NSE8_812 Reliable Study Questions - Valid NSE8_812 Exam Topics

DOWNLOAD the newest Prep4sureGuide NSE8_812 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1AZP09T08Cea3EAlsKnc7SFEY_k2CbJBx

There are a lot of the functions on our NSE8_812 exam questions to help our candidates to reach the best condition befor they take part in the real exam. I love the statistics report function and the timing function most. The statistics report function helps the learners find the weak links and improve them accordingly. The timing function of our NSE8_812 training quiz helps the learners to adjust their speed to answer the questions and keep alert and our NSE8_812 study materials have set the timer.

Fortinet NSE8_812 Exam covers a wide range of topics related to network security, including network design, implementation, and troubleshooting using the Fortinet security products. NSE8_812 exam also evaluates the candidate's knowledge of the latest network security threats and solutions, as well as their ability to recommend the best security solutions for different network environments.

>> NSE8_812 Reliable Study Questions <<

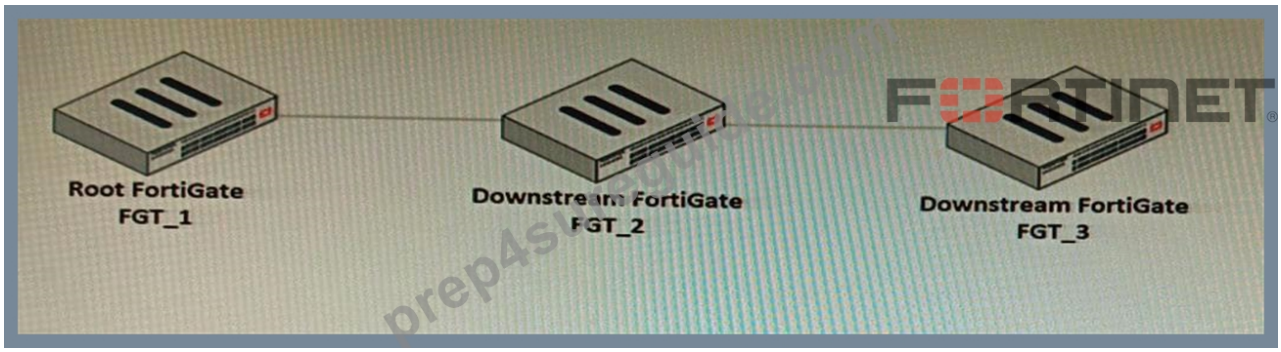
Valid NSE8_812 Exam Topics & Practice NSE8_812 Tests

Do you feel Fortinet NSE8_812 exam preparation is tough? Prep4sureGuide desktop and web-based online Fortinet NSE8_812 practice test software will give you a clear idea about the final NSE8_812 Test Pattern. Practicing with the Fortinet NSE8_812 practice test, you can evaluate your Fortinet NSE8_812 exam preparation.

Fortinet NSE8_812 exam assesses the candidate's knowledge and skills in various areas such as network security, cloud security, application security, and endpoint security. NSE8_812 Exam is designed for professionals who have several years of experience in the field of cybersecurity and have a deep understanding of Fortinet products.

Fortinet NSE 8 - Written Exam (NSE8_812) Sample Questions (Q36-Q41):

NEW QUESTION # 36
Refer to the exhibit.



You have deployed a security fabric with three FortiGate devices as shown in the exhibit. FGT_2 has the following configuration:

```
config system csf
set fabric-object-unification local
end
```

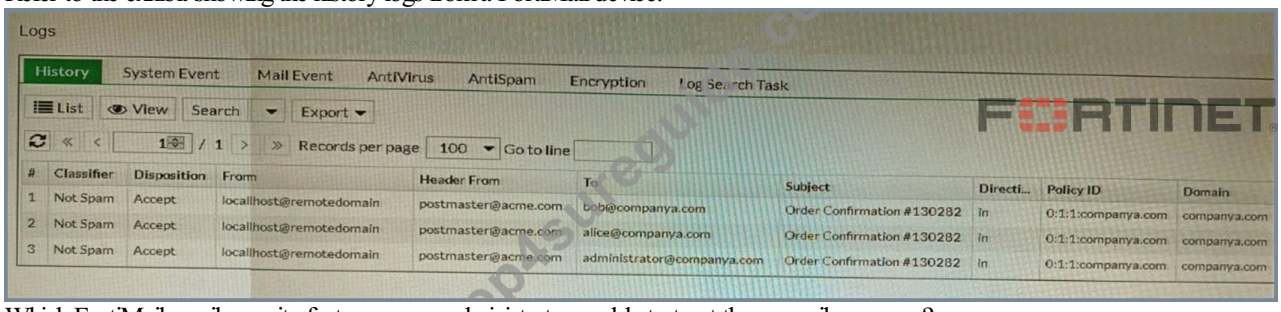
FGT_1 and FGT_3 are configured with the default setting. Which statement is true for the synchronization of fabric-objects?

- A. Objects from the root FortiGate will only be synchronized to FGT__2.
- B. Objects from the FortiGate FGT_2 will be synchronized to the upstream FortiGate.
- C. Objects from the root FortiGate will not be synchronized to any downstream FortiGate.
- D. Objects from the root FortiGate will only be synchronized to FGT_3.

Answer: D

Explanation:
https://docs.fortinet.com/document/fortigate/6.4.0/new-features/520820/improvements-to-synchronizing- objects-across-the-security-fabric-6-4-4

NEW QUESTION # 37
Refer to the exhibit showing the history logs from a FortiMail device.



Which FortiMail email security feature can an administrator enable to treat these emails as spam?

- A. DKIM validation in a session profile
- B. Sender domain validation in a session profile
- C. Impersonation analysis in an antispam profile
- D. Soft fail SPF validation in an antispam profile

Answer: C

Explanation:
Impersonation analysis is a feature that detects emails that attempt to impersonate a trusted sender, such as a company executive or a well-known brand, by using spoofed or look-alike email addresses. This feature can help prevent phishing and business email compromise (BEC) attacks. Impersonation analysis can be enabled in an antispam profile and applied to a firewall policy.
References:https://docs.fortinet.com/document/fortimail
/6.4.0/administration-guide/103663/impersonation-analysis
https://docs.fortinet.com/document/fortimail/7.2.0/cookbook/221814/protecting-against-email-impersonation- in-fortimail

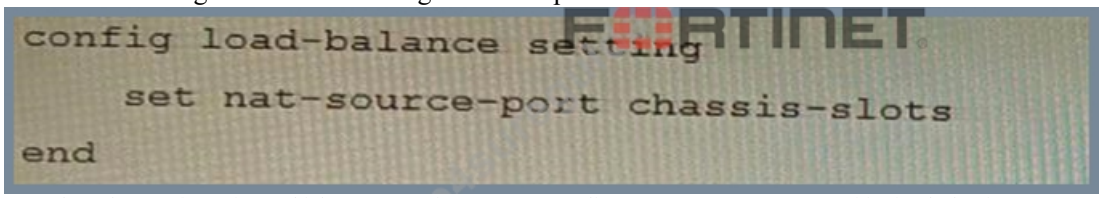
NEW QUESTION # 38
Which two methods are supported for importing user defined Lookup Table Data into the FortiSIEM?
(Choose two.)

- A. SCP
- B. Report
- C. FTP
- D. API

Answer: B,D

Explanation:
FortiSIEM supports two methods for importing user defined Lookup Table Data:
* Report: You can import lookup table data from a report. This is the most common method for importing lookup table data.
* API: You can also import lookup table data using the FortiSIEM API. This is a more advanced method that allows you to import lookup table data programmatically.
FTP, SCP, and other file transfer protocols are not supported for importing lookup table data into FortiSIEM.

NEW QUESTION # 39
Review the following FortiGate-6000 configuration excerpt:



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 equally distributes SNAT source ports across chassis slots.
- D. It statically distributes SNAT source ports to operating FPCs or FPMs

Answer: D

Explanation:
https://docs.fortinet.com/document/fortigate/7.4.1/fortigate-6000-administration-guide/81276/controlling-snat- port-partitioning-behavior
"chassis-slots this option statically allocates SNAT source ports to all FPCs that are enabled when you enter the command. If you disable an FPC from the CLI, the SNAT source ports assigned to that FPC will not be re- allocated to the remaining FPCs. All FPCs that are still operating will maintain the same SNAT source port allocation and active sessions being processed by the still operating FPCs will not be affected."

NEW QUESTION # 40
Refer to the exhibits.

Exhibit A

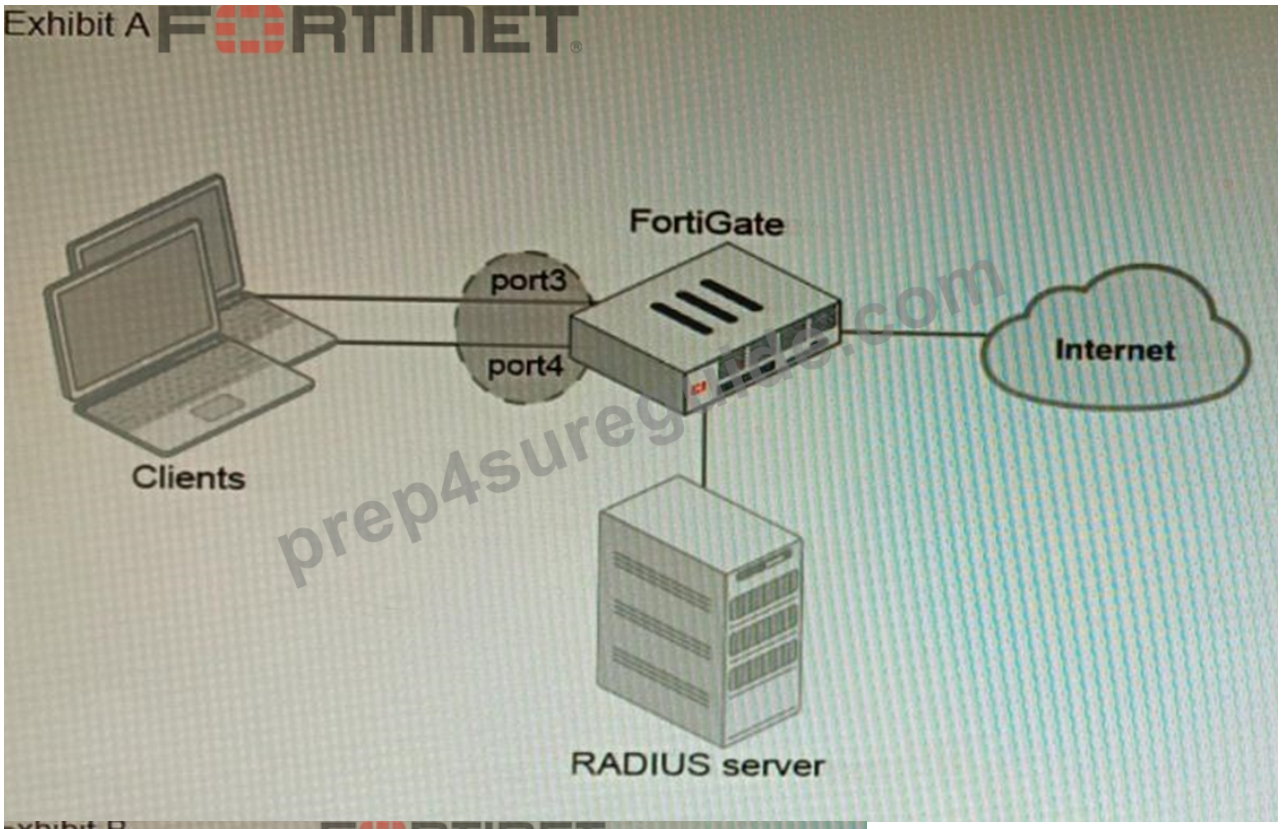


Exhibit B

```
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. Ports 3 and 4 can be part of different switch interfaces.
- B. Devices connected directly to ports 3 and 4 can perform 802 1X authentication.
- C. Client devices must have 802 1X authentication enabled
- D. FortiGate devices with NP6 and hardware switch interfaces cannot support 802.1X authentication.

Answer: B,C

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 single switch 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 "ssl-inspection". 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. Reference:
https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/hardware-switch-interfaces
https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/19662/802-1x-authentication

NEW QUESTION # 41
.....

P.S. Free & New NSE8_812 dumps are available on Google Drive shared by Prep4sureGuide: https://drive.google.com/open?id=1AZP09T08Cea3EAlsKnc7SFEY_k2CbJBx