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

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 external sources. 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 2

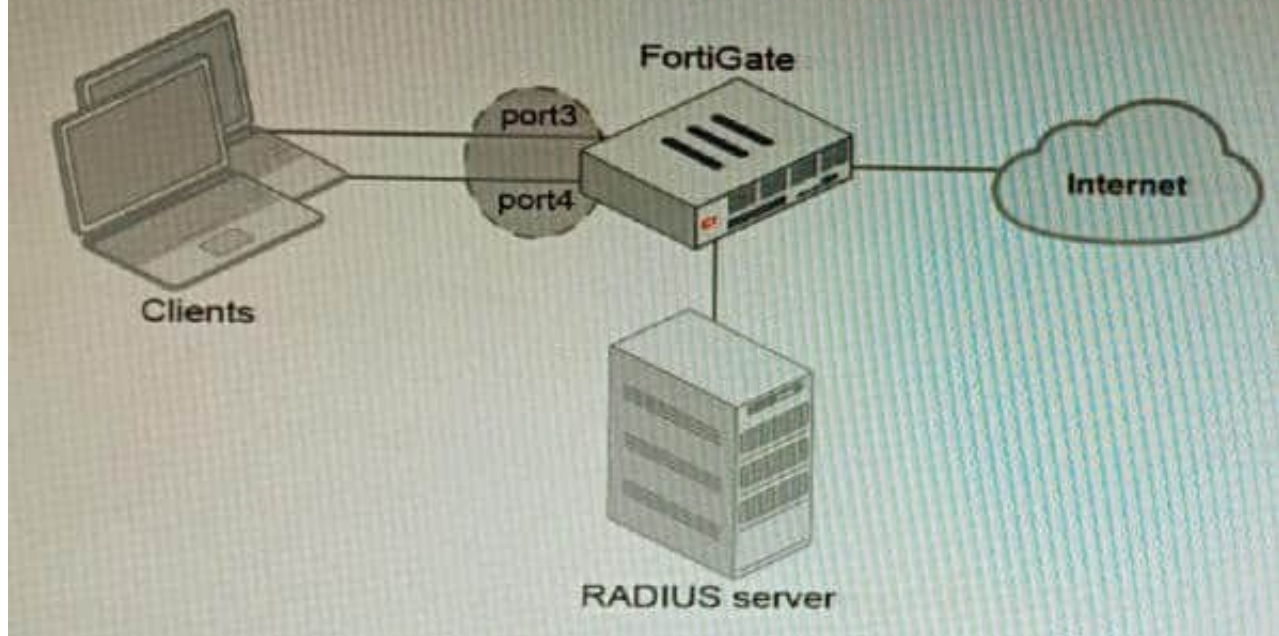Refer to the exhibits.

Exhibit A

Exhibit B

```
get hardware npu np6 port-list
Chip XAUI Ports Max Cross-chip
Speed offloading
------ ---- ------- ----- -----------
np6_0 0 port1 1G Yes
0 port2 1G Yes
0 port3 1G Yes
0 port4 1G Yes
0 port5 1G Yes
0 port6 1G Yes
0 port7 1G Yes
0 port8 1G Yes
1 port9 1G Yes
1 port10 1G Yes
...
3 port28 1G Yes
3 s1 1G Yes
3 s2 1G Yes
3 vw1 1G Yes
3 vw2 1G Yes
------ ---- ------- ----- -----------
```

A customer is looking for a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E.

Referring to the exhibits, which two conditions allow authentication to the client devices before assigning an IP address? (Choose two.)

A. FortiGate devices with NP6 and hardware switch interfaces cannot support 802.1X authentication.

B. Devices connected directly to ports 3 and 4 can perform 802 1X authentication.

C. Ports 3 and 4 can be part of different switch interfaces.

D. Client devices must have 802 1X authentication enabled

Correct Answer: BD

Explanation: The customer wants to deploy a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E device. A hardware switch interface is an interface that combines multiple physical interfaces into one logical interface, allowing them to act as a singleswitch with one IP address and one set of security policies. The customer wants to use 802.1X authentication for this solution, which is a standard protocol for port-based network access control (PNAC) that authenticates clients based on their credentials before granting them access to

network resources. One condition that allows authentication to the client devices before assigning an IP address is that devices connected directly to ports 3 and 4 can perform 802.1X authentication. This is because ports 3 and 4 are part of the hardware switch interface named "lan", which has an IP address of 10.10.10.254/24 and an inbound SSL inspection profile named "sslinspection". The inbound SSL inspection profile enables the FortiGate device to intercept and inspect SSL/TLS traffic from clients before forwarding it to servers, which allows it to apply security policies and features such as antivirus, web filtering, application control, etc. However, before performing SSL inspection, the FortiGate device needs to authenticate the clients using 802.1X authentication, which requires the clients to send their credentials (such as username and password) to the FortiGate device over a secure EAP (Extensible Authentication Protocol) channel. The FortiGate device then verifies the credentials with an authentication server (such as RADIUS or LDAP) and grants or denies access to the clients based on the authentication result. Therefore, devices connected directly to ports 3 and 4 can perform 802.1X authentication before assigning an IP address. Another condition that allows authentication to the client devices before assigning an IP address is that client devices must have 802.1X authentication enabled. This is because 802.1X authentication is a mutual process that requires both the client devices and the FortiGate device to support and enable it. The client devices must have 802.1X authentication enabled in their network settings, which allows them to initiate the authentication process when they connect to the hardware switch interface of the FortiGate device. The client devices must also have an 802.1X supplicant software installed, which is a program that runs on the client devices and handles the communication with the FortiGate device using EAP messages. The client devices must also have a trusted certificate installed, which is used to verify the identity of the FortiGate device and establish a secure EAP channel. Therefore, client devices must have 802.1X authentication enabled before assigning an IP address. References: https:// docs.fortinet.com/document/fortigate/7.0.0/administration- guide/19662/hardware-switchinterfaceshttps://docs.fortinet.com/document/fortigate/7.0.0/administration- guide/19662/802-1x-authentication

QUESTION 3

You must analyze an event that happened at 20:37 UTC. One log relevant to the event is extracted from FortiGate logs:

The devices and the administrator are all located in different time zones Daylight savings time (DST) is disabled The FortiGate is at GMT-1000. The FortiAnalyzer is at GMT-0800 Your browser local time zone is at GMT-03.00

You want to review this log on FortiAnalyzer GUI, what time should you use as a filter?

A. 20:37:08

B. 10:37:08

C. 17:37:08

D. 12.37:08

Correct Answer: C

Explanation: To review this log on FortiAnalyzer GUI, the administrator should use the time filter that matches the local time zone of FortiAnalyzer, which is GMT-0800. Since the log was generated at 20:37 UTC (GMT+0000), the corresponding time in GMT-0800 is

20:37 - 8 hours = 12:37. However, since DST is disabled on FortiAnalyzer, the administrator should add one hour to

account for daylight saving time difference, resulting in 12:37 + 1 hour = 13:37. Therefore, the time filter to use is 13:37:08. References:https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration- guide/103664/time-zone-and-daylight-saving-time

---

QUESTION 4

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 5

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.

NSE8_812 PDF Dumps   NSE8_812 Practice Test   NSE8_812 Study Guide