NSE5_FAZ-7.0^{Q&As}

Fortinet NSE 5 - FortiAnalyzer 7.0

Pass Fortinet NSE5_FAZ-7.0 Exam with 100% Guarantee

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

https://www.pass2lead.com/nse5_faz-7-0.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

An administrator has configured the following settings:

config system fortiview settings set resolve-ip enable end

What is the significance of executing this command?

A. Use this command only if the source IP addresses are not resolved on FortiGate.

B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.

C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.

D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Correct Answer: D

Reference: https://community.fortinet.com/t5/Fortinet-Forum/Hostnames-in- FortiAnalyzer/m-p/95351?m=156950

QUESTION 2

What is required to authorize a FortiGate on FortiAnalyzer using Fabric authorization?

A. A FortiGate ADOM

B. The FortiGate serial number

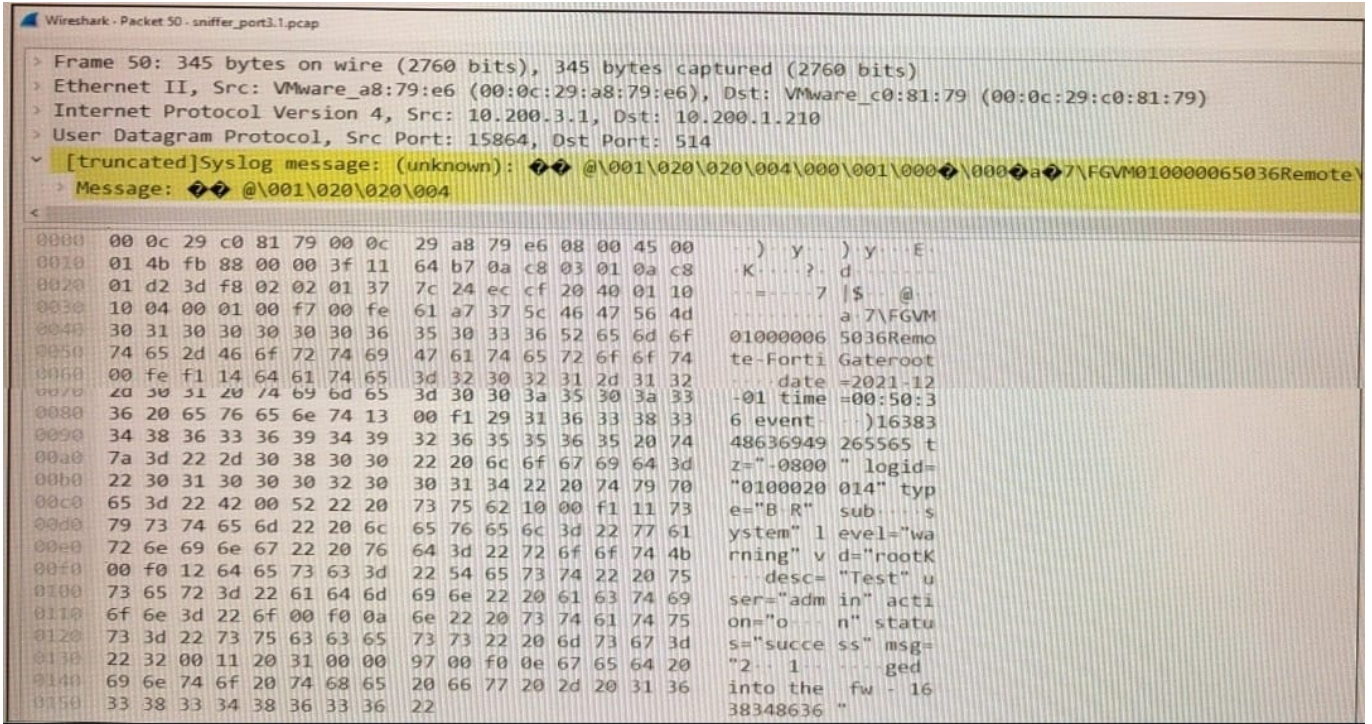C. A pre-shared key

D. Valid FortiAnalyzer credentials

Correct Answer: D

This method requires that both FortiGate and FortiAnalyzer are running version 7.0.1 or higher. It is also required that the FortiGate administrator has valid credentials to log in on FortiAnalyzer and complete the registration. FortiAnalyzer_7.0_Study_Guide-Online pag. 93
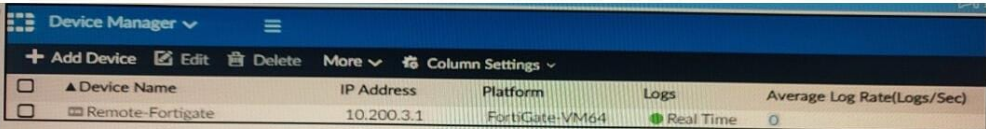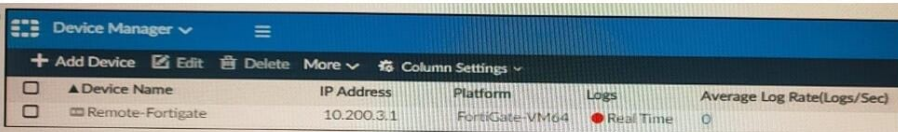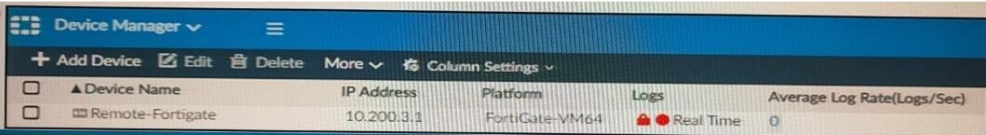
QUESTION 3

Refer to the exhibit.

Which image corresponds to the packet capture shown in the exhibit?

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

QUESTION 4

How are logs forwarded when FortiAnalyzer is using aggregation mode?

A. Logs are forwarded as they are received and content files are uploaded at a scheduled time.

B. Logs and content files are stored and uploaded at a scheduled time.

C. Logs are forwarded as they are received.

D. Logs and content files are forwarded as they are received.

Correct Answer: B

https://www.fortinetguru.com/2020/07/log-forwarding-fortianalyzer-fortios-6-2-3/
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/420493/modes Reference:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/63238/what-is- the-difference-between-log-forward-and-
log-aggregation-modes

QUESTION 5

In order for FortiAnalyzer to collect logs from a FortiGate device, what configuration is required? (Choose two.)

A. Remote logging must be enabled on FortiGate

B. Log encryption must be enabled

C. ADOMs must be enabled

D. FortiGate must be registered with FortiAnalyzer

Correct Answer: AD

Pg 70: "after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the
FortiGate device is configured to send logs to the FortiAnalyzer unit."

https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6- Administration%20Guide.pdf

Pg 45: "ADOMs must be enabled to support the logging and reporting of NON- FORTIGATE devices, such as
FortiCarrier, FortiClientEMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox."