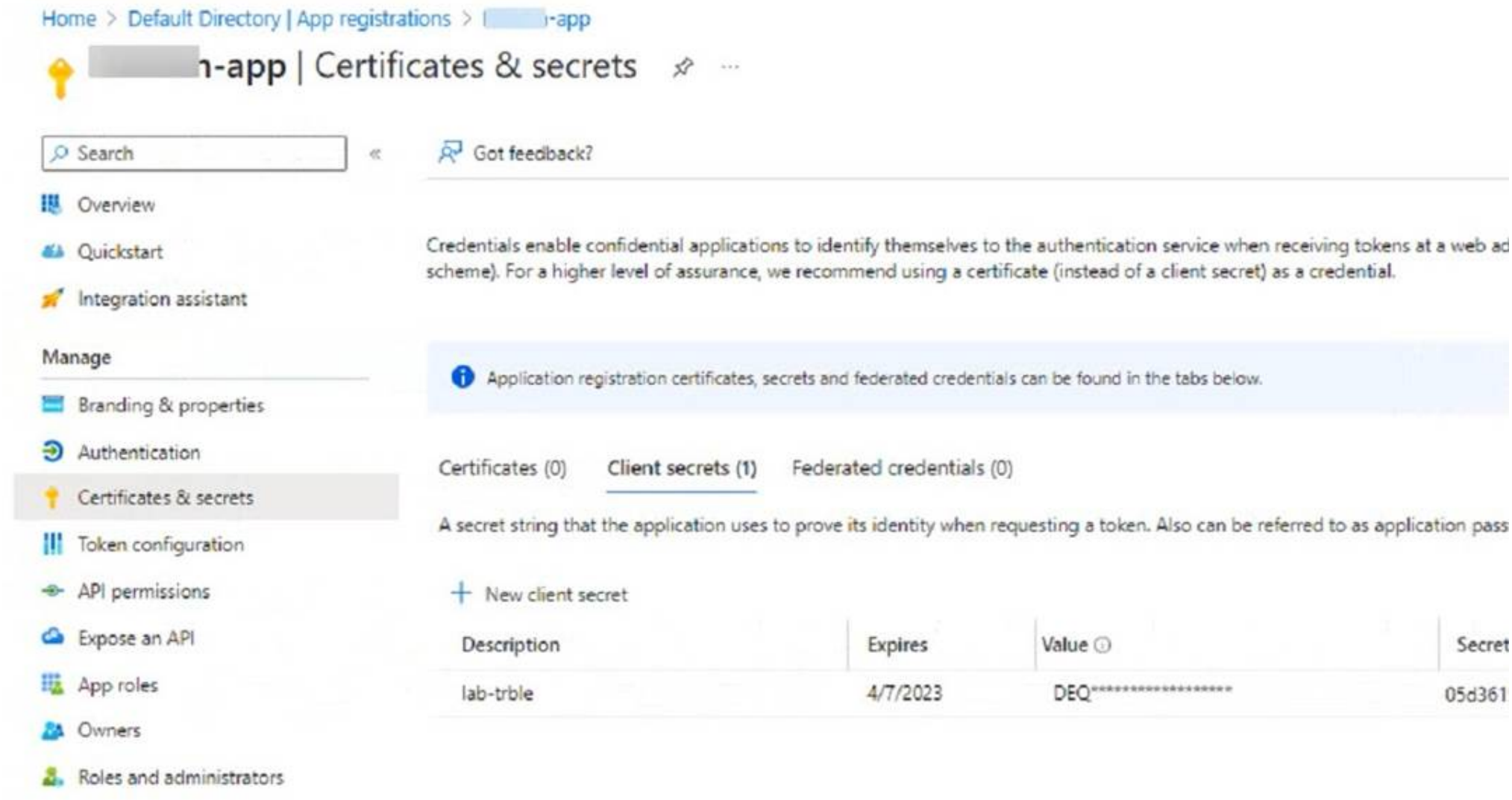
A. Amazon S3 bucket
B. AWS Security Hub
C. AWS Transit Gateway
D. Amazon CloudWatch

Answer: CD

Explanation:
For automating the process of adding new spoke VPCs in a transit VPC architecture within Amazon Web Services (AWS), the two relevant features are:
? AWS Transit Gateway (Option C):This service is crucial for managing connectivity between VPCs and other networks without routing traffic through the public internet. It acts as a hub that controls how traffic is routed among all the connected networks, which simplifies network management and minimizes latency.
? Amazon CloudWatch (Option D):CloudWatch provides monitoring and observability services that are essential for managing the health and performance of the AWS infrastructure, including Transit Gateways. It allows administrators to set alarms and react to changes in AWS resources, which is vital for the dynamic addition and integration of new spoke VPCs into the transit VPC architecture.
References:AWS official documentation on Transit Gateways and CloudWatch details these services' roles in enhancing network management and monitoring, essential for effective and automated transit VPC operations.

NEW QUESTION 7

Refer to the exhibit



An administrator is trying to deploy a FortiGate VM in Microsoft Azure using Terraform However, during the configuration, the Azure client secret is no longer visible in the Azure portal.
How would the administrator obtain the Azure client secret to configure on Terratorm?

A. The administrator must create a new Azure account
B. Log in to the Azure CLI with power user to obtain the client secret
C. The administrator can create a new client secret
D. The administrator must obtain the client secret through Azure Cloud Shell.

Answer: C

Explanation:
The Azure client secret is a one-time value that is only visible when it is created. If the administrator loses or forgets the client secret, they cannot retrieve it from the Azure portal. However, they can create a new client secret and use it to configure Terraform. To create a new client secret, they need to follow these steps12:
? Sign in to the Azure portal and navigate to the Azure Active Directory service.
? Select the application name under the App Registrations.
? Select Certificates & Secrets > New client secret to create a new client secret.
? Add a description and an expiration date for the client secret and select Add.
? Copy the value of the new client secret immediately as it will not be shown again. References:
? Generate new Client Secret and link to key-vault | Microsoft Learn
? Azure Quickstart - Set and retrieve a secret from Key Vault using Azure portal | Microsoft Learn

NEW QUESTION 8
You are adding a new spoke to the existing transit VPC environment using the AWS Cloud Formation template. Which two components must you use for this deployment? (Choose two.)

A. The OSPF AS value used for the hub.
B. The Amazon CloudWatch tag value.
C. The BGPASN value used for the transit VPC.
D. The tag value of the spoke

Answer: CD

Explanation:
When using an AWS CloudFormation template to add a new spoke to an existing transit VPC environment, the necessary components are:
? The BGPASN value used for the transit VPC (Option C):BGP Autonomous System Number (ASN) is required for setting up BGP routing between the transit VPC and the new spoke. This number uniquely identifies the system in BGP routing and is crucial for correct routing and avoiding routing conflicts.
? The tag value of the spoke (Option D):Tags in AWS are used to identify and manage resources. The tag value assigned to a spoke VPC helps in organizing, managing, and locating the VPC within the larger AWS environment. Tags are essential for automation scripts and policies that depend on specific identifiers to apply configurations or rules.
References:AWS CloudFormation and AWS Transit Gateway documentation provide guidance on the use of BGPASN and tags for managing and automating VPC deployments effectively.

NEW QUESTION 9
Which statement about Transit Gateway (TGW) in Amazon Web Services (AWS) is true?

A. TGW can have multiple TGW route tables.
B. Both the TGW attachment and propagation must be in the same TGW route table

C. A TGW attachment can be associated with multiple TGW route tables.
D. The TGW default route table cannot be disabled.

Answer: A

Explanation:
According to the AWS documentation for Transit Gateway, a transit gateway is a network transit hub that connects VPCs and on-premises networks. A transit gateway route table is a set of rules that determines how traffic is routed among the attachments to the transit gateway1.
A transit gateway can have multiple route tables, and you can associate different attachments with different route tables. This allows you to control how traffic is routed between your VPCs and VPNs based on your network design and security requirements1. The other options are incorrect because:
? Both the TGW attachment and propagation must be in the same TGW route table
is not true. You can associate an attachment with one route table and enable propagation from another attachment to a different route table. This allows you to separate the routing domains for your attachments1.
? A TGW attachment can be associated with multiple TGW route tables is not true.
You can only associate an attachment with one route table at a time. However, you can change the association at any time1.
? The TGW default route table cannot be disabled is not true. You can disable the
default route table by deleting all associations and propagations from it. However, you cannot delete the default route table itself1.
1: Transit Gateways - Amazon Virtual Private Cloud

NEW QUESTION 10
Refer to the exhibit.

```
Azure-HA-Passive # diagnose debug application azd -1
Debug messages will be on for 30 minutes.
Azure-HA-Passive # diagnose debug enable
FGT-HA-Slave # azd running in secondary mode, will notupdate
HA event
HA state: primary
azd sdn connector 'AZ-Connector' getting token
size: 1268
token expire in: 3600 seconds
AZ-Connector: resourcegroup: NSE7-HA-RG, sub: "<Removed string>"
Disable interface: port1
Disable interface: port2
get pubip FGTAPClusterPublicIP in resource group NSE7-HA-RG
azd api failed, url
=https://management.azure.com/subscriptions/<Removed String>/resourceGroups/NSE7-HA-
RG/providers/Microsoft.Network/publicIPAddres
ses/FGTAPClusterPublicIP?api-version=2022-06-01, rc = 403,
{"error":{"code":"AuthorizationFailed","message":"The client '<Removed String>' with ob
ect id '<Removed String>' does not have authorization to perform action
'Microsoft.Network/publicIPAddresses/read' over scope '/subscriptions/<Removed
String>/resourceGroups/NSE7-HA-
RG/providers/Microsoft.Network/publicIPAddresses/FGTAPClusterPublicIP' or the scope is
invalid. If access was recen
tly granted, please refresh your credentials."}}
```

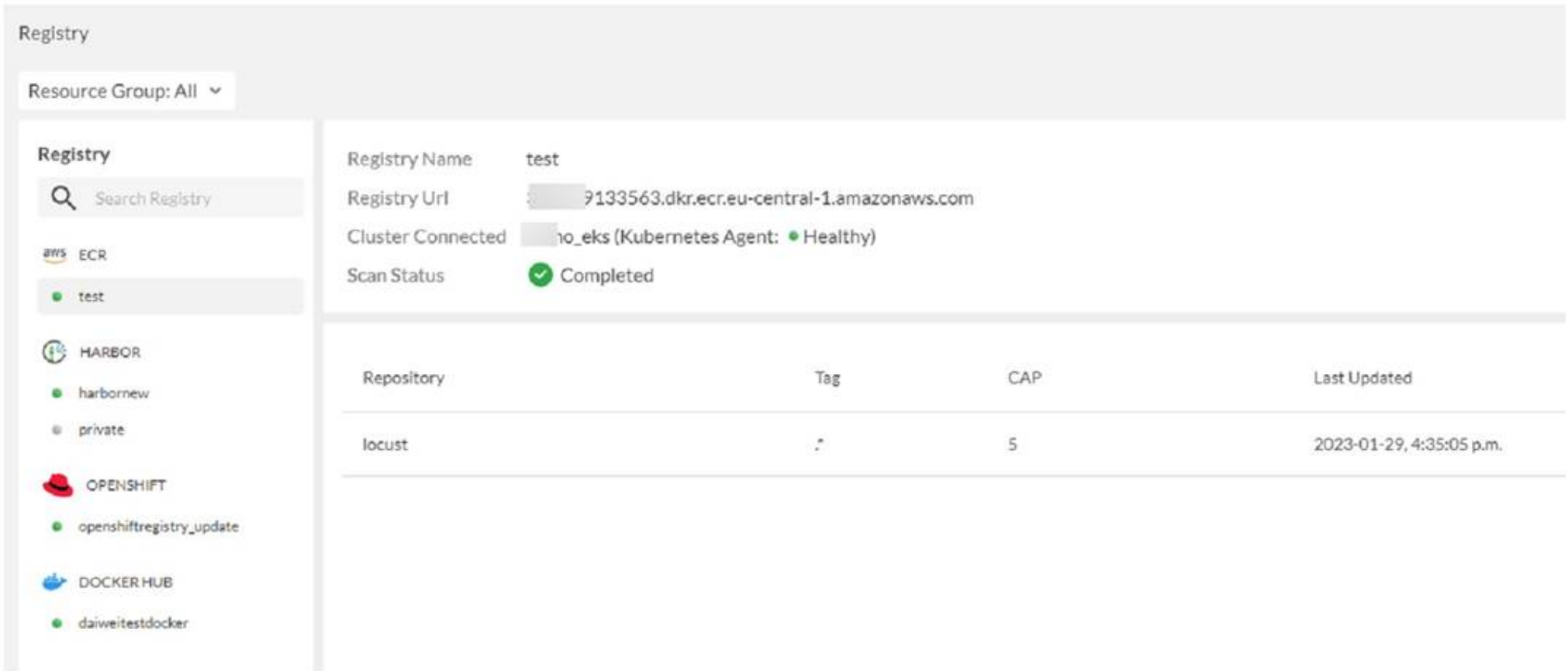
You are troubleshooting a FortiGate HA floating IP issue with Microsoft Azure. After the failover, the new primary device does not have the previous primary device floating IP address.

A. FortiGate port4 does not have internet access.
B. A wrong client secret credential is used
C. The error is caused by credential time expiration.
D. The Azure service principle account must have a contributor role.

Answer: D

Explanation:
In this scenario, the issue is caused by the Azure service principle account nothaving a contributor role. This is required for the FortiGate HA floating IP to work properly. Without this role, the new primary device will not have the previous primary device floating IP address after failover. References: Fortinet Public Cloud Security knowledge source documents or study guide.
https://docs.fortinet.com/product/fortigate-public-cloud/7.2

NEW QUESTION 10
Refer to the exhibit



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 13
Refer to the exhibit.

Variables

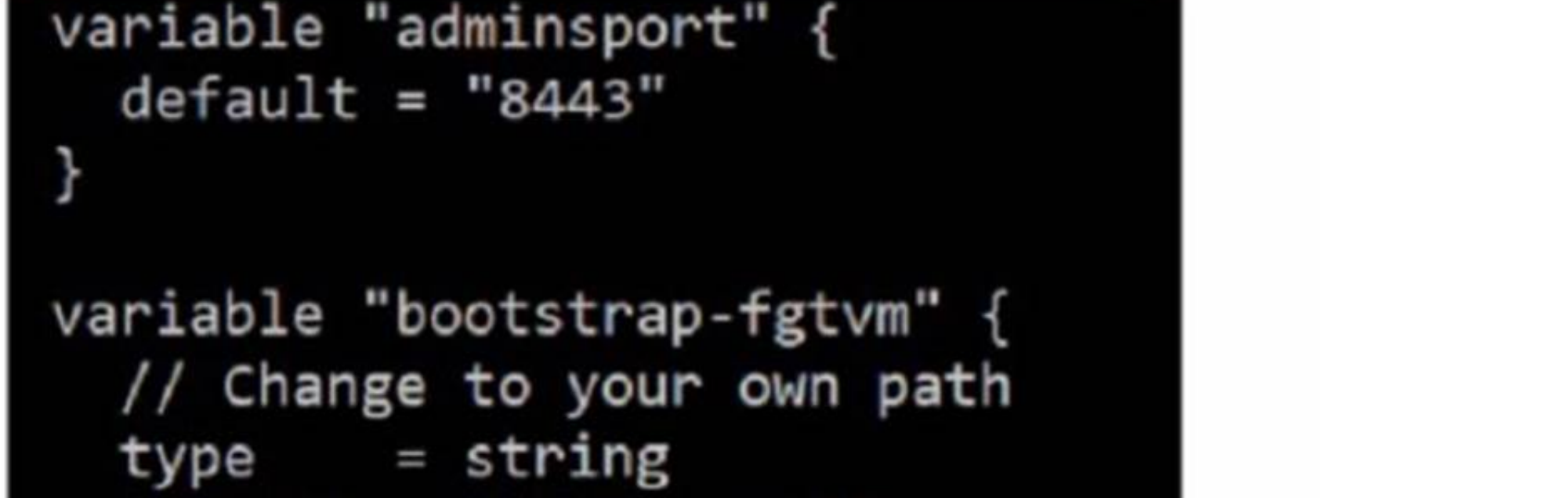
```
variable "size" {
  default = "c5n.xlarge"
}

//  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



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.

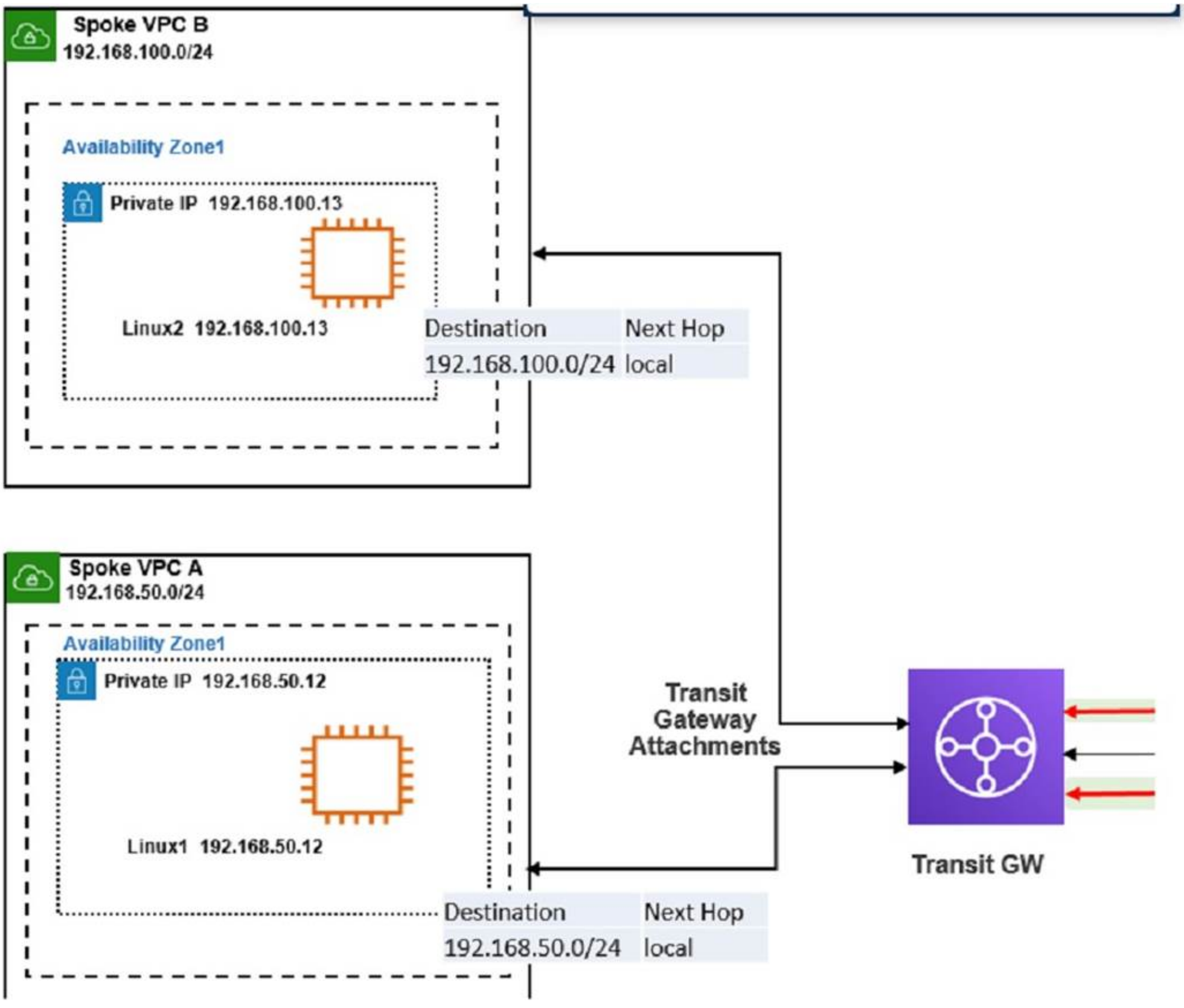
NEW QUESTION 14
In an SD-WAN TGW Connect topology, which three initial steps are mandatory when routing traffic from a spoke VPC to a security VPC through a Transit Gateway? (Choose three.)

A. From the spoke VPC internal routing table, point 0.0.0.0/0 traffic to the TGW
B. From the security VPC TGW subnet routing table: point 0.0.0.0/0 traffic to theFortiGate internal port
C. From the security VPC TGW subnet routing table: point 0.0.0.0/0 traffic to the TGW
D. From the security VPC FortiGate internal subnet routing table, point 0.0.0.0/0 traffic to the TGW
E. From both spoke VPCs and the security VPC, point 0.0.0.0/0 traffic to the Internet Gateway

Answer: ABD

Explanation:
? Spoke VPC Routing: The 0.0.0.0/0 (default) route in the spoke VPC must point to the Transit Gateway attachment for traffic to reach other VPCs or external destinations.
? Security VPC Routing: Traffic from the security VPC needs to pass through the FortiGate for inspection and security controls. Therefore, the 0.0.0.0/0 route in the security VPC's TGW subnet routing table must point to the FortiGate's internal port.
? FortiGate Routing: The FortiGate's internal subnet must have its 0.0.0.0/0 route
configured to point to the Transit Gateway attachment, allowing traffic to be returned to other VPCs or reach the internet.
In an SD-WAN TGW Connect topology, when routing traffic from a spoke VPC to a security VPC through a Transit Gateway, the mandatory initial steps include:
? From the spoke VPC internal routing table, point 0.0.0.0/0 traffic to the TGW
(Option A):This step is crucial for ensuring that all traffic from the spoke VPC destined for external networks is directed through the Transit Gateway, allowing for centralized management and security inspection.
? From the security VPC TGW subnet routing table: point 0.0.0.0/0 traffic to the
FortiGate internal port (Option B):Routing all traffic from the TGW subnet in the security VPC to the FortiGate's internal port ensures that traffic is subjected to the necessary security policies and inspections provided by the FortiGate appliance before it proceeds to other destinations or returns to the spoke VPCs.
? From the security VPC FortiGate internal subnet routing table, point 0.0.0.0/0
