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.leads4pass.com/nse8_812.html

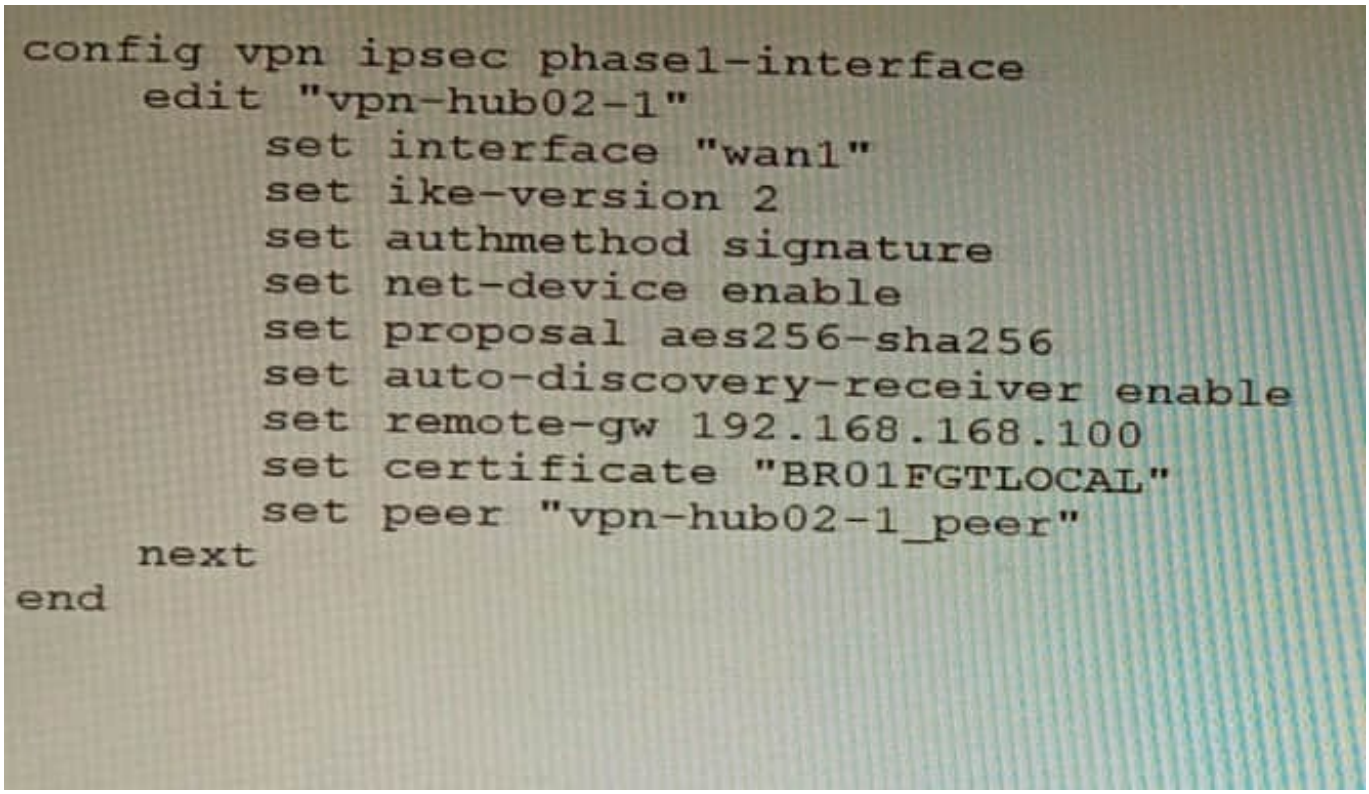
100% Passing Guarantee
100% Money Back Assurance

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

Refer to the exhibit.



To facilitate a large-scale deployment of SD-WAN/ADVPN with FortiGate devices, you are tasked with configuring the FortiGate devices to support injecting of IKE routes on the ADVPN shortcut tunnels. Which three commands must be added or changed to the FortiGate spoke config vpn ipsec phasei-interface options referenced in the exhibit for the VPN interface to enable this capability? (Choose three.)

A. set net-device disable

B. set mode-cfg enable

C. set ike-version 1

D. set add-route enable

E. set mode-cfg-allow-client-selector enable

Correct Answer: BDE

B must be set to enable mode-cfg, which is required for injecting IKE routes on the ADVPN shortcut tunnels.

D must be set to enable add-route, which is the command that actually injects the IKE routes.

E must be set to enable mode-cfg-allow-client-selector, which allows custom phase 2 selectors to be configured.

The other options are incorrect. Option A is incorrect because net-device disable is not required for injecting IKE routes on the ADVPN shortcut tunnels. Option C is incorrect because IKE version 1 is not supported for ADVPN.

References:

Phase 2 selectors and ADVPN shortcut tunnels | FortiGate / FortiOS 7.2.0 Configuring SD-WAN/ADVPN with FortiGate | FortiGate / FortiOS 7.2.0

QUESTION 2

A retail customer with a FortiADC HA cluster load balancing five webservers in L7 Full NAT mode is receiving reports of users not able to access their website during a sale event. But for clients that were able to connect, the website works fine.

CPU usage on the FortiADC and the web servers is low, application and database servers are still able to handle more traffic, and the bandwidth utilization is under 30%.

Which two options can resolve this situation? (Choose two.)

A. Change the persistence rule to LB_PERSIS_SSL_SESSJD.

B. Add more web servers to the real server poof

C. Disable SSL between the FortiADC and the web servers

D. Add a connection-pool to the FortiADC virtual server

Correct Answer: BD

Option B: Adding more web servers to the real server pool will increase the overall capacity of the load balancer, which should help to resolve the issue of users not being able to access the website.

Option D: Adding a connection-pool to the FortiADC virtual server will allow the load balancer to cache connections to the web servers, which can help to improve performance and reduce the number of dropped connections. Option A:

Changing the persistence rule to LB_PERSIS_SSL_SESSJD would only be necessary if the current persistence rule is not working properly. In this case, the CPU usage on the FortiADC and the web servers is low, so the persistence rule is

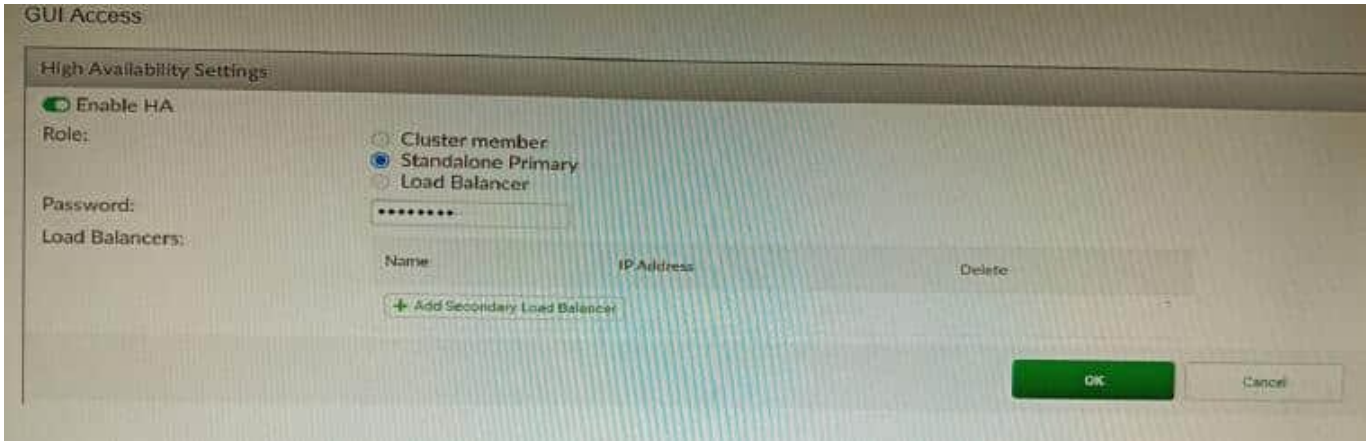
likely not the issue.

Option C: Disabling SSL between the FortiADC and the web servers would reduce the load on the FortiADC, but it would also make the website less secure. Since the bandwidth utilization is under 30%, it is unlikely that disabling SSL would

resolve the issue. Reference: https://docs.fortinet.com/document/fortiadc/7.2.1/handbook/970956/configuring- virtual-servers

QUESTION 3

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 4

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 5

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