NSE8_812 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.pass4itsure.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 feature must you enable on the BGP neighbors to accomplish this goal?

A. Graceful-restart

B. Deterministic-med

C. Synchronization

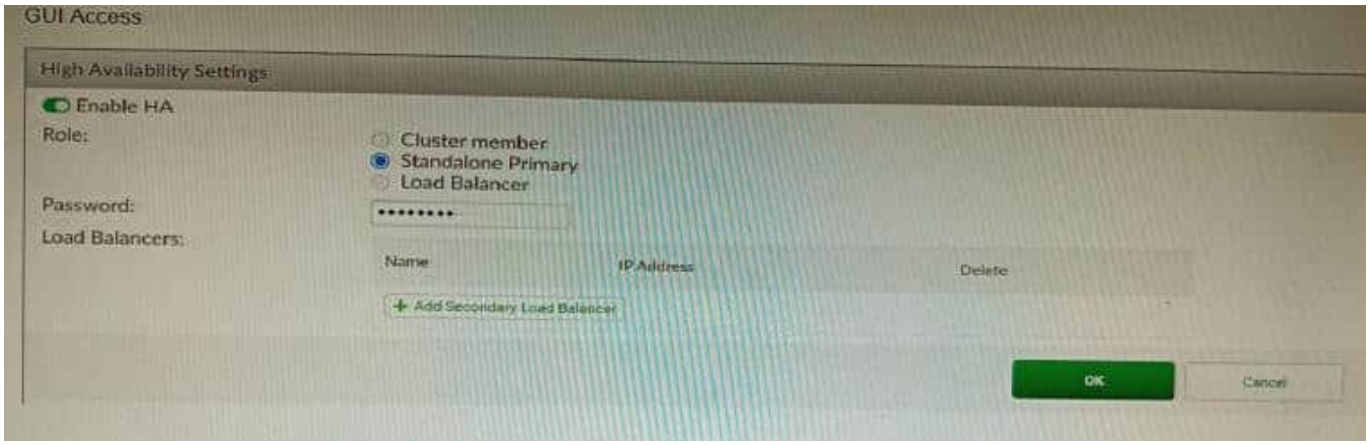
D. Soft-reconfiguration

Correct Answer: A

Explanation: Graceful-restart is a feature that allows BGP neighbors to maintain their routing information during a BGP restart or failover event, without disrupting traffic forwarding or causing route flaps. Graceful-restart works by allowing a BGP speaker (the restarting router) to notify its neighbors (the helper routers) that it is about to restart or failover, and request them to preserve their routing information and forwarding state for a certain period of time (the restart time). The helper routers then mark the routes learned from the restarting router as stale, but keep them in their routing table and continue forwarding traffic based on them until they receive an end-of-RIB marker from the restarting router or until the restart time expires. This way, graceful-restart can minimize traffic disruption and routing instability during a BGP restart or failover event. References:https://docs.fortinet.com/document/fortigate/7.0.0/cookbook/19662/bgp- graceful-restart

QUESTION 2

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



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

Review the following FortiGate-6000 configuration excerpt:

```
config load-balance setting
    set nat-source-port chassis-slots
end
```

Based on the configuration, which statement is correct regarding SNAT source port partitioning behavior?

A. It dynamically distributes SNAT source ports to operating FPCs or FPMs.

B. It is the default SNAT configuration and preserves active sessions when an FPC or FPM goes down.

C. It statically distributes SNAT source ports to operating FPCs or FPMs

D. It equally distributes SNAT source ports across chassis slots.

Correct Answer: A

Explanation: The configuration excerpt shows that the SNAT source port partitioning behavior is set to dynamic. This means that the FortiGate will dynamically distribute SNAT source ports to operating FPCs or FPMs. This ensures that active

sessions are not interrupted if an FPC or FPM goes down.

The other options are incorrect. Option B is incorrect because the default SNAT configuration is static. Option C is incorrect because the configuration excerpt does not specify that SNAT source ports are statically distributed. Option D is

incorrect because the SNAT source ports are not evenly distributed across chassis slots. Here are some additional details about SNAT source port partitioning behavior:

SNAT source port partitioning behavior can be set to dynamic or static.

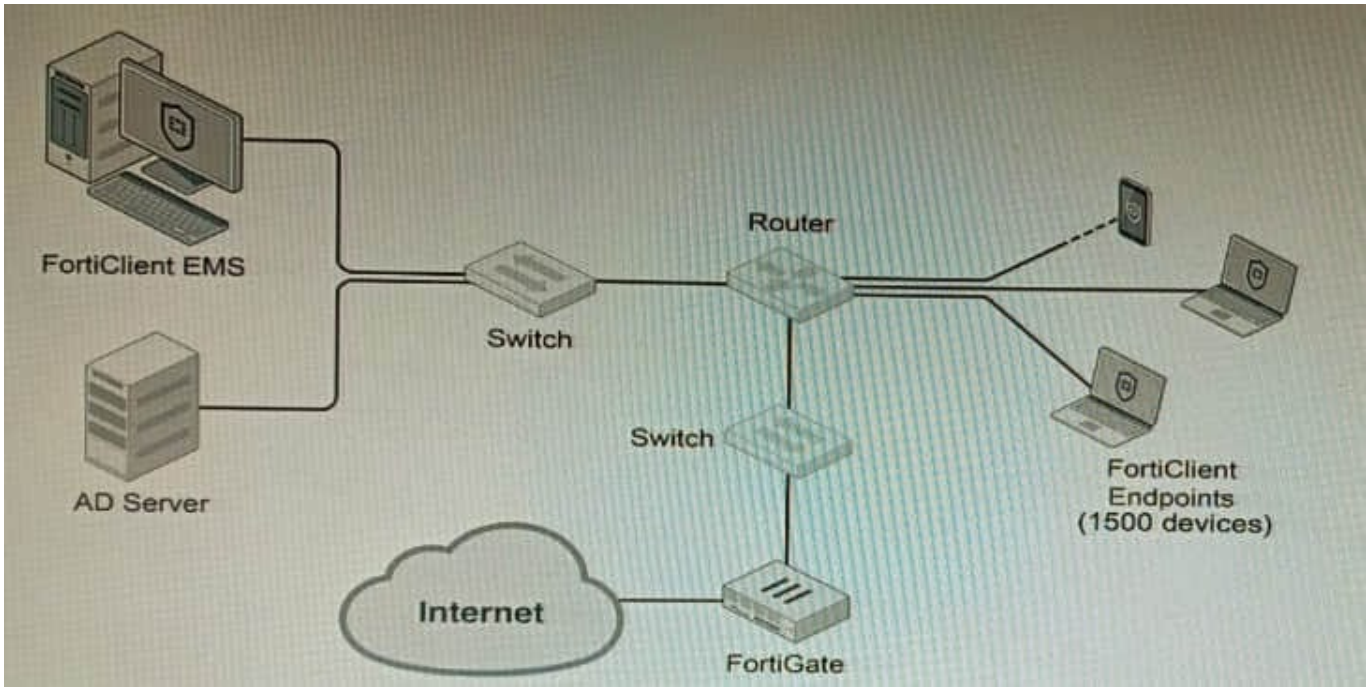
The default SNAT configuration is static.

Dynamic SNAT source port partitioning ensures that active sessions are not interrupted if an FPC or FPM goes down.

Static SNAT source port partitioning can improve performance by reducing the number of SNAT lookups.

QUESTION 4

Refer to the exhibit.



A customer wants FortiClient EMS configured to deploy to 1500 endpoints. The deployment will be integrated with FortiOS and there is an Active Directory server.

Given the configuration shown in the exhibit, which two statements about the installation are correct? (Choose two.)

A. If no client update time is specified on EMS, the user will be able to choose the time of installation if they wish to delay.

B. A client can be eligible for multiple enabled configurations on the EMS server, and one will be chosen based on first priority

C. You can only deploy initial installations to Windows clients.

D. You must use Standard or Enterprise SQL Server rather than the included SQL Server Express

E. The Windows clients only require "File and Printer Sharing0 allowed and the rest is handled by Active Directory group policy

Correct Answer: AE

A is correct because if no client update time is specified on EMS, the user will be able to choose the time of installation if they wish to delay. This is because the FortiClient EMS server will not force the installation on the client. E is correct

because the Windows clients only require "File and Printer Sharing" allowed and the rest is handled by Active Directory group policy. This is because the Active Directory group policy will configure the Windows clients to automatically install

FortiClient and the FortiClient EMS server will only need to push the initial configuration to the clients.

The other options are incorrect. Option B is incorrect because a client can only be eligible for one enabled configuration on the EMS server. Option C is incorrect because you can deploy initial installations to both Windows and macOS

clients.

Option D is incorrect because you can use the included SQL Server Express to deploy FortiClient EMS.

References:

Deploying FortiClient EMS | FortiClient / FortiOS 7.4.0 - Fortinet Document Library Configuring FortiClient EMS | FortiClient / FortiOS 7.4.0 - Fortinet Document Library

FortiClient EMS installation requirements | FortiClient / FortiOS 7.4.0 - Fortinet Document Library

QUESTION 5

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.