traffic to the TGW (Option D):This configuration ensures that traffic returning from the security processes handled by the FortiGate is routed back through the Transit Gateway, maintaining the integrity of the secure transit path and ensuring proper routing back to the originating spoke or onward to the internet.
References:These steps align with best practices for implementing SD-WAN solutions in a cloud environment, ensuring that all traffic is appropriately routed through security appliances for necessary controls and monitoring, asdetailed in the Fortinet SD-WAN documentation and AWS Transit Gateway connectivity guidelines.

NEW QUESTION 18
Refer to the exhibit



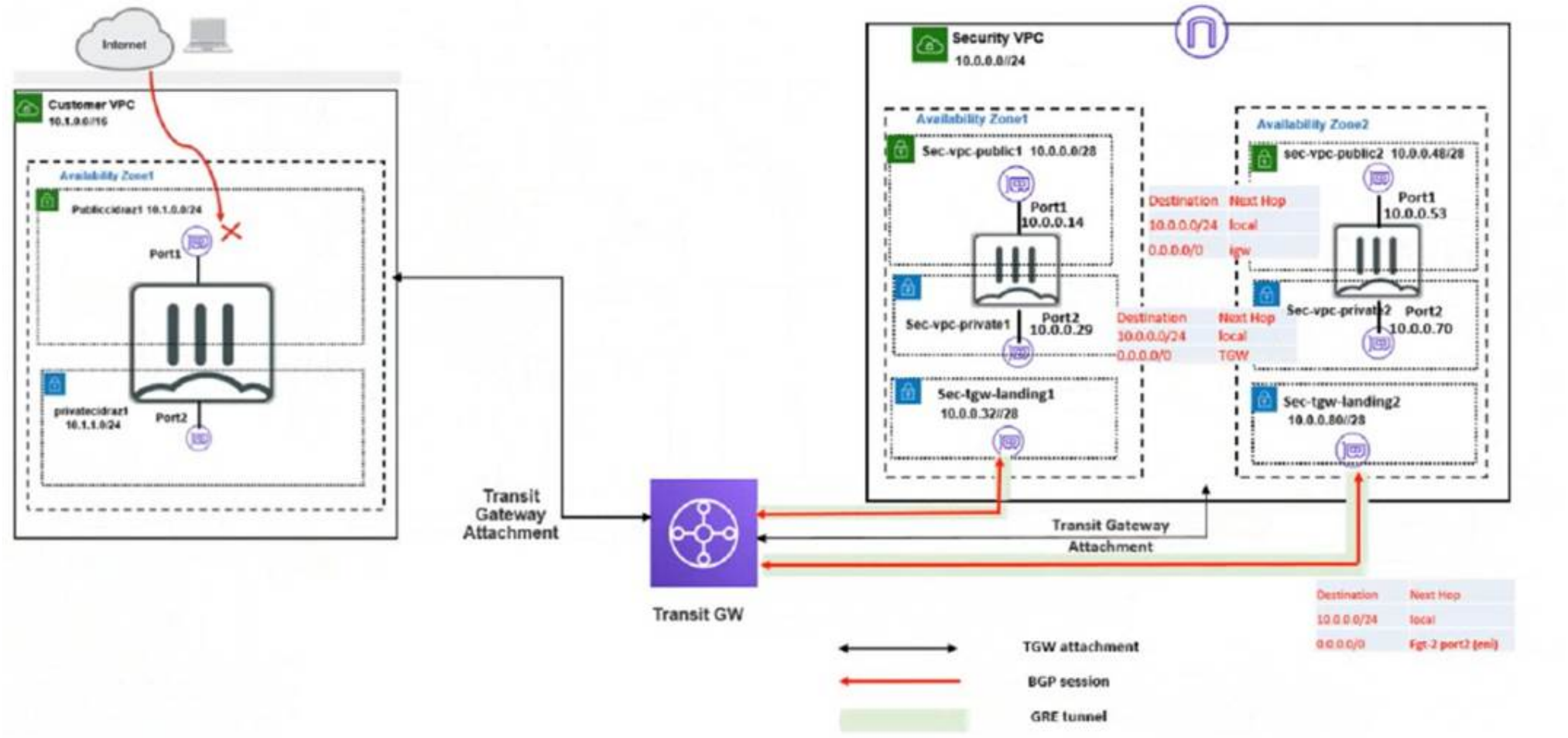
The exhibit shows a customer deployment of two Linux instances and their main routing table in Amazon Web Services (AWS). The customer also created a Transit Gateway (TGW) and two attachments
Which two steps are required to route traffic from Linux instances to the TGWQ (Choose two.)

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 23
Refer to the exhibit



In your Amazon Web Services (AWS), you must allow inbound HTTPS access to the Customer VPC FortiGate VM from the internet However, your HTTPS connection to the FortiGate VM in the Customer VPC is not successful.
Also, you must ensure that the Customer VPC FortiGate VM sends all the outbound Internet traffic through the Security VPC How do you correct this Issue with minimal configuration changes?
(Choose three.)

A. Add a route With your local internet public IP address as thedestination and target transit gateway
B. Add route destination 0 0.0 0/0 to target the transit gateway
C. Add a route With your local internet public IP address as the destination and target internet gateway
D. Deploy an internet gateway, associate an EIP in the private subnet, edit route tables, and add a new route destination0.0.0.0/0 to the target internet gateway
E. Deploy an internet gateway, associate an EIP in the public subnet, and attach the internet gateway to the Customer VPC,

Answer: BDE

Explanation:
* B. Add route destination 0.0.0.0/0 to target the transit gateway. This will ensure that the Customer VPC FortiGate VM sends all the outbound internet traffic through the Security VPC, where it can be inspected by the Security VPC FortiGate VMs1. The transit gateway is a network device that connects multiple VPCs and on-premises networks in a hub-and-spoke model2. D. Deploy an internet gateway, associate an EIP in the private subnet, edit route tables, and add a new route destination 0.0.0.0/0 to the target internet gateway. This will allow inbound HTTPS access to the Customer VPC FortiGate VM from the internet, by creating a public route for the private subnet where the FortiGate VM is located3. An internet gateway is a service that enables communication between your VPC and the internet4. An EIP is a public IPv4 address that you can allocate to your AWS account and associate with your resources. E. Deploy an internet gateway, associate an EIP in the public subnet, and attach the internet gateway to the Customer VPC. This will also allow inbound HTTPS access to the Customer VPC FortiGate VM from the internet, by creating a public route for the public subnet where the FortiGate VM is located3. This is an alternative solution to option D, depending on which subnet you want to use for the FortiGate VM.
The other options are incorrect because:
? Adding a route with your local internet public IP address as the destination and target transit gateway will not allow inbound HTTPS access to the Customer VPC FortiGate VM from the internet, because it will only apply to traffic coming from your specific IP address, not from any other source on the internet1. Moreover, it will not ensure that the outbound internet traffic goes through the Security VPC, because it will only apply to traffic going to your specific IP address, not to any other destination on the internet1.
? Adding a route with your local internet public IP address as the destination and target internet gateway will not allow inbound HTTPS access to the Customer VPC FortiGate VM from the internet, because it will bypass the Security VPC and send the traffic directly to the Customer VPC1. Moreover, it will not ensure that the outbound internet traffic goes through the Security VPC, because it will only apply to traffic going to your specific IP address, not to any other destination on the internet1.

NEW QUESTION 28
You are using Red Hat Ansible to change the FortiGate VM configuration.
What is the minimum number of files you must create and which file must you use to configure the target FortiGate IP address?

A. Create two files and use the .yami file.
B. Create two files and use the hosts file
C. Create one file and use the variable file
D. Create three files and use the .yarai file.

Answer: B

Explanation:
In using Red Hat Ansible for changing the configuration of a FortiGate VM, the minimum number of files you must create and the file to configure the target FortiGate IP address are:
* B.Create two files and use the hosts file.
? Ansible Playbook File (YAML):The playbook file, which is typically a YAML file, contains the desired states and tasks that Ansible will execute on the target hosts.
? Inventory File (Hosts):The inventory file, commonly namedhosts, is where you define the target machines, including the FortiGate VM's IP address. Ansible uses this file to determine on which machines to run the playbook.
By creating these two files, you will have the necessary components to configure Ansible for the deployment. The playbook contains the automation tasks, and the

hosts file lists the machines where those tasks will be executed.
References:This structure is specified in the Ansible documentation, which details the use of playbooks and inventory files to manage and configure target systems.

NEW QUESTION 29
When adding the Amazon Web Services (AWS) account to the FortiCNP, which three mandatory configuration steps must you follow? (Choose three.)

A. Add AWS accounts through FortiCNP.
B. Enable cloud protection through AWS Guard Duty and AWS Inspector
C. Accept FortiCNP to create CloudTrail for the account
D. Enable cross-reg Ion aggregation
E. Launch the CloudFormation template.

Answer: ACE

Explanation:
When adding the Amazon Web Services (AWS) account to the FortiCNP, you must follow these three mandatory configuration steps:
? Add AWS accounts through FortiCNP. This is the first step to enable cloud protection for your AWS account. You can add one or multiple accounts automatically or manually. You need to provide the AWS account ID and a name for the account. You also need to select the optional permissions to be granted to FortiCNP as needed1.
? Accept FortiCNP to create CloudTrail for the account. This is required for FortiCNP to collect and analyze the AWS API calls and events. You can choose to let FortiCNP create a CloudTrail for the account or use an existing one. You also need to specify the aggregation region for the CloudTrail1.
? Launch the CloudFormation template. This is required for FortiCNP to create a stack and a role in your AWS account. The stack contains the resources that FortiCNP needs to access and monitor your AWS account. The role allows FortiCNP to assume it and perform actions on your behalf. You need to enter a custom or default role name and a unique UUID that is designated for your company on FortiCNP1.
References: Add AWS Account Automatically https://docs.fortinet.com/document/forticnp/22.4.a/online-help/246021/add-aws-account- automatically

NEW QUESTION 32
Refer to the exhibit.

