Number: NSE7_OTS-7.2
Passing Score: 800
Time Limit: 120
File Version: 2.0

Exam Code: NSE7_OTS-7.2

Exam Name: Fortinet NSE 7 - OT Security 7.2

Exam A

QUESTION 1
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

Correct Answer: A
Section:

QUESTION 2
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.

Correct Answer: A
Section:

QUESTION 3
To increase security protection in an OT network, how does application control on ForliGate 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

Correct Answer: B

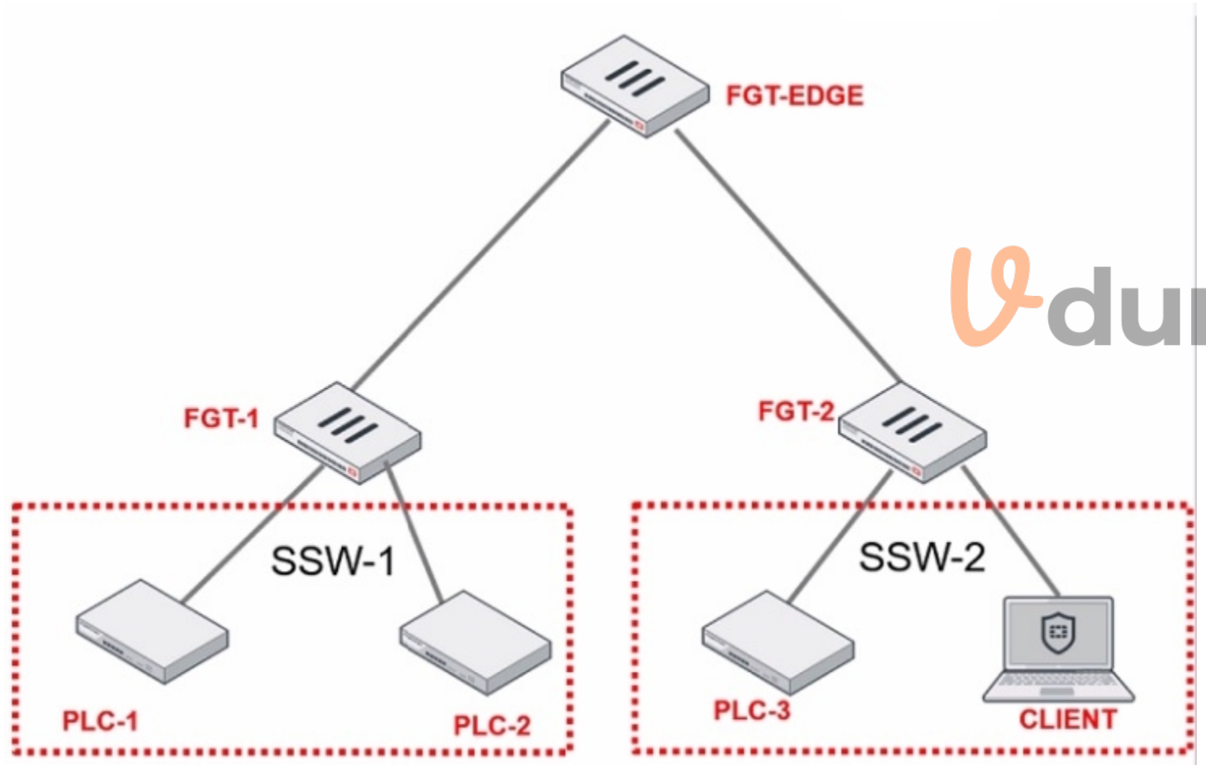
Section:

QUESTION 4
What are two critical tasks the OT network auditors must perform during OT network risk assessment and management? (Choose two.)

A. Planning a threat hunting strategy
B. Implementing strategies to automatically bring PLCs offline
C. Creating disaster recovery plans to switch operations to a backup plant
D. Evaluating what can go wrong before it happens

Correct Answer: A, C
Section:

QUESTION 5
Refer to the exhibit.



PLC-3 and CLIENT can send traffic to PLC-1 and PLC-2. FGT-2 has only one software switch (SSW-1) connecting both PLC-3 and CLIENT. PLC-3 and CLIENT cannot send traffic to each other.
Which two statements about the traffic between PCL-1 and PLC-2 are true? (Choose two.)

A. The switch on FGT-2 must be hardware to implement micro-segmentation.
B. Micro-segmentation on FGT-2 prevents direct device-to-device communication.
C. Traffic must be inspected by FGT-EDGE in OT networks.
D. FGT-2 controls intra-VLAN traffic through firewall policies.

