

Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0

https://www.2passeasy.com/dumps/NSE5_FAZ-7.0/



NEW QUESTION 1

Which SQL query is in the correct order to query the database in the FortiAnalyzer?

- A. SELECT devid FROM Slog GROUP BY devid WHERE * user' =* USERI'
- B. SELECT devid WHERE 'u3er'='USERI' FROM \$ log GROUP BY devid
- C. SELECT devid FROM Slog- WHERE *user' =' USERI' GROUP BY devid
- D. FROM Slog WHERE 'user* =' USERI' SELECT devid GROUP BY devid

Answer: C

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:

- FROM
- WHERE
- GROUP BY
- ORDER BY
- LIMIT
- OFFSET

Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide.

NEW QUESTION 2

What is the purpose of using prefilters when configuring event handlers?

- A. They limit which logs are checked for matches by the other filters.
- B. They can filter the logs before they are processed by FortiAnalyzer
- C. They download new filters to be used in event handlers.
- D. They are common filters applied simultaneously to all event handlers.

Answer: A

NEW QUESTION 3

Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?

- A. Antivirus logs
- B. Web filter logs
- C. IPS logs
- D. Application control logs

Answer: B

NEW QUESTION 4

An administrator has moved FortiGate A from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

- A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
- B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
- C. Logs will be presented in both ADOMs immediately after the move.
- D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the ADOM1 SQL database.

Answer: BD

NEW QUESTION 5

Which statement about sending notifications with incident updates is true?

- A. Notifications can be sent only when an incident is created or deleted.
- B. You must configure an output profile to send notifications by email.
- C. Each incident can send notifications to a single external platform.
- D. Each connector used can have different notification settings.

Answer: D

NEW QUESTION 6

After generating a report, you notice the information you were expecting to see is not included in it. What are two possible reasons for this scenario? (Choose two.)

- A. You enabled auto-cache with extended log filtering.
- B. The logfile service has not indexed all the expected logs.
- C. The logs were overwritten by the data retention policy.
- D. The time frame selected in the report is wrong.

Answer: BC

NEW QUESTION 7

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with IPsec? (Choose two.)

- A. Must configure the FortiAnalyzer end of the tunnel only--the FortiGate end is auto-negotiated.
- B. Must establish an IPsec tunnel ID and pre-shared key.
- C. IPsec cannot be enabled if SSL is enabled as well.
- D. IPsec is only enabled through the CLI on FortiAnalyzer.

Answer: BD

Explanation:

Option B is correct because you must establish an IPsec tunnel ID and pre-shared key to secure the communication between FortiAnalyzer and FortiGate with IPsec12. The tunnel ID is a unique identifier for each tunnel and the pre-shared key is a secret passphrase that authenticates the peers.
Option D is correct because IPsec is only enabled through the CLI on FortiAnalyzer1. You cannot configure IPsec settings through the GUI on FortiAnalyzer.

NEW QUESTION 8

You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

- A. FortiAnalyzer uses log fetching to retrieve the logs when back online
- B. FortiGate uses the miglogd process to cache the logs
- C. The logfiled process stores logs in offline mode
- D. Logs are dropped

Answer: B

Explanation:

If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the miglogd process will drop cached logs. When the connection between the two devices is restored, the miglogd process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer will keep logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). But it is not intended for a lengthy FortiAnalyzer outage.

NEW QUESTION 9

What can the CLI command # diagnose test application oftpd 3 help you to determine?

- A. What devices and IP addresses are connecting to FortiAnalyzer
- B. What logs, if any, are reaching FortiAnalyzer
- C. What ADOMs are enabled and configured
- D. What devices are registered and unregistered

Answer: A

Explanation:

https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

NEW QUESTION 10

Logs are being deleted from one of your ADOMs earlier than the configured setting for archiving in your data policy. What is the most likely problem?

- A. The total disk space is insufficient and you need to add other disk.
- B. CPU resources are too high.
- C. The ADOM disk quota is set too low based on log rates.
- D. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device.

Answer: C

Explanation:

https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG_FAZ/1100_Storage/0017_Deleted%20device%20logs.htm
<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion>

NEW QUESTION 10

Refer to the exhibit.

The screenshot shows the 'New Administrator' configuration page in FortiAnalyzer. The 'User Name' is 'remoteadmin'. The 'Admin Type' is 'GROUP'. The 'GROUP' dropdown is set to 'remoteservergroup'. The checkbox 'Match all users on remote server' is checked and highlighted with a red box. Other fields include 'Avatar' (a green circle with 'R'), 'Comments' (empty), 'Admin Profile' (Super_User), 'Administrative Domain' (All ADOMs), 'JSON API Access' (None), 'Trusted Hosts' (OFF), and 'Meta Fields' (Advanced Options >).

The exhibit shows “remoteservergroup” is an authentication server group with LDAP and RADIUS servers. Which two statements express the significance of enabling “Match all users on remote server” when configuring a new administrator? (Choose two.)

- A. It creates a wildcard administrator using LDAP and RADIUS servers.
- B. Administrator can log in to FortiAnalyzer using their credentials on remote servers LDAP and RADIUS.
- C. Use remoteadmin from LDAP and RADIUS servers will be able to log in to FortiAnalyzer at anytime.
- D. It allows administrators to use two-factor authentication.

Answer: AB

NEW QUESTION 13

What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)

- A. RADIUS
- B. Local
- C. LDAP
- D. PKI
- E. TACACS+

Answer: ACE

NEW QUESTION 17

Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy. What is the most likely problem?

- A. CPU resources are too high
- B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device
- C. The total disk space is insufficient and you need to add other disk
- D. The ADOM disk quota is set too low, based on log rates

Answer: D

NEW QUESTION 18

Which statement is true about sending notifications with incident updates?

- A. Notifications can be sent only when an incident is updated or deleted.
- B. If you use multiple fabric connectors, all connectors must have the same notification settings
- C. Notifications can be sent only by email.
- D. You can send notifications to multiple external platforms

Answer: D

Explanation:

You can add more than one fabric connector, each with the same or different notification settings. The receiving side of the connector must be configured for the notifications to be sent successfully.

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 34: Fabric connectors also enable FortiAnalyzer to send notifications to ITSM platforms when a new incident is created or for any subsequent updates.

NEW QUESTION 21

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?
execute sql-local rebuild-adom <new-ADOM-name>

- A. To reset the disk quota enforcement to default
- B. To remove the analytics logs of the device from the old database
- C. To migrate the archive logs to the new ADOM
- D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Answer: D

Explanation:

- Are the device's analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:

```
# exe sql-local rebuild-adom <new-ADOM-name>
```

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 128: Are the device analytics logs required for reports in the new ADOM? If so, rebuild the new ADOM database

NEW QUESTION 26

An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mail server that can be used to send email. What could be the problem?

- A. Fortinet is assigned the Standard_ User administrator profile.
- B. A trusted host is configured.
- C. ADOM mode is configured with Advanced mode.
- D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A

Explanation:

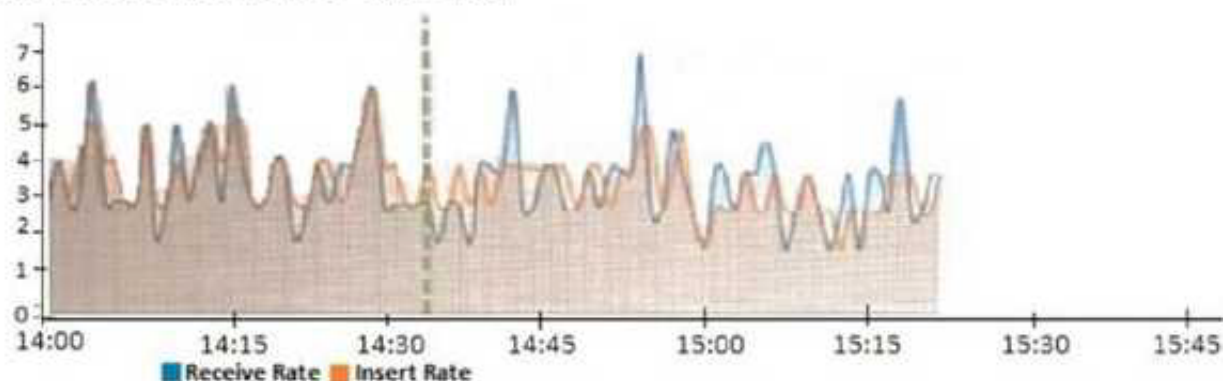
- Super_User, which, like in FortiGate, provides access to all device and system privileges.
- Standard_User, which provides read and write access to device privileges, but not system privileges.
- Restricted_User, which provides read access only to device privileges, but not system privileges. Access to the Management extensions is also removed.
- No_Permissions_User, which provides no system or device privileges. Can be used, for example, to temporarily remove access granted to existing admins.

FortiAnalyzer_7.0_Study_Guide-Online page 42

NEW QUESTION 29

View the exhibit.

Insert Rate vs Receive Rate - Last 1 hour



What does the data point at 14:35 tell you?

- A. FortiAnalyzer is dropping logs.
- B. FortiAnalyzer is indexing logs faster than logs are being received.
- C. FortiAnalyzer has temporarily stopped receiving logs so older logs' can be indexed.
- D. The sqlplugind daemon is ahead in indexing by one log.

Answer: B

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wi>

NEW QUESTION 31

Which statement about the FortiSIEM management extension is correct?

- A. Allows you to manage the entire life cycle of a threat or breach.
- B. Its use of the available disk space is capped at 50%.
- C. It requires a licensed FortiSIEM supervisor.
- D. It can be installed as a dedicated VM.

Answer: A

NEW QUESTION 34

Which two statements are true regarding fabric connectors? (Choose two.)

- A. Configuring fabric connectors to send notification to ITSM platform upon incident creation Is more efficient than third-party information from the FortiAnalyzer API.
- B. Fabric connectors allow to save storage costs and improve redundancy.
- C. Storage connector service does not require a separate license to send logs to cloud platform.
- D. Cloud-Out connections allow you to send real-time logs to pubic cloud accounts like Amazon S3, Azure Blob , and Google Cloud.

Answer: AD

NEW QUESTION 36

What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

- A. The size of newly generated reports is optimized to conserve disk space.
- B. FortiAnalyzer local cache is used to store generated reports.
- C. When new logs are received, the hard-cache data is updated automatically.
- D. The generation time for reports is decreased.

Answer: CD

NEW QUESTION 39

Which two methods can you use to send event notifications when an event occurs that matches a configured event handler? (Choose two.)

- A. SMS
- B. Email
- C. SNMP
- D. IM

Answer: BC

NEW QUESTION 41

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

- A. From the VM host manager, add an additional virtual disk and use the #execute lvm extend <disk number> command to expand the storage
- B. From the VM host manager, expand the size of the existing virtual disk
- C. From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk
- D. From the VM host manager, add an additional virtual disk and rebuild your RAID array

Answer: A

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848>

NEW QUESTION 44

When you perform a system backup, what does the backup configuration contain? (Choose two.)

- A. Generated reports
- B. Device list
- C. Authorized devices logs
- D. System information

Answer: BD

Explanation:

https://help.fortinet.com/fa/cli-olh/5-6-5/Content/Document/1400_execute/backup.htm

NEW QUESTION 45

Which statements are correct regarding FortiAnalyzer reports? (Choose two)

- A. FortiAnalyzer provides the ability to create custom reports.
- B. FortiAnalyzer allows you to schedule reports to run.
- C. FortiAnalyzer includes pre-defined reports only.
- D. FortiAnalyzer allows reporting for FortiGate devices only.

Answer: AB

NEW QUESTION 46

What purposes does the auto-cache setting on reports serve? (Choose two.)

- A. To reduce report generation time
- B. To automatically update the hcache when new logs arrive
- C. To reduce the log insert lag rate
- D. To provide diagnostics on report generation time

Answer: AB

NEW QUESTION 49

What does the disk status Degraded mean for RAID management?

- A. One or more drives are missing from the FortiAnalyzer uni
- B. The drive is no longer available to the operating system.
- C. The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.
- D. The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.
- E. The hard drive is no longer being used by the RAID controller

Answer: D

NEW QUESTION 50

For proper log correlation between the logging devices and FortiAnalyzer, FortiAnalyzer and all registered devices should:

- A. Use DNS
- B. Use host name resolution
- C. Use real-time forwarding
- D. Use an NTP server

Answer: D

NEW QUESTION 53

What are analytics logs on FortiAnalyzer?

- A. Log type Traffic logs.
- B. Logs that roll over when the log file reaches a specific size.
- C. Logs that are indexed and stored in the SQL.
- D. Raw logs that are compressed and saved to a log file.

Answer: C

NEW QUESTION 57

Which two statements express the advantages of grouping similar reports? (Choose two.)

- A. Improve report completion time.
- B. Conserve disk space on FortiAnalyzer by grouping multiple similar reports.
- C. Reduce the number of hcache tables and improve auto-hcache completion time.
- D. Provides a better summary of reports.

Answer: AC

NEW QUESTION 58

An administrator has configured the following settings:

```
config system global
set log-checksum md5-auth
end
```

What is the significance of executing this command?

- A. This command records the log file MD5 hash value.
- B. This command records passwords in log files and encrypts them.
- C. This command encrypts log transfer between FortiAnalyzer and other devices.
- D. This command records the log file MD5 hash value and authentication code.

Answer: D

NEW QUESTION 62

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results. Similarly, which feature you can use for FortiView?

- A. Export to Report Chart
- B. Export to PDF
- C. Export to Chart Builder
- D. Export to Custom Chart

Answer: A

NEW QUESTION 66

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

- A. Mail server
- B. Output profile
- C. SFTP server
- D. Report scheduling

Answer: AB

NEW QUESTION 69

If you upgrade your FortiAnalyzer firmware, what report elements can be affected?

- A. Output profiles
- B. Report settings
- C. Report scheduling
- D. Custom datasets

Answer: D

NEW QUESTION 72

Why must you wait for several minutes before you run a playbook that you just created?

- A. FortiAnalyzer needs that time to parse the new playbook.
B. FortiAnalyzer needs that time to back up the current playbooks.
C. FortiAnalyzer needs that time to ensure there are no other playbooks running.
D. FortiAnalyzer needs that time to debug the new playbook.

Answer: A

NEW QUESTION 77

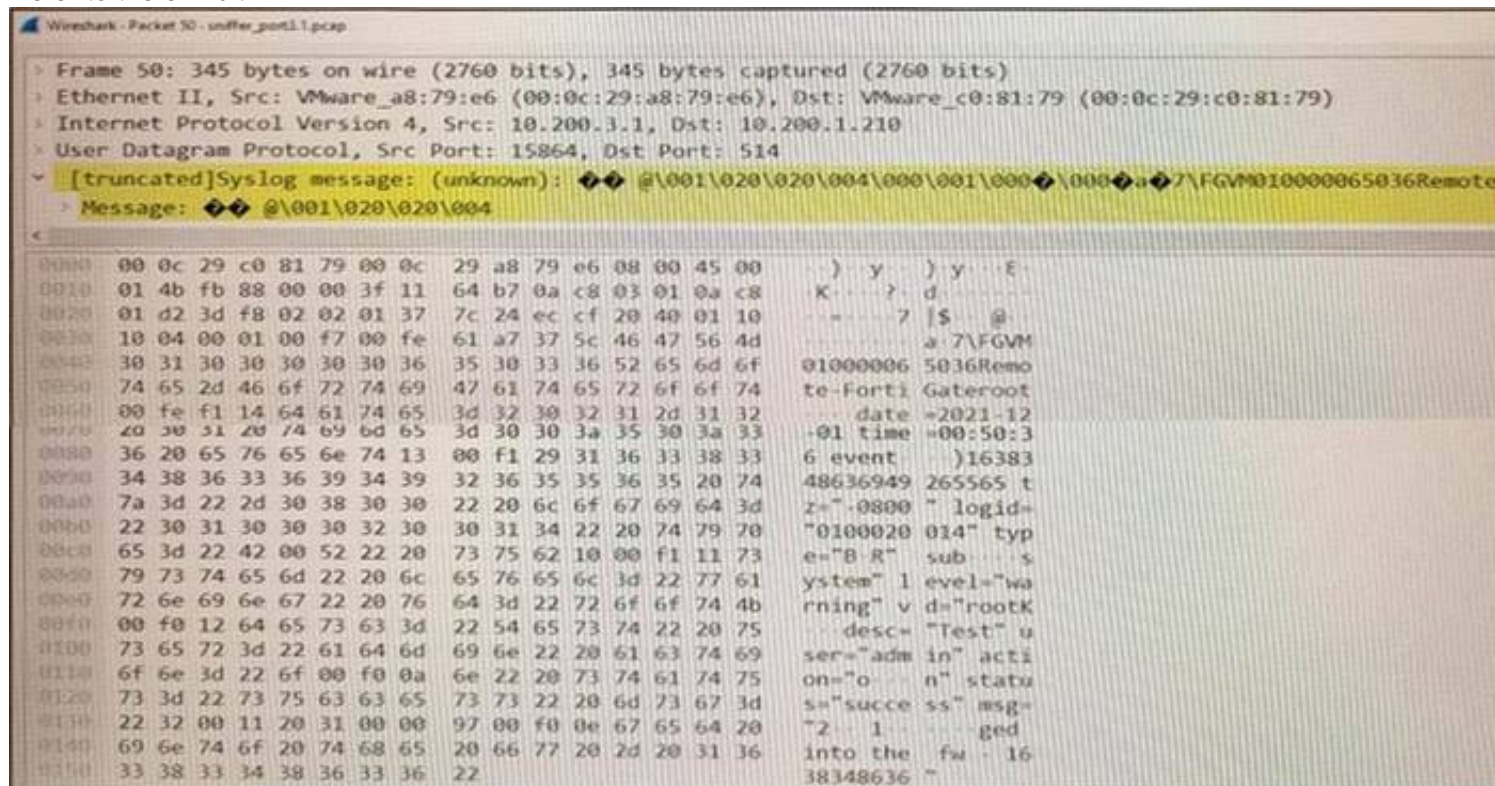
Which log will generate an event with the status Contained?

- A. An IPS log with action=pass.
B. A WebFilter log with action=dropped.
C. An AV log with action=quarantine.
D. An AppControl log with action=blocked.

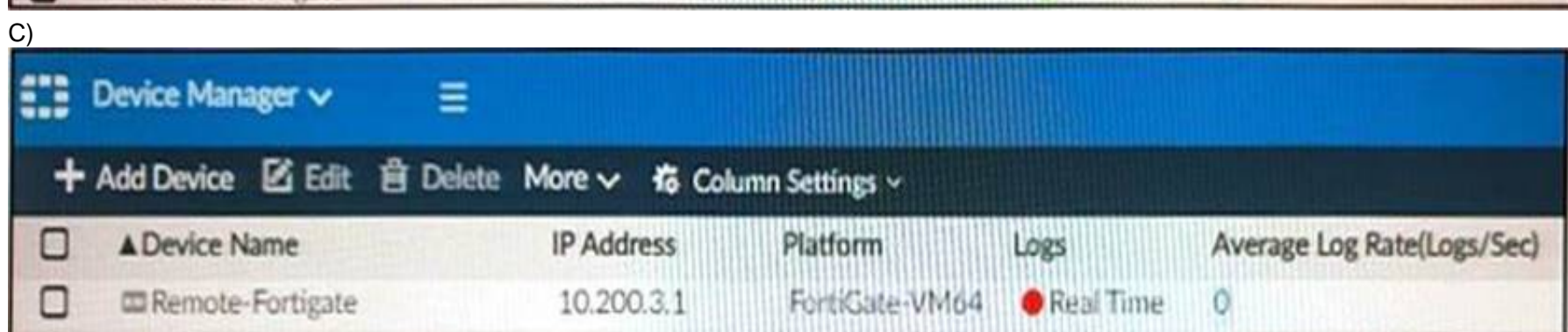
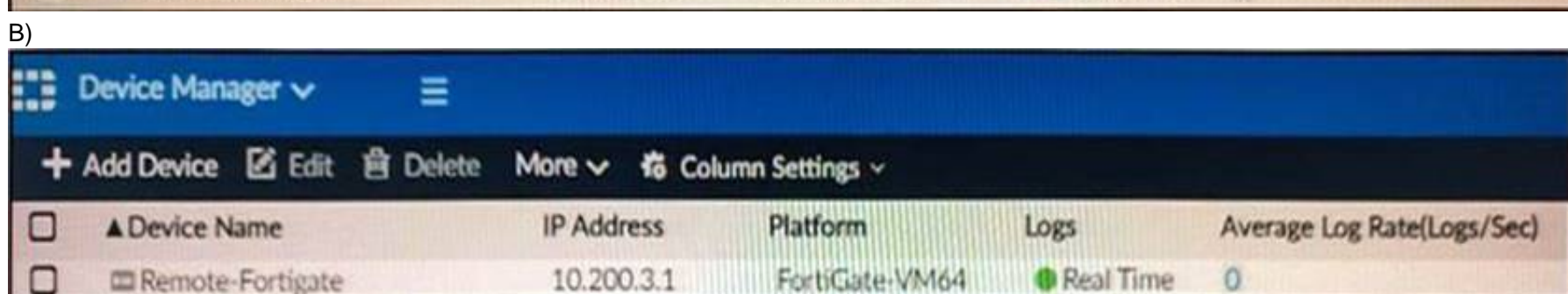
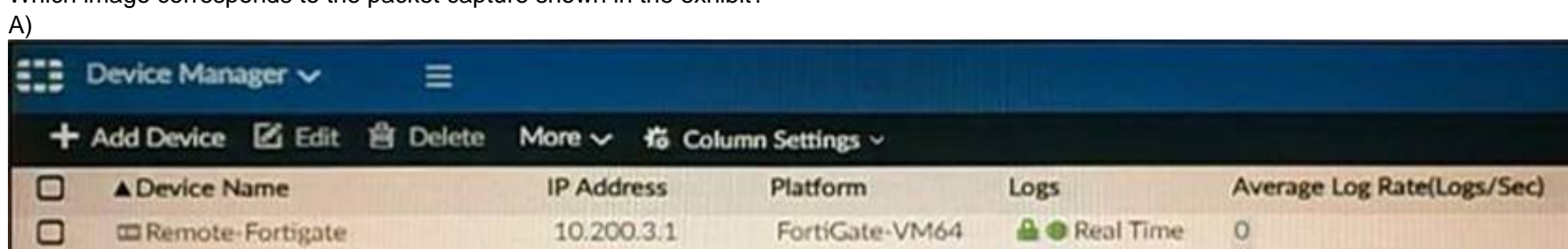
Answer: C

NEW QUESTION 79

Refer to the exhibit.



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



Device Manager					
+ Add Device Edit Delete More Column Settings					
<input type="checkbox"/>	▲ Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-Fortigate	10.200.3.1	FortiGate-VM64	 Real Time	0

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 81

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5_FAZ-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE5_FAZ-7.0 Product From:

https://www.2passeasy.com/dumps/NSE5_FAZ-7.0/

Money Back Guarantee

NSE5_FAZ-7.0 Practice Exam Features:

- * NSE5_FAZ-7.0 Questions and Answers Updated Frequently
- * NSE5_FAZ-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_FAZ-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE5_FAZ-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year