

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

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

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 FSSO.
- 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: D

NEW QUESTION 5

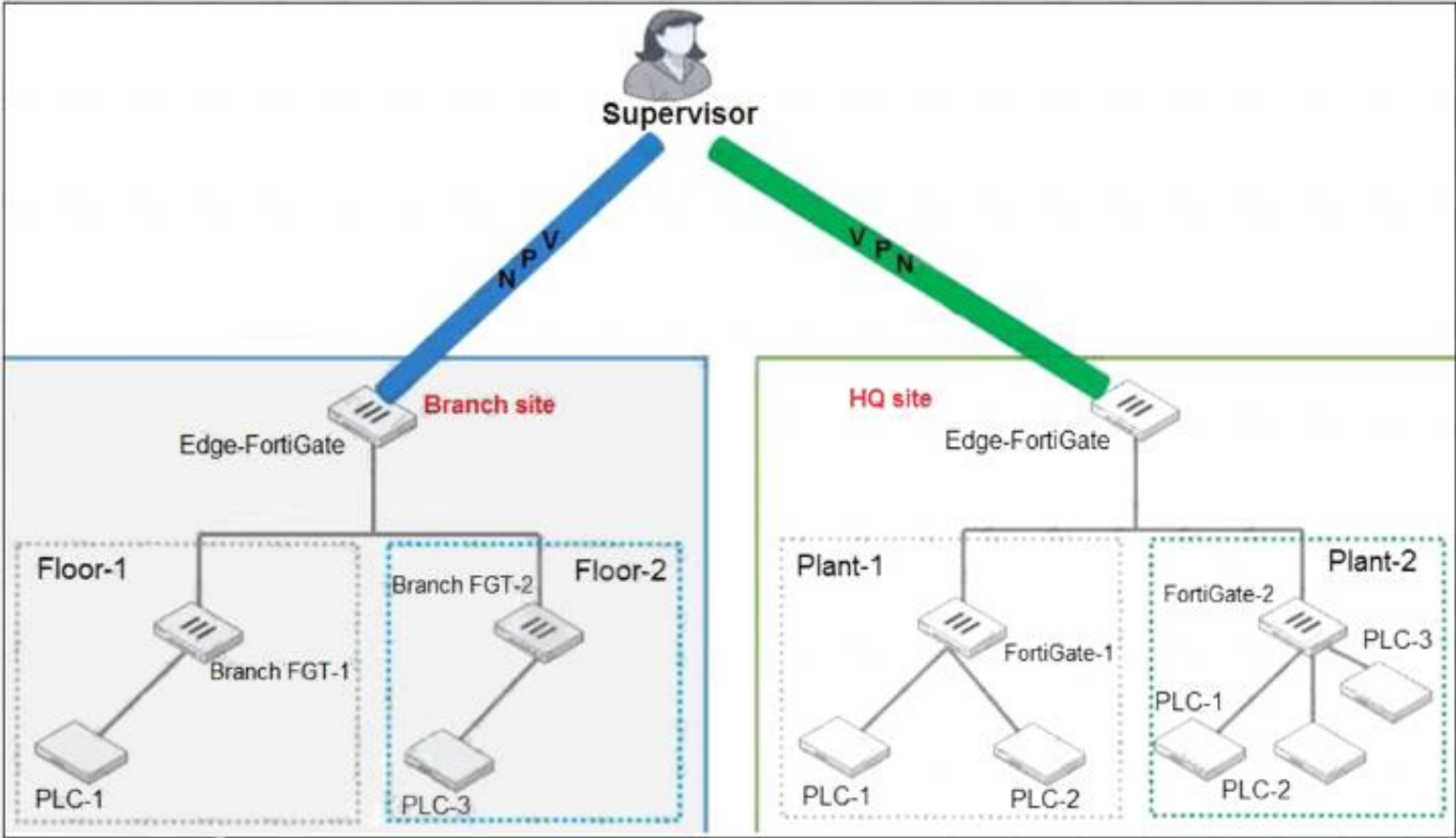
Which three Fortinet products can be used for device identification in an OT industrial control system (ICS)? (Choose three.)

- A. FortiNAC
- B. FortiManager
- C. FortiAnalyzer
- D. FortiSIEM
- E. FortiGate

Answer: ACD

NEW QUESTION 6

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 7

Refer to the exhibit.



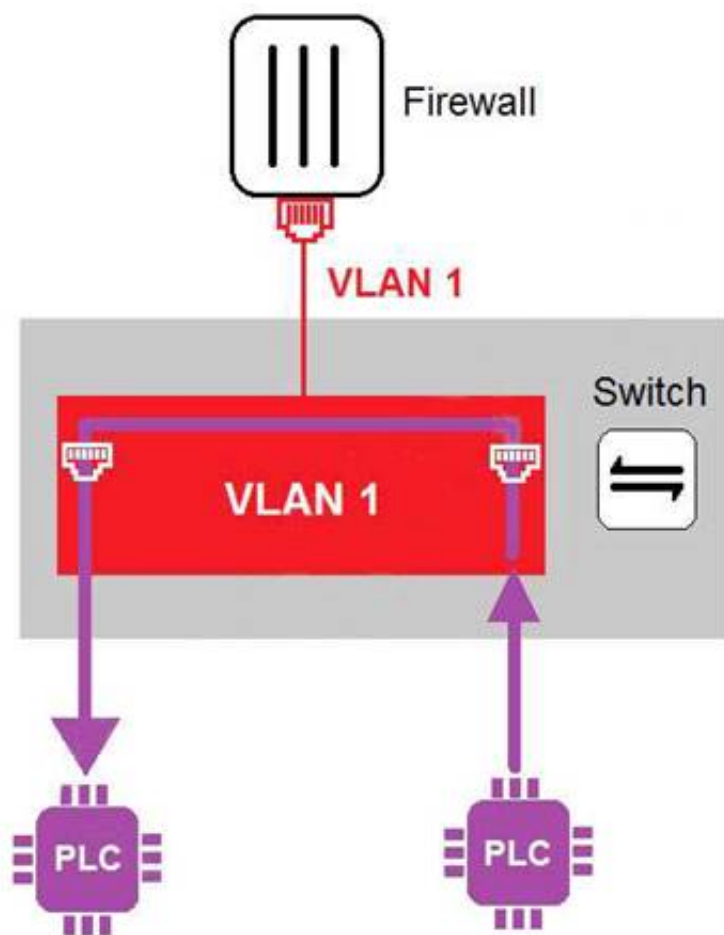
Based on the Purdue model, which three measures can be implemented in the control area zone using the Fortinet Security Fabric? (Choose three.)

- 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: BCD

NEW QUESTION 8

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 9

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 10

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: C

NEW QUESTION 10

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 12

Refer to the exhibit.

```
config system interface
    edit VLAN101_dmz
        set forward-domain 101
    next
    edit VLAN101_internal
        set forward-domain 101
    end
```

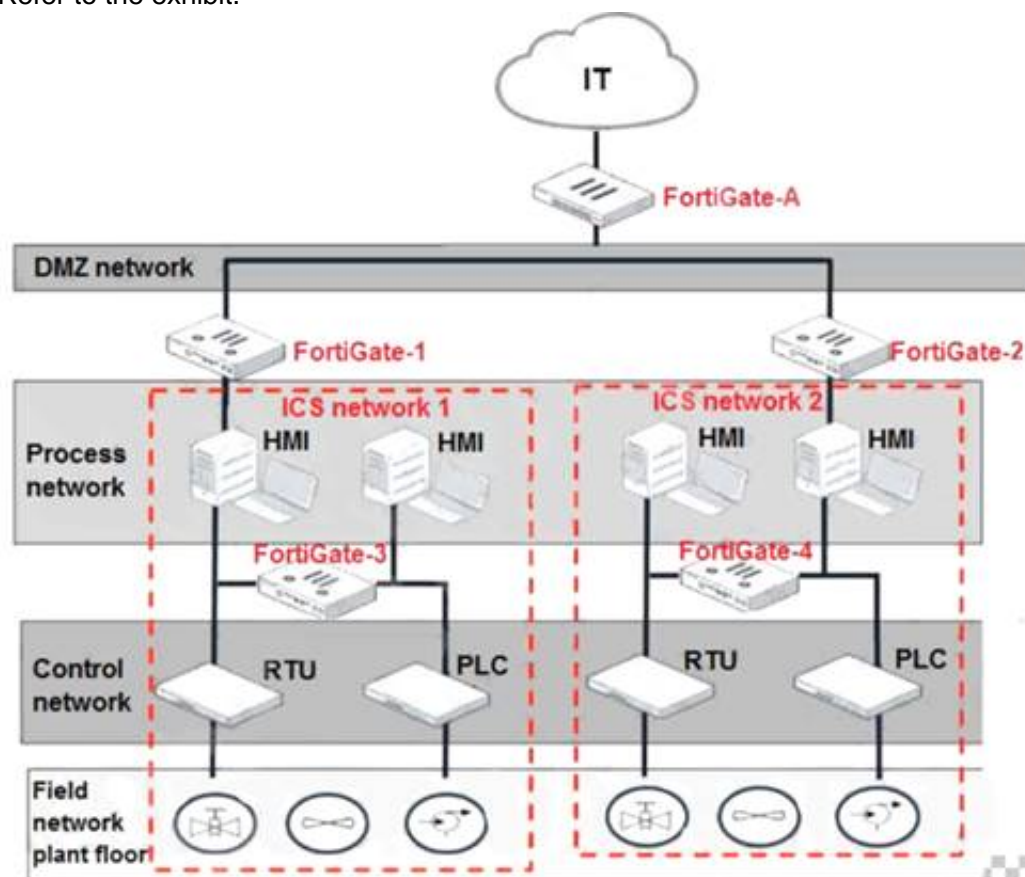
Given the configurations on the FortiGate, which statement is true?

- 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 13

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: CD

NEW QUESTION 18

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: ABD

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 28

.....

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](#)