PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 6 - Cloud Security 7.0 for AWS

Fortinet NSE6_WCS-7.0

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, AWS Infrastructure	6
Topic 2, FortiGate-VM Deployment	3
Topic 3, VPC Traffic Flow	2
Topic 4, AWS Services	7
Topic 5, FortiGate-VM High Availability	1
Topic 6, FortiGate-VM Autoscaling	1
Topic 7, AWS Transit Gateway	3
Total	23

QUESTION NO: 1

An administrator is troubleshooting intermittent traffic loss between an application subnet and a FortiGate-VM interface in the same VPC. The administrator needs AWS-level evidence showing whether traffic was accepted or rejected at the network-interface level, without capturing packet contents.

Which two statements about VPC Flow Logs are correct? (Choose two.)

A. VPC Flow Logs can publish flow-log records to Amazon CloudWatch Logs or Amazon S3.

B. VPC Flow Logs record packet payloads for accepted and rejected traffic.

C. VPC Flow Logs can be enabled for a VPC, a subnet, or an individual network interface.

D. VPC Flow Logs record only traffic rejected by network ACLs.

ANSWER: A C

Explanation:

VPC Flow Logs can publish flow-log records to Amazon CloudWatch Logs or Amazon S3. The records include metadata such as source and destination addresses, ports, protocol, bytes, and the ACCEPT or REJECT action.

VPC Flow Logs do not capture packet payloads. They can be enabled for a VPC, subnet, or individual network interface, making them useful for isolating AWS network-control issues affecting a FortiGate-VM or workload.

QUESTION NO: 2

An organization has three VPCs: a workload VPC, an inspection VPC containing FortiGate-VM appliances, and a shared-services VPC. The workload VPC is peered with the inspection VPC, and the inspection VPC is peered with the shared-services VPC.

The organization wants workload traffic to reach shared services through the inspection VPC. Route tables are configured in all three VPCs, but traffic cannot traverse the two peering connections.

Which AWS solution supports this connectivity model?

A. AWS Transit Gateway

B. An additional route table associated with the inspection subnet

C. A second internet gateway attached to the inspection VPC

D. An Elastic IP address associated with each FortiGate-VM interface

ANSWER: A

Explanation:

VPC peering does not support transitive routing. A VPC cannot use one peering connection to reach another VPC through an intermediate peered VPC, even when route tables contain the intended routes.

A Transit Gateway provides a hub-and-spoke routing model in which all three VPCs can be attached to the transit gateway. Transit Gateway route tables can then direct workload-to-shared-services traffic through the inspection design as required.