



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 1

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 2

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 3

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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.

Show Suggested Answer

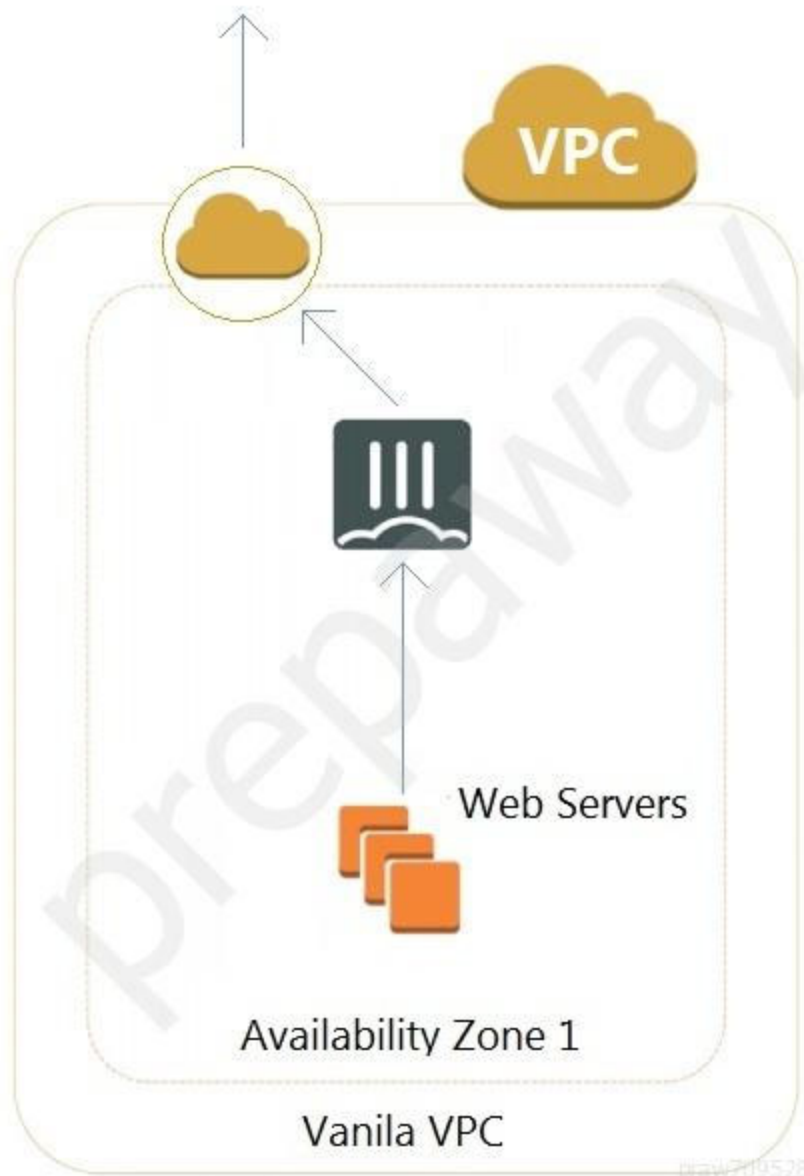


Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 4

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)



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.

Show Suggested Answer

Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 5

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

The screenshot shows the FortiGate VM64-AZUREONDEMAND management interface. The left sidebar shows the navigation menu with 'Policy & Objects' expanded and 'Addresses' selected. The main content area displays a table of address objects. The 'AzureLab' object is highlighted in red, indicating an error. A modal window is open for the 'AzureLab' object, showing its configuration details. The 'Resolved To' field contains a warning icon and the text 'Unresolved dynamic address: AzureLab'. The 'References' field shows '0'.

Name	Type	Details
AzureLab	Dynamic (AZURE)	AzureLab
Address	AzureLab	0.0.0.0/0
Type	Dynamic	Tag (IP Address)
Sub Type	Fabric Connector Address	0.0.0.0/0
SDN Connector	Lab	10.212.134.200 - 10.212.134.210
Filter	tag.fortigate-lab	0.0.0.0/0
Interface	any	gmail.com
Resolved To	Unresolved dynamic address: AzureLab	login.microsoft.com
References	0	login.microsoftonline.com

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?

- Run diagnose debug application azd -l on FortiGate.
- In the Microsoft Azure portal, set the correct tag values for the windows server.
- 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.
- Delete the address object and recreate a new address object with the type set to FQDN.

Show Suggested Answer

Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 6

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

**Summary**

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 7

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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.

Show Suggested Answer





Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 8

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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.

Show Suggested Answer







Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 9

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 10

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 11

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

```
207     "osDisk": {
208         "osType": "Linux",
209         "name": "sstentazfgt0402build3232disk01",
210         "caching": "ReadWrite",
211         "createOption": "Empty",
212         "managedDisk": {
213             "storageAccountType": "Standard_LRS"
214         },
215         "diskSizeGB": 2
216     },
217     "dataDisks": [
218         {
219             "lun": 0,
220             "name": "sstentazfgt0402build3232disk02",
221             "createOption": "Empty",
222             "caching": "None",
223             "managedDisk": {
224                 "storageAccountType": "Standard_LRS"
225             },
226             "diskSizeGB": 30
227         }
228     ]
229 },
```

praw709528

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 12

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 13

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

The screenshot shows the AWS Management Console interface for configuring a VPC. The 'Route Tables' section is active, and the 'Public-route' (rtb-051b77e3c10a46085) is selected. The 'Routes' tab is open, displaying a table of routes for this route table.

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?

- 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.
- 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.
- 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.
- 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.

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 14

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 15

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 16

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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.

Show Suggested Answer







Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 17

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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.

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 18

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

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 #
```

praw709528

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 19

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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

Show Suggested Answer





Actual exam question from Fortinet's NSE7\_PBC-6.4

Question #: 20

Topic #: 1

[\[All NSE7\\_PBC-6.4 Questions\]](#)

---

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.

Show Suggested Answer

