

Fortinet

Exam Questions NSE7_OTIS-6.4

Fortinet NSE 7 - OT Security 6.4



NEW QUESTION 1

An OT supervisor needs to protect their network by implementing security with an industrial signature database on the FortiGate device. Which statement about the industrial signature database on FortiGate is true?

- A. A supervisor must purchase an industrial signature database and import it to the FortiGate.
- B. An administrator must create their own database using custom signatures.
- C. By default, the industrial database is enabled.
- D. A supervisor can enable it through the FortiGate CLI.

Answer: D

NEW QUESTION 2

What two advantages does FortiNAC provide in the OT network? (Choose two.)

- A. It can be used for IoT device detection.
- B. It can be used for industrial intrusion detection and prevention.
- C. It can be used for network micro-segmentation.
- D. It can be used for device profiling.

Answer: CD

NEW QUESTION 3

Refer to the exhibit.

Active Rules x Windows Installed Patches x Router/Switch Image Distribution x						
Device Name	Device Type	Vendor	Device Type Model	Device Hardware Model	Device Image File	Count
SJ-QA-A-IOS-JunOffice	Cisco	IOS	1760		C1700-advsecurityk9-mz.123-8.T4.bin	1
SJ-Main-Cat6500	Cisco	IOS	WS-C6509		s72033-advipservicesk9_wan-mz.122-33.SX11.bin	1
ph-network-3560_1	Cisco	IOS	WS-C3560G-48PS-S		c3560-advipservicesk9-mz.122-25.SEE4.bin	1

An OT administrator ran a report to identify device inventory in an OT network. Based on the report results, which report was run?

- A. A FortiSIEM CMDB report
- B. A FortiAnalyzer device report
- C. A FortiSIEM incident report
- D. A FortiSIEM analytics report

Answer: A

NEW QUESTION 4

An OT administrator configured and ran a default application risk and control report in FortiAnalyzer to learn more about the key application crossing the network. However, the report output is empty despite the fact that some related real-time and historical logs are visible in the FortiAnalyzer. What are two possible reasons why the report output was empty? (Choose two.)

- A. The administrator selected the wrong logs to be indexed in FortiAnalyzer.
- B. The administrator selected the wrong time period for the report.
- C. The administrator selected the wrong devices in the Devices section.
- D. The administrator selected the wrong hcache table for the report.

Answer: BD

NEW QUESTION 5

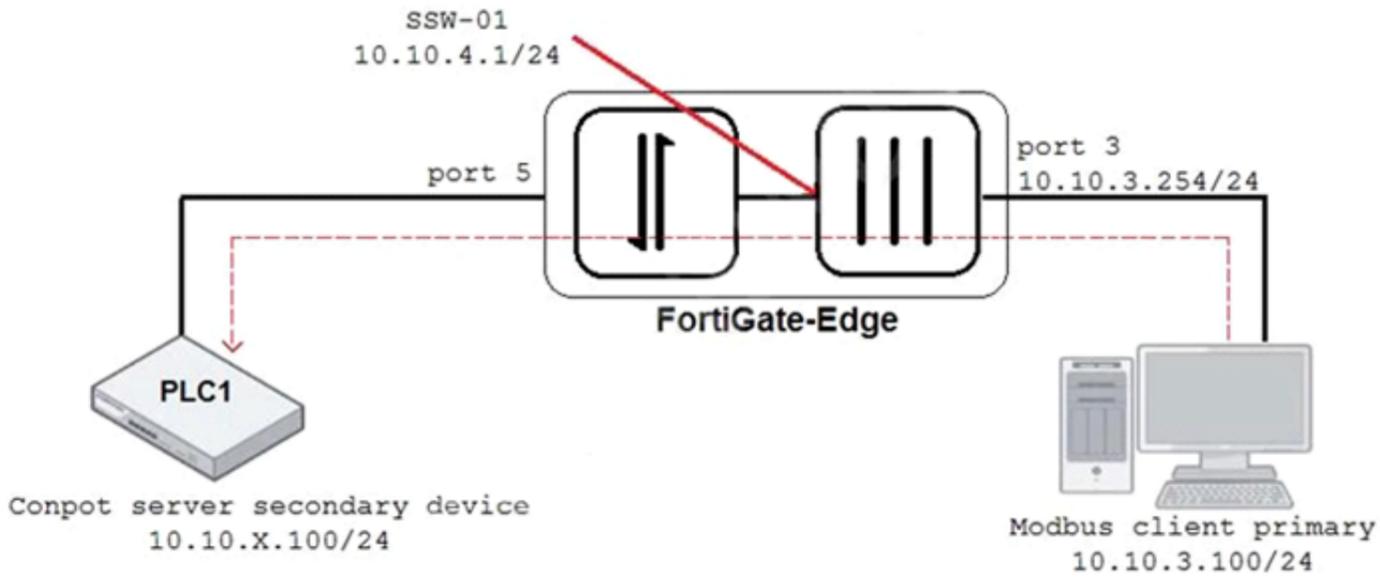
Which three Fortinet products can be used for device identification in an OT industrial control system (ICS)? (Choose three.)

- A. FortiNAC
- B. FortiManager
- C. FortiAnalyzer
- D. FortiSIEM
- E. FortiGate

Answer: ACD

NEW QUESTION 6

Refer to the exhibit.



An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modbus traffic in the OT network. The FortiGate-Edge device is configured with a software switch interface ssw-01.

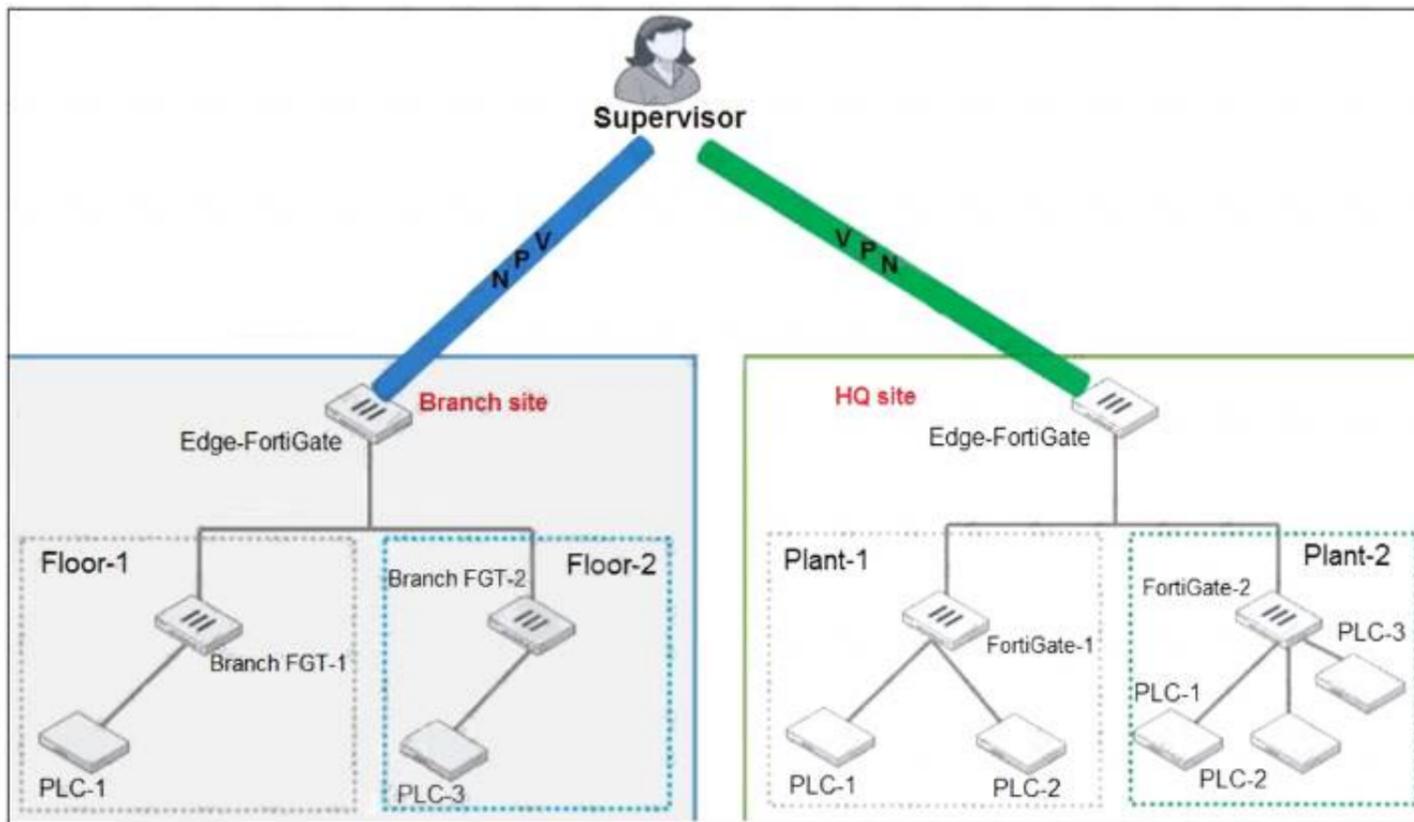
Based on the topology shown in the exhibit, which two statements about the successful simulation of traffic between client and server are true? (Choose two.)

- A. The FortiGate-Edge device must be in NAT mode.
- B. NAT is disabled in the FortiGate firewall policy from port3 to ssw-01.
- C. The FortiGate devices is in offline IDS mode.
- D. Port5 is not a member of the software switch.

Answer: AC

NEW QUESTION 7

Refer to the exhibit.



You need to configure VPN user access for supervisors at the breach and HQ sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must you do to achieve this objective?

- A. You must use a FortiAuthenticator.
- B. You must register the same FortiToken on more than one FortiGate.
- C. You must use the user self-registration server.
- D. You must use a third-party RADIUS OTP server.

Answer: A

NEW QUESTION 8

Refer to the exhibit.



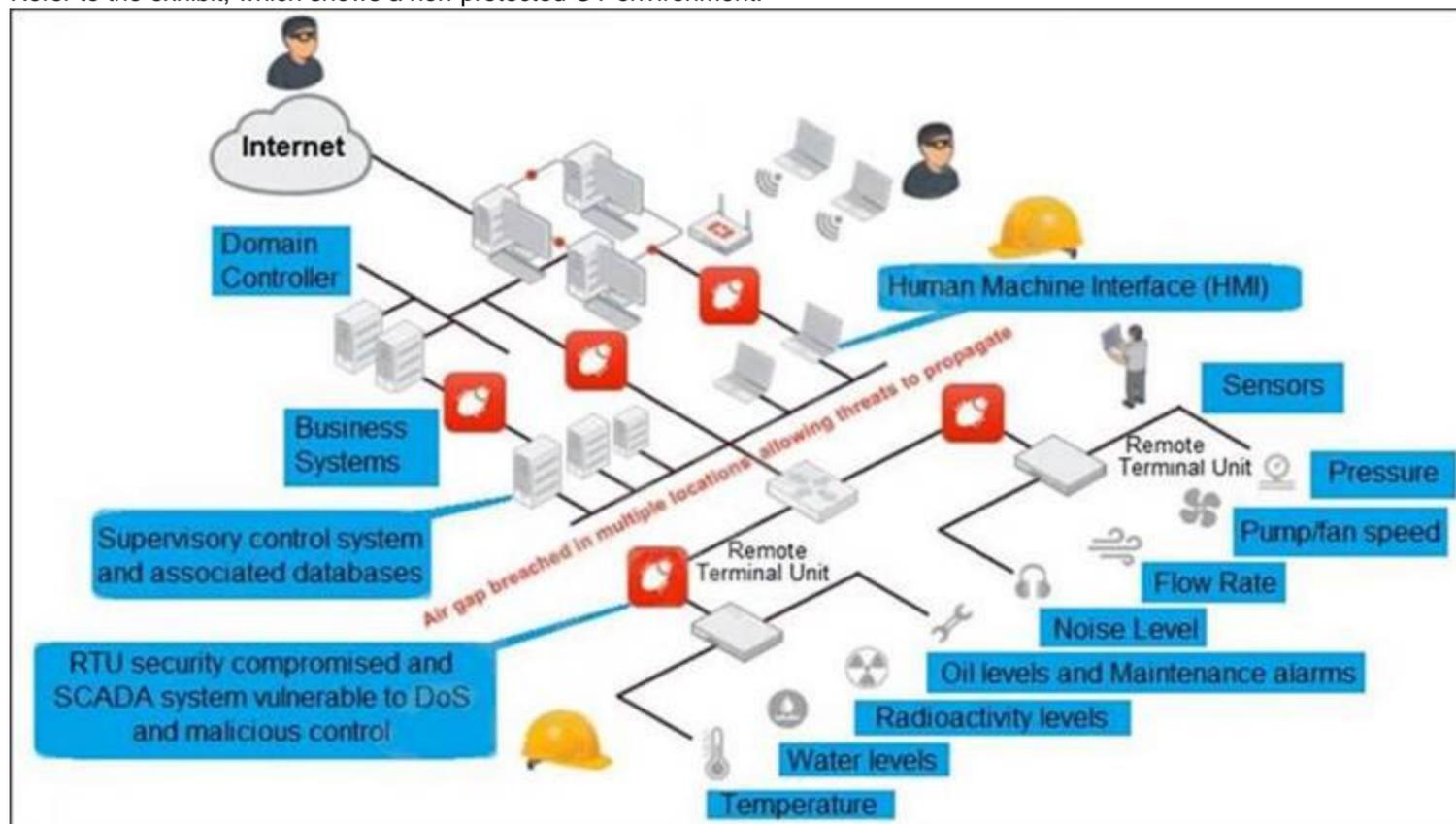
Based on the Purdue model, which three measures can be implemented in the control area zone using the Fortinet Security Fabric? (Choose three.)

- A. FortiGate for SD-WAN
- B. FortiGate for application control and IPS
- C. FortiNAC for network access control
- D. FortiSIEM for security incident and event management
- E. FortiEDR for endpoint detection

Answer: BCD

NEW QUESTION 9

Refer to the exhibit, which shows a non-protected OT environment.



An administrator needs to implement proper protection on the OT network. Which three steps should an administrator take to protect the OT network? (Choose three.)

- A. Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.
- B. Deploy a FortiGate device within each ICS network.
- C. Configure firewall policies with web filter to protect the different ICS networks.
- D. Configure firewall policies with industrial protocol sensors
- E. Use segmentation

Answer: ACD

NEW QUESTION 10

An OT network architect must deploy a solution to protect fuel pumps in an industrial remote network. All the fuel pumps must be closely monitored from the corporate network for any temperature fluctuations. How can the OT network architect achieve this goal?

- A. Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature security rule on the corporate network.
- B. Configure a fuel server on the corporate network, and deploy a FortiSIEM with a single pattern temperature performance rule on the remote network.
- C. Configure a fuel server on the remote network, and deploy a FortiSIEM with a single pattern temperature performance rule on the corporate network.
- D. Configure both fuel server and FortiSIEM with a single-pattern temperature performance rule on the corporate network.

Answer: B

NEW QUESTION 10

An OT architect has deployed a Layer 2 switch in the OT network at Level 1 the Purdue model-process control. The purpose of the Layer 2 switch is to segment traffic between PLC1 and PLC2 with two VLANs. All the traffic between PLC1 and PLC2 must first flow through the Layer 2 switch and then through the FortiGate

device in the Level 2 supervisory control network.
 What statement about the traffic between PLC1 and PLC2 is true?

- A. The Layer 2 switch rewrites VLAN tags before sending traffic to the FortiGate device.
- B. The Layer 2 switches routes any traffic to the FortiGate device through an Ethernet link.
- C. PLC1 and PLC2 traffic must flow through the Layer-2 switch trunk link to the FortiGate device.
- D. In order to communicate, PLC1 must be in the same VLAN as PLC2.

Answer: C

NEW QUESTION 12

An OT administrator is defining an incident notification policy using FortiSIEM and would like to configure the system with a notification policy. If an incident occurs, the administrator would like to be able to intervene and block an IP address or disable a user in Active Directory from FortiSIEM. Which step must the administrator take to achieve this task?

- A. Configure a fabric connector with a notification policy on FortiSIEM to connect with FortiGate.
- B. Create a notification policy and define a script/remediation on FortiSIEM.
- C. Define a script/remediation on FortiManager and enable a notification rule on FortiSIEM.
- D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIEM.

Answer: C

NEW QUESTION 13

Refer to the exhibit.

```
config system interface
  edit VLAN101_dmz
    set forward-domain 101
  next
  edit VLAN101_internal
    set forward-domain 101
end
```

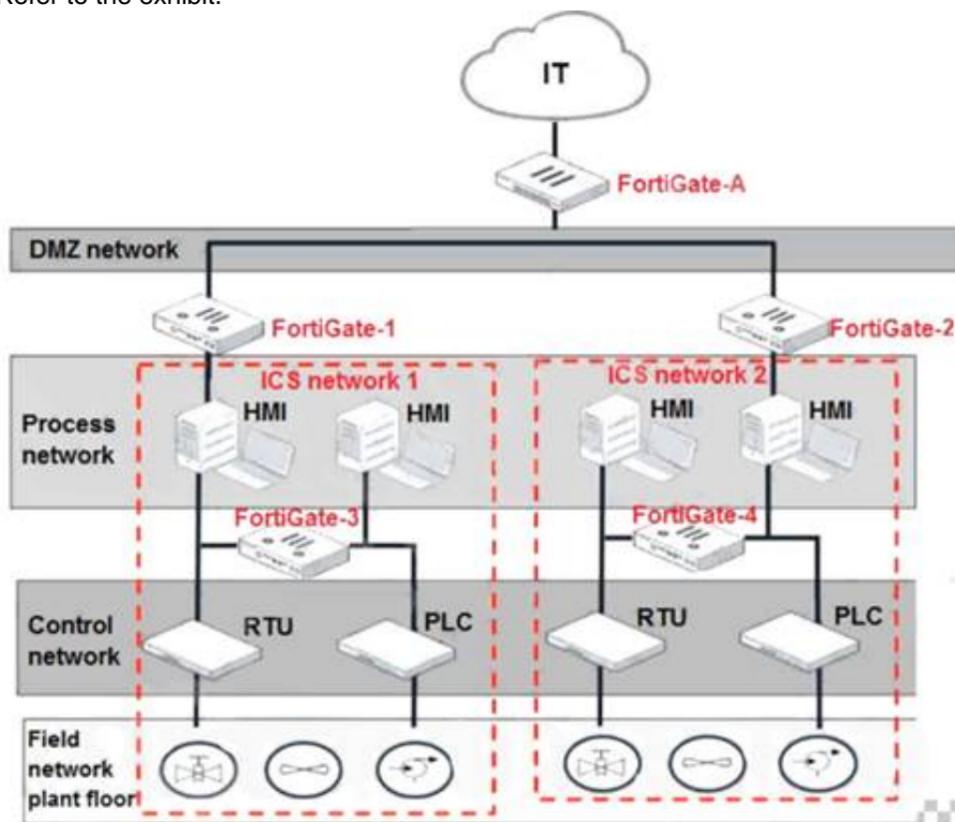
Given the configurations on the FortiGate, which statement is true?

- A. FortiGate is configured with forward-domains to reduce unnecessary traffic.
- B. FortiGate is configured with forward-domains to forward only domain controller traffic.
- C. FortiGate is configured with forward-domains to forward only company domain website traffic.
- D. FortiGate is configured with forward-domains to filter and drop non-domain controller traffic.

Answer: A

NEW QUESTION 18

Refer to the exhibit.



Based on the topology designed by the OT architect, which two statements about implementing OT security are true? (Choose two.)

- A. Firewall policies should be configured on FortiGate-3 and FortiGate-4 with industrial protocol sensors.
- B. Micro-segmentation can be achieved only by replacing FortiGate-3 and FortiGate-4 with a pair of FortiSwitch devices.
- C. IT and OT networks are separated by segmentation.
- D. FortiGate-3 and FortiGate-4 devices must be in a transparent mode.

Answer: CD

NEW QUESTION 22

What are two benefits of a Nozomi integration with FortiNAC? (Choose two.)

- A. Enhanced point of connection details
- B. Direct VLAN assignment
- C. Adapter consolidation for multi-adapter hosts
- D. Importation and classification of hosts

Answer: AB

NEW QUESTION 26

You are investigating a series of incidents that occurred in the OT network over past 24 hours in FortiSIEM. Which three FortiSIEM options can you use to investigate these incidents? (Choose three.)

- A. Security
- B. IPS
- C. List
- D. Risk
- E. Overview

Answer: CDE

NEW QUESTION 31

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE7_OTIS-6.4 Practice Exam Features:

- * NSE7_OTIS-6.4 Questions and Answers Updated Frequently
- * NSE7_OTIS-6.4 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_OTIS-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_OTIS-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_OTIS-6.4 Practice Test Here](#)