



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



NSE7_OTS-7.2 Dumps
NSE7_OTS-7.2 Braindumps
NSE7_OTS-7.2 Real Questions
NSE7_OTS-7.2 Practice Test
NSE7_OTS-7.2 Actual Questions



Fortinet

NSE7_OTS-7.2

Trustworthy for Fortinet Certified Solution Specialist (FCSS)



Question: 137

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: A,D

Question: 138

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 FortiSIE
- C. Define a script/remediation on FortiManager and enable a notification rule on FortiSIE
- D. Deploy a mitigation script on Active Directory and create a notification policy on FortiSIE

Answer: B

Explanation:

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/06918379-afd1-11e9-a989-00505692583a/Standalone_PDF.pdf

Question: 139

An OT supervisor has configured LDAP and FSSO for the authentication. The goal is that all the users be authenticated against passive authentication first and, if passive authentication is not successful, then users should be challenged with active authentication.

What should the OT supervisor do to achieve this on FortiGate?

- A. Configure a firewall policy with LDAP users and place it on the top of list of firewall policies.
- B. Enable two-factor authentication with FSS
- C. Configure a firewall policy with FSSO users and place it on the top of list of firewall policies.
- D. Under config user settings configure set auth-on-demand implicit.

Answer: C

Question: 140

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: A,D,E

Question: 141

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

Question: 142

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 CL

Answer: D

Question: 143

Refer to the exhibit.

Maint	Device	Type	Organization	Avail Status	Perf Status	Security Status
●	FG240D3913800441	Fortinet FortiOS	Super	●	●	✖
●	SJ-QA-F-Lnx-CHK	Checkpoint FireWall	Super	●	●	⚠
●	FAPS321C-default	Fortinet FortiAP	Super		●	●

You are navigating through FortiSIEM in an OT network.

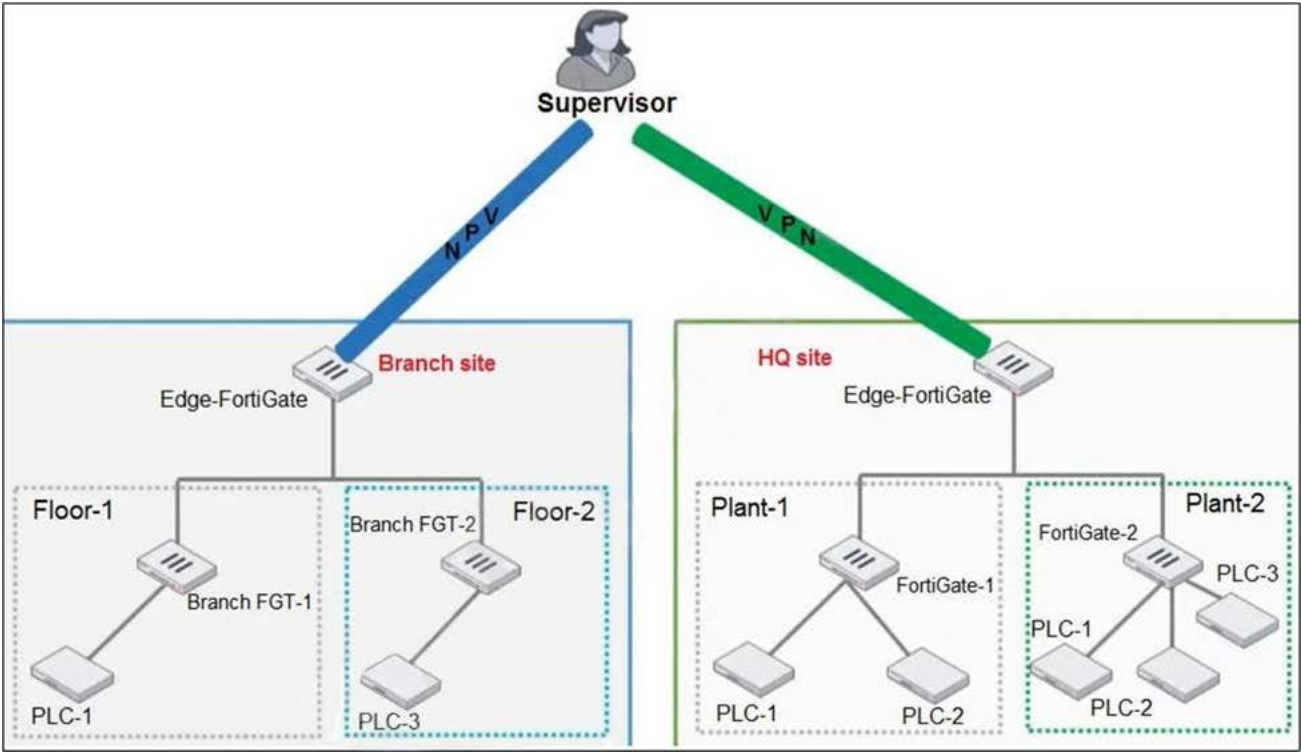
How do you view information presented in the exhibit and what does the FortiGate device security status tell you?

- 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 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

Question: 144

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

Question: 145

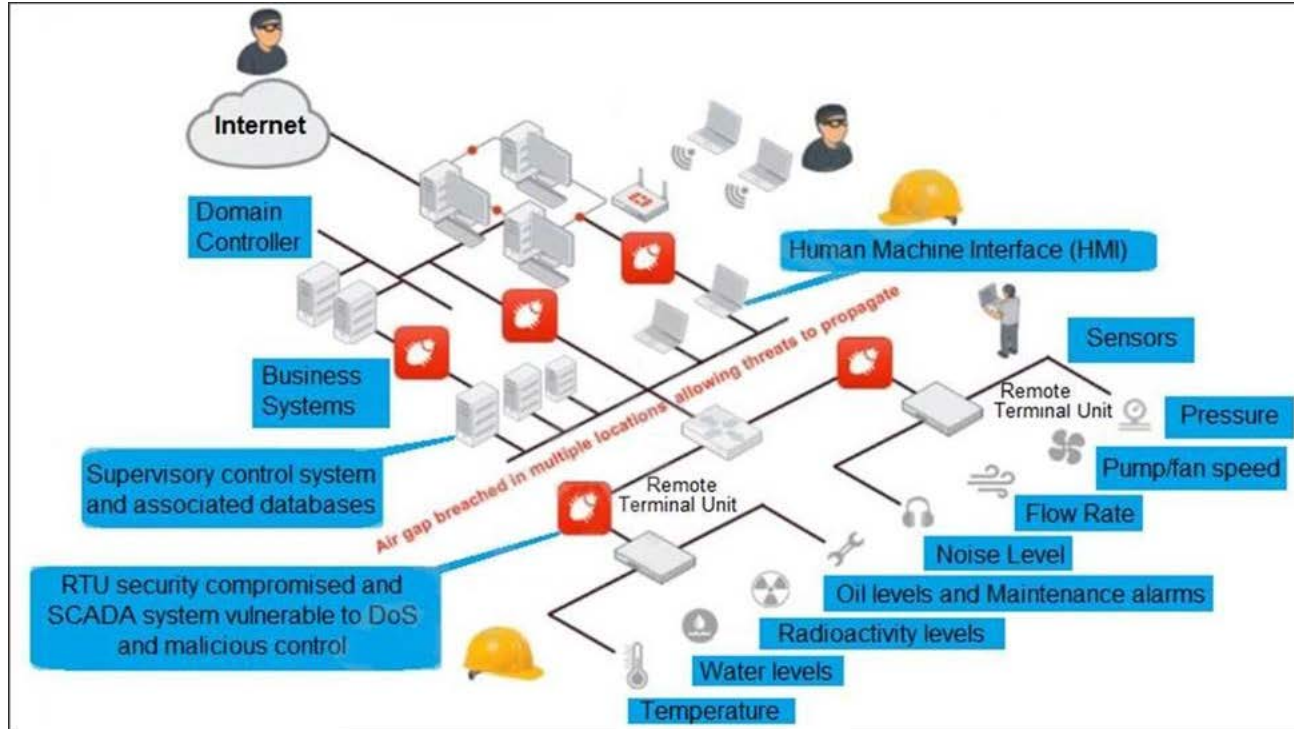
What are two benefits of a Nozomi integration with FortiNAC? (Choose two.)

- A. Enhanced point of connection details
- B. Direct VLAN assignment
- C. Adapter consolidation for multi-adapter hosts
- D. Importation and classification of hosts

Answer: A,C,D

Question: 146

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: A,B,D,E

Question: 147

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.

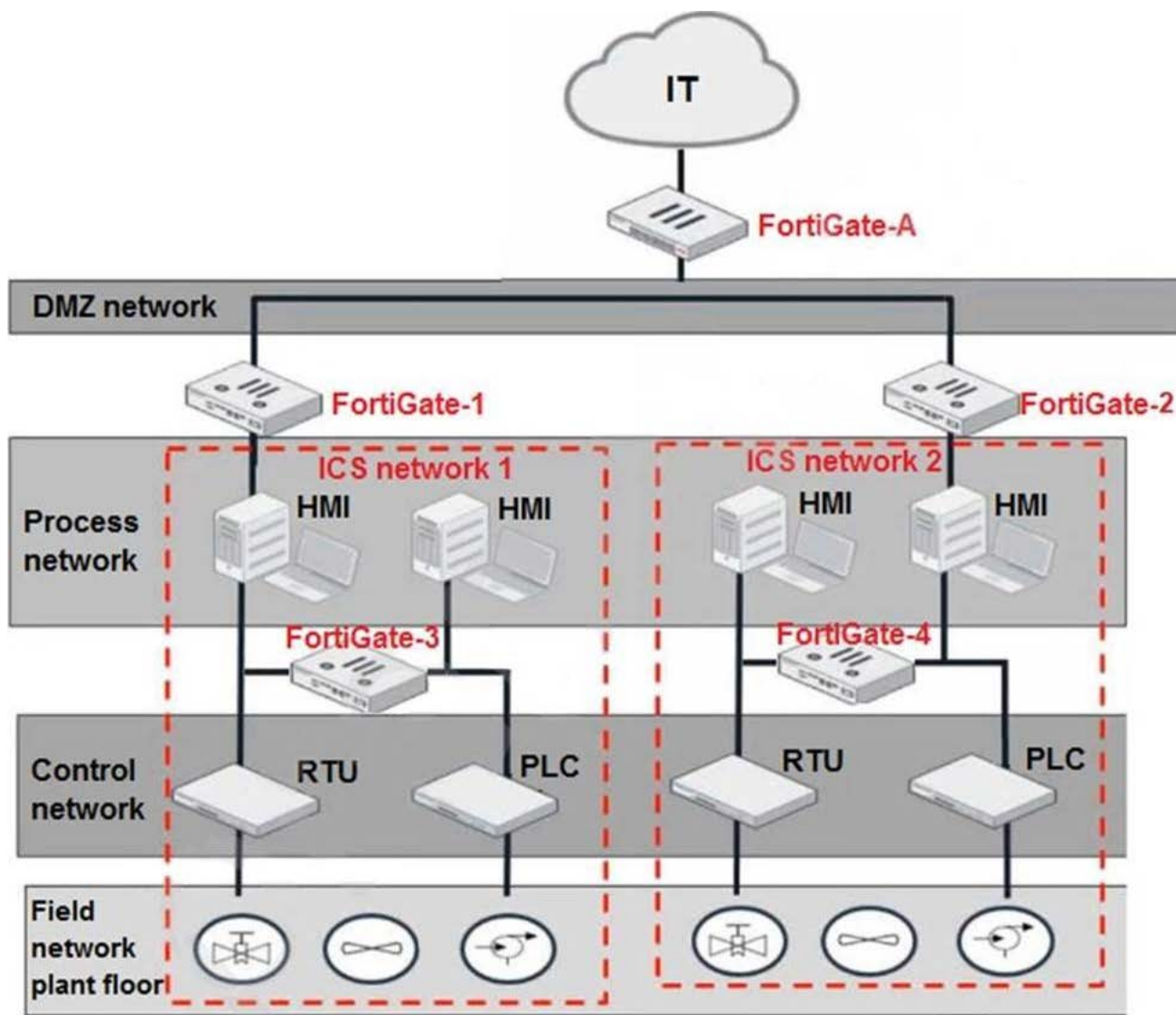
What is a possible reason?

- 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: A

Question: 148

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: A,C

Question: 149

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 FortiSo

Answer: A,B

Explanation:

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

Question: 150

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: A,B,C

Question: 151

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



SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps: *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests: *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success: *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support: *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>
Kill your exam at First Attempt....Guaranteed!