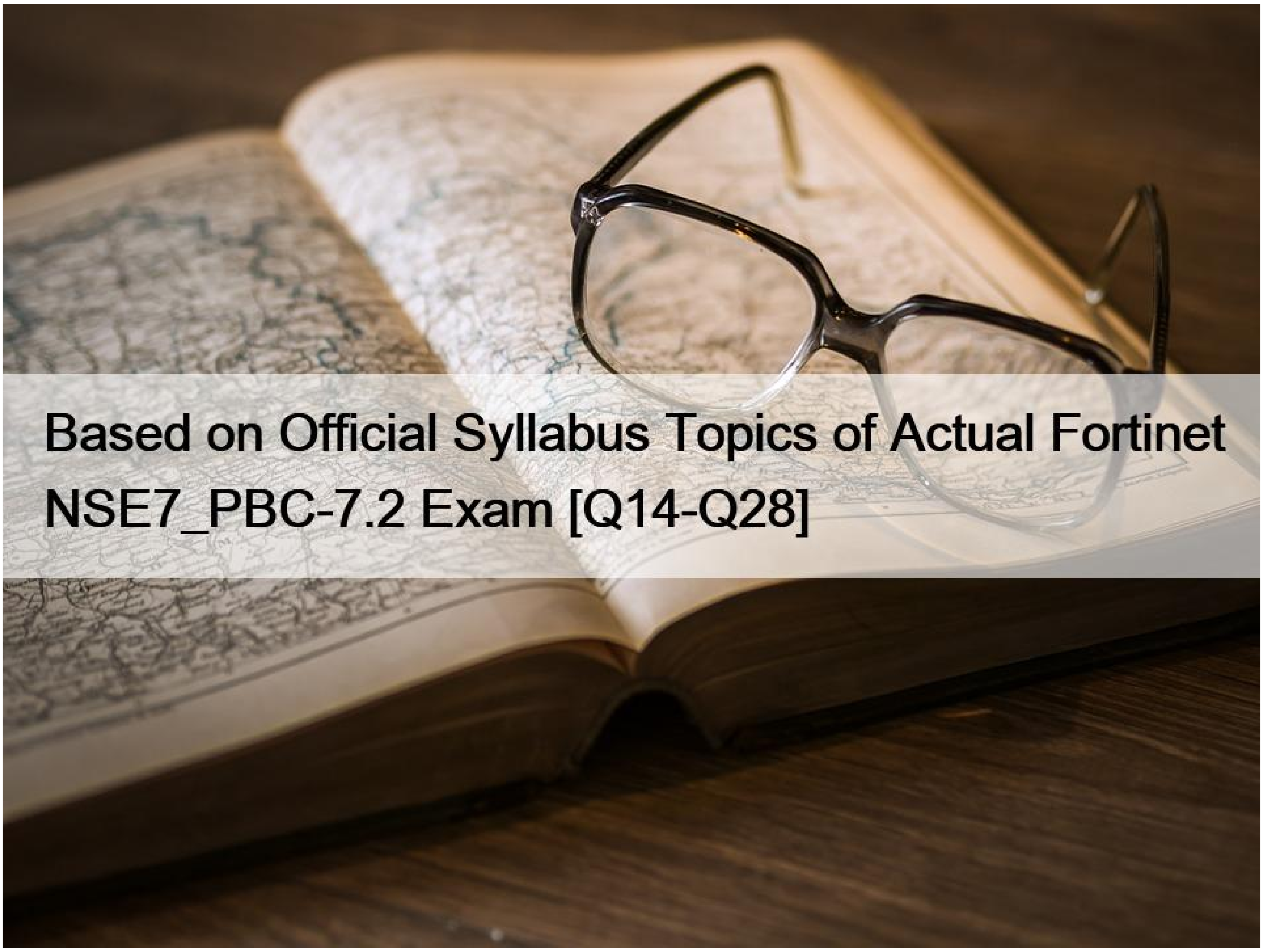
Based on Official Syllabus Topics of Actual Fortinet NSE7_PBC-7.2 Exam [Q14-Q28



Based on Official Syllabus Topics of Actual Fortinet NSE7_PBC-7.2 Exam Free NSE7_PBC-7.2 Dumps are Available for Instant Access

Fortinet NSE7_PBC-7.2 certification exam is designed to test the knowledge and skills of professionals in public cloud security. Fortinet NSE 7 - Public Cloud Security 7.2 certification is highly valued in the IT industry, as it provides evidence of expertise in securing public cloud environments. NSE7_PBC-7.2 exam covers a range of topics, including cloud security fundamentals, cloud-specific threats and vulnerabilities, as well as advanced cloud security techniques.

NEW QUESTION 14

You are troubleshooting an Azure SDN connectivity issue with your FortiGate VM Which two queries does that SDN connector use to interact with the Azure management API? (Choose two.)

* The first query is targeted to a special IP address to get a token.
* The first query is targeted to IP address 8.8
* There is only one query initiating from FortiGate port1 &#8211;
* Some queries are made to manage public IP addresses.
Explanation

The Azure SDN connector uses two types of queries to interact with the Azure management API. The first query is targeted to a special IP address to get a token. This token is used to authenticate the subsequent queries. The second type of query is used to retrieve information about the Azure resources, such as virtual machines, network interfaces, network security groups, and public IP addresses. Some queries are made to manage public IP addresses, such as assigning or releasing them from the FortiGate VM.
References: Configuring an SDN connector in Azure, Azure SDN connector using service principal, Troubleshooting Azure SDN connector

NEW QUESTION 15

You need a solution to safeguard public cloud-hosted web applications from the OWASP Top 10 vulnerabilities. The solution must support the same region in which your applications reside, with minimum traffic cost Which solution meets the requirements?
* Use FortiADC
* Use FortiCNP
* Use FortiWebCloud
* Use FortiGate
Explanation

The correct answer is C. Use FortiWebCloud.

