NSE7_PBC-6.4.VCEplus.premium.exam.30q

Number: NSE7_PBC-6.4
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

NSE7_PBC-6.4

Fortinet NSE 7 – Public Cloud Security 6.4

Version 1.0

Exam A

QUESTION 1
When configuring the FortiCASB policy, which three configuration options are available? (Choose three.)

A. Intrusion prevention policies
B. Threat protection policies
C. Data loss prevention policies
D. Compliance policies
E. Antivirus policies

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/bf017449-572a-11e9-81a4-00505692583a/forticasb-4.1.0-admin-guide.pdf (62)

QUESTION 2
You have been tasked with deploying FortiGate VMs in a highly available topology on the Amazon Web Services (AWS) cloud. The requirements for your deployment are as follows:

- You must deploy two FortiGate VMs in a single virtual private cloud (VPC), with an external elastic load balancer which will distribute ingress traffic from the internet to both FortiGate VMs in an active-active topology.
- Each FortiGate VM must have two elastic network interfaces: one will connect to a public subnet and other will connect to a private subnet.
- To maintain high availability, you must deploy the FortiGate VMs in two different availability zones.

How many public and private subnets will you need to configure within the VPC?

A. One public subnet and two private subnets
B. Two public subnets and one private subnet
C. Two public subnets and two private subnets
D. One public subnet and one private subnet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
You are deploying Amazon Web Services (AWS) GuardDuty to monitor malicious or unauthorized behaviors related to AWS resources. You will also use the Fortinet `aws-lambda-guardduty` script to translate feeds from AWS GuardDuty findings into a list of malicious IP addresses. FortiGate can then consume this list as an external threat feed.

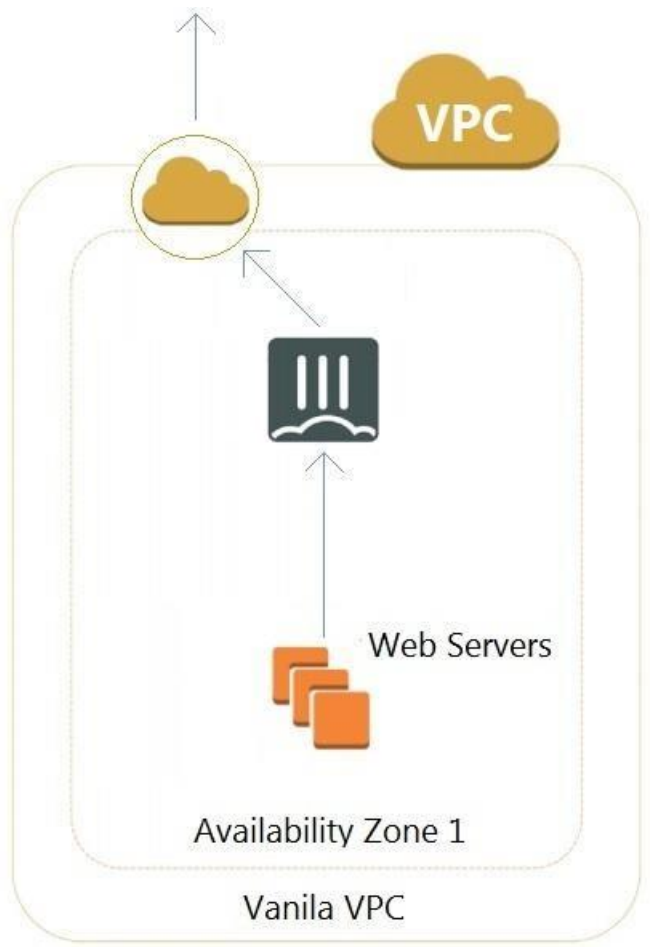
Which Amazon AWS services must you subscribe to in order to use this feature?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ed901ad2-4424-11e9-94bf-00505692583a/FortiOS_6.2.0_AWS_Cookbook.pdf

QUESTION 4



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 Web servers to the Internet. The FortiGate policies are configured to allow all outbound traffic; however, the traffic is not reaching the FortiGate internal interface.

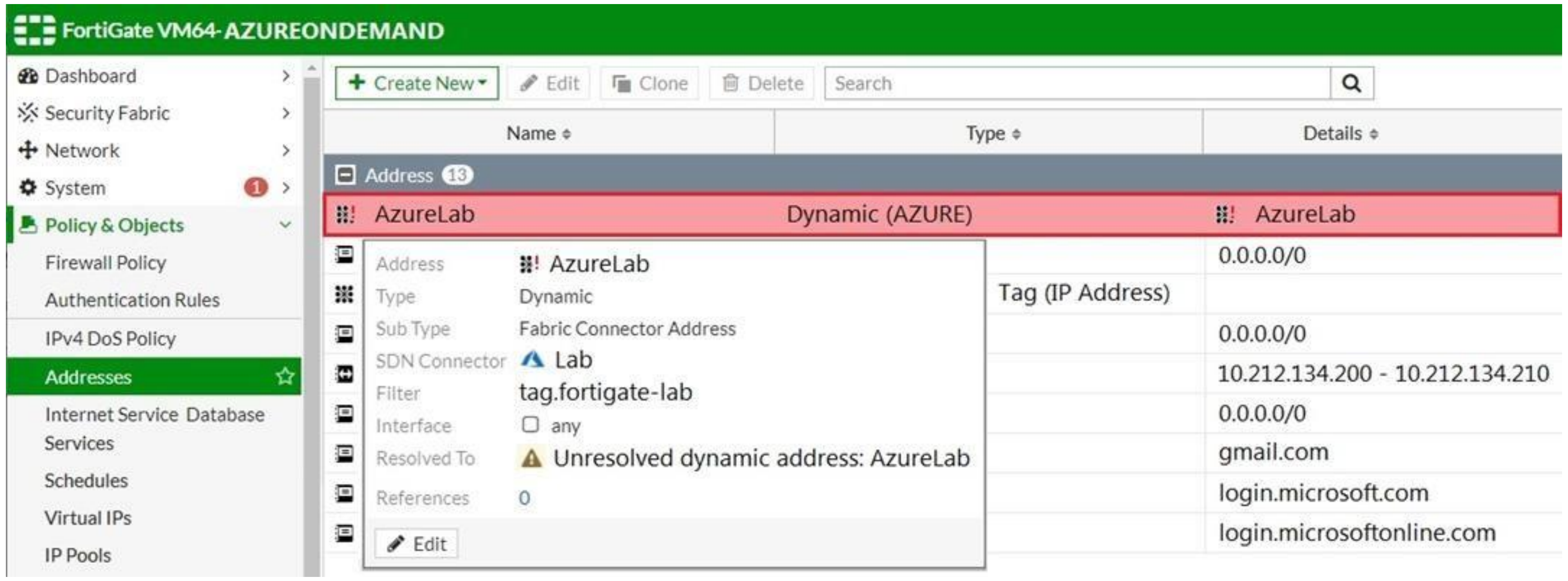
What are two possible reasons for this behavior? (Choose two.)

