NSE8_812$^{\text{Q\&As}}$

Network Security Expert 8 Written Exam

Pass Fortinet NSE8_812 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/nse8_812.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which two statements are correct on a FortiGate using the FortiGuard Outbreak Protection Service (VOS)? (Choose two.)

A. The FortiGuard VOS can be used only with proxy-base policy inspections.

B. If third-party AV database returns a match the scanned file is deemed to be malicious.

C. The antivirus database queries FortiGuard with the hash of a scanned file

D. The AV engine scan must be enabled to use the FortiGuard VOS feature

E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database.

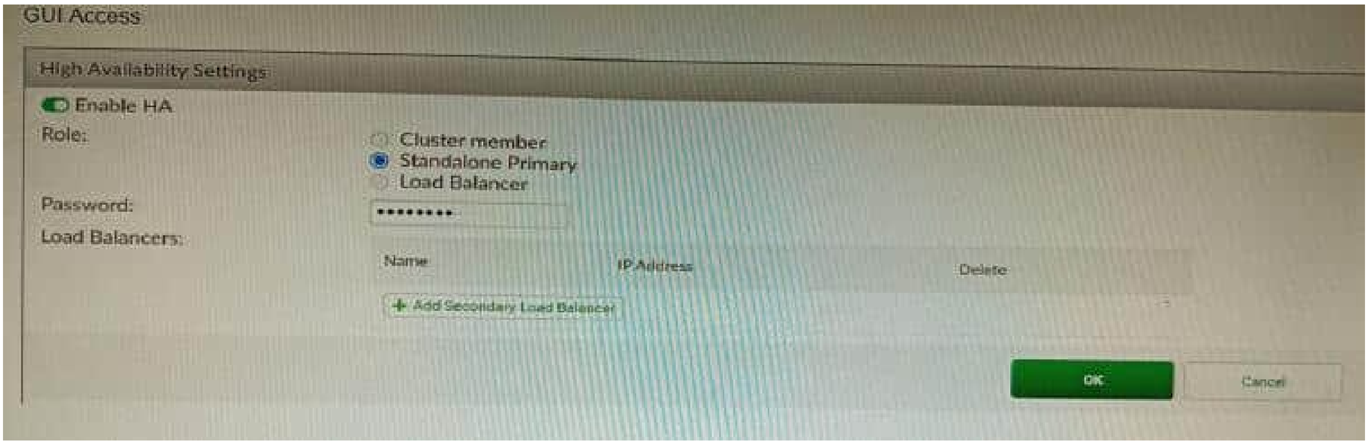
Correct Answer: CE

C. The antivirus database queries FortiGuard with the hash of a scanned file. This is how the FortiGuard VOS service works. The FortiGate queries FortiGuard with the hash of a scanned file, and FortiGuard returns a list of known malware signatures that match the hash.

E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database. This is where the FortiGuard VOS service gets its hash signatures from. The FortiGuard Global Threat Intelligence database is updated regularly with new malware signatures.

QUESTION 2

Refer to the exhibit, which shows the high availability configuration for the FortiAuthenticator (FAC1).



GUI Access

High Availability Settings

● Enable HA

Role: ○ Cluster member ● Standalone Primary ○ Load Balancer

Password: •••••••••

Load Balancers:

Name	IP Address	Delete

Based on this information, which statement is true about the next FortiAuthenticator (FAC2) member that will join an HA cluster with this FortiAuthenticator (FAC1)?

A. FAC2 can only process requests when FAC1 fails.

B. FAC2 can have its HA interface on a different network than FAC1.

C. The FortiToken license will need to be installed on the FAC2.

D. FSSO sessions from FAC1 will be synchronized to FAC2.

Correct Answer: D

Explanation: When FortiAuthenticator operates in cluster mode, it provides active-passive failover and synchronization of all configuration and data, including FSSO sessions, between the cluster members. Therefore, if FAC1 is the active unit and FAC2 is the standby unit, any FSSO sessions from FAC1 will be synchronized to FAC2. If FAC1 fails, FAC2 will take over the active role and continue to process the FSSO sessions. References:https://docs.fortinet.com/document/fortiauthenticator/6.1.2/administration- guide/122076/high-availability

QUESTION 3

You are migrating the branches of a customer to FortiGate devices. They require independent routing tables on the LAN side of the network.

After reviewing the design, you notice the firewall will have many BGP sessions as you have two data centers (DC) and two ISPs per DC while each branch is using at least 10 internal segments.

Based on this scenario, what would you suggest as the more efficient solution, considering that in the future the number of internal segments, DCs or internet links per DC will increase?

A. No change in design is needed as even small FortiGate devices have a large memory capacity.

B. Acquire a FortiGate model with more capacity, considering the next 5 years growth.

C. Implement network-id, neighbor-group and increase the advertisement-interval

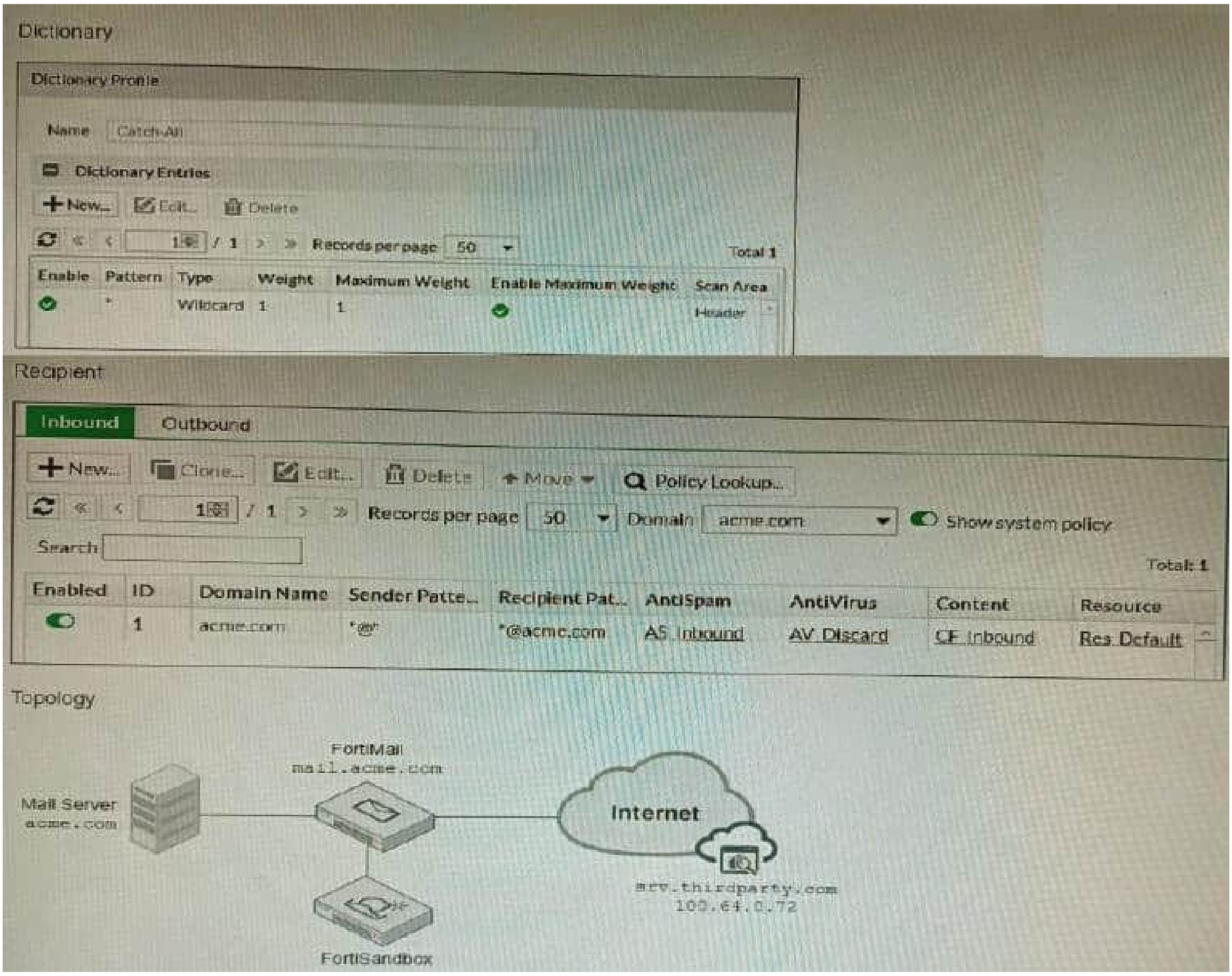
D. Redesign the SD-WAN deployment to only use a single VPN tunnel and segment traffic using VRFs on BGP

Correct Answer: D

Explanation: Using multiple VPN tunnels and BGP sessions for each internal segment is not scalable and efficient, especially when the number of segments, DCs or internet links per DC increases. A better solution is to use a single VPN tunnel per branch and segment traffic using virtual routing and forwarding (VRF) instances on BGP. This way, each VRF can have its own routing table and BGP session, while sharing the same VPN tunnel. References:https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/sd-wan- with-vrf-and-bgp

QUESTION 4

Refer to the exhibits.



Dictionary

Dictionary Profile

Name: Catch-All

Dictionary Entries

Enable	Pattern	Type	Weight	Maximum Weight	Enable Maximum Weight	Scan Area
✓	*	Wildcard	1	1	✓	Header

Recipient

Enabled	ID	Domain Name	Sender Patte...	Recipient Pat...	AntiSpam	AntiVirus	Content	Resource
●	1	acme.com	*@*	*@acme.com	AS_Inbound	AV_Discard	CF_Inbound	Res_Default

Topology

The exhibits show a FortiMail network topology, Inbound configuration settings, and a Dictionary Profile.

You are required to integrate a third-party\\'s host service (srv.thirdparty.com) into the e-mail processing path.

All inbound e-mails must be processed by FortiMail antispam and antivirus with FortiSandbox integration. If the email is clean, FortiMail must forward it to the third-party service, which will send the email back to FortiMail for final delivery, FortiMail must not scan the e-mail again.

Which three configuration tasks must be performed to meet these requirements? (Choose three.)

A. Change the scan order in FML-GW to antispam-sandbox-content.

B. Apply the Catch-Ail profile to the CFInbound profile and configure a content action profile to deliver to the srv. thirdparty. com FQDN

C. Create an access receive rule with a Sender value of srv. thirdparcy.com, Recipient value of *@acme.com, and action value of Safe

D. Apply the Catch-AII profile to the ASinbound profile and configure an access delivery rule to deliver to the 100.64.0.72 host.

E. Create an IP policy with a Source value of 100. 64 .0.72/32, enable precedence, and place the policy at the top of the list.

Correct Answer: ABE

A is correct because the scan order must be changed to antispam-sandbox- content in order for FortiMail to scan the email for spam and viruses before forwarding it to the third-party service.

B is correct because the Catch-All profile must be applied to the CFInbound profile in order for FortiMail to forward clean emails to the third-party service. E is correct because an IP policy must be created with a Source value of 100.64.0.72/32

in order to allow emails from the third-party service to be delivered to FortiMail.

The other options are not necessary to meet the requirements. Option C is not necessary because the access receive rule will already allow emails from the third-party service to be received by FortiMail. Option D is not necessary because

the Catch-All profile already allows emails to be delivered to any destination. Here are some additional details about integrating a third-party service into the FortiMail email processing path:

The third-party service must be able to receive emails from FortiMail and send them back to FortiMail.

The third-party service must be able to communicate with FortiMail using the SMTP protocol.

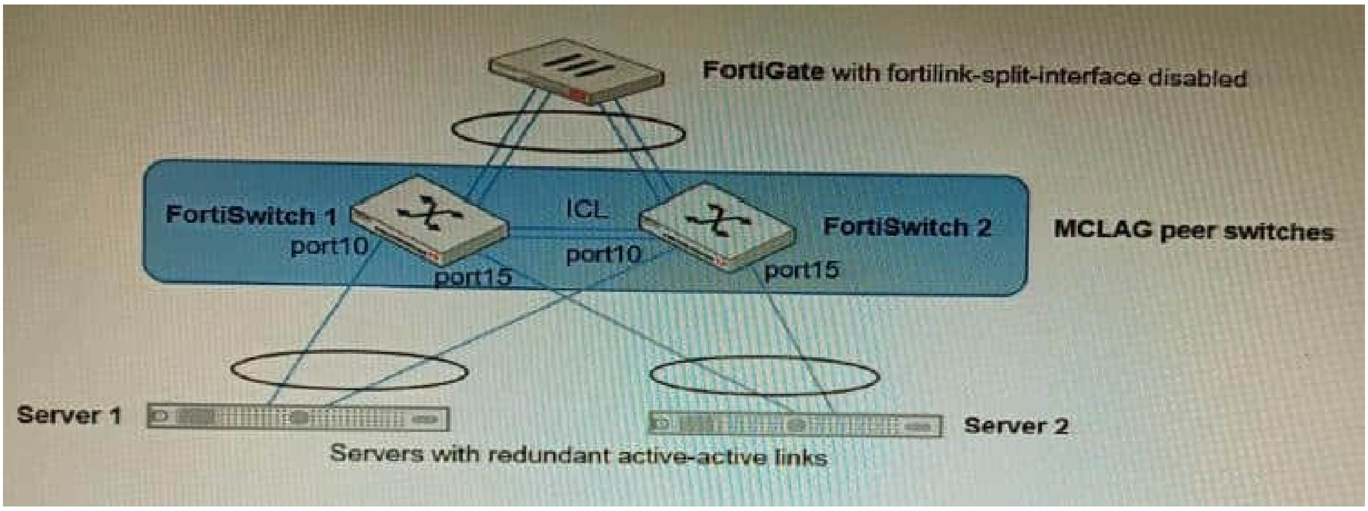
The third-party service must be able to authenticate with FortiMail using the SMTP AUTH protocol.

Once the third-party service is integrated into the FortiMail email processing path, all inbound emails will be processed by FortiMail as usual. If the email is clean, FortiMail will forward it to the third-party service. The third-party service will then

send the email back to FortiMail for final delivery. FortiMail will not scan the email again.

QUESTION 5

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