# Fortinet

## Exam Questions FCSS_SOC_AN-7.4

FCSS - Security Operations 7.4 Analyst

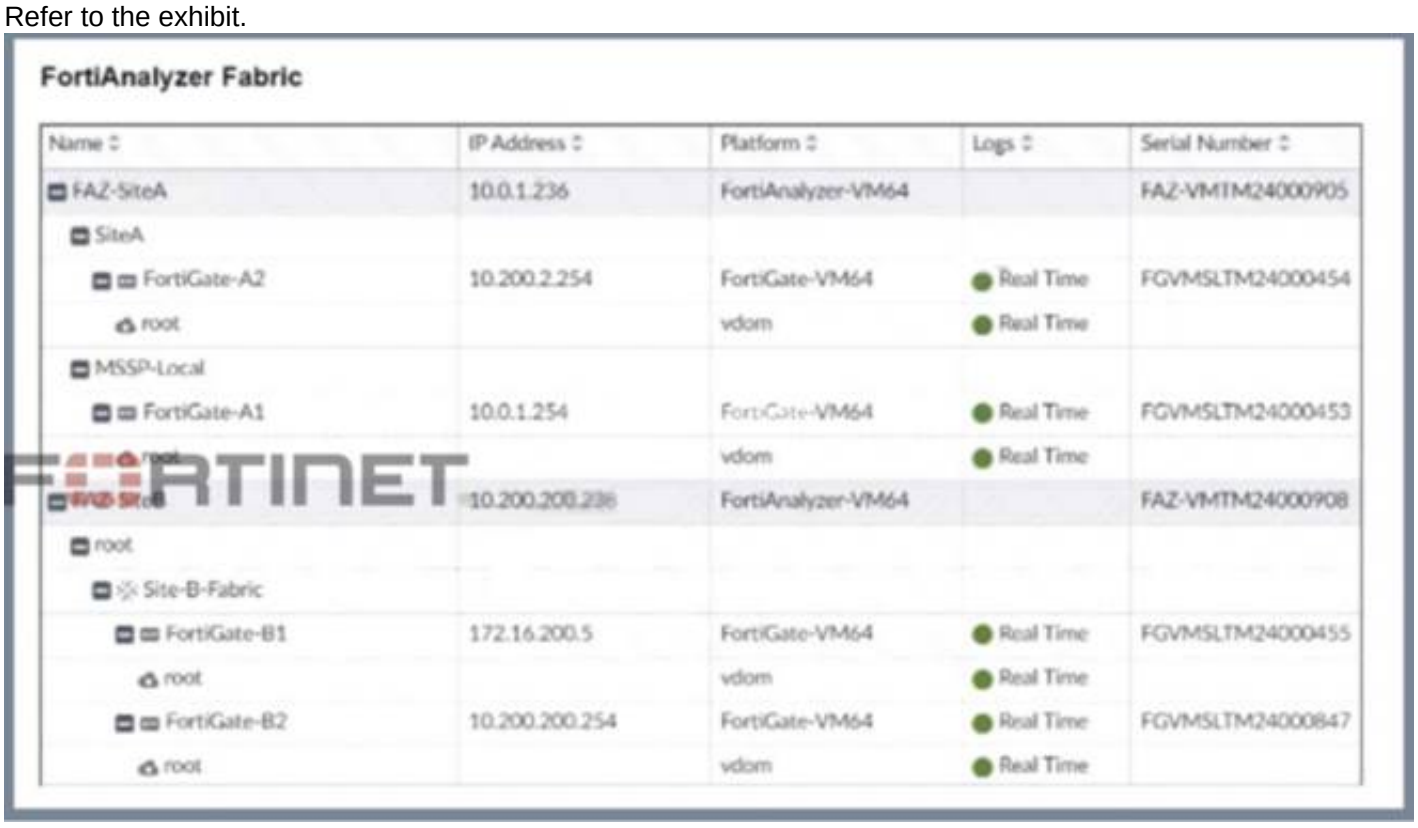
**NEW QUESTION 1**
According to the National Institute of Standards and Technology (NIST) cybersecurity framework, incident handling activities can be divided into phases.
In which incident handling phase do you quarantine a compromised host in order to prevent an adversary from using it as a stepping stone to the next phase of an attack?

A. Containment
B. Analysis
C. Eradication
D. Recovery

**Answer:** A

**Explanation:**
NIST Cybersecurity Framework Overview:
The NIST Cybersecurity Framework provides a structured approach for managing and mitigating cybersecurity risks. Incident handling is divided into several phases to systematically address and resolve incidents.
Incident Handling Phases:
Preparation: Establishing and maintaining an incident response capability.
Detection and Analysis: Identifying and investigating suspicious activities to confirm an incident.
Containment, Eradication, and Recovery:
Containment: Limiting the impact of the incident.
Eradication: Removing the root cause of the incident.
Recovery: Restoring systems to normal operation.
Containment Phase:
The primary goal of the containment phase is to prevent the incident from spreading and causing further damage.
Quarantining a Compromised Host:
Quarantining involves isolating the compromised host from the rest of the network to prevent adversaries from moving laterally and causing more harm.
Techniques include network segmentation, disabling network interfaces, and applying access controls.

**NEW QUESTION 2**
Refer to the exhibit.


FortiAnalyzer Fabric

| Name | IP Address | Platform | Logs | Serial Number |
|---|---|---|---|---|
| FAZ-SiteA | 10.0.1.236 | FortiAnalyzer-VM64 | | FAZ-VMTM24000905 |
| SiteA | | | | |
| FortiGate-A2 | 10.200.2.254 | FortiGate-VM64 | Real Time | FGVMSLTM24000454 |
| root | | vdom | Real Time | |
| MSSP-Local | | | | |
| FortiGate-A1 | 10.0.1.254 | FortiGate-VM64 | Real Time | FGVMSLTM24000453 |
| root | | vdom | Real Time | |
| [illegible] | 10.200.200.236 | FortiAnalyzer-VM64 | | FAZ-VMTM24000908 |
| root | | | | |
| Site-B-Fabric | | | | |
| FortiGate-B1 | 172.16.200.5 | FortiGate-VM64 | Real Time | FGVMSLTM24000455 |
| root | | vdom | Real Time | |
| FortiGate-B2 | 10.200.200.254 | FortiGate-VM64 | Real Time | FGVMSLTM24000847 |
| root | | vdom | Real Time | |

Assume that all devices in the FortiAnalyzer Fabric are shown in the image.
Which two statements about the FortiAnalyzer Fabric deployment are true? (Choose two.)

A. FortiGate-B1 and FortiGate-B2 are in a Security Fabric.
B. There is no collector in the topology.
C. All FortiGate devices are directly registered to the supervisor.
D. FAZ-SiteA has two ADOMs enabled.

**Answer:** AD

**Explanation:**
Understanding the FortiAnalyzer Fabric:
The FortiAnalyzer Fabric provides centralized log collection, analysis, and reporting for connected FortiGate devices.
Devices in a FortiAnalyzer Fabric can be organized into different Administrative Domains (ADOMs) to separate logs and management.
Analyzing the Exhibit:
FAZ-SiteAandFAZ-SiteBare FortiAnalyzer devices in the fabric.
FortiGate-B1andFortiGate-B2are shown under theSite-B-Fabric, indicating they are part of the same Security Fabric.
FAZ-SiteAhas multiple entries under it:SiteAandMSSP-Local, suggesting multiple ADOMs are enabled.
Evaluating the Options:
Option A:FortiGate-B1 and FortiGate-B2 are underSite-B-Fabric, indicating they are indeed part of the same Security Fabric.
Option B:The presence of FAZ-SiteA and FAZ-SiteB as FortiAnalyzers does not preclude the existence of collectors. However, there is no explicit mention of a separate collector role in the exhibit.
Option C:Not all FortiGate devices are directly registered to the supervisor. The exhibit shows hierarchical organization under different sites and ADOMs.
Option D:The multiple entries underFAZ-SiteA(SiteA and MSSP-Local) indicate that FAZ-SiteA has two ADOMs enabled.
Conclusion:
FortiGate-B1 and FortiGate-B2 are in a Security Fabric.

FAZ-SiteA has two ADOMs enabled.
References:
Fortinet Documentation on FortiAnalyzer Fabric Topology and ADOM Configuration.
Best Practices for Security Fabric Deployment with FortiAnalyzer.

**NEW QUESTION 3**
Refer to the exhibit,

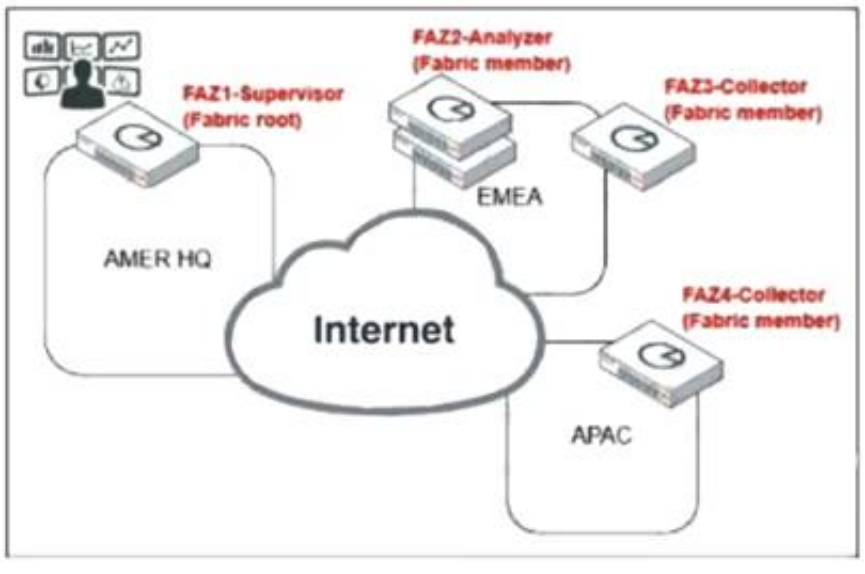

which shows the partial output of the MITRE ATT&CK Enterprise matrix on FortiAnalyzer. Which two statements are true? (Choose two.)

A. There are four techniques that fall under tactic T1071.
B. There are four subtechniques that fall under technique T1071.
C. There are event handlers that cover tactic T1071.
D. There are 15 events associated with the tactic.

**Answer:** BC

**Explanation:**
Understanding the MITRE ATT&CK Matrix:
The MITRE ATT&CK framework is a knowledge base of adversary tactics and techniques based on real-world observations.
Each tactic in the matrix represents the "why" of an attack technique, while each technique represents "how" an adversary achieves a tactic.
Analyzing the Provided Exhibit:
The exhibit shows part of the MITRE ATT&CK Enterprise matrix as displayed on FortiAnalyzer.
The focus is on technique T1071 (Application Layer Protocol), which has subtechniques labeled T1071.001, T1071.002, T1071.003, and T1071.004.
Each subtechnique specifies a different type of application layer protocol used for Command and Control (C2):
T1071.001 Web Protocols
T1071.002 File Transfer Protocols
T1071.003 Mail Protocols
T1071.004 DNS
Identifying Key Points:
Subtechniques under T1071:There are four subtechniques listed under the primary technique T1071, confirming that statement B is true.
Event Handlers for T1071:FortiAnalyzer includes event handlers for monitoring various tactics and techniques. The presence of event handlers for tactic T1071 suggests active monitoring and alerting for these specific subtechniques, confirming that statement C is true.
Misconceptions Clarified:
Statement A (four techniques under tactic T1071) is incorrect because T1071 is a single technique with four subtechniques.
Statement D (15 events associated with the tactic) is misleading. The number 15 refers to the techniques under the Application Layer Protocol, not directly related to the number of events.
Conclusion:
The accurate interpretation of the exhibit confirms that there are four subtechniques under technique T1071 and that there are event handlers covering tactic T1071.
References:
MITRE ATT&CK Framework documentation.
FortiAnalyzer Event Handling and MITRE ATT&CK Integration guides.

**NEW QUESTION 4**
Exhibit:




Which observation about this FortiAnalyzer Fabric deployment architecture is true?

A. The AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor.
B. The AMER HQ SOC team must configure high availability (HA) for the supervisor node.
C. The EMEA SOC team has access to historical logs only.

D. The APAC SOC team has access to FortiView and other reporting functions.

**Answer:** A

**Explanation:**
Understanding FortiAnalyzer Fabric Deployment:
FortiAnalyzer Fabric deployment involves a hierarchical structure where the Fabric root (supervisor) coordinates with multiple Fabric members (collectors and analyzers).
This setup ensures centralized log collection, analysis, and incident response across geographically distributed locations.
Analyzing the Exhibit:
FAZ1-Supervisoris located at AMER HQ and acts as the Fabric root.
FAZ2-Analyzeris a Fabric member located in EMEA.
FAZ3-CollectorandFAZ4-Collectorare Fabric members located in EMEA and APAC, respectively.
Evaluating the Options:
Option A:The statement indicates that the AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor. This is true because automation playbooks and certain orchestration tasks typically require local execution capabilities which may not be fully supported on the supervisor node.
Option B:High availability (HA) configuration for the supervisor node is a best practice for redundancy but is not directly inferred from the given architecture.
Option C:The EMEA SOC team having access to historical logs only is not correct since FAZ2-Analyzer provides full analysis capabilities.
Option D:The APAC SOC team has access to FortiView and other reporting functions through FAZ4-Collector, but this is not explicitly detailed in the provided architecture.
Conclusion:
The most accurate observation about this FortiAnalyzer Fabric deployment architecture is that the AMER HQ SOC team cannot run automation playbooks from the Fabric supervisor.
References:
Fortinet Documentation on FortiAnalyzer Fabric Deployment.
Best Practices for FortiAnalyzer and Automation Playbooks.

**NEW QUESTION 5**
Refer to the exhibits.
**Event Handler**


You configured a custom event handler and an associated rule to generate events whenever FortiMail detects spam emails. However, you notice that the event handler is generating events for both spam emails and clean emails.
Which change must you make in the rule so that it detects only spam emails?

A. In the Log Type field, select Anti-Spam Log (spam)
B. Disable the rule to use the filter in the data selector to create the event.
C. In the Trigger an event when field, select Within a group, the log field Spam Name (snane) has 2 or more unique values.

**Answer:** A

**Explanation:**
Understanding the Custom Event Handler Configuration:
The event handler is set up to generate events based on specific log data.
The goal is to generate events specifically for spam emails detected by FortiMail.
Analyzing the Issue:
The event handler is currently generating events for both spam emails and clean emails.
This indicates that the rule's filtering criteria are not correctly distinguishing between spam and non-spam emails.
Evaluating the Options:
Option A:Selecting the "Anti-Spam Log (spam)" in the Log Type field will ensure that only logs related to spam emails are considered. This is the most straightforward and accurate way to filter for spam emails.
Option B:Typingtype==spamin the Log filter by Text field might help filter the logs, but it is not as direct and reliable as selecting the correct log type.
Option C:Disabling the rule to use the filter in the data selector to create the event does not address the issue of filtering for spam logs specifically.
Option D:Selecting "Within a group, the log field Spam Name (snane) has 2 or more unique values" is not directly relevant to filtering spam logs and could lead to incorrect filtering criteria.
Conclusion:
The correct change to make in the rule is to select "Anti-Spam Log (spam)" in the Log Type field.
This ensures that the event handler only generates events for spam emails.

References:
Fortinet Documentation on Event Handlers and Log Types.
Best Practices for Configuring FortiMail Anti-Spam Settings.

**NEW QUESTION 6**
When configuring a FortiAnalyzer to act as a collector device, which two steps must you perform?(Choose two.)

A. Enable log compression.
B. Configure log forwarding to a FortiAnalyzer in analyzer mode.
C. Configure the data policy to focus on archiving.
D. Configure Fabric authorization on the connecting interface.

**Answer:** BD

**Explanation:**
Understanding FortiAnalyzer Roles:
FortiAnalyzer can operate in two primary modes: collector mode and analyzer mode.
Collector Mode: Gathers logs from various devices and forwards them to another FortiAnalyzer operating in analyzer mode for detailed analysis.
Analyzer Mode: Provides detailed log analysis, reporting, and incident management.
Steps to Configure FortiAnalyzer as a Collector Device:
* A. Enable Log Compression:
While enabling log compression can help save storage space, it is not a mandatory step specifically required for configuring FortiAnalyzer in collector mode.
Not selected as it is optional and not directly related to the collector configuration process.
B. Configure Log Forwarding to a FortiAnalyzer in Analyzer Mode:
Essential for ensuring that logs collected by the collector FortiAnalyzer are sent to the analyzer FortiAnalyzer for detailed processing.
Selected as it is a critical step in configuring a FortiAnalyzer as a collector device.
Step 1: Access the FortiAnalyzer interface and navigate to log forwarding settings.
Step 2: Configure log forwarding by specifying the IP address and necessary credentials of the FortiAnalyzer in analyzer mode.

**NEW QUESTION 7**
Which two ways can you create an incident on FortiAnalyzer? (Choose two.)

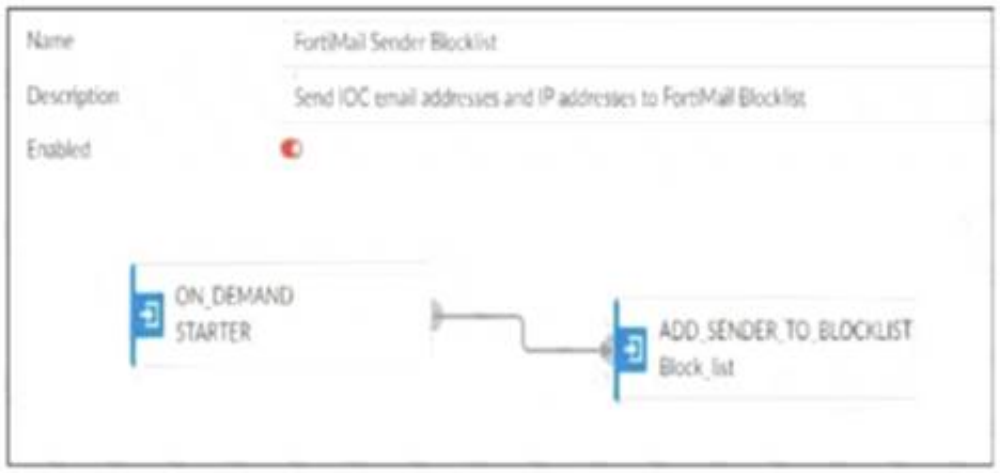
A. Using a connector action
B. Manually, on the Event Monitor page
C. By running a playbook
D. Using a custom event handler

**Answer:** BD

**Explanation:**
Understanding Incident Creation in FortiAnalyzer:
FortiAnalyzer allows for the creation of incidents to track and manage security events.
Incidents can be created both automatically and manually based on detected events and predefined rules.
Analyzing the Methods:
Option A:Using a connector action typically involves integrating with other systems or services and is not a direct method for creating incidents on FortiAnalyzer.
Option B:Incidents can be created manually on the Event Monitor page by selecting relevant events and creating incidents from those events.
Option C:While playbooks can automate responses and actions, the direct creation of incidents is usually managed through event handlers or manual processes.
Option D:Custom event handlers can be configured to trigger incident creation based on specific events or conditions, automating the process within FortiAnalyzer.
Conclusion:
The two valid methods for creating an incident on FortiAnalyzer are manually on the Event Monitor page and using a custom event handler.
References:
Fortinet Documentation on Incident Management in FortiAnalyzer.
FortiAnalyzer Event Handling and Customization Guides.

**NEW QUESTION 8**
Refer to the exhibits.

**Playbook configuration**




**FortiMail connector actions**


The FortiMail Sender Blocklist playbook is configured to take manual input and add those entries to the FortiMail abc. com domain-level block list. The playbook is configured to use a FortiMail connector and the ADD_SENDER_TO_BLOCKLIST action.
Why is the FortiMail Sender Blocklist playbook execution failing7

A. You must use the GET_EMAIL_STATISTICS action first to gather information about email messages.
B. FortiMail is expecting a fully qualified domain name (FQDN).
C. The client-side browser does not trust the FortiAnalzyer self-signed certificate.
D. The connector credentials are incorrect

**Answer:** B

**Explanation:**
Understanding the Playbook Configuration:
The playbook "FortiMail Sender Blocklist" is designed to manually input email addresses or IP addresses and add them to the FortiMail block list.
The playbook uses a FortiMail connector with the actionADD_SENDER_TO_BLOCKLIST.
Analyzing the Playbook Execution:
The configuration and actions provided show that the playbook is straightforward, starting with anON_DEMAND STARTERand proceeding to theADD_SENDER_TO_BLOCKLISTaction.
The action description indicates it is intended to block senders based on email addresses or domains.
Evaluating the Options:
Option A:UsingGET_EMAIL_STATISTICSis not required for the task of adding senders to a block list. This action retrieves email statistics and is unrelated to the block list configuration.
Option B:The primary reason for failure could be the requirement for a fully qualified domain name (FQDN). FortiMail typically expects precise information to ensure the correct entries are added to the block list.
Option C:The trust level of the client-side browser with FortiAnalyzer's self-signed certificate does not impact the execution of the playbook on FortiMail.
Option D:Incorrect connector credentials would result in an authentication error, but the problem described is more likely related to the format of the input data.
Conclusion:
The FortiMail Sender Blocklist playbook execution is failing because FortiMail is expecting a fully qualified domain name (FQDN).
References:
Fortinet Documentation on FortiMail Connector Actions.
Best Practices for Configuring FortiMail Block Lists.

**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

## FCSS_SOC_AN-7.4 Practice Exam Features:

* FCSS_SOC_AN-7.4 Questions and Answers Updated Frequently

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

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

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