A. The web servers are not configured with the default gateway.
B. The Internet gateway (IGW) is not added to VPC (virtual private cloud).
C. AWS source and destination checks are enabled on the FortiGate interfaces.
D. AWS security groups may be blocking the traffic.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5



Name	Type	Details
Address 13		
AzureLab	Dynamic (AZURE)	AzureLab
		0.0.0.0/0
	Tag (IP Address)	
		0.0.0.0/0
		10.212.134.200 - 10.212.134.210
		0.0.0.0/0
		gmail.com
		login.microsoft.com
		login.microsoftonline.com

Address	AzureLab
Type	Dynamic
Sub Type	Fabric Connector Address
SDN Connector	Lab
Filter	tag.fortigate-lab
Interface	□ any
Resolved To	⚠ Unresolved dynamic address: AzureLab
References	0

Refer to the exhibit. Your senior administrator successfully configured a FortiGate fabric connector with the Azure resource manager, and created a dynamic address object on the FortiGate VM to connect with a windows server in Microsoft Azure. However, there is now an error on the dynamic address object, and you must resolve the issue.

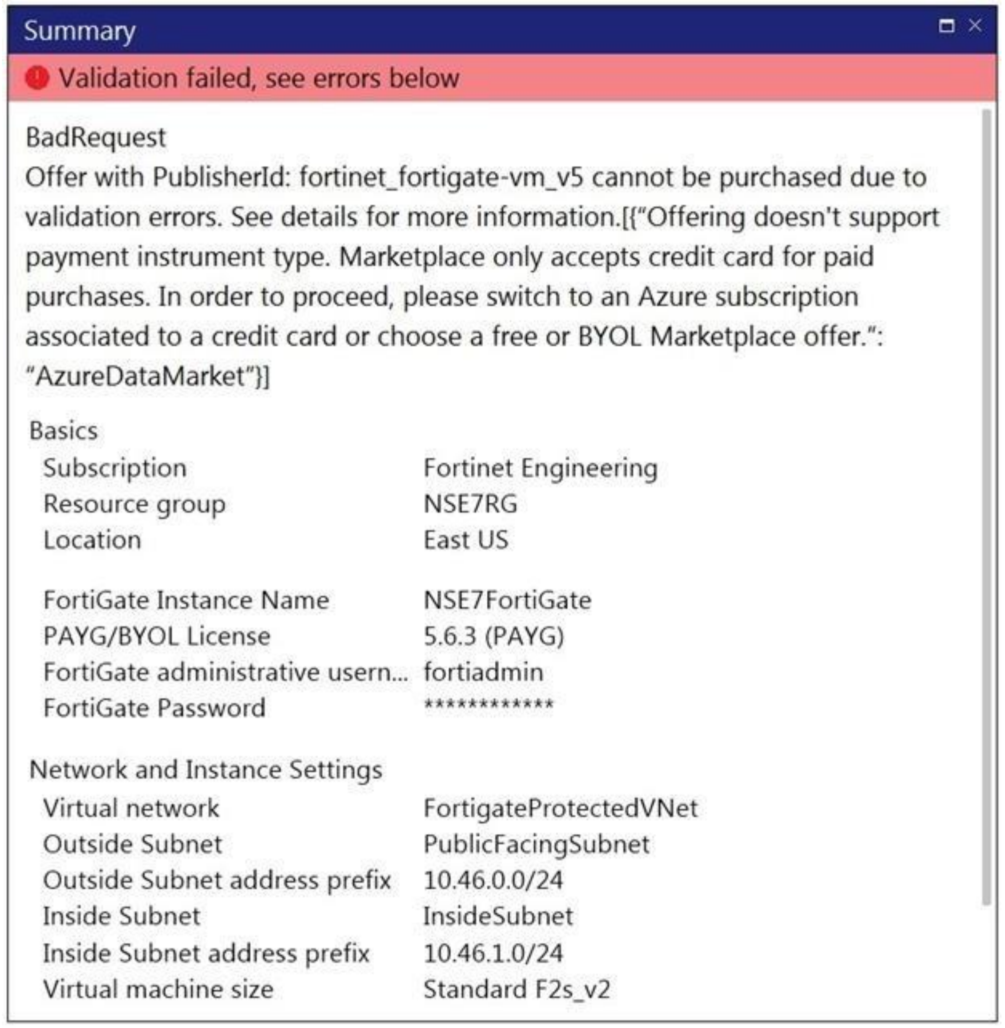
How do you resolve this issue?

