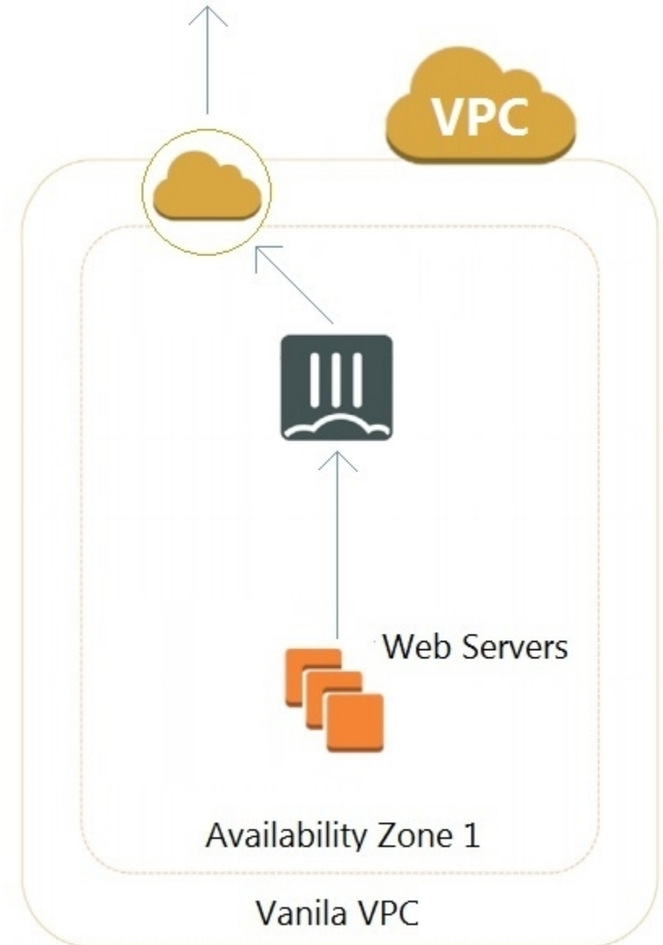
Number: NSE7_PBC-7.2
Passing Score: 800.0
Time Limit: 120.0
File Version: 4.0

Exam Code: NSE7_PBC-7.2

Exam Name: Fortinet NSE 7 - Public Cloud Security 7.2

Exam A

QUESTION 1
Refer to the exhibit.



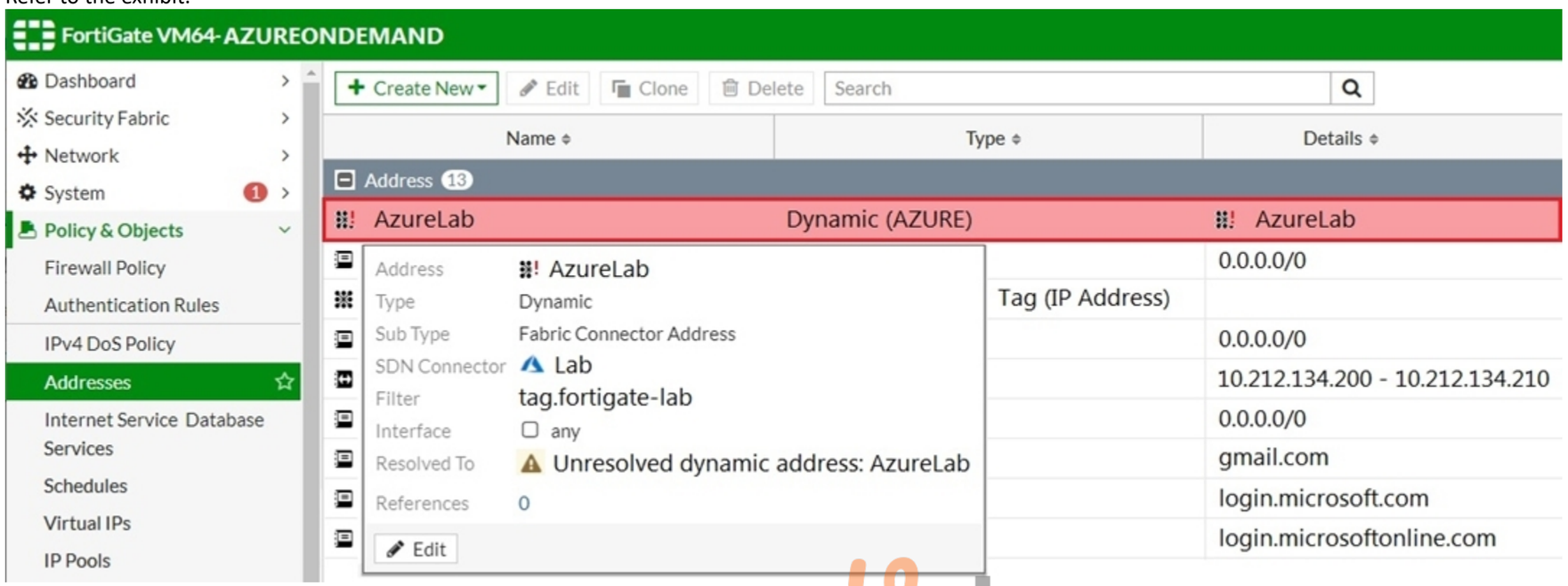
A customer has deployed an environment in Amazon Web Services (AWS) and is now trying to send outbound traffic from the Web servers to the Internet. The FortiGate policies are configured to allow all outbound traffic; however, the traffic is not reaching the FortiGate internal interface.
What are two 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: C, D
Section:
Explanation:

