Exam Questions NSE5_FAZ-7.2

Fortinet NSE 5 - FortiAnalyzer 7.2

https://www.2passeasy.com/dumps/NSE5_FAZ-7.2/

NEW QUESTION 1
Which SQL query is in the correct order to query the database in the FortiAnslyzer?

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

Answer: C

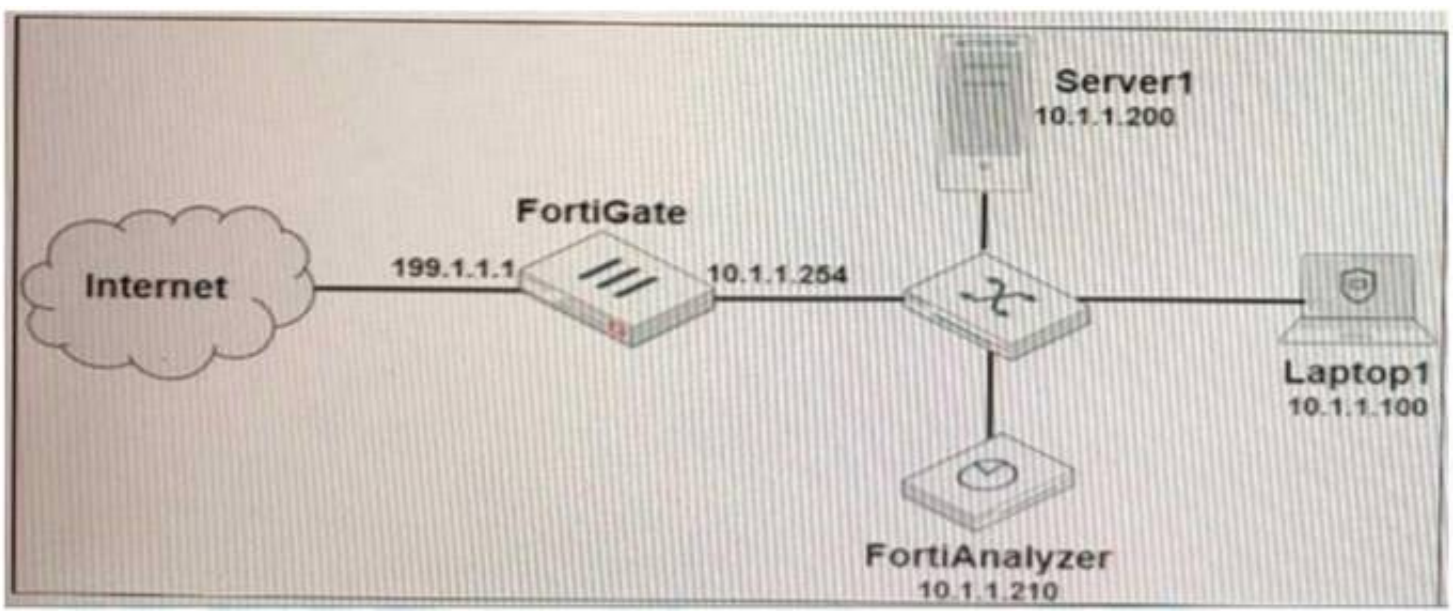
Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:
•FROM
•WHERE
•GROUP BY
•ORDER BY
• LIMIT
• OFFSET
Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide.

NEW QUESTION 2
What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

A. Chart Builder
B. Export to Report Chart
C. Dataset Library
D. Custom View

Answer: B

NEW QUESTION 3
Refer to the exhibit.



Laptopt is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin" and coming from Laptop1:
Which filter will achieve the desired result?

A. operation-login & performed_on=="GUI(10.1.1.100)" & user!=admin
B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
C. operation-login & dstip==10.1.1.210 & userl-admin
D. operation-login & performed_on=="GUI(10.1.1.210)' & user!=admin

Answer: A

Explanation:
On there the task was to create a filter for failed logins from any other location but the local computer: "Add the text performed_on!~10.0.1.10. This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer."

NEW QUESTION 4
A rogue administrator was accessing FortiAnalyzer without permission, and you are tasked to see what activity was performed by that rogue administrator on FortiAnalyzer.
What can you do on FortiAnalyzer to accomplish this?

A. Click FortiView and generate a report for that administrator.
B. Click Task Monitor and view the tasks performed by that administrator.
C. Click Log View and generate a report for that administrator.
D. View the tasks performed by the rogue administrator in Fabric View.

Answer: B

NEW QUESTION 5
What are two benefits of using fabric connectors? (Choose two.)

A. They allow FortiAnalyzer to send logs in real-time to public cloud accounts.
B. You do not need an additional license to send logs to the cloud platform.
C. Fabric connectors allow you to improve redundancy.
D. Using fabric connectors is more efficient than using third-party polling with API.

Answer: AC

NEW QUESTION 6
What are two of the key features of FortiAnalyzer? (Choose two.)

A. Centralized log repository
B. Cloud-based management
C. Reports
D. Virtual domains (VDOMs)

Answer: AC

NEW QUESTION 7
Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

A. ADOMs are enabled by default.
B. ADOMs constrain other administrator's access privileges to a subset of devices in the device list.
C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
D. All administrators can create ADOMs--not just the admin administrator.

Answer: BC

NEW QUESTION 8
Which item must you configure on FortiAnalyzer to email generated reports automatically?

A. Output profile
B. Report scheduling
C. SFTP server
D. SNMP server

Answer: A

NEW QUESTION 9
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 10
By default, what happens when a log file reaches its maximum file size?

A. FortiAnalyzer overwrites the log files.
B. FortiAnalyzer stops logging.
C. FortiAnalyzer rolls the active log by renaming the file.
D. FortiAnalyzer forwards logs to syslog.

Answer: C

NEW QUESTION 10
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 14
What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the device log settings?

A. The log file is stored as a raw log and is available for analytic support.
B. The log file rolls over and is archived.
C. The log file is purged from the database.
D. The log file is overwritten.

Answer: B

NEW QUESTION 17
In the FortiAnalyzer FortiView, source and destination IP addresses from FortiGate devices are not resolving to a hostname.
How can you resolve the source and destination IP addresses, without introducing any additional performance impact to FortiAnalyzer?

A. Resolve IP addresses on a per-ADOM basis to reduce delay on FortiView while IPs resolve
B. Configure # set resolve-ip enable in the system FortiView settings
C. Configure local DNS servers on FortiAnalyzer
D. Resolve IP addresses on FortiGate

Answer: D

Explanation:
https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/
“As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only”

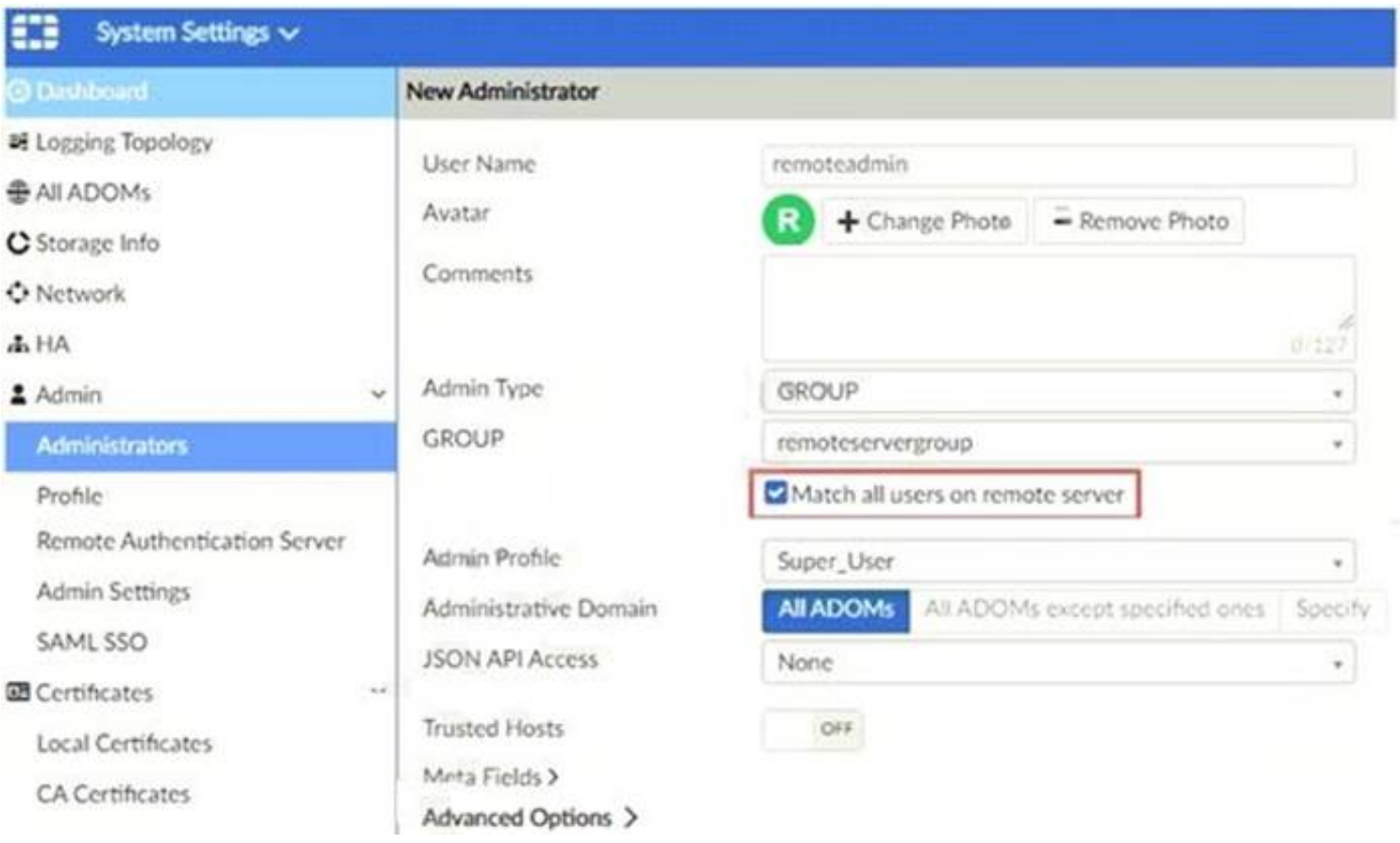
NEW QUESTION 18
What can the CLI command # diagnose test application oftpd 3 help you to determine?

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 23
Refer to the exhibit.



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 28

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 32
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 36
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 mall 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

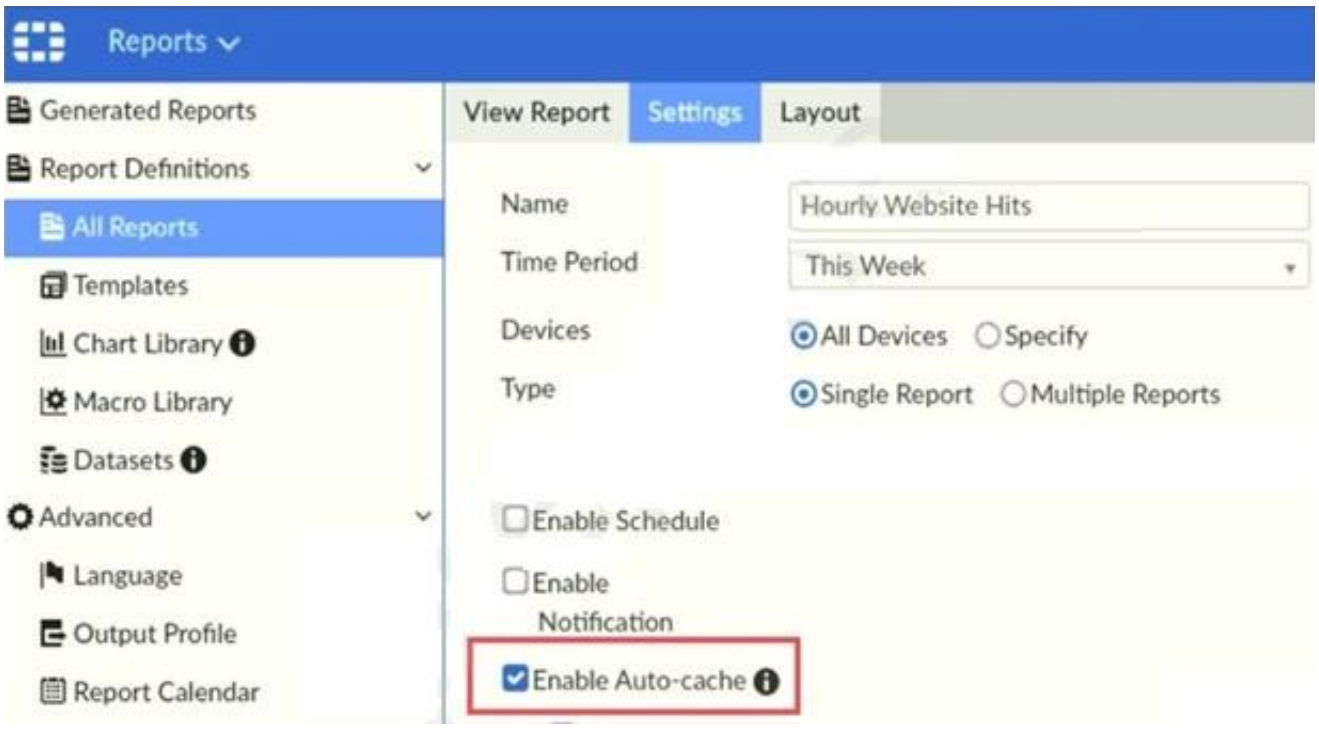
NEW QUESTION 40
What is the purpose of employing RAID with FortiAnalyzer?

A. To introduce redundancy to your log data
B. To provide data separation between ADOMs
C. To separate analytical and archive data
D. To back up your logs

Answer: A

Explanation:
https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%

NEW QUESTION 41
Refer to the exhibit.



Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)

A. Report size will be optimized to conserve disk space on FortiAnalyzer.

B. Reports will be cached in the memory.
C. This feature is automatically enabled for scheduled reports.
D. Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

Answer: CD

Explanation:
"Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already."
FortiAnalyzer_7.0_Study_Guide-Online page 306

NEW QUESTION 46
Which daemon is responsible for enforcing raw log file size?

A. logfiled
B. oftpd
C. sqlplugind
D. miglogd

Answer: A

NEW QUESTION 51
You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed.
What is the recommended method to replace the disk?

A. Shut down FortiAnalyzer and then replace the disk
B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level
C. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running
D. Perform a hot swap

Answer: A

Explanation:
supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with software RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta-

NEW QUESTION 53
Which two constraints can impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

A. License type
B. Disk size
C. Total quota
D. RAID level

Answer: BD

Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

NEW QUESTION 56
On the RAID management page, the disk status is listed as Initializing.
What does the status Initializing indicate about what the FortiAnalyzer is currently doing?

A. FortiAnalyzer is ensuring that the parity data of a redundant drive is valid
B. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state
C. FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant
D. FortiAnalyzer is functioning normally

Answer: C

NEW QUESTION 59
The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device. What can be the reason for this failure?

A. FortiAnalyzer is in an HA cluster.
B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
C. ADOMs are not enabled on FortiAnalyzer.
D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.

Answer: C

NEW QUESTION 61
Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

A. System information

B. Logs from registered devices
C. Report information
D. Database snapshot

Answer: AC

Explanation:
What does the System Configuration backup include?
System information, such as the device IP address and administrative user information. Device list, such as any devices you configured to allow log access.
Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.
FortiAnalyzer_7.0_Study_Guide-Online pag. 29
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 29: What does the System Configuration backup include?
• System information, such as the device IP address and administrative user information
• Device list, such as any devices you configured to allow log access
• Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

NEW QUESTION 65
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 66
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 70
You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.
What does the disk quota refer to?

A. The maximum disk utilization for each device in the ADOM
B. The maximum disk utilization for the FortiAnalyzer model
C. The maximum disk utilization for the ADOM type
D. The maximum disk utilization for all devices in the ADOM

Answer: D

NEW QUESTION 72
What FortiGate process caches logs when FortiAnalyzer is not reachable?

A. logfiled
B. sqlplugind
C. oftpd
D. miglogd

Answer: D

NEW QUESTION 74
Which statements are correct regarding FortiAnalyzer reports? (Choose two)

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

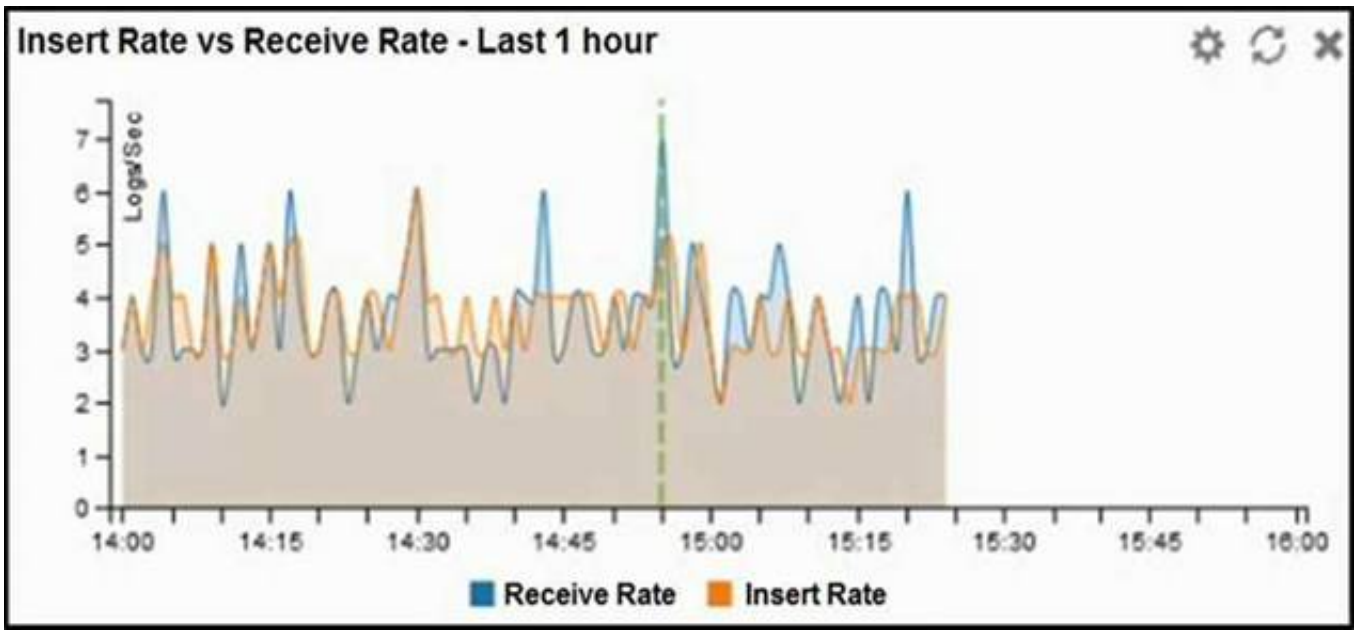
Answer: AB

NEW QUESTION 79
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 80
Refer to the exhibit.



What does the data point at 14:55 tell you?

A. The received rate is almost at its maximum for this device
B. The sqlplugind daemon is behind in log indexing by two logs
C. Logs are being dropped
D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

Answer: D

NEW QUESTION 83
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 84
FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days.
What is the most likely problem?

A. Quota enforcement is acting on analytical data before a report is complete
B. Logs are rolling before the report is run
C. CPU resources are too high
D. Disk utilization for archive logs is set for 15 days

Answer: B

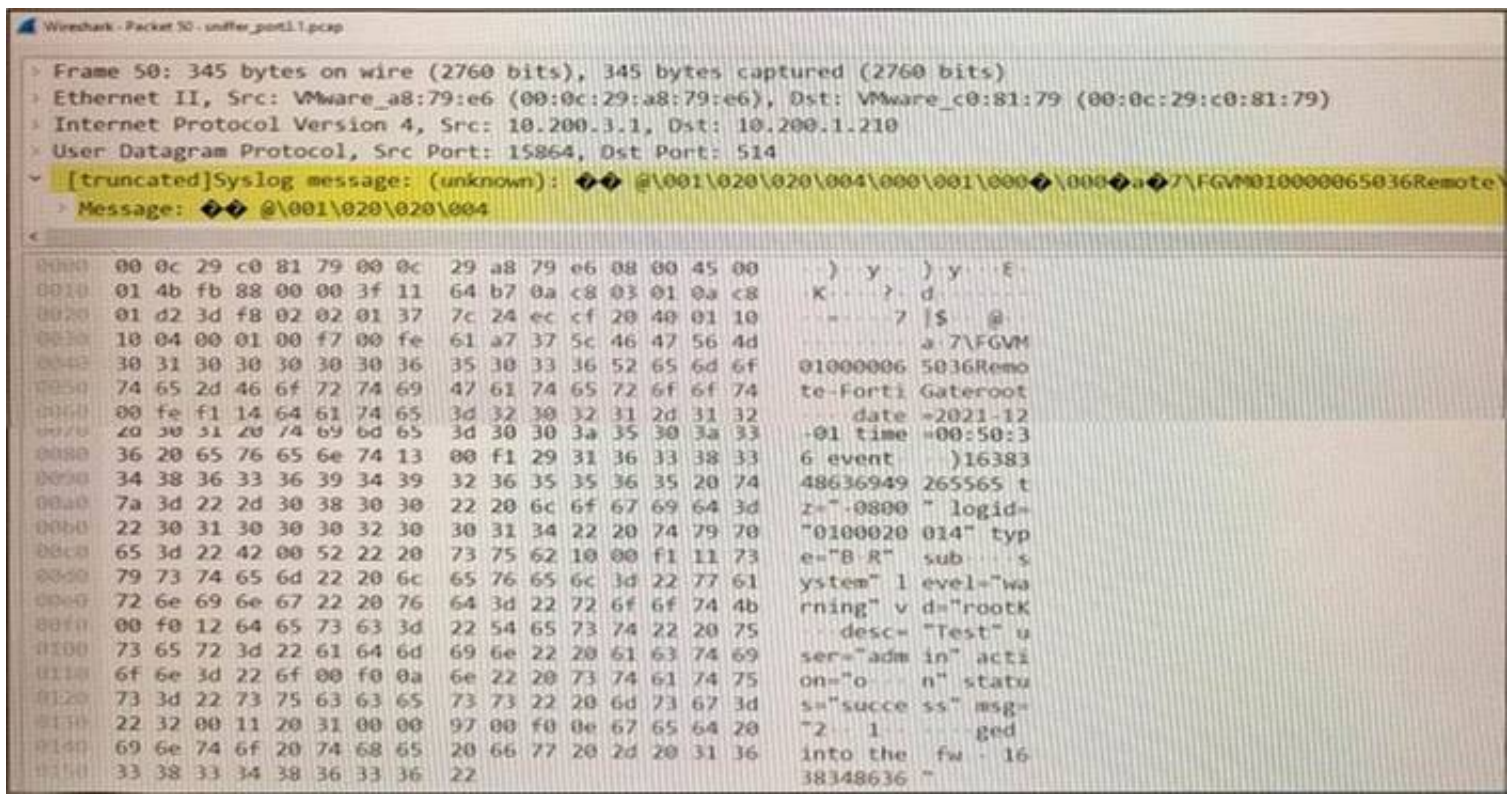
NEW QUESTION 86
Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

A. Incidents dashboards
B. Threat hunting
C. FortiView Monitor
D. Outbreak alert services

Answer: B

Explanation:
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

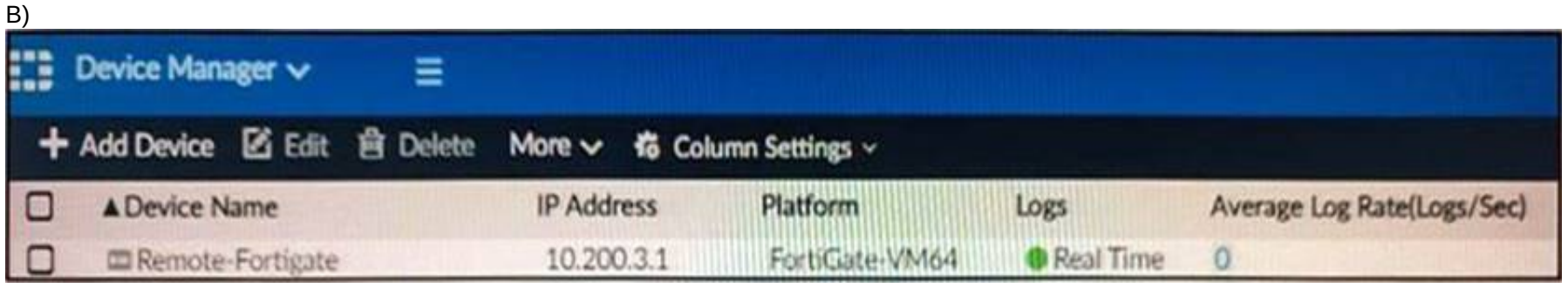
NEW QUESTION 87
Refer to the exhibit.



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

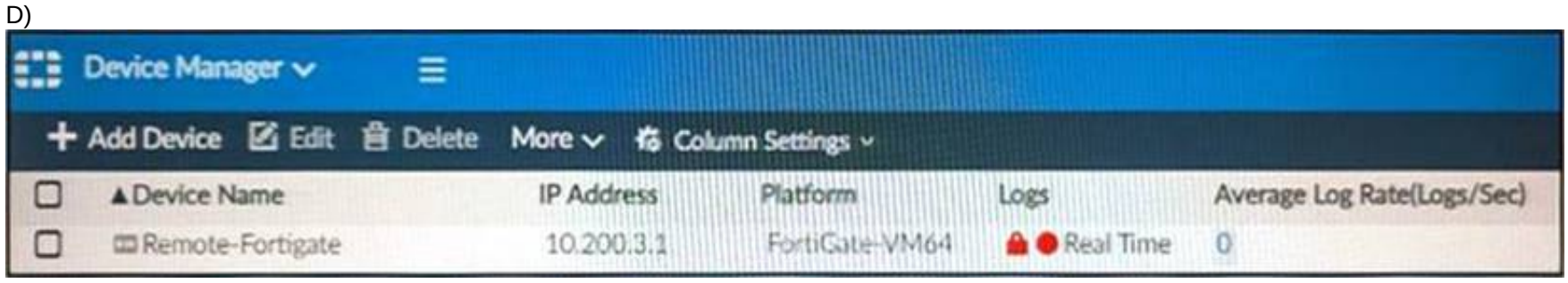
A)

B)



C)

D)



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

Answer: C

NEW QUESTION 88
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5_FAZ-7.2 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-7.2 Product From:

https://www.2passeasy.com/dumps/NSE5_FAZ-7.2/

Money Back Guarantee

NSE5_FAZ-7.2 Practice Exam Features:

* NSE5_FAZ-7.2 Questions and Answers Updated Frequently

* NSE5_FAZ-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_FAZ-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_FAZ-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year