A. Run `diagnose debug application azd -l` on FortiGate.
B. In the Microsoft Azure portal, set the correct tag values for the windows server.
C. In the Microsoft Azure portal, access the windows server, obtain the private IP address, and assign the IP address under the FortiGate-VM AzureLab address object.
D. Delete the address object and recreate a new address object with the type set to FQDN.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6



Validation failed, see errors below

BadRequest
Offer with PublisherId: fortinet_fortigate-vm_v5 cannot be purchased due to validation errors. See details for more information.[{"Offering doesn't support payment instrument type. Marketplace only accepts credit card for paid purchases. In order to proceed, please switch to an Azure subscription associated to a credit card or choose a free or BYOL Marketplace offer.": "AzureDataMarket"}]

Basics

Subscription	Fortinet Engineering
Resource group	NSE7RG
Location	East US
FortiGate Instance Name	NSE7FortiGate
PAYG/BYOL License	5.6.3 (PAYG)
FortiGate administrative usern...	fortiadmin
FortiGate Password	************

Network and Instance Settings

Virtual network	FortigateProtectedVNet
Outside Subnet	PublicFacingSubnet
Outside Subnet address prefix	10.46.0.0/24
Inside Subnet	InsideSubnet
Inside Subnet address prefix	10.46.1.0/24
Virtual machine size	Standard F2s_v2

Refer to the exhibit. You are deploying a FortiGate-VM in Microsoft Azure using the PAYG/On-demand licensing model. After you configure the FortiGate-VM, the validation process fails, displaying the error shown in the exhibit.

What caused the validation process to fail?

A. You selected the incorrect resource group.
B. You selected the Bring Your Own License (BYOL) licensing mode.
C. You selected the PAYG/On-demand licensing model, but did not select correct virtual machine size.
D. You selected the PAYG/On-demand licensing model, but did not associate a valid Azure subscription.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
An Amazon Web Services (AWS) auto-scale FortiGate cluster has just experienced a scale-down event, terminating a FortiGate in availability zone C.

This has now black-holed the private subnet in this availability zone.

What action will the worker node automatically perform to restore access to the black-holed subnet?

A. The worker node applies a route table from a non-black-holed subnet to the black-holed subnet.
B. The worker node moves the virtual IP of the terminated FortiGate to a running FortiGate on the worker node's private subnet interface.
C. The worker node modifies the route table applied to the black-holed subnet changing its default route to point to a running FortiGate on the worker node's private subnet interface.

D. The worker node migrates the subnet to a different availability zone.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which two statements about the Amazon Cloud Services (AWS) network access control lists (ACLs) are true? (Choose two.)

A. Network ACLs are stateless, and inbound and outbound rules are used for traffic filtering.
B. Network ACLs are stateful, and inbound and outbound rules are used for traffic filtering.
C. Network ACLs must be manually applied to virtual network interfaces.
D. Network ACLs support allow rules and deny rules.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

QUESTION 9
When an organization deploys a FortiGate-VM in a high availability (HA) (active/active) architecture in Microsoft Azure, they need to determine the default timeout values of the load balancer probes.

In the event of failure, how long will Azure take to mark a FortiGate-VM as unhealthy, considering the default timeout values?

A. Less than 10 seconds
B. 30 secondsC. 20 seconds
D. 16 seconds

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

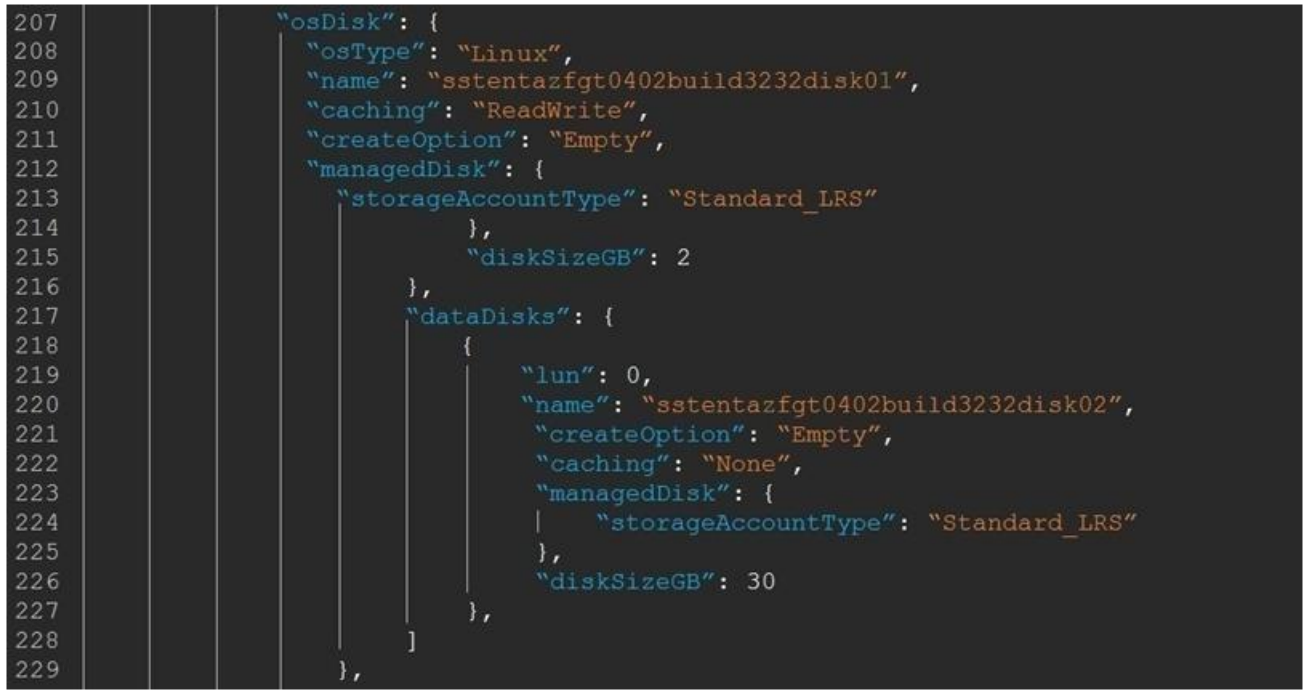
QUESTION 10 Which three properties are configurable Microsoft Azure network security group rule settings?
(Choose three.)

A. Action
B. Sequence number
C. Source and destination IP ranges
D. Destination port ranges
E. Source port ranges

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

QUESTION 11



```
"osDisk": {
  "osType": "Linux",
  "name": "sstentazfgt0402build3232disk01",
  "caching": "ReadWrite",
  "createOption": "Empty",
  "managedDisk": {
    "storageAccountType": "Standard_LRS"
            },
            "diskSizeGB": 2
        },
        "dataDisks": {
            {
                "lun": 0,
                "name": "sstentazfgt0402build3232disk02",
                 "createOption": "Empty",
                 "caching": "None",
                 "managedDisk": {
                 |    "storageAccountType": "Standard_LRS"
                 },
                 "diskSizeGB": 30
            },
        ]
    },
```

Refer to the exhibit. You attempted to deploy the FortiGate-VM in Microsoft Azure with the JSON template, and it failed to boot up. The exhibit shows an excerpt from the JSON template.

What is incorrect with the template?

A. The `LUN ID` is not defined.
B. FortiGate-VM does not support `managedDisk` from Azure.
C. The `caching` parameter should be `None`.
D. The `CreateOptions` parameter should be `FromImage`.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

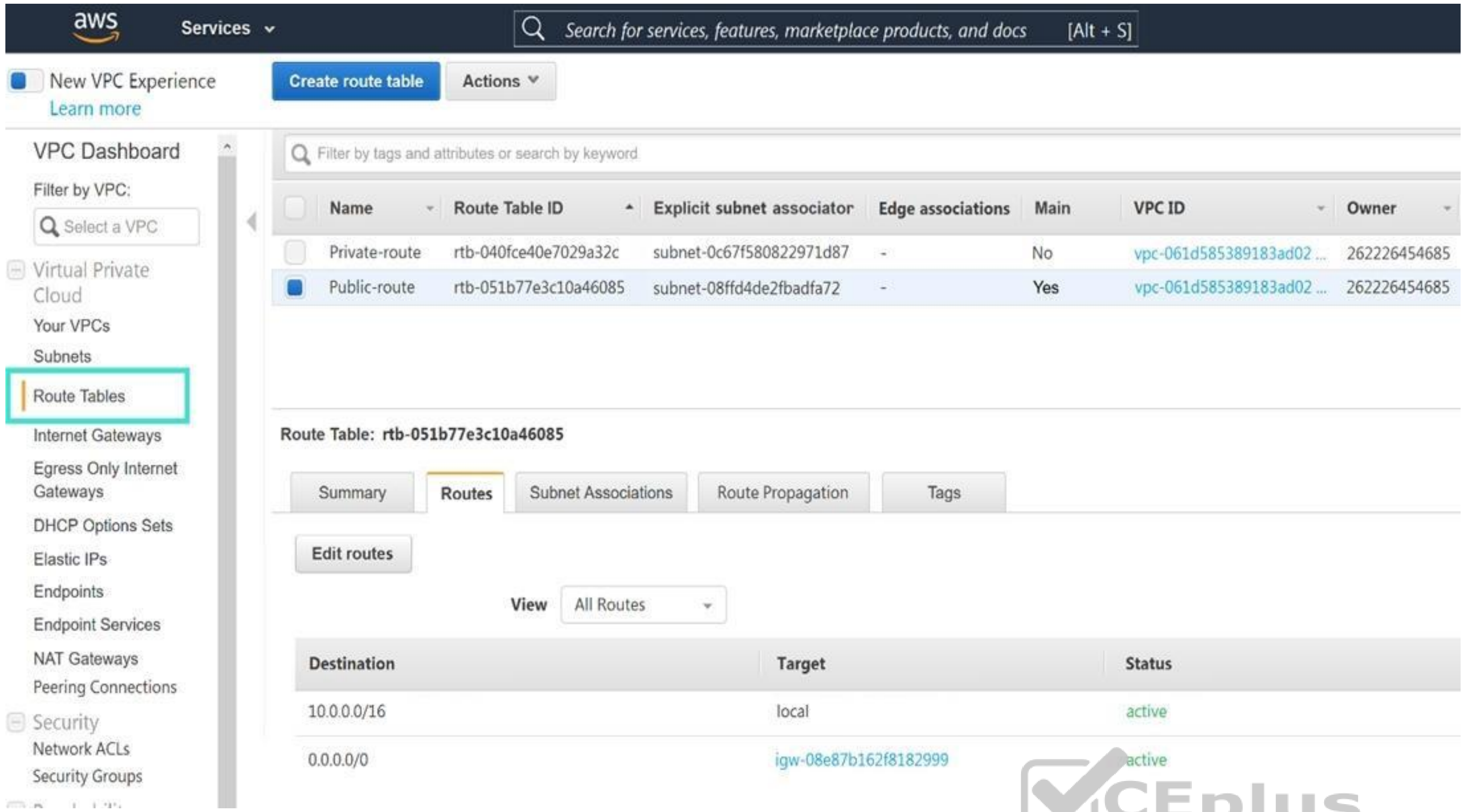
QUESTION 12 Which two statements about Microsoft Azure network security groups are true? (Choose two.)

A. Network security groups can be applied to subnets and virtual network interfaces.
B. Network security groups can be applied to subnets only.
C. Network security groups are stateless inbound and outbound rules used for traffic filtering.
D. Network security groups are a stateful inbound and outbound rules used for traffic filtering.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

QUESTION 13



	Name	Route Table ID	Explicit subnet associator	Edge associations	Main	VPC ID	Owner
□	Private-route	rtb-040fce40e7029a32c	subnet-0c67f580822971d87	-	No	vpc-061d585389183ad02 ...	262226454685
■	Public-route	rtb-051b77e3c10a46085	subnet-08ffd4de2fbadfa72	-	Yes	vpc-061d585389183ad02 ...	262226454685

Route Table: rtb-051b77e3c10a46085

View: All Routes

Destination	Target	Status
10.0.0.0/16	local	active
0.0.0.0/0	igw-08e87b162f8182999	active

Refer to the exhibit. In your Amazon Web Services (AWS) virtual private cloud (VPC), you must allow outbound access to the internet and upgrade software on an EC2 instance, without using a NAT instance. This specific EC2 instance is running in a private subnet: `10.0.1.0/24`.

Also, you must ensure that the EC2 instance source IP address is not exposed to the public internet. There are two subnets in this VPC in the same availability zone, named public (`10.0.0.0/24`) and private (`10.0.1.0/24`).

How do you achieve this outcome with minimum configuration?

A. Deploy a NAT gateway with an EIP in the private subnet, edit the public main routing table, and change the destination route `0.0.0.0/0` to the target NAT gateway.
B. Deploy a NAT gateway with an EIP in the public subnet, edit route tables, select Public-route, and delete the route destination `10.0.0.0/16` to target local.
C. Deploy a NAT gateway with an EIP in the private subnet, edit route tables, select Private-route, and add a new route destination `0.0.0.0/0` to the target internet gateway.
D. Deploy a NAT gateway with an EIP in the public subnet, edit route tables, select Private-route and add a new route destination `0.0.0.0/0` to target the NAT gateway.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 What is the bandwidth limitation of an Amazon Web Services (AWS) transit gateway VPC attachment?

A. Up to 1.25 Gbps per attachment
B. Up to 50 Gbps per attachment
C. Up to 10 Gbps per attachment
D. Up to 1 Gbps per attachment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf (5)

QUESTION 15 A company deployed a FortiGate-VM with an on-demand license using Amazon Web Services (AWS) Market Place Cloud Formation template. After deployment, the administrator cannot remember the default admin password.

What is the default admin password for the FortiGate-VM instance?

A. The admin password cannot be recovered and the customer needs to deploy the FortiGate-VM again.
B. <blank>
C. admin
D. The instance-ID value

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/aws-cookbook/828256/connecting-to-the-fortigate-vm

QUESTION 16
You have been asked to secure your organization’s salesforce application that is running on Microsoft Azure, and find an effective method for inspecting shadow IT activities in the organization. After an initial investigation, you find that many users access the salesforce application remotely as well as on-premises. Your goal is to find a way to get more visibility, control over shadow IT-related activities, and identify any data leaks in the salesforce application. Which three steps should you take to achieve your goal? (Choose three.)

A. Deploy and configure FortiCASB with a Fortinet FortiCASB subscription license.
B. Configure FortiCASB and set up access rights, privileges, and data protection policies.
C. Use FortiGate, FortiGuard, and FortiAnalyzer solutions.
D. Deploy and configure FortiCWP with a workload guardian license.
E. Deploy and configure FortiGate with Security Fabric solutions, and FortiCWP with a storage guardian advance license.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Your company deploys FortiGate VM devices in high availability (HA) (active-active) mode with Microsoft Azure load balancers using the Microsoft Azure ARM template. Your senior administrator instructs you to connect to one of the FortiGate devices and configure the necessary firewall rules. However, you are not sure now to obtain the correct public IP address of the deployed FortiGate VM and identify the access ports.

How do you obtain the public IP address of the FortiGate VM and identify the correct ports to access the device?

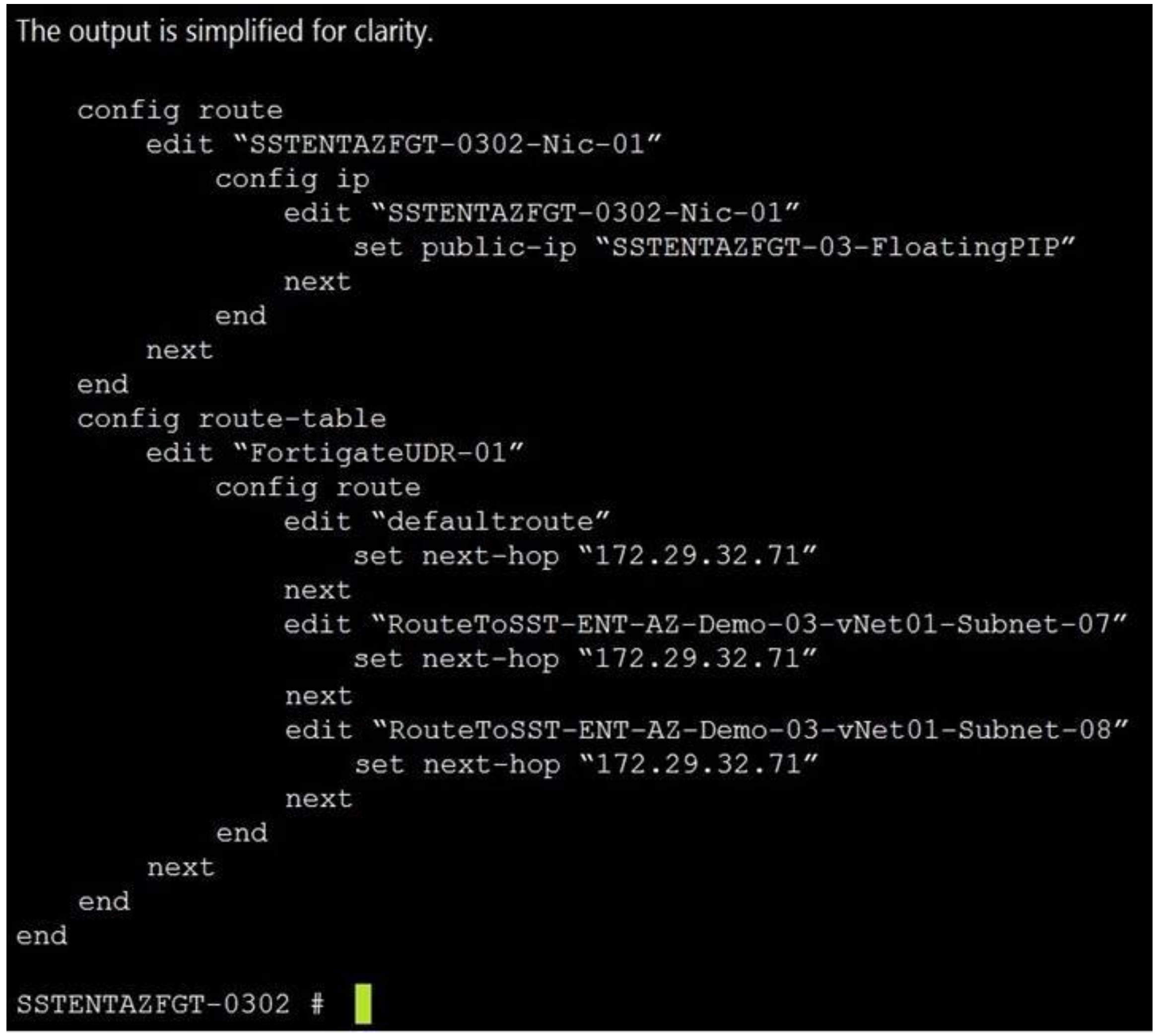
A. In the configured load balancer, access the inbound NAT rules section.
B. In the configured load balancer, access the backend pools section.
C. In the configured load balancer, access the inbound and outbound NAT rules section.
D. In the configured load balancer, access the health probes section.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: https://www.fortinet.com/content/dam/fortinet/assets/deployment-guides/dg-fortigate-high-availability-azure.pdf

QUESTION 18



```
The output is simplified for clarity.

    config route
        edit “SSTENTAZFGT-0302-Nic-01”
            config ip
                edit “SSTENTAZFGT-0302-Nic-01”
                    set public-ip “SSTENTAZFGT-03-FloatingPIP”
                next
            end
        next
    end
    config route-table
        edit “FortigateUDR-01”
            config route
                edit “defaultroute”
                    set next-hop “172.29.32.71”
                next
                edit “RouteToSST-ENT-AZ-Demo-03-vNet01-Subnet-07”
                    set next-hop “172.29.32.71”
                next
                edit “RouteToSST-ENT-AZ-Demo-03-vNet01-Subnet-08”
                    set next-hop “172.29.32.71”
                next
            end
        next
    end
end

SSTENTAZFGT-0302 #
```

Refer to the exhibit. Consider an active-passive HA deployment in Microsoft Azure. The exhibit shows an excerpt from the passive FortiGate-VM node.

If the active FortiGate-VM fails, what are the results of the API calls made by the FortiGate named `SSTENTAZFGT-0302`? (Choose two.)

A. `SSTENTAZFGT-03-FloatingPIP` is assigned to the IP configuration with the name `SSTENTAZFGT-0302-Nic-01`, under the network interface `SSTENTAZFGT-0302-Nic-01`
B. `172.29.32.71` is set as a next hop IP for all routes under `FortigateUDR-01`
C. The network interface of the active unit moves to itself
D. `SSTENTAZFGT-03-FloatingPIP` public IP is assigned to NIC `SSTENTAZFGT-0302-Nic-01`

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which two Amazon Web Services (AWS) topologies support east-west traffic inspection within the AWS cloud by the FortiGate VM? (Choose two.)

A. A single VPC deployment with multiple subnets and a NAT gateway
B. A single VPC deployment with multiple subnets
C. A multiple VPC deployment utilizing a transit VPC topology

D. A multiple VPC deployment utilizing a transit gateway

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-aws-reference-architecture.pdf

QUESTION 20
You have previously deployed an Amazon Web Services (AWS) transit virtual private cloud (VPC) with a pair of FortiGate firewalls (VM04 / c4.xlarge) as your security perimeter. You are beginning to see high CPU usage on the FortiGate instances.

Which action will fix this issue?

A. Convert the `c4.xlarge` instances to `m4.xlarge` instances.
B. Migrate the transit VPNs to new and larger instances (VM08 / c4.2xlarge).
C. Convert from IPsec tunnels to generic routing encapsulation (GRE) tunnels, for the VPC peering connections.
D. Convert the transit VPC firewalls into an auto-scaling group and launch additional EC2 instances in that group.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 Which two statements about Amazon Web Services (AWS) networking are correct?
(Choose two.)

A. Proxy ARP entries are disregarded.
B. 802.1q VLAN tags are allowed inside the same virtual private cloud.
C. AWS DNS reserves the first host IP address of each subnet.
D. Multicast traffic is not allowed.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.aws.amazon.com/sdkfornet/v3/apidocs/items/EC2/TIEC2.html

QUESTION 22
An organization deploys a FortiGate-VM (VM04 / c4.xlarge) in Amazon Web Services (AWS) and configures two elastic network interfaces (ENIs). Now, the same organization wants to add additional ENIs to support different workloads in their environment.

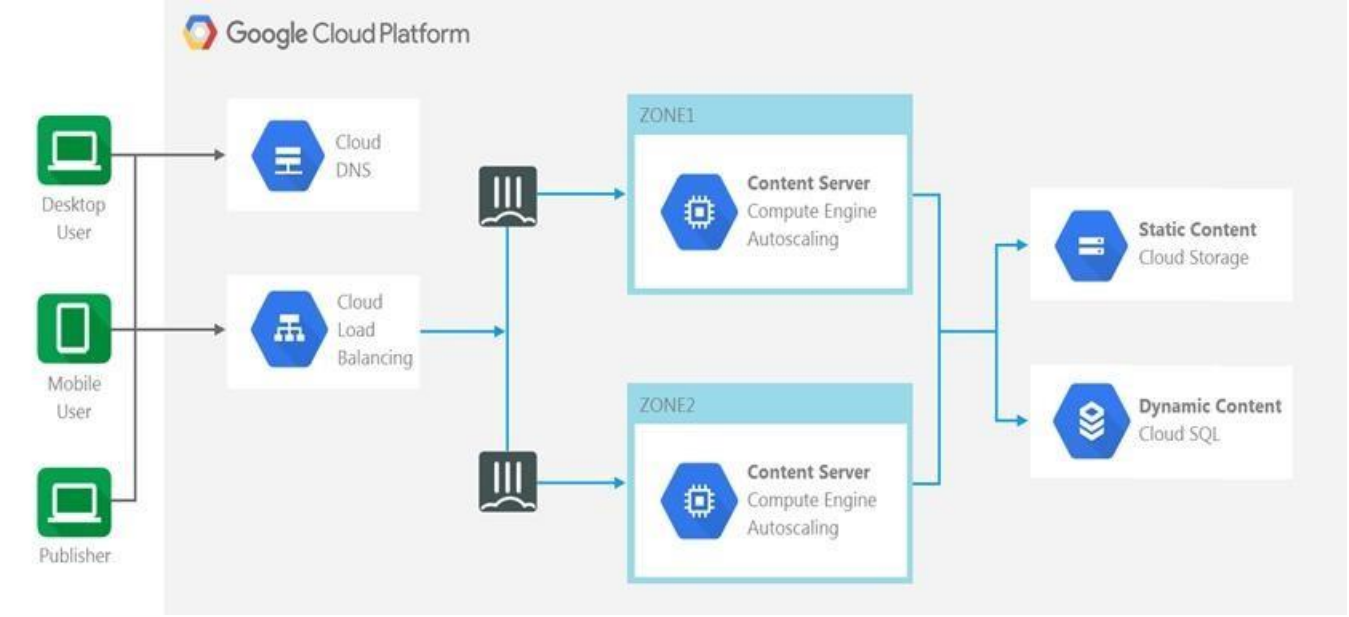
Which action can you take to accomplish this?

A. None, you cannot create and add additional ENIs to an existing FortiGate-VM.
B. Create the ENI, shut down FortiGate, attach the ENI to FortiGate, and then start FortiGate.
C. Create the ENI, attach it to FortiGate, and then restart FortiGate.
D. Create the ENI and attach it to FortiGate.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9e3b59dc-ba0b-11e9-a989-00505692583a/FortiOS_6.2_AWS_Cookbook.pdf

QUESTION 23



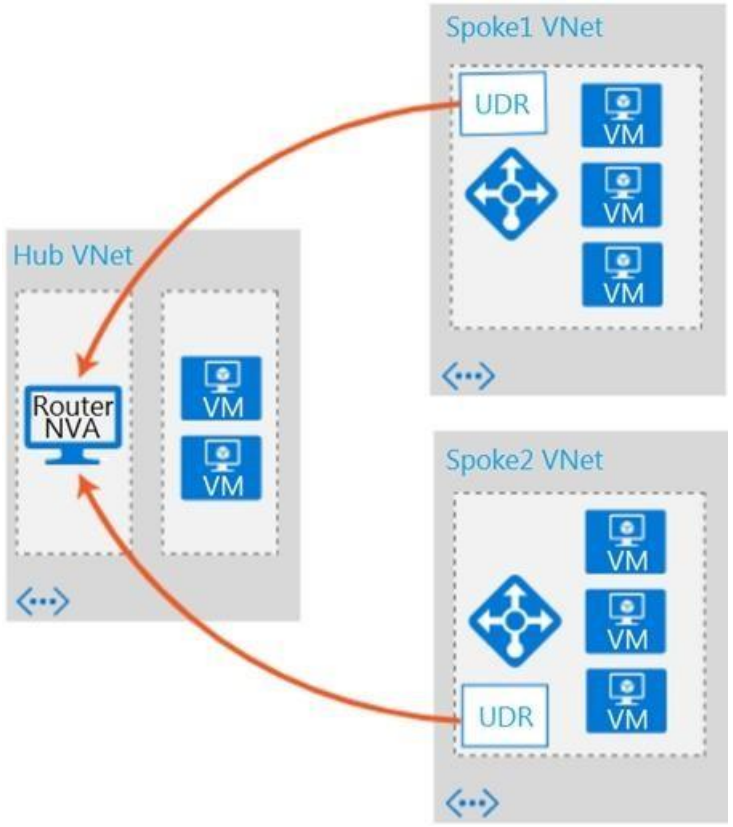
Refer to the exhibit. The exhibit shows a topology where multiple connections from clients to the same FortiGate-VM instance, regardless of the protocol being used, are required. Which two statements are correct? (Choose two.)

A. The design shows an active-active FortiGate-VM architecture.
B. The **Cloud Load Balancer Session Affinity** setting should be changed to CLIENT_IP.
C. The design shows an active-passive FortiGate-VM architecture.
D. The **Cloud Load Balancer Session Affinity** setting should use the default value.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24



Refer to the exhibit. Which two conditions will enable you to segregate and secure the traffic between the hub and the spokes in Microsoft Azure? (Choose two.)

A. Implement the FortiGate-VM network virtual appliance (NVA) in the hub and use user-defined routes (UDRs) in the spokes.
B. Use ExpressRoute to interconnect the hub VNets and spoke VNets.
C. Configure VNet peering between the spokes only.
D. Configure VNet peering between the hub and spokes.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
An organization deployed a FortiGate-VM in the Google Cloud Platform and initially configured it with two vNICs. Now, the same organization wants to add additional vNICs to this existing FortiGate-VM to support different workloads in their environment.

How can they do this?

A. They can create additional vNICs using the Cloud Shell.
B. They cannot create and add additional vNICs to an existing FortiGate-VM.
C. They can create additional vNICs in the UI console.
D. They can use the Compute Engine API Explorer.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/62d32ecf-687f-11ea-9384-00505692583a/FortiOS-6.4-GCP_Cookbook.pdf

QUESTION 26
You have been asked to develop an Azure Resource Manager infrastructure as a code template for the FortiGate-VM, that can be reused for multiple deployments. The deployment fails, and errors point to the `storageAccount` name. Which

two are restrictions for a `storageAccount` name in an Azure Resource Manager template? (Choose two.)