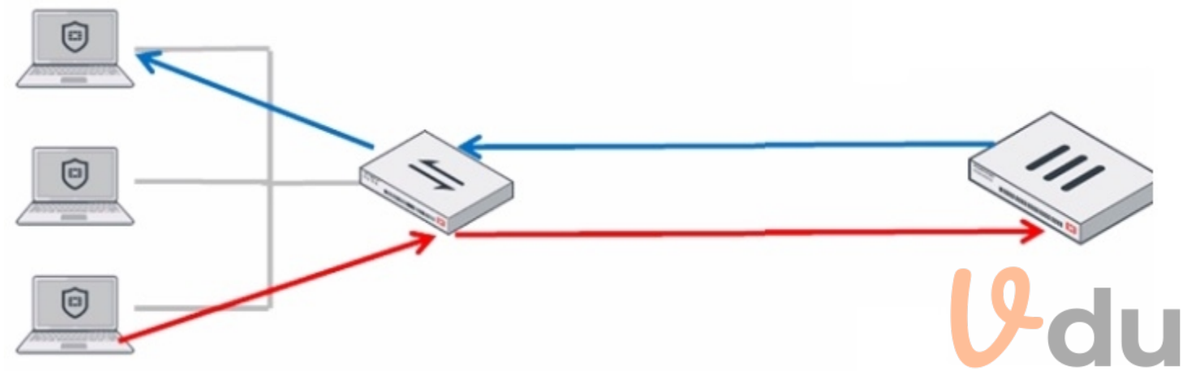
Correct Answer: B, D
Section:

QUESTION 6
Which three Fortinet products can you use for device identification in an OT industrial control system (ICS)? (Choose three.)

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

Correct Answer: A, D, E
Section:

QUESTION 7
Refer to the exhibit.



In order for a FortiGate device to act as router on a stick, what configuration must an OT network architect implement on FortiGate to achieve inter-VLAN routing?

A. Set a unique forward domain on each interface on the network.
B. Set FortiGate to operate in transparent mode.
C. Set a software switch on FortiGate to handle inter-VLAN traffic.
D. Set a FortiGate interface with the switch to operate as an 802.1 q trunk.

Correct Answer: D
Section:

QUESTION 8
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.

Correct Answer: A, B

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

QUESTION 9
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

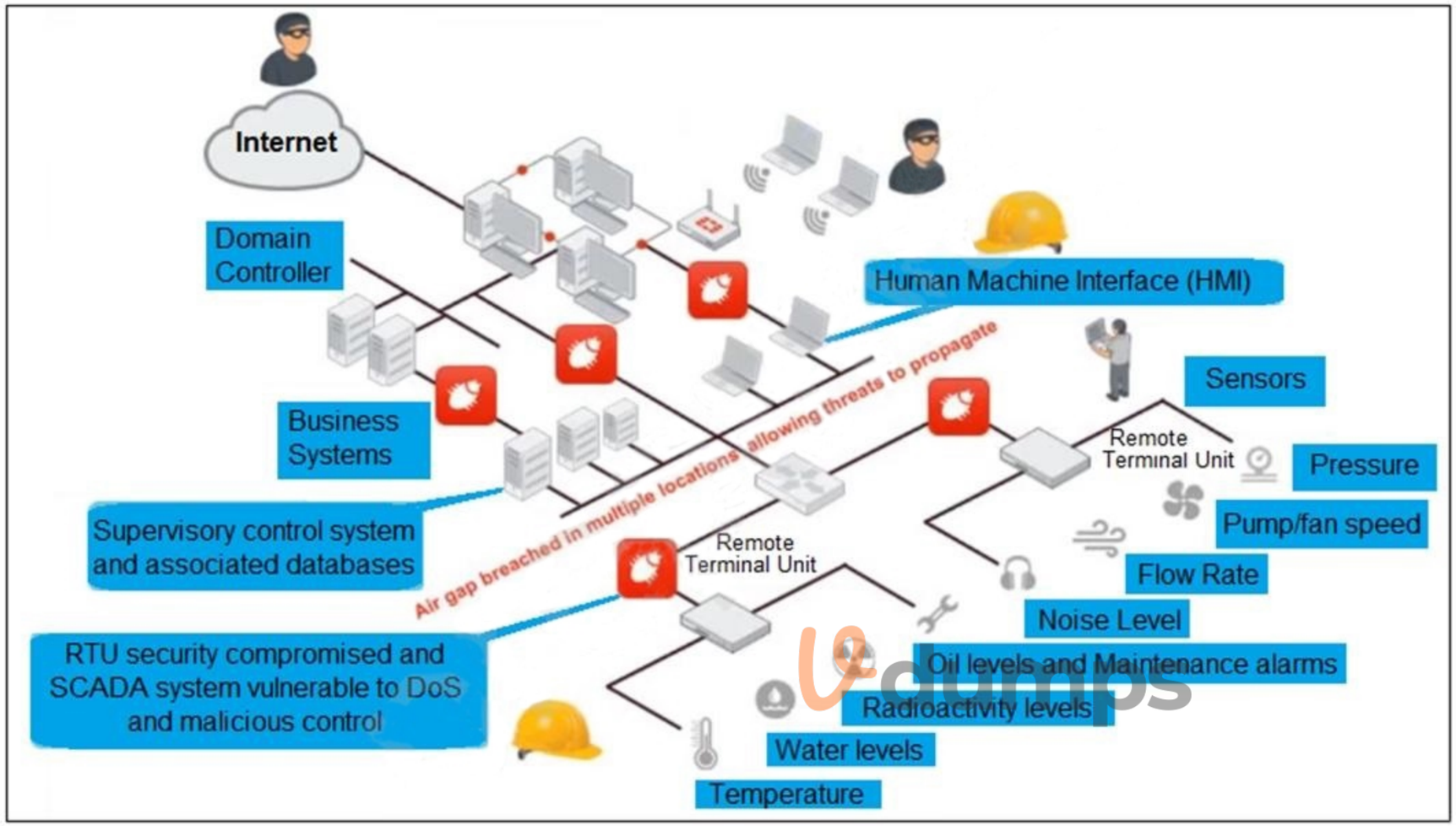
Correct Answer: C, D, E
Section:

QUESTION 10
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

Correct Answer: A, D, E
Section:
Explanation:
https://docs.fortinet.com/document/fortinac/9.2.0/administration-guide/15797/user-host-profiles

QUESTION 11
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

Correct Answer: A, C, D
Section:

QUESTION 12
Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Which statement about the interfaces shown in the exhibit is true?

A. port2, port2-vlan10, and port2-vlan1 are part of the software switch interface.
B. The VLAN ID of port1-vlan1 can be changed to the VLAN ID 10.
C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain
D. port1, port1-vlan10, and port1-vlan1 are in different broadcast domains

Correct Answer: D
Section:

QUESTION 13
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

Correct Answer: C
Section:

QUESTION 14
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.

Correct Answer: A, D
Section:
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.

QUESTION 15
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

Correct Answer: D
Section:

QUESTION 16
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.

Correct Answer: B, C
Section:
Explanation:
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/32cb817d-a307-11eb-b70b-00505692583a/FortiAnalyzer-7.0.0-Administration_Guide.pdf

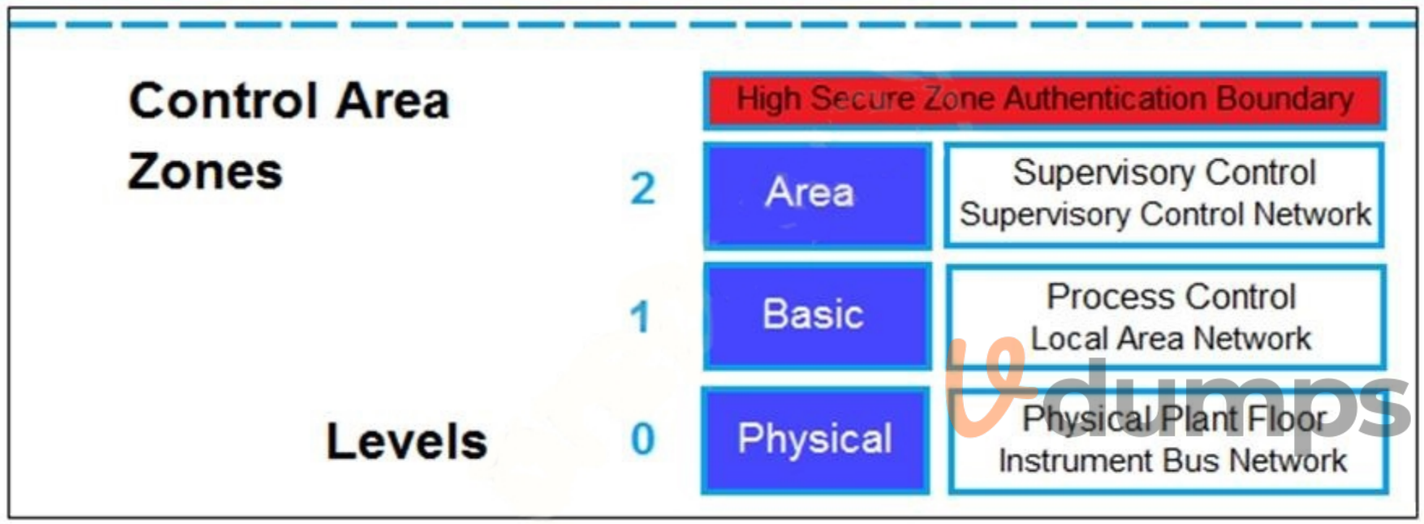
QUESTION 17
An OT supervisor needs to protect their network by implementing security with an industrial signature database on the FortiGate device.

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 CLI.

Correct Answer: D
Section:

QUESTION 18
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

Correct Answer: B, C, E
Section:

QUESTION 19
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

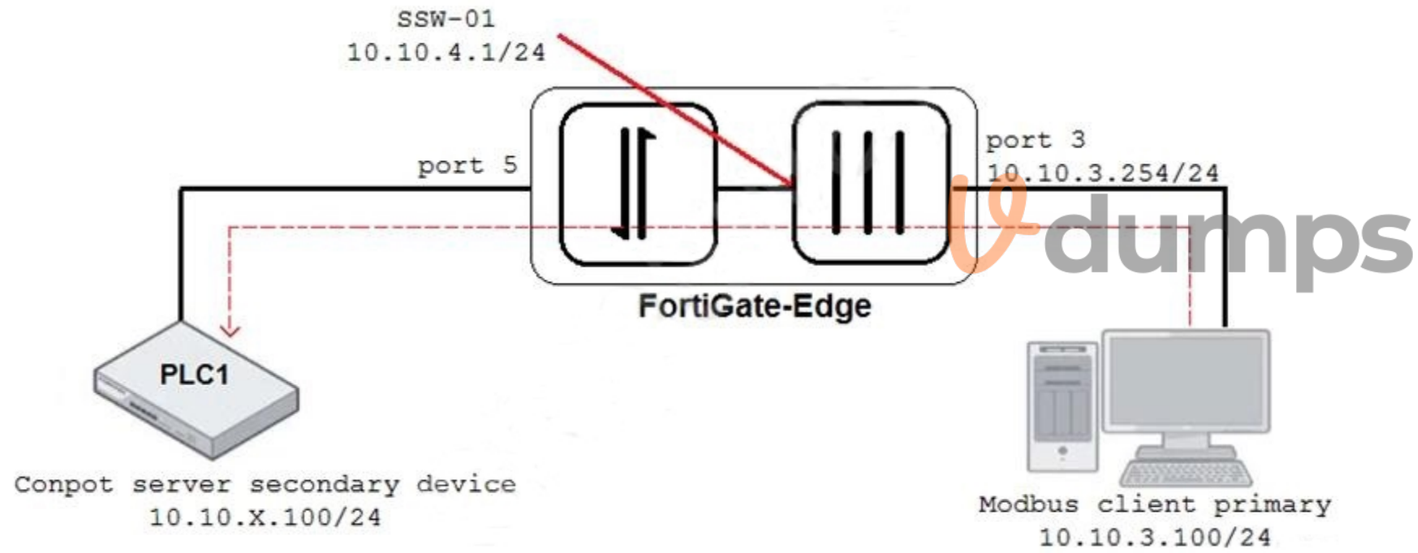
Correct Answer: C
Section:

QUESTION 20
As an OT administrator, it is important to understand how industrial protocols work in an OT network.
Which communication method is used by the Modbus protocol?

A. It uses OSI Layer 2 and the primary device sends data based on request from secondary device.
B. It uses OSI Layer 2 and both the primary/secondary devices always send data during the communication.
C. It uses OSI Layer 2 and both the primary/secondary devices send data based on a matching token ring.
D. It uses OSI Layer 2 and the secondary device sends data based on request from primary device.

Correct Answer: D
Section:

QUESTION 21
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.

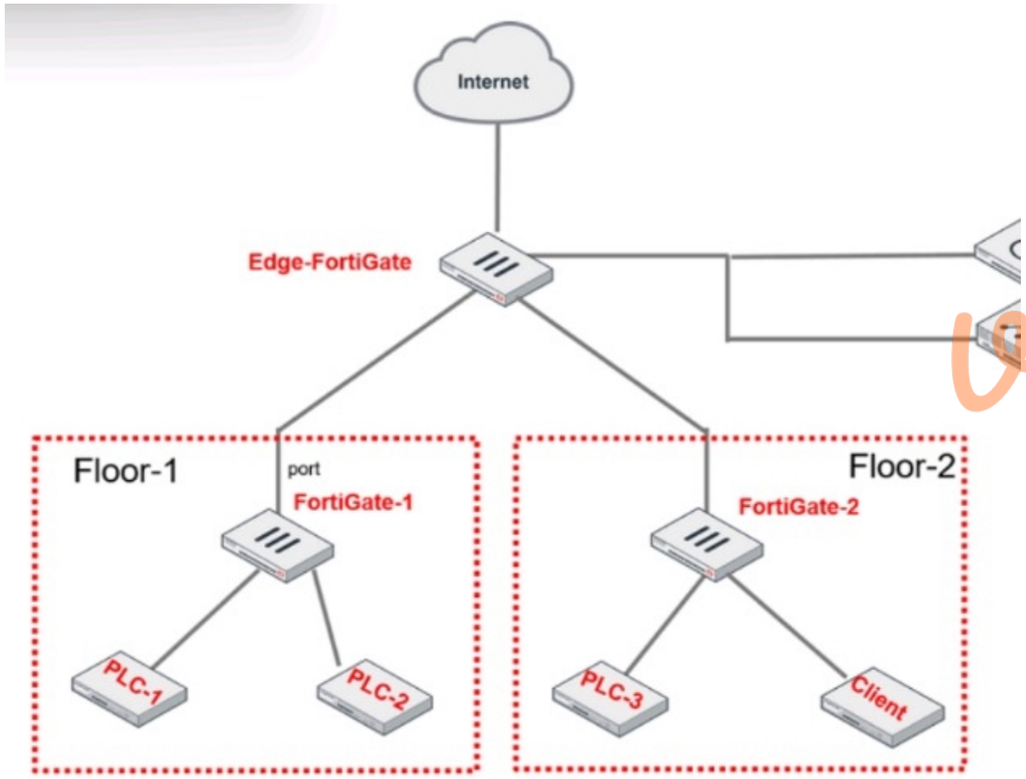
Correct Answer: A, B
Section:

QUESTION 22
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.

Correct Answer: C
Section:
Explanation:
This way, FortiSIEM can discover and monitor everything attached to the remote network and provide security visibility to the corporate network

QUESTION 23
Refer to the exhibit.



PLC-3 and CLIENT can send traffic to PLC-1 and PLC-2. FGT-2 has only one software switch (SSW-1) connecting both PLC-3 and CLIENT. PLC-3 and CLIENT can send traffic to each other at the Layer 2 level.
What must the OT admin do to prevent Layer 2-level communication between PLC-3 and CLIENT?

A. Set a unique forward domain for each interface of the software switch.
B. Create a VLAN for each device and replace the current FGT-2 software switch members.
C. Enable explicit intra-switch policy to require firewall policies on FGT-2.
D. Implement policy routes on FGT-2 to control traffic between devices.

Correct Answer: A, B
Section:

QUESTION 24
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

Correct Answer: D
Section:

QUESTION 25
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.

Correct Answer: B, C
Section:

QUESTION 26
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.

Correct Answer: B
Section:

QUESTION 27
Which type of attack posed by skilled and malicious users of security level 4 (SL 4) of IEC 62443 is designed to defend against intentional attacks?

A. Users with access to moderate resources
B. Users with low access to resources
C. Users with unintentional operator error
D. Users with substantial resources

Correct Answer: C
Section:

QUESTION 28

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/loT reports

Correct Answer: B
Section:

QUESTION 29
The OT network analyst run different level of reports to quickly explore failures that could put the network at risk. Such reports can be about device performance. Which FortiSIEM reporting method helps to identify device failures?

A. Business service reports
B. Device inventory reports
C. CMDB operational reports
D. Active dependent rules reports

Correct Answer: C
Section:

QUESTION 30
Which statemenl about the IEC 104 protocol is true?

A. IEC 104 is used for telecontrol SCADA in electrical engineering applications.
B. IEC 104 is IEC 101 compliant in old SCADA systems.
C. IEC 104 protects data transmission between OT devices and services.
D. IEC 104 uses non-TCP/IP standards.

Correct Answer: A
Section: