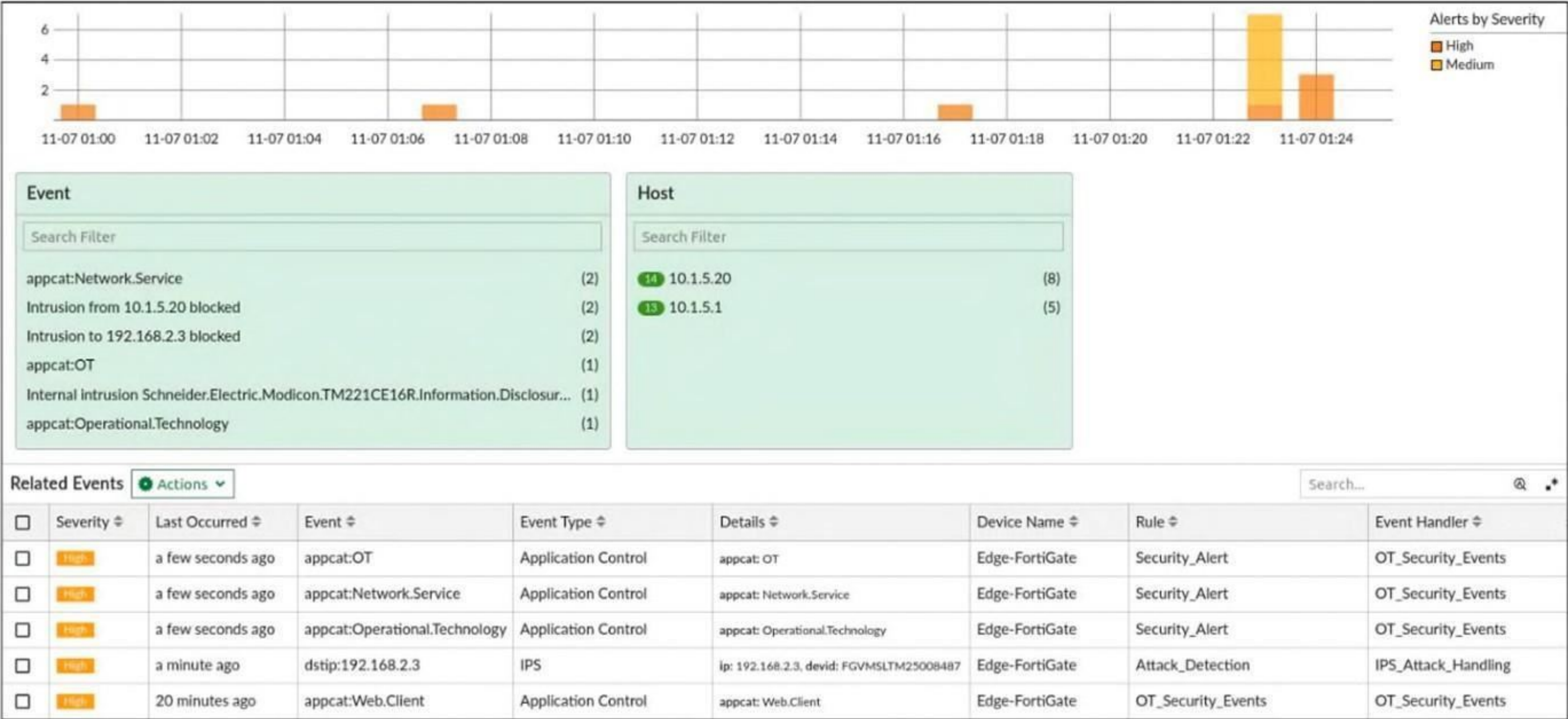


Fortinet.NSE6_OTS_AR-7.6.v2026-09-05.q76

Exam Code:	NSE6_OTS_AR-7.6
Exam Name:	Fortinet NSE 6 - OT Security 7.6 Architect
Certification Provider:	Fortinet
Free Question Number:	76
Version:	v2026-09-05
# of views:	106
# of Questions views:	762
https://www.freecram.net/torrent/Fortinet.NSE6_OTS_AR-7.6.v2026-09-05.q76.html	

NEW QUESTION: 1
Refer to the exhibit.

FortiAnalyzer Event Monitor page



A FortiAnalyzer Event Monitor page is shown.

Based on the Event Monitor page, which two statements are correct? (Choose two.)

- A. Thirteen events are related to the host with the IP address 10.1.5.1.
- B. The OT_Security_Events event handler has more than one rule configured.
- C. There are five high-severity events.
- D. The device with the IP address 192.168.2.3 is under attack.

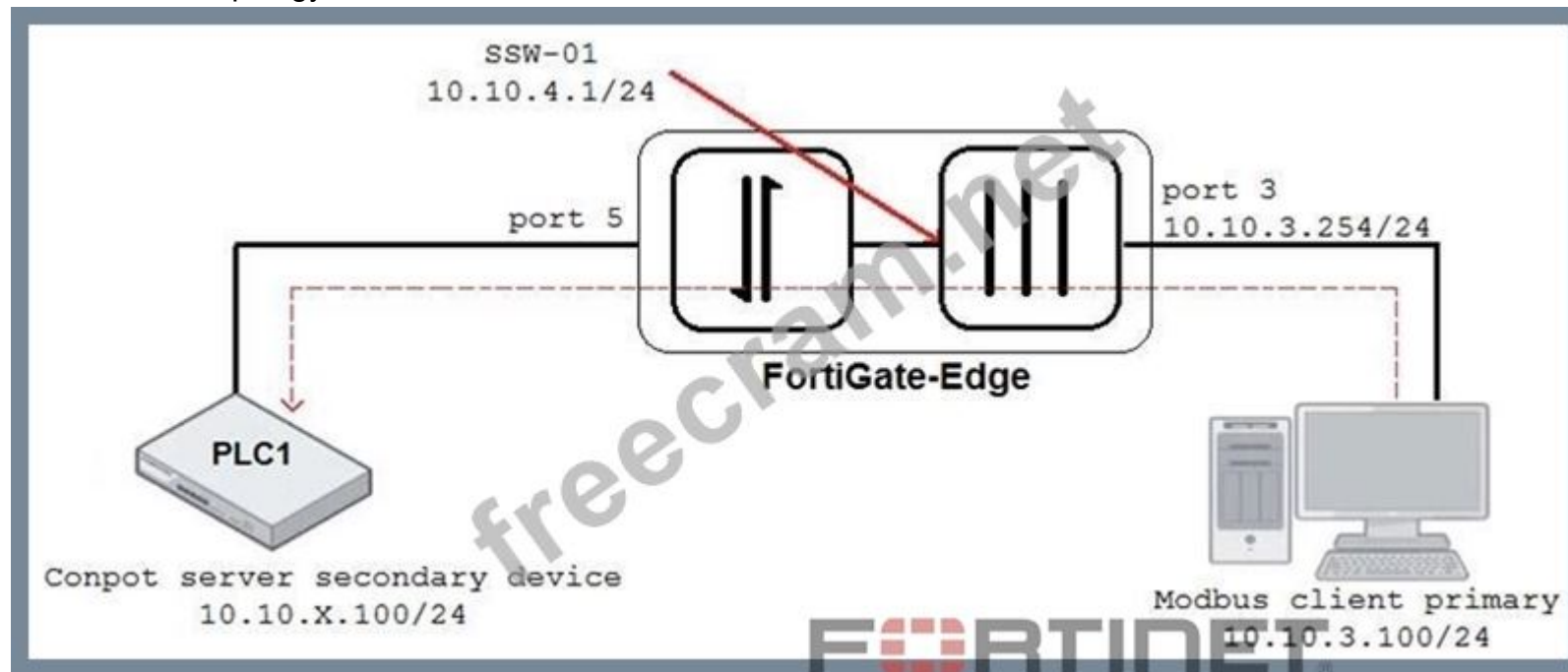
Answer: (SHOW ANSWER)

The presence of multiple events associated with the OT_Security_Events handler indicates that it is using more than one rule to generate events. The IPS event referencing the device with IP 192.168.2.3 and showing mitigation confirms that this device is being targeted by attacks.

NEW QUESTION: 2

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 devices is in offline IDS mode.
- B. NAT is disabled in the FortiGate firewall policy from port3 to ssw-01.
- C. Port5 is not a member of the software switch.
- D. The FortiGate-Edge device must be in NAT mode.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 3

Refer to the exhibit.



A Logical Topology page of a FortiGate device is shown. Your OT company wants to gain visibility into the network. You decide to implement device detection with the Security Fabric. Based on the exhibit, which statement is correct? (Choose one answer)

- A. Device Detection is enabled on the other identified device.
- B. The other identified device must be authorized on the root FortiGate.
- C. The other identified device must be authorized on FortiAnalyzer.

D. Device Detection is enabled on port3.

Answer: ([SHOW ANSWER](#))

The correct answer is A. Device Detection is enabled on the other identified device .

The study guide explains that device identification is a "useful feature for the Security Fabric topology view" and that "FortiGate detects most third-party devices in your network and adds them to the topology view of the Security Fabric." It also states that in the interfaces section, you can enable device detection , and this detection is what allows FortiGate to identify devices based on observed traffic.

In the exhibit, the tooltip distinguishes between "1 device requires authorization" and "1 other identified device." That means the unauthorized device is a separate FortiGate/Fabric member issue, while the other identified device is simply a detected third-party device shown in the topology because device detection is working. Therefore, the correct interpretation is that device detection is enabled for that identified device.

Option B is incorrect because the exhibit does not say the other identified device requires authorization.

Option C is not supported by the study guide, and option D is too specific because no evidence in the exhibit confirms that the detection was enabled specifically on port3 .

NEW QUESTION: 4

Refer to the exhibit. From your analysis of the output, which statement about the output is true?

```
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] =  
14273, [recvBitsPerSec] = 6324.714286, [inIntfUtil] = 0.000632, [sentBytes64] =  
82014, [sentBitsPerSec] = 1171  
5.285714, [outIntfUtil] = 0.001172, [recvPkts64] = 449, [sentPkts64] = 255,  
[inIntfPktErr] = 0, [inIntfPktErrPct] = 0.000000, [outIntfPktErr] =0,  
[outIntfPktErrPct] = 0.000000, [inIntfPktDiscarded] =0, [inIntfPktDiscardedPct] =
```

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: ([SHOW ANSWER](#))

ph_dev_mon is a PAM event. Hostname is WIN2K8DC (a win server) not Fortigate.

NEW QUESTION: 5

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 ([LEAVE A REPLY](#))

FortiNAC learns about endpoints connecting to the network using multiple methods, and one of the key methods in wireless network integrations is through RADIUS communication.

When a device attempts to connect, RADIUS requests provide MAC address information to FortiNAC.

FortiNAC can also use SNMP traps (link traps or MAC notification traps) and traffic monitoring, but RADIUS is the main standard method for wireless MAC address acquisition.

NEW QUESTION: 6

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 are true about FortiSoC and SOAR features on FortiAnalyzer? (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: ([SHOW ANSWER](#))

You must choose the proper operator in an event handler so the event actually fires, and playbooks let you automate SOC tasks (response actions) on FortiAnalyzer.

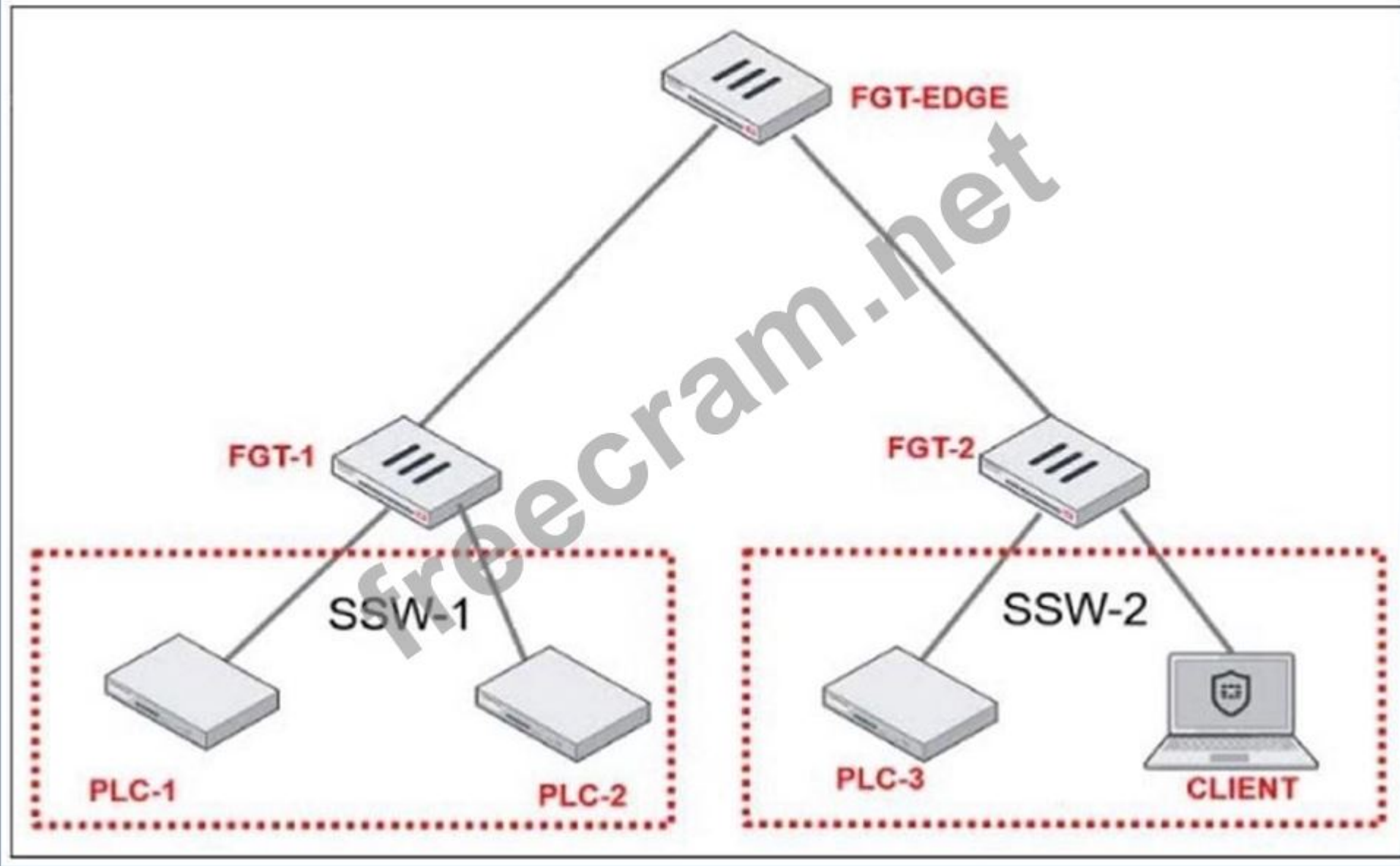
NEW QUESTION: 7

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-2) connecting both PLC-3 and CLIENT. PLC-3 and CLIENT can send traffic to each other at the layer 2 level.

What must the operational technology (OT) admin do to prevent layer 2-level communication between PLC-3 and CLIENT?

Network topology

FORTINET®



- 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: ([SHOW ANSWER](#))

Set the software switch to explicit intra-switch policy so traffic between its member ports must pass through FortiGate policies instead of being bridged at Layer 2. This stops PLC-3 and CLIENT from communicating directly at L2.

NEW QUESTION: 8

In your OT environment, you want to detect the devices passively. Which two methods must you implement?

(Choose two answers)

- A. SSH
- B. SNMP

- C. Vendor OUI
- D. Network traffic

Answer: C,D ([LEAVE A REPLY](#))

The correct answers are C. Vendor OUI and D. Network traffic .

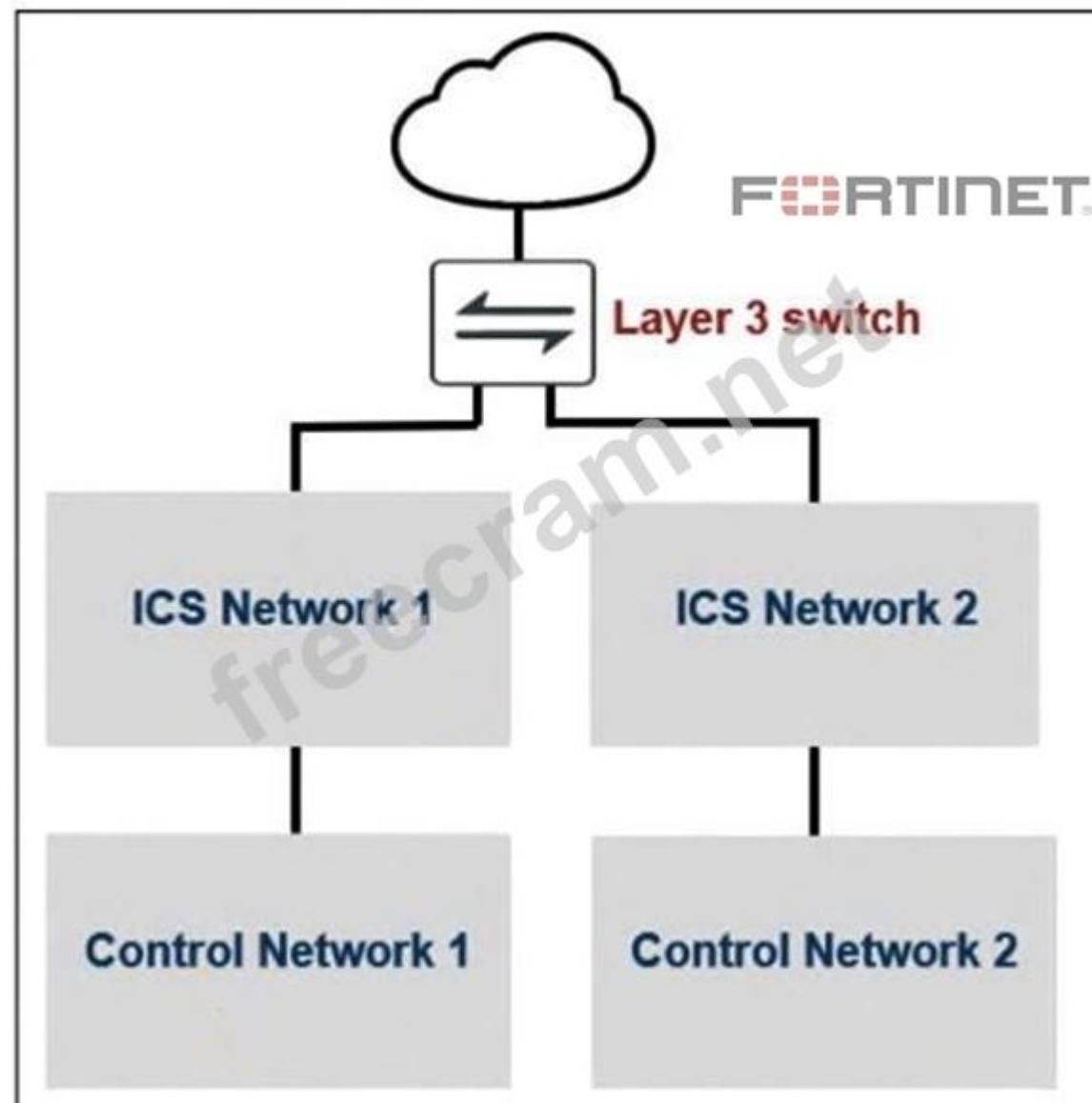
The study guide explicitly separates active/direct profiling methods from passive/non-direct methods and states that "In OT environments, passive methods are preferred over active methods." It then lists the methods that do not require FortiNAC to interact directly with the device being profiled. Among those methods are "Network traffic: gathered from the infrastructure" and "Vendor OUI: determined by the MAC address gathered from the infrastructure." That directly matches options C and D .

Options A and B are incorrect because SSH and SNMP are shown in the guide under the direct/active profiling methods. The guide's point is that passive detection avoids directly scanning or interacting with OT endpoints, since that can negatively affect performance in industrial environments. Because the question specifically asks for passive detection methods, the correct pair is Vendor OUI and Network traffic .

NEW QUESTION: 9

Refer to the exhibit.

Logical topology



A partial OT network is shown.

You must improve the security of this OT network and implement internal segmentation between network 1 and the network 2.

How can you achieve the segmentation?

- A. You can configure universal ZTNA.
- B. You can configure one traffic VDOM.
- C. You can configure an explicit software switch.
- D. You can configure forward domain IDs for each network.

Answer: ([SHOW ANSWER](#))

Forward domain IDs allow segmentation of traffic within the same Layer 3 infrastructure by assigning separate domains to different networks, effectively isolating Network 1 and Network 2 while still using the same physical device.

NEW QUESTION: 10

Refer to the exhibit. A partial Application Sensor profile is shown.

Partial Application Sensor profile

Name

Comments 0/255

Categories

☒ Mixed ☐ All Categories

- ☒ Business (158, 11)
- ☒ Collaboration (263, 16)
- ☒ Game (83)
- ☒ Generative AI (30, 23)
- ☒ Network Service (338)
- ☒ P2P (55)
- ☒ Remote Access (99)
- ☒ Storage/Backup (156, 24)
- ☒ Video/Audio (148, 16)
- ☒ Web Client (24)
- ☒ Cloud/IT (68, 2)
- ☒ Email (76, 11)
- ☒ General Interest (235, 11)
- ☒ Mobile (3)
- ☒ Operational Technology (3386, 37)
- ☒ Proxy (200)
- ☒ Social Media (111, 28)
- ☒ Update (48)
- ☒ VoIP (23)
- ☒ Unknown Applications

☒ Network Protocol Enforcement

Application and Filter Overrides

[+ Create New](#) [Edit](#) [Delete](#)

Priority	Details	Type	Action
1	Modbus_Read.Holding.Registers	Application	Allow
2	Modbus	Application	Block

When you apply this profile in a firewall policy, which two statements are correct? (Choose two answers)

- A. Modbus write commands are blocked.
- B. OT signatures are enabled.
- C. All OT protocols are monitored.
- D. A log is provided for each Modbus read holding registers command.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 11

Refer to the exhibit.

Basic Event Handler

Status ☒

Name * Handle_Alert

Description 0/1024

Event Handler Type Basic Correlation

MITRE Tech ID Click to select

Data Selector Click to select

Automation Stitch ☒

A basic event handler is shown. You have enabled Automation Stitch to automate the handling of an alert.

Which two steps must you take to use this automation stitch? (Choose two answers)

- A. You must configure Action on FortiAnalyzer.
- B. You must configure a Playbook task on FortiAnalyzer.
- C. You must configure a FortiAnalyzer event handler trigger on FortiGate.
- D. You must configure Rules on FortiAnalyzer.

Answer: ([SHOW ANSWER](#))

The correct answers are C and D .

Option D is correct because the study guide states that the configuration of an event handler can include

"Rules" and explains that "Rules are granular conditions" and "Event handlers can have one or more rules." It further states that "FortiAnalyzer uses event handlers to filter all incoming logs" and "If logs match the conditions configured in an event handler, FortiAnalyzer generates an event." Therefore, to use the automation stitch, you must define the rules on FortiAnalyzer so the event handler can actually generate the event that starts the automation flow.

Option C is also correct. The study guide explains that "When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification" to the FortiGate side, and in the attack-detection example it says "FortiAnalyzer parses the logs and notifies the root FortiGate" and then

"The root FortiGate triggers the action." It also explicitly shows "Stitches configured on root FortiGate." This means the FortiGate must have the corresponding automation trigger configured for the FortiAnalyzer event handler notification.

Option A is incorrect because the study guide does not describe configuring an Action on FortiAnalyzer as the required step for this FortiAnalyzer-to-FortiGate automation-stitch flow. Option B is also incorrect because playbooks are a different FortiAnalyzer automation mechanism; the question specifically refers to using the Automation Stitch option in the event handler.

NEW QUESTION: 12

Which statement about the IEC 104 protocol is true?

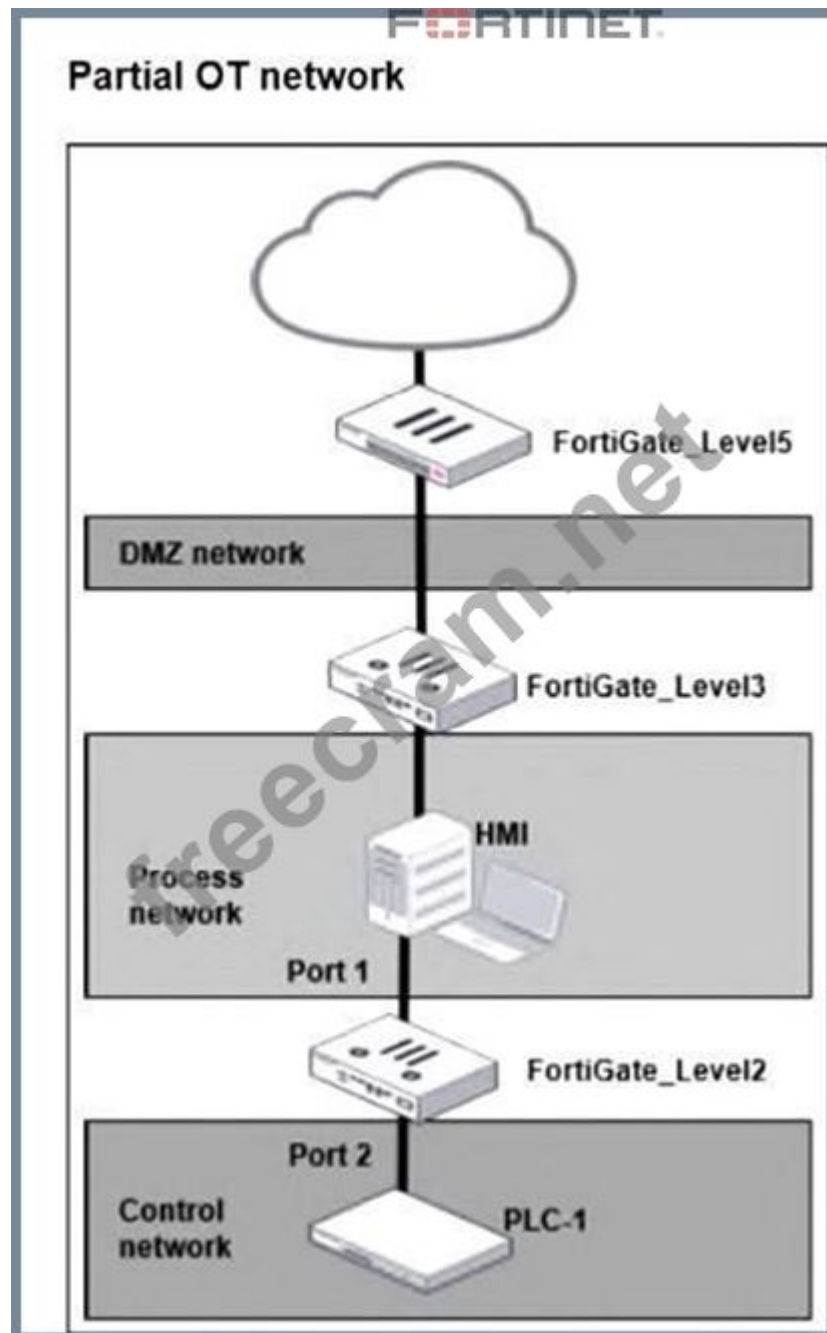
- A. IEC 104 is used for telecontrol SCADA in electrical engineering applications.
- B. IEC 104 is IEC 101 compliant in old SCADA systems.
- C. IEC 104 protects data transmission between OT devices and services.
- D. IEC 104 uses non-TCP/IP standards.

Answer: ([SHOW ANSWER](#))

IEC 104 is a widely used protocol in the field of Supervisory Control and Data Acquisition (SCADA) for electrical engineering applications, specifically telecontrol. It's designed to facilitate communication between control stations and substations in power grids.

NEW QUESTION: 13

Refer to the exhibits.



Partial firewall policy configuration



A partial OT network and the Security Profiles section of the FortiGate_Level2 firewall policy are shown.

You have configured the FortiGate_Level2 firewall policy with a virtual patching profile because PLC-1 has vulnerabilities. A penetration test performed from the HMI device still reports vulnerabilities visible on PLC-1.

Which two additional parameters must you enable on FortiGate_Level2? (Choose two.)

- A. OT application control
- B. OT signatures
- C. Device detection on port2
- D. Device detection on port1

Answer: ([SHOW ANSWER](#))

Virtual patching relies on OT-specific IPS signatures to detect and block exploitation attempts, so OT signatures must be enabled. Additionally, device detection must be enabled on the interface connected to the PLC to properly identify the OT device and apply the correct protection.

NEW QUESTION: 14

An OT architect has deployed a Layer 2 switch in the OT network at Level 1 in the Purdue model- process control. The purpose of the Layer 2 switch is to segment traffic between PLC1 and PLC2 with two VLANs.

All the traffic between PLC1 and PLC2 must first flow through the Layer 2 switch and then through the FortiGate device in the Level 2 supervisory control network.

Which statement about the traffic between PLC1 and PLC2 is true?

- A. In order to communicate, PLC1 must be in the same VLAN as PLC2.
- B. The Layer 2 switch rewrites VLAN tags before sending traffic to the FortiGate device.
- C. The Layer 2 switch routes any traffic to the FortiGate device through an Ethernet link.
- D. The FortiGate must be configured as a "Router on a stick" for intra-PLC communication.

Answer: ([SHOW ANSWER](#))

With PLC1 and PLC2 in separate VLANs on a Layer 2 switch, inter-VLAN traffic must be routed.

The FortiGate provides that routing and policy control by using VLAN subinterfaces on a single physical link ("router on a stick"), so all PLC1↔PLC2 traffic passes through it.

NEW QUESTION: 15

Refer to the exhibit. An OT administrator ran a report to identify device inventory in an OT network. Based on the report results, which report was run?

Active Rules x Windows Installed Patches x Router/Switch Image Distribution x

BackExport

1/1

Device Name	Device Type	Vendor	Device Type	Model	Device Hardware Model	Device Image File	Count
SJ-QA-A-IOS-JunOffice	Cisco	IOS		1760		C1700-advsecurityk9-mz.123-8.T4.bin	1
SJ-Main-Cat6500	Cisco	IOS		WS-C6509		s72033-advipservicesk9_wan-mz.122-33.SX11.bin	1
ph-network-3560_1	Cisco	IOS		WS-C3560G-48PS-S		c3560-advipservicesk9-mz.122-25.SEE4.bin	1

- A. A FortiSIEM incident report
- B. A FortiAnalyzer device report
- C. A FortiSIEM CMDDB report
- D. A FortiSIEM analytics report

Answer: (SHOW ANSWER)

NEW QUESTION: 16

To increase security protection in an OT network, how does application control on FortiGate 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

Answer: (SHOW ANSWER)

FortiGate's application control identifies OT traffic by deep-inspecting the industrial protocols carried in the flows (Modbus, DNP3, IEC-104, etc.). It matches protocol signatures to classify the application and enforce policy.

Valid NSE6_OTs_AR-7.6 Dumps shared by EduDump.com for Helping Passing NSE6_OTs_AR-7.6 Exam! EduDump.com now offer the **newest NSE6_OTs_AR-7.6 exam dumps**, the EduDump.com NSE6_OTs_AR-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com NSE6_OTs_AR-7.6 dumps with Test Engine here: https://www.edudump.com/exams/Fortinet/NSE6_OTs_AR-7.6/premium/ (153 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 17

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

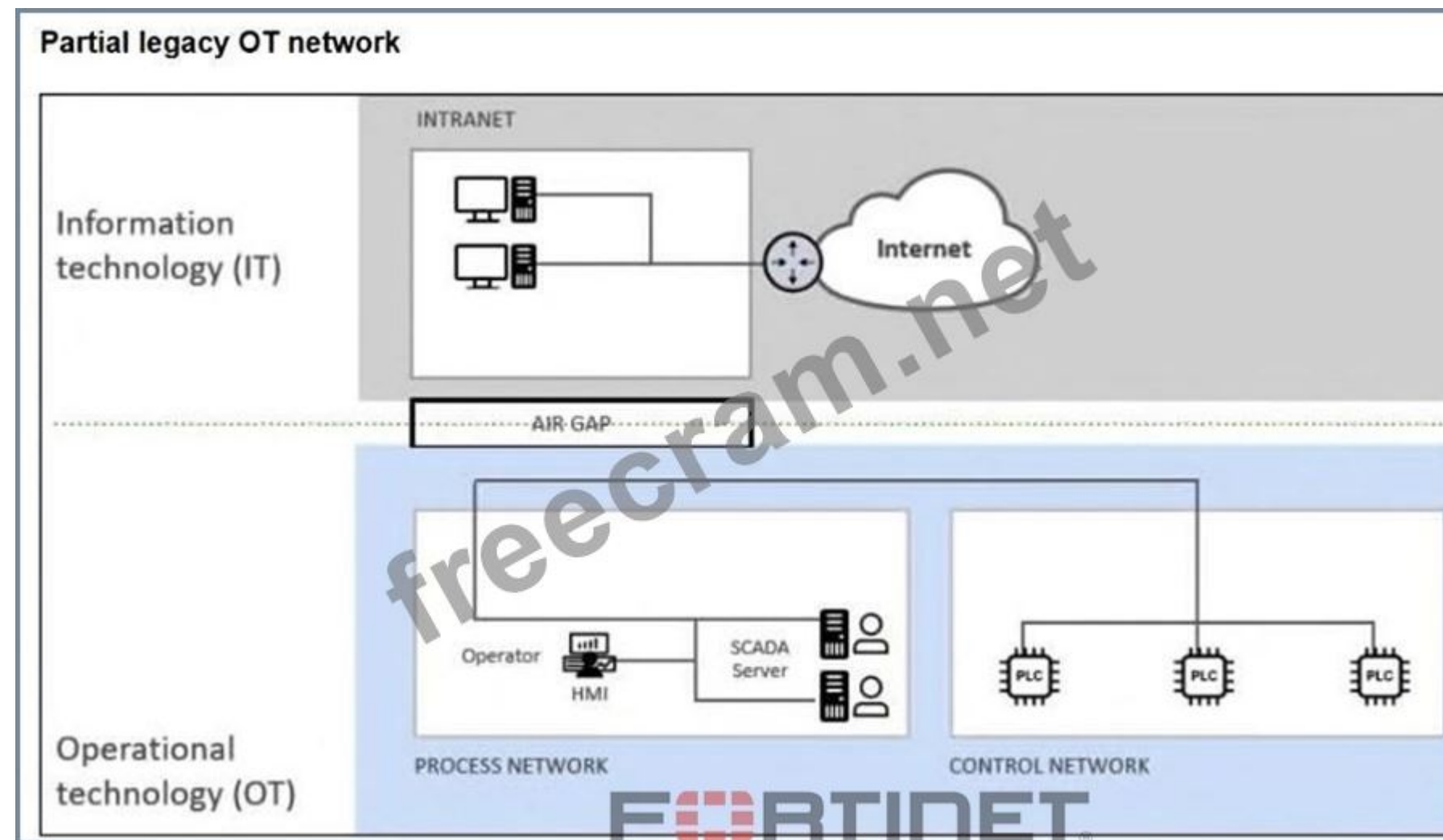
- A. FortiNAC
- B. FortiManager
- C. FortiAnalyzer
- D. FortiSIEM
- E. FortiGate

Answer: ([SHOW ANSWER](#))

NGFW, FortiNAC and FortiSIEM can be used in an OT network to achieve asset identification and management.

NEW QUESTION: 18

Refer to the exhibit.



A partial legacy OT network is shown.

You must improve this historically flat OT network and minimize the risk of lateral movement.

Which action must you perform?

- A. You must add two-factor authentication.
- B. You must implement SD-WAN.
- C. You must segment the network with a hardware switch.
- D. You must implement micro-segmentation with firewall policies.

Answer: ([SHOW ANSWER](#))

Micro-segmentation using firewall policies creates granular control between devices and zones within the OT network, effectively limiting lateral movement and reducing the attack surface.

NEW QUESTION: 19

Refer to the exhibit.

Creation of a new automation trigger

Create New Automation Trigger

 **FortiAnalyzer Event Handler** A specified FortiAnalyzer event handler was triggered. 

Name

Description 0/255

FortiAnalyzer Event Handler

 Configure a FortiAnalyzer connection to utilize FortiAnalyzer event handlers:

- FortiAnalyzer

Event handler name

Event severity ☐

Event tag ☐

Brave-Dumps.com ☐

No entries



An automation trigger creation wizard is shown. You want to automate some tasks in your OT network. In a FortiGate device, you create a new automation trigger based on a FortiAnalyzer event handler. When you want to configure the Event handler name field, the event handler created in FortiAnalyzer is not shown.

What are two reasons for this? (Choose two answers)

- A. You must configure the Fabric settings on the FortiGate device.
- B. You must enable Automation Stitch in the event handler on FortiAnalyzer.
- C. You must click + Create in the Event handler name field.
- D. You must add the FortiGate device to FortiAnalyzer and authorize it.

Answer: ([SHOW ANSWER](#))

The correct answers are A and B .

Option B is correct because the study guide states that "When a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification" to FortiGate. If Automation Stitch is not enabled in the FortiAnalyzer event handler, that handler will not be usable for the FortiGate automation- stitch workflow. The guide also explains that the configuration of each event handler can include

"Automation stitches" and "Rules," showing that this is a required part of the FortiAnalyzer-to-FortiGate automation path.

Option A is also correct. The study guide explains the automation flow in the Security Fabric:

"FortiAnalyzer parses the logs and notifies the root FortiGate" and then "The root FortiGate triggers the action." That means FortiGate must have the FortiAnalyzer connection configured through the Security Fabric side before it can consume FortiAnalyzer event handlers. The warning in the exhibit about configuring a FortiAnalyzer connection also points directly to that requirement.

Option C is incorrect because + Create is not the reason the existing event handler is missing; it is only an interface control. Option D is not the best answer for this item because the question is about why the event handler name list on FortiGate is empty for FortiAnalyzer-triggered automation. The study guide's verified requirements for that workflow are the FortiAnalyzer-to-FortiGate Fabric connection and enabling Automation Stitch on the FortiAnalyzer event handler.

NEW QUESTION: 20

Refer to the exhibit. 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?

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			

- A. In the PCI logging dashboard and there are one or more high-severity security incidents for the FortiGate device.
- B. In the widget dashboard and there are one or more high-severity incidents for the FortiGate device.
- C. In the business service dashboard and there are one or more high-severity security incidents for the FortiGate device.
- D. In the summary dashboard and there are one or more high-severity security incidents for the FortiGate device.

Answer: (SHOW ANSWER)

NEW QUESTION: 21

You want to protect OT devices that are not updated against known vulnerabilities so you apply virtual patching to the firewall policies. What must you check to confirm that the OT devices are virtually patched?

(Choose one answer)

- A. The output of the CLI command get virtual-patch profile
- B. The output of the CLI command get rule otp status
- C. The OT View page
- D. The Asset Identity List page

Answer: (SHOW ANSWER)

NEW QUESTION: 22

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. By default, the industrial database is enabled.
- B. A supervisor can enable it through the FortiGate CLI.
- C. A supervisor must purchase an industrial signature database and import it to the FortiGate.
- D. An administrator must create their own database using custom signatures.

Answer: (SHOW ANSWER)

NEW QUESTION: 23

You want to improve the security of your OT network and therefore deploy a FortiGate device with the OT signatures database. Which two statements about this database are true? (Choose two answers)

- A.** You must install a valid OT security service license.
- B.** You must import the OT signatures database manually.
- C.** The OT signatures database is enabled by default.
- D.** You must set exclude-signatures to none in the console line interface.

Answer: ([SHOW ANSWER](#))

The correct answers are A and D .

Option A is correct because the study guide states that for OT protocol coverage, "a valid OT security service license is required to receive updates on both intrusion prevention and application control signatures." It also shows "Valid license required" in the FortiGuard subscriptions section for OT protocol coverage. This confirms that a valid OT security service license is required to use and maintain the OT signatures database correctly.

Option D is also correct because the guide explicitly shows the CLI configuration used "To enable OT signatures" :

```
config ips global
```

```
set exclude-signatures none
```

```
end
```

It then states that "By default, OT signatures are excluded from the signatures lists on the GUI until you enable them on the CLI." This directly confirms that you must set exclude-signatures to none in the CLI to enable OT signatures.

Option B is incorrect because the study guide does not say you manually import the OT signatures database.

Instead, it explains that FortiGuard maintains updated OT signatures and that a valid license is required to receive updates. Option C is incorrect because the guide clearly says OT signatures are excluded by default until enabled from the CLI.

NEW QUESTION: 24

You want to automate some tasks in your OT network. Which three configurations are directly available in a new basic event handler on FortiAnalyzer? (Choose three answers)

- A.** Send alert email
- B.** Create a report
- C.** Quarantine an attacker
- D.** Automatically create an incident
- E.** Automation stitch

Answer: ([SHOW ANSWER](#))

According to the OT Security 7.6 Architect study guide regarding FortiAnalyzer Event Management:

Notification Options: When configuring a new event handler, FortiAnalyzer provides several built-in notification methods to alert administrators when specific log criteria are met. The most common and direct method is Send alert email (Option A).

Incident Management: To streamline the SOC workflow, an event handler can be configured to Automatically create an incident (Option D) based on the triggered event. This moves the event into the Incident Manager for further analysis.

Security Fabric Integration: In the 7.6 architecture, event handlers can directly trigger an Automation stitch (Option E). This allows the FortiAnalyzer to notify the root FortiGate to take action (like running a CLI script or changing a policy) across the Security Fabric.

Exclusions: Create a report (Option B) is typically a task performed by a Playbook or a scheduled report job, not a direct setting inside the basic event handler configuration. Quarantine an attacker (Option C) is an action that results from an automation stitch or playbook, but it is not a direct configuration toggle within the event handler itself.

NEW QUESTION: 25

In the Purdue model, at which level are physical assets like the Industrial Internet of Things (IIoT) placed?

- A. At Level 5 only
- B. At Level 1 only
- C. Above Level 4
- D. Below Level 3.5

Answer: (SHOW ANSWER)

In the Purdue model, Level 1 represents basic control and physical processes, where sensors, actuators, and IIoT devices interact directly with the physical environment.

NEW QUESTION: 26

Refer to the exhibit.

Firewall Policy page

Firewall Policy page

</

A firewall policy page is shown. To improve the security of your OT network, you have configured a Supervisor profile in the firewall policies, as shown in the exhibit. However, a supervisor is reporting that he cannot ping PLC-1. What are the two reasons? (Choose two answers)

- A. The supervisor must first authenticate using a protocol such as HTTPS or Telnet.
- B. The Supervisor profile is not configured in the remote server.
- C. The firewall policy ID 8 is not enabled.
- D. The CLI parameter auth-on-demand is set to always.

Answer: (SHOW ANSWER)

The correct answers are A and C .

Option A is correct because the study guide explains that with active authentication , FortiGate prompts the user only when they use "an acceptable login protocol." It states: "When you use only active authentication, if all possible policies that could match the source IP address have authentication enabled, then the user will receive a login prompt (assuming they use an acceptable login protocol)." A direct ping to PLC-1 uses ICMP , which is not the kind of login protocol used to trigger user authentication.

So the supervisor must first authenticate through a protocol such as HTTPS or Telnet , then the ICMP traffic can match the authenticated policy.

Option C is also correct because the exhibit shows policy ID 8 greyed out, meaning it is not enabled. That policy appears above the Supervisor_access (9) policy and allows broader access to PLC-1 , whereas policy 9 is limited to ALL_ICMP . The study guide explains that "Because the user has not yet authenticated, the user group aspect of the traffic does not match" and FortiGate continues searching for another complete match. In this case, with policy 8 disabled, the supervisor is left with only the ICMP rule, which cannot be used to perform the initial login step needed for active authentication.

Option B is not supported by the exhibit. Option D is incorrect because auth-on-demand always would force authentication prompts more aggressively, but the core problem here is that the user is trying to start with ICMP and the broader policy that could permit the initial authenticated access is disabled.

NEW QUESTION: 27

An organization has deployed an entry-level FortiGate device in their operational technology (OT) network. The administrator is looking for a simple solution to detect and block all network intrusions in that specific part of the network without any false positive activities.

Which solution should the administrator use to achieve this goal?

- A.** Configure a local-in firewall policy.
- B.** Block all foreign inbound traffic.
- C.** Enable intrusion prevention system (IPS) and use the regular signature database.
- D.** Enable the industrial signature database in the IPS global setting.

Answer: ([SHOW ANSWER](#))

Enabling the IPS industrial signature database focuses detection on OT/ICS protocols and known attack patterns, giving accurate blocking with minimal false positives on an entry-level FortiGate.

NEW QUESTION: 28

Which three device profiling methods of FortiNAC are considered non-direct? (Choose three.)

- A.** TCP
- B.** IP range
- C.** Location
- D.** Network traffic
- E.** SSH

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 29

FortiAnalyzer is implemented in the OT network to receive logs from responsible FortiGate devices. The logs must be processed by FortiAnalyzer.

In this scenario, which statement is correct about the purpose of FortiAnalyzer receiving and processing multiple log messages from a given PLC or RTU?

- A.** To isolate PLCs or RTUs in the event of external attacks
- B.** To configure event handlers and take further action on FortiGate
- C.** To determine which type of messages from the PLC or RTU causes issues in the plant
- D.** To help OT administrators configure the network and prevent breaches

Answer: ([SHOW ANSWER](#))

FortiAnalyzer acts as a centralized log management and analytics platform that collects security and operational logs from devices like FortiGate and from OT devices such as PLCs and RTUs. By processing multiple log messages, FortiAnalyzer helps identify which specific types of messages or events from PLCs or RTUs may cause failures, anomalies, or operational issues in the plant.

This detailed insight into device behavior aids OT administrators in pinpointing communication or security issues affecting operational technology.

FortiAnalyzer provides aggregated analysis, threat detection, compliance reporting, and detailed root cause analytics relevant to OT environments.

NEW QUESTION: 30

Refer to the exhibit.

Partial Incident Analysis page



Audit History

2025-11-23 05:56:02

Report attached to incident IN00000005.

By: admin

Report attached to incident IN00000005.

2025-11-23 05:55:18

New Incident Created

Incident IN00000005 is created.

2025-11-23 05:47:58

Events attached to incident IN00000005.

Events attached to incident IN00000005.

2025-11-23 05:48:21

Start 2025-11-23 05:47:58

Now

Expand All

Reports

+ Add - Delete

Search

☐ Report Name	Format	Time Range	Devices	Status
☐ Operational Technology (OT) Security Risk report-2025-11-23-0554-0800_87	PDF	2025/11/16 - 2025/11/23	3 Devices	13s

A partial Incident Analysis page is shown. How was the 360-Degree Security Review OT report attached to the incident? (Choose one answer)

- A. Automatically by a stitch
- B. Automatically by an event handler
- C. Automatically by a playbook
- D. Manually by an administrator

Answer: (SHOW ANSWER)

The study guide says playbooks are used to automate tasks such as running reports and creating/updating incidents . It also says that after a playbook is triggered, it flows through its configured tasks.

It further shows a sample playbook sequence where an event is detected, an incident is created , a report runs , and details are attached to the incident . That is exactly the kind of workflow shown in the incident analysis view.

By contrast, the study guide says event handlers generate events when logs match configured rules. Event handlers are for detection, not for attaching reports to incidents.

NEW QUESTION: 31

Which standard is the most important to OT security across all industrial sectors?

- A. NIST CSF
- B. IEC 62443
- C. HIPAA
- D. GDPR

Answer: ([SHOW ANSWER](#))

IEC 62443 is the primary international standard specifically designed for securing industrial automation and control systems across all OT sectors, providing comprehensive guidelines for policies, procedures, and technical controls.

Valid NSE6_OTC_AR-7.6 Dumps shared by EduDump.com for Helping Passing NSE6_OTC_AR-7.6 Exam! EduDump.com now offer the **newest NSE6_OTC_AR-7.6 exam dumps**, the EduDump.com NSE6_OTC_AR-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com NSE6_OTC_AR-7.6 dumps with Test Engine here: https://www.edudump.com/exams/Fortinet/NSE6_OTC_AR-7.6/premium/ (153 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 32

Refer to the exhibit. You are creating a new operational technology (OT) rule to monitor Modbus protocol traffic on FortiSIEM.

Which action must you take to ensure that all Modbus messages on the network match the rule?

A new OT rule

Edit SubPattern

Name:

industrial_protocol_monitor

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
	Destination TCP/UDP Port	IN	Group: OT Ports		OR	

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
	COUNT(Matched Events)	>=	1		AND	

Group By:

Attribute	Row	Move
Source TCP/UDP Port		
Destination TCP/UDP Port		
Event Type		
Reporting IP		

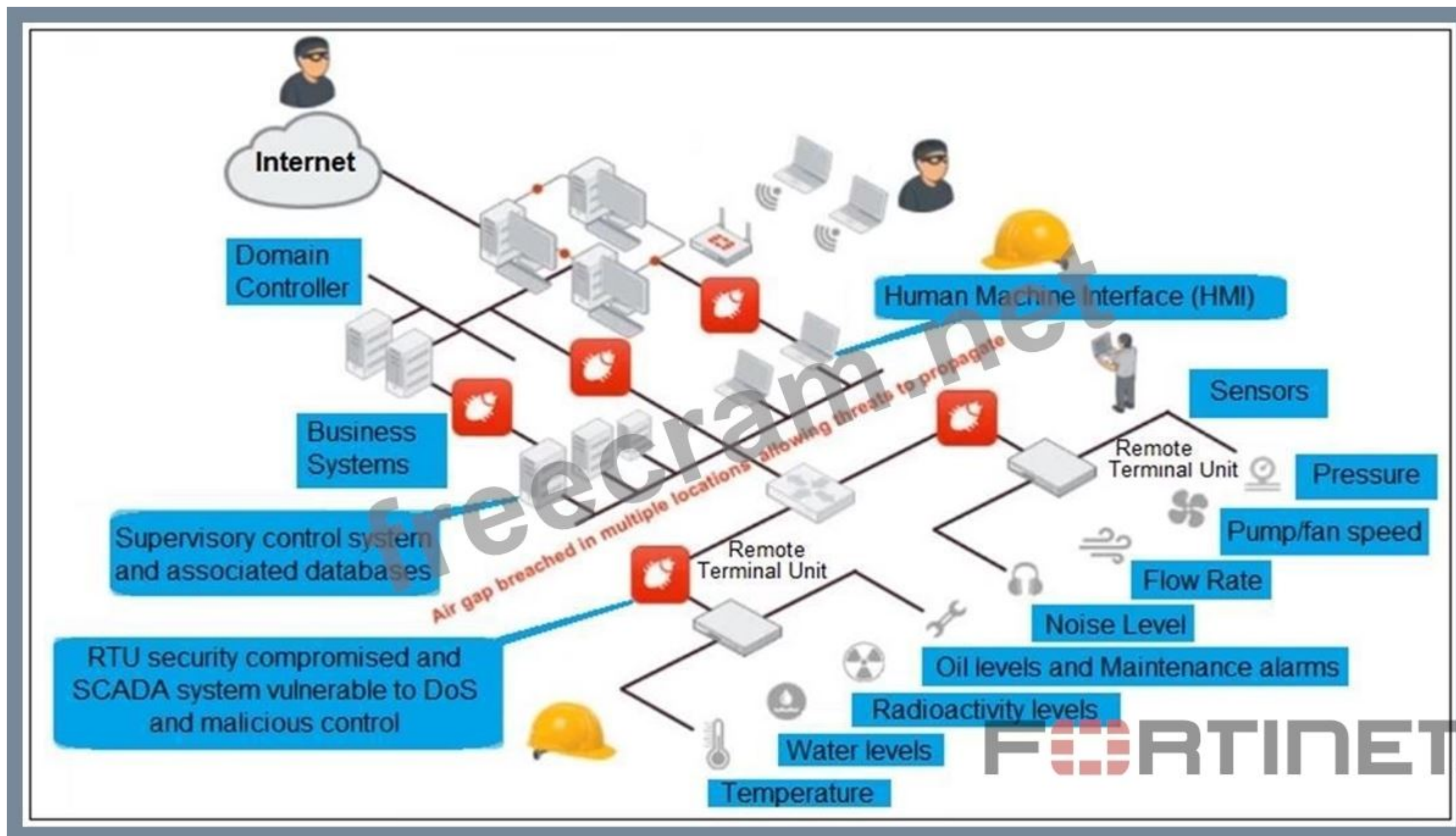
- A. The condition on the SubPattern filter must use the AND logical operator.
- B. Add a new condition to filter Modbus traffic based on the source TCP/UDP port.
- C. In the Group By section, remove all attributes that are not configured in the Filter section.
- D. In the Aggregate section, set the attribute value to equal to or greater than 0.

Answer: (SHOW ANSWER)

The current Aggregate condition is set to COUNT(Matched Events) >= 1, which only triggers the rule after at least one event. To ensure all Modbus messages (including the first one) match the rule, the condition must be >= 0, so every event is considered, including the very first occurrence.

NEW QUESTION: 33

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. Use segmentation
- B. Deploy an edge FortiGate between the internet and an OT network as a one-arm sniffer.
- C. Deploy a FortiGate device within each ICS network.
- D. Configure firewall policies with industrial protocol sensors
- E. Configure firewall policies with web filter to protect the different ICS networks.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 34

Which three protocols are used as industrial Ethernet protocols? (Choose three.)

- A. PROFINET
- B. EtherCAT

- C. M12
- D. EtherNet/IP
- E. RJ45

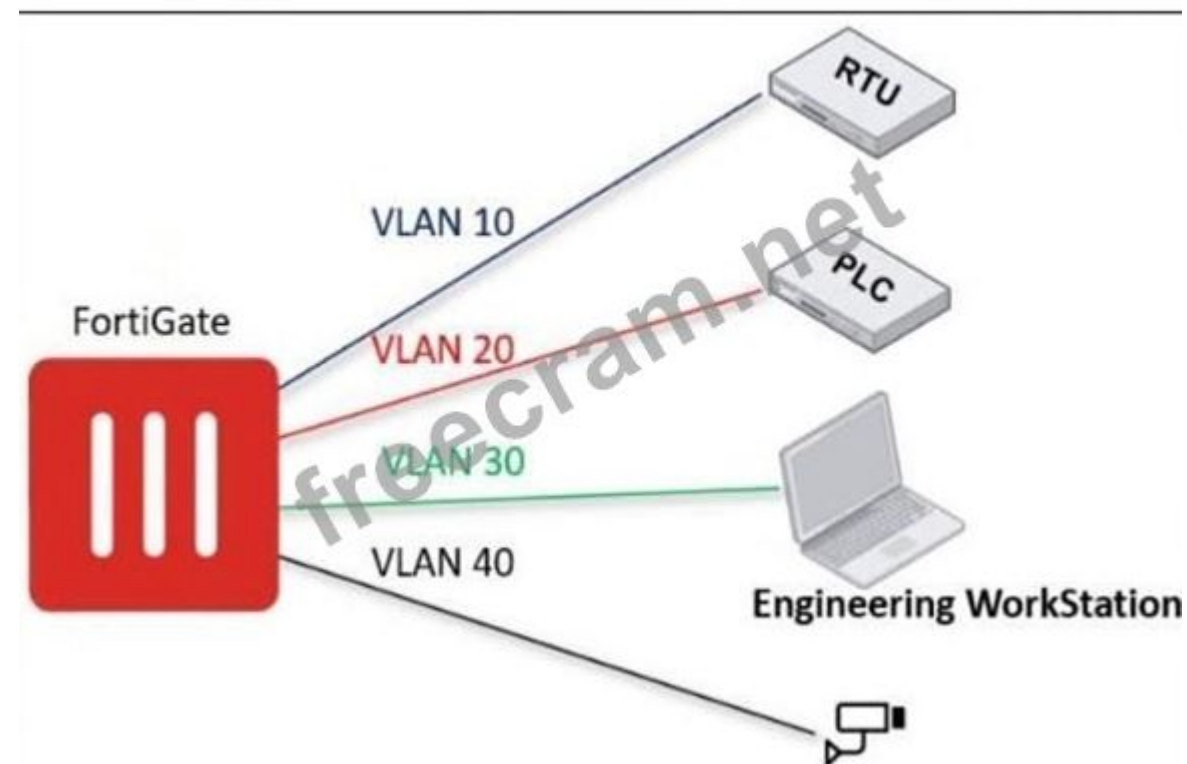
Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

Refer to the exhibit.

Logical topology

FORTINET



A partial OT network is shown.

You want to enforce access control from Engineering Workstation to PLC.

How can you achieve this on FortiGate?

- A. You must create forward domain IDs.
- B. You must set the software switch to implicit.
- C. You must add authentication in the corresponding firewall policy.
- D. You must create VDOMs.

Answer: C ([LEAVE A REPLY](#))

Access control from the Engineering Workstation to the PLC is enforced by applying authentication in the firewall policy that governs traffic between their VLANs. This ensures only authenticated users or devices are allowed to reach the PLC.

NEW QUESTION: 36

What is the primary objective of implementing SD-WAN in operational technology (OT) networks?

