

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 administrator has configured FSSO and local firewall authentication. A user who is part of a user group is not prompted for 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 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

When you create a user or host profile, which three criteria can you use? (Choose three.)

- A. Host or user group memberships
- B. Administrative group membership
- C. An existing access control policy
- D. Location
- E. Host or user attributes

Answer: ADE

NEW QUESTION 5

Refer to the exhibit.

Active Rules x Windows Installed Patches x Router/Switch Image Distribution x

BackExport

1/1

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 6

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 7

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 8

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 9

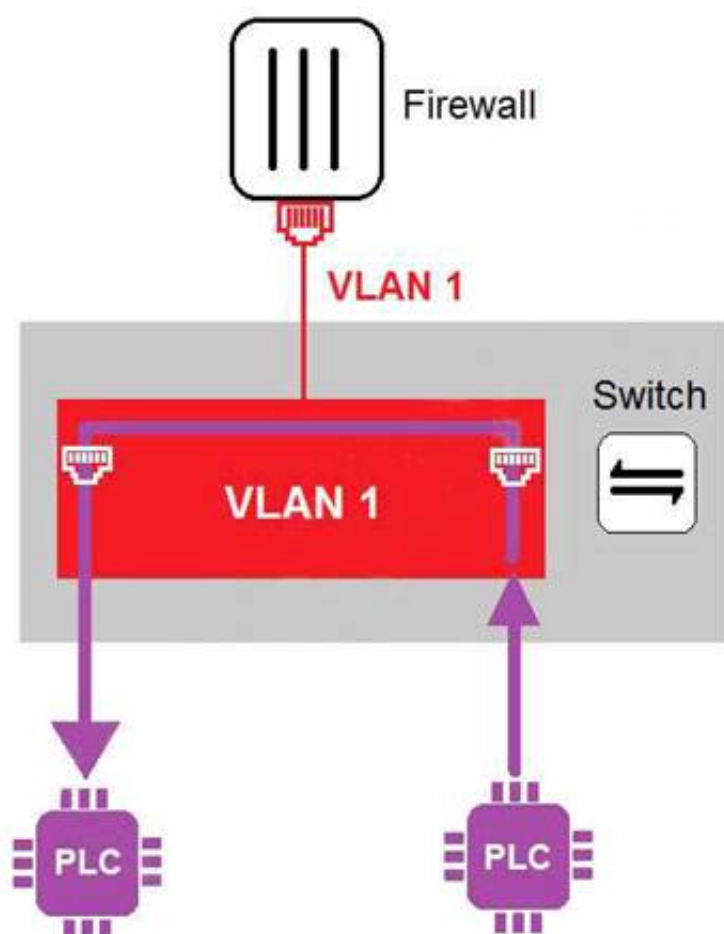
An OT network administrator is trying to implement active authentication. Which two methods should the administrator use to achieve this? (Choose two.)

- A. Two-factor authentication on FortiAuthenticator
- B. Role-based authentication on FortiNAC
- C. FSSO authentication on FortiGate
- D. Local authentication on FortiGate

Answer: AB

NEW QUESTION 10

Refer to the exhibit



In the topology shown in the exhibit, both PLCs can communicate directly with each other, without going through the firewall.

Which statement about the topology is true?

- A. PLCs use IEEE802.1Q protocol to communicate each other.
- B. An administrator can create firewall policies in the switch to secure between PLCs.
- C. This integration solution expands VLAN capabilities from Layer 2 to Layer 3.
- D. There is no micro-segmentation in this topology.

Answer: D

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 13

When device profiling rules are enabled, which devices connected on the network are evaluated by the device profiling rules?

- A. Known trusted devices, each time they change location
- B. All connected devices, each time they connect
- C. Rogue devices, only when they connect for the first time
- D. Rogue devices, each time they connect

Answer: C

NEW QUESTION 16

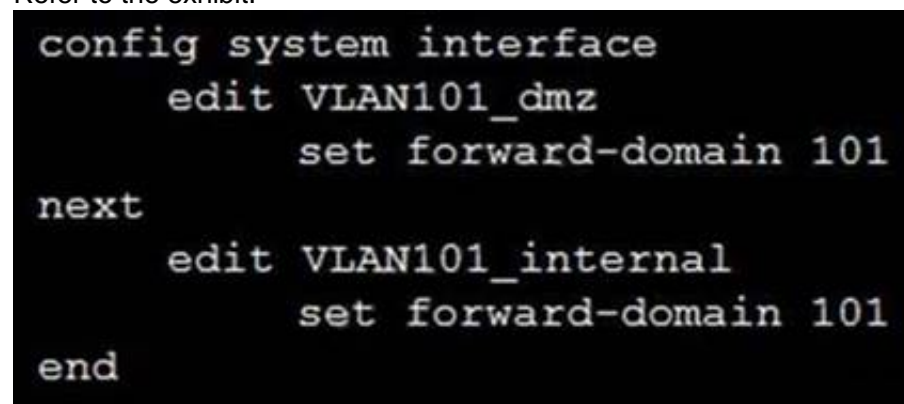
An OT administrator deployed many devices to secure the OT network. However, the SOC team is reporting that there are too many alerts, and that many of the alerts are false positive. The OT administrator would like to find a solution that eliminates repetitive tasks, improves efficiency, saves time, and saves resources. Which products should the administrator deploy to address these issues and automate most of the manual tasks done by the SOC team?

- A. FortiSIEM and FortiManager
- B. FortiSandbox and FortiSIEM
- C. FortiSOAR and FortiSIEM
- D. A syslog server and FortiSIEM

Answer: C

NEW QUESTION 17

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 20

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 21

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 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 29

.....

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](#)