Fortinet NSEI_OTS_AR-7.6 Dumps

Shared by Vang on 10-08-2026

For More Free Questions and Preparation Resources

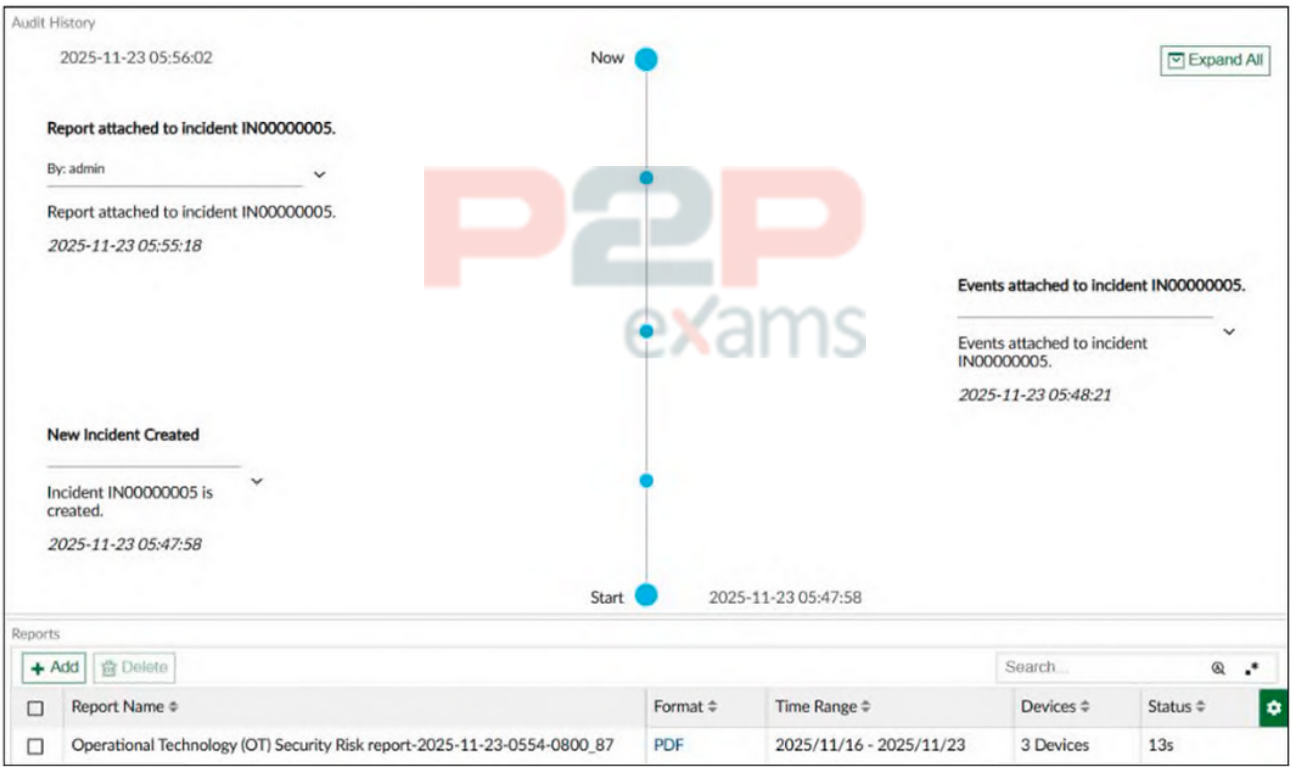
Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

Partial Incident Analysis page



A partial Incident Analysis page is shown. How was the 360-Degree Security Review OT report attached to the incident? (Choose one answer)

Options:

A- Automatically by a stitch
B- Automatically by an event handler
C- Automatically by a playbook
D- Manually by an administrator

Answer:

D

Explanation:

The study guide says playbooks are used to automate tasks such as running reports and creating/updating incidents. It also says that after a playbook is triggered, it flows through its

configured tasks.

It further shows a sample playbook sequence where an event is detected, an incident is created, a report runs, and details are attached to the incident. That is exactly the kind of workflow shown in the incident analysis view.

By contrast, the study guide says event handlers generate events when logs match configured rules. Event handlers are for detection, not for attaching reports to incidents.

Question 2

Question Type: MultipleChoice

In your OT environment, you want to detect the devices passively. Which two methods must you implement? (Choose two answers)

Options:

A- SSH
B- SNMP
C- Vendor OUI
D- Network traffic

Answer:

C, D

Explanation:

The correct answers are C. Vendor OUI and D. Network traffic.

The study guide explicitly separates active/direct profiling methods from passive/non-direct methods and states that ''In OT environments, passive methods are preferred over active methods.'' It then lists the methods that do not require FortiNAC to interact directly with the device being profiled. Among those methods are ''Network traffic: gathered from the infrastructure'' and ''Vendor OUI: determined by the MAC address gathered from the infrastructure.'' That directly matches options C and D.

Options A and B are incorrect because SSH and SNMP are shown in the guide under the direct/active profiling methods. The guide's point is that passive detection avoids directly scanning or interacting with OT endpoints, since that can negatively affect performance in industrial environments. Because the question specifically asks for passive detection methods,

the correct pair is Vendor OUI and Network traffic.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

Firewall Policy page

Policy	ID	Source	Destination	Schedule	Service	Action	Type	Security Profiles
LAN (port5) → port2								
PLC1_access (8)	8	all Supervisor	PLC-1	always	ALL	ACCEPT	Standard	no-inspection
Supervisor_access (9)	9	all Supervisor	PLC-1	always	ALL_ICMP	ACCEPT	Standard	no-inspection
Floor-2_Access (7)	7	all Management	all	always	ALL_ICMP	ACCEPT	Standard	no-inspection

A firewall policy page is shown. To improve the security of your OT network, you have configured a Supervisor profile in the firewall policies, as shown in the exhibit. However, a supervisor is reporting that he cannot ping PLC-1. What are the two reasons? (Choose two answers)

Options:

A- The supervisor must first authenticate using a protocol such as HTTPS or Telnet.
B- The Supervisor profile is not configured in the remote server.
C- The firewall policy ID 8 is not enabled.
D- The CLI parameter auth-on-demand is set to always.

Answer:

A, C

Explanation:

The correct answers are A and C.

Option A is correct because the study guide explains that with active authentication, FortiGate prompts the user only when they use ''an acceptable login protocol.'' It states: ''When you use only active authentication, if all possible policies that could match the source IP address have authentication enabled, then the user will receive a login prompt (assuming they use an acceptable login protocol).'' A direct ping to PLC-1 uses ICMP, which is not the kind of login protocol used to trigger user authentication. So the supervisor must first authenticate through a

protocol such as HTTPS or Telnet, then the ICMP traffic can match the authenticated policy.

Option C is also correct because the exhibit shows policy ID 8 greyed out, meaning it is not enabled. That policy appears above the Supervisor_access (9) policy and allows broader access to PLC-1, whereas policy 9 is limited to ALL_ICMP. The study guide explains that ''Because the user has not yet authenticated, the user group aspect of the traffic does not match'' and FortiGate continues searching for another complete match. In this case, with policy 8 disabled, the supervisor is left with only the ICMP rule, which cannot be used to perform the initial login step needed for active authentication.

Option B is not supported by the exhibit. Option D is incorrect because auth-on-demand always would force authentication prompts more aggressively, but the core problem here is that the user is trying to start with ICMP and the broader policy that could permit the initial authenticated access is disabled.

Question 4

Question Type: MultipleChoice

You want to improve access control for your large OT network using passive authentication. What must you configure on FortiGate? (Choose one answer)

Options:

A- Fortinet Single-Sign On (FSSO)
B- Local users
C- Two-factor authentication
D- A FortiAuthenticator device as a remote server

Answer:

A

Explanation:

The correct answer is A. Fortinet Single-Sign On (FSSO). The study guide states under Active and Passive Authentication that for passive authentication, ''User does not receive a login prompt from FortiGate'', ''Credentials are determined automatically'', and specifically ''FSSO, RSSO, and NTLM can be used.'' It then explains that passive authentication occurs with the single sign-on method and explicitly identifies Fortinet SSO (FSSO) as one of those methods.

The guide also says: ''For passive authentication, you can implement FSSO. FSSO allows users

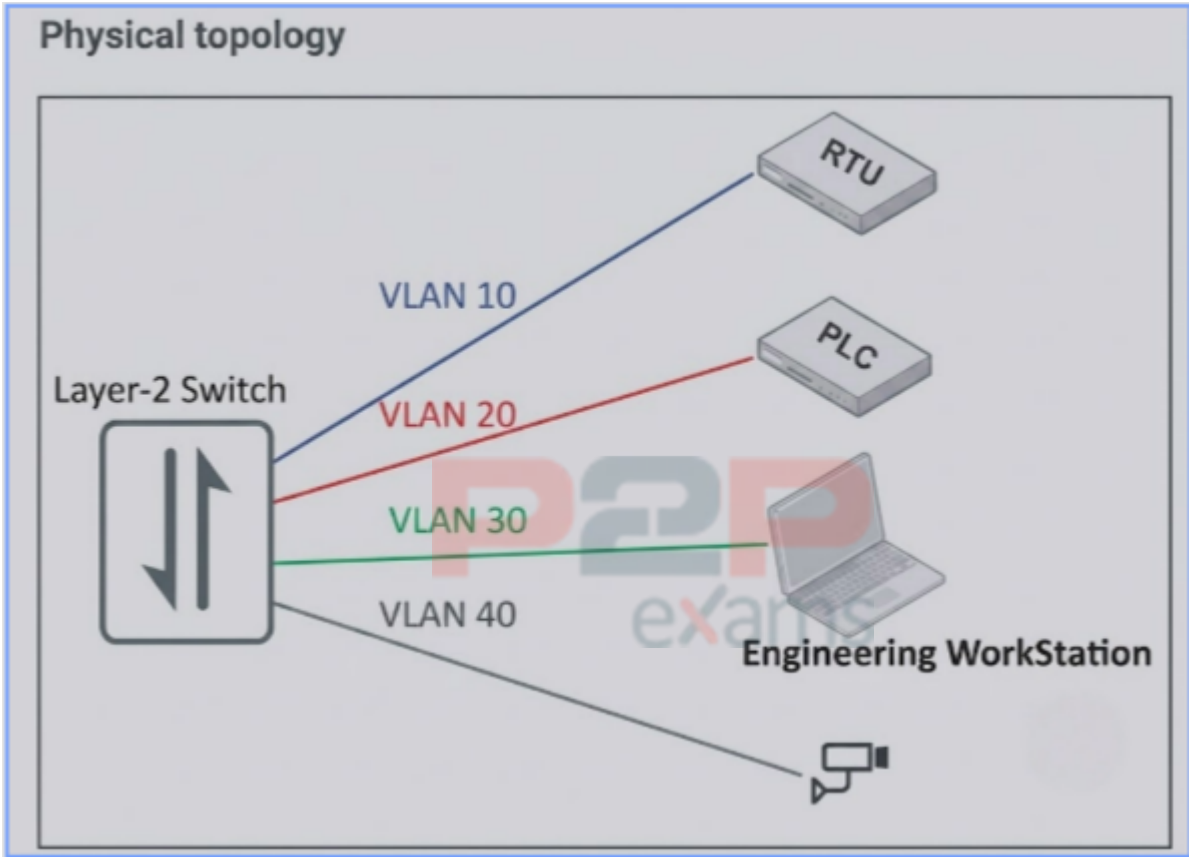
who have already authenticated on the network through another system to be transparently identified. After initial login to any system on the network, users can access allowed resources without being prompted for credentials.'' That is exactly what the question asks for: improving access control in a large OT network using passive authentication.

The other options do not match passive authentication. Local users are part of local authentication, two-factor authentication adds an extra security factor but still uses active authentication, and FortiAuthenticator as a remote server supports centralized authentication for mid-to-large networks, but by itself it is not the specific passive-authentication method being asked here. The study guide is explicit that the FortiGate configuration for passive authentication is FSSO.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.



A partial OT network is shown. You have configured the FortiGate device with VLANs to segment the OT network. The supervisor now wants to connect to the PLC from the Engineering Workstation. How can you allow access from the Engineering Workstation to the PLC? (Choose one answer)

Options:

A- You must configure intra-switch-policy as explicit.
B- You must configure intra-switch-policy as implicit.
C- You must configure forward domain IDs.
D- You must configure a layer 3 switch.

Answer:

D

Explanation:

The correct answer is D. You must configure a layer 3 switch.

The study guide explains that ''Layer 2 devices can add or remove tags'' but ''cannot modify them.'' It then states that ''A layer 3 device, such as a router or FortiGate, can modify the VLAN tag before routing the packet. This allows them to route traffic between VLANs.'' It also explicitly describes ''Router on a Stick'' as ''a way to allow routing between VLANs.'' Since the exhibit shows a layer-2 switch and the Engineering Workstation and PLC are placed in different VLANs, inter-VLAN communication requires layer-3 routing.

The other options do not solve this requirement. intra-switch-policy explicit/implicit applies to a software switch, where member interfaces are in the same broadcast domain and same subnet, not to routing between separate VLANs. forward domain IDs are used in transparent mode to confine broadcasts to specific broadcast domains; they do not provide inter-VLAN access. Therefore, to let the Engineering Workstation in one VLAN reach the PLC in another VLAN, you need a layer 3 routing function, which matches option D.

Question 6

Question Type: MultipleChoice

You want to improve the security of your OT network and therefore deploy a FortiGate device with the OT signatures database. Which two statements about this database are true? (Choose two answers)

Options:

A- You must install a valid OT security service license.
B- You must import the OT signatures database manually.

C- The OT signatures database is enabled by default.
D- You must set exclude-signatures to none in the console line interface.

Answer:

A, D

Explanation:

The correct answers are A and D.

Option A is correct because the study guide states that for OT protocol coverage, ''a valid OT security service license is required to receive updates on both intrusion prevention and application control signatures.'' It also shows ''Valid license required'' in the FortiGuard subscriptions section for OT protocol coverage. This confirms that a valid OT security service license is required to use and maintain the OT signatures database correctly.

Option D is also correct because the guide explicitly shows the CLI configuration used ''To enable OT signatures'':

config ips global

set exclude-signatures none

end

It then states that ''By default, OT signatures are excluded from the signatures lists on the GUI until you enable them on the CLI.'' This directly confirms that you must set exclude-signatures to none in the CLI to enable OT signatures.

Option B is incorrect because the study guide does not say you manually import the OT signatures database. Instead, it explains that FortiGuard maintains updated OT signatures and that a valid license is required to receive updates. Option C is incorrect because the guide clearly says OT signatures are excluded by default until enabled from the CLI.