- A. Replace standard links with lower cost connections
- B. Enhance network performance of OT applications
- C. Reduce security risk and threat attacks

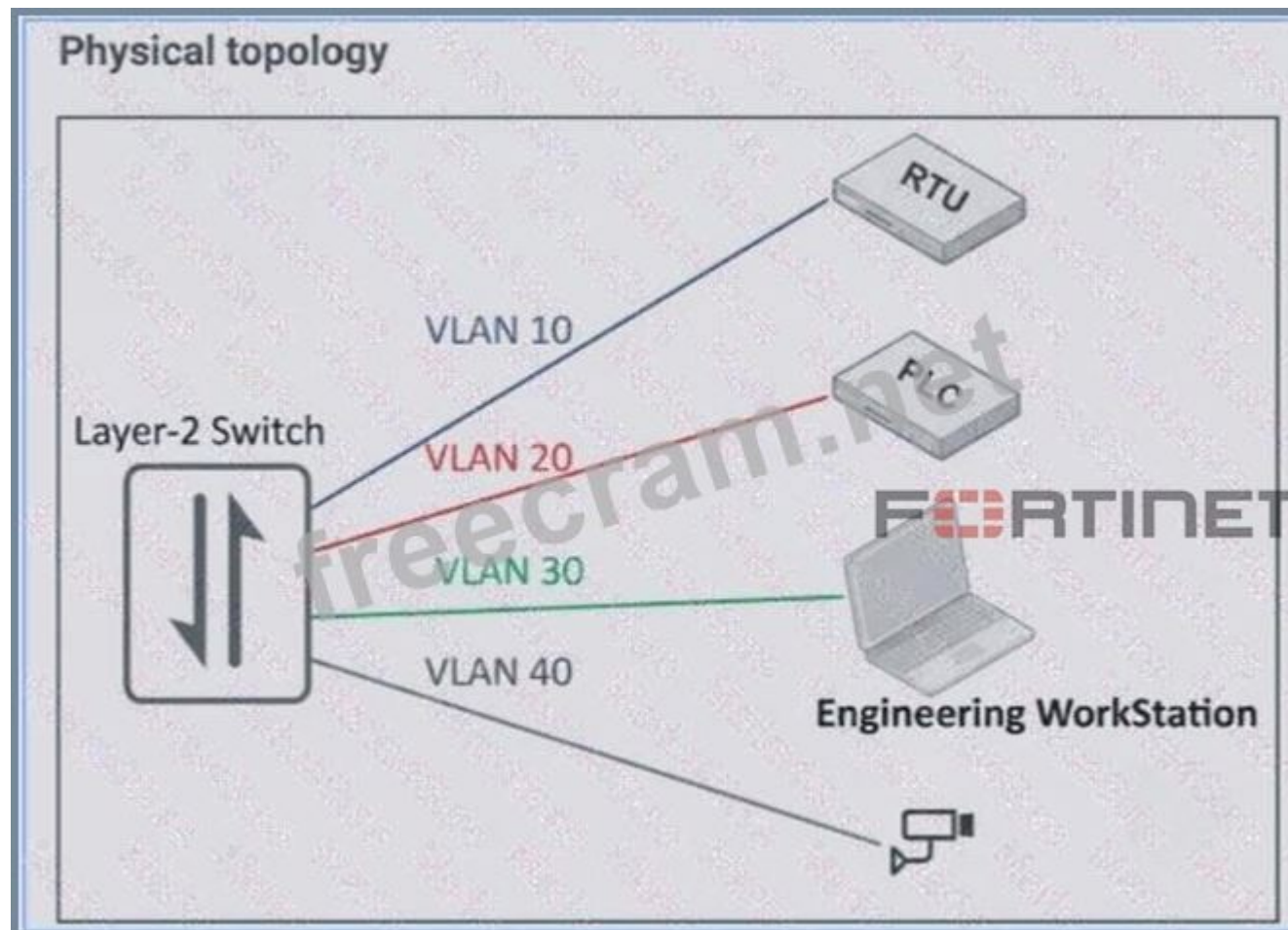
D. Remove centralized network security policies.

Answer: ([SHOW ANSWER](#))

The primary objective of implementing SD-WAN in operational technology (OT) networks is to enhance the performance and reliability of OT applications. SD-WAN optimizes traffic routing based on application requirements, network conditions, and business priorities, ensuring low latency and high availability for critical OT applications. This is essential in OT environments, where the performance of applications directly impacts operational efficiency and safety.

NEW QUESTION: 37

Refer to the exhibit.



A partial OT network is shown. You have configured the FortiGate device with VLANs to segment the OT network. The supervisor now wants to connect to the PLC from the Engineering Workstation. How can you allow access from the Engineering Workstation to the PLC? (Choose one answer)

- A. You must configure intra-switch-policy as explicit.
- B. You must configure intra-switch-policy as implicit.
- C. You must configure forward domain IDs.
- D. You must configure a layer 3 switch.

Answer: ([SHOW ANSWER](#))

The correct answer is D. You must configure a layer 3 switch .

The study guide explains that "Layer 2 devices can add or remove tags" but "cannot modify them." It then states that "A layer 3 device, such as a router or FortiGate, can modify the VLAN tag before routing the packet. This allows them to route traffic between VLANs." It also explicitly describes

"Router on a Stick" as "a way to allow routing between VLANs." Since the exhibit shows a layer-2 switch and the Engineering Workstation and PLC are placed in different VLANs, inter-VLAN communication requires layer-3 routing.

The other options do not solve this requirement. intra-switch-policy explicit/implicit applies to a software switch , where member interfaces are in the same broadcast domain and same subnet, not to routing between separate VLANs. forward domain IDs are used in transparent mode to confine broadcasts to specific broadcast domains; they do not provide inter-VLAN access. Therefore, to let the Engineering Workstation in one VLAN reach the PLC in another VLAN, you need a layer 3 routing function , which matches option D .

NEW QUESTION: 38

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.

Answer: ([SHOW ANSWER](#))

Modbus is master/slave: the master (primary) polls; a slave (secondary) replies only when requested. That fits "secondary sends data based on request from primary device."

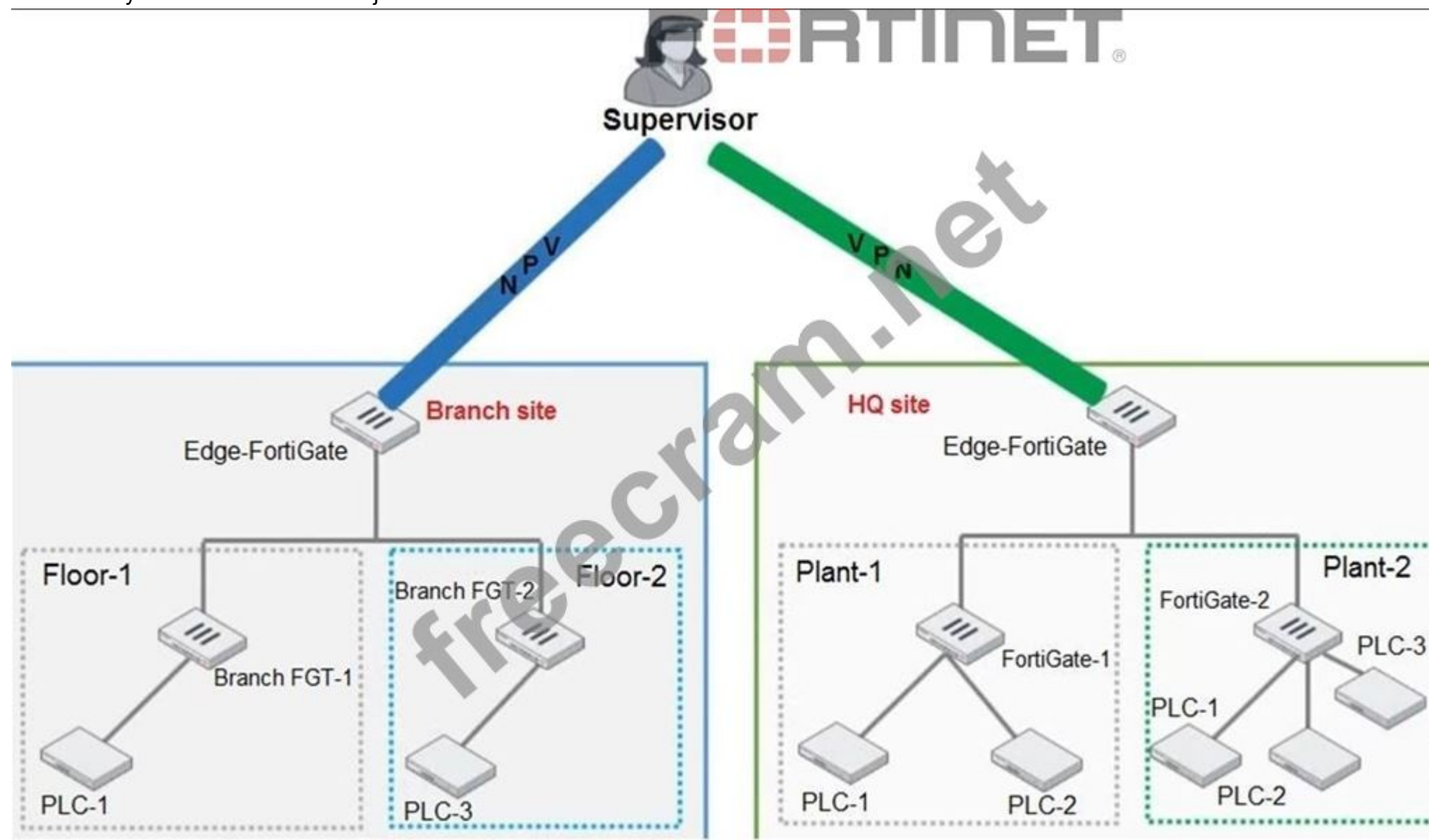
NEW QUESTION: 39

Refer to the exhibit, which shows a nonprotected OT environment. An administrator needs to implement appropriate protection on the OT network.

Which three steps should an administrator take to protect the OT network? (Choose three.)

NEW QUESTION: 40

Refer to the exhibit. You need to configure VPN user access for supervisors at the branch 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 register the same FortiToken on more than one FortiGate.
- B. You must use a third-party RADIUS OTP server.
- C. You must use the user self-registration server.
- D. You must use a FortiAuthenticator.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 41

Which two statements about FortiSIEM are true? (Choose two.)

- A. FortiSIEM can receive and collect data from network devices and applications.
- B. FortiSIEM can receive data from certain devices in SQL format.
- C. FortiSIEM can receive data from any network device and application.
- D. FortiSIEM cannot receive data from a Windows server without an agent.

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 42

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: ([SHOW ANSWER](#))

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.

NEW QUESTION: 43

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

Answer: ([SHOW ANSWER](#))

Planning a threat hunting strategy is essential for proactively searching for threats and vulnerabilities in the OT environment before they manifest into attacks.

Evaluating what can go wrong before it happens is a core part of risk assessment, involving the identification and analysis of potential risks and their impacts on OT systems.

Implementing strategies to automatically bring PLCs offline is generally not a responsible or safe approach in OT environments because it could disrupt critical industrial processes.

Creating disaster recovery plans is important for overall business continuity but is not primarily a task of auditors during risk assessment-it is more of a broader business continuity or incident response responsibility.

NEW QUESTION: 44

A supervisor is configuring a software switch on a FortiGate device. What must the supervisor configure on FortiGate to control the traffic between member interfaces on the software switch, using firewall policies?

- A. The supervisor must add different VLAN interfaces to the software switch.
- B. The supervisor must configure the software switch with at least one wireless interface and one VLAN interface.
- C. The supervisor must configure intra-switch-policy to explicit.
- D. The supervisor must configure a separate forward domain for the software switch.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 45

Refer to the exhibit. Which statement about the interfaces shown in the exhibit is true?

	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

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 46

Which two of the following features do most industrial protocols lack? (Choose two.)

- A. Real-time data exchange
- B. Deterministic timing
- C. TLS encryption
- D. Authentication

Answer: ([SHOW ANSWER](#))

Most legacy OT/industrial protocols were built for speed and determinism, not security, so they typically omit built-in TLS encryption and authentication mechanisms.

Valid NSE6_OTS_AR-7.6 Dumps shared by EduDump.com for Helping Passing NSE6_OTS_AR-7.6 Exam! EduDump.com now offer the newest NSE6_OTS_AR-7.6 exam dumps, the EduDump.com NSE6_OTS_AR-7.6 exam questions have been updated and answers have been corrected get the newest EduDump.com NSE6_OTS_AR-7.6 dumps with Test Engine here: https://www.edudump.com/exams/Fortinet/NSE6_OTS_AR-7.6/premium/ (153 Q&As Dumps, 35%OFF Special Discount Code: freecram)

NEW QUESTION: 47

Refer to the exhibits.

Partial Incident Analysis page

Incident Analysis

High

IPS_Attack_Handling: dstip:192.168.2.3 IN00000005

Toggle Widget

Save

Reset

Undo

Rollback

Columns

Incident Summary

Incident Number

IN00000005

Incident Name

IPS_Attack_Handling: dstip:192.168.2.3

Incident Date / Time

2025-11-23 05:47:50

Incident Update Date / Time

2025-11-23 07:14:40

Incident Category

Denial of Service (DoS)

MITRE Tech ID

Click to select

Severity

High Brave-Dumps.com

Status

New

Affected Endpoint

10.1.5.20

Description

Brave-Dumps.com

Assigned To

Not Assigned

Affected Endpoint/User

No related user available.

Last Seen

2025-11-23 05:47:50

Topology

10.1.5.20

Addresses

MAC: bc:24:11:8a:69:8f
IP: 10.1.5.20

Operating System

Unknown

Brave-Dumps.com

Comments

Brave-Dumps.com

POST

Affected Assets

Endpoint	User	IP Address	MAC Address
10.1.5.20	No enough info	10.1.5.20	bc:24:11:8a:69:8f

Brave-Dumps.com

Events

View Logs

Search in Log View

Dismiss

Details

Event	Count	Severity	Suppress	Outbreak Name	Last Occurrence	Handler	Indicators
User login/logout failed	2	High			2025-11-23 05:47:50	Local Device Event	Brave-Dumps.com

Log details related to the event

logDetails	
Action	dropped
Action	dropped
Attack ID	37447
Attack Name	Triangle.Research.Nano-10.PLC.Crafted.Packet.Data.Length.DoS
CVE ID	CVE-2013-5741
Date	2025-11-23
Date/Time	2025-11-23 05:47:44
Destination City	ReservedBrave-Dumps.com
Destination Country	Reserved
Destination End User ID	3
Destination Endpoint ID	101
Destination Geo ID	1000000000
Destination IP	192.168.2.3
Destination Interface	port2
Destination Interface ...	undefined
Destination Port	502
Device ID	FGVMSLUM25008487
Device Name	Edge-PortGate
Device Time	2025-11-23 05:47:44
Device Time Zone	UTC
Direction	outgoing
Event Time	2025-11-23 05:47:44.767674046
Event Type	signatureBrave-Dumps.com
Host Name	192.168.2.3
Incident Serial No.	234881260
Severity	Alert
Log Flag	0
Log ID	0419016384
Message	SCADA: Triangle.Research.Nano-10.PLC.Crafted.Packet.Data.Length.DoS
Policy ID	7
Policy Type	policyBrave-Dumps.com
Policy UUID	00ce3004-9f70-51f0-c4e0-8eaaa4753fa0
Profile	high_security
Protocol	6

A partial Incident Analysis page and the log details related to the event are shown. An attack is reported on your OT network. You analyze the corresponding incident. Based on the information provided on the Incident Analysis page and the log details, which two statements are correct? (Choose two answers)

- A. The attack uses the Modbus protocol.
- B. The attack is mitigated.
- C. The attack uses the IEC 104 protocol.
- D. The event severity is high.
- E. The target device IP address is 10.1.5.20.

Answer: (SHOW ANSWER)

Based on the technical data provided in the exhibits and the OT Security 7.6 Architect curriculum:

* Industrial Protocol Identification (Statement A) : The log details exhibit clearly shows that the Destination Port used in the attack is 502 . According to the study guide ' s section on Industrial Protocol Protection , the standard port used by the Modbus TCP protocol is 502 . Furthermore, the attack name identifies a " Triangle.Research.Nano-10.PLC, " which are industrial controllers commonly utilizing Modbus for communications.

* Attack Mitigation (Statement B) : The log details specify that the Action taken by the FortiGate (Edge-FortiGate) was dropped . In cybersecurity and Fortinet fabric operations, dropping a packet associated with an IPS signature means the traffic was blocked from reaching its target, thereby mitigating the attack.

* Target IP Address (Statement E) : The log detail explicitly lists the Destination IP as 192.168.2.3 .

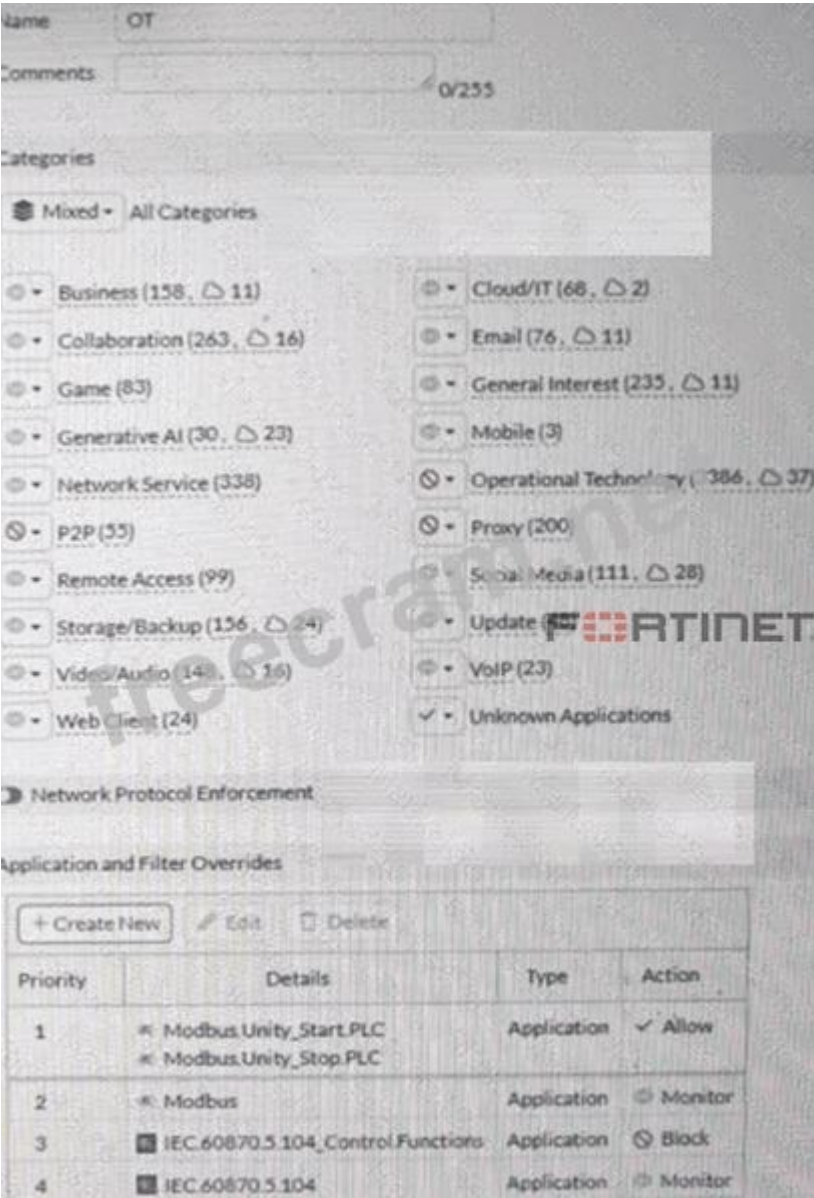
The Incident Analysis page also titles the incident with dstip:192.168.2.3. While the " Affected Endpoint " is shown as 10.1.5.20 , in an " outgoing " attack direction (as shown in the log), this likely refers to the internal source/attacker IP, whereas the target is the destination IP (192.168.2.3). Thus, Statement E is incorrect.

* Protocol Conflict (Statement C) : The IEC 104 protocol typically utilizes port 2404 . Since the log specifies port 502, Statement C is incorrect.

* Severity Distinction (Statement D) : While the Incident severity is marked as High , the question specifically asks about event severity. The " Events " table at the bottom of the Incident Analysis page shows a " User login/logout failed " event with a medium severity. Because there is a distinction in the management console between the severity of individual events and the aggregated incident, and Statement A and B are technically definitive based on port and action, A and B are the correct architectural choices.

NEW QUESTION: 48

Refer to the exhibit.



A partial Application Sensor profile is shown. When you apply this profile in a firewall policy, which two statements are correct? (Choose two answers)

- A. A log is provided for each IEC command.
- B. A log is provided for each Modbus command.
- C. OT signatures are enabled.
- D. All OT protocols are blocked.

Answer: (SHOW ANSWER)

The correct answers are A and C .

Option C is correct because the profile clearly contains the Operational Technology category and specific OT application signatures such as Modbus and IEC.60870.5.104 . The study guide says "You can use application control signatures to detect OT protocols" and "You can filter to a specific OT protocol." That means OT application signatures are active in this sensor profile.

Option A is correct because the guide explains that application control works at different levels: "Detection of protocol (one detection per session)" and "Message level (one detection per protocol message)." It also says you can use application signatures for "granular message type identification." In the exhibit, IEC.

60870.5.104.Control.Functions is explicitly configured, which is a granular IEC message/control-level signature rather than only a protocol-level match. That means logging and control can occur at the IEC command level.

Option B is not correct because the profile shows Modbus configured at the parent protocol level as Monitor, while the guide states that the "parent signature takes precedence over the child signature." Since protocol-level detection is one detection per session, that does not mean FortiGate will necessarily log each Modbus command individually.

Option D is incorrect because even though the broader Operational Technology category is set to block, the profile includes specific application and filter overrides for Modbus and IEC 104 behavior. So the resulting effect is not simply that all OT protocols are blocked.

NEW QUESTION: 49

Refer to the exhibits.



A partial Basic Event Handler page on FortiAnalyzer and the creation of a trigger in a FortiGate device are shown. To improve the protection of your OT network, you want to automate the handling of compromised devices notified through FortiAnalyzer. You have configured an event handler named Alert_trigger as shown in the exhibit. When you create the trigger on the FortiGate device, the Event handler name field does not provide the Alert_trigger option. What two actions must you perform to make the Alert_trigger option available? (Choose two answers)

- A. You must click + Create in the Event handler name field.
- B. You must authorize the FortiGate device on FortiAnalyzer.

- C. You must configure the FortiAnalyzer setting on the FortiGate device.
- D. You must configure the trigger on the root FortiGate.

Answer: (SHOW ANSWER)

The correct answers are C and D .

Option C is correct because the study guide explains that when "a handler generates an event with the automation stitch option enabled, FortiAnalyzer sends a notification" and, in the Security Fabric workflow, "FortiAnalyzer parses the logs and notifies the root FortiGate." This means FortiGate must first have the FortiAnalyzer connection configured so it can consume FortiAnalyzer event handlers and use them in automation. The wizard message in the exhibit also points to this requirement by indicating that a FortiAnalyzer connection must be configured.

Option D is also correct because the study guide explicitly says that in this automation flow "the root FortiGate triggers the action" and shows "Stitches configured on root FortiGate." Therefore, if you want the FortiAnalyzer event handler to appear and be usable for automation, the trigger must be configured on the root FortiGate , not on an arbitrary downstream FortiGate.

Option A is incorrect because + Create is only a GUI control and does not solve the missing-event-handler visibility problem. Option B is not identified in the study guide as the requirement for making a FortiAnalyzer event handler available in the FortiGate automation trigger list.

NEW QUESTION: 50

Refer to the exhibit.



A Virtual Patching profile is shown. You have recently updated your SCADA system and would like to apply the SCADA virtual patching profile. Which two statements about this profile are correct? (Choose two answers)

- A. Only the vulnerability Schneider.Electric.ClearSCADA.HTTP.Interface.XSS is still present.
- B. Low severity signatures are not blocked for the device with the MAC address 12:12:12:12:12:12.
- C. This profile blocks critical severity signatures for all the devices.
- D. The device with the MAC address 11:11:11:11:11:11 is considered to have no vulnerabilities.

Answer: ([SHOW ANSWER](#))

The correct answers are B and D .

Option B is correct because the profile has Medium , High , and Critical selected, while Low severity is not selected. That means low-severity virtual patching signatures are not enforced by this profile. So for the device with MAC address 12:12:12:12:12 , low-severity signatures are not blocked. The study guide explains virtual patching as device-specific protection where "FortiGate caches the signatures and mitigation rules that apply to each device" and applies them when the related traffic matches the firewall policy.

Option D is correct because the Virtual Patching Exemptions table shows a row with the MAC address 11:

11:11:11:11 and no specific signature listed. The study guide states that in the Virtual Patching profile you can "Exempt a specific device with the MAC address or a specific signature." A MAC-only exemption means that specific device is excluded from virtual patching enforcement, so in practical terms it is treated as having no applicable vulnerabilities in this profile.

Option C is incorrect because the profile does not block critical signatures for all devices. The exemptions list proves that at least one device can be excluded by MAC address, and a specific signature can also be exempted. Therefore, enforcement is not universal across all devices.

Option A is incorrect because the entry Schneider.Electric.ClearSCADA.HTTP.Interface.XSS appears as a specific signature exemption , not as the only remaining vulnerability. The profile display is showing exemptions, not a statement that only one vulnerability is still present.

NEW QUESTION: 51

What is the main OT component for monitoring and controlling industrial processes? (Choose one answer)

- A.** Programmable Logical Controller (PLC)
- B.** Supervisory Control and Data Acquisition (SCADA)
- C.** Industrial Control System (ICS)
- D.** Industrial Internet of Things (IIoT)

Answer: ([SHOW ANSWER](#))

The correct answer is C. Industrial Control System (ICS) . The study guide states that "ICS is a main component of OT" and "consists of systems used for monitoring and controlling industrial processes." It also explains that ICS includes various devices, systems, controls, and networks that manage industrial processes, and that the most common types are SCADA and distributed control systems (DCS) . This makes ICS the primary OT component for monitoring and controlling industrial processes.

The other options are related OT components, but they are not the best answer to this wording. SCADA collects real-time data and helps visualize and control the OT environment, but it is described as a system within the broader ICS structure. PLC devices collect and transmit real-time data and connect sensors and RTUs to SCADA, while IIoT refers to sensors, actuators, and other connected field devices. Therefore, the overarching main OT component for monitoring and controlling industrial processes is ICS .

NEW QUESTION: 52

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: ([SHOW ANSWER](#))

Local authentication on a FortiGate and two-factor authentication via FortiAuthenticator both require the user to actively present credentials (and an OTP), which is the essence of active authentication.

NEW QUESTION: 53

You want to monitor the performance of your specific OT sensors. Where must you fine-tune the event handling for these sensors on FortiSIEM?

- A.** In the Risk Summary section on the Dashboard tab

- B.** In the rule on the Resources tab
- C.** In the Investigation section on the Analytics tab
- D.** In the business services group on the CMDB tab

Answer: ([SHOW ANSWER](#))

Fine-tuning event handling for specific sensors in FortiSIEM is done within the rule configuration, where conditions, thresholds, and logic are adjusted to control how events are generated and processed.

NEW QUESTION: 54

According to the IEC 62443 standard, your security level is 4 . What is your OT environment defending against? (Choose one answer)

- A.** Intentional cyberthreats posed by skilled malicious users
- B.** An intentional attack with low resources
- C.** A syndicate of cyber extortion with extensive resources
- D.** A casual exposure

Answer: ([SHOW ANSWER](#))

According to the OT Security 7.6 Architect study guide regarding IEC 62443 Security Levels :

* Security Level 4 (SL 4) Definition : This level provides " Protection against intentional violation using sophisticated means with extended resources, specific skills, and high motivation " .

* Real-World Application : The study guide specifically notes: " If you are facing a syndicate of cyber extortionists with extensive resources and capabilities, then you should strive for security level 4 " .

* Comparison to other levels :

* SL 1 : Protection against " casual or unintentional system violation " .

* SL 2 : Protection against " intentional violation using simple means with low resources " .

* SL 3 : Protection against " intentional violation using sophisticated means with moderate resources " .

NEW QUESTION: 55

Refer to the exhibit.

Partial Application Sensor profile

Name: OT

Comments: 0/255

Categories

☒ Mixed • All Categories

- ☐ Business (158, 11)
- ☐ Collaboration (263, 16)
- ☐ Game (83)
- ☐ Generative AI (30, 23)
- ☐ Network Service (336)
- ☒ P2P (55)
- ☐ Remote Access (99)
- ☐ Storage/Backup (156, 24)
- ☐ Video/Audio (148, 16)
- ☐ Web Client (24)
- ☐ Cloud/IT (68, 2)
- ☐ Email (77)
- ☐ General Internet (235, 11)
- ☐ Mobile (3)
- ☐ Operational Technology (3366, 3)
- ☐ Proxy (200)
- ☐ Social Media (111, 28)
- ☐ Update (48)
- ☐ VoIP (23)
- ☒ Unknown Applications

☒ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	Modbus_Read.Holding.Registers	Application	✓ Allow
2	Modbus	Application	⊗ Block

A partial Application Sensor profile is shown. When you apply this profile in firewall policy, which two statements are correct? (Choose two answers)

- A. OT signatures are enabled.
- B. All OT protocols are monitored.
- C. Modbus write commands are blocked.
- D. A log is provided for each Modbus read holding registers command.

Answer: (SHOW ANSWER)

The correct answers are A and C . The study guide explains that "You can use application control signatures to detect OT protocols" and that application control provides "granular message type identification." In the exhibit, the Operational Technology application category is included in the Application Sensor profile, so OT application signatures are enabled in this profile.

Option C is also correct because the override table shows Modbus_Read.Holding.Registers = Allow and Modbus = Block . The study guide states that you can use specific granular application control signatures to allow a specific Modbus command and block all others , and it also shows that application control can identify read and write commands separately at message level.

Therefore, Modbus write commands are blocked by this profile.

Option B is incorrect because the profile is not simply monitoring all OT protocols; it contains a Block action for Modbus. Option D is incorrect because the study guide links OT protocol visibility specifically to the monitor status , while in the exhibit Modbus_Read.Holding.Registers is set to Allow , not Monitor .

NEW QUESTION: 56

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: ([SHOW ANSWER](#))

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

NEW QUESTION: 57

As an OT network administrator, you are required to generate reports that primarily use the same type of data sent to FortiSIEM. These reports are based on the preloaded analytic searches. Which two actions can you take on FortiSIEM to enhance running reports for future use? (Choose two.)

- A.** Create custom reports to process additional analytic searches.
- B.** Export the preloaded analytics searches to an external syslog server
- C.** Save the analytic searches and turn them into report definitions.
- D.** Automate running these reports upon receiving new logs

Answer: ([SHOW ANSWER](#))

Create custom reports to process additional analytic searches: FortiSIEM allows you to create custom reports tailored to specific requirements. This is useful if the preloaded analytic searches do not completely fulfill your reporting needs or if additional data processing is required.

Save the analytic searches and turn them into report definitions: FortiSIEM enables you to save analytic searches and convert them into reusable report definitions. These report definitions can then be used to generate consistent reports based on the same criteria in the future.

NEW QUESTION: 58

Refer to the exhibit. An operational technology (OT) network security audit concluded that the application sensor does not block the IEC.60870.5.104_Information.Trasfer.C.BO.NA.1 signature. Which change must the OT network administrator make?

Application control

New Application Sensor

110 Cloud Applications require deep inspection.
0 policies are using this profile.

Name

Comments 0/255

Categories

☒ All Categories

☒ Business (153, 6)

☒ Game (86)

☒ Network.Service (333)

☒ Social.Media (117, 30)

☒ VoIP (23)

☒ Cloud.IT (67, 1)

☒ General.Interest (236, 9)

☒ P2P (56)

☒ Storage.Backup (161, 19)

☒ Web.Client (24)

☒ Collaboration (267, 16)

☒ Industrial (225)

☒ Proxy (180)

☒ Update (49)

☒ Unknown Applications

☒ Email (77, 12)

☒ Mobile (3)

☒ Remote.Access (97)

☒ Video/Audio (153, 17)

☐ Network Protocol Enforcement

Application and Filter Overrides

+ Create New

Edit

Delete

Priority	Details	Type	Action
1	IEC.60870.5.104_Information.Transfer IEC.60870.5.104_Control.Functions IEC.60870.5.104_Control.Functions.STARTDT.ACT IEC.60870.5.104_Control.Functions.STARTDT.CON	Application	Monitor
2	IEC.60870.5.104_Information.Transfer.C.BO.NA.1	Application	Block

2

- A. Set all application categories to apply default actions.
- B. Change the security action of the industrial category to monitor.
- C. Update the priority of the C.BO.NA.1 signature override to 1.
- D. Remove IEC.60870.5.104_Information.Transfer.C.BO.NA.1 from the first filter override.

Answer: [\(SHOW ANSWER\)](#)

The current configuration assigns priority 2 to the IEC.60870.5.104_Information.Transfer.C.BO.NA.1 application signature and sets it to Block. Priority 1 contains broader IEC.60870.5.104_Information.Transfer entries set to Monitor, which overrides the block action due to higher priority. To ensure that the C.BO.NA.1 signature is blocked, it must have higher priority than the general monitoring rule.

NEW QUESTION: 59

Drag and Drop Question

Match each industrial protocol to its corresponding characteristics.
Select each OT industrial protocol in the column on the left and drag and drop it into the blank space next to its corresponding characteristics in the column on the right. After matching a device type to its characteristics, you can move it again if you want to change your answer by clicking the industrial protocol name. You must match all four industrial protocols to their characteristics in the work area.

Industrial protocol

EtherCAT

POWERLINK

Modbus

Ethernet over industrial protocol

Characteristics

Mainly used for the transmission of process data

Offers real-time data transmission in primary-secondary configuration

Uses client/server communication

Based entirely on Ethernet standards

Answer:

Industrial protocol

EtherCAT

POWERLINK

Modbus

Ethernet over industrial protocol

Characteristics

EtherCAT

POWERLINK

Modbus

Ethernet over industrial protocol

Mainly used for the transmission of process data

Offers real-time data transmission in primary-secondary configuration

Uses client/server communication

Based entirely on Ethernet standards

NEW QUESTION: 60

Refer to the exhibits. A partial Basic Event Handler page on FortiAnalyzer and the creation of a trigger in a FortiGate device are shown.

Partial Basic Event Handler page

Edit Basic Event Handler

Status: ☒ Alert_trigger

Description:

MITRE Tech ID:

Data Selector:

Automation Stitch: ☒

Creation of a trigger

Create New Automation Trigger

FortiAnalyzer Event Handler: A specified FortiAnalyzer event handler was triggered.

Name:

Description:

FortiAnalyzer Event Handler

Configure a FortiAnalyzer connection to utilize FortiAnalyzer event handlers:

- FortiAnalyzer

Event handler name:

Event settings: ☐

To improve the protection of your OT network, you want to automate the handling of compromised devices notified through FortiAnalyzer.

You have configured an event handler as shown in the exhibit. When you create the trigger on the FortiGate device, the Event handler name field does not provide the Alert_trigger option.

What two actions must you perform to make the Alert_trigger option available? (Choose two answers)

- A. You must click + Create in the Event handler name field.
- B. You must configure the FortiAnalyzer setting on the FortiGate device.
- C. You must authorize the FortiGate device on FortiAnalyzer
- D. You must configure the trigger on the root FortiGate.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 61

Which statement is correct about processing matched rogue devices by FortiNAC?

- A. FortiNAC cannot revalidate matched devices.
- B. FortiNAC remembers the matching rule of the rogue device.
- C. FortiNAC disables matching rule of previously-profiled rogue devices.

D. FortiNAC matches the rogue device with only one device profiling rule.

Answer: ([SHOW ANSWER](#))

When FortiNAC matches a rogue device to a profiling rule, it remembers that matching rule.

FortiNAC revalidates the device against that rule each time it connects or at user-defined intervals.

If the device no longer matches the rule on revalidation, FortiNAC can automatically disable the device as a safeguard.

FortiNAC does not disable matching rules for previously profiled rogue devices, nor does it match a rogue device with only one profiling rule exclusively. Profiling rules can be multiple, but the device is associated with the rule it first matched.

Valid NSE6_OTS_AR-7.6 Dumps shared by EduDump.com for Helping Passing NSE6_OTS_AR-7.6 Exam! EduDump.com now offer the **newest NSE6_OTS_AR-7.6 exam dumps**, the EduDump.com NSE6_OTS_AR-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com NSE6_OTS_AR-7.6 dumps with Test Engine here: https://www.edudump.com/exams/Fortinet/NSE6_OTS_AR-7.6/premium/ (153 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 62

When device profiling rules are enabled, which devices connected on the network are evaluated by the device profiling rules?

- A. All connected devices, each time they connect
- B. Known trusted devices, each time they change location
- C. Rogue devices, each time they connect
- D. Rogue devices, only when they connect for the first time

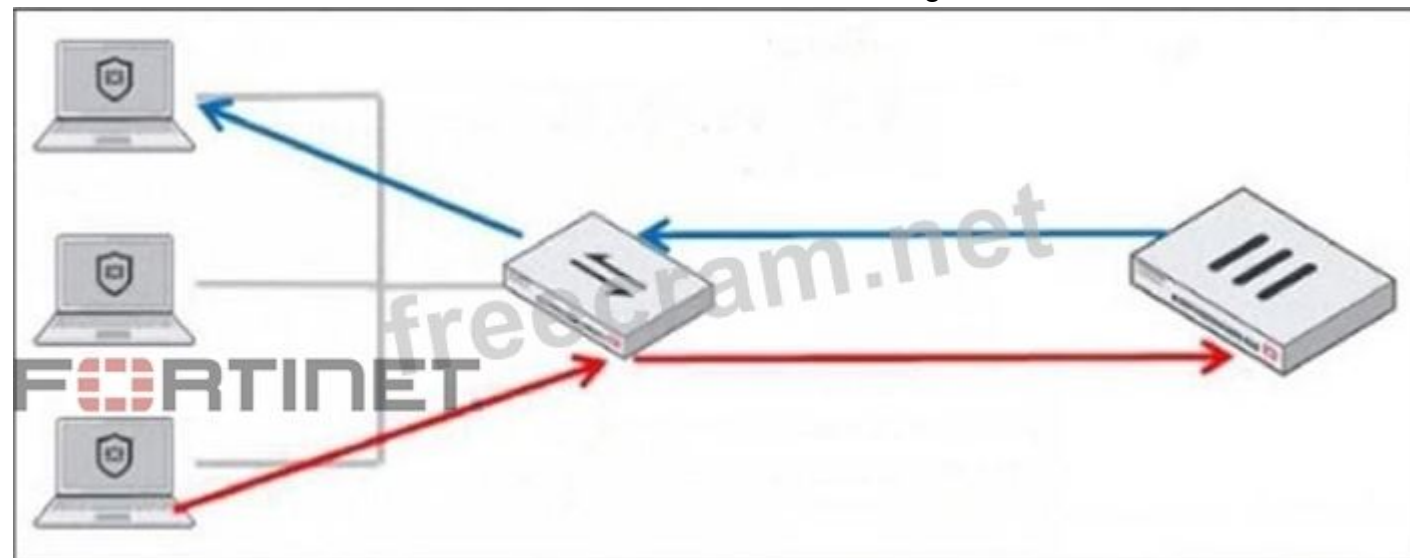
Answer: ([SHOW ANSWER](#))

NEW QUESTION: 63

Refer to the exhibit. An OT network architect must implement inter-VLAN routing in the topology.

Traffic from each client is tagged with a unique VLAN. Each client is directly connected to a Layer 2 switch.

Which action must the OT network architect take to achieve this goal?



- A. Make FortiGate a router on a stick.
- B. Set the same forward domain on each switch interface.

- C. Configure a software switch to handle traffic for each client.
- D. Replace the switch with a Layer 3 device.

Answer: A ([LEAVE A REPLY](#))

With clients in separate VLANs on a Layer 2 switch, inter-VLAN traffic must be routed. Creating VLAN subinterfaces on a single FortiGate physical port ("router on a stick") lets the FortiGate route and apply policy between those VLANs.

NEW QUESTION: 64

Refer to the exhibit.



The OT devices behind the ruggedized FortiGate have vulnerabilities and you want to apply a virtual patching profile in the firewall policy. Why is Virtual Patching not available in the Security Profiles section? (Choose one answer)

- A. You must enable Virtual Patching in the Feature Visibility section.
- B. You must have a ruggedized FortiGate allowing the virtual patching feature.
- C. You must enable OT signatures.
- D. You must have a valid OT security service license.

Answer: (SHOW ANSWER)

The correct answer is A. You must enable Virtual Patching in the Feature Visibility section .

The study guide states clearly that "By default, virtual patching profiles are hidden on the GUI, and you must enable them through System > Feature Visibility." That exactly matches the situation in the exhibit, where Virtual Patching does not appear under Security Profiles . So the issue is not that the feature is unsupported, but that it is simply hidden in the GUI until it is enabled.

The other options do not answer the question being asked. A valid OT security service license is required for virtual patching signatures and protection workflow, and OT signatures are relevant to IPS-based OT protection, but those do not explain why the menu item itself is missing from the Security Profiles section .

The guide specifically identifies Feature Visibility as the reason the Virtual Patching profile is not shown in the GUI. Therefore, the required action is to enable Virtual Patching in System > Feature Visibility .

NEW QUESTION: 65

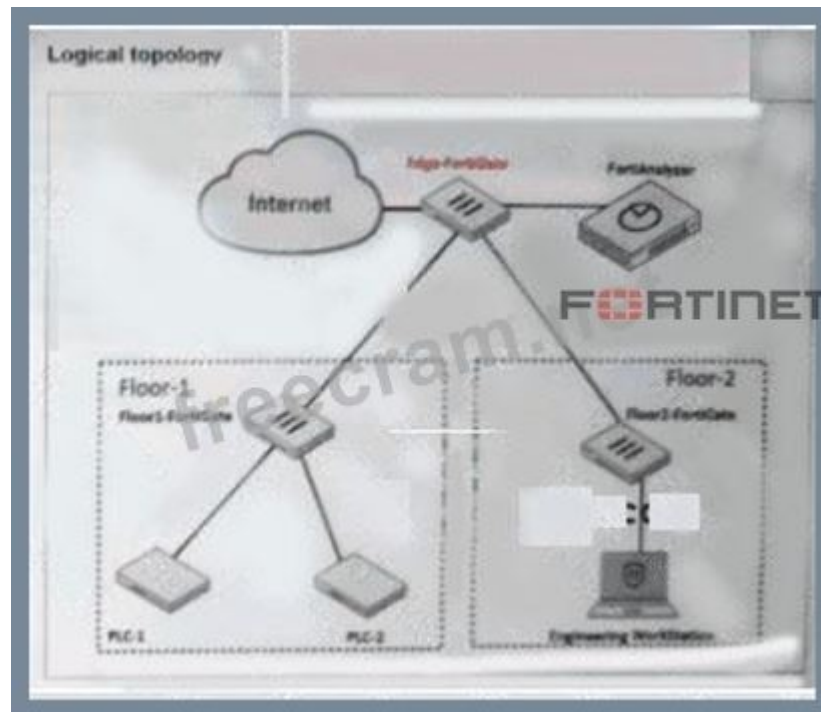
What is the next step if FortiGate cannot detect a device locally? (Choose one answer)

- A. FortiGate queries the local device database (CIDB).
- B. FortiGate queries OT servers through service connectors.
- C. FortiGate queries FortiGuard servers.
- D. FortiGate queries the profiling rules.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 66

Refer to the exhibit.



A partial OT network is shown. You want to configure an automated alert sent by FortiAnalyzer when an attack occurs on a FortiGate device. Which two configurations must you implement? (Choose two answers)

- A. You must configure a stitch on the root FortiGate.
- B. You must configure a LOCALHOST task in the FortiAnalyzer playbook.
- C. You must configure an intrusion prevention security profile on all FortiGate devices.
- D. You must configure an event handler on FortiAnalyzer.

Answer: ([SHOW ANSWER](#))

The correct answers are A and D . The study guide provides a direct use case called Attack Detection and Automated Alert . It states: "A downstream FortiGate detects an attack and sends logs to FortiAnalyzer. FortiAnalyzer parses the logs and notifies the root FortiGate. The root FortiGate triggers the action, which in this case, is a notification to the administrator." The same slide also explicitly shows "Stitches configured on root FortiGate." This confirms that to send the automated alert, you must configure the automation stitch on the root FortiGate .

The second required configuration is an event handler on FortiAnalyzer . The guide explains that "Event handlers generate events" and that "FortiAnalyzer uses event handlers to filter all incoming logs. If logs match the conditions configured in an event handler, FortiAnalyzer generates an event." Since FortiAnalyzer must detect the attack from the received logs before notifying the root FortiGate, an event handler is required on FortiAnalyzer.

Option B is incorrect because the study guide does not identify a LOCALHOST task as the required configuration for this attack-alert flow. Option C is also incorrect because the question asks what must be configured to enable the automated alert workflow . An IPS profile may detect some attacks, but the required automation path in the study guide is specifically event handler on FortiAnalyzer + stitch on the root FortiGate .

NEW QUESTION: 67

You want to improve access control for your large OT network using passive authentication. What must you configure on FortiGate? (Choose one answer)

- A. Fortinet Single-Sign On (FSSO)
- B. Local users
- C. Two-factor authentication

D. A FortiAuthenticator device as a remote server

Answer: ([SHOW ANSWER](#))

The correct answer is A. Fortinet Single-Sign On (FSSO) . The study guide states under Active and Passive Authentication that for passive authentication, "User does not receive a login prompt from FortiGate" ,

"Credentials are determined automatically" , and specifically "FSSO, RSSO, and NTLM can be used." It then explains that passive authentication occurs with the single sign-on method and explicitly identifies Fortinet SSO (FSSO) as one of those methods.

The guide also says: "For passive authentication, you can implement FSSO. FSSO allows users who have already authenticated on the network through another system to be transparently identified. After initial login to any system on the network, users can access allowed resources without being prompted for credentials." That is exactly what the question asks for: improving access control in a large OT network using passive authentication .

The other options do not match passive authentication. Local users are part of local authentication, two- factor authentication adds an extra security factor but still uses active authentication, and FortiAuthenticator as a remote server supports centralized authentication for mid-to-large networks, but by itself it is not the specific passive-authentication method being asked here. The study guide is explicit that the FortiGate configuration for passive authentication is FSSO .

NEW QUESTION: 68

You want to improve access control for your large OT network using passive authentication. What must you configure on FortiGate?

A. A FortiAuthenticator device as a remote server

B. Local users

C. Two-factor authentication

D. Fortinet Single-Sign On (FSSO)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 69

What triggers Layer 2 polling of infrastructure devices connected in the network?

A. A matched profiling rule

B. A linkup or linkdown trap

C. A matched security policy

D. A failed Layer 3 poll

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 70

As the first step in your OT network protection plan, you must identify the OT protocols that the FortiGate device supports. Which two configurations must you implement on this FortiGate device?
(Choose two answers)

A. You must enable Device detection on all the interfaces.

B. You must implement an Application Control security profile that monitors OT.

C. You must enable the OT signatures.

D. You must implement an Intrusion Prevention security profile that monitors OT.

Answer: ([SHOW ANSWER](#))

The correct answers are B and C . The study guide states that "You can use application control signatures to detect OT protocols" and that "Application control detects the protocols used in applications like Modbus, IEC 104, and the contents of the telecontrol messages" . It also shows that a Modbus application control profile can be enabled on a firewall policy "for OT protocol visibility in the monitor status." This directly supports B , because application control is the feature used to identify and monitor OT protocols on FortiGate.

The guide also explains under IPS that "By default, OT signatures are excluded from the signatures lists on the GUI until you enable them on the CLI" using `config ips global and set exclude-signatures none`.

Once enabled, FortiGate can use those OT signatures for OT-aware inspection and protection. That supports C as the second required configuration. A is related to device discovery, not protocol identification, and D is focused on exploit and vulnerability detection rather than the first-step goal of identifying OT protocols.

NEW QUESTION: 71

Refer to the exhibit. The IPS profile is added on all of the security policies on FortiGate. For an OT network, which statement of the IPS profile is true?

Add Signatures

Type

FilterSignature

Action

Default

Packet logging

EnableDisable

Status

EnableDisableDefault

Filter

APPSCADA

Search

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 507					
7T.IGSS.ODBC.Server.Memory.Corruption		Server	Windows	Block	
7Technologies.IGSS.SCADA.System.Directory...		Server	Windows	Pass	CVE-2011-1565 CVE-2011-1566
A32S.Botnet		Server Client	All	Block	
AAEH.Botnet		Server	All	Block	
AARC.Botnet		Server Client	All	Block	
ABB.MicroSCADA.Wserver.Command.Execut...		Server	Windows	Block	
ABB.Multiple.Products.RobNetScanHost.exe...		Server	Windows	Block	CVE-2012-0245

0%507

OK

Cancel

- A. FortiGate has no IPS industrial signature database enabled.
- B. The listed IPS signatures are classified as SCADA applications.
- C. All IPS signatures are overridden and must block traffic match signature patterns.
- D. The IPS profile inspects only traffic originating from SCADA equipment.

Answer: (SHOW ANSWER)

NEW QUESTION: 72

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: ([SHOW ANSWER](#))

Fortinet Single Sign-On (FSSO) includes a method called passive authentication. This allows FortiGate to identify and authenticate a user based on their existing Windows login session without prompting the user again for credentials.

Because of this passive authentication, the user will not see a prompt for credentials when accessing resources protected by FortiGate.

This behavior is expected in FSSO deployments where FortiGate can retrieve user login information from the domain controller or through the FSSO agent.

The other options (Security Fabric, two-factor with RADIUS, FortiNAC DHCP fingerprint) are less relevant to this scenario or would not explain the lack of prompt during authentication.

NEW QUESTION: 73

With the limit of using one firewall device, the administrator enables multi-VDOM on FortiGate to provide independent multiple security domains to each ICS network.

Which statement ensures security protection is in place for all ICS networks?

- A. Each traffic VDOM must have a direct connection to FortiGuard services to receive the required security updates.
- B. The management VDOM must have access to all global security services.
- C. Each VDOM must have an independent security license.
- D. Traffic between VDOMs must pass through the physical interfaces of FortiGate to check for security incidents.

Answer: ([SHOW ANSWER](#))

In a multi-VDOM setup, one VDOM typically acts as the management VDOM (often called "root") which manages global settings and security services like FortiGuard updates.

This management VDOM handles access to global security services that benefit all traffic VDOMs.

Individual traffic VDOMs process their own traffic and enforce security policies but rely on the management VDOM for centralized access to global security services.

Each VDOM does not need an independent security license; the license is for the device as a whole.

Traffic between VDOMs does not need to pass through physical interfaces to be inspected; inter-VDOM links and policies handle traffic inspection.

Each VDOM does not require direct FortiGuard connections; this can be centralized in the management VDOM.

NEW QUESTION: 74

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

Answer: ([SHOW ANSWER](#))

FortiNAC continuously collects identity records, profiles, and classifies devices in OT networks using a variety of methods including active and passive scanning.

FortiGate contributes by providing session and flow data that helps in device identification and classification.

FortiSIEM aggregates security and operational data from various sources including FortiGate and FortiNAC to provide comprehensive visibility and identification.

NEW QUESTION: 75

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?

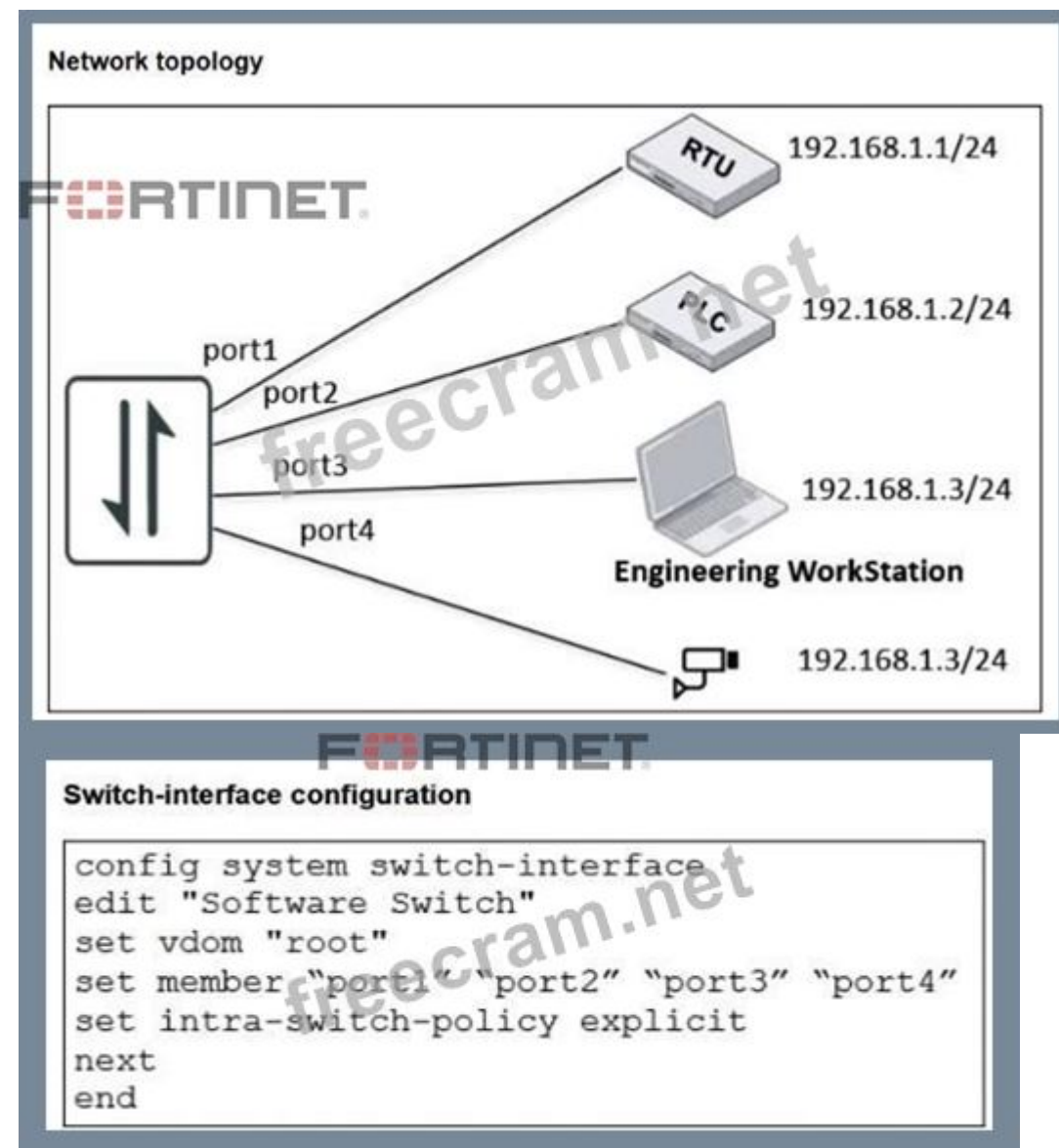
- A. FortiGate
- B. FortiEDR
- C. FortiSwitch
- D. FortiNAC

Answer: ([SHOW ANSWER](#))

Network Access Policies are used to dynamically provision access to connecting endpoints, based on the matched user/host profiles associated with the network access configuration.

NEW QUESTION: 76

Refer to the exhibits.



The network topology and the software-switch configuration are shown.

Why is Engineering Workstation not able to access the PLCs?

- A. Engineering Workstation and PLC are in different broadcast domains.

- B. The switch is not a layer 3 switch.
- C. The port2 and port3 interfaces do not have the same forward domain ID.
- D. A firewall policy to allow Engineering Workstation to access PLC is missing.

Answer: (SHOW ANSWER)

The software switch is configured with intra-switch-policy explicit, which means traffic between member interfaces is not allowed automatically. Communication from the Engineering Workstation on port3 to the PLC on port2 requires an explicit firewall policy permitting that access.

Valid NSE6_OTC_AR-7.6 Dumps shared by EduDump.com for Helping Passing NSE6_OTC_AR-7.6 Exam! EduDump.com now offer the **newest NSE6_OTC_AR-7.6 exam dumps**, the EduDump.com NSE6_OTC_AR-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com NSE6_OTC_AR-7.6 dumps with Test Engine here: https://www.edudump.com/exams/Fortinet/NSE6_OTC_AR-7.6/premium/ (153 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

Valid NSE6_OTC_AR-7.6 Dumps shared by EduDump.com for Helping Passing NSE6_OTC_AR-7.6 Exam! EduDump.com now offer the **newest NSE6_OTC_AR-7.6 exam dumps**, the EduDump.com NSE6_OTC_AR-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com NSE6_OTC_AR-7.6 dumps with Test Engine here: https://www.edudump.com/exams/Fortinet/NSE6_OTC_AR-7.6/premium/ (153 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)