



CERTSWARRIOR

Fortinet

FCSS_EFW_AD-7.4

FCSS - Enterprise Firewall 7.4 Administrator

Questions&AnswersPDF

ForMoreInformation:

<https://www.certswarrior.com/>

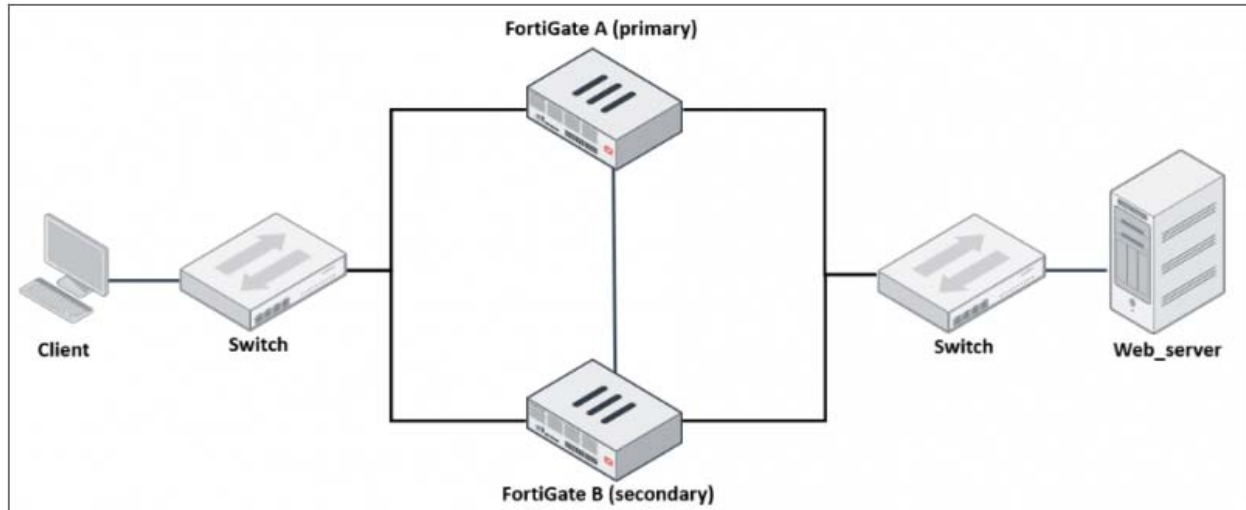
Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Latest Version: 6.0

Question: 1







Refer to the exhibits.



```

FortiGate_A # config system ha
FortiGate_A # show
config system ha
    set group-name "Fortinet"
    set mode a-a
    set password ENC ltj/cXx5WiX6
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
end

```

From	To	Source	Destination	Service	Action	NAT	Inspection Mode	Security Profiles
 port3	 port1	 Client	 Server	 DNS  HTTPS  HTTP	✓ ACCEPT	✓ NAT	Proxy-based	<div>AV default</div> <div>WEB default</div> <div>SSL deep-inspection</div>

The exhibits show a network diagram, the output from the command config system ha, and a firewall policy. What source MAC address does the web server detect when a user accesses it?

Response:

- A. The virtual MAC address of FortiGate B.
- B. The physical MAC address of FortiGate B.
- C. The virtual MAC address of FortiGate A.
- D. The physical MAC address of FortiGate A.

Answer: B

Question: 2

What does the dirty flag mean in a FortiGate session?

Response:

- A. Traffic has been blocked by the antivirus inspection.
- B. The next packet must be re-evaluated against the firewall policies.
- C. The session must be removed from the former primary unit after an HA failover.
- D. Traffic has been identified as from an application that is not allowed.

Answer: B

Question: 3

An administrator wants to simplify a new hub-and-spoke network deployment with the BGP recommended configuration. Which two sections on FortiManager must the administrator use? (Choose two.)

Response:

- A. Provisioning Templates
- B. Meta Fields
- C. Metadata Variables
- D. Automation Stitch

Answer: A,C

Question: 4

Which statement about administrative domains (ADOMs) on FortiManager is true?

Response:

- A. The number of configurable ADOMs is based on the FortiManager FortiCare service contract.
- B. The ADOM feature can be enabled by any administrative user.
- C. FortiGate devices with multiple VDOMs must be assigned to the same ADOM on FortiManager.
- D. ADOMs allow grouping of managed devices based on management criteria and administrative access.

Answer: D

Question: 5

An administrator must ensure that users cannot access sites containing malware and spyware, while also protecting them from phishing attempts. What is the most resource-efficient method to block access to these sites?

Response:

- A. Enable antivirus profiles to scan all web traffic and block downloads from these malicious sites.
- B. Configure FortiGuard Web Filtering and block the categories malware, spyware, and phishing to prevent access to such sites.
- C. Create a custom IPS policy to monitor and block all outbound traffic related to malware, spyware, and phishing sites.
- D. Set up a DNS filter and block domains related to these categories to stop users from reaching malicious content.

Answer: B

Question: 6

A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem?

(Choose two.)

Response:

- A. Firewall monitor.
- B. Policy monitor.
- C. Logs.
- D. Crashlogs.

Answer: C,D

Question: 7

The CLI command `set intelligent-mode <enable | disable>` controls the IPS engine's adaptive scanning behavior. Which of the following statements describes IPS adaptive scanning?

Response:

- A. Determines the optimal number of IPS engines required based on system load.
- B. Downloads signatures on demand from FDS based on scanning requirements.
- C. Determines when it is secure enough to stop scanning session traffic.
- D. Choose a matching algorithm based on available memory and the type of inspection being performed.

Answer: C

Question: 8

One firewall policy in an enterprise firewall is essentially used for IPS. Which configuration must the administrator check in this firewall policy to validate optimum performance for IPS?

Response:

- A. set cp-accel-mode enable
- B. set inspection-mode proxy
- C. set offload enable
- D. set np-acceleration enable

Answer: D

Question: 9

What are two impacts on applications if adjusting the TCP Maximum Segment Size (MSS) on FortiGate? (Choose two.)

Response:

- A. The MSS configuration is prone to errors since it requires a thorough understanding of the network path.
- B. The packet count increases adding unnecessary TCP headers when the MSS value is increased.
- C. The overall data throughput is decreased when there is a decrease in MSS value.
- D. The network efficiency improves when there is a decrease in MSS value.

Answer: A,C

Question: 10

How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

Response:

- A. FortiManager can download and maintain local copies of FortiGuard databases.
- B. FortiManager supports only FortiGuard push to managed devices.
- C. FortiManager will respond to update requests only if they originate from a managed device.
- D. FortiManager does not support rating requests.

Answer: A



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