Vendor: Fortinet

Exam Code: NSE7_PBC-6.4

Exam Name: Fortinet NSE 7 - Public Cloud Security 6.4

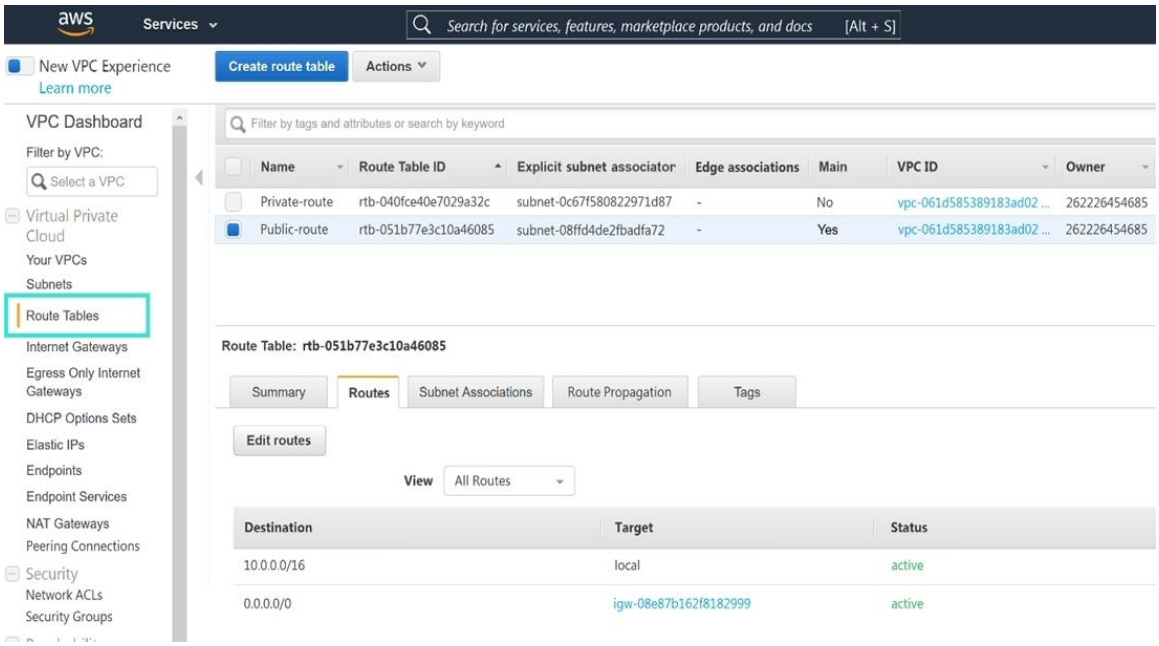
Version: DEMO

QUESTION 1
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.

Answer: AD
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 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 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.

Answer: D
Explanation:
You must put the Nat Gateway (NGW) on subnet with defult route to IGW.
And after that route the traffic from private subnet to the NGW, the nat gateway forward the traffic to IGW.

QUESTION 3
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

Answer: B
Explanation:
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 4
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.

Answer: A
Explanation:
Inbound NAT rules
These rules are applied to a specific host and are not load-balanced. As such, these are typically used for management.
https://docs.fortinet.com/document/fortigate-public-cloud/6.0.0/use-case-high-availability-for-fortigate-on-azure/224311/basic-concepts

QUESTION 5
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

Answer: A
Explanation:
- 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.
https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview

QUESTION 6
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.

Answer: B
Explanation:
AWS GuardDuty is a managed threat detection service that monitors malicious or unauthorized behaviors/ activities related to AWS resources. GuardDuty provides visibility of logs called "findings", and Fortinet provides a Lambda script called "aws-lambda-guardduty", which translates feeds from AWS GuardDuty findings into a list of malicious IP addresses in an S3 location, which a FortiGate-VM can consume as an external threat feed after being configured to point to the list's URL. To use this feature, you must subscribe to "GuardDuty, CloudWatch, S3, and DynamoDB." https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/aws-administration-guide/908646/ populating-threat-feeds-with-guardduty

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**