```
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
    set session-pickup-nat enable
    set session-pickup-expectation enable
    set override disable
end

config system standalone-cluster
    edit 0
        set peerip 10.0.1.x
        set syncvd "root"
    next
end
```

You deployed an HA active-active load balance sandwich with two FortiGate VMs in Microsoft Azure.
After the deployment, you prefer to use FGSP to synchronize sessions, and allowasymmetric return traffic In the environment, FortiGate port 1 and port 2 are facing external and internal load balancers respectively
What IP address must you use in the peerip configuration?

A. The opposite FortiGate port 1 IP address.
B. The public load balancer port 2 IP address
C. The internal load balancer port 1 IP address.
D. The opposite FortiGate port 2 IP address.

Answer: D

Explanation:
In an HA active-active load balance configuration with FortiGate VMs, especially in Microsoft Azure where FGSP (FortiGate Session Life Support Protocol) is used for session synchronization, the correct configuration for thepeeripis: D.The opposite FortiGate port 2 IP address.

? HA Synchronization Requirements:FGSP requires direct communication between the FortiGates to synchronize the session table. This synchronization typically occurs over a dedicated HA link that connects the HA pair.
? Asymmetric Traffic Considerations:FGSP allows asymmetric traffic to rejoin the correct session by synchronizing session information, including NAT and TCP sequence tracking between the FortiGate units in a cluster.
? Configuration Specifics:For port 2, which is facing the internal load balancer, thepeeripshould be set to the corresponding port 2 IP address of the opposite FortiGate. This allows the internal interfaces to communicate directly with each other for session synchronization purposes, which is crucial in an active-active deployment to ensure sessions persist during failover scenarios. References:The choice of using port 2's IP address for FGSP is supported by the Fortinet documentation, which explains how FortiGates should be configured for HA, especially in cloud environments where traditional HA links may not be available.

NEW QUESTION 33
What is the main advantage of using SD-WAN Transit Gateway Connect over traditional SD-WAN?

A. It eliminates the use of ECMP
B. You can use GRE-based tunnel attachments
C. You can combine it with IPsec to achieve higher bandwidth
D. You can use BGP over IPsec for maximum throughput

Answer: B

Explanation:
? Simplified and Scalable Connectivity: Transit Gateway Connect allows you to establish GRE tunnels to your SD-WAN appliances natively within the AWS network. This eliminates the complexity of managing individual IPsec VPN connections, especially as your cloud presence grows.
? Potential for Enhanced Performance: GRE offers lower overhead compared to IPsec, which can result in higher throughput for bandwidth-intensive SD-WAN applications.
? Flexibility: While IPsec is supported for scenarios requiring strong encryption, the focus on GRE highlights the performance and scalability benefits that are often prioritized when integrating SD-WAN with AWS.
? Dynamic Routing: The integration with BGP further streamlines network management by automating route updates and distribution.
Addressing the IPsec Consideration:
It's important to acknowledge that SD-WAN Transit Gateway Connect does support IPsec. If your question is specifically framed within the context of Fortinet's FCSS 7.2 materials and they emphasize the hybrid usage of GRE and IPsec, then a modified answer might be appropriate:

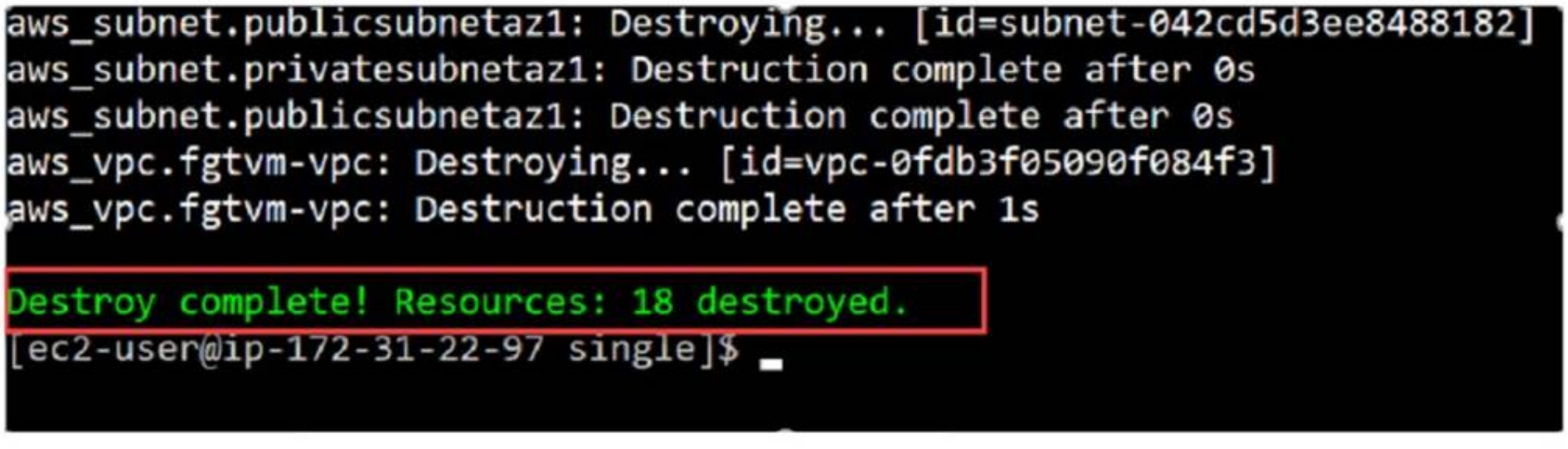
NEW QUESTION 38
A Network security administrator is searching for a solution to secure traffic going in and out of the container infrastructure.
In which two ways can Fortinet container security help secure container infrastructure?(Choose two.)

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 42
Refer to the exhibit



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 46
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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