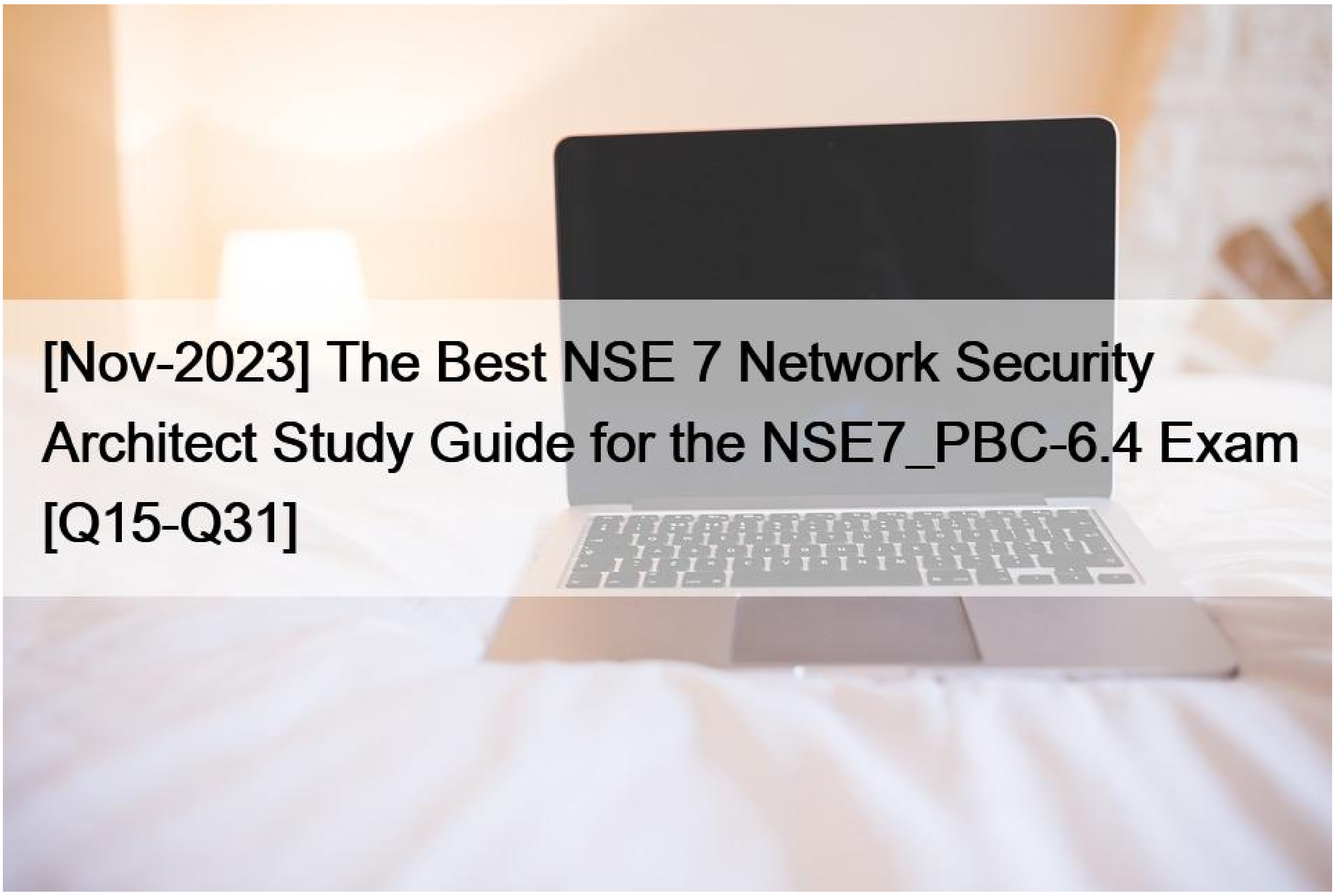
[Nov-2023 The Best NSE 7 Network Security Architect Study Guide for the NSE7_PBC-6.4 Exam [Q15-Q31



[Nov-2023] The Best NSE 7 Network Security Architect Study Guide for the NSE7_PBC-6.4 Exam

NSE7_PBC-6.4 certification guide Q&A from Training Expert ValidBraindumps Q15. Which two statements about Amazon Web Services (AWS) networking are correct? (Choose two.)

