NSE4_FGT-6.2Q&As

Fortinet NSE 4 - FortiOS 6.2

Pass Fortinet NSE4_FGT-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/nse4_fgt-6-2.html

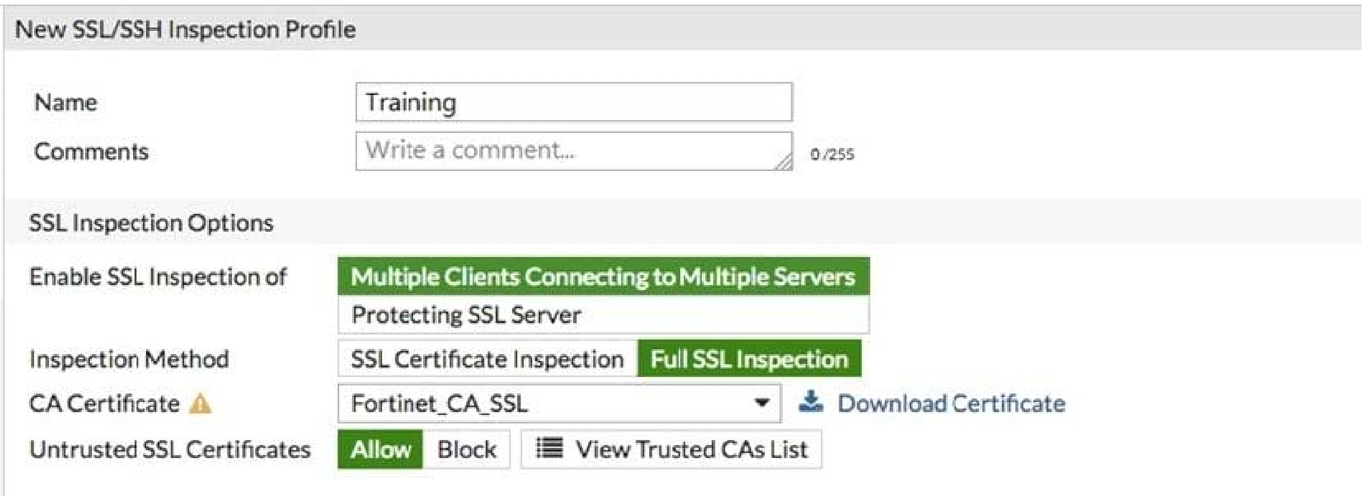
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

An employee connects to the https://example.com on the Internet using a web browser. The web server\\'s certificate was signed by a private internal CA. The FortiGate that is inspecting this traffic is configured for full SSL inspection.

This exhibit shows the configuration settings for the SSL/SSH inspection profile that is applied to the policy that is invoked in this instance. All other settings are set to defaults. No certificates have been imported into FortiGate. View the exhibit and answer the question that follows.



New SSL/SSH Inspection Profile

Name: Training

Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL Inspection of: Multiple Clients Connecting to Multiple Servers | Protecting SSL Server

Inspection Method: SSL Certificate Inspection | Full SSL Inspection

CA Certificate ⚠: Fortinet_CA_SSL

Untrusted SSL Certificates: Allow | Block

Which certificate is presented to the employee\\'s web browser?

A. The web server\\'s certificate.

B. The user\\'s personal certificate signed by a private internal CA.

C. A certificate signed by Fortinet_CA_SSL.

D. A certificate signed by Fortinet_CA_Untrusted.

Correct Answer: D

QUESTION 2

What files are sent to FortiSandbox for inspection in flow-based inspection mode?

A. All suspicious files that do not have their hash value in the FortiGuard antivirus signature database.

B. All suspicious files that are above the defined oversize limit value in the protocol options.

C. All suspicious files that match patterns defined in the antivirus profile.

D. All suspicious files that are allowed to be submitted to FortiSandbox in the antivirus profile.

Correct Answer: C

QUESTION 3

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.

B. Only secondary FortiGate devices are rebooted.

C. Uninterruptable upgrade is enabled by default.

D. Traffic load balancing is temporally disabled while upgrading the firmware.

Correct Answer: BD

QUESTION 4

Which of the following static routes are not maintained in the routing table?

A. Named Address routes

B. Dynamic routes

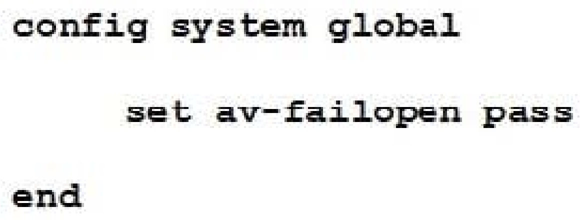
C. ISDB routes

D. Policy routes

Correct Answer: D

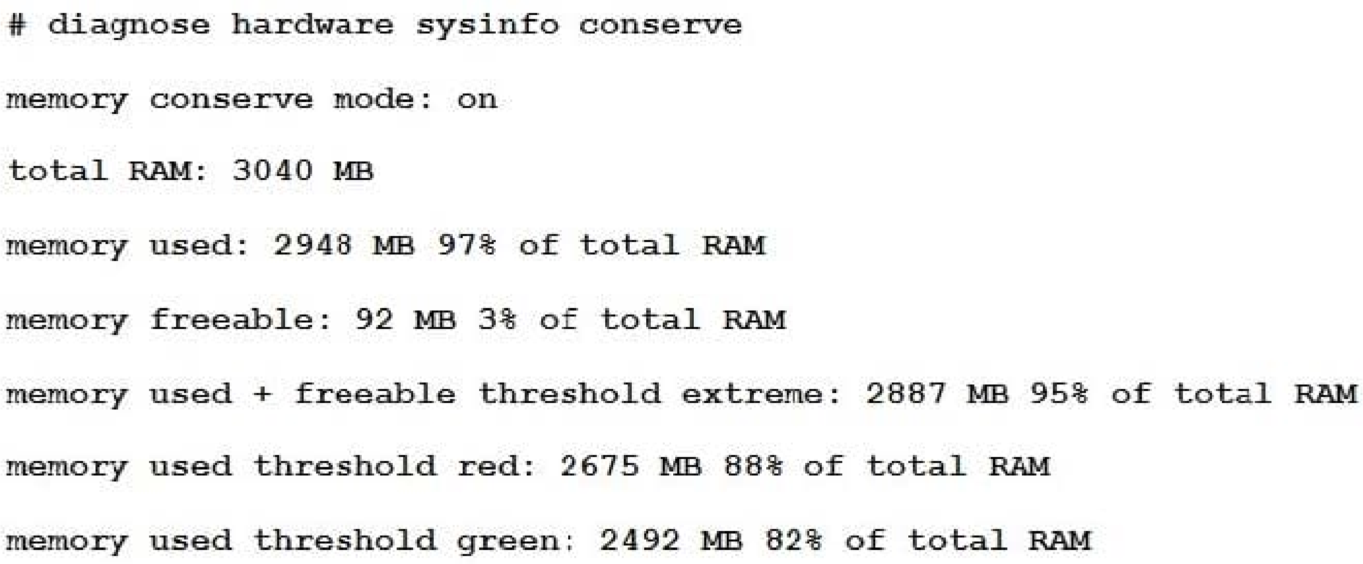
QUESTION 5

Examine this FortiGate configuration:



```
config system global
      set av-failopen pass
end
```

Examine the output of the following debug command:



```
# diagnose hardware sysinfo conserve

memory conserve mode: on

total RAM: 3040 MB

memory used: 2948 MB 97% of total RAM

memory freeable: 92 MB 3% of total RAM

memory used + freeable threshold extreme: 2887 MB 95% of total RAM

memory used threshold red: 2675 MB 88% of total RAM

memory used threshold green: 2492 MB 82% of total RAM
```

Based on the diagnostic outputs above, how is the FortiGate handling the traffic for new sessions that require inspection?

A. It is allowed, but with no inspection

B. It is allowed and inspected as long as the inspection is flow based

C. It is dropped.

D. It is allowed and inspected, as long as the only inspection required is antivirus.

Correct Answer: A