KillTest

Mejor calidad. Mejor servicio

Preguntas de práctica

https://www.killtest.es

Actualizaciones gratuitas durante un año

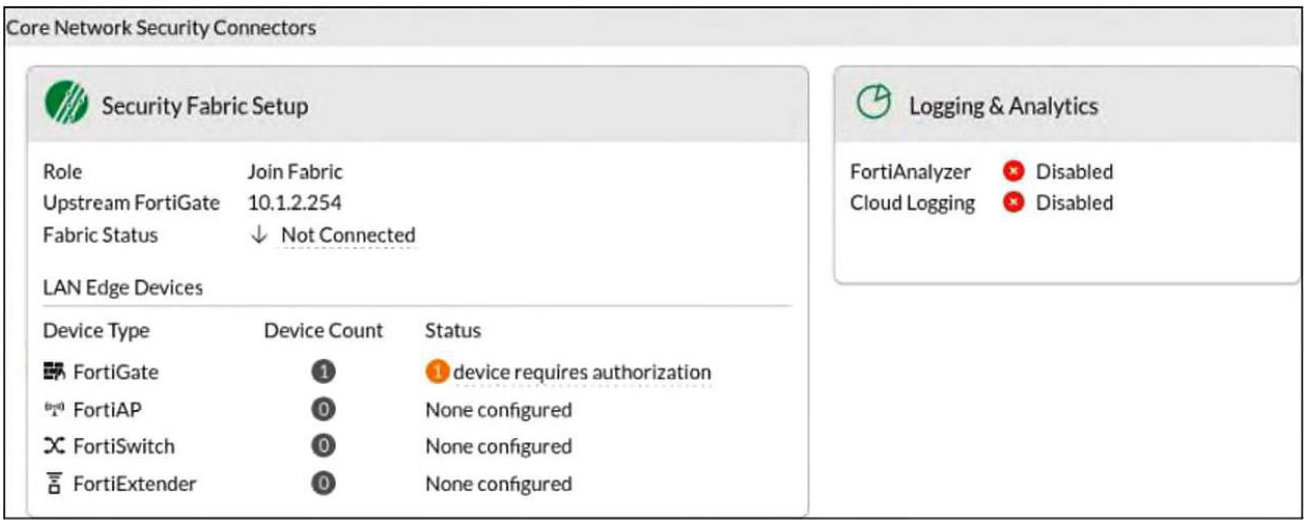
Exam : **NSEI_OTS_AR-7.6**

Title : Fortinet NSE I - 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:

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

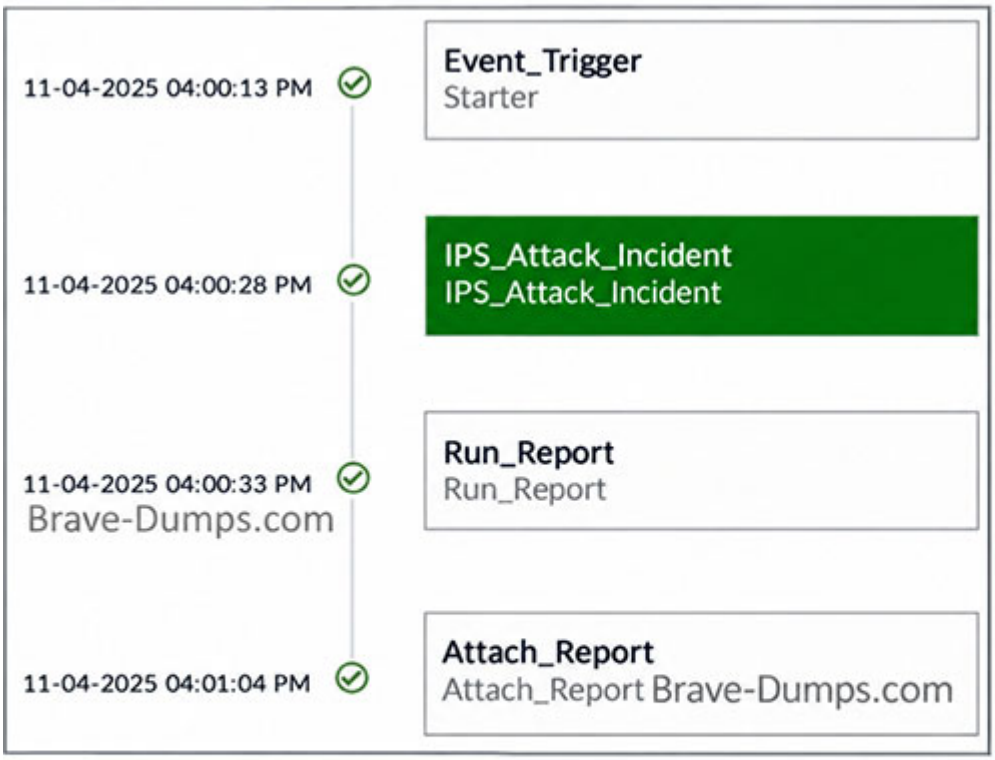
FortiGate sends logs to FortiAnalyzer, then FortiAnalyzer parses the logs and notifies the root FortiGate, after which the root FortiGate triggers the action. This shows that FortiAnalyzer must be configured so it can communicate with FortiGate through the Security Fabric.

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:

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

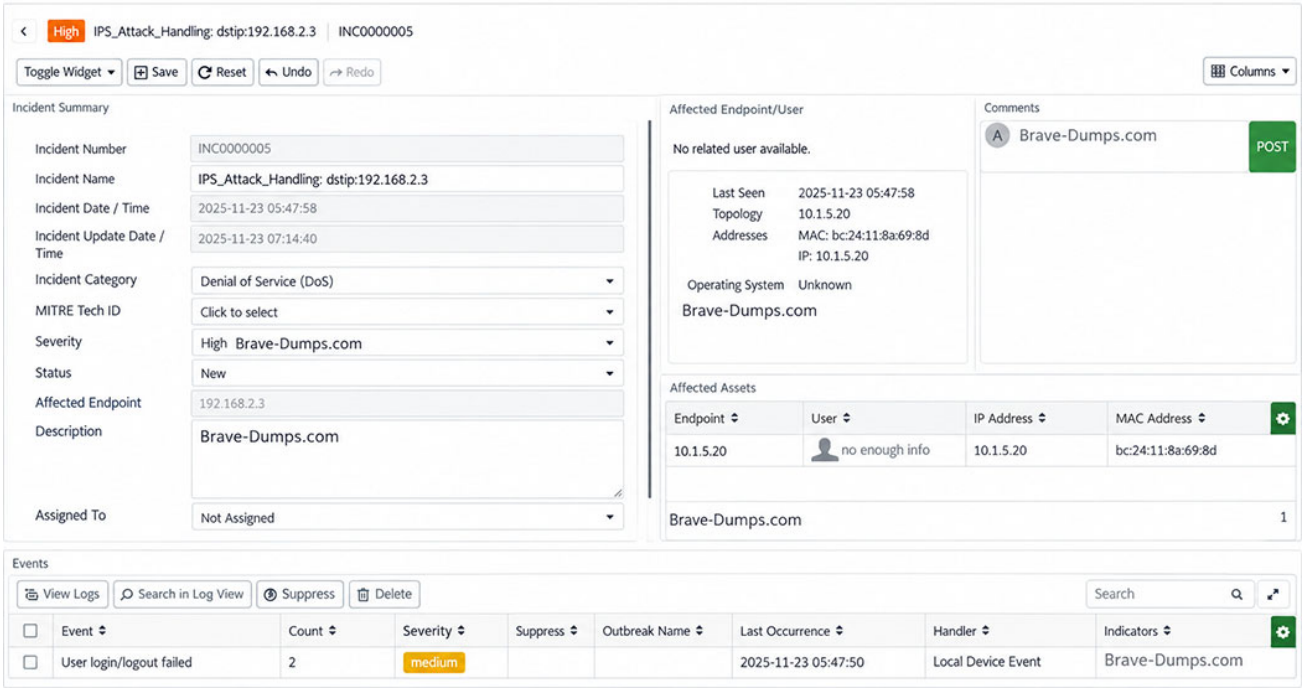
Answer: A

Explanation:

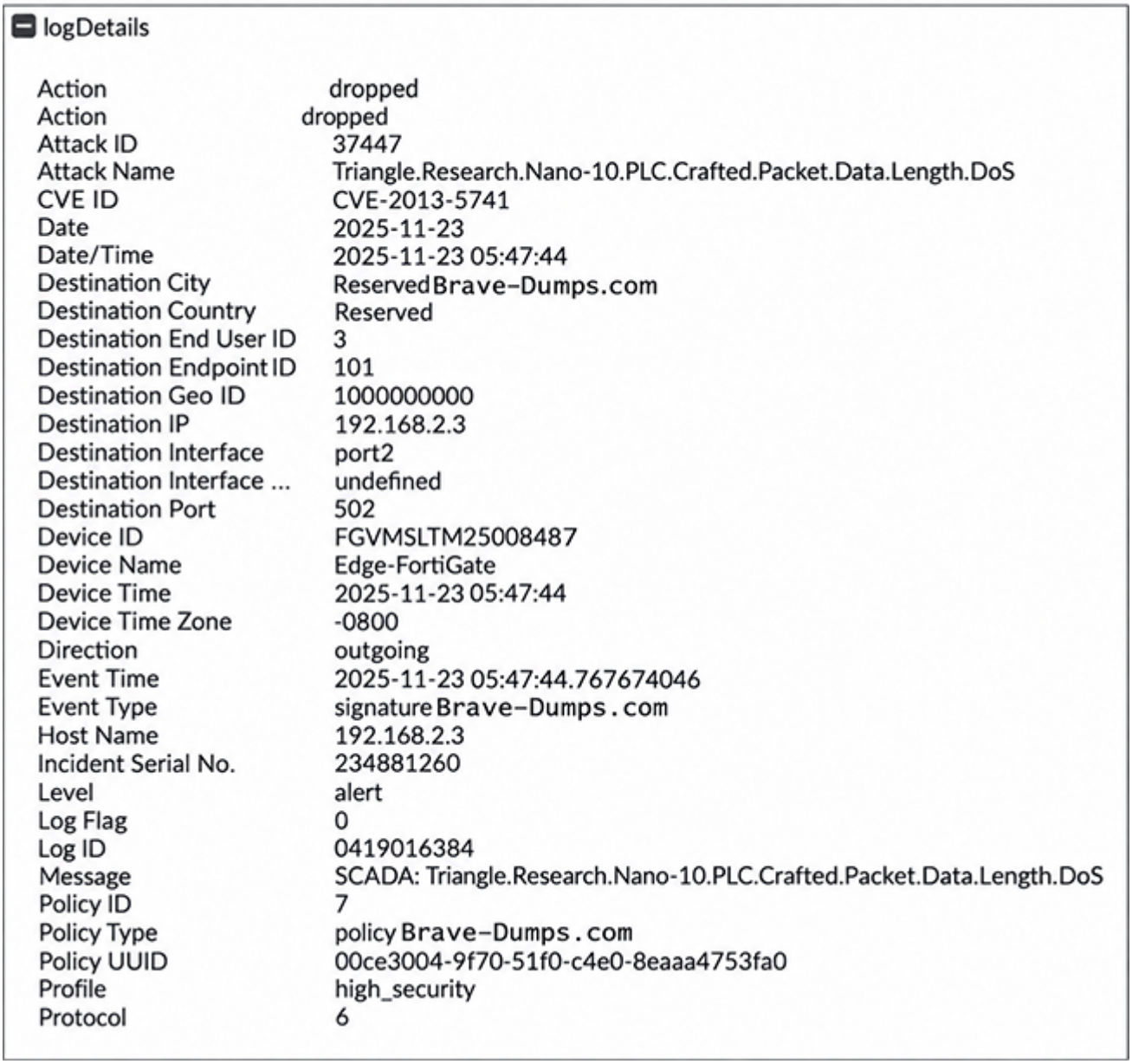
Based on the provided exhibits from the FortiAnalyzer playbook engine: Therefore, the Run_Report task was triggered (as part of the playbook) by an IPS_Attack_Handling event.

5.Refer to the exhibits.

Partial Incident Analysis page



Log details related to the event



logDetails

Action	dropped
Action	dropped
Attack ID	37447
Attack Name	Triangle.Research.Nano-10.PLC.Crafted.Packet.Data.Length.DoS
CVE ID	CVE-2013-5741
Date	2025-11-23
Date/Time	2025-11-23 05:47:44
Destination City	Reserved Brave-Dumps.com
Destination Country	Reserved
Destination End User ID	3
Destination Endpoint ID	101
Destination Geo ID	1000000000
Destination IP	192.168.2.3
Destination Interface	port2
Destination Interface ...	undefined
Destination Port	502
Device ID	FGVMSLTM25008487
Device Name	Edge-FortiGate
Device Time	2025-11-23 05:47:44
Device Time Zone	-0800
Direction	outgoing
Event Time	2025-11-23 05:47:44.767674046
Event Type	signature Brave-Dumps.com
Host Name	192.168.2.3
Incident Serial No.	234881260
Level	alert
Log Flag	0
Log ID	0419016384
Message	SCADA: Triangle.Research.Nano-10.PLC.Crafted.Packet.Data.Length.DoS
Policy ID	7
Policy Type	policy Brave-Dumps.com
Policy UUID	00ce3004-9f70-51f0-c4e0-8eaaa4753fa0
Profile	high_security
Protocol	6

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: