



# Fortinet

## Exam Questions NSE7\_OTS-7.2

Fortinet NSE 7 - OT Security 7.2

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

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:** BC

#### Explanation:

[https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/32cb817d-a307-11eb-b70b-00505692583a/FortiAnalyzer-7.0.0-Administration\\_Guide.pdf](https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/32cb817d-a307-11eb-b70b-00505692583a/FortiAnalyzer-7.0.0-Administration_Guide.pdf)

#### NEW QUESTION 2

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 3

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:** BCE

#### NEW QUESTION 4

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 5

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 6

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 7

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:** B

#### Explanation:

<https://fusecommunity.fortinet.com/blogs/silviu/2022/04/12/fortisiempublishingscript>

#### NEW QUESTION 8

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:** C

#### Explanation:

This way, FortiSIEM can discover and monitor everything attached to the remote network and provide security visibility to the corporate network

#### 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:** AD

#### NEW QUESTION 10

Refer to the exhibit.

Edit SubPattern

Name: industrial\_protocol\_monitor

Filters:

Paren	Attribute	Operator	Value
<div>+</div> <div>-</div>	Destination TCP/UDP Port	IN	Group: OT Ports
<div>+</div> <div>-</div>	Source TCP/UDP Port	IN	Group: OT Ports

Aggregate:

Paren	Attribute	Operator	Value
<div>+</div> <div>-</div>	COUNT( Matched Events )	>=	1

Group By:

Attribute	Row	Move
Reporting IP	<div>+</div> <div>-</div>	<div>↑</div> <div>↓</div>
Event Type	<div>+</div> <div>-</div>	<div>↑</div> <div>↓</div>
Destination TCP/UDP Port	<div>+</div> <div>-</div>	<div>↑</div> <div>↓</div>
Source TCP/UDP Port	<div>+</div> <div>-</div>	<div>↑</div> <div>↓</div>

An operational technology rule is created and successfully activated to monitor the Modbus protocol on FortiSIEM. However, the rule does not trigger incidents despite Modbus traffic and application logs being received correctly by FortiSIEM. Which statement correctly describes the issue on the rule configuration?

- A. The first condition on the SubPattern filter must use the OR logical operator.
- B. The attributes in the Group By section must match the ones in Filters section.
- C. The Aggregate attribute COUNT expression is incompatible with the filters.
- D. The SubPattern is missing the filter to match the Modbus protocol.

Answer: B

#### NEW QUESTION 10

Refer to the exhibit and analyze the output.

```
[PH_DEV_MON_NET_INTF_UTIL] : [eventSeverity] =PHL_INFO, [filename] =phPerfJob.cpp,
[lineNumber] =6646, [intfName]= Intel [R] PRO_100 MT Network
Connection, [intfAlias] =, [hostname] =WIN2K8DC, [hostIpAddr] = 192.168.69.6,
[pollIntv] =56, [recvBytes64] =
44273, [recvBitsPerSec] = 6324.714286, [inIntfUtil] = 0.000632, [sentBytes64] =
82014, [sentBitsPerSec] = 1171
6.285714, [outIntfUtil] = 0.001172, [recvPkts64] = 449, [sentPkts64] = 255,
[inIntfPktErr] = 0, [inIntfPktErrPct] = 0.000000, [outIntfPktErr] =0,
[outIntfPktErrPct] = 0.000000, [inIntfPktDiscarded] =0, [inIntfPktDiscardedPct] =
```

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: C

#### NEW QUESTION 11

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 16

As an OT network administrator, you are managing three FortiGate devices that each protect different levels on the Purdue model. To increase traffic visibility, you are required to implement additional security measures to detect exploits that affect PLCs.

Which security sensor must implement to detect these types of industrial exploits?

- A. Intrusion prevention system (IPS)
- B. Deep packet inspection (DPI)
- C. Antivirus inspection
- D. Application control

**Answer:** B

#### NEW QUESTION 20

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:** A

#### NEW QUESTION 25

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:** AB

#### Explanation:

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

#### NEW QUESTION 26

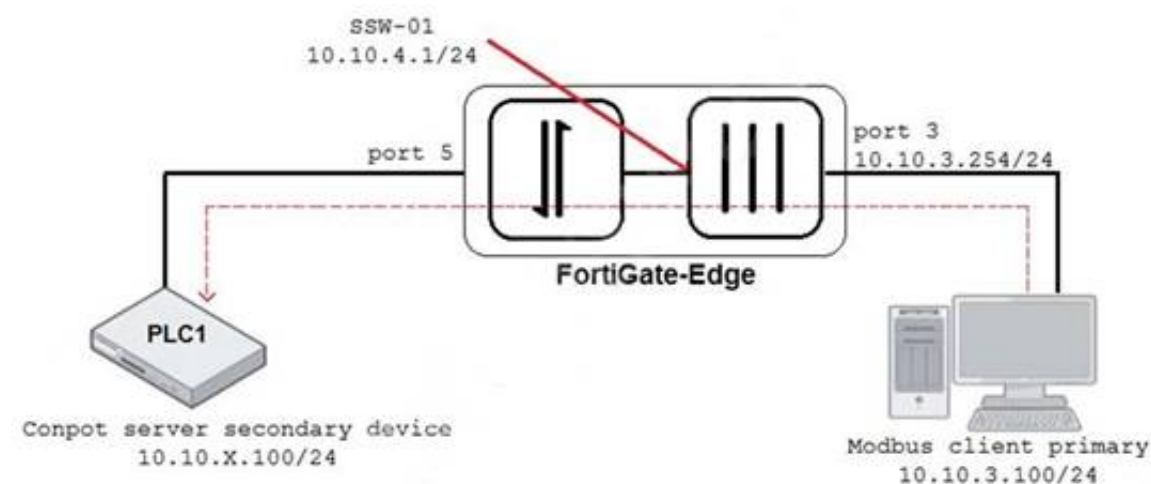
Which two statements are true when you deploy FortiGate as an offline IDS? (Choose two.)

- A. FortiGate receives traffic from configured port mirroring.
- B. Network traffic goes through FortiGate.
- C. FortiGate acts as network sensor.
- D. Network attacks can be detected and blocked.

**Answer:** BC

#### NEW QUESTION 30

Refer to the exhibit.



An OT architect has implemented a Modbus TCP with a simulation server Conpot to identify and control the Modbus 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 device is in offline IDS mode.
- D. Port5 is not a member of the software switch.

**Answer:** AB

#### NEW QUESTION 33

Refer to the exhibits.



Edit Policy

Name ⓘ

INBOUBD\_PLC-2

Incoming Interface

wan1

Outgoing Interface

Floor\_SSW

Source

all

+

Destination

PLC-2

+

Schedule

always

Service

ALL

+

Action

☒ ACCEPT

☐ DENY

Inspection Mode

Flow-based

Proxy-based

Firewall/Network Options

NAT

☒

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

☐

Protocol Options

PROT default

Security Profiles

AntiVirus

☐

Web Filter

☐

DNS Filter

☐

Application Control

☒ APP

lec\_104\_transfer\_sensor

IPS

☐

File Filter

☐

SSL Inspection

☐ certificate-inspection

Which statement is true about the traffic passing through to PLC-2?

- A. IPS must be enabled to inspect application signatures.
- B. The application filter overrides the default action of some IEC 104 signatures.
- C. IEC 104 signatures are all allowed except the C.BO.NA 1 signature.
- D. SSL Inspection must be set to deep-inspection to correctly apply application control.

Answer: B

NEW QUESTION 36

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 40

.....

## Relate Links

**100% Pass Your NSE7\_OTS-7.2 Exam with ExamBible Prep Materials**

[https://www.exambible.com/NSE7\\_OTS-7.2-exam/](https://www.exambible.com/NSE7_OTS-7.2-exam/)

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>