Fortinet

NSE6_WCS-6.4 Exam

NSE 6

Questions & Answers

(Demo Version - Limited Content)

Version: 4.0

Question: 1

An administrator has deployed an environment in AWS and is now trying to send outbound traffic from the web servers to the internet through FortiGate. The FortiGate policies are configured to allow all outbound traffic. however. the traffic is not reaching the FortiGate internal interface.

Which two statements Can be the reasons for this behavior? (Choose two)

A. FortiGate is not configured as a default gateway tor web servers.

B. Internet Gateway (IGW) is not configured for VPC.

C. AWS security groups are blocking the traffic.

D. AWS source destination checks are enabled on the FortiGate internal interfaces.

Answer: CD

Explanation:

Question: 2

You are network connectivity issues between two VMS deployed in AWS. One VM is a FortiGate located on subnet •LAN- that is part Of the VPC "Encryption". The Other VM is a Windows server located on the subnet "servers" Which is also in the "Encryption" VPC. You are unable to ping the Windows server from FortiGate.

What is the reason for this?

A. You have not created a VPN to allow traffic between those subnets.

B. By default. AWS does not allow ICMP traffic between subnets.

C. The default AWS Network Access Control List (NACL) does not allow this traffic.

D. The firewall in the Windows VM is blocking the traffic.

Answer: D

Explanation:

Question: 3

Your company deployed a FortiSandb0X for AWS.

Which statement is correct about FortiSandbox for AWS?

A. FortiSandbox for AWS does not need more resources because it performs only management and analysis tasks.

B. The FortiSandbox manager is installed on AWS platform and analyzes the results of the sandboxing process received from on-premises Windows instances.

C. FortiSandbox for AWS comes as hybrid solution. The FortiSandb0X manager is installed on-premises and analyzes the results Of the sandboxing process received from AWS EC2 instances

D. FortiSandbox deploys new EC2 instances with the custom Windows and Linux VMS, then it sends malware, runs it, and captures the results for analysis.

Answer: A

Explanation:

Question: 4

An organization has created a VPC and deployed a FortiGate-VM (VM04 /c4.xlarge) in AWS, FortiGate-VM is initially configured With two Elastic Network Interfaces
(ENIs). The primary ENI of FortiGate-VM is configured for a public subnet. and the second ENI is configured for a private subnet. In order to provide internet access. they now want to add an EIP to the primary ENI of FortiGate, but the EIP assignment is failing.

Which action would allow the EIP assignment to be successful?

A. Shut down the FortiGate VM. if it is running. assign the EIP to the primary ENI. and then power it on.

B. Create and associate a public subnet With the primary ENI Of FortiGate, and then assign the EIP to the primary ENI.

C. Create and attach a public routing table to the public subnet, associate the public subnet With the primary ENI Of FortiGate. and then assign the EP to the primary ENI.

D. Create and attach an Internet gateway to the VPC. and then assign the EIP to the primary ENI Of FortiGate.

Answer: D

Explanation:

Question: 5

HOW is traffic failover handled in a FortiGate active-active cluster deployed in AWS?

A. The elastic load balancer handles traffic failover using FGCP.

B. The elastic load balancer handles bi-directional traffic failover using a health probe.

C. All FortiGate cluster members send health probes using a dedicated interface.

D. All FortiGate cluster members use unicast FGCP_

Answer: B

Thank You for trying NSE6_WCS-6.4 PDF Demo

Start Your NSE6_WCS-6.4 Preparation