You need to check if source/destination are enabled. Public_Cloud_6.4_Study_Guide Page 67

QUESTION 2
Refer to the exhibit.

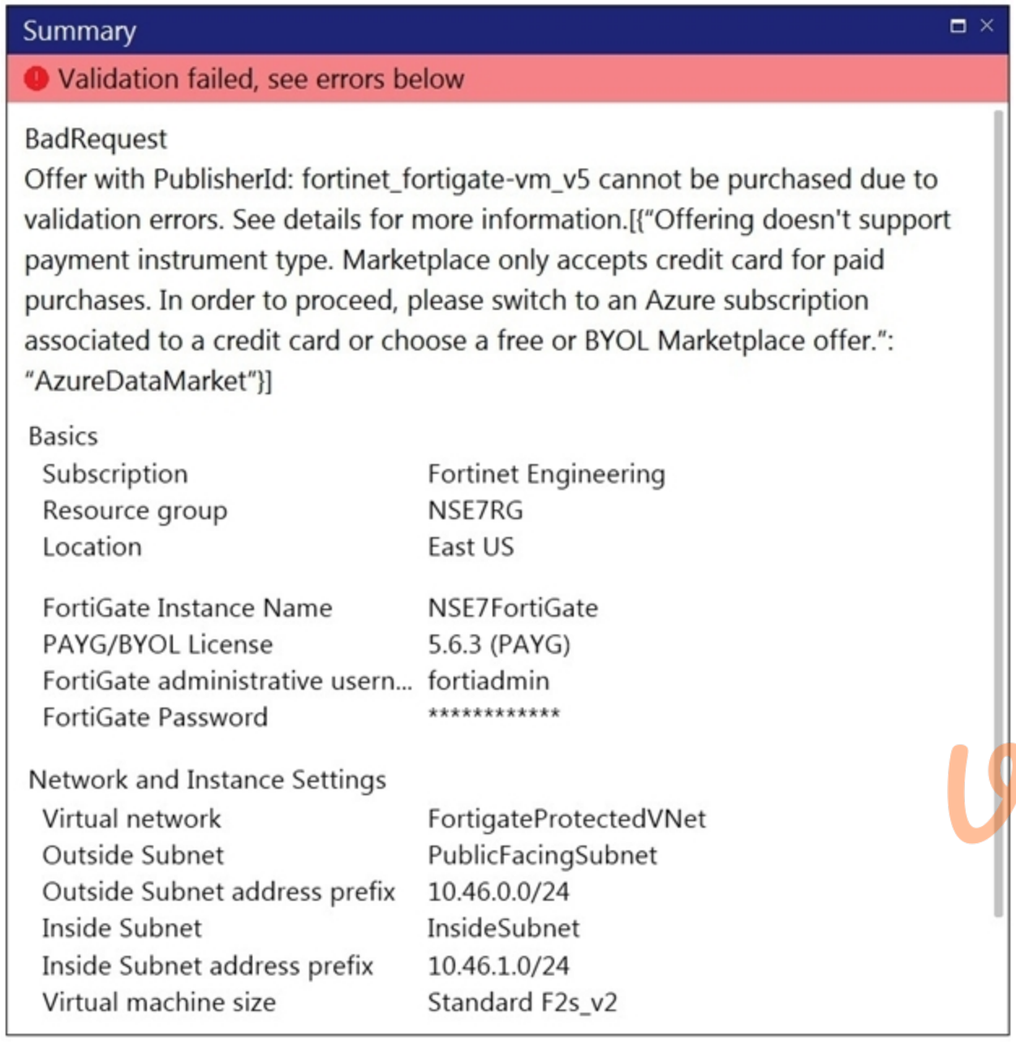


Your senior administrator successfully configured a FortiGate fabric connector with the Azure resource manager, and created a dynamic address object on the FortiGate VM to connect with a windows server in Microsoft Azure. However, there is now an error on the dynamic address object, and you must resolve 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: B
Section:
Explanation:
https://docs.fortinet.com/document/fortigate-public-cloud/6.2.0/azure-administration-guide/985498/troubleshooting-azure-fabric-connector

QUESTION 3
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: D
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources

QUESTION 4
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: C
Section:
Explanation:
Official documentation, failover process on a single AZ, https://github.com/fortinet/aws-cloudformation-templates/blob/main/FGCP/7.0/SingleAZ/README.md#failover-process || Outbound failover is provided by reassigning the secondary IP addresses of ENI1\port2 from FortiGate 1's private interface to FortiGate 2's private interface. ##Additionally any route targets referencing FortiGate 1's private interface will be updated to reference FortiGate 2's private interface.##
https://github.com/fortinet/aws-cloudformation-templates/tree/master/LambdaAA-RouteFailover/6.0

QUESTION 5
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: A, D
Section:
Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
https://aws.amazon.com/premiumsupport/knowledge-center/security-network-acl-vpc-endpoint/
-Network ACLs are stateless. You must define rules for both outbound and inbound traffic.

QUESTION 6
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 seconds
C. 20 seconds
D. 16 seconds

Correct Answer: A
Section:
Explanation:
https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview
-If your application produces a time-out response just before the next probe arrives, the detection of the events will take 5 seconds plus the duration of the application time-out when the probe arrives. You can assume the detection to take slightly over 5 seconds.
-If your application produces a time-out response just after the next probe arrives, the detection of the events won't begin until the probe arrives and times out, plus another 5 seconds. You can assume the detection to take just under 10 seconds.
Assume the reaction to a time-out response will take a minimum of 5 seconds and a maximum of 10 seconds to react to the change.

QUESTION 7
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: A, D, E
Section:
Explanation:
Under 'Default security rules' we read source, destination, source port, destination port and access. However under 'Security rules' we read action, port ranges and source and destination, and essentially Options A, C, D and E are valid are those parameters can be configured. I would mark A D and E and source/destination port are to be seen in the table, maybe old documentation. https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

QUESTION 8
Refer to the exhibit.

```
"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
  },
]
},
```

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

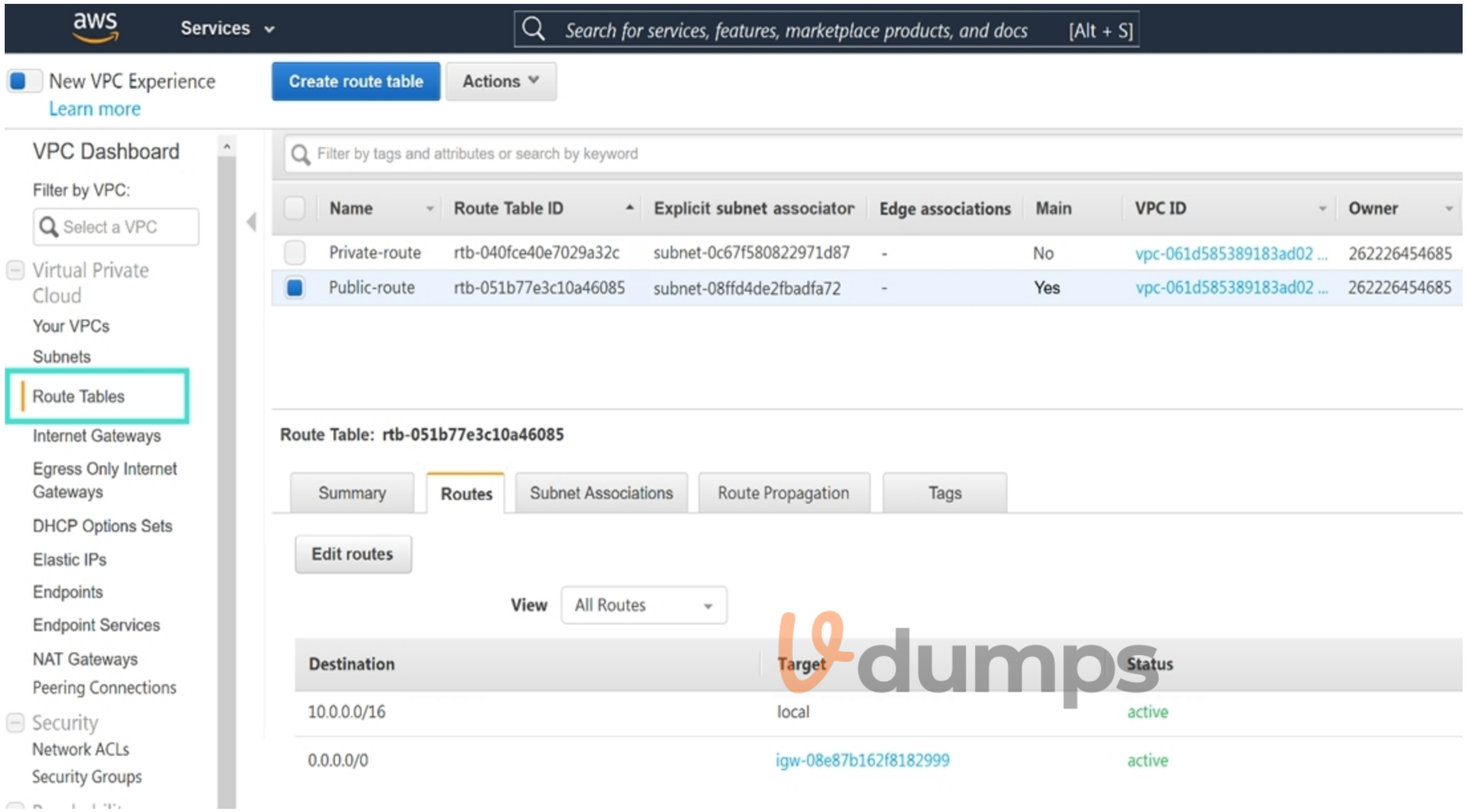
Section:
Explanation:
https://github.com/fortinet/azure-templates/blob/main/FortiGate/A-Single-VM/azuredeploy.json

QUESTION 9
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: A, D
Section:
Explanation:
You can deploy resources from several Azure services into an Azure virtual network. For a complete list, see Services that can be deployed into a virtual network. You can associate zero, or one, network security group to each virtual network subnet and network interface in a virtual machine. The same network security group can be associated to as many subnets and network interfaces as you choose. https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

QUESTION 10
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: D
Section:
Explanation:
AWS NAT gateway allows instances in a private subnet to connect to the internet or other AWS services without using NAT instance. the main routing table sends internet traffic from the private subnet instances to the NAT gateway, then NAT gateway sends traffic to the IGW using the source IP address of the elastic IP address.
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.

QUESTION 11

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: B
Section:
Explanation:
-The maximum bandwidth per 'VPC attachment', AWS Direct Connect gateway, or peered transit gateway connection Up to 50 Gbps https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-quotas.html with Transit Gateway, Maximum bandwidth (burst) per Availability Zone per VPC connection is 50 Gbps. VPC peering has no aggregate bandwidth. Individual instance network performance limits and flow limits (10 Gbps within a placement group and 5 Gbps otherwise) apply to both options. Only VPC peering supports placement groups.
Reference: https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf

QUESTION 12
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:

QUESTION 13
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: A, B, C
Section:

QUESTION 14
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: A
Section:
Explanation:
From the resource group Overview page, click the external load balancer name to load it. From the navigation column, click Inbound NAT Rules. https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/azure-administration-guide/889158/connecting-to-the-fortigate-vm-instances
https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-networking#azure-virtual-machine-scale-sets-with-azure-load-balancer it is more economical and secure to associate a public IP address to a load balancer or to an individual virtual machine (also known as a jumpbox), which then routes incoming connections to scale set virtual machines as needed (for example, through inbound NAT rules).

QUESTION 15
Refer to the exhibit.

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

SSTENTAZFGT-0302 #
```

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: A, B
Section:

QUESTION 16
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: C, D
Section:
Explanation:
Multi-VPC design. AWS recommends segmenting networks at the VPC level. In this approach, workloads are grouped together at the VPC level instead of the subnet level. All traffic between VPCs will be inspected by network security virtual firewalls at each VPC or at a shared VPC. Design patterns such as Transit VPC or AWS Transit Gateway can be used to achieve this in an automated and scalable fashion.