Fortinet

FCP_GCS_AD-7.6 Exam

FCP - Google Cloud Security 7.6 Administrator

Questions & Answers
Demo

Version: 4.0

Question: 1

An administrator wants to use the FortiGate automation stitch feature to quarantine compromised hosts.

Which native Google Cloud service should the administrator integrate with FortiGate to achieve this?

A. Google Cloud Interconnect

B. Google Cloud Run functions

C. Google Cloud App_ Engine

D. Google Cloud IAM

Answer: B

Explanation:

Google Cloud Run allows you to run serverless containerized functions that can be triggered by FortiGate automation stitches to perform actions such as quarantining compromised hosts. It is the native service best suited for automating responses in cloud environments.

Question: 2

You have been tasked with deploying an active-active FortiGate high-availability cluster in Google Cloud.

How can you ensure that traffic will flow symmetrically?

A. Enable the layer 3 unified threat management scanning feature on FortiGate.

B. Google Cloud performs NAT on incoming traffic for external passthrough network load balancers. No action is needed.

C. There is no need to ensure traffic symmetry because FortiGate can effectively inspect asymmetric traffic.

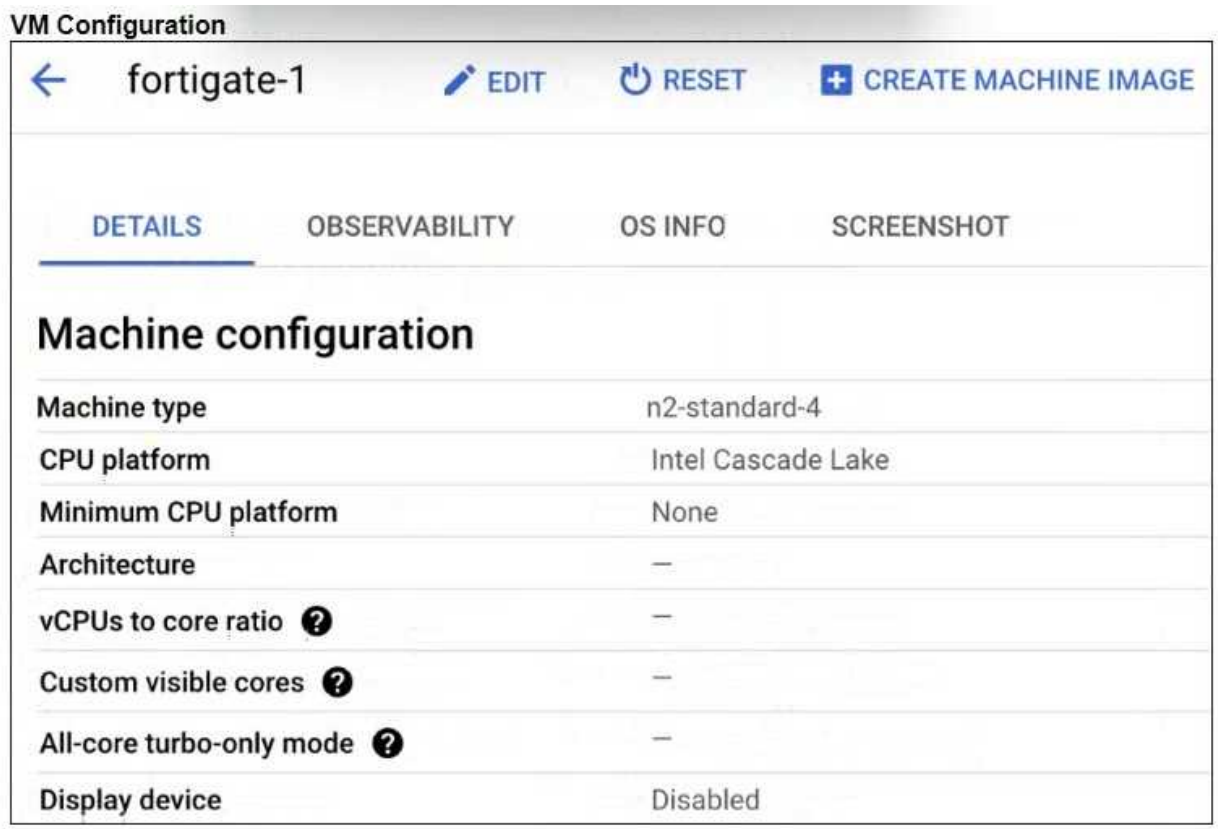
D. Deploy internal passthrough network load balancers on both sides of the cluster they support symmetric hashing.

Answer: D

Explanation:

Question: 3

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:

VPC peering allows connectivity between multiple VPCs without needing additional interfaces on FortiGate, enabling the existing FortiGate to protect multiple VPCs beyond its physical interface limits.

Adding a second FortiGate and configuring active-active HA enables scaling network protection for more VPCs by distributing traffic across multiple FortiGate instances, overcoming the network interface limit per VM.

Question: 4

An organization is deploying an active-passive high availability (HA) cluster using passthrough load balancers in Google Cloud.

What is a critical factor for ensuring successful HA formation, failover, and traffic flow?

A. Unicast FortiGate Clustering Protocol (FGCP) must be used.

B. VDOM exceptions must be configured.

C. Incoming traffic must be source NATed to ensure traffic flow symmetry.

D. There can be more than two cluster members.

Answer: C

Explanation:

Source NAT ensures that traffic is symmetric by keeping the source IP consistent, which is critical for

proper failover and session synchronization in an active-passive HA cluster using passthrough load balancers.

Question: 5

Refer to the exhibit.

Diagnose output

```
passive # diagnose debug application gcpd -1
passive # diagnose debug enable

...

passive # HA event
eip cluster-ip-vpm(34.68.13.24) is attached in remote instance: us-central1-c/fgt-vpm, should be moved to local
[pid 9000]: failover eip: cluster-ip-vpm(34.68.13.24)
[pid 9000]: get nics info for instance fgt-vpm
[pid 9000]: get instance nic: nic0, 172.16.0.2, vpc-vpm, accessConfig(external-nat), eip(34.68.13.24), tier(PREMIUM)
[pid 9000]: get instance nic: nic1, 172.16.1.2, vpc2-vpm
[pid 9000]: get instance nic: nic2, 172.16.2.2, vpc3-vpm, accessConfig(external-nat), eip(34.66.4.139), tier(PREMIUM)
[pid 9000]: nic0 of instance fgt-vpm is using eip 34.68.13.24
[pid 9000]: remove eip 34.68.13.24 from instance fgt-vpm(nic0).
gcpd checking route: internal-route-vpm
failover route: internal-route-vpm, move next hop from 172.16.1.2 to 172.16.1.3
[pid 9004]: failover route: internal-route-vpm
[pid 9004]: remove route internal-route-vpm on next hop 172.16.1.2
gcpd checking forwardrule: fgt-forwarding-rule
failover forwardrule: fgt-forwarding-rule, move target from fgt-target-vpm to fgt-target2-vpm
[pid 9006]: failover forwardrule: fgt-forwarding-rule
[pid 9006]: set target forwardrule fgt-forwarding-rule point to target instance fgt-target2-vpm
[pid 9004]: route internal-route-vpm is updated to next hop 172.16.1.3 successfully.
[pid 9000]: attach eip 34.68.13.24 to instance fgt-2-vpm(nic0).
[pid 9000]: eip cluster-ip-vpm(34.68.13.24) is attached to local successfully.
[pid 9006]: forwardrule fgt-forwarding-rule is updated to next hop fgt-target2-vpm successfully.
==== gcpd ha failover exit ====
```

An administrator is troubleshooting an issue when a high-availability (HA) failover occurs.

Which conclusion can you draw from the debug output?

A. The HA cluster is accessible using HTTPS on 34.68.13.24 and 34.66.4.139.

B. The health check has successfully updated the internal custom route to forward all internal traffic to 172.16.1.3.

C. Both cluster members are located in the same zone.

D. The HA cluster is deployed using the software-defined network (SDN) connector.

Answer: B

Explanation:

The debug output shows the internal route being updated and moved to the new next hop (172.16.1.3), indicating the health check and failover process successfully redirected internal traffic to the active HA node.