Fortinet

Exam Questions NSE7_OTS-7.2

Fortinet NSE 7 - OT Security 7.2

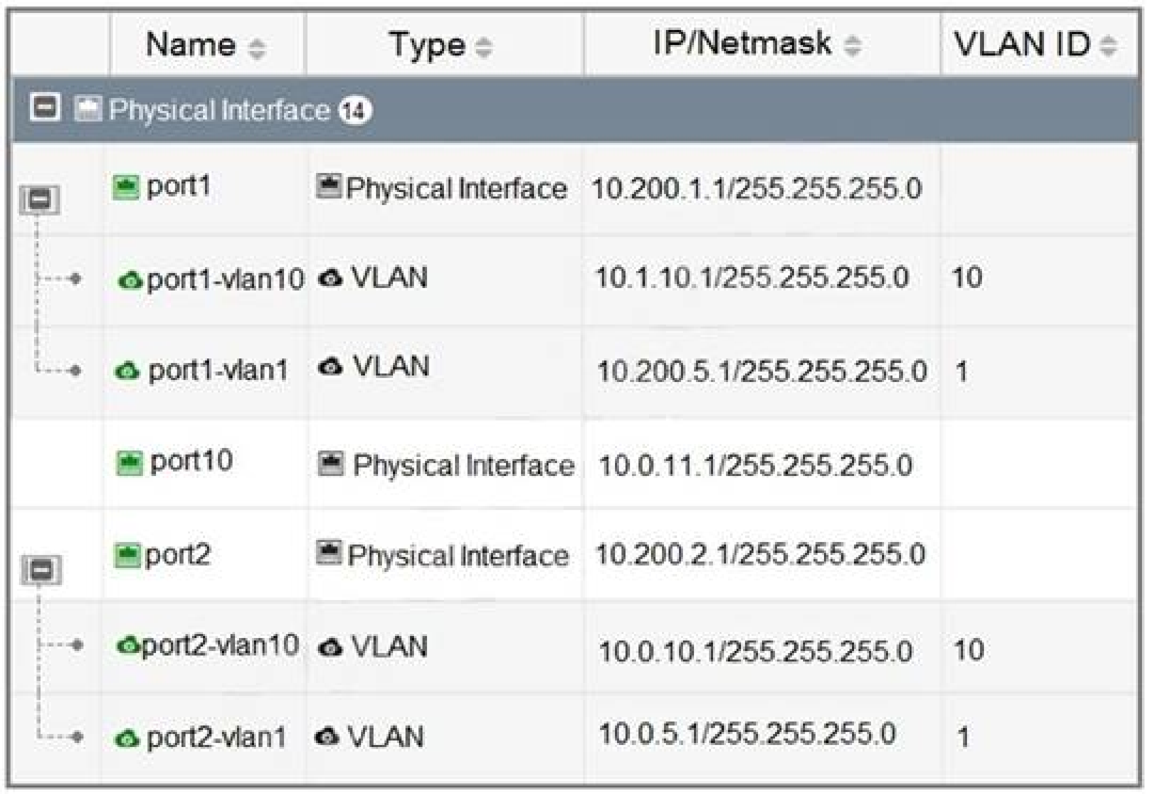
NEW QUESTION 1
An OT administrator configured and ran a default application risk and control report in FortiAnalyzer to learn more about the key application crossing the network. However, the report output is empty despite the fact that some related real-time and historical logs are visible in the FortiAnalyzer.
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

NEW QUESTION 2
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

Answer: D

NEW QUESTION 3
Which three methods of communication are used by FortiNAC to gather visibility information? (Choose three.)

A. SNMP
B. ICMP
C. API
D. RADIUS
E. TACACS

Answer: ACD

NEW QUESTION 4
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 5
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

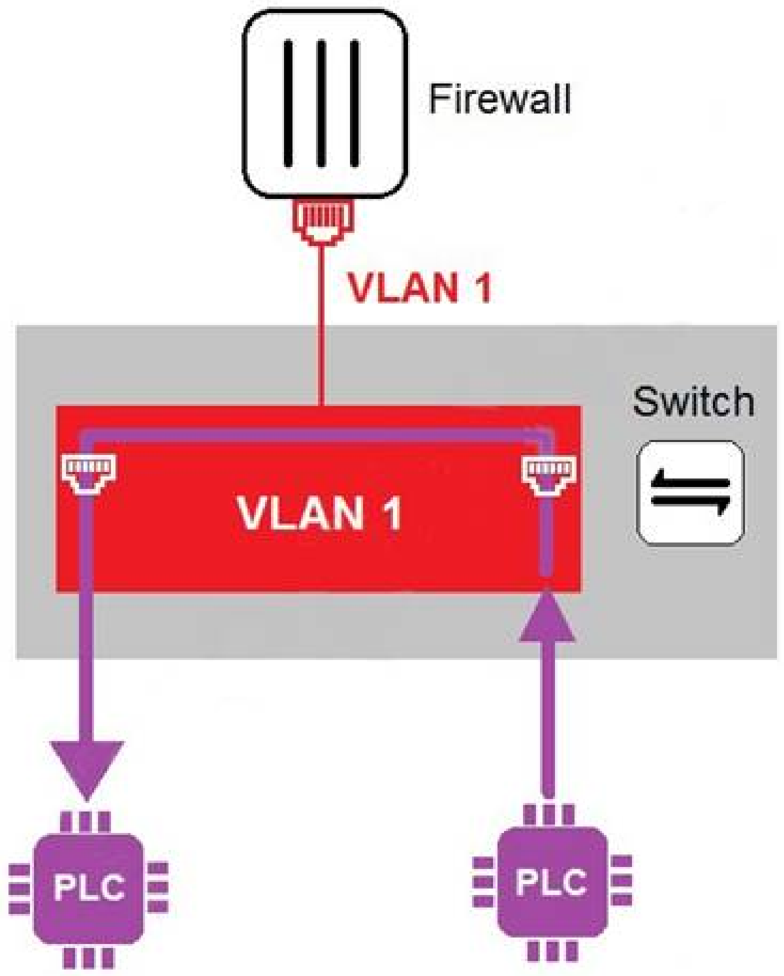
NEW QUESTION 6
An OT administrator is defining an incident notification policy using FortiSIEM and would like to configure the system with a notification policy. If an incident occurs, the administrator would like to be able to intervene and block an IP address or disable a user in Active Directory from 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 7
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.

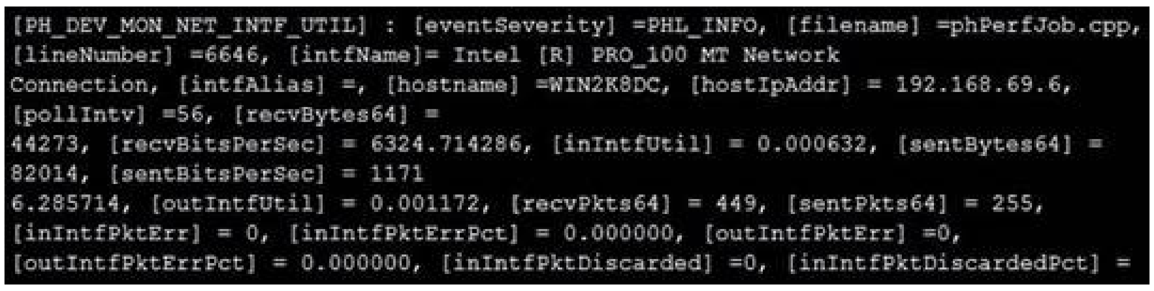
Answer: D

NEW QUESTION 8
An OT network consists of multiple FortiGate devices. The edge FortiGate device is deployed as the secure gateway and is only allowing remote operators to access the ICS networks on site.
Management hires a third-party company to conduct health and safety on site. The third- party company must have outbound access to external resources.
As the OT network administrator, what is the best scenario to provide external access to the third-party company while continuing to secure the ICS networks?

A. Configure outbound security policies with limited active authentication users of the third- party company.
B. Create VPN tunnels between downstream FortiGate devices and the edge FortiGate to protect ICS network traffic.
C. Split the edge FortiGate device into multiple logical devices to allocate an independent VDOM for the third-party company.
D. Implement an additional firewall using an additional upstream link to the internet.

Answer: C

NEW QUESTION 9
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 10
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

Answer: C

NEW QUESTION 10
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 13
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

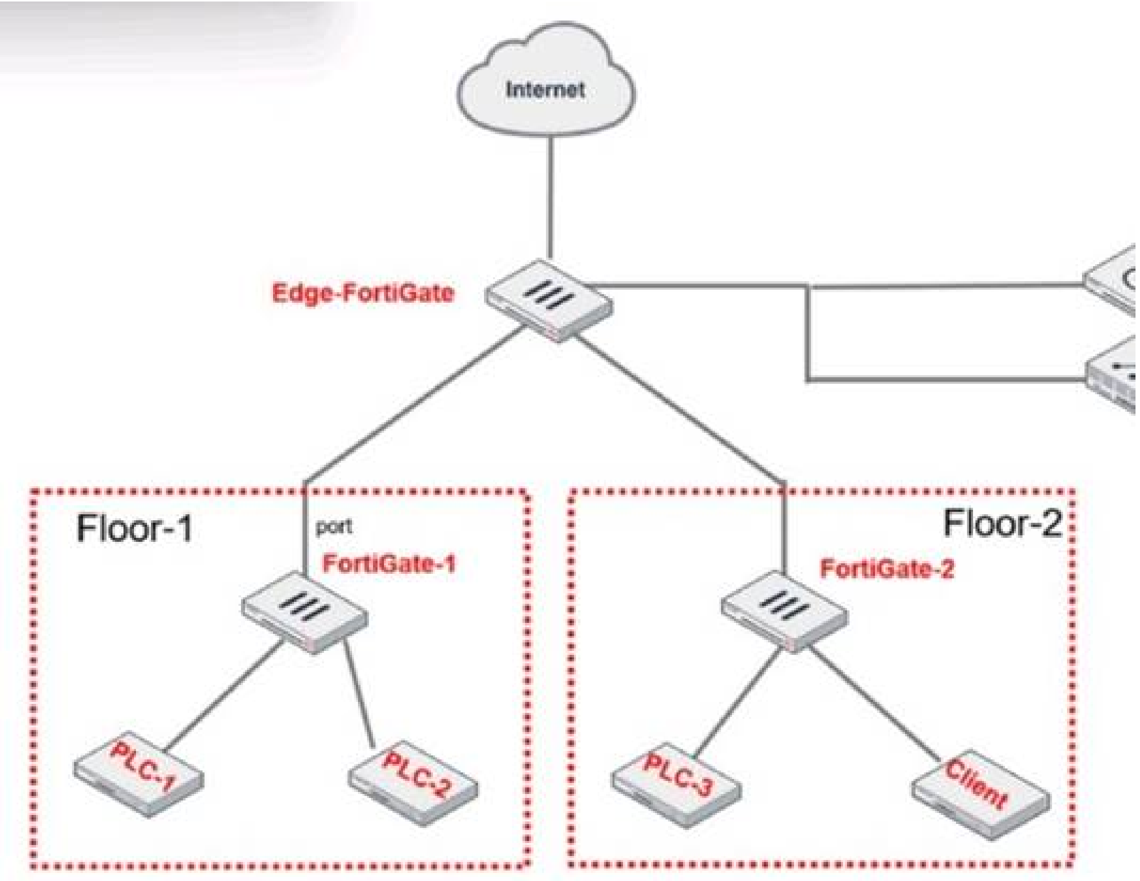
Answer: B

NEW QUESTION 15
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 17
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.

Answer: AB

NEW QUESTION 19
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: ADE

Explanation:
A. FortiNAC - FortiNAC is a network access control solution that provides visibility and control over network devices. It can identify devices, enforce access policies, and automate threat response.
* D. FortiSIEM - FortiSIEM is a security information and event management solution that can collect and analyze data from multiple sources, including network devices and servers. It can help identify potential security threats, as well as monitor compliance with security policies and regulations.
* E. FortiAnalyzer - FortiAnalyzer is a central logging and reporting solution that collects and analyzes data from multiple sources, including FortiNAC and FortiSIEM. It can provide insights into network activity and help identify anomalies or security threats.
Reference:
Fortinet NSE 7 - OT Security 6.4 Study Guide, Chapter 4: OT Security Devices, page 4-20.

NEW QUESTION 22
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

Answer: ADE

Explanation:
https://docs.fortinet.com/document/fortinac/9.2.0/administration-guide/15797/user-host-profiles

NEW QUESTION 23
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: A

Explanation:
An OT network architect can accomplish the goal of securing control area zones with a single network access policy to provision devices to any number of different networks on a FortiGate device.

NEW QUESTION 26
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 30
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.

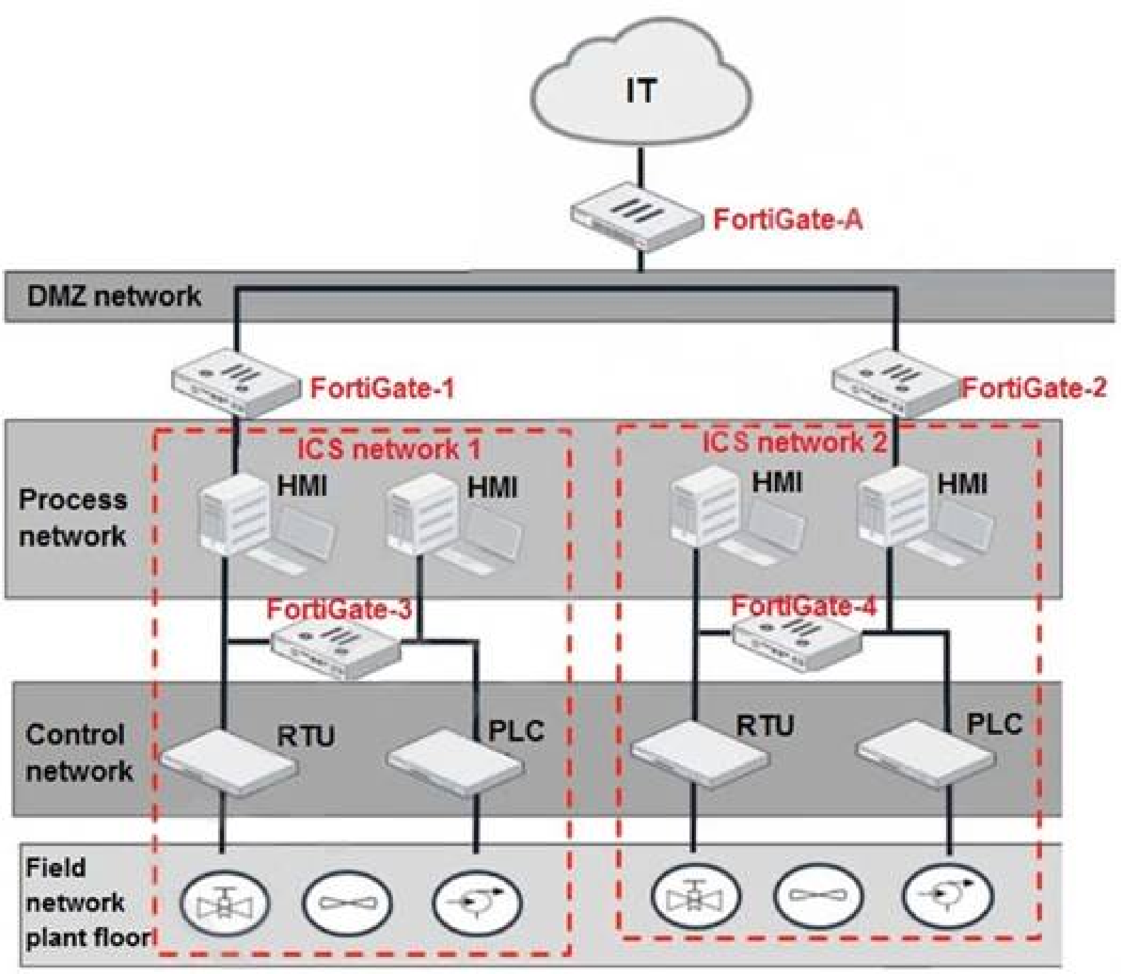
Answer: BC

NEW QUESTION 35
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 39
Refer to the exhibit.



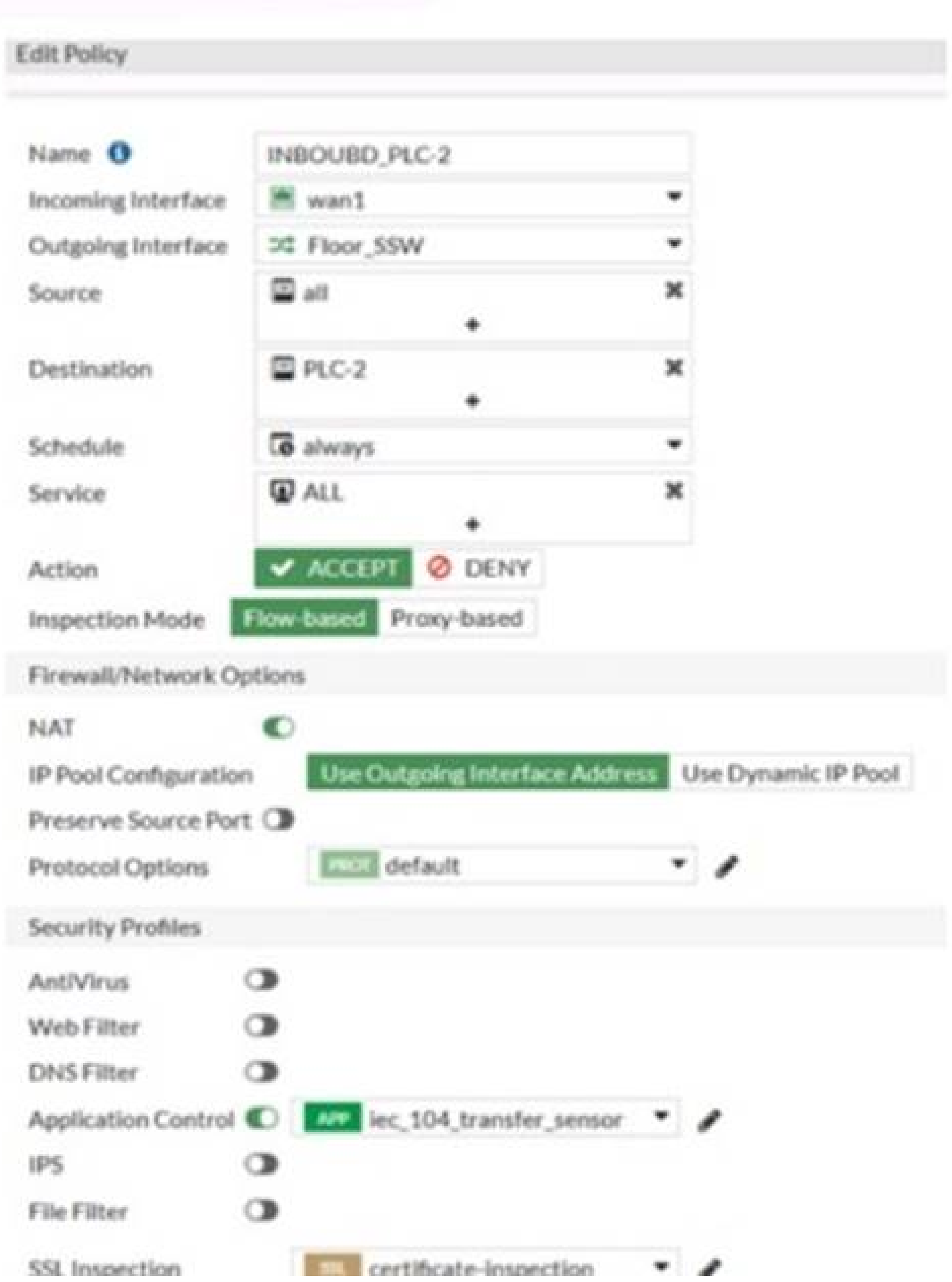
Based on the topology designed by the OT architect, which two statements about implementing OT security are true? (Choose two.)

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: AC

NEW QUESTION 42
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

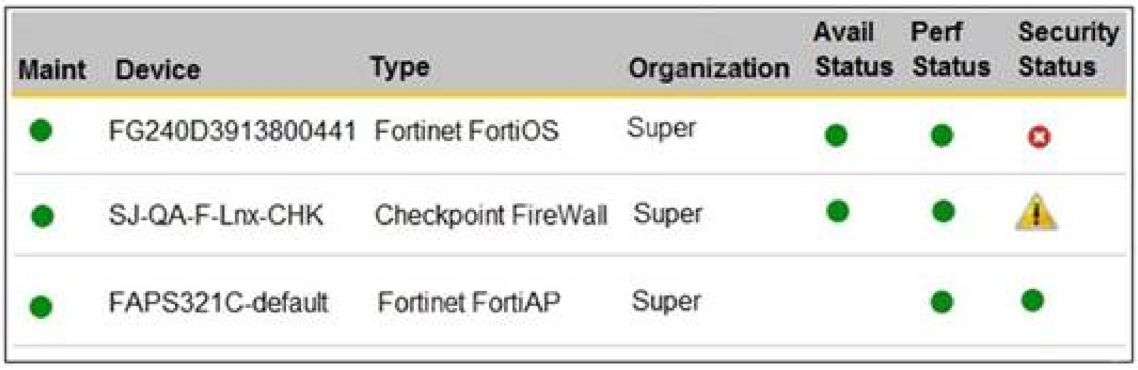
AntiVirus: ○
Web Filter: ○
DNS Filter: ○
Application Control: ● APP iec_104_transfer_sensor
IPS: ○
File Filter: ○
SSL Inspection: SSL certificate-inspection

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 45
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

NEW QUESTION 49

......