

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

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 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

Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)

- A. SNMP
- B. ICMP
- C. API
- D. RADIUS
- E. TACACS

Answer: ACD

NEW QUESTION 6

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 7

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 8

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 9

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 10

Refer to the exhibit.

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

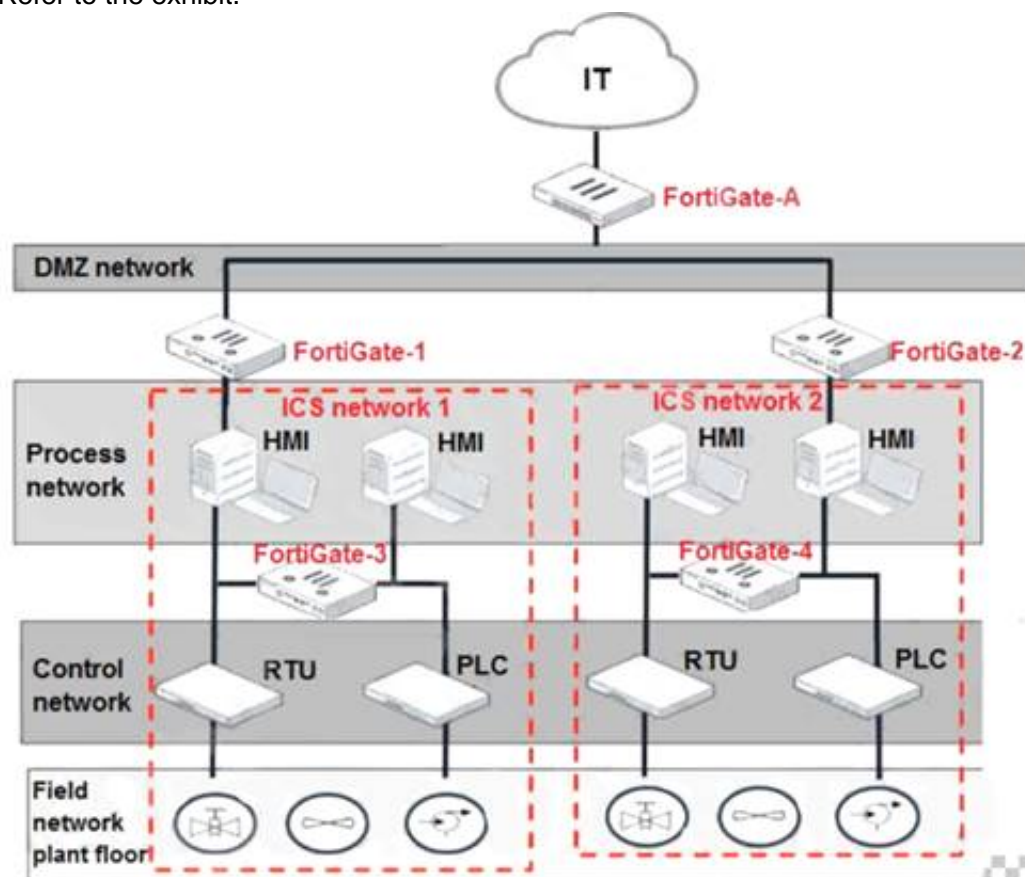
Given the configurations on the FortiGate, which statement is true?

- 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 10

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 15

Which three criteria can a FortiGate device use to look for a matching firewall policy to process traffic? (Choose three.)

- A. Services defined in the firewall policy.
- B. Source defined as internet services in the firewall policy
- C. Lowest to highest policy ID number
- D. Destination defined as internet services in the firewall policy
- E. Highest to lowest priority defined in the firewall policy

Answer: ABD

NEW QUESTION 19

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 20

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 23

.....

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_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

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_OTS-6.4 Practice Test Here](#)