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.passapply.com/nse8_812.html

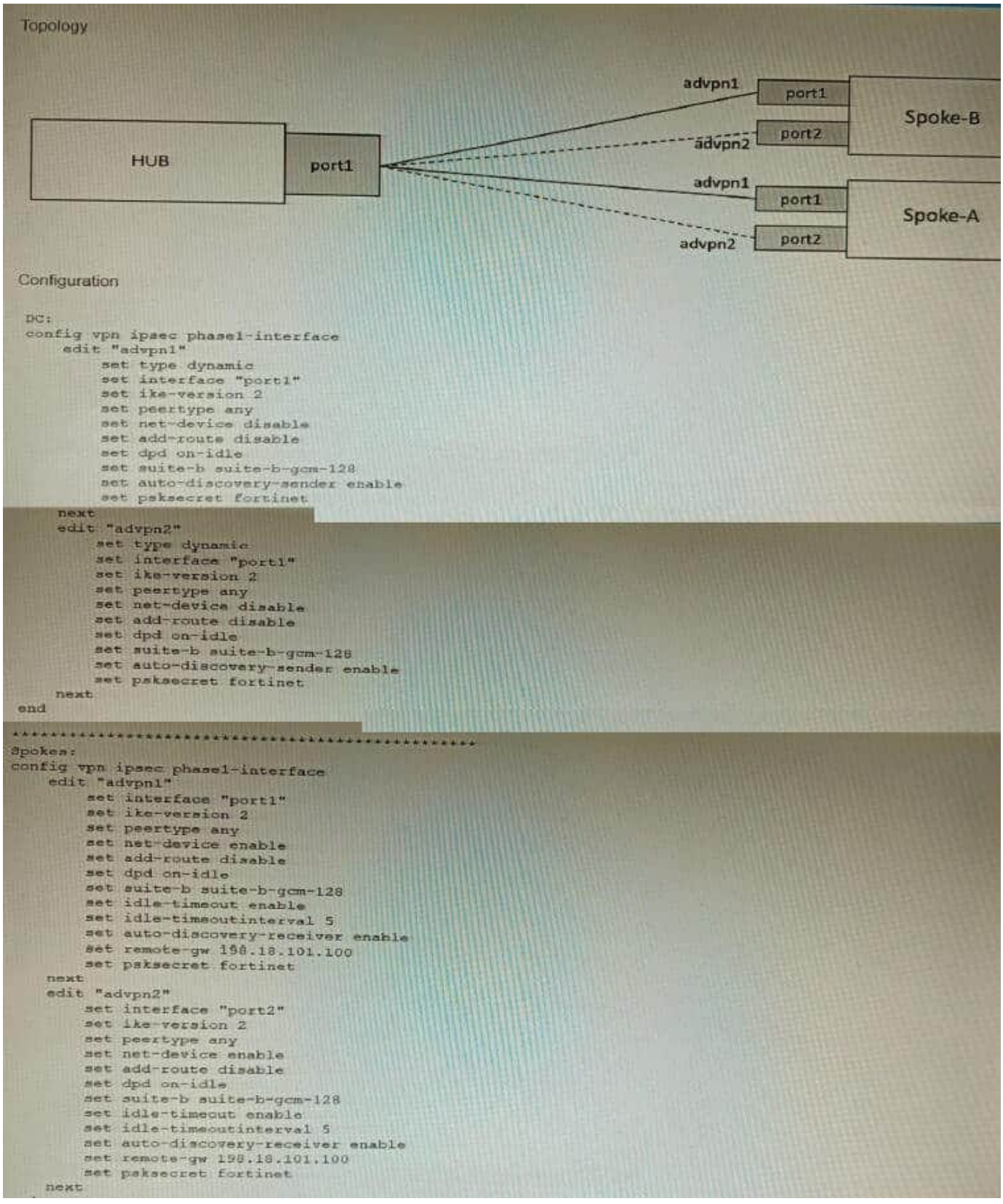
100% Passing Guarantee
100% Money Back Assurance

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 exhibits.



The exhibits show a diagram of a requested topology and the base IPsec configuration.

A customer asks you to configure ADVPN via two internet underlays. The requirement is that you use one interface with a single IP address on DC FortiGate.

In this scenario, which feature should be implemented to achieve this requirement?

A. Use network-overlay id

B. Change advpn2 to IKEv1

C. Use local-id

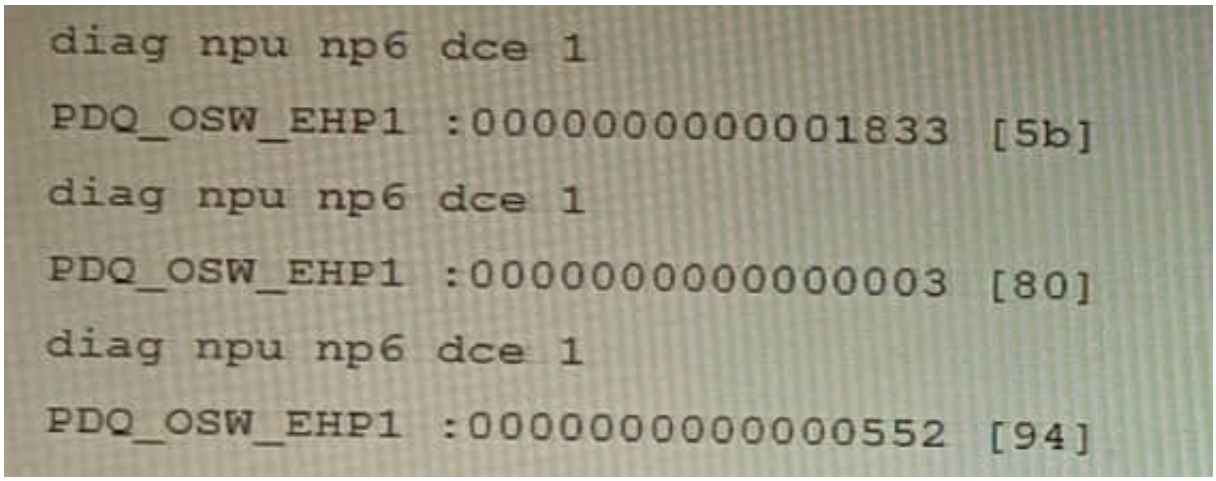
D. Use peer-id

Correct Answer: A

Explanation: A is correct because using network-overlay id allows you to configure multiple ADVPN tunnels on a single interface with a single IP address on the DC FortiGate. This is explained in the FortiGate Administration Guide under ADVPN > Configuring ADVPN > Configuring ADVPN on the hub. References:
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn
https://docs.fortinet.com/document/fortigate/7.4.0/administration- guide/978793/advpn/978794/configuring-advpn

QUESTION 2

You are running a diagnose command continuously as traffic flows through a platform with NP6 and you obtain the following output: Given the information shown in the output, which two statements are true? (Choose two.)



A. Enabling bandwidth control between the ISF and the NP will change the output

B. The output is showing a packet descriptor queue accumulated counter

C. Enable HPE shaper for the NP6 will change the output

D. Host-shortcut mode is enabled.

E. There are packet drops at the XAUI.

Correct Answer: BE

Explanation: The diagnose command shown in the output is used to display information about NP6 packet descriptor queues. The output shows that there are 16 NP6 units in total, and each unit has four XAUI ports (XA0-XA3). The output also shows that there are some non-zero values in the columns PDQ ACCU (packet descriptor queue accumulated counter) and PDQ DROP (packet descriptor queue drop counter). These values indicate that there are some packet descriptor queues that have reached their maximum capacity and have dropped some packets at the XAUI ports. This could be caused by congestion or misconfiguration of the XAUI ports or the ISF (Internal Switch Fabric). References:https://docs.fortinet.com/document/fortigate/7.0.0/cli- reference/19662/diagnose-np6-pdq

The output is showing a packet descriptor queue accumulated counter, which is a measure of the number of packets that have been dropped by the NP6 due to congestion. The counter will increase if there are more packets than the NP6 can handle, which can happen if the bandwidth between the ISF and the NP is not sufficient or if the HPE shaper is enabled. The output also shows that there are packet drops at the XAUI, which is the interface between the NP6 and the FortiGate\\'s backplane. This means that the NP6 is not able to keep up with the traffic and is dropping packets. The other statements are not true. Host-shortcut mode is not enabled, and enabling bandwidth control between the ISF and the NP will not change the output. HPE shaper is a feature that can be enabled to improve performance, but it will not change the output of the diagnose command. Reference: https://docs.fortinet.com/document/fortigate/7.4.0/hardware-acceleration/48875/diagnose-npu-np6-dce-np6-id-number-of-dropped-np6-packets

QUESTION 3

A customer is planning on moving their secondary data center to a cloud-based IaaS. They want to place all the Oracle-based systems Oracle Cloud, while the other systems will be on Microsoft Azure with ExpressRoute service to their main

data center.

They have about 200 branches with two internet services as their only WAN connections. As a security consultant you are asked to design an architecture using Fortinet products with security, redundancy and performance as a priority.

Which two design options are true based on these requirements? (Choose two.)

A. Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud.

B. Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure.

C. Branch FortiGate devices must be configured as VPN clients for the branches\\' internal network to be able to access Oracle services without using public IPs.

D. Two ExpressRoute services to the main data center are required to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge

Correct Answer: AC

A. Systems running on Azure will need to go through the main data center to access the services on Oracle Cloud. This is because the Oracle Cloud is not directly connected to the Azure Cloud. The traffic will need to go through the main

data center in order to reach the Oracle Cloud.

C. Branch FortiGate devices must be configured as VPN clients for the branches\\' internal network to be able to access Oracle services without using public IPs. This is because the Oracle Cloud does not allow direct connections from the

internet. The traffic will need to go through the FortiGate devices in order to reach the Oracle Cloud.

The other options are not correct.

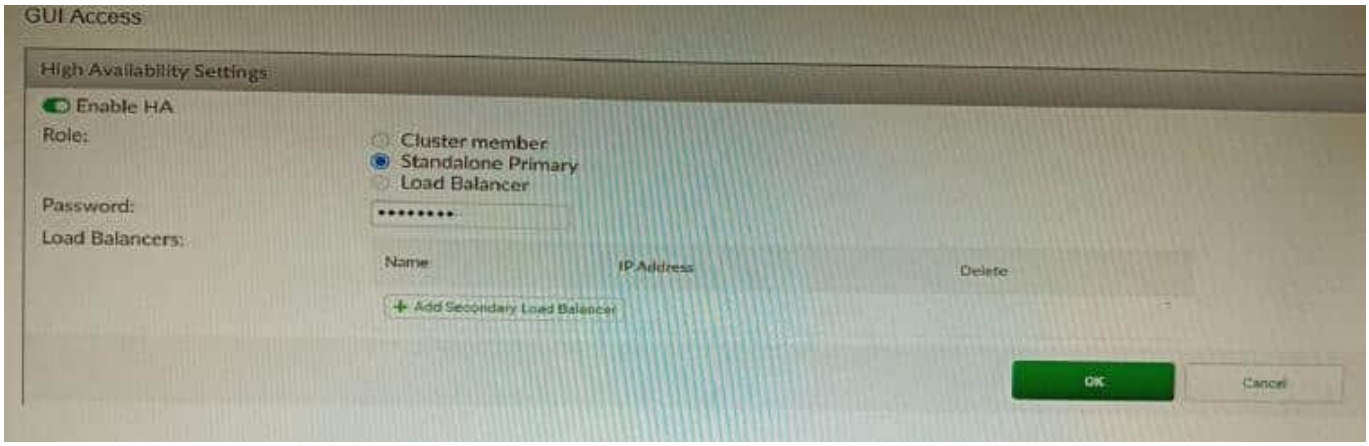
B. Use FortiGate VM for IPSEC over ExpressRoute, as traffic is not encrypted by Azure. This is not necessary. Azure does encrypt traffic over ExpressRoute. D. Two ExpressRoute services to the main data center are required to implement

SD-WAN between a FortiGate VM in Azure and a FortiGate device at the data center edge. This is not necessary. A single ExpressRoute service can be used to implement SD-WAN between a FortiGate VM in Azure and a FortiGate device at

the data center edge.

QUESTION 4

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.

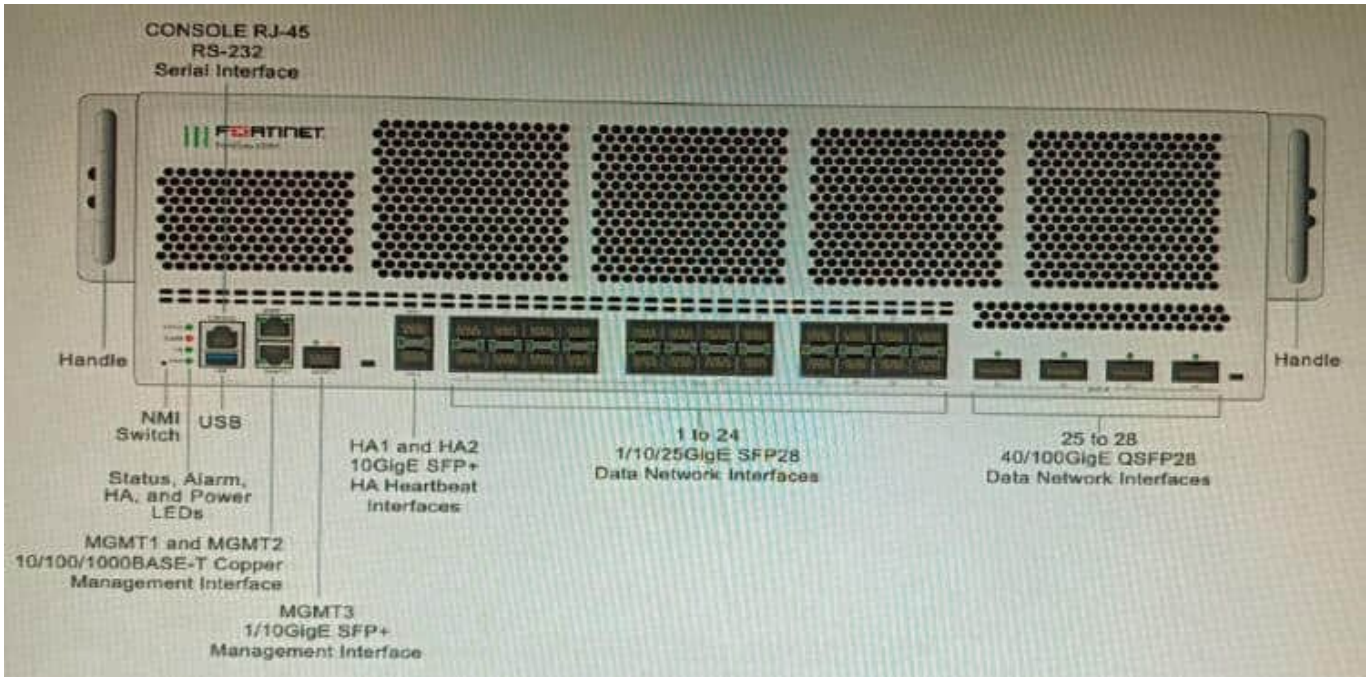
D. FSSO sessions from FAC1 will be synchronized to FAC2.

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 5

Refer to the exhibit.



You are deploying a FortiGate 6000F. The device should be directly connected to a switch. In the future, a new hardware module providing higher speed will be installed in the switch, and the connection to the FortiGate must be moved to this higher-speed port.

You must ensure that the initial FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port speed is defined.

How should the initial connection be made?

A. Connect the switch on any interface between ports 21 to 24

B. Connect the switch on any interface between ports 25 to 28

C. Connect the switch on any interface between ports 1 to 4

D. Connect the switch on any interface between ports 5 to 8.

Correct Answer: C

Explanation: The FortiGate 6000F has 24 1/10/25-Gbps SFP28 data network interfaces (1 to 24). These interfaces are divided into the following interface groups: 1 to 4, 5 to 8, 9 to 12, 13 to 16, 17 to 20, and 21 to 24. The ports 25 to 28 are

40/100-Gbps QSFP28 data network interfaces.

The initial connection should be made to any interface between ports 1 to 4. This is because the ports 21 to 24 are part of the same interface group, and changing the speed of one of these ports will affect the speeds of all of the ports in the

group. The ports 5 to 8 are also part of the same interface group, so they should not be used for the initial connection. The new hardware module that will be installed in the switch will provide higher speed ports. When this module is installed,

the speed of the ports 21 to 24 will be increased. However, this will not affect the ports 1 to 4, because they are not part of the same interface group.

Therefore, the initial connection should be made to any interface between ports 1 to 4, in order to ensure that the FortiGate interface connected to the switch does not affect any other port when the new module is installed and the new port

speed is defined.

Reference:

FortiGate 6000F Front Panel Interfaces: https://docs.fortinet.com/document/fortigate- 6000/hardware/fortigate-6000f-system-guide/827055/front-panel-interfaces