



Vendor: Fortinet

Exam Code: NSE6_OTP_AR-7.6

Exam Name: Fortinet NSE 6 - OT Security 7.6 Architect

Version: DEMO

QUESTION 1

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

Core Network Security Connectors section

Core Network Security Connectors

Security Fabric Setup

Role: Join Fabric

Upstream FortiGate: 10.1.2.254

Fabric Status: ↓ Not Connected ⓘ

LAN Edge Devices

Device Type	Device Count	Status
FortiGate	3	ⓘ device requires authorization
FortiAP	1	None configured
FortiSwitch	1	None configured
FortiExtender	1	None configured

Logging & Analytics

FortiAnalyzer: ⓧ Disabled

Cloud Logging: ⓧ Disabled

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

QUESTION 2

To improve visibility into the risks in your OT network, you would like to create a new report on FortiAnalyzer.

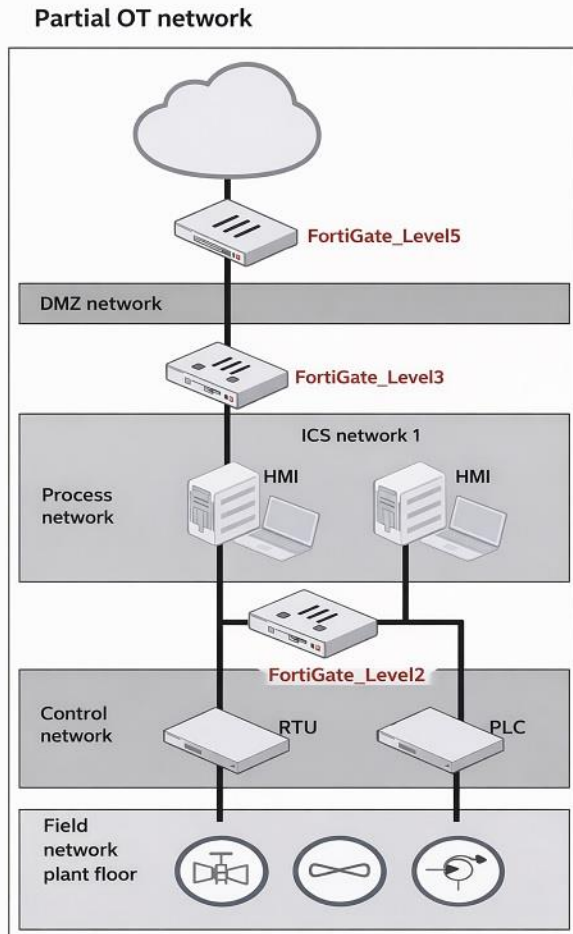
What must you do to create this report? (Choose one answer)

- A. Create a template or use an existing one.
- B. Import a report created in FortiSIEM.
- C. Enable the FortiAnalyzer Fabric settings.
- D. Clone a predefined report to create a new one.

Answer: A

QUESTION 3

Refer to the exhibit. A partial OT network is shown.



In this OT network, you must add additional security measures to detect OT protocols and, therefore, increase the traffic visibility.
Which security sensor must you implement to detect the OT protocols in this network? (Choose one answer)

- A. Device detection on all the FortiGate interfaces
- B. Inline IDS on FortiGate_Level3
- C. Application sensor set to monitor on all the FortiGate devices
- D. IPS sensor on FortiGate Level5

Answer: C

QUESTION 4

Refer to the exhibits. A partial Basic Event Handler page on FortiAnalyzer and the creation of a trigger in a FortiGate device are shown.

Partial Basic Event Handler page

Edit Basic Event Handler

Status ☒ Alert_trigger

Description 0/1024

MITRE Tech ID Click to select

Data Selector Click to select

Automation Stitch ☒

Creation of a trigger

Create New Automation Trigger

FortiAnalyzer Event Handler A specified FortiAnalyzer event handler was triggered.

Name Compromised_Device_Trigger

Description 0/255

FortiAnalyzer Event Handler

Configure a FortiAnalyzer connection to utilize FortiAnalyzer event handlers:

- FortiAnalyzer

Event handler name

Event settings ☐ Search + Create

No entries

To improve the protection of your OT network, you want to automate the handling of compromised devices notified through FortiAnalyzer. You have configured an event handler as shown in the exhibit. When you create the trigger on the FortiGate device, the Event handler name field does not provide the Alert_trigger option. What two actions must you perform to make the Alert_trigger option available? (Choose two answers)

- A. You must click + Create in the Event handler name field.
- B. You must authorize the FortiGate device on FortiAnalyzer
- C. You must configure the FortiAnalyzer setting on the FortiGate device.
- D. You must configure the trigger on the root FortiGate.

Answer: BC

QUESTION 5

Refer to the exhibit. A partial Application Sensor profile is shown.

Partial Application Sensor profile

Name

Comments 0/255

Categories

Mixed ▾ All Categories

☒ Business (158, ▴ 11)
☒ Collaboration (263, ▴ 16)
☒ Game (83)
☒ Generative AI (30, ▴ 23)
☒ Network Service (338)
☒ Remote Access (99)
☒ Storage/Backup (156, ▴ 24)
☒ Video/Audio (148, ▴ 16)
☒ Web Client (24)

☒ Cloud/IT (68, 2)
☒ Email (76, ▴ 11)
☒ General Interest (235, ▴ 11)
☒ Mobile (3)
☒ Operational Technology (3386, ▴ 37)
☒ Proxy (200)
☒ Social Media (111, ▴ 28)
☒ Update (48)
☒ VoIP (23)
☒ Unknown Applications

☒ Network Protocol Enforcement

Application and Filter Overrides

+ Create New Edit Delete

Priority	Details	Type	Action
1	☒ Modbus_Read.Holding.Registers	Application	☒ Allow
2	☒ Modbus	Application	☒ Block

When you apply this profile in a firewall policy, which two statements are correct? (Choose two answers)

- A. OT signatures are enabled.
- B. All OT protocols are monitored.
- C. Modbus write commands are blocked.
- D. A log is provided for each Modbus read holding registers command.

Answer: AC

QUESTION 6

Refer to the exhibit. A Run_report task is shown.

Name	Run_report
Description	
Connector	Click to select ▼
Action	Run Report ▼
Report ⓘ	Playbook Starter ▼ A
Time Period	Q ▼
Filter	Playbook Starter

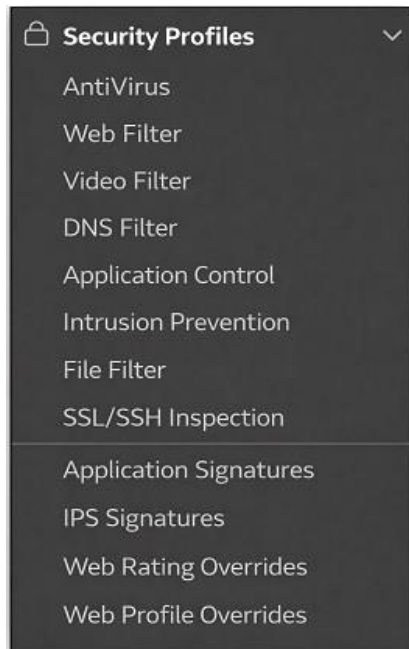
You want to automate the generation of a newly created report on FortiAnalyzer. When you configure the Run_report task in Playbook, why is the report not shown in the Report field? (Choose two answers)

- A. You must first configure the connector.
- B. You must first enable Extended Log Filtering in the report.
- C. You must first enable Auto-cache in the report.
- D. You must first configure an event handler.
- E. You must first select Playbook Starter, and then select the newly created report.

Answer: AC

QUESTION 7

Refer to the exhibit. The OT devices behind the ruggedized FortiGate have vulnerabilities and you want to apply a virtual patching profile in the firewall policy.



Why is Virtual Patching not available in the Security Profiles section? (Choose one answer)

- A. You must enable Virtual Patching in the Feature Visibility section.
- B. You must have a ruggedized FortiGate allowing the virtual patching feature.
- C. You must enable OT signatures.
- D. You must have a valid OT security service license.

Answer: A

QUESTION 8

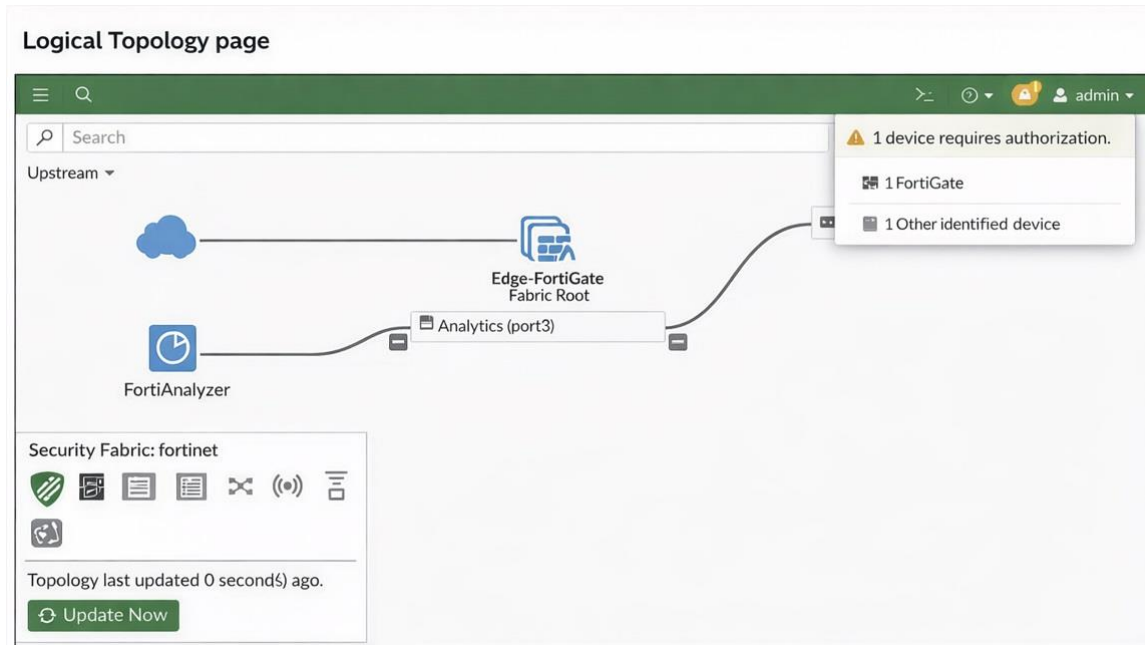
Which industrial protocol does not support VLANs? (Choose one answer)

- A. not support VLANs? C
- B. Ethernet over industrial protocol
- C. EtherCAT
- D. Modbus over TCP

Answer: C

QUESTION 9

Refer to the exhibit. A Logical Topology page of a FortiGate device is shown.



Your OT company wants to gain visibility into the network. You decide to implement device detection with the Security Fabric.

Based on the exhibit, which statement is correct? (Choose one answer)

- A. Device Detection is enabled on the other identified device.
- B. The other identified device must be authorized on the root FortiGate.
- C. The other identified device must be authorized on FortiAnalyzer.
- D. Device Detection is enabled on port3.

Answer: B

QUESTION 10

Refer to the exhibit. A Virtual Patching profile is shown.

Virtual Patching profile

Name

Severity

☐ Information
☐ Low

☒ Medium
☒ High

☒ Critical

Action

☒ Allow
☒ Block

Logging

☒ Enable
☐ Disable

Comments

Virtual Patching Exemptions

+ Create new
Edit
Delete

☐	Status	Device (MAC Address)	Virtual Patch Signature
☐	Enabled	11:11:11:11:11:11	
☐	Enabled	12:12:12:12:12:12	Schneider.Electric.ClearSCADA.HTTPInterface.XSS

+ Create new
Edit
Delete

You have recently updated your SCADA system and would like to apply the SCADA virtual patching profile.

Which two statements about this profile are correct? (Choose two answers)

- A. Only the vulnerability Schneider.Electric.ClearSCADA.HTTP.Interface.XSS is still present.
- B. Low severity signatures are not blocked for the device with the MAC address 12:12:12:12:12:12.
- C. This profile blocks critical severity signatures for all the devices.
- D. The device with the MAC address 11:11:11:11:11:11 is considered to have no vulnerabilities.

Answer: BD

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14