Fortinet

Exam Questions FCP_FAZ_AN-7.6

Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst

NEW QUESTION 1
Which statement about sending notifications with incident update is true?

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

Answer: A

Explanation:
In FortiOS and FortiAnalyzer,incident notificationscan be sent to multiple external platforms, not limited to a single method such as email. Fortinet's security fabric and integration capabilities allow notifications to be
sent through various fabric connectors and third-party integrations. This flexibility is designed to ensure that incident updates reach relevant personnel or systems using preferred communication channels, such as email, Syslog, SNMP, or integration with SIEM platforms.
Let??s review each answer option for clarity:
* Option A: You can send notifications to multiple external platforms
* This is correct. Fortinet??s notification system is capable of sending updates to multiple platforms, thanks to its support for fabric connectors and external integrations. This includes options such as email, Syslog, SNMP, and others based on configured connectors.
* Option B: Notifications can be sent only by email
* This is incorrect. Although email is a common method, FortiOS and FortiAnalyzer support multiple notification methods through various connectors, allowing notifications to be directed to different platforms as per the organization??s setup.
* Option C: If you use multiple fabric connectors, all connectors must have the same settings
* This is incorrect. Each fabric connector can have its unique configuration, allowing different connectors to be tailored for specific notification and integration requirements.
* Option D: Notifications can be sent only when an incident is updated or deleted
* This is incorrect. Notifications can be sent upon the creation of incidents, as well as upon updates or deletion, depending on the configuration.
:According to FortiOS and FortiAnalyzer 7.4.1 documentation, notifications for incidents can be configured across various platforms by using multiple connectors, and they are not limited to email alone. This capability is part of the Fortinet Security Fabric, allowing for a broad range of integrations with external systems and platforms for effective incident response.

NEW QUESTION 2
You mustfind a specific security event log in the FortiAnalyzer logs displayed in FortiView, but, so far, you have been uncuccessful.
Which two tasks should you perform to investigate why you are having this issue? (Choose two.)

A. Open .gz log files in FortiView.
B. Rebuild the SQL database and check FortiView.
C. Review the ADOM data policy
D. Check logs in the Log Browse

Answer: AB

NEW QUESTION 3
You find that as part of your role as an analyst, you frequently search log View using the same parameters. Instead of defining your search filters repeatedly, what can you do to save time?

A. Configure a custom dashboard.
B. Configure a custom view.
C. Configure a data selector.
D. Configure a marco and apply it to device groups.

Answer: B

Explanation:
When you frequently use the same search parameters in FortiAnalyzer??s Log View, setting up a reusable filter or view can saveconsiderable time. Here??s an analysis of each option:
* Option A - Configure a Custom Dashboard:
* Custom dashboards are useful for displaying a variety of widgets and summaries on network activity, performance, and threat data, but they are not designed for storing specific search filters for log views.
* Conclusion:Incorrect.
* Option B - Configure a Custom View:
* Custom views in FortiAnalyzer allow analysts to save specific search filters and configurations.
By setting up a custom view, you can retain your frequently used search parameters and quickly access them without needing to reapply filters each time. This option is specifically designed to streamline the process of recurring log searches.
* Conclusion:Correct.
* Option C - Configure a Data Selector:
* Data selectors are used to define specific types of data for FortiAnalyzer reports and widgets.
They are useful in reports but are not meant for saving and reusing log search parameters in Log View.
* Conclusion:Incorrect.
* Option D - Configure a Macro and Apply It to Device Groups:
* Macros in FortiAnalyzer are generally used for automation tasks, not for saving log search filters.
Applying macros to device groups does not fulfill the requirement of saving specific log view search parameters.
* Conclusion:Incorrect.
Conclusion:
* Correct Answer B. Configure a custom view.
Custom views allow you to save specific search filters, enabling quick access to frequently used parameters in Log View.
References:
FortiAnalyzer 7.4.1 documentation on creating and using custom views for log searches.

NEW QUESTION 4
Which statement about automation connectors in FortiAnalyzer is true?

A. An ADOM with the Fabric type comes with multiple connectors configured.
B. The local connector becomes available after you configured any external connector.
C. The local connector becomes available after you connectors are displayed.
D. The actions available with FortiOS connectors are determined by automation rules configured on FortiGate.

