Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

NEW QUESTION 1
An administrator has moved a FortiGate device 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 present in both ADOMs immediately after the move.
D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the database.

Answer: AD

Explanation:
When a device is moved from one ADOM to another, analytics logs can be moved automatically, but you may need to rebuild the database for the logs to be fully transferred and usable in the new ADOM. Archived logs, however, do not move automatically between ADOMs.

NEW QUESTION 2
Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

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

Answer: C

Explanation:
RAID level affects how much disk space is reserved for redundancy and fault tolerance. For example, RAID 1 mirrors data, meaning you need more space for redundancy, while RAID 5 or RAID 6 reserves space for parity.
Disk size directly influences the total available and reserved space since the larger the disk, the more space may need to be reserved for system functions, logs, and other operations.
The total quota and license type do not directly impact the reserved disk space, though they do influence other aspects of capacity and functionality.

NEW QUESTION 3
Refer to the exhibit.

```
FortiGate # diagnose test application fgtlogd 4
Queues in all miglogds: cur:31  total-so-far:4642589
global log dev statistics:
faz=180191781, faz_cloud=0, fds_log=0
faz 0: sent=180189698, failed=4507, cached=0, dropped=0
```

Based on the output, what can you conclude about the FortiAnalyzer logging status?

A. The connection between FortiGate and FortiAnalyzer is overloaded.
B. FortiGate has logs to send, but FortiAnalyzer is unavailable.
C. FortiGate is configured to send logs in batches.
D. FortiGate is sending logs again after it performed a reboot.

Answer: B

Explanation:
The output shows that FortiGate has sent a large number of logs (sent=180189698), but some logs have failed to be sent (failed=4507). This suggests that FortiAnalyzer was temporarily unavailable or had an issue receiving logs, leading to the failure count. There are no logs cached or dropped, indicating FortiGate is still attempting to send logs but with some failures.

NEW QUESTION 4
Which three RAID configurations provide fault tolerance on FortiAnalyzer? (Choose three.)

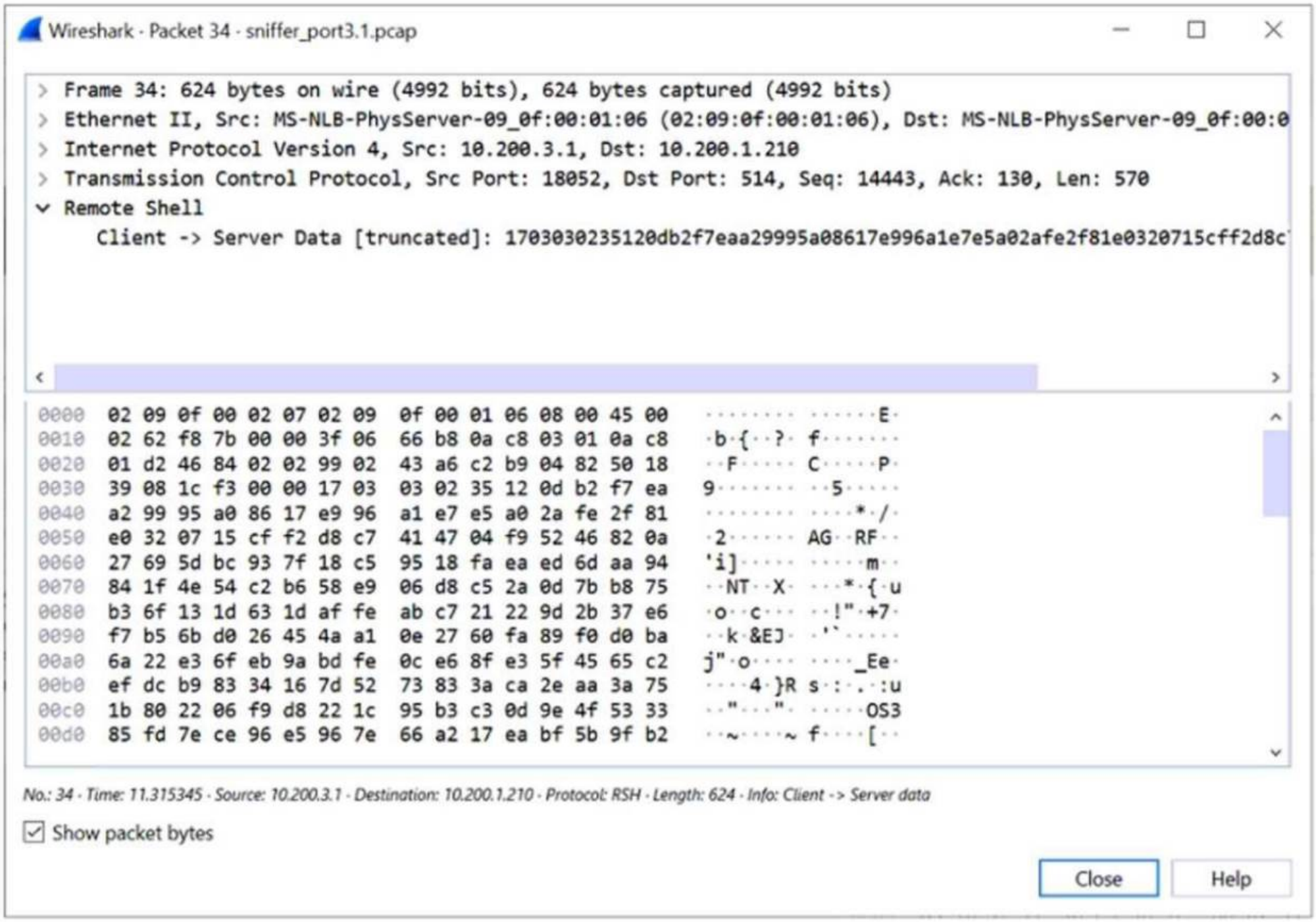
A. RAIDO
B. RAID 5
C. RAID1
D. RAID 6+0
E. RAID 0+0

Answer: BCD

Explanation:
RAID 1 provides fault tolerance through disk mirroring.
RAID 5 provides fault tolerance by using distributed parity across multiple disks. RAID 6+0 combines striping with double parity, offering enhanced fault tolerance.
RAID 0 and RAID 0+0 do not provide any fault tolerance, as they focus on performance through data striping but offer no redundancy.

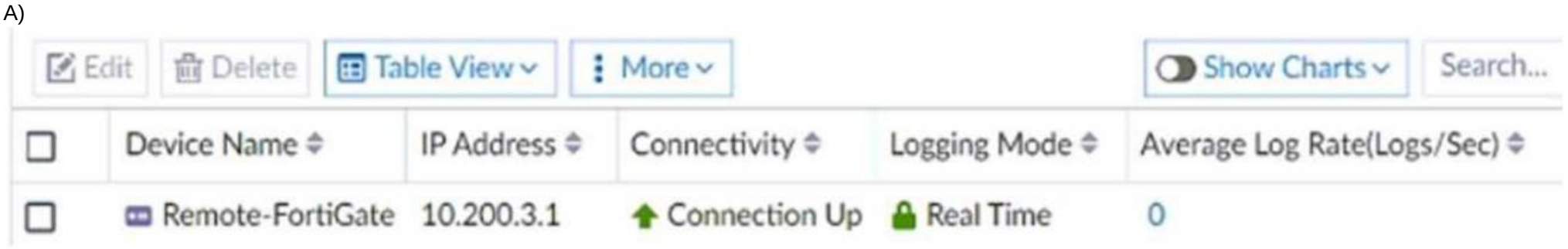
NEW QUESTION 5
Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark

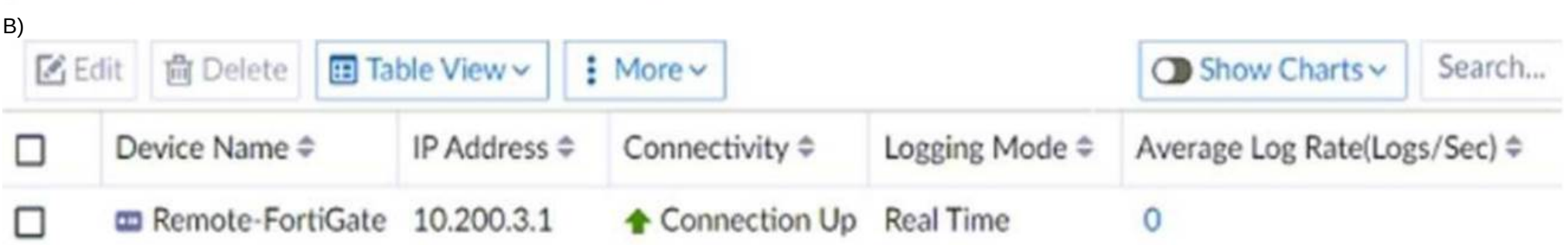


Which image corresponds to the packet capture shown in the exhibit?

A)

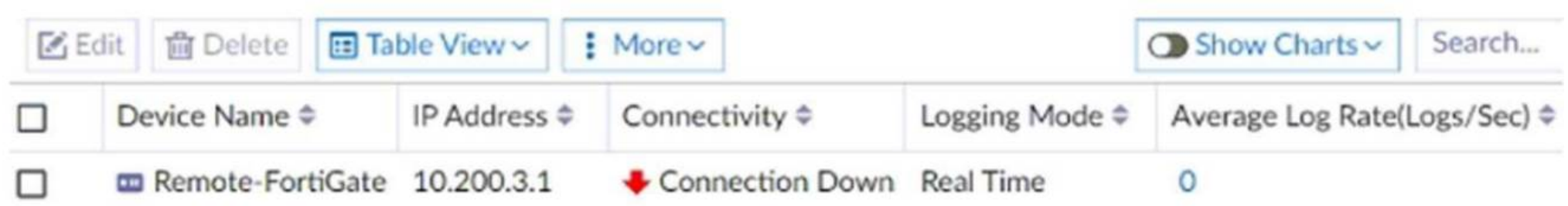


B)



C)

D)



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Chosen image shows the device Remote-FortiGate with the IP 10.200.3.1 and a connection status of "Connection Up," which is consistent with the packet capture details showing active communication between the client and server.

NEW QUESTION 6
Which feature can you configure to add redundancy to FortiAnalyzer?

A. Primary and secondary DNS
B. VLAN interfaces
C. IPv6 administrative access
D. Link aggregation

Answer: D

Explanation:
Link aggregation is a method used to combine multiple network connections in parallel to increase throughput and provide redundancy in case one of the links fail. This feature is used in network appliances, including FortiAnalyzer, to add redundancy to the network connections, ensuring that there is a backup path for traffic if the primary path becomes unavailable.
Reference: The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

NEW QUESTION 7
Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)

A. Configure trusted hosts.
B. Limit access to specific virtual domains.
C. Fabric connectors to external LDAP servers.
D. Use administrator profiles.

Answer: AD

Explanation:
Configure trusted hosts.
Trusted hosts restrict administrative access to FortiAnalyzer by limiting the IP addresses or subnets from which administrators can log in.
Use administrator profiles.
Administrator profiles define roles and permissions, restricting what specific administrators can access and manage on FortiAnalyzer.
The other options are not applicable because:
Limiting access to specific virtual domains is not applicable to FortiAnalyzer, as virtual domains (VDOMs) are a concept used in FortiGate, not FortiAnalyzer.
Fabric connectors to external LDAP servers are used for authentication purposes but do not directly restrict administrative access based on roles or IP addresses.

NEW QUESTION 8
Which statement about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer is true?

A. If devices were registered to FortiAnalyzer before forming a cluster, you can manually add them togethe
B. FortiAnalyzer distinguishes each cluster member by the IP addresses in log message header
C. If the HA primary device becomes unavailable, you must remove it from the HA cluster list on FortiAnalyze
D. The FortiGate HA cluster must be in active-passive mode in order to avoid conflict.

Answer: B

Explanation:
This allows FortiAnalyzer to correctly identify and process logs from different members of the HA cluster.

NEW QUESTION 9
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

Explanation:
FortiAnalyzer acts as a central repository for collecting and storing logs from multiple Fortinet devices. This centralized log management facilitates efficient analysis, search, and correlation of logs from across the network.
FortiAnalyzer provides robust reporting capabilities, allowing users to generate detailed reports based on collected logs and data. These reports can include insights on security events, network performance, and compliance.
Cloud-based management is not a primary feature of FortiAnalyzer, as it is typically an on-premises appliance, although it can integrate with cloud services.
Virtual domains (VDOMs) are a feature of FortiGate devices, allowing them to be partitioned into multiple virtual domains for administrative and policy separation.
FortiAnalyzer itself does not provide VDOMs.

NEW QUESTION 10

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCP_FAZ_AD-7.4 Practice Exam Features:

* FCP_FAZ_AD-7.4 Questions and Answers Updated Frequently

* FCP_FAZ_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FAZ_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FAZ_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year