FortiWebCloud is a SaaS cloud-based web application firewall (WAF) that protects public cloud hosted web applications from the OWASP Top 10, zero day threats, and other application layer attacks1.FortiWebCloud also includes robust features such as API discovery and protection, bot mitigation, threat analytics, and advanced reporting2.FortiWebCloud supports multiple regions across the world, and you can choose the region that is closest to your applications to minimize traffic cost3.

The other options are incorrect because:

FortiADC is an application delivery controller that provides load balancing, acceleration, and security for web applications.It is not a dedicated WAF solution and does not offer the same level of protection as FortiWebCloud4.

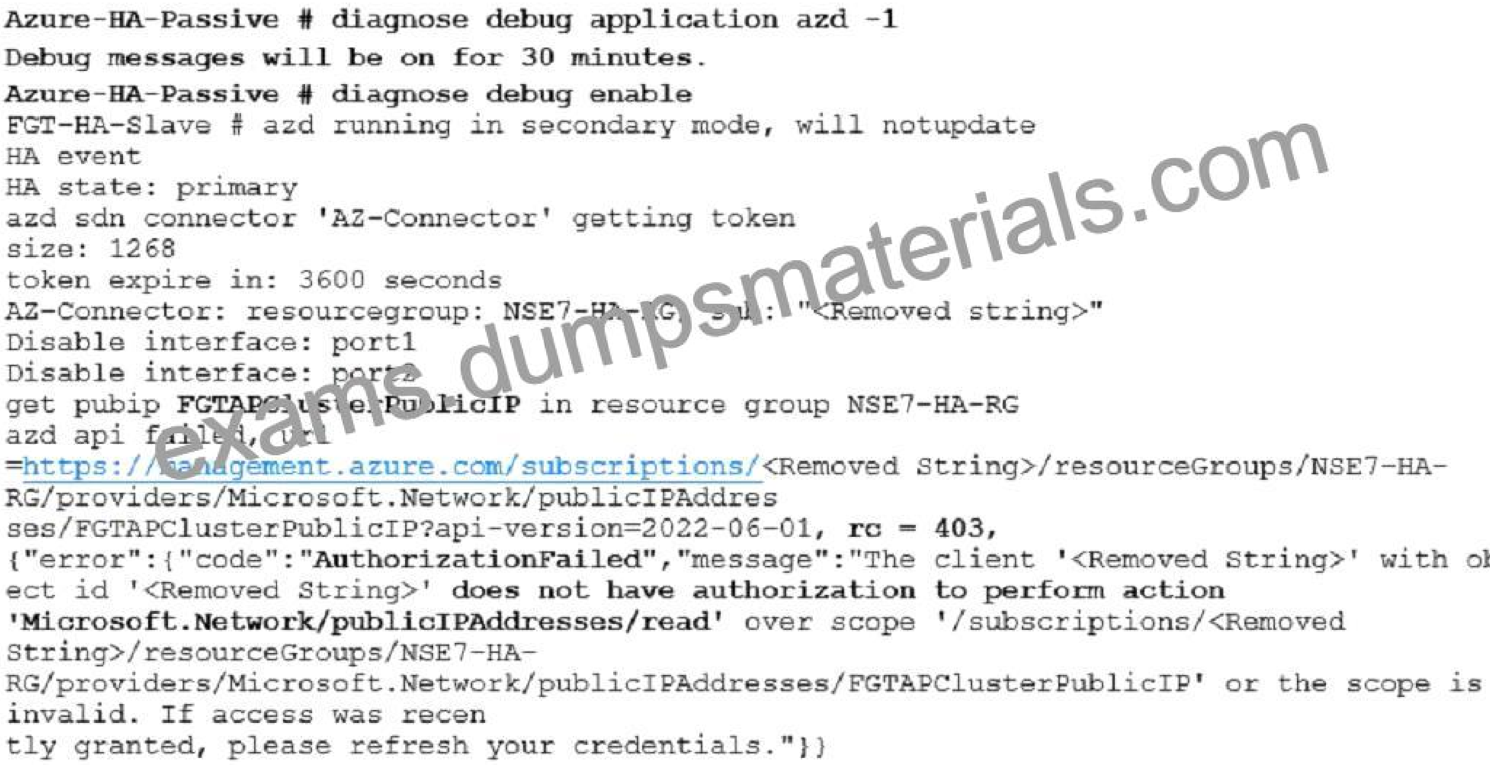
FortiCNP is a cloud-native platform that provides security and visibility for containerized applications.It is not a WAF solution and does not protect web applications from the OWASP Top 10 vulnerabilities5.

FortiGate is a next-generation firewall (NGFW) that provides network security and threat prevention. It is not a WAF solution and doesnot offer the same level of protection as FortiWebCloud for web applications.It also requires additional configuration and management to deploy in the public cloud6.

1:Overview | FortiWeb Cloud 23.3.0 &#8211; Fortinet Documentation2:Web Application Firewall (WAF) & API Protection | Fortinet3: [FortiWeb Cloud WAF-as-a-Service | Fortinet]4: [Application Delivery Controller (ADC) | Fortinet]5: [Fortinet Cloud Native Platform | Fortinet]6: [FortiGate Next-Generation Firewall (NGFW) | Fortinet]

NEW QUESTION 16

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.

What could be the possible issue With this scenario?
* FortiGate port4 does not have internet access.
* A wrong client secret credential is used
* The error is caused by credential time expiration.
* The Azure service principle account must have a contributor role.
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 17

You are tasked with deploying a FortiGate HA solution in Amazon Web Services (AWS) using Terraform What are two steps you must take to complete this deployment? (Choose two.)
* Enable automation on the AWS portal.
* Create an AWS Identity and Access Management (IAM) user With permissions.
* Use CloudSheIl to install Terraform.
* Create an AWS Active Directory user with permissions.

Explanation

To deploy a FortiGate HA solution in AWS using Terraform, you need to create an AWS IAM user with permissions to access the AWS resources and services required by the FortiGate-VM. You also need to use CloudShell to install Terraform, which is a tool for building, changing, and versioning infrastructure as code.

References:

Deploying FortiGate-VM using Terraform | AWS Administration Guide

Setting up IAM roles | AWS Administration Guide

Launching the instance using roles and user data | AWS Administration Guide Terraform by HashiCorp

NEW QUESTION 18

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.)
* Use ECMP and VPN to achieve higher bandwidth.
* Use transit VPC to build multiple VPC connections to the on-premises data center
* 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
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 &#8211; Transit VPC on AWS2:Fortinet Documentation Library &#8211; Deploying FortiGate VMs on AWS

NEW QUESTION 19

You are tasked with deploying a FortiGate HA solution in Amazon Web Services (AWS) using Terraform What are two steps you must take to complete this deployment? (Choose two.)

- Create an AWS Identity and Access Management (IAM) user With permissions.
- Enable automation on the AWS portal.
- Use CloudShell to install Terraform.
- Create an AWS Active Directory user with permissions.

Explanation

To deploy a FortiGate HA solution in AWS using Terraform, you need to create an AWS IAM user with permissions to access the AWS resources and services required by the FortiGate-VM. You also need to use CloudShell to install Terraform, which is a tool for building, changing, and versioning infrastructure as code.

References:

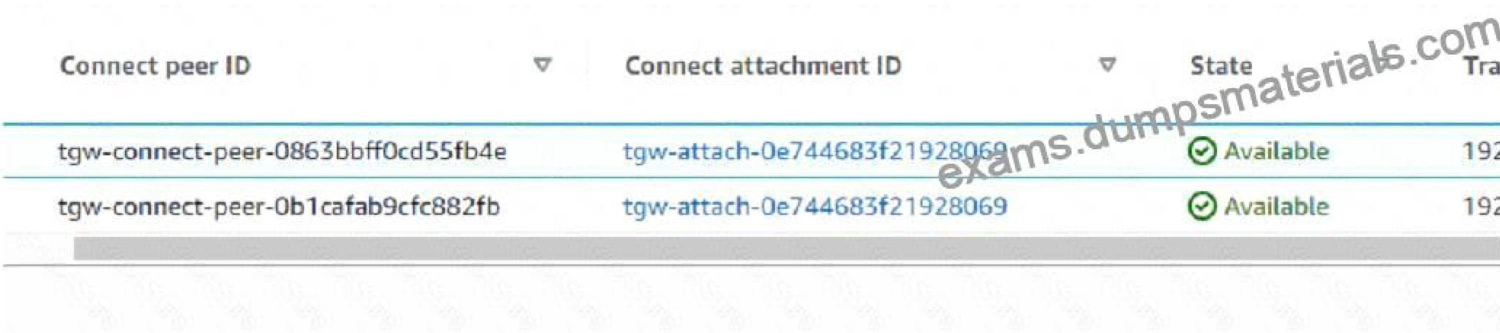
Deploying FortiGate-VM using Terraform | AWS Administration Guide

Setting up IAM roles | AWS Administration Guide

Launching the instance using roles and user data | AWS Administration Guide Terraform by HashiCorp

NEW QUESTION 20

Refer to Exhibit:



Connect peer ID	Connect attachment ID	State	Tra
tgw-connect-peer-0863bbff0cd55fb4e	tgw-attach-0e744683f21928069	✓ Available	192
tgw-connect-peer-0b1cafab9cfc882fb	tgw-attach-0e744683f21928069	✓ Available	192

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.)

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

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.

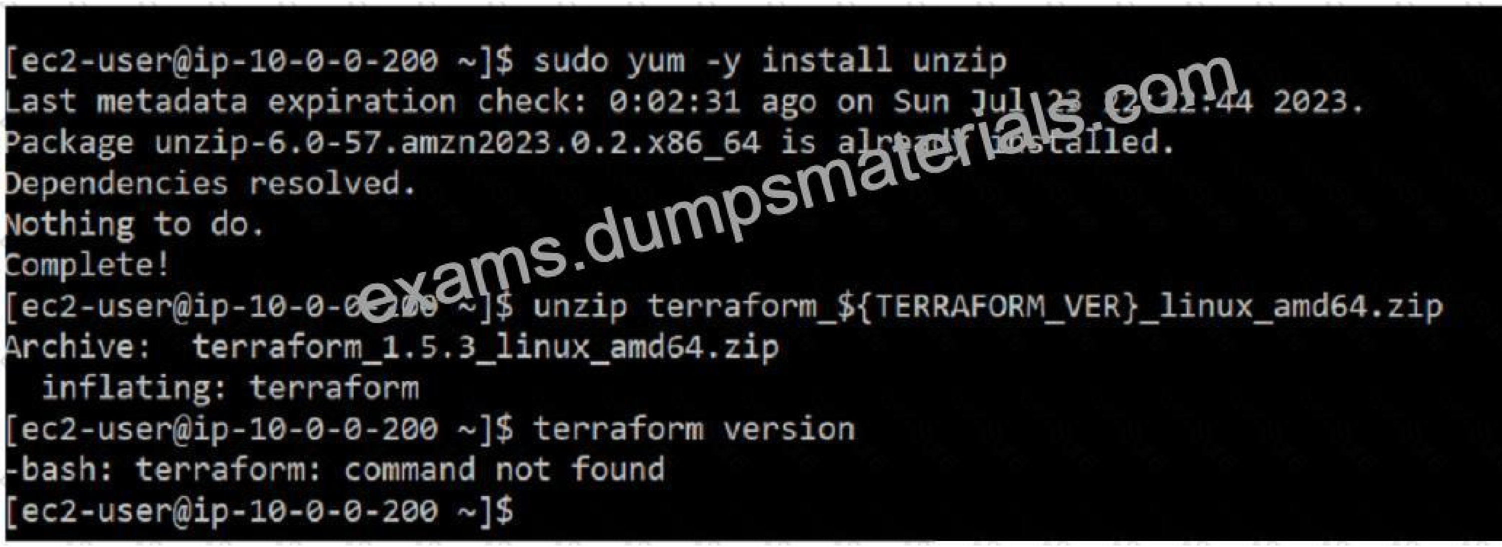
The other options are incorrect because:

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 21

Refer to the exhibit



```
[ec2-user@ip-10-0-0-200 ~]$ sudo yum -y install unzip
Last metadata expiration check: 0:02:31 ago on Sun Jul 23 22:12:44 2023.
Package unzip-6.0-57.amzn2023.0.2.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-10-0-0-200 ~]$ unzip terraform_${TERRAFORM_VER}_linux_amd64.zip
Archive:  terraform_1.5.3_linux_amd64.zip
  inflating: terraform
[ec2-user@ip-10-0-0-200 ~]$ terraform version
-bash: terraform: command not found
[ec2-user@ip-10-0-0-200 ~]$
```

You are tasked with deploying FortiGate using Terraform. When you run the terraform version command during the Terraform installation, you get an error message.

What could be the reason that you are getting the command not found error?

* You must move the binary file to the bin directory.
* You must change the directory location to the root directory
* You must assign correct permissions to the ec2-user.
* You must reinstall Terraform

Explanation

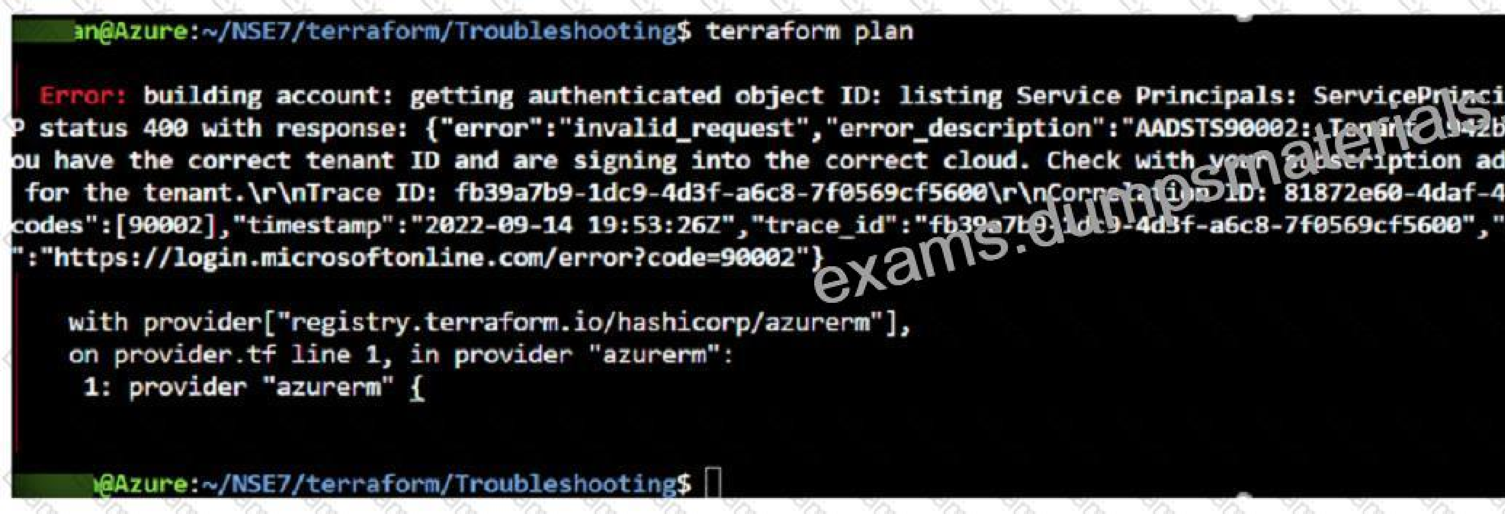
According to the Terraform documentation for installing Terraform on Linux1, you need to download a zip archive that contains a single binary file called terraform. You need to unzip the archive and move the binary file to a directory that is included in your system&#8217;s PATH environment variable, such as /usr/local/bin. This way, you can run the terraform command from any directory without specifying the full path1.

If you do not move the binary file to the bin directory, you will get a command not found error when you try to run the terraform version command, as shown in the screenshot. To fix this error, you need to move the binary file to the bin directory or specify the full path of the binary file when running the command1.

1: Install Terraform | Terraform &#8211; HashiCorp Learn

NEW QUESTION 22

Refer to Exhibit:



```
[redacted]an@Azure:~/NSE7/terraform/Troubleshooting$ terraform plan

 Error: building account: getting authenticated object ID: listing Service Principals: ServicePrinci
P status 400 with response: {"error":"invalid_request","error_description":"AADSTS90002: Tenant '942b
ou have the correct tenant ID and are signing into the correct cloud. Check with your subscription ad
 for the tenant.\r\nTrace ID: fb39a7b9-1dc9-4d3f-a6c8-7f0569cf5600\r\nCorrelation ID: 81872e60-4daf-4
codes":[90002],"timestamp":"2022-09-14 19:53:26Z","trace_id":"fb39a7b9-1dc9-4d3f-a6c8-7f0569cf5600","
":"https://login.microsoftonline.com/error?code=90002"}

   with provider["registry.terraform.io/hashicorp/azurerm"],
   on provider.tf line 1, in provider "azurerm":
    1: provider "azurerm" {


[redacted]@Azure:~/NSE7/terraform/Troubleshooting$ 
```

After the initial Terraform configuration in Microsoft Azure, the terraform plan command is run Which two statements about running the plan command are true? (Choose two.)
* The terraform plan command will deploy the rest of the resources except the service principle details.
* You cannot run the terraform apply command before the terraform plan command.
* You must run the terraform init command once, before the terraform plan command
* The terraform plan command makes terraform do a dry run.
A is incorrect because the terraform plan command will not deploy any resources at all. It will only show the changes that would be made if the terraform apply command was run. The error message in the exhibit indicates that the service principal details are invalid, which means that Terraform cannot authenticate to Azure and cannot create any resources1.

B is incorrect because you can run the terraform apply command without running the terraform plan command first. The terraform apply command will automatically generate a new plan and prompt you to approve it before applying it2. However, running the terraform plan command first can help you preview the changes and avoid any unwanted or unexpected actions.

C is correct because you must run the terraform init command once before the terraform plan command.

The terraform init command initializes a working directory containing Terraform configuration files. It downloads and installs the provider plugins required for your configuration, such as the Azure provider2. It also creates a hidden directory called .terraform to store the plugin binaries and other metadata1. Without running the terraform init command, the terraform plan command will fail because it cannot find the required plugins or modules.

D is correct because the terraform plan command makes Terraform do a dry run. A dry run is a simulation of what would happen if you executed a certain action, without actually performing it. The terraform plan command creates an execution plan, which is a description of the actions that Terraform would take to make your infrastructure match your configuration2. The execution plan shows you what resources will be created, modified, or destroyed, and what attributes will be changed. The execution plan does not affect your infrastructure or state file until you apply it with the terraform apply command1.

NEW QUESTION 23

What are three important steps required to get Terraform ready using Microsoft Azure Cloud Shell? (Choose three.)
* Set up a storage account in Azure.
* use the -O command to download Terraform.
* Subscribe to Terraform in Azure.
* Move the Terraform file to the bin directory.
* Use the wget (te=aform vession) command to upload Terraform.
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

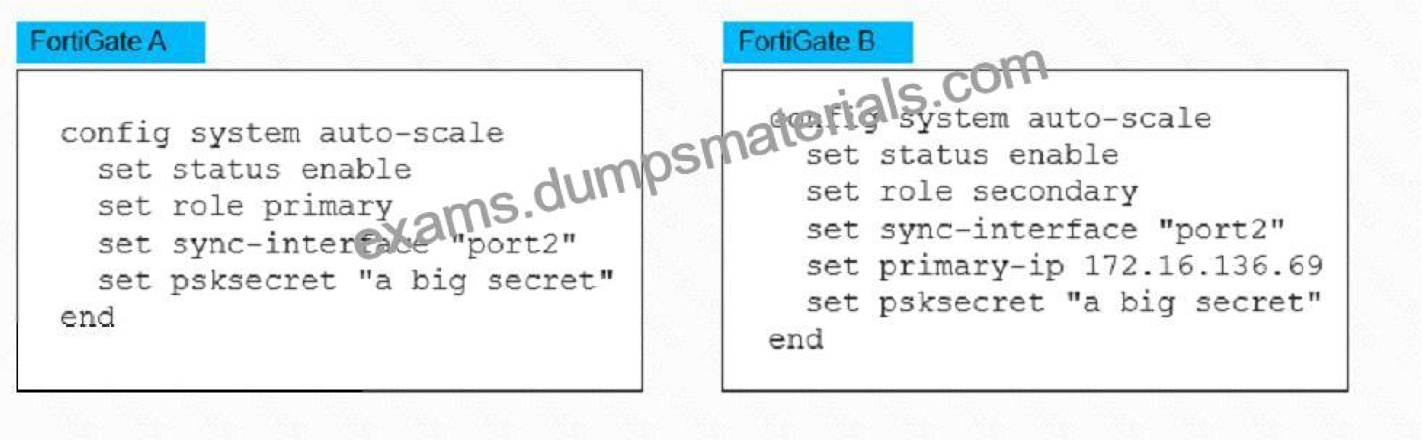
Configure Terraform in Azure Cloud Shell with Bash

wget(1) &#8211; Linux man page

Terraform by HashiCorp

NEW QUESTION 24

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.)

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

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.

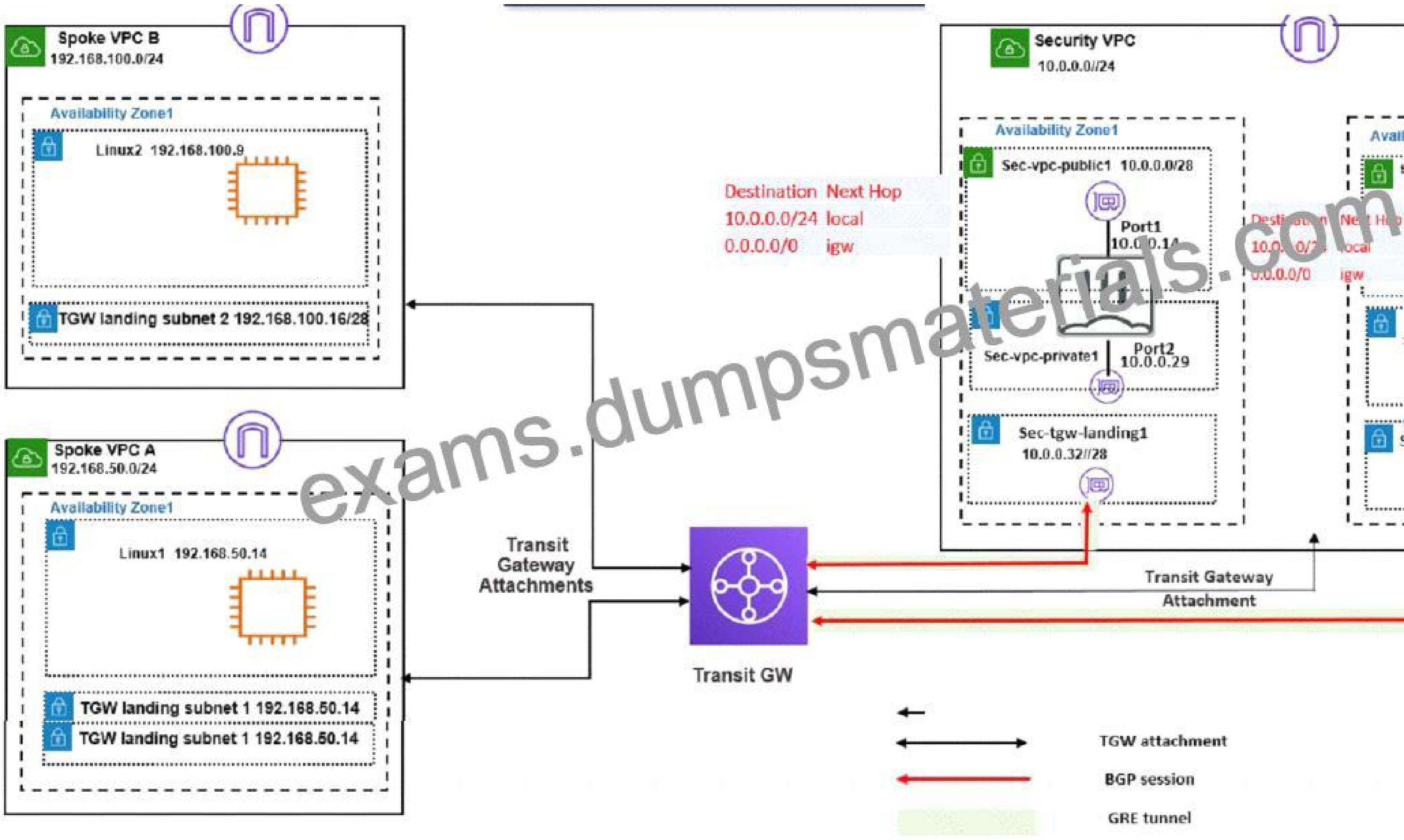
The other options are incorrect because:

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 25

Refer to the exhibit



A customer has deployed an environment in Amazon Web Services (AWS) and is now trying to send outbound traffic from the Linux1 and Linux2 instances to the internet through the security VPC (virtual private cloud). The FortiGate policies are configured to allow all outbound traffic; however, the traffic is not reaching the FortiGate internal interface. Assume there are no issues with the Transit Gateway (TGW) configuration Which two settings must the customer add to correct the issue? (Choose two.)

* Both landing subnets in the spoke VPCs must have a 0.0.0.0/0 traffic route to the Internet Gateway (IOW).
* Both landing subnets in the spoke VPCs must have a 0.0 00/0 traffic route to the TGW
* Both landing subnets in the security VPC must have a 0.0.0.0/0 traffic route to the FortiGate port2.
* The four landing subnets in all the VPCs must have a 0.0 0 0/0 traffic route to the TGW

Explanation

The correct answer is B and C. Both landing subnets in the spoke VPCs must have a 0.0.0.0/0 traffic route to the TGW. Both landing subnets in the security VPC must have a 0.0.0.0/0 traffic route to the FortiGate port2.

According to the AWS documentation for Transit Gateway, a transit gateway is a network transit hub that connects VPCs and on-premises networks. To send outbound traffic from the Linux instances to the internet through the security VPC, you need to do the following steps:

In the main subnet routing table in the spoke VPCs, 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.

In the main subnet routing table in the security VPC, add a new route with destination 0.0.0.0/0, next hop FortiGate port2. This route directs all traffic from the TGW to the FortiGate internal interface, where it can be inspected and allowed by the FortiGate policies.

The other options are incorrect because:

Adding a 0.0.0.0/0 traffic route to the Internet Gateway (IGW) in the spoke VPCs is not correct, as this would bypass the TGW and the security VPC and send all traffic directly to the internet.

Adding a 0.0.0.0/0 traffic route to the TGW in all the VPCs is not necessary, as only the spoke VPCs need to send traffic to the TGW. The security VPC needs to send traffic to the FortiGate port2.

Transit Gateways &#8211; Amazon Virtual Private Cloud:Fortinet Documentation Library &#8211; Deploying FortiGate VMs on AWS

NEW QUESTION 26

Which two attachments are necessary to connect a transit gateway to an existing VPC with BGP? (Choose two)
* A transport attachment
* A BGP attachment
* A connect attachment
* A GRE attachment
Explanation

The correct answer is A and C. A transport attachment and a connect attachment are necessary to connect a transit gateway to an existing VPC with BGP.

According to the AWS documentation for Transit Gateway, a transit gateway is a network transit hub that connects VPCs and on-premises networks. To connect a transit gateway to an existing VPC with BGP, you need to do the following steps:

Create a transport attachment. A transport attachment is a resource that connects a VPC or VPN to a transit gateway. You can specify the BGP options for the transport attachment, such as the autonomous system number (ASN) and the BGP peer IP address.

Create a connect attachment. A connect attachment is a resource that enables you to use your own appliance to provide network services for traffic that flows through the transit gateway. You can use a connect attachment to route traffic between the transport attachment and your appliance using GRE tunnels and BGP.

The other options are incorrect because:

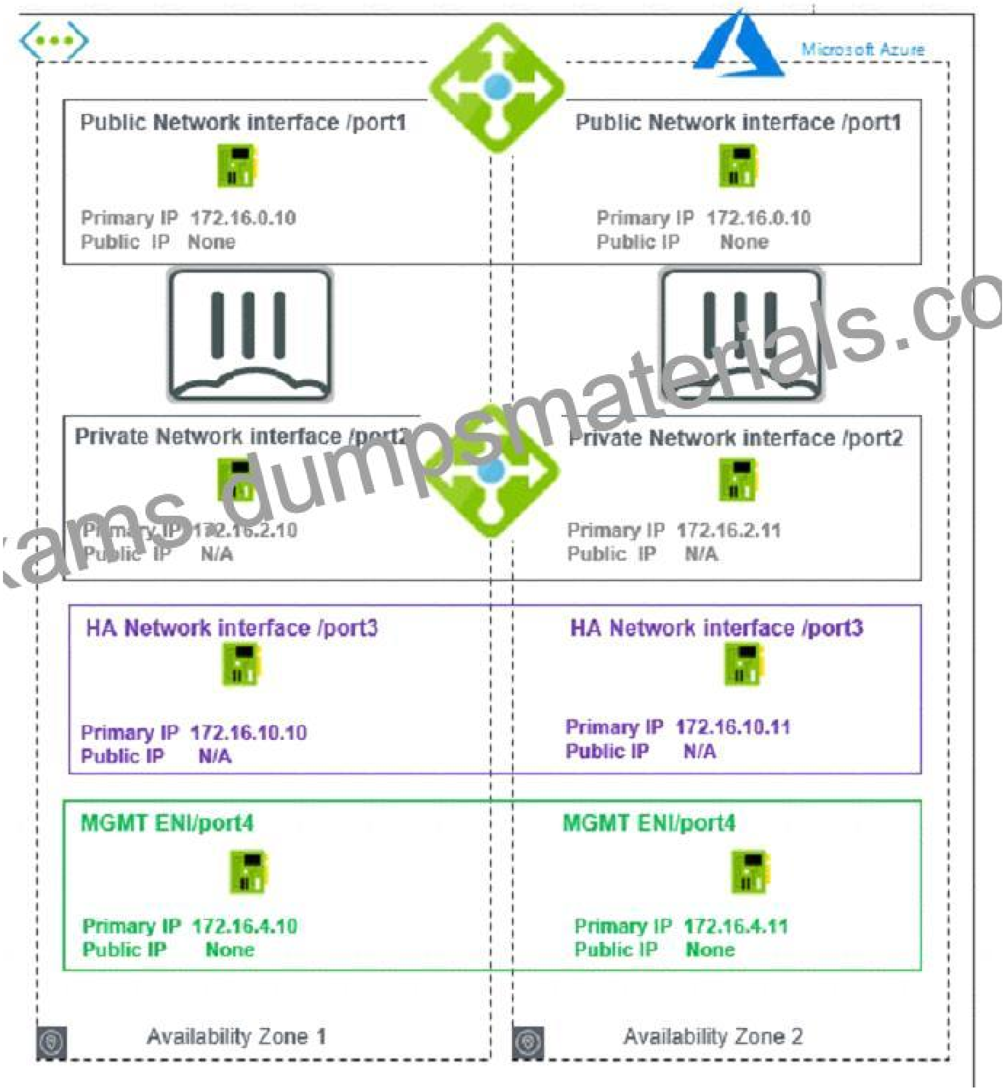
A BGP attachment is not a valid type of attachment for a transit gateway. BGP is a protocol that enables dynamic routing between the transit gateway and the VPC or VPN.

A GRE attachment is not a valid type of attachment for a transit gateway. GRE is a protocol that encapsulates packets for tunneling purposes. GRE tunnels are established between the connect attachment and your appliance.

[Transit Gateways &#8211; Amazon Virtual Private Cloud] : [Transit Gateway Connect &#8211; Amazon Virtual Private Cloud]

NEW QUESTION 27

Refer to the exhibit



You are deploying two FortiGate VMS in HA active-passive mode with load balancers in Microsoft Azure Which two statements are true in this load balancing scenario? (Choose two.)
* The FortiGate public IP is the next-hop for all the traffic.
* An internal load balancer listener is the next-hop for outgoing traffic.
* You must add a route to the Microsoft VIP used for the health check.
* A dedicated management interface can be used for load balancing.
A is incorrect because the FortiGate public IP is not the next-hop for all the traffic. The FortiGate public IP is only used for incoming traffic from the internet. The Azure load balancer distributes the incoming traffic to the active FortiGate VM based on a health probe123. The FortiGate public IP is not used for outgoing traffic or internal traffic.

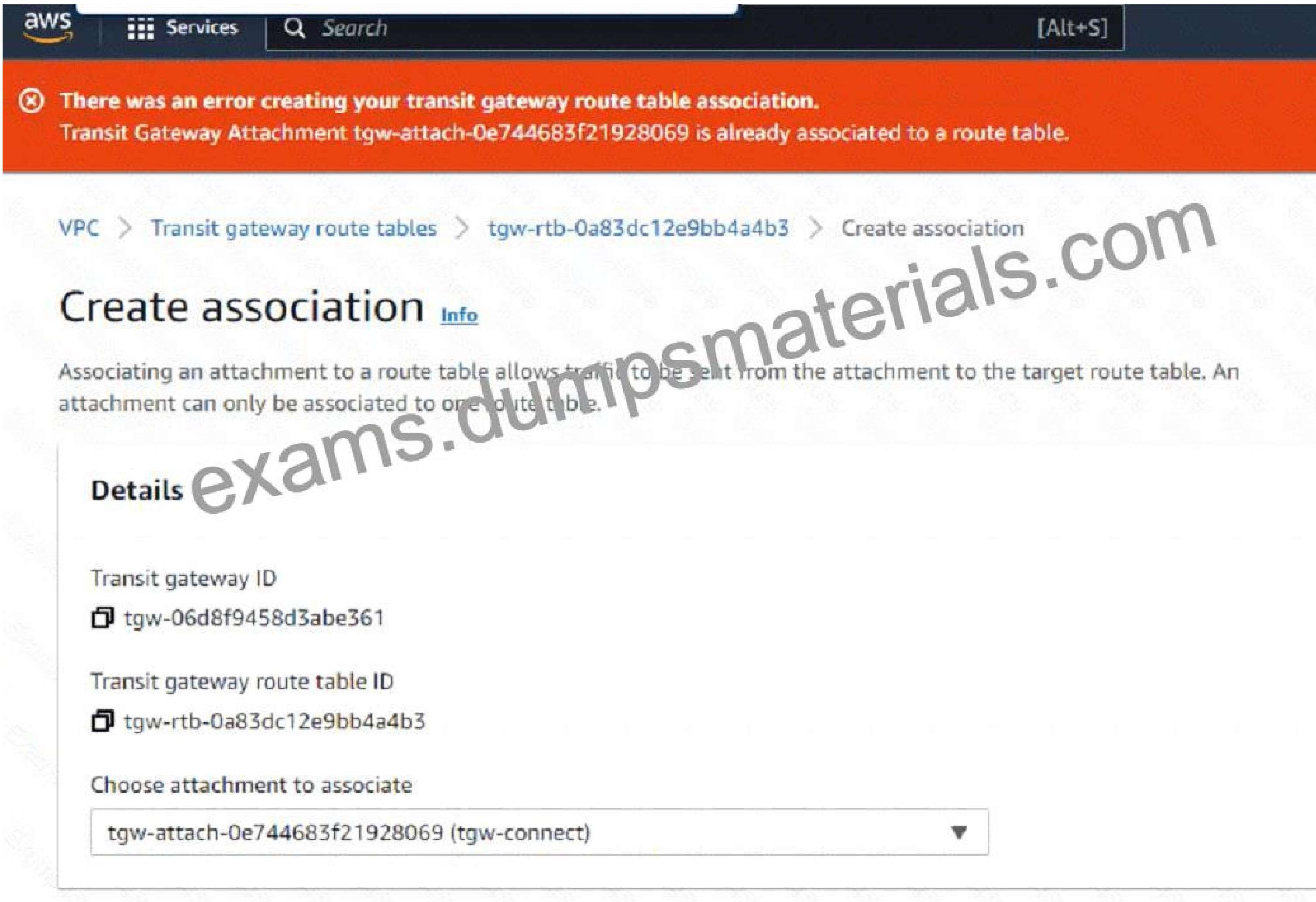
B is correct because an internal load balancer listener is the next-hop for outgoing traffic. The internal load balancer listener is configured with a floating IP address that is assigned to the active FortiGate VM. The internal load balancer listener also has a health probe to monitor the status of the FortiGate VMs123. The internal load balancer listener forwards the outgoing traffic to the internet through the public load balancer.

C is incorrect because you do not need to add a route to the Microsoft VIP used for the health check. The Microsoft VIP is an internal IP address that is used by the Azure load balancer to send health probes to the FortiGate VMs123. The Microsoft VIP is not reachable from outside the Azure network and does not require any routing configuration on the FortiGate VMs.

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

NEW QUESTION 28

Refer to the exhibit.



There was an error creating your transit gateway route table association.
Transit Gateway Attachment tgw-attach-0e744683f21928069 is already associated to a route table.

VPC > Transit gateway route tables > tgw-rtb-0a83dc12e9bb4a4b3 > Create association

Create association Info

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated to one route table.

Details

Transit gateway ID
tgw-06d8f9458d3abe361

Transit gateway route table ID
tgw-rtb-0a83dc12e9bb4a4b3

Choose attachment to associate
tgw-attach-0e744683f21928069 (tgw-connect) ▼

You are configuring a second route table on a Transit Gateway to accommodate east-west traffic inspection between two VPCs_ However, you are getting an error during the transit gateway route table association With the Connect attachment.

Which action Should you take to fulfill your requirement?
* Add both Associations and Propagations in the second TGW route table.
* Delete the both Connect and Transport attachments from the first TGW route table
* Add a static route in the Routes section
* In the second route table: create a propagation with the Connect attachment.
Explanation

The error message indicates that the Connect attachment is already associated with another transit gateway route table. You cannot associate the same attachment with more than one route table. However, you can propagate the same attachment to multiple route tables. Therefore, to fulfill your requirement of configuring a second route table for east-west traffic inspection between two VPCs, you need to create a propagation with the Connect attachment in the second route table. This will allow the second route table to learn the routes from the Connect attachment and forward the traffic to the securityVPC1. You also need to associate the second route table with the Transport attachment, which is the transit gateway attachment for the security VPC1.

References:

Transit gateway route tables &#8211; Amazon VPC | AWS Documentation

Getting started with transit gateways &#8211; Amazon VPC | AWS Documentation

Configuring TGW route tables | FortiGate Public Cloud 7.4.0 | Fortinet Document Library

Fortinet NSE7_PBC-7.2 certification exam is a comprehensive test that covers a wide range of topics related to cloud security. NSE7_PBC-7.2 exam includes questions on cloud computing, virtualization, network security, and Fortinet Security Fabric. NSE7_PBC-7.2 exam is designed to test the skills of professionals who manage public cloud environments using Fortinet's Security Fabric. NSE7_PBC-7.2 exam consists of multiple-choice questions that test the knowledge and skills of the candidate.

The Most In-Demand NSE7_PBC-7.2 Pass Guaranteed Quiz :
https://www.dumpsmaterials.com/NSE7_PBC-7.2-real-torrent.html]