KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

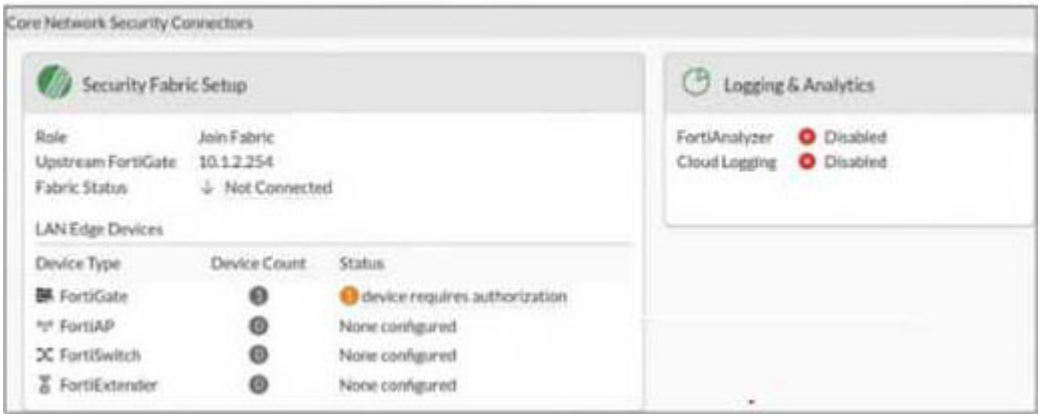
Exam : **NSE6_OTS_AR-7.6**

Title : Fortinet NSE 6 - OT Security 7.6 Architect

Version : DEMO

1.Refer to the exhibit.

Core Network Security Connectors section



The Core Network Security Connectors page of the FortiGate-2 device is shown.

Which statement is correct? (Choose one answer)

A. FortiGate-2 serves as Fabric Root.

B. You must enable Security Fabric Connection on the FortiGate-2 interface.

C. You must configure the FortiAnalyzer settings on FortiGate-2.

D. FortiGate-2 is not authorized on the root FortiGate.

Answer: D

Explanation:

Based on the provided exhibit and the OT Security 7.6 Architect curriculum regarding the Fortinet Security Fabric:

Fabric Role: The exhibit clearly shows that FortiGate-2 has the role set to Join Fabric. This confirms it is a downstream device and not the Fabric Root (eliminating Option A).

Upstream Connection: The device is configured to point to an Upstream FortiGate at IP address 10.1.2.254.

Fabric Status: The status is currently displayed as Not Connected. In a standard Fortinet Security Fabric deployment, once a downstream device is configured to join the fabric, it sends a request to the upstream root device. The root FortiGate must then explicitly authorize the downstream unit before the connection is established and the status changes to "Connected."

Authorization Requirement: The "Not Connected" status, while having the upstream IP correctly configured, is the classic indicator that the authorization step is pending on the root FortiGate.

Furthermore, under the LAN Edge Devices section, it shows another downstream FortiGate requiring authorization on this specific unit, highlighting that authorization is a manual security requirement for all stages of the Fabric hierarchy.

FortiAnalyzer Status: While the Logging & Analytics section shows FortiAnalyzer is Disabled, this is a configuration choice and does not prevent the Security Fabric from connecting; therefore, configuring it is not the solution to the connectivity status shown (eliminating Option C).

In summary, FortiGate-2 cannot join the fabric until an administrator logs into the Root FortiGate (10.1.2.254) and authorizes the join request from FortiGate-2.

2.You want FortiAnalyzer to trigger an automation stitch on a FortiGate device automatically.

What must you configure on FortiAnalyzer to enable direct communication with FortiGate? (Choose one answer)

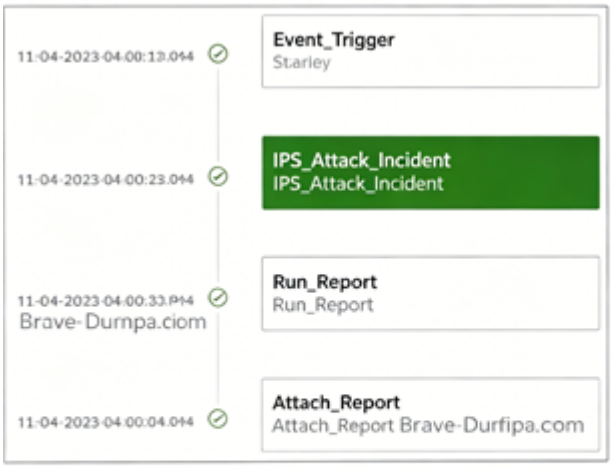
A. A Fabric connector
B. A playbook task
C. The Fabric settings
D. An event handler
Answer: C
Explanation:
The verified answer is
C. The Fabric settings. The study guide ties FortiAnalyzer-triggered actions to the Security Fabric relationship with FortiGate, not to playbook tasks or standalone event handlers alone. It explains that “within the Security Fabric environment, FortiAnalyzer is a key element in the creation of automation stitches” and shows the flow where a downstream FortiGate sends logs to FortiAnalyzer, then FortiAnalyzer parses the logs and notifies the root FortiGate, after which the root FortiGate triggers the action. This shows that FortiAnalyzer must be configured so it can communicate with FortiGate through the Security Fabric.
The guide also states that FortiAnalyzer is the foundation of the Security Fabric, providing logging, reporting, analytics, and automation for Fabric devices and endpoints. It further explains that the FortiAnalyzer Fabric connector consolidates the traffic logs within the Security Fabric. This confirms that the automation workflow depends on proper Security Fabric integration. A playbook task is used for automated SOC actions, and an event handler is used to generate events from logs, but neither one alone establishes the direct communication path needed between FortiAnalyzer and FortiGate. Therefore, the required configuration on FortiAnalyzer is the Fabric settings.

3.For the installation of your first FortiGate device, you want to minimize the impact in your OT network. Therefore, you deploy it initially as an offline IDS.
Which two statements about this deployment are correct? (Choose two answers)
A. The FortiGate device acts as a network sensor.
B. The cybersecurity visibility increases with the security profiles.
C. Attacks, including zero-day attacks, are blocked.
D. OT traffic flows through the FortiGate device.
Answer: A, B
Explanation:
Deploying a FortiGate in offline IDS (also known as one-arm sniffer mode) is a common strategy in OT environments for several reasons found in the study guide:
Priority of Availability: In OT, availability and safety are critically important and prioritized higher than in IT. An offline IDS minimizes impact because it does not sit in the direct path of production traffic.
Network Sensor Role: In this mode, the FortiGate is connected to a mirror/SPAN port on a switch. It acts as a network sensor, receiving a copy of the traffic rather than having the traffic flow through it. This confirms Statement A is correct and Statement D is incorrect.
Passive vs. Active: The guide explicitly states that in OT environments, passive methods are preferred over active methods to avoid negatively impacting performance or causing process interruptions.
Depth of Visibility: Even though the device is offline, you apply security profiles (such as IPS, Application Control, and Antivirus) to the sniffer interface. This allows the FortiGate to analyze the copied traffic and provide deep visibility into the OT assets and their behaviors. This confirms Statement B is correct.
Detection vs. Prevention: An IDS (Intrusion Detection System) is passive; it can detect threats but cannot

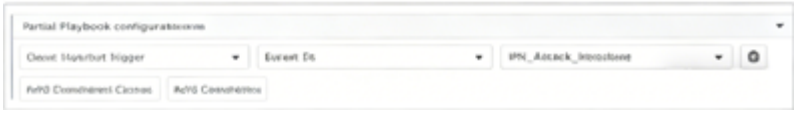
reset connections or drop packets to block attacks. Therefore, it cannot block zero-day attacks, making Statement C incorrect.

4.Refer to the exhibits.

Partial Playbook Monitor view



Partial Playbook configuration



A partial view of the Playbook Monitor page and the corresponding playbook configuration are shown. Based on the monitor page and the configuration of the playbook, what has triggered the Run_Report task? (Choose one answer)

A. An IPS_Attack_Handling event

B. An IPS incident creation

C. An Event_Trigger log

D. An IPS_Attack_Incident log

Answer: A

Explanation:

Based on the provided exhibits from the FortiAnalyzer playbook engine:

Playbook Trigger Condition: The Partial Playbook configuration exhibit shows that the playbook is set to trigger based on a condition where the Basic Handler Name is Equal To IPS_Attack_Handling.

Event vs. Log: In FortiAnalyzer, the field Basic Handler Name is a property of an Event record, indicating the specific Event Handler that generated it. A playbook configured with this condition is triggered by an Event, not directly by a raw log.

Playbook Execution Flow: The Partial Playbook Monitor view shows the execution sequence:

Event_Trigger (Starter): This is the entry point of the playbook, which matches the condition defined in the configuration.

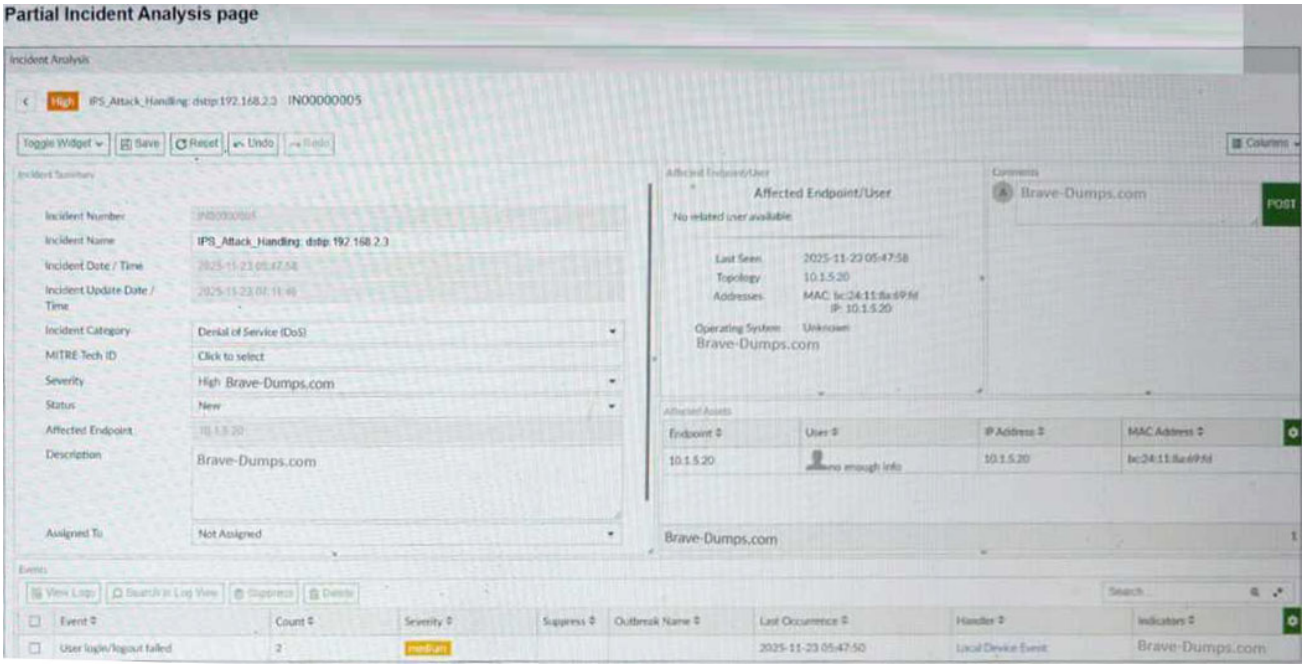
IPS_Attack_Incident: The first task executed after the trigger.

Run_Report: The task in question, which is executed as part of the automated workflow initiated by the starter.

Conclusion: Since the playbook's "Starter" is defined by the IPS_Attack_Handling handler name, an event produced by that handler is the root trigger for the entire playbook execution, including the

Run_Report task.
Therefore, the Run_Report task was triggered (as part of the playbook) by an IPS_Attack_Handling event.

5.Refer to the exhibits.



A partial Incident Analysis page and the log details related to the event are shown. An attack is reported on your OT network. You analyze the corresponding incident.

Based on the information provided on the Incident Analysis page and the log details, which two statements are correct? (Choose two answers)

A. The attack uses the Modbus protocol.

B. The attack is mitigated.

C. The attack uses the IEC 104 protocol.

D. The event severity is high.

E. The target device IP address is 10.1.5.20.

Answer: A, B

Explanation:

Based on the technical data provided in the exhibits and the OT Security 7.6 Architect curriculum:

Industrial Protocol Identification (Statement A): The log details exhibit clearly shows that the Destination Port used in the attack is 502. According to the study guide's section on Industrial Protocol Protection,

the standard port used by the Modbus TCP protocol is 502. Furthermore, the attack name identifies a "Triangle.Research.Nano-10.PLC," which are industrial controllers commonly utilizing Modbus for communications.
Attack Mitigation (Statement B): The log details specify that the Action taken by the FortiGate (Edge-FortiGate) was dropped. In cybersecurity and Fortinet fabric operations, dropping a packet associated with an IPS signature means the traffic was blocked from reaching its target, thereby mitigating the attack.
Target IP Address (Statement E): The log detail explicitly lists the Destination IP as 192.168.2.3. The Incident Analysis page also titles the incident with dstip:192.168.2.3. While the "Affected Endpoint" is shown as 10.1.5.20, in an "outgoing" attack direction (as shown in the log), this likely refers to the internal source/attacker IP, whereas the target is the destination IP (192.168.2.3). Thus, Statement E is incorrect.
Protocol Conflict (Statement C): The IEC 104 protocol typically utilizes port 2404. Since the log specifies port 502, Statement C is incorrect.
Severity Distinction (Statement D): While the Incident severity is marked as High, the question specifically asks about event severity. The "Events" table at the bottom of the Incident Analysis page shows a "User login/logout failed" event with a medium severity. Because there is a distinction in the management console between the severity of individual events and the aggregated incident, and Statement A and B are technically definitive based on port and action, A and B are the correct architectural choices.