NSE8_812 Q&As

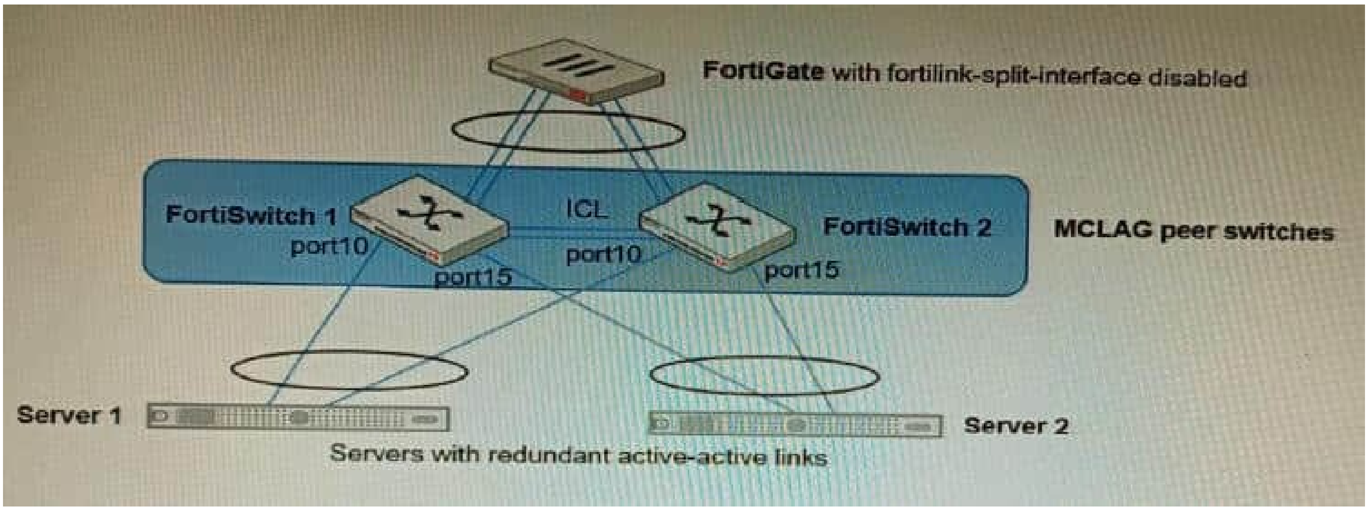
Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Refer to the exhibit.


FortiGate with fortilink-split-interface disabled
FortiSwitch 1
port10
port15
ICL
port10
FortiSwitch 2
port15
MCLAG peer switches
Server 1
Server 2
Servers with redundant active-active links

You have been tasked with replacing the managed switch Forti Switch 2 shown in the topology. Which two actions are correct regarding the replacement process? (Choose two.)

A. After replacing the FortiSwitch unit, the automatically created trunk name does not change

B. CLAG-ICL needs to be manually reconfigured once the new switch is connected to the FortiGate

C. After replacing the FortiSwitch unit, the automatically created trunk name changes.

D. MCLAG-ICL will be automatically reconfigured once the new switch is connected to the FortiGate.

Correct Answer: AB

A is correct because the automatically created trunk name is based on the MAC address of the FortiSwitch unit. When the FortiSwitch unit is replaced, the MAC address will change, but the trunk name will not change. B is correct because CLAG-ICL is a manually configured link aggregation group. When the FortiSwitch unit is replaced, the CLAG-ICL configuration will need to be manually reconfigured on the new FortiSwitch unit. The other options are incorrect. Option C is incorrect because the automatically created trunk name does not change when the FortiSwitch unit is replaced. Option D is incorrect because MCLAG-ICL is a manually configured link aggregation group and will not be automatically reconfigured when the FortiSwitch unit is replaced. References: Configuring link aggregation on FortiSwitches | FortiSwitch / FortiOS 7.0.4 - Fortinet Document Library Managing FortiLink | FortiGate / FortiOS 7.0.4 - Fortinet Document Library

QUESTION 2

You want to use the MTA adapter feature on FortiSandbox in an HA-Cluster. Which statement about this solution is true?

A. The configuration of the MTA Adapter Local Interface is different than on port1.

B. The MTA adapter is only available in the primary node.

C. The MTA adapter mode is only detection mode.

D. The configuration is different than on a standalone device.

Correct Answer: B

Explanation: The MTA adapter feature on FortiSandbox is a feature that allows FortiSandbox to act as a mail transfer agent (MTA) that can receive, inspect, and forward email messages from externalsources. The MTA adapter feature can be used to integrate FortiSandbox with third-party email security solutions that do not support direct integration with FortiSandbox, such as Microsoft Exchange Server or Cisco Email Security Appliance (ESA). The MTA adapter feature can also be used to enhance email security by adding an additional layer of inspection and filtering before delivering email messages to the final destination. The MTA adapter feature can be enabled on FortiSandbox in an HA-Cluster, which is a configuration that allows two FortiSandbox units to synchronize their settings and data and provide high availability and load balancing for sandboxing services. However, one statement about this solution that is true is that the MTA adapter is only available in the primary node. This means that only one FortiSandbox unit in the HA- Cluster can act as an MTA and receive email messages from external sources, while the other unit acts as a backup node that can take over the MTA role if the primary node fails or loses connectivity. This also means that only one IP address or FQDN can be used to configure the external sources to send email messages to the FortiSandbox MTA, which is the IP address or FQDN of the primary node. References: https://docs.fortinet.com/document/fortisandbox/3.2.0/administration-guide/19662/mail- transfer-agent-mtahttps://docs.fortinet.com/document/fortisandbox/3.2.0/administration-guide/19662/high-availability-ha

QUESTION 3

You are responsible for recommending an adapter type for NICs on a FortiGate VM that will run on an ESXi Hypervisor. Your recommendation must consider performance as the main concern, cost is not a factor. Which adapter type for the NICs will you recommend?

A. Native ESXi Networking with E1000

B. Virtual Function (VF) PCI Passthrough

C. Native ESXi Networking with VMXNET3

D. Physical Function (PF) PCI Passthrough

Correct Answer: C

Explanation: The FortiGate VM is a virtual firewall appliance that can run on various hypervisors, such as ESXi, Hyper-V, KVM, etc. The adapter type for NICs on a FortiGate VM determines the performance and compatibility of the network interface cards with the hypervisor and the physical network. There are different adapter types available for NICs on a FortiGate VM, such as E1000, VMXNET3, SR-IOV, etc. If performance is the main concern and cost is not a factor, one option is to use native ESXi networking with VMXNET3 adapter type for NICs on a FortiGate VM that will run on an ESXi hypervisor. VMXNET3 is a paravirtualized network interface card that is optimized for performance in virtual machines and supports features such as multiqueue support, Receive Side Scaling (RSS), Large Receive Offload (LRO), IPv6 offloads, and MSI/MSI-X interrupt delivery. Native ESXi networking means that the FortiGate VM uses the standard virtual switch (vSwitch) or distributed virtual switch (dvSwitch) provided by the ESXi hypervisor to connect to the physical network. This option can provide high performance and compatibility for NICs on a FortiGate VM without requiring additional hardware or software components. References: https://docs.fortinet.com/document/fortigate/7.0.0/vm-installation- for-vmware-esxi/19662/installing-fortigate-vm-on-vmware- esxihttps://docs.fortinet.com/document/fortigate/7.0.0/vm-installationfor-vmware- esxi/19662/networking

QUESTION 4

SD-WAN is configured on a FortiGate. You notice that when one of the internet links has high latency the time to resolve names using DNS from FortiGate is very high.

You must ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work. What should you configure?

A. Configure local out traffic to use the outgoing interface based on SD-WAN rules with a manual defined IP associated to a loopback interface and configure an SD-WAN rule from the loopback to the DNS server.

