Fortinet

Exam Questions NSE7_PBC-7.2

Fortinet NSE 7 - Public Cloud Security 7.2

NEW QUESTION 1
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 2
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.

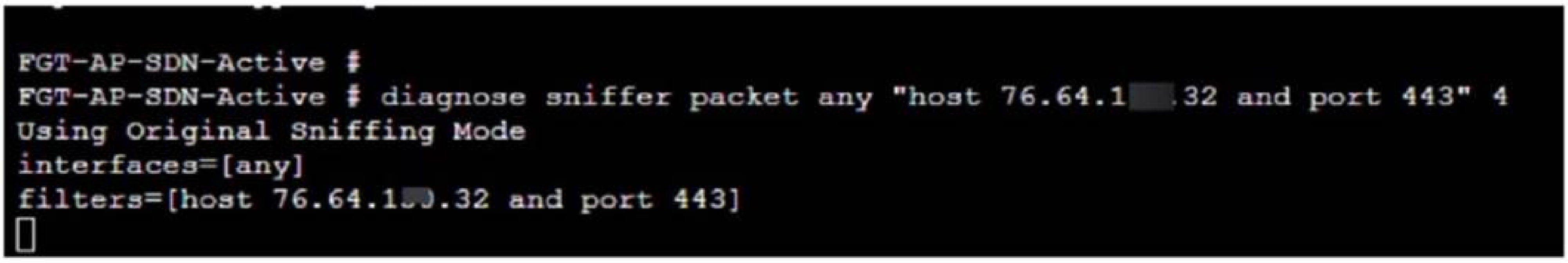
NEW QUESTION 3
You are adding a new spoke to the existing transit VPC environment using the AWS Cloud Formation template. Which two components must you use for this deployment? (Choose two.)

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 4
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]
```

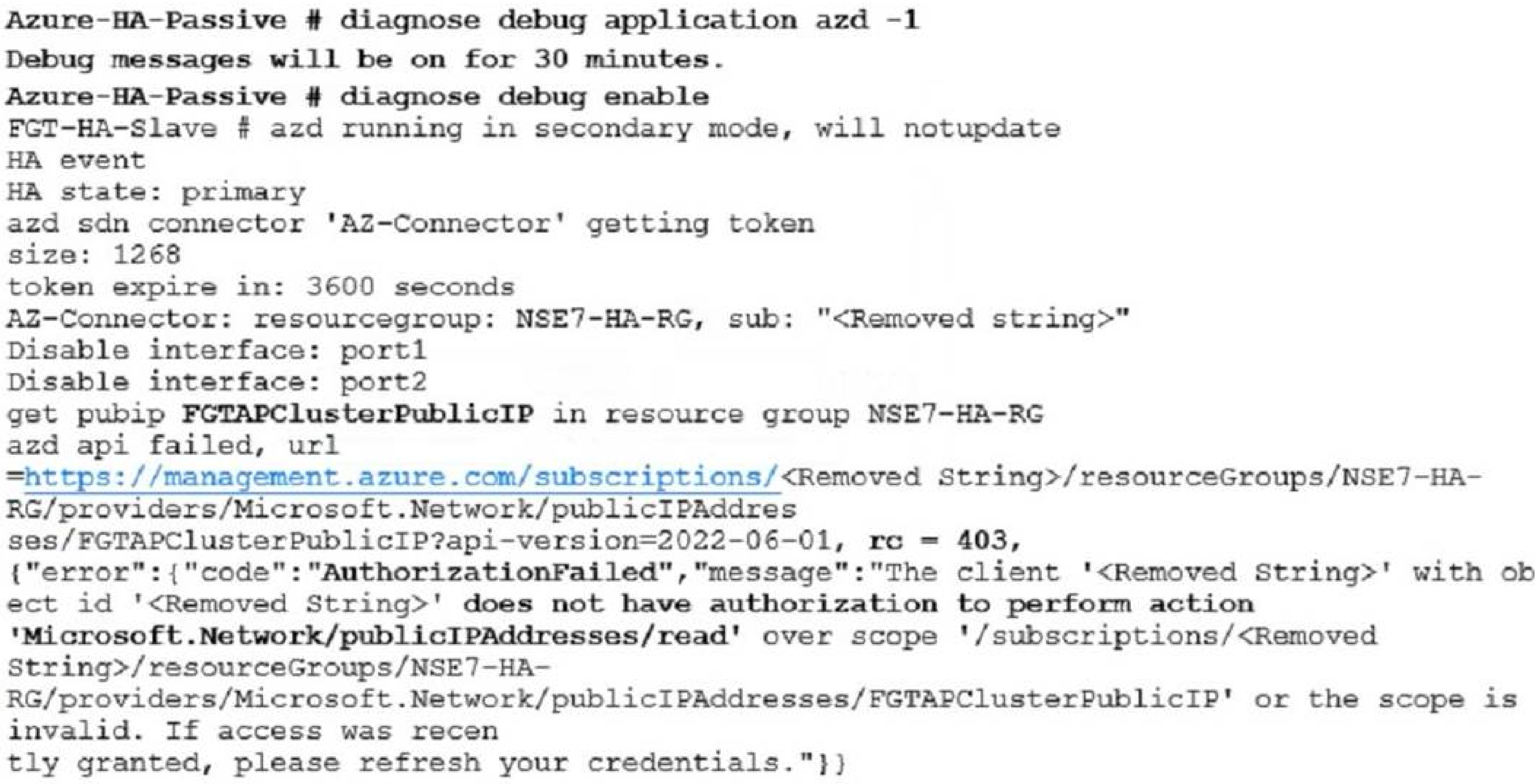
An administrator has deployed a FortiGate VM in Amazon Web Services (AWS) and is trying to access it using its public IP address from their local computer However, the connection is not successful and at the same time FortiGate is not receiving any HTTPS or SSH traffic to its external interface
What 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 5
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."}}
```

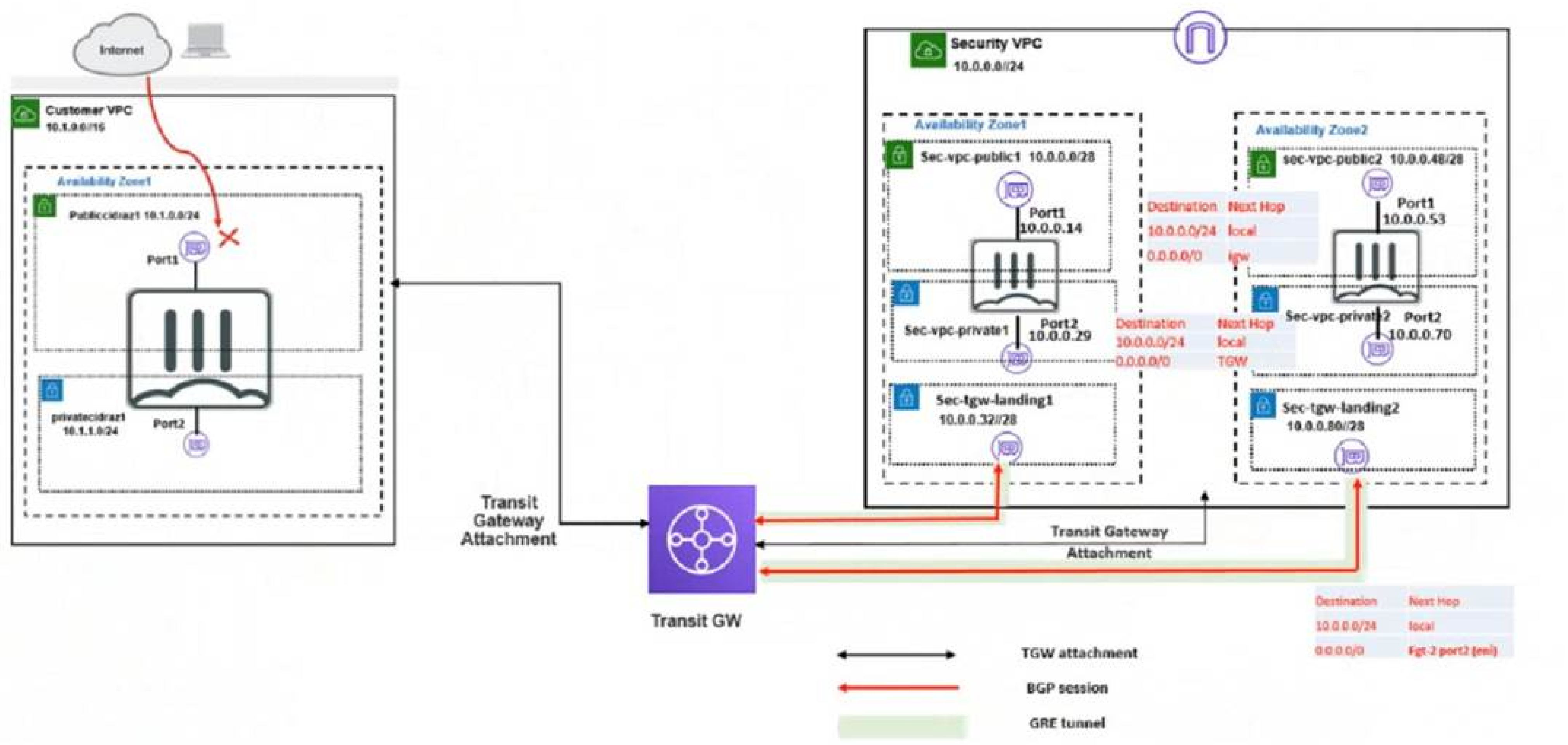
You are troubleshooting a FortiGate HA floating IP issue with Microsoft Azure. After the failover, the new primary device does not have the previous primary device floating IP address.

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 6
Refer to the exhibit



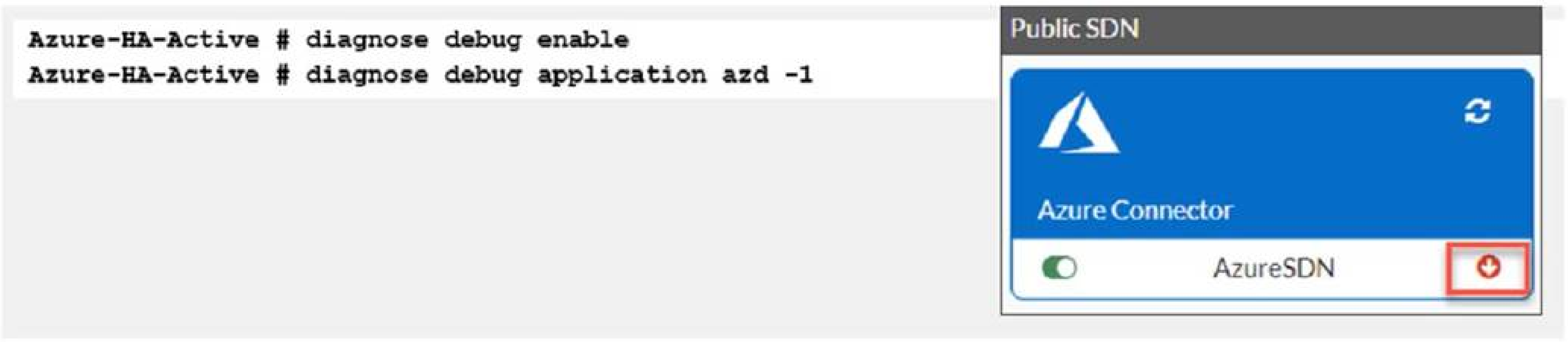
In your Amazon Web Services (AWS), you must allow inbound HTTPS access to the Customer VPC FortiGate VM from the internet However, your HTTPS connection to the FortiGate VM in the Customer VPC is not successful.
Also, you must ensure that the Customer VPC FortiGate VM sends all the outbound Internet 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 7
Refer to Exhibit:



```
Azure-HA-Active # diagnose debug enable
Azure-HA-Active # diagnose debug application azd -1
```

You are troubleshooting a Microsoft Azure SDN connector issue on your FortiGate VM in Azure

Which three settings should you check while troubleshooting this problem? (Choose three.)

A. Use the show vdom command to see hidden VDOMs.
B. use the diag sys va command.
C. Ensure FortiGate port4 can resolve DNS.
D. Ensure FortiGate portl has internet access
E. Ensure IP address 169.254.169_254 is not blocked

Answer: CDE

Explanation:
The three settings that should be checked while troubleshooting this problem are:
? Ensure FortiGate port4 can resolve DNS. This is because the Azure SDN connector requires DNS resolution to communicate with the Azure API1. If the FortiGate port4 cannot resolve DNS, the SDN connector will not be able to retrieve the Azure resources and display them in the GUI.
? Ensure FortiGate portl has internet access. This is because the Azure SDN connector requires internet access to communicate with the Azure API1. If the FortiGate portl does not have internet access, the SDNconnector will not be able to connect to the Azure cloud and display an error in the CLI.
? Ensure IP address 169.254.169_254 is not blocked. This is because the Azure SDN connector uses this IP address to obtain metadata information from the Azure instance2. If this IP address is blocked by a firewall policy or a network ACL, the SDN connector will not be able to get the required information and display an error in the CLI.

NEW QUESTION 8
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 9
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 10
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.)

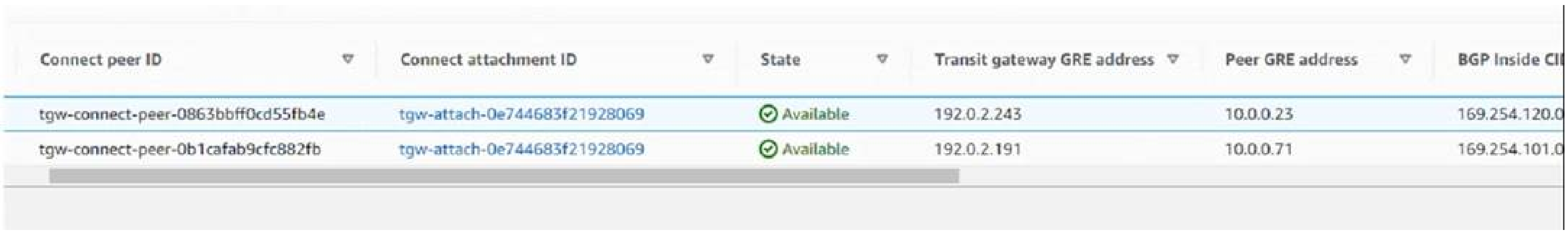
A. Use ECMP and VPN to achieve higher bandwidth.
B. Use transit VPC to build multiple VPC connections to the on-premises data center
C. Use a transit VPC with hub and spoke topology to create multiple VPN connections to the on-premises data center.
D. Use the transit gateway attachment With VPN option 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 10
Refer to Exhibit:



Connect peer ID	Connect attachment ID	State	Transit gateway GRE address	Peer GRE address	BGP Inside CI
tgw-connect-peer-0863bbff0cd55fb4e	tgw-attach-0e744683f21928069	✓ Available	192.0.2.243	10.0.0.23	169.254.120.0
tgw-connect-peer-0b1cafab9cfc882fb	tgw-attach-0e744683f21928069	✓ Available	192.0.2.191	10.0.0.71	169.254.101.0

The exhibit shows the Connect Peers settings on Amazon Web Services (AWS) transit gateway attachments With two FortiGate VMS in a security VPC.
Which two statements are correct? (Choose two.)

A. The peer GRE address is the FortiGate external interface IP address.
B. The Transit Gateway GRE address is auto-generated
C. The BGP inside CIDR blocks can be any CIDR block with /29
D. The Peer GRE address is the FortiGate internal interface IP address

Answer: AB

Explanation:
* A. The peer GRE address is the FortiGate external interface IP address. This is the IP address of the FortiGate interface that is connected to the transit gateway attachment subnet1. This IP address is used to establish the GRE tunnel between the FortiGate and the transit gateway2. B. The Transit Gateway GRE address is auto-generated. This is the IP address of the transit gateway that is used to establish the GRE tunnel with the FortiGate2. This IP address is automatically assigned by AWS from the Transit Gateway CIDR range that you specify when you create the Connect attachment3.
The other options are incorrect because:
? The BGP inside CIDR blocks cannot be any CIDR block with /29. They must be a /29 CIDR block from the 169.254.0.0/16 range for IPv4, or a /125 CIDR block from the fd00::/8 range for IPv64. These are the inside IP addresses that are used for BGP peering over the GRE tunnel4.
? The Peer GRE address is not the FortiGate internal interface IP address. The internal interface IP address is used to route traffic from the FortiGate to the VPC subnet where the third-party appliance (such as SD-WAN) is located1. The Peer GRE address is used to route traffic from the FortiGate to the transit gateway over the GRE tunnel2.

NEW QUESTION 12
......