

## Exam Questions NSE7\_OT5-7.2

Fortinet NSE 7 - OT Security 7.2

[https://www.2passeasy.com/dumps/NSE7\\_OT5-7.2/](https://www.2passeasy.com/dumps/NSE7_OT5-7.2/)



**NEW QUESTION 1**

Refer to the exhibit.

Device Name	Device Type	Vendor	Device Type Model	Device Hardware Model	Device Image File	Count
SJ-QA-A-IOS-JunOffice	Cisco		IOS	1760	C1700-advsecurity9-mz.123-8.T4.bin	1
SJ-Main-Cat6500	Cisco		IOS	WS-C6509	s72033-advservicesk9_wan-mz.122-33.SX01.bin	1
ph-network-3560_1	Cisco		IOS	WS-C3560G-48PS-S	c3560-advservicesk9-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 2**

How can you achieve remote access and internet availability in an OT network?

- A. Create a back-end backup network as a redundancy measure.
- B. Implement SD-WAN to manage traffic on each ISP link.
- C. Add additional internal firewalls to access OT devices.
- D. Create more access policies to prevent unauthorized access.

**Answer:** B

**NEW QUESTION 3**

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:** AD

**Explanation:**

The two benefits of a Nozomi integration with FortiNAC are enhanced point of connection details and importation and classification of hosts. Enhanced point of connection details allows for the identification and separation of traffic from multiple points of connection, such as Wi-Fi, wired, cellular, and VPN. Importation and classification of hosts allows for the automated importing and classification of host and device information into FortiNAC. This allows for better visibility and control of the network.

**NEW QUESTION 4**

To increase security protection in an OT network, how does application control on FortiGate detect industrial traffic?

- A. By inspecting software and software-based vulnerabilities
- B. By inspecting applications only on nonprotected traffic
- C. By inspecting applications with more granularity by inspecting subapplication traffic
- D. By inspecting protocols used in the application traffic

**Answer:** B

**NEW QUESTION 5**

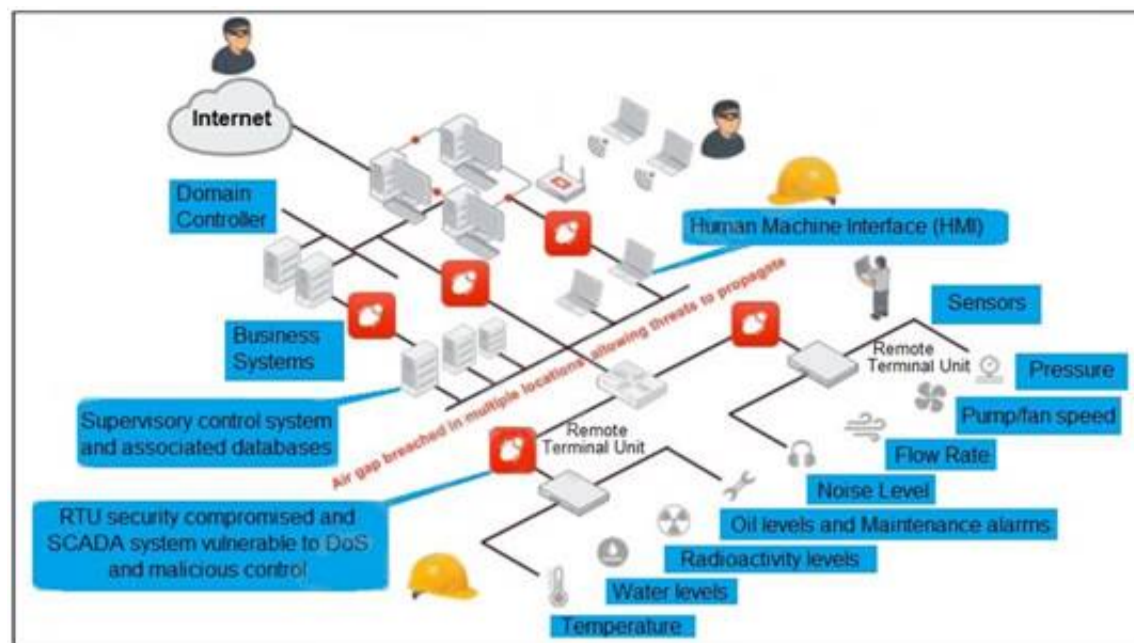
You are investigating a series of incidents that occurred in the OT network over past 24 hours in FortiSIEM. Which three FortiSIEM options can you use to investigate these incidents? (Choose three.)

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

**Answer:** CDE

**NEW QUESTION 6**

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 7**

The OT network analyst runs different level of reports to quickly explore threats that exploit the network. Such reports can be run on all routers, switches, and firewalls. Which FortiSIEM reporting method helps to identify these type of exploits of image firmware files?

- A. CMDB reports
- B. Threat hunting reports
- C. Compliance reports
- D. OT/IoT reports

**Answer:** B

**NEW QUESTION 8**

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:** AD

**NEW QUESTION 9**

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:** ADE

**Explanation:**

The three criteria that a FortiGate device can use to look for a matching firewall policy to process traffic are:

- \* A. Services defined in the firewall policy - FortiGate devices can match firewall policies based on the services defined in the policy, such as HTTP, FTP, or DNS.
- \* D. Destination defined as internet services in the firewall policy - FortiGate devices can also match firewall policies based on the destination of the traffic, including destination IP address, interface, or internet services.
- \* E. Highest to lowest priority defined in the firewall policy - FortiGate devices can prioritize firewall policies based on the priority defined in the policy. The device will process traffic against the policy with the highest priority first and move down the list until it finds a matching policy.

Reference:

Fortinet NSE 7 - Enterprise Firewall 6.4 Study Guide, Chapter 4: Policy Implementation, page 4-18.

**NEW QUESTION 10**

Which three common breach points can be found in a typical OT environment? (Choose three.)

- A. Global hat
- B. Hard hat
- C. VLAN exploits

- D. Black hat
- E. RTU exploits

**Answer:** BDE

#### NEW QUESTION 10

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:** AD

#### Explanation:

Typically, in a microsegmented network, NGFWs are used in conjunction with VLANs to implement security policies and to inspect and filter network communications. Fortinet FortiSwitch and FortiGate NGFW offer an integrated approach to microsegmentation.

#### NEW QUESTION 11

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 14

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 15

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7\_OTIS-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7\_OTIS-7.2 Product From:

[https://www.2passeasy.com/dumps/NSE7\\_OTIS-7.2/](https://www.2passeasy.com/dumps/NSE7_OTIS-7.2/)

## Money Back Guarantee

### **NSE7\_OTIS-7.2 Practice Exam Features:**

- \* NSE7\_OTIS-7.2 Questions and Answers Updated Frequently
- \* NSE7\_OTIS-7.2 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE7\_OTIS-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE7\_OTIS-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year