B. Configure an SD-WAN rule to the DNS server and use the FortiGate interface IPs in the source address.

C. Configure two DNS servers and use DNS servers recommended by the two internet providers.

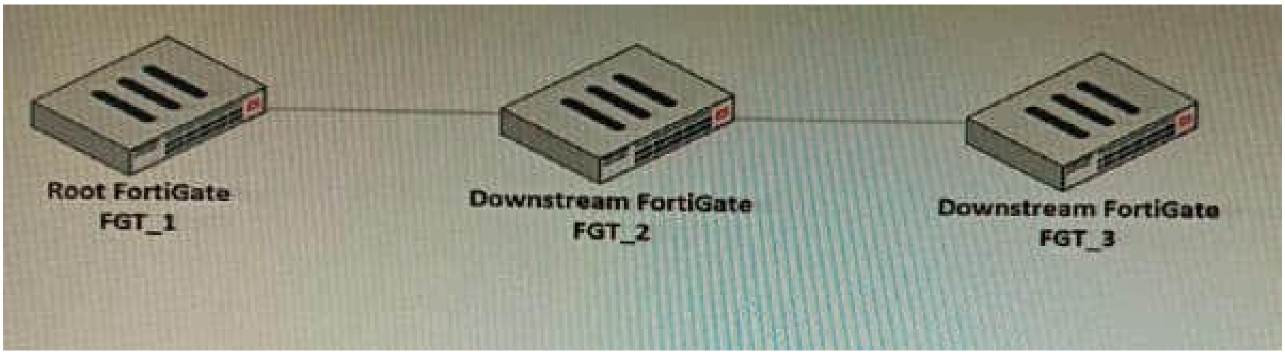
D. Configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD-WAN rule to the DNS server.

Correct Answer: D

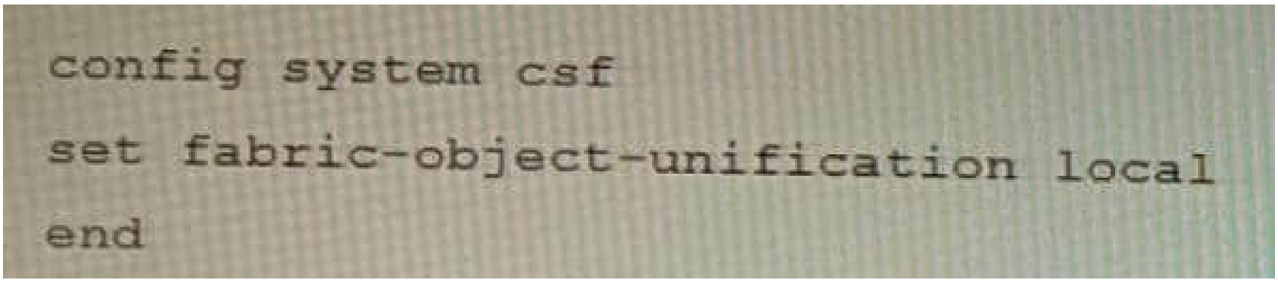
Explanation: SD-WAN is a feature that allows users to optimize network performance and reliability by using multiple WAN links and applying rules based on various criteria, such as latency, jitter, packet loss, etc. One way to ensure that the FortiGate DNS resolution times are as low as possible with the least amount of work is to configure local out traffic to use the outgoing interface based on SD-WAN rules with the interface IP and configure an SD- WAN rule to the DNS server. This means that the FortiGate will use the best WAN link available to send DNS queries to the DNS server according to the SD-WAN rule, and use its own interface IP as the source address. This avoids NAT issues and ensures optimal DNS performance. References: https://docs.fortinet.com/document/fortigate/7.0.0/sd- wan/19662/sd-wan

QUESTION 5

Refer to the exhibit.



You have deployed a security fabric with three FortiGate devices as shown in the exhibit. FGT_2 has the following configuration:



```
config system csf
set fabric-object-unification local
end
```

FGT_1 and FGT_3 are configured with the default setting. Which statement is true for the synchronization of fabric-objects?

A. Objects from the FortiGate FGT_2 will be synchronized to the upstream FortiGate.

B. Objects from the root FortiGate will only be synchronized to FGT__2.

C. Objects from the root FortiGate will not be synchronized to any downstream FortiGate.

D. Objects from the root FortiGate will only be synchronized to FGT_3.

Correct Answer: C

Explanation: The fabric-object-unification setting on FGT_2 is set to local, which means that objects will not be synchronized to any other FortiGate devices in the security fabric. The default setting for fabric-object-unification is default, which

means that objects will be synchronized from the root FortiGate to all downstream FortiGate devices. Since FGT_2 is not the root FortiGate and the fabric-object-unification setting is set to local, objects from the root FortiGate will not be

synchronized to FGT_2.

Reference:

Synchronizing objects across the Security Fabric:

https://docs.fortinet.com/document/fortigate/6.4.0/administration- guide/880913/synchronizing-objects-across-the-security-fabric