# Fortinet

## FCP_FAZ_AN-7.4 Exam

### FCP - FortiAnalyzer 7.4 Analyst

**Questions & Answers**
**Demo**

# Version: 5.0

## Question: 1

Which log will generate an event with the status Unhandled?

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

**Answer: B**

Explanation:

In FortiOS 7.4.1 and FortiAnalyzer 7.4.1, the "Unhandled" status in logs typically signifies that the FortiGate encountered a security event but did not take any specific action to block or alter it. This usually occurs in the context of Intrusion Prevention System (IPS) logs.
IPS logs with action=pass: When the IPS engine inspects traffic and determines that it does not match any known attack signatures or violate any configured policies, it assigns the action "pass". Since no action is taken to block or modify this traffic, the status is logged as "Unhandled."
Let's look at why the other options are incorrect:
An AV log with action=quarantine: Antivirus (AV) logs with the action "quarantine" indicate that a file was detected as malicious and moved to quarantine. This is a definitive action, so the status wouldn't be "Unhandled."
A WebFilter log will action=dropped: WebFilter logs with the action "dropped" indicate that web traffic was blocked according to the configured web filtering policies. Again, this is a specific action taken, not an "Unhandled" event.
An AppControl log with action=blocked: Application Control logs with the action "blocked" mean that an application was denied access based on the defined application control rules. This is also a clear action, not "Unhandled."

## Question: 2

Exhibit.

| Event | Event Status | Event Type | Severity |
|---|---|---|---|
| bujyqttatbsd.findhere.org (1) | Mitigated | Web Filter | Low |
| Web request to suspicious destination from 10.0.3.20 blocked | Mitigated | Web Filter | Low |

Which statement about the event displayed is correct?

A. The risk source is isolated.

B. The security risk was blocked or dropped.
C. The security event risk is considered open.
D. An incident was created from this event.

**Answer: B**

Explanation:
In FortiOS and FortiAnalyzer logging systems, when an event has a status of "Mitigated" in the Event Status column, it typically indicates that the system took action to address the identified threat. In this case, the Web Filter blocked the web request to a suspicious destination, and the event status "Mitigated" confirms that the action was successfully implemented to neutralize or block the security risk.
Let's review the answer options:
Option A: The risk source is isolated.
This is incorrect because "isolated" would imply that FortiGate took further steps to prevent the source device from communicating with the network. There is no indication of isolation in this event status.
Option B: The security risk was blocked or dropped.
This is correct. The "Mitigated" status, along with the Web Filter event type and the accompanying description, implies that the FortiGate or FortiAnalyzer successfully blocked or dropped the suspicious web request, which corresponds to the term "mitigated."
Option C: The security event risk is considered open.
This is incorrect because an open status would indicate that no action was taken, or the threat is still present. The "Mitigated" status indicates that the threat has been addressed.
Option D: An incident was created from this event.
This option is not correct or evident based on the given display. Although FortiAnalyzer or FortiGate could escalate certain events to incidents, this is not indicated here.
Reference:
The FortiOS 7.4.1 and FortiAnalyzer 7.4.1 documentation specify that "Mitigated" status in logs means the identified threat was handled, usually by blocking or dropping the action associated with the event, particularly with Web Filter and Security Policy logs.

## Question: 3

Which statement describes archive logs on FortiAnalyzer?

A. Logs that are indexed and stored in the SQL database
B. Logs a FortiAnalyzer administrator can access in FortiView
C. Logs compressed and saved in files with the .gz extension
D. Logs previously collected from devices that are offline

**Answer: C**

Explanation:
In FortiAnalyzer, archive logs refer to logs that have been compressed and stored to save space. This process involves compressing the raw log files into the .gz format, which is a common compression format used in Fortinet systems for archived data. Archiving is essential in FortiAnalyzer to optimize storage and manage long-term retention of logs without impacting performance.

Let's examine each option for clarity:
Option A: Logs that are indexed and stored in the SQL database
This is incorrect. While some logs are indexed and stored in an SQL database for quick access and searchability, these are not classified as archive logs. Archived logs are typically moved out of the database and compressed.
Option B: Logs a FortiAnalyzer administrator can access in FortiView
This is incorrect because FortiView primarily accesses logs that are active and indexed, not archived logs. Archived logs are stored for long-term retention but are not readily available for immediate analysis in FortiView.
Option C: Logs compressed and saved in files with the .gz extension
This is correct. Archive logs on FortiAnalyzer are stored in compressed .gz files to reduce space usage. This archived format is used for logs that are no longer immediately needed in the SQL database but are retained for historical or compliance purposes.
Option D: Logs previously collected from devices that are offline
This is incorrect. Although archived logs may include data from devices that are no longer online, this is not a defining characteristic of archive logs.
Reference: FortiAnalyzer 7.4.1 documentation and configuration guides outline that archived logs are stored in compressed files with the .gz extension to conserve storage space, ensuring FortiAnalyzer can handle a larger volume of logs over extended periods.

## Question: 4

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 notifications can 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.
Reference: 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.

## Question: 5

Which statement about the FortiSOAR management extension is correct?

A. It requires a FortiManager configured to manage FortiGate.
B. It runs as a docker container on FortiAnalyzer.
C. It requires a dedicated FortiSOAR device or VM.
D. It does not include a limited trial by default.

## Answer: C

Explanation:
The FortiSOAR management extension is designed as an independent security orchestration, automation, and response (SOAR) solution that integrates with other Fortinet products but requires its own dedicated device or virtual machine (VM) environment. FortiSOAR is not natively integrated as a container or service within FortiAnalyzer or FortiManager, and it operates separately to manage complex security workflows and incident responses across various platforms.
Let's examine each option to determine the correct answer:
Option A: It requires a FortiManager configured to manage FortiGate
This is incorrect. FortiSOAR operates independently of FortiManager. While FortiSOAR can receive input or data from FortiGate (often managed by FortiManager), it does not require FortiManager to be part of its setup.
Option B: It runs as a docker container on FortiAnalyzer
This is incorrect. FortiSOAR does not run as a container within FortiAnalyzer. It requires its own dedicated environment, either as a physical device or a virtual machine, due to the resource requirements and specialized functions it performs.
Option C: It requires a dedicated FortiSOAR device or VM
This is correct. FortiSOAR is deployed as a standalone device or VM, which enables it to handle the intensive processing needed for orchestrating security operations, integrating with third-party tools, and automating responses across an organization's security infrastructure.
Option D: It does not include a limited trial by default
This is incorrect. FortiSOAR installations may come with trial options or demos in specific scenarios, especially for evaluation purposes. This depends on licensing and deployment policies.
Reference: The FortiSOAR platform, as outlined in Fortinet product documentation, is a standalone SOAR solution that requires a dedicated device or VM for deployment. It integrates with Fortinet's Security Fabric but operates separately from FortiAnalyzer, FortiManager, and FortiGate, focusing on advanced incident management and security automation.