FCPGoogle Cloud Security 7.6 Administrator

Fortinet FCP_GCS_AD-7.6

Version Demo

Total Demo Questions: 4

Total Premium Questions: 44

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Google Cloud infrastructure	24
Topic 2, FortiGate-VM deployment	12
Topic 3, FortiGate-VM configuration	1
Topic 4, FortiGate-VM traffic management	4
Topic 5, FortiGate-VM security	2
Topic 6, FortiGate-VM operations	1
Total	44

QUESTION NO: 1

Which architecture inspection type in Google Cloud is most closely associated with Google Cloud Interconnect?

A. Outbound north-south traffic inspection

B. Inbound north-south traffic inspection

C. Hybrid cloud inspection

D. East-west traffic inspection

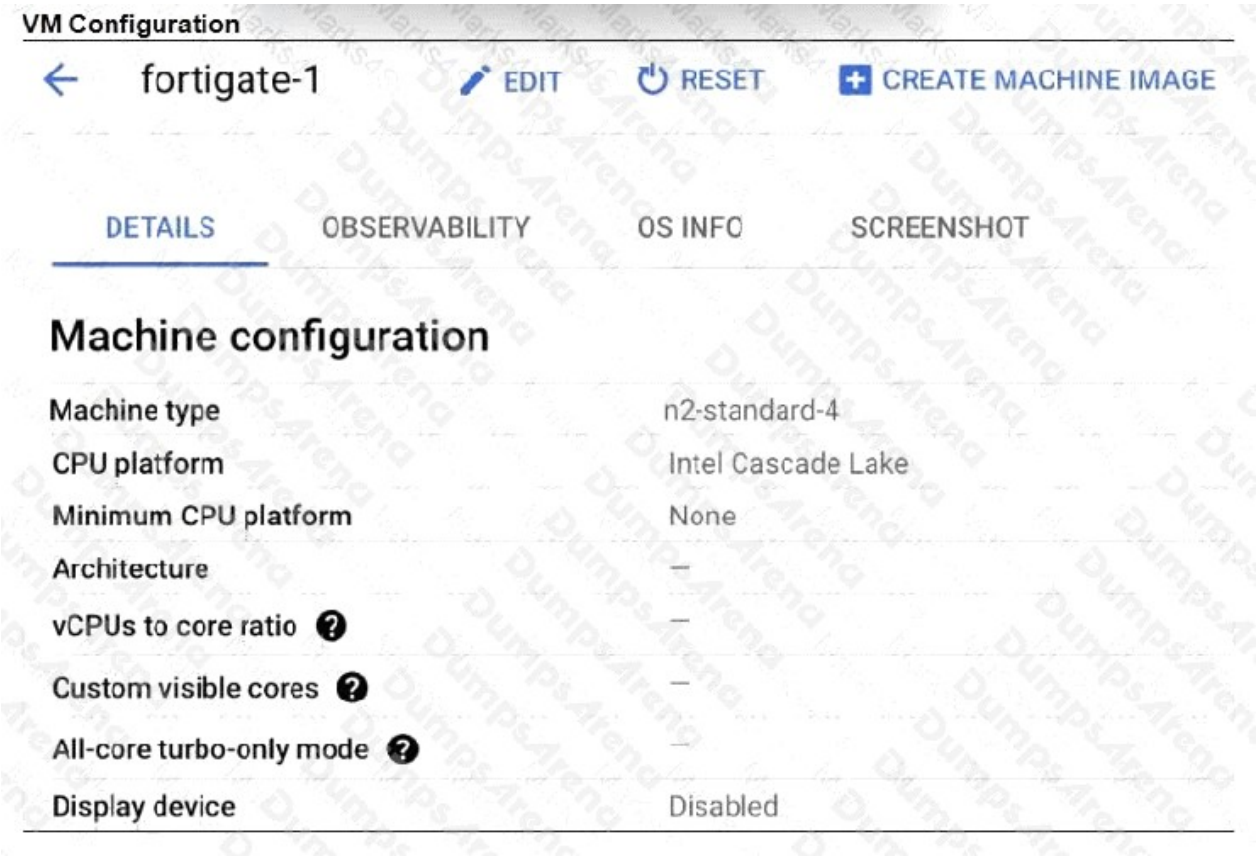
ANSWER: C

Explanation:

Hybrid cloud inspection is the inspection architecture most closely associated with Google Cloud Interconnect because Interconnect provides private, high-throughput connectivity between an on-premises environment and Google Cloud virtual private cloud networks. This creates a hybrid deployment in which traffic crosses the boundary between enterprise networks and cloud workloads. A FortiGate-VM deployed in Google Cloud can therefore be positioned to inspect, control, and log traffic exchanged over those hybrid paths, applying firewall policy and security services consistently to workloads and resources on both sides of the connection. Google Cloud describes Cloud Interconnect as extending an on-premises network to Google Cloud through a highly available, low-latency connection, which is precisely the connectivity model addressed by hybrid-cloud inspection designs. The relevant architecture focus is the secure integration of cloud and on-premises networks, including routed traffic entering or leaving Google Cloud through Interconnect attachments. See the Google Cloud Interconnect overview and Fortinet's FortiGate for Google Cloud administration guide for deployment and traffic-security context.

QUESTION NO: 2

Refer to the exhibit.



An organization has four virtual private cloud networks and deployed a FortiGate to protect the VPCs. FortiGate is configured with four network interfaces and each network interface is assigned one of the four VPCs.

The organization is expanding and plans to add two more VPCs.

Which two options can the organization use to support the two new VPCs? (Choose two.)

A. Modifying the FortiGate configuration to add two more network interfaces

B. Utilizing VPC peering

C. Deleting FortiGate and replacing it with a Google Cloud machine type that supports six network interfaces

D. Adding a second FortiGate and configuring both FortiGate devices as an active-active high-availability cluster.

ANSWER: B D

Explanation:

Utilizing VPC peering is a valid way to extend connectivity to the additional VPC networks without requiring the existing FortiGate instance to receive a directly attached interface for every VPC. VPC Network Peering provides private IP connectivity between peered VPC networks and can exchange eligible custom routes. The organization can therefore design routing so that traffic requiring security inspection is directed through the FortiGate-connected network, while maintaining the necessary route advertisements, firewall rules, and appliance-routing design.

Adding a second FortiGate and configuring both FortiGate devices as an active-active high-availability cluster is also a scaling approach. A second FortiGate provides additional interface and traffic-processing capacity, allowing the deployment to accommodate the added VPC connectivity instead of being constrained by the original instance layout. The HA design should use consistent FortiGate policies and routing, together with the Google Cloud mechanisms required to steer traffic to the appropriate active member. This enables the security deployment to expand while retaining FortiGate inspection and resiliency. Google documents the behavior and routing considerations for VPC Network Peering, and Fortinet provides deployment guidance for FortiGate on Google Cloud.

QUESTION NO: 3

Your organization is selecting a web application firewall deployment for an internet-facing application in Google Cloud. The security team requires control of detailed WAF settings and requires the WAF to perform SSL offloading and load balancing for the protected application.

Which two requirements favor FortiWeb VM rather than FortiWeb Cloud? (Choose two.)

A. Highly customizable WAF rules and settings

B. SSL offloading and load balancing

C. A fully managed WAF service with minimal appliance administration

D. Outbound address translation for private backend instances

E. Private IP connectivity between separate VPC networks

ANSWER: A B

Explanation:

FortiWeb VM is appropriate when the organization requires appliance-level control of WAF configuration and settings, and when it requires SSL offloading and load-balancing functions in the application traffic path. The VM deployment allows the organization to operate and configure the FortiWeb appliance directly in Google Cloud.

FortiWeb Cloud is a fully managed WAF service and is appropriate when reducing infrastructure-management responsibility is the primary requirement. Cloud NAT and VPC Network Peering are networking services and do not provide web application firewall functionality.

QUESTION NO: 4

An organization hosts a public HTTPS application behind a Google Cloud external Application Load Balancer. The organization wants to block common web attacks and apply rate limiting at Google Cloud edge locations before requests reach the application backends.

Which service should the administrator use?

A. Google Cloud Armor

B. Cloud NAT

C. Cloud Router

D. Google Cloud Interconnect

ANSWER: A

Explanation:

Google Cloud Armor is designed to protect applications exposed through supported Google Cloud load balancers. A Cloud Armor security policy can apply preconfigured WAF protections, IP-based controls, and rate limiting before traffic reaches the application backends.

Cloud NAT is for outbound translation, while Cloud Router exchanges dynamic routes. FortiGate can provide firewall inspection, but Cloud Armor is the native Google Cloud service that enforces this type of edge security policy on the external Application Load Balancer.