Fortinet

Exam Questions NSE7_OTS-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
An OT network architect needs to secure control area zones with a single network access policy to provision devices to any number of different networks.
On which device can this be accomplished?

A. FortiGate
B. FortiEDR
C. FortiSwitch
D. FortiNAC

Answer: D

NEW QUESTION 3
An OT administrator has configured FSSO and local firewall authentication. A user who is part of a user group is not prompted from credentials during authentication.
What is a possible reason?

A. FortiGate determined the user by passive authentication
B. The user was determined by Security Fabric
C. Two-factor authentication is not configured with RADIUS authentication method
D. FortiNAC determined the user by DHCP fingerprint method

Answer: D

NEW QUESTION 4
In a wireless network integration, how does FortiNAC obtain connecting MAC address information?

A. RADIUS
B. Link traps
C. End station traffic monitoring
D. MAC notification traps

Answer: A

NEW QUESTION 5
An administrator wants to use FortiSoC and SOAR features on a FortiAnalyzer device to detect and block any unauthorized access to FortiGate devices in an OT network.
Which two statements about FortiSoC and SOAR features on FortiAnalyzer are true? (Choose two.)

A. You must set correct operator in event handler to trigger an event.
B. You can automate SOC tasks through playbooks.
C. Each playbook can include multiple triggers.
D. You cannot use Windows and Linux hosts security events with FortiSoC.

Answer: BC

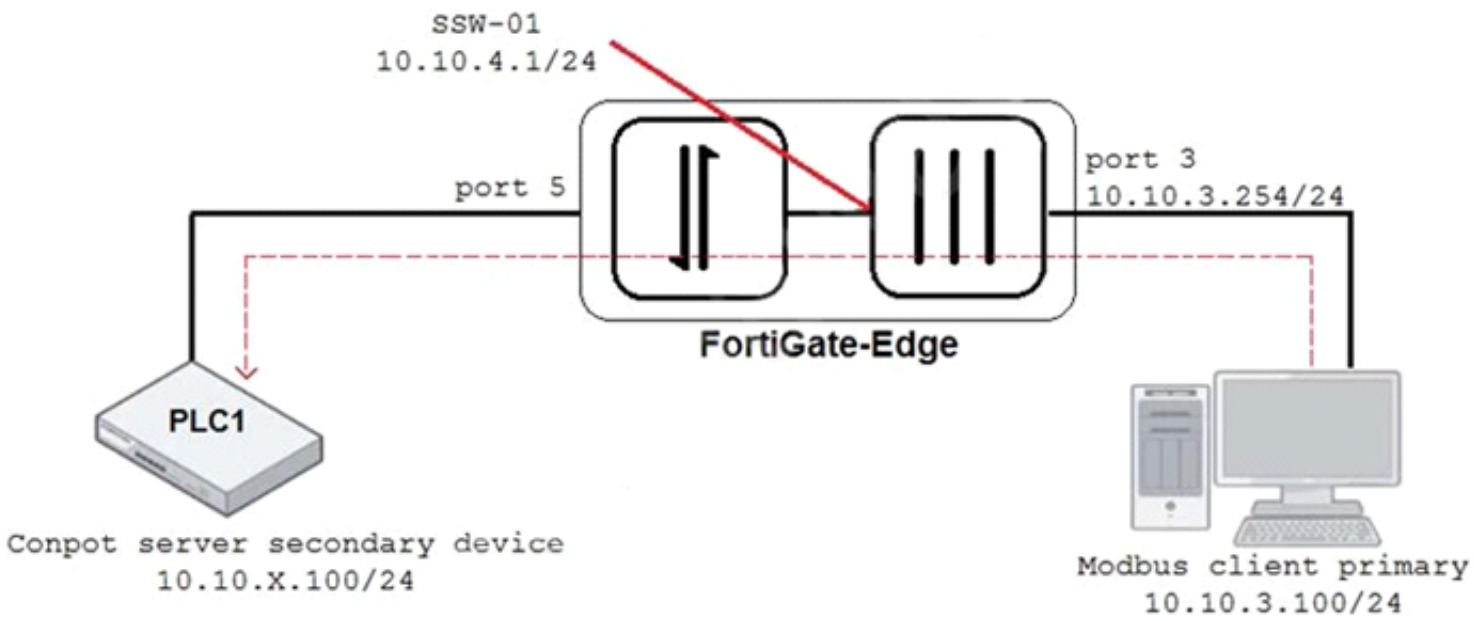
Explanation:
Ref: https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/268882/fortisoc

NEW QUESTION 6
What triggers Layer 2 polling of infrastructure devices connected in the network?

A. A failed Layer 3 poll
B. A matched security policy
C. A matched profiling rule
D. A linkup or linkdown trap

Answer: D

NEW QUESTION 7
Refer to the exhibit.

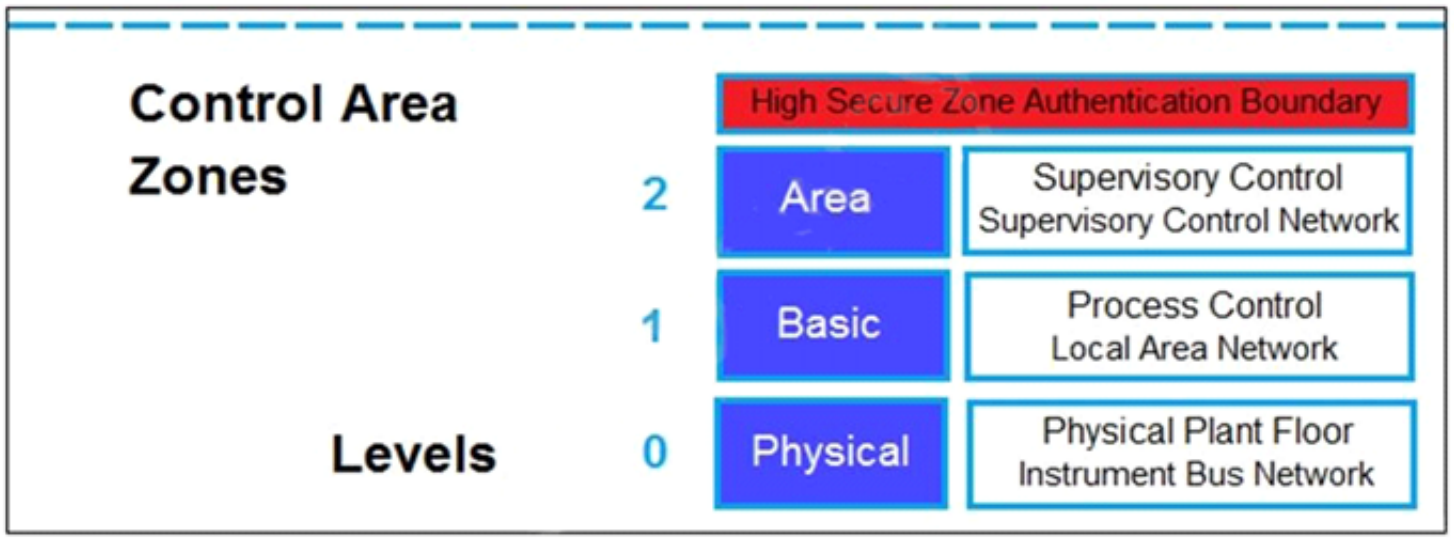


An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modus traffic in the OT network. The FortiGate-Edge device is configured with a software switch interface ssw-01.
Based on the topology shown in the exhibit, which two statements about the successful 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 8
Refer to the exhibit.

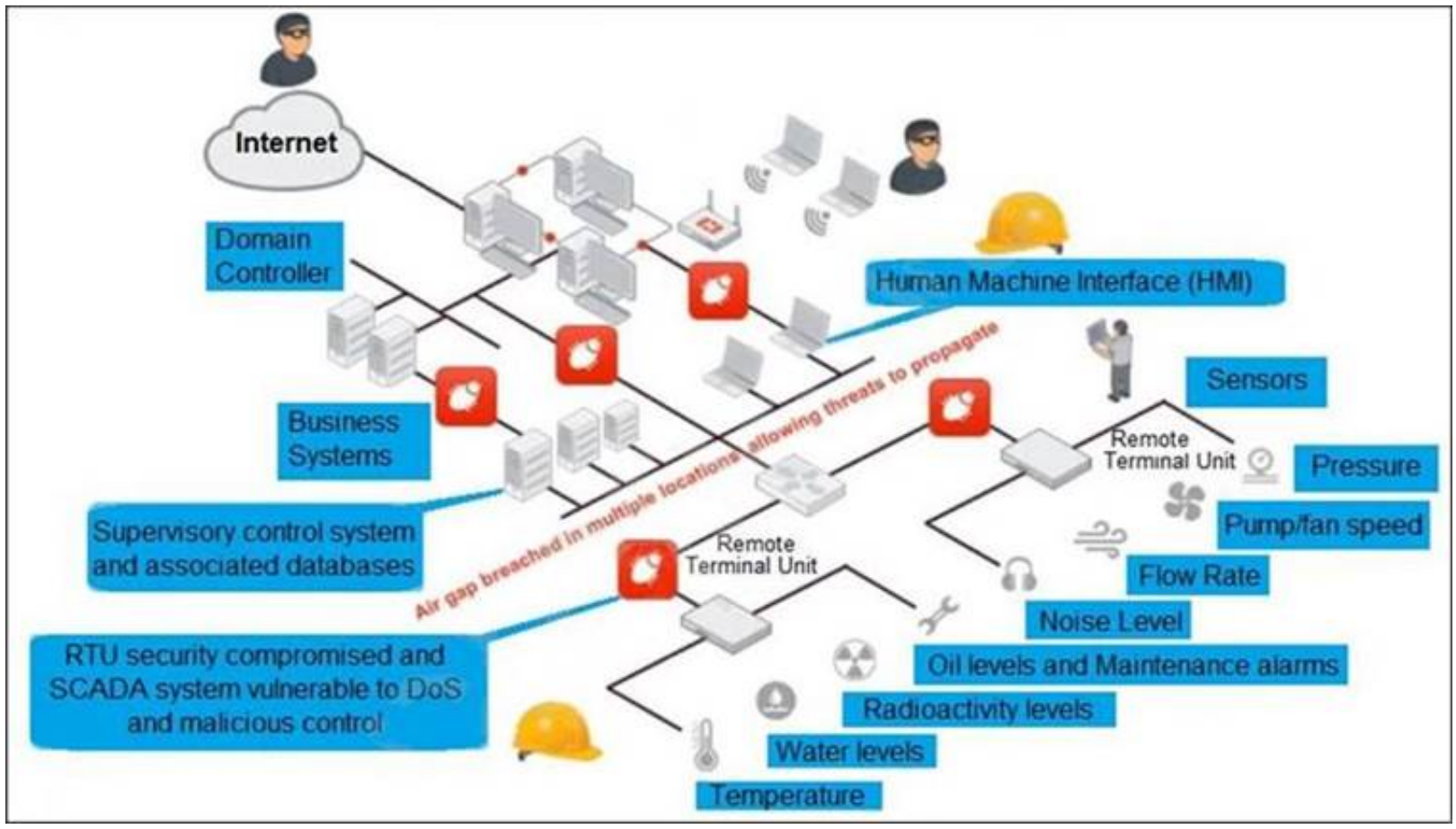


Based on the Purdue model, which three measures can be implemented in the control area zone using the Fortinet Security Fabric? (Choose three.)

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 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 10
Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Which statement about the interfaces shown in the exhibit is true?

A. port2, port2-vlan10, and port2-vlan1 are part of the software switch interface.
B. The VLAN ID of port1-vlan1 can be changed to the VLAN ID 10.
C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain

D. port1, port1-vlan10, and port1-vlan1 are in different broadcast domains

Answer: D

NEW QUESTION 11
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
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 17
What can be assigned using network access control policies?

A. Layer 3 polling intervals
B. FortiNAC device polling methods
C. Logical networks
D. Profiling rules

Answer: D

NEW QUESTION 19
Refer to the exhibit.

Maint	Device	Type	Organization	Avail Status	Perf Status	Security Status
●	FG240D3913800441	Fortinet FortiOS	Super	●	●	⊗
●	SJ-QA-F-Lnx-CHK	Checkpoint FireWall	Super	●	●	⚠
●	FAPS321C-default	Fortinet FortiAP	Super		●	●

You are navigating through FortiSIEM in an OT network.
How do you view information presented in the exhibit and what does the FortiGate device security status tell you?

A. In the PCI logging dashboard and there are one or more high-severity security incidents for the FortiGate device.
B. In the summary dashboard and there are one or more high-severity security incidents for the FortiGate device.
C. In the widget dashboard and there are one or more high-severity incidents for the FortiGate device.
D. In the business service dashboard and there are one or more high-severity security incidents for the FortiGate device.

Answer: B

NEW QUESTION 24
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 26
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

NSE7_OTS-6.4 Practice Exam Features:

* NSE7_OTS-6.4 Questions and Answers Updated Frequently

* NSE7_OTS-6.4 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_OTS-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_OTS-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year