Answer: D

NEW QUESTION 5
Which two statement regarding the outbreak detection service are true? (Choose two.)

A. An additional license is required.
B. It automatically downloads new event handlers and reports.
C. Outbreak alerts are available on the root ADOM only.
D. New alerts are received by email.

Answer: BC

NEW QUESTION 6
Refer to the exhibit with partial output:

Your colleague exported a playbook and has sent it to you for review. You open the file in a text editor and observer the output as shown in the exhibit.
Which statement about the export is true?

A. The export data type is zipped.
B. The playbook is misconfigured.
C. The option to include the connector was not selected.
D. Your colleague put a password on the export.

Answer: A

Explanation:
In the exhibit, the data structure shows a checksum field and a data field with a long, seemingly encoded string. This format is indicative of a file that has been compressed or encoded for storage and transfer.
Export Data Type:
The data field is likely a base64-encoded string, which is commonly used to represent binary data in text format. Base64 encoding is often applied to data that has been compressed (zipped) for easier handling and transfer. The checksum field, with an MD5 hash, provides a way to verify the integrity of the data after decompression.
Option Analysis:
* A. The export data type is zipped: Correct. The compressed and encoded format of the data suggests that the export is in a zipped format, allowing for efficient storage and transfer.
* B. The playbook is misconfigured: There is no indication of misconfiguration in this exhibit. The presence of the checksum and data fields aligns with standard export practices.
* C. The option to include the connector was not selected: There is no evidence in the output to conclude that connectors are missing. Connectors are typically listed separately and would not directly affect the checksum and encoded data structure.
* D. Your colleague put a password on the export: There??s no indication of password protection in the exhibit. Password protection would likely alter the data structure, and there would be some mention of encryption.
Conclusion:
Correct Answer:A. The export data type is zipped.
This answer is consistent with the typical use of base64 encoding for compressed (zipped) data exports in FortiAnalyzer.
[References:, FortiAnalyzer 7.4.1 documentation on exporting playbooks and data compression methods.,]

NEW QUESTION 7
How does FortiAnalyzer block indicators? (Choose one answer))

A. It uses an automation script to update FortiGate with the block list.
B. It uses a FortiManager connector to send the block list.

C. It uses a FortiClient EMS connector to send the block list.
D. It uses a webhook to allow FortiGate to send the block list.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract of knowledge of FortiAnalyzer 7.6 Study guide documents:
The FortiAnalyzer study guide states that blocking suspicious indicators is performed by integrating FortiAnalyzer withFortiManager(not by directly pushing a block list to FortiGate). Specifically:"To use this feature, you must set up an authorized FortiManager connector for the FortiAnalyzer on the Fabric Connector page of FortiAnalyzer."
It then explains the backend mechanism:"In the back end, a playbook called Block_indicator runs every 5 minutes to send the information to FortiManager."After a successful run,"the blocked indicator is pushed to the FortiManager External Resource list."From there, FortiManager can create threat feeds/security profiles/policy blocks and push policies to FortiGate as needed—however, the study guide clarifies:??The Blocked status on FortiAnalyzer confirms that the list is updated on FortiManager, but it is not synced to FortiGate.??
Therefore, FortiAnalyzer blocks indicators by using aFortiManager connectorand sending the block information to FortiManager (Option B).

NEW QUESTION 8
Exhibit.

```
FAZ # diagnose fortilogd lograte
last 5 seconds: 70.0, last 30 seconds: 132.1, last 60 seconds: 133.3

FAZ # diagnose fortilogd msgrate
last 5 seconds: 1.4, last 30 seconds: 1.6, last 60 seconds: 1.6
```

What can you conclude about the output?

A. The message rate being lower that the log rate is normal.
B. Both messages and logs are almost finished indexing.
C. There are more traffic logs than event logs.
D. The output is ADOM specific

Answer: A

Explanation:
In this output, we see two diagnostic commands executed on a FortiAnalyzer device:
diagnose fortilogd lograte: This command shows the rate at which logs are being processed by the FortiAnalyzer in terms of log entries per second.
diagnose fortilogd msgrate: This command displays the message rate, or the rate at which individual messages are being processed.
The values provided in the exhibit output show:
Log rate (lograte): Consistently high, showing values such as 70.0, 132.1, and 133.3 logs per second over different time intervals.
Message rate (msgrate): Lower values, around 1.4 to 1.6 messages per second. Explanation
Interpretation of log rate vs. message rate: In FortiAnalyzer, the log rate typically refers to the rate of logs being stored or indexed, while the message rate refers to individual messages within these logs. Given that a single log entry can contain multiple messages, it's common to see a lower message rate relative to the log rate.
Understanding normal operation: In this case, the message rate being lower than the log rate is expected and typical behavior. This discrepancy can arise because each log entry may bundle multiple related messages, reducing the message rate relative to the log rate.
Conclusion
Correct Answer A. The message rate being lower than the log rate is normal.
This aligns with thenormal operational behavior of FortiAnalyzer in processing logs and messages.
There is no indication that both logs and messages are nearly finished indexing, as that would typically show diminishing rates toward zero, which is not the case here. Additionally, there's no information in this output about specific ADOMs or a comparison between traffic logs and event logs. Thus, options B, C, and D are incorrect.
[References:, FortiOS 7.4.1 and FortiAnalyzer 7.4.1 command guides for diagnose fortilogd lograte and diagnose fortilogd msgrate.,]

NEW QUESTION 9
Exhibit.

What can you conclude about these search results? (Choose two.)

A. They can be downloaded to a file.
B. They are sortable by columns and customizable.
C. They are not available for analysis in FortiView.
D. They were searched by using text mode.

Answer: AD

NEW QUESTION 10
You created a playbook on FortiAnalyzer that uses a FortiOS connector. When configuring the FortiGate side, which type of trigger must be used so that the actions in an automation stich are available in the FortiOS connector?

A. FortiAnalyzer Event Handler
B. Fabric Connector event
C. FortiOS Event Log
D. Incoming webhook

Answer: D

Explanation:
When using FortiAnalyzer to create playbooks that interact with FortiOS devices, an Incoming Webhook trigger is required on the FortiGate side to make the actions in an automation stitch accessible through the FortiOS connector. The incoming webhook trigger allows FortiAnalyzer to initiate actions on FortiGate by sending HTTP POST requests to specified endpoints, which in turn trigger automation stitches defined on the FortiGate.
Here's an analysis of each option:
Option A: FortiAnalyzer Event Handler
This is incorrect. The FortiAnalyzer Event Handler is used within FortiAnalyzer itself for handling log events and alerts, but it does not trigger automation stitches on FortiGate.
Option B: Fabric Connector event
This is incorrect. Fabric Connector events are related to Fortinet's Security Fabric integrations but are not specifically used to trigger FortiGate automation stitches from FortiAnalyzer.
Option C: FortiOS Event Log
This is incorrect. While FortiOS event logs can be used for monitoring, they are not designed to trigger automation stitches directly from FortiAnalyzer.
Option D: Incoming webhook
This is correct. The Incoming Webhook trigger on FortiGate enables it to receive requests from FortiAnalyzer, allowing playbooks to activate automation stitches defined on the FortiGate device. This method is commonly used to integrate actions from FortiAnalyzer to FortiGate via the FortiOS connector.
Reference: According to FortiOS and FortiAnalyzer documentation, when integrating FortiAnalyzer
playbooks with FortiGate automation stitches, the recommended trigger type on FortiGate is an Incoming Webhook, allowing FortiAnalyzer to interact with FortiGate??s automation framework through the FortiOS connector.

NEW QUESTION 10
When managing incidents on FortiAnlyzer, what must an analyst be aware of?

A. You can manually attach generated reports to incidents.
B. The status of the incident is always linked to the status of the attach event.
C. Severity incidents rated with the level High have an initial service-level agreement (SLA) response time of 1 hour.
D. Incidents must be acknowledged before they can be analyzed.

Answer: A

Explanation:
In FortiAnalyzer's incident management system, analysts have the option to manually manage incidents, which includes attaching relevant reports to an incident for further investigation and documentation. This feature allows analysts to consolidate information, such as detailed reports on suspicious activity, into an incident record, providing a comprehensive view for incident response.
Let's review the other options to clarify why they are incorrect:
Option A: You can manually attach generated reports to incidents
This is correct. FortiAnalyzer allows analysts to manually attach reports to incidents, which is beneficial for providing additional context, evidence, or analysis related to the incident. This functionality is part of the incident management process and helps streamline information for tracking and resolution.
Option B: The status of the incident is always linked to the status of the attached event
This is incorrect. The status of an incident on FortiAnalyzer is managed independently of the status of any attached events. An incident can contain multiple events, each with different statuses, but the incident itself is tracked separately.
Option C: Severity incidents rated with the level High have an initial service-level agreement (SLA) response time of 1 hour
This is incorrect. While incidents have severity levels, specific SLA response times are typically set according to the organization??s incident response policy, and FortiAnalyzer does not impose a default
SLA response time of 1 hour for high-severity incidents.
Option D: Incidents must be acknowledged before they can be analyzed
This is incorrect. Incidents on FortiAnalyzer can be analyzed even if they are not yet acknowledged. Acknowledging an incident is often part of the workflow to mark it as being actively addressed, but it is not a prerequisite for analysis.
Reference: According to FortiAnalyzer documentation, analysts can attach reports to incidents manually, making option A correct. This feature enables better tracking and documentation within the incident management system on FortiAnalyzer.

NEW QUESTION 13
Refer to the exhibit.

```
FAZ # diagnose fortilogd lograte
last 5 seconds: 78.8, last 30 seconds: 132.1, last 60 seconds: 133.3

FAZ # diagnose fortilogd msgrate
last 5 seconds: 1.4, last 30 seconds: 1.6, last 60 seconds: 1.6
```

What can you conclude about the output?

A. The low indexing values require investigation.
B. The output is not ADOM specific.
C. There are more event logs thantraffic logs.
D. The log rate higher than the message rate is not normal.

Answer: D

NEW QUESTION 16
You are trying to configure a task in the playbook editor to run a report.
However, when you try to select the desired playbook, you do to see it listed.
What is the reason?

A. The report does not have auto-cache and extended log filtering enabled.
B. The playbook is currently running and will be available after it is finished.
C. You must create a trigger to run the report first.
D. The report has no result and must be reconfigured.

Answer: C

NEW QUESTION 19
Which two parameters does FortiAnalyzer use to identify an indicator of compromise (IOC)? (Choose two answers)

A. IP address
B. URL
C. Policy ID
D. Application category

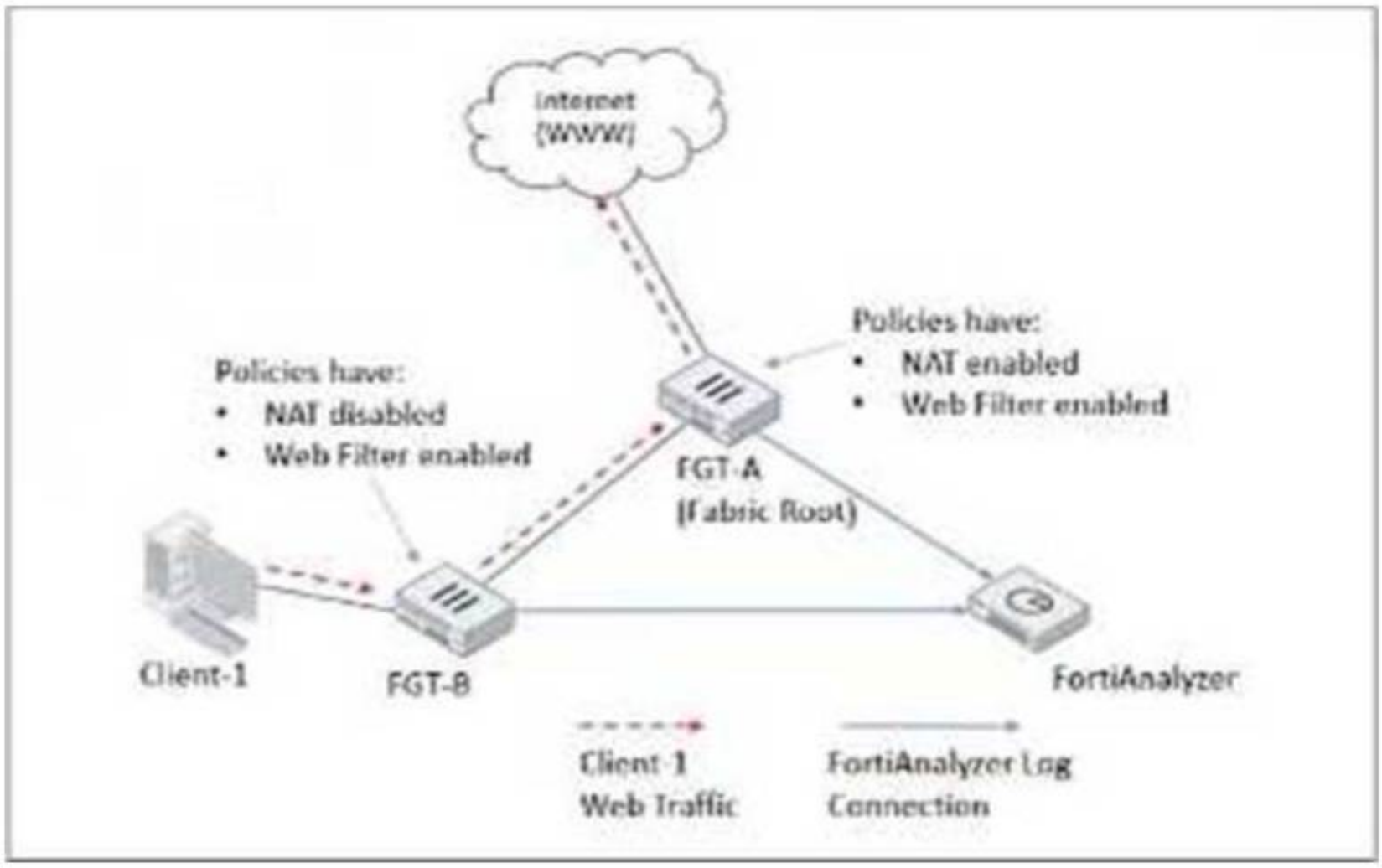
Answer: AB

NEW QUESTION 22
Which statement correctly describes one Difference between templates and reports?

A. Reports provide mora configuration options than templates
B. Templates can becloned, but reports cannot be cloned.
C. Reports support macros, but templates do not.
D. Template are mapped to device group
E. while reports are mapped to ADOMs

Answer: D

NEW QUESTION 25
Refer to Exhibit:



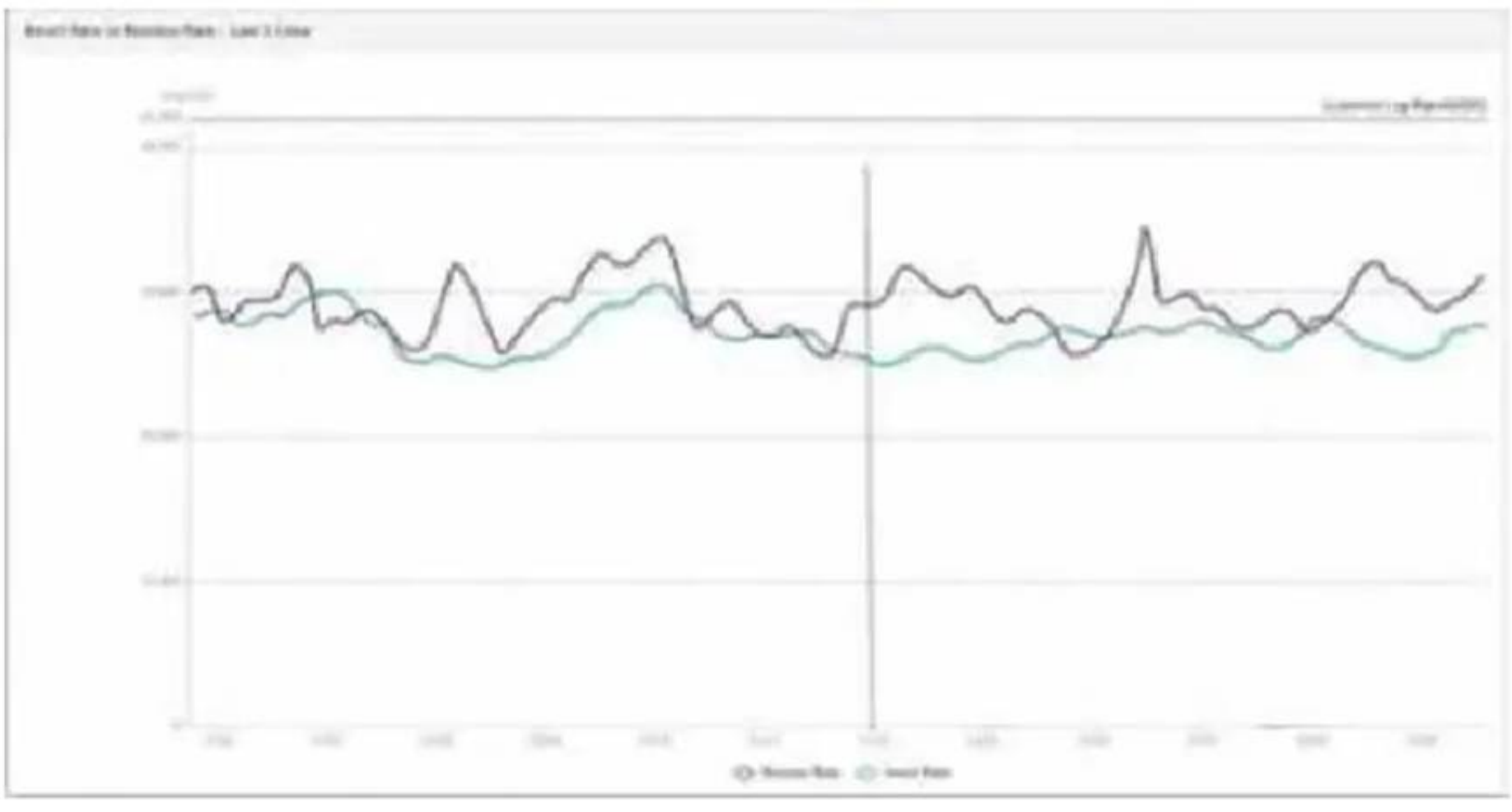
Client-1 is trying to access the internet for web browsing.
All FortiGate devices in the topology are part of a Security Fabric with logging to FortiAnalyzer configured. All firewall policies have logging enabled. All web filter profiles are configured to log only violations.
Which statement about the logging behavior for this specific traffic flow is true?

A. Only FGT-B will create traffic logs.
B. FGT-B will see the MAC address of FGT-A as the destination and notifies FGT-A to log this flow.
C. FGT B will create traffic logs and will create web filter logs if it detects a violation.
D. Only FGT-A will create web filter logs if it detects a violation.

Answer: D

Explanation:
The study guide explains that in a Security Fabric,traffic logging is not duplicatedacross FortiGates for the same session:??Traffic logging for a session ?? is always carried out by the first FortiGate that handled it??and if a FortiGate receives traffic from a peer FortiGate MAC,"it does not generate a new traffic log for that session."
For UTM (web filtering) logs, the study guide states:"When configured, upstream devices complete UTM logging."
In the illustrated example, it further clarifies the role split:"All traffic from Client-1 is first received by FGT-B, which creates traffic logs for the initial session?? [then] forwarded to FGT-A?? [and]FGT-A ?? applies web filtering ?? and generates the relevant UTM logs as necessary."
Because web filter profiles are configured tolog only violations, web filter (UTM) logs will be generated only when a violation is detected—and per the study guide behavior, that UTM logging is done by theupstreamFortiGate (FGT-A). Therefore,only FGT-A will create web filter logs if it detects a violation(Option D)

NEW QUESTION 28
Exhibit.



What does the data point at 12:20 indicate?

A. The loginsert log time is increasing.
B. FortiAnalyzer is using its cache to avoid dropping logs.
C. The performance of FortiAnalyzer is below the baseline.
D. The sqiplugind service is caught up with the logs

Answer: A

NEW QUESTION 29
Which two external servers can you configure to validate administrator logins? (Choose two.)

A. Syslog
B. LDAP
C. RADIUS
D. Only locally by FortiAnalyzer

Answer: ABC

NEW QUESTION 32
A FortiAnalyzer device could use which security method to secure the transfer of log data from FortiGate devices?

A. SSL
B. IPSec
C. Direct serial connection
D. S/MIME

Answer: B

NEW QUESTION 34
.....

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_AN-7.6 Practice Exam Features:

* FCP_FAZ_AN-7.6 Questions and Answers Updated Frequently

* FCP_FAZ_AN-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FAZ_AN-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FAZ_AN-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year