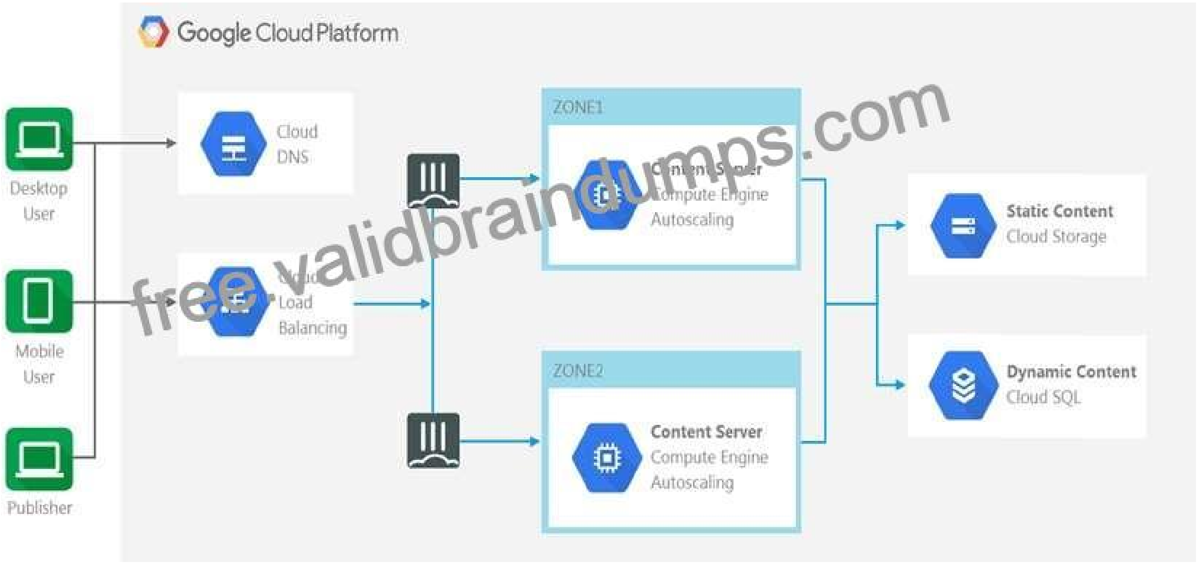
* Proxy ARP entries are disregarded.

* 802.1q VLAN tags are allowed inside the same virtual private cloud.

* AWS DNS reserves the first host IP address of each subnet.

* Multicast traffic is not allowed.

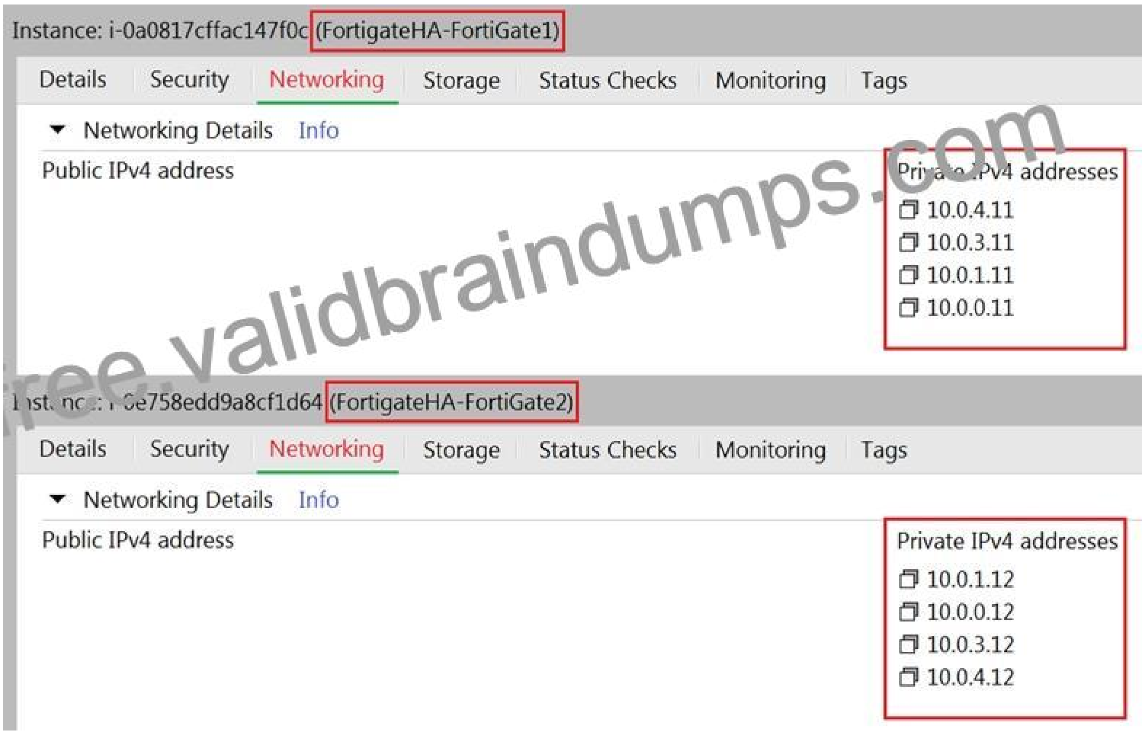
Q16.