A. The `uniqueString()` function must be used.
B. The `storageAccount` name must use special characters.
C. The `storageAccount` name must be in lowercase.
D. The `storageAccount` name must contain between 3 and 24 alphanumeric characters.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

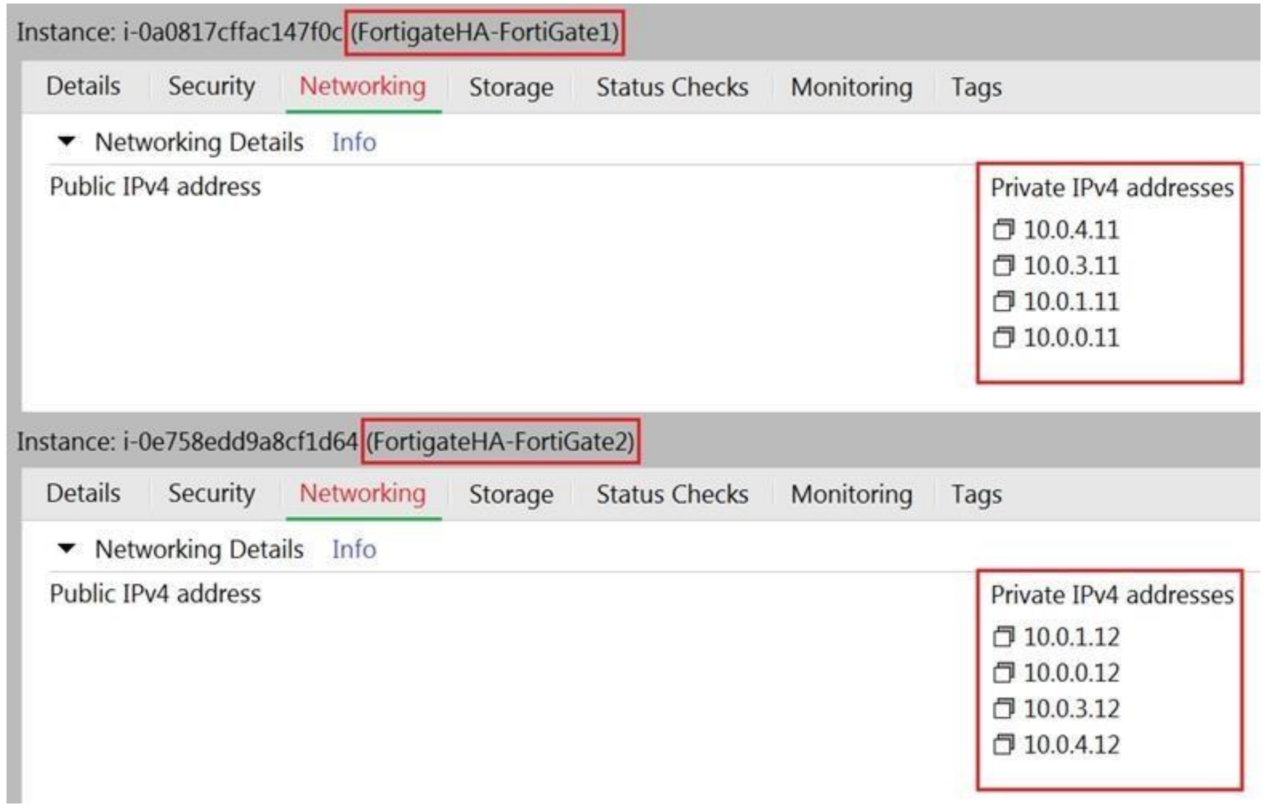
QUESTION 27 Which statement about FortiSandbox in Amazon Web Services (AWS) is true?

A. In AWS, virtual machines (VMs) that inspect files do not have to be reset after inspecting a file.
B. FortiSandbox in AWS uses Windows virtual machines (VMs) to inspect files.
C. In AWS, virtual machines (VMs) that inspect files are constantly up and running.
D. FortiSandbox in AWS can have a maximum of eight virtual machines (VMs) that inspect files.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28



Instance: i-0a0817cffac147f0c (FortigateHA-FortiGate1)

Public IPv4 address

Private IPv4 addresses
10.0.4.11
10.0.3.11
10.0.1.11
10.0.0.11

Instance: i-0e758edd9a8cf1d64 (FortigateHA-FortiGate2)

Public IPv4 address

Private IPv4 addresses
10.0.1.12
10.0.0.12
10.0.3.12
10.0.4.12

Refer to the exhibit. You are configuring an active-passive FortiGate clustering protocol (FGCP) HA configuration in a single availability zone in Amazon Web Services (AWS), using a cloud formation template.
After deploying the template, you notice that the AWS console has IP information listed in the FortiGate VM firewalls in the HA configuration. However, within the configuration of FortiOS, you notice that port1 is using an IP of `10.0.0.13`, and port2 is using an IP of `10.0.1.13`.

What should you do to correct this issue?

A. Configure FortiOS to use static IP addresses with the IP addresses reflected in the ENI primary IP address configuration (as per the exhibit).
B. Delete the deployment and start again. You have in put the wrong parameters during the cloud formation template deployment.
C. Configure FortiOS to use DHCP so that it will get the correct IP addresses on the ports.
D. Nothing, in AWS cloud, it is normal for a FortiGate ENI primary IP address to be different than the FortiOS IP address configuration.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Customer XYZ has an ExpressRoute connection from Microsoft Azure to a data center. They want to secure communication over ExpressRoute, and to install an in-line FortiGate to perform intrusion prevention system (IPS) and antivirus scanning.

Which three methods can the customer use to ensure that all traffic from the data center is sent through FortiGate over ExpressRoute? (Choose three.)

A. Install FortiGate in Azure and build a VPN tunnel to the data center over ExpressRoute
B. Configure a user-defined route table
C. Enable the redirect option in ExpressRoute to send data center traffic to a user-defined route table
D. Configure the gateway subnet as the subnet in the user-defined route table
E. Define a default route where the next hop IP is the FortiGate WAN interface

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
You need to deploy FortiGate VM devices in a highly available topology in the Microsoft Azure cloud. The following are the requirements of your deployment:

- Two FortiGate devices must be deployed; each in a different availability zone.
- Each FortiGate requires two virtual network interfaces: one will connect to a public subnet and the other will connect to a private subnet.
- An external Microsoft Azure load balancer will distribute ingress traffic to both FortiGate devices in an active-active topology.
- An internal Microsoft Azure load balancer will distribute egress traffic from protected virtual machines to both FortiGate devices in an active-active topology.
- Traffic should be accepted or denied by a firewall policy in the same way by either FortiGate device in this topology.

Which FortiOS CLI configuration can help reduce the administrative effort required to maintain the FortiGate devices, by synchronizing firewall policy and object configuration between the FortiGate devices?

A. `config system sdn-connector`
B. `config system ha`
C. `config system auto-scale`
D. `config system session-sync`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/84777/using-standalone-configuration-synchronization