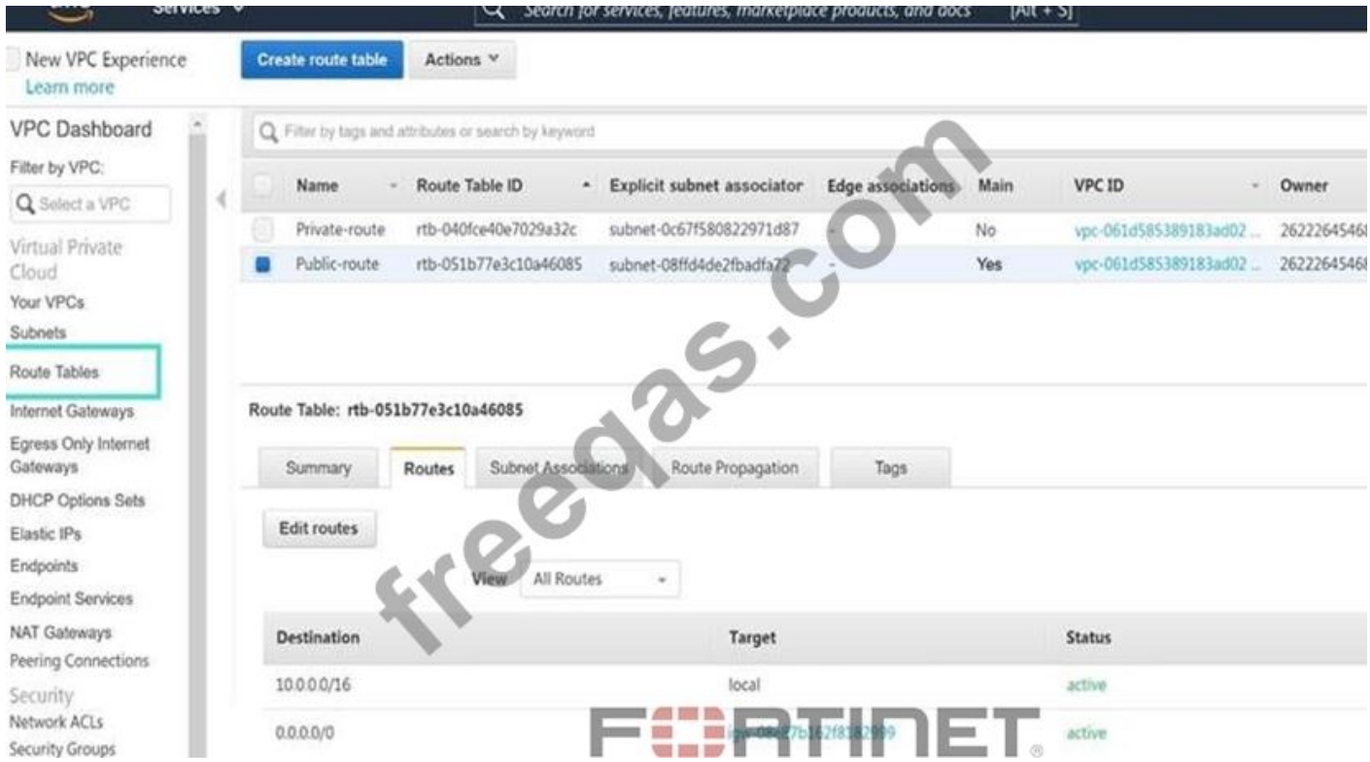
Fortinet.NSE7_PBC-6.4.v2022-04-09.q15

Exam Code:	NSE7_PBC-6.4
Exam Name:	Fortinet NSE 7 - Public Cloud Security 6.4
Certification Provider:	Fortinet
Free Question Number:	15
Version:	v2022-04-09
# of views:	820
# of Questions views:	150
https://www.freeqas.com/qa/Fortinet/NSE7_PBC-6.4/Fortinet.NSE7_PBC-6.4.v2022-04-09.q15.html	

NEW QUESTION: 1
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 cannot create and add additional vNICs to an existing FortiGate-VM.
B. They can use the Compute Engine API Explorer.
C. They can create additional vNICs in the UI console.
D. They can create additional vNICs using the Cloud Shell.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
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 route tables, select Private-route, and add a new route destination 0.0.0.0/0 to the target internet 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 public subnet, edit route tables, select Private-route and add a new route destination 0.0.0.0/0 to target the NAT gateway.

D. 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.

Answer: (SHOW ANSWER)

NEW QUESTION: 3

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

Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

NEW QUESTION: 4
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. Deploy and configure FortiCWP with a workload guardian license.
C. Configure FortiCASB and set up access rights, privileges, and data protection policies.
D. Deploy and configure FortiGate with Security Fabric solutions, and FortiCWP with a storage guardian advance license.
E. Use FortiGate, FortiGuard, and FortiAnalyzer solutions.
Answer: A,C,E (LEAVE A REPLY)

NEW QUESTION: 5
What is the bandwidth limitation of an Amazon Web Services (AWS) transit gateway VPC attachment?
A. Up to 10 Gbps per attachment
B. Up to 1 Gbps per attachment
C. Up to 50 Gbps per attachment
D. Up to 1.25 Gbps per attachment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
Which statement about FortiSandbox in Amazon Web Services (AWS) is true?
A. FortiSandbox in AWS can have a maximum of eight virtual machines (VMs) that inspect files.
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. In AWS, virtual machines (VMs) that inspect files do not have to be reset after inspecting a file.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
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.

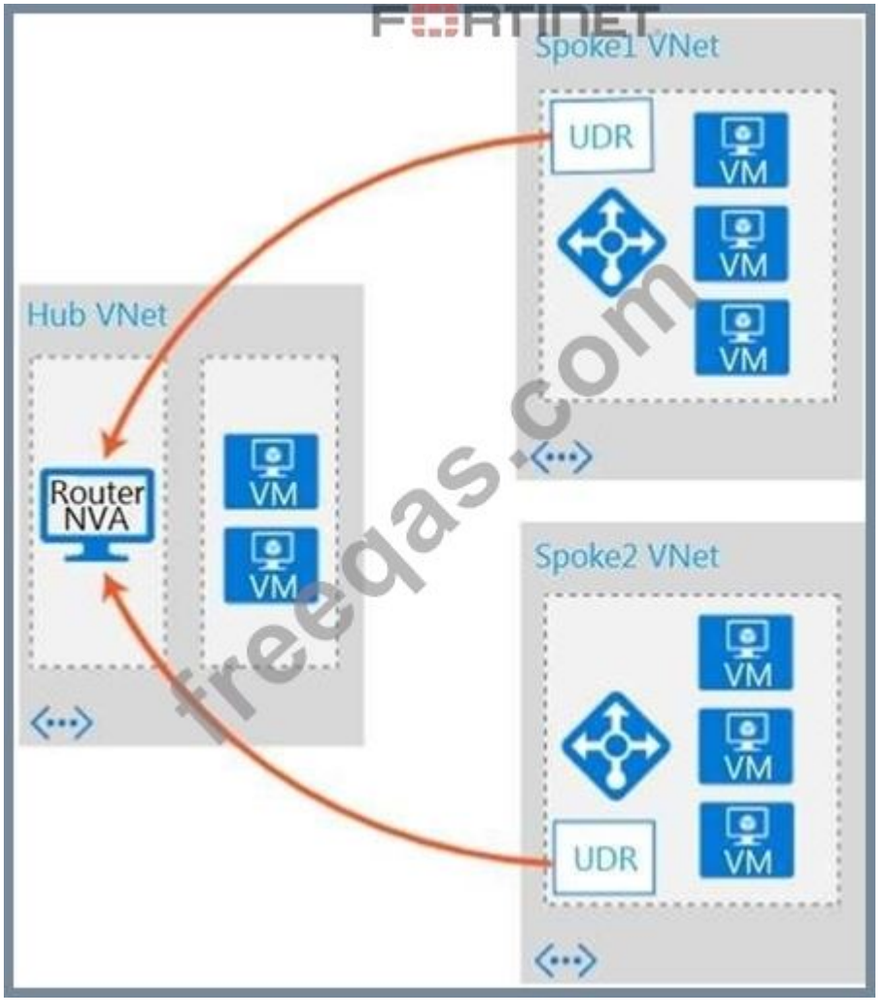
Which action will fix this issue?
A. Convert the c4.xlarge instances to m4.xlarge instances.
B. Convert the transit VPC firewalls into an auto-scaling group and launch additional EC2 instances in that group.
C. Migrate the transit VPNs to new and larger instances (VM08 / c4.2xlarge).
D. Convert from IPsec tunnels to generic routing encapsulation (GRE) tunnels, for the VPC peering connections.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
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 session-sync
B. config system sdn-connector
C. config system ha
D. config system auto-scale
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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-guarddutyscript 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.
Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 10
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
Answer: D (LEAVE A REPLY)
Explanation/Reference: https://docs.fortinet.com/document/fortigate/6.2.0/aws-cookbook/828256/connecting-to-the- fortigate-vm

NEW QUESTION: 11


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

NEW QUESTION: 12
Which three properties are configurable Microsoft Azure network security group rule settings? (Choose three.)
A. Sequence number
B. Source port ranges
C. Action
D. Destination port ranges
E. Source and destination IP ranges
Answer: (SHOW ANSWER)

NEW QUESTION: 13
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.
Answer: (SHOW ANSWER)
Explanation/Reference: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

NEW QUESTION: 14
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. One public subnet and one private subnet
C. Two public subnets and two private subnets
D. Two public subnets and one private subnet
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
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.
Answer: D (LEAVE A REPLY)