Fortinet.NSE6_FAZ-7.2.by.Sem.19q

Number: NSE6_FAZ-7.2
Passing Score: 800
Time Limit: 120
File Version: 2.0

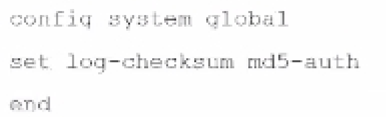
Exam Code: NSE6_FAZ-7.2

Exam Name: Fortinet NSE 6 - FortiAnalyzer 7.2 Administrator

Exam A

QUESTION 1

An administrator has configured the following settings:



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

What is the purpose of executing these commands?

A. To record the hash value and authentication code of log files.

B. To encrypt log transfer between FortiAnalyzer and other devices.

C. To verify the integrity of the log files received.

D. To create the secure channel used by the OFTP process.

Correct Answer: C
Section:
Explanation:

The purpose of executing the provided CLI commands, which include setting the log-checksum to md5-auth, is to ensure the integrity of the log files. This setting is used to record the MD5 hash value of log files, which is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. By using MD5 authentication, FortiAnalyzer ensures that the log files have not been altered or tampered with during transit, thereby verifying their integrity upon receipt. This is not related to encrypting log transfers, scheduling reports, or creating secure channels for OFTP (Over-the-FortiGate Protocol) processes.

QUESTION 2

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

A. Each cluster member sends its logs directly to FortiAnalyzer.

B. You must add the device lo the cluster first, and then registers the cluster with FortiAnalyzer.

C. FortiAnalyzer distinguishes each cluster member by its MAC address.

D. Only the primary device in the cluster communicates with FortiAnalyzer.

Correct Answer: D
Section:
Explanation:

In a FortiGate high availability (HA) cluster, only the primary device sends its logs to the FortiAnalyzer. This is to ensure that logs are not duplicated between the primary and secondary devices in the cluster. The configuration of the FortiAnalyzer server on the FortiGate is such that the HA primary device is set as the server that forwards the logs.
Reference: FortiAnalyzer 7.4.1 Administration Guide, sections mentioning HA cluster configuration and log forwarding.

QUESTION 3

Which two statements are true regarding FortiAnalyzer system backups? (Choose two.)

A. Existing reports can be included in the backup files.

B. The system reserves at least 5% to 20% disk space for backup files.

C. Scheduled system backups can be configured only from the CLI.

D. Backup files can be uploaded to SCP and SFTP servers.

Correct Answer: A, D

Section:
Explanation:
FortiAnalyzer allows for the inclusion of existing reports in the backup files, providing a comprehensive backup of configurations and data. Additionally, the backup files can be configured to be uploaded to SCP and SFTP servers, ensuring secure transfer and offsite storage of backup data. This can be configured both in the GUI and the CLI, providing flexibility in how backups are scheduled and managed.
Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Scheduling automatic backups' section.

QUESTION 4
In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

A. The traffic destination is another FoitiGate in the fabric.
B. Log redundancy is configured in the fabric.
C. The upstream FortiGate is configured to do NAT.
D. The downstream device cannot connect to FortiAnalyzer.

Correct Answer: D
Section:
Explanation:
In a Fortinet Security Fabric, an upstream FortiGate may create traffic logs for sessions initiated on downstream FortiGate devices if the downstream device is unable to connect to FortiAnalyzer. This allows for continuity of logging and ensures that session logs are captured and stored even if the downstream device loses its connection to the log management system.
Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Fortinet Security Fabric' section.

QUESTION 5
Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

A. LDAP servers IP addresses added as trusted hosts
B. One or more remote LDAP servers
C. A local wildcard administrator account
D. An administrator group

Correct Answer: B, D
Section:
Explanation:
To allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group, you must configure one or more remote LDAP servers and an administrator group. First, you configure the LDAP server(s) by specifying the server name, IP, and other details such as the Common Name Identifier and Distinguished Name. Then, you add the LDAP server to a user group. Finally, you create an administrator account that uses this user group for authentication, allowing any user from the specified LDAP group to authenticate.
Reference: FortiAnalyzer 7.2 Administrator Guide, 'Configuring remote authentication for administrators using LDAP' section.

QUESTION 6
Which two statements are true regarding the log synchronization states for HA on FortiAnalyzer? (Choose two.)

A. Log Data Sync provides real-time log synchronization to all backup devices.
B. When Log Data Sync is turned on, the backup device reboots and then rebuilds the log database with the synchronized logs.
C. With Initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
D. By default. Log Data Sync is disabled on all backup devices.

Correct Answer: A, C
Section:
Explanation:

For HA on FortiAnalyzer, Log Data Sync ensures real-time log synchronization among all cluster members, including backup devices. This feature is enabled by default. The Initial Logs Sync state is triggered when a new unit is added to an HA cluster, where the primary unit synchronizes its logs with the newly added unit. After the initial synchronization, the secondary unit reboots and rebuilds its log database with the synchronized logs.
Reference: FortiAnalyzer 7.2 Administrator Guide, 'Log synchronization' section.

QUESTION 7
An administrator, fortinet, can 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 alert emails.
What can be the problem?

A. ADOM mode is configured with Advanced mode.
B. fortinet is assigned the Standard_User administrative profile.
C. A trusted host is configured.
D. fortinet is assigned Restricted_User administrative profile.

Correct Answer: B
Section:
Explanation:
If the administrator 'fortinet' can view logs and perform device management tasks but cannot create a mail server for alert emails, it is likely due to the administrative profile assigned to them. The Standard_User administrative profile may restrict certain administrative functions, such as creating mail servers. To perform all administrative tasks, including creating mail servers, a higher privilege profile, such as Super_Admin, might be required.
Reference: FortiAnalyzer 7.2 Administrator Guide, 'Mail Server' section.

QUESTION 8
Which two statements are true regarding fabric connectors? (Choose two.)

A. Using fabric connectors is more efficient than third-party polling information from the FortiAnalyzer API
B. Cloud-out connectors allow you to send real-time logs to public cloud accounts like Amazon S3.
C. Fabric connectors allow you to save storage costs and improve redundancy.
D. The storage connector service does not require a separate license to send logs to the cloud platform.

Correct Answer: A, D
Section:
Explanation:
Fabric connectors in FortiAnalyzer, such as security fabric connectors (e.g., FortiClient EMS, FortiMail, FortiCASB) and storage connectors (e.g., Amazon S3, Azure Blob Container, Google Cloud Storage), provide efficient integration and data sharing capabilities. Using fabric connectors for direct integration with FortiAnalyzer is more efficient and reliable than relying on third-party applications to poll information through the FortiAnalyzer API. Additionally, the ability to send logs to cloud storage platforms like Amazon S3, Azure Blob, and Google Cloud directly through storage connectors is a built-in feature that does not require an additional license, thus saving on storage costs and improving redundancy without incurring extra licensing fees.
Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Fabric Connectors' and 'Storage connectors' sections.

QUESTION 9
Which statement is true about ADOMs?

A. When a FortiAnalyzer Fabric is implemented, the default ADOM mode is set to advanced.
B. A fabric ADOM can include all the device types supported by FortiAnalyzer.
C. You can change the ADOM mode only through the GUI.
D. In normal mode, you cannot change the disk quota of the ADOM after its creation.

Correct Answer: B

Section:
Explanation:
Regarding ADOMs (Administrative Domains) in FortiAnalyzer, a fabric ADOM is capable of including all device types that FortiAnalyzer supports. This is part of the flexibility offered by ADOMs to manage and report on logs from various devices within a Fortinet security fabric. ADOMs can be enabled to support non-FortiGate devices as well, and the root ADOM in Fabric ADOMs provides visibility into all Security Fabric devices. Additionally, it should be noted that in normal mode, you cannot assign different FortiGate VDOMs to different ADOMs, while in advanced mode, you can, which provides a more granular control over the log data from individual VDOMs.
Reference: FortiAnalyzer 7.4.1 Administration Guide, 'ADOMs' and 'ADOM device modes' sections.

QUESTION 10
Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

A. When in collector mode. FortiAnalyzer offloads the log receiving task to the analyzer.
B. Analyzer mode is the default operating mode.
C. For the collector, you should allocate most of the disk space to analytics logs.
D. When in analyzer mode. FortiAnalyzer supports event management and reporting features.

Correct Answer: B, D
Section:
Explanation:
The default operating mode for FortiAnalyzer is analyzer mode. In this mode, FortiAnalyzer provides full functionality for event management and reporting features. This mode is intended for environments where comprehensive analysis and reporting are required. It allows FortiAnalyzer to collect, analyze, and store logs, as well as generate reports and manage events.
Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Operating modes' section.

QUESTION 11
Which statement is true when you are upgrading the firmware on an HA cluster made up of throe FortiAnalyzer devices?

A. All FortiAnalyzer devices will be upgraded at the same time.
B. Enabling uninterruptible-upgrade prevents normal operations from being interrupted during the upgrade.
C. You can perform the firmware upgrade using only a console connection.
D. First, upgrade the secondary devices, and then upgrade the primary device.

Correct Answer: D
Section:
Explanation:
In an HA cluster, the firmware upgrade process involves upgrading the secondary devices first. This approach ensures that the primary device can continue to handle traffic and maintain the operational stability of the network while the secondary devices are being upgraded. Once the secondary devices have successfully upgraded their firmware and are operational, the primary device can then be upgraded. This method minimizes downtime and maintains network integrity during the upgrade process.
When upgrading firmware in a High Availability (HA) cluster of FortiAnalyzer units, the recommended practice is to first upgrade the secondary devices before upgrading the primary device. This approach ensures that the primary device, which coordinates the cluster's operations, remains functional for as long as possible, minimizing the impact on log collection and analysis. Once the secondary devices are successfully upgraded and operational, the primary device can be upgraded, ensuring a smooth transition and maintaining continuous operation of the cluster.
Reference: FortiAnalyzer 7.2 Administrator Guide - 'System Administration' and 'High Availability' sections.

QUESTION 12
What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

A. Shul down FortiAnalyzer and replace the disk.
B. Perform a hot swap of the disk.
C. Run execute format disk to format and restart the FortiAnalyzer device.
D. There is no need to do anything because the disk will self-recover.

Correct Answer: B
Section:
Explanation:
In systems that support hardware RAID, hot swapping allows for the replacement of a failed disk without shutting down the system. This capability is crucial for maintaining uptime and ensuring data redundancy and availability, especially in critical environments. The RAID controller rebuilds the data on the new disk using redundancy data from the other disks in the array, ensuring no data loss and minimal impact on system performance. In the context of a FortiAnalyzer unit equipped with hardware RAID support, the optimal approach to addressing a hard disk failure is to perform a hot swap of the disk. Hardware RAID configurations are designed to provide redundancy and fault tolerance, allowing for the replacement of a failed disk without the need to shut down the system. Hot swapping enables the administrator to replace the faulty disk with a new one while the system is still running, and the RAID controller will rebuild the data on the new disk, restoring the RAID array to its fully operational state.
Reference: FortiAnalyzer 7.2 Administrator Guide - 'Hardware Maintenance' and 'RAID Management' sections.

QUESTION 13
After you have moved a registered logging device out of one ADOM and into a new ADOM, you run the following command: execute sql-local rebuild-adom <new-ADOM-name>
What is the purpose of running this CLI command?

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

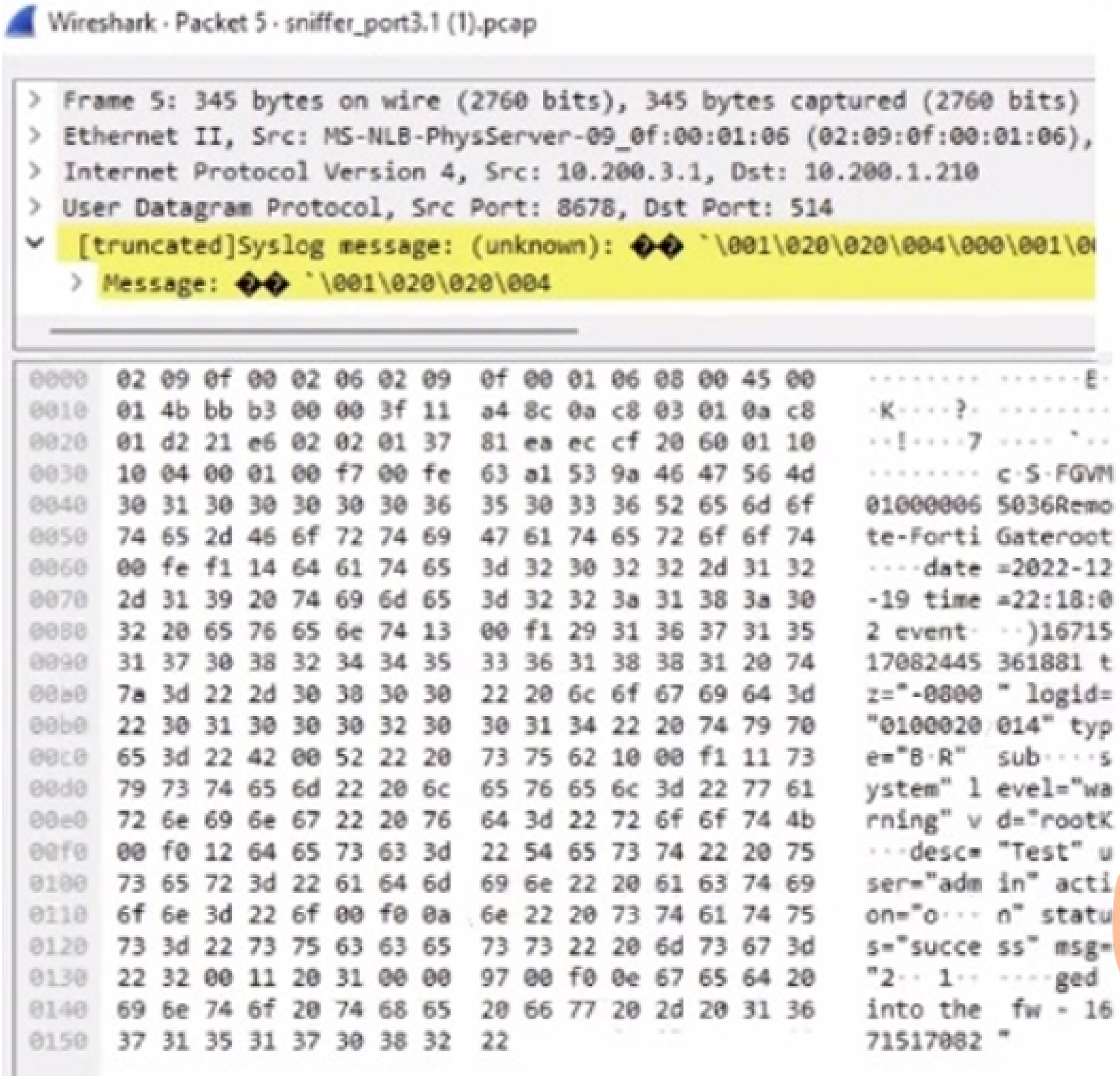
Correct Answer: C
Section:
Explanation:
When you move a registered logging device from one ADOM (Administrative Domain) to another in FortiAnalyzer, it's essential to ensure that the analytical logs for the moved device are available in the new ADOM to maintain continuity in reporting and log analysis. The command execute sql-local rebuild-adom <new-ADOM-name> is used specifically for this purpose. Running this command populates the new ADOM with the analytical logs of the moved device, enabling you to generate accurate and comprehensive reports based on the historical data of the device in its new ADOM context. This process ensures that the transition of devices between ADOMs does not lead to a loss of analytical insight or reporting capabilities for the device's traffic and events.

QUESTION 14
You finished registering a FortiGate device. After traffic starts to flow through FortiGate. you notice that only some of the logs expected are being received on FortiAnalyzer.
What could be the reason for the logs not arriving on FortiAnalyzer?

A. FortiGate does not have logging configured correctly.
B. This FortiGate model is not fully supported.
C. This FortiGate is part of an HA cluster but it is the secondary device.
D. FortiGate was added to the wrong ADOM type.

Correct Answer: A
Section:
Explanation:
When only some of the expected logs from a FortiGate device are being received on FortiAnalyzer, it often indicates a configuration issue on the FortiGate side. Proper logging configuration on FortiGate involves specifying what types of logs to generate (e.g., traffic, event, security logs) and ensuring that these logs are directed to the FortiAnalyzer unit for storage and analysis. If the logging settings on FortiGate are not correctly configured, it could result in incomplete log data being sent to FortiAnalyzer. This might include missing logs for certain types of traffic or events that are not enabled for logging on the FortiGate device. Ensuring comprehensive logging is enabled and correctly directed to FortiAnalyzer is crucial for full visibility into network activities and for the effective analysis and reporting of security incidents and network performance.

QUESTION 15
Refer to the exhibit.



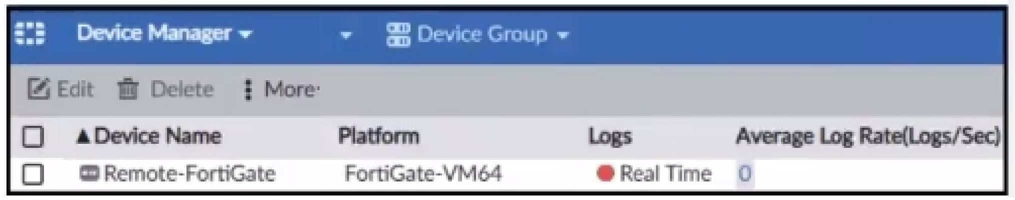
Wireshark · Packet 5 · sniffer_port3.1 (1).pcap

```
> Frame 5: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits)
> Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:01:06 (02:09:0f:00:01:06),
> Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
> User Datagram Protocol, Src Port: 8678, Dst Port: 514
v [truncated]Syslog message: (unknown): �� `\001\020\020\004\000\001\0
   > Message: �� `\001\020\020\004

0000  02 09 0f 00 02 06 02 09  0f 00 01 06 08 00 45 00   ········ ······E·
0010  01 4b bb b3 00 00 3f 11  a4 8c 0a c8 03 01 0a c8   ·K····?· ········
0020  01 d2 21 e6 02 02 01 37  81 ea ec cf 20 60 01 10   ··!····7 ···· `··
0030  10 04 00 01 00 f7 00 fe  63 a1 53 9a 46 47 56 4d   ········ c·S·FGVM
0040  30 31 30 30 30 30 30 36  35 30 33 36 52 65 6d 6f   01000006 5036Remo
0050  74 65 2d 46 6f 72 74 69  47 61 74 65 72 6f 6f 74   te-Forti Gateroot
0060  00 fe f1 14 64 61 74 65  3d 32 30 32 32 2d 31 32   ····date =2022-12
0070  2d 31 39 20 74 69 6d 65  3d 32 32 3a 31 38 3a 30   -19 time =22:18:0
0080  32 20 65 76 65 6e 74 13  00 f1 29 31 36 37 31 35   2 event· ··)16715
0090  31 37 30 38 32 34 34 35  33 36 31 38 38 31 20 74   17082445 361881 t
00a0  7a 3d 22 2d 30 38 30 30  22 20 6c 6f 67 69 64 3d   z="-0800 " logid=
00b0  22 30 31 30 30 30 32 30  30 31 34 22 20 74 79 70   "0100020 014" typ
00c0  65 3d 22 42 00 52 22 20  73 75 62 10 00 f1 11 73   e="B·R"  sub····s
00d0  79 73 74 65 6d 22 20 6c  65 76 65 6c 3d 22 77 61   ystem" l evel="wa
00e0  72 6e 69 6e 67 22 20 76  64 3d 22 72 6f 6f 74 4b   rning" v d="rootK
00f0  00 f0 12 64 65 73 63 3d  22 54 65 73 74 22 20 75   ···desc= "Test" u
0100  73 65 72 3d 22 61 64 6d  69 6e 22 20 61 63 74 69   ser="adm in" acti
0110  6f 6e 3d 22 6f 00 f0 0a  6e 22 20 73 74 61 74 75   on="o··· n" statu
0120  73 3d 22 73 75 63 63 65  73 73 22 20 6d 73 67 3d   s="succe ss" msg=
0130  22 32 00 11 20 31 00 00  97 00 f0 0e 67 65 64 20   "2·· 1·· ····ged 
0140  69 6e 74 6f 20 74 68 65  20 66 77 20 2d 20 31 36   into the  fw - 16
0150  37 31 35 31 37 30 38 32  22                        71517082 "
```

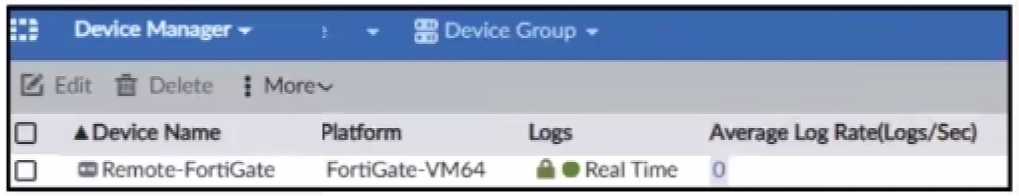
Which image corresponds to the packet capture shown in the exhibit?

A)



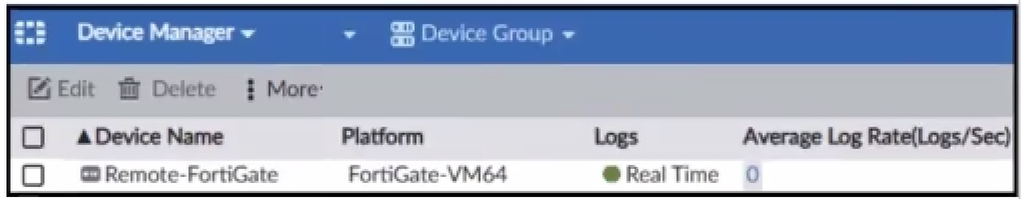
□	▲Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-FortiGate	FortiGate-VM64	🔴 Real Time	0

B)



□	▲Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-FortiGate	FortiGate-VM64	🔒 🟢 Real Time	0

C)



□	▲Device Name	Platform	Logs	Average Log Rate(Logs/Sec)
□	Remote-FortiGate	FortiGate-VM64	🟢 Real Time	0

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

Correct Answer: A
Section:
Explanation:
The exhibit shows a packet capture with a syslog message containing a log event from a FortiGate device. This log event includes several details such as the date, time, and event message. The corresponding image that matches this packet capture would be the one which shows that the FortiGate device has logs being received in real-time, as indicated by the highlighted section in the packet capture where it mentions 'real-time'. Therefore, Option A is the correct answer because it shows logs with 'Real Time' status for the FortiGate-VM64 device, indicating that this FortiAnalyzer is currently receiving real-time logs from the device, matching the activity in the packet capture.
Reference: Based on the provided exhibits and the real-time logging information, correlated with the knowledge from the FortiAnalyzer 7.2 Administrator documentation regarding log reception and device management.

QUESTION 16
Which items must you configure on FortiAnalyzer to send its reports to an external server?

A. Report schedule
B. Mail server
C. Fabric connector
D. Output profile

Correct Answer: D
Section:
Explanation:
To send reports from FortiAnalyzer to an external server, you must configure the output profile. This involves specifying the method (FTP, SFTP, or SCP), server IP, username, password, and the directory where the report will be saved. Additionally, you have the option to delete the report after it has been uploaded to the server.
Reference: FortiAnalyzer 7.2 Administrator Guide, 'Enable uploading of generated reports to a server' section.

QUESTION 17
Which statement is true about using aggregation mode on FortiAnalyzer?

A. Aggregation mode supports log filters.
B. Aggregation mode can work with syslog servers.
C. In aggregation mode, logs and content files are forwarded in real time.
D. Aggregation mode can be configured only on the CLI.

Correct Answer: B
Section:
Explanation:
In aggregation mode, FortiAnalyzer stores logs received from devices and forwards them at a specified time each day to avoid duplication. It is specifically designed to work between two FortiAnalyzer units and does not support syslog or CEF servers. Additionally, aggregation mode configurations are limited to CLI commands log-forward and log-forward-service.
Reference: FortiAnalyzer 7.2 Administrator Guide, 'Aggregation' and 'CLI Commands for Aggregation Mode' sections.

QUESTION 18
Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

A. Disk size
B. Total quota

C. RAID level

D. License type

Correct Answer: A, C
Section:
Explanation:
The amount of reserved disk space required by FortiAnalyzer is influenced by the disk size and the RAID level. The system reserves a portion of the disk space for system use and unexpected quota overflow, with the rest available for device allocation. The RAID level determines the disk size and the reserved disk quota level, with different RAID configurations leading to variations in the reserved space.
Reference: FortiAnalyzer 7.2 Administrator Guide, 'Disk Space Allocation' and 'RAID Level Impact' sections.

QUESTION 19
Which FortiAnalyzer command erases all device settings, images, databases, and logs on disk, but preserves The network configuration?

A. execute factory-reset

B. execute format disk

C. execute formatlogdisk

D. execute reset all-except---ip

Correct Answer: A
Section:
Explanation:
The FortiAnalyzer command execute factory-reset is used to erase all device settings, images, databases, and logs on disk but preserves the current IP address and route information. This command effectively resets the FortiAnalyzer to its factory settings while maintaining its network configuration, allowing it to be quickly reconfigured with the same network settings.
Reference: FortiAnalyzer 7.4.1 Administration Guide, 'Reset Commands' section.