Fortinet

Exam Questions NSE7_OTS-6.4

Fortinet NSE 7 - OT Security 6.4

NEW QUESTION 1
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 2
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 3
Refer to the exhibit.

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
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
Refer to the exhibit and analyze the output.

Which statement about the output is true?

A. This is a sample of a FortiAnalyzer system interface event log.
B. This is a sample of an SNMP temperature control event log.
C. This is a sample of a PAM event type.
D. This is a sample of FortiGate interface statistics.

Answer: A

NEW QUESTION 7
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 8
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 9
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 10
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 10
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 13
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 15
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 16
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 19
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 ofFortiSwitch 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 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
Refer to the exhibit.

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 security 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 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

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_OTS-6.4 Practice Test Here](https://www.surepassexam.com/NSE7_OTS-6.4-exam-dumps.html)