Refer to the exhibit. The exhibit shows a topology where multiple connections from clients to the same FortiGate-VM instance, regardless of the protocol being used, are required.

Which two statements are correct? (Choose two.)
* The design shows an active-active FortiGate-VM architecture.
* The Cloud Load Balancer Session Affinity setting should be changed to CLIENT_IP.
* The design shows an active-passive FortiGate-VM architecture.
* The Cloud Load Balancer Session Affinity setting should use the default value.

Q17. Refer to the exhibit.



Instance: i-0a0817cffac147f0c (FortigateHA-FortiGate1)

Details | Security | Networking | Storage | Status Checks | Monitoring | Tags

Networking Details Info

Public IPv4 address

Private IPv4 addresses
10.0.4.11
10.0.3.11
10.0.1.11
10.0.0.11

Instance: i-0e758edd9a8cf1d64 (FortigateHA-FortiGate2)

Details | Security | Networking | Storage | Status Checks | Monitoring | Tags

Networking Details Info

Public IPv4 address

Private IPv4 addresses
10.0.1.12
10.0.0.12
10.0.3.12
10.0.4.12

You are configuring an active-passive FortiGate clustering protocol (FGCP) HA configuration in a single availability zone in Amazon Web Services (AWS), using a cloud formation template.

After deploying the template, you notice that the AWS console has IP information listed in the FortiGate VM firewalls in the HA configuration. However, within the configuration of FortiOS, you notice that port1 is using an IP of 10.0.0.13, and port2 is using an IP of 10.0.1.13.

What should you do to correct this issue?
* Configure FortiOS to use static IP addresses with the IP addresses reflected in the ENI primary IP address configuration (as per the exhibit).
* Delete the deployment and start again. You have in put the wrong parameters during the cloud formation template deployment.
* Configure FortiOS to use DHCP so that it will get the correct IP addresses on the ports.
* Nothing, in AWS cloud, it is normal for a FortiGate ENI primary IP address to be different than the FortiOS IP address configuration.

Q18. You have been tasked with deploying FortiGate VMs in a highly available topology on the Amazon Web Services (AWS) cloud. The requirements for your deployment are as follows:

*You must deploy two FortiGate VMs in a single virtual private cloud (VPC), with an external elastic load balancer which will distribute ingress traffic from the internet to both FortiGate VMs in an active-active topology.

*Each FortiGate VM must have two elastic network interfaces: one will connect to a public subnet and other will connect to a private subnet.

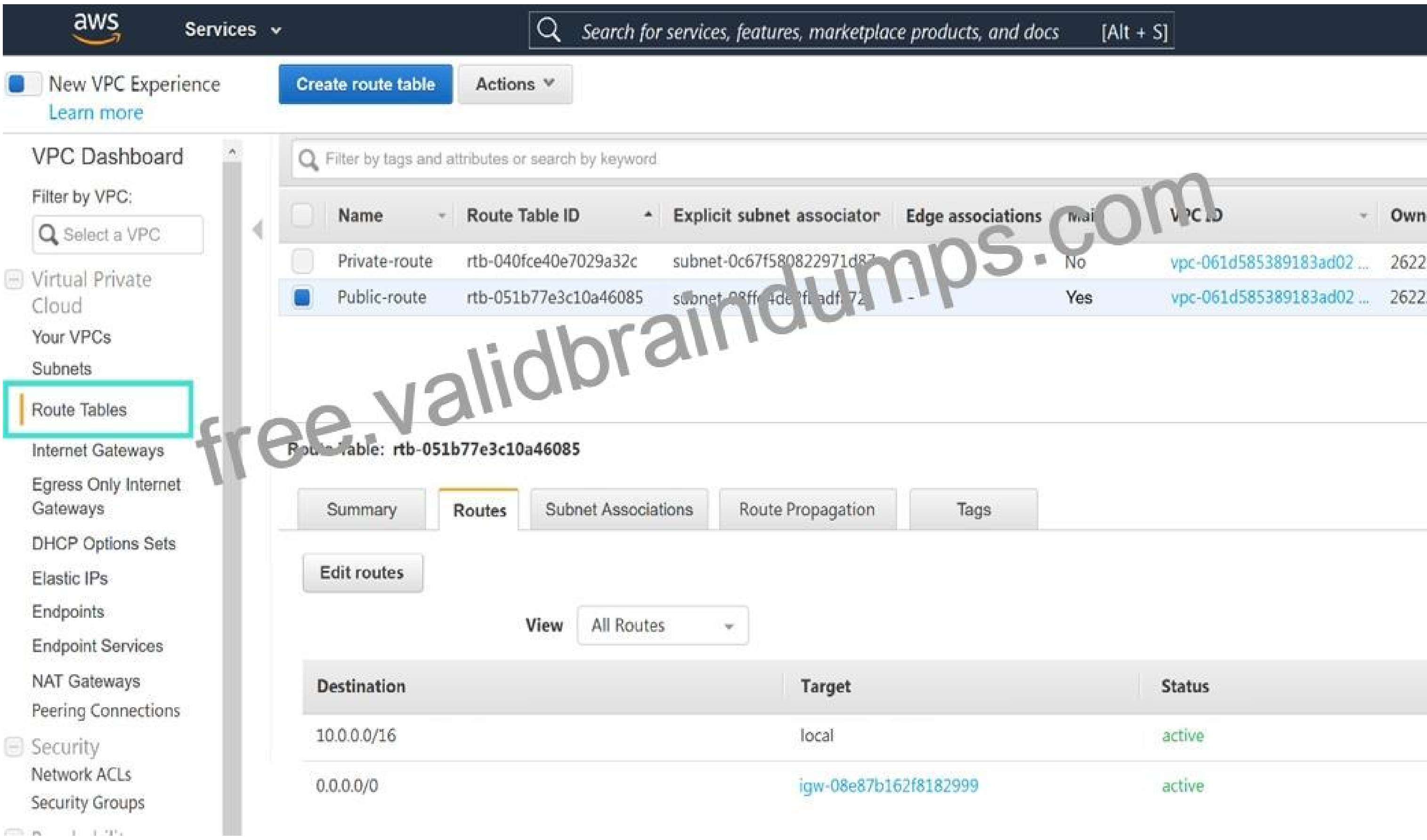
*To maintain high availability, you must deploy the FortiGate VMs in two different availability zones.

How many public and private subnets will you need to configure within the VPC?
* One public subnet and two private subnets
* Two public subnets and one private subnet
* Two public subnets and two private subnets
* One public subnet and one private subnet
Explanation

https://github.com/fortinet/aws-cloudformation-templates/blob/master/LambdaAA-RouteFailover/6.0/README

https://github.com/fortinet/aws-cloudformation-templates/tree/master/LambdaAA-RouteFailover/6.0

Q19. Refer to the exhibit.



	Name	Route Table ID	Explicit subnet associatior	Edge associations	Mai	VPC ID	Own
□	Private-route	rtb-040fce40e7029a32c	subnet-0c67f580822971d87	-	No	vpc-061d585389183ad02 ...	2622
☑	Public-route	rtb-051b77e3c10a46085	subnet-08ff[illegible]	-	Yes	vpc-061d585389183ad02 ...	2622

Route Table: rtb-051b77e3c10a46085

Destination	Target	Status
10.0.0.0/16	local	active
0.0.0.0/0	igw-08e87b162f8182999	active

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?
* 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.
* 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.
* 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.
* 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.

Q20. An organization deploys a FortiGate-VM (VM04 / c4.xlarge) in Amazon Web Services (AWS) and configures two elastic network interfaces (ENIs). Now, the same organization wants to add additional ENIs to support different workloads in their environment.

Which action can you take to accomplish this?
* None, you cannot create and add additional ENIs to an existing FortiGate-VM.
* Create the ENI, shut down FortiGate, attach the ENI to FortiGate, and then start FortiGate.

* Create the ENI, attach it to FortiGate, and then restart FortiGate.
* Create the ENI and attach it to FortiGate.
Explanation

https://docs.fortinet.com/document/fortigate-public-cloud/6.2.0/aws-administration-guide/903457 AWS says that you can attach a network interface to an instance when it&#8217;s running (hot attach), when it&#8217;s stopped (warm attach), or when the instance is being launched (cold attach). It applies to windows:

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/best-practices-for-configuring-network-interfaces

Q21. What is the bandwidth limitation of an Amazon Web Services (AWS) transit gateway VPC attachment?
* Up to 1.25 Gbps per attachment
* Up to 50 Gbps per attachment
* Up to 10 Gbps per attachment
* Up to 1 Gbps per attachment
Explanation/Reference: https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf (5)

Q22. An organization deployed a FortiGate-VM in the Google Cloud Platform and initially configured it with two vNICs. Now, the same organization wants to add additional vNICs to this existing FortiGate-VM to support different workloads in their environment.

How can they do this?
* They can create additional vNICs using the Cloud Shell.
* They cannot create and add additional vNICs to an existing FortiGate-VM.
* They can create additional vNICs in the UI console.
* They can use the Compute Engine API Explorer.
Explanation

GCP Limitations: You cannot add or remove network interfaces from an existing VM.

https://cloud.google.com/vpc/docs/create-use-multiple-interfaces#limitations

Q23. Which three properties are configurable Microsoft Azure network security group rule settings? (Choose three.)
* Action
* Sequence number
* Source and destination IP ranges
* Destination port ranges
* Source port ranges
Explanation/Reference: https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Q24. What is the bandwidth limitation of an Amazon Web Services (AWS) transit gateway VPC attachment?
* Up to 1.25 Gbps per attachment
* Up to 50 Gbps per attachment
* Up to 10 Gbps per attachment
* Up to 1 Gbps per attachment

Q25. Which three properties are configurable Microsoft Azure network security group rule settings? (Choose three.)
* Action
* Sequence number
* Source and destination IP ranges

* Destination port ranges
* Source port ranges
Explanation

Under &#8220;Default security rules&#8221; we read source, destination, source port, destination port and access. However under &#8220;Security rules&#8221; we read action, port ranges and source and destination, and essentially Options A, C, D and E are valid are those parameters can be configured. I would mark A D and E and source/destination port are to be seen in the table, maybe old documentation.

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Q26. 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?
* Less than 10 seconds
* 30 seconds
* 20 seconds
* 16 seconds
Explanation

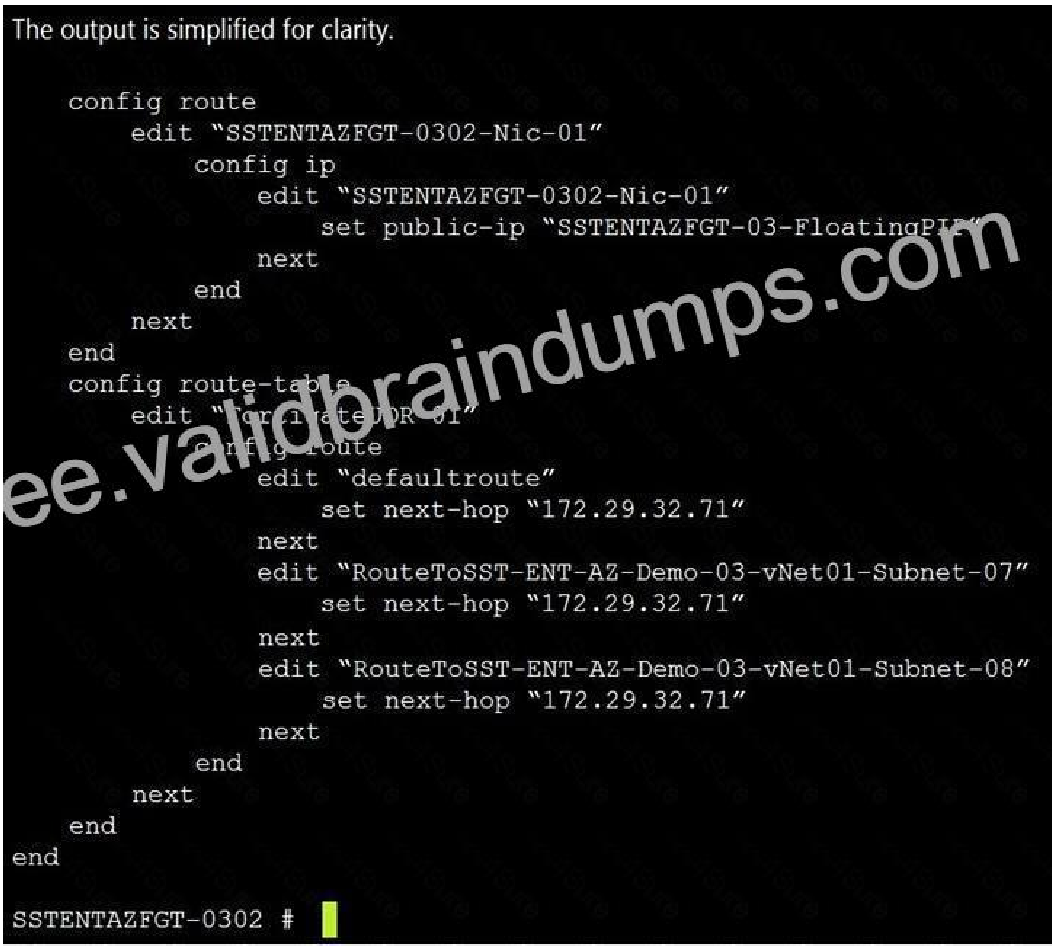
https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview

-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&#8217;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.

Q27. Refer to the exhibit.



The output is simplified for clarity.

```
    config route
        edit “SSTENTAZFGT-0302-Nic-01”
            config ip
                edit “SSTENTAZFGT-0302-Nic-01”
                    set public-ip “SSTENTAZFGT-03-FloatingPIP”
                next
            end
        next
    end
    config route-table
        edit “FortigateUDR-01”
            config route
                edit “defaultroute”
                    set next-hop “172.29.32.71”
                next
                edit “RouteToSST-ENT-AZ-Demo-03-vNet01-Subnet-07”
                    set next-hop “172.29.32.71”
                next
                edit “RouteToSST-ENT-AZ-Demo-03-vNet01-Subnet-08”
                    set next-hop “172.29.32.71”
                next
            end
        next
    end
end

SSTENTAZFGT-0302 #
```

Consider an active-passive HA deployment in Microsoft Azure. The exhibit shows an excerpt from the passive FortiGate-VM node.

If the active FortiGate-VM fails, what are the results of the API calls made by the FortiGate named SSTENTAZFGT-0302? (Choose two.)

* SSTENTAZFGT-03-FloatingPIP is assigned to the IP configuration with the name SSTENTAZFGT-

0302-Nic-01, under the network interface SSTENTAZFGT-0302-Nic-01

* 172.29.32.71 is set as a next hop IP for all routes under FortigateUDR-01

* The network interface of the active unit moves to itself

* SSTENTAZFGT-03-FloatingPIP public IP is assigned to NIC SSTENTAZFGT-0302-Nic-01

Q28. You need to deploy FortiGate VM devices in a highly available topology in the Microsoft Azure cloud. The following are the requirements of your deployment:

* Two FortiGate devices must be deployed; each in a different availability zone.

* Each FortiGate requires two virtual network interfaces: one will connect to a public subnet and the other will connect to a private subnet.

* An external Microsoft Azure load balancer will distribute ingress traffic to both FortiGate devices in an active- active topology.

* An internal Microsoft Azure load balancer will distribute egress traffic from protected virtual machines to both FortiGate devices

in an active-active topology.

* Traffic should be accepted or denied by a firewall policy in the same way by either FortiGate device in this topology.

Which FortiOS CLI configuration can help reduce the administrative effort required to maintain the FortiGate devices, by synchronizing firewall policy and object configuration between the FortiGate devices?
* config system sdn-connector
* config system ha
* config system auto-scale
* config system session-sync

Q29. When configuring the FortiCASB policy, which three configuration options are available? (Choose three.)
* Intrusion prevention policies
* Threat protection policies
* Data loss prevention policies
* Compliance policies
* Antivirus policies

Q30. A company deployed a FortiGate-VM with an on-demand license using Amazon Web Services (AWS) Market Place Cloud Formation template. After deployment, the administrator cannot remember the default admin password.

What is the default admin password for the FortiGate-VM instance?
* The admin password cannot be recovered and the customer needs to deploy the FortiGate-VM again.
* <blank>
* admin
* The instance-ID value

Q31. When configuring the FortiCASB policy, which three configuration options are available? (Choose three.)
* Intrusion prevention policies
* Threat protection policies
* Data loss prevention policies
* Compliance policies
* Antivirus policies
Explanation

Policy setting allows you to configure each policy to fit the need of your usage. You can select any type of Policy (Data Analysis, Threat Protection or Compliance)

https://docs.fortinet.com/document/forticasb/20.1.0/online-help/482958/policy-configuration

The Best Fortinet NSE7_PBC-6.4 Study Guides and Dumps of 2023:
https://www.validbraindumps.com/NSE7_PBC-6.